FIPS 140-2 Non-Proprietary Security Policy for the Cisco MDS 9506, 9509, 9216i, and 9513 Multi-Layer SAN Switches

FIPS 140-2 Non-Proprietary Security Policy

Level 2 Validation

Document Version: Version 1.17

October 1, 2009

INTRODUCTION

This is a non-proprietary Cryptographic Module Security Policy for the MDS 9506, 9509, 9216i, and 9513 multi-layer SAN switches from Cisco Systems, Inc., referred to in this document as the modules, appliances, or as previously stated. This security policy describes how modules meet the security requirements of FIPS 140-2 and how to run the modules in a FIPS 140-2 mode of operation.

This policy was prepared as part of the Level 2 FIPS 140-2 validation of the MDS 9506, 9509, 9216i, and 9513 multi-layer SAN switches.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 - Security Requirements for Cryptographic Modules) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST website at http://csrc.nist.gov/groups/STM/cmvp/.

FIPS 140-2 Submission Package

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence
- Finite State Machine
- Other supporting documentation as additional references

With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Documentation is proprietary to Cisco Systems, Inc. and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Cisco Systems, Inc. See "Obtaining Technical Assistance" section on page 25 for more information.

FIPS 140-2 NON-PROPRIETARY SECURITY POLICY FOR THE CISCO MDS 9506, 9509, 9216I, AND 9513 MULTI-LAYER SAN SWITCHES

Overview

The Cisco MDS 9000 Series Multilayer SAN Switches can help lower the total cost of ownership of the most demanding storage environments. By combining a robust and flexible hardware architecture with multiple layers of network and storage-management intelligence, the Cisco MDS 9000 Series helps you build highly available, scalable storage networks with advanced security and unified management.

Consisting of the Cisco MDS 9500 Series of Multilayer Directors, the Cisco MDS 9200 Multilayer Fabric Switches, and the Cisco MDS 9100 Series of fixed configuration fabric switches, the Cisco MDS 9000 Family provides a full line of products to meet requirements for storage networks of all sizes and architectures. The Cisco MDS 9000 Family delivers intelligent network services such as virtual storage-area networks (VSANs), comprehensive security, advanced traffic management, sophisticated diagnostics, and unified SAN management. In addition, the Cisco MDS 9500 Series and the Cisco MDS 9200 Series provide multiprotocol and multitransport integration and an open platform for embedding intelligent storage services such as network-based virtualization. With its multilayer approach to network and storage intelligence, the Cisco MDS 9000 Family ushers in a new era in storage networking.

The Cisco MDS 9500 Multilayer Directors elevate the standard for director-class switches. Providing industry-leading availability, scalability, security, and management, the Cisco MDS 9500 Series allows you to deploy high-performance SANs with lowest TCO. Layering a rich set of intelligent features onto a high-performance, protocol-agnostic switch fabric, the Cisco MDS 9500 Series of Multilayer Directors addresses the stringent requirements of large-data-center storage environments. Available in 6- , 9- , and 13-slot configurations, the Cisco MDS 9500 Series supports up to 528 4/2/1-Gbps autosensing Fibre Channel ports in a single chassis and up to 1,056 Fibre Channel ports per rack. The Cisco MDS 9500 Series also supports up to 44 10-Gbps Fibre Channel ports. With an industry-leading 1.44 Tbps of system bandwidth, the Cisco MDS 9500 Series is ready for integration of future 8-Gbps modules.

This validation includes the Cisco MDS 9216i with its supervisor card, as well as the Cisco MDS 9506, 9509, and 9513 modules with one or two Supervisor 1 or Supervisor 2 cards. The following hardware and software version apply:

•Cisco MDS 9216i (hardware version 1)
•Cisco MDS 9506 (hardware version 1)
•Cisco MDS 9509 (hardware version 2)
•Cisco MDS 9513 (hardware version 1)
•Cisco MDS 9500 Series Supervisor 1 card (hardware version 16)
•Cisco MDS 9500 Series Supervisor 2 card (hardware version 4)
•Cisco MDS 9216i Supervisor card (hardware version 13)
•Cisco SAN OS version 3.2(2c) and NX-OS version 4.1(3a)

Module Validation Level

The following table lists the level of validation for each area in the FIPS PUB 140-2.

No.	Area Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	2
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key management	2
8	Electromagnetic Interface/Electromagnetic Compatibility	2
9	Self-Tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

Table 1 – Validation Level by Section

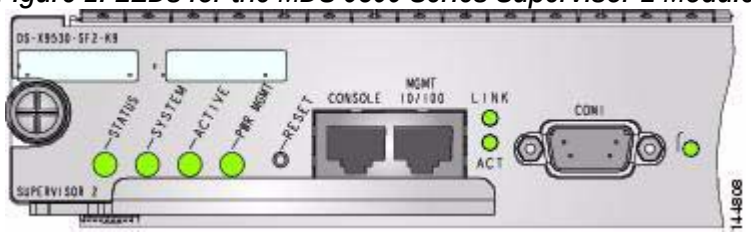
Physical Characteristics and Module Interfaces

The cryptographic boundary is defined as the module chassis. For the MDS 9506, MDS 9509, and MDS 9513 modules, one or two supervisor cards can be used and are included in the cryptographic boundary. The MDS 9216i has an integrated supervisor card.

The MDS modules require that a special opacity shield be installed over certain air vents to operate in FIPS-approved mode. The shield decreases the effective size of the vent holes, reducing visibility within the cryptographic boundary to FIPS-approved specifications. Detailed installation instructions for the shield are provided in the documentation that accompanies the shield in the FIPS kit.

Figure 1, Figure 2, and Figure 3 show the Cisco MDS 9000 series front panel LEDs.

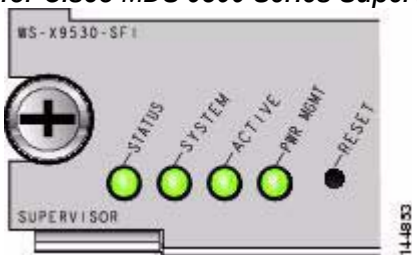
Figure 1: LEDs for the MDS 9500 Series Supervisor-2 Module



LED	Status	Description
Status	Green	All diagnostics pass. The module is operational (normal initialization sequence).
	Orange	One of the following occurs: •The module is booting or running diagnostics (normal initialization sequence). •An over temperature condition occurred (a minor threshold was exceeded during environmental monitoring).

	Red	One of the following occurred: •The diagnostic test failed. The module is not operational because a fault occurred during the initialization sequence. •An over temperature condition occurred (a major threshold was exceeded during environmental monitoring).
System	Green	All chassis environmental monitors are reporting OK.
	Orange	One of the following occurred: •The power supply failed or the power supply fan failed. •Incompatible power supplies are installed. •The redundant clock failed.
	Red	The temperature of the supervisor module exceeded the major threshold.
Active	Green	The Supervisor-2 module is operational and active.
	Orange	The Supervisor-2 module is in standby mode.
Pwr Mgmt	Green	Sufficient power is available for all modules.
	Orange	Sufficient power is not available for all modules.
Link	Green	MGMT 10/100/1000 ethernet link is up.
	Off	No link.
Act	Green	MGMT 10/100 ethernet activity traffic is flowing through port
	Off	No link or no traffic.
Compact Flash	Green	The external CompactFlash card is being accessed.
	Off	No activity.

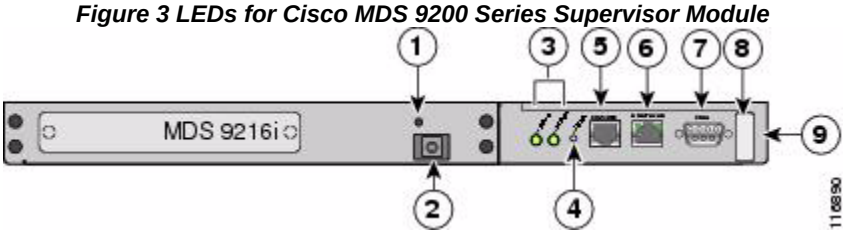
Figure 2 LEDs for Cisco MDS 9500 Series Supervisor-1 Module



LED	Status	Description
Status	Green	All diagnostics pass. The module is operational (normal initialization sequence).

	Orange	One of the following occurs: •The module is booting or running diagnostics (normal initialization sequence). •An over temperature condition occurred (a minor threshold was exceeded during environmental monitoring).
	Red	One of the following occurred: •The diagnostic test failed. The module is not operational because a fault occurred during the initialization sequence. •An over temperature condition occurred (a major threshold was exceeded during environmental monitoring).
System	Green	All chassis environmental monitors are reporting OK.
	Orange	One of the following occurred: •The power supply failed or the power supply fan failed. •Incompatible power supplies are installed. •The redundant clock failed.
	Red	The temperature of the supervisor module exceeded the major threshold.
Active	Green	The Supervisor module is operational and active.
	Orange	The Supervisor module is in standby mode.
Pwr Mgmt	Green	Sufficient power is available for all modules.
	Orange	Sufficient power is not available for all modules.

Figure 3 LEDs for Cisco MDS 9200 Series Supervisor Module



Item	LED Name	Status	Description
1	N/A	N/A	ESD socket (for ESD strap)
2	N/A	N/A	Grounding pad (beneath tape)
3	Status	Green	All diagnostics pass. The module is operational (normal initialization sequence).

		Orange	One of the following occurs or occurred: •The module is booting or running diagnostics (normal initialization sequence). •The inlet air temperature of the system exceeded the maximum system operating temperature limit (a minor environmental warning). To ensure maximum product life, you should immediately correct the environmental temperature and restore the system to normal operation.
		Red	One of the following occurred: •The diagnostic test failed. The module is not operational because a fault occurred during the initialization sequence. •The inlet air temperature of the system exceeded the safe operating temperature limits of the card (a major environmental warning). The card shut down to prevent permanent damage. The system will be shut down after two minutes if this condition is not cleared.
3	System	Green	All chassis environmental monitors are reporting OK
		Orange	One of the following occurs or occurred: •The power supply failed or the power supply fan failed. •Incompatible power supplies are installed. •The redundant clock failed.
		Red	The temperature of the supervisor module exceeded the major threshold.
4	N/A	N/A	Reset button.
5	N/A	N/A	Console port.
6	Link	Green	MGMT 10/100 Ethernet link is up.
		Off	No link
6	Activity	Green	MGMT 10/100 Ethernet traffic is flowing through port
		Off	No link or no traffic
7	N/A	N/A	COM1 port
8	N/A	N/A	Asset tag
9	N/A	N/A	9200 Series chassis

Each module provides a number of physical and logical interfaces to the device, and the physical interfaces provided by the module are mapped to four FIPS 140-2 defined logical interfaces: data input, data output, control input, and status output. The logical interfaces and their mapping are described in Table 2.

Table 2 Cisco MDS Series 9000 Physical Interface/Logical Interface Mapping

Physical Interface	FIPS 140-2 Logical Interface
MGMT Port	Data Input Interface
MGMT Port	Data Output Interface
MGMT Port	Control Input Interface

MGMT Port Status LED	Status Output Interface
Main Power Plug	Power Interface

Roles and Services

The module can be accessed via SSHv2 by the Crypto Officer role and the User role. Once a SSHv2 tunnel is established, all packets between the SSH client and the SSH server are encrypted/decrypted by the SSH session key.

As required by FIPS 140-2, there are two main roles in the module that operators may assume: a Crypto Officer role and User role. The modules support role-based authentication, and the respective services for each role are described in the "Crypto Officer Services" section on page 8, and the "User Services" section on page 8.

Crypto Officer Services

The Crypto Officer role is responsible for the configuration and maintenance of the module. The Crypto Officer can be authenticated by entering correct Crypto Officer username/password via SSH or SNMP v3 connection. In addition, the module can also authenticate the Crypto Officer via a valid Crypto Officer certificate issued by a trust Certificate Authority. The Crypto Officer services consist of the following:

- Configure the Module: define network interfaces and settings; set the protocols the module will support; enable interfaces and network services; set system date and time; load authentication information; generate SSH RSA/DSA keypairs; and configure authentication servers, filters and access lists for interfaces and users, and privileges
- Define Rules and Filters: create packet Filters that are applied to User data streams on each interface. Each Filter consists of a set of Rules, which define a set of packets to permit or deny based on characteristics such as protocol ID, addresses, ports, TCP connection establishment, or packet direction.
- Manage the Module: log off users, shutdown or reload the module, view complete configurations, view full status, manage user rights, and restore configurations.
- Perform Self Test: launch self test capabilities of the modules.

In addition to the above services, the Crypto Officer also has access to all User services listed below.

User Services

A User enters the system via an SSHv2 session or SNMP v3 on a MGMT port. In addition, the User role also can be authenticated using a valid User certificate issued by a trusted Certificate Authority. The module will prompt the User for their password. If the password is correct, the User is allowed entry to the executive program. The services available to the User role consist of the following:

- Status Functions: view the configuration, routing tables, image version currently running, module configurations, memory status, packet statistics, and view physical interface status.
- Network Functions: initiate diagnostic network services (i.e., ping and traceroute)

•Directory Services: display directory of files kept in flash memory, delete files in a directory,

Unauthenticated Services

While in an unauthenticated state, operation of module LEDs can be observed.

Critical Security Parameters

The services accessing the Critical Service Parameters (CSPs), the type of access, and which role accesses the CSPs, are listed in Table 3. CSPs are discussed more fully in Table 5.

CSP/Role/Service Access Policy	Critical Security Parameter	CSP 1	CSP 2	CSP 3	CSP 4	CSP 5	CSP 6	CSP 7
Role/Service								
User Role								
Status Functions								
Network Functions						rwd		
Directory Services								
Crypto-Officer Role								
Configure the Module		rwd	rwd	rwd	rwd	rwd	rwd	rwd
Define Roles and Filters		rwd	rwd	rwd	rwd	rwd	rwd	rwd
Status Functions								
Manage the Module		rwd	rwd	rwd	rwd	rwd	rwd	rwd

r = read w = write d = delete

Authentication Mechanisms

The module supports using a password for authenticating users. To log on to the modules for management purposes, an operator must connect to it using SSHv2 via the MGMT port and provide a password. Table 4 describes the estimated strength of the authentication mechanism.

Table 4 Estimated Strength of Authentication Mechanism

Authentication Type	Strength
Password mechanism	Passwords must be a minimum of 8 characters (see Secure Operation section of this document). The password can consist of alphanumeric values (a-z, A-Z, 0-9) yielding 62 choices per character. The probability of a successful random attempt is 1/62^8, which is less than 1/1,000,000.

Certificate based authentication	The modules supports a public key based authentication with 512, 768, 1024 or 2048 (for RSA) bit keys. A 1024-bit RSA key has at least 80-bits of equivalent strength. The probability of a successful random attempt is 1/2^80, which is less than 1/1,000,000. A 2048-bit RSA key has at least 112-bits of equivalent strength. The probability of a successful random attempt is 1/2^112, which is less than 1/1,000,000. 512-bit and 768-bit RSA key sizes are not supported in FIPS mode of operation.

The MDS 9506, 9509, 9216i, and 9513 multi-layer SAN switches provide protection against random authentication or password guessing within a one-minute period. Specifically:

•Using passwords: It is possible for an unauthorized user to enter one password per second. This would result in 60 attempts per one minute period. This would leave a probability of one in 500 million. Thus, the probability of an authentication within a one-minute period is much less than one in 100,000.

•Using RSA digital signatures: The MDS modules process 156,000 packets per second. With a 1024-bit RSA key of at least 80-bits of equivalent strength, the probability of gaining access to the module is one in (2^80)/156,000. Thus, the probability of a successful random authentication within a one-minute period is much less than one in 100,000.

Cryptographic Key Management

The appliances use a variety of Critical Security Parameters during operation. Table 5 includes a complete list of CSPs used by various services and protocols.

Table 5 Cryptographic Keys Used by the MDS 9000 Series Multi-Layer SAN Switches

#	Key/CSP Name	Generation/Algorithm	Description	Storage	Zeroization
1	Diffie-Hellman Key Pairs	ANSI X9.31 Appendix A.2.4 using the 2-key Triple DES Algorithm / DH	DH group 14 (2048 bits of keying strength)	SDRAM (plaintext)	Resetting or rebooting the module
2	SSH Host Keys	RSA/DSA	The SSH host keys (from the SSH host server) for the module. RSA public key sizes 1024 - 2048 bits; DSA key size 1024 bits	NVRAM (plain text)	SSH host keys are zeroized by either deleting them (via **no ssh key**) or by overwriting them with a new value of the key

3	SSH Session Keys	Diffie-Hellman	The SSH session keys for the module. These keys are agreed upon using DH between the module and SSH client. These keys are either Triple-DES or AES keys.	SDRAM (plain text)	SSH session keys are zeroized once the SSH session is closed.
4	SSH Client Keys	RSA/DSA	The SSH client keys are generated by the SSH client and used by the SSH client to connect to the SSH server. RSA public key sizes 1024 - 2048 bits; DSA key size 1024 bits	SDRAM (plain text)	SSH client keys are zeroized by rebooting or resetting the module.
5	Password table	User Generated Secret	Critical security parameters used to authenticate the User/Crypto officer logging in on to the machine	NVRAM (plain text)	Overwriting the passwords with new ones
6	RNG Seed	ANSI X9.31 Appendix A.2.4 using the 2-key Triple DES Algorithm	RNG Seed is a 64-bit seed for ANSI X9.31 Appendix A.2.4 using the 2-key Triple DES Algorithm	SDRAM (plaintext)	Resetting or rebooting the module
7	RNG Seed Key	ANSI X9.31 Appendix A.2.4 using the 2-key Triple DES Algorithm	RNG Seed Key is a 128-bit seed key for ANSI X9.31 Appendix A.2.4 using the 2-key Triple DES Algorithm	SDRAM (plaintext)	Resetting or rebooting the module

Self-Tests

The modules include an array of self-tests that are run during startup and periodically during operations to prevent any secure data from being released and to insure all components are functioning correctly. Table 6 lists the modules power-on self-tests:

Table 6 MDS 9000 Series Power-On Self-Tests

Implementation	Tests Performed
SAN OS and NX-OS	•Software/firmware Test •DSA KAT (signature/verification) •RSA KAT (signature/verification) •AES KAT •Triple DES KAT •SHA-1 KAT •HMAC SHA-1 KAT •RNG KAT

The modules perform all power-on self-tests automatically at boot. All power-on self-tests must pass before a User/Crypto Officer can perform services. The power-on self-tests are performed after the cryptographic systems are initialized but prior to the initialization of the network ports; this prevents the module from passing any data during a power-on self-test failure. In the unlikely event that a power-on self-test fails, the module's Status LED will turn RED, followed by a module reboot. An error message can be viewed via the **show logging nvram** command on the SSH Command Line Interface.

Table 7 lists the conditional self-tests performed by the modules.

Table 7 MDS 9000 Series Conditional Self-Tests

Implementation	Tests Performed
SAN OS and NX-OS	•Pairwise consistency test for RSA •Pairwise consistency test for DSA •Continuous Random Number Generator Test for the FIPS-approved RNGs and non-approved RNGs

Mitigation of Other Attacks

The modules do not claim to mitigate any attacks in a FIPS-approved mode of operation.

Secure Operation

The MDS 9506, 9509, 9216i, and 9513 multi-layer SAN switches meet FIPS 140-2 Level 2 requirements. This section describes how to place and keep the modules in a FIPS-approved mode of operation. Operating the modules without maintaining the following settings will remove the modules from the FIPS-approved mode of operation.

Crypto Officer Guidance - System Initialization

The modules were validated with SAN OS version 3.2(2c)and NX-OS 4.1(3a). This is the only allowable image for FIPS-approved mode of operation.
The Crypto Officer must configure and enforce the following initialization procedures:

Step 1 Disable diagnostic output to the console/VTY
switch# no debug all

Step 2 Define a User role password and a Crypto Officer role password. Ensure passwords are at least 8 characters long.

Step 3 Load User and Crypto Officer certificates into the module.

Step 4 Apply tamper evident labels as described in the "Tamper Evidence" section below.

Step 5 Configure the module into a FIPS mode of operation
enable fips mode

Step 6 Enable FIPS security logging
debug security events

Step 7 Ensure the persistent configuration contains the configuration necessary to enable FIPS mode of operation
copy running-config startup-config

Step 8 Reboot the module.

Note: After initial configuration, tamper evidence labels must be placed over the Console and COM1 ports as indicated in the Tamper Evidence section of this policy. Subsequent configuration of the module must take place using SSHv2 sessions via the MGMT port.

Crypto Officer Guidance - System Configuration

Note: The MDS module web interface cannot be used for device configuration. To operate in FIPS mode, the Crypto Officer must perform the following steps:

Step 1 Configure the module such that any remote connections via SSHv2 are secured using FIPS-approved algorithms.
Step 2 Configure SNMP v3 using FIPS-approved algorithms for authenticated, secure SNMP gets and sets.

Note: The SNMP v3 protocol derives the SNMP v3 session key from the User Password to encrypt or decrypt the packets between the SNMP v3 manager and agents. Since password-based key derivation methods are not to be used in the FIPS mode, these exchanged packets will be considered as plaintext in FIPS mode of operation.

Note: RADIUS/TACACS+ is not supported in the FIPS mode of operation.

Note: The following FIPS-approved protocols are not allowed in FIPS mode of operation for this validation
- IPSec
- IKE

Approved Cryptographic Algorithms

The appliances support many different cryptographic algorithms; however, only the following FIPS approved algorithms may be used while in the FIPS mode of operation:

- AES encryption/decryption
- Triple DES encryption/decryption
- SHA-1 hashing
- HMAC-SHA-1 for hashed message authentication
- RSA signing and verifying
- DSA signing and verifying
- RNG based on ANSI X9.31 Appendix A.2.4 using the 2-key Triple DES algorithm

Note: Pursuant to the DES Transition Plan and the approval of the Withdrawal of Federal Information Processing Standard (FIPS) 46-3, Data Encryption Standard (DES); FIPS 74, Guidelines for Implementing and Using the NBS Data Encryption Standard; and FIPS 81, DES Modes of Operation, the DES algorithm should not be used in FIPS approved mode of operation. For the DSA algorithm, key sizes of only 1024 bits (key strength of 80 bits) can be used in FIPS mode of operation.

Each cryptographic implementation of the SAN OS software has achieved the certifications listed in *Table 8 Algorithm Certificates*

Algorithm	Supervisor 1	Supervisor 2
AES	662	663
Triple DES	609	610
DSA	245	246
SHS	695	696
RNG	382	383
RSA	306	307
HMAC-SHA-1	344	345

Each cryptographic implementation of the NX-OS software has achieved the certifications listed in *Table 9 Algorithm Certificates*

Algorithm	Supervisor 1 and Supervisor 2
AES	1188
Triple DES	856
DSA	392
SHS	1095
RNG	656
RSA	569
HMAC-SHA-1	688

Non-FIPS Approved Algorithms Allowed in FIPS Mode

The modules implement the following non-FIPS-approved cryptographic algorithms, but allowed in FIPS mode:

- Diffie-Hellman (allowed for use in FIPS mode) (key agreement; key establishment methodology provides 112 bits of encryption strength)

Non-FIPS Approved Algorithms

The modules implement the following non-FIPS-approved cryptographic algorithms:

- DES
- RC4
- MD5
- MD5 HMAC

Non-FIPS approved algorithms cannot be used in FIPS mode of operation.

Opacity Shields

To operate in FIPS mode, each MDS module must have a shield installed to ensure proper conformance to FIPS opacity requirements. These opacity shields are included in a separately orderable FIPS Kit (Part Number DS-FIPS-KIT=). The shields are installed on the left side (as you face the front) of the module as follows:

Step 1 Unpack the included fasteners (both pushpin actuators and expanding grommets).
Step 2 Align the opacity shield on the left side of the module such that the straight cut, open end is toward the front of the module and the closed end is towards the rear. Locate the mounting holes toward the outside of the shield (three each, top and bottom). Do not use the mounting holes along the middle of the shield.
Step 3 Beginning with one of the upper corners, place one expanding grommet in a mounting hole.

Note: It is recommended to use an awl or similar object to break a small hole through the opacity foam material. This facilitates passing the grommet through the material. It is important that these grommets are free of material during installation.

Step 4 With one grommet inserted, place the shield against the left side of the module chassis, aligning the grommet with the upper most corner hole in the chassis. Hold the shield in place.
Step 5 Firmly insert a pushpin actuator into the expanding grommet.
Step 6 Align the other upper corner mounting hole with a corresponding hole in the chassis. Place one expanding grommet in the hole, followed by a pushpin actuator. Repeat for the remaining mounting holes along the outside edges of the shield.

Note: The opacity shield frame does bow, so you may need to apply pressure to install along the mid-hardware locations.

Tamper Evidence

All Critical Security Parameters are stored and protected within each appliance's tamper evident enclosure. The Crypto Officer is responsible for properly placing all tamper evident labels. The security labels recommended for FIPS 140-2 compliance are provided in the FIPS Kit (Part Number DS-FIPS-KIT=). These security labels are very fragile and cannot be removed without clear signs of damage to the labels.

The Crypto Officer should inspect the tamper evident labels periodically to verify they are intact and the serial numbers on the applied tamper evident labels match the records in the security log.

To operate in a FIPS compliant mode, any slot not populated with a module must be populated with an appropriate slot cover. The slot covers are included with each module, and additional covers may be ordered from Cisco. The following procedures must be followed to apply tamper evidence labels on modules or slot covers:

Figure 4 MDS 9506 Front Tamper Evident Label Placement

Figure 5 MDS 9506 Rear Tamper Evident Label Placement

Figure 6 MDS 9506 Right Side Tamper Evident Label Placement

Step 1 Turn off and unplug the system before cleaning the chassis and applying labels.
Step 2 Clean the chassis of any grease, dirt, or oil before applying the tamper evident labels. Alcohol-based cleaning pads are recommended for this purpose.
Step 3 Two tamper evidence labels should be placed so that one half of each tamper evidence label covers the front of the fan-bank module and the other half covers the module case. Any attempt to remove the fan-bank will leave tamper evidence.
Step 4 For each supervisor module or module cover installed in the chassis, place a tamper evidence label so that one half of the label covers the right side of the supervisor module or module cover and the other half covers the right side of the chassis. Any attempt to remove a module will leave tamper evidence.
Step 5 For each power supply or power supply cover installed in the module, place a tamper evidence label so that one half of the label covers the enclosure and the other half covers the front of the power supply or power supply cover. Any attempt to install or remove a power supply will leave tamper evidence.
Step 6 For each supervisor module installed, place a tamper evidence label so that one half of the label covers the Compact Flash slot. Any attempt to install or remove a Compact Flash card will leave tamper evidence.
Step 7 Two tamper evidence labels (one on the top, and one on the bottom) should be placed so that one half of each label attaches to one side of the opacity shield, and the other half attaches to the chassis itself. Any attempt to remove the opacity shield will leave tamper evidence.
Step 8 Place one tamper evidence label over the Console port and one label over the COM1 port. Any attempt to access either of these ports will leave tamper evidence.
Step 9 Record the serial numbers of the labels applied to the system in a security log.

The tamper evident seals are produced from a special thin gauge vinyl with self-adhesive backing. Any attempt to open the device will damage the tamper evident seals or the material of the modules cover. Because the tamper evident seals have non-repeated serial numbers, they may be inspected for damage and compared against the applied serial numbers to verify that the modules has not been tampered with. Tamper evident seals can also be inspected for signs of tampering, which include the following: curled corners, rips, and slices. The word “OPEN” may appear if the label was peeled back.

Figure 7 MDS 9509 Front Tamper Evident Label Placement

Figure 8 MDS 9509 Right Side Tamper Evident Label Placement

Step 1 Turn off and unplug the system before cleaning the chassis and applying labels.
Step 2 Clean the chassis of any grease, dirt, or oil before applying the tamper evident labels. Alcohol-based cleaning pads are recommended for this purpose.
Step 3 Two tamper evidence labels should be placed so that one half of each tamper evidence label covers the front of the fan-bank module and the other half covers the module case. Any attempt to remove the fan-bank will leave tamper evidence.
Step 4 For each supervisor module or module cover installed in the chassis, place a tamper evidence label so that one half of the label covers the right side of the supervisor module or module cover and the other half covers the right side of the chassis. Any attempt to remove a module will leave tamper evidence.
Step 5 For each power supply or power supply cover installed in the module, place a tamper evidence label so that one half of the label covers the enclosure and the other half covers the front of the power supply or power supply cover. Any attempt to install or remove a power supply will leave tamper evidence.
Step 6 For each supervisor module installed, place a tamper evidence label so that one half of the label covers the Compact Flash slot. Any attempt to install or remove a Compact Flash card will leave tamper evidence.
Step 7 Two tamper evidence labels (one on the top, and one on the bottom) should be placed so that one half of each label attaches to one side of the opacity shield, and the other half attaches to the chassis itself. Any attempt to remove the opacity shield will leave tamper evidence.
Step 8 Place one tamper evidence label over the Console port and one label over the COM1 port. Any attempt to access either of these ports will leave tamper evidence.
Step 9 Record the serial numbers of the labels applied to the system in a security log.

The tamper evident seals are produced from a special thin gauge vinyl with self-adhesive backing. Any attempt to open the device will damage the tamper evident seals or the material of the modules cover. Because the tamper evident seals have non-repeated serial numbers, they may be inspected for damage and compared against the applied serial numbers to verify that the modules has not been tampered with. Tamper evident seals can also be inspected for signs of tampering, which include the following: curled corners, rips, and slices. The word “OPEN” may appear if the label was peeled back.

MDS 9216i

Figure 9 MDS 9216i Front Tamper Evident Label Placement

Figure 10 MDS 9216i Rear Tamper Evident Label Placement

Figure 11 MDS 9216i Right Side Tamper Evident Label Placement

Step 1 Turn off and unplug the system before cleaning the chassis and applying labels.
Step 2 Clean the chassis of any grease, dirt, or oil before applying the tamper evident labels. Alcohol-based cleaning pads are recommended for this purpose.
Step 3 Two tamper evidence labels should be placed so that one half of each tamper evidence label covers the front of the fan-bank module and the other half covers the module case. Any attempt to remove the fan-bank will leave tamper evidence.
Step 4 For each supervisor module or module cover installed in the chassis, place a tamper evidence label so that one half of the label covers the right side of the supervisor module or module cover and the other half covers the right side of the chassis. Any attempt to remove a module will leave tamper evidence.
Step 5 For each power supply or power supply cover installed in the module, place a tamper evidence label so that one half of the label covers the enclosure and the other half covers the front

of the power supply or power supply cover. Any attempt to install or remove a power supply will leave tamper evidence.

Step 6 For each supervisor module installed, place a tamper evidence label so that one half of the label covers the Compact Flash slot. Any attempt to install or remove a Compact Flash card will leave tamper evidence.

Step 7 Two tamper evidence labels (one on the top, and one on the bottom) should be placed so that one half of each label attaches to one side of the opacity shield, and the other half attaches to the chassis itself. Any attempt to remove the opacity shield will leave tamper evidence.

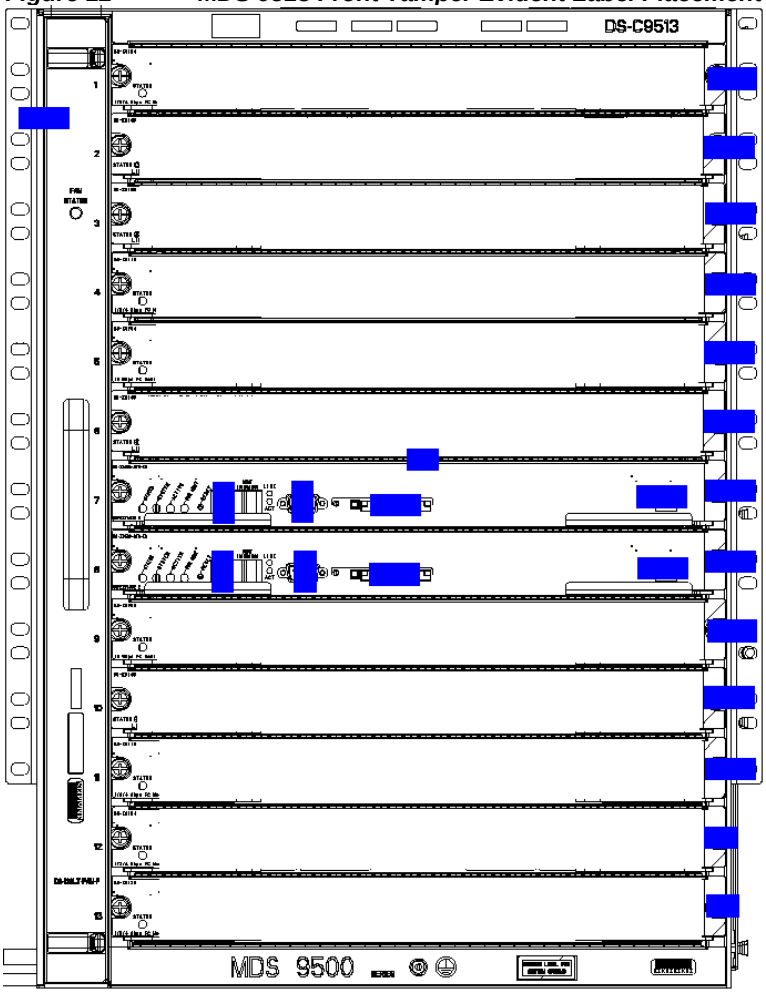
Step 8 Place one tamper evidence label over the Console port and one label over the COM1 port. Any attempt to access either of these ports will leave tamper evidence.

Step 9 Record the serial numbers of the labels applied to the system in a security log.

The tamper evident seals are produced from a special thin gauge vinyl with self-adhesive backing. Any attempt to open the device will damage the tamper evident seals or the material of the modules cover. Because the tamper evident seals have non-repeated serial numbers, they may be inspected for damage and compared against the applied serial numbers to verify that the modules has not been tampered with. Tamper evident seals can also be inspected for signs of tampering, which include the following: curled corners, rips, and slices. The word “OPEN” may appear if the label was peeled back.

MDS 9513

Figure 12 MDS 9513 Front Tamper Evident Label Placement



Step 1 Turn off and unplug the system before cleaning the chassis and applying labels.

Step 2 Clean the chassis of any grease, dirt, or oil before applying the tamper evident labels. Alcohol-based cleaning pads are recommended for this purpose.
Step 3 For each supervisor module or module cover installed in the chassis, place a tamper evidence label so that one half of the label covers the right side of the supervisor module or module cover and the other half covers the right side of the chassis. Any attempt to remove a supervisor module or cover will leave tamper evidence.
Step 4 Two tamper evidence labels (one on the top, and one on the bottom) should be placed so that on half of each label attaches to the front side of the module, and the other half attaches to the left side of the module.
Step 5 For each power supply or power supply cover installed in the module, place a tamper evidence label so that one half of the label covers the enclosure and the other half covers the front of the power supply or power supply cover. Any attempt to install or remove a power supply will leave tamper evidence.
Step 6 For each supervisor module installed, place a tamper evidence label so that one half of the label covers the Compact Flash slot. Any attempt to install or remove a Compact Flash card will leave tamper evidence.
Step 7 Two tamper evidence labels (one on the top, and one on the bottom) should be placed so that one half of each label attaches to one side of the opacity shield, and the other half attaches to the chassis itself. Any attempt to remove the opacity shield will leave tamper evidence.
Step 8 Place one tamper evidence label over the Console port and one label over the COM1 port. Any attempt to access either of these ports will leave tamper evidence.
Step 9 Record the serial numbers of the labels applied to the system in a security log.

The tamper evident seals are produced from a special thin gauge vinyl with self-adhesive backing. Any attempt to open the device will damage the tamper evident seals or the material of the modules cover. Because the tamper evident seals have non-repeated serial numbers, they may be inspected for damage and compared against the applied serial numbers to verify that the modules has not been tampered with. Tamper evident seals can also be inspected for signs of tampering, which include the following: curled corners, rips, and slices. The word “OPEN” may appear if the label was peeled back.

Related Documentation

This document deals only with operations and capabilities of the modules in the technical terms of a FIPS 140-2 cryptographic device security policy. More information is available on the modules from the sources listed in this section and from the following source:

- The NIST Cryptographic Module Validation Program website (http://csrc.nist.gov/groups/STM/cmvp/index.html) contains contact information for answers to technical or sales-related questions for the modules.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL: http://www.cisco.com/techsupport
You can access the Cisco website at this URL: http://www.cisco.com

You can access international Cisco websites at this URL:
http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL: http://www.cisco.com/go/marketplace/

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL: http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco SystemsAttn:
Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:
http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- •Report security vulnerabilities in Cisco products.
- •Obtain assistance with security incidents that involve Cisco products.
- •Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:
http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:
http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- •Emergencies — security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- •Nonemergencies — psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- •1 877 228-7302
- •1 408 525-6532

Tip: We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*. Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:
http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html
The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if

you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL: http://www.cisco.com/techsupport
Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL: http://tools.cisco.com/RPF/register/register.do

Note: Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the Tools & Resources link under Documentation & Tools. Choose Cisco Product Identification Tool from the Alphabetical Index drop-down list, or click the Cisco Product Identification Tool link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting show command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:
http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:
Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)EMEA: +32 2 704 55 55USA: 1 800 553-2447
For a complete list of Cisco TAC contacts, go to this URL:
http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL: http://www.cisco.com/go/marketplace/
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL: http://www.ciscopress.com
- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL: http://www.cisco.com/packet
- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL: http://www.cisco.com/go/iqmagazine or view the digital edition at this URL: http://ciscoiq.texterity.com/ciscoiq/sample/
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL: http://www.cisco.com/ipj
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL: http://www.cisco.com/en/US/products/index.html

• Networking Professionals Connection is an interactive website for networking professionals ng products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:Networking Professionals Connection is an interactive website for networking professionals to share http://www.cisco.com/discuss/networking
•World-class networking training is available from Cisco. You can view current offerings at this URL: http://www.cisco.com/en/US/learning/index.html