

Catalyst 6509 Switch, Cisco 7606 Router, and Cisco 7609 Router with VPN Services Module Certification Note

This is the non-proprietary Cryptographic Module Security Policy for the Catalyst 6509 switch and the Cisco 7606 and Cisco 7609 routers with the VPN Services Module:

- Hardware Version
 - Catalyst 6509 switch
 - Cisco 7606 router
 - Cisco 7609 router
- Backplane chassis
 - Hardware Version 3.0 (Catalyst 6509 switch)
 - Hardware Version 1.0 (Cisco 7606 router)
 - Hardware Version 1.0 (Cisco 7609 router)
- Supervisor Engine—Hardware Version 3.2
- VPN Services Module—Hardware Version 1.2; Firmware Version; 12.2(14)SY3

This security policy describes how the Catalyst 6509 switch and the Cisco 7606 and Cisco 7609 routers with the VPN Services Module meet the security requirements of FIPS 140-2, and describes how to operate the hardware devices in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the Catalyst 6509 switch and the Cisco 7606 and Cisco 7609 routers with the VPN Services Module.

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/cryptval/.



Contents

This document contains the following sections:

- References, page 2
- Document Organization, page 2
- Catalyst 6509 Switch and Cisco 7606 and Cisco 7609 Routers, page 4
- Catalyst 6509/Cisco 7606/Cisco 7609 Cryptographic Module, page 6
- Roles and Services, page 10
- Installing the Opacity Shield on the Catalyst 6509 Switch, page 12
- Installing the Opacity Shield on the Cisco 7600 Series Routers, page 15
- Physical Security, page 18
- Cryptographic Key Management, page 21
- Key Zeroization, page 25
- Self-Tests, page 25
- Secure Operation of the Catalyst 6509 Switch and the Cisco 7606 and Cisco 7609 Routers, page 26
- Obtaining Documentation and Submitting a Service Request, page 28

References

This publication deals only with operations and capabilities of the Catalyst 6509 switch and the Cisco 7606 and Cisco 7609 routers in the technical terms of a FIPS 140-2 Cryptographic Module Security Policy. More information is available on the Catalyst 6509 switch and the Cisco 7606 and Cisco 7609 routers and the entire Catalyst 6500 series switches and Cisco 7600 series routers from the following sources:

The Catalyst 6500 series switch product descriptions can be found at:

http://www.cisco.com/en/US/products/hw/switches/ps708/index.html

• The Cisco 7600 series router product descriptions can be found at:

http://www.cisco.com/en/US/products/hw/routers/ps368/index.html

- For answers to technical or sales related questions, refer to the contacts listed on the Cisco Systems website at www.cisco.com.
- For answers to technical or sales-related questions for the module, refer to the NIST Validated Modules website at http://csrc.nist.gov/cryptval.

Document Organization

The Security Policy document is part of the FIPS 140-2 Submission Package. The Submission Package also contains the following documents:

- Vendor Evidence
- Finite State Machine
- Module Software Listing

• Other supporting documentation as additional references

This publication provides an overview of the Catalyst 6509 switch and the Cisco 7606 and Cisco 7609 routers and explains the secure configuration and operation of the modules. This introduction section is followed by the "Catalyst 6509 Switch and Cisco 7606 and Cisco 7609 Routers" section which details the general features and functionality of the Catalyst 6509 switch and Cisco 7606 and Cisco 7609 routers. The "Secure Operation of the Catalyst 6509 Switch and the Cisco 7606 and Cisco 7609 Routers" section specifically addresses the required configuration for the FIPS-approved mode of operation.

With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Submission documentation is Cisco-proprietary and is releasable only under appropriate non-disclosure agreements. For access to these documents, contact Cisco Systems.

Catalyst 6509 Switch and Cisco 7606 and Cisco 7609 Routers

Branch office networking requirements are dramatically evolving, driven by web and e-commerce applications to enhance productivity and merging the voice and data infrastructure to reduce costs. The Catalyst 6509 switch and the Cisco 7606 and Cisco 7609 routers with the VPN Services Module offer versatility, integration, and security to branch offices. With numerous network modules and service modules available, the modular architecture of the Cisco router easily allows interfaces to be upgraded to accommodate network expansion. The Catalyst 6509 switch and the Cisco 7606 and Cisco 7609 routers provide a scalable, secure, manageable remote access server that meets FIPS 140-2 Level 2 requirements, as a multi-chip standalone module. This section describes the general features and functionality provided by the Catalyst 6509 switch (see Figure 1), the Cisco 7606 router (see Figure 2), and the Cisco 7609 router (see Figure 3).



Figure 1

Catalyst 6509 Switch





Catalyst 6509/Cisco 7606/Cisco 7609 Cryptographic Module

The cryptographic boundary is defined as encompassing the following:

- Top, front, left, right, and bottom surfaces of a chassis.
- All portions of the backplane of the chassis that are not designed to accommodate a network module or a service module.
- The inverse of the three-dimensional space within the chassis that would be occupied by any installed network module or a service module which does not perform approved cryptographic functions, or any installed power supply.
- The connection apparatus between the network module or service module and the motherboard and daughterboard that hosts the network module or service module.

The cryptographic boundary does not include the network module or service module itself unless it performs approved cryptographic functions. In other words, the cryptographic boundary encompasses all hardware components within the chassis except any installed nonapproved cryptographic network modules or service modules and the power supply submodules. Service modules that are currently available include the Network Access Module (NAM), a Firewall Services Module, and a VPN Services Module. All of the functionality described in this publication is provided by components within this cryptographic boundary.

The service modules require that a special opacity shield be installed over the intake-side air vents in order to operate in FIPS-approved mode. The shield decreases the surface area of the vent holes, reducing visibility within the cryptographic boundary to FIPS-approved specifications. Detailed installation instructions for the shield are provided in this publication.

The Catalyst 6509 switch and the Cisco 7606 and Cisco 7609 routers incorporate a single VPN Services Module cryptographic accelerator card. The VPN Services Module is installed in a chassis module slot.

Cisco IOS features such as tunneling, data encryption, and termination of remote access WANs using IPsec, Layer 2 forwarding and Layer 2 tunneling protocols make the Catalyst 6509 switch and the Cisco 7606 and Cisco 7609 routers with VPN Services Module an ideal platform for building virtual private networks or outsourced dial solutions. The RISC-based processor provides the power needed for the dynamic requirements of the remote branch office.

Module Interfaces

The switch and router chassis physical interfaces are located on the supervisor engine front panel. (See Figure 4.)



Figure 4 Supervisor Engine Physical Interfaces

The Catalyst 6509 switch and the Cisco 7606 and Cisco 7609 routers provide console ports, fixed Ethernet interfaces, nine network and service module slots on the Catalyst 6509 switch and Cisco 7609 router chassis, and six network and service module slots on the Cisco 7606 router chassis. Network modules support a variety of LAN and WAN connectivity interfaces, such as the following: Ethernet, ATM, serial, ISDN BRI, and integrated CSU/DSU options for primary and backup WAN connectivity.

An network module or a service module is installed in one of the chassis slots, which are located on the front panel of the chassis. The modules interface directly with the supervisor engine, and cannot perform cryptographic functions; they only serve as a data input and data output physical interface.

The supervisor engine has two Ethernet uplink ports. The supervisor engine also has an RJ-45 connector for a console terminal for local system access. The Ethernet ports have LINK LEDs. Power is supplied to the module from the power supply through the backplane. Figure 4 shows the LEDs located on the Catalyst 6509 switch and the Cisco 7606 and Cisco 7609 routers. Table 1 describes the LEDs.

LED	Color/State	Description	
STATUS	Green	All diagnostics pass. The module is operational (normal initialization sequence).	
	Orange	The module is booting or running diagnostics (normal initialization sequence).	
		An over-temperature condition has occurred. (A minor temperature threshold has been exceeded during environmental monitoring.)	
	Red	The diagnostic test failed. The module is not operational because a fault occurred during the initialization sequence.	
		An over-temperature condition has occurred. (A major temperature threshold has been exceeded during environmental monitoring.)	
SYSTEM ¹	Green	All chassis environmental monitors are reporting OK.	
	Orange	The power supply has failed or the power supply fan has failed.	
		Incompatible power supplies are installed.	
		The redundant clock has failed.	
		One VTT ² module has failed or the VTT module temperature minor threshold has been exceeded.	
	Red	Two VTT modules fail or the VTT module temperature major threshold has been exceeded.	
		The temperature of the supervisor engine major threshold has been exceeded. ³	
ACTIVE	Green	The supervisor engine is operational and active.	
	Orange	The supervisor engine is in standby mode.	
POWER MGMT	Green	Sufficient power is available for all modules.	
	Orange	Sufficient power is not available for all modules.	
SWITCH LOAD		If the switch is operational, the switch load meter indicates (as an approximate percentage) the current traffic load over the backplane.	
PCMCIA		The PCMCIA LED is lit when no Flash PC card is installed in the slot, and it goes off when you insert a Flash PC card.	
LINK	Green	The port is operational.	
	Orange	The link has been disabled by software.	
	Flashing Orange	The link is bad and has been disabled due to a hardware failure.	
	Off	No signal is detected.	

Table 1 Catalyst 6509 Switch and Cisco 7606 and 7609 Router LEDs

LED	Color/State	Description		
VPN Services Module				
STATUS	STATUS Green All non-FIPS-related diagnostic tests pass. The n operational. ⁴			
	Red	A diagnostic test other than an individual port test failed.		
	Orange	Indicates one of three conditions:		
	• The module is running through its boot an sequence.			
		• The module is disabled.		
• The module is in the shutdown state.		• The module is in the shutdown state.		
	Off	The module power is off.		

Table 1 Catalyst 6509 Switch and Cisco 7606 and 7609 Router LEDs (continued)

1. The SYSTEM and PWR MGMT LED indications on a redundant supervisor engine are synchronized to the active supervisor engine.

2. VTT = voltage termination module. The VTT module terminates signals on the Catalyst switching bus.

3. If no redundant supervisor engine is installed and there is a VTT module minor or major over-temperature condition, the system shuts down.

4. Enter the show crypto eli command to determine whether the FIPS-related self-tests passed.

All of these physical interfaces are separated into the logical interfaces from FIPS 140-2 as described in Table 2.

Table 2 FIPS 140-2 Logical Interfaces

Switch and Router Physical Interfaces	FIPS 140-2 Logical Interface
Ethernet ports	Data input interface
Network and service module interfaces	
Console port	
Compact flash (PCMCIA) slot	
Ethernet ports	Data output interface
Network and service module interfaces	
Console port	
Compact flash (PCMCIA) slot	
Ethernet ports	Control input interface
Network and service module interfaces	
Console port	
Reset button	

Switch and Router Physical Interfaces	FIPS 140-2 Logical Interface	
Ethernet ports	Status output interface	
Network and service module interfaces		
STATUS LED (Supervisor Engine 2)		
SYSTEM LED		
ACTIVE LED		
PWR MGMT LED		
PCMCIA LED		
Switch Load LED		
Network Port LINK LEDs		
STATUS LED (VPN Services module)		
CONSOLE Port		
Backplane	Power interface	

Table 2 FIPS 140-2 Logical Interfaces (continued)

Roles and Services

Authentication is role-based. There are two main roles in the router that operators may assume: the crypto officer role and the user role. The administrator of the router assumes the crypto officer role in order to configure and maintain the router using crypto officer services, while the users only use the basic user services. Both roles are authenticated by providing a valid username and password. The configuration of the encryption and decryption functionality is performed only by the crypto officer after authentication to the crypto officer role by providing a valid crypto officer username and password. After the crypto officer configures the encryption and decryption functionality, the user can use this functionality after authentication to the user role by providing a valid user username and password. The crypto officer can also use the encryption and decryption functionality after authentication to the crypto officer role by providing a valid user username and password. The crypto officer can also use the encryption and decryption functionality after authentication to the crypto officer role by providing a valid user username and password. The crypto officer can also use the encryption and decryption functionality after authentication to the crypto officer role.

The module supports RADIUS and TACACS+ for authentication and they are used in the FIPS mode. A complete description of all the management and configuration capabilities of the Catalyst 6509 switch and the Cisco 7606 and Cisco 7609 routers can be found in the *Performing Basic System Management* manual and in the online help for the switch or the router.

The user and crypto officer passwords and the RADIUS/TACACS+ shared secrets must each be at least eight alphanumeric characters in length. If only the integers 0 to 9 are used without repetition for an 8-digit PIN, the probability of randomly guessing the correct sequence is 1 in 1,814,400. If you include the rest of the alphanumeric characters, the probability of guessing the correct sequence is decreased drastically. See the "Secure Operation of the Catalyst 6509 Switch and the Cisco 7606 and Cisco 7609 Routers" section on page 26 for more information.

Crypto Officer Role

During initial configuration of the router, the crypto officer password (the "enable" password) is defined. A crypto officer may assign permission to access the crypto officer role to additional accounts, which creates additional crypto officers.

The crypto officer role is responsible for the configuration and maintenance of the router. The crypto officer services consist of the following:

- Configuring the router—Defines network interfaces and settings, creates command aliases, sets the protocols the switch or router will support, enables interfaces and network services, sets system date and time, and loads authentication information.
- Defining rules and filters—Creates 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 characteristics such as protocol ID, addresses, ports, TCP connection establishment, or packet direction.
- Status functions—Views the router configuration, routing tables, and active sessions, uses the **Get** commands to view SNMP MIB II statistics, health, temperature, memory status, voltage, and packet statistics, reviews accounting logs, and views physical interface status.
- Managing the switch or the router—Logs off users, shuts down or reloads the switch or router, manually backs up switch or router configurations, views complete configurations, manages user rights, and restores switch or router configurations.
- Setting encryption and bypass—Sets up the configuration tables for IP tunneling. Sets keys and algorithms to be used for each IP range or allow plaintext packets to be set from a specified IP address.
- Changing port adapters—Inserts and removes adapters in a port adapter slot.

User Services

A user enters the system by accessing the console port with a terminal program. Cisco IOS prompts the user for their password. If the password is correct, the user is allowed entry to the Cisco IOS executive program. The user services consist of the following:

- Status functions—Views state of interfaces, state of Layer 2 protocols, and version of Cisco IOS currently running.
- Network functions—Connects to other network devices (using outgoing TELNET or PPP) and initiates diagnostic network services (that is, ping, mtrace).
- Terminal functions—Adjusts the terminal session (for example, locks the terminal, adjusts flow control).
- Directory Services—Displays the directory of files kept in flash memory.

Installing the Opacity Shield on the Catalyst 6509 Switch

The opacity shield is designed to be installed while the Catalyst 6509 switch is operating without creating an electrical hazard or damage to the system. You will need some clearance between adjacent racks in order to perform this procedure.

To install an opacity shield on the Catalyst 6509 switch (see Figure 5), follow these steps:

- Step 1 The opacity shield is designed to be installed on a Catalyst 6509 chassis that is already rack-mounted. If your Catalyst 6509 chassis is not rack-mounted, install the chassis in the rack using the procedures contained in the *Catalyst 6500 Series Switches Installation Guide*. If your Catalyst 6509 chassis is already rack-mounted, proceed to step 2.
- **Step 2** Open the FIPS kit packaging (part number CVPN6500FIPS/KIT=). The kit contains the following items:
 - A packaged opacity shield assembly with installation hardware for the Catalyst 6509 and Catalyst 6509-E switch chassis (part number 800-26335-xx).
 - A packaged opacity shield assembly with installation hardware for the Catalyst 6506 and Catalyst 6506-E switch chassis (part number 800-27009-xx).
 - An envelope with 60 FIPS tamper evidence labels.
 - An envelope containing a disposable ESD wrist strap.

Note

The opacity shield part number is located on the outside of the protective packaging.

- **Step 3** Remove the bag with the part number 800-26335-xx. This is the opacity shield kit for the Catalyst 6509 switch chassis. Set the other opacity shield kit aside.
- Step 4 Open the protective packaging and remove the opacity shield and the two bags of installation hardware. The opacity shield is identified by the label 6509-E that is silk-screened adjacent to some of the holes on the shield. Retain the fastener bag labeled 69-1482-xx. Set the second bag of installation hardware aside; you will not need it for this installation.
- Step 5 Open the bag of installation hardware and remove two M3 thumbscrews and four M3 snap rivet fasteners. The snap rivet fasteners come assembled; you need to separate the two pieces of the snap rivet fastener by removing the snap rivet pin from the snap rivet sleeve before you install them in the opacity shield.



Extra snap fasteners are included in the bag of installation hardware in case of loss or damage.

- **Step 6** Start the two M3 thumbscrews in the corresponding M3 threaded holes. (The two M3 threaded holes do not have a 6509-E silk-screened next to them.) Do not thread the thumbscrews too far into the opacity shield; two or three turns are sufficient.
- **Step 7** Open the envelope containing the disposable ESD wrist strap. Attach the disposable ESD wrist strap to your wrist. Attach the other end of the wrist strap to exposed metal on the chassis.
- **Step 8** Position the opacity shield over the air intake side of the chassis so that the two thumbscrews on the opacity shield are aligned with the unused top and bottom L-bracket screw holes on the chassis.
- **Step 9** Press the opacity shield firmly against the side of the chassis and secure the opacity shield to the chassis with the two thumbscrews.

Step 10 Position the rivet sleeve over one of the square cutouts on the opacity shield. Refer to Figure 5 for snap rivet fastener placement. Press the rivet sleeve through the cutout, through the opacity shield material, and through one of the chassis air vent perforations.



You might need to try different cutouts to find the one cutout that aligns correctly with a chassis air vent perforation.

Step 11 Push the rivet pin through the rivet sleeve until you hear a click.



e If you do not hear a click, remove and inspect the snap rivet fastener. If the rivet sleeve appears expanded or damaged, discard the snap rivet fastener and use a new one from the extras supplied in the bag of fasteners.

Step 12 Repeat step 10 and step 11 for the remaining three snap rivet fasteners. Refer to Figure 5 for snap rivet fastener placement.

<u>/</u> Caution

Due to decreased airflow when using the opacity shield, which is required for FIPS 140-2 validation, short-term operation as specified by GR-63-CORE at 55° C is impacted. Short-term operation requirements will only be met at 40° C. Without the opacity shield installed, the system will meet the short-term operations requirements at 55° C.

/Ì\ Caution

We recommend that you replace the opacity shield every three months to prevent dust build-up and the possibility of overheating the chassis. If the environment is especially dusty, inspect and replace the opacity shield more often.



If you need to remove the Catalyst 6509 chassis from the rack, you must first remove the opacity shield. With the opacity shield installed, the chassis is too wide to slide out of the rack.



Installing the Opacity Shield on the Catalyst 6509 Switch



Installing the Opacity Shield on the Cisco 7600 Series Routers

This section describes how to install the opacity shield on the Cisco 7606 router. The opacity shield, associated installation hardware, and tamper evidence labels are part of the Cisco 7600 FIPS kit (part number CVPN7600FIPS/KIT=). The opacity shield is designed to be installed on the Cisco 7606 router while the system is operating without creating an electrical hazard or damage to the system. You will need some clearance between adjacent racks in order to perform this procedure.

The opacity shield is not required for the Cisco 7609 router chassis. The Cisco 7609 router chassis satisfies the FIPS opacity requirement without an external shield.

To install an opacity shield on the Cisco 7606 router chassis (see Figure 6), follow these steps:

- Step 1 The opacity shield is designed to be installed on a Cisco 7606 chassis that is already rack-mounted. If your Cisco 7606 chassis is not rack-mounted, install the chassis in the rack using the procedures contained in the *Cisco 7600 Series Router Installation Guide*. If your Cisco 7606 chassis is already rack-mounted, proceed to step 2.
- Step 2 Open the FIPS kit packaging (part number CVPN7600FIPS/KIT=). The kit contains the following:
 - An opacity shield assembly for the Cisco 7606 router (part number 800-26211-xx). The opacity shield part number is located on the outside of the protective packaging.
 - A bag containing the installation hardware (In some kits there is no bag; the installation hardware is premounted in the opacity shield.
 - An envelope with 30 FIPS tamper evidence labels and a disposable ESD wrist strap.
- **Step 3** Remove the opacity shield from its protective packaging.
 - **a.** If the thumbscrews and the snap rivet fasteners are already installed on the opacity shield, remove the four snap rivet fasteners from the opacity shield; leave the thumbscrews installed. Proceed to step 5.



Verify that the thumbscrews are started only two or three turns in the opacity shield.

b. If the opacity shield comes with a bag of installation hardware (69-1483-xx), open the bag and remove the two thumbscrews and four snap rivet fasteners. The snap rivet fasteners come assembled; you need to separate the two pieces of the snap rivet fastener by removing the snap rivet pin from the snap rivet sleeve before you install them. Proceed to step 4.

Note Extra snap rivet fasteners are included in the bag of installation hardware in case of loss or damage.

- **Step 4** Start the two thumbscrews in the corresponding threaded holes in the opacity shield (see Figure 6); two or three turns is sufficient. Do not thread the thumbscrews too far into the opacity shield.
- Step 5 Open the envelope containing the disposable ESD wrist strap. Attach the disposable ESD wrist strap to your wrist. Attach the other end of the wrist strap to exposed metal on the chassis.
- **Step 6** Position the opacity shield over the air intake side of the chassis so that the two thumbscrews on the opacity shield are aligned with the unused top and bottom L-bracket screw holes on the chassis.
- **Step 7** Press the opacity shield firmly against the side of the chassis and secure the opacity shield to the chassis with the two thumbscrews.

- **Step 8** Position the rivet sleeve over one of the square cutouts on the opacity shield. Refer to Figure 6 for snap rivet fastener placement. Press the rivet sleeve through the cutout, through the opacity shield material, and through one of the chassis air vent perforations.
 - Note
- You might need to try different cutouts to find the one cutout that aligns correctly with a chassis air vent perforation.
- **Step 9** Push the rivet pin through the rivet sleeve until you hear a click.



- If you do not hear a click, remove and inspect the snap rivet fastener. If the rivet sleeve appears expanded or damaged, discard the snap rivet fastener and use a new one from the extras supplied in the bag of fasteners.
- **Step 10** Repeat step 8 and step 9 for the remaining three snap rivet fasteners. Refer to Figure 6 for snap rivet fastener placement.

/ľ\ Caution

Due to decreased airflow when using the opacity shield, which is required for FIPS 140-2 validation, short-term operation as specified by GR-63-CORE at 55° C is impacted. Short-term operation requirements will only be met at 40° C. Without the opacity shield installed, the system will meet the short-term operations requirements at 55° C.



We recommend that you change the opacity shield every three months to prevent dust build-up and the possibility of overheating the chassis. If the environment is especially dusty, inspect and replace the opacity shield more often.



If you need to remove the Catalyst 6509 chassis from the rack, you must first remove the opacity shield. With the opacity shield installed, the chassis is too wide to slide out of the rack.



Figure 6 Installing the Opacity Shield on the Cisco 7606 Router

Physical Security

The router is entirely encased by a thick steel chassis. Nine module slots are provided on the Catalyst 6509 switch and the Cisco 7609 router; six module slots are provided on the Cisco 7606 router. On-board LAN connectors and console connectors are provided on the supervisor engines, and the power cable connection and a power switch are provided on the power supply of both models. The individual modules that comprise the switch or the router may be removed to allow access to the internal components of each module.

Any chassis slot that is not populated with a module must have a slot cover installed in order to operate in a FIPS compliant mode. The slot covers are included with each chassis, and additional slot covers may be ordered from Cisco. Use the procedure described here to apply tamper evidence labels to the network modules and the service modules.



Use the same procedure to apply tamper evidence labels to the slot covers.

After the router or the switch has been configured to meet FIPS 140-2 Level 2 requirements, the router or the switch cannot be accessed without indicating signs of tampering. To seal the system with serialized tamper-evidence labels, follow these steps:

- **Step 1** Remove any grease, dirt, or oil from the cover by using alcohol-based cleaning pads before applying the tamper evidence labels. The chassis temperature should be above 10° C (50° F).
- Step 2 Place labels on the chassis as shown in either Figure 7 (Catalyst 6509 switch), Figure 8 (Cisco 7606 router), or Figure 9 (Cisco 7609 router).
 - **a.** Fan tray—The tamper evidence label should be placed so that one half of the label adheres to the front of the fan tray and the other half adheres to the left side of the chassis. Any attempt to remove the fan tray will damage the tamper seal, which indicates tampering has occurred.
 - b. Modules—For each Supervisor Engine 2, VPN Services Module, network module, or blank module cover installed in the chassis, place a tamper evidence label so that one half of the label adheres to the right side of the module and the other half adheres to the right side of the chassis. Place a second tamper evidence label so that one half of the label adheres to the left side of the module and the other half adheres to the left side of the module and the other half adheres to the left side of the module and the other seal, which indicates tampering has occurred.
 - **c.** Power supply—For each power supply or power supply blank cover installed in the chassis, place a tamper evidence label so that one half of the label adheres to the front of the power supply or power supply blank cover and the other half adheres to the chassis. Any attempt to remove the fan tray will damage the tamper seal, which indicates tampering has occurred.
 - **d.** Opacity shield—Four labels should be applied to the opacity shield (mounted on the right side of the chassis) as follows:
 - Place one label so that one half of the label adheres to the top of the opacity shield and the other half adheres to the chassis.
 - Place one label so that one half of the label adheres to the left side of the opacity shield and the other half adheres to the chassis.

- Place one label so that one half of the label adheres to the right side of the opacity shield and the other half adheres to the chassis.
- For the Catalyst 6509 switch chassis only, place one label so that one half of the label adheres to the bottom of the opacity shield and the other half adheres to the right side of the chassis.
- For the Cisco 7606 router chassis only, place one label so that one half of the label adheres to the bottom of the opacity shield and the other half adheres to the bottom of the chassis.



e The Cisco 7609 router does not have an opacity shield.

- Step 3 Place labels on each supervisor engine installed in the chassis as shown in either Figure 7 (Catalyst 6509 switch), Figure 8 (Cisco 7606 router), or Figure 9 (Cisco 7609 router).
 - **a.** Place a tamper evidence label so that one half of the label adheres to the PCMCIA slot and the other half adheres to the Supervisor Engine 2 faceplate. Any attempt to install or remove a Flash PC card will damage the tamper seal, which indicates tampering has occurred.
 - **b.** Place a tamper evidence label so that one half of the label adheres to the GBIC transceiver installed in the supervisor engine 2 network interface uplink port and the other half adheres to the Supervisor Engine 2 faceplate. Any attempt to remove a GBIC transceiver will damage the tamper seal, which indicates tampering has occurred.
 - **c.** Place a tamper evidence label so that it completely covers an unpopulated network interface uplink port. Any attempt to install a GBIC transceiver in the network interface uplink port will damage the tamper seal, which indicates tampering has occurred.



The tamper seal label adhesive completely cures within five minutes.

Figure 7 Catalyst 6509 Switch Chassis Tamper Evidence Label Placement





Figure 8 Cisco 7606 Router Chassis Tamper Evidence Label Placement





The tamper evidence seals are made from a special thin-gauge vinyl with self-adhesive backing. Any attempt to open the chassis, remove the modules or power supplies, or remove the opacity shield will damage the tamper evidence seals or the painted surface and metal of the chassis. Because the tamper evidence seals have nonrepeated serial numbers, they may be inspected for damage and compared against the applied serial numbers to verify that the module has not been tampered with. Tamper evidence seals can also be inspected for signs of tampering, which include the following: curled corners, bubbling, crinkling, rips, tears, and slices. The word "OPEN" may appear if the label was peeled back.

Cryptographic Key Management

The switch or the router securely administers both cryptographic keys and other critical security parameters such as passwords. The tamper evidence seals provide physical protection for all keys. Keys are also password protected and can be zeroized by the crypto officer. Keys are exchanged manually and entered electronically using manual key exchange or Internet Key Exchange (IKE).

Chassis containing the VPN Services Module and a cryptographic accelerator card support DES (56-bit) (only for legacy systems) and 3DES (168-bit) IPsec encryption, MD5 and SHA-1 hashing, and hardware support for RSA signature generation.

The module supports the critical security parameters (CSPs) as described in Table 3.

CSP Number	Key or CSP Name	Description	Storage
1	.key	This is the seed key for X9.31 PRNG. This key is stored in DRAM and updated periodically after 400 bytes are generated; hence, it is zeroized periodically. The operator also can turn off the router to zeroize this key.	DRAM (plaintext)
2	secret_number	The private exponent used in Diffie-Hellman (DH)DIexchange. It is zeroized after a DH shared secret has been(pgenerated.(p)	
3	skeyid	The shared secret within IKE exchange. It is zeroized when an IKE session is terminated.I	
4	skeyid_d	The shared secret within IKE exchange. It is zeroized when an IKE session is terminated.	DRAM (plaintext)
5	skeyid_a	The shared secret within IKE exchange. It is zeroized when an IKE session is terminated.	DRAM (plaintext)
6	skeyid_e	The shared secret within IKE exchange. It is zeroized when an IKE session is terminated.	DRAM (plaintext)
7	transform_key1	The IKE session encrypt key. It is zeroized when an IKE definition of the definition	
8	transform_key2	The IKE session authentication key. It is zeroized when an IKE session is terminated.IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	
9	crypto_private_key	The RSA private key. The crypto key zeroize command zeroizes this key.	NVRAM (plaintext)

Table 3 Critical Security Parameters

CSP Number	Key or CSP Name	Description	Storage
10	pre_shared_key	The key used to generate IKE key id during preshared-key authentication. The no crypto isakmp key command zeroizes it. This key can have two forms based on whether the key is related to the hostname or the IP address.	NVRAM (plaintext)
11	hmac_data	This key generates keys 3, 4, 5 and 6. This key is zeroized after generating those keys.	DRAM (plaintext)
12	sig_key	The RSA public key used to validate signatures within IKE. These keys are expired either when the certificate revocation list (CRL) expires or after 5 seconds if no CRL exists. This key is deleted after the expiration happens and before a new public key structure is created. This key does not need to be zeroized because it is a public key.	DRAM (plaintext)
13	secret_1_0_0	The fixed key used in Cisco vendor-ID generation. This key is embedded in the module binary image and can be deleted by erasing the flash memory.	NVRAM (plaintext)
14	transform_key3	The IPsec encryption key. It is zeroized when IPsec session is terminated.	DRAM (plaintext)
15	transform_key4	The IPsec authentication key. It is zeroized when IPsec session is terminated.	DRAM (plaintext)
16	signature	The RSA public key of the CA. The no crypto ca trust <i>label</i> command invalidates the key and it frees the public key label that prevents use of the key. This key does not need to be zeroized because it is a public key.	NVRAM (plaintext)
17	dnssec_zone_key	This key is a public key of the DNS server. It is zeroized using the no crypto ca trust <i>label</i> command which invalidates the DNS server's public key and frees the public key label, preventing the use of that key. This label is different from the label in the above key. This key does not need to be zeroized because it is a public key.	NVRAM (plaintext)
18	SLL session key	The SSL session key. It is zeroized when the SSL connection is terminated.	DRAM (plaintext)
19	ARAP key	The ARAP key that is hardcoded in the module binary image. This key can be deleted by erasing the flash memory.	Flash (plaintext)
20	ARAP password	This is an ARAP user password used as an authentication key. A function uses this key in a DES algorithm for authentication.	DRAM (plaintext)
21	config key	The key used to encrypt values of the configuration file. This key is zeroized when the command no key config-key is issued.	NVRAM (plaintext)

Table 3 Critical Security Parameters (continued)

CSP Number	Key or CSP Name	Description	Storage
22	authentication key	This key is used by the router to authenticate itself to the peer. The router or switch gets the password (that is used as this key) from the AAA server and sends it onto the peer. The password retrieved from the AAA server is zeroized upon completion of the authentication attempt.	DRAM (plaintext)
23	ssh server key	The RSA public key used in SSH. It is zeroized after the termination of the SSH session. This key does not need to be zeroized because it is a public key.	DRAM (plaintext)
24	PPP authentication key	The authentication key used in PPP. This key is in the DRAM and not zeroized at runtime. To zeroize the key, you can turn off the switch or the router.	DRAM (plaintext)
25	authentication key2	This key is used by the router to authenticate itself to the peer. The key is identical to key 22 except that it is retrieved from the local database (on the switch or router). Issuing the command no username password zeroizes the password (that is used as this key) from the local database.	NVRAM (plaintext)
26	ssh encryption key	This is the SSH session key. It is zeroized when the SSH session is terminated.	DRAM (plaintext)
27	User Password	The password of the user role. This password is zeroized by overwriting it with a new password.	NVRAM (plaintext)
28	CO Enable Password	The plaintext password of the cryptographic officer (CO) role. This password is zeroized by overwriting it with a new password.	NVRAM (plaintext)
29	CO Enable Secret Password	The ciphertext password of the cryptographic officer (CO) role. The algorithm used to encrypt this password is not FIPS approved; this password is considered plaintext for FIPS purposes. This password is zeroized by overwriting it with a new password.	NVRAM (plaintext)
30	Radius shared secret	The RADIUS shared secret. This shared secret is zeroized by executing the no form of the RADIUS shared-secret set command.	NVRAM (plaintext) DRAM (plaintext)
31	TACACS+ shared secret	The TACACS+ shared secret. This shared secret is zeroized by executing the no form of the TACACS+ shared-secret set command.	NVRAM (plaintext) DRAM (plaintext)

Table 3 Critical Security Parameters (continued)

Table 4 lists the services accessing the CSPs, the type of access and which role accesses the CSPs.

I

SRDI/Role/ Service Access Policy	Security Relevant Data Item	Critical Security Parameters
Role/Service		
User Role		<u> </u>
Status Functions		<u> </u>
Network Functions		• CSP 1–20 (R)
		• CSP 22–27 (R)
Terminal Functions		
Directory Functions		
Crypto-Officer Role		
Configure the Router		• CSP 13 (R/W/D)
		• CSP 19 (R/W/D)
		• CSP 21 (R/W/D)
		• CSP 25 (R/W/D)
Define Rules and Filters		
Status Functions		
Manage the Router		CSP 1 (R)
		CSP 20-22 (R/W/D)
		CSP 24 (D)
		CSP 27–31 (R/W/D)
Set Encryption/Bypass		
Change Port Adapters		—

Table 4 Role and Service Access to Critical Security Parameters (CSPs)

The module supports the following:

- DES (only for legacy systems)
- 3DES
- SHA-1
- MD-5
- MD-4
- SHA-1
- HMAC
- DES MAC
- Triple-DES MAC
- MD5 HMAC
- Diffie-Hellman
- RSA [for digital signatures and encryption/decryption (for IKE authentication)]



The MD-5, MD-5 HMAC, and MD-4 algorithms are disabled when operating in FIPS mode.

The module supports three types of key management schemes:

- A symmetric manual key exchange method. DES and 3DES keys and HMAC-SHA-1 keys are exchanged manually and entered electronically.
- The IKE method with support for exchanging preshared keys manually and entering electronically.
 - The preshared keys are used with Diffie-Hellman key agreement technique to derive DES or 3DES keys.
 - The preshared key is also used to derive HMAC-SHA-1 key.
- The IKE with RSA signature authentication.

All preshared keys are associated with the CO role that created the keys and the CO role is protected by a password. Therefore, the CO password is associated with all the pre-shared keys. The crypto officer needs to be authenticated to store keys. All Diffie-Hellman (DH) keys agreed upon for individual tunnels are directly associated with that specific tunnel only through the IKE protocol.

Key Zeroization

All of the keys and CSPs of the module can be zeroized. Refer to the description column of Table 3 for information on methods to zeroize each key and CSP.

Self-Tests

To prevent any secure data from being released, it is important to test the cryptographic components of a security module to ensure that all components are functioning correctly. The router or switch includes an array of self-tests that are run during startup and periodically during operations. If any of the self-tests fail, the router transitions into an error state. Within the error state, all secure data transmission is halted and the router outputs status information indicating the failure.

Cisco IOS Software Self-Tests

- Power-up tests
 - Firmware integrity test
 - RSA signature Known Answer Test (KAT) (both signature and verification)
 - DES KAT
 - TDES KAT
 - AES KAT
 - SHA-1 KAT

Γ

- PRNG KAT
- Power-up bypass test
- Diffie-Hellman self-test
- HMAC SHA-1 KAT
- Conditional tests
 - Conditional bypass test
 - Pair-wise consistency test on RSA signature
 - Continuous random number generator tests

VPN Services Module (Cryptographic Accelerator) Self-Tests

- Power-up tests
 - Firmware integrity test
 - DES KAT
 - TDES KAT
 - SHA-1 KAT
- Conditional tests
 - Continuous random number generator test

Secure Operation of the Catalyst 6509 Switch and the Cisco 7606 and Cisco 7609 Routers

The Catalyst 6509 switch and the Cisco 7606 router and the Cisco 7609 router with the VPN Services Module meets all the Level 2 requirements for FIPS 140-2. Follow the setting guidelines provided in the following sections to place the module in a FIPS-approved mode of operation. Operating this router or switch without maintaining the following settings will remove the module from the FIPS-approved mode of operation.

Initial Setup

Before configuring the router or switch, note these requirements:

- The crypto officer must ensure that the VPN Services Module cryptographic accelerator card is installed in the chassis by visually confirming the presence of the VPN Services Module.
- The crypto officer must apply tamper evidence labels as described in the "Physical Security" section on page 18 of this document.
- Only the crypto officer may add and remove network modules. When removing the tamper evidence label, the crypto officer should remove the entire label from the chassis and clean the cover of any grease, dirt, or oil with an alcohol-based cleaning pad. The crypto officer must reapply tamper evidence labels on the router as described in the "Physical Security" section on page 18.
- The crypto officer must apply the opacity shield as described in the "Physical Security" section on page 18of this document.

Initializing and Configuring the System

To initialize and configure the system, the crypto officer must perform the following operations:

- The crypto officer must perform the initial configuration. Cisco IOS Release 12.2(14)SY3 is the only allowable image; no other image may be loaded.
- The value of the boot field must be 0x0101 (the factory default). This setting disables the break from the console to the ROM monitor and automatically boots the Cisco IOS image. From the **configure terminal** command line, the crypto officer enters the following syntax:

config-register 0x0101

• The crypto officer must create the enable password for the crypto officer role. The password must be at least eight characters and is entered when the crypto officer first engages the **enable** command. The crypto officer enters the following syntax at the "#" prompt:

```
enable secret [PASSWORD]
```

- The crypto officer must always assign passwords (of at least eight characters) to users.
- Identification and authentication on the console port is required for users. From the **configure terminal** command line, the crypto officer enters the following syntax:

```
line con 0
password [PASSWORD]
login local
```

- The crypto officer shall only assign users to a privilege level 1 (the default).
- The crypto officer shall not assign a command to any privilege level other than its default.
- The crypto officer may configure the module to use RADIUS or TACACS+ for authentication. Configuring the module to use RADIUS or TACACS+ for authentication is optional. If the module is configured to use RADIUS or TACACS+, the Crypto-Officer must define RADIUS or TACACS+ shared secret keys that are at least 8 characters long.
- If the crypto officer loads any Cisco IOS image onto the switch or router, this will put the switch or router into a non-FIPS mode of operation.

IPsec Requirements and Cryptographic Algorithms

Two types of key management method are allowed in FIPS mode: Internet Key Exchange (IKE) and IPsec manually entered keys.

Although the Cisco IOS implementation of IKE allows a number of algorithms, only the following algorithms are allowed in a FIPS 140-2 configuration:

- ah-sha-hmac
- esp-des
- esp-sha-hmac
- esp-3des
- esp-aes

The following algorithms are not FIPS approved and should be disabled:

- MD-4 and MD-5 for signing
- MD-5 HMAC

Protocols

All SNMP operations must be performed within a secure IPsec tunnel.

Remote Access

Telnet access to the system is only allowed through a secure IPsec tunnel between the remote system and the module. The Crypto officer must configure the module so that any remote connections using Telnet are secured through IPsec.

SSH access to the system is only allowed if SSH is configured to use a FIPS-approved algorithm. The Crypto officer must configure the module so that SSH uses only FIPS-approved algorithms.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

© 2005, Cisco Systems, Inc. All rights reserved. Printed in USA.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.