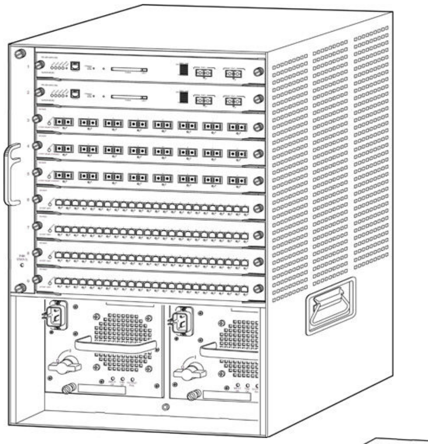
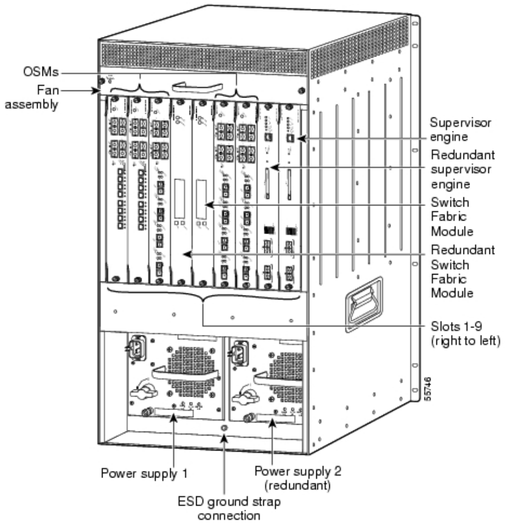
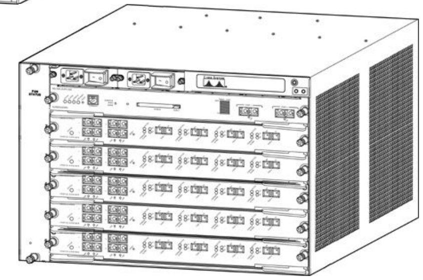
Cisco Catalyst 6509 Switch, 7606 and 7609 Routers with VPN Services Module




OSMs
Fan assembly
Supervisor engine
Redundant supervisor engine
Switch Fabric Module
Redundant Switch Fabric Module
Slots 1-9 (right to left)
55746
Power supply 1
Power supply 2 (redundant)
ESD ground strap connection



FIPS 140-2
Non-Proprietary Security Policy

Level 2 Validation
Version 1.5
April 21, 2004

Table of Contents

1 Introduction

1.1 Purpose

This is the non-proprietary Cryptographic Module Security Policy for the Cisco Catalyst 6509 Switch, 7606 and 7609 Routers with VPN Services module (Hardware Version: 6509, 7606 and 7609; Backplane chassis: Hardware Version 3.0 (6509), 1.0 (7606) and 1.0 (7609); Supervisor Blade: Hardware Version 3.2; VPN Accelerator Blade: Hardware Version 1.2 , Firmware Version: 12.2(14)SY3). This security policy describes how the Catalyst 6509 Switch, 7606 and 7609 Routers with VPN Services Module meet the security requirements of FIPS 140-2, and how to operate them 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, 7606 and 7609 Routers with 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/.

1.2 References

This document deals only with operations and capabilities of the Catalyst 6509 Switch, 7606 and 7609 Routers in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the Catalyst 6509 Switch, 7606 and 7609 Routers and the entire 6500 and 7600 series from the following sources:

- The Cisco Systems website contains information on the full line of products at www.cisco.com. The 6500 Series product descriptions can be found at: http://www.cisco.com/en/US/products/hw/switches/ps708/index.html.
  The 7600 Series 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 please refer to the contacts listed on the Cisco Systems website at www.cisco.com.
- The NIST Validated Modules website (http://csrc.nist.gov/cryptval) contains contact information for answers to technical or sales-related questions for the module

1.3 Terminology

In this document, the Cisco Catalyst 6509 Switch, 7606 and 7609 Routers with VPN Services Module are referred to the 6509, 7606 and 7609, the 6509 switch, 7606 router and 7609 router, the routers, the modules, or the systems.

1.4 Document Organization

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

- ♦ Vendor Evidence document
- ♦ Finite State Machine

- Module Software Listing
- Other supporting documentation as additional references

This document provides an overview of the Cisco Catalyst 6509 Switch, 7606 and 7609 Routers and explains the secure configuration and operation of the modules. This introduction section is followed by Section 2, which details the general features and functionality of the Catalyst 6509 Switch, 7606 and 7609 Router. Section 3 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, please contact Cisco Systems.

2 The 6509 Switch/7606 and 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 Cisco Catalyst 6509 Switch, 7606 and 7609 Routers with VPN Services Module offer versatility, integration, and security to branch offices. With numerous Network Modules (NMs) and Service Modules (SMs) available, the modular architecture of the Cisco router easily allows interfaces to be upgraded to accommodate network expansion. The Cisco 6509, 7606 and 7609 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 Cisco 6509 switch, 7606 and 7609 routers.

2.1 The 6509/7606/7609 Cryptographic Module

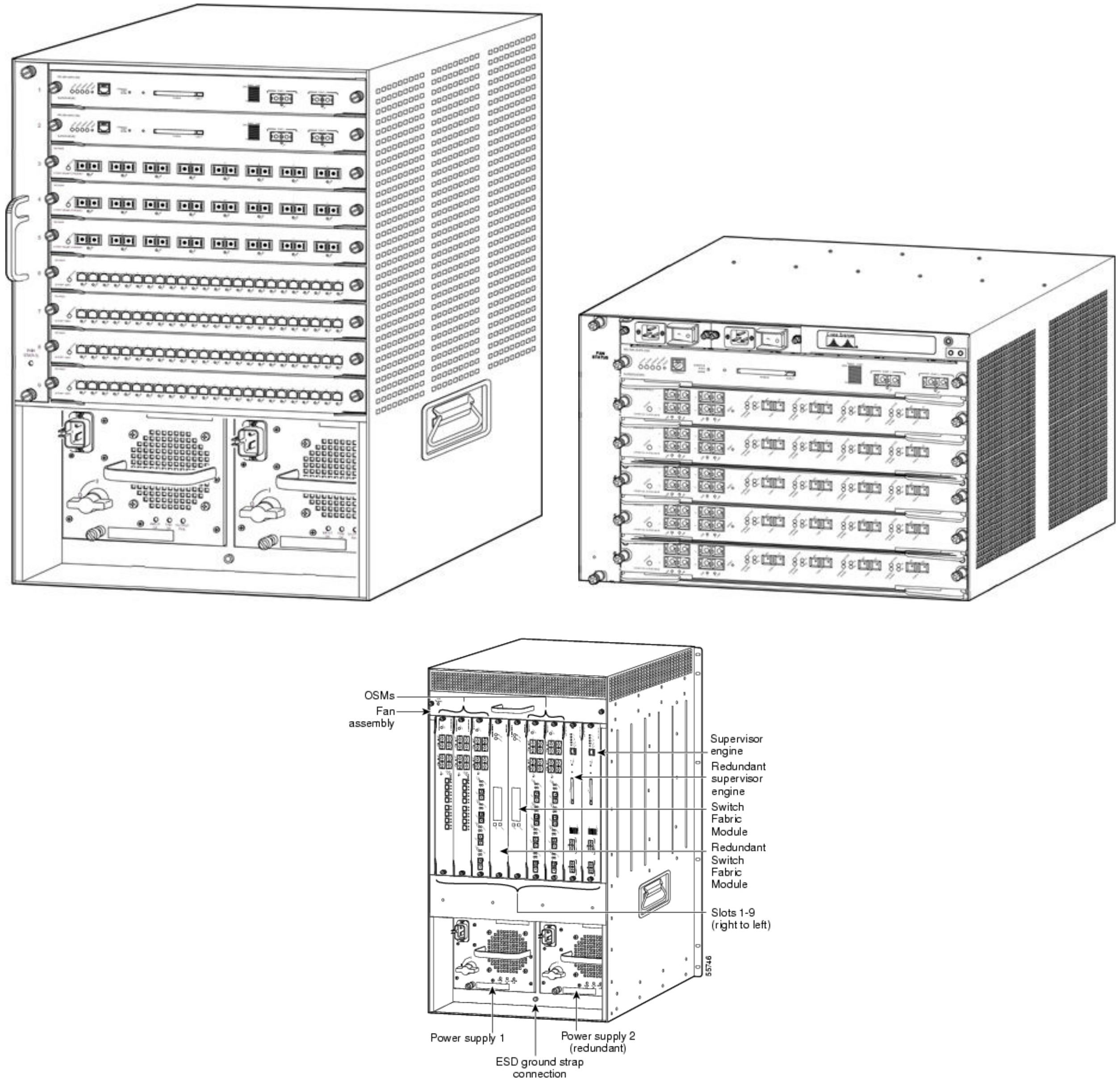

OSMs
Fan assembly
Supervisor engine
Redundant supervisor engine
Switch Fabric Module
Redundant Switch Fabric Module
Slots 1-9 (right to left)
Power supply 1
Power supply 2 (redundant)
ESD ground strap connection
55746

Figure 1 - The 6509 Switch, 7606 and 7609 Routers

The cryptographic boundary is defined as encompassing the “top,” “front,” “left,” “right,” and “bottom” surfaces of the case; all portions of the “backplane” of the case which are not designed to accommodate a NM or SM; and the inverse of the three-dimensional space within the case that would be occupied by any installed NM or SM which does not perform Approved cryptographic functions or any installed power supply module. The cryptographic boundary includes the connection apparatus between the NM/SM and the motherboard/daughterboard that hosts the NM/SM, but the boundary does not include the NM/SM itself unless it performs Approved cryptographic functions. In other words, the cryptographic boundary encompasses all hardware components within the case of the device except any installed non-Approved cryptographic NMs/SMs and the power supply sub-modules. Currently available Service Modules include a

Network Access Module (NAM), a Firewall Module, and a VPN Services Module. All of the functionality discussed in this document is provided by components within this cryptographic boundary.

The modules require that a special opacity shield be installed over the right-hand-side air vents (shown on the right-hand side of the modules in Figure 1) in order 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.

The Cisco 6509 Switch, 7606 and 7609 Routers incorporate a single VPN Services Module cryptographic accelerator card. The VPN Services Module is installed in an NM/SM slot.

Cisco IOS features such as tunneling, data encryption, and termination of Remote Access WANs via IPSec, Layer 2 Forwarding (L2F) and Layer 2 Tunneling Protocols (L2TP) make the Cisco 6509, 7606 and 7609 with VPN Services Module an ideal platform for building virtual private networks or outsourced dial solutions. The modules' RISC-based processor provides the power needed for the dynamic requirements of the remote branch office.

2.2 Module Interfaces

The interfaces for the routers are located on the front panel as shown in Figure 2.

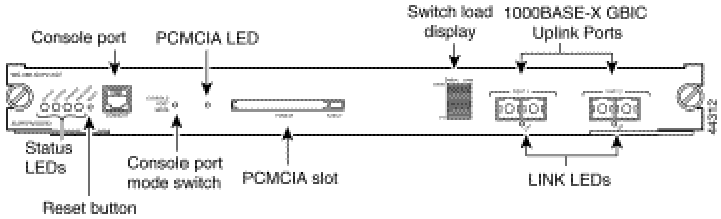


Figure 2 – 6509, 7606 and 7609 Physical Interfaces

The Cisco Catalyst 6509 Switch, 7606 and 7609 Routers feature console ports, fixed Ethernet interfaces, nine Cisco Network/Service Module slots on the 6509 and 7609, and six Network/Service Module slots on the 7606. Network modules support a variety of LAN and WAN connectivity interfaces, for example: Ethernet, ATM, serial, ISDN BRI, and integrated CSU/DSU options for primary and backup WAN connectivity.

An NM/SM is inserted into one of the NM/SM slots, which are located on the front panel of both routers. NMs/SMs interface directly with the processor, and cannot perform cryptographic functions; they only serve as a data input and data output physical interface.

The router has two Ethernet uplink ports. The module 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 sub-module via the backplane. Figure 2 shows the LEDs located on the 6509, 7606 and 7609 with descriptions detailed in Table 1 below.

LED	Indication	Description
Supervisor 2 Module		
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[3].
	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.
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 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.
VPN Services Module		
STATUS	Green	All non-FIPS-related diagnostic tests pass. The module is 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 and self-test diagnostic sequence. • The module is disabled. • The module is in the shutdown state.
	Off	The module power is off.

[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.
4Execute the command "`show crypto eli`" to determine whether the FIPS-related self-tests passed.

Table 1 – 6509, 7606 and 7609 LEDs and Descriptions

All of these physical interfaces are separated into the logical interfaces from FIPS 140-2 as described in the following table:

Router Physical Interface	FIPS 140-2 Logical Interface
Ethernet Ports Network/Service Module Interface Console Port Compact Flash Slot	Data Input Interface
Ethernet Ports Network/Service Module Interface Console Port Compact Flash Slot	Data Output Interface
Ethernet Ports Network/Service Module Interface Console Port Reset Button	Control Input Interface
Ethernet Ports Network/Service Module Interface Status LED (Supervisor 2) System LED Active LED PWR MGMT LED PCMCIA LED Switch Load LED Network Port LINK LEDs Status LED (VPN Services Module) Console Port	Status Output Interface
Backplane	Power Interface

Table 2 – FIPS 140-2 Logical Interfaces

2.3 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 exercise only 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. Once the Crypto Officer configured 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. 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 Cisco Catalyst 6509 Switch, 7606 and 7609 Routers can be found in the *Performing Basic System Management* manual and in the online help for the router.

The User and Crypto Officer passwords and the RADIUS/TACACS+ shared secrets must each be at least 8 alphanumeric characters in length. See Section 3, *Secure Operation of the Cisco 6509 Switch, 7606 and 7609 Router*, for more information. If only integers 0-9 are used without repetition for an 8 digit PIN, the probability of randomly guessing the correct sequence is 1 in 1,814,400. Including the rest of the alphanumeric characters drastically decreases the odds of guessing the correct sequence.

2.3.1 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, thereby creating 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:

- **Configure the router**: define network interfaces and settings, create command aliases, set the protocols the router will support, enable interfaces and network services, set system date and time, and load authentication information.
- **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 characteristics such as protocol ID, addresses, ports, TCP connection establishment, or packet direction.
- **Status Functions**: view the router configuration, routing tables, active sessions, use Gets to view SNMP MIB II statistics, health, temperature, memory status, voltage, packet statistics, review accounting logs, and view physical interface status
- **Manage the router**: log off users, shutdown or reload the router, manually back up router configurations, view complete configurations, manager user rights, and restore router configurations.
- **Set Encryption/Bypass**: set up the configuration tables for IP tunneling. Set keys and algorithms to be used for each IP range or allow plaintext packets to be set from specified IP address.
- **Change Port Adapters**: insert and remove adapters in a port adapter slot.

2.3.2 User Services

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

- **Status Functions**: view state of interfaces, state of layer 2 protocols, version of IOS currently running
- **Network Functions**: connect to other network devices (via outgoing telnet or PPP) and initiate diagnostic network services (*i.e.*, ping, mtrace)

- **Terminal Functions:** adjust the terminal session (e.g., lock the terminal, adjust flow control)
- **Directory Services**: display directory of files kept in flash memory

2.4 Physical Security

The router is entirely encased by a thick steel chassis. Nine NM slots are provided on the 6509 and 7609, and six NM slots are provided on the 7606. On-board LAN connectors and console connectors are provided on the routers, and the power cable connection and a power switch are provided on the power supply of both models. The individual modules (or "blades") that comprise the router may be removed to allow access to the internal components of each blade.

Any NM/SM slot, which is not populated with a NM/SM, must be populated with an appropriate slot cover in order to operate in a FIPS compliant mode. The slot covers are included with each router, and additional covers may be ordered from Cisco. The same procedure mentioned below to apply tamper evidence labels for NMs/SMs must also be followed to apply tamper evidence labels for the slot covers.

Once the router has been configured in to meet FIPS 140-2 Level 2 requirements, the router cannot be accessed without signs of tampering. To seal the system, apply serialized tamper-evidence labels as follows:

1. Clean the cover of any grease, dirt, or oil before applying the tamper evidence labels. Alcohol-based cleaning pads are recommended for this purpose. The temperature of the router should be above 10°C.
2. Place a label on the router as shown in Figure 3. The tamper evidence label should be placed so that one half of the tamper evidence label covers the front of the fan-bank module and the other half covers the left side of the router. Any attempt to remove the fan-bank will leave tamper evidence.
3. Place labels on the router as shown in Figure 3. For each Supervisor 2 module, VPN Services Module, network module, or network module cover installed in the router, place a tamper evidence label so that one half of the label covers the right side of the Supervisor 2 module, VPN Services Module, network module, or network module cover and the other half covers the right side of the router. Any attempt to remove a network module will leave tamper evidence.
4. Place labels on the router as shown in Figure 3. For each Supervisor 2 module installed in the router, place a tamper evidence label so that one half of the label covers the Compact Flash slot and the other half covers the Supervisor 2 module. Any attempt to install or remove a Compact Flash card will leave tamper evidence.
5. Place labels on the router as shown in Figure 3. For each Supervisor 2 module installed in the router, place a tamper evidence label so that one half of the label covers an installed Supervisor 2 Network Interface module and the other half covers the Supervisor 2 module. Any attempt to remove a Supervisor 2 Network Module will leave tamper evidence.

6. Place labels on the router as shown in Figure 3. For each Supervisor 2 module installed in the router that has an unpopulated Network Interface port, place a tamper evidence label so that it completely covers the unpopulated Network Interface port opening. Any attempt to install a network Interface port will leave tamper evidence.
7. Place labels on the router as shown in Figure 3. For each power supply or power supply cover installed in the router, 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.
8. Place labels on the router as shown in Figure 3. Four labels should be applied to the Opacity Shield in the right side of the chassis as follows: one label should be placed so that one half of the label covers the top of the Opacity Shield and the other half covers the top of the chassis; one label should be placed so that one half of the label covers the left side of the Opacity Shield and the other half covers the front of the chassis; one label should be placed so that one half of the label covers the right side of the Opacity Shield and the other half covers the rear of the chassis; for the 6509 only, one label should be placed so that one half of the label covers the bottom of the Opacity Shield and the other half covers the right side of the chassis; and for the 7606 only, one label should be placed so that one half of the label covers the bottom of the Opacity Shield and the other half covers the bottom of the chassis. The 7609 does not have an opacity shield.
9. The labels completely cure within five minutes.

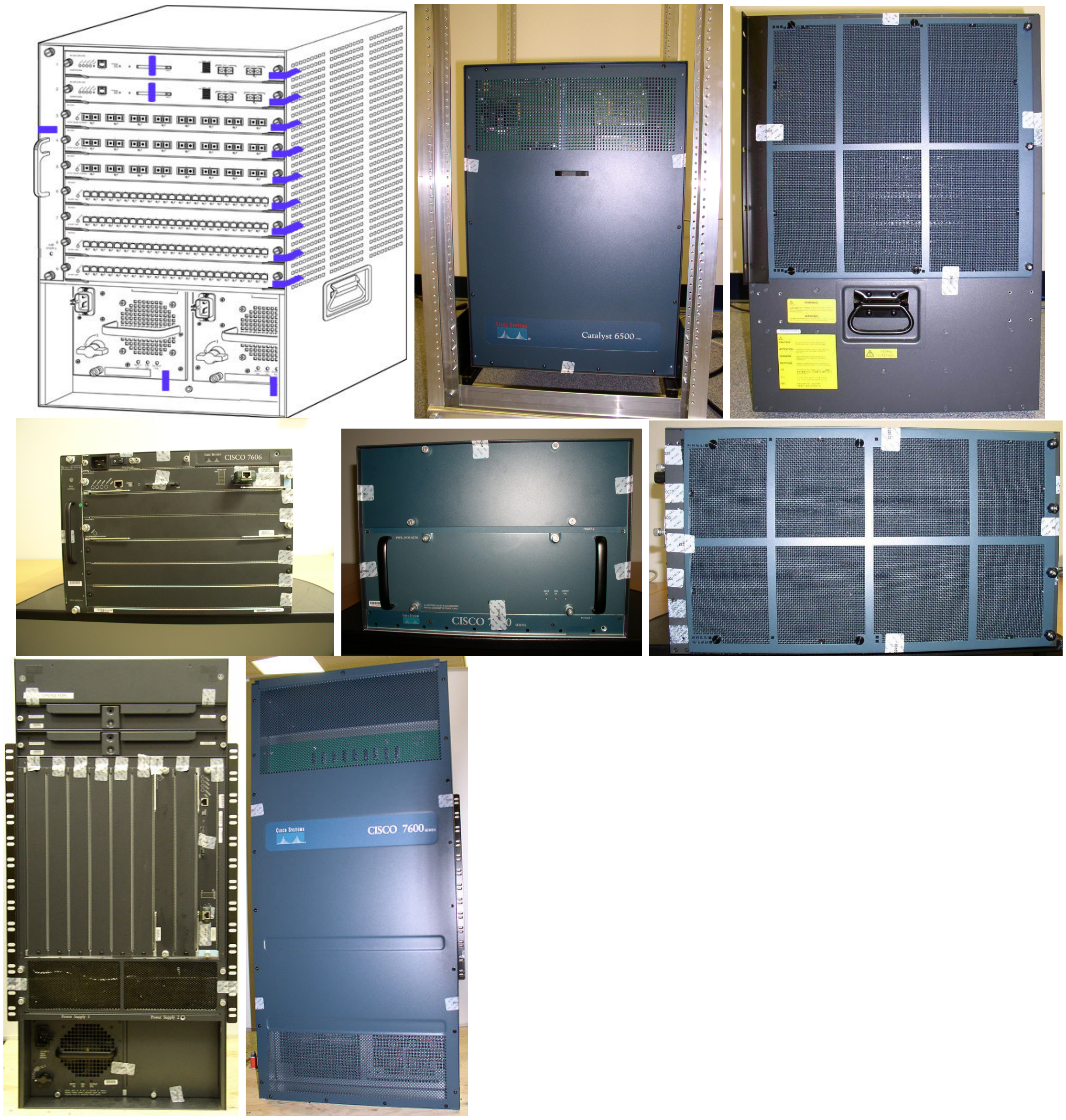


Figure 3 – 6509, 7606 and 7609 Tamper Evidence Label Placement

The tamper evidence seals are produced from a special thin-gauge vinyl with self-adhesive backing. Any attempt to open the router, remove Network Modules, or remove the front faceplate will damage the tamper evidence seals or the painted surface and metal of the module cover. Since the tamper evidence seals have non-repeated serial numbers, they may be inspected for damage and compared against the applied serial numbers to verify that the module has not been tampered. 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.

2.5 Cryptographic Key Management

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. All keys are also protected by the password-protection on the Crypto Officer role login, and can be zeroized by the Crypto Officer. Keys are exchanged manually and entered electronically via manual key exchange or Internet Key Exchange (IKE).

The modules contain the VPN Services Module, a cryptographic accelerator card which provides 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 following critical security parameters (CSPs):

#	CSP Name	Description	Storage
1	CSP 1	This is the seed key for X9.31 PRNG. This key is stored in DRAM and updated periodically after the generation of 400 bytes; hence, it is zeroized periodically. Also, the operator can turn off the router to zeroize this key.	DRAM (plaintext)
2	CSP 2	The private exponent used in Diffie-Hellman (DH) exchange. Zeroized after DH shared secret has been generated.	DRAM (plaintext)
3	CSP 3	The shared secret within IKE exchange. Zeroized when IKE session is terminated.	DRAM (plaintext)
4	CSP 4	Same as above	DRAM (plaintext)
5	CSP 5	Same as above	DRAM (plaintext)
6	CSP 6	Same as above	DRAM (plaintext)
7	CSP 7	The IKE session encrypt key. The zeroization is the same as above.	DRAM (plaintext)
8	CSP 8	The IKE session authentication key. The zeroization is the same as above.	DRAM (plaintext)
9	CSP 9	The RSA private key. “crypto key zeroize” command zeroizes this key.	NVRAM (plaintext)
10	CSP 10	The key used to generate IKE skeyid during preshared-key authentication. “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	CSP 11	This key generates keys 3, 4, 5 and 6. This key is zeroized after generating those keys.	DRAM (plaintext)
12	CSP 12	The RSA public key used to validate signatures within IKE. These keys are expired either when CRL (certificate revocation list) expires or 5 secs after if no CRL exists. After above expiration happens and before a new public key structure is created this key is deleted.	DRAM (plaintext)

		This key does not need to be zeroized because it is a public key; however, it is zeroized as mentioned here.	
13	CSP 13	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.	NVRAM (plaintext)
14	CSP 14	The IPSec encryption key. Zeroized when IPSec session is terminated.	DRAM (plaintext)
15	CSP 15	The IPSec authentication key. The zeroization is the same as above.	DRAM (plaintext)
16	CSP 16	The RSA public key of the CA. “no crypto ca trust <label>” command invalidates the key and it frees the public key label which in essence prevent use of the key. This key does not need to be zeroized because it is a public key.	NVRAM (plaintext)
17	CSP 17	This key is a public key of the DNS server. Zeroized using the same mechanism as above. “no crypto ca trust <label>” command invalidate the DNS server’s public key and it frees the public key label which in essence prevent 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	CSP 18	The SSL session key. Zeroized when the SSL connection is terminated.	DRAM (plaintext)
19	CSP 19	The ARAP key that is hardcoded in the module binary image. This key can be deleted by erasing the Flash.	Flash (plaintext)
20	CSP 20	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	CSP 21	The key used to encrypt values of the configuration file. This key is zeroized when the “no key config-key” is issued.	NVRAM (plaintext)
22	CSP 22	This key is used by the router to authenticate itself to the peer. The router itself 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	CSP 23	The RSA public key used in SSH. Zeroized after the termination of the SSH session. This key does not need to be zeroized because it is a public key; However, it is zeroized as mentioned here.	DRAM (plaintext)
24	CSP 24	The authentication key used in PPP. This key is in the DRAM and not zeroized at runtime. One can turn off the router to zeroize this key because it is stored in DRAM.	DRAM (plaintext)
25	CSP 25	This key is used by the router to authenticate itself to	NVRAM

		the peer. The key is identical to #22 except that it is retrieved from the local database (on the router itself). Issuing the "no username password" zeroizes the password (that is used as this key) from the local database.	(plaintext)
26	CSP 26	This is the SSH session key. It is zeroized when the SSH session is terminated.	DRAM (plaintext)
27	CSP 27	The password of the User role. This password is zeroized by overwriting it with a new password.	NVRAM (plaintext)
28	CSP 28	The plaintext password of the CO role. This password is zeroized by overwriting it with a new password.	NVRAM (plaintext)
29	CSP 29	The ciphertext password of the CO role. However, the algorithm used to encrypt this password is not FIPS approved. Therefore, this password is considered plaintext for FIPS purposes. This password is zeroized by overwriting it with a new password.	NVRAM (plaintext)
30	CSP 30	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	CSP 31	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

The services accessing the CSPs, the type of access and which role accesses the CSPs are listed in the Table 4.

SRDI/Role/Service Access Policy	Security Relevant Data Item	CSP 1	CSP 2	CSP 3	CSP 4	CSP 5	CSP 6	CSP 7	CSP 8	CSP 9	CSP 10	CSP 11	CSP 12	CSP 13	CSP 14	CSP 15	CSP 16	CSP 17	CSP 18	CSP 19	CSP 20	CSP 21	CSP 22	CSP 23	CSP 24	CSP 25	CSP 26	CSP 27	CSP 28	CSP 29	CSP 30	CSP 31
Role/Service																																
User role																																
Status Functions																																
Network Functions		r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r		r	r	r	r	r	r				
Terminal Functions																																
Directory Services																																
Crypto-Officer Role																																
Configure the Router														r w d						r w d		r w d				r w d						
Define Rules and Filters																																
Status Functions																																
Manage the Router		d																			r w d	r w d	r w d		d			r w d	r w d	r w d	r w d	r w d
Set Encryption/Bypass		r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d		r w d	r w d	r w	r w d	r w d					r w d	r w		r w d					
Change Port Adapters																																

Table 4 – Role and Service Access to CSPs

The module supports DES (only for legacy systems), 3DES, SHA-1, MD-5, MD-4, SHA-1 HMAC, DES MAC, Triple-DES MAC, MD5 HMAC, Diffie-Hellman, and 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:

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

All pre-shared 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 via the IKE protocol.

Key Zeroization:
All of the keys and CSPs of the module can be zeroized. Please refer to the Description column of Table 3 for information on methods to zeroize each key and CSP.

2.6 Self-Tests

In order to prevent any secure data from being released, it is important to test the cryptographic components of a security module to insure all components are functioning correctly. The router 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.

2.6.1 Self-tests performed by the IOS image:

Power-up tests

Firmware integrity test
RSA signature KAT (both signature and verification)
DES KAT
TDES KAT
AES KAT
SHA-1 KAT
PRNG KAT
Power-up bypass test

Diffie-Hellman self-test
HMAC SHA-1 KAT

Conditional tests

Conditional bypass test
Pairwise consistency test on RSA signature
Continuous random number generator tests

2.6.2 Self-tests performed by the VPN Services Module (cryptographic accelerator):

Power-up tests

Firmware integrity test
DES KAT
TDES KAT
SHA-1 KAT

Conditional tests

Continuous random number generator test

3 Secure Operation of the Cisco 6509 Switch, 7606 and 7609 Router

The Cisco 6509 switch and 7606 router with VPN Services Module meet all the Level 2 requirements for FIPS 140-2. Follow the setting instructions provided below to place the module in a FIPS-Approved mode of operation. Operating this router without maintaining the following settings will remove the module from the FIPS-Approved mode of operation.

3.1 Initial Setup

1. The Crypto Officer must ensure that the VPN Services Module cryptographic accelerator card is installed in the module by visually confirming the presence of the VPN services module.
2. The Crypto Officer must apply tamper evidence labels as described in Section 2.4 of this document.
3. Only a Crypto Officer may add and remove Network Modules. When removing the tamper evidence label, the Crypto Officer should remove the entire label from the router and clean the cover of any grease, dirt, or oil with an alcohol-based cleaning pad. The Crypto Officer must re-apply tamper evidence labels on the router as described in Section 2.4.
4. The Crypto Officer must apply the opacity shield as described in Section 2.1 of this document.

3.2 System Initialization and Configuration

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

```
config-register 0x0101
```

3. The Crypto Officer must create the “enable” password for the Crypto Officer role. The password must be at least 8 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]
```

5. The Crypto Officer must always assign passwords (of at least 8 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
```

6. The Crypto Officer shall only assign users to a privilege level 1 (the default).

7. The Crypto Officer shall not assign a command to any privilege level other than its default.
8. 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.
9. If the Crypto Officer loads any IOS image onto the router, this will put the router into a non-FIPS mode of operation.

3.3 IPSec Requirements and Cryptographic Algorithms

1. There are two types of key management method that are allowed in FIPS mode: Internet Key Exchange (IKE) and IPSec manually entered keys.
2. Although the 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
3. The following algorithms are not FIPS approved and should be disabled:
    - MD-4 and MD-5 for signing
    - MD-5 HMAC

3.4 Protocols

1. All SNMP opertaions must be performed within a secure IPSec tunnel.

3.5 Remote Access

1. Telnet access to the module is only allowed via a secure IPSec tunnel between the remote system and the module. The Crypto officer must configure the module so that any remote connections via telnet are secured through IPSec.
2. SSH access to the module 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.

CISCO EDITOR'S NOTE: You may now include all standard Cisco information included in all documentation produced by Cisco. Be sure that the following line is in the legal statements at the end of the document:

> *By printing or making a copy of this document, the user agrees to use this information for product evaluation purposes only. Sale of this information in whole or in part is not authorized by Cisco Systems.*