Cisco 7606-S and 7609-S Routers with Supervisor SUP720-3B

FIPS 140-2 Non Proprietary Security Policy
Level 2 Validation

Version 0.5

May, 2011

Table of Contents

1 Introduction

1.1 Purpose

This document is the non-proprietary Cryptographic Module Security Policy for the Cisco 7606-S and 7609-S Routers with Supervisor SUP720-3B. This security policy describes how the Cisco 7606-S and 7609-S Routers with Supervisor SUP720-3B (Hardware Version: Chassis: 7606-S and 7609-S with SUP720-3B; Firmware Version: 15.1(2)S) meet the security requirements of FIPS 140-2, and how to operate the router with on-board crypto enabled in a secure FIPS 140-2 mode. This policy was prepared as part of the Level **2** FIPS 140-2 validation of the Cisco 7606-S and 7609-S Routers with Supervisor SUP720-3B.

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/index.html.

1.2 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	3
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
	Overall module validation level	**2**

Table 1 Module Validation Level

1.3 References

This document deals only with operations and capabilities of the Cisco 7606-S and 7609-S Routers with Supervisor SUP720-3B in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the routers from the following sources:

The Cisco Systems website contains information on the full line of Cisco Systems routers. Please refer to the following website:

http://www.cisco.com/en/US/prod/collateral/routers/ps368/ps371/product_data_sheet0900aecd8057f3c8.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/groups/STM/cmvp/validation.html) contains contact information for answers to technical or sales-related questions for the module.

1.4 Terminology

In this document, the Cisco 7606-S and 7609-S Routers with Supervisor SUP720-3B is referred to as the router, the module, or the system.

1.5 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
Other supporting documentation as additional references

This document provides an overview of the Cisco 7606-S and 7609-S Routers with Supervisor SUP720-3B and explains the secure configuration and operation of the module. This introduction section is followed by Section 2, which details the general features and functionality of the router. Section 3 specifically addresses the required configuration for the FIPS-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 Cisco 7606-S and 7609-S Routers with Supervisor SUP720-3B

The Cisco 7600-S Router is a compact, high-performance router designed in a 6-slot and 9-slot form factor for deployment at the network edge, where robust performance and IP/Multiprotocol Label Switching (MPLS) services are necessary to meet the requirements of both enterprises and service providers. It enables Carrier Ethernet service providers to deploy an advanced network infrastructure that supports a range of IP video and triple-play (voice, video, and data) system applications in both the residential and business services markets. The Cisco 7600-S also delivers WAN and metropolitan-area network (MAN) networking solutions at the enterprise edge. The following subsections describe the physical characteristics of the routers.

2.1 Cryptographic Module Physical Characteristics

Figure 1 - Cisco 7606-S Router

Figure 2 - Cisco 7609-S Router

The cryptographic boundary is defined as being the physical enclosure of the chassis.

The cryptographic boundary is illustrated in Figures 1 and 2 above as the dark border around the module.

All of the functionality described in this publication is provided by components within this cryptographic boundary. The module incorporates one or more supervisor blades.

2.2 Module Interfaces

The module features the following interfaces:

1. Two SFP Ethernet ports
2. One 10/100/1000 Ethernet port
3. One serial console port
4. Four Status LEDs
5. Two Disk LEDs
6. Three Link LEDs
7. Two CompactFlash Type II slots (disabled via TEL)

These interfaces are depicted in the figures below:

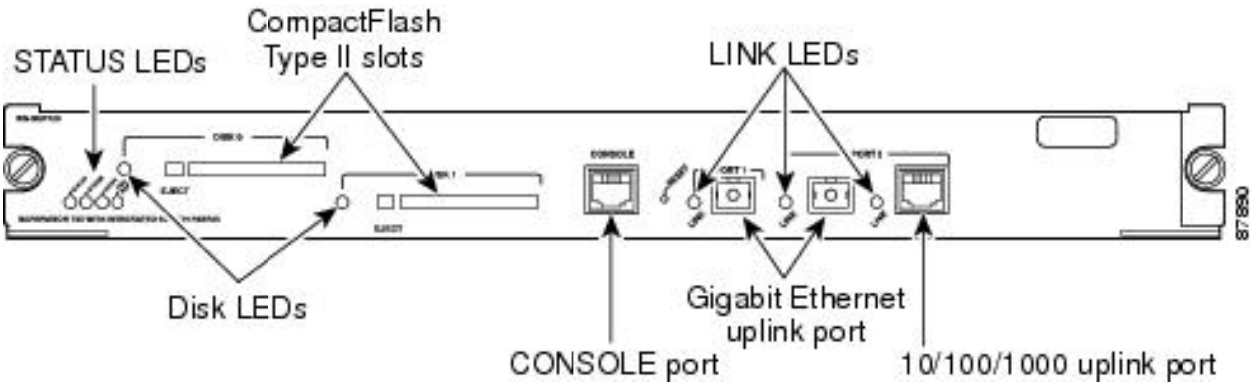


Figure 3 - SUP 720-3B interfaces

The following tables provide more detailed information conveyed by the LEDs on the front and rear panel of the router:

Name	State	Description
Status	Green	All diagnostics pass. The supervisor engine is operational (normal initialization sequence).
	Orange	The supervisor engine is booting or running diagnostics (normal initialization sequence)
	Red	The diagnostic test (including FIPS POSTs) failed. The supervisor engine is not operational because a fault occurred during the initialization sequence.
System	Green	All chassis environmental monitors are reporting OK.
	Orange	A minor hardware problem has been detected.
	Red	A major hardware problem has occurred
Active	Green	The supervisor engine is operational and active.
	Orange	The supervisor engine is in standby mode.

PWR MGMT	Orange	Power-up mode; running self-diagnostics.
	Green	Power management is functioning normally and sufficient power is available for all modules.
	Orange	A minor power management problem has been detected. There is insufficient power for all modules to power up.
	Red	A major power failure has occurred.
DISK 0 and DISK 1	N/A	These LEDs are illuminated green when the installed Flash PC card is being accessed and is performing either a read operation or a write operation.

Table 2 – LED Indicators

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

Router Physical Interface	FIPS 140-2 Logical Interface
Gigabit/SFP Ethernet ports Console Port	Data Input Interface
Gigabit/SFP Ethernet ports Console Port	Data Output Interface
Gigabit/SFP Ethernet ports Console Port	Control Input Interface
Gigabit/SFP Ethernet ports Console Port LEDs	Status Output Interface
Power plug	Power Interface

Table 3 – FIPS 140-2 Logical Interfaces

2.3 Roles and Services

Authentication in the module is identity-based. There are two main roles in the router that operators can assume:

1. the Crypto Officer role and
2. the User role.

The administrators 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. A detailed list of services attributed to each role can be found in section 2.3.2

2.3.1 Authentication

The module provides password based and digital signature based authentication. Crypto Officers are always authenticated using passwords whereas a User can be authenticated either via a password or digital signature.

a. Password based Authentication

The security policy stipulates that all user passwords and shared secrets must be 8 alphanumeric characters, so the password space is 2.8 trillion possible passwords. The possibility of randomly guessing a password is thus far less than one in one million. To exceed a one in 100,000 probability of a successful random password guess in one minute, an attacker would have to be capable of 28 million password attempts per minute, which far exceeds the operational capabilities of the module to support.

b. Digital signature based Authentication

When using RSA based authentication, RSA key pair has modulus size of 1024 bit to 2048 bit, thus providing between 80 bits and 112 bits of strength. Assuming the low end of that range, an attacker would have a 1 in 2^{80} chance of randomly obtaining the key, which is much stronger than the one in a million chance required by FIPS 140-2. To exceed a one in 100,000 probability of a successful random key guess in one minute, an attacker would have to be capable of approximately $1.8x10^{21}$ attempts per minute, which far exceeds the operational capabilities of the modules to support.

2.3.2 Services

a. User Services

Users can access the system via the console port with a terminal program or SSH session to an Ethernet port. The IOS prompts the User for username and password. If the password is correct, the User is allowed entry to the IOS executive program. In addition to username/password combination, RSA digital certificates can be used to authenticate the user over the SSH session.

The services available to the User role consist of the following:

Services & Access	Description	Keys & CSPs
Status Functions (r, x)	View state of interfaces and protocols, version of IOS currently running.	User password
Network	Connect to other network devices	DRBG seed, DRBG V, DH

Functions (r, w, x, z)	through SSH, telnet, PPP, etc. and initiate diagnostic network services (i.e., ping, mtrace).	shared secret, DH private exponent, SSH Private key, SSH session key
Terminal Functions	Adjust the terminal session (e.g., lock the terminal, adjust flow control).	N/A
Directory Services	Display directory of files kept in flash memory.	N/A
Perform Self-Tests	Perform the FIPS 140 start-up tests on demand	N/A

Table 4 - User Services

b. Crypto Officer Services

During initial configuration of the router, the Crypto Officer password (the "enable" password) is defined. A Crypto Officer can 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. Just like the User, the Crypto Officer can access the router via the console port or via SSH session.

The Crypto Officer services consist of the following:

Services & Access	Description	Keys & CSPs
Configure the router (r, w, z)	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.	User password, Enable password, RADIUS secret, TACACS+ secret, DH shared secret, Router Authentication key, PPP authentication key, SSH private key
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.	N/A
View Status Functions (r, x)	View the router configuration, routing tables, active sessions, use gets to view SNMP MIB statistics, health, temperature, memory status, voltage, packet statistics, review accounting logs, and view physical interface	User password, Enable password, RADIUS secret, TACACS+ secret, DH shared secret, Router Authentication key, PPP authentication key, SSH private key

	status.	
Manage the router (r, w)	Log off users, shutdown or reload the router, erase the flash memory, manually back up router configurations, view complete configurations, manager user rights, and restore router configurations.	User password, Enable password, RADIUS secret, TACACS+ secret, DH shared secret, Router Authentication key, PPP authentication key, SSH private key
Perform Self-Tests	Perform the FIPS 140 start-up tests on demand	N/A

r: read, w: write, x: execute, z: zeroize

Table 5 - Crypto Officer Services

2.3.3 Unauthenticated Services

The services available to unauthenticated users are:

- Viewing the status output from the module's LEDs
- Powering the module on and off using the power switch on the third-party chassis

2.4 Physical Security

This module is a multi-chip standalone cryptographic module.

The FIPS 140-2 level 2 physical security requirements for the modules are met by the use of opacity shields covering the front panels of modules to provide the required opacity and tamper evident seals to provide the required tamper evidence. The following sections illustrate the physical security provided by the module.

The tamper evident labels and opacity shields shall be installed for the module to operate in a FIPS Approved mode of operation. The following table shows the number of tamper evident labels and opacity shields. The CO is responsible for securing and having control at all times of any unused tamper evident labels.

Model	Tamper Evident Labels	Opacity Shields
7606-S	20	1
7609-S	15	N/A

Table 6 – TELs

2.4.1 Module Opacity

To install an opacity shield on the module, follow these steps:

1. The opacity shield is designed to be installed on a Catalyst 7606-S chassis that is already rack-mounted. If your Cisco 7606-S chassis is not rack-mounted, install the chassis in the

rack using the procedures contained in *Cisco 7600 Series Router Installation Guide*. If your Cisco 7606-S chassis is already rack-mounted, proceed to step 2.

2. Open the FIPS kit packaging (part number CVPN7600FIPS/KIT=). The kit contains the following items:
   - An opacity shield assembly for the Cisco 7606-S router (part number 800-26211). 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.
3. Remove the opacity shield from its protective packaging.
   - 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.
     Note: Verify that the thumbscrews are started only two or three turns in the opacity shield.
   - If the opacity shield comes with a bag of installation hardware (69-1483), 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.
   - Start the two thumbscrews in the corresponding threaded holes in the opacity shield (see Figure 5); two or three turns is sufficient. Do not thread the thumbscrews too far into the opacity shield.
   - 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.
   - 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 L-bracket screw holes on the chassis.
   - Press the opacity shield firmly against the side of the chassis and secure the opacity shield to the chassis with the two thumbscrews.

4. 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.
   Note: You might need to try different cutouts to find the one cutout that aligns correctly with a chassis air vent perforation.
5. Push the rivet pin through the rivet sleeve until you hear a click.
   Note: 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.
6. Repeat step 4 and step 5 for the remaining three snap rivet fasteners.

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.

Caution: 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.

Note: If you need to remove the 7606-S 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.

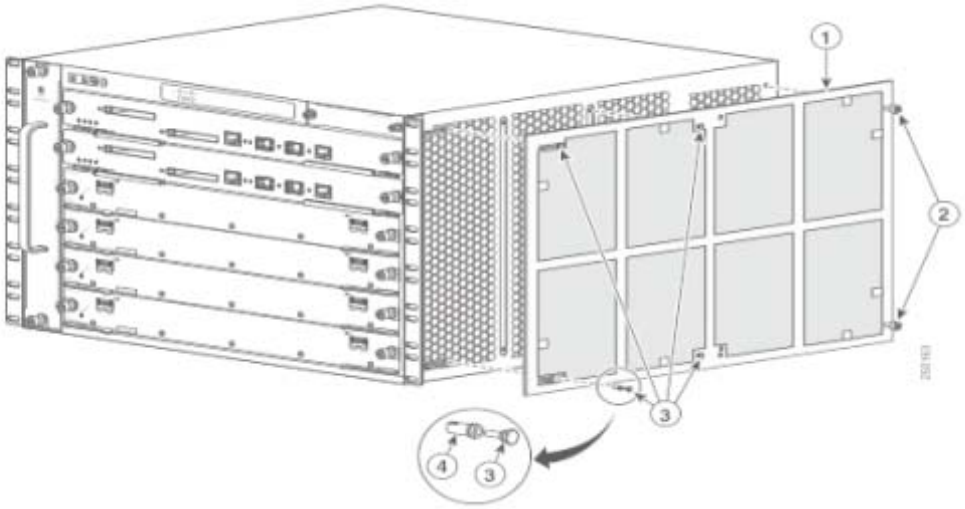


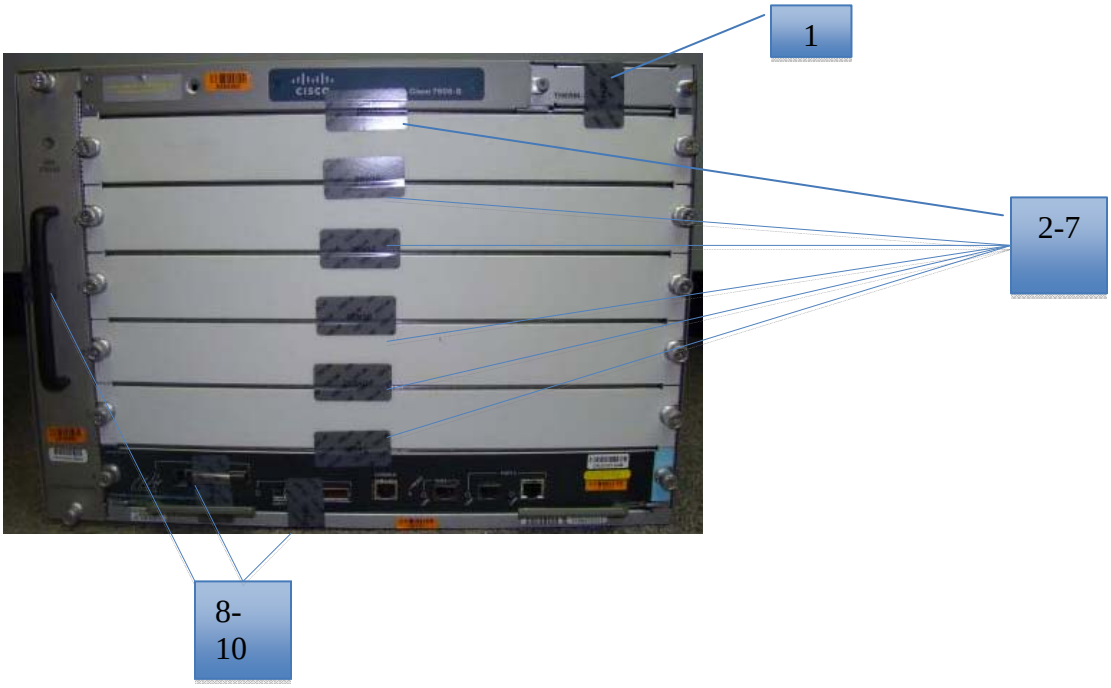
Figure 4 - Installing the Opacity Shield on the Cisco 7606-S Router

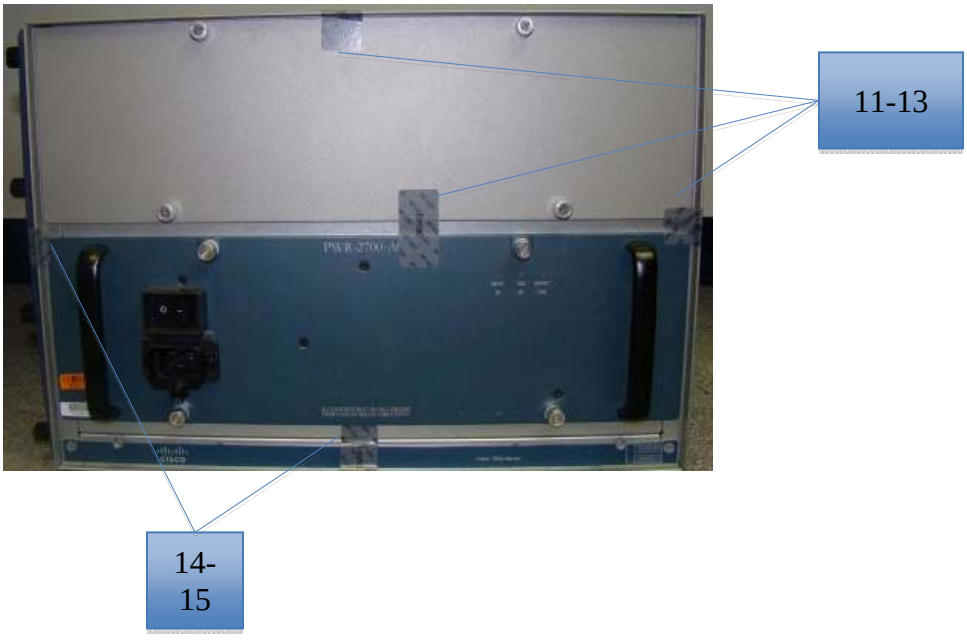
The 7609-S does not require any opacity shields.

2.4.2 Tamper Evidence

Once the module has been configured to meet overall FIPS 140-2 Level 2 requirements, the module cannot be accessed without signs of tampering. The CO shall inspect for signs of tampering periodically.

To seal the system, apply serialized tamper-evidence labels as depicted in the figures below.





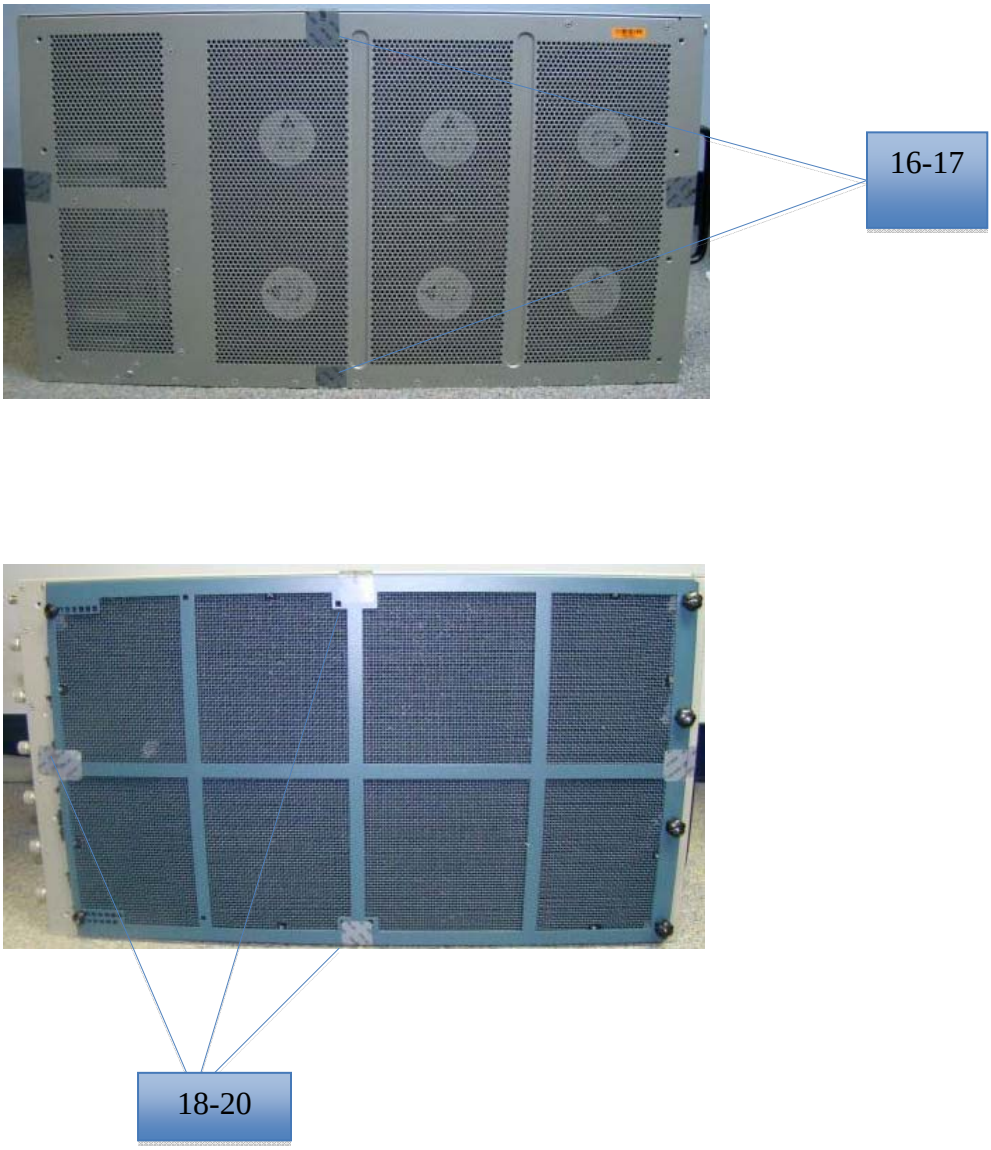
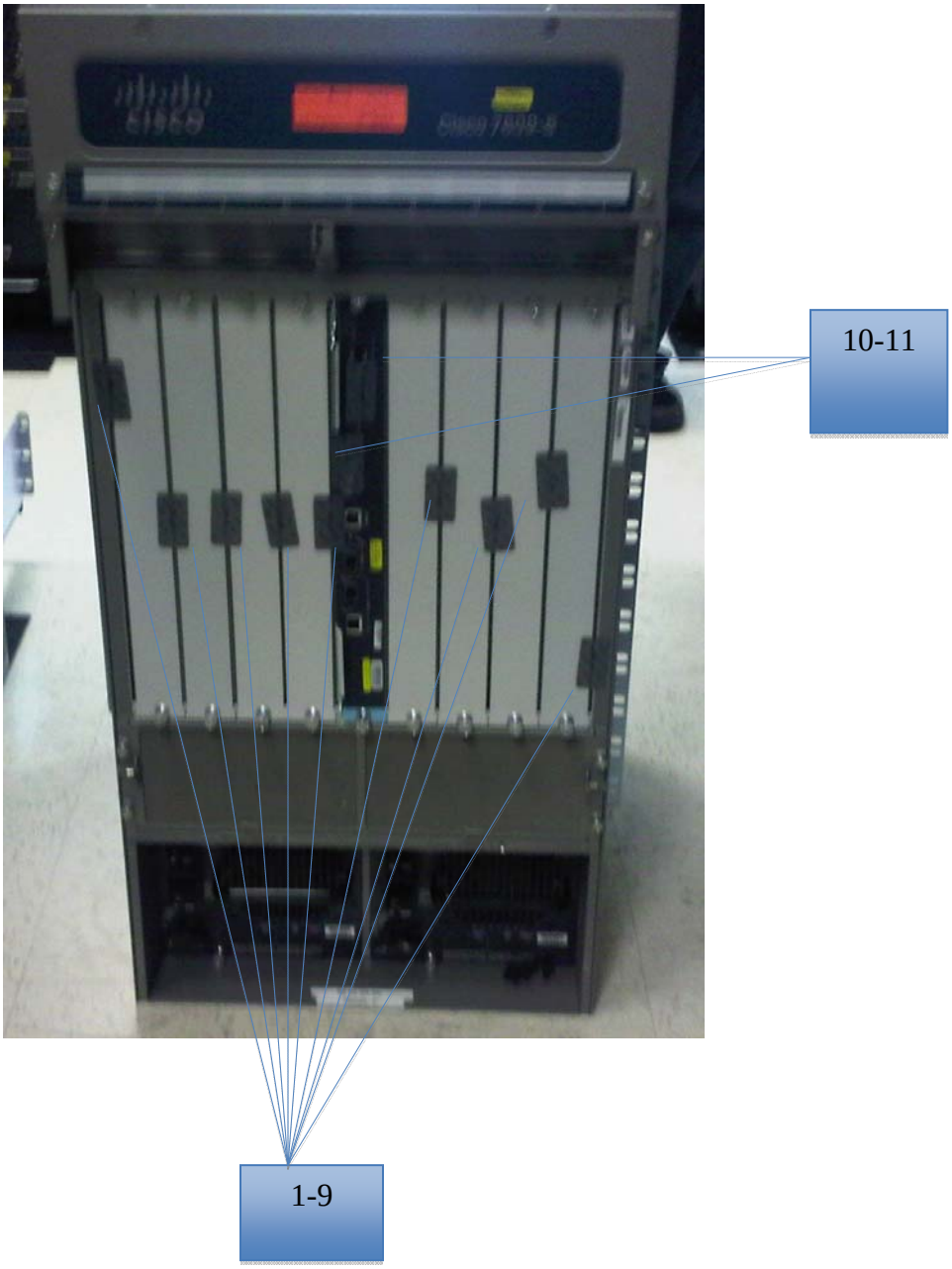


Figure 5 - TEL placement for 7606-S



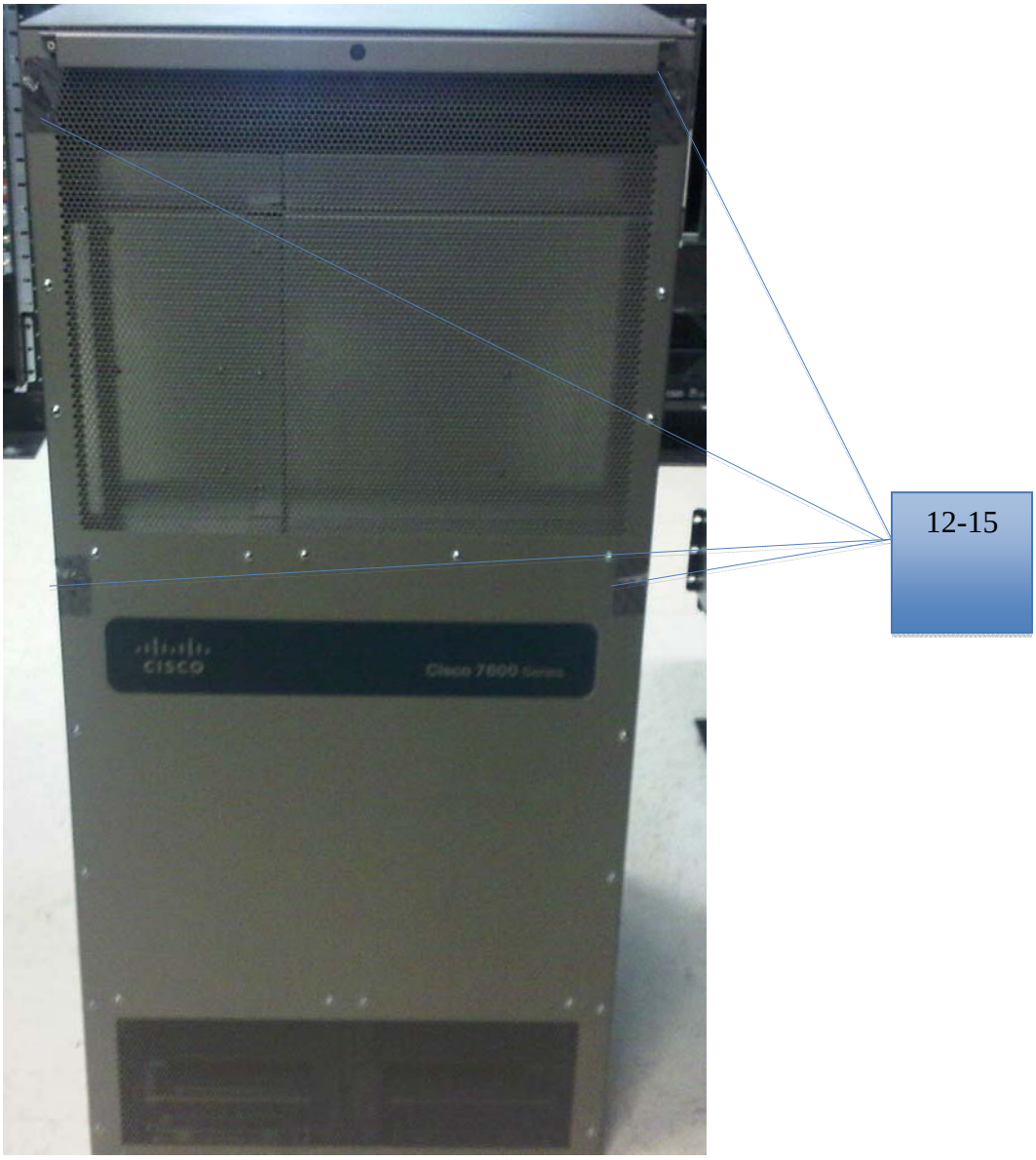


Figure 6 - TEL placement for 7609-S

2.5 Cryptographic Algorithms

The module implements a variety of approved and non-approved algorithms.

2.5.1 Approved Cryptographic Algorithms

The routers support the following FIPS-2 approved algorithm implementations:

Algorithm	
	IOS
AES	1634
Triple-DES	1070
SHS	1439
HMAC	961
DRBG	88
RSA	808

Table 7 Approved Cryptographic Algorithms

2.5.2 Non-FIPS Approved Algorithms Allowed in FIPS Mode

The module supports the following non-FIPS approved algorithms which are permitted for use in the FIPS approved mode:

- Diffie-Hellman (key agreement; key establishment methodology provides between 80 and 156 bits of encryption strength)
- RSA (key wrapping; key establishment methodology provides between 80 and 112 bits of encryption strength)

2.5.3 Non-Approved Cryptographic Algorithms

The module supports the following non-approved cryptographic algorithms that shall not be used in FIPS mode of operation:

- DES
- DES MAC
- MD5
- MD4
- HMAC MD5
- Non Approved RNGs

2.6 Cryptographic Key Management

The router securely administers both cryptographic keys and other critical security parameters such as passwords. All keys and CSPs are also protected by the password-protection provided by the crypto-officer logins and can be zeroized by either the Crypto Officer or User. Zeroization consists of overwriting the memory that stored the key or refreshing the volatile memory. Keys are both manually and electronically distributed but entered electronically. Manual distribution is used for pre-shared keys whereas SSH is used for electronic distribution.

The module supports the following types of key management schemes:

1. Pre-shared key exchange via electronic key entry. Triple-DES/AES key and HMAC-SHA-1 key are exchanged and entered electronically.
2. Diffie-Hellman key exchange is used to establish the Triple-DES or AES keys during SSHv2 exchange.

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 SSH protocol. RSA Public keys are entered into the modules using digital certificates which contain relevant data such as the name of the public key's owner, which associates the key with the correct entity. All other keys are associated with the user/role that entered them.

The module supports the following keys and critical security parameters (CSPs):

ID	Algorithm	Size	Description	Origin	Storage	Zeroization Method
General Keys/CSPs						
User password	Password	8 characters	Used to authenticate User role	Configured by Crypto Officer	NVRAM (plaintext)	Zeroized by overwriting with new password
Enable password	Password	8 characters	Used to authenticate Crypto Officer role	Configured during module initialization	NVRAM (plaintext)	Zeroized by overwriting with new password
RADIUS secret	Shared Secret	128 bits	Used to authenticate RADIUS server to module	Configured by Crypto Officer	NVRAM (plaintext)	Zeroized by "# no radius-server key"
TACACS+ secret	Shared Secret	128 bits	Used to authenticate TACACS+ server to module	Configured by Crypto Officer	NVRAM (plaintext)	Zeroized by "# no tacacs-server key"
DRBG Seed	SP 800-90	128-bits	This is the seed for SP 800-90 DRBG.	Generated by entropy source via the CTR_DRBG derivation function	DRAM (plaintext)	power cycle the device

DRBG V	SP 800-90	256-bits	This is the seed key for SP 800-90 DRBG.	generated from entropy source via the CTR_DRBG derivation function	DRAM (plaintext)	power cycle the device
Diffie Hellman shared secret	DH	1024-4096 bits	This is the shared secret agreed upon as part of DH exchange	N/A	DRAM (plaintext)	Zeroized upon deletion
Diffie Hellman private exponent	DH	1024-4096 bits	The private exponent used in Diffie-Hellman (DH) exchange.	Generated using FIPS approved DRBG	DRAM (plaintext)	Automatically after shared secret generated.
SSH keys/CSPs						
SSH Private key	RSA	1024-2048 bits	This is the SSH private key used to authenticate the module	Generated or entered like any RSA key	NVRAM (plaintext)	Zeroized by either deletion (via # crypto key zeroize rsa) or by overwriting with a new value of the key
SSH session key	Triple-DES/AES	3-key Triple-DES 128/192/256 bits AES keys	This is the symmetric SSH key used to protect SSH session	Created as part of SSH session set-up	DRAM (plaintext)	Zeroized automatically when SSH session is closed

Table 8 Cryptographic Keys and CSPs

2.7 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.

2.7.1 Self-tests performed by the IOS image

- IOS Self Tests
  - POST tests
    - AES Known Answer Test
    - RSA Signature Known Answer Test (both signature/verification)
    - Software/firmware test

        - DRBG Known Answer Test
        - HMAC-SHA-1 Known Answer Test
        - SHA-1/256/512 Known Answer Test
        - Triple-DES Known Answer Test
    - Conditional tests
        - Pairwise consistency test for RSA signature keys
        - Continuous random number generation test for approved and non-approved RNGs

3 Secure Operation

The module meets all the Level 2 requirements for FIPS 140-2. Follow the setting instructions provided below to place the module in FIPS-approved mode. Operating this router without maintaining the following settings will remove the module from the FIPS approved mode of operation.

3.1 System Initialization and Configuration

1. The Crypto Officer must perform the initial configuration. IOS version 15.1(2)S, filename: c7600s72033-adventerprisek9-mz.151-2.S.bin is the only allowable image; no other image should be loaded.
2. The value of the boot field must be 0x0102. 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 0x0102
```

3. The Crypto Officer must create the "enable" password for the Crypto Officer role. The password must be at least 8 characters (all digits; all lower and upper case letters; and all special characters except '?' are accepted) 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]
```

4. 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
```

5. The Crypto Officer shall only assign users to a privilege level 1 (the default).
6. The Crypto Officer shall not assign a command to any privilege level other than its default.

7. 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. RADIUS and TACACS+ shared secret key sizes must be at least 8 characters long.
8. Loading any IOS image onto the router is not allowed while in FIPS mode of operation.

3.2 Protocols

1. SNMPv3 is allowed in FIPS mode of operation. SNMPv3 uses FIPS approved cryptographic algorithms however from a FIPS perspective SNMPv3 is considered to be a plaintext session since the key derivation used as by SNMPv3 is not FIPS compliant.

3.3 Remote Access

1. 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. Note that all users must still authenticate after remote access is granted.