Cisco 7600 Series Routers with Supervisor RSP720

FIPS 140-2 Non Proprietary Security Policy
Level 1 Validation

Version 0.6

January, 2013

Table of Contents

1 Introduction

1.1 Purpose

This document is the non-proprietary Cryptographic Module Security Policy for the Cisco 7600 Series Routers with Supervisor RSP720. This security policy describes how the Cisco 7600 Series Routers with Supervisor RSP720 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 1 FIPS 140-2 validation of the Cisco 7600 Series Routers with Supervisor RSP720.

The module may be deployed in multiple configurations of line cards and supervisor cards installed in the module chassis. The following table identifies the possible combinations of hardware.

Chassis					Supervisor Cards								SPA Card
7603-S	7604	7606-S	7609-S	7613	Single RSP720-3CXL-10GE	Dual RSP720-3CXL-10GE	Single RSP720-3C-10GE	Dual RSP720-3C-10GE	Single RSP720-3CXL-GE	Dual RSP720-3CXL-GE	Single RSP720-3C-GE	Dual RSP720-3C-GE	ws-ipsec-3
X					X								X (up to 2)
X							X						X (up to 2)
X									X				X (up to 2)
X											X		X (up to 2)
	X				X								X (up to 3)
	X					X							X (up to 2)
	X						X						X (up to 3)
	X							X					X (up to 2)
	X								X				X (up to 3)
	X									X			X (up to 2)
	X										X		X (up to 3)
	X											X	X (up to 2)
		X			X								X (up to 5)
		X				X							X (up to 4)

Chassis					Supervisor Cards								SPA Card
7603-S	7604	7606-S	7609-S	7613	Single RSP720-3CXL-10GE	Dual RSP720-3CXL-10GE	Single RSP720-3C-10GE	Dual RSP720-3C-10GE	Single RSP720-3CXL-GE	Dual RSP720-3CXL-GE	Single RSP720-3C-GE	Dual RSP720-3C-GE	ws-ipsec-3
		X					X						X (up to 5)
		X						X					X (up to 4)
		X							X				X (up to 5)
		X								X			X (up to 4)
		X									X		X (up to 5)
		X										X	X (up to 4)
			X		X								X (up to 8)
			X			X							X (up to 7)
			X				X						X (up to 8)
			X					X					X (up to 7)
			X						X				X (up to 8)
			X							X			X (up to 7)
			X								X		X (up to 8)
			X									X	X (up to 7)
				X	X								X (up to 12)
				X		X							X (up to 11)
				X			X						X (up to 12)
				X				X					X (up to 11)
				X					X				X (up to 12)
				X						X			X (up to 11)
				X							X		X (up to 12)
				X								X	X (up to 11)

The following components have been included in this FIPS validation:

Model	Version

Chassis	
7603-S	7603-S
7604	7604
7606-S	7606-S
7609-S	7609-S
7613	7613
Supervisors	
RSP720-3CXL-10GE	V07
RSP720-3C-10GE	V07
RSP720-3CXL-GE	V14
RSP720-3C-GE	V13
Slot Cover	
SPA-BLANK	–F0
VPN Services Port Adapter (SPA)	
ws-ipsec-3	V02
IOS	
IOS firmware	15.1(3)S3

Table 1 Hardware and Firmware Versions

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	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	3
4	Finite State Model	1
5	Physical Security	1
6	Operational Environment	N/A
7	Cryptographic Key management	1
8	Electromagnetic Interface/Electromagnetic Compatibility	1
9	Self-Tests	1
10	Design Assurance	2
11	Mitigation of Other Attacks	1
	Overall module validation level	**1**

Table 2 Module Validation Level

1.3 References

This document deals only with operations and capabilities of the Cisco 7600 Series Routers with Supervisor RSP720 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 7600 Series Routers with Supervisor RSP720 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 7600 Series Routers with Supervisor RSP720 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 7600 Series Routers with Supervisor RSP720

The Cisco 7600 Router is a compact, high-performance router designed in 3, 4, 6, 9 and 13-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

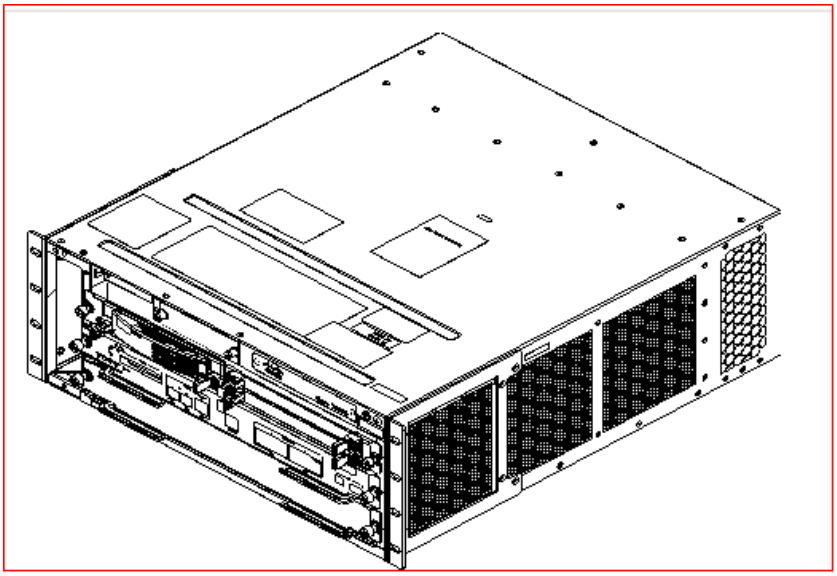

Figure 1 7603-S

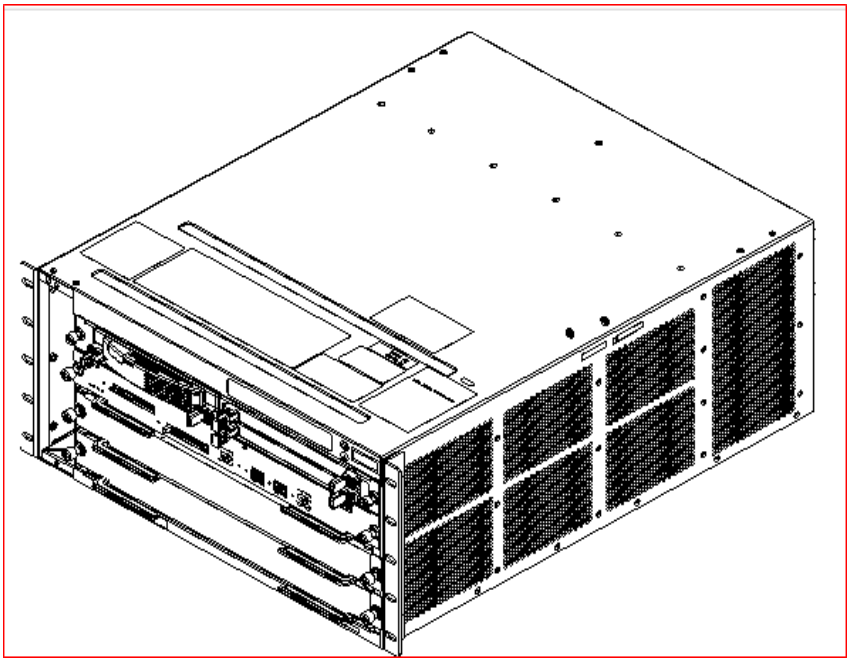

Figure 2 7604

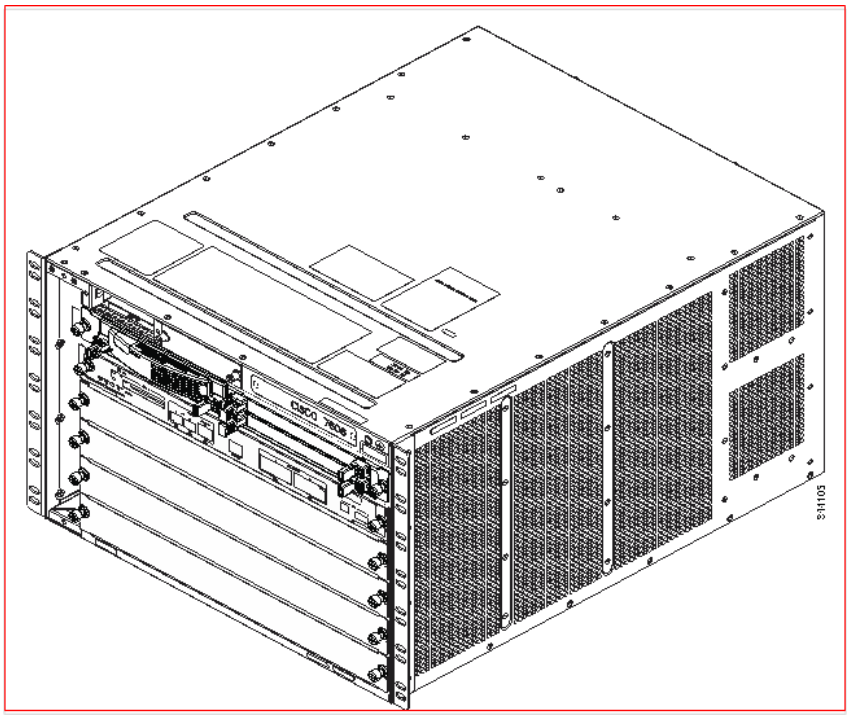

Figure 3 7606-S

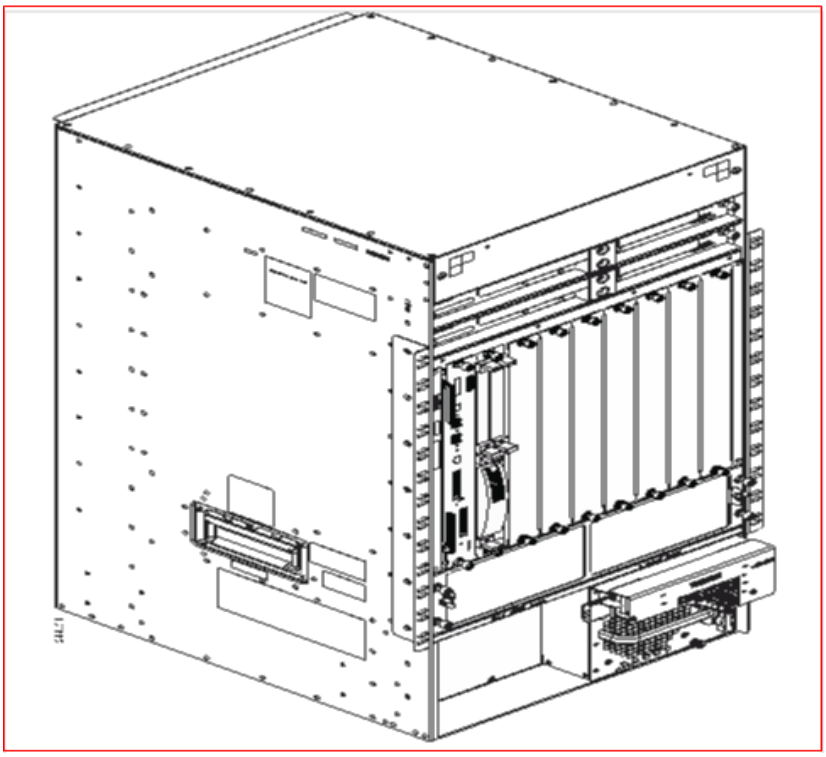

Figure 4 7609-S

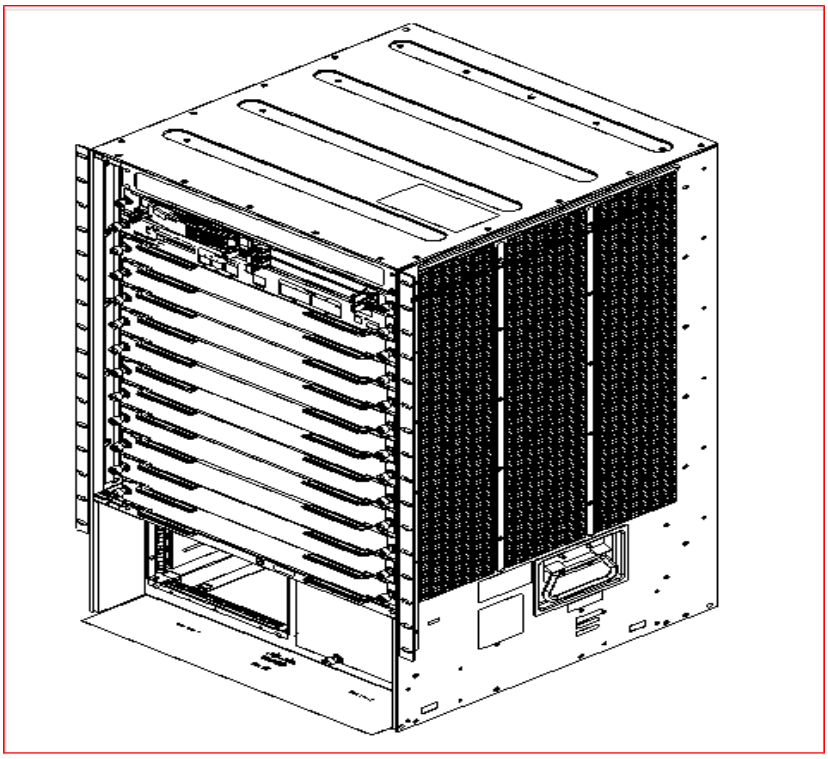

Figure 5 7613

This module is a multi-chip standalone cryptographic module. The cryptographic boundary is defined as being the physical enclosure of the chassis and is illustrated in figures 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 two supervisor cards, and one or more line cards in a single configuration.

NOTE: All cards/slot covers must be installed such that the module boundary is maintained and the connections to the cards are not exposed.

2.2 Module Interfaces

The module features the following interfaces:

FIPS 140-2 Logical Interface	RSP720-3C-GE/ RSP720-3CXL-GE	RSP720-3C-10GE/ RSP720-3CXL-10GE
Data Input Interface	Gigabit SFP ports (2) 10/100/1000 Ethernet port (1) Console Port	Gigabit SFP ports (2) 10/100/1000 Ethernet port (1) 10 GE X2 ports (2) Console Port
Data Output Interface	Gigabit SFP ports (2) 10/100/1000 Ethernet port (1) Console Port	Gigabit SFP ports (2) 10/100/1000 Ethernet port (1) 10 GE X2 ports (2) Console Port
Control Input Interface	Gigabit SFP ports (2) 10/100/1000 Ethernet port (1) Console Port	Gigabit SFP ports (2) 10/100/1000 Ethernet port (1) 10 GE X2 ports (2) Console Port
Status Output Interface	Gigabit SFP ports (2) 10/100/1000 Ethernet port (1) Console Port LEDs	Gigabit SFP ports (2) 10/100/1000 Ethernet port (1) 10 GE X2 ports (2) Console Port LEDs
Power Interface	Power plug (on the chassis)	
Disabled interfaces (via TEL)	Compact Flash Type II slots and USB ports on each RSP720-3C/3CXL-10GE card	

Table 3 - FIPS 140-2 Interfaces

These interfaces are depicted in the figures below:

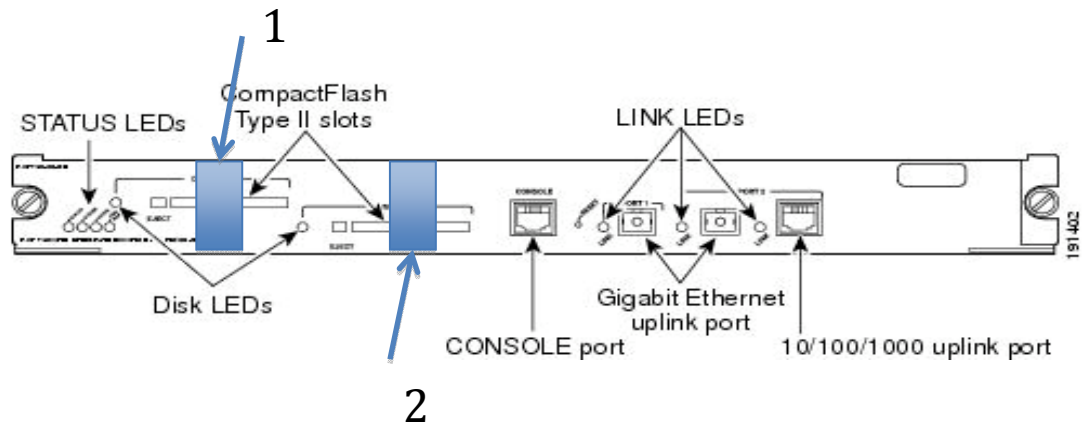

Figure 6 – RSP720-3C-GE/RSP720-3CXL-GE interfaces

NOTE: In Figure 6 above, the tamper seals labeled 1 and 2 cover compact flash slots.

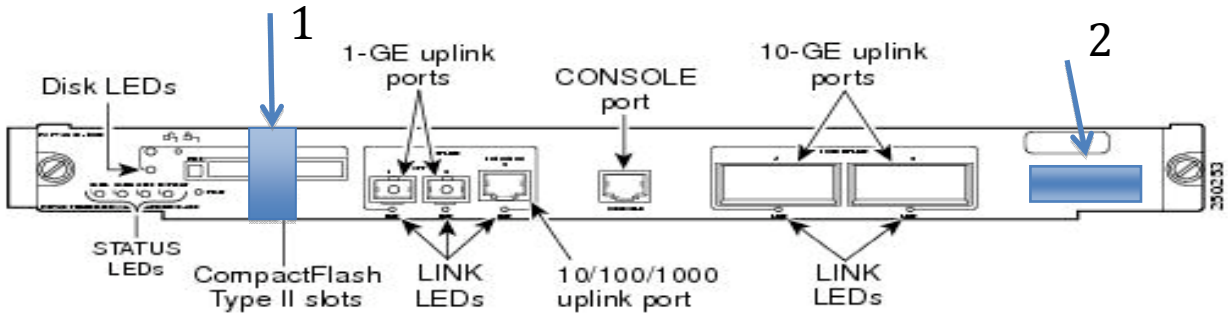

Figure 7 - RSP720-3C-10GE/RSP720-3CXL-10GE interfaces

Note: In Figure 7 above, tamper seal 1 covers one compact flash slot and tamper seal 2 covers two USB ports (two USB ports can be covered by one TEL on each RSP720-3C/3CXL-10GE card).

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 RSP is operational (normal initialization sequence)
	Orange	The module is booting or running diagnostics (normal initialization sequence)

	Yellow	Minor hardware problems.
	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
	Blinking Red	Continuous backplane stall
Active	Green	The RSP is operational and active.
	Orange	The RSP 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	Green	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.
Link	Green	The port is operational
	Orange	The port is disabled
	Flashing Orange	The port is bad
	Off	The supervisor engine or RSP is powering up or the port is enabled and there is no link

Table 4 – LED Indicators

2.3 Roles and Services

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

1. Crypto Officer role
2. 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 v2.0 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 Functions (r, w, x, z)	Connect to other network devices through FIPS approved services such as IKE, IPSec, DMVPN, SSH, telnet, PPP, etc. and initiate diagnostic network services (i.e., ping, mtrace).	DRBG seed, DRBG V, DH shared secret, DH private exponent, SSH RSA Private key, SSH session encryption 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
VPN functions (x)	Negotiation and encrypted data transport via VPN	skeyid, skeyid_d, IKE session encrypt key, IKE session authentication key, ISAKMP pre-shared key, IKE RSA Authentication private key, IPSec encryption key, IPSec authentication key
Perform Self-Tests	Perform the FIPS 140 start-up tests on demand	N/A

Table 5 - 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	User password, Enable password, RADIUS secret,

	aliases, set the protocols the router will support, enable interfaces and network services, set system date and time, and load authentication information.	TACACS+ secret, DH shared secret, Router Authentication key, , SSH RSA private key, ISAKMP pre-shared key, IKE RSA Authentication 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 status.	User password, Enable password, RADIUS secret, TACACS+ secret, DH shared secret, Router Authentication key, , SSH RSA private key
Manage the router (r, w, z)	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, , SSH RSA private key, skeyid, skeyid_d, IKE session encrypt key, IKE session authentication key, ISAKMP pre-shared key, IKE RSA Authentication private key, IPSec encryption key, IPSec authentication key
Set Encryption/Bypass (w)	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	ISAKMP pre-shared key, IKE RSA Authentication private key

	set from specified IP address.	
Perform Self-Tests	Perform the FIPS 140 start-up tests on demand	N/A

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

Table 6 - Crypto Officer Services

The following documents may be referenced for configuration of the services provided by the module:

- Cisco IOS Configuration Fundamentals Command Reference: www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_book.html
- Cisco IOS Security Command Reference: www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html

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
- Perform bypass services

2.4 Mitigation of Other Attacks

The module uses Tamper Evident Labels (TEL) to limit access to Compact Flash ports and USB ports (two USB ports are available on each RSP720-3C/3CXL-10GE card only) on RSP720 supervisors.

The tamper evident labels 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. The CO is responsible for securing and having control at all times of any unused tamper evident labels. If the CO must remove or change TELs (tamper-evidence labels) for any reason, the CO must examine the location from which the TEL was removed and ensure that no residual debris is still remaining on the chassis or card. If residual debris remains, the CO must remove the debris using a damp cloth.

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

The labels recommended for FIPS 140-2 compliance are provided in the FIPS kit (Cisco-FIPS-KIT=).

Model	Tamper Evident Labels
RSP7203C-GE/RSP720-3CXL-GE	2
RSP7203C-10GE/RSP720-3CXL-10GE	2

Table 7 – TELs

To limit access to Compact Flash card and USB ports, apply serialized tamper-evidence labels as depicted in the figures below.

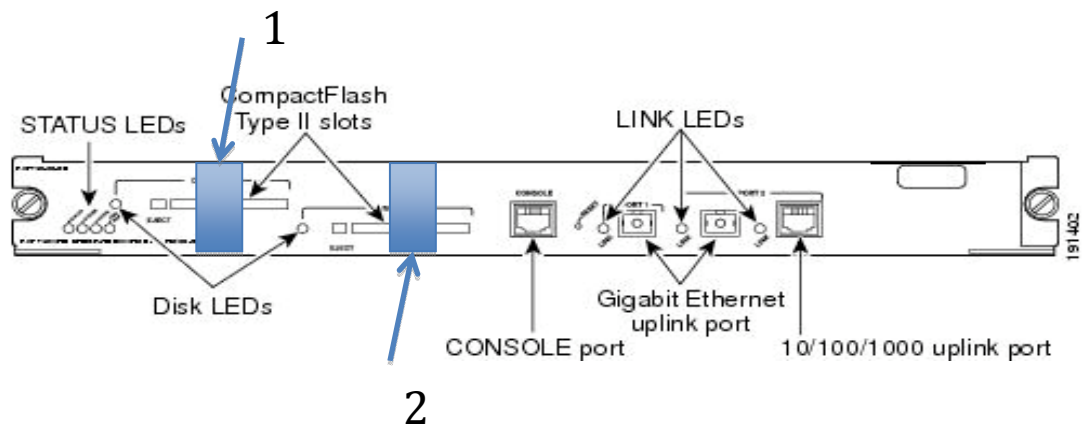

Figure 8 RSP720-3C-GE/RSP720-3CXL-GE

NOTE: In Figure 8 above, the tamper seals labeled 1 and 2 cover compact flash slots.

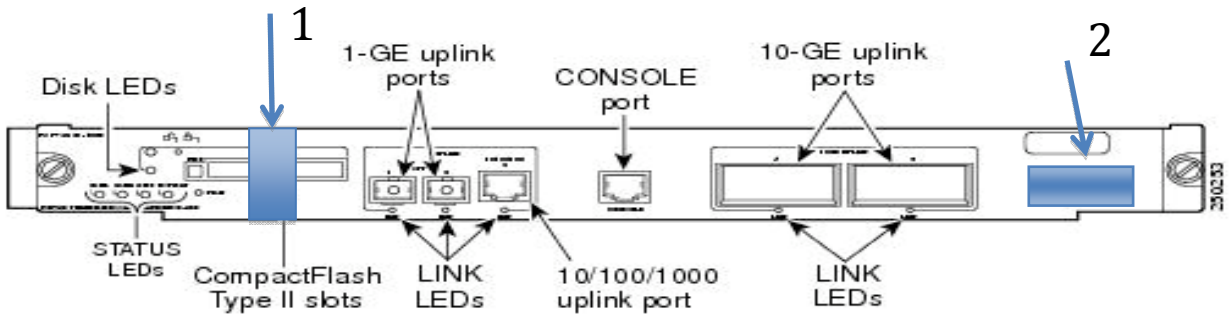

Figure 9 RSP720-3C-10GE/RSP720-3CXL-10GE

Note: In Figure 9 above, tamper seal 1 covers one compact flash slot and tamper seal 2 covers two USB ports (two USB ports can be covered by one TEL on each RSP720-3C/3CXL-10GE card).

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	ws-ipsec-3
AES	2036	598
Triple-DES	1312	569
SHS	1781	647
HMAC	1234	348
DRBG	198	N/A
RSA	1056	N/A

Table 8 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)

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

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:

- Diffie-Hellman (key establishment methodology provides between 80 and 112 bits of encryption strength)
- Internet Key Exchange Key Establishment (IKEv1/IKEv2)

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 and IKE protocols. 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 secret	Password	8 characters	Used to authenticate Crypto Officer role	Configured by Crypto Officer	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 entropy input	SP 800-90	256-bits	This is the entropy for SP 800-90 DRBG	Generated by internal entropy source	DRAM (plaintext)	Power cycle the device
DRBG Key	SP 800-90	256-bits	Internal key value used as part of SP 800-90 DRBG	Generated from entropy source via the CTR_DRBG derivation function	DRAM (plaintext)	Power cycle the device
DRBG Seed	SP 800-90	384-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	128-bits	Internal V value used as part of SP 800-90 CTR_DRBG	generated from entropy source via the CTR_DRBG derivation function	DRAM (plaintext)	power cycle the device

Diffie-Hellman shared secret	Diffie-Hellman	256 bits	This is the shared secret agreed upon as part of DH exchange	Derived in the module	DRAM (plaintext)	Zeroized upon deletion
Diffie-Hellman private exponent	Diffie-Hellman	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 RSA Private key	RSA	1024-2048 bits	This is the SSH private key used to authenticate the module	Generated using FIPS approved DRBG	NVRAM (plaintext)	Zeroized by either deletion (via # crypto key zeroize rsa) or by overwriting with a new value of the key
SSH session authentication key	HMAC-SHA-1	160-bits	This key is used to preform the authentication between the SSH client and SSH server	Derived as part of SSH session set-up	DRAM (plaintext)	Zeroized automatically when SSH sessions is closed
SSH session encryption key	Triple-DES/AES	Triple-DES (Key Size 168 bits)/AES (Key Size 128/192/256 bits)	This is the symmetric SSH key used to protect SSH session	Derived as part of SSH session set-up	DRAM (plaintext)	Zeroized automatically when SSH session is closed
IKE keys/CSPs						
skeyid	HMAC-SHA-1	160 bits	This is the key used for HMAC-SHA-1 during IKE	Value derived from the shared secret within IKE exchange	DRAM (plaintext)	Automatically after IKE session terminated.
skeyid_d	HMAC-SHA-1	160 bits	This is the IKE key derivation key for non ISAKMP security associations	Value derived from the shared secret within IKE exchange	DRAM (plaintext)	Automatically after IKE session terminated.
IKE session encrypt key	Triple-DES/AES	Triple-DES (Key Size 168 bits)/AES (Key Size 128/192/256 bits)	This is the key used to encrypt IKE sessions	Value derived from the shared secret within IKE exchange	DRAM (plaintext)	Automatically after IKE session terminated.
IKE session authentication key	HMAC-SHA-1	160 bits	This key is used to authenticate IKE sessions	Value derived from the shared secret within IKE exchange	DRAM (plaintext)	Automatically after IKE session terminated.

ISAKMP pre-shared key	Shared Secret	8 characters	The key used to generate IKE skeyid during preshared-key authentication. This key can have two forms based on whether the key is related to the hostname or the IP address.	Configured by Crypto Officer	NVRAM (plaintext)	Zeroized by "# no crypto isakmp key"
IKE RSA Authentication private key	RSA	1024-4096 bits	RSA private key for IKE authentication.	Generated using FIPS approved DRBG	NVRAM (plaintext)	Zeroized by "# crypto key zeroize rsa"
IPSec keys/CSPs						
IPSec encryption key	Triple-DES/AES	3-key Triple-DES 128/192/256 bits AES keys	This is the symmetric encryption key for IPSec	Derived as part of IPSec session	DRAM (plaintext)	Zeroized by "# Clear Crypto IPSec SA"
IPSec authentication key	HMAC-SHA-1	160 bits	This is the authentication key for IPSec	Derived as part of IPSec session	DRAM (plaintext)	Zeroized by "# Clear Crypto IPSec SA"

Table 9 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 Known Answer Test
    - Firmware Integrity Test
    - DRBG Known Answer Test
    - HMAC SHA-1 Known Answer Test
    - SHA-1Known Answer Test
    - Triple-DES Known Answer Test
  - Conditional tests
    - Pairwise consistency test for RSA

        - Continuous random number generation test for approved and non-approved RNGs
        - Conditional Bypass self-test

- ws-ipsec-3 Self Tests
    - POST tests
        - AES Known Answer Test
        - HMAC SHA-1 Known Answer Test
        - SHA-1 Known Answer Test
        - Triple-DES Known Answer Test

    - Conditional tests
        N/A

3 Secure Operation

The module meets all the Level 1 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 apply tamper evidence labels as described in the section "Mitigation of Other Attacks" above.
2. The Crypto Officer must perform the initial configuration. IOS version 15.1(3)S3, filename: c7600rsp72043-adventerprisek9-mz.151-3.S3.bin is the only allowable image; no other image should be loaded.
3. 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
```

4. 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]
```

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

3.2 IPSec Requirements and Crypto Algorithms

The only type of key management method allowed in FIPS mode is Internet Key Exchange (IKE).
Although the Cisco implementation of IKE allows a number of algorithms, only the following algorithms are allowed in a FIPS 140-2 configuration:

- ap-sha-hmac
- esp-sha-hmac
- esp-3des
- esp-aes

The following algorithms are not FIPS approved and should not be used during FIPS-approved mode:

- DES
- MD-5 for signing

3.3 Protocols

1. SNMP v3 over a secure IPSec tunnel may be employed for authenticated, secure SNMP gets and sets.

3.4 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.

3.5 Identifying Router Operation in an Approved Mode

The following activities are required to verify that that the module is operating in an Approved mode of operation.

1. Verify that the length of User and Crypto Officer passwords and all shared secrets are at least eight (8) characters long, include at least one letter, and include at least one number character, as specified in the “Secure Operation” section of this document.
2. Issue the following commands: 'show crypto ipsec sa' and 'show crypto isakmp policy' to verify that only FIPS approved algorithms are used.