Cisco Firepower Threat Defense Cryptographic Module

FIPS 140-2 Non Proprietary Security Policy
Level 2 Validation

Version 1.2

July 23, 2020

1 Introduction

1.1 Purpose

This is the non-proprietary cryptographic module security policy for the Cisco Firepower Threat Defense Cryptographic Module running in FTD firmware version 6.4. This security policy describes how this module meets the security requirements of FIPS 140-2 Level 2 and how to run the module in a FIPS 140-2 mode of operation. This Security Policy may be freely distributed.

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 with the specification of the security rules listed in Table 1 above, under which the Cisco Firepower Threat Defense Cryptographic Module will operate, including the rules derived from the requirements of FIPS 140-2, FIPS 140-2 IG and additional rules imposed by Cisco Systems, Inc. More information is available on the module from the following sources:

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

http://www.cisco.com/c/en/us/products/index.html
http://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/roadmap/fxos-roadmap.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 Firepower Threat Defense Cryptographic Module identified is referred to as Cryptographic Module, CM, Module, Modules, Appliances or Systems.

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

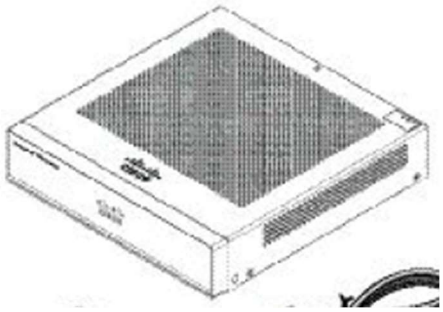
This document provides an overview of the Cisco Firepower Threat Defense Cryptographic Module identified above and explains the secure layout, configuration and operation of the module. This introduction section is followed by Section 2, which details the general features and functionality of the module. 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 Firepower (FPR) 1K and 2K Series Appliances

The Cisco Firepower 1K and 2K appliances can be deployed either as a Next-Generation Firewall (NGFW) or as a Next-Generation IPS (NGIPS on 2K unit). Which are perfect from the internet edge all the way in to the data center.

Cisco FPR1010 with 650 Mbps throughput is a desktop unit. Both Cisco FPR1120 and Cisco FPR1140 are rack mount units. Both FPR1120 and FPR1140 have the same physical appearance, but the FPR1120 provides 1.5 Gbps throughput, and FPR1140 offers 2.2 Gbps throughput.



Firepower 1010

Firepower 1120 and 1140

The Cisco Firepower 2K is four identical looking appliances, FPR2110 and FPR2120 models offer 1.9 and 3 Gbps of firewall throughput and FPR2130 and FPR2140 models providing 5 and 8.5 Gbps of firewall throughput.

Firepower 2100 Series

When deployed as the Next-Generation Firewall (NGFW), they use the Cisco Firepower Threat Defense. The sections throughout this SP detail the FIPS compliance of the Cryptographic Module contained within the FTD which houses ASA, FX-OS and Firepower solutions found. The ASA delivers enterprise-class firewall for businesses, improving security at the Internet edge, high performance and throughput for demanding enterprise data centers. The ASA solution offers the combination of the industry's most deployed stateful firewall with a comprehensive range of next-generation network security services, intrusion prevention system (IPS), content security, secure unified communications, TLSv2, SSHv2, IKEv2 and Cryptographic Cipher Suite B.

The Firepower eXtensible Operating System (FX-OS), a next-generation network and content security solutions, provides a web interface that makes it easy to configure platform settings and interfaces, provision devices, and monitor system status. The FX-OS is part of the Cisco Application Centric Infrastructure (ACI) Security Solution and provides an agile, open, built for scalability, consistent control, and simplified management. The FX-OS provides the following features:

- Modular chassis-based security system—provides high performance, flexible input/output configurations, and scalability.
- Firepower Chassis Manager—graphical user interface provides streamlined, visual representation of current chassis status and simplified configuration of chassis features.
- FX-OS CLI—provides command-based interface for configuring features, monitoring chassis status, and accessing advanced troubleshooting features.

The Firepower provides balanced security effectiveness with productivity. The module is designed to help handle network traffic in a way that complies with an organization’s security policy—guidelines for protecting the network. An organization’s security policy may also include an acceptable use policy (AUP), which provides employees with guidelines of how they may use systems.

The module has been tested on the following platforms:

FPR1010	FPR1120	FPR1140
FPR2110	FPR2120	FPR2130
FPR2140		

2.1 Cryptographic Module Characteristics

The module is contained in the Cisco Firepower 1K and 2K appliances executing on the Intel Atom processor (FPR1K) or Intel Xeon processors with Cavium Octeon as the hardware accelerator (FPR2K). The module uses a non-modifiable operational environment.

2.2 Cryptographic Boundary

The module is a multi-chip standalone cryptographic module. The cryptographic boundary is defined as the module’s chassis unit encompassing the "top," "front," "left," "right," “rear” and "bottom" surfaces of the case representing the module’s physical perimeter. Diagram 1 below is the block diagram showing the module running on each hardware platform.

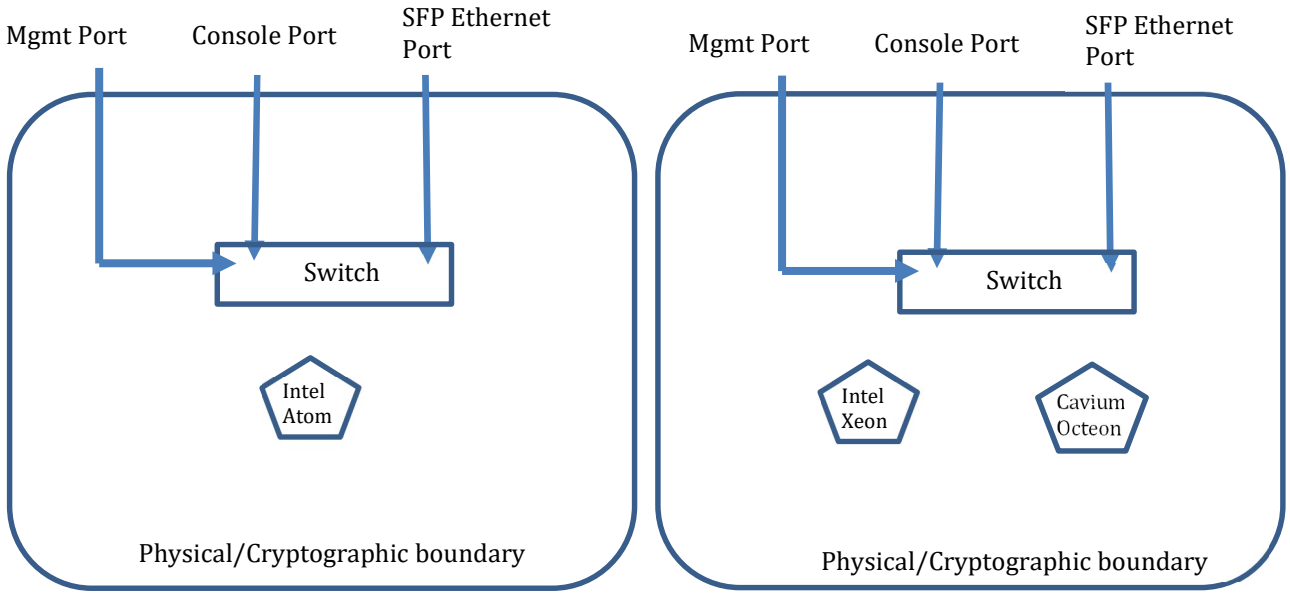


Diagram 1 Block Diagram, FPR1K unit on Left and FPR2K unit on the right

2.3 Module Interfaces

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 module provides no power to external devices and takes in its power through normal power input/cord. The logical interfaces and their mapping are described in the following table:

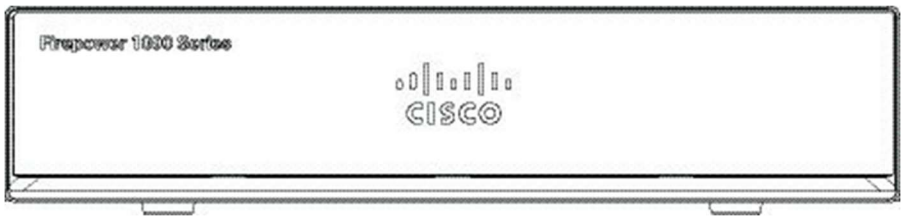
FIPS 140-2 Logical Interface	1K and 2K Physical Interfaces
Data Input	MGMT Port Console port SFP/SFP+ Ethernet and/or RJ-45 Gigabit Ethernet Ports
Data Output	MGMT Port Console port SFP/SFP+ Ethernet and/or RJ-45 Gigabit Ethernet Ports
Control Input	MGMT Port Console port SFP/SFP+ Ethernet and/or RJ-45 Gigabit Ethernet Ports
Status Output	MGMT Port Console port SFP/SFP+ Ethernet and/or RJ-45 Gigabit Ethernet Ports LEDs

Table 2 Logical/Physical Boundary Interfaces

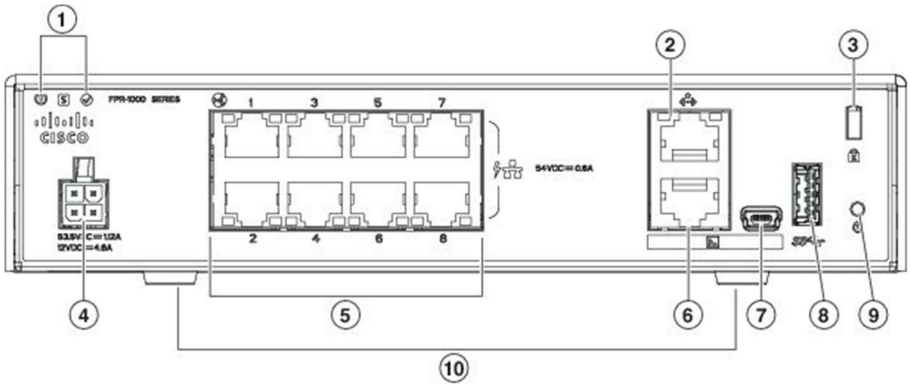
Note: Each module has USB ports, but they are considered to be disabled after the Crypto-Officer applied the TEL labels.

2.4 FPR1K Front and Rear Panels

FPR1010 Front

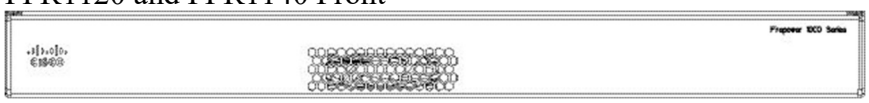


FPR1010 Rear

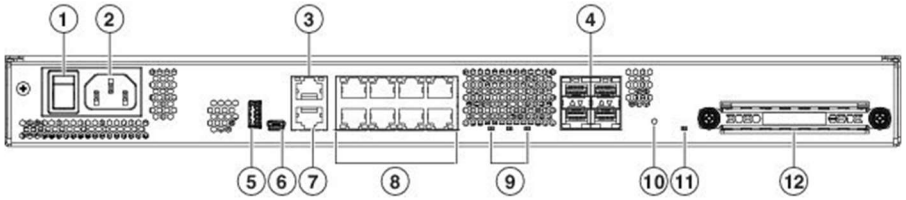


1	Status LED	2	Mgmt Port
3	Lock Slot	4	Power cord socket
5	Network data ports	6	Console port
7	USB port (not to use in FIPS mode)	8	USB port (not to use in FIPS mode)
9	Reset button	10	Rubber feet

FPR1120 and FPR1140 Front



FPR1120 and FPR1140 Rear

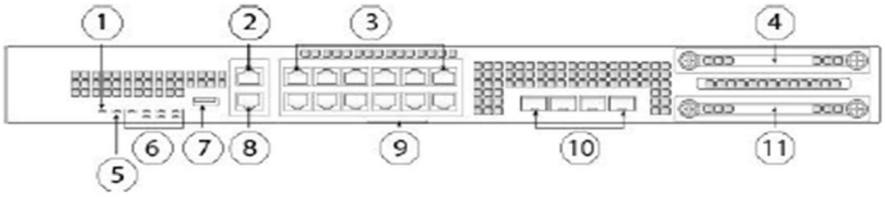


1	Power switch	2	Power cord socket
3	Mgmt Port	4	SFP ports
5	USB port (not to use in FIPS mode)	6	USB port (not to use in FIPS mode)
7	Console port	8	Network data ports
9	Status LED	10	Reset button

11	SSD LED	12	SSD BAY

2.5 FPR2K Front and Rear Panels

FPR2110 and FPR2120 Front

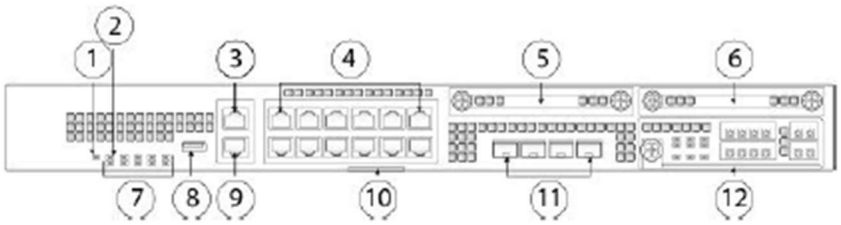


1	**Power LED**	**2**	**One Gigabit Ethernet management port**
3	**12 RJ-45 1G/100M/10M auto duplex/auto MDI-X Base-T ports** **Ethernet 1 through 12 labeled top to bottom, left to right**	**4**	**SSD 1**
5	**Locator beacon**	**6**	**System LEDs**
7	**Type A USB 2.0 port**	**8**	**RJ-45 console port**
9	**Pull-out label card**	**10**	**Four fixed SFP (1G) ports (2110 and 2120)** **Fiber ports 13 through 16 labeled left to right**
11	**SSD 2**		

FPR2110 and FPR2120 Rear

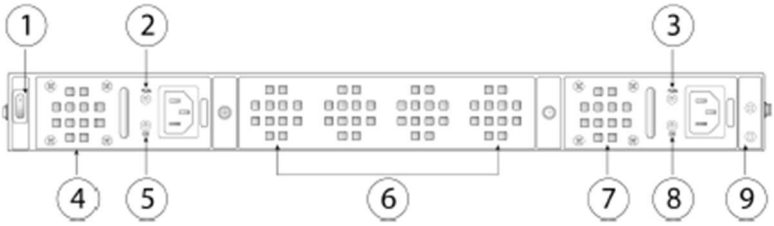
1	**Power on/off switch**	**2**	**Fixed power supply module**
3	**Fixed fan tray**	**4**	**Location of the two-post grounding lug** **Note** The two-post grounding lug is included in the accessory kit.

FPR2130 and FPR2140 Front



1	Power LED	**2**	Locator LED
3	One Gigabit Ethernet management port	**4**	12 RJ-45 1G/100M/10M auto duplex/auto MDI-X Base-T ports Ethernet 1 through 12 labeled top to bottom, left to right
5	SSD 1	**6**	SSD 2
7	System LEDs	**8**	Type A USB 2.0 port
9	RJ-45 console port	**10**	Pull-out label card
11	Four fixed SFP+ (1G/10G) ports (2130 and 2140) Fiber ports 13 through 16 labeled left to right	**12**	Network Module (network module slot 1)

FPR2130 and FPR2140 Rear



1	Power on/off switch	**2**	Power supply module 1 FAIL LED
3	Power supply module 2 FAIL LED	**4**	Power supply module 1
5	Power supply module 1 OK LED	**6**	Fan tray
7	Power supply module 2	**8**	Power supply module 2 OK LED
9	Location of the two-post grounding lug **Note** The two-post grounding lug is included in the accessory kit.		

2.6 Roles and Services

The module can be accessed in one of the following ways:

- Console
- SSHv2
- HTTPS/TLSv1.2
- IPSec/IKEv2

Authentication is identity-based. As required by FIPS 140-2, there are two roles that operators may assume: Crypto Officer role and User role. The module upon initial access to the module authenticates both of these roles. The module also supports RADIUS and TACACS+ as another means of authentication, allowing the storage of usernames and passwords on an external server as opposed to using the module's internal database for storage.

The User and Crypto Officer passwords and all other shared secrets must each be at least eight (8) characters long, including at least one six (6) alphabetic characters, (1) integer number and one (1) special character in length (enforced procedurally). See the Secure Operation section for more information. Given these restrictions, the probability of randomly guessing the correct sequence is one (1) in 6,326,595,092,480 (this calculation is based on the assumption that the typical standard American QWERTY computer keyboard has 10 Integer digits, 52 alphabetic characters, and 32 special characters providing 94 characters to choose from in total). The calculation should be 52x52x52x52x52x52x32x10 = 6,326,595,092,480. Therefore, the associated probability of a successful random attempt is approximately 1 in 6,326,595,092,480, which is less than the 1 in 1,000,000 required by FIPS 140-2.

In addition, for multiple attempts to use the authentication mechanism during a one-minute period, under the optimal modern network condition, if an attacker would only get 60,000 guesses per minute. Therefore, the associated probability of a successful random attempt during a one-minute period is 60,000/ 6,326,595,092,480 = 1/105,443,251, which is less than 1 in 100,000 required by FIPS 140-2.

Additionally, when using RSA based authentication, RSA key pair has modulus size of 2048 bits, thus providing 112 bits of strength, which means an attacker would have a 1 in 2112 chance of randomly obtaining the key, which is much stronger than the one in a million chances 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 8.65x1031 (2112 /60 = 8.65 x 1031) attempts per second, which far exceeds the operational capabilities of the module to support.

2.7 User Services

A User enters the system by accessing the Console port, SSHv2, or HTTPS/TLSv1.2. The User role can be authenticated via either User Name/Password or RSA based authentication method. The module prompts the User for username and password. If the password is correct, the User is allowed entry to the module management functionality. The other means of accessing the console is via an IPSec session. This session is authenticated either using a shared secret or RSA digital signature authentication mechanism. The services available to the User role accessing the CSPs, the type of access – read (r), write (w) and zeroized/delete (d) – and which role accesses the CSPs are listed below:

Services	Description	Keys and CSPs Access
Status Functions	View the module configuration, routing tables, active sessions health, and view physical interface status.	Operator password (r, w, d)
Terminal Functions	Adjust the terminal session (e.g., lock the terminal, adjust flow control).	Operator password (r, w, d)
Directory Services	Display directory of files kept in flash memory.	Operator password (r, w, d)
Self-Tests	Execute the FIPS 140 start-up tests on demand.	N/A
IPSec VPN	Negotiation and encrypted data transport via IPSec VPN.	Operator password, skeyid, skeyid_d, SKEYSEED, IKE session encrypt key, IKE session authentication key, ISAKMP preshared, IKE authentication private Key, IKE authentication public key, ECDSA private key, ECDSA public key, IPSec encryption key, IPSec authentication key, DRBG entropy input, DRBG seed, DRBG V and DRBG key (r, w, d)
SSHv2 Functions	Negotiation and encrypted data transport via SSHv2.	Operator password, SSHv2 RSA private key, SSHv2 RSA public key, SSHv2 integrity key, SSHv2 session key, DRBG entropy input, DRBG seed, DRBG V and DRBG key (r, w, d)
HTTPS Functions (TLSv1.2)	Negotiation and encrypted data transport via HTTPS/TLSv1.2.	Operator password, DRBG entropy input, DRBG Seed, DRBG V, DRBG Key, ECDSA private key, ECDSA public key, TLS RSA private key, TLS RSA public key, TLS pre-master secret, TLS master secret, TLS encryption keys and TLS integrity key (r, w, d)

Table 3 User Services

2.8 Crypto Officer Services

The Crypto Officer role is responsible for the configuration of the module. A Crypto Officer enters the system by accessing the Console port, SSHv2, HTTPS/TLSv1.2 or IPSec/IKEv2. The CO role can be authenticated via either User Name/Password or RSA based authentication method. The services available to the Crypto Officer role accessing the CSPs, the type of access – read (r), write (w) and zeroized/delete (d) – and which role accesses the CSPs are listed below:

Services	Description	Keys and CSPs Access
Configure the Security	Define network interfaces and settings, create command aliases, set the protocols the appliance will support, enable interfaces and network services, set system date and time, and load authentication information.	Operator password, Crypto Officer password, SSHv2 RSA private key, SSHv2 RSA public key, SSHv2 integrity key, SSHv2 session key, TLS RSA private key, TLS RSA public key, TLS pre-master secret, TLS master secret, TLS encryption keys, TLS integrity key, ISAKMP preshared, IKE session encrypt key, IKE session authentication key, IKE authentication private Key, IKE authentication public key, IPSec encryption key and IPSec authentication key (r, w, d)
Firmware Installation	Install the firmware during the System Initialization.	N/A
Configure External Authentication Server	Configure Client/Server authentication.	RADIUS secret, TACACS+ secret (r, w, d)
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.	Operator password, Crypto Officer password (r, w, d)
View Status Functions	View the appliance configuration, routing tables, active sessions health, temperature, memory status, voltage, packet statistics, review accounting logs, and view physical interface status.	Operator password, Crypto Officer password (r, w, d)
HTTPS/TLS (TLSv1.2)	Configure HTTPS/TLS parameters, provide entry and output of CSPs.	DRBG entropy input, DRBG Seed, DRBG V, DRBG Key, ECDSA private key, ECDSA public key, TLS RSA private key, TLS RSA public key, TLS pre-master secret, TLS master secret, TLS encryption keys and TLS integrity key (r, w, d)
IPSec VPN	Configure IPSec VPN parameters, provide entry and output of CSPs.	DRBG entropy input, DRBG Seed, DRBG V, DRBG Key, ISAKMP preshared, skeyid, skeyid_d, SKEYSEED, IKE session encrypt key, IKE session authentication key, IKE authentication private Key, IKE authentication public key,

		ECDSA private key, ECDSA public key, IPSec encryption key, IPSec authentication key (r, w, d)
SSHv2 Function	Configure SSHv2 parameter, provide entry and output of CSPs.	DRBG entropy input, DRBG Seed, DRBG V, DRBG Key, Diffie-Hellman private key, Diffie-Hellman public key, Diffie-Hellman Shared Secret, EC Diffie-Hellman private key, EC Diffie-Hellman public key, EC Diffie-Hellman Shared Secret, SSHv2 private key, SSHv2 public key,SSHv2 integrity key and SSHv2 session key (r, w, d)
Self-Tests	Execute the FIPS 140 start-up tests on demand.	N/A
User services	The Crypto Officer has access to all User services.	Operator password (r, w, d)
Zeroization	Zeroize cryptographic keys/CSPs by running the zeroization methods classified in table 6, Zeroization column.	All CSPs (d)

Table 4 Crypto Officer Services

2.9 Non-FIPS mode Services

The cryptographic module in addition to the above listed FIPS mode of operation can operate in a non-FIPS mode of operation. This is not a recommended operational mode but because the associated RFC's for the following protocols allow for non-approved algorithms and non-approved key sizes a non-approved mode of operation exist. So those services listed above with their FIPS approved algorithms in addition to the following services with their non-approved algorithms and non-approved keys sizes are available to the User and the Crypto Officer. Prior to using any of the Non-Approved services listed in Table 5 below, the Crypto Officer must zeroize all CSPs which places the module into the non-FIPS mode of operation, and vice versa.

Services [1]	**Non-Approved Algorithms**
SSH	Hashing: MD5 MACing: HMAC MD5 Symmetric: DES Asymmetric: 768-bit/1024-bit RSA (key transport), 1024-bit Diffie-Hellman
IPSec	Hashing: MD5 MACing: HMAC MD5 Symmetric: DES, RC4 Asymmetric: 768-bit/1024-bit RSA (key transport), 1024-bit Diffie-Hellman
TLS	Symmetric: DES, RC4 Asymmetric: 768-bit/1024-bit RSA (key transport), 1024-bit Diffie-Hellman

Table 5 Non-approved algorithms in the Non-FIPS mode services

Neither the User nor the Crypto Officer are allowed to operate any of these services while in FIPS mode of operation.

All services available can be found at https://www.cisco.com/c/en/us/td/docs/security/firepower/622/fdm/fptd-fdm-config-guide-622.html.

2.10 Unauthenticated Services

The services for someone without an authorized role are to view the status output from the module's LED pins and cycle power.

[1] These approved services become non-approved when using any non-approved algorithms or non-approved key or curve sizes. When using approved algorithms and key sizes these services are approved.

2.11 Operational Environment

The module is a hardware module. The Cisco operating system provides a proprietary and non-modifiable operating system. Thus, the requirements from FIPS 140-2 level 2, section 4.6.1, are not applicable to the module.

2.12 Cryptographic Key/CSP Management

The module administers both cryptographic keys and other critical security parameters such as passwords. All keys and CSPs are protected by the password-protection of the Crypto Officer role login, and can be zeroized by the Crypto Officer. 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. Persistent keys with manual distribution are used for pre-shared keys whereas protocols such as IKE, TLS and SSH are used for electronic distribution.

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. Only an authenticated Crypto Officer can view the keys. All Diffie-Hellman (DH)/ECDH keys agreed upon for individual tunnels are directly associated with that specific tunnel only via the IKE protocol. All other keys are associated with the user/role that entered them. The entropy source (NDRNG) within the module provides at least 256 bits of entropy to seed SP800-90a DRBG for use in key generation.

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
DRBG entropy input	SP800-90A CTR_DRBG (AES-256)	384-bits	This is the entropy for SP 800-90A CTR_DRBG. Used to construct the seed.	DRAM (plaintext)	Power cycle the device
DRBG seed	SP800-90A CTR_DRBG (AES-256)	384-bits	Input to the DRBG that determines the internal state of the DRBG. Generated using DRBG derivation function that includes the entropy input from the entropy source.	DRAM (plaintext)	Power cycle the device
DRBG V	SP800-90A CTR_DRBG (AES-256)	128-bits	The DRBG V is one of the critical values of the internal state upon which the security of this DRBG mechanism depends. Generated first during DRBG instantiation and then subsequently updated using the DRBG update function.	DRAM (plaintext)	Power cycle the device
DRBG key	SP800-90A CTR_DRBG (AES-256)	256-bits	Internal critical value used as part of SP 800-90A CTR_DRBG. Established per SP 800-90A CTR_DRBG.	DRAM (plaintext)	Power cycle the device
Diffie-Hellman shared secret	DH	2048 – 4096 bits	The shared secret used in Diffie-Hellman (DH) exchange. Established per the Diffie-Hellman key agreement.	DRAM (plaintext)	Power cycle the device

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
Diffie-Hellman private key	DH	224-384 bits	The private key used in Diffie-Hellman (DH) exchange. This key is generated by calling SP800-90A DRBG.	DRAM (plaintext)	Power cycle the device
Diffie Hellman public key	DH	2048 – 4096 bits	The public key used in Diffie-Hellman (DH) exchange. This key is derived per the Diffie-Hellman key agreement.	DRAM (plaintext)	Power cycle the device
EC Diffie-Hellman shared Secret	ECDH	P-256, P-384, P-521 Curves	The shared secret used in Elliptic Curve Diffie-Hellman (ECDH) exchange. Established per the Elliptic Curve Diffie-Hellman (ECDH) protocol.	DRAM (plaintext)	Power cycle the device
EC Diffie-Hellman private key	ECDH	P-256, P-384, P-521 Curves	Used in establishing the session key for an IPSec session. The private key used in Elliptic Curve Diffie-Hellman (ECDH) exchange. This key is established per the EC Diffie-Hellman key agreement	DRAM (plaintext)	Power cycle the device
EC Diffie-Hellman public key	ECDH	P-256, P-384, P-521 Curves	Used in establishing the session key for an IPSec session. The public key used in Elliptic Curve Diffie-Hellman (ECDH) exchange. This key is established per the EC Diffie-Hellman key agreement	DRAM (plaintext)	Power cycle the device
skeyid	Keying material	160 bits	A shared secret known only to IKE peers. It was established via key derivation function defined in SP800-135 KDF and it will be used for deriving other keys in IKE protocol implementation.	DRAM (plaintext)	Automatically when IPSec/IKE session is terminated
skeyid_d	Keying material	160 bits	A shared secret known only to IKE peers. It was derived via key derivation function defined in SP800-135 KDF (IKEv2) and it will be used for deriving IKE session authentication key.	DRAM (plaintext)	Automatically when IPSec/IKE session is terminated
SKEYSEED	Keying material	160 bits	A shared secret known only to IKE peers. It was derived via key derivation function defined in SP800-135 KDF (IKEv2) and it will be used for deriving IKE session authentication key.	DRAM (plaintext)	Automatically when IPSec/IKE session is terminated
ISAKMP preshared	Shared Secret	Variable 8 plus characters	The secret used to derive IKE skeyid when using preshared secret authentication. This CSP is entered by the Crypto Officer.	NVRAM (plaintext)	Overwrite with new secret

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
IKE authentication private Key	RSA/ECDSA	RSA (2048 bits) or ECDSA (Curves: P-256/P-384)	RSA/ECDSA private key used in IKE authentication. This key is generated by calling SP800-90A DRBG.	NVRAM (plaintext)	Zeroized by RSA/ECDSA keypair deletion command
IKE authentication public key	RSA/ECDSA	RSA (2048 bits) or ECDSA (Curves: P-256/P-384)	RSA/ECDSA public key used in IKE authentication. The key is derived in compliance with FIPS 186-4 RSA/ECDSA key pair generation method in the module.	NVRAM (plaintext)	Zeroized by RSA/ECDSA keypair deletion command
IKE session encryption key	Triple-DES/AES	Triple-DES 192 bits or AES 128/192/256 bits	The IKE session (IKE Phase I) encrypt key. This key is derived via key derivation function defined in SP800-135 KDF (IKEv2).	DRAM (plaintext)	Automatically when IPSec/IKE session is terminated
IKE session authentication key	HMAC-SHA-1/256/384/512	160-512 bits	The IKE session (IKE Phase I) authentication key. This key is derived via key derivation function defined in SP800-135 KDF (IKEv2).	DRAM (plaintext)	Automatically when IPSec/IKE session is terminated
IPSec encryption key	Triple-DES/AES/AES-GCM	Triple-DES 192 bits or AES 128/192/256 bits	The IPSec (IKE phase II) encryption key. This key is derived via a key derivation function defined in SP800-135 KDF (IKEv2).	DRAM (plaintext)	Automatically when IPSec/IKE session is terminated
IPSec authentication key	HMAC-SHA-1/256/384/512	160-512 bits	The IPSec (IKE Phase II) authentication key. This key is derived via a key derivation function defined in SP800-135 KDF (IKEv2).	DRAM (plaintext)	Automatically when IPSec/IKE session is terminated
Operator password	Password	8 plus characters	The password of the User role. This CSP is entered by the User.	NVRAM (plaintext)	Overwrite with new password
Crypto Officer password	Password	8 plus characters	The password of the CO role. This CSP is entered by the Crypto Officer.	NVRAM (plaintext)	Overwrite with new password
RADIUS secret	Shared Secret	16 characters	The RADIUS shared secret. Used for RADIUS Client/Server authentication. This CSP is entered by the Crypto Officer.	NVRAM (plaintext)	Overwrite with new secret
TACACS+ secret	Shared Secret	16 characters	The TACACS+ shared secret. Used for TACACS+ Client/Server authentication. This CSP is entered by the Crypto Officer.	NVRAM (plaintext)	Overwrite with new secret
SSHv2 private key	RSA	2048 bits modulus	The SSHv2 private key used in SSHv2 connection. This key is generated by calling SP 800-90A DRBG.	NVRAM (plaintext)	Zeroized by RSA keypair deletion command

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
SSHv2 public key	RSA	2048 bits modulus	The SSHv2 public key used in SSHv2 connection. This key is derived in compliance with FIPS 186-4 RSA key pair generation method in the module.	NVRAM (plaintext)	Zeroized by RSA keypair deletion command
SSHv2 integrity key	HMAC-SHA-1	160 bits	Used for SSH connections integrity to assure the traffic integrity. This key is derived via key derivation function defined in SP800-135 KDF (SSH).	DRAM (plaintext)	Automatically when SSH session is terminated
SSHv2 session key	Triple-DES/AES	Triple-DES 192 bits or AES 128/192/256 bits	This is the SSHv2 session key. It is used to encrypt all SSHv2 data traffics traversing between the SSHv2 Client and SSHv2 Server. This key is derived via key derivation function defined in SP800-135 KDF (SSH).	DRAM (plaintext)	Automatically when SSH session is terminated
ECDSA private key	ECDSA	Curves: P-256, 384, 521	Signature generation used in IKE/IPSec and TLS. This key is generated by calling SP 800-90A DRBG.	NVRAM (plaintext)	Zeroized by ECDSA keypair deletion command
ECDSA public key	ECDSA	Curves: P-256, 384, 521	Signature verification used in IKE/IPSec and TLS. This key is derived in compliance with FIPS 186-4 ECDSA key pair generation method in the module.	NVRAM (plaintext)	Zeroized by ECDSA keypair deletion command
TLS RSA private key	RSA	2048 bits	Identity certificates for the security appliance itself and also used in TLS negotiations.	NVRAM (plaintext)	Zeroized by RSA keypair deletion command
TLS RSA public key	RSA	2048 bits	Identity certificates for the security appliance itself and also used in TLS negotiations. This key is derived in compliance with FIPS 186-4 RSA key pair generation method in the module.	NVRAM (plaintext)	Zeroized by RSA keypair deletion command
TLS pre-master secret	keying material	At least eight characters	Keying material created/derived using asymmetric cryptography from which new HTTPS session keys can be created. This key entered into the module in cipher text form, encrypted by RSA public key.	DRAM (plaintext)	Automatically when TLS session is terminated
TLS master secret	keying material	48 Bytes	Keying material used to derive other HTTPS/TLS keys. This key was derived from TLS pre-master secret during the TLS session establishment	DRAM (plaintext)	Automatically when TLS session is terminated

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
TLS encryption keys	Triple-DES/AES/AES-GCM	Triple-DES 192 bits or AES 128/192/256 bits	Used in HTTPS/TLS connections to protect the session traffic. This key was derived in the module.	DRAM (plaintext)	Automatically when TLS session is terminated
TLS integrity key	HMAC-SHA 256/384	256-384 bits	Used for TLS integrity to assure the traffic integrity. This key was derived in the module.	DRAM (plaintext)	Automatically when TLS session is terminated

Table 6 Cryptographic Keys and CSPs

2.13 Cryptographic Algorithms

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

Approved Cryptographic Algorithms

The module supports the following FIPS 140-2 approved algorithm implementations:

Algorithm	Cisco Security Crypto (FX-OS and ASA) in Cisco FPR1K	Cisco Security Crypto (FX-OS and ASA) in Cisco FPR2K	Cavium CN7XXX Octeon in Cisco FPR2K
AES (128/192/256 CBC, GCM)	#C784	#4905	#3301
Triple-DES (CBC, 3-key)	#C784	#2559	#1881
SHS (SHA-1/256/384/512)	#C784	#4012	#2737
HMAC (SHA-1/256/384/512)	#C784	#3272	#2095
ECDSA (KeyGen, SigGen, SigVer; P-256, P-384, P-521)	#C784	#1254	N/A
RSA (PKCS1_V1_5; KeyGen, SigGen, SigVer; 2048 bits)	#C784	#2678	N/A
DRBG (CTR_DRBG)	#C784	#1735	#819
CVL Component (IKEv2, TLSv1.2, SSHv2)	#C784	#1521	N/A
CKG (vendor affirmed)	N/A	N/A	N/A

Table 7 Approved Cryptographic Algorithms and Associated Certificate Number

Notes:

- There are some algorithm modes that were tested but not implemented by the module. Only the algorithms, modes, and key sizes that are implemented by the module are shown in this table.
- The module's AES-GCM implementation conforms to IG A.5 scenario #1 following RFC 5288 for TLS and RFC 7296 for IPSec/IKEv2. The module is compatible with TLSv1.2 and provides support for the acceptable GCM cipher suites from SP 800-52 Rev1, Section 3.3.1. The operations of one of the two parties involved in the TLS key establishment scheme were performed entirely within the cryptographic boundary of the

module being validated. The counter portion of the IV is set by the module within its cryptographic boundary. When the IV exhausts the maximum number of possible values for a given session key, the first party, client or server, to encounter this condition will trigger a handshake to establish a new encryption key. In case the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established. The module uses RFC 7296 compliant IKEv2 to establish the shared secret SKEYSEED from which the AES GCM encryption keys are derived. The operations of one of the two parties involved in the IKE key establishment scheme shall be performed entirely within the cryptographic boundary of the module being validated. When the IV exhausts the maximum number of possible values for a given session key, the first party, client or server, to encounter this condition will trigger a handshake to establish a new encryption key. In case the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established.

- No parts of the SSH, TLS and IPSec protocols, other than the KDF, have been tested by the CAVP and CMVP.
- Each of TLS, SSH and IPSec protocols governs the generation of the respective Triple-DES keys. Refer to RFC 5246 (TLS), RFC 4253 (SSH) and RFC 6071 (IPSec) for details relevant to the generation of the individual Triple-DES encryption keys. The user is responsible for ensuring the module limits the number of encryptions with the same key to 2^{20}.
- In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation as per scenario 1 of section 5 in SP800-133. The resulting generated seed used in the asymmetric key generation are the unmodified output from SP800-90A DRBG.

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 (CVL Certs. #1521 and #C784, key agreement; key establishment methodology provides between 112 and 150 bits of encryption strength)
- EC Diffie-Hellman (CVL Certs. #1521 and #C784, key agreement; key establishment methodology provides between 128 and 256 bits of encryption strength)
- RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength)
- NDRNG (non-deterministic random number generator)

Non-Approved Cryptographic Algorithms

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

- Diffie-Hellman (key agreement; key establishment methodology less than 112 bits of encryption strength; non-compliant)
- RSA (key wrapping; key establishment methodology less than 112 bits of encryption strength; non-compliant)
- DES
- HMAC MD5
- MD5
- RC4

- HMAC-SHA1 is not allowed with key size under 112-bits

2.14 Self-Tests

The modules include an array of self-tests that are run during startup and periodically during operations to prevent any secure data from being released and to ensure all components are functioning correctly.

Self-tests performed

- Cisco Security Crypto (FX-OS and ASA) POSTs
  - AES Encrypt/Decrypt KATs
  - AES-GCM KAT
  - DRBG KATs (Note: DRBG Health Tests as specified in SP800-90A Section 11.3 are performed)
  - ECDSA (Sign and Verify) Power on Self-Test
  - Firmware Integrity Test (SHA-512)
  - HMAC-SHA-1 KAT
  - HMAC-SHA-256 KAT
  - HMAC-SHA-384 KAT
  - HMAC-SHA-512 KAT
  - RSA KATs (separate KAT for signing; separate KAT for verification)
  - SHA-1 KAT
  - Triple-DES Encrypt/Decrypt KATs
- Cisco Security Crypto (FX-OS and ASA) Conditional tests
  - RSA pairwise consistency test
  - ECDSA pairwise consistency test
  - CRNGT for SP800-90A DRBG
  - CRNGT for NDRNG
- Hardware POSTs (Cavium CN7XXX Octeon in FPR2k)
  - AES Encrypt/Decrypt KATs
  - AES-GCM KAT
  - DRBG KATs (Note: DRBG Health Tests as specified in SP800-90A Section 11.3 are performed)
  - HMAC-SHA-1 KAT
  - HMAC-SHA-256 KAT
  - HMAC-SHA-384 KAT
  - HMAC-SHA-512 KAT
  - SHA-1 KAT
  - SHA-256 KAT
  - SHA–384 KAT
  - SHA-512 KAT
  - Triple-DES Encrypt/Decrypt KATs
- Hardware Conditional Tests (Cavium CN7XXX Octeon in FPR2K)
  - CRNGT for SP800-90A DRBG
  - CRNGT for NDRNG

The module performs all power-on self-tests automatically when the power is applied. All power-on self-tests must be passed before a User/Crypto Officer can perform services. The

power-on self-tests are performed after the cryptographic systems are initialized but prior to the initialization of the LAN's interfaces; this prevents the module from passing any data during a power-on self-test failure. In the unlikely event that a power-on self-test fails, an error message is displayed on the console followed by a security appliance reboot.

2.15 Physical Security

The FIPS 140-2 level 2 physical security requirements for the modules are met by the use of opacity shield covering the front panel of the module to provide the required opacity, and the Tamper Evident Labels (TELs) to provide the required tamper evidence.

Opacity Shield Security

The following table shows the tamper labels and opacity shields that shall be installed on the modules to operate in a FIPS approved mode of operation. The CO is responsible for using, securing and having control at all times of any unused tamper evident labels. Actions to be taken when any evidence of tampering should be addressed within the site security program.

Models	Number Tamper labels	Tamper Evident Labels	Number Opacity Shields	Opacity Shields
FPR1010	4	AIR-AP-FIPSKIT=	1	800-44098-01
FPR1120 and 1140	9	AIR-AP-FIPSKIT=	1	800-45098-01
FPR2110, 2120, 2130 and 2140	7	AIR-AP-FIPSKIT=	1	69-100250-01

Table 8 TEL and Opacity Shield Part Numbers

Opacity Shield installation

Inspection of the opacity shields should be incorporated into facility security procedures to include how often to inspect and any recording of the inspection. It is recommended inspection of the opacity shield occur at least every 30 days but this is the facilities Security Manager decision.

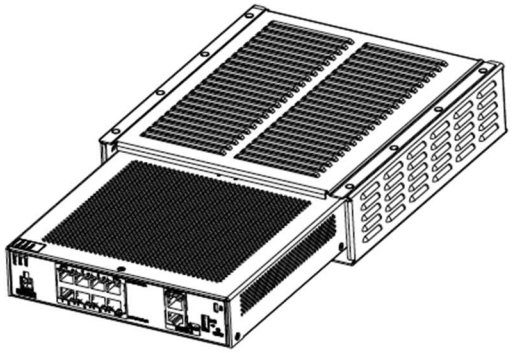
Opacity Shield installation

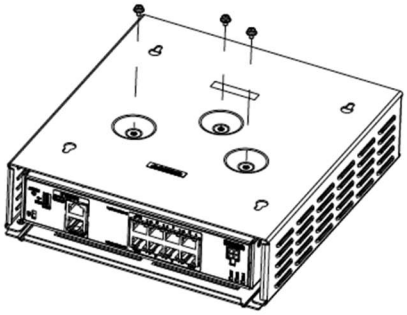
Inspection of the opacity shields should be incorporated into facility security procedures to include how often to inspect and any recording of the inspection. It is recommended inspection of the opacity shield occur at least every 30 days but this is the facilities Security Manager decision.

For Cisco FPR1010

Step 1: Slide the FPR1010 into the opacity

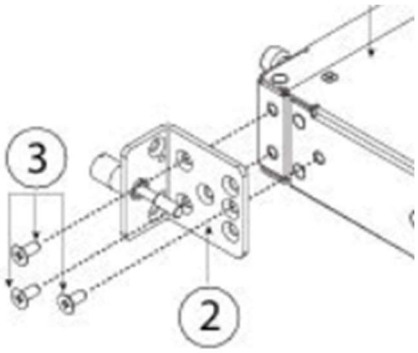
Step 2: Add three screws to bottom of opacity into the FPR1010.





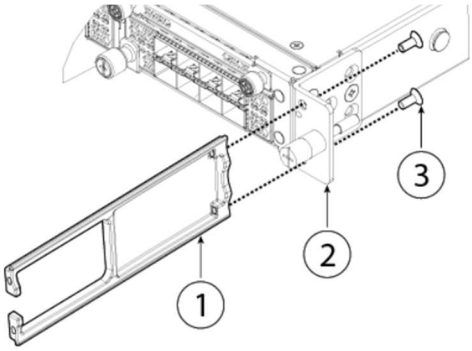
For Cisco FPR1120, FPR1140, FPR2110, FPR2120, FPR2130 and FPR2140

Step 1: Attach the Slide Rail Locking Bracket to the Side of the Chassis



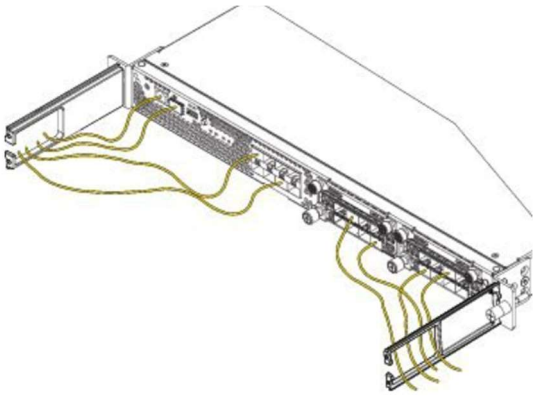
#2 Slide rail locking bracket
#3 countersink phillips screws

Step 2: Attach the Cable Management Bracket to the Slide Rail Locking Bracket

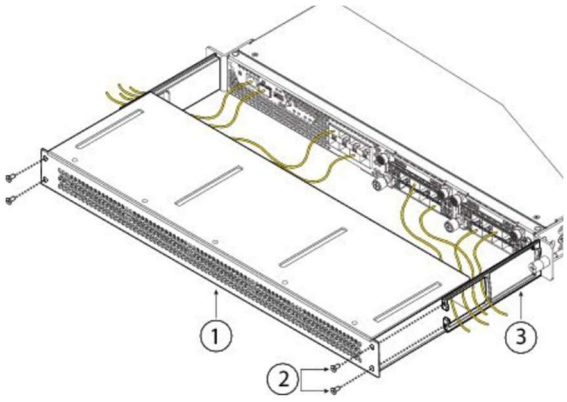


#1 Cable bracket
#2 Slide rail locking bracket
#3 countersink phillips screws

Step 3: Route the Cables through the Cable Management Brackets



Step 4: Attach the FIPS Opacity Shield to the Cable Management Brackets



#1 Opacity Shield
#2 Countersink phillips screws
#3 Cable bracket

Tamper Evidence Label (TEL) Placement

The tamper evident labels (TELs) shall be installed on the module prior to operating in FIPS mode. TELs shall be applied as depicted in the figures below. Any unused TELs must be securely stored, accounted for, and maintained by the CO in a protected location.

Should the CO have to remove, change or replace TELs 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.

Any deviation of the TELs placement by unauthorized operators such as tearing, misconfiguration, removal, change, replacement or any other change in the TELs from its original configuration as depicted below shall mean the module is no longer in FIPS mode of

operation. Returning the system back to FIPS mode of operation requires the replacement of the TELs as depicted below and any additional requirement per the site security policy which are out of scope of this Security Policy. To seal the system, apply tamper-evidence labels as depicted in the figures below.

I, Photos for the FPR1K series module with the TELs while in the FIPS mode.

Figure 1: FPR1010 front view

Figure 2: FPR1010 back view

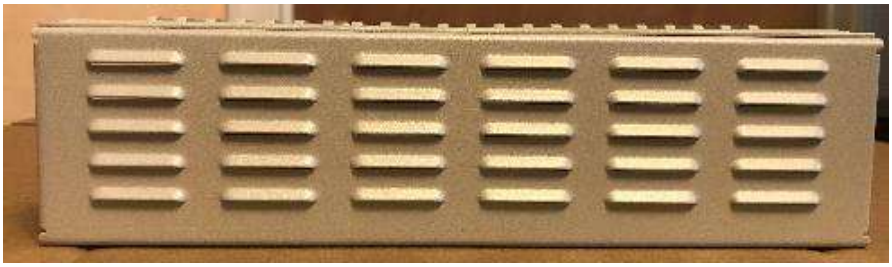


Figure 3: FPR1010 left view

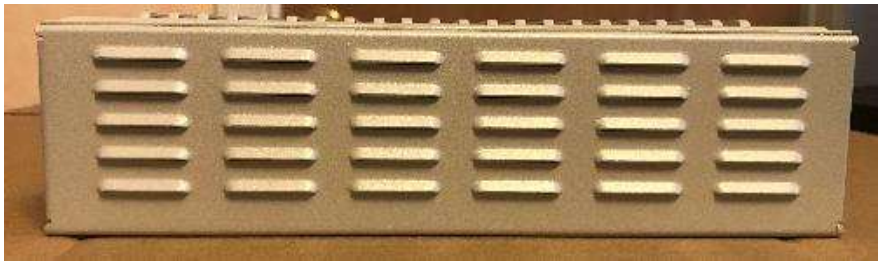


Figure 4: FPR1010 right view

Figure 5: FPR1010 top view

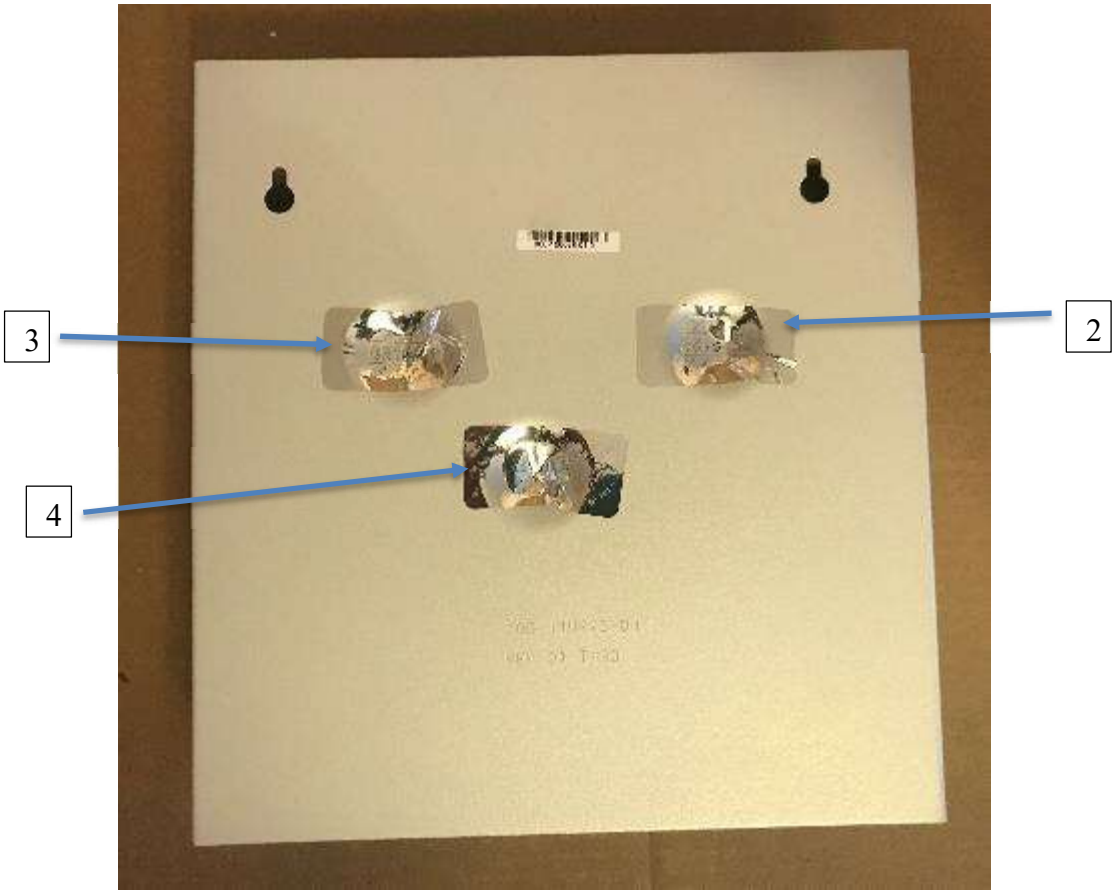


Figure 6: FPR1010 bottom view

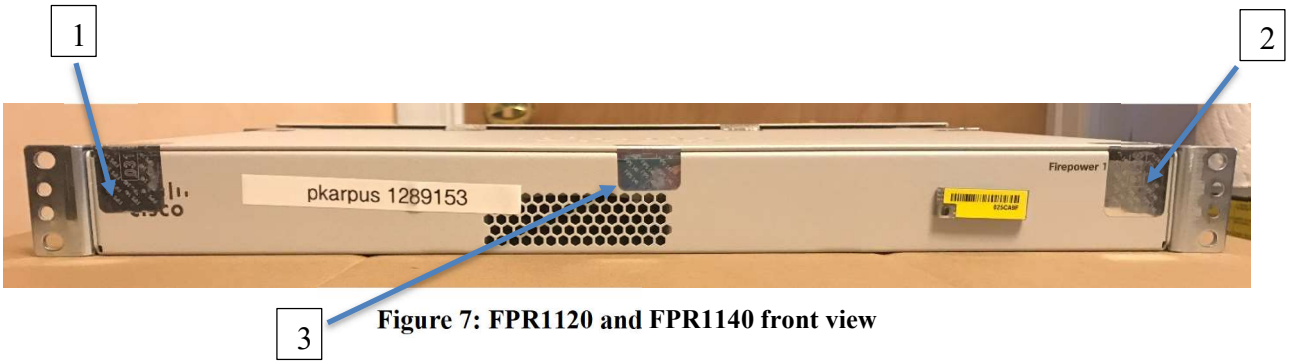


Figure 7: FPR1120 and FPR1140 front view

Figure 8: FPR1120 and FPR1140 back view

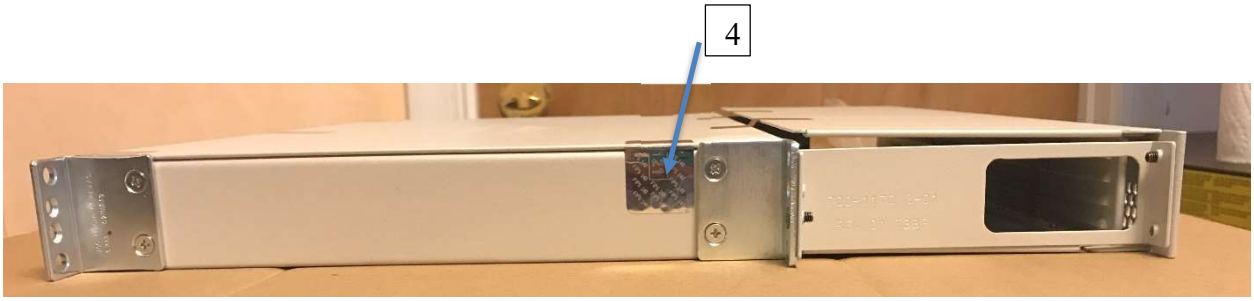


Figure 9: FPR1120 and FPR1140 left view

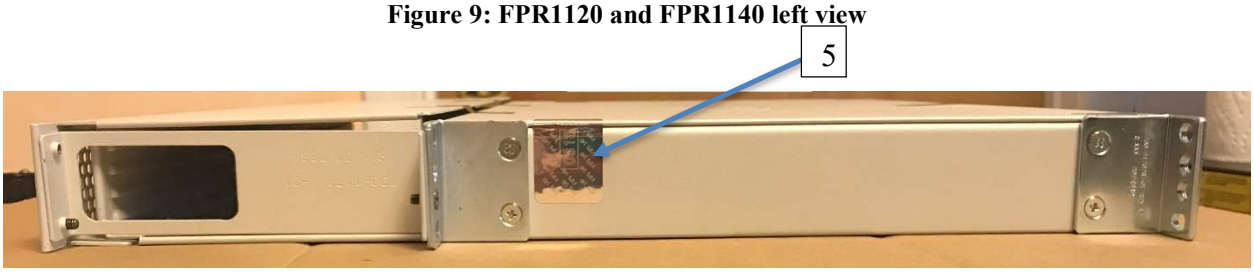


Figure 10: FPR 1120 and FPR1140 right view

Figure 11: FPR1120 and FPR1140 top view

Figure 12: FPR1120 and FPR1140 bottom view

II, Photos for the FPR2110, FPR2120, FPR2130 and FPR2140 with the TELs while in the FIPS mode.

Figure 13: FPR2110, FPR2120, FPR2130 and FPR2140 front view

Figure 14: FPR2110, FPR2120, FPR2130 and FPR2140 back view

Figure 15: FPR2110, FPR2120, FPR2130 and FPR2140 left view

Figure 16: FPR2110, FPR2120, FPR2130 and FPR2140 right view

Figure 17: FPR2110, FPR2120, FPR2130 and FPR2140 bottom view

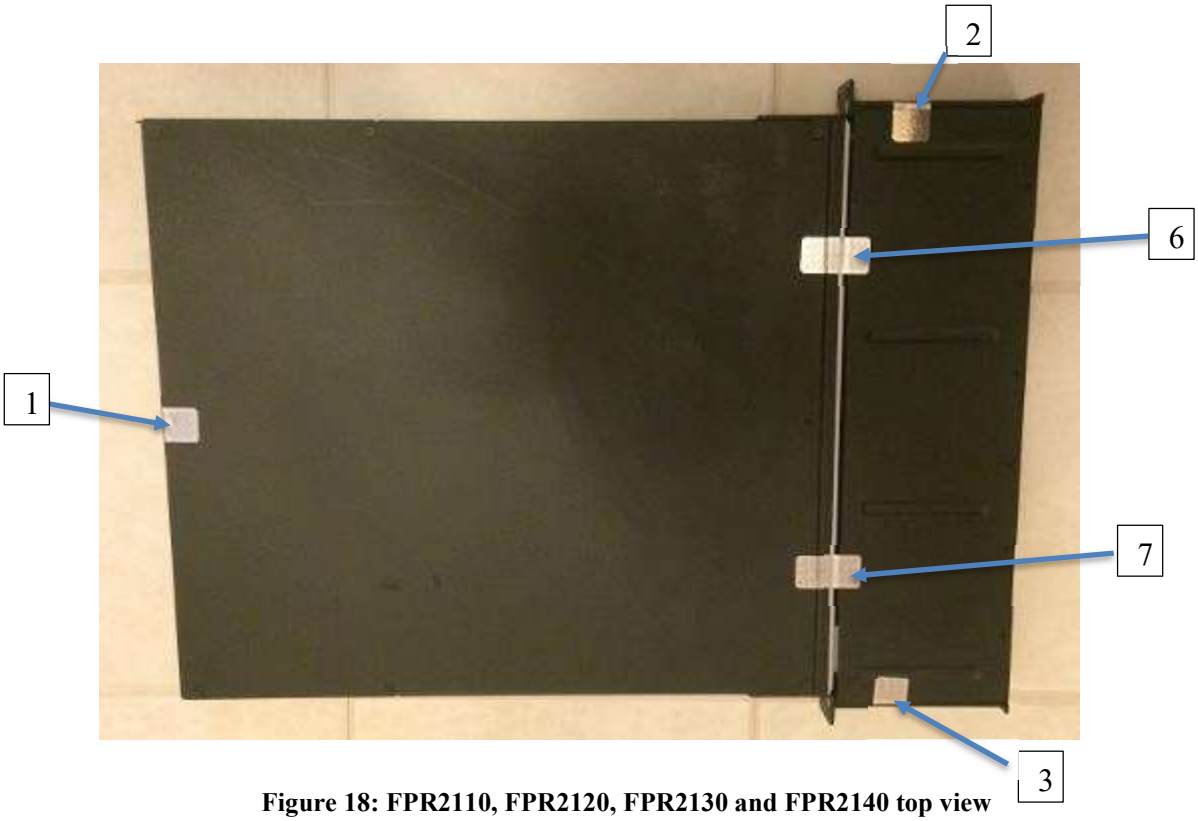


Figure 18: FPR2110, FPR2120, FPR2130 and FPR2140 top view

Appling Tamper Evidence Labels

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

Step 2: Clean the chassis of any grease, dirt, or oil before applying the tamper evident labels. Alcohol-based cleaning pads are recommended for this purpose.

Step 3: Apply a label to cover the module as shown in the figures above.

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

Inspection of the tamper seals should be incorporated into facility security to include how often to inspect and any recording of the inspection. It is recommended inspection of TELs occur at least every 30 days but this is the facilities Security Manager decision.

3 Secure Operations

The module meets all the Level 2 requirements for FIPS 140-2. The module is shipped only to authorized operators by the vendor, and the modules are shipped in Cisco boxes with Cisco adhesive, so if tampered with the recipient will notice. Follow the setting instructions provided below to place the module in FIPS-approved mode. Operating this module without maintaining the following settings will remove the module from the FIPS approved mode of operation.

3.1 Crypto Officer Guidance - System Initialization

The module was validated with firmware version 6.4. This is the only allowable image for FIPS-approved mode of operation.

The Crypto Officer must configure and enforce the following initialization steps:

Step 1: The Crypto Officer must install opacity shield as described in Section 2.15 of this document.

Step 2: The Crypto Officer must apply tamper evidence labels as described in Section 2.15 of this document.

Step 3: Install Smart Licensing for Triple-DES/AES licenses to require the module to use Triple-DES and AES.

Step 4: Enable “FIPS Mode” to allow the module to internally enforce FIPS-compliant behavior. This is done from an FMC unit (selecting CC mode set FIPS mode).

Step 5: After step 4, please issue the following command to verify the FIPS mode:

> show running-config fips

fips enable

Note: the output from ‘show fips-mode’ should be “FIPS Mode Admin State: Enabled”

Step 6: Configure the module to use SSHv2. Note that all operators must still authenticate after remote access is granted. The CO shall only use FIPS approved/Allowed cryptographic algorithms listed above for SSHv2 configuration.

Step 7: If using a RADIUS/TACACS+ server for authentication, please configure an IPSec/TLS tunnel to secure traffic between the module and the RADIUS/TACACS+ server. The RADIUS/TACACS+ shared secret must be at least 8 characters long.

Step 8: Configure the module such that any remote connections via Telnet are secured through IPSec.

Step 9: Configure the module such that only FIPS-approved algorithms are used for IPSec tunnels.

Step 10: Configure the module such that error messages can only be viewed by Crypto Officer.

Step 11: Disable the TFTP server.

Step 12: Disable HTTP for performing system management in FIPS mode of operation. HTTPS with TLS should always be used for Web-based management. The CO shall only use FIPS approved/Allowed cryptographic algorithms listed above for TLS configuration.

Step 13: Ensure that installed digital certificates are signed using FIPS approved algorithms.

Step 14: Reboot the module.