



Cisco Firepower 4100 and Cisco Firepower 9300 Series

**FIPS 140-2 Non Proprietary Security Policy
Level 2 Validation**

Documentation Version 0.9

January 7, 2021

Table of Contents

1	INTRODUCTION.....	3
1.1	PURPOSE.....	3
1.2	MODULE VALIDATION LEVEL	3
1.3	REFERENCES.....	3
1.4	TERMINOLOGY	4
1.5	DOCUMENT ORGANIZATION	4
2	CISCO FIREPOWER 4100 AND 9300 SERIES OVERVIEW.....	5
2.1	CISCO FX-OS CRYPTOGRAPHIC MODULE	6
2.2	CRYPTOGRAPHIC MODULE CHARACTERISTICS	6
2.3	CRYPTOGRAPHIC BOUNDARY	6
2.4	MODULE INTERFACES.....	7
	4100 Series Front.....	8
	4100 Series Rear.....	9
	9300 Series Front.....	9
	9300 Series Rear.....	10
2.5	ROLES AND SERVICES.....	10
2.6	USER SERVICES	11
2.7	CRYPTO OFFICER SERVICES.....	12
2.8	NON-FIPS MODE SERVICES	13
2.9	UNAUTHENTICATED SERVICES	14
2.10	OPERATIONAL ENVIRONMENT	14
2.11	CRYPTOGRAPHIC KEY/CSP MANAGEMENT.....	14
2.12	CRYPTOGRAPHIC ALGORITHMS	19
	Approved Cryptographic Algorithms	19
	Non-FIPS Approved Algorithms Allowed in FIPS Mode	20
	Non-Approved Cryptographic Algorithms	21
	Approved Cryptographic Algorithms from Embedded Module	21
	Non-FIPS Approved Algorithms Allowed in FIPS Mode from Embedded Module.....	22
	Non-Approved Cryptographic Algorithms from Embedded Module	22
2.13	SELF-TESTS	23
2.14	PHYSICAL SECURITY.....	24
	Opacity Shield installation.....	24
	Tamper Evidence Label (TEL) Placement.....	26
	Applying Tamper Evidence Labels	33
3	SECURE OPERATION	33
3.1	CRYPTO OFFICER GUIDANCE - SYSTEM INITIALIZATION	33

1 Introduction

1.1 Purpose

This is the non-proprietary Security Policy for Cisco Firepower 4100 and Cisco Firepower 9300 Series running firmware version 2.6. 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 <https://csrc.nist.gov/Projects/cryptographic-module-validation-program>.

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 4100 and Cisco Firepower 9300 Series 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 (<https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules>) contains contact information for answers to technical or sales-related questions for the module.

1.4 Terminology

In this document, the Cisco Firepower 4100 and Cisco Firepower 9300 Series identified are referred to as Cisco FX-OS Cryptographic Module, FX-OS, 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 FX-OS Cryptographic Module identified above and explains the secure layout, configuration and operation. This introduction section is followed by Section 2, which details the general features and functionality of the appliances. 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 4100 and 9300 Series Overview

The Cisco Firepower 4100 security appliance is a standalone modular security services platform with a one RU form factor. It is capable of running multiple security services simultaneously and so is targeted at the data center as a multi-service platform. It comprises a front-end “Management IO” (MIO) function and one Security Service card with x86 CPU complex. The MIO cards are the central place for all customer and management traffic as well as inter-card communications.



Image 1 Firepower 4110, 4115, 4120, 4125, 4140, 4145 and 4150

The 4100 Series has dual multi-core processors, dual AC power supply modules, one 200 to 400-GB SSD, and 64 to 256-GB of DDR4 RAM depending on the model.

Cisco Firepower 4100 Security Appliance includes:

- FPR4110-NGFW-K9
- FPR4115-NGFW-K9
- FPR4120-NGFW-K9
- FPR4125-NGFW-K9
- FPR4140-NGFW-K9
- FPR4145-NGFW-K9
- FPR4150-NGFW-K9

The Cisco Firepower 9300 security appliance is a next generation network and content security platform. Its modular standalone chassis offers high-performance and flexible I/O options that enables it to run multiple security services simultaneously. The Firepower 9300 security appliance contains a supervisor management I/O card called the Firepower 9300 Supervisor. The Supervisor provides chassis management.



Image 2 Firepower 9300

Cisco Firepower 9300 Security Appliance with High Performance Security Module (SM)

- FPR9K-Sup (SM-24)
- FPR9K-Sup (SM-36)
- FPR9K-Sup (SM-40)
- FPR9K-Sup (SM-44)
- FPR9K-Sup (SM-48)
- FPR9K-Sup (SM-56)

The Cisco Firepower 4100 and Cisco Firepower 9300 Series, when deployed as next-generation firewall (NGFW) appliances, use FX-OS Cryptographic Module and the embedded Cisco® Adaptive Security Appliance Cryptographic Module (ASA-CM). The ASA-CM has been certified with FIPS 140-2 Cert. #3789. Thus, the sections throughout this SP detail the FIPS compliance of FX-OS.

2.1 Cisco FX-OS Cryptographic Module

The Firepower eXtensible Operating System (FX-OS) provides a web interface that makes it easy to configure platform settings and interfaces, provision devices, and monitor system status.

The management I/O card found in both the 4100 and 9300 units runs the Cisco Firepower eXtensible Operating System (FX-OS) version 2.6, a next-generation network and content security solutions. 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.
- FX-OS REST API—allows users to programmatically configure and manage their chassis.

2.2 Cryptographic Module Characteristics

The Cisco FX-OS Cryptographic Module is contained on the Management I/O (MIO) card in the 4100 and 9300 Series appliances. This Cryptographic Module contains the crypto services for SSHv2, SNMPv3, HTTPS/TLSv1.2 and StrongSwan (IPSec/IKEv2).

2.3 Cryptographic Boundary

The module is a hardware, multi-chip standalone crypto module. The cryptographic boundary is defined as the 4100/9300 series chassis unit encompassing the "top," "front," "left," "right,"

“rear” and "bottom" surfaces of the case (the red dashed area surround the black box representing the module’s physical perimeter). In the diagram 1, the Management I/O card (inside the blue rectangle) is the hardware platform executing FX-OS cryptographic module, and the FIPS 140-2 validated, embedded ASA blade (the red rectangle) executes the ASA-CM’s firmware.

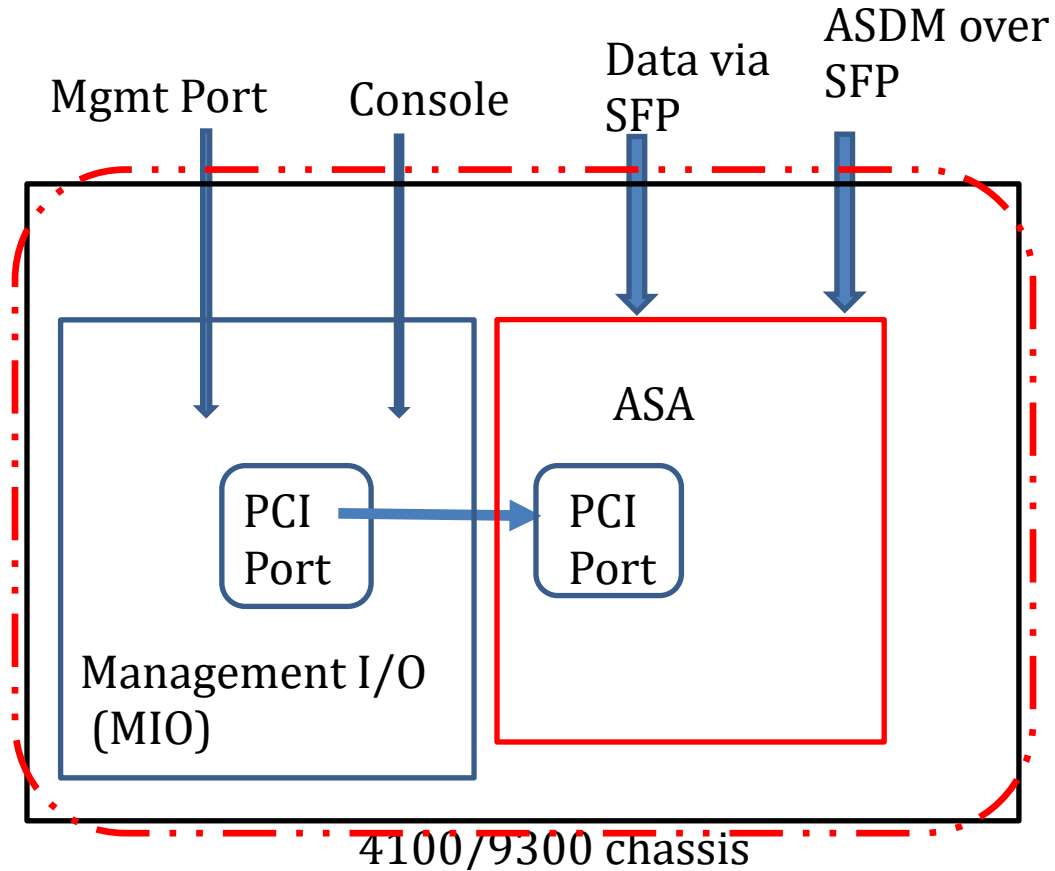


Diagram 1 Block Diagram

2.4 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 provided 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:

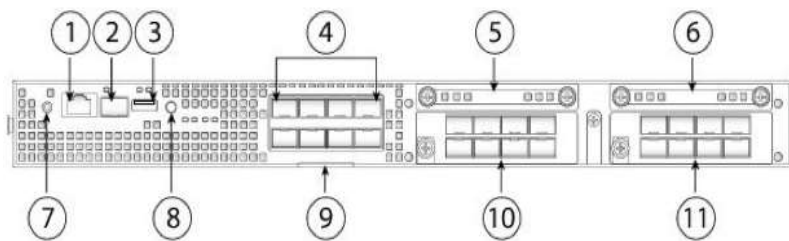
FIPS 140-2 Logical Interface	4100 and 9300 Physical Interfaces
Data Input	MGMT Port Console port SFP/SFP+ Ethernet and/or RJ-45 GigE Ports
Data Output	MGMT Port Console port SFP/SFP+ Ethernet and/or RJ-45 GigE Ports
Control Input	MGMT Port

	Console port SFP/SFP+ Ethernet and/or RJ-45 GigE Ports
Status Output	MGMT Port Console port SFP/SFP+ Ethernet and/or RJ-45 GigE Ports LEDs

Table 2 Hardware/Physical Boundary Interfaces

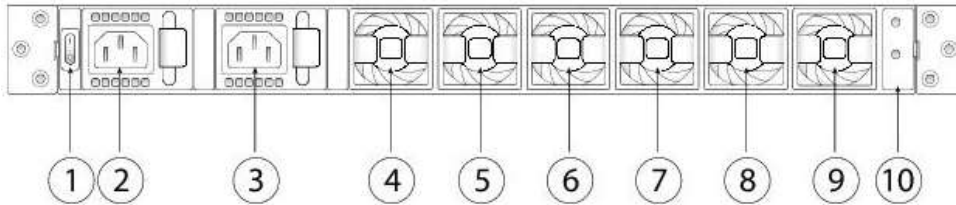
Note: Each module has a USB port, but it is considered to be disabled once the Crypto-Officer has applied the TEL label.

4100 Series Front



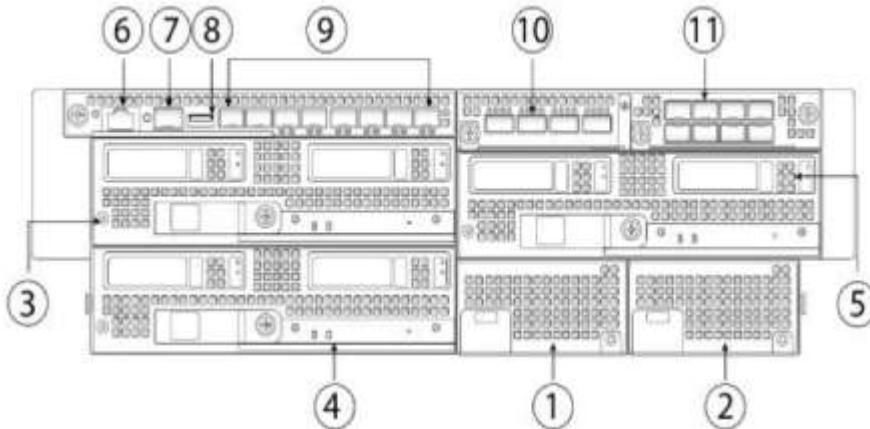
1	RJ-45 console port	2	1 Gigabit Ethernet management port
3	Type A USB port	4	Eight fixed SFP+ (1G/10G) ports are provided (network module slot 1) Gigabit Ethernet 1/1 through 1/8 labeled left to right, top to bottom
5	SSD 1	6	SSD 2
7	Power LED	8	Locator LED
9	Pull out label card	10	Network Module (network module slot 2) Note The 10G network module is shown.
11	Network Module (network module slot 3) Note The 10G network module is shown.		

4100 Series Rear



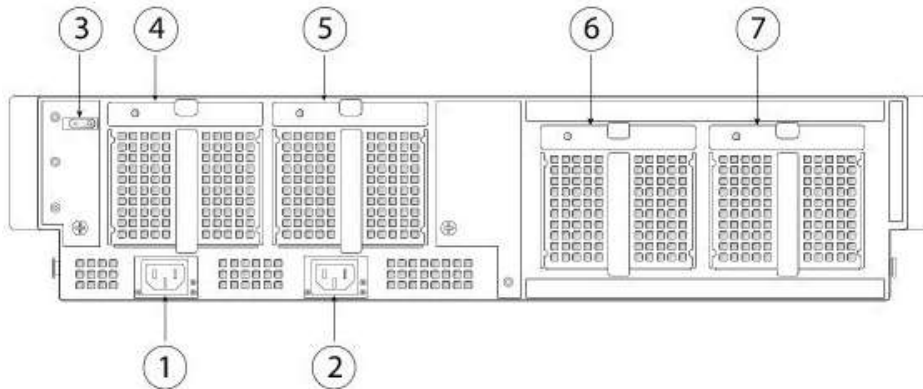
1	Power on/off switch	2	Power supply module 1
3	Power supply module 2	4	Fan module 1
5	Fan module 2	6	Fan module 3
7	Fan module 4	8	Fan module 5
9	Fan module 6	10	Location for the two-post grounding lug Note The two-post grounding lug is included in the accessory kit.

9300 Series Front



1	Power supply module PSU-1	2	Power supply module PSU-2
3	Security Module 1	4	Security Module 3
5	Security Module 2	6	RJ-45 console port
7	1 Gigabit Ethernet management port	8	USB port
9	Eight 10 Gigabit Ethernet data ports (Gigabit Ethernet 1/1 through 1/8)	10	Network Module (network module slot 2)
11	Network Module (network module slot 3)		

9300 Series Rear



1	Power feed for PSU-2	2	Power feed for PSU-1
3	On/Off switch	4	Fan module FAN-1
5	Fan module FAN-2	6	Fan module FAN-3
7	Fan module FAN-4		

In addition, for details of the Cryptographic Boundary and the associated physical/logical interfaces of the embedded Cisco ASA Cryptographic Module (ASA-CM), please refer to the corresponding Security Policy for more information. The ASA-CM module has been certified with FIPS 140-2 Cert. #3789.

2.5 Roles and Services

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

- SSHv2
- HTTPS/TLSv1.2
- IPSec/IKEv2
- SNMPv3

Authentication is identity-based. As required by FIPS 140-2, there are two roles that operators may assume: a 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 $52 \times 52 \times 52 \times 52 \times 52 \times 52 \times 32 \times 10 = 6,326,595,092,480$. 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 2^{112} 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 8.65×10^{31} ($2^{112} / 60 = 8.65 \times 10^{31}$) attempts per second, which far exceeds the operational capabilities of the module to support.

2.6 User Services

A User enters the system by either SSHv2 or HTTPS/TLSv1.2. The User role can be authenticated via either Username/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/IKEv2 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.	N/A
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
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, 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, keyid, skeyid_d, SKEYSEED, IKE session encrypt key, IKE session authentication key, ISAKMP preshared, IKE authentication private Key, IKE authentication 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, Diffie-Hellman private key, Diffie-Hellman public key, Diffie-Hellman Shared Secret, EC Diffie-Hellman private key, EC Diffie-Hellman public

Services	Description	Keys and CSPs Access
		key, EC Diffie-Hellman Shared Secret, SSH Traffic Keys, 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, TLS RSA private key, TLS RSA public key, TLS pre-master secret and TLS encryption keys and TLS Integrity Key (r, w, d)

Table 3 User Services

2.7 Crypto Officer Services

A Crypto Officer (CO) enters the system by accessing SSH v2 or HTTPS/TLSv1.2. The CO role can be authenticated via either Username/Password or RSA based authentication method. The other means of accessing the console is via an IPSec/IKEv2 session. This session is authenticated either using a shared secret or RSA digital signature authentication mechanism. A Crypto Officer may assign permission to access the Crypto Officer role to additional accounts, thereby creating additional Crypto Officers.

The Crypto Officer role is responsible for the configuration of the module. 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.	ISAKMP preshared, 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, Operator password, Enable password, IKE session encrypt key, IKE session authentication key, IKE authentication private Key, IKE authentication public key, IPSec encryption key, IPSec authentication key (r, w, d)
Firmware integrity	Execute firmware integrity verification	Integrity test key (r, w, d)
RADIUS / TACACS+ functions	Provide entry of shared secret CSP	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, Enable 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.	N/A
HTTPS/TLS (TLSv1.2)	Configure HTTPS/TLS parameters, provide entry and output of CSPs.	DRBG entropy input, DRBG Seed, DRBG V, DRBG 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 Functions	Configure IPSec VPN parameters, provide entry and output of CSPs.	ISAKMP preshared, 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, skeyid, skeyid_d, SKEYSEED, IKE session encrypt key, IKE session authentication key, IKE authentication private Key, IKE authentication public key, DRBG entropy input, DRBG Seed, DRBG V, DRBG Key, IPSec encryption key, IPSec authentication key (r, w, d)

SSHv2 Functions	Configure SSHv2 parameter, provide entry and output of CSPs.	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, SSHv2 session key, DRBG entropy input, DRBG Seed, DRBG V and DRBG 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)
SNMPv3 Functions	Configure SNMPv3 MIB and monitor status.	SNMPv3 Password, SNMPv3 engineID, SNMP session key (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

2.8 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 in Section 2.8, the Crypto Officer must zeroize all CSPs which places the module into the non-FIPS mode of operation.

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: MD5 Symmetric: DES, RC4 Asymmetric: RSA (key transport), 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.

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.

To put the module back into the FIPS mode from the non-FIPS mode, the CO must zeroize all Keys/CSPs used in non-FIPS mode, and then strictly follow up the steps in section 3 of this document to put the module into the FIPS mode.

All services available can be found at Cisco Firepower 4100/9300 FXOS CLI Configuration Guide, 2.6(1). Updated: July 2, 2020

https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/fxos261/cli-guide/b_CLI_ConfigGuide_FXOS_261.html. This site lists the configuration guidance.

2.9 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.

In addition, for details regarding the Roles, Services and Authentication provided by the embedded ASA-CM cryptographic module, please refer to the Security Policy for more information. The ASA-CM module has been certified with FIPS 140-2 Cert. #3789.

2.10 Operational Environment

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

2.11 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. 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 entropy source falls into IG 7.14, Scenario #1a: A hardware module with an entropy-generating NDRNG inside the module's cryptographic boundary. The entropy source provides at least 256 bits of entropy to seed SP800-90a DRBG for the use of 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.	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
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

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
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
sketid	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)	Power cycle the device
sketid_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)	Power cycle the device
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)	Power cycle the device
IKE session encrypt key	Triple-DES/AES	192 bits Triple-DES or 128/192/256 bits AES	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 session is terminated
IKE session authentication key	HMAC-SHA-1	160 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 session is terminated

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
ISAKMP preshared	Pre-shared secret	Variable 8 plus characters	The secret used to derive IKE keyid when using preshared secret authentication. This CSP is entered by the Crypto Officer.	NVRAM (plaintext)	Erase the secret
IKE authentication private Key	RSA	RSA (2048 bits)	RSA private key used in IKE authentication. This key is generated by calling SP800-90A DRBG.	DRAM (plaintext)	Zeroized by RSA keypair deletion command
IKE authentication public key	RSA	RSA (2048 bits)	RSA public key used in IKE authentication. This key is derived in compliance with FIPS 186-4 RSA key pair generation method in the module.	DRAM (plaintext)	Zeroized by RSA keypair deletion command
IPsec encryption key	Triple-DES, AES and AES-GCM	192 bits Triple-DES or 128/192/256 bits AES	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 session is terminated
IPsec authentication key	HMAC-SHA-1	160 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 session is terminated
Operator password	Password	8 plus characters	The password of the User role. This CSP was entered by the User.	NVRAM (plaintext)	Erase the password
Enable password	Password	8 plus characters	The password of the CO role. This CSP was entered by the Crypto Officer.	NVRAM (plaintext)	Erase the 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)	Erase the 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)	Erase the 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 session key	Triple-DES/AES	192 bits Triple-DES or 128/192/256 bits AES	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
SSHv2 integrity key	HMAC-SHA-1	160 bits	Used for SSHv2 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
TLS RSA private key	RSA	2048 bits	Identity certificates for the security appliance itself and also used in TLS session 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 RSA public key	RSA	2048 bits	Identity certificates for the security appliance itself and also used in TLS session 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	Shared Secret	At least eight characters	Shared secret created/derived using asymmetric cryptography from which new HTTPS/TLS 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 128/192/256;	192 bits Triple-DES or 128/192/256 bits AES	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-SHA1/256/384/512	160-512 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
SNMPv3 password	Password	256 bits	The password use to setup SNMPv3 connection. This key is entered by Crypto Officer.	NVRAM (plaintext)	Erase the password
SNMPv3 authentication key	HMAC-SHA-1	160 bits	Authentication key used to protect SNMP traffic integrity. This key is derived via key derivation function defined in SP800-135 KDF (SNMPv3).	DRAM (plaintext)	Automatically when SNMP session is terminated
SNMPv3 session key	AES	128 bits	Encryption key used to protect SNMP traffic. This key is derived via key derivation function defined in SP800-135 KDF (SNMPv3).	DRAM (plaintext)	Automatically when SNMP session is terminated
Integrity test key	RSA-2048 Public key	2048 bits	A hard coded key used for firmware power-up/load integrity verification.	Hard coded for firmware integrity testing	Zeroized by erasing the firmware image

Table 6 Cryptographic Keys and CSPs

In addition, for details of the Cryptographic Keys and CSPs provided by the embedded Cisco ASA Cryptographic Module (ASA-CM), please refer to the corresponding Security Policy for more information. The ASA-CM module has been certified with FIPS 140-2 Cert. #3789.

2.12 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 (Firmware)
AES (128/192/256 bits CBC, GCM)	C784
Triple-DES (CBC, 3-key)	C784
SHS (SHA-1/256/384/512)	C784

HMAC (SHA-1/256/384/512)	C784
RSA (PKCS1_V1_5; KeyGen, SigGen, SigVer; 2048 bits)	C784
DRBG (CTR_DRBG)	C784
CVL Component (IKEv2, TLSv1.2, SSHv2, SNMPv3)	C784
CKG (vendor affirmed)	

Table 7 Approved Cryptographic Algorithms and Associated Certificate Number

Note:

- There are some algorithm modes that were tested but not used 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, SNMP and IPSec protocols, other than the KDF's, 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 depicted in section 6 of SP800-133. The resulting generated symmetric key and the 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 Cert. #C784, key agreement; key establishment methodology provides between 112 and 150 bits of encryption strength)

- EC Diffie-Hellman (CVL Cert. #C784, key agreement; key establishment methodology provides between 128 and 256 bits of encryption strength)
- NDRNG (entropy source)
- RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength)

Non-Approved Cryptographic Algorithms

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

- DES
- Diffie-Hellman (key agreement; key establishment methodology less than 112 bits of encryption strength; non-compliant)
- HMAC-MD5
- HMAC-SHA-1 is not allowed with key size under 112-bits
- MD5
- RC4
- RSA (key wrapping; key establishment methodology less than 112 bits of encryption strength; non-compliant)

In addition, the embedded ASA-CM cryptographic module (FIPS Cert. #3789) also provides the following FIPS approved algorithm certificates and non-approved algorithms.

Approved Cryptographic Algorithms from Embedded Module

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

	Cisco Security Crypto (Firmware)	On-board Chip (Cavium Nitrox III)	On-board Chip (Cavium Nitrox V)
AES (128/192/256 CBC, GCM)	4905/C784	2034/2035	C1026
Triple-DES (CBC, 3-key)	2559/C784	1311	C1026
SHS (SHA-1/256/384/512)	4012/C784	1780	C1026
HMAC (SHA-1/256/384/512)	3272/C784	1233	C1026
RSA (KeyGen, SigGen and SigVer; PKCS1_V1_5; 2048bits)	2678/C784		
ECDSA (PKG, SigGen and SigVer; P-256, P-384, P-521)	1254/C784		
CTR_DRBG (AES-256)	1735/C784		
HASH_DRBG (SHA-512)		197	C1026
CVL Component (IKEv2, TLSv1.2, SSHv2)	1521/C784		
CKG (vendor affirmed)			

Table 7 Approved Cryptographic Algorithms and Associated Certificate Numbers

Note:

- 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 KDFs, 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 depicted in section 6 of 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 from Embedded Module

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)
- RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength)
- NDRNG (entropy source)

Non-Approved Cryptographic Algorithms from Embedded Module

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

In addition, the embedded cryptographic module with FIPS 140-2 Cert. #3789 also provides the following FIPS approved algorithm certificates and non-approved algorithms.

2.13 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

- POSTs
 - AES-CBC Encrypt/Decrypt KATs
 - DRBG KAT (Note: DRBG Health Tests as specified in SP800-90A Section 11.3 are performed)
 - Firmware Integrity Test (using RSA 2048 with SHA-512)
 - HMAC (SHA-1/256/384/512) KATs
 - RSA KATs (separate KAT for signing; separate KAT for verification)
 - SHA-1 KAT
 - Triple-DES-CBC Encrypt/Decrypt KATs
- Conditional tests
 - RSA pairwise consistency test
 - CRNGT to SP800-90A DRBG
 - CRNGT to NDRNG (entropy source)

The security appliances perform 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 security appliances 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.

In addition, for details of the Self-Tests conducted by the embedded ASA-CM cryptographic module, please refer to the Security Policy for more information. The ASA-CM module has been certified with FIPS 140-2 Cert. #3789.

2.14 Physical Security

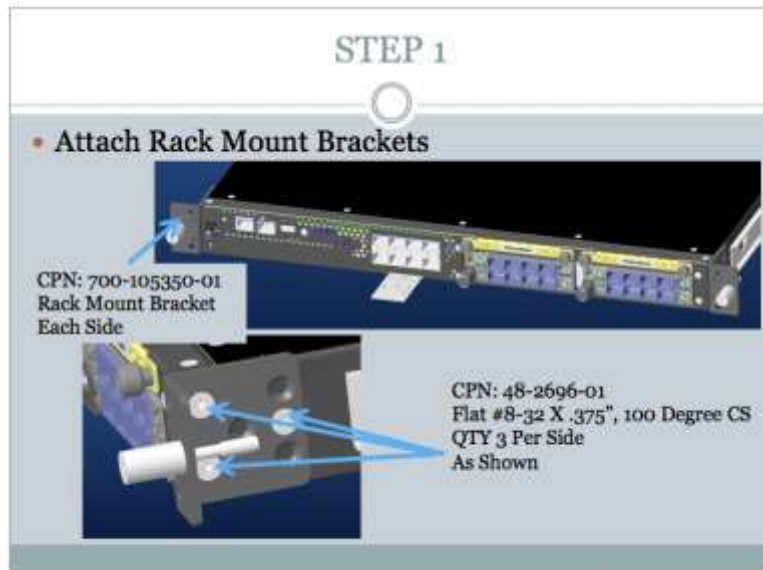
The FIPS 140-2 level 2 physical security requirements for the modules are met by the use of opacity shields covering the front panels of modules to provide the required opacity and tamper evident seals to provide the required tamper evidence.

The following 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 site security program.

Models	Number Tamper labels	Tamper Evident Labels	Number Opacity Shields	Opacity Shields
FPR4110, 4115, 4120, 4125, 4140, 4145 and 4150	15	Cisco_TEL.FIPS_Kit	1	69-100250-01
FPR9300 (SM24, SM-36, SM-40, SM-44, SM-48 and SM-56)	12	Cisco_TEL.FIPS_Kit	1	800-102843-01

Opacity Shield installation

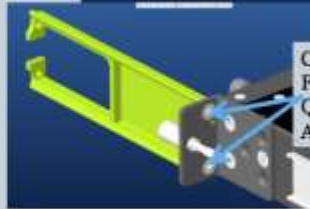
4100 Series



STEP 2

• Attach Cable Brackets

CPN: 700-106377-01
Cable Bracket
Each Side

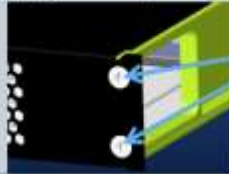
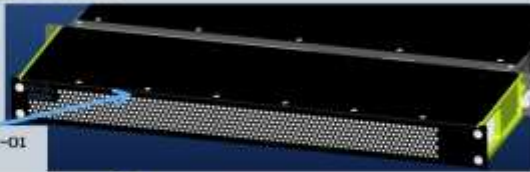


CPN: 48-2696-01
Flat #8-32 X .375", 100 Degree CS
QTY 2 Per Side
As Shown

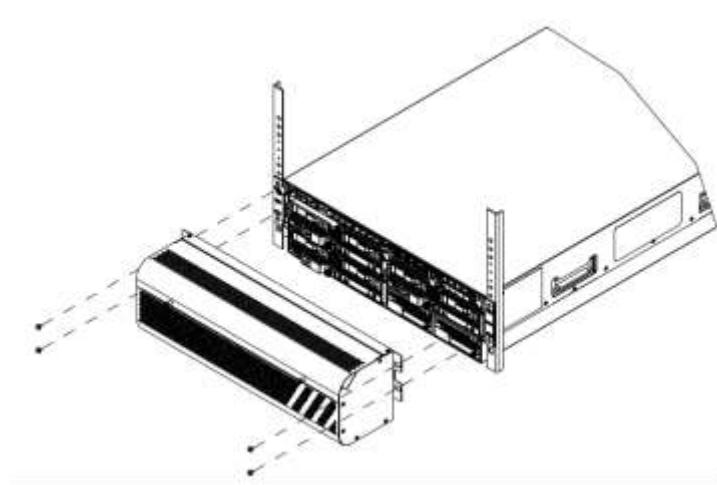
STEP 3

• Attach FIPS Bracket

CPN: 800-102699-01
FIPS Bracket



CPN: 48-2696-01
Flat #8-32 X .375", 100 Degree CS
QTY 2 Per Side
As Shown



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

Tamper Evidence Label (TEL) Placement

The tamper evident seals (hereinafter referred to as tamper evident labels (TEL)) shall be installed on the security devices containing 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 (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.

Any deviation of the TELs placement such as tearing, misconfiguration, removal, change, replacement or any other change in the TELs from its original configuration as depicted below by unauthorized operators 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 TEL 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.



Figure 1: FPR4100 Series Front view (no TEL present on front)



Figure 2: FPR4100 Series Right Side
(Right side has TEL #1 overlapping top and side)



Figure 3: FPR4100 Series Left Side
(Left side has TEL #2 overlapping top and side)

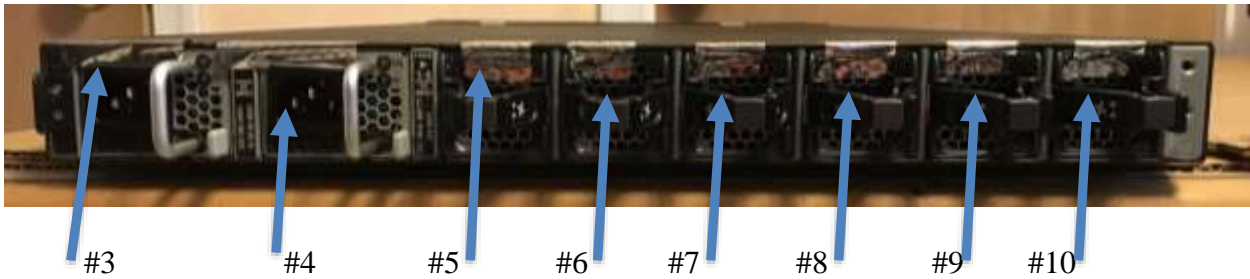


Figure 4: FPR4100 Series Rear view
(Rear has TEL #3, #4, #5, #6, #7, #8, #9 and #10 overlapping top and plug-in)

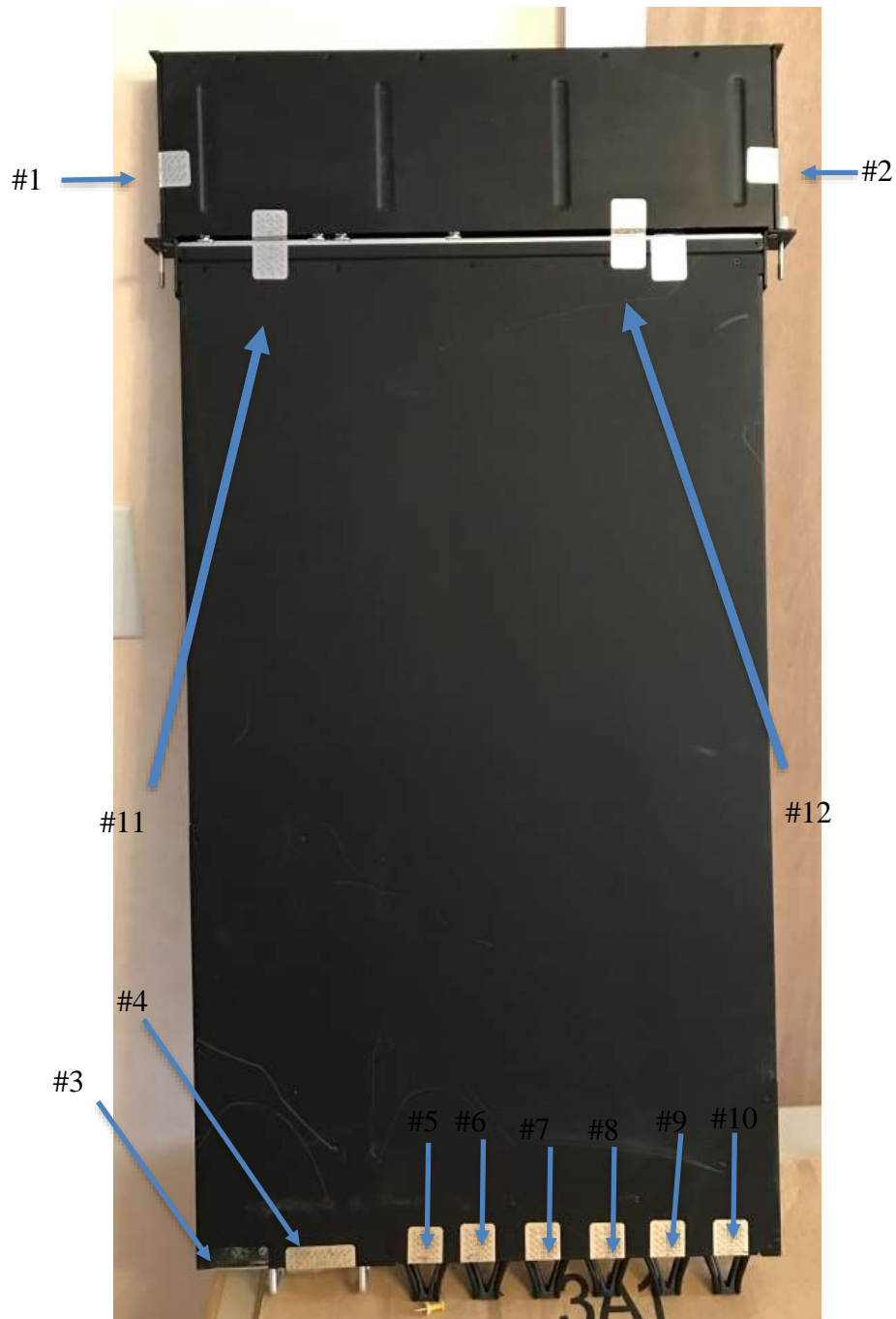


Figure 5: FPR4100 Series Top view
(Top shows TEL #11 and #12 overlapping opacity shield and 4000 chassis, also present is TEL #1,2,3,4,5,6,7,8,9,10)



Figure 6: FPR4100 Series Bottom view
(Bottom shows TEL #13 and #14 overlapping opacity shield and 4000 chassis)



Figure 7: FPR9300 Series Front view
(Front opacity shield has TEL #1 and #2)



Figure 8: FPR9300 Series Right view (Right side has no TELs)



Figure 9: FPR9300 Series Left view (Left side has no TELs)



Figure 10: FPR9300 Series Rear view
(Rear has TEL #3, #4, #5, #6, each overlapping chassis and plug-in and #7 on bottom)



Figure 11: FPR9300 Series Top view
(Top has TEL #8 and #9 overlapping opacity shield and top of chassis, also present is TEL #3, #4, #5 and #6 listed on Back view. TEL #12 partially obscured inside the opacity shield, overlapping front of chassis and top of chassis covering the USB)



Figure 12: FPR9300 Series Bottom view

(Bottom has TEL #10 and #11 overlapping opacity shield and bottom of chassis, also present is TEL #7 overlapping bottom and back of plug-in)

Please note that the 4100 and 9300 series modules provide the described level 2 physical security protections. These protections also secure the embedded cryptographic module (which was validated for level 1 physical security).

Applying Tamper Evidence Labels

Step 1: Turn off and unplug the system 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 security appliance as shown in figures above and allow the label to cure for a minimum of 12 hours.

The tamper evident seals are produced from a special thin gauge vinyl with self-adhesive backing. Any attempt to open the device will damage the tamper evident seals or the material of the security appliance cover. Because the tamper evident seals 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 seals can also be inspected for signs of tampering, which include the following: curled corners, rips, and slices. The word “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 30 days but this is the facilities Security Manager decision.

3 Secure Operation

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 Cisco FX-OS Cryptographic Module was validated with FX-OS version 2.6, which is the only allowable firmware for the current FIPS-approved mode of operation. The Crypto Officer must configure and enforce the following initialization steps.

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

Step 1: The Crypto Officer must install opacity shields as described in Section 2.13 of this document.

Step 2: The Crypto Officer must apply tamper evidence labels as described in Section 2.13 of this document.

Step 3: Install for Smart Licensing for Triple-DES/AES licenses to require the security appliances to use Triple-DES and AES (for data traffic and SSH).

Step 4: Enable “FIPS Mode” to allow the security appliances to internally enforce FIPS-compliant behavior, such as run power-on self-tests and bypass test, using the following command:

```
security # [enable | disable] fips-mode
security # commit-buffer
security # connect local-mgmt
security # reboot
```

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

```
security # show fips-mode
```

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

Step 6: SSH host key created during first-time setup of a device was hard coded to 1024 bits, you must destroy this old host key and generate a new one.

```
system/services # delete ssh-server host-key
system/services # commit-buffer
system/services # set ssh-server host-key rsa 2048
system/services # commit-buffer
system/services # create ssh-server host-key
system/services # commit-buffer
system/services # show ssh-server host-key
```

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: Reboot the security appliances.

In addition, for the Secure Operations steps required for the embedded cryptographic module (ASA-CM), please refer to the Security Policy for more information. The ASA-CM module has been certified with FIPS 140-2 Cert. #3789.