Cisco Firepower 4100 and Cisco Firepower 9300 Series

FIPS 140-2 Non Proprietary Security Policy
Level 2 Validation

Version 0.3

May 24, 2017

Table of Contents

1 Introduction

1.1 Purpose

This is the non-proprietary Security Policy for Cisco Firepower 4100 and Cisco Firepower 9300 Series running firmware version 2.0. 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 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 (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 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 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 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, 4120, 4140 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.

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

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 validated by the CMVP and has 140-2 certificate #2898. Thus, the sections throughout this SP detail the FIPS compliance of FX-OS.

Firepower 4100 and 9300 Series comprises the following platforms:

- FPR4110
- FPR4120
- FPR4140
- FPR4150
- FPR9300-SM24
- FPR9300-SM36

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 2.0, 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 SSH, SNMP, HTTPS, StrongSwan (IPsec/IKEv2) and cURL.

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 software.
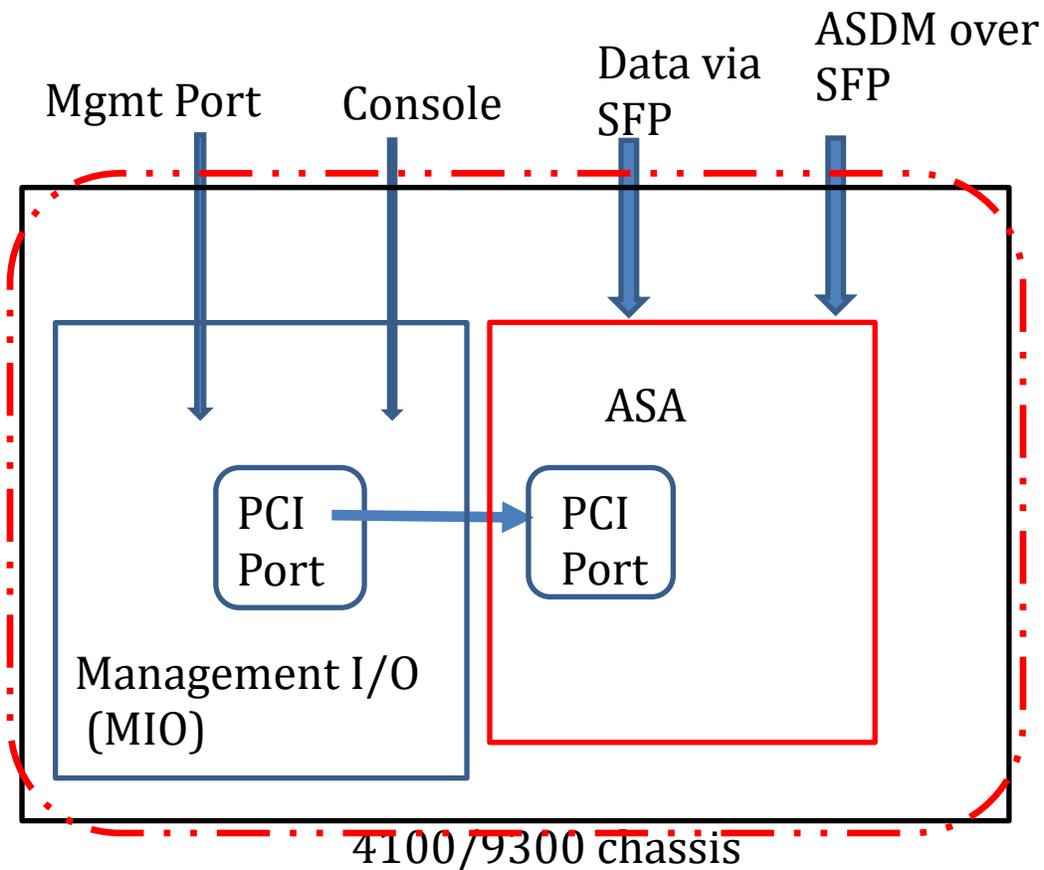
Diagram 1 Block Diagram

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 Serial Console port USB Port
Data Output	MGMT Port Serial Console port USB Port
Control Input	MGMT Port Serial Console port
Status Output	MGMT Port Serial Console port USB Port 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
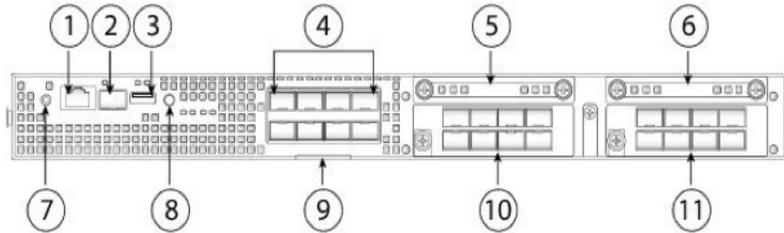
1	RJ-45 console port	2	1 Gigabit Ethernet management port
3	Type A USB port	4	Eight fixed SFP+ (1G/10G) ports are provided (network module slot 1) Gigabit Ethernet 1/1 through 1/8 labeled left to right, top to bottom
5	SSD 1	6	SSD 2
7	Power LED	8	Locator LED
9	Pull out label card	10	Network Module (network 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 Rear
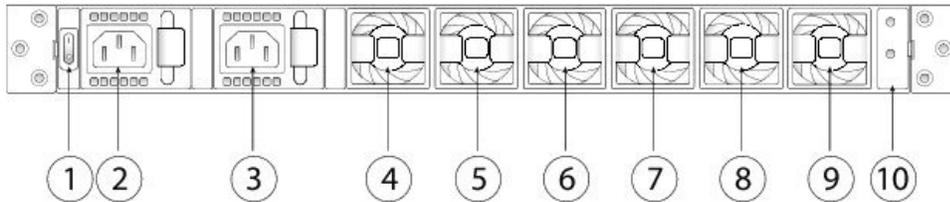
1	Power on/off switch	2	Power supply module 1
3	Power supply module 2	4	Fan module 1
5	Fan module 2	6	Fan module 3
7	Fan module 4	8	Fan module 5
9	Fan module 6	10	Location for the two-post grounding lug **Note** The two-post grounding lug is included in the accessory kit.

9300 Series Front
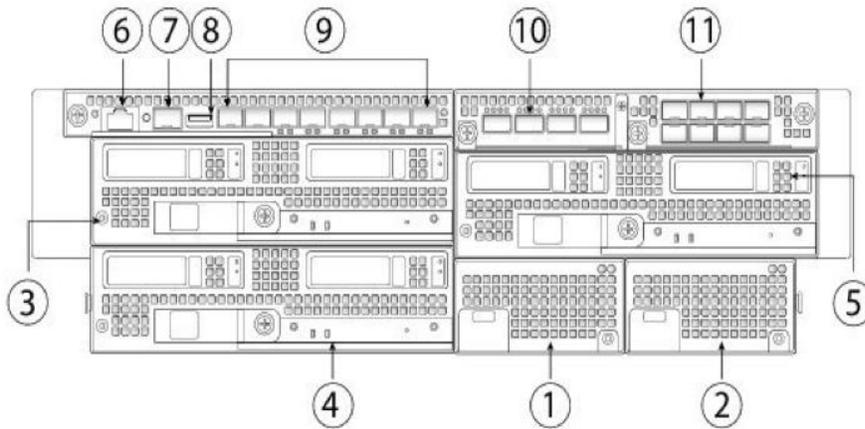
1	Power supply module PSU-1	2	Power supply module PSU-2
3	Security Module 1	4	Security Module 3
5	Security Module 2	6	RJ-45 console port
7	1 Gigabit Ethernet management port	8	USB port
9	Eight 10 Gigabit Ethernet data ports (Gigabit Ethernet 1/1 through 1/8)	10	Network Module (network module slot 2)
11	Network Module (network module slot 3)		

9300 Series Rear
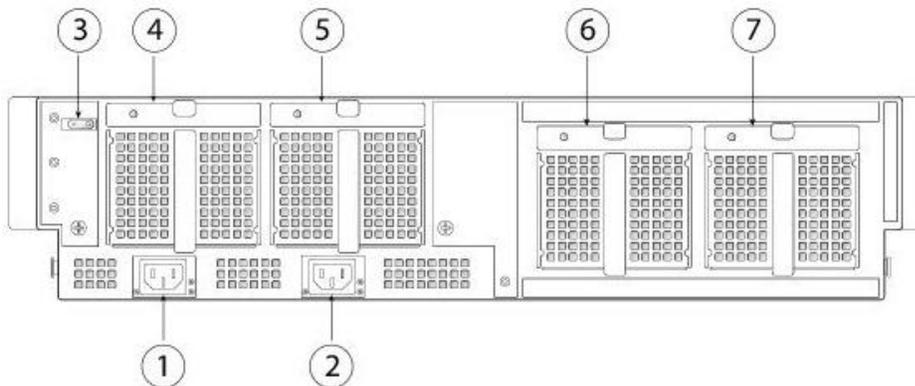
1	Power feed for PSU-2	2	Power feed for PSU-1
3	On/Off switch	4	Fan module FAN-1
5	Fan module FAN-2	6	Fan module FAN-3
7	Fan module FAN-4		

In addition, for details of the Cryptographic Boundary and the associated physical/logical interfaces of the embedded ASA-CM cryptographic module, please refer to certificate number #2898's Security Policy for more information.

2.5 Roles and Services

The appliances can be accessed in one of the following ways:
- SSHv2
- HTTPS
- IPsec
- SNMP
- cURL

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 shared secrets must each be at a minimum eight (8) characters long. There must be at least one special character and at least one number character (enforced procedurally) along with six additional characters taken from the 26 upper case, 26 lower case, 10 numbers and 32 special characters. See the Secure Operation section for more information. If six (6) special/alpha/number characters, one (1) special character and one (1) number are used without repetition for an eight (8) digit value, the probability of randomly guessing the correct sequence is one (1) in 187,595,543,116,800. This is calculated by performing 94 x 93 x 92 x 91 x 90 x 89 x 32 x 10. In order to successfully guess the sequence in one minute would require the ability to make over 3,126,592,385,280 guesses per second, which far exceeds the operational capabilities of the module.

Additionally, when using RSA based authentication, RSA key pair has modulus size of 2048 bits, thus providing 112 bits of strength. Assuming the low end of that range, 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 chance required by FIPS 140-2. To exceed a one in 100,000 probability of a successful random key guess in one minute, an attacker would have to be capable of approximately 8.65×10^{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 SSH or HTTPS/TLS. 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, IPsec encryption key, IPsec authentication key (r, w, d)
SSH Functions	Negotiation and encrypted data transport via SSH.	Operator password, SSH Traffic Keys (r, w, d)
HTTPS Functions (TLS)	Negotiation and encrypted data transport via HTTPS.	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 Traffic Keys (r, w, d)

Table 3 User Services

2.7   Crypto Officer Services

A Crypto Officer enters the system by accessing the console port with a terminal program or SSH v2 session to a LAN port or the 10/100/1000 management Ethernet port. The Crypto Officer authenticates in the same manner as a User. 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, 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)
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.	Operator password, Enable 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, TLS RSA private key, TLS RSA public key, TLS pre-master secret, TLS Traffic Keys (r, w, d)

IPsec VPN	Configure IPsec VPN parameters, provide entry and output of CSPs.	ISAKMP preshared, 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)
SSH v2	Configure SSH v2 parameter, provide entry and output of CSPs.	DH private DH public key, DH Shared Secret, ECDH private ECDH public key, ECDH Shared Secret, SSHv2 Private Key, SSHv2 Public 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)
SNMPv3	Configure SNMPv3 MIB and monitor status.	SNMPv3 Password, snmpEngineID, SNMP session key (r, w, d)
cURL	Uses TLS/SSL and is used for sending messages to Cisco's Smart Licensing back-end.	DRBG entropy input, DRBG Seed, DRBG V, DRBG Key, TLS RSA private key, TLS RSA public key, TLS pre-master secret, TLS Traffic Keys (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

---

[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.

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 http://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60.pdf. This site lists all configuration guides.

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 cryptographic module, please refer to certificate number #2898's Security Policy.

2.10   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 comes from a process of extracting bits from dev/urandom and fed into the DRBG.

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
DRBG entropy input	SP800-90A CTR_DRBG	384-bits	This is the entropy for SP 800-90A CTR_DRBG. Software based entropy source used to construct seed.	DRAM (plaintext)	Power cycle the device

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
DRBG Seed	SP800-90A CTR_DRBG	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	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	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, 3072, 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, 256, 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, 3072, 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

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
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	Shared Secret	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
skeyid_d	Shared Secret	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	Shared Secret	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	168 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
ISAKMP preshared	Pre-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
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)	Automatically when IPsec session is terminated

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
IKE authentication public key	RSA	RSA (2048 bits)	RSA public key used in IKE authentication. Internally generated by the module.	DRAM (plaintext)	Automatically when IPsec session is terminated
IPsec encryption key	Triple-DES, AES and AES-GCM	168 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 is entered by the User.	NVRAM (plaintext)	Overwrite with new password
Enable 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)	/security/radius/ server # delete key
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)	/security/tacacs/ server # delete key
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.	DRAM (plaintext)	Automatically when SSH session is terminated
SSHv2 Public Key	RSA	2048 bits modulus	The SSHv2 public key used in SSHv2 connection. This key is internally generated by the module.	DRAM (plaintext)	Automatically when SSH session is terminated

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
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
TLS RSA private key	RSA	2048 bits	Identity certificates for the security appliance itself and also used in TLS session negotiations. This key was generated by calling FIPS approved DRBG.	DRAM (plaintext)	Automatically when TLS session is terminated
TLS RSA public key	RSA	2048 bits	Identity certificates for the security appliance itself and also used in TLS session negotiations. This key was generated by calling FIPS approved DRBG.	DRAM (plaintext)	Automatically when TLS session is terminated
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 traffic keys	Triple-DES/AES 128/192/256 HMAC-SHA1/256/384/512	192 bits Triple-DES or 128/192/256 bits AES	Used in HTTPS/TLS connections. Generated using TLS protocol. This key was derived in the module.	DRAM (plain text)	Automatically when TLS session is terminated
SNMPv3 password	Shared Secret	256 bits	The password use to setup SNMPv3 connection. This key is entered by Crypto Officer.	NVRAM (plaintext)	Overwrite with new password
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)	Power cycle the device
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 commands 'install platform platform-vers' and 'scope auto-install'

Table 6 Cryptographic Keys and CSPs

In addition, for details of the Cryptographic Keys and CSPs provided by the embedded cryptographic module, please refer to certificate number #2898's Security Policy.

2.11 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	Certificate
AES (128/192/256 bit CBC, GCM)	4307
Triple-DES (CBC, 3-key)	2328
SHS (SHA-1/256/384/512)	3546
HMAC (SHA-1/256/384/512)	2843
RSA (PKCS1_V1_5; KeyGen, SigGen, SigVer; 2048 bits)	2328
DRBG (CTR_DRBG)	1368
CVL Component (IKEv2, TLS, SSH, SNMP)	1023

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 6071 for IPsec and RFC 5288 for TLS. The module uses basically a 96-bit IV, which is comprised of a 4 byte salt unique to the crypto session and 8 byte monotonically increasing counter. The module generates new AES-GCM keys if the module loses power.

- The SSH, TLS, SNMP and IPSec protocols have not been reviewed or tested by the CAVP and CMVP.

Non-FIPS Approved Algorithms Allowed in FIPS Mode

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

- Diffie-Hellman (key agreement; key establishment methodology provides between 112 and 150 bits of encryption strength)
- EC Diffie-Hellman (key agreement; key establishment methodology provides between 128 and 256 bits of encryption strength)
- HMAC MD5 is allowed in FIPS mode strictly for TLS
- MD5 is allowed in FIPS mode strictly for TLS
- NDRNG
- 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-SHA1 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)

Note: The non-approved algorithms HMAC MD5 and MD5 are not allowed in FIPS mode when not used with TLS.

In addition, the embedded cryptographic module (FIPS 140-2 Cert. #2898) 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:

Algorithms		
	ASA OS (Firmware)	ASA on-board (Cavium Nitrox III)
AES (128/192/256 CBC, GCM)	4249	2034/2035
Triple-DES (CBC, 3-key)	2304	1311
SHS (SHA-1/256/384/512)	3486	1780
HMAC (SHA-1/256/384/512)	2787	1233
RSA (PKCS1_V1_5; 2048 bits)	2298	
ECDSA (P-256, P-384, P-521)	989	
DRBG (SHA-512)	1328	197
CVL Component (IKEv2, TLS, SSH)	1002	

Table 8 Approved Algorithm CAVP 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 embedded module's AES-GCM implementation conforms to IG A.5 scenario #1 following RFC 6071 for IPsec and RFC 5288 for TLS. The module uses basically a 96-bit IV, which is comprised of a 4 byte salt unique to the crypto session and 8 byte monotonically increasing counter. The module generates new AES-GCM keys if the module loses power.

- The SSH, TLS and IPSec protocols have not been reviewed or tested by the CAVP and CMVP.

Non-FIPS Approved Algorithms Allowed in FIPS Mode from Embedded Module

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

- Diffie-Hellman (key agreement; key establishment methodology provides between 112 and 150 bits of encryption strength)
- RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength)
- NDRNG
- HMAC MD5 is allowed in FIPS mode strictly for TLS
- MD5 is allowed in FIPS mode strictly for TLS

Non-Approved Cryptographic Algorithms from Embedded Module

The embedded 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)
- DES
- HMAC MD5
- MD5
- RC4
- RSA (key wrapping; key establishment methodology less than 112 bits of encryption strength; non-compliant)
- HMAC-SHA1 is not allowed with key size under 112-bits

Note: The non-approved algorithms HMAC MD5 and MD5 are not allowed in FIPS mode when not used with TLS.

2.12 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 insure all components are functioning correctly.

Self-tests performed

- POSTs
  - AES 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 KAT
  - HMAC-SHA-256 KAT
  - HMAC-SHA-384 KAT
  - HMAC-SHA-512 KAT

- o RSA KATs (separate KAT for signing; separate KAT for verification)
- o SHA-1 KAT
- o Triple-DES Encrypt/Decrypt KATs

- Conditional tests
  - o RSA pairwise consistency test
  - o Continuous Random Number Generator test for SP800-90A DRBG
  - o Continuous Random Number Generator test for NDRNG

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 cryptographic module, please refer to certificate number #2898 Security Policy.

2.13 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.

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 site security program.

Models	Number Tamper labels	Tamper Evident Labels	Number Opacity Shields	Opacity Shields
FPR4110, 4120, 4140 and 4150	15	Cisco_TEL.FIPS_Kit	1	69-100250-01
FPR9300-SM24 and FPR9300-SM36	12	Cisco_TEL.FIPS_Kit	1	800-102843-01

Opacity Shield installation

4100 Series

STEP 1

- **Attach Rack Mount Brackets**
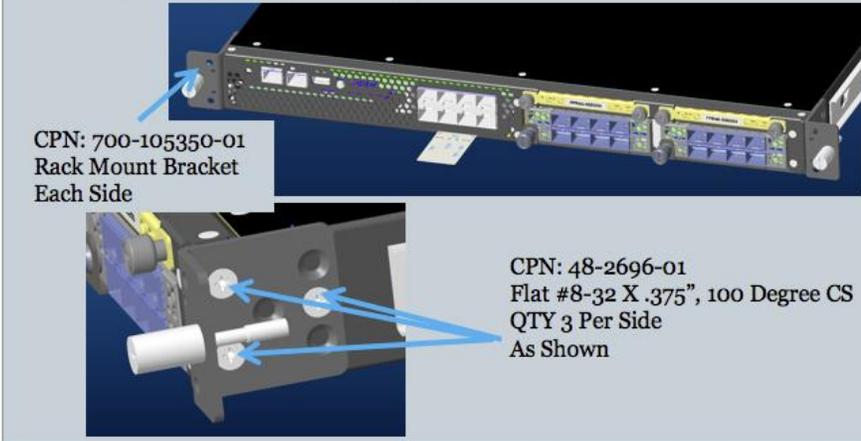
CPN: 700-105350-01
Rack Mount Bracket
Each Side

CPN: 48-2696-01
Flat #8-32 X .375", 100 Degree CS
QTY 3 Per Side
As Shown

STEP 2

- **Attach Cable Brackets**
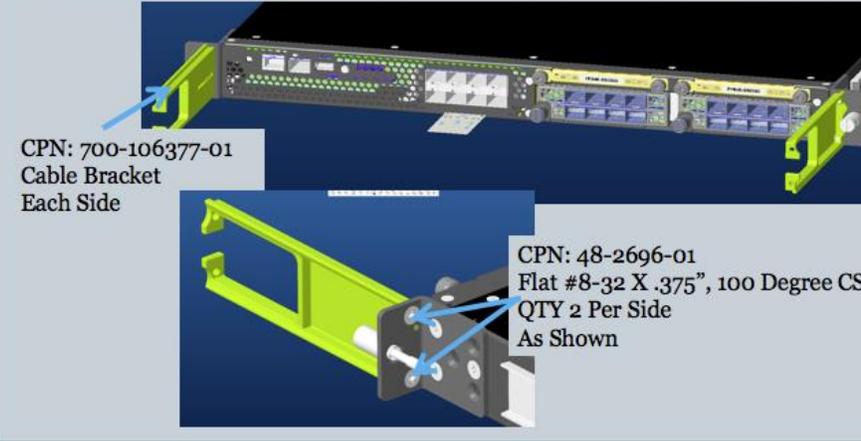
CPN: 700-106377-01
Cable Bracket
Each Side

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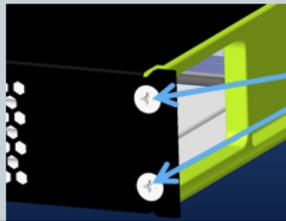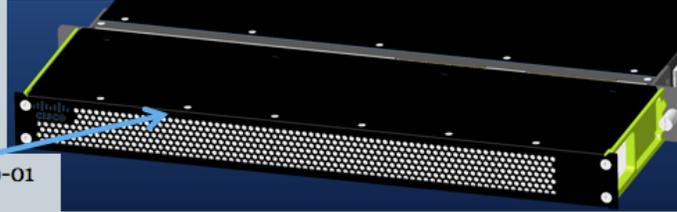
CPN: 48-2696-01
Flat #8-32 X .375", 100 Degree CS
QTY 2 Per Side
As Shown

9300 Series
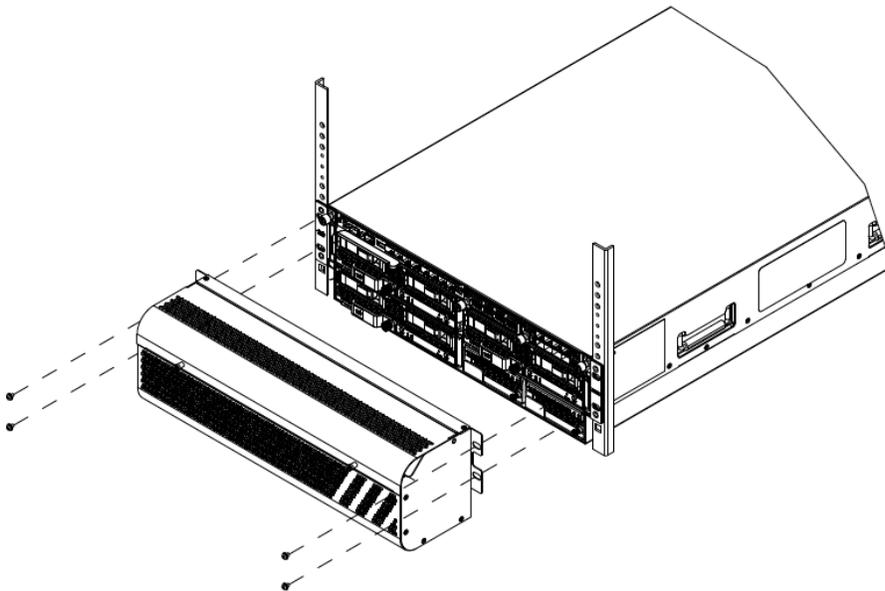
Inspection of the opacity shields should be incorporated into facility security posture to include how often to inspect and any recording of the inspection. It is recommended 30 days but this is the facilities Security Manager decision.

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: Front 4110, 4120, 4140 and 4150 (no TEL present on front)

#1

Figure 2: Right Side 4110, 4120, 4140 and 4150
(Right side has TEL #1 overlapping top and side)

#2

Figure 3: Left Side 4110, 4120, 4140 and 4150
(Left side has TEL #2 overlapping top and side)
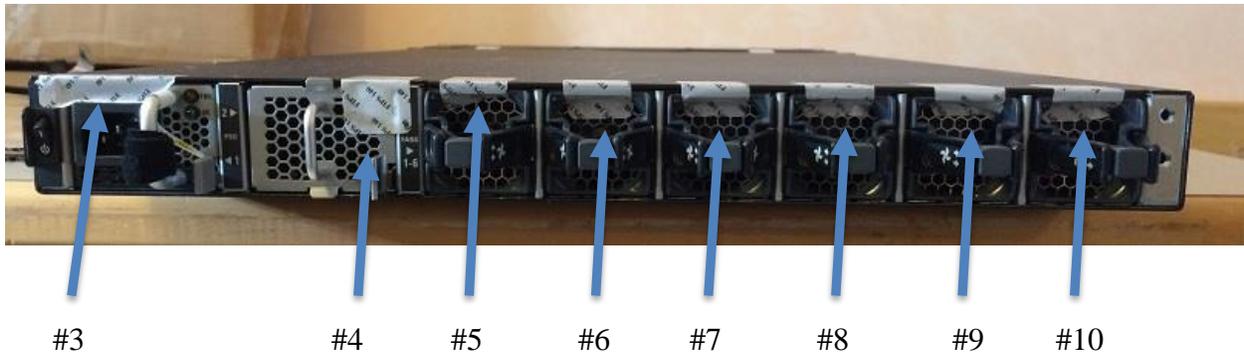
#3   #4   #5   #6   #7   #8   #9   #10

Figure 4: Rear 4110, 4120, 4140 and 4150
(Rear has TEL #3, #4, #5, #6, #7, #8, #9 and #10 overlapping top and plug-in)


#11   #12
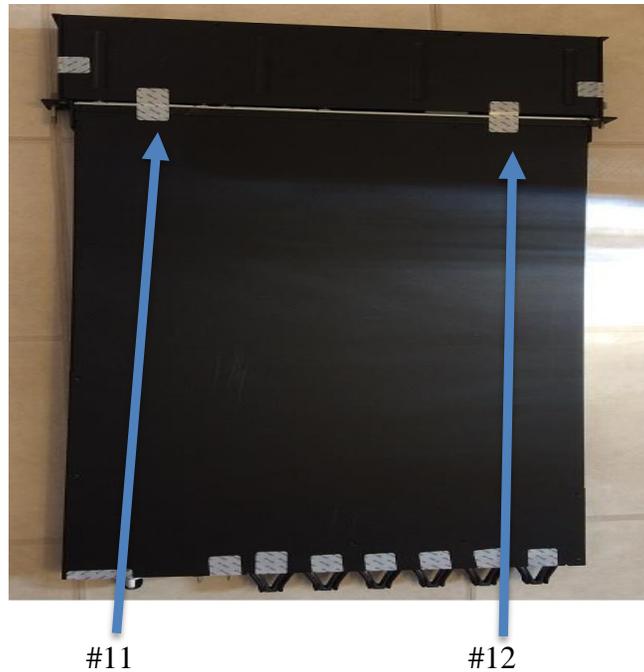
Figure 5: Top 4110, 4120, 4140 and 4150
(Top shows TEL #11 and #12 overlapping opacity shield and 4000 chassis, also present is TEL
#1,2,3,4,5,6,7,8,9,10)

13   #14   #15 (used to cover USB port)

Figure 6: Bottom 4110, 4120, 4140 and 4150
(Bottom shows TEL #13 and # 14 overlapping opacity shield and 4000 chassis, TEL #15 partially obscured inside the opacity shield, overlapping front of chassis and bottom of chassis covering the USB)

#1   #2

Figure 7: Front 9300 Series
(Front opacity shield has TEL #1 and #2)

Figure 8: Right Side 9300 Series (Right side has no TELs)

Figure 9: Left Side 9300 Series (Left side has no TELs)

#3   #4   #7   #5   #6
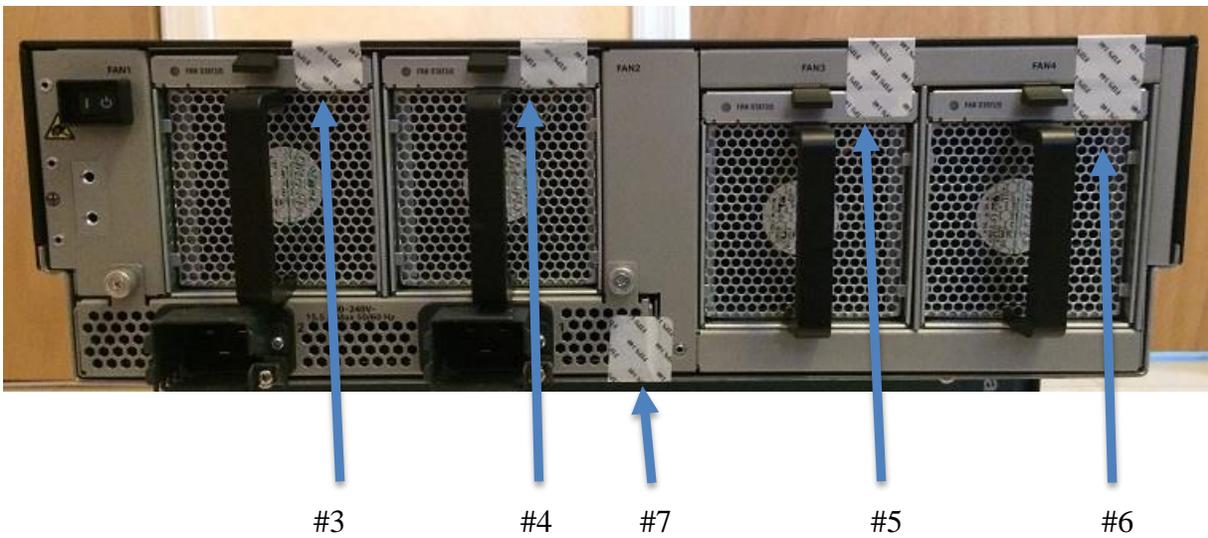
Figure 10: Rear 9300 Series
(Rear has TEL #3, #4, #5, #6 and #7 on bottom, each overlapping chassis and plug-in)

#8   #9   #12 (used to cover USB port)

Figure 11: Top 9300 Series
(Top has TEL #8 and #9 overlapping opacity shield and top of chassis, also present is TEL #3,4,5,6 and 7. TEL #12 partially obscured inside the opacity shield, overlapping front of chassis and top of chassis covering the USB)

#10   #11
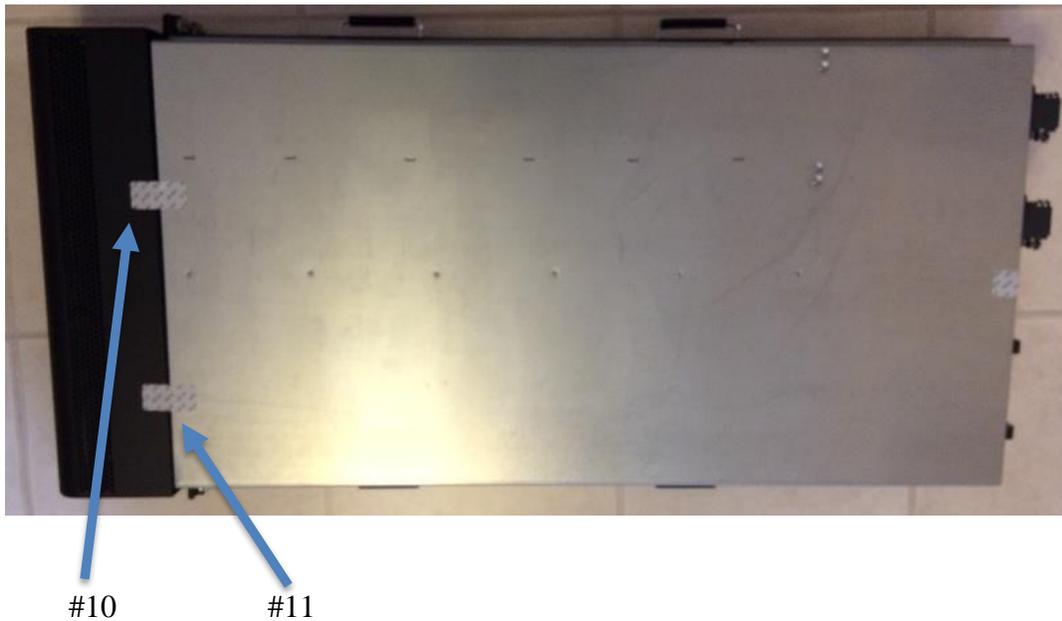
Figure 12: Bottom 9300 Series
(Bottom has TEL #10 and #11 overlapping opacity shield and bottom of chassis, also present is TEL #7 overlapping bottom and back of plug-in)

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

Appling 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.

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 2.0 (File fxos-k9.2.0.1.141.SPA). These are the only allowable images 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 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, please refer to certificate number #2898's Security Policy.