Cisco Firepower 2100 Cryptographic Module

FIPS 140-2 Non Proprietary Security Policy
Level 2 Validation

Documentation Version 1.3

Last Update: February 12, 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 2100 APPLIANCE FAMILY OVERVIEW 5

2.1 CISCO FX-OS WITH FX-OS CRYPTO LIBRARY 6
2.2 CISCO ASA WITH ASA CRYPTO LIBRARY 6
2.3 CRYPTOGRAPHIC MODULE CHARACTERISTICS 6
2.4 CRYPTOGRAPHIC BOUNDARY 6
2.5 MODULE INTERFACES 7
2.6 FRONT AND REAR PANELS 8
2110 and 2120 Front 8
2110 and 2120 Rear 8
2130 and 2140 Front 9
2130 and 2140 Rear 9
2.7 ROLES AND SERVICES 10
2.8 USER SERVICES 11
2.9 CRYPTO OFFICER SERVICES 11
2.10 NON-FIPS MODE SERVICES 13
2.11 UNAUTHENTICATED SERVICES 13
2.12 CRYPTOGRAPHIC KEY/CSP MANAGEMENT 14
2.13 CRYPTOGRAPHIC ALGORITHMS 18
Approved Cryptographic Algorithms 18
Non-FIPS Approved Algorithms Allowed in FIPS Mode 20
Non-Approved Cryptographic Algorithms 20
2.14 PHYSICAL SECURITY 21
Opacity Shield Security 21
Opacity Shield installation 22
Tamper Evidence Label (TEL) placement 22

3 SECURE OPERATION 24

3.1 CRYPTO OFFICER GUIDANCE - SYSTEM INITIALIZATION 24
3.2 CRYPTO OFFICER GUIDANCE - SYSTEM CONFIGURATION 26

1 Introduction

1.1 Purpose

This is the non-proprietary Security Policy for the Cisco Firepower 2100 Cryptographic Module running firmware 9.12. This security policy describes how this module containing two cryptographic libraries meets the security requirements of FIPS 140-2 Level 2 and how to run this 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/groups/computer-security-division/security-testing-validation-and-measurement.

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 2100 Cryptographic Module will operate, including the rules derived from the requirements of FIPS 140-2, FIPS 140-2 IG and additional rules imposed by Cisco Systems, Inc. More information is available on the module from the following sources:

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

http://www.cisco.com/c/en/us/products/index.html
https://www.cisco.com/c/en/us/support/security/firepower-2100-series/tsd-products-support-series-home.html

For answers to technical or sales related questions please refer to the contacts listed on the Cisco Systems website at www.cisco.com.

© Copyright 2021 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

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 2100 Cryptographic Module identified running two cryptographic libraries is referred to as Cisco Firepower 2100 Cryptographic Module, Cisco Firepower 2100 CM, FX-OS Crypto Library, ASA Crypto Library or Module.

1.5 Document Organization

The Security Policy document is part of the FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

Vendor Evidence document
Finite State Machine
Other supporting documentation as additional references

This document provides an overview of the Cisco Firepower 2100 Cryptographic Module identified above and explains the secure layout, configuration and operation of the module. This introduction section is followed by Section 2, which details the general features and functionality of the module. Section 3 specifically addresses the required configuration for the FIPS-mode of operation.

With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Submission Documentation is Cisco-proprietary and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Cisco Systems.

© Copyright 2021 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

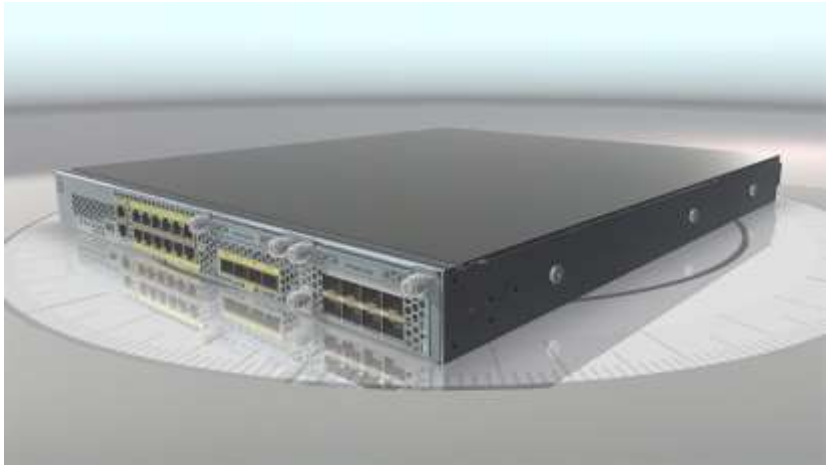
2 Cisco Firepower 2100 Appliance Family Overview

The Cisco Firepower 2100 Series NGFW appliances can be deployed either as a Next-Generation Firewall (NGFW) or as a Next-Generation IPS (NGIPS). They are perfect for the Internet edge and all the way in to the data center. There are four identical externally looking, new models: Firepower 2110 and 2120 models offer 1.9 and 3 Gbps of firewall throughput while Firepower 2130 and 2140 models provide 5 and 8.5 Gbps respectively of firewall throughput. When deployed as next-generation firewall (NGFW) appliances, it uses the Cisco Firepower 2100 Cryptographic Module.

Cisco Firepower 2100 Series include the following appliances:

- FPR 2110 (part number: FPR2110-NGFW-K9)
- FPR 2120 (part number: FPR2120-NGFW-K9)
- FPR 2130 (part number: FPR2130-NGFW-K9)
- FPR 2140 (part number: FPR2140-NGFW-K9)

FPR 2110 and FPR 2120



FPR 2130 and FPR 2140

© Copyright 2021 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

2.1 Cisco FX-OS with FX-OS Crypto Library

The Cisco **F**irepower e**X**tensible **O**perating **S**ystem (FX-OS) running on the 2100 Series is a next-generation network and content security solutions which provides a web interface that makes it easy to configure platform settings and interfaces, provision devices, and monitor system status. The FX-OS is part of the Cisco Application Centric Infrastructure (ACI) Security Solution and provides an agile, open, built for scalability, consistent control, and simplified management. The FX-OS provides the following features:

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

2.2 Cisco ASA with ASA Crypto Library

The Cisco ASA delivers enterprise-class firewall for businesses, improving security at the Internet edge, high performance and throughput for demanding enterprise data centers. It is available in a blade form factor that can be integrated into the Cisco Firepower 2100 Series.

The ASA solution offers a combination of the industry's most deployed stateful firewall along with a comprehensive range of next-generation network security services, intrusion prevention system (IPS), content security, secure unified communications, SSHv2, SNMPv3, HTTPS/TLSv1.2 and StrongSwan (IPSec/IKEv2).

2.3 Cryptographic Module Characteristics

The Cisco Firepower 2100 Cryptographic Module contains FX-OS Cryptographic Library running on the Intel 64-bit Xeon and the ASA Cryptographic Library executing on the Cavium Octeon processor, providing the cryptographic services required for their perspective hosts within the module.

2.4 Cryptographic Boundary

The module is a hardware, multi-chip standalone crypto module. The cryptographic boundary is defined as the 2100 series chassis unit encompassing the "top," "front," "left," "right," “rear” and "bottom" surfaces of the case representing the module’s physical perimeter. Diagram 1 below is the block diagram showing two independent crypto libraries running on the same hardware platform (the rectangle area).

© Copyright 2021 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

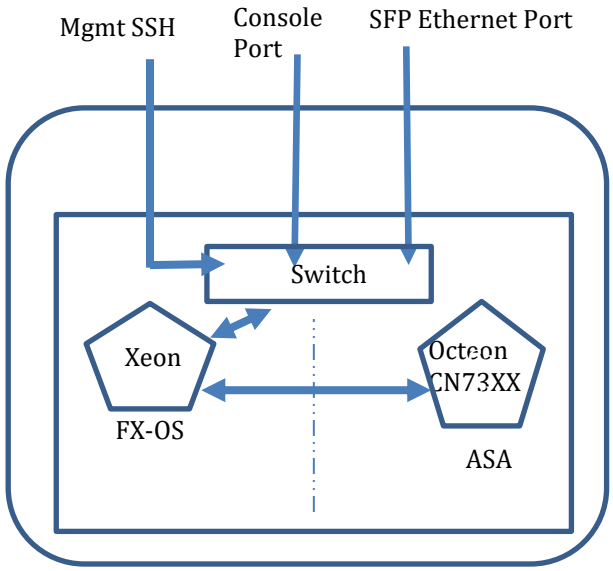


Diagram 1 Block Diagram

2.5 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	2100 Physical Interfaces
Data Input	MGMT Port Console port SFP/SFP+ Ethernet and/or RJ-45 Gigabit Ethernet Ports
Data Output	MGMT Port Console port SFP/SFP+ Ethernet and/or RJ-45 Gigabit Ethernet Ports
Control Input	MGMT Port Console port SFP/SFP+ Ethernet and/or RJ-45 Gigabit Ethernet Ports
Status Output	MGMT Port Console port SFP/SFP+ Ethernet and/or RJ-45 Gigabit Ethernet Ports LEDs

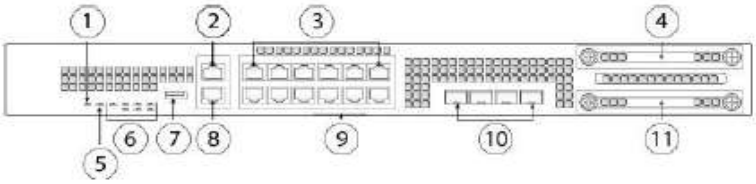
Table 2 Hardware/Physical Boundary Interfaces

Note: Each module has a Type A USB 2.0 port, but it is considered to be disabled once the Crypto-Officer has applied the Opacity Shield.

© Copyright 2021 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

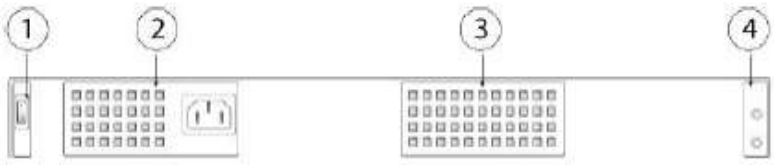
2.6 Front and Rear Panels

2110 and 2120 Front



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

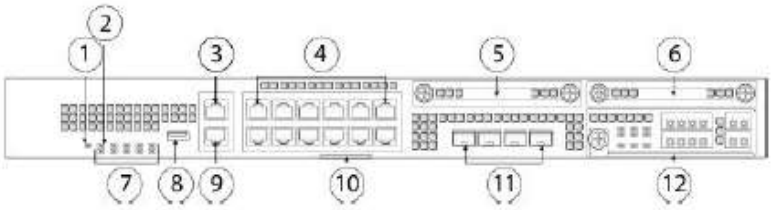
2110 and 2120 Rear



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

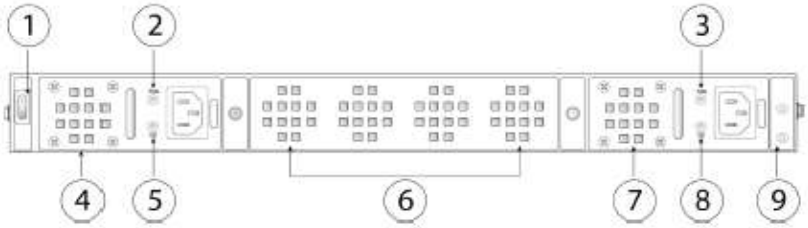
© Copyright 2021 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

2130 and 2140 Front



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

2130 and 2140 Rear



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

© Copyright 2021 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

2.7 Roles and Services

The module 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 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. If not using TACACS+, then the module automatically assigns the authenticated identity to the user role (and the operator can escalate their privileges by issuing the "enable" command and providing the enable password). When using the TACACS+, the CO can configure the module to behave in the same was as when using a local user database, or the CO can configure the TACACS+ server to respond with the identity's privilege level (in addition to whether or not they should be granted access) and the module will automatically place the operator into the highest role supported by their privilege level.

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

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

Additionally, when using RSA based authentication, RSA key pair has modulus size of 2048 bits, thus providing 112 bits of strength, which means an attacker would have a 1 in 2^112 chance of randomly obtaining the key, which is much stronger than the one in a million chances required by FIPS 140-2. Similarly, for multiple attempts to use the authentication mechanism during a one-minute period, under the optimal modern network condition, an attacker would probably get 60,000 guesses per minute. Therefore, the associated probability of a successful random attempt during a one-minute period is 60,000/ 2^112 = 1/8.67x10^28, which is less than 1 in 100,000 required by FIPS 140-2.

© Copyright 2021 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

2.8 User Services

A User accesses the system through a console port, SSHv2, SNMPv3 or HTTPS/TLSv1.2 to one of the data input interfaces listed in Table 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, DRBG entropy input, DRBG seed, DRBG V, DRBG key, Diffie-Hellman private key, Diffie-Hellman public key, Diffie-Hellman shared secret, EC Diffie-Hellman private key, EC Diffie-Hellman public key, EC Diffie-Hellman shared secret, skeyid, skeyid_d, SKEYSEED, IKE session encryption 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, DRBG entropy input, DRBG seed, DRBG V, DRBG key, Diffie-Hellman private key, Diffie-Hellman public key, Diffie-Hellman shared secret, EC Diffie-Hellman private key, EC Diffie-Hellman public key, EC Diffie-Hellman shared secretSSHv2 integrity key DRBG entropy input, DRBG seed, DRBG V, DRBG key, SSHv2 RSA private key, SSHv2 RSA public key, SSHv2 integrity key and SSHv2 session key (r, w, d)
HTTPS Functions (TLSv1.2)	Negotiation and encrypted data transport via HTTPS/TLSv1.2.	Operator password, DRBG entropy input, DRBG Seed, DRBG V, DRBG key, ECDSA private key, ECDSA public key, TLS RSA private key, TLS RSA public key, TLS pre-master secret, TLS master secret, TLS encryption keys and TLS integrity key (r, w, d)

Table 3 User Services

2.9 Crypto Officer Services

A Crypto Officer enters the system by accessing the console port with a terminal program or SSHv2, SNMPv3 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.

© Copyright 2021 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

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.	DRBG entropy input, DRBG seed, DRBG V, DRBG key, Diffie-Hellman private key, Diffie-Hellman public key, Diffie-Hellman shared secret, EC Diffie-Hellman private key, EC Diffie-Hellman public key, EC Diffie-Hellman shared secret, SSHv2 private key, SSHv2 public key, SSHv2 session key, SSHv2 integrity key, ECDSA private key, ECDSA public key, TLS RSA private key, TLS RSA public key, TLS pre-master secret, TLS master secret, TLS encryption keys, TLS integrity key, ISAKMP preshared, skeyid, skeyid_d, SKEYSEED, IKE session encryption key, IKE session authentication key, IKE authentication private Key, IKE authentication public key, IPSec encryption key, IPSec authentication key, SNMPv3 Password and SNMPv3 session key (r, w, d)
Firmware integrity	Install the firmware during the System Initialization.	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
Configure Encryption/Bypass	Set up the configuration tables for IP tunneling. Set preshared keys and algorithms to be used for each IP range or allow plaintext packets to be set from specified IP address.	Operator password, Enable 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, ISAKMP preshared, IKE session encrypt key, IKE session authentication key, 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)
HTTPS/TLS (TLSv1.2)	Configure HTTPS/TLS parameters, provide entry and output of CSPs.	DRBG entropy input, DRBG Seed, DRBG V, DRBG key, ECDSA private key, ECDSA public key, TLS RSA private key, TLS RSA public key, TLS pre-master secret, TLS master secret, TLS encryption keys and TLS integrity key (r, w, d)
IPSec VPN Functions	Configure IPSec VPN parameters, provide entry and output of CSPs.	DRBG entropy input, DRBG seed, DRBG V, DRBG key, Diffie-Hellman private key, Diffie-Hellman public key, Diffie-Hellman shared secret, EC Diffie-Hellman private key, EC Diffie-Hellman public key, EC Diffie-Hellman shared secret, ISAKMP preshared, skeyid, skeyid_d, SKEYSEED, IKE session encryption key, IKE session authentication key, 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	Configure SSH v2 parameter, provide entry and output of CSPs.	DRBG entropy input, DRBG Seed, DRBG V, DRBG key, Diffie-Hellman private key, Diffie-Hellman public key, Diffie-Hellman shared secret, EC Diffie-Hellman private key, EC Diffie-Hellman public key, EC Diffie-Hellman shared secret, SSHv2 private key, SSHv2 public key, SSHv2 integrity key and SSHv2 session key (r, w, d)
Self-Tests	Execute the FIPS 140 start-up tests on demand.	N/A
User services	The Crypto Officer has access to all User services.	Operator password (r, w, d)
SNMPv3	Configure SNMPv3 MIB and monitor status.	SNMPv3 Password, SNMPv3 authentication key, SNMPv3 session key (r, w, d)

© Copyright 2021 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Zeroization	Zeroize cryptographic keys/CSPs by running the zeroization methods classified in table 6, Zeroization column.	All CSPs (d)

Table 4 Crypto Officer Services

2.10 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 2.10, the Crypto Officer must zeroize all CSPs which places the module into the non-FIPS mode of operation. Neither the User nor the Crypto Officer are allowed to operate any of these services while in 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

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 CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide, 9.12. Updated: June 25, 2020.

https://www.cisco.com/c/en/us/td/docs/security/asa/asa912/configuration/general/asa-912-general-config.html. This site lists all configuration guides for the module.

2.11 Unauthenticated Services

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

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

© Copyright 2021 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

2.12 Cryptographic Key/CSP Management

The module administers both cryptographic keys and other critical security parameters such as passwords. All keys and CSPs are protected by the password-protection of the Crypto Officer role login, and can be zeroized by the Crypto Officer. Zeroization consists of overwriting the memory that stored the key or refreshing the volatile memory. Keys are both manually and electronically distributed but entered electronically. Persistent keys with manual distribution are used for pre-shared secret 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 module 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	384-bits	This is the entropy for SP 800-90A CTR_DRBG. It is used to construct the DRBG seed.	DRAM (plaintext)	Power cycle the device
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	2048–4096 bits	The shared secret used in Diffie-Hellman exchange. Established per the Diffie-Hellman protocol.	DRAM (plaintext)	Power cycle the device

© Copyright 2021 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

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

© Copyright 2021 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
IKE session encrypt key	Triple-DES/AES	Triple-DES 192 bits or AES 128/192/256 bits	The IKE session (IKE Phase I) encrypt key. This key is derived via key derivation function defined in SP800-135 KDF (IKEv2).	DRAM (plaintext)	Automatically when IPSec session is terminated
IKE session authentication key	HMAC-SHA-1/256/384/512	160-512 bits	The IKE session (IKE Phase I) authentication key. This key is derived via key derivation function defined in SP800-135 KDF (IKEv2).	DRAM (plaintext)	Automatically when IPSec 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)	Erase the secret
IKE authentication private Key	RSA/ECDSA	RSA (2048 bits) or ECDSA (Curves: P-256, P-384, P-521)	RSA/ECDSA private key used in IKE authentication. This key is generated by calling SP800-90A DRBG.	NVRAM (plaintext)	Zeroized by RSA/ECDSA keypair deletion command
IKE authentication public key	RSA/ECDSA	RSA (2048 bits) or ECDSA (Curves: P-256, P-384, P-521)	RSA/ECDSA public key used in IKE authentication. The key is derived in compliance with FIPS 186-4 RSA/ECDSA key pair generation method in the module.	NVRAM (plaintext)	Zeroized by RSA/ECDSA keypair deletion command
IPSec encryption key	Triple-DES/AES/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-1/256/384/512	160-512 bits	The IPSec (IKE Phase II) authentication key. This key is derived via a key derivation function defined in SP800-135 KDF (IKEv2).	DRAM (plaintext)	Automatically when IPSec session is terminated
Operator password	Password	8 plus characters	The password of the User role. This CSP is entered by the User.	NVRAM (plaintext)	Erase the password
Enable password	Password	8 plus characters	The password of the CO role. This CSP is 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

© Copyright 2021 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
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 RSA private key used in SSHv2 connection. This key is generated by calling SP 800-90A DRBG.	NVRAM (plaintext)	Zeroized by RSA keypair deletion command
SSHv2 public key	RSA	2048 bits modulus	The RSA public key used in SSHv2 connection. The key is derived in compliance with FIPS 186-4 RSA key pair generation method in the module.	NVRAM (plaintext)	Zeroized by RSA keypair deletion command
SSHv2 integrity key	HMAC-SHA-1	160 bits	Used for 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
SSHv2 session key	Triple-DES/AES	Triple-DES 192 bits or AES 128/192/256 bits	This is the SSHv2 session key. It is used to encrypt all SSHv2 data traffics traversing between the SSHv2 Client and SSHv2 Server. This key is derived via key derivation function defined in SP800-135 KDF (SSH).	DRAM (plaintext)	Automatically when SSH session is terminated
ECDSA private key	ECDSA	Curves: P-256, P-384, P-521	Signature generation used in IPSec/IKEv2 and TLSv1.2. This key is generated by calling SP 800-90A DRBG.	NVRAM (plaintext)	Zeroized by ECDSA keypair deletion command
ECDSA public key	ECDSA	Curves: P-256, P-384, P-521	Signature verification used in IPSec/IKEv2 and TLSv1.2. This key is derived in compliance with FIPS 186-4 ECDSA key pair generation method in the module.	NVRAM (plaintext)	Zeroized by ECDSA keypair deletion command
TLS RSA private key	RSA	2048 bits	Identity certificates for the security appliance itself and also used in TLSv1.2 session negotiations. This key is generated by calling SP 800-90A DRBG.	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

© Copyright 2021 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
TLS pre-master secret	Shared Secret	At least eight characters	Shared secret created/derived using asymmetric cryptography from which new HTTPS/TLSv1.2 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/TLSv1.2 keys. This key was derived from TLSv1.2 pre-master secret during the TLS session establishment	DRAM (plaintext)	Automatically when TLS session is terminated
TLS encryption keys	Triple-DES/AES/AES-GCM	Triple-DES 192 bits or AES 128/192/256 bits	Used in HTTPS/TLSv1.2 connections to protect the session traffic. This key was derived in the module.	DRAM (plaintext)	Automatically when TLS session is terminated
TLS integrity key	HMAC-SHA-256/384	256-384 bits	Used for TLSv1.2 integrity to assure the traffic integrity. This key was derived in the module.	DRAM	Automatically when TLS session is terminated
SNMPv3 password	Shared Secret	256 bits	The password is used 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 integrity verification.	Hard coded for firmware integrity testing	Zeroized by erasing the firmware image

Table 6 Cryptographic Keys and CSPs

2.13 Cryptographic Algorithms

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

Approved Cryptographic Algorithms

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

© Copyright 2021 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Algorithm	FX-OS Crypto Library	ASA Crypto Library
AES (128/192/256 CBC, GCM)	4905	4234
Triple-DES (CBC, 3-key)	2559	2293
SHS (SHA-1/256/384/512)	4012	3471
HMAC (SHA-1/256/384/512)	3272	2772
ECDSA (KeyGen, SigGen, SigVer; P-256, P-384, P-521)	N/A	1254
RSA (PKCS1_v1.5; KeyGen, SigGen, SigVer; 2048 bits)	2678	2286
CTR_DRBG (AES-256)	1735	1317
CVL Component (IKEv2, TLSv1.2, SSHv2, SNMPv3) [2]	1521	983
CKG (vendor affirmed)	N/A	N/A

Table 7 Approved Cryptographic Algorithms and Associated Certificate Number

Notes:

- 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 counter portion of the IV is set by the module within its cryptographic boundary. When the nonce_explicit part of 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. 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.
- 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}.
- No parts of the SSH, TLS, SNMP and IPSec protocols, other than the KDF, have been tested by the CAVP and CMVP.
- 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 is the unmodified output from SP800-90A DRBG.

[2] CVL Cert. #1521 implements the KDF for IKEv2, TLSv1.2 and SSHv2; CVL Cert. #983 implements the KDF for IKEv2, TLSv1.2, SSHv2 and SNMPv3 protocols.

© Copyright 2021 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Non-FIPS Approved Algorithms Allowed in FIPS Mode

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

- Diffie-Hellman (CVL Certs. #983 and #1521, key agreement; key establishment methodology provides between 112 and 150 bits of encryption strength)
- EC Diffie-Hellman (CVL Certs. #983 and #1521, 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-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)

2.14 Self-Tests

Self-tests performed

- FX-OS Crypto Library POSTs
  - AES-CBC Encrypt/Decrypt KATs
  - AES-GCM 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
  - RSA KATs (separate KAT for signing; separate KAT for verification)
  - SHA-1 KAT
  - Triple-DES-CBC Encrypt/Decrypt KATs
- FX-OS Crypto Library Conditional tests
  - RSA pairwise consistency test
  - CRNGT for SP800-90A DRBG
  - CRNGT for NDRNG

© Copyright 2021 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

- ASA Crypto Library POSTs
  - AES-CBC Encrypt/Decrypt KATs
  - AES-GCM Encrypt/Decrypt KATs
  - DRBG KAT (Note: DRBG Health Tests as specified in SP800-90A Section 11.3 are performed)
  - ECDSA (Sign and Verify) Power on Self-Test
  - HMAC-SHA-1 KAT
  - HMAC-SHA-256 KAT
  - HMAC-SHA-384 KAT
  - HMAC-SHA-512 KAT
  - RSA KATs (separate KAT for signing; separate KAT for verification)
  - SHA-1 KAT
  - SHA-256 KAT
  - SHA–384 KAT
  - SHA-512 KAT
  - Triple-DES-CBC Encrypt/Decrypt KATs
- ASA Crypto Library Conditional tests
  - RSA pairwise consistency test
  - ECDSA pairwise consistency test
  - Conditional IPSec Bypass test
  - CRNGT for SP800-90A DRBG
  - CRNGT for NDRNG

The security module performs all power-on self-tests automatically when the power is applied. All power-on self-tests must be passed before a User/Crypto Officer can perform services. The power-on self-tests are performed after the cryptographic systems are initialized but prior to the initialization of the LAN's interfaces; this prevents the security module from passing any data during a power-on self-test failure. In the unlikely event that a power-on self-test fails, an error message is displayed on the console followed by a security appliance reboot.

2.15 Physical Security

The FIPS 140-2 level 2 physical security requirements for the modules are met by the use of opacity 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
FPR2110, FPR2120, FPR2130, FPR2140	7	AIR-AP-FIPSKIT=	1	69-100250-01

© Copyright 2021 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Opacity Shield installation

2100 Series

Inspection of the opacity shields should be incorporated into facility security procedures to include how often to inspect and any recording of the inspection. It is recommended inspection occur at least every 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.

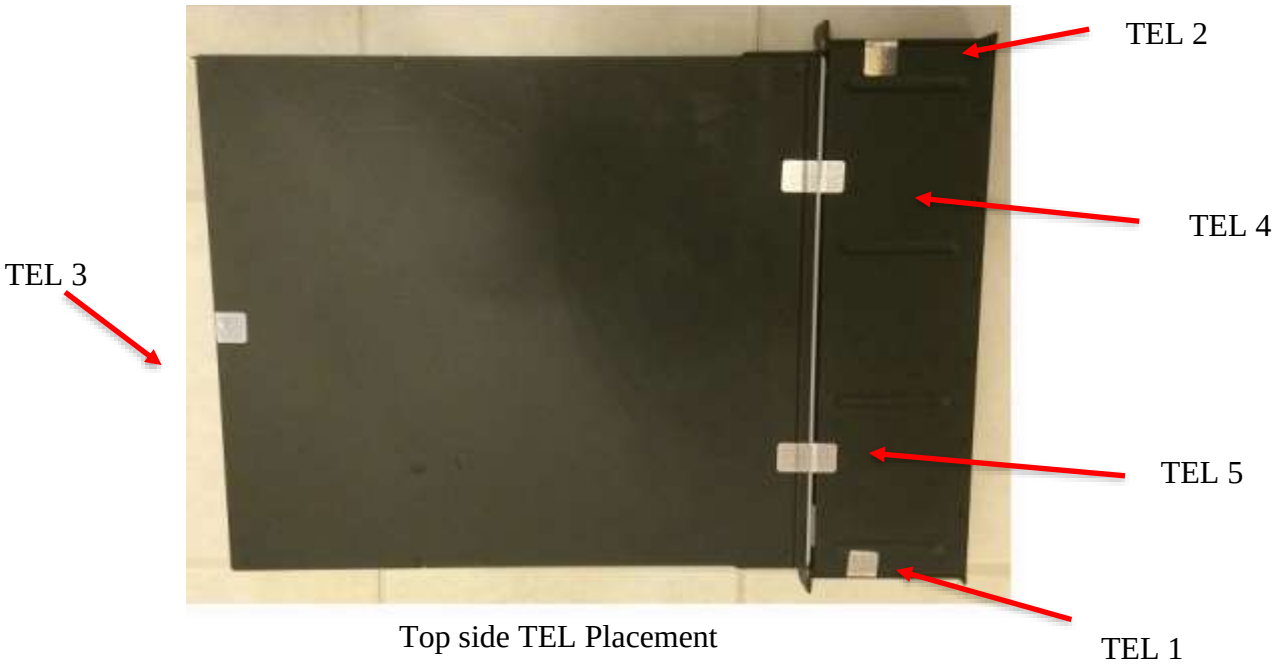
Any deviation of the TELs placement by unauthorized operators such as tearing, misconfiguration, removal, change, replacement or any other change in the TELs from its original configuration as depicted below shall mean the module is no longer in FIPS mode of operation. Returning the system back to FIPS mode of operation requires the replacement of the TELs as depicted below and any additional requirement per the site security policy which are out of scope of this Security Policy. To seal the system, apply tamper-evidence labels as depicted in the figures below.

Front side TEL Placement

Left side TEL Placement

Right side TEL Placement

© Copyright 2021 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.



Top side TEL Placement

Bottom side TEL Placement

Rear side TEL Placement

© Copyright 2021 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

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 and allow the label to cure for a minimum of 12 hours.

The tamper evident labels 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 labels have non-repeated serial numbers, they may be inspected for damage and compared against the applied serial numbers to verify that the security appliance has not been tampered with. Tamper evident labels can also be inspected for signs of tampering, which include the following: curled corners, rips, and slices. The word “FIPS” or “OPEN” may appear if the label was peeled back.

Inspection of the tamper seals should be incorporated into facility security to include how often to inspect and any recording of the inspection. It is recommended 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 Firepower 2100 Cryptographic Module runs FX-OS and ASA both contained within a single firmware image with version 9.12. This is the only allowable firmware image for this current FIPS-approved mode of operation.

The Crypto Officer must configure and enforce the following security steps for Tamper labels and opacity shield:

Step 1: The Crypto Officer must install opacity shields as described in Section 2.14 of this document.

Step 2: The Crypto Officer must apply tamper evidence labels as described in Section 2.14 of this document.

Step 3: The Crypto officer shall update the default User name (admin) and the default password (Admin123).

© Copyright 2021 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Step 4: The Crypto Officer should follow up the commands below to put the module into the FIPS mode.

firepower# scope security

firepower/security #enable fips-mode

firepower/security # exit

firepower# connect local-mgmt

firepower (local-mgmt)# reboot

Step 5: At the FXOS prompt type connect asa to get to the ASA prompt.

firepower# connect asa

Attaching to ASA CLI ... Press 'Ctrl+a then d' to detach.

Type help or '?' for a list of available commands.

ciscoasa>

Step 6: Configure ASA

ciscoasa> **en**
ciscoasa#

Note, the Crypto Officer needs to connect the platform to cisco.com to obtain the license for ASA.

ciscoasa> en

ciscoasa#

ciscoasa# license smart register idtoken [enter in token]

ciscoasa# configure terminal

ciscoasa(config)#license smart
ciscoasa(config)# sh lic all

ciscoasa(config)#fips enable

© Copyright 2021 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

3.2 Crypto Officer Guidance - System Configuration

To operate in FIPS mode, the Crypto Officer must perform the following steps:
Step 1: Assign users a Privilege Level of 1.

Step 2: Define RADIUS and TACACS+ shared secret keys that are at least 8 characters long and secure traffic between the security module and the RADIUS/TACACS+ server via IPSec tunnel.
Note: Perform this step only if RADIUS/TACAS+ is configured, otherwise proceed.

Step 3: Configure the security module such that any remote connections via Telnet are secured through IPSec.

Step 4: Configure the security module such that only FIPS-approved algorithms are used for IPSec tunnels.

Step 5: Configure the security module such that error messages can only be viewed by Crypto Officer.

Step 6: Disable the TFTP server.

Step 7: Disable HTTP for performing system management in FIPS mode of operation. HTTPS with TLS should always be used for Web-based management.

Step 8: Ensure that installed digital certificates are signed using FIPS approved algorithms.

© Copyright 2021 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.