Cisco Firepower Threat Defense on 4K/9K Cryptographic Module

FIPS 140-2 Non Proprietary Security Policy
Level 1 Validation

Version 1.4

June 8, 2020

1 Introduction

1.1 Purpose

This is the non-proprietary cryptographic module security policy for the Cisco Firepower Threat Defense on 4K/9K Cryptographic Module. The firmware version is 6.4. This security policy describes how this module meets the security requirements of FIPS 140-2 Level 1 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	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	3
4	Finite State Model	1
5	Physical Security	1
6	Operational Environment	N/A
7	Cryptographic Key management	1
8	Electromagnetic Interface/Electromagnetic Compatibility	1
9	Self-Tests	1
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A
	Overall module validation level	**1**

Table 1 Module Validation Level

1.3 References

This document deals with the specification of the security rules listed in Table 1 above, under which the Cisco Firepower Threat Defense on 4K/9K Cryptographic Module will operate, including the rules derived from the requirements of FIPS 140-2, FIPS 140-2 IG and additional rules imposed by Cisco Systems, Inc. More information is available on the module from the following sources:

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

http://www.cisco.com/c/en/us/products/index.html
http://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/roadmap/fxos-roadmap.html

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

The NIST Validated Modules website (http://csrc.nist.gov/groups/STM/cmvp/validation.html) contains contact information for answers to technical or sales-related questions for the module.

1.4 Terminology

In this document, the Cisco Firepower Threat Defense on 4K/9K Cryptographic Module identified is referred to as CM, FTD CM, Module or the System.

1.5 Document Organization

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

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

This document provides an overview of the Cisco Firepower Threat Defense on 4K/9K 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 appliance. 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 Threat Defense Cryptographic Module Overview

Cisco Firepower Threat Defense (FTD) which consolidates the ASA, Firepower and FX-OS providing next-generation firewall services, including stateful firewalling, routing, Next-Generation Intrusion Prevention System (NGIPS), Application Visibility and Control (AVC), URL filtering, and Advanced Malware Protection (AMP). A Threat Defense can be used in single context mode, and in routed or transparent mode to support TLSv1.2, SSHv2, IKEv2 and Cryptographic Cipher Suite B. All using Cisco FIPS Object module for cryptographic support.

The Cisco Firepower Threat Defense (FTD) runs on the Application Blade houses inside Cisco Firepower 4100 and Cisco Firepower 9300 Series. This Security Policy detail the FIPS compliance for the FTD running on the following platforms.

Figure 1 Firepower 4100 series

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

Cisco Firepower 4100 Series Security Appliances

- Cisco Firepower 4110 Security Appliance (FPR4110)
- Cisco Firepower 4115 Security Appliance (FPR4115)
- Cisco Firepower 4120 Security Appliance (FPR4120)
- Cisco Firepower 4125 Security Appliance (FPR4125)
- Cisco Firepower 4140 Security Appliance (FPR4140)
- Cisco Firepower 4145 Security Appliance (FPR4145)
- Cisco Firepower 4150 Security Appliance (FPR4150)

Figure 2 Firepower 9300 Series

The 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.

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

- Cisco Firepower 9300 with SM-24 (FPR9K-SM-24)
- Cisco Firepower 9300 with SM-36 (FPR9K-SM-36)
- Cisco Firepower 9300 with SM-40 (FPR9K-SM-40)
- Cisco Firepower 9300 with SM-44 (FPR9K-SM-44)
- Cisco Firepower 9300 with SM-48 (FPR9K-SM-48)
- Cisco Firepower 9300 with SM-56 (FPR9K-SM-56)

2.1 Cryptographic Module Characteristics

The Cisco FTD CM is an integrated network security module housed in a single application blade architecture (Figure 3), which is designed to integrate into the FPR4100 or FPR9300 Series Appliances High Performance Security Module. Once integrated, the module provides enhanced security, reliability, and performance. Delivering industry-leading firewall data rates, this module provides exceptional scalability to meet the needs of today's dynamic organizations.

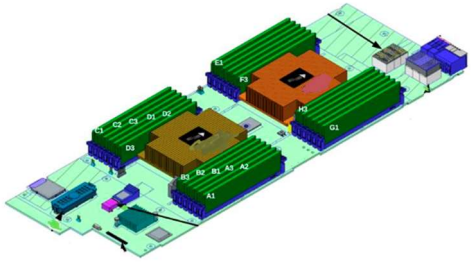

Figure 3 Cisco Firepower Threat Defense (FTD) Application Blade

2.2 Cryptographic Boundary

The module is a multi-chip embedded hardware crypto module. The cryptographic boundary is defined as the physical perimeter of the application blade running inside the FPR 4300/9300 series chassis unit.

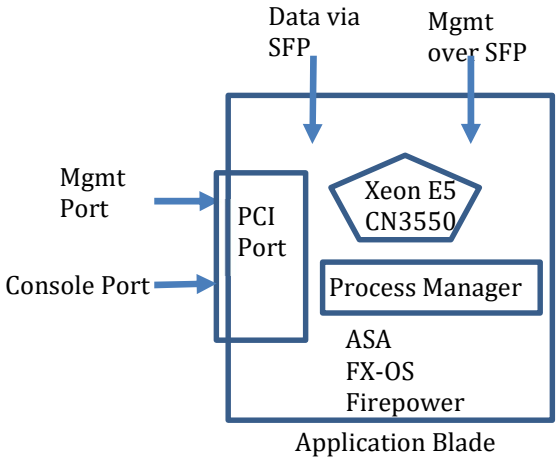

Diagram 1 Block Diagram

2.3 Module Interfaces

The module provides a number of physical and logical interfaces to the device, and the physical interfaces provided by the module are mapped to the following FIPS 140-2 defined logical interfaces: data input, data output, control input, status output, and power. The logical interfaces and their mapping are described in the following table:

FIPS 140-2 Logical Interface	Module Physical Interface
Data Input	SFP Ethernet Ports PCI port
Data Output	SFP Ethernet Ports PCI port
Control Input	SFP Ethernet Ports PCI port
Status Output	SFP Ethernet Ports PCI port LED

Table 2 Hardware/Physical Boundary Interfaces

2.4 Roles, Services, and Authentication

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

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

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

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

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

Additionally, when using RSA based authentication, RSA key pair has modulus size of 2048 bits, thus providing 112 bits of strength, which means an attacker would have a 1 in 2^{112} chance of randomly obtaining the key, which is much stronger than the one in a million chances required by FIPS 140-2. To exceed a one in 100,000 probability of a successful random key guess in one minute, an attacker would have to be capable of approximately 8.65×10^{31} ($2^{112}/60 = 8.65 \times 10^{31}$) attempts per second, which far exceeds the operational capabilities of the module to support.

2.5 User Services

A User enters the system by accessing either Console port, SSHv2 or HTTPS/TLSv1.2. The User role can be authenticated via either Username/Password or RSA based authentication method. The module prompts the User for username and password. If the password is correct, the User is allowed entry to the module management functionality. The other means of accessing the console is via an IPSec 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

Services	Description	Keys and CSPs Access
IPSec VPN	Negotiation and encrypted data transport via IPSec VPN.	Operator password, DRBG entropy input, DRBG Seed, DRBG V, DRBG key, 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 (r, w, d)
SSHv2 Functions	Negotiation and encrypted data transport via SSHv2.	Operator password, DRBG entropy input, DRBG Seed, DRBG V and 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 C, 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

2.6 Crypto Officer Services

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

Services	Description	Keys and CSPs Access
Configure the Security	Define network interfaces and settings, create command aliases, set the protocols the router will support, enable interfaces and network services, set system date and time, change factory default user name/password and load authentication information.	DRBG entropy input, DRBG seed, DRBG V, DRBG key, DRBG C, Diffie-Hellman private key, Diffie-Hellman public key, Diffie-Hellman shared secret, EC Diffie-Hellman private key, EC Diffie-Hellman public key, EC Diffie-Hellman shared secret, SSHv2 private key, SSHv2 public key, SSHv2 integrity key, SSHv2 session key, 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 and IPSec authentication key (r, w, d)
Firmware Initialization	Conduct the firmware initialization.	N/A
Configure External Authentication Server	Configure Client/Server authentication.	RADIUS secret, TACACS+ secret
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,	Operator password, Enable password (r, w, d)

	voltage, packet statistics, review accounting logs, and view physical interface status.	
HTTPS/TLS (TLSv1.2)	Configure HTTPS/TLS parameters, provide entry and output of CSPs.	DRBG entropy input, DRBG seed, DRBG V, DRBG key, DRBG C, ECDSA private key, ECDSA public key, TLS pre-master secret, TLS master secret, TLS encryption keys and TLS integrity key (r, w, d)
IPSec VPN	Configure IPSec VPN parameters, provide entry and output of CSPs.	DRBG entropy input, DRBG seed, DRBG V, DRBG key, DRBG C, 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 and IPSec authentication key (r, w, d)
SSHv2 Function	Configure SSH v2 parameter, provide entry and output of CSPs.	DRBG entropy input, DRBG seed, DRBG V, DRBG key, DRBG C, 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)
Zeroization	Zeroize cryptographic keys/CSPs by running the zeroization methods classified in table 6, Zeroization column.	All CSPs (d)

Table 4 Crypto Officer Services

2.7 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 2.7, 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: HMAC MD5 Symmetric: DES, RC4 Asymmetric: 768-bit/1024-bit RSA (key transport), 1024-bit Diffie-Hellman
TLS	Symmetric: DES, RC4 Asymmetric: 768-bit/1024-bit RSA (key transport), 1024-bit Diffie-Hellman

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

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

[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.

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.

2.8 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.

2.9 Cryptographic Key/CSP Management

The module administers both cryptographic keys and other critical security parameters such as passwords. All keys and CSPs are protected by the password-protection of the Crypto Officer role login, and can be zeroized by the Crypto Officer. Zeroization consists of overwriting the memory that stored the key or refreshing the volatile memory. Keys are both manually and electronically distributed but entered electronically. Persistent keys with manual distribution are used for pre-shared keys whereas protocols such as IKE, TLS and SSH are used for electronic distribution.

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

Name	CSP Type	Size	Description/Generation/Derivation	Storage	Zeroization
DRBG entropy input	SP800-90A CTR_DRBG (AES-256) or HASH_DRBG (SHA-512)	384 bits/512bits	This is the entropy input for SP 800-90A CTR_DRBG and HASH_DRBG, used to construct seed.	DRAM (plaintext)	Power cycle the device
DRBG seed	SP800-90A CTR_DRBG (AES-256) or HASH_DRBG (SHA-512)	384 bits/888 bits	Input to the DRBG that determines the internal state of the DRBG. Generated using DRBG derivation function that includes the entropy input from the entropy source.	DRAM (plaintext)	Power cycle the device
DRBG V	SP800-90A CTR _DRBG (AES-256) or HASH_DRBG (SHA-512)	128 bits/888 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 (using AES-256)	256 bits	Internal critical value used as part of SP 800-90A CTR_DRBG. Established per SP 800-90A CTR_DRBG.	DRAM (plaintext)	Power cycle the device

Name	CSP Type	Size	Description/Generation/Derivation	Storage	Zeroization
DRBG C	SP800-90A HASH_DRBG (SHA-512)	888 bits	Internal critical value used as part of SP 800-90A HASH_DRBG. Established per SP 800-90A HASH_DRBG.	DRAM (plaintext)	Power cycle the device
Diffie-Hellman shared secret	DH	2048 – 4096 bits	The shared secret used in Diffie-Hellman (DH) exchange (as part of SSH, IKE/IPSec, and TLS). Established per the Diffie-Hellman key agreement.	DRAM (plaintext)	Power cycle the device
Diffie-Hellman private key	DH	224-384 bits	The private key used in Diffie-Hellman (DH) exchange (as part of SSH, IKE/IPSec, and TLS). 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 (as part of SSH, IKE/IPSec, and TLS). This key is derived per the Diffie-Hellman key agreement. Note that the public key is a cryptographic key, but not considered a CSP.	DRAM (plaintext)	Power cycle the device
EC Diffie-Hellman shared Secret	ECDH	P-256, P-384, P-521 Curves	The shared secret used in Elliptic Curve Diffie-Hellman (ECDH) exchange. Established per the Elliptic Curve Diffie-Hellman (ECDH) protocol.	DRAM (plaintext)	Power cycle the device
EC Diffie-Hellman private key	ECDH	P-256, P-384, P-521 Curves	Used in establishing the session key for an IPSec session. The private key used in Elliptic Curve Diffie-Hellman (ECDH) exchange. This key is established per the EC Diffie-Hellman key agreement	DRAM (plaintext)	Power cycle the device
EC Diffie-Hellman public key	ECDH	P-256, P-384, P-521 Curves	Used in establishing the session key for an IPSec session. The public key used in Elliptic Curve Diffie-Hellman (ECDH) exchange. This key is established per the EC Diffie-Hellman key agreement. Note that the public key is a cryptographic key, but not considered a CSP.	DRAM (plaintext)	Power cycle the device
skeyid	Keying material	160 bits	A shared secret known only to IKE peers. It was established via key derivation function defined in SP800-135 KDF and it will be used for deriving other keys in IKE protocol implementation.	DRAM (plaintext)	Automatically when IPSec/IKE session is terminated
skeyid_d	Keying material	160 bits	A shared secret known only to IKE peers. It was derived via key derivation function defined in SP800-135 KDF (IKEv2) and it will be used for deriving IKE session authentication key.	DRAM (plaintext)	Automatically when IPSec/IKE session is terminated
SKEYSEED	Keying material	160 bits	A shared secret known only to IKE peers. It was derived via key derivation function defined in SP800-135 KDF (IKEv2) and it will be used for deriving IKE session authentication key.	DRAM (plaintext)	Automatically when IPSec/IKE session is terminated
ISAKMP preshared	Shared Secret	Variable 8 plus characters	The secret used to derive IKE skeyid when using preshared secret authentication. This CSP is entered by the Crypto Officer.	NVRAM (plaintext)	Zeroized by replacing a new secret

Name	CSP Type	Size	Description/Generation/Derivation	Storage	Zeroization
IKE authentication private Key	RSA/ECDSA	RSA (2048 bits) or ECDSA (Curves: P-256/P-384)	RSA/ECDSA private key used in IKE authentication. This key is generated by calling SP800-90A DRBG.	NVRAM (plaintext)	Zeroized by RSA/ECDSA keypair deletion command
IKE authentication public key	RSA/ECDSA	RSA (2048 bits) or ECDSA (Curves: P-256/P-384)	RSA/ECDSA public key used in IKE authentication. The key is derived in compliance with FIPS 186-4 RSA/ECDSA key pair generation method in the module. Note that the public key is a cryptographic key, but not considered a CSP.	NVRAM (plaintext)	Zeroized by RSA/ECDSA keypair deletion command
IKE session encryption key	Triple-DES/AES	192 bits Triple-DES or 128/192/256 bits AES	The IKE session (IKE Phase I) encrypt key. This key is derived via key derivation function defined in SP800-135 KDF (IKEv2).	DRAM (plaintext)	Automatically when IPSec/IKE session is terminated
IKE session authentication key	HMAC-SHA-256/384/512	256-512 bits	The IKE session (IKE Phase I) authentication key. This key is derived via key derivation function defined in SP800-135 KDF (IKEv2).	DRAM (plaintext)	Automatically when IPSec/IKE session is terminated
IPSec encryption key	Triple-DES, AES and AES-GCM	Triple-DES 192 bits or AES 128/192/256 bits	The IPSec (IKE phase II) encryption key. This key is derived via a key derivation function defined in SP800-135 KDF (IKEv2).	DRAM (plaintext)	Automatically when IPSec/IKE session is terminated
IPSec authentication key	HMAC-SHA-256/384/512	256-512 bits	The IPSec (IKE Phase II) authentication key. This key is derived via a key derivation function defined in SP800-135 KDF (IKEv2).	DRAM (plaintext)	Automatically when IPSec/IKE session is terminated
Operator password	Password	8 plus characters	The password of the User role. This CSP is entered by the User.	NVRAM (plaintext)	Overwrite with new password
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)	Overwrite with new secret
TACACS+ secret	Shared Secret	16 characters	The TACACS+ shared secret. Used for TACACS+ Client/Server authentication. This CSP is entered by the Crypto Officer.	NVRAM (plaintext)	Overwrite with new secret
SSHv2 private key	RSA	2048 bits modulus	The SSHv2 private key used in SSHv2 connection. This key is generated by calling SP 800-90A DRBG.	NVRAM (plaintext)	Zeroized by RSA keypair deletion command
SSHv2 public key	RSA	2048 bits modulus	The SSHv2 public key used in SSHv2 connection. This key is derived in compliance with FIPS 186-4 RSA key pair generation method in the module. Note that the public key is a cryptographic key, but not considered a CSP.	NVRAM (plaintext)	Zeroized by RSA keypair deletion command

Name	CSP Type	Size	Description/Generation/Derivation	Storage	Zeroization
SSHv2 integrity key	HMAC-SHA-1	160 bits	Used for SSH connections integrity to assure the traffic integrity. This key is derived via key derivation function defined in SP800-135 KDF (SSH).	DRAM (plaintext)	Automatically when SSH session is terminated
SSHv2 session key	Triple-DES/AES	Triple-DES 192 bits or AES 128/192/256 bits	This is the SSHv2 session key. It is used to encrypt all SSHv2 data traffics traversing between the SSHv2 Client and SSHv2 Server. This key is derived via key derivation function defined in SP800-135 KDF (SSH).	DRAM (plaintext)	Automatically when SSH session is terminated
ECDSA private key	ECDSA	Curves: P-256, 384, 521	Signature generation used in IKE/IPSec and TLS. This key is generated by calling SP 800-90A DRBG.	NVRAM (plaintext)	Zeroized by ECDSA keypair deletion command
ECDSA public key	ECDSA	Curves: P-256, 384, 521	Signature verification used in IKE/IPSec and TLS. This key is derived in compliance with FIPS 186-4 ECDSA key pair generation method in the module. Note that the public key is a cryptographic key, but not considered a CSP.	NVRAM (plaintext)	Zeroized by ECDSA keypair deletion command
TLS RSA private key	RSA	2048 bits	Identity certificates for the security appliance itself and also used in TLS negotiations. 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 negotiations. This key is derived in compliance with FIPS 186-4 RSA key pair generation method in the module. Note that the public key is a cryptographic key, but not considered a CSP.	NVRAM (plaintext)	Zeroized by RSA keypair deletion command
TLS pre-master secret	keying material	At least eight characters	Keying material used to derive TLS master secret during the TLS protocol implementation. This key is entered into the module in cipher text form, encrypted by RSA public key.	DRAM (plaintext)	Automatically when TLS session is terminated
TLS master secret	keying material	48 Bytes	Keying material used to derive other HTTPS/TLS keys. This key was derived from TLS pre-master secret during the TLS session establishment.	DRAM (plaintext)	Automatically when TLS session is terminated
TLS encryption keys	Triple-DES/AES/AES-GCM	Triple-DES 192 bits or AES 128/192/256 bits	Used in HTTPS/TLS connections to protect the session traffic. This key was derived in the module.	DRAM (plaintext)	Automatically when TLS session is terminated
TLS Integrity Key	HMAC-SHA 256/384	256-384 bits	Used for TLS integrity to assure the traffic integrity. This key was derived in the module.	DRAM (plaintext)	Automatically when TLS session is terminated

Table 6 Cryptographic Keys and CSPs

2.10 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:

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

Table 7 Approved Cryptographic Algorithms and Associated Certificate Numbers

Notes:

- There are some algorithm modes that were tested but not implemented by the module. Only the algorithms, modes, and key sizes that are implemented by the module are shown in this table.
- The module's AES-GCM implementation conforms to IG A.5 scenario #1 following RFC 5288 for TLS and RFC 7296 for IPSec/IKEv2. The module is compatible with TLSv1.2 and provides support for the acceptable GCM cipher suites from SP 800-52 Rev1, Section 3.3.1. The operations of one of the two parties involved in the TLS key establishment scheme were performed entirely within the cryptographic boundary of the module being validated. The counter portion of the IV is set by the module within its cryptographic boundary. When the IV exhausts the maximum number of possible values for a given session key, the first party, client or server, to encounter this condition will trigger a handshake to establish a new encryption key. In case the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established. The module uses RFC 7296 compliant IKEv2 to establish the shared secret SKEYSEED from which the AES GCM encryption keys are derived. The operations of one of the two parties involved in the IKE key establishment scheme shall be performed entirely within the cryptographic boundary of the module being validated. When the IV exhausts the maximum number of possible values for a given session key, the first party, client or server, to encounter this condition will trigger a handshake to establish a new encryption key. In case the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established.
- No parts of the SSH, TLS and IPSec protocols, other than the KDFs, have been tested by the CAVP and CMVP.
- Each of TLS, SSH and IPSec protocols governs the generation of the respective Triple-DES keys. Refer to RFC 5246 (TLS), RFC 4253 (SSH) and RFC 6071 (IPSec) for details relevant to the generation of the individual Triple-DES encryption keys. The user is responsible for ensuring the module limits the number of encryptions with the same key to 2^{20}.

- In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation as per scenario 1 of section 5 in SP800-133. The resulting generated seed used in the asymmetric key generation is the unmodified output from SP800-90A DRBG.

Non-FIPS Approved Algorithms Allowed in FIPS Mode

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

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

Non-Approved Cryptographic Algorithms

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

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

2.11 Self-Tests

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

Self-tests performed

- Cisco Security Crypto POSTs (Firmware)
  - AES CBC Encrypt/Decrypt KATs
  - AES GCM KAT
  - DRBG KAT (Note: DRBG Health Tests as specified in SP800-90A Section 11.3 are performed)
  - Firmware Integrity Test (SHA-512)
  - 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
- On-board Chip POSTs (Hardware)
    - AES CBC Encrypt/Decrypt KATs
    - DRBG KAT (Note: DRBG Health Tests as specified in SP800-90A Section 11.3 are performed)
    - HMAC-SHA-1 KAT
    - HMAC-SHA-256 KAT
    - HMAC-SHA-384 KAT
    - HMAC-SHA-512 KAT
    - SHA-1 KAT
    - Triple-DES CBC Encrypt/Decrypt KATs
- Conditional tests - Cisco Security Crypto (Firmware)
    - RSA PWCT
    - ECDSA PWCT
    - Conditional Bypass Test
    - CRNGT for SP800-90A DRBG
    - CRNGT for NDRNG
- Conditional tests - On-board Chip (Hardware)
    - CRNGT for SP800-90A DRBG

The security appliance 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 appliance 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.

3 Secure Operation

The module meets all the Level 1 requirements for FIPS 140-2. The module is shipped only to authorized operators by the vendor, and modules are shipped in Cisco boxes with Cisco adhesive, so if tampered with the recipient will notice. Follow the setting instructions provided below to place the module in FIPS-approved mode. Operating this module without maintaining the following settings will remove the module from the FIPS approved mode of operation.

3.1 Crypto Officer Guidance - System Initialization

The module was validated with FTD version 6.4. It is the only allowed firmware version for FIPS-approved mode of operation. The Crypto Officer must configure and enforce the following initialization steps:

Step 1: Power on the system.

Step 2: When prompted, log in with the username **admin** and the password **cisco123**.
you have chosen to setup a new Security Appliance.
Continue? (yes/no): **y**

Enter the password for "admin": **[enter new password]**
Confirm the password for "admin": **[enter new password again]**

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

Step 4: Choose the option of "enable FIPS Mode" from the HTTPS/TLSv1.2 connection or type in "enable fips" from the Console connection to enable the FIPS mode.

Step 5: Configure the module to use SSHv2. Note that all operators must still authenticate after remote access is granted. The CO shall only use FIPS approved/Allowed cryptographic algorithms listed above for SSHv2 configuration.

Step 6: 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 7: Configure the module such that any remote connections via Telnet are secured through IPSec.

Step 8: Configure the module such that only FIPS-approved algorithms are used for IPSec tunnels.

Step 9: Configure the module such that error messages can only be viewed by Crypto Officer.

Step 10: Disable the TFTP server.

Step 11: Disable HTTP for performing system management in FIPS mode of operation. HTTPS with TLS should always be used for Web-based management. The CO shall only use FIPS approved/Allowed cryptographic algorithms listed above for TLS configuration.

Step 12: Ensure that installed digital certificates are signed using FIPS approved algorithms.

Step 13: Reboot the module.