Cisco Firepower Threat Defense Virtual (FTDv) Cryptographic Module

FIPS 140-2 Non Proprietary Security Policy
Level 1 Validation

Version 1.4

October 26, 2020

Table of Contents

1 Introduction

1.1 Purpose

This is the non-proprietary Security Policy for the Cisco Firepower Threat Defense Virtual (FTDv) Cryptographic Module. The software 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 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	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	3
4	Finite State Model	1
5	Physical Security	N/A
6	Operational Environment	1
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 only with the operations and capabilities of the Cisco Firepower Threat Defense Virtual (FTDv) Cryptographic Module outlined in Table 1 above as it relates to the technical terms of a FIPS 140-2 cryptographic module. Additional information can be found at the following Cisco sites:

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

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

The NIST Validated Modules website (https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules) contains contact information for answers to technical or sales-related questions for the module.

1.4 Terminology

In this document, the Cisco Firepower Threat Defense Virtual (FTDv) Cryptographic Module is referred to as FTDv 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 module identified in section 1.1 above and explains the secure layout, configuration and operation of the module. This introduction section is followed by Section 2, which details the general features and functionality of the module. Section 3 specifically addresses the required configuration for the FIPS-mode of operation.

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

2 Cisco Firepower Threat Defense Virtual (FTDv) Cryptographic Module

The module is a virtualized version of the Firepower Threat Defense module which provides balanced security effectiveness with productivity. This solution offers the combination of the industry's most deployed stateful firewall with a comprehensive range of next-generation network security services, intrusion prevention system (IPS), content security, secure unified communications, TLSv1.2, SSHv2, IKEv2, and Cryptographic Cipher Suite B, all running in a virtual environment.

2.1 Cryptographic Module Physical Characteristics

The module is an integrated network security software module, which is designed to integrate onto many different servers with various hypervisors. 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.

For the purposes of this validation, the module was tested in the lab on the following servers:

OS	Hypervisor	Hardware	Processor
FXOS version 2	VMware ESXi 6.0	Cisco UCS C220 M5	Intel Xeon Silver 4110
FXOS version 2	VMware ESXi 6.5	Cisco UCS C220 M5	Intel Xeon Silver 4110
FXOS version 2	NFVIS 3	ENCS 5412	Intel Xeon D-1528

Table 2 Testing Configuration

Cisco does not restrict the use of any hypervisor. Along with supporting ESXi and NFVIS listed above Cisco also supports the use of KVM’s and AWS (cloud service) on Cisco UCS and NFVIS on ENCS platforms.

Additionally, the CMVP makes no statement as to the correct operation of the module or the security strengths of the generated keys when ported to an operational environment which is not listed on the validation certificate.

2.2 Cryptographic Boundary

The module is defined as a multi-chip standalone software module (inside red dashed area), with the physical boundary being defined as the hard case enclosure around which everything runs. Then the cryptographic boundary is the FTD virtual module, including the Guest OS/FTD, API and FOM. Please see Diagram 1 below for the details.

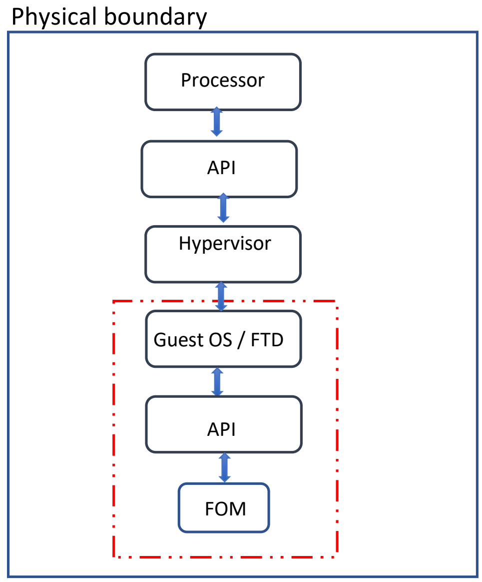

Diagram 1 Block Diagram

Note: Block Diagram above comprises the following components

- Processor: Chip handling all processes.
- API: Application programming interface between hypervisor and processor
- Hypervisor: VMWare ESXi 6.0, 6.5 or NFVIS 3
- Guest OS/FTD: FTD module running on FXOS version 2 (Guest OS)
- API: Application programming interface between the module and FOM library
- FOM: Cisco FIPS Object Module (a Cisco proprietary crypto library)

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:

Physical Port/Interface	FTD Virtual	FIPS 140-2 Interface
Host System Ethernet (10/100/1000) Ports; Host System Serial Port	Virtual Ethernet Ports, Virtual Serial Port	**Data Input Interface**
Host System Ethernet (10/100/1000) Ports; Host System Serial Port	Virtual Ethernet Ports, Virtual Serial Port	**Data Output Interface**
Host System Ethernet (10/100/1000) Ports; Host System Serial Port	Virtual Ethernet Ports, Virtual Serial Port	**Control Input Interface**
Host System Ethernet (10/100/1000) Ports; Host System Serial Port	Virtual Ethernet Ports, Virtual Serial Port	**Status Output Interface**

Table 3 Hardware/Physical Boundary Interfaces

2.4 Roles, Services, and Authentication

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

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

Authentication is identity-based. Each user is authenticated by the module upon initial access to the module. As required by FIPS 140-2, there are two roles in the security appliances that operators may assume: Crypto Officer and User. Both are authenticated on access to the module. The administrator of the security appliances assumes the Crypto Officer role in order to configure and maintain the module using Crypto Officer services, while the Users exercise only the basic User services.

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 8.65x10^31 (2^112 /60 = 8.65 x 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 either Serial Console, SSH, or HTTPS/TLS. The User role can be authenticated via either User Name/Password or RSA based authentication method. The module prompts the User for username and password. If the password is correct, the User is allowed entry to the module management functionality. The other means of accessing the console is via an IPSec/IKEv2 session. This session is authenticated using 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 state of interfaces and protocols, version of software currently running.	Operator password (r)
Terminal Functions	Adjust the terminal session (e.g., lock the terminal, adjust flow control).	Operator password (r)
Directory Services	Display directory of files kept in flash memory.	Operator password (r)
Self-Tests	Execute the FIPS 140 start-up tests on demand.	N/A
IPsec VPN Functions	Negotiation and encrypted data transport via IPSec VPN.	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, DRBG entropy input, DRBG seed, DRBG V and DRBG key (r, w, d)
SSHv2 Functions	Negotiation and encrypted data transport via SSH.	DH private key, DH public key, DH shared secret, ECDH private key, ECDH public key, ECDH shared secret, SSHv2 RSA private key, SSHv2 RSA public key, SSHv2 session key, SSHv2 integrity key DRBG seed, DRBG entropy input, DRBG V and DRBG key (r, w, d)
HTTPS/TLS (TLSv1.2) Functions	Negotiation and encrypted data transport via HTTPS.	TLS RSA private keys, TLS RSA public keys, TLS pre-master secret, TLS master secret, TLS encryption key TLS integrity key, DRBG entropy input, DRBG seed, DRBG V, DRBG key (r, w, d)

Table 4 User Services

2.6 Crypto Officer Services

The Crypto Officer 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 can be authenticated via either Password or RSA based authentication method. The other means of accessing the console is via an IPSec/IKEv2 session. This session is authenticated using RSA digital signature authentication mechanism. The services available to the Crypto Officer 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, 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 keys, TLS RSA public keys, 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)
Software Initialization	Conduct the software initialization.	Integrity test key (r, w, d)
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, Crypto Officer (CO) password (r)
View Status Functions	View the module's configuration, routing tables, active sessions health, temperature, memory status, voltage, packet statistics, review accounting logs, and view physical interface status.	Operator password, Crypto Officer (CO) password (r)

HTTPS/TLS (TLSv1.2) Functions	Configure HTTPS/TLSv1.2 parameters, provide entry and output of CSPs.	TLS RSA private keys, TLS RSA public keys, TLS pre-master secret, TLS master secret, TLS encryption key, TLS integrity key, DRBG entropy input, DRBG seed, DRBG V and DRBG key (r, w, d)
IPsec VPN Functions	Configure IPsec VPN parameters, provide entry and output of CSPs.	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)
Configure Encryption/Bypass Service	Configure Encryption or Bypass service	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 SSHv2 parameter, provide entry and output of CSPs.	DH private key, DH public key, DH shared secret, ECDH private key, ECDH public key, ECDH shared secret, SSHv2 RSA private key, SSHv2 RSA public key, SSHv2 session key, SSHv2 integrity key, DRBG entropy input, DRBG seed, DRBG V and DRBG key (r, w, d)
Self-Tests	Execute the FIPS 140 start-up tests on demand.	N/A
User Services	The Crypto Officer has access to all User services.	Operator password (r, w, d)
Zeroization	Zeroize cryptographic keys/CSPs by running the zeroization methods classified in table 6, Zeroization column.	All CSPs (d)

Table 5 Crypto Officer Services

More services related information, including the service inputs, corresponding service outputs, and the authorized role or roles in which the service can be performed are available at Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.4.0, Updated: June 9, 2020. https://www.cisco.com/c/en/us/td/docs/security/firepower/640/fdm/fptd-fdm-config-guide-640.html.

2.7 Non-FIPS mode Services

The cryptographic module supports both FIPS mode and non-FIPS mode of operations. By selecting non-Approved services listed in Section 2.7, the Crypto Officer is placing the module into a non-FIPS mode of operation. The Keys/CSPs used in FIPS mode cannot be used in in non-approved FIPS mode, and vice versa. Prior to using any of the Non-Approved services in Table 6, the Crypto Officer must zeroize all CSPs used in FIPS mode of operation. Neither the User nor the Crypto Officer are allowed to operate any of these services in Table 5 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), ECDSA, Diffie-Hellman

[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.

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

Table 6 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.

Likewise, the complete services supported by the module are available at Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.4.0, Updated: June 9, 2020. https://www.cisco.com/c/en/us/td/docs/security/firepower/640/fdm/fptd-fdm-config-guide-640.html.

2.8 Unauthenticated Services

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

2.9 Cryptographic Key/CSP Management

The module administers both cryptographic keys and CSPs (critical security parameters). The Crypto Officer needs to be authenticated to manage the cryptographic keys and CSPs. The zeroization of cryptographic keys or CSPs consists of overwriting the memory that stored the key or refreshing the volatile memory. Keys are electronically distributed and electronically entered.

All pre-shared secrets are associated with the CO role that created the secrets. The Crypto Officer needs to be authenticated to manage the cryptographic keys and CSPs. All Diffie-Hellman (DH)/EC Diffie-Hellman (ECDH) keying materials agreed upon for individual tunnels are directly associated with that specific tunnel. 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/CSPs are associated with the CO role or User role that created them

The module is a software module that contains an approved DRBG that is seeded exclusively from one known entropy source located within the operational environment inside the module's physical boundary but the outside the logical boundary, which is complaint with FIPS 140-2 IG 7.14 #1 (b). The module provides at least 256 bits entropy to instantiate the DRBG.

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
DRBG entropy input	SP800-90A CTR_DRBG (using AES-256)	384-bits	This is the entropy for SP 800-90A CTR_DRBG, used to construct the seed.	DRAM (plaintext)	Power cycle the device
DRBG seed	SP800-90A CTR_DRBG (using AES-256)	384-bits	Input to the DRBG that determines the internal state of the DRBG. Generated using DRBG derivation function that includes the entropy input from the entropy source.	DRAM (plaintext)	Power cycle the device
DRBG V	SP800-90A CTR_DRBG	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	DRAM (plaintext)	Power cycle the device

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
			instantiation and then subsequently updated using the DRBG update function.		
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 (DH) exchange. Established per the Diffie-Hellman key agreement.	DRAM (plaintext)	Power cycle the device
Diffie-Hellman private key	DH	224-384 bits	The private key used in Diffie-Hellman (DH) exchange. This key is generated by calling SP800-90A DRBG.	DRAM (plaintext)	Power cycle the device
Diffie Hellman public key	DH	2048 - 4096 bits	The public key used in Diffie-Hellman (DH) exchange. This key is derived per the Diffie-Hellman key agreement. 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	EC DH	Curves: P-256, P-384, P-521	The shared secret used in Elliptic Curve Diffie-Hellman (ECDH) exchange. Established per the EC Diffie-Hellman (ECDH) protocol.	DRAM (plaintext)	Power cycle the device
EC Diffie-Hellman private key	EC DH	Curves: P-256, P-384, P-521	The private key used in EC Diffie-Hellman (DH) exchange. This key is generated by calling SP800-90A DRBG.	DRAM (plaintext)	Power cycle the device
EC Diffie Hellman public key	EC DH	Curves: P-256, P-384, P-521	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)	Power cycle the device
skeyid_d	Keying material	160 bits	Keying material 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	Keying material 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

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
IKE session encryption key	Triple-DES, AES and AES-GCM	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)	Power cycle the device
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)	Power cycle the device
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/ECDSA	RSA (2048 bits) or ECDSA (Curves: P-256, P384, 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, P384, P-521)	RSA/ECDSA public key used in IKE authentication. This 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
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)	Power cycle the device
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)	Power cycle the device
Crypto Officer (CO) password	Password	8 plus characters	The password of the CO role. This CSP is entered by the Crypto Officer.	NVRAM (plaintext)	Erase the password
Operator password	Password	8 plus characters	The password of the User role. This CSP is entered by the User.	NVRAM (plaintext)	Erase the password
RADIUS secret	Shared Secret	16 characters	The RADIUS shared secret. Used for RADIUS Client/Server authentication. This CSP is entered by the Crypto Officer.	NVRAM (plaintext)	Erase the secret
TACACS+ secret	Shared Secret	16 characters	The TACACS+ shared secret. Used for TACACS+ Client/Server authentication. This CSP is entered by the Crypto Officer.	NVRAM (plaintext)	Erase the secret
SSHv2 private key	RSA	2048 bits modulus	The SSHv2 private key used in SSHv2 connection. This key is generated by calling SP 800-90A DRBG.	NVRAM (plaintext)	Zeroized by RSA keypair deletion command

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
SSHv2 public key	RSA	2048 bits modulus	The SSHv2 public key used in SSHv2 connection. This key is derived in compliance with FIPS 186-4 RSA key pair generation method in the module. Note that the public key is a cryptographic key, but not considered a CSP	NVRAM (plaintext)	Zeroized by RSA keypair deletion command
SSHv2 session key	Triple-DES/AES	192 bits Triple-DES or 128/192/256 bits AES	This is the SSHv2 session key. It is used to encrypt all SSHv2 data traffics traversing between the SSHv2 Client and SSHv2 Server. This key is derived via key derivation function defined in SP800-135 KDF (SSH).	DRAM (plaintext)	Power cycle the device
SSHv2 integrity key	HMAC-SHA-1	160 bits	Used for SSH connections integrity to assure the traffic integrity. This key was derived in the module.	DRAM (plaintext)	Automatically when SSH session is terminated
ECDSA private key	ECDSA	Curves: P-256, P384, P-521	Key pair generation, signature generation/Verification. 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, P384, P-521	Key pair generation, signature generation/Verification. 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 keys	RSA	2048 bits	Identity certificates for the security appliance itself and also used in IPSec, TLSv1.2, and SSH negotiations. This key was generated by calling FIPS approved DRBG.	NVRAM (plaintext)	Zeroized by RSA keypair deletion command
TLS RSA public keys	RSA	2048 bits	Identity certificates for the security appliance itself and also used in IPSec, TLSv1.2, and SSH negotiation. 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 TLSv1.2 master key during the TLSv1.2 session establishment. This key entered into the module in cipher text form, encrypted by RSA public key.	DRAM (plaintext)	Automatically when TLS session is terminated.

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
TLS master secret	keying material	48 Bytes	Keying material used to derive other TLSv1.2 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 and AES-GCM	Triple-DES 192 bits or AES 128/192/256 bits	TLSv1.2 encryption keys. Used to protect the data traversing between the TLSv1.2 Client and Server. This key is derived via key derivation function defined in SP800-135 KDF (TLSv1.2).	DRAM (plaintext)	Automatically when TLS session is terminated
TLS integrity key	HMAC-SHA-256/384	256-384 bits	TLSv1.2 integrity key. Used to ensure the data integrity traversing between the TLSv1.2 Client and Server. This key is derived via key derivation function defined in SP800-135 KDF (TLSv1.2).	DRAM (plaintext)	Automatically when TLS session is terminated
Integrity test key	RSA	2048 bits	A hard coded key used for software power-up integrity verification.	Hard coded for software integrity testing	Uninstall the module

Table 7 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	Algorithm Implementation
	Cisco Security Crypto Virtual
AES (128/192/256 CBC, GCM)	5008
Triple-DES (CBC, 3-key)	2584
SHS (SHA-1/256/384/512)	4074
HMAC (SHA-1/256/384/512)	3329
RSA (KeyGen; PKCS1_V1_5; KeyGen, SigGen, SigVer; 2048 bits)	2703
ECDSA (KeyGen, SigGen, SigVer; P-256, P-384, P-521)	1277
DRBG (AES-256_CTR)	1828
CVL Component (TLSv1.2, SSHv2 and IKEv2)	1561
CKG (vendor affirmed)	

Table 8 Approved Cryptographic Algorithms and Associated Certificate Number

Notes:

- There are some algorithm modes that were tested but not implemented by the module. Only the algorithms, modes, and key sizes that are implemented by the module are shown in this table.
- The module's AES-GCM implementation conforms to IG A.5 scenario #1 following RFC 5288 for TLS. 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.

- 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 and IPSec protocols, other than the KDFs, 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 per scenario 1 of section 5 in SP800-133. The resulting generated seed used in the asymmetric key generation are the unmodified output from SP800-90A DRBG.

Non-FIPS Approved Algorithms Allowed in FIPS Mode

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

- Diffie-Hellman (CVL Cert. #1561, key agreement; key establishment methodology provides between 112 and 150 bits of encryption strength)
- EC Diffie-Hellman (CVL Cert. #1561, key agreement; key establishment methodology provides between 128 and 256 bits of encryption strength)
- RSA (key wrapping; key establishment methodology provides 112 of encryption strength)
- NDRNG

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

2.11 Self-Tests

The module includes 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

- POST Tests
  - AES-CBC Known Answer Tests (Separate encrypt and decrypt)
  - AES-GCM Known Answer Tests (Separate encrypt and decrypt)
  - DRBG Known Answer Test (Note: DRBG Health Tests as specified in SP800-90A Section 11.3 are performed)
  - ECDSA (Sign and Verify) Power on Self-Test
  - HMAC (SHA-1/256/384/512) Known Answer Tests
  - RSA Known Answer Tests (Separate KAT for signing; Separate KAT for verification)
  - SHA-1 Known Answer Test
  - Software Integrity Test (RSA 2048 bits with SHA-512)
  - Triple-DES-CBC Known Answer Tests (Separate encrypt and decrypt)
- Conditional Tests
  - RSA PWCT (Pairwise Consistency Test)
  - ECDSA PWCT
  - Conditional Bypass Test
  - CRNGT for SP800-90A DRBG
  - CRNGT for NDRNG

Note: DRBGs will not be available should the NDRNG become unavailable. This will in turn make the associated security service/CSP outlined above in Table 6 non-available.

The module performs all power-on self-tests automatically at boot 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 Virtual LAN's interfaces; this prevents the module from passing any data during a power-on self-test failure. In the unlikely event that a power-on or conditional self-test fails, an error message is displayed on the console followed by a module 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 the module is 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

This module was validated with FTDv version 6.4 (Software Images: Cisco_Firepower_Threat_Defense_Virtual-6.4.0-102.tar with Cisco_FTD_Patch-6.4.0.1-17.sh.REL.tar). Those are the only allowable software images for the current FIPS-approved mode of operation. The Crypto Officer must configure and enforce the following initialization steps:

1. Once the unit is powered up and ready you will see a login prompt, login with the default username and password which is admin/Admin123

2. When the Firepower Threat Defense system boots, a setup wizard prompts you for the New CO password[1], configurations, accept EULA, System Name, DNS setup, etc. Please note that the 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 cases, 26 lower cases, 10 numbers and 32 special characters.

3. Review the Setup wizard settings. Defaults or previously entered values appear in brackets. To accept previously entered values, press **Enter**.

4. Complete the system configuration as prompted.

5. The VMware console may display messages as your settings are implemented. When finished, the device reminds you to register this device to a Cisco Firepower Management Center, and displays the CLI prompt.

6. Verify the setup was successful when the console returns to the firepower # prompt. Note: To successfully register the Firepower Threat Defense Virtual with the Cisco Licensing Authority, the Firepower Threat Defense Virtual requires Internet access.

7. Log into FTDv SSH and enter show network. To examine what has been set-up

8. Register the module into Firepower Management Center (FMC) for the further configuration. More information about the module registration into FMC and detailed configuration information can be found out in Firepower Management Center Configuration Guide. Version 6.4, Updated: September 23, 2020. https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64.html.

9. System >Licenses>Smart Licenses, add and verify licenses.

10. Install Triple-DES/AES SMART license to use Triple-DES and AES (for data traffic and SSH).

    Note: 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 CO is responsible for ensuring the module limits the number of encryptions with the same key to 2^20. Please refer to Firepower Management Center Configuration Guide. Version 6.4, Updated: September 23, 2020 for more configuration information. https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64.html

11. On FMC, go to Device >> Platform setting associated to the FTD IP. Then create and select CC option and save. This sets FIPS mode.

12. If using a RADIUS/TACACS+ server for authentication, the CO shall configure a secure tunnel (for example, IPSec/IKEv1.2, TLSv1.2, etc.) to secure traffic between the module and the RADIUS/TACACS+ server. The RADIUS shared secret or TACACS+ shared secret must be at least 8 characters long.

13. Reboot the module.