Cisco Firepower Threat Defense Virtual (FTDv) Cryptographic Module

FIPS 140-2 Non Proprietary Security Policy
Level 1 Validation

Version 1.1

December 13, 2018

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 6.2. 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	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 (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 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 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 5.5	Cisco C220 M4	Intel Xeon E5
FXOS version 2	VMware ESXi 6.0	Cisco C220 M4	Intel Xeon E5

Table 2 Testing Configuration

The following Cisco platforms are Vendor affirmed:

UCSB-B200-M4
UCSB-C220-M4S
UCSB-C240-M4SX
UCSB-C240-M4L
UCSB-C460-M4
UCS-EN120S-M2
UCS-EN120E-208
USC-E140S-M2
UCS-E180D-M2
UCS-E160S-M3
UCSB-B200-M5
UCSC-C220-M5
UCSC-C240-M5
UCSC-C480-M5
ENCS-5406
ENCS-5408
ENCS-5412

The following Hypervisors are Vendor affirmed:

ESXi 5.0
ESXi 5.5
ESXi 6.0
NFVIS

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 (red dash box), while the physical boundary is defined as the hard case enclosure around the Server on which everything runs. Then the logical boundary is the FTD virtual module, hypervisor, API and processor.

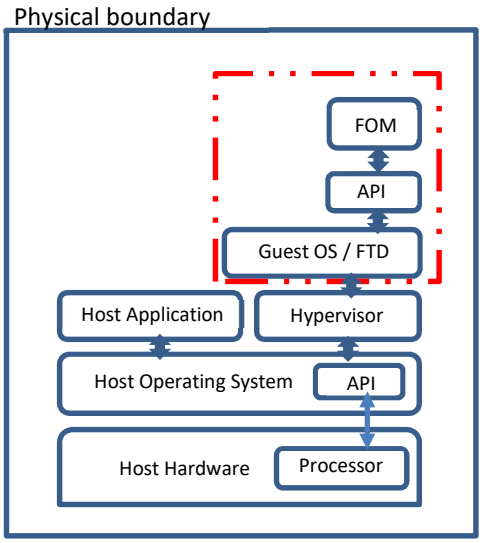

Diagram 1 Block Diagram

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:

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

Table 2 Hardware/Physical Boundary Interfaces

2.4 Roles and Services

The appliances 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 User role. The module upon initial access to the module authenticates both of these roles. The module also supports RADIUS and TACACS+ as another

means of authentication, allowing the storage of usernames and passwords on an external server as opposed to using the module's internal database for storage.

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

Additionally, when using RSA based authentication, RSA key pair has modulus size of 2048 bits, thus providing 112 bits of strength. Assuming the low end of that range, an attacker would have a 1 in 2^{112} chance of randomly obtaining the key, which is much stronger than the one in a million chance required by FIPS 140-2. To exceed a one in 100,000 probability of a successful random key guess in one minute, an attacker would have to be capable of approximately $8.65x10^{31}$ 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 SSHv2 or HTTPS/TLSv1.2. 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 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 state of interfaces and protocols, version of IOS currently running.	Operator password (r, w, d)
Terminal Functions	Adjust the terminal session (e.g., lock the terminal, adjust flow control).	Operator password (r, w, d)
Directory Services	Display directory of files kept in flash memory.	Operator password (r, w, d)
Self-Tests	Execute the FIPS 140 start-up tests on demand.	N/A
IPsec VPN	Negotiation and encrypted data transport via IPSec VPN.	Operator password, skeyid, skeyid_d, SKEYSEED, IKE session encrypt key, IKE session authentication key, ISAKMP preshared, IKE authentication private key, IKE authentication public key, IPsec encryption key, IPsec authentication key, DRBG entropy input, DRBG seed, DRBG V and DRBG key (r, w, d)
SSHv2 Functions	Negotiation and encrypted data transport via SSH.	Operator password, SSHv2 private key, SSHv2 public key, SSHv2 session key, SSHv2 integrity key, DRBG entropy input, DRBG Seed, DRBG V and DRBG Key (r, w, d)
HTTPS Functions (TLSv1.2)	Negotiation and encrypted data transport via HTTPS.	Operator password, 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, DRBG entropy input, DRBG seed, DRBG V and DRBG key (r, w, d)

Table 3 User Services

2.6 Crypto Officer Services

A Crypto Officer (CO) enters the system by accessing the console port with a terminal program, SSHv2 or TLSv1.2 session to a virtual LAN port or the virtual 10/100/1000 management Ethernet port. The CO role can be authenticated via either CO role User Name/Password or RSA based authentication method. A Crypto Officer may assign permission to access the Crypto Officer role to additional accounts, thereby creating additional Crypto Officers.

The Crypto Officer role is responsible for the configuration of the module. The services available to the Crypto Officer role accessing the CSPs, the type of access – read (r), write (w) and zeroized/delete (d) – and which role accesses the CSPs are listed below:

Services	Description	Keys and CSPs Access
Configure the Security	Define network interfaces and settings, create command aliases, set the protocols the 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 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)
Software Installation	Software installation.	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, Enable password (r, w, d)
View Status Functions	View the router configuration, routing tables, active sessions health, temperature, memory status, voltage, packet statistics, review accounting logs, and view physical interface status.	Operator password, Enable password (r, w, d)
TLS VPN (TLSv1.2) Functions	Configure SSL VPN parameters, provide entry and output of CSPs.	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, DRBG entropy input, DRBG seed, DRBG V and DRBG key (r, w, d)
IPsec VPN	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)
SSH v2 Functions	Configure SSH v2 parameter, provide entry and output of CSPs.	SSHv2 Private Key, SSHv2 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 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: MD5 Symmetric: DES, RC4 Asymmetric: RSA (key transport), ECDSA, 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.

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 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

[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.

associates the key with the correct entity. All other keys/CSPs are associated with the CO role or User role that created 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	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 (using AE-256)	128-bits	The DRBG V is one of the critical values of the internal state upon which the security of this DRBG mechanism depends. Generated first during DRBG instantiation and then subsequently updated using the DRBG update function.	DRAM (plaintext)	Power cycle the device
DRBG key	SP800-90A CTR_DRBG (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
Diffie-Hellman Shared Secret	DH	2048 - 4096 bits	The shared secret used in Diffie-Hellman (DH) exchange. Established per the Diffie-Hellman key agreement.	DRAM (plaintext)	Power cycle the device
Diffie-Hellman private key	DH	224-384 bits	The private key used in Diffie-Hellman (DH) exchange. This key is generated by calling SP800-90A DRBG.	DRAM (plaintext)	Power cycle the device
Diffie Hellman public key	DH	2048 - 4096 bits	The public key used in Diffie-Hellman (DH) exchange. This key is derived per the Diffie-Hellman key agreement.	DRAM (plaintext)	Power cycle the device
EC Diffie-Hellman Shared Secret	EC DH	Curves: P-256, P-384, P-521	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	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.	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

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
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
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	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/P-384/512)	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-384/512)	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	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
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

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
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	2048bits modulus	The SSHv2 public key used in SSHv2 connection. This key is derived in compliance with FIPS 186-4 RSA key pair generation method in the module	NVRAM (plaintext)	Zeroized by RSA keypair deletion command
SSHv2 session key	Triple-DES/AES	192 bits Triple-DES or 128/192/256 bits AES	This is the SSHv2 session key. It is used to encrypt all SSHv2 data traffics traversing between the SSHv2 Client and SSHv2 Server. This key is derived via key derivation function defined in SP800-135 KDF (SSH).	DRAM (plaintext)	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-256,384,521	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-256,384,521	Key pair generation, signature generation/Verification. This key is derived in compliance with FIPS 186-4 ECDSA key pair generation method in the module.	NVRAM (plaintext)	Zeroized by ECDSA keypair deletion command
Enable secret	Shared Secret	At least eight characters	The obfuscated password of the CO role. However, the algorithm used to obfuscate this password is not FIPS approved. Therefore, this password is considered plaintext for FIPS purposes. This password is zeroized by overwriting it with a new password. The Crypto Officer optionally configures the module to obfuscate the Enable password. This CSP is entered by the Crypto Officer.	NVRAM (plaintext)	Overwrite with new secret
TLS RSA private keys	RSA	2048 bits	Identity certificates for the security appliance itself and also used in IPSec,	NVRAM (plaintext)	Zeroized by RSA keypair

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
			TLS, and SSH negotiations. This key was generated by calling FIPS approved DRBG.		deletion command
TLS RSA public keys	RSA	2048 bits	Identity certificates for the security appliance itself and also used in TLS negotiation. This key is derived in compliance with FIPS 186-4 RSA key pair generation method in the module.	NVRAM (plaintext)	Zeroized by RSA keypair deletion command
TLS pre-master secret	keying material	At least eight characters	Keying material used to derive TLS master key during the TLS 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.
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 and AES-GCM	Triple-DES 192 bits or AES 128/192/256 bits	Used in HTTPS connections. Generated using TLS protocol. 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
Integrity test key	RSA 2048 with SHA-512	2048 bits	A hard coded key used for software power-up integrity verification.	Hard coded for software integrity testing	Uninstall the module

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 certificates

Algorithm	Certificate
AES (128/192/256 bits 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 SigGen, SigVer; 2048 bits)	2703
ECDSA (KeyGen, SigGen, SigVer; P-256, P-384, P-521)	1277
DRBG (AES256_CTR)	1828
CVL Component (IKEv2, TLSv1.2, SSHv2)	1561
CKG (vendor affirmed)	

Table 7 Approved Cryptographic Algorithms

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 7296 for IPsec/IKEv2 and 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 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. 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 symmetric key and the seed used in the asymmetric key generation are the unmodified output from SP800-90A DRBG.

Non-FIPS Approved Algorithms Allowed in FIPS Mode

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

- Diffie-Hellman (CVL Cert. #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; key establishment methodology less than 112 bits of encryption strength; non-compliant)

- HMAC MD5
- MD5
- RC4
- HMAC-SHA1 is not allowed with key size under 112-bits

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 insure all components are functioning correctly.

Self-tests performed

- FTDv Self Tests
    - POSTs – Cisco Security Crypto Virtual
        - AES 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-1/256/384/512) KATs
        - RSA Known Answer Tests (Separate KAT for signing; Separate KAT for verification)
        - SHA-1/256/384/512 KATs
        - Software Integrity Test (RSA 2048 with SHA-512)
        - Triple-DES Encrypt/Decrypt KATs
    - Conditional tests - Cisco Security Crypto Virtual
        - RSA pairwise consistency test
        - ECDSA pairwise consistency test
        - Conditional IPSec 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

The module was validated with software version 6.2 (File Cisco_FTD_Patch-6.2.2.3-66.sh.REL.tar). This is the only allowable image for FIPS-approved mode of operation.

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

Step 1: Use the VMware Virtual Machine Properties

1. Right-click the name of your new virtual appliance, then select **Edit Settings** from the context menu, or click **Edit virtual machine settings** from the **Getting Started** tab in the main window.

2. Make sure the **Memory**, **CPUs**, and **Hard disk 1** settings are set to the defaults, as described in Default Virtual Appliance Settings.

The memory setting and the number of virtual CPUs for the appliance are listed on the left side of the window. To see the hard disk **Provisioned Size**, click **Hard disk 1**.

3. Confirm the **Network adapter 1** settings are as follows, making changes if necessary:

a. Under **Device Status**, enable the **Connect at power on** check box.

b. Under **MAC Address**, manually set the MAC address for your virtual appliance's management interface.

Manually assign the MAC address to your virtual appliance to avoid MAC address changes or conflicts from other systems in the dynamic pool.

Additionally, for virtual Cisco Firepower Management Centers, setting the MAC address manually ensures that you will not have to re-request licenses from Cisco if you ever have to reimage the appliance.

c. Under **Network Connection**, set the **Network label** to the name of the management network for your virtual appliance.

4. Click **OK**.

Step 2: Launch Firepower Device Manager

1. From a client on the same subnet as the Firepower Threat Defense Virtual, open a browser.

2. Log into Firepower Device Manager. Assuming you did not go through initial configuration in the CLI, open Firepower Device Manager at **https:** *//ip-address*, where the address is **https://192.168.45.45**.

3. Log in with the username **admin**, password **Admin123**.

4. If this is the first time logging into the system, and you did not use the CLI setup wizard, you are prompted to read and accept the End User License Agreement and change the admin password. You must complete these steps to continue.

5. Configure the following options for the outside and management interfaces and click **Next**.

6. Click **Finish**.

Step 3: Move to FX-OS side

1. scope security > enable fips-mode
   write
   reboot system