Cisco Firepower Management Center Virtual (FMCv) Cryptographic Module

FIPS 140-2 Non Proprietary Security Policy
Level 1 Validation

Document Version 1.0

October 5, 2020

1 Introduction

1.1 Purpose

This is the non-proprietary Cryptographic Module Security Policy for Cisco Firepower Management Center Virtual (FMCv) Cryptographic Module (software version 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 with the specification of the security rules listed in Table 1 above, under which the Cisco Firepower Management Center Virtual (FMCv) Cryptographic Module will operate, including the rules derived from the requirements of FIPS 140-2, FIPS 140-2IG 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:

https://www.cisco.com/c/en/us/products/index.html
https://www.cisco.com/c/en/us/products/security/firepower-management-center/index.html

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

The NIST Validated Modules 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 Management Center Virtual (FMCv) Cryptographic Module identified is referred to as Cisco Firepower Management Center Virtual Cryptographic Module, FMC virtual module, FMCv, Module, virtual 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 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 Management Center Virtual (FMCv) Cryptographic Module

The Cisco Firepower Management Center Virtual (FMCv) Cryptographic Module is a virtualized version of the Firepower Management Center which provides complete and unified management over firewalls, application control, intrusion prevention, URL filtering, and advanced malware protection, easily go from managing a firewall to controlling applications to investigating and remediating malware outbreaks.

The module now becomes the centralized point for event and policy management as does the Cisco Firepower Management Center for the following solutions:

- Cisco Firepower Next-Generation Firewall (NGFW)
- Cisco ASA with FirePOWER Services
- Cisco Firepower Next-Generation IPS (NGIPS)
- Cisco FirePOWER Threat Defense
- Cisco Advanced Malware Protection (AMP)

The module also controls the network management features on devices: switching, routing, NAT, as well as TLSv1.2 and SSHv2 services.

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

Guest OS	Hypervisor	Hardware	Processor
FXOS version 2	VMware ESXi 6.0	Cisco C220 M5	Intel Xeon Silver 4110
FXOS version 2	VMware ESXi 6.5	Cisco C220 M5	Intel Xeon Silver 4110

Table 2 Testing Configuration

The following platforms are Vendor affirmed:

B200 M4	B200 M5	C220 M4	C220 M5	C240 M4
C240 M5	C460 M4	C480 M5	E140S M2	E160S M3
EN120E-208	EN120S M2	E180D M2	ENCS 5406	ENCS 5408
ENCS 5412				

The following Hypervisors with varying versions work with the FMCv are Vendor affirmed:

KVM
AWS
Oracle VM
VMware ESXi 5.X
VMware ESXi 6.X

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.

2.1 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 FMC virtual module, including the Guest OS/FMC, API and FOM. Please see Diagram 1 below for the details.

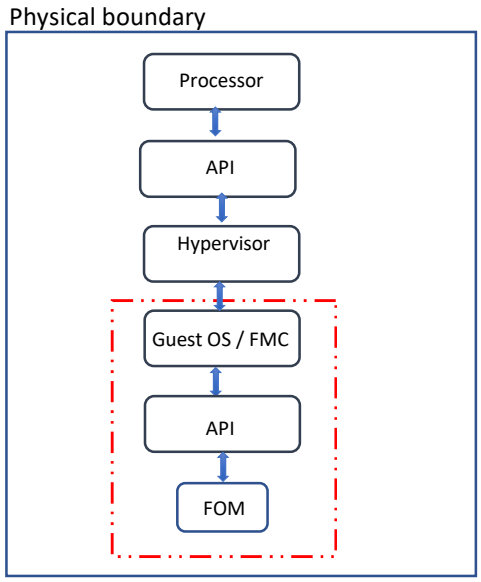

Diagram 1 Block Diagram

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 or 6.5
- Guest OS/FMC: FMC 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)

2.2 Module Interfaces

The module provides a number of physical and logical interfaces to the device, and the physical interfaces provided by the module are mapped to the following FIPS 140-2 defined logical interfaces: data input, data output, control input, status output, and power. The module provides no power to external devices and takes in its power through normal power input/cord. The logical interfaces and their mapping are described in the following table:

Physical Port/Interface	FMC Virtual	FIPS 140-2 Logical 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)	Virtual Ethernet Ports,	**Control Input Interface**

Ports; Host System Serial Port	Virtual Serial Port	
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

2.3 Roles, Services, and Authentication

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

- SSHv2
- Serial Console
- HTTPS/TLSv1.2

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 role and User role. 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.

2.4 User Services

A User enters the system by accessing the console port using either Serial Console, 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 HTTPS/TLS 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/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
SSHv2 Functions	Negotiation and encrypted data transport via SSH.	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/TLS (TLSv1.2) Functions	Negotiation and encrypted data transport via HTTPS	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 session key and TLS integrity key (r, w, d)

Table 4 User Services

2.5 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 User Name/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/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 session key, 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)
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, w, d)
View Status	View the module configuration, routing tables, active sessions health,	Operator password, Crypto Officer (CO)password (r,

Functions	temperature, memory status, voltage, packet statistics, review accounting logs, and view physical interface status.	w, d)
HTTPS/TLS (TLSv1.2) Functions	Configure HTTPS/TLSv1.2 parameters, provide entry and output of CSPs.	TLS RSA private key, TLS RSA public key, 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)
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 7, Zeroization column.	All CSPs (d)

Table 5 Crypto Officer Services

2.6 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 algorithms with the listed services in Section 2.6, the Crypto Officer must zeroize all CSPs. The use of any of the non-approved algorithms constitutes placing the module into a 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
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

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

To put the module back into the FIPS mode from the non-FIPS mode, the CO must zeroize all Keys/CSPs used in non-FIPS mode, and then strictly follow up the steps in section 3 of this document to put the module into the FIPS mode.

All services available can be found at Firepower Management Center Configuration Guide, Version 6.4 (Last Modified: 2020-08-03), which lists the configuration guidance. https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64.html.

[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.

2.7 Unauthenticated Service

The only service available to someone without an authorized role is to cycle the power.

2.8 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 and can be zeroized by the Crypto Officer. Zeroization consists of overwriting the memory that stored the key or refreshing the volatile memory.

All keys are associated with the Crypto Officer that created the keys, and the Crypto Officer is protected by a password. 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. RSA public keys are entered into the modules using digital certificates which contain relevant data such as the name of the public key's owner, which associates the key with the correct entity. All other keys are associated with the User that entered 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	384-bits	This is the entropy for SP 800-90A CTR_DRBG, used to construct seed.	DRAM (plaintext)	Power cycle the device
DRBG seed	SP800-90A CTR_DRBG	384-bits	Input to the DRBG that determines the internal state of the DRBG. Generated using DRBG derivation function that includes the entropy input 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 instantiation and then subsequently updated using the DRBG update function.	DRAM (plaintext)	Power cycle the device
DRBG key	SP800-90A CTR_DRBG	256-bits	Internal critical value used as part of SP 800-90A CTR_DRBG. Established per SP 800-90A CTR_DRBG.	DRAM (plaintext)	Power cycle the device
Diffie-Hellman shared secret	DH	2048 - 4096 bits	The shared secret used in Diffie-Hellman (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	DRAM (plaintext)	Power cycle the device

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
			generated by calling SP800-90A DRBG.		
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 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. Note that the public key is a cryptographic key, but not considered a CSP.	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)	Procedurally erase the password
Crypto Officer (CO) password	Password	8 plus characters	The password of the CO role. This CSP is entered by the Crypto Officer.	NVRAM (plaintext)	Procedurally erase the password
SSHv2 private Key	RSA	2048 bits	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	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	Triple-DES 192 bits or AES 128/192/256	This is the SSHv2 session key. It is used to encrypt all SSHv2 data traffics traversing between the SSHv2 Client and SSHv2 Server.	DRAM (plaintext)	Automatically when SSH session is terminated

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
		bits	This key is derived via key derivation function defined in SP800-135 KDF (SSH).		
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
TLS RSA private key	RSA	2048 bits	Used for RSA signature signing in TLS connection This key was generated by calling FIPS approved DRBG.	NVRAM (plain text)	Zeroized by RSA keypair deletion command
TLS RSA public key	RSA	2048 bits	Used for RSA signature verification in TLS 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 (plain text)	Zeroized by RSA keypair deletion command
ECDSA private key	ECDSA	Curves: P-256, 384, 521	Signature generation used in 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 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 pre-master secret	keying material	8 plus 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 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 session key	Triple-DES/AES/AES-GCM	Triple-DES 192 bits or AES	Used in TLS connections to protect the session traffic. This key was derived in the module.	DRAM (plaintext)	Automatically when TLS session is

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
		128/192/256 bits			terminated
TLS integrity key	HMAC-SHA-256/384	256-384 bits	Used for TLS connections 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 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

2.9 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)	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.
- Each of TLS and SSH protocols governs the generation of the respective Triple-DES keys. Refer to RFC 5246 (TLS) and RFC 4253 (SSH) 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 SSH and TLS 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 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 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)

2.10 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 pairwise-consistency test (Sign and Verify)
    - HMAC (SHA-1/256/384/512) Known Answer Tests
    - RSA Known Answer Tests (Separate KAT for signing; Separate KAT for verification)
    - SHA (SHA-1/256/384/512) Known Answer Test

    - Software Integrity Test (RSA 2048 bits)
    - Triple-DES-CBC Known Answer Tests (Separate encrypt and decrypt)

- Conditional tests
    - RSA pairwise consistency test
    - ECDSA pairwise consistency 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 7 non-available.

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

This module was validated with FMCv version 6.4 (Software Images: Cisco_Firepower_Mgmt_Center_Virtual_VMware-6.4.0-102.tar.gz and Cisco_Firepower_Mgmt_Center_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:

Step 1: For all Management Centers, the setup process must be completed by logging into the Management Center's web interface and specifying initial configuration options on a setup page.

Step 2: Choose System > Configuration (Choose **SSH** or **HTTPS** or a combination of these options to specify which ports you want to enable for these IP addresses).

Step 3: You must change the password for the `admin` account. This account has Administrator privileges and cannot be deleted.

Note: It is required to use a strong password that is at least eight alphanumeric characters of mixed case and includes at least one numeric character. Avoid using words that appear in a dictionary.

Step 4: System>Licenses>Smart Licenses, add and verify licenses (*Firepower Management Center Configuration Guide provides more detailed information)*
Install Triple-DES/AES SMART license to use Triple-DES and AES (for data traffic and SSH).

Step 5: System > Configuration; Devices > Platform Settings; STIG Compliance, choose Enable STIG Compliance; Click on save. The CO shall only use FIPS approved/Allowed cryptographic algorithms listed above.

Step 6: Reboot the security appliances.

In addition, more configuration information for Cisco FMCv (v6.4) can be found at Firepower Management Center Configuration Guide, Version 6.4 (Last Modified: 2020-08-03).
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64.html