Cisco 8800 Series Routers

Hardware Version: 8818-SYS, 8812-SYS and 8808-SYS

Supervisor Card: 8800-RP

Line Cards: 8800-LC-36FH, 8800-LC-48H

Fabric Cards: 8818-FC, 8812-FC and 8808-FC

Firmware Version: IOS-XR 7.0

Cisco Systems, Inc.

FIPS 140-2 Non-Proprietary Security Policy
Level 1 Validation

Version 1.0

October 20, 2021

Table of Contents

1 Introduction

1.1 Purpose

This document is the non-proprietary Cryptographic Module Security Policy for the Cisco 8800 Series Routers running Firmware Version IOS-XR 7.0. This security policy describes how the modules listed below meet the security requirements of FIPS 140-2 level 1, and how to operate the routers with on-board crypto enabled in a secure FIPS 140-2 mode. The Cisco 8800 Series Routers has primary SKUs that are covered in this validation effort as listed below:

Chassis	Supervisor card	Line card	Fabric card
8818-SYS	8800-RP	8800-LC-36FH	8818-FC
8812-SYS		8800-LC-48H	8812-FC
8808-SYS			8808-FC

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/Projects/Cryptographic-Module-Validation-Program.

1.2 Modules Validation Level

The following table lists the level of validation for each area in the FIPS PUB 140-2.

Table 1: Modules Validation Level

No.	Area Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	3
4	Finite State Model	1
5	Physical Security	1
6	Operational Environment	N/A
7	Cryptographic Key management	1
8	Electromagnetic Interface/Electromagnetic Compatibility	1
9	Self-Tests	1
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A
	Overall module validation level	**1**

1.3 References

This document deals only with operations and capabilities of the modules in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the routers from the following sources:

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

Cisco 8800 Series Routers -

https://www.cisco.com/c/en/us/products/routers/8000-series-routers/index.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 modules.

1.4 Terminology

In this document, the Cisco 8800 Series Routers is referred to as 8800 series routers, the routers, the devices, the cryptographic modules, or the modules.

1.5 Document Organization

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

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

This document provides an overview of the Cisco 8800 Series Routers and explains the secure configuration and operation of the modules. This introduction section is followed by Section 2, which details the general features and functionality of the router. 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 8800 Series Routers

The modules are multiple-chip standalone cryptographic modules. The cryptographic boundary is defined as encompassing the “top,” “front,” “left,” “right,” “rear,” and “bottom” surfaces of the chassis for the routers.

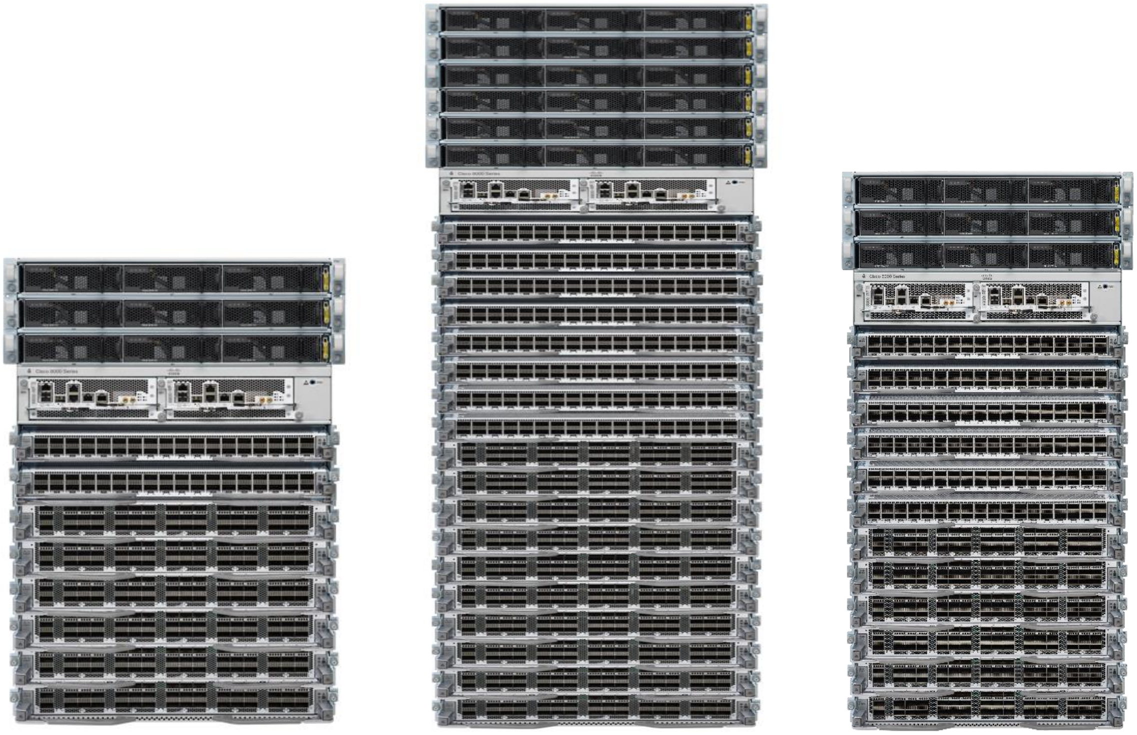

Figure 1: Front View of Cisco 8800 Series Routers – 8808-SYS (left), 8818-SYS (middle) and 8812-SYS(right)

The illustration above shows a Cisco 8800 Series Routers. All the router models have same appearance. The number of line card slots distinguish the models. Rear side of the routers include fan trays and power plugs:

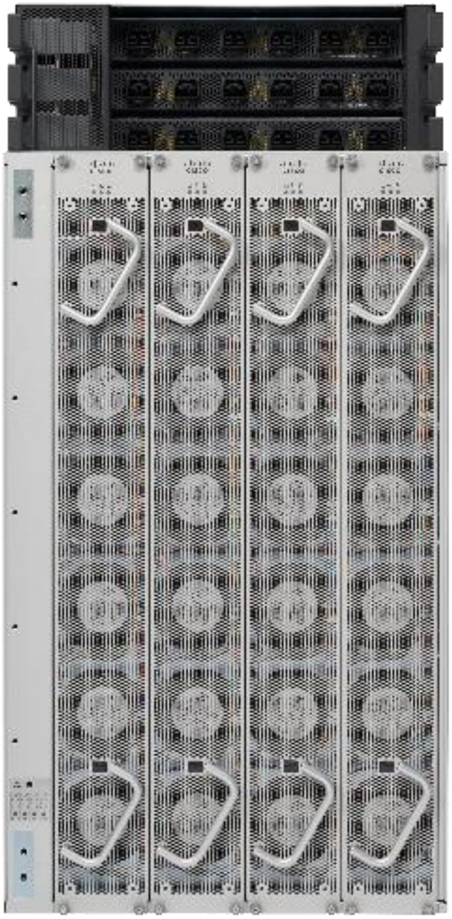

Figure 2: Rear View of Cisco 8800 Series Routers

8818-SYS, 8812-SYS and 8808-SYS are Cisco 18 slots/33RU, 12 slots/21 RU and 8 slots/16RU systems, respectively. The chassis supports distributed forwarding across multiple field replaceable units (FRUs) and do not have any ports or interface built into it.

Route Processor card (8800-RP), shown in Figure 3 below, manages all routing operations on the Cisco 8800 Series Routers.

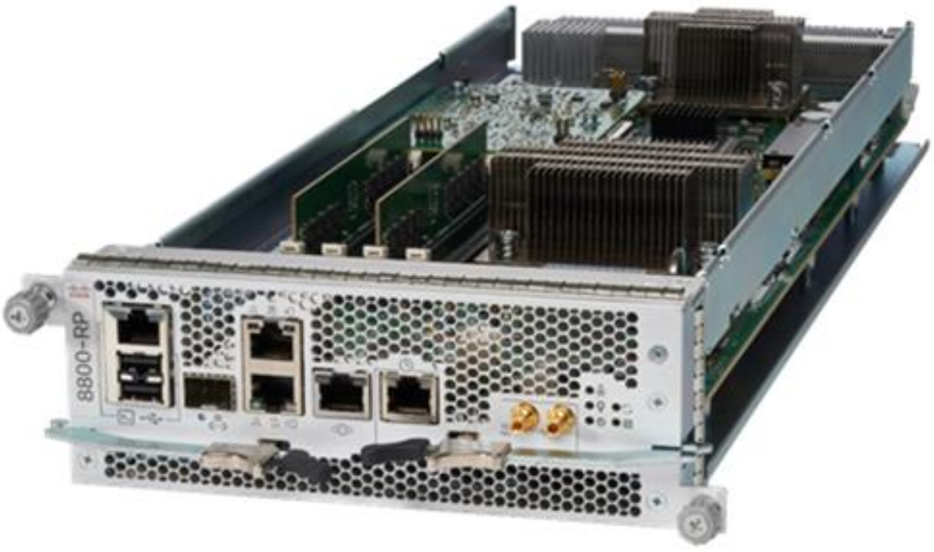

Figure 3: Route Processor card (8800-RP)

The RP has the following ports in it:

- Console RS-232 Serial Port RJ45
- Two Universal Serial Bus (USB) Ports Type-A
- Control Plane Expansion SFP/SFP+ port
- Management Ethernet (10/100/1000-Mbps) RJ-45 (Copper) port LAN
- IEEE 1588 Precision Time Protocol (PTP)
- SyncE BITS/DTI/J.211
- G.703 Time-of-Day (TOD)
- Mini coaxial connector for 10 MHz
- Mini coaxial connector for 1 PPS

The 8800 series routers support two models of line cards, 8800-LC-36FH and 8800-LC-48H. 8800-LC-36FH includes 36QSFPDD-56 ports and upto 144 ports of 100 Gbe. It also supports QSFP+, QSFP28, and QSFP28-DD interfaces. MACsec capable 8800-LC-48H line card supports 48 QSFP28 ports and QSFP+ optics for 10G and 40G compatibility.

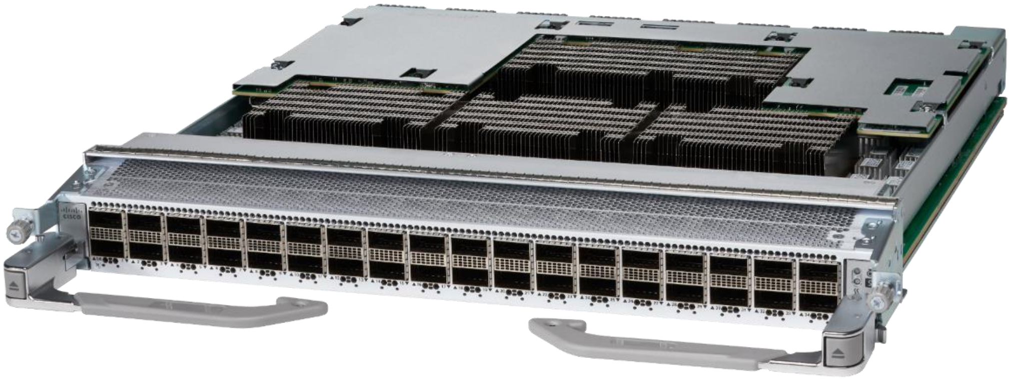

Figure 4: 8800-LC-36FH

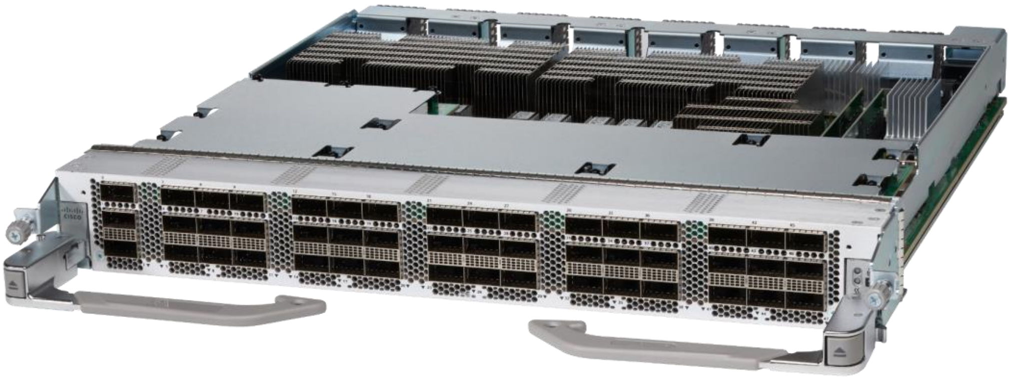

Figure 5: 8800-LC-48H

The routers switch fabric is powered by fabric cards (8818-FC, 8812-FC and 8808-FC) that provide line rate redundancy. The fabric cards do not include any ports or interfaces and same in appearance for all three models.

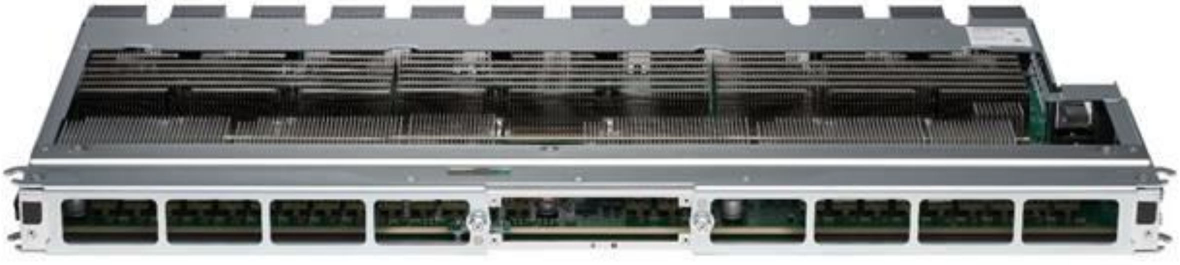

Figure 6: Fabric Card

The modules provide a number of physical and logical interfaces to the device, and the physical interfaces provided by the modules 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 tables.

Table 2: Cisco 8800 Series Routers Physical Interface/Logical Interface Mapping

FIPS 140-2 Logical Interface	Physical Interfaces
Data Input Interface, Data Output Interface	QSFPDD-56 / QSFP28 / QSFP+ Control Plane Expansion SFP/SFP+ port Management Ethernet (10/100/1000-Mbps) RJ-45 (Copper) port LAN
Control Input Interface	Console RS-232 Serial Port RJ45 Two Universal Serial Bus (USB) Ports Type-A Control Plane Expansion SFP/SFP+ port Management Ethernet (10/100/1000-Mbps) RJ-45 (Copper) port LAN IEEE 1588 Precision Time Protocol (PTP) SyncE BITS/DTI/J.211 G.703 Time-of-Day (TOD) Mini coaxial connector for 10 MHz Mini coaxial connector for 1 PPS
Status Output Interface	Console RS-232 Serial Port RJ45 QSFPDD-56 / QSFP28 / QSFP+ Control Plane Expansion SFP/SFP+ port Management Ethernet (10/100/1000-Mbps) RJ-45 (Copper) port LAN Light Emitting Diode (LED) • Chassis LEDs • Fan tray LED • Power supply LED • Port Status LEDs
Power Interface	AC/DC power connector

Note: the modules include a 1000BASE-T management and Baseboard Management Controller (BMC) port, which should not be accessed in FIPS mode of operation.

2.1 Roles, Services and Authentication

The modules support identity-based authentication. Each user is authenticated upon initial access to the modules. There are two roles in the routers that may be assumed: Crypto-Officer (CO) role and the User role. The administrator of the routers assumes the CO role in order to configure and maintain the routers, while the Users are processes that exercise security services over the network.

2.1.1 User Role

The role is assumed by users utilizing pass through traffic via Data Input/ Output Interfaces defined in Table 2. From a logical view, user activity exists in the data-plane. Users are not authenticated for the "Traffic Routing Services" that do not permit an operator to modify, disclose or substitute CSPs and do not affect the security of the module or the security of the information being protected by the module as permitted by Implementation Guidance (IG) 3.1 and IG 3.4.

Users are authenticated by MACsec authentication for "Secured Dataplane" service but the MACsec CAK (connectivity Association Key) is configured by the CO and the MACsec encryption key used to encrypt the MACsec session is derived using the CAK that is configured by CO. The CO can only configure the MACsec CAK by using one of the authentication methods described in Section 2.1.2 of the document.

The services available to the User role accessing the CSPs, the type of access – read (r), write (w), execute (e) and zeroized/delete (d) – are listed below:

Table 3 - User Services

Services	Description	Keys and CSPs Access
Secured Dataplane	MACsec Network Functions: authentication, access control, confidentiality and data integrity services provided by the MACsec protocol	MACsec Security Association Key (SAK), MACsec Connectivity Association Key (CAK), MACsec Key Encryption Key (KEK), MACsec Integrity Check Key (ICK), Pairwise Master Key (PMK), Pairwise Transient Key (PTK), DRBG entropy input, DRBG V, DRBG Key (w, e, d)
Traffic Routing Services	Pass through traffic without authentication. The rule must have been previously configured by the Crypto Officer.	N/A

2.1.2 Crypto-Officer Role

This role is assumed by an authorized CO connecting to the routers via CLI through the console port and performing management functions and modules configuration. IOS-XR prompts the CO for their username and password, and, if the password is validated against the CO's password in IOS-XR memory, the CO is allowed entry to the IOS-XR executive program. A CO can assign permission to access the CO role to additional accounts, thereby creating additional COs.

CO passwords and SNMPv3 passwords must be at a minimum eight (8) characters long. The Secure Operation sections procedurally enforces the password must contain at least one special character and at least one number character along with six additional characters taken from the 26-upper case, 26-lower case, 10-numbers and 32-special characters (procedurally enforced). This requirement gives (26 + 26 + 10 + 32 =) 94 options of character to choose from. Without repetition of characters, the number of probable combinations is the combined probability from 6 characters (94x93x92x91x90x89) times one special character (32) times 1 number (10), which turns out to be

(94x93x92x91x90x89x32x10 =) 187,595,543,116,800. Therefore, the associated probability of a successful random attempt is approximately 1 in 187,595,543,116,800, which is less than 1 in 1,000,000 required by FIPS 140-2. It takes 1-2 seconds for the password to be entered and the for the module to verify the password. Hence, assuming the module can perform one (1) attempt per second, one minute would require the ability to make over (187,595,543,116,800 / 60 =) 3,126,592,385,280 guesses per minute. Therefore, the associated probability of a successful random attempt for a minute is approximately 1 in 3,126,592,385,280, which is less than the 1 in 100,000 required by FIPS 140-2.

The CO may authenticate using RSA or ECDSA algorithm as well. RSA key pair has a modulus size of either 2048 or 3072 bits, thus providing at least 112-bits of strength. ECDSA requires only 224-bit sized public keys to provide the same 112-bit security level. Assuming the low end of that range of security strength (112-bits), 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. The fastest network connection supported by the modules over management interfaces are 1 Gb/s. Hence, at most 1 ×10^9 × 60s = 6 × 10^10 = 60,000,000,000 bits of data can be transmitted in one minute. Therefore, the probability that a random attempt will succeed, or a false acceptance will occur in one minute is:

1:(2^112 possible keys/(6 × 10^10 bits per minute)/112 bits per key))

1:(2^112 possible keys/5,357,142,85.7 keys per minute)

1:9.7×10^24

Therefore, the associated probability of a successful random attempt for a minute is approximately 1 in 9.7×10^24, which is less than the 1 in 100,000 required by FIPS 140-2.

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

Table 4 - Crypto-Officer Services

Services	Description	Keys and CSPs Access
Initialization	Setup initial configuration as mentioned in Secure Operation section of this security policy.	CO password, DH private key, DH public key, SSH RSA private key, SSH RSA public key, SNMPv3 integrity key, TLS Server RSA private key, TLS Server RSA public key, SNMPv3 privacy passphrase, SNMPv3 authentication passphrase, snmpEngineID (w)
Define Rules and Filters	Define network interfaces and settings, create command aliases, set the protocols the router will support, enable interfaces and	CO password (r, w, e, d)

Services	Description	Keys and CSPs Access
	network services, set system date and time, and load authentication information. Log off users, shutdown or reload the router, manually back up router configurations, view complete configurations, manage user rights, and restore router configurations. 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.	
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.	CO password (r, w, e, d)
Configure Encryption	Set up the configuration tables for secured traffic using MACsec.	MACsec Connectivity Association Key (CAK) (r, w, e, d)
Remote Management Access	Setup SSHv2, TLS1.2 and SNMPv3 access for remote management	DH private key, DH public key, DH Shared Secret, SSH RSA private key, SSH RSA public key, SSHv2 session key, SSHv2 integrity key, SNMPv3 session key, SNMPv3 integrity key, TLS Server RSA private key, TLS Server RSA public key, TLS pre-master secret, TLS encryption keys, DRBG entropy input, DRBG V, DRBG Key (w, e, d) SNMPv3 privacy passphrase, SNMPv3 authentication passphrase, snmpEngineID (r, w, d)

Services	Description	Keys and CSPs Access
Self-Tests	Execute the FIPS 140 start-up tests on demand	N/A
Zeroization	Zeroize cryptographic keys/CSPs by reloading the modules	All CSPs (d)

2.1.3 Unauthorized Role

The services for someone without an authorized role are:

System Status: An unauthorized operator can observe the system status by viewing the LEDs on the module, which show network activity and overall operational status.

Power Cycle: An unauthorized operator can power cycle the module.

2.1.4 Services Available in Non-FIPS Mode of Operation

The cryptographic modules in addition to 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. The modules are considered to be in a non-FIPS mode of operation when it is not configured per section 3 (Secure Operation of the Routers). The FIPS approved services listed in Table 8 become non-approved services when using any non-approved algorithms or non-approved key or curve sizes.

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

Services [1]	Non-Approved Algorithms
SSHv2	Hash: MD5 MAC: HMAC MD5 Symmetric: DES Asymmetric: 768-bit/1024-bit RSA (key transport), 1024-bit Diffie-Hellman

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

TLS 1.2	Symmetric: DES, RC4 Asymmetric: 768-bit/1024-bit RSA (key transport), 1024-bit Diffie-Hellman
SNMP v1/v2	Hash: MD5 Symmetric: DES
IPsec	Hashing: SHA-1 Symmetric: Triple-DES, AES
EAP-TLS	Symmetric: AES MAC: AES CMAC

2.2 *Cryptographic Algorithms*

The modules implement a variety of approved and non-approved algorithms.

Approved Cryptographic Algorithms

The routers support the following FIPS-2 approved algorithm implementations:

Table 6 – Algorithm Certificates

Algorithms	CAVP #A388: CiscoSSL FOM Cryptographic Algorithm Implementation[2]	CAVP #C1668: GCM-AES Crypto Core	CAVP #C2139: IOS-XR Firmware Image Signing
AES	**CBC(128, 192, 256),** CCM(128, 192, 256), CFB1/8/128(128, 192, 256), **CMAC(128, 192, 256),** **CTR(128, 192, 256),** **ECB(128, 192, 256),** **GCM(128, 192, 256),** KW(128, 192, 256), OFB (128, 192, 256) XTS(128, 256)	ECB (128, 256), **GCM (128, 256),** **GMAC (128, 256),** **XPN (128, 256)**	N/A
KAS-SSC (vendor affirmed)[3]	**DH (Group 14)** **ECDH (Curve: P-256, P-384, P-521)**	N/A	N/A
KBKDF	**KDF Mode: Counter** **MAC Mode: HMAC-SHA-1, HMAC-SHA2-224, HMAC-SHA2-**	N/A	

[2] AES-XTS was tested as part of CAVP algorithm testing, but it is not utilized by the modules.

[3] Shared Secret Computation using the Discrete Logarithm Cryptography; vendor affirmed to SP 800-56A rev3 per IG D.1-Rev3

	256, HMAC-SHA2-384, HMAC-SHA2-512		
DRBG	**CTR-AES** (128, 192, **256**), SHA-1, SHA2-224, SHA2-384, SHA2-512 HMAC (SHA-1, SHA2-224, SHA2-384, SHA2-512)	N/A	N/A
HMAC	**HMAC SHA-1,** HMAC SHA2-224**, HMAC SHA2-256, HMAC SHA2-384, HMAC SHA2-512**	N/A	N/A
ECDSA	**KeyGen, KeyVer, SigGen, SigVer** (Curve: B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, **P-256, P-384, P-521**)	N/A	N/A
SP 800-135 CVL	IKEv2 **SNMP** SRTP **SSH** **TLS**	N/A	N/A
KTS	**KTS (AES Cert. #A388 and HMAC Cert. #A388; key establishment methodology provides between 128 and 256 bits of encryption strength); AES modes: AES 128/192/256-bit CTR, AES 128/192/256-bit CBC and AES 128/192/256-bit GCM**	N/A	N/A
KTS	N/A	**KTS (AES Cert. #C1668; key establishment methodology provides 128 or 256 bits of encryption strength); AES modes: AES 128 and 256-bit GCM/GCM-XPN**	N/A
RSA	**KeyGen (186-4) 2048-, 3072-bits modulus** SigGen (186-2 ANSI X9.31, PKCS 1.5, PKCSPSS) 4096-bits modulus, **SigGen (186-4 ANSI X9.31, PKCS 1.5, PKCSPSS) 2048-, 3072-bits modulus,** **SigVer (186-4 ANSI X9.31, PKCS 1.5, PKCSPSS) 2048-, 3072-bits modulus**	N/A	**RSA 2048 SIgVer**
SHS	**SHA-1,** SHA2-224, **SHA2-256, SHA2-384, SHA2-512**	N/A	**SHA-256**
Triple-DES	**CBC**, CFB1/8/64, **CTR, ECB,** OFB (keying option: 1)	N/A	N/A

DSA	Keygen (2048, 3072), PQGGen (2048, 3072), PQGVer (2048, 3072), Siggen (2048, 3072), Sigver (2048, 3072)	N/A	N/A
CKG	**Vendor affirmed**	N/A	N/A

Notes:

There are some algorithm modes that were tested but not implemented by the modules. The algorithms, modes, and key sizes that are used by any services by the modules are shown in this table in **bold** font.

The modules' AES-GCM implementation conforms to IG A.5 scenario #1 following RFC 5288 for TLS. The modules are compatible with TLSv1.2 and provides support for the acceptable GCM cipher suites from SP 800-52 Rev1, Section 3.3.1.

The 64-bit counter portion of the 96-bit IV is set by the modules within its cryptographic boundary. When the IV exhausts the maximum number of possible values (0 to 2^{64} - 1) 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 modules' power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established.

The AES GCM IV is generated internally in the cryptographic module in accordance with IEEE 802.1AE and its amendments. The IV length used is 96 bits (per SP 800-38D and FIPS 140-2 IG A.5). The AES GCM IV construction is performed in compliance with IEEE 802.1AE and its amendments. If the module loses power, then new AES GCM keys should be established. The module should only be used with CMVP FIPS 140-2 validation modules when supporting the MACsec protocol for providing Peer, Authenticator functionality. The Peer and the Authenticator Modules Security Policies shall state that the link between the Peer and the Authenticator should be secured to prevent the possibility for an attacker to introduce foreign equipment into the local area network.

No parts of the SSH, SNMPv3 and TLS protocols, other than the KDFs, have been tested by the CAVP and CMVP. Each of TLS and SNMPv3 protocols governs the generation of the respective Triple-DES keys. Refer to RFC 5246 (TLS) for details relevant to the generation of the individual Triple-DES encryption keys. The user is responsible for ensuring the modules limit the number of encryptions with the same key to 2^{20}.

In accordance with FIPS 140-2 IG D.12, the cryptographic modules perform Cryptographic Key Generation as per scenario 1 of section 4 in SP800-133 rev2. 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

RSA PKCS#1 v1.5 (key wrapping; key establishment methodology provides between 112 and 128 bits of encryption strength; non-compliant less than 112 bits of encryption strength) when used with modulus size of 2048 bits or greater

NDRNG to seed FIPS approved DRBG (256 bits)

Non-FIPS Approved Algorithms

The cryptographic modules implement the following non-Approved algorithms that are not used in FIPS mode of operation:

MD5 (MD5 does not provide security strength to TLS protocol)
HMAC-MD5
RC4
DES

2.3 Cryptographic Key/CSP Management

The modules securely administer both cryptographic keys and other critical security parameters such as passwords. All keys are also protected by the password-protection on the CO role login and can be zeroized by the CO. Keys are exchanged and entered electronically. Persistent keys are entered by the CO via the console port CLI, transient keys are generated or established and stored in DRAM.

Table 7 lists the secret and private cryptographic keys and CSPs used by the modules.

Table 7 – Cryptographic Keys and CSPs

ID	Algorithm	Size	Description	Storage	Zeroization Method
General Keys/CSPs					
DRBG V	800-90A CTR_DRBG	128-bits	Generated by entropy source via the CTR_DRBG derivation function.	DRAM (plaintext)	Power cycle
DRBG key	SP 800-90A CTR_DRBG	384-bits	This is the 256-bit DRBG key used for SP 800-90 CTR_DRBG	DRAM (plaintext)	Power cycle
DRBG entropy input	SP 800-90A CTR_DRBG	256-bits	HW based entropy source output used to construct seed	DRAM (plaintext)	Power cycle
DRBG seed	SP 800-90A CTR_DRBG	256-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

ID	Algorithm	Size	Description	Storage	Zeroization Method
CO password	Password	Variable (8+ characters)	Used to authenticate local users	NVRAM (plaintext)	Zeroized by overwriting with new password
Diffie-Hellman public key	DH	2048 bits	The public exponent used in Diffie-Hellman (DH) exchange.	DRAM (plaintext)	Automatically after shared secret generated
Diffie-Hellman private key	DH	224 bits	The private exponent used in Diffie-Hellman (DH) exchange.	DRAM (plaintext)	Automatically after shared secret generated.
EC Diffie-Hellman public key	ECDH	P-256, P-384, P-521	The public exponent used in EC Diffie-Hellman (ECDH) exchange.	DRAM (plaintext)	Automatically after shared secret generated
EC Diffie-Hellman private key	ECDH	P-256, P-384, P-521	The private exponent used in ECDH exchange.	DRAM (plaintext)	Automatically after shared secret generated
EC Diffie-Hellman shared secret	ECDH	P-256, P-384, P-521	This is the shared secret agreed upon as part of ECDH exchange	DRAM (plaintext)	Automatically after session ends or via power cycle
Diffie-Hellman shared secret	DH	2048 bits	This is the shared secret agreed upon as part of DH exchange	DRAM (plaintext)	Automatically after session ends or via power cycle
SSHv2					
SSHv2 public key	RSA, ECDSA	2048-3072 bits modulus, ECDSA p-256, p-384 and p-521	SSH public key used in SSH session establishment	NVRAM (plaintext)	'# crypto key zeroize rsa' '# crypto key zeroize ecdsa'
SSHv2 private key	RSA, ECDSA	2048-3072 bits modulus, ECDSA p-	SSH private key used in SSH session establishment	NVRAM (plaintext)	'# crypto key zeroize rsa'

ID	Algorithm	Size	Description	Storage	Zeroization Method
		256, p-384 and p-521			‘# crypto key zeroize ecdsa’
SSHv2 session key	AES	128-, 192- and 256-bits CTR	This is the SSH session symmetric key.	DRAM (plaintext)	Automatically when SSH session terminated
SSHv2 integrity key	HMAC	HMAC SHA-1, HMAC SHA-256 and HMAC SHA-512	This is the SSH integrity MAC key.	DRAM (plaintext)	Automatically when SSH session terminated
TLS1.2					
TLS server RSA public key	RSA	2048-3072 bits modulus	RSA public key used in TLS negotiations.	NVRAM (plaintext)	‘# crypto key zeroize rsa’
TLS server RSA private key	RSA	2048-3072 bits modulus	Identity certificates for module itself and also used in TLS negotiations.	NVRAM (plaintext)	‘# crypto key zeroize rsa’
TLS pre-master secret	Keying material	384-bits	Shared secret created using asymmetric cryptography from which new HTTPS session keys can be created.	DRAM (plaintext)	Automatically when session terminated.
TLS Master Secret	Keying material	48-bytes	Keying material used to derive other HTTPS/TLS keys. This key was derived from the TLS pre-master secret during the TLS session establishment	DRAM (plaintext)	Automatically when session terminated.
TLS encryption key	AES	AES CBC/GCM 128/192/256-bits	This is the TLS session key	DRAM (plaintext)	Automatically when session terminated.

ID	Algorithm	Size	Description	Storage	Zeroization Method
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 session terminated.
SNMPv3					
snmpEngineID	Shared secret	32-bits	Unique string to identify the SNMP engine	NVRAM (plaintext)	'# no snmp-server engineID local engineid-string', overwriitten with new engine ID
SNMPv3 authentication passphrase	Password	Variable (8+ characters)	This secret is used to derive HMAC-SHA1 key for SNMPv3 authentication	NVRAM (plaintext)	Removing "snmp-server" configuration or overwritten with new password
SNMPv3 privacy passphrase	Password	Variable (8+ characters)	This secret is used to derive AES key for SNMPv3 privacy	NVRAM (plaintext)	Removing "snmp-server" configuration or overwritten with new password
SNMPv3 integrity key	HMAC	256 bits	Provides integrity to SNMPv3 traffic	DRAM (plaintext)	Power cycle
SNMPv3 session key	AES	128-bit	Encrypts SNMPv3 traffic	DRAM (plaintext)	Power cycle
MACsec					
MACsec Connectivity Association Key (CAK)	Hex string	32 or 64 bytes	A CO configured pre-shared secret key possessed by members of a MACsec connectivity association to secure control plane traffic	NVRAM (plaintext)	Overwritten with new a key

ID	Algorithm	Size	Description	Storage	Zeroization Method
MACsec Integrity Check Key (ICK)	AES-GCM, AES-GCM-XPN	128/256 bits	Used to prove an authorized peer sent the message. Derived from the CAK using the SP800-108 KDF.	DRAM (plaintext)	Automatically when session expires or power cycle
MACsec Key Encryption Key (KEK)	AES-CMAC	128/256 bits	Used to transmit Security Association Key (SAK) to other peers of a MACsec connectivity association. Derived from the CAK using the SP800-108 KDF.	DRAM (plaintext)	Automatically when session expires or power cycle
MACsec Security Association Key (SAK)	AES-GCM, AES-GCM-XPN	128-, 256-bits	Derived from the CAK and used by the device network ports for securing User network traffic.	DRAM (plaintext)	Automatically when session expires or power cycle

2.4 Self-Tests

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

2.4.1 Power-On Self-Tests (POSTs)

- Firmware Integrity Test (RSA PKCS#1 v1.5 (2048 bits) signature verification with SHA-512)
- CiscoSSL FIPS Object Module Algorithm Implementation Known Answer Tests (Note: KATs marked by asterisk are implemented but not used by any services implemented by the module in Approved mode of operation):
  - AES (encrypt/decrypt) ECB KATs
  - AES-CCM (encrypt/decrypt) KATs*
  - AES-GCM (encrypt/decrypt) KATs
  - AES-CMAC (encrypt/decrypt) KAT
  - AES-XTS (encrypt/decrypt) KATs*
  - SP800-90A CTR_DRBG KAT
  - FIPS 186-4 DSA Sign/Verify Test*
  - FIPS 186-4 ECDSA Sign/Verify Test
  - HMAC-SHA1, -224*, -256, -384, -512 KATs
  - FIPS 186-4 RSA (sign/verify) KATs
  - SHA-1 KAT

    - Software Integrity Test (HMAC-SHA1)
    - Triple-DES ECB (encrypt/decrypt) KATs
    - KBKDF KAT
    - SP800-90A DRBG section 11.3 health tests
- Hardware Algorithm Implementation Known Answer Tests:
    - AES (encrypt/decrypt) GCM and XPN KATs

2.4.2 Conditional Tests

- CiscoSSL FIPS Object Module Algorithm Implementation Conditional Tests:
    - Pairwise consistency tests for RSA and ECDSA
    - SP 800-90A CTR_DRBG Continuous random number generation tests
    - Continuous Random Number Generation test for non-approved DRBG (entropy) on 256-bits

The devices perform all power-on self-tests automatically at boot. All power-on self-tests must be passed before each role starts to perform services.

2.5 Physical Security

The cryptographic modules entirely contained within production-grade enclosure. The chassis of the modules have removable covers.

3 Secure Operation of Cisco 8800 Series Routers

The routers meet all the overall Level 1 requirements for FIPS 140-2. Follow the setup instructions provided below to place the modules in FIPS-approved mode. Operating this Routers without maintaining the following settings will remove the modules from the FIPS approved mode of operation.

3.1 System Initialization and Configuration

The module does not provide any initial credential from the factory. The CO must follow procedural controls to control access to the module[4] and initialize the authentication mechanisms.

1. Initially the router does not have any user configuration. The system prompts you to specify the username of the root user as well as a secret (password).

```
--- Administrative User Dialog ---

Enter root-system username: [username]
Enter secret: [password]
Enter secret again: [password]

RP/0/0/CPU0:Jan 10 12:50:53.105 : exec[65652]: %MGBL-CONFIG-6-DB_COMMIT :
'Administration configuration committed by system'. Use 'show configuration
commit changes 2000000009' to view the changes.
Use the 'admin' mode 'configure' command to modify this configuration.

User Access Verification

Username: [username]
Password: [password]
RP/0/0/CPU0:router#
```

2. The CO must always assign passwords (of at least 8 characters, including at least one letter and at least one number) to users. Identification and authentication on the console/auxiliary port is required for accessing the module. From the "configure terminal" command line, the CO enters the following syntax:

```
router#configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

router(config)#line con 0

router(config-line)#password [password]

router(config-line)#login
```

3. Configure Management port from the "configure terminal" command line.

```
router(config)#interface MgmtEth [Forward interface in Rack/Slot/Instance/Port format]

router(config-if)#ipv4 address 172.18.189.38 255.255.255.224

router(config-if)#no shutdown

router(config-if)#exit

router(config)#router static address-family ipv4 unicast [A.B.C.D/length] [default-gateway]

router(config)#commit
```

4. Enable debug message logging followed by turn on the FIPS 140-2 mode of operation.

[4] Note: the modules include a 1000BASE-T management and Baseboard Management Controller (BMC) port, which should not be accessed in FIPS mode of operation.

```
router(config)#logging buffered debugging
router(config)#crypto fips-mode
router(config)#commit
```

Issue the following command to enable FIPS mode on the 8800-LC-48H line card.

```
router(config)# hw-module macsec-fips-post location {location | all}
router(config)#commit
```

Note: On reload the device will be in the FIPS Approved Mode of Operation.

```
router(config)#reload location all
```

5. Perform these steps to configure the FIPS compliant keys.

Please note that the following steps must be done after FIPS 140-2 mode of operation (shown in step 4). FIPS 140-2 standard mandates to keep the critical security parameters separated between FIPS and non-FIPS mode of operations. Any existing key or key-chain should be deleted by the CO and recreated once step 4 is performed successfully.

a. Configuring FIPS compliant keys for any purpose

```
router#crypto key generate rsa [usage-keys | general-keys] key label
router(config)# crypto key generate rsa
```

b. Configuring FIPS compliance key chain

```
router(config)#key chain [key-chain-name]
router(config-key-chain)#key [key-id]
router(config-key-chain-[key-id])#cryptographic-algorithm {HMAC-SHA-256 | SHA-1}
router(config-key-chain)#commit
```

c. Configuring FIPS compliant Certificates

```
router(config)#crypto ca trustpoint [ca-name] rsakeypair [key label]
router(config-key-chain)#commit
```

d. Configuring FIPS-compliant MACsec involves creating a MACsec keychain, key, policy and applying MACsec configuration on physical interfaces.

Configuring MACsec Pre-shared Key

```
router(config)# key chain [key-chain-name] macsec
router(config-[key-chain-name]-MacSec)# key [key]
```

Note: 'key' is a hex string of even length and max 64 bytes

```
router(config-[key-chain-name]-MacSec-[key])# keystring [32 or 64 byte of hex string] cryptographic-algorithm {aes-128-cmac | aes-256-cmac}
router(config-[key-chain-name]-MacSec-[key])# lifetime {hh:mm:ss} {1-31} month year [time length]
router(config)#commit
```

Configuring MACsec Pre-shared Key

```
router(config)# macsec-policy mac_policy
router(config-mac_policy)# cipher-suite { GCM-AES-128 | GCM-AES-256 | GCM-AES-XPN-128 | GCM-AES-XPN-256 }

router(config-mac_policy)# conf-offset [offset_value]

router(config-mac_policy)# key-server-priority [priority]

router(config-mac_policy)# security-policy must-secure

router(config-mac_policy)# window-size [window size]

router(config-mac_policy)# include-icv-indicator

router(config)#commit
```

Applying MACsec Configuration on an Interface

```
router(config)# interface [location]

router(config-if)# macsec psk-keychain [mac_chain] policy [policy]

router(config)#commit
```

e. Configuring FIPS-compliant SNMPv3 Server

```
router(config)#snmp-server user username groupname {v3 [ auth sha {clear | encrypted} auth-password [priv {3des |aes { 128 | 192 | 256} } {clear | encrypted } priv-password]] } [SDROwner | SystemOwner] access-list-name

router(config)#commit
```

f. Configuring FIPS-compliant SSHv2 Client and Server

```
router# ssh {ipv4-address | ipv6-address} cipher aes {128-CBC | 192-CBC | 256-CBC} username username

router#configure

router(config)#ssh server v2

router(config)#commit
```

g. Configuring FIPS-compliant TLS1.2 only as part of gRPC protocol. Please note that only FIPS-compliant TLS cipher suite is offered for the protocol.

```
router(config)# grpc {address-family | dscp | max-request-per-user | max-request-total | max-streams | max-streams-per-user | no-tls | service-layer | tls-cipher | tls-mutual | tls

router(config)#commit
```

NOTE: The keys and CSPs generated in the cryptographic module during FIPS mode of operation cannot be used when the module transitions to non-FIPS mode and vice versa. While the module transitions from FIPS to non-FIPS mode or from non-FIPS to FIPS mode, all the keys and CSPs are to be zeroized by the Crypto Officer.

Note: 3-key Triple-DES has been implemented in the module and is FIPS approved until December 31, 2023. Should the CMVP disallow the usage of Triple-DES post-December 31, 2023, then users must not configure Triple-DES.

3.2 Disable FIPS Mode of Operation

To transition from the FIPS mode of operation to a non-FIPS mode of operation, the Cryptographic Officer shall zeroize all keys and CSP’s that were generated in the FIPS approved mode and remove the FIPS mode command from the configuration. For key zeroization, please refer to the “Zeroization Method” column in Table 7 of this document. To remove the FIPS mode, use the commands below from configuration:

```
router(config)#no crypto fips-mode

router(config)#commit
```

Issue the following command to disable FIPS mode on the 8800-LC-48H line card.

```
router(config)# no hw-module macsec-fips-post location {location | all}

router(config)#commit
```

Note: On reload the device will be in a non-FIPS Approved Mode of Operation.

```
router(config)#reload location all
```

3.3 Verify FIPS Mode of Operation

Use the command lines to display the FIPS configuration information. The router CLI output shows running status for FIPS mode of operation.

```
RP/0/RP0/CPU0:router#show logging | include fips

Wed Mar 25 21:09:30.384 UTC

RP/0/RP0/CPU0:Mar 25 14:38:36.509 UTC: locald_DLRSC[353]: %SECURITY-LOCALD-6-LOCAL_CMD_ACCT : CLI CMD:
"crypto fips-mode" by admin from TTY /dev/pts/0 console
```

To display the FIPS mode on the 8800-LC-48H line card, use the following command.

```
router(config)# show hw-module macsec-fips-post [ location {location | all}]
```

Example

```
Router#show hw-module macsec-fips-post location all
Wed Jun 17 09:36:31.932 UTC

Location       Configured     Applied          Action
--------------------------------------------------------------
0/0/CPU0       NO             NO               NONE
0/11/CPU0      YES            NO               RELOAD
```

After location reload:

```
Router#show hw-module macsec-fips-post location all
Wed Jun 17 10:03:57.263 UTC

Location       Configured     Applied          Action
--------------------------------------------------------------
0/0/CPU0       NO             NO               NONE
0/11/CPU0      YES            YES              NONE
```

3.4 Transition of module to and from Approved mode of Operation (FIPS mode)

The keys and CSPs generated by the cryptographic module during FIPS mode of operation cannot be used when the module transitions to non-FIPS mode and vice versa. While the module transitions from FIPS to non-FIPS mode or from non-FIPS to FIPS mode, all the keys and CSPs are to be zeroized by the Crypto Officer.

For transition from FIPS to non-FIPS mode, the Crypto Officer had to zeroize the module to delete all plaintext secret and private cryptographic keys and CSPs as defined in the Table 7 of this non-proprietary FIPS 140-2 Security Policy document and the Crypto Officer had to issue “no crypto fips-mode” command in addition to those defined in Table 7 of this document.