Cisco Catalyst 8300 Series Edge Platforms
FIPS 140-2 Non-Proprietary Security Policy
Level 1 Validation

Firmware Version:

IOS-XE 17.3

Hardware Version:

C8300-1N1S-6T, C8300-1N1S-4T2X, C8300-2N2S-6T, C8300-2N2S-4T2X

Network Interface Module Version:

C-NIM-1X

Document Version 0.4
January 20, 2023

Table of Contents

List of Tables

1 Introduction

This is a non-proprietary cryptographic module Security Policy for Cisco Catalyst 8300 Series Edge Platforms; referred to in this document as “C8300” or the “modules”. This security policy describes how the modules meet the security requirements of FIPS 140-2 Level 1 and how to run the modules in a FIPS 140-2 mode of operation. This document 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:

https://csrc.nist.gov/groups/STM/cmvp/index.html.

1.1 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 modules from the following sources:

- The Cisco Systems, Inc. website (http://www.cisco.com) contains information on the full line of products from Cisco
- The National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) website (https://csrc.nist.gov/groups/STM/cmvp/index.html) contains contact information for answers to technical or sales-related questions for the modules

1.2 FIPS 140-2 Submission Package

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

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

This document provides an overview of the Cisco Catalyst 8300 Series Edge Platforms and explains the secure configuration and operation of the modules. This introduction section is followed by Section 2 through Section 8, which details the general features and functionality of the appliances. Section 9 specifically addresses the required configuration for the FIPS-mode of operation.

Except for 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, Inc.

2 Modules Description

2.1 Cisco C8300 (C8300-1N1S-6T, C8300-1N1S-4T2X, C8300-2N2S-6T, C8300-2N2S-4T2X)

The Cisco C8300 (C8300-1N1S-6T, C8300-1N1S-4T2X, C8300-2N2S-6T, and C8300-2N2S-4T2X) revolutionize WAN communications in the enterprise branch. With new levels of built-in intelligent network capabilities and convergence, it specifically addresses the growing need for application-aware networking in distributed enterprise sites. These locations tend to have lean IT resources. But they often also have a growing need for direct communication with both private data centers and public clouds across diverse links, including Multiprotocol Label Switching (MPLS), VPNs, and the Internet.

Cisco C8300 family of routers provide you with Cisco® Software Defined WAN (SDWAN) software features and a converged branch infrastructure. Along with superior throughput, these capabilities form the building blocks of next-generation branch-office WAN solutions.

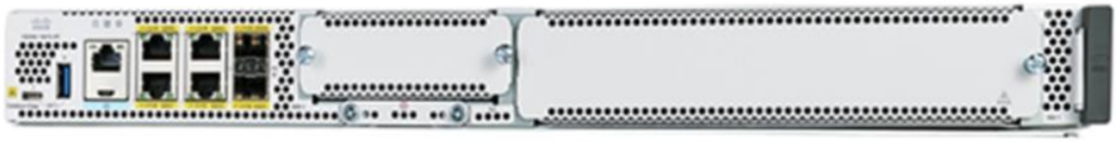

Figure 1 – Front Cisco C8300-1N1S-6T

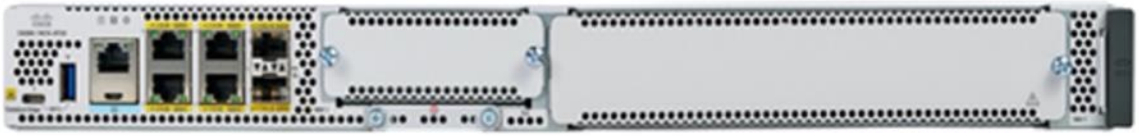

Figure 2 – Front Cisco C8300-1N1S-4T2X

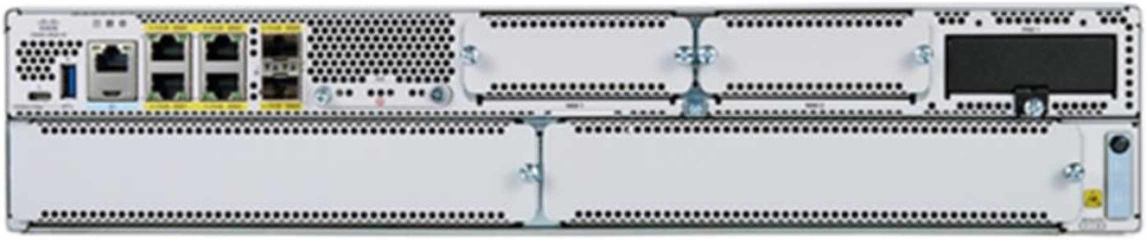

Figure 3 – Front Cisco C8300-2N2S-6T

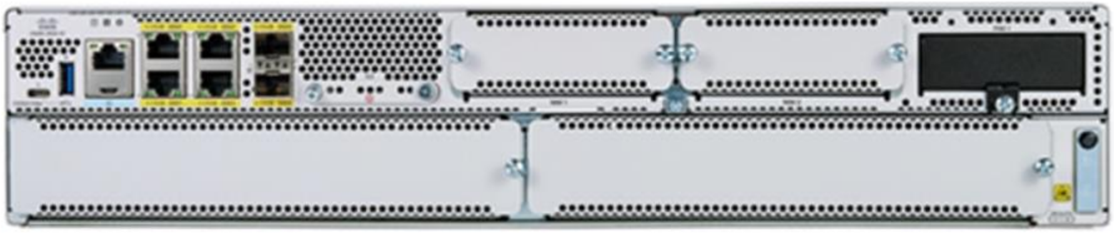

Figure 4 – Front Cisco C8300-2N2S-4T2X

The back panel of the modules contains the fan and power supply. Detailed pictures showing the ports and interfaces on the front and back of the modules is available in Section 4 below.

2.2 Network Interface Module (C-NIM-1X)

The C-NIM-1X Network Interface Module (NIM) is a software-configurable high-speed connectivity routing port network interface module for the Cisco Catalyst 8300 Series Edge Platforms. The network interface module provides increased density of ethernet interfaces on the Cisco C8300 routers. The C-NIM-1X has a Broadcom BCM82757 processor and is required to support MACsec communications. Figure 9 shows the network interface module.

Figure 5 - C-NIM-1X NIM

2.3 Tested Configurations

Table 1 below lists components included in the validated configuration.

Table 1 - Validated Configuration Components

Category	Configuration Item
Hardware`	C8300-1N1S-6T • Intel Xeon D-1563N (Broadwell)
	C8300-1N1S-4T2X • Intel Xeon D-1573N (Broadwell)
	C8300-2N2S-6T • Intel Xeon D-2148NT (Skylake)
	C8300-2N2S-4T2X with an

Category	Configuration Item
	- Intel Xeon D-2168NT (Skylake)
	C-NIM-1X - MACsec support - Broadcom BCM82757 processor
Firmware	IOS-XE 17.3
Cryptographic Library	IC2Mrel5a

2.4 FIPS and non-FIPS modes of operation

The modules support a FIPS and non-FIPS mode of operation. The non-FIPS mode of operation is not a recommended operational mode; however, because the modules allow for non-approved algorithms and non-approved key sizes, a non-approved mode of operation exists. Table 2 below lists protocols available within the modules and indicates the mode of operation where the protocol is available.

Table 2 - Protocol Availability

Protocol	FIPS	non-FIPS
SSH	✓	✓
IPsec	✓	✓
SNMPv3	✓	✓
MACsec	✓	✓
TLS		✓

A protocol used in a non-FIPS mode is non-compliant.

If the device is in the non-FIPS mode of operation, the Cryptographic Officer (CO) must follow instructions provided in Section 9 of this Security Policy to transition the modules into a FIPS-Approved mode of operation. The FIPS-Approved mode supports the approved and allowed algorithms, functions and protocols identified in Section 7 of this document. The FIPS-Approved mode of operation is entered when the modules is configured for FIPS mode (detailed in Section 9) and all power-on self-tests (POST) pass successfully.

2.5 Modules Validation Level

Table 3 below lists the level of validation for each area in this SP as it relates to FIPS PUB 140-2.

Table 3 - Module 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

No.	Area Title	Level
6	Operational Environment	N/A
7	Cryptographic Key management	1
8	Electromagnetic Interface/Electromagnetic Compatibility	1
9	Self-Tests	1
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A
Overall	**Overall module validation level**	**1**

3 Cryptographic Boundary

The cryptographic boundary for the Cisco C8300-1N1S-6T, C8300-1N1S-4T2X, C8300-2N2S-6T, and C8300-2N2S-4T2X is defined as encompassing the "top," "bottom," "front," "back," "left" and "right" surfaces of the case. Included in this physical boundary is the Cisco TRNG Core (Entropy Source Validation (ESV) certificate #E4) entropy source. The entropy source is used solely to seed the IC2M DRBG. All raw noise is conditioned using a SHA2-256 vetted conditioning function. See Table 13 below for the applicable CAVP certificate[1]. A raw entropy value of at least 0.25 bits of min entropy per bit of data is claimed for the Cisco TRNG Core entropy source. The output of the SHA2-256 conditioning function contains 256 bits of data per 256-bit block.

4 Cryptographic Module Ports and Interfaces

The modules provide physical and logical interfaces to the device. 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.

Figure 6 and Table 4 below provide a mapping of physical interfaces to logical interfaces for the front of the C8300-1N1S-6T and C8300-1N1S-4T2X.

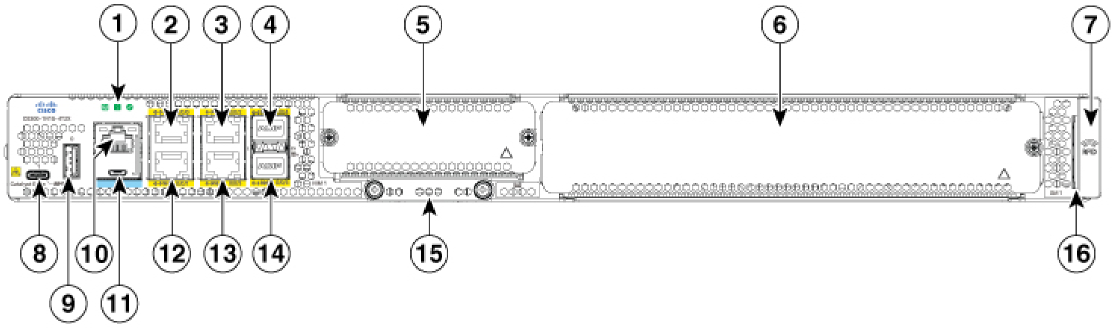

Figure 6 - Front - C8300-1N1S-6T/C8300-1N1S-4T2X

Table 4 – Front - Physical to Logical Interface Mapping - C8300-1N1S-6T/C8300-1N1S-4T2X

#	Physical Interfaces	FIPS 140-2 Logical Interfaces
1	LED	Status Output
2	RJ-45 Gigabit (Gb) Ethernet port (1G 0/0/0)	Data Input/Output Control Input/Status Output
3	RJ-45 Gigabit Ethernet port (1G 0/0/2)	Data Input/Output Control Input/Status Output

[1] The CAVP certificate contains algorithms that are not used by the module and are out of scope for this validation.

#	Physical Interfaces	FIPS 140-2 Logical Interfaces
4	SFP+/10 Gigabit Ethernet port (10G 0/0/4) ports SFP/1 Gigabit Ethernet port (1G 0/0/4) ports	Data Input/Output Control Input/Status Output
5	NIM Slot1	N/A
6	SM Slot 1	N/A
7	RFID (Optional)	N/A
8	USB Type C (3.0) (USB 1)	N/A
9	USB Type A (3.0) (USB 0)	N/A
10	RJ-45 Console port	Control Input/Status Output
11	Micro-USB Console port	Control Input/Status Output
12	RJ-45 Gigabit Ethernet port (1G 0/0/1)	Data Input/Output Control Input/Status Output
13	RJ-45 Gigabit Ethernet port (1G 0/0/3)	Data Input/Output Control Input/Status Output
14	SFP+/10 Gigabit Ethernet port (10G 0/0/5) for C8300-1N1S-6T SFP/1 Gigabit Ethernet port (1G 0/0/5) for C8300-1N1S-4T2X	Data Input/Output Control Input/Status Output
15	M.2 USB/NVMe storage	N/A
16	Device Label Tray	N/A

Figure 7 and Table 5 below provide a mapping of physical interfaces to logical interfaces for the back of the C8300-1N1S-6T and C8300-1N1S-4T2X.

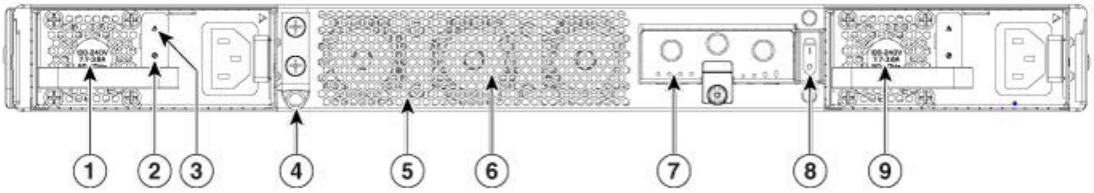

Figure 7 – Back - C8300-1N1S-6T/C8300-1N1S-4T2X

Table 5 - Back - Physical to Logical Interface Mapping - C8300-1N1S-6T/C8300-1N1S-4T2X

#	Physical Interfaces	FIPS 140-2 Logical Interfaces
1	AC/DC power supply unit (PSU1	Power Supply
2	Power, Preset, OK, LED	Status Output
3	ALARM Fail LED	Status Output
4	Ground lug	N/A
5	Fan tray vent	N/A
6	3-Internal Fan tray	N/A
7	PIM Slot 1	N/A
8	Power Switch	Control Input
9	AC/DC Power Supply Unit (PSU0)	Power Supply

Figure 8 and Table 6 below provide a mapping of physical interfaces to logical interfaces for the front of the C8300-2N2S-6T and C8300-2N2S-4T2X.

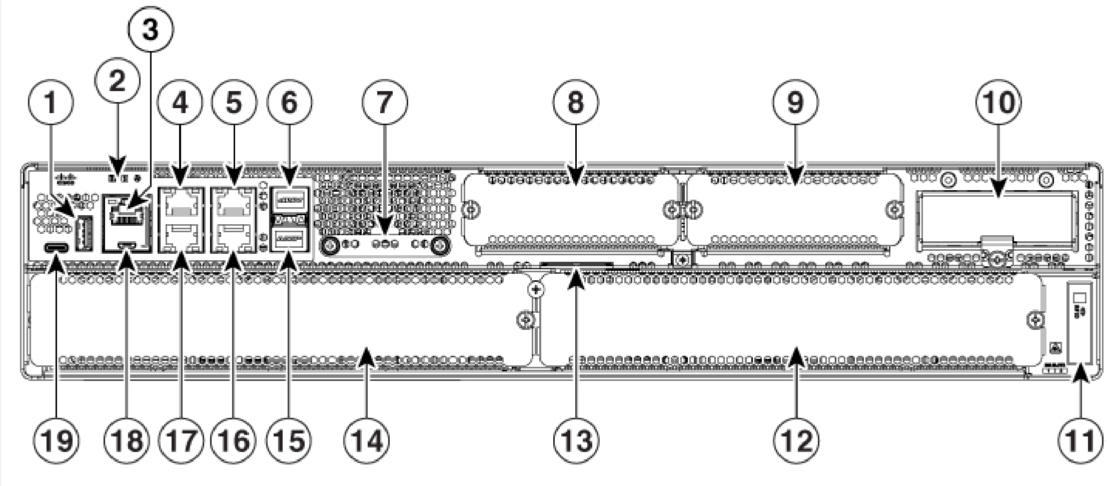

Figure 8 – Front - C8300-2N2S-6T/C8300-2N2S-4T2X

Table 6 - Front - Physical to Logical Interface Mapping - C8300-2N2S-6T/C8300-2N2S-4T2X

#	Physical Interfaces	FIPS 140-2 Logical Interfaces
1	USB Type A (3.0) (USB 0)	N/A
2	LED	Status Output
3	RJ-45 Console port	Control Input/Status Output
4	RJ-45 Gigabit Ethernet port (1G 0/0/0)	Data Input/Output Control Input/Status Output
5	RJ-45 Gigabit Ethernet port (1G 0/0/2)	Data Input/Output Control Input/Status Output
6	SFP+/10 Gigabit Ethernet port (10G 0/0/4) for C8300-2N2S-6T SFP/1 Gigabit Ethernet port (1G 0/0/4) for C8300-2N2S-4T2X	Data Input/Output Control Input/Status Output
7	NIM Slot1 M.2 USB/NVMe storage	N/A
8	NIM Slot 1	N/A
9	NIM Slot 2	N/A
10	PIM Slot 1	N/A
11	RFID (Optional)	N/A
12	SM Slot 2	N/A
13	Device Label Tray	N/A
14	SM Slot 1	N/A
15	SFP+/10 Gigabit Ethernet port (10G 0/0/5) for C8300-2N2S-6T SFP/1 Gigabit Ethernet port (1G 0/0/5) for C8300-2N2S-4T2X	Data Input/Output Control Input/Status Output
16	RJ-45 Gigabit Ethernet port (1G 0/0/3)	Data Input/Output Control Input/Status Output
17	RJ-45 Gigabit Ethernet port (1G 0/0/1)	Data Input/Output Control Input/Status Output
18	Micro-USB Console	Control Input/Status Output
19	USB Type C (3.0) (USB 1)	N/A

Figure 9 and Table 7 below provide a mapping of physical interfaces to logical interfaces for the back of the C8300-2N2S-6T and C8300-2N2S-4T2X.

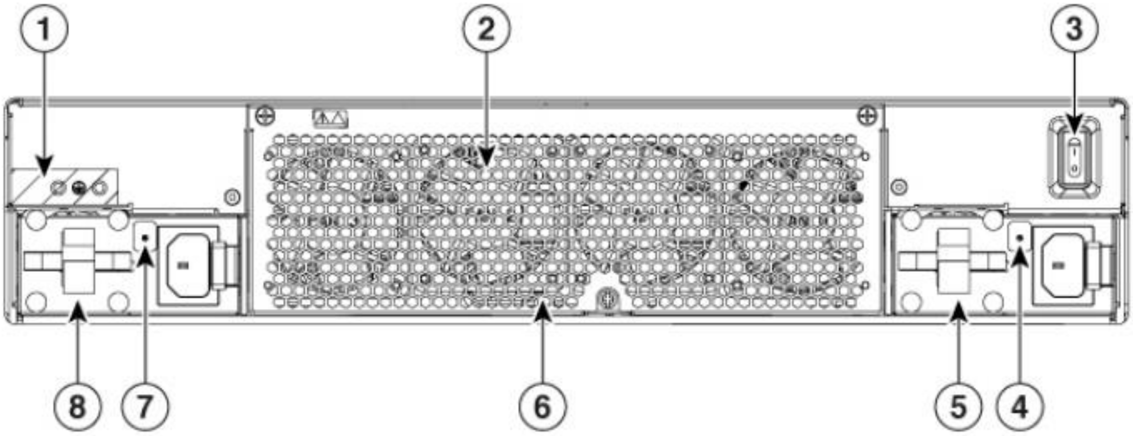

Figure 9 – Back - C8300-2N2S-6T/C8300-2N2S-4T2X

Table 7 – Back - Physical to Logical Interface Mapping - C8300-2N2S-6T/C8300-2N2S-4T2X

#	Physical Interfaces	FIPS 140-2 Logical Interfaces
1	Ground Lug	N/A
2	FRU Fan tray	N/A
3	Power Switch	Control Input
4	PSU0 Power LED	Status Output
5	PSU0	Power Supply
6	POE Power Module 0/1, behind removable Fan tray	N/A
7	PSU1 Power LED	Status Output
8	PSU1	Power Supply

Figure 9 and Table 7 above provide a mapping of physical interfaces to logical interfaces for the C-NIM-1X.

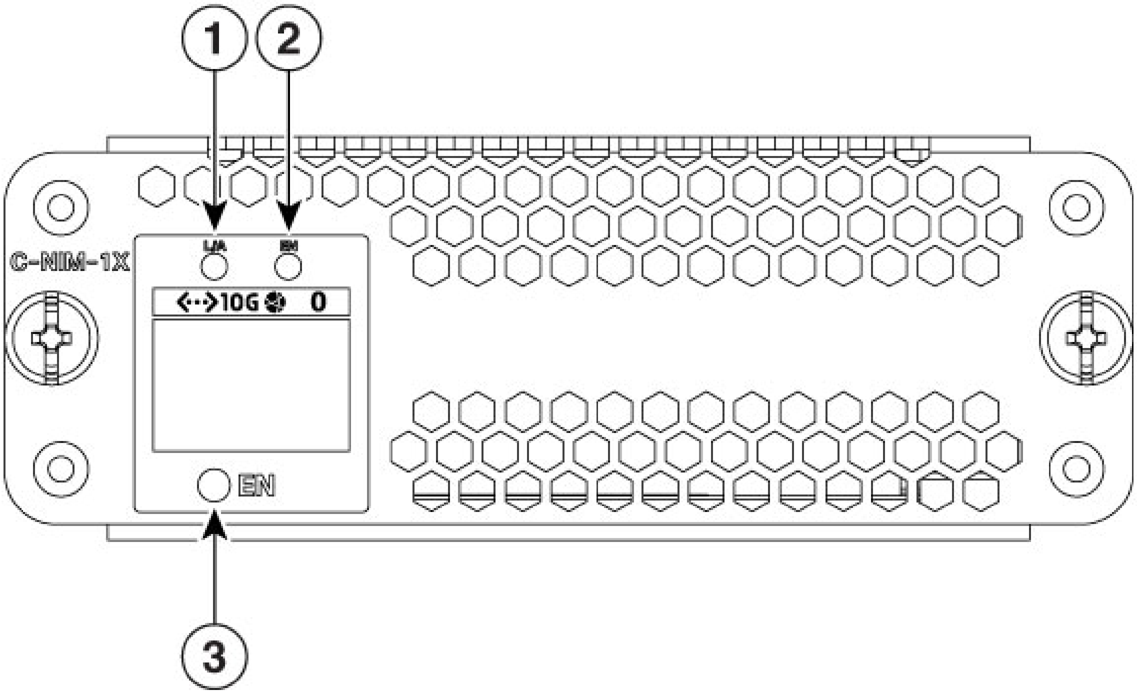

Figure 10 – Front - C-NIM-1X

Table 8 – Front - Physical to Logical Interface Mapping - C-NIM-1X

#	Physical Interfaces	FIPS 140-2 Logical Interfaces
1	Link LED	Status Output
2	SFP LED	Status Output
3	Power LED	Status Output
4	SFP+/10 Gigabit Ethernet port	Data Input/Output Control Input

5 Roles, Services, and Authentication

The modules support identity-based authentication. In FIPS-Approved mode, operators may assume the following roles:

- **User Role** - This role performs general security services including cryptographic operations and other approved security functions. The product documentation refers to this role as a management user with level 1 privilege.
- **CO Role** - This role performs the cryptographic initialization and management operations. It performs the loading of optional certificates and key-pairs and the zeroization of the modules. The product documentation refers to this role as a management user with level 15 privilege.

The modules do not support a Maintenance Role.

5.1 User Services

Table 9 below lists all User role services available within the module.

Table 9 - User Services (r = read, w = write, d = delete)

Services & Access	Description	Keys & CSPs
System Status	The LEDs show the network activity ("Green" if the interfaces are up and running, "Flashing yellow" if the interfaces are coming up and no LED activity when there is no connection to the network interfaces), overall operational status ("Red" indicates module failure and "Green" indicates that module is operational).	N/A
Random Number Generation	Key generation and seeds for asymmetric key generation	DRBG entropy input, DRBG seed, DRBG v, DRBG Key – r, w, d
Key Exchange	Key exchange over Diffie-Hellman and EC Diffie-Hellman	Diffie-Hellman public key, Diffie-Hellman private key, Diffie-Hellman shared secret, EC Diffie-Hellman Public Key, EC Diffie-Hellman Private Key, EC Diffie-Hellman shared secret – w, d
Module Read-only Configuration	Viewing of configuration settings	N/A

5.2 Crypto Officer Services

Table 10 below lists all CO role services available within the module.

Table 10 - Crypto Officer Services (r = read, w = write, d = delete)

Services & Access	Description	Keys & CSPs
Self-Test and Initialization	Cryptographic algorithm tests, firmware integrity tests, module initialization.	N/A (No keys are accessible)

Services & Access	Description	Keys & CSPs
System Status	The LEDs show the network activity (“Green” if the interfaces are up and running, “Flashing yellow” if the interfaces are coming up and no LED activity when there is no connection to the network interfaces), overall operational status (“Red” indicates module failure and “Green” indicates that module is operational) and the command line “status commands” output system status (“show fips” command would result in indicating whether the module is in FIPS mode or not).	N/A (No keys are accessible)
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
Random Number Generation	Key generation and seeds for asymmetric key generation	DRBG entropy input, DRBG seed, DRBG v, DRBG Key – r, w, d
Key Exchange	Key exchange over Diffie-Hellman and EC Diffie-Hellman	Diffie-Hellman public key, Diffie-Hellman private key, Diffie-Hellman shared secret, EC Diffie-Hellman Public Key, EC Diffie-Hellman Private Key, EC Diffie-Hellman shared secret – w, d
Zeroization	Zeroize CSPs and cryptographic keys by cycling power to zeroize all cryptographic keys stored in DRAM. The CSPs stored in Flash can be zeroized by overwriting with a new value.	All Keys and CSPs will be destroyed – d
Module Configuration	Selection of non-cryptographic configuration settings	N/A
Power Cycle	Reboot/reloading the module	All ephemeral Keys and CSPs will be destroyed - d
Secured Dataplane	Secure communications at data link layer between module and peer device using MACsec.	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) – r, w, d

Services & Access	Description	Keys & CSPs
IPsec	Secure communications between module and a client.	skeyid, skeyid_d, IKE session encryption key, IKE session authentication key, IKE RSA private key, IKE RSA public key, IPSec session encryption key, IPSec session authentication key, IPSec authentication key, IPSec encryption key, ISAKMP preshared – r, w, d
SNMPv3	Non-security related monitoring by the CO using SNMPv3	snmpEngineID, SNMPv3 Password, SNMP session key – w, d
SSH	Establishment and subsequent data transfer of a SSH session for use between the module and the CO.	SSH encryption key, SSH integrity key, SSH RSA private key – r, w, d
Firmware loading	Loads the Cisco firmware and performs an integrity test using an RSA digital signature.	Integrity Test public key – r, w, d

Table 11: Crypto Officer Services (r = read, w = write, d = delete)

5.3 User and CO Authentication

The CO role is assumed by an authorized CO connecting to the modules via CLI, SSH and GUI. The OS prompts the CO for a username and password. If the password is validated against the password stored in memory, the CO is authenticated and allowed to execute CO services. Each username is unique and configurable by the CO. The password feedback mechanism does not provide information that could be used to determine the authentication data. The User role monitors the modules via CLI and SSH.

5.3.1 Password Based Authentication

The CO and User passwords and all shared secrets must each be at least eight (8) characters long. Passwords must include at least one (1) special character and at least one (1) number, along with six additional characters taken from the 26 upper case, 26 lower case, 10 numbers and 32 special characters. Password requirements are enforced by policy. See Section 9 below for more information.

If six (6) special/alpha/number characters, one (1) special character and one (1) alphabet are used without repetition for an eight (8) character long, the probability of randomly guessing the correct sequence is one (1) in 164,290,949,222,400 (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.

Since it is claimed to be for 8 digits with no repetition, then the calculation should be 32x10x92x91x90x89x88x87). Therefore, for each attempt to use the authentication mechanism, the associated probability of a successful random attempt is approximately 1 in 164,290,949,222,400, which is less than the 1 in 1,000,000 required by FIPS 140-2.

The maximum number of possible attempts per minute is 5 for Password Authentication via console. Therefore, the probability of a success with multiple consecutive attempts in a one-minute period is 5/164,290,949,222,400 which is less than the 1 in 100,000 required by FIPS 140-2.

The modules only support sixteen (16) concurrent SSH sessions and maximum number of possible attempts per minute is 8 for each SSH session. Therefore, the probability of a success with multiple consecutive attempts in a one-minute period is (8*16)/ 164,290,949,222,400 which is less than the 1 in 100,000 required by FIPS 140-2.

The modules support three hundred (300) concurrent GUI sessions and the maximum number of possible attempts per minute is 10 for Password Authentication for each GUI session. Therefore, the probability of a success with multiple consecutive attempts in a one-minute period is (10*300)/164,290,949,222,400 which is less than the 1 in 100,000 required by FIPS 140-2.

5.3.2 SSH Public-key Authentication

The CO and User role also supports public key authentication for remotely accessing the modules via SSH. RSA has modulus size of 2048 bit, thus providing 112 bits of strength. 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 10 Gb/s. Hence, at most $10 \times 10^9 \times 60s = 6 \times 10^{11}$ = 600,000,000,000 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:

$$1:(2^{112} \text{ possible keys}/(6 \times 10^{11} \text{ bits per minute})/112 \text{ bits per key}))$$
$$1:(2^{112} \text{ possible keys}/5{,}357{,}142{,}857 \text{ keys per minute})$$
$$1:9.7\times10^{23}$$

Therefore, the associated probability of a successful random attempt for a minute is approximately 1 in 9.7×10^{23}, which is less than the 1 in 100,000 required by FIPS 140-2.

5.4 Unauthenticated User Services

Following are services available to an Unauthenticated Operator:

- **View system status:** An Unauthenticated Operator may observe the system status by viewing the LEDs on the modules, which show network activity and overall operational status. The Unauthenticated Operator can also view boot up/power-on self-test logs on the console port, which does not disclose any security relevant information
- **Power Cycle:** An Unauthenticated Operator can power cycle the modules. Once the power-on self-tests have completed successfully, the modules return to an operational state. This state is indicated by a solid green LED

The modules do not support a bypass capability.

6 Cryptographic Key/CSP Management

The modules securely administer both cryptographic keys and other critical security parameters, such as passwords. All keys and CSPs are protected by the password-protection of the CO role login and can be zeroized by the CO. Zeroization consists of overwriting the memory that stored the key or refreshing the volatile memory. Keys are exchanged and entered electronically via Internet Key Exchange (IKE) or SSH.

Table 12 below lists all keys and critical security parameters (CSPs) supported by the modules.

Table 12 - Keys and CSPs

Key/CSP Name	Algorithm	Description	Key Size	Storage	zeroization
DRBG entropy input	SP 800-90A CTR_DRBG	HW-based entropy source output used to construct seed.	256-bits	DRAM	Power cycle
DRBG seed	SP 800-90A CTR_DRBG	Input to the DRBG that determines the internal state of the DRBG. Generated using DRBG derivation function that includes the entropy input from a hardware-based entropy source.	384 bits	DRAM	Power cycle
DRBG V	SP 800-90A CTR_DRBG	Internal V value used as part of SP 800-90A CTR_DRBG.	128 bits	DRAM	Power cycle
DRBG Key	SP 800-90A CTR_DRBG	This is the 256-bit DRBG key used for SP 800-90A CTR_DRBG.	256 bits	DRAM	Power cycle
Diffie-Hellman public key	Diffie-Hellman	The public key used in Diffie-Hellman (DH) Exchange.	2048-4096 bits	DRAM	Power cycle
Diffie-Hellman private key	Diffie-Hellman	The private key used in Diffie-Hellman (DH) Exchange.	224-379 bits	DRAM	Power cycle
Diffie-Hellman shared secret	Diffie-Hellman	The shared exponent used in Diffie-Hellman (DH) exchange. Created per the Diffie-Hellman protocol.	2048-4096 bits	DRAM	Power cycle
EC Diffie-Hellman public key	Diffie-Hellman (Groups 19, 20 and 21)	P-256, P-384 and P-521 public key used in EC Diffie-Hellman exchange. This key is derived per the Diffie-Hellman key agreement.	P-256, P-384 and P-521	DRAM (plaintext)	Power cycle
EC Diffie-Hellman private key	Diffie-Hellman (Groups 19, 20 and 21)	P-256, P-384 and P-521 private key used in EC Diffie-Hellman exchange. Generated by calling the SP 800-90A CTR-DRBG.	P-256, P-384 and P-521	DRAM (plaintext)	Power cycle

Key/CSP Name	Algorithm	Description	Key Size	Storage	zeroization
EC Diffie-Hellman shared secret	Diffie-Hellman (Groups 19, 20 and 21)	P-256, P-384 and P-521 shared secret derived in EC Diffie-Hellman exchange	P-256, P-384 and P-521	DRAM (plaintext)	Power cycle
Operator password	Password, at least eight characters	The password of the operator. This CSP is entered by the Cryptographic Officer	Variable (8+ characters)	Flash (plaintext)	Overwrite with new password
Enable Password	Password, at least eight characters	The password of the operator. This CSP is entered by the Cryptographic Officer.	Variable (8+ characters)	Flash (plaintext)	Overwrite with new password
Enable secret	Password, 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 Cryptographic Operator optionally configures the module to obfuscate the Enable password. This CSP is entered by the Cryptographic Officer.	Variable (8+ characters)	Flash (plaintext)	Overwrite with new secret
SKEYSEED	HMAC	Shared secret known only to IKE peers. Used to derive IKE session keys. Derived by using key derivation function defined in SP800-135 KDF (IKEv2).	160-384 bits	DRAM (plaintext)	Power cycle
Skeyid	HMAC	It was derived by using 'IKE pre-shared' and other non-secret values through the key derivation function defined in SP800-135 KDF (IKEv2).	160-384 bits	DRAM (plaintext)	Power cycle
skeyid_d	HMAC	It was derived by using skeyid, Diffie-Hellman shared secret and other non-secret values through key derivation function defined in SP800-135 KDF (IKEv2).	160-384-bits	DRAM (plaintext)	Power cycle

Key/CSP Name	Algorithm	Description	Key Size	Storage	zeroization
IKE session encryption key	AES-CBC, AES-GCM	The IKE session encrypt key is derived by using key derivation functions defined in SP800-135 KDF (IKEv2). Used for IKE payload protection.	AES-CBC (128-bit, 192-bit, 256-bit) AES-GCM (128-bit, 256-bit)	DRAM (plaintext)	Power cycle
IKE session authentication key	HMAC	The IKE session) authentication key is derived by using key derivation functions defined in SP800-135 KDF (IKEv2). Used for payload integrity verification.	160-512 bits	DRAM (plaintext)	Power cycle
IKE public key	RSA	This key generated by calling the SP 800-90A CTR-DRBG.	2048/3072/4096 bits	Flash (plaintext)	Overwrite with new key or use "crypto key zeroize rsa"
IKE private key	RSA	This key generated by calling the SP 800-90A CTR-DRBG.	2048/3072/4096 bits	Flash (plaintext)	Overwrite with new key or use "crypto key zeroize rsa"
IKE pre-shared	Shared secret	This shared secret was manually entered by CO for IKE pre-shared key-based authentication mechanism.	8 chars	Flash (plaintext)	Overwrite with new secret or use "no crypto isakmp key" command zeroizes it.
IPSec authentication key	HMAC	The IPsec authentication key is derived using the KDF defined in SP800-135 KDF (IKEv2). Used to authenticate the IPSec peer.	160 – 512 bits	DRAM (plaintext)	Automatically when IPsec session terminated or during Power Cycle.

Key/CSP Name	Algorithm	Description	Key Size	Storage	zeroization
IPSec encryption key	AES-CBC, AES-GCM, .	The IPsec encryption key is derived using key derivation function defined in SP800-135 KDF (IKEv2). Used to Secure IPSec traffic.	AES-CBC (128-bit, 192-bit, 256-bit) AES-GCM (128-bit, 256-bit)	DRAM (plaintext)	Automatically when IPsec session terminated or during power cycle.
snmpEngineID	Shared secret	Unique string to identify the SNMP engine.	32-bits	Flash (plaintext)	Overwrite with new engine ID
SNMPv3 Password	Shared Secret	This secret is used to derive HMAC-SHA1 key for SNMPv3 Authentication.	32 bytes	Flash (plaintext)	Overwrite with new password
SNMPv3 session key	AES-CFB	Encrypts SNMPv3 traffic.	128-bit	DRAM (plaintext)	Power cycle
SSH Encryption Key	AES-GCM and AES-CBC	Symmetric AES key for encrypting SSH.	AES-CBC (128-bit, 192-bit, 256-bit) AES-GCM (128-bit, 256-bit)	DRAM (plaintext)	Power cycle
SSH Integrity Key	HMAC	Used for SSH integrity protection.	SHA2-256 and SHA2-512 bits	DRAM (plaintext)	Power cycle

Key/CSP Name	Algorithm	Description	Key Size	Storage	zeroization
SSH Public/Private Key Pair	RSA	PKCS#1 v.1.5 generated by calling the SP 800-90A CTR-DRBG.	MOD 2048/3072/4096	Flash (plaintext)	SSH private/public key is zeroized by either deletion (via # crypto key zeroize rsa) or by overwriting with a new value of the key.
MACsec Connectivity Association Key (CAK)	Hex string	A CO configured pre-shared secret key possessed by members of a MACsec connectivity association to secure control plane traffic.	16 or 32 bytes	NVRAM (plaintext)	Overwritten with new a key.
MACsec Integrity Check Key (ICK)	AES-GCM	Used to prove an authorized peer sent the message. Derived from the CAK using the SP800-108 KDF.	128/256 bits	DRAM (plaintext)	Automatically when session expires or power cycle.
MACsec Key Encryption Key (KEK)	AES-CMAC	Used to transmit Security Association Key (SAK) to other peers of a MACsec connectivity association. Derived from the CAK using the SP800-108 KDF.	128/256 bits	DRAM (plaintext)	Automatically when session expires or power cycle.
MACsec Security Association Key (SAK)	AES-GCM	Derived from the CAK and used by the device network ports for securing User network traffic.	128-, 256-bits	DRAM (plaintext)	Automatically when session expires or power cycle

7 Cryptographic Algorithms

7.1 Approved Cryptographic Algorithms

Cryptographic operations are supported by the following:

- **Firmware:** IC2Mrel5a
- **Hardware:** Broadcom BCM82757

The modules support many different cryptographic algorithms. However, only FIPS-Approved algorithms are used while in the FIPS-Approved mode of operation. Table 13 below lists FIPS-Approved algorithms implemented in the modules.

Table 13 - FIPS-Approved Algorithms

Algorithm[2]	Supported Mode	Cert. #
IC2Mrel5a		
AES	ECB (128, 192, 256); CBC (128, 192, 256); CFB128 (128, 192, 256), GCM (128, 192, 256), CMAC (128, 256).	A1462
SP800-108 (KBKDF)	KDF Mode: Counter MAC Mode: HMAC-SHA-1	
SP800-135 (CVL)	IKEv2 KDF, SSH KDF, SNMP KDF Note: The IKEv2, SSH, and SNMP protocols have not been reviewed or tested by the CAVP and CMVP.	
DRBG	CTR (using AES-256)	
ECDSA	Key Generation (P-256, P-384, P-521) Key Verification (P-256, P-384) Signature Generation (P-256 with SHA2-256 and P-384 with SHA2-384) Signature Verification (P-256 with SHA2-256 and P-384 with SHA2-384)	
HMAC	SHA-1, SHA2-256, SHA2-384, SHA2-512	
RSA	RSA Key Generation (2048 w/SHA2-256, 3072 w/SHA2-256 and 4096 w/SHA2-256) PKCS 1.5: 2048-4096 bit key RSA Signature Generation 2048 w/ SHA2-256/384/512, 3072 w/SHA2-256/384/512 and 4096 w/SHA2-256/384/512) RSA Signature Verification (2048 w/ SHA1, SHA2-256/384/512, 3072 w/ SHA1, SHA2-256/384/512 and 4096 w/ SHA1, SHA2-256/384/512)	
SHS	SHA-1, SHA2-256, SHA2-384, SHA2-512	

[2] Not all algorithms/modes tested on the CAVP validation certificates are implemented in the module.

Algorithm[2]	Supported Mode	Cert. #
KAS-SSC (SP800-56Arev3)	KAS FFC SSC: Mod Sizes: FB, FC, modp-2048, modp-3072, modp-4096 Scheme: dhEphem KAS ECC SSC: Curves: P-256, P-384, P-521 Scheme: Ephemeral Unified	
CKG (SP800-133rev2)	Vendor Affirmed	
SP800-90B ENT	Physical Noise Source	E4
Broadcom BCM82757/ C-NIM-1X		
AES	GCM (128, 256)	4550
Tam 2.0 (Vetted conditioning function for Cisco TRNG Core)		
SHS	SHA2-256	C2181

NOTES:

1. KTS (AES-GCM Cert. #A1462; key establishment methodology provides 128 or 256 bits of encryption strength)
2. KTS (AES-CBC Cert. #A1462 and HMAC Cert. #A1462; key establishment methodology provides between 128 and 256 bits of encryption strength)
3. KTS (AES-GCM Cert. #4550; key establishment methodology provides 128 or 256 bits of encryption strength).
4. KAS-SSC (Cert. #A1462; key establishment methodology provides between 112 and 256 bits of encryption strength for KAS-ECC-SSC and 112 and 200 bits of encryption strength for KAS-FFC-SSC).
5. The modules' AES-GCM implementations conforms to IG A.5 Provision #1 following RFC 7296 for IPSec/IKEv2. The AES GCM IV is generated according to RFC5282 and RFC4106 and is used only in the context of the IPSec/IKEv2 protocol as allowed in IG A.5. The modules use RFC 7296 compliant IKEv2 to establish the shared secret SKEYSEED from which the AES GCM encryption keys are derived. Method ii) was used by the tester to demonstrate the modules' compliance with the IPSec provision for the AES GCM IV generation in IG A.5. The restoration of the IV is in accordance with scenario 3 in IG A.5 in that a new AES GCM key is established. 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 modules' power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established which is in accordance with scenario 3 in IG A.5.
6. For the SSH Encryption GCM key, the IV construction is in accordance with RFC 5647 Section 7. A 96-bit IV is constructed using a 32-bit fixed field and a 64-bit invocation counter field. The invocation field is treated as a 64-bit integer and is incremented after each invocation of AES-GCM to process a binary packet. A 32-bit block counter is also used. The counter is initially set to 1 and incremented as

each keystream block of 128-bits is produced. The counter portion of the IV is set by the module within its cryptographic boundary. The use of AES GCM for SSH meets FIPS 140-2 IG A.5 scenario #4.

7. The AES GCM IV is generated internally in the cryptographic modules 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 modules lose power, then new AES GCM keys should be established. The modules 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.
8. CVL Cert. #A1462 support the KDF (key derivation function) used in each of IKEv2, SSH and SNMPv3 protocols. IKEv2, SSH and SNMPv3 protocols have not been reviewed or tested by the CAVP and CMVP. Please refer IG D.11, bullet 2 for more information.
9. CKG (vendor affirmed) Cryptographic Key Generation; SP 800-133rev2. In accordance with FIPS 140-2 IG D.12, the cryptographic modules perform Cryptographic Key Generation as per scenario 1 of section 4 in SP800-133rev2. The resulting generated symmetric key and the seed used in the asymmetric key generation are the unmodified output from SP800-90A DRBG.
10. There are algorithms, modes, and keys that have been CAVP tested but not implemented by the module. Only the algorithms, modes/methods, and key lengths/curves/moduli shown in this table are implemented by the module.

7.2 Non-Approved Algorithms allowed for use in FIPS-mode

The module supports the following non-approved, but allowed cryptographic algorithms:

- RSA[3] (key wrapping; key establishment methodology provides between 112 and 132 bits of encryption strength. RSA with less than 112-bit of security strength is non-compliant and may not be used).

7.3 Non-Approved Services/Algorithms

The cryptographic module implements the following non-approved algorithms that are not permitted for use in FIPS 140-2 mode of operations. These algorithms may only be used once the CO has taken the modules out of a FIPS-Approved mode of operation. See Section 9 below for instructions on taking the modules out of a FIPS-Approved mode of operation.

Service	Non-Approved Algorithm

[3] As per IG D.9, the RSA Key Wrapping uses RSA modulus of 2048, 3072 and 4096 bit long that uses PKCS#1-v1.5 scheme and is not complaint with any revision of SP800-56B.

SSH (non-compliant)	Symmetric: TDES Asymmetric: 1024-bit RSA, 1024-bit Diffie-Hellman
TLS 1.0 (non-compliant)	MACing: HMAC SHA-2 Symmetric: AES CBC, AES GCM Asymmetric: 1024/2048/2072/4096-bit RSA, 1024/2048-bit Diffie-Hellman, P-256/P-384/P-521 EC Diffie-Hellman
IPsec (non-compliant)	Hashing: MD5 MACing: HMAC MD5 Symmetric: DES, TDES Asymmetric: 1024-bit RSA, 768/1024/1536-bit Diffie-Hellman
SNMP (non-compliant)	Hashing: MD5 MACing: HMAC MD5 Symmetric: DES, TDES Asymmetric: 1024-bit RSA, 1024-bit Diffie-Hellman

7.4 Self-Tests

The modules include 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. The modules implement the following power-on self-tests:

Firmware Integrity Test (RSA 2048 with SHA-256)

IOS Common Cryptographic Module Known Answer Tests:

- AES CBC (128-bit) encryption KAT
- AES CBC (128-bit) decryption KAT
- AES GCM (256-bit) encryption KAT
- AES GCM (256-bit) decryption KAT
- Diffie-Hellman shared secret computation KAT (SP800-56a rev3)
- EC Diffie-Hellman shared secret computation KAT (SP800-56a rev3)
- ECDSA (P-256 and P-384) Sign and Verify PCT
- SHA-1 KAT
- SHA2-256 KAT
- SHA2-384 KAT
- SHA2-512 KAT
- HMAC SHA-1 KAT
- HMAC SHA2-256 KAT
- HMAC SHA2-384 KAT
- HMAC SHA2-512 KAT
- RSA 2048 Sign and Verify KATs

- SP800-135 KDF KATs: IKEv2 KDF, SSH KDF, SNMP KDF
- SP800-108 KBKDF KAT
- SP 800-90A AES-CTR DRBG KAT
- SP 800-90A Section 11 Health Tests

Broadcom BCM82757 Known Answer Tests:

- AES GCM (256-bit) encryption KAT
- AES GCM (256-bit) decryption KAT

The module performs all power-on self-tests automatically at boot. All power-on self-tests must be passed before a role can perform services. The power-on self-tests are performed after the cryptographic systems are initialized but prior to the initialization of the LAN's interfaces; this prevents the module from passing any data during a power-on self-test failure. If any of the self-tests fail, the module halts and enters a critical error state.

Once the modules are operating in a FIPS-Approved mode of operation, the following conditional self-tests can be performed:

- Continuous Random Number Generator Test for the FIPS-Approved DRBG
- Repetition Count Test (RCT) on the digitized output of noise source
- Adaptive Proportions Test (APT) on the digitized output of the noise source
- Dead Ring Test (DRT) on the digitized output of the noise source
- ECDSA pairwise consistency test
- RSA pairwise consistency test
- Firmware Load Test (RSA 2048-bit with SHA2-256) – used to verify integrity of the firmware to be loaded into the module.

If any of the conditional self-tests fail, an error is returned to the module. The service is not performed. However, the module remails in an operational state. The CO may re-attempt the service or perform a new service. If the Firmware Load Test fails, the new firmware is not loaded, but the modules remail in an operational state.

8 Physical Security

The modules are production grade multi-chip standalone cryptographic modules that meet level 1 physical security requirements.

9 Secure Operation

The modules meet all Level 1 requirements for FIPS 140-2. The module is shipped only to authorized operators by the vendor, and the modules are shipped in Cisco boxes with Cisco adhesive. If evidence of tampering exists, contact Cisco immediately. Follow the setting instructions provided below to place the module in a FIPS-approved mode. Operating this module without maintaining the following settings will remove the modules from a FIPS-Approved mode of operation.

The modules are shipped to the customer site without the firmware pre-installed. The CO must perform the following steps to download, install, and configure the device to place it in a FIPS-Approved mode of operation:

1. Download the module's correct FIPS-Approved firmware image (via a secure method from https://software.cisco.com/)
2. Verify the integrity of the firmware image file (by calculating an MD5 or a SHA2-512 checksum value of the downloaded image file and comparing it with values provided on the Cisco download page),
3. Install the firmware onto the device
4. Follow the initialization steps defined in Section 9.1 below

Only after all configuration is complete, the device is restarted and all power-on self-tests have completed successfully, will the device be operating in a FIPS-Approved mode of operation.

The modules are validated with the IOS-XE 17.3 firmware running the IC2Mrel5a cryptographic module. Any firmware versions other than IOS-XE 17.3, loaded into the modules are out of the scope of this validation and require a separate FIPS 140-2 validation. Follow the setting instructions provided below to place the module in FIPS-Approved mode. Operating the module without maintaining the following settings will remove the module from the FIPS-Approved mode of operation.

9.1 System Initialization and Configuration

The CO must perform the following steps to place the module in a FIPS-Approved mode of operation:

1. The value of the boot field must be 0x2102. This setting disables break from the console to the ROM monitor and automatically boots. From the "configure terminal" command line, the CO enters the following:

   ```
   >config-register 0x2102
   ```

2. The CO must set up the operators of the module. Procedurally, the password must be at least 8 characters (procedurally enforced by policy), including at least one letter and at least one number, and is entered when the CO first engages the "configure terminal" command. The CO enters the following syntax at the "#" prompt:

```
>configure terminal
>username [USERNAME] privilege 15 password [PASSWORD]
```

3. For the created operators, identification and authentication on the console/auxiliary port is required for Users. From the “configure terminal” command line, the CO enters the following:

   ```
   >line con 0
   >login local
   ```

4. Enable FIPS-Approved Mode of Operations. From the “configure terminal” command line, the CO enters the following:

   ```
   >platform ipsec fips-mode
   ```

5. Exist “configuration terminal” mode, save the configuration, and reload the device.

   ```
   >exit
   >wr
   >reload
   ```

   The device will reload. Once all POST has completed successfully and the firmware has loaded the module will be in a FIPS-Approved mode of operation. The CO can confirm the FIPS status by entering the following at the # prompt:

   ```
   >show fips status
   ```

NOTE: The keys and CSPs generated in the cryptographic module during FIPS-Approved mode of operation cannot be used when the module transitions between non-FIPS mode and FIPS-Approved mode. All keys and CSPs must be zeroized by the CO.

For transition from FIPS to non-FIPS mode, the CO must zeroize the modules to delete all plaintext secret and private cryptographic keys and CSPs as defined in Table 12 above. Once the keys are zeroized, the CO must enter “configuration terminal” mode and enter the following command to take the module out of FIPS mode:

```
>no platform ipsec fips-mode
```

9.2 IPsec Requirements and Cryptographic Algorithms

The only type of key management that is allowed in FIPS mode is Internet Key Exchange (IKE). The following FIPS-Approved algorithms are to be used in the validated configuration:

- ah-sha-hmac

- ah-sha256-hmac
- ah-sha384-hmac
- ah-sha512-hmac
- esp-sha-hmac
- esp-sha256-hmac
- esp-sha384-hmac
- esp-sha512-hmac
- esp-aes
- esp-gcm

The following algorithms shall not be used:

- MD-5 for signing
- MD-5 HMAC
- DES

9.3 Remote Access

SSH access to the modules is allowed in FIPS-Approved mode of operation, using SSH v2 and a FIPS-Approved algorithm.

SNMPv3 communications with the modules is allowed in FIPS-Approved mode.

9.4 Key Strength

Key sizes with security strength of less than 112-bits shall not be used in FIPS-Approved mode.

10 Related Documentation

This document deals only with operations and capabilities of the security appliances in the technical terms of a FIPS 140-2 cryptographic device Security Policy. More information is available at the following:

- The NIST Cryptographic Module Validation Program website (http://csrc.nist.gov/groups/STM/cmvp/index.html) contains contact information for answers to technical or sales-related questions for the security appliances.
- Cisco C8300 Software Configuration Guide:
  Software Configuration Guide
- For LED related information please read *Hardware Installation Guide for Cisco Catalyst 8300 Series Edge Platforms* (Hardware Installation Guide for Cisco Catalyst 8300 Series Edge Platforms)

11 Acronyms and Terms

Table 14 below lists terms and acronyms that may be used in this document.

Table 14 – Terms and Acronyms

Acronym	Definition
AC	Alternating Current
AES	Advanced Encryption Standard
CKG	Cryptographic Key Generation
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CO	Cryptographic Officer
CSP	Critical Security Parameter
DC	Direct Current
DRAM	Dynamic Random-Access Memory
DRBG	Deterministic Random Bit Generator
EC	Elliptic Curve
ECDH	Elliptic Curve Diffie-Helman
ECDSA	Elliptic Curve Digital Signature Algorithm
ESP	Embedded Services Processor
ESV	Entropy Source Validation
FIPS	Federal Information Processing Standard
FRU	Field Replaceable Unit
Gb	Gigabits
GCM	Galois Counter Mode
GUI	Graphical User Interface
HMAC	Hash Message Authentication Code
IEEE	Institute of Electrical and Electronic Engineers
IG	Implementation Guidance
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol security
ISAKMP	Internet Security Association and Key Management Protocol
IT	Information Technology
IV	Initialization Vector
KAT	Known Answer Test
KDF	Key Derivation Function
LAN	Local Area Network
LED	Light Emitting Diode
MAC	Message Authentication Code
MPLS	Multiprotocol Label Switching
N/A	Not Applicable
NDRNG	Non-Deterministic Random Number Generator
NIM	Network Interface Module
NIST	National Institute of Standards and Technology

Acronym	Definition
NVMe	Non-Volatile Memory Express
NVRAM	Non-Volatile Random-Access Memory
OS	Operating System
PIN	Personal Identification Number
POST	Power-On Self-Test
PSU	Power Supply Unit
PUB	Publication
RAM	Random-Access Memory
RCT	Repetitive Count Test
RFC	Request For Comment
RJ	Registered Jack
RNG	Random Number Generator
RP	Route Processor
RSA	Rivest Shamir and Adleman
SDWAN	Software Defined Wide Area Network
SFP	Small Form-Factor Pluggable
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SP	Security Policy
SP	Special Publication
SSH	Secure Shell
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TRNG	True Random Number Generator
USB	Universal Serial Bus
VPN	Virtual Private Network
WAN	Wide Area Network