Cisco Systems, Inc.

Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module

FIPS 140-3 Non-Proprietary Security Policy

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

This is Cisco Systems, Inc. non-proprietary security policy for the Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module (hereinafter referred to as ASA, ASA-CM or Module), version 9.20. The following details how this module meets the security requirements of FIPS 140-3, SP 800-140 and ISO/IEC 19790 for a Security Level 1 Hardware cryptographic module.

The security requirements cover areas related to the design and implementation of a cryptographic module. These areas include cryptographic module specification; cryptographic module interfaces; roles, services, and authentication; software/firmware security; operational environment; physical security; non-invasive security; sensitive security parameter management; self-tests; life-cycle assurance; and mitigation of other attacks. The following table indicates the actual security levels for each area of the cryptographic module.

1.2 Security Levels

Section	Title	Security Level
1	General	1
2	Cryptographic module specification	1
3	Cryptographic module interfaces	1
4	Roles, services, and authentication	3
5	Software/Firmware security	1
6	Operational environment	1
7	Physical security	1
8	Non-invasive security	N/A
9	Sensitive security parameter management	1
10	Self-tests	1
11	Life-cycle assurance	1
12	Mitigation of other attacks	N/A
	Overall Level	1

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

This module is a multi-chip embedded hardware cryptographic module deployed under the Next-Generation Firewall (NGFW) with Adaptive Security Appliance (ASA). The module's operational environment is Limited**.**

Cisco ASA is an integrated network security system providing enterprise-class firewall with a comprehensive range of next-generation network security services, intrusion prevention system (IPS), content security and secure unified communications, HTTPS/TLSv1.2, SSHv2, IPsec/IKEv2, SNMPv3 and Cryptographic Cipher Suite B using the ASA Cryptographic Module.

Module Type: Hardware

Module Embodiment: Multi-Chip Embedded

Module Characteristics:

Cryptographic Boundary:

The Cisco ASA-CM is an integrated network security module housed in a single blade architecture, which is designed to integrate into the Cisco Firepower 4100 or 9300 Series Appliances. Once integrated, the ASA-CM provides enhanced security, reliability, and performance. Delivering industry-leading firewall data rates, this module provides exceptional scalability to meet the needs of today's dynamic organizations.

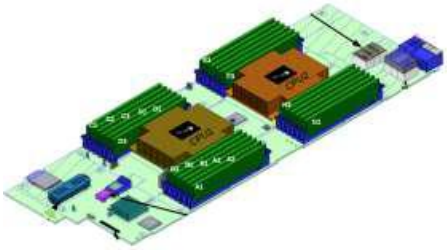

Figure 1 ASA-CM

Tested Operational Environment's Physical Perimeter (TOEPP):
The TOEPP is defined as the entire chassis unit's physical perimeter encompassing the "top," "front," "left," "right," "rear" and "bottom" surfaces of the case, and shown in the figures below and in the Physical Security section. The FPR 4112, FPR 4115, FPR 4125 and FPR 4145 have the same exterior features while FPR 9300 SM-40, FPR 9300 SM-48, and FPR 9300 SM-56 have the same exterior features. Where they differ is in Firewall throughput, IPS throughput, IPsec VPN throughput and number of VPN peers allowed.

Figure 2 FPR 4112, FPR 4115, FPR 4125, FPR 4145 – Front Panel

Figure 3 FPR 4112, FPR 4115, FPR 4125, FPR 4145 - Back Panel

Figure 4 FPR 9300 SM40, FPR 9300 SM48 and FPR 9300 SM56 – Front Panel

Figure 5 FPR 9300 SM40, FPR 9300 SM48 and FPR 9300 SM56 – Back Panel

The hardware version can be verified by using the command `show version` as an example, this command will output “Hardware: FPR4K-SM-32S.” Additionally, the front panels of chassis for the FPR 4112, FPR 4115, FPR 4125, FPR 4145 (Figure 2) are identical, and display “Cisco 4100 series” on the front panel. The chassis for the FPR 9300 SM40, FPR 9300 SM48 and FPR 9300 SM56 (Figure 3) show “Cisco 9k.”

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
FPR 4112	FPR4K-SM-12S	9.20	Intel Xeon Silver 4116 (Skylake) & NITROX-V, Marvell Semiconductor, NITROX	N/A
FPR 4115	FPR4K-SM-24S	9.20	Intel Xeon Silver 4116 (Skylake) & NITROX-V, Marvell Semiconductor, NITROX	N/A
FPR 4125	FPR4K-SM-32S	9.20	Intel Xeon Gold 6130T (Skylake) & NITROX-V, Marvell Semiconductor, NITROX	N/A
FPR 4145	FPR4K-SM-44S	9.20	Intel Xeon Gold 6152 (Skylake) & NITROX-V, Marvell Semiconductor, NITROX	N/A
FPR 9300 SM-40	FPR9K-SM-40	9.20	Intel Xeon Gold 6138T (Skylake) & NITROX-V, Marvell Semiconductor, NITROX	N/A
FPR 9300 SM-48	FPR9K-SM-48	9.20	Intel Xeon Platinum 8160 (Skylake) & NITROX-V, Marvell Semiconductor, NITROX	N/A
FPR 9300 SM-56	FPR9K-SM-56	9.20	Intel Xeon Platinum 8176 (Skylake) & NITROX-V, Marvell Semiconductor, NITROX	N/A

Table 2: Tested Module Identification – Hardware

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

2.3 Excluded Components

N/A for this module.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved Mode of Operation	The module as recommended by Cisco is configured to have the Approved Mode enabled. In the Approved Mode, only Approved algorithms can be configured.	Approved	Approved mode indicator: "FIPS is currently enabled."
Non-Approved Mode of Operation	The module is configured to have the Approved Mode disabled (Which is not recommended by Cisco). In the Non-Approved Mode, both Non-Approved and Approved algorithms can be configured.	Non-Approved	Non-Approved mode indicator: "FIPS is currently disabled."

Table 3: Modes List and Description

The module supports an Approved and a Non-Approved mode of operation.

Mode change instructions and status indicators:

The module will operate in the Approved mode of operation once the configuration steps for the Approved mode in section 11.1 are completed. The module upon successful completion of all pre-operational self-tests and cryptographic algorithm self-tests from both hardware and firmware implementations will be operational.

Although **not recommended by Cisco**. the module can be configured into the Non-Approved mode by following the configuration steps for the Non-Approved mode in section 11.1.

Degraded Mode Description:

The module does not implement a degraded mode of operation.

2.5 Algorithms

Approved Algorithms:

CiscoSSL FOM Cryptographic Implementation

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A4446	Key Length - 128, 256	SP 800-38A
AES-GCM	A4446	Key Length - 128, 256	SP 800-38D
Counter DRBG	A4446	Prediction Resistance - Yes Mode - AES-128, AES-192, AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-4)	A4446	Curve - P-256, P-384, P-521 Secret Generation Mode - Testing Candidates	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A4446	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A4446	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4

Algorithm	CAVP Cert	Properties	Reference
HMAC-SHA-1	A4446	Key Length - Key Length: 256-448 Increment 8, Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA2-224	A4446	Key Length - Key Length: 256-448 Increment 8, Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA2-256	A4446	Key Length - Key Length: 256-448 Increment 8, Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA2-384	A4446	Key Length - Key Length: 256-448 Increment 8, Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512	A4446	Key Length - Key Length: 256-448 Increment 8, Key Length: 8-524288 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A4446	Domain Parameter Generation Methods - P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-FFC-SSC Sp800-56Ar3	A4446	Domain Parameter Generation Methods - ffdhe2048, ffdhe3072, ffdhe4096, modp-2048, modp-3072, modp-4096 Scheme - dhEphem - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDF IKEv2 (CVL)	A4446	Diffie-Hellman Shared Secret Length - Diffie-Hellman Shared Secret Length: 2048 Derived Keying Material Length - Derived Keying Material Length: 3072 Hash Algorithm - SHA-1	SP 800-135 Rev. 1
KDF SNMP (CVL)	A4446	Password Length - Password Length: 256, 64	SP 800-135 Rev. 1
KDF SSH (CVL)	A4446	Cipher - AES-128, AES-192, AES-256 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
RSA KeyGen (FIPS186-4)	A4446	Key Generation Mode - B.3.4 Modulo - 2048, 3072, 4096 Hash Algorithm - SHA2-256 Private Key Format - Standard	FIPS 186-4
RSA SigGen (FIPS186-4)	A4446	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096	FIPS 186-4
RSA SigVer (FIPS186-4)	A4446	Signature Type - ANSI X9.31, PKCS 1.5, PKCSPSS Modulo - 1024, 2048, 3072, 4096	FIPS 186-4
Safe Primes Key Generation	A4446	Safe Prime Groups - ffdhe2048, ffdhe3072, ffdhe4096, modp-2048, modp-3072, modp-4096	SP 800-56A Rev. 3
SHA-1	A4446	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-224	A4446	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4

Algorithm	CAVP Cert	Properties	Reference
SHA2-256	A4446	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-384	A4446	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-512	A4446	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
TLS v1.2 KDF RFC7627 (CVL)	A4446	Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1

Table 4: Approved Algorithms - CiscoSSL FOM Cryptographic Implementation

Marvell Cavium Nitrox V

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	C1026	Key Length - 128, 256	SP 800-38A
AES-GCM	C1026	Key Length - 128, 256	SP 800-38D
HMAC-SHA-1	C1026	-	FIPS 198-1
HMAC-SHA2-256	C1026	-	FIPS 198-1
HMAC-SHA2-384	C1026	-	FIPS 198-1
HMAC-SHA2-512	C1026	-	FIPS 198-1
SHA-1	C1026	Message Length - Message Length: 0-51200 Increment 8	FIPS 180-4
SHA2-256	C1026	Message Length - Message Length: 0-51200 Increment 8	FIPS 180-4
SHA2-384	C1026	Message Length - Message Length: 0-102400 Increment 8	FIPS 180-4
SHA2-512	C1026	Message Length - Message Length: 0-102400 Increment 8	FIPS 180-4

Table 5: Approved Algorithms - Marvell Cavium Nitrox V

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG	Key Type:Asymmetric	N/A	The cryptographic module performs Cryptographic Key Generation (CKG) for asymmetric keys as per sections 4 and 5 in SP800-133rev2 (vendor affirmed) and FIPS 140-3 IG D.H. A seed (i.e., the random value) used in asymmetric key generation is a direct output from SP800-90Arev1 CTR_DRBG (A4446)

Table 6: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

Name	Use and Function
3DES	Used for symmetric encryption in SSHv2, TLSv1, TLSv1.2, IPsec/IKEv2, and SNMPv3
ChaCha20-poly1305	Used for authenticated symmetric encryption in SSHv2, and TLSv1.3

Table 7: Non-Approved, Not Allowed Algorithms

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
KAS-ECC-KeyGen (SSHv2)	CKG KAS-KeyGen	KAS ECC keygen used in SSHv2 service	Bit-strength Caveat:Provides between 128 and 256 bits encryption strength	Counter DRBG: (A4446) CKG: ()
KAS-FFC-KeyGen (SSHv2)	CKG KAS-KeyGen	KAS FFC keygen used in SSHv2 service	Bit-strength Caveat:Provides between 112 and 152 bits encryption strength	Counter DRBG: (A4446) Safe Primes Key Generation: (A4446) Safe Prime Groups: modp-2048, modp-3072, modp-4096 CKG: ()
KAS-ECC-KeyGen (TLSv1.2)	CKG KAS-KeyGen	KAS ECC keygen used in TLSv1.2 service	Bit-strength Caveat:Provides between 128 and 256 bits encryption strength	Counter DRBG: (A4446) CKG: ()

Name	Type	Description	Properties	Algorithms
KAS-FFC-KeyGen (TLSv1.2)	CKG KAS-KeyGen	KAS FFC keygen used in TLSv1.2 service	Bit-strength Caveat:Provides between 112 and 152 bits encryption strength	Counter DRBG: (A4446) Safe Primes Key Generation: (A4446) Safe Prime Groups: ffdhe2048, ffdhe3072, ffdhe4096 CKG: ()
KAS-ECC-KeyGen (IKEv2)	CKG KAS-KeyGen	KAS ECC keygen used in IKEv2 service	Bit-strength Caveat:Provides between 128 and 256 bits encryption strength	Counter DRBG: (A4446) CKG: ()
KAS-FFC-KeyGen (IKEv2)	CKG KAS-KeyGen	KAS FFC keygen used in IKEv2 service	Bit-strength Caveat:Provides between 112 and 152 bits encryption strength	Counter DRBG: (A4446) Safe Primes Key Generation: (A4446) Safe Prime Groups: modp-2048, modp-3072, modp-4096 CKG: ()
KAS-ECC (SSHv2)	KAS-Full	KAS-ECC for SSHv2 Service	Bit-strength Caveat:Provides between 128 and 256 bits of encryption strength	KAS-ECC-SSC Sp800-56Ar3: (A4446) KDF SSH: (A4446)
KAS-FFC (SSHv2)	KAS-Full	KAS-FFC for SSHv2 Service	Bit-strength Caveat:Provides between 112 to 152 bits of encryption strength	KAS-FFC-SSC Sp800-56Ar3: (A4446) Domain Parameter Generation Methods: MODP-2048, MODP-3072, MODP-4096

Name	Type	Description	Properties	Algorithms
				KDF SSH: (A4446)
KAS-ECC (TLSv1.2)	KAS-Full	KAS-ECC for TLSv1.2 Service	Bit-strength Caveat:Provides between 128 and 256 bits of encryption strength	KAS-ECC-SSC Sp800-56Ar3: (A4446) TLS v1.2 KDF RFC7627: (A4446)
KAS-FFC (TLSv1.2)	KAS-Full	KAS-FFC for TLSv1.2 Service	Bit-strength Caveat:Provides between 112 to 152 bits of encryption strength	KAS-FFC-SSC Sp800-56Ar3: (A4446) Domain Parameter Generation Methods: ffdhe2048, ffdhe3072, ffdhe4096 TLS v1.2 KDF RFC7627: (A4446)
KAS-ECC (IKEv2)	KAS-Full	KAS-ECC for IKEv2 Service	Bit-strength Caveat:Provides between 128 and 256 bits of encryption strength	KAS-ECC-SSC Sp800-56Ar3: (A4446) KDF IKEv2: (A4446)
KAS-FFC (IKEv2)	KAS-Full	KAS-FFC for IKEv2 Service	Bit-strength Caveat:Provides between 112 and 152 bits of encryption strength	KAS-FFC-SSC Sp800-56Ar3: (A4446) Domain Parameter Generation Methods: MODP-2048, MODP-3072, MODP-4096 KDF IKEv2: (A4446)
KTS (TLSv1.2 with AES and HMAC)	KTS-Wrap	KTS via TLSv1.2 service by using AES and HMAC	Bit-strength Caveat:Provides 128 or 256 bits of encryption strength	AES-CBC: (A4446) Key Length: 128, 256 HMAC-SHA-1: (A4446) HMAC-SHA2-

Name	Type	Description	Properties	Algorithms
				256: (A4446) HMAC-SHA2-384: (A4446) SHA-1: (A4446) SHA2-256: (A4446) SHA2-384: (A4446)
KTS (TLSv1.2 with AES-GCM)	KTS-Wrap	KTS via TLSv1.2 service by using AES-GCM	Bit-strength Caveat:Provides 128 or 256 bits of encryption strength	AES-GCM: (A4446) Key Length: 128, 256
KTS (SSHv2 with AES and HMAC)	KTS-Wrap	KTS via SSHv2 service by using AES and HMAC	Bit-strength Caveat:Provides 128 or 256 bits of encryption strength	AES-CBC: (A4446) Key Length: 128, 256 HMAC-SHA-1: (A4446) HMAC-SHA2-256: (A4446) SHA-1: (A4446) SHA2-256: (A4446)
KTS (SSHv2 with AES-GCM)	KTS-Wrap	KTS via SSHv2 service by using AES-GCM	Bit-strength Caveat:Provides 128 or 256 bits of encryption strength	AES-GCM: (A4446) Key Length: 128, 256
RSA KeyGen (SSHv2, TLSv1.2, IKEv2)	AsymKeyPair-KeyGen CKG	RSA KeyGen for SSHv2, TLSv1.2, and IKEv2 services		RSA KeyGen (FIPS186-4): (A4446) Counter DRBG: (A4446) CKG: () Key Type: Asymmetric
ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2)	AsymKeyPair-KeyGen CKG	ECDSA KeyGen for SSHv2, TLSv1.2 and IKEv2 services		ECDSA KeyGen (FIPS186-4): (A4446) Counter DRBG: (A4446) CKG: ()

Name	Type	Description	Properties	Algorithms
				Key Type: Asymmetric
RSA SigGen (SSHv2, TLSv1.2, IKEv2)	DigSig-SigGen	RSA SigGen for SSHv2, TLSv1.2, and IKEv2 services		RSA SigGen (FIPS186-4): (A4446)
ECDSA SigGen (SSHv2, TLSv1.2 and IKEv2)	DigSig-SigGen	ECDSA SigGen for TLSv1.2, and IKEv2 services		ECDSA SigGen (FIPS186-4): (A4446)
RSA SigVer (SSHv2, TLSv1.2, and IKEv2)	DigSig-SigVer	RSA SigVer for SSHv2, TLSv1.2, and IKEv2 services		RSA SigVer (FIPS186-4): (A4446)
ECDSA SigVer (SSHv2, TLSv1.2, and IKEv2)	DigSig-SigVer	ECDSA SigVer for TLSv1.2 and IKEv2 services		ECDSA SigVer (FIPS186-4): (A4446)
Session Encryption/Decryption (SSHv2)	BC-Auth BC-UnAuth	SSHv2 session protection.		AES-CBC: (A4446) Key Length: 128, 256 AES-GCM: (A4446) Key Length: 128, 256
Session Encryption/Decryption (TLSv1.2)	BC-Auth BC-UnAuth	TLSv1.2 session protection.		AES-GCM: (A4446) Key Length: 128, 256 AES-CBC: (A4446) Key Length: 128, 256
Session Encryption/Decryption (IPSec/IKE)	BC-Auth BC-UnAuth	IPSec/IKE session protection.		AES-CBC: (A4446, C1026) AES-GCM: (A4446, C1026)
Session Encryption/Decryption (SNMPv3)	BC-UnAuth	SNMPv3 sesssion protection.		AES-CBC: (A4446)
Session Authentication (SSHv2)	MAC	SSHv2 session authentication.		HMAC-SHA-1: (A4446) HMAC-SHA2-256: (A4446) SHA-1: (A4446)

Name	Type	Description	Properties	Algorithms
				SHA2-256: (A4446)
Session Authentication (TLSv1.2)	MAC	TLSv1.2 session authentication.		HMAC-SHA-1: (A4446) HMAC-SHA2-256: (A4446) HMAC-SHA2-384: (A4446) SHA-1: (A4446) SHA2-256: (A4446) SHA2-384: (A4446)
Session Authentication (IPSec/IKEv2)	MAC	IPSec/IKEv2 session authentication.		HMAC-SHA-1: (A4446, C1026) HMAC-SHA2-256: (A4446, C1026) HMAC-SHA2-384: (A4446, C1026) HMAC-SHA2-512: (A4446, C1026) SHA-1: (A4446, C1026) SHA2-256: (A4446, C1026) SHA2-384: (A4446, C1026) SHA2-512: (A4446, C1026)
Session Authentication (SNMPv3)	MAC	SNMPv3 session authentication.		HMAC-SHA-1: (A4446) SHA-1: (A4446) HMAC-SHA2-384: (A4446) SHA2-256: (A4446) SHA2-384: (A4446) HMAC-SHA2-

Name	Type	Description	Properties	Algorithms
				224: (A4446) SHA2-224: (A4446) HMAC-SHA2-256: (A4446)
SSHv2 Keying Materials Development	KAS-135KDF	SSHv2 session keying materials, used to derive SSHv2 session keys.		KDF SSH: (A4446)
TLSv1.2 Keying Materials Development	KAS-135KDF	TLSv1.2 session keying materials, used to derive TLS session keys.		TLS v1.2 KDF RFC7627: (A4446)
IPSec/IKEv2 Keying Materials Development	KAS-135KDF	IPSec/IKEv2 session keying materials, used to derive IPSec/IKEv2 session keys.		KDF IKEv2: (A4446)
SNMPv3 Keying Materials Development	KAS-135KDF	SNMPv3 session keying materials, used to derive SNMPv3 session keys.		KDF SNMP: (A4446)
Firmware Load Test	MAC	MAC for firmware load test		HMAC-SHA2-512: (A4446)
DRBG Function	DRBG	Used for DRBG generation		Counter DRBG: (A4446)

Table 8: Security Function Implementations

2.7 Algorithm Specific Information

- The module's AES-GCM implementation conforms to Implementation Guidance C.H scenario #1d following RFC 5647 for SSH. A new IV parameter is generated by the module for each AES-GCM encryption. As shown in Section 7.1 of RFC 5647, the IV consists of a 4-byte fixed field and an 8-byte invocation counter. The initial IV value is generated as shown in Figure 1 of RFC 5647 and the fixed field of this IV remains the same for the duration of the session. Therefore, the method for minimizing the (key, IV) collision probability within the same session depends entirely on the management of the invocation field of the IV. The invocation counter is treated as a 64-bit integer and is

incremented by one when performing an AES-GCM encryption of a new binary packet. The formation of binary packets is explained in Section 7.2 of RFC 5647.

- The module's AES-GCM implementation conforms to Implementation Guidance C.H 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 keys for the client and server negotiated in the TLSv1.2 handshake process (client_write_key and server_write_key) are compared and the module aborts the session if the key values are identical.The operations of one of the two parties involved in the TLS key establishment scheme were performed entirely within the cryptographic boundary of the module being validated. The counter portion of the IV is set by the module within its cryptographic boundary. When the IV exhausts the maximum number of possible values for a given session key, the first party, client or server, to encounter this condition will trigger a handshake to establish a new encryption key. In case the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established.

- The module uses RFC 7296 compliant IKEv2 to establish the shared secret SKEYSEED from which the AES GCM encryption keys are derived. Two keys established by IKEv2 for one security association (one key for encryption in each direction between the parties) are not identical and abort the session if they are. When the IV exhausts the maximum number of possible values for a given session key, the first party, client or server, to encounter this condition will trigger a handshake to establish a new encryption key. In case the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established.

- The module was algorithm tested based on the FIPS 186-4 standard Digital Signatures. According to IG C.K, this module is 186-5 compliant as all 186-4 CAVP tests performed are mathematically identical to the 186-5 CAVP tests. The Module does not support 186-4 DSA or RSA X9.31 for Signature Generation or Signature Verification.

2.8 RBG and Entropy

Cert Number	Vendor Name
E3	Cisco Systems, Inc.

Table 9: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Cisco Jitter Entropy Source	Non-Physical	Intel Xeon Platinum 8160 (Skylake), Intel Xeon Platinum 8176 (Skylake), Intel Xeon Silver 4116 (Skylake), Intel Xeon Gold 6130T (Skylake), Intel Xeon Gold 6138T (Skylake), Intel Xeon Gold 6152 (Skylake)	256 bits	Full Entropy	A2810 (SHA3-256)

Table 10: Entropy Sources

The module implements a Deterministic Random Bit Generator (DRBG) based on SP800-90Arev1, CTR_DRBG with Algo Cert. #A4446.

The DRBG is used internally by the module (e.g. to generate symmetric keys, seeds for asymmetric key pairs, and random numbers for security functions). The DRBG is seeded by the entropy source described in the table above. The CTR_DRBG (AES-128/192/256) enables Derivation Function capability. The DRBG is instantiated with a 384-bits long entropy input (corresponding to 384 bits of entropy) and provides at least 256 bits security strength for the cryptographic keys generation while in the approved mode.

The Cisco JENT entropy source implementation generates an output that is considered to have full entropy. More information can be found in the public use document for ESV Cert. #E3.

2.9 Key Generation

The module generates RSA, ECDSA, KAS-ECC-SSC, and KAS-FFC-SSC asymmetric key pairs compliant with FIPS 186-4, using a NIST SP 800-90Arev1 CTR_DRBG for random number generation. In accordance with FIPS 140-3 IG D.H, the cryptographic module performs CKG for asymmetric keys as per section 5.1 of NIST SP 800-133rev2 (vendor affirmed) by obtaining a random bit string directly from an approved DRBG. The random bit string supports the required security strength requested by the calling application (without any V, as described in Additional Comments 2 of IG D.H.).

2.10 Key Establishment

The module provides the following key/SSP establishment services in the approved mode of operation:

KAS-FFC Shared Secret Computation:

- The module provides SP800-56Arev3 compliant key establishment according to FIPS 140-3 IG D.F scenario 2 path (2) with KAS-FFC shared secret computation. The shared secret computation provides between 112 and 152 bits of encryption strength.

- The module supports the use of the safe primes defined in RFC 4419 (SSH), RFC 7919 (TLS) and RFC 3526 (IKE). Note that the module only implements domain parameter generation, key pair generation and verification, and shared secret computation.

    - SSH (RFC 4419):
        - MODP-2048 (ID = 14)
        - MODP-3072 (ID = 15)
        - MODP-4096 (ID = 16)
    - TLS (RFC 7919):
        - ffdhe2048 (ID = 256)
        - ffdhe3072 (ID = 257)
        - ffdhe4096 (ID = 258)
    - IKE (RFC 3526):

        - MODP-2048 (ID = 14)
        - MODP-3072 (ID = 15)
        - MODP-4096 (ID = 16)

KAS-ECC Shared Secret Computation:

- The module provides SP800-56Arev3 compliant key establishment according to FIPS 140-3 IG D.F scenario 2 path (2) with KAS-ECC shared secret computation. The shared secret computation provides between 128 and 256 bits of encryption strength.

- The modules NIST recommended curves correspond to the curves uses in these industry protocols

    - TLS (RFC 4492):
        - P-256 (secp256r1)
        - P-384 (secp384r1)
        - P-521 (secp521r1)

    - IKE (RFC 5903):
        - P-256 (secp256r1)
        - P-384 (secp384r1)
        - P-521 (secp521r1)

The module also provides the following key transport mechanisms:

- Key wrapping using AES-GCM with a security strength of 128 or 256 bits.
- Key wrapping using AES-CBC with a security strength of 128 or 256 bits with HMAC-SHA-1, HMAC-SHA2-256 or HMAC-SHA2-384.

2.11 Industry Protocols

The module supports SSHv2, TLS v1.2, SNMPv3 and IPsec/IKEv2 industrial protocols. Please refer to the Security Function Implementations Table for more information. No parts of IPSec/IKEv2, SNMPv3, SSH and TLS protocols, other than the KDFs, have been tested by the CAVP and CMVP.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
SFP Ethernet Ports, PCI port	Data Input	Data input into the module for all the services defined in Approved Services Table, including TLSv1.2, SSHv2, SNMPv3 and IPsec/IKEv2 service data.
SFP Ethernet Ports, PCI port	Data Output	Data output from the module for all the services defined in Approved Services Table, including TLSv1.2, SSHv2, SNMPv3 and IPsec/IKEv2 service data.
SFP Ethernet Ports, PCI port	Control Input	Control Data input into the module for all the services defined in Approved Services Table, including TLSv1.2, SSHv2, SNMPv3 and IPsec/IKEv2 service data.

Physical Port	Logical Interface(s)	Data That Passes
SFP Ethernet Ports, PCI port, LED	Status Output	Status Information output from the module.
N/A	Control Output	N/A
Power Interface	Power	Provide the power supply to the module.

Table 11: Ports and Interfaces

The module's physical perimeter encompasses the case of the tested platform mentioned in Table 2. The module provides physical ports which are mapped to logical interfaces provided by the module (data input, data output, control input, control output and status output) as above. The module's data output interface will be disabled when performing pre-operational self-tests, loading new firmware, zeroizing keys, or when in an error state.

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Password	The minimum length is eight (8) characters (94 possible characters). The configuration supports at most ten failed attempts to authenticate in a one-minute period.	Password Based	The probability that a random attempt will succeed or a false acceptance will occur is 1/(94^8) which is less than 1/1,000,000.	The probability of successfully authenticating to the module within one minute is 10/(94^8), which is less than 1/100,000.
RSA-Based Certificate	The modules support RSA public-key based authentication mechanism using a minimum of RSA 2048 bits, which provides 112 bits of security strength. The probability that a random attempt will succeed is 1/(2^112) which is less than 1/1,000,000. For multiple attacks during a one-minute period, as the module at its highest	RSA SigVer (FIPS186-4) (A4446)	The probability that a random attempt will succeed is 1/(2^112). Please refer to Description section in this table for more details.	The probability of successfully authenticating to the module within a one minute period is 17,000 * 60 = 1,020,000/(2^112). Please refer to Description section in this table for more details.

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
	can support at most 17,000 new sessions per second to authenticate in a one-minute period, the probability of successfully authenticating to the module within a one minute period is 17,000 * 60 = 1,020,000/(2^112), which is less than 1/100,000.			
ECDSA-Based Certificate	The modules support ECDSA public-key based authentication mechanism using a minimum of curve P-256, which provides 128 bits of security strength. The probability that a random attempt will succeed is 1/(2^128) which is less than 1/1,000,000. For multiple attacks during a one-minute period, as the module at its highest can support at most 17,000 new sessions per second to authenticate in a one-minute period, the probability of successfully authenticating to the module within a one minute period is 17,000 * 60 = 1,020,000/(2^128), which is less than 1/100,000.	ECDSA SigVer (FIPS186-4) (A4446)	The probability that a random attempt will succeed is 1/(2^128) which is less than 1/1,000,000. Please refer to Description section in this table for more details.	The probability of successfully authenticating to the module within a one minute period is 17,000 * 60 = 1,020,000/(2^128). Please refer to Description section in this table for more details.

Table 12: Authentication Methods

The module implements identity-based authentication. The module supports Crypto Officer role and the User role. The module also allows the concurrent operators.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Identity	CO	Password RSA-Based Certificate ECDSA-Based Certificate
User	Identity	User	Password RSA-Based Certificate ECDSA-Based Certificate

Table 13: Roles

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Show Status	Provide Module's current status (return codes and/or syslog messages)	N/A	Command used to show Module's Status	Module's Operational Status	None	Crypto Officer User
Show Version	Provide Module's name and version information	N/A	Command to show version	Module's ID and versioning information	None	Crypto Officer User
Perform Self-Tests	Perform Self-Tests (Pre-operational self-test and Conditional Self-Tests)	N/A	Command to trigger Self-Test	Status of the self-tests results	None	Crypto Officer User Unauthenticated
Perform Zeroization	Perform Zeroization	N/A	Command to zeroize the module	Status of the SSPs zeroization	None	Crypto Officer - DRBG Entropy Input: Z - Counter DRBG

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Seed: Z - Counter DRBG Internal State V: Z - Counter DRBG Key: Z - User Password: Z - Crypto Officer Password: Z - Firmware Load Test Key: Z - SSH DH Private Key: Z - SSH DH Public Key: Z - SSH Peer DH Public Key: Z - SSH DH Shared Secret: Z - SSH ECDH Private Key: Z - SSH ECDH Public Key: Z - SSH Peer ECDH Public Key: Z - SSH ECDH Shared Secret: Z - SSH RSA Private Key:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Z - SSH RSA Public Key: Z - SSH ECDSA Private Key: Z - SSH ECDSA Public Key: Z - SSH Session Encryption Key: Z - SSH Session Authentication Key: Z - TLS DH Private Key: Z - TLS DH Public Key: Z - TLS Peer DH Public Key: Z - TLS DH Shared Secret: Z - TLS ECDH Private Key: Z - TLS ECDH Public Key: Z - TLS Peer ECDH Public Key: Z - TLS ECDH Shared Secret: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- TLS ECDSA Private Key: Z - TLS ECDSA Public Key: Z - TLS RSA Private Key: Z - TLS RSA Public Key: Z - TLS Master Secret: Z - TLS Session Encryption Key: Z - TLS Session Authentication Key: Z - IPSec/IKE DH Private Key: Z - IPSec/IKE DH Public Key: Z - IPSec/IKE Peer DH Public Key: Z - IPSec/IKE DH Shared Secret: Z - IPSec/IKE ECDH Private Key: Z - IPSec/IKE ECDH Public Key: Z - IPSec/IKE Peer ECDH

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Public Key: Z - IPSec/IKE ECDH Shared Secret: Z - IPSec/IKE ECDSA Private Key: Z - IPSec/IKE ECDSA Public Key: Z - IPSec/IKE RSA Private Key: Z - IPSec/IKE RSA Public Key: Z - IPSec/IKE Pre-shared Secret: Z - SKEYSEED: Z - IPSec/IKE Session Encryption Key: Z - IPSec/IKE Authentication Key: Z - SNMPv3 Shared Secret: Z - SNMPv3 Encryption Key: Z - SNMPv3 Authentication Key: Z
Configure Network	Sets configuration of the systems	N/A	Commands to configure the network	Status of the completion of network	None	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
				configuration status		
Account Management	Manage User Account	N/A	Commands to create User account	Account status	None	Crypto Officer
Crypto Officer Authentication	CO Role Authentication	N/A	CO Authentication Request	Status of the CO authentication	None	Crypto Officer - Crypto Officer Password: W,Z
User Authentication	User Role Authentication	N/A	User role authentication request	Status of the User role authentication	None	User - User Password: W,Z
Configure Bypass Capability	Sets the Bypass capability	N/A	CLI Bypass commands	Status of the completion of Bypass capability configuration	None	Crypto Officer
Configure SSHv2 Function	Configure SSHv2 Function	Status Mode Indicator "FIPS is currently enabled" and SSHv2 configuration success status message	Commands to configure SSHv2	Status of the completion of the SSHv2 configuration	KTS (TLSv1.2 with AES and HMAC) KTS (TLSv1.2 with AES-GCM) KTS (SSHv2 with AES and HMAC) KTS (SSHv2 with AES-GCM) RSA KeyGen (SSHv2, TLSv1.2, IKEv2) ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2) DRBG Function	Crypto Officer - SSH RSA Private Key: W,E - SSH RSA Public Key: W,E - SSH ECDSA Private Key: W,E - SSH ECDSA Public Key: W,E - DRBG Entropy Input: W,E - Counter DRBG Seed: W,E - Counter

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						DRBG Internal State V: W,E - Counter DRBG Key: W,E
Configure HTTPS over TLSv1.2 Function	Configure HTTPS over TLSv1.2 Function	Status Mode Indicator "FIPS is currently enabled" and HTTPS over TLSv1.2 configuration success status message	Commands to configure TLSv1.2	Status of the completion of TLSv1.2 configuration	KTS (TLSv1.2 with AES and HMAC) KTS (TLSv1.2 with AES-GCM) KTS (SSHv2 with AES and HMAC) KTS (SSHv2 with AES-GCM) RSA KeyGen (SSHv2, TLSv1.2, IKEv2) ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2) DRBG Function	Crypto Officer - TLS ECDSA Private Key: W,E - TLS ECDSA Public Key: W,E - TLS RSA Private Key: W,E - TLS RSA Public Key: W,E - DRBG Entropy Input: W,E - Counter DRBG Seed: W,E - Counter DRBG Internal State V: W,E - Counter DRBG Key: W,E
Configure IPsec/IKEv2 Function	Configure IPSec/IKEv2 Function	Status Mode Indicator "FIPS is currently enabled" with IPsec/IKEv2 configuration	Commands to configure IPsec/IKEv2	Status of the completion of IPsec/IKEv2 configuration	KTS (TLSv1.2 with AES and HMAC) KTS (TLSv1.2 with AES-GCM) KTS (SSHv2 with AES and HMAC) KTS (SSHv2 with AES-GCM) RSA KeyGen	Crypto Officer - IPSec/IKE ECDSA Private Key: W,E - IPSec/IKE ECDSA Public Key: W,E - IPSec/IKE

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		success status message			(SSHv2, TLSv1.2, IKEv2) ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2) DRBG Function	RSA Private Key: W,E - IPSec/IKE RSA Public Key: W,E - IPSec/IKE Pre-shared Secret: W,E - DRBG Entropy Input: W,E - Counter DRBG Seed: W,E - Counter DRBG Internal State V: W,E - Counter DRBG Key: W,E
Configure SNMPv3 Function	Configure SNMPv3 Function	Status Mode Indicator "FIPS is currently enabled" and SNMPv3 configuration success status message	Commands to configure SNMPv3	Status of the completion of SNMPv3 configuration	KTS (TLSv1.2 with AES and HMAC) KTS (TLSv1.2 with AES-GCM) KTS (SSHv2 with AES and HMAC) KTS (SSHv2 with AES-GCM)	Crypto Officer - SNMPv3 Shared Secret: W,E - SNMPv3 Encryption Key: W,E - SNMPv3 Authentication Key: W,E
Run SSHv2 Function	Execute SSHv2 Function	Status Mode Indicator "FIPS is currently enabled" and successful SSHv2 log message	Initiate SSHv2 tunnel establishment	Status of SSHv2 tunnel establishment	KAS-ECC-KeyGen (SSHv2) KAS-FFC-KeyGen (SSHv2) KAS-ECC (SSHv2) KAS-FFC (SSHv2) KTS (SSHv2 with AES and	Crypto Officer - SSH DH Private Key: W,E - SSH DH Public Key: W,E - SSH Peer DH Public Key: W,E - SSH DH

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					HMAC) KTS (SSHv2 with AES-GCM) RSA SigGen (SSHv2, TLSv1.2, IKEv2) ECDSA SigGen (SSHv2, TLSv1.2 and IKEv2) RSA SigVer (SSHv2, TLSv1.2, and IKEv2) ECDSA SigVer (SSHv2, TLSv1.2, and IKEv2) Session Encryption/Decryption (SSHv2) Session Authentication (SSHv2) SSHv2 Keying Materials Development DRBG Function	Shared Secret: W,E - SSH ECDH Private Key: W,E - SSH ECDH Public Key: W,E - SSH Peer ECDH Public Key: W,E - SSH ECDH Shared Secret: W,E - SSH RSA Private Key: W,E - SSH RSA Public Key: W,E - SSH ECDSA Private Key: W,E - SSH ECDSA Public Key: W,E - SSH Session Encryption Key: W,E - SSH Session Authentication Key: W,E - DRBG Entropy Input: W,E - Counter DRBG Seed: W,E - Counter

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						DRBG Internal State V: W,E - Counter DRBG Key: W,E User - SSH DH Private Key: W,E - SSH DH Public Key: W,E - SSH Peer DH Public Key: W,E - SSH DH Shared Secret: W,E - SSH ECDH Private Key: W,E - SSH ECDH Public Key: W,E - SSH Peer ECDH Public Key: W,E - SSH ECDH Shared Secret: W,E - SSH RSA Private Key: W,E - SSH RSA Public Key: W,E - SSH ECDSA Private Key: W,E - SSH ECDSA

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Public Key: W,E - SSH Session Encryption Key: W,E - SSH Session Authentication Key: W,E - DRBG Entropy Input: W,E - Counter DRBG Seed: W,E - Counter DRBG Internal State V: W,E - Counter DRBG Key: W,E
Run HTTPS over TLSv1.2 Function	Execute HTTPS over TLSv1.2 function	Status Mode Indicator "FIPS is currently enabled" and successful HTTPS over TLSv1.2 log message	Initiate TLSv1.2 tunnel establishment request	Status of TLSv1.2 tunnel establishment	KAS-ECC-KeyGen (TLSv1.2) KAS-FFC-KeyGen (TLSv1.2) KAS-ECC (TLSv1.2) KAS-FFC (TLSv1.2) KTS (TLSv1.2 with AES and HMAC) KTS (TLSv1.2 with AES-GCM) RSA SigGen (SSHv2, TLSv1.2, IKEv2) ECDSA SigGen (SSHv2, TLSv1.2 and IKEv2)	Crypto Officer - TLS DH Private Key: W,E - TLS DH Public Key: W,E - TLS Peer DH Public Key: W,E - TLS DH Shared Secret: W,E - TLS ECDH Private Key: W,E - TLS ECDH Public Key: W,E - TLS Peer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					RSA SigVer (SSHv2, TLSv1.2, and IKEv2) ECDSA SigVer (SSHv2, TLSv1.2, and IKEv2) Session Encryption/Decryption (TLSv1.2) Session Authentication (TLSv1.2) TLSv1.2 Keying Materials Development DRBG Function	ECDH Public Key: W,E - TLS ECDH Shared Secret: W,E - TLS ECDSA Private Key: W,E - TLS ECDSA Public Key: W,E - TLS RSA Private Key: W,E - TLS RSA Public Key: W,E - TLS Master Secret: W,E - TLS Session Encryption Key: W,E - TLS Session Authentication Key: W,E - DRBG Entropy Input: W,E - Counter DRBG Seed: W,E - Counter DRBG Internal State V: W,E - Counter DRBG Key: W,E User

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- TLS DH Private Key: W,E - TLS DH Public Key: W,E - TLS Peer DH Public Key: W,E - TLS DH Shared Secret: W,E - TLS ECDH Private Key: W,E - TLS ECDH Public Key: W,E - TLS Peer ECDH Public Key: W,E - TLS ECDH Shared Secret: W,E - TLS ECDSA Private Key: W,E - TLS ECDSA Public Key: W,E - TLS RSA Private Key: W,E - TLS RSA Public Key: W,E - TLS Master Secret: W,E - TLS Session Encryption

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key: W,E - TLS Session Authentication Key: W,E - DRBG Entropy Input: W,E - Counter DRBG Seed: W,E - Counter DRBG Internal State V: W,E - Counter DRBG Key: W,E
Run IPSec/IKEv2 Function	Execute IPsec/IKEv2 Function	Status Mode Indicator "FIPS is currently enabled" and succesful IPsec/IKEv2 log message	Initiate IPsec/IKEv2 tunnel establishment request	Status of IPSec/IKEv2 tunnel establishment	KAS-ECC-KeyGen (IKEv2) KAS-FFC-KeyGen (IKEv2) KAS-ECC (IKEv2) KAS-FFC (IKEv2) RSA SigGen (SSHv2, TLSv1.2, IKEv2) ECDSA SigGen (SSHv2, TLSv1.2 and IKEv2) RSA SigVer (SSHv2, TLSv1.2, and IKEv2) ECDSA SigVer (SSHv2, TLSv1.2, and IKEv2) Session Encryption/Decryption (IPSec/IKE)	Crypto Officer - IPSec/IKE DH Private Key: W,E - IPSec/IKE DH Public Key: W,E - IPSec/IKE Peer DH Public Key: W,E - IPSec/IKE DH Shared Secret: W,E - IPSec/IKE ECDH Private Key: W,E - IPSec/IKE ECDH Public Key: W,E - IPSec/IKE Peer ECDH Public Key: W,E - IPSec/IKE

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					Session Authentication (IPSec/IKEv2) IPSec/IKEv2 Keying Materials Development DRBG Function	ECDH Shared Secret: W,E - IPSec/IKE ECDSA Private Key: W,E - IPSec/IKE ECDSA Public Key: W,E - IPSec/IKE RSA Private Key: W,E - IPSec/IKE RSA Public Key: W,E - IPSec/IKE Pre-shared Secret: W,E - SKEYSEED: W,E - IPSec/IKE Session Encryption Key: W,E - IPSec/IKE Authentication Key: W,E - DRBG Entropy Input: W,E - Counter DRBG Seed: W,E - Counter DRBG Internal State V: W,E - Counter DRBG Key: W,E User - IPSec/IKE

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						DH Private Key: W,E - IPSec/IKE DH Public Key: W,E - IPSec/IKE Peer DH Public Key: W,E - IPSec/IKE DH Shared Secret: W,E - IPSec/IKE ECDH Private Key: W,E - IPSec/IKE ECDH Public Key: W,E - IPSec/IKE Peer ECDH Public Key: W,E - IPSec/IKE ECDH Shared Secret: W,E - IPSec/IKE ECDSA Private Key: W,E - IPSec/IKE ECDSA Public Key: W,E - IPSec/IKE RSA Private Key: W,E - IPSec/IKE RSA Public Key: W,E - IPSec/IKE Pre-shared Secret: W,E - SKEYSEED

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						: W,E - IPSec/IKE Session Encryption Key: W,E - IPSec/IKE Authentication Key: W,E - DRBG Entropy Input: W,E - Counter DRBG Seed: W,E - Counter DRBG Internal State V: W,E - Counter DRBG Key: W,E
Run SNMPv3 Function	Execute SNMPv3 Function	Status Mode Indicator "FIPS is currently enabled" and successful SNMPv3 log message	Initiate SNMPv3 tunnel establishment request	Status of SNMPv3 tunnel establishment	Session Encryption/Decryption (SNMPv3) Session Authentication (SNMPv3) SNMPv3 Keying Materials Development	Crypto Officer - SNMPv3 Shared Secret: W,E - SNMPv3 Encryption Key: W,E - SNMPv3 Authentication Key: W,E User - SNMPv3 Shared Secret: W,E - SNMPv3 Encryption Key: W,E - SNMPv3 Authentication Key: W,E
Firmware Load Test	Execute the	Successful	Commands to load	Outcome of the	Firmware Load Test	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	Firmware Load Test	Firmware Loading status message	new firmware image	Firmware Load Test		- Firmware Load Test Key: R

Table 14: Approved Services

4.4 Non-Approved Services

Name	Description	Algorithms	Role
SSHv2	Run SSHv2 using non-approved algorithms. Non-Approved mode indicator "FIPS is currently disabled" and successful SSHv2 log message demonstrates the non-approved service	3DES ChaCha20-poly1305	Crypto Officer, User
TLSv1	Run TLSv1 in the non-approved mode using non-approved algorithms. Non-Approved mode indicator "FIPS is currently disabled" and successful TLSv1 log message demonstrates the non-approved service	3DES	Crypto Officer, User
TLSv1.2	Run TLSv1.2 using non-approved algorithms. Non-Approved mode indicator "FIPS is currently disabled" and successful TLSv1.2 log message demonstrates the non-approved service	3DES	Crypto Officer, User
TLSv1.3	Run TLSv1.3 in the non-approved mode using non-approved algorithms. Non-Approved mode indicator "FIPS is currently disabled" and successful TLSv1.3 log message demonstrates the non-approved service	ChaCha20-poly1305	Crypto Officer, User
IPsec/IKEv2	Run IPsec/IKEv2 using non-approved algorithms. Non-Approved mode indicator "FIPS is currently disabled" and successful IPsec/IKEv2 log message demonstrates the non-approved service	3DES	Crypto Officer, User
SNMPv3	Run SNMPv3 using non-approved algorithms. Non-Approved mode indicator "FIPS is currently disabled" and successful SNMPv3 log message demonstrates the non-approved service	3DES	Crypto Officer, User

Table 15: Non-Approved Services

4.5 External Software/Firmware Loaded

The module supports the firmware load test by using HMAC-SHA2-512 (HMAC Cert. #A4446) for the new validated firmware to be uploaded into the module. A Firmware Load Test Key was preloaded to the module's binary at the factory and used for firmware load test. In order to load new firmware, the Crypto Officer must authenticate to the module before loading the firmware. This ensures that unauthorized access and use of the module is not performed. The module will

load the new update upon reboot. The update attempt will be rejected if the verification fails. Any firmware loaded into the module that is not shown on the module certificate, is out of scope of this validation and requires a separate FIPS 140-3 validation.

4.6 Bypass Actions and Status

The module implements alternating Bypass service. Traffic output from the module's data output interface can be cryptographically protected via IPSec/IKE VPN, or passed as plaintext (Bypass state), depending on the VPN tunnel establishment on the dedicated data output interface. The operator shall assume Crypto Officer role so as to configure IPSec/IKE VPN capability. If no IPSec/IKE VPN was configured, Module would enter the Bypass state.

Before the module executes the Bypass service (sending out plaintext traffic via the data output interface), the module would conduct two independent internal actions to prevent the inadvertent bypass of plaintext data due to a single error. The Crypto Officer can use commands "show access-list" and "show crypto ipsec sa" to verify the module's Bypass status. In Bypass tests fail, the module would enter an error state, and drop the traffic.

4.7 Cryptographic Output Actions and Status

The module implements Self-initiated cryptographic output capability without external operator request. The Crypto Officer shall configure self-initiated cryptographic output capability. Prior to executing the self-initiated cryptographic output capability, the module conducts two independent internal actions to activate the capability to prevent the inadvertent output due to a single error.

4.8 Additional Information

The module supports unauthenticated service. The unauthenticated operator can trigger the self-test service by power-cycling the module, and is able to observe the module's LEDs status.

5 Software/Firmware Security

5.1 Integrity Techniques

The module is provided in the form of binary executable code. To ensure firmware security, the module is protected by RSA 2048 bits with SHA2-512 (RSA Cert. #A4446) algorithm. A Firmware Integrity Test Key (non-SSP) was preloaded to the module's binary at the factory and used for firmware integrity test only at the pre-operational self-test. The module uses the RSA 2048 bits modulus public key to verify the digital signature. If the firmware integrity test fails, the module would enter to an Error state with all crypto functionality inhibited.

5.2 Initiate on Demand

Integrity test is performed as part of the Pre-Operational Self-Tests. It is automatically executed at power-on. The operator can power-cycle or reboot the tested platform to initiate the firmware integrity test on-demand.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

7 Physical Security

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Production-grade components with standard passivation	N/A	N/A

Table 16: Mechanisms and Actions Required

The module utilizes a production-grade enclosure.

8 Non-Invasive Security

N/A for this module.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
DRAM	Volatile Memory	Dynamic
Flash	Non-Volatile Memory	Static

Table 17: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Peer Public Key Input	External (Outside of the Module's Boundary)	Module	Plaintext	Automated	Electronic	
Module Public Key Output	Module	External (Outside	Plaintext	Automated	Electronic	

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
		of the Module's Boundary)				
Password/Secret Input via SSHv2 encrypted by AES and HMAC	External (Outside of the Module's Boundary)	Module	Encrypted	Automated	Electronic	KTS (SSHv2 with AES and HMAC)
Password/Secret Input via SSHv2 encrypted by AES-GCM	External (Outside of the Module's Boundary)	Module	Encrypted	Automated	Electronic	KTS (SSHv2 with AES-GCM)
Password/Secret Input via TLSv1.2 encrypted by AES and HMAC	External (Outside of the Module's Boundary)	Module	Encrypted	Automated	Electronic	KTS (TLSv1.2 with AES and HMAC)
Password/Secret Input via TLSv1.2 encrypted by AES-GCM	External (Outside of the Module's Boundary)	Module	Encrypted	Automated	Electronic	KTS (TLSv1.2 with AES-GCM)

Table 18: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Zeroization Command	CO issues zeroization service	The zeroization command will erase all SSPs stored in the DRAM or in the Flash of the module.	'configure factory-default' command
Session termination	Zeroization upon session termination	Session termination will automatically zeroize all session based temporary SSPs	Terminate session
Reboot	Zeroization upon rebooting the module	Reboot to zeroize all temporary SSPs stored in Module's DRAM	Reboot

Table 19: SSP Zeroization Methods

Please note that the Firmware Load Test Key is only used for Firmware Load Test Authentication and not subject to the zeroization requirement.

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
DRBG Entropy Input	Used to seed the DRBG	384 bits - at least 256 bits	Entropy Input - CSP			DRBG Function
Counter DRBG Seed	Used in DRBG Generation	256, 320 or 384 bits - 128, 192 or 256 bits	DRBG Seed - CSP			DRBG Function
Counter DRBG Internal State V	Used in DRBG Generation	128 bits - 128 bits	DRBG Internal State - CSP			DRBG Function
Counter DRBG Key	Used in DRBG Generation	128, 192 or 256 bits - 128, 192 or 256 bits	DRBG Internal State - CSP			DRBG Function
User Password	User authentication	8-30 Characters - 8-30 Characters	Authentication Data - CSP			
Crypto Officer Password	Crypto Officer authentication	8-30 Characters - 8-30 Characters	Authentication Data - CSP			
Firmware Load Test Key	Used for Firmware Load Test	112 bits - 112 bits	Public Key - CSP			Firmware Load Test
SSH DH Private Key	Used to derive the SSH DH Shared Secret	MODP-2048, MODP-3072, MODP-4096 -	Private Key - CSP	KAS-FFC-KeyGen (SSHv2)		KAS-FFC (SSHv2)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		112-152 bits				
SSH DH Public Key	Used to derive SSH DH Shared Secret	MODP-2048, MODP-3072, MODP-4096 - 112-152 bits	Public Key - PSP		KAS-FFC-KeyGen (SSHv2)	
SSH Peer DH Public Key	Used to derive SSH DH Shared Secret	MODP-2048, MODP-3072, MODP-4096 - 112-152 bits	Public Key - PSP			KAS-FFC (SSHv2)
SSH DH Shared Secret	Used to derive SSH Session Encryption Keys, SSH Session Authentication Keys	MODP-2048, MODP-3072, MODP-4096 - 112-152 bits	Shared Secret - CSP		KAS-FFC (SSHv2)	SSHv2 Keying Materials Development
SSH ECDH Private Key	Used to derive the SSH ECDH Shared Secret	Curves: 256, 384, 521 bits - 128 to 256 bits	Private Key - CSP	KAS-ECC-KeyGen (SSHv2)		KAS-ECC (SSHv2)
SSH ECDH Public Key	Used to derive SSH ECDHE Shared Secret	Curves: 256, 384, 521 bits - 128-256 bits	Public Key - PSP		KAS-ECC-KeyGen (SSHv2)	
SSH Peer ECDH Public Key	Used to derive SSH DH Shared Secret	Curves: 256, 384, 521 bits - 128 to 256 bits	Public Key - PSP			KAS-ECC (SSHv2)
SSH ECDH	Used to derive SSH Session	Curves: 256, 384, 521	Shared Secret - CSP		KAS-ECC (SSHv2)	SSHv2 Keying Materials Development

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Shared Secret	Encryption Keys, SSH Session Authentication Keys	bits - 128 to 256 bits				
SSH RSA Private Key	Used for SSH session authentication	Modulus 2048 and 3072 bits - 112-128 bits	Private Key - CSP	RSA KeyGen (SSHv2, TLSv1.2, IKEv2)		RSA SigGen (SSHv2, TLSv1.2, IKEv2)
SSH RSA Public Key	Used for SSH sessions aiuthentication	Modulus 2048 and 3072 bits - 112-128 bits	Public Key - PSP		RSA KeyGen (SSHv2, TLSv1.2, IKEv2)	
SSH ECDSA Private Key	Used for SSH session authentication	Curves: 256, 384, 521 bits - 128 to 256 bits	Private Key - CSP	ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2)		ECDSA SigGen (SSHv2, TLSv1.2 and IKEv2)
SSH ECDSA Public Key	Used for SSH sessions aiuthentication	Curves: 256, 384, 521 bits - 128 to 256 bits	Public Key - PSP		ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2)	
SSH Session Encryption Key	Used for SSH Session confidentiality protection	128-256 bits - 128-256 bits	Session Key - CSP		SSHv2 Keying Materials Development	Session Encryption/Decryption (SSHv2)
SSH Session Authentication Key	Used for SSH Session integrity protection	At least 160 bits - At least 160 bits	Session Key - CSP		SSHv2 Keying Materials Development	Session Authentication (SSHv2)
TLS DH Private Key	Used to Derive TLS DH Shared Secret	ffdhe2048 - 112 bits	Private Key - CSP	KAS-FFC-KeyGen (TLSv1.2)		KAS-FFC (TLSv1.2)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
TLS DH Public Key	Used to Derive TLS DH Shared Secret	ffdhe2048 - 112 bits	Public Key - PSP		KAS-FFC-KeyGen (TLSv1.2)	
TLS Peer DH Public Key	Used to derive TLS DH Shared Secret	ffdhe2048 - 112 bits	Public Key - PSP			KAS-FFC (TLSv1.2)
TLS DH Shared Secret	This CSP is also referred to TLS pre-master secret if Diffie-Hellman is used for TLS key agreement. This CSP is used for TLS master secret derivation	ffdhe2048 - 112 bits	Shared Secret - CSP		KAS-FFC (TLSv1.2)	TLSv1.2 Keying Materials Development
TLS ECDH Private Key	Used to Derive TLS ECDH Shared Secret	Curves P-256, P-384, and P-521 - 128-256 bits	Private Key - CSP	KAS-ECC-KeyGen (TLSv1.2)		KAS-ECC (TLSv1.2)
TLS ECDH Public Key	Used to Derive TS ECDH Shared Secret	Curves P-256, P-384, and P-521 - 128-256 bits	Public Key - PSP		KAS-ECC-KeyGen (TLSv1.2)	
TLS Peer ECDH Public Key	Used to derive IKE ECDH Shared Secret	Curves: P-256, P-384, P-521 - 128-256 bits	Public Key - PSP			KAS-ECC (TLSv1.2)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
TLS ECDH Shared Secret	This CSP is also referred to TLS pre-master secret if EC Diffie-Hellman is used for TLS key agreement. This CSP is used for TLS master secret derivation	Curves p-256, P-384, P-521 - 128-256 bits	Shared Secret - CSP		KAS-ECC (TLSv1.2)	TLSv1.2 Keying Materials Development
TLS ECDSA Private Key	Used to support CO and Admin HTTPS interfaces	Curves P-256, P-384, P-521 - 128-256 bits	Private Key - CSP	ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2)		ECDSA SigGen (SSHv2, TLSv1.2 and IKEv2)
TLS ECDSA Public Key	Used to support CO and User HTTPS Interfaces	Curves P-256, P-384, P-521 - 128-256 bits	Public Key - PSP		ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2)	
TLS RSA Private Key	Used to support CO and Admin HTTPS Interfaces	Modulus 2048 and 3072 bits - 112-128 bits	Private Key - CSP	RSA KeyGen (SSHv2, TLSv1.2, IKEv2)		RSA SigGen (SSHv2, TLSv1.2, IKEv2)
TLS RSA Public Key	Used to support CO and User HTTPS interfaces	Modulus 2048 and 3072 bits - 112-128 bits	Public Key - PSP		RSA KeyGen (SSHv2, TLSv1.2, IKEv2)	
TLS Master Secret	Used to protect HTTPS Session.	At least 112 bits - At	Master Secret - CSP		TLSv1.2 Keying Materials	TLSv1.2 Keying Materials Development

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	Pre-master secret	least 112 bits			Development	
TLS Session Encryption Key	Used to protect HTTPS Session. TLS Master secret	128-256 bits - 128-256 bits	Session Key - CSP		TLSv1.2 Keying Materials Development	Session Encryption/Decryption (TLSv1.2)
TLS Session Authentication Key	Used to protect HTTPS Session. TLS master secret	at least 112 bits - at least 112 bits	Session Key - CSP		TLSv1.2 Keying Materials Development	Session Authentication (TLSv1.2)
IPSec/IKE DH Private Key	Used to derive IPSec/IKE DH Shared Secret	MODP-2048, MODP-3072, MODP-4096 - 112-152 bits	Private Key - CSP	KAS-FFC-KeyGen (IKEv2)		KAS-FFC (IKEv2)
IPSec/IKE DH Public Key	Used to derive IPSec/IKE DH Shared Secret	MODP-2048, MODP-3072, MODP-4096 - 112-152 bits	Public Key - PSP		KAS-FFC-KeyGen (IKEv2)	
IPSec/IKE Peer DH Public Key	Used to derive IPSec/IKE DH Shared Secret	MODP-2048, MODP-3072, MODP-4096 - 112-152 bits	Public Key - PSP			KAS-FFC (IKEv2)
IPSec/IKE DH Shared Secret	Used to derive IPSec/IKE Session Encryption Keys, IPSec/IKE	MODP-2048, MODP-3072, MODP-4096 -	Shared Secret - CSP		KAS-FFC (IKEv2)	IPSec/IKEv2 Keying Materials Development

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	Authentication Keys	112-152 bits				
IPSec/IKE ECDH Private Key	Used to derive IPSec/IKE ECDH Shared Secrets	Curves P-256, P-384, P-521 - 128-256 bits	Private Key - CSP	KAS-ECC-KeyGen (IKEv2)		KAS-ECC (IKEv2)
IPSec/IKE ECDH Public Key	Used to derive IPSec/IKE ECDH Shared Secrets	Curves P-256, P-384, P-521 - 128-256 bits	Public Key - PSP		KAS-ECC-KeyGen (IKEv2)	
IPSec/IKE Peer ECDH Public Key	Used to derive IPSec/IKE ECDH Shared Secrets	Curves P-256, P-384, P-521 - 128-256 bits	Public Key - PSP			KAS-ECC (IKEv2)
IPSec/IKE ECDH Shared Secret	Used to derive IPSec/IKE ECDH Shared Secrets	Curves P-256, P-384, P-521 - 128-256 bits	Shared Secret - CSP		KAS-ECC (IKEv2)	IPSec/IKEv2 Keying Materials Development
IPSec/IKE ECDSA Private Key	Used for IPSec/IKE peer authentication	Curves P-256, P-384, P-521 - 128-256 bits	Private Key - CSP	ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2)		ECDSA SigGen (SSHv2, TLSv1.2 and IKEv2)
IPSec/IKE ECDSA Public Key	Used for IPSec/IKE peer authentication	Curves P-256, P-384, P-521 - 128-256 bits	Public Key - PSP		ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2)	
IPSec/IKE RSA Private Key	Used for IPSec/IKE peer authentication	Modulus 2048 or 3072 - 112 or 128 bits	Private Key - CSP	RSA KeyGen (SSHv2, TLSv1.2, IKEv2)		RSA SigGen (SSHv2, TLSv1.2, IKEv2)
IPSec/IKE RSA Public Key	Used for IPSec/IKE peer	Modulus 2048 or 3072 -	Public Key - PSP		RSA KeyGen (SSHv2,	

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	authentication	112 or 128 bits			TLSv1.2, IKEv2)	
IPSec/IKE Pre-shared Secret	Used for IPSec/IKE peer authentication	16-32 bytes characters - 16-32 bytes characters	shared secret - CSP			
SKEYSEED	Keying material used to derive the IPSec/IKE Session Encryption Key and IPSec/IKE Authentication Key	160 bits - 160 bits	Keying Material - CSP		IPSec/IKE v2 Keying Materials Development	Session Authentication (IPSec/IKEv2) Session Encryption/Decryption (IPSec/IKE)
IPSec/IKE Session Encryption Key	Used to secure IPSec/IKEv2 session confidentiality	128-256 bits - 128-256 bits	Session Key - CSP		IPSec/IKE v2 Keying Materials Development	Session Encryption/Decryption (IPSec/IKE)
IPSec/IKE Authentication Key	Used to secure IPSec/IKEv2 session integrity	at least 160 bits - at least 160 bits	Session Key - CSP		IPSec/IKE v2 Keying Materials Development	Session Authentication (IPSec/IKEv2)
SNMPv3 Shared Secret	Used for SNMPv3 user authentication	8-32 characters - N/A	Authentication Secret - CSP			
SNMPv3 Encryption Key	Used to protect SNMPv3 traffic confidentiality	128 bits - 128 bits	Encryption Key - CSP		SNMPv3 Keying Materials Development	Session Encryption/Decryption (SNMPv3)
SNMPv3 Authentication Key	Used to secure SNMPv3 traffic integrity	At least 112 bits - At least 112 bits	Authentication Key - CSP		SNMPv3 Keying Materials Development	Session Authentication (SNMPv3)

Table 20: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DRBG Entropy Input		DRAM:Plaintext	Until Reboot	Zeroization Command Session termination Reboot	Counter DRBG Seed:Used With Counter DRBG Internal State V:Used With Counter DRBG Key:Used With
Counter DRBG Seed		DRAM:Plaintext	Until Reboot	Zeroization Command Session termination Reboot	DRBG Entropy Input:Used With Counter DRBG Internal State V:Used With Counter DRBG Key:Used With
Counter DRBG Internal State V		DRAM:Plaintext	Until Reboot	Zeroization Command Session termination Reboot	DRBG Entropy Input:Used With Counter DRBG Seed:Used With Counter DRBG Key:Used With
Counter DRBG Key		DRAM:Plaintext	Until Reboot	Zeroization Command Session termination Reboot	DRBG Entropy Input:Used With Counter DRBG Seed:Used With Counter DRBG Internal State V:Used With
User Password	Password/Secret Input via TLSv1.2 encrypted by AES-GCM Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM Password/Sec	Flash:Encrypted		Zeroization Command	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	ret Input via SSHv2 encrypted by AES and HMAC				
Crypto Officer Password	Password/Secret Input via TLSv1.2 encrypted by AES-GCM Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM Password/Secret Input via SSHv2 encrypted by AES and HMAC	Flash:Encrypted		Zeroization Command	
Firmware Load Test Key		Flash:Plaintext		N/A	
SSH DH Private Key		DRAM:Plaintext	While SSH tunnel is on	Zeroization Command Session termination Reboot	SSH DH Public Key:Paired With SSH Peer DH Public Key:Used With
SSH DH Public Key	Module Public Key Output	DRAM:Plaintext	While SSH tunnel is on	Zeroization Command Session termination Reboot	SSH DH Private Key:Paired With
SSH Peer DH Public Key	Peer Public Key Input	DRAM:Plaintext	While SSH tunnel is on	Zeroization Command Session	SSH DH Private Key:Used With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				termination Reboot	
SSH DH Shared Secret		DRAM:Plaintext	While SSH tunnel is on	Zeroization Command Session termination Reboot	SSH DH Private Key:Derived From SSH DH Public Key:Derived From
SSH ECDH Private Key		DRAM:Plaintext	While SSH tunnel is on	Zeroization Command Session termination Reboot	SSH ECDH Public Key:Paired With SSH Peer ECDH Public Key:Used With
SSH ECDH Public Key	Module Public Key Output	DRAM:Plaintext	While SSH tunnel is on	Zeroization Command Session termination Reboot	SSH ECDH Private Key:Paired With
SSH Peer ECDH Public Key	Peer Public Key Input	DRAM:Plaintext	While SSH tunnel is on	Zeroization Command Session termination Reboot	SSH ECDH Private Key:Used With
SSH ECDH Shared Secret		DRAM:Plaintext	While SSH tunnel is on	Zeroization Command Session termination Reboot	SSH ECDH Private Key:Derived From SSH ECDH Public Key:Derived From
SSH RSA Private Key		Flash:Plaintext		Zeroization Command	SSH RSA Public Key:Paired With
SSH RSA Public Key	Module Public Key Output	Flash:Plaintext		Zeroization Command	SSH RSA Private Key:Paired With
SSH ECDSA Private Key		Flash:Plaintext		Zeroization Command	SSH ECDSA Public Key:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
SSH ECDSA Public Key	Module Public Key Output	Flash:Plaintext		Zeroization Command	SSH ECDSA Private Key:Paired With
SSH Session Encryption Key		DRAM:Plaintext	While SSH tunnel is on	Zeroization Command Session termination Reboot	SSH Session Authentication Key:Used With
SSH Session Authentication Key		DRAM:Plaintext	While SSH tunnel is on	Zeroization Command Session termination Reboot	SSH Session Encryption Key:Used With
TLS DH Private Key		DRAM:Plaintext	While TLS tunnel is on	Zeroization Command Session termination Reboot	TLS DH Public Key:Paired With TLS Peer DH Public Key:Used With
TLS DH Public Key	Module Public Key Output	DRAM:Plaintext	While TLS tunnel is on	Zeroization Command Session termination Reboot	TLS DH Private Key:Paired With
TLS Peer DH Public Key	Peer Public Key Input	DRAM:Plaintext	while TLS tunnel is on	Zeroization Command Session termination Reboot	TLS DH Private Key:Used With
TLS DH Shared Secret		DRAM:Plaintext	While TLS tunnel is on	Zeroization Command Session termination Reboot	TLS ECDH Private Key:Derived From TLS Peer ECDH Public Key:Derived From
TLS ECDH Private Key		DRAM:Plaintext	While TLS tunnel is on	Zeroization Command	TLS ECDH Public Key:Paired With TLS Peer ECDH

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				Session termination Reboot	Public Key:Used With
TLS ECDH Public Key	Module Public Key Output	DRAM:Plaintext	While TLS tunnel is on	Zeroization Command Session termination Reboot	TLS ECDH Private Key:Paired With
TLS Peer ECDH Public Key	Peer Public Key Input	DRAM:Plaintext	while TLS tunnel is on	Zeroization Command Session termination Reboot	TLS ECDH Private Key:Used With
TLS ECDH Shared Secret		DRAM:Plaintext	While TLS tunnel is on	Zeroization Command Session termination Reboot	TLS ECDH Private Key:Derived From TLS Peer ECDH Public Key:Derived From
TLS ECDSA Private Key		Flash:Plaintext		Zeroization Command	TLS ECDSA Public Key:Paired With
TLS ECDSA Public Key	Module Public Key Output	Flash:Plaintext		Zeroization Command	TLS ECDSA Private Key:Paired With
TLS RSA Private Key		Flash:Plaintext		Zeroization Command	TLS RSA Public Key:Paired With
TLS RSA Public Key	Module Public Key Output	Flash:Plaintext		Zeroization Command	TLS RSA Private Key:Paired With
TLS Master Secret		DRAM:Plaintext	While TLS tunnel is on	Zeroization Command Session termination Reboot	TLS ECDH Shared Secret:Derived From
TLS Session Encryption Key		DRAM:Plaintext	While TLS tunnel is on	Zeroization Command Session	TLS Session Authentication Key:Used With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				termination Reboot	
TLS Session Authentication Key		DRAM:Plaintext	While TLS tunnel is on	Zeroization Command Session termination Reboot	TLS Session Encryption Key:Used With
IPSec/IKE DH Private Key		DRAM:Plaintext	While IPSec/IKE v2 tunnel is on	Zeroization Command Session termination Reboot	IPSec/IKE DH Public Key:Paired With IPSec/IKE Peer DH Public Key:Used With
IPSec/IKE DH Public Key	Module Public Key Output	DRAM:Plaintext	While IPSec/IKE v2 tunnel is on	Zeroization Command Session termination Reboot	IPSec/IKE DH Private Key:Paired With
IPSec/IKE Peer DH Public Key	Peer Public Key Input	DRAM:Plaintext	while IPSec/IKE tunnel is on	Zeroization Command Session termination Reboot	IPSec/IKE DH Private Key:Used With
IPSec/IKE DH Shared Secret		DRAM:Plaintext	While IPSec/IKE v2 tunnel is on	Zeroization Command Session termination Reboot	SKEYSEED:Used With
IPSec/IKE ECDH Private Key		DRAM:Plaintext	While IPSec/IKE v2 tunnel is on	Zeroization Command Session termination Reboot	IPSec/IKE ECDH Public Key:Paired With IPSec/IKE Peer ECDH Public Key:Used With
IPSec/IKE ECDH Public Key	Module Public Key Output	DRAM:Plaintext	While IPSec/IKE	Zeroization Command	IPSec/IKE ECDH Private Key:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
			v2 tunnel is on	Session termination Reboot	
IPSec/IKE Peer ECDH Public Key	Peer Public Key Input	DRAM:Plaintext	While IPSec/IKE v2 tunnel is on	Zeroization Command Session termination Reboot	IPSec/IKE ECDH Private Key:Used With
IPSec/IKE ECDH Shared Secret		DRAM:Plaintext	While IPSec/IKE v2 tunnel is on	Zeroization Command Session termination Reboot	SKEYSEED:Used With
IPSec/IKE ECDSA Private Key		Flash:Plaintext		Zeroization Command	IPSec/IKE ECDSA Public Key:Paired With
IPSec/IKE ECDSA Public Key	Module Public Key Output	Flash:Plaintext		Zeroization Command	IPSec/IKE ECDSA Private Key:Paired With
IPSec/IKE RSA Private Key		Flash:Plaintext		Zeroization Command	IPSec/IKE RSA Public Key:Paired With
IPSec/IKE RSA Public Key	Module Public Key Output	Flash:Plaintext		Zeroization Command	IPSec/IKE RSA Private Key:Paired With
IPSec/IKE Pre-shared Secret	Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Sec	Flash:Plaintext	While IPSec/IKE v2 tunnel is on	Zeroization Command	SKEYSEED:Derived to

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	ret Input via TLSv1.2 encrypted by AES-GCM				
SKEYSEED		DRAM:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Session termination Reboot	IPSec/IKE DH Shared Secret:Derived From IPSec/IKE ECDH Shared Secret:Derived From IPSec/IKE Pre-shared Secret:Derived From
IPSec/IKE Session Encryption Key		DRAM:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Session termination Reboot	IPSec/IKE DH Shared Secret:Derived From IPSec/IKE ECDH Shared Secret:Derived From
IPSec/IKE Authentication Key		DRAM:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Session termination Reboot	IPSec/IKE DH Shared Secret:Derived From IPSec/IKE ECDH Shared Secret:Derived From
SNMPv3 Shared Secret	Password/Secret Input via TLSv1.2 encrypted by AES-GCM Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM	DRAM:Plaintext	While SNMPv3 tunnel is on	Zeroization Command	SNMPv3 Encryption Key:Derive To SNMPv3 Authentication Key:Derive To

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	Password/Secret Input via SSHv2 encrypted by AES and HMAC				
SNMPv3 Encryption Key		DRAM:Plaintext	While SNMPv3 tunnel is on	Zeroization Command Session termination Reboot	SNMPv3 Shared Secret:Derived From
SNMPv3 Authentication Key		DRAM:Plaintext	While SNMPv3 tunnel is on	Zeroization Command Session termination Reboot	SNMPv3 Shared Secret:Derived From SNMPv3 Encryption Key:Used With

Table 21: SSP Table 2

9.5 Transitions

- SHA-1: The module includes an implementation of SHA-1 for hashing and digital signature verification. This implementation will be non-Approved for all uses starting January 1, 2031.

- FIPS 186-4/186-5: As of February 5, 2024, the CMVP does not accept module submissions that implement DSA or RSA X9.31 in the approved mode, other than for signature verification which is approved for legacy use. This module does not implement DSA or RSA X9.31 for signature generation and therefore is unaffected by the current transition from 186-4 to 186-5. As detailed in section 2.7, the CAVP testing performed on the 186-4 algorithms is mathematically similar to the testing performed on the 186-5 algorithms and therefore this module claims compliance with 186-5. This means that no timeline exists in which any of the implemented algorithms will transition from approved to non-approved.

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
RSA SigVer (FIPS186-4) (A4446)	RSA SigVer 2048 bits with SHA2-512	KAT	SW/FW Integrity	Module is in normal state	RSA SigVer

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
Pre-Operational Bypass Test	N/A	N/A	Bypass	Module is in normal state	N/A

Table 22: Pre-Operational Self-Tests

The module performs the following self-tests, including the pre-operational self-tests and Conditional self-tests. Prior to the module providing any data output via the data output interface, the module performs and passes the pre-operational self-tests. Following the successful pre-operational self-tests, the module executes the Conditional Cryptographic Algorithm Self-tests (CASTs). If anyone of the self-tests fails, the module transitions into an error state and outputs the error message via the module's status output interface. While the module is in the error state, all data through the data output interface and all cryptographic operations are disabled. The error state can only be cleared by reloading the module. All self-tests must be completed successfully before the module transitions to the operational state.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC Encrypt KAT (A4446)	256 bits	KAT	CAST	Module is in normal state	Encrypt	Power Up
AES-CBC Decrypt KAT (A4446)	256 bits	KAT	CAST	Module is in normal state	Decrypt	Power Up
AES-GCM Authenticated Encrypt KAT (A4446)	256 bits	KAT	CAST	Module is in normal state	Authenticated Encrypt	Power Up
AES-GCM Authenticated Decrypt KAT (A4446)	256 bits	KAT	CAST	Module is in normal state	Authenticated Decrypt	Power Up
Counter DRBG Instantiate/Generate/Reseed KAT (A4446)	AES-128	KAT	CAST	Module is in normal state	Instantiate, Generate, and Reseed KATs	Power Up
ECDSA SigGen (FIPS186-4) KAT (A4446)	P-256 curve with SHA2-256	KAT	CAST	Module is in normal state	ECDSA SigGen KAT	Power Up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ECDSA SigVer (FIPS186-4) KAT (A4446)	P-256 curve with SHA2-256	KAT	CAST	Module is in normal state	ECDSA SigVer KAT	Power Up
HMAC-SHA-1 KAT (A4446)	SHA-1	KAT	CAST	Module is in normal state	HMAC-SHA-1	Power Up
HMAC-SHA2-256 KAT (A4446)	SHA2-256	KAT	CAST	Module is in normal state	HMAC-SHA2-256	Power Up
HMAC-SHA2-384 KAT (A4446)	SHA2-384	KAT	CAST	Module is in normal state	HMAC-SHA2-384	Power Up
HMAC-SHA2-512 KAT (A4446)	SHA2-512	KAT	CAST	Module is in normal state	HMAC-SHA2-512	Power Up
KAS-ECC-SSC Sp800-56Ar3 KAT (A4446)	P-256 Curve	KAT	CAST	Module is in normal state	Primitive Z KAT	Power Up
KAS-FFC-SSC Sp800-56Ar3 KAT (A4446)	MODP-2048	KAT	CAST	Module is in normal state	Primitive Z KAT	Power Up
RSA SigGen (FIPS186-4) KAT (A4446)	2048 bit modulus with SHA2-256	KAT	CAST	Module is in normal state	RSA SigGen KAT	Power Up
RSA SigVer (FIPS186-4) KAT (A4446)	2048 bit modulus with SHA2-256	KAT	CAST	Module is in normal state	RSA SigVer KAT	Power Up
KDF IKEv2 KAT (A4446)	N/A	KAT	CAST	Module is in normal state	N/A	Power Up
KDF SNMP KAT (A4446)	N/A	KAT	CAST	Module is in normal state	N/A	Power Up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
KDF SSH KAT (A4446)	N/A	KAT	CAST	Module is in normal state	N/A	Power Up
TLS v1.2 KDF RFC7627 KAT (A4446)	N/A	KAT	CAST	Module is in normal state	N/A	Power Up
SHA-1 KAT (A4446)	N/A	KAT	CAST	Module is in normal state	N/A	Power Up
AES-CBC Encrypt KAT (C1026)	128 bits	KAT	CAST	Module is in normal state	Encrypt KAT	Power Up
AES-CBC Decrypt KAT (C1026)	128 bits	KAT	CAST	Module is in normal state	Decrypt KAT	Power Up
AES-GCM Authenticated Encrypt KAT (C1026)	128 bits	KAT	CAST	Module is in normal state	Encrypt KAT	Power Up
AES-GCM Authenticated Decrypt KAT (C1026)	128 bits	KAT	CAST	Module is in normal state	Decrypt KAT	Power Up
HMAC-SHA-1 KAT (C1026)	SHA-1	KAT	CAST	Module is in normal state	HMAC-SHA-1	Power Up
HMAC-SHA2-256 KAT (C1026)	SHA2-256	KAT	CAST	Module is in normal state	HMAC-SHA2-256	Power Up
HMAC-SHA2-384 KAT (C1026)	SHA2-384	KAT	CAST	Module is in normal state	HMAC-SHA2-384	Power Up
HMAC-SHA2-512 KAT (C1026)	SHA2-512	KAT	CAST	Module is in normal state	HMAC-SHA2-512	Power Up
ECDSA KeyGen (FIPS186-4) PCT (A4446)	N/A	PCT	PCT	Module is in	ECDSA	Performs all required

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				normal state		pair-wise consistency tests on the newly generated key pairs before the first operational use.
RSA KeyGen (FIPS186-4) PCT (A4446)	N/A	PCT	PCT	Module is in normal state	RSA	Performs all required pair-wise consistency tests on the newly generated key pairs before the first operational use.
KAS-ECC-SSC Sp800-56Ar3 PCT (A4446)	N/A	PCT	PCT	Module is in normal state	N/A	Performs all required pair-wise consistency tests on the newly generated key pairs before the first operational use.
KAS-FFC-SSC Sp800-56Ar3 PCT (A4446)	N/A	PCT	PCT	Module is in normal state	N/A	Performs all required pair-wise consistency tests on the newly

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						generated key pairs before the first operational use.
Firmware Load Test	HMAC-SHA2-512	KAT	SW/FW Load	Module is in normal state	N/A	When firmware has been uploaded to the module
Conditional Bypass	N/A	N/A	Bypass	Module is in normal state	N/A	Performs conditional bypass test before first operational use of bypass service
Entropy 90B Start-up Repetition Count Test (RCT)	Repetition Count Test	RCT	CAST	Module is in normal state	Designed to quickly detect catastrophic failures that cause the noise source to become "stuck" on a single output value for a long period of time	Power up
Entropy 90B Start-up Adaptive Proportion Test (APT)	Adaptive Proportion Test	APT	CAST	Module is in normal state	Designed to detect a large loss of entropy that might occur as a result of some physical failure or environment	Power up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
					al change affecting the noise source	
Entropy 90B Continuous Repetition Count Test (RCT)	Repetition Count Test	RCT	CAST	Module is in normal state	Designed to quickly detect catastrophic failures that cause the noise source to become "stuck" on a single output value for a long period of time	Entropy data is generated from the Entropy Source - Continuous
Entropy 90B Continuous Adaptive Proportion Test (APT)	Adaptive Proportion Test	APT	CAST	Module is in normal state	Designed to detect a large loss of entropy that might occur as a result of some physical failure or environmental change affecting the noise source	Entropy data is generated from the Entropy Source - Continuous

Table 23: Conditional Self-Tests

The module performs on-demand self-tests initiated by the operator, by powering off and powering the module back on. The full suite of self-tests is then executed. The same procedure may be employed by the operator to perform periodic self-tests.

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA SigVer (FIPS186-4) (A4446)	KAT	SW/FW Integrity	Recommend every 60 days	Reboot

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Pre-Operational Bypass Test	N/A	Bypass	Recommend every 60 days	Reboot

Table 24: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CBC Encrypt KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
AES-CBC Decrypt KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
AES-GCM Authenticated Encrypt KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
AES-GCM Authenticated Decrypt KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
Counter DRBG Instantiate/Generate/Reseed KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
ECDSA SigGen (FIPS186-4) KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
ECDSA SigVer (FIPS186-4) KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
HMAC-SHA-1 KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
HMAC-SHA2-256 KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
HMAC-SHA2-384 KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
HMAC-SHA2-512 KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
KAS-ECC-SSC Sp800-56Ar3 KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
KAS-FFC-SSC Sp800-56Ar3 KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA SigGen (FIPS186-4) KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
RSA SigVer (FIPS186-4) KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
KDF IKEv2 KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
KDF SNMP KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
KDF SSH KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
TLS v1.2 KDF RFC7627 KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
SHA-1 KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
AES-CBC Encrypt KAT (C1026)	KAT	CAST	Recommend every 60 days	Reboot
AES-CBC Decrypt KAT (C1026)	KAT	CAST	Recommend every 60 days	Reboot
AES-GCM Authenticated Encrypt KAT (C1026)	KAT	CAST	Recommend every 60 days	Reboot
AES-GCM Authenticated Decrypt KAT (C1026)	KAT	CAST	Recommend every 60 days	Reboot
HMAC-SHA-1 KAT (C1026)	KAT	CAST	Recommend every 60 days	Reboot
HMAC-SHA2-256 KAT (C1026)	KAT	CAST	Recommend every 60 days	Reboot
HMAC-SHA2-384 KAT (C1026)	KAT	CAST	Recommend every 60 days	Reboot
HMAC-SHA2-512 KAT (C1026)	KAT	CAST	Recommend every 60 days	Reboot
ECDSA KeyGen (FIPS186-4) PCT (A4446)	PCT	PCT	Recommend every 60 days	Reboot

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA KeyGen (FIPS186-4) PCT (A4446)	PCT	PCT	Recommend every 60 days	Reboot
KAS-ECC-SSC Sp800-56Ar3 PCT (A4446)	PCT	PCT	Recommend every 60 days	Reboot
KAS-FFC-SSC Sp800-56Ar3 PCT (A4446)	PCT	PCT	Recommend every 60 days	Reboot
Firmware Load Test	KAT	SW/FW Load	N/A	N/A
Conditional Bypass	N/A	Bypass	N/A	N/A
Entropy 90B Start-up Repetition Count Test (RCT)	RCT	CAST	N/A	N/A
Entropy 90B Start-up Adaptive Proportion Test (APT)	APT	CAST	N/A	N/A
Entropy 90B Continuous Repetition Count Test (RCT)	RCT	CAST	N/A	N/A
Entropy 90B Continuous Adaptive Proportion Test (APT)	APT	CAST	N/A	N/A

Table 25: Conditional Periodic Information

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Error State	If self-test tests fail, the module is put into an error state	Self-test failure	Reboot the module	System Halt

Table 26: Error States

If any of the above-mentioned self-tests fail, the module reports the error and enters the Error state. In the Error State, no cryptographic services are provided, and data output is prohibited. The only method to recover from the error state is to reboot the module and perform the self-tests, including the pre-operational firmware integrity test and the conditional CASTs. The module will only enter into the operational state after successfully passing the pre-operational firmware integrity test and the conditional CASTs.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The validated module firmware was installed onto the respective test platforms listed in Table 2 above. Any firmware loaded into the module that is not shown on the module certificate, is out of

scope of this validation and requires a separate FIPS 140-3 validation. The Crypto Officer must configure and enforce the following initialization steps.

Secure Installation
The Crypto Officer must ensure that:

- The module is installed in a secure physical location.
- Physical access to the module is restricted to authorized personnel only.

Approved Mode of Operation:

Step 1: Crypto Officer performs the following configurations:

ciscoasa# configure terminal
Note, the Crypto Officer needs to connect the platform to cisco.com to obtain the license for ASA from Cisco.
ciscoasa(config)# license smart register idtoken [token data]
ciscoasa(config)#license smart
ciscoasa(config-smart-lic)# show license all
Smart Licensing Status
==========
Smart Licensing is ENABLED

-OR-

ciscoasa(config-smart-lic)# show license summary
Smart Licensing is ENABLED
Registration:

Step 2: Enable “Approved Mode” on the module to allow the module to operate in the approved mode of operation. While in the approved mode, any non-approved algorithms or services will be rejected by the module automatically.
ciscoasa(config)# fips enable

Note: Approved mode will not take effect until the operator saves configuration and reboots the device. Rebooting the device will force new self-test.

Once the module is rebooted, use the following command to check module’s approved mode status
ciscoasa(config)# show fips
FIPS is currently enabled.

While in the Approved mode, the `show fips` command will output “FIPS is currently enabled” and the module will enforce that only approved algorithms and services described in this Security Policy may be used.

Step 3: Crypto Officer can verify the firmware and hardware version installed and running
ciscoasa(config)# show version

Step 4: Crypto Officer will need to configure ASA

ciscoasa> en
ciscoasa# conf t
ciscoasa(config)#

Step 5: Assign users a Privilege Level of 1.

ciscoasa(config)# username <username> password <password> privilege 1

Step 6: Configure IP address for unit and all distant endpoints.

ciscoasa(config)# ip address <ip-address> <mask>

Step 7: Configure the security module so that any remote connections via Telnet are secured through IPSec.

ciscoasa(config)# crypto map interface
ciscoasa(config)# access-list
ciscoasa(config)# protocol esp encryption aes
ciscoasa(config)# protocol esp integrity sha-256

Note: If the destined IP address is not within access-list, after running two internal independent actions defined in section 4.6 above, the module would enter the Bypass state.

Step 8: Configure the security services by using the algorithms from section 2.5 Approved Algorithms table in this document for all security connections (SSHv2, TLSv1.2, SNMPv3 and IPSec/IKEv2). Note the module will reject any configuration with algorithms not listed in Approved Algorithm Table after the module is operated in approved mode.

Here is an example of configuring the approved algorithms for the security services:

SSH:

ciscoasa(config)# ssh cipher encryption custom aes128-gcm@openssh.com
ciscoasa(config)# ssh cipher integrity custom hmac-sha2-256
ciscoasa(config)# ssh key-exchange group ecdh-sha2-nistp256

TLSv1.2:

ciscoasa(config)# ssl cipher tlsv1.2 ecdhe-rsa-aes128-sha

SNMPv3:

ciscoasa(config)# snmp-server user <SNMP username> <group name> v3 auth sha <auth password> priv aes 128 <priv password>

IKEv2:

ciscoasa(config)# crypto ikev2 policy <policy number>
ciscoasa(config)# encryption aes

ciscoasa(config)# integrity sha256
ciscoasa(config)# group 14

IPsec:

ciscoasa(config)# crypto ipsec ikev2 ipsec-proposal <name your proposal>
ciscoasa(config)# protocol esp encryption aes
ciscoasa(config)# protocol esp integrity sha-256

The module cannot be configured with any non-approved algorithms. Only algorithms described in this Security Policy can be used to configure the modules security services.

Step 9: Configure the security module so that error messages can only be viewed by Crypto Officer.

ciscoasa(config)# privilege show level 15 mode exec command logging

Step 10: Disable the TFTP server.

ciscoasa(config)# policy-map global_policy
ciscoasa(config)# class inspection_default
ciscoasa(config)# no inspect tftp

Step 11: Disable HTTP for performing system management in approved mode of operation. HTTPS with TLS should always be used for Web-based management.

ciscoasa(config)# no http server enable

Step 12: Save the configuration.

ciscoasa(config)# write memory

Step 13: Reboot the module.

ciscoasa(config)# reload

Non-Approved Mode of Operation:
To change the mode of operation to the “Non-Approved” mode (**which is not recommended by Cisco**) the following commands must be used:

ciscoasa(config)# configure factory-default
ciscoasa(config)# no fips enable

Note: This will remove the entire configuration and zeroize all SSPs; Non-Approved mode will not take effect until the operator saves configuration and reboots the device. Rebooting the device will force new self-test.

Once the module is rebooted, use the following command to check module’s non-approved mode status

ciscoasa(config)# show fips
FIPS is currently disabled.

While in the Non-Approved mode, the `show fips` command will output “FIPS is currently disabled” and the module will allow both Approved and Non-Approved algorithms and services described in this Security Policy to be used.

11.2 Administrator Guidance

Further Specific Administrator guidance can be found in the ASA Series General Operations CLI Configuration Guide: https://www.cisco.com/c/en/us/td/docs/security/asa/asa919/configuration/general/asa-919-general-config.html

11.3 Non-Administrator Guidance

Further Non-Administrator guidance can be found in the Datasheets for Firepower series 4100 and 9300: https://www.cisco.com/c/en/us/products/collateral/security/firepower-4100-series/datasheet-c78-742474.html and https://www.cisco.com/c/en/us/products/collateral/security/firepower-9000-series/datasheet-c78-742471.html

12 Mitigation of Other Attacks

N/A for this module.