Palo Alto Networks

SD-WAN ION Core Crypto Module

Software Version: 1.0

FIPS 140-3 Non-Proprietary Security Policy

Documentation Version: 1.3

Last Update: June 11, 2024

Palo Alto Networks, Inc.
www.paloaltonetworks.com

Revision Date: June 11, 2024
Document Version: 1.3

Table of Contents

1. General

The table below provides the security levels of the various sections of FIPS 140-3 in relation to the Palo Alto Networks SD-WAN ION Core Crypto Module with software version 1.0, hereinafter referred to as the Module.

The Palo Alto Networks SD-WAN ION Core Crypto Module is utilized in hardware and software ION form factors. These enable the integration of a diverse set of wide area network (WAN) connection types, improve application performance and visibility, enhance security and compliance, and reduce the overall cost and complexity of a WAN.

The Module contains the following libraries:

- Palo Alto Networks SD-WAN Instant-On Network (ION) Crypto Library - I
- Palo Alto Networks SD-WAN Instant-On Network (ION) Crypto Library - II

ISO/IEC 24759 Section 6. [Number Below]	FIPS 140-3 Section Title	Security Level
1	General	1
2	Cryptographic module specification	1
3	Cryptographic module interfaces	1
4	Roles, services, and authentication	1
5	Software/Firmware security	1
6	Operational environment	1
7	Physical security	N/A
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

Table 1 – Security Levels

The module is designed to meet an overall security level of 1.

2. Cryptographic Module Specification

The module is a software module running on a multi-chip standalone general-purpose computing platform. FIPS 140-3 conformance testing was performed at Security Level 1 with the following configurations noted in the table 2 below.

#	Operating System	Hardware Platform	Processor	PAA/Acceleration
1	ION 6.1	ION 1200	Intel Atom C3436L	With PAA
2	ION 6.1	ION 1200	Intel Atom C3436L	Without PAA
3	ION 6.1	ION 1200-C-NA	Intel Atom C3436L	With PAA
4	ION 6.1	ION 1200-C-NA	Intel Atom C3436L	Without PAA
5	ION 6.1	ION 1200-C-ROW	Intel Atom C3436L	With PAA
6	ION 6.1	ION 1200-C-ROW	Intel Atom C3436L	Without PAA
7	ION 6.1	ION 1200-C-5G-WW	Intel Atom C3436L	With PAA
8	ION 6.1	ION 1200-C-5G-WW	Intel Atom C3436L	Without PAA
9	ION 6.1	ION 1200-S	Intel Atom C3436L	With PAA
10	ION 6.1	ION 1200-S	Intel Atom C3436L	Without PAA
11	ION 6.1	ION 1200-S-C-NA	Intel Atom C3436L	With PAA
12	ION 6.1	ION 1200-S-C-NA	Intel Atom C3436L	Without PAA
13	ION 6.1	ION 1200-S-C-ROW	Intel Atom C3436L	With PAA

14	ION 6.1	ION 1200-S-C-ROW	Intel Atom C3436L	Without PAA
15	ION 6.1	ION 1200-S-C-5G-WW	Intel Atom C3436L	With PAA
16	ION 6.1	ION 1200-S-C-5G-WW	Intel Atom C3436L	Without PAA
17	ION 6.1	ION 3200	Intel Atom C3558R	With PAA
18	ION 6.1	ION 3200	Intel Atom C3558R	Without PAA
19	ION 6.1	ION 5200	Intel Atom C5325	With PAA
20	ION 6.1	ION 5200	Intel Atom C5325	Without PAA
21	ION 6.1	ION 9200	Intel Atom P5362	With PAA
22	ION 6.1	ION 9200	Intel Atom P5362	Without PAA

Table 2 – Tested Operational Environments

#	Operating System	Hardware Platform
1	AWS	Dependent on Provider
2	Azure	Dependent on Provider
3	Google Cloud	Dependent on Provider
4	OCI	Dependent on Provider
5	ION 7108V	GPC
6	ION 3108V	GPC

Table 3 – Vendor Affirmed Operational Environments

The CMVP makes no statement as to the correct operation of the module or the security strengths of the generated keys when ported to an operational environment which is not listed on the validation certificate.

Modes of Operation

The module has one approved mode of operation and is always in approved mode of operation after initial operations are performed (See Section 11). The module does not claim implementation of a degraded mode of operation. Section 4 provides details on the service indicator implemented by the module.

The tables below list all Approved or Vendor-affirmed security functions of the module, including specific key size(s) (in bits unless noted otherwise) employed for Approved services, and implemented modes of operation. There are some algorithm modes that were tested but not implemented by the module. Only the algorithms, modes, and key sizes that are implemented by the module are shown in these tables.

CAVP Cert	Algorithm and Standard	Mode/Method	Description/Key Size(s) / Key Strength(s)	Use / Function
A3566	AES: • FIPS 197 • SP 800-38D	ECB	128, 192, and 256 bits	Data Encryption/Decryption
A3566	AES: • FIPS 197 • SP 800-38A	CBC	128, 192, and 256 bits	Data Encryption/Decryption
A3566	AES: • FIPS 197 • SP 800-38A	CTR	128, 192, and 256 bits	Data Encryption/Decryption
A3566	AES: • FIPS 197 • SP 800-38D	GCM	128, 192, and 256 bits	Data Encryption/Decryption
A3566	KDF SSH: • SP 800-135rev1 (CVL)	KDF SSHv2	N/A	SP800-135rev1 compliant Key Derivation
A3566	KDF TLS: • SP 800-135rev1 (CVL)	KDF TLS 1.2	N/A	SP800-135rev1 compliant Key Derivation

CAVP Cert	Algorithm and Standard	Mode/Method	Description/Key Size(s) / Key Strength(s)	Use / Function
A3566	KDF KEv2: • SP 800-135rev1 (CVL)	KDF IKEv2	N/A	SP800-135rev1 compliant Key Derivation
A3566	KDF SNMP: • SP 800-135rev1 (CVL)	KDF SNMPv3	N/A	SP800-135rev1 compliant Key Derivation
A3566	DRBG: • SP 800-90Arev1	CTR_DRBG (AES-256 bits) Derivation Function Enabled: Yes	N/A	Deterministic Random Bit Generation
A3566	KAS-SSC • SP 800-56Arev3	KAS-ECC-SSC Ephemeral Unified	KAS-ECC-SSC with P-256, P-384, P-521; key establishment methodology provides between 128 and 256 bits of encryption strength	KAS-ECC Shared Secret Computation
A3566	KAS • SP 800-56Arev3	KAS (ECC) Scheme: ephemeralUnified: KAS Role: initiator, responder	KAS (ECC): Curves: P-256, P-384, P-521; Key establishment methodology provides between 128 and 256 bits of encryption strength	Key Agreement Scheme per SP800-56Arev3 with key derivation function (SP800-135rev1) Note: The module's KAS (ECC) implementation is FIPS140-3 IG D.F Scenario 2 (path 2) compliant
A3566	ECDSA • FIPS 186-4	ECDSA KeyGen	Curves: P-224, P-256, P-384, P-521	ECDSA Key Generation
A3566	ECDSA • FIPS 186-4	ECDSA SigGen	Curves: P-224, P-256, P-384, P-521	ECDSA Digital Signature Generation
A3566	ECDSA • FIPS 186-4	ECDSA SigVer	Curves: P-224, P-256, P-384, P-521	ECDSA Digital Signature Verification
A3566	HMAC • FIPS 198-1	HMAC-SHA-1	At least 160 bits	Message Authentication
A3566	HMAC • FIPS 198-1	HMAC-SHA2-224	At least 160 bits	Message Authentication
A3566	HMAC • FIPS 198-1	HMAC-SHA2-256	At least 160 bits	Message Authentication
A3566	HMAC • FIPS 198-1	HMAC-SHA2-384	At least 160 bits	Message Authentication
A3566	HMAC • FIPS 198-1	HMAC-SHA2-512	At least 160 bits	Message Authentication
A3566	KTS • SP800-38F	KTS (AES Cert. #A3566)	128, 192, and 256 bits Key establishment methodology provides between 128 and 256 bits of encryption strength	Key Transport using AES-GCM
A3566	KTS • SP800-38F	KTS (AES Cert. #A3566 and HMAC Cert. #A3566)	128, 192, and 256 bits Key establishment methodology provides between 128 and 256 bits of encryption strength	Key Transport using AES and HMAC
A3566	RSA • FIPS 186-4	RSA KeyGen (PKCS#1 v1.5)	Modulus: 2048 and 3072 bits	RSA Key Generation
A3566	RSA • FIPS 186-4	RSA SigGen (PKCS#1 v1.5)	Modulus: 2048 and 3072 bits	RSA Digital Signature Generation
A3566	RSA • FIPS 186-4	RSA SigVer (PKCS#1 v1.5)	Modulus: 2048 and 3072 bits	RSA Digital Signature Verification
A3566	SHS • FIPS 180-4	SHA-1	N/A	Hashing Note: SHA-1 is not used for digital signature generation
A3566	SHS • FIPS 180-4	SHA2-224	N/A	Hashing

CAVP Cert	Algorithm and Standard	Mode/Method	Description/Key Size(s) / Key Strength(s)	Use / Function
A3566	SHS • FIPS 180-4	SHA2-256	N/A	Hashing
A3566	SHS • FIPS 180-4	SHA2-384	N/A	Hashing
A3566	SHS • FIPS 180-4	SHA2-512	N/A	Hashing
Vendor Affirmed	CKG (SP 800-133rev2)	Section 5	Cryptographic Key Generation; SP 800-133rev2 and IG D.H.	Key Generation Note: The cryptographic module performs Cryptographic Key Generation (CKG) for asymmetric keys as per section 5 in SP800-133rev2 (vendor affirmed). A seed (i.e., the random value) used in asymmetric key generation is a direct output from SP800-90Arev1 DRBG (DRBG Cert. #A3566).

Table 4 – Approved Algorithms (Crypto Library – I)

CAVP Cert	Algorithm and Standard	Mode/Method	Description/Key Size(s) / Key Strength(s)	Use / Function
A3572	AES: • FIPS 197 • SP 800-38A	CBC	128 or 256 bits	Data Encryption/Decryption
A3572	AES: • FIPS 197 • SP 800-38D	GCM	128 or 256 bits	Data Encryption/Decryption
A3572	KDF TLS: • SP 800-135rev1 (CVL)	KDF TLS v1.2	N/A	SP800-135rev1 compliant Key Derivation
A3572	DRBG: • SP 800-90Arev1	DRBG with HMAC-SHA2-512	N/A	Deterministic Random Bit Generation
A3572	KAS-SSC • SP 800-56Arev3	KAS-ECC-SSC Ephemeral Unified	KAS-ECC-SSC with P-256, P-384, P-521; Key establishment methodology provides between 128 256 bits of encryption strength	KAS-ECC Shared Secret Computation
A3572	KAS • SP 800-56Arev3	KAS (ECC) Scheme: ephemeralUnified: KAS Role: initiator, responder	KAS (ECC): Curves: P-256, P-384, P-521; Key establishment methodology provides between 128 and 256 bits of encryption strength	Key Agreement Scheme per SP800-56Arev3 with key derivation function (SP800-135rev1) Note: The module's KAS (ECC) implementation is FIPS140-3 IG D.F Scenario 2 (path 2) compliant
A3572	ECDSA • FIPS 186-4	ECDSA KeyGen	Curves: P-224, P-256, P-384, P-521	ECDSA Key Generation
A3572	HMAC • FIPS 198-1	HMAC-SHA2-256	At least 160 bits	Message Authentication
A3572	HMAC • FIPS 198-1	HMAC-SHA2-384	At least 160 bits	Message Authentication
A3572	HMAC • FIPS 198-1	HMAC-SHA2-512	At least 160 bits	Message Authentication
A3572	KTS • SP800-38F	KTS (AES Cert. #A3572)	128 or 256 bits Key establishment methodology provides 128 or 256 bits of encryption strength	Key Transport using AES-GCM

CAVP Cert	Algorithm and Standard	Mode/Method	Description/Key Size(s) / Key Strength(s)	Use / Function
A3572	KTS • SP800-38F	KTS (AES Cert. #A3572 and HMAC Cert. #A3572)	128 or 256 bits Key establishment methodology provides 128 or 256 bits of encryption strength	Key Transport using AES and HMAC
A3572	RSA • FIPS 186-4	RSA SigVer (PKCS#1 v1.5)	Modulus: 2048 bits	Digital Signature Verification
A3572	SHS • FIPS 180-4	SHA2-256	N/A	Hashing
A3572	SHS • FIPS 180-4	SHA2-384	N/A	Hashing
A3572	SHS • FIPS 180-4	SHA2-512	N/A	Hashing
Vendor Affirmed	CKG (SP 800-133rev2)	Section 5	Cryptographic Key Generation; SP 800-133rev2 and IG D.H.	Key Generation Note: The cryptographic module performs Cryptographic Key Generation (CKG) for asymmetric keys as per section 5 in SP800-133rev2 (vendor affirmed). A seed (i.e., the random value) used in asymmetric key generation is a direct output from SP800-90Arev1 DRBG (DRBG Cert. #A3572).

Table 5 – Approved Algorithms (Crypto Library – II)

Notes:

- The module's AES-GCM implementation conforms to FIPS 140-3 IG 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 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.
- No parts of the SSH, TLS, SNMP and IPSec/IKE protocols, other than the KDFs, have been tested by the CAVP and CMVP.

Vendor Name	Certificate Number
Palo Alto Networks	E68
Palo Alto Networks	E71

Table 6 - Entropy Certificates

Notes:

- ESV Cert. #E68 is for the module running on tested platform ION-1200, ION 1200-C-NA, ION 1200-C-ROW, ION 1200-C-5G-WW, ION 1200-S, ION 1200-S-C-NA, ION 1200-S-C-ROW, ION 1200-S-C-5G-WW and ION 3200
- ESV Cert. #E71 is for the module running on tested platform ION 5200 and ION 9200

As the module can only be operated in the Approved mode of operation with algorithms listed in Tables 4 - 5, the following options defined in SP 800-140B are not applicable for this document:

- Non-Approved Algorithms Allowed in Approved Mode of Operation
- Non-Approved Algorithms Allowed in Approved Mode of Operation with No Security Claimed
- Non-Approved Algorithms Not Allowed in Approved Mode of Operation

Cryptographic Boundary

Figure 1 below depicts the cryptographic boundary (yellow area with the blue dashed lines) and the physical perimeter (red dashed line). The cryptographic boundary includes all of the software components of the cryptographic libraries. The physical perimeter is the Tested Operational Environment's Physical Perimeter (TOEPP) on which the module runs.

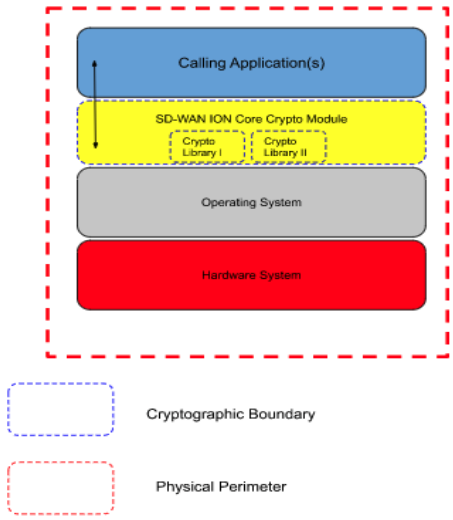

Figure 1– Cryptographic Boundary

3. Cryptographic Module Interfaces

The module's physical perimeter encompasses the case of the tested platform mentioned in Table 2. The module provides its logical interfaces via Application Programming Interface (API) calls. The logical interfaces provided by the module are mapped onto the FIPS 140-3 interfaces (data input, data output, control input, control output and status output) as follows.

Physical Port	Logical Interface	Data that passes over port/interface
N/A	Data Input Interface	API input parameters for data
N/A	Data Output Interface	API output parameters for data
N/A	Control Input Interface	API function calls
N/A	Control Output Interface	N/A
N/A	Status Output Interface	Return values, and or log messages

Table 7 – Ports and Interfaces

4. Roles, Services, and Authentication

The module supports role-based authentication, and provides a Crypto Officer role. The Crypto Officer role has the ability to perform all tasks and administrative actions.

Role	Service	Input	Output
Crypto Officer	Self-Test	Command to trigger Self-Test	Status of the self-tests results
Crypto Officer	Zeroize	Command to initiate the SSPs zeroization	Status of the SSPs zeroization
Crypto Officer	Show Version	Command to show version	Module's name/ID and versions
Crypto Officer	Show Status	Command to show status	Module's status information
Crypto Officer	Configure Network	Commands to configure the module	Status of the completion of network related configuration
Crypto Officer	Configure SSHv2 Function	Commands to configure SSHv2	Status of the completion of SSHv2 configuration
Crypto Officer	Configure TLSv1.2 Function	Commands to configure TLSv1.2	Status of the completion of TLSv1.2 configuration
Crypto Officer	Configure SNMPv3 Function	Commands to configure SNMPv3	Status of the completion of SNMPv3 configuration
Crypto Officer	Configure IPsec/IKEv2 Function	Commands to configure IPSec/IKEv2	Status of the completion of IPSec/IKEv2 configuration
Crypto Officer	Run SSHv2 Function	Initiate SSHv2 tunnel establishment request	Status of SSHv2 tunnel establishment
Crypto Officer	Run TLSv1.2 Function	Initiate TLSv1.2 tunnel establishment request	Status of TLSv1.2 tunnel establishment
Crypto Officer	Run SNMPv3 Function	Initiate SNMPv3 tunnel establishment request	Status of SNMPv3 tunnel establishment
Crypto Officer	Run IPSec/IKEv2 Function	Initiate of IPSec/IKEv2 tunnel establishment	Status of IPSec/IKEv2 tunnel establishment

Table 8 – Roles, Services Commands, Input and Output

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and / or SSPs	Indicator
Self-Test	Initiate and run the pre-operational self-tests	HMAC-SHA2-256	Software Integrity Test Key (Not a SSP)	Crypto Officer	N/A	None
Zeroize	Zeroize all unprotected SSPs stored in the module	N/A	All	Crypto Officer	Z	None
Show Version	Provides the module's name/ID and versions	N/A	N/A	Crypto Officer	N/A	None
Show Status	Provides the module's current status and information	N/A	N/A	Crypto Officer	N/A	None
Configure Network	Perform the Module's Network Configuration	RSA Sigver	TLS RSA Public Key	Crypto Officer	G/R/W/E	Global indicator and Configuration logs
Configure SSHv2 Function	Create a secure SSHv2 channel	AES-CTR; CKG; CTR_DRBG; ECDSA KeyGen; ECDSA SigGen; ECDSA SigVer; HMAC-SHA-1; HMAC-SHA2-256; HMAC-SHA2-512;	DRBG Entropy Input (CSP); DRBG Seed (CSP); DRBG Internal State V Value (CSP); DRBG Key (CSP); SSH ECDHE Private Key (CSP);	Crypto Officer	G/R/W/E	Global indicator and SSH connection log message

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and / or SSPs	Indicator
		KAS-SSC (ECC); KAS (ECC); KDF SSH	SSH ECDHE Public Key (PSP); Peer SSH ECDHE Public Key (PSP); SSH ECDHE Shared Secret (CSP); SSH ECDSA Private Key (CSP); SSH ECDSA Public Key (PSP); SSH Session Encryption Key (CSP); SSH Session Authentication Key (CSP)			
Configure TLSv1.2 Function	Create a secure TLSv1.2 channel	AES-CBC; AES-GCM; CKG; CTR_DRBG; HMAC_DRBG; HMAC-SHA2-256; HMAC-SHA2-384; KAS-SSC (ECC); KAS (ECC); KTS; RSA KeyGen; RSA SigGen; RSA SigVer; KDF TLS	DRBG Entropy Input (CSP); DRBG Seed (CSP); DRBG Internal State V Value (CSP); DRBG Key (CSP); TLS RSA Private Key (CSP); TLS RSA Public Key (PSP); TLS ECDHE Private Key (CSP); TLS ECDHE Public Key (PSP); Peer TLS ECDHE Public Key (PSP); TLS ECDHE Shared Secret (CSP); TLS Pre-Master Secret (CSP); TLS Master Secret (CSP); TLS Session Encryption Key (CSP); TLS Session Authentication Key (CSP);	Crypto Officer	G/R/W/E	Global indicator and TLS success log message
Configure SNMPv3 Function	Create a secure SNMPv3 channel	AES-CBC; HMAC-SHA-1; KDF SNMP	SNMPv3 Authentication Secret (CSP); SNMPv3 Session Encryption Key (CSP); SNMPv3 Session Authentication Key (CSP);	Crypto Officer	G/R/W/E	Global indicator and SNMPv3 success log message
Configure IPsec/IKEv2 Function	Create IPSec/IKEv2 tunnel	AES-CBC; CKG; CTR_DRBG; HMAC-SHA-1; HMAC-SHA2-256; HMAC-SHA2-384; HMAC-SHA2-512; KAS-SSC (ECC); KAS (ECC); RSA KeyGen; RSA SigGen; RSA SigVer; KDF IKEv2	DRBG Entropy Input (CSP); DRBG Seed (CSP); DRBG Internal State V Value (CSP); DRBG Key (CSP); IPSec/IKE Pre-Shared Secret (CSP); IPSec/IKE RSA Private Key (CSP); IPSec/IKE RSA Public Key (PSP); IPSec/IKE ECDHE Private Key (CSP); IPSec/IKE ECDHE Public Key (PSP); IPSec/IKE ECDHE Shared Secret (CSP); IPSec/IKE Session Encryption Key (CSP); IPSec/IKE Session Authentication Key (CSP);	Crypto Officer	G/R/W/E	Global indicator and IPSec success log message
Run SSHv2 Function	Negotiation and encrypted data transport via SSH	AES-CTR; CKG; CTR_DRBG; ECDSA KeyGen; ECDSA SigGen;	DRBG Entropy Input (CSP); DRBG Seed (CSP); DRBG Internal State V Value (CSP); DRBG Key (CSP);	Crypto Officer	G/R/W/E	Global indicator and SSH connection log message

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and / or SSPs	Indicator
		ECDSA SigVer; HMAC-SHA-1; HMAC-SHA2-256; HMAC-SHA2-512; KAS-SSC (ECC); KAS (ECC); KDF SSH	SSH ECDHE Private Key (CSP); SSH ECDHE Public Key (PSP); Peer SSH ECDHE Public Key (PSP); SSH ECDHE Shared Secret (CSP); SSH ECDSA Private Key (CSP); SSH ECDSA Public Key (PSP); SSH Session Encryption Key (CSP); SSH Session Authentication Key (CSP);			
Run TLSv1.2 Function	Negotiation and encrypted data transport via TLS	AES-CBC; AES-GCM; CKG; CTR_DRBG; HMAC_DRBG; HMAC-SHA2-256; HMAC-SHA2-384; KAS-SSC (ECC); KAS (ECC); KTS; RSA KeyGen; RSA SigGen; RSA SigVer; KDF TLS	DRBG Entropy Input (CSP); DRBG Seed (CSP); DRBG Internal State V Value (CSP); DRBG Key (CSP); TLS RSA Private Key (CSP); TLS RSA Public Key (PSP); TLS ECDHE Private Key (CSP); TLS ECDHE Public Key (PSP); Peer TLS ECDHE Public Key (PSP); TLS ECDHE Shared Secret (CSP); TLS Pre-Master Secret (CSP); TLS Master Secret (CSP); TLS Session Encryption Key (CSP); TLS Session Authentication Key (CSP);	Crypto Officer	G/R/W/E	Global indicator and TLS success log message
Run SNMPv3 Function	Negotiation and encrypted data transport via SNMPv3	AES-CBC; HMAC-SHA-1; KDF SNMP	SNMPv3 Authentication Secret (CSP); SNMPv3 Session Encryption Key (CSP); SNMPv3 Session Authentication Key (CSP);	Crypto Officer	G/R/W/E	Global indicator and SNMPv3 success log message
Run IPSec/IKEv2 Function	Negotiation and encrypted data transport via IPSec	AES-CBC; CKG; CTR_DRBG; HMAC-SHA-1; HMAC-SHA2-256; HMAC-SHA2-384; HMAC-SHA2-512; KAS-SSC (ECC); KAS (ECC); RSA KeyGen; RSA SigGen; RSA SigVer; KDF IKEv2	DRBG Entropy Input (CSP); DRBG Seed (CSP); DRBG Internal State V Value (CSP); DRBG Key (CSP); IPSec/IKE Pre-Shared Secret (CSP); IPSec/IKE RSA Private Key (CSP); IPSec/IKE RSA Public Key (PSP); IPSec/IKE ECDHE Private Key (CSP); IPSec/IKE ECDHE Public Key (PSP); IPSec/IKE ECDHE Shared Secret (CSP); IPSec/IKE Session Encryption Key (CSP); IPSec/IKE Session Authentication Key (CSP);	Crypto Officer	G/R/W/E	Global indicator and IPSec/IKEv2 success log message

Table 9 – Approved Services

G = Generate: The module generates or derives the SSP.

R = Read: The SSP is read from the module (e.g. the SSP is output).

W = Write: The SSP is updated, imported, or written to the module.

E = Execute: The module uses the SSP in performing a cryptographic operation.

Z = Zeroise: The module zeroizes the SSP.

Unauthenticated Services

Unauthenticated Users can run the self-test service by power-cycling the tested platform.

5. Software/Firmware Security

Integrity Techniques

The module performs the Software Integrity test by using HMAC-SHA2-256 (HMAC Cert. #A3566) during the Pre-Operational Self-Test. A Software 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. At Module's initialization, the integrity of the runtime executable is verified using an HMAC-SHA2-256 digest which is compared to a value computed at build time. If at the load time the MAC does not match the stored, known MAC value, the module would enter an Error state with all crypto functionality inhibited.

Integrity Test 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 module to initiate the software integrity test on-demand. This automatically performs the integrity test of all firmware components included within the boundary of the module.

6. Operational Environment

The module is a modifiable operational environment as per FIPS 140-3 Level 1 specifications. The operating system is restricted to a single operator mode of operation. The application that makes calls to the module is the single user of the module even when the application is serving multiple clients.

See Table 2 for details regarding what platforms the module was tested on.

7. Physical Security

As the module is a software only module, the physical security requirements are not applicable.

8. Non-Invasive Security

No approved non-invasive attack mitigation test metrics are defined at this time.

9. Sensitive Security Parameters

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import/Export	Establish-ment	Storage	Zeroization	Use & Related Keys
DRBG Entropy Input (CSP)	At least 256 bits	N/A	Obtained from the Entropy Source within TOEPP (GPS INT Pathways)	Import to the module via Module's API	N/A	DRAM (plaintext)	Zeroized when the tested platform is powered down	Used to seed the DRBG

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import/Export	Establish-ment	Storage	Zeroization	Use & Related Keys
				Export: No		Note: The module does not provide persistent keys/ SSPs storage		
DRBG Seed (CSP)	256 bits	CTR_DRBG Cert. #A3566; HMAC_DRBG Cert. #A3572	Internally Derived from entropy input string as defined by SP 800-90Arev1 DRBG	Import: No Export: No	N/A	DRAM (plaintext) Note: The module does not provide persistent keys/ SSPs storage	Zeroized when the tested platform is powered down	Random number generation
DRBG Internal State V value (CSP)	256 bits	CTR_DRBG Cert. #A3566; HMAC_DRBG Cert. #A3572	Internally Derived from entropy input string as defined by SP 800-90Arev1 DRBG	Import: No Export: No	N/A	DRAM (plaintext) Note: The module does not provide persistent keys/ SSPs storage	Zeroized when the tested platform is powered down	Random number generation
DRBG Key (CSP)	256 bits	CTR_DRBG Cert. #A3566; HMAC_DRBG Cert. #A3572	Internally Derived from entropy input string as defined by SP 800-90Arev1 DRBG	Import: No Export: No	N/A	DRAM (plaintext) Note: The module does not provide persistent keys/ SSPs storage	Zeroized when the tested platform is powered down	Random number generation
TLS RSA Private Key (CSP)	112-128 bits (Modulus: 2048, 3072 bits)	CKG; DRBG; RSA KeyGen; RSA SigGen; Certs. #A3566 and #A3572	Internally generated conformant to SP800-133r2 (CKG) using FIPS 186-4 RSA key generation method, and the random value used in key generation is generated using SP 800-90Arev1 DRBG	Import: No Export: No	N/A	HDD (plaintext) Note: The module does not provide persistent keys/ SSPs storage	Zeroized by SSP/CSP/PSP Zeroization Command	Used for TLS peer authentication
TLS RSA Public Key (PSP)	112-128 bits (Modulus: 2048, 3072 bits)	RSA KeyGen; RSA SigVer; Certs. #A3566 and #A3572	Internally derived per the FIPS 186-4 RSA key generation method	Import: No Export: Yes, to the TLS peer	N/A	HDD (plaintext) Note: The module does not provide persistent keys/ SSPs storage	Zeroized by SSP/CSP/PSP Zeroization Command	Used for TLS peer authentication
TLS ECDHE Private Key (CSP)	128 – 256 bits (Curves: P-256, P-384, P-521)	CKG; DRBG; KAS-ECC-SSC; Certs. #A3566 and #A3572	Internally generated conformant to SP800-133r2 (CKG) using SP 800-56Arev3 EC Diffie-Hellman key generation method, and the random value used in key generation is generated using SP 800-90Arev1 DRBG	Import: No Export: No	N/A	DRAM (plaintext) Note: The module does not provide persistent keys/ SSPs storage	Zeroized when the tested platform is powered down	Used to derive TLS ECDHE Shared Secret
TLS ECDHE Public Key (PSP)	128 – 256 bits (Curves: P-256, P-384, P-521)	KAS-ECC-SSC; Certs. #A3566 and #A3572	Internally derived internally per the EC Diffie-Hellman key agreement (SP800-56Arev3)	Import: No Export: Yes, to the TLS peer	N/A	DRAM (plaintext) Note: The module does not provide persistent keys/ SSPs storage	Zeroized when the tested platform is powered down	Used to derive TLS ECDHE Shared Secret
Peer TLS ECDHE Public Key (PSP)	Curves: P-256, P-384, P-521	N/A	N/A	Import: Enter into the Module via Module's API Export: No	N/A	DRAM (plaintext) Note: The module does not provide persistent keys/ SSPs storage	Zeroized when the tested platform is powered down	Used to derive TLS ECDHE Shared Secret
TLS ECDHE Shared Secret (CSP)	128 – 256 bits (Curves: P-256, P-384, P-521)	KAS-ECC-SSC; KAS (ECC); Certs. #A3566 and #A3572	Internally derived using SP800-56A rev3 EC Diffie-Hellman shared secret computation	Import: No Export: No	N/A	DRAM (plaintext) Note: The module does not provide persistent keys/ SSPs storage	Zeroized when the tested platform is powered down	Used to derive TLS Session Encryption Keys, TLS Session Authentication Keys
TLS Pre-Master Secret (CSP)	384 bits	N/A	Internally derived via key derivation function defined in SP800-135rev1 KDF (TLSv1.2)	Import: No Export: No	N/A	DRAM (plaintext) Note: The module does not provide persistent keys/ SSPs storage	Zeroized when the tested platform is powered down	Used to derive TLS Master Secret
TLS Master Secret (CSP)	384 bits	N/A	Internally derived via key derivation function defined in SP800-135rev1 KDF (TLSv1.2)	Import: No Export: No	N/A	DRAM (plaintext) Note: The module does not provide persistent keys/ SSPs storage	Zeroized when the tested platform is powered down	Used to derive TLS Encryption Keys, TLS Authentication Keys.
TLS Session Encryption Key (CSP)	128 or 256 bits	AES-CBC; AES-GCM; KDF TLS KTS; Certs. #A3566 and #A3572	Internally derived via key derivation function defined in SP 800-135rev1 KDF (TLSv1.2)	Import: No Export: No	N/A	DRAM (plaintext) Note: The module does not provide persistent keys/ SSPs storage	Zeroized when the tested platform is powered down	Used to secure TLS session confidentiality

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import/Export	Establish-ment	Storage	Zeroization	Use & Related Keys
TLS Session Authentication Key (CSP)	At least 112 bits	HMAC-SHA2-256; HMAC-SHA2-384; KDF TLS KTS; Certs. #A3566 and #A3572	Internally derived via key derivation function defined in SP800-135 rev1 KDF TLSv1.2	Import: No Export: No	N/A	DRAM (plaintext) Note: The module does not provide persistent keys/ SSPs storage	Zeroized when the tested platform is powered down	Used to secure the TLS session integrity
IPSec/IKE Pre-Shared Secret (CSP)	2048 bits characters	N/A	N/A	Import: Encrypted by using TLS/SSH session key Export: No	MD/EE	HDD (plaintext) Note: The module does not provide persistent keys/ SSPs storage	Zeroized by SSP/CSP/PSP Zeroization Command	Used for IPSec/IKE peer authentication
IPSec/IKE RSA Private Key (CSP)	112 or 128 bits (Modulus: 2048 or 3072 bits)	CKG; DRBG; RSA SigGen; Cert# A3566	Internally generated conformant to SP800-133r2 (CKG) using FIPS 186-4 RSA key generation method, and the random value used in key generation is generated using SP800-90Arev1 DRBG	Import: No Export: No	N/A	HDD (plaintext) Note: The module does not provide persistent keys/ SSPs storage	Zeroized by SSP/CSP/PSP Zeroization Command	Used for IPSec/IKE peer authentication
IPSec/IKE RSA Public Key (PSP)	112 or 128 bits (Modulus: 2048 or 3072 bits)	RSA SigVer; Cert. #A3566	Internally derived per the FIPS 186-4 RSA key generation method	Import: No Export: to the IKE Peer application	N/A	HDD (plaintext) Note: The module does not provide persistent keys/ SSPs storage	Zeroized by SSP/CSP/PSP Zeroization Command	Used for IPSec/IKE peer authentication
IPSec/IKE ECDHE Private Key (CSP)	128 or 192 bits (Curves: P-256 or P-384)	CKG; DRBG; KAS-ECC-SSC; KAS (ECC); Cert. #A3566	Internally generated conformant to SP800-133r2 (CKG) using SP800-56Arev3 EC Diffie-Hellman key generation method, and the random value used in key generation is generated using SP800-90Arev1 DRBG	Import: No Export: No	N/A	DRAM (plaintext) Note: The module does not provide persistent keys/ SSPs storage	Zeroized when the tested platform is powered down	Used to derive IPSec/IKE ECDHE Shared Secret
IPSec/IKE ECDHE Public Key (PSP)	128 or 192 bits (Curves: P-256 or P-384)	KAS-ECC-SSC; KAS (ECC); Cert. #A3566	Internally derived internally per the EC Diffie-Hellman key agreement (SP800-56Arev3)	Import: No Export: to the IKE Peer application	N/A	DRAM (plaintext) Note: The module does not provide persistent keys/ SSPs storage	Zeroized when the tested platform is powered down	Used to derive IPSec/IKE ECDHE Shared Secret
IPSec/IKE ECDHE Shared Secret (CSP)	128 or 192 bits (Curves: P-256 or P-384)	KAS-ECC-SSC; KAS (ECC); Cert. #A3566	Internally derived using SP800-56A rev3 EC Diffie-Hellman shared secret computation	Import: No Export: No	N/A	DRAM (plaintext) Note: The module does not provide persistent keys/ SSPs storage	Zeroized when the tested platform is powered down	Used to derive IPSec/IKE Session Encryption Keys, IPSec/IKE Authentication Keys
IPSec/IKE Session Encryption Key (CSP)	128-256 bits	AES-CBC; KDF IKEv2; Cert. #A3566	Internally derived via key derivation function defined in SP800-135rev1 KDF (IKEv2)	Import: No Export: No	N/A	DRAM (plaintext) Note: The module does not provide persistent keys/ SSPs storage	Zeroized when the tested platform is powered down	Used to secure IPSec/IKEv2 session confidentiality
IPSec/IKE Session Authentication Key (CSP)	At least 112 bits	HMAC-SHA-1; HMAC-SHA2-256; HMAC-SHA2-384; HMAC-SHA2-512; KDF IKEv2; Cert. #A3566	Internally derived via key derivation function defined in SP800-135rev1 KDF (IKEv2)	Import: No Export: No	N/A	DRAM (plaintext) Note: The module does not provide persistent keys/ SSPs storage	Zeroized when the tested platform is powered down	Used to secure IPSec/IKEv2 session integrity
SNMPv3 Authentication Secret (CSP)	8 characters minimum	N/A	N/A	Import: Encrypted by using TLS/SSH session key Export: No	MD/EE	HDD (plaintext) Note: The module does not provide persistent keys/ SSPs storage	Zeroized by SSP/CSP/PSP Zeroization Command	Used for SNMPv3 User authentication
SNMPv3 Session Encryption Key (CSP)	128 bits	AES-CFB; KDF SNMP; Cert. #A3566	Internally derived via key derivation function defined in SP800-135rev1 KDF (SNMPv3)	Import: No Export: No	N/A	DRAM (plaintext) Note: The module does not provide persistent keys/ SSPs storage	Zeroized when the tested platform is powered down	Used to secure SNMPv3 session confidentiality
SNMPv3 Session Authentication Key (CSP)	At least 112 bits	HMAC-SHA-1; KDF SNMP; Cert. #A3566	Internally derived via key derivation function defined in SP800-135rev1 KDF (SNMPv3)	Import: No Export: No	N/A	DRAM (plaintext) Note: The module does not provide persistent keys/ SSPs storage	Zeroized when the tested platform is powered down	Used to secure SNMPv3 session integrity
SSH ECDHE Private Key (CSP)	128-256 bits	CKG; DRBG; KAS-ECC-SSC; KAS (ECC);	Internally generated conformant to SP800-133r2 (CKG) using SP800-56Arev3 EC	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized when the tested platform is powered down	Used to derive the SSH ECDHE Shared Secret

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import/Export	Establish-ment	Storage	Zeroization	Use & Related Keys
	(Curves: P-256, P-384, or P-521)	Cert. #A3566	Diffie-Hellman key generation method, and the random value used in key generation is generated using SP800-90Arev1 DRBG			Note: The module does not provide persistent keys/ SSPs storage		
SSH ECDHE Public Key (PSP)	128-256 bits (Curves: P-256, P-384, or P-521)	KAS-ECC-SSC; KAS (ECC); Cert. #A3566	Internally derived internally per the EC Diffie-Hellman key agreement (SP800-56Arev3)	Import: No Export: Yes, to the SSH peer	N/A	DRAM (plaintext) Note: The module does not provide persistent keys/ SSPs storage	Zeroized when the tested platform is powered down	Used to derive the SSH ECDHE Shared Secret
Peer SSH ECDHE Public Key (PSP)	128-256 bits (Curves: P-256, P-384, or P-521)	KAS-ECC-SSC; KAS (ECC); Cert.#A3566	N/A	Import: Enter into the Module via the Module's API Export: No	N/A	DRAM (plaintext) Note: The module does not provide persistent keys/ SSPs storage	Zeroized when the tested platform is powered down	Used to derive SSH ECDHE Shared Secret
SSH ECDHE Shared Secret (CSP)	128-256 bits (Curves: P-256, P-384, or P-521)	CKG; DRBG; KAS-ECC-SSC; Cert. #A3566	Internally derived using SP800-56A rev3 EC Diffie-Hellman shared secret computation	Import: No Export: No	N/A	DRAM (plaintext) Note: The module does not provide persistent keys/ SSPs storage	Zeroized when the tested platform is powered down	Used to derive SSH Session Encryption Keys, SSH Session Authentication Keys
SSH ECDSA Private Key (CSP)	128-256 bits (Curves: P-256, P-384, or P-521)	CKG; DRBG; ECDSA KeyGen; ECDSA SigGen; Cert. #A3566	Internally generated conformant to SP800-133r2 (CKG) using FIPS 186-4 ECDSA Key Generation method, and the random value used in key generation is generated using SP800-90Arev1 DRBG	Import: No Export: No	N/A	HDD (plaintext) Note: The module does not provide persistent keys/ SSPs storage	Zeroized by SSP (CSP/PSP) Zeroization Command	Used for SSH session authentication
SSH ECDSA Public Key (PSP)	128-256 bits (Curves: P-256, P-384, or P-521)	ECDSA KeyGen; ECDSA SigVer; Cert. #A3566	Internally derived per the FIPS 186-4 ECDSA Keypair generation method	Import: No Export: Yes, to the SSH peer	N/A	HDD (plaintext) Note: The module does not provide persistent keys/ SSPs storage	Zeroized by SSP/CSP/PSP Zeroization Command	Used for SSH session authentication
SSH Session Encryption Key (CSP)	128 - 256 bits	AES-CTR; KDF SSH; KTS; Cert. #A3566	Internally derived via key derivation function defined in SP 800-135rev1 KDF (SSHv2)	Import: No Export: No	N/A	DRAM (plaintext) Note: The module does not provide persistent keys/ SSPs storage	Zeroized when the tested platform is powered down	Used for SSH session confidentiality protection
SSH Session Authentication Key (CSP)	At least 112 bits	KDF SSH; KTS; HMAC-SHA-1; HMAC-SHA2-256; HMAC-SHA2-512; Cert. #A3566	Internally derived via key derivation function defined in SP 800-135rev1 KDF (SSHv2)	Import: No Export: No	N/A	DRAM (plaintext) Note: The module does not provide persistent keys/ SSPs storage	Zeroized when the tested platform is powered down	Used for SSH session integrity protection

Table 10– SSPs

Entropy Source(s)	Minimum Number of Bits of Entropy	Details
Palo Alto Networks DRNG Entropy Source	0.6 bits entropy per sample with sample bit: 1 bit	Please refer to ESV Cert. #E68
Palo Alto Networks DRNG Entropy Source	0.6 bits entropy per sample with sample bit: 1 bit	Please refer to ESV Cert. #E71

Table 11 - Non-Deterministic Random Number Generation Specification

10. Self-Tests

The modules perform the following self-tests, including the pre-operational self-tests and Conditional self-tests.

Pre-Operational Self-Tests

Algorithm	Self-Test Details
SHS	KAT using SHA2-256
HMAC	KAT using HMAC- SHA2-256
Software integrity	Using HMAC-SHA2-256

Table 12 - Pre-Operational Self-Tests

The modules also perform the following Cryptographic Algorithm Self-Tests (CASTs), which can be initiated by rebooting the module. All self-tests run without operator intervention.

Conditional Self-Tests

Cryptographic Algorithm Self-Tests (CASTs)

Algorithm	Self-Test Details
AES	AES-ECB 256 bits Encryption KAT
AES	AES-ECB 256 bits Decryption KAT
AES	AES-CBC 256 bits Encryption KAT
AES	AES-CBC 256 bits Decryption KAT
AES	AES-GCM 256 bits Encryption KAT
AES	AES-GCM 256 bits Decryption KAT
DRBG	CTR_DRBG KAT: Instantiate KAT: Generate KAT: Reseed Note: DRBG Health Tests as specified in SP800-90Arev1 DRBG Section 11.3 are performed)
ECDSA	KAT using P-224 with SHA2-256 (ECDSA Signature Generation)
ECDSA	KAT using P-224 with SHA2-256 (ECDSA Signature Verification)
HMAC	KAT using HMAC-SHA-1
HMAC	KAT using HMAC-SHA2-224
HMAC	KAT using HMAC-SHA2-256
HMAC	KAT using HMAC-SHA2-384
HMAC	KAT using HMAC-SHA2-512
KAS-ECC-SSC	KAT for KAS-ECC-SSC (Shared Secret Computation) primitive Z value
KDF IKEv2	KAT for KDF IKEv2
KDF SSH	KAT for KDF SSH
KDF SNMP	KAT for KDF SNMP
KDF TLS	KAT for KDF TLSv
RSA	KAT using 2048 bits modulus with SHA2-256 (RSA Signature Generation)
RSA	KAT using 2048 bits modulus with SHA2-256 (RSA Signature Verification)
SHS	KAT using SHA-1

Table 13 – CASTs (Crypto Library I)

Algorithm	Self-Test Details
AES	AES-CBC 256 bits Encryption KAT
AES	AES-CBC 256 bits Decryption KAT
AES	AES-GCM 256 bits Encryption KAT

AES	AES-GCM 256 bits Encryption KAT
ECDSA	KAT using P-224 with SHA2-256 (ECDSA Signature Generation)
ECDSA	KAT using P-224 with SHA2-256 (ECDSA Signature Verification)
DRBG	HMAC_DRBG (SHA2-512) KAT: Instantiate KAT: Generate KAT: Reseed Note: DRBG Health Tests as specified in SP800-90Arev1 DRBG Section 11.3 are performed)
HMAC	KAT using SHA2-256
HMAC	KAT using SHA2-384
HMAC	KAT using SHA2-512
KAS-ECC-SSC	KAT for KAS-ECC-SSC (Shared Secret Computation) primitive Z value
KDF TLS	KAT for KDF TLS
RSA	KAT using 2048 bits modulus with SHA2-256 (RSA Signature Generation)
RSA	KAT using 2048 bits modulus with SHA2-256 (RSA Signature Verification)

Table 14 – CASTs (Crypto Library II)

Algorithm	Self-Test Details
SP 800-90B Health Tests	The module's entropy source implements Start-up and Continuous health tests defined in SP800-90B, section 4.2. The entropy source utilizes Developer-Defined Alternatives to the Continuous Health Tests which is defined in SP 800-90B section 4.5.

Table 15 - Entropy Source Health Tests

Conditional Pair-Wise Consistency Tests

Algorithm	Self-Test Details
RSA	RSA Pairwise consistency test (PCT)
ECDSA	ECDSA PCT
KAS-ECC-SSC	SP800-56Ar3 KAS-ECC-SSC PCT

Table 16 - Conditional Pair-Wise Consistency Tests (Crypto Library I)

Algorithm	Self-Test Details
RSA	RSA Pairwise consistency test (PCT)
ECDSA	ECDSA PCT
SP800-56Ar3 KAS-ECC-SSC	SP800-56Ar3 KAS-ECC-SSC PCT

Table 17 - Conditional Pair-Wise Consistency Tests (Crypto Library II)

Periodic/On-Demand Self-Test

The module performs on-demand self-tests initiated by the operator, by power cycling or rebooting the tested platform. The full suite of self-tests is then executed. The same procedure may be employed by the operator to perform periodic self-tests.

It is recommended that the Crypto Officer perform periodic testing of the module's on-demand self-tests every 60 days to ensure all components are functioning correctly.

Error Handling

If any of the above-mentioned self-tests fail, the module reports the cause of the error and enters an error state (there is only one 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 software 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. The table 18 below shows the different causes that lead to the Error State and the status indicators reported.

Cause of Error	Error State Indicator
Failed Pre-Operational Software Integrity Test	Integrity check failed at <location>
Failed Conditional CAST	<Crypto Library>: FIPS Self-test failed for <algorithm> Entering error state
Failed Conditional PCT	Key verification failed
SP 800-90B Entropy Source Start-up/Continuous health tests	No random numbers are generated and key generation is halted

Table 18 - Error State Indicators

11. Life-Cycle Assurance

The sections below highlight the details for each stage.

Secure Delivery Procedures

The module is built into ION 6.1. There is no standalone delivery of the module as a software library. The vendor's internal development process guarantees that the correct version of the module goes with the intended OS.

Secure Operation

The module meets all the Level 1 requirements for FIPS 140-3. Follow the secure operations provided below to place the module in the Approved mode.

The software version is 1.0. The module is initiated into the Approved mode of operation via the following procedure. Note that a Palo Alto ION device running ION 6.1 is needed to access the APIs of the module.

1. Prepare ION device for use and power-on
2. Using the Controller, navigate to the device that is to be initiated
3. Select "FIPS"
    a. Click "proceed" to begin initialization procedure
4. The module will begin initialization that includes the following:
    a. Zeroization of any sensitive information or data
    b. Power cycle of the device followed by running all self-tests
5. Once initialization is complete, the module provides the following status output:
    a. Device Mode: "fips"
    b. Self-tests: "Power-up self test successful"

Once the module has completed initialization into the Approved mode of operation, any non-Approved configurations/algorithms are rejected automatically by the module and an error message is output.

End of Life / Sanitization

End of life dates for the module are announced publicly via Palo Alto Networks' services website. Crypto Officers should follow the procedure below for the secure destruction of their module:

Note: This process will cause the module to no longer function after it has wiped all configurations and keys.

1. Access the module as Crypto Officer
2. Execute command: “disable system”
    a. Confirm command
3. Module will begin zeroization process and wipe all security parameters and configurations

12. Mitigation of Other Attacks

This module is not designed to mitigate against any other attacks outside of the FIPS 140-3 scope.