Palo Alto Networks

SD-WAN Instant-On Network (ION) Devices ION 1200, ION 1200-S, ION 3200, ION 5200, and ION 9200

Firmware Version: 6.1.2

FIPS 140-3 Non-Proprietary Security Policy

Documentation Version: 1.3

Last Update: June 17, 2024

Palo Alto Networks, Inc.
www.paloaltonetworks.com

Revision Date: June 17, 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 Instant-On Network (ION) Devices ION 1200, ION 1200-S, ION 3200, ION 5200, and ION 9200 (hereinafter referred to as the Module or ION module).

The Palo Alto Networks SD-WAN Instant-On Network (ION) Devices 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. Built with the intent to reduce remote infrastructure, Palo Alto Networks SD-WAN ION devices enable the cloud-delivered branch.

ISO/IEC 24759 Section 6. [Number Below]	FIPS 140-3 Section Title	Security Level
1	General	2
2	Cryptographic Module Specification	2
3	Cryptographic Module Interfaces	2
4	Roles, Services, and Authentication	2
5	Software/Firmware Security	2
6	Operational Environment	N/A
7	Physical Security	2
8	Non-invasive Security	N/A
9	Sensitive Security Parameter Management	2
10	Self-tests	2
11	Life-Cycle Assurance	2
12	Mitigation of Other Attacks	N/A

Table 1 - Security Levels

The module is designed to meet an overall security level 2.

2. Cryptographic Module Specification

The module is a hardware multiple-chip standalone cryptographic module. FIPS 140-3 conformance testing was performed at Security Level 2 with the configurations noted in the table 2 below.

Model	Hardware [Part Number and Version]	Firmware Version	Distinguishing Features
ION 1200	ION 1200	6.1.2	See Cryptographic Module Interfaces section
ION 1200	ION 1200-C-NA	6.1.2	
ION 1200	ION 1200-C-ROW	6.1.2	
ION 1200	ION 1200-C-5G-WW	6.1.2	
ION 1200-S	ION 1200-S	6.1.2	
ION 1200-S	ION 1200-S-C-NA	6.1.2	
ION 1200-S	ION 1200-S-C-ROW	6.1.2	
ION 1200-S	ION 1200-S-C-5G-WW	6.1.2	
ION 3200	ION 3200	6.1.2	
ION 5200	ION 5200	6.1.2	
ION 9200	ION 9200	6.1.2	

Table 2 - Tested Operational Environments

Cryptographic Boundary

The module's cryptographic boundary 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.

Figure 1 - ION 1200

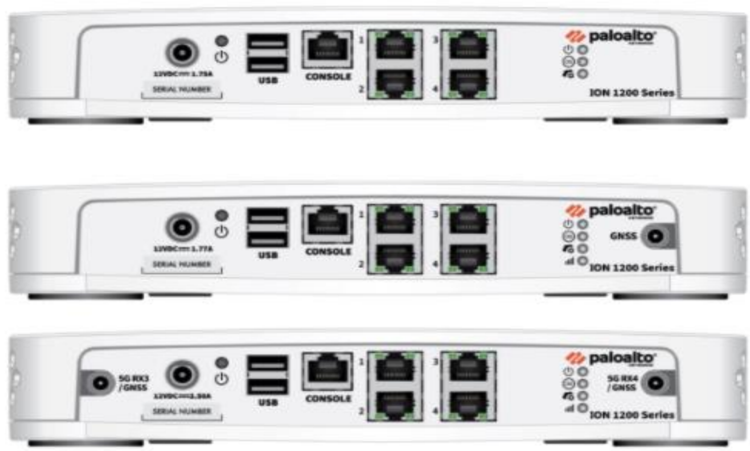

Figure 2 - ION 1200 (Top), ION 1200-C-NA/ION 1200-C-ROW (Middle), and ION 1200-C-5G-WW (Bottom) front interfaces

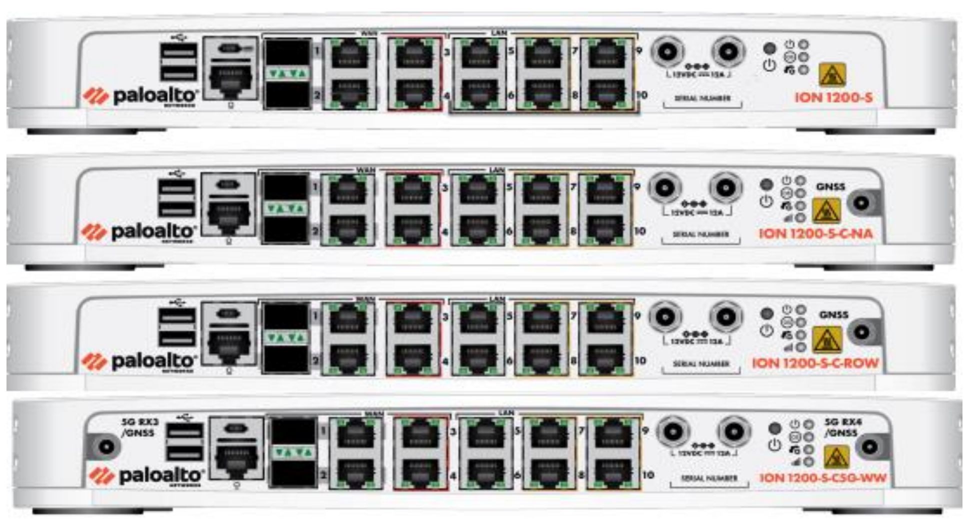

Figure 3 - ION 1200-S (Top), ION 1200-S-C-NA/ION 1200-S-C-ROW (Middle), and ION 1200-S-C-5G-WW (Bottom) front interfaces

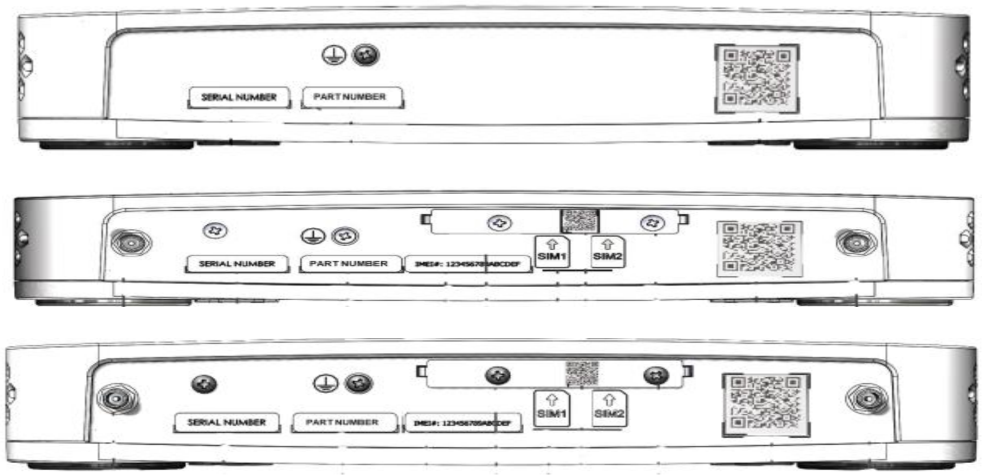

Figure 4 - ION 1200 (Top), ION 1200-C-NA/ION 1200-C-ROW (Middle), and ION 1200-C-5G-WW (Bottom) Rear Interfaces

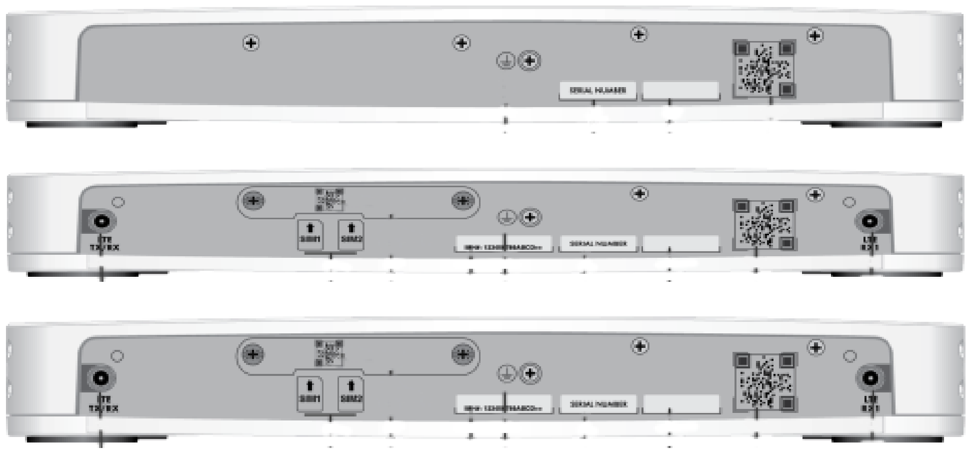

Figure 5 - ION 1200-S (Top), ION 1200-S-C-NA/ION 1200-S-C-ROW (Middle), and ION 1200-S-C-5G-WW (Bottom) Rear Interfaces

Figure 6 - ION 3200 Front Interfaces

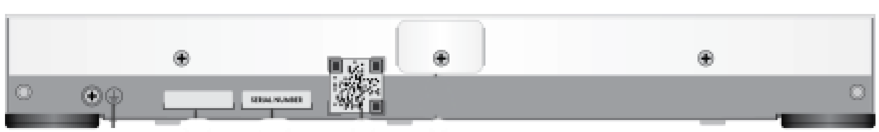

Figure 7 - ION 3200 Rear Interfaces

Figure 8 - ION 5200 Front Interfaces

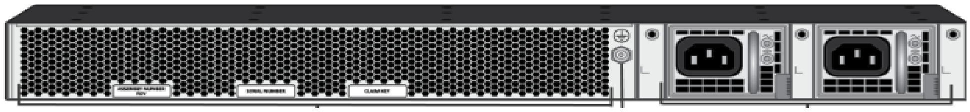

Figure 9 - ION 5200 Rear Interfaces

Figure 10 - ION 9200 Front Interfaces

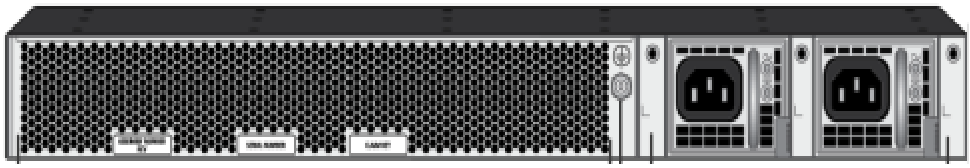

Figure 11 - ION 9200 Rear Interfaces

Modes of Operation

The module has one approved mode of operation and is always in the 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 3-6 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
A3563	AES: ● FIPS 197 ● SP 800-38D	ECB	128, 192, and 256 bits	Data Encryption/Decryption
A3563	AES: ● FIPS 197 ● SP 800-38A	CBC	128, 192, and 256 bits	Data Encryption/Decryption
A3563	AES: ● FIPS 197 ● SP 800-38A	CTR	128, 192, and 256 bits	Data Encryption/Decryption
A3563	AES: ● FIPS 197 ● SP 800-38D	GCM	128, 192, and 256 bits	Data Encryption/Decryption
A3563	KDF SSH: ● SP 800-135rev1 (CVL)	KDF SSHv2	N/A	SP800-135rev1 compliant Key Derivation
A3563	KDF TLS: ● SP 800-135rev1 (CVL)	KDF TLSv1.2	N/A	SP800-135rev1 compliant Key Derivation
A3563	KDF IKEv2:	KDF IKEv2	N/A	SP800-135rev1 compliant Key Derivation

CAVP Cert	Algorithm and Standard	Mode/Method	Description/Key Size(s) / Key Strength(s)	Use / Function
	• SP 800-135rev1 (CVL)			
A3563	KDF SNMP: • SP 800-135rev1 (CVL)	KDF SNMPv3	N/A	SP800-135rev1 compliant Key Derivation
A3563	DRBG: • SP 800-90Arev1	CTR_DRBG (AES-256 bits) Derivation Function Enabled: Yes	N/A	Deterministic Random Bit Generation
A3563	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
A3563	KAS (ECC) • 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
A3563	ECDSA • FIPS 186-4	ECDSA KeyGen	Curves: P-224, P-256, P-384, P-521	ECDSA Key Generation
A3563	ECDSA • FIPS 186-4	ECDSA SigGen	Curves: P-224, P-256, P-384, P-521	ECDSA Digital Signature Generation
A3563	ECDSA • FIPS 186-4	ECDSA SigVer	Curves: P-224, P-256, P-384, P-521	ECDSA Digital Signature Verification
A3563	HMAC • FIPS 198-1	HMAC-SHA-1	At least 160 bits	Message Authentication
A3563	HMAC • FIPS 198-1	HMAC-SHA2-224	At least 160 bits	Message Authentication
A3563	HMAC • FIPS 198-1	HMAC-SHA2-256	At least 160 bits	Message Authentication
A3563	HMAC • FIPS 198-1	HMAC-SHA2-384	At least 160 bits	Message Authentication
A3563	HMAC • FIPS 198-1	HMAC-SHA2-512	At least 160 bits	Message Authentication
A3563	KTS • SP800-38F	KTS (AES Cert. #A3563)	128, 192, and 256 bits	Key Transport using AES-GCM; Key establishment methodology provides between 128 and 256 bits of encryption strength
A3563	KTS • SP800-38F	KTS (AES Cert. #A3563 and HMAC Cert. #A3563)	128, 192, and 256 bits	Key Transport using AES and HMAC; Key establishment methodology provides

CAVP Cert	Algorithm and Standard	Mode/Method	Description/Key Size(s) / Key Strength(s)	Use / Function
				between 128 and 256 bits of encryption strength
A3563	RSA • FIPS 186-4	RSA KeyGen (PKCS#1 v1.5)	Modulus: 2048 and 3072 bits	RSA Key Generation
A3563	RSA • FIPS 186-4	RSA SigGen (PKCS#1 v1.5)	Modulus: 2048 and 3072 bits	RSA Digital Signature Generation
A3563	RSA • FIPS 186-4	RSA SigVer (PKCS#1 v1.5)	Modulus: 2048 and 3072 bits	RSA Digital Signature Verification
A3563	SHS • FIPS 180-4	SHA-1	N/A	Hashing Note: SHA-1 is not used for digital signature generation
A3563	SHS • FIPS 180-4	SHA2-256	N/A	Hashing
A3563	SHS • FIPS 180-4	SHA2-384	N/A	Hashing
A3563	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 CTR_DRBG (DRBG Cert. #A3563).

Table 3 - Approved Algorithms (Crypto Library - I)

CAVP Cert	**Algorithm and Standard**	**Mode/Method**	**Description/Key Size(s) / Key Strength(s)**	**Use / Function**
A3564	AES: • FIPS 197 • SP 800-38A	CBC	128 or 256 bits	Data Encryption/Decryption
A3564	AES: • FIPS 197 • SP 800-38D	GCM	128 or 256 bits	Data Encryption/Decryption
A3564	KDF TLS: • SP 800-135rev1 (CVL)	TLS 1.2 KDF	N/A	SP800-135rev1 compliant Key Derivation
A3564	DRBG: • SP 800-90Arev1	DRBG with HMAC-SHA2-512	N/A	Deterministic Random Bit Generation
A3564	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

CAVP Cert	Algorithm and Standard	Mode/Method	Description/Key Size(s) / Key Strength(s)	Use / Function
A3564	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
A3564	ECDSA ● FIPS 186-4	ECDSA KeyGen	Curves: P-224, P-256, P-384, P-521	ECDSA Key Generation
A3564	ECDSA ● FIPS 186-4	ECDSA KeyVer	Curves: P-224, P-256, P-384, P-521	ECDSA Key Verification
A3564	HMAC ● FIPS 198-1	HMAC-SHA2-256	At least 160 bits	Message Authentication
A3564	HMAC ● FIPS 198-1	HMAC-SHA2-384	At least 160 bits	Message Authentication
A3564	HMAC ● FIPS 198-1	HMAC-SHA2-512	At least 160 bits	Message Authentication
A3564	KTS ● SP800-38F	KTS (AES Cert. #A2386)	128 or 256 bits	Key Transport using AES-GCM; Key establishment methodology provides 128 or 256 bits of encryption strength
A3564	KTS ● SP800-38F	KTS (AES Cert. #A2386 and HMAC Cert. #A2386)	128 or 256 bits	Key Transport using AES and HMAC; Key establishment methodology provides 128 or 256 bits of encryption strength
A3564	RSA ● FIPS 186-4	RSA SigVer (PKCS#1 v1.5)	Modulus: 2048 bits	Digital Signature Verification
A3564	SHS ● FIPS 180-4	SHA2-256	N/A	Hashing
A3564	SHS ● FIPS 180-4	SHA2-384	N/A	Hashing
A3564	SHS ● FIPS 180-4	SHA2-512	N/A	Hashing
Vendor Affirmed	CKG (SP 800-133rev2)	Section 5.1, Section 5.2	Cryptographic Key Generation; SP 800-133rev2 and IG D.I.	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 CTR_DRBG (DRBG Cert. #A3564).

Table 4 - Approved Algorithms (Crypto Library – II)

CAVP Cert	Algorithm and Standard	Mode/Method	Description/Key Size(s) / Key Strength(s)	Use / Function
A3565	AES: • [FIPS 197; SP 800-38A]	CBC	128 or 256 bits	Data Encryption/Decryption
A3565	HMAC • [FIPS 198-1]	HMAC-SHA2-256	At least 160 bits	Message Authentication
A3565	HMAC • [FIPS 198-1]	HMAC-SHA2-384	At least 160 bits	Message Authentication
A3565	HMAC • FIPS 198-1	HMAC-SHA2-512	At least 160 bits	Message Authentication
A3565	SHS • FIPS 180-4	SHA2-256	N/A	Hashing
A3565	SHS • FIPS 180-4	SHA2-384	N/A	Hashing
A3565	SHS • FIPS 180-4	SHA2-512	N/A	Hashing

Table 5 - Approved Algorithms (Crypto Library - IV)

CAVP Cert	Algorithm and Standard	Mode/Method	Description/Key Size(s) / Key Strength(s)	Use / Function
C170	RSA FIPS 186-4	RSA SigVer (PKCS#1 v1.5)	Modulus: 2048 bits	Digital Signature Verification
C170	SHS • FIPS 180-4	SHA-1	N/A	Hashing Note: SHA-1 is not used for digital signature generation
C170	SHS • FIPS 180-4	SHA2-256	N/A	Hashing

Table 6 - Approved Algorithms (Crypto Library V)

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 7 - Entropy Certificates

Notes:

- ESV Cert. #E68 is for 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 ION 5200 and ION 9200

As the module can only be operated in the Approved mode of operation, and any algorithms not listed in the tables 3-6 above will be rejected by the module while in the approved mode, the options defined in SP 800-140B for the following categories are missing from 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

3. Cryptographic Module Interfaces

The module provides a number of physical and logical interfaces to the device, and the physical interfaces provided by the module are mapped to the following FIPS 140-3 defined logical interfaces: data input, data output, control input, control output (N/A), status output, and power. The logical interfaces and their mapping are described in the following tables.

Physical Port	ION 1200 Qty	ION 1200-C-NA Qty	ION 1200-C-ROW Qty	ION 1200-C-5G-WW Qty
LEDs	4	5	5	5
USBs	2 x Type-A (Functionally Disabled)	2 x Type-A (Functionally Disabled)	2 x Type-A (Functionally Disabled)	2 x Type-A (Functionally Disabled)
Console	1 x RJ-45	1 x RJ-45	1 x RJ-45	1 x RJ-45
Ethernet	4 x RJ-45	4 x RJ-45	4 x RJ-45	4 x RJ-45
Uplink Connector	None	3	3	4
Power	1	1	1	1

Table 8 - ION 1200 Interface Quantity

Note: All USB ports on each ION 1200 module are functionally disabled.

Physical Port	Logical Interface	Data that passes over port/interface
Ethernet and Uplink Connector	Data Input	Data input into the module for all the services defined in Approved Services Table, including TLSv1.2, SSHv2, IPsec/IKEv2 and SNMPv3 service data.
Ethernet and Uplink Connector	Data Output	Data output from the module for all the services defined in Approved Services Table, including TLSv1.2, SSHv2, IPsec/IKEv2 and SNMPv3 service data.
Ethernet and Uplink Connector	Control Input	Control Data input into the module for all the services defined in Approved Services Table, including TLSv1.2, SSHv2, IPsec/IKEv2 and SNMPv3 service data.
Console, Ethernet, Uplink Connector and LEDs	Status Output	Status Information output from the module.
N/A	Control Output	N/A
Power	N/A	Provide the Power Supply to the module.

Table 9 - Ports and Interfaces (ION 1200)

Physical Port	ION 1200-S Qty	ION 1200-S-C-NA Qty	ION 1200-S-C-ROW Qty	ION 1200-S-C-5G-WW Qty
USB	2 x USB 3.0 (Functionally Disabled)	2 x USB 3.0 (Functionally Disabled)	2 x USB 3.0 (Functionally Disabled)	2 x USB 3.0 (Functionally Disabled)

Console	1	1	1	1
Micro USB	1	1	1	1
SFP/RJ-45 Combo port	Ports 1 and 2 (SFP/RJ-45 Combo)	Ports 1 and 2 (SFP/RJ-45 Combo)	Ports 1 and 2 (SFP/RJ-45 Combo)	Ports 1 and 2 (SFP/RJ-45 Combo)
ByPass Pair (Note: This is not for FIPS 140-3 Bypass Service)	Ports 3 and 4	Ports 3 and 4	Ports 3 and 4	Ports 3 and 4
Ethernet Ports	Ports 5 - 10 (Access Ports) Ports 7 - 10 (PoE)	Ports 1 - 10 (Access Ports) Ports 7 - 10 (PoE)	Ports 1 - 10 (Access Ports) Ports 7 - 10 (PoE)	Ports 1 - 10 (Access Ports) Ports 7 - 10 (PoE)
LEDs	3	4	4	4
Power	2	2	2	2
Uplink Connector	N/A	3	3	4

Table 10 - ION 1200-S Interface Quantity

Note: All USB and Micro USB ports on each ION 1200-S module are functionally disabled.

Physical Port	Logical Interface	Data that passes over port/interface
Ethernet, PoE, SFP/RJ-45 Combo port, ByPass Pair, and Uplink Connector	Data Input	Data input into the module for all the services defined in Approved Services Table, including TLSv1.2, SSHv2, IPsec/IKEv2 and SNMPv3 service data.
Ethernet, PoE, SFP/RJ-45 Combo port, ByPass Pair, and Uplink Connector	Data Output	Data output from the module for all the services defined in Approved Services Table, including TLSv1.2, SSHv2, IPsec/IKEv2 and SNMPv3 service data.
Ethernet, PoE, SFP/RJ-45, and Uplink Connector	Control Input	Control Data input into the module for all the services defined in Approved Services Table, including TLSv1.2, SSHv2, IPsec/IKEv2 and SNMPv3 service data.
Console, Ethernet, PoE, ByPass Pair, SFP/RJ-45 Combo port, Uplink Connector, and LEDs	Status Output	Status Information output from the module.
N/A	Control Output	N/A
Power	N/A	Provide the Power Supply to the module.

Table 11 - Ports and Interfaces (ION 1200-S)

Physical Port	ION 3200 Qty
USB	2 x USB 3.0(Functionally Disabled)
Console	1 x RJ-45 serial console port
Micro USB	1 x USB Type B console connector
SFP / RJ-45 Combo port	Ports 1 and 2 (SFP/RJ-45)
ByPass Pair (Note: This is not for FIPS 140-3 Bypass Service)	Ports 3 and 4 (RJ-45)
Ethernet or PoE	Ports 5 - 10 (RJ-45) Ports 7 - 10 (PoE)
LEDs	3
Power	2

Table 12 - ION 3200 Interface Quantity

Note: All USB ports on ION 3200 module are functionally disabled.

Physical Port	Logical Interface	Data that passes over port/interface
Ethernet, PoE, ByPass Pair, SFP/RJ-45 Combo port	Data Input	Data input into the module for all the services defined in Approved Services Table, including TLSv1.2, SSHv2, IPsec/IKEv2 and SNMPv3 service data. Status of the module via LEDs.
Ethernet, PoE, ByPass Pair, SFP/RJ-45 Combo port	Data Output	Data output from the module for all the services defined in Approved Services Table, including TLSv1.2, SSHv2, IPsec/IKEv2 and SNMPv3 service data. Status of the module via LEDs.
Ethernet, PoE, SFP/RJ-45 Combo port	Control Input	Control Data input into the module for all the services defined in Approved Services Table, including TLSv1.2, SSHv2, IPsec/IKEv2 and SNMPv3 service data
Console, ByPass Pair, Ethernet, PoE, SFP/RJ-45 Combo port, and LEDs	Status Output	Status Information output from the module.
N/A	Control Output	N/A
Power	N/A	Provides the power supply to the module.

Table 13 - Ports and Interfaces (ION 3200)

Physical Port	ION 5200 Qty
ByPass Pair (Note: This is not for FIPS 140-3 Bypass Service)	Ports 1 - 4
PoE	Ports 9 - 12
SFP+	Ports 13 - 16
Ethernet	Ports 5 - 8, Ports 17-19 (RJ-45)
Console	1 x RJ-45 serial console port
USB	1
Micro USB	1
LEDs	9
Power	2

Table 14 - ION 5200 Interface Quantity

Note: All USB and Micro USB ports on each ION 5200 module are functionally disabled.

Physical Port	Logical Interface	Data that passes over port/interface
Ethernet, PoE, ByPass Pair, SFP+/RJ-45 Combo port	Data Input	Data input into the module for all the services defined in Approved Services Table, including TLSv1.2, SSHv2, IPsec/IKEv2 and SNMPv3 service data. Status of the module via LEDs.
Ethernet, PoE, ByPass Pair, SFP+/RJ-45 Combo port	Data Output	Data output from the module for all the services defined in Approved Services Table, including TLSv1.2, SSHv2, IPsec/IKEv2 and SNMPv3 service data. Status of the module via LEDs.
Ethernet, PoE, SFP+/RJ-45 Combo port	Control Input	Control Data input into the module for all the services defined in Approved Services Table, including TLSv1.2, SSHv2, IPsec/IKEv2 and SNMPv3 service data.
Console, ByPass Pair, Ethernet, PoE, SFP+/RJ-45 Combo port, and LEDs	Status Output	Status Information output from the module.
N/A	Control Output	N/A
Power	N/A	Provides the power supply to the module.

Table 15 - Ports and Interfaces (ION 5200) Interface Descriptions

Physical Port	ION 9200 Qty
ByPass Pair (Note: This is not for FIPS 140-3 Bypass Service)	Ports 1 - 8
PoE	Ports 9 - 12
SFP+	Ports 13 - 22
Ethernet	Ports 23 - 25 (RJ-45)
Console	1 x RJ-45 serial console port
USB	1
Micro USB	1
LEDs	9
Power	2

Table 16 - ION 9200 Interface Quantity

Note: All USB and Micro USB ports on each ION 9200 module are functionally disabled.

Physical Port	Logical Interface	Data that passes over port/interface
Ethernet, PoE, ByPass Pair, SFP+	Data Input	Data input into the module for all the services defined in Approved Services Table, including TLSv1.2, SSHv2, IPsec/IKEv2 and SNMPv3 service data. Status of the module via LEDs.
Ethernet, PoE, ByPass Pair, SFP+	Data Output	Data output from the module for all the services defined in Approved Services Table, including TLSv1.2, SSHv2, IPsec/IKEv2 and SNMPv3 service data. Status of the module via LEDs.
Ethernet, PoE, SFP+	Control Input	Control Data input into the module for all the services defined in Approved Services Table, including TLSv1.2, SSHv2, IPsec/IKEv2 and SNMPv3 service data.
Console, ByPass Pair, Ethernet, PoE, SFP+ and LEDs	Status Output	Status Information output from the module.
N/A	Control Output	N/A
Power	N/A	Provides the power supply to the module.

Table 17 - Ports and Interfaces (ION 9200) Interface Descriptions

Note: All USB ports on each ION 9200 module are functionally disabled.

4. Roles, Services, and Authentication

The modules all support role-based authentication, and provide the Crypto Officer role and the User role. The Crypto Officer role has the ability to perform all tasks and administrative actions while the User is read-only.

Role	Service	Input	Output
Crypto Officer	Crypto Officer Role Authentication	Crypto Officer role authentication request	Status of Crypto Officer role authentication
Crypto Officer	Perform Self-Test	Command to trigger Self-Test	Status of the self-tests results
Crypto Officer	Perform Zeroization	Command to initiate the SSPs zeroization	Status of the SSPs zeroization
Crypto Officer	Firmware Update	Command to upload a new validated firmware	Status of the updated firmware installation
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

Table 18 - Roles, Services Commands, Input and Output (Crypto Officer)

Role	Service	Input	Output
User	User Role Authentication	User role authentication request	Status of User role authentication
User	Show Version	Command to show version	Module's name/ID and versions
User	Show Status	Initialize show status command	Module's status information
User	Run SSHv2 Function	Initiate SSHv2 tunnel establishment request	Status of SSHv2 tunnel establishment
User	Run TLSv1.2 Function	Initiate TLSv1.2 tunnel establishment request	Status of TLSv1.2 tunnel establishment
User	Run SNMPv3 Function	Initiate SNMPv3 tunnel establishment request	Status of SNMPv3 tunnel establishment
User	Run IPsec/IKEv2 Function	Initiate IPsec/IKEv2 tunnel establishment request	Status of IPSec/IKEv2 tunnel establishment

Table 19 - Roles, Services Commands, Input and Output (User)

Role	Authentication Method	Authentication Strength
User	Password/Pre-shared Secret	The modules support Password based authentication mechanism using the minimum length is eight (8) characters password (94 possible characters from the keyboard). 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. For multiple attacks during a one-minute period, as the module supports at most 3 failed attempts to authenticate in a one-minute period, the probability of successfully authenticating to the module within one minute is 3/(94^8), which is less than 1/100,000. This calculation is based on the assumption that the typical standard American QWERTY computer keyboard has 10 Integer digits, 52 alphabetic characters, and 32 special characters providing 94 characters to choose from in total.
Crypto Officer, User	RSA	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 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.
User	ECDSA	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.

Table 20 - Roles and Authentication

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and / or SSPs	Indicator
Crypto Officer role Authenticatio n	Crypto Officer Role Authentication	RSA SigVer	Crypto Officer Authentication RSA Public Key (PSP)	Crypto Officer	W/E/Z	CO role successful login status
Perform Self-Test	Initiate and run the pre-operational self-tests pre-operational self-tests	HMAC-SHA2-256	Firmware Integrity Test Key (Non-SSP)	Crypto Officer	N/A	None
Perform Zeroization	Zeroize all unprotected SSPs stored in the module	N/A	All	Crypto Officer	Z	None
Firmware Update	The module's firmware is updated to a new version	RSA Signature Verification	Firmware Update Key (SSP)	Crypto Officer	E	Firmware update completion message
Show Version	Provides the module's name/ID and versions	N/A	N/A	Crypto Officer/ User	N/A	None
Show Status	Provides the module's current status and information	N/A	N/A	Crypto Officer/ User	N/A	None
Configure Network	Perform the Module's Network Configuration	N/A	N/A	Crypto Officer	G/R/W/E	Global indicator and Configuratio n logs
Configure SSHv2 Function	Create a secure SSHv2 channel	AES-CTR; CKG; CTR_DRBG; ECDSA KeyGen; ECDSA KeyVer; ECDSA SigGen; ECDSA SigVer; HMAC-SHA-1; HMAC-SHA2-256; HMAC-SHA2-512; KAS-SSC (ECC); KAS (ECC); KDF SSH	DRBG Entropy Input (CSP); DRBG Seed (CSP); DRBG Internal State V Value (CSP); DRBG Key (CSP); 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)	Crypto Officer	G/R/W/E	Global indicator and SSH connection log message
Configure TLSv1.2 Function	Create a secure TLSv1.2 channel	AES-CBC; AES-GCM; CKG;	DRBG Entropy Input (CSP); DRBG Seed (CSP);	Crypto Officer	G/R/W/E	Global indicator and

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and / or SSPs	Indicator
		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 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)			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
User role Authentication	User Role Authentication	N/A	User Password (CSP)	User	W/E	N/A
Run SSHv2 Function	Negotiation and encrypted data transport via SSH	AES-CTR; CKG; CTR_DRBG;	DRBG Entropy Input (CSP); DRBG Seed (CSP); DRBG Internal State V Value (CSP);	User	G/R/W/E	Global indicator and SSHv2 Function

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and / or SSPs	Indicator
		ECDSA KeyGen; ECDSA KeyVer; ECDSA SigGen; ECDSA SigVer; HMAC-SHA-1; HMAC-SHA2-256; HMAC-SHA2-512; KAS-SSC (ECC); KAS (ECC); KDF SSH	DRBG Key (CSP); 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);			running status message
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)	User	G/R/W/E	Global indicator and TLSv1.2 Function running status 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)	User	G/R/W/E	Global indicator and SNMPv3 Function running status 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;	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);	User	G/R/W/E	Global indicator and IPSec/IKEv2 Function running status message

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and / or SSPs	Indicator
		HMAC-SHA2-512; KAS-SSC (ECC); KAS (ECC); RSA KeyGen; RSA SigGen; RSA SigVer; KDF IKEv2	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)			

Table 21 - 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 zeroises the SSP.

Unauthenticated Services

Unauthenticated Users can run the self-test service by power-cycling the module by removing the power and re-applying.

5. Software/Firmware Security

Integrity Techniques

The module performs the Firmware Integrity test by using HMAC-SHA2-256 (HMAC Cert. #A3563) during the Pre-Operational Self-Test. 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. 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.

The module also supports the firmware load test by using RSA 2048 bits with SHA2-256 (RSA Cert. #A3563) 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 into the module before loading any 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.

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 firmware 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 Operational Environment requirements are not applicable as the module does not contain modifiable operational environments. The operational environment is non-modifiable. New firmware versions within the scope of this validation must be validated through the FIPS 140-3 CMVP. Any other firmware loaded into these modules is out of the scope of this validation and requires a separate FIPS 140-3 validation.

7. Physical Security

The module's physical security includes tamper evident labels that are utilized to meet FIPS 140-3 Level 2 requirements. Details regarding the label placement are noted below:

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper Evident Labels	30 days	Verify integrity of tamper-evident seals in the locations identified in the FIPS Kit Installation Guide. Label integrity to be verified within the module's operating temperature range. TEL Quantity Required on each Module: Qty. 3 - ION 1200; Qty 4 - ION 1200-C-NA, ION 1200-C-ROW, ION 1200-C-5G-WW; Qty. 3 - ION 1200-S, ION 1200-S-C-NA, ION 1200-S-C-ROW, ION 1200-S-C-5G-WW; Qty. 3 - ION 3200; Qty. 12 - ION 5200/9200
Opacity Shield	30 days	Verify integrity of the front opacity shield such that it has not been tampered, scratched, or warped

Table 22 - Physical Security Inspection Guidelines

Kit Part Numbers

The module requires the following for physical security requirements:

- [ION 1200, ION 1200-C-NA, ION 1200-C-ROW, ION 1200-C-5G-WW]: Kit P/N 920-000363
- [ION 1200-S, ION 1200-S-C-NA, ION 1200-S-C-ROW, ION 1200-S-C-5G-WW]: Kit P/N 920-000363
- ION 3200: Kit P/N 920-000363
- ION 5200, ION 9200: Kit P/N 920-000333

If additional labels are needed, the CO will need to contact Palo Alto Networks.

ION 1200

The following section demonstrates how to apply the tamper evident labels (TELs) to the ION 1200 modules. The enclosure of the modules is the same.

The tamper evident labels shall be installed on the security devices containing the module prior to operating in Approved mode. TELs shall be applied as depicted in the figures below. Any unused TELs must be securely stored, accounted for, and maintained by the Crypto Officer (CO) in a protected location.

Should the CO have to remove, change or replace TELs for any reason, the CO must examine the location from which the TEL was removed and ensure that no residual debris is still remaining on the chassis or card. If residual debris remains, the CO must remove the debris using a damp cloth.

Any deviation of the TELs placement by unauthorized operators such as tearing, misconfiguration, removal, change, replacement or any other change in the TELs from its original configuration as depicted below shall mean the module is no longer in Approved mode of operation. Returning the system back to Approved mode of operation requires the replacement of the TELs as depicted below and any additional requirement per the site security policy which are out of scope of this Security Policy.

The ION 1200 requires 3 tamper evident labels while the ION 1200-C-NA/ION 1200-C-ROW/ION 1200-C-5G-WW require 4 tamper evident labels. The figures below detail the location of the labels.

Figure 12 - ION 1200 Front View

Figure 13 - ION 1200-C-5G-WW Front View

Figure 14 - ION 1200-C-NA and ION 1200-C-ROW Front View

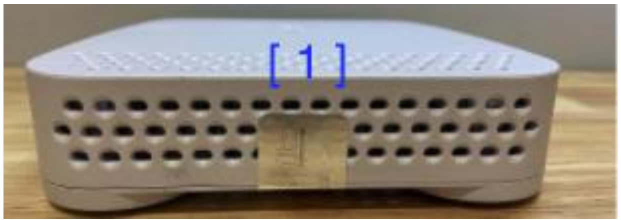

Figure 15 - ION 1200 Left View (same for all models)

Figure 16 - ION 1200 Right View (same for all models)

Figure 17 - ION 1200 Top View

Figure 18 - ION 1200-C-5G-WW/ION 1200-C-NA/ION 1200-C-ROW Top View

Figure 19 - ION 1200 Rear View

Figure 20 - ION 1200 Bottom View

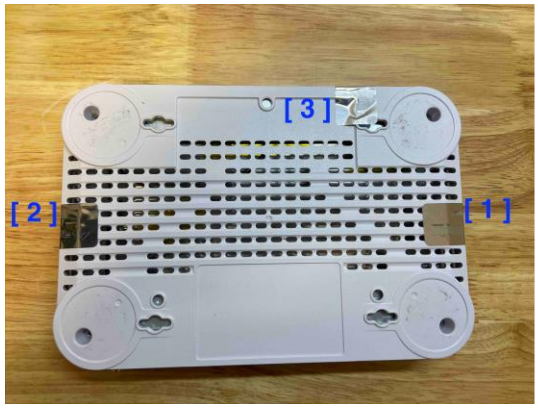

Figure 21 - ION 1200-C-5G-WW/ION 1200-C-NA/ION 1200-C-ROW Bottom View

Figure 21A - ION 1200-S Rear View

Figure 21B - ION 1200-S-C-NA, ION 1200-S-C-ROW, ION 1200-S-C-5G-WW Rear View

Figure 21C - ION 1200-S, ION 1200-S-C-NA, ION 1200-S-C-ROW, ION 1200-S-C-5G-WW Bottom View

ION 3200

The ION 3200 requires 3 tamper labels, which are placed at the following locations.

Figure 22 - ION 3200 Rear View

Figure 23 - ION 3200 Bottom View

Figure 24 - ION 3200 Left Side View

Figure 25 - ION 3200 Right Side View

ION 5200 / 9200

The ION 5200 and ION 9200 use the same FIPS kit and have the same installation. The figure below demonstrates the tamper label placement along with the front opacity shield.

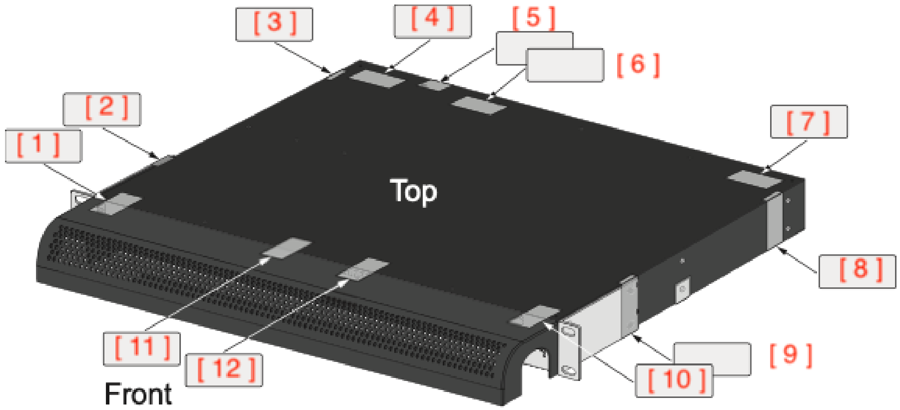

Figure 26 - ION 5200/9200 FIPS Kit Installation

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)	256 bits	N/A	Obtained from the Entropy Source located within module's cryptographic boundary	Import to the module via Module's API Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used to seed the DRBG
DRBG Seed (CSP)	256 bits	CTR_DRBG; Cert. #A3563; HMAC_DRBG; Cert. #A3564	Internally Derived from entropy input string as defined by SP800-90Arev1 DRBG	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Random number generation
DRBG Internal State V Value	256 bits	CTR_DRBG; Cert. #A3563; HMAC_DRBG; Cert. #A3564	Internally Derived from entropy input string as defined by SP800-90Arev1 DRBG	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Random number generation
DRBG Key (CSP)	256 bits	CTR_DRBG; Cert. #A3563; HMAC_DRBG; Cert. #A3564	Internally Derived from entropy input string as defined by SP800-90Arev1 DRBG	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Random number generation
Crypto Officer Authentication RSA Public Key (PSP)	2048 bits	SHA-1; SHA2-256; RSA SigVer Cert. #C170	Pre-loaded at the factory	Import: No Export: No	N/A	Embedded in the module's executable binary in HDD (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used for CO role authentication
User Password (CSP)	8 characters minimum	N/A	N/A	Import to the Module encrypted by TLS/SSH session key Export: No	MD/EE	HDD (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used for User role authentication
Firmware Load Test Key (CSP)	112 bits (Modulus: 2048 bits)	RSA SigVer Cert. #A3563	Pre-loaded at the build time (in the module's binary)	Import: No Export: No	N/A	Embedded in the module's executable binary in HDD (plaintext)	N/A (Note: This key is only used for Firmware Load Test and not subject to the zeroization requirement)	Used for Firmware Load Test
TLS RSA Private Key (CSP)	112 - 128 bits (Modulus: 2048, 3072 bits)	CKG; DRBG; RSA KeyGen; RSA SigGen; Certs. #A3563 and #A3564	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)	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 SigVer; Certs. #A3563 and #A3564	Internally derived per the FIPS 186-4 RSA key generation method	Import: No Export to the TLS peer via the Module's data output interface	N/A	HDD (plaintext)	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. #A3563 and #A3564	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)	Zeroized by SSP (CSP/PSP) Zeroization Command	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. #A3563 and #A3564	Internally derived internally per the EC Diffie-Hellman key agreement (SP800-56Arev3)	Import: No Export to the TLS peer via the Module's data output interface	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used to derive TLS ECDHE Shared Secret
Peer TLS ECDHE Public Key (PSP)	128 – 256 bits (Curves: P-256, P-384, P-521)	N/A	N/A	Import to the Module via Module's data input interface Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used to derive TLS ECDHE Shared Secret

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import/Export	Establish-ment	Storage	Zeroization	Use & Related Keys
TLS ECDHE Shared Secret (CSP)	128 – 256 bits (Curves: P-256, P-384, P-521)	KAS-ECC-SSC; KAS-ECC; Certs. #A3563 and #A3564	Internally derived Using SP800-56Ar3 ECDH shared secret computation Generated	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used to derive TLS Session Encryption Keys, TLS Session Authentication Keys
TLS Pre-Master Secret (CSP)	384 bits	Keying Material	Internally derived per SP800-135 rev1 KDF (TLSv1.2)	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used to derive TLS Master Secret
TLS Master Secret (CSP)	384 bits	Keying Material	Internally derived per SP800-135 rev1 KDF (TLSv1.2)	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	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. #A3563 and #A3564	Internally derived via key derivation function defined in SP 800-135rev1 KDF (TLSv1.2)	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used to secure TLS session confidentiality
TLS Session Authentication Key (CSP)	At least 112 bits	KDF TLS; KTS; HMAC-SHA2-256; HMAC-SHA2-384; Certs. #A3563 and #A3564	Internally derived via key derivation function defined in SP800-135 rev1 KDF TLSv1.2	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used to secure the TLS session integrity
IPSec/IKE Pre-Shared Secret (CSP)	2048 bits	N/A	N/A	Import: Encrypted by using TLS/SSH session key Export: No	MD/EE	HDD (plaintext)	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 KeyGen; RSA SigGen; Cert. #A3563	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)	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. #A3563	Internally derived per the FIPS 186-4 RSA key generation method	Import: No Export to the IPSec/IKE peer via the Module's data output interface	N/A	HDD (plaintext)	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; Cert. #A3563	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)	Zeroized by SSP (CSP/PSP) Zeroization Command	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 Cert. #A3563	Internally derived per the EC Diffie-Hellman key agreement (SP800-56A rev3)	Import: No Export to the IPSec/IKE peer	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	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. #A3563	Internally derived using SP800-56A rev3 ECDH shared secret computation	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	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;	Internally derived via key derivation function defined in SP800-135rev1 KDF (IKEv2)	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used to secure IPSec/IKEv2 session confidentiality

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import/Export	Establish-ment	Storage	Zeroization	Use & Related Keys
		Certs. #A3563 and #A3565						
IPSec/IKE Session Authentication Key (CSP)	At least 112 bits	HMAC-SHA-1; HMAC-SHA2-256; HMAC-SHA2-384; HMAC-SHA2-512; KDF IKEv2; Certs. #A3563 and #A3565	Internally derived via key derivation function defined in SP800-135rev1 KDF (IKEv2)	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	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)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used for SNMPv3 User authentication
SNMPv3 Session Encryption Key (CSP)	128 bits	AES-CFB; KDF SNMPv3; Cert. #A3563	Internally derived via key derivation function defined in SP800-135rev1 KDF (SNMPv3)	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used to secure SNMPv3 session confidentiality
SNMPv3 Session Authentication Key (CSP)	160 bits	HMAC-SHA-1; KDF SNMPv3; Cert. #A3563	Internally derived via key derivation function defined in SP800-135rev1 KDF (SNMPv3)	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used to secure SNMPv3 session integrity
SSH ECDHE Private Key (CSP)	128-256 bits (Curves: P-256, P-384, or P-521)	CKG; DRBG; KAS-ECC-SSC; Cert. #A3563	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)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used to derive the SSH ECDHE Shared Secret
SSH ECDHE Public Key (PSP)	P-256, P-384, or P-521	KAS-ECC-SSC; Cert. #A3563	Internally derived internally per the EC Diffie-Hellman key agreement (SP800-56Arev3)	Import: No Export to the SSH peer via the Module's data output interface	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used to derive the SSH ECDHE Shared Secret
SSH ECDHE Shared Secret (CSP)	128-256 bits (Curves: P-256, P-384, or P-521)	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)	Zeroized by SSP (CSP/PSP) Zeroization Command	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. #A3563	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)	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 SigVer; Cert. #A3563	Internally derived per the FIPS 186-4 RSA key generation method	Import: No Export to the SSH peer via the Module's data output interface	N/A	HDD (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used for SSH session authentication
SSH Session Encryption Key (CSP)	128, 192, or 256 bits	AES-CTR; KDF SSH; KTS; Cert. #A3563	Internally derived via key derivation function defined in SP 800-135rev1 KDF (SSHv2)	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used for SSH session confidentiality protection
SSH Session Authentication Key (CSP)	At least 160 bits	KDF SSH; KTS; HMAC-SHA-1; HMAC-SHA2-256; HMAC-SHA2-512; Cert. #A3563	Internally derived via key derivation function defined in SP800-135 KDF (SSH)	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used for SSH session integrity protection

Table 23 – SSPs

Notes:

1. To initiate zeroization, see Section End of Life / Sanitization in this document for more details.
2. The zeroization operations shall be performed under the control of the CO role.
3. The zeroized SSPs cannot be retrieved or reused. Once the command is initiated, the SSPs are overwritten with 0s.

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 24 - 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
Firmware integrity	Using HMAC-SHA2-256

Table 25 - Crypto Library I 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-GCM	AES-GCM 256 bits Encryption KAT
AES-GCM	AES-GCM 256 bits Decryption KAT
DRBG	CTR_DRBG (AES-256) KAT: Instantiate; KAT: Generate; KAT: Reseed Note: DRBG Health Tests as specified in SP800-90Arev1 Section 11.3 are performed)
ECDSA SigGen	KAT using P-224 with SHA2-256 (ECDSA Signature Generation)
ECDSA SigVer	KAT using P-224 with SHA2-256 (ECDSA Signature Verification)

Algorithm	Self-Test Details
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 IKEv2 KDF
KDF SNMP	KAT for SNMPv3 KDF
KDF SSH	KAT for SSHv2 KDF
KDF TLS	KAT for TLSv1.2 KDF
RSA SigGen	KAT using 2048 bits modulus with SHA2-256 (RSA Signature Generation)
RSA SigVer	KAT using 2048 bits modulus with SHA2-256 (RSA Signature Verification)
SHS	KAT using SHA-1

Table 26 – CASTs (Crypto Library I)

Algorithm	Self-Test Details
AES	AES-CBC 256 bits Encryption KAT
AES	AES-CBC 256 bits Decryption KAT
AES-GCM	AES-GCM 256 bits Encryption KAT
AES-GCM	AES-GCM 256 bits Encryption KAT
DRBG	HMAC_DRBG (SHA2-512) KAT: Instantiate; KAT: Generate KAT: Reseed Note: DRBG Health Tests as specified in SP800-90Arev1 Section 11.3 are performed)
ECDSA SigGen	KAT using P-224 with SHA2-256 (ECDSA Signature Generation)
ECDSA SigVer	KAT using P-224 with SHA2-256 (ECDSA Signature Verification)
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 TLSv1.2 KDF
RSA SigGen	KAT using 2048 bits modulus with SHA2-256 (RSA Signature Generation)
RSA SigVer	KAT using 2048 bits modulus with SHA2-256 (RSA Signature Verification)
SHS	KAT using SHA-1

Table 27 – CASTs (Crypto Library II)

Algorithm	Self-Test Details
AES	AES-CBC 128 bits Encryption KAT
AES	AES-CBC 128 bits Decryption KAT
HMAC	KAT using SHA2-256
HMAC	KAT using SHA2-384
HMAC	KAT using SHA2-512

Table 28 –CASTs (Crypto Library IV)

Algorithm	Self-Test Details
RSA	KAT using 2048 bit key, SHA2-256 (RSA Signature Verification)

SHS	KAT using SHA2-256

Table 29 –CASTs (Crypto Library V)

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 30 - Entropy Source Health Tests

Conditional Pair-Wise Consistency Tests

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

Table 31 - Conditional Pair-Wise Consistency Tests (Crypto Library I)

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

Table 32 - Conditional Pair-Wise Consistency Tests (Crypto Library II)

Conditional Firmware Load Test

Conditional Self-Tests Algorithm	Self-Test Details
Firmware Load Test	RSA 2048 with SHA2-256 Signature Verification

Table 33 - Conditional Firmware Load Test (Crypto Library I)

Periodic/On-Demand Self-Test

The module performs on-demand self-tests initiated by the operator, by power cycling the module. 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 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. The table 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 Firmware 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
Failed Firmware Load Test	Verification Failure
SP 800-90B Entropy Source Start-up/Continuous health tests	No random numbers are generated and key generation is halted

Table 35 - Error State Indicators

11. Life-Cycle Assurance

All ION devices are designed to handle the various stages of a module's life-cycle. The sections below highlight the details for each stage.

Secure Delivery Procedures

The security of the module is maintained during the transfer of these products from production sites to the customer through the following mechanisms:

- Email from Palo Alto Networks, Inc. confirming the order and includes tracking number(s). When the package arrives at the customer site, the customer checks the tracking number on the package with the tracking number supplied by Palo Alto Networks, Inc.
- The customer also checks the integrity of the package by inspecting the integrity of the security tape and the seals of the package for tampering. Any damages to the security tape and the seals of the package would require the customer to contact Palo Alto.
- The hardware and applicable documentation are delivered in the same package.

Secure Operation

The module meets all the Level 2 requirements for FIPS 140-3. Follow the secure operations provided below to place the module in approved mode. Operating this module without maintaining the following settings will remove the module from the approved mode of operation. The module runs firmware version 6.1.2. This is the only allowable firmware image for this current approved mode of operation. The module is initiated into the Approved mode of operation via the following procedure:

1. The Crypto Officer must apply tamper evidence labels as described in Section "Physical Security" of this document
2. Power on the ION Module
3. Using the Controller, navigate to the device that is to be initiated
    a. Note: The module authenticates the Crypto Officer using default authentication (Root CA), and then replaces the default information with a specific one from the Controller (CO role)
4. Click the three bullets next to the device
5. Select "FIPS"
    a. Click "proceed" to begin initialization procedure
6. 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
7. 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, the module automatically enforces a login certificate change for the Crypto Officer. 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 modules 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 via SSH with Crypto Officer
2. Authenticate using proper credentials
3. Execute command: "disable system"
   a. Confirm command
4. Module will begin zeroization process and wipe all security parameters and configurations within the module's boundary

12. Mitigation of Other Attacks

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