Palo Alto Networks SD-WAN Instant-On Network (ION) Devices

ION 1200 and ION 9000

Firmware Version: 5.6.3

FIPS 140-3 Non-Proprietary Security Policy

Palo Alto Networks, Inc.
www.paloaltonetworks.com

Revision Date: May 31, 2024
Document Version: 1.3

Table of Contents

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 and ION 9000 with firmware version 5.6.3 (hereinafter referred to as the Module or ION module).

The Palo Alto Networks SD-WAN Instant-On Network (ION) Devices ION 1200 and ION 9000 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.

Cryptographic Module Specification

FIPS 140-3 conformance testing was performed at Security Level 2 with the following configurations noted in the table 2 below.

Cryptographic Boundary

The module is a hardware multiple-chip standalone cryptographic module. The cryptographic boundary is defined as the entire modules' chassis unit encompassing the "top," "front," "left," "right," "rear" and "bottom" surfaces of the case, and shown in the Physical Security section. These modules are described in more detail in the Cryptographic Module Interfaces section.

Figure 1 - ION 1200

Figure 2 - ION 9000

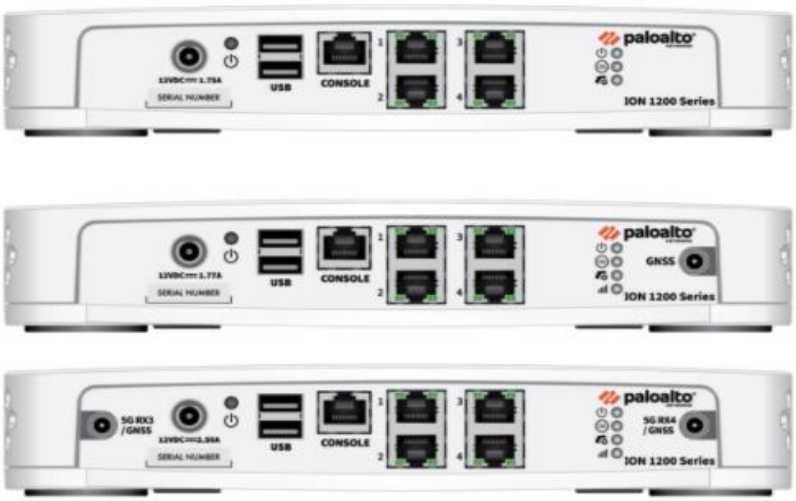

Figure 3 - ION 1200 (Top), ION 1200-C-NA/ION 1200-C-ROW (Middle), and ION 1200-C-5G-WW (Bottom) Front Interfaces

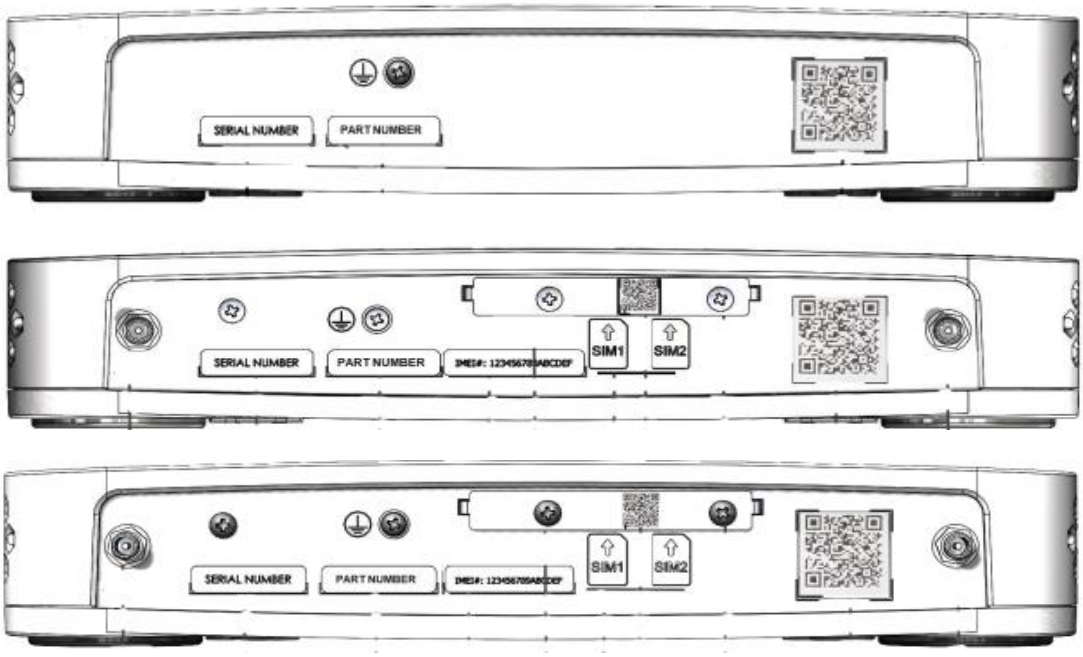

Figure 4 - ION 1200 (Top), ION 1200-C-NA/ION 1200-C-ROW (Middle), and ION 1200-C-5G-WW (Bottom) Rear Interfaces

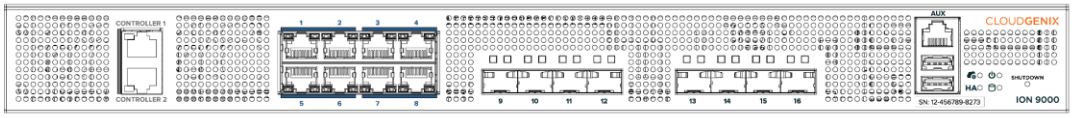

Figure 5 - ION 9000 Front Interfaces

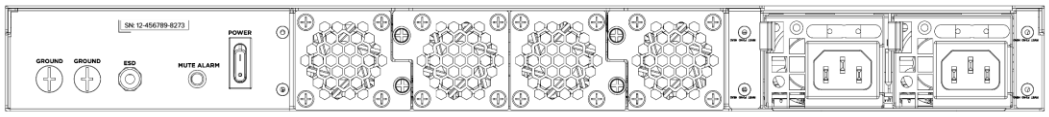

Figure 6 - ION 9000 Rear Interfaces

Model	Hardware [Part Number and Version]	Firmware Version	Distinguishing Features
ION 1200	ION 1200 ION 1200-C-NA ION 1200-C-ROW ION 1200-C-5G-WW	5.6.3	See Cryptographic Module Interfaces section
ION 9000	ION 9000	5.6.3	

Table 2 - Cryptographic Module Tested Configuration

Note: The part number for Tamper Evidence Label (TEL) can be found in section Physical security of this document.

Modes of operation

By default, the module is delivered with a non-Approved mode of operation but supports an Approved mode of operation. Once the module is configured to operate in the Approved mode of operation by following the steps in section "Secure Operation" of this document by the Crypto Officer, the module can only operate in the Approved mode. The module does not claim implementation of a degraded mode of operation.

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
A2385	AES: ● FIPS 197 ● SP 800-38D	ECB	128, 192, and 256 bits	Data Encryption/Decryption
A2385	AES: ● FIPS 197 ● SP 800-38A	CBC	128, 192, and 256 bits	Data Encryption/Decryption
A2385	AES: ● FIPS 197 ● SP 800-38A	CTR	128, 192, and 256 bits	Data Encryption/Decryption
A2385	AES: ● FIPS 197 ● SP 800-38D	GCM	128, 192, and 256 bits	Data Encryption/Decryption
A2385	CVL (KDF-SSH): ● SP 800-135rev1	SSHv2 KDF	N/A	SP800-135rev1 compliant Key Derivation
A2385	CVL (KDF-TLS): ● SP 800-135rev1	TLS 1.2 KDF	N/A	SP800-135rev1 compliant Key Derivation
A2385	CVL (KDF-IKEv2): ● SP 800-135rev1	IKEv2 KDF	N/A	SP800-135rev1 compliant Key Derivation

CAVP Cert	Algorithm and Standard	Mode/Method	Description/Key Size(s) / Key Strength(s)	Use / Function
A2385	CVL (KDF-SNMP): ● SP 800-135rev1	SNMPv3 KDF	N/A	SP800-135rev1 compliant Key Derivation
A2385	DRBG: ● SP 800-90Arev1	CTR_DRBG (AES-256 bits) Derivation Function Enabled: Yes	N/A	Deterministic Random Bit Generation
A2385	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
A2385	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 X1 (path 2) compliant
A2385	ECDSA ● FIPS 186-4	ECDSA KeyGen	Curves: P-224, P-256, P-384, P-521	ECDSA Key Generation
A2385	ECDSA ● FIPS 186-4	ECDSA KeyVer	Curves: P-224, P-256, P-384, P-521	ECDSA Key Verification
A2385	ECDSA ● FIPS 186-4	ECDSA SigGen	Curves: P-224, P-256, P-384, P-521	ECDSA Digital Signature Generation
A2385	ECDSA ● FIPS 186-4	ECDSA SigVer	Curves: P-224, P-256, P-384, P-521	ECDSA Digital Signature Verification
N/A	ENT (P) ● SP800-90B	N/A	N/A	Physical Entropy source used for seeding DRBGs
A2385	HMAC ● FIPS 198-1	HMAC-SHA-1	160 bits	Message Authentication
A2385	HMAC ● FIPS 198-1	HMAC-SHA2-224	224 bits	Message Authentication
A2385	HMAC ● FIPS 198-1	HMAC-SHA2-256	256 bits	Message Authentication
A2385	HMAC ● FIPS 198-1	HMAC-SHA2-384	384 bits	Message Authentication
A2385	HMAC ● FIPS 198-1	HMAC-SHA2-512	512 bits	Message Authentication
A2385	KTS ● SP800-38F	KTS (AES Cert. #A2385)	128, 192, and 256 bits	Key Transport using AES-GCM;

CAVP Cert	Algorithm and Standard	Mode/Method	Description/Key Size(s) / Key Strength(s)	Use / Function
				Key establishment methodology provides between 128 and 256 bits of encryption strength
A2385	KTS ● SP800-38F	KTS (AES Cert. #A2385 and HMAC Cert. #A2385)	128, 192, and 256 bits	Key Transport using AES and HMAC; Key establishment methodology provides between 128 and 256 bits of encryption strength
A2385	RSA ● FIPS 186-4	RSA KeyGen (PKCS#1 v1.5)	Modulus: 2048 and 3072 bits	RSA Key Generation
A2385	RSA ● FIPS 186-4	RSA SigGen (PKCS#1 v1.5)	Modulus: 2048 and 3072 bits	RSA Digital Signature Generation
A2385	RSA ● FIPS 186-4	RSA SigVer (PKCS#1 v1.5)	Modulus: 2048 and 3072 bits	RSA Digital Signature Verification
A2385	SHS ● FIPS 180-4	SHA-1	N/A	Hashing Note: SHA-1 is not used for digital signature generation
A2385	SHS ● FIPS 180-4	SHA2-224	N/A	Hashing
A2385	SHS ● FIPS 180-4	SHA2-256	N/A	Hashing
A2385	SHS ● FIPS 180-4	SHA2-384	N/A	Hashing
A2385	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.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. #A2385)

Table 3 - Approved Algorithms (Crypto Library I)

CAVP Cert	Algorithm and Standard	Mode/Method	Description/Key Size(s) / Key Strength(s)	Use / Function
A2386	AES: ● FIPS 197 ● SP 800-38A	CBC	128 or 256 bits	Data Encryption/Decryption
A2386	AES: ● FIPS 197 ● SP 800-38D	GCM	128 or 256 bits	Data Encryption/Decryption
A2386	CVL (KDF-TLS): ● SP 800-135rev1	TLS 1.2 KDF	TLSv1.2 with SHA2-256/384	SP800-135rev1 compliant Key Derivation
A2386	DRBG: ● SP 800-90Arev1	DRBG with HMAC-SHA2-512	N/A	Deterministic Random Bit Generation
A2386	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
A2386	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 X1 (path 2) compliant
A2386	ECDSA ● FIPS 186-4	ECDSA KeyGen	Curves: P-224, P-256, P-384, P-521	ECDSA Key Generation
A2386	ECDSA ● FIPS 186-4	ECDSA KeyVer	Curves: P-224, P-256, P-384, P-521	ECDSA Key Verification
A2386	HMAC ● FIPS 198-1	HMAC-SHA2-256	256 bits	Message Authentication
A2386	HMAC ● FIPS 198-1	HMAC-SHA2-384	384 bits	Message Authentication
A2386	HMAC ● FIPS 198-1	HMAC-SHA2-512	512 bits	Message Authentication
A2386	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
A2386	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

CAVP Cert	Algorithm and Standard	Mode/Method	Description/Key Size(s) / Key Strength(s)	Use / Function
				128 or 256 bits of encryption strength
A2386	RSA ● FIPS 186-4	RSA SigVer (PKCS#1 v1.5)	Modulus: 2048 bits	Digital Signature Verification
A2386	SHS ● FIPS 180-4	SHA-1	N/A	Hashing Note: SHA-1 is not used for digital signature generation
A2386	SHS ● FIPS 180-4	SHA2-224	N/A	Hashing
A2386	SHS ● FIPS 180-4	SHA2-256	N/A	Hashing
A2386	SHS ● FIPS 180-4	SHA2-384	N/A	Hashing
A2386	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.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 HMAC_DRBG (DRBG Cert. #A2386)

Table 4 - Approved Algorithms (Crypto Library II)

CAVP Cert	Algorithm and Standard	Mode/Method	Description/Key Size(s) / Key Strength(s)	Use / Function
A2387	AES: ● FIPS 197 ● SP 800-38D	CBC	128 or 256 bits	Data Encryption/Decryption
A2387	HMAC ● FIPS 198-1	HMAC-SHA2-256	256 bits	Message Authentication
A2387	HMAC ● FIPS 198-1	HMAC-SHA2-384	384 bits	Message Authentication
A2387	HMAC ● FIPS 198-1	HMAC-SHA2-512	512 bits	Message Authentication
A2387	SHS ● FIPS 180-4	SHA-1	N/A	Hashing
A2387	SHS ● FIPS 180-4	SHA2-256	N/A	Hashing
A2387	SHS ● FIPS 180-4	SHA2-384	N/A	Hashing

A2387	SHS • FIPS 180-4	SHA2-512	N/A	Hashing

Table 5 - Approved Algorithms (Crypto Library III)

CAVP Cert	Algorithm and Standard	Mode/Method	Description/Key Size(s) / Key Strength(s)	Use / Function
A2388	AES: • FIPS 197 • SP 800-38D	CBC	128 or 256 bits	Data Encryption/Decryption
A2388	HMAC • FIPS 198-1	HMAC-SHA2-256	256bits	Message Authentication
A2388	HMAC • FIPS 198-1	HMAC-SHA2-384	384 bits	Message Authentication
A2388	HMAC • FIPS 198-1	HMAC-SHA2-512	512 bits	Message Authentication
A2388	SHS • FIPS 180-4	SHA2-256	N/A	Hashing
A2388	SHS • FIPS 180-4	SHA2-384	N/A	Hashing
A2388	SHS • FIPS 180-4	SHA2-512	N/A	Hashing

Table 6 - Approved Algorithms (Crypto Library IV)

CAVP Cert	Algorithm and Standard	Mode/Method	Description/Key Size(s) / Key Strength(s)	Use / Function
RSA Cert. #1819	RSA • FIPS 186-4	RSA SigVer (PKCS#1 v1.5)	Modulus: 2048 bits	Digital Signature Verification
SHS Cert. #2919	SHS • FIPS 180-4	SHA-1	N/A	Hashing Note: SHA-1 is not used for digital signature generation
SHS Cert. #2919	SHS • FIPS 180-4	SHA2-256	N/A	Hashing
RSA Cert. #1820	RSA FIPS 186-4	RSA SigVer (PKCS#1 v1.5)	Modulus: 2048 bits	Digital Signature Verification
SHS Cert. #2920	SHS • FIPS 180-4	SHA-1	N/A	Hashing Note: SHA-1 is not used for digital signature generation
SHS Cert. #2920	SHS • FIPS 180-4	SHA2-256	N/A	Hashing
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 7 - Approved Algorithms (Crypto Library V)

Notes:

- 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.
- The module's AES-GCM implementation conforms to 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 IKE protocols, other than the KDFs, have been tested by the CAVP and CMVP.

As the module can only be operated in the Approved mode of operation, and any algorithms not listed in the tables 3-8 above will be rejected by the module while in the approved mode, the tables defined in SP800-140B 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

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 table.

Physical Port	Logical Interface	Data that passes over port/interface
Console, Ethernet and Uplink Connector	Data Input	Data input into the module for all services defined in Tables 12 and 13, including TLSv1.2, SSHv2, IPsec/IKEv2 and SNMPv3 service data.
Console, Ethernet and Uplink Connector	Data Output	Data output from the module for all services defined in Tables 12 and 13, including TLSv1.2, SSHv2, IPsec/IKEv2 and SNMPv3 service data.
Console, Ethernet, Uplink Connector	Control Input	Control Data input into the module for all services defined in Tables 12 and 13, 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 8 - Ports and Interfaces (ION 1200 Interface Descriptions)

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

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 9 - ION 1200 Interface Quantity

Physical Port	Logical Interface	Data that passes over port/interface
AUX, Controller, Internet/LAN/WAN, SFP+	Data Input	Data input into the module for all services defined in Tables 12 and 13, including TLSv1.2, SSHv2, IPsec/IKEv2 and SNMPv3 service data. Status of the module via LEDs
AUX, Controller, Internet/LAN/WAN, SFP+	Data Output	Data output from the module for all services defined in Tables 12 and 13, including TLSv1.2, SSHv2, IPsec/IKEv2 and SNMPv3 service data. Status of the module via LEDs
AUX, Controller, Internet/LAN/WAN, SFP+	Control Input	Control Data input into the module for all services defined in Tables 12 and 13, including TLSv1.2, SSHv2, IPsec/IKEv2 and SNMPv3 service data
LEDs, AUX, Controller, Internet/LAN/WAN, 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 10 - Ports and Interface (ION 9000 Interface Descriptions)

Note: USB ports on each ION 9000 module are functionally disabled

Physical Port	ION 9000 Qty
LEDs	4
USB Ports	2 x Type-A (Functionally Disabled)
AUX Port	1 x RJ-45
Controller Ports	2 x RJ-45
Internet/LAN/WAN Ports	8
SFP+ Ports	8
Power Port	1

Table 11 - ION 9000 Interface Quantity

Roles, Services, and Authentication

The modules all support role-based authentication, and provide a Crypto Officer and 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	Self-Test	Command to trigger Self-Test	Status of the self-tests results
Crypto Officer	Zeroize	Command to zeroize the module	Status of the SSPs zeroization
Crypto Officer	CO Authentication	CO role authentication request	Status of the CO role authentication
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 versioning information
Crypto Officer	Show Status	Command to show status	Module's status information
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

Role	Service	Input	Output
Crypto Officer	Configure Network and Create User Account	Commands to configure the module	Status of the completion of network related 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 12 - Roles, Service Commands, Input and Output (Crypto Officer)

Role	Service	Input	Output
User	User Authentication	User role authentication request	Status of the User role authentication
User	Show Status	Command to show status	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 13 - Roles, Service Commands, Input and Output (User)

Role	Authentication Method	Authentication Strength
Crypto Officer, User	RSA	The security modules support public-key based authentication using a minimum of RSA 2048 bits. The minimum equivalent strength supported is 112 bits. The probability that a random attempt will succeed is 1/(2^112) which is less than 1/1,000,000. The probability of successfully authenticating to the module within a one minute period is 1,020,000/(2^112), which is less than 1/100,000. The module at its highest can support at most 17,000 new sessions per second to authenticate in a one-minute period.
User	ECDSA	When configuring the smallest curve P-256, the probability that a random attempt will succeed, or a false acceptance will occur is 1/2^128, which is less than 1/1,000,000. 17,000 attempts are allowed in a one-minute period. Therefore, the probability of a random success in a one-minute period is 1,020,000/2^128, which is less than 1/100,000.
User	Password/Pre-shared Secret	The minimum length is eight (8) characters (94 possible characters). The probability that a random attempt will succeed or a false acceptance will occur is 1/(94^8) which is less than 1/1,000,000. The probability of successfully authenticating to the module within one minute is 3/(94^8), which is less than 1/100,000. The configuration supports at most 3 failed attempts to authenticate in a one-minute period. 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.

Table 14 - Roles and Authentication

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
Self-Test	The module runs pre-operational self-tests and conditional algorithm Self-tests (CASTs)	N/A	Firmware Integrity Test Key (non-SSP)	Crypto Officer	N/A	Global indicator and Self-test completion message
Zeroize	Zeroize service destroys all SSPs in the module	N/A	All	Crypto Officer	Z	N/A
Firmware Update	The module's firmware is updated to a new version	RSA SigVer	Firmware update test key (non-SSP)	Crypto Officer	E	Global indicator and Firmware update completion message
CO Authentication	CO role authentication	RSA SigVer	Crypto Officer Authentication RSA Public Key	Crypto Officer	G/R/W/E	Global indicator and CO role authentication status
User Authentication	User role authentication	N/A	User Password	User	G/R/W/E	N/A
Show Version	Provides Module's current name/ID and versioning information	N/A	N/A	Crypto Officer	N/A	N/A
Show Status	Provides Module's current status information	N/A	N/A	Crypto Officer, User	N/A	N/A
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) SSH-KDF	DRBG Entropy Input; DRBG Seed, Internal State V value, and DRBG Key; SSH ECDHE Private Key; SSH ECDHE Public Key; SSH ECDHE Shared Secret; SSH Host Public Key; SSH Host Private Key; SSH Session Encryption Key; SSH Session Authentication Key	Crypto Officer	G/R/W/E	Global indicator and SSH connection success log message
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) RSA KeyGen RSA SigGen RSA SigVer TLS-KDF	DRBG Entropy Input; DRBG Seed, Internal State V value, and DRBG Key; TLS RSA Private Key; TLS RSA Public Key; TLS Pre-Master Secret; TLS Master Secret; TLS ECDHE Private Key; TLS ECDHE Public key; TLS ECDHE Shared Secret; TLS Session Encryption Keys; TLS Session Authentication Key	Crypto Officer	G/R/W/E	Global indicator and TLS connection success log message
Configure Network and Create User Account	Configuration is sent/updated for the module	RSA SigVer, SHA-1 SHA2-256	Crypto Officer Authentication RSA Public Key; User Password	Crypto Officer	G/R/W/E	Global indicator and Configuration logs
Configure SNMPv3 Function	Create a secure SNMPv3 channel	AES-CFB HMAC-SHA-1 SNMP-KDF	SNMPv3 Authentication Secret; SNMPv3 Session Encryption Key;	Crypto Officer	G/R/W/E	Global indicator and SNMP

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
			SNMPv3 Session Authentication Key			connection success log message
Configure IPsec/IKEv2 Function	Create IPSec/IKEv2 tunnel	AES-CBC, AES-GCM, 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, IKE-KDF	DRBG Entropy Input; DRBG Seed, Internal State V value, and DRBG Key; IPSec Pre-Shared Secret; IPSec/IKE RSA Private Key; IPSec/IKE RSA Public Key; IPSec/IKE ECDHE Private Key; IPSec/IKE ECDHE Public Key; IPSec/IKE ECDHE Shared Secret; IPSec/IKE Session Encryption Key; IPSec/IKE Session Authentication Key	Crypto Officer	G/R/W/E	Global indicator and IPSec/IKE connection success log message
Run SSHv2 Function	Negotiation and encrypted data transport via SSH	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) KTS; SSH-KDF	DRBG Entropy Input; DRBG Seed, Internal State V value, and DRBG Key; SSH ECDHE Private Key; SSH ECDHE Public Key; SSH ECDHE Shared Secret; SSH Host Public Key; SSH Host Private Key; SSH Session Encryption Key; SSH Session Authentication Key	User	G/R/W/E	Global indicator and SSHv2 Function 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, TLS-KDF	DRBG Entropy Input; DRBG Seed, Internal State V value, and DRBG Key; TLS RSA Private Key; TLS RSA Public Key; TLS Pre-Master Secret; TLS Master Secret; TLS ECDHE Private Key; TLS ECDHE Public key; TLS ECDHE Shared Secret; TLS Session Encryption Keys; TLS Session Authentication Key	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-CFB HMAC-SHA-1 SNMP-KDF	SNMPv3 Authentication Secret; SNMPv3 Session Encryption Key; SNMPv3 Session Authentication Key	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, AES-GCM, 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,	DRBG Entropy Input; DRBG Seed, Internal State V value, and DRBG Key; IPSec Pre-Shared Secret; IPSec/IKE RSA Private Key; IPSec/IKE RSA Public Key; IPSec/IKE ECDHE Private Key; IPSec/IKE ECDHE Public Key; IPSec/IKE ECDHE Shared Secret; IPSec/IKE Session Encryption Key;	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
		IKE-KDF	IPSec/IKE Session Authentication Key			

Table 15 – 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 module by removing the power and re-applying.

Software/Firmware Security

Integrity Techniques

The module performs the Firmware Integrity test by using HMAC-SHA2-256 (HMAC Cert. #A2385) 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 to 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. #A2385) for the new validated firmware to be uploaded into the module. A Firmware Load Test Key (non-SSP) 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 software integrity test on-demand. This automatically performs the integrity test of all firmware components included within the boundary of the module.

Operational Environment

The FIPS 140-3 Operational Environment requirements are not applicable as the module is not operated in a modifiable operational environment. The operational environment is limited as the modules include a firmware load service to support necessary updates. 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.

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 on ION 1200 Qty. 4 on ION 1200-C-NA, ION 1200-C-ROW, and ION 1200-C-5G-WW Qty. 6 on ION 9000

Table 16 – Physical Security Inspection Guidelines

Kit Part Numbers

The module requires the following for physical security requirements:

- ION 1200 (ION 1200, ION 1200-C-NA, ION 1200-C-ROW, ION 1200-C-5G-WW) FIPS Kit: P/N 920-000363
- ION 9000 FIPS Kit: P/N 920-000311

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

ION 1200, ION 1200-C-NA, ION 1200-C-ROW, and ION 1200-C-5G-WW Physical Security

The following section demonstrates how to apply the tamper evident labels (TELs) to the ION 1200 module. 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 the 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 CO in a protected location.

Should the CO have to remove, change or replace TELs (tamper-evidence labels) 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 the Approved mode of operation. Returning the system back to the 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 7 – ION 1200 Front View

Figure 8 – ION 1200-C-5G-WW Front View

Figure 9 – ION 1200-C-NA and ION 1200-C-ROW Front View

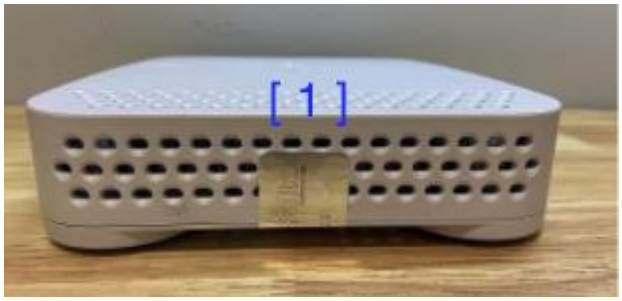

Figure 10 – ION 1200 Left View (same for all models)

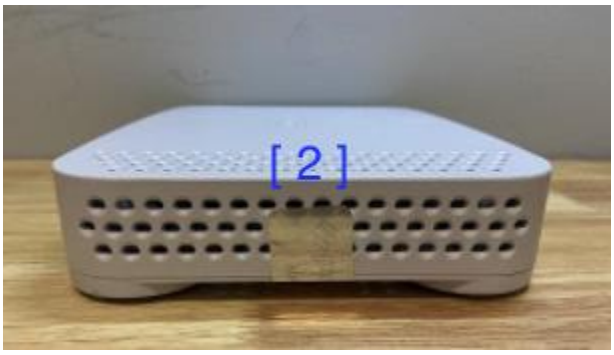

Figure 11 – ION 1200 Right View (same for all models)

Figure 12 – ION 1200 Top View

Figure 13 – ION 1200 Rear View

Figure 14 – ION 1200-C-5G-WW/ION 1200-C-NA/ION 1200-C-ROW Top View

Figure 15 – ION 1200 Bottom View

Figure 16 – ION 1200-C-5G-WW/ION 1200-C-NA/ION 1200-C-ROW Bottom View

ION 9000 Physical Security

The following section demonstrates how to apply the tamper evident labels to the ION 9000 module. The module requires a total of six tamper evident labels. The figures below detail the location of the labels.

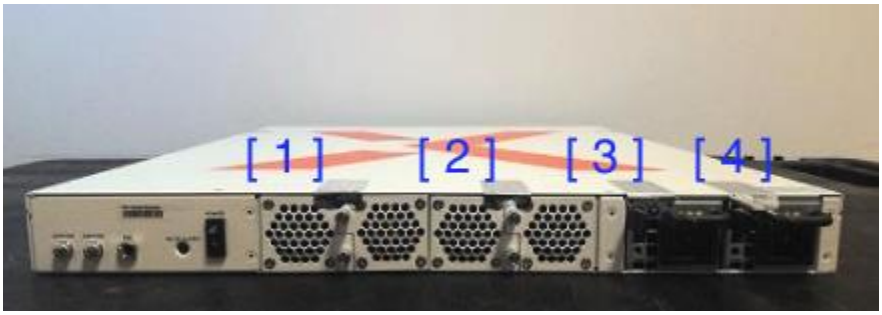

Figure 17 – Rear view of ION 9000

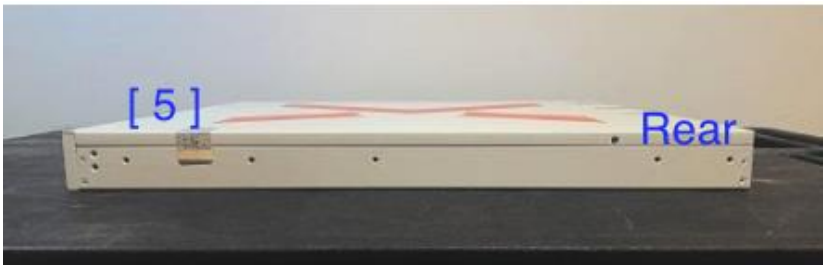

Figure 18 – Left side view of ION 9000

Figure 19 – Right side view of ION 9000


Figure 20 – Front side view of ION 9000


Figure 21 – Top side view of ION 9000

Figure 22 – Bottom side view of ION 9000

Non-Invasive Security

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

Sensitive Security Parameters

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import/ Export	Establishment	Storage	Zeroization	Use & Related Keys
Non-Protocol Related SSPs								
DRBG Entropy Input (CSP)	384 bits	N/A	Generated from noise source	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used to seed the DRBG
DRBG Seed, Internal State V value, and DRBG Key (CSP)	256 bits	N/A	Internally Derived from entropy input string as defined by SP800-90Arev1	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used DRBG generation.
Crypto Officer Authentication RSA Public Key (PSP)	2048 bits	RSA SigVer SHA-1; SHA2-256 RSA Certs. #1819, #1820, and C170 SHS Cert. #2919, #2920 and C170	Pre-loaded at the factory	Import: No Export: No	N/A	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: Encrypted by using TLS/SSH session key Export: No	MD/EE	HDD (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used for User authentication
TLS Protocol SSPs								
TLS RSA Private Key (CSP)	2048 bits	CKG DRBG RSA KeyGen; RSA SigGen Cert# A2386	Internally generated conformant to SP800-133rev2 (CKG) using FIPS 186-4 RSA/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)	2048 bits	RSA KeyGen; RSASigVer; Cert# A2386	Internally derived per the FIPS 186-4 RSA key generation method	Import: No Export: to the TLS Peer application	N/A	HDD (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used for TLS peer authentication
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)	Zeroized by SSP (CSP/PSP) Zeroization Command	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)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used to derive TLS Encryption Keys, TLS Authentication Keys
TLS ECDHE Private Key (CSP)	P-256, P-384, P-521	CKG DRBG KAS-ECC-SSC Cert. #A2386	Internally generated conformant to SP800-133rev2 (CKG) using SP800-56Arev3 EC	Import: No 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	Establishment	Storage	Zeroization	Use & Related Keys
			Diffie-Hellman key generation method, and the random value used in key generation is generated using SP800-90Arev1 DRBG					
TLS ECDHE Public key (PSP)	P-256, P-384, P-521	CKG DRBG KAS-ECC-SSC Cert. #A2386	Internally derived internally per the EC Diffie-Hellman key agreement (SP800-56Arev3)	Import: No Export: to the TLS Peer application	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used to derive TLS ECDHE Shared Secret
TLS ECDHE Shared Secret (CSP)	P-256, P-384, P-521	CKG DRBG KAS-ECC-SSC KAS (ECC) Cert. #A2386	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 TLS Session Encryption Keys, TLS Session Authentication Keys.
TLS Session Encryption Key (CSP)	128 or 256 bits	AES-CBC; AES-GCM; CVL (TLS KDF) KTS; Cert. #A2385 AES-CBC; Cert. #A2387	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)	256 -512 bits	HMAC-SHA2-256; HMAC-SHA2-384; CVL (TLS KDF) KTS; Cert. #A2386 HMAC-SHA2-256; HMAC-SHA2-384; Cert. #A2387	Internally derived via key derivation function defined in SP800-135rev1 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/IKEv2 Protocol SSPs								
IPSec 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 Keys (CSP)	2048, 3072 bits	CKG; DRBG; RSA SigGen Cert# A2385	Internally generated conformant to SP800-133rev2 (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 Keys (PSP)	2048, 3072 bits	CKG; DRBG; RSA SigVer Cert# A2385	Internally derived per the FIPS 186-4 RSA key generation method	Import: No Export: to the IKE Peer application	N/A	HDD (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used for IPSec/IKE peer authentication
IPSec/IKE ECDHE Private Key (CSP)	P-256 or P-384	CKG; DRBG; KAS-ECC-SSC Cert. #A2385	Internally generated conformant to SP800-133rev2 (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)	P-256 or P-38	CKG; DRBG; KAS-ECC-SSC Cert. #A2385	Internally derived internally per the EC Diffie-Hellman key agreement (SP800-56Arev3)	Import: No Export: to the IKE Peer application	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)	P-256 or P-384	CKG; DRBG; KAS-ECC-SSC Cert. #A2385	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 IPSec/IKE Session Encryption Keys, IPSec/IKE Authentication Keys
IPSec/IKE Session Encryption Key (CSP)	128, 192, or 256 bits	AES-CBC; CVL (IKEv2 KDF) Certs. #A2385 and #A2385; AES-CBC; Cert. #A2388	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,
IPSec/IKE Session Authentication Key	160 -512 bits	HMAC-SHA-1; HMAC-SHA2-256;	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

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import/ Export	Establishment	Storage	Zeroization	Use & Related Keys
(CSP)		HMAC-SHA2-384; HMAC-SHA2-512; CVL (IKEv2 KDF) Cert. #A2385 HMAC-SHA-1; HMAC-SHA2-256; HMAC-SHA2-384; HMAC-SHA2-512 Cert. #A2388						
SNMPv3 Protocol SSPs								
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; CVL (SNMPv3 KDF) Cert. #A2385	Internally derived via key derivation function defined in SP800-135rev1 KDF (SNMPv3)	Import: No Export: No	N/A	HDD (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used to secure SNMPv3 session confidentiality
SNMPv3 Session Authentication Key (CSP)	160 bits	HMAC-SHA-1; CVL (SNMPv3 KDF) Cert. #A2385	Internally derived via key derivation function defined in SP800-135rev1 KDF (SNMPv3)	Import: No Export: No	N/A	HDD (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used to secure SNMPv3 session integrity
SSHv2 Protocol SSPs								
SSH ECDHE Private Key (CSP)	P-256, P-384, or P-521	CKG; DRBG; KAS-ECC-SSC Cert. #A2385	Internally generated conformant to SP800-133rev2 (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	CKG; DRBG; KAS-ECC-SSC Cert. #A2385	Internally derived internally per the EC Diffie-Hellman key agreement (SP800-56Arev3)	Import: No Export: to the SSH Peer application	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used to derive the SSH ECDHE Shared Secret
SSH ECDHE Shared Secret (CSP)	P-256, P-384, or P-521	CKG; DRBG; KAS-ECC-SSC Cert. #A2385	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 Host Private Key (CSP)	P-256, P-384, or P-521	CKG; DRBG; ECDSA KeyGen; ECDSa KeyVer ECDSA SigGen Cert. #A2385	Internally generated conformant to SP800-133rev2 (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 Host Public Key (PSP)	P-256, P-384, or P-521	CKG; DRBG; ECDSA KeyGen; ECDSA KeyVer; ECDSA SigVer Cert. #A2385	Internally derived per the FIPS 186-4 ECDSA key generation method	Import: No Export: to the SSH Peer application	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; KTS; CVL (SSH KDF) Cert. #A2385	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)	160 -512 bits	HMAC-SHA-1; HMAC-SHA2-256; HMAC-SHA2-512; CVL (SSH KDF) KTS Cert. #A2385	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 integrity protection

Table 17 - 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.

RBG Entropy Source (s)

Entropy Source (s)	Minimum Number of Bits of Entropy	Details
ENT (P) Intel CPU with RDSEED Hardware entropy source	256 bits	Entropy provided by Intel's CPU with RDSEED as the noise source and the Linux Kernel (/dev/random) as the conditioner to provide at least 256 bits of the entropy to seed each DRBG (Cert. #A2385 and Cert. #A2386). The SHA-1 as a vetted conditioner used in Linux Kernel has been ACVP tested with the SHS Cert. #A2387.

Table 18 - Non-Deterministic Random Number Generation Specification

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 19 - 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
CTR_DRBG	KAT: CTR_DRBG 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)
SHS	KAT using SHA-1
SHS	KAT using SHA2-224
SHS	KAT using SHA2-256
SHS	KAT using SHA2-384

Algorithm	Self-Test Details
SHS	KAT using SHA2-512
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
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)
KAS-ECC-SSC	KAT for KAS-ECC-SSC (Shared Secret Computation) primitive Z value
IKEv2 KDF	KAT for IKEv2 KDF
SSH KDF	KAT for SSHv2 KDF
TLS KDF	KAT for TLSv1.2 KDF

Table 20 –Crypto Library I CASTs

Algorithm	Self-Test Details
SP800-90Arev1 DRBG	KAT: HMAC_DRBG (SHA2-512) KAT: Instantiate KAT: Generate KAT: Reseed
SHS	KAT using SHA-1
HMAC	KAT using SHA2-224
HMAC	KAT using SHA2-256
HMAC	KAT using SHA2-384
HMAC	KAT using SHA2-512
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
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_DRBG	KAT: CTR_DRBG KAT: Instantiate KAT: Generate KAT: Reseed *Note: DRBG Health Tests as specified in SP800-90Arev1 Section 11.3 are performed)*
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)
KAS-ECC-SSC	KAT for KAS-ECC-SSC (Shared Secret Computation) primitive Z value
TLS KDF	KAT for TLSv1.2 KDF

Table 21 –Crypto Library II CASTs

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 SHA2-512
SHS	KAT using SHA2-256
SHS	KAT using SHA2-384
SHS	KAT using SHA2-512

Table 22 –Crypto Library III and IV CASTs

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

Table 23 – Crypto Library V CASTs

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 24 - Crypto Library I Conditional Pair-Wise Consistency Tests

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 25 - Crypto Library II Conditional Pair-Wise Consistency Tests

Conditional Firmware Load Test

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

Table 26 - Crypto Library I Conditional Firmware Load Test

Entropy Source Health-Tests

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 27 - Entropy Source Health Tests

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 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 28 - Error State Indicators

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
- 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, and only includes an Approved mode of operation. Once the module has been received, the Crypto Officer shall follow the secure operations provided below to place the module in the Approved mode. The module runs firmware version 5.6.3. 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 device
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
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 displays 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 password change for the Crypto Officer. Any non-approved configurations/algorithms are rejected automatically by the module and an error message is output.

The Crypto Officer shall load the FIPS 140-3 validated firmware only to maintain validation.

End of Life / Sanitization

End of life dates for software and hardware 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

Administrator/User Guidance

Palo Alto Networks provides documentation for all products, which can be accessed here:

https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/prisma/prisma-sd-wan/prisma-sd-wan-admin/prisma-sd-wan-admin.pdf

The ION devices include the following Administrator's Guide that shall be used by the Crypto Officer:

Prisma SD-WAN Administrator’s Guide (Revision Date: September 14, 2021)

Mitigation of Other Attacks

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