Palo Alto Networks, Inc.

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

FIPS 140-3 Non-Proprietary Security Policy

Palo Alto Networks, Inc.
www.paloaltonetworks.com

Revision Date: March 17, 2026
Document Version: 1.0

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

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 3200H, ION 5200, and ION 9200 (hereinafter referred to as the Module or ION module).

1.2 Security Levels

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
	Overall Level	2

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

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.

Module Type: Hardware

Module Embodiment: Multi-Chip Standalone

Cryptographic Boundary:

The 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. These modules are described in more detail further below in this section.

Tested Operational Environment's Physical Perimeter (TOEPP):

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

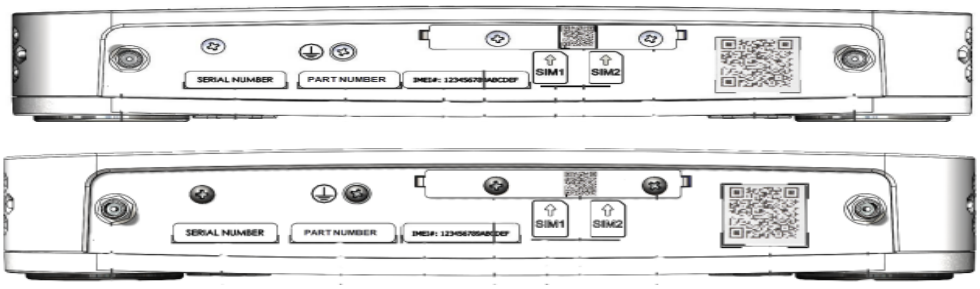

Figure 4 - ION 1200 (Top), ION 1200-C-NA/ION 1200-C-ROW (Middle), and ION 1200-C-5G-WW (Bottom) Rear Interfaces

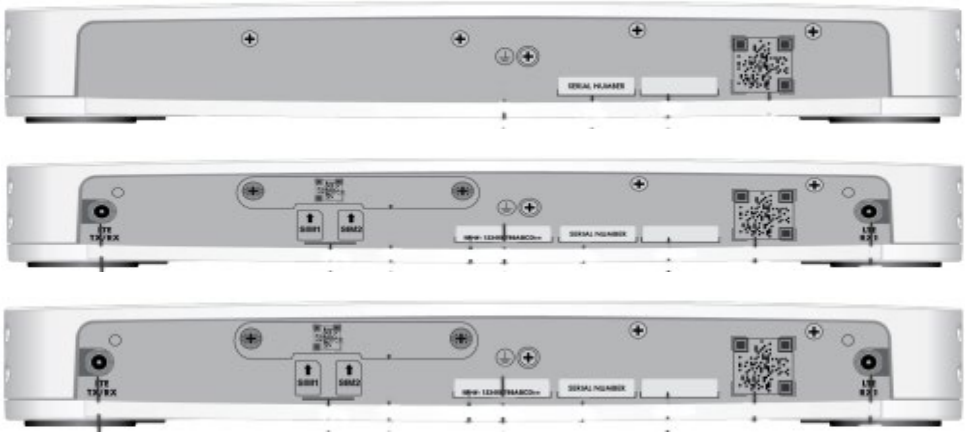

Figure 5 - ION 1200-S (Top), ION 1200-S-C-NA/ION 1200-S-C-ROW (Middle), and ION 1200-S-C-5G-WW (Bottom) Rear Interfaces

Figure 6 - ION 3200 Front Interfaces

Figure 7 - ION 3200 Rear Interfaces

Figure 8 - ION 3200H Front Interfaces

Figure 9 - ION 3200H-C5G-WW Front Interfaces

Figure 10 - ION 3200H/ION 3200H-C5G-WW Rear Interfaces

Figure 11 - ION 5200 Front Interfaces

Figure 12 - ION 5200 Rear Interfaces

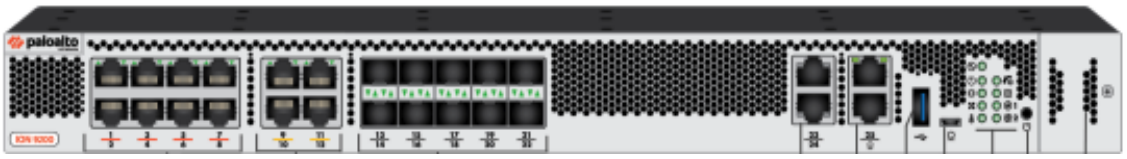

Figure 13 - ION 9200 Front Interfaces

Figure 14 - ION 9200 Rear Interfaces

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
ION 1200	ION 1200	6.4.2	Intel Atom C3436L	LEDs, Console, Ethernet, Uplink, Power
ION 1200-C-NA	ION 1200-C-NA	6.4.2	Intel Atom C3436L	LEDs, Console, Ethernet, Uplink Connector, Power
ION 1200-C-ROW	ION 1200-C-ROW	6.4.2	Intel Atom C3436L	LEDs, Console, Ethernet, Uplink Connector, Power
ION 1200-C-5G-WW	ION 1200-C-5G-WW	6.4.2	Intel Atom C3436L	LEDs, Console, Ethernet, Uplink Connector, Power
ION 1200-S	ION 1200-S	6.4.2	Intel Atom C3436L	Console, Micro USB, SFP/RJ-45 Combo, ByPass Pair, Ethernet Ports, LEDs, Power
ION 1200-S-C-NA	ION 1200-S-C-NA	6.4.2	Intel Atom C3436L	Console, Micro USB, SFP/RJ-45 Combo, ByPass Pair, Ethernet Ports, LEDs, Power, Uplink Connector
ION 1200-S-C-ROW	ION 1200-S-C-ROW	6.4.2	Intel Atom C3436L	Console, Micro USB, SFP/RJ-45 Combo, ByPass Pair, Ethernet Ports, LEDs, Power, Uplink Connector
ION 1200-S-C5G-WW	ION 1200-S-C5G-WW	6.4.2	Intel Atom C3436L	Console, Micro USB, SFP/RJ-45 Combo, ByPass Pair, Ethernet Ports, LEDs, Power, Uplink Connector
ION 3200	ION 3200	6.4.2	Intel Atom C3558R	Console, Micro USB, SFP / RJ-45 Combo Port, ByPass Pair, Ethernet or PoE, LEDs, Power
ION 3200H	ION 3200H	6.4.2	Intel Atom C3708	Console, Micro USB, SFP / RJ-45 Combo Port, ByPass Pair, Ethernet, LEDs, Power
ION 3200H-C5G-WW	ION 3200H-C5G-WW	6.4.2	Intel Atom C3708	Console, Micro USB, SFP / RJ-45 Combo Port, ByPass Pair, Ethernet, LEDs, Power
ION 5200	ION 5200	6.4.2	Intel Atom C5325	ByPass Pair, PoE, SFP+, Ethernet, Console, Micro USB, LEDs, Power
ION 9200	ION 9200	6.4.2	Intel Atom P5362	ByPass Pair, PoE, SFP+, Ethernet, Console, Micro USB, LEDs, Power

Table 2: Tested Module Identification – Hardware

Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets):

N/A for this module.

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

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

N/A for this module.

2.3 Excluded Components

N/A for this module.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved Mode	The module has one approved mode of operation and is always in approved mode after initialization	Approved	"Device Mode: fips" output via the status output interface upon entering the Approved Mode after initialization

Table 3: Modes List and Description

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.

2.5 Algorithms

Approved Algorithms:

Crypto Library - I

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A6185	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB128	A6185	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CTR	A6185	Direction - Decrypt, Encrypt Key Length - 128, 192, 256 Payload Length - Payload Length: 128 Supports Counter larger than maximum value - No Incremental Counter - Yes Counter Tests Performed - Yes	SP 800-38A
AES-GCM	A6185	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256 Tag Length - 104, 112, 120, 128, 32, 64, 96 IV Length - IV Length: 96, 1024	SP 800-38D

Algorithm	CAVP Cert	Properties	Reference
		Payload Length - Payload Length: 504-1024 Increment 8 AAD Length - AAD Length: 0-1024 Increment 8	
Counter DRBG	A6185	Prediction Resistance - No, Yes Mode - AES-128, AES-192, AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-5)	A6185	Curve - P-256, P-384, P-521 Secret Generation Mode - extra bits, testing candidates	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A6185	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512 Component - No	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A6185	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	FIPS 186-5
HMAC-SHA-1	A6185	MAC - MAC: 80-160 Increment 8 Key Length - Key Length: 256-1120 Increment 8	FIPS 198-1
HMAC-SHA2-256	A6185	MAC - MAC: 128-256 Increment 8 Key Length - Key Length: 256-1120 Increment 8	FIPS 198-1
HMAC-SHA2-384	A6185	MAC - MAC: 192-384 Increment 8 Key Length - Key Length: 256-1120 Increment 8	FIPS 198-1
HMAC-SHA2-512	A6185	MAC - MAC: 256-512 Increment 8 Key Length - Key Length: 256-1120 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A6185	Domain Parameter Generation Methods - P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDF IKEv2 (CVL)	A6185	Initiator Nonce Length - Initiator Nonce Length: 512 Responder Nonce Length - Responder Nonce Length: 512 Diffie-Hellman Shared Secret Length - Diffie-Hellman Shared Secret Length: 2048 Derived Keying Material Length - Derived Keying Material Length: 1056-3072 Increment 8 Hash Algorithm - SHA-1, SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
KDF SNMP (CVL)	A6185	Password Length - Password Length: 64, 2048 Engine ID - 00100020003000400050, 12345678901234567890	SP 800-135 Rev. 1
KDF SSH (CVL)	A6185	Cipher - AES-128, AES-192, AES-256 Hash Algorithm - SHA-1, SHA2-256, SHA2-512	SP 800-135 Rev. 1
RSA KeyGen (FIPS186-5)	A6185	Key Generation Mode - probable Modulo - 2048, 3072 Primality Tests - 2powSecStr Info Generated By Server - No Private Key Format - standard Public Exponent Mode - random	FIPS 186-5
RSA SigGen (FIPS186-5)	A6185	Modulo - 2048, 3072 Signature Type - pkcs1v1.5, pss	FIPS 186-5

Algorithm	CAVP Cert	Properties	Reference
RSA SigVer (FIPS186-5)	A6185	Hash Pair - Hash Algorithm - SHA2-512 Modulo - 2048, 3072 Signature Type - pkcs1v1.5, pss Mask Function - mgf1 Public Exponent Mode - random	FIPS 186-5
SHA-1	A6185	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4
SHA2-256	A6185	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4
SHA2-384	A6185	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4
SHA2-512	A6185	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4
TLS v1.2 KDF RFC7627 (CVL)	A6185	Hash Algorithm - SHA2-256, SHA2-384, SHA2-512 Key Block Length - Key Block Length: 1024	SP 800-135 Rev. 1

Table 4: Approved Algorithms - Crypto Library - I

Crypto Library - II

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A6186	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38A
AES-GCM	A6186	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 128, 256 Tag Length - 128 IV Length - IV Length: 96, 1024 Payload Length - Payload Length: 64-256 Increment 8 AAD Length - AAD Length: 0, 256	SP 800-38D
Counter DRBG	A6186	Prediction Resistance - No Supports Reseed - Yes Mode - AES-256 Derivation Function Enabled - No Additional Input - Additional Input: 0-384 Increment 16 Entropy Input - Entropy Input: 384 Nonce - Nonce: 0 Personalization String Length - Personalization String Length: 0-384 Increment 16 Returned Bits - 2048	SP 800-90A Rev. 1
HMAC-SHA2-256	A6186	MAC - MAC: 128-256 Increment 8 Key Length - Key Length: 256-1120 Increment 8	FIPS 198-1
HMAC-SHA2-384	A6186	MAC - MAC: 192-384 Increment 8 Key Length - Key Length: 256-1120 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A6186	Domain Parameter Generation Methods - P-256, P-384, P-521 Scheme -	SP 800-56A Rev. 3

Algorithm	CAVP Cert	Properties	Reference
		ephemeralUnified - KAS Role - initiator, responder	
RSA SigVer (FIPS186-5)	A6186	Hash Pair - Hash Algorithm - SHA2-224 Modulo - 2048 Signature Type - pkcs1v1.5 Public Exponent Mode - random	FIPS 186-5
SHA2-256	A6186	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4
SHA2-384	A6186	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4
TLS v1.2 KDF RFC7627 (CVL)	A6186	Hash Algorithm - SHA2-256, SHA2-384 Key Block Length - Key Block Length: 1024	SP 800-135 Rev. 1

Table 5: Approved Algorithms - Crypto Library - II

Crypto Library - IV

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A6188	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38A
HMAC-SHA2-256	A6188	MAC - MAC: 128-256 Increment 8 Key Length - Key Length: 256-1120 Increment 8	FIPS 198-1
HMAC-SHA2-384	A6188	MAC - MAC: 192-384 Increment 8 Key Length - Key Length: 256-1120 Increment 8	FIPS 198-1
HMAC-SHA2-512	A6188	MAC - MAC: 256-512 Increment 8 Key Length - Key Length: 256-1120 Increment 8	FIPS 198-1
SHA2-256	A6188	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4
SHA2-384	A6188	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4
SHA2-512	A6188	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4

Table 6: Approved Algorithms - Crypto Library - IV

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG	Key Type:Asymmetric	N/A	SP 800-133r2 Section 4, example 1

Table 7: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

N/A for this module.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
KAS-ECC-KeyGen (SSH)	CKG KAS-KeyGen	KAS ECC keygen used in SSHv2 service	Bit-strength Caveat:Provides between 128 and 256 bits of encryption strength	Counter DRBG: (A6185) CKG: ()
KAS-ECC-KeyGen (TLSv1.2)	CKG KAS-KeyGen	KAS ECC keygen used in TLSv1.2 service	Bit-strength Caveat:Provides between 128 and 256 bits of encryption strength	Counter DRBG: (A6185, A6186) CKG: () Key Type: Asymmetric
KAS-ECC-KeyGen (IPSec/IKE)	CKG KAS-KeyGen	KAS ECC keygen used in IPSec/IKEv2 service	Bit-strength Caveat:Provides between 128 and 192 bits of encryption strength	Counter DRBG: (A6185) CKG: ()
KAS-ECC (SSH)	KAS-Full	Full KAS-ECC Key Agreement used for SSHv2 service	IG:IG D.F Scenario 2, path(2), split Key confirmation:no Key derivation:IG 2.4.B SP 800-135rev1 CVL Caveat:Key establishment methodology provides between 128 and 256 bits of security strength	KAS-ECC-SSC Sp800-56Ar3: (A6185) KDF SSH: (A6185)
KAS-ECC (TLSv1.2)	KAS-Full	Full KAS-ECC Key Agreement used for TLSv1.2 service	IG:IG D.F Scenario 2, path (2), split Key confirmation:no Key derivation:IG 2.4.B SP 800-135rev1 CVL Caveat:Key	KAS-ECC-SSC Sp800-56Ar3: (A6186, A6185) TLS v1.2 KDF RFC7627: (A6186, A6185)

Name	Type	Description	Properties	Algorithms
			establishment methodology provides between 128 and 256 bits of security strength	
KAS-ECC (IPSec/IKE)	KAS-Full	Full KAS-ECC Key Agreement used for IPSec/IKEv2 service	IG:IG D.F Scenario 2, path (2), split Key confirmation:no Key derivation:IG 2.4.B SP 800-135rev1 CVL Caveat:Key establishment methodology provides between 128 and 192 bits of encryption strength	KAS-ECC-SSC Sp800-56Ar3: (A6185) Domain Parameter Generation Methods: P-256, P-384 KDF IKEv2: (A6185)
KTS (TLSv1.2 with AES and HMAC)	KTS-Unwrap	KTS via TLSv1.2 service by using AES and HMAC	Standard:SP 800-38F IG D.G:"Combination" method - approved symmetric encryption method together with an approved authentication method Caveat:Key establishment methodology provides between 128 and 256 bits of security strength	AES-CBC: (A6186) HMAC-SHA2-256: (A6186) HMAC-SHA2-384: (A6186) SHA2-256: (A6186) SHA2-384: (A6186)
KTS (TLSv1.2 with AES-GCM)	KTS-Unwrap	KTS via TLSv1.2 service by using AES-GCM	Standard:SP 800-38F IG D.G:approved authenticated symmetric encryption mode Caveat:Key establishment methodology provides between 128 and 256 bits of security strength	AES-GCM: (A6186)

Name	Type	Description	Properties	Algorithms
SSH ECDSA KeyGen	CKG AsymKeyPair-KeyGen	ECDSA KeyGen for SSHv2		ECDSA KeyGen (FIPS186-5): (A6185) Counter DRBG: (A6185) CKG: ()
SSH ECDSA SigGen	DigSig-SigGen	ECDSA SigGen for SSHv2		ECDSA SigGen (FIPS186-5): (A6185)
SSH ECDSA SigVer	DigSig-SigVer	ECDSA SigVer for SSHv2		ECDSA SigVer (FIPS186-5): (A6185)
TLS RSA KeyGen	CKG AsymKeyPair-KeyGen	RSA KeyGen for TLSv1.2		RSA KeyGen (FIPS186-5): (A6185) Counter DRBG: (A6185) CKG: ()
TLS RSA SigGen	DigSig-SigGen	RSA SigGen for TLSv1.2		RSA SigGen (FIPS186-5): (A6185)
TLS RSA SigVer	DigSig-SigVer	RSA SigVer for TLSv1.2		RSA SigVer (FIPS186-5): (A6186, A6185)
IPSec/IKE RSA KeyGen	CKG AsymKeyPair-KeyGen	RSA KeyGen for IPSec/IKEv2		RSA KeyGen (FIPS186-5): (A6185) Counter DRBG: (A6185) CKG: ()
IPSec/IKE RSA SigGen	DigSig-SigGen	RSA SigGen for IPSec/IKEv2		RSA SigGen (FIPS186-5): (A6185)
IPSec/IKE RSA SigVer	DigSig-SigVer	RSA SigVer for IPSec/IKEv2		RSA SigVer (FIPS186-5): (A6185)
Session Encryption/Decryption (SSH)	BC-UnAuth	SSHv2 session protection		AES-CTR: (A6185)
Session Encryption/Decryption (TLSv1.2)	BC-Auth BC-UnAuth	TLSv1.2 session protection		AES-CBC: (A6186, A6185) AES-GCM: (A6186, A6185)
Session Encryption/Decryption (IPSec/IKE)	BC-UnAuth	IPSec/IKE session protection		AES-CBC: (A6188, A6185)
Session Encryption/Decryption (SNMPv3)	BC-UnAuth	SNMPv3 session protection		AES-CFB128: (A6185)
Session Authentication (SSHv2)	MAC	SSHv2 session authentication		HMAC-SHA-1: (A6185) HMAC-SHA2-

Name	Type	Description	Properties	Algorithms
				256: (A6185) HMAC-SHA2-512: (A6185) SHA-1: (A6185) SHA2-256: (A6185) SHA2-512: (A6185)
Session Authentication (TLSv1.2)	MAC	TLSv1.2 session authentication		HMAC-SHA2-256: (A6186, A6185) HMAC-SHA2-384: (A6186, A6185) SHA2-256: (A6186, A6185) SHA2-384: (A6186, A6185)
Session Authentication (IPSec/IKE)	MAC	IPSec/IKE session authentication		HMAC-SHA-1: (A6185) HMAC-SHA2-256: (A6188, A6185) HMAC-SHA2-384: (A6188, A6185) HMAC-SHA2-512: (A6188, A6185) SHA-1: (A6185) SHA2-256: (A6188, A6185) SHA2-384: (A6188, A6185) SHA2-512: (A6188, A6185)
Session Authentication (SMPv3)	MAC	SNMPv3 session authentication		HMAC-SHA-1: (A6185) SHA-1: (A6185)
SSHv2 Keying Materials Development	KAS-135KDF	SSHv2 session keying materials, used to derive SSHv2 session keys.		KDF SSH: (A6185)
TLSv1.2 Keying Materials Development	KAS-135KDF	TLSv1.2 session keying materials, used to derive TLSv1.2 session keys		TLS v1.2 KDF RFC7627: (A6186, A6185)
IPSec/IKE Keying Materials Development	KAS-135KDF	IPSec/IKE session keying materials, used to derive		KDF IKEv2: (A6185)

Name	Type	Description	Properties	Algorithms
		IPSec/IKE session keys		
SNMPv3 Keying Materials Development	KAS-135KDF	SNMPv3 session keying materials, used to derive SNMPv3 session keys		KDF SNMP: (A6185)
Firmware Load Test	DigSig-SigVer	Signature verification for firmware load test		RSA SigVer (FIPS186-5): (A6185) SHA2-256: (A6185)
DRBG Function	DRBG	Used for DRBG generation		Counter DRBG: (A6185, A6186)

Table 8: Security Function Implementations

2.7 Algorithm Specific Information

AES-GCM

- 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 SP800-52 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. The keys for the client and server negotiated in the TLSv1.2 handshake process (client_write_key and server_write_key) are compared and the module aborts the session if the key values are identical. In case the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established.

- The module uses RFC 7296 compliant IKEv2 to establish the shared secret SKEYSEED from which the AES GCM encryption keys are derived. The operations of one of the two parties involved in the IKE key establishment scheme shall be performed entirely within the cryptographic boundary of the module being validated. 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. Two keys established by IKEv2 for one security association (one key for encryption in each direction between the parties) are not identical and abort the session if they are. 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.

SHA-1

- The module implements SHA-1 for use in non-digital-signature applications.

As the module can only be operated in the Approved mode of operation, any algorithms not listed above will be rejected by the module while in the approved mode.

2.8 RBG and Entropy

Cert Number	Vendor Name
E68	Palo Alto Networks, Inc.
E71	Palo Alto Networks, Inc.

Table 9: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Palo Alto Networks DRNG Entropy Source - Denverton 16 Core Die with FCBGA1310 Package	Physical	Intel Atom C3436L, Intel Atom C3558R, Intel Atom C3708	128 bits	Full Entropy	A2153 (AES-CBC-MAC)
Palo Alto Networks DRNG Entropy Source - Snow Ridge 24-Core Die with FCBGA2106 Package	Physical	Intel Atom C5325, Intel Atom P5362	128 bits	Full Entropy	A2541 (AES-CBC-MAC)

Table 10: Entropy Sources

The operational environment is detailed in the Public Use Document for Entropy Certificate E68 and E71. The “Palo Alto Networks DRNG Entropy Source” is described as a feedback stabilized metastable latch that provides 128 bits of full entropy per sample. The entropy source is called multiple times in order to seed the DRBGs.

The module implements two approved DRBGs based on SP800-90Arev1, including CTR_DRBG with Algo Cert. #A6185, and CTR_DRBG with Algo Cert. #A6186. Those two DRBGs are used internally by the module (e.g. to generate seeds for asymmetric key pairs, and random numbers for security functions).

Each DRBG is seeded by the entropy source described in the table above. The module implements CTR_DRBG (Cert. #A6185) with Derivation Function and CTR_DRBG (Cert. #A6186) without Derivation Function capability. Given that the module’s entropy source provides full entropy, CTR_DRBG without a derivation function is compliant with IG D.L. Each DRBG is instantiated with a 384-bits long entropy input (corresponding to 384 bits of entropy) and provides at least 256 bits security strength for the cryptographic key generation while in the approved mode.

Note:

- ESV Cert. #E68 is for validated entropy source running on each of 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, ION 3200, ION 3200H, and ION 3200H-C5G-WW tested platforms
- ESV Cert. #E71 is for validated entropy source running on each of ION 5200 and ION 9200 tested platforms

2.9 Key Generation

The module generates RSA, ECDSA, and ECDH asymmetric key pairs compliant with FIPS 186-5, using a NIST SP 800-90Ar1 CTR DRBG for random number generation. In accordance with FIPS 140-3 IG D.H, the cryptographic module performs CKG for asymmetric keys as per section 5.1 of NIST SP 800-133rev2 (vendor affirmed) by obtaining a random bit string directly from an approved DRBG. The random bit string supports the required security strength requested by the calling application (without any V, as described in Additional Comments 2 of IG D.H.).

2.10 Key Establishment

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

KAS-ECC Shared Secret Computation:

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

2.11 Industry Protocols

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

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
Ethernet, PoE, SFP+, SFP/RJ-45 Combo port, 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 TLS v1.2, SSHv2, IPSec/IKEv2, and SNMPv3 service data
Ethernet, PoE, SFP+, SFP/RJ-45 Combo port, 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 TLS v1.2, SSHv2, IPSec/IKEv2, and SNMPv3 service data
Ethernet, PoE, SFP+, SFP/RJ-45 Combo port, SFP+/RJ-45 Combo port, and Uplink Connector	Control Input	Control Data input into the module for all the services defined in Approved Services Table, including TLS v1.2, SSHv2, IPSec/IKEv2, and SNMPv3 service data
N/A	Control Output	N/A
Console, Ethernet, PoE, SFP+, SFP/RJ-45 Combo port, SFP+/RJ-45 Combo port, ByPass Pair, Uplink Connector and LEDs	Status Output	Status information output from the module

Physical Port	Logical Interface(s)	Data That Passes
Power	Power	Provide the power supply to the module

Table 11: Ports and 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 table above.

Notes:

1. All USB ports on each module are functionally disabled
2. The “Bypass Pair” interfaces do not perform the Bypass service

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
RSA-Based Certificate	The modules support RSA public-key based authentication mechanism using a minimum of RSA 2048 bits	RSA SigVer (FIPS186-5) (A6185)	With a minimum modulus size of 2048, 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.
Password/Pre-shared Secret	The minimum length is eight (8) characters (94 possible characters). The configuration supports at most three failed attempts to authenticate in a one-minute period.	Password Based	The probability that a random attempt will succeed or a false acceptance will occur is 1/(94^8) which is less than 1/1,000,000. 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	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.

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
			characters to choose from in total.	

Table 12: Authentication Methods

The modules all support role-based authentication, and provide the Crypto Officer role and the User role.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Role	CO	RSA-Based Certificate
User	Role	User	Password/Pre-shared Secret

Table 13: Roles

The Crypto Officer role has the ability to perform all tasks and administrative actions while the User is read-only.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Self-Test	Initiate and run the pre-operational self-tests	None	Command to trigger self-test	Status of the self-test results	None	Crypto Officer - Firmware Integrity Test Key: E User - Firmware Integrity Test Key: E Unauthenticated - Firmware Integrity Test Key: E
Zeroization	Zeroize all unprotected SSPs stored in the module	None	Command to initiate the SSPs zeroization	Status of the SSPs zeroization	None	Crypto Officer - DRBG Entropy Input (A6185): Z - DRBG Seed (A6185): Z - DRBG Internal State V value (A6185): Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- DRBG Key (A6185): Z - DRBG Entropy Input (A6186): Z - DRBG Seed (A6186): Z - DRBG Internal State V value (A6186): Z - DRBG Key (A6186): Z - User Password: Z - Crypto Officer Authentication RSA Public Key: Z - TLS RSA Private Key: Z - TLS RSA Public Key: Z - TLS ECDHE Private Key: Z - TLS ECDHE Public Key: Z - Peer TLS ECDHE Public Key: Z - TLS ECDHE Shared Secret: Z - TLS RSA Pre-Master Secret: Z - TLS Master Secret: Z - TLS Session Encryption Key: Z - TLS Session

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Authentication Key: Z - IPSec/IKE Pre-Shared Secret: Z - IPSec/IKE RSA Private Key: Z - IPSec/IKE RSA Public Key: Z - IPSec/IKE ECDHE Private Key: Z - IPSec/IKE ECDHE Public Key: Z - Peer IPSec/IKE ECDHE Public Key: Z - IPSec/IKE ECDHE Shared Secret: Z - SKEYSEED: Z - IPSec/IKE Session Encryption Key: Z - IPSec/IKE Session Authentication Key: Z - SNMPv3 Authentication Secret: Z - SNMPv3 Session Encryption Key: Z - SNMPv3 Session Authentication Key: Z - SSH ECDHE Private Key: Z - SSH

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						ECDHE Public Key: Z - Peer SSH ECDHE Public Key: Z - SSH ECDHE Shared Secret: Z - SSH ECDSA Private Key: Z - SSH ECDSA Public Key: Z - SSH Session Encryption Key: Z - SSH Session Authentication Key: Z
Firmware Update	The module's firmware is updated to a new version	Approved Mode Indicator and successful Firmware update completion system log message	Command to upload a new validated firmware	Status of the updated firmware installation	Firmware Load Test	Crypto Officer - Firmware Load Test Key: E
Crypto Officer Role Authentication	Crypto Officer Role Authentication	Approved Mode Indicator and CO role successful authentication system log message	Crypto Officer role authentication request	Status of Crypto Officer role authentication	None	Crypto Officer - Crypto Officer Authentication RSA Public Key: E
User Role Authentication	User Role Authentication	Approved Mode Indicator and User role successful authentication system	User role authentication request	Status of User role authentication	None	User - User Password: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		log message				
Show Version	Provides the module's name/ID and versions	None	Command to show version	Module's name/ID and versions	None	Crypto Officer
Show Status	Provides the module's current status and information	None	Command to show status	Module's status information	None	Crypto Officer User
Configure Network	Perform the module's network configuration	Approved Mode Indicator and successful network configuration system log message	Commands to configure the module	Status of the completion of network related configuration	None	Crypto Officer
Configure SSHv2 Function	Create a secure SSHv2 channel	Approved Mode Indicator and successful SSHv2 configuration system log message	Commands to configure SSHv2	Status of the completion of SSHv2 configuration	SSH ECDSA KeyGen DRBG Function	Crypto Officer - SSH ECDSA Private Key: G,W - SSH ECDSA Public Key: G,W - DRBG Entropy Input (A6185): E - DRBG Seed (A6185): E - DRBG Internal State V value (A6185): E - DRBG Key (A6185): E - DRBG Entropy Input (A6186): E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- DRBG Seed (A6186): E - DRBG Internal State V value (A6186): E - DRBG Key (A6186): E
Configure TLSv1.2 Function	Create a secure TLSv1.2 channel	Approved Mode Indicator and successful TLSv1.2 configuration system log message	Commands to configure TLSv1.2	Status of the completion of TLSv1.2 configuration	TLS RSA KeyGen DRBG Function	Crypto Officer - TLS RSA Private Key: G,W - TLS RSA Public Key: G,W - DRBG Entropy Input (A6185): E - DRBG Seed (A6185): E - DRBG Internal State V value (A6185): E - DRBG Key (A6185): E - DRBG Entropy Input (A6186): E - DRBG Seed (A6186): E - DRBG Internal State V value (A6186): E - DRBG Key (A6186): E
Configure SNMPv3 Function	Create a secure SNMPv3 channel	Approved Mode Indicator and successful SNMPv3	Commands to configure SNMPv3	Status of the completion of SNMPv3	KTS (TLSv1.2 with AES and HMAC) KTS (TLSv1.2 with AES-GCM)	Crypto Officer - SNMPv3 Authentication Secret: W

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		configuration system log message		configuration		
Configure IPSec/IKEv2 Function	Create IPSec/IKEv2 tunnel	Approved Mode Indicator and successful IPSec/IKE v2 configuration system log message	Commands to configure IPSec/IKE v2	Status of the completion of IPSec/IKE v2 configuration	KTS (TLSv1.2 with AES and HMAC) KTS (TLSv1.2 with AES-GCM) IPSec/IKE RSA KeyGen DRBG Function	Crypto Officer - IPSec/IKE Pre-Shared Secret: W - IPSec/IKE RSA Private Key: G,W - IPSec/IKE RSA Public Key: G,W - DRBG Entropy Input (A6185): E - DRBG Seed (A6185): E - DRBG Internal State V value (A6185): E - DRBG Key (A6185): E - DRBG Entropy Input (A6186): E - DRBG Seed (A6186): E - DRBG Internal State V value (A6186): E - DRBG Key (A6186): E
Run SSHv2 Function	Negotiation and encrypted data transport via SSH	Approved Mode Indicator and successful SSHv2 service system log message	Initiate SSHv2 tunnel establishment request	Status of SSHv2 tunnel establishment	KAS-ECC-KeyGen (SSH) KAS-ECC (SSH) SSH ECDSA SigGen SSH ECDSA SigVer Session Encryption/Decry	Crypto Officer - SSH ECDHE Private Key: G,W,E - SSH ECDHE Public Key:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					ption (SSH) Session Authentication (SSHv2) SSHv2 Keying Materials Development DRBG Function	G,R,W - Peer SSH ECDHE Public Key: W,E - SSH ECDHE Shared Secret: G,W,E - SSH ECDSA Private Key: E - SSH ECDSA Public Key: R - SSH Session Encryption Key: G,W,E - SSH Session Authentication Key: G,W,E - DRBG Entropy Input (A6185): E - DRBG Seed (A6185): E - DRBG Internal State V value (A6185): E - DRBG Key (A6185): E - DRBG Entropy Input (A6186): E - DRBG Seed (A6186): E - DRBG Internal State V value (A6186): E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- DRBG Key (A6186): E User - SSH ECDHE Private Key: G,W,E - SSH ECDHE Public Key: G,R,W - Peer SSH ECDHE Public Key: W,E - SSH ECDHE Shared Secret: G,W,E - SSH ECDSA Private Key: E - SSH ECDSA Public Key: R - SSH Session Encryption Key: G,W,E - SSH Session Authentication Key: G,W,E - DRBG Entropy Input (A6185): E - DRBG Seed (A6185): E - DRBG Internal State V value (A6185): E - DRBG Key (A6185): E - DRBG Entropy

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Input (A6186): E - DRBG Seed (A6186): E - DRBG Internal State V value (A6186): E - DRBG Key (A6186): E
Run TLSv1.2 Function	Negotiation and encrypted data transport via TLS	Approved Mode Indicator and successful TLSv1.2 service system log message	Initiate TLSv1.2 tunnel establishment request	Status of SNMPv3 tunnel establishment	KAS-ECC-KeyGen (TLSv1.2) KAS-ECC (TLSv1.2) KTS (TLSv1.2 with AES and HMAC) KTS (TLSv1.2 with AES-GCM) TLS RSA SigGen TLS RSA SigVer Session Encryption/Decryption (TLSv1.2) Session Authentication (TLSv1.2) TLSv1.2 Keying Materials Development DRBG Function	Crypto Officer - TLS RSA Private Key: E - TLS RSA Public Key: R - TLS ECDHE Private Key: G,W,E - TLS ECDHE Public Key: G,R,W - Peer TLS ECDHE Public Key: W,E - TLS ECDHE Shared Secret: G,W,E - TLS RSA Pre-Master Secret: W,E - TLS Master Secret: G,W,E - TLS Session Encryption Key: G,W,E - TLS Session Authentication Key: G,W,E - DRBG

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Entropy Input (A6185): E - DRBG Seed (A6185): E - DRBG Internal State V value (A6185): E - DRBG Key (A6185): E - DRBG Entropy Input (A6186): E - DRBG Seed (A6186): E - DRBG Internal State V value (A6186): E - DRBG Key (A6186): E User - TLS RSA Private Key: E - TLS RSA Public Key: R - TLS ECDHE Private Key: G,W,E - TLS ECDHE Public Key: G,R,W - Peer TLS ECDHE Public Key: W,E - TLS ECDHE Shared Secret: G,W,E - TLS RSA Pre-Master

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Secret: W,E - TLS Master Secret: G,W,E - TLS Session Encryption Key: G,W,E - TLS Session Authentication Key: G,W,E - DRBG Entropy Input (A6185): E - DRBG Seed (A6185): E - DRBG Internal State V value (A6185): E - DRBG Key (A6185): E - DRBG Entropy Input (A6186): E - DRBG Seed (A6186): E - DRBG Internal State V value (A6186): E - DRBG Key (A6186): E
Run SNMPv2 Function	Negotiation and encrypted data transport via SNMPv3	Approved Mode Indicator and successful SNMPv3 service system log message	Initiate SNMPv3 tunnel establishment request	Status of SNMPv3 tunnel establishment	Session Encryption/Decryption (SNMPv3) Session Authentication (SMPv3) SNMPv3 Keying Materials Development	Crypto Officer - SNMPv3 Authentication Secret: E - SNMPv3 Session Encryption Key: G,W,E - SNMPv3 Session Authenticatio

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						n Key: G,W,E User - SNMPv3 Authentication Secret: E - SNMPv3 Session Encryption Key: G,W,E - SNMPv3 Session Authentication Key: G,W,E
Run IPSec/IKEv2 Function	Negotiation and encrypted data transport via IPSec	Approved Mode Indicator and successful IPSec/IKE v2 service system log message	Initiate IPSec/IKE v2 tunnel establishment request	Status of IPSec/IKE v2 tunnel establishment	KAS-ECC-KeyGen (IPSec/IKE) KAS-ECC (IPSec/IKE) IPSec/IKE RSA SigGen IPSec/IKE RSA SigVer Session Encryption/Decryption (IPSec/IKE) Session Authentication (IPSec/IKE) IPSec/IKE Keying Materials Development DRBG Function	Crypto Officer - IPSec/IKE Pre-Shared Secret: E - IPSec/IKE RSA Private Key: E - IPSec/IKE RSA Public Key: R - IPSec/IKE ECDHE Private Key: G,W,E - IPSec/IKE ECDHE Public Key: G,R,W - Peer IPSec/IKE ECDHE Public Key: W,E - IPSec/IKE ECDHE Shared Secret: G,W,E - SKEYSEED: G,W,E - IPSec/IKE Session Encryption Key: G,W,E - IPSec/IKE Session

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Authentication Key: G,W,E - DRBG Entropy Input (A6185): E - DRBG Seed (A6185): E - DRBG Internal State V value (A6185): E - DRBG Key (A6185): E - DRBG Entropy Input (A6186): E - DRBG Seed (A6186): E - DRBG Internal State V value (A6186): E - DRBG Key (A6186): E User - IPSec/IKE Pre-Shared Secret: E - IPSec/IKE RSA Private Key: E - IPSec/IKE RSA Public Key: R - IPSec/IKE ECDHE Private Key: G,W,E - IPSec/IKE ECDHE Public Key: G,R,W - Peer IPSec/IKE ECDHE Public Key:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						W,E - IPSec/IKE ECDHE Shared Secret: G,W,E - SKEYSEED: G,W,E - IPSec/IKE Session Encryption Key: G,W,E - IPSec/IKE Session Authentication Key: G,W,E - DRBG Entropy Input (A6185): E - DRBG Seed (A6185): E - DRBG Internal State V value (A6185): E - DRBG Key (A6185): E - DRBG Entropy Input (A6186): E - DRBG Seed (A6186): E - DRBG Internal State V value (A6186): E - DRBG Key (A6186): E

Table 14: 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.

4.4 Non-Approved Services

N/A for this module.

4.5 External Software/Firmware Loaded

The module supports the firmware load test by using RSA 2048 bits with SHA2-256 (RSA Cert. # A6185) 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. Any firmware/software loaded into this module that is not shown on the module certificate, is out of the scope of this validation and requires a separate FIPS 140-3 validation.

4.6 Cryptographic Output Actions and Status

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

4.7 Additional Information

The module supports Unauthenticated service, where the unauthenticated users can run the self-test service by power-cycling the module.

5 Software/Firmware Security

5.1 Integrity Techniques

The module performs the Firmware Integrity test by using HMAC-SHA2-256 (HMAC Cert. #A6185) 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 MAC 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.

5.2 Initiate on Demand

Integrity test is performed as part of the Pre-Operational Self-Tests. It is automatically executed at power-on. The operator can power-cycle or reboot the 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

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

7 Physical Security

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Tamper Evidence 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 3 - ION 3200H / ION 3200H-C5G-WW; 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
Production grade components	N/A	N/A

Table 15: Mechanisms and Actions Required

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.

7.2 User Placed Tamper Seals

ION 1200/1200-S

Number: The ION 1200 requires 3 FIPS tamper evident labels while the ION 1200-C-NA/ION 1200-C-ROW/ION 1200-C-5G-WW require 4 FIPS tamper evident labels.

Placement:

Figure 15 - ION 1200 Front View

Figure 16 - ION 1200-C-5G-WW Front View

Figure 17 - ION 1200-C-NA and ION 1200-C-ROW Front View

Figure 18 - ION 1200 Left View (same for all models)

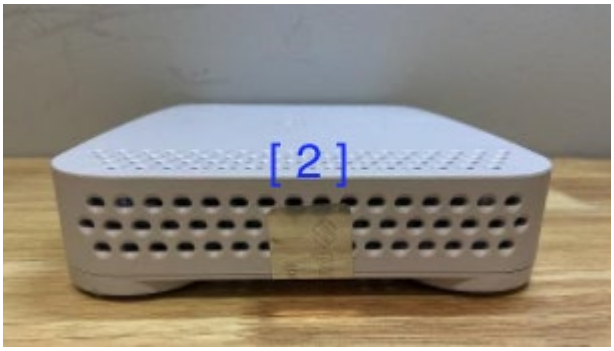

Figure 19 - ION 1200 Right View (same for all models)


Figure 20 - ION 1200 Top View

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

Figure 22 - ION 1200 Rear View

Figure 23 - ION 1200 Bottom View

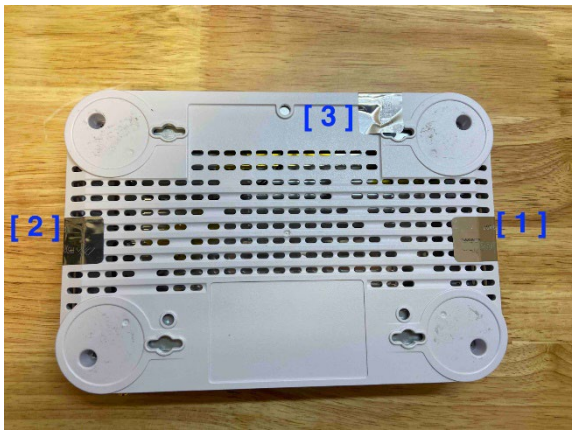

Figure 24 - ION 1200-C-5G-WW/ION 1200-C-NA/ION 1200-C-ROW Bottom View

Figure 25 - ION 1200-S Rear View

Figure 26 - ION 1200-S-C-NA, ION 1200-S-C-ROW, ION 1200-S-C-5G-WW Rear View

Figure 27 - ION 1200-S, ION 1200-S-C-NA, ION 1200-S-C-ROW, ION 1200-S-C-5G-WW Bottom View

Surface Preparation: Clean the chassis of any grease, dirt, or oil before applying the tamper evident labels. Alcohol-based cleaning pads are recommended for this purpose.

Operator Responsible for Securing Unused Seals: Crypto Officer

Part Numbers:

- ION 1200: Kit P/N 920-000363
- ION 1200-S: Kit P/N 920-000363

ION 3200

Number: Three (3) labels

Placement:

Figure 28 - ION 3200 Rear View

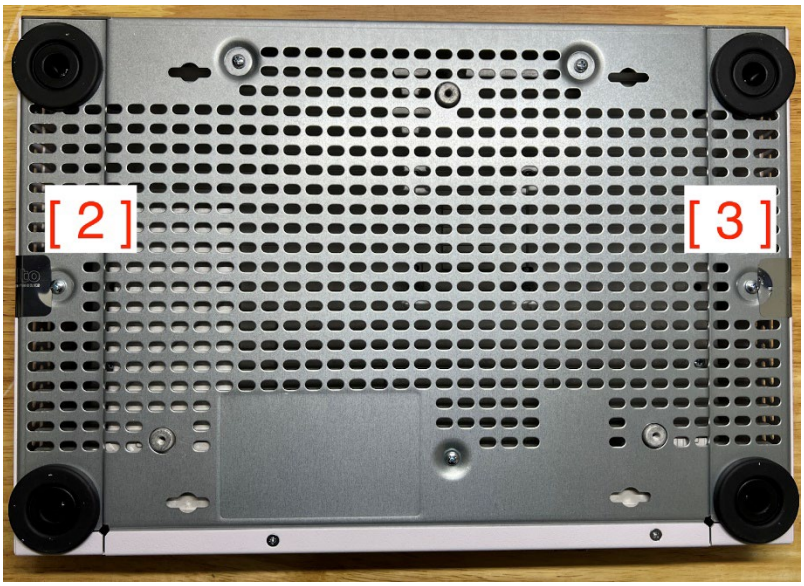

Figure 29 - ION 3200 Bottom View

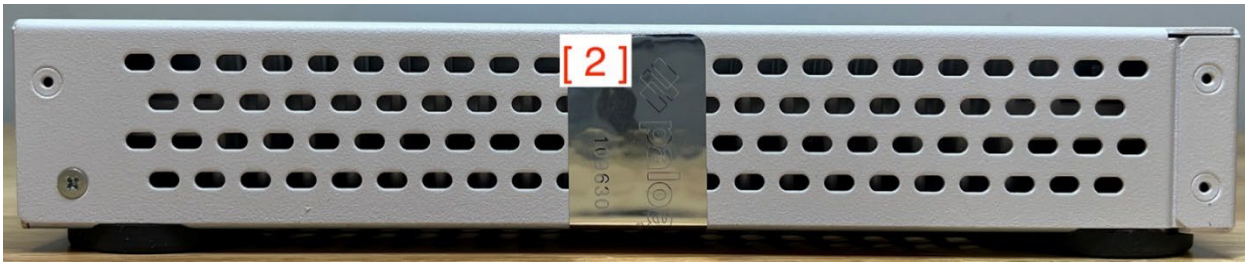

Figure 30 - ION 3200 Left Side View

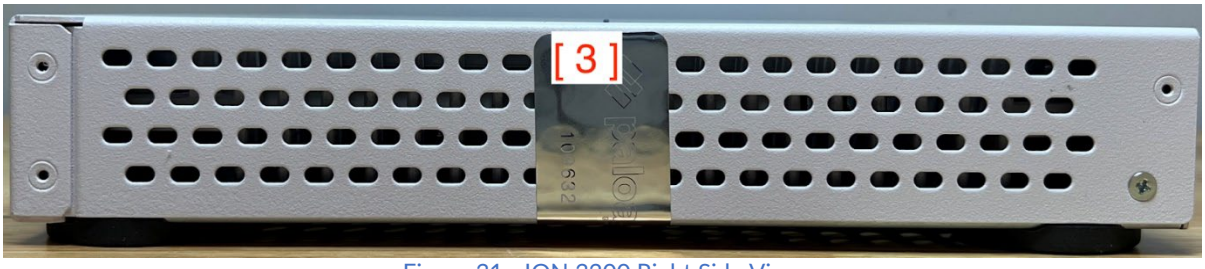

Figure 31 - ION 3200 Right Side View

Surface Preparation: Clean the chassis of any grease, dirt, or oil before applying the tamper evident labels. Alcohol-based cleaning pads are recommended for this purpose.

Operator Responsible for Securing Unused Seals: Crypto Officer

Part Numbers: ION 3200: Kit P/N 920-000363

ION 3200H/ION 3200H-C5G-WW

Number: Three (3) Labels

Placement:

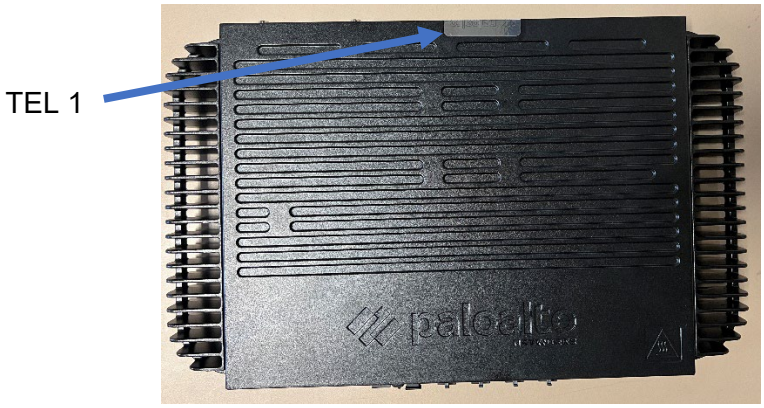

Figure 32 - 3200H Top

Figure 33 – 3200H Bottom

Figure 34 – 3200H Front

Figure 35 – 3200H Back

Figure 36 – 3200H Left

Figure 37 – 3200H Right

Surface Preparation: Clean the chassis of any grease, dirt, or oil before applying the tamper evident labels. Alcohol-based cleaning pads are recommended for this purpose.

Operator Responsible for Securing Unused Seals: Crypto Officer

Part Numbers: ION 3200H/ION 3400H-C5G-WW: Kit P/N 920-000363

ION 5200/9200

Number: Twelve (12) labels

Placement:

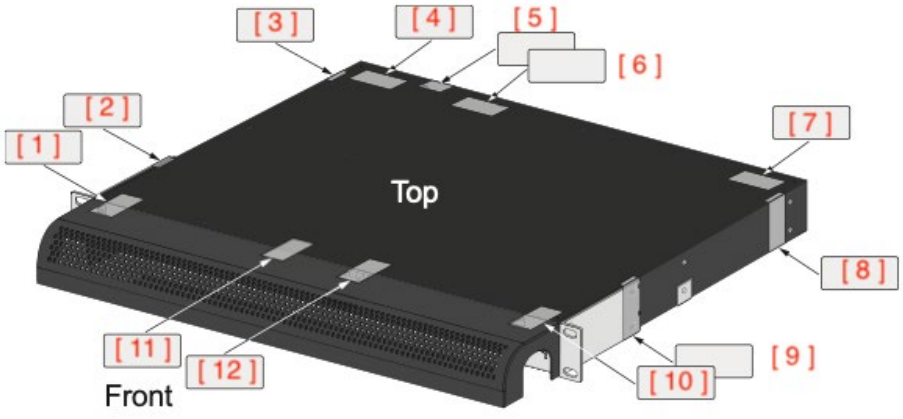

Figure 38 - ION 5200/9200 FIPS Kit Installation

Surface Preparation: Clean the chassis of any grease, dirt, or oil before applying the tamper evident labels. Alcohol-based cleaning pads are recommended for this purpose.

Operator Responsible for Securing Unused Seals: Crypto Officer

Part Numbers: ION 5200, ION 9200: Kit P/N 920-000333

7.3 Filler Panels

ION 5200/9200 Opacity shield

The opacity shield is included in the FIPS kit alongside the tamper evidence labels with part number: Kit P/N 920-000333

8 Non-Invasive Security

N/A for this module

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
RAM	Volatile Memory	Dynamic
HDD	Non-Volatile Memory	Static

Table 16: Storage Areas

9.2 SSP Input-Output Methods

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

Table 17: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Zeroization Command	CO issues zeroization service	The zeroization command will overwrite all SSPs stored in the RAM or in the HDD within the TOEPP with zeros.	"Disable System" command
Power Down	Operator powers the module off	Powering off the module will overwrite all SSPs stored in the RAM within the TOEPP with zeros.	"Debug reboot" command or unplugging module

Zeroization Method	Description	Rationale	Operator Initiation
Session Termination	Zeroization upon session termination	Session termination will automatically overwrite all session based temporary SSPs with zeros.	Terminate session

Table 18: SSP Zeroization Methods

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.
4. The Firmware Load Test Key is only used for Firmware Load Test Authentication and not subject to the zeroization requirement.

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
DRBG Entropy Input (A6185)	Used to seed the DRBG	256 - 256 bits	Entropy Input - CSP			DRBG Function
DRBG Seed (A6185)	Used in DRBG Generation	256 - 256 bits	DRBG Seed - CSP			DRBG Function
DRBG Internal State V value (A6185)	Used in DRBG Generation	256 - 256 bits	DRBG Internal State V value - CSP			DRBG Function
DRBG Key (A6185)	Used in DRBG Generation	256 - 256 bits	DRBG Key - CSP			DRBG Function
DRBG Entropy Input (A6186)	Used to seed the DRBG	256 - 256 bits	Entropy Input - CSP			DRBG Function
DRBG Seed (A6186)	Used in DRBG Generation	256 - 256 bits	DRBG Seed - CSP			DRBG Function
DRBG Internal State V value (A6186)	Used in DRBG Generation	256 - 256 bits	DRBG Internal State V value - CSP			DRBG Function
DRBG Key (A6186)	Used in DRBG Generation	256 - 256 bits	DRBG Key - CSP			DRBG Function

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Crypto Officer Authentication RSA Public Key	Used for CO role authentication	2048 bits - 112 bits	Public Key - PSP			
User Password	Used for User role authentication	8 Characters minimum - 8 Characters minimum	Authentication Data - CSP			
Firmware Load Test Key	Used for Firmware Load Test	2048 bits - 112 bits	Public Key - CSP			Firmware Load Test
TLS RSA Private Key	Used for TLS peer authentication	2048, 3072 bits - 112, 128 bits	Private Key - CSP	TLS RSA KeyGen		TLS RSA SigGen
TLS RSA Public Key	Used for TLS peer authentication	2048, 3072 bits - 112, 128 bits	Public Key - PSP		TLS RSA KeyGen	
TLS ECDHE Private Key	Used to derive TLS ECDHE Shared Secret	P-256, P-384, P-521 - 128, 192, 256 bits	Private Key - CSP	KAS-ECC-KeyGen (TLSv1.2)		KAS-ECC (TLSv1.2)
TLS ECDHE Public Key	Used to derive TLS ECDHE Shared Secret	P-256, P-384, P-521 - 128, 192, 256 bits	Public Key - PSP		KAS-ECC-KeyGen (TLSv1.2)	
Peer TLS ECDHE Public Key	Used to derive TLS ECDHE shared secret	P-256, P-384, P-521 - 128, 192, 256 bits	Public Key - PSP			KAS-ECC (TLSv1.2)
TLS ECDHE Shared Secret	Used to derive TLS Master Secret	P-256, P-384, P-521 - 128, 192, 256 bits	Shared Secret - CSP		KAS-ECC (TLSv1.2)	TLSv1.2 Keying Materials Development
TLS RSA Pre-Master Secret	Used to derive TLS Master Secret	384 - 384 bits	Pre-Master Secret - CSP			TLSv1.2 Keying Materials Development
TLS Master Secret	Used to derive TLS Encryption	384 - 384 bits	Master Secret - CSP		TLSv1.2 Keying Materials	TLSv1.2 Keying Materials Development

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	Keys, TLS Authentication Keys				Development	
TLS Session Encryption Key	Used to secure TLS session confidentiality	128 or 256 bits - 128 or 256 bits	Session Key - CSP		TLSv1.2 Keying Materials Development	Session Encryption/Decryption (TLSv1.2)
TLS Session Authentication Key	Used to secure TLS session integrity	at least 112 bits - at least 112 bits	Session Key - CSP		TLSv1.2 Keying Materials Development	Session Authentication (TLSv1.2)
IPSec/IKE Pre-Shared Secret	Used for IPSec/IKE peer authentication	2048 bits characters - 2048 bits characters	Shared Secret - CSP			
IPSec/IKE RSA Private Key	Used for IPSec/IKE peer authentication	2048, 3072 bits - 112, 128 bits	Private Key - CSP	IPSec/IKE RSA KeyGen		IPSec/IKE RSA SigGen
IPSec/IKE RSA Public Key	Used for IPSec peer authentication	2048, 3072 bits - 112, 128 bits	Public Key - PSP		IPSec/IKE RSA KeyGen	
IPSec/IKE ECDHE Private Key	Used to derive IPSec/IKE ECDHE Shared Secret	P-256, P-384 - 128, 192 bits	Private Key - CSP	KAS-ECC-KeyGen (IPSec/IKE)		KAS-ECC (IPSec/IKE)
IPSec/IKE ECDHE Public Key	Used to derive IPSec/IKE ECDHE Shared Secret	P-256, P-384 - 128, 192 bits	Public Key - PSP		KAS-ECC-KeyGen (IPSec/IKE)	
Peer IPSec/IKE ECDHE Public Key	Used to derive IPSec/IKE ECDHE Shared Secrets	P-256, P-384 - 128, 192 bits	Public Key - PSP			KAS-ECC (IPSec/IKE)
IPSec/IKE ECDHE Shared Secret	Used to derive IPSec/IKE Session Encryption	P-256, P-384 - 128, 192 bits	Shared Secret - CSP		KAS-ECC (IPSec/IKE)	IPSec/IKE Keying Materials Development

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	Keys, IPSec/IKE Authentication Keys					
SKEYSEED	Keying material used to derive the IPSec/IKE Session Encryption Key and IPSec/IKE Authentication Key	384 - 384 bits	Keying Material - CSP		IPSec/IKE Keying Materials Development	IPSec/IKE Keying Materials Development
IPSec/IKE Session Encryption Key	Used to secure IPSec/IKE session confidentiality	128, 192 bits - 128, 192 bits	Session Key - CSP		IPSec/IKE Keying Materials Development	Session Encryption/Decryption (IPSec/IKE)
IPSec/IKE Session Authentication Key	Used to secure IPSec/IKE session integrity	at least 112 bits - at least 112 bits	Session Key - CSP		IPSec/IKE Keying Materials Development	Session Authentication (IPSec/IKE)
SNMPv3 Authentication Secret	Used for SNMPv3 User authentication	8 characters minimum - 8 characters minimum	Authentication Secret - CSP			
SNMPv3 Session Encryption Key	Used to secure SNMPv3 session confidentiality	128 bits - 128 bits	Session Key - CSP		SNMPv3 Keying Materials Development	Session Encryption/Decryption (SNMPv3)
SNMPv3 Session Authentication Key	Used to secure SNMPv3 session integrity	160 bits - at least 112 bits	Session Key - CSP		SNMPv3 Keying Materials Development	Session Authentication (SMPv3)
SSH ECDHE Private Key	Used to derive the SSH ECDHE Shared Secret	P-256, P-384, P-521 - 128, 192, 256 bits	Private Key - CSP	KAS-ECC-KeyGen (SSH)		KAS-ECC (SSH)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
SSH ECDHE Public Key	Used to derive the SSH ECDHE Shared Secret	P-256, P-384, P-521 - 128, 192, 256 bits	Public Key - PSP		KAS-ECC-KeyGen (SSH)	
Peer SSH ECDHE Public Key	Used to derive SSH ECDHE Shared Secret	P-256, P-384, P-521 - N/A	Public Key - PSP			KAS-ECC (SSH)
SSH ECDHE Shared Secret	Used to derive SSH Session Encryption Keys, SSH Session Authentication Keys	P-256, P-384, P-521 - 128, 192, 256 bits	Shared Secret - CSP		KAS-ECC (SSH)	SSHv2 Keying Materials Development
SSH ECDSA Private Key	Used for SSH session authentication	P-256, P-384, P-521 - 128, 192, 256 bits	Private Key - CSP	SSH ECDSA KeyGen		SSH ECDSA SigGen
SSH ECDSA Public Key	Used for SSH Session authentication	P-256, P-384, P-521 - 128, 192, 256	Public Key - PSP		SSH ECDSA KeyGen	
SSH Session Encryption Key	Used for SSH session confidentiality protection	128, 192, 256 bits - 128, 192, 256 bits	Session Key - CSP		SSHv2 Keying Materials Development	Session Encryption/Decryption (SSH)
SSH Session Authentication Key	Used for SSH session integrity protection	at least 160 bits - at least 160 bits	Session Key - CSP		SSHv2 Keying Materials Development	Session Authentication (SSHv2)
Firmware Integrity Test Key	Used for Firmware Integrity Pre-Operational Self-test. Not an SSP but included for completeness	256 bits - 256 bits	Firmware Integrity Key - Neither			HMAC-SHA2-256 (A6185)

Table 19: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DRBG Entropy Input (A6185)		RAM:Plaintext		Zeroization Command Power Down	
DRBG Seed (A6185)		RAM:Plaintext		Zeroization Command Power Down	
DRBG Internal State V value (A6185)		RAM:Plaintext		Zeroization Command Power Down	
DRBG Key (A6185)		RAM:Plaintext		Zeroization Command Power Down	
DRBG Entropy Input (A6186)		RAM:Plaintext		Zeroization Command Power Down	
DRBG Seed (A6186)		RAM:Plaintext		Zeroization Command Power Down	
DRBG Internal State V value (A6186)		RAM:Plaintext		Zeroization Command Power Down	
DRBG Key (A6186)		RAM:Plaintext		Zeroization Command Power Down	
Crypto Officer Authentication RSA Public Key		HDD:Plaintext		Zeroization Command	
User Password	Password/Secret Input via TLSv1.2 decrypted by AES and HMAC Password/Secret Input via TLSv1.2 decrypted by AES-GCM	HDD:Plaintext		Zeroization Command	
Firmware Load Test Key		HDD:Plaintext		N/A	
TLS RSA Private Key		HDD:Plaintext		Zeroization Command	
TLS RSA Public Key	Module Public Key Output	HDD:Plaintext		Zeroization Command	
TLS ECDHE Private Key		RAM:Plaintext	While TLS tunnel is on	Zeroization Command Power Down Session Termination	
TLS ECDHE Public Key	Module Public Key Output	RAM:Plaintext	While TLS tunnel is on	Zeroization Command Power Down	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				Session Termination	
Peer TLS ECDHE Public Key	Peer Public Key Input	RAM:Plaintext	While TLS tunnel is on	Zeroization Command Power Down Session Termination	
TLS ECDHE Shared Secret		RAM:Plaintext	While TLS tunnel is on	Zeroization Command Power Down Session Termination	
TLS RSA Pre-Master Secret	Password/Secret Input via TLSv1.2 decrypted by AES and HMAC Password/Secret Input via TLSv1.2 decrypted by AES-GCM	RAM:Plaintext	While TLS tunnel is on	Zeroization Command Power Down Session Termination	
TLS Master Secret		RAM:Plaintext	While TLS tunnel is on	Zeroization Command Power Down Session Termination	
TLS Session Encryption Key		RAM:Plaintext	While TLS tunnel is on	Zeroization Command Power Down Session Termination	
TLS Session Authentication Key		RAM:Plaintext	While TLS tunnel is on	Zeroization Command Power Down Session Termination	
IPSec/IKE Pre-Shared Secret	Password/Secret Input via TLSv1.2 decrypted by AES and HMAC Password/Secret Input via TLSv1.2 decrypted by AES-GCM	HDD:Plaintext		Zeroization Command	
IPSec/IKE RSA Private Key		HDD:Plaintext		Zeroization Command	
IPSec/IKE RSA Public Key	Module Public Key Output	HDD:Plaintext		Zeroization Command	
IPSec/IKE ECDHE Private Key		RAM:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Power Down	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				Session Termination	
IPSec/IKE ECDHE Public Key	Module Public Key Output	RAM:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Power Down Session Termination	
Peer IPSec/IKE ECDHE Public Key	Peer Public Key Input	RAM:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Power Down Session Termination	
IPSec/IKE ECDHE Shared Secret		RAM:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Power Down Session Termination	
SKEYSEED		RAM:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Power Down Session Termination	
IPSec/IKE Session Encryption Key		RAM:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Power Down Session Termination	
IPSec/IKE Session Authentication Key		RAM:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Power Down Session Termination	
SNMPv3 Authentication Secret	Password/Secret Input via TLSv1.2 decrypted by AES and HMAC Password/Secret Input via TLSv1.2 decrypted by AES-GCM	HDD:Plaintext		Zeroization Command	
SNMPv3 Session Encryption Key		RAM:Plaintext	While SNMPv3 tunnel is on	Zeroization Command Power Down Session Termination	
SNMPv3 Session Authentication Key		RAM:Plaintext	While SNMPv3 tunnel is on	Zeroization Command Power Down Session Termination	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
SSH ECDHE Private Key		RAM:Plaintext	While SSHv2 tunnel is on	Zeroization Command Power Down Session Termination	
SSH ECDHE Public Key	Module Public Key Output	RAM:Plaintext	While SSHv2 tunnel is on	Zeroization Command Power Down Session Termination	
Peer SSH ECDHE Public Key	Peer Public Key Input	RAM:Plaintext	While SSHv2 tunnel is on	Zeroization Command Power Down Session Termination	
SSH ECDHE Shared Secret		RAM:Plaintext	While SSHv2 tunnel is on	Zeroization Command Power Down Session Termination	
SSH ECDSA Private Key		HDD:Plaintext		Zeroization Command	
SSH ECDSA Public Key	Module Public Key Output	HDD:Plaintext		Zeroization Command	
SSH Session Encryption Key		RAM:Plaintext	While SSHv2 tunnel is on	Zeroization Command Power Down Session Termination	
SSH Session Authentication Key		RAM:Plaintext	While SSHv2 tunnel is on	Zeroization Command Power Down Session Termination	
Firmware Integrity Test Key		HDD:Plaintext		N/A	

Table 20: SSP Table 2

9.5 Transitions

SHA-1
This implementation will be non-Approved for all uses starting January 1, 2031. At this time, the user should move to SHA2, which is available in this module.

Minimum Key Size
The module implements keys that are 112 bits in strength. This implementation will be non-Approved for all uses starting January 1, 2031. At this time, the user should move to keys of 128 bit strength or greater.

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
Firmware Integrity Test	HMAC-SHA2-256	KAT	SW/FW Integrity	Module is in normal state	Hash Comparison

Table 21: Pre-Operational Self-Tests

Note: The module performs conditional algorithm self-test (CAST) for HMAC-SHA2-256 and SHA2-256 before performing the firmware integrity test.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC Encrypt KAT (A6185)	256 bits	KAT	CAST	Module is in normal state	Encrypt	Power Up
AES-CBC Decrypt KAT (A6185)	256 bits	KAT	CAST	Module is in normal state	Decrypt	Power Up
AES-GCM Encrypt KAT(A6185)	256 bits	KAT	CAST	Module is in normal state	Encrypt	Power Up
AES-GCM Decrypt KAT (A6185)	256 bits	KAT	CAST	Module is in normal state	Decrypt	Power Up
Counter DRBG Instantiate KAT (A6185)	AES-256	KAT	CAST	Module is in normal state	Instantiate KAT	Power Up
Counter DRBG Generate KAT (A6185)	AES-256	KAT	CAST	Module is in normal state	Generate KAT	Power Up
Counter DRBG Reseed KAT (A6185)	AES-256	KAT	CAST	Module is in normal state	Reseed KAT	Power Up
ECDSA SigGen (FIPS186-5) KAT (A6185)	P-224 with SHA2-256	KAT	CAST	Module is in normal state	Sign	Power Up
ECDSA SigVer (FIPS186-5) KAT (A6185)	P-224 with SHA2-256	KAT	CAST	Module is in normal state	Verify	Power Up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA-1 KAT (A6185)	N/A	KAT	CAST	Module is in normal state	N/A	Power Up
HMAC-SHA-1 KAT (A6185)	HMAC-SHA-1	KAT	CAST	Module is in normal state	N/A	Power Up
HMAC-SHA2-256 KAT (A6185)	HMAC-SHA2-256	KAT	CAST	Module is in normal state	N/A	Power Up
HMAC-SHA2-384 KAT (A6185)	HMAC-SHA2-384	KAT	CAST	Module is in normal state	N/A	Power Up
HMAC-SHA2-512 KAT (A6185)	HMAC-SHA2-512	KAT	CAST	Module is in normal state	N/A	Power Up
RSA SigGen (FIPS186-5) KAT (A6185)	2048 bit modulus with SHA2-256	KAT	CAST	Module is in normal state	Sign	Power Up
RSA SigVer (FIPS186-5) KAT (A6185)	2048 bit modulus with SHA2-256	KAT	CAST	Module is in normal state	Verify	Power Up
KAS-ECC-SSC Sp800-56Ar3 KAT (A6185)	Curve P-256	KAT	CAST	Module is in normal state	N/A	Power Up
KDF IKEv2 KAT (A6185)	N/A	KAT	CAST	Module is in normal state	N/A	Power Up
KDF SSH KAT (A6185)	N/A	KAT	CAST	Module is in normal state	N/A	Power Up
KDF SNMP KAT (A6185)	N/A	KAT	CAST	Module is in normal state	N/A	Power Up
TLS v1.2 KDF RFC7627 KAT (A6185)	N/A	KAT	CAST	Module is in normal state	N/A	Power Up
RSA KeyGen (FIPS186-5) PCT (A6185)	2048 bit modulus with SHA2-256	PCT	PCT	Module is in normal state	N/A	Performs on newly generated key pairs before first operational use
ECDSA KeyGen (FIPS186-5) PCT (A6185)	Curve P-256 with SHA2-256	PCT	PCT	Module is in normal state	N/A	Performs on newly generated key pairs before first

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						operational use
KAS-ECC-SSC Sp800-56Ar3 PCT (A6185)	Curve P-256 with SHA2-256	PCT	PCT	Module is in normal state	N/A	Performs on newly generated key pairs before first operational use
Firmware Load Test	RSA 2048 SigVer with SHA2-256	KAT	SW/FW Load	Module is in normal state	Verify	When firmware has been uploaded to the module
AES-CBC Encrypt KAT (A6186)	256 bits	KAT	CAST	Module is in normal state	Encrypt	Power Up
AES-CBC Decrypt KAT (A6186)	256 bits	KAT	CAST	Module is in normal state	Decrypt	Power Up
AES-GCM Encrypt KAT(A6186)	256 bits	KAT	CAST	Module is in normal state	Encrypt	Power Up
AES-GCM Decrypt KAT (A6186)	256 bits	KAT	CAST	Module is in normal state	Decrypt	Power Up
Counter DRBG Instantiate KAT (A6186)	AES-256	KAT	CAST	Module is in normal state	Instantiate KAT	Power Up
Counter DRBG Generate KAT (A6186)	AES-256	KAT	CAST	Module is in normal state	Generate KAT	Power Up
Counter DRBG Reseed KAT (A6186)	AES-256	KAT	CAST	Module is in normal state	Reseed KAT	Power Up
RSA SigVer (FIPS186-5) KAT (A6186)	2048 bit modulus with SHA2-256	KAT	CAST	Module is in normal state	Verify	Power Up
HMAC-SHA2-256 KAT (A6186)	HMAC-SHA2-256	KAT	CAST	Module is in normal state	N/A	Power Up
HMAC-SHA2-384 KAT (A6186)	HMAC-SHA2-384	KAT	CAST	Module is in normal state	N/A	Power Up
KAS-ECC-SSC Sp800-	Curve P-256	KAT	CAST	Module is in normal state	N/A	Power Up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
56Ar3 KAT (A6186)						
TLS v1.2 KDF RFC7627 KAT (A6186)	N/A	KAT	CAST	Module is in normal state	N/A	Power Up
KAS-ECC-SSC Sp800-56Ar3 PCT (A6186)	Curve P-256 with SHA2-256	PCT	PCT	Module is in normal state	N/A	Performs on newly generated key pairs before first operational use
AES-CBC Encrypt KAT (A6188)	256 bits	KAT	CAST	Module is in normal state	Encrypt	Power Up
AES-CBC Decrypt KAT (A6188)	256 bits	KAT	CAST	Module is in normal state	Decrypt	Power Up
HMAC-SHA2-256 KAT (A6188)	HMAC-SHA2-256	KAT	CAST	Module is in normal state	N/A	Power Up
HMAC-SHA2-384 KAT (A6188)	HMAC-SHA2-384	KAT	CAST	Module is in normal state	N/A	Power Up
HMAC-SHA2-512 KAT (A6188)	HMAC-SHA2-512	KAT	CAST	Module is in normal state	N/A	Power Up
Entropy 90B Start-up Repetition Count Test (RCT)	Repetition Count Test	RCT	CAST	Module is in normal state	Designed to quickly detect catastrophic failures that cause the noise source to become "stuck" on a single output value for a long period of time	Power Up
Entropy 90B Start-up Adaptive Proportion Test (APT)	Adaptive Proportion Test	APT	CAST	Module is in normal state	Designed to detect a large loss of entropy that might occur as a result of some physical failure or environmental change affecting the noise source	Power Up
Entropy 90B Continuous Repetition Count Test (RPT)	Repetition Count Test	RCT	CAST	Module is in normal state	Designed to quickly detect catastrophic failures that cause the noise source to become "stuck" on a single output	Entropy data is generatd from the Entropy Source - Continuous

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
					value for a long period of time	
Entropy 90B Continuous Adaptive Proportions Test (APT)	Adaptive Proportions Test	APT	CAST	Module is in normal state	Designed to detect a large loss of entropy that might occur as a result of some physical failure or environmental change affecting the noise source	Entropy data is generated from the Entropy Source - Continuous

Table 22: Conditional Self-Tests

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

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Firmware Integrity Test	KAT	SW/FW Integrity	60 Days	Reboot

Table 23: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CBC Encrypt KAT (A6185)	KAT	CAST	60 Days	Reboot
AES-CBC Decrypt KAT (A6185)	KAT	CAST	60 Days	Reboot
AES-GCM Encrypt KAT(A6185)	KAT	CAST	60 Days	Reboot
AES-GCM Decrypt KAT (A6185)	KAT	CAST	60 Days	Reboot
Counter DRBG Instantiate KAT (A6185)	KAT	CAST	60 Days	Reboot
Counter DRBG Generate KAT (A6185)	KAT	CAST	60 Days	Reboot
Counter DRBG Reseed KAT (A6185)	KAT	CAST	60 Days	Reboot
ECDSA SigGen (FIPS186-5) KAT (A6185)	KAT	CAST	60 Days	Reboot

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ECDSA SigVer (FIPS186-5) KAT (A6185)	KAT	CAST	60 Days	Reboot
SHA-1 KAT (A6185)	KAT	CAST	60 Days	Reboot
HMAC-SHA-1 KAT (A6185)	KAT	CAST	60 Days	Reboot
HMAC-SHA2-256 KAT (A6185)	KAT	CAST	60 Days	Reboot
HMAC-SHA2-384 KAT (A6185)	KAT	CAST	60 Days	Reboot
HMAC-SHA2-512 KAT (A6185)	KAT	CAST	60 Days	Reboot
RSA SigGen (FIPS186-5) KAT (A6185)	KAT	CAST	60 Days	Reboot
RSA SigVer (FIPS186-5) KAT (A6185)	KAT	CAST	60 Days	Reboot
KAS-ECC-SSC Sp800-56Ar3 KAT (A6185)	KAT	CAST	60 Days	Reboot
KDF IKEv2 KAT (A6185)	KAT	CAST	60 Days	Reboot
KDF SSH KAT (A6185)	KAT	CAST	60 Days	Reboot
KDF SNMP KAT (A6185)	KAT	CAST	60 Days	Reboot
TLS v1.2 KDF RFC7627 KAT (A6185)	KAT	CAST	60 Days	Reboot
RSA KeyGen (FIPS186-5) PCT (A6185)	PCT	PCT	60 Days	Reboot
ECDSA KeyGen (FIPS186-5) PCT (A6185)	PCT	PCT	60 Days	Reboot
KAS-ECC-SSC Sp800-56Ar3 PCT (A6185)	PCT	PCT	60 Days	Reboot
Firmware Load Test	KAT	SW/FW Load	60 Days	Reboot
AES-CBC Encrypt KAT (A6186)	KAT	CAST	60 Days	Reboot
AES-CBC Decrypt KAT (A6186)	KAT	CAST	60 Days	Reboot
AES-GCM Encrypt KAT(A6186)	KAT	CAST	60 Days	Reboot

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-GCM Decrypt KAT (A6186)	KAT	CAST	60 Days	Reboot
Counter DRBG Instantiate KAT (A6186)	KAT	CAST	60 Days	Reboot
Counter DRBG Generate KAT (A6186)	KAT	CAST	60 Days	Reboot
Counter DRBG Reseed KAT (A6186)	KAT	CAST	60 Days	Reboot
RSA SigVer (FIPS186-5) KAT (A6186)	KAT	CAST	60 Days	Reboot
HMAC-SHA2-256 KAT (A6186)	KAT	CAST	60 Days	Reboot
HMAC-SHA2-384 KAT (A6186)	KAT	CAST	60 Days	Reboot
KAS-ECC-SSC Sp800-56Ar3 KAT (A6186)	KAT	CAST	60 Days	Reboot
TLS v1.2 KDF RFC7627 KAT (A6186)	KAT	CAST	60 Days	Reboot
KAS-ECC-SSC Sp800-56Ar3 PCT (A6186)	PCT	PCT	60 Days	Reboot
AES-CBC Encrypt KAT (A6188)	KAT	CAST	60 Days	Reboot
AES-CBC Decrypt KAT (A6188)	KAT	CAST	60 Days	Reboot
HMAC-SHA2-256 KAT (A6188)	KAT	CAST	60 Days	Reboot
HMAC-SHA2-384 KAT (A6188)	KAT	CAST	60 Days	Reboot
HMAC-SHA2-512 KAT (A6188)	KAT	CAST	60 Days	Reboot
Entropy 90B Start-up Repetition Count Test (RCT)	RCT	CAST	N/A	N/A
Entropy 90B Start-up Adaptive Proportion Test (APT)	APT	CAST	N/A	N/A
Entropy 90B Continuous Repetition Count Test (RPT)	RCT	CAST	N/A	N/A

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Entropy 90B Continuous Adaptive Proportions Test (APT)	APT	CAST	N/A	N/A

Table 24: Conditional Periodic Information

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.

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Error State	In the Error State, no cryptographic services are provided, and data output is prohibited.	Self-test failure	Reboot the module	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"; Failed SP 800-90B Entropy Source Start-up/Continuous health tests: No random numbers are generated and key generation is halted

Table 25: Error States

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.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

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 6.4.2. 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.

11.2 Administrator Guidance

Prisma SD-WAN Administrator's Guide from https://docs.paloaltonetworks.com/

11.3 Non-Administrator Guidance

There is no specific Non-Administrator guidance.

11.4 End of Life

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.