Palo Alto Networks

Palo Alto Networks Instant-On Networks (ION) devices ION 1000, ION 2000, ION 3000, ION 7000, and ION 9000

FIPS 140-2 Level 2 Non-Proproprietary Security Policy

Document Version Number: 1.3

Table of Contents

1. Module Overview

The CloudGenix® SD-WAN Instant-On Network (ION) models of hardware 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 your WAN. Built with the intent to reduce remote infrastructure, CloudGenix SD-WAN enables the cloud-delivered branch.

The module is a Multi-Chip Standalone module. FIPS 140-2 conformance testing was performed at Security Level 2. The following configurations were tested by the lab.

Table 1: Configurations tested by the lab.

Module Name and Version	Firmware version
ION 1000	5.5.1
ION 2000	5.5.1
ION 3000	5.5.1
ION 7000	5.5.1
ION 9000	5.5.1

The Cryptographic Module meets FIPS 140-2 Level 2 requirements.

Table 2: Module Security Level Statement.

FIPS Security Area	Security Level
Cryptographic Module Specification	2
Module Ports and Interfaces	2
Roles, Services and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

The cryptographic boundary of the module is the enclosure that contains components of the module. The enclosure of the cryptographic module is opaque within the visible spectrum. The module uses tamper evident labels to provide the evidence of tampering.

Figure 1: ION 1000

Figure 2: ION 2000

Figure 3: ION 3000

Figure 4: ION 7000

Figure 5: ION 9000

The module conforms to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (i.e., for business use).

2. Modes of Operation

The module is intended to always operate in the FIPS approved mode.

The Crypto Officer must invoke the user interface using default password. Crypto Officer must change the default password during the installation.

Configuring any of the following features disables the FIPS mode.

- MD5 for SNMP or IPSec
- DH using keys that are less than 2048 bits for IPSec
- DES for SNMP
- SNMPv2

2.1 Approved Cryptographic Functions

The following approved cryptographic algorithms are used in FIPS approved mode of operation.

CAVP Cert	Library	Algorithm	Standard	Model/ Method	Key Lengths, Curves or Moduli	Use
C1994	CloudGenix ION Crypto Library-1	AES	FIPS 197, SP 800-38D	CBC, CTR, GCM[1]	128, 192, 256	Data Encryption/ Decryption
					128, 192, 256	KTS (AES CBC Cert. #C1994 and HMAC Cert. #C1994; key establishment methodology provides between 128 and 256 bits of encryption strength)
C1927	CloudGenix ION Crypto Library-2		FIPS 197, SP 800-38D	CBC, GCM[1]	128, 256	Data Encryption/ Decryption
					256	KTS (AES GCM Cert. #C1927)
C1926	CloudGenix ION Crypto Library-3		FIPS 197	CBC	128, 192, 256	Data Encryption/ Decryption
C1944	CloudGenix ION Crypto Library-4		FIPS 197	CBC	128, 192, 256	
C1994	CloudGenix ION Crypto Library-1	DRBG	SP 800-90A	CTR_DRBG	256	Deterministic Random Bit Generation[3]

CAVP Cert	Library	Algorithm	Standard	Model/ Method	Key Lengths, Curves or Moduli	Use
C1927	CloudGenix ION Crypto Library-2			HMAC_Based DRBG with SHA2-512		
C1994	CloudGenix ION Crypto Library-1	CVL Partial EC-DH	SP 800-56A	ECC	B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521	Shared Secret Computation
C1927	CloudGenix ION Crypto Library-2				P-256, P-384, P-521	
C1994	CloudGenix ION Crypto Library-1	HMAC	FIPS 198-1	HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	160, 224, 256, 384, 512	Message Authentication KTS
C1927	CloudGenix ION Crypto Library-2			HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512		
C1926	CloudGenix ION Crypto Library-3					
C1944	CloudGenix ION Crypto Library-4					

CAVP Cert	Library	Algorithm	Standard	Model/ Method	Key Lengths, Curves or Moduli	Use
C1994	CloudGenix ION Crypto Library-1	Triple-DES	SP 800-67	TCBC	168	Data Encryption/ Decryption[2]
C1926	CloudGenix ION Crypto Library-3					
C1994	CloudGenix ION Crypto Library-1	SHS	FIPS 180-4	SHA-1, SHA-224, SHA-256, SHA-384 SHA-512		Message Digest
C1927	CloudGenix ION Crypto Library-2					
C1926	CloudGenix ION Crypto Library-3			SHA-256, SHA-384 SHA-512		
C1944	CloudGenix ION Crypto Library-4					
C1994	CloudGenix ION Crypto Library-1	RSA	FIPS 186-4, FIPS 186-2 (verification only)	SHA-1, SHA-224 SHA-256 SHA-384 SHA-512 ANSIX9.31; PKCS1 v1.5, PSS	1024 (verification only), 1536 (verification only), 2048, 3072	Key Generation Digital Signature Generation and Verification

CAVP Cert	Library	Algorithm	Standard	Model/ Method	Key Lengths, Curves or Moduli	Use
C1927	CloudGenix ION Crypto Library-2		FIPS 186-4	SHA-1, SHA-224 SHA-256 SHA-384 SHA-512 PKCS1 v1.5	1024, 2048	Digital Signature Verification
C1994	CloudGenix ION Crypto Library-1	ECDSA	FIPS 186-4		P-192[6], P-224, P-256, P-384, P-521, K-163[6], K-233, K-283, K-409, K-571, B-163[6], B-233, B-283, B-409, B-571	Digital Signature Generation and Verification, Key Generation
C1994	CloudGenix ION Crypto Library-1	CVL KDF IKEv2, SNMP, TLS 1.2, SSH	SP 800-135			Key Derivation[4]
C1927	CloudGenix ION Crypto Library-2	CVL KDF TLS 1.2				

CAVP Cert	Library	Algorithm	Standard	Model/ Method	Key Lengths, Curves or Moduli	Use
CKG (vendor affirmed)		Cryptogra-phic Key Generation	SP 800-133			Key Generation[5]

Table 3: Approved Cryptographic Functions

Note 1: not all CAVS tested modes of the algorithms are used in this module.

Note 2: any firmware 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 140-2 validation.

[1]The module's AES-GCM implementation complies with IG A.5 scenario 1 and RFC 5288. AES-GCM is only used in TLS version 1.2. The module's AES-GCM implementation complies with IG A.5 scenario 1 and RFC 5288, and supports acceptable GCM cipher suites from Section 3.3.1 of SP 800-52 Rev 1 or SP 800-52 Rev 2. AES-GCM is only used in TLS version 1.2. When the IV exhausts the maximum number of possible values for a given session key, the first party, client or server, that encounters this condition will trigger a handshake to establish a new encryption key. New AES-GCM keys are generated by the module if the module loses power.

[2]Operators are responsible for ensuring that the same Triple-DES key is not used to encrypt more than 2^16 64-bit data blocks. Although the key is 168 bits, the bit strength is only 112 bits.

[3]The minimum number of bits of entropy generated by the module is 256 bits.

[4]No parts of these protocols, other than the KDF, have been tested by the CAVP and CMVP.

[5]The module directly uses the output of the DRBG. The generated seed used in the asymmetric key generation is an unmodified output from DRBG. Section 4 "Using the Output of a Random Bit Generator" of SP 800-133 is applicable.

[6] These curves are only approved for Signature Verification.

2.2 Non-FIPS Approved But Allowed Cryptographic Functions.

Table 4: Non-FIPS Approved But Allowed Cryptographic Functions

Algorithm	Caveat	Use
EC DH using at least 224 bits key	Provides between 112 and 256 bits of encryption strength	Used for key establishment in TLS handshake and SSH handshake.
DH using at least 2048 bits key	Provides between 112 and 201 bits of encryption strength.	Used for key establishment in SSH handshake and IKE handshake.
NDRNG[1]		Used to seed SP 800-90A DRBG.

[1]The minimum number of bits of entropy generated by the module is 256 bits.

2.3 Non-Approved and non-Allowed algorithms

Table 5: Non-Approved and non-Allowed algorithms

Algorithm	Use
MD5	SNMP and IPSec in non-approved mode
DH using keys that are less than 2048 bits	IPSec in non-approved mode
DES	SNMP in non-approved mode

3. Ports and interfaces

The following table describes physical ports and logical interfaces of the module.

Table 5.1: Ports and Interfaces of ION 1000

Port Name	Count	Interface(s)
Ethernet Ports	Type: 1 GE Copper (4)	Data Input, Data Output, Control Input, Status Output
Serial Console Port	1	Data Input, Data Output, Control Input, Status Output
USB Ports	2 USB 2.0	Not used

Port Name	Count	Interface(s)
Power Switch	1	Control Input
Power Port	1	Power Input
LEDs	4	Status Output

Table 5.2: Ports and Interfaces of ION 2000

Port Name	Count	Interface(s)
Ethernet Ports	Type: 1 GE Copper (5)	Data Input, Data Output, Control Input, Status Output
Serial Console Port	1	Data Input, Data Output, Control Input, Status Output
USB Ports	2 USB 2.0	Not used
Power Switch	1	Control Input
Power Port	1	Power Input
LEDs	3	Status Output

Table 5.3: Ports and Interfaces of ION 3000

Port Name	Count	Interface(s)
Ethernet Ports	Type: 1 GE Copper (14)	Data Input, Data Output, Control Input, Status Output
Serial Console Port	1	Data Input, Data Output, Control Input, Status Output
USB Ports	2 USB 2.0	Not used
Power Switch	1	Control Input
Power Port	1	Power Input
LEDs	2	Status Output

Table 5.4: Ports and Interfaces of ION 7000

Port Name	Count	Interface(s)
Ethernet Ports	Type: 1 GE Copper (10) Type: 10 Ge SFP+ (6)	Data Input, Data Output, Control Input, Status Output
Serial Console Port	1	Data Input, Data Output, Control Input, Status Output
USB Ports	2 USB 2.0	Not used
Power Switch	1	Control Input
Power Port	2	Power Input
LEDs	4	Status Output

Table 5.5: Ports and Interfaces of ION 9000

Port Name	Count	Interface(s)
Ethernet Ports	Type: 1 GE Copper (10) Type: 10 Ge SFP+ (8)	Data Input, Data Output, Control Input, Status Output
Serial Console Port	1	Data Input, Data Output, Control Input, Status Output
USB Ports	2 USB 2.0	Not used
Power Switch	1	Control Input
Power Port	2	Power Input
LEDs	8	Status Output

Note: All devices have 2 LEDs for each of the Ethernet ports.

4. Roles, Services and Authentication

The module supports role-based authentication. The module supports a Crypto Officer role and a User Role. The Crypto Officer installs and administers the module. The Users use the cryptographic services

provided by the module. The module supports concurrent operators. The module provides the following services.

Table 6.1: Roles and Services

Service	Corresponding Roles	Types of Access to Cryptographic Keys and CSPs R – Read E - Execute W – Write or Create Z – Zeroize
Run Self-test	Crypto Officer	N/A
Reboot	Crypto Officer	N/A
Zeroize	Crypto Officer	All: Z
Firmware update	Crypto Officer	Firmware update key: R, E
Show status	Crypto Officer User	IPsec Keys: R,W,E TLS Keys: R,W,E CTR_DRBG CSPs : R,W HMAC_DRBG CSPs: R,W
SSH Login	Crypto Officer	Password: R, W SSH Keys: R,W, E CTR_DRBG CSPs : R,W
TLS Tunnel	Crypto Officer	TLS Keys: R,W,E CTR_DRBG CSPs : R,W HMAC_DRBG CSPs: R,W
Configuration	Crypto Officer	Password: R, W SSH Keys: R,W, E TLS Keys: R,W, E CTR_DRBG CSPs : R,W HMAC_DRBG CSPs: R,W
SNMPv3	Crypto Officer	Password: R, W SNMP Keys: R,W,E
IPsec Tunnel	Crypto Officer User	IPsec Keys: R,W,E CTR_DRBG CSPs : R,W

The module supports the following authentication mechanisms.

Table 6.2: Authentication Mechanisms

Role	Authentication Mechanisms
CO Role	Passwords (Minimum 8 characters) The module uses passwords of at least 8 printable

Role	Authentication Mechanisms
	characters. Total number of password permutations with eight characters is 95^8 = 6,634,204,312,890,625. Therefore the probability is less than one in 1,000,000 that a random attempt will succeed or a false acceptance will occur. Only five password attempts per minute are allowed by the module. The likelihood of success after one minute is approximately $7.5*10^{-16}$, well below one in 100,000. RSA key (at least 2048 bits) The module uses at least 2048 bits RSA key, which corresponds to 112 bits of security. 2^-112 is significantly less than 1/1,000,000. Therefore the probability is less than one in 1,000,000 that a random attempt will succeed or a false acceptance will occur. The number of attempts in 1 minute is limited to about 10,000. The likelihood of success after one minute is approximately $1.9*10^{-30}$, well below one in 100,000.
User Role	IPSec PSK (2048 bits) The module uses 2048 bits IPSec PSK. 2^-2048 is significantly less than 1/1,000,000. Therefore the probability is less than one in 1,000,000 that a random attempt will succeed or a false acceptance will occur. The number of handshakes in 1 minute is limited to about 50,000. The likelihood of success after one minute is approximately $1.5*10^{-612}$, well below one in 100,000.

5. Cryptographic Keys and CSPs

The table below describes cryptographic keys and CSPs used by the module.

Table 7: Cryptographic Keys and CSPs

Key	Description/Usage	Storage
TLS master secret Established using KDF TLS 1.2	Used to derive TLS encryption key and TLS HMAC Key	RAM in plaintext
TLS pre-master secret Established using EC DH	Used to derive TLS master secret	RAM in plaintext
TLS AES key Established using KDF TLS 1.2	Used during encryption and decryption of data within the TLS protocol	RAM in plaintext
TLS HMAC key Established using KDF TLS 1.2	Used to protect integrity of data within the TLS protocol	RAM in plaintext
TLS RSA public keys Established during the TLS handshake	Used during the TLS handshake	RAM in plaintext Hard drive in plaintext
TLS EC Diffie-Hellman public and private keys Established using CTR / HMAC DRBG	Used during the TLS handshake to establish the shared secret	RAM in plaintext
CTR_DRBG CSPs: entropy input, V and Key HMAC_DRBG CSPs: entropy input, V and Key Established using NDRNG	Used during generation of random numbers	RAM in plaintext
Passwords Set by operators	Used for operator authentication	RAM in plaintext Hard drive in plaintext
IPSec PSK Set by operators	Used for operator authentication	RAM in plaintext Hard drive in plaintext
IPSec Diffie-Hellman public and private keys Established using CTR_DRBG	Used during the IPSec handshake to establish the shared secret	RAM in plaintext
IPSec AES keys Established using KDF IKEv2	Used during encryption and decryption of data within the IPSec protocol	RAM in plaintext

Key	Description/Usage	Storage
IPSec Triple-DES keys Established using KDF IKEv2	Used during encryption and decryption of data within the IPSec protocol	RAM in plaintext
IPSec HMAC keys Established using KDF IKEv2	Used to protect integrity of data within the IPSec protocol	RAM in plaintext
Firmware update RSA key Set at the factory	Used to protect integrity during firmware update	RAM in plaintext Hard drive in plaintext
SNMP Secret Set by operators	Used to establish SNMP sessions	RAM in plaintext Hard drive in plaintext
SSH AES key Established using KDF SSH	Used during encryption and decryption of data within the SSH protocol	RAM in plaintext
SSH HMAC key Established using KDF SSH	Used to protect integrity of data within the SSH protocol	RAM in plaintext
SSH RSA public and private keys Established using CTR_DRBG	Used to authenticate the SSH handshake	RAM in plaintext Hard drive in plaintext
SSH ECDSA public and private keys Established using CTR_DRBG	Used to authenticate the SSH handshake	RAM in plaintext Hard drive in plaintext
SSH Diffie-Hellman public and private keys Established using CTR_DRBG	Used during the SSH handshake to establish the shared secret	RAM in plaintext
SSH EC Diffie-Hellman public and private keys Established using CTR_DRBG	Used during the SSH handshake to establish the shared secret	RAM in plaintext

Note: public keys are not considered CSPs

Note: Zeroization is achieved by the "*disable system*" command

6. Self-tests

The module performs the following power-up and conditional self-tests. Upon failure or a power-up or conditional self-test the module halts its operation.

The following table describes self-tests implemented by the module.

Table 8: Self-Tests

Algorithm	Power up Test
AES	KAT using ECB, CBC and GCM modes (encryption/decryption)
Triple-DES	KAT using CBC mode (encryption/decryption)
SHS	KAT using SHA1, SHA224, SHA256, SHA384, and SHA512
HMAC	KAT using SHA1, SHA224, SHA256, SHA384 and SHA512
SP800-90A DRBG	KAT: CTR_DRBG HASH_DRBG HMAC_DRBG
RSA	KAT using 2048 bit key, SHA-256
Firmware integrity	MD5 checksum during bootup
ECC CDH	Shared secret computation
ECDSA	Pairwise Consistency Test (sign/verify) using P-224, K-233 and SHA512
	Conditional Test
SP800-90A DRBG	Continuous Random Number Generator test
	DRBG health tests Performed per SP 800-90A Section 11.3
NDRNG	Continuous Random Number Generator test
RSA	Pairwise consistency test on generation of a key pair
Firmware load	RSA using 2048 bit key
ECDSA	Pairwise consistency test on generation of a key pair

7. Physical Security

The cryptographic module consists of production-grade components. The enclosure of the cryptographic module is opaque within the visible spectrum. The removable covers are protected with tamper-evident seals. The tamper evident labels are applied at the factory to provide evidence of tampering if a panel is removed. The Crypto Officer must note the locations of the tamper evidence labels upon receipt of the module. The Crypto Officer must check the integrity of the tamper evident labels periodically thereafter. If the tamper-evident seals are broken or missing, the Crypto Officer must halt the operation of the module.

8. References

Table 9: References

Reference	Specification
[ANS X9.31]	Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)
[FIPS 140-2]	Security Requirements for Cryptographic modules, May 25, 2001
[FIPS 180-4]	Secure Hash Standard (SHS)
[FIPS 186-2/4]	Digital Signature Standard
[FIPS 197]	Advanced Encryption Standard
[FIPS 198-1]	The Keyed-Hash Message Authentication Code (HMAC)
[FIPS 202]	SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions
[PKCS#1 v2.1]	RSA Cryptography Standard
[PKCS#5]	Password-Based Cryptography Standard
[PKCS#12]	Personal Information Exchange Syntax Standard
[SP 800-38A]	Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode
[SP 800-38B]	Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication
[SP 800-38C]	Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality

Reference	Specification
[SP 800-38D]	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC
[SP 800-38F]	Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping
[SP 800-56A]	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
[SP 800-56B]	Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography
[SP 800-56C]	Recommendation for Key Derivation through Extraction-then-Expansion
[SP 800-67R1]	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher
[SP 800-89]	Recommendation for Obtaining Assurances for Digital Signature Applications
[SP 800-90A]	Recommendation for Random Number Generation Using Deterministic Random Bit Generators
[SP 800-108]	Recommendation for Key Derivation Using Pseudorandom Functions
[SP 800-132]	Recommendation for Password-Based Key Derivation
[SP 800-135]	Recommendation for Existing Application –Specific Key Derivation Functions