Palo Alto Networks Inc.

Panorama 10.2 M-200, M-300, M-600 and M-700

FIPS 140-3 Non-Proprietary Security Policy

Table of Contents

1 General 5
1.1 Overview 5
1.2 Security Levels 5
2 Cryptographic Module Specification 6
2.1 Description 6
2.2 Tested and Vendor Affirmed Module Version and Identification 8
2.3 Excluded Components 9
2.4 Modes of Operation 9
2.5 Algorithms 9
2.6 Security Function Implementations 12
2.7 Algorithm Specific Information 19
2.8 RBG and Entropy 20
2.9 Key Generation 21
2.10 Key Establishment 21
2.11 Industry Protocols 22
3 Cryptographic Module Interfaces 22
3.1 Ports and Interfaces 22
4 Roles, Services, and Authentication 22
4.1 Authentication Methods 22
4.2 Roles 23
4.3 Approved Services 24
4.4 Non-Approved Services 41
4.5 External Software/Firmware Loaded 41
5 Software/Firmware Security 41
5.1 Integrity Techniques 41
5.2 Initiate on Demand 41
6 Operational Environment 42
6.1 Operational Environment Type and Requirements 42
7 Physical Security 42
7.1 Mechanisms and Actions Required 42
7.2 User Placed Tamper Seals 43
7.2.1 Panorama M-200 43
7.2.2 Panorama M-300 46
7.2.3 Panorama M-600 50
7.2.4 Panorama M-700 55

8 Non-Invasive Security 58
9 Sensitive Security Parameters Management 58
9.1 Storage Areas 58
9.2 SSP Input-Output Methods 58
9.3 SSP Zeroization Methods 59
9.4 SSPs 60
10 Self-Tests 74
10.1 Pre-Operational Self-Tests 74
10.2 Conditional Self-Tests 74
10.3 Periodic Self-Test Information 77
10.4 Error States 79
10.5 Operator Initiation of Self-Tests 80
11 Life-Cycle Assurance 80
11.1 Installation, Initialization, and Startup Procedures 80
11.2 Administrator Guidance 81
11.3 Non-Administrator Guidance 81
11.4 Design and Rules 81
11.5 End of Life 81
12 Mitigation of Other Attacks 82

List of Tables

Table 1: Security Levels 6
Table 2: Tested Module Identification – Hardware 8
Table 3: Modes List and Description 9
Table 4: Approved Algorithms 11
Table 5: Vendor-Affirmed Algorithms 11
Table 6: Security Function Implementations 19
Table 7: Entropy Certificates 20
Table 8: Entropy Sources 21
Table 9: Ports and Interfaces 22
Table 10: Authentication Methods 23
Table 11: Roles 23
Table 12: Approved Services 41
Table 13: Mechanisms and Actions Required 43
Table 14: Storage Areas 58
Table 15: SSP Input-Output Methods 59
Table 16: SSP Zeroization Methods 60
Table 17: SSP Table 1 67
Table 18: SSP Table 2 74
Table 19: Pre-Operational Self-Tests 74
Table 20: Conditional Self-Tests 77
Table 21: Pre-Operational Periodic Information 78
Table 22: Conditional Periodic Information 79
Table 23: Error States 79

List of Figures

No table of figures entries found.

1 General

1.1 Overview

The Panorama 10.2 M-200, M-300, M-600 and M-700 from Palo Alto Networks Inc., hereafter referred to as “Panorama M-Series”, “Panorama HW”, “modules”, or the “cryptographic modules” are multi-chip standalone cryptographic modules designed to fulfill FIPS 140-3 level 2 requirements. Panorama M-Series management appliances provide centralized management and visibility of Palo Alto Networks next generation firewalls. From a central location, you can gain insight into applications, users, and content traversing the firewalls. The knowledge of what is on the network, in conjunction with safe application enablement policies, maximizes protection and control while minimizing administrative effort. Your security team can centrally perform analysis, reporting, and forensics with the aggregated data over time, or on data stored on the local firewall.

The Panorama M-Series management appliances’ individual management and logging components can be separated in a distributed manner to accommodate large volumes of log data. Panorama M-Series management appliances can be deployed in the following ways:

● Centralized: In this scenario, all Panorama management and logging functions are combined into a single device.

● Distributed: you can separate the management and logging functions across multiple devices, splitting the functions between managers and log collectors.
    - o Panorama: The Panorama manager is responsible for handling the tasks associated with policy and device configuration across all managed devices. The manager analyzes the data stored in managed log collectors for centralized reporting.
    - o Management-Only: Providing the ability to perform all functions of Panorama with the exception of logging.
    - o Log Collector: Organizations with high logging volume and retention requirements can deploy dedicated Panorama log collector devices that will aggregate log information from multiple managed firewalls.

● Panorama on the M-600 and M-700 supports an additional mode, the PAN-DB private cloud. The PAN-DB private cloud is an on-premise solution that is suitable for organizations that prohibit or restrict the use of the PAN-DB public cloud service. With this on-premise solution, you can deploy one or more M-600/M-700 appliances as PAN-DB servers within your network or data center.

This document may freely be reproduced and distributed in its entirety.

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	3
5	Software/Firmware security	2
6	Operational environment	N/A
7	Physical security	2

Section	Title	Security Level
8	Non-invasive security	N/A
9	Sensitive security parameter management	2
10	Self-tests	2
11	Life-cycle assurance	3
12	Mitigation of other attacks	N/A
	Overall Level	2

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

Panorama M-Series management appliances provide centralized management and visibility of Palo Alto Networks next generation firewalls. From a central location, you can gain insight into applications, users, and content traversing the firewalls. The knowledge of what is on the network, in conjunction with safe application enablement policies, maximizes protection and control while minimizing administrative effort. Your security team can centrally perform analysis, reporting, and forensics with the aggregated data over time, or on data stored on the local firewall.

Module Type: Hardware

Figure 1. M-200 Front

Figure 2. M-200 Rear

Figure 3. M-300 Front

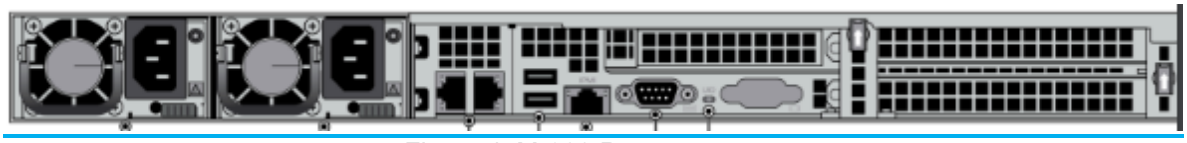

Figure 4. M-300 Rear

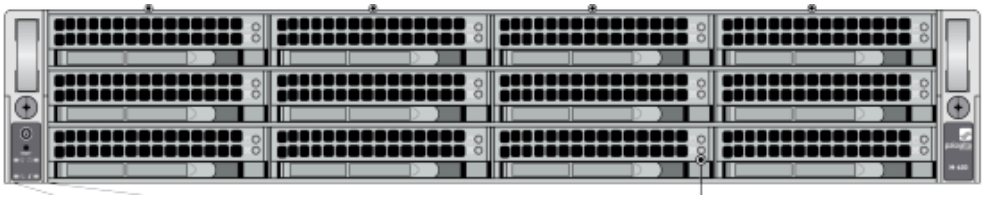

Figure 5. M-600 Front

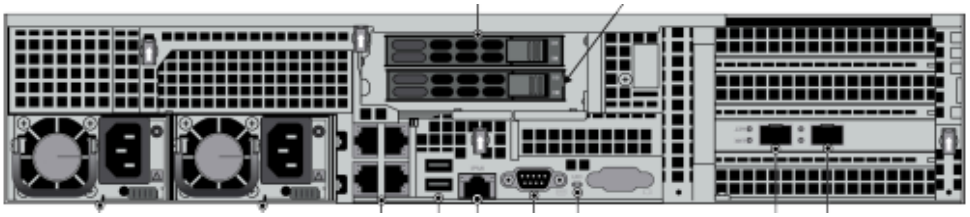

Figure 6. M-600 Rear

Figure 7. M-700 Front

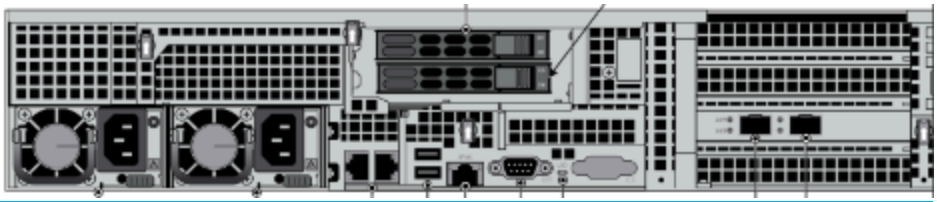

Figure 8. M-700 Rear

Module Embodiment: Multi-Chip Standalone

Cryptographic Boundary:

The cryptographic boundary consists of the physical perimeter of the hardware appliances with the physical kits installed. Please refer to the Physical Security section of this document for depictions of the modules with the physical kits installed.

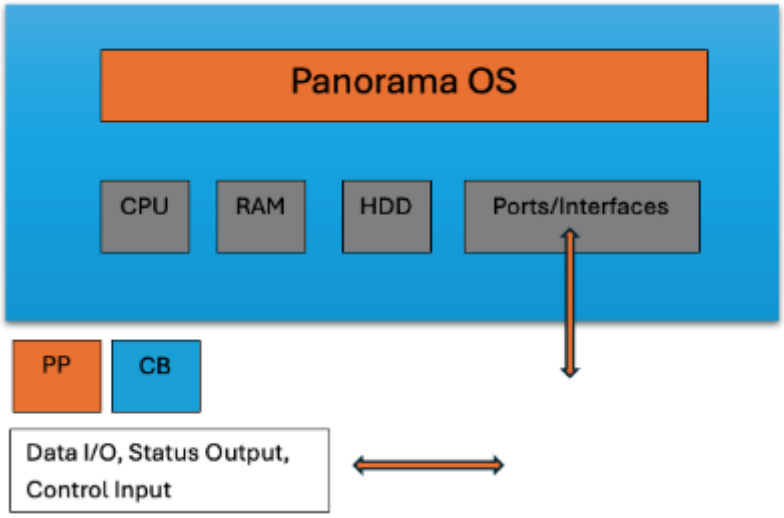

Figure 9. Block Diagram

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
Panorama M-200	910-000176 with 920-000208	10.2.3-h1	Intel Xeon E5-2620 V4	RJ45 interfaces, USB ports, LEDs
Panorama M-300	910-000271 with 920-000319	10.2.3-h1	Intel Xeon (Silver) 4310	RJ45 interfaces, USB ports, LEDs
Panorama M-600	910-000175 with 920-000209	10.2.3-h1	Intel Xeon E5-2680 V4	RJ45 interfaces, USB ports, LEDs, SFP+ ports
Panorama M-700	910-000270 with 920-000318	10.2.3-h1	Intel Xeon (Silver) 4316	RJ45 interfaces, USB ports, LEDs, SFP+ ports

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:

The module only operates in an approved mode of operation and is in the approved mode when installed, initialized and configured per section 11.1 of the Security Policy.

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	Global indicator ("FIPS-CC")

Table 3: Modes List and Description

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A2906	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB128	A2906	Direction - Decrypt, Encrypt Key Length - 128	SP 800-38A
AES-CTR	A2906	Direction - Decrypt, Encrypt Key Length - 128, 192, 256 Payload Length - Payload Length: 8-128 Increment 8 Supports Counter larger than maximum value - No Incremental Counter - No Counter Tests Performed - No	SP 800-38A
AES-GCM	A2906	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 256	SP 800-38D
Counter DRBG	A2906	Prediction Resistance - No, Yes Supports Reseed - Yes Mode - AES-256 Derivation Function Enabled - No, Yes Additional Input - Additional Input: 0-384	SP 800-90A Rev. 1

Algorithm	CAVP Cert	Properties	Reference
		Increment 8 Entropy Input - Entropy Input: 256-384 Increment 8, Entropy Input: 384 Nonce - Nonce: 0, Nonce: 128 Personalization String Length - Personalization String Length: 0-384 Increment 8 Returned Bits - 512	
ECDSA KeyGen (FIPS186-4)	A2906	Curve - P-256, P-384, P-521 Secret Generation Mode - Testing Candidates	FIPS 186-4
ECDSA KeyVer (FIPS186-4)	A2906	Curve - P-256, P-384, P-521	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A2906	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A2906	Curve - P-256, P-384, P-521 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
HMAC-SHA-1	A2906	MAC - MAC: 160 Key Length - Key Length: 256-2048 Increment 8	FIPS 198-1
HMAC-SHA2-224	A2906	MAC - MAC: 224 Key Length - Key Length: 256-2048 Increment 8	FIPS 198-1
HMAC-SHA2-256	A2906	MAC - MAC: 256 Key Length - Key Length: 256-2048 Increment 8	FIPS 198-1
HMAC-SHA2-384	A2906	MAC - MAC: 384 Key Length - Key Length: 256-2048 Increment 8	FIPS 198-1
HMAC-SHA2-512	A2906	MAC - MAC: 512 Key Length - Key Length: 256-2048 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A2906	Domain Parameter Generation Methods - P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-FFC-SSC Sp800-56Ar3	A2906	Domain Parameter Generation Methods - MODP-2048 Scheme - dhEphem - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDF SNMP (CVL)	A2906	Password Length - Password Length: 64, 2048 Engine ID - 80001F88043030303030343935323630	SP 800-135 Rev. 1
KDF SSH (CVL)	A2906	Cipher - AES-128, AES-192, AES-256 Hash Algorithm - SHA-1, SHA2-256, SHA2-512	SP 800-135 Rev. 1
KDF TLS (CVL)	A2906	TLS Version - v1.2 Hash Algorithm - SHA2-256, SHA2-384	SP 800-135 Rev. 1
RSA KeyGen (FIPS186-4)	A2906	Key Generation Mode - B.3.6 Modulo - 2048, 3072, 4096	FIPS 186-4

Algorithm	CAVP Cert	Properties	Reference
		Primality Tests - Table C.2 Info Generated By Server - No Public Exponent Mode - Fixed Fixed Public Exponent - 010001 Private Key Format - Standard	
RSA SigGen (FIPS186-4)	A2906	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096	FIPS 186-4
RSA SigVer (FIPS186-4)	A2906	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096	FIPS 186-4
Safe Primes Key Generation	A2906	Safe Prime Groups - MODP-2048	SP 800-56A Rev. 3
Safe Primes Key Verification	A2906	Safe Prime Groups - MODP-2048	SP 800-56A Rev. 3
SHA-1	A2906	Message Length - Message Length: 8-65536 Increment 8	FIPS 180-4
SHA2-224	A2906	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-256	A2906	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-384	A2906	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-512	A2906	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4

Table 4: Approved Algorithms

Note: Only the algorithms specified in the table above are supported by the module in approved mode of operation.

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG	Key Type:Asymmetric	N/A	Cryptographic Key Generation; SP 800-133rev2 and IG D.H (symmetric keys and asymmetric seeds) from Section 4 Example 1

Table 5: 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
Firmware Load Test	DigSig-SigVer	Signature verification for firmware load test		RSA SigVer (FIPS186-4): (A2906) Modulus: RSA 2048 with SHA2-256 SHA2-256: (A2906)
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 encryption strength	KAS-ECC-SSC Sp800-56Ar3: (A2906) KDF SSH: (A2906) SHA-1: (A2906) SHA2-256: (A2906) SHA2-512: (A2906)
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 establishment methodology provides between 128 and 256 bits of encryption strength	KAS-ECC-SSC Sp800-56Ar3: (A2906) KDF TLS: (A2906) HMAC-SHA2-256: (A2906) HMAC-SHA2-384: (A2906) SHA2-256: (A2906) SHA2-384: (A2906)

Name	Type	Description	Properties	Algorithms
KAS-ECC-KeyGen (SSH)	KAS-KeyGen CKG	KAS ECC keygen used in SSHv2 service		Counter DRBG: (A2906) AES-CTR: (A2906)
KAS-ECC-KeyGen (TLSv1.2)	KAS-KeyGen CKG	KAS ECC keygen used in TLSv1.2 service		Counter DRBG: (A2906) AES-CTR: (A2906)
KAS-FFC (SSH)	KAS-Full	Full KAS-FFC 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 112 bits of encryption strength	KAS-FFC-SSC Sp800-56Ar3: (A2906) KDF SSH: (A2906) Safe Primes Key Generation: (A2906) Safe Primes Key Verification: (A2906) SHA-1: (A2906) SHA2-256: (A2906) SHA2-512: (A2906)
KAS-FFC (TLSv1.2)	KAS-Full	Full KAS-FFC 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 establishment methodology provides 112 bits of encryption strength	KAS-FFC-SSC Sp800-56Ar3: (A2906) KDF TLS: (A2906) Safe Primes Key Generation: (A2906) Safe Primes Key Verification: (A2906) HMAC-SHA2-256: (A2906) HMAC-SHA2-384: (A2906) SHA2-256: (A2906)

Name	Type	Description	Properties	Algorithms
				SHA2-384: (A2906)
KAS-FFC-KeyGen (SSH)	KAS-KeyGen CKG	KAS FFC keygen used in SSHv2 service		Counter DRBG: (A2906) AES-CTR: (A2906)
KAS-FFC-KeyGen (TLSv1.2)	KAS-Full	KAS FFC keygen used in TLSv1.2 service		Counter DRBG: (A2906) AES-CTR: (A2906)
KTS (SSHv2 with AES and HMAC)	KTS-Wrap	KTS via SSHv2 service by using AES and HMAC	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	AES-CBC: (A2906) HMAC-SHA2-256: (A2906) HMAC-SHA2-384: (A2906) SHA2-256: (A2906) SHA2-384: (A2906)
KTS (SSHv2 with AES-GCM)	KTS-Wrap	KTS via SSHv2 service by using AES-GCM	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	AES-GCM: (A2906) AES-CBC: (A2906)
KTS (TLSv1.2 with AES and HMAC)	KTS-Wrap	KTS via TLSv1.2 service by	IG:IG D.F Scenario 2 Path 2, split	AES-CBC: (A2906) HMAC-SHA2-

Name	Type	Description	Properties	Algorithms
		using AES and HMAC	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	256: (A2906) HMAC-SHA2-384: (A2906) SHA2-256: (A2906) SHA2-384: (A2906)
KTS (TLSv1.2 with AES-GCM)	KTS-Wrap	KTS via TLSv1.2 service by using AES-GCM	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	AES-GCM: (A2906) AES-CBC: (A2906)
Session Authentication (SMPv3)	MAC	SNMPv3 session authentication		HMAC-SHA-1: (A2906) HMAC-SHA2-224: (A2906) SHA-1: (A2906) SHA2-224: (A2906)
Session Authentication (SSHv2)	MAC	SSHv2 session authentication		HMAC-SHA-1: (A2906) HMAC-SHA2-256: (A2906) HMAC-SHA2-512: (A2906) SHA-1: (A2906) SHA2-256: (A2906)

Name	Type	Description	Properties	Algorithms
				SHA2-512: (A2906)
Session Authentication (TLSv1.2)	MAC	TLSv1.2 session authentication		HMAC-SHA2-256: (A2906) HMAC-SHA2-384: (A2906) SHA2-256: (A2906) SHA2-384: (A2906)
Session Encryption/Decryption (SNMPv3)	BC-Auth BC-UnAuth	SNMPv3 session protection		AES-CFB128: (A2906)
Session Encryption/Decryption (SSH)	BC-Auth BC-UnAuth	SSHv2 session protection		AES-CBC: (A2906) AES-CTR: (A2906) AES-GCM: (A2906)
Session Encryption/Decryption (TLSv1.2)	BC-Auth BC-UnAuth	TLSv1.2 session protection		AES-CBC: (A2906) AES-GCM: (A2906)
SNMPv3 Keying Materials Development	KAS-135KDF	SNMPv3 session keying materials, used to derive SNMPv3 session keys		KDF SNMP: (A2906) SHA-1: (A2906)
SSH ECDSA KeyGen	AsymKeyPair-KeyGen CKG	ECDSA KeyGen for SSHv2		ECDSA KeyGen (FIPS186-4): (A2906) Counter DRBG: (A2906) AES-CTR: (A2906)
SSH ECDSA SigGen	DigSig-SigGen	ECDSA SigGen for SSHv2		ECDSA SigGen (FIPS186-4): (A2906) SHA2-224: (A2906) SHA2-256: (A2906) SHA2-384: (A2906)

Name	Type	Description	Properties	Algorithms
				SHA2-512: (A2906)
SSH ECDSA SigVer	DigSig-SigVer	ECDSA SigVer for SSHv2		ECDSA SigVer (FIPS186-4): (A2906) ECDSA KeyVer (FIPS186-4): (A2906) SHA-1: (A2906) SHA2-224: (A2906) SHA2-256: (A2906) SHA2-384: (A2906) SHA2-512: (A2906)
SSH RSA KeyGen	AsymKeyPair-KeyGen CKG	ECDSA KeyGen for SSHv2		RSA KeyGen (FIPS186-4): (A2906) Counter DRBG: (A2906) AES-CTR: (A2906) SHA2-256: (A2906) SHA2-384: (A2906) SHA2-512: (A2906)
SSH RSA SigGen	DigSig-SigGen	ECDSA SigGen for SSHv2		RSA SigGen (FIPS186-4): (A2906) SHA2-256: (A2906) SHA2-384: (A2906) SHA2-512: (A2906)
SSH RSA SigVer	DigSig-SigVer	RSA SigVer for SSHv2		RSA SigVer (FIPS186-4): (A2906) SHA-1: (A2906) SHA2-256:

Name	Type	Description	Properties	Algorithms
				(A2906) SHA2-384: (A2906) SHA2-512: (A2906)
SSHv2 Keying Materials Development	KAS-135KDF	SSHv2 session keying materials, used to derive SSHv2 session keys.		KDF SSH: (A2906) SHA-1: (A2906) SHA2-256: (A2906) SHA2-512: (A2906)
TLS ECDSA KeyGen	AsymKeyPair-KeyGen CKG	ECDSA KeyGen for TLSv1.2		ECDSA KeyGen (FIPS186-4): (A2906) Counter DRBG: (A2906) AES-CTR: (A2906)
TLS ECDSA SigGen	DigSig-SigGen	ECDSA SigGen for TLSv1.2		ECDSA SigGen (FIPS186-4): (A2906) SHA2-224: (A2906) SHA2-256: (A2906) SHA2-384: (A2906) SHA2-512: (A2906)
TLS ECDSA SigVer	DigSig-SigVer	ECDSA SigVer for TLSv1.2		ECDSA SigVer (FIPS186-4): (A2906) SHA-1: (A2906) SHA2-256: (A2906) SHA2-384: (A2906) SHA2-512: (A2906)
TLS RSA KeyGen	AsymKeyPair-KeyGen CKG	RSA KeyGen for TLSv1.2		Counter DRBG: (A2906)

Name	Type	Description	Properties	Algorithms
				RSA KeyGen (FIPS186-4): (A2906) AES-CTR: (A2906) SHA2-256: (A2906) SHA2-384: (A2906) SHA2-512: (A2906)
TLS RSA SigGen	DigSig-SigGen	RSA SigGen for TLSv1.2		RSA SigGen (FIPS186-4): (A2906) SHA2-256: (A2906) SHA2-384: (A2906) SHA2-512: (A2906)
TLS RSA SigVer	DigSig-SigVer	RSA SigVer for TLSv1.2		RSA SigVer (FIPS186-4): (A2906) SHA-1: (A2906) SHA2-256: (A2906) SHA2-384: (A2906) SHA2-512: (A2906)
TLSv1.2 Keying Materials Development	KAS-135KDF	TLSv1.2 session keying materials, used to derive TLSv1.2 session keys		KDF TLS: (A2906) HMAC-SHA2-256: (A2906) HMAC-SHA2-384: (A2906) SHA2-256: (A2906) SHA2-384: (A2906)

Table 6: Security Function Implementations

2.7 Algorithm Specific Information

The module is compliant to IG C.H: GCM is used in the context of TLS, SSH:

- For TLS, The GCM implementation meets Scenario 1 of IG C.H: it is used in a manner compliant with SP 800-52rev2 and in accordance with Section 4 of RFC 5288 for TLS key establishment, and ensures when the nonce_explicit part of the IV exhausts all possible values for a given session key, that a new TLS handshake is initiated per sections 7.4.1.1 and 7.4.1.2 of RFC 5246. During operational testing, the module was tested against an independent version of TLS and found to behave correctly
    - From this RFC, the GCM cipher suites in use are TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, and TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384.
- For SSH, the module meets Scenario 1 of IG C.H. The module conforms to RFCs 4252, 4253, and 5647. The fixed field is 32 bits in length and is derived using the SSH KDF; this ensures the fixed field is unique for any given GCM session. The invocation field is 64 bits in length and is incremented for each invocation of GCM; this prevents the IV from repeating until the entire invocation field space of 264 is exhausted. (It would take hundreds of years for this to occur.)

In all of the above cases, the none explicit is always generated deterministically. AES GCM keys are zeroized when the module is power-cycled. For each new TLS or SSH session, a new AES GCM key is established.

The module is compliant to IG C.F:

The module utilizes Approved modulus sizes 2048, 3072, and 4096 bits for RSA signatures. This functionality has been CAVP tested as noted above. The minimum number of Miller Rabin tests for each modulus size is implemented according to Table C.2 of FIPS 186-4. For modulus size 4096, the module implements the largest number of Miller-Rabin tests shown in Table C.2. RSA SigVer is CAVP tested for all three supported modulus sizes as noted above. The module does not perform FIPS 186-2 SigVer. All supported modulus sizes are CAVP testable and tested as noted above. The module does not implement RSA key transport in the approved mode.

2.8 RBG and Entropy

Cert Number	Vendor Name
E64	Palo Alto
E65	Palo Alto
E66	Palo Alto

Table 7: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Palo Alto Networks DRNG Entropy	Physical	Intel Corporation Intel(R) Core(R),	128	128	AES-CBC-MAC (A2165)

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Source - Broadwell EP 10-Core Die with FCLGA2011 Package		Intel(R) Xeon(R) Broadwell-EP-10 FCLGA2011 Intel(R) Xeon(R) E5-2620 V4 Processor			
Palo Alto Networks DRNG Entropy Source - Broadwell EP 15-Core Die with FCLGA2011 Package	Physical	Intel Corporation Intel(R) Xeon(R) Broadwell-EP-15 FCLGA2011 Intel(R) Xeon(R) E5-2690 V4 Processor	128	128	AES-CBC-MAC (A2165)
Palo Alto Networks DRNG Entropy Source - Ice Lake 28-Core Die with FCLGA4189 Package	Physical	Intel Corporation Intel(R) Xeon(R) Ice Lake-28 FCLGA4189 Intel(R) Xeon(R) Gold 5315Y Processor	128	128	AES-CBC-MAC (A2518)

Table 8: Entropy Sources

The Intel DRNG utilizes a vetted conditioner (AES-CBC-MAC) that outputs full entropy (128-bits per 128-bits of output). Upon boot, the AES-256 Counter DRBG (security strength of 256-bits) requests 384-bits from the Intel DRNG entropy source. Therefore, it is fully seeded with 384 bits of entropy.

2.9 Key Generation

The module implements CKG where symmetric keys and seeds used for asymmetric key pair generation are produced using the unmodified/direct output of the DRBG.

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 (1) with KAS-ECC shared secret computation. The shared secret computation provides between 128 and 256 bits of encryption strength.
- KAS-FFC Shared Secret Computation
  - The module provides SP800-56Arev3 compliant key establishment according to FIPS 140-3 IG D.F scenario 2 path (1) with KAS-FFC shared secret computation. The shared secret computation provides between 112 and 150 bits of encryption strength.

2.11 Industry Protocols

- TLS 1.2
- SSHv2
- SNMPv3

No parts of the SSH, TLS and SNMP protocols other than the KDFs, have been tested by the CAVP/CMVP.

3 Cryptographic Module Interfaces

The modules are multi-chip standalone modules with ports and interfaces as shown below. The modules do not implement a control output interface.

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
LED	Status Output	Module status via LED indicators
Power	Power	N/A
RJ45 Console	Status Output	Self-test output
RJ45 Ethernet	Data Input Data Output Control Input Status Output	TLS, SSH
SFP+ (M-600, M-700)	Data Input Data Output Control Input Status Output	TLS

Table 9: Ports and Interfaces

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.	Single-Factor Cryptographic Software.	With a minimum modulus size of 2048, the probability that a random attempt will	The probability of successfully authenticating to the module within a one minute period is 288,000,000/(2^112). The module supports at most 4,800,000 new sessions per second.

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
			succeed is 1/(2^112).	
ECDSA-Based Certificate	The modules support ECDSA public-key based authentication mechanism using a minimum ECDSA curve of P-256.	Single-Factor Cryptographic Software.	With a minimum curve of P-256, the probability that a random attempt will succeed is 1/(2^128).	The probability of successfully authenticating to the module within a one minute period is 288,000,000/(2^112). The module supports at most 4,800,000 new sessions per second.
Password	Password based authentication	Memorized Secret (Unique Username/password).	The minimum length is eight (8) characters (95 possible characters). The probability that a random attempt will succeed or a false acceptance will occur is 1/(958).	The probability of successfully authenticating to the module within one minute is 10/(95^8). The firewall's configuration supports at most ten failed attempts to authenticate in a one-minute period.

Table 10: Authentication Methods

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Identity	CO	RSA-Based Certificate ECDSA-Based Certificate Password
User	Identity	User	RSA-Based Certificate ECDSA-Based Certificate Password

Table 11: Roles

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Access CLI	Connect to module's CLI via SSH	System Logs	Input command for CLI	Configuration items via CLI	KAS-ECC (SSH) KAS-ECC-KeyGen (SSH) KAS-FFC (SSH) KAS-FFC-KeyGen (SSH) KTS (SSHv2 with AES and HMAC) KTS (SSHv2 with AES-GCM) Session Authentication (SSHv2) Session Encryption/Decryption (SSH) SSH ECDSA KeyGen SSH ECDSA SigGen SSH ECDSA SigVer SSH RSA KeyGen SSH RSA SigGen SSH RSA SigVer SSHv2 Keying Materials Development	Crypto Officer - CO, User Password: W,E - DRBG Key: G,E - DRBG Seed: G,E - DRBG V: G,E - ECDSA Private Keys: G,W,E - ECDSA Public Keys: G,R,W,E - Entropy Input String: G,E - RSA Private Keys: G,W,E - RSA Public Keys: G,R,W,E - SSH Client Public Key: W,E - SSH DHE/ECDHE Private Components: G,E,Z - SSH DHE/ECDHE Public Components: G,R,W,E,Z - SSH Host

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Public Key: W,E - SSH Session Authentication Keys: G,E,Z - SSH Session Encryption Keys: G,E,Z - SSH Shared Secret: G,E,Z
Access Web Portal	Connect to module's web portal to invoke services. (Panorama or Management-Only Mode	System Logs	Accessing web browser	Module options via web browser	KAS-ECC (TLSv1.2) KAS-ECC-KeyGen (TLSv1.2) KAS-FFC (TLSv1.2) KAS-FFC-KeyGen (TLSv1.2) KTS (TLSv1.2 with AES and HMAC) KTS (TLSv1.2 with AES-GCM) Session Authentication (TLSv1.2) Session Encryption/Decryption (TLSv1.2) TLS ECDSA KeyGen TLS ECDSA SigGen TLS ECDSA SigVer TLS RSA KeyGen TLS RSA SigGen TLS RSA	Crypto Officer - CA Certificates: G,R,W,E - DRBG Key: G,E - DRBG Seed: G,E - DRBG V: G,E - ECDSA Private Keys: G,W,E - Entropy Input String: G,E - RSA Private Keys: G,W,E - TLS DHE/ECDHE Private Components: G,E,Z - TLS DHE/ECDHE Public Components: G,R,W,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					SigVer TLSv1.2 Keying Materials Development	- TLS Encryption Keys: G,E,Z - TLS HMAC Keys: G,E,Z - TLS Master Secret: G,E,Z - TLS Pre-Master Secret: G,E,Z
Configure High Availability	Configure High Availability communication settings (Panorama or Management-Only Mode)	System and Configuration Logs	Configuring high availability	High availability configured	SSH RSA SigVer SSH ECDSA SigVer	Crypto Officer - ECDSA Public Keys: G,R,W,E - RSA Public Keys: G,R,W,E
Configure Managed Log Collectors	Setup and manage other Log Collector management, communication and storage settings View current deployment information on the managed Log Collectors. It also allows you	System and Configuration Logs	Configuring log collectors	Operation of log collectors	None	Crypto Officer - CO, User Password: W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	to manage firmware versions and schedule updates on managed log collectors. (Panorama or Management-Only Mode)					
Manage PAN-DB Administrative Access	Update Administrator password. (PAN-DB Mode only)	System and Configuration Logs	Commands to manage PAN-DB	Administrator password changed	None	Crypto Officer - CO, User Password: W,E
Manage Panorama Administrative Access	Define access control methods via admin profiles, configure administrators and password profiles Configure local user database, authentication profiles, sequence of methods and access domains. (Panoram	System and Configuration Logs	Configuring admin access	Admin access rights and configurations	SSH ECDSA SigVer SSH RSA SigVer	Crypto Officer - CO, User Password: W,E - ECDSA Public Keys: G,R,W,E - RSA Public Keys: G,R,W,E - SSH Client Public Key: W,E - SSH Host Public Key: W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	a, Management-Only, or Log Collector Mode)					
Monitor System Status and Logs	Review system status via the panorama system CLI, dashboard and logs; show status. (Panorama or Management-Only Mode)	System Logs	Commands for system status / logs	Current status of module and functions	None	Crypto Officer User
Panorama Certificate Management	Manage RSA/ECDSA certificates and private keys, certificate profiles, revocation status, and usage; show status. (Panorama, Management-Only, or Log Collector Mode)	System and Configuration Logs	Configuring certificates	Certificate output and status	SSH ECDSA KeyGen SSH ECDSA SigGen SSH ECDSA SigVer SSH RSA KeyGen SSH RSA SigGen SSH RSA SigVer TLS ECDSA KeyGen TLS ECDSA SigGen TLS ECDSA SigVer TLS RSA KeyGen TLS RSA SigGen TLS RSA SigVer	Crypto Officer - DRBG Key: G,E - DRBG Seed: G,E - DRBG V: G,E - ECDSA Private Keys: G,W,E - ECDSA Public Keys: G,R,W,E - Entropy Input String: G,E - RSA Private Keys: G,W,E - RSA Public

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Keys: G,R,W,E
Panorama Firmware Update	Download and install firmware updates	System and Configuration Logs	Uploading new firmware	Installation of new firmware	Firmware Load Test	Crypto Officer - Public key for firmware content load test: W,E
Panorama Log Collector Setup	Presents configuration options for management interfaces and communication for peer services Import, Export, Save, Load, revert and validate Panorama configurations and state. (Log Collector Mode only)	System and Configuration Logs	Configure options for log collectors	Log collectors operation	KAS-ECC (SSH) KAS-ECC-KeyGen (SSH) KAS-FFC (SSH) KAS-FFC-KeyGen (SSH) KTS (SSHv2 with AES and HMAC) KTS (SSHv2 with AES-GCM) Session Authentication (SSHv2) Session Encryption/Decryption (SSH) SSH ECDSA KeyGen SSH ECDSA SigGen SSH ECDSA SigVer SSH RSA KeyGen SSH RSA SigGen SSH RSA SigVer SSHv2 Keying Materials Development	Crypto Officer - CA Certificates: R,W,E - CO, User Password: W,E - DRBG Key: G,E - DRBG Seed: G,E - DRBG V: G,E - ECDSA Private Keys: G,W,E - ECDSA Public Keys: G,R,W,E - Entropy Input String: G,E - RSA Private Keys: G,W,E - RSA Public Keys: G,R,W,E - SSH Client Public Key: W,E - SSH DHE/ECDH

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						E Private Components: G,E,Z - SSH DHE/ECDHE Public Components: G,R,W,E,Z - SSH Host Public Key: W,E - SSH Session Authentication Keys: G,E,Z - SSH Session Encryption Keys: G,E,Z - SSH Shared Secret: G,E,Z
Panorama Log Setting	Configure log forwarding (Panorama or Management-Only Mode)	Configuration Logs	Configuring log settings	Log setting operations	None	Crypto Officer
Panorama Manager Setup	Presents configuration options for management interfaces and communication for peer services (e.g., SNMP,	System and Configuration Logs	Configuring items on Panorama	Panorama settings configured	KAS-ECC (SSH) KAS-ECC (TLSv1.2) KAS-ECC-KeyGen (SSH) KAS-ECC-KeyGen (TLSv1.2) KAS-FFC (SSH) KAS-FFC (TLSv1.2) KAS-FFC-	Crypto Officer - CA Certificates: G,R,W,E - CO, User Password: W,E - DRBG Key: G,E - DRBG Seed: G,E - DRBG V: G,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	RADIUS). Import, Export, Save, Load, revert and validate Panorama configurations and state role (Panorama or Management-Only Mode)				KeyGen (SSH) KAS-FFC-KeyGen (TLSv1.2) KTS (SSHv2 with AES and HMAC) KTS (SSHv2 with AES-GCM) KTS (TLSv1.2 with AES and HMAC) KTS (TLSv1.2 with AES-GCM) Session Authentication (SMPv3) Session Authentication (SSHv2) Session Authentication (TLSv1.2) Session Encryption/Decryption (SNMPv3) Session Encryption/Decryption (SSH) Session Encryption/Decryption (TLSv1.2) SNMPv3 Keying Materials Development SSH ECDSA KeyGen SSH ECDSA SigGen SSH ECDSA SigVer SSH RSA KeyGen SSH RSA SigGen SSH RSA	- ECDSA Private Keys: G,W,E - ECDSA Public Keys: G,R,W,E - Entropy Input String: G,E - Protocol Secrets: W,E - RSA Private Keys: G,W,E - RSA Public Keys: G,R,W,E - SNMPv3 Authentication Key: G,E,Z - SNMPv3 Authentication Secret: W,E - SNMPv3 Privacy Secret: G,E,Z - SNMPv3 Session Key: G,E,Z - SSH Client Public Key: W,E - SSH DHE/ECDHE Private Components: G,E,Z - SSH DHE/ECDHE Public

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					SigVer SSHv2 Keying Materials Development TLS ECDSA KeyGen TLS ECDSA SigGen TLS ECDSA SigVer TLS RSA KeyGen TLS RSA SigGen TLS RSA SigVer	Components: G,R,W,E,Z - SSH Host Public Key: W,E - SSH Session Authentication Keys: G,E,Z - SSH Session Encryption Keys: G,E,Z - SSH Shared Secret: G,E,Z - TLS DHE/ECDHE Private Components: G,E,Z - TLS DHE/ECDHE Public Components: G,R,W,E,Z - TLS Encryption Keys: G,E,Z - TLS HMAC Keys: G,E,Z - TLS Master Secret: G,E,Z - TLS Pre-Master Secret: G,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Panorama PAN-DB Setup	Presents configuration options for management interfaces and communication for peer services Import, Export, Save, Load, revert and validate Panorama configurations and state. (PAN-DB Mode only)	System Logs	Configuring PAN-DB configurations	PAN-DB functions operational	KAS-ECC (SSH) KAS-ECC-KeyGen (SSH) KAS-FFC (SSH) KAS-FFC-KeyGen (SSH) KTS (SSHv2 with AES and HMAC) KTS (SSHv2 with AES-GCM) Session Authentication (SSHv2) Session Encryption/Decryption (SSH) SSH ECDSA KeyGen SSH ECDSA SigGen SSH ECDSA SigVer SSH RSA KeyGen SSH RSA SigGen SSH RSA SigVer SSHv2 Keying Materials Development	Crypto Officer - CA Certificates: R,W,E - CO, User Password: W,E - DRBG Key: G,E - DRBG Seed: G,E - DRBG V: G,E - ECDSA Private Keys: G,W,E - ECDSA Public Keys: G,R,W,E - Entropy Input String: G,E - RSA Private Keys: G,W,E - RSA Public Keys: G,R,W,E - SSH Client Public Key: W,E - SSH DHE/ECDHE Private Components: G,E,Z - SSH DHE/ECDHE Public Components: G,R,W,E,Z - SSH Host

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Public Key: W,E - SSH Session Authentication Keys: G,E,Z - SSH Session Encryption Keys: G,E,Z - SSH Shared Secret: G,E,Z
Panorama Server Profiles	Configure communication parameters and information for peer servers (Panorama or Management-Only Mode)	System Logs	Configuring server profile settings	Communication parameters setup	KAS-ECC (SSH) KAS-ECC (TLSv1.2) KAS-ECC-KeyGen (SSH) KAS-ECC-KeyGen (TLSv1.2) KAS-FFC (SSH) KAS-FFC (TLSv1.2) KAS-FFC-KeyGen (SSH) KAS-FFC-KeyGen (TLSv1.2) KTS (SSHv2 with AES and HMAC) KTS (SSHv2 with AES-GCM) KTS (TLSv1.2 with AES and HMAC) KTS (TLSv1.2 with AES-GCM) Session Authentication (SMPv3) Session Authentication	Crypto Officer - CA Certificates: R,W,E - CO, User Password: W,E - DRBG Key: G,E - DRBG Seed: G,E - DRBG V: G,E - ECDSA Private Keys: G,W,E - ECDSA Public Keys: G,R,W,E - Entropy Input String: G,E - Protocol Secrets: W,E - RSA Private Keys: G,W,E - RSA

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					(SSHv2) Session Authentication (TLSv1.2) Session Encryption/Decryption (SNMPv3) Session Encryption/Decryption (SSH) Session Encryption/Decryption (TLSv1.2) SNMPv3 Keying Materials Development SSH ECDSA KeyGen SSH ECDSA SigGen SSH ECDSA SigVer SSH RSA KeyGen SSH RSA SigGen SSH RSA SigVer SSHv2 Keying Materials Development TLS ECDSA KeyGen TLS ECDSA SigGen TLS ECDSA SigVer TLS RSA KeyGen TLS RSA SigGen TLS RSA SigVer	Public Keys: G,R,W,E - SNMPv3 Authentication Key: G,E,Z - SNMPv3 Authentication Secret: W,E - SNMPv3 Privacy Secret: G,E,Z - SNMPv3 Session Key: G,E,Z - SSH Client Public Key: W,E - SSH DHE/ECDHE Private Components: G,E,Z - SSH DHE/ECDHE Public Components: G,R,W,E,Z - SSH Host Public Key: W,E - SSH Session Authentication Keys: G,E,Z - SSH Session Encryption Keys: G,E,Z - SSH Shared Secret:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						G,E,Z - TLS DHE/ECDHE Private Components: G,E,Z - TLS DHE/ECDHE Public Components: G,R,W,E,Z - TLS Encryption Keys: G,E,Z - TLS HMAC Keys: G,E,Z - TLS Master Secret: G,E,Z - TLS Pre-Master Secret: G,E,Z
Self-Test	Run power up self-tests on demand by power cycling the module.	System Logs	Initiating self-test	Completion of self-tests	None	Crypto Officer - Public key for firmware content load test: W,E
Setup Managed Devices and Deployment	Set-up and define managed devices, device groups for firewalls. Configure device deployment application	Configuration Logs	Setting up devices	Controlling managed devices	None	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	s and licenses. View current deployment information on the managed firewalls. It also allows you to manage firmware versions and schedule updates on the managed firewalls and managed log collectors. (Panorama or Management-Only Mode)					
Show Status	View status of the module	FIPS-CC Mode Indicator	Initiating show status command	Status of module provided	None	Crypto Officer Unauthenticated
Show Version	Query the module to display the version	Version displayed via System Logs / CLI / UI	Input command for show version	Version information	None	Crypto Officer
System Audit	Allows review of limited configuration and system	System Logs	Commands for showing device setup	System details	None	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	status via SNMPv3, logs, dashboard, show status, and configuration screens. CO Only: Provides configuration commit capability. (Panorama, Management-Only, or PAN-DB Mode)					
System Provisioning	Perform panorama licensing, diagnostics, debug functions, manage Panorama support information and switch between Panorama Management-only, and Logger modes. (Panorama or Management-Only Mode)	System and Configuration logs	Input commands for system provisioning	System setup functions	None	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Zeroize	Zeroize all SSPs	Zeroization Indicator	Initiating zeroize command	Zeroization performed on module	None	Unauthenticated - CA Certificates: Z - CO, User Password: Z - DRBG Key: Z - DRBG Seed: Z - DRBG V: Z - ECDSA Private Keys: Z - ECDSA Public Keys: Z - Entropy Input String: Z - Firmware integrity verification key: Z - Protocol Secrets: Z - Public key for firmware content load test: Z - RSA Private Keys: Z - RSA Public Keys: Z - SNMPv3 Authentication Key: Z - SNMPv3 Authentication Secret: Z - SNMPv3 Privacy

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Secret: Z - SNMPv3 Session Key: Z - SSH Client Public Key: Z - SSH DHE/ECDHE Private Components: Z - SSH DHE/ECDHE Public Components: Z - SSH Host Public Key: Z - SSH Session Authentication Keys: Z - SSH Session Encryption Keys: Z - SSH Shared Secret: Z - TLS DHE/ECDHE Private Components: Z - TLS DHE/ECDHE Public Components: Z - TLS Encryption Keys: Z - TLS HMAC Keys: Z - TLS

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Master Secret: Z - TLS Pre-Master Secret: Z

Table 12: Approved Services

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. #A2906) 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.

5 Software/Firmware Security

5.1 Integrity Techniques

The module performs the Firmware Integrity test by using HMAC-SHA2-256 and ECDSA signature verification (HMAC and ECDSA Cert. #A2906) during the Pre-Operational Self-Test. In addition, the module also conducts the firmware load test by using RSA 2048 with SHA2-256 (Cert. #A2906) for the new validated firmware to be uploaded into the module. The pre-operational self-tests can be initiated by power cycling the module. When this is performed, the module automatically runs the cryptographic algorithm self-tests in addition to the pre-operational firmware integrity test.

The module's executable code is in the form of the compiled firmware image loaded onto the module.

5.2 Initiate on Demand

The pre-operational self-tests can be initiated by power cycling the module. When this is performed, the module automatically runs the cryptographic algorithm self-tests in addition to the pre-operational firmware integrity test.

6 Operational Environment

6.1 Operational Environment Type and Requirements

The FIPS 140-3 Area 5 Operational Environment requirements are not applicable because the module contains a limited operational environment. The operational environment is limited since the module includes a firmware load service to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-3 CMVP. Any other firmware loaded into this module is out of the scope of this validation and requires a separate FIPS 140-3 validation.

Type of Operational Environment: Limited

7 Physical Security

7.1 Mechanisms and Actions Required

The multi-chip standalone modules are production quality containing standard passivation. Chip components are protected by an opaque enclosure. There are tamper-evident seals that are applied on the modules by the Crypto-Officer. There are fifteen (15) for the M-200, fifteen (15) for the M-300, twenty-one (21) for the M-600, and twenty-one (21) for the M-700. All unused seals are to be controlled by the Crypto-Officer. The seals prevent removal of the opaque enclosure without evidence. The Crypto-Officer must ensure that the module surface is clean and dry. Tamper evident seals must be pressed firmly onto the adhering surfaces during installation and once applied, the Crypto-Officer shall permit 24 hours of cure time for all tamper evident seals. The seals prevent removal of the opaque enclosure without evidence. The Crypto-Officer should inspect the seals and shields for evidence of tamper every 30 days. If the seals show evidence of tamper, the Crypto-Officer should assume that the modules have been compromised and contact support.

Mechanism	Inspection Frequency	Inspection Guidance
Tamper-Evident Seals	30 days	(M-200, M-300) Verify integrity of tamper-evident seals in the locations identified in Section 7 of this Security Policy.
Front and Rear Opacity Shields Side Rails	30 days	(M-200, M-300) Verify that opacity shields and side rails have not been loosened or deformed from their original shape, thereby reducing their effectiveness.
Top Overlays	30 days	(M-200, M-300) Verify top overlays have not been removed or deformed. All edges should maintain strong adhesion characteristics.
Tamper Evident Seals	30 days	(M-600, M-700) Verify integrity of tamper-evident seals in the locations specified in Section 7 of this Security Policy.
Front and Rear Opacity Shields	30 days	(M-600, M-700) Verify that the front and rear opacity shields have not been deformed from their original shape, thereby reducing their effectiveness

Mechanism	Inspection Frequency	Inspection Guidance
Vent Overlays	30 days	(M-600, M-700) Verify that the vent overlays have not been removed or deformed. All edges should maintain strong adhesion characteristics

Table 13: Mechanisms and Actions Required

7.2 User Placed Tamper Seals

7.2.1 Panorama M-200

Number: Panorama M-200 requires 15 Tamper Seals

Placement: M-200 Tamper Seal Installation (15 Seals)

1. Replace the top cover with the physical top cover.
    a. Remove the VOID WARRANTY label and cover screws (replacement label included in the kit).
    M-200 appliance—Remove the Void Warranty label that covers the left top cover screw then use a Phillips-head screwdriver to remove both screws as indicated in the illustration.
    b. Simultaneously depress the two (2) release buttons on top of the cover and slide the cover toward the back of the appliance to remove it.
    c. Slide the top cover (does not have vents) on the appliance until the release buttons click. Reinsert and slide cover into position and secure with the two (2) screws.

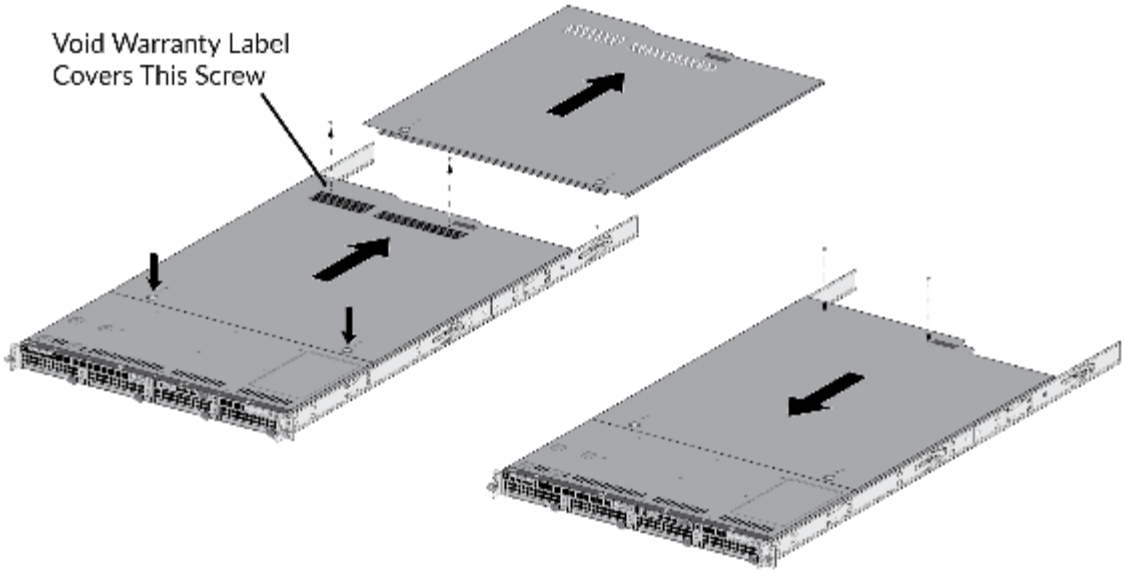

Figure 10. M-200: Top Cover Replacement

2. On the left side of the M-200, firmly apply seven (7) tamper-evident seals as indicated in the illustration.

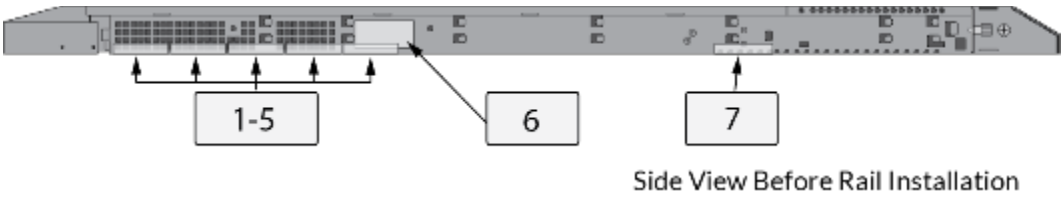

Figure 11. M-200: Side View Before Rail Installation

Install the inner rack mount rail brackets as described in the “M-200 and M-600 Appliance Hardware Reference”. The front rack bracket that you replace in the next step is located on the front inner rails.

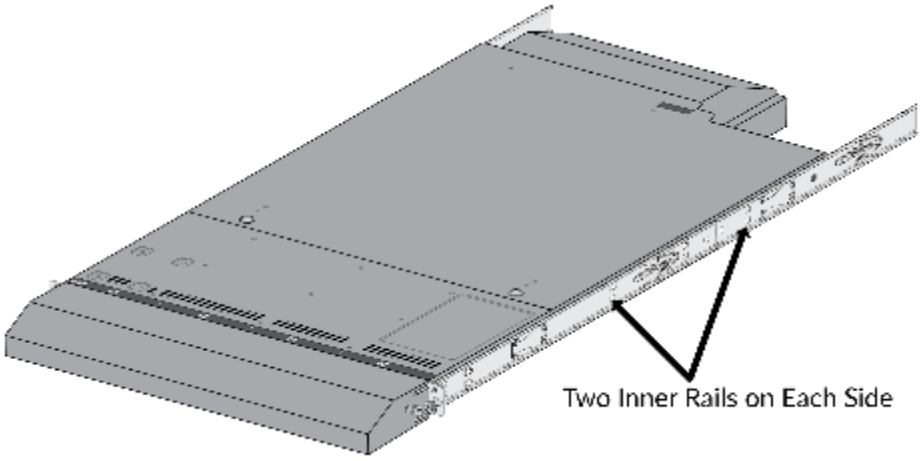

Figure 12. M-200: Inner Rack Mount Rail Brackets

3. Attach the front cover brackets.
Replace the front rack-mount brackets (one bracket on each side) that are part of the inner-rack rails with the rack-mount brackets by removing and then reinstalling two screws on each bracket. The handles have standoffs that are used to secure the front cover.

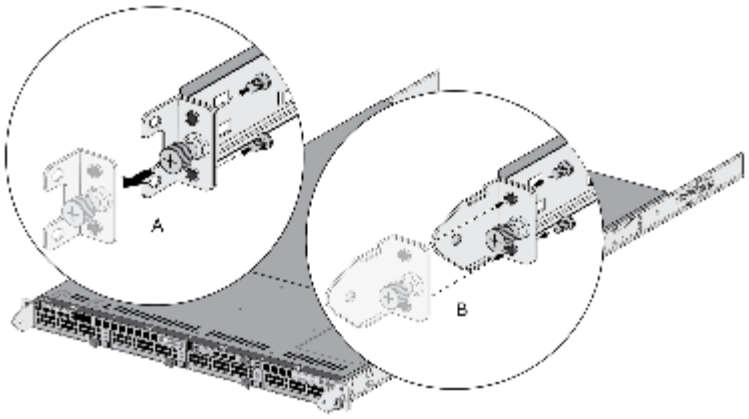

Figure 13. M-200: Replacing Front Rack-Mount Brackets

4. Attach the physical kit front cover to the front of the appliance.
Slide the M-200 physical kit front cover over the brackets and secure the cover by turning the thumb screws clockwise (one thumb screw on each side).

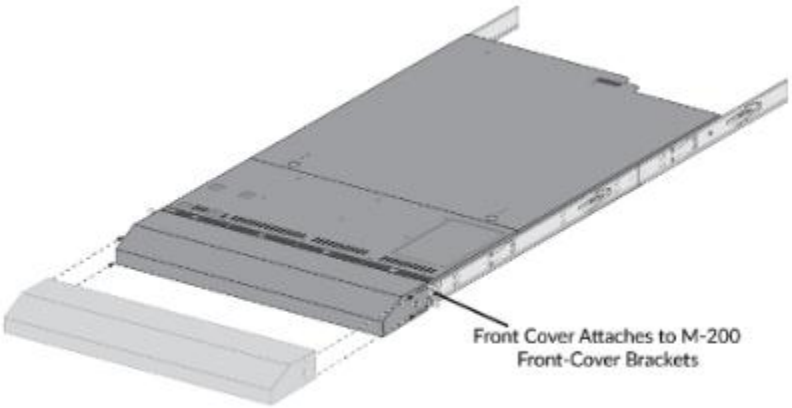

Figure 14. M-200: Attach Physical Kit Front Cover

5. Attach the physical kit back cover to the back of the appliance. Slide the back cover onto the back of the appliance, insert two M4 x 0.7 x 8mm (one (1) screw on each side), and turn the screws clockwise to secure the cover.
6. Apply a tamper-evident seal to each location shown in the following M-200 illustrations. Ensure you apply two
(2) tamper-evident seals on the power supplies (see seals #14 and #15 on the rear illustration). Before you apply the tamper-evident seals, ensure that the appliance and physical kit surfaces are clean and dry. Firmly press one (1) seal on to each of the locations shown in the

illustrations. Avoid touching the seals for at least 24 hours to allow time for the seals to properly adhere to the appliance and physical kit surfaces.

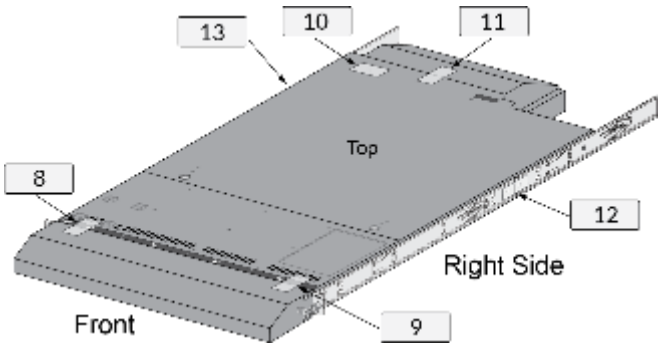

Figure 15. M-200: Seal locations on Top and Right Side

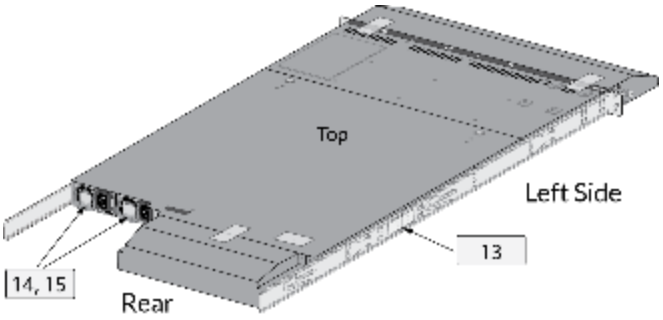

Figure 16. M-200: Seal Locations on Left Side and Rear

Surface Preparation: Clean the chassis of any grease, dirt, or oil before applying the tamper evident seals

Operator Responsible for Securing Unused Seals: Crypto Officer

Part Numbers: 920-000208

7.2.2 Panorama M-300

Number: Panorama M-300 requires 15 Tamper Seals

Placement: M-300 Tamper Seal Installation (15 Seals)

Replace the top cover with the FIPS top cover.

a. Remove the VOID WARRANTY label and cover screws (replacement label included in the kit).

M-300 appliance—Remove the Void Warranty label that covers the left top cover screw then use a Phillips-head screwdriver to remove both screws as indicated in the illustration.
b. Simultaneously depress the two (2) release buttons on top of the cover and slide the cover toward the back of the appliance to remove it.
c. Slide the physical kit top cover (does not have vents) on the appliance until the release buttons click. Reinsert and slide cover into position and secure with the two (2) screws.

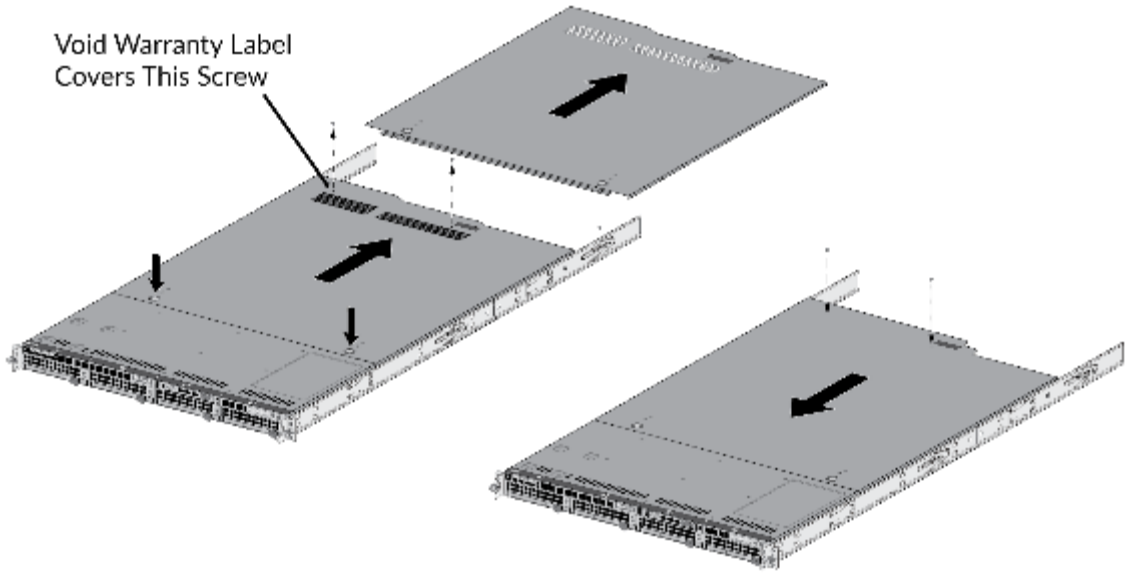

Figure 17. M-300: Top Cover Replacement

On the left side of the M-300, firmly apply seven (7) tamper-evident seals as indicated in the illustration.

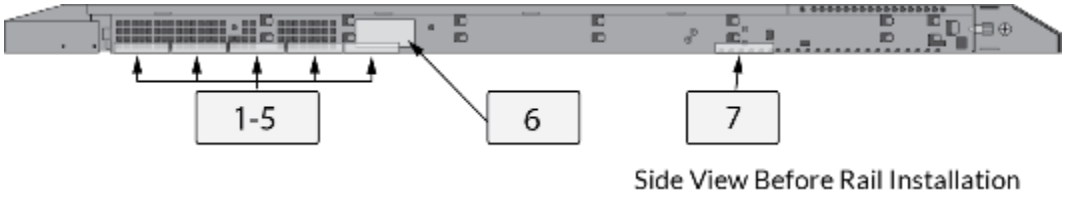

Figure 18. M-300: Side View Before Rail Installation

Install the inner rack mount rail brackets as described in the “M-300 and M-700 Appliance Hardware Reference”. The front rack bracket that you replace in the next step is located on the front inner rails.

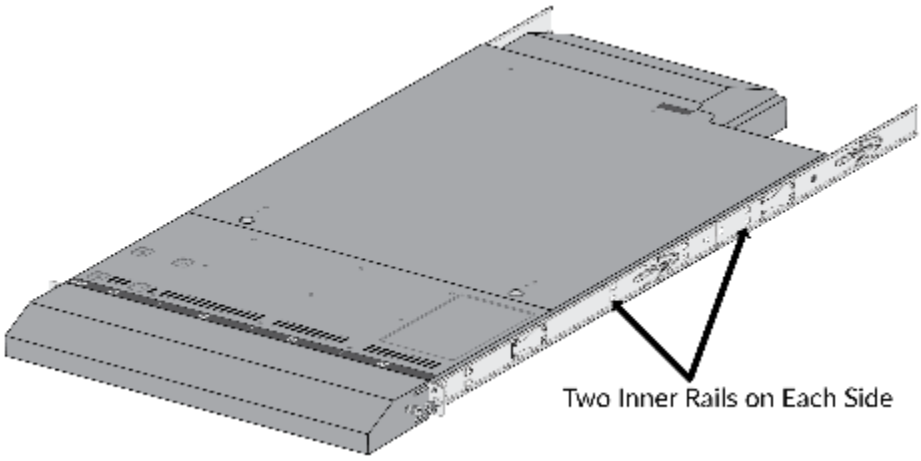

Figure 19. M-200: Inner Rack Mount Rail Brackets

Attach the physical kit front cover brackets.
Replace the front rack-mount brackets (one bracket on each side) that are part of the inner-rack rails with the physical kit rack-mount brackets by removing and then reinstalling two screws on each bracket. The physical kit handles have standoffs that are used to secure the front cover.

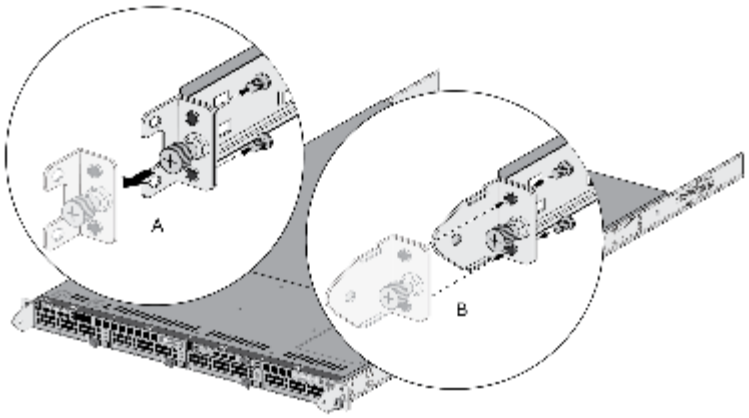

Figure 20. M-300: Replacing Front Rack-Mount Brackets

Attach the physical kit front cover to the front of the appliance.
Slide the M-300 physical kit front cover over the physical kit brackets and secure the cover by turning the thumb screws clockwise (one thumb screw on each side).

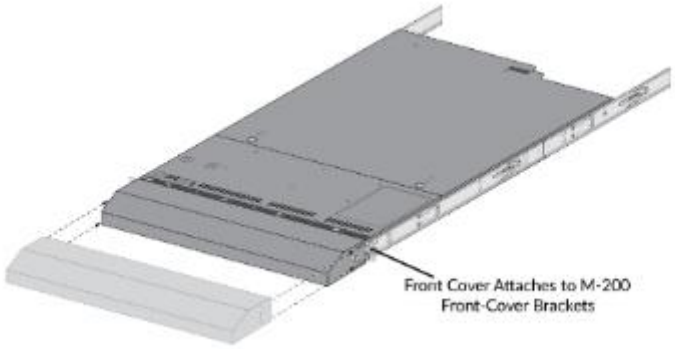

Figure 21. M-300: Attach Physical Kit Front Cover

Attach the physical kit back cover to the back of the appliance.
Slide the back cover onto the back of the appliance, insert two M4 x 0.7 x 8mm (one (1) screw on each side), and turn the screws clockwise to secure the cover.
Apply a tamper-evident seal to each location shown in the following M-300 illustrations.

Ensure you apply two (2) tamper-evident seals on the power supplies (see seals #14 and #15 on the rear illustration).

Note: Before you apply the tamper-evident seals, ensure that the appliance and physical kit surfaces are clean and dry. Firmly press one (1) seal on to each of the locations shown in the illustrations. Avoid touching the seals for at least 24 hours to allow time for the seals to properly adhere to the appliance and physical kit surfaces.

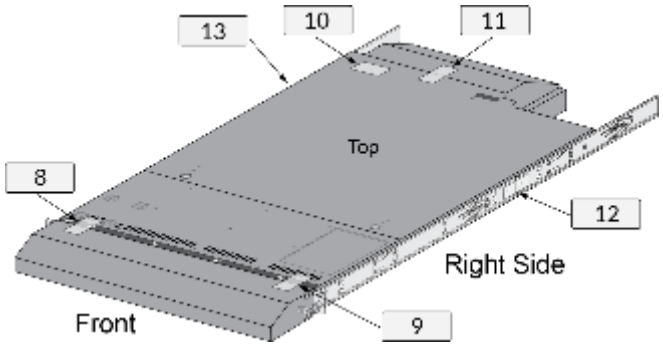

Figure 22. M-300: Seal locations on Top and Right Side

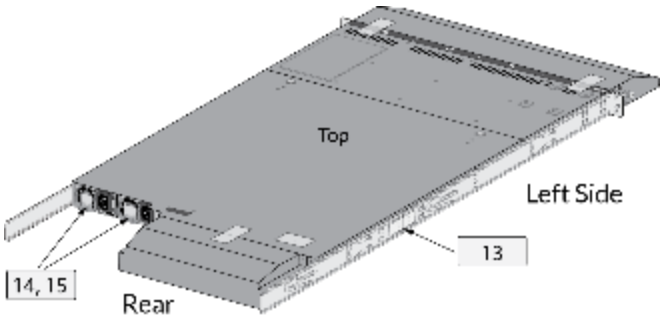

Figure 23. M-300: Seal Locations on Left Side and Rear

Surface Preparation: Clean the chassis of any grease, dirt, or oil before applying the tamper evident seals.

Operator Responsible for Securing Unused Seals: Crypto Officer

Part Numbers: 920-000319

7.2.3 Panorama M-600

Number: Panorama M-600 requires 21 Tamper Seals

Placement: M-600 Tamper Seal Installation (21 Seals)

Replace the top cover with the FIPS top cover.
Remove the VOID WARRANTY label and cover screws (replacement label included in the kit). Remove the Void Warranty label that covers the left side cover screw then use a Phillips-head screwdriver to remove both screws as indicated in the illustration.

b. Simultaneously depress the two (2) release buttons on top of the cover and slide the cover toward the back of the appliance to remove it.

c. Slide the physical kit top cover (does not have vents) on the appliance until the release buttons click. Replace the two screws that you removed from the old cover

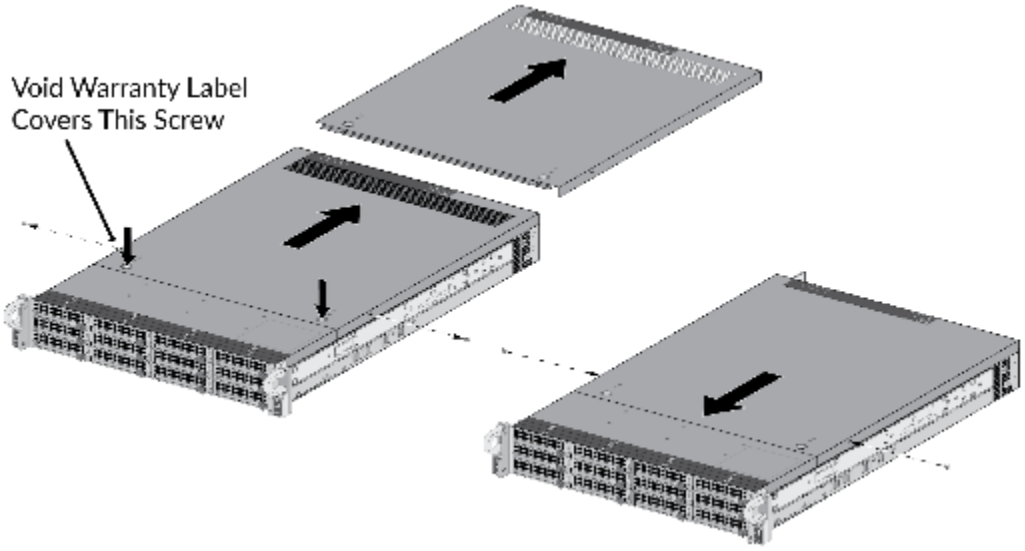

Figure 24. M-600: Top Cover Replacement

Attach the physical front cover brackets.

Remove the front pull handles by removing two (2) screws from each handle (one (1) handle on each side), insert the M-600 physical kit front-cover brackets under each handle, and then replace the handles and secure them using the screws that you removed. The physical kit handles have standoffs that are used to secure the front cover.

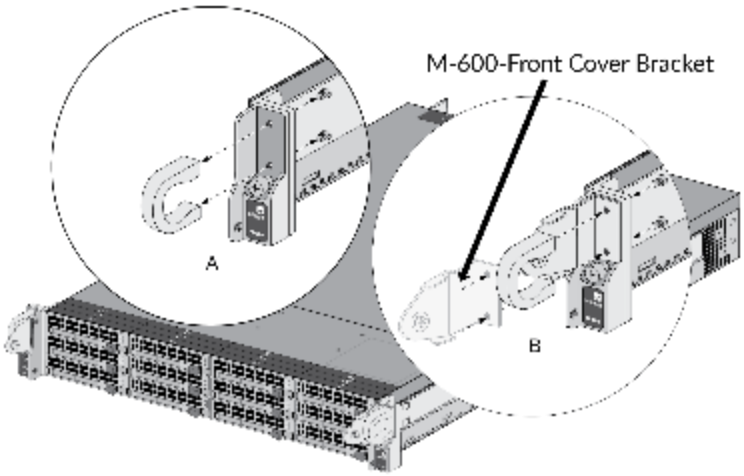

Figure 25. M-600: Front Cover Bracket

Attach the physical kit front cover to the front of the appliance.
Slide the M-600 physical kit front cover over the physical kit pull handle brackets and secure the cover by turning the thumb screws clockwise (one thumb screw on each side).

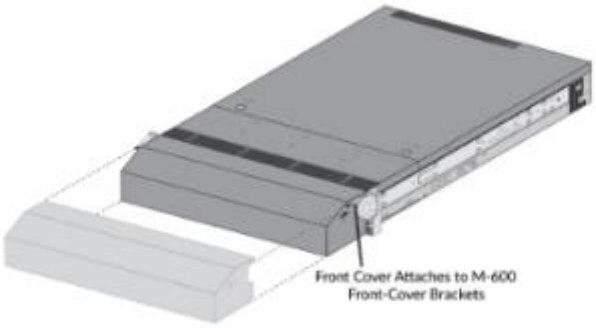

Figure 26. M-600: Physical Kit Front Cover

4. Install a tamper-evident seal on the back of the appliance. This is seal #13 in the M-600. You need to install this seal before you install the M-600 physical kit back cover. 5. Attach the physical kit back cover to the back of the appliance. a. Slide the back cover onto the back of the appliance and turn the two (2) thumb screws clockwise until tight (one (1) screw on each side) to secure the cover. 6. Apply a tamper-evident seal to each location shown in the following M-600 illustrations below. Also install the overlay stickers to cover vent openings (two (2) stickers on each side). You then install tamper-evident seals over the overlay stickers. Apply two (2) tamper-evident seals on the back side of the right rack handle (see seals #18 and #19 on the left side). Apply two (2) tamper-evident seals on the power supplies (see seals #11 and #12 with rear inset). Note: Before you apply the tamper-evident seals, ensure that the appliance and physical kit surfaces are clean and dry. Firmly press one (1) seal on to each of the locations shown in the illustrations. Avoid touching the seals for at least 24 hours to allow time for the seals to properly adhere to the appliance and physical kit surfaces.

M-600 Seal Placement (21 Seals)

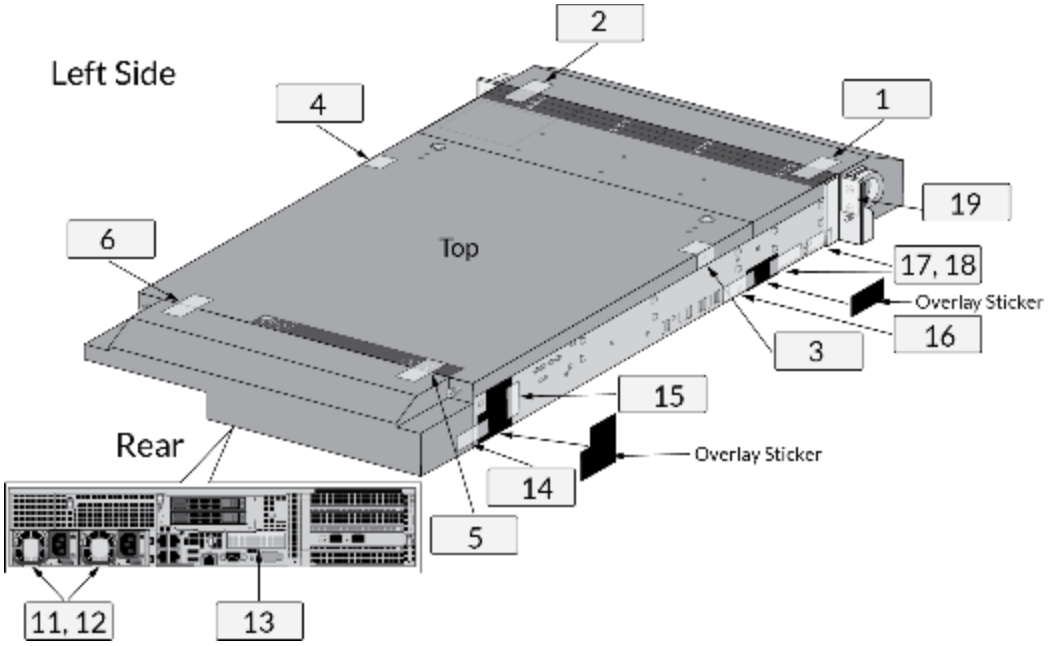

Figure 27. M-600: Tamper Seal Locations (Top and Rear)

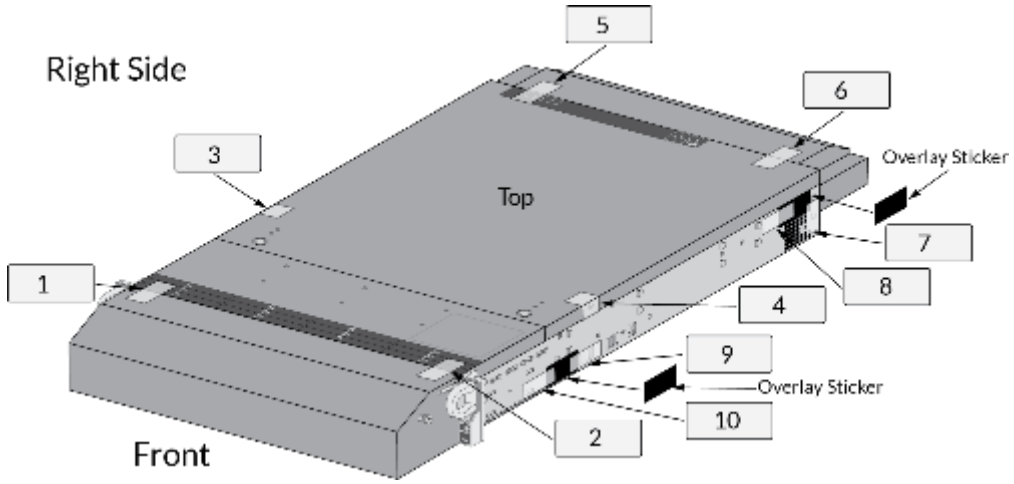

Figure 28. M-600: Tamper Seal Locations (Top and Front)

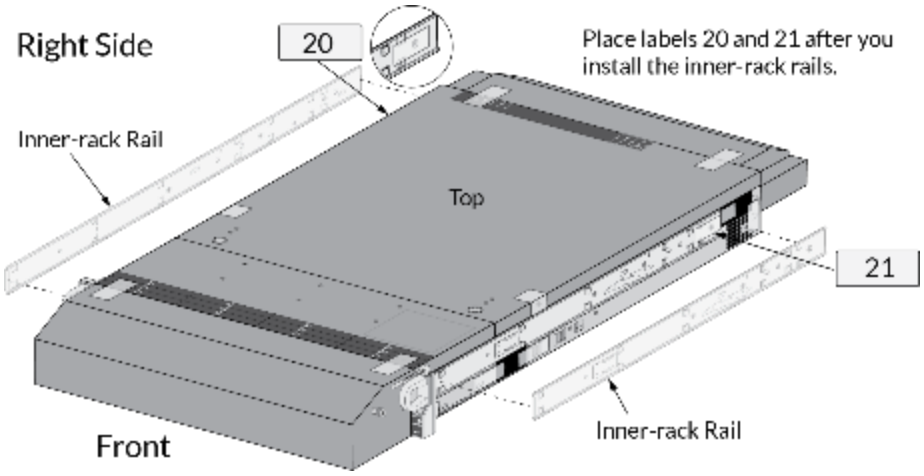

Figure 29. M-600: Tamper Seals Location for Side Rails

Surface Preparation: Clean the chassis of any grease, dirt, or oil before applying the tamper evident seals.

Operator Responsible for Securing Unused Seals: Crypto Officer

Part Numbers: 920-000209

7.2.4 Panorama M-700

Number: Panorama M-700 requires 21 Tamper Seals

Placement: M-700 Tamper Seal Installation (21 Seals)

1. Replace the top cover with the physical kit top cover.
a. Remove the VOID WARRANTY label and cover screws (replacement label included in the kit). Remove the Void Warranty label that covers the left side cover screw then use a Phillips-head screwdriver to remove both screws as indicated in the illustration.

b. Simultaneously depress the two (2) release buttons on top of the cover and slide the cover toward the back of the appliance to remove it.

c. Slide the physical kit top cover (does not have vents) on the appliance until the release buttons click. Replace the two screws that you removed from the old cover

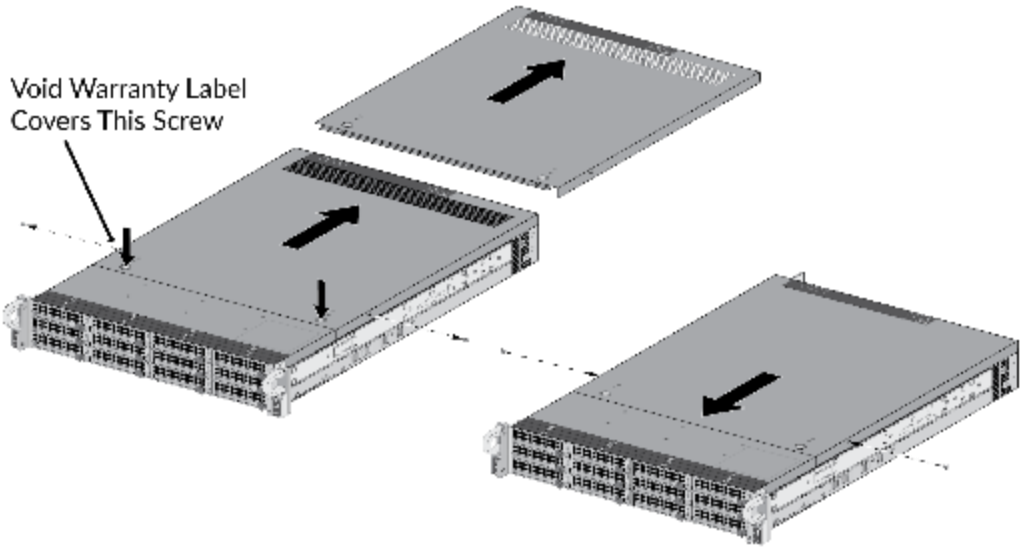

Figure 30. M-700: Top Cover Replacement

2. Attach the physical kit front cover brackets.

Remove the front pull handles by removing two (2) screws from each handle (one (1) handle on each side), insert the M-700 physical kit front-cover brackets under each handle, and then replace the handles and secure them using the screws that you removed. The physical kit handles have standoffs that are used to secure the front cover.

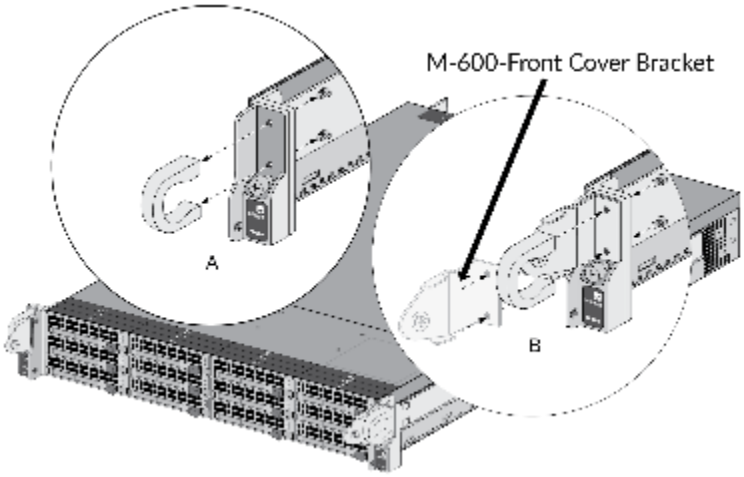

Figure 31. M-700: Front Cover Bracket

Attach the physical kit front cover to the front of the appliance. Slide the M-700 physical front cover over the physical kit pull handle brackets and secure the cover by turning the thumb screws clockwise (one thumb screw on each side).

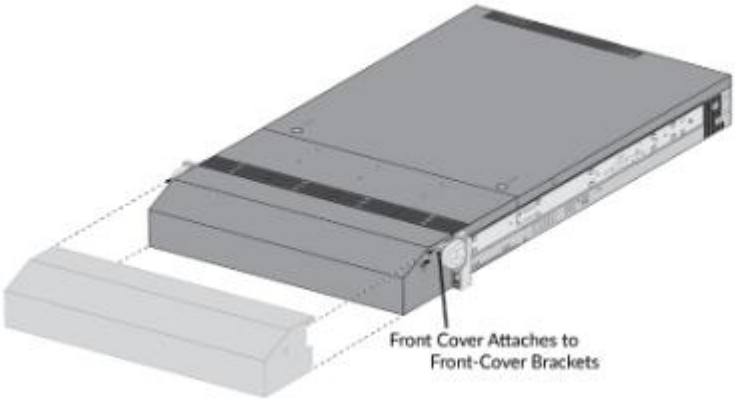

Figure 32. M-700: Physical Kit Front Cover

Install a tamper-evident seal on the back of the appliance. This is seal #13 in the M-700. You need to install this seal before you install the M-700 physical kit back cover.

5. Attach the physical kit back cover to the back of the appliance.

a. Slide the back cover onto the back of the appliance and turn the two (2) thumb screws clockwise until tight (one (1) screw on each side) to secure the cover.

6. Apply a tamper-evident seal to each location shown in the following M-700 illustrations below. Also install the overlay stickers to cover vent openings (two (2) stickers on each side). You then install tamper-evident seals over the overlay stickers. Apply two (2) tamper-evident seals on the back side of the right rack handle (see seals #18 and #19 on the left side). Apply two (2) tamper-evident seals on the power supplies (see seals #11 and #12 with rear inset).

Note: Before you apply the tamper-evident seals, ensure that the appliance and physical kit surfaces are clean and dry. Firmly press one (1) seal on to each of the locations shown in the illustrations. Avoid touching the seals for at least 24 hours to allow time for the seals to properly adhere to the appliance and physical kit surfaces.

M-700 Seal Placement (21 Seals)

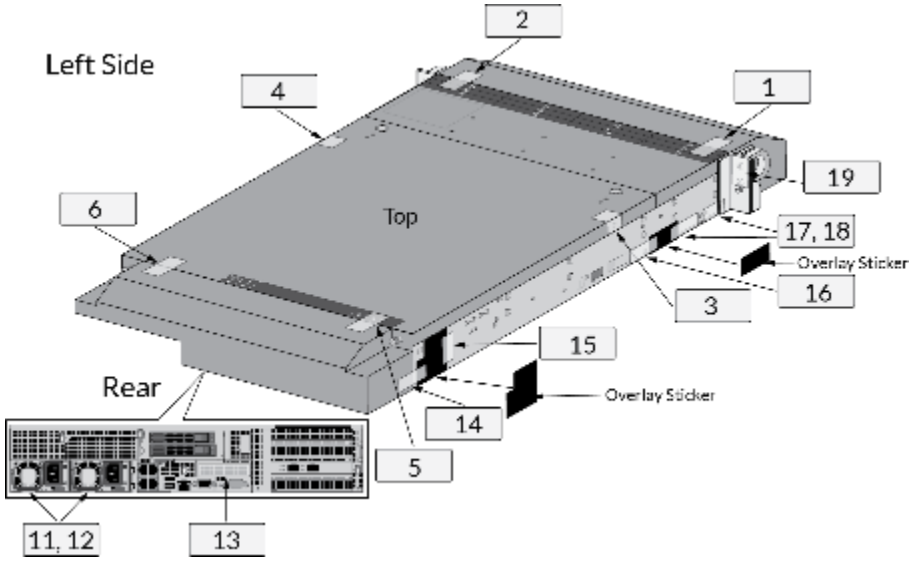

Figure 33. M-700: Tamper Seal Locations (Top and Rear)

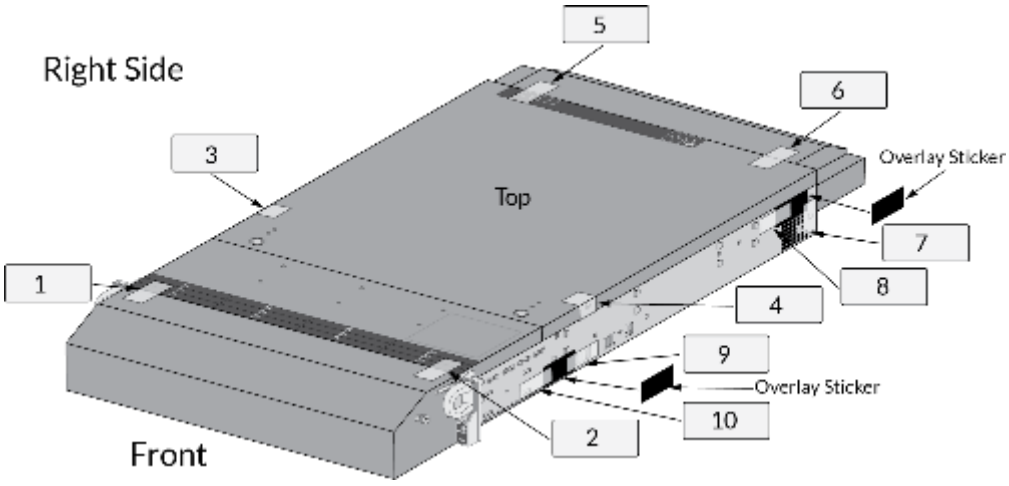

Figure 34. M-700: Tamper Seal Locations (Top and Front)

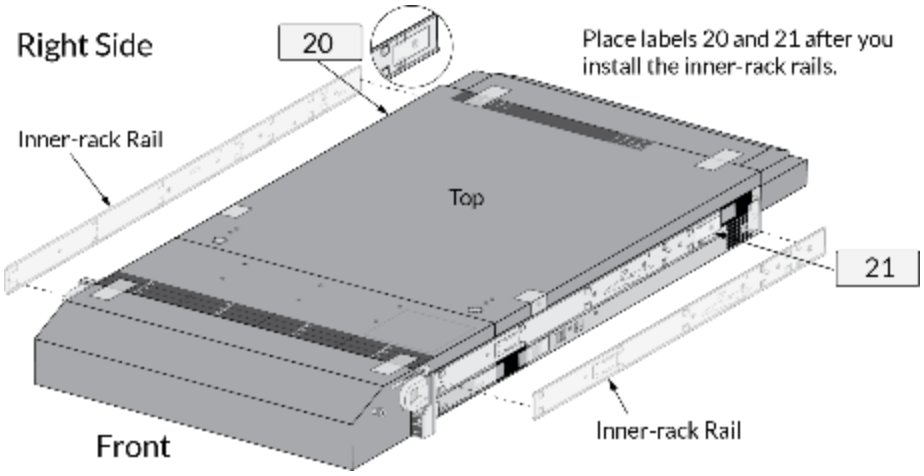

Figure 35. M-700: Tamper Seals Location for Side Rails

Surface Preparation: Clean the chassis of any grease, dirt, or oil before applying the tamper evident seals.

Operator Responsible for Securing Unused Seals: Crypto Officer

Part Numbers: 920-000318

8 Non-Invasive Security

N/A for this module.

9 Sensitive Security Parameters Management

9.1 Storage Areas

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

Table 14: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Module Public Key Output	HDD	External (outside of module's boundary)	Plaintext	Automated	Electronic	
Password/Secret Input via SSHv2 encrypted by AES and HMAC	External (outside of module's boundary)	HDD	Encrypted	Automated	Electronic	KTS (SSHv2 with AES and HMAC)
Password/Secret Input via SSHv2 encrypted by AES-GCM	External (outside of module's boundary)	HDD	Encrypted	Automated	Electronic	KTS (SSHv2 with AES-GCM)
Password/Secret Input via TLSv1.2 encrypted by AES and HMAC	External (outside of module's boundary)	HDD	Encrypted	Automated	Electronic	KTS (TLSv1.2 with AES and HMAC)
Password/Secret Input via TLSv1.2 encrypted by AES-GCM	External (outside of module's boundary)	HDD	Encrypted	Automated	Electronic	KTS (TLSv1.2 with AES-GCM)
Peer Public Key Input	External (outside of module's boundary)	HDD	Plaintext	Automated	Electronic	

Table 15: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Power Cycle/Session Termination	Operator powers the module off or session terminates	Powering off the module or terminating the session will	Command via CLI or WebUI or by unplugging module

Zeroization Method	Description	Rationale	Operator Initiation
		erase all SSPs stored in the RAM of the module.	
Zeroization Command	CO issues zeroization service	The zeroization command will erase all SSPs stored in the RAM or in the Flash of the module.	Entering into maintenance mode and selecting Factory Reset

Table 16: SSP Zeroization Methods

The following procedure will zeroize the module and must be performed under the control of the operator:

● Access the module's CLI via SSH and command the module to enter maintenance mode ("debug system maintenance-mode"); the module will reboot
● Note: Establish a serial connection to the console port
● After reboot, select "Continue."
● Select "Factory Reset"
● The module will perform a zeroization, and provide the following message once complete:
● "Factory Reset Status: Success"

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
CA Certificates	ECDSA/RSA Public key - Used to trust a root CA intermediate CA and leaf /end entity certificates (RSA 2048, 3072, and 4096 bits) (ECDSA P-256, P-384, and P-521)	2048 bits – 4096 bits; 128 - 256 bits - 112 bits, 128 bits, 150 bit; 128 bits, 192 bits, 256 bits	Public Key - PSP	TLS ECDSA KeyGen TLS RSA KeyGen		TLS ECDSA SigGen TLS ECDSA SigVer TLS RSA SigGen TLS RSA SigVer
CO, User Password	Authentication string with a minimum length of eight (8) characters.	8 characters minimum - N/A	Authentication Data - CSP			
DRBG Key	AES 256 CTR DRBG state Key used in	256 bits - 256 bits	DRBG Key - CSP	Counter DRBG (A2906)		Counter DRBG (A2906)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	the generation of a random values					
DRBG Seed	DRBG seed coming from the entropy source Seed length = 384 bits	384 bits - 256 bits	DRBG Seed - CSP	Entropy as per SP 800-90B		Counter DRBG (A2906)
DRBG V	AES 256 CTR DRBG state V used in the generation of a random values	128 bits - 128 bits	DRBG Internal State V value - CSP	Counter DRBG (A2906)		Counter DRBG (A2906)
ECDSA Private Keys	ECDSA Private key for generation of signatures and authentication (P-256, P-384, or P-521)	128 - 256 bits - 128 bits, 192 bits, 256 bits	Private Key - CSP	ECDSA KeyGen (FIPS186-4) (A2906)		TLS ECDSA SigGen
ECDSA Public Keys	ECDSA public keys managed as certificates for the verification of signatures, establishment of TLS, operator authentication and peer authentication. (ECDSA P-256, P-384, or P-521)	128 - 256 bits - 128 bits, 192 bits, 256 bits	Public Key - PSP	ECDSA KeyGen (FIPS186-4) (A2906)		TLS ECDSA SigVer
Entropy Input String	Entropy input string coming from the entropy source Input length = 384 bits	384 bits - 256 bits	- CSP	Entropy as per SP 800-90B		Counter DRBG (A2906)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Firmware integrity verification key	Used to check the integrity of all firmware code (HMAC-SHA-256 and ECDSA P-256) (Note: This is not considered an SSP)	128 bits - 128 bits	Integrity verification key - Neither	Pre-Loaded		
Protocol Secrets	Secrets used by RADIUS or TACACS+ (8 characters minimum)	8 characters minimum - N/A	Authentication Data - CSP			
Public key for firmware content load test	Used to authenticate firmware and content to be installed on the firewall (RSA 2048 with SHA-256)	112 bits - 112 bits	Public Key - PSP	Pre-Loaded		Firmware Load Test
RSA Private Keys	RSA Private keys for generation of signatures, authentication or key establishment. (RSA 2048, 3072, or 4096-bit)	2048 - 4096 bits - 112 bits, 128 bits, 150 bits	Private Key - CSP	RSA KeyGen (FIPS186-4) (A2906)		TLS RSA SigGen
RSA Public Keys	RSA public keys managed as certificates for the verification of signatures, establishment of TLS, operator authentication and peer authentication. (RSA 2048,	2048 - 4096 bits - 112 bits, 128 bits, 150 bits	Public Key - PSP	RSA KeyGen (FIPS186-4) (A2906)		TLS RSA SigVer

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	3072, or 4096-bit)					
SNMPv3 Authentication Key	HMAC-SHA-1/224/256/384/512 Authentication protocol key (160 bits)	160 bits, 224 bits, 256 bits, 384 bits, or 512 bits - 160 bits, 224 bits, 256 bits, 384 bits, or 512 bits	Session Key - CSP	KDF SNMP (A2906)		Session Authentication (SMPv3)
SNMPv3 Authentication Secret	Used to support SNMPv3 services (Minimum 8 characters)	8 characters minimum - N/A	Authentication Key - CSP			SNMPv3 Keying Materials Development
SNMPv3 Privacy Secret	Used to support SNMPv3 services (Minimum 8 characters)	8 characters minimum - N/A	Authentication Key - CSP			SNMPv3 Keying Materials Development
SNMPv3 Session Key	Privacy protocol encryption key (AES 128/192/256 CFB)	128 - 256 bits - 128 bits, 256 bits	Session Key - CSP	KDF SNMP (A2906)		Session Encryption/Decryption (SNMPv3)
SSH Client Public Key	Public RSA key used to authenticate client. (RSA 2048, 3072, and 4096 bits)	2048, 3072, 4096 bits - 112 bits, 128 bits, 150 bits	Public Key - PSP			SSH RSA SigVer

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
SSH DHE/ECDHE Private Components	Diffie Hellman or EC Diffie-Hellman private (DH Group 14, ECDH P-256, ECDH P-384, ECDH P-521)	2048 bits; 128 - 256 bits - 112 bits; 128 bits, 192 bits, 256 bits	Private Key - CSP	KAS-ECC-KeyGen (SSH) KAS-FFC-KeyGen (SSH)	KAS-ECC (SSH) KAS-FFC (SSH)	SSHv2 Keying Materials Development
SSH DHE/ECDHE Public Components	Diffie Hellman or EC Diffie-Hellman public component (DH Group 14, ECDH P-256, ECDH P-384, ECDH P-521)	2048 bits; 128 - 256 bits - 112 bits; 128 bits, 192 bits, 256 bits	Public Key - PSP	KAS-ECC-KeyGen (SSH) KAS-FFC-KeyGen (SSH)	KAS-ECC (SSH) KAS-FFC (SSH)	SSHv2 Keying Materials Development
SSH Host Public Key	SSH Host Public Key (RSA 2048, RSA 3072, RSA 4096, ECDSA P-256, P-384, or P-521)	2048 - 4096 bits; 128 - 256 bits - 112 bits, 128 bits, 150 bits; 128 bits, 192 bits, 256 bits	Public Key - PSP	SSH ECDSA KeyGen SSH RSA KeyGen		SSH ECDSA SigVer SSH RSA SigVer
SSH Session Authentication Keys	Authentication keys used in all SSH connections to the security module's command line interface (HMAC-SHA-	160, 256, or 512 bits - 160 bits, 256 bits, or 512 bits	Session Key - CSP	KDF SSH (A2906)	KAS-ECC (SSH) KAS-FFC (SSH)	Session Authentication (SSHv2)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	1, HMAC-SHA2-256, HMAC-SHA2-512) (160, 256, 512 bits)					
SSH Session Encryption Keys	Used in all SSH connections to the security module's command line interface. (128, 192, or 256 bits: AES CBC or CTR) (128 or 256 bits: AES GCM)	128 - 256 bits - 128 bits, 256 bits	Session Key - CSP	KDF SSH (A2906)	KAS-ECC (SSH) KAS-FFC (SSH)	Session Encryption/Decryption (SSH)
SSH Shared Secret	Diffie Hellman or EC Diffie-Hellman shared secret (DH MODP-2048, ECDH P-256, ECDH P-384, ECDH P-521)	128 - 512 bits - 128 - 256 bits	Shared Secret - CSP	KDF SSH (A2906)		KAS-ECC (SSH) KAS-FFC (SSH)
TLS DHE/ECDHE Private Components	Ephemeral Diffie-Hellman private FFC or EC component used in TLS (DHE 2048, ECDHE P-256, P-384, P-521)	2048 bits - 4096 bits 128 - 256 bits - 112 bits,128 bits, 150 bits; 128 bits, 192 bits, 256 bits	Private Key - CSP	KAS-ECC-KeyGen (TLSv1.2) KAS-FFC-KeyGen (TLSv1.2)	KAS-ECC-KeyGen (TLSv1.2) KAS-FFC-KeyGen (TLSv1.2)	TLSv1.2 Keying Materials Development
TLS DHE/ECDHE Public	Diffie_Hellman or EC Diffie-Hellman Ephemeral	2048 bits - 4096 bits	Public Key - PSP	KAS-ECC-KeyGen (TLSv1.	KAS-ECC (TLSv1.2)	TLSv1.2 Keying Materials Development

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Components	values used in key agreement (DHE 2048, ECDHE P-256, P-384, P-521)	128 - 256 bits - 112 bits, 128 bits, 150 bits; 128 bits, 192 bits, 256 bits		2) KAS-FFC-KeyGen (TLSv1.2)	KAS-FFC (TLSv1.2)	
TLS Encryption Keys	AES (128 or 256 bit) keys used in TLS connections (GCM; CBC)	128 - 256 bits - 128 bits, 256 bits	Session Key - CSP	KDF TLS (A2906)	KAS-ECC (TLSv1.2)	Session Encryption/Decryption (TLSv1.2)
TLS HMAC Keys	HMAC keys used in TLS connections (HMAC-SHA2-256/384) (256, 384 bits)	256 - 384 bits - - 256 bits, 384 bits	Session Key - CSP	KDF TLS (A2906)	KAS-ECC-KeyGen (TLSv1.2) KAS-FFC-KeyGen (TLSv1.2) KAS-ECC (TLSv1.2)	Session Authentication (TLSv1.2)
TLS Master Secret	Secret value used to derive the TLS session keys	384 bits - 384 bits	Master Secret - CSP	KDF TLS (A2906)	KAS-ECC (TLSv1.2) KAS-FFC (TLSv1.2)	TLSv1.2 Keying Materials Development
TLS Pre-Master Secret	Secret value used to derive the TLS Master Secret along with client and server random nonces	2048 bits; 256 bits, 384 bits, 521 bits - 112	Shared Secret - CSP	KDF TLS (A2906)	KAS-ECC (TLSv1.2) KAS-FFC (TLSv1.2)	TLSv1.2 Keying Materials Development

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		bits; 256 bits, 384 bits, 521 bits				

Table 17: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
CA Certificates	Peer Public Key Input Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM	RAM:Plaintext HDD:Plaintext	Duration of use	Zeroization Command Power Cycle/Session Termination	ECDSA Private Keys:Encrypts ECDSA Public Keys:Encrypts RSA Private Keys:Encrypts RSA Public Keys:Encrypts
CO, User Password	Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM	HDD:Obfuscated		Zeroization Command	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM				
DRBG Key		RAM:Plaintext	Duration of use	Power Cycle/Session Termination	Entropy Input String:Paired With DRBG Key:Paired With
DRBG Seed		RAM:Plaintext	Duration of use	Power Cycle/Session Termination	Entropy Input String:Paired With DRBG V:Paired With
DRBG V		RAM:Plaintext	Duration of use	Power Cycle/Session Termination	
ECDSA Private Keys	Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM	RAM:Plaintext HDD:Plaintext	Duration of use	Zeroization Command Power Cycle/Session Termination	ECDSA Public Keys:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
ECDSA Public Keys	Peer Public Key Input Module Public Key Output Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM	RAM:Plaintext HDD:Plaintext	Duration of use	Zeroization Command	ECDSA Private Keys:Paired With
Entropy Input String		RAM:Plaintext	Duration of use	Power Cycle/Session Termination	Entropy Input String:Paired With DRBG V:Paired With DRBG Key:Paired With
Firmware integrity verification key		HDD:Plaintext			
Protocol Secrets	Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by	HDD:Plaintext RAM:Plaintext	Duration of use	Zeroization Command	DRBG Seed:Paired With DRBG Key:Paired With DRBG V:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	AES-GCM Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM				
Public key for firmware content load test		HDD:Plaintext			
RSA Private Keys	Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM	RAM:Plaintext HDD:Plaintext	Duration of use	Zeroization Command Power Cycle/Session Termination	RSA Public Keys:Paired With
RSA Public Keys	Peer Public Key Input Module Public Key Output Password/Secret Input via TLSv1.2 encrypted by	RAM:Plaintext HDD:Plaintext	Duration of use	Zeroization Command	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM				
SNMPv3 Authentication Key		RAM:Plaintext HDD:Plaintext	Duration of use	Zeroization Command	SNMPv3 Authentication Secret:Derived From SNMPv3 Privacy Secret:Derived From
SNMPv3 Authentication Secret	Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM	RAM:Plaintext HDD:Plaintext	Duration of use	Zeroization Command	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
SNMPv3 Privacy Secret	Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM	RAM:Plaintext HDD:Plaintext	Duration of use	Zeroization Command	
SNMPv3 Session Key		RAM:Plaintext HDD:Plaintext	Duration of use	Zeroization Command	SNMPv3 Authentication Secret:Derived From SNMPv3 Privacy Secret:Derived From
SSH Client Public Key	Peer Public Key Input Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM Password/Secret Input via SSHv2 encrypted by AES and	RAM:Plaintext HDD:Plaintext	Duration of use	Zeroization Command	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM				
SSH DHE/ECDHE Private Components		RAM:Plaintext	Duration of use	Power Cycle/Session Termination	SSH DHE/ECDHE Public Components:Paired With
SSH DHE/ECDHE Public Components	Peer Public Key Input Module Public Key Output	RAM:Plaintext	Duration of use	Power Cycle/Session Termination	SSH DHE/ECDHE Private Components:Paired With
SSH Host Public Key		RAM:Plaintext HDD:Plaintext	Duration of use	Zeroization Command	
SSH Session Authentication Keys		RAM:Plaintext	Duration of use	Power Cycle/Session Termination	SSH DHE/ECDHE Public Components:Derived From SSH DHE/ECDHE Private Components:Derived From
SSH Session Encryption Keys		RAM:Plaintext	Duration of use	Power Cycle/Session Termination	SSH DHE/ECDHE Private Components:Derived From SSH DHE/ECDHE Public Components:Derived From
SSH Shared Secret		RAM:Plaintext	Duration of use	Power Cycle/Session Termination	
TLS DHE/ECDHE Private Components		RAM:Plaintext	Duration of use	Power Cycle/Session Termination	TLS DHE/ECDHE Public Components:Paired With
TLS DHE/ECDHE Public	Peer Public Key Input	RAM:Plaintext	Duration of use	Power Cycle/Sessi	TLS DHE/ECDHE Private

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Components	Module Public Key Output			on Termination	Components:Paired With
TLS Encryption Keys		RAM:Plaintext	Duration of use	Power Cycle/Session Termination	TLS Master Secret:Derived From
TLS HMAC Keys		RAM:Plaintext	Duration of use	Power Cycle/Session Termination	TLS Master Secret:Derived From
TLS Master Secret		RAM:Plaintext	Duration of use	Power Cycle/Session Termination	TLS Pre-Master Secret:Derived From
TLS Pre-Master Secret		RAM:Plaintext	Duration of use	Power Cycle/Session Termination	

Table 18: SSP Table 2

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
ECDSA SigVer (FIPS186-4) (A2906)	P-256	KAT	SW/FW Integrity	Self-Test successful	Signature Verification
HMAC-SHA2-256 (A2906)	SHA2-256	KAT	SW/FW Integrity	Self-Test successful	Keyed Checksum

Table 19: Pre-Operational Self-Tests

Verified with HMAC-SHA2-256 and ECDSA P-256
Note: the ECDSA and HMAC-SHA2-256 KATs are performed prior to the firmware integrity test

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB	128 Bits	KAT	CAST	Self-test output	Decrypt	After each power-on or via

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Decrypt (A2906)				message		self-test command
AES-GCM Decrypt (A2906)	256 Bits	KAT	CAST	Self-test output message	Decrypt	After each power-on or via self-test command
AES-GCM Encrypt (A2906)	256 Bits	KAT	CAST	Self-test output message	Encrypt	After each power-on or via self-test command
Counter DRBG (A2906)	N/A	KAT	CAST	Self-test output message	SP 800-90Arev1 Instantiate/Generate/Reseed Known Answer Tests	After each power-on or via self-test command
ECDSA / KAS-ECC	256 Bit Minimum	PCT	PCT	System log messages	ECDSA / KAS-ECC pairwise consistency test	On session
ECDSA SigGen (FIPS186-4) (A2906)	256 Bits	KAT	CAST	Self-test output message	Sign	After each power-on or via self-test command
ECDSA SigVer (FIPS186-4) (A2906)	256 Bits	KAT	CAST	Self-test output message	Verify	After each power-on or via self-test command
Firmware Load Test	2048 Bit	FW Load Test	SW/FW Load	System log messages	Firmware load test on content load	On session
HMAC-SHA-1 (A2906)	160 Bits	KAT	CAST	Self-test output message	Keyed Hash	After each power-on or via self-test command
HMAC-SHA2-224 (A2906)	224 Bits	KAT	CAST	Self-test output message	Keyed Hash	After each power-on or via self-test command
HMAC-SHA2-	256 Bits	KAT	CAST	Self-test output	Keyed Hash	After each power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
256 (A2906)				message		or via self-test command
HMAC-SHA2-384 (A2906)	384 Bits	KAT	CAST	Self-test output message	Keyed Hash	After each power-on or via self-test command
HMAC-SHA2-512 (A2906)	512 Bits	KAT	CAST	Self-test output message	Keyed Hash	After each power-on or via self-test command
KAS-ECC-SSC Sp800-56Ar3 (A2906)	256 Bits	KAT	CAST	Self-test output message	KAS Computation	After each power-on or via self-test command
Safe Primes Key Generation (A2906)	2048 Bits Minimum	PCT	PCT	System log messages	KAS-FCC pairwise consistency test	On session
KAS-FFC-SSC Sp800-56Ar3 (A2906)	2048 Bits	KAT	CAST	Self-test output message	KAS Computation	After each power-on or via self-test command
RSA	2048 Bits Minimum	PCT	PCT	System log messages	RSA pairwise consistency test	On session
RSA SigGen (FIPS186-4) (A2906)	2048 Bits	KAT	CAST	Self-test output message	Sign	After each power-on or via self-test command
RSA SigVer (FIPS186-4) (A2906)	2048 Bits	KAT	CAST	Self-test output message	Verify	After each power-on or via self-test command
SHA-1 (A2906)	160 Bits	KAT	CAST	Self-test output	Hash	After each power-on or via

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				message		self-test command
SHA2-256 (A2906)	256 Bits	KAT	CAST	Self-test output message	Hash	After each power-on or via self-test command
SHA2-384 (A2906)	384 Bits	KAT	CAST	Self-test output message	Hash	After each power-on or via self-test command
SHA2-512 (A2906)	512 Bits	KAT	CAST	Self-test output message	Hash	After each power-on or via self-test command
SP 800-90B RCT/APT Health Tests on Entropy Source	N/A	Fault-Detection	CAST	Self-test output message	Health tests done on entropy source	After each power-on or via self-test command
SP 800-135rev1 SSH KDF with SHA-256	N/A	KAT	CAST	Self-test output message	SSHv2 with SHA-256	After each power-on or via self-test command
SP 800-135rev1 TLS 1.2 with SHA-256 KDF	N/A	KAT	CAST	Self-test output message	TLSv1.2 with SHA-256	After each power-on or via self-test command
SP 800-56A Rev 3 Assurance Tests	N/A	Critical Functions	Critical Function	System log messages	Assurance tests for SP 800-56A Rev3	On session

Table 20: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ECDSA SigVer (FIPS186-4) (A2906)	KAT	SW/FW Integrity	On Demand	Manually or Scheduled
HMAC-SHA2-256 (A2906)	KAT	SW/FW Integrity	On Demand	Manually or Scheduled

Table 21: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-ECB Decrypt (A2906)	KAT	CAST	On Demand	Manually or Scheduled
AES-GCM Decrypt (A2906)	KAT	CAST	On Demand	Manually or Scheduled
AES-GCM Encrypt (A2906)	KAT	CAST	On Demand	Manually or Scheduled
Counter DRBG (A2906)	KAT	CAST	On Demand	Manually or Scheduled
ECDSA / KAS-ECC	PCT	PCT	On session	On session
ECDSA SigGen (FIPS186-4) (A2906)	KAT	CAST	On Demand	Manually or Scheduled
ECDSA SigVer (FIPS186-4) (A2906)	KAT	CAST	On Demand	Manually or Scheduled
Firmware Load Test	FW Load Test	SW/FW Load	On session	On session
HMAC-SHA-1 (A2906)	KAT	CAST	On Demand	Manually or Scheduled
HMAC-SHA2-224 (A2906)	KAT	CAST	On Demand	Manually or Scheduled
HMAC-SHA2-256 (A2906)	KAT	CAST	On Demand	Manually or Scheduled
HMAC-SHA2-384 (A2906)	KAT	CAST	On Demand	Manually or Scheduled
HMAC-SHA2-512 (A2906)	KAT	CAST	On Demand	Manually or Scheduled
KAS-ECC-SSC Sp800-56Ar3 (A2906)	KAT	CAST	On Demand	Manually or Scheduled
Safe Primes Key Generation (A2906)	PCT	PCT	On session	On session
KAS-FFC-SSC Sp800-56Ar3 (A2906)	KAT	CAST	On Demand	Manually or Scheduled
RSA	PCT	PCT	On session	On session

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA SigGen (FIPS186-4) (A2906)	KAT	CAST	On Demand	Manually or Scheduled
RSA SigVer (FIPS186-4) (A2906)	KAT	CAST	On Demand	Manually or Scheduled
SHA-1 (A2906)	KAT	CAST	On Demand	Manually or Scheduled
SHA2-256 (A2906)	KAT	CAST	On Demand	Manually or Scheduled
SHA2-384 (A2906)	KAT	CAST	On Demand	Manually or Scheduled
SHA2-512 (A2906)	KAT	CAST	On Demand	Manually or Scheduled
SP 800-90B RCT/APT Health Tests on Entropy Source	Fault-Detection	CAST	On Demand	Manually or Scheduled
SP 800-135rev1 SSH KDF with SHA-256	KAT	CAST	On Demand	Manually or Scheduled
SP 800-135rev1 TLS 1.2 with SHA-256 KDF	KAT	CAST	On Demand	Manually or Scheduled
SP 800-56A Rev 3 Assurance Tests	Critical Functions	Critical Function	On session	On session

Table 22: Conditional Periodic Information

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Conditional Firmware Load Test Failure	Signature verification fails on firmware load	Signature verification failure	N/A	System prints Invalid image message.
Conditional Pairwise Consistency or Critical Functions Test Failure	Module fails a PCT or critical functions test	PCT / Critical functions test	Reset session	System log prints an error message.
Self-Test / Integrity Test Failure	Module fails a self-test or integrity test	Self-test or Integrity Test failure	Reboot Module or Factory Reset	FIPS-CC mode failure. <Algorithm test> failed.

Table 23: Error States

Data output shall be inhibited during self-tests and error states.

10.5 Operator Initiation of Self-Tests

Perform a power cycle or via the 'Self-Tests' service by entering CLI command "request restart system"

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The following procedure will put the modules into the Approved mode of operation:

- Install physical kit opacity shields and tamper evidence seals according to the Physical Security Policy section. Physical kits must be correctly installed to operate in the Approved mode of operation. The tamper evidence seals and opacity shields shall be installed for the module to operate in the Approved mode of operation.
- During initial boot up, break the boot sequence via the console port connection (by pressing the maint button when instructed to do so) to access the main menu.
- Select "Continue."
- Select the "Set FIPS-CC Mode" option to enter the Approved mode.
- Select "Enable FIPS-CC Mode".
- When prompted, select "Reboot" and the module will re-initialize and continue into "FIPS-CC" mode (Approved mode).
- The module will reboot.
- In "FIPS-CC" mode, the console port is available as a status output port.
- Once the module has finished booting, the Crypto Officer can authenticate using the default credentials that come with the module
    - Once authenticated, the module will automatically require the operator to change their password; and the default credential is overwritten

The module will automatically indicate the Approved mode of operation in the following manner:

- Status output interface will indicate "**** FIPS-CC MODE ENABLED ****" via the CLI session.
- Status output interface will indicate "FIPS-CC mode enabled successfully" via the console port.
- The module will display "FIPS-CC" at all times in the status bar at the bottom of the web interface.

Should one or more power-up self-tests fail, the Approved mode of operation will not be achieved. Feedback will consist of:

- The module will output "FIPS-CC failure"
- The module will reboot and enter a state in which the reason for the reboot can be determined.
- To determine which self-test caused the system to reboot into the error state, connect the console cable and follow the on-screen instructions to view the self-test output.

Note: Disabling FIPS-CC mode causes a complete factory reset, which is described in section 11.6.

Non-Compliant State

Failure to follow the directions in the Approved Mode of Operation above or rules noted in Section 11 will result in the module operating in a non-compliant state, which is considered out of scope of this validation.

11.2 Administrator Guidance

The Administrator Guidance can be obtained from Palo Alto Network's public site:
https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin

https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/advanced-url-filtering/advanced-url-filtering-administration.pdf

To place the module in a configuration that supports logging capabilities or URL categorization (PAN-DB), refer to the Administrator Guidance documents noted above.

11.3 Non-Administrator Guidance

N/A for this module.

11.4 Design and Rules

In FIPS-CC mode, the following rules shall apply:

- When FIPS-CC mode is enabled, the operator shall not install plugins.
  - Checked via CLI using "show plugins installed"
- When FIPS-CC mode is enabled, the operator shall not use TACACS+. RADIUS may be used but must be protected by TLS protocol.
  - Checked via CLI using "show deviceconfig" command

11.5 End of Life

The following procedure will zeroize the module:

- Access the module's CLI via SSH, and command the module to enter maintenance mode; the module will reboot
  - Note: Establish a serial connection to the console port
- After reboot, select "Continue."
- Select "Factory Reset"
- The module will perform a zeroization, and provide the following message once complete:
  - "Factory Reset Status: Success"

Note: Following the completion of this procedure, the module will be placed back into an uninitialized state.

12 Mitigation of Other Attacks

N/A for this module.