Panorama 8.1 M-100, M-200, M-500 and M-600

FIPS 140-2 Non-Proprietary Security Policy

Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com

Date: 6/5/2019

Change Record

Table 1 - Change Record

Date	Author	Description of Change
8/02/2018	Quang Trinh	Initial Authoring
9/21/2018	Quang Trinh	Add FIPS Kits description for M-200 and M-600
10/18/2018	Quang Trinh	Update based on physical security testing, add CAVP algorithm certificates
11/16/2018	Quang Trinh	Update based on operational testing
12/18/2018	Quang Trinh	Update based on UL comments
6/5/2019	Quang Trinh	Updates to address CMVP comments

Contents

1 Module Overview 7
2 Mode of Operation 12
2.1 FIPS 140-2 Approved Mode of Operation 12
2.2 Selecting Panorama, Management-Only, and PAN-DB Approved modes of operation 13
2.3 Security Levels for the Panorama Mode, Management-Only Mode, and the PAN-DB Mode 14
2.4 Selecting Panorama Log Collector Approved Mode of Operation 15
2.5 Security Level for Panorama Log Collector Mode 15
2.6 Non-Approved Mode of Operation 16
2.7 Approved and Allowed Algorithms 16
2.8 Non-Approved, Non-Allowed Algorithms in Non-Approved Mode 20
3 Ports and Interfaces 21
4 Identification and Authentication Policy 29
4.1 Assumption of Roles 29
5 Security Parameters 31
6 Access Control Policy 33
6.1 Roles and Services 33
6.2 Unauthenticated Services 37
7 Operational Environment 38
8 Security Rules 38
9 Physical Security Policy 41
9.1 Physical Security Mechanisms 41
9.2 Operator Required Actions 42
10 Mitigation of Other Attacks Policy 43
11 References 43
12 Definitions and Acronyms 43
Appendix A – M-100 - FIPS Accessories/Tamper Seal Installation (28 Seals) 44
Appendix B – M-200 - FIPS Accessories/Tamper Seal Installation (Fifteen (15) Seals) 50
Appendix C – M-500 - FIPS Accessories/Tamper Seal Installation (12 Seals) 54
Appendix D – M-600 - FIPS Accessories/Tamper Seal Installation (21 Seals) 62

Tables

Table 1 - Change Record 2
Table 2 – Validated Version Information 12
Table 3 – Module Security Level Specification 14
Table 4 – Module Security Level Specification 15
Table 5 – FIPS Approved Algorithms Used in Current Module 16
Table 6 - FIPS Allowed Algorithms Used in Current Module 19
Table 7 - Supported Protocols in FIPS Approved Mode 20
Table 8 - Non-Approved, Non-Allowed Algorithms Used in Current Module 20
Table 9 – M-100 FIPS 140-2 Ports and Interfaces 22
Table 10 – M-200 FIPS 140-2 Ports and Interfaces 23
Table 11 – M-200 FIPS 140-2 Ports and Interfaces 24
Table 12 – M-500 Ports and Interfaces 25
Table 13 – M-600 Front Ports and Interfaces 27
Table 14 – M-600 Back Ports and Interfaces 28
Table 15 – Panorama or Management-Only Mode - Roles and Required Identification and Authentication 29
Table 16 - Log Collector Mode - Role and Required Identification and Authentication 29
Table 17 - PAN-DB Mode - Role and Required Identification and Authentication 30
Table 18 - Strengths of Authentication Mechanisms 30
Table 19 - Private Keys and CSPs 31
Table 20 - Public Keys 32
Table 21 - Authenticated Services – Panorama M-100/M-200/M-500/M-600 Manager (Panorama or Management-Only Mode) 34
Table 22 - Authenticated Services – Panorama M-100/M-200/M-500/M-600 Log Collector Mode 36
Table 23 - Authenticated Services – Panorama M-500/M-600 Private Pan-DB Mode 37
Table 24 - Unauthenticated Services 37
Table 25 - Inspection/Testing of Physical Security Mechanisms 42

Figures

Figure 1 – Front of M-100 7
Figure 2 – Front of M-100 with FIPS Kit 8
Figure 3 – Rear of M-100 with FIPS Kit 8
Figure 4 – Front of M-200 8
Figure 5 – Front of M-200 with FIPS Kit 8
Figure 6 – Rear of M-200 with FIPS Kit 9
Figure 7 –Front of M-500 9
Figure 8 – Front of M-500 with FIPS Kit 9

Figure 9 – Rear of M-500 with FIPS Kit 10
Figure 10 – Right Side of M-500 with FIPS Kit 10
Figure 11 – Left Side of M-500 with FIPS Kit 10
Figure 12 –Front of M-600 10
Figure 13– Front of M-600 with FIPS Kit 11
Figure 14 – Rear of M-600 with FIPS Kit 11
Figure 15 – Right Side of M-600 with FIPS Kit 11
Figure 16 – Left Side of M-600 with FIPS Kit 11
Figure 17 – M-100 Ports and Interfaces (Front and Back) 21
Figure 18 – M-200 Front Panel Ports and Interfaces 23
Figure 19 – M-200 Back Panel Ports and Interfaces 24
Figure 20 – M-500 Front Panel Ports and Interfaces 25
Figure 21 – M-500 Back Panel Ports and Interfaces 25
Figure 22 – M-600 Front Panel Ports and Interfaces 27
Figure 23 – M-600 Back Panel Ports and Interfaces 28
Figure 24 – M-100: Remove Screws on Rear Side 44
Figure 25 – M-100: Attach Rear Opacity Shield 45
Figure 26 – M-100: Apply Tamper Seals and Vent Overlays 46
Figure 27 – M-100: Apply Rail Kit 47
Figure 28 – M-100: Remove Front Plastic Bracket Covers and Screws 47
Figure 29 – M-100: Install Front Opacity Shield 48
Figure 30 – M-100: Install Outer Rails 49
Figure 31 – M-200: Top Cover Replacement 50
Figure 32 – M-200: Side View Before Rail Installation 51
Figure 33 – M-200: Inner Rack Mount Rail Brackets 51
Figure 34 – M-200: Replacing Front Rack-Mount Brackets 52
Figure 35 – M-200: Attach FIPS Front Cover 52
Figure 36 – M-200: Seal locations on Top and Right Side 53
Figure 37 – M-200: Seal Locations on Left Side and Rear 53
Figure 38 – M-500: Remove Front Handles and Modules 54
Figure 39 – M-500: Secure the Front Brackets 55
Figure 40 – M-500: Attach Pull Handles and Front Modules 55
Figure 41 – M-500: Install Front Opacity Shield 56
Figure 42 – M-500: Front Opacity Shield Installed 56
Figure 43 – M-500: Install Rear Opacity Shield Tray 57
Figure 44 – M-500: Install Rear Opacity Shield 58
Figure 45 – M-500: Apply Vent Overlays 59
Figure 46 – M-500: Apply Tamper Seals on Vent Overlays and Side Opening 59
Figure 47 – M-500: Install Rail Kit 60
Figure 48 – M-500: Apply Tamper Seals on the Bottom of the Appliance 60

Figure 49 – M-500: Apply Tamper Seals on the Top and Sides of the Appliance 61
Figure 50 – M-600: Top Cover Replacement 62
Figure 51 – M-600: Front Cover Bracket 63
Figure 52 – M-600:FIPS Front Cover 63
Figure 53 – M-600: Tamper Seal Locations (Top and Rear) 64
Figure 54 – M-600: Tamper Seal Locations (Top and Front) 65
Figure 55 – M-600:Tamper Seals Location for Side Rails 65

1 Module Overview

Panorama 8.1 M-100, M-200, M-500 and M-600 module 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 management appliances' individual management and logging components can be separated in a distributed manner to accommodate large volumes of log data. Panorama 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.
    - 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.
    - Management-Only: Providing the ability to perform all functions of Panorama with the exception of logging.
    - 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-500 and M-600 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-500/M-600 appliances as PAN-DB servers within your network or data center.

The Palo Alto Networks Panorama management appliances are multi-chip standalone modules, and are shown in the figures below. The M-100 is demonstrated in Figure 1 through Figure 3, M-200 is demonstrated in Figure 4 through Figure 6, the M-500 is demonstrated in Figure 7 through Figure 11, and M-600 is demonstrated in Figure 12 through Figure 16. The cryptographic boundary is defined by the external perimeter of the appliance including the FIPS kit.

M-100

Figure 1 – Front of M-100

Figure 2 – Front of M-100 with FIPS Kit

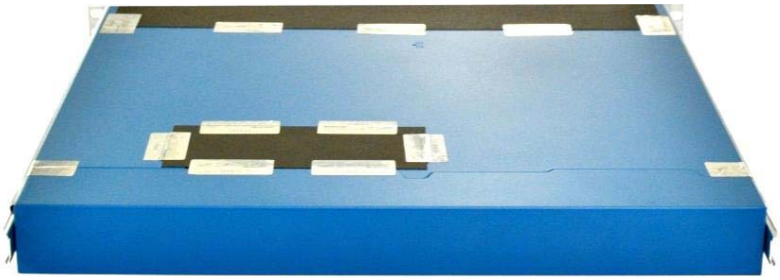

Figure 3 – Rear of M-100 with FIPS Kit

M-200

Figure 4 – Front of M-200

Figure 5 – Front of M-200 with FIPS Kit

Figure 6 – Rear of M-200 with FIPS Kit

M-500

Figure 7 –Front of M-500

Figure 8 – Front of M-500 with FIPS Kit

Figure 9 – Rear of M-500 with FIPS Kit

Figure 10 – Right Side of M-500 with FIPS Kit

Figure 11 – Left Side of M-500 with FIPS Kit

M-600

Figure 12 –Front of M-600

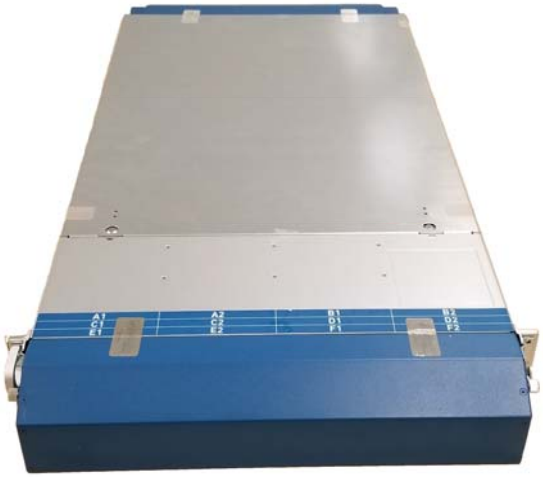

Figure 13– Front of M-600 with FIPS Kit

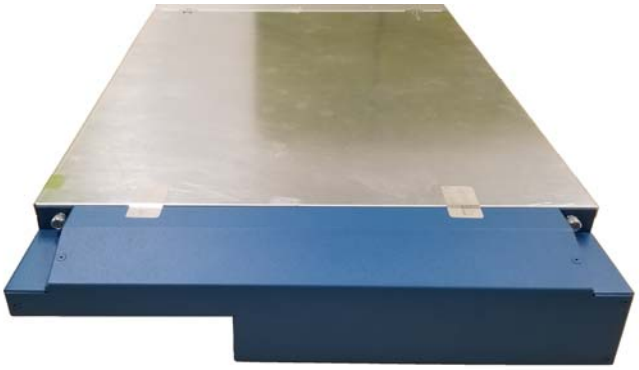

Figure 14 – Rear of M-600 with FIPS Kit

Figure 15 – Right Side of M-600 with FIPS Kit

Figure 16 – Left Side of M-600 with FIPS Kit

Details regarding the versioning and hardware are displayed in Table 2 below.

Table 2 – Validated Version Information

Module	Part Number	Hardware Version	FIPS Kit Part Number	FIPS Kit Version	Firmware Version
Panorama M-100 1TB RAID: 2 x 1TB RAID Certified HDD for 1TB of RAID Storage	910-000030	00D	920-000140	00A	8.1.6
Panorama M-100 4TB RAID: 8 x 1TB RAID Certified HDD for 4TB of RAID Storage	910-000092	00D	920-000140	00A	8.1.6
Panorama M-200	910-000176	00A	920-000208	00A	8.1.6
Panorama M-500	910-000073	00D	920-000145	00A	8.1.6
Panorama M-600	910-000175	00A	920-000209	00A	8.1.6

2 Mode of Operation

2.1 FIPS 140-2 Approved Mode of Operation

The module provides both FIPS 140-2 Approved and non-Approved modes of operation. The module is configured during initialization to operate only in an Approved or non-Approved mode of operation when in the operational state. The module cannot alternate service by service between Approved and non-Approved modes of operation.

The following procedure will configure the Approved mode of operation:

- The tamper evidence seals and opacity shields must be installed as per Section 9. The FIPS kit must be correctly installed to operate in the Approved mode of operation.
- During initial boot up, break the boot sequence via the console port connection (by entering 'maint' 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 the Approved mode.
- The module will reboot.
- In the Approved mode, the console port is available only as a status output port.

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.

2.2 Selecting Panorama, Management-Only, and PAN-DB Approved Modes of Operation

Panorama appliances support multiple configurations that provide varying services. The Cryptographic Officer can initialize the module into different Approved modes of operation. The primary and default mode of operation is the Panorama mode. The Management-Only mode of operation is the same as Panorama mode except there is no log collecting service. The Log Collector mode of operation is a secondary mode that provides a focused log collecting and forwarding capability. Directions to convert the appliance into the Log Collector mode are discussed below in Section 2.4. The M-500 and M-600 provide a fourth mode, PAN-DB Private Cloud server.

Convert the M-100/M-200/M-500/M-600 appliance from Panorama mode to the Management-Only mode:

- Log into the CLI via SSH
- Enter “request system system-mode management-only”
- Enter “Y” to confirm the change to Management-Only mode.
- The system will reboot and perform the required power on self-tests.

Convert the M-100/M-200/M-500/M-600 appliance from Management-Only mode to the Panorama mode:

- Log into the CLI via SSH
- Enter “request system system-mode panorama”
- Enter “Y” to confirm the change to Panorama mode.
- The system will reboot and perform the required power on self-tests.

Convert the M-500/M-600 appliance from Panorama Manager mode to the dedicated PAN-DB Private Cloud mode:

- Log into the CLI via SSH
- Enter “request system system-mode panurldb”
- Enter “Y” to confirm the change to PAN-DB Private Cloud mode.
- The system will reboot and perform the required power on self-tests.

Convert the M-500/M-600 appliance from PAN-DB mode to the Panorama Manager mode:

- Log into the CLI via SSH
- Enter “request system system-mode panorama”
- Enter “Y” to confirm the change to Panorama mode.
- The system will reboot and perform the required power on self-tests.

2.3 Security Levels for the Panorama Mode, Management-Only Mode, and the PAN-DB Mode

The cryptographic modules meet the overall requirements applicable to Level 2 security of FIPS 140-2.

Table 3 – Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	2
Module Ports and Interfaces	2
Roles, Services and Authentication	3
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A
Note: When initialized in Panorama, Management-Only, or PAN-DB Private Cloud mode, the module supports Level 3, identity based authentication.	

2.4 Selecting Panorama Log Collector Approved Mode of Operation

Convert the M-100/M-200/M-500/M-600 appliance from Panorama mode to the dedicated Panorama Log Collector mode:

- Log into the CLI via SSH
- Enter “request system system-mode logger”
- Enter “Y” to confirm the change to Panorama Log Collector mode.
- The system will reboot and perform the required power on self-tests.

Convert the M-100/M-200/M-500/M-600 appliance from Panorama Log Collector mode to the Panorama mode:

- Log into the CLI via SSH
- Enter “request system system-mode panorama”
- Enter “Y” to confirm the change to Panorama mode.
- The system will reboot and perform the required power on self-tests.

2.5 Security Level for Panorama Log Collector Mode

The cryptographic modules meet the overall requirements applicable to Level 2 security of FIPS 140-2.

Table 4 – Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	2
Module Ports and Interfaces	2
Roles, Services and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A
When initialized in Panorama Log Collector mode, the module supports Level 2 role based authentication.	

2.6 Non-Approved Mode of Operation

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

- During initial boot up, break the boot sequence via the console port connection (by entering 'maint' 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 "Disable FIPS-CC Mode".
- When prompted, select "Reboot" and the module will re-initialize and continue into the Approved mode.
- The module will reboot.

2.7 Approved and Allowed Algorithms

The cryptographic module supports the following FIPS Approved algorithms in all the Approved modes.

Table 5 – FIPS Approved Algorithms Used in Current Module

FIPS Approved Algorithm	CAVP Cert. #
AES [FIPS 197, SP800-38A]: Functions: Encryption, Decryption ECB, CBC, CTR modes; Encrypt/Decrypt; 128, 192 and 256-bit CFB128 mode; Encrypt/Decrypt; 128-bit Note: AES-OFB, AES-CFB1, AES-CFB8 and AES-CFB128 (192, 256 bit) were also tested but are not available for use	5890
AES-CCM [SP800-38C]: Encrypt and Decrypt, 128-bit Note: AES-CCM was tested but is not used by the module except for the self-test.	5890
AES-GCM [SP800-38D]: Encrypt and Decrypt, 128 and 256-bit Note 1: GCM IV handling is compliant with FIPS IG A.5 and SP800-38D.** Note 2: GCM 192-bit was tested but is not used by the module.	5890
CKG: Function: Key Generation Method 1: Asymmetric Key Generation; SP800-133 §6, seed results from an unmodified DRBG output	Vendor Affirmed

FIPS Approved Algorithm	CAVP Cert. #
Method 2: Symmetric Key Generation; SP800-133 §7.1 (symmetric key results from an unmodified DRBG output), §7.2, and §7.3	
CVL: ECDSA Signature Generation • P-256 SHA: SHA-224, SHA-256, SHA-384, SHA-512 • P-384 SHA: SHA-224, SHA-256, SHA-384, SHA-512 Note: P-224 was tested, but not used by the module	2122
CVL: Elliptical Curve Diffie-Hellman Exchange [SP800-56A] -ECC CDH Primitive (Section 5.7.1.2) - P-256, P-384, P-521 -KAS-ECC all except KDF	2119
CVL: Diffie-Hellman Exchange [SP800-56A] KAS-FFC all except KDF - Parameter sets: FB and FC	2119
CVL: KDF, Application Specific [SP800-135] -TLS 1.0/1.1/1.2 KDF -SNMPv3 KDF -SSHv2 KDF Note: - IKE v1/v2 KDF were tested but are not used by the module.	2120
CVL: RSA [SP800-56B] Function: Key Transport -RSADP	2121
DRBG [SP800-90A] -CTR DRBG with AES-256 Derivation function enabled.	2451
DSA [FIPS 186-4] -Key Generation: 2048 bits -Prerequisite to CVL #2119	1485
ECDSA [FIPS 186-4] - Key Pair Generation P-256, P-384 and P-521 - PKV P-256, P-384, and P-521 - Signature Generation P-256, P-384 and P-521; with all SHA-2 sizes* - Signature Verification P-256, P-384 and P-521; with SHA-1 and all SHA-2 sizes* Note: P-224 was tested, but not used by the module	1570

FIPS Approved Algorithm	CAVP Cert. #
*Does not include the "short SHA-512" sizes SHA-512/224 or SHA-512/256	
HMAC [FIPS 198] - HMAC-SHA-1 with λ=96, 160 - HMAC-SHA-256 with λ=256 - HMAC-SHA-384 with λ=384 - HMAC-SHA-512 with λ=512	3865
KAS: SP 800-56A Rev.2 Elliptic Curve Diffie-Hellman Exchange (CVL Certs. #2119 and #2120, vendor affirmed; key agreement; key establishment methodology provides between 128 and 256 bits of encryption strength)	Vendor Affirmed
SP 800-56A Rev.2 Diffie-Hellman Exchange (CVL Certs. #2119 and #2120, vendor affirmed; key agreement; key establishment methodology provides 112 bits of encryption strength)	Vendor Affirmed
KTS [SP800-38F §3.1]: - AES-GCM (128 or 256 bits) (Key wrapping; key establishment methodology provides 128 bits or 256 bits of encryption strength)	5890
KTS [SP800-38F §3.1]: - AES-CBC (128/192/256 bits) plus HMAC - AES-CTR (128/192/256 bit) plus HMAC (Key wrapping; key establishment methodology provides between 128 bits and 256 bits of encryption strength)	AES 5890 HMAC 3865
RSA [FIPS 186-4] - Key Pair Generation: 2048 and 3072 bits - Signature Generation (ANSI X9.31, RSASSA-PKCS1_v1-5, RSASSA-PSS): 2048, 3072, and 4096-bit with hashes (SHA-1^{+}/256/384/512) - Signature Verification (ANSI X9.31, RSASSA-PKCS1_v1-5, RSASSA-PSS): 1024^{++}, 2048, 3072, 4096-bit (per IG A.14) with hashes (SHA-1/224^{+++}/256/384/512) $^{+}$: Only used for signature generation in SSH in the Approved Mode $^{++}$: This size is not supported for RSASSA-PKCS1_v1-5 $^{+++}$: This Hash algorithm is not supported for ANSI X9.31	3086
SHA-1 and SHA-2 [FIPS 180-4] SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	4641

FIPS Approved Algorithm	CAVP Cert. #
Functions: Digital Signature Generation, Digital Signature Verification, non-Digital Signature Applications Note: SHA-224 was tested, but is not used by the module.	

** The module is compliant to IG A.5: GCM is used in the context of TLS and SSH:

- For TLS, The GCM implementation meets Option 1 of IG A.5: it is used in a manner compliant with SP 800-52 and in accordance with Section 4 of RFC 5288 for TLS key establishment. (From this RFC, the GCM cipher suites in use are TLS_RSA_WITH_AES_128_GCM_SHA256, TLS_RSA_WITH_AES_256_GCM_SHA384, 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.) During operational testing, the module was tested against an independent version of TLS and found to behave correctly.
- For SSH, the module meets Option 4 of IG A.5. 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 2^{64} is exhausted. (It would take hundreds of years for this to occur.)

In all of the above cases, the nonce_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 keys is established.

The cryptographic module supports the following non-FIPS Approved algorithms that are allowed for use in FIPS-CC mode in all Approved modes.

Table 6 - FIPS Allowed Algorithms Used in Current Module

FIPS Allowed Algorithm
Diffie-Hellman (CVL Cert. #2119 with CVL Cert. #2120, key agreement; key establishment methodology provides 112 bits of encryption strength)
CMAC - A self-test is performed for this algorithm, but it is not used by the module.
MD5 (within TLS)
NDRNG (seeding source) This provides a minimum of 256 bits of entropy to M-100, M-200, and M-600 DRBG, and 128 bits of entropy for M-500 DRBG.
RSA wrap and unwrap, non-compliant to SP800-56B RSA (CVL Cert. #2121, key wrapping; key establishment methodology provides 112 or 128 bits of encryption strength)

Table 7 - Supported Protocols in FIPS Approved Mode

Supported Protocols*
TLS v1.0[1], v1.1 and 1.2
SSHv2
SNMPv3

**Note: these protocols were not reviewed or tested by the CMVP or CAVP.*

2.8 Non-Approved, Non-Allowed Algorithms in Non-Approved Mode

The cryptographic module supports the following non-Approved algorithms. No security claim is made in the current module for any of the following non-Approved algorithms. All algorithms in this mode of operation are deemed as non-compliant.

Table 8 - Non-Approved, Non-Allowed Algorithms Used in Current Module

Non-FIPS Allowed Algorithms in Non-Approved Mode
Digital Signatures (non-Approved strengths, non-compliant): RSA Key Generation: 512, 1024, 4096 RSA signature generation: Modulus bit length less than 2048 or greater than 4096 bits; up to 16384 bits RSA signature verification: Modulus bit length less than 1024 or greater than 4096 bits; up to 16384 bits ECDSA: B, K, P curves not equal to P-256, P-384 or P-521 DSA: 768 to 4096 bits
Encrypt/Decrypt: Camellia, SEED, Triple-DES(non-compliant), Blowfish, CAST, RC4, DES
Hashing: RIPEMD, MD5
Firmware Integrity Check: HMAC-SHA-256
Key Exchange (non-Approved strengths): Elliptic Curve Diffie-Hellman: B, K, P curves not equal to P-256, P-384 or P-521 Diffie-Hellman: 768, 1024 and 1536 bit modulus RSA: Less than 2048 bit modulus

[1] See vendor imposed security rule #4 in Section 8

Non-FIPS Allowed Algorithms in Non-Approved Mode
Message Authentication: UMAC, HMAC-MD5, HMAC-RIPEMD

3 Ports and Interfaces

The M-100 module provides the following ports and interfaces.

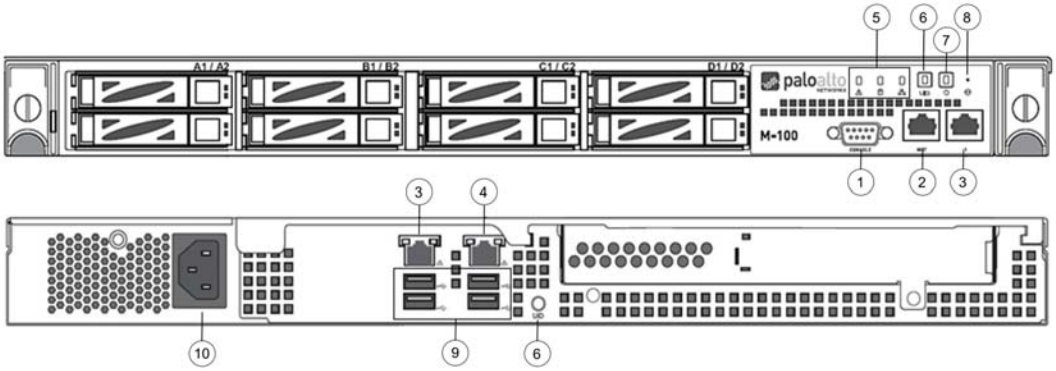

Figure 17 – M-100 Ports and Interfaces (Front and Back)

Table 9 – M-100 FIPS 140-2 Ports and Interfaces

Interface		Name and Description	Qty.	FIPS 140-2 Designation
1	DB9	Console port	1	Status output
2	RJ45	Management and data communication (MGT)	1	Data input, control input, data output, status output
3	RJ45	Port 1 (Front) and Port 2 (Rear) 10/100/1000 Ethernet	2	Data input, control input, data output, status output
4	RJ45	Port 3 (Rear) 10/100/1000 Ethernet	1	Data input, control input, data output, status output
5	Front LEDs	System Health, Internal HDD activity, LAN Activity	3	Status output
6	UID button with LED (Front and Back)	Button that activates a flashing LED on front and back of chassis to help identify physical location	2	Control input, status output
7	Power Button with LED	Power on and shut down device	1	Control input, status output
8	NMI Button	Disabled	1	Disabled
9	USB	Disabled	4	Disabled
10	Power Port	Power interface	1	Power input
Note: The slots A1/A2, B1/B2, C1/C2, D1/D2 are hard drive bays, which are depicted as populated in Figure 17. The 1TB model, P/N: 910-000030, will have two slots populated, while the 4TB model, P/N: 910-000092, will have all eight slots populated.				

The M-200 module provides the following ports and interfaces.

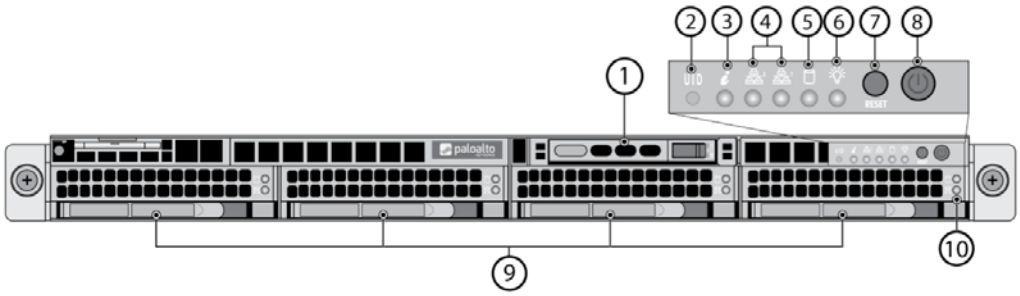

Figure 18 – M-200 Front Panel Ports and Interfaces

Table 10 – M-200 FIPS 140-2 Ports and Interfaces

Interface		Name and Description	Qty.	FIPS 140-2 Designation
1	NA	System drive used for operating system	1	NA
2	Unique Identification (UID) button	Button that activates a flashing LED on front and back of chassis to help identify physical location	1	Control input
3	System Info LED	Indicate system information such as overheat condition, fan or power failures	1	Status output
4	Network actvitiy LEDs	Blinking green indicates network activity	2	Status output
5	Hard disk LED	Blinking yellow indicates activity	1	Status output
6	Power LED	Solid green indicates power is on	1	Status output
7	Reset button	Button to reboot the appliance	1	Control input
8	Power button	Power on and shut down appliance	1	Control input
9	NA	Hard disks used for log storage	4	NA
10	Hard disk LEDs	Indicate disk activity or failure	2	Status output

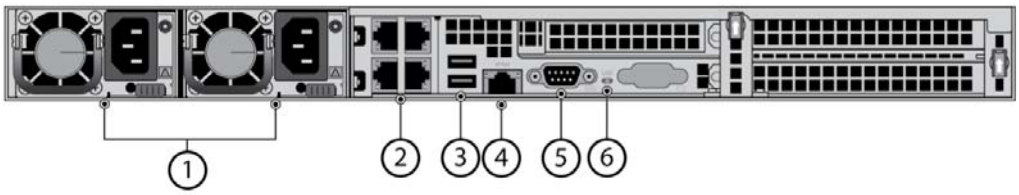

Figure 19 – M-200 Back Panel Ports and Interfaces

Table 11 – M-200 FIPS 140-2 Ports and Interfaces

Interface		Name and Description	Qty.	FIPS 140-2 Designation
1	Power	Power supplies	2	Power In
2	RJ45	Management and 10/100/1000 Ethernet Ports	4	Data input, control input, data output, status output
3	USB	Disabled	2	Disabled
4	IPMI	Disabled	1	Disabled
5	DB9	Console port	1	Status output
6	Unique Identification (UID) LED	UID LED that illuminates bright blue when you push the UID button on the front of the appliance	1	Status output

The M-500 module provides the following ports and interfaces.

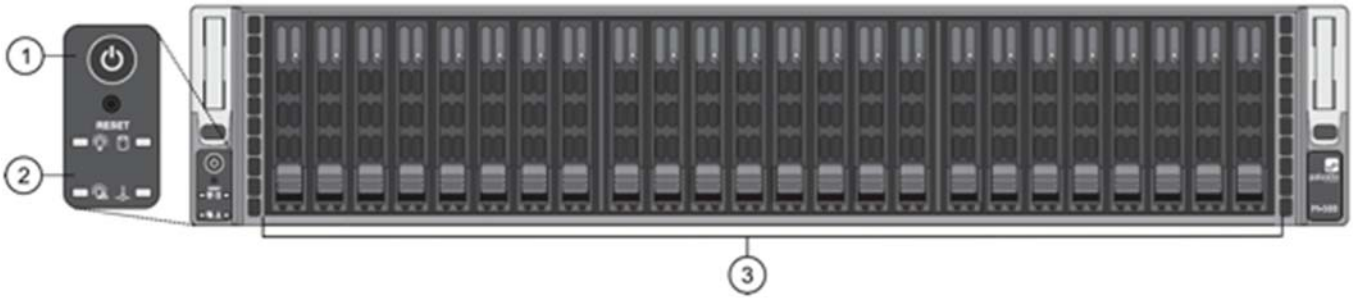

Figure 20 – M-500 Front Panel Ports and Interfaces

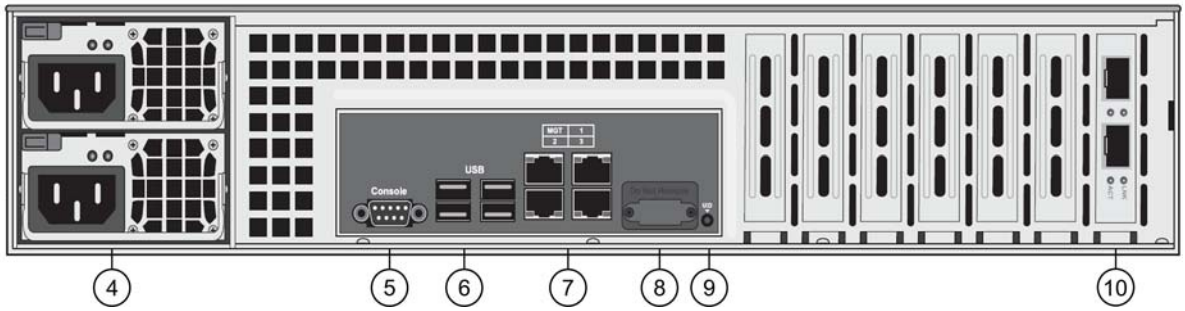

Figure 21 – M-500 Back Panel Ports and Interfaces

Table 12 – M-500 Ports and Interfaces

Interface		Name and Description	Qty.	FIPS 140-2 Designation
1	Power Button and Reset	Reboot or shut down device	2	Control input
2	Front LED Panel	Power, Power failure, HDD, Overheat/Fan failure	4	Status output
3	Drives LEDs	Left LED—drive failure Right LED—activity	48	Status output
4	Power	Power supplies	2	Power In
5	DB9	Console	1	Status Output
6	USB	USB (Reserved for future use)	4	Disabled
7	RJ45	MGT Ethernet 10/100/1000	1	Data input, Control input, Data output, Status output

Interface		Name and Description	Qty.	FIPS 140-2 Designation
		Ethernet 1, 2, 3	3	Data input, Control input, Data output, Status Output
8	VGA	Graphic port (Reserved for future use)	1	Disabled
9	UID button with LED	Button that activates LED on front and back of chassis to help identify physical location	1	Control input, Status output
10	SFP Ports	10 Gigabit Ethernet enhanced Small Form-Factor Pluggable (SFP+) ports	2	Data Input, Control input, Data Output, Status Output
Note: By default, the M-500 appliance ships with Qty. 8 1TB drives installed in drive bays A1 – D2. Qty. 8 additional drives can be installed in drive bays E1 – H2. Drive bays I1 – L2 can be utilized for adding additional drives.				

The M-600 module provides the following ports and interfaces.

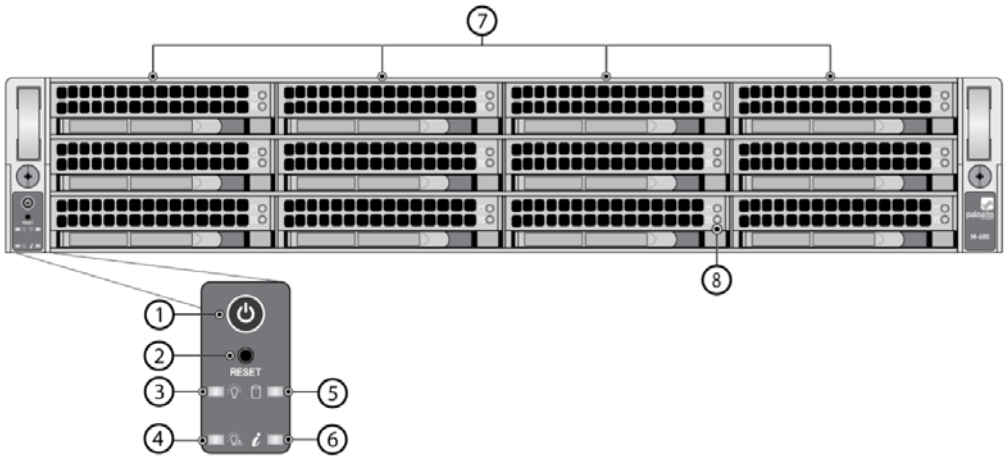

Figure 22 – M-600 Front Panel Ports and Interfaces

Table 13 – M-600 Front Ports and Interfaces

Interface		Name and Description	Qty.	FIPS 140-2 Designation
1	Power button	Power on and shut down appliance	1	Control input
2	Reset button	Button to reboot the appliance	1	Control input
3	Power LED	Solid green indicates power is on	1	Status output
4	Power failure LED	Solid red indicates power supply failed or no power source	1	Status output
5	Hard disk LED	Blinking yellow indicates activity	1	Status output
6	System Info LED	Indicate system information such as overheat condition, fan or power failures	1	Status output
7	NA	Hard disks used for log storage	4	NA
8	Hard disk LEDs	Indicate disk activity or failure	2	Status output

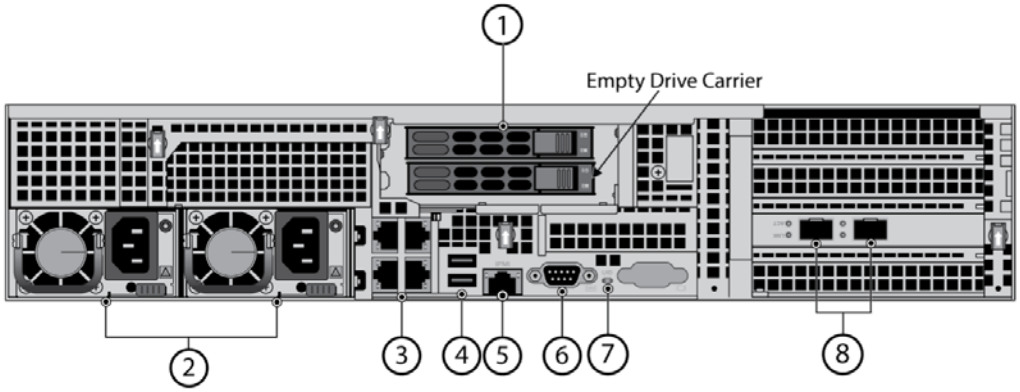

Figure 23 – M-600 Back Panel Ports and Interfaces

Table 14 – M-600 Back Ports and Interfaces

Interface		Name and Description	Qty.	FIPS 140-2 Designation
1	NA	System drive used for operating system	1	NA
2	Power	Power supplies	2	Power In
3	RJ45	Management and 10/100/1000 Ethernet Ports	4	Data input, control input, data output, status output
4	USB	Disabled	2	Disabled
5	IPMI	Disabled	1	Disabled
6	DB9	Console port	1	Status output
7	UID button with LED (Front and Back)	Button that activates a flashing LED on front and back of chassis to help identify physical location	2	Control input, status output
8	SFP Ports	10 Gigabit Ethernet enhanced Small Form-Factor Pluggable (SFP+) ports	2	Data Input, Control input, Data Output, Status Output

4 Identification and Authentication Policy

4.1 Assumption of Roles

The module supports distinct operator roles. The cryptographic module in Panorama mode, Management-Only mode, or PAN-DB mode enforces the separation of roles using unique authentication credentials associated with operator accounts. The Log Collector mode only supports one role, the Crypto-Officer role.

The module supports concurrent operators.

The module does not provide a maintenance role or bypass capability.

Table 15 – Panorama or Management-Only Mode - Roles and Required Identification and Authentication

Role	Description	Authentication Type	Authentication Data
Crypto-Officer (CO)	This role has administrative capabilities for Panorama Manager services. The CO has the ability to create other CO and User accounts that have limited service access.	Identity-based operator authentication	Username and password and/or certificate/public key based authentication.
User	This User role has read-only access defined for a set of configuration and status information	Identity-based operator authentication	Username and password and/or certificate/public key based authentication.

Table 16 - Log Collector Mode - Role and Required Identification and Authentication

Role	Description	Authentication Type	Authentication Data
Crypto-Officer (CO)	This role has administrative capabilities for Log Collector services.	Role-based operator authentication	Username and Password and/or public key based authentication

Table 17 - PAN-DB Mode - Role and Required Identification and Authentication

Role	Description	Authentication Type	Authentication Data
Crypto-Officer (CO)	This role has administrative capabilities for PAN-DB services.	Identity-based operator authentication	Username and Password
User	This User role has read-only access defined for a set of configuration and status information.	Identity-based operator authentication	Username and Password

Table 18 - Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Username and Password	The minimum password length is six (6) characters (95 possible characters). The probability that a random attempt will succeed or a false acceptance will occur is $1/(95^6)$ which is less than 1/1,000,000. The probability of successfully authenticating to the module within one-minute is $10/(95^6)$, which is less than 1/100,000. The Panorama's configuration supports at most ten attempts to authenticate in a one-minute period.
Certificate/public key based authentication	The security modules support certificate-based authentication using RSA 2048, RSA 3072, RSA 4096, ECDSA P-256, ECDSA P-384 or ECDSA P-521. The minimum equivalent strength supported is 112 bits. The probability that a random attempt will succeed is $1/(2^{112})$ which is less than 1/1,000,000. The probability of successfully authenticating to the module within a one-minute period is $3,600,000/(2^{112})$, which is less than 1/100,000. The device supports at most 60,000 new sessions per second to authenticate in a one-minute period.

5 Security Parameters

Table 19 - Private Keys and CSPs

Key/CSP	Description
ECDSA Private Keys	Supports establishment of TLS session keys, SSH host authentication, and certificate signing keys (ECDSA P-256, P-384, P-521)
RSA Private Keys	Supports establishment of TLS session keys, SSH host authentication, and certificate signing keys (RSA 2048, 3072 or 4096 bits)
TLS DHE private Components	Diffie-Hellman private component used in TLS connections (DH Group 14, L = 2048, N >=224)
TLS ECDHE Private Components	EC Diffie-Hellman private component used in TLS connections (ECDHE P-256, P-384, P-521)
TLS Pre-Master Secret	Secret value used to derive the TLS Master Secret along with client and server random nonces
TLS Master Secret	Secret value used to derive the TLS session keys
TLS Encryption keys	AES session keys used in TLS connections (128 or 256 bits; CBC or GCM)
TLS HMAC keys	HMAC-SHA-1/256/384 session keys used in TLS connections
SSH DH private components	Diffie-Hellman private component (DH Group 14, L=2048, N >=224)
SSH ECDH private components	EC Diffie-Hellman private component (P-256, P-384, P-521)
SSH Session Encryption key	AES session key used in SSH connections (128, 192, 256 bits: CBC or CTR) (128 or 256 bits: GCM)
SSH Session Authentication key	Session key used in SSH connections (HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-512)
Operator passwords	Password for operator authentication
DRBG seed and state	DRBG seed coming from the NDRNG and AES 256 CTR DRBG state used in the generation of a random values
SNMPv3 Secrets	SNMPv3 Authentication Secret and Privacy Secret
SNMPv3 Keys	AES CFB Privacy key and HMAC- SHA-1 Authentication keys

Key/CSP	Description
RADIUS Secret	Authentication key for RADIUS server (must be minimum of 6 characters)
Note: All CSP and keys defined may be accessed by the Manager and Log-Collector modes while the PAN-DB mode only supports some of the CSP/keys defined. For details regarding what CSPs are supported in each mode, please see Tables 17 – 19 above. The CSPs and keys may be shared between the Approved modes of operation.	

Table 20 - Public Keys

Key Name	Description
CA Certificates	RSA and/or ECDSA keys used to extend trust for certificates.
RSA Public Keys / Certificates	RSA Public keys managed as certificates for the verification of signatures, establishment of TLS, operator authentication and peer authentication. (RSA 2048, 3072, or 4096 bits)
ECDSA Public Keys / Certificates	ECDSA public keys managed as certificates for the verification of signatures, establishment of TLS, operator authentication and peer authentication (ECDSA P-256, P-384, P-521)
Client Authentication Public Key	Used to authenticate the end user (ECDSA P-256, P-384, P-521; RSA 2048, 3072, 4096 bits)
TLS DHE public components	Used in key agreement (DH Group 14)
TLS ECDHE public components	Used in key agreement (ECDHE P-256, P-384, P-521)
SSH DH public components	Used in key agreement (DH Group 14)
SSH ECDH public components	Used in key agreement (P-256, P-384, P-521)
SSH Host RSA public key	Used in SSH public key authentication process (RSA 2048, 3072, or 4096 bits)
SSH Host ECDSA public key	Used in SSH public key authentication process (ECDSA P-256, P-384, P-521)
SSH Client RSA public key	Used in SSH public key authentication process (RSA 2048, 3072, or 4096 bits)
Firmware Authentication Key	RSA key used to authenticate firmware (2048 bits)
Firmware Integrity Check Key	Used to check the integrity of crypto-related code (HMAC-SHA-256* and ECDSA P-256)

Key Name	Description
	*Keys used to perform power-up self-tests are not CSPs as per IG 7.4
Note: All keys defined may be accessed by the Manager and Log-Collector modes while PAN-DB mode only supports some of the keys defined. For details regarding what CSPs are supported in each mode, please see Tables 17 – 19 above. The keys may be shared between the Approved modes of operation.	

6 Access Control Policy

6.1 Roles and Services

The Approved and non-Approved mode of operation provide identical services. While in the Approved mode of operation all authenticated services and CSPs are accessed via authenticated SSH or TLS sessions. Access is restricted to authenticated operators only and no interface is provided to modify the public or private key.

For all authenticated services the following CSPs and public keys may be executed:

- TLS Management Access
  - ECDSA Private Keys/Public Keys
  - RSA Private Keys/Public Keys
  - TLS DHE Private/Public Components
  - TLS ECDHE Private/Public Components
  - TLS Pre-Master Secret
  - TLS Master Secret
  - TLS Encryption keys
  - TLS HMAC keys
- SSH Management Access
  - SSH DH public components
  - SSH ECDH public components
  - SSH Host RSA public key
  - SSH Host ECDSA public key
  - SSH Client RSA public key (Manager Mode only)

SNMPv3 authentication is supported but is not a method of module administration and does not allow read/write access of CSPs. Approved and allowed algorithms, relevant CSP and public keys related to these protocols are used to access the following services. CSP access by services is further described in the following tables. Additional service information and administrator guidance for Panorama can be found at https://www.paloaltonetworks.com/documentation.html

The Crypto-Officer may access all services, and through the “management of administrative access” service may define multiple Crypto-Officer roles with limited services. The User role provides read-only access to the System Audit service. When configured in the default mode, Panorama Manager provides services via web-browser based interface and a command line interface (CLI). For the Panorama Log Collector mode and PAN-DB mode, only the CLI is available for management.

The services listed below are also available in the non-Approved mode. In the non-Approved mode, non-Approved algorithms and non-Approved algorithm strengths are used to access these services.

Table 21 - Authenticated Services – Panorama M-100/M-200/M-500/M-600 Manager (Panorama or Management-Only Mode)

Service	Description	CSP/Key Access
System Provisioning	Perform panorama licensing, diagnostics, debug functions, manage Panorama support information and switch between Panorama Manager, Logger, and PAN-DB modes.	N/A
System Audit	Allows review of limited configuration and system status via SNMPv3, logs, dashboard, show status, and configuration screens. Provides no configuration commit capability.	N/A
Panorama Firmware Update	Download and install software and firmware updates	Signature verification with RSA public key
Panorama Manager Setup	Presents configuration options for management interfaces and communication for peer services (e.g., SNMP, RADIUS). Import, Export, Save, Load, revert and validate Panorama configurations and state	Import or Export RSA/ECDSA Private/Public Keys Import SNMPv3 Secrets Creation RADIUS Secret
Manage Panorama Administrative Access	Define access control methods via admin role profiles, configure administrators and password profiles Configure local user database, authentication profiles, sequence of methods and access domains	Import, modify, or delete operator passwords Import, modify, or delete SSH Client RSA public keys Modify SSH Host RSA public key and SSH Host ECDSA public key Modify, Read, or delete TLS Pre-master secret, TLS Master secret and TLS public keys Execute/Read/Write DRBG seed and state
Configure High Availability	Configure High Availability communication settings	N/A

Service	Description	CSP/Key Access
Panorama Certificate Management	Manage RSA/ECDSA certificates and private keys, certificate profiles, revocation status, and usage; show status.	Import or export RSA /ECDSA private/public keys Generate RSA/ECDSA private/public keys Sign RSA/ECDSA private keys Execute/Read/Write DRBG seed and state
Panorama Log settings	Configure log forwarding	N/A
Panorama Server Profiles	Configure communication parameters and information for peer servers such as Syslog, SNMP trap servers, email servers and authentication servers	Import SNMPv3 Secrets Execute/Read SNMPv3 keys
Setup Managed Devices and Deployment	Set-up and define managed devices, device groups for firewalls Configure device deployment applications and licenses View current deployment information on the managed firewalls. It also allows you to manage software versions and schedule updates on the managed firewalls and managed log collectors.	N/A
Configure managed Device Templates	Define and manage common base configuration templates for managed firewalls. Template configurations define settings that are required for the management of the firewalls on the network.	Import or export RSA/ECDSA private/public keys Signature generation with RSA/ECDSA private keys Generate RSA/ECDSA private/public keys Execute/Read/Write DRBG seed and state
Configure Managed Device Groups	Define and manage common base of policies and data objects for managed firewalls in configured device groups	N/A

Service	Description	CSP/Key Access
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 to manage software versions and schedule updates on managed log collectors.	Modify operator passwords
Monitor system status and logs	Review system status via the panorama system CLI, dashboard and logs; show status.	N/A
Monitor network activity	Review aggregated information across all managed firewalls and show status. The aggregated view provides actionable information on trends in user activity, traffic patterns, and potential threats across your entire network.	N/A
Switch Context	Browses a managed firewall's web based user interface.	N/A

Table 22 - Authenticated Services – Panorama M-100/M-200/M-500/M-600 Log Collector Mode

Service	Description	CSP Access
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	Import or Export RSA/ECDSA Private/Public Keys
Panorama Firmware Update	Download and install software and firmware updates.	Signature verification with RSA public key
Manage Panorama Administrative Access	Update Administrator password	Import or modify operator passwords
Panorama Certificate Management	Manage RSA/ECDSA certificates and private keys, certificate profiles, revocation status, usage; and show status.	Import or export RSA/ECDSA private/public keys

Service	Description	CSP Access
		Generate RSA/ECDSA private/public keys Sign with RSA/ECDSA private keys Execute/Read/Write DRBG seed and state

Table 23 - Authenticated Services – Panorama M-500/M-600 Private Pan-DB Mode

Service	Description	CSP Access
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	N/A
System Audit	Allows review of limited configuration and system status via SNMPv3, logs, dashboard, show status, and configuration screens. Provides no configuration commit capability.	N/A
Panorama Firmware Update	Download and install software and firmware updates	Signature verification with RSA public key
Manage PAN-DB Administrative Access	Define access control methods via admin role profiles	Import or modify operator passwords

6.2 Unauthenticated Services

The cryptographic module supports the following unauthenticated services:

Table 24 - Unauthenticated Services

Service	Description
Zeroize	The device will overwrite all CSPs. The zeroization procedure is invoked when the operator performs a factory reset. The operator must be present to observe the method has completed successfully or in control via a remote management session. During the zeroization procedure, no other services are available.

	Procedures to perform zeroization: • During initial boot up, break the boot sequence via the console port connection (by entering 'maint' when instructed to do so) to access the main menu. • Select "Continue." • Select the "Factory Reset" option to enter the Approved mode. • Select "Factory Reset". • When prompted, select "Reboot" and the module will re-initialize and continue into the Approved mode. • The module will reboot.
Self-Tests	Run power up self-tests on demand by power cycling the module. Execute/Read access to FW integrity Check key.
Show Status (LEDs)	View hardware status (on/off) of the module via the LEDs.

7 Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the module contains a non-modifiable 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 140-2 CMVP. Any other firmware loaded into this module is out of the scope of this validation and require a separate FIPS 140-2 validation.

8 Security Rules

The module design corresponds to the module security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 2 module.

1. The cryptographic module provides distinct operator roles. When the module has not been placed in a valid role, the operator does not have access to any cryptographic services.
2. The Panorama M-100, M-200, M-500 and M-600 cryptographic modules supports initialization as a Log Collector in an Approved mode of operation with Level 2 role-based authentication or support initialization as a Panorama Manager or PAN-DB (M-500 and M-600 only) in an Approved mode of operation with Level 3 identity-based authentication.
3. The cryptographic module clears previous authentications on power cycle.
4. The cryptographic module performs the following tests for all Approved modes:
    A. Power up Self-Tests
        1. Cryptographic algorithm tests

a. AES Encrypt Known Answer Test
b. AES Decrypt Known Answer Test
c. AES CMAC Known Answer Test
d. AES GCM Encrypt Known Answer Test
e. AES GCM Decrypt Known Answer Test
f. AES CCM Encrypt Known Answer Test
g. AES CCM Decrypt Known Answer Test
h. ECDSA Sign Known Answer Test
i. ECDSA Verify Known Answer Test
j. RSA Sign Known Answer Test
k. RSA Verify Known Answer Test
l. RSA Encrypt Known Answer Test
m. RSA Decrypt Known Answer Test
n. HMAC-SHA-1 Known Answer Test
o. HMAC-SHA-256 Known Answer Test
p. HMAC-SHA-384 Known Answer Test
q. HMAC-SHA-512 known Answer Test
r. SHA-1 Known Answer Test
s. SHA-256 Known Answer Test
t. SHA-384 Known Answer Test
u. SHA-512 Known Answer Test
v. DRBG Known Answer Test
w. ECDH Known Answer Test
x. DH Known Answer Test
y. SP800-90A Section 11.3 Health Tests

B. Firmware Integrity Test – HMAC-SHA-256 and ECDSA P-256.
C. Conditional Self-Tests
    1. Continuous Random Number Generator (RNG) test – performed on NDRNG and DRBG
    2. ECDSA Pairwise Consistency Test Sign/Verify
    3. RSA Pairwise Consistency Test Sign/Verify and Encrypt/Decrypt
    4. Firmware Load Test – Verify RSA 2048 with SHA-256 signature on firmware at time of load
D. If any conditional test fails, the module will output 'FIPS-CC failure' and the specific test that failed.

5. The operator is capable of commanding the module to perform the power-up self-test by cycling power of the module.
6. Upon re-configuration to/from the Log Collector mode or PAN-DB mode of operation from/to the Manager mode, the cryptographic module reboots and perform all power-up self-tests.
7. Power-up self-tests do not require any operator action.

8. Data output is inhibited during power-up self-tests and error states.
9. Processes performing key generation and zeroization processes are logically isolated from the logical data output paths.
10. The module does not output intermediate key generation values.
11. Status information output from the module does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
12. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
13. The module maintains separation between concurrent operators.
14. The module does not support a maintenance interface or role.
15. The module does not have any external input/output devices used for entry/output of data.
16. The module does not enter or output plaintext CSPs.

Vendor imposed security rules:

1. When configured, the module automatically logs out the operator when the cryptographic module remains inactive in any valid role for the administrator specified time interval.
2. When configured, the module enforces a timed access protection mechanism that supports at most ten authentication attempts per minute. After the administrator specified number of consecutive unsuccessful password validation attempts has occurred, the cryptographic module shall enforce a wait period of at least one (1) minute before any more login attempts can be attempted. This wait period shall be enforced even if the module power is momentarily removed.
3. When FIPS-CC mode is enabled, the operator shall not install plugins. If a plugin is install, the module shall be configured in non-Approved mode of operation.
4. When FIPS-CC mode is enabled, TLSv1.0 is disabled. The operator should not re-enable TLSv1.0. TLSv1.0 can be used in an Approved mode of operation (Approved TLS KDF algorithm); however, TLS v1.0 protocol is no longer considered as secure because of the Cipher Block Chaining IV attack, a client of the module could use a vulnerable implementation.
5. When FIPS-CC mode is enabled, the operator shall not use TACACS+. RADIUS may be used but must be protected by TLS protocol. If TACAS+ or RADIUS without TLS protocol are set, the module shall be configured in non-Approved mode of operation.
6. The operator shall not generate 4096-bit RSA key in FIPS-CC mode. If the operator wants to generate 4096-bit RSA key, the module shall be configured in non-Approved mode of operation.

9 Physical Security Policy

9.1 Physical Security Mechanisms

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 twenty-eight (28) tamper-evident seals for the M-100, fifteen (15) for the M-200, twelve (12) for the M-500, and twenty-one (21) for the M-600. 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.

Note: For ordering information, see Table 2 for FIPS kit part numbers and versions. Opacity shields are included in the FIPS kits.

Refer to Appendix A to D for instructions on installation and placement of the tamper seals and opacity shields. The locations of the tamper-evident seals implemented on the M-100, M-200, M-500, and M-600 are shown in Appendix A to Appendix D, respectively.

9.2 Operator Required Actions

Table 25 - Inspection/Testing of Physical Security Mechanisms

Model	Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
M-100 M-200	Tamper Evident Seals	30 days	Verify integrity of tamper-evident seals in the locations identified in Appendix A and C of this Security Policy.
M-100 M-200	Front and Rear Opacity Shields Side Rails	30 days	Verify that opacity shields and side rails have not been loosened or deformed from their original shape, thereby reducing their effectiveness.
M-100	Top Overlays	30 days	Verify top overlays have not been removed or deformed. All edges should maintain strong adhesion characteristics.
M-500 M-600	Tamper Evident Seals	30 days	Verify integrity of tamper-evident seals in the locations specified in Appendix B and D.
M-500 M-600	Front and Rear Opacity Shields	30 days	Verify that the front and rear opacity shields have not been deformed from their original shape, thereby reducing their effectiveness.
M-500 M-600	Vent Overlays	30 days	Verify that the vent overlays have not been removed or deformed. All edges should maintain strong adhesion characteristics.

10 Mitigation of Other Attacks Policy

The module has not been designed to mitigate any specific attacks outside of the scope of FIPS 140-2, so these requirements are not applicable.

11 References

[FIPS 140-2] FIPS Publication 140-2 Security Requirements for Cryptographic Modules

12 Definitions and Acronyms

AES – Advanced Encryption Standard

CA – Certificate Authority

CLI – Command Line Interface

CO – Cryptographic Officer

DB9 – D-sub series, E size, 9 pins.

DH – Diffie-Hellman

DRBG – Deterministic Random Bit Generator

FIPS – Federal Information Processing Standard

HA – High Availability

HMAC – (Keyed) Hashed Message Authentication Code

LED – Light Emitting Diode

NDRNG – Non-deterministic random number generator

NMI – Non-Maskable Interrupt

RJ45 – Networking Connector

RSA – Algorithm developed by Rivest, Shamir and Adleman

SHA – Secure Hash Algorithm

TLS – Transport Layer Security

USB – Universal Serial Bus

Appendix A – M-100 - FIPS Accessories/Tamper Seal Installation (28 Seals)

Step 1: From the rear of the module, remove the six (6) screws and port cover, as shown. Retain screws and port cover for the Step 2.

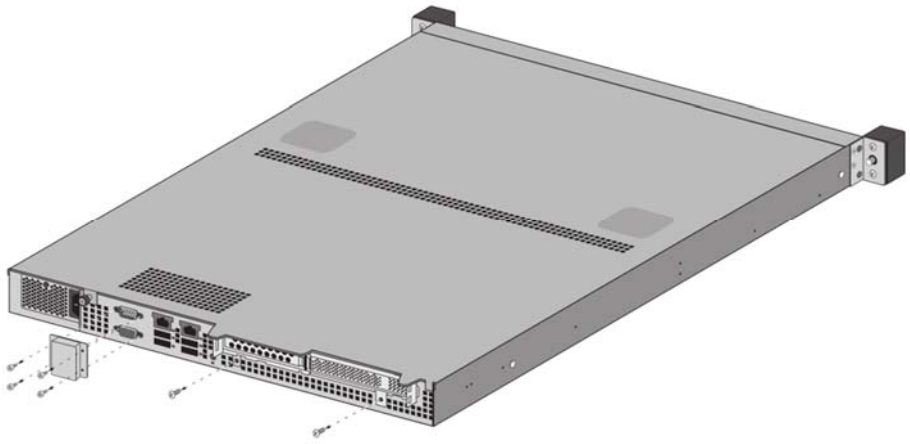

Figure 24 – M-100: Remove Screws on Rear Side

Step 2: Attach the rear opacity shields.

A. Using two (2) #6-32 3/8” screws, attach the lower rear cover bracket. Replace the port cover and secure with the four (4) screws that you removed in Step 1.
B. Use four (4) #4-40 1/4” screws to attach the rear cover to the bracket.

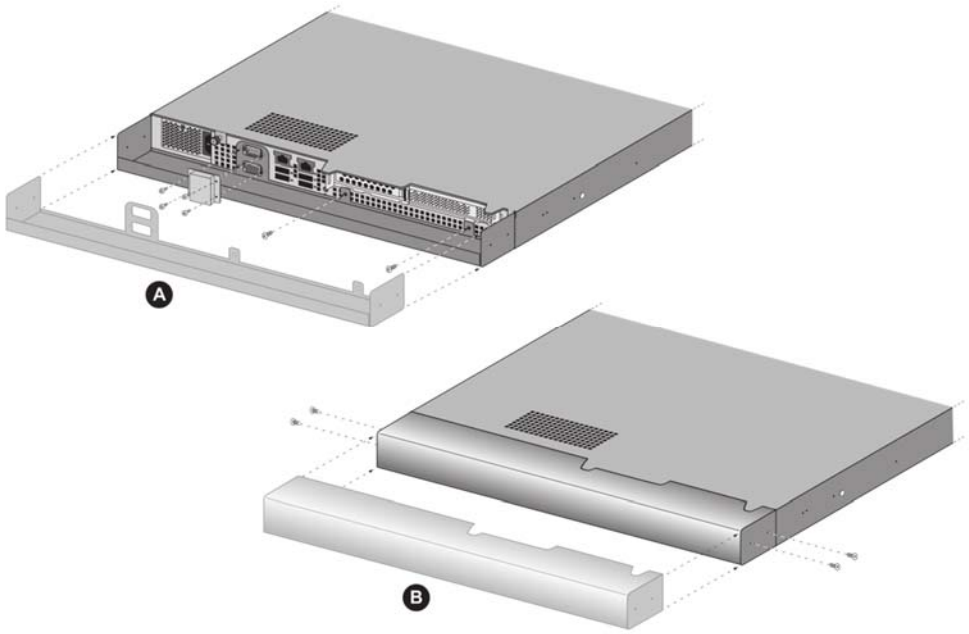

Figure 25 – M-100: Attach Rear Opacity Shield

Step 3: Apply tamper-evident seals (two (2) seals) to the seam of the rear cover and rear outer edges of the appliance (seals #1 and #2 in the illustration below). Apply tamper-evident seals to the left and right sides covering the side holes (two (2) seals #3 and #4). Apply top air vent overlay covers and tamper-evident seals (sixteen (16) seals #5-#10 and #11-#20).

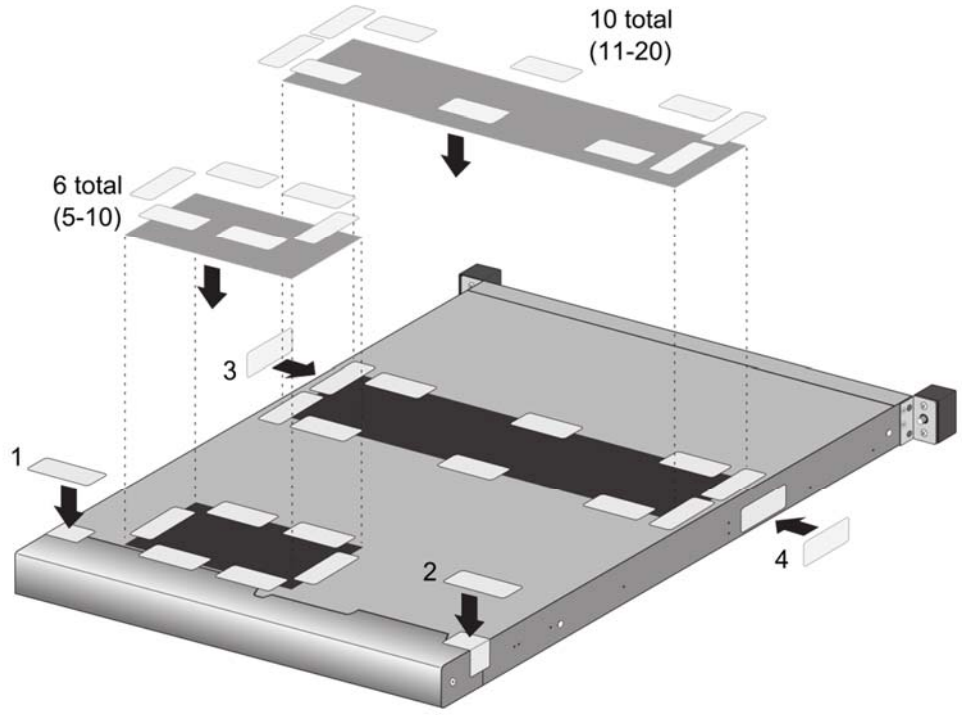

Figure 26 – M-100: Apply Tamper Seals and Vent Overlays

Step 4: Place side inner rails to each side of the module and attach using rail kit screws.

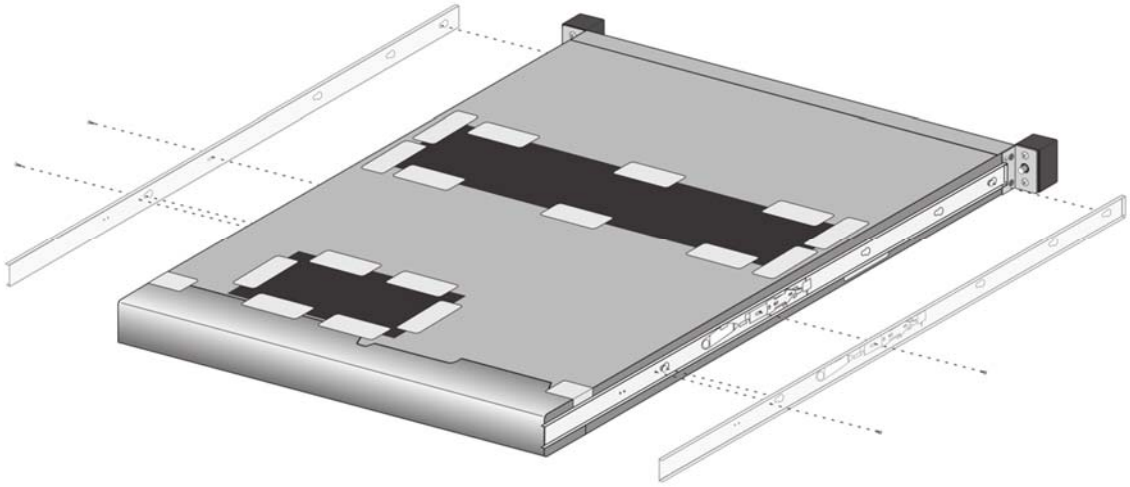

Figure 27 – M-100: Apply Rail Kit

Step 5: Remove the two (2) front plastic bracket covers and screws. Remove and retain the two (2) captive screws from the plastic covers.

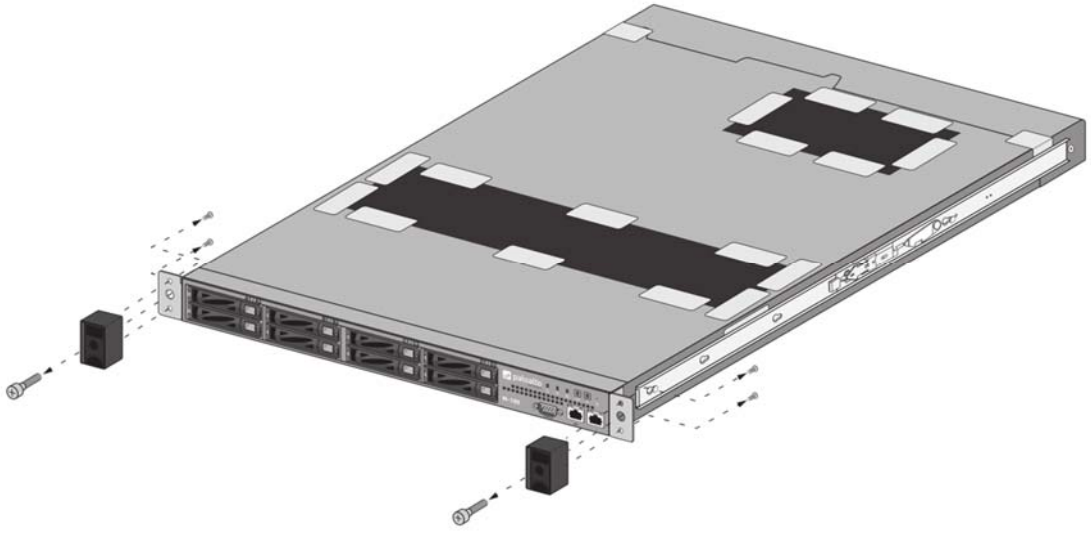

Figure 28 – M-100: Remove Front Plastic Bracket Covers and Screws

Step 6: Install front opacity shield and attach to brackets using four (4) 4-40 x 0.25-inch screws and thread a captive screw through each side of the front cover bracket, as shown. Affix four (4) tamper seals on top and bottom of module as shown.

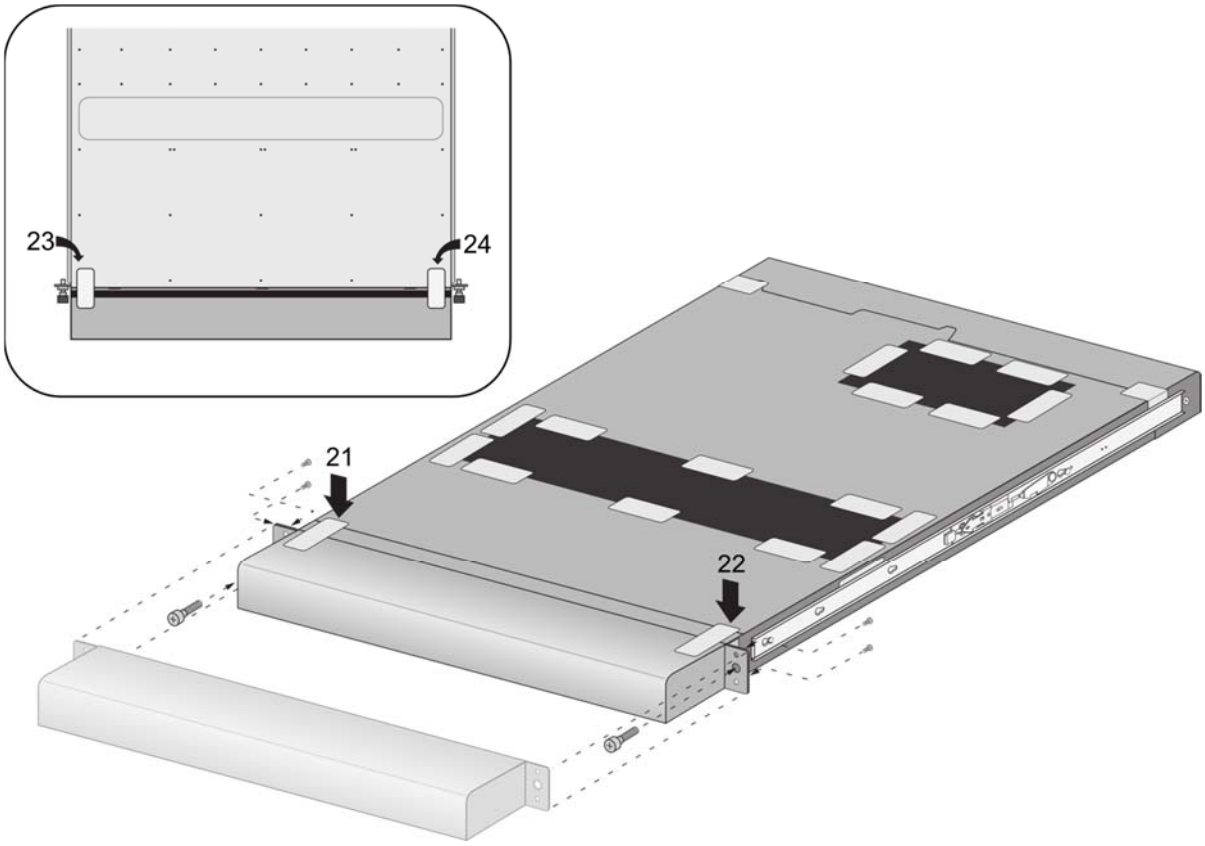

Figure 29 – M-100: Install Front Opacity Shield

Step 7 – Slide module into outer rails and attach outer rails and apply four (4) seals overlapping the rack mount bracket and the module sides.

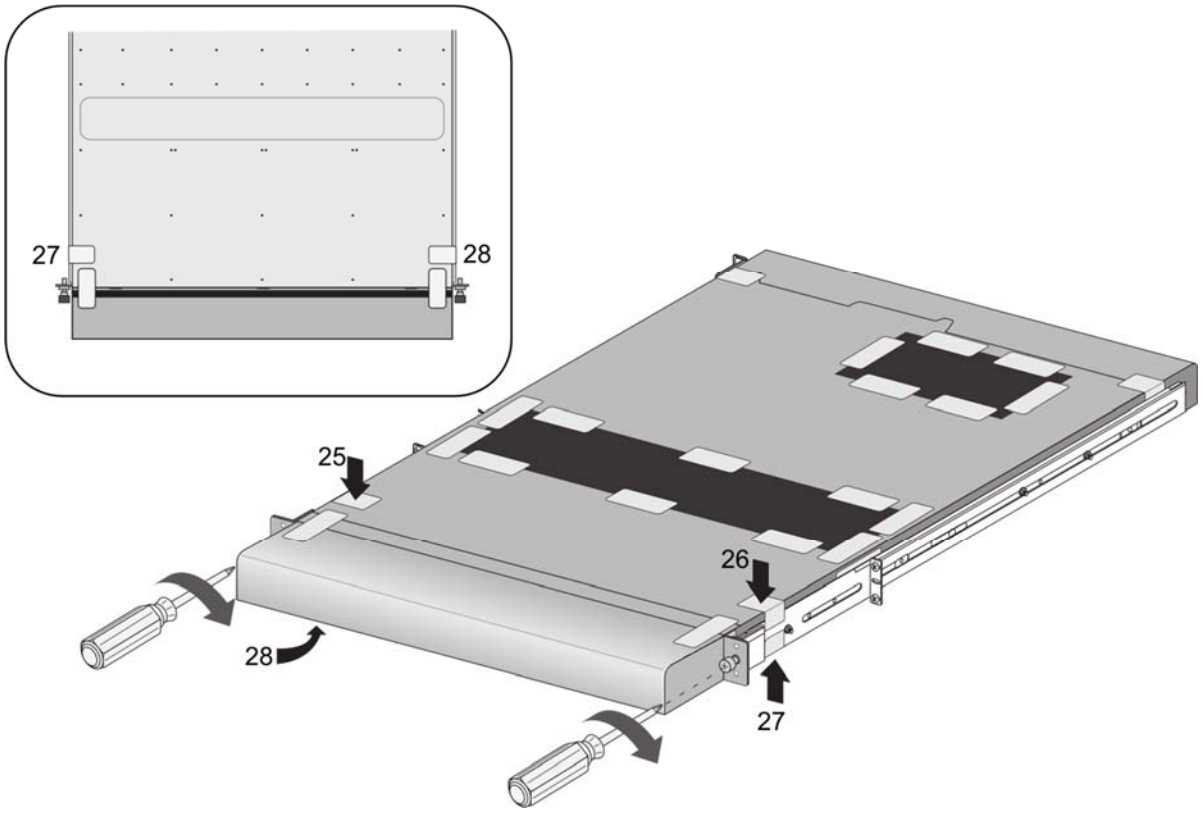

Figure 30 – M-100: Install Outer Rails

Appendix B – M-200 - FIPS Accessories/Tamper Seal Installation (Fifteen (15) Seals)

1. 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-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 FIPS 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.

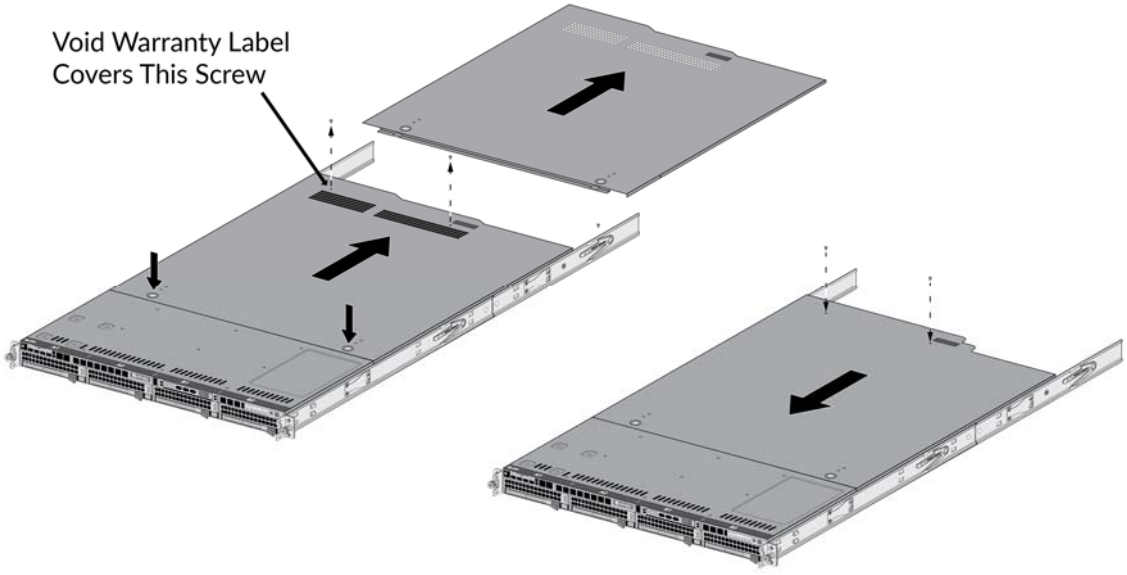

Figure 31 – M-200: Top Cover Replacement

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

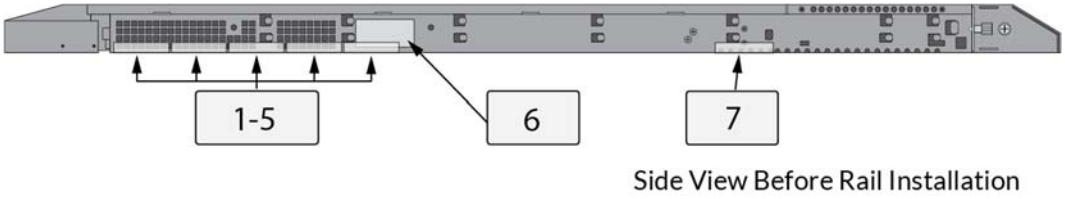

Figure 32 – M-200: Side View Before Rail Installation

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.

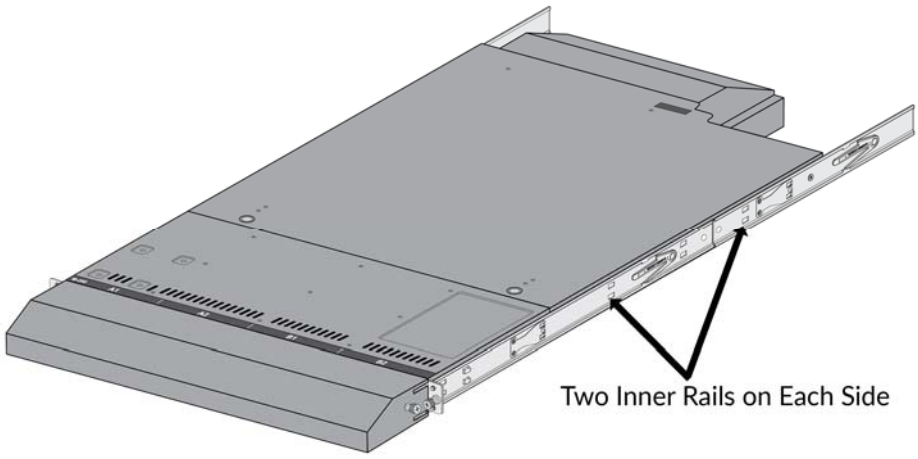

Figure 33 – M-200: Inner Rack Mount Rail Brackets

3. Attach the FIPS front cover brackets.

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

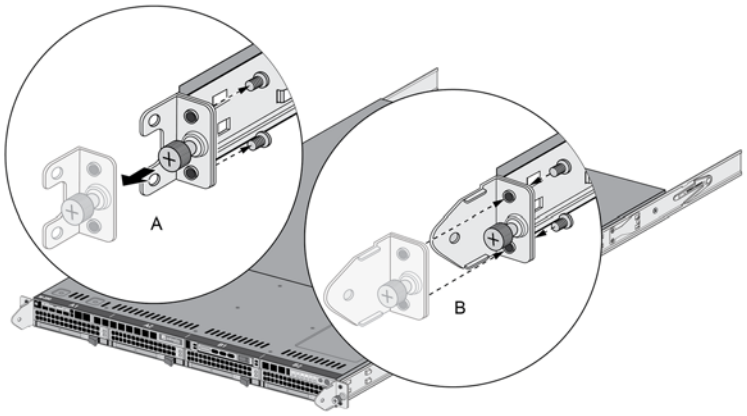

Figure 34 – M-200: Replacing Front Rack-Mount Brackets

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

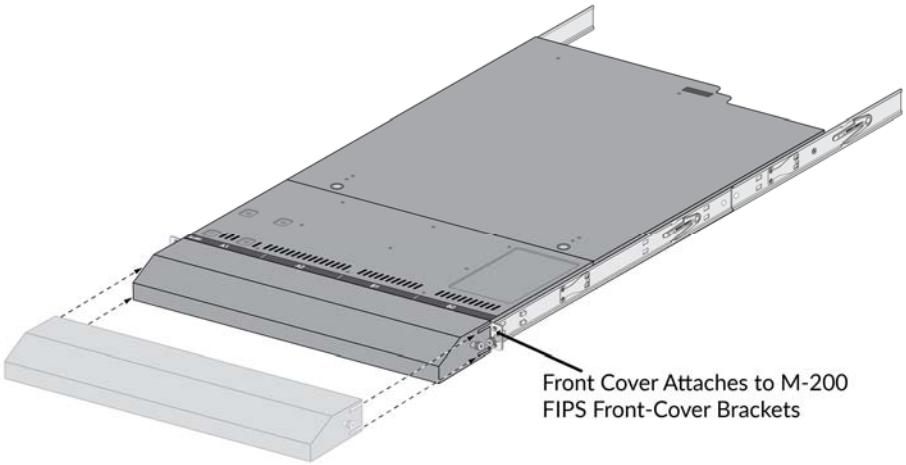

Figure 35 – M-200: Attach FIPS Front Cover

5. Attach the FIPS 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 FIPS 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 FIPS kit surfaces.

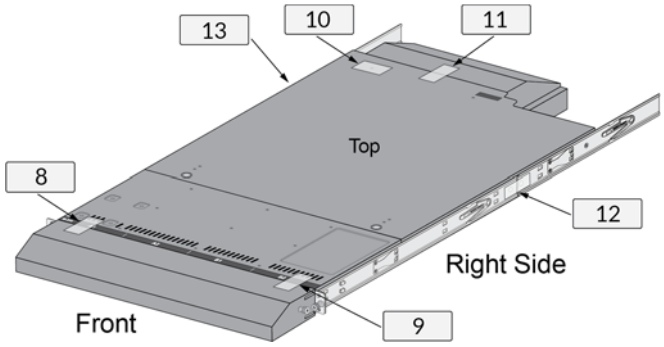

Figure 36 – M-200: Seal locations on Top and Right Side

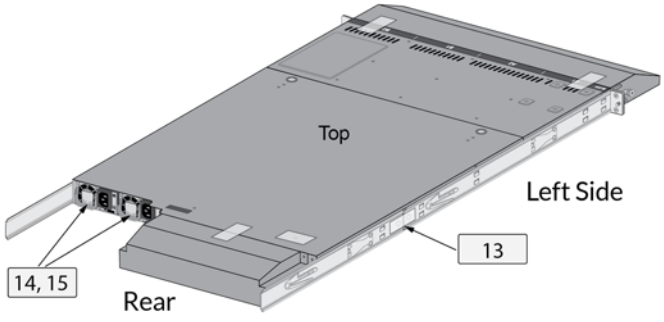

Figure 37 – M-200: Seal Locations on Left Side and Rear

Appendix C – M-500 - FIPS Accessories/Tamper Seal Installation (12 Seals)

Step 1:

Remove the two pull handles and front modules on the left and right side of the appliance by removing the three (3) screws located behind each handle/module. There is no need to disconnect the LED circuit board attached to the end of the ribbon cable. Retain these screws for Step 2.

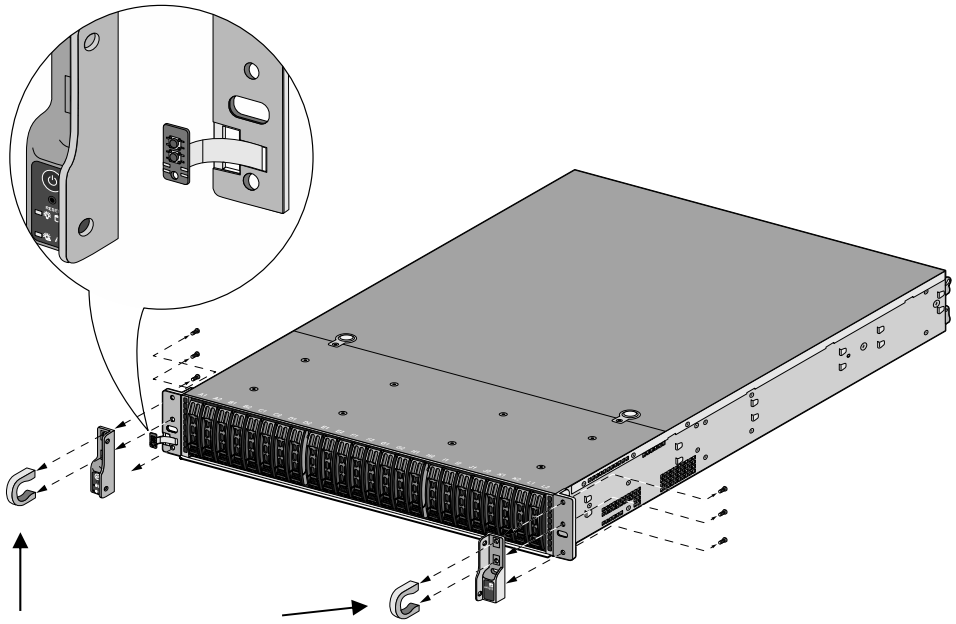

Figure 38 – M-500: Remove Front Handles and Modules

Step 2:

Attach the left and right front cover brackets to the appliance using the six (6) screws that you removed in Step 1. First attach the brackets using the bottom screws (one on each side) as shown in Figure 39, ensuring that you feed the ribbon cable and LED circuit board through the left bracket. Replace the front modules and secure them using the middle and top screws on each side as shown in Figure 40.

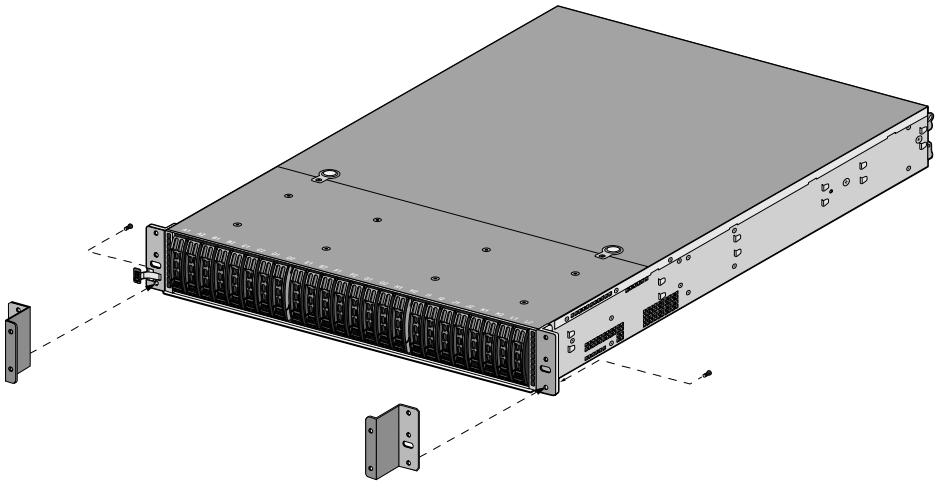

Figure 39 – M-500: Secure the Front Brackets

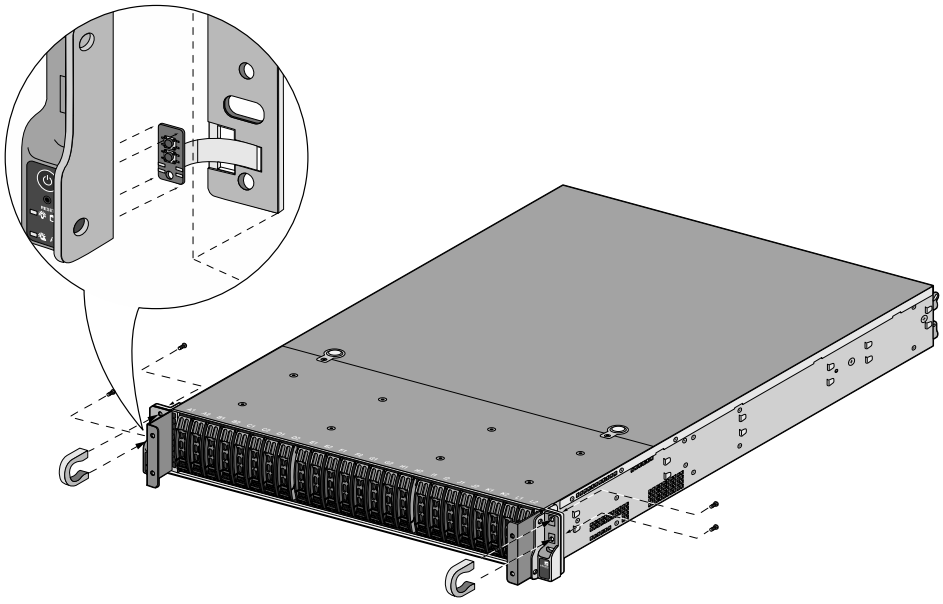

Figure 40 – M-500: Attach Pull Handles and Front Modules

Step 3:

Secure the front opacity shield to the right and left front brackets that you installed in Step 2. Use two (2) screws (provided) on each side.

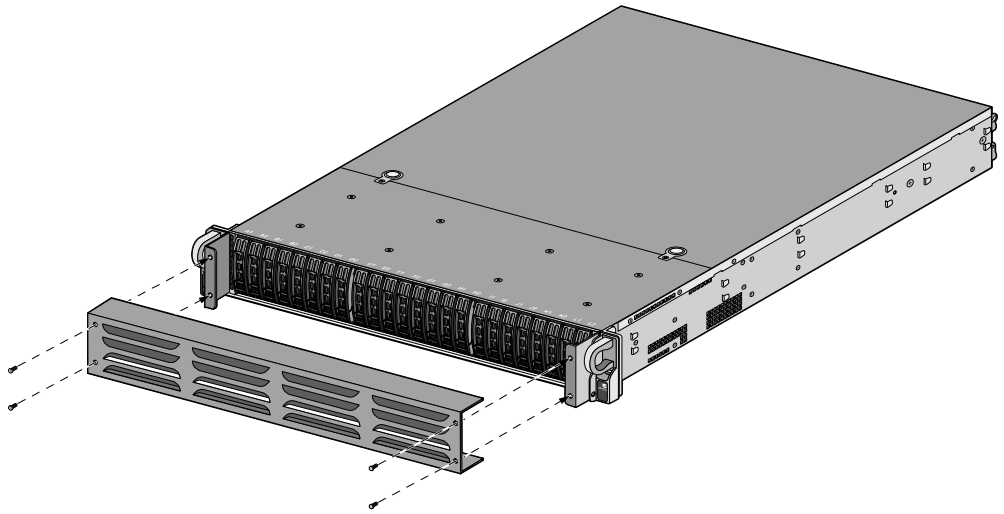

Figure 41 – M-500: Install Front Opacity Shield

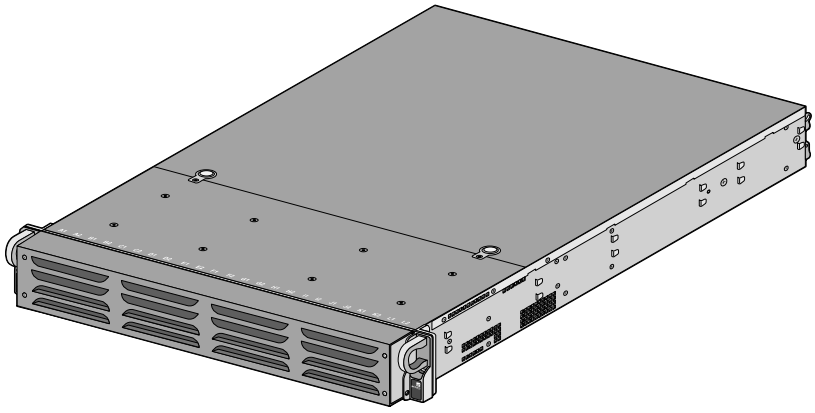

Figure 42 – M-500: Front Opacity Shield Installed

Step 4:

Attach the rear opacity shield tray to the appliance. First, remove the two (2) screws (shown in Figure 43) from the appliance and use these screws to secure the rear opacity shield tray.

Note: Install the back cables (power cords and network/management cables) because you will not be able to access these ports after the next step.

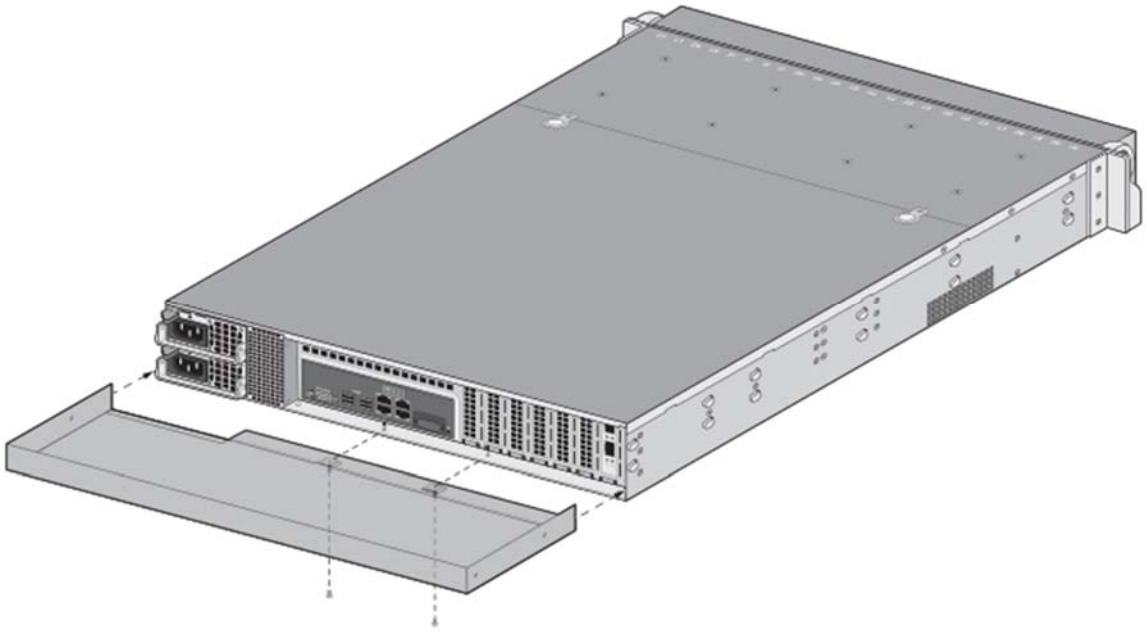

Figure 43 – M-500: Install Rear Opacity Shield Tray

Step 5:

Place the rear opacity shield on top of the rear opacity shield tray ensuring that you run the cables through the opening at the bottom. Secure the opacity shields with two (2) screws (provided) on each side.

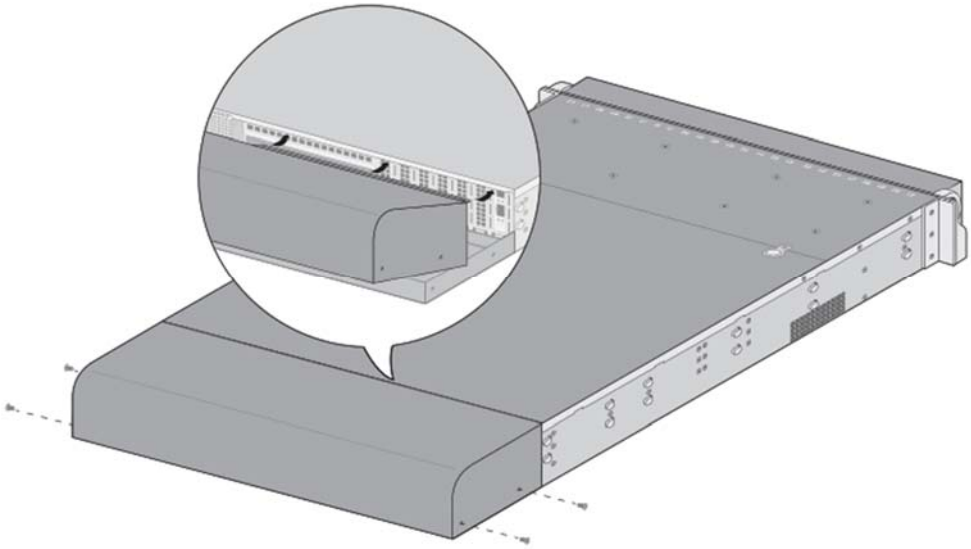

Figure 44 – M-500: Install Rear Opacity Shield

Step 6:

Cover the vent openings as shown in Figure 45 by applying one (1) overlay sticker over the left side vent and one (1) overlay sticker over the right side vent. Each overlay requires two (2) tamper seals as shown in Figure 46 (A). Also apply one (1) additional tamper seal as shown in Figure 46 (B) #5.

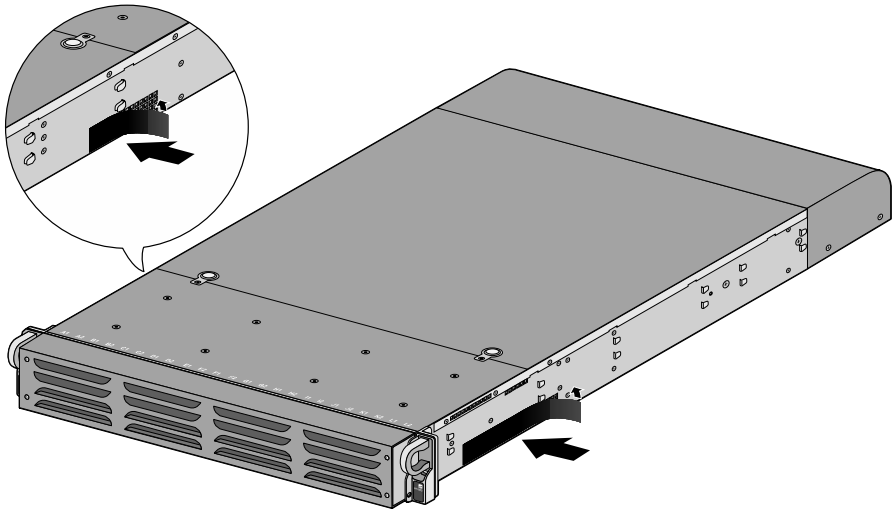

Figure 45 – M-500: Apply Vent Overlays

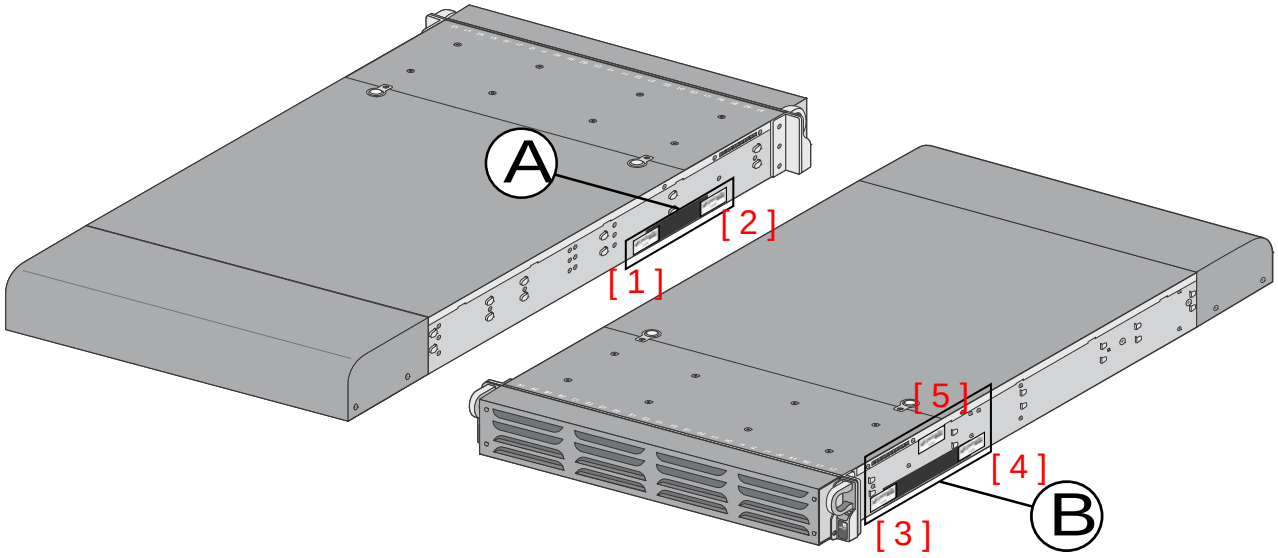

Figure 46 – M-500: Apply Tamper Seals on Vent Overlays and Side Opening

Step 7:

Re-attach the rail kit to the appliance as shown in Figure 47 and then add three (3) tamper seals to the bottom of the appliance as shown in Figure 48. One (1) tamper seal prevents tampering of the front opacity shield connected to the bottom of the appliance and two (2) tamper seals wrap around the upper and lower rear opacity shields to prevent tampering of the rear opacity shields.

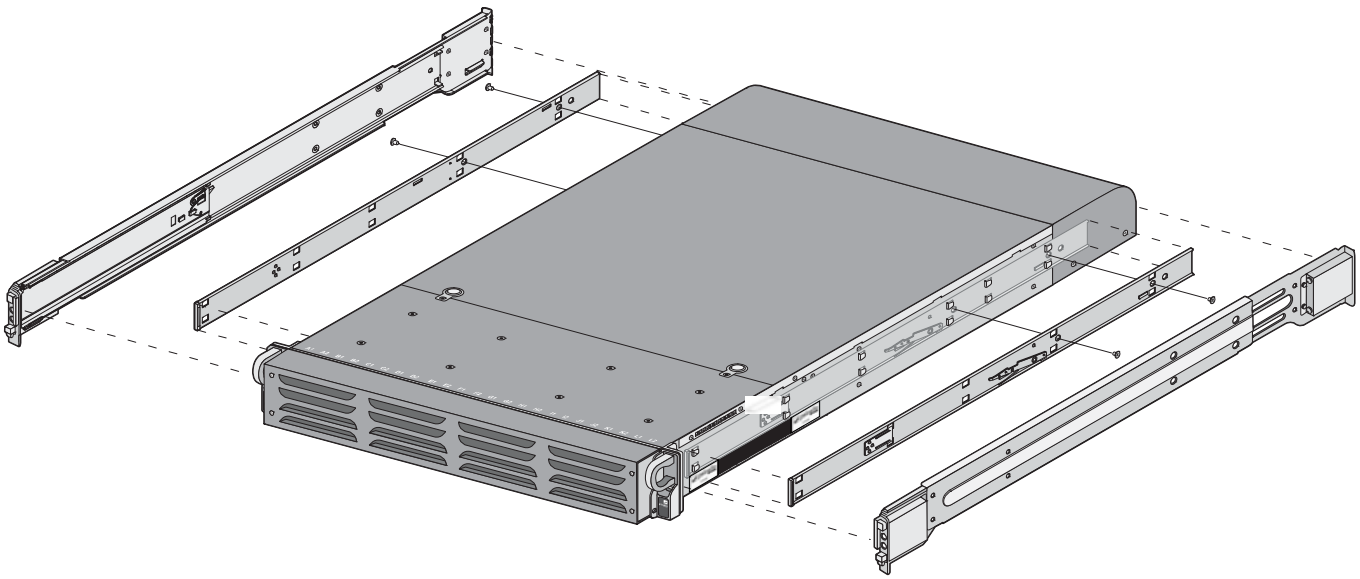

Figure 47 – M-500: Install Rail Kit

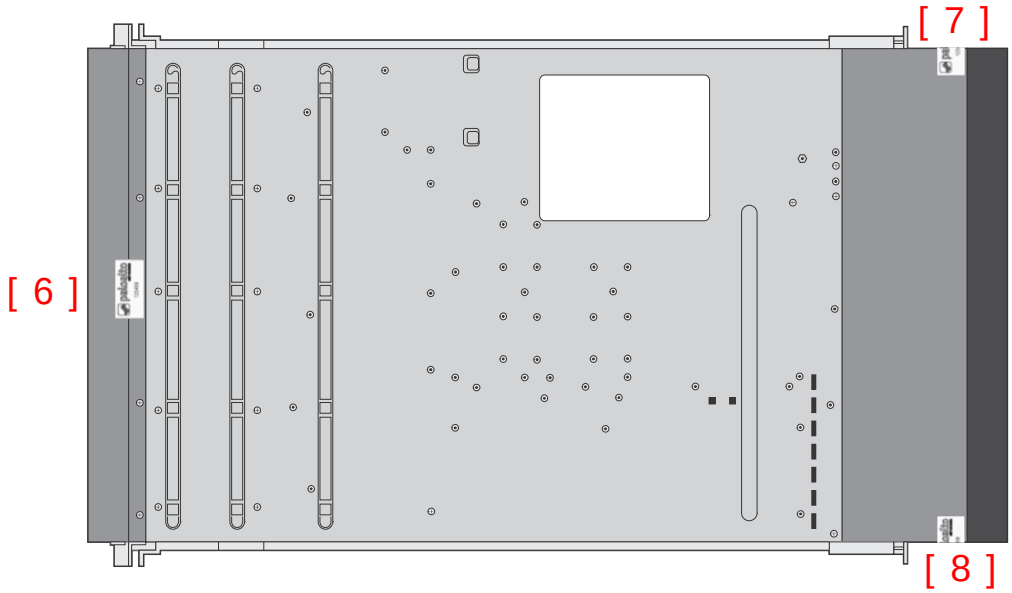

Figure 48 – M-500: Apply Tamper Seals on the Bottom of the Appliance

Step 8:

Place four (4) tamper seals on the top of the appliance. Two (2) tamper seals (#9 and #11) prevent tampering of the top front and rear opacity shields and two (2) tamper seals (#10 and #12) prevents someone from attempting to access the vent overlays by sliding the rail kit. This completes the FIPS kit installation.

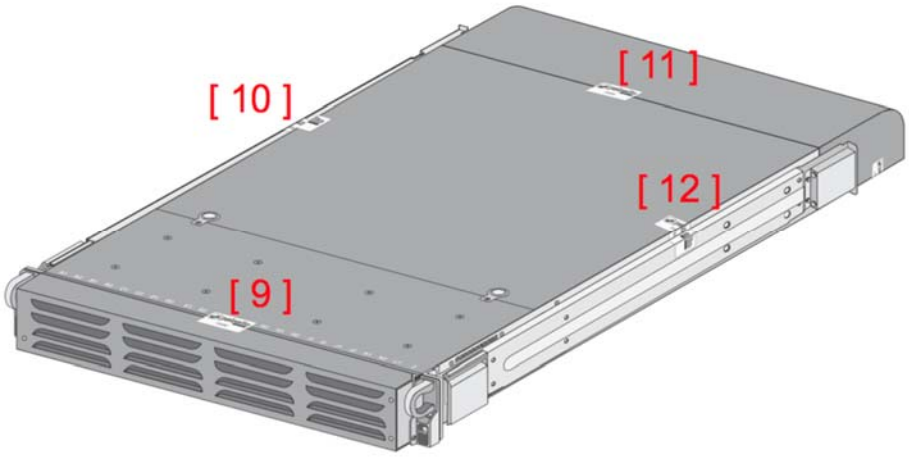

Figure 49 – M-500: Apply Tamper Seals on the Top and Sides of the Appliance

Appendix D – M-600 - FIPS Accessories/Tamper Seal Installation (21 Seals)

1. Replace the top cover with the FIPS 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 FIPS 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

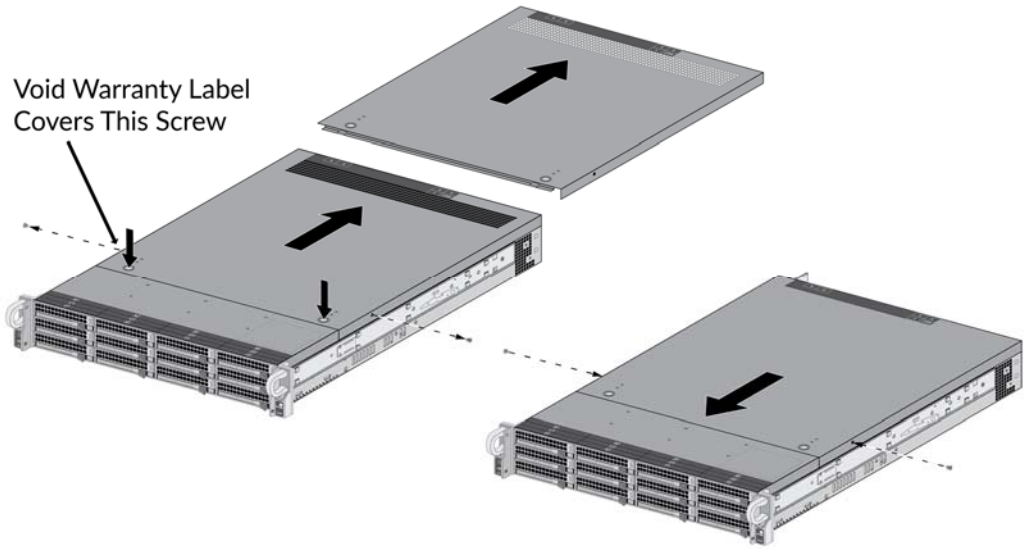

Figure 50 – M-600: Top Cover Replacement

2. Attach the FIPS 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 FIPS front-cover brackets under each handle, and then replace the handles and secure them using the screws that you removed. The FIPS handles have standoffs that are used to secure the front cover.

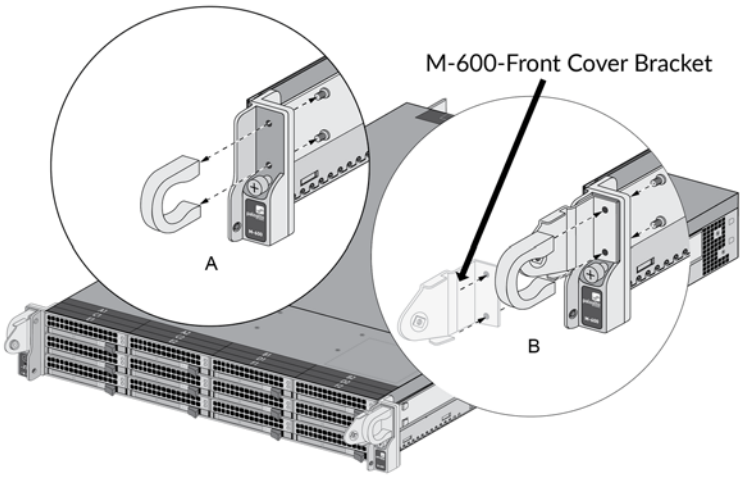

Figure 51 – M-600: Front Cover Bracket

3. Attach the FIPS front cover to the front of the appliance.

Slide the M-600 FIPS front cover over the FIPS pull handle brackets and secure the cover by turning the thumb screws clockwise (one thumb screw on each side).

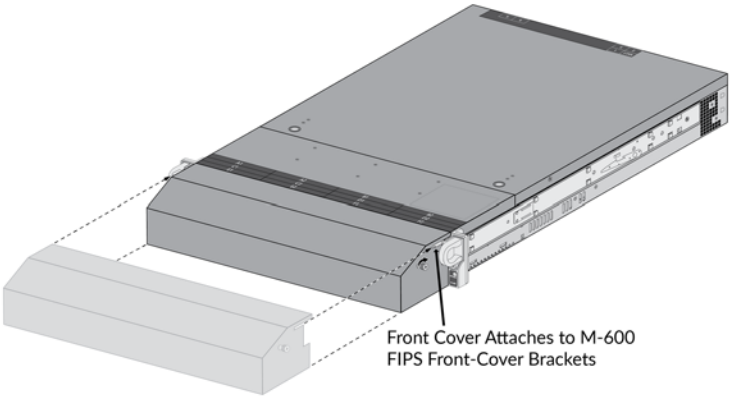

Figure 52 – M-600:FIPS Front Cover

4. Install a tamper-evident seal on the back of the appliance. This is seal #13 in the M-600 Figure 53. You need to install this seal before you install the M-600 FIPS back cover.
5. Attach the FIPS 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 in Figure 54). Apply two (2) tamper-evident seals on the power supplies (see seals #11 and #12 with rear inset of Figure 53).

    Before you apply the tamper-evident seals, ensure that the appliance and FIPS 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 FIPS kit surfaces.

M-600 Seal Placement (21 Seals)

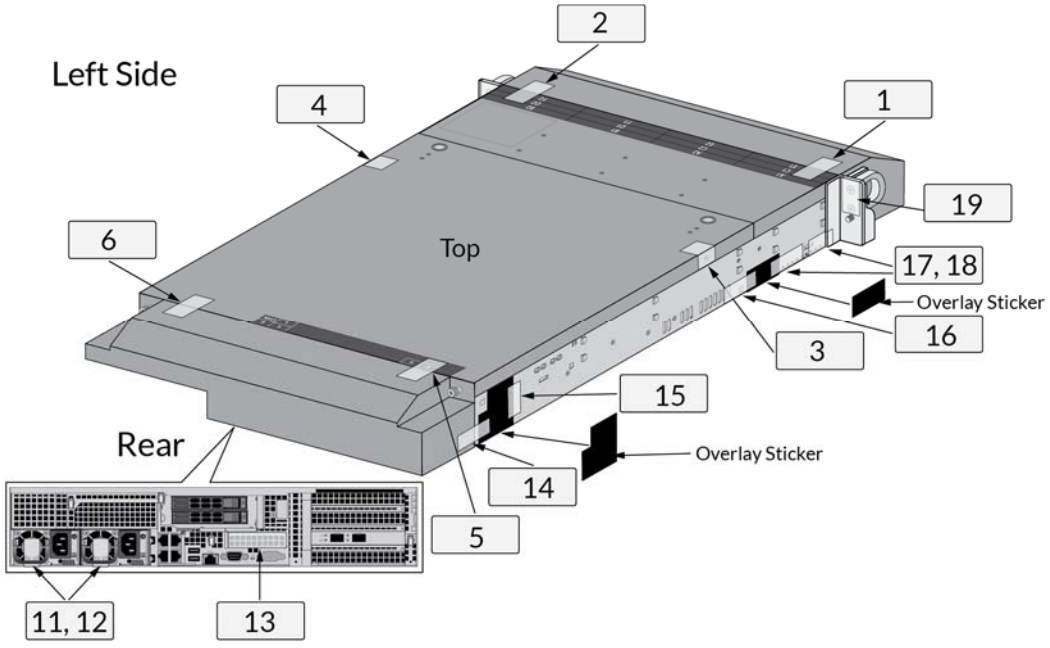

Figure 53 – M-600: Tamper Seal Locations (Top and Rear)

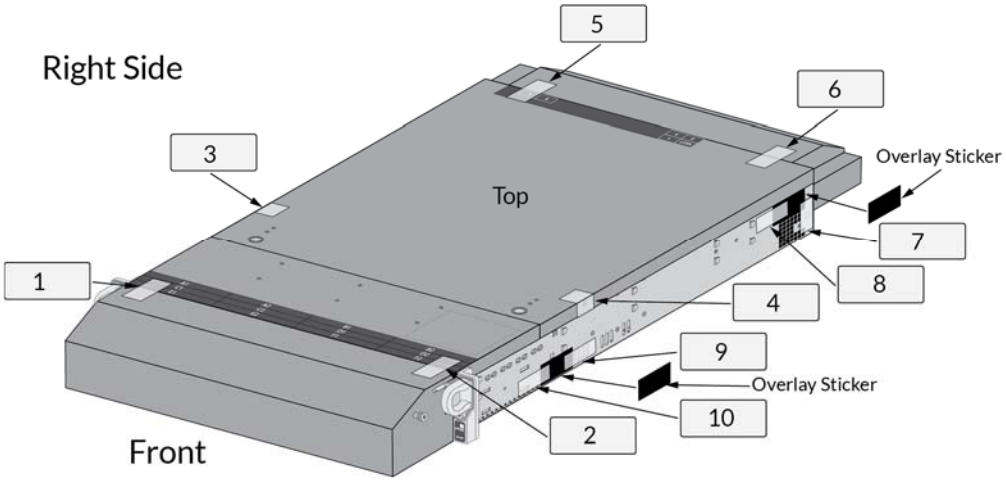

Figure 54 – M-600: Tamper Seal Locations (Top and Front)

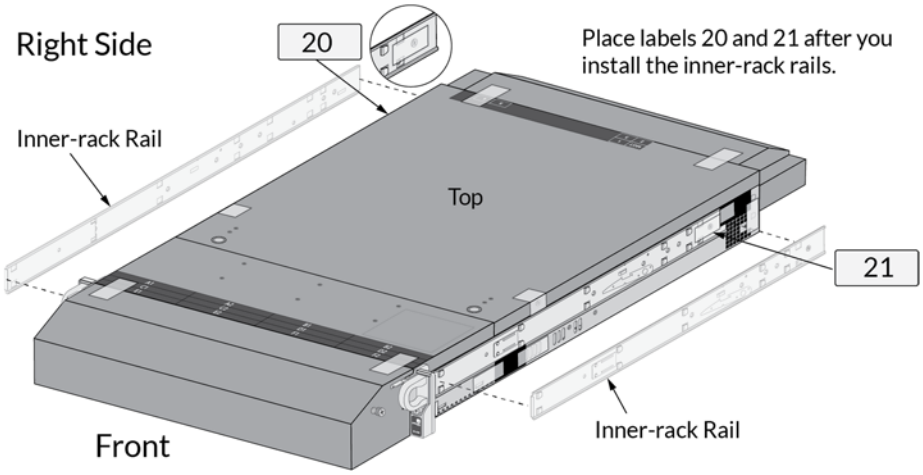

Figure 55 – M-600:Tamper Seals Location for Side Rails