Panorama M-100 and M-500

FIPS 140-2 Non-Proprietary Security Policy

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

Date: 10/1/2018

Change Record

Table 1 - Change Record

Date	Author	Description of Change
3/20/2017	A. Shahhosseini	Initial Authoring
12/27/2017	A. Shahhosseini	Updates for new firmware version (8.0.3)
1/12/2018	A. Shahhosseini	Updates to address CMVP comments
4/11/2018	A. Shahhosseini	Added firmware version 8.0.9
10/1/2018	A. Shahhosseini	Added firmware version 8.0.12 and 8.0.13

Contents

Tables

Figures

1 Module Overview

Panorama 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.
    - Manager: 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.
    - 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 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 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, while the M-500 is demonstrated in Figure 4 through Figure 8. 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 Hardware 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	8.0.3, 8.0.9, 8.0.12, or 8.0.13
Panorama M-100 4TB RAID: 8 x 1TB RAID Certified HDD for 4TB of RAID Storage	910-000092	00D	920-000140	00A	8.0.3, 8.0.9, 8.0.12, or 8.0.13
Panorama M-500	910-000073	00D	920-000145	00A	8.0.3, 8.0.9, 8.0.12, or 8.0.13

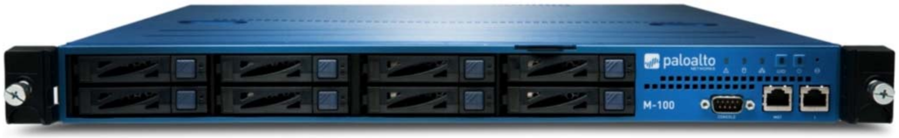

Figure 1 – Front of M-100

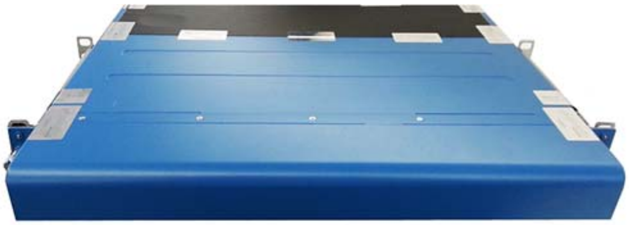

Figure 2 – Front of M-100 with FIPS Kit

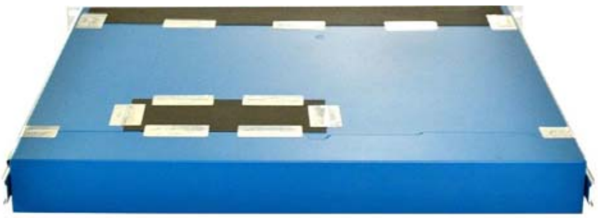

Figure 3 – Rear of M-100 with FIPS Kit

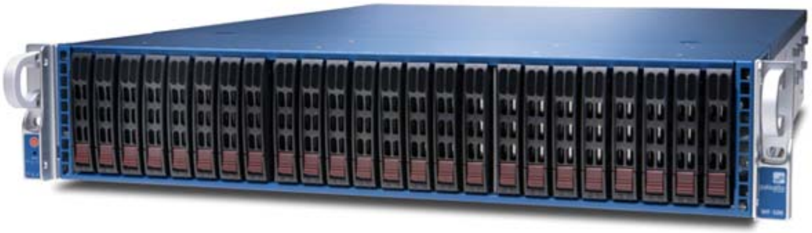

Figure 4 –Front of M-500

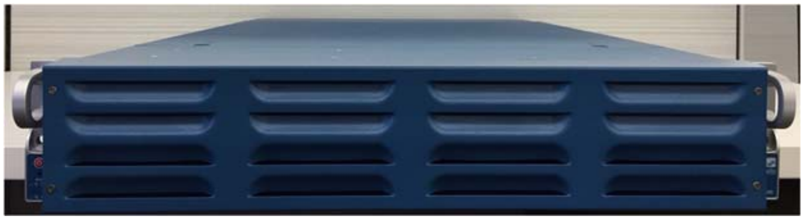

Figure 5 – Front of M-500 with FIPS Kit

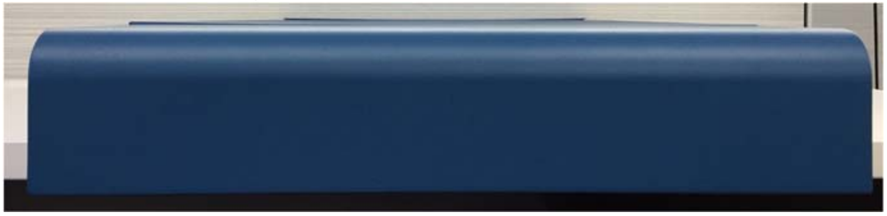

Figure 6 – Rear of M-500 with FIPS Kit

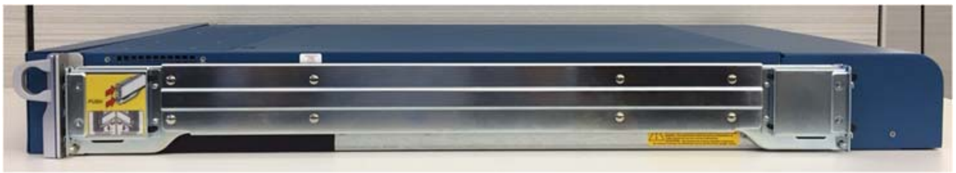

Figure 7 – Right View of M-500 with FIPS Kit

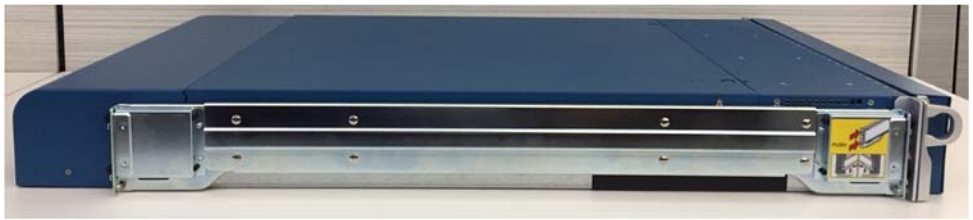

Figure 8 – Left View of M-500 with FIPS Kit

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 Manager 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 Manager mode. The Log Collector mode of operation is a secondary mode that provides a focused log forwarding capability. Directions to convert the appliance into the Log Collector mode are discussed below in Section 2.4. The M-500 provides a third mode, PAN-DB Private Cloud server.

Convert the M-100/M-500 appliance from Panorama Log Collector 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 Manager mode.

- The system will reboot and perform the required power on self-tests.

Convert the M-500 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 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 Manager mode.
- The system will reboot and perform the required power on self-tests.

2.3 Security Levels for the Panorama Manager 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	3
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 Manager 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-500 appliance from Panorama Manager 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.

See Section 2.2 for directions on changing from the Panorama Log Collector mode back to the Panorama Manager mode.

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	3
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 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 CFB mode; Encrypt/Decrypt; 128-bit Note: CCM 128-bit, OFB, CFB 192-bit and CFB 256-bit modes were tested but not used by the module.	4532
AES-GCM [SP800-38D]: Encrypt and Decrypt, 128 and 256-bit Functions: Authenticated Encryption, Authenticated Decryption Note 1: GCM is used compliant with SP 800-52 and used in accordance to Section 4 of RFC 5288 for TLS key establishment. Note 2: GCM 192-bit was tested but is not used by the module. Note 3: GCM is used compliant with IG A.5 (option 4) for SSH key establishment.	4532
CVL: Elliptical Curve Diffie-Hellman Exchange [SP800-56A] -ECC CDH Primitive (Section 5.7.1.2) -KAS-ECC all except KDF	1211
CVL: Diffie-Hellman Exchange [SP800-56A] KAS-FFC all except KDF	1211
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.	1212
CVL: RSA [SP800-56B] Function: Key Transport -RSADP	1213
CKG: Function: Key Generation Method 1: Asymmetric Key Generation (SP800-133 §6) Method 2: Symmetric Key Generation (SP800-133 §7.1, 7.2, 7.3)	VA
DRBG [SP800-90A]	

FIPS Approved Algorithm	CAVP Cert. #
-CTR DRBG with AES-256	1489
DSA [FIPS 186-4] -Key Pair Generation: 2048 bits	1207
ECDSA [FIPS 186-4] -Key Pair Generation: P-256, P-384, P-521 -Signature Generation: P-256, P-384, and P-521 -Signature Verification: P-256, P-384, and P-521 Note: PKV P-256, P-384 were tested but are not used by the module.	1103, CVL 1214
HMAC-SHA-1/HMAC-SHA-256/HMAC-SHA-384/HMAC-SHA-512 [FIPS 198-1] Functions: Generation, Verification	2990
KAS: SP 800-56A Rev.2 Diffie-Hellman Exchange (CVL Certs. #1211 and #1212, vendor affirmed; key agreement; key establishment methodology provides 112 bits of encryption strength)	N/A
KAS: SP 800-56A Rev.2 Elliptic Curve Diffie-Hellman Exchange (CVL Certs. #1211 and #1212, vendor affirmed; key agreement; key establishment methodology provides between 128 and 256 bits of encryption strength)	N/A
KTS [SP800-38F §3.1]: AES-GCM (Key wrapping; key establishment methodology provides between 128 bits and 256 bits of encryption strength)	4532
KTS [SP800-38F §3.1]: AES-CBC plus HMAC AES-CTR plus HMAC (Key wrapping; key establishment methodology provides between 128 bits and 256 bits of encryption strength)	4532 (AES) 2990 (HMAC)
RSA [FIPS 186-4] - Key Pair Generation: 2048 and 3072-bit - Signature Generation (ANSI X9.31, RSASSA-PKCS1_v1-5, RSASSA-PSS): 2048 and 3072-bit with hashes (SHA-1*/256/384/512) - Signature Verification (ANSI X9.31, RSASSA-PKCS1_v1-5, RSASSA-PSS): 1024, 2048 and 3072-bit with hashes (SHA-1/256/384/512) *Only used for signature generation in SSH in the Approved Mode	2467

FIPS Approved Algorithm	CAVP Cert. #
SHA-1, SHA-256, SHA-384, SHA-512 [FIPS 180-4] Functions: Digital Signature Generation, Digital Signature Verification, non-Digital Signature Applications Note: SHA-224 was tested but is not used by the module.	3713

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. #1211 with CVL Cert. #1212, key agreement; key establishment methodology provides 112 bits of encryption strength)
MD5 (within TLS)
NDRNG (seeding source) This provides a minimum of 256 bits of entropy.
RSA (key wrapping, key establishment methodology provides 112 bits or 128 bits of encryption strength)

Table 7 - Supported Protocols in FIPS Approved Mode

Supported Protocols*
TLS v1.0, 1.1 and 1.2
SSHv2
SNMPv3

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

2.7 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
Firmware Integrity Check: HMAC-MD5
Hashing: RIPEMD, MD5
Encrypt/Decrypt: Camellia, ARCFOUR, SEED, Triple-DES, Blowfish, CAST, RC4
Message Authentication: UMAC, HMAC-MD5, HMAC-RIPEMD
Digital Signatures (non-Approved strengths or non-Approved Hashes): RSA, ECDSA, DSA
Key Exchange (non-Approved strengths): EC Diffie-Hellman (sect571r1, sect571k1, sect409k1, sect409r1, sect283k1, sect283r1, secp256k1, sect239k1, sect233k1, sect233r1, secp224k1, secp224r1, sect193r1, sect193r2, secp192k1, secp192r1, sect163k1, sect163r1, sect163r2, secp160k1, secp160r1, secp160r2 Diffie-Hellman (1024 bits) Non-signature verification RSA (Less than 2048 bits)

3 Ports and Interfaces

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

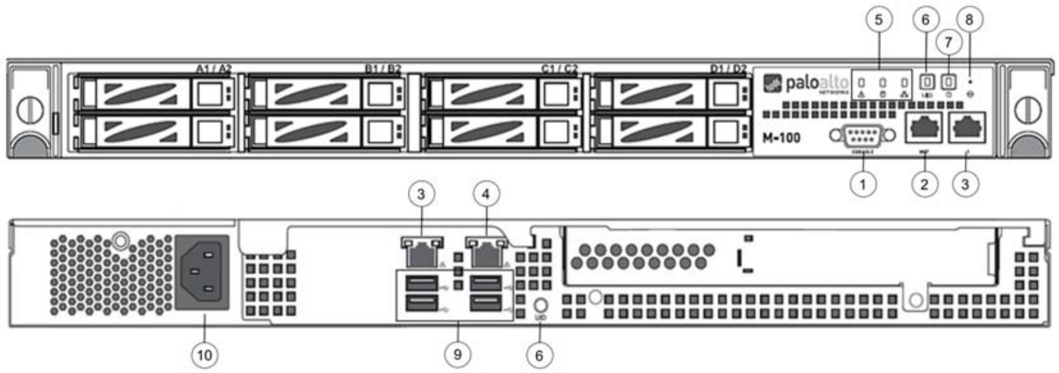

Figure 9 – M-100 Ports and Interfaces

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

Interface		Name and Description	Qty.	FIPS 140-2 Designation
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 9. 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-500 module provides the following ports and interfaces.

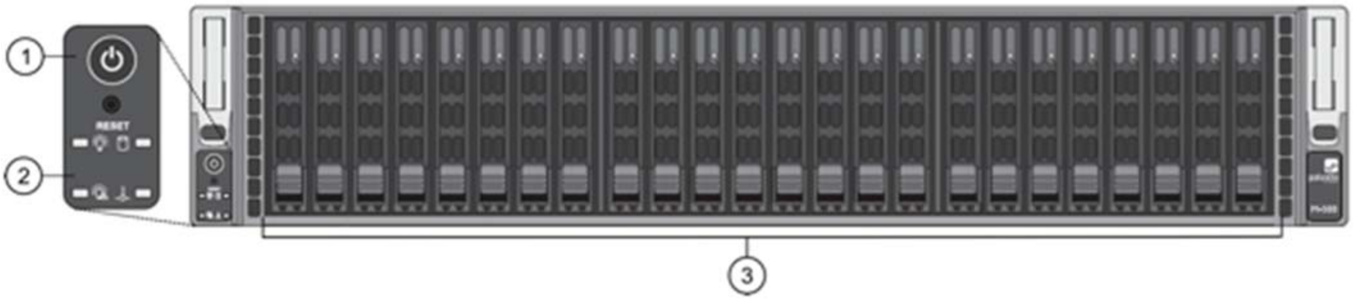

Figure 10 – M-500 Front ports and Interfaces

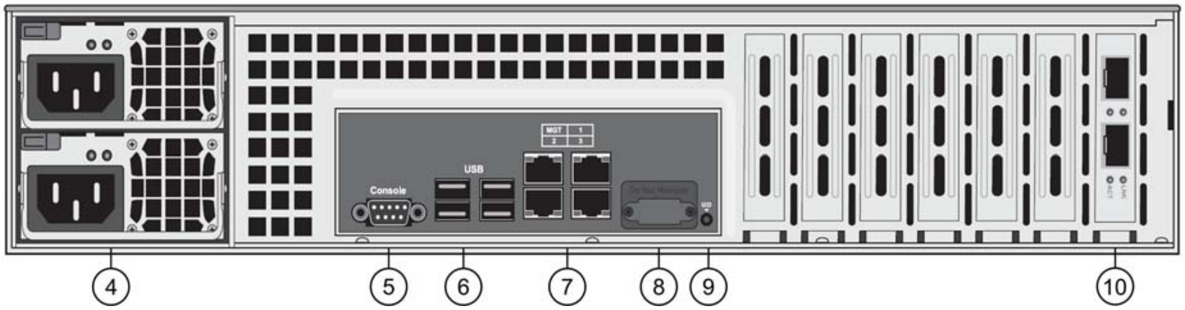

Figure 11 – M-500 Back ports and Interfaces

Table 10 – 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	2	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.				

4 Identification and Authentication Policy

4.1 *Assumption of Roles*

The module supports distinct operator roles. The cryptographic module in Manager mode and PAN-DB mode enforce 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 11 – Manager 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 12 - 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

Table 13 - 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 14 - 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 module supports four (4) authentication requests per one (1) second, which is equal to 240 attempts per minute. The probability of successfully authenticating to the module within one minute is 240/(95^6), which is less than 1/100,000.
Certificate/public key based authentication	The security modules support certificate-based authentication using RSA 2048, RSA 3072, ECDSA P-256 or ECDSA P-384. For RSA, 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. For ECDSA, the minimum equivalent strength supported is 128 bits. The probability that a random attempt will succeed is 1/(2^{128}), 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^{128}), 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 15 - 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 or 3072 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 or P-521)
TLS Pre-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	AES 256 CTR DRBG used in the generation of a random values
SNMPv3 Secrets	SNMPv3 Authentication Secret and Privacy Secret
SNMPv3 Keys	AES Privacy key and HMAC- SHA-1 Authentication keys

Key/CSP	Description
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 below. The CSPs and keys may be shared between the Approved modes of operation.	

Table 16 - Public Keys

Key Name	Description
CA certificates	Used to extend trust for certificates (RSA or ECDSA)
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 or 3072 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 or P-384)
Client Authentication Public Key	Used to authenticate the end user (ECDSA P-256 or P-384; RSA 2048 or 3072 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 or 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 or 3072 bits)
SSH Host ECDSA public key	Used in SSH public key authentication process (ECDSA P-256, P-384, or P-521)
SSH Client RSA public key	Used in SSH public key authentication process (RSA 2048 or 3072 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) *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 below. 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.

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 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 17 - Authenticated Services – Panorama M-100/M-500 Manager

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 and configuration screens. Provides no configuration commit capability.	N/A
Panorama Firmware Update	Download and install software and firmware updates	N/A
Panorama Manager Setup	Presents configuration options for management interfaces and communication for peer services (e.g., SNMP). Import, Export, Save, Load, revert and validate Panorama configurations and state	Import or Export RSA/ECDSA Private/Public Keys Import SNMPv3 Secrets
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
Configure High Availability	Configure High Availability communication settings	N/A
Panorama Certificate Management	Manage RSA/ECDSA certificates and private keys, certificate profiles, revocation status and usage.	Import or export RSA /ECDSA private/public keys Generate RSA/ECDSA private/public keys Sign RSA/ECDSA private keys Execute DRBG seed and state

Service	Description	CSP/Key Access
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 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
Configure Managed Device Groups	Define and manage common base of policies and data objects for managed firewalls in configured device groups	N/A
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.	N/A

Service	Description	CSP/Key Access
Monitor network activity	Review aggregated information across all managed firewalls. This 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 18 - Authenticated Services – Panorama M-100/M-500 Log Collector

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.	N/A
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 and usage.	Import or export RSA/ECDSA private/public keys Generate RSA/ECDSA private/public keys Sign with RSA/ECDSA private keys Execute DRBG seed and state

Table 19 - Authenticated Services – Panorama M-500 Private Pan-DB

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 and configuration screens. Provides no configuration commit capability.	N/A
Panorama Firmware Update	Download and install software and firmware updates	N/A
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 20 - 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.
Self-Tests	Run power up self-tests on demand by power cycling the module. Execute access to FW integrity Check key.
Show Status (LEDs)	View status of the module via the LEDs.
Show Status (SNMPv2c)	SNMPv2c provides system status and information. There is neither read nor write access to CSPs.

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 and M-500 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 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 GCM Encrypt Known Answer Test
            d. AES GCM Decrypt Known Answer Test
            e. AES CCM Encrypt Known Answer Test
            f. AES CCM Decrypt Known Answer Test
            g. ECDSA Sign Known Answer Test
            h. ECDSA Verify Known Answer Test
            i. RSA Sign Known Answer Test
            j. RSA Verify Known Answer Test
            k. RSA Encrypt Known Answer Test
            l. RSA Decrypt Known Answer Test
            m. HMAC-SHA-1 Known Answer Test
            n. HMAC-SHA-256 Known Answer Test
            o. HMAC-SHA-384 Known Answer Test
            p. HMAC-SHA-512 known Answer Test
            q. SHA-1 Known Answer Test

r. SHA-256 Known Answer Test
s. SHA-384 Known Answer Test
t. SHA-512 Known Answer Test
u. DRBG Known Answer Test
v. ECDH Known Answer Test
w. DH Known Answer Test
x. 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.

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 labels that are applied on the modules by the Crypto-Officer. There are 28 tamper-evident labels for the M-100 and 12 for the M-500. All unused labels are to be controlled by the Crypto-Officer. The labels prevent removal of the opaque enclosure without evidence. The Crypto-Officer must ensure that the module surface is clean and dry. Tamper evident labels 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 labels. The labels prevent removal of the opaque enclosure without evidence. The Crypto-Officer should inspect the labels and shields for evidence of tamper every 30 days. If the labels 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 and B for instructions on installation and placement of the tamper labels and opacity shields. The locations of the tamper evident labels implemented on the M-100 and M-500 are shown in Appendix A and Appendix B, respectively.

9.2 *Operator Required Actions*

Table 21 - Inspection/Testing of Physical Security Mechanisms

Model	**Physical Security Mechanisms**	**Recommended Frequency of Inspection/Test**	**Inspection/Test Guidance Details**
M-100	Tamper Evident Labels	30 days	Verify integrity of tamper evident labels in the locations identified in Appendix A of this Security Policy.
M-100	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	Tamper Evident Labels	30 days	Verify integrity of tamper evident labels in the locations specified in Appendix B.
M-500	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	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

13 Appendix A – M-100 - FIPS Accessories/Tamper Label Installation (28 Labels)

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

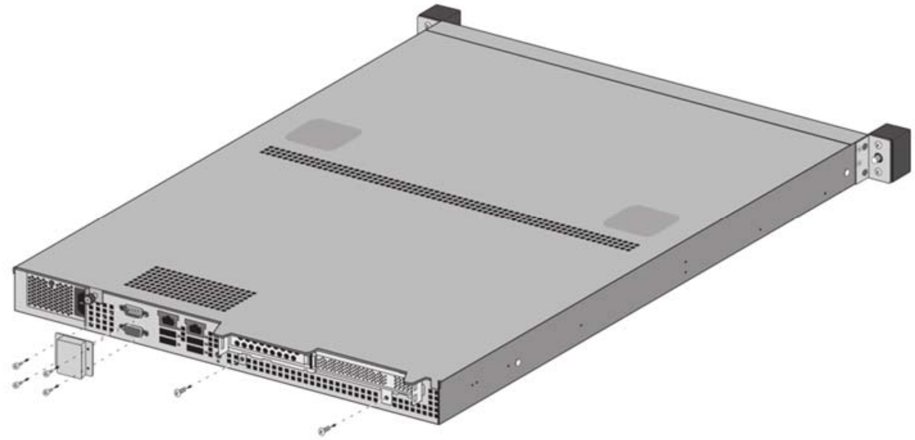

Figure 12 - Remove Screws on Rear Side

Step 2: Attach the rear opacity shields.

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

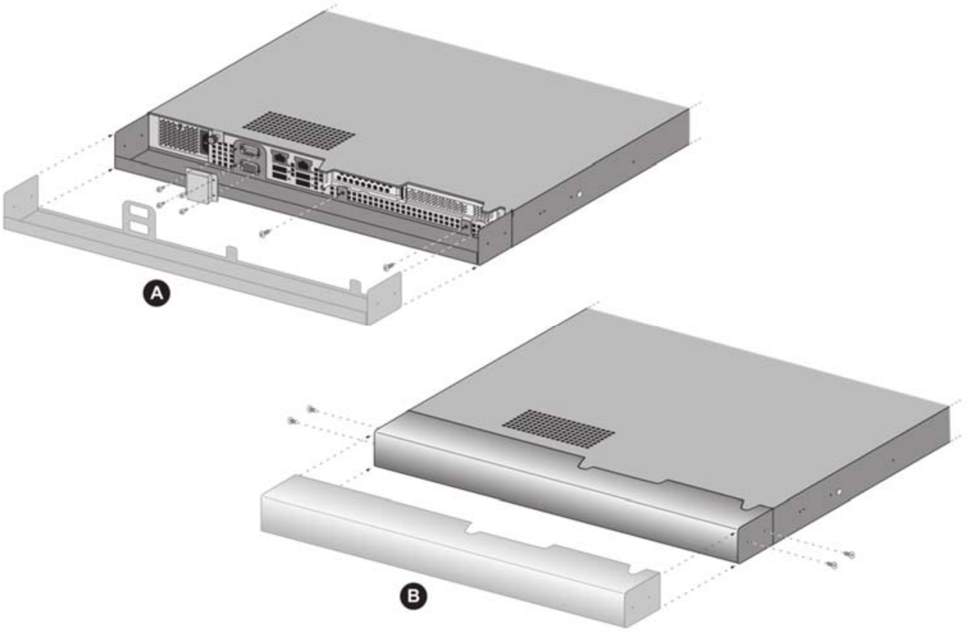

Figure 13 - Attach Rear Opacity Shield

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

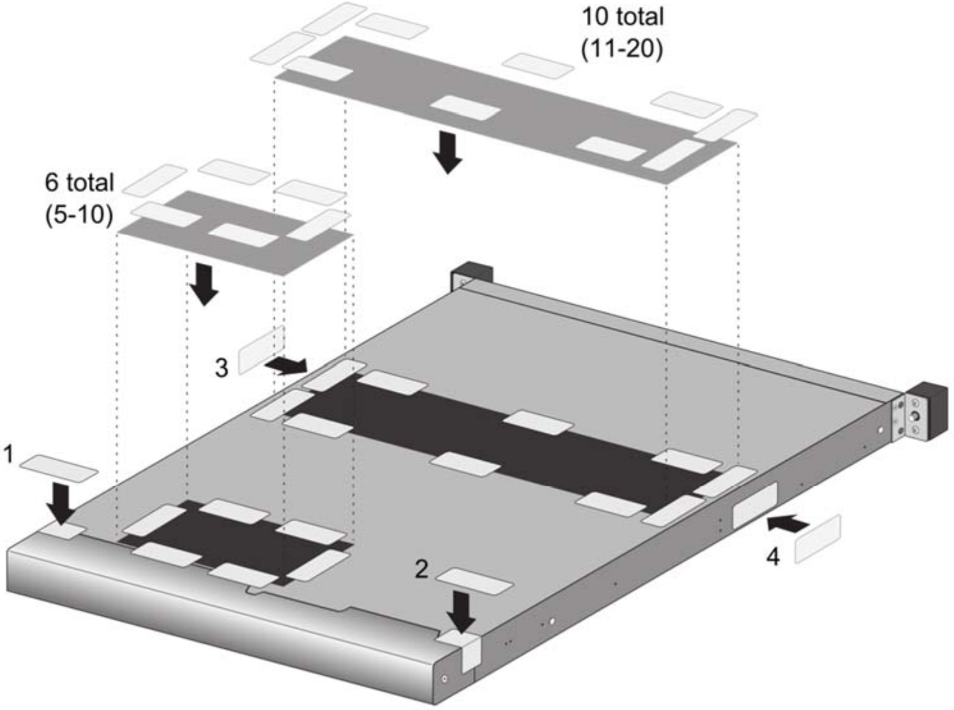

Figure 14 - Apply Tamper Seals and Vent Overlays

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

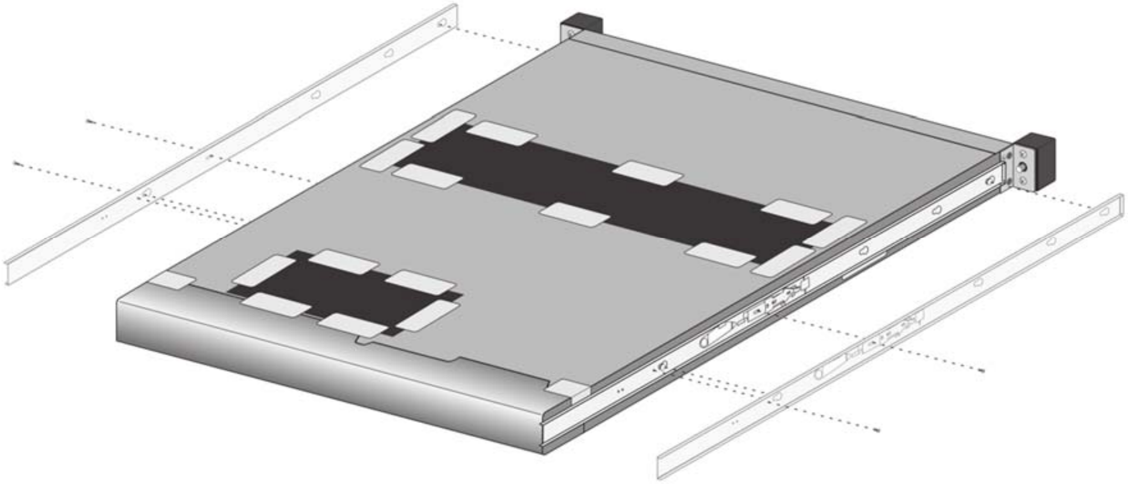

Figure 15 - Apply Rail Kit

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

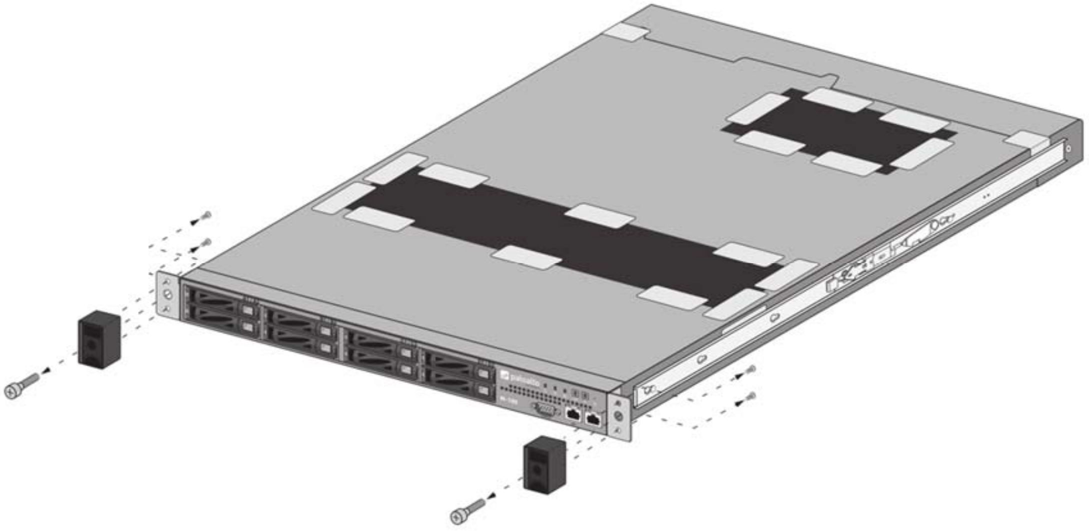

Figure 16 - Remove Front Plastic Bracket Covers and Screws

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

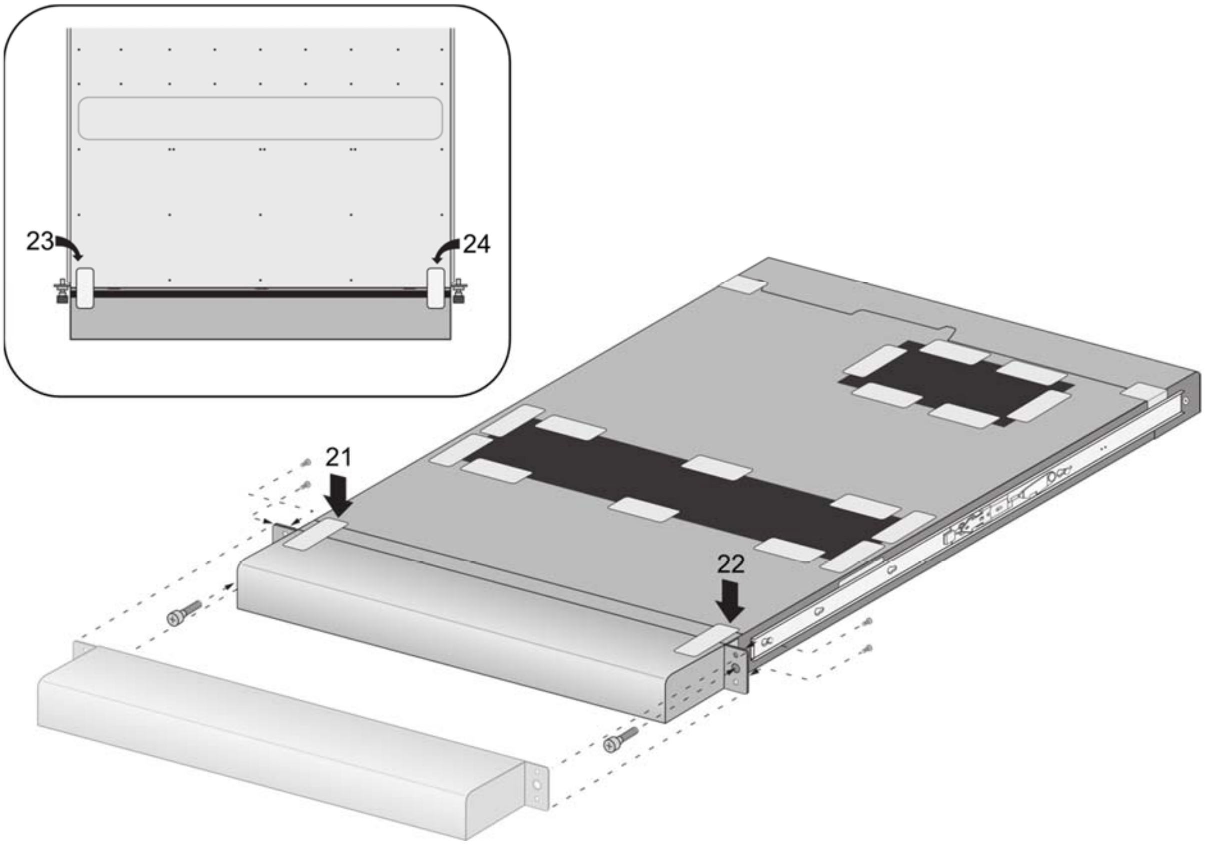

Figure 17 - Install Front Opacity Shield

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

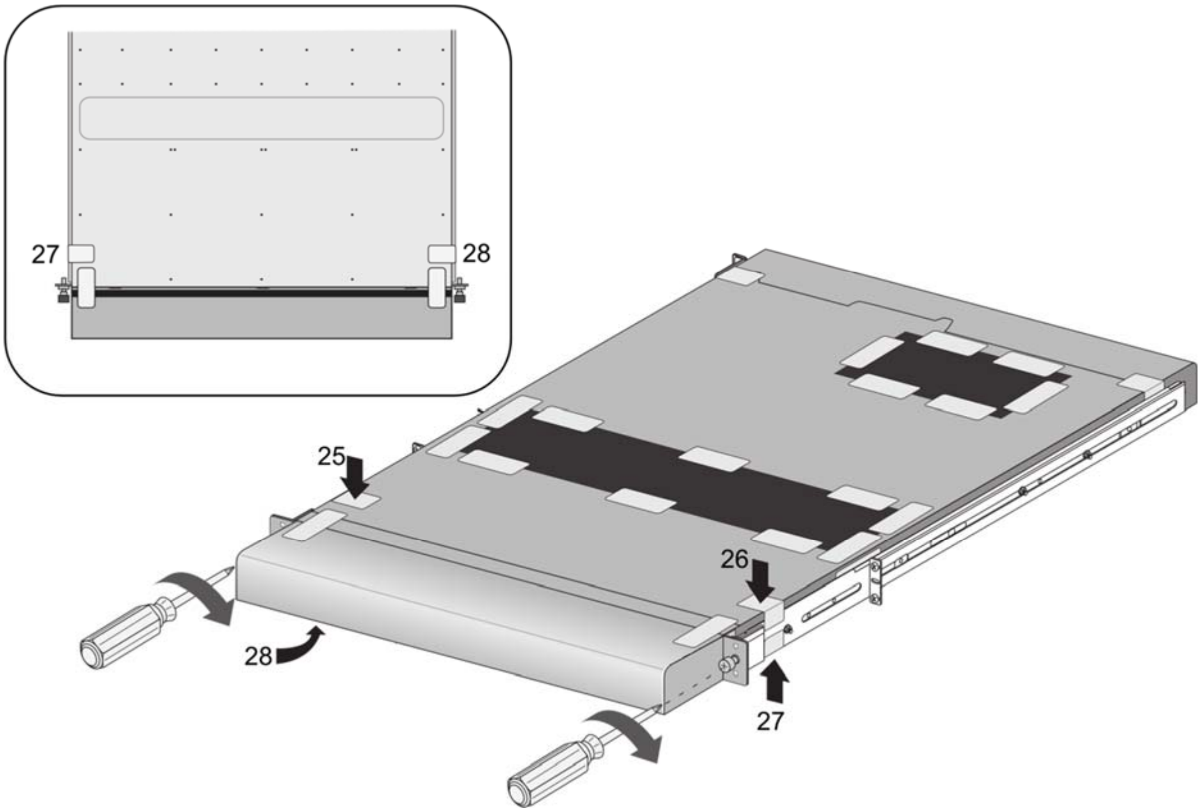

Figure 18 - Install Outer Rails

14 Appendix B – M-500 - FIPS Accessories/Tamper Label Installation (12 Labels)

Step 1:

Remove the two pull handles and front modules on the left and right side of the appliance by removing the three 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.

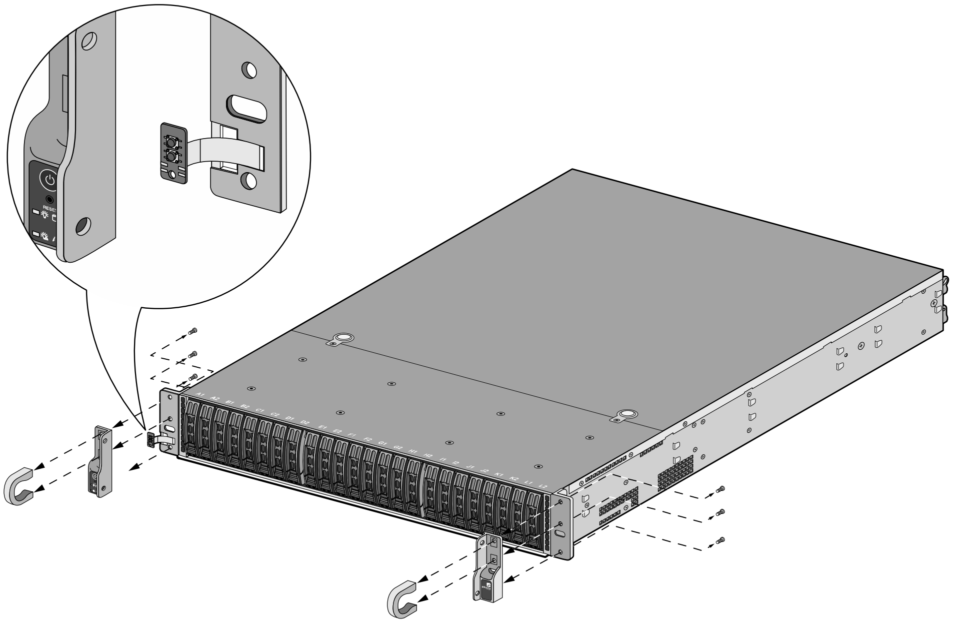

Figure 19 - Remove Front Handles and Modules

Step 2:

Attach the left and right front cover brackets to the appliance using the six screws that you removed in Step 1. First attach the brackets using the bottom screws (one on each side) as shown in Figure 20, 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 21.

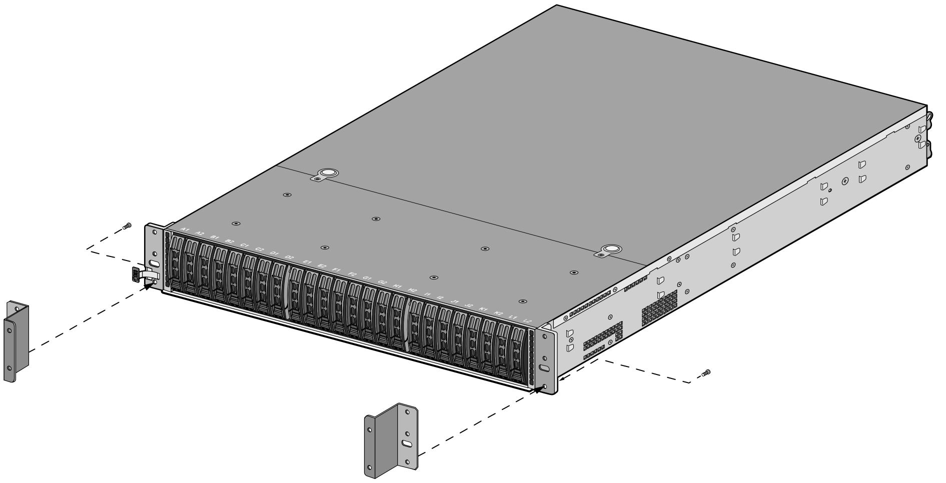

Figure 20 - Secure the Front Brackets

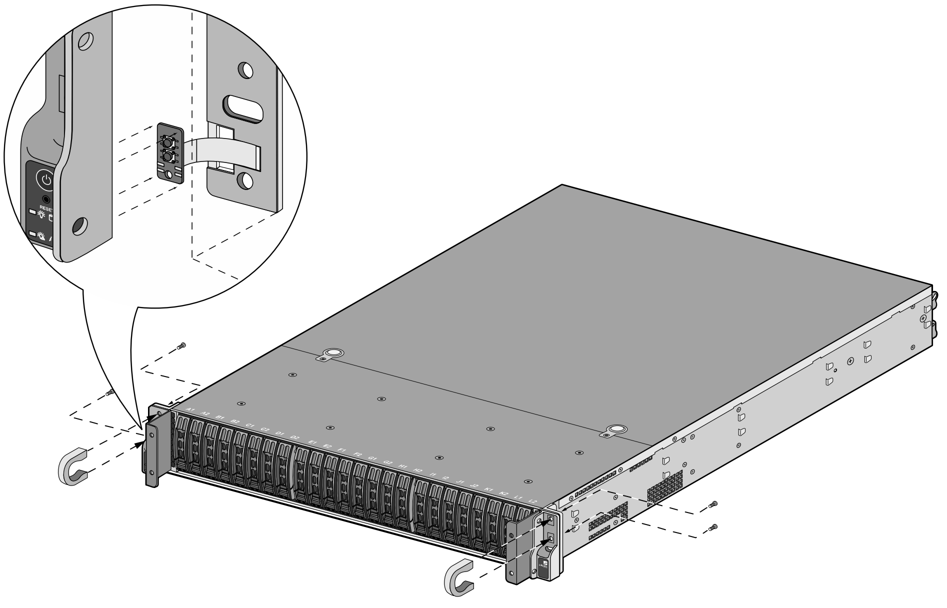

Figure 21 - Attach Pull Handles and Front Modules

Step 3:

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

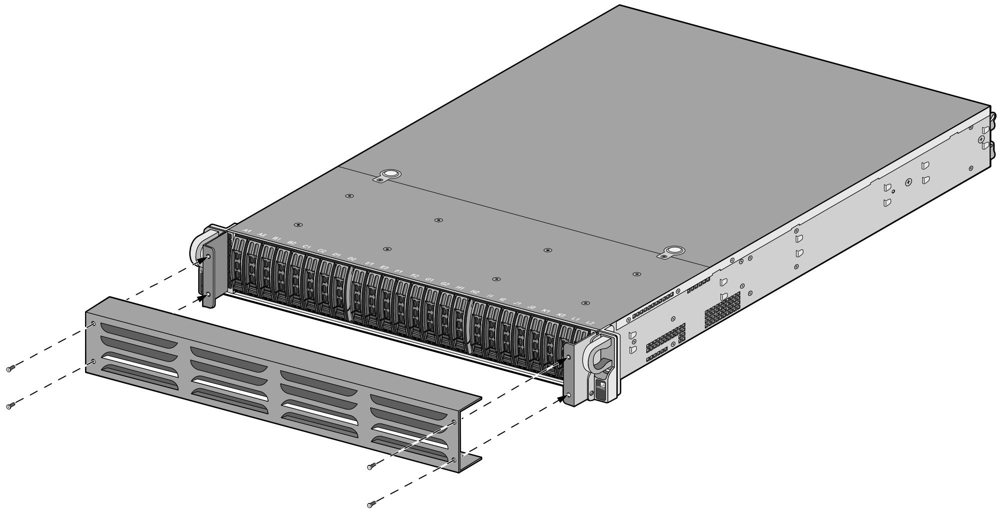

Figure 22 – Install Front Opacity Shield

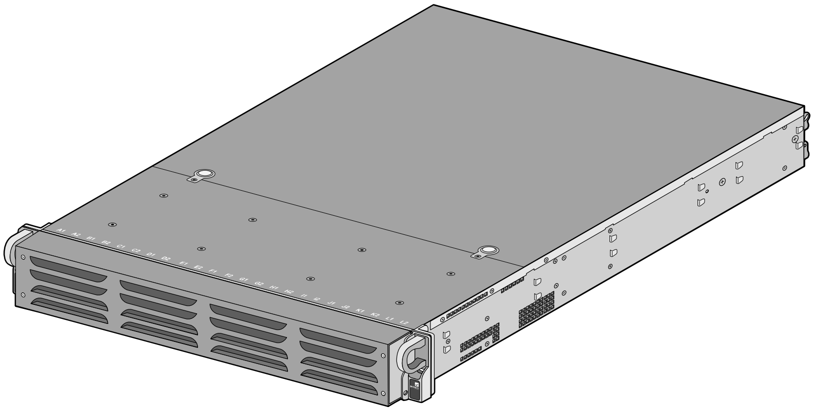

Figure 23 – Front Opacity Shield Installed

Step 4:

Attach the rear opacity shield tray to the appliance. First, remove the two screws (shown in Figure 24) 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.

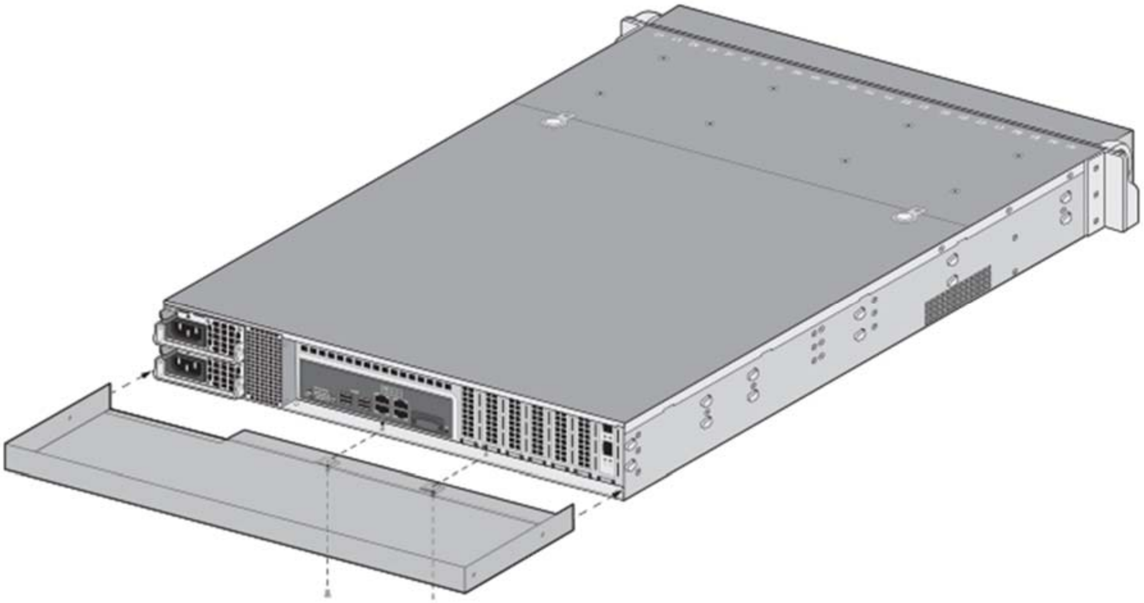

Figure 24 – Install Rear Opacity Shield Tray

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 screws (provided) on each side.

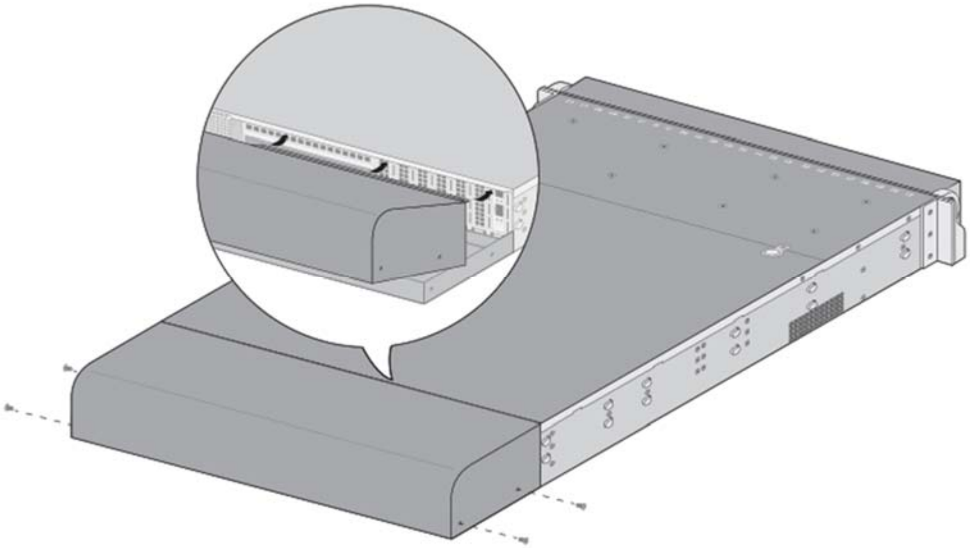

Figure 25 – Install Rear Opacity Shield

Step 6:

Cover the vent openings as shown in Figure 26 by applying one overlay sticker over the left side vent and one overlay sticker over the right side vent. Each overlay requires two tamper labels as shown in Figure 27. Also apply one additional tamper label as shown in Figure 27 Item 5.

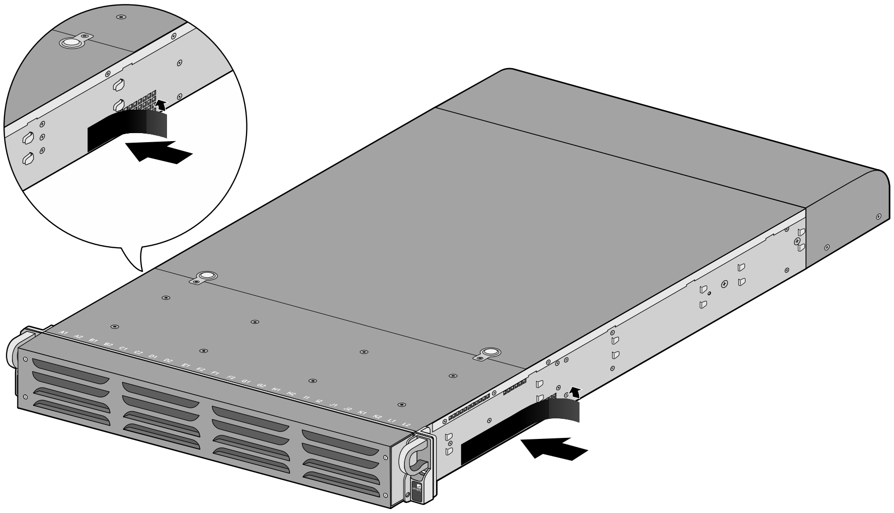

Figure 26 – Apply Vent Overlays

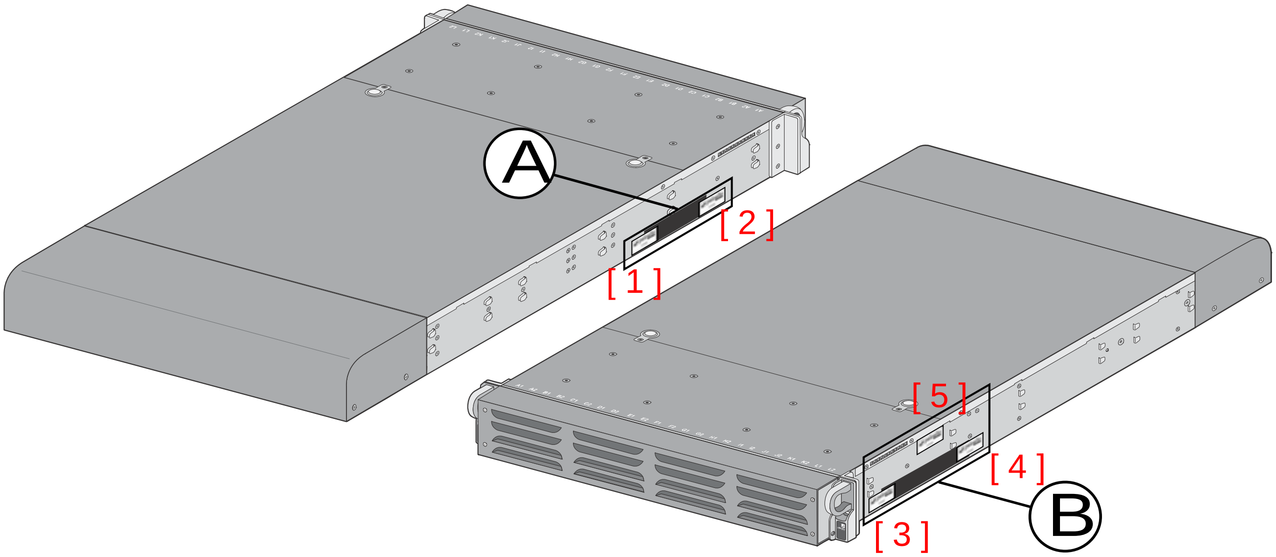

Figure 27 – Apply Tamper Labels on Vent Overlays and Side Opening

Step 7:

Re-attach the rail kit to the appliance as shown in Figure 28 and then add three tamper labels to the bottom of the appliance as shown in Figure **29**. One tamper label prevents tampering of the front opacity shield connected to the bottom of the appliance and two tamper labels wrap around the upper and lower rear opacity shields to prevent tampering of the rear opacity shields.

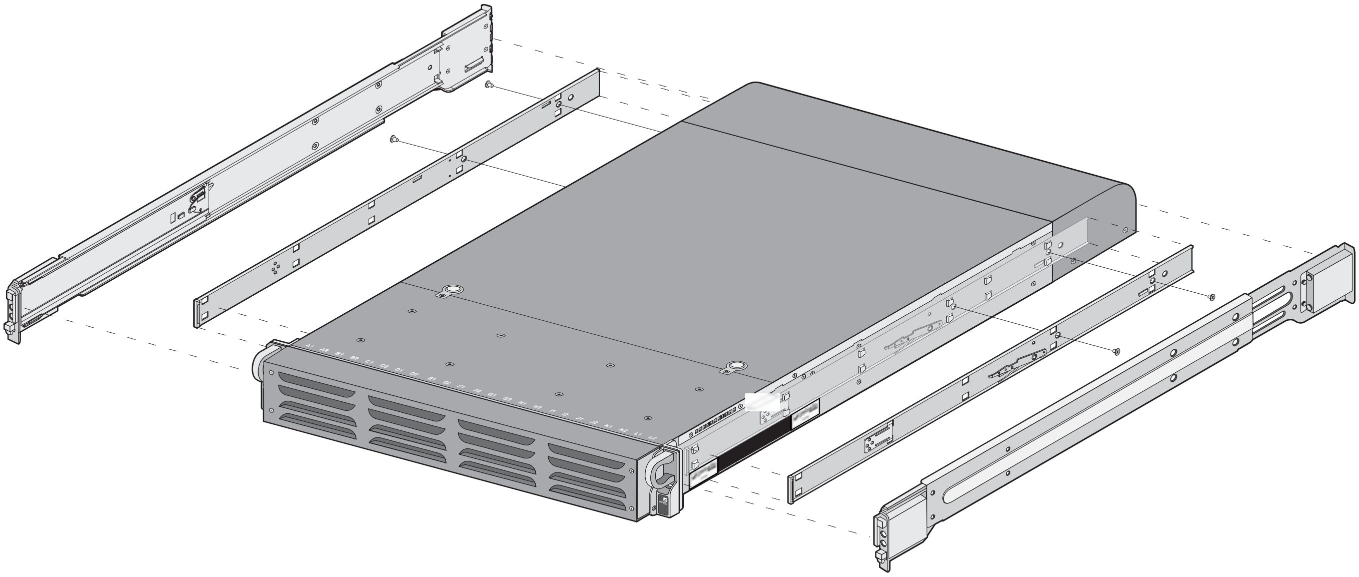

Figure 28 – Install Rail Kit

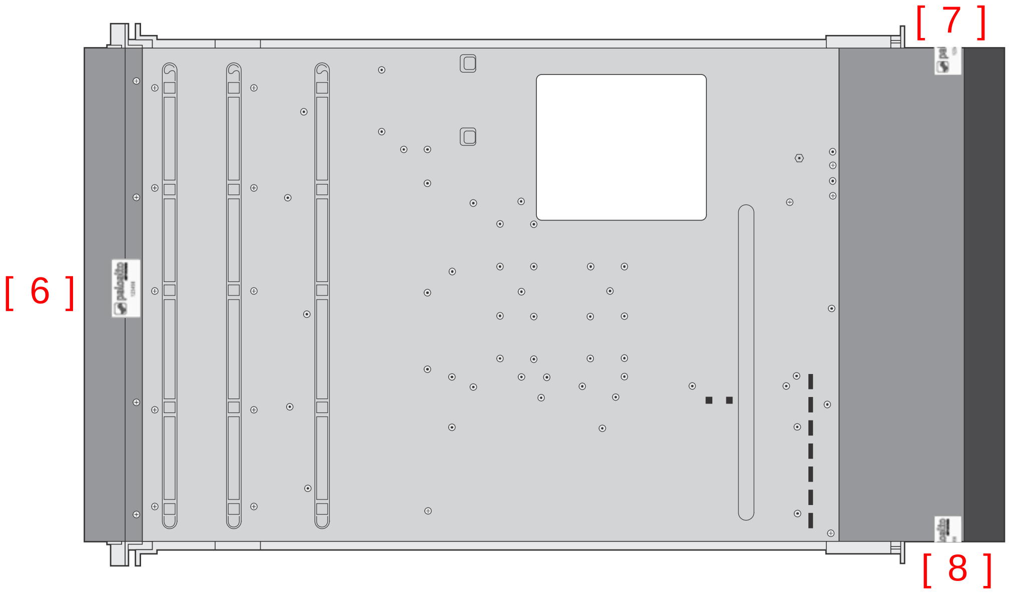

Figure 29 **– Apply Tamper Labels on the Bottom of the Appliance**

Step 8:

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

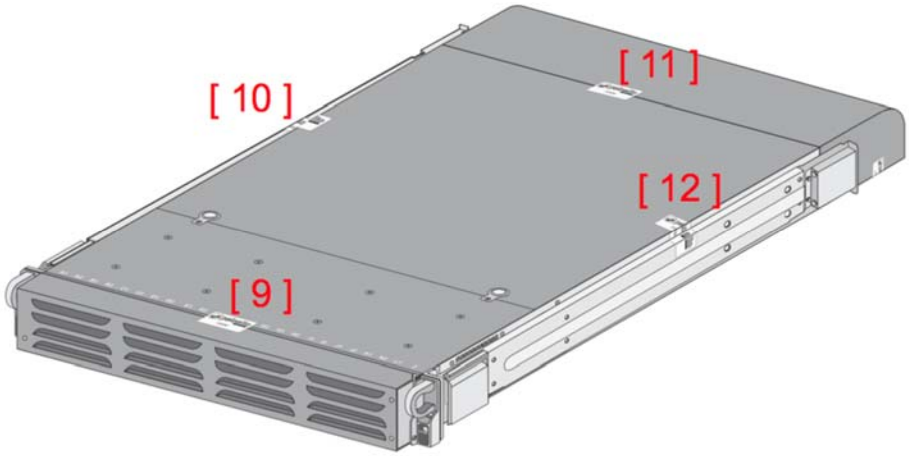

Figure 30 – Apply Tamper Labels on the Top and Sides of the Appliance