Palo Alto Networks

Panorama 10.1 on Hardware Appliances

FIPS 140-3 Non-Proprietary Security Policy

Version: 1.1

Revision Date: August 29, 2024

Palo Alto Networks, Inc.
www.paloaltonetworks.com

Table of Contents

1. General

The Panorama 10.1 on Hardware Appliances from Palo Alto Networks Inc., hereafter referred to as “Panorama M-Series”, “modules”, or the “cryptographic modules” are multi-chip standalone hardware cryptographic modules designed to fulfill FIPS 140-3 level 2 requirements. Panorama M-Series management appliances provide centralized management and visibility of Palo Alto Networks next generation firewalls. From a central location, you can gain insight into applications, users, and content traversing the firewalls. The knowledge of what is on the network, in conjunction with safe application enablement policies, maximizes protection and control while minimizing administrative effort. Your security team can centrally perform analysis, reporting, and forensics with the aggregated data over time, or on data stored on the local firewall.

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

- Centralized: In this scenario, all Panorama management and logging functions are combined into a single device.
- Distributed: you can separate the management and logging functions across multiple devices, splitting the functions between managers and log collectors.
    - 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 cryptographic module meets the overall requirements applicable to Level 2 security of FIPS 140-3.

Table 1 - Security Levels

ISO/IEC 24759 Section 6.	FIPS 140-3 Section Title	Security Level
1	General	2
2	Cryptographic Module Specification	2
3	Cryptographic Module Interfaces	2
4	Roles, Services, Authentication	3
5	Software/Firmware Security	2
6	Operational Environment	N/A
7	Physical Security	2
8	Non-Invasive Security	N/A
9	Sensitive Security Parameter Management	2
10	Self-Tests	2
11	Life-Cycle Assurance	3
12	Mitigation of Other Attacks	N/A
Overall Level		2

2. Cryptographic Module Specification

The configurations for this validation are highlighted in Table 2.

Table 2 - Cryptographic Module Tested Configuration

Module	Hardware	Firmware Version	Distinguishing Features
Panorama M-200	910-000176 Physical Kit: 920-000208	10.1.5	RJ45 interfaces, USB ports (disabled), LEDs
Panorama M-500	910-000073 Physical Kit: 920-000145	10.1.5	RJ45 interfaces, USB ports (disabled), LEDs
Panorama M-600	910-000175 Physical Kit: 920-000209	10.1.5	RJ45 interfaces, USB ports (disabled), LEDs, SFP+ ports

Approved Mode of Operation

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

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

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

- Status output interface will indicate “**** FIPS-CC MODE ENABLED ****” via the CLI session.
- Status output interface will indicate “FIPS-CC mode enabled successfully” via the console port.
- The module will display “FIPS-CC” at all times in the status bar at the bottom of the web interface.
- The module will display “fips-cc” when “show system info” is entered via the CLI

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

- The module will output “FIPS-CC failure”
- The module will reboot and enter a state in which the reason for the reboot can be determined.

- To determine which self-test caused the system to reboot into the error state, connect the console cable and follow the on-screen instructions to view the self-test output.

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

Selecting Panorama, Management-Only, and PAN-DB System Modes

Panorama M-Series appliances support multiple configurations that provide varying services. The Cryptographic Officer can initialize the module into different system modes. The primary and default system mode is the Panorama mode. The Management-Only system mode is the same as Panorama mode except there is no log collecting service. The Log Collector system mode 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. The M-500 and M-600 provide a fourth system mode, PAN-DB Private Cloud server.

Convert the 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-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.

Selecting Panorama Log Collector System Mode

Convert the 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-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.

NOTE: Changing the System Mode does not change the FIPS-CC Mode.

Non-Compliant State

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

Zeroization

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

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

Approved and Allowed Algorithms

The following table details the cryptographic algorithms and their algorithm certificates. Only the algorithms, modes, and key sizes specified in this table are used by the module. The CAVP certificate may contain more tested options than listed in this table.

Table 3 - Approved Algorithms

CAVP Cert	Algorithm and Standard	Mode/Method	Description/Key Size(s)/Key Strength(s)	Use/Function
A2137	AES-CBC [SP 800-38A]	CBC	128, 192 and 256 bits	Encryption Decryption
A2137	AES-CFB128 [SP 800-38A]	CFB128	128 bits	Encryption Decryption
A2137	AES-CTR [SP 800-38A]	CTR	128, 192 and 256 bits	Encryption Decryption
A2137	AES-GCM [SP 800-38D]	GCM**	128 and 256 bits	Encryption Decryption
A2137	Counter DRBG [SP 800-90Arev1]	Counter DRBG	AES 256 bits with Derivation Function Enabled	Random Bit Generator

A2137	ECDSA KeyGen (FIPS 186-4)	ECDSA KeyGen	P-256, P-384, P-521	Key Generation
A2137	ECDSA KeyVer (FIPS 186-4)	ECDSA KeyVer	P-256, P-384, P-521	Public Key Validation
A2137	ECDSA SigGen (FIPS 186-4)	ECDSA SigGen	P-256, P-384, P-521 with SHA2-224, SHA2-256, SHA2-384, and SHA2-512	Signature Generation
A2137	ECDSA SigVer (FIPS 186-4)	ECDSA SigVer	P-256, P-384, P-521 with SHA-1, SHA2-224, SHA2-256, SHA2-384, and SHA2-512	Signature Verification
A2137	HMAC-SHA-1 [FIPS 198-1]	HMAC	HMAC-SHA-1 with λ=160	Authentication for protocols
A2137	HMAC-SHA2-224 [FIPS 198-1]	HMAC	HMAC-SHA2-224 with λ=224	Authentication for protocols
A2137	HMAC-SHA2-256 [FIPS 198-1]	HMAC	HMAC-SHA2-256 with λ=256	Authentication for protocols
A2137	HMAC-SHA2-384 [FIPS 198-1]	HMAC	HMAC-SHA2-384 with λ=384	Authentication for protocols
A2137	HMAC-SHA2-512 [FIPS 198-1]	HMAC	HMAC-SHA2-512 with λ=512	Authentication for protocols
A2137	KAS-ECC-SSC Sp800-56Ar3	KAS	Ephemeral Unified Model: P-256/P-384/P-521	Key Exchange
A2137	KAS-FFC-SSC SP 800-56Ar3	KAS	dhEphem: MODP-2048	Key Exchange
A2137	KDF SNMP [SP 800-135rev1] (CVL)	SNMPv3 KDF	Engine ID: 80001F8804303030303030343935323630	SNMPv3
A2137	KDF SSH [SP 800-135rev1] (CVL)	SSHv2 KDF	SHA-1, SHA2-256, SHA2-512	SSH
A2137	KDF TLS [SP 800-135rev1] (CVL)	TLS 1.0/1.1 KDF, TLS1.2 KDF	TLS v1.0/1.1 TLS v1.2 Hash Algorithm: SHA2-256, SHA2-384	TLS
A2137	RSA KeyGen (FIPS 186-4)	RSA KeyGen (FIPS 186-4)	2048, 3072, and 4096 bits	Key Pair Generation
A2137	RSA SigGen (FIPS 186-4)	RSA SigGen (FIPS 186-4)	(ANSI X9.31, RSASSA-PKCS1_v1-5, RSASSA-PSS): 2048, 3072, and 4096-bit with hashes SHA2-256/384/512	Signature Generation
A2137	RSA SigVer (FIPS 186-4)	RSA SigVer (FIPS 186-4)	(ANSI X9.31, RSASSA-PKCS1_v1-5, RSASSA-PSS): 2048, 3072, 4096-bit (per IG C.F) with hashes SHA-1 and SHA2-224+++/256/384/512 (Signature Verification) +++ This Hash algorithm is not supported for ANSI X9.31	Signature Verification
A2137	SHA-1 [FIPS 180-4]	SHA	SHA-1	Digital Signature Generation/Verification Non-Digital Signature Applications (e.g. component of HMAC)
A2137	SHA2-224 [FIPS 180-4]	SHA2	SHA-224	Digital Signature Generation/Verification Non-Digital Signature Applications (e.g. component of HMAC)
A2137	SHA2-256 [FIPS 180-4]	SHA2	SHA-256	Digital Signature Generation/Verification

				Non-Digital Signature Applications (e.g. component of HMAC)
A2137	SHA2-384 [FIPS 180-4]	SHA2	SHA-384	Digital Signature Generation/Verification Non-Digital Signature Applications (e.g. component of HMAC)
A2137	SHA2-512 [FIPS 180-4]	SHA2	SHA-512	Digital Signature Generation/Verification Non-Digital Signature Applications (e.g. component of HMAC)
A2137	Safe Primes Key Generation [RFC 3526]	Safe Primes Key Generation	MODP-2048	Safe Primes Key Generation
A2137	Safe Primes Key Verification [RFC 3526]	Safe Primes Key Verification	MODP-2048	Safe Primes Key Verification
A2165	Conditioning Component AES-CBC-MAC SP 800-90B	AES-CBC-MAC	128 bits	Intel Conditioner for Entropy Source
AES Cert. #A2137 and HMAC Cert. #A2137	KTS [SP 800-38F]	SP 800-38A, FIPS 198-1, and SP 800-38F. KTS (key wrapping and unwrapping) per IG D.G.	128, 192, and 256-bit keys providing 128, 192, or 256 bits of encryption strength	Key Wrapping. AES-CBC or AES-CTR with HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384, or HMAC-SHA2-512
AES-GCM Cert. #A2137	KTS [SP 800-38F]	SP 800-38D and SP 800-38F. KTS (key wrapping and unwrapping) per IG D.G.	128 and 256-bit keys providing 128 or 256 bits of encryption strength	Key Wrapping. AES-GCM.
ESV Cert. #E129	SP 800-90B	ESV	Palo Alto Networks DRNG RDSEED Entropy Source	Entropy
ESV Cert. #E130	SP 800-90B	ESV	Palo Alto Networks RTC Entropy Source	Entropy
KAS-ECC-SSC Cert. #A2137, KDF SSH Cert. #A2137	KAS [SP 800-56Arev3]	SP 800-56Arev3. KAS-ECC per IG D.F Scenario 2 path (2).	P-256, P-384, and P-521 curves providing 128, 192, or 256 bits of encryption strength	Key Exchange with protocol KDF
KAS-ECC-SSC Cert. #A2137, KDF TLS Cert. #A2137	KAS [SP 800-56Arev3]	SP 800-56Arev3. KAS-ECC per IG D.F Scenario 2 path (2).	P-256, P-384, and P-521 curves providing 128, 192, or 256 bits of encryption strength	Key Exchange with protocol KDF
KAS-FFC-SSC Cert. #A2137, KDF SSH Cert. #A2137	KAS [SP 800-56Arev3]	SP 800-56Arev3. KAS-FFC per IG D.F Scenario 2 path (2).	2048-bit key providing 112 bits of encryption strength	Key Exchange with protocol KDF
KAS-FFC-SSC Cert. #A2137, KDF TLS	KAS [SP 800-56Arev3]	SP 800-56Arev3. KAS-FFC per IG D.F Scenario 2 path (2).	2048-bit key providing 112 bits of encryption strength	Key Exchange with protocol KDF

Cert. #A2137				
Vendor Affirmed	CKG (SP 800-133rev2)	Section 5.1, Section 5.2	Cryptographic Key Generation; SP 800-133 and IG D.I.	Key Generation Note:The seeds used for asymmetric key pair generation are produced using the unmodified/direct output of the DRBG

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

- For TLS, The GCM implementation meets Scenario 1 of IG C.H: it is used in a manner compliant with SP 800-52 and in accordance with Section 4 of RFC 5288 for TLS key establishment, and ensures when the nonce_explicit part of the IV exhausts all possible values for a given session key, that a new TLS handshake is initiated per sections 7.4.1.1 and 7.4.1.2 of RFC 5246. During operational testing, the module was tested against an independent version of TLS and found to behave correctly.
    - From this RFC 5288, the GCM cipher suites in use are
      TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
      TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
      TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, and
      TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

- For SSH, the module meets Scenario 1 of IG C.H. The module conforms to RFCs 4252, 4253, and 5647. The fixed field is 4-byte 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 8-byte 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, which can take hundreds of years. (In FIPS-CC Mode, SSH rekey is automatically configured at 1 GB of data or 1 hour, whichever comes first.)

In all 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 key is established.

The module is compliant to IG C.F:

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

The module does not have any algorithms that fall under:

- Non-Approved Algorithms Allowed in the Approved Mode of Operation
- Non-Approved Algorithms Not Allowed in the Approved Mode of Operation

The following table documents the module's algorithms that are non-approved and not allowed for use in the approved mode of operation.

Table 4A - Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed

Algorithm	Caveat	Use / Function
MD5	Only allowed as the PRF in TLSv1.1 per IG 2.4.AOnly allowed as the PRF in TLSv1.0 and v1.1 per IG 2.4.A	Message digest used in TLSv1.0 / v1.1 KDF only

Table 5 - Supported Protocols in the Approved Mode

Supported Protocol
TLSv1.1, v1.2
SSHv2
SNMPv3

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

Module Diagrams

Figures 1 - 6 depict the modules and their interfaces. The cryptographic boundary includes the physical perimeter of the enclosure of the appliance with the physical kit installed and all logical components within. Please refer to the appendices for depictions of the modules with the physical kits installed.

Figure 1 - M-200 Front

Figure 2 - M-200 Rear

Figure 3 - M-500 Front

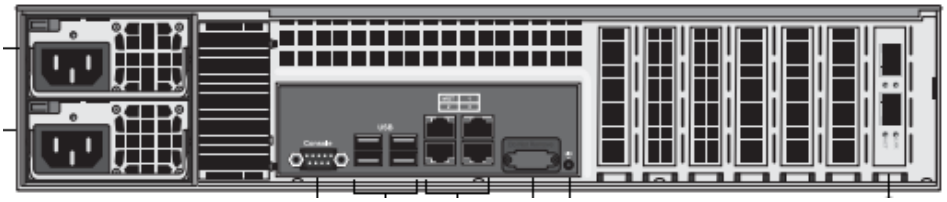

Figure 4 - M-500 Rear

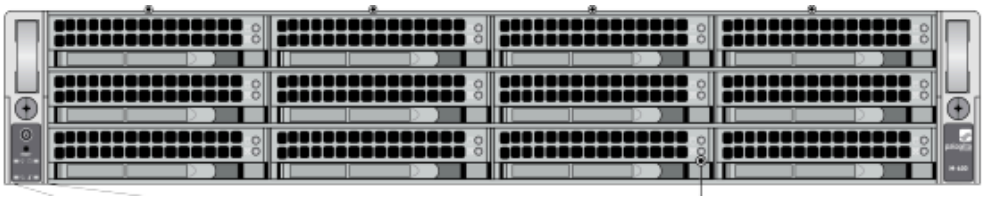

Figure 5 - M-600 Front

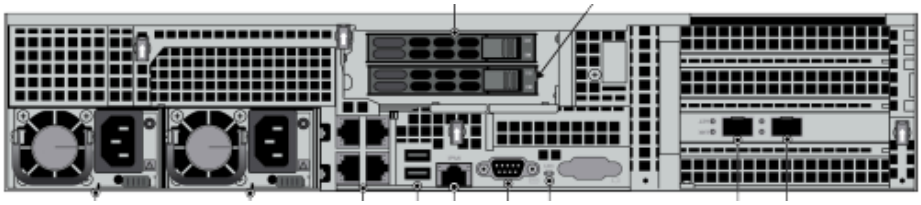

Figure 6 - M-600 Rear

3. Cryptographic Module Interfaces

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

Table 6 - Ports and Interfaces

Physical Interface	Logical Interface	Data that passes over port/interface
LED	Status output	Module status via LED indicators
Power	Power	N/A
RJ45 Console	Status output	Self-test output
RJ45 Ethernet	Data input, control input, control output, data output, status output	TLS, SSH
SFP+ *(M-600)*	Data input, control input, data output, status output	TLS

4. Roles, Services, and Authentication

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 (CO) role.

The module supports concurrent operators.

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

Table 7 – Roles, Service Commands, Input and Output

Role	Service	Input	Output
CO	Show Version	Query module for version	Module provides version
CO	System Provisioning	Configuring and managing system configurations (e.g., IP address, system time, etc.) via CLI or WebUI	Confirmation of service via Configuration Logs
CO, User	Access web portal	Connect to web portal from TLS client.	Confirmation of service via Configuration Logs
CO, User	Access CLI	Connect to SSH server from SSH client	Confirmation of service via Configuration Logs
CO	Panorama Firmware Update	Loading new image	Message output noting version updated successfully via System Logs
CO	Panorama Manager Setup	Configuring and managing Manager configurations (e.g., HTTPS, NTP, etc.) via CLI or WebUI	Confirmation of service via Configuration Logs
CO	Manage Panorama Administrative Access	Configuring and managing Administrative configurations (e.g., creating user accounts, setting authentication method, etc.) via CLI or WebUI	Confirmation of service via Configuration Logs
CO	Configure High Availability	Configuring and managing High Availability (HA) configuration via CLI or WebUI	Confirmation of service via Configuration Logs
CO	Panorama Certificate Management	Configuring and managing certificates via CLI or WebUI	Confirmation of service via Configuration Logs
CO	Panorama Log Setting	Configuring and managing log settings via CLI or WebUI	Confirmation of service via Configuration Logs
CO	Panorama Server Profiles	Configuring and managing Server configurations (e.g. SNMP, etc.) via CLI or WebUI	Confirmation of service via Configuration Logs
CO	Setup Managed Devices and Deployment	Configuring and managing Managed Devices configurations (e.g., Versions, Licenses, etc.) via CLI or WebUI	Confirmation of service via Configuration Logs
CO	Configure Managed Log Collectors	Configuring and managing Managed Log Collectors configurations via CLI or WebUI	Confirmation of service via Configuration Logs

CO, Unauthenticated	Zeroize	Zeroize from CLI	Zeroization Indicator
CO, User, Unauthenticated	Self-Test	Run self-test via CLI or WebUI	Output results via System Logs
CO, User	Show Status	Show status via CLI or WebUI	FIPS-CC Mode Indicator
CO, User	System Audit	View system audit records via CLI or WebUI	Audit records via System Logs
CO, User	Monitor System Status and Logs	View system status records via CLI or WebUI	System status via System Logs
CO	Panorama Log Collector Setup	Configuring and managing Log Collectors configurations via CLI	Confirmation of service via Configuration Logs
CO	Panorama Pan-DB Setup	Configuring and managing Pan-DB URL configurations via CLI	Confirmation of service via Configuration Logs
CO	Manage Pan-DB Administrative Access	Configuring and managing Administrator password via CLI	Confirmation of service via Configuration Logs

Table 10 - Roles and Authentication

Role	Authentication Method	Authentication Strength
CO	Memorized Secret (Unique Username/password) and/or Single-Factor Cryptographic Software (certificate common name / public key-based authentication)	Password-based Minimum length is eight[1] (8) characters (95 possible characters). The probability that a random attempt will succeed or a false acceptance will occur is $1/(95^8)$ which is less than 1/1,000,000. The probability of successfully authenticating to the module within one minute is $10/(95^8)$, which is less than 1/100,000. The module's configuration supports at most ten failed attempts to authenticate in a one-minute period. Certificate/Public key-based The security modules support public-key based authentication using RSA 2048 and certificate-based authentication using RSA 2048, RSA 3072, RSA 4096, ECDSA P-256, P-384, or 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 $10/(2^{112})$, which is less than 1/100,000. The module in FIPS-CC mode allows at most 10 failed attempts before a lockout occurs.
User	Memorized Secret (Unique Username/password) and/or Single-Factor Cryptographic Software (certificate common name / public key-based authentication)	

[1] In FIPS-CC Mode, the module checks and enforces the minimum password length of eight (8) as specified in SP 800-63B. Passwords are securely stored hashed with salt value, with very restricted access control, and rate limiting mechanism for authentication attempts.

Access Control Policy

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.

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://docs.paloaltonetworks.com/.

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.

SSP Access Rights

The table below defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as:

G = Generate: The module generates or derives the SSP.

R = Read: The SSP is read from the module (e.g. the SSP is output).

W = Write: The SSP is updated, imported, or written to the module.

E = Execute: The module uses the SSP in performing a cryptographic operation.

Z = Zeroise: The module zeroises the SSP.

Table 11 - Approved Services

Service	Description	Approved Security Functions		Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
Show Version	Query the module to display the version	N/A		N/A	CO	N/A	Version displayed via System Logs / CLI / UI
System Provisioning	Perform panorama licensing, diagnostics, debug functions, manage Panorama support information and switch between Panorama Management-only, and Logger modes. (Panorama or Management-Only Mode)	N/A		N/A	CO	N/A	System and Configuration logs
Access web portal	Connect to module's web portal to invoke services. (Panorama or Management-Only Mode)	RSA SigVer (186-4)		CA Certificates	CO, User	G/R/E/W	System Logs
		RSA SigVer (186-4)		RSA Public Keys		G/R/E/W	
		ECDSA SigVer (186-4)		ECDSA Public Keys		G/R/E/W	
		KAS	KDF TLS (CVL), MD5	TLS Pre-Master Secret		G/E/Z	
			KDF TLS (CVL), MD5	TLS Master Secret		G/E/Z	

			CKG, ECDSA KeyGen (FIPS 186-4), ECDSA KeyVer (FIPS 186-4), KAS-ECC-SSC, KAS-FFC-SSC, Safe Primes Key Generation, Safe Primes Key Verification	TLS DHE/ECDHE Private Components		G/E/Z	
				TLS DHE/ECDHE Public Components		G/E/Z	
		KTS	HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-384	TLS HMAC Keys		G/E/Z	
			AES-CBC	TLS Encryption Keys		G/E/Z	
		KTS	AES-GCM	TLS Encryption Keys		G/E/Z	
		Counter DRBG, ESV		DRBG Seed	CO	G/E	System Logs
				DRBG V			
				DRBG Key			
				Entropy Input String			
Access CLI	Connect to module's CLI via SSH	KTS	HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-512	SSH Session Authentication Keys	CO, User	G/E/Z	System Logs
			AES-CBC AES-CTR	SSH Session Encryption Keys		G/E/Z	
		KTS	AES-GCM			G/E/Z	
		KAS	KDF SSH (CVL)	SSH DHE/ECDHE Private Components		G/E/Z	
			KAS-ECC-SSC KAS-FFC-SSC Safe Primes Key Generation Safe Primes Key Verification	SSH DHE/ECDHE Public Components		G/E/R/W/Z	
		Counter DRBG, ESV		DRBG Seed	CO	G/E	System Logs
				DRBG V			
				DRBG Key			
				Entropy Input String			
Panorama Firmware Update	Download and install firmware updates	RSA SigVer (FIPS 186-4)		Public Key for Firmware Load Test	CO	W/E	System and Configuration logs
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 role (Panorama or Management-Only Mode)	CKG RSA KeyGen (FIPS 186-4) RSA SigGen (FIPS 186-4)		RSA Private Keys	CO	G/W/E	System and Configuration logs
		CKG ECDSA KeyGen (FIPS 186-4) ECDSA SigGen (FIPS 186-4)		ECDSA Private Keys		G/W/E	
		RSA SigVer (FIPS 186-4)		RSA Public Keys		G/R/E/W	
		ECDSA SigVer (FIPS 186-4)		ECDSA Public Keys		G/R/E/W	
		KDF SNMP (CVL)		SNMPv3 Authentication Secret		W/E	
		KDF SNMP (CVL)		SNMPv3 Privacy Secret		W/E	
		HMAC-SHA-1 HMAC-SHA2-224 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512		SNMPv3 Authentication Key		G/E/Z	
		AES-CFB128		SNMPv3 Session Key		G/E/Z	

		RSA SigVer (FIPS 186-4) ECDSA SigVer (FIPS 186-4)		CA Certificates		G/R/E/W	
		KAS	KDF TLS (CVL), MD5	TLS Pre-Master Secret		G/E/Z	
			KDF TLS (CVL), MD5	TLS Master Secret		G/E/Z	
			CKG, ECDSA KeyGen (FIPS 186-4), ECDSA KeyVer (FIPS 186-4), KAS-ECC-SSC, KAS-FFC-SSC, Safe Primes Key Generation, Safe Primes Key Verification	TLS DHE/ECDHE Private Components		G/E/Z	
				TLS DHE/ECDHE Public Components		G/E/R/W/Z	
		KTS	HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-384	TLS HMAC Keys		G/E/Z	
			AES-CBC	TLS Encryption Keys		G/E/Z	
		KTS	AES-GCM	TLS Encryption Keys		G/E/Z	
		KTS	HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-512	SSH Session Authentication Keys		G/E/Z	
			AES-CBC, AES-CTR	SSH Session Encryption Keys		G/E/Z	
		KTS	AES-GCM				
		KAS	KDF SSH KAS-ECC-SSC KAS-FFC-SSC Safe Primes Key Generation, Safe Primes Key Verification	SSH DHE/ECDHE Private Components		G/E/Z	
				SSH DHE/ECDHE Public Components		G/E/R/W/Z	
		Counter DRBG, ESV		DRBG Seed	CO	G/E	System Logs
				DRBG V			
				DRBG Key			
				Entropy Input String			
Manage Panorama Administrative Access	Define access control methods via admin profiles, configure administrators and password profiles Configure local user database, authentication profiles, sequence of methods and access domains.	N/A		CO, User Password	CO	G/E/W	System and Configuration logs

	(Panorama, Management-Only, or Log Collector Mode)	RSA SigVer (FIPS 186-4)	SSH Client Public Key		W/E	
		RSA SigVer (FIPS 186-4) ECDSA SigVer (FIPS 186-4)	SSH Host Public Key		G/R/E/W	
Configure High Availability	Configure High Availability communication settings (Panorama or Management-Only Mode)	RSA SigVer (FIPS 186-4)	RSA Public Key	CO	G/R/E/W	Configuration Logs
		ECDSA SigVer (FIPS 186-4)	ECDSA Public Key		G/R/E/W	
Panorama Certificate Management	Manage RSA/ECDSA certificates and private keys, certificate profiles, revocation status, and usage; show status. (Panorama, Management-Only, or Log Collector Mode)	ECDSA SigGen (FIPS 186-4) RSA SigGen (FIPS 186-4)	RSA Private Keys ECDSA Private Keys	CO	G/R/W/E	System and Configuration logs
		ECDSA SigVer (FIPS 186-4) RSA SigVer (FIPS 186-4)	RSA Public Keys ECDSA Public Keys		G/R/W/E	
		Counter DRBG, ESV	DRBG Seed		G/E	
			DRBG V			
			DRBG Key			
			Entropy Input String			
Panorama Log Setting	Configure log forwarding (Panorama or Management-Only Mode)	N/A	N/A	CO	N/A	Configuration Logs
Panorama Server Profiles	Configure communication parameters and information for peer servers (Panorama or Management-Only Mode)	KDF SNMP (CVL)	SNMPv3 Authentication Secret	CO	W/E	System Logs
		KDF SNMP (CVL)	SNMPv3 Privacy Secret		W/E	
		HMAC-SHA-1 HMAC-SHA2-224 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512	SNMPv3 Authentication Key		G/E/Z	
		AES-CFB128	SNMPv3 Session Key		G/E/Z	
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 firmware versions and schedule updates on the managed	N/A	N/A	CO	N/A	Configuration Logs

	firewalls and managed log collectors. (Panorama or Management-Only Mode)					
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 firmware versions and schedule updates on managed log collectors. (Panorama or Management-Only Mode)	N/A	CO, User Password	CO	G/E/W	System and Configuration logs
Zeroize	Zeroize all SSPs	N/A	All SSPs	CO, Unauthenticated	Z	Zeroization Indicator
Self-Test	Run power up self-tests on demand by power cycling the module.	N/A	Firmware Integrity Verification Key	CO, User, Unauthenticated	E	System Logs
Show Status	View status of the module	N/A	N/A	CO, User	N/A	FIPS-CC Mode Indicator
System Audit	Allows review of limited configuration and system status via SNMPv3, logs, dashboard, show status, and configuration screens. CO Only: Provides configuration commit capability. (Panorama, Management-Only, or PAN-DB Mode)	N/A	N/A	CO, User	N/A	System Logs
Monitor System Status and Logs	Review system status via the panorama system CLI, dashboard and logs; show status. (Panorama or Management-Only Mode)	N/A	N/A	CO, User	N/A	System Logs
Panorama Log Collector Setup	Presents configuration options for management interfaces and communication for peer services Import, Export, Save, Load, revert and validate Panorama configurations and state. (Log Collector Mode only)	CKG RSA KeyGen (FIPS 186-4) RSA SigGen (FIPS 186-4)	RSA Private Keys	CO	G/W/E	System and Configuration logs
		CKG ECDSA KeyGen (FIPS 186-4) ECDSA SigGen (FIPS 186-4)	ECDSA Private Keys		G/W/E	

		RSA SigVer (FIPS 186-4)		RSA Public Keys		G/R/E/W	
		ECDSA SigVer (FIPS 186-4)		ECDSA Public Keys		G/R/E/W	
		KAS	KDF TLS (CVL), MD5	TLS Pre-Master Secret		G/E/Z	
			KDF TLS (CVL), MD5	TLS Master Secret		G/E/Z	
			CKG, ECDSA KeyGen (FIPS 186-4), ECDSA KeyVer (FIPS 186-4), KAS-ECC-SSC, KAS-FFC-SSC, Safe Primes Key Generation, Safe Primes Key Verification	TLS DHE/ECDHE Private Components		G/E/Z	
				TLS DHE/ECDHE Public Components		G/E/R/W/Z	
		KTS	HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-384	TLS HMAC Keys		G/E/Z	
			AES-CBC	TLS Encryption Keys		G/E/Z	
		KTS	AES-GCM	TLS Encryption Keys		G/E/Z	
		KTS	HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-512	SSH Session Authentication Keys		G/E/Z	
			AES-CBC, AES-CTR	SSH Session Encryption Keys		G/E/Z	
		KTS	AES-GCM				

		KAS	KDF SSH (CVL)	SSH DHE/ECDHE Private Components		G/E/Z	
			KAS-ECC-SSC KAS-FFC-SSC Safe Primes Key Generation, Safe Primes Key Verification				
		Counter DRBG, ESV		DRBG Seed		G/E	
				DRBG V			
				DRBG Key			
				Entropy Input String			
Panorama Pan-DB Setup	Presents configuration options for management interfaces and communication for peer services Import, Export, Save, Load, revert and validate Panorama configurations and state. (PAN-DB Mode only)	KAS	KDF TLS (CVL), MD5	TLS Pre-Master Secret	CO	G/E/Z	System Logs
			KDF TLS (CVL), MD5	TLS Master Secret		G/E/Z	
			CKG, ECDSA KeyGen (FIPS 186-4), ECDSA KeyVer (FIPS 186-4), KAS-ECC-SSC, KAS-FFC-SSC, Safe Primes Key Generation, Safe Primes Key Verification	TLS DHE/ECDHE Private Components		G/E/Z	
				TLS DHE/ECDHE Public Components		G/E/R/W/Z	
		KTS	HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-384	TLS HMAC Keys		G/E/Z	
			AES-CBC	TLS Encryption Keys		G/E/Z	
		KTS	AES-GCM	TLS Encryption Keys		G/E/Z	
		KTS	HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-512	SSH Session Authentication Keys		G/E/Z	

			AES-CBC, AES-CTR	SSH Session Encryption Keys		G/E/Z	
		KTS	AES-GCM				
		KAS	KDF SSH (CVL)	SSH DHE/ECDHE Private Components		G/E/Z	
			KAS-ECC-SSC KAS-FFC-SSC Safe Primes Key Generation, Safe Primes Key Verification				
		Counter DRBG, ESV		DRBG Seed		G/E	
				DRBG V			
				DRBG Key			
				Entropy Input String			
Manage Pan-DB Administrative Access	Update Administrator password. (PAN-DB Mode only)	N/A		CO, User Password	CO	G/E/W	System and Configuration logs

Note: Configuration/System Logs for Approved services above will indicate FIPS-CC mode is enabled and that the service succeeded.

5. Software/Firmware Security

The module performs the Firmware Integrity test by using HMAC-SHA-256 and ECDSA signature verification (HMAC and ECDSA Cert. #A2137) during the Pre-Operational Self-Test. In addition, the module also conducts the firmware load test by using RSA 2048 with SHA-256 (Cert. #A2137) for the new validated firmware to be uploaded into the module via the Panorama Firmware Update service. The Firmware Integrity Verification key and Public key for Firmware Load Test used for the Firmware Integrity and Firmware Load test, respectively, are generated externally and delivered as part of the module firmware image.

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

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

6. Operational Environment

The FIPS 140-3 Area 5 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 140-3 CMVP. Any other firmware loaded into this module is out of the scope of this validation and requires a separate FIPS 140-3 validation.

7. Physical Security

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 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 physical kit part numbers and versions. Opacity shields are included in the physical kits.

Operator Required Actions

The following table provides information regarding the various physical security mechanisms, and their recommended frequency of inspection/test.

Table 14 - Physical Security Inspection Guidelines

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

Front and Rear Opacity Shields	30 days	(M-500, M-600) Verify that the front and rear opacity shields have not been deformed from their original shape, thereby reducing their effectiveness.
Vent Overlays	30 days	(M-500, M-600) Verify that the vent overlays have not been removed or deformed. All edges should maintain strong adhesion characteristics.

Refer to the following sections for instructions on installation and placement of the tamper seals and opacity shields.

M-200 Tamper Seal Installation (15 Seals)

1. Replace the top cover with the physical top cover.
   a. Remove the VOID WARRANTY label and cover screws (replacement label included in the kit).

      M-200 appliance—Remove the Void Warranty label that covers the left top cover screw then use a Phillips-head screwdriver to remove both screws as indicated in the illustration.

   b. Simultaneously depress the two (2) release buttons on top of the cover and slide the cover toward the back of the appliance to remove it.
   c. Slide the top cover (does not have vents) on the appliance until the release buttons click. Reinsert and slide cover into position and secure with the two (2) screws.

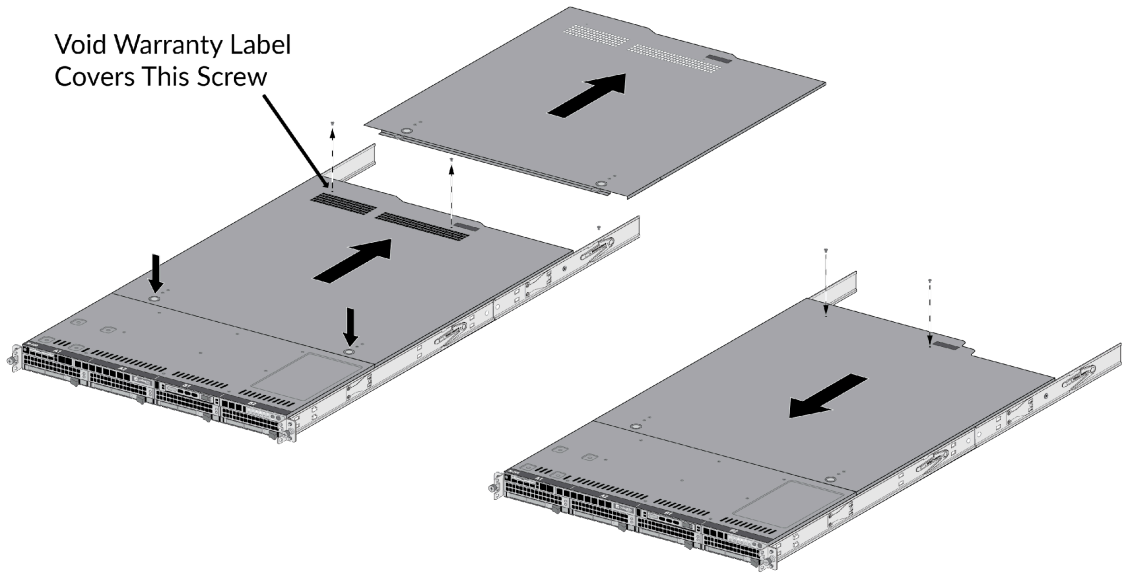

Figure 7 – M-200: Top Cover Replacement

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

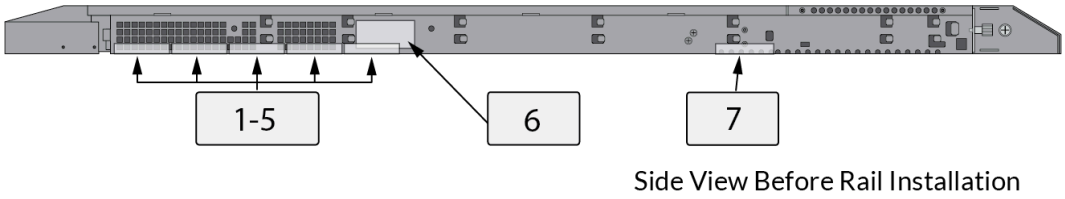

Figure 8 – M-200: Side View Before Rail Installation

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.

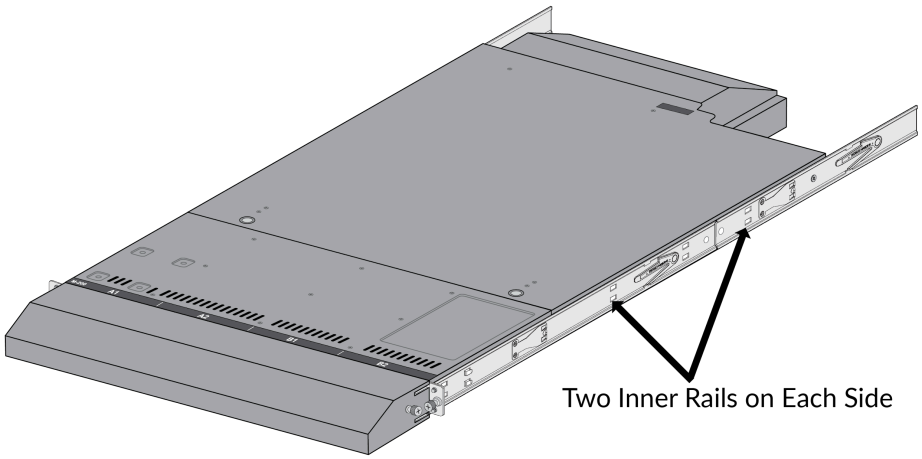

Figure 9 – M-200: Inner Rack Mount Rail Brackets

3. Attach the front cover brackets.

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

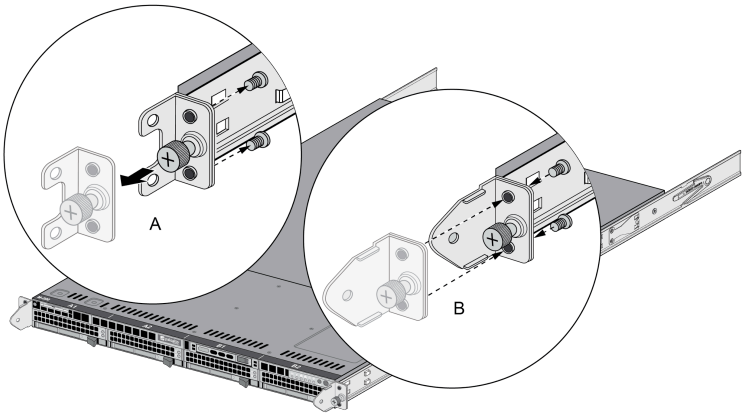

Figure 10 – M-200: Replacing Front Rack-Mount Brackets

4. Attach the physical kit front cover to the front of the appliance.

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

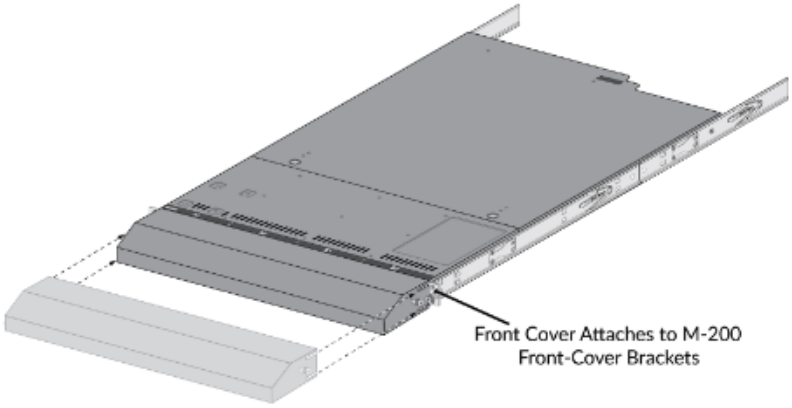

Figure 11 – M-200: Attach Physical Kit Front Cover

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

   Slide the back cover onto the back of the appliance, insert two M4 x 0.7 x 8mm (one (1) screw on each side), and turn the screws clockwise to secure the cover.

6. Apply a tamper-evident seal to each location shown in the following M-200 illustrations. Ensure you apply two (2) tamper-evident seals on the power supplies (see seals #14 and #15 on the rear illustration).

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

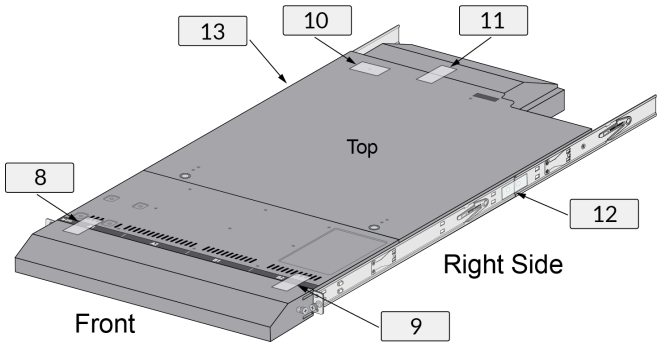

Figure 12 – M-200: Seal locations on Top and Right Side

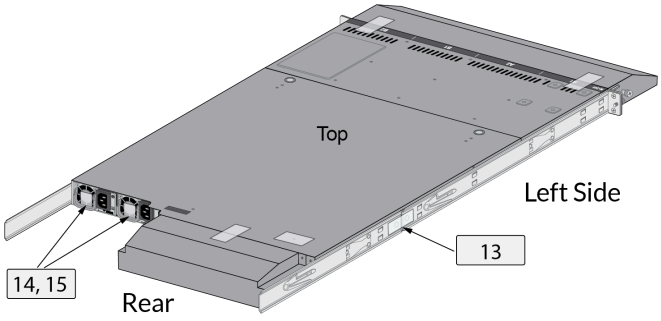

Figure 13 – M-200: Seal Locations on Left Side and Rear

M-500 Tamper Seal Installation (15 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.

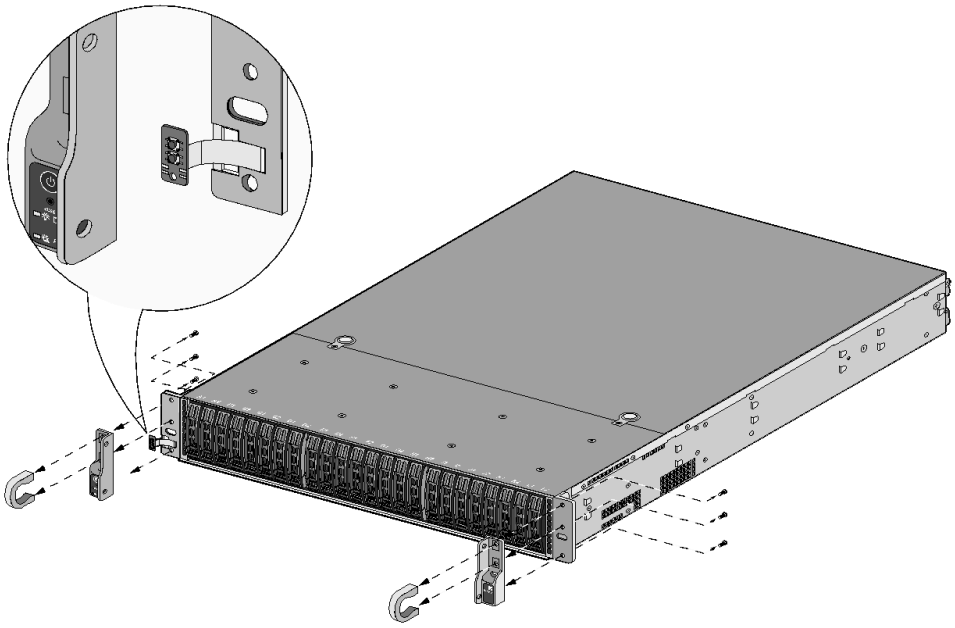

Figure 14 – M-500: Remove Front Handles and Modules

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 15, 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 16.

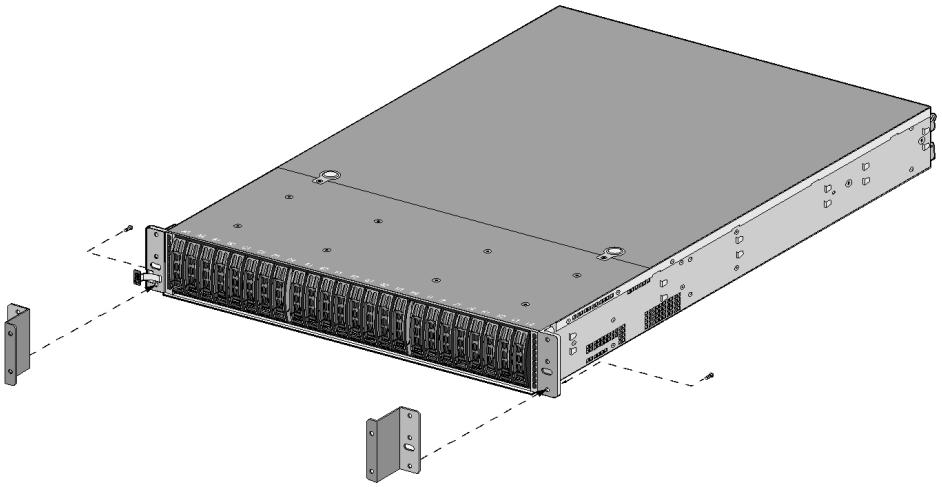

Figure 15 – M-500: Secure the Front Brackets

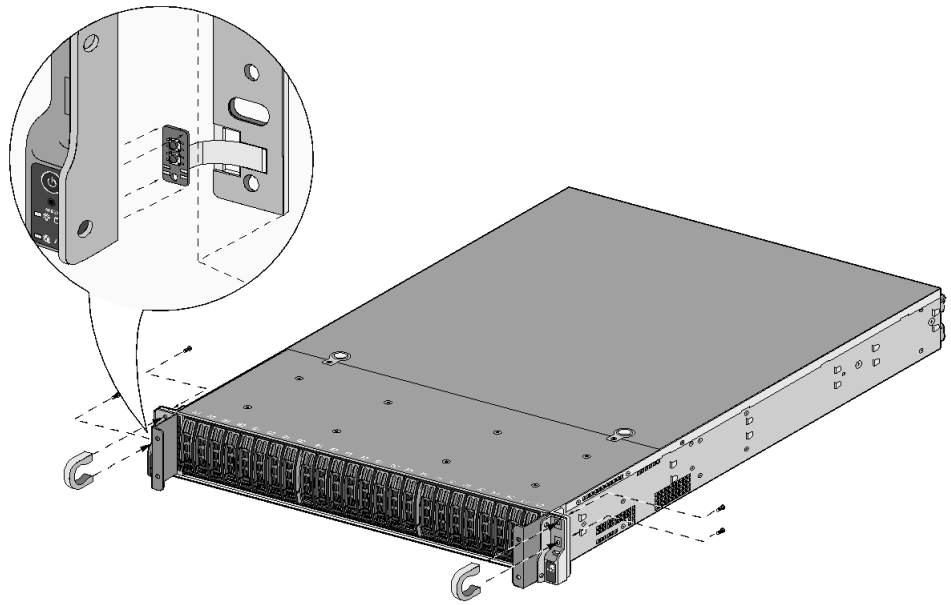

Figure 16 – M-500: Attach Pull Handles and Front Modules

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.

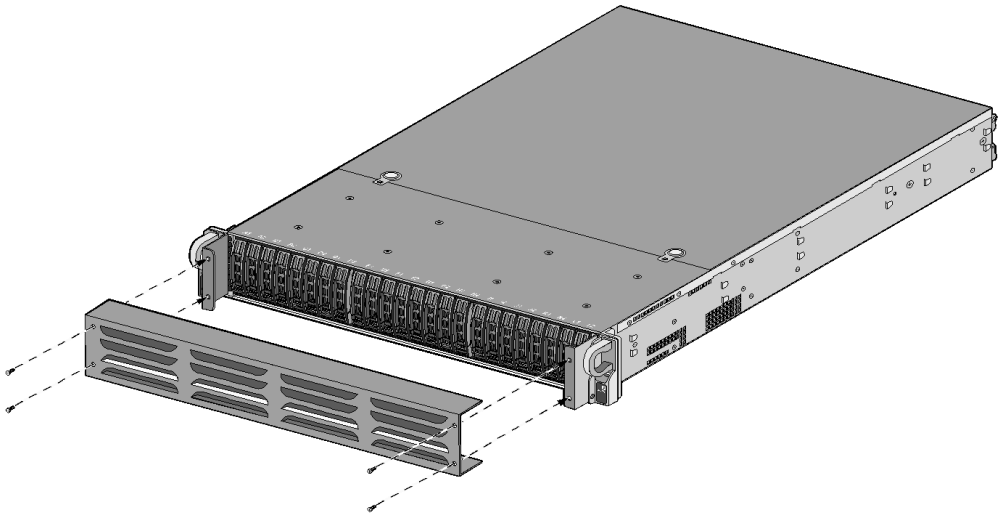

Figure 17 – M-500: Install Front Opacity Shield

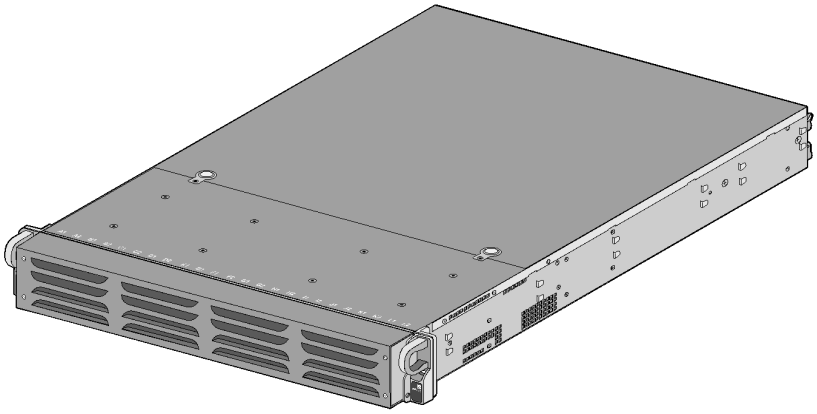

Figure 18 – M-500: Front Opacity Shield Installed

Step 4:
Attach the rear opacity shield tray to the appliance. First, remove the two (2) screws (shown in Figure 19) 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.

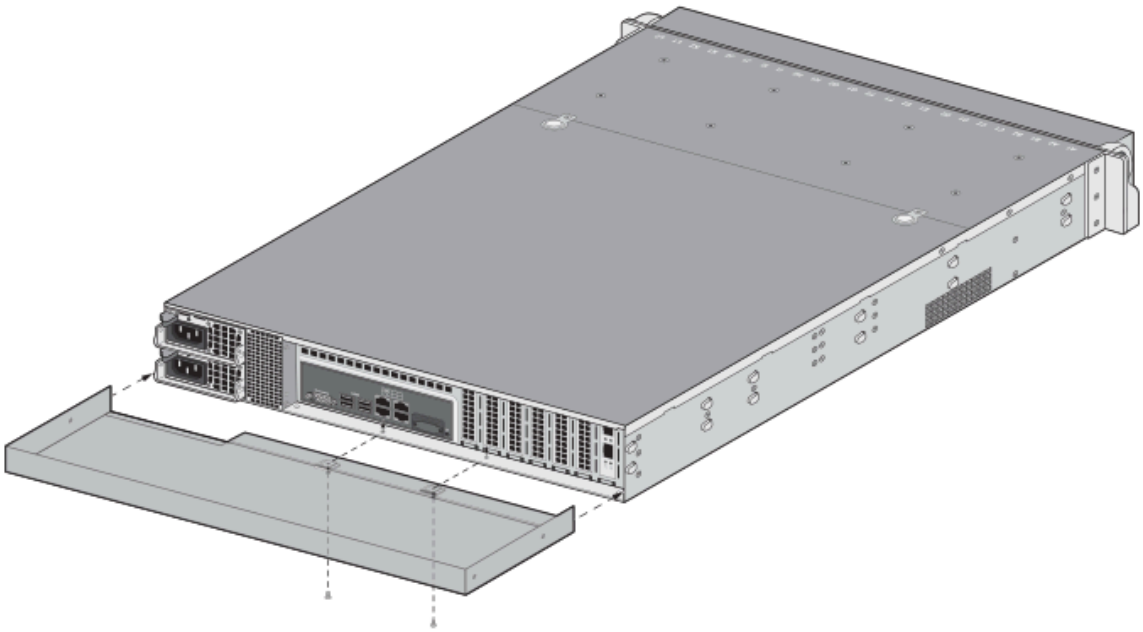

Figure 19 – M-500: Install Rear Opacity Shield Tray

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.

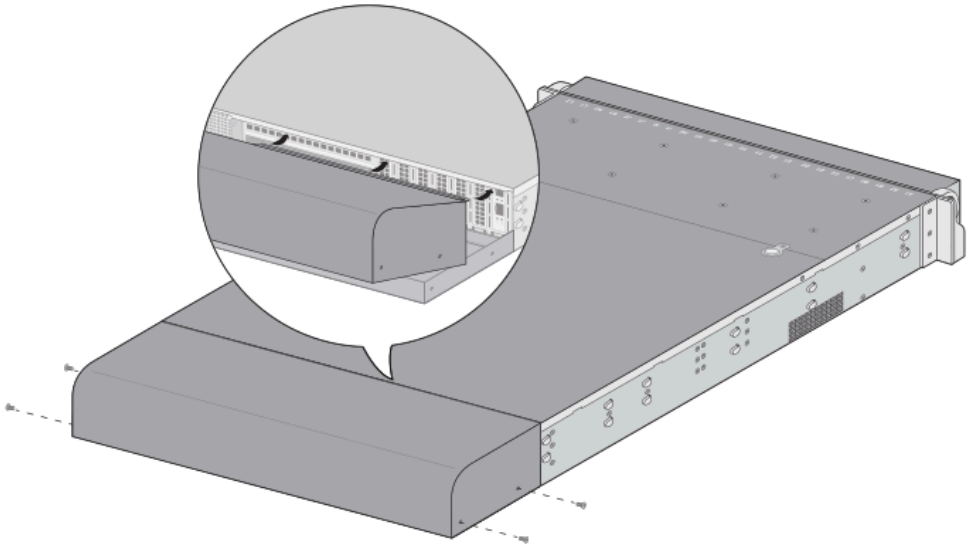

Figure 20 – M-500: Install Rear Opacity Shield

Step 6:

Cover the vent openings as shown in Figure 21 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 22 (B) #5.

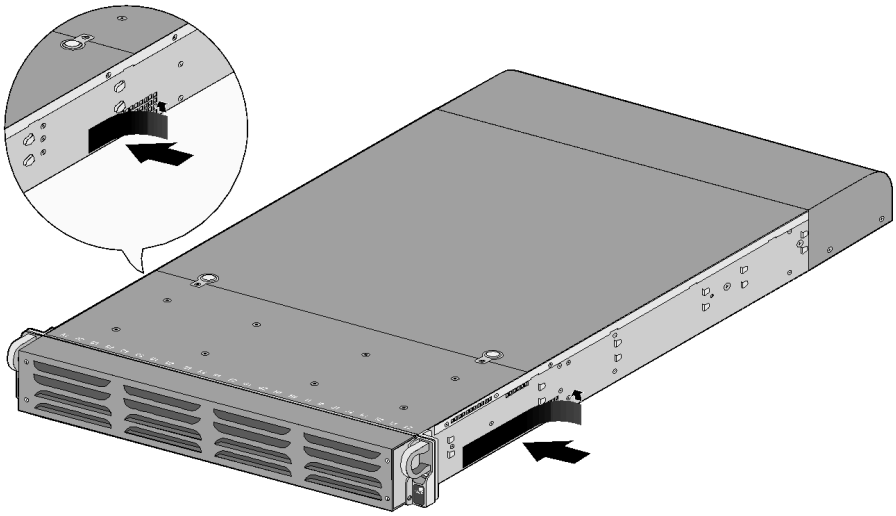

Figure 21 – M-500: Apply Vent Overlays

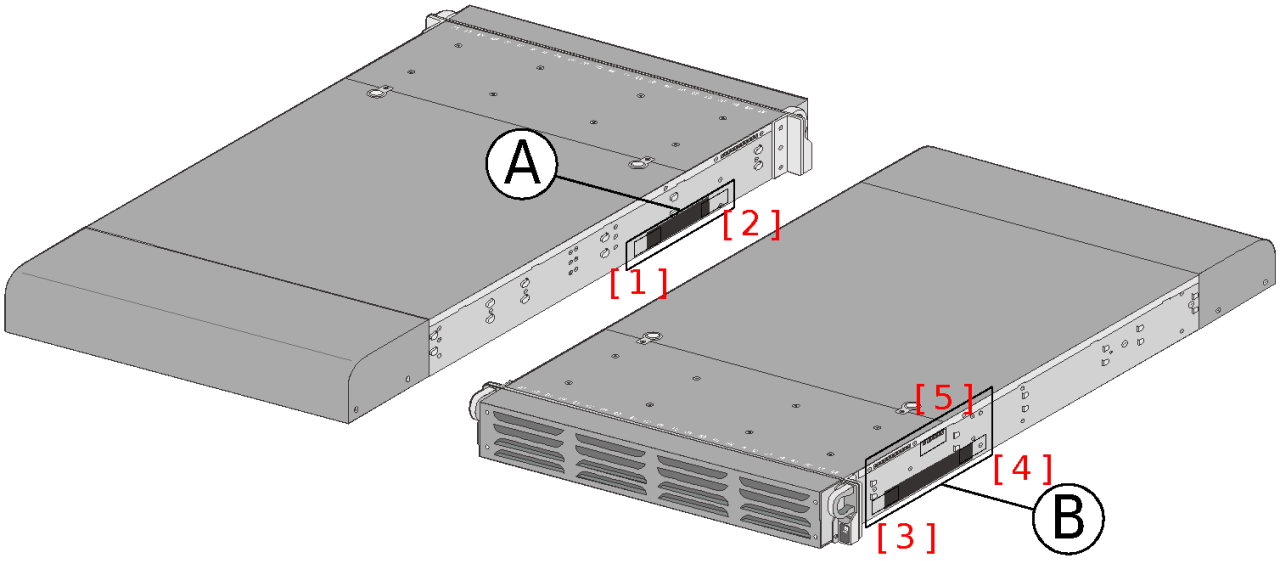

Figure 22 – M-500: Apply Tamper Seals on Vent Overlays and Side Opening

Step 7: Re-attach the rail kit to the appliance as shown in Figure 23 and then add three (3) tamper seals to the bottom of the appliance as shown in Figure 24. 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.

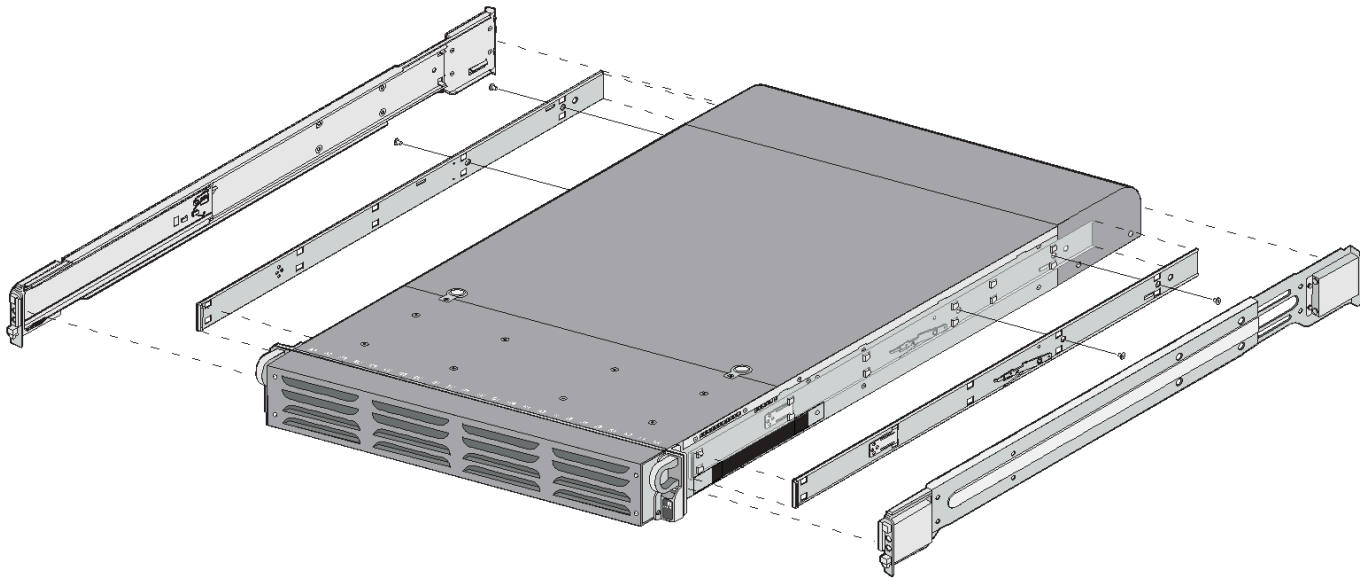

Figure 23 – M-500: Install Rail Kit

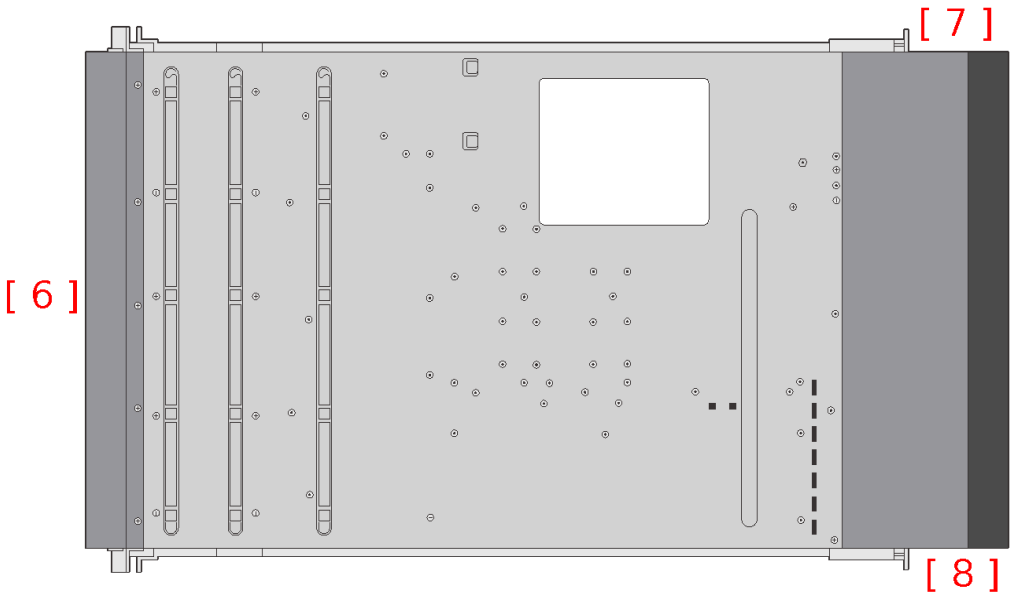

Figure 24 – M-500: Apply Tamper Seals on the Bottom of the Appliance

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.

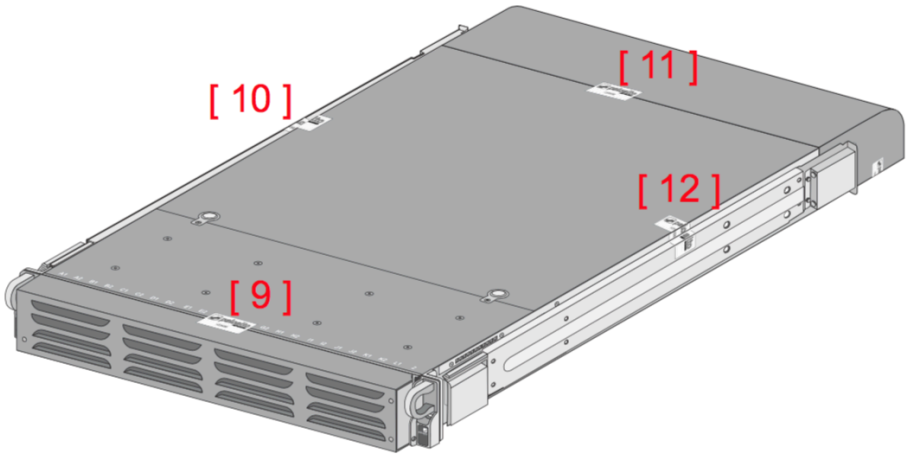

Figure 25 – M-500: Apply Tamper Seals on the Top and Sides of the Appliance

M-600 Tamper Seal Installation (21 Seals)

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

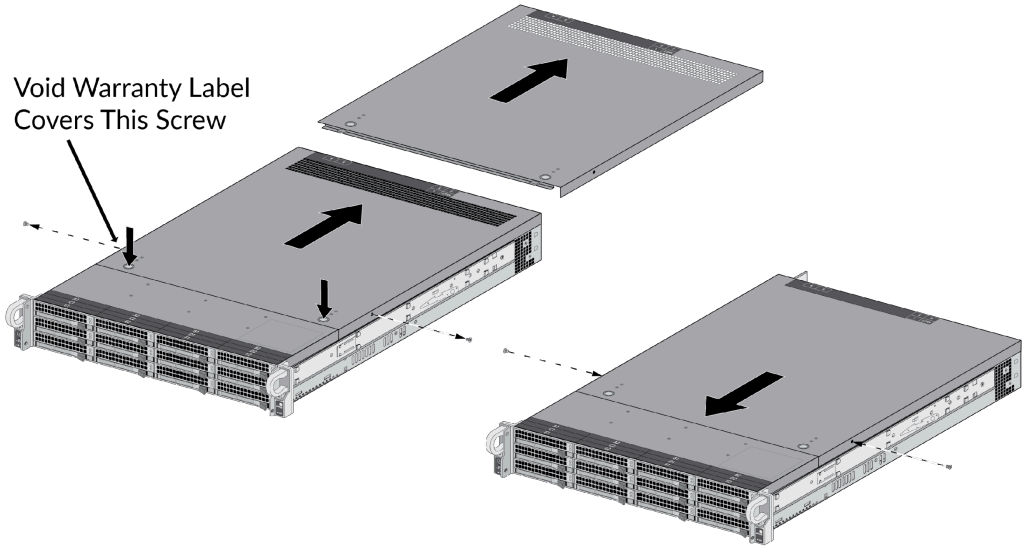

Figure 26 – M-600: Top Cover Replacement

2. Attach the physical front cover brackets.

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

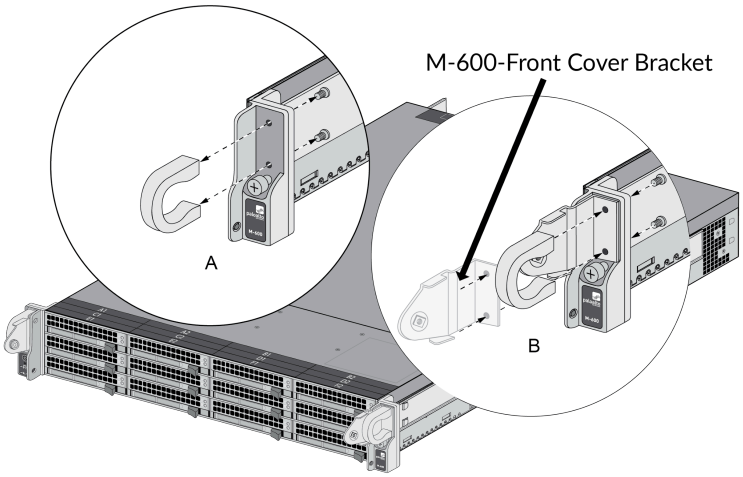

Figure 27 – M-600: Front Cover Bracket

3. Attach the physical kit front cover to the front of the appliance.

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

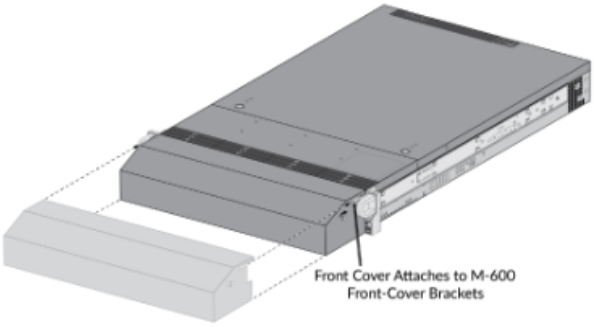

Figure 28 – M-600: Physical Kit Front Cover

4. Install a tamper-evident seal on the back of the appliance. This is seal #13 in the M-600 Figure 29. You need to install this seal before you install the M-600 physical kit back cover.
5. Attach the physical kit back cover to the back of the appliance.
    a. Slide the back cover onto the back of the appliance and turn the two (2) thumb screws clockwise until tight (one (1) screw on each side) to secure the cover.
6. Apply a tamper-evident seal to each location shown in the following M-600 illustrations below.
   Also install the overlay stickers to cover vent openings (two (2) stickers on each side). You then install tamper-evident seals over the overlay stickers. Apply two (2) tamper-evident seals on the back side of the right rack handle (see seals #18 and #19 on the left side in Figure 29). Apply two (2) tamper-evident seals on the power supplies (see seals #11 and #12 with rear inset of Figure 29).

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

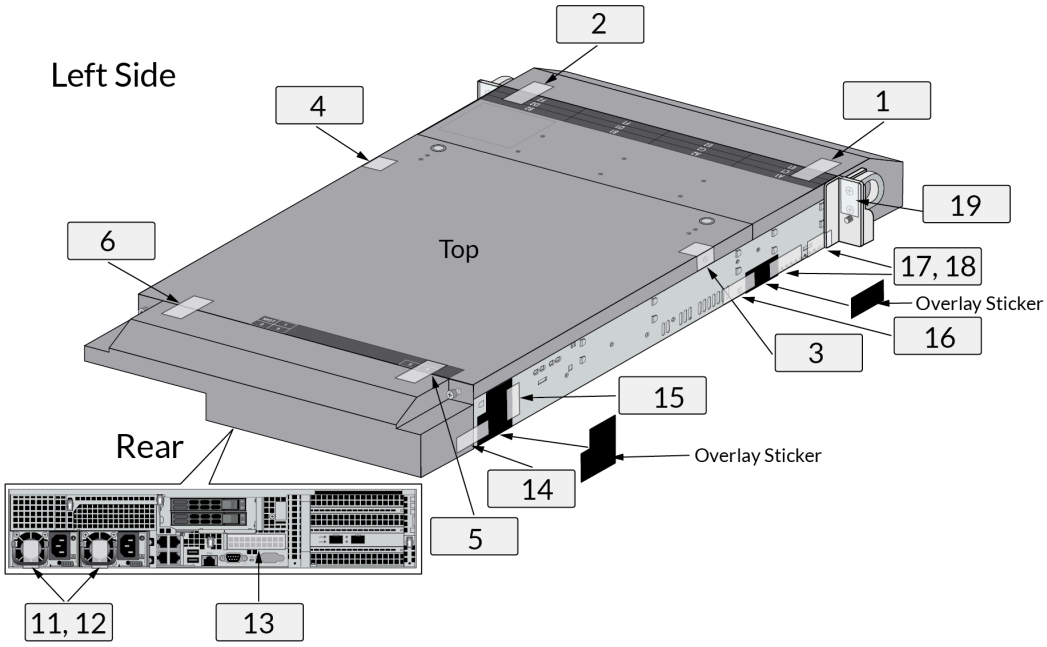

Figure 29 – M-600: Tamper Seal Locations (Top and Rear)

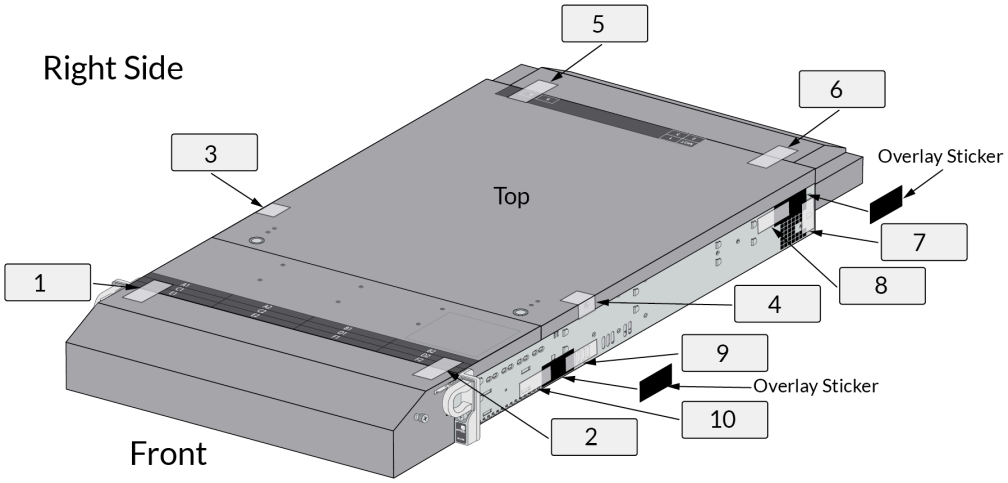

Figure 30 – M-600: Tamper Seal Locations (Top and Front)

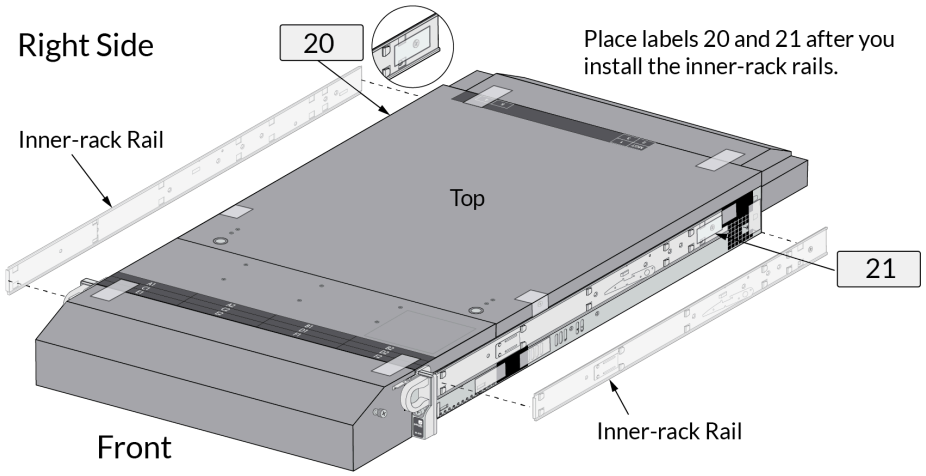

Figure 31 – M-600: Tamper Seals Location for Side Rails

8. Non-Invasive Security

There are currently no defined Approved non-invasive attack mitigation test metrics in SP 800-140F.

9. Sensitive Security Parameters Management

The following table details all the sensitive security parameters utilized by the module.

“TLS or SSH Session Key Encrypted” corresponds to the following KTS entries listed in the Approved Algorithms table:

- AES Cert. #A2137, HMAC Cert. #A2137
- AES-GCM Cert. #A2137

“SSH, KAS SP 800-56A Rev. 3” corresponds to the following KAS entries listed in the Approved Algorithms table:

- KAS-ECC-SSC Cert. #A2137, KDF SSH Cert. #A2137
- KAS-FFC-SSC Cert. #A2137, KDF SSH Cert. #A2137

“TLS, KAS SP 800-56A Rev. 3” corresponds to the following KAS entries listed in the Approved Algorithms table:

- KAS-ECC-SSC Cert. #A2137, KDF TLS Cert. #A2137
- KAS-FFC-SSC Cert. #A2137, KDF TLS Cert. #A2137

Table 15 - SSPs

Key/SSP/Name /Type	Strength	Security Function and Cert. Number	Generation	Import/Export	Establishment	Storage	Zeroization[1]	Use & Related Keys
CA Certificates	112 - 256 bits	RSA SigVer (FIPS 186-4) ECDSA SigVer (FIPS 186-4) Cert. #A2137	DRBG, FIPS 186-4	TLS or SSH Session Key Encrypted	N/A	HDD/RAM – plaintext	HDD – Zeroize Service RAM - Zeroize at session termination	ECDSA/RSA Public key - Used to trust a root CA intermediate CA and leaf /end entity certificates (RSA 2048, 3072, and 4096 bits) (ECDSA P-256, P-384, and P-521)
RSA Public Keys	112 - 150 bits	RSA SigVer (FIPS 186-4) Cert. #A2137	DRBG, FIPS 186-4	TLS or SSH Session Key Encrypted or Plaintext TLS handshake	N/A	HDD/RAM – plaintext	Zeroize Service	RSA public keys managed as certificates for the verification of signatures, establishment of TLS, operator authentication and peer authentication. (RSA 2048, 3072, or 4096-bit)
RSA Private Keys	112 - 150 bits	RSA SigGen (FIPS 186-4) Cert. #A2137	DRBG, FIPS 186-4	TLS or SSH Session Key Encrypted	N/A	HDD/RAM – plaintext	HDD – Zeroize Service RAM - Zeroize at session termination	RSA Private keys for generation of signatures, authentication or key establishment. (RSA 2048, 3072, or 4096-bit)
ECDSA Public Keys	128 - 256 bits	ECDSA SigVer (FIPS 186-4) Cert. #A2137	DRBG, FIPS 186-4	TLS or SSH Session Key Encrypted or Plaintext TLS handshake	N/A	HDD/RAM – plaintext	Zeroize Service	ECDSA public keys managed as certificates for the verification of signatures, establishment of TLS, operator authentication and peer authentication. (ECDSA P-256, P-384, or P-521)
ECDSA Private Keys	128 - 256 bits	ECDSA SigGen (FIPS 186-4) Cert. #A2137	DRBG, FIPS 186-4	TLS or SSH Session Key Encrypted	N/A	HDD/RAM – plaintext	HDD – Zeroize Service RAM - Zeroize at session termination	ECDSA Private key for generation of signatures and authentication (P-256, P-384, or P-521)
TLS DHE/ECDHE Private Components	128 - 256 bits	KAS-ECC-SSC KAS-FFC-SSC Cert. #A2137	DRBG, SP 800-56A Rev. 3	N/A	N/A	RAM - plaintext	Zeroize at session termination	KAS-FFC or KAS-ECC Ephemeral values used in key agreement (KAS-FFC MODP-2048, KAS-ECC P-256, P-384, P-521)
TLS DHE/ECDHE Public Components	128 - 256 bits	KAS-ECC-SSC KAS-FFC-SSC Cert. #A2137	DRBG, SP 800-56A Rev. 3	Plaintext - TLS handshake	N/A	N/A	Zeroize at session termination	KAS-FFC or KAS-ECC Ephemeral values used in key agreement (KAS-FFC MODP-2048, KAS-ECC P-256, P-384, P-521)
TLS Pre-Master Secret	112 bits minimum	KDF TLS Cert. #A2137, MD5 (No Security Claimed)	KAS-ECC-SSC or KAS-FFC-SSC, SP 800-56A Rev. 3	N/A	N/A	RAM – plaintext	Zeroize at session termination	Secret value used to derive the TLS Master Secret along with client and server random nonces
TLS Master Secret	384 bits	KDF TLS Cert. #A2137, MD5 (No Security Claimed)	KDF TLS (CVL)	N/A	N/A	RAM – plaintext	Zeroize at session termination	Secret value used to derive the TLS session keys

TLS Encryption Keys	128 or 256 bits	AES-CBC or AES-GCM Cert. #A2137	KDF TLS (CVL)	N/A	TLS, KAS SP 800-56A Rev. 3	RAM - plaintext	Zeroize at session termination	AES (128 or 256 bit) keys used in TLS connections (GCM; CBC)
TLS HMAC Keys	160 - 256 bits	HMAC-SHA2-256 HMAC-SHA2-384 Cert. #A2137	KDF TLS (CVL)	N/A	TLS, KAS SP 800-56A Rev. 3	RAM - plaintext	Zeroize at session termination	HMAC keys used in TLS connections (HMAC-SHA-1, HMAC-SHA2-256/384) (160, 256, 384 bits)
SSH DHE/ECDHE Private Components	112 - 256 bits	KAS-ECC-SSC KAS-FFC-SSC Cert. #A2137	DRBG, SP 800-56A Rev. 3	N/A	N/A	RAM - plaintext	Zeroize at session termination	KAS-FFC or KAS-ECC public component (KAS-FFC MODP-2048, KAS-ECC P-256, KAS-ECC P-384, KAS-ECC P-521)
SSH DHE/ECDHE Public Components	112 - 256 bits	KAS-ECC-SSC KAS-FFC-SSC Cert. #A2137	DRBG, SP 800-56A Rev. 3	Plaintext SSH handshake	N/A	RAM - plaintext	Zeroize at session termination	KAS-FFC or KAS-ECC public component (KAS-FFC MODP-2048, KAS-ECC P-256, KAS-ECC P-384, KAS-ECC P-521)
SSH Host Public Key	112 - 256 bits	RSA SigVer (FIPS 186-4) ECDSA SigVer (FIPS 186-4) Cert. #A2137	DRBG, FIPS 186-4	N/A	N/A	HDD/RAM – plaintext	Zeroize Service	SSH Host Public Key (RSA 2048, RSA 3072, RSA 4096, ECDSA P-256, P-384, or P-521)
SSH Client Public Key	112 - 150 bits	RSA SigVer (FIPS 186-4) Cert. #A2137	N/A	TLS or SSH Session Key Encrypted	N/A	HDD/RAM – plaintext	Zeroize Service	Public RSA key used to authenticate client. (RSA 2048, 3072, and 4096 bits)
SSH Session Encryption Keys	128 - 256 bits	AES-CBC, AES-CTR, or AES-GCM Cert. #A2137	KDF SSH (CVL)	N/A	SSH, KAS SP 800-56A Rev. 3	RAM - plaintext	Zeroize at session termination	Used in all SSH connections to the security module's command line interface. (128, 192, or 256 bits: CBC or CTR) (128 or 256 bits: GCM)
SSH Session Authentication Keys	160 - 256 bits	HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-512 Cert. #A2137	KDF SSH (CVL)	N/A	SSH, KAS SP 800-56A Rev. 3	RAM - plaintext	Zeroize at session termination	Authentication keys used in all SSH connections to the security module's command line interface (HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-512) (160, 256, 512 bits)
Firmware integrity verification key	128 bits	HMAC-SHA2-256, ECDSA SigVer (FIPS 186-4) Cert. #A2137	Factory preload	Import only, TLS or SSH Session Key Encrypted	N/A	HDD - plaintext	N/A	Used to check the integrity of all software code (HMAC-SHA-256 and ECDSA P-256) *(Note: This is not considered an SSP)*
Public Key for Firmware Load Test	112 bits	RSA SigVer (FIPS 186-4) Cert. #A2137	Factory preload	Import only, TLS or SSH Session Key Encrypted	N/A	HDD - plaintext	N/A	Used to authenticate firmware and content to be installed on the appliance (RSA 2048 with SHA-256)
CO, User Password	N/A	SHA2-256 Cert. #A2137	External	TLS or SSH Session Key Encrypted	N/A	HDD - a password hash (SHA2-256)	Zeroize Service	Authentication string with a minimum length of eight (8) characters.
Protocol Secrets	N/A	N/A	External	TLS or SSH Session Key Encrypted	N/A	HDD/RAM – plaintext	Zeroize Service	Secrets used by RADIUS (8 characters minimum)
Entropy Input String	256 bits	CKG (vendor affirmed), Counter DRBG	Entropy as per SP 800-90B	N/A	N/A	RAM - plaintext	Power cycle	Entropy input string coming from the entropy source

		Cert. #A2137						Input length = 384 bits
DRBG Seed	256 bits	CKG (vendor affirmed), Counter DRBG Cert. #A2137	Entropy as per SP 800-90B	N/A	N/A	RAM - plaintext	Power cycle	DRBG seed and input string coming from the entropy source and AES 256 CTR DRBG state (V and Key) used in the generation of a random values Input length = 128 bits Seed length = 384 bits
DRBG Key	256 bits	CKG (vendor affirmed), Counter DRBG Cert. #A2137	Entropy as per SP 800-90B	N/A	N/A	RAM - plaintext	Power cycle	AES 256 CTR DRBG state Key used in the generation of a random values
DRBG V	128 bits	CKG (vendor affirmed), Counter DRBG Cert. #A2137	Entropy as per SP 800-90B	N/A	N/A	RAM - plaintext	Power cycle	AES 256 CTR DRBG state V used in the generation of a random values
SNMPv3 Authentication Secret	N/A	KDF SNMP (CVL) Cert. #A2137	N/A	TLS or SSH Session Key Encrypted	N/A	HDD/RAM – plaintext	Zeroize Service	Used to support SNMPv3 services (Minimum 8 characters)
SNMPv3 Privacy Secret	N/A	KDF SNMP (CVL) Cert. #A2137	N/A	TLS or SSH Session Key Encrypted	N/A	HDD/RAM – plaintext	Zeroize Service	Used to support SNMPv3 services (Minimum 8 characters)
SNMPv3 Authentication Key	160 - 256 bits	HMAC-SHA-1 HMAC-SHA2-224 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512 Cert. #A2137	KDF SNMP (CVL)	N/A	N/A	HDD/RAM - Plaintext	Zeroize Service	HMAC–SHA-1/224/256 /384/512 Authentication protocol key (160 bits)
SNMPv3 Session Key	128 - 256 bits	AES-CFB128 Cert. #A2137	KDF SNMP (CVL)	N/A	N/A	HDD/RAM - Plaintext	Zeroize Service	Privacy protocol encryption key (AES 128/192/256 CFB)

Note: SSPs are implicitly zeroized when power is lost, or explicitly zeroized by the zeroize service. In the case of implicit zeroization, the SSPs are implicitly overwritten with random values due to their ephemeral memory being reset upon power loss. For the zeroization service and zeroization at session termination, the SSP's memory location is overwritten with random values.

Table 16 – Non-Deterministic Random Number Generation Specification

Entropy Source	Minimum number of bits of entropy	Details
Palo Alto Networks DRNG RDSEED Entropy Source	256 bits	ESV Cert. #129 When initialized per Section 11, the DRBG is seeded with 256 bits of entropy.
Palo Alto Networks RTC Entropy Source	256 bits	ESV Cert. #130 When initialized per Section 11, the DRBG is seeded with 256 bits of entropy.

10. Self-Tests

The cryptographic module performs the following tests below. The operator can command the module to perform the pre-operational and cryptographic algorithm self-tests by cycling power of the module; these tests do not require any additional operator action.

Pre-operational Self-Tests

Pre-operational Firmware Integrity Test

- Verified with HMAC-SHA-256 and ECDSA P-256

Note: the ECDSA and HMAC-SHA-256 KATs are performed prior to the Firmware Integrity Test

Conditional self-tests

Cryptographic algorithm self-tests

- AES 128-bit ECB Encrypt Known Answer Test
- AES 128-bit ECB Decrypt Known Answer Test
- AES 128-bit CMAC Known Answer Test*
- AES 256-bit GCM Encrypt Known Answer Test
- AES 256-bit GCM Decrypt Known Answer Test
- AES 192-bit CCM Encrypt Known Answer Test*
- AES 192-bit CCM Decrypt Known Answer Test*
- RSA 2048-bit PKCS#1 v1.5 with SHA-256 Sign Known Answer Test
- RSA 2048-bit PKCS#1 v1.5 with SHA-256 Verify Known Answer Test
- RSA 2048-bit Encrypt Known Answer Test*
- RSA 2048-bit Decrypt Known Answer Test*
- ECDSA P-256 with SHA-512 Sign Known Answer Test
- ECDSA P-256 with SHA-512 Verify Known Answer Test
- HMAC-SHA-1 Known Answer Test
- HMAC-SHA-256 Known Answer Test
- HMAC-SHA-384 Known Answer Test
- HMAC-SHA-512 Known Answer Test
- SHA-1 Known Answer Test
- SHA-256 Known Answer Test
- SHA-384 Known Answer Test
- SHA-512 Known Answer Test
- DRBG SP 800-90Arev1 Instantiate/Generate/Reseed Known Answer Tests
- SP 800-90Arev1 Instantiate/Generate/Reseed Section 11.3 Health Tests
- SP 800-56Ar3 KAS-FFC-SSC 2048-bit Known Answer Test
- SP 800-56Ar3 KAS-ECC-SSC P-256 Known Answer Test
- SP 800-135rev1 TLS 1.0/1.1 KDF Known Answer Test
- SP 800-135rev1 TLS 1.2 KDF with SHA-256 Known Answer Test
- SP 800-135rev1 SSH KDF with SHA-256 Known Answer Tests
- SP 800-135rev1 IKEv2 KDF Known Answer Tests*
  Note: Supported by the module cryptographic implementation, but only utilized for CAST
- SP 800-90B RCT/APT Health Tests on Entropy Source
  Note: The SP 800-90B Health Tests are implemented by the entropy source.

**Note: Supported by the module cryptographic implementation, but only utilized for CAST*

Conditional Pairwise Consistency Self-Tests

- RSA Pairwise Consistency Test

- ECDSA/KAS-ECC Pairwise Consistency Test
- KAS-FFC Pairwise Consistency Test

Conditional Firmware Load test

- Firmware Load Test – Verify RSA 2048 with SHA-256 signature on firmware at time of load

Conditional Critical Functions Tests

- SP 800-56A Rev. 3 Assurance Tests (Based on Sections 5.5.2, 5.6.2, and 5.6.3)

Error Handling

In the event of a conditional test failure, the module will output a description of the error. These are summarized below.

Table 17 - Errors and Indicators

Cause of Error	Error State Indicator
Conditional Cryptographic Algorithm Self-Test or Firmware Integrity Test Failure	FIPS-CC mode failure. <Algorithm test> failed.
Conditional Pairwise Consistency or Critical Functions Test Failure	System log prints an error message.
Conditional Firmware Load Test Failure	System prints Invalid image message.

11. Life-cycle Assurance

When FIPS-CC mode is enabled, the module runs all the required items noted in Section 10 Self-Tests. The vendor provided life-cycle assurance documentation that describes configuration management, design, finite state model, development, testing, delivery + operation, end of life procedures, and guidance. For details regarding the secure installation, initialization, startup, and operation of the module, see section “Modes of Operation”.

Palo Alto Network provides an Administrator Guide for additional information noted in the “References” section of this Security Policy.

Module Enforced 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 140-3 Level 2 module.

1. The cryptographic module shall provide distinct operator roles. When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
2. The cryptographic module provides identity-based authentication
3. The cryptographic module shall clear previous authentications on power cycle.

4. The module shall support the generation of key material with the approved DRBG. The entropy provided must be greater than or equal to the strength of the key being generated.
1. Data output shall be inhibited during power-up self-tests and error states.
2. Processes performing key generation and zeroization processes shall be logically isolated from the logical data output paths.
3. The module does not output intermediate key generation values.
4. Status information output from the module shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
5. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
6. The module maintains separation between concurrent operators.
7. The module does not support a maintenance interface or role.
8. The module does not have any external input/output devices used for entry/output of data.
9. The module does not enter or output plaintext CSPs.

Vendor imposed security rules

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

1. The operator shall not enable TLSv1.0 or use RSA for key wrapping; it is disabled by default.
    a. Checked via CLI using “show shared” command
2. When FIPS-CC mode is enabled, the operator shall not install plugins.
    a. Checked via CLI using “show plugins installed”
3. When FIPS-CC mode is enabled, the operator shall not use TACACS+. RADIUS may be used but must be protected by TLS protocol.
    a. Checked via CLI using “show deviceconfig” command
4. Once boot-up is complete, the module requires a minimum system uptime of 1 hour shall pass before the module can be used to ensure proper instantiation of the DRBG.
    a. Verify uptime via the following command: “show system info | match uptime”
    b. After this time, the server certificate (i.e. CA Certificate with Public/Private keys) and SSH Host Keys shall be regenerated using the following procedure:
        i. Login via CLI and issue the following commands:
            1. set deviceconfig system ssh profiles mgmt-profiles server-profiles <Name> default-hostkey key-type <RSA/ECDSA> <Key Size>
            2. set deviceconfig system ssh regenerate-hostkeys mgmt key-type <RSA/ECDSA> key-length <Key Size>
            3. set deviceconfig system ssh mgmt server-profile <Name>
            4. commit (Once complete, exit configure state)
            5. set ssh service-restart mgmt
        ii. Login via WebUI and create a new certificate chain
            1. Create new certificates via Device > Certificate Management > Certificates
            2. Navigate to Device > Setup > Management > General Settings > Click the gear icon
                a. Select “SSL/TLS Service Profile” and create a new profile with the certificates generated in previous step
                b. Click OK and commit the configuration

Failure to follow these Security Rules will cause the module to operate in a non-compliant state.

Key to Entity

The cryptographic module associates all keys (secret, private, or public) stored within, entered into or output from the module with authenticated operators of the module. Keys stored within the module are only made available to authenticated operators via TLS or SSH. Keys are only input or output from the module by the authenticated operator via a SSH or TLS protected communication. Any attempt to intervene in the key to entity relationship would require defeating the module TLS or SSH encryption and authentication/integrity mechanism.

12. Mitigation of Other Attacks

The module is not designed to mitigate any specific attacks outside the scope of FIPS 140-3. These requirements are not applicable.

13. References

[FIPS 140-3] FIPS Publication 140-3 Security Requirements for Cryptographic Modules

[AGD] Panorama Administrator's Guide Version 10.1

14. Definitions and Acronyms

AES – Advanced Encryption Standard
CA – Certificate Authority
CLI – Command Line Interface
CO – Crypto-Officer
CSP – Critical Security Parameter
CVL – Component Validation List
DB9 – D-sub series, E size, 9 pins
DES – Data Encryption Standard
DH – Diffie-Hellman
DRBG – Deterministic Random Bit Generator
EDC – Error Detection Code
ECDH – Elliptical Curve Diffie-Hellman
ECDSA – Elliptical Curve Digital Signature Algorithm
FIPS – Federal Information Processing Standard
HMAC – (Keyed) Hashed Message Authentication Code
KDF – Key Derivation Function
LED – Light Emitting Diode
RJ45 – Networking Connector
RNG –Random number generator
RSA – Algorithm developed by Rivest, Shamir and Adleman
SHA – Secure Hash Algorithm
SNMP – Simple Network Management Protocol
SSH – Secure Shell
TLS – Transport Layer Security
USB – Universal Serial Bus
VGA – Video Graphics Array