Panorama M-100

FIPS 140-2 Non-Proprietary Security Policy

Palo Alto Networks
4401 Great America Parkway
Santa Clara, CA 95054
www.paloaltonetworks.com

Version: A

Revision Date: 7/29/2015

Change Record

Table 1 - Change Record

Revision	Date	Author	Description of Change
A	7/29/2015	R.Bishop	Initial Authoring

Contents

Tables

Figures

1 Module Overview

Panorama M-100 provides 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-100 management appliance individual management and logging components can be separated in a distributed manner to accommodate large volumes of log data. Panorama M-100 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 M-100 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.
  - Panorama M-100 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.

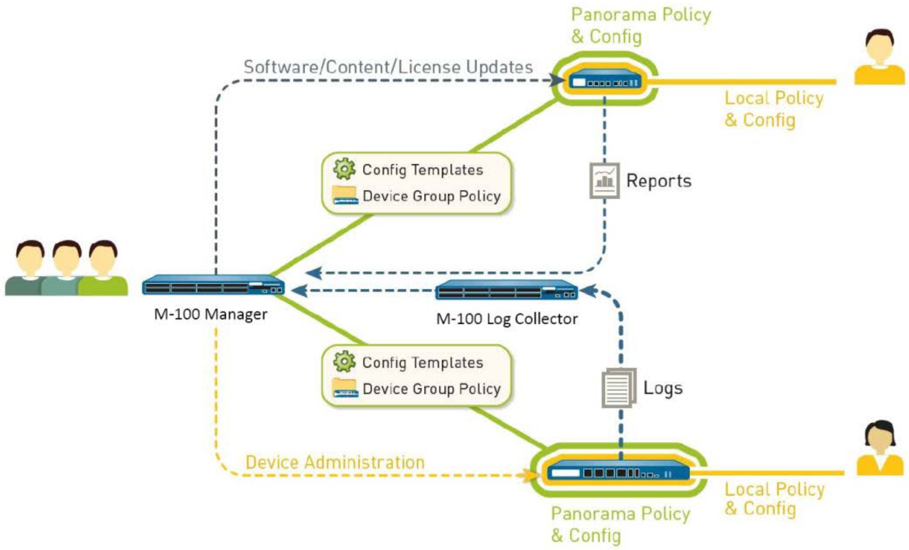


Figure 1 - Panorama M-100 Deployment

The Palo Alto Networks Panorama M-100 is a multi-chip standalone module. The M-100 is shown in Figure 2. Figures 3 and 4 provide images of the module with the FIPS kit's opacity shields in place. Table 2 below provides the names and versions of the validated modules.

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	6.1.3
Panorama M-100 4TB RAID: 8 x 1TB RAID Certified HDD for 4TB of RAID Storage	910-000092	00D	920-000140	00A	6.1.3

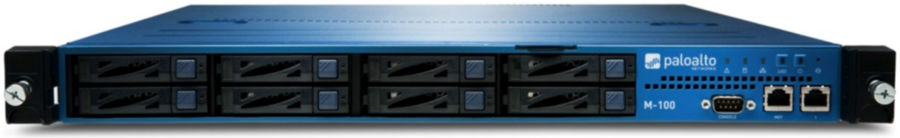


Figure 2 –Front/Top of M-100

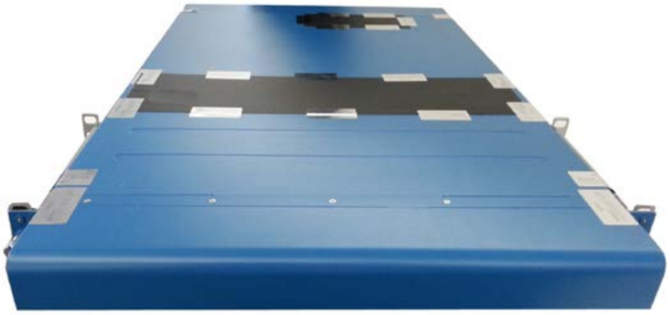


Figure 3 –Top/Front of M-100 with FIPS kit

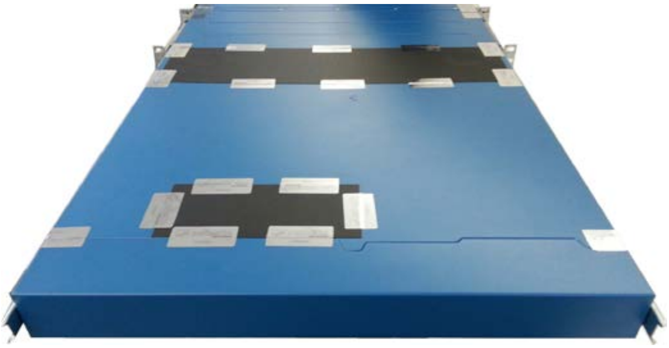


Figure 4 – Top/Rear of M-100 with FIPS kit

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 following procedure will configure the Approved mode of operation:

- The tamper evidence seals and opacity shields must be installed per Section 9. 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 CCEAL4 Mode” option to enter Approved mode.
- Select “Enable CCEAL4 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 “**** CCEAL4 MODE ENABLED ****” via the CLI session.
- Status output interface will indicate “CCEAL4 mode enabled successfully” via the console port.
- The module will display “CC” at all times in the status bar at the bottom of the web interface.

2.2 Selecting Panorama Manager and Log Collector Approved modes of operation

Panorama M-100 supports two configurations that provide varying services. The module can be initialized into two 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.

Convert the M-100 appliance from Panorama Manager mode to the dedicated Log Collector mode:

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

Convert the M-100 appliance from Panorama Log Collector mode to the Manager mode:

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

2.3 Security Level

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	2 or 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 Manger mode the module supports Level 3, identity based authentication. When initialized in Panorama Logger mode the module supports Level 2, role based authentication.	

2.4 Approved and Allowed Algorithms

The cryptographic module supports the following FIPS Approved algorithms.

Table 4 - FIPS Approved Algorithms Used in Current Module

FIPS Approved Algorithm	CAVP Cert. #
AES: ECB, CBC, CFB, OFB modes; Encrypt/Decrypt; 128, 192 and 256-bit CTR mode; 128-bit	3180
FIPS 186-4 RSA : - Key Generation: 2048 and 3072-bit - Signature Generation: 2048 and 3072-bit - Signature Verification: 1024, 2048 and 3072-bit	1616
HMAC-SHA-1, HMAC-SHA-256	2006
SHA-1, SHA-256, SHA-384, SHA-512	2632
SP800-90A AES 128 CTR DRBG	662

FIPS Approved Algorithm	CAVP Cert. #
SP 800-135 KDF – TLS 1.0, SNMPv3, SSH v2 Note: TLS 1.1 is not supported by the module.	425

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

Table 5 - FIPS Allowed Algorithms Used in Current Module

FIPS Allowed Algorithm
Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength)
RSA (key wrapping, key establishment methodology provides a minimum of 112 bits of encryption strength)
AES (Cert# 3180 key wrapping; key establishment methodology provides 128 or 256 bits of encryption strength)
Non-Approved NDRNG (seeding source)
MD5 (within TLS only)

Table 6 - Supported Protocols in FIPS Approved Mode

Supported Protocols
TLS v1.0
SSH v2
SNMP v2c,v3

Note: These protocols have not been reviewed or tested by the CAVP or the CMVP.

2.5 Non-Approved Mode of Operation

All services and security functions available in the Approved mode are also available in the non-Approved mode of operation. The cryptographic module additional supports the following non-Approved algorithms in the non-Approved mode of operation. No security claim is made in the current module for any of the following non-Approved algorithms.

Table 7 - Non-Approved, Non-Allowed Algorithms Used in Current Module

Non-FIPS Allowed Algorithms in Non-Approved Mode
Signature generation and key establishment using RSA 512 and RSA 1024 certificates
Digital signatures using MD5 and SHA-1
MD5 – used for hashing
RC4 – used to encrypt SSL communications with the security module.

Non-FIPS Allowed Algorithms in Non-Approved Mode
Camellia - used to encrypt SSL communications with the security module.
RC2 - used to encrypt SSL communications with the security module.
SEED - used to encrypt SSL communications with the security module.
DES - used to encrypt SSL communications with the security module.

3 Ports and Interfaces

The module provides the following ports and interfaces.

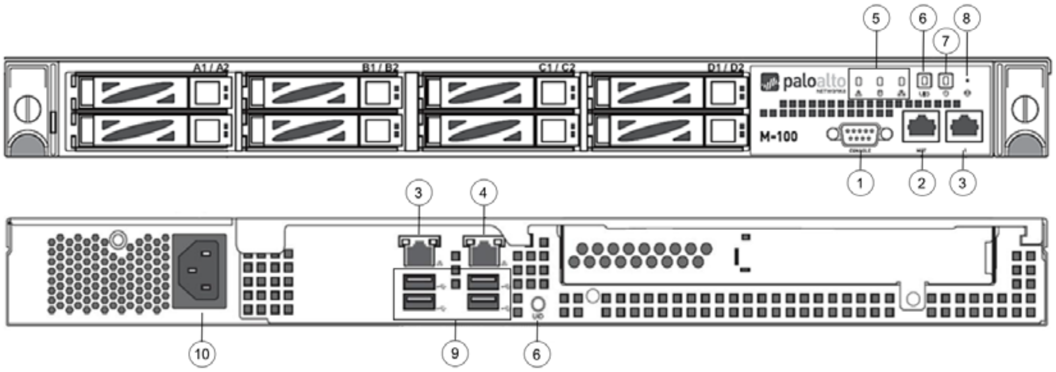


Figure 5 – Ports and Interfaces

Table 8 - Panorama FIPS 140-2 Ports and Interfaces

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

4 Identification and Authentication Policy

4.1 *Assumption of Roles*

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

The module supports concurrent operators.

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

Table 9 – 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 10 - 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	Password or certificate/public key based authentication.

Table 11 - Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Username and Password	Minimum password length is 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 4 authentication requests per 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 at a minimum 2048-bit RSA keys. Such keys possess an equivalent strength of 112 bits. The probability that a random attempt will succeed is 1/(2^{112}) which is less than 1/1,000,000. The firewall supports at most 60,000 new sessions per second to authenticate in a one-minute period 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.

5 Security Parameters

Table 12 - Private Keys and CSPs

Key/CSP	Description
RSA Private Keys	RSA Private keys support establishment of TLS session keys, SSH host authentication, user private keys and certificate signing keys.
TLS DH private Components	Diffie-Hellman private component (≥ 224 bits)
TLS Pre-master Secret	Secret value used to derive the TLS session keys
TLS Encryption keys	AES 128, 256 session keys used in TLS connections
TLS MAC keys	HMAC-SHA1 session keys used in TLS connections (≥ 128 bits)
SSH DH private components	Diffie-Hellman private component (≥ 224 bits)
SSH encryption key	AES 128, 192, 256 session key used in SSH connections
SSH authentication key	HMAC-SHA1 session key used in SSH connections (≥ 128 bits)
Operator passwords	Password for operator authentication.
DRBG seed and state	AES 128 CTR DRBG used in the generation of a random values

Key/CSP	Description
SNMPv3 Secrets	SNMPv3 Authentication Secret and Privacy Secret
SNMPv3 Keys	AES Privacy key and HMAC- SHA 1 Authentication keys
Note: All CSP and keys defined may be accessed by the Manager and Log-Collector modes. The CSP and keys may be shared between the Approved modes of operation.	

Table 13 - Public Keys

Key Name	Description
CA certificates	Used to extend trust for certificates
RSA Public Keys / Certificates	RSA Public keys managed as certificates for the verification of signatures, establishment of TLS, operator authentication and peer authentication. (2048 or 3072 bits)
TLS DH public components	Used in key agreement (2048 bits)
SSH DH public components	Used in key agreement (2048 bits)
SSH Host public key	Used in SSH public key authentication process (2048 bits)
SSH Client public key	Used in SSH public key authentication process (≥ 2048 bits)
Firmware Authentication Key	RSA key used to authenticate firmware (2048 bits)
Note: All keys defined may be accessed by the Manager and Log-Collector modes. 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 modes 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. 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 services as listed in Tables 14 and 15. CSP access by services is further described in the following table. Additional service information and administrator guidance for Panorama M-100 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 M-100 Manager provides services via web-browser based interface and a command line interface (CLI). For Panorama M-100 Log Collector mode, only the CLI is available for management.

Table 14 - Authenticated Services – Panorama M-100 Manager

Service	Description	CSP Access
System Provisioning	Perform panorama licensing, diagnostics, debug functions, manage Panorama support information and switch between Panorama Manager and Logger	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 Software 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 Private 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 public keys
Configure High Availability	Configure High Availability communication settings	N/A
Panorama Certificate Management	Manage RSA certificates and private keys certificate profiles, revocation status and usage.	Import or export RSA private keys Generate RSA private keys Sign RSA private keys Execute DRBG seed and state
Panorama Log settings	Configure log forwarding	N/A
Panorama Server Profiles	Configure communication parameters and information for peer servers such as Syslog, SNMP trap servers, email servers and authentication servers.	Import SNMPv3 Secrets

Service	Description	CSP Access
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 private keys Signature generation with RSA private keys Generate RSA private 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
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 15 - Authenticated Services – Panorama M-100 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 Private Keys
Panorama Software 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 certificates and private keys certificate profiles, revocation status and usage.	Import or export RSA private keys Generate RSA private keys Sign with RSA private keys DRBG seed and state

6.2 Unauthenticated Services

The cryptographic module supports the following unauthenticated services:

Table 16 - 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.
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. There is no security claimed from this service.

7 Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the module contains a non-modifiable operational environment.

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 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 Panorama M-100 cryptographic module shall support initialization as a Log Collector in an Approved mode of operation with Level 2 role-based authentication or support initialization as a Panorama Manager in an Approved mode of operation with Level 3 identity-based authentication.
3. The cryptographic module shall clear previous authentications on power cycle.
4. The cryptographic module shall perform the following tests
    - A. Power up Self-Tests
        1. Cryptographic algorithm tests
            - a. AES Encrypt Known Answer Test
            - b. AES Decrypt Known Answer Test
            - c. RSA Sign Known Answer Test
            - d. RSA Verify Known Answer Test
            - e. HMAC-SHA-1 Known Answer Test
            - f. HMAC-SHA-256 Known Answer Test
            - g. SHA-1 Known Answer Test
            - h. SHA-256 Known Answer Test
            - i. SHA-384 Known Answer Test
            - j. SHA-512 Known Answer Test
            - k. DRBG Known Answer Test
            - l. SP 800-90A Health Tests
            - m. DH Parameter Test
            - n. DH Known Answer Test
    - B. Firmware Integrity Test – A 128 bit EDC is calculated on non-security related code. Security related code is verified with SHA-256.
    - C. Conditional Self-Tests
        1. Continuous Random Number Generator (RNG) test – performed on NDRNG and DRBG (128 bits)
        2. RSA Pairwise Consistency Test Sign/Verify and Encrypt/Decrypt
        3. Firmware Load Test – Verify RSA 2048 signature on firmware at time of load
    - D. If any conditional test fails, the module will output 'CC EAL4 failure' and the specific test that failed.

5. The operator shall be 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 of operation from/to the Manager mode, the cryptographic module shall reboot and perform all power-up self-tests.
7. Power-up self-tests shall not require any operator action.
8. Data output shall be inhibited during power-up self-tests and error states.
9. Processes performing key generation and zeroization processes shall be 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 shall 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. If the cryptographic module remains inactive in any valid role for the administrator specified time interval, the module automatically logs out the operator.
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 have occurred, the cryptographic module shall enforce a wait period of at least 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 seals that are applied on the modules by the Crypto-Officer. 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 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 seals. The seals prevent removal of the opaque enclosure without evidence. The Crypto-Officer should inspect the seals and shields for evidence of tamper every 30 days. If the seals show evidence of tamper, the Crypto-Officer should assume that the modules have been compromised and contact support.

Note: For ordering information, see Table 2 for FIPS kit part numbers and versions. Opacity shields are included in the FIPS kits. Tamper seals are not available to be ordered separately.

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

9.2 *Operator Required Actions*

Table 17 - Inspection/Testing of Physical Security Mechanisms

Model	Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
M-100	Tamper Evident Seals	30 days	Verify integrity of tamper evident seals in the locations identified in the FIPS Kit Installation Guide and 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.

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

EDC – Error Detection Code

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

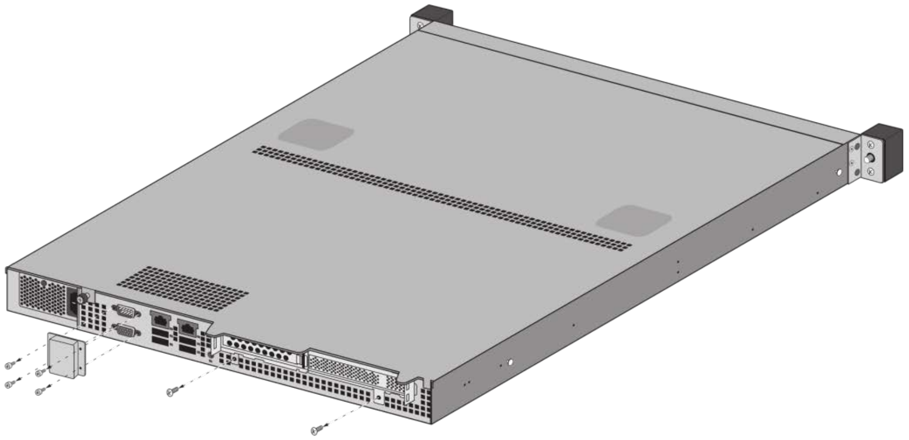
SHA – Secure Hash Algorithm

TLS – Transport Layer Security

USB – Universal Serial Bus

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

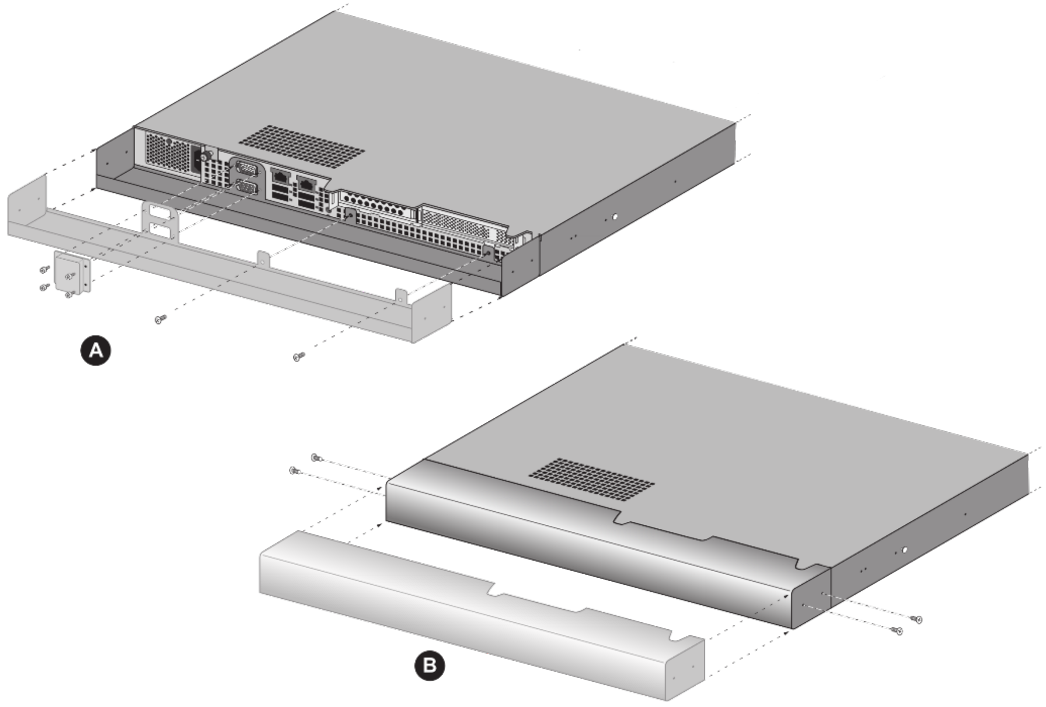
Step 1: From the rear of the module, remove the six screws and port cover, as shown. Retain screws and port cover for the Step 2.



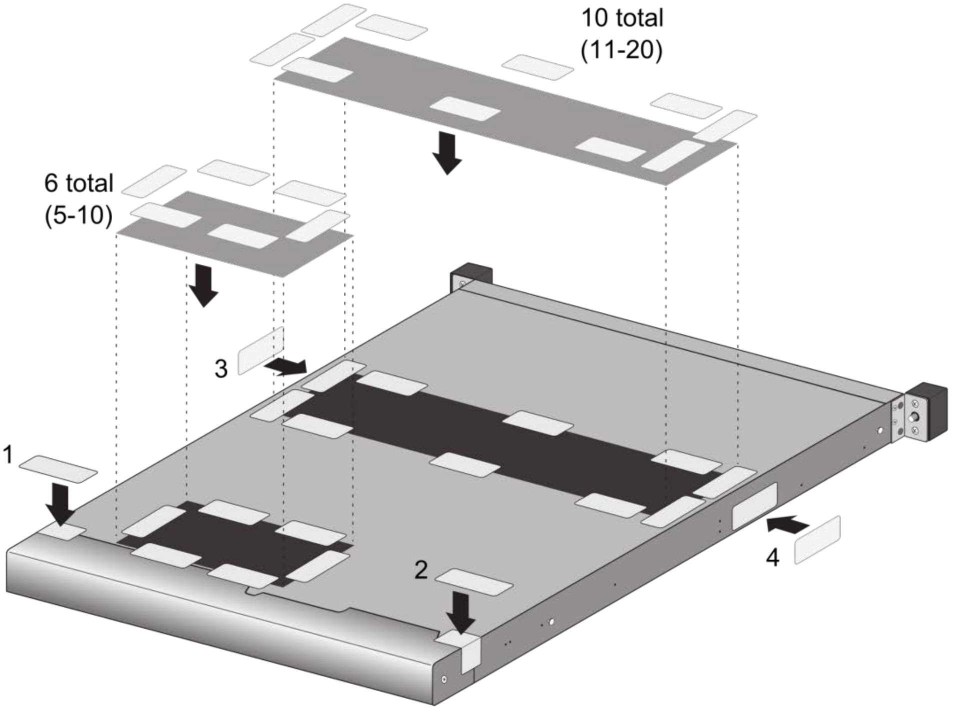
Step 2: Attach the rear opacity shields.

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. Note: The power-cord should be connected at this point.

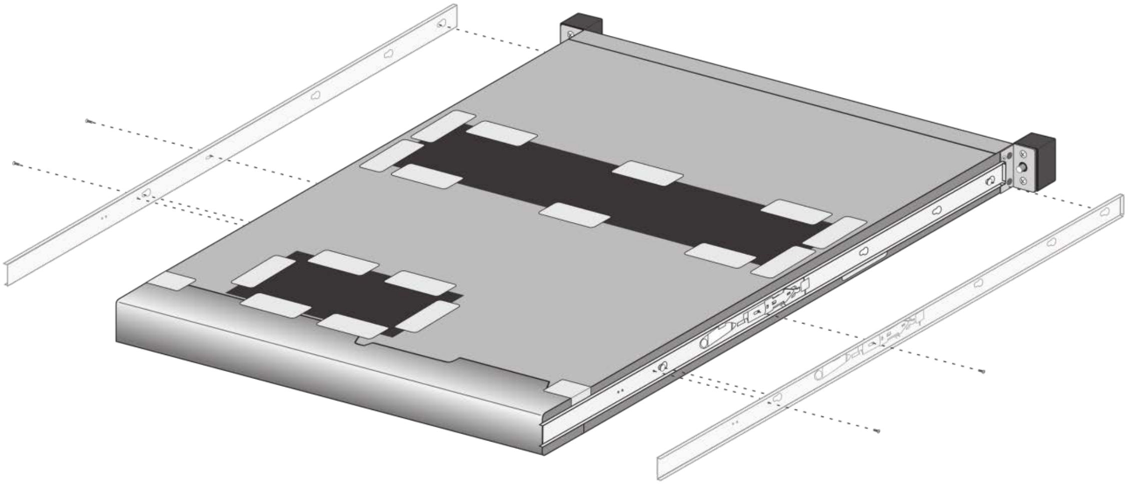
B. Use four #4-40 1/4” screws to attach the rear cover to the bracket.



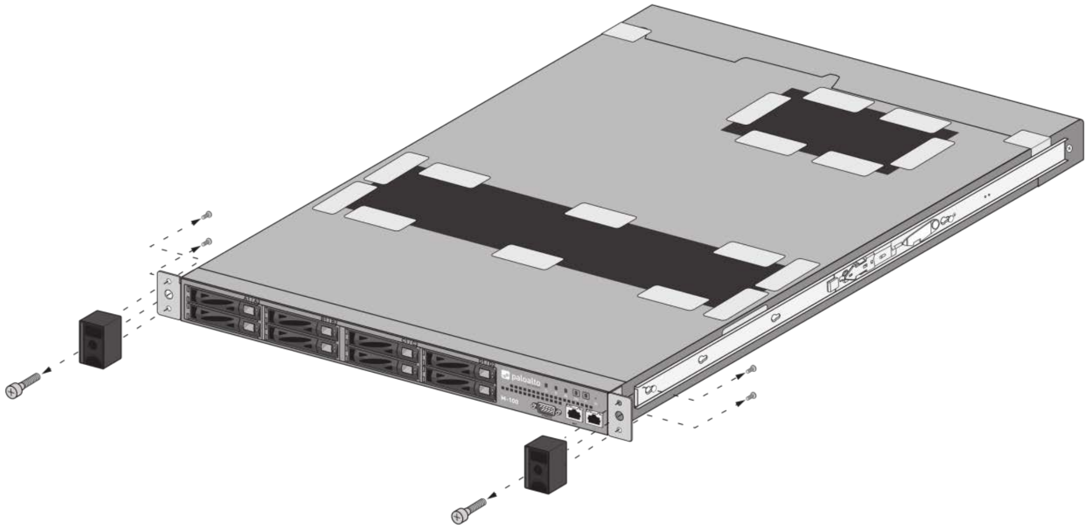
Step 3: Apply tamper evident seals (two labels) to the seam of the rear cover and rear outer edges of the appliance (labels numbered 1 and 2 in the illustration). Apply tamper evident seals to the left and right sides covering the side holes (2 labels numbered 3 and 4). Apply top air vent overlay covers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



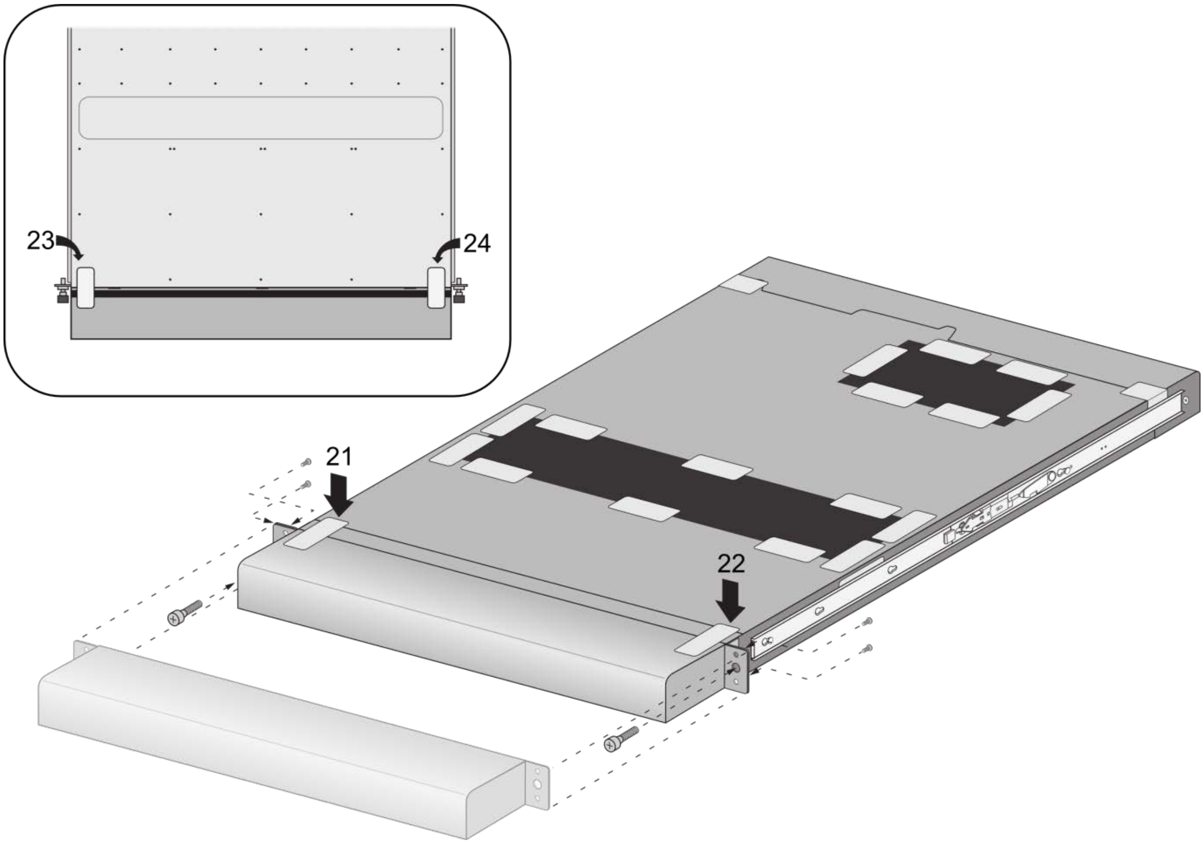
Step 4: Place side inner rails to each side of the module and attach using rail kit screws.



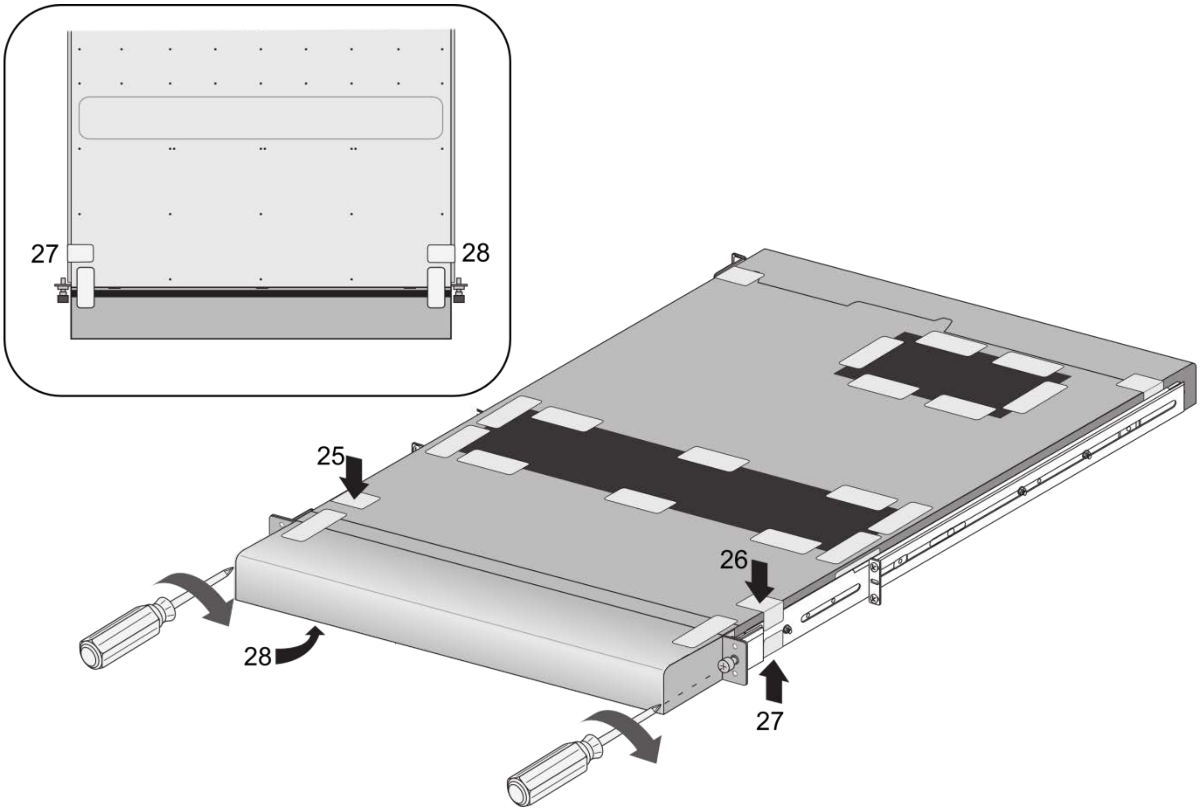
Step 5: Remove the two front plastic bracket covers and screws. Remove and retain the two captive screws from the plastic covers.



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.



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


27
28
25
26
28
27