WildFire WF-500
FIPS 140-2
Non-Proprietary Security Policy

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

Version: G

Revision Date: 11/18/2016

`

Change Record

Table 1 - Change Record

Revision	Date	Author	Description of Change
A	12/10/2015	A. Shahhosseini	Initial authoring
B	3/7/2016	A. Shahhosseini	Response to CMVP comments
C	8/23/2016	A. Shahhosseini	Updated content with new firmware version (7.1.3)
D	10/27/2016	A. Shahhosseini	Updates to address CMVP comments
E	11/9/2016	A. Shahhosseini	Updates to address CMVP comments
F	11/16/2016	A. Shahhosseini	Updates to address CMVP comments
G	11/18/2016	A. Shahhosseini	Updates to address CMVP comments

Contents

Tables

Figures

Module Overview

WildFire WF-500 identifies unknown malware, zero-day exploits, and Advanced Persistent Threats (APTs) through dynamic analysis, and automatically disseminates protection in near real-time to help security teams meet the challenge of advanced cyber-attacks.

Unknown files are analyzed by WildFire in a scalable sandbox environment where new threats are identified and protections are automatically developed and delivered in the form of an update. The result is a unique, closed loop approach to controlling cyber threats that begins with positive security controls to reduce the attack surface, inspection of all traffic, ports, and protocols to block all known threats, and rapid detection of unknown threats by observing their actual behavior.

The Palo Alto Networks WildFire WF-500 is a multi-chip standalone module. The module is shown in Figure 1. The module boundary is the outer chassis enclosure. The cryptographic boundary includes all of the logical components of the modules and the boundary is the physical enclosure of the WF-500. Figure 2 through Figure 5 provide images of the module with the FIPS kit's opacity shields in place. See Section 1.9 for details regarding the module's physical security mechanisms.

Table 2 - Validated Version Information

Module	Part Number	Hardware Version	FIPS Kit Part Number	FIPS Kit Hardware Version	Firmware Version
WF-500	910-000097-00G	Rev G	920-000145	00A	7.1.3

Figure 1 – Front View of WF-500

Figure 2 - Front View of WF-500 with Opacity Shield

Figure 3 - Rear View of WF-500 with Opacity Shield

Figure 4 - Right View of WF-500 with Opacity Shields

Figure 5 - Left View of WF-500 with Opacity Shields

Mode of Operation

1.1 Security Levels

The cryptographic module meets the overall requirements applicable to Level 2 security of FIPS 140-2.

Table 3 - Module Security Level Specification

Security Requirements Section	Levels
Cryptographic Module Specification	3
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	3
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A

1.2 FIPS 140-2 Approved Mode of Operation

The module provides both a FIPS 140-2 Approved and non-Approved mode of operation.

The following procedure will place the module into the Approved mode of operation:

- Install module and interface connections in addition to the FIPS kit.
- The tamper evident labels and opacity shields must be installed as per Appendix A for the module to operate in the FIPS Approved mode of operation.
- Apply power to the device.
- Establish a serial connection to the console port, and command the module to enter into maintenance mode. The module will reboot, and then enter maintenance mode.
- After reboot, select “Continue.”
- Select the “Set FIPS-CC” option, and press enter.
- Select “Enable FIPS-CC Mode”, and press enter.
- When prompted, select “Reboot” and the module will re-initialize and continue into the Approved mode.
- The module will reboot.
- In the Approved mode, the console port is available only as a status output port.

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

- Status output interface will indicate "**** FIPS-CC MODE ENABLED ****" via the CLI session.
- Status output interface will indicate "FIPS-CC mode enabled successfully" via the console port.

Should one or more power-up self-tests fail, the module will not enter the FIPS Approved mode of operation. 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 by following the on-screen instructions.

1.3 Approved and Allowed Algorithms

The cryptographic module has the following CAVP certificates:

Table 4 – CAVP Certificates for FIPS Approved Algorithms

FIPS Approved Algorithm	CAVP Cert. #
AES ECB, CBC, CFB, OFB, CTR modes (encrypt/decrypt): 128, 192, 256 bits CCM: 128 bits GCM (encrypt/decrypt): 128, 256 bits Note: GCM is used compliant with SP 800-52 and used in accordance to Section 4 of RFC 5288 for TLS key establishment.	4020
CVL (SP 800-56A) EC Diffie-Hellman Exchange except KDF P-256, P-384, Diffie-Hellman Exchange 2048	849
CVL (SP800-135: TLS 1.0/1.1/1.2, SSH, SNMP)	848
CVL (SP800-56A: Section 5.7.1.2) P-256 and P-384	874
DRBG SP800-90A AES 256 CTR DRBG	1198
ECDSA (FIPS 186-4) ECDSA P-256, P-384, P-521 Signature Verification	896 CVL 873
HMAC HMAC-SHA-1/256/384	2622
RSA (FIPS 186-4) Key Generation: 2048, 3072 bits Signature Generation: 2048 and 3072 bits Signature Verification: 1024, 2048, 3072 bits	2064
SHA	3316

FIPS Approved Algorithm	CAVP Cert. #
SHA-1, SHA-256, SHA-384, SHA-512	
SP800-56A Rev. 2 EC Diffie-Hellman Exchange (with CVL Certs. #848 and #849, key agreement; key establishment methodology provides 128 or 192 bits of encryption strength)	Vendor Affirmed

Note: For specifics regarding what is supported in the Approved mode, see subsequent sections below in this document.

The cryptographic module supports the following non-FIPS Approved algorithms that are allowed for use in the Approved mode of operation:

Table 5 - FIPS Allowed Algorithms Used in the Approved Mode

FIPS Allowed Algorithms
Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength)
MD5 (within TLS)
Non-Approved NDRNG (used to seed DRBG) This provides a minimum of 256 bits of entropy.
RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength)

Table 6 - Supported Protocols in the Approved Mode

Supported Protocols
TLS v1.0/1.1, 1.2
SSHv2
SNMPv2c, v3

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

1.4 Non-Approved, Non-Allowed Algorithms

The cryptographic module supports the following non-Approved algorithms. No security claim is made in the current module for any of the following non-Approved algorithms.

Table 7 - Non-Approved, Non-Allowed Algorithms Used in the Non-Approved Mode

Non-FIPS Algorithms in Non-Approved Mode
Encrypt/Decrypt – Triple-DES (non-compliant), CAST, ARCFOUR, Blowfish, Camellia, SEED, RC2, RC4
Key Exchange using non-Approved strengths – Diffie-Hellman (1024), RSA (Less than 2048 bits), EC Diffie-Hellman (sect571r1, sect571k1, secp521r1, sect409k1, sect409r1, sect283k1, sect283r1, secp256k1, sect239k1, sect233k1, sect233r1, secp224k1, secp224r1, sect193r1, sect193r2, secp192k1, secp192r1, sect163k1, sect163r1, sect163r2, secp160k1, secp160r1, secp160r2)

Non-FIPS Algorithms in Non-Approved Mode
Message Authentication – HMAC-MD5, UMAC, HMAC-RIPEMD
Hashing – MD5, RIPEMD
Digital Signatures (non-Approved strengths or using SHA-1): RSA, ECDSA, DSA

Ports and Interfaces

The WF-500 provides the following ports and interfaces:

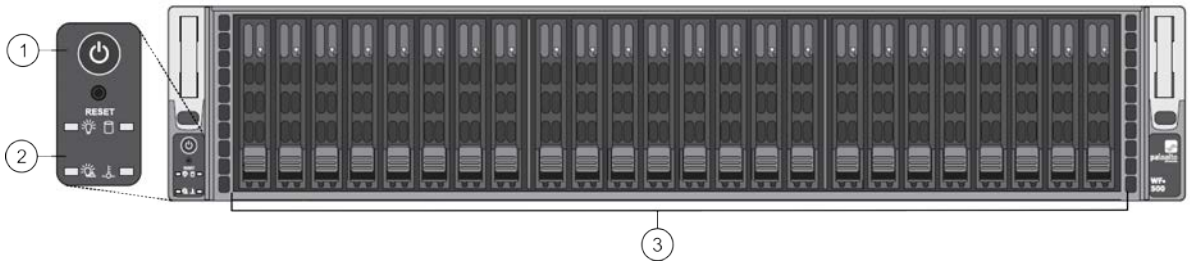

Figure 6 - Front ports and Interfaces

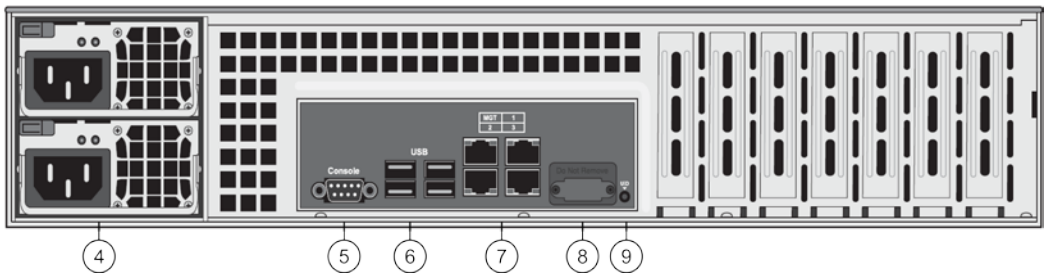

Figure 7 - Rear ports and Interfaces

Table 8 – WF-500 Ports and Interfaces

Interface		Name and Description	Qty.	FIPS 140-2 Designation
1	Power Button and Reset	Reboot or shut down device	2	Control input
2	Front LED Panel	Power, Power Failure, HDD, Overheat/Fan Failure	4	Status output
3	Drive LEDs	Left LED—drive failure Right LED—drive activity	48	Status output
4	Power	Power supplies	2	Power Input
5	DB9	Console *(Note: In the Approved mode, the Console port is only available as Status output)*	1	Data input, Control input, Data output, Status output
6	USB	Disabled *(Note: Reserved for future use)*	4	N/A - Disabled
7	RJ45	MGT Ethernet 10/100/1000	1	Data input, Control input, Data output, Status output
		Ethernet 1 VM (Note: In the Approved mode, this port is disabled)	1	Data input, Data output

Interface		Name and Description	Qty.	FIPS 140-2 Designation
		Ethernet 2 and 3 *(Note: Reserved for future use)*	2	N/A - Disabled
8	VGA	Graphic port *(Note: Reserved for future use)*	1	N/A - Disabled
9	UID button with LED	Button that activates LED on front and back of chassis to help identify physical location	1	Control input, Status output

Identification and Authentication Policy

1.5 Assumption of Roles

The module supports distinct operator roles. The cryptographic module enforces the separation of roles using unique authentication credentials associated with operator accounts.

The module supports concurrent operators.

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

Table 9 – Roles and Authentication

Role	Description	Authentication Type	Authentication Data
Crypto-Officer (CO)	This role has read, write, execute, and delete capabilities for all 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
User	This User role has read-only access defined for a set of configuration and status information.	Identity-based operator authentication	Username and password

Table 10 - Strength of Authentication Mechanism

Authentication Mechanism	Strength of Mechanism
Username and Password	The minimum length of a password 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 a maximum of 10 failed attempts to authenticate into the module in a one-minute period. If the maximum number of attempts is reached, the operator is locked out for a configurable time period (1 minute to indefinitely). Therefore, the probability of successfully authenticating to the module within a one-minute period is $10/(95^6)$, which is less than 1/100,000.

Security Parameters

The module contains the following keys and Critical Security Parameters (CSP):

Table 11 - Private Keys and CSPs

CSP #	Key/CSP	Description
1	RSA Private keys	RSA 2048 Private keys support establishment of TLS session keys, and host authentication.
2	TLS DH Private Components	Diffie-Hellman private component (≥ 224 bits). (DHE 2048, ECDHE P-256, P-384)
3	TLS Pre-Master Secret	Secret value used to derive TLS session keys.
4	TLS Encryption keys	AES (128 or 256 bit; CBC or GCM) session keys used in TLS connections.
5	TLS MAC keys	HMAC session keys (minimum HMAC-SHA-1/SHA-256/SHA-384) used in TLS connections.
6	SSH DH Private Components	Diffie-Hellman private component (≥ 224 bits).
7	SSH Session Encryption key	AES (128, 192, or 256 bit; CTR or CBC) session keys used in SSH connections.
8	SSH Session Authentication key	HMAC session keys (HMAC-SHA-1) used in SSH connections.
9	CO, User Password	Password for operator authentication (minimum 6 characters).
10	DRBG Seed and State	AES CTR DRBG used in the generation of random values.
11	SNMPv3 Secrets	SNMPv3 Authentication and Privacy Secrets

CSP #	Key/CSP	Description
12	SNMPv3 Keys	AES Session and HMAC-SHA-1 Authentication Keys

Table 12 - Public Keys

Key Name	Description
RSA Public Keys / CA Certificates	RSA Public keys managed as certificates for the verification of signatures, establishment of TLS (2048 bits).
ECDSA Public Keys / Certificates	ECDSA public keys managed as certificates for verification of signatures and establishment of TLS ECDSA P-256, P-384, or P-521
TLS DH Public components	Used in key agreement (DHE 2048, ECDHE P-256, P-384)
SSH DH Public components	Used in key agreement (2048 bits).
SSH Host RSA Public key	SSH Host Public Key (2048 bits).
Firmware Authentication Key	RSA key used to authenticate firmware (2048 bits).

Access Control Policy

1.6 Roles and Services

The Approved and non-Approved mode of operation provide identical services. While in the Approved mode of operation all authenticated services are accessed via SSH or TLS sessions. Approved and allowed algorithms, relevant CSPs and public keys related to these protocols are accessed to support the following services. CSP access by services is further described in the following tables.

The Crypto-Officer may access all services, and has the ability to define multiple Crypto-Officer roles. The User role provides read-only access to the system via the System Audit service.

Table 13 - Authenticated Services

CO Services	Description
System Operational Management	Perform system management functions including firmware updates, licensing, diagnostics and debug functions.
System Configuration Management	Presents configuration options for management interfaces and communication for peer services. Import, Export, Save, Load, revert and validate configurations and state. Define access control methods via admin role profiles, configure administrators/users, and password profiles. Configure operators and authentication profiles.
Data Analysis Management	Configure data submission, analysis and reporting functions.
Check Status	Review system, configuration, debug logs, and show configurations.
User services	**Description**
System Audit	Allows review of limited configuration and system status via logs, dashboard and configuration screens. Provides no configuration commit capability.

1.7 Unauthenticated Services

The cryptographic module supports the following unauthenticated services:

Table 14 - Unauthenticated Services

Service	Description
Zeroize	The device will overwrite all CSPs. The zeroization procedure is invoked when the operator performs a factory reset or exits out of the Approved mode of operation. The operator must be present to observe that the method has completed successfully or the operator must be in control of the module 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	View status of the module via the LEDs.
SNMP	SNMPv2c provides system status and information. There is neither read nor write access to CSPs.

1.8 CSP Access Rights

The following table defines the access to CSPs and the different module services. While in the Approved mode, all authenticated services and CSPs are accessed via authenticated TLS or SSH sessions. Approved and allowed algorithms, relevant CSPs, and public keys related to these protocols are used to access the services as listed in Table 15. The modes of access shown in the table are defined as:

R = Read: The module reads the CSP.

W = Write: The module writes the CSP. This write access is performed after a CSP is either imported into the module, generated by the module, or if the module overwrites an existing CSP.

Z = Zeroize: The module zeroizes the CSP.

Table 15 - CSP Access Rights within Roles and Services

Role	Authorized Service	Mode	CSP Access
CO	System Operational Management	RW	1, 2, 3, 4, 5, 6, 7, 8, 9
CO	System Configuration Management	RW	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12
CO	Data Analysis Management	RW	1, 2, 3, 4, 5, 6, 7, 8, 9
CO	Check Status	R	1, 6, 7, 8, 9
User	System Audit	R	1, 6, 7, 8, 9 (W possible for User Password only)

Unauthenticated	Zeroize	Z	All CSPs are zeroized.
Unauthenticated	Self-Tests	N/A	N/A
Unauthenticated	Show Status (LEDs)	N/A	N/A
Unauthenticated	SNMP	N/A	N/A

Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable. The operational environment is limited since the Module includes a firmware load service to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this module is out of the scope of this validation and require a separate FIPS 140-2 validation.

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 a 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 cryptographic module shall clear previous authentications on power cycle.
3. 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. AES GCM Encrypt Known Answer Test
            d. AES GCM Decrypt Known Answer Test
            e. AES CCM Encrypt Known Answer Test
            f. AES CCM Decrypt Known Answer Test
            g. RSA Sign Known Answer Test
            h. RSA Verify Known Answer Test
            i. ECDSA Sign Known Answer Test
            j. ECDSA Verify Known Answer Test
            k. DH Known Answer Test
            l. HMAC (HMAC-SHA-1/256/384) Known Answer Test
            m. SHA-1 Known Answer Test
            n. SHA-256 Known Answer Test
            o. SHA-384 Known Answer Test
            p. SHA-512 Known Answer Test
            q. DRBG Known Answer Test

r. ECDH Known Answer Test
s. SP 800-90A Section 11.3 Health Tests

B. Firmware Integrity Test – HMAC-SHA-256 and ECDSA P-256.
C. Critical Functions Tests
    1. N/A
D. Conditional Self-Tests
    1. Continuous Random Number Generator (RNG) test – performed on NDRNG and DRBG, 128 bits
    2. Firmware Load Test – Verify RSA 2048 signature on firmware at time of load
    3. RSA Pairwise Consistency Test

If any self-tests or conditional test fails, the module will output 'FIPS-CC failure' and the specific test that failed.

4. Power-up self-tests shall not require any operator action.
5. The operator shall be capable of commanding the module to perform the power-up self-test by power cycling the module.
6. Data output shall be inhibited during power-up self-tests and error states.
7. Processes performing key generation and zeroization processes shall be logically isolated from the logical data output paths.
8. The module does not output intermediate key generation values.
9. Status information output from the module shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
10. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
11. The module maintains separation between concurrent operators.
12. The module does not support a maintenance interface or role.
13. The module does not have any external input/output devices used for entry/output of data.
14. The module does not allow the input or output of plaintext CSPs.
15. The module provides a warning, "Your device is still configured with the default admin account credentials. Please change your password prior to deployment" to inform the operator to change their default authentication data.

Vendor imposed security rules:

16. If the cryptographic module remains inactive in any valid role for the administrator specified time interval, the module automatically logs out the operator.
17. 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.

Physical Security Policy

1.9 Physical Security Mechanisms

The multi-chip standalone module is production quality, and contains standard passivation. Chip components are protected by an opaque enclosure. There are tamper evident labels that are applied on the module by the Crypto-Officer, and any unused labels are to be controlled by the Crypto-Officer. The Crypto-Officer must ensure that the module surface is clean and dry before applying the labels. The labels prevent removal of the opaque enclosure without evidence, which should be inspected by the Crypto-Officer every 30 days for evidence of tamper. If the labels or opacity shields show evidence of tamper, the Crypto-Officer should assume that the module has been compromised and contact Customer Support.

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

Refer to Appendix A for instructions regarding installation of the tamper labels and opacity shields. Tamper evident labels must be pressed firmly onto the adhering surfaces during installation, and once applied, the Crypto-Officer shall permit 24 hours of cure time for all tamper evident labels. The placement of the twelve (12) tamper evident labels are shown in Appendix A.

1.10 Operator Required Actions

Table 16 - Inspection/Testing of Physical Security Mechanisms

Model	Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
WF-500	Tamper Evident Labels	30 days	Verify integrity of tamper evident labels in the locations specified in Appendix A.
WF-500	Front and Rear Opacity Shields	30 days	Verify that the front and rear opacity shields have not been deformed from their original shape, thereby reducing their effectiveness.
WF-500	Vent Overlays	30 days	Verify that the vent overlays have not been removed or deformed. All edges should maintain strong adhesion characteristics.

Mitigation of Other Attacks

These requirements are not applicable as the module has not been designed to mitigate any specific attacks outside of the scope of FIPS 140-2.

References

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

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
NDRNG – Non-Deterministic Random Number Generator
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

Appendix A – WF-500 FIPS Kit Installation Guide (12 Tamper Evident Labels)

Step 1:

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

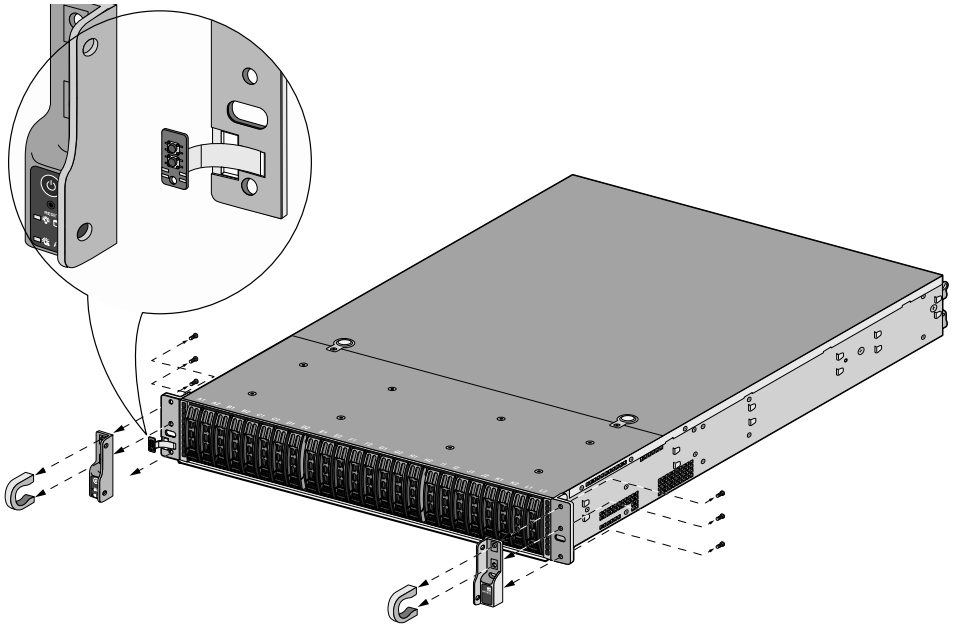

Figure 8 – Remove Front Handles and Modules

Step 2:

Attach the left and right front cover brackets to the appliance using the six screws that you removed in Step 1. First attach the brackets using the bottom screws (one on each side) as shown in Figure 9, 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 10.

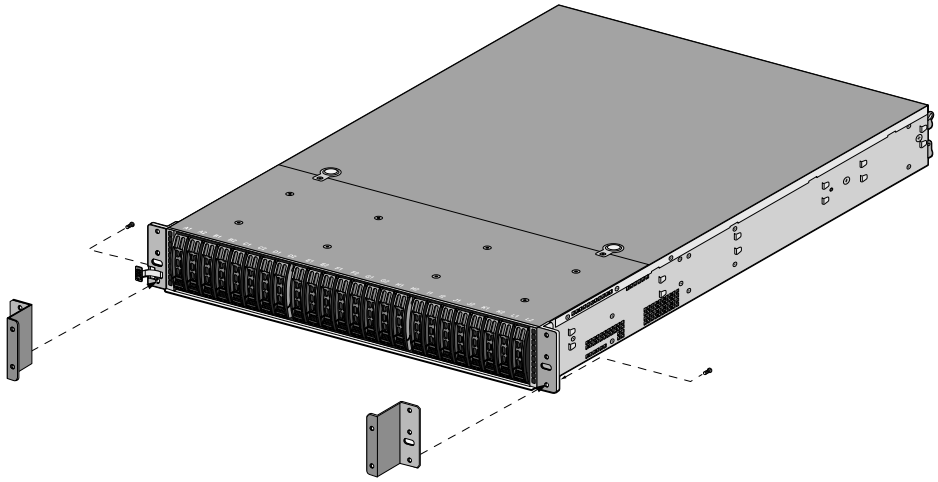

Figure 9 – Secure the Front Brackets

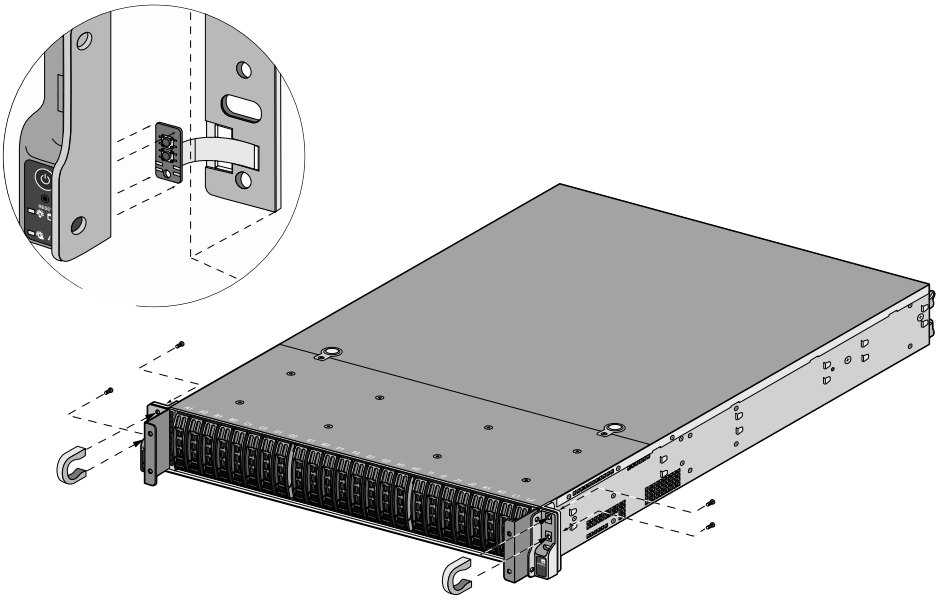

Figure 10 - Attach Pull Handles and Front Modules

Step 3:

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

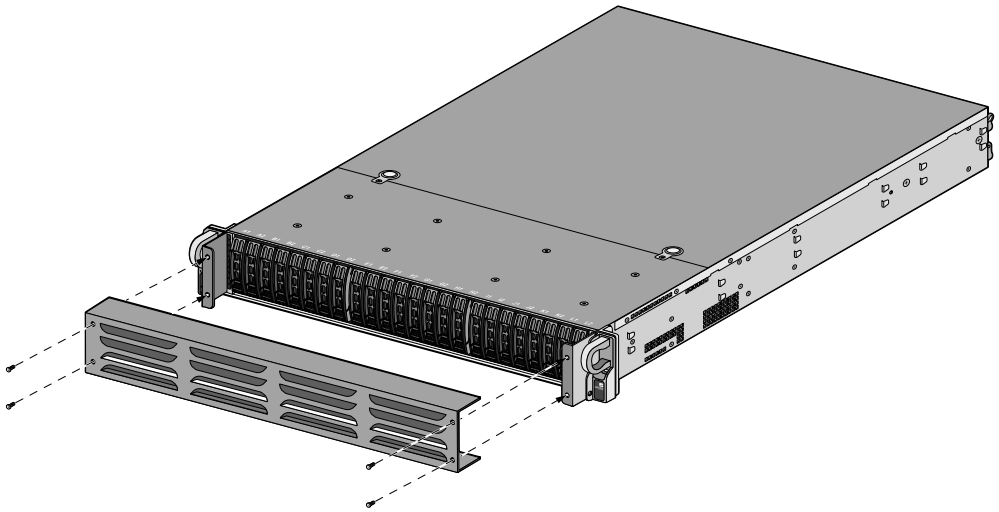

Figure 11 – Install Front Opacity Shield

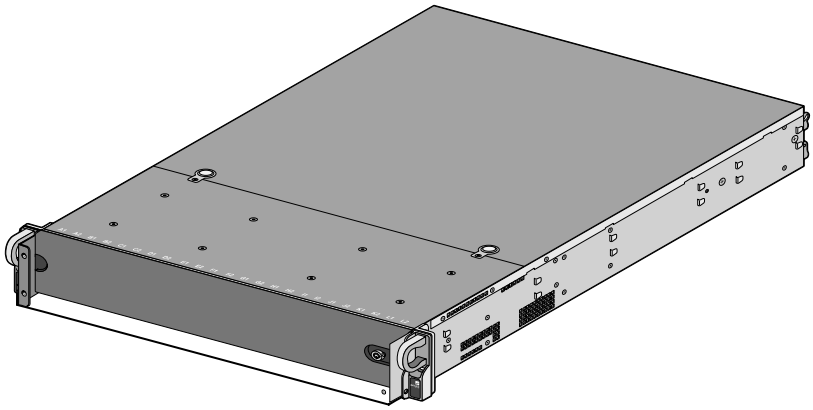

Figure 12 – Front Opacity Shield Installed

Step 4:

Attach the rear opacity shield tray to the appliance. First, remove the two screws (shown in Figure 13) 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.

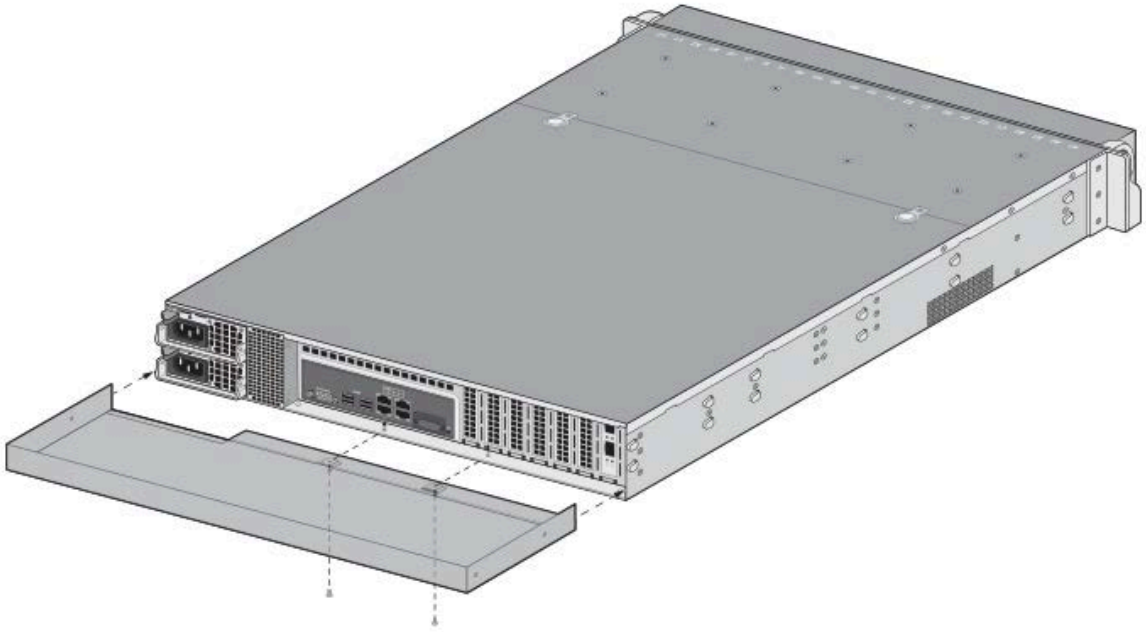

Figure 13 – Install Rear Opacity Shield Tray

Step 5:

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

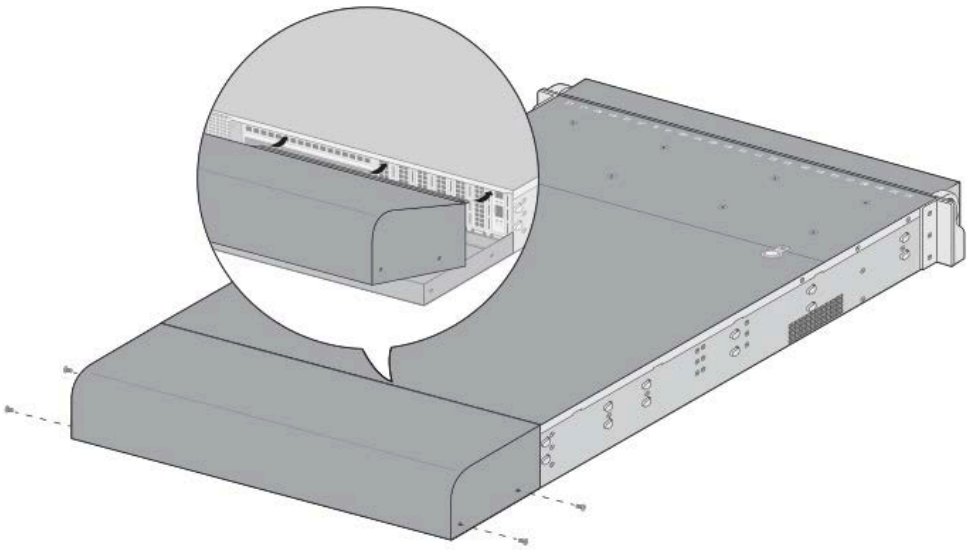

Figure 14 – Install Rear Opacity Shield

Step 6:

Cover the vent openings as shown in Figure 15 by applying one overlay sticker over the left side vent and one overlay sticker over the right side vent. Each overlay requires two tamper labels as shown in Figure 16. Also apply one additional tamper label as shown in Figure 16 Item 5.

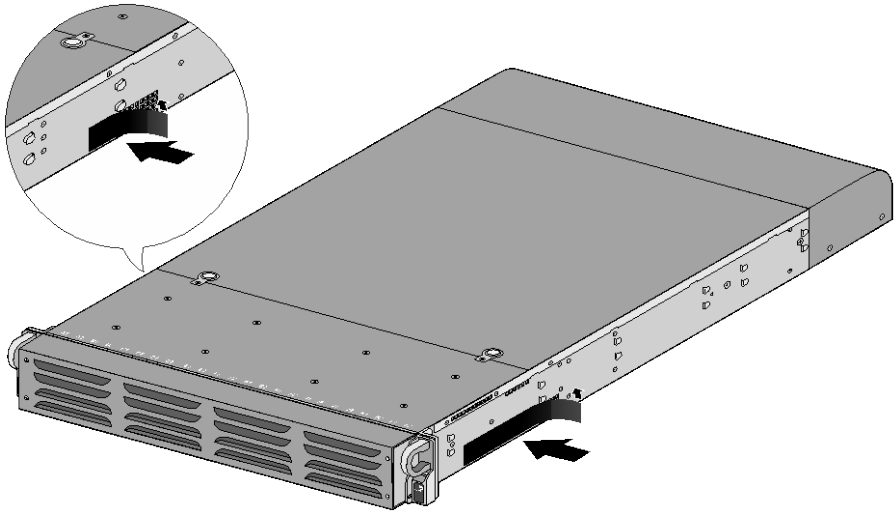

Figure 15 – Apply Vent Overlays

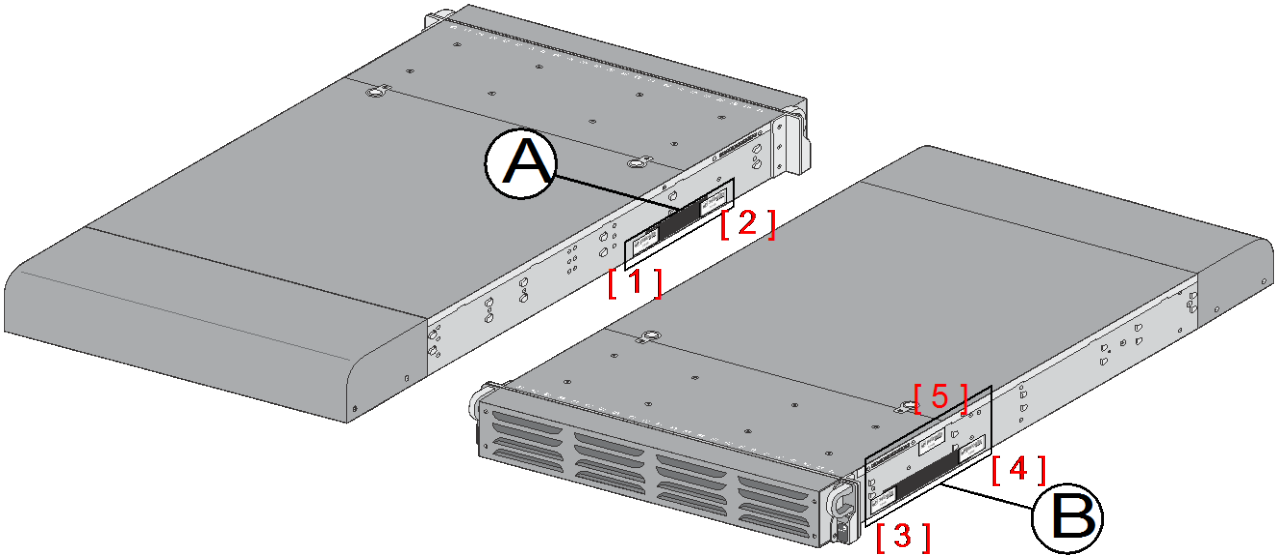

Figure 16 – Apply Tamper Labels on Vent Overlays and Side Opening

Step 7:

Attach the rail kit to the appliance as shown in Figure 17 and then add three tamper labels to the bottom of the appliance as shown in Figure 18. One tamper label prevents tampering of the front opacity shield connected to the bottom of the appliance and two tamper labels wrap around the upper and lower rear opacity shields to prevent tampering of the rear opacity shields.

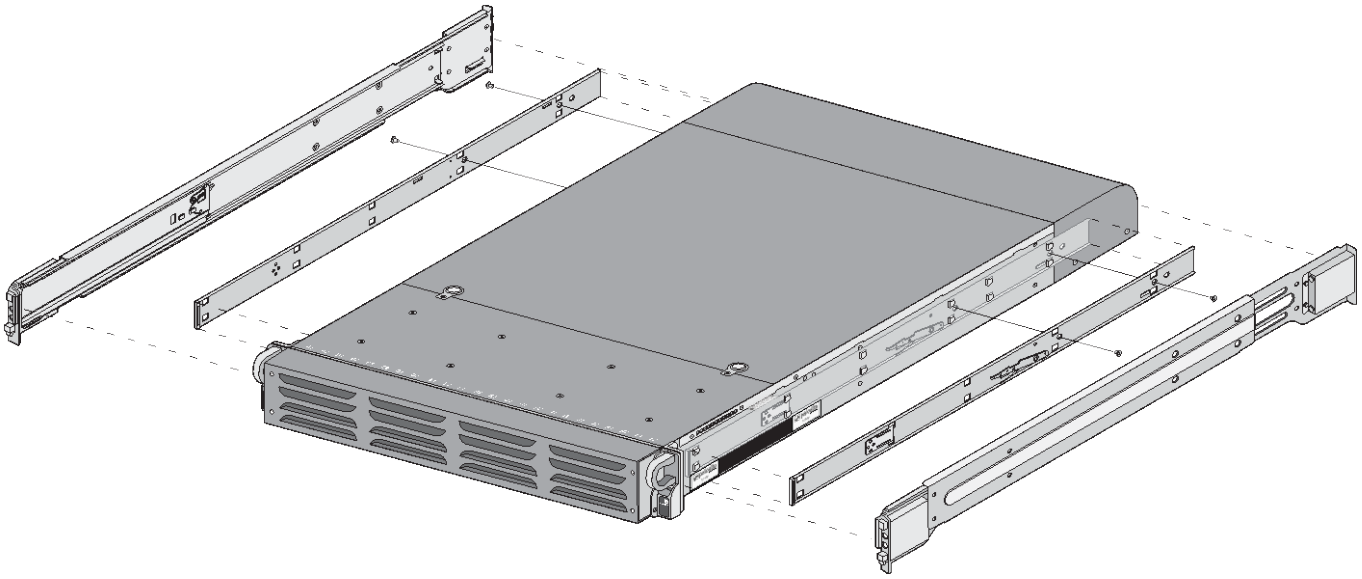

Figure 17 – Install Rail Kit

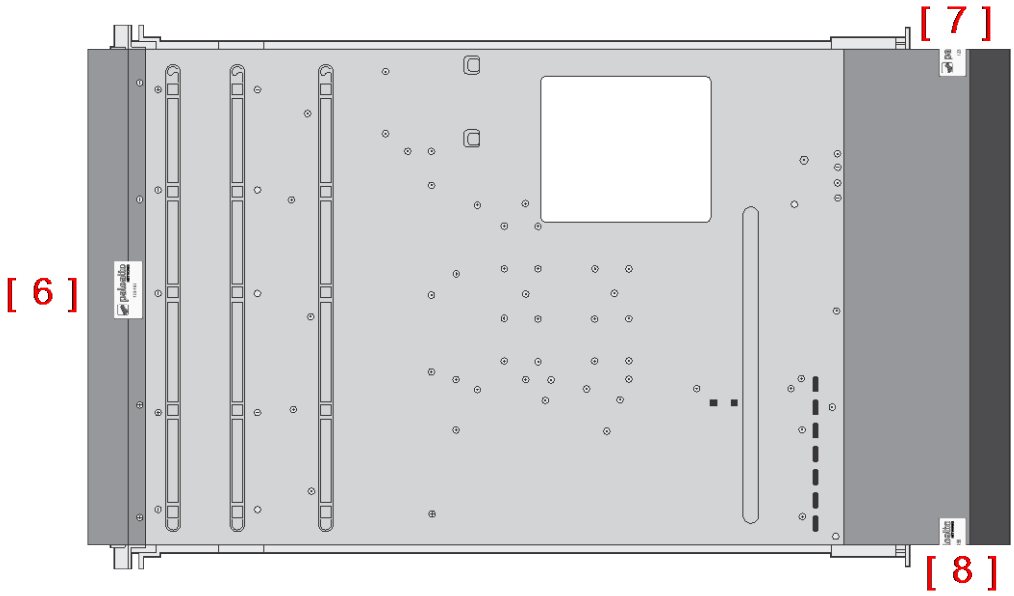

Figure 18 – Apply Tamper Labels on the Bottom of the Appliance

Step 8:

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

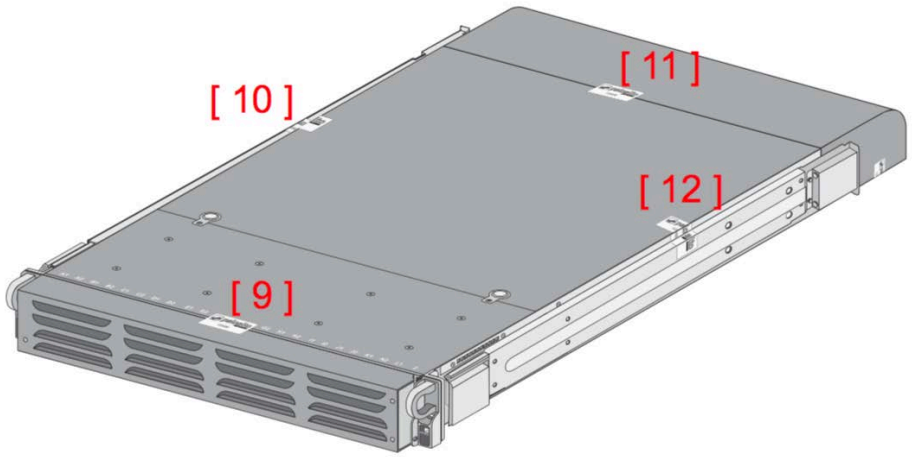

Figure 19 – Apply Tamper Labels on the Top and Sides of the Appliance