

WildFire WF-500

FIPS 140-2

Non-Proprietary Security Policy

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

Date: 6/5/2019

www.paloaltonetworks.com © 2019 Palo Alto Networks. Non-proprietary security policy may be reproduced only in its original entirety (without revision). Palo Alto Networks, PAN-OS, and WildFire are trademarks of Palo Alto Networks, Inc. All other trademarks are the property of their respective owners.

1 Change Record

Table 1 - Change Record

Date	Author	Description of Change
12/12/2018	A. Shahhosseini	initial authoring
6/5/2019	A. Shahhosseini	Updates in response to CMVP comments

2 Contents

1. Change Record.....	2
2. 2	
3. Contents	3
4. Tables.....	4
5. Figures	4
6. 5	
7. Module Overview	6
8. Mode of Operation	8
1.1 Security Levels.....	8
1.2 FIPS 140-2 Approved Mode of Operation	8
1.3 Approved and Allowed Algorithms	10
1.4 Non-Approved, Non-Allowed Algorithms	13
9. Ports and Interfaces.....	15
10. Identification and Authentication Policy	16
1.5 Assumption of Roles	16
11. Security Parameters	17
12. Access Control Policy	20
1.6 Roles and Services.....	20
1.7 Unauthenticated Services	21
1.8 CSP Access Rights.....	21
13. Operational Environment	22
14. Security Rules	22
1.9 Physical Security Mechanisms	25
1.10 Operator Required Actions	25
15. Mitigation of Other Attacks	26
16. References	26
17. Definitions and Acronyms	26
18. Appendix A – WF-500 FIPS Kit Installation Guide (12 Tamper-Evident Seals).....	27

3 Tables

Table 1 - Change Record	2
Table 2 - Validated Version Information.....	6
Table 3 - Module Security Level Specification	8
Table 4 – CAVP Certificates for FIPS Approved Algorithms	10
Table 5 – FIPS Allowed Algorithms Used in the Approved Mode.....	13
Table 6 - Supported Protocols in the Approved Mode	13
Table 7 - Non-Approved, Non-Allowed Algorithms Used in the Non-Approved Mode	14
Table 8 – WF-500 Ports and Interfaces.....	15
Table 9 – Roles and Authentication	16
Table 10 - Strength of Authentication Mechanism	17
Table 11 - Private Keys and CSPs	17
Table 12 - Public Keys	19
Table 13 - Authenticated Services	20
Table 14 – Unauthenticated Services	21
Table 15 – CSP and Public Key Access Rights within Roles and Services	21
Table 16 - Inspection/Testing of Physical Security Mechanisms	25

4 Figures

Figure 1 – Front View of WF-500	6
Figure 2 - Front View of WF-500 with Opacity Shield.....	6
Figure 3 - Rear View of WF-500 with Opacity Shield	7
Figure 4 - Right Side of WF-500 with Opacity Shields.....	7
Figure 5 - Left Side of WF-500 with Opacity Shields.....	7
Figure 6 - Front ports and Interfaces	15
Figure 7 - Rear ports and Interfaces	15
Figure 8 – Remove Front Handles and Modules.....	27
Figure 9 – Secure the Front Brackets.....	28
Figure 10 - Attach Pull Handles and Front Modules	28
Figure 11 – Install Front Opacity Shield	29
Figure 12 – Front Opacity Shield Installed	29
Figure 13 – Install Rear Opacity Shield Tray	30
Figure 14 – Install Rear Opacity Shield	31
Figure 15 – Apply tamper-evident Seals on Vent Overlays	32
Figure 16 – Apply tamper-evident Seals on Vent Overlays and Side Opening	32
Figure 17 – Install Rail Kit.....	33
Figure 18 – Apply tamper-evident seals on the Bottom of the Appliance	33

Figure 19 – Apply tamper-evident seals on the Top and Sides of the Appliance34

1 Module Overview

The WildFire WF-500 module 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 8.1 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	920-000145	00A	8.1.6



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 Side of WF-500 with Opacity Shields



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

2 Mode of Operation

2.1 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	2
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

2.2 FIPS 140-2 Approved Mode of Operation

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

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

- Install module and interface connections in addition to the FIPS kit.
- The tamper-evident seals 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.

2.3 non-Approved Mode of Operation

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

- Access the module’s CLI via SSH, and command the module to enter maintenance mode; the module will reboot
 - Note: Establish a serial connection to the console port
- After reboot, select “Continue.”
- Select the “Set FIPS-CC” option, and press enter.
- Select “Disable FIPS-CC Mode”, and press enter.
- The module will disable FIPS-CC mode, and perform a factory reset (zeroization)
- Once complete, the module will provide the following status output:
 - “Set FIPS-CC Mode Status: Success”

The following procedure will zeroize the module:

- Access the module’s CLI via SSH, and command the module to enter 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”

2.4 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 [FIPS 197, SP800-38A]: Functions: Encryption, Decryption ECB, CBC, CTR modes; Encrypt/Decrypt; 128, 192 and 256-bit CFB128 mode; Encrypt/Decrypt; 128-bit Note: AES-OFB, AES-CFB1, AES-CFB8 and AES-CFB128 (192, 256 bit) were also tested but are not available for use.	5890
AES-CCM [SP800-38C]: Encrypt and Decrypt, 128-bit Note: AES-CCM was tested but is not used by the module except for the self-test.	5890
AES-GCM [SP800-38D]: Encrypt and Decrypt, 128 and 256-bit Functions: Authenticated Encryption, Authenticated Decryption Note 1: GCM IV handling is compliant with FIPS IG A.5 and SP800-38D.* Note 2: GCM 192-bit was tested but is not used by the module.	5890
CKG [SP800-133]: Function: Key Generation Method 1: Asymmetric Key Generation; SP800-133 §6, seed results from an unmodified DRBG output Method 2: Symmetric Key Generation; SP800-133 §7.1 (symmetric key results from an unmodified DRBG output), §7.2, and §7.3	Vendor Affirmed
CVL: ECDSA Signature Generation <ul style="list-style-type: none"> • P-256 SHA: SHA-224, SHA-256, SHA-384, SHA-512 • P-384 SHA: SHA-224, SHA-256, SHA-384, SHA-512 Note: P-224 was tested, but not used by the module	2122
CVL: Elliptical Curve Diffie-Hellman Exchange [SP800-56A] -ECC CDH Primitive (Section 5.7.1.2) Curves: P-256, P-384, P-521 -KAS-ECC all except KDF Curves: P-256, P-384, P-521	2119
CVL: Diffie-Hellman Exchange [SP800-56A] KAS-FFC all except KDF Parameter Sets: FB and FC	2119
CVL: KDF, Application Specific [SP800-135] -TLSv1.0/1.1/1.2 KDF -SNMPv3 KDF -SSHv2 KDF	2120

FIPS Approved Algorithm	CAVP Cert. #
-IKEv2 KDF Note: IKEv1 KDFs were tested, but are not used by the module.	
CVL: RSA [SP800-56B] Functions: Key Transport -RSADP	2121
DRBG [SP800-90A] -CTR DRBG with AES-256 Derivation function enabled	2451
DSA [FIPS 186-4] -Key Generation: 2048 bits -Prerequisite to CVL #2119	1485
ECDSA [FIPS 186-4] -Key Pair Generation: P-256, P-384, P-521 -Public Key Validation: P-256, P-384, P-521 -Signature Generation: P-256, P-384, and P-521 with hashes (SHA-256/384/512) -Signature Verification: P-256, P-384, and P-521 with hashes (SHA-1/256/384/512) Note: P-224 was tested, but not used by the module	1570
HMAC [FIPS 198] - HMAC-SHA-1 with $\lambda=96, 160$ - HMAC-SHA-256 with $\lambda=256$ - HMAC-SHA-384 with $\lambda=384$ - HMAC-SHA-512 with $\lambda=512$	3865
KAS: SP 800-56A Rev.2 Diffie-Hellman Exchange (CVL Certs. #2119 and #2120, vendor affirmed; key agreement; key establishment methodology provides 112 bits of encryption strength)	Vendor Affirmed
KAS: SP 800-56A Rev.2 Elliptic Curve Diffie-Hellman Exchange (CVL Certs. #2119 and #2120, vendor affirmed; key agreement; key establishment methodology provides between 128 and 256 bits of encryption strength)	Vendor Affirmed
KTS [SP800-38F §3.1]: AES-GCM	AES 5890

FIPS Approved Algorithm	CAVP Cert. #
(Key wrapping; key establishment methodology provides 128 bit or 256 bits of encryption strength)	
KTS [SP800-38F §3.1]: AES-CBC (128/192/256 bits) plus HMAC AES-CTR (128/192/256 bits) plus HMAC (Key wrapping; key establishment methodology provides between 128 bit and 256 bits of encryption strength)	AES 5890 HMAC 3865
RSA [FIPS 186-4] - Key Pair Generation: 2048 and 3072 - Signature Generation (ANSI X9.31, RSASSA-PKCS1_v1-5, RSASSA-PSS): 2048, 3072, and 4096-bit with hashes (SHA-1 ⁺ /256/384/512) - Signature Verification (ANSI X9.31, RSASSA-PKCS1_v1-5, RSASSA-PSS): 1024 ⁺⁺ , 2048, 3072, 4096-bit (per IG A.14) with hashes (SHA-1/224 ⁺⁺⁺ /256/384/512) ⁺ : Only used for signature generation in SSH in the Approved Mode ⁺⁺ : This size is not supported for RSASSA-PKCS1_v1-5 ⁺⁺⁺ : This Hash algorithm is not supported for ANSI X9.31	3086
SHA-1, SHA-256, SHA-384, SHA-512 [FIPS 180-4] Functions: Digital Signature Generation, Digital Signature Verification, non-Digital Signature Applications (Note: SHA-224 was tested, but is not used by the module)	4641

* The module is compliant to IG A.5: GCM is used in the context of TLS, IPsec/IKEv2, SSH, and IPsec/IKEv1:

- For TLS, The GCM implementation meets Option 1 of IG A.5: it is used in a manner compliant with SP 800-52 and in accordance with Section 4 of RFC 5288 for TLS key establishment. (From this RFC, the GCM cipher suites in use are TLS_RSA_WITH_AES_128_GCM_SHA256, TLS_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, and TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384.) During operational testing, the module was tested against an independent version of TLS and found to behave correctly.
- For IPsec/IKEv2, The GCM implementation meets Option 1 of IG A.5: it is used in a manner compliant with RFCs 4106 and 7296 (RFC 5282 is not applicable, as the module does not use GCM within IKEv2 itself). During operational testing, the module was tested against an independent version of IPsec with IKEv2 and found to behave correctly.
- For SSH, the module meets Option 4 of IG A.5. The fixed field is 32 bits in length and is derived using the SSH KDF; this ensures the fixed field is unique for any given GCM session. The invocation field is 64 bits in length and is incremented for each invocation of GCM; this prevents the IV from repeating until the entire invocation field space of 2⁶⁴ is exhausted. (It would take hundreds of years for this to occur.)

In all of the above cases, the nonce_explicit is always generated deterministically. AES GCM keys are zeroized when the module is power-cycled. For each new TLS or SSH session, a new AES GCM keys is established.

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, non-compliant to SP800-56A [safe primes: L=2048, N=2047] (key agreement; key establishment methodology provides 112 bits of encryption strength)
CMAC – A self-test is performed for this algorithm, but it is not used by the module.
MD5 (within TLS)
Non-Approved NDRNG (used to seed DRBG) This provides a minimum of 256 bits of entropy.
RSA (CVL Cert. #2121, key wrapping; key establishment methodology provides 112 or 128 bits of encryption strength)

Table 6 - Supported Protocols in the Approved Mode

Supported Protocols*
TLSv1.0 ¹ , v1.1 and v1.2
SSHv2
SNMPv3
IPsec and IKEv2

(*): These protocols have not been tested or reviewed by the CMVP or the CAVP.

2.5 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.

¹ See vendor imposed security rule #1.A in Section 8

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

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

3 Ports and Interfaces

The WF-500 provides the following ports and interfaces:

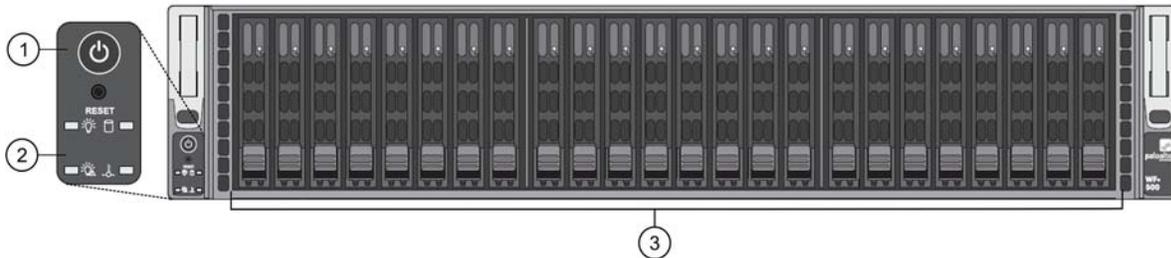


Figure 6 - Front Ports and Interfaces

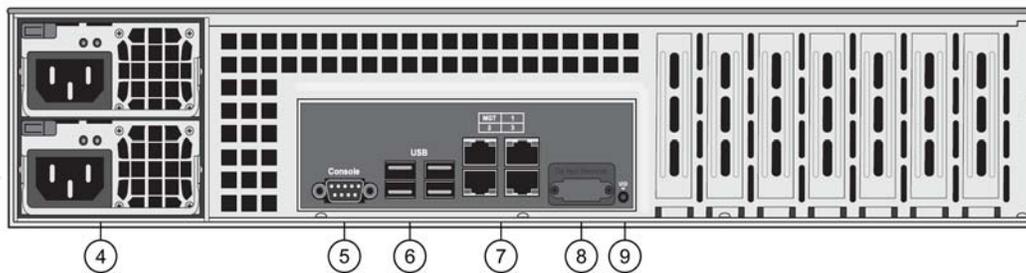


Figure 7 - Rear Ports and Interfaces

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 (<i>Note: In the Approved mode, the Console port is only available as Status output</i>)	1	Data input, Control input, Data output, Status output
6	USB	Disabled except for power	4	Disabled except for power
7	RJ45	MGT Ethernet 10/100/1000	1	Data input, Control input, Data output, Status output

Interface		Name and Description	Qty.	FIPS 140-2 Designation
		Ethernet 1	1	Data input, Data output
		Ethernet 2 and 3	2	Data input, Data output
8	VGA	Graphic port (<i>Note: Reserved for future use</i>)	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

4 Identification and Authentication Policy

4.1 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 and/or Public Key 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 Public Key Authentication
Peer-to-peer VPN	Peer to peer VPN session for cluster.	Identity-based operator authentication	Certificate based authentication

Table 10 - Strength of Authentication Mechanism

Authentication Mechanism	Strength of Mechanism
Username and Password	<p>The minimum length of a password is six (6) characters (95 possible characters). The probability that a random attempt will succeed or a false acceptance will occur is $1/(95^6)$, which is less than $1/1,000,000$.</p> <p>The module supports a maximum of 10 failed attempts to authenticate into the module in a one (1) minute period. If the maximum number of attempts is reached, the operator is locked out for a configurable time period (one (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 $1/100,000$.</p>
Certificate/Public Key based authentication	<p>The module supports authentication using RSA 2048, 3072, 4096 bits or ECDSA P-256/P-384/P-521.</p> <p>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 (1) minute period is $6,000/(2^{112})$, which is less than $1/100,000$. The device supports up to 100 new sessions per second.</p>

5 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/ECDSA Private keys	Private keys support establishment of TLS, IPsec/IKE, and SSH host authentication. (RSA 2048, 3072, or 4096 bits; ECDSA P-256, P-384, or P-521)
2	TLS ECDHE/DHE Private Components	Diffie-Hellman private component (DH (L=2048, N >=224), (ECDHE P-256, P-384, P-521))
3	TLS Pre-Master Secret	Secret value used to derive the TLS Master Secret along with client and server random nonces
4	TLS Master Secret	Secret value used to derive the TLS session keys

CSP #	Key/CSP	Description
5	TLS Encryption keys	AES (128 or 256 bit; CBC or GCM) session keys used in TLS connections.
6	TLS HMAC keys	HMAC session keys (HMAC-SHA-1/SHA-256/SHA-384) used in TLS connections.
7	SSH ECDH/DH Private Components	ECDH and Diffie-Hellman private component (DH 2048 bits, ECDH P-256, P-384, P-521)
8	SSH Session Encryption key	AES session keys used in SSH connections. (128, 192, or 256 bits; CBC, CTR) (128 or 256 bits: GCM)
9	SSH Session Authentication key	HMAC session keys used in SSH connections. (HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-512)
10	CO, User Password	Password for operator authentication (minimum 6 characters).
11	DRBG Seed and State	DRBG seed coming from the NDRNG and AES 256 CTR DRBG state (V and Key) used in the generation of a random values
12	SNMPv3 Secrets	SNMPv3 Authentication and Privacy Secrets
13	SNMPv3 Keys	AES Session and HMAC-SHA-1 Authentication Keys
14	IPSec/IKE Diffie-Hellman Private Components	Diffie-Hellman (Group 14) private components
15	IPSec/IKE EC Diffie-Hellman Private Components	EC Diffie-Hellman (Group 19, 20) private components
16	IPSec/IKE Session Keys	Encryption keys for session (128 or 256 bits: AES GCM or CBC)
17	IPSec/IKE Authentication Keys	HMAC keys for authentication (HMAC-SHA-256/384/512)
18	RADIUS Secret	Secret used by RADIUS (minimum length of six (6) characters)

Table 12 - Public Keys

Key	Key Name	Description
A	RSA Public Keys / CA Certificates	RSA Public keys managed as certificates for the verification of signatures, establishment of TLS. (RSA 2048 bit minimum)
B	ECDSA Public Keys / CA Certificates	ECDSA public keys managed as certificates for verification of signatures and establishment of TLS. (ECDSA P-256, P-384, or P-521)
C	TLS ECDHE/DHE Public components	Used in key agreement. (DHE 2048, ECDHE P-256, P-384, P-521)
D	SSH ECDH/DH Public components	Used in key agreement. (2048 bits, P-256, P-384, P-521)
E	SSH Client RSA Public Key	Public key used to authenticate client. (RSA 2048, 3072, or 4096 bits)
F	SSH Host RSA/ECDSA Public key	SSH Host Public Key used to authenticate the host. (RSA 2048, 3072, or 4096 bits; ECDSA P-256, P-384, or P-521)
G	Firmware Authentication Key	RSA key used to authenticate firmware (2048 bits)
H	Firmware Integrity Check Key	Used to check the integrity of the crypto-related code (HMAC-SHA-256* and ECDSA P-256) *Keys used to perform power-up self-tests are not CSPs as per IG 7.4
I	IPSec /IKE Diffie-Hellman Public Components	Diffie-Hellman (Group 14) public components.
J	IPSec /IKE EC Diffie-Hellman Public Components	Diffie-Hellman (Group 19, 20) public components.

6 Access Control Policy

6.1 Roles and Services

The Approved and non-Approved mode of operation provide identical services. While in the Approved mode of operation all authenticated services 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. The Peer-to-Peer VPN role consists in managing the establishment of VPN connections between several WildFire WF-500 modules.

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	<p>Presents configuration options for management interfaces and communication for peer services.</p> <p>Import, Export, Save, Load, revert and validate configurations and state.</p> <p>Define access control methods via admin role profiles, configure administrators/users, and password profiles.</p> <p>Configure operators and authentication profiles</p>
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.
Peer-to-Peer VPN Services	Description
IKE/IPsec configuration	Configuring IKE/IPsec setup for peer to peer VPN.

6.2 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 hardware status of the module via the LEDs.
SNMP	SNMPv2c provides system status and information. There is neither read nor write access to CSPs.

6.3 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. The read access is performed when a CSP is either exported from the module or executed by a security function.

W = Write: The module writes the CSP. The 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 and Public Key Access Rights within Roles and Services

Role	Authorized Service	CSP Access (from Tables 11 & 12)
CO	System Operational Management	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 14, 15, 16, A, B, C, D, E, F, G, H, H, I, J – RW

		F, H – R
CO	System Configuration Management	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, F, G – RW
CO	Data Analysis Management	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 – RW
CO	Check Status	1, 7, 8, 9, 10, 11 – R
User	System Audit	1, 7, 8, 9, 10, 11 – R (W possible for User Password only)
Peer to Peer VPN	IKE/IPsec configuration	1, 11, 14, 15, 16, 17, A, B, I, J – RW
Unauthenticated	Zeroize	All CSPs are zeroized.
Unauthenticated	Self-Tests	H - R
Unauthenticated	Show Status (LEDs)	N/A
Unauthenticated	SNMP	N/A

7 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.

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 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 CMAC Known Answer Test

- d. AES GCM Encrypt Known Answer Test
 - e. AES GCM Decrypt Known Answer Test
 - f. AES CCM Encrypt Known Answer Test
 - g. AES CCM Decrypt Known Answer Test
 - h. RSA Sign Known Answer Test
 - i. RSA Verify Known Answer Test
 - j. RSA Encrypt Known Answer Test
 - k. RSA Decrypt Known Answer Test
 - l. ECDSA Sign Known Answer Test
 - m. ECDSA Verify Known Answer Test
 - n. DH Known Answer Test
 - o. HMAC (HMAC-SHA-1/256/384/512) Known Answer Test
 - p. SHA-1 Known Answer Test
 - q. SHA-256 Known Answer Test
 - r. SHA-384 Known Answer Test
 - s. SHA-512 Known Answer Test
 - t. DRBG Known Answer Test
 - u. ECDH Known Answer Test
 - v. 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
 - 4. ECDSA Pairwise Consistency Test
 - 5. If any conditional test fails, the module will output description of the error.

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 one (1) minute before any more login attempts can be attempted.
18. In FIPS-CC mode, the following rules shall apply:
 - A. The operator should not enable TLSv1.0; it is disabled by default.
Note that TLSv1.0 can be used in an Approved mode of operation (Approved TLS KDF algorithm); however, TLSv1.0 protocol is no longer considered as secure because of the Cipher Block Chaining IV attack, a client of the module could use a vulnerable implementation.
 - B. If using RADIUS, it must be configured using TLS. If RADIUS without TLS protocol is set, the module shall be configured in non-Approved mode of operation.
 - C. The operator shall not generate 4096-bit RSA key in FIPS-CC mode. If the operator wants to generate 4096-bit RSA key, the module shall be configured in non-Approved mode of operation.
 - D. Physical Security Policy

8.1 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 seals that are applied on the module by the Crypto-Officer, and any unused seals are to be controlled by the Crypto-Officer. The Crypto-Officer must ensure that the module surface is clean and dry before applying the seals. The seals 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 seals 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 version. Opacity shields are included in the FIPS kits.

Refer to Appendix A for instructions regarding installation of the tamper seals and opacity shields. 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 placement of the twelve (12) tamper-evident seals are shown in Appendix A.

8.2 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 Seals	30 days	Verify integrity of tamper-evident seals 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.

9 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.

10 References

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

11 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

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

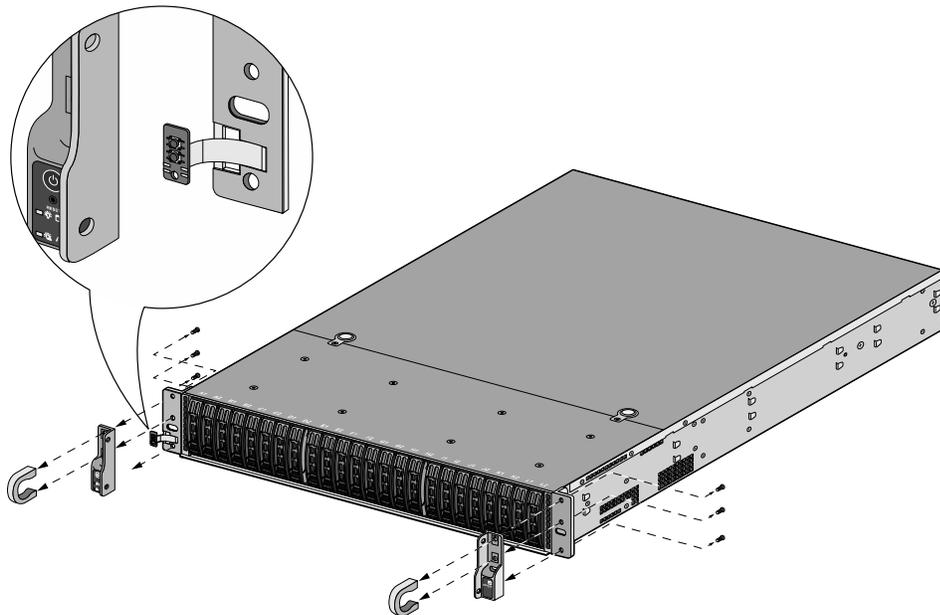


Figure 8 – Remove Front Handles and Modules

Step 2:

Attach the left and right front cover brackets to the appliance using the six (6) screws that were removed in Step 1. First attach the brackets using the bottom screws (one (1) 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.

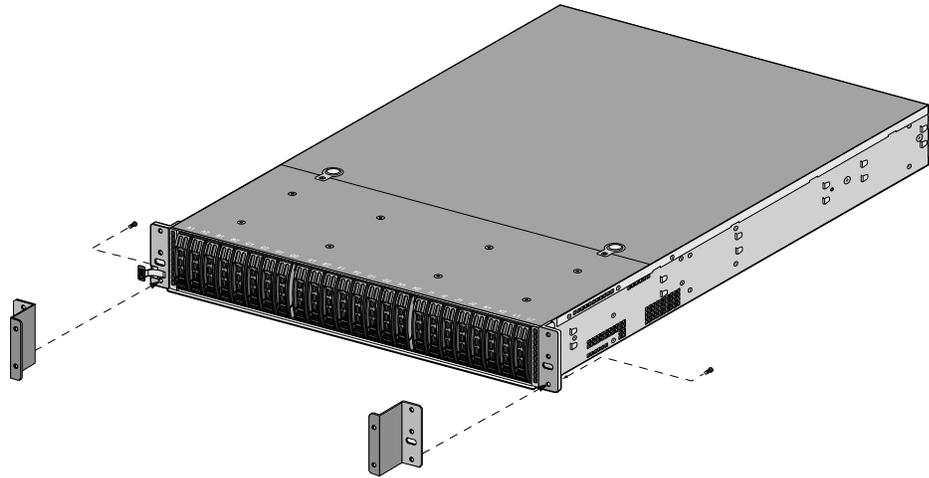


Figure 9 – Secure the Front Brackets

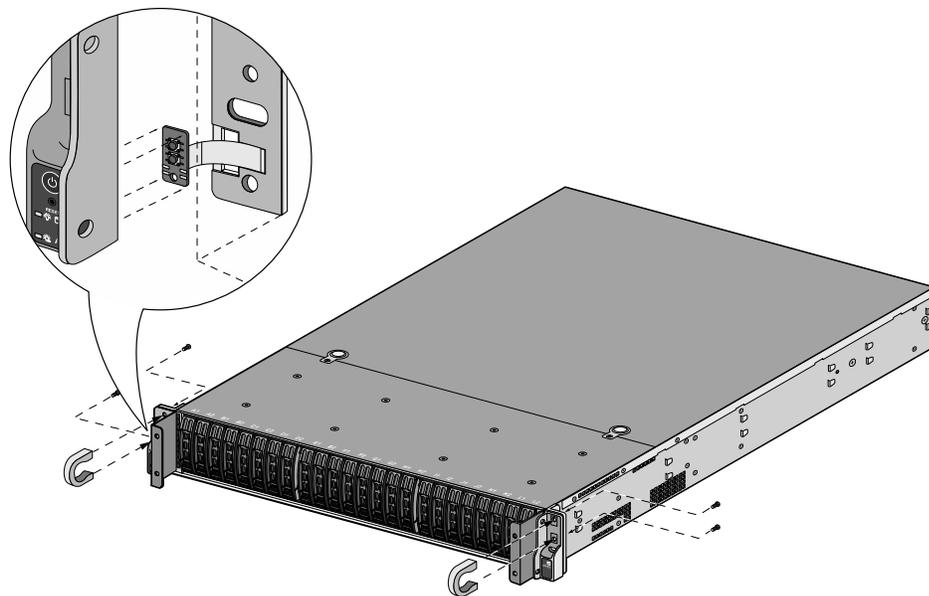


Figure 10 - Attach Pull Handles and Front Modules

Step 3:

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

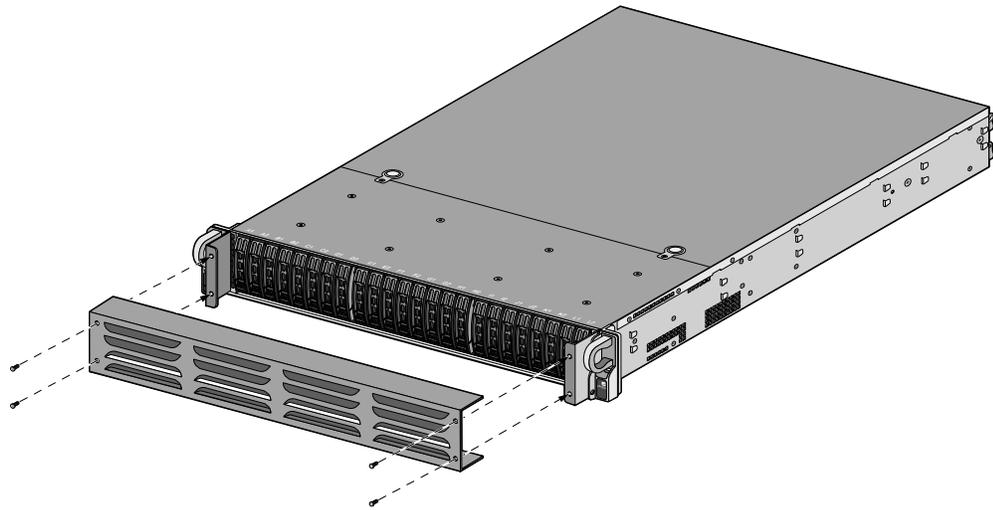


Figure 11 – Install Front Opacity Shield

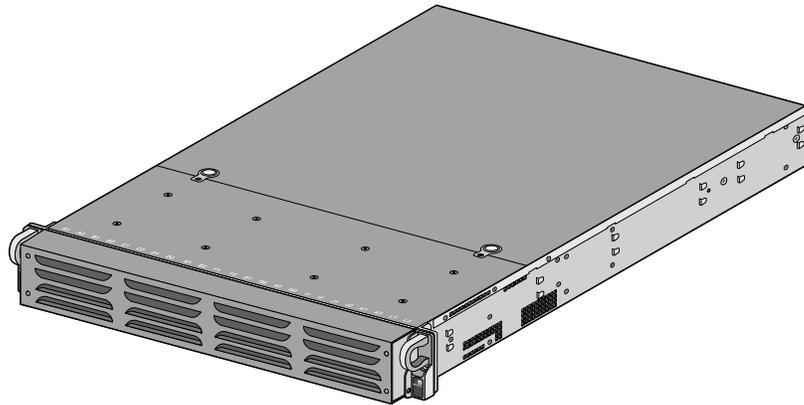


Figure 12 – Front Opacity Shield Installed

Step 4:

Attach the rear opacity shield tray to the appliance. First, remove the two (2) 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.

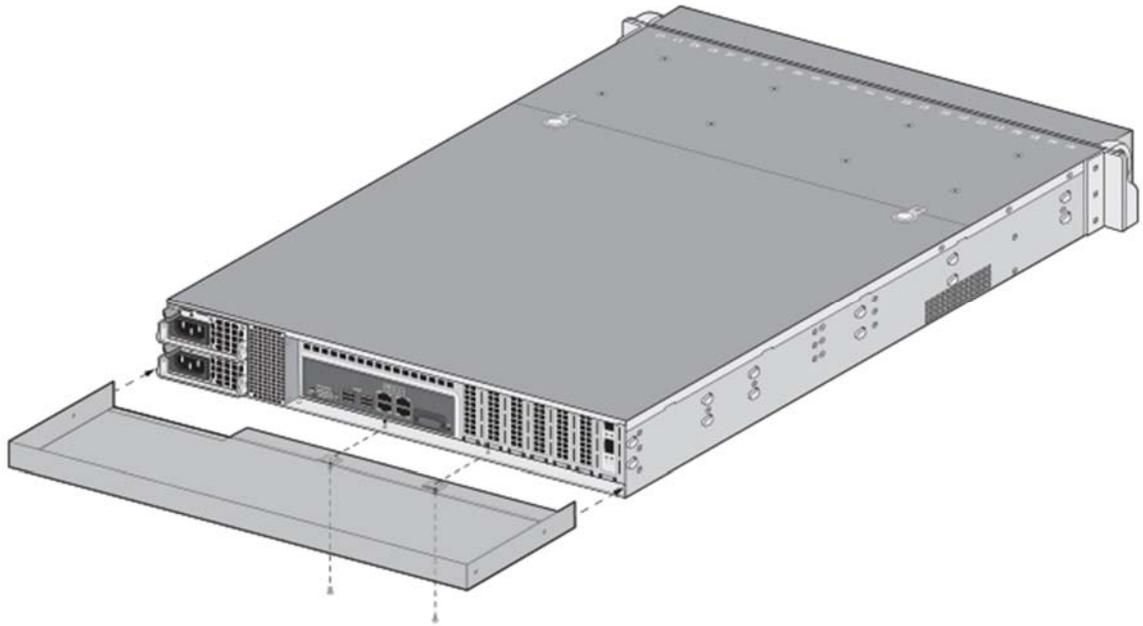


Figure 13 – Install Rear Opacity Shield Tray

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 (2) screws (provided) on each side.

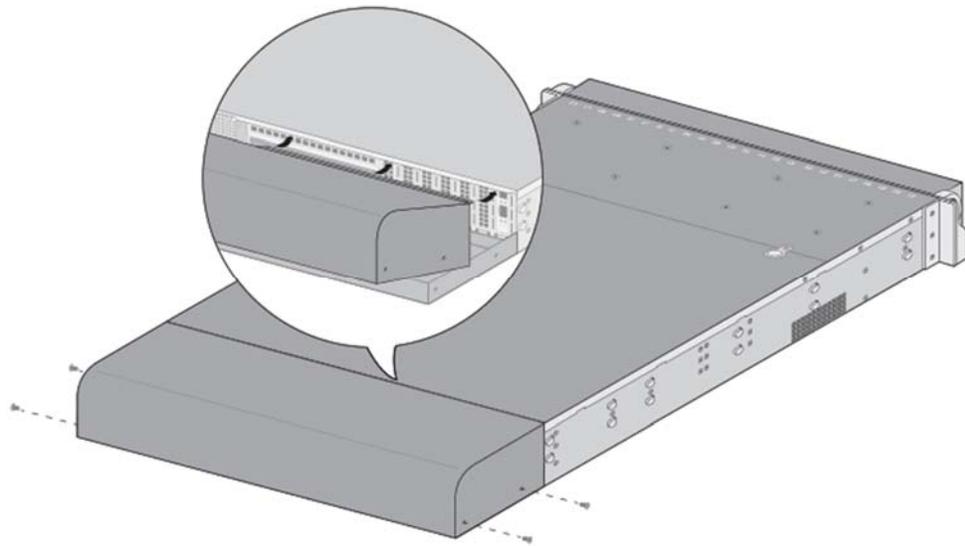


Figure 14 – Install Rear Opacity Shield

Step 6:

Cover the vent openings as shown in Figure 15 by applying one (1) overlay tamper-evident seal over the left side vent and one overlay tamper-evident seal over the right side vent. Each overlay requires two (2) tamper-evident seals as shown in Figure 16. Also apply one (1) additional tamper-evident seal as shown in Figure 16, #5.

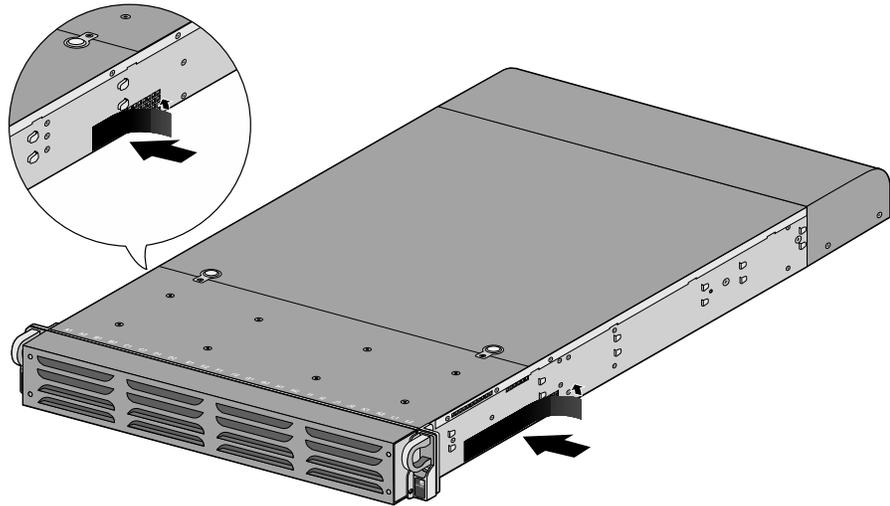


Figure 15 – Apply Tamper-Evident Seals on Vent Overlays

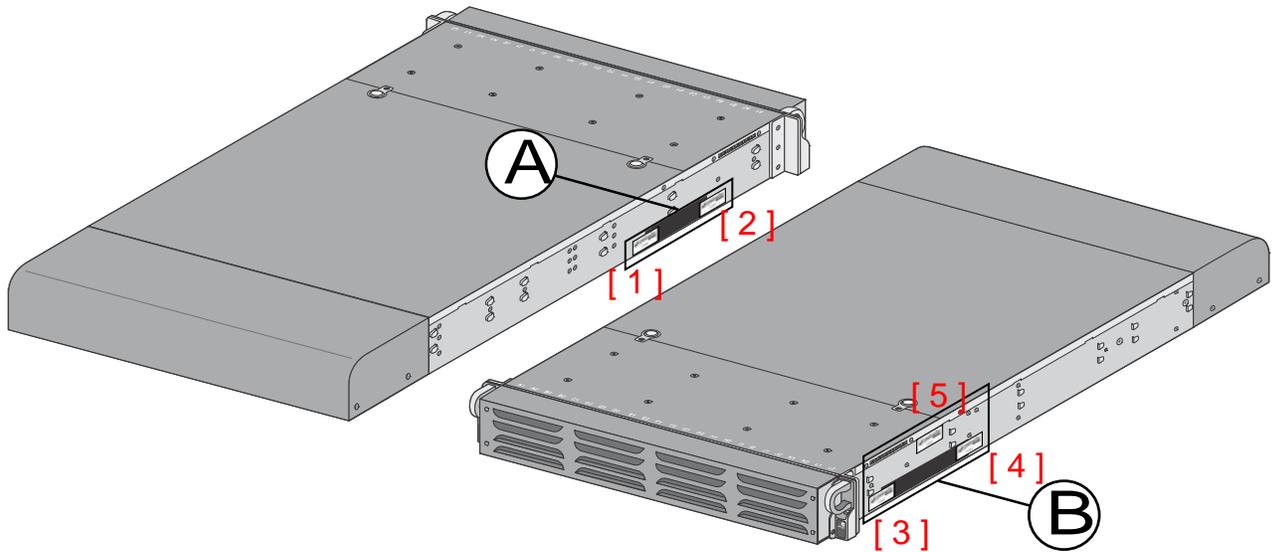


Figure 16 – Apply Tamper-Evident Seals on Vent Overlays and Side Opening

Step 7:

Attach the rail kit to the appliance as shown in Figure 17 and then add three (3) tamper-evident seals to the bottom of the appliance as shown in Figure 18. One (1) tamper-evident seal prevents tampering of the front opacity shield connected to the bottom of the appliance and two (2) tamper-evident seals wrap around the upper and lower rear opacity shields to prevent tampering of the rear opacity shields.

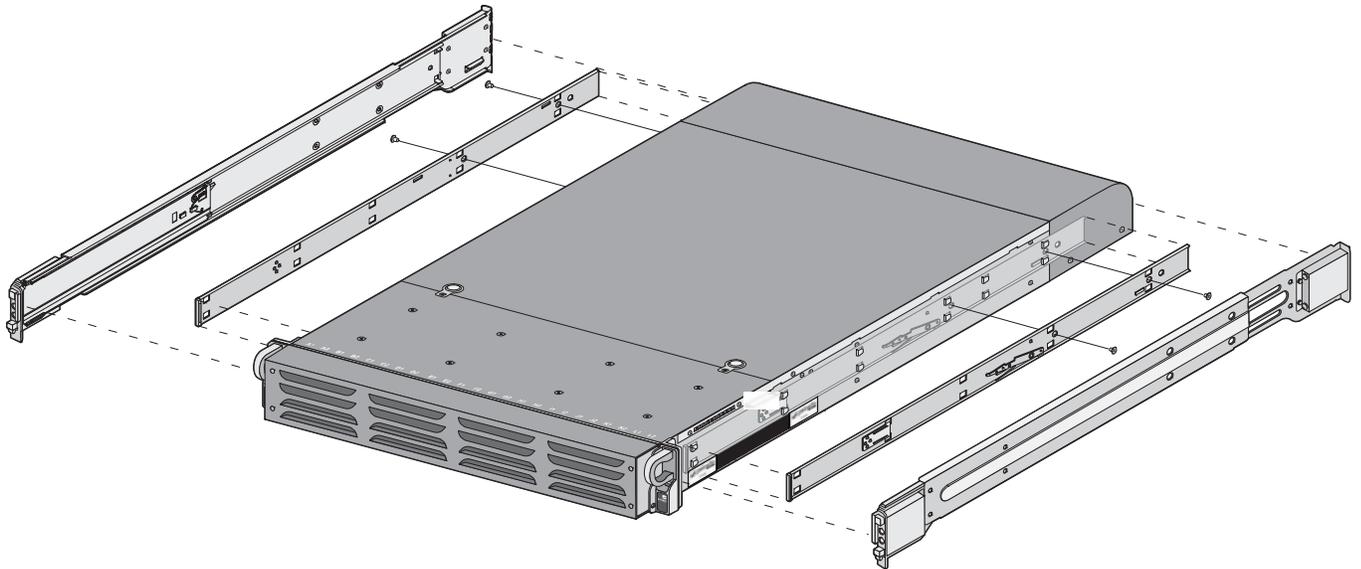


Figure 17 – Install Rail Kit

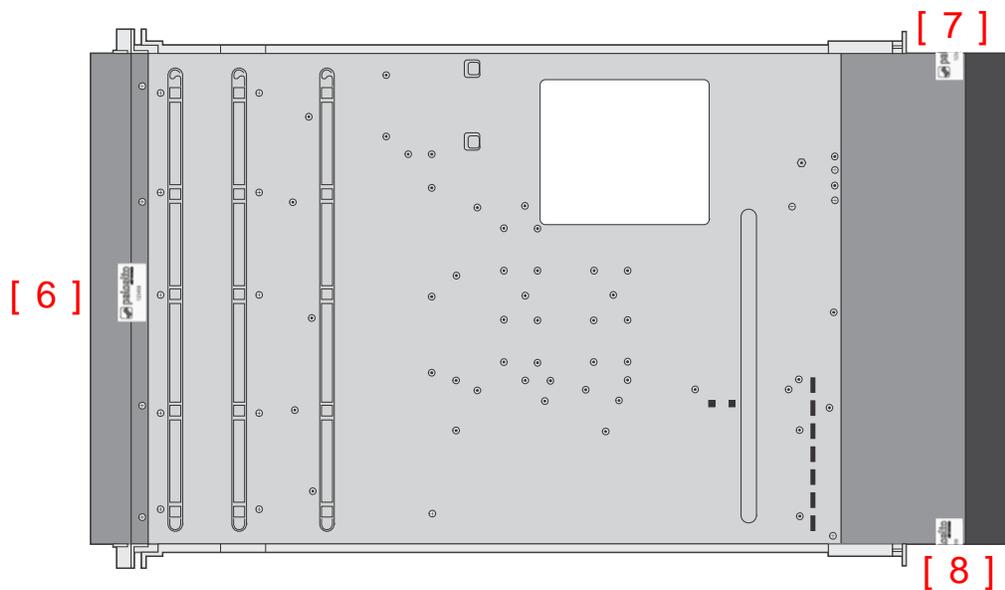


Figure 18 – Apply Tamper-Evident Seals on the Bottom of the Appliance

Step 8:

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

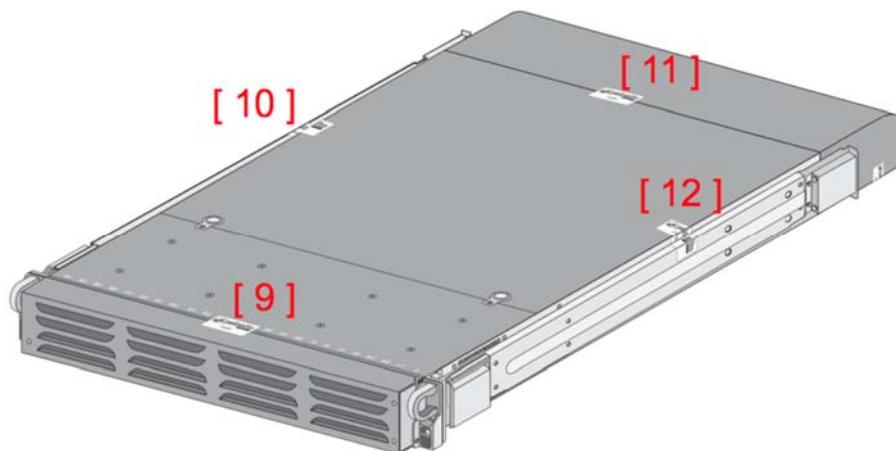


Figure 19 – Apply Tamper-Evident Seals on the Top and Sides of the Appliance