WildFire 10.2

WF-500 and WF-500-B

FIPS 140-3 Non-Proprietary Security Policy

Version: 1.2

Revision Date: August 28, 2024

Palo Alto Networks, Inc.
www.paloaltonetworks.com

Table of Contents

1. General

The Wildfire 10.2 WF-500 and WF-500-B from Palo Alto Networks Inc., hereafter referred to as "Wildfire" or the "cryptographic module" is a multi-chip standalone cryptographic module designed to fulfill FIPS 140-3 level 2 requirements. The WildFire 10.2 WF-500 and WF-500-B 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 (WF) 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 cryptographic module meets the overall requirements applicable to Level 2 security of FIPS 140-3.

Table 1- Security Levels

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

2. Cryptographic Module Specification

The Palo Alto Networks, Inc. WF-500-B is a multi-chip standalone module. The cryptographic boundary includes all firmware components contained within the physical enclosure of the module. Figures below provide images of the module with the physical kit's opacity shields in place. See the Physical Security section for details regarding the module's physical security mechanisms.

Table 2 - Cryptographic Module Tested Configuration

Model	Hardware	Firmware Version	Distinguishing Features
WF-500	910-000097 Physical Kit: 920-000145	10.2.3-h1	RJ45 interfaces, USB ports, LEDs
WF-500-B	910-000270 Physical Kit: 920-000318	10.2.3-h1	RJ45 interfaces, USB ports, LEDs, SFP+ ports

Approved Mode of Operation

The following section details the procedure necessary to place the module into the Approved mode of operation.

- Install module and interface connections in addition to the physical kit.
- The tamper-evident seals and opacity shields must be installed as per Appendix A for the module to operate in the 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.
  - During initial boot up, break the boot sequence via the console port connection (by pressing the maint button when instructed to do so) to access the main menu.
- Select "Continue."
- Select the "Set FIPS-CC Mode" option to enter the Approved mode.
- 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.
- Once the module has finished booting, the Crypto Officer can authenticate using the default credentials that come with the module
  - Once authenticated, the module will automatically require the operator to change their password; and the default credential is overwritten

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

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

Should one or more power-up self-tests fail, the module will not enter the 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.

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

Non-Compliant State

Failure to follow the directions in the Approved Mode of Operation above and Section 11 will result in the module operating in a non-compliant state.

Zeroization

To initiate the zeroization service, perform the following steps:

- 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"

Uninitialized State

If the module does not successfully transition into the Approved mode of operation, or zeroization is performed, the module will be in an uninitialized state. It is required to initialize the module in order to perform cryptographic functions.

Approved and Allowed Algorithms

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

Table 3 - Approved Algorithms

CAVP Cert	Algorithm and Standard	Mode/Method	Description / Key Size(s) / Key Strength(s)	Use / Function
A2518	Conditioning Component AES-CBC-MAC SP 800-90B	AES-CBC-MAC	128 bits	Vetted conditioning component for ESV Cert. #64
A2906	AES-CBC [SP 800-38A]	CBC	128, 192 and 256 bits	Encryption Decryption
A2906	AES-CFB128 [SP 800-38A]	CFB128	128 bits	Encryption Decryption
A2906	AES-CTR [SP 800-38A]	CTR	128, 192 and 256 bits	Encryption Decryption
A2906	AES-GCM [SP 800-38D]	GCM**	128 and 256 bits	Encryption Decryption
A2906	Counter DRBG [SP 800-90Arev1]	CTR DRBG	AES 256 bits with Derivation Function Enabled	Random Bit Generator
A2906	ECDSA KeyGen (FIPS 186-4)	ECDSA KeyGen	P-256, P-384, P-521	Key Generation
A2906	ECDSA KeyVer	ECDSA KeyVer	P-256, P-384, P-521	Public Key Validation

	(FIPS 186-4)			
A2906	ECDSA SigGen (FIPS 186-4)	ECDSA SigGen	P-256, P-384, P-521 with SHA2-224, SHA2-256, SHA2-384, and SHA2-512	Signature Generation
A2906	ECDSA SigVer (FIPS 186-4)	ECDSA SigVer	P-256, P-384, P-521 with SHA-1, SHA2-224, SHA2-256, SHA2-384, and SHA2-512	Signature Verification
A2906	HMAC-SHA-1 [FIPS 198-1]	HMAC	HMAC-SHA-1 with λ= 160	Authentication for protocols
A2906	HMAC-SHA2-224 [FIPS 198-1]	HMAC	HMAC-SHA2-224 with λ=224	Authentication for protocols
A2906	HMAC-SHA2-256 [FIPS 198-1]	HMAC	HMAC-SHA2-256 with λ=256	Authentication for protocols
A2906	HMAC-SHA2-384 [FIPS 198-1]	HMAC	HMAC-SHA2-384 with λ=384	Authentication for protocols
A2906	HMAC-SHA2-512 [FIPS 198-1]	HMAC	HMAC-SHA2-512 with λ=512	Authentication for protocols
A2906	KAS-ECC-SSC (SP 800-56Ar3)	KAS	Ephemeral Unified Model: P-256/P-384/P-521	Key Exchange
A2906	KAS-FFC-SSC (SP 800-56Ar3)	KAS	dhEphem: MODP-2048	Key Exchange
A2906	KDF IKEv2 [SP 800-135rev1] (CVL)	IKEv2 KDF	SHA2-256, SHA2-384, SHA2-512	IKEv2
A2906	KDF SNMP [SP 800-135rev1] (CVL)	SNMPv3 KDF	Engine ID: 80001F88043030303030343935323630	SNMPv3
A2906	KDF SSH [SP 800-135rev1] (CVL)	SSHv2 KDF	SHA-1, SHA2-256, SHA2-512	SSH
A2906	KDF TLS [SP 800-135rev1] (CVL)	TLS1.2 KDF	TLS v1.2 Hash Algorithm: SHA2-256, SHA2-384	TLS
A2906	RSA KeyGen (FIPS 186-4)	RSA KeyGen (FIPS 186-4)	2048, 3072, and 4096 bits	Key Pair Generation
A2906	RSA SigGen (FIPS 186-4)	RSA SigGen (FIPS 186-4)	(ANSI X9.31, RSASSA-PKCS1_v1-5, RSASSA-PSS): 2048, 3072, and 4096-bit with hashes SHA2-256/384/512	Signature Generation
A2906	RSA SigVer (FIPS 186-4)	RSA SigVer (FIPS 186-4)	(ANSI X9.31, RSASSA-PKCS1_v1-5, RSASSA-PSS): 2048, 3072, 4096-bit (per IG C.F) with hashes SHA-1 and SHA2-224+++/256/384/512 (Signature Verification) +++ This Hash algorithm is not supported for ANSI X9.31	Signature Verification
A2906	SHA-1 [FIPS 180-4]	SHA	SHA-1	Digital Signature Generation/Verification Non-Digital Signature Applications (e.g. component of HMAC)
A2906	SHA2-224 [FIPS 180-4]	SHA2	SHA-224	Digital Signature Generation/Verification

				Non-Digital Signature Applications (e.g. component of HMAC)
A2906	SHA2-256 [FIPS 180-4]	SHA2	SHA-256	Digital Signature Generation/Verification Non-Digital Signature Applications (e.g. component of HMAC)
A2906	SHA2-384 [FIPS 180-4]	SHA2	SHA-384	Digital Signature Generation/Verification Non-Digital Signature Applications (e.g. component of HMAC)
A2906	SHA2-512 [FIPS 180-4]	SHA2	SHA-512	Digital Signature Generation/Verification Non-Digital Signature Applications (e.g. component of HMAC)
A2906	Safe Primes Key Generation [RFC 3526]	Safe Primes Key Generation	MODP-2048	Safe Primes Key Generation
A2906	Safe Primes Key Verification [RFC 3526]	Safe Primes Key Verification	MODP-2048	Safe Primes Key Verification
AES Cert. # A2906 and HMAC Cert. # A2906	KTS [SP 800-38F]	SP 800-38A, FIPS 198-1, and SP 800-38F. KTS (key wrapping and unwrapping) per IG D.G.	128, 192, and 256-bit keys providing 128, 192, or 256 bits of encryption strength	Key Wrapping
AES-GCM Cert. # A2906	KTS [SP 800-38F]	SP 800-38D and SP 800-38F. KTS (key wrapping and unwrapping) per IG D.G.	128 and 256-bit keys providing 128 or 256 bits of encryption strength	Key Wrapping
ESV Cert. #E64	SP 800-90B	ESV	Palo Alto Networks DRNG Entropy Source	Entropy
ESV Cert. #E130	SP 800-90B	ESV	Palo Alto Networks DRNG Entropy Source	Entropy
KAS-ECC-SSC Cert. #A2906, KDF IKEv2 Cert. #A2906	KAS [SP 800-56Arev3]	SP 800-56Arev3. KAS-ECC per IG D.F Scenario 2 path (2).	P-256, P-384 curves providing 128 or 192 bits of encryption strength	Key Exchange with protocol KDF
KAS-ECC-SSC Cert. #A2906, KDF SSH Cert. #A2906	KAS [SP 800-56Arev3]	SP 800-56Arev3. KAS-ECC per IG D.F Scenario 2 path (2).	P-256, P-384, and P-521 curves providing 128, 192, or 256 bits of encryption strength	Key Exchange with protocol KDF
KAS-ECC-SSC Cert. #A2906, KDF TLS Cert. #A2906	KAS [SP 800-56Arev3]	SP 800-56Arev3. KAS-ECC per IG D.F Scenario 2 path (2).	P-256, P-384, and P-521 curves providing 128, 192, or 256 bits of encryption strength	Key Exchange with protocol KDF
KAS-FFC-SSC Cert. #A2906, KDF IKEv2 Cert. #A2906	KAS [SP 800-56Arev3]	SP 800-56Arev3. KAS-FFC per IG D.F Scenario 2 path (2).	2048-bit key providing 112 bits of encryption strength	Key Exchange with protocol KDF
KAS-FFC-SSC Cert. #A2906, KDF SSH Cert. #A2906	KAS [SP 800-56Arev3]	SP 800-56Arev3. KAS-FFC per IG D.F Scenario 2 path (2).	2048-bit key providing 112 bits of encryption strength	Key Exchange with protocol KDF
KAS-FFC-SSC Cert. #A2906, KDF TLS Cert. #A2906	KAS [SP 800-56Arev3]	SP 800-56Arev3. KAS-FFC per IG D.F Scenario 2 path (2).	2048-bit key providing 112 bits of encryption strength	Key Exchange with protocol KDF
Vendor Affirmed	CKG (SP 800-133rev2)	Section 5.1, Section 5.2	Cryptographic Key Generation; SP 800-	Key Generation

			133 and IG D.I (asymmetric seeds).	Note: The seeds used for asymmetric key pair generation are produced using the unmodified/direct output of the DRBG

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

- For TLS, The GCM implementation meets Scenario 1 of IG C.H: it is used in a manner compliant with SP 800-52 and in accordance with Section 4 of RFC 5288 for TLS key establishment, and ensures when the nonce_explicit part of the IV exhausts all possible values for a given session key, that a new TLS handshake is initiated per sections 7.4.1.1 and 7.4.1.2 of RFC 5246. During operational testing, the module was tested against an independent version of TLS and found to behave correctly.
    - From this RFC 5288, the GCM cipher suites in use are TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, and TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384.)
- For IPsec/IKEv2, The GCM implementation meets Scenario 1 of IG C.H: 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), and ensures when the module exhausts all possible values for a given session key that this triggers a rekey condition. 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 Scenario 1 of IG C.H. The module conforms to RFCs 4252, 4253, and 5647. The fixed field is 4-byte in length and is derived using the SSH KDF; this ensures the fixed field is unique for any given GCM session. The invocation field is 8-byte in length and is incremented for each invocation of GCM; this prevents the IV from repeating until the entire invocation field space of 2^{64} is exhausted, which can take hundreds of years. (In FIPS-CC Mode, SSH rekey is automatically configured at 1 GB of data or 1 hour, whichever comes first.)

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

The module is compliant to IG C.F:

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

The module does not have any algorithms that fall under:

- Non-Approved Algorithms Allowed in the Approved Mode of Operation
- Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed
- Non-Approved Algorithms Not Allowed in the Approved Mode of Operation

Table 4 - Supported Protocols in the Approved Mode

Supported Protocols*
TLS 1.2
SSHv2
SNMPv3
IPsec and IKEv2

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

Module Diagrams

Figures 1 - 4 depict the modules and their interfaces. Please refer to the appendix for depictions of the module with the physical kit installed.

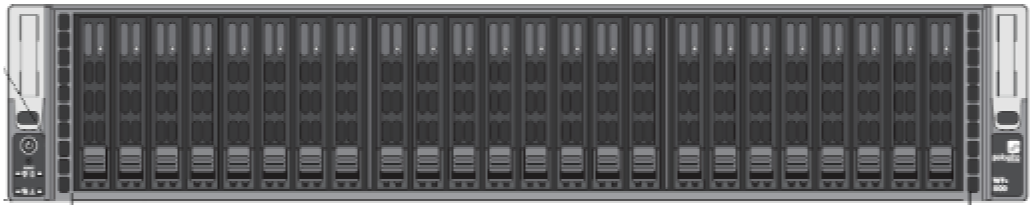

Figure 1 - WF-500 Front

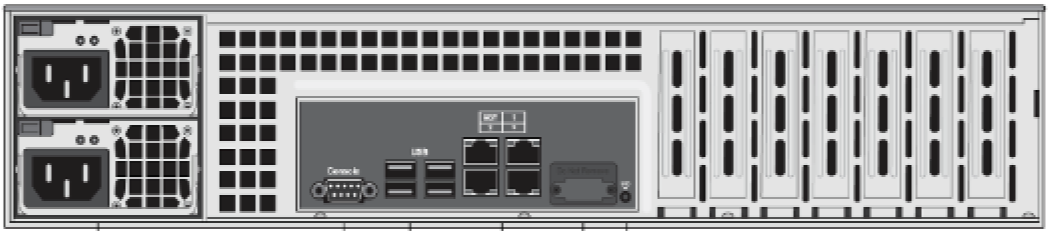

Figure 2 - WF-500 Rear

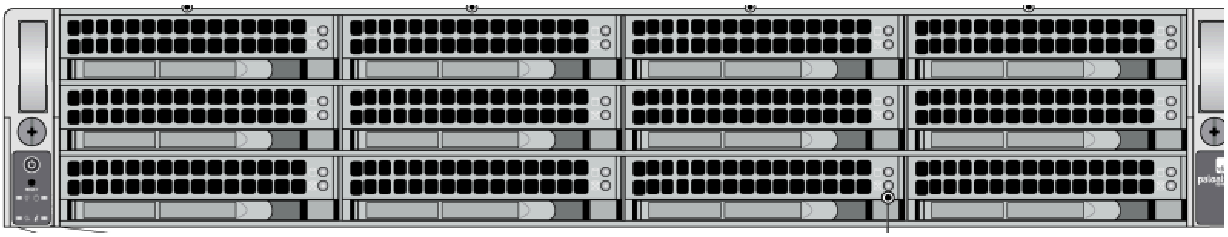

Figure 3 - WF-500-B Front

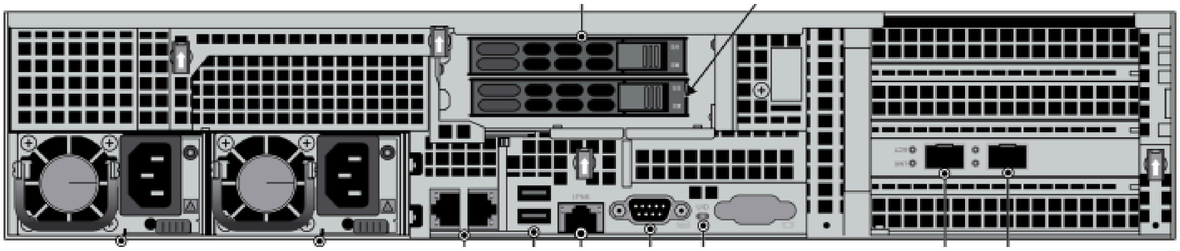

Figure 4 - WF-500-B Rear

3. Cryptographic Module Interfaces

The module is a multi-chip standalone with ports and interfaces as shown below. The module does not implement a control output interface.

Table 5 - Ports and Interfaces

Physical Interface	Logical Interface	Data that passes over port/interface
LED	Status output	Module status via LED indicators
Console	Status output	Self-test output
Power	Power	N/A
RJ45 Ethernet	Data input, control input, data output, status output	TLS, IPSec, or SSH
SFP+ (WF-500-B)	Data input, control input, data output, status output	TLS

Note: USB and IPMI ports are present but not used (i.e. disabled).

4. Roles, Services, and Authentication

Services

When initialized into 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 WF-500 and WF-500-B modules.

Table 6 – Roles, Service Commands, Input and Output

Role	Service	Input	Output
CO	Show Version	Query module for version	Module provides version
CO	System Operational Management	Configuring and managing networking parameter configuration, logging configuration, and other non-security relevant configuration via CLI	Confirmation of service via Configuration Logs
CO	System Configuration Management	Configuring and managing cryptographic parameters and setting/modifying security policy, including creating User accounts and additional CO accounts via CLI	Confirmation of service via Configuration Logs
CO	Data Analysis Management	Configure data submission, analysis and reporting functions via CLI	Confirmation of service via Configuration Logs
CO	Check Status	Query status of the module via CLI	Module status information via CLI or System Logs
CO	Firmware Update	Loading new image	System log noting version updated successfully
User	System Audit	View the System Logs via CLI	System Logs
Peer-to-Peer VPN	IKE/IPsec configuration	Initialize VPN connection	Confirmation of service via System Logs
Unauthenticated	Zeroize	Initialize factory reset via Maintenance Mode	Confirmation of zeroization via console output
Unauthenticated	Self-Tests	Power removal	Confirmation of self-test output/logs
Unauthenticated	Show Status	N/A	LEDs

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 with identity-based authentication.

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

Table 7 – Roles and Authentication

Role	Authentication Method	Authentication Strength
Crypto-Officer (CO)	Memorized Secret (Unique Username/password) and/or Single-Factor Cryptographic Software (certificate common name / public key-based authentication	Password-based Minimum length is eight (8) characters[1] (95 possible characters). The probability that a random attempt will succeed or a false acceptance will occur is 1/(95^8) which is less than 1/1,000,000. The probability of successfully authenticating to the module within one minute is 10/(95^8), which is less than 1/100,000. The module's configuration supports at most ten failed attempts to authenticate in a one-minute period. Certificate/Public key-based The security modules support public-key based authentication using RSA 2048 and certificate-based authentication using RSA 2048, RSA 3072, RSA 4096, ECDSA P-256, P-384, or P-521. The minimum equivalent strength supported is 112 bits. The probability that a random attempt will succeed is 1/(2^{112}) which is less than 1/1,000,000. The probability of successfully authenticating to the module within a one minute period is 6,000/(2^{112}), which is less than 1/100,000. The module supports at most 100 new sessions per second to authenticate in a one-minute period.
User	Memorized Secret (Unique Username/password) and/or Single-Factor Cryptographic Software (certificate common name / public key-based authentication	
Peer-to-peer VPN	Memorized Secret (Unique Username/password) and/or Single-Factor Cryptographic Software (certificate common name / public key-based authentication	Certificate/Public key-based The security modules support public-key based authentication using RSA 2048 and certificate-based authentication using RSA 2048, RSA 3072, RSA 4096, ECDSA P-256, P-384, or P-521.

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

		The minimum equivalent strength supported is 112 bits. The probability that a random attempt will succeed is 1/(2^{112}) which is less than 1/1,000,000. The probability of successfully authenticating to the module within a one minute period is 6,000/(2^{112}), which is less than 1/100,000. The module supports at most 100 new sessions per second to authenticate in a one-minute period.

SSP Access Rights

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

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

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

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

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

Z = Zeroise: The module zeroises the SSP.

Table 8 – Approved Services

Service	Description	Approved Security Functions		Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
Show Version	Query the module to display the version	N/A		N/A	CO	N/A	Version displayed via System Logs / CLI
System Operational Management	Perform system management functions including firmware updates, licensing, diagnostics and debug functions.	CKG RSA KeyGen (FIPS 186-4) RSA SigGen (FIPS 186-4)		RSA Private Keys	CO	G/W/E	System Logs
		CKG ECDSA KeyGen (FIPS 186-4) ECDSA SigGen (FIPS 186-4)		ECDSA Private Keys	CO	G/W/E	System Logs
		KAS	KDF TLS	TLS Pre-Master Secret	CO	G/E/Z	System Logs
			KDF TLS	TLS Master Secret	CO	G/E/Z	System Logs
			CKG, ECDSA KeyGen (FIPS 186-4), ECDSA KeyVer (FIPS 186-4), KAS-ECC-SSC, KAS-FFC-SSC, Safe Primes Key Generation, Safe Primes Key Verification	TLS DHE/ECDHE Private Components	CO	G/E/Z	System Logs
				TLS DHE/ECDHE Public Components	CO	G/E/R/W/Z	System Logs
		KTS	HMAC-SHA2-256 HMAC-SHA2-384	TLS HMAC Keys	CO	G/E/Z	System Logs
			AES-CBC	TLS Encryption Keys	CO	G/E/Z	System Logs
		KTS	AES-GCM				
		KAS	KDF SSH (CVL)	SSH DHE/ECDHE Private Components	CO	G/E/Z	System Logs

			KAS-ECC-SSC KAS-FFC-SSC Safe Primes Key Generation, Safe Primes Key Verification	SSH DHE/ECDHE Public Components		G/E/R/W/Z	System Logs
		KTS	HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-512	SSH Session Authentication Keys	CO	G/E/Z	System Logs
			AES-CBC, AES-CTR	SSH Session Encryption Keys	CO	G/E/Z	System Logs
		KTS	AES-GCM				
		N/A		CO, User Password	CO	G/E/W	System Logs
		Counter DRBG, ESV		DRBG Seed	CO	G/E	System Logs
				DRBG V			
				DRBG Key			
				Entropy Input String			
		KAS	KDF IKEv2 (CVL)	IPSec/IKE DHE/ECDHE Public Components	CO	G/E/Z	System Logs
			CKG, ECDSA KeyGen (FIPS 186-4), ECDSA KeyVer (FIPS 186-4), KAS-ECC-SSC, KAS-FFC-SSC, Safe Primes Key Generation, Safe Primes Key Verification	IPSec/IKE DHE/ECDHE Private Components	CO	G/E/Z	System Logs
		KTS	HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512	IPSec/IKE Authentication Keys	CO	G/E/Z	System Logs
			AES-CBC	IPSec/IKE Session Keys			
		KTS	AES-GCM	IPSec/IKE Session Keys	CO	G/E/Z	System Logs
		N/A		RADIUS Secret	CO	W/E	System Logs
		RSA SigVer (FIPS 186-4)		RSA Public Keys	CO	G/R/E/W	System Logs
		ECDSA SigVer (FIPS 186-4)		ECDSA Public Keys	CO	G/R/E/W	System Logs
		RSA SigVer (FIPS 186-4)		SSH Client RSA Public Key	CO	W/E	System Logs
		RSA SigVer (FIPS 186-4) ECDSA SigVer (FIPS 186-4)		SSH Host Public Key	CO	G/R/E/W	System Logs
		HMAC-SHA2-256, ECDSA SigVer (FIPS 186-4)		Firmware Integrity Verification Key	CO	E	System Logs
		RSA SigVer (FIPS 186-4)		Public Key for Firmware Load Test	CO	W/E	System Logs
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	CKG RSA KeyGen (FIPS 186-4) RSA SigGen (FIPS 186-4)		RSA Private Keys	CO	G/W/E	System Logs
		CKG ECDSA KeyGen (FIPS 186-4) ECDSA SigGen (FIPS 186-4)		ECDSA Private Keys	CO	G/W/E	System Logs
		KAS	KDF TLS	TLS Pre-Master Secret	CO	G/E/Z	System Logs
			KDF TLS	TLS Master Secret	CO	G/E/Z	System Logs
			CKG, ECDSA KeyGen (FIPS 186-4), ECDSA KeyVer (FIPS 186-4), KAS-ECC-SSC, KAS-FFC-SSC, Safe Primes Key Generation, Safe Primes Key Verification	TLS DHE/ECDHE Private Components	CO	G/E/Z	System Logs
				TLS DHE/ECDHE Public Components	CO	G/E/R/W/Z	System Logs

	administrators/users, and password profiles. Configure operators and authentication profiles.	KAS	KDF SSH (CVL)	SSH DHE/ECDHE Private Components	CO	G/E/Z	System Logs
			KAS-ECC-SSC KAS-FFC-SSC Safe Primes Key Generation, Safe Primes Key Verification	SSH DHE/ECDHE Public Components		G/E/R/W/Z	System Logs
		KTS	HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-512	SSH Session Authentication Keys	CO	G/E/Z	System Logs
			AES-CBC, AES-CTR	SSH Session Encryption Keys	CO	G/E/Z	System Logs
		KTS	AES-GCM				
		N/A		CO, User Password	CO	G/E/W	System Logs
		Counter DRBG, ESV		DRBG Seed	CO	G/E	System Logs
				DRBG V			
				DRBG Key			
				Entropy Input String			
		KDF SNMP (CVL)		SNMPv3 Authentication Secret	CO	W/E	System Logs
		KDF SNMP (CVL)		SNMPv3 Privacy Secret	CO	W/E	System Logs
		HMAC-SHA-1 HMAC-SHA2-224 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512		Authentication Key	CO	G/E/Z	System Logs
		AES-CFB128		Session Key	CO	G/E/Z	System Logs
		KAS	KDF IKEv2 (CVL)	IPSec/IKE DHE/ECDHE Public Components	CO	G/E/Z	System Logs
			CKG, ECDSA KeyGen (FIPS 186-4), ECDSA KeyVer (FIPS 186-4), KAS-ECC-SSC, KAS-FFC-SSC, Safe Primes Key Generation, Safe Primes Key Verification	IPSec/IKE DHE/ECDHE Private Components	CO	G/E/Z	System Logs
		KTS	HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512	IPSec/IKE Authentication Keys	CO	G/E/Z	System Logs
			AES-CBC	IPSec/IKE Session Keys			
		KTS	AES-GCM	IPSec/IKE Session Keys	CO	G/E/Z	System Logs
		N/A		RADIUS Secret	CO	W/E	System Logs
		RSA SigVer (FIPS 186-4) ECDSA SigVer (FIPS 186-4)		SSH Host Public Key	CO	G/R/E/W	System Logs
		HMAC-SHA2-256, ECDSA SigVer (FIPS 186-4)		Firmware Integrity Verification Key	CO	E	System Logs
Data Analysis Management	Configure data submission, analysis and reporting functions.	CKG RSA KeyGen (FIPS 186-4) RSA SigGen (FIPS 186-4)		RSA Private Keys	CO	G/W/E	System Logs
		CKG ECDSA KeyGen (FIPS 186-4) ECDSA SigGen (FIPS 186-4)		ECDSA Private Keys	CO	G/W/E	System Logs
		KAS	KDF TLS	TLS Pre-Master Secret	CO	G/E/Z	System Logs
			KDF TLS	TLS Master Secret	CO	G/E/Z	System Logs
			CKG, ECDSA KeyGen (FIPS 186-4), ECDSA KeyVer (FIPS 186-4), KAS-ECC-SSC, KAS-FFC-SSC, Safe	TLS DHE/ECDHE Private Components	CO	G/E/Z	System Logs
				TLS DHE/ECDHE Public Components	CO	G/E/R/W/Z	System Logs

			Primes Key Generation, Safe Primes Key Verification				
		KTS	HMAC-SHA2-256 HMAC-SHA2-384	TLS HMAC Keys	CO	G/E/Z	System Logs
			AES-CBC	TLS Encryption Keys	CO	G/E/Z	System Logs
		KTS	AES-GCM				
		KAS	KDF SSH (CVL)	SSH DHE/ECDHE Private Components	CO	G/E/Z	System Logs
			KAS-ECC-SSC KAS-FFC-SSC Safe Primes Key Generation, Safe Primes Key Verification	SSH DHE/ECDHE Public Components		G/E/R/W/Z	System Logs
		KTS	HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-512	SSH Session Authentication Keys	CO	G/E/Z	System Logs
			AES-CBC, AES-CTR	SSH Session Encryption Keys	CO	G/E/Z	System Logs
		KTS	AES-GCM				
		N/A		CO, User Password	CO	G/E/W	System Logs
		Counter DRBG, ESV		DRBG Seed	CO	G/E	System Logs
				DRBG V			
				DRBG Key			
				Entropy Input String			
Check Status	Review system, configuration, debug logs, and show configurations.	CKG RSA KeyGen (FIPS 186-4) RSA SigGen (FIPS 186-4)		RSA Private Keys	CO	G/W/E	System Logs
		CKG ECDSA KeyGen (FIPS 186-4) ECDSA SigGen (FIPS 186-4)		ECDSA Private Keys	CO	G/W/E	System Logs
		KAS	KDF SSH (CVL)	SSH DHE/ECDHE Private Components	CO	G/E/Z	System Logs
			KAS-ECC-SSC KAS-FFC-SSC Safe Primes Key Generation, Safe Primes Key Verification	SSH DHE/ECDHE Public Components		G/E/R/W/Z	System Logs
		KTS	HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-512	SSH Session Authentication Keys	CO	G/E/Z	System Logs
			AES-CBC, AES-CTR	SSH Session Encryption Keys	CO	G/E/Z	System Logs
		KTS	AES-GCM				
		N/A		CO, User Password	CO	G/E/W	System Logs
		Counter DRBG, ESV		DRBG Seed	CO	G/E	System Logs
				DRBG V			
				DRBG Key			
				Entropy Input String			
		KDF SNMP (CVL)		SNMPv3 Authentication Secret	CO	W/E	System Logs
		KDF SNMP (CVL)		SNMPv3 Privacy Secret	CO	W/E	System Logs
		HMAC-SHA-1 HMAC-SHA2-224 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512		Authentication Key	CO	G/E/Z	System Logs
		AES-CFB128		Session Key	CO	G/E/Z	System Logs
Firmware Update	Used to load/install new firmware	RSA SigVer (FIPS 186-4)		Public Key for Firmware Load Test	CO	W/E	System Logs

System Audit	Allows review of limited configuration and system status via logs, dashboard and configuration screens. Provides no configuration commit capability.	CKG RSA KeyGen (FIPS 186-4) RSA SigGen (FIPS 186-4)		RSA Private Keys	CO	G/W/E	System Logs
		CKG ECDSA KeyGen (FIPS 186-4) ECDSA SigGen (FIPS 186-4)		ECDSA Private Keys	CO	G/W/E	System Logs
		KAS	KDF SSH (CVL)	SSH DHE/ECDHE Private Components	CO	G/E/Z	System Logs
			KAS-ECC-SSC KAS-FFC-SSC Safe Primes Key Generation, Safe Primes Key Verification	SSH DHE/ECDHE Public Components		G/E/R/W/Z	System Logs
		KTS	HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-512	SSH Session Authentication Keys	CO	G/E/Z	System Logs
			AES-CBC, AES-CTR	SSH Session Encryption Keys	CO	G/E/Z	System Logs
		KTS	AES-GCM				
		N/A		CO, User Password	CO	G/E/W	System Logs
		Counter DRBG, ESV		DRBG Seed	CO	G/E	System Logs
				DRBG V			
				DRBG Key			
				Entropy Input String			
IKE/IPsec Configuration	Configures IKE/IPsec setup for peer to peer VPN.	CKG RSA KeyGen (FIPS 186-4) RSA SigGen (FIPS 186-4)		RSA Private Keys	Peer to Peer VPN	G/W/E	System Logs
		CKG ECDSA KeyGen (FIPS 186-4) ECDSA SigGen (FIPS 186-4)		ECDSA Private Keys	Peer to Peer VPN	G/W/E	System Logs
		Counter DRBG, ESV		DRBG Seed	Peer to Peer VPN	G/E	System Logs
				DRBG V			
				DRBG Key			
				Entropy Input String			
		KAS	KDF IKEv2	IPSec/IKE DHE/ECDHE Public Components	Peer to Peer VPN	G/E/Z	System Logs
			CKG, ECDSA KeyGen (FIPS 186-4), ECDSA KeyVer (FIPS 186-4), KAS-ECC-SSC, KAS-FFC-SSC, Safe Primes Key Generation, Safe Primes Key Verification	IPSec/IKE DHE/ECDHE Private Components	Peer to Peer VPN	G/E/Z	System Logs
		KTS	HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512	IPSec/IKE Authentication Keys	Peer to Peer VPN	G/E/Z	System Logs
			AES-CBC	IPSec/IKE Session Keys			
		KTS	AES-GCM	IPSec/IKE Session Keys	Peer to Peer VPN	G/E/Z	System Logs
		RSA SigVer (FIPS 186-4)		RSA Public Keys CA Certificates	Peer to Peer VPN	G/R/E/W	System Logs
		ECDSA SigVer (FIPS 186-4)		ECDSA Public Keys CA Certificates	Peer to Peer VPN	G/R/E/W	System Logs

Zeroize	Destroys all keys in the module	N/A	All Keys and SSPs	CO	Z	Console Output / Zeroization indicator
Self-Tests	Run power up self-tests on demand by power cycling the module.	HMAC-SHA2-256, ECDSA SigVer (FIPS 186-4)	Firmware Integrity Verification Key	CO	E	System Logs
Show Status (LEDs)	View hardware status of the module via the LEDs.	N/A	N/A	All	N/A	LEDs

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

5. Software/Firmware Security

The module performs the Firmware Integrity test by using HMAC-SHA-256 and ECDSA signature verification (HMAC and ECDSA Cert. #A2906) during the Pre-Operational Self-Test. In addition, the module also conducts the firmware load test by using RSA 2048 with SHA-256 (Cert. #A2906) for the new validated firmware to be uploaded into the module.

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

6. Operational Environment

The FIPS 140-3 Operational Environment requirements are not applicable because the module does not contain a modifiable operational environment. The operational environment is limited since the module includes a firmware load service to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-3 CMVP. Any other firmware loaded into the module is out of the scope of this validation and requires a separate FIPS 140-3 validation.

7. Physical Security

Physical Security Mechanisms

The multi-chip standalone 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 tampering. 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 physical kit part numbers and version. Opacity shields are included in the physical kits.

Operator Required Actions

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

Table 9 - Physical Security Inspection Guidelines

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper-Evident Seals	30 days	Verify integrity of tamper-evident seals in the locations specified in the appendix.
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.
Vent Overlays	30 days	Verify that the vent overlays have not been removed or deformed. All edges should maintain strong adhesion characteristics.

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

WF-500 Tamper Seal Installation (12 Seals)

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.

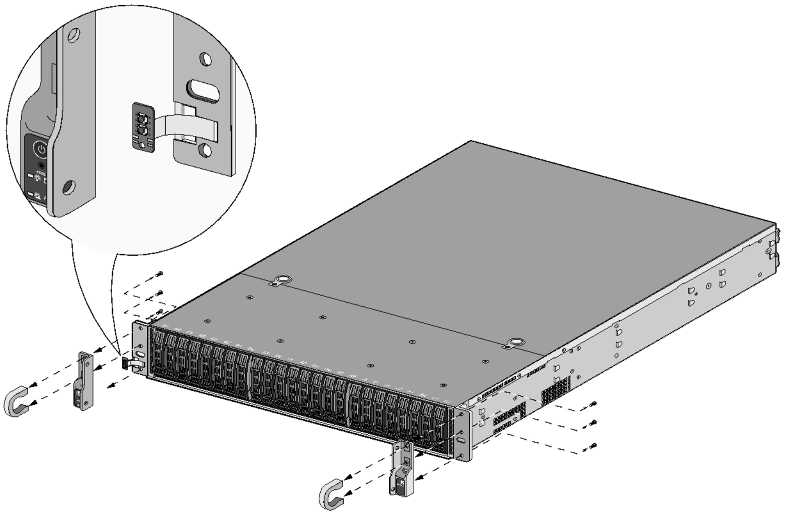

Figure 5 - Remove Front Handles and Modules

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 6, 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 7.

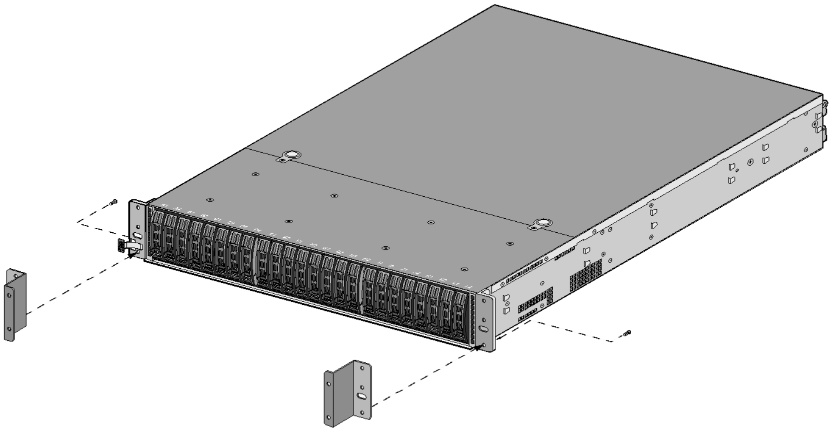

Figure 6 – Secure the Front Brackets

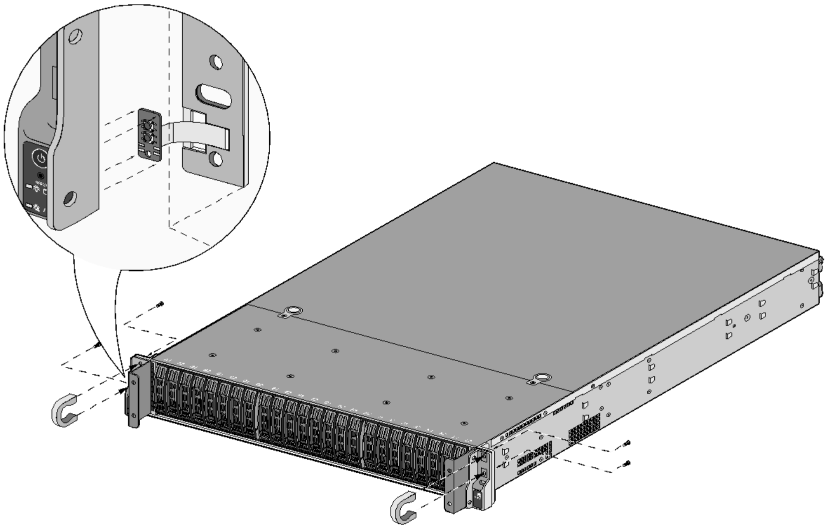

Figure 7 - Attach Pull Handles and Front Modules

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.

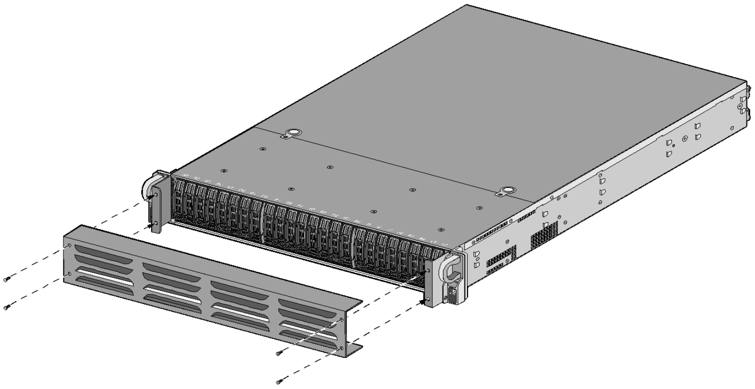

Figure 8 – Install Front Opacity Shield

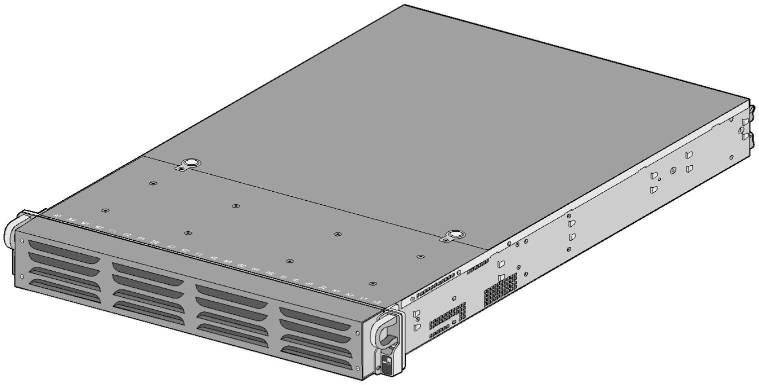

Figure 9 – Front Opacity Shield Installed

4. Attach the rear opacity shield tray to the appliance. First, remove the two (2) screws (shown in Figure 10) 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.

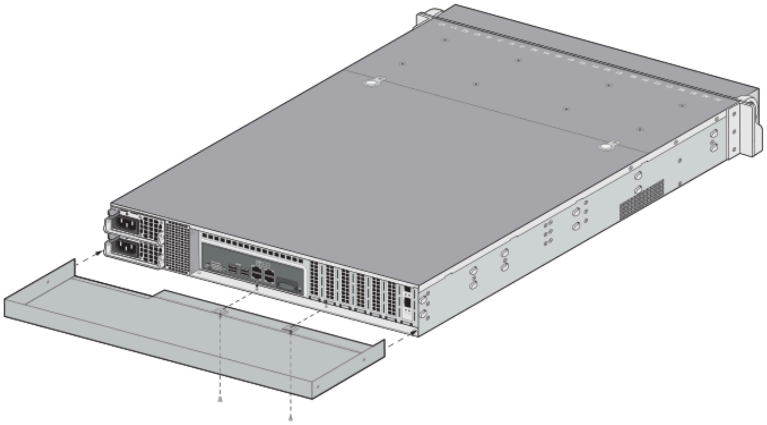

Figure 10 – Install Rear Opacity Shield Tray

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.

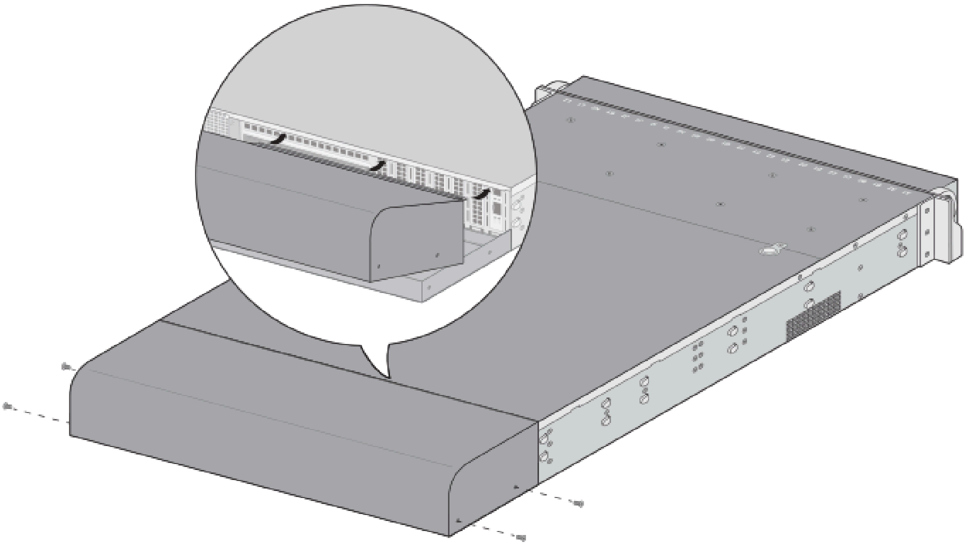

Figure 11 – Install Rear Opacity Shield

6. Cover the vent openings as shown in Figure 12 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 13. Also apply one (1) additional tamper-evident seal as shown in Figure 13, #5.

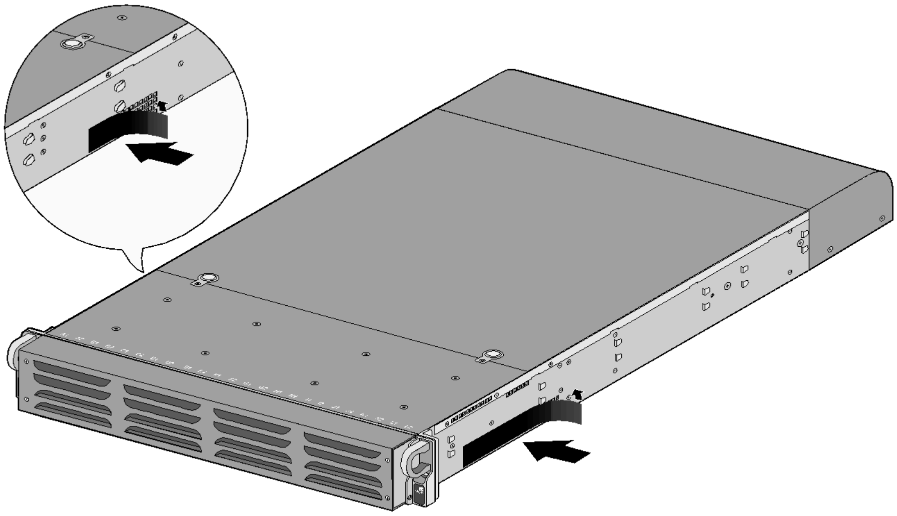

Figure 12 – Apply Tamper-Evident Seals on Vent Overlays

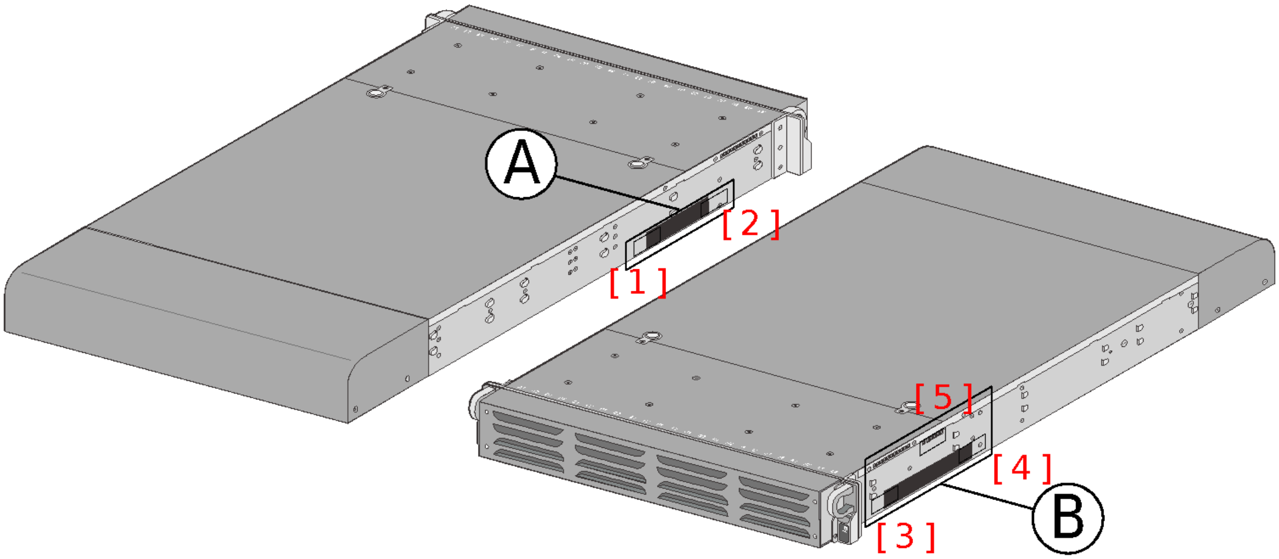

Figure 13 – Apply Tamper-Evident Seals on Vent Overlays and Side Opening

7. Attach the rail kit to the appliance as shown in Figure 14 and then add three (3) tamper-evident seals to the bottom of the appliance as shown in Figure 15. 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.

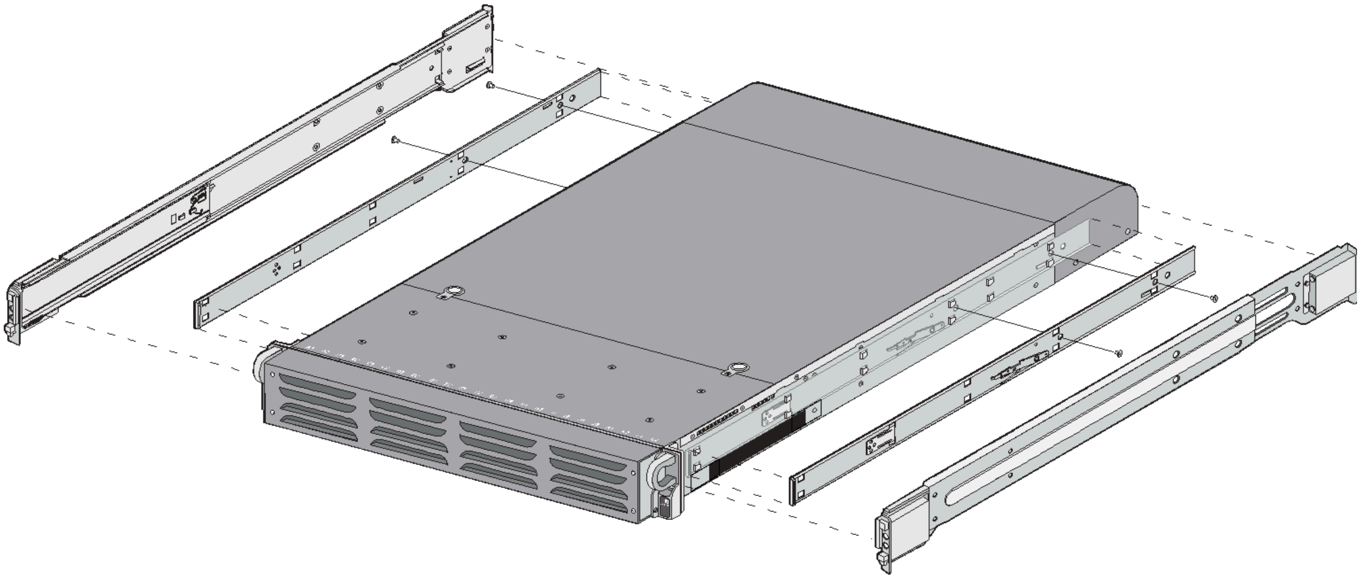

Figure 14 – Install Rail Kit

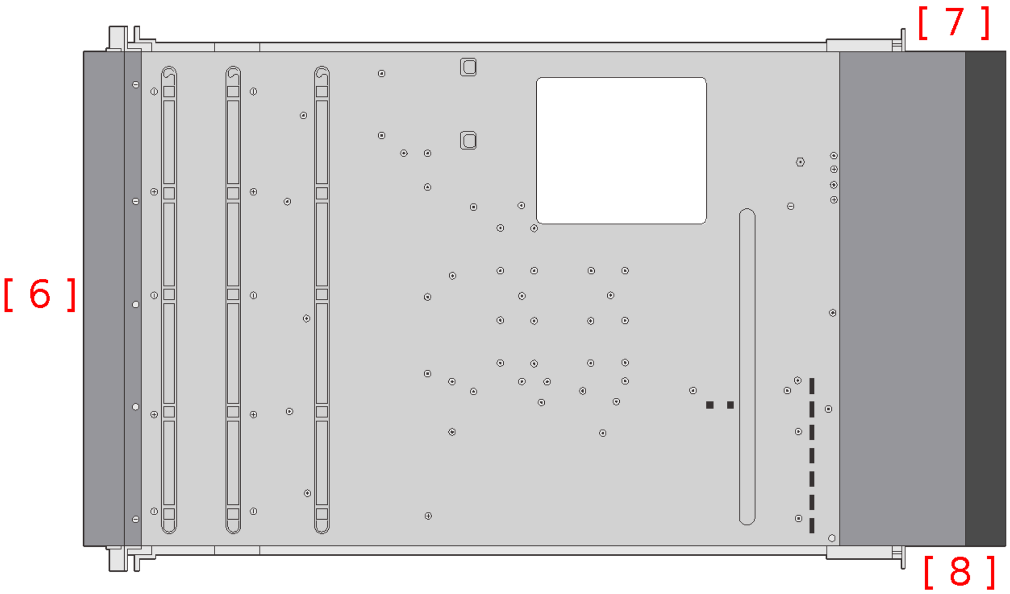

Figure 15 – Apply Tamper-Evident Seals on the Bottom of the Appliance

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

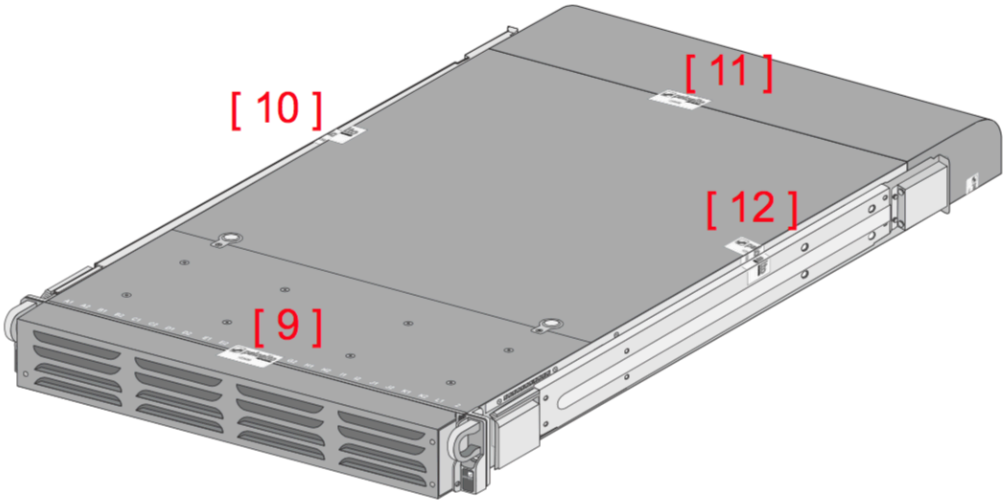

Figure 16 – Apply Tamper Seals on the Top and Sides of the Appliance

WF-500-B Tamper Seal Installation (21 Seals)

1. Replace the top cover with the physical kit top cover.

    a. Remove the VOID WARRANTY label and cover screws (replacement label included in the kit).

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

b. Simultaneously depress the two (2) release buttons on top of the cover and slide the cover toward the back of the appliance to remove it.

c. Slide the physical kit top cover (does not have vents) on the appliance until the release buttons click. Replace the two screws that you removed from the old cover

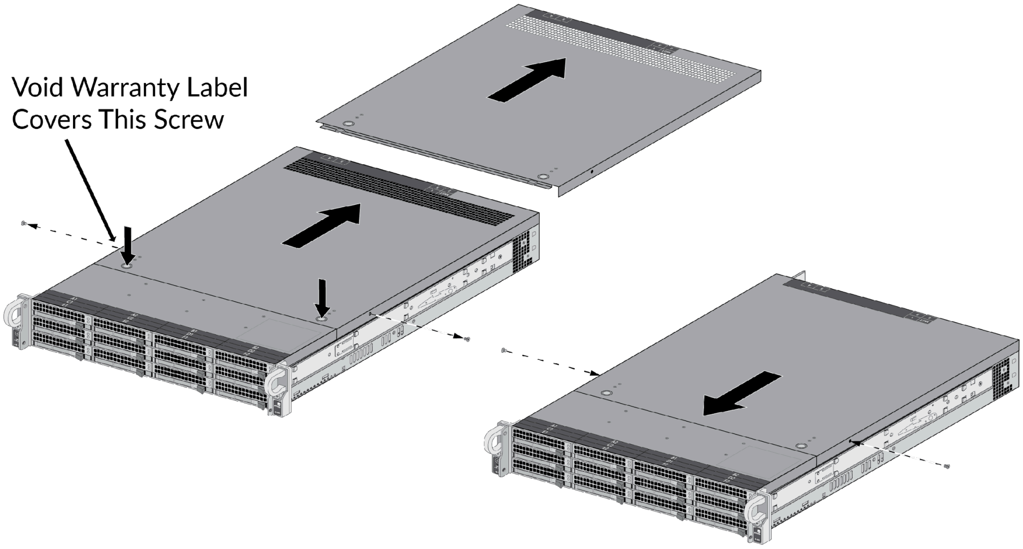

Figure 17 – WF-500-B: Top Cover Replacement

2. Attach the physical kit front cover brackets.

   Remove the front pull handles by removing two (2) screws from each handle (one (1) handle on each side), insert the WF-500-B physical kit front-cover brackets under each handle, and then replace the handles and secure them using the screws that you removed. The physical kit handles have standoffs that are used to secure the front cover.

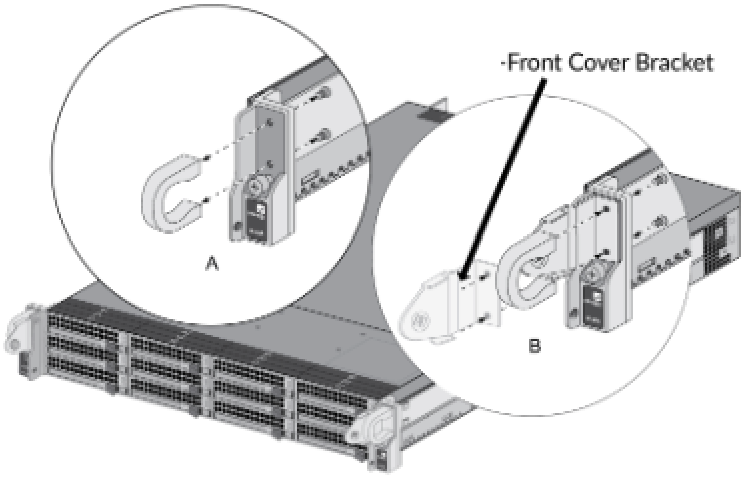

Figure 18 – WF-500-B: Front Cover Bracket

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

   Slide the WF-500-B physical kit front cover over the physical kit pull handle brackets and secure the cover by turning the thumb screws clockwise (one thumb screw on each side).

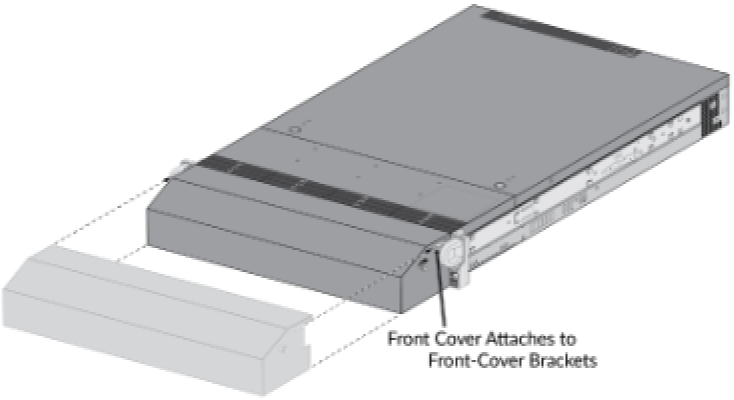

Figure 19 – WF-500-B: FIPS Front Cover

4. Install a tamper-evident seal on the back of the appliance. This is seal #13 in the WF-500-B Figure 19. You need to install this seal before you install the WF-500-B physical kit back cover.

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

    a. Slide the back cover onto the back of the appliance and turn the two (2) thumb screws clockwise until tight (one (1) screw on each side) to secure the cover.

6. Apply a tamper-evident seal to each location shown in the following WF-500-B illustrations below. Also install the overlay stickers to cover vent openings (two (2) stickers on each side). You then install tamper-evident seals over the overlay stickers. Apply two (2) tamper-evident seals on the back side of the right rack handle (see seals #18 and #19 on the left side in Figure 19). Apply two (2) tamper-evident seals on the power supplies (see seals #11 and #12 with rear inset of Figure 19).

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

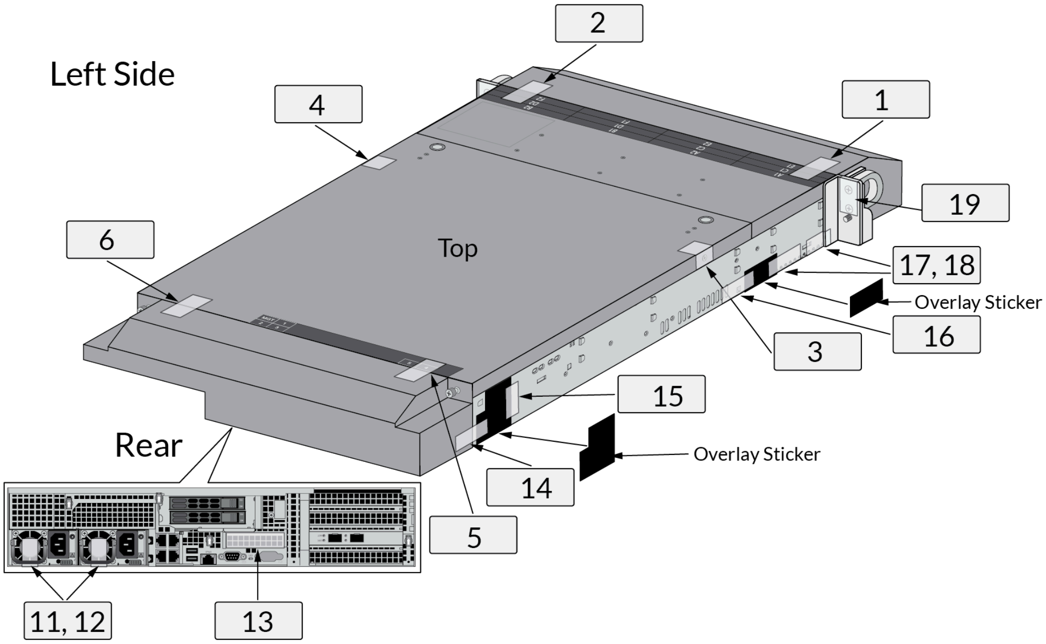

Figure 20 – WF-500-B: Tamper Seal Locations (Top and Rear)

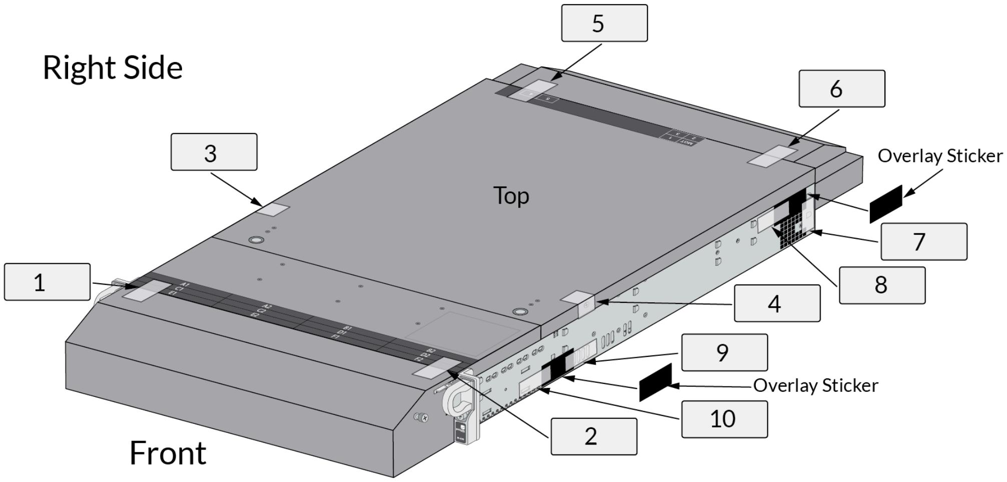

Figure 21 – WF-500-B: Tamper Seal Locations (Top and Front)

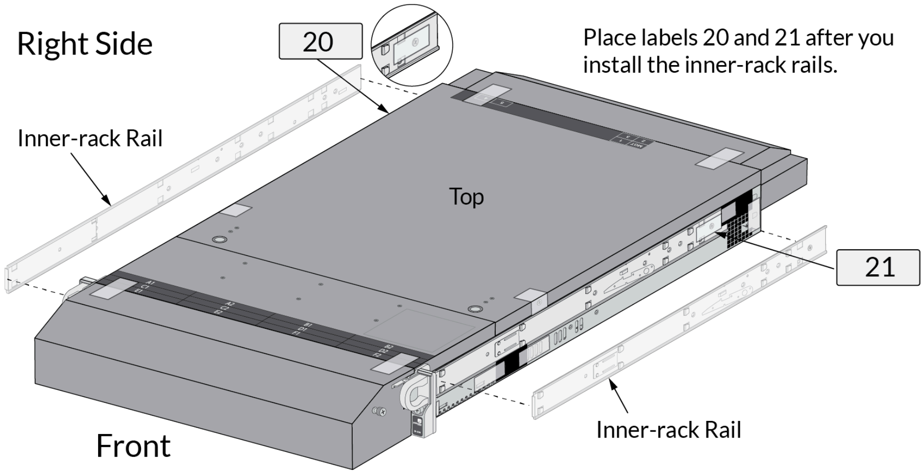
Right Side
20
Place labels 20 and 21 after you install the inner-rack rails.
Inner-rack Rail
Top
21
Inner-rack Rail
Front

Figure 22 – WF-500-B: Tamper Seals Location for Side Rails

8. Non-Invasive Security

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

9. Sensitive Security Parameters

The module contains the following SSPs:

Table 12 – SSPs

Key/SSP/Name/Type	Strength	Security Function and Cert. Number	Generation	Import/Export	Establishment	Storage	Zeroization	Use & Related Keys
CA Certificates	112 bits minimum	RSA SigVer (FIPS 186-4) ECDSA SigVer (FIPS 186-4) Cert. #A2906	DRBG, FIPS 186-4	TLS or SSH Session Key Encrypted	N/A	HDD/RAM – plaintext	HDD – Zeroize Service RAM - Zeroize at session termination	ECDSA/RSA Public key - Used to trust a root CA intermediate CA and leaf /end entity certificates (RSA 2048, 3072, and 4096 bits) (ECDSA P-256, P-384, and P-521)
RSA Public Keys	112 bits minimum	RSA SigVer (FIPS 186-4) Cert. #A2906	DRBG, FIPS 186-4	TLS or SSH Session Key Encrypted or Plaintext TLS handshake	N/A	HDD/RAM – plaintext	Zeroize Service	RSA public keys managed as certificates for the verification of signatures, establishment of TLS, operator authentication and peer authentication. (RSA 2048, 3072, or 4096-bit)

RSA Private Keys	112 bits minimum	RSA SigGen (FIPS 186-4) Cert. #A2906	DRBG, FIPS 186-4	TLS or SSH Session Key Encrypted	N/A	HDD/RAM – plaintext	HDD – Zeroize Service RAM - Zeroize at session termination	RSA Private keys for generation of signatures, authentication or key establishment. (RSA 2048, 3072, or 4096-bit)
ECDSA Public Keys	128 bits minimum	ECDSA SigVer (FIPS 186-4) Cert. #A2906	DRBG, FIPS 186-4	TLS or SSH Session Key Encrypted or Plaintext TLS handshake	N/A	HDD/RAM – plaintext	Zeroize Service	ECDSA public keys managed as certificates for the verification of signatures, establishment of TLS, operator authentication and peer authentication. (ECDSA P-256, P-384, or P-521)
ECDSA Private Keys	128 bits minimum	ECDSA SigGen (FIPS 186-4) Cert. #A2906	DRBG, FIPS 186-4	TLS or SSH Session Key Encrypted	N/A	HDD/RAM – plaintext	HDD – Zeroize Service RAM - Zeroize at session termination	ECDSA Private key for generation of signatures and authentication (P-256, P-384, or P-521)
TLS DHE/ECDHE Private Components	112 bits minimum	KAS-ECC-SSC KAS-FFC-SSC Cert. #A2906	DRBG, SP 800-56A Rev. 3	N/A	N/A	RAM - plaintext	Zeroize at session termination	Ephemeral Diffie-Hellman private FFC or EC component used in TLS (DHE 2048, ECDHE P-256, P-384, P-521)
TLS DHE/ECDHE Public Components	112 bits minimum	KAS-ECC-SSC KAS-FFC-SSC Cert. #A2906	DRBG, SP 800-56A Rev. 3	Plaintext - TLS handshake	N/A	N/A	Zeroize at session termination	Diffie_Hellman or EC Diffie-Hellman Ephemeral values used in key agreement (DHE 2048, ECDHE P-256, P-384, P-521)
TLS Pre-Master Secret	N/A	KDF TLS, Cert. #A2906	KAS SP 800-56A Rev. 3	N/A	N/A	RAM – plaintext	Zeroize at session termination	Secret value used to derive the TLS Master Secret along with client and server random nonces
TLS Master Secret	N/A	KDF TLS Cert. #A2906	KDF TLS	N/A	N/A	RAM – plaintext	Zeroize at session termination	Secret value used to derive the TLS session keys
TLS Encryption Keys	128 bits minimum	AES-CBC or AES-GCM Cert. #A2906	KDF TLS	N/A	TLS, KAS SP 800-56A Rev. 3	RAM - plaintext	Zeroize at session termination	AES (128 or 256 bit) keys used in TLS connections (GCM; CBC)
TLS HMAC Keys	256 bits minimum	HMAC-SHA2-256 HMAC-SHA2-384 Cert. #A2906	KDF TLS	N/A	TLS, KAS SP 800-56A Rev. 3	RAM - plaintext	Zeroize at session termination	HMAC keys used in TLS connections (SHA-256, 384) (256, 384 bits)
SSH DHE/ECDHE Private Components	112 bits minimum	KAS-ECC-SSC KAS-FFC-SSC Cert. #A2906	DRBG, SP 800-56A Rev. 3	N/A	N/A	RAM - plaintext	Zeroize at session termination	Diffie Hellman or EC Diffie-Hellman private (DH Group 14, ECDH P-256, ECDH P-384, ECDH P-521)
SSH DHE/ECDHE Public Components	112 bits minimum	KAS-ECC-SSC KAS-FFC-SSC Cert. #A2906	DRBG, SP 800-56A Rev. 3	Plaintext SSH handshake	N/A	RAM - plaintext	Zeroize at session termination	Diffie Hellman or EC Diffie-Hellman public component (DH Group 14, ECDH P-256, ECDH P-384, ECDH P-521)
SSH Host Public Key	112 bits minimum	RSA SigVer (FIPS 186-4) ECDSA SigVer (FIPS 186-4) Cert. #A2906	DRBG, FIPS 186-4	N/A	N/A	HDD/RAM – plaintext	Zeroize Service	SSH Host Public Key (RSA 2048, RSA 3072, RSA 4096, ECDSA P-256, P-384, or P-521)
SSH Client Public Key	112 bits minimum	RSA SigVer (FIPS 186-4)	N/A	Encrypted via SSH or TLS	N/A	HDD/RAM – plaintext	Zeroize Service	Public RSA key used to authenticate client.

		Cert. #A2906						(RSA 2048, 3072, and 4096 bits)
SSH Session Encryption Keys	128 bits minimum	AES-CBC, AES-CTR, or AES-GCM Cert. #A2906	KDF SSH	N/A	SSH, KAS SP 800-56A Rev. 3	RAM - plaintext	Zeroize at session termination	Used in all SSH connections to the security module's command line interface. (128, 192, or 256 bits: CBC or CTR) (128 or 256 bits: GCM)
SSH Session Authentication Keys	160 bits minimum	HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-512 Cert. #A2906	KDF SSH	N/A	SSH, KAS SP 800-56A Rev. 3	RAM - plaintext	Zeroize at session termination	Authentication keys used in all SSH connections to the security module's command line interface (HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-512) (160, 256, 512 bits)
IPSec/IKE DHE/ECDHE Private Components	112 bits minimum	KAS-ECC-SSC KAS-FFC-SSC Cert. #A2906	DBRG, SP 800-56A Rev. 3	N/A	N/A	RAM - plaintext	Power cycle	Diffie-Hellman or EC Diffie-Hellman private component used in key establishment (DHE 2048, ECDHE P-256, P-384)
IPSec/IKE DHE/ECDHE Public Components	112 bits minimum	KAS-ECC-SSC KAS-FFC-SSC Cert. #A2906	DRBG, SP 800-56A Rev. 3	N/A	N/A	RAM - plaintext	Power cycle	Diffie-Hellman or EC Diffie-Hellman public component used in key agreement (DHE 2048, ECDHE P-256, P-384)
IPSec/IKE Session Keys	128 bits minimum	AES-CBC, AES-GCM Cert. #A2906	N/A	N/A	IPSec/IKE	RAM - plaintext	Zeroize at session termination	Used to encrypt IKE/IPSec data. These are AES CBC or GCM (128 or 256 bits)
IPSec/IKE Authentication Keys	160 bits minimum	HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512 Cert. #A2906	N/A	N/A	IPSec/IKE	RAM - plaintext	Zeroize at session termination	HMAC keys for authentication (HMAC-SHA-256/384/512) (key size 256, 384, 512 bits)
Firmware Integrity Verification key	128 bits	HMAC-SHA2-256, ECDSA SigVer (FIPS 186-4) Cert. #A2906	FIPS 186-4	N/A	N/A	HDD - plaintext	N/A	Used to check the integrity of crypto-related code. (HMAC-SHA-256 and ECDSA P-256) (*Note: This is not considered an SSP*)
Public key for Firmware Load Test	112 bits	RSA SigVer (FIPS 186-4) Cert. #A2906	FIPS 186-4	N/A	N/A	HDD - plaintext	N/A	Used to authenticate firmware and content to be installed on the module (RSA 2048 with SHA-256)
CO, User Password	N/A	SHA2-256 Cert. #A2906	External	Encrypted via SSH or TLS	N/A	HDD - a password hash (SHA2-256)	Zeroize Service	Authentication string with a minimum length of eight (8) characters.
Protocol Secrets	N/A	N/A	N/A	Encrypted via SSH or TLS	N/A	HDD/RAM – plaintext	Zeroize Service	Secrets used by RADIUS or TACACS+ (8 characters minimum)
Entropy Input String	256 bits	CKG (vendor affirmed), Counter DRBG Cert. #A2906	Entropy as per SP 800-90B	N/A	N/A	RAM - plaintext	Power cycle	Entropy input string coming from the entropy source Input length = 384 bits
DRBG Seed	256 bits	CKG (vendor	Entropy as per	N/A	N/A	RAM - Plaintext	Power cycle	DRBG seed coming from the entropy source

		affirmed), Counter DRBG Cert. #A2906	SP 800-90B					Seed length = 384 bits
DRBG Key	256 bits	CKG (vendor affirmed), Counter DRBG Cert. #A2906	Entropy as per SP 800-90B	N/A	N/A	RAM - plaintext	Power cycle	AES 256 CTR DRBG state Key used in the generation of a random values
DRBG V	128 bits	CKG (vendor affirmed), Counter DRBG Cert. #A2906	Entropy as per SP 800-90B	N/A	N/A	RAM - plaintext	Power cycle	AES 256 CTR DRBG state V used in the generation of a random values
SNMPv3 Authentication Secret	N/A	KDF SNMP Cert. #A2906	N/A	TLS/SSH	N/A	HDD/RAM – plaintext	Zeroize Service	Used to support SNMPv3 services (Minimum 8 characters)
SNMPv3 Privacy Secret	N/A	KDF SNMP Cert. #A2906	N/A	TLS/SSH	N/A	HDD/RAM – plaintext	Zeroize Service	Used to support SNMPv3 services (Minimum 8 characters)
Authentication Key	160 bits minimum	HMAC-SHA-1 HMAC-SHA2-224 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512 Cert. #A2906	SNMPv3 KDF	N/A	N/A	HDD/RAM – plaintext	Zeroize Service	HMAC–SHA-1/224/256/384/512 Authentication protocol key (160 bits)
Session Key	128 bits minimum	AES-CFB128 Cert. #A2906	SNMPv3 KDF	N/A	N/A	HDD/RAM - Plaintext	Zeroize Service	Privacy protocol encryption key (AES-CFB128)

Table 13 - Non-Deterministic Random Number Generation Specification

Entropy Source	Minimum number of bits of entropy	Details
Palo Alto Networks DRNG Entropy Source	256 bits	ESV Cert. #E64 Entropy source provides full entropy, which is provided in the 384 bit seed.
Palo Alto Networks RTC Entropy Source	256 bits	ESV Cert. #E130 When initialized per Section 11, the DRBG is seeded with 256 bits of entropy

10. Self-Tests

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

Pre-operational Self-Tests

Pre-operational Firmware Integrity Test

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

Note: the ECDSA and HMAC-SHA-256 KATs are performed prior to the Firmware integrity test

Conditional self-tests

Cryptographic algorithm self-tests

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

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

Conditional Pairwise Consistency Self-Tests

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

Conditional Firmware Load test

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

Conditional Critical Functions Tests

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

Error Handling

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

Table 14 - Errors and Indicators

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

11. Life Cycle Assurance

The vendor provided life-cycle assurance documentation that describes configuration management, design, finite state model, development, testing, delivery + operation, end of life procedures, and guidance. For details regarding the secure installation, initialization, startup, and operation of the module, see section "Approved Mode of Operation" in Section 2.

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

Vendor imposed security rules

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

1. The operator shall not enable TLSv1.0 or use RSA for key wrapping; it is disabled by default
   A. Checked via CLI using "show shared" command
2. If using RADIUS, it must be configured using TLS 1.2.
   A. Checked via CLI using "show shared" command
3. Once boot-up is complete, the WF-500 requires a minimum system uptime of 1 hour before the module can be used to ensure proper instantiation of the DRBG.
   A. Verify uptime via the following command: "show system info | match uptime"
   B. After this time, regenerate any items previously present such as the SSH keys using the following procedure:
      1. Login via CLI and issue the following command:
         a. debug system ssh-key-reset all

12. Mitigation of Other Attacks

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

13. Definitions and Acronyms

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