PA-3060 and PA-7080 Firewalls Non-Proprietary Security Policy

Palo Alto Networks

Revision Date: 1/3/2018

Change Record

Table 1 - Change Record

Date	Author	Description of Change
3/14/2016	Richard Bishop	Initial authoring
11/18/2016	Richard Bishop	Update module version to 7.1.3
1/3/2018	Amir Shahhosseini	Updates for SP800-131A

Contents

Tables

Figures

Module Overview

Palo Alto Networks offers a full line of next-generation security appliances that range from the PA-200, designed for enterprise remote offices, to the PA-7080, which is a modular chassis designed for high-speed datacenters. Our platform architecture is based on our single-pass software engine, PAN-OS, for networking, security, threat prevention, and management functionality that is consistent across all platforms. The devices differ only in capacities, performance, and physical configuration.

The Palo Alto Networks PA-3060 and PA-7080 Firewalls (hereafter referred to as the modules) are multi-chip standalone modules that provide network security by enabling enterprises to see and control applications, users, and content – not just ports, IP addresses, and packets – using three unique identification technologies: App-ID, User-ID, and Content-ID. These identification technologies, found in Palo Alto Networks' enterprise firewalls, enable enterprises to create business-relevant security policies – safely enabling organizations to adopt new applications, instead of the traditional "all-or-nothing" approach offered by traditional port-blocking firewalls used in many security infrastructures.

Features and Benefits

- **Application visibility and control:** Accurate identification of the applications traversing the network enables policy-based control over application usage at the firewall, the strategic center of the security infrastructure.
- **Visualization tools:** Graphical visibility tools, customizable reporting and logging enables administrators to make a more informed decision on how to treat the applications traversing the network.
- **Application browser:** Helps administrators quickly research what the application is, its' behavioral characteristics and underlying technology resulting in a more informed decision making process on how to treat the application.
- **User-based visibility and control:** Seamless integration with enterprise directory services (Active Directory, LDAP, eDirectory) facilitates application visibility and policy creation based on user and group information, not just IP address. In Citrix and terminal services environments, the identity of users sitting behind Citrix or terminal services can be used to enable policy-based visibility and control over applications, users and content. An XML API enables integration with other, 3rd party user repositories.
- **Real-time threat prevention:** Detects and blocks application vulnerabilities, viruses, spyware, and worms; controls web activity; all in real-time, dramatically improving performance and accuracy.
- **File and data filtering:** Taking full advantage of the in-depth application inspection being performed by App-ID, administrators can implement several different types of policies that reduce the risk associated with unauthorized file and data transfer.

- **Legacy firewall support:** Support for traditional inbound and outbound port-based firewall rules mixed with application-based rules smooth the transition to a Palo Alto Networks next generation firewall.
- **Networking architecture**: Support for dynamic routing (OSPF, RIP, BGP), virtual wire mode and layer 2/layer 3 modes facilitates deployment in nearly any networking environment.
- **Policy-based Forwarding**: Forward traffic based on policy defined by application, source zone/interface, source/destination address, source user/group, and service.
- **Virtual Systems**: Create multiple virtual "firewalls" within a single device as a means of supporting specific departments or customers. Each virtual system can include dedicated administrative accounts, interfaces, networking configuration, security zones, and policies for the associated network traffic.
- **VPN connectivity**: Secure site-to-site connectivity is enabled through standards-based IPSec VPN support while remote user access is delivered via SSL VPN connectivity.
- **Quality of Service (QoS):** Deploy traffic shaping policies (guaranteed, maximum and priority) to enable positive policy controls over bandwidth intensive, non-work related applications such as streaming media while preserving the performance of business applications.
- **Real-time bandwidth monitor:** View real-time bandwidth and session consumption for applications and users within a selected QoS class.
- **Purpose-built platform:** combines single pass software with parallel processing hardware to deliver the multi-Gbps performance necessary to protect today's high speed networks.

Note: Modules are shown in figures with no opacity shields included to demonstrate module interfaces and other physical characteristics. Pictures are included of each chassis with the opacity shields in place.

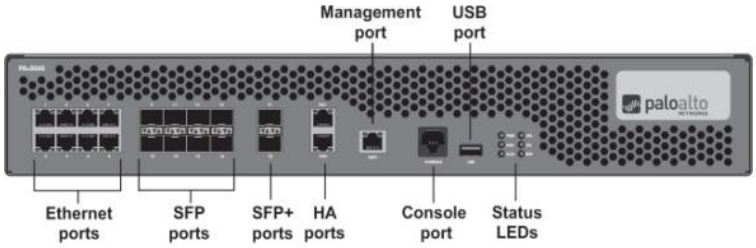


Figure 1: - PA-3060 Front Image

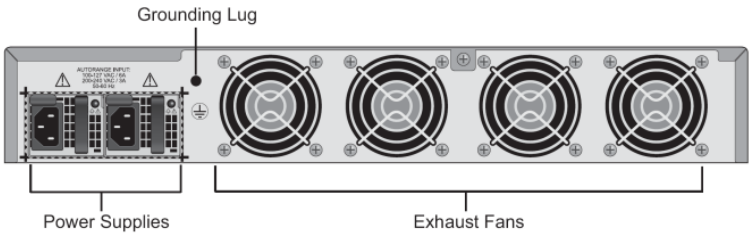


Figure 2: - PA-3060 Back Image

Figure 3 - PA-3060 Front Opacity Shield and Side

Figure 4 - PA-3060 Rear Opacity Shield and Side

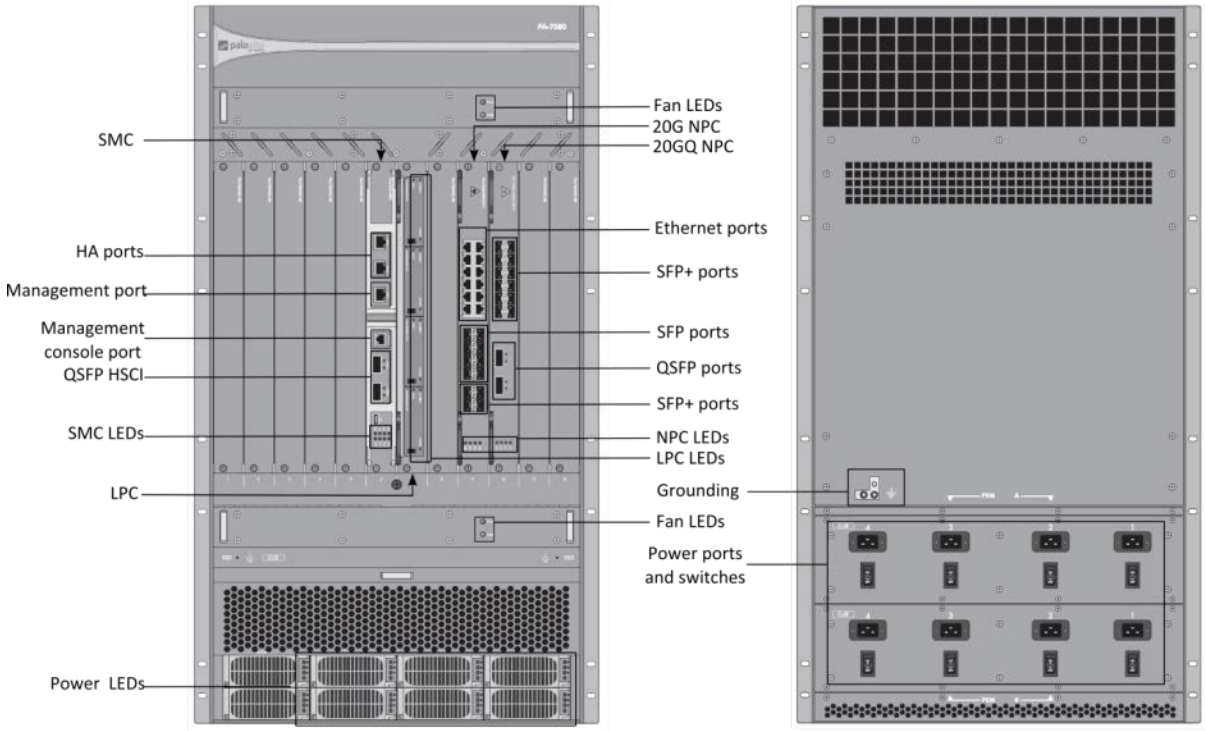


Figure 5 - PA-7080 Interfaces

Figure 6 - PA-7080 Front with Opacity Shield

Figure 7 - PA-7080 Rear

The configurations for this validation are:

Table 2 - Validated Version Information

Module	Part Number	Hardware Version	FIPS Kit Part Number	FIPS Kit Hardware Version	FW
PA-3060	910-000104-00C	Rev. C	920-000138-00A	Rev. A	7.1.3
PA-7080 *	910-000122-00A	Rev. A	920-000119-00A	Rev. A	7.1.3

* Palo Alto Networks PA-7080 firewall is tested with different Network Processing Cards (NPC), and any NPC may be configured for use in the Approved mode of operation.

- 910-000028-00B: PAN-PA-7000-20G-NPC
- 910-000117-00A: PAN-PA-7000-20GQ-NPC
- 910-000137-00A: PAN-PA-7000-20GXM-NPC
- 910-000136-00A : PAN-PA-7000-20GQXM-NPC

Figure 8 depicts the logical block diagram for the modules. The cryptographic boundary includes all of the logical components of the modules and the boundary is the physical enclosure of the firewall.

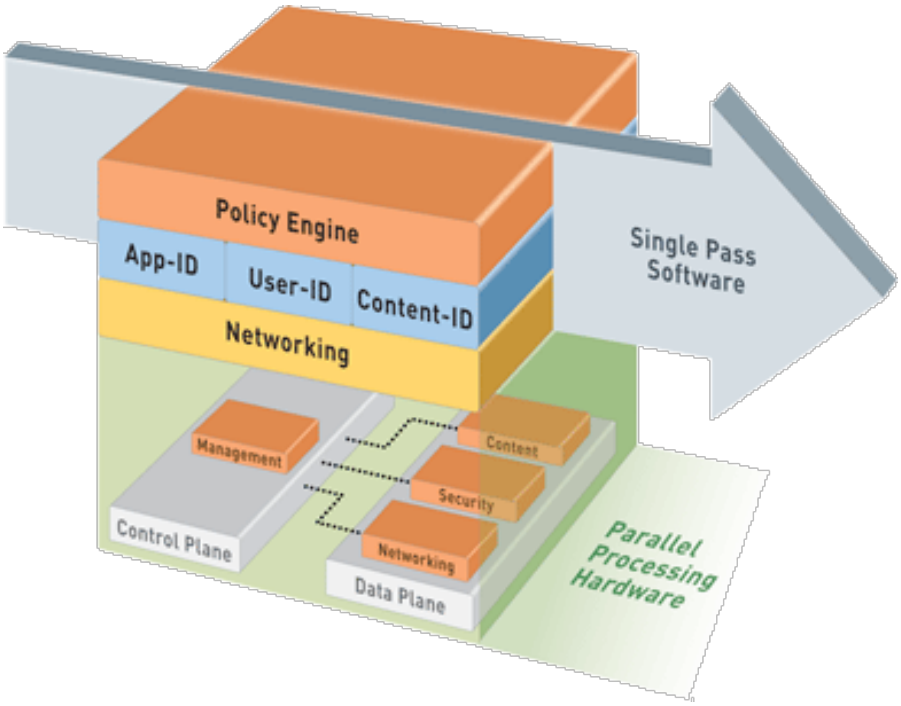


Figure 8 - Logical Diagram

Security Level

The cryptographic modules meet the overall requirements applicable to Level 2 security of FIPS 140-2.

Table 3 - Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	2
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

Modes of Operation

FIPS Approved Mode of Operation

The modules support both a FIPS-CC mode (FIPS Approved mode) and a Non-Approved mode. The following procedure will put the modules into the FIPS-approved mode of operation:

- Install FIPS kit opacity shields and tamper evidence seals according to the Physical Security Policy section. FIPS kits must be correctly installed to operate in the Approved mode of operation. The tamper evidence seals and opacity shields shall be installed for the module to operate in a FIPS Approved mode of operation.
- During initial boot up, break the boot sequence via the console port connection (by pressing the maint button when instructed to do so) to access the main menu.
- Select “Continue.”
- Select the “Set FIPS-CC Mode” option to enter CC mode.
- Select “Enable FIPS-CC Mode”.
- When prompted, select “Reboot” and the module will re-initialize and continue into CC mode (FIPS mode).
- The module will reboot.
- In FIPS-CC mode, the console port is available as a status output port.

- If using RADIUS or TACACS+, configure the service route via an IPSec tunnel. Otherwise, skip this step.

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

- Status output interface will indicate "**** FIPS-CC MODE ENABLED ****" via the CLI session.
- Status output interface will indicate "FIPS-CC mode enabled successfully" via the console port.
- The module will display "FIPS-CC" at all times in the status bar at the bottom of the web interface.

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

- The module will output "FIPS-CC failure"
- The module will reboot and enter a state in which the reason for the reboot can be determined.
- To determine which self-test caused the system to reboot into the error state, connect the console cable and follow the on-screen instructions to view the self-test output.

Approved and Allowed Algorithms

The cryptographic modules support the following FIPS Approved algorithms.

Table 4 - FIPS Approved Algorithms Used in the Module

FIPS Approved Algorithm	CAVP Cert. #
AES: - ECB, CBC, CFB1, CFB8, CFB128, OFB, CTR modes; Encrypt/Decrypt; 128, 192 and 256-bit (AES OFB was tested but is not available for use) AES-CCM - 128-bit AES-GCM - 128 and 256-bit Note: GCM is used compliant with SP 800-52 and used in accordance to Section 4 of RFC 5288 for TLS key establishment. GCM is also compliant with RFC 6071 for use in IPSec.	4020
SP 800-135 KDF – TLS 1.0/1.1/1.2, SNMPv3, SSH, IKEv1/v2*	CVL 848
SP 800-56A except KDF	CVL 849
FIPS186-4 ECDSA Signature Generation: P-256, P-384, P-521	CVL 873
SP 800-56A Section 5.7.1.2 P-256, P-384	CVL 874
SP 800-90A CTR DRBG: AES 256	1198
ECDSA - Key Pair Generation: P-256, P-384 - Signature Generation: P-256, P-384, and P-521 - Signature Verification: P-256, P-384, and P-521	896
HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	2622

FIPS Approved Algorithm	CAVP Cert. #
KTS [SP800-38F Section 3.1] AES-GCM (Key wrapping; key establishment methodology provides between 128 and 256 bits of encryption strength)	AES 4020
KTS [SP800-38F Section 3.1] AES-CBC plus HMAC AES-CTR plus HMAC (Key wrapping; key establishment methodology provides between 128 and 256 bits of encryption strength)	AES 4020 HMAC 2622
FIPS 186-4 RSA : - Key Generation: 2048 and 3072-bit - Signature Generation: 2048 and 3072-bit - Signature Verification: 1024, 2048, and 3072-bit	2064
SHA-1, SHA-256, SHA-384, SHA-512	3316
SP 800-56A rev2 EC Diffie-Hellman Exchange (with CVL Certs. #848 and #849, key agreement; key establishment methodology provides 128 or 192 bits of encryption strength)	Vendor Affirmed

The cryptographic modules support the following non-FIPS Approved algorithms that are allowed for use in FIPS-CC mode.

Table 5 - FIPS Allowed Algorithms Used in the Module

FIPS Allowed Algorithm
Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength)
MD5 (within TLS)
NDRNG (used to seed SP800-90A DRBG) This provides a minimum of 256 bits of entropy.
RSA (key wrapping, key establishment methodology provides 112 or 128 bits of encryption strength)

Table 6 - Supported Protocols in FIPS Approved Mode

Supported Protocols*
TLSv1.0, 1.1 and v1.2
SSHv2
IPSec, IKEv1 and v2
SNMPv2/v3

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

Non-Approved, Non-Allowed Algorithms

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

Table 7 - Non-Approved Mode of Operation

Non-Approved Algorithms in Non-FIPS mode
Hashing: MD5, RIPEMD
Encrypt/Decrypt: Blowfish, Camellia, CAST, DES, RC4, SEED, Triple-DES
Message Authentication: HMAC-MD5, HMAC-RIPEMD, UMAC
Digital Signatures (non-Approved strengths or SHA-1 in Signature Generation): DSA, ECDSA, RSA
Key Exchange (non-Approved strengths): Diffie-Hellman (768, 1024, and 1536 bit) EC Diffie-Hellman (sect571r1, sect571k1, secp521r1, sect409k1, sect409r1, sect283k1, sect283r1, secp256k1, sect239k1, sect233k1, sect233r1, secp224k1, secp224r1, sect193r1, sect193r2, secp192k1, secp192r1, sect163k1, sect163r1, sect163r2, secp160k1, secp160r1, secp160r2) RSA: Less than 2048-bit modulus

Ports and Interfaces

The modules are multi-chip standalone modules with ports and interfaces as shown below.

Table 8- PA-3060 FIPS 140-2 Ports and Interfaces

Interface	PA-3060 Qty	FIPS 140-2 Designation	Name and Description
RJ45	1	Data input, control input, data output, status output	Console port
RJ45	1	Data input, control input, data output, status output	Out of band management
RJ45	2	Data input, control input, data output, status output	10/100/1000 HA Ethernet interface
SFP+	2	Data input, control input, data output, status output	Ethernet optical 10-gigabit interface

Interface	PA-3060 Qty	FIPS 140-2 Designation	Name and Description
SFP	8	Data input, control input, data output, status output	Ethernet optical gigabit interface
RJ45	8	Data input, control input, data output, status output	10/100/1000 Ethernet interface
100-240 V	2	Power input	Power interface
LEDs	6	Status output	Status indicators
USB	1	Disabled except for power	Future Use

Table 9 - PA-7080 FIPS 140-2 Ports and Interfaces

Interface	Chassis[a] Qty	20G or 20GXM NPC [b] Qty	20GQ or 20GQXM NPC [b] Qty	FIPS 140-2 Designation	Name and Description
RJ45	1	N/A	N/A	Data input, control input, data output, status output	Console port
RJ45	1	N/A	N/A	Data input, control input, data output, status output	Out of band management
RJ45	N/A	12	N/A	Data input, control input, data output, status output	10/100/1000 Ethernet Interfaces
SFP	N/A	8	N/A	Data input, control input, data output, status output	Ethernet optical gigabit interfaces
SFP+	N/A	4	12	Data input, control input, data output, status output	Ethernet optical 10-gigabit interface
RJ45	2	N/A	N/A	Data input, control input, data output, status output	10/100/1000 HA Ethernet interface
HSCI	2	N/A	N/A	Data input, control input, data output, status output	QSFP HA interface
QSFP	N/A	N/A	2	Data input, control input, data output, status output	IEEE 802.3ba interface
100-240 V	4	N/A	N/A	Power input	Power interface
LEDs	52[f]	52[c]	32[c]	Status output	Status indicators

USB	1	N/A	N/A	Disabled except for power	Used in manufacturing

a. The PA-7000 series chassis includes two cards that are installed in the front slots of the chassis. These cards include the following: The Switch Management Card (SMC) provides management connectivity to the chassis and the Log Processing Card (LPC) handles all log processing and log storage for the firewall.

b. NPC (Network Processing Card) - The PA-7080 may contain up to ten (10) NPC cards. At least one (1) Network Processing Cards (NPC) must be installed before the firewall can process data traffic. The PA-7000-20GXM-NPC and PA-7000-20GQXM-NPC doubles the memory of the PA-7000-20G-NPC and PA-7000-20GQ-NPC respectively, enabling support for eight million sessions (up from four million).

c. NPC - With the four (4) standard status LED, each networking interface contains two (2) LED, the link status and activity LED.

d. PA-7080 - Status LED count (40) includes the following: 4 for fan status, 12 for the LPC and 20 for the SMC, 16 for power supplies.

Identification and Authentication Policy

Assumption of Roles

The modules support four distinct operator roles, User and Cryptographic Officer (CO), Remote Access VPN, and Site-to-site VPN. The cryptographic modules enforce the separation of roles using unique authentication credentials associated with operator accounts. The modules support concurrent operators.

The modules do not provide a maintenance role or bypass capability.

Table 10 - Roles and Required Identification and Authentication

Role	Description	Authentication Type	Authentication Data
CO	This role has access to all configuration, show status and update services offered by the modules. Within the PAN-OS software, this role maps to the "Superuser" administrator role.	Identity-based operator authentication	Username/password and/or certificate based authentication
User	This role has limited access to services offered by the modules. This role does not have access to modify or view the passwords associated with other administrator accounts, it may not view CSPs of any type stored on the module. The User may change their own password. Within the PAN-OS software, this role maps to the "Superuser (read-only)" administrator role (also referred to as "Superreader").	Identity-based operator authentication	Username/password and/or certificate based authentication
Remote Access VPN (RA VPN)	Remote user accessing the network via VPN.	Identity-based operator authentication	Username/password and/or certificate based authentication
Site-to-site VPN (S-S VPN)	Remote VPN device establishing a VPN session to facilitate access to the network.	Identity-based operator authentication	IKE/IPSec Pre-shared keys - Identification with the IP Address and authentication with the Pre-Shared Key or certificate based authentication

Table 11 - Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Username and Password	Minimum length is 6 characters (95 possible characters). The probability that a random attempt will succeed or a false acceptance will occur is $1/(95^6)$ which is less than 1/1,000,000. The probability of successfully authenticating to the module within one minute is $10/(95^6)$, which is less than 1/100,000. The firewall's configuration supports at most ten failed attempts to authenticate in a one-minute period.
Certificate based authentication	The security modules support certificate-based authentication using RSA 2048, RSA 3072, ECDSA P-256, P-384, or P-521. For RSA, 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 $3,600,000/(2^{112})$, which is less than 1/100,000. The firewall supports at most 60,000 new sessions per second to authenticate in a one-minute period. For ECDSA, the minimum equivalent strength supported is 128 bits. The probability that a random attempt will succeed is $1/(2^{128})$ which is less than 1/1,000,000. The probability of successfully authenticating to the module within a one minute period is $3,600,000/(2^{128})$, which is less than 1/100,000. The firewall supports at most 60,000 new sessions per second to authenticate in a one-minute period.
IKE/IPSec pre-shared keys	The 160 bit key length supports 2^{160} different combinations. The probability of successfully authenticating to the module is $1/(2^{160})$, which is less than 1/1,000,000. The number of authentication attempts is limited by the number of new connections per second supported (120,000) on the fastest platform of the Palo Alto Networks firewalls. The probability of successfully authenticating to the module within a one minute period is $7,200,000/(2^{160})$, which is less than 1/100,000.

Access Control Policy

Roles and Services

The Approved and non-Approved mode of operation provide identical services. While in the Approved mode of operation, all CO and User 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 services listed below are also available in the non-Approved mode. In the Non-Approved mode SSH, TLS, and VPN processes will use non-Approved Algorithms and Approved algorithms with non-Approved strength.

Table 12 - Authenticated Service Descriptions

Service	Description
Security Configuration Management	Configuring and managing cryptographic parameters and setting/modifying security policy, creating User accounts and additional CO accounts, as well as configuring usage of third party external HSMs.
Other Configuration	Networking parameter configuration, logging configuration, and other non-security relevant configuration.
View Other Configuration	Read-only of non-security relevant configuration (see above).
Show Status	View status via the web interface, command line interface or VPN session.
VPN	Provide network access for remote users or site-to-site connections.
Firmware update	Provides a method to update the firmware on the firewall.

Note: Additional information on the services the module provides can be found at https://www.paloaltonetworks.com/documentation.html

Table 13 - Authenticated Services

Service	Crypto Officer	User	RA VPN	S-S VPN
Security Configuration Management	Y	Y[(a)]	N	N
Other Configuration	Y	N	N	N
View Other Configuration	Y	Y	N	N
Show Status	Y	Y	Y	Y

VPN	N	N	Y	Y
Firmware update	Y	N	N	N
a. The User role has use of this service only to change their own password				

Unauthenticated Services

The cryptographic module supports the following unauthenticated services:

Table 14 - Unauthenticated Services

Service	Description
Zeroize	The device will overwrite all CSPs.
Self-Tests	Run power up self-tests on demand by power cycling the module.
Show Status (LEDs)	View status of the module via the LEDs.

The zeroization procedure is invoked when the operator exits CC (FIPS) mode. The procedure consists of overwriting keystore files, formatting the harddisk, and overwriting with a reinstalled firmware image. The operator must be in control of the module during the entire procedure to ensure that it has successfully completed. During the zeroization procedure, no other services are available.

Definition of Critical Security Parameters (CSPs)

The modules contain the following CSPs:

Table 15 - CSPs

CSP #	CSP/Key Name	Type	Description
1	RSA Private Keys	RSA	RSA private keys for verification of signatures, authentication or key establishment. (RSA 2048 or 3072-bit)
2	ECDSA Private Keys	ECDSA	ECDSA Private key for verification of signatures and authentication (P-256, P-384 or P-521)
3	TLS PreMaster Secret	TLS Secret	Secret value used to derive the TLS session keys
4	TLS DH Private Components	DH	Diffie-Hellman private FFC or EC component used in TLS (DHE 2048, ECDHE P-256, P-384)

CSP #	CSP/Key Name	Type	Description
5	TLS HMAC Keys	HMAC	TLS integrity and authentication session keys (SHA-1, SHA-256, SHA-384)
6	TLS Encryption Keys	AES	TLS encryption session keys (128 and 256 CBC or GCM)
7	SSH Session Authentication Keys	HMAC	Authentication keys used in all SSH connections to the security module's command line interface.(SHA-1)
8	SSH Session Encryption Keys	AES	Used in all SSH connections to the security module's command line interface. (128, 192, and 256 CBC or CTR)
9	SSH DH Private Components	DH	Diffie-Hellman private component used in key establishment (DHE 2048)
10	S-S VPN IPSec/IKE Authentication Keys	HMAC	(SHA-1, SHA-256, SHA-384, or SHA-512) Used to authenticate the peer in an IKE/IPSec tunnel connection.
11	S-S VPN IPSec/IKE Session Keys	AES	Used to encrypt IKE/IPSec data. These are AES (128, 192, and 256 CBC) IKE keys and (128, 192, and 256 CBC, 128 CCM, 128 and 256 GCM) IPSec keys
12	S-S VPN IPSec/IKE Diffie-Hellman Private Component	DH	Diffie-Hellman (Group 14, 19 and 20) private component used in key establishment
13	S-S VPN IPSEC Pre-Shared Keys	Part of HMAC	Manually distributed by an administrator in the CO role. Used in authentication.
14	RA VPN IPSec Session Keys	AES	(128 CBC, 128 and 256 GCM) Used to encrypt remote access sessions utilizing IPSec.
15	RA VPN IPSec Authentication HMAC	HMAC	(SHA-1) Used in authentication of remote access IPSec data.
16	Firmware Code Integrity Check	HMAC	Used to check the integrity of crypto-related code. (HMAC-SHA-256)
17	Firmware Content Encryption Key	AES-256	Used to decrypt firmware, software, and content.
18	Password	Password	Authentication string with a minimum length of 6 characters.
19	DRBG Seed/State	DRBG	Used by DRBG. The state includes the V and the Key.

CSP #	CSP/Key Name	Type	Description
20	SNMPv3 Secrets	SNMPv3 Secrets	SNMPv3 Authentication Secret and Privacy Secret
21	SNMPv3 Keys	SNMPv3 Keys	AES Privacy key and HMAC-SHA-1 Authentication keys

Note: The CSPs in Volatile memory locations are zeroized by overwrite with a pseudo random pattern followed by read-verify. Intermediate plaintext key material (CSP) is zeroized when it is copied from one to another memory location. All keys (CSPs) are zeroized when they expire. Session keys (CSPs) are zeroized as soon as the associated session has ended/timed out/ or been closed. Private keys (CSPs) are zeroized when their corresponding public keys (certificates) expire.

Definition of Public Keys

The modules contain the following public keys:

Table 16 - Public Keys

Key Name	Description
CA Certificates	Used to extend trust for certificates
ECDSA Public Keys/Certificates	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)
RSA Public Keys/Certificates	RSA Public keys managed as certificates for the verification of signatures, establishment of TLS, operator authentication and peer authentication. (RSA 2048 or 3072-bit)
TLS DH Public Components	Used in key agreement (DHE 2048, ECDHE P-256, P-384)
SSH DH Public Components	Used in key agreement (DHE 2048)
SSH Host Public Key	SSH Host Public Key (RSA 2048)
SSH Client Public Key	SSH Client RSA Public Key (RSA 2048)
S-S VPN - IPSec/IKE Diffie-Hellman Public Component	Used in key agreement (DHE 2048, ECDHE P-256, P-384)
Public Key for Firmware Content Load Test	Used to authenticate firmware and content to be installed on the firewall (RSA 2048)

Definition of CSPs Modes of Access

Table 17 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as:

- **R** = Read: The module reads the CSP. The read access is typically performed before the module uses the CSP.
- **W** = Write: The module writes the CSP. The write access is typically performed after a CSP is imported into the module, or the module generates a CSP, or the module overwrites an existing CSP.
- **Z** = Zeroize: The module zeroizes the CSP.

Table 17 - CSP Access Rights within Roles & Services

Role	Authorized Service	Mode	Cryptographic Key or CSP
CO	Security Configuration Management	RW	1, 2, 3, 4, 5, 6, 7, 8, 9, 16, 17, 18, 19, 20, 21
CO	Other Configuration	RW	1, 2, 3, 4, 5, 6, 7, 8, 9
User	Security Configuration Management	W	18 (operator's own password)
User, CO	Show Status	R	1, 2, 3, 4, 5, 6, 7, 8, 9
Unauthenticated	Zeroize	Z	All CSPs are zeroized.
S-S VPN	VPN	R	10, 11, 12, 13
RA VPN	VPN	R	1, 2, 3, 4, 5, 6, 14, 15
CO	Firmware Update	RW	17
Unauthenticated	Self-Tests	N/A	N/A
Unauthenticated	Show Status (LEDs)	N/A	N/A

Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because 7000 Firewalls do not contain modifiable operational environments. The operational environment is limited since the Module includes a firmware load service to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this module is out of the scope of this validation and require a separate FIPS 140-2 validation.

Security Rules

The module design corresponds to the module security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 2 module.

FIPS 140-2 Security Rules

1. The cryptographic module shall provide four distinct operator roles. These are the User role, Remote Access VPN role, Site-to-site VPN role, and the Cryptographic Officer role.
2. The cryptographic module shall provide identity-based authentication.
3. The cryptographic module shall clear previous authentications on power cycle.
4. When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
5. The cryptographic module shall perform the following tests
    A. Power Up Self-Tests
        1. Cryptographic algorithm tests
            a. AES Encrypt Known Answer Test
            b. AES Decrypt Known Answer Test
            c. AES GCM Encrypt Known Answer Test
            d. AES GCM Decrypt Known Answer Test
            e. AES CCM Encrypt Known Answer Test
            f. AES CCM Decrypt Known Answer Test
            g. RSA Sign Known Answer Test
            h. RSA Verify Known Answer Test
            i. ECDSA Sign Known Answer Test
            j. ECDSA Verify Known Answer Test
            k. HMAC-SHA-1 Known Answer Test
            l. HMAC-SHA-256 Known Answer Test
            m. HMAC-SHA-384 Known Answer Test
            n. HMAC-SHA-512 Known Answer Test
            o. SHA-1 Known Answer Test
            p. SHA-256 Known Answer Test
            q. SHA-384 Known Answer Test

r. SHA-512 Known Answer Test
s. DRBG SP800-90A Known Answer Tests
t. SP 800-90A Section 11.3 Health Tests
u. DH Known Answer Test
v. ECDH Known Answer Test

2. Firmware Integrity Test –verified with HMAC-SHA-256 and ECDSA P-256.

B. Critical Functions Tests
1. N/A

C. Conditional Self-Tests
1. Continuous Random Number Generator (RNG) test – performed on NDRNG and DRBG
2. RSA Pairwise Consistency Test (when a key generation fails, the error message displayed is "Cannot verify key and certificate.")
3. ECDSA Pairwise Consistency Test (when a key generation fails, the error message displayed is "Cannot verify key and certificate.")
4. Firmware Load Test – Verify RSA 2048 with SHA-256 signature on firmware at time of load
5. If any conditional test fails, the module will output a description of the error condition.

6. The operator shall be capable of commanding the module to perform the power-up self-test by cycling power of the module.
7. Power-up self-tests do not require any operator action.
8. Data output shall be inhibited during power-up self-tests, zeroization and error states.
9. Status information does 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 enter or output plaintext CSPs.
15. The module does not output intermediate key generation values.

Vendor imposed security rules:

1. If the cryptographic module remains inactive in any valid role for the administrator specified time interval, the module automatically logs out the operator.
2. 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. This wait period shall be enforced even if the module power is momentarily removed.

Physical Security Mechanisms

The multi-chip standalone modules are production quality containing standard passivation. Chip components are protected by an opaque enclosure. There are tamper evident seals that are applied on the modules by the Crypto-Officer. All unused seals are to be controlled by the Crypto-Officer. The seals prevent removal of the opaque enclosure without evidence. The Crypto-Officer must ensure that the module surface is clean and dry. Tamper evident labels must be pressed firmly onto the adhering surfaces during installation and once applied the Crypto-Officer shall permit 24 hours of cure time for all tamper evident labels. The Crypto-Officer should inspect the seals and shields for evidence of tamper every 30 days. If the seals show evidence of tamper, the Crypto-Officer should assume that the modules have been compromised and contact Customer Support.

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

Refer to Appendix A and B for instructions on installation of the tamper seals and opacity shields.

Refer to Appendix A for instructions on installation of the tamper seals and opacity shields for the PA-3060. The locations of the eight (8) tamper evident seals on the PA-3060 module are shown in Figure 9 through Figure 12.

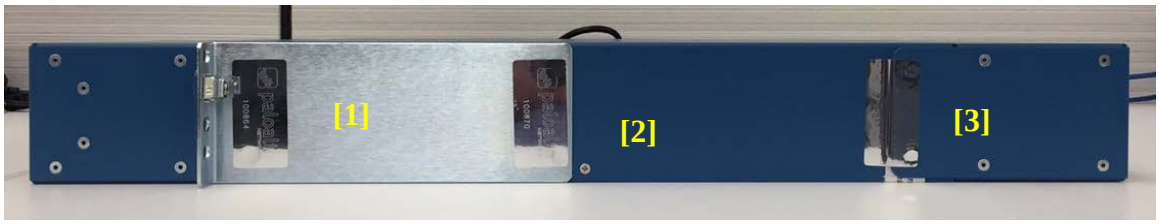


Figure 9 – PA-3060 Right side

Figure 10 – PA-3060 Left side

Figure 11 – PA-3060 Front/Top Tamper Seal Placement

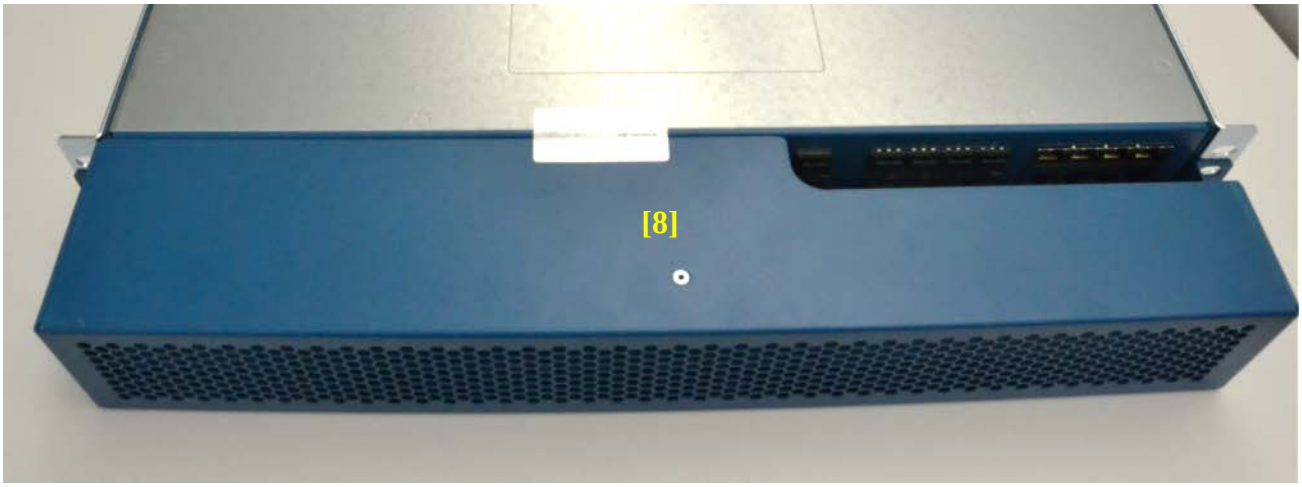


Figure 12 – PA-3060 Front/Bottom Tamper Seal Placement

Refer to Appendix B for instructions on installation of the tamper seals and opacity shields for the PA-7080. The locations of the ten (10) tamper evident seals implemented on the PA-7080 Series modules are shown in Figure 13 through Figure 16.

Figure 13 - PA-7080 Tamper Seal Placement for Rear (6)

Figure 14 - PA-7080 Tamper Seal Placement on Front Fan Trays(2)

Figure 15 - PA-7080 Tamper Seal Placement on Left Side for Front Opacity Shield (1)

Figure 16 - PA-7080 Tamper Seal Placement on Right Side for Front Opacity Shield (1)

Operator Required Actions

Table 18 - Inspection/Testing of Physical Security Mechanisms

Model	Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
PA-3060 and PA-7080	Tamper Evident Seals	30 days	*Verify integrity of tamper evident seals in the locations identified in the FIPS Kit Installation Guide. Seal integrity to be verified within the modules operating temperature range.*
PA-3060	Front and Rear Covers	30 days	*Verify that front and rear covers have not been deformed from their original shape, thereby reducing their effectiveness*
PA-7080	Front Cover, Opacity Lip and Cable Management	30 days	*Verify that front cover, opacity lip and cable management have not been deformed from their original shape, thereby reducing their effectiveness*

Mitigation of Other Attacks Policy

The module has not been designed to mitigate any specific attacks outside of the scope of FIPS 140-2, so these requirements are not applicable.

Definitions and Acronyms

API – Application Programming Interface

App-ID – Application Identification - Palo Alto Networks' ability to identify applications and apply security policy based on the ID rather than the typical port and protocol-based classification.

BGP – Border Gateway protocol – Dynamic routing protocol

CA – Certificate authority

Content-ID – Content Identification – Palo Alto Networks' threat prevention features including Antivirus, Antispyware, and Intrusion Prevention.

CO – Cryptographic Officer

DB9 – Console port connector

DLP – Data loss prevention

Gbps – Gigabits per second

HA – High Availability

HSCI - High Speed Chassis Interconnect

IKE – Internet Key Exchange

IP – Internet Protocol

IPSec – Internet Protocol Security

LDAP – Lightweight Directory Access Protocol

LED – Light Emitting Diode

NDRNG – Non-deterministic random number generator

OCSP – Online Certificate Status Protocol

OSPF – Open Shortest Path First – Dynamic routing protocol

PAN-OS – Palo Alto Networks' Operating System

QoS – Quality of Service

QSFP - Quad Small Form-factor Pluggable

RA VPN – Remote Access Virtual Private Network

RIP – Routing Information Protocol – Dynamic routing protocol

RJ45 – Networking Connector

RNG –Random number generator

S-S VPN – Site to site Virtual Private Network

SFP – Small Form-factor Pluggable Transceiver

SSL – Secure Sockets Layer

TLS – Transport Layer Security

USB – Universal Serial Bus

User-ID – User Identification – Palo Alto Networks' ability to apply security policy based on who initiates the traffic rather than the typical IP-based approach.

VPN – Virtual Private Network

XFP – 10 Gigabit Small Form Factor Pluggable Transceiver

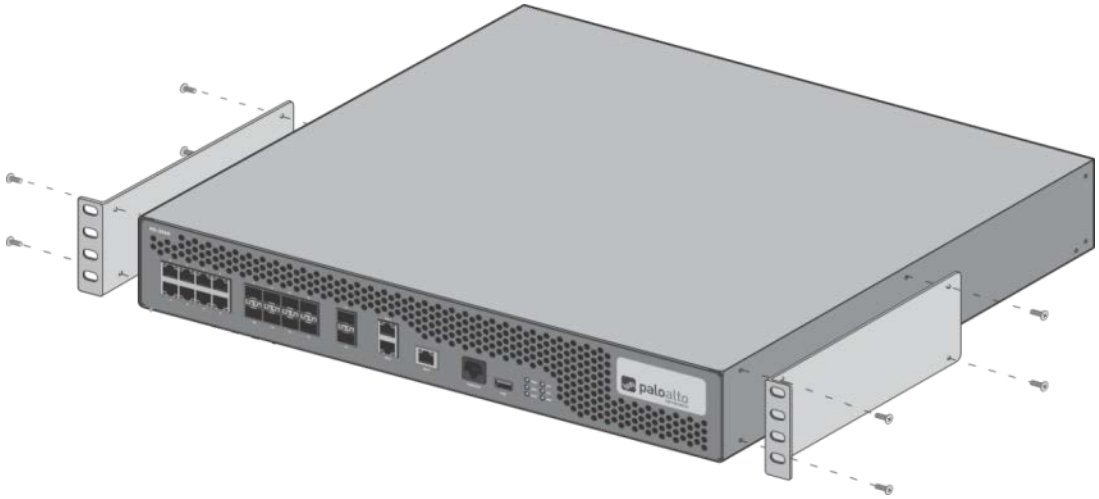
XML – Extensible Markup Language

Reference Documents

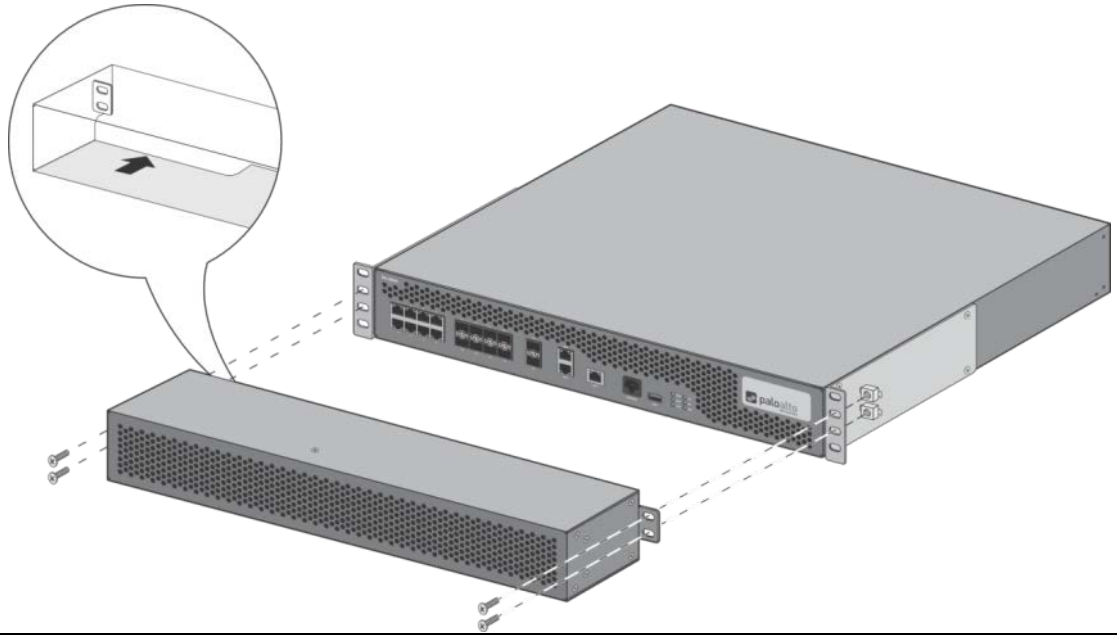
FIPS 140-2 - FIPS Publication 140-2 Security Requirements for Cryptographic Modules

Appendix A - PA-3060 - FIPS Accessories/Tamper Seal Installation (8 Seals)

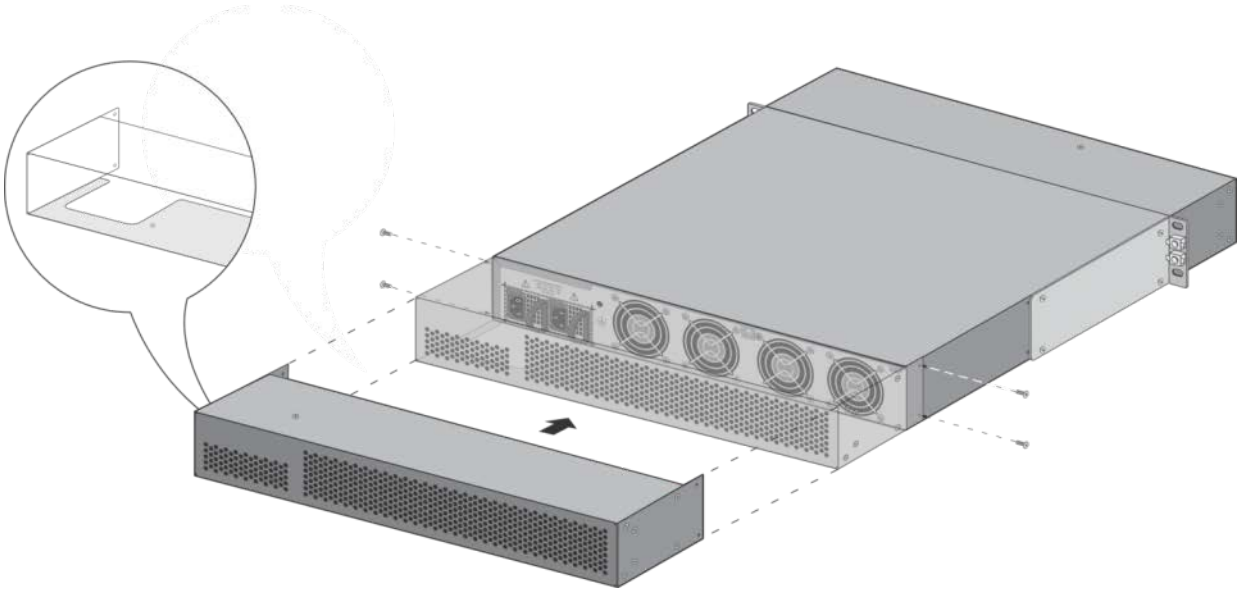
1. From the front of the PA-3060, attach the Left and Right Front Cover brackets using the screws provided.



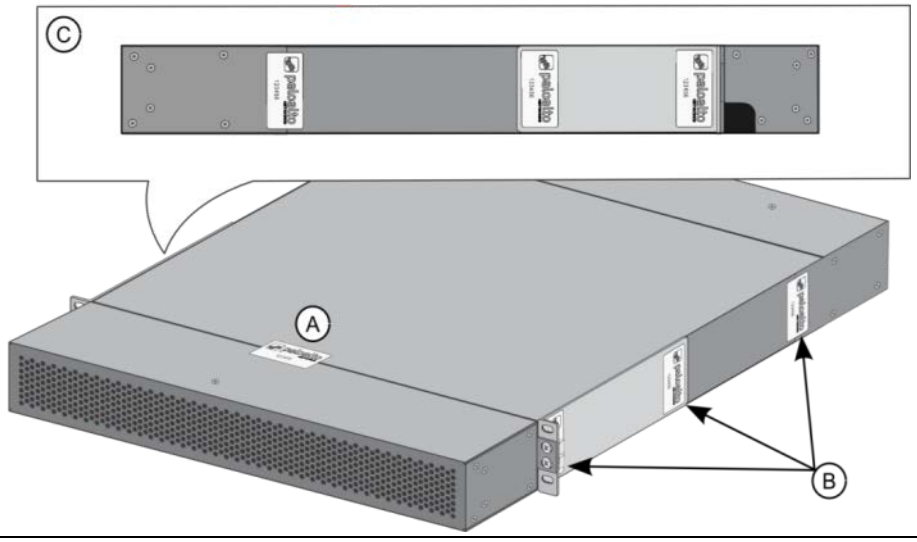
2. Attach Front cover to the front of the PA-3060 using the brackets and the supplied bolts and nuts. Ensure the gap in the cover is positioned below the networking interfaces.



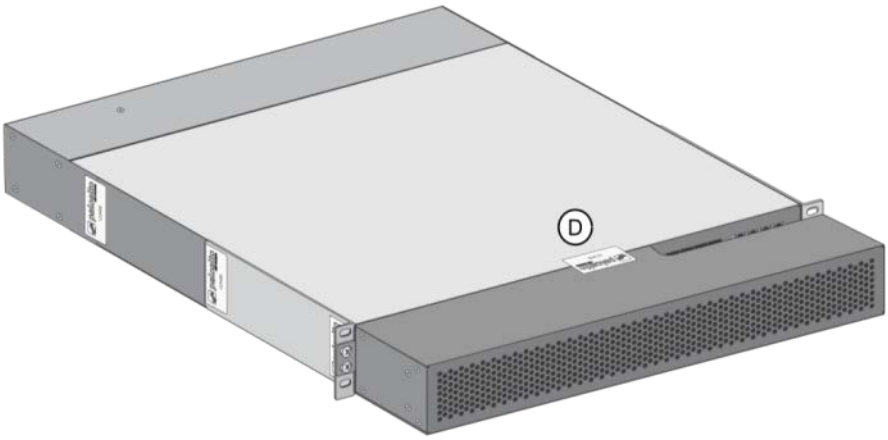
3. Attach Rear Cover to the rear of the PA-3060. Ensure the gap in the cover is positioned below the power supplies.



4. Affix tamper evident labels as follows.
    A. Attach a tamper label to the top of the module overlapping the front opacity shield and the PA-3060.
    B. Attach three (3) labels to the right side of the PA-3060 covering each screw used to attach the front bracket and rear opacity cover.
    C. Attach three (3) labels to the left side of the PA-3060 covering each screw used to attach the front bracket and rear opacity cover.

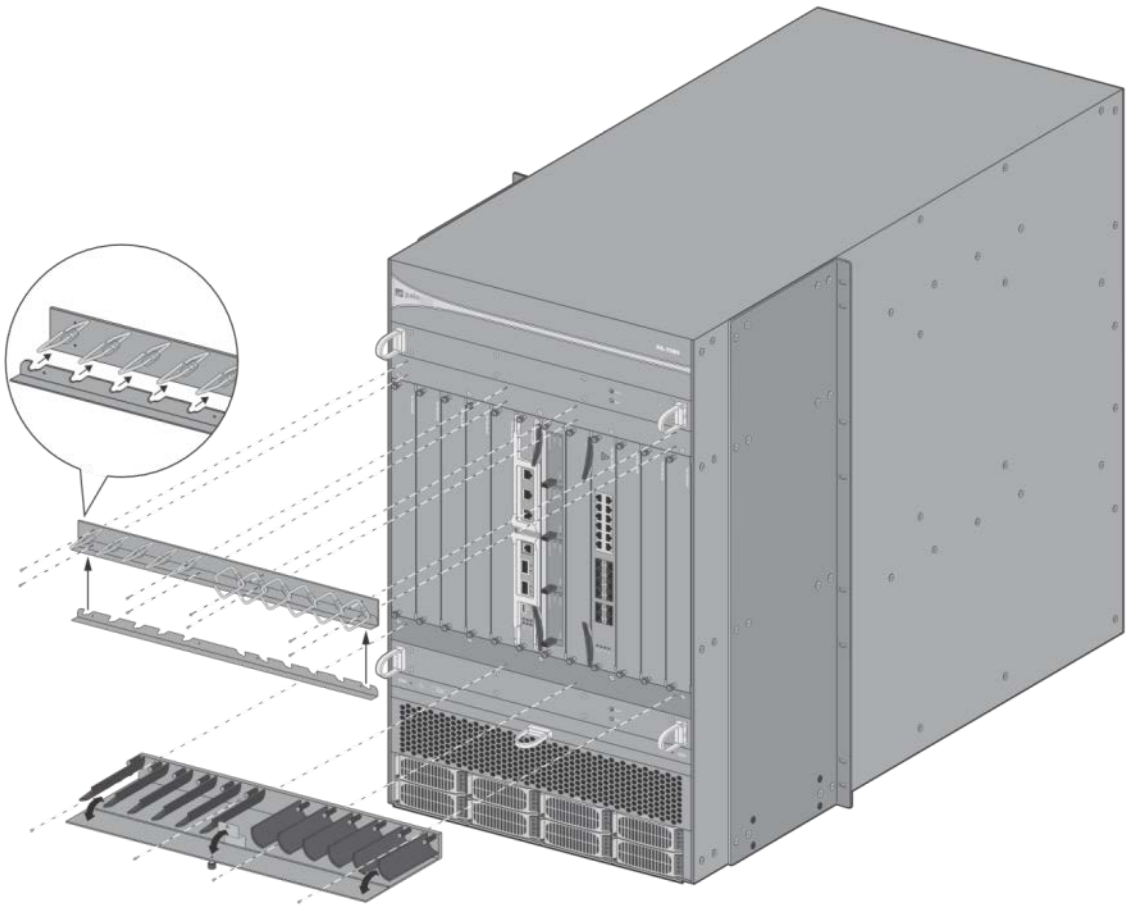


5. Viewing the bottom of the PA-3060.
   D. Attach a tamper label overlapping the front opacity shield and the PA-3060.

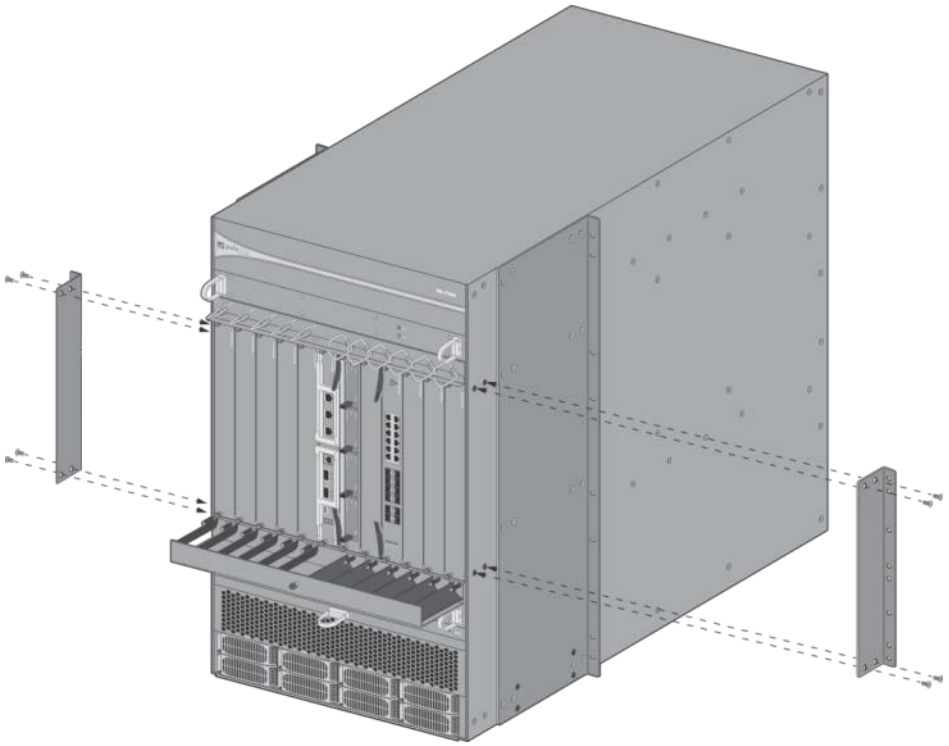


Appendix B - PA-7080 - FIPS Accessories/Tamper Seal Installation (10 Seals)

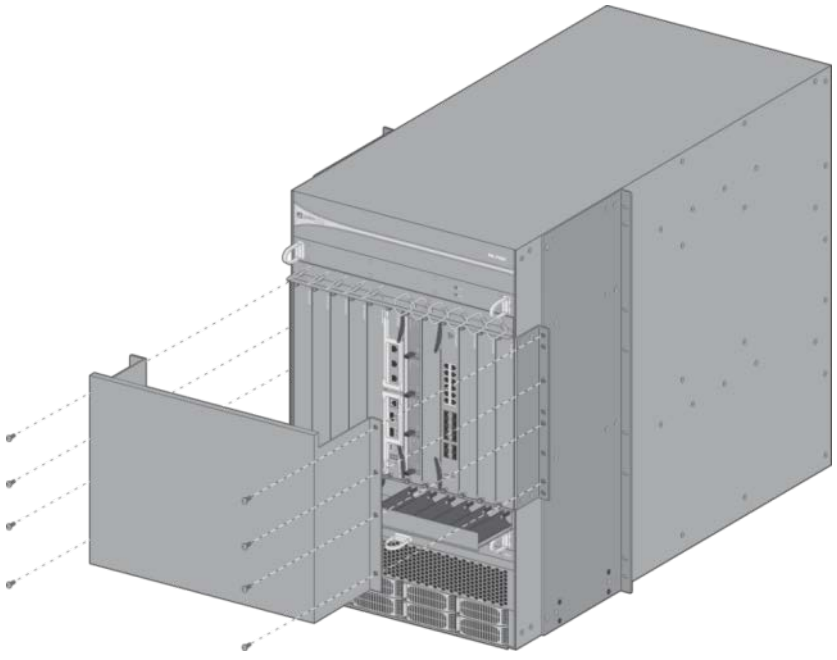
1. Using the supplied screws attach the Cable Manger Kit with upper opacity lip to the front of the PA-7080, as shown.



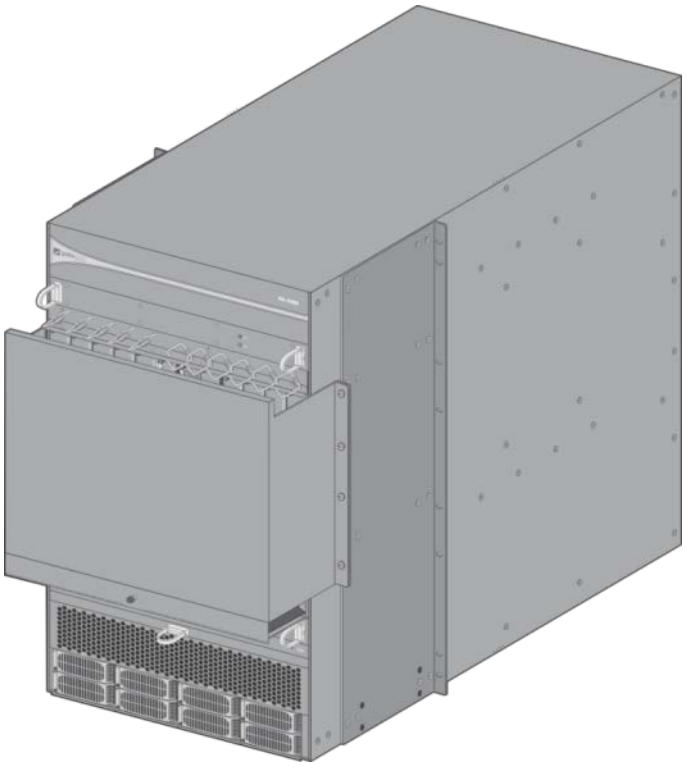
2. Using the supplied screws, attach the Left and Right Front Cover brackets to the sides of the PA-7080, as shown.



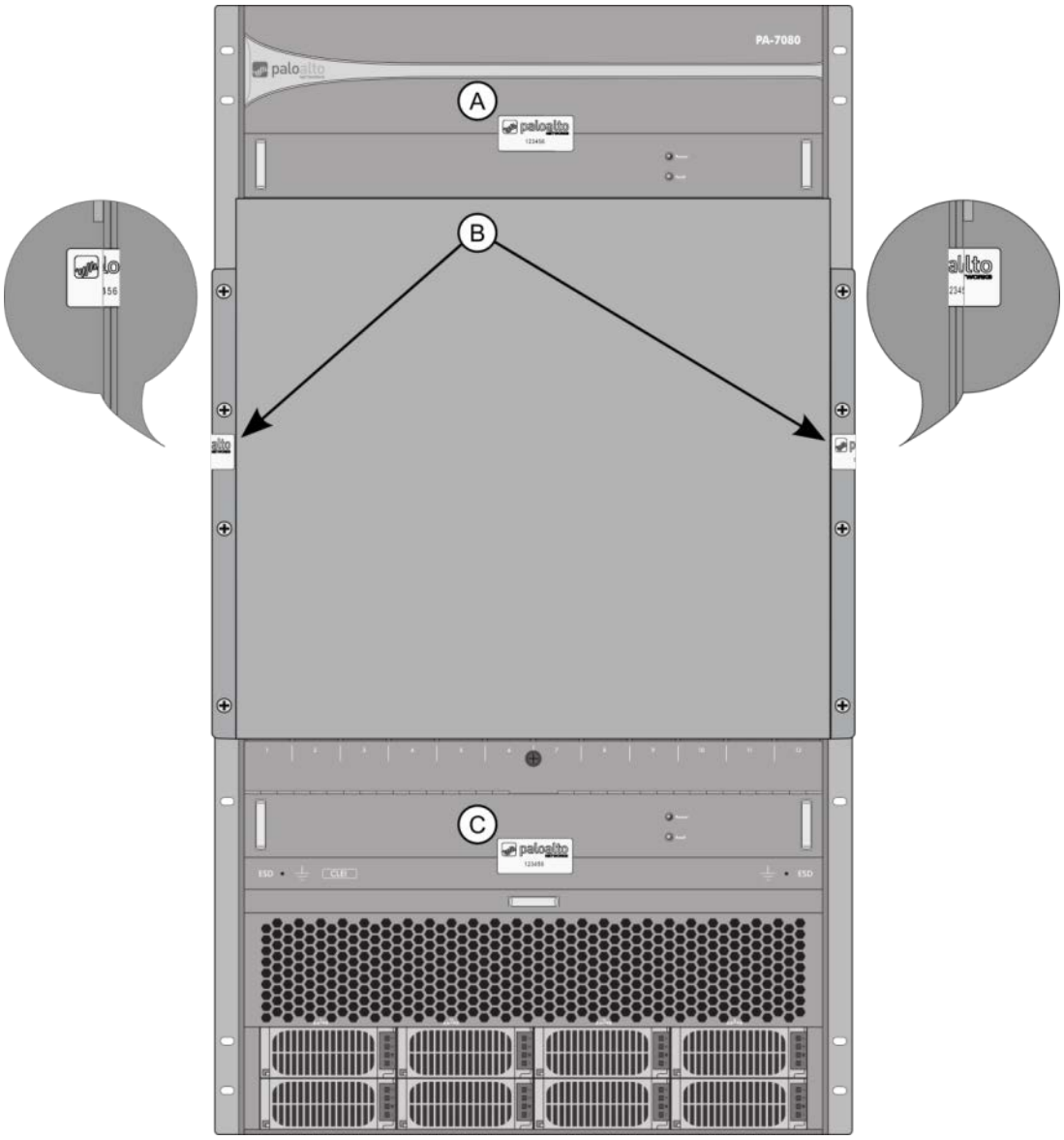
3. Using the supplied screws attach front opacity shield to the PA-7080 as shown.



4. The final assembly for the PA-7080 with the FIPS kit is as shown.



5. Facing the front of the PA-7080:
   A. Affix one (1) label to the front and center of the exhaust fan tray. Ensure the label overlaps the seam with the front PA-7080 branding panel as shown. (1 total)
   B. Affix one (1) label to the left and right outer edge of mounting flanges for the front opacity shield. Labels should fold over the edge of the cover flange and mounting bracket onto the side of the PA-7080. (2 total)
   C. Affix one (1) label to the front and center of the air intake fan tray. Ensure the label overlaps the seam with the PA-7080 electrostatic discharge port panel as shown. (1 total)



6. Facing the rear of the PA-7080;
   D. Affix one (1) label to the left and right outer edge of the upper back panel. Labels should be placed just below the rear exhaust vent as shown. Labels should wrap around onto the sides of the PA-7080 (2 total).
   E. Affix one (1) label to the left and right outer edges of each power entry module as shown. Labels should wrap around onto the sides of the PA-7080 (4 total).