Palo Alto Networks, Inc.

PAN-OS 11.1/11.2 running on PA-400 Series, PA-800 Series, PA-1400 Series, PA-3200 Series, PA-3400 Series, PA-5200 Series, PA-5400 Series, PA-5450, PA-7000 Series, and PA-7500 NGFWs

FIPS 140-3 Non-Proprietary Security Policy

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

This document may freely be reproduced and distributed in its entirety.

The table below provides the security levels of the various sections of FIPS 140-3 in relation to the Palo Alto Networks Hardware Next-Generation Firewalls that include the on PA-400 Series, PA-800 Series, PA-1400 Series, PA-3200 Series, PA-3400 Series, PA-5200 Series, PA-5400 Series, PA-5450, PA-7000 Series, and PA-7500.

1.2 Security Levels

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

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The module provides 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.

Module Type: Hardware

Module Embodiment: Multi-Chip Standalone

Module Characteristics :

Cryptographic Boundary:

The cryptographic boundary is defined as the entire chassis unit's physical perimeter encompassing the "top," "front," "left," "right," "rear" and "bottom" surfaces of the case, and shown in the figures below and in the Physical Security section. These modules are described in more detail further below in this section.

PA-410

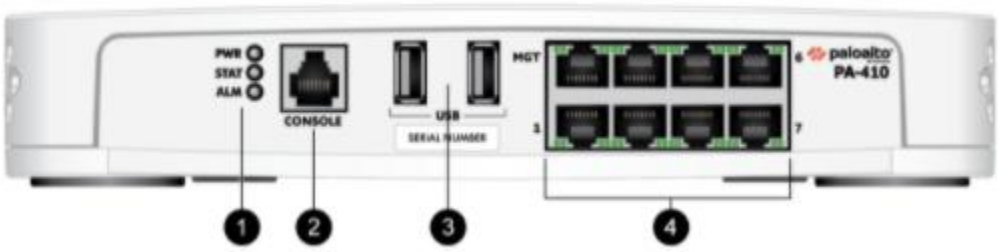


Figure 1 - PA-410 Front

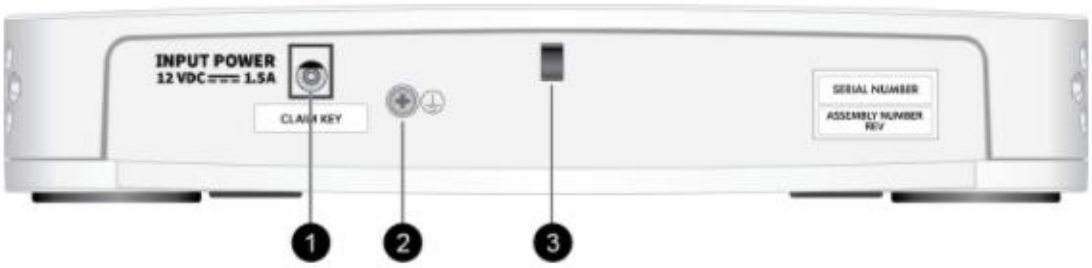
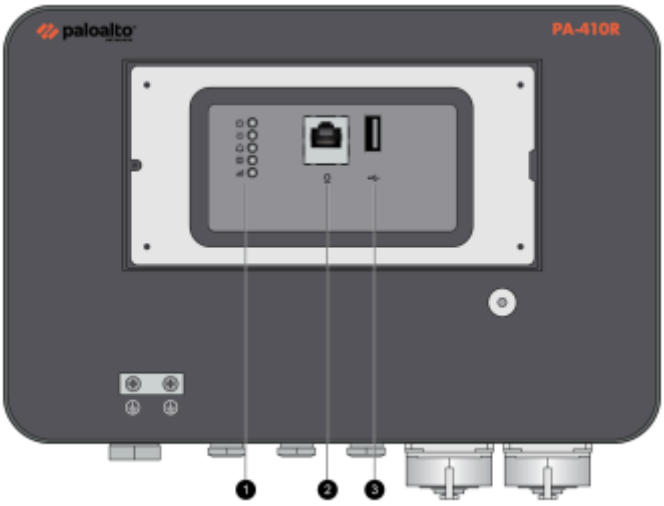


Figure 2 - PA-410 Rear

PA-410R/PA-410R-5G



PA-415 / PA-445

Figure 3 - PA-415/445 Front

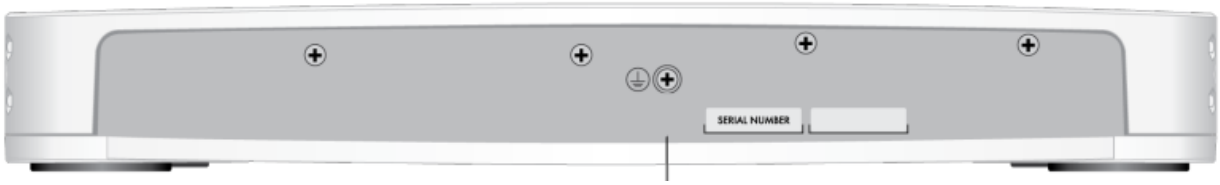


Figure 4 - PA-415/445 Rear

PA-415-5G

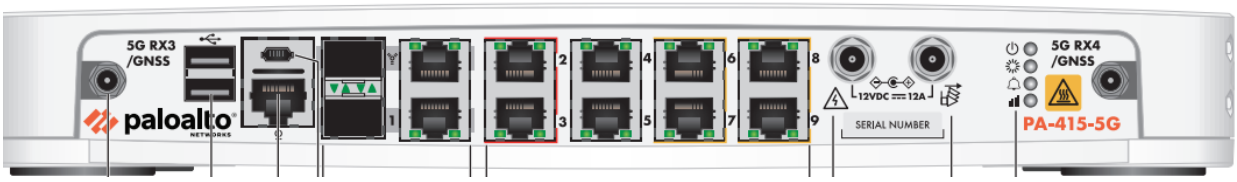


Figure 5 - PA-415-5G Front

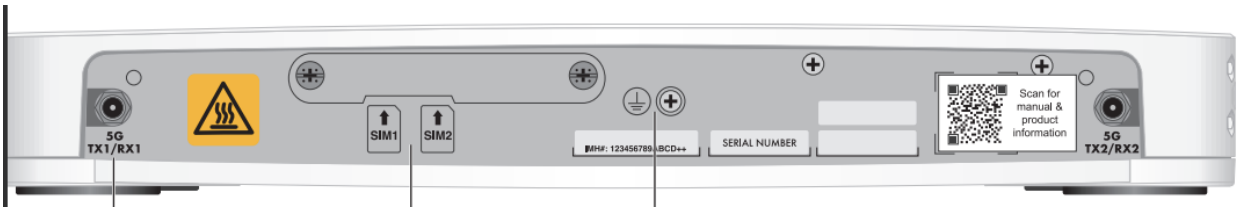


Figure 6 - PA-415-5G Rear

PA-450R

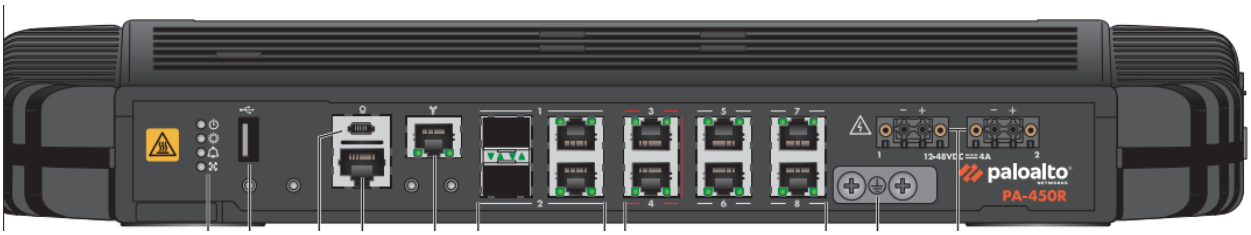


Figure 7 - PA-450R Front

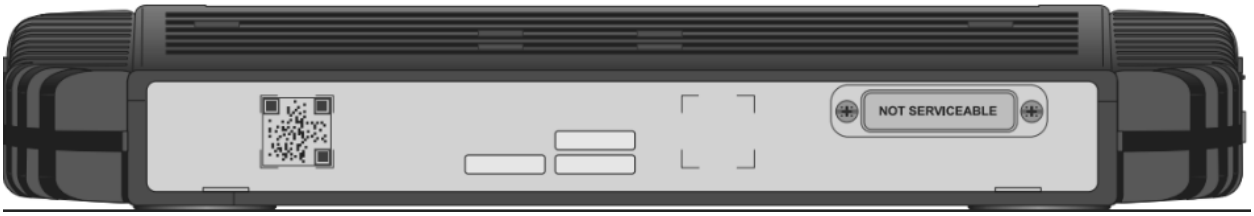


Figure 8 - PA-450R Rear

PA-450R-5G

Figure 9 - PA-450R-5G Front

Figure 10 - PA-450R-5G Rear

PA-455

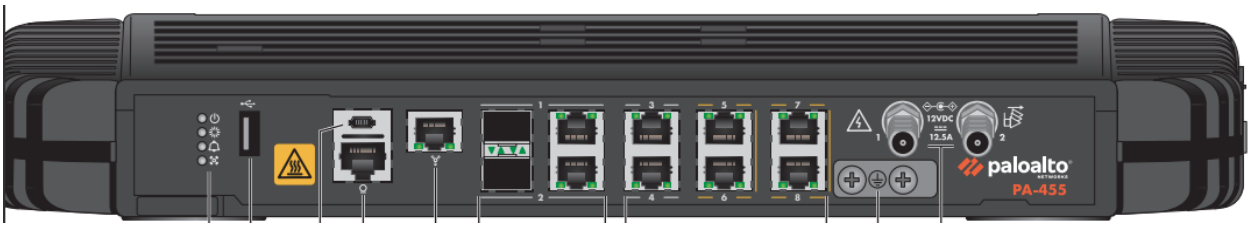


Figure 11 - PA-455 Front

Figure 12 - PA-455 Rear

PA-455-5G

Figure 13 - PA-455-5G Front

Figure 14 - PA-455-5G Rear

PA-440/PA-450/PA-460

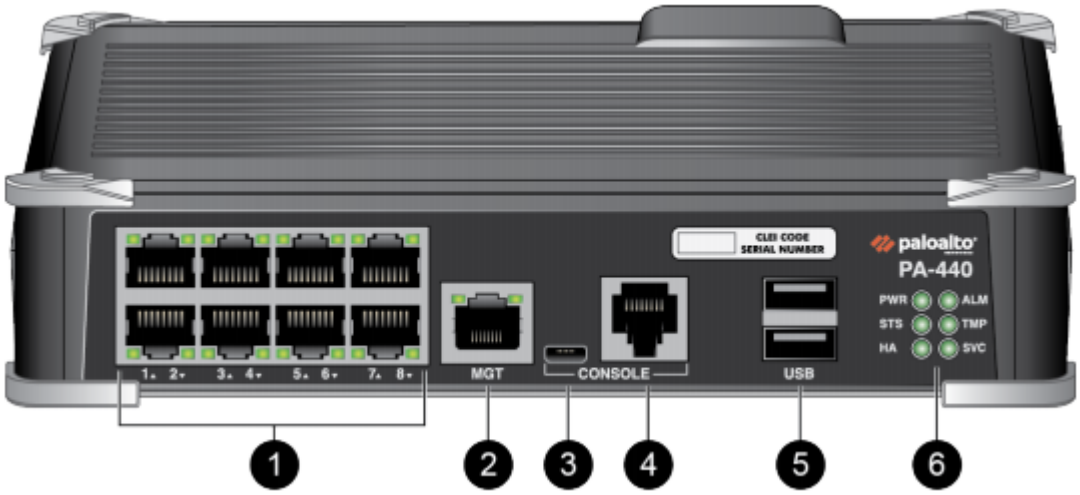


Figure 15 - PA-400 Front (PA-440/450/460 front panels are identical)

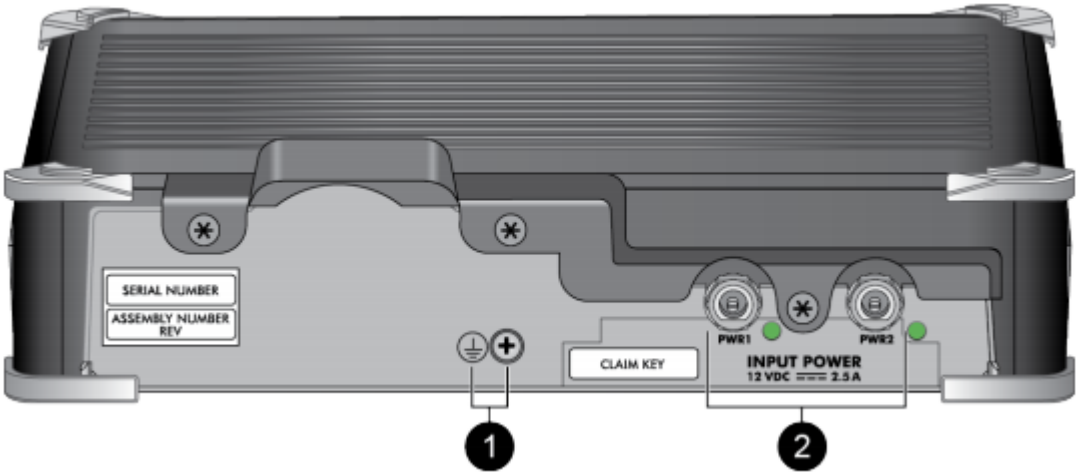


Figure 16 - PA-400 Rear (PA-440/450/460 rear panels are identical)

PA-1400 Series

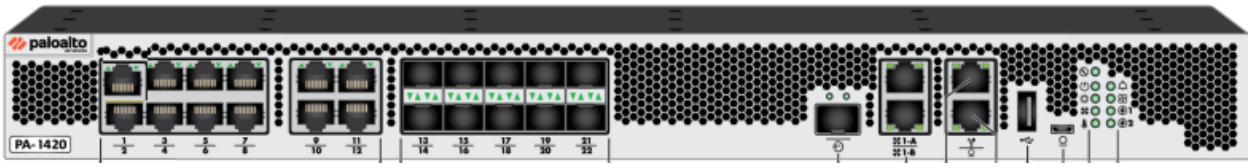


Figure 17 - PA-1400 Series Front

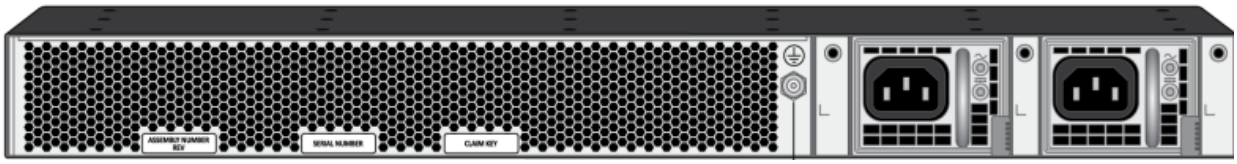


Figure 18 - PA-1400 Series Rear

PA-3200 Series

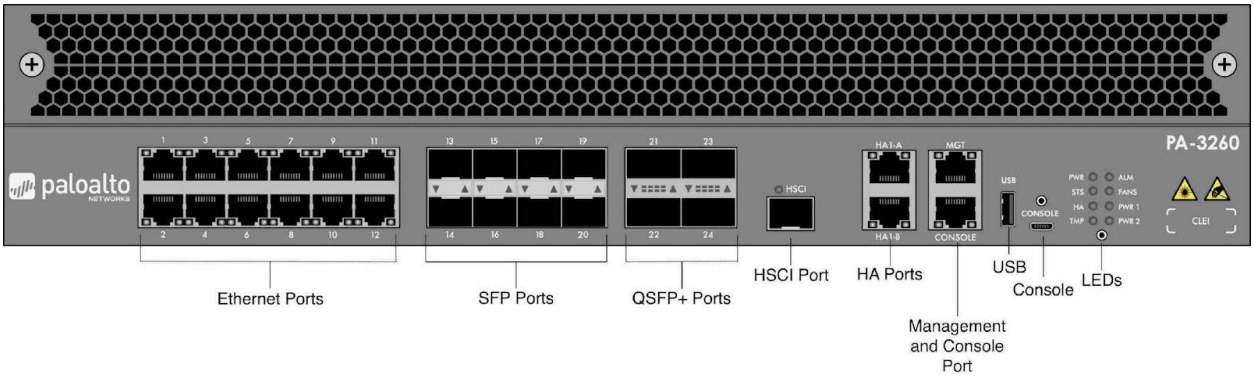


Figure 19 - PA-3200 Series Front

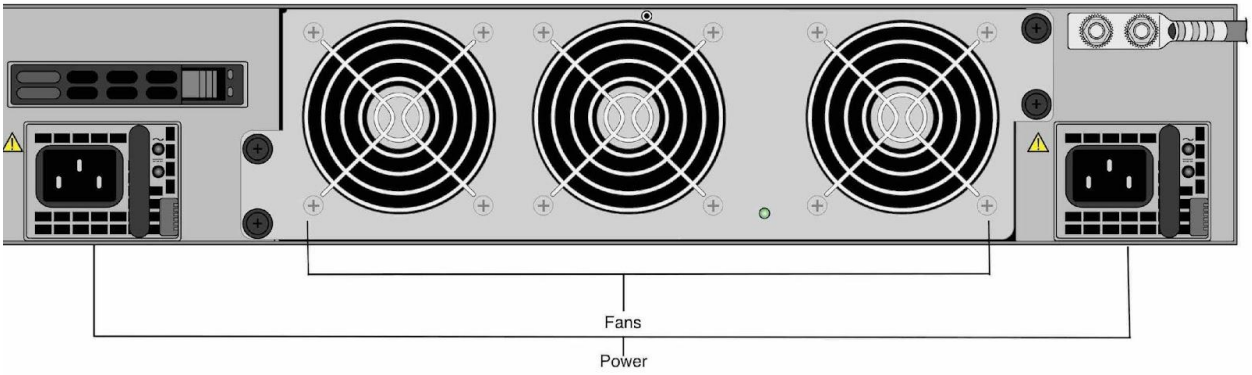


Figure 20 - PA-3200 Series Rear

PA-3400 Series

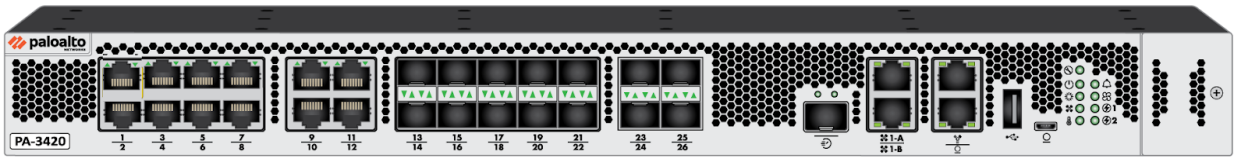


Figure 21 - PA-3410/3420 Front

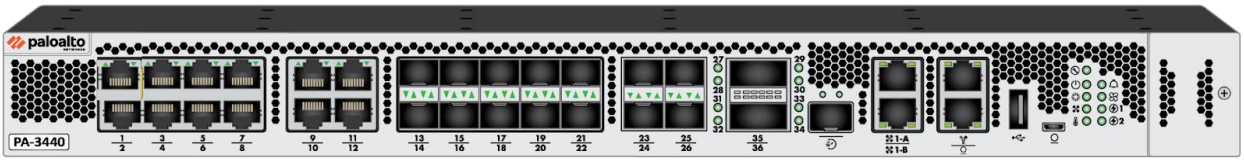


Figure 22 - PA-3430/3440 Front

Figure 23 - PA-3400 Rear

PA-5200 Series

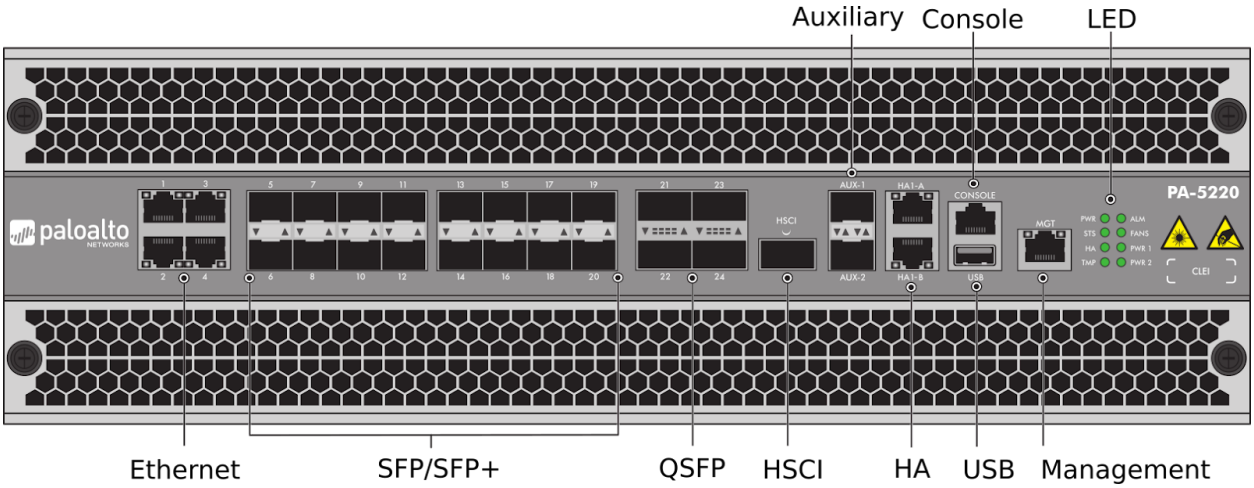


Figure 24 - PA-5200 Series Front

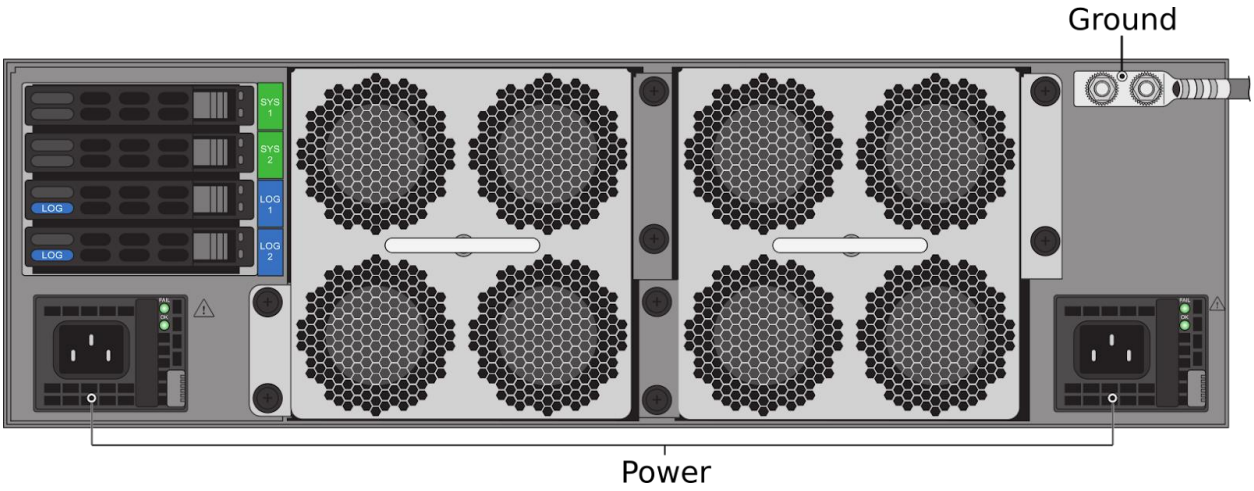


Figure 25 - PA-5200 Rear

PA-5400 Series

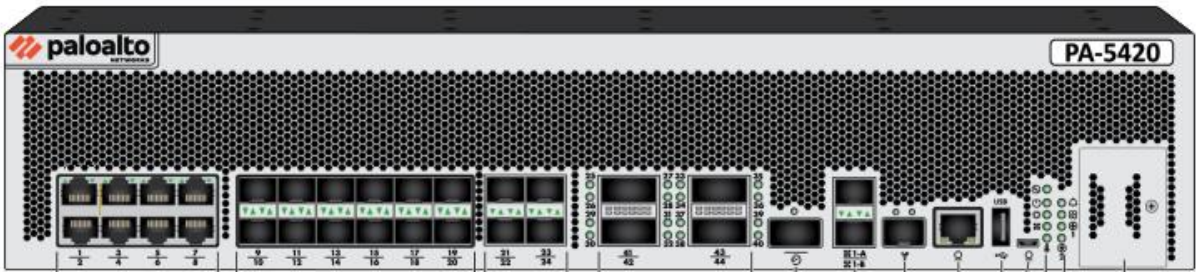


Figure 26 - PA-5410/5420/5430/5440/5445 Front (Note: All modules are identical)

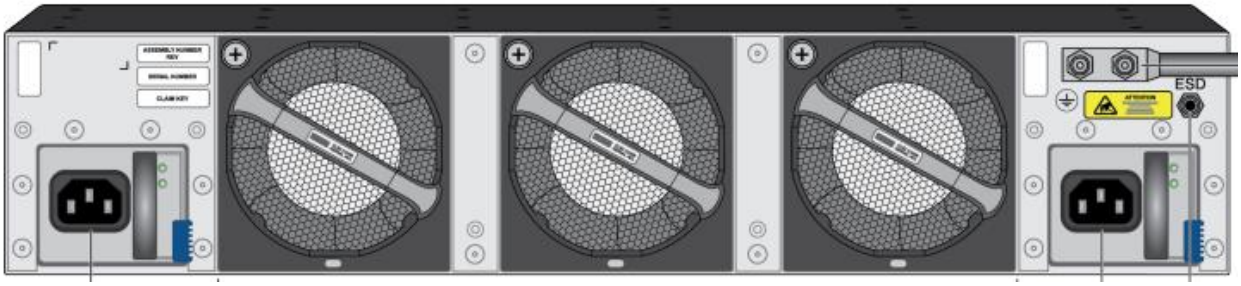


Figure 27 - PA-5410/5420/5430/5440/5445 Rear (Note: All modules are identical)

PA-5450

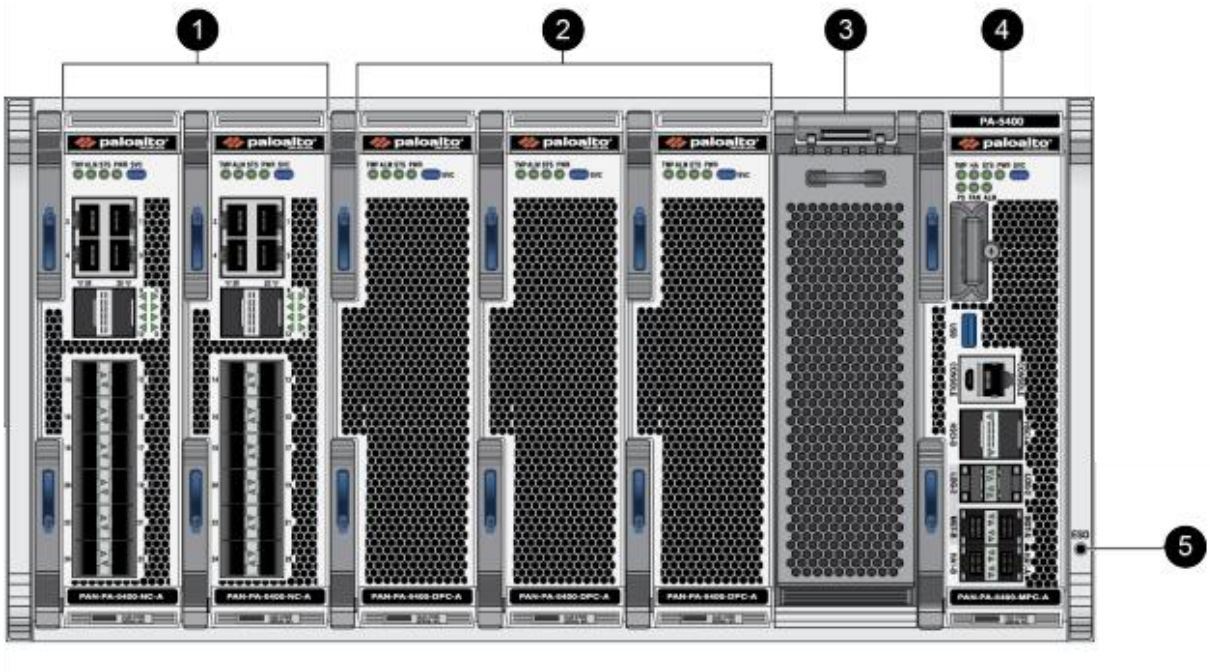


Figure 28 - PA-5450 Front

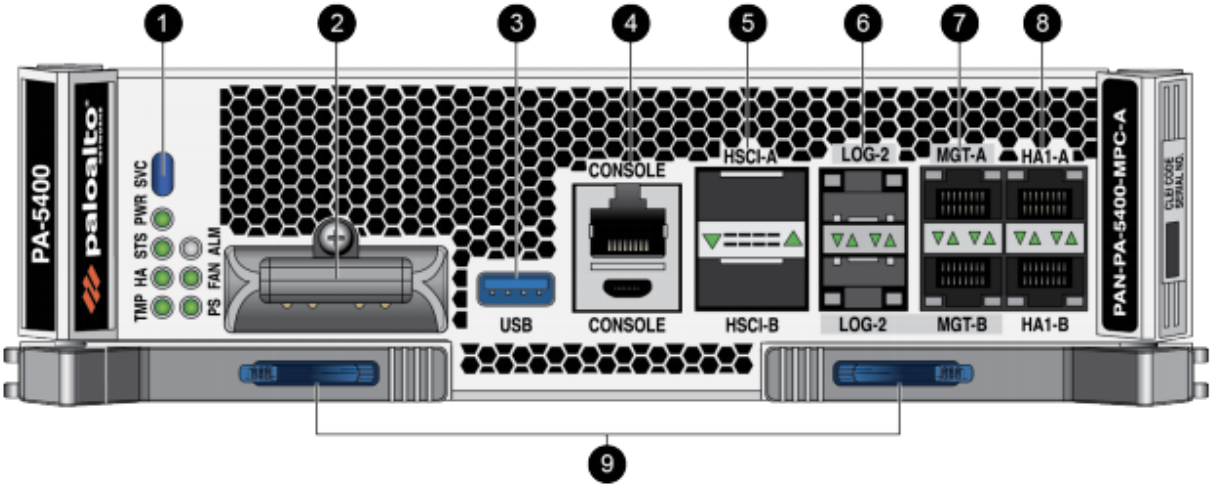


Figure 29 - PA-5450 Management Processor Card

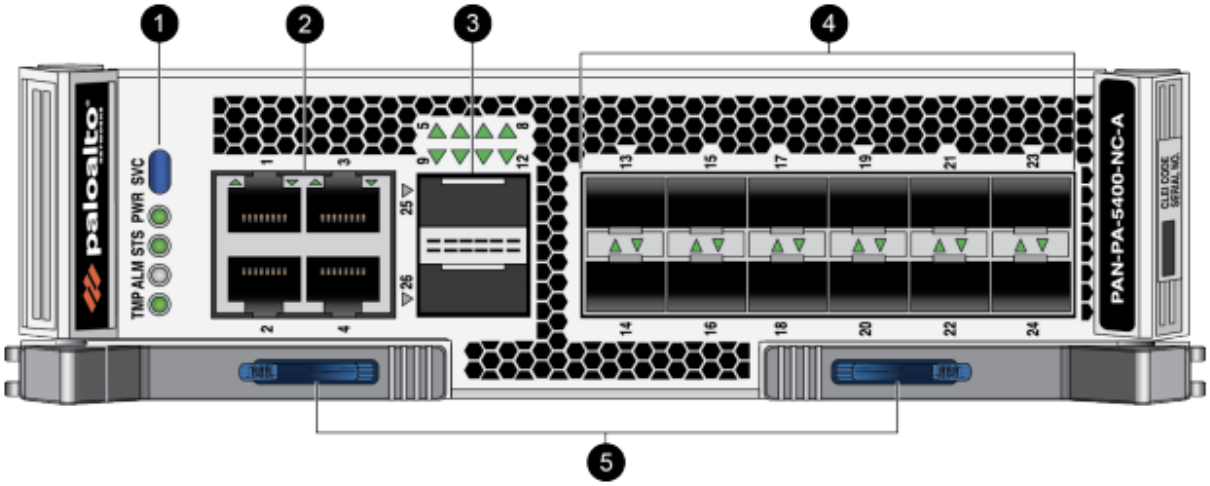


Figure 30 - PA-5450 Networking Card

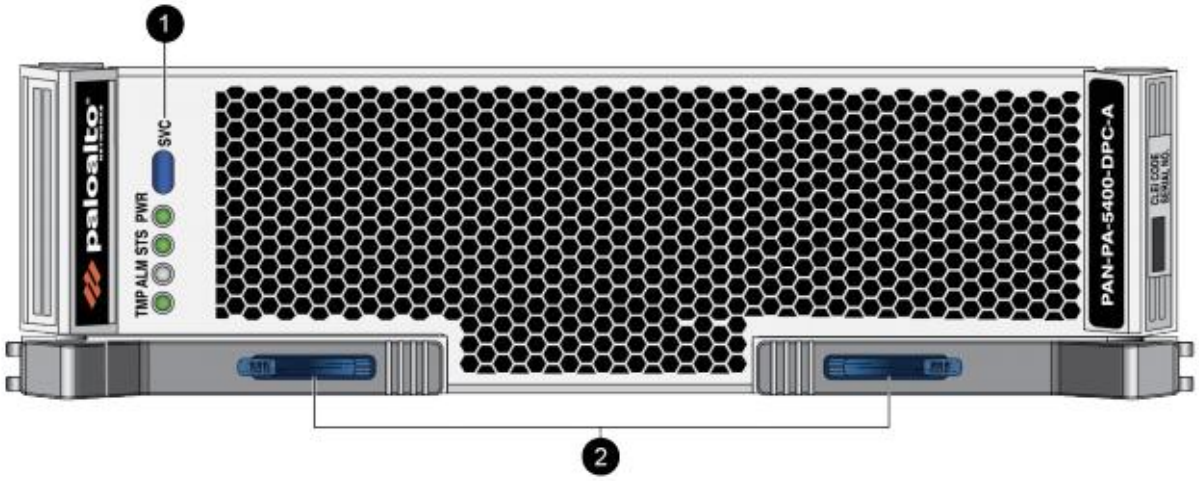


Figure 31 - PA-5450 Data Processing Card

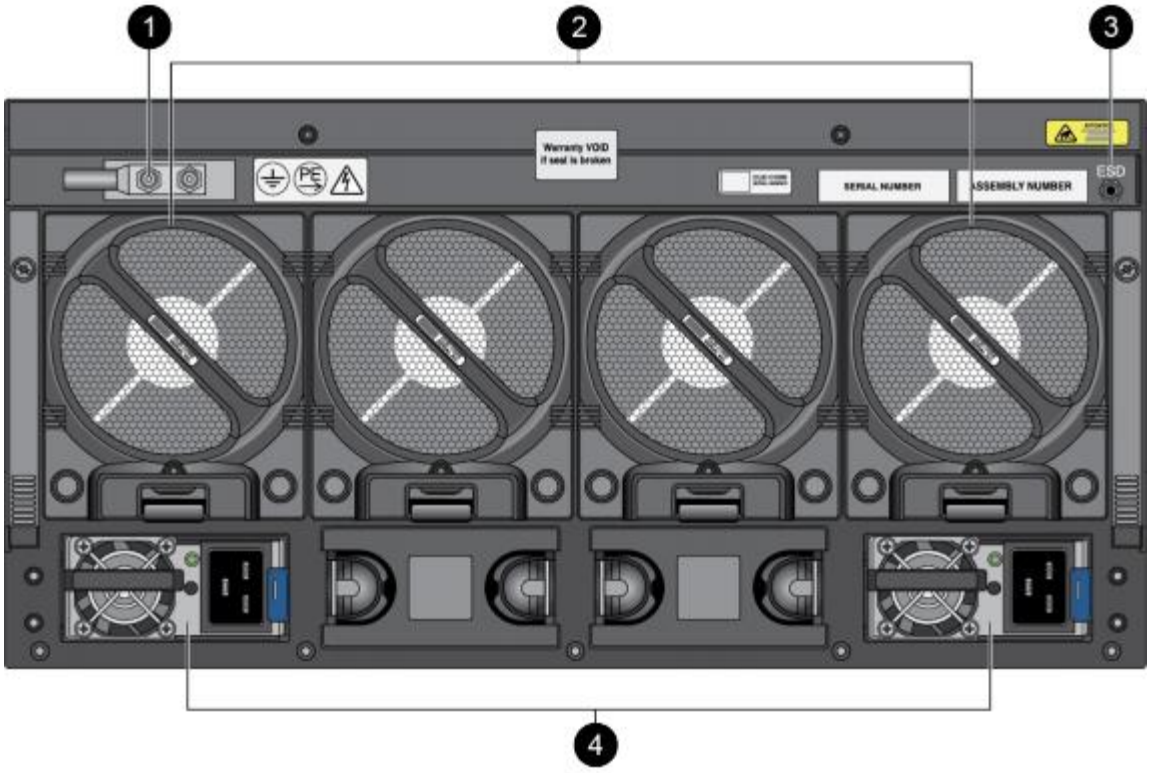


Figure 32 - PA-5450 Rear

PA-7050

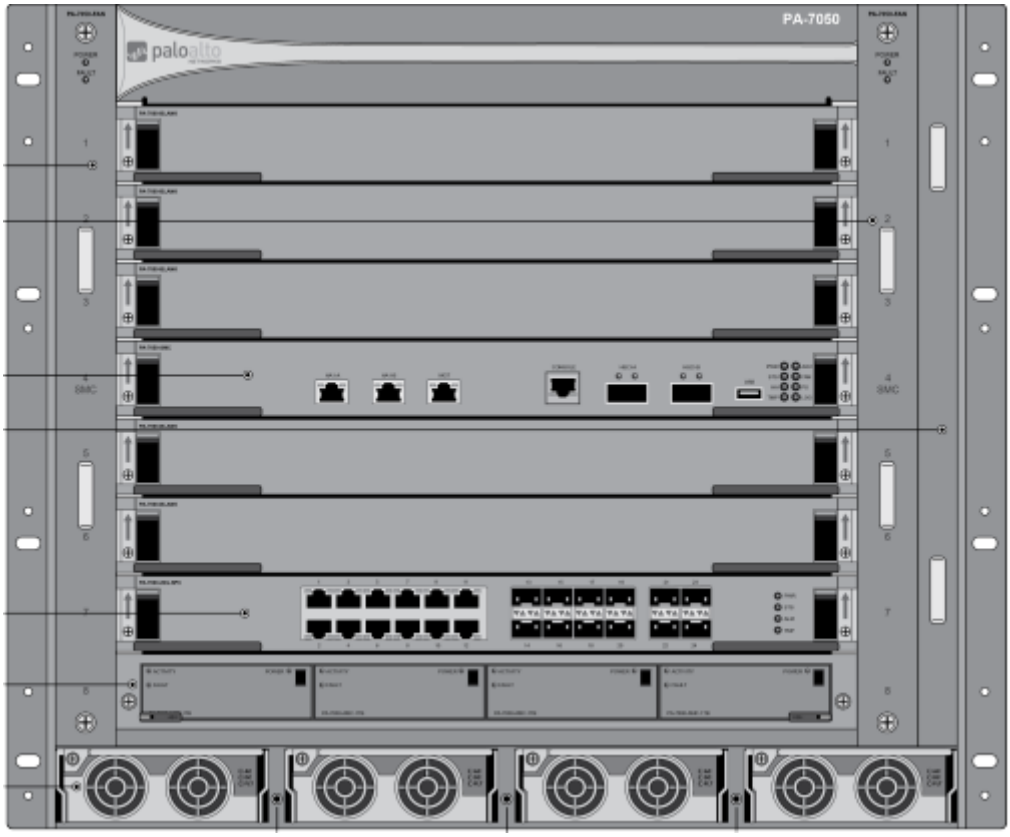


Figure 33 - PA-7050 Front

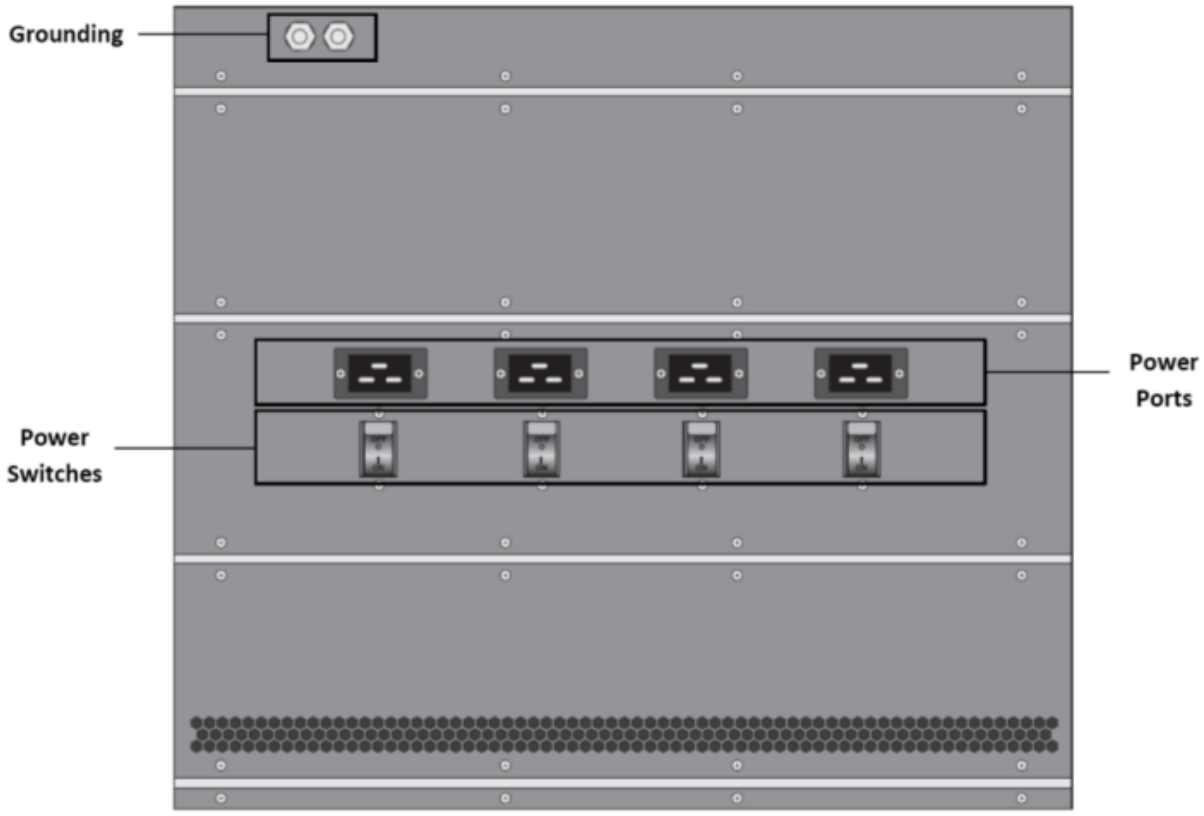


Figure 34 - PA-7050 Back

PA-7080

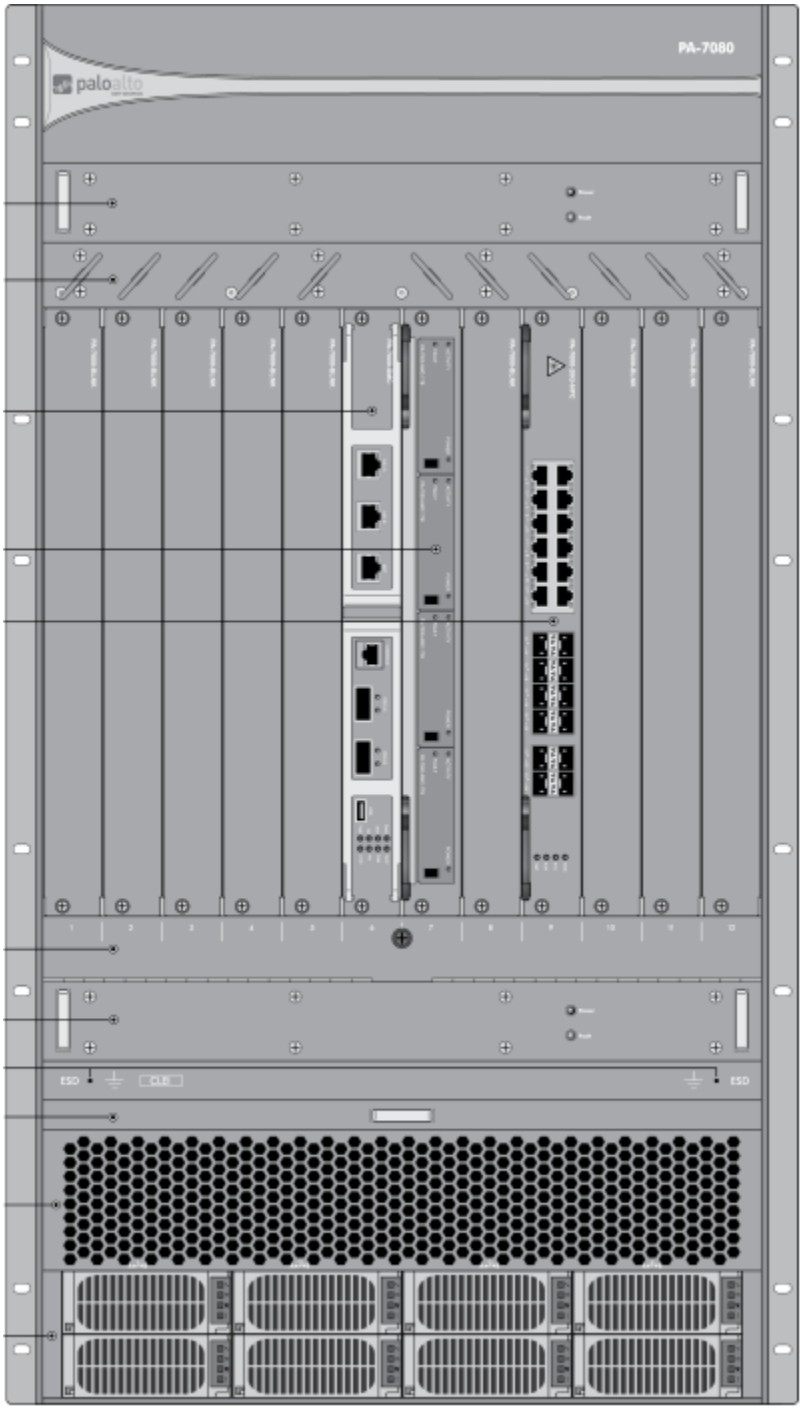


Figure 35- PA-7080 Front

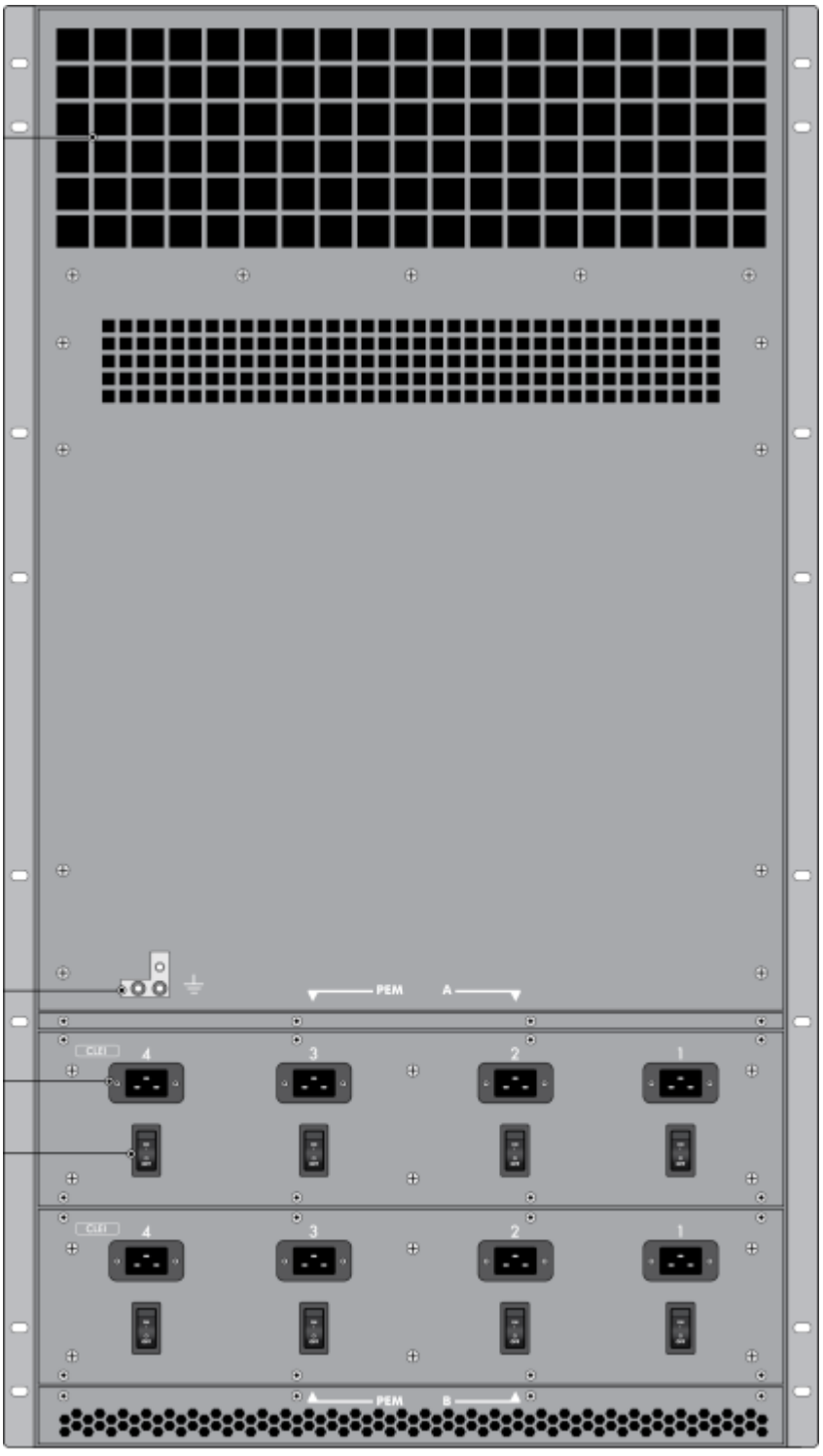


Figure 36 - PA-7080 Back

PA-7500

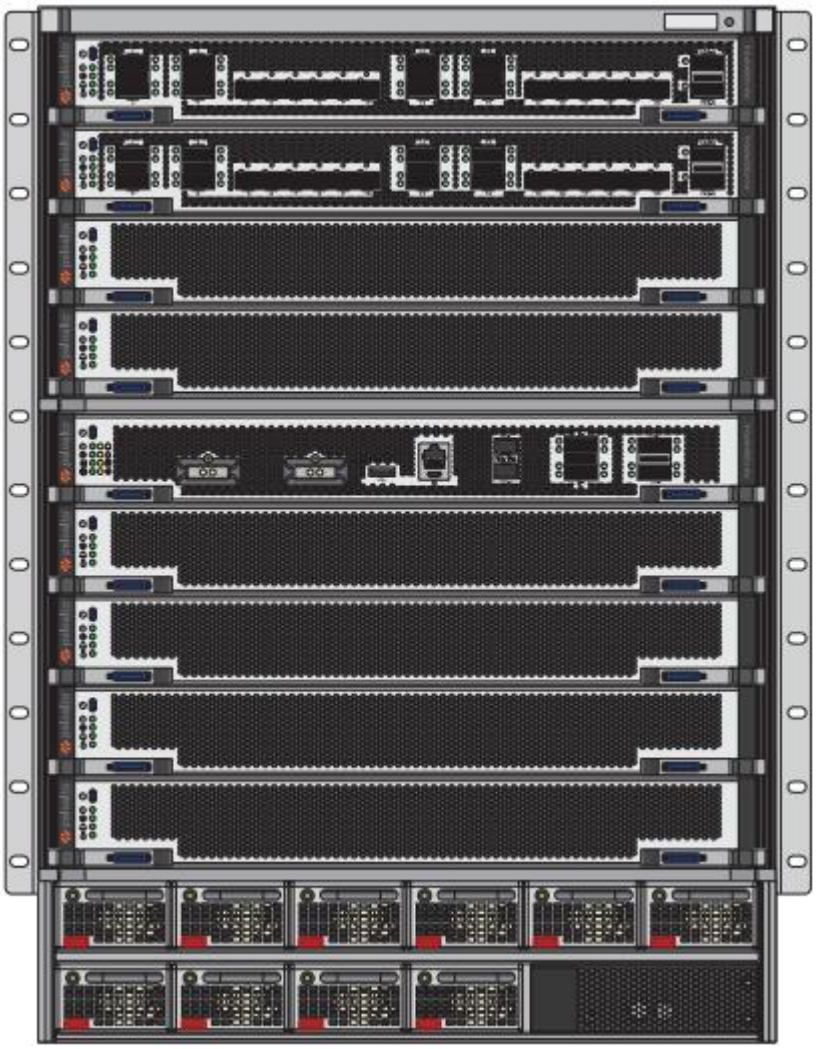


Figure 37 - PA-7500 Front

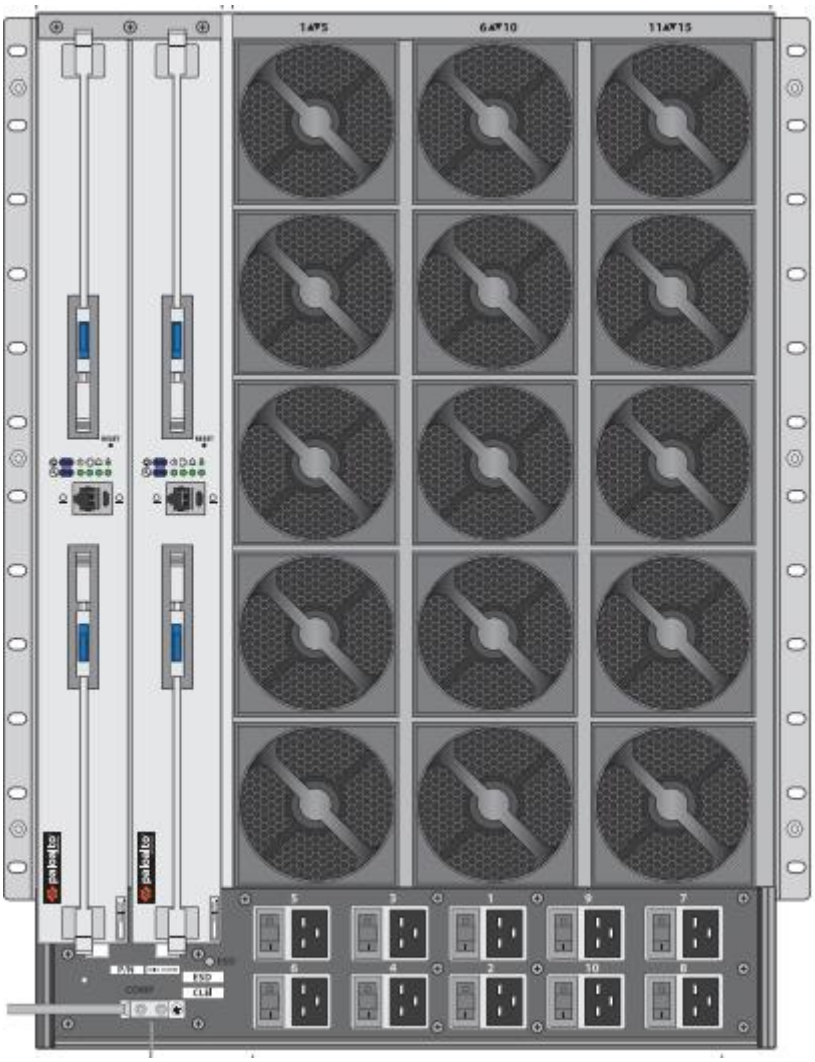


Figure 38 - PA-7500 Rear

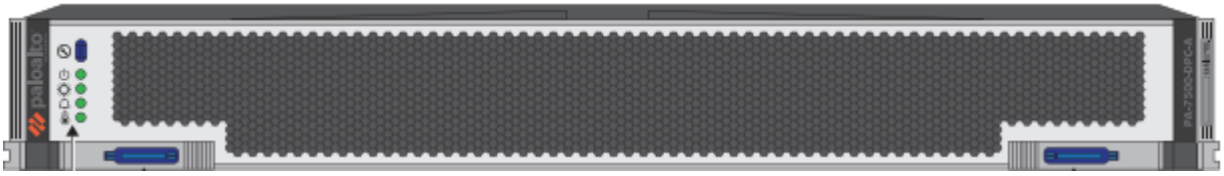


Figure 39 - PA-7500 DPC

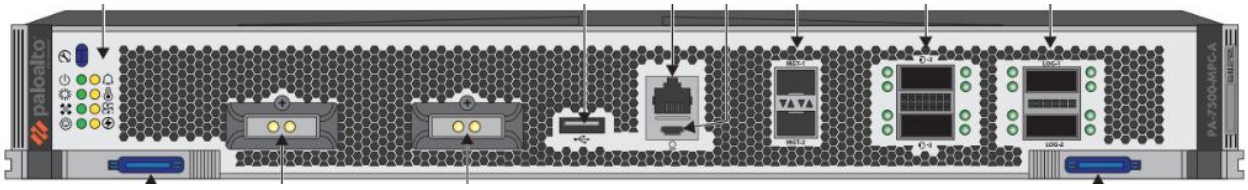


Figure 40 - PA-7500 MPC

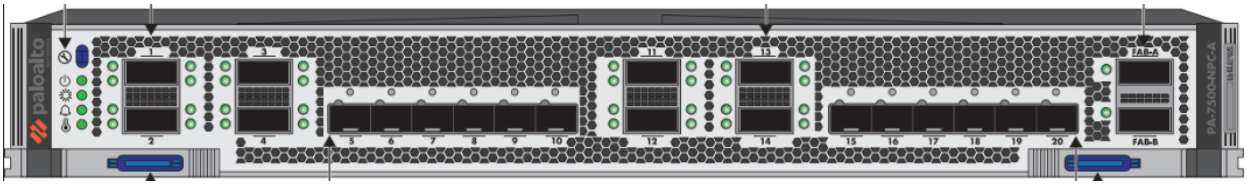


Figure 41 - PA-7500 NPC

Figure 38 depicts the logical block diagram for the modules. The Tested Operational Environment's Physical Perimeter (TOEPP) includes all of the logical components of the modules, and the boundary is the physical enclosure of the firewall.

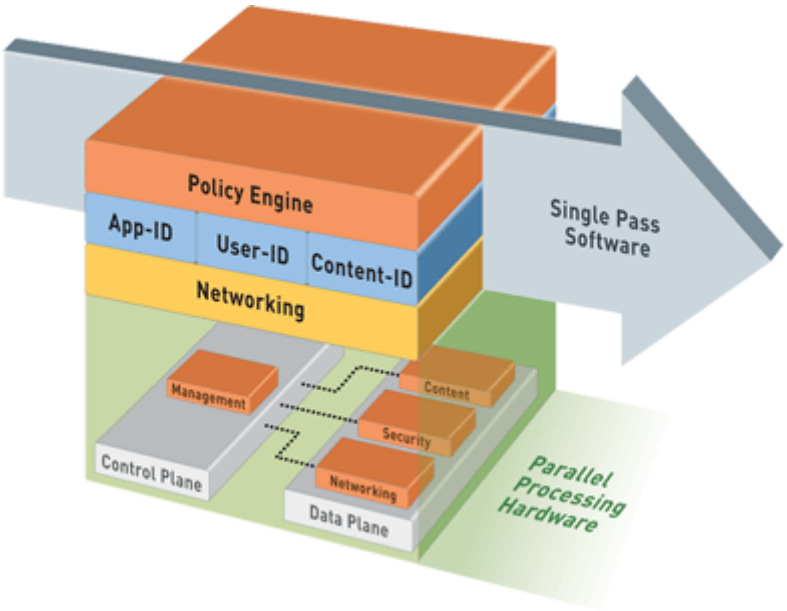


Figure 42 - Block Diagram

Tested Operational Environment's Physical Perimeter (TOEPP):

See above.

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
PA-1410	910-000267; Physical Kit: 920-000392	11.1.8, 11.2.5	Intel Atom C5325 (Parker Ridge)	RJ45 ports, SFP/SFP+ ports, HSCI ports, USB ports, Micro-USB, LED, Power
PA-1420	910-000269; Physical Kit: 920-000392	11.1.8, 11.2.5	Intel Atom C5325 (Parker Ridge)	RJ45 ports, SFP/SFP+ ports, HSCI ports, USB ports, Micro-USB, LED, Power
PA-3220	910-000162; Physical Kit: 920-000212	11.1.8	Intel Pentium D1517 (Broadwell) and Cavium OCTEON III CN7350 (cnMIPS64)	RJ45 ports, SFP/SFP+ ports, QSFP+ ports, HSCI ports, USB ports, Micro-USB, LED, Power
PA-3250	910-000163; Physical Kit: 920-000212	11.1.8	Intel Pentium D1517 (Broadwell) and Cavium OCTEON III CN7350 (cnMIPS64)	RJ45 ports, SFP/SFP+ ports, QSFP+ ports, HSCI ports, USB ports, Micro-USB, LED, Power
PA-3260	910-000164; Physical Kit: 920-000212	11.1.8	Intel Pentium D1517 (Broadwell) and Cavium OCTEON III CN7360 (cnMIPS64)	RJ45 ports, SFP/SFP+ ports, QSFP+ ports, HSCI ports, USB ports, Micro-USB, LED, Power
PA-3410	910-000241; Physical Kit: 920-000392	11.1.8, 11.2.5	Intel Atom P5332 (Snow Ridge)	1 x 1000Base-T (management) - RJ-45, 1 x 10Gb Ethernet (HA) - SFP+, 1 x console - RJ-45, 1 x management (USB) - micro-USB, 10 x 1Gb Ethernet/10Gb Ethernet - SFP/SFP+, 12 x 1/2.5/5/10GBase-T - RJ-45, 2 x 1000Base-T (HA) - RJ-45, 4 x 25Gb Ethernet - SFP28
PA-3420	910-000242; Physical Kit: 920-000392	11.1.8, 11.2.5	Intel Atom P5342 (Snow Ridge)	1 x 1000Base-T (management) - RJ-45, 1 x 10Gb Ethernet (HA) - SFP+, 1 x console - RJ-45, 1 x

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
				management (USB) - micro-USB, 10 x 1Gb Ethernet/10Gb Ethernet - SFP/SFP+, 12 x 1/2.5/5/10GBase-T - RJ-45, 2 x 1000Base-T (HA) - RJ-45, 4 x 25Gb Ethernet - SFP28
PA-3430	910-000243; Physical Kit: 920-000392	11.1.8, 11.2.5	Intel Atom P5352 (Snow Ridge)	1 x 1000Base-T (management) - RJ-45, 1 x 10Gb Ethernet (HA) - SFP+, 1 x console - RJ-45, 1 x management (USB) - micro-USB, 10 x 1Gb Ethernet/10Gb Ethernet - SFP/SFP+, 12 x 1/2.5/5/10GBase-T - RJ-45, 2 x 1000Base-T (HA) - RJ-45, 4 x 25Gb Ethernet - SFP28
PA-3440	910-000244; Physical Kit: 920-000392	11.1.8, 11.2.5	Intel Atom P5362 (Snow Ridge)	1 x 1000Base-T (management) - RJ-45, 1 x 10Gb Ethernet (HA) - SFP+, 1 x console - RJ-45, 1 x management (USB) - micro-USB, 10 x 1Gb Ethernet/10Gb Ethernet - SFP/SFP+, 12 x 1/2.5/5/10GBase-T - RJ-45, 2 x 1000Base-T (HA) - RJ-45, 4 x 25Gb Ethernet - SFP28
PA-410	910-000231; Physical Kit: 920-000454	11.1.8, 11.2.5	Intel Atom C3436L (Denverton)	RJ45 interfaces, USB, LED, Power supply, Ground stud
PA-410R	910-000312; Physical Kit: 920-000454	11.1.8, 11.2.5	Intel Atom C3508 (Denverton)	LEDs, Console, RJ-45 interfaces, SFP, Power
PA-410R-5G	910-000321; Physical Kit: 920-000454	11.1.8, 11.2.5	Intel Atom C3508 (Denverton)	LEDs, Console, RJ-45 interfaces, SFP, Power
PA-415	910-000280; Physical Kit: 920-000455	11.1.8, 11.2.5	Intel Atom C3436L (Denverton)	RJ45 ports, SFP/SFP+ ports, USB ports, Micro-USB, LED, Power

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
PA-415-5G	910-000287; Physical Kit: 920-000455	11.1.8, 11.2.5	Intel Atom C3436L (Denverton)	Console, SFP / RJ-45 ports, Ethernet RJ-45, Power, LED
PA-440	910-000212; Physical Kit: 920-000454	11.1.8, 11.2.5	Intel Atom C3558R (Denverton)	RJ 45 interfaces, USB, LEDs, Micro USB
PA-445	910-000281; Physical Kit: 920-000455	11.1.8, 11.2.5	Intel Atom C3558R (Denverton)	Console, SFP/RJ-45 ports, Ethernet RJ-45, Power, LEDs
PA-450	910-000232; Physical Kit: 920-000454	11.1.8, 11.2.5	Intel Atom C3758R (Denverton)	RJ 45 interfaces, USB, LEDs, Micro USB
PA-450R	910-000311; Physical Kit: 920-000454	11.1.8, 11.2.5	Intel Atom C3708 (Denverton)	LEDs, Console, SFP/RJ-45 ports, Power
PA-450R-5G	910-000319; Physical Kit: 920-000454	11.1.8, 11.2.5	Intel Atom C3708 (Denverton)	LEDs, Console, SFP/RJ-45 ports, Power
PA-455	910-000323; Physical Kit: 920-000454	11.1.8, 11.2.5	Intel Atom C3758R (Denverton)	LEDs, Console, RJ-45, SFP/RJ-45 Ports, Power
PA-455-5G	910-000451; Physical Kit: 920-000454	11.2.5	Intel Atom C3708 (Denverton)	LEDs, Console, SFP/RJ-45 Ports, RJ-45, Power
PA-460	910-000230; Physical Kit: 920-000454	11.1.8, 11.2.5	Intel Atom C3758R (Denverton)	RJ 45 interfaces, USB, LEDs, Micro USB
PA-5220	910-000132; Physical Kit: 920-000186	11.1.8, 11.2.5	Intel Xeon D-1548 (Broadwell) and Cavium OCTEON III CN7885 (cnMIPS64)	RJ45 ports, SFP/SFP+, QSFP28 port, QSFP+ ports, HSCI ports, SFTP+ ports, Power supply, LEDs, USB
PA-5250	910-000131; Physical Kit: 920-000186	11.1.8, 11.2.5	Intel Xeon D-1567 (Broadwell) and Cavium OCTEON III CN7890 (cnMIPS64)	RJ45 ports, SFP/SFP+, QSFP28 port, QSFP+ ports, HSCI ports, SFTP+ ports, Power supply, LEDs, USB

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
PA-5260	910-000125; Physical Kit: 920-000186	11.1.8, 11.2.5	Intel Xeon D-1567 (Broadwell) and Cavium OCTEON III CN7890 (cnMIPS64)	RJ45 ports, SFP/SFP+, QSFP28 port, QSFP+ ports, HSCI ports, SFTP+ ports, Power supply, LEDs, USB
PA-5280	910-000157; Physical Kit: 920-000186	11.1.8, 11.2.5	Intel Xeon D-1567 (Broadwell) and Cavium OCTEON III CN7890 (cnMIPS64)	RJ45 ports, SFP/SFP+, QSFP28 port, QSFP+ ports, HSCI ports, SFTP+ ports, Power supply, LEDs, USB
PA-5410	910-000252; Physical Kit: 920-000320	11.1.11, 11.2.8	AMD EPYC 7352 (Zen 2)	1 x 1000Base-X (management) – SFP, 1 x 40Gb Ethernet (management) - QSFP+, 1 x console - RJ-45, 1 x micro-USB, 12 x 10Gb Ethernet - SFP+, 2 x 1 Gigabit Ethernet (High Availability) – SFP, 4 x 25Gb Ethernet - SFP28, 4 x 40Gb Ethernet/100Gb Ethernet - QSFP28, 8 x 1/2.5/5/10GBase-T - RJ-45
PA-5420	910-000253; Physical Kit: 920-000320	11.1.11, 11.2.8	AMD EPYC 7452 (Zen 2)	1 x 1000Base-X (management) – SFP, 1 x 40Gb Ethernet (management) - QSFP+, 1 x console - RJ-45, 1 x micro-USB, 12 x 10Gb Ethernet - SFP+, 2 x 1 Gigabit Ethernet (High Availability) – SFP, 4 x 25Gb Ethernet - SFP28, 4 x 40Gb Ethernet/100Gb Ethernet - QSFP28, 8 x 1/2.5/5/10GBase-T - RJ-45
PA-5430	910-000254; Physical Kit: 920-000320	11.1.11, 11.2.8	AMD EPYC 7642 (Zen 2)	1 x 1000Base-X (management) – SFP, 1 x 40Gb Ethernet (management) - QSFP+, 1 x console - RJ-45,

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
				1 x micro-USB, 12 x 10Gb Ethernet - SFP+, 2 x 1 Gigabit Ethernet (High Availability) – SFP, 4 x 25Gb Ethernet - SFP28, 4 x 40Gb Ethernet/100Gb Ethernet - QSFP28, 8 x 1/2.5/5/10GBase-T - RJ-45
PA-5440	910-000255; Physical Kit: 920-000320	11.1.11, 11.2.8	AMD EPYC 7742 (Zen 2)	1 x 1000Base-X (management) – SFP, 1 x 40Gb Ethernet (management) - QSFP+, 1 x console - RJ-45, 1 x micro-USB, 12 x 10Gb Ethernet - SFP+, 2 x 1 Gigabit Ethernet (High Availability) – SFP, 4 x 25Gb Ethernet - SFP28, 4 x 40Gb Ethernet/100Gb Ethernet - QSFP28, 8 x 1/2.5/5/10GBase-T - RJ-45
PA-5445	910-000261; Physical Kit: 920-000320	11.1.11, 11.2.8	AMD EPYC 7713P (Zen 3)	1 x 1000Base-X (management) – SFP, 1 x 40Gb Ethernet (management) - QSFP+, 1 x console - RJ-45, 1 x micro-USB, 12 x 10Gb Ethernet - SFP+, 2 x 1 Gigabit Ethernet (High Availability) – SFP, 4 x 25Gb Ethernet - SFP28, 4 x 40Gb Ethernet/100Gb Ethernet - QSFP28, 8 x 1/2.5/5/10GBase-T - RJ-45
PA-5450	910-000223, Physical Kit: 920-000309; PA-5400 BC-A: 920-000293, PA-5400 MPC-A: 910-000195, PA-5400 NC-A: 910-000194, PA-5400	11.1.8, 11.2.5	Intel Xeon D-2187NT (Skylake)	Networking cards, Data processing cards, Base cards, Management processor cards, Electrostatic Discharge, LEDs, Logging Drive Corner, USB, Console port, HSCI-A/B, Logging ports, Management Ports, HA ports, Ejector Tabs, RJ45, QSFP28,

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
	DPC-A: 910-000204			SFP/SFP+, Ground Studs, Fans, Power
PA-7050	910-000102, Physical Kit: 920-000112; PAN-PA-7050-SMC-B: 910-000185 PAN-PA-7000-DPC-A: 910-000169 PAN-PA-7000-LFC-A: 910-000183 PAN-PA-7000-100G-NPC-A: 910-000156	11.1.8, 11.2.5	Intel Xeon D-1567 (Broadwell) and Cavium OCTEON III CN7890 (cnMIPS64)	Networking cards, Log/Data processing cards, Log forwarding cards, Management processor cards, RJ45 ports, SFP ports, SFP+ ports, HSCI ports, QSFP+ ports, Power supply, Power Switch, LEDs, USB
PA-7080	910-000122, Physical Kit: Physical Kit: 920-000119; PAN-PA-7080-SMC-B: 910-000186 PAN-PA-7000-DPC-A: 910-000169 PAN-PA-7000-LFC-A: 910-000183 PAN-PA-7000-100G-NPC-A: 910-000156	11.1.8, 11.2.5	Intel Xeon D-1567 (Broadwell) and Cavium OCTEON III CN7890 (cnMIPS64)	Networking cards, Log/Data processing cards, Log forwarding cards, Management processor cards, RJ45 ports, SFP+, HSCI, QSFP+, Power Switch, LEDs, USB
PA-7500	910-000297, Physical Kit: 920-000362; 910-000275 (DPC), 910-000227 (SFC), 910-000229 (NPC), 910-000262 (MPC)	11.1.9	Intel Atom P5752 (Snow Ridge) and Intel Xeon D-2798NX (Ice Lake) and Intel Atom C3758R (Denverton)	Management Processing Card,Network Processing Cards, Data Processing Cards, Switch Fabric Cards, USB, LEDs, RJ-45 Console, Micro USB Console, SFP/SFP+/SFP28, HSCI, QSFP28, QSFP-DD, Fabric ports, SFP-DD
PA-820	910-000120; Physical Kit: 920-000185	11.1.8	Cavium OCTEON III CN7240 (cnMIPS64)	RJ45 Ports, Micro-USB, SFP, SFP/SFP+, Power, LEDs, USB

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
PA-850	910-000119; Physical Kit: 920-000185	11.1.8	Cavium OCTEON III CN7240 (cnMIPS64)	RJ45 Ports, Micro-USB, SFP, SFP/SFP+, Power, LEDs, USB

Table 2: Tested Module Identification – Hardware

Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets):

N/A for this module.

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

2.3 Excluded Components

N/A

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved Mode	The module has one approved mode of operation and is always in approved mode after initialization	Approved	Global indicator (“FIPS-CC”)

Table 3: Modes List and Description

Mode Change Instructions and Status:

Note: The module supports a “maintenance mode” which corresponds to an uninitialized state. The maintenance mode does not support any approved security functions. Please refer to section 11 of this document for further detail.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A3453	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CCM	A3453	Key Length - 128	SP 800-38C
AES-CFB128	A3453	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CTR	A3453	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-GCM	A3453	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 256	SP 800-38D
Counter DRBG	A3453	Prediction Resistance - No, Yes Mode - AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-4)	A3453	Curve - P-256, P-384, P-521 Secret Generation Mode - Testing Candidates	FIPS 186-4
ECDSA KeyVer (FIPS186-4)	A3453	Curve - P-256, P-384, P-521	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A3453	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A3453	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
HMAC-SHA-1	A3453	Key Length - Key Length: 256-2048 Increment 8	FIPS 198-1
HMAC-SHA2-224	A3453	Key Length - Key Length: 256-2048 Increment 8	FIPS 198-1
HMAC-SHA2-256	A3453	Key Length - Key Length: 256-2048 Increment 8	FIPS 198-1
HMAC-SHA2-384	A3453	Key Length - Key Length: 256-2048 Increment 8	FIPS 198-1
HMAC-SHA2-512	A3453	Key Length - Key Length: 256-2048 Increment 8	FIPS 198-1

Algorithm	CAVP Cert	Properties	Reference
KAS-ECC-SSC Sp800-56Ar3	A3453	Domain Parameter Generation Methods - P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-FFC-SSC Sp800-56Ar3	A3453	Domain Parameter Generation Methods - MODP-2048, MODP-3072, MODP-4096 Scheme - dhEphem - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDF IKEv2 (CVL)	A3453	Diffie-Hellman Shared Secret Length - Diffie-Hellman Shared Secret Length: 256, 384, 2048 Derived Keying Material Length - Derived Keying Material Length: 800-3072 Increment 8 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
KDF SNMP (CVL)	A3453	Password Length - Password Length: 64, 2048	SP 800-135 Rev. 1
KDF SSH (CVL)	A3453	Cipher - AES-128, AES-192, AES-256 Hash Algorithm - SHA-1, SHA2-256, SHA2-512	SP 800-135 Rev. 1
RSA KeyGen (FIPS186-4)	A3453	Key Generation Mode - B.3.6 Modulo - 2048, 3072, 4096 Primality Tests - Table C.2 Private Key Format - Standard	FIPS 186-4
RSA SigGen (FIPS186-4)	A3453	Signature Type - PKCS 1.5 Modulo - 2048, 3072, 4096	FIPS 186-4
RSA SigVer (FIPS186-4)	A3453	Signature Type - PKCS 1.5 Modulo - 2048, 3072, 4096	FIPS 186-4
Safe Primes Key Generation	A3453	Safe Prime Groups - MODP-2048, MODP-3072, MODP-4096	SP 800-56A Rev. 3
Safe Primes Key Verification	A3453	Safe Prime Groups - MODP-2048, MODP-3072, MODP-4096	SP 800-56A Rev. 3
SHA-1	A3453	Message Length - Message Length: 8-65536 Increment 8	FIPS 180-4
SHA2-224	A3453	Message Length - Message Length: 0-65536 Increment 8, Message Length: 8-65536 Increment 8	FIPS 180-4
SHA2-256	A3453	Message Length - Message Length: 0-65536 Increment 8, Message Length: 8-65536 Increment 8	FIPS 180-4

Algorithm	CAVP Cert	Properties	Reference
SHA2-384	A3453	Message Length - Message Length: 0-65536 Increment 8, Message Length: 8-65536 Increment 8	FIPS 180-4
SHA2-512	A3453	Message Length - Message Length: 0-65536 Increment 8, Message Length: 8-65536 Increment 8	FIPS 180-4
TLS v1.2 KDF RFC7627 (CVL)	A3453	Hash Algorithm - SHA2-256, SHA2-384	SP 800-135 Rev. 1

Table 4: Approved Algorithms

Note: Only the algorithms specified in the table above are supported by the module in approved mode of operation.

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG	Key Type:Symmetric and Asymmetric	N/A	Cryptographic Key Generation; SP 800-133rev2 and IG D.H (symmetric keys and asymmetric seeds) from Section 4 Example 1

Table 5: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

N/A for this module.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
CKG	CKG	Symmetric key generation for AES		Counter DRBG: (A3453)

Name	Type	Description	Properties	Algorithms
Firmware Load Test	DigSig-SigVer	Signature verification for firmware load test		RSA SigVer (FIPS186-4): (A3453) Modulus: RSA-2048 with SHA2-256 SHA2-256: (A3453)
IPSec/IKE ECDSA KeyGen	AsymKeyPair-KeyGen CKG	ECDSA KeyGen for IPSec/IKEv2		ECDSA KeyGen (FIPS186-4): (A3453) Counter DRBG: (A3453) CKG: () Key Type: Symmetric and Asymmetric
IPSec/IKE ECDSA SigGen	DigSig-SigGen	ECDSA SigGen for IPSec/IKEv2		ECDSA SigGen (FIPS186-4): (A3453) Counter DRBG: (A3453)
IPSec/IKE ECDSA SigVer	DigSig-SigVer	ECDSA SigVer for IPSec/IKEv2		ECDSA SigVer (FIPS186-4): (A3453) ECDSA KeyVer (FIPS186-4): (A3453)
IPSec/IKE Keying Materials Development	KAS-135KDF	IPSec/IKE session keying materials, used to derive IPSec/IKE session keys		KDF IKEv2: (A3453)
IPSec/IKE RSA KeyGen	AsymKeyPair-KeyGen CKG	RSA KeyGen for IPSec/IKEv2		RSA KeyGen (FIPS186-4): (A3453) Counter

Name	Type	Description	Properties	Algorithms
				DRBG: (A3453) CKG: () Key Type: Symmetric and Asymmetric
IPSec/IKE RSA SigGen	DigSig-SigGen	RSA SigGen for IPSec/IKEv2		RSA SigGen (FIPS186-4): (A3453)
IPSec/IKE RSA SigVer	DigSig-SigVer	RSA SigVer for IPSec/IKEv2		RSA SigVer (FIPS186-4): (A3453)
KAS-ECC (IPSec/IKE)	KAS-Full	Full KAS-ECC Key Agreement used for IPSec/IKEv2 service	IG:IG D.F Scenario 2 Path 2, split Key Confirmation:No Key Derivation:IG 2.4.B SP 800-135rev1 CVL Caveat:Key establishment methodology providing 128, 192, or 256 bits of security strength	KAS-ECC-SSC Sp800-56Ar3: (A3453) KDF IKEv2: (A3453) SHA2-256: (A3453) SHA2-384: (A3453) SHA2-512: (A3453)
KAS-ECC (SSH)	KAS-Full	Full KAS-ECC Key Agreement used for SSHv2 service	IG:IG D.F Scenario 2 Path 2, split Key Confirmation:No Key Derivation:No Caveat:Key establishment methodology providing between 128 and 256 bits of security strength	KAS-ECC-SSC Sp800-56Ar3: (A3453) KDF SSH: (A3453) SHA2-256: (A3453) SHA2-384: (A3453) SHA2-512: (A3453)
KAS-ECC (TLSv1.2)	KAS-Full	Full KAS-ECC Key Agreement	IG:IG D.F Scenario 2 Path 2, split	KAS-ECC-SSC Sp800-56Ar3:

Name	Type	Description	Properties	Algorithms
		used for TLSv1.2 service	Key Confirmation:No Key Derivation:No Caveat:Key establishment methodology providing between 128 and 256 bits of security strength	(A3453) TLS v1.2 KDF RFC7627: (A3453)
KAS-ECC-KeyGen (IPSec/IKE)	CKG KAS-KeyGen	KAS ECC keygen used in IPSec/IKEv2 service	Strength:P-256, P-384, and P-521 curves providing 128, 192, or 256 bits of encryption strength	Counter DRBG: (A3453) CKG: () Key Type: Symmetric and Asymmetric
KAS-ECC-KeyGen (SSH)	CKG KAS-KeyGen	KAS ECC keygen used in SSHv2 service	Strength:P-256, P-384, and P-521 curves providing 128, 192, or 256 bits of encryption strength	Counter DRBG: (A3453) CKG: () Key Type: Symmetric and Asymmetric
KAS-ECC-KeyGen (TLSv1.2)	CKG KAS-KeyGen	KAS ECC keygen used in TLSv1.2 service	Strength:P-256, P-384, and P-521 curves providing 128, 192, or 256 bits of encryption strength	Counter DRBG: (A3453) CKG: () Key Type: Symmetric and Asymmetric
KAS-FFC (IPSec/IKE)	KAS-Full	Full KAS-FFC Key Agreement used for IPSec/IKEv2 service	IG:IG D.F Scenario 2 Path 2, split Key Confirmation:No Key Derivation:IG 2.4.B SP 800-135rev1 CVL Caveat:Key establishment methodology providing	KAS-FFC-SSC Sp800-56Ar3: (A3453) KDF IKEv2: (A3453) SHA2-256: (A3453) SHA2-384: (A3453) SHA2-512: (A3453)

Name	Type	Description	Properties	Algorithms
			between 112 and 150 bits of security strength.	
KAS-FFC (SSH)	KAS-Full	Full KAS-FFC Key Agreement used for SSHv2 service	IG:IG D.F Scenario 2 Path 2, split Key Confirmation:No Key Derivation:IG 2.4.B SP 800-135rev1 CVL Caveat:Key establishment methodology providing 112 bits of security strength	KAS-FFC-SSC Sp800-56Ar3: (A3453) KDF SSH: (A3453) SHA2-256: (A3453) SHA2-384: (A3453) SHA2-512: (A3453)
KAS-FFC (TLSv1.2)	KAS-Full	Full KAS-FFC Key Agreement used for TLSv1.2 service	IG:IG D.F Scenario 2 Path 2, split Key Confirmation:No Key Derivation:IG 2.4.B SP 800-135rev1 CVL Caveat:Key establishment methodology providing 112 bits of security strength	KAS-FFC-SSC Sp800-56Ar3: (A3453) TLS v1.2 KDF RFC7627: (A3453) Safe Primes Key Generation: (A3453) Safe Primes Key Verification: (A3453)
KAS-FFC-KeyGen (IPSec/IKE)	CKG KAS-KeyGen	KAS FFC keygen used in IPSec/IKEv2 service	Strength:2048, 3072, and 4096-bit keys providing 112, 128, or 150 bits of encryption strength	Counter DRBG: (A3453) CKG: () Key Type: Symmetric and Asymmetric
KAS-FFC-KeyGen (SSH)	CKG KAS-KeyGen	KAS FFC keygen used in SSHv2 service	Strength:2048-bit key providing 112 bits of encryption strength	Counter DRBG: (A3453) CKG: () Key Type:

Name	Type	Description	Properties	Algorithms
				Symmetric and Asymmetric
KAS-FFC-KeyGen (TLSv1.2)	CKG KAS-KeyGen	KAS FFC keygen used in TLSv1.2 service	Strength:2048-bit key providing 112 bits of encryption strength	Counter DRBG: (A3453) CKG: () Key Type: Symmetric and Asymmetric
KTS (SSHv2 with AES and HMAC)	KTS-Wrap	KTS via SSHv2 service by using AES and HMAC	Standard:SP 800-38F IG D.G:Approved Key Wrapping Caveat:Key establishment methodology providing between 128 and 256 bits of security strength	AES-CBC: (A3453) HMAC-SHA2-256: (A3453) HMAC-SHA2-384: (A3453) SHA2-256: (A3453) SHA2-384: (A3453)
KTS (SSHv2 with AES-GCM)	KTS-Wrap	KTS via SSHv2 service by using AES-GCM	Standard:SP 800-38F IG D.G:Approved Key Wrapping Caveat:Key establishment methodology providing between 128 and 256 bits of security strength	AES-GCM: (A3453)
KTS (TLSv1.2 with AES and HMAC)	KTS-Wrap	KTS via TLSv1.2 service by using AES and HMAC	Standard:SP 800-38F IG D.G:Approved Key Wrapping Caveat:Key establishment methodology providing between 128 and 256 bits of security strength	AES-CBC: (A3453) HMAC-SHA2-256: (A3453) HMAC-SHA2-384: (A3453) SHA2-256: (A3453) SHA2-384: (A3453)

Name	Type	Description	Properties	Algorithms
				TLS v1.2 KDF RFC7627: (A3453)
KTS (TLSv1.2 with AES-GCM)	KTS-Wrap	KTS via TLSv1.2 service by using AES-GCM	Standard:SP 800-38F IG D.G:Approved Key Wrapping Caveat:Key establishment methodology providing between 128 and 256 bits of security strength	TLS v1.2 KDF RFC7627: (A3453) AES-GCM: (A3453)
Session Authentication (IPSec/IKE)	MAC	IPSec/IKE session authentication		HMAC-SHA-1: (A3453) HMAC-SHA2-256: (A3453) HMAC-SHA2-384: (A3453) HMAC-SHA2-512: (A3453) SHA-1: (A3453) SHA2-256: (A3453) SHA2-384: (A3453) SHA2-512: (A3453)
Session Authentication (SMPv3)	MAC	SNMPv3 session authentication		HMAC-SHA-1: (A3453) SHA-1: (A3453) HMAC-SHA2-224: (A3453) SHA2-224: (A3453)

Name	Type	Description	Properties	Algorithms
Session Authentication (SSHv2)	MAC	SSHv2 session authentication		HMAC-SHA-1: (A3453) HMAC-SHA2-256: (A3453) HMAC-SHA2-512: (A3453) SHA-1: (A3453) SHA2-256: (A3453) SHA2-384: (A3453)
Session Authentication (TLSv1.2)	MAC	TLSv1.2 session authentication		HMAC-SHA2-256: (A3453) HMAC-SHA2-384: (A3453) SHA2-256: (A3453) SHA2-384: (A3453)
Session Encryption/Decryption (IPSec/IKE)	BC-Auth BC-UnAuth	IPSec/IKE session protection		AES-CBC: (A3453) AES-CCM: (A3453) AES-GCM: (A3453)
Session Encryption/Decryption (SNMPv3)	BC-Auth BC-UnAuth	SNMPv3 session protection		AES-CFB1: (A3453) AES-CFB8: (A3453) AES-CFB128: (A3453)
Session Encryption/Decryption (SSH)	BC-Auth BC-UnAuth	SSHv2 session protection		AES-CBC: (A3453) AES-CTR: (A3453) AES-GCM: (A3453)
Session Encryption/Decryption (TLSv1.2)	BC-Auth BC-UnAuth	TLSv1.2 session protection		AES-CBC: (A3453)

Name	Type	Description	Properties	Algorithms
				AES-GCM: (A3453)
SNMPv3 Keying Materials Development	KAS-135KDF	SNMPv3 session keying materials, used to derive SNMPv3 session keys		KDF SNMP: (A3453)
SSH ECDSA KeyGen	AsymKeyPair-KeyGen CKG	ECDSA KeyGen for SSHv2		ECDSA KeyGen (FIPS186-4): (A3453) Counter DRBG: (A3453) CKG: () Key Type: Symmetric and Asymmetric
SSH ECDSA SigGen	DigSig-SigGen	ECDSA SigGen for SSHv2		ECDSA SigGen (FIPS186-4): (A3453)
SSH ECDSA SigVer	DigSig-SigVer	ECDSA SigVer for SSHv2		ECDSA SigVer (FIPS186-4): (A3453) ECDSA KeyVer (FIPS186-4): (A3453)
SSH RSA KeyGen	AsymKeyPair-KeyGen CKG	ECDSA KeyGen for SSHv2		RSA KeyGen (FIPS186-4): (A3453) Counter DRBG: (A3453) CKG: () Key Type: Symmetric and Asymmetric
SSH RSA SigGen	DigSig-SigGen	ECDSA SigGen for SSHv2		RSA SigGen (FIPS186-4): (A3453) SHA2-256:

Name	Type	Description	Properties	Algorithms
				(A3453) SHA2-384: (A3453) SHA2-512: (A3453)
SSH RSA SigVer	DigSig-SigVer	RSA SigVer for SSHv2		RSA SigVer (FIPS186-4): (A3453) SHA2-256: (A3453) SHA2-384: (A3453) SHA2-512: (A3453) SHA2-224: (A3453)
SSHv2 Keying Materials Development	KAS-135KDF	SSHv2 session keying materials, used to derive SSHv2 session keys.		KDF SSH: (A3453)
TLS ECDSA KeyGen	AsymKeyPair-KeyGen CKG	ECDSA KeyGen for TLSv1.2		ECDSA KeyGen (FIPS186-4): (A3453) Counter DRBG: (A3453) CKG: () Key Type: Symmetric and Asymmetric
TLS ECDSA SigGen	DigSig-SigGen	ECDSA SigGen for TLSv1.2		ECDSA SigGen (FIPS186-4): (A3453) Counter DRBG: (A3453) SHA2-224: (A3453) SHA2-256: (A3453) SHA2-384:

Name	Type	Description	Properties	Algorithms
				(A3453) SHA2-512: (A3453)
TLS ECDSA SigVer	DigSig-SigVer	ECDSA SigVer for TLSv1.2		ECDSA SigVer (FIPS186-4): (A3453) ECDSA KeyVer (FIPS186-4): (A3453) SHA2-224: (A3453) SHA2-256: (A3453) SHA2-384: (A3453) SHA2-512: (A3453)
TLS RSA KeyGen	AsymKeyPair-KeyGen CKG	RSA KeyGen for TLSv1.2		RSA KeyGen (FIPS186-4): (A3453) TLS v1.2 KDF RFC7627: (A3453) CKG: () Key Type: Symmetric and Asymmetric Counter DRBG: (A3453)
TLS RSA SigGen	DigSig-SigGen	RSA SigGen for TLSv1.2		RSA SigGen (FIPS186-4): (A3453) SHA2-256: (A3453) SHA2-384: (A3453) SHA2-512: (A3453)
TLS RSA SigVer	DigSig-SigVer	RSA SigVer for TLSv1.2		RSA SigVer (FIPS186-4): (A3453) SHA2-224:

Name	Type	Description	Properties	Algorithms
				(A3453) SHA2-256: (A3453) SHA2-384: (A3453) SHA2-512: (A3453)
TLSv1.2 Keying Materials Development	KAS-135KDF	TLSv1.2 session keying materials, used to derive TLSv1.2 session keys		TLS v1.2 KDF RFC7627: (A3453)

Table 6: Security Function Implementations

2.7 Algorithm Specific Information

IG C.F Conformance

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 the middle-column of Table B.1 of FIPS 186-5. 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.

IG C.H Conformance

GCM is used in the context of TLS, IPsec/IKEv2, SSH:

- For TLS, The GCM implementation meets Scenario 1 of IG C.H: it is used in a manner compliant with SP 800-52rev2 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, 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). 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 32 bits in length and is derived using the SSH KDF; this ensures the fixed field is unique for any given GCM session. The invocation field is 64 bits in length and is incremented for each invocation of GCM; this prevents the IV from repeating until the entire invocation field space of 264 is exhausted. (It would take hundreds of years for this to occur.)

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

IG C.K Conformance

The CAVP testing for Cert. #A3453 was performed prior to the transition date for this IG. Additionally, The FIPS 186-4 CAVP implemented in this module tests are mathematically identical to FIPS 186-5 tests.

2.8 RBG and Entropy

Cert Number	Vendor Name
E27	Advanced Micro Devices (AMD)
E128	Palo Alto Networks
E162	Palo Alto Networks
E68	Palo Alto Networks
E70	Palo Alto Networks
E71	Palo Alto Networks
E72	Palo Alto Networks
E73	Palo Alto Networks

Table 7: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
AMD Random Number Generator	Physical	EPYC 7xx2 Family EPYC 7xx3 Family	128 bits	1.31221 bits	

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Octeon III Entropy Source (CN7xxx)	Physical	Cavium OCTEON III CN7350 (cnMIPS64), Cavium OCTEON III CN7360 (cnMIPS64), Cavium OCTEON III CN7890 (cnMIPS64), Cavium OCTEON III CN7240 (cnMIPS64), Cavium OCTEON III CN7240 (cnMIPS64)	80 bits	40.535	
Palo Alto Networks DRNG Entropy Source - Broadwell 16-Core Die with FCBGA1667 Package	Physical	Intel Corporation Intel(R) Xeon(R) Broadwell-16 FCBGA1667 Intel(R) Xeon(R) D-1557 Processor	128 bits	128 bits	CAVP Cert. #A2165 (AES-CBC-MAC)
Palo Alto Networks DRNG Entropy Source - Broadwell 8-Core Die with FCBGA1667 Package	Physical	Intel Pentium D1517 (Broadwell), Intel Xeon D-1548 (Broadwell)	128 bits	128 bits	CAVP Cert. #A2165 (AES-CBC-MAC)
Palo Alto Networks DRNG Entropy Source - Denverton 16 Core Die with FCBGA1310 Package	Physical	Intel Atom C3436L (Denverton), Intel Atom C3508 (Denverton), Intel Atom C3558R (Denverton), Intel Atom C3758R (Denverton), Intel Atom C3708 (Denverton)	128 bits	128 bits	CAVP Cert. #A2153 (AES-CBC-MAC)
Palo Alto Networks DRNG Entropy Source - Intel Xeon D-22 Series Processor Core Die with FCBGA2579 Package	Physical	Intel Xeon D-2798NX (Ice Lake)	128 bits	128 bits	CAVP Cert. #A2518 (AES-CBC-MAC)
Palo Alto Networks DRNG Entropy Source -	Physical	Intel Xeon D-2187NT (Skylake)	128 bits	128 bits	CAVP Cert. #A2138 (AES-CBC-MAC)

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Skylake-18 Core Die with FCBGA2518 Package					
Palo Alto Networks DRNG Entropy Source - Snow Ridge 24-Core Die with FCBGA2106 Package	Physical	Intel Atom C5325 (Parker Ridge), Intel Atom P5332 (Snow Ridge), Intel Atom P5342 (Snow Ridge), Intel Atom P5352 (Snow Ridge), Intel Atom P5362 (Snow Ridge), Intel Atom P5752 (Snow Ridge)	128 bits	128 bits	CAVP Cert. #A2165 (AES-CBC-MAC)

Table 8: Entropy Sources

The AMD RNG is estimated to provide a minimum of 1.31221 bits of entropy per 128-bit output. Upon boot, the AES-256 Counter DRBG (security strength of 256-bits) is directly seeded with 7569408 bits of data from the RDSEED instruction for 77,598 bits of entropy. Therefore, the AES-256 Counter DRBG is fully seeded upon initial instantiation.

The Intel DRNG utilizes a vetted conditioner (AES-CBC-MAC) that outputs full entropy (128-bits per 128-bits of output). Upon boot, the AES-256 Counter DRBG (security strength of 256-bits) requests 384-bits from the Intel DRNG entropy source. Therefore, it is fully seeded with 384 bits of entropy.

The Octeon III Entropy Source is estimated to provide a minimum of 0.50668693116 bits per bit of output. Upon boot, the AES-256 Counter DRBG (security strength of 256-bits) requests 384-bits from the entropy source. Therefore, the DRBG is initially seeded with at least 194 bits of entropy upon initial instantiation of the DRBG. This is greater than the 112-bit minimum, but less than the maximum-security strength of the CTR DRBG. Therefore, the module requires the caveat "The module generates SSPs (e.g., keys) whose strengths are modified by available entropy".

2.9 Key Generation

The module implements CKG where symmetric keys and seeds used for asymmetric key pair generation are produced using the unmodified/direct output of the DRBG.

2.10 Key Establishment

The module provides the following key/SSP establishment services in the approved mode of operation:

- KAS-ECC Shared Secret Computation
    - The module provides SP800-56Arev3 compliant key establishment according to FIPS 140-3 IG D.F scenario 2 path (1) with KAS-ECC shared secret computation. The shared secret computation provides between 128 and 256 bits of encryption strength.
- KAS-FFC Shared Secret Computation
    - The module provides SP800-56Arev3 compliant key establishment according to FIPS 140-3 IG D.F scenario 2 path (1) with KAS-FFC shared secret computation. The shared secret computation provides between 112 and 150 bits of encryption strength.

2.11 Industry Protocols

The module supports the following industry protocols:

- TLS 1.2
- SSHv2
- IPSec and IKEv2
- SNMPv3

No parts of the SSH, TLS, SNMP and IPSec/IKE protocols, other than the KDFs, have been tested by the CAVP/CMVP.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
HSCI (PA-1400 Series, PA-3200 Series, PA-3400 Series, PA-5200 Series, PA-5450, PA-7000 Series, PA-7500)	Data Input Data Output Control Input Status Output	SSH traffic/packets
LED	Status Output	Module status via LED indicators
Micro USB Console (PA-800 Series, PA-1400 Series, PA-3200 Series, PA-3400 Series, PA-415/PA-445, PA-440/PA-450/PA-460, PA-450R, PA-450R-5G, PA-415-5G, PA-455, PA-455-5G, PA-5400 Series, PA-5450, PA-7050, PA-7080, PA-7500)	Status Output	Self-test output
Power	Power	N/A
Power switch (PA-7000 Series, PA-7500)	Control Input	Power input switch

Physical Port	Logical Interface(s)	Data That Passes
QSFP+ (PA-3260, PA-3430/PA-3440, PA-5250, PA-5260, PA-5280, PA-5400 Series, PA-7000 Series, PA-7500)	Data Input Data Output Control Input Status Output	TLS, IPsec, or SSHt traffic/packets
QSFP28 (PA-3400 Series, PA-5200 Series, PA-5400 Series, PA-5450, PA-7000 Series, PA-7500)	Data Input Data Output Control Input Status Output	TLS, IPsec, or SSH traffic/packets
RJ45 Console	Status Output	Self-test output
RJ45 Ethernet	Data Input Data Output Control Input Status Output	TLS, IPSec traffic/packets
RJ45 HA (PA-1400 Series, PA-3200 Series, PA-5200 Series, PA-5400 Series, PA-5450, PA-7050, PA-7080)	Data Input Data Output Control Input Status Output	SSH traffic/packets
RJ45 Log (PA-5450)	Data Input Data Output Control Input Status Output	TLS, IPsec traffic/packets
RJ45 MGT (PA-400 Series, PA-1400 Series, PA-3200 Series, PA-3400 Series, PA-440/PA-450/PA-460, PA-5400 Series, PA-5450, PA-7000 Series)	Data Input Data Output Control Input Status Output	TLS, SSH traffic/packets
SFP (PA-415, PA-415-5G, PA-445, PA-455, PA-455-5G, PA-450R, PA-450R-5G, PA-410R, PA-410R-5G, PA-800 Series, PA-1400 Series, PA-3200 Series, PA-3400 Series, PA-5200 Series, PA-7000 Series, PA-7500)	Data Input Data Output Control Input Status Output	TLS, IPSec, or SSH traffic/packets

Physical Port	Logical Interface(s)	Data That Passes
SFP+ (PA-800 Series, PA-1400 Series, PA-3200 Series, PA-3400 Series, PA-5200 Series, PA-5400 Series, PA-5450, PA-7050, PA-7080, PA-7500)	Data Input Data Output Control Input Status Output	TLS, IPSec, or SSH traffic/packets
SFP28 (PA-3400 Series, PA-5400 Series, PA-7500)	Data Input Data Output Control Output Status Output	TLS, IPSec traffic/packets
Uplink Connector (PA-410R-5G, PA-450R-5G, PA-415-5G, PA-455-5G)	Data Input Data Output Status Output	TLS, IPSec traffic/packets, or SSH packets

Table 9: Ports and Interfaces

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
RSA-Based Certificate	The modules support RSA public-key based authentication mechanism using a minimum of RSA 2048 bits	RSA SigVer (FIPS186-4) (A3453)	With a minimum modulus size of 2048, the probability that a random attempt will succeed is 1/(2^112).	The probability of successfully authenticating to the module within a one minute period is 288,000,000/(2^112). The module supports at most 4,800,000 new sessions per second.
ECDSA-Based Certificate	The modules support ECDSA public-key based authentication mechanism using a minimum	ECDSA SigVer (FIPS186-4) (A3453)	With a minimum curve of P-256, the probability that a random attempt will succeed is 1/(2^128).	The probability of successfully authenticating to the module within a one minute period is 288,000,000/(2^112). The module supports at

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
	ECDSA curve of P-256			most 4,800,000 new sessions per second.
Password	Password based authentication	Password Based	The minimum length is eight (8) characters (95 possible characters). The probability that a random attempt will succeed or a false acceptance will occur is 1/(95^8).	The probability of successfully authenticating to the module within one minute is 10/(95^8). The firewall's configuration supports at most ten failed attempts to authenticate in a one-minute period.
Pre-Shared Secret	PSK authentication	Password Based	The pre-shared key authentication method has a minimum security strength of 95^6. The probability of successfully authenticating to the module is 1/(956). The number of authentication attempts is limited by the number of new connections per second supported (4,800,000) on the fastest platform of the Palo Alto Networks firewalls.	The probability of successfully authenticating to the module within a one minute period is 288,000,000/(95^6).

Table 10: Authentication Methods

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Identity	Crypto Officer	RSA-Based Certificate ECDSA-Based Certificate Password Pre-Shared Secret
User	Identity	User	RSA-Based Certificate ECDSA-Based Certificate

Name	Type	Operator Type	Authentication Methods
			Password Pre-Shared Secret
Remote Access VPN (RA VPN)	Identity	Crypto Officer	RSA-Based Certificate ECDSA-Based Certificate Password Pre-Shared Secret
Site-to-Site VPN (S-S VPN)	Identity	Crypto Officer	Password Pre-Shared Secret

Table 11: Roles

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Firmware Update	Provides a method to update the firmware of the module	Configuration/ System Logs	Uploading new firmware	Status of the updated firmware installation	Firmware Load Test	Crypto Officer - Public key for firmware content load test: E
Other Configuration	Networking parameter configuration, logging configuration, and other non-security relevant configuration	Configuration/ System Logs	Input configurations for other setup functions	Module uses configuration	KAS-ECC (SSH) KAS-ECC (TLSv1.2) KAS-ECC-KeyGen (SSH) KAS-ECC-KeyGen (TLSv1.2) KAS-FFC (SSH) KAS-FFC (TLSv1.2) KAS-FFC-KeyGen (SSH) KAS-FFC-KeyGen (TLSv1.2) KTS (SSHv2 with AES and HMAC) KTS (SSHv2	Crypto Officer - CO, User, RA VPN Password: G,W,E - DHE/ECDHE Shared Secret Z: G,R,E - DRBG Key: G,E - DRBG Seed : G,E - DRBG V: G,E - ECDSA Private Keys: G,W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					with AES-GCM) KTS (TLSv1.2 with AES and HMAC) KTS (TLSv1.2 with AES-GCM) SNMPv3 Keying Materials Development SSH ECDSA KeyGen SSH ECDSA SigGen SSH ECDSA SigVer SSH RSA KeyGen SSH RSA SigGen SSH RSA SigVer SSHv2 Keying Materials Development Session Authentication (SMPv3) Session Authentication (SSHv2) Session Authentication (TLSv1.2) Session Encryption/Decryption (SNMPv3) Session Encryption/Decryption (SSH) Session	- Entropy Input String: G,E - IKEv2 SKEYSEED: G,R,E - RSA Private Keys: G,W,E - SNMPv3 Authentication Key: G,R,E - SNMPv3 Session Key: G,R,E - SSH Client Public Key: W,E - SSH DHE/ECDHE Private Components: G,E,Z - SSH DHE/ECDHE Public Components: G,R,W,E,Z - SSH Host Public Key: G,R,W,E - SSH Session Authentica

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					Encryption/Decryption (TLSv1.2) TLS ECDSA KeyGen TLS ECDSA SigGen TLS ECDSA SigVer TLS RSA KeyGen TLS RSA SigGen TLS RSA SigVer TLSv1.2 Keying Materials Development CKG	tion Keys: G,E,Z - SSH Session Encryption Keys: G,E,Z - TLS DHE/ECDHE Private Components: G,E,Z - TLS DHE/ECDHE Public Components: G,R,W,E,Z - TLS Encryption Keys: G,E,Z - TLS HMAC Keys: G,E,Z - TLS Master Secret: G,E,Z - TLS Pre-Master Secret: G,E,Z
Security Configuration Management	Configuring and managing cryptographic parameters and setting/mod	Configuration/ System Logs	Input configuration for various cryptographic functions	Module uses the configuration for cryptographic purposes	KAS-ECC (SSH) KAS-ECC (TLSv1.2) KAS-ECC-KeyGen (SSH) KAS-ECC-KeyGen	Crypto Officer - CA Certificates: G,R,W,E - CO, User, RA

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	ifying security policy, including creating User accounts and additional CO accounts				(TLSv1.2) KAS-FFC (SSH) KAS-FFC (TLSv1.2) KAS-FFC-KeyGen (SSH) KAS-FFC-KeyGen (TLSv1.2) KTS (SSHv2 with AES and HMAC) KTS (SSHv2 with AES-GCM) KTS (TLSv1.2 with AES and HMAC) KTS (TLSv1.2 with AES-GCM) SNMPv3 Keying Materials Development SSH ECDSA KeyGen SSH ECDSA SigGen SSH ECDSA SigVer SSH RSA KeyGen SSH RSA SigGen SSH RSA SigVer SSHv2 Keying Materials Development Session Authentication (SMPv3)	VPN Password: G,W,E - DHE/ECDHE Shared Secret Z: G,R,E - DRBG Key: G,E - DRBG Seed : G,E - DRBG V: G,E - ECDSA Private Keys: G,W,E - ECDSA Public Keys: G,R,W,E - Entropy Input String: G,E - IKEv2 SKEYSEED: G,R,E - Protocol Secrets: W,E - Public key for firmware content load test: W,E - RSA Private Keys: G,W,E - RSA Public

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					Session Authentication (SSHv2) Session Authentication (TLSv1.2) Session Encryption/Decryption (SNMPv3) Session Encryption/Decryption (SSH) Session Encryption/Decryption (TLSv1.2) TLS ECDSA KeyGen TLS ECDSA SigGen TLS ECDSA SigVer TLS RSA KeyGen TLS RSA SigGen TLS RSA SigVer TLSv1.2 Keying Materials Development CKG	Keys: G,R,W,E - SNMPv3 Authentication Key: G,R,E - SNMPv3 Authentication Secret: W,E - SNMPv3 Privacy Secret: W,E - SNMPv3 Session Key: G,R,E - SSH Client Public Key: W,E - SSH DHE/ECDHE Private Components: G,E,Z - SSH DHE/ECDHE Public Components: G,R,W,E,Z - SSH Host Public Key: G,R,W,E - SSH Session Authentica

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						tion Keys: G,E,Z - SSH Session Encryption Keys: G,E,Z - TLS DHE/ECDHE Private Components: G,E,Z - TLS DHE/ECDHE Public Components: G,R,W,E,Z - TLS Encryption Keys: G,E,Z - TLS HMAC Keys: G,E,Z - TLS Master Secret: G,E,Z - TLS Pre-Master Secret: G,E,Z
Self-Tests	Initiates self-tests and integrity test	System Logs	Self-test command or rebooting the module	Status of the self-tests	None	Crypto Officer - Firmware integrity verification key : E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Show Status	Provides status information of the module	Configuration/ System Logs	Initiate show status command	Module provides status output of module	None	Crypto Officer - CO, User, RA VPN Password: G,W,E - DRBG Key: G,E - DRBG Seed : G,E - DRBG V: G,E - ECDSA Private Keys: E - Entropy Input String: G,E - RSA Private Keys: E - SSH DHE/ECDHE Private Components: G,E,Z - SSH DHE/ECDHE Public Components: G,R,W,E,Z - SSH Session Authentication Keys: G,E,Z - SSH Session Encryptio

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						n Keys: G,E,Z - TLS DHE/ECDHE Private Components: G,E,Z - TLS DHE/ECDHE Public Components: G,R,W,E,Z - TLS Encryption Keys: G,E,Z - TLS HMAC Keys: G,E,Z - TLS Master Secret: G,E,Z - TLS Pre-Master Secret: G,E,Z Unauthenticated User - CO, User, RA VPN Password: G,W,E - DRBG Key: G,E - DRBG Seed : G,E - DRBG

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						V: G,E - ECDSA Private Keys: E - Entropy Input String: G,E - RSA Private Keys: E - SSH DHE/ECDHE Private Components: G,E,Z - SSH DHE/ECDHE Public Components: G,R,W,E,Z - SSH Session Authentication Keys: G,E,Z - SSH Session Encryption Keys: G,E,Z - TLS DHE/ECDHE Private Components: G,E,Z - TLS DHE/ECDHE Public Componen

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						ts: G,R,W,E, Z - TLS Encryption Keys: G,E,Z - TLS HMAC Keys: G,E,Z - TLS Master Secret: G,E,Z - TLS Pre-Master Secret: G,E,Z
Show Status (LEDs)	Provides status of the module	LEDs	N/A	Status of the module via LEDs	None	Crypto Officer
Show Version	Shows the version of the module	Version displayed via System Logs / CLI / UI	Input command for version	Module displays version information	None	Crypto Officer
View Other Configuration	Read-only of non-security relevant configuration	Configuration/ System Logs	Initiate command to read configuration	Module provides configuration details	None	Crypto Officer - CO, User, RA VPN Password: W,E User - CO, User, RA VPN Password: W,E
VPN	Provide network	Configuration/ System Logs	Initiating VPN	Module provides	IPSec/IKE ECDSA	Remote Access

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	access for remote users or site-to-site connection		connections	VPN connection	KeyGen IPSec/IKE ECDSA SigGen IPSec/IKE ECDSA SigVer IPSec/IKE Keying Materials Development IPSec/IKE RSA KeyGen IPSec/IKE RSA SigGen IPSec/IKE RSA SigVer KAS-ECC (IPSec/IKE) KAS-ECC-KeyGen (IPSec/IKE) KAS-FFC (IPSec/IKE) KAS-FFC-KeyGen (IPSec/IKE) Session Authentication (IPSec/IKE) Session Encryption/Decryption (IPSec/IKE) CKG	VPN (RA VPN) - CA Certificates: W,E - DRBG Key: G,E - DRBG Seed : G,E - DRBG V: G,E - ECDSA Private Keys: E - ECDSA Public Keys: W,E - Entropy Input String: G,E - RA VPN IPSec Authentication : G,E,Z - RA VPN IPSec Session Keys: G,E,Z - RSA Private Keys: E - RSA Public Keys: W,E - S-S VPN IPSec Pre-Shared Keys: W,E - S-S VPN IPSec/IKE DHE or

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						ECDHE Private Components: G,E,Z - S-S VPN IPSec/IKE DHE or ECDHE Public Components: G,R,W,E,Z - S-S VPN IPSec/IKE Session Keys: G,E,Z - TLS DHE/ECDHE Private Components: G,E,Z - TLS DHE/ECDHE Public Components: G,R,W,E,Z - TLS Encryption Keys: G,E,Z - TLS HMAC Keys: G,E,Z - TLS Master Secret: G,E,Z - TLS Pre-

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Master Secret: G,E,Z Site-to-Site VPN (S-S VPN) - CA Certificates: W,E - DRBG Key: G,E - DRBG Seed : G,E - DRBG V: G,E - ECDSA Private Keys: E - ECDSA Public Keys: W,E - Entropy Input String: G,E - RA VPN IPSec Authentication : G,E,Z - RA VPN IPSec Session Keys: G,E,Z - RSA Private Keys: E - RSA Public Keys: W,E - S-S VPN IPSec Pre-Shared

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Keys: W,E - S-S VPN IPSec/IKE DHE or ECDHE Private Components: G,E,Z - S-S VPN IPSec/IKE DHE or ECDHE Public Components: G,R,W,E,Z - S-S VPN IPSec/IKE Session Keys: G,E,Z - TLS DHE/ECDHE Private Components: G,E,Z - TLS DHE/ECDHE Public Components: G,R,W,E,Z - TLS Encryption Keys: G,E,Z - TLS HMAC Keys: G,E,Z - TLS

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Master Secret: G,E,Z - TLS Pre-Master Secret: G,E,Z
Zeroize	Zeroize all keys in the module	Zeroization indicator	Initiating zeroization command	Status of the zeroization process	None	Unauthenticated - CA Certificates: Z - CO, User, RA VPN Password: Z - DHE/ECDHE Shared Secret Z: Z - DRBG Key: Z - DRBG Seed : Z - DRBG V: Z - ECDSA Private Keys: Z - ECDSA Public Keys: Z - Entropy Input String: Z - IKEv2 SKEYSEED: Z - Protocol Secrets: Z - Public key for

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						firmware content load test: Z - RA VPN IPSec Authentication : Z - RA VPN IPSec Session Keys: Z - RSA Private Keys: Z - RSA Public Keys: Z - S-S VPN IPSec Pre-Shared Keys: Z - S-S VPN IPSec/IKE Authentication Keys: Z - S-S VPN IPSec/IKE DHE or ECDHE Private Components: Z - S-S VPN IPSec/IKE DHE or ECDHE Public Components: Z - S-S VPN IPSec/IKE Session

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Keys: Z - SNMPv3 Authentication Key: Z - SNMPv3 Authentication Secret: Z - SNMPv3 Privacy Secret: Z - SNMPv3 Session Key: Z - SSH DHE/ECDHE Private Components: Z - SSH DHE/ECDHE Public Components: Z - SSH Host Public Key: Z - SSH Session Authentication Keys: Z - SSH Session Encryption Keys: Z - TLS DHE/ECDHE Private Componen

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						ts: Z - TLS DHE/ECDHE Public Components: Z - TLS Encryption Keys: Z - TLS HMAC Keys: Z - TLS Master Secret: Z - TLS Pre-Master Secret: Z

Table 12: Approved Services

4.4 Non-Approved Services

N/A for this module.

4.5 External Software/Firmware Loaded

The module supports the firmware load test by using RSA 2048 bits with SHA2-256 (RSA Cert. #A3453) for the new validated firmware to be uploaded into the module. A Firmware Load Test Key was preloaded to the module's binary at the factory and used for firmware load test. In order to load new firmware, the Crypto Officer must authenticate into the module before loading any firmware. This ensures that unauthorized access and use of the module is not performed. The module will load the new update upon reboot. The update attempt will be rejected if the verification fails.

5 Software/Firmware Security

The module's executable code is in the form of the compiled firmware image loaded onto the module.

5.1 Integrity Techniques

The module performs the Firmware Integrity test by using HMAC-SHA-256 and ECDSA signature verification (HMAC and ECDSA Cert. #A3453) during the Pre-Operational Self-Test.

5.2 Initiate on Demand

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

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

7 Physical Security

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Tamper-Evident Seals	30 days	Verify integrity of tamper-evident seals in the locations identified in the Physical Kit Installation Guide. Seal integrity to be verified within the modules operating temperature range.
Top/Bottom/Front/Rear Opacity shields or covers	30 days	Verify that the plenums/opacity shields or covers have not been deformed from their original shape, thereby reducing their effectiveness

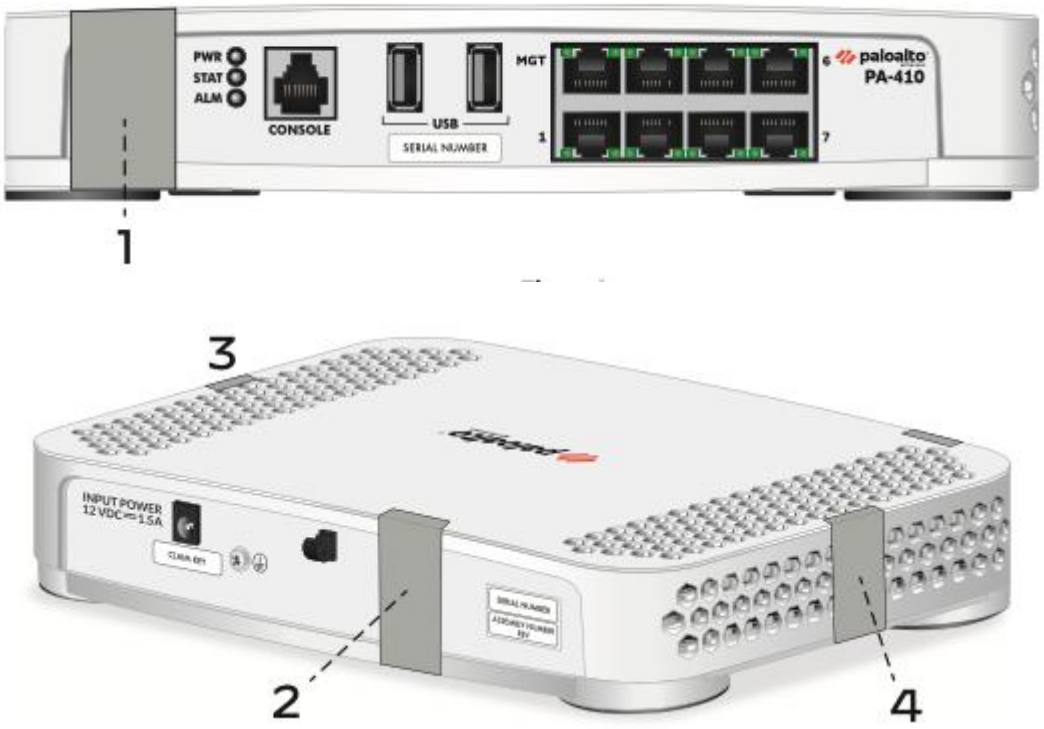
Table 13: Mechanisms and Actions Required

7.2 User Placed Tamper Seals

PA-410

Number: The PA-410 requires 4 tamper evident labels.

Placement:



Surface Preparation: Clean the chassis of any grease, dirt, or oil before applying the tamper evident labels

Operator Responsible for Securing Unused Seals: Crypto Officer

Part Numbers: 920-000454

PA-410R / PA-410R-5G
Number: The PA-410R series requires 6 tamper labels

Placement:


[2]
[3]
[1]
[4]


[5]

Surface Preparation: Clean the chassis of any grease, dirt, or oil before applying the tamper evident labels

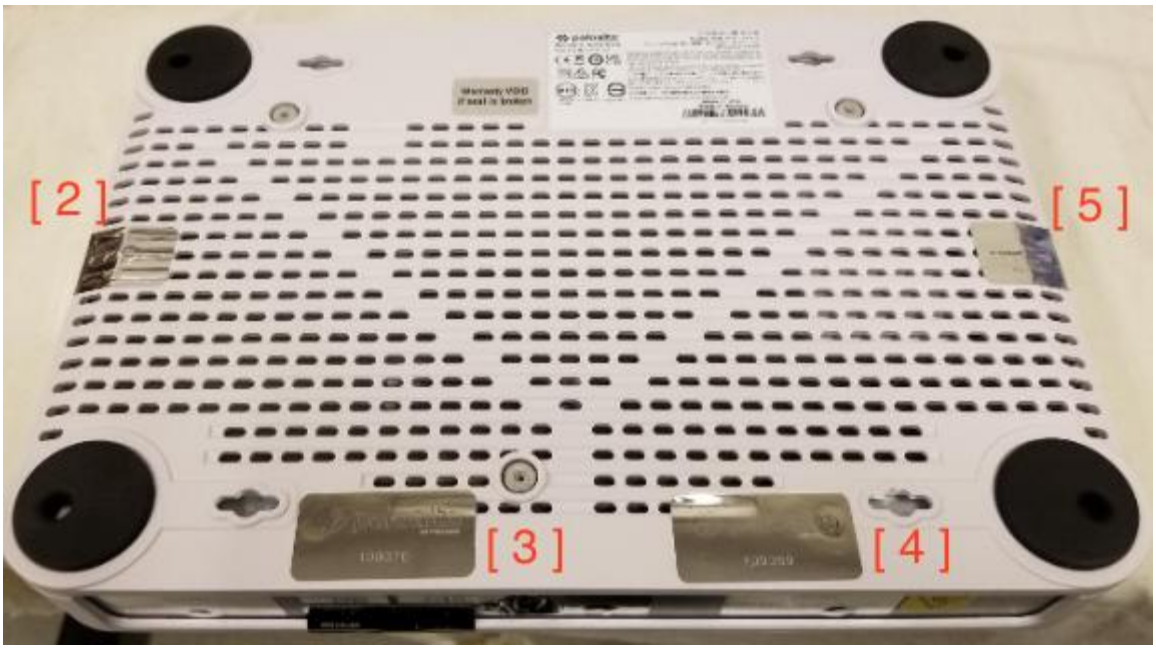
Operator Responsible for Securing Unused Seals: Crypto Officer

Part Numbers: 920-000455

PA-415

Number: The PA-415 requires 5 tamper evident labels

Placement:



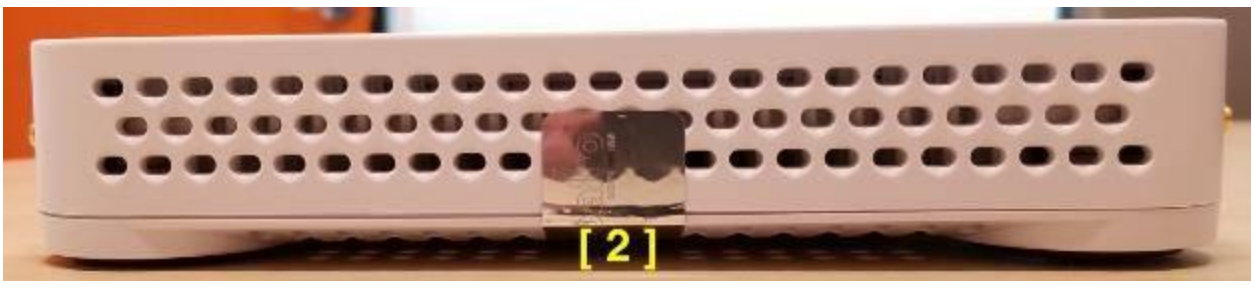
Surface Preparation: Clean the chassis of any grease, dirt, or oil before applying the tamper evident labels

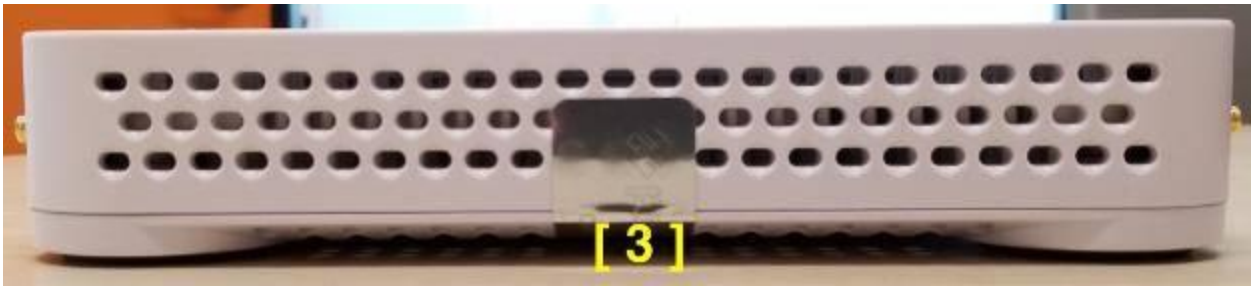
Operator Responsible for Securing Unused Seals: Crypto Officer

Part Numbers: 920-000455

PA-415-5G
Number: 3

Placement:





Surface Preparation: Clean the chassis of any grease, dirt, or oil before applying the tamper evident labels

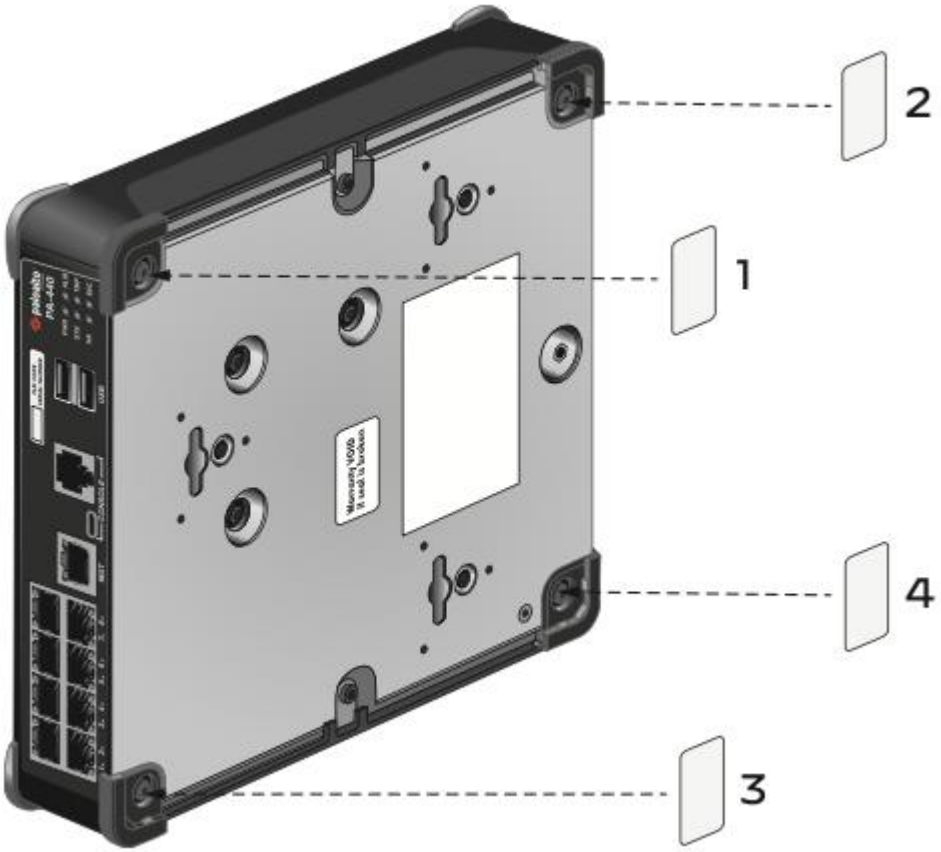
Operator Responsible for Securing Unused Seals: Crypto Officer

Part Numbers: 920-000454

PA-440/450/460

Number: The PA-440/450/460 require 4 tamper evident labels

Placement:



Surface Preparation: Clean the chassis of any grease, dirt, or oil before applying the tamper evident labels

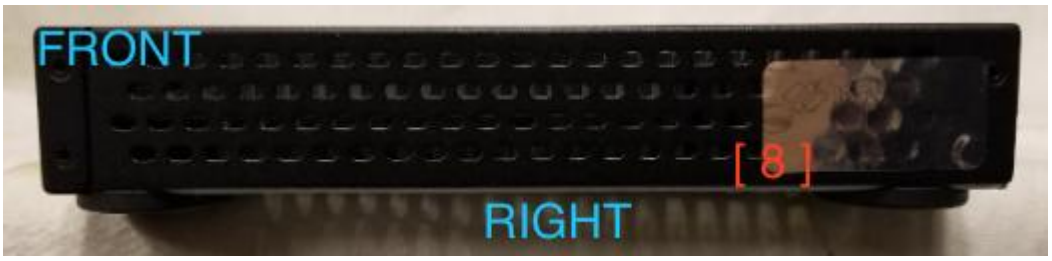
Operator Responsible for Securing Unused Seals: Crypto Officer

Part Numbers: 920-000454

PA-445

Number: The PA-445 requires 8 tamper evident labels.

Placement:



Surface Preparation: Clean the chassis of any grease, dirt, or oil before applying the tamper evident labels

Operator Responsible for Securing Unused Seals: Crypto Officer

Part Numbers: 920-000455

PA-450R / PA-450R-5G / PA-455
Number: 3

Placement:

Surface Preparation: Clean the chassis of any grease, dirt, or oil before applying the tamper evident labels

Operator Responsible for Securing Unused Seals: Crypto Officer

Part Numbers: 920-000454

PA-455-5G
Number: 2

Placement:

Surface Preparation: Clean the chassis of any grease, dirt, or oil before applying the tamper evident labels

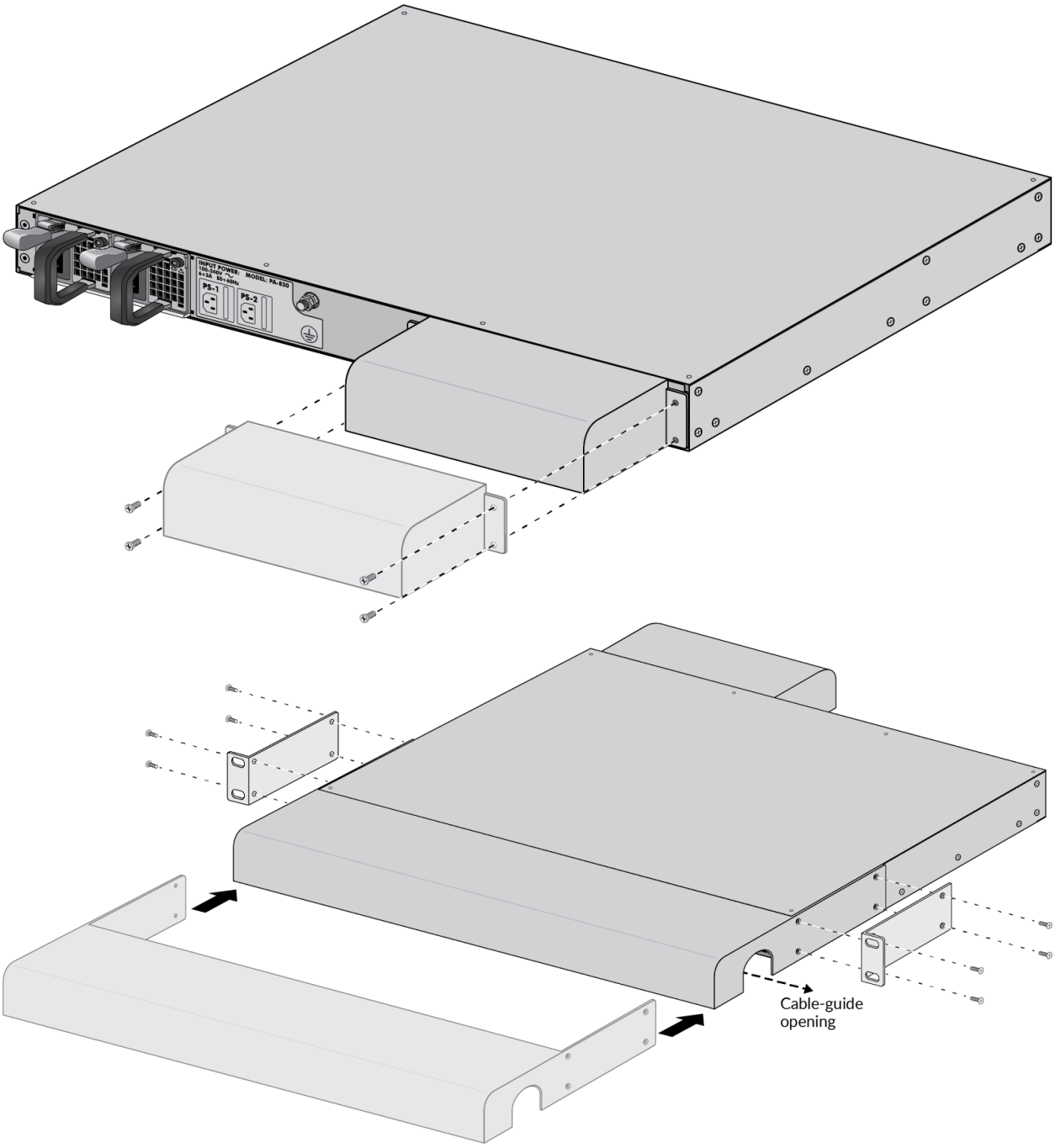
Operator Responsible for Securing Unused Seals: Crypto Officer

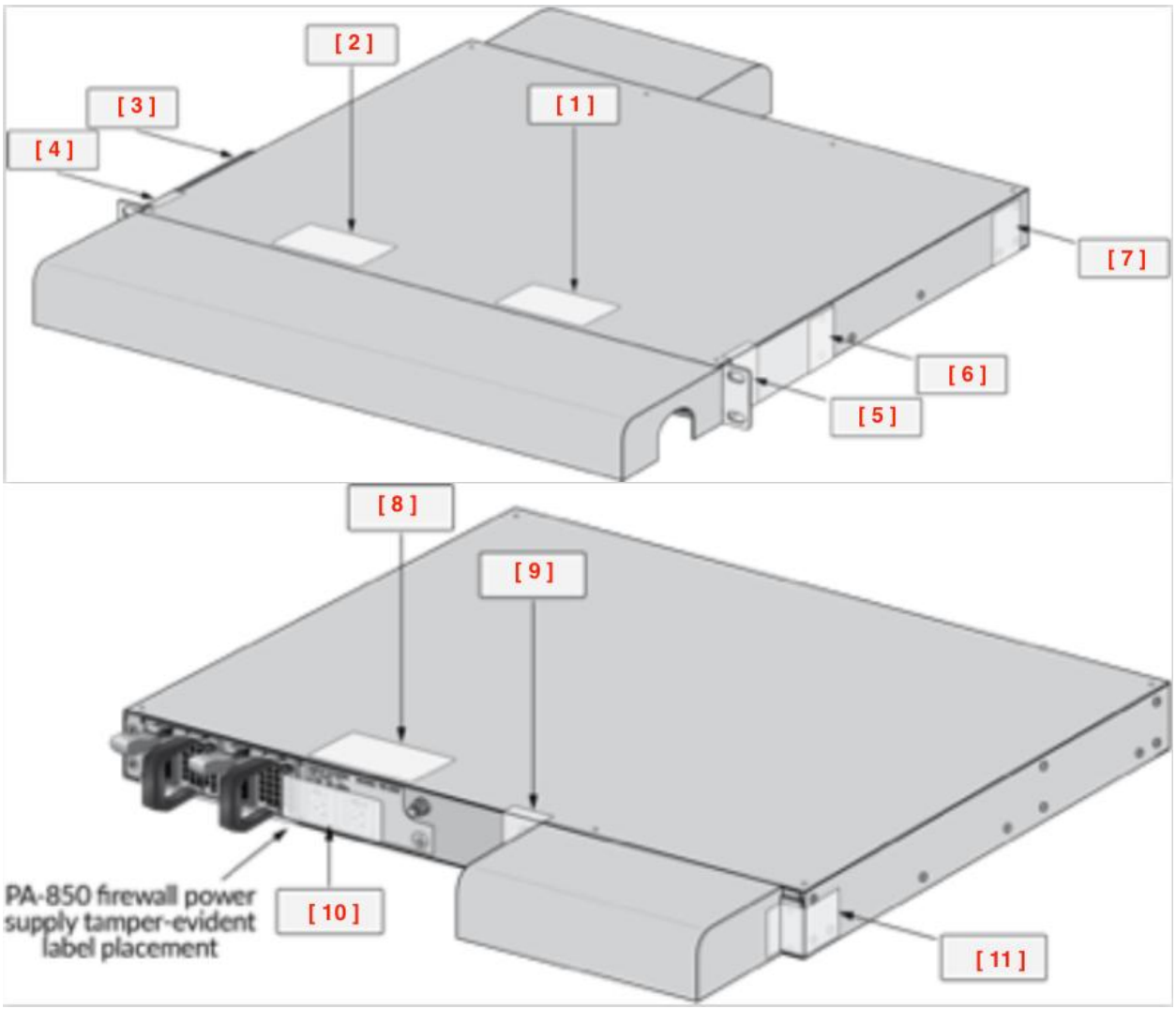
Part Numbers: 920-000454

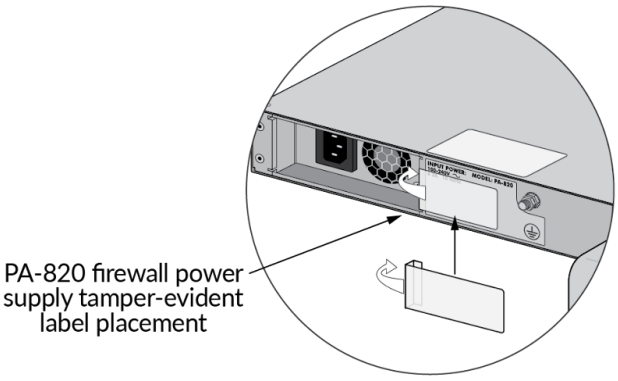
PA-800

Number: The PA-800 series requires 11 tamper evident labels

Placement:


PS-1
PS-2
Cable-guide
opening





Surface Preparation: Clean the chassis of any grease, dirt, or oil before applying the tamper evident labels

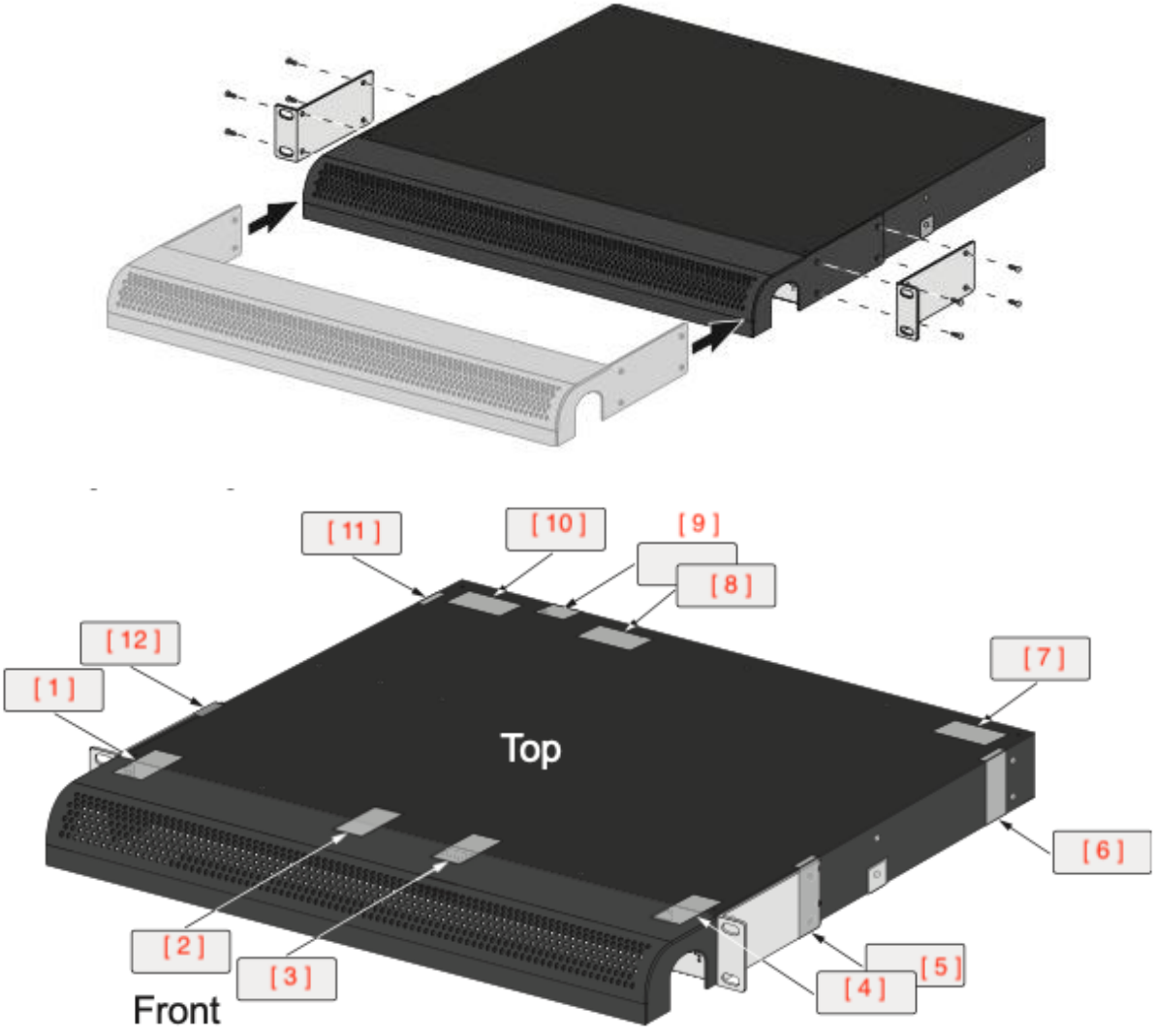
Operator Responsible for Securing Unused Seals: Crypto Officer

Part Numbers: 920-000185

PA-1400 and PA-3400

Number: The PA-1400 and PA-3400 series require 12 tamper evident labels

Placement:



Surface Preparation: Clean the chassis of any grease, dirt, or oil before applying the tamper evident labels

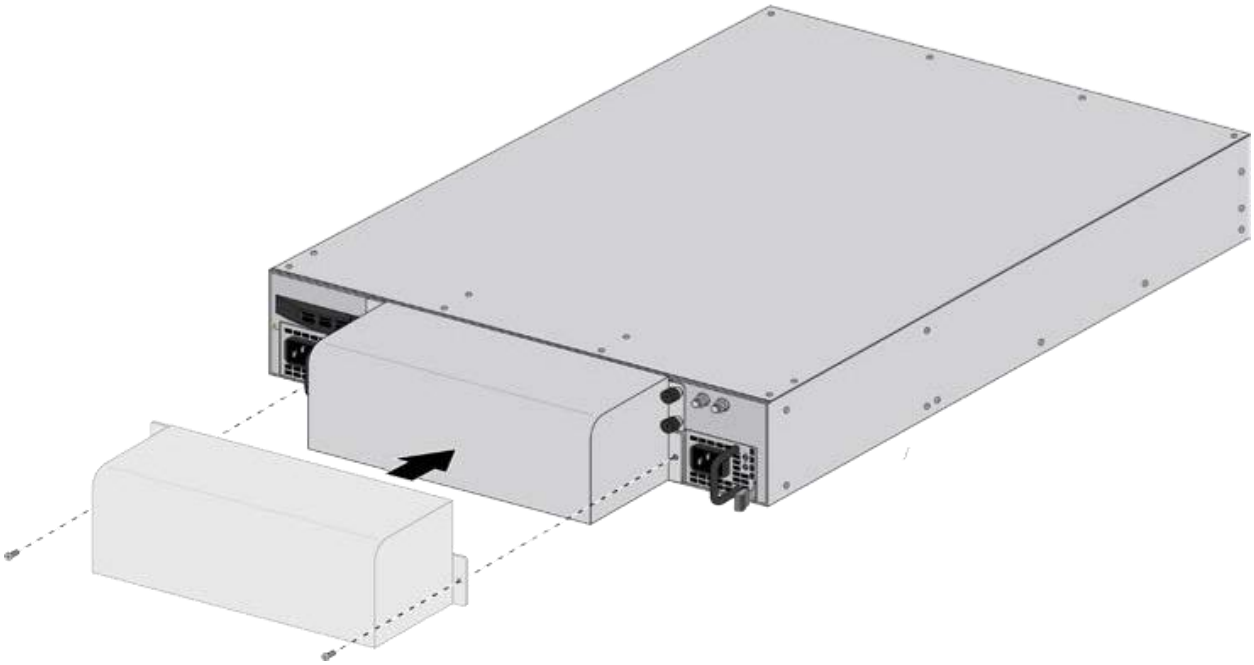
Operator Responsible for Securing Unused Seals: Crypto Officer

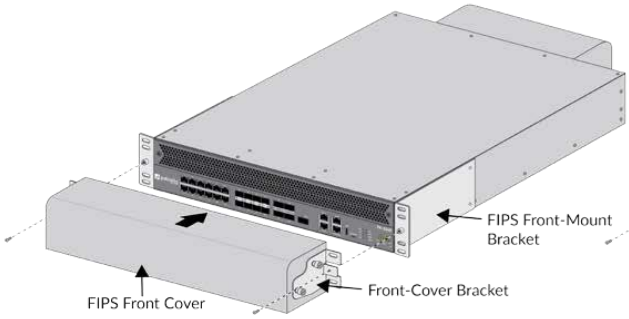
Part Numbers: 920-000392

PA-3200

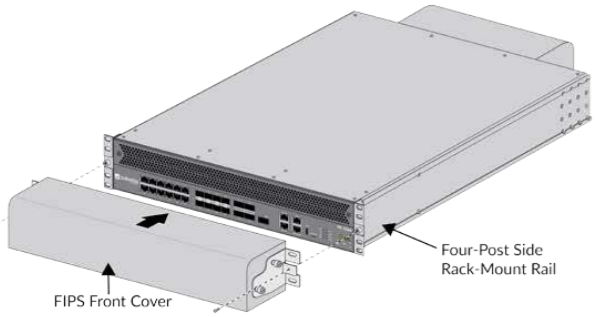
Number: The PA-3200 requires 19 tamper evident labels

Placement:

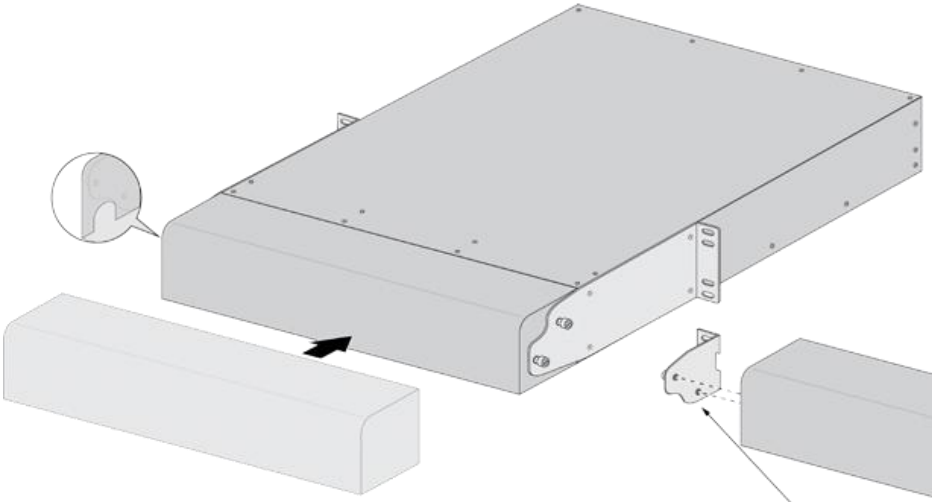




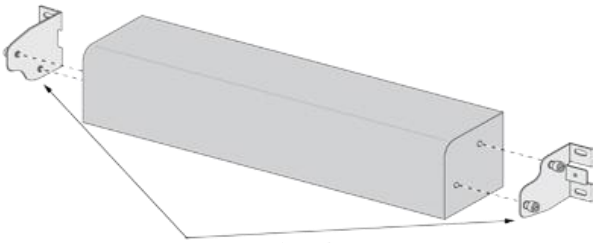
Front-Mount Install



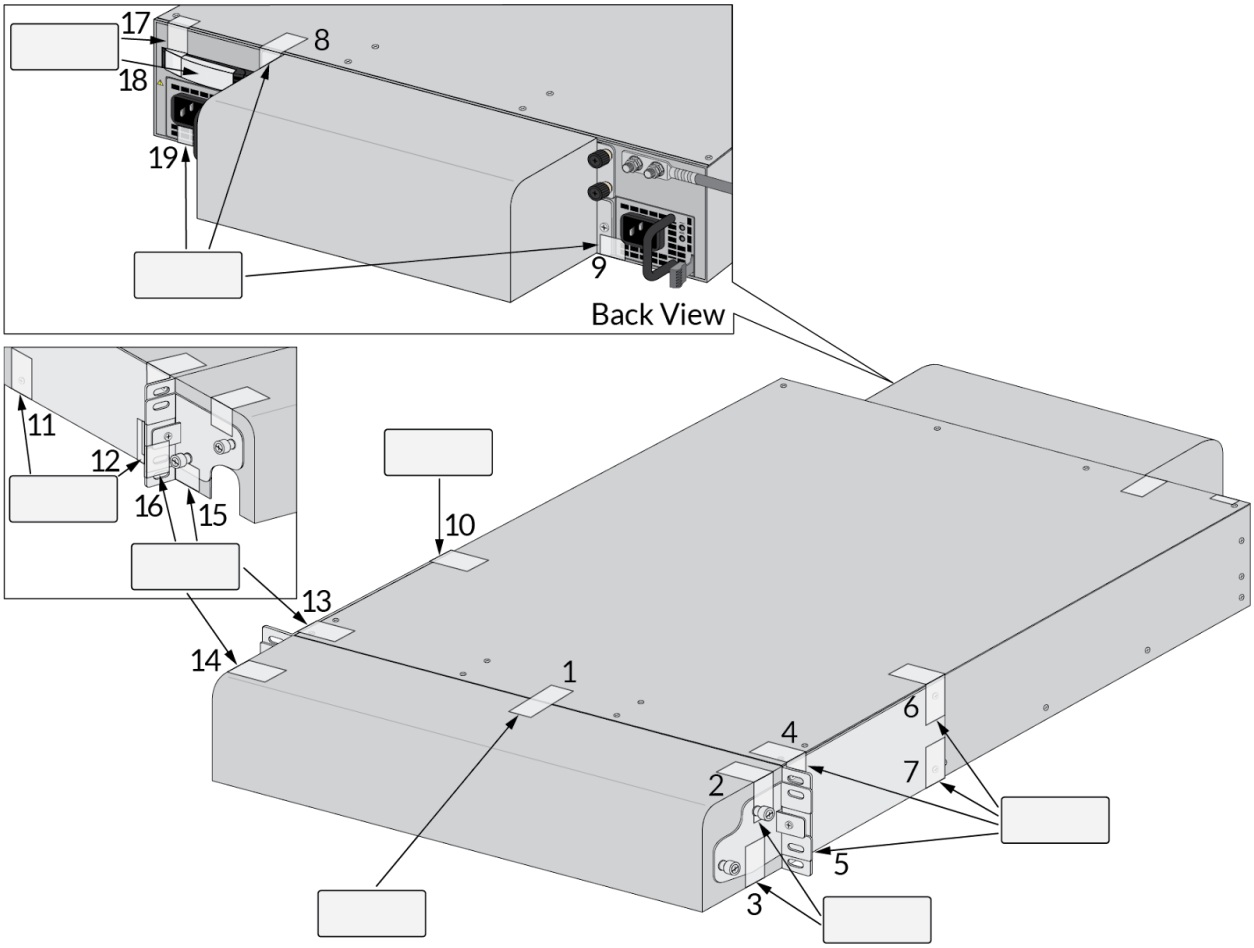
Four-Post Rack Kit Install



Front Cover Mid-Mount Bracket Install



Remove Front Cover Brackets for
Mid-Mount Bracket Install



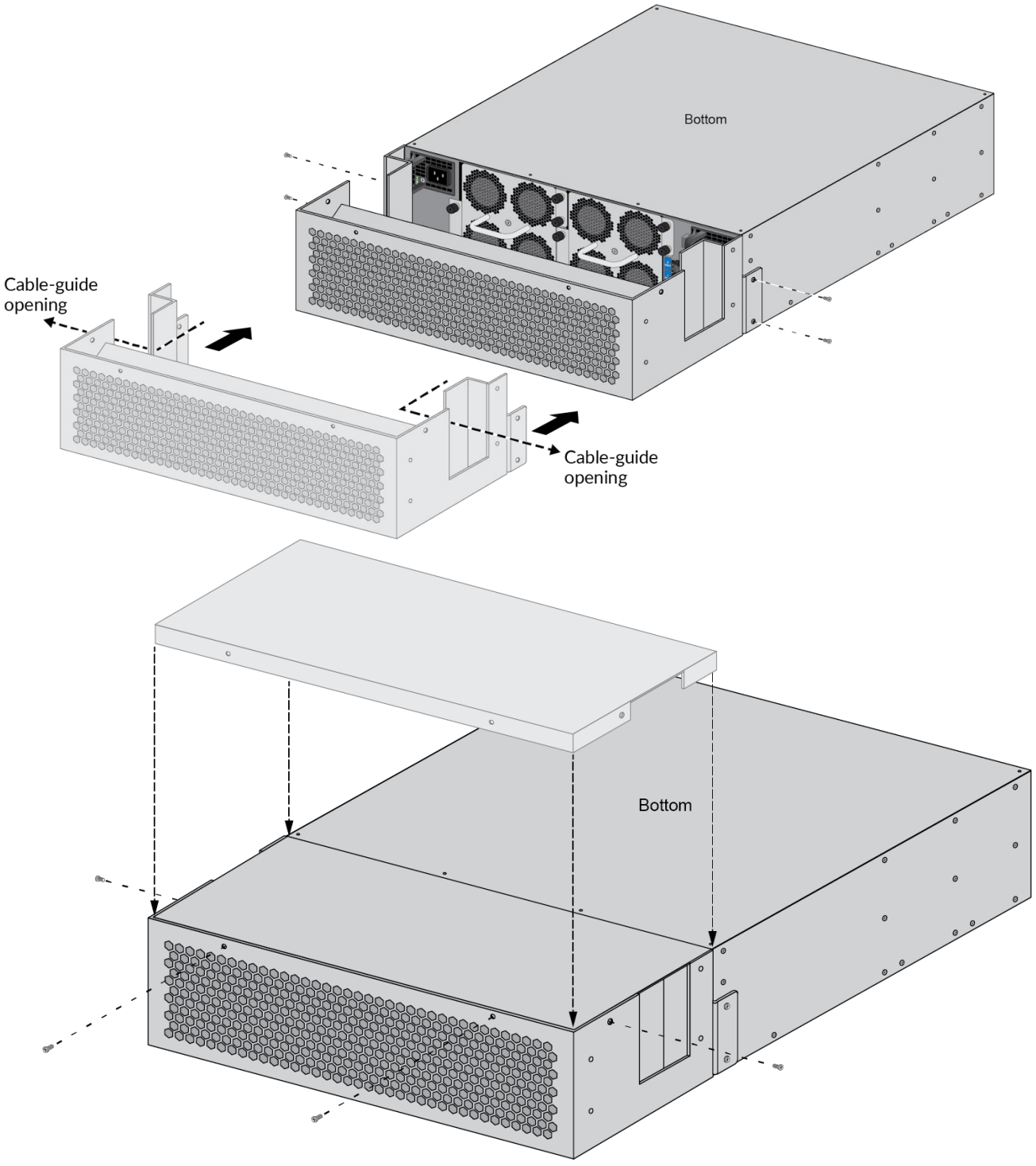
Surface Preparation: Clean the chassis of any grease, dirt, or oil before applying the tamper evident labels

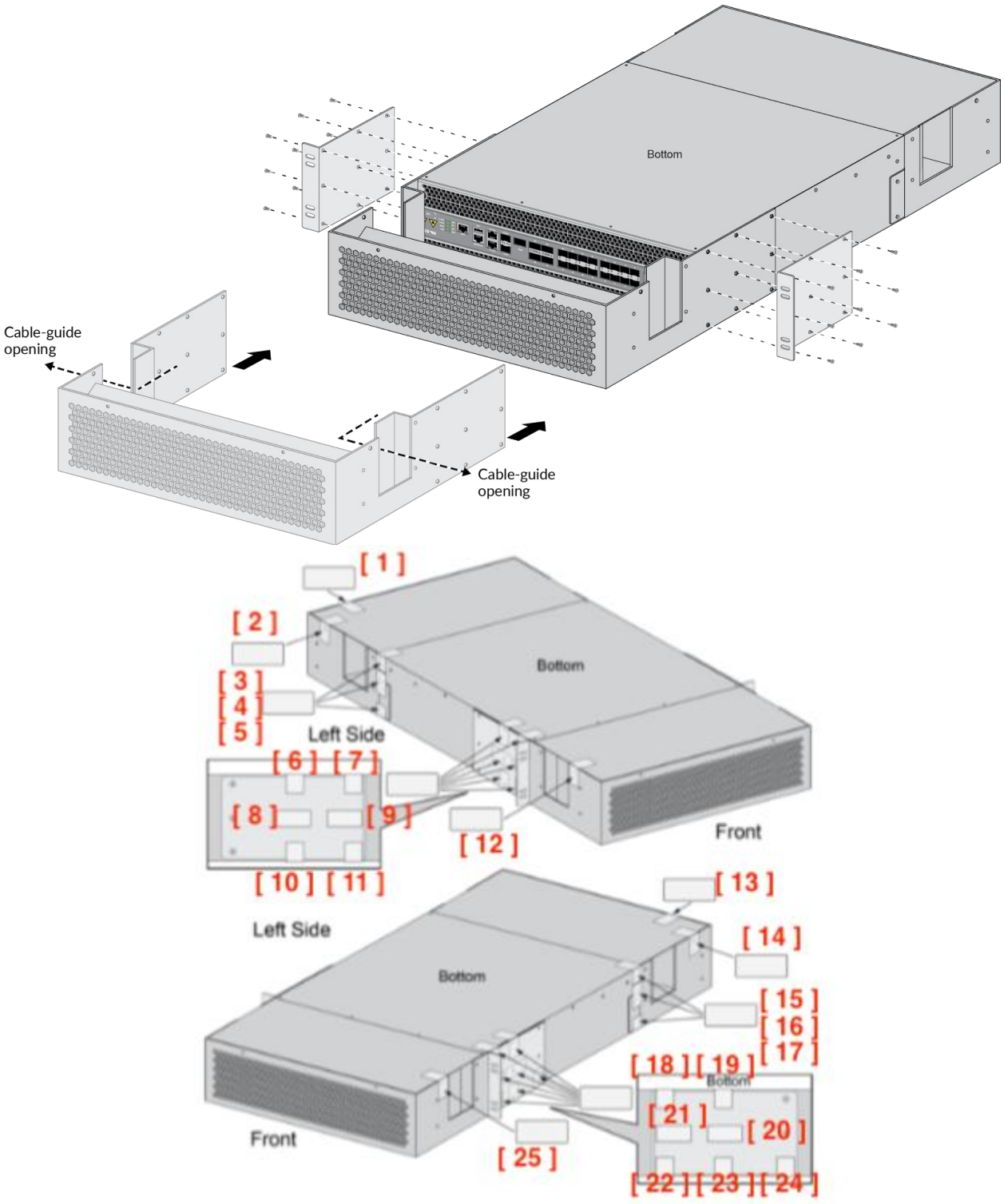
Operator Responsible for Securing Unused Seals: Crypto Officer

Part Numbers: 920-000212

PA-5200
Number: The PA-5200 series requires 28 tamper evident labels

Placement:


Bottom
Cable-guide opening
Cable-guide opening
Bottom



Surface Preparation: Clean the chassis of any grease, dirt, or oil before applying the tamper evident labels

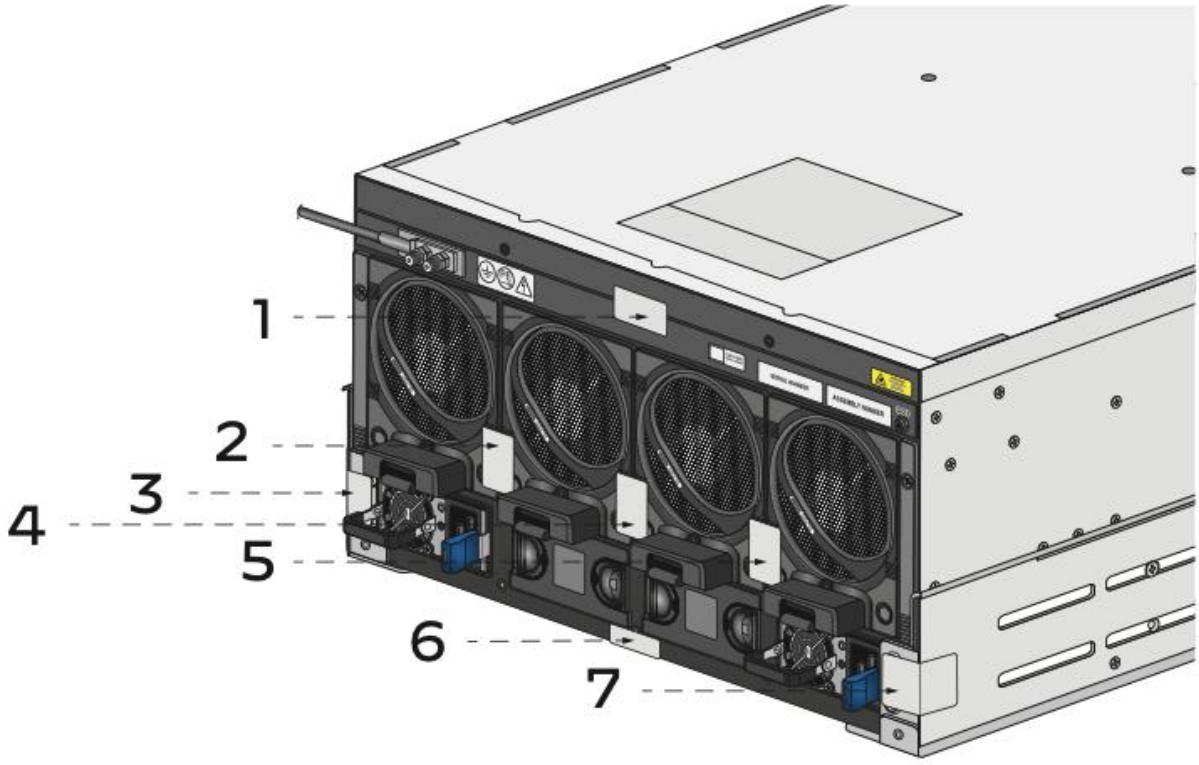
Operator Responsible for Securing Unused Seals: Crypto Officer

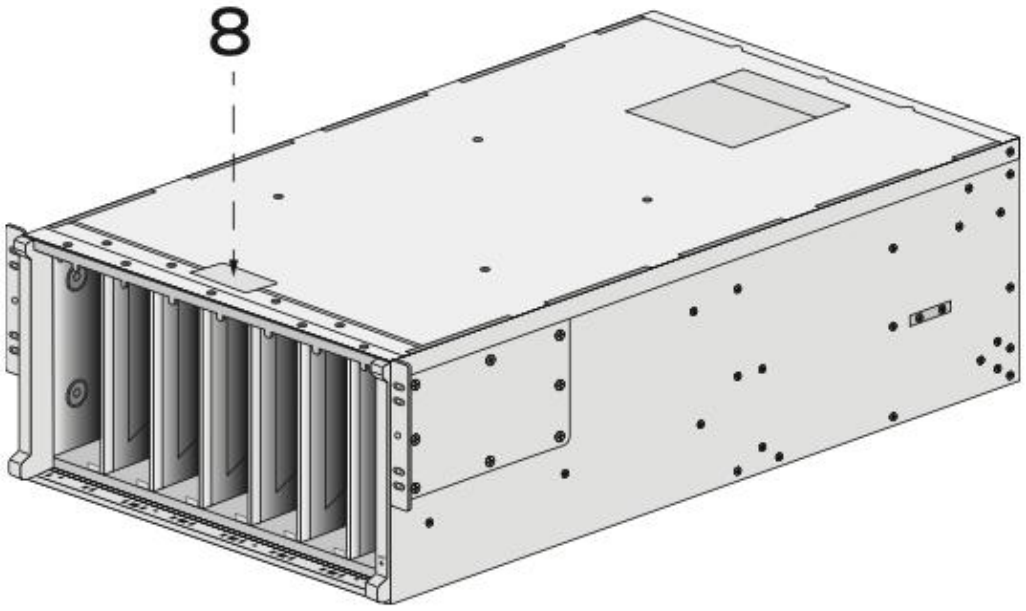
Part Numbers: 920-000186

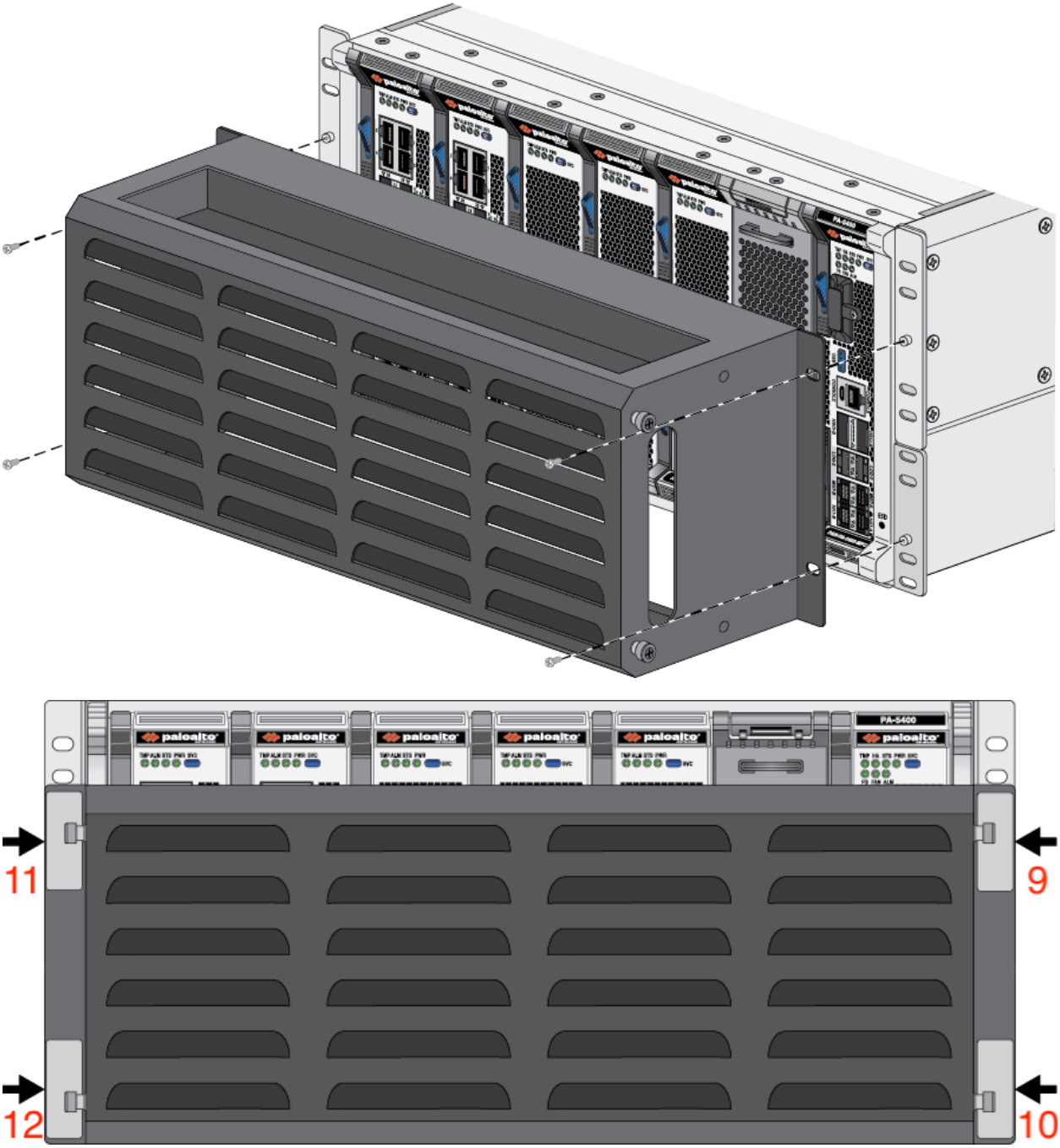
PA-5450

Number: The PA-5450 requires 12 tamper evident labels

Placement:







Surface Preparation: Clean the chassis of any grease, dirt, or oil before applying the tamper evident labels

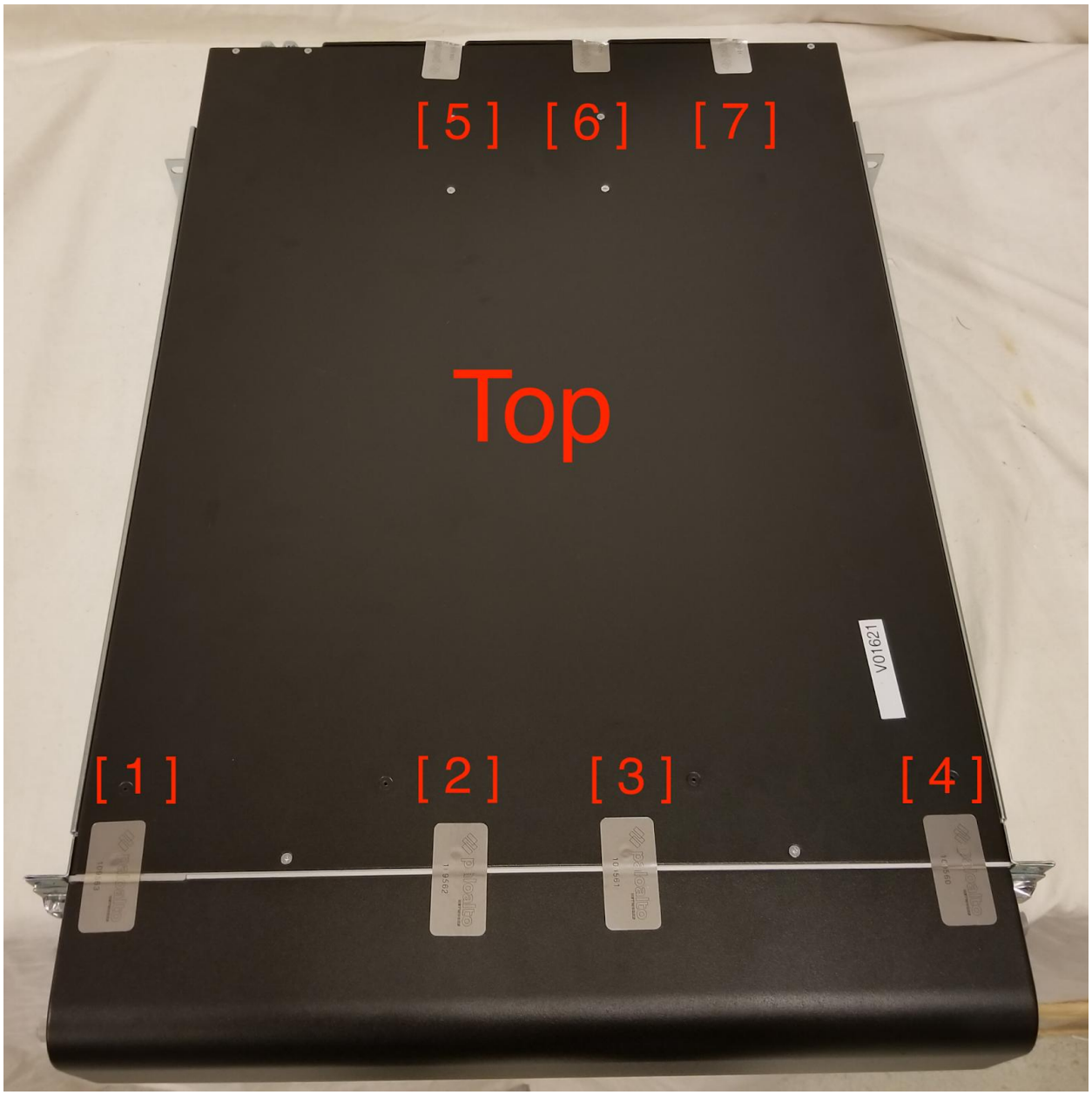
Operator Responsible for Securing Unused Seals: Crypto Officer

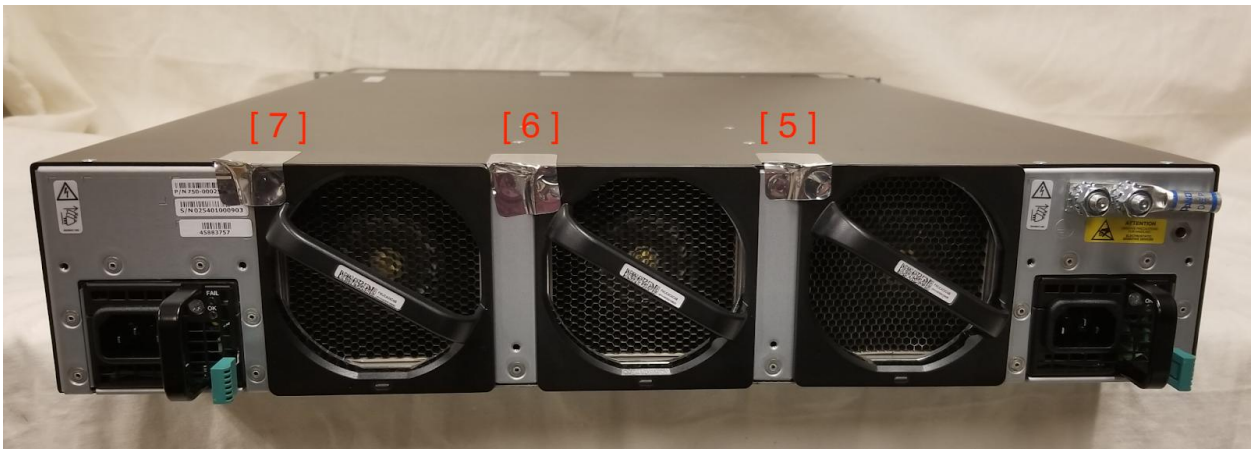
Part Numbers: 920-000309

PA-5400

Number: The PA-5400 series requires 11 tamper evident labels

Placement:





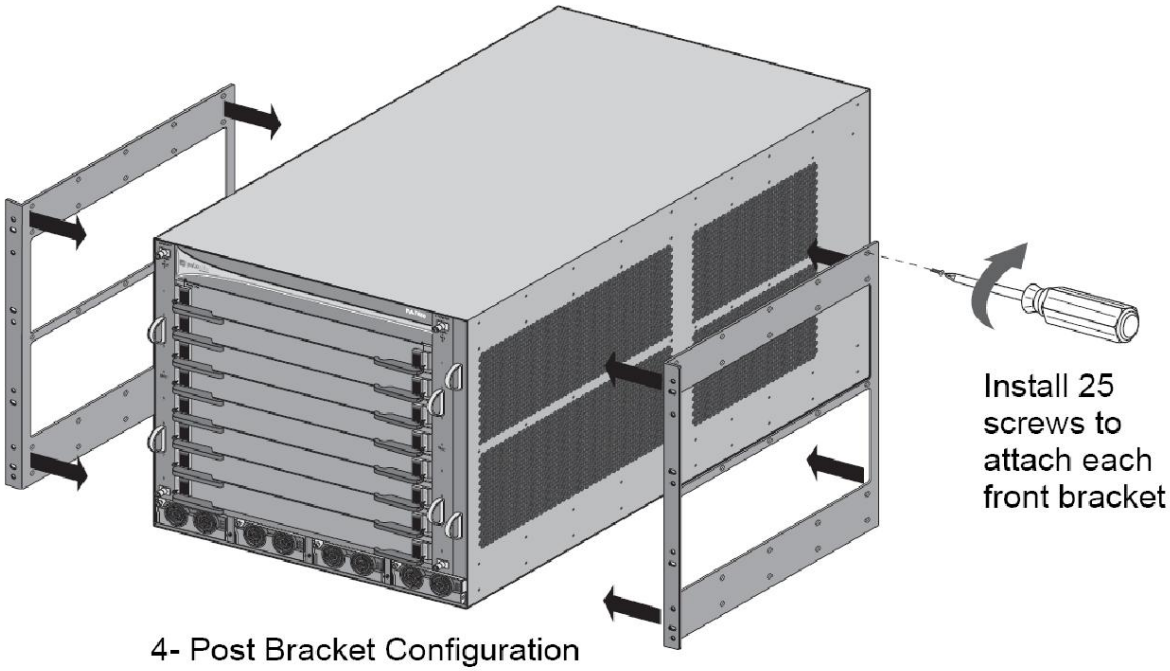
Surface Preparation: Clean the chassis of any grease, dirt, or oil before applying the tamper evident labels

Operator Responsible for Securing Unused Seals: Crypto Officer

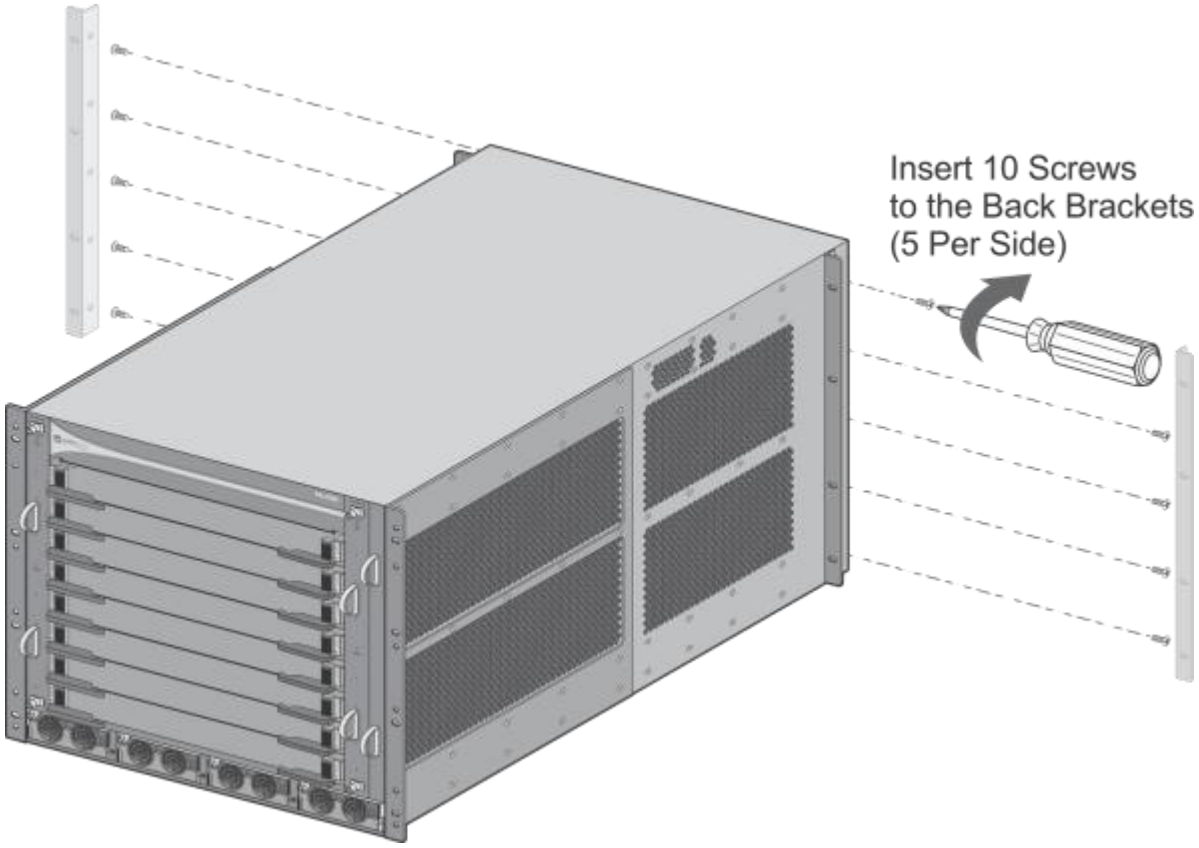
Part Numbers: 920-000320

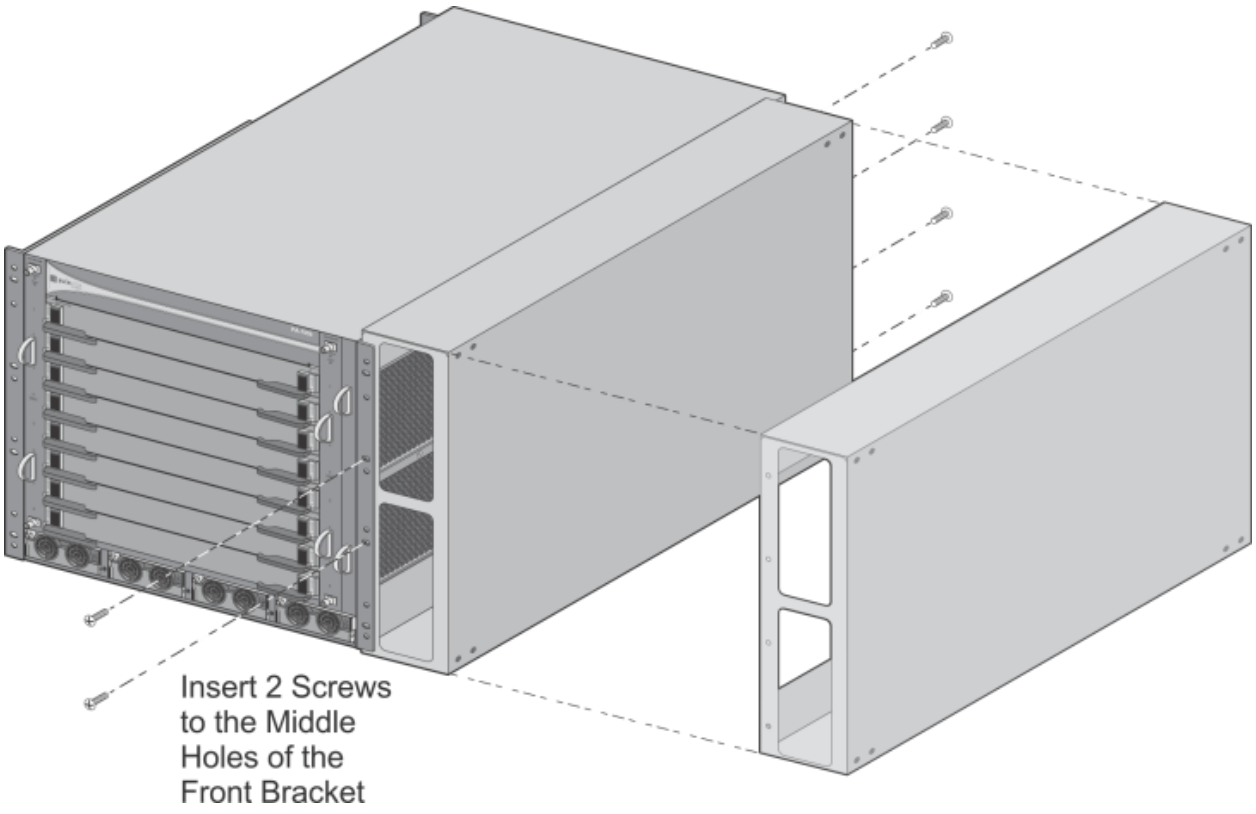
PA-7050
Number: The PA-7050 requires 24 tamper evident labels

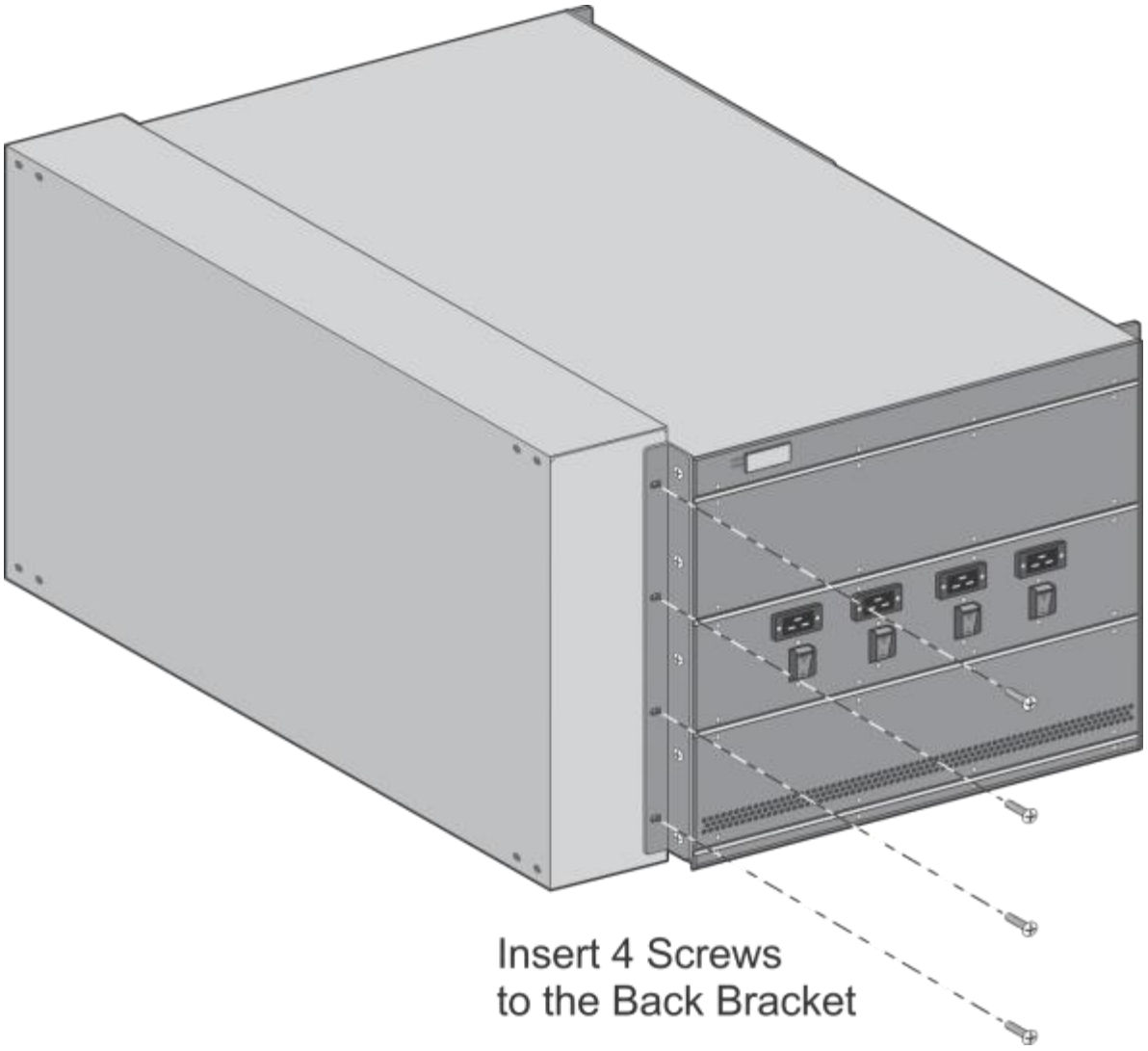
Placement:

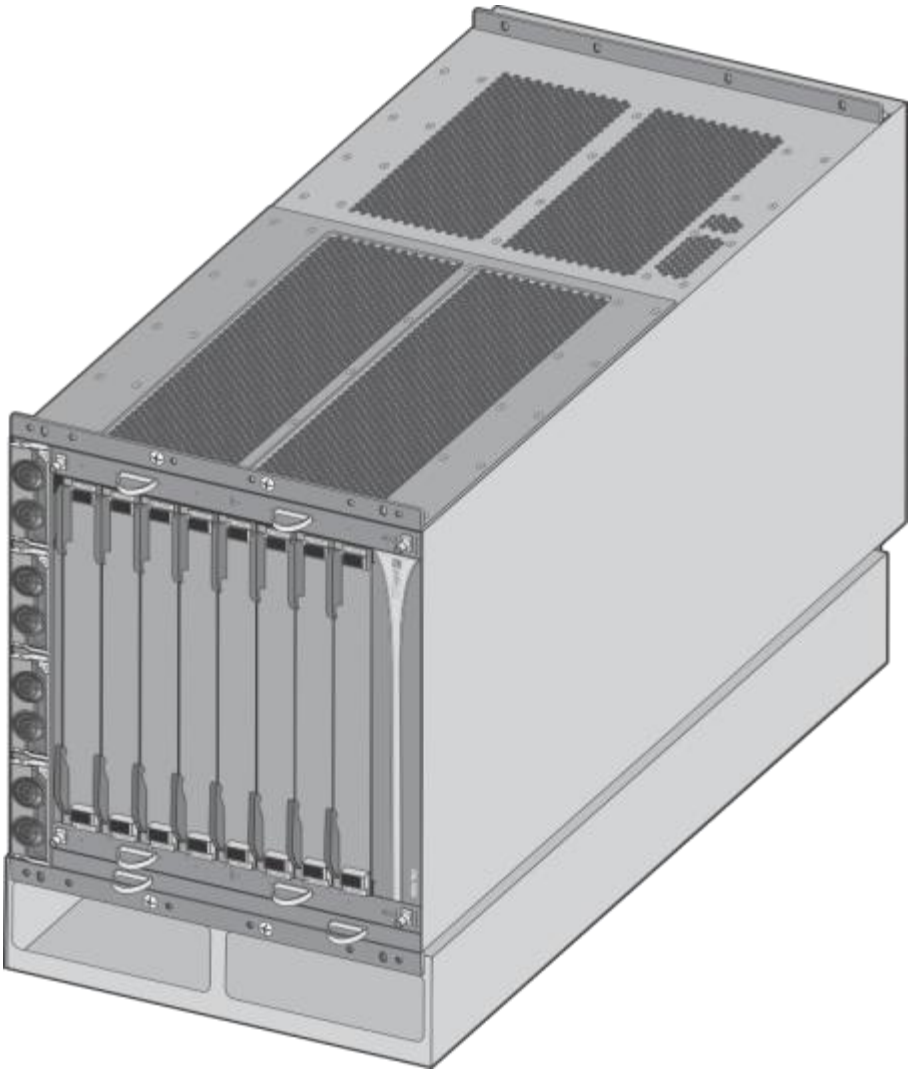


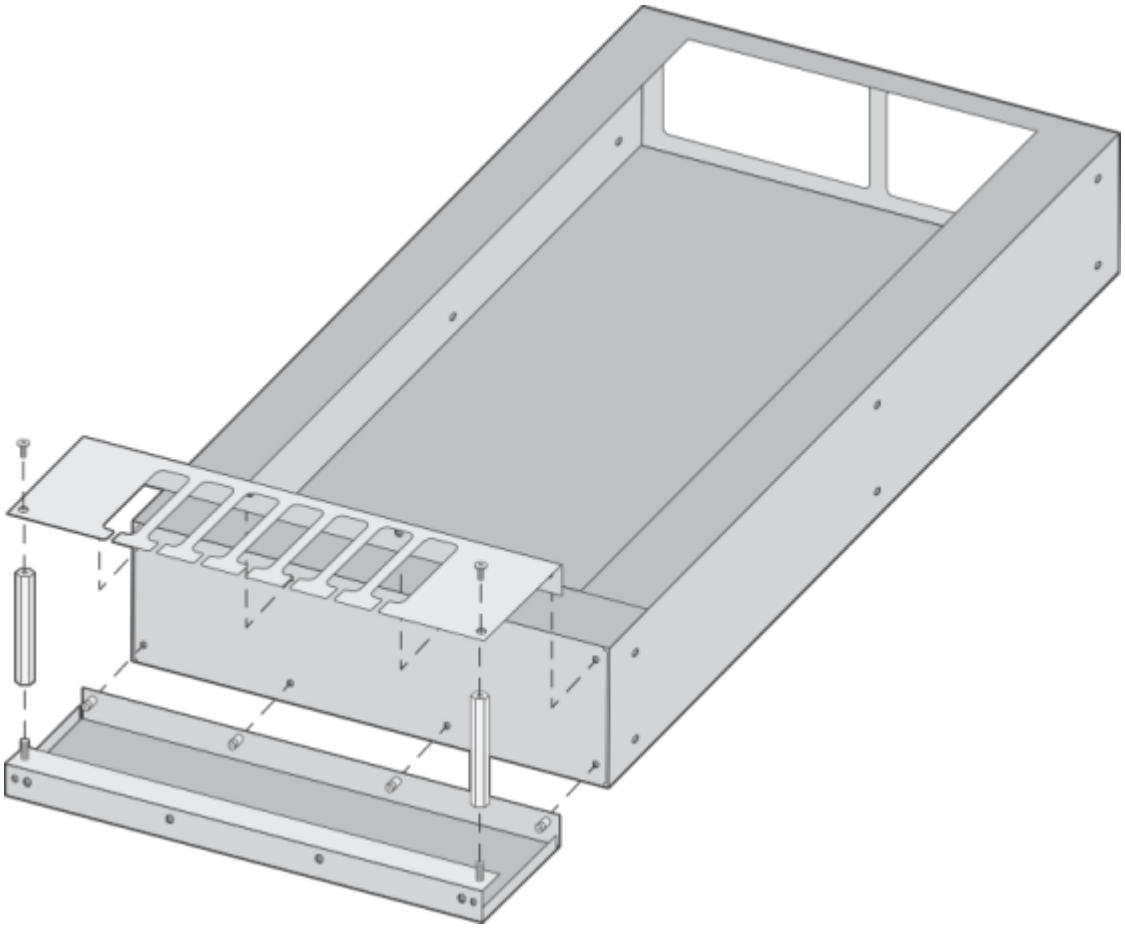
4- Post Bracket Configuration

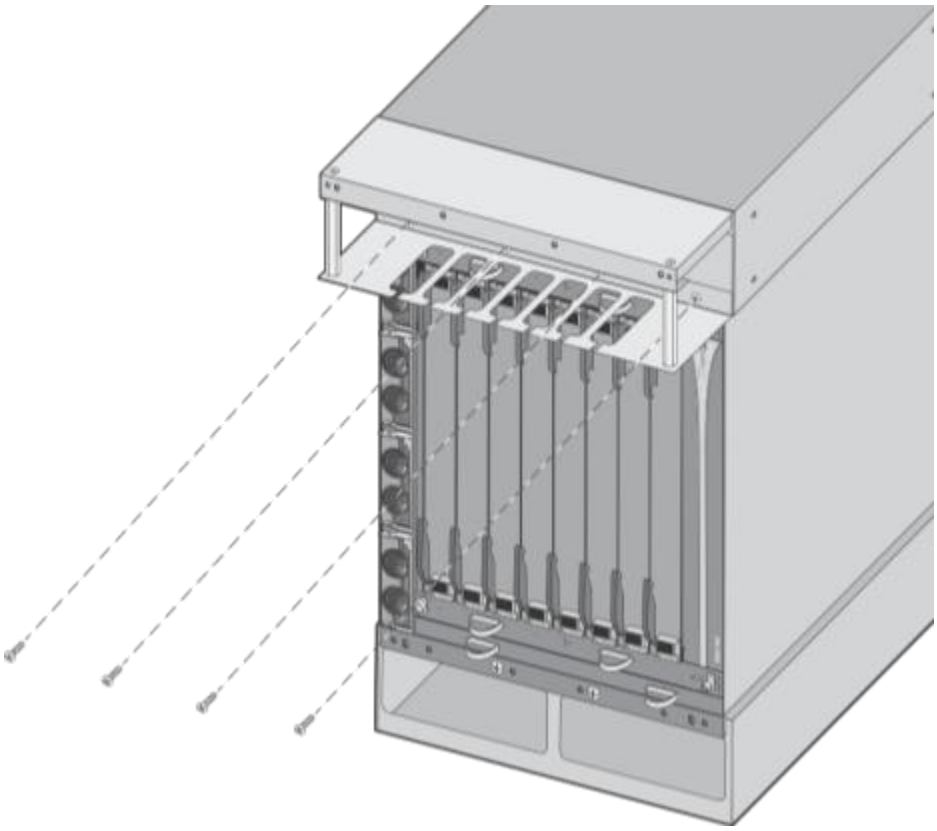


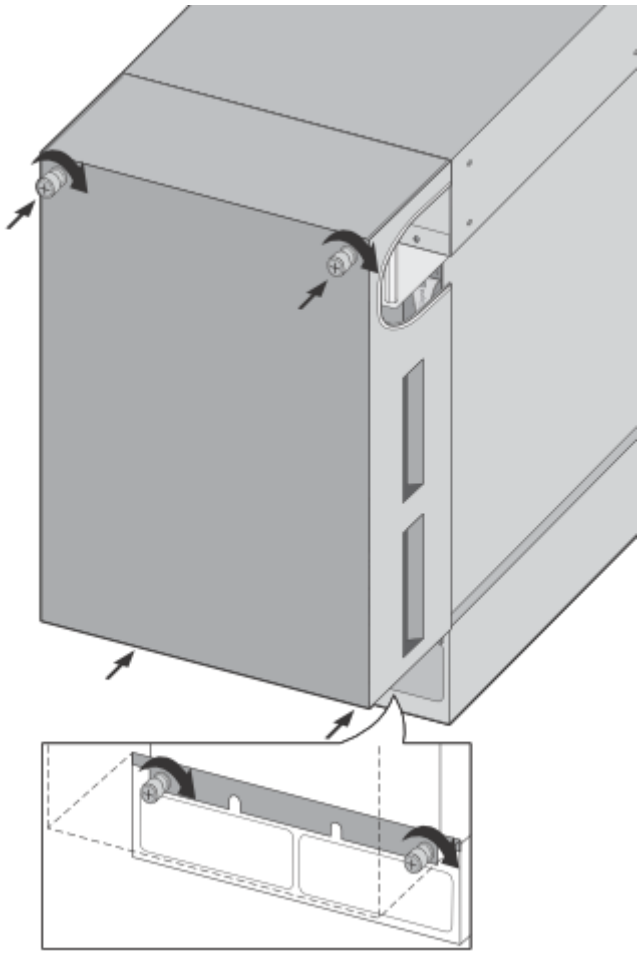

Insert 2 Screws
to the Middle
Holes of the
Front Bracket

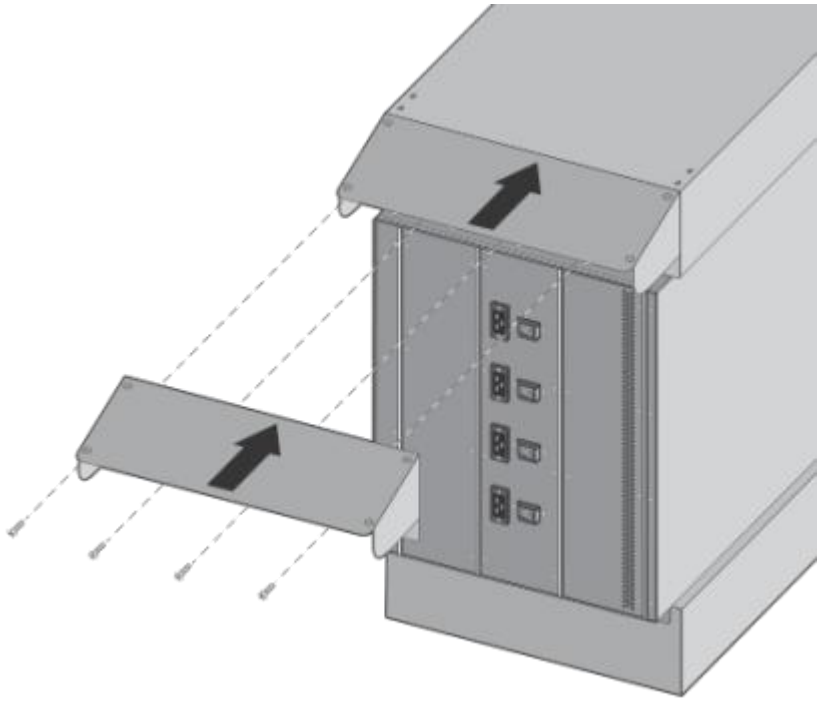

Insert 4 Screws
to the Back Bracket

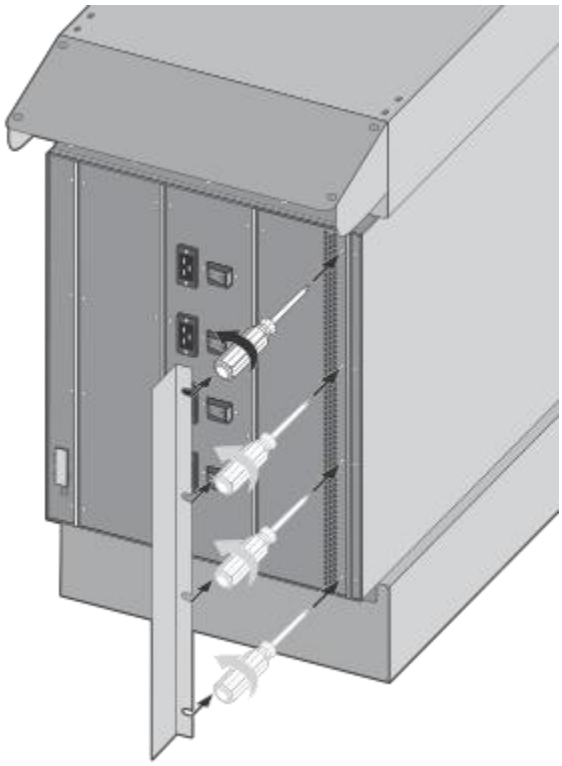


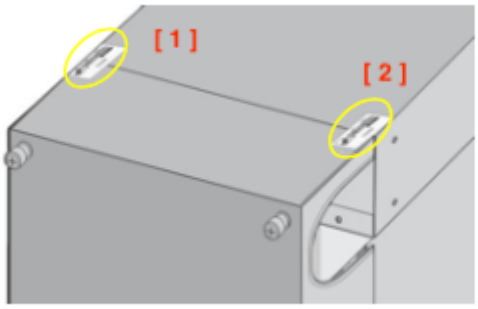


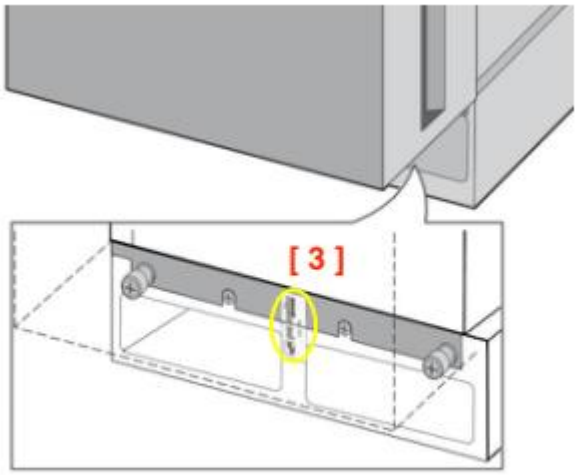


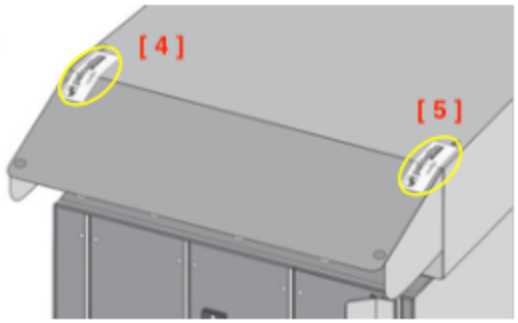


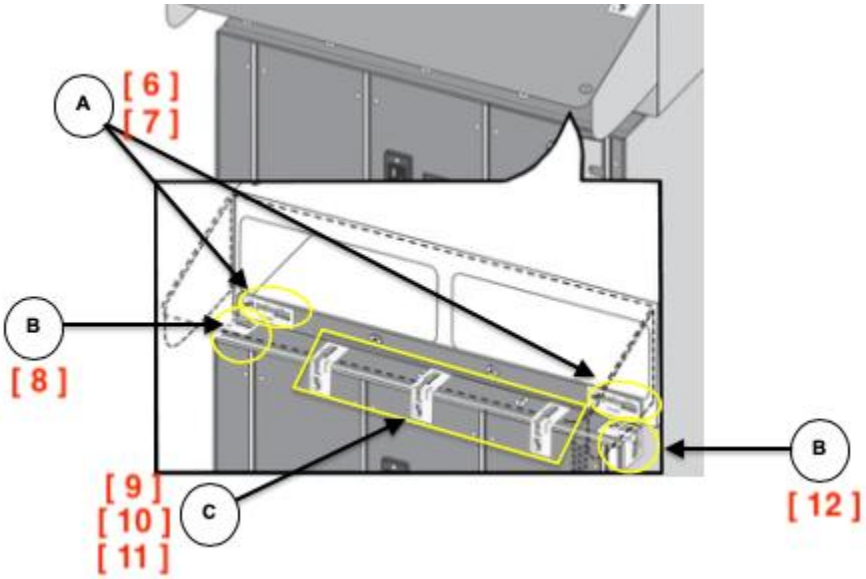


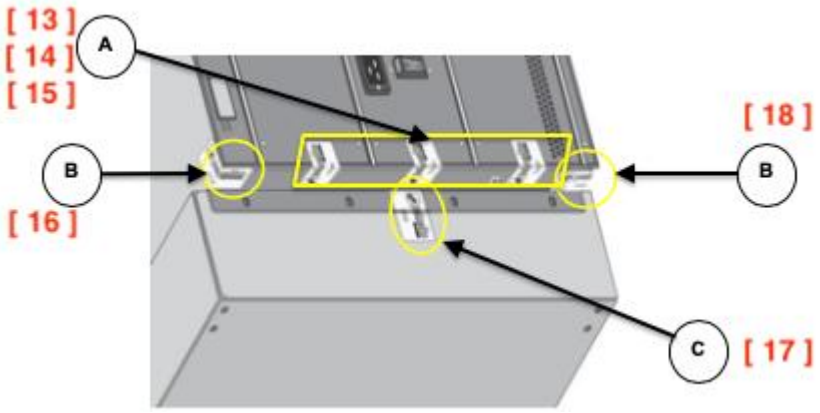


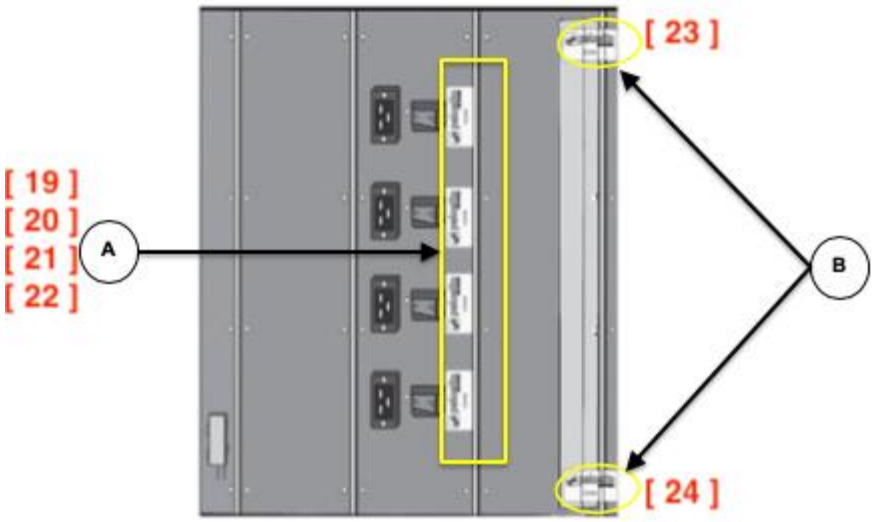

[1]
[2]


[3]


[4]
[5]


A
[6]
[7]
B
[8]
[9]
[10]
[11]
C
B
[12]


[13]
[14]
[15]
A
B
[16]
[18]
B
C
[17]



Surface Preparation: Clean the chassis of any grease, dirt, or oil before applying the tamper evident labels

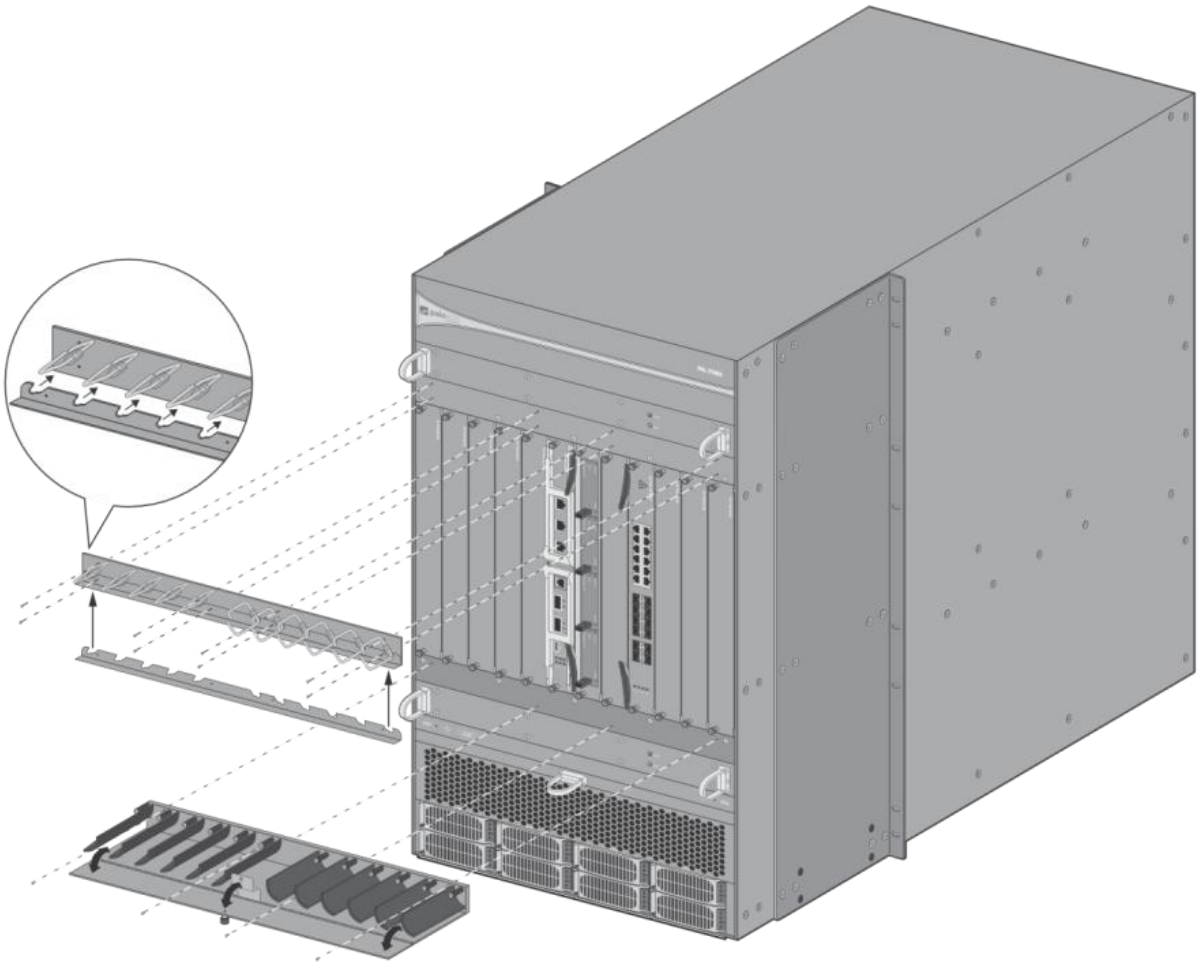
Operator Responsible for Securing Unused Seals: Crypto Officer

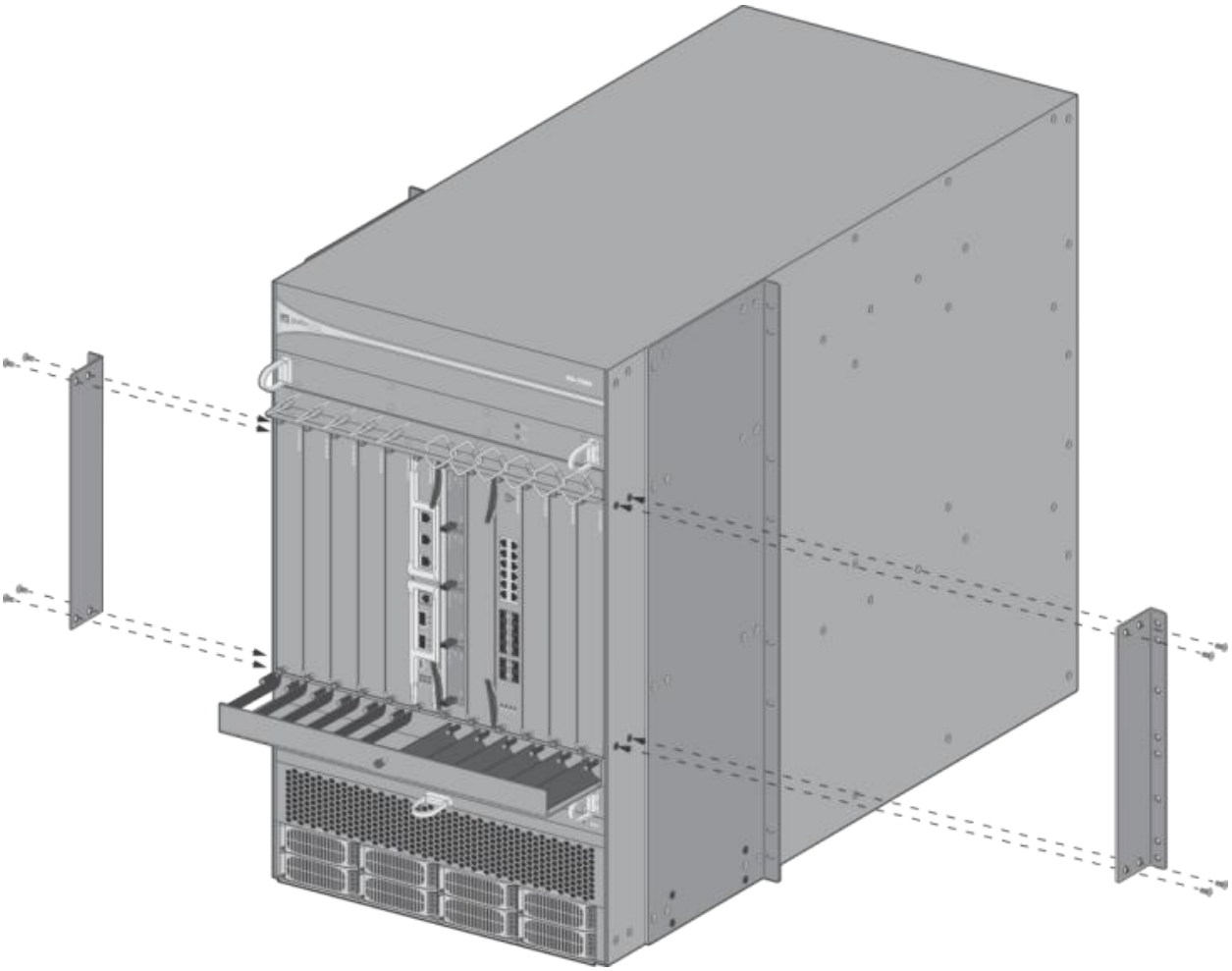
Part Numbers: 920-000112

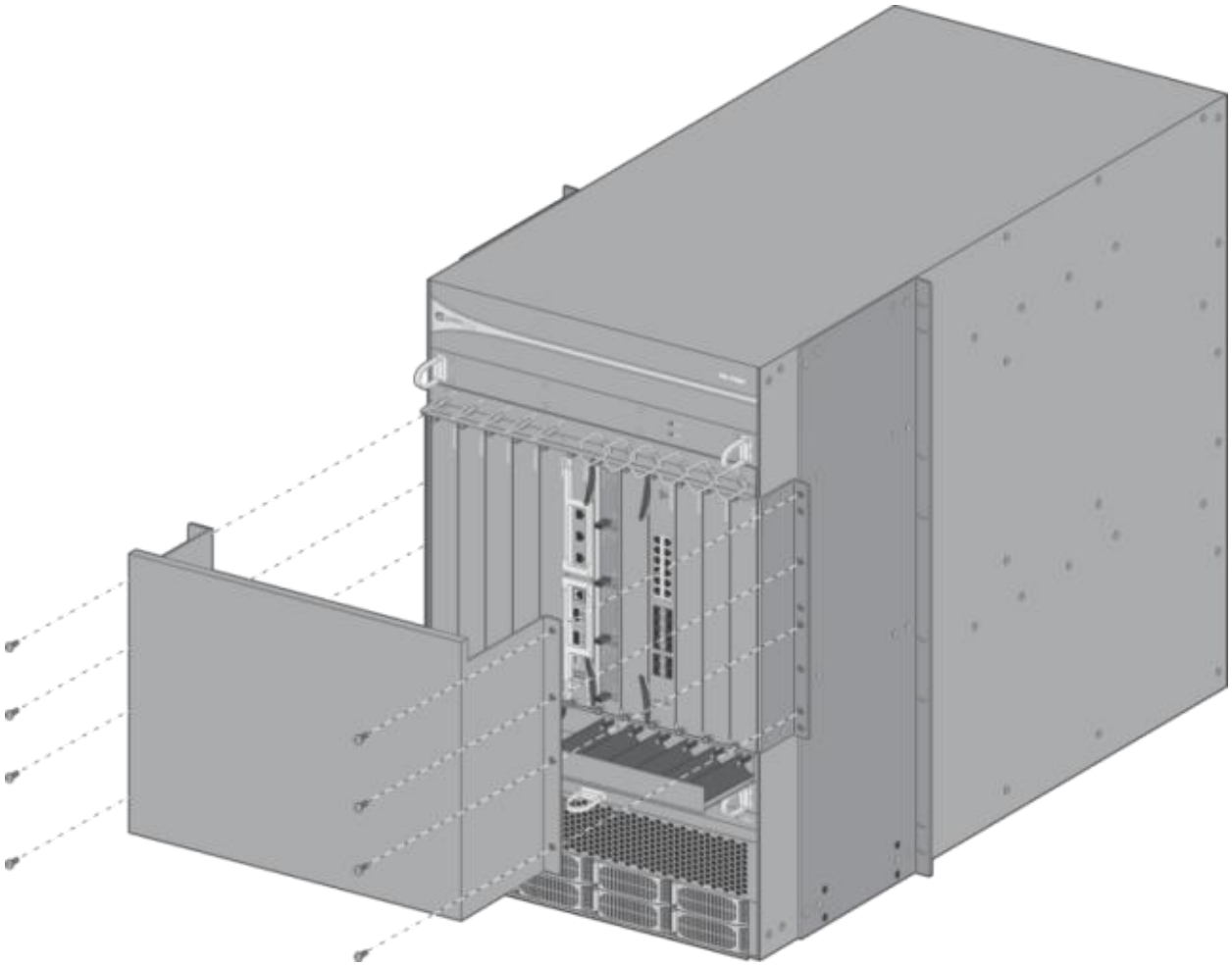
PA-7080

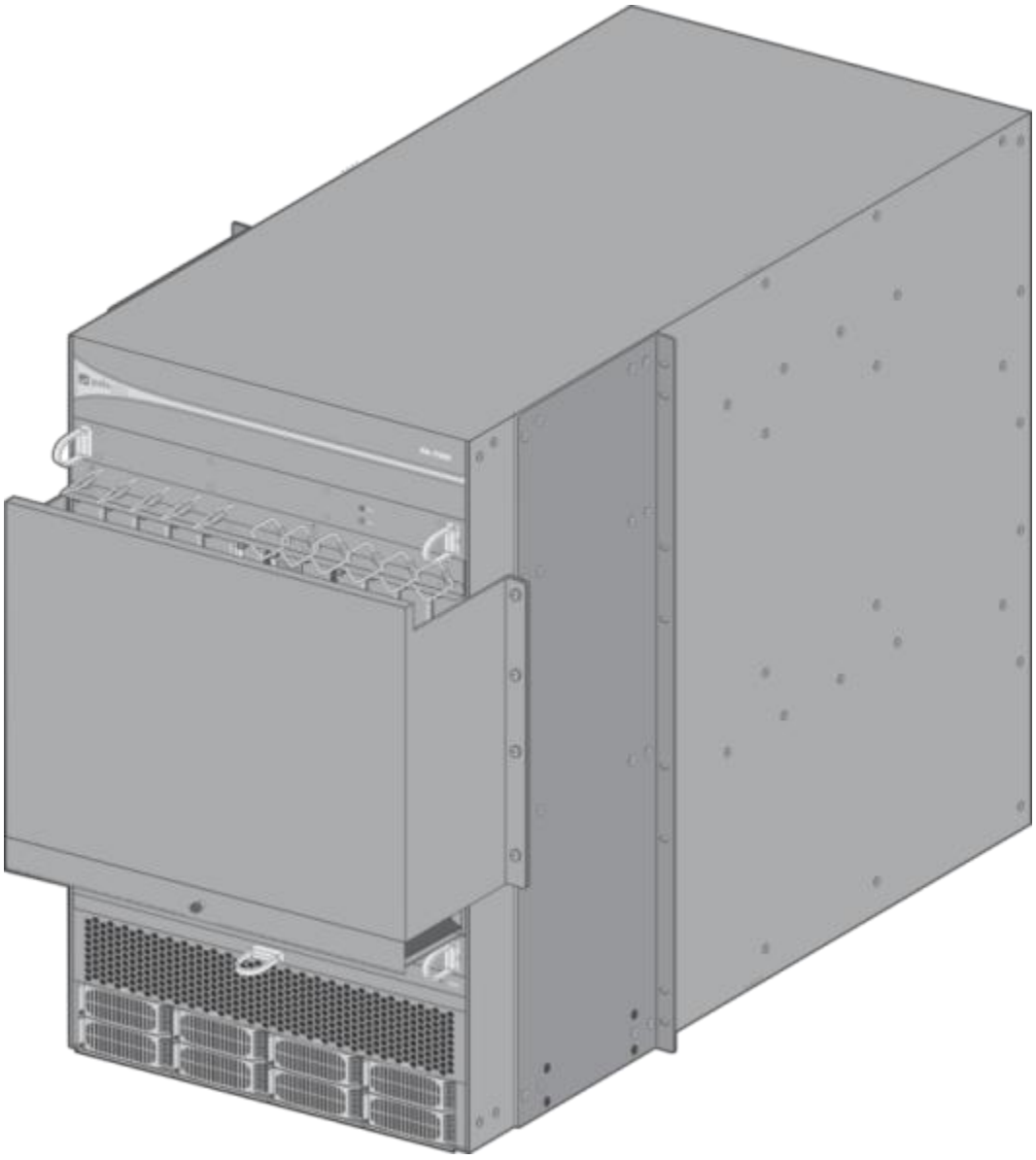
Number: The PA-7080 requires 10 tamper evident labels

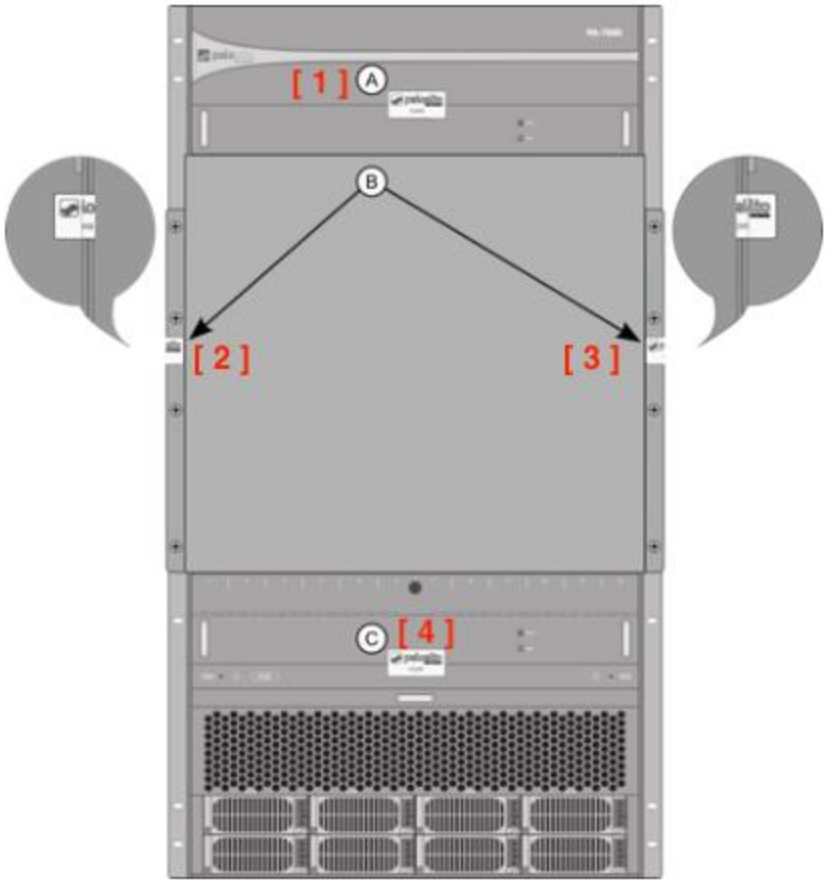
Placement:

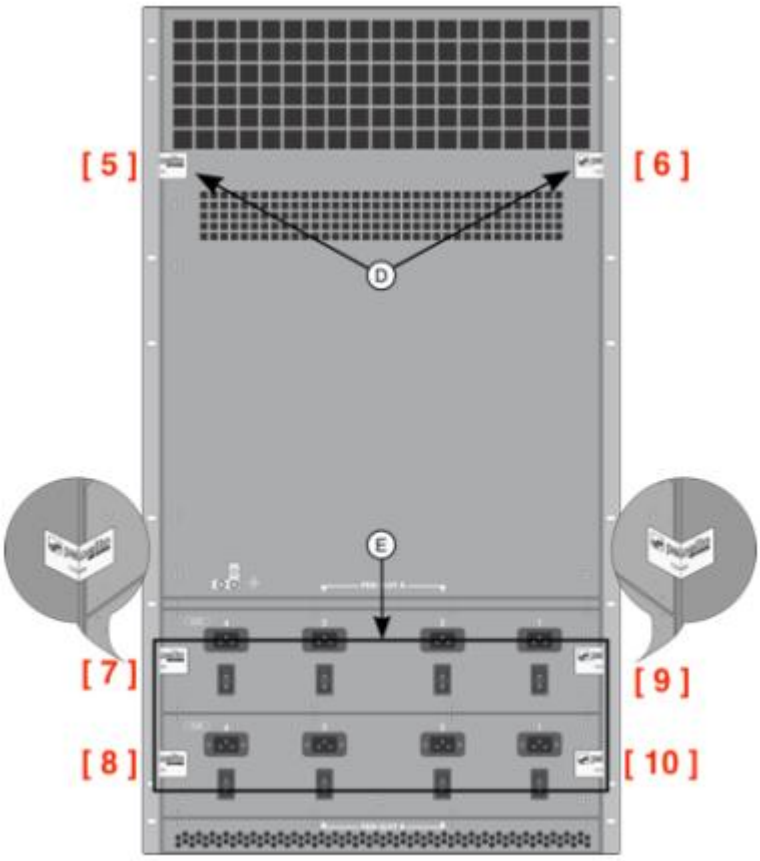









[1]
A
B
[2]
[3]
C
[4]



Surface Preparation: Clean the chassis of any grease, dirt, or oil before applying the tamper evident labels

Operator Responsible for Securing Unused Seals: Crypto Officer

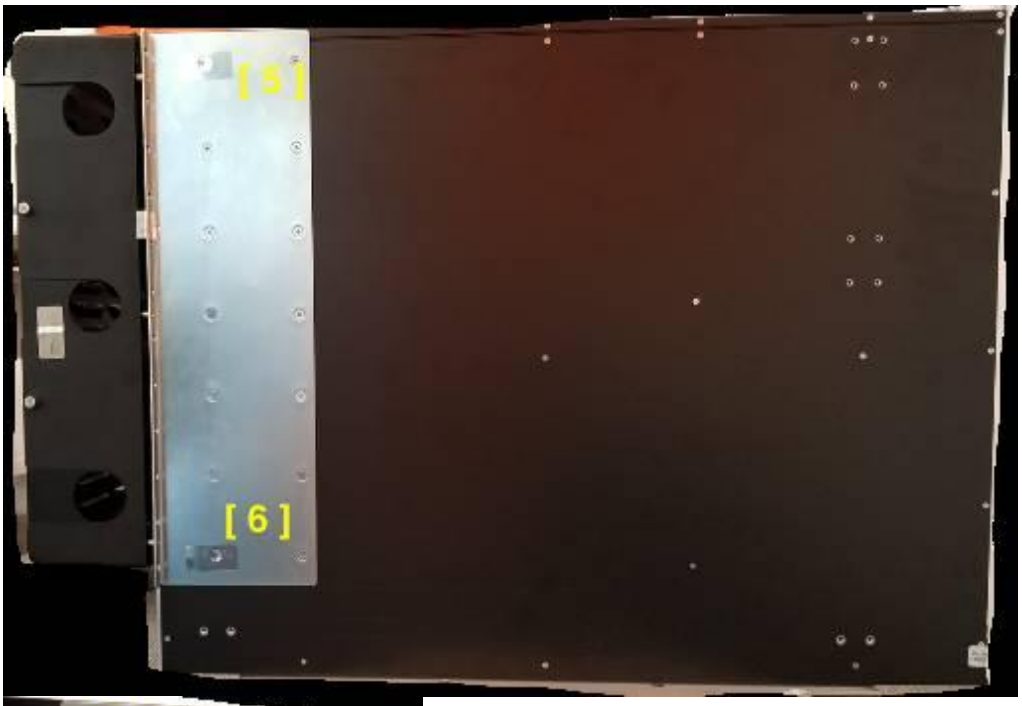
Part Numbers: 920-000119

PA-7500
Number: 17

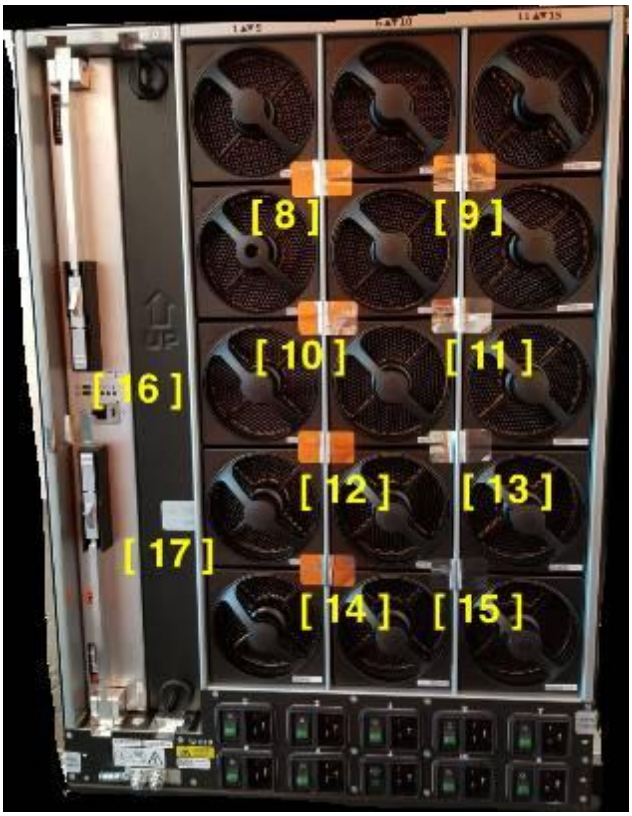
Placement:


[2]
[1]


[3]
[4]


[5]
[6]


[7]
[8]



Surface Preparation: Clean the chassis of any grease, dirt, or oil before applying the tamper evident labels

Operator Responsible for Securing Unused Seals: Crypto Officer

Part Numbers: 920-000362

8 Non-Invasive Security

N/A

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
HDD	Non-Volatile Memory	Static
RAM	Volatile Memory	Dynamic

Table 14: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Module Public Key Output	HDD	External (Outside of the Module's Boundary)	Plaintext	Automated	Electronic	
Password/Secret Input via SSHv2 encrypted by AES and HMAC	External (outside of module's boundary)	HDD	Encrypted	Automated	Electronic	KTS (SSHv2 with AES and HMAC)
Password/Secret Input via SSHv2 encrypted by AES-GCM	External (outside of module's boundary)	HDD	Encrypted	Automated	Electronic	KTS (SSHv2 with AES-GCM)
Password/Secret Input via TLSv1.2 encrypted by AES and HMAC	External (outside of module's boundary)	HDD	Encrypted	Automated	Electronic	KTS (TLSv1.2 with AES and HMAC)
Password/Secret Input via TLSv1.2 encrypted by AES-GCM	External (outside of module's boundary)	HDD	Encrypted	Automated	Electronic	KTS (TLSv1.2 with AES-GCM)
Peer Public Key Input	External (outside of module's boundary)	HDD	Plaintext	Automated	Electronic	

Table 15: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Power Cycle / Session Termination	Operator powers the module off or session terminates	Powering off the module or terminating the session will erase all SSPs stored in the RAM of the module.	Command via CLI or WebUI or by unplugging module
Zeroization Command	CO issues zeroization service	The zeroization command will erase all SSPs stored in the RAM or in the Flash of the module.	Entering into maintenance mode and selecting Factory Reset

Table 16: SSP Zeroization Methods

Once the module is rebooted and zeroization is initiated, the module cannot be accessed in any way and the zeroization process cannot be stopped, thus the SSPs would not be compromised during the time of zeroization. The Crypto Officer shall be in control of the module until the zeroization process is complete.

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
CA Certificates	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)	2048 bits, 3072 bits, 4096 bits; 256 bits, 384 bits, 521 bits - 112 bits,128 bits, 150 bits; 128 bits,192 bits, 256 bits	Public Key - PSP	SSH ECDSA KeyGen SSH RSA KeyGen TLS ECDSA KeyGen TLS RSA KeyGen		TLS RSA SigGen TLS RSA SigVer TLS ECDSA SigGen TLS ECDSA SigVer

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
CO, User, RA VPN Password	Authentication string with a minimum length of eight (8) characters	8 characters minimum - N/A	Authentication Data - CSP			
DHE/ECDHE Shared Secret Z	Used to derive encryption keys	2048 bits, 3072 bits, 4096 bits; 256 bits, 384 bits, 521 bits - 112 bits,128 bits, 150 bits; 128 bits,192 bits, 256 bits	Key Agreement shared secret - CSP	KDF IKEv2 (A3453) KDF SSH (A3453)		KAS-ECC (IPSec/IKE) KAS-FFC (IPSec/IKE)
DRBG Key	AES 256 CTR DRBG state Key used in the generation of a random values	256 bits - 256 bits	DRBG Key - CSP	Counter DRBG (A3453)		Counter DRBG (A3453)
DRBG Seed	DRBG seed coming from the entropy source Seed length = 384 bits	384 bits - 256 bits	DRBG Seed - CSP	Entropy Source		Counter DRBG (A3453)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
DRBG V	AES 256 CTR DRBG state V used in the generation of a random values	128 bits - 128 bits	DRBG Internal State V value - CSP	Counter DRBG (A3453)		Counter DRBG (A3453)
ECDSA Private Keys	ECDSA Private key for generation of signatures and authentication (P-256, P-384, or P-521)	256 bits, 384 bits, 521 bits - 128 bits, 192 bits, 256 bits	Private Key - CSP	SSH ECDSA KeyGen TLS ECDSA KeyGen		TLS ECDSA SigGen
ECDSA Public Keys	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)	256 bits, 284 bits, 521 bits - 128 bits, 192 bits, 256 bits	Public Key - PSP	SSH ECDSA KeyGen TLS ECDSA KeyGen		TLS ECDSA SigVer
Entropy Input String	Entropy input string coming from the entropy source Input length = 384 bits	384 bits - 256 bits	DRBG CSP - CSP	Entropy Source		Counter DRBG (A3453)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Firmware integrity verification key	Used to check the integrity of all software code (HMAC-SHA-256 and ECDSA P-256) (Note: This is not considered an SSP)	128 bits - 128 bits	Integrity verification key - Neither	External - Factory Pre-Loaded		
IKEv2 SKEYSEED	Used to derive encryption keys	160 bits, 256 bits, 384 bits, or 512 bits - 160 bits, 256 bits, 384 bits, or 512 bits	Key Agreement seed - CSP	KDF IKEv2 (A3453)		KAS-ECC (IPSec/IKE) KAS-FFC (IPSec/IKE)
Protocol Secrets	Secrets used by RADIUS or TACACS+ (8 characters minimum)	8 characters minimum - N/A	Authentication Data - CSP			
Public key for firmware content load test	Used to authenticate software/firmware and content to be installed on the firewall (RSA 2048 with SHA-256)	112 bits - 112 bits	Public Key - PSP	External - Factory Pre-Loaded		Firmware Load Test

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
RA VPN IPSec Authentication	(HMAC-SHA-1, 160 bits) Used in authentication of remote access IPSec data.	160 bits - 160 bits	Session Key - CSP	CKG		Session Authentication (IPSec/IKE)
RA VPN IPSec Session Keys	Used to encrypt remote access sessions utilizing IPSec. (AES 128-CBC, 128/256-GCM)	128 bits, 256 bits - 128 bits, 256 bits	Session Key - CSP	CKG		Session Encryption/Decryption (IPSec/IKE)
RSA Private Keys	RSA Private keys for generation of signatures, authentication or key establishment. (RSA 2048, 3072, or 4096-bit)	2048 bits, 3072 bits, 4096 bits - 112 bits,128 bits, 150 bits	Private Key - CSP	SSH RSA KeyGen TLS RSA KeyGen		TLS RSA SigGen
RSA Public Keys	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)	2048 bits, 3072 bits, 4096 bits - 112 bits,128 bits, 150 bits	Public Key - PSP	SSH RSA KeyGen TLS RSA KeyGen		TLS RSA SigVer

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
S-S VPN IPSec Pre-Shared Keys	PSK used in conjunction with HMAC listed above for authentication. Entered into the module by the Crypto Officer once authenticated	N/A - N/A	Shared Secret - CSP	KDF IKEv2 (A3453)		IPSec/IKE Keying Materials Development
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. (160, 256, 384, 512 bits)	160 bits, 256 bits, 384 bits, or 512 bits - 160 bits, 256 bits, 384 bits, or 512 bits	Session Key - CSP	KDF IKEv2 (A3453)	KAS-ECC (IPSec/IKE) KAS-FFC (IPSec/IKE)	Session Authentication (IPSec/IKE)
S-S VPN IPSec/IKE DHE or ECDHE Private Components	Diffie-Hellman or EC Diffie-Hellman private component used in key establishment (DHE 2048, DHE 3072, DHE 4096, ECDHE P-256, P-384, P-521)	2048 bits, 3072 bits, 4096 bits; 256 bits, 384 bits, 521 bits - 112 bits,128 bits, 150	Private Key - CSP	KAS-ECC-KeyGen (IPSec/IKE) KAS-FFC-KeyGen (IPSec/IKE)		IPSec/IKE Keying Materials Development

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		bits; 128 bits,192 bits, 256 bits				
S-S VPN IPSec/IKE DHE or ECDHE Public Components	Diffie-Hellman or EC Diffie-Hellman public component used in key agreement (DHE 2048, DHE 3072, DHE 4096, ECDHE P-256, P-384, P-521)	2048 bits, 3072 bits, 4096 bits; 256 bits, 384 bits, 521 bits - 112 bits,128 bits, 150 bits; 128 bits,192 bits, 256 bits	Public Key - PSP	KAS-ECC-KeyGen (IPSec/IKE) KAS-FFC-KeyGen (IPSec/IKE)		IPSec/IKE Keying Materials Development
S-S VPN IPSec/IKE Session Keys	Used to encrypt IKE/IPSec data. These are AES (128, 192, or 256 CBC) IKE keys and (128, 192 or 256 CBC, 128 CCM, 128 or 256 GCM) IPSec keys	128 - 256 bits - 128 bits minimum	Session Key - CSP	KDF IKEv2 (A3453)	KAS-ECC (IPSec/IKE) KAS-FFC (IPSec/IKE)	Session Encryption/Decryption (IPSec/IKE)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
SNMPv3 Authentication Key	HMAC–SHA-1/224/256/384/512 Authentication protocol key (160 bits)	160 bits, 224 bits, 256 bits, 384 bits, or 512 bits - 160 bits, 224 bits, 256 bits, 384 bits, or 512 bits	Session Key - CSP	KDF SNMP (A3453)		Session Authentication (SMPv3)
SNMPv3 Authentication Secret	Used to support SNMPv3 services (Minimum 8 characters)	8 characters minimum - N/A	Authentication Key - CSP			SNMPv3 Keying Materials Development
SNMPv3 Privacy Secret	Used to support SNMPv3 services (Minimum 8 characters)	8 characters minimum - N/A	Authentication Key - CSP			SNMPv3 Keying Materials Development
SNMPv3 Session Key	Privacy protocol encryption key (AES 128/192/256 CFB)	128 - 256 bits - 128 bits minimum	Session Key - CSP	KDF SNMP (A3453)		Session Encryption/Decryption (SNMPv3)
SSH Client Public Key	Public RSA key used to authenticate client. (RSA	2048 bits, 3072 bits,	Public Key - PSP			SSH RSA SigVer

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	2048, 3072, and 4096 bits)	4096 bits; 256 bits, 384 bits, 521 bits - 112 bits,128 bits, 150 bits; 128 bits,192 bits, 256 bits				
SSH DHE/ECDHE Private Components	Diffie Hellman or EC Diffie-Hellman private (DH Group 14, ECDH P-256, ECDH P-384, ECDH P-521)	2048 bits; 256 bits, 384 bits, 521 bits - 112 bits;128 bits,192 bits, 256 bits	Private Key - CSP	KAS-ECC-KeyGen (SSH) KAS-FFC-KeyGen (SSH)		SSHv2 Keying Materials Development
SSH DHE/ECDHE Public Components	Diffie Hellman or EC Diffie-Hellman public component (DH Group 14, ECDH P-256, ECDH	2048 bits; 256 bits, 384 bits, 521 bits - 112 bits;12	Public Key - PSP	KAS-ECC-KeyGen (SSH) KAS-FFC-KeyGen (SSH)	KAS-ECC (SSH) KAS-FFC (SSH)	SSHv2 Keying Materials Development

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	P-384, ECDH P-521)	8 bits,192 bits, 256 bits				
SSH Host Public Key	SSH Host Public Key (RSA 2048, RSA 3072, RSA 4096, ECDSA P-256, P-384, or P-521)	2048 bits, 3072 bits, 4096 bits; 256 bits, 384 bits, 521 bits - 112 bits,128 bits, 150 bits; 128 bits,192 bits, 256 bits	Public Key - PSP	SSH ECDSA KeyGen SSH RSA KeyGen		SSH ECDSA SigVer SSH RSA SigVer
SSH Session Authentication Keys	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)	160 bits, 256 bits, or 512 bits - 160 bits, 256 bits, or 512 bits	Session Key - CSP	KDF SSH (A3453)		Session Authentication (SSHv2)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
SSH Session Encryption Keys	Used in all SSH connections to the security module's command line interface. (128, 192, or 256 bits: AES CBC or CTR) (128 or 256 bits: AES GCM)	128 bits, 256 bits - 128 bits, 256 bits	Session Key - CSP	KDF SSH (A3453)		Session Encryption/Decryption (SSH)
TLS DHE/ECDHE Private Components	Ephemeral Diffie-Hellman private FFC or EC component used in TLS (DHE 2048, ECDHE P-256, P-384, P-521)	2048 bits, 3072 bits, 4096 bits; 256 bits, 384 bits, 521 bits - 112 bits,128 bits, 150 bits; 128 bits,192 bits, 256 bits	Private Key - CSP	KAS-ECC-KeyGen (SSH) KAS-ECC-KeyGen (TLSv1.2) KAS-FFC-KeyGen (SSH) KAS-FFC-KeyGen (TLSv1.2)		TLSv1.2 Keying Materials Development
TLS DHE/ECDHE Public Components	Diffie_Hellman or EC Diffie-Hellman Ephemeral values used in key agreement	2048 bits, 3072 bits, 4096 bits; 256 bits,	Public Key - PSP	KAS-ECC-KeyGen (SSH) KAS-ECC-KeyGen (TLSv1.	KAS-ECC (TLSv1.2) KAS-FFC (TLSv1.2)	TLSv1.2 Keying Materials Development

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	(DHE 2048, ECDHE P-256, P-384, P-521)	384 bits, 521 bits - 112 bits,128 bits, 150 bits; 128 bits,192 bits, 256 bits		2) KAS-FFC-KeyGen (IPSec/IKE) KAS-FFC-KeyGen (SSH)		
TLS Encryption Keys	AES (128 or 256 bit) keys used in TLS connections (GCM; CBC)	128 bits, 256 bits - 128 bits, 256 bits	Session Key - CSP		KAS-ECC (TLSv1.2) KAS-FFC (TLSv1.2)	Session Encryption/Decryption (TLSv1.2)
TLS HMAC Keys	HMAC keys used in TLS connections (HMAC-SHA2-256/384) (256, 384 bits)	256 bits, 384 bits - 256 bits, 384 bits	Session Key - CSP		KAS-ECC (TLSv1.2) KAS-FFC (TLSv1.2)	Session Authentication (TLSv1.2)
TLS Master Secret	Secret value used to derive the TLS session keys	384 bits - 384 bits	Master Secret - CSP		KAS-ECC (TLSv1.2) KAS-FFC (TLSv1.2)	TLSv1.2 Keying Materials Development
TLS Pre-Master Secret	Secret value used to derive the TLS Master Secret along with	2048 bits; 256 bits, 384	Shared Secret - CSP		KAS-ECC (TLSv1.2) KAS-	TLSv1.2 Keying Materials Development

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	client and server random nonces	bits, 521 bits - 112 bits; 256 bits, 384 bits, 521 bits			FFC (TLSv1.2)	

Table 17: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
CA Certificates	Peer Public Key Input Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM	HDD:Plaintext		Zeroization Command Power Cycle / Session Termination	RSA Public Keys:Encrypts RSA Private Keys:Encrypts ECDSA Public Keys:Encrypts ECDSA Private Keys:Encrypts
CO, User, RA VPN Password	Password/Secret Input via TLSv1.2	HDD:Obfuscated		Zeroization Command	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM				
DHE/ECDHE Shared Secret Z		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	SSH DHE/ECDHE Private Components:Paired With SSH DHE/ECDHE Public Components:Paired With S-S VPN IPSec/IKE DHE or ECDHE Public Components:Paired With S-S VPN IPSec/IKE DHE or ECDHE Private Components:Paired With
DRBG Key		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	Entropy Input String:Paired With DRBG Seed :Paired With DRBG V:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DRBG Seed		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	Entropy Input String:Paired With DRBG Key:Paired With DRBG V:Paired With
DRBG V		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	Entropy Input String:Paired With DRBG Seed :Paired With DRBG Key:Paired With
ECDSA Private Keys	Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM	HDD:Plaintext		Zeroization Command Power Cycle / Session Termination	ECDSA Public Keys:Paired With
ECDSA Public Keys	Peer Public Key Input Module Public Key Output Password/Secret Input via TLSv1.2 encrypted by AES and	HDD:Plaintext		Zeroization Command	ECDSA Private Keys:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM				
Entropy Input String		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	DRBG Seed :Paired With DRBG Key:Paired With DRBG V:Paired With
Firmware integrity verification key		HDD:Plaintext		N/A	
IKEv2 SKEYSEED		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	S-S VPN IPSec/IKE DHE or ECDHE Private Components:Paired With S-S VPN IPSec/IKE DHE or ECDHE Public Components:Paired With
Protocol Secrets	Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Sec	HDD:Plaintext		Zeroization Command	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	ret Input via TLSv1.2 encrypted by AES-GCM Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM				
Public key for firmware content load test		HDD:Obfuscated		N/A	
RA VPN IPSec Authentication		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	
RA VPN IPSec Session Keys		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	
RSA Private Keys	Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM Password/Secret Input via SSHv2	HDD:Plaintext		Zeroization Command	RSA Public Keys:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM				
RSA Public Keys	Peer Public Key Input Module Public Key Output Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM	HDD:Plaintext		Zeroization Command	RSA Private Keys:Paired With
S-S VPN IPSec Pre-Shared Keys	Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via	RAM:Plaintext HDD:Plaintext	Duration of use	Zeroization Command	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	TLSv1.2 encrypted by AES-GCM Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM				
S-S VPN IPSec/IKE Authentication Keys		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	S-S VPN IPSec/IKE DHE or ECDHE Private Components:Derived From S-S VPN IPSec/IKE DHE or ECDHE Public Components:Derived From
S-S VPN IPSec/IKE DHE or ECDHE Private Components		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	S-S VPN IPSec/IKE DHE or ECDHE Public Components:Paired With
S-S VPN IPSec/IKE DHE or ECDHE Public Components		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	S-S VPN IPSec/IKE DHE or ECDHE Private Components:Paired With
S-S VPN IPSec/IKE Session Keys		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	S-S VPN IPSec/IKE DHE or ECDHE Private Components:Derived From S-S VPN IPSec/IKE DHE or ECDHE

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					Public Components:Derived From
SNMPv3 Authentication Key		RAM:Plaintext HDD:Plaintext	Duration of use (Plaintext)	Zeroization Command	SNMPv3 Authentication Secret:Derived From SNMPv3 Privacy Secret:Derived From
SNMPv3 Authentication Secret	Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM	RAM:Plaintext HDD:Plaintext	Duration of use (Plaintext)	Zeroization Command	
SNMPv3 Privacy Secret	Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM Password/Secret Input via	RAM:Plaintext HDD:Plaintext	Duration of use (Plaintext)	Zeroization Command	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM				
SNMPv3 Session Key		RAM:Plaintext HDD:Plaintext	Duration of use (Plaintext)	Zeroization Command	SNMPv3 Authentication Secret:Derived From SNMPv3 Privacy Secret:Derived From
SSH Client Public Key	Peer Public Key Input Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM	RAM:Plaintext HDD:Plaintext	Duration of use (Plaintext)	Zeroization Command	
SSH DHE/ECDHE Private Components		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	SSH DHE/ECDHE Public Components:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
SSH DHE/ECDHE Public Components	Peer Public Key Input Module Public Key Output	RAM:Plaintext	Duration of use	Power Cycle / Session Termination	SSH DHE/ECDHE Private Components:Paired With
SSH Host Public Key		RAM:Plaintext HDD:Plaintext	Duration of use (Plaintext)	Zeroization Command	RSA Private Keys:Paired With
SSH Session Authentication Keys		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	SSH DHE/ECDHE Public Components:Derived From SSH DHE/ECDHE Private Components:Derived From CA Certificates:Authenticates RSA Public Keys:Authenticates RSA Private Keys:Authenticates ECDSA Public Keys:Authenticates ECDSA Private Keys:Authenticates CO, User, RA VPN Password:Authenticates
SSH Session Encryption Keys		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	SSH DHE/ECDHE Public Components:Derived From SSH DHE/ECDHE Private Components:Derived From CA Certificates:Decrypts RSA Public Keys:Decrypts

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					RSA Private Keys:Decrypts ECDSA Public Keys:Decrypts ECDSA Private Keys:Decrypts CO, User, RA VPN Password:Decrypts
TLS DHE/ECDHE Private Components		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	TLS DHE/ECDHE Public Components:Paired With
TLS DHE/ECDHE Public Components	Peer Public Key Input Module Public Key Output	RAM:Plaintext	Duration of use	Power Cycle / Session Termination	TLS DHE/ECDHE Private Components:Paired With
TLS Encryption Keys		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	TLS Master Secret:Derived From CA Certificates:Decrypts RSA Public Keys:Decrypts RSA Private Keys:Decrypts ECDSA Public Keys:Decrypts ECDSA Private Keys:Decrypts CO, User, RA VPN Password:Decrypts
TLS HMAC Keys		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	TLS Master Secret:Authenticates CA Certificates:Authenticates RSA Public Keys:Authenticates RSA Private Keys:Authenticates ECDSA Public Keys:Authenticates

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					ECDSA Private Keys:Authenticates CO, User, RA VPN Password:Authenticates
TLS Master Secret		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	TLS Pre-Master Secret:Derived From
TLS Pre-Master Secret		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	TLS DHE/ECDHE Private Components:Derived From TLS DHE/ECDHE Public Components:Derived From

Table 18: SSP Table 2

9.5 Transitions

Key Sizes

- Key sizes with a security strength less than 128-bits will be non-Approved for all uses starting January 1, 2031.

SHA-1

- The module implements SHA-1 for use in non-digital signature applications. This implementation will be non-Approved for all uses starting January 1, 2031.

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
ECDSA SigVer (FIPS186-4) (A3453)	256 bits	KAT	SW/FW Integrity	Self-Test successful	Signature Verification
HMAC-SHA2-256 (A3453)	SHA2-256	KAT	SW/FW Integrity	Self-Test successful	Keyed Checksum

Table 19: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES GCM Decrypt	256 Bits	KAT	CAST	Self-test output message	Decrypt	After each power-on or via self-test command
AES GCM Encrypt	256 Bits	KAT	CAST	Self-test output message	Encrypt	After each power-on or via self-test command
AES-CCM Decrypt	192 Bits	KAT	CAST	Self-test output message	Decrypt	After each power-on or via self-test command
AES-CCM Encrypt	192 Bits	KAT	CAST	Self-test output message	Encrypt	After each power-on or via self-test command
AES-ECB Decrypt (A3453)	128 bits	KAT	CAST	Self-test output message	Decrypt	After each power-on or via self-test command
Counter DRBG (A3453)	128 bits, 192 bits, 256 bits	KAT	CAST	Self-test output message	SP 800-90Arev1 Instantiate/Generate/Reseed Known Answer Tests	After each power-on or via self-test command
ECDSA KeyGen (FIPS186-4) (A3453)	256 Bit Minimum	PCT	PCT	System log messages	ECDSA / KAS-ECC pairwise consistency test	On session
ECDSA SigGen (FIPS186-4) (A3453)	256 Bits	KAT	CAST	Self-test output message	Sign	After each power-on or via self-test command

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ECDSA SigVer (FIPS186-4) (A3453)	256 Bits	KAT	CAST	Self-test output message	Verify	After each power-on or via self-test command
Firmware Load Test	RSA 2048 with SHA-256	FW Load Test	SW/FW Load	System log messages	Firmware load test on content load	On session
HMAC-SHA-1 (A3453)	160 Bits	KAT	CAST	Self-test output message	Keyed Hash	After each power-on or via self-test command
HMAC-SHA2-256 (A3453)	256 Bits	KAT	CAST	Self-test output message	Keyed Hash	After each power-on or via self-test command
HMAC-SHA2-384 (A3453)	384 Bits	KAT	CAST	Self-test output message	Keyed Hash	After each power-on or via self-test command
HMAC-SHA2-512 (A3453)	512 Bits	KAT	CAST	Self-test output message	Keyed Hash	After each power-on or via self-test command
KAS-ECC-SSC Sp800-56Ar3 (A3453)	256 Bits	KAT	CAST	Self-test output message	KAS Computation	After each power-on or via self-test command
KAS-FFC-SSC Sp800-56Ar3 (A3453)	2048 Bits	KAT	CAST	Self-test output message	KAS Computation	After each power-on or via self-test command
KDF IKEv2 (A3453)	SHA2-256	KAT	CAST	Self-test output message	IKEv2 with SHA-256	After each power-on or via

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						self-test command
KDF SSH (A3453)	SHA2-256	KAT	CAST	Self-test output message	SSHv2 with SHA-256	After each power-on or via self-test command
RSA KeyGen (FIPS186-4) (A3453)	2048 Bit Minimum	PCT	PCT	System log messages	RSA pairwise consistency test	On session
RSA SigGen (FIPS186-4) (A3453)	2048 Bits	KAT	CAST	Self-test output message	Sign	After each power-on or via self-test command
RSA SigVer (FIPS186-4) (A3453)	2048 Bits	KAT	CAST	Self-test output message	Verify	After each power-on or via self-test command
Safe Primes Key Generation (A3453)	2048 Bit Minimum	PCT	PCT	System log messages	KAS-FCC pairwise consistency test	On session
SHA-1 (A3453)	160 Bits	KAT	CAST	Self-test output message	Hash	After each power-on or via self-test command
SHA2-256 (A3453)	256 Bits	KAT	CAST	Self-test output message	Hash	After each power-on or via self-test command
SHA2-384 (A3453)	384 Bits	KAT	CAST	Self-test output message	Hash	After each power-on or via self-test command

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA2-512 (A3453)	512 Bits	KAT	CAST	Self-test output message	Hash	After each power-on or via self-test command
SP 800-90B RCT/APT Health Tests on Entropy Source	SP 800-90B, section 4 health tests	Fault-Detection	CAST	Self-test output message	Health tests done on entropy source	After each power-on or via self-test command
SP 800-56A Rev 3 Assurance Tests	Full public key validation	Critical Functions	Critical Function	System log messages	Assurance tests for SP 800-56A Rev3	On session
TLS v1.2 KDF RFC7627 (A3453)	SHA2-256	KAT	CAST	Self-test output message	TLSv1.2 with SHA-256	After each power-on or via self-test command

Table 20: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ECDSA SigVer (FIPS186-4) (A3453)	KAT	SW/FW Integrity	On Demand	Manually or Scheduled
HMAC-SHA2-256 (A3453)	KAT	SW/FW Integrity	On Demand	Manually or Scheduled

Table 21: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES GCM Decrypt	KAT	CAST	On Demand	Manually or Scheduled
AES GCM Encrypt	KAT	CAST	On Demand	Manually or Scheduled

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CCM Decrypt	KAT	CAST	On Demand	Manually or Scheduled
AES-CCM Encrypt	KAT	CAST	On Demand	Manually or Scheduled
AES-ECB Decrypt (A3453)	KAT	CAST	On session	Manually or Scheduled
Counter DRBG (A3453)	KAT	CAST	On Demand	Manually or Scheduled
ECDSA KeyGen (FIPS186-4) (A3453)	PCT	PCT	On session	On session
ECDSA SigGen (FIPS186-4) (A3453)	KAT	CAST	On Demand	Manually or Scheduled
ECDSA SigVer (FIPS186-4) (A3453)	KAT	CAST	On Demand	Manually or Scheduled
Firmware Load Test	FW Load Test	SW/FW Load	On session	On session
HMAC-SHA-1 (A3453)	KAT	CAST	On Demand	Manually or Scheduled
HMAC-SHA2-256 (A3453)	KAT	CAST	On Demand	Manually or Scheduled
HMAC-SHA2-384 (A3453)	KAT	CAST	On Demand	Manually or Scheduled
HMAC-SHA2-512 (A3453)	KAT	CAST	On Demand	Manually or Scheduled
KAS-ECC-SSC Sp800-56Ar3 (A3453)	KAT	CAST	On Demand	Manually or Scheduled
KAS-FFC-SSC Sp800-56Ar3 (A3453)	KAT	CAST	On Demand	Manually or Scheduled
KDF IKEv2 (A3453)	KAT	CAST	On Demand	Manually or Scheduled
KDF SSH (A3453)	KAT	CAST	On Demand	Manually or Scheduled
RSA KeyGen (FIPS186-4) (A3453)	PCT	PCT	On session	On session
RSA SigGen (FIPS186-4) (A3453)	KAT	CAST	On Demand	Manually or Scheduled

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA SigVer (FIPS186-4) (A3453)	KAT	CAST	On Demand	Manually or Scheduled
Safe Primes Key Generation (A3453)	PCT	PCT	On session	On session
SHA-1 (A3453)	KAT	CAST	On Demand	Manually or Scheduled
SHA2-256 (A3453)	KAT	CAST	On Demand	Manually or Scheduled
SHA2-384 (A3453)	KAT	CAST	On Demand	Manually or Scheduled
SHA2-512 (A3453)	KAT	CAST	On Demand	Manually or Scheduled
SP 800-90B RCT/APT Health Tests on Entropy Source	Fault-Detection	CAST	On Demand	Manually or Scheduled
SP 800-56A Rev 3 Assurance Tests	Critical Functions	Critical Function	On session	On session
TLS v1.2 KDF RFC7627 (A3453)	KAT	CAST	On Demand	Manually or Scheduled

Table 22: Conditional Periodic Information

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Conditional Firmware Load Test Failure	Signature verification fails on firmware load	Signature verification failure	N/A	System prints Invalid image message.
Conditional Pairwise Consistency or Critical Functions Test Failure	Module fails a PCT or critical functions test	PCT / Critical functions test	Reset session	System log prints an error message.
Self-Test / Integrity Test Failure	Module fails a self-test or integrity test	Self-test or Integrity Test failure	Reboot Module or Factory Reset	FIPS-CC mode failure. <Algorithm test> failed.

Table 23: Error States

10.5 Operator Initiation of Self-Tests

Perform a power cycle or via the ‘Self-Tests’ service.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

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

- Install physical kit opacity shields and tamper evidence seals according to the Physical Security Policy section. Physical kits must be correctly installed to operate in the Approved mode of operation. The tamper evident seals and opacity shields shall be installed for the module to operate in the 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 the Approved mode.
- Select “Enable FIPS-CC Mode”.
- When prompted, select “Reboot” and the module will re-initialize and continue into “FIPS-CC” mode (Approved mode).
- The module will reboot.
- In “FIPS-CC” mode, the console port is available 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.
- 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 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.

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

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

11.2 Administrator Guidance

The Administrator Guidance can be obtained from Palo Alto Network's public site:

https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/11-1/pan-os-admin/pan-os-admin.pdf

11.3 Non-Administrator Guidance

N/A

11.4 Design and Rules

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

1. The operator should not enable or use TLSv1.3
    a. Checked via CLI using "show profiles" command
2. If using RADIUS, it must be configured using TLS.
    a. Checked via CLI using "show shared" command
3. If using TACACS+, configure the service route via an IPSec tunnel, and ensure the TACACS+ server is configured for a minimum password length of eight (8) characters or greater.
    a. Checked via CLI using "show deviceconfig" command

11.5 End of Life

The following procedure will zeroize the module:

- Access the module's CLI via SSH, and command the module to enter "maintenance mode"; the module will reboot
    - Note: Establish a serial connection to the console port
- After reboot, select "Continue."
- Select "Factory Reset"
- The module will perform a zeroization, and provide the following message once complete:
    - "Factory Reset Status: Success"

Note: Following the completion of this procedure, the module will be placed back into an uninitialized state.

Please note that the “maintenance mode” does not correspond to a maintenance role or maintenance access interface per FIPS 140-3. No approved security functions are available in this mode, and no SSPs are accessed in this mode. Only the “Zeroize” service listed in section 4.3 of this document is available in this mode, which is permitted to be unauthenticated per Additional Comment #5 of IG 4.1.A, and the “Show Status” service to view error information, which is permitted to be unauthenticated per resolution ‘e’ of IG 4.1.A.

11.6 Additional Information

Module enforced 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 140-3 Level 2 module.

1. The cryptographic module provides 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 provides identity-based authentication.
3. The cryptographic module clears previous authentications on each power cycle.
4. When the module has not been placed in a valid role, the operator does not have access to any cryptographic services.
5. Data output is inhibited during power-up self-tests, zeroization and error states.
6. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
7. There are no restrictions on which keys or SSPs are zeroized by the zeroization service.
8. The module maintains separation between concurrent operators.
9. The module does not support a maintenance interface or role.
10. The module does not have any external input/output devices used for entry/output of data.
11. The module does not enter or output plaintext SSPs.
12. The module does not output intermediate key generation values.
13. Pre-shared keys used for IKE/IPSec must be at least 6 bytes in length, but no more than 255 bytes.

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

1. The operator should not enable/use TLSv1.3
2. If using RADIUS, it must be configured using TLS.
    a. Checked via CLI using “show shared” command
3. If using TACACS+, configure the service route via an IPSec tunnel, and ensure the TACACS+ server is configured for a minimum password length of eight (8) characters or greater.
    a. Checked via CLI using “show deviceconfig” command

12 Mitigation of Other Attacks

N/A