# PA-200, PA-500, PA-2000 Series, PA-3000 Series, PA-4000 Series, PA-5000 Series and PA-7050 Firewalls Security Policy

Version: P

Palo Alto Networks

Revision Date: 6/15/2016

www.paloaltonetworks.com © 2016 Palo Alto Networks. This non-proprietary security policy may be reproduced only in its original entirety (without revision). Palo Alto Networks, PAN-OS, and Panorama are trademarks of Palo Alto Networks, Inc. All other trademarks are the property of their respective owners.

P/N 880-000018-00N

# Change Record

**Table 1 - Change Record**

| Revision | Date | Author | Description of Change |
|---|---|---|---|
| A | 8/23/2010 | N. Campagna | Initial authoring |
| B | 1/24/2011 | N. Campagna | Added detail to the identity and authentication of IPSec endpoints. |
| C | 5/31/2011 | N. Campagna | Added FW Version 3.1.7-h1 |
| D | 6/15/2011 | N. Campagna | Added PA-5000 Series and updated firmware version |
| E | 3/9/2012 | Jake Bajic | Updates related to FW Version 4.0.10, TLS, SSHv2, IPSec/IKEv1 and RSA |
| F | 4/20/2012 | Jake Bajic | Updated algorithms certificate numbers |
| G | 6/7/2012 | Jake Bajic | Minor updates |
| H | 1/2/2013 | Jake Bajic | Addressing CMVP comments |
| I | 7/29/13 | Jake Bajic | Updated with new production part numbers |
| J | 9/17/13 | Jake Bajic | Updates related to PAN-OS 5.0.8, added PA-200 and PA-3000 Series |
| K | 1/15/14 | Jake Bajic | Updates PAN-OS 5.0.11 |
| L | 3/14/2014 | Richard Bishop | Added additional PA-200 and PA-3000 Series information and minor edits |
| M | 9/5/2014 | Richard Bishop | Updates related to PAN-OS 6.0, added PA-7050 |
| N | 3/3/2015 | Richard Bishop | Added PAN-OS version 6.0.8. |
| O | 4/26/2016 | Amir Shahhosseini | Added PAN-OS version 6.0.13 (DRBG update) |
| P | 6/15/2016 | Amir Shahhosseini | Updates for CMVP comments |

# Contents

1 Module Overview ..... 6
2 Security Level ..... 21
3 Modes of Operation ..... 22
*FIPS Approved Mode of Operation* ..... *22*
*Approved and Allowed Algorithms* ..... *23*
*Non-Approved, Non-Allowed Algorithms* ..... *24*
*4* Ports and Interfaces ..... 25
5 Identification and Authentication Policy ..... 29
*Assumption of Roles* ..... *29*
6 Access Control Policy ..... 31
*Roles and Services* ..... *31*
*Unauthenticated Services* ..... *32*
*Definition of Critical Security Parameters (CSPs)* ..... *32*
*Definition of Public Keys* ..... *34*
*Definition of CSPs Modes of Access* ..... *35*
7 Operational Environment ..... 36
8 Security Rules ..... 36
9 Physical Security Policy ..... 38
*Physical Security Mechanisms* ..... *38*
*Operator Required Actions* ..... *50*
10 Mitigation of Other Attacks Policy ..... 51
11 References ..... 51
12 Definitions and Acronyms ..... 51
13 Appendix A - PA-200 - FIPS Accessories/Tamper Seal Installation (5 Seals) ..... 53
14 Appendix B - PA-500 - FIPS Accessories/Tamper Seal Installation (12 Seals) ..... 56
15 Appendix C - PA-2000 Series - FIPS Accessories/Tamper Seal Installation (10 Seals) ..... 63
16 Appendix D - PA-3000 Series - FIPS Accessories/Tamper Seal Installation (7 Seals) ..... 66
17 Appendix E - PA-4000 Series – FIPS Accessories/Tamper Seal Installation (10 Seals) ..... 69
18 Appendix F - PA-5000 Series - FIPS Accessories/Tamper Seal Installation (17 Seals) ..... 73
19 Appendix G - PA-7050 Series - FIPS Accessories/Tamper Seal Installation (24 Seals) ..... 76

## Tables

Table 1 - Change Record ..... 2
Table 2 - Validated Version Information ..... 19
Table 3 - Module Security Level Specification ..... 21
Table 4 - FIPS Approved Algorithms Used in the Module ..... 23
Table 5 - FIPS Allowed Algorithms Used in the Module ..... 23
Table 6 - Supported Protocols in FIPS Approved Mode ..... 24
Table 7 - Non-Approved, Non-Allowed Algorithms Used in the Module ..... 24
Table 8 - PA-200 FIPS 140-2 Ports and Interfaces ..... 25
Table 9 - PA-500 FIPS 140-2 Ports and Interfaces ..... 25
Table 10 - PA-2000 Series FIPS 140-2 Ports and Interfaces ..... 26
Table 11 - PA-3000 Series FIPS 140-2 Ports and Interfaces ..... 26
Table 12 - PA-4000 Series FIPS 140-2 Ports and Interfaces ..... 27
Table 13 - PA-5000 Series FIPS 140-2 Ports and Interfaces ..... 27
Table 14 - PA-7050 FIPS 140-2 Ports and Interfaces ..... 28
Table 15 - Roles and Required Identification and Authentication ..... 29
Table 16 - Strengths of Authentication Mechanisms ..... 30
Table 17 - Authenticated Service Descriptions ..... 31
Table 18 - Authenticated Services ..... 31
Table 19 - Unauthenticated Services ..... 32
Table 20 - Private Keys and CSPs ..... 32
Table 21 - Public Keys ..... 34
Table 22 - CSP Access Rights within Roles & Services ..... 35
Table 23 - Inspection/Testing of Physical Security Mechanisms ..... 50

## Figures

Figure 1 - PA-200 Front Image ..... 8
Figure 2 - PA-200 Back Image ..... 8
Figure 3 - PA-200 with Front Opacity Shield and Cage Enclosure ..... 8
Figure 4 - PA-500 Front Image ..... 9
Figure 5 - PA-500 Back Image ..... 9
Figure 6 - PA-500 with Front Opacity Shield ..... 9
Figure 7 - PA-500 with Side Opacity Shield ..... 9
Figure 8 - PA-2020 / PA-2050 Front Images ..... 10
Figure 9 - PA-2020 / PA-2050 Back Image ..... 10
Figure 10 - PA-2020 / PA-2050 Front Opacity Shield ..... 11
Figure 11 - PA-2020 / PA-2050 with Side Opacity Shield ..... 11
Figure 12 - PA-3020 / PA-3050 Front Images ..... 11
Figure 13 - PA-3020 / PA-3050 Back Image ..... 12
Figure 14 - PA-3020 / PA-3050 Opacity Shield ..... 12
Figure 15 - PA-3020 / PA-3050 side with Opacity Shield ..... 12
Figure 16 - PA-4020 / PA-4050 Front Image ..... 13
Figure 17 - PA-4060 Front Image ..... 13
Figure 18 - PA-4020 / PA-4050 / PA-4060 Back Image ..... 13

Figure 19 - PA-4020 / PA-4050 / PA-4060 Left Side with Opacity Shield ..... 14
Figure 20 - PA-5020 Front Image ..... 14
Figure 21 - PA-5050/PA-5060 Front Image ..... 14
Figure 22 - PA-5000 Series Back Image ..... 15
Figure 23 - PA-5000 Series Left Side with front Opacity Shield ..... 15
Figure 24 - PA-7050 Ports and Interface View ..... 16
Figure 25 - PA-7050 Front view with Opacity Shields ..... 17
Figure 26 - PA-7050 Rear view with Opacity Shields ..... 17
Figure 27 - PA-7050 Front and Right Side with Opacity Shields ..... 18
Figure 28 - PA-7050 Rear and Left Side with Opacity Shields ..... 18
Figure 29 - Logical Diagram ..... 20
Figure 30 - PA-200 Left Side and Top Tamper Seal Placement (3) ..... 38
Figure 31 - PA-200 Right Side Tamper Seal Placement (2) ..... 38
Figure 32 - PA-500 Front Tamper Seal Placement (1) ..... 39
Figure 33 - PA-500 Left Side Tamper Seal Placement (3) ..... 39
Figure 34 - PA-500 Right Side Tamper Seal Placement (2) ..... 39
Figure 35 - PA-500 Rear Tamper Seal Placement (6) ..... 40
Figure 36 - PA-2000 Series Front Tamper Seal Placement (1) ..... 41
Figure 37 - PA-2000 Series Left Side Tamper Seal Placement (3) ..... 41
Figure 38 - PA-2000 Series Right Side Tamper Seal Placement (3) ..... 42
Figure 39 - PA-2000 Series Rear Tamper Seal Placement (3) ..... 42
Figure 40 - PA-3000 Series Tamper Seal Placement (3) ..... 43
Figure 41 - PA-3000 Series Tamper Seal Placement (2) ..... 43
Figure 42 - PA-3000 Series Tamper Seal Placement (2) ..... 43
Figure 43 - PA-4000 Series Rear Tamper Seal Placement – From Top (4) ..... 44
Figure 44 - PA-4000 Series Rear Side Tamper Seal Placement – From Underside (4) ..... 44
Figure 45 - PA-4000 Series Right Side Tamper Seal Placement (1) ..... 44
Figure 46 - PA-4000 Series Left Side Tamper Seal Placement (1) ..... 45
Figure 47 - PA-5000 Series Rear Tamper Seal Placement (9) ..... 46
Figure 48 - PA-5000 Series Right Side Tamper Seal Placement (4) ..... 46
Figure 49 - PA-5000 Series Left Side Tamper Seal Placement (4) ..... 47
Figure 50 - PA-7050 Tamper Seal Placement for Top Plenum (1-4) ..... 48
Figure 51 - PA-7050 Tamper Seal Placement for Bottom Plenum (5-6) ..... 48
Figure 52 - PA-7050 Tamper Seal Placement for Rear Panels (7-12), Power Switches (13-16) and Opacity Shields (17-20) ..... 49
Figure 53 - PA-7050 Tamper Seal Placement for Top Plenum Bracket (21-22) ..... 49
Figure 54 - PA-7050 Tamper Seal Placement for Bottom Plenum Bracket (23-24) ..... 50

# 1 Module Overview

Palo Alto Networks offers a full line of next-generation security appliances that range from the PA-200, designed for enterprise remote offices, to the PA-7050, which is a modular chassis designed for high-speed datacenters. Our platform architecture is based on our single-pass software engine, PAN-OS, for networking, security, threat prevention, and management functionality that is consistent across all platforms. The devices differ only in capacities, performance, and physical configuration.

The Palo Alto Networks PA-200, PA-500, PA-2000 Series, PA-3000 Series, PA-4000 Series, PA-5000 Series, and PA-7050 firewalls (hereafter referred to as the modules) are multi-chip standalone modules that provide network security by enabling enterprises to see and control applications, users, and content – not just ports, IP addresses, and packets – using three unique identification technologies: App-ID, User-ID, and Content-ID. These identification technologies, found in Palo Alto Networks' enterprise firewalls, enable enterprises to create business-relevant security policies – safely enabling organizations to adopt new applications, instead of the traditional "all-or-nothing" approach offered by traditional port-blocking firewalls used in many security infrastructures.

### Features and Benefits

- **Application visibility and control:** Accurate identification of the applications traversing the network enables policy-based control over application usage at the firewall, the strategic center of the security infrastructure.
- **Visualization tools:** Graphical visibility tools, customizable reporting and logging enables administrators to make a more informed decision on how to treat the applications traversing the network.
- **Application browser:** Helps administrators quickly research what the application is, its' behavioral characteristics and underlying technology resulting in a more informed decision making process on how to treat the application.
- **User-based visibility and control:** Seamless integration with enterprise directory services (Active Directory, LDAP, eDirectory) facilitates application visibility and policy creation based on user and group information, not just IP address. In Citrix and terminal services environments, the identity of users sitting behind Citrix or terminal services can be used to enable policy-based visibility and control over applications, users and content. An XML API enables integration with other, 3rd party user repositories.
- **Real-time threat prevention:** Detects and blocks application vulnerabilities, viruses, spyware, and worms; controls web activity; all in real-time, dramatically improving performance and accuracy.
- **File and data filtering:** Taking full advantage of the in-depth application inspection being performed by App-ID, administrators can implement several different types of policies that reduce the risk associated with unauthorized file and data transfer.
- **Legacy firewall support:** Support for traditional inbound and outbound port-based firewall rules mixed with application-based rules smooth the transition to a Palo Alto Networks next generation firewall.
- **Networking architecture**: Support for dynamic routing (OSPF, RIP, BGP), virtual wire mode and layer 2/layer 3 modes facilitates deployment in nearly any networking environment.

- **Policy-based Forwarding**: Forward traffic based on policy defined by application, source zone/interface, source/destination address, source user/group, and service.
- **Virtual Systems**: Create multiple virtual "firewalls" within a single device as a means of supporting specific departments or customers. Each virtual system can include dedicated administrative accounts, interfaces, networking configuration, security zones, and policies for the associated network traffic.
- **VPN connectivity**: Secure site-to-site connectivity is enabled through standards-based IPSec VPN support while remote user access is delivered via SSL VPN connectivity.
- **Quality of Service (QoS):** Deploy traffic shaping policies (guaranteed, maximum and priority) to enable positive policy controls over bandwidth intensive, non-work related applications such as streaming media while preserving the performance of business applications.
- **Real-time bandwidth monitor:** View real-time bandwidth and session consumption for applications and users within a selected QoS class.
- **Purpose-built platform:** combines single pass software with parallel processing hardware to deliver the multi-Gbps performance necessary to protect today's high speed networks.

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

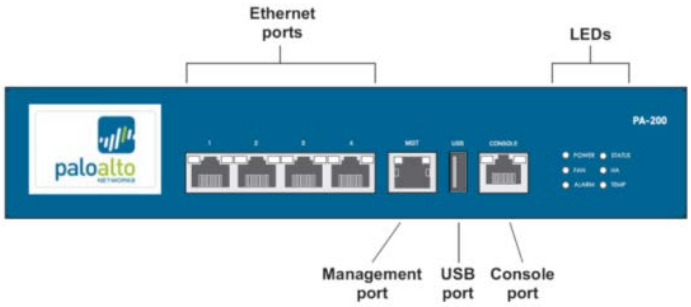



**Figure 1 - PA-200 Front Image**

**Figure 2 - PA-200 Back Image**

**Figure 3 - PA-200 with Front Opacity Shield and Cage Enclosure**

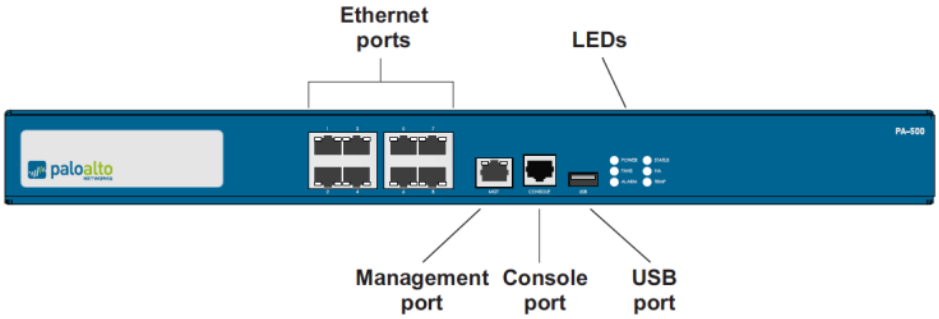



**Figure 4 - PA-500 Front Image**

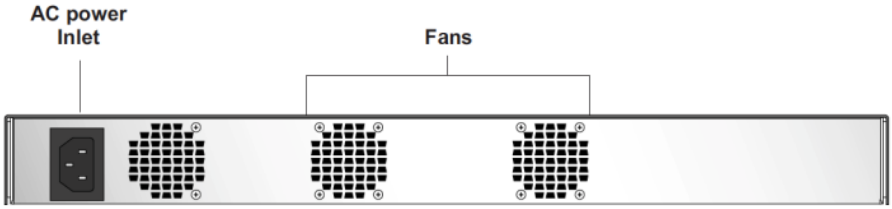



**Figure 5 - PA-500 Back Image**

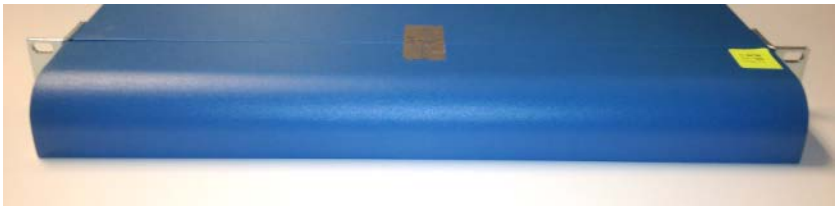


**Figure 6 - PA-500 with Front Opacity Shield**

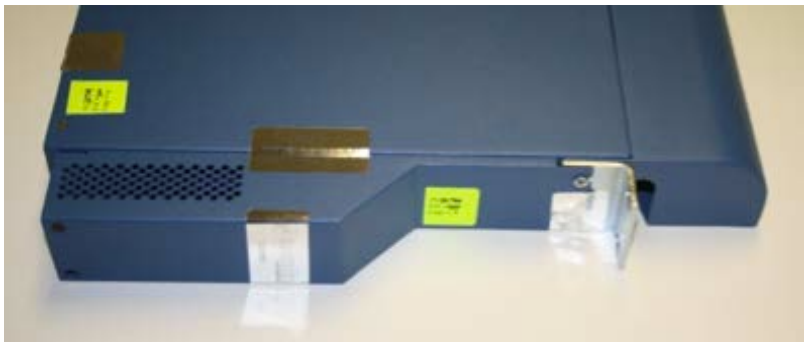


**Figure 7 - PA-500 with Side Opacity Shield**

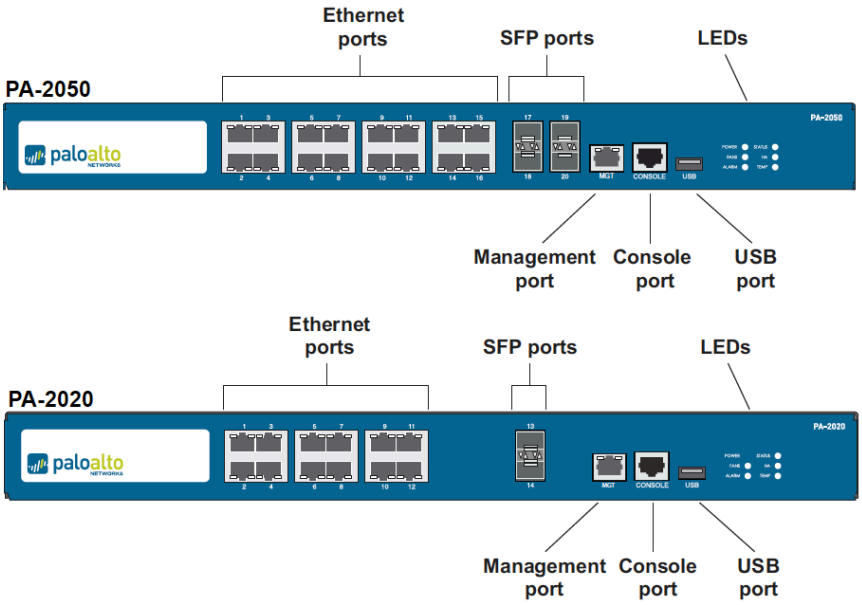



**Figure 8 - PA-2020 / PA-2050 Front Images**

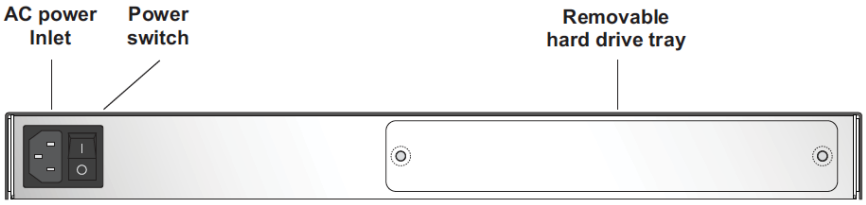



**Figure 9 - PA-2020 / PA-2050 Back Image**

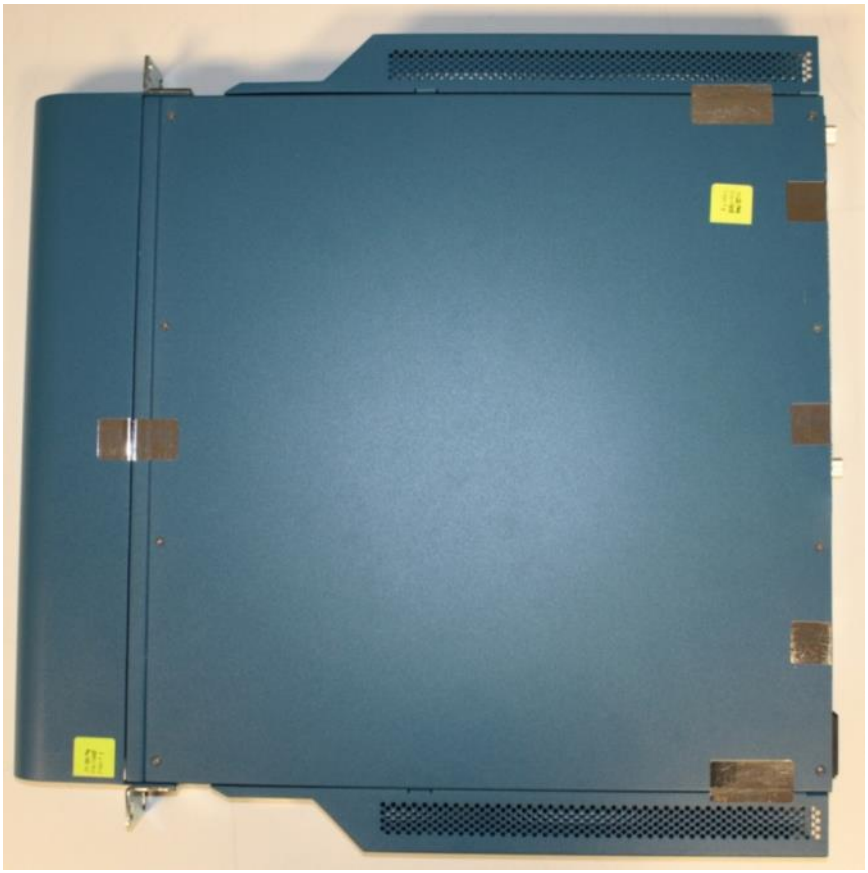


**Figure 10 - PA-2020 / PA-2050 Front Opacity Shield**

**Figure 11 - PA-2020 / PA-2050 with Side Opacity Shield**

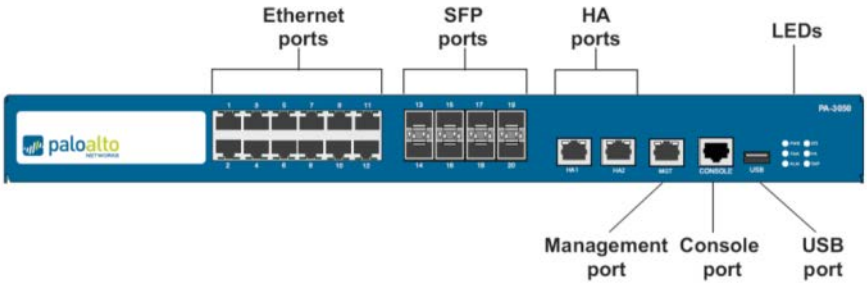



**Figure 12 - PA-3020 / PA-3050 Front Images**

**Figure 13 - PA-3020 / PA-3050 Back Image**

**Figure 14 - PA-3020 / PA-3050 Opacity Shield**

**Figure 15 - PA-3020 / PA-3050 side with Opacity Shield**

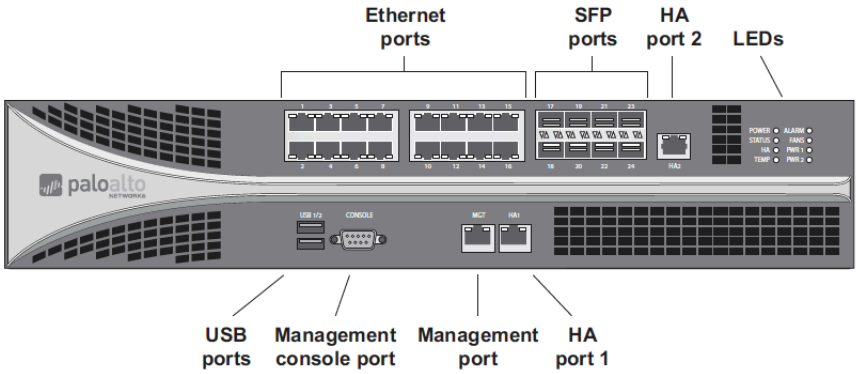



**Figure 16 - PA-4020 / PA-4050 Front Image**

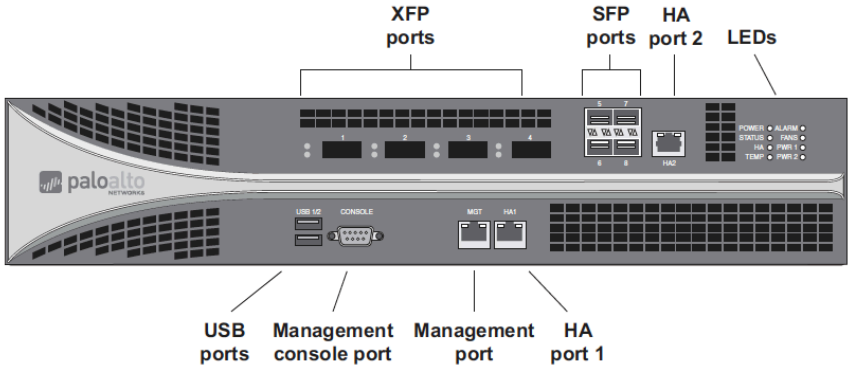



**Figure 17 - PA-4060 Front Image**

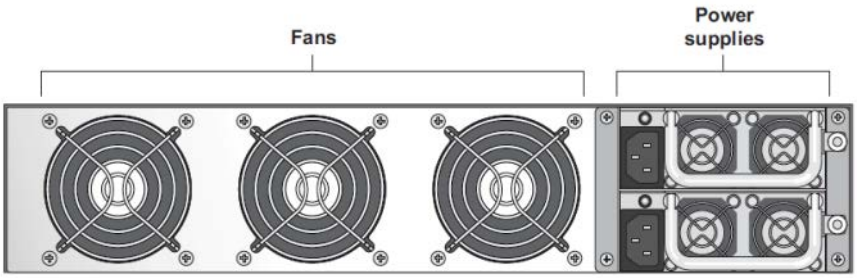



**Figure 18 - PA-4020 / PA-4050 / PA-4060 Back Image**

**Figure 19 - PA-4020 / PA-4050 / PA-4060 Left Side with Opacity Shield**

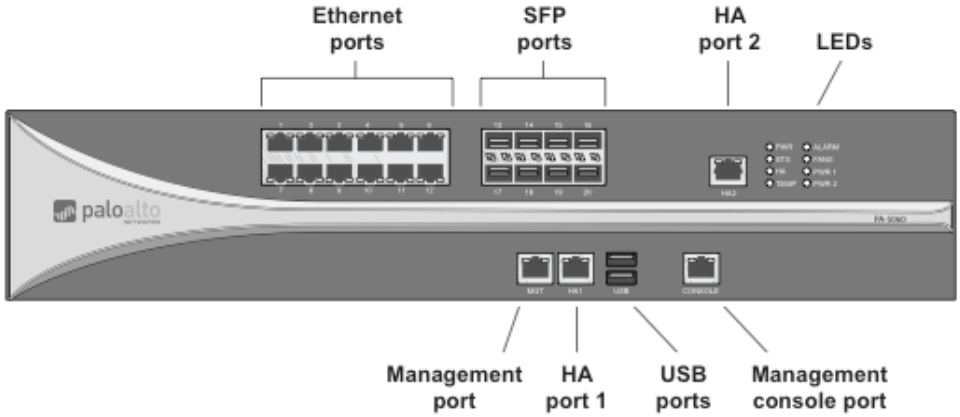



**Figure 20 - PA-5020 Front Image**

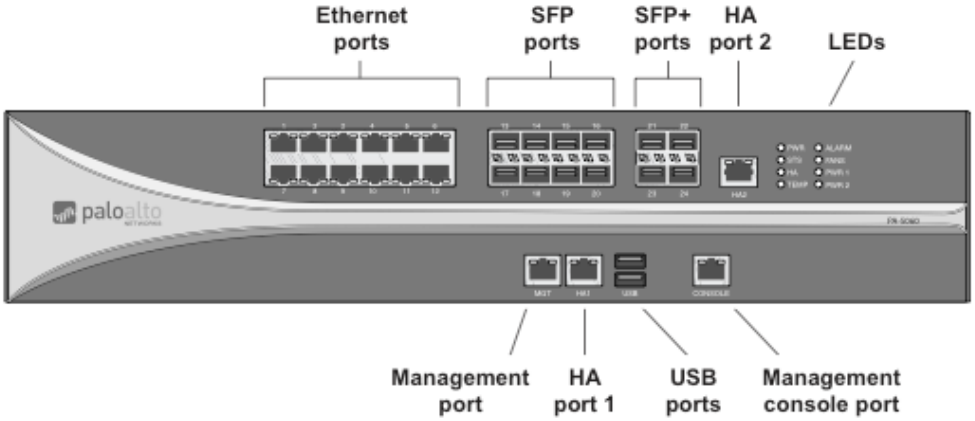



**Figure 21 - PA-5050/PA-5060 Front Image**

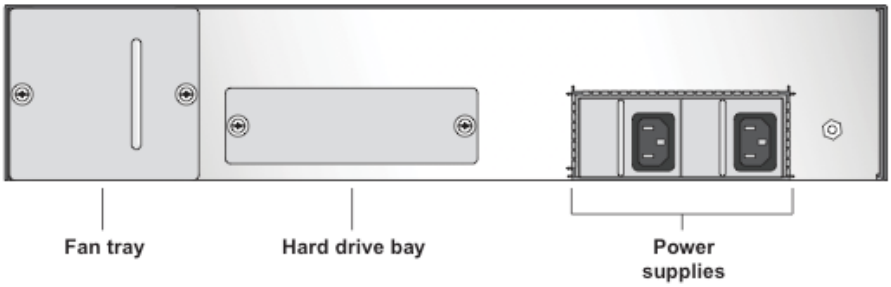



**Figure 22 - PA-5000 Series Back Image**

**Figure 23 - PA-5000 Series Left Side with front Opacity Shield**

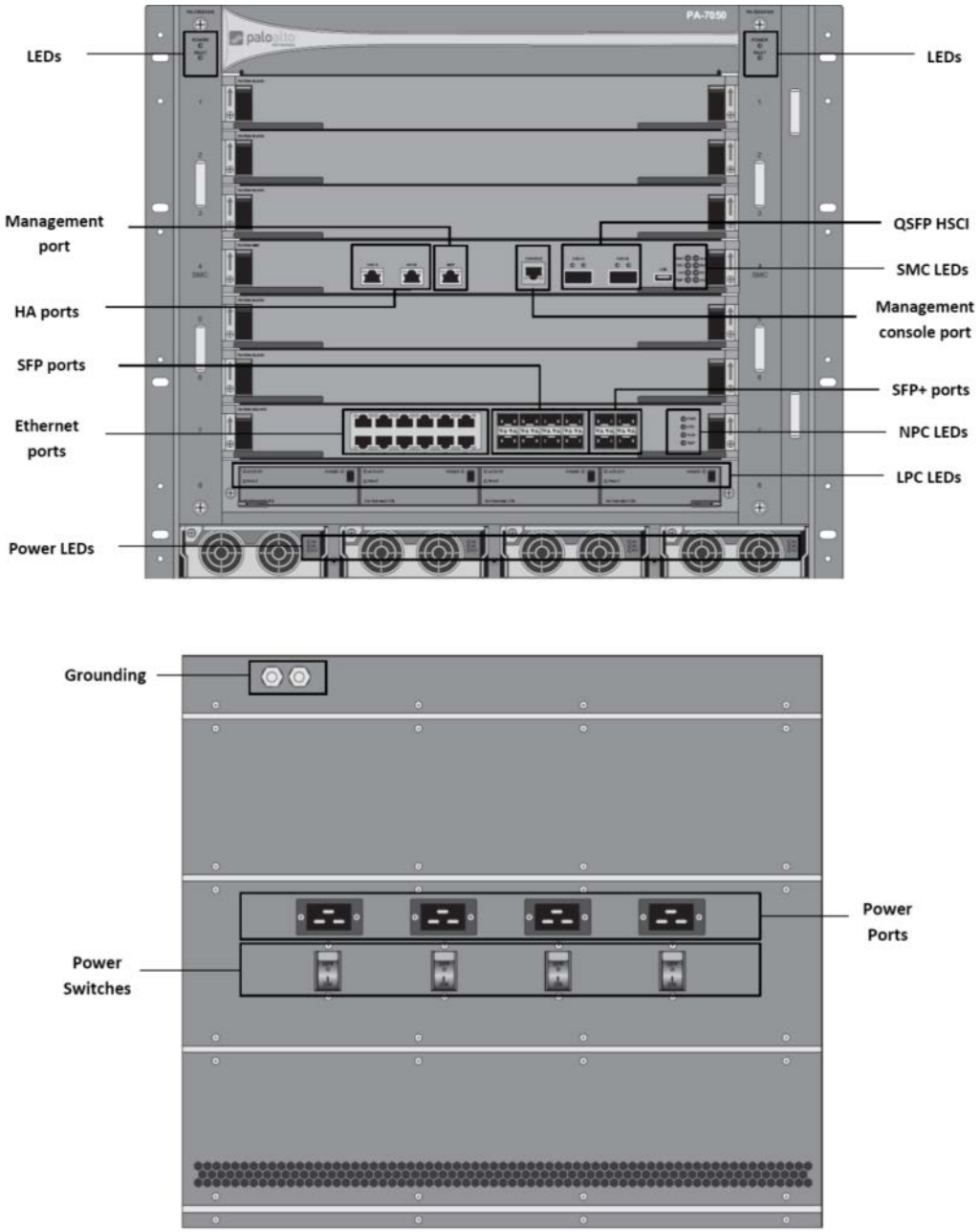



**Figure 24 - PA-7050 Ports and Interface View**

**Figure 25 - PA-7050 Front view with Opacity Shields**

**Figure 26 - PA-7050 Rear view with Opacity Shields**

**Figure 27 - PA-7050 Front and Right Side with Opacity Shields**

**Figure 28 - PA-7050 Rear and Left Side with Opacity Shields**

The configurations for this validation are:

**Table 2 - Validated Version Information**

| Module | Part Number | Hardware Version | FIPS Kit Part Number | FIPS Kit Hardware Version | Firmware Versions[1] |
|---|---|---|---|---|---|
| PA-200 | 910-000015-00E | Rev. E | 920-000084-00A | Rev. A | 6.0.13 |
| PA-500 | 910-000006-00O | Rev. O | 920-000005-00A | Rev. A | 6.0.13 |
| PA-500-2GB | 910-000094-00O | Rev. O | 920-000005-00A | Rev. A | 6.0.13 |
| PA-2020 | 910-000004-00Z | Rev. Z | 920-000004-00A | Rev. A | 6.0.13 |
| PA-2050 | 910-000003-00Z | Rev. Z | 920-000004-00A | Rev. A | 6.0.13 |
| PA-3020 | 910-000017-00J | Rev. J | 920-000081-00A | Rev. A | 6.0.13 |
| PA-3050 | 910-000016-00J | Rev. J | 920-000081-00A | Rev. A | 6.0.13 |
| PA-4020 | 910-000002-00AB | Rev. AB | 920-000003-00A | Rev. A | 6.0.13 |
| PA-4050 | 910-000001-00AB | Rev. AB | 920-000003-00A | Rev. A | 6.0.13 |
| PA-4060 | 910-000005-00S | Rev. S | 920-000003-00A | Rev. A | 6.0.13 |
| PA-5020 | 910-000010-00F | Rev. F | 920-000037-00A | Rev. A | 6.0.13 |
| PA-5050 | 910-000009-00F | Rev. F | 920-000037-00A | Rev. A | 6.0.13 |
| PA-5060 | 910-000008-00F | Rev. F | 920-000037-00A | Rev. A | 6.0.13 |
| PA-7050 | 910-000102-00B with 910-000028-00B | Rev. B | 920-000112-00A | Rev. A | 6.0.13 |

[1] Note: Firmware version 6.0.13 is the latest version that includes the DRBG implementation. Versions 6.0.3 and 6.0.8 were previously validated, but included the RNG implementation. This note is for historical purposes only.

Figure 29 depicts the logical block diagram for the modules. The cryptographic boundary includes all of the logical components of the modules and the boundary is the physical enclosure of the firewall.

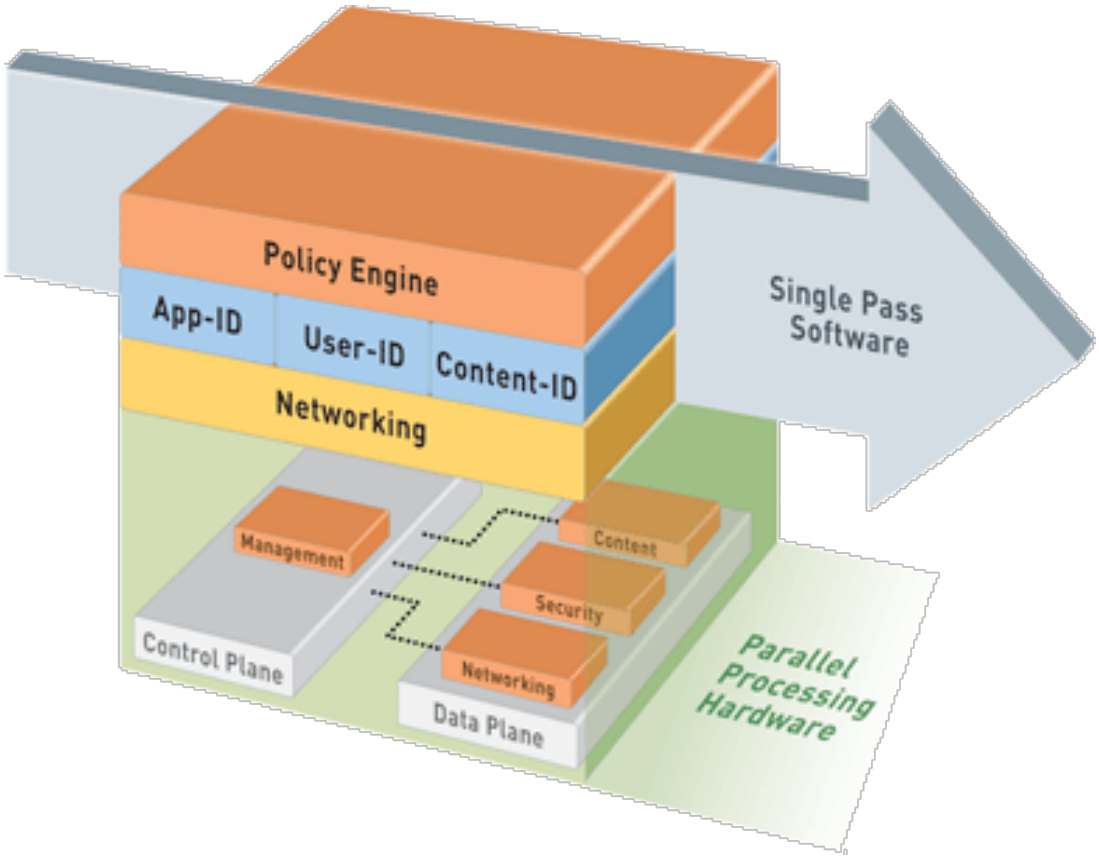



**Figure 29 - Logical Diagram**

# 2 Security Level

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

**Table 3 - Module Security Level Specification**

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

# 3 Modes of Operation

***FIPS Approved Mode of Operation***

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

- Install FIPS kit opacity shields and tamper evidence seals according to Section 9. FIPS kits must be correctly installed to operate in the Approved mode of operation.
- The tamper evidence seals and opacity shields shall be installed for the module to operate in a FIPS Approved mode of operation.
- During initial boot up, break the boot sequence via the console port connection (by pressing the maint button when instructed to do so) to access the main menu.
- Select “Continue.”
- Select the “Set CCEAL4 Mode” option to enter CC mode.
- Select “Enable CCEAL4 Mode”.
- When prompted, select “Reboot” and the module will re-initialize and continue into CC mode (FIPS mode).
- The module will reboot.
- In CC mode, the console port is available as a status output port.

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

- Status output interface will indicate “**** CCEAL4 MODE ENABLED ****” via the CLI session.
- Status output interface will indicate “CCEAL4 mode enabled successfully” via the console port.
- The module will display “CC” at all times in the status bar at the bottom of the web interface.

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

- The module will output “CC EAL4 failure”
- The module will reboot and enter a state in which the reason for the reboot can be determined.
- To determine which self-test caused the system to reboot into the error state, connect the console cable and follow the on-screen instructions to view the self-test output.

### *Approved and Allowed Algorithms*

*The cryptographic modules support the following FIPS Approved algorithms.*

**Table 4 - FIPS Approved Algorithms Used in the Module**

| FIPS Approved Algorithm | CAVP Cert. # |
|---|---|
| AES:<br>- ECB, CBC, CFB1, CFB8, CFB128, OFB modes; Encrypt/Decrypt; 128, 192 and 256-bit<br>- CTR mode; 128-bit | 3931<br>3932 |
| AES-CCM | 3931 |
| FIPS 186-4 RSA:<br>- Key Generation: 2048 and 3072-bit<br>- Signature Generation: 2048 and 3072-bit<br>- Signature Verification: 1024, 2048 and 3072-bit | 2008<br>2009 |
| HMAC-SHA-1, HMAC-SHA-256 | 2554<br>2555 |
| SHA-1, SHA-256, SHA-384, SHA-512 | 3241<br>3242 |
| SP800-90A DRBG AES 128 CTR | 1140<br>1141 |
| SP 800-135 KDF – TLS, SNMPv3, SSH, IKEv1 | 782 (CVL)<br>783 (CVL) |

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

**Table 5 - FIPS Allowed Algorithms Used in the Module**

| FIPS Allowed Algorithm |
|---|
| Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength) |
| RSA (key wrapping, key establishment methodology provides 112 bits of encryption strength) |
| NDRNG (seeding source) |
| MD5 (within TLS) |

**Table 6 - Supported Protocols in FIPS Approved Mode**

| Supported Protocols |
|---|
| TLSv1.0 and v1.2 |
| SSHv2 |
| IPSec/IKEv1 |
| SNMP |

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

### *Non-Approved, Non-Allowed Algorithms*

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

**Table 7 - Non-Approved, Non-Allowed Algorithms Used in the Module**

| Non-FIPS Allowed Algorithms in Non-FIPS Mode |
|---|
| MD5 – used for hashing of non-security relevant data; in CHAP authentication with RADIUS servers; in authentication for OSPF, RIP, and BGP dynamic routing protocols; for password hashing on Data Leakage Protection and Administrator passwords; and to integrity check URL filtering database downloads (note this is in addition to HMAC-SHA-1 authentication/integrity check). MD5 is also used to authenticate communications with the security module. MD5 is also used to hash administrator passwords. |
| RC4 – used to encrypt SSL communications with the security module. |
| Camellia - used to encrypt SSL communications with the security module. |
| RC2 - used to encrypt SSL communications with the security module. |
| SEED - used to encrypt SSL communications with the security module. |
| DES - used to encrypt SSL communications with the security module. |

# 4 Ports and Interfaces

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

**Table 8 - PA-200 FIPS 140-2 Ports and Interfaces**

| Interface | PA-200 Qty | FIPS 140-2 Designation | Name and Description |
|---|---|---|---|
| RJ45 | 1 | Data input, control input, data output, status output | Console port |
| RJ45 | 1 | Data input, control input, data output, status output | Out of band management |
| RJ45 | 4 | Data input, control input, data output, status output | 10/100/1000 Ethernet interface |
| DC-12V | 1 | Power input | Power interface |
| LEDs | 6 | Status output | Status indicators |
| USB | 1 | Disabled except for power | Used in manufacturing |

**Table 9 - PA-500 FIPS 140-2 Ports and Interfaces**

| Interface | PA-500 Qty | FIPS 140-2 Designation | Name and Description |
|---|---|---|---|
| RJ45 | 1 | Data input, control input, data output, status output | Console port |
| RJ45 | 1 | Data input, control input, data output, status output | Out of band management |
| RJ45 | 8 | Data input, control input, data output, status output | 10/100/1000 Ethernet interface |
| 100-240 Vcc | 1 | Power input | Power interface |
| LEDs | 6 | Status output | Status indicators |
| USB | 1 | Disabled except for power | Used in manufacturing |

**Table 10 - PA-2000 Series FIPS 140-2 Ports and Interfaces**

| Interface | PA-2050 Qty | PA-2020 Qty | FIPS 140-2 Designation | Name and Description |
|---|---|---|---|---|
| RJ45 | 1 | 1 | Data input, control input, data output, status output | Console port |
| RJ45 | 1 | 1 | Data input, control input, data output, status output | Out of band management |
| SFP | 4 | 2 | Data input, control input, data output, status output | Ethernet optical gigabit interface |
| RJ45 | 16 | 12 | Data input, control input, data output, status output | 10/100/1000 Ethernet interface |
| 100-240 Vcc | 1 | 1 | Power input | Power interface |
| LEDs | 6 | 6 | Status output | Status indicators |
| USB | 1 | 1 | Disabled except for power | Used in manufacturing |

**Table 11 - PA-3000 Series FIPS 140-2 Ports and Interfaces**

| Interface | PA-3050 Qty | PA3020 Qty | FIPS 140-2 Designation | Name and Description |
|---|---|---|---|---|
| RJ45 | 1 | 1 | Data input, control input, data output, status output | Console port |
| RJ45 | 1 | 1 | Data input, control input, data output, status output | Out of band management |
| RJ45 | 2 | 2 | Data input, control input, data output, status output | 10/100/1000 HA Ethernet interface |
| SFP | 8 | 8 | Data input, control input, data output, status output | Ethernet optical gigabit interface |
| RJ45 | 12 | 12 | Data input, control input, data output, status output | 10/100/1000 Ethernet interface |
| 100-240 Vcc | 1 | 1 | Power input | Power interface |
| LEDs | 6 | 6 | Status output | Status indicators |
| USB | 1 | 1 | Disabled except for power | Used in manufacturing |

**Table 12 - PA-4000 Series FIPS 140-2 Ports and Interfaces**

| Interface | PA-4060 Qty | PA-4050 Qty | PA-4020 Qty | FIPS 140-2 Designation | Name and Description |
|---|---|---|---|---|---|
| DB9 | 1 | 1 | 1 | Data input, control input, data output, status output | Console port |
| RJ45 | 1 | 1 | 1 | Data input, control input, data output, status output | Out of band management |
| XFP | 4 | 0 | 0 | Data input, control input, data output, status output | Ethernet optical 10-gigabit interface |
| SFP | 4 | 8 | 8 | Data input, control input, data output, status output | Ethernet optical gigabit interfaces |
| RJ45 | 2 | 2 | 2 | Data input, control input, data output, status output | 10/100/1000 HA Ethernet interface |
| RJ45 | 0 | 16 | 16 | Data input, control input, data output, status output | 10/100/1000 Ethernet Interfaces |
| 100-240 Vcc | 2 | 2 | 2 | Power input | Power interface |
| LEDs | 8 | 8 | 8 | Status output | Status indicators |
| USB | 2 | 2 | 2 | Disabled except for power | Used in manufacturing |

**Table 13 - PA-5000 Series FIPS 140-2 Ports and Interfaces**

| Interface | PA-5060 Qty | PA-5050 Qty | PA-5020 Qty | FIPS 140-2 Designation | Name and Description |
|---|---|---|---|---|---|
| RJ45 | 1 | 1 | 1 | Data input, control input, data output, status output | Console port |
| RJ45 | 1 | 1 | 1 | Data input, control input, data output, status output | Out of band management |
| SFP+ | 4 | 4 | 0 | Data input, control input, data output, status output | Ethernet optical 10-gigabit interface |
| SFP | 8 | 8 | 8 | Data input, control input, data output, status output | Ethernet optical gigabit interfaces |
| RJ45 | 2 | 2 | 2 | Data input, control input, data output, status output | 10/100/1000 HA Ethernet interface |

| Interface | PA-5060 Qty | PA-5050 Qty | PA-5020 Qty | FIPS 140-2 Designation | Name and Description |
|---|---|---|---|---|---|
| RJ45 | 12 | 12 | 12 | Data input, control input, data output, status output | 10/100/1000 Ethernet Interfaces |
| 100-240 Vcc | 2 | 2 | 2 | Power input | Power interface |
| LEDs | 8 | 8 | 8 | Status output | Status indicators |
| USB | 2 | 2 | 2 | Disabled except for power | Used in manufacturing |

**Table 14 - PA-7050 FIPS 140-2 Ports and Interfaces**

| Interface | Chassis[1] Qty | NPC [2] Qty | FIPS 140-2 Designation | Name and Description |
|---|---|---|---|---|
| RJ45 | 1 | N/A | Data input, control input, data output, status output | Console port |
| RJ45 | 1 | N/A | Data input, control input, data output, status output | Out of band management |
| RJ45 | 0 | 12 | Data input, control input, data output, status output | 10/100/1000 Ethernet Interfaces |
| SFP | 0 | 8 | Data input, control input, data output, status output | Ethernet optical gigabit interfaces |
| SFP+ | 0 | 4 | Data input, control input, data output, status output | Ethernet optical 10-gigabit interface |
| RJ45 | 2 | N/A | Data input, control input, data output, status output | 10/100/1000 HA Ethernet interface |
| QSFP | 2 | N/A | Data input, control input, data output, status output | HSCI HA interface |
| 100-240 Vcc | 4 | N/A | Power input | Power interface |
| LEDs[3] | 36 | 4 | Status output | Status indicators |
| USB | 1 | N/A | Disabled except for power | Used in manufacturing |

1. The PA-7050 chassis includes two cards that are installed in the front slots of the chassis. These cards include the following: The Switch Management Card (SMC) provides management connectivity to the chassis and the Log Processing Card (LPC) handles all log processing and log storage for the firewall.
2. NPC (Network Processing Card). The PA-7050 may contain up to six(6) NPC cards (p/n 910-000028) At least one Network Processing Cards (NPC) must be installed before the firewall can process data traffic. Up to five more NPCs can be added to expand port density and processing.
3. The chassis Status LED count includes the following; 4 for fan status, 12 for the LPC and 8 for the SMC, 12 for power supply.

# 5 Identification and Authentication Policy

***Assumption of Roles***

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

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

**Table 15 - Roles and Required Identification and Authentication**

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

**Table 16 - Strengths of Authentication Mechanisms**

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

# 6 Access Control Policy

***Roles and Services***

The services listed below are available in both FIPS Approved and non-Approved mode.

**Table 17 - Authenticated Service Descriptions**

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

**Note: Additional information on the services the module provides can be found at https://live.paloaltonetworks.com/community/documentation**

**Table 18 - Authenticated Services**

| Service | Crypto Officer | User | RA VPN | S-S VPN |
|---|---|---|---|---|
| Security Configuration Management | Y | N | N | N |
| Other Configuration | Y | N | N | N |
| View Other Configuration | Y | Y | N | N |
| Show Status | Y | Y | Y | Y |
| VPN | N | N | Y | Y |
| Firmware update | Y | N | N | N |

### *Unauthenticated Services*

The cryptographic module supports the following unauthenticated services:

**Table 19 - Unauthenticated Services**

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

The zeroization procedure is invoked when the operator exits CC (FIPS) mode. The procedure consists of overwriting the Master Key used to encrypt all CSPs. The operator must be in control of the module during the entire procedure to ensure that it has successfully completed. During the zeroization procedure, no other services are available.

### *Definition of Critical Security Parameters (CSPs)*

The modules contain the following CSPs:

**Table 20 - Private Keys and CSPs**

| CSP # | Key Name | Type | Description |
|---|---|---|---|
| 1 | Web interface private keys | RSA | Decrypts TLS session key and provides authentication services (admin web interface, captive portal, SSL VPN, packet inspection) |
| 2 | TLS PreMaster Secret | TLS Secret | Secret value used to derive the TLS session keys |
| 3 | TLS DH Private Components | DH | Diffie Hellman (Group 14) 2048 bit private component used in key establishment |
| 4 | TLS-HMAC | HMAC-SHA-1 | Authentication keys used in all https connections to the security module's web interface. |
| 5 | TLS session keys | AES | Used in all https connections to the security module's web interface. |
| 6 | SSH-Firewall private key | RSA | Used to identify the security appliance in SSH. The security modules support 512, 1024, and 2048 bit keys and only 2048 bit keys are supported in CC (FIPS) mode. |
| 7 | SSH-HMAC | HMAC-SHA-1 | Authentication keys used in all SSH connections to the security module's command line interface. |
| 8 | SSH session keys | AES | Used in all SSH connections to the security module's command line interface. |

| CSP # | Key Name | Type | Description |
|---|---|---|---|
| 9 | SSH DH Private Components | DH | Diffie Hellman (Group 14) 2048 bit private component used in key establishment |
| 10 | S-S VPN IPSec/IKEv1 authentication | HMAC-SHA-1 | Used to authenticate the peer in an IKE/IPSec tunnel connection. |
| 11 | S-S VPN IPSec/IKEv1 session key | AES | Used to encrypt IKE/IPSec data. These are AES (128 bit, 192 bit, 256 bit) keys. |
| 12 | S-S VPN IPSec/IKEv1 Diffie Hellman Private Components | DH | Diffie Hellman (Group 14) 2048 bit private component used in key establishment |
| 13 | S-S VPN IPSEC pre-shared keys | Part of HMAC | Manually distributed by an administrator in the CO role. Used in authentication. |
| 14 | RA VPN IPSec session key | AES-128 | Used to encrypt remote access sessions utilizing IPSec. |
| 15 | RA VPN IPSec authentication HMAC | HMAC-SHA-1 | Used in authentication of remote access IPSec data. |
| 16 | Firmware code integrity check | HMAC-SHA-256 | Used to check the integrity of crypto-related code. |
| 17 | Firmware Content encryption key | AES-256 | Used to decrypt firmware, software, and content. |
| 18 | CO, User, RA VPN Password | Password | Entered by the Operator. |
| 19 | Master Key | AES-256 | Used to encrypt crypto-related files on the firewall. |
| 20 | DRBG Seed / State | DRBG | Used by the DRBG. The state includes V and the Key. |
| 21 | DLP Private key | RSA | Used to encrypt DLP data. Only 2048 bit keys are supported. |

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

### *Definition of Public Keys*

The modules contain the following public keys:

**Table 21 - Public Keys**

| Key Name | Type | Description |
|---|---|---|
| Web interface certificates | RSA-2048 | Used to establish TLS sessions between firewall and user for web interface (management), captive portal, and remote access SSL VPN portal |
| CA certificate | RSA-2048 | Used to trust a CA for SSL decryption sessions |
| Client CA certificate | RSA-2048 | Used to verify client certificates for firewall administrators |
| Client OCSP verify CA certificate | RSA-2048 | Used for certificate validation via OCSP |
| TLS peer public key | RSA-2048 | Cert coming in from web server in outbound TLS decryption - used to encrypt the session key for client session with web server |
| TLS DH public components | DH – 2048 (Group 14) | Used in key agreement |
| SSH DH public components | DH – 2048 (Group 14) | Used in key agreement |
| SSH – Firewall public key | RSA-2048 | Used firewall in authentication process |
| S-S VPN - IPSec/IKEv1 Diffie Hellman public component | DH – 2048 (Group 14) | Used in key agreement |
| Public key for firmware content load test | RSA-2048 | Used to authenticate firmware and content to be installed on the firewall |
| DLP public key | RSA-2048 | Used to encrypt data loss prevention data |
| Client public key | RSA-2048 | Used to authenticate User, CO, or remote access VPN users |

### *Definition of CSPs Modes of Access*

Table 22 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as:

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

**Table 22 - CSP Access Rights within Roles & Services**

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

# 7 Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the PA-200, PA-500, PA-2000 Series, PA-3000 Series, PA-4000 Series, PA-5000 Series, and PA-7050 Firewalls do not contain modifiable operational environments.

# 8 Security Rules

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

1. The cryptographic module shall provide four distinct operator roles. These are the User role, Remote Access VPN role, Site-to-site VPN role, and the Cryptographic Officer role.
2. The cryptographic module shall provide identity-based authentication.
3. The cryptographic module shall clear previous authentications on power cycle.
4. When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
5. The cryptographic module shall perform the following tests
    A. Power up Self-Tests
        1. Cryptographic algorithm tests
            a. AES Encrypt Known Answer Test
            b. AES Decrypt Known Answer Test
            c. CCM Known Answer Test
            d. RSA Sign Known Answer Test
            e. RSA Verify Known Answer Test
            f. HMAC-SHA-1 Known Answer Test
            g. HMAC-SHA-256 Known Answer Test
            h. SHA-1 Known Answer Test
            i. SHA-256 Known Answer Test
            j. SHA-384 Known Answer Test
            k. SHA-512 Known Answer Test
            l. DH Parameter Test
            m. DRBG Known Answer Test
            n. SP800-90A Section 11.3 Health Tests
    B. Firmware Integrity Test – A 128 bit EDC (using MD5) is calculated on non-security related code. Security related code is verified with HMAC-SHA-256.
    C. Critical Functions Tests
        1. N/A
    D. Conditional Self-Tests
        1. Continuous Random Number Generator (RNG) test – performed on NDRNG and DRBG, 128 bits
        2. RSA Pairwise Consistency Test (when a key generation fails, the error message displayed is “Cannot verify key and certificate. Maybe the passphrase is incorrect.”)

3. Firmware Load Test – Verify RSA 2048 signature on firmware at time of load
4. If any conditional test fails, the module will output 'CCEAL4 failure' and the specific test that failed.

6. The operator shall be capable of commanding the module to perform the power-up self-test by cycling power of the module.
7. Power-up self-tests do not require any operator action.
8. Data output shall be inhibited during key generation, self-tests, zeroization, and error states.
9. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
10. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
11. The module maintains separation between concurrent operators.
12. The module does not support a maintenance interface or role.
13. The module does not have any external input/output devices used for entry/output of data.
14. The module does not enter or output plaintext CSPs.
15. The module does not output intermediate key generation values.

Vendor imposed security rules:

1. The module does not support the update of the logical serial number or vendor ID.
2. The module does not provide access to revenue related data structures while plaintext CSPs are present.
3. If the cryptographic module remains inactive in any valid role for the administrator specified time interval, the module automatically logs out the operator.
4. The module enforces a timed access protection mechanism that supports at most ten authentication attempts per minute. After the administrator specified number of consecutive unsuccessful Password validation attempts have occurred, the cryptographic module shall enforce a wait period of at least 1 minute before any more login attempts can be attempted. This wait period shall be enforced even if the module power is momentarily removed.

# 9 Physical Security Policy

***Physical Security Mechanisms***

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

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

Refer to Appendix A for instructions on installation of the tamper seals and opacity shields. The locations of the five (5) tamper evident seals implemented on the PA-200 are shown in Figure 30 through Figure 31

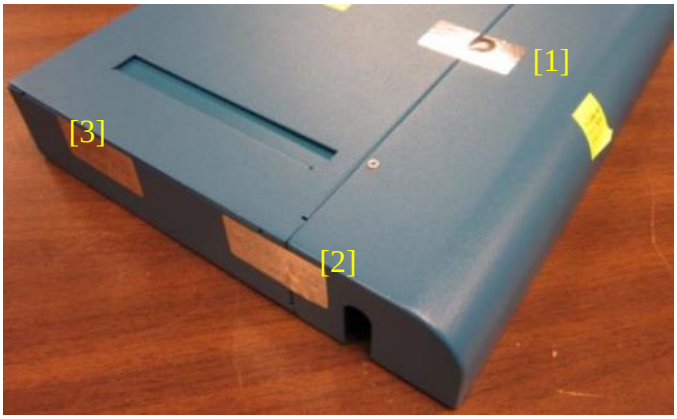



**Figure 30 - PA-200 Left Side and Top Tamper Seal Placement (3)**

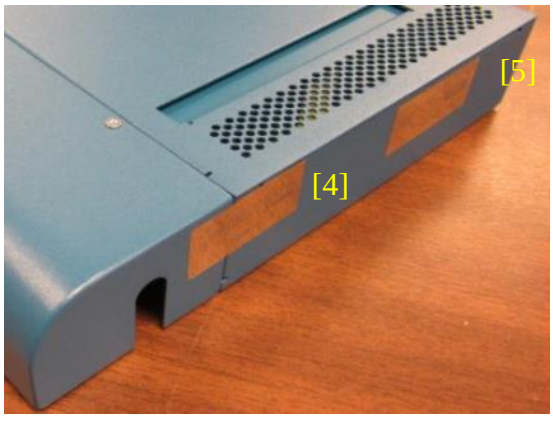



**Figure 31 - PA-200 Right Side Tamper Seal Placement (2)**

Refer to Appendix B for instructions on installation of the tamper seals and opacity shields. The locations of the twelve (12) tamper evident seals implemented on the PA-500 are shown in Figure 32 through Figure 35

**Figure 32 - PA-500 Front Tamper Seal Placement (1)**

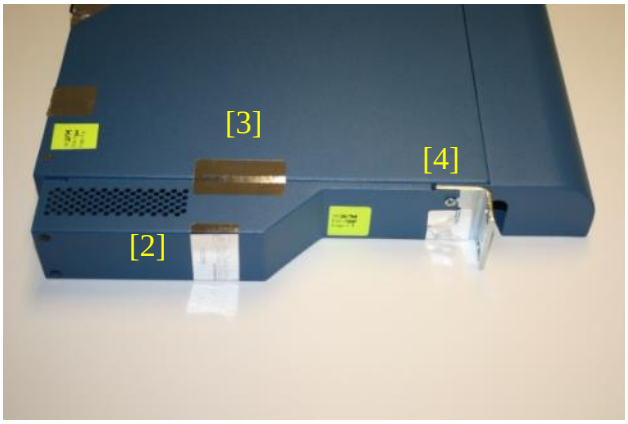



**Figure 33 - PA-500 Left Side Tamper Seal Placement (3)**

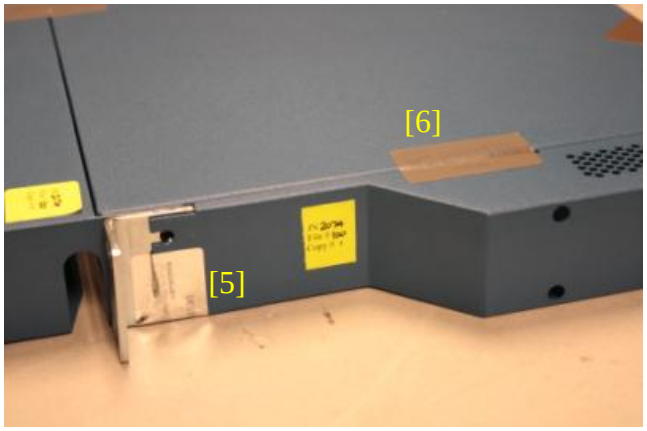



**Figure 34 - PA-500 Right Side Tamper Seal Placement (2)**

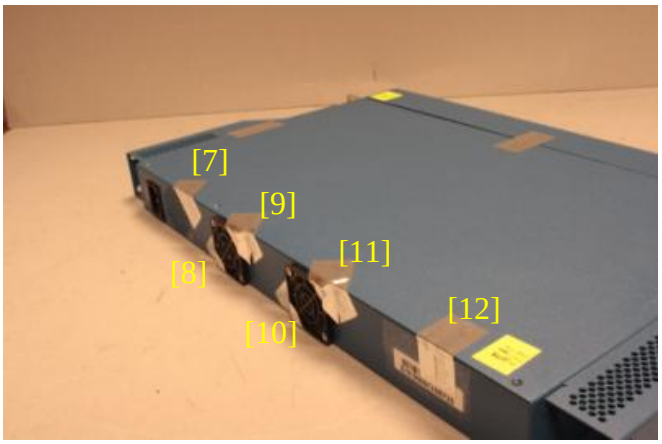



**Figure 35 - PA-500 Rear Tamper Seal Placement (6)**

Refer to Appendix C for instructions on installation of the tamper seals and opacity shields. The locations of the ten (10) tamper evident seals on the PA-2000 Series modules are shown in Figure 36 through Figure 39

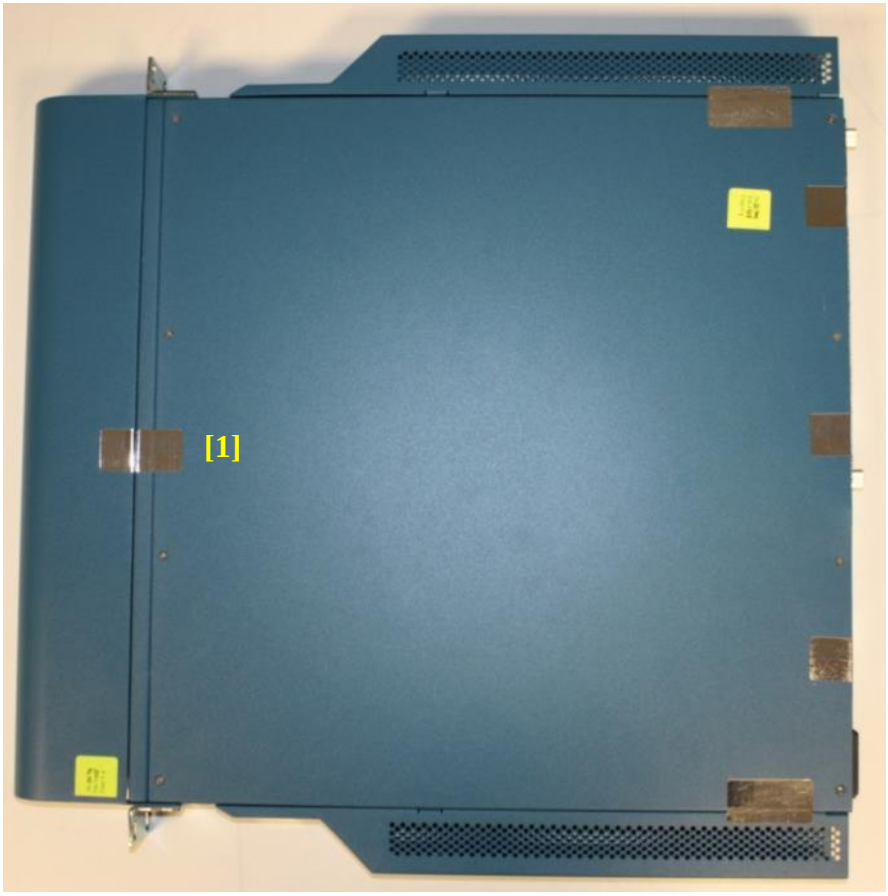



**Figure 36 - PA-2000 Series Front Tamper Seal Placement (1)**

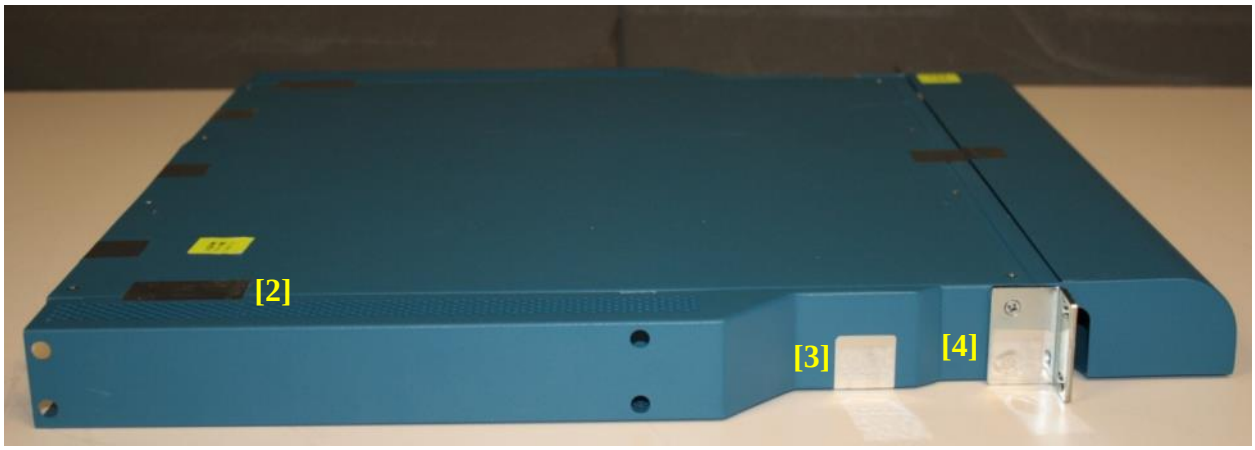



**Figure 37 - PA-2000 Series Left Side Tamper Seal Placement (3)**

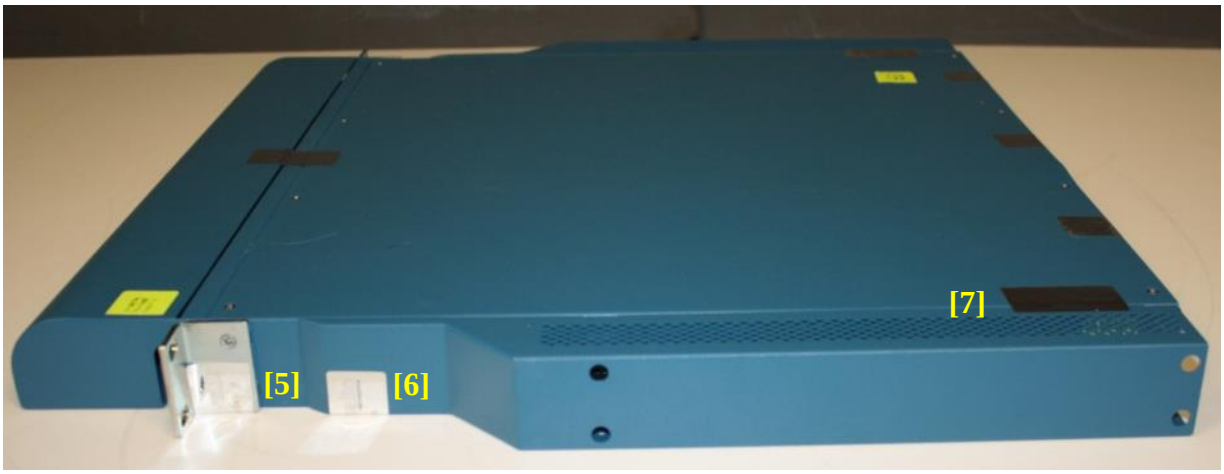



**Figure 38 - PA-2000 Series Right Side Tamper Seal Placement (3)**

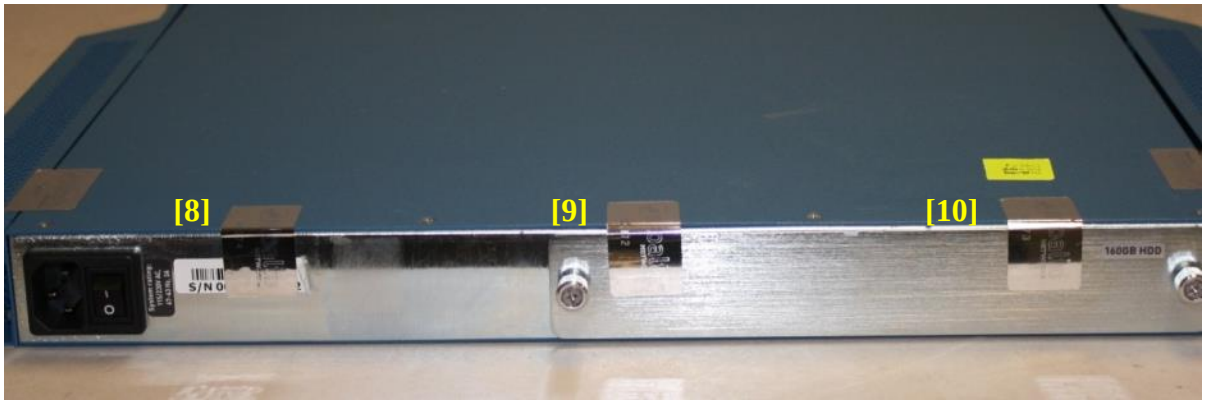



**Figure 39 - PA-2000 Series Rear Tamper Seal Placement (3)**

Refer to Appendix D for instructions on installation of the tamper seals and opacity shields. The locations of the seven (7) tamper evident seals on the PA-3000 Series modules are shown in Figure 40 through Figure 42

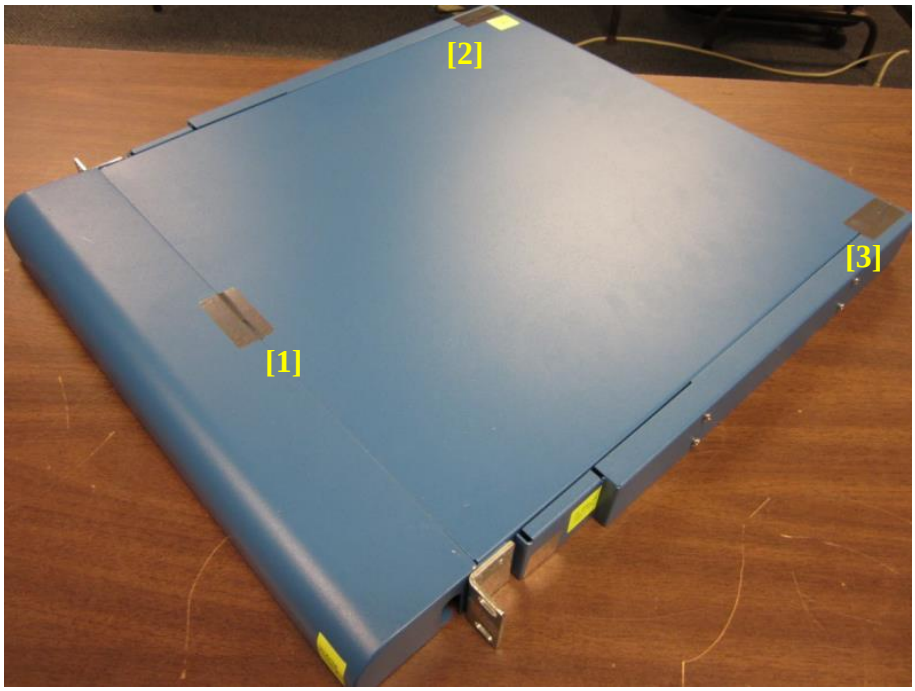



**Figure 40 - PA-3000 Series Tamper Seal Placement (3)**

**Figure 41 - PA-3000 Series Tamper Seal Placement (2)**

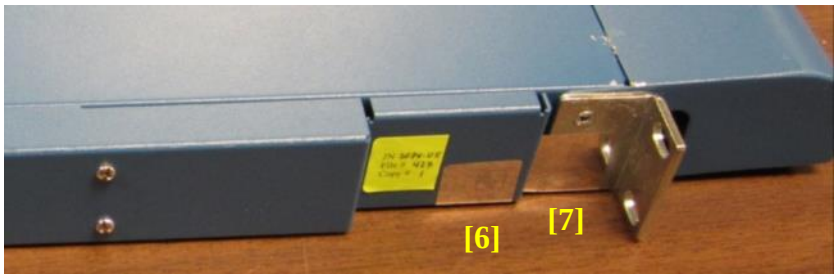



**Figure 42 - PA-3000 Series Tamper Seal Placement (2)**

Refer to Appendix E for instructions on installation of the tamper seals and opacity shields. The locations of the ten (10) tamper evident seals implemented on the PA-4000 Series modules are shown in Figure 43 through Figure 46 below.

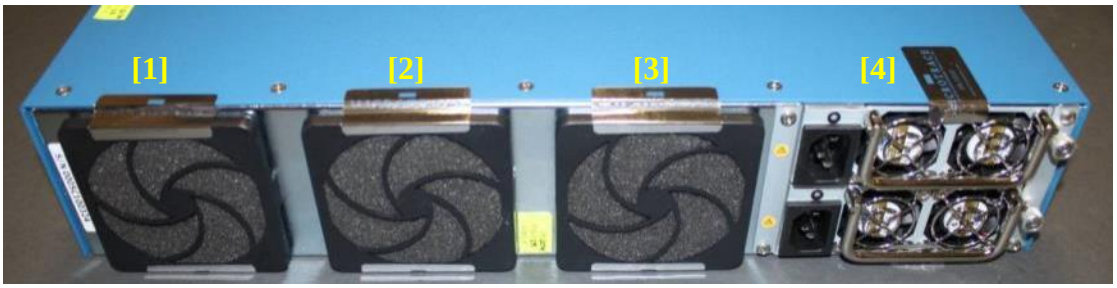



**Figure 43 - PA-4000 Series Rear Tamper Seal Placement – From Top (4)**

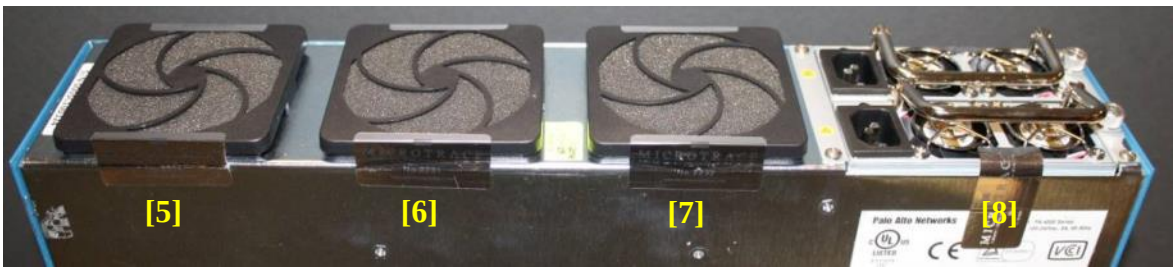



**Figure 44 - PA-4000 Series Rear Side Tamper Seal Placement – From Underside (4)**

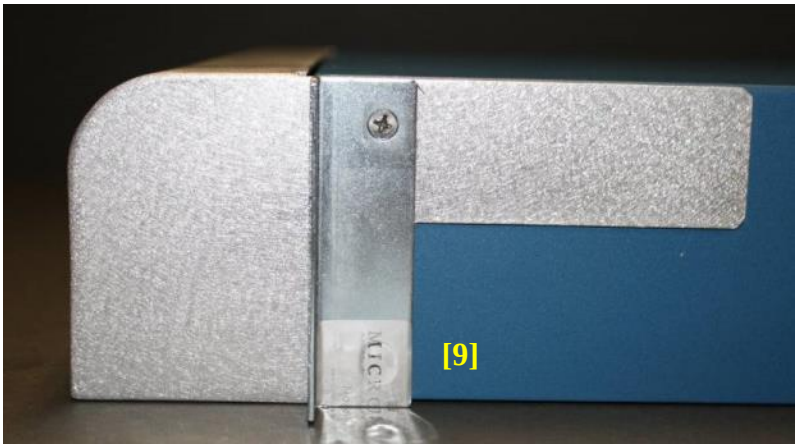



**Figure 45 - PA-4000 Series Right Side Tamper Seal Placement (1)**

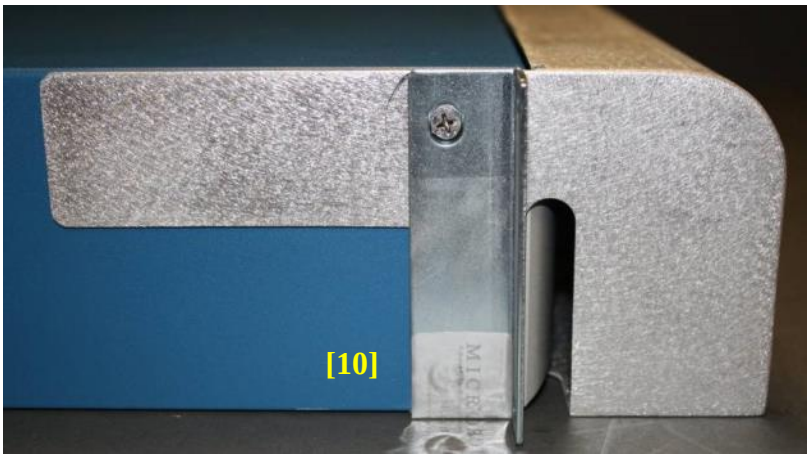



**Figure 46 - PA-4000 Series Left Side Tamper Seal Placement (1)**

Refer to Appendix F for instructions on installation of the tamper seals and opacity shields. The locations of the seventeen (17) tamper evident seals implemented on the PA-5000 Series modules are shown in Figure 47 through Figure 49 below

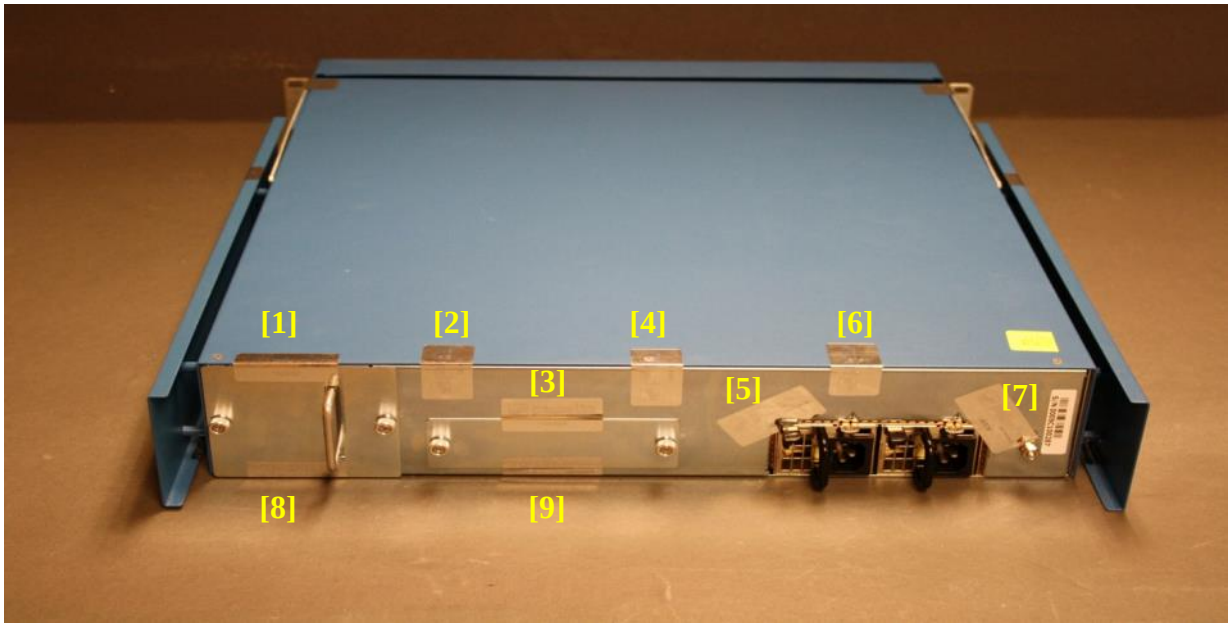



**Figure 47 - PA-5000 Series Rear Tamper Seal Placement (9)**

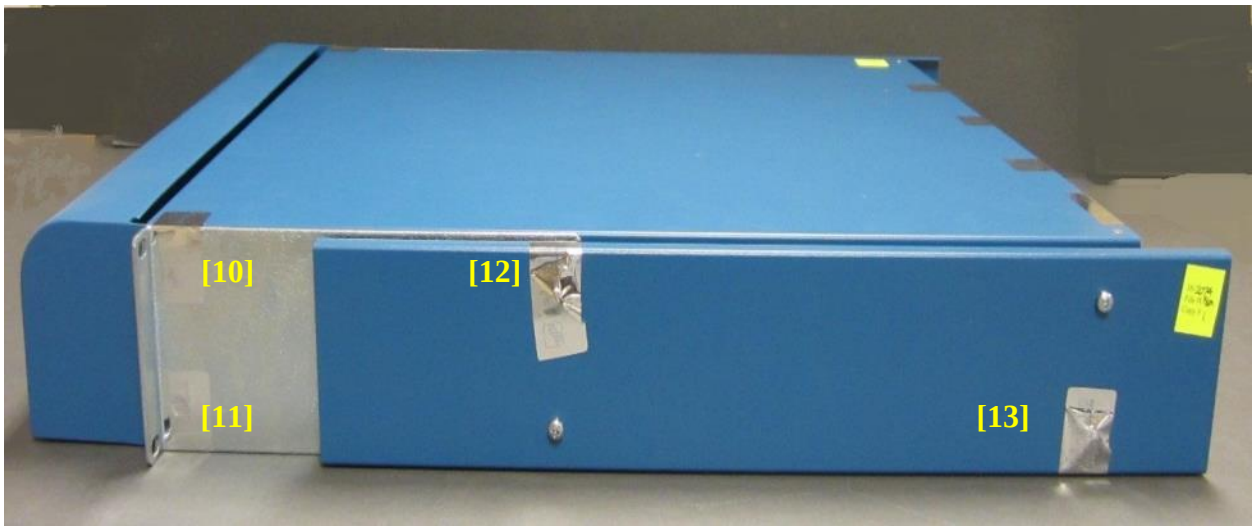
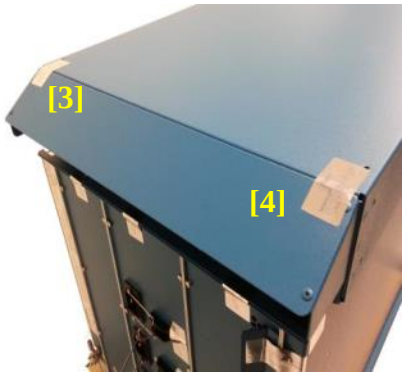



**Figure 48 - PA-5000 Series Right Side Tamper Seal Placement (4)**

**Figure 49 - PA-5000 Series Left Side Tamper Seal Placement (4)**

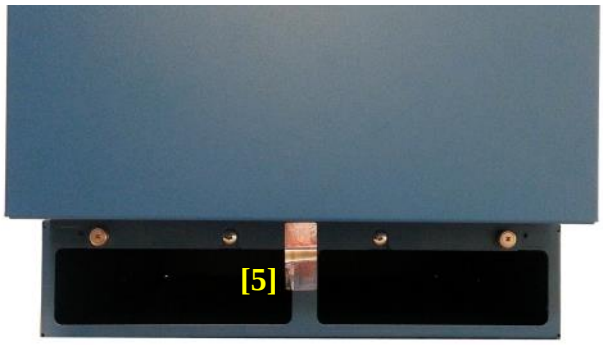
Refer to Appendix G for instructions on installation of the tamper seals and opacity shields. The locations of the twenty-four (24) tamper evident seals implemented on the PA-7050 Series modules are shown in Figure 50 through Figure 54 below.

Front

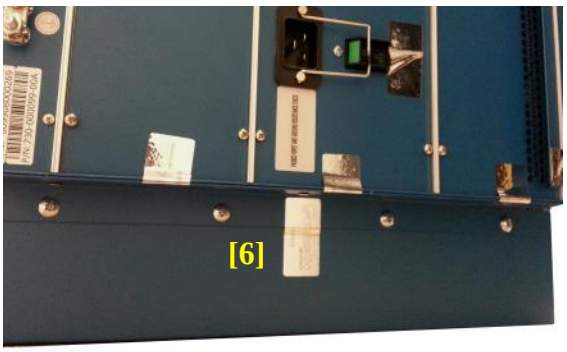



Rear

**Figure 50 - PA-7050 Tamper Seal Placement for Top Plenum (1-4)**




Front




Rear

**Figure 51 - PA-7050 Tamper Seal Placement for Bottom Plenum (5-6)**

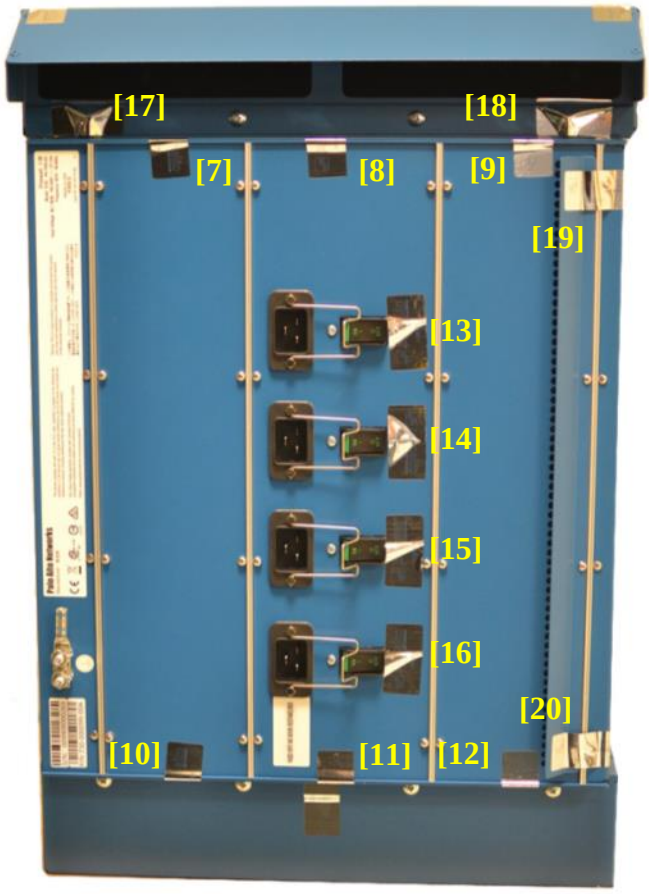



**Figure 52 - PA-7050 Tamper Seal Placement for Rear Panels (7-12), Power Switches (13-16) and Opacity Shields (17-20)**

**Figure 53 - PA-7050 Tamper Seal Placement for Top Plenum Bracket (21-22)**

**Figure 54 - PA-7050 Tamper Seal Placement for Bottom Plenum Bracket (23-24)**

### *Operator Required Actions*

**Table 23 - Inspection/Testing of Physical Security Mechanisms**

| Model | Physical Security Mechanisms | Recommended Frequency of Inspection/Test | Inspection/Test Guidance Details |
|---|---|---|---|
| PA-7050, PA-5060, PA-5050, PA-5020, PA-4060, PA-4050, PA-4020, PA-3050, PA-3020, PA-2050, PA-2020, PA-500, PA 200 | Tamper Evident Seals | 30 days | *Verify integrity of tamper evident seals in the locations identified in the FIPS Kit Installation Guide. Seal integrity may be verified within the modules operating temperature range, between 0 and 50 C.* |
| PA-7050 | Top, Bottom, Front and Rear Opacity Shields | 30 days | *Verify that the plenums and opacity shields have not been deformed from their original shape, thereby reducing their effectiveness* |
| PA-5060, PA-5050, PA-5020, PA-3050, PA-3020, PA-2050, PA-2020, PA-500 | Front Cover and Side Opacity Shields | 30 days | *Verify that front cover and side opacity shields have not been deformed from their original shape, thereby reducing their effectiveness* |
| PA-4020, PA-4050, PA-4060 | Front Cover | 30 days | *Verify that front cover has not been deformed from its original shape thereby reducing its effectiveness* |
| PA-200 | Front cover and Cage Enclosure | 30 days | *Verify that front cover and cage enclosure have not been deformed from their original shape, thereby reducing their effectiveness* |

# 10 Mitigation of Other Attacks Policy

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

# 11 References

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

# 12 Definitions and Acronyms

API – Application Programming Interface

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

BGP – Border Gateway protocol – Dynamic routing protocol

CA – Certificate authority

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

CO – Cryptographic Officer

DB9 – Console port connector

DLP – Data loss prevention

Gbps – Gigabits per second

HA – High Availability

HSCI - High Speed Chassis Interconnect

IKE – Internet Key Exchange

IP – Internet Protocol

IPSec – Internet Protocol Security

LDAP – Lightweight Directory Access Protocol

LED – Light Emitting Diode

NDRNG – Non-deterministic random number generator

OCSP – Online Certificate Status Protocol

OSPF – Open Shortest Path First – Dynamic routing protocol

PAN-OS – Palo Alto Networks' Operating System

QoS – Quality of Service

RA VPN – Remote Access Virtual Private Network

RIP – Routing Information Protocol – Dynamic routing protocol

RJ45 – Networking Connector

RNG –Random number generator

S-S VPN – Site to site Virtual Private Network

SFP – Small Form-factor Pluggable Transceiver

SSL – Secure Sockets Layer

TLS – Transport Layer Security

USB – Universal Serial Bus

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

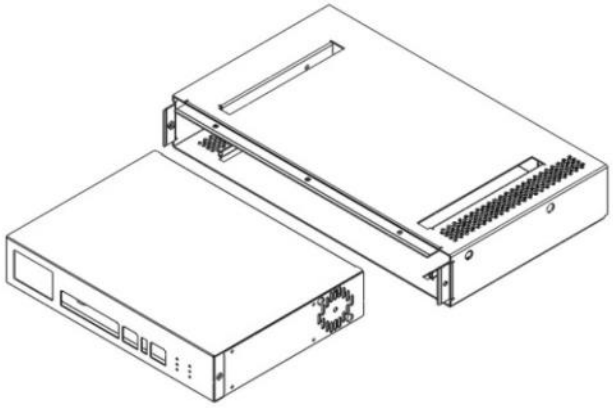
VPN – Virtual Private Network

XFP – 10 Gigabit Small Form Factor Pluggable Transceiver

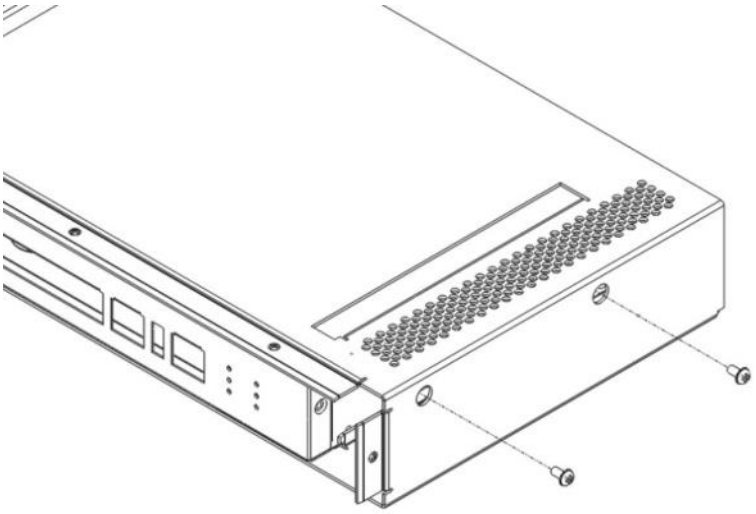
XML – Extensible Markup Language

# 13 Appendix A - PA-200 - FIPS Accessories/Tamper Seal Installation (5 Seals)

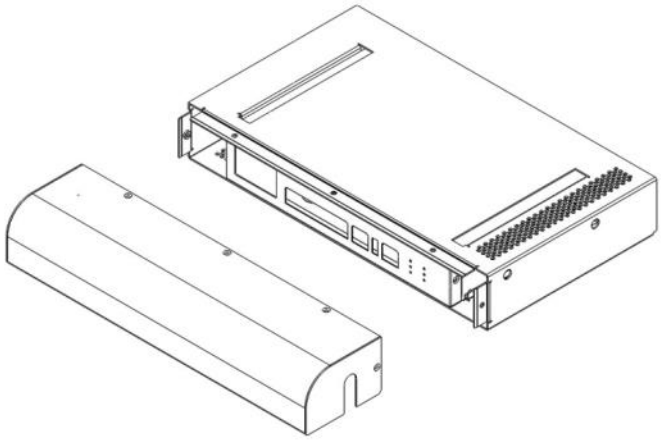
1. Insert the PA-200 unit into the cage.



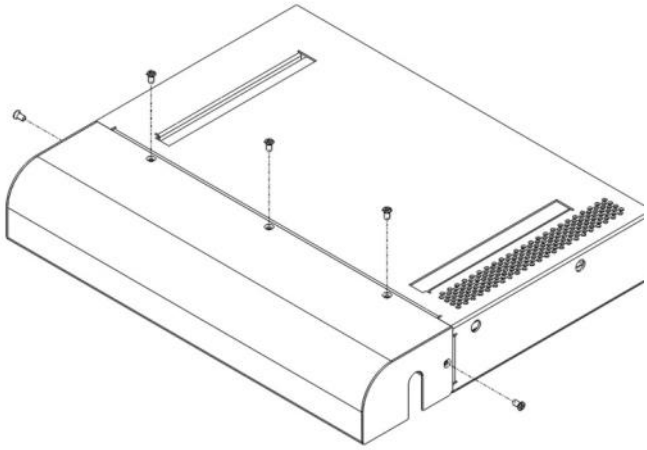
2. Secure right side of the PA-200 unit to the cage with (2x) 4-40x1/2” screws provided in the kit. Repeat for the left side of the cage.



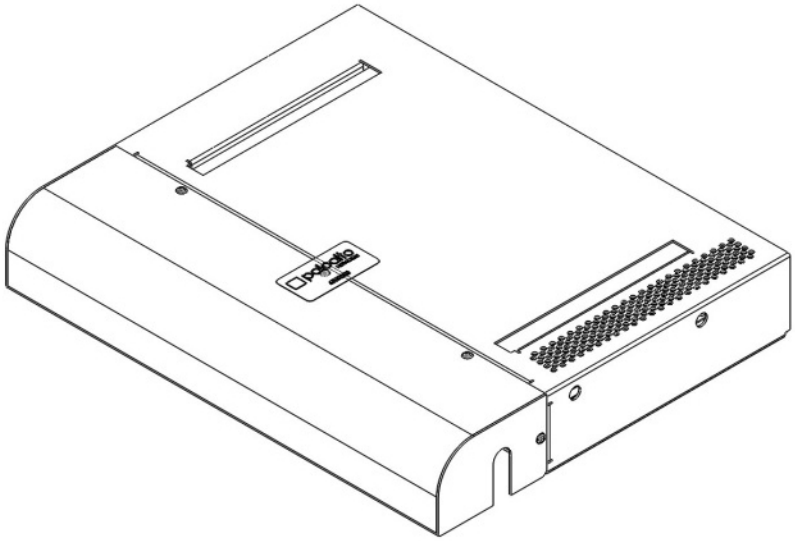
3. Install the front panel with the curve side up to the front cage.



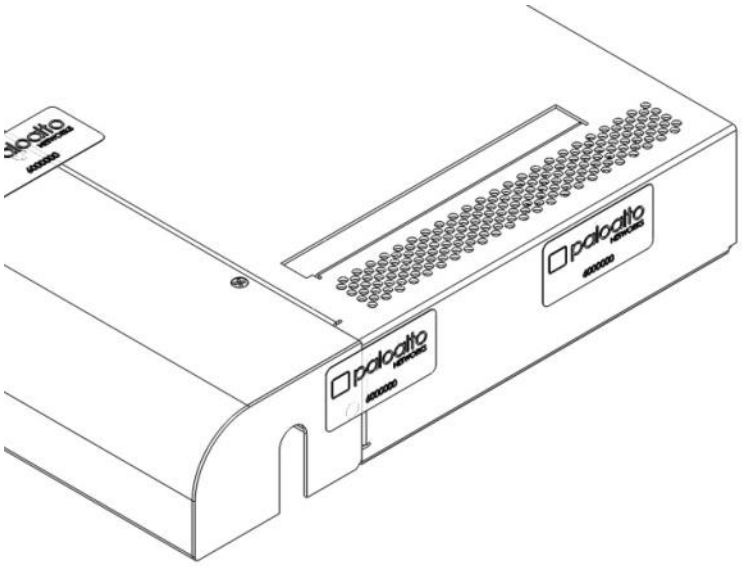
4. Secure the front panel to the cage with (5x) 4-40x3/16” screws.



5. Affix a tamper seal on the top middle of the front panel screw.

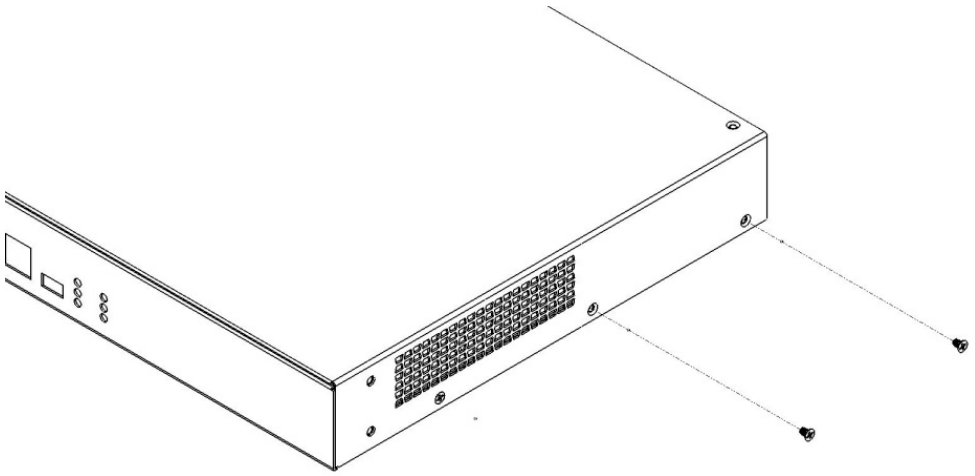


6. Affix two tamper seals over both screw mounting holes on the cage and right side screw on the front panel. Repeat for the left side

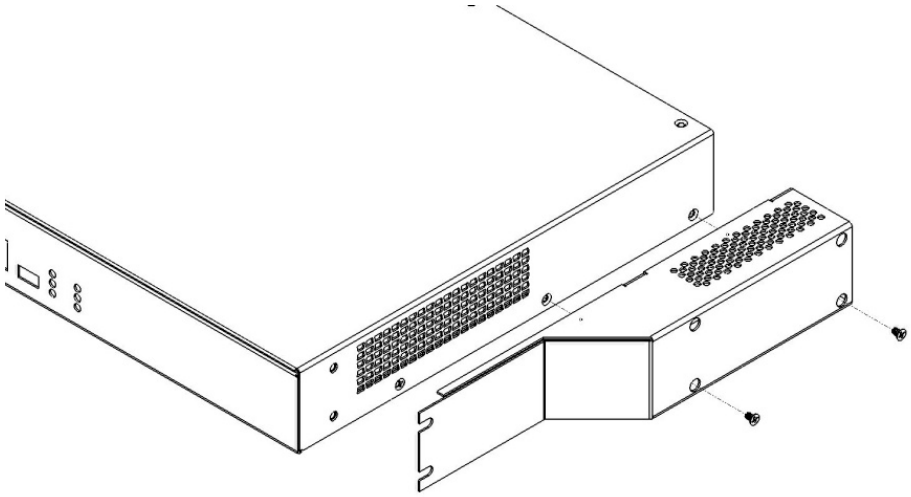


# 14 Appendix B - PA-500 - FIPS Accessories/Tamper Seal Installation (12 Seals)

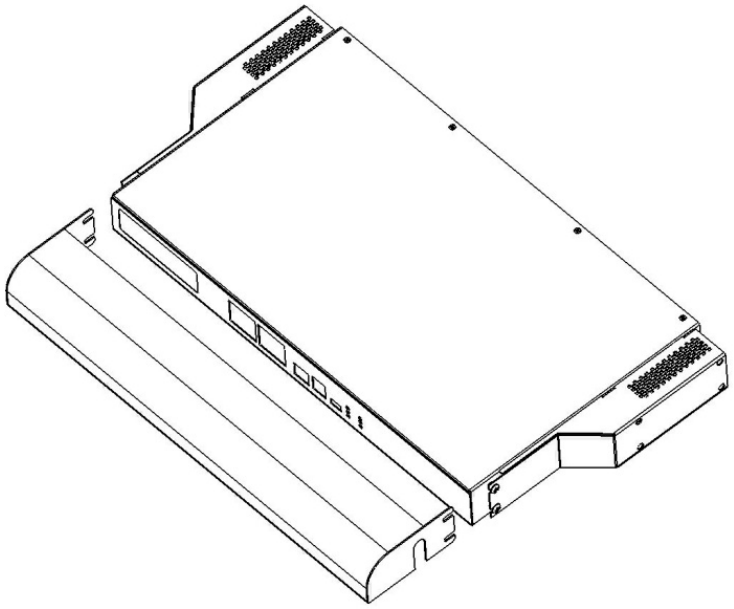
1. Remove the right side cover screws. Repeat for the left side cover screws.



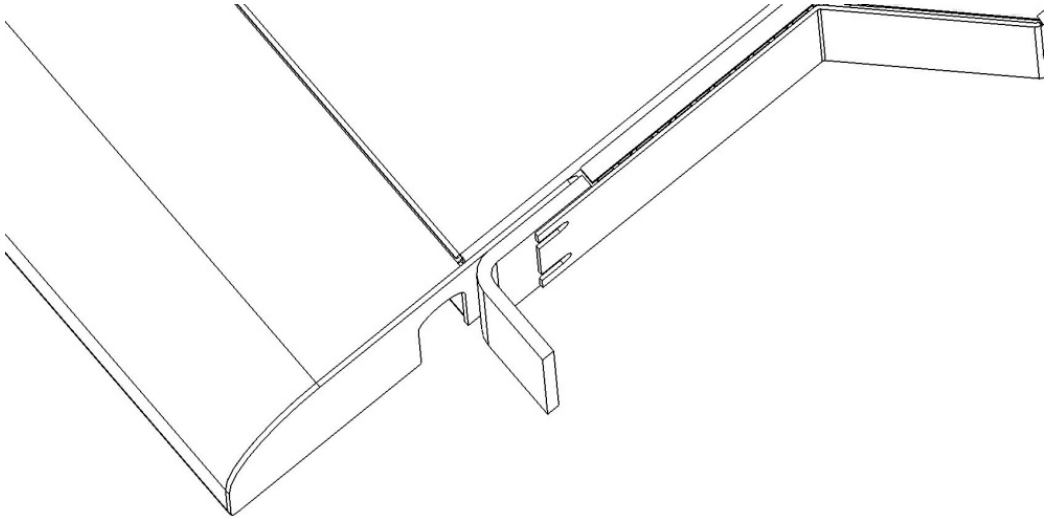
2. Install the right side FIPS opacity shield and secure with 2x #4-40x1/4" SEMS screws provided in the kit. Repeat for the left side.



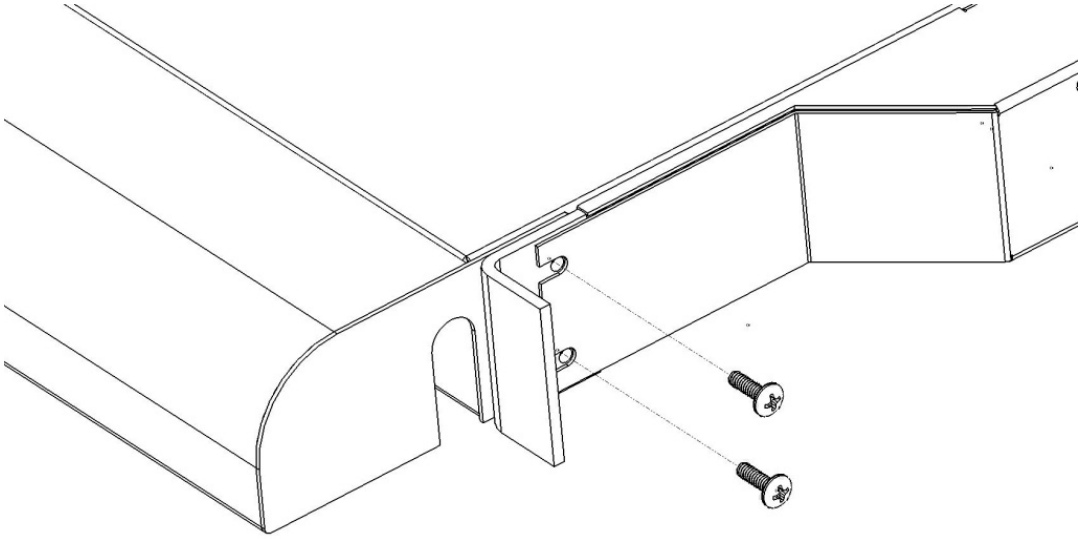
3. Install the front FIPS panel with the curve side up and align with the ear mounting screw holes.



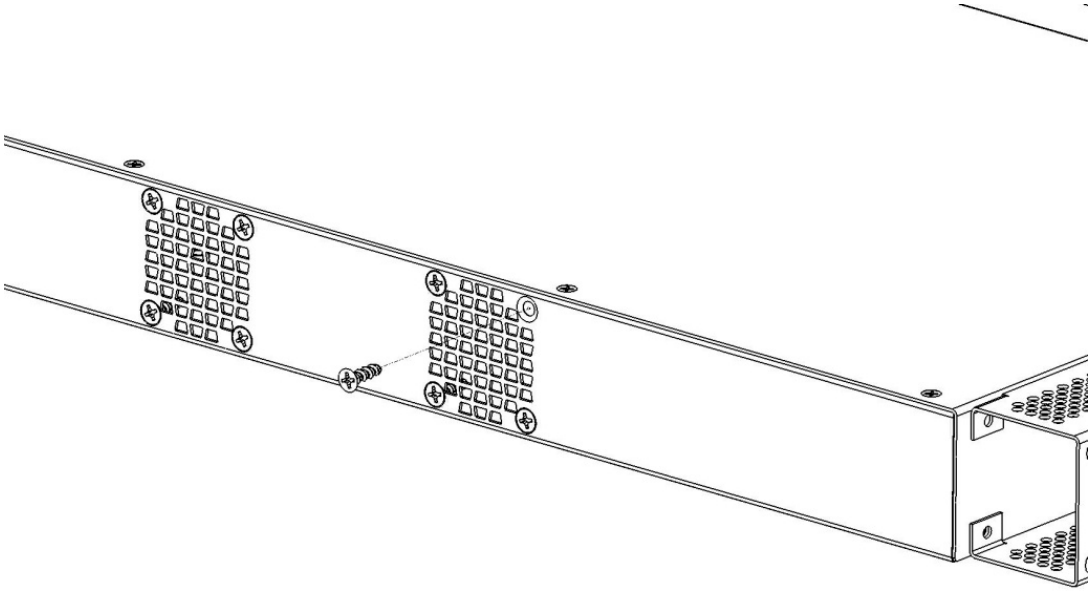
4. Sandwich the right side mounting ear between the front panel and the opacity shield. Repeat with the left side of the chassis.



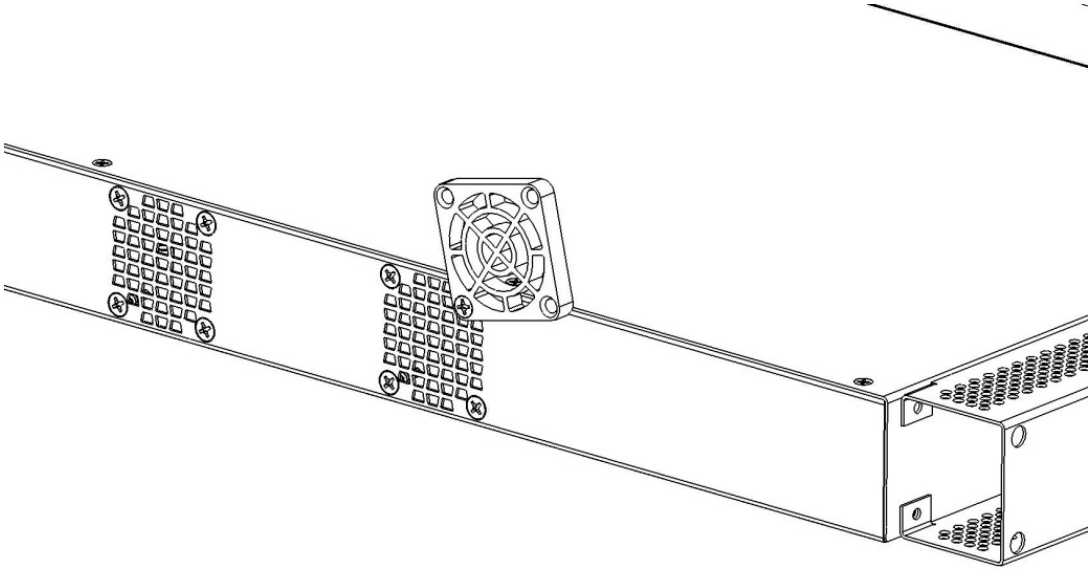
5. Install and secure the right side mounting ear with (2x) #6-32x1/2” Truss screws provided in the kit. Repeat on the left side.



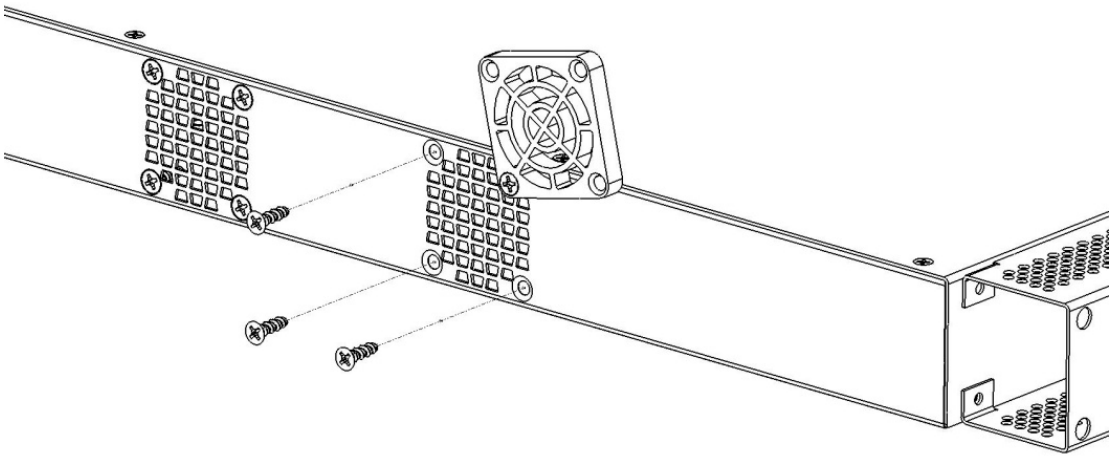
6. Remove 1x upper-right fan screw.



7. Install and partially tighten the screw on one of the fan guard mounting holes.

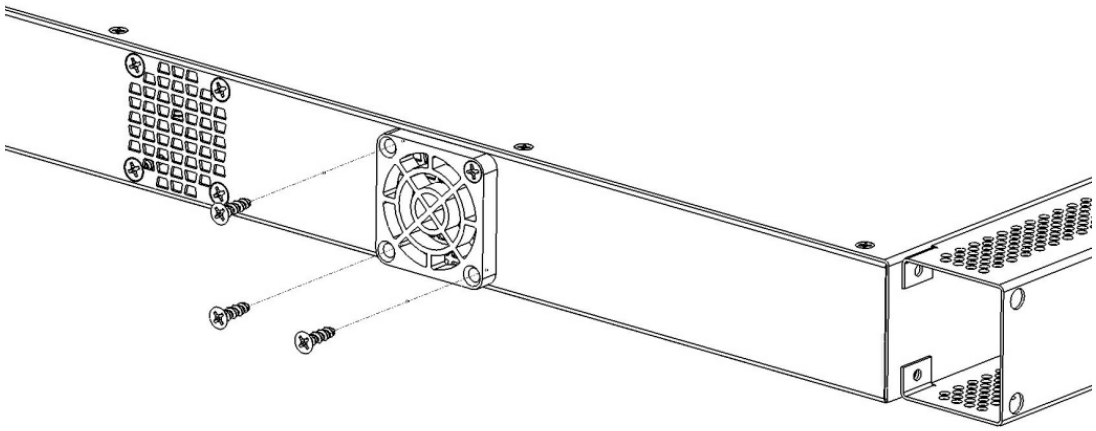


8. Remove the other 3x fan screws.



10. Align the fan guard and secure with 3x screws as shown. Repeat the installation steps for the other fan.

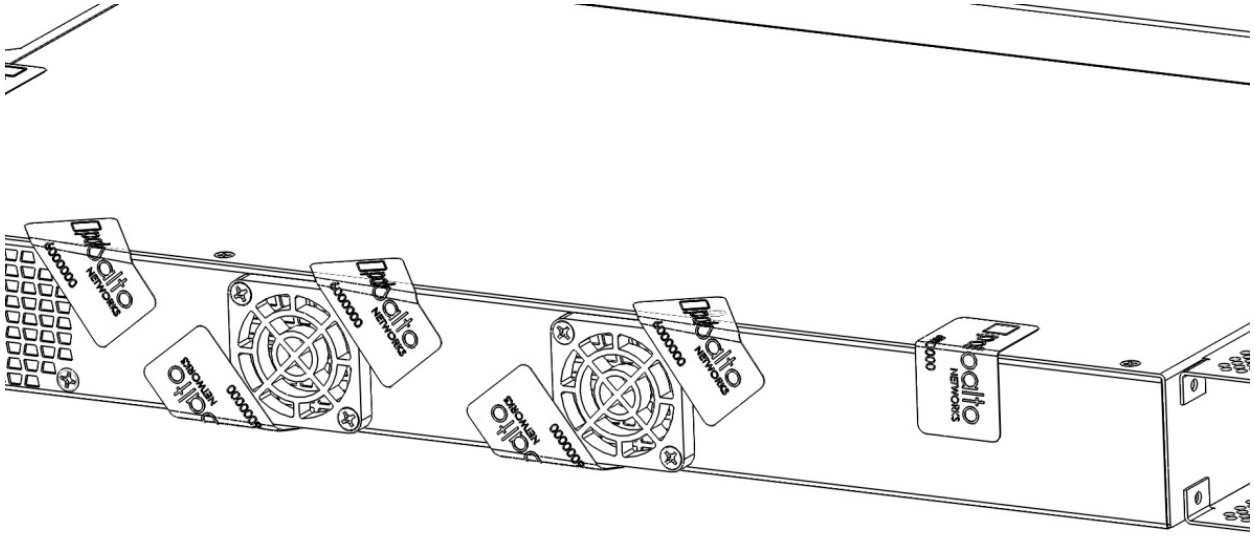
Caution: The fan guard may crack if you over-tighten the screws.



11. Affix one tamper seal over top cover/rear left chassis.

Affix one tamper seal over the upper PSU screw.

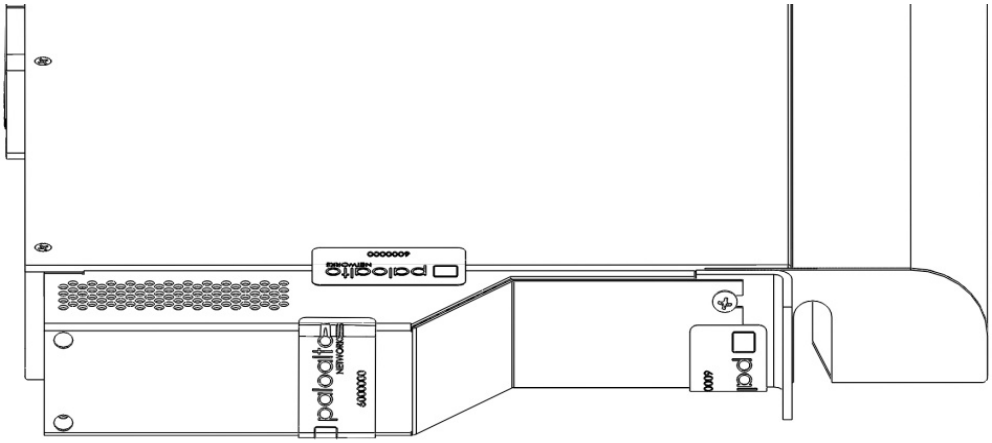
Affix four tamper seals over the fan cover screws.



12 Affix a tamper seal over both screw access holes on the left side opacity shield.

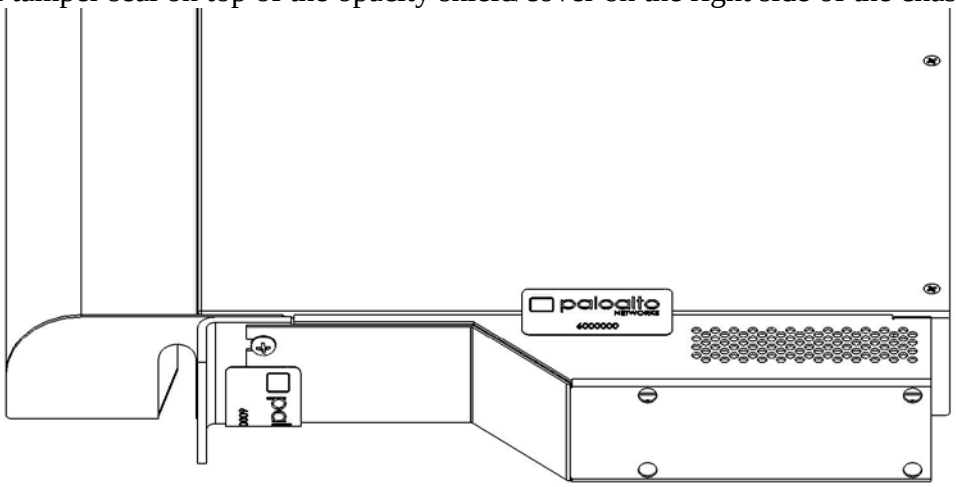
Affix a tamper seal over the bottom ear screw on the left side of the chassis.

Affix a tamper seal on top of the opacity shield/cover on the left side of the chassis.

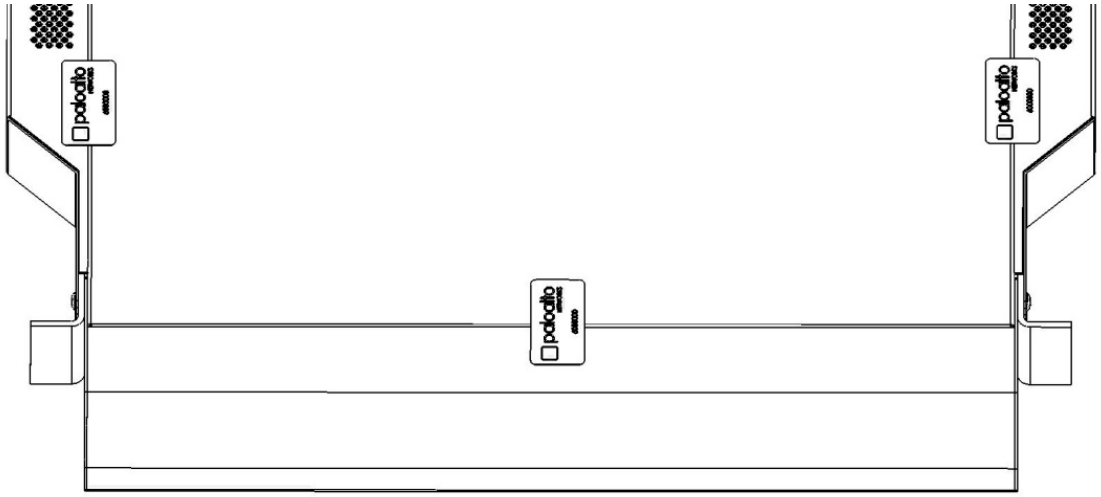


13. Affix a tamper seal over the bottom ear screw on the right side of the chassis.

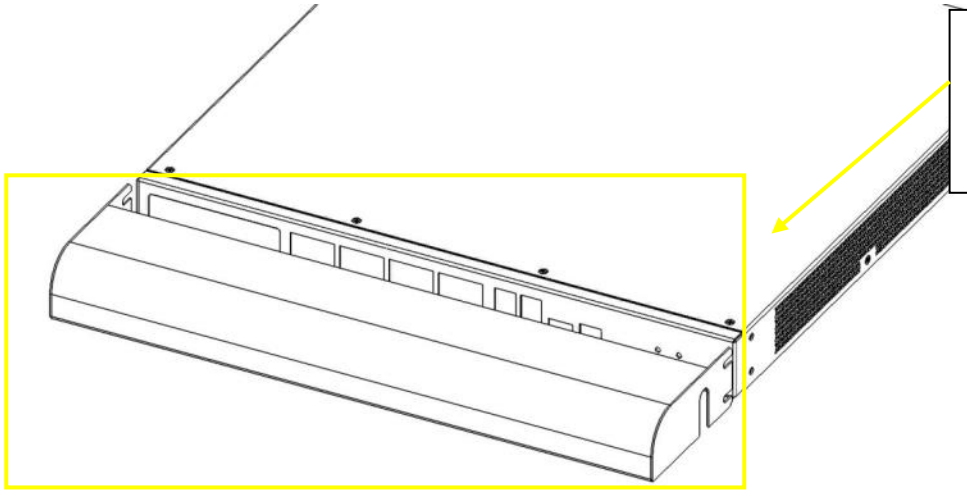
Affix a tamper seal on top of the opacity shield/cover on the right side of the chassis.



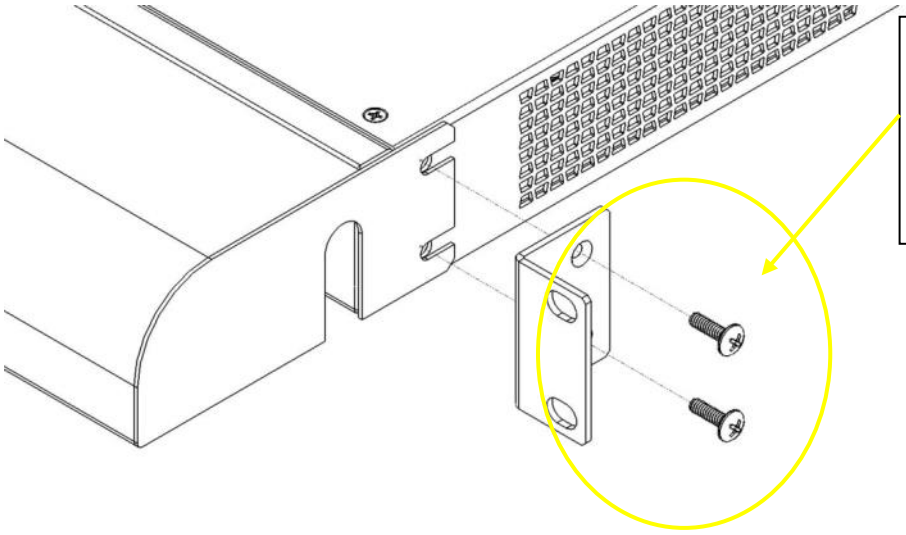
14. Affix a tamper seal on the top of the cover and panel.



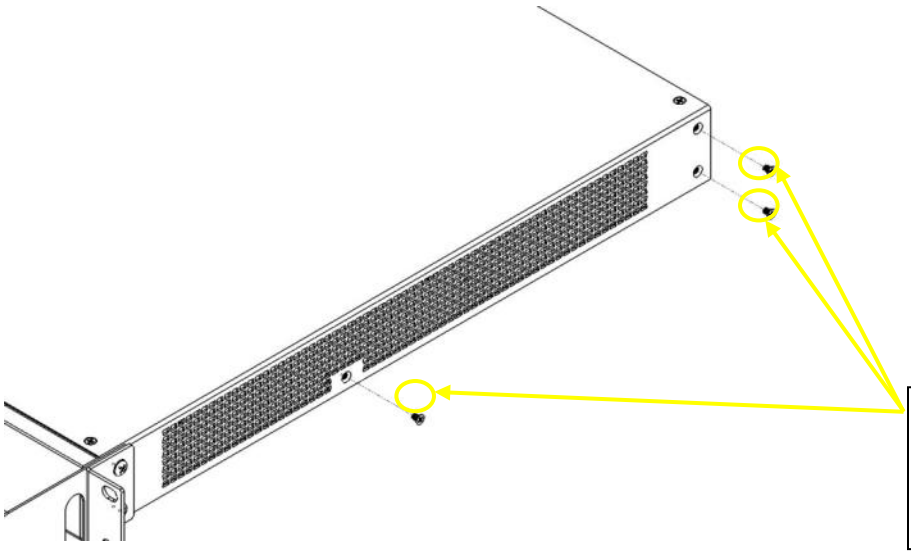
# 15 Appendix C - PA-2000 Series - FIPS Accessories/Tamper Seal Installation (10 Seals)



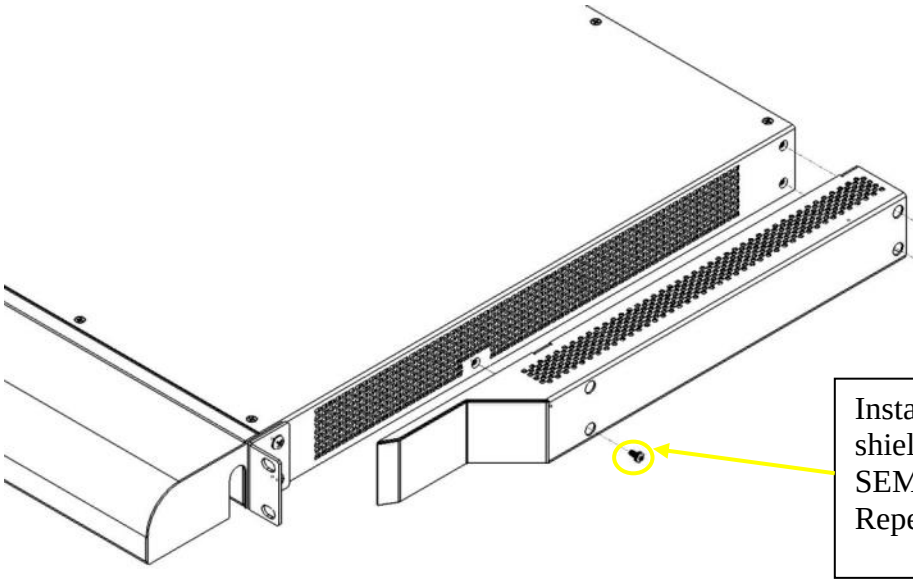
Install the front panel with the curve side up and line it up to the left and right side ear mounting holes.



Install and secure the right side mounting ear with (2x) 6-32x1/2” screws provided in the kit. Repeat the same step on the left side of the chassis.



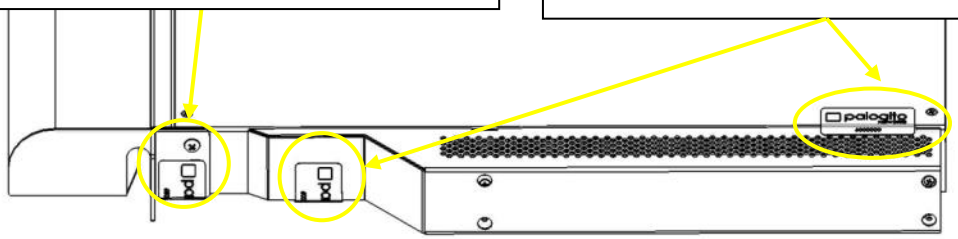
Remove the right side cover screws. Repeat the same steps for the left side cover screws.

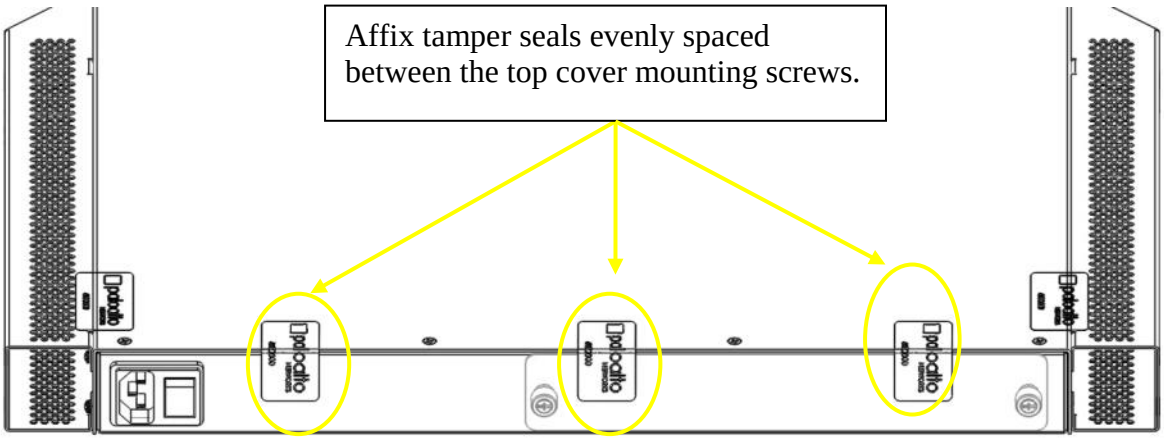


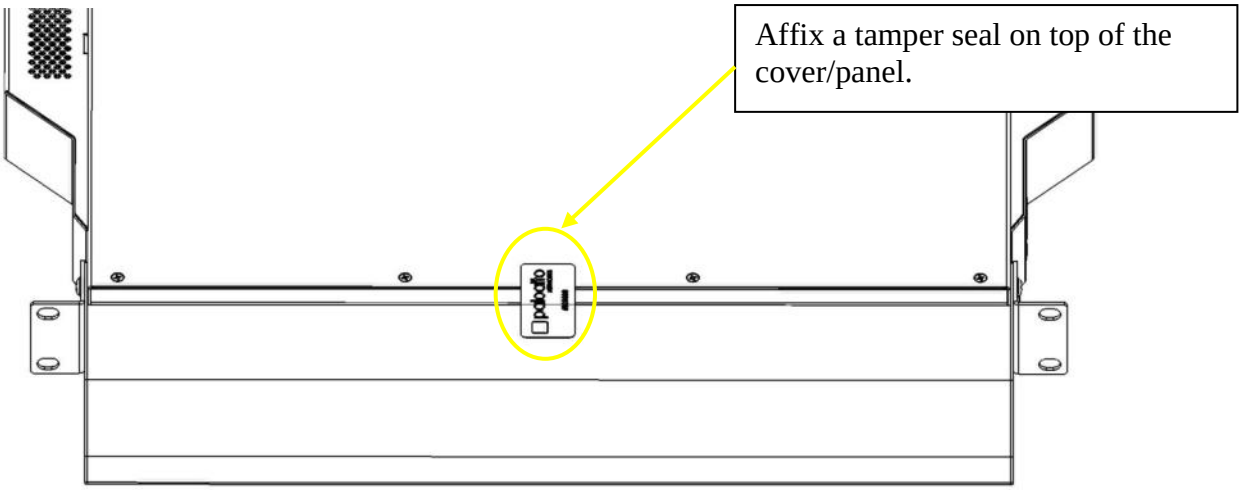
Install the right side FIPS opacity shield and secure with 3x #4-40x1/4" SEM screws provided by the kit. Repeat the same steps for the left side.

Affix a tamper seal to cover the right side bottom ear mounting bracket screw. Repeat the same steps for the left side.

Affix a tamper seal at right side of the chassis between the top cover and the FIPS opacity shield. Affix another tamper seal between the bottom chassis and the FIPS opacity shield. Repeat the same steps for the left side.

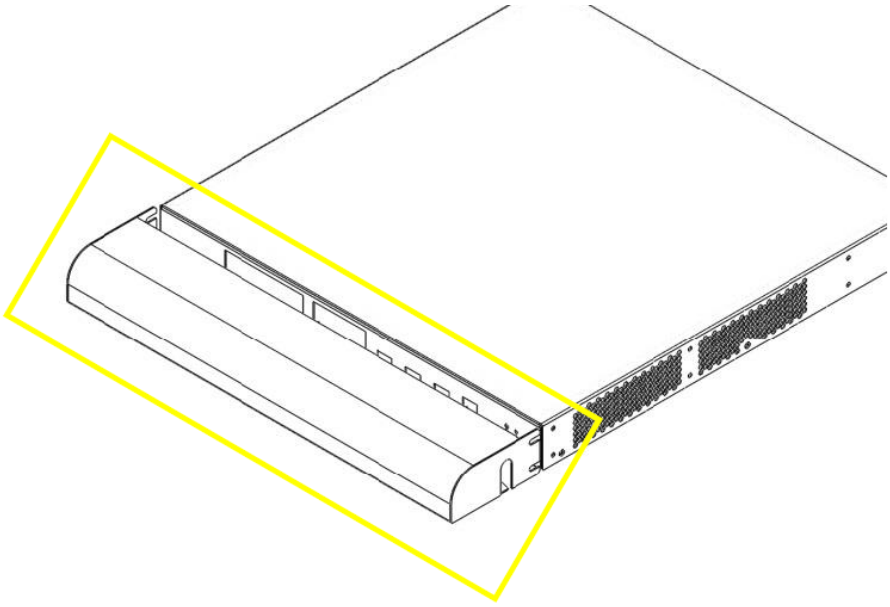



Affix tamper seals evenly spaced between the top cover mounting screws.

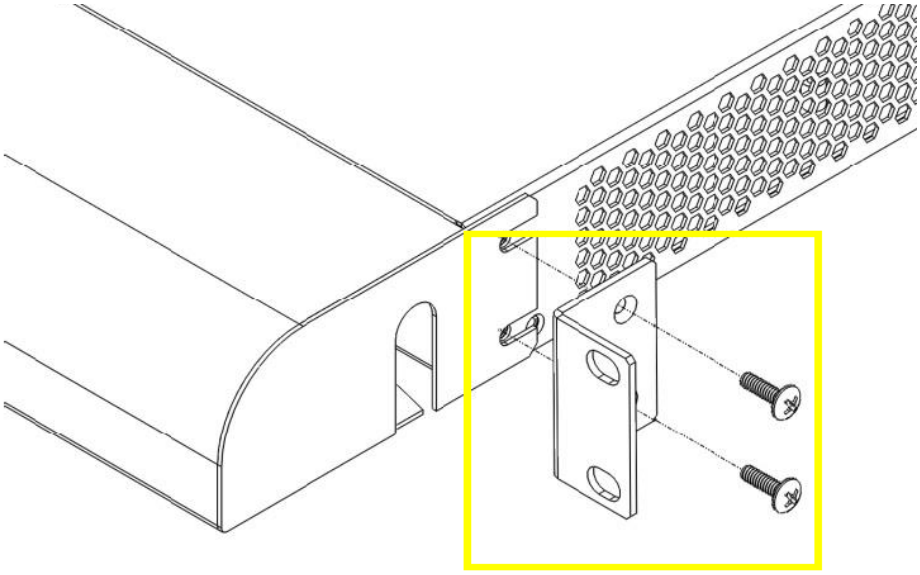

Affix a tamper seal on top of the cover/panel.

# 16 Appendix D - PA-3000 Series - FIPS Accessories/Tamper Seal Installation (7 Seals)

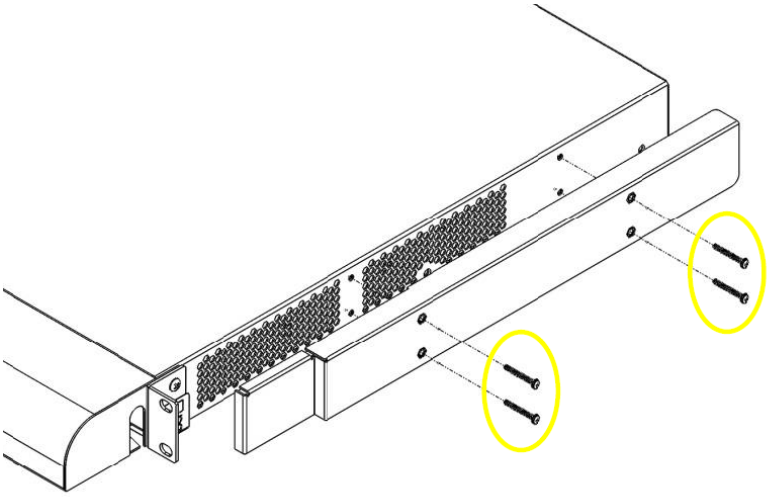
1. Install the front panel with the curve side up and line it up to the left and right side ear mounting holes.



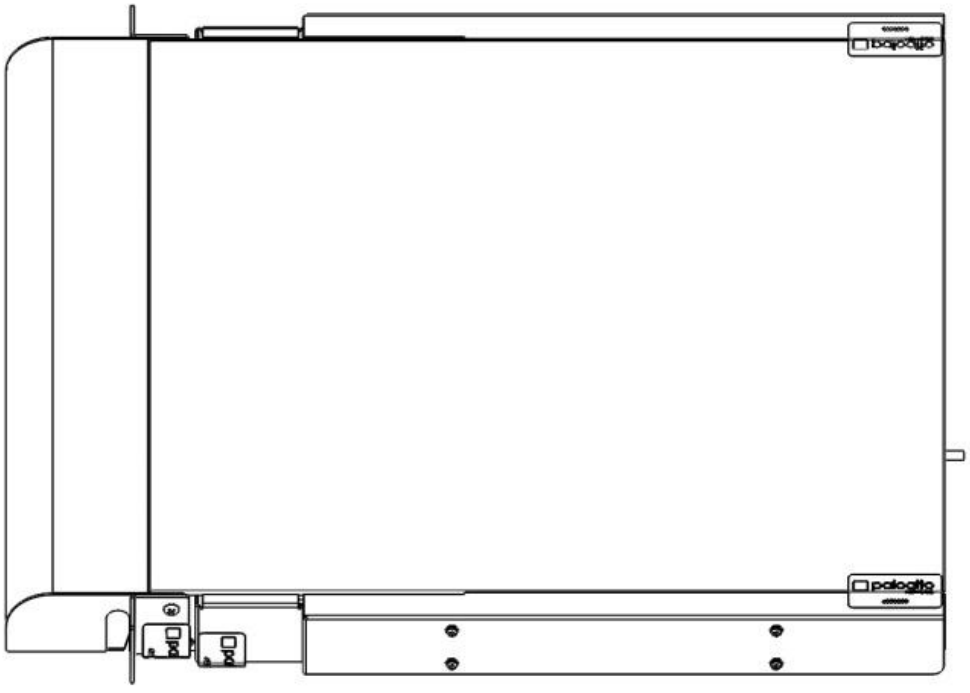
2. Install and secure the right side mounting ear and (2x) 6-32x1/2” screws provided in the kit. Repeat the same step on the left side of the chassis.



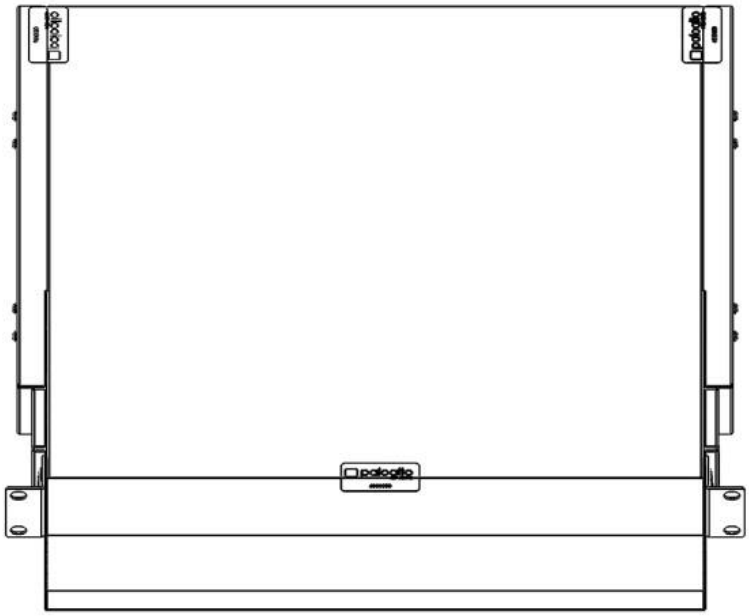
3. Install the right side FIPS plenum and secure with (4x) #6-32x1” SEM screws provided by the kit. Repeat the same steps for the left side.



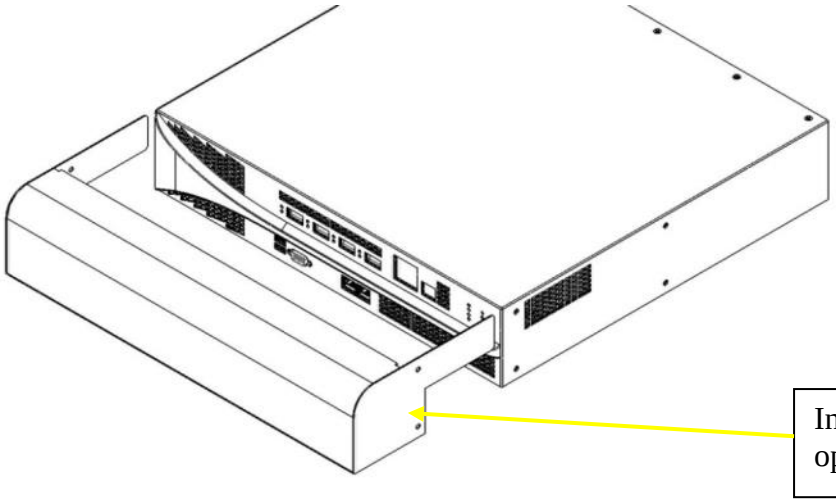
4. Affix a tamper seal to cover the right side bottom ear mounting bracket screw. Repeat the same steps for the left side.
   Affix a tamper seal at right side of the chassis between the top cover and the FIPS plenum. Affix another tamper seal between the bottom of the chassis and the FIPS plenum. Repeat the same steps for the left side.



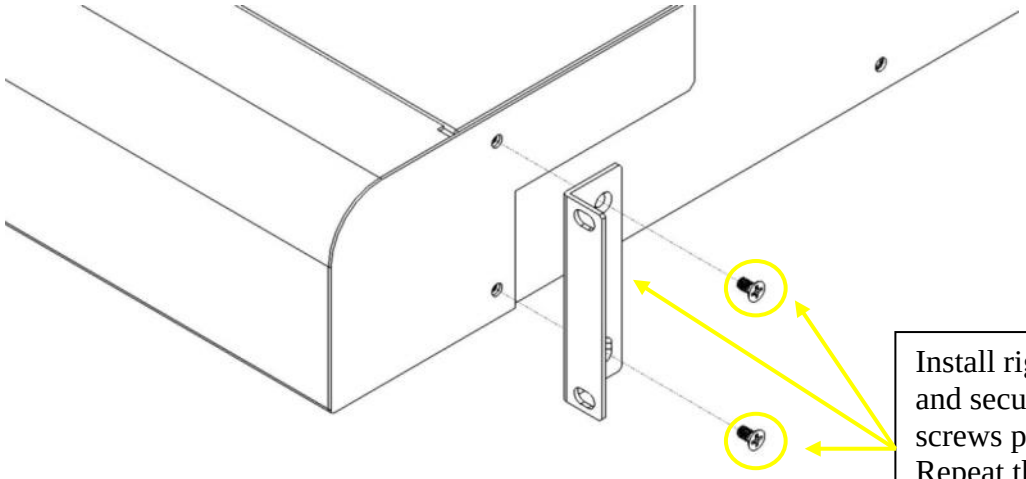
5. Affix a tamper seal on top of the cover / panel.



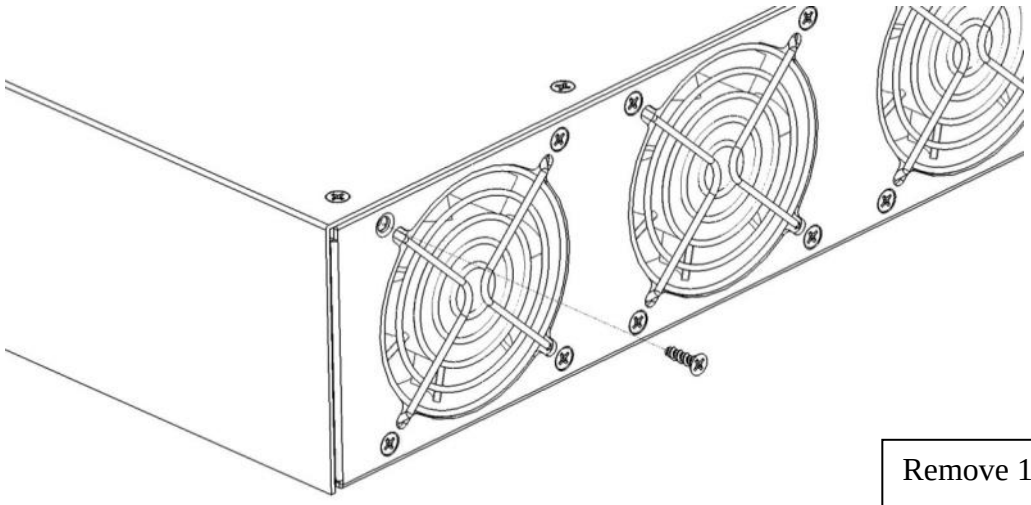
# 17 Appendix E - PA-4000 Series – FIPS Accessories/Tamper Seal Installation (10 Seals)



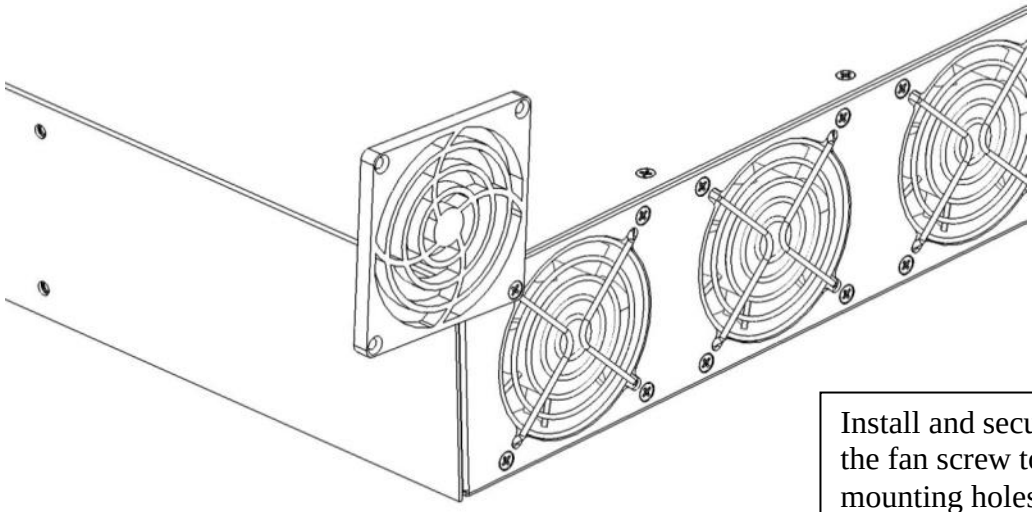
Install the front panel FIPS opacity shield as shown.



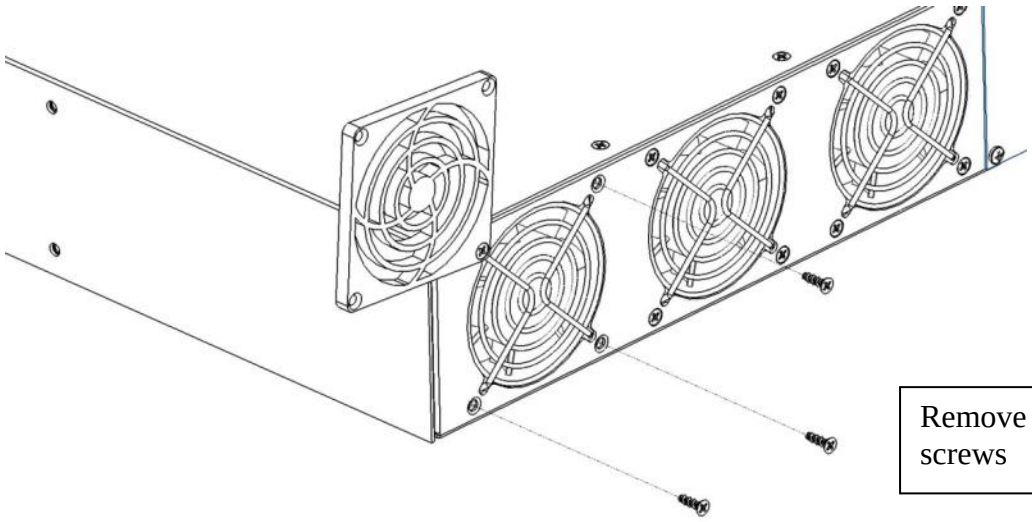
Install right mounting bracket and secure with (2x) 8-32x3/8” screws provided by the kit. Repeat the same steps for the right mounting bracket.



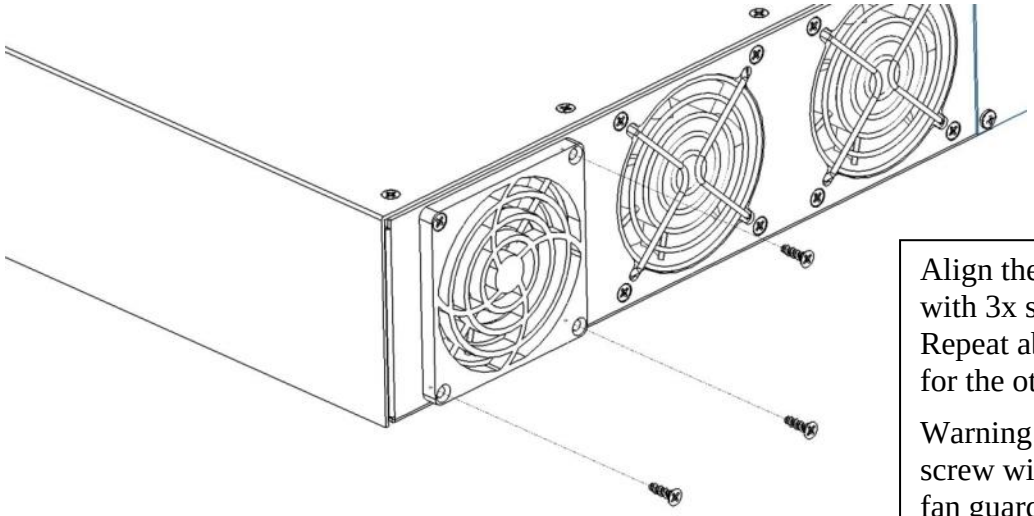
Remove 1x upper-left fan screw.



Install and secure the fan guard with the fan screw to one of the fan guard mounting holes as shown.

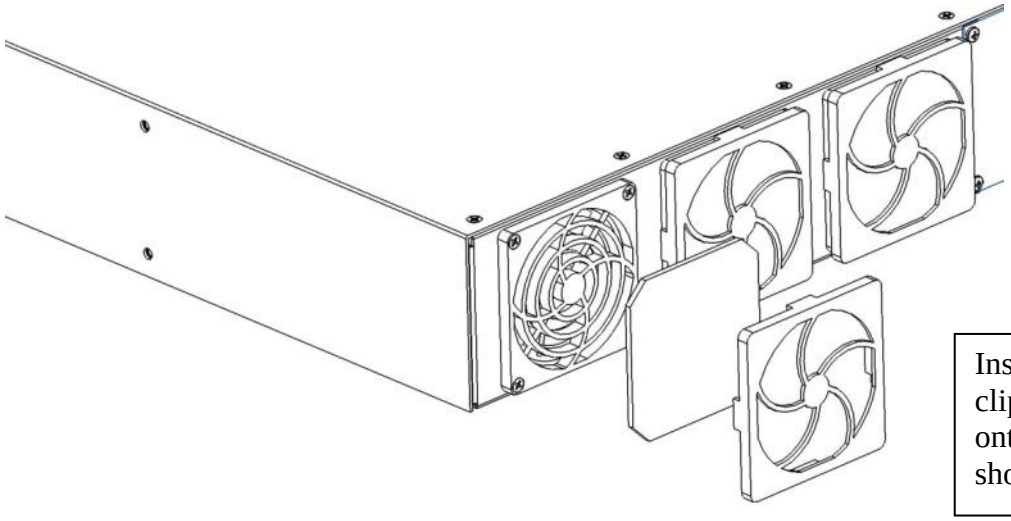


Remove the other 3x fan screws

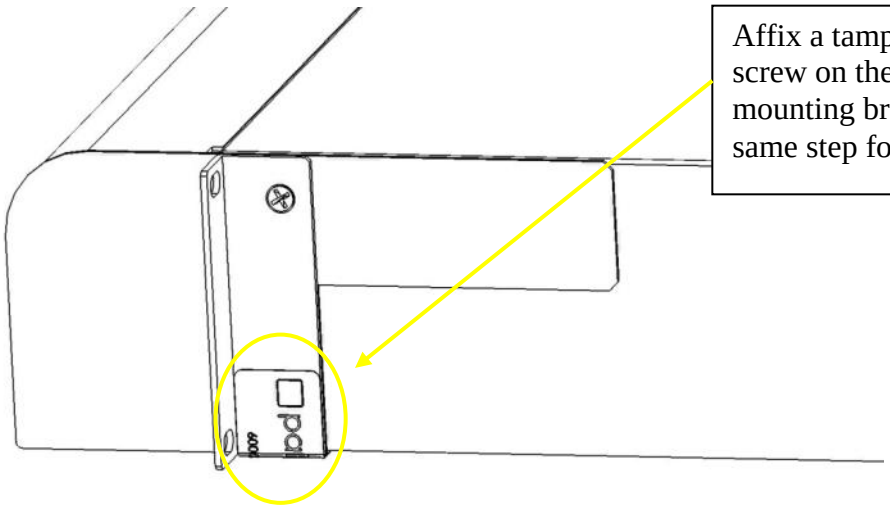


Align the fan guard and secure with 3x screws as shown. Repeat above installation steps for the other fans.

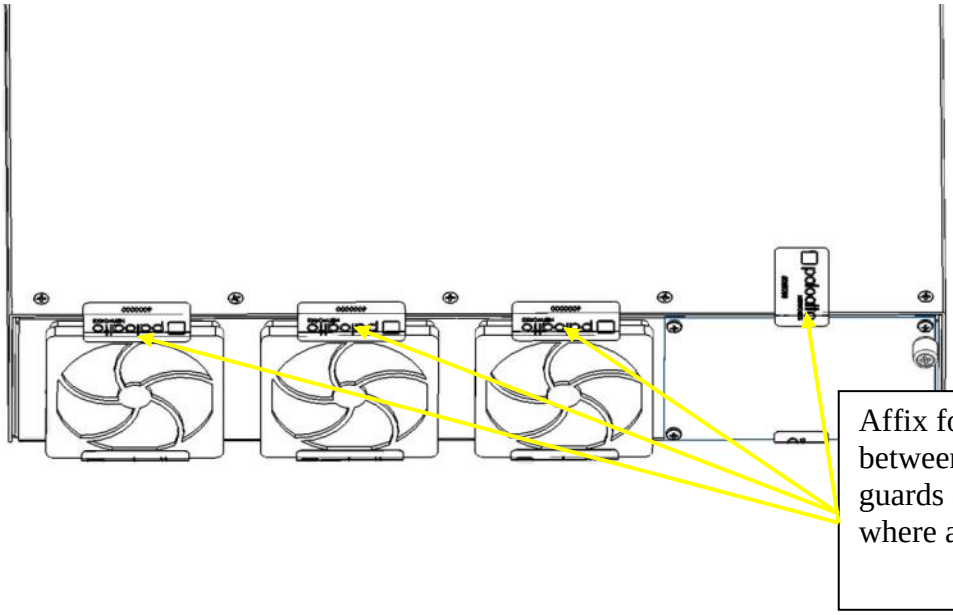
Warning: Over tighten the screw will result cracking the fan guard.



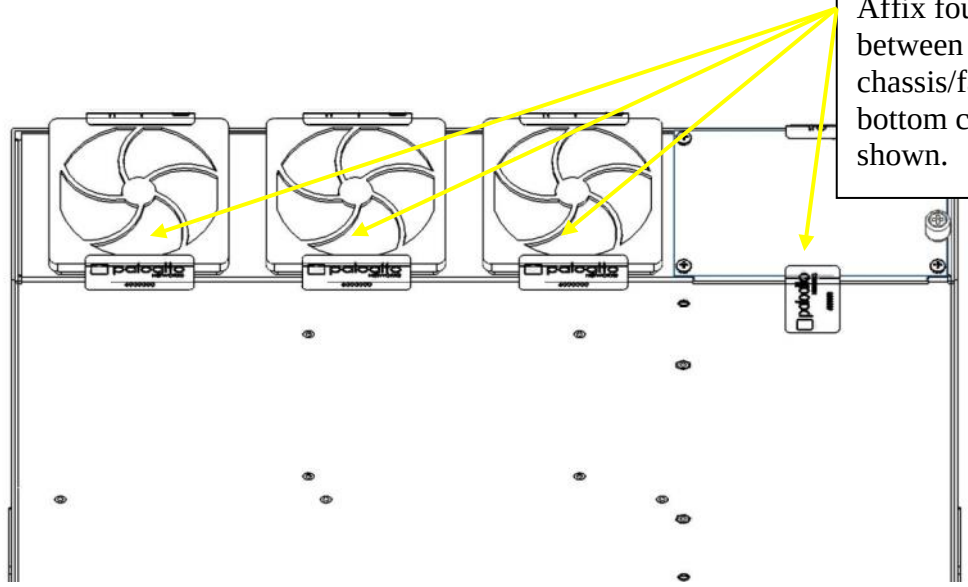
Install the fan filter and clip on the fan guard cover onto the fan guard as shown.



Affix a tamper proof seal over screw on the lower right side mounting bracket. Repeat the same step for left side bracket.



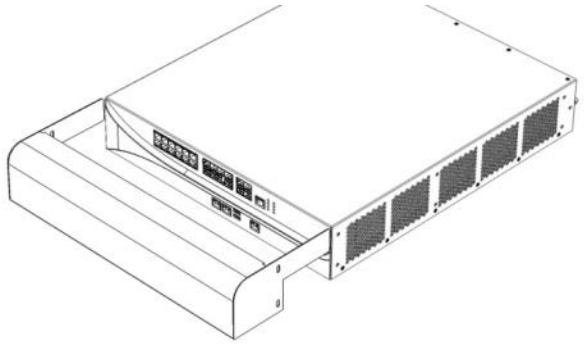
Affix four tamper proof seals between the top cover/fan guards and top cover/PSU where as shown.



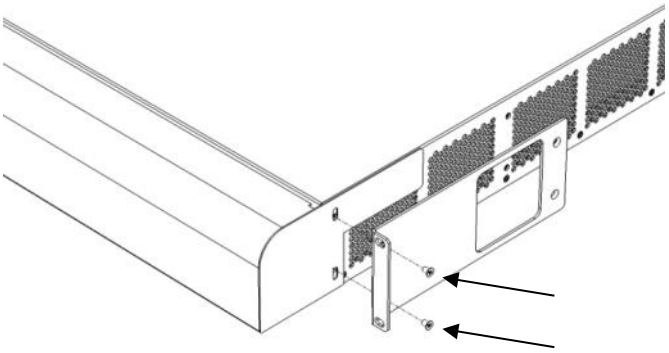
Affix four tamper proof seals between the bottom chassis/fan guards and bottom chassis/PSU where as shown.

# 18 Appendix F - PA-5000 Series - FIPS Accessories/Tamper Seal Installation (17 Seals)

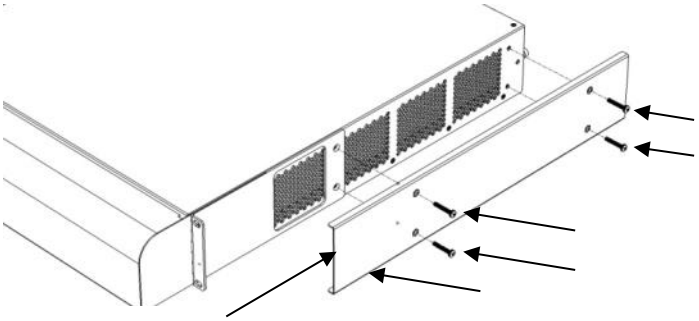
6. Install the front panel.



7. Install the right FIPS mounting bracket and secure with (2x) #8-32x3/8" screws provided in the original accessory kit. Repeat for the left mounting bracket.

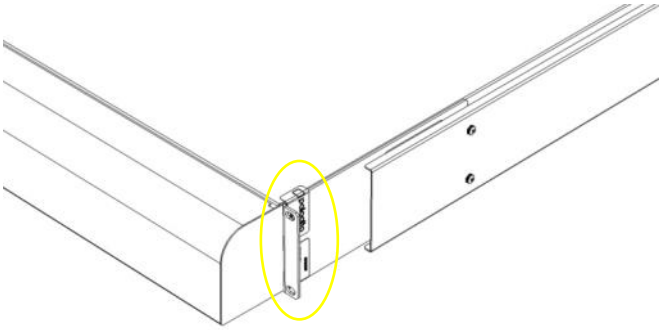


8. Install the side panel on the right side of the chassis and secure with (4x) #8-32x1.00"L screws. Place the leading edge towards front of the chassis. Repeat for the left side of the chassis.

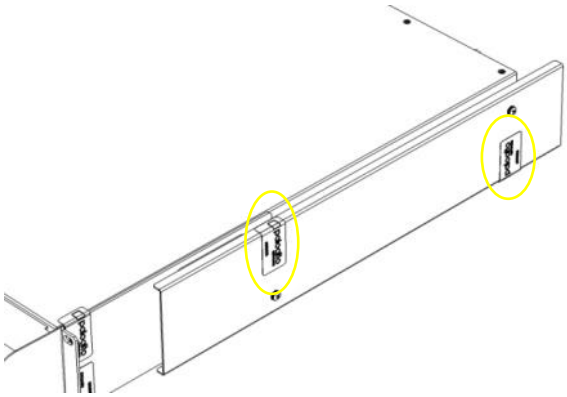


Leading Edge

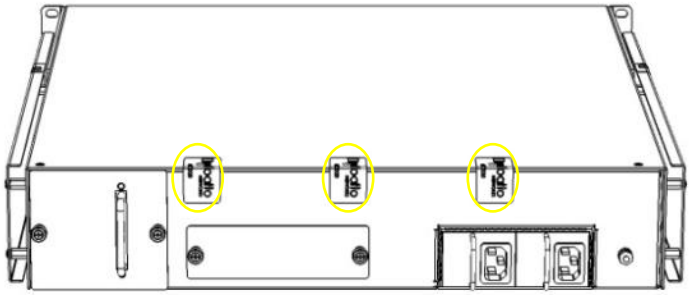
9. Affix two tamper evident labels over both upper and lower screws on the FIPS mounting bracket. Repeat for the left side panel.



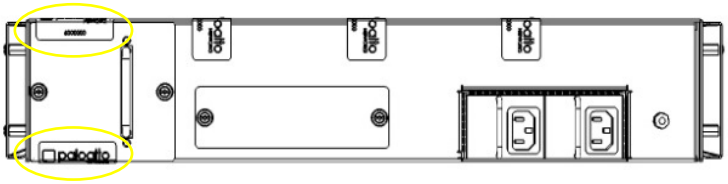
10. Affix two tamper evident labels over front upper and rear lower of the right side panel screws. Repeat for the left side panel.



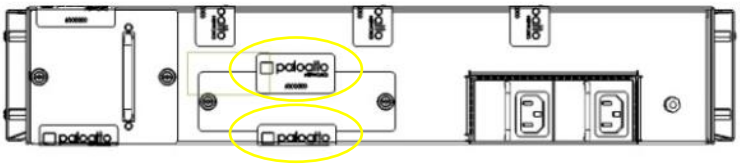
11. Affix three tamper evident labels on the top cover /rear chassis. Ensure the top cover screws are covered by the labels.



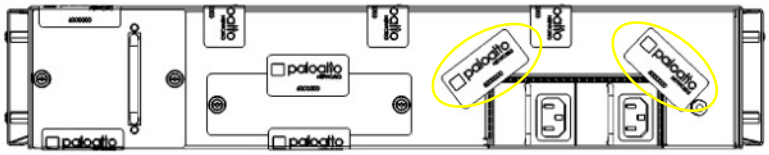
12. Affix a tamper evident label on the top cover/fan access panel.
    Affix another tamper evident label on the bottom chassis/fan access panel.



13. Affix a tamper evident label on upper HDD access panel/rear chassis.
    Affix a tamper evident label on lower HDD access panel/rear chassis.

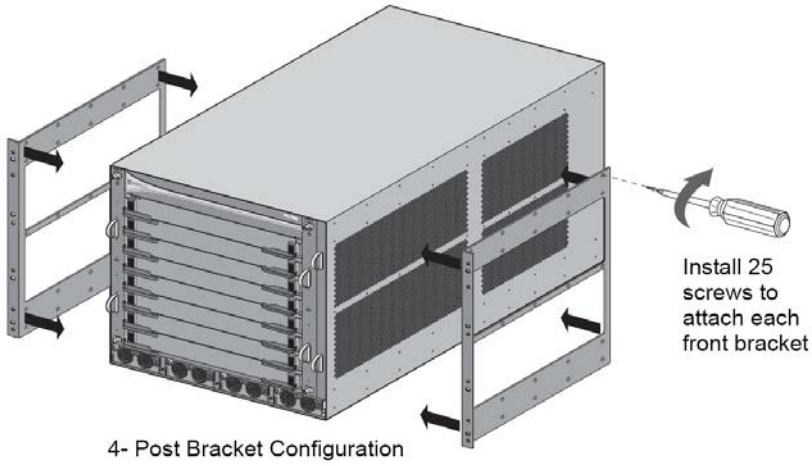


14. Affix a tamper evident label on the upper left PSU/rear chassis.
    Affix a tamper evident label on the upper right PSU/rear chassis.

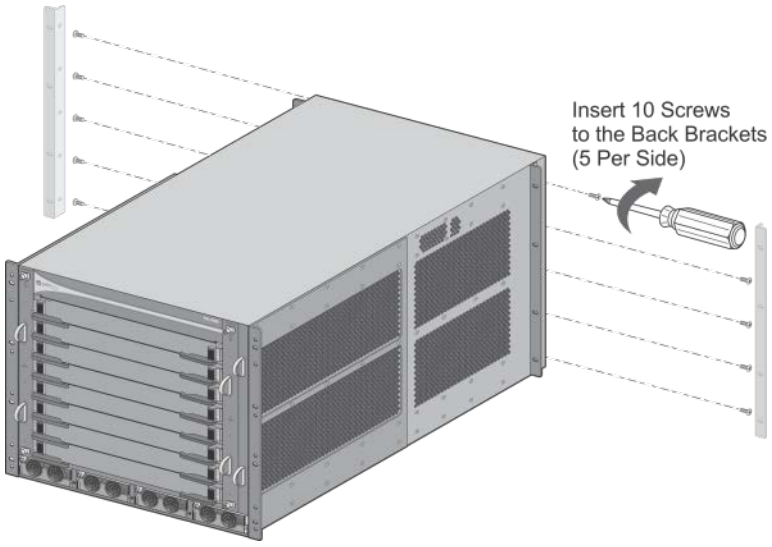


# 19 Appendix G - PA-7050 Series - FIPS Accessories/Tamper Seal Installation (24 Seals)

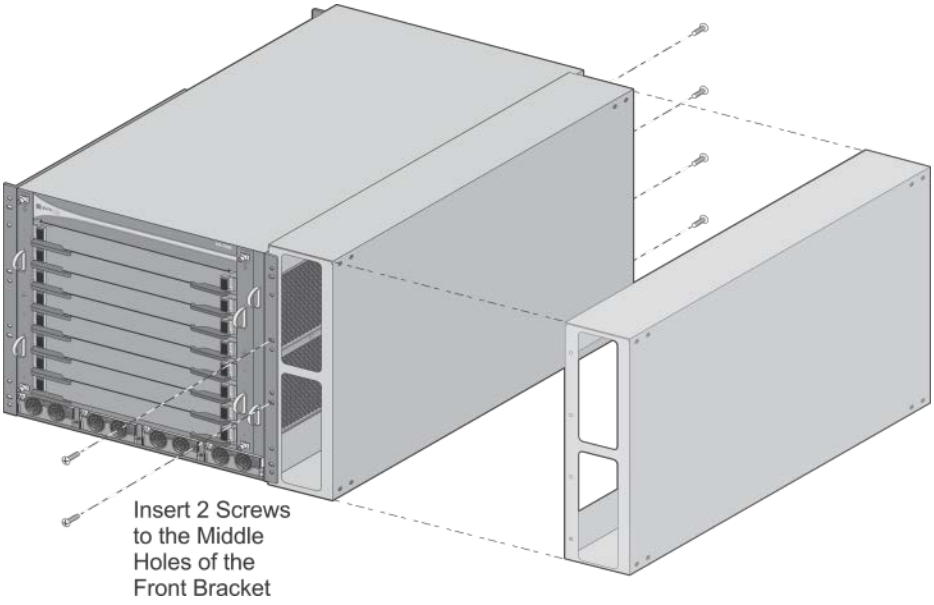
1. Attach front right rack mount brackets in 4-post rack position. Do not attach rear rack mount brackets. Note that brackets are rotated 180 degrees, so the screw holes lineup and the rack mount holes are now on the front of the chassis.



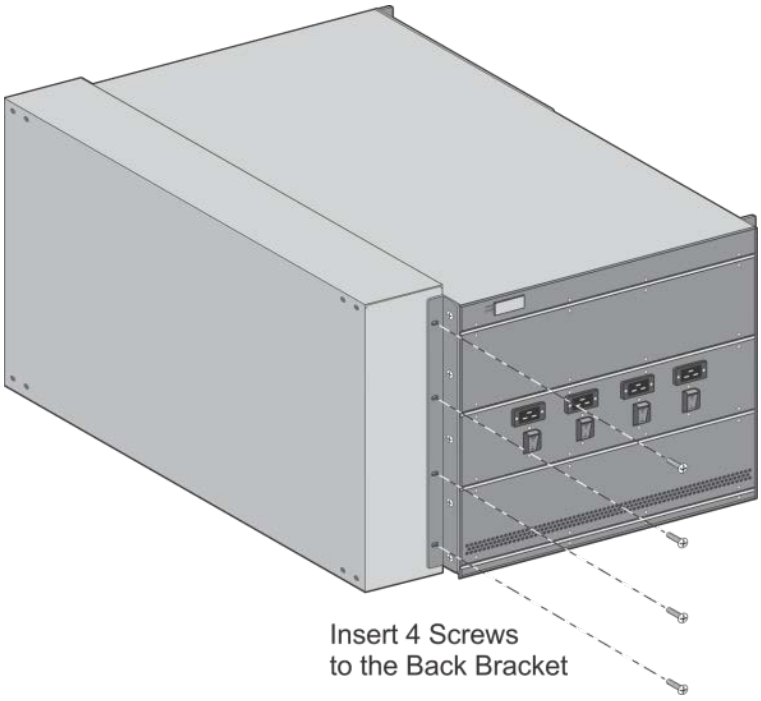

2. Align right plenum bracket with 5 open screw holes. Attach air plenum brackets using 5 of the remaining bracket screws as shown. Repeat for left side.



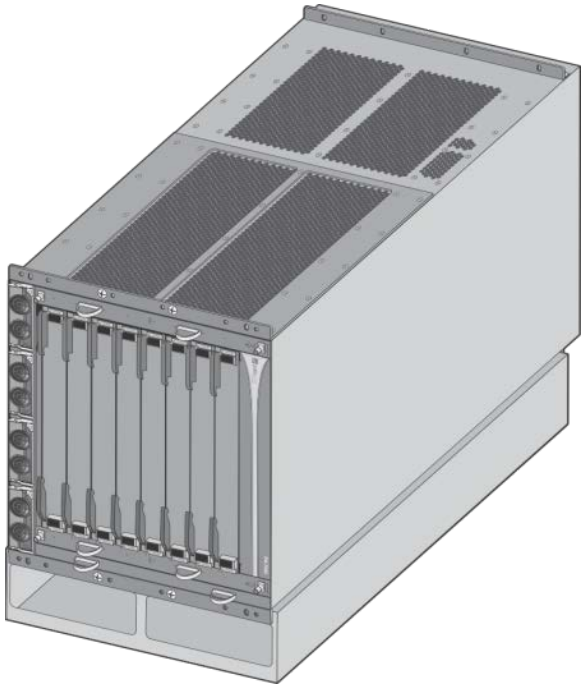
3. Attach bottom plenum to the front right rack mount bracket. Place only the middle two screws.



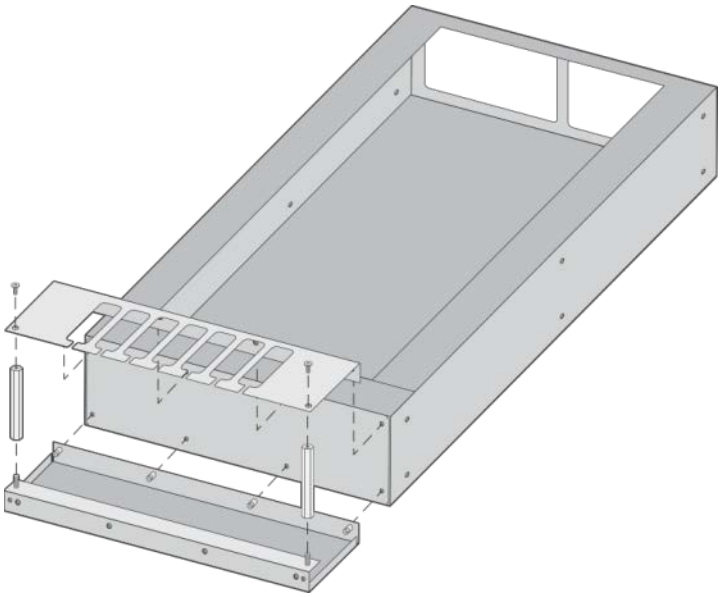

4. Attach the bottom plenum to the rearward right plenum bracket.



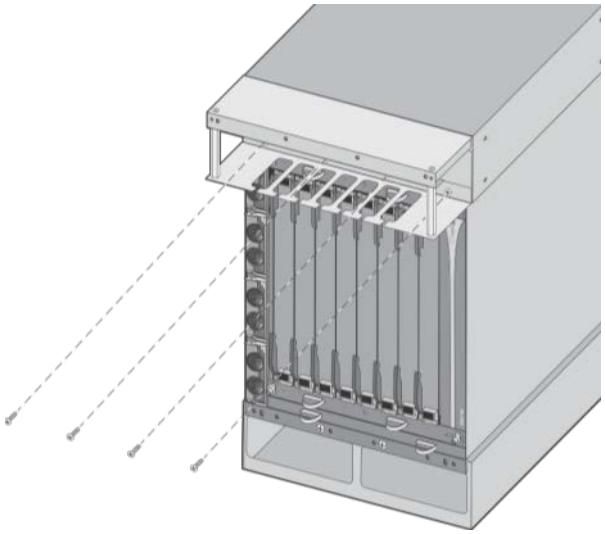
5. Rotate PA-7050 chassis clockwise 90 degrees onto the bottom plenum.



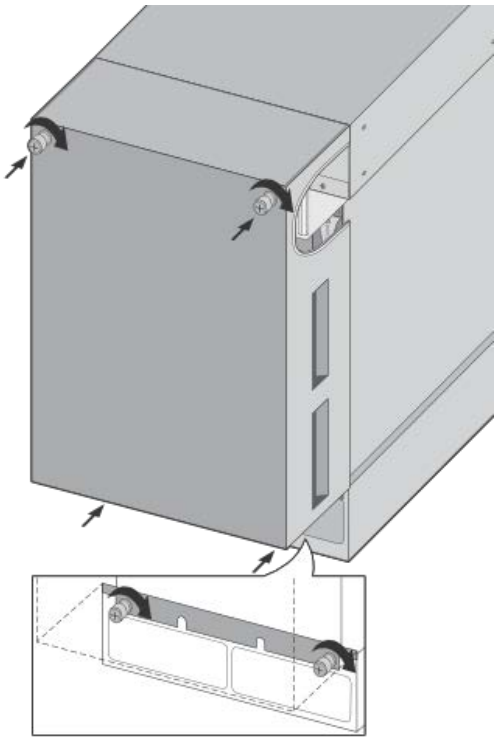
6. Assemble top plenum and cable guide hardware.



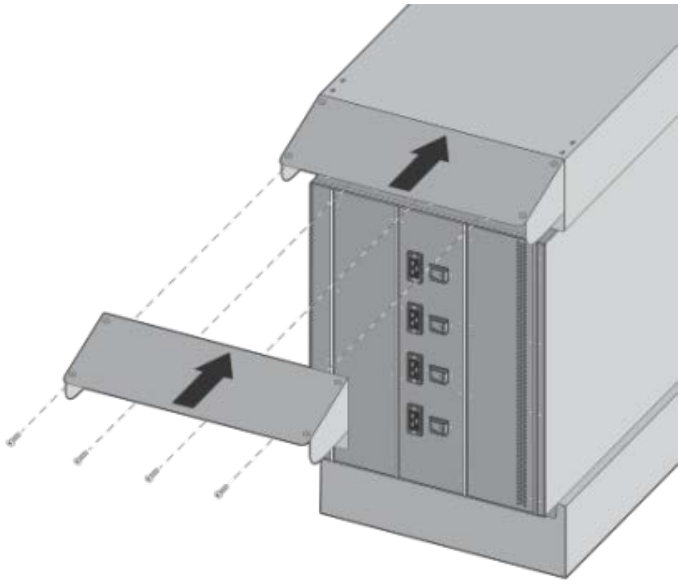
7. Attach top plenum to the front left rack mount bracket



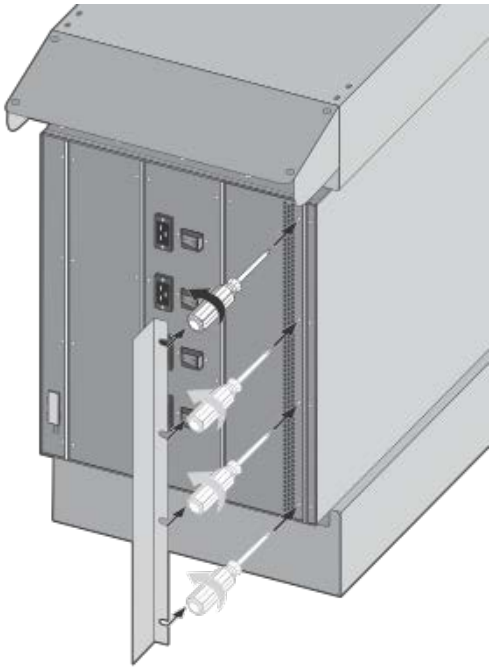
8. Attach front opacity shield using the four captive screws



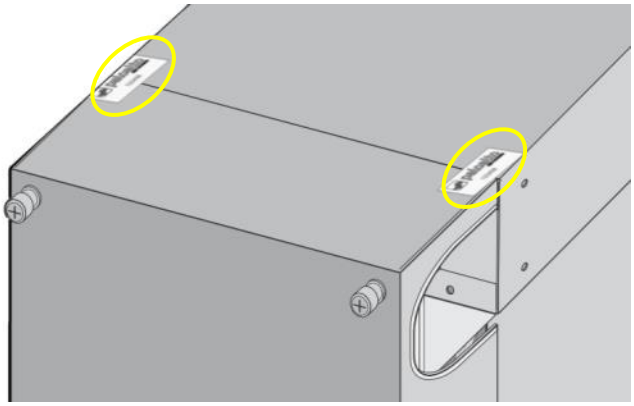
9. Attach top plenum to the rearward left plenum bracket along with plenum's rear opacity shield as shown



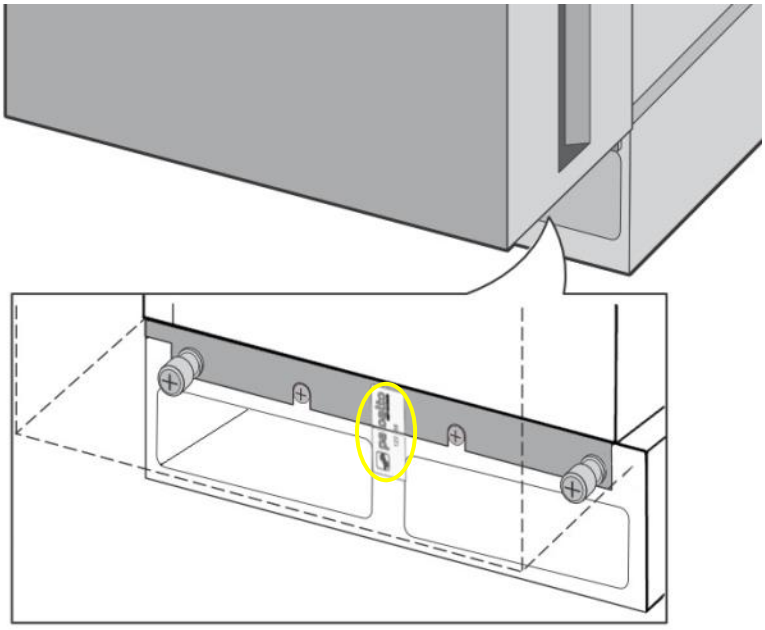
10. Loosen four screws on the panel containing the power supply vent. Insert the power supply vent opacity shield and tighten screws.



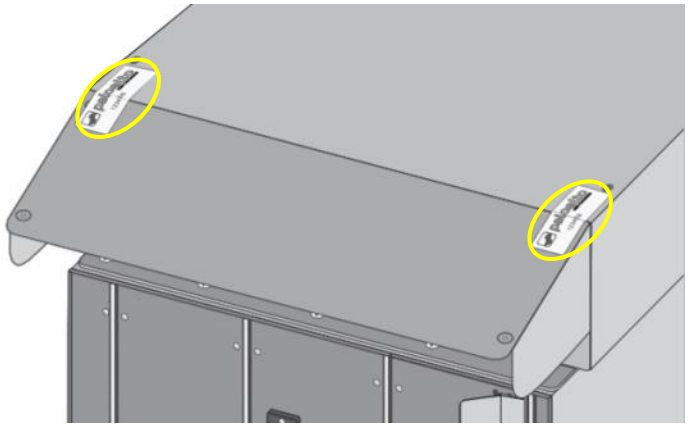
11. Facing the front of the module, affix two (2) labels to top of the front opacity shield, one near left edge and one near the right edge. Ensure the labels, when placed, overlap onto the top of the plenum, as shown. (2 total)



12. Facing the front of the module affix one (1) label centered to the bottom of the front opacity shield to the bottom air plenum, as shown. (1 total)

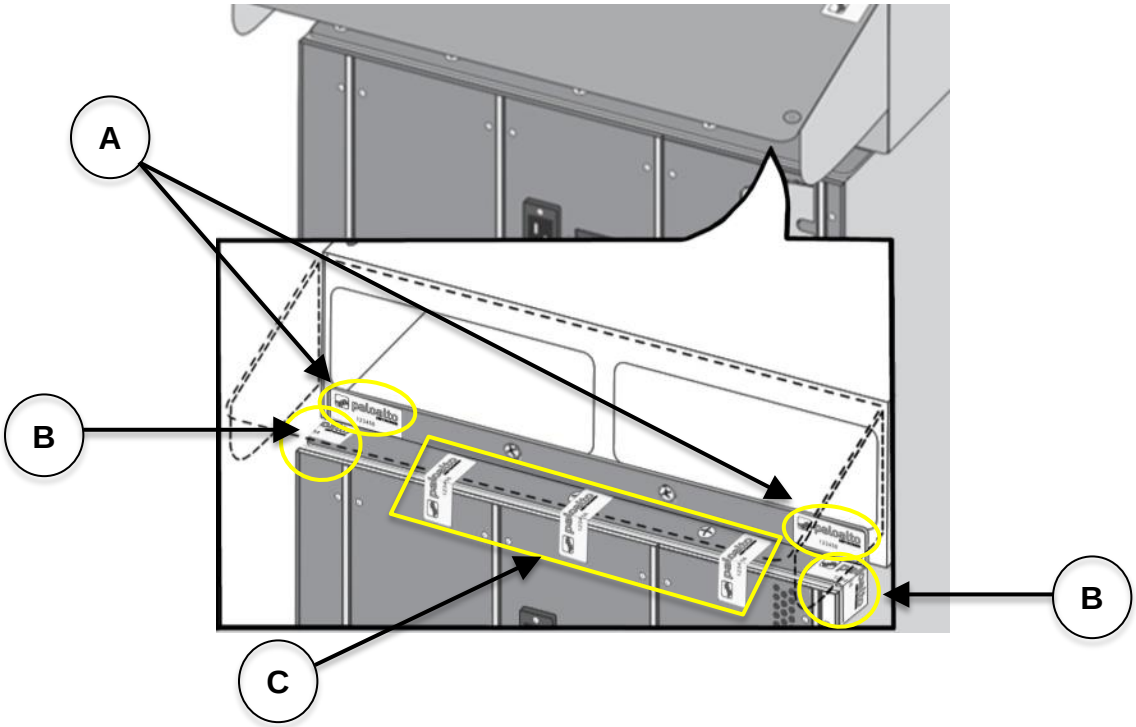


13. Facing the rear of the module, affix two (2) labels to top of the rear opacity shield, one near left edge and one near the right edge. Ensure the labels, when placed, overlap onto the top of the plenum, as shown. (2 total)



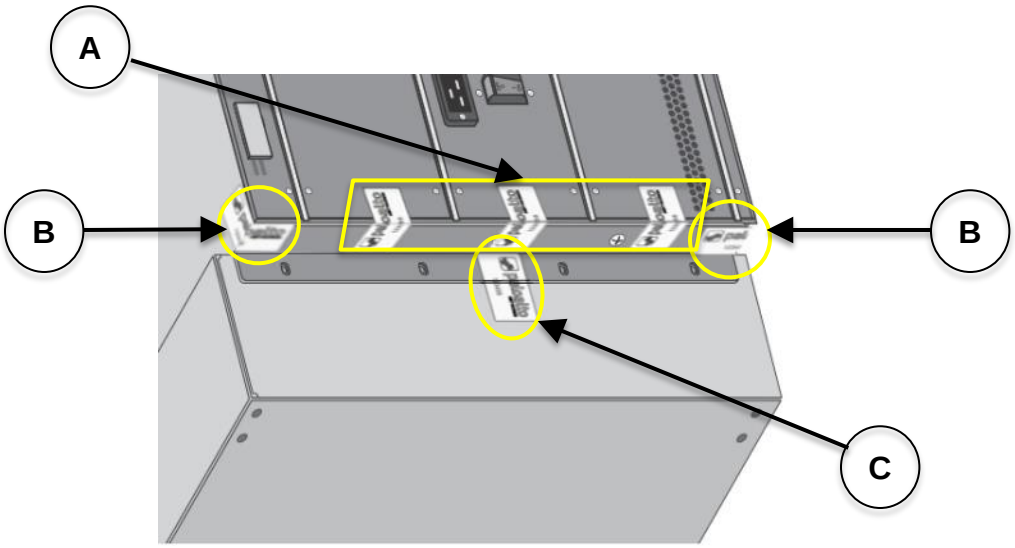
14. Facing the rear of the module;
    A. Affix one (1) label to the top plenum/opacity shield, covering the left and right outermost screws, as shown.
    B. Affix one (1) label to the left and right edge of the top plenum bracket folding over the outer edge of the module, as shown.
    C. Affix one (1) label to the top of each rear panel (3 panels). Ensure that the labels lap onto the top rear plenum brackets, as shown.

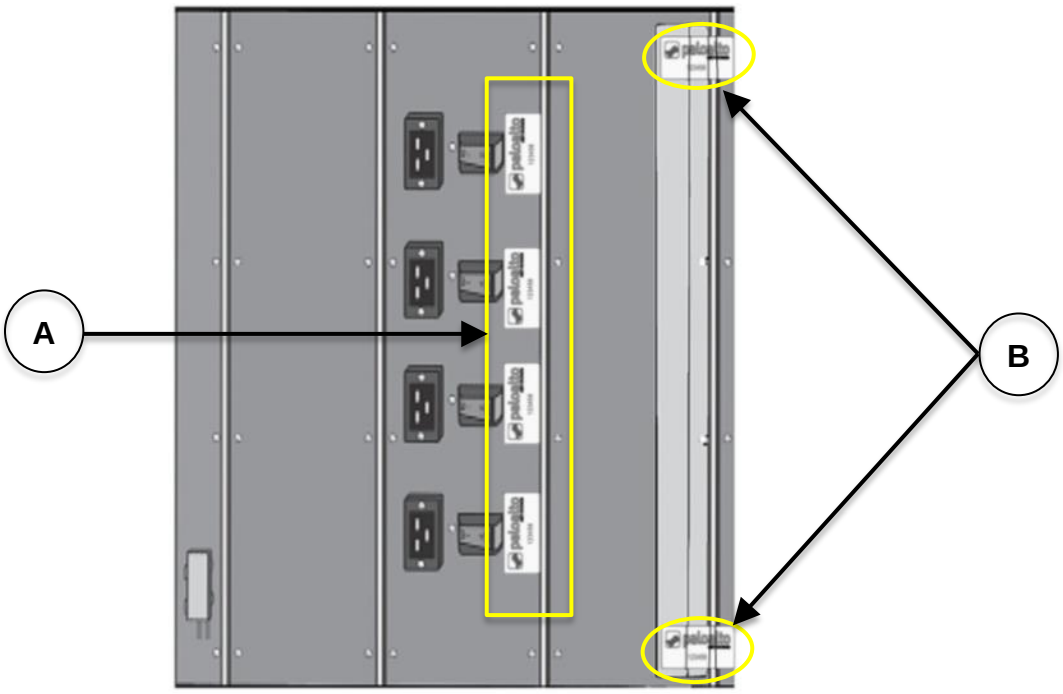
    (7 total)



15. Facing the rear of the module,
    A. Affix one (1) label to the bottom of each rear panel (3 panels). Ensure that the labels laps onto the bottom rear plenum brackets, as shown.
    B. Affix one (1) label to the left and right edge of the bottom plenum bracket folding over the outer edge of the module, as shown.
    C. Affix one (1) label to the bottom plenum's rear side and the bottom plenum rear bracket.

(6 total)



16. Facing the rear of the module;
    A. Affix one (1) label to cover one screw for each power switch, as shown.
    B. Affix one (1) label to the top and bottom of the vent opacity shield, as shown. Please ensure that the captive screw is covered.

    (6 total)