paloalto TECHDOCS

PA-7500 Next-Gen Firewall Hardware Reference

docs.paloaltonetworks.com

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

April 1, 2025

Table of Contents

Before You Begin

Read the following topics before you install or service a Palo Alto Networks® next-generation firewall or appliance.**The following topics apply to all Palo Alto Networks firewalls and appliances except where noted.**

- Upgrade/Downgrade Considerations for Firewalls and Appliances
- Tamper Proof Statement
- Third-Party Component Support
- Product Safety Warnings

Upgrade/Downgrade Considerations for Firewalls and Appliances

The following table lists all hardware features that have upgrade or downgrade impact. Make sure you understand all upgrade/downgrade considerations before you upgrade or downgrade from the specified version of PAN-OS.

Feature	Release	Upgrade Considerations	Downgrade Considerations
PA-7000 Log Forwarding Card (LFC)	10.0	If you are using an LFC with a PA-7000 Series Firewall, when you upgrade to PAN-OS 10.0, you must configure the management plane or dataplane interface for the service route because the LFC ports do not support the requirements for the service route. We recommend using the dataplane interface for the Data Services service route.	n/a
Upgrading a PA-7000 Series Firewall with a first generation switch management card (PA-7050-SMC or PA-7080-SMC)	PAN-OS 8.0 and later	Before upgrading the firewall, run the following CLI command to check the flash drive's status: **`debug system disk-smart-info disk-1`**. If the value for attribute ID #232, **Available_Reservd_Space 0x0000**, is greater than 20, then proceed with the upgrade. If the value is less than 20, then contact support for assistance.	Before downgrading the firewall, run the following CLI command to check the flash drive's status: **`debug system disk-smart-info disk-1`**. If the value for attribute ID #232, **Available_Reservd_Space 0x0000**, is greater than 20, then proceed with the downgrade. If the value is less than 20, then contact support for assistance.

Tamper Proof Statement

To ensure that products purchased from Palo Alto Networks were not tampered with during shipping, verify the following upon receipt of each product:

- The tracking number provided to you electronically when ordering the product matches the tracking number that is physically labeled on the box or crate.
- The integrity of the tamper-proof tape used to seal the box or crate is not compromised.
- The integrity of the warranty label on the firewall or appliance is not compromised.

(PA-7000 Series firewalls only) PA-7000 Series firewalls are modular systems and therefore do not include a warranty label on the firewall.

Third-Party Component Support

Before you consider installing third-party hardware, read the Palo Alto Networks Third-Party Component Support statement.

Product Safety Warnings

To avoid personal injury or death for yourself and others and to avoid damage to your Palo Alto Networks hardware, be sure you understand and prepare for the following warnings before you install or service the hardware. You will also see warning messages throughout the hardware reference where potential hazards exist.

All Palo Alto Networks products with laser-based optical interfaces comply with 21 CFR 1040.10 and 1040.11.

The following safety warnings apply to all Palo Alto Networks firewalls and appliances, unless a specific hardware model is specified.

- When installing or servicing a Palo Alto Networks firewall or appliance hardware component that has exposed circuits, ensure that you wear an electrostatic discharge (ESD) strap. Before handling the component, make sure the metal contact on the wrist strap is touching your skin and that the other end of the strap is connected to earth ground.

  French Translation: Lorsque vous installez ou que vous intervenez sur un composant matériel de pare-feu ou de dispositif Palo Alto Networks qui présente des circuits exposés, veillez à porter un bracelet antistatique. Avant de manipuler le composant, vérifiez que le contact métallique du bracelet antistatique est en contact avec votre peau et que l'autre extrémité du bracelet est raccordée à la terre.
- Use grounded and shielded Ethernet cables (when applicable) to ensure agency compliance with electromagnetic compliance (EMC) regulations.

  French Translation: Des câbles Ethernet blindés reliés à la terre doivent être utilisés pour garantir la conformité de l'organisme aux émissions électromagnétiques (CEM).
- (PA-3200, PA-5200, PA-5400, PA-7000, and PA-7500 firewalls only) At least two people are recommended for unpacking, handling, and relocating the heavier firewalls.
- Do not connect a supply voltage that exceeds the input range of the firewall or appliance. For details on the electrical range, refer to electrical specifications in the hardware reference for your firewall or appliance.

  French Translation: Veillez à ce que la tension d'alimentation ne dépasse pas la plage d'entrée du pare-feu ou du dispositif. Pour plus d'informations sur la mesure électrique, consulter la rubrique des caractéristiques électriques dans la documentation de votre matériel de pare-feu ou votre dispositif.
- (Devices with serviceable batteries only) Do not replace a battery with an incorrect battery type; doing so can cause the replacement battery to explode. Dispose of used batteries according to local regulations.

  French Translation: Ne remplacez pas la batterie par une batterie de type non adapté, cette dernière risquerait d'exploser. Mettez au rebut les batteries usagées conformément aux instructions.
- I/O ports are intended for intra-building connections only and not intended for OSP (Outside Plant) connections or any network connections subject to external voltage surge events.

• 	(All Palo Alto Networks appliances with two or more power supplies) Caution: Shock hazard Disconnect all power cords (AC or DC) from the power inputs to fully de-energize the hardware. **French Translation:** (Tous les appareils Palo Alto Networks avec au moins deux sources d'alimentation) Débranchez tous les cordons d'alimentation (c.a. ou c.c.) des entrées d'alimentation et mettez le matériel hors tension.
• 	(PA-7000 Series firewalls only) Caution: High touch current Connect to earth before connecting to the power supply. Ensure that the protective earthing conductor is connected to the provided ground lug on the rear side of the firewall.
• 	(PA-7000 Series firewalls only) When removing a fan tray from a PA-7000 Series firewall, first pull the fan tray out about 1 inch (2.5cm) and then wait a minimum of 10 seconds before extracting the entire fan tray. This allows the fans to stop spinning and helps you avoid serious injury when removing the fan tray. You can replace a fan tray while the firewall is powered on but you must replace it within 45 seconds and you can only replace one fan tray at a time to prevent the thermal protection circuit from shutting down the firewall. **French Translation:** (Pare-feu PA-7000 uniquement) Lors du retrait d'un tiroir de ventilation d'un pare-feu PA-7000, retirez tout d'abord le tiroir sur 2,5 cm, puis patientez au moins 10 secondes avant de retirer complètement le tiroir de ventilation. Cela permet aux ventilateurs d'arrêter de tourner et permet d'éviter des blessures graves lors du retrait du tiroir. Vous pouvez remplacer un tiroir de ventilation lors de la mise sous tension du pare-feu. Toutefois, vous devez le faire dans les 45 secondes et vous ne pouvez remplacer qu'un tiroir à la fois, sinon le circuit de protection thermique arrêtera le pare-feu.

The following applies only to Palo Alto Networks firewalls that support a direct current (DC) power source:

French Translation: Les instructions suivantes s'appliquent uniquement aux pare-feux de Palo Alto Networks prenant en charge une source d'alimentation en courant continu (c.c.):

- Do not connect or disconnect energized DC wires to the power supply.

  French Translation: Ne raccordez ni débranchez de câbles c.c. sous tension à la source d'alimentation.
- The DC system must be earthed at a single (central) location.

  French Translation: Le système c.c. doit être mis à la terre à un seul emplacement (central).
- The DC supply source must be located within the same premises as the firewall.

  French Translation: La source d'alimentation c.c. doit se trouver dans les mêmes locaux que ce pare-feu.
- The DC battery return wiring on the firewall must be connected as an isolated DC (DC-I) return.

  French Translation: Le câblage de retour de batterie c.c. sur le pare-feu doit être raccordé en tant que retour c.c. isolé (CC-I).
- The firewall must be connected either directly to the DC supply system earthing electrode conductor or to a bonding jumper from an earthing terminal bar or bus to which the DC supply system earthing electrode conductor is connected.

  French Translation: Ce pare-feu doit être branché directement sur le conducteur à électrode de mise à la terre du système d'alimentation c.c. ou sur le connecteur d'une barrette/d'un bus à bornes de mise à la terre auquel le conducteur à électrode de mise à la terre du système d'alimentation c.c. est raccordé.
- The firewall must be in the same immediate area (such as adjacent cabinets) as any other equipment that has a connection between the earthing conductor of the DC supply circuit and the earthing of the DC system.

  French Translation: Le pare-feu doit se trouver dans la même zone immédiate (des armoires adjacentes par exemple) que tout autre équipement doté d'un raccordement entre le conducteur de mise à la terre du même circuit d'alimentation c.c. et la mise à la terre du système c.c.
- Do not disconnect the firewall in the earthed circuit conductor between the DC source and the point of connection of the earthing electrode conductor.

  French Translation: Ne débranchez pas le pare-feu du conducteur du circuit de mise à la terre entre la source d'alimentation c.c. et le point de raccordement du conducteur à électrode de mise à la terre.
- Install all firewalls that use DC power in restricted access areas only. A restricted access area is where access is granted only to craft (service) personnel using a special tool, lock and key, or other means of security, and that is controlled by the authority responsible for the location.

  French Translation: Tous les pare-feux utilisant une alimentation c.c. sont conçus pour être installés dans des zones à accès limité uniquement. Une zone à accès limité correspond à une zone dans laquelle l'accès n'est autorisé au personnel (de service) qu'à l'aide d'un outil spécial,

cadenas ou clé, ou autre dispositif de sécurité, et qui est contrôlée par l'autorité responsable du site.

- Install the firewall DC ground cable only as described in the power connection procedure for the firewall that you are installing. You must use the American wire gauge (AWG) cable specified and torque all nuts to the torque value specified in the installation procedure for your firewall.

  French Translation: Installez le câble de mise à la terre c.c. du pare-feu comme indiqué dans la procédure de raccordement à l'alimentation pour le pare-feu que vous installez. Utilisez le câble American wire gauge (AWG) indiqué et serrez les écrous au couple indiqué dans la procédure d'installation de votre pare-feu pare-feu.

- The firewall permits the connection of the earthed conductor of the DC supply circuit to the earthing conductor at the equipment as described in the installation procedure for your firewall.

  French Translation: Ce pare-feu permet de raccorder le conducteur de mise à la terre du circuit d'alimentation c.c. au conducteur de mise à la terre de l'équipement comme indiqué dans la procédure d'installation du pare-feu.

- A suitably-rated DC mains disconnect device must be provided as part of the building installation.

  French Translation: Un interrupteur d'isolement suffisant doit être fourni pendant l'installation du bâtiment.

PA-7500 Series Firewall Overview

The PA-7500 Series firewalls are high-performance modular firewalls designed for large enterprise environments. These multi-blade chassis leverages either AC or DC power, includes a TPM module for PAN-OS key storage and security, and uses hot-swappable slot cards to allow for expansion as needs grow. There are a total of nine horizontally-oriented slots on the front of the chassis where you can install a Management Processing Card (MPC), multiple Network Processing Cards (NPCs), and multiple Data Processing Cards (DPCs). At least one MPC, NPC, and DPC are required for the firewall to operate. The back of the chassis has two vertically-oriented slots that can accommodate up to two Switch Fabric Cards (SFCs)

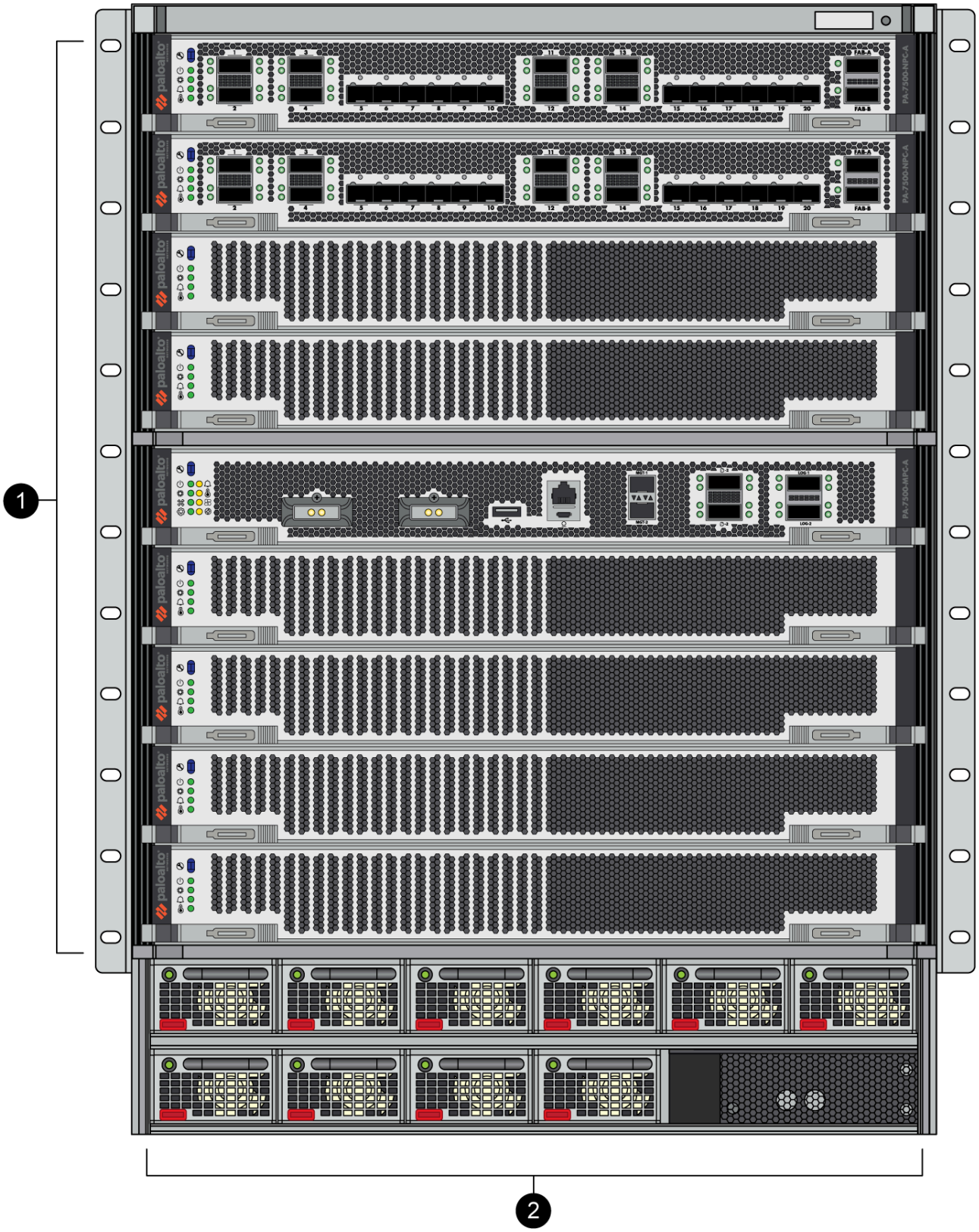
First Supported PAN-OS® Software Release:

- **PAN-OS 11.1**—PA-7500 Firewall
- PA-7500 Series Firewall Front and Back Panel Descriptions
  - PA-7500 Series Front Panel
  - PA-7500 Series Back Panel
- PA-7500 Series Module and Interface Card Descriptions
  - PA-7500 Series Firewall Management Processing Card (MPC)
  - PA-7500 Series Firewall Data Processing Card (DPC)
  - PA-7500 Series Firewall Network Processing Card (NPC)
  - PA-7500 Series Firewall Switch Fabric Card (SFC)

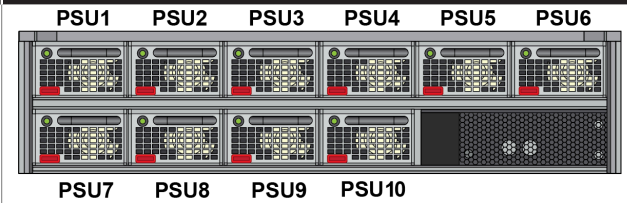
PA-7500 Series Firewall Front and Back Panel Descriptions

PA-7500 Series Front Panel

The following image shows the front panel of the PA-7500 Series firewall and the table describes each front panel component.

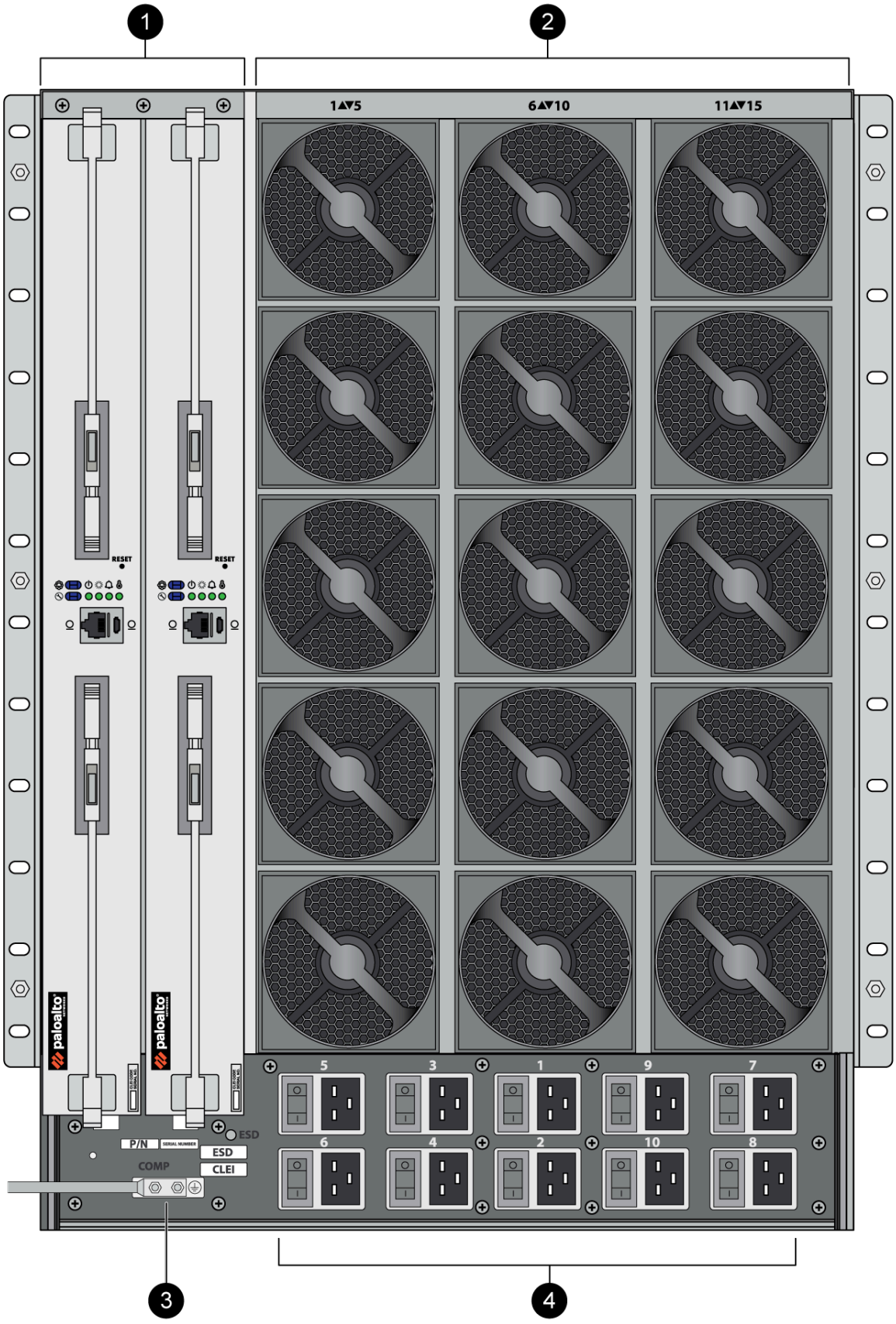


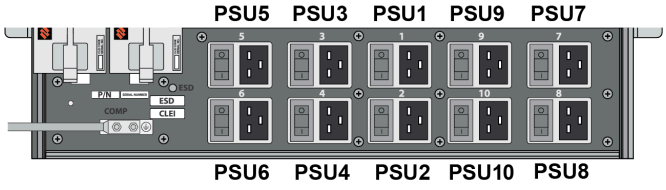
Item	Component	Description
1	Front slot cards	Nine slots that house line cards to provide connectivity, performance, and management functionality to the firewall. From top to bottom, the chassis supports the following card(s) in each slot: • 1—NPC and DPC • 2—NPC and DPC • 3—NPC and DPC • 4—NPC and DPC • 5—MPC (required) • 6—NPC and DPC • 7—NPC and DPC • 8—NPC and DPC • 9—NPC and DPC View the PA-7500 Series Module and Interface Card Descriptions for more information on the slot cards and their components.
2	Power supplies	Ten power supply slots that provide AC or DC power to the chassis. A chassis with low line input voltage (90V, 110/120V, 132V) requires a minimum of eight power supplies while a chassis with high line input voltage (180V, 200/240V, 305V) requires a minimum of four power supplies. *The minimum number of power supplies (four for high line and eight for low line) are not enough to establish full power redundancy in a fully loaded chassis.* *To provide full redundancy using high line power supplies, you must install eight power supplies. A fully redundant power configuration means that half of the installed power supplies can fail and the appliance and all installed line cards still function.* On the front panel of the chassis, the power supplies are numbered as follows:

Item	Component	Description
		 For more information on connecting power to the firewall, see Connect Power to the PA-7500 Series Firewall.

PA-7500 Series Back Panel

The following image shows the back panel of the PA-7500 Series firewall and the table describes each back panel component.



Item	Component	Description
1	Back slot cards	Two slots that house Switch Fabric Cards (SFCs). One SFC must be installed while a second SFC can be installed for redundancy. View the PA-7500 Series Module and Interface Card Descriptions for more information on the slot cards and their components.
2	Fan assemblies	Up to fifteen fan assemblies that provide the appliance with cooling and ventilation. The dual-rotor fan assemblies can be individually replaced.
3	Ground stud	Two-post stud used to ground the appliance to earth ground. Use the provided ground lug to connect a grounded cable to the two-post stud.
4	Power supplies	Ten power supply slots that provide AC or DC power to the chassis. A chassis with low line input voltage (90V, 110/120V, 132V) requires a minimum of eight power supplies while a chassis with high line input voltage (180V, 200/240V, 305V) requires a minimum of four power supplies. *The minimum number of power supplies (four for high line and eight for low line) are not enough to establish full power redundancy in a fully loaded chassis.* *To provide full redundancy using high line power supplies, you must install eight power supplies. A fully redundant power configuration means that half of the installed power supplies can fail and the appliance and all installed line cards still function.* On the back panel of the chassis, the power supplies are numbered as follows:  For more information on connecting power to the firewall, see Connect Power to the PA-7500 Series Firewall.

PA-7500 Series Module and Interface Card Descriptions

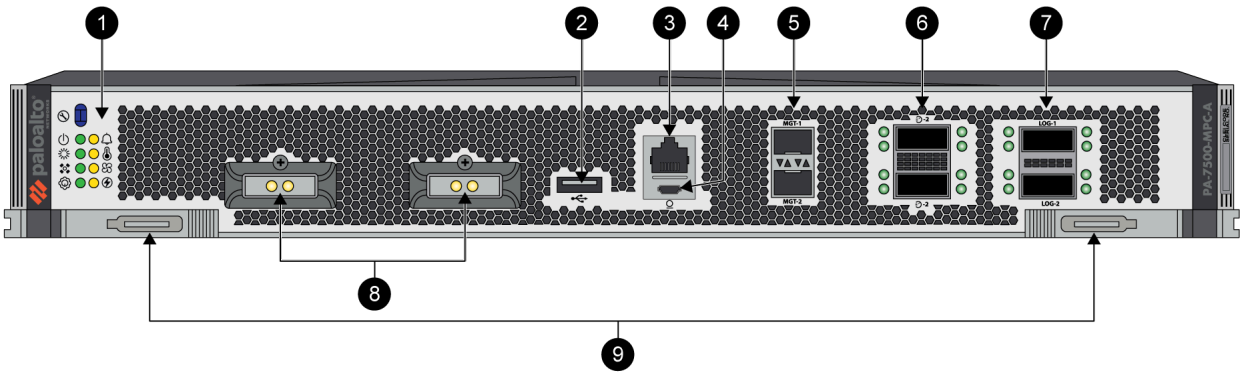
The following topics list the components and features of each PA-7500 Series firewall interface card.

- PA-7500 Series Firewall Management Processing Card (MPC)
- PA-7500 Series Firewall Network Processing Card (NPC)
- PA-7500 Series Firewall Data Processing Card (DPC)
- PA-7500 Series Firewall Switch Fabric Card (SFC)

PA-7500 Series Firewall Management Processing Card (MPC)

The Management Processing Card (MPC) provides the firewall with a management interface, first packet processing, logging interfaces, and inter-chassis HSCI ports. The MPC must be installed in slot 5 of the chassis.

The following image shows the PA-7500 MPC and the table below describes each labeled component.



Item	Component	Description
1	LED Indicators	Eight LEDs that indicate the status of various hardware components. For details on the LEDs, see Interpret the PA-7500 Series Firewall Interface Card LEDs
2	USB Port	One USB port that accepts a USB flash drive that contains a bootstrap bundle (PAN-OS configuration) that enables you to bootstrap the firewall. Bootstrapping enables you to provision the firewall with a specific configuration, license it, and make it operational on the network.
3	RJ-45 Console Port	Use the RJ-45 console port to connect a management computer to the firewall using a 9-pin serial-to-RJ-45 cable and terminal emulation software. The console port has a baud rate of 115,200 8-N-1.

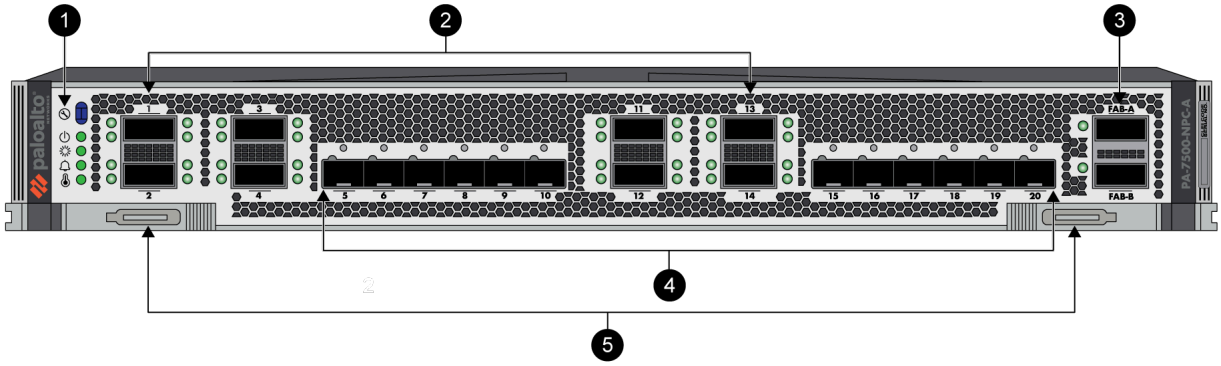
Item	Component	Description
		The console connection provides access to firewall boot messages, the Maintenance Recovery Tool (MRT), and the command line interface (CLI).
4	Micro USB Console Port	Use the Micro USB console port to connect a management computer to the firewall using a standard Type-A USB-to-micro USB cable and terminal emulation software. The console port has a baud rate of 115,200 8-N-1. The console connection provides access to firewall boot messages, the Maintenance Recovery Tool (MRT), and the command line interface (CLI).
5	Management Ports	Two SFP/SFP+/SFP28 management ports providing 1Gbps/10Gbps/25Gbps connectivity that are used to access the management interface. MGT-1 and MGT-2 are bundled by default as a single logical interface called **bond0**. The two bonded ports provide redundancy, which enables the management interface to remain active if one interface goes down. To manage the firewall, change your management computer IP address to 192.168.1.2, connect an SFP+ cable from your computer to one of the MGT ports and browse to https:// 192.168.1.1. The default login name is admin and the default password is admin.
6	HSCI-A and HSCI-B (High Speed Chassis Interconnect) Ports	QSFP-DD interfaces used to connect two PA-7500 Series firewalls in a NGFW clustering configuration. Each port offers 100Gbps or 400Gbps connectivity and is used to maintain a dual active data plane with a single active control plane. In a typical installation, HSCI-A on the first firewall connects directly to HSCI-A on the second firewall and HSCI-B on the first firewall connects to HSCI-B on the second firewall. The purpose of HSCI-B is to provide redundancy. *The lower port, HSCI-B, may be harder to access if HSCI-A has an installed optic.*
7	Logging Ports	Two QSFP28 logging ports that offer 40Gbps or 100Gbps connectivity and are used as log interfaces. If both ports are up, LOG-1 becomes the active interface and LOG-2 becomes the standby interface.

Item	Component	Description
		You must Configure Log Forwarding to forward logs from the log interface to one or more log collectors. If the log interface is not configured, the management interface is used to forward logs instead.
8	Logging Drive Covers	Secure the two logging drives in the MPC. By default, the MPC does not have a logging drive installed. For information about installing a logging drive, see Replace a PA-7500 Series Firewall Logging Drive.
9	Ejector Tabs	Push tabs that are used to insert or replace the interface card.

PA-7500 Series Firewall Network Processing Card (NPC)

The Network Processing Card (NPC) provides the firewall with network connectivity. An NPC can be installed in slots 1, 2, 3, 4, 6, 7, 8, and 9.

The following image shows the PA-7500 NPC and the table below describes each labeled component.



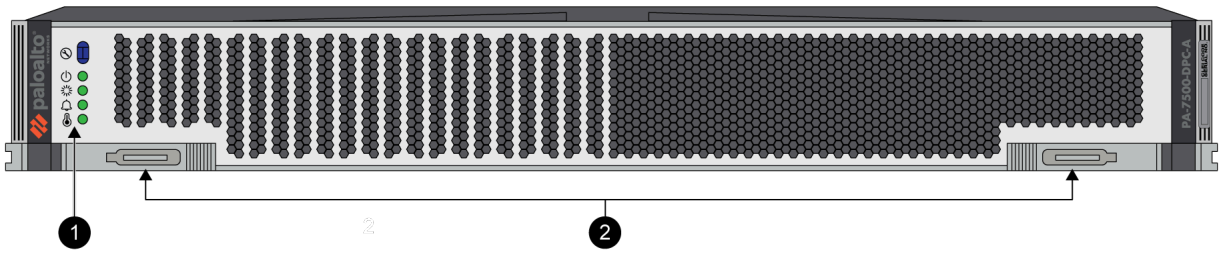
Item	Component	Description
1	LED Indicators	Five LEDs that indicate the status of various hardware components. For details on the LEDs, see Interpret the PA-7500 Series Firewall Interface Card LEDs.
2	QSFP-DD Ports	Eight form-factor pluggable QSFP-DD Ethernet ports that support 400Gbps, 100Gbps (QSFP28), and 40Gbps (QSFP+) connectivity depending on the optics installed. Each interface also supports breakout mode to create four 100Gbps, 25Gbps, or 10Gbps ports each depending on the optics installed. The ports are broken out as follows:

Item	Component	Description
		• Port 1 — Ports 21, 22, 23, and 24 • Port 2 — Ports 25, 26, 27, and 28 • Port 3 — Ports 29, 30, 31, and 32 • Port 4 — Ports 33, 34, 35, and 36 • Port 11 — Ports 37, 38, 39, and 40 • Port 12 — Ports 41, 42, 43, and 44 • Port 13 — Ports 45, 46, 47, and 48 • Port 14 — Ports 49, 50, 51, and 52 *The lower row of ports may be harder to access if the port above it has an installed optic.*
3	Fabric Ports	Two fabric ports that are currently unusable and reserved for a future release.
4	SFP-DD Ports	Twelve 10Gbps/25Gbps/100Gbps SFP-DD ports that support SFP28, SFP+, and SFP optics.
5	Ejector Tabs	Push tabs that are used to insert or replace the interface card.

PA-7500 Series Firewall Data Processing Card (DPC)

The Data Processing Card (DPC) provides the firewall with additional processing power and capacity. A DPC can be installed in slots 1, 2, 3, 4, 6, 7, 8, and 9.

The following image shows the PA-7500 DPC and the table below describes each labeled component.



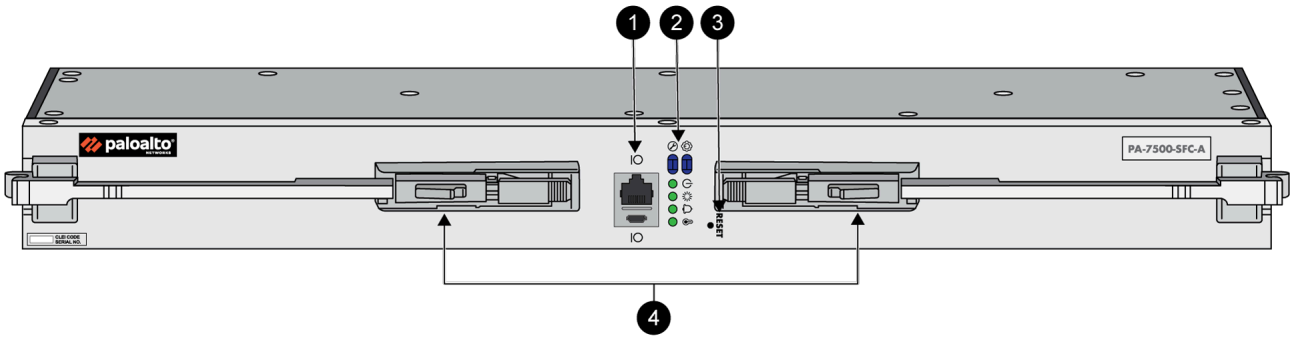
Item	Component	Description
1	LED Indicators	Four LEDs that indicate the status of various hardware components. For details on the LEDs, see Interpret the PA-7500 Series Firewall LEDs.

Item	Component	Description
2	Ejector Tabs	Push tabs that are used to insert or replace the interface card.

PA-7500 Series Firewall Switch Fabric Card (SFC)

The Switch Fabric Card (SFC) provides data plane connectivity to the other interface cards. It also acts like a control plane processor for the chassis. An SFC can be installed in one or both of the two back slots of the chassis. The second SFC is used for redundancy.

The following image shows the PA-7500 SFC and the table below describes each labeled component.



Item	Component	Description
1	RJ-45 and Micro USB Console Ports	**RJ-45 Console Port** Use the console port to connect a management computer to the firewall using a 9-pin serial-to-RJ-45 cable and terminal emulation software. **Micro USB Console Port** Use the console port to connect a management computer to the firewall using a standard Type-A USB-to-micro USB cable and terminal emulation software. The console connection provides access to firewall boot messages, the Maintenance Recovery Tool (MRT), and the SFC Debug Mode tool.
2	LED Indicators	Four LEDs that indicate the status of various hardware components. For details on the LEDs, see Interpret the PA-7500 Series Firewall LEDs.
3	Reset Button	A small button that, with the help of a pin, can be used to reset the SFC and its associated front slot cards.

Item	Component	Description
4	Ejector Handles	Handles that are used to insert or replace the interface card.

PA-7500 Series Firewall Installation

The PA-7500 Series firewall is a modular system that requires you to install several components, such as interface cards, during the installation process. Due to the weight of the firewall, we recommend that you first install the firewall appliance into the rack and then install the interface cards. After the firewall is installed in the rack (with all components installed), connect power, verify that the interface cards are functioning, and then connect the network and management cables.

The PA-7500 Series firewalls ship with racking equipment and cables that enable you to install the firewall in your deployment environment.

- Install the PA-7500 Series Firewall in an Equipment Rack
- Install a PA-7500 Series Firewall Interface Card
- Connect Power to the PA-7500 Series Firewall
  - Determine Power Requirements of the PA-7500 Series Firewalls
  - Connect AC Power to the PA-7500 Series Firewall
  - Connect DC Power to the PA-7500 Series Firewall
  - View Power Statistics of the PA-7500 Series Firewalls
- Connect Cables to the PA-7500 Series Firewall

Install the PA-7500 Series Firewall in an Equipment Rack

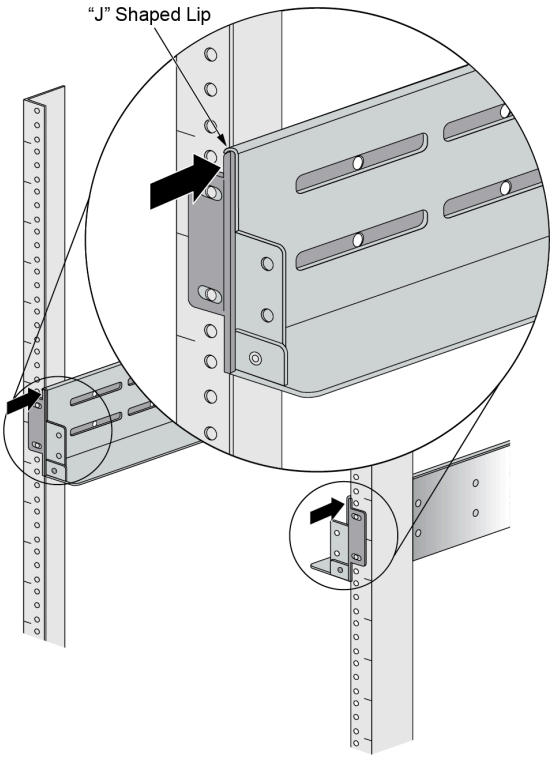
The following procedure describes how to install the PA-7500 Series firewall in an equipment rack.

The PA-7500 chassis and the interface cards (MPC, NPC, DPC, and SFC) ship in separate boxes and it is recommended that you install the cards after you rack-mount the appliance. This will prevent any damage to the cards that could occur during rack mounting and will reduce the weight of the appliance. To further reduce the weight, remove the fan assemblies and power supplies. The PA-7500 requires 14 RU (rack units) of rack space. Unless specified, screws are not provided.

Read the following safety information before you proceed:

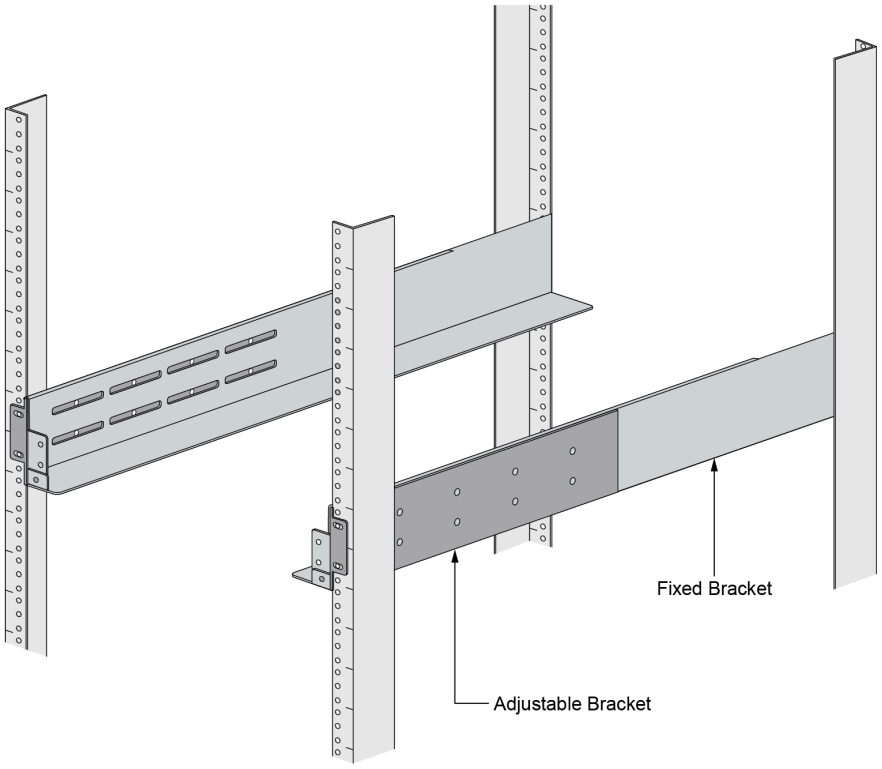
- Elevated ambient operating temperature—If the PA-7500 Series firewall is installed in a closed or multi-unit rack assembly, the ambient operating temperature of the rack environment may be greater than the ambient room temperature. Verify that the ambient temperature of the rack assembly does not exceed the maximum rated ambient temperature requirements listed in PA-7500 Series Firewall Environmental Specifications.
- Reduced airflow—Ensure that the airflow required for safe operation is not compromised by the rack installation.
- Mechanical loading—Ensure that the rack-mounted firewall does not cause hazardous conditions due to uneven mechanical loading.
- Circuit overloading—Ensure that the circuit that supplies power to the firewall is sufficiently rated to avoid circuit overloading or excess load on supply wiring. See PA-7500 Series Firewall Electrical Specifications.
- Reliable earthing—Maintain reliable earthing of rack-mounted equipment. Pay special attention to power connections other than direct connections to the branch circuit (such as use of power strips or extension cords) to ensure that the firewall does not exceed power ratings for connected hardware.

STEP 1 | Slide one of the adjustable mounting brackets into the “J” shaped lip on the top edge of one of the fixed mounting brackets. Repeat with the second adjustable and fixed mounting brackets.



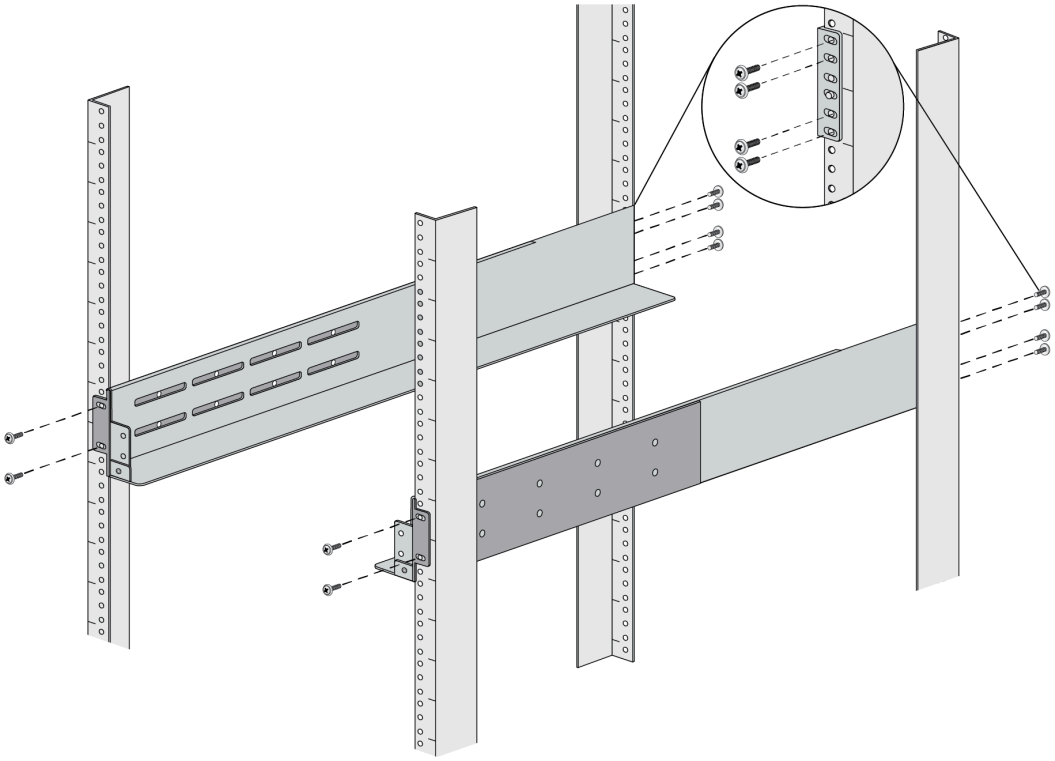
STEP 2 | Position the bottom edges of the fixed and adjustable brackets to the bottom of the 14 RU rack space reserved for the PA-7500. Align the slotted holes of the fixed mounting bracket

to the holes on the front side of the equipment frame being used. Similarly, align the slotted holes in the adjustable mounting bracket to the holes on the rear of the equipment frame.

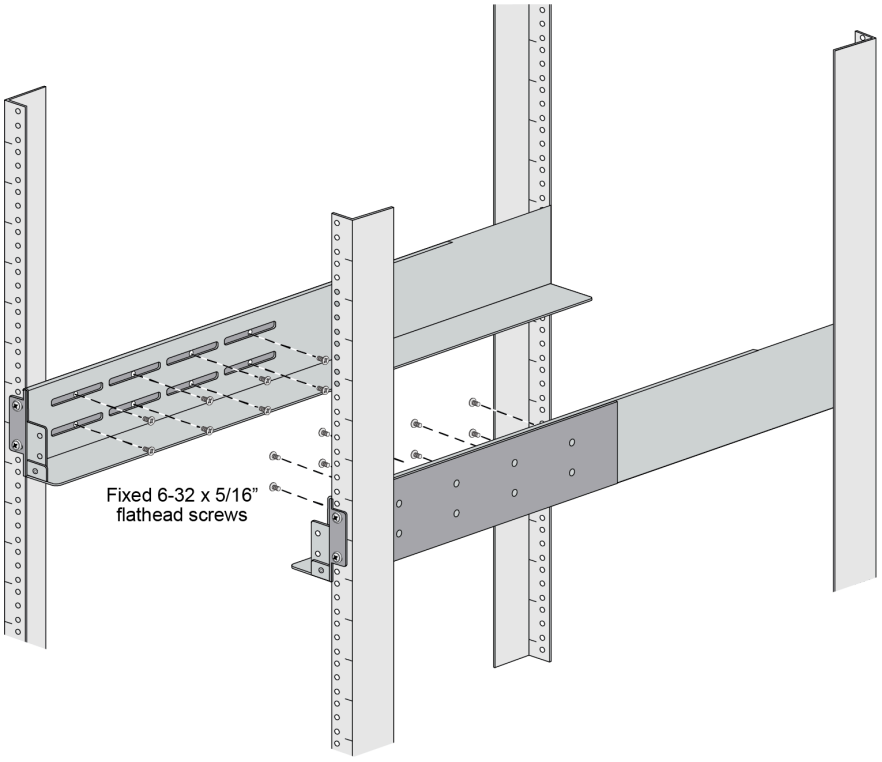


STEP 3 | Adjust the brackets to fit the depth of the equipment frame, then secure the brackets to the equipment frame with mounting screws (not provided) compatible with your equipment frame. Tighten the screws to their recommended torque value.

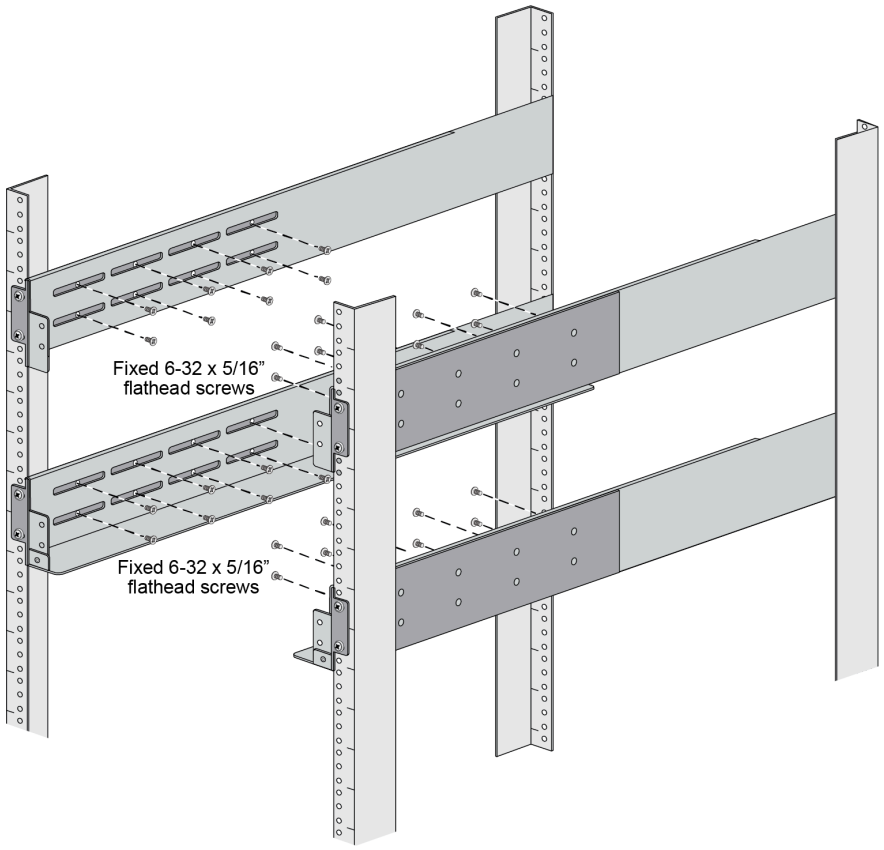
The mounting brackets are designed for equipment frames that are up to 32” deep (81.3 cm).



STEP 4 | Use the provided 6-32 x 5/16 flathead screws to secure the adjustable bracket to the fixed bracket. A minimum of 6 screws are required for each side.

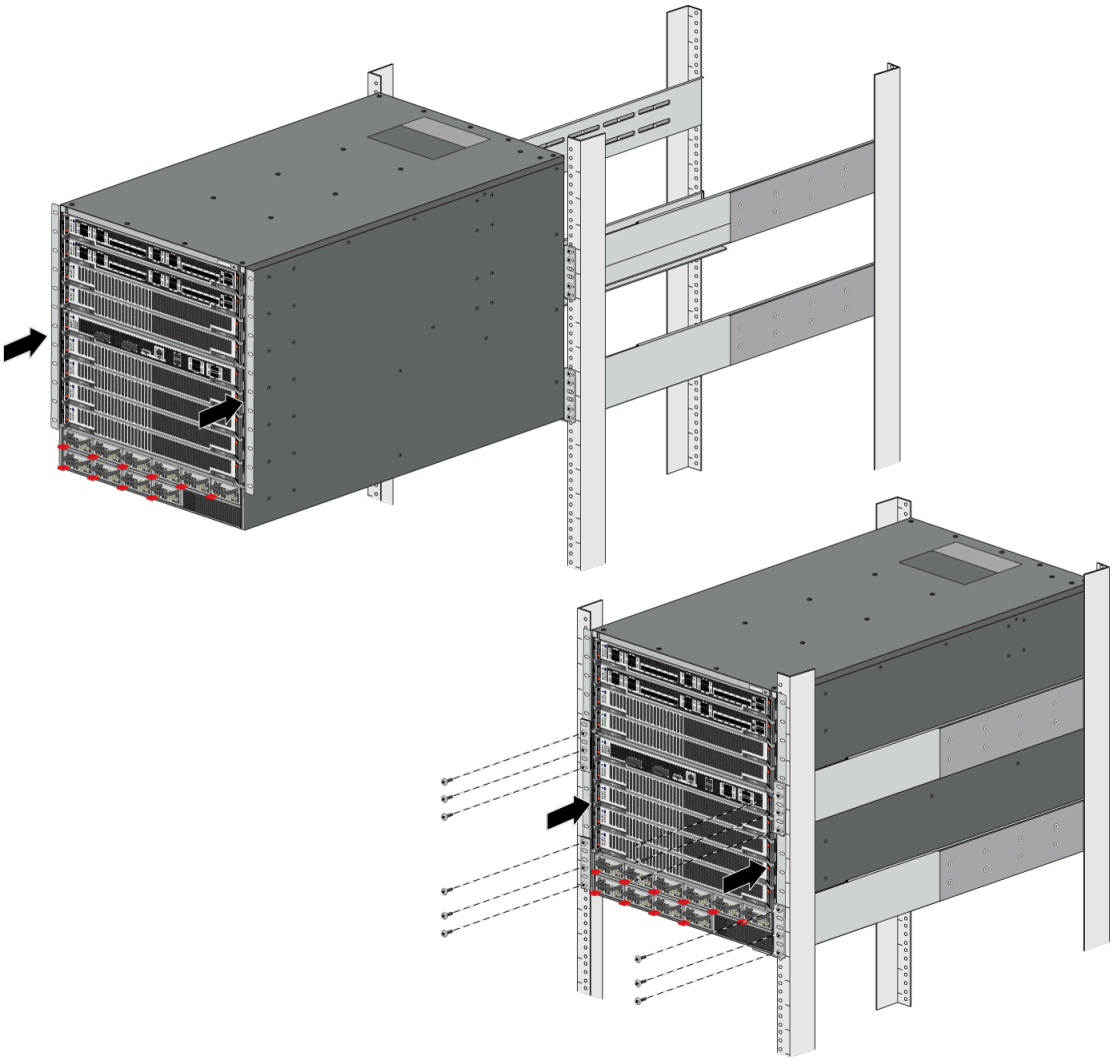


STEP 5 | Repeat Steps 1 through 4 for the mid and top mount brackets.

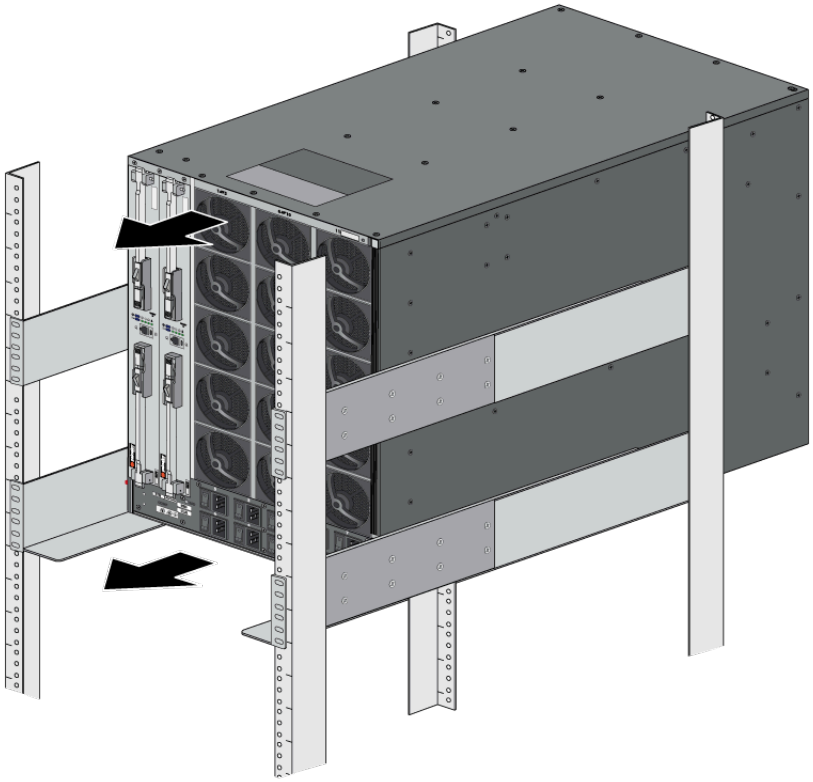


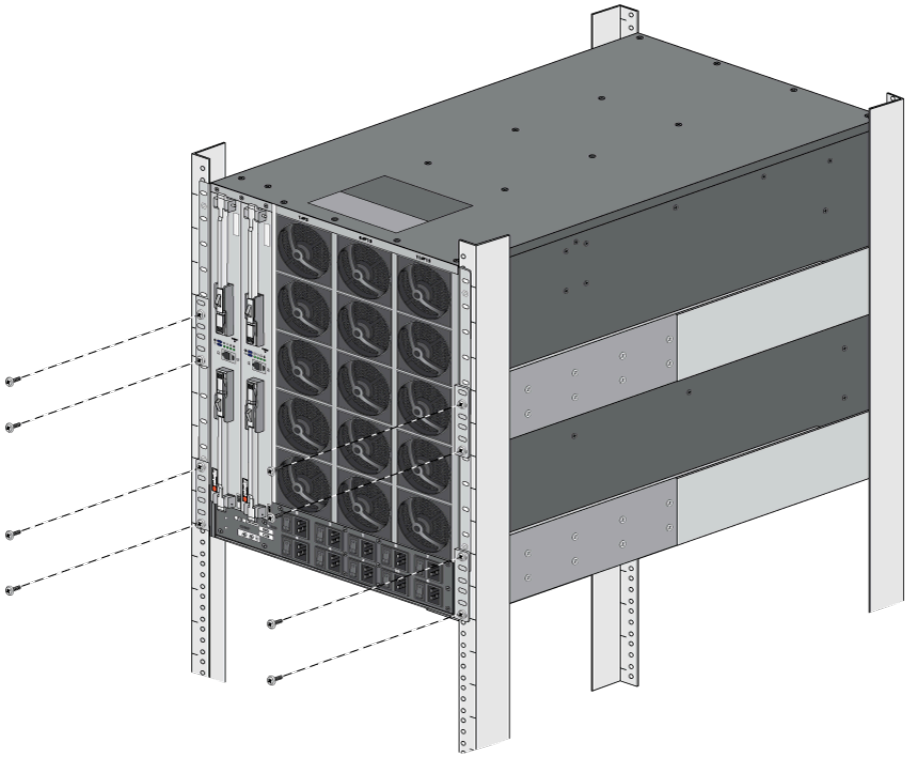
STEP 6 | Slide the PA-7500 on the brackets that were previously mounted to the equipment frame until the front mounting flanges of the PA-7500 are flush against the mounting surface of the equipment frame.

STEP 7 | Secure the PA-7500 to the equipment frame on both sides using 8 screws per bracket (not provided). The screws must be compatible with your equipment frame.



STEP 8 | Use the provided 8-32 x 3/8” Phillips panhead screws to secure the back side of the PA-7500 to the previously mounted brackets.





Install a PA-7500 Series Firewall Interface Card

The Management Processing Card (MPC), Network Processing Card (NPC), and Data Processing Card (DPC) are installed on the front panel of the chassis. The process to install each of these interface cards is the same.

The following chassis front slots (numbered from top to bottom) can support the following interface cards:

- 1—NPC and DPC
- 2—NPC and DPC
- 3—NPC and DPC
- 4—NPC and DPC
- 5—MPC (required)
- 6—NPC and DPC
- 7—NPC and DPC
- 8—NPC and DPC
- 9—NPC and DPC

Up to two Switch Fabric Cards (SFC) can be installed on the back of the chassis. The process to install the SFC is similar to the other interface cards.

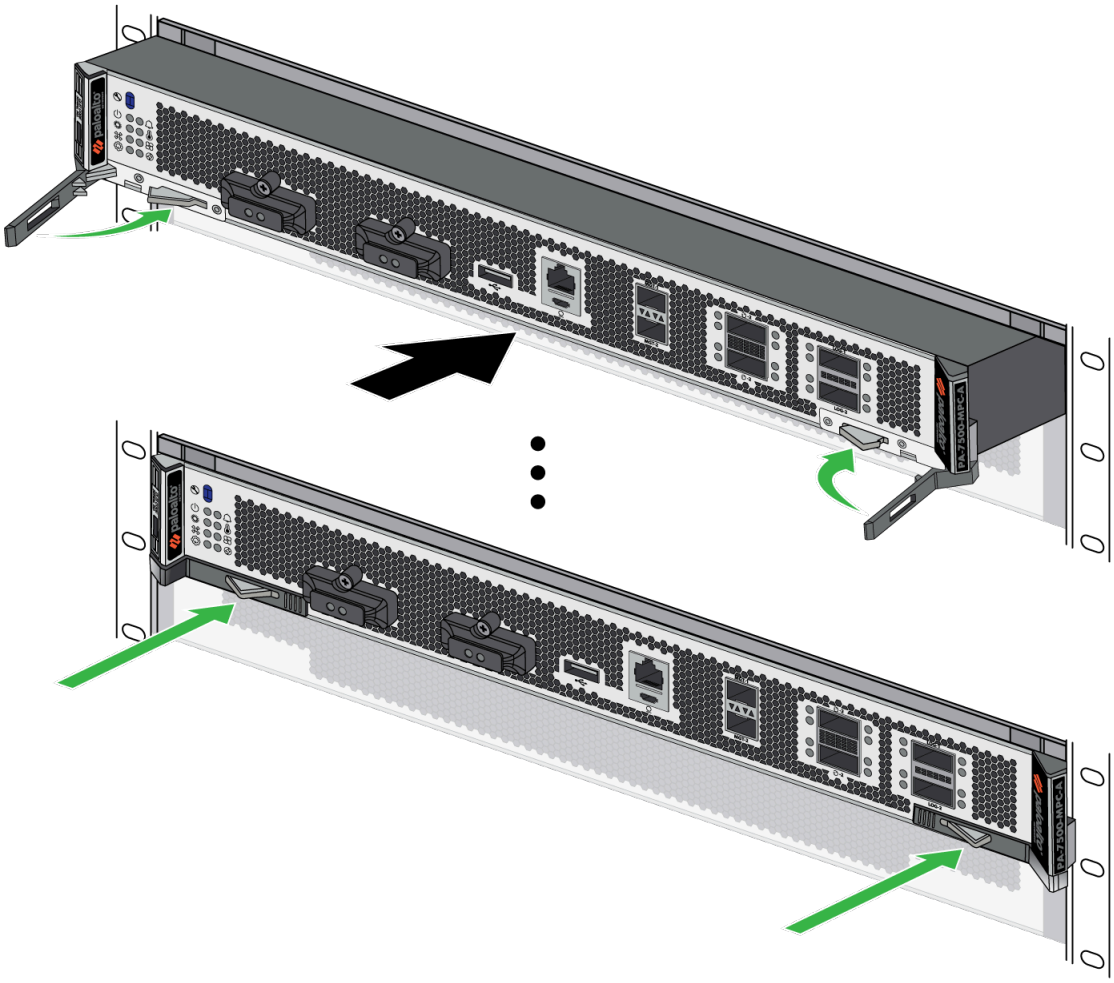
STEP 1 | Attach the provided ESD strap to your wrist and plug the other end in to the ESD port location on the appliance.

STEP 2 | Remove the interface card from the antistatic bag.

The cards are heavy and should be removed and replaced in their antistatic bags on a table or other flat, stable surface. Ensure that the card connectors do not make contact with other surfaces or objects.

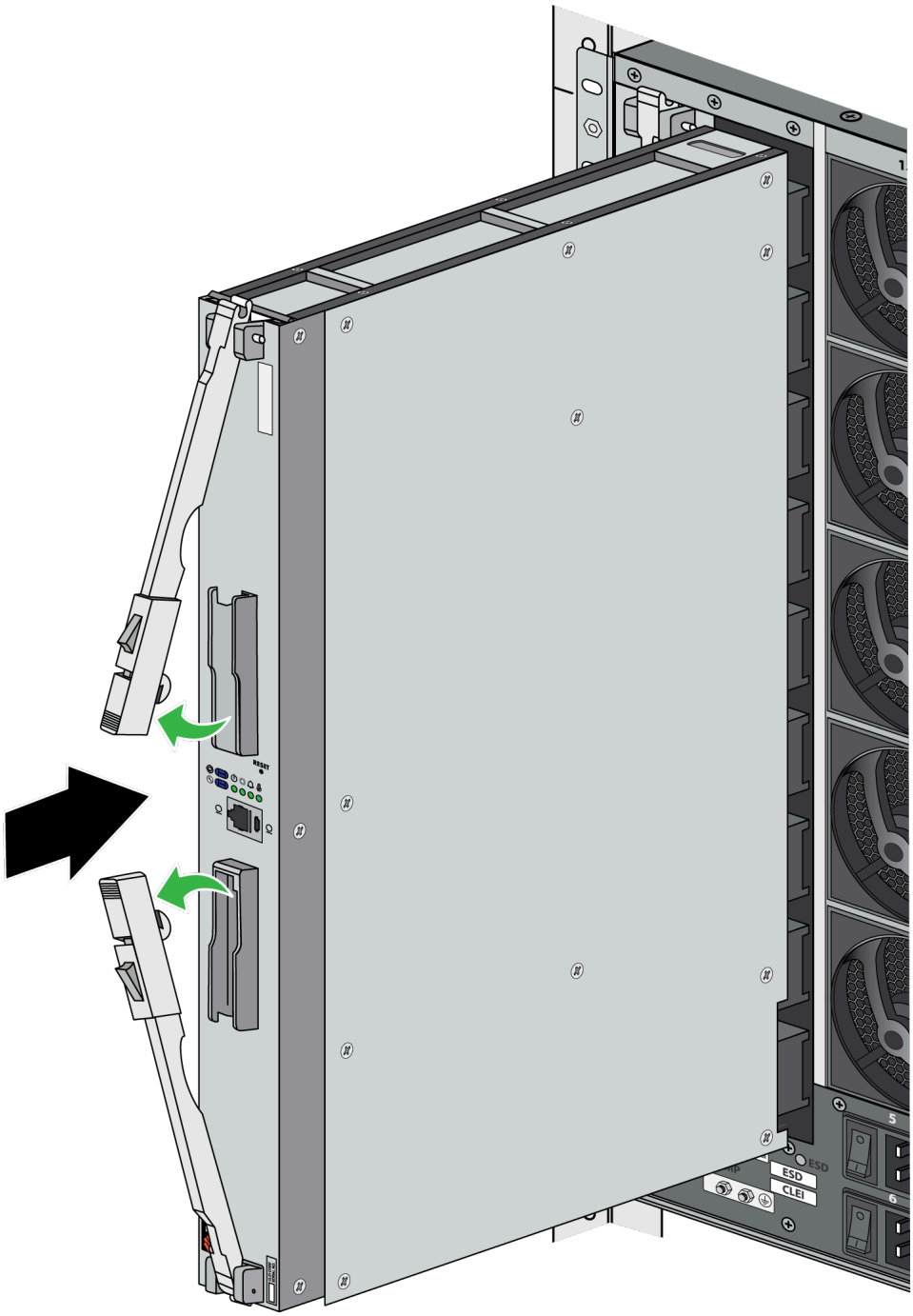
(MPC, NPC, and DPC) Push the left and right ejector tabs towards each other to allow the ejector handles to rotate into an open position. Then gently push the interface card into the

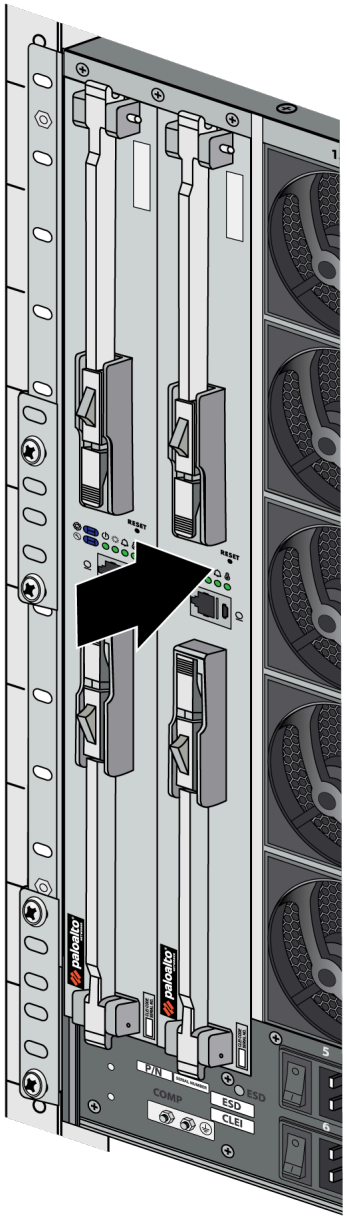
appropriate slot until the card reaches the end of the slot. Close the ejector handles to ensure that the card is secure in place.



(SFC) Pull the ejector tabs away from the center and rotate the handles outwards. Then gently push the interface card into the appropriate slot until the card reaches the end of the slot.

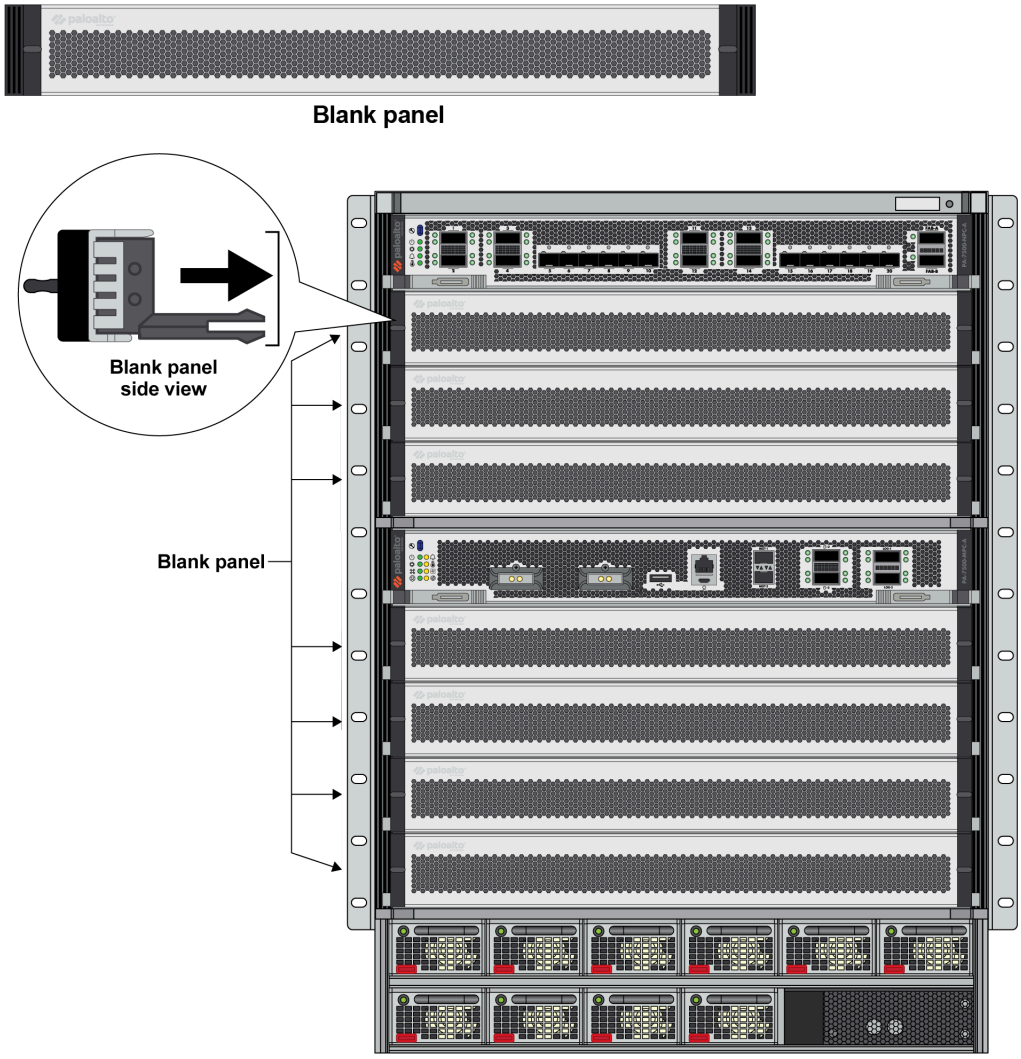
Close the ejector handles in unison; the card is secure in place when the latches are roughly parallel to the plastic guides that they are seated inside.





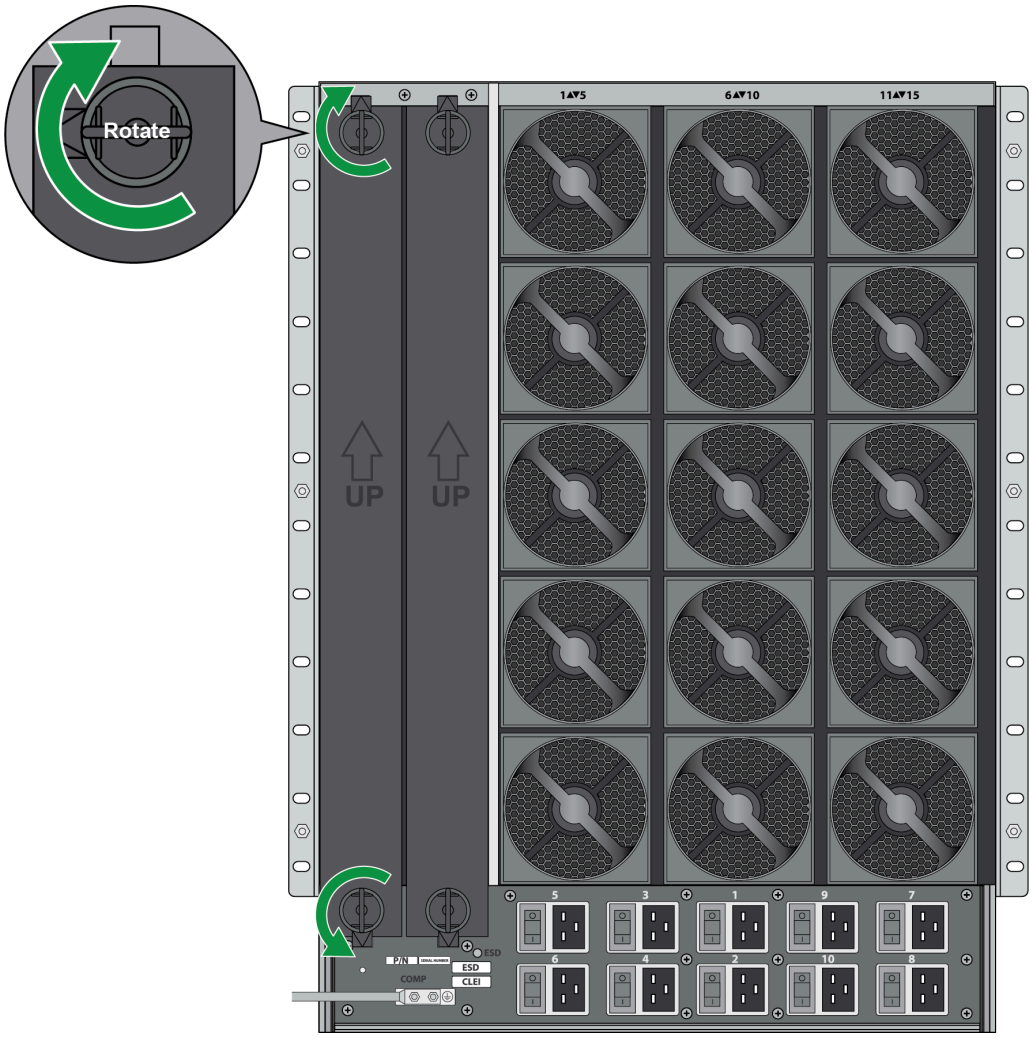
STEP 3 | Install blanks in all unused slots to help maintain chassis air flow.

1. (MPC, NPC, and DPC) Insert the blank into the front slot. Ensure that the two prongs on either side of the blank fit within the ridges on the inside of the chassis.



   To remove the blank, grip the two handles and pull it outwards. Some force may be necessary to remove the blank.

2. (SFC) Insert the blank into the back slot. Secure the blank in place by turning the two thumb tabs so that they lock into the chassis.



To remove the blank, turn the thumb tabs so that it is unlocked from the chassis. Pull the blank outwards.

Connect Power to the PA-7500 Series Firewall

The PA-7500 Series firewall supports up to ten AC or DC power supplies. A chassis with low line input voltage (90V, 110/120V, 132V) requires a minimum of eight power supplies while a chassis with high line input voltage (180V, 200/240V, 305V) requires a minimum of four power supplies. The following topics describe how to connect power to a PA-7500 Series firewall. After you power on the firewall, you can View Power Statistics of the PA-7500 Series Firewalls.

- Determine Power Requirements of the PA-7500 Series Firewalls
- Connect AC Power to the PA-7500 Series Firewall
- Connect DC Power to the PA-7500 Series Firewall
- View Power Statistics of the PA-7500 Series Firewalls

Determine Power Requirements of the PA-7500 Series Firewalls

The AC and DC power supplies support two ranges of voltages: low line (90V, 110/120V, 132V) and high line (180V, 200/240V, 305V). Depending on the input voltage, the power supply will support 1800W (for low line) and 3600W (for high line). The input voltage range determines the number of power supplies needed for the chassis. A chassis with low line input voltage requires a minimum of eight power supplies while a chassis with high line input voltage requires a minimum of four power supplies.

The minimum number of power supplies (four for high line and eight for low line) are not enough to establish full power redundancy in a fully loaded chassis.

To provide full redundancy using high line power supplies, you must install eight power supplies. A fully redundant power configuration means that half of the installed power supplies can fail and the appliance and all installed line cards still function.

You can find power information for PA-7500 Series hardware components in PA-7500 Series Firewall Component Electrical Specifications. To view power statistics on an active PA-7500, see View Power Statistics of the PA-7500 Series Firewalls.

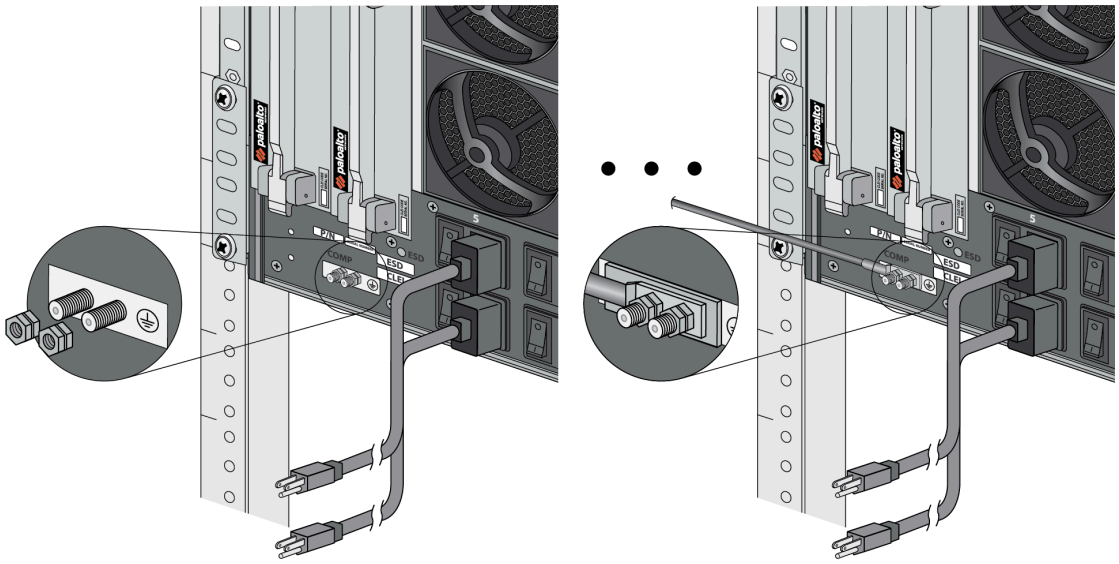
Connect AC Power to the PA-7500 Series Firewall

The following procedure describes how to connect AC power to the PA-7500 Series firewall. The AC power supplies support 100 to 240VAC power input. A minimum of four power supplies is required.

STEP 1 | Read the Product Safety Warnings.

STEP 2 | Put the provided ESD wrist strap on your wrist ensuring that the metal contact is touching your skin. Then attach (snap) one end of the ground cable to the wrist strap and remove the alligator clip from the banana clip on the other end of the ESD grounding cable. Plug the banana clip end into one of the ESD ports located on the appliance before handling ESD sensitive hardware.

STEP 3 | Remove the four nuts from the ground studs located on the back of the appliance.



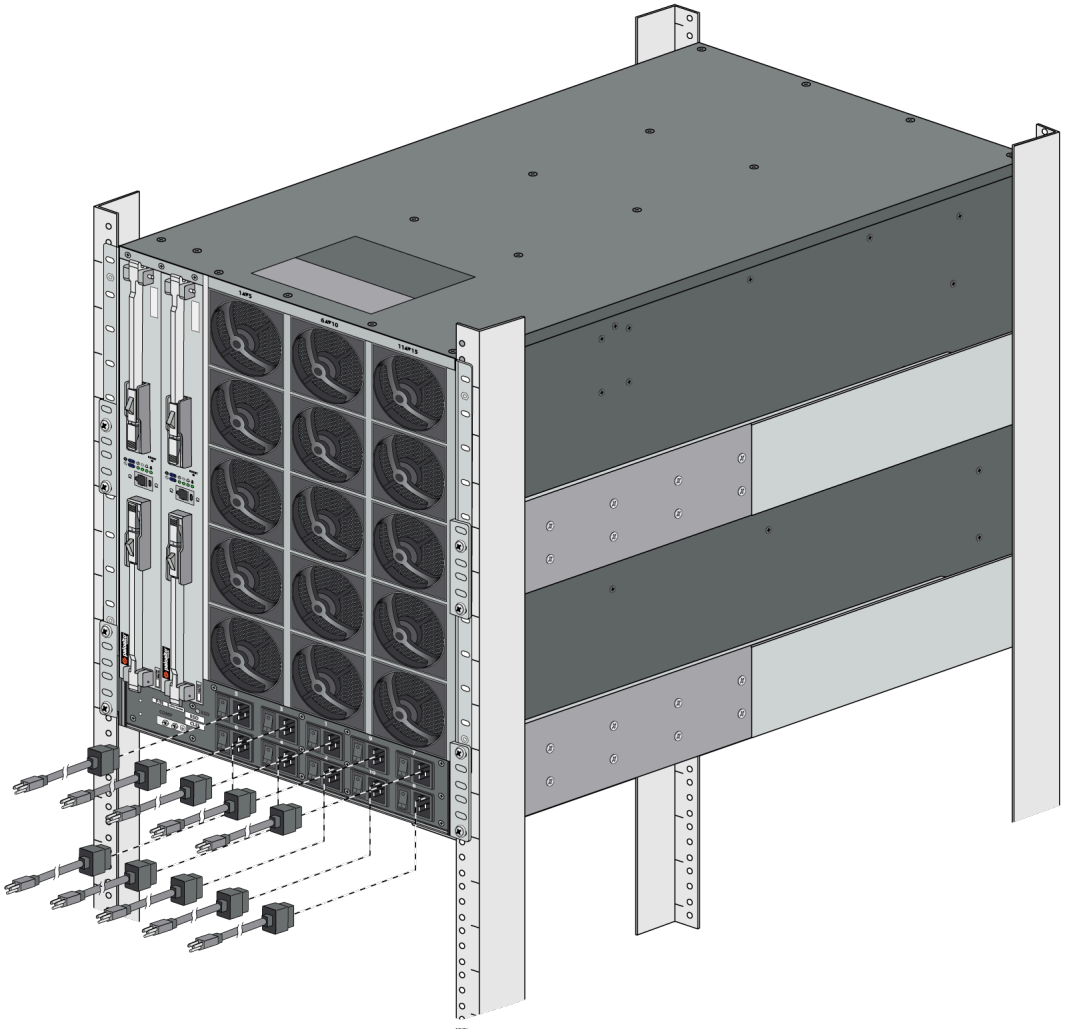
STEP 4 | Crimp a 6-AWG wire to the provided grounding lug and connect the other end to your earth ground point.

The crimp tool is not included with the appliance. It is recommended that you use a Panduit CT-3001/ST crimp tool for this procedure. Refer to the manufacturer's specifications for more information.

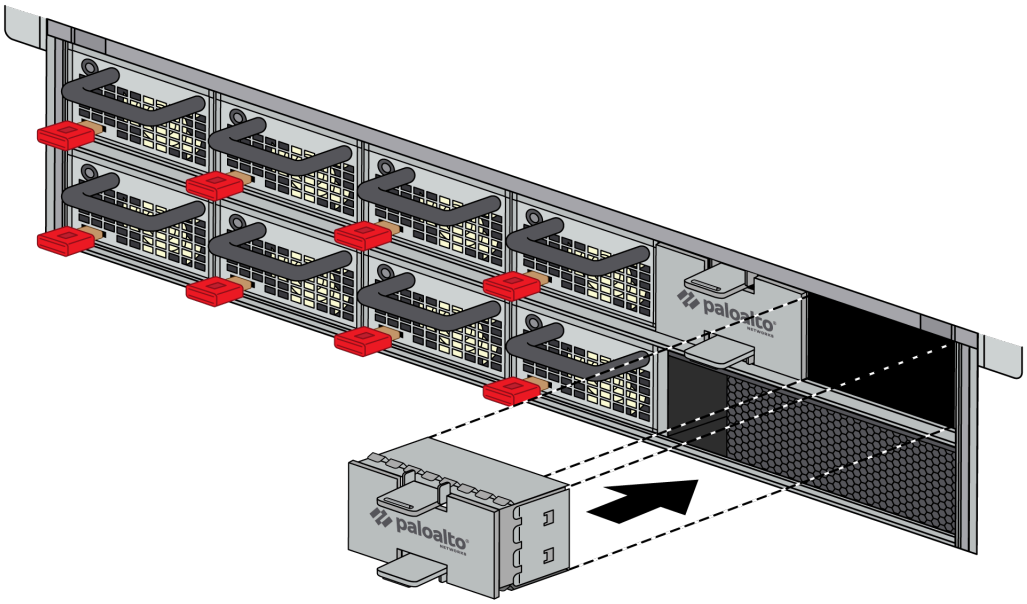
STEP 5 | Connect the two-post lug connector to the two-post ground studs on the appliance using the provided nuts and torque each nut to 50 in-lbs. Be careful not to strip the nuts and lug studs.

STEP 6 | Connect the power supply to a 120VAC 15-amp circuit breaker or 240VAC 20-amp circuit breaker using the provided power cords. Repeat this step for each additional power supply,

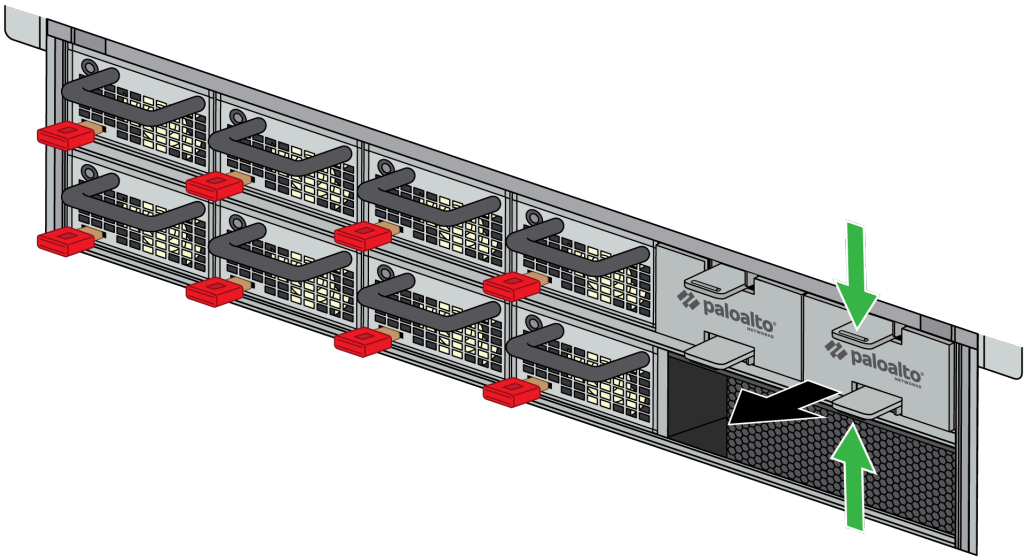
ensuring that each pair of power supplies is connected to its own circuit breaker. This ensures power redundancy and allows for planned electrical circuit maintenance.



STEP 7 | Install blanks into any unused power supply slots to help maintain chassis air flow. Slide the blank into the slot until the thumb tabs click into the locked position.



To remove the blanks, press the thumb tabs towards each other and then pull the blank outwards.



STEP 8 | After each AC cable is securely connected, turn on the power source and the appliance will power on.

Connect DC Power to the PA-7500 Series Firewall

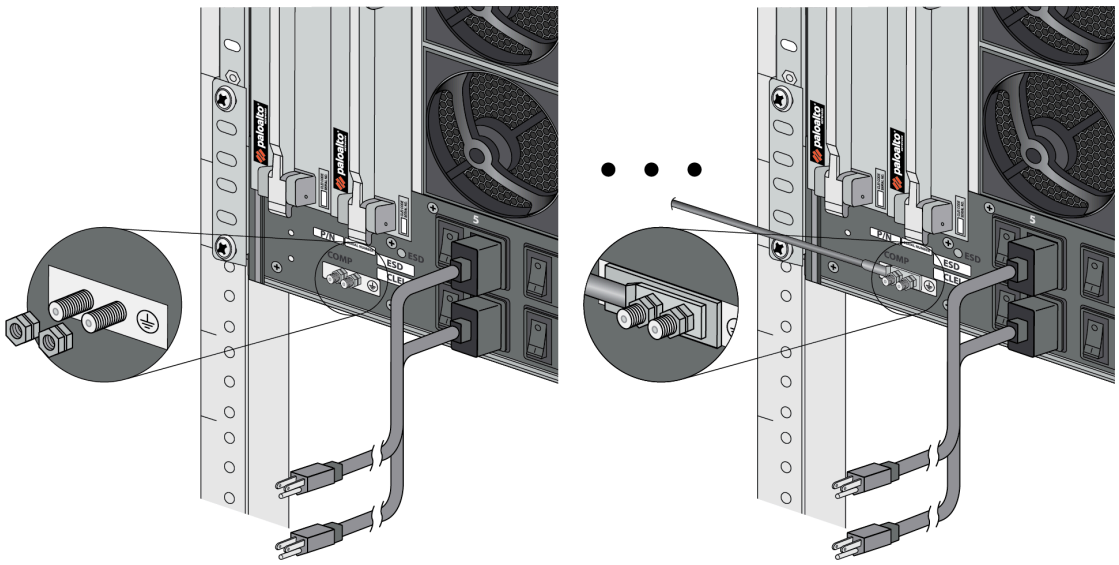
The following procedure describes how to connect DC power to the PA-7500 Series firewall. The DC power supplies support 48 to 60VDC power input. A minimum of four power supplies is required.

STEP 1 | Read the Product Safety Warnings.

STEP 2 | Put the provided ESD wrist strap on your wrist ensuring that the metal contact is touching your skin. Then attach (snap) one end of the ground cable to the wrist strap and remove the alligator clip from the banana clip on the other end of the ESD grounding cable. Plug the banana clip end into one of the ESD ports located on the appliance before handling ESD sensitive hardware.

STEP 3 | Ensure that your DC power feed is powered off.

STEP 4 | Remove the four nuts from the ground studs located on the back of the appliance.



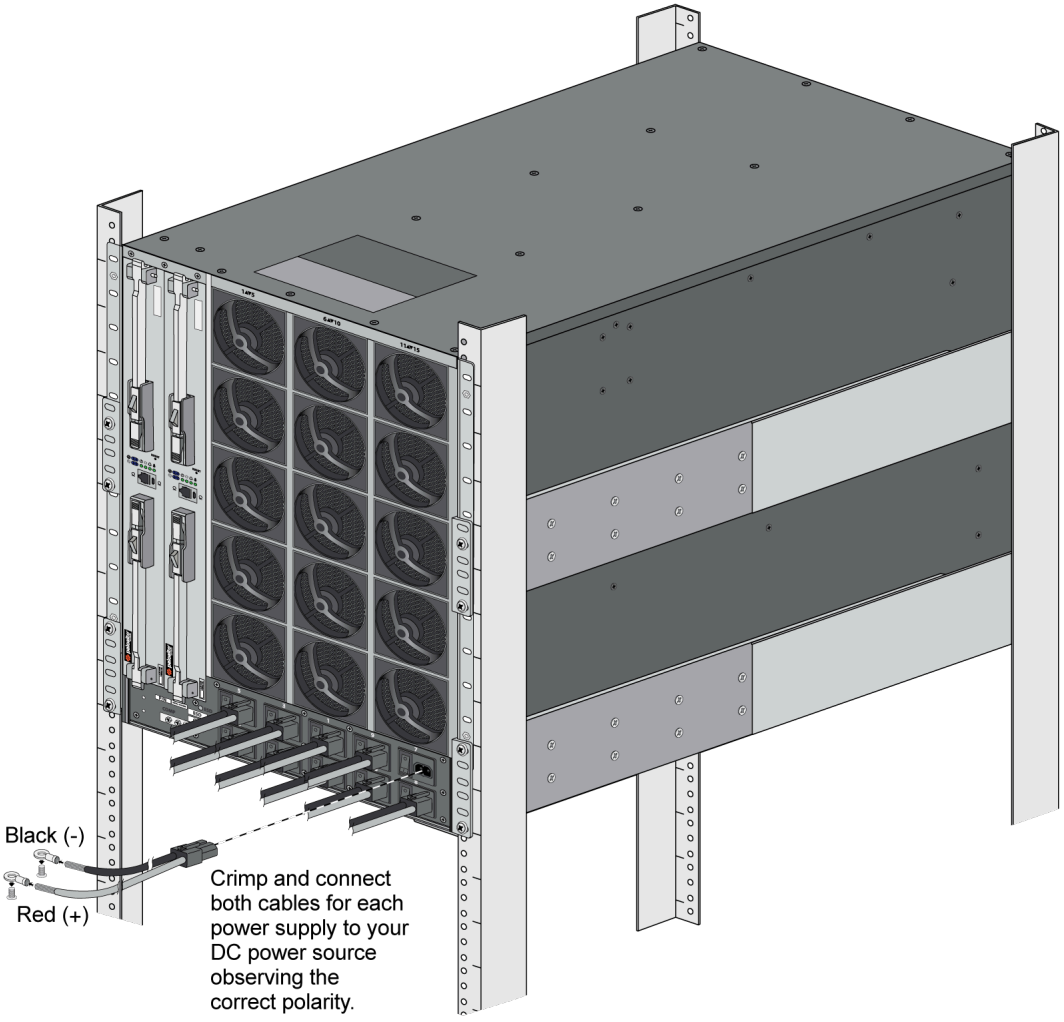
STEP 5 | Crimp a 6-AWG wire to the provided grounding lug and connect the other end to your earth ground point.

The crimp tool is not included with the appliance. It is recommended that you use a Panduit CT-3001/ST crimp tool for this procedure. Refer to the manufacturer's specifications for more information.

STEP 6 | Connect the two-post lug connector to the two-post ground studs on the appliance using the provided nuts and torque each nut to 50 in-lbs. Be careful not to strip the nuts and lug studs.

STEP 7 | Prepare the DC power cable (not included) by crimping the bare wire ends of the cables using lugs (not included) designed for your DC power source. Each cable dongle has one red wire and one black wire. Connect the red wire to the DC negative (-48VDC) terminal of your DC power source. Connect the black wire to the DC positive (RTN) terminal of your DC power source. Do this for each of the power supplies you are installing, ensuring that each

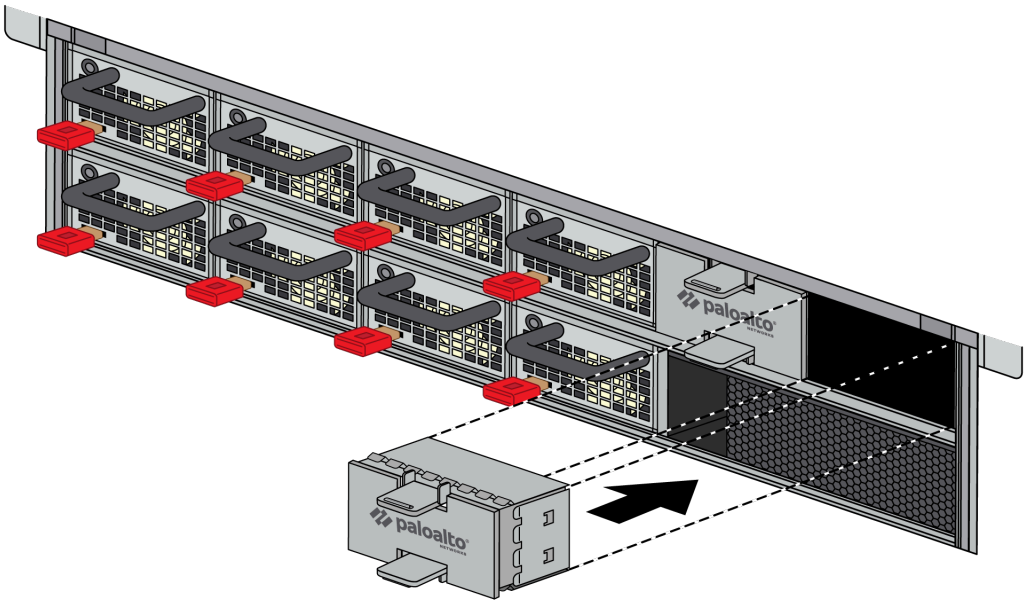
pair of power supplies is connected to its own power circuit breaker. This ensures power redundancy and allows for planned electrical circuit maintenance.



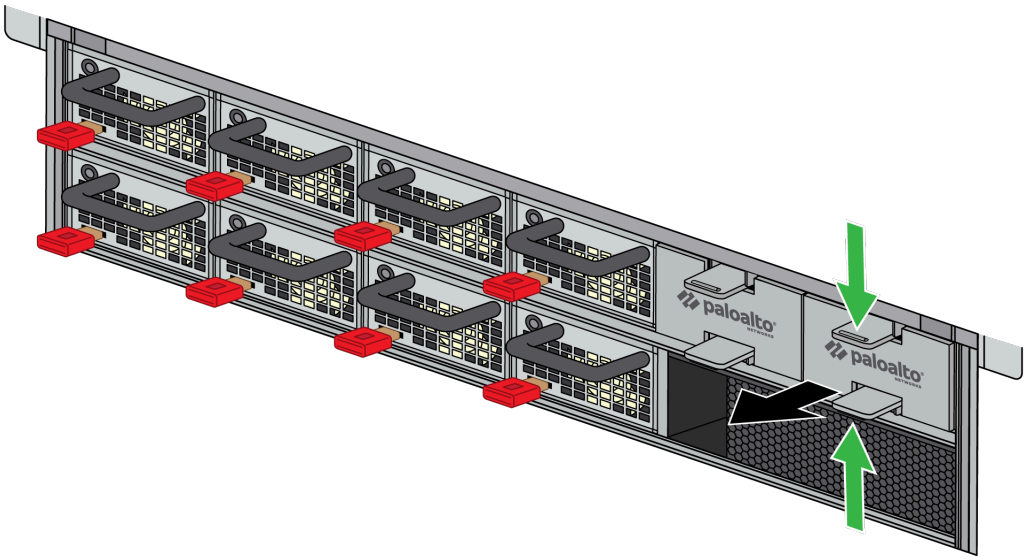
STEP 8 | Connect the other ends of the DC cables to the front of the DC power supplies by pushing the plastic connector into the DC power supply until it clicks into place.

When cabling the DC power supply to your power source, ensure that you route the cable in such a way that it does not put pressure on the plastic clips located at the front of the DC power supplies. It is best to route the cables first and then plug the cables into the power supplies.

STEP 9 | Install blanks into any unused power supply slots to help maintain chassis air flow. Slide the blank into the slot until the thumb tabs click into the locked position.



To remove the blanks, press the thumb tabs towards each other and then pull the blank outwards.



STEP 10 | After each DC cable is securely connected, turn on the power source and the appliance will power on.

View Power Statistics of the PA-7500 Series Firewalls

Use the following information to learn how to view active power statistics on a PA-7500 Series firewall to help you ensure power redundancy and to plan for growth.

This information will also help you Determine Power Requirements of the PA-7500 Series Firewalls.

*The power numbers provided by the **show chassis power** command represent power calculated by the firewall power management software and does not represent the exact measured power. The difference allows margin for thermal conditions and component aging factors. This CLI output helps you know how much power is required to prevent the appliance from overloading under extreme conditions.*

1. Using a terminal emulator, such as PuTTY, launch an SSH session to the firewall.
2. Run the following command:

```
admin@PA-7500> show chassis power
```

3. View the output for information on the status of each component and the current power rating.

For example, the following table shows the CLI output (in table format) from a PA-7500. The output shows each front slot (1 to 9), each back slot (10 to 11), the status of each component, and the rated power consumption for each component.

Example Power Output from a PA-7500 Firewall

Slot	Component	Status	Power (w)
1	NPC	Traffic	580
2	DPC	Traffic	1082
3	DPC	Traffic	1086
4	NPC	Traffic	585
5	MPC	Traffic	460
6	NPC	Traffic	592
7	DPC	Traffic	1077
8	NPC	Traffic	589
9	DPC	Traffic	1080
10	SFC	Traffic	330

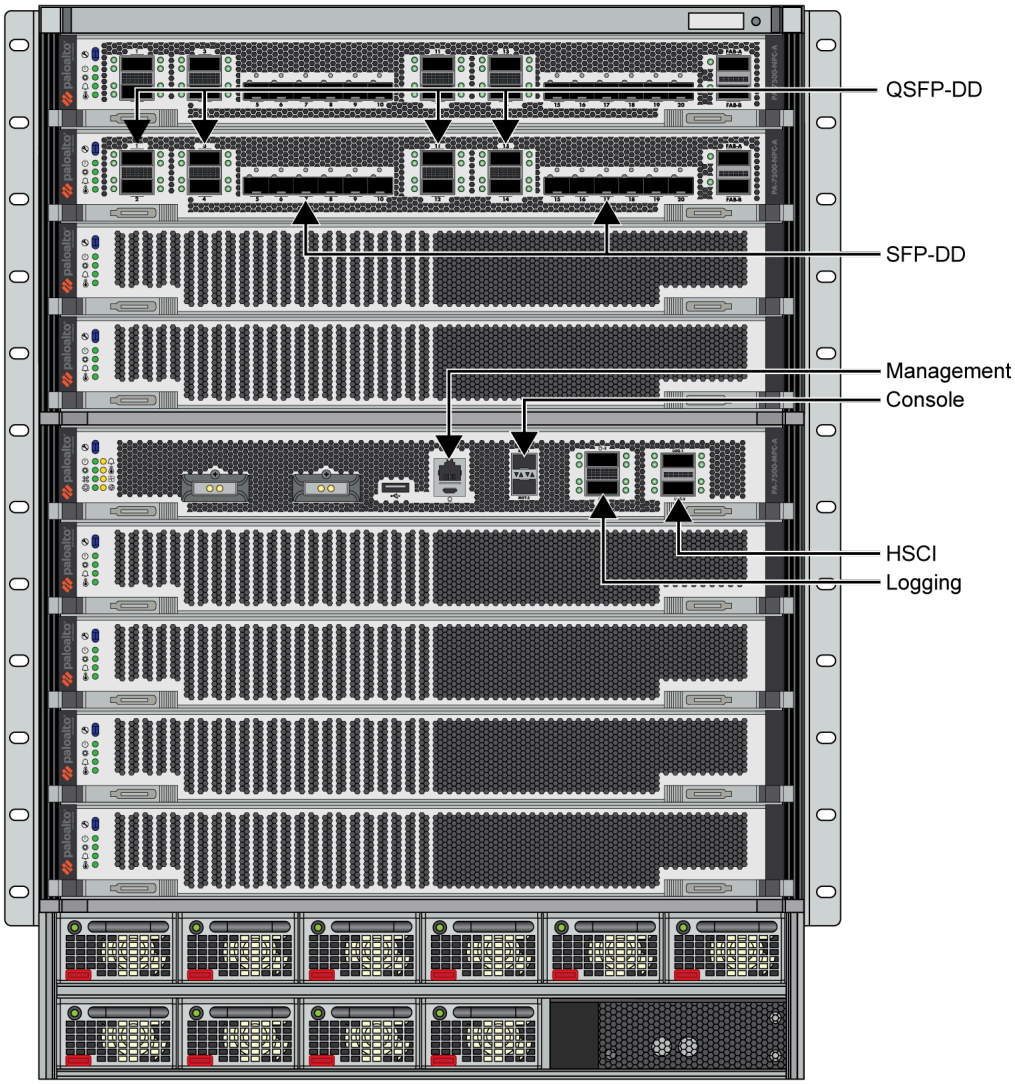
Slot	Component	Status	Power (w)
11	SFC	Standby	309

Connect Cables to the PA-7500 Series Firewall

After you Connect Power to the PA-7500 Series Firewall, connect your management computer to the management port (MGT) on the firewall Management Processing Card (MPC) so you can begin the initial configuration. You can optionally connect your management computer to the console port, also on the MPC, which provides a serial connection to the firewall and enables you to view the bootup messages and manage the firewall using the command line interface (CLI).

You then configure the Ethernet ports on the Network Processing Card (NPC) and connect these ports to your switch or router.

The next image shows the PA-7500 firewall cable connections.



The lower QSFP-DD ports on the Management Processing Card (MPC) and Network Processing Card (NPC) may be harder to access if the upper QSFP-DD port has an installed optic.

PA-7500 Series Firewall LED Definitions

Interpret the PA-7500 Series Firewall LEDs

The following table describes the definitions of the LEDs located on the power supplies and fan assemblies. For the interface card LED definitions, see Interpret the PA-7500 Series Firewall Interface Card LEDs.

The AC and DC power supplies have a FAIL and an OK LED.

AC Power Supply	
Solid Green	Power output is on.
Blinking Green (0.5Hz)	Standby mode. AC power is present but only at 12VSB (Volts Standby).
Solid Yellow	Power supply critical failure.
Off	No AC power or AC power cord is unplugged.

DC Power Supply	
Solid Green	Power output is on.
Blinking Green (0.5Hz)	Standby mode. DC power is present but only at 12VSB (Volts Standby).
Solid Yellow	Power supply critical failure.
Off	No DC power.

Fan Assembly	
Green	The fan trays and all fans are operating normally.
Red	A fan in the fan tray failed (see Replace a PA-7500 Series Firewall Fan Assembly)

Interpret the PA-7500 Series Firewall Interface Card LEDs

Consult the following topics to view the LED definitions of each interface card and its ports.

- PA-7500 Series Firewall MPC LEDs
- PA-7500 Series Firewall NPC LEDs
- PA-7500 Series Firewall DPC LEDs
- PA-7500 Series Firewall SFC LEDs

PA-7500 Series Firewall MPC LEDs

The following table describes how to interpret the status LEDs on a Management Processing Card (MPC).

LED	Description
	Service Allows a remote administrator to illuminate the LED on a specific front-slot card so an on-site technician can locate the card. • **Off**—The firewall is operating normally. • **Blue**—The firewall is instructed by the CLI or Web Interface to enable this LED.
	Power • **Green**—The firewall is powered on. • **Yellow**—The firewall is shutting down or there is an issue with one or more power rails. • **Off**—The firewall is not powered on or an error occurred with the internal power system (for example, power is not within tolerance levels).

LED	Description
	**Status** • **Green**—The firewall is operating normally. • **Yellow**—The firewall is booting.
	**NGFW Clustering** The LED behavior for this functionality is not implemented yet.
	**Active MPC** • **Green**—The MPC is enabled.
	**Alarm** • **Off**—The firewall is operating normally. • **Red**—A hardware failure, such as a power supply failure, a firewall failure that caused an HA failover, a drive failure, or the hardware overheated and exceeded the high temperature threshold.
	**Temperature** • **Green**—The firewall temperature is normal. • **Yellow**—The firewall temperature is outside tolerance levels. See the PA-7500 Series Firewall Environmental Specifications for the operating temperature range.
	**Fans** • **Green**—The fan tray and all fans are operating normally. • **Red**—A fan has failed.
	**Power Supplies** • **Green**—The power supplies are operating normally. • **Red**—A power supply is present but is not working.

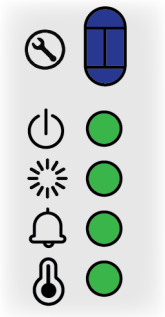
The following table describes how to interpret the LEDs on the MPC ports.

LED	Description
LOG-1 and LOG-2 (QSFP28)	The QSFP28 ports have four LEDs each; the LED illuminated depends on the transceiver that is installed.

LED	Description
	On the zQSFP ports, the left LED glows yellow when a 1Gbps transceiver is connected and the right LED glows green when a 10Gbps transceiver is connected. When operating at 25Gbps speed, the right LED glows teal. The color of the LED differs based on the port speed. • 1Gbps—Yellow • 10Gbps—Green • 25Gbps—Teal • 40Gbps—Yellow • 100Gbps—Blue • **Solid Color**—The firewall network link is up. • **Blinking Color**—The firewall is processing network activity.
HSCI-A and HSCI-B (QSFP28)	The QSFP28 ports have four LEDs each. *On the QSFP28 ports, the LEDs are illuminated based on breakout status. Breaking out the port to 10Gbps causes all LEDs to glow green. Breaking out the port to 100Gbps causes all LEDs to glow teal. If the port is not broken out, the LEDs glow yellow for 40Gbps and blue for 400Gbps.*

PA-7500 Series Firewall NPC LEDs

The following table describes how to interpret the status LEDs on a Network Processing Card (NPC).



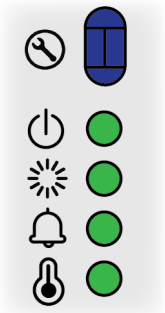
LED	Description
	Service Allows a remote administrator to illuminate the LED on a specific front-slot card so an on-site technician can locate the card. • **Off**—The firewall is operating normally. • **Blue**—The firewall is instructed by the CLI or Web Interface to enable this LED.
	Power • **Green**—The firewall is powered on. • **Off**—The firewall is not powered on or an error occurred with the internal power system (for example, power is not within tolerance levels).
	Status • **Green**—The firewall is operating normally. • **Yellow**—The firewall is booting.
	Alarm • **Red**—A hardware failure, such as a power supply failure, a firewall failure that caused an HA failover, a drive failure, or the hardware overheated and exceeded the high temperature threshold. • **Off**—The firewall is operating normally.
	Temperature • **Green**—The firewall temperature is normal. • **Yellow**—The firewall temperature is outside tolerance levels. See the PA-7500 Series Firewall Environmental Specifications for the operating temperature range.

The following table describes how to interpret the LEDs on the NPC ports.

LED	Description
SFP, SFP+, and SFP28	The SFP, SFP+ and SFP28 ports have four LEDs each; the LED illuminated depends on the transceiver that is installed. The color of the LED differs based on the port speed. • 1Gbps—Yellow • 10Gbps—Green • 25Gbps—Teal • 40Gbps—Yellow • 100Gbps—Blue • **Solid Color**—The firewall network link is up. • **Blinking Color**—The firewall is processing network activity.
QSFP+ and QSFP28	The QSFP+ and QSFP28 ports have four LEDs each. *On the QSFP28 ports, the LEDs are illuminated based on breakout status. Breaking out the port to 10Gbps causes all LEDs to glow green. Breaking out the port to 100Gbps causes all LEDs to glow teal. If the port is not broken out, the LEDs glow yellow for 40Gbps and blue for 400Gbps.*

PA-7500 Series Firewall DPC LEDs

The following table describes how to interpret the status LEDs on a Data Processing Card (DPC).



LED	Description
	**Service** Allows a remote administrator to illuminate the LED on a specific front-slot card so an on-site technician can locate the card. • **Off**—The firewall is operating normally. • **Blue**—The firewall is instructed by the CLI or Web Interface to enable this LED.
	**Power** • **Green**—The firewall is powered on. • **Off**—The firewall is not powered on or an error occurred with the internal power system (for example, power is not within tolerance levels).
	**Status** • **Green**—The firewall is operating normally. • **Yellow**—The firewall is booting.
	**Alarm** • **Red**—A hardware failure, such as a power supply failure, a firewall failure that caused an HA failover, a drive failure, or the hardware overheated and exceeded the high temperature threshold. • **Off**—The firewall is operating normally.
	**Temperature** • **Green**—The firewall temperature is normal. • **Yellow**—The firewall temperature is outside tolerance levels. See the PA-7500 Series Firewall Environmental Specifications for the operating temperature range.

PA-7500 Series Firewall SFC LEDs

The following table describes how to interpret the status LEDs on a Switch Fabric Card (SFC).

LED	Description
	Service Allows a remote administrator to illuminate the LED on a specific front-slot card so an on-site technician can locate the card. • **Off**—The firewall is operating normally. • **Blue**—The firewall is instructed by the CLI or Web Interface to enable this LED.
	Active/Standby • **Green**—Active • **Yellow**—Standby
	Power • **Green**—The firewall is powered on. • **Off**—The firewall is not powered on or an error occurred with the internal power system (for example, power is not within tolerance levels).
	Status • **Green**—The firewall is operating normally. • **Yellow**—The firewall is booting.
	Alarm • **Red**—A hardware failure, such as a power supply failure, a firewall failure that caused an HA failover, a drive failure, or the hardware overheated and exceeded the high temperature threshold. • **Off**—The firewall is operating normally.
	Temperature • **Green**—The firewall temperature is normal.

LED	Description
	• **Yellow**—The firewall temperature is outside tolerance levels. See the PA-7500 Series Firewall Environmental Specifications for the operating temperature range.

PA-7500 Series Firewall Maintenance

The following topics describes how to replace field-serviceable components on a PA-7500 Series firewall. For an overview of the hardware components, see PA-7500 Series Firewall Overview.

- Replace a PA-7500 Series Firewall AC or DC Power Supply
- Replace a PA-7500 Series Firewall Interface Card
- Replace a PA-7500 Series Firewall Interface Card in a NGFW Cluster
- Replace a PA-7500 Series Firewall Fan Assembly
- Replace a PA-7500 Series Firewall System Drive
- Replace a PA-7500 Series Firewall Logging Drive

Replace a PA-7500 Series Firewall AC or DC Power Supply

The following instructions describe how to replace a power supply in a PA-7500 Series firewall.

STEP 1 | Put the provided ESD wrist strap on your wrist ensuring that the metal contact is touching your skin. Then attach (snap) one end of the ground cable to the wrist strap and remove the alligator clip from the banana clip on the other end of the ESD grounding cable. Plug the banana clip end into one of the ESD ports located on the appliance before handling ESD sensitive hardware.

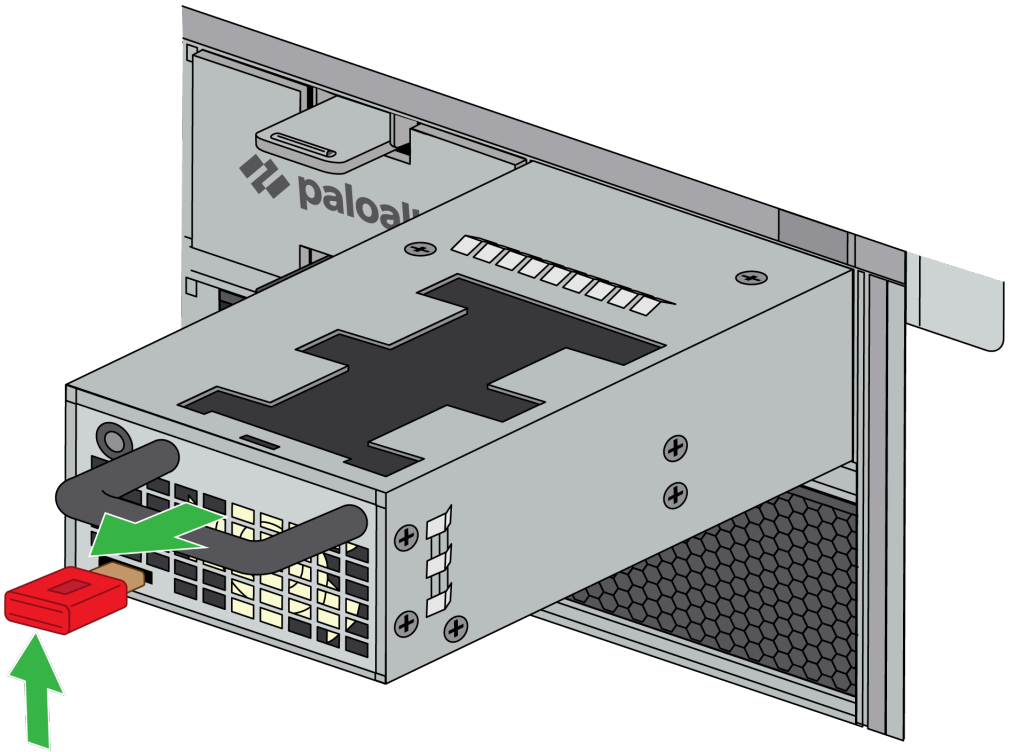
STEP 2 | Locate the failed power supply by viewing the system logs or by viewing the LED on the front of the power supply. A red LED indicates a failed power supply. For details on the power supply LEDs, see Interpret the PA-7500 Series Firewall LEDs.

STEP 3 | Shut off power to the failed power supply.

(AC only) Unplug and remove the power cord (leaving the cord in place can cause arcing inside the appliance).

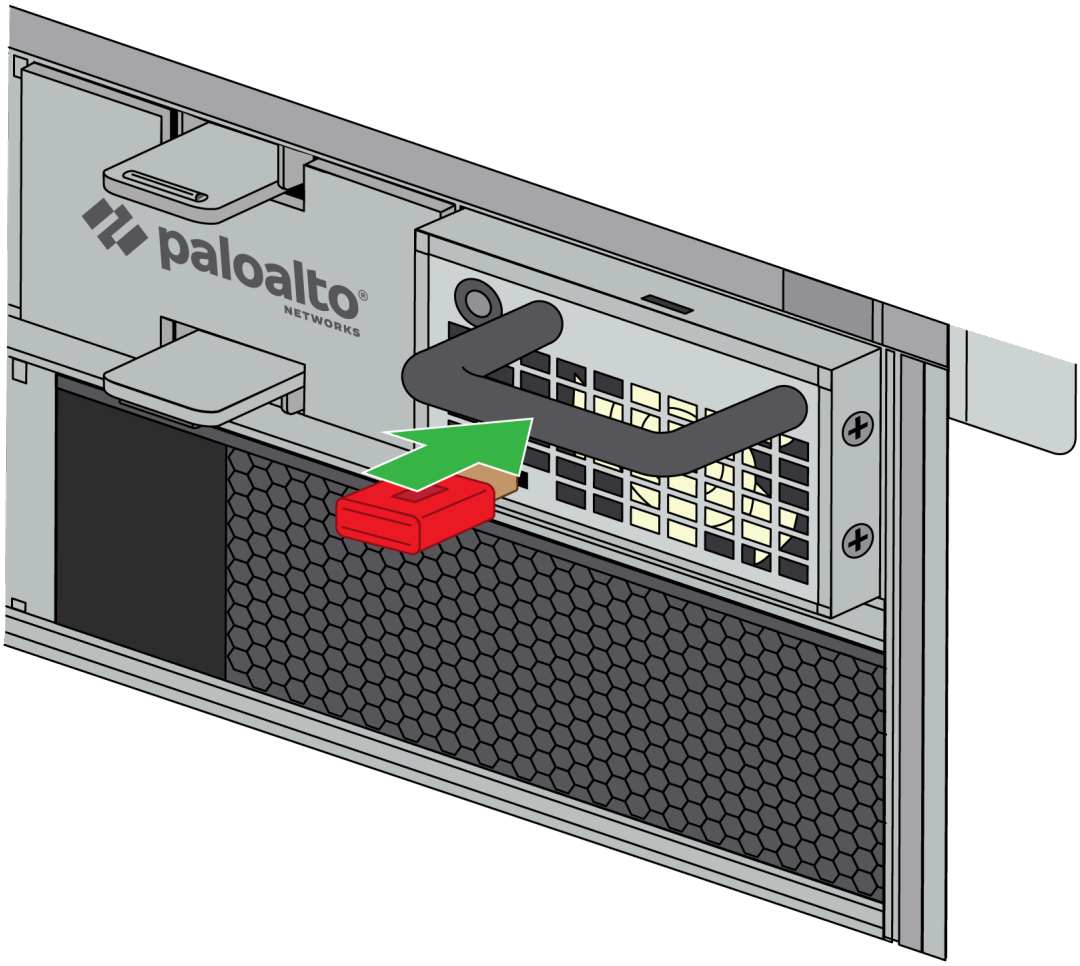
(DC only) Power off the DC power source that is connected to the failed DC power supply.

STEP 4 | Facing the rear side of the appliance, push the power supply latch handle upwards with your thumb to disengage the latch from the appliance. With the latch still pushed up, pull on the metal handle to slide the power supply out.



STEP 5 | Remove the replacement power supply from the packaging.

STEP 6 | Slide the new power supply into the empty power supply slot until you hear the latch click into place. Pull on the metal handle to ensure that the power supply latch is fully engaged and the power supply is locked into the appliance.



STEP 7 | Turn on power to the new power supply.

(AC only) Plug the power cable into the corresponding AC power module on the back of the appliance. The new power supply turns on and the LED will turn green.

(DC only) Insert the DC power cable back into the power supply ensuring that the notches line up correctly. The plastic clips on each side of the connector will clip into place as you seat the cable.

When cabling the DC power supply to your power source, ensure that you route the cable in such a way that it does not put pressure on the plastic clips located at the front of the power supply. It is best to route and secure the cable first and then plug the cable into the power supply.

Replace a PA-7500 Series Firewall Interface Card

The procedures to replace the Management Processing Card (MPC), Network Processing Card (NPC), and Data Processing Card (DPC) are the same. The Switch Fabric Card (SFC), located on the back of the chassis, has a similar procedure.

If your PA-7500 is in a NGFW cluster, you must follow the procedures for replacing an interface card in a NGFW cluster.

The replacement MPC ships with a factory default configuration and version of PAN-OS. You may need to upgrade or downgrade the PAN-OS version to your preferred version and you will need to restore the firewall configuration from a backup.

To learn how to create a backup of your PAN-OS configuration, see Save and Export Firewall Configurations.

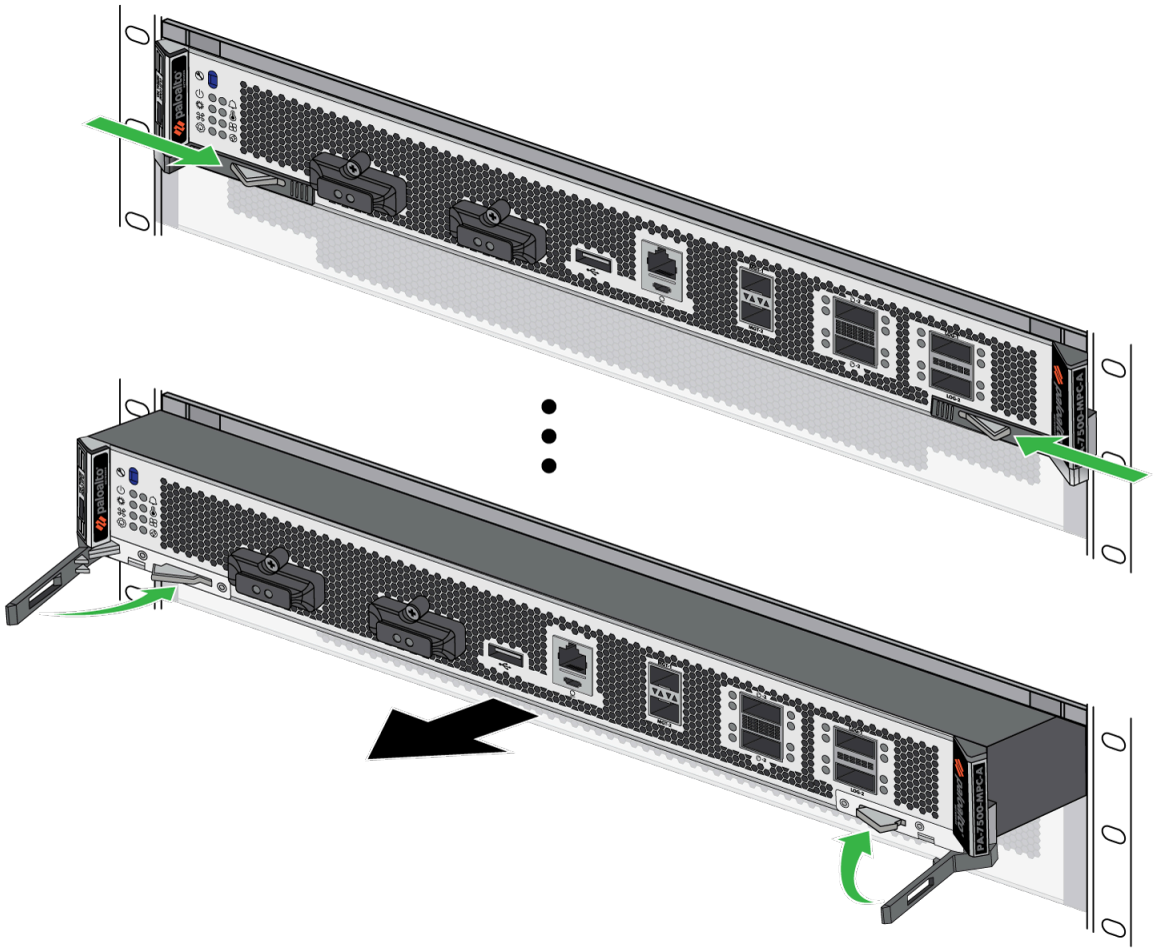
If an NPC fails, the card will reboot and attempt to recover. If the card does not recover, it will change to a down state. If there is only one functioning NPC in the appliance and the NPC fails after three recovery attempts, the firewall will reboot to attempt to recover the card.

STEP 1 | Put the provided ESD wrist strap on your wrist ensuring that the metal contact is touching your skin. Then attach (snap) one end of the ground cable to the wrist strap and remove the alligator clip from the banana clip on the other end of the ESD grounding cable. Plug the banana clip end into one of the ESD ports located on the appliance before handling ESD sensitive hardware.

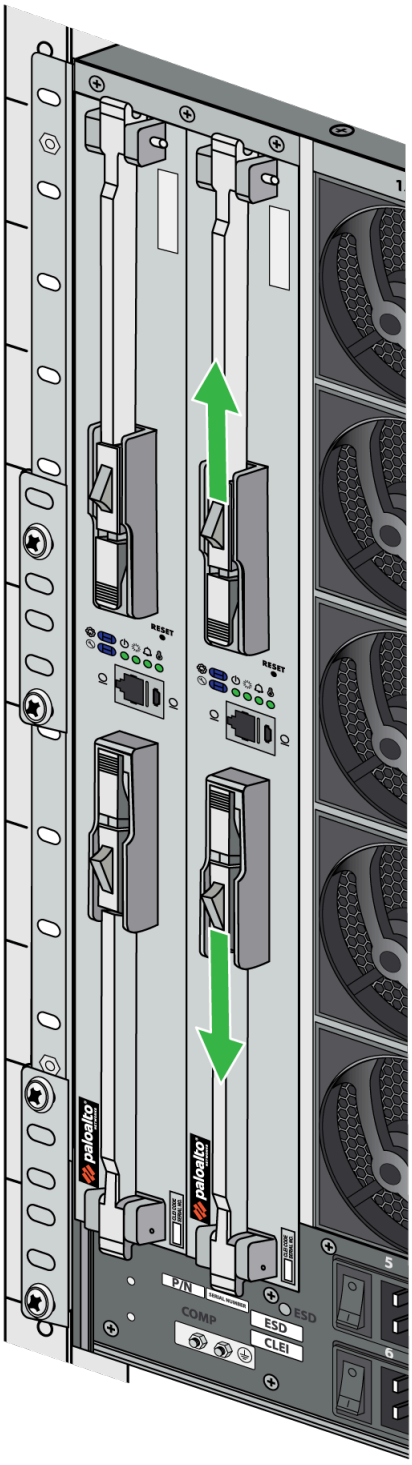
STEP 2 | (MPC only) Ensure that the PA-7500 firewall is powered off and that the fans are not still spinning.

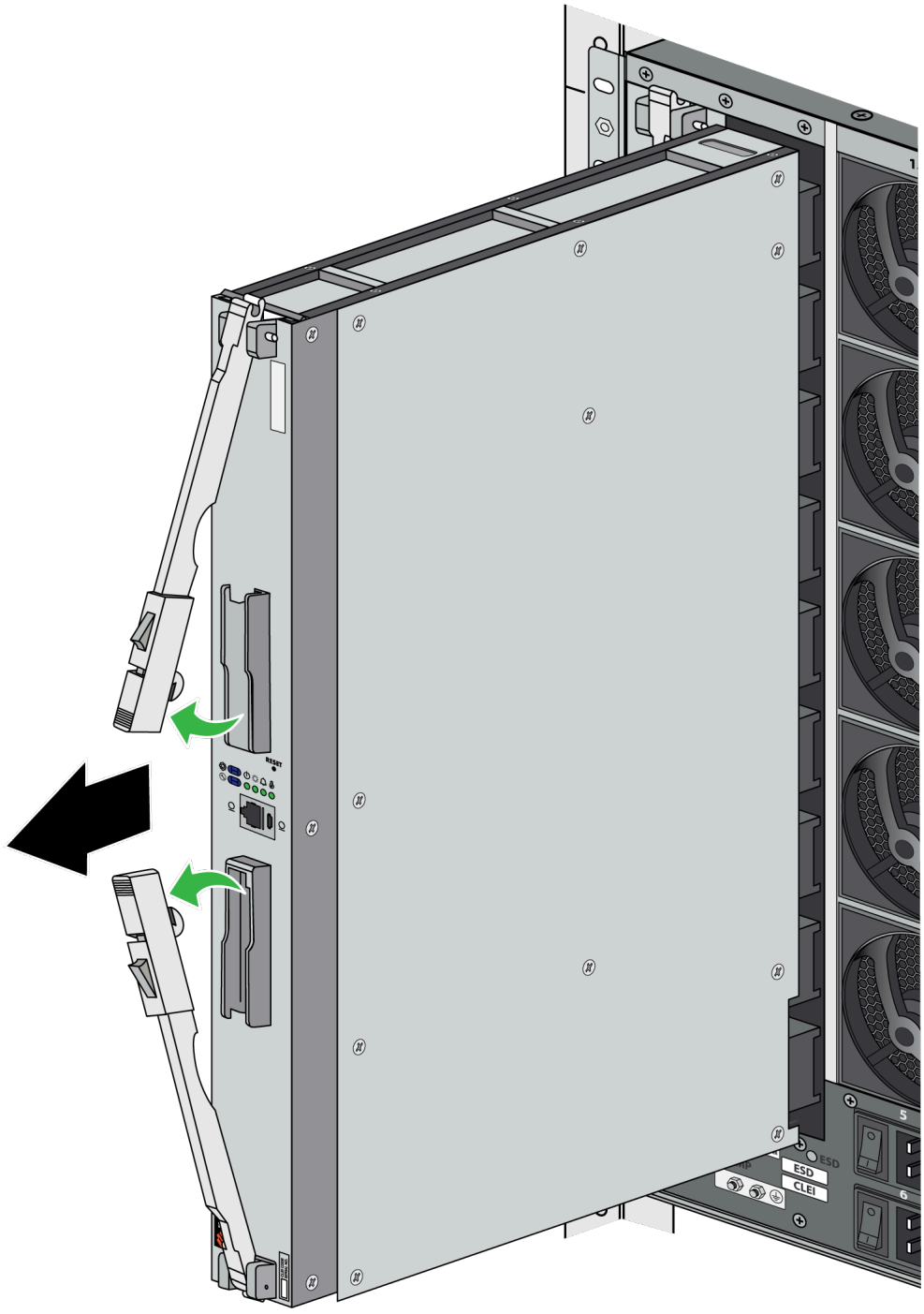
STEP 3 | Unlock the interface card.

- (MPC, NPC, and DPC) Push the ejector tabs on the card towards the center, prompting a click. This will cause ejector handles on the front of the card to rotate outward and unlock the card.



- (SFC) Push the ejector tabs on the card away from the center, prompting a click. This will allow the ejector handles to rotate outward and unlock the card.





STEP 4 | Grip the ejector handles and gently pull the card out of its slot.

The cards are heavy and should be removed and replaced in their antistatic bags on a table or other flat, stable surface. Ensure that the card connectors do not make contact with other surfaces or objects.

STEP 5 | Retrieve your replacement card and install it into the appropriate slot.

The following chassis front slots (numbered from top to bottom) can support the following interface cards:

- 1—NPC and DPC
- 2—NPC and DPC
- 3—NPC and DPC
- 4—NPC and DPC
- 5—MPC (required)
- 6—NPC and DPC
- 7—NPC and DPC
- 8—NPC and DPC
- 9—NPC and DPC

The two slots on the back of the chassis support SFCs.

STEP 6 | (MPC only) Boot the appliance with the new MPC installed. When prompted, log in and reset the firewall to factory default settings.

STEP 7 | (MPC only) Restore your previous device configuration.

Replace a PA-7500 Series Firewall Interface Card in a NGFW Cluster

If your PA-7500 firewall is in a NGFW Clustering configuration, there are additional steps to take when removing and replacing an MPC, NPC, DPC, or SFC. These procedures vary from card to card and make reference to the steps of physically uninstalling and installing the hardware.

- Replace a PA-7500 Series Firewall MPC in a NGFW Cluster
- Replace a PA-7500 Series Firewall NPC in a NGFW Cluster
- Replace a PA-7500 Series Firewall DPC in a NGFW Cluster
- Replace a PA-7500 Series Firewall SFC in a NGFW Cluster

Replace a PA-7500 Series Firewall MPC in a NGFW Cluster

STEP 1 | (If the faulty MPC still works and the node is connected to Panorama)

1. Suspend the node either by using Panorama or the following CLI command: **`request cluster node state suspend`**.
2. Wait until the node is in the Suspended state. Verify the state using the following CLI command: **`show cluster local state`**.

STEP 2 | Disconnect all connections to and from the MPC, then power off the firewall.

STEP 3 | Unlock the MPC and remove it from the chassis.

STEP 4 | Install the replacement MPC.

STEP 5 | Reconnect all connections to and from the MPC, then power on the firewall.

STEP 6 | Log in to the serial console of the firewall using a terminal emulation application such as PuTTY, then perform a factory reset of the firewall.

STEP 7 | After the factory reset has completed, connect to the MPC through the serial console and re-configure the management IP address. **Commit** the change and verify that there is a management network connection.

STEP 8 | Reconfigure your network settings such as hostname, management IP, and DNS servers.

STEP 9 | Connect to the firewall's management IP and retrieve the license for the device. Upgrade the device to the same software version as the former node of the cluster.

STEP 10 | Reconfigure your Panorama server and **commit** the changes. Verify that the node is connected.

If Panorama shows the node as `not connected`, reset the connection to Panorama.

STEP 11 | After the node has reconnected to Panorama, issue the following command to initiate the cluster update to the node: **`request cluster-update name [cluster_name]`**. Once the update is finished, the node reboots.

STEP 12 | Use either Panorama or the CLI to push the firewall cluster from Panorama to the cluster on the node.

- **Panorama**— Select **Commit**, then **Push to Devices**. Select the firewall cluster tab, then **Push** the cluster configuration.
- **CLI**— Enter the following command: **`commit-all firewall-cluster name [cluster_name]`**.

Use the following command to monitor the cluster setup progress: ***`show cluster local state`***.

STEP 13 | Verify that all the nodes in the cluster are online by issuing the following command: **`show cluster nodes`**.

STEP 14 | From Panorama, re-push the template and device-group settings to the cluster. Select **Commit**, then **Push to Devices**.

Replace a PA-7500 Series Firewall NPC in a NGFW Cluster

STEP 1 | Disconnect all connections to and from the NPC.

If this NPC is still functioning prior to replacement, any traffic using orphan ports or LAGs may encounter interruption during this procedure.

STEP 2 | Unlock the NPC and remove it from the chassis.

STEP 3 | Install the replacement NPC.

STEP 4 | Reconnect all the connections to and from the new NPC, including any transceivers that were previously installed.

STEP 5 | Verify the slot and serial number of the new NPC using the following CLI command: **`show chassis inventory`**.

STEP 6 | Monitor the NPC boot process using the following command: **`show chassis status slot [0]`** where [0] is the number of the slot in which the new NPC is installed.

STEP 7 | Once the NPC is up, verify that all existing links and network connections are working.

Replace a PA-7500 Series Firewall DPC in a NGFW Cluster

STEP 1 | Unlock the DPC and remove it from the chassis.

STEP 2 | Install the replacement DPC.

STEP 3 | Verify the slot and serial number of the new DPC using the following CLI command: **`show chassis inventory`**.

STEP 4 | Monitor the DPC boot process using the following command: **`show chassis status slot [0]`** where [0] is the number of the slot in which the new DPC is installed. When the DPC is fully online, the **`Card Status`** reads **`Up`**.

Replace a PA-7500 Series Firewall SFC in a NGFW Cluster

STEP 1 | (If the faulty SFC still works and the node is connected to Panorama)

1. Suspend the node either by using Panorama or the following CLI command: **`request cluster node state suspend`**.
2. Wait until the node is in the Suspended state. Verify the state using the following CLI command: **`show cluster local state`**.

STEP 2 | Power off the firewall.

STEP 3 | Unlock the SFC and remove it from the chassis.

STEP 4 | Install the replacement SFC.

STEP 5 | Log in to the serial console of the firewall using a terminal emulation application such as PuTTY, then perform a factory reset of the firewall.

STEP 6 | After the factory reset has completed, connect to the MPC through the serial console and re-configure the management IP address. **Commit** the change and verify that there is a management network connection.

STEP 7 | Reconfigure your network settings such as hostname, management IP, and DNS servers.

STEP 8 | Connect to the firewall's management IP and retrieve the license for the device. Upgrade the device to the same software version as the former node of the cluster.

STEP 9 | Reconfigure your Panorama server and **commit** the changes. Verify that the node is connected.

If Panorama shows the node as `not connected`, reset the connection to Panorama.

STEP 10 | After the node has reconnected to Panorama, issue the following command to initiate the cluster update to the node: **`request cluster-update name [cluster_name]`**. Once the update is finished, the node reboots.

STEP 11 | Use either Panorama or the CLI to push the firewall cluster from Panorama to the cluster on the node.

- **Panorama**— Select **Commit**, then **Push to Devices**. Select the firewall cluster tab, then **Push** the cluster configuration.
- **CLI**— Enter the following command: **`commit-all firewall-cluster name [cluster_name]`**.

Use the following command to monitor the cluster setup progress: ***`show cluster local state`***.

STEP 12 | Verify that all the nodes in the cluster are online by issuing the following command: **`show cluster nodes`**.

STEP 13 | From Panorama, re-push the template and device-group settings to the cluster. Select **Commit**, then **Push to Devices**.

Replace a PA-7500 Series Firewall Fan Assembly

The PA-7500 Series firewall can support up to fifteen dual-rotor, single fan assemblies on its rear side. Each single fan assembly can be individually removed and replaced. When a fan is functioning as expected, the LED on the fan assembly will be green. If a fan fails, the fault LED on the fan assembly will turn red. If this occurs, replace the fan immediately to avoid service interruption. If two or more fans fail, the firewall shuts down.

You can replace a failed fan assembly while the firewall is powered on; however, you must use the CLI to view the non-failed fan speeds to assess how much time you have before the thermal protection circuit automatically shuts down the firewall. Issue the following command to check the speed of the fans that you are not replacing:

```
admin@PA-7500> show system environmentals fans
```

If the non-failed fans are operating at less than 12,000 RPM, there is no absolute time limit to replace the fan assembly.

If the non-failed fans are operating at 12,000 RPM or higher, or if there are two or more fans missing, there is a time limit of 120 seconds starting when the fan assembly is removed to replace it before the thermal protection circuit automatically powers down the firewall.

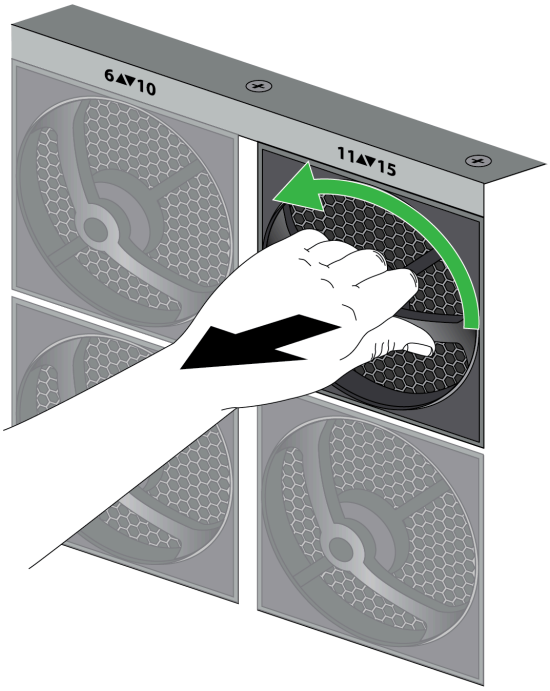
STEP 1 | Put the provided ESD wrist strap on your wrist ensuring that the metal contact is touching your skin. Then attach (snap) one end of the ground cable to the wrist strap and remove the alligator clip from the banana clip on the other end of the ESD grounding cable. Plug the banana clip end into the ESD port located on the appliance before handling ESD sensitive hardware.

When removing a fan assembly, first pull the fan assembly out about 1 inch (2.5cm) and wait 10 seconds. This allows enough time for the working fans to stop spinning.

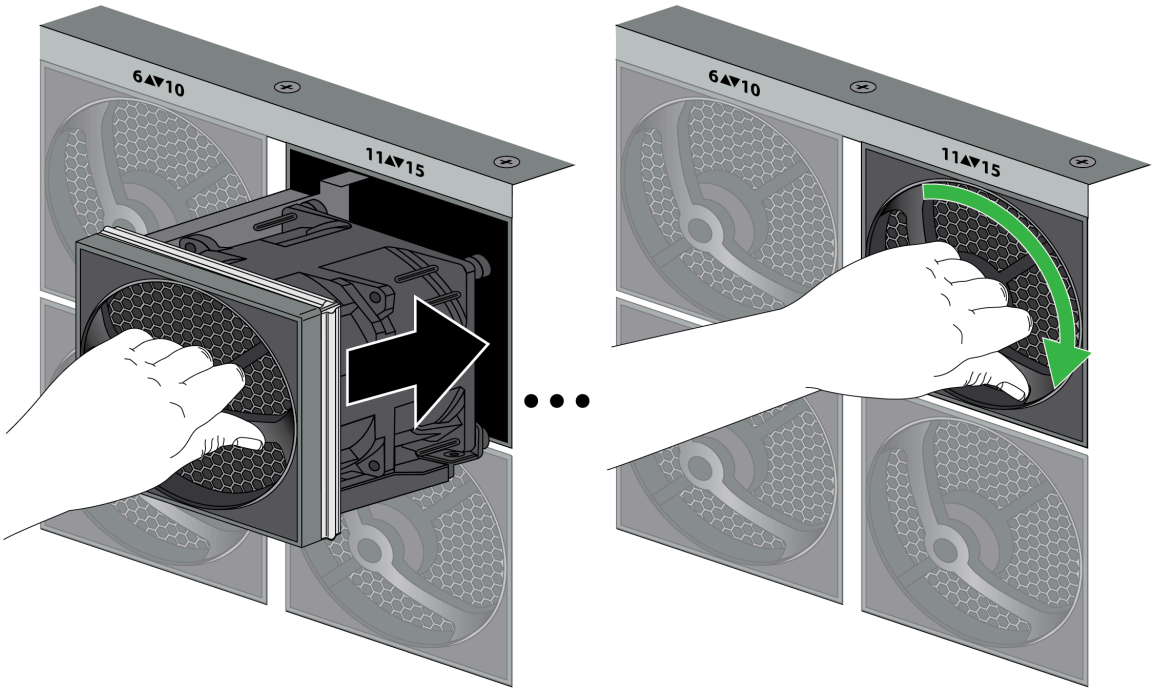
STEP 2 | Remove the replacement fan assembly from the packaging and have it ready.

STEP 3 | Identify the failed fan assembly by checking the fault LEDs of each fan. In the event of a failure, the LED on the fan assembly will be red.

STEP 4 | Grip the failed fan assembly by the handle and turn it to the left. Gently pull the fan assembly out of its slot.



STEP 5 | Install the replacement fan by sliding it into the vacant fan slot. Turn the handle to the right to secure the fan assembly in place.



STEP 6 | Verify that the new fan assembly is operational by noting the status of the fan assembly LED and the fan LED on the Management Processing Card (MPC). The individual fan assembly LED shows green if it is functioning as expected. Similarly, the fan LED on the MPC also

shows green if all fans are working as expected. You can also view the status of the fan trays by entering the following command:

```
admin@PA-7500> show system environmentals fan-tray
```

To view the status of each fan on a fan tray, run the following command:

```
admin@PA-7500> show system environmentals fans
```

Replace a PA-7500 Series Firewall System Drive

The Network Processing Card (NPC) and Data Processing Card (DPC) each feature a single Solid State Drive (SSD) containing the files of the PA-7500 Series firewall. The procedure to replace the SSD in each card is similar.

STEP 1 | Identify the failed drive and determine the drive model using the **`show system raid detail`** CLI command.

When the system drives are functioning normally, all system drive partitions show both drives with the status `clean`. If a system drive fails, the `Overall System Drives RAID status` shows `degraded`, one or more failed partition array shows `clean`, `degraded`.

STEP 2 | Remove the failed drive from the RAID 1 array. In this example, run the following command to remove drive `Sys1` from the array:

```
admin@PA-7500> request system raid remove sys1
```

STEP 3 | Confirm that the failed drive is removed from all partitions.

STEP 4 | Ensure that you have access to an ESD work surface for placement of the interface card.

STEP 5 | Put the provided ESD wrist strap on your wrist ensuring that the metal contact is touching your skin. Then attach (snap) one end of the ground cable to the wrist strap and remove the alligator clip from the banana clip on the other end of the ESD grounding cable. Plug the banana clip end into the ESD port located on the chassis before handling ESD sensitive hardware.

STEP 6 | Remove the NPC or DPC from the chassis. See Replace a PA-7500 Series Firewall Interface Card for details on removing an interface card.

STEP 7 | Place the interface card on an ESD work surface. Detach your wrist strap's ground cable from the ESD port on the appliance and securely attach the alligator clip to the new ESD surface.

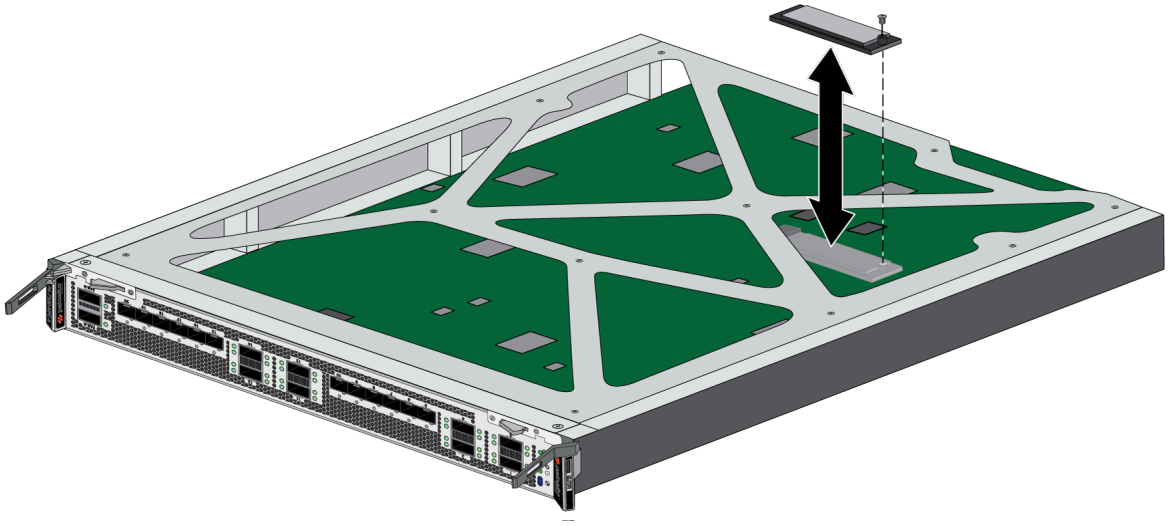
STEP 8 | Locate the SSD by flipping the interface card upside down. The SSD is located under the metal plate. See Step 10 for images identifying the SSD locations.

STEP 9 | Remove the retention screw for the SSD.

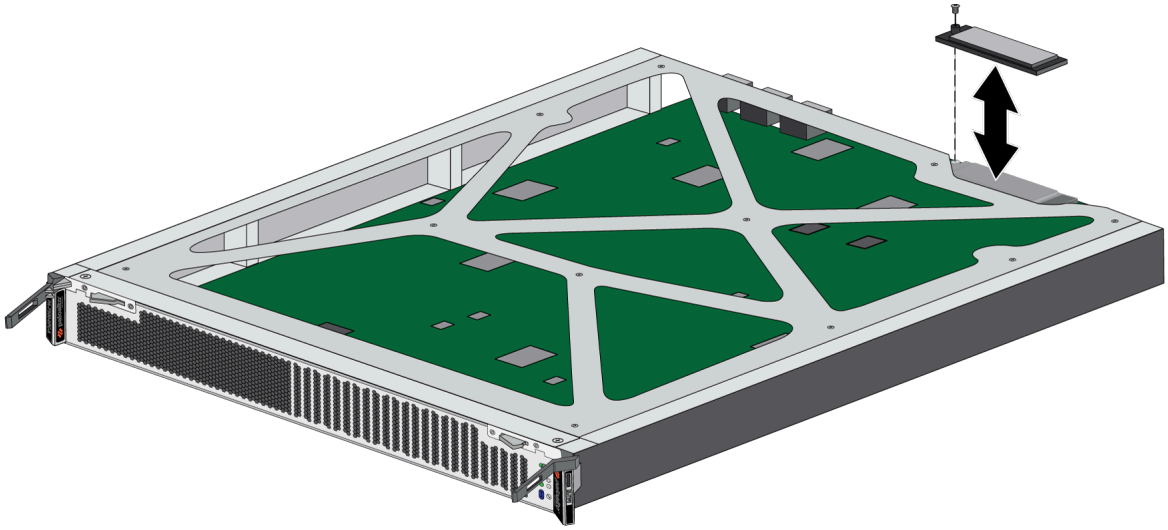
The plastic standoff becomes loose after the retention screw is removed. Do not lose the standoff as it is needed when installing the new SSD.

STEP 10 | Gently pull the SSD away from its mating connector. Place the old SSD to the side.

NPC



DPC



STEP 11 | Slide the new SSD into the vacant mating connector. Ensure that the SSD aligns with the plastic standoff on the card.

STEP 12 | Fasten the retention screw back into place at a torque of 4 in-lbs.

Exceeding a torque of 4 in-lbs will damage the equipment.

STEP 13 | Before re-installing the interface card into the chassis, plug the banana clip end of your ESD wrist strap into one of the ESD ports located on the chassis.

STEP 14 | Slide the interface card back into its slot. See Install a PA-7500 Series Firewall Interface Card for more information.

Replace a PA-7500 Series Firewall Logging Drive

The Management Processing Card (MPC) contains two slots for logging drives. The following procedure describes how to install or replace a logging drive.

STEP 1 | Identify the failed drive and determine the drive model by running the following operational command:

```
admin@PA-7500> show system disk details
```

STEP 2 | Remove the failed drive by running the following command:

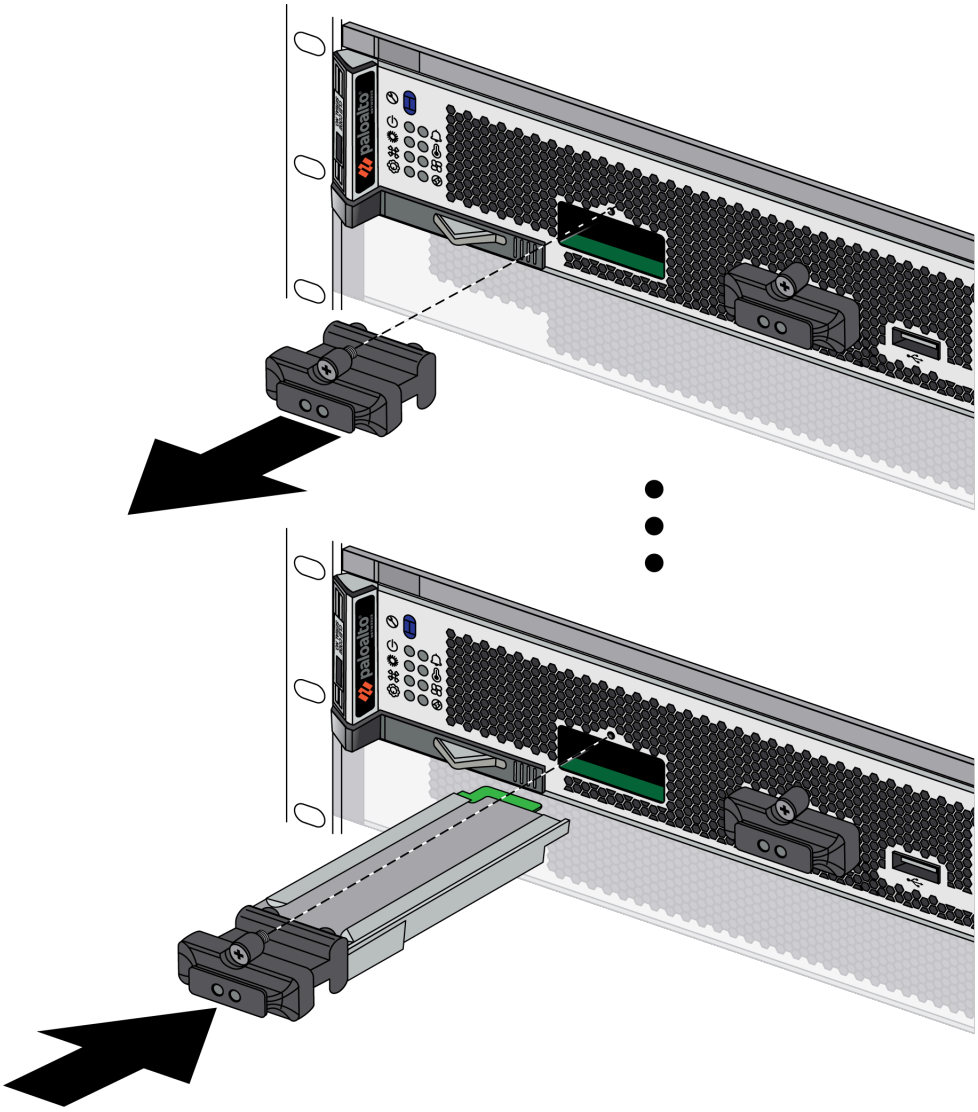
```
admin@PA-7500> request system disk remove <name of disk>
```

STEP 3 | Attach an ESD strap to your wrist and plug the other end in to the ESD port location on the chassis.

STEP 4 | Loosen the retaining screw on the logging drive blank cover while gently pulling on the pull tab. Proceed until the logging drive blank cover can be pulled out from the MPC faceplate.

STEP 5 | Remove the failed logging drive from the opening in the MPC faceplate.

STEP 6 | Insert the replacement logging drive. Align the retainer screw with the threaded hole in the MPC faceplate.



STEP 7 | Once the logging drive is fully seated, tighten the retainer screw to 4 in-lbs.

Exceeding a torque of 4.5 in-lbs will damage the equipment.

STEP 8 | Add the logging drive to the system. Enter the following CLI command:

```
admin@PA-7500> request system disk add nvme0n1
```

Executing this command will delete all data on the drive being added.

Adding the logging drive can take a few minutes. Use ***admin@PA-7500> show system disk details*** *to check the status. The* **Reason** *field displays* `Admin enabled` *when the process is complete.*

STEP 9 | Enable the newly added logging drive by entering the following CLI command:

```
admin@PA-7500> request logdb-migrate logging-drive start
```

The firewall automatically reboots after enabling the new logging drive.

PA-7500 Series Firewall Specifications

PA-7500 Series Firewall Physical Specifications

The following table describes the PA-7500 Series firewall physical specifications.

Specification	Value
Rack units	**Rack units**—14RU
Dimensions	**Chassis** • Height—24.4" (61.98 cm) • Depth—31.0" (78.74 cm) • Width—17.4" (44.20 cm) **Front slot card (MPC, DPC, and NC)** • Height—2.1" (5.33 cm) • Depth—20.7" (52.58 cm) • Width—16.6" (42.16 cm) **Switch fabric card (SFC)** • Height—21.4" (54.36 cm) • Depth—10.8" (27.43 cm) • Width—2.1" (5.33 cm) **Power supply** • Height—1.6" (4.06 cm) • Depth—20.9" (53.09 cm) • Width—2.7" (6.86 cm)
Weight	**Chassis**—Up to 460 lbs (208.65 kg) depending on installed components. **Management processing card (MPC)**—18.5 lbs (8.39 kg) **Network processing card (NPC)**—21.3 lbs (9.66 kg) **Data processing card (DPC)**—19.75 lbs (8.96 kg) **Switch fabric card (SFC)**—12.9 lbs (5.85 kg) **Fan assembly**—2 lbs (0.91 kg) **Power supply (AC)**—4.6 lbs (2.09 kg) **Power supply (DC)**—4.8 lbs (2.18 kg)
Power supply configurations	Ten AC or DC power supplies. The AC and DC power supplies are hot-swappable.

PA-7500 Series Firewall Electrical Specifications

PA-7500 Series Firewall Component Electrical Specifications

The following table describes the PA-7500 Series firewall power consumption values for the hardware components at different levels of load. The first table includes different values for a chassis operating at 25°C (77° F) and the second table covers a chassis operating at 40°C (104° F). For power configuration planning, see Determine Power Requirements of the PA-7500 Series Firewalls.

25°C				
Component	**Quantity**	**Idle (Watts)**	**Typical (Watts)**	**Fully Loaded (Watts)**
Management Processing Card (MPC)	1	337W	428W	450W
Network Processing Card (NPC)	1	533W	563W	570W
Data Processing Card (DPC)	1	531W	971W	1,081W
Switch Fabric Card (SFC)	1	303W	318W	321W
Fan Assembly	15	1,095W	1,095W	1,095W

40°C				
Component	**Quantity**	**Idle (Watts)**	**Typical (Watts)**	**Fully Loaded (Watts)**
Management Processing Card (MPC)	1	347W	582W	640W
Network Processing Card (NPC)	1	553W	593W	603W

40°C				
Component	**Quantity**	**Idle (Watts)**	**Typical (Watts)**	**Fully Loaded (Watts)**
Data Processing Card (DPC)	1	558W	994W	1,103W
Switch Fabric Card (SFC)	1	308W	327W	331W
Fan Assembly	15	2,310W	2,310W	2,310W

PA-7500 Series Firewall Power Cord Types

The PA-7500 Series firewalls ship with four AC or four DC power supplies by default. You can order up to six additional power supplies (ten total) and power cords are included with each power supply.

The table below lists all the power cords supported on the PA-7500 Series firewall.

SKU Number	Description
PAN-PWR-C19-AUS	AC power cord with IEC-60320 C19 and AS/NZS 4417 cord ends, 3 m
PAN-PWR-C19-EU	AC power cord with IEC-60320 C19 and CEE 7/7 SCHUKO cord ends, 3 m
PAN-PWR-C19-JP	AC power cord with IEC-60320 C19 and NEMA L6-20P cord ends, 3 m
PAN-PWR-C19-TW	AC power cord with IEC-60320 C19 and CNS 10917-3 cord ends, 3 m
PAN-PWR-C19-UK	AC power cord with IEC-60320 C19 and BS 1363 UK13 cord ends, 3 m
PAN-PWR-C19-US	AC power cord with IEC-60320 C19 and NEMA 6-20P cord ends, 3 m
PAN-PWR-C19-US-L	AC power cord with IEC-60320 C19 and locking NEMA L6-20P cord ends, 3 m
PAN-PWR-C19-BR	Power Cord, Brazil, 16A, 250V, NBR14136 (IEC 60906-1) to IEC-60320-C19, 10-FT, Brazilian INMETRO certified
PAN-PWR-C19-C20	Power Cord, North America, 20A, 250V, IEC C19 to IEC C20, 10ft

SKU Number	Description
PAN-PWR-C19-C14	Power Cord, North America, 15A, 250V, IEC C19 to IEC C14, 10ft
PAN-PWR-C19-US-120V	Power Cord, North America, 15A, 125V, C19 to NEMA 5-15P, 10ft
PAN-PWR-C19-JP-120V	Power Cord, Japan, 15A, 125V, JISC8303 to C19, 10ft, PSE Certified

PA-7500 Series Firewall Environmental Specifications

The following table describes PA-7500 Series firewall environmental specifications.

Specification	Value
Operating temperature range	0° to 50°C (32°F to 122°F)
Storage temperature range	-20° to 70°C (-4°F to 158°F)
Humidity	5% to 90% non-condensing
Chassis airflow	Front-to-back

PA-7500 Series Firewall Compliance Statements

Palo Alto Networks obtains regulatory compliance certifications to comply with the laws and regulations in each country where there are requirements applicable to our products. Our products meet standards for product safety and electromagnetic compatibility when used for their intended purpose.

To view compliance statements for the PA-7500 Series firewalls, see Compliance Statements.

Compliance Statements

The following are the PA-7500 Series firewall hardware statements:

- **VCCI**

  This section provides the compliance statement for the Voluntary Control Council for Interference by Information Technology Equipment (VCCI), which governs radio frequency emissions in Japan.

  The following information is in accordance to VCCI Class A requirements:

  この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI-A

  Translation: This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take corrective actions.

- **NEBS Requirements**

  The following lists the Network Equipment Building System (NEBS) requirements for PA-7500 Series firewalls.

  - The firewall is intended to be installed in a Network Telecommunication Facility (Central Office) as part of a Common Bonding Network (CBN) or Isolated Bonding Network (IBN). Bare conductors must be coated with an appropriate antioxidant compound before crimp connections are made. All unplated connectors, braided strap, and bus bars must be brought to a bright finish and then coated with an antioxidant before they are connected.
  - Fastening hardware must be compatible with the materials being joined and must preclude loosening, deterioration, and electrochemical corrosion of the hardware and the joined materials.
  - The firewall is suitable for connection to the Central Office or Customer Premise Equipment (CPE).
  - The DC battery return wiring on the firewall must be connected as an isolated DC return (DC-I).

  The intra-building ports (RJ-45 Ethernet ports, AUX ports, HA ports, and the MGT port) of the equipment or subassembly are suitable for connection to only intra-building or unexposed wiring or cabling. The intra-building port(s) of the equipment or subassembly must not be metallically connected to interfaces that connect to the Outside Plant (OSP) or its wiring. These interfaces are designed for use as intra-building interfaces only (Type 2 or Type 4 ports as described in GR-1089-CORE, Issue 6) and require isolation from the exposed OSP cabling. The addition of primary protectors is not sufficient protection to connect these interfaces metallically to OSP wiring.

  The firewall must be connected to an external Special Protection Device (SPD) when installed and connected to commercial AC power.

- **BSMI EMC Statement**—User warning: This is a Class A product. When used in a residential environment it may cause radio interference. In this case, the user will be required to take adequate measures.
  - **Manufacturer**—Flextronics International.
  - **Country of Origin**—Made in the USA with parts of domestic and foreign origin.
- **CE (European Union (EU) Electromagnetic Compatibility Directive)**—This device is herewith confirmed to comply with the requirements set out in the Council Directive on the Approximation of the Laws of the Member States relating to Electromagnetic Compatibility Directive (2014/30/EU).

  The above product conforms with Low Voltage Directive 2014/35/EU and complies with the requirements relating to electrical equipment designed for use within certain voltage limits.
- **Federal Communications Commission (FCC) statement for a Class A digital device or peripheral**—This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
  - Reorient or relocate the receiving antenna.
  - Increase the separation between the equipment and receiver.
  - Connect the equipment to an outlet on a circuit that is different from the one to which the receiver is connected.
  - Consult the dealer or an experienced radio/TV technician for help.
- **ICES (Canadian Department Compliance Statement)**—This Class A digital apparatus complies with Canadian ICES-003.

  French translation: Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.
- **Korean Communications Commission (KCC) Class A Statement**—This equipment is an electromagnetic compatible device for business purposes (Class A). The provider or user should be aware that the equipment is intended for use outside the home.
- **Technischer Überwachungsverein (TUV)**

Risk of explosion if battery is replaced by an incorrect type. Dispose of used battery according to local regulations.

