paloalto TECHDOCS

PA-500 Series 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

July 29, 2025

Table of Contents

Before You Begin

Read the following topics before you install or service the PA-500 Series firewall.

- Safety and Compliance
- Parts List and Required Tools

Safety and Compliance

Read the Safety Warnings prior to installing the PA-500 Series firewall hardware. This section also lists compliance and regulatory statements that apply to the firewall.

- Safety Warnings
- Compliance Statements
- Tamper Proof Statement
- Third-Party Component Support

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.

- 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).
- 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.
- 

  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.

- 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.

Compliance Statements

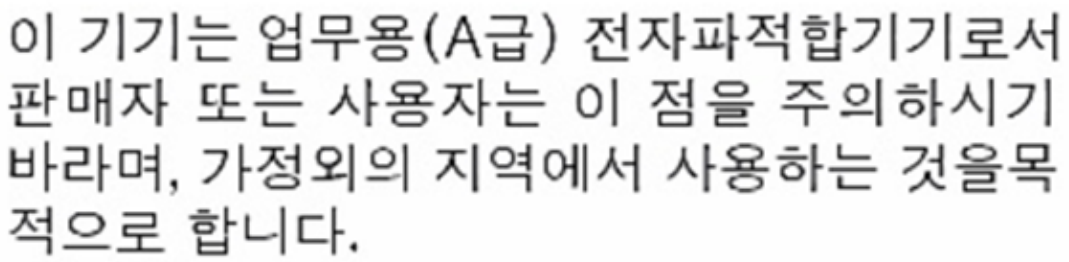
The following lists the PA-500 Series firewall hardware compliance statements:

- **BSMI EMC Statement**: 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.
- **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.
  - (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.
- **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 requirements relating to electrical equipment designed for use within certain voltage limits.

- **KCC**: 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.

- **Product Safety**: Product Ambient Temperature:
  - 0~40 degrees C

  Risk of explosion if battery is replaced by an incorrect type. Dispose of used battery according to local regulations.
- **Federal Communications Commission (FCC) statement for a Class A and B digital device or peripheral**
  - Class A requirements

    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:
    - 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**
  - (Class A requirements)

    This Class A digital apparatus complies with Canadian ICES-003. Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.
- **United Kingdom Declaration of Conformity (UKCA) Directives**
  - This equipment complies with the requirements set out in the UK Electrical Equipment (Safety) Regulations 2016 and Electromagnetic Compatibility Regulations 2016.

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.

Third-Party Component Support

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

Parts List and Required Tools

The following table lists the items that are shipped with the PA-500 Series firewall.

Table 1: Parts List

Quantity	Item
1	PA-500 Series Firewall
1	Ethernet cable
1	USB to Micro USB Console Cable
1	AC Power Adapter

The following tools are either required or recommended when installing the PA-500 Series firewall hardware.

- ESD wrist strap
- Equipment rack screws
- #1 Phillips-head screwdriver

PA-500 Series Firewall Overview

The Palo Alto Networks® PA-500 Series Next-Generation firewalls include the PA-520, PA-540, PA-545-POE, PA-550, PA-555-POE, and PA-560. These firewalls are designed for small organizations or branch offices and include the following main features: a TPM module for PAN-OS key storage and security, ZTP functionality, Power Over Ethernet (PoE) support for select models, and active/passive and active/active high availability (HA). All PA-500 Series firewalls can make use of dual power adapters for load sharing and power redundancy (the second power adapter is sold separately). The PA-500 Series firewall enables you to secure your organization through advanced visibility and control of applications, users, and content.

First Supported PAN-OS® Software Releases:

- **PAN-OS 12.1.2** — PA-520, PA-540, PA-545-POE, PA-550, PA-555-POE, and PA-560
- PA-500 Series Firewall Front Panel
- PA-500 Series Firewall Back Panel

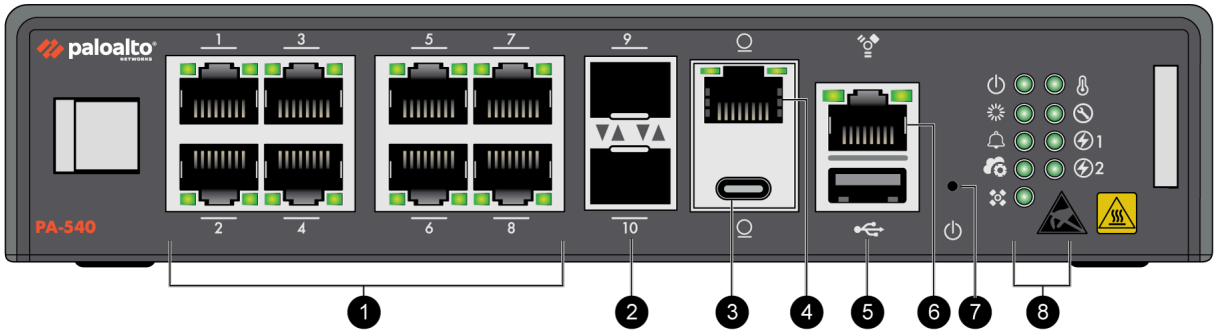
PA-500 Series Firewall Front Panel

View the front panel components of your PA-500 Series firewall.

- PA-520 and PA-540
- PA-550 and PA-560
- PA-545-POE and PA-555-POE

To review the specifications of supported Palo Alto Networks® interfaces and transceivers, refer to the datasheet.

The following image shows the front panel of the PA-520 and PA-540, which have similar front panel components (PA-540 pictured). The main difference is that the PA-520 does not have SFP ports. The table describes each front panel component.

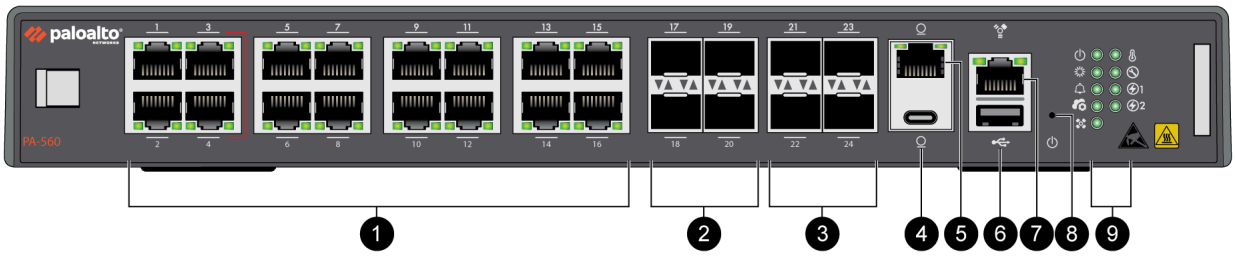


Item	Component	Description
1	RJ-45 Ports	Eight copper RJ-45 10Mbps/100Mbps/1Gbps ports for network traffic. *Port 1 is a Zero Touch Provisioning (ZTP) port. The ZTP port can be used to automatically provision the firewall.*
(PA-540 only) 2	SFP Ports	Two SFP 1Gbps ports for network traffic.
3	Console port	Use this port to connect a management computer to the

Item	Component	Description
	(USB-C)	firewall using a standard USB-C cable. The console connection provides access to firewall boot messages, the Maintenance Recovery Tool (MRT), and the command line interface (CLI).
4	Console port (RJ-45)	Use this port to connect a management computer to the firewall using a RJ-45 to USB cable and terminal emulation software. The console connection provides access to firewall boot messages, the Maintenance Recovery Tool (MRT), and the command line interface (CLI). Use the following settings to configure your terminal emulation software to connect to the console port: • Data rate: 115200 • Data bits: 8 • Parity: none • Stop bits: 1 • Flow control: None
5	USB Port	One USB port for debugging and administration only. Use the port to bootstrap the firewall. Bootstrapping enables you to provision the firewall with a specific PAN-OS configuration and then license it and make it operational on your network.
6	Management Port	Use this RJ-45 1Gbps port to access the management web interface and perform administrative tasks. The

Item	Component	Description
		firewall also uses this port for management services, such as retrieving licenses and updating threat and application signatures.
7	Reset Button	A pin press reset button that can be used to gracefully shut down the firewall.
8	LED Status Indicators	Nine LEDs that indicate the status of the firewall hardware components (see PA-500 Series Firewall LED Definitions).

The following image shows the front panel of the PA-550 and PA-560, which have similar front panel components (PA-560 pictured). The table describes each front panel component.



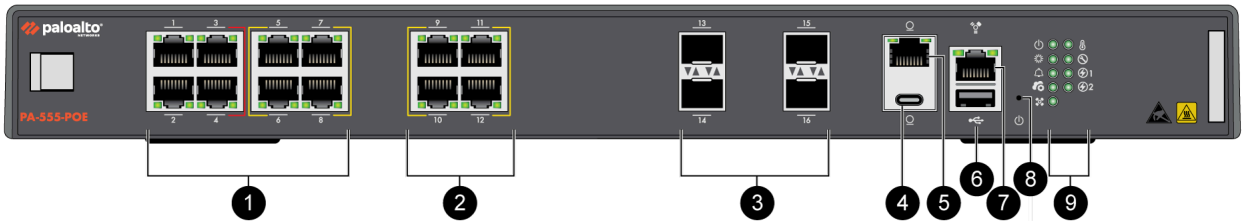
Item	Component	Description
1	RJ-45 Ports	**PA-550** Twelve copper RJ-45 10Mbps/100Mbps/1Gbps ports for network traffic. **PA-560** Sixteen copper RJ-45 10Mbps/100Mbps/1Gbps ports for network traffic.

Item	Component	Description
		Port 1 is a Zero Touch Provisioning (ZTP) port. The ZTP port can be used to automatically provision the firewall. *Ports 3 and 4 are fail-open ports. They can be configured to provide a pass-through connection despite power or operating system failure.*
2	SFP Ports	**PA-550** Two SFP 1Gbps ports for network traffic. (Ports 13 and 14) **PA-560** Four SFP 1Gbps ports for network traffic. (Ports 17 through 20)
3	SFP/SFP+ Ports	**PA-550** Two SFP/SFP+ 1Gbps/10Gbps ports for network traffic. (Ports 15 and 16) **PA-560** Four SFP/SFP+ 1Gbps/10Gbps ports for network traffic. (Ports 21 through 24)
4	Console port (USB-C)	Use this port to connect a management computer to the firewall using a standard USB-C cable.

Item	Component	Description
		The console connection provides access to firewall boot messages, the Maintenance Recovery Tool (MRT), and the command line interface (CLI).
5	Console port (RJ-45)	Use this port to connect a management computer to the firewall using a RJ-45 to USB cable and terminal emulation software. The console connection provides access to firewall boot messages, the Maintenance Recovery Tool (MRT), and the command line interface (CLI). Use the following settings to configure your terminal emulation software to connect to the console port: • Data rate: 115200 • Data bits: 8 • Parity: none • Stop bits: 1 • Flow control: None
6	USB Port	One USB port for debugging and administration only. Use the port to bootstrap the firewall. Bootstrapping enables you to provision the firewall with a specific PAN-OS configuration and then license it and make it operational on your network.
7	Management Port	Use this RJ-45 1Gbps port to access the management web interface and perform administrative tasks. The firewall also uses this port for management services, such as retrieving licenses

Item	Component	Description
		and updating threat and application signatures.
8	Reset Button	A pin press reset button that can be used to gracefully shut down the firewall.
9	LED Status Indicators	Nine LEDs that indicate the status of the firewall hardware components (see PA-500 Series Firewall LED Definitions).

The following image shows the front panel of the PA-545-POE and PA-555-POE, which have similar front panel components (PA-555-POE pictured). The table describes each front panel component.



Item	Component	Description
1	RJ-45 Ports	Eight copper RJ-45 10Mbps/100Mbps/1Gbps ports for network traffic. *Port 1 is a Zero Touch Provisioning (ZTP) port. The ZTP port can be used to automatically provision the firewall.*

Item	Component	Description
		Ports 3 and 4 are fail-open ports. They can be configured to provide a pass-through connection despite power or operating system failure. **PA-545-POE** Ports 9 through 12 are Power over Ethernet (PoE) ports that can transfer up to 181W of power to a connected device. **PA-555-POE** Ports 5 through 12 are Power over Ethernet (PoE) ports that can transfer up to 332W of power to a connected device.
2	RJ-45 mGig Ports	**PA-545-POE** Four RJ-45 mGig 1Gbps/2.5Gbps ports for network traffic. Ports 9 through 12 are Power over Ethernet (PoE) ports that can transfer up to 181W of power to a connected device. **PA-555-POE** Four RJ-45 mGig 1Gbps/2.5Gbps ports for network traffic. Ports 5 through 12 are Power over Ethernet (PoE) ports that can transfer up to 332W of power to a connected device.
3	SFP/SFP+ Ports	**PA-545-POE** Four SFP 1Gbps ports for network traffic. (Ports 13 through 16) **PA-555-POE**

Item	Component	Description
		Four SFP/SFP+ 1Gbps/10Gbps ports for network traffic. (Ports 13 through 16 support SFP; Ports 15 and 16 support SFP+)
4	Console port (USB-C)	Use this port to connect a management computer to the firewall using a standard USB-C cable. The console connection provides access to firewall boot messages, the Maintenance Recovery Tool (MRT), and the command line interface (CLI).
5	Console port (RJ-45)	Use this port to connect a management computer to the firewall using a RJ-45 to USB cable and terminal emulation software. The console connection provides access to firewall boot messages, the Maintenance Recovery Tool (MRT), and the command line interface (CLI). Use the following settings to configure your terminal emulation software to connect to the console port: • Data rate: 115200 • Data bits: 8 • Parity: none • Stop bits: 1 • Flow control: None
6	USB Port	One USB port for debugging and administration only. Use the port to bootstrap the firewall. Bootstrapping enables you to provision the firewall with a

Item	Component	Description
		specific PAN-OS configuration and then license it and make it operational on your network.
7	Management Port	Use this RJ-45 1Gbps port to access the management web interface and perform administrative tasks. The firewall also uses this port for management services, such as retrieving licenses and updating threat and application signatures.
8	Reset Button	A pin press reset button that can be used to gracefully shut down the firewall.
9	LED Status Indicators	Nine LEDs that indicate the status of the firewall hardware components (see PA-500 Series Firewall LED Definitions).

PA-500 Series Firewall Back Panel

View the back panel components of your PA-500 Series firewall.

- PA-520, PA-540, and PA-550
- PA-545-POE and PA-555-POE
- PA-560

The following image shows the back panel of the PA-520 and PA-540, which have similar back panel components (PA-540 pictured). The table describes each back panel component.

Item	Component	Description
1	Power Adapter Inputs	Two DC power inputs. One power supply is required, while a second power supply can be used for redundancy.
2	Ground Stud	Use the single post ground stud to connect the firewall to earth ground (ground cable not included).

The following image shows the back panel of the PA-550. The table describes each back panel component.

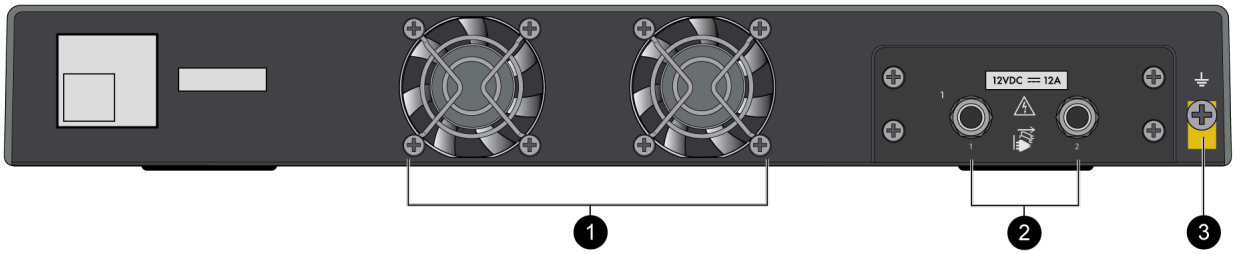
Item	Component	Description
1	Power Adapter Inputs	Two DC power inputs. One power supply is required, while a second power supply can be used for redundancy.

Item	Component	Description
2	Ground Stud	Use the single post ground stud to connect the firewall to earth ground (ground cable not included).

The following image shows the back panel of the PA-545-POE and PA-555-POE, which have similar back panel components. The table describes each back panel component.

Item	Component	Description
1	Power Adapter Inputs	Two DC power inputs. One power supply is required, while a second power supply can be used for redundancy.
2	Ground Stud	Use the single post ground stud to connect the firewall to earth ground (ground cable not included).

The following image shows the back panel of the PA-560. The table describes each back panel component.



Item	Component	Description
1	Fans	Two single-rotor fans that provide cooling to the firewall. The fans are not field replaceable.
2	Power Adapter Inputs	Two DC power inputs. One power supply is required, while a second power supply can be used for redundancy.

Item	Component	Description
3	Ground Stud	Use the single post ground stud to connect the firewall to earth ground (ground cable not included).

PA-500 Series Firewall Installation

Use the following topics to install and set up the PA-500 Series firewall hardware.

- Install the PA-500 Series Firewall in an Equipment Rack
- Set Up a Connection to the PA-500 Series Firewall
- Connect Power to the PA-500 Series Firewall

Install the PA-500 Series Firewall in an Equipment Rack

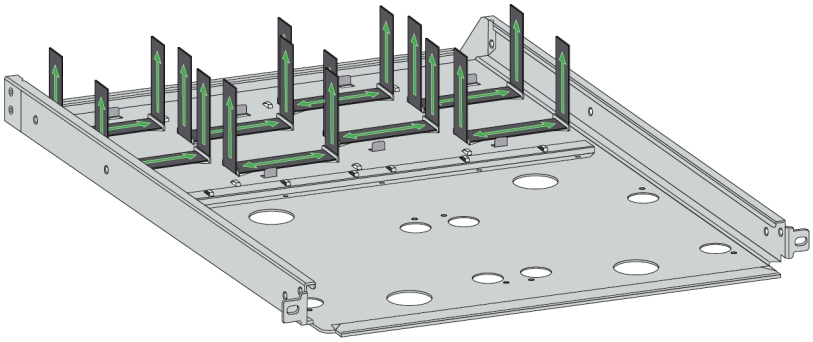
There are different rack mount SKUs that enable you to install a PA-500 Series firewall in a four-post 19" rack. The rack mount SKU used and the number of firewalls you can install depends on which PA-500 Series firewall you are installing.

- **PA-520 and PA-540** — Up to two firewalls (with up to two power adapters each) can be installed in the PAN-1RU-4POST-RACK-11.
- **PA-550 and PA-560** — One firewall and up to two power adapters can be installed in the PAN-1RU-4POST-RACK-11.
- **PA-545-POE and PA-555-POE** — One firewall and up to two power adapters can be installed in the PAN-1RU-4POST-RACK-12.

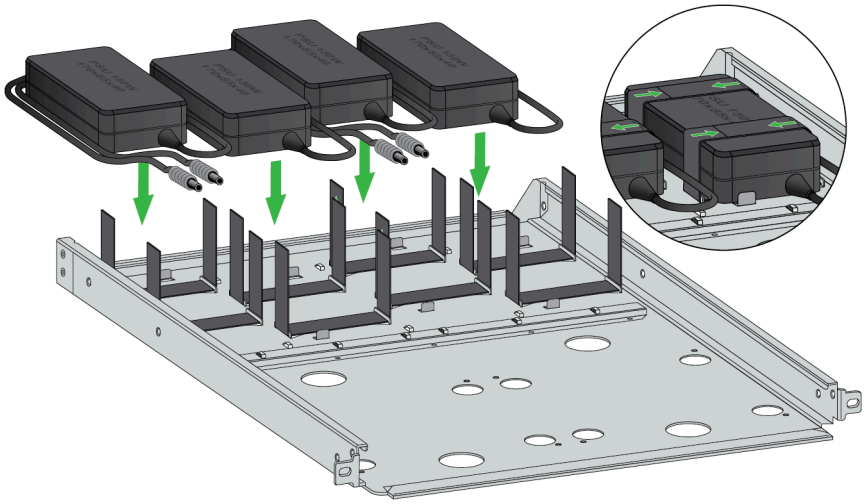
STEP 1 | Secure the power adapter(s) to the mounting tray.

PAN-1RU-4POST-RACK-11

1. For each power adapter being installed (for a maximum of four for the PA-520 and PA-540 and a maximum of two for the PA-550 and PA-560), feed two Velcro straps through the openings at the dedicated power adapter locations on the mounting tray.

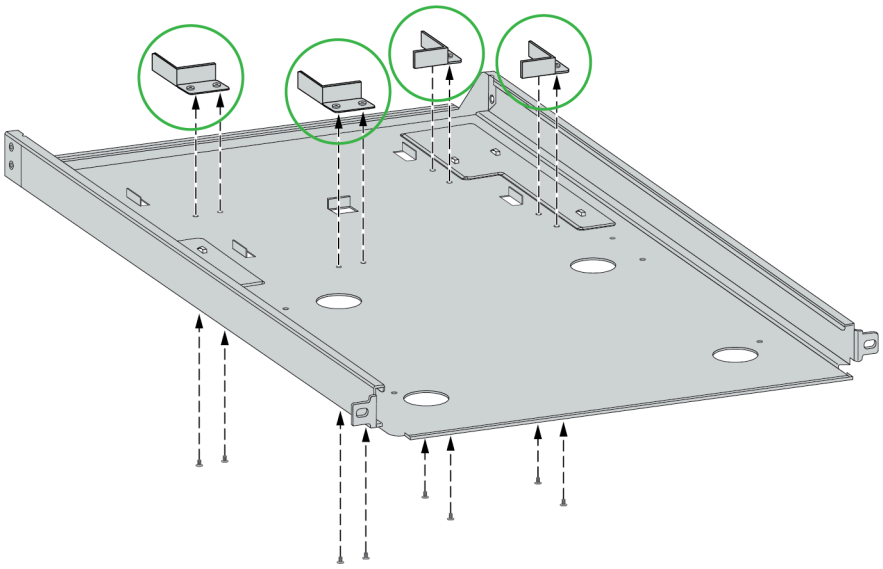


2. Place each power adapter into its designated location, then wrap both Velcro straps over the top of the adapter so that the adapter is fixed in place.

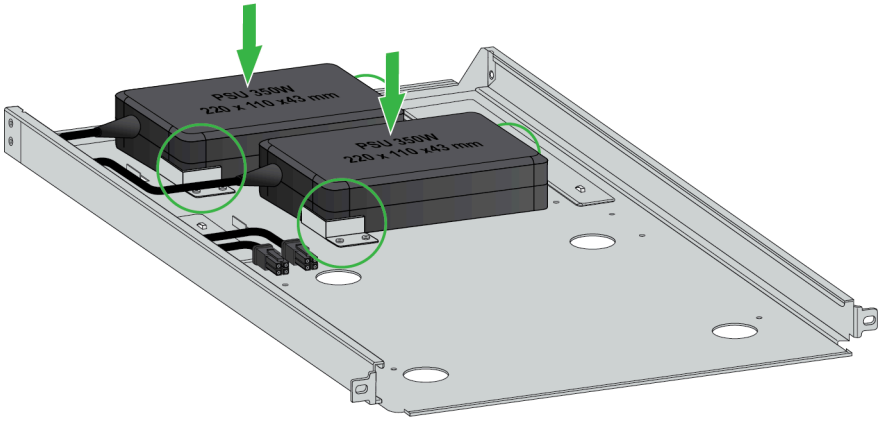


PAN-1RU-4POST-RACK-12

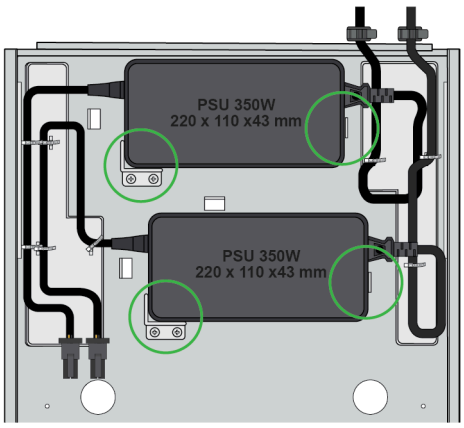
1. For each power adapter being installed (for a maximum of two), install two stoppers into the designated locations on the mounting tray. Use two #6-32 screws to secure each stopper from the underside of the mounting tray.



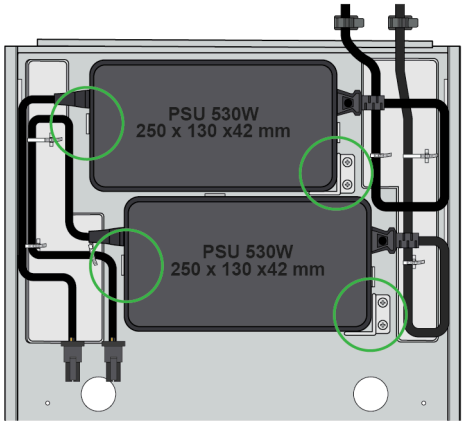
2. Place each power adapter into the location between the two installed stoppers.



350W Power Adapter



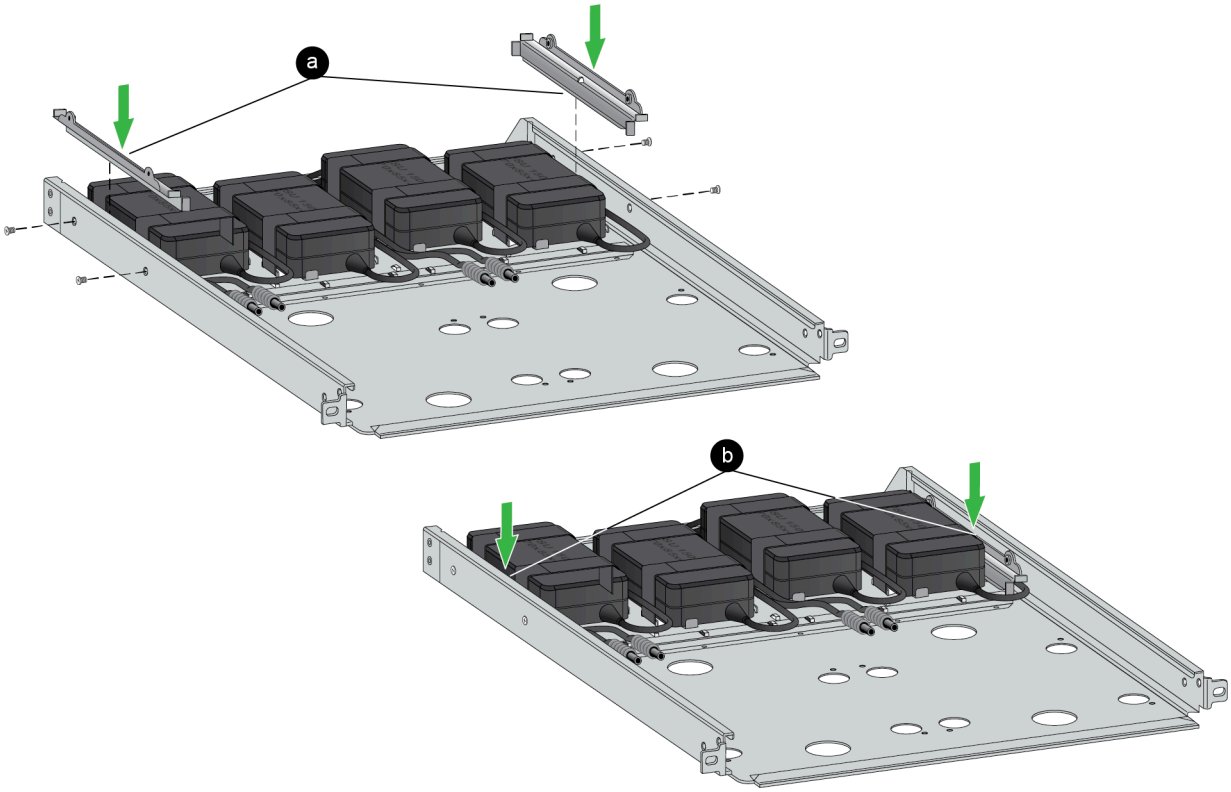
530W Power Adapter



STEP 2 | Route the power cables through paths on the mounting tray.

PAN-1RU-4POST-RACK-11

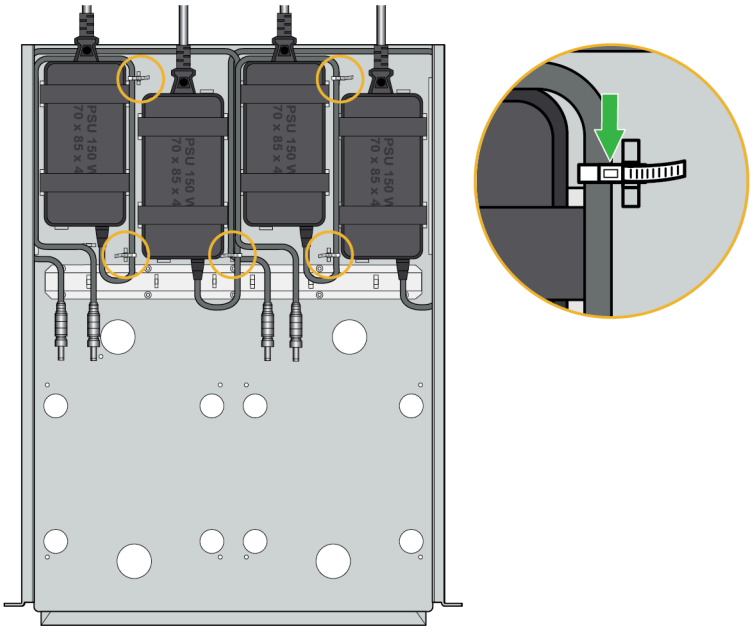
1. Route the initial segment of the power cables (that plugs into the firewall) along the wall of the mounting tray. Use two #6-32 screws to install a routing cover over each wall of the mounting tray so that the power cable is contained within.



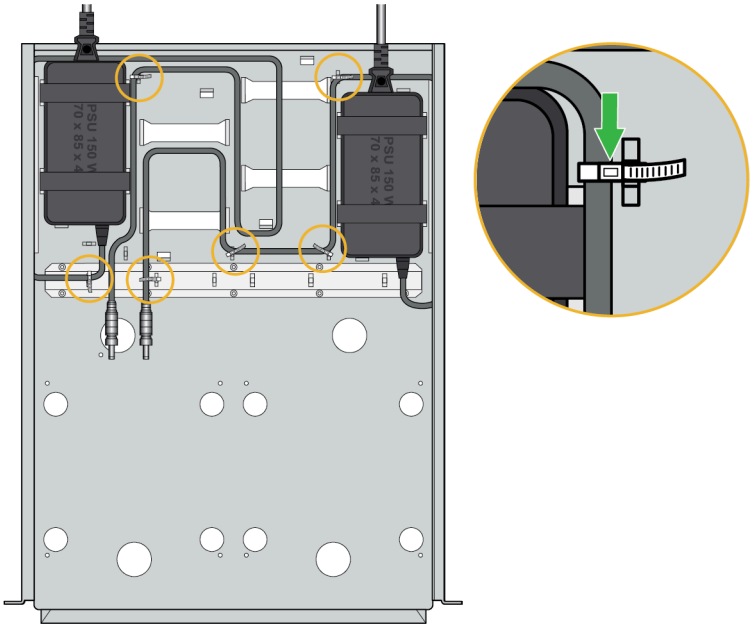
2. Using the following images as references, guide the remaining length of the power cables along the mounting tray. Thread the provided cable ties through the lances and cutouts in

the mounting tray. Wrap the cable ties around the power cables, ensuring that the power cables are fixed in place.

PA-520 and PA-540



PA-550 and PA-560

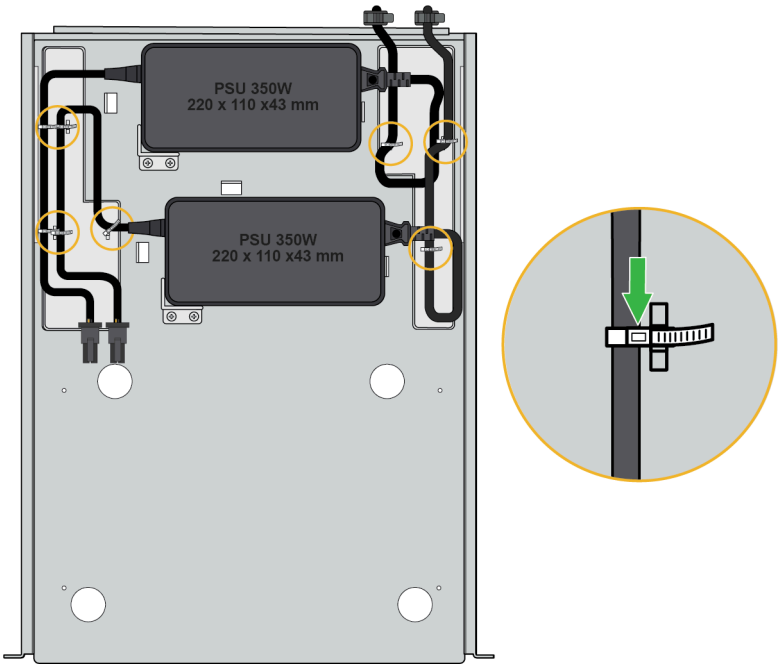


PAN-1RU-4POST-RACK-12

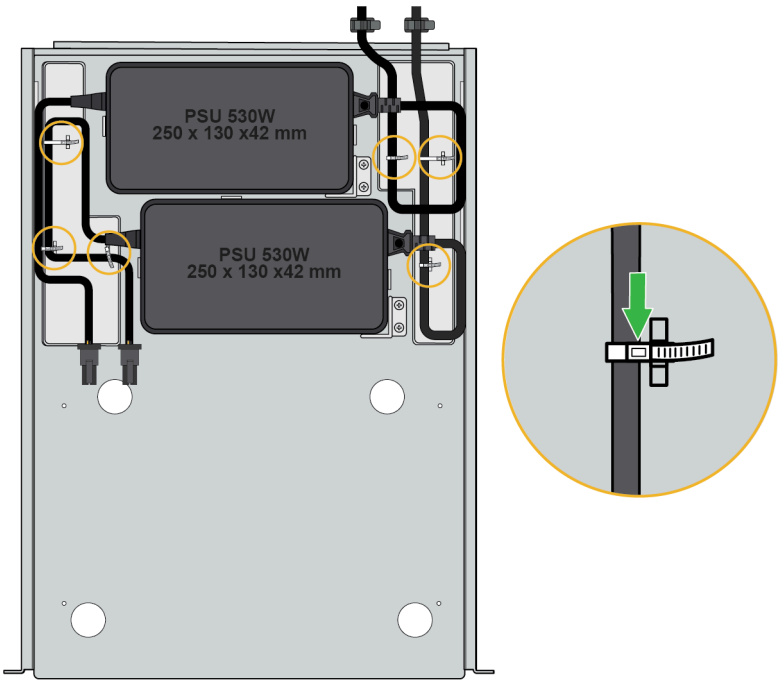
1. Using the following images as references, guide the remaining length of the power cables along the mounting tray. Thread the provided cable ties through the lances and cutouts in

the mounting tray. Wrap the cable ties around the power cables, ensuring that the power cables are fixed in place.

350W Power Adapter



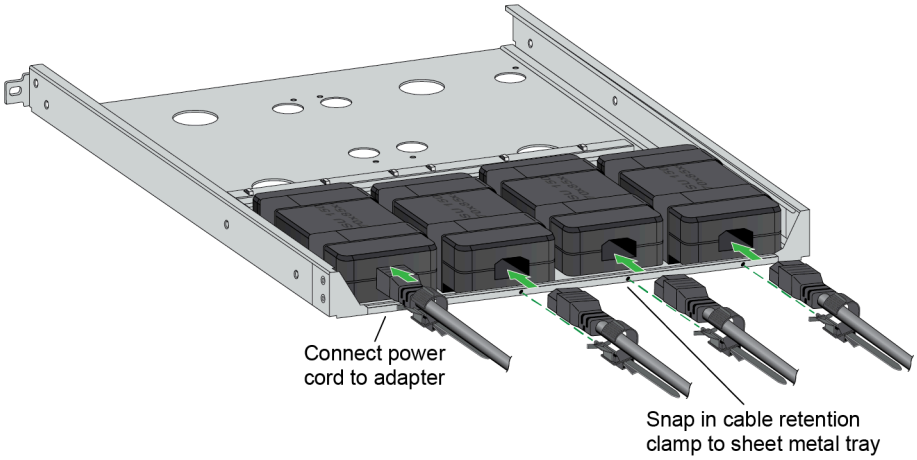
530W Power Adapter



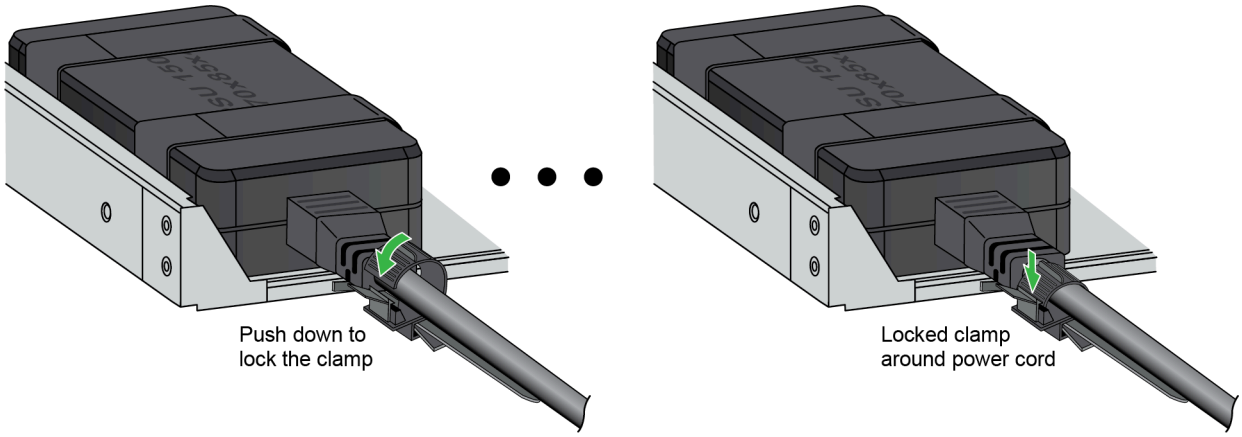
STEP 3 | Install retention clamps over the power cord that plugs into your power source.

PAN-1RU-4POST-RACK-11

1. Connect the power cords into each power adapter.
2. Thread each power cord through a retention clamp, then snap the retention clamp to the mounting tray.

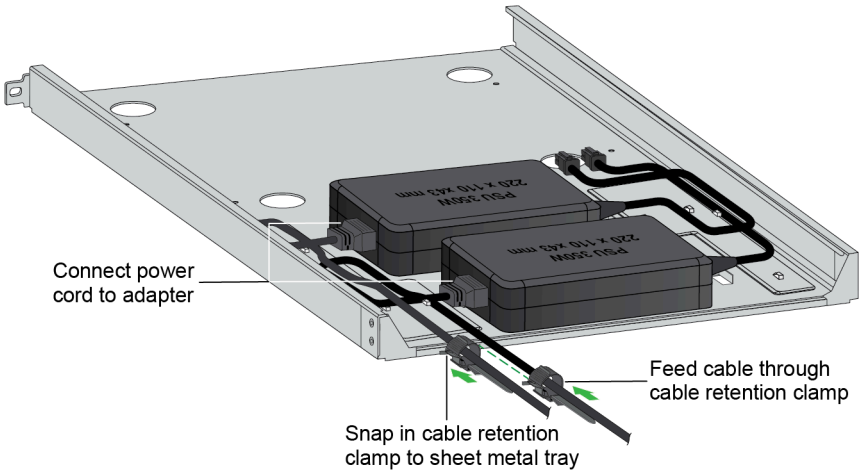


3. Tighten the retention clamp so that the power cord is locked in place.

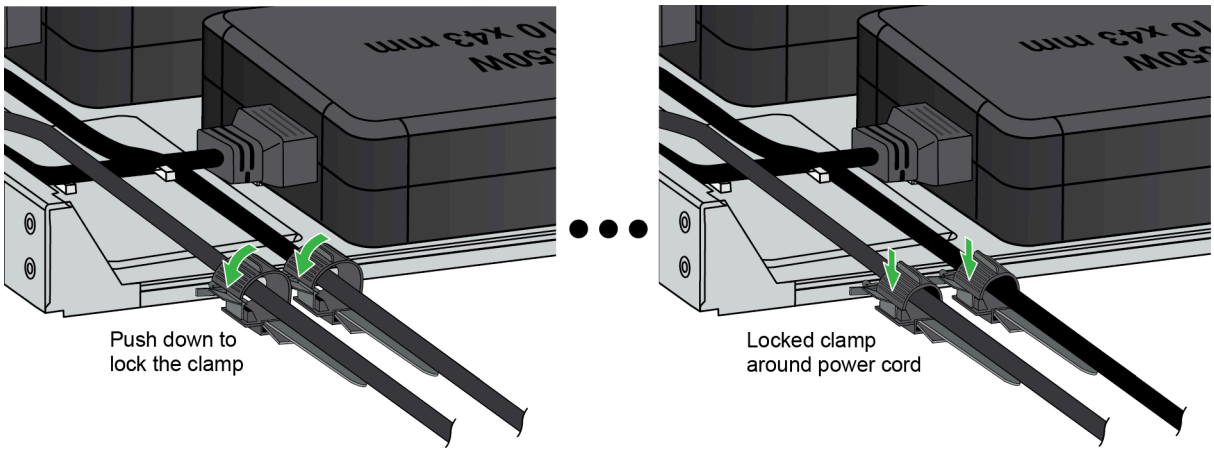


PAN-1RU-4POST-RACK-12

1. Connect the power cords into the power adapter.
2. Thread each power cord through a retention clamp, then snap the retention clamp to the mounting tray.



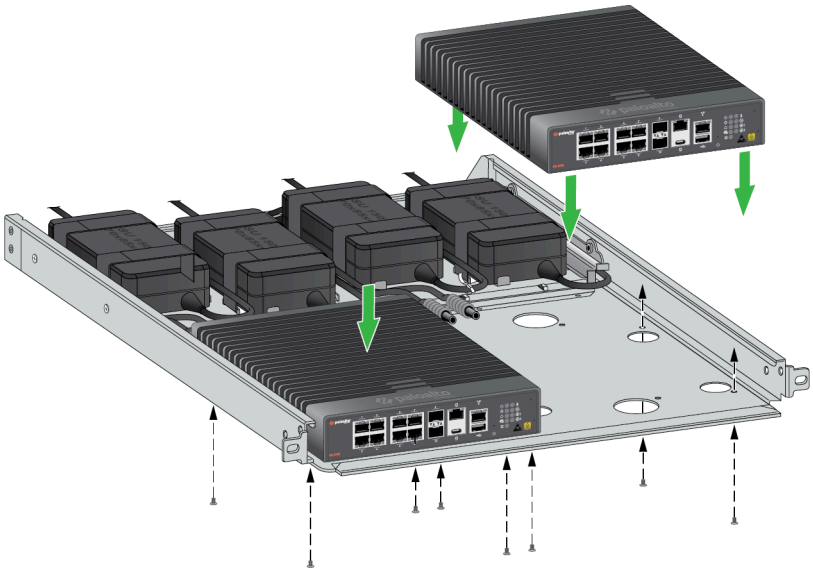
3. Tighten the retention clamp so that the power cord is locked in place.



STEP 4 | Install the firewall in the mounting tray.

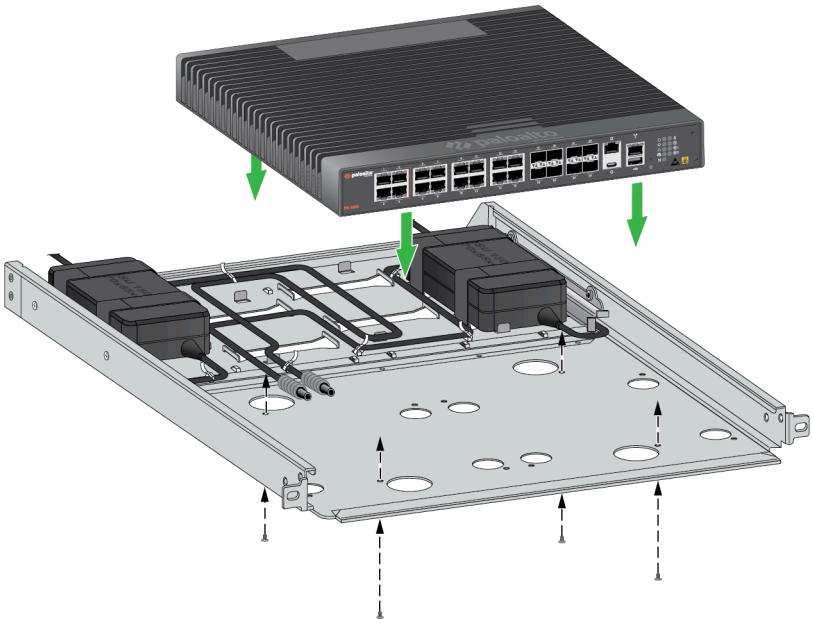
PAN-1RU-4POST-RACK-11 (PA-520 and PA-540)

1. Align the four rubber feet of each device to the mounting tray, then secure it using four M3 x 6mm flathead screws. Repeat if you are installing a second firewall.



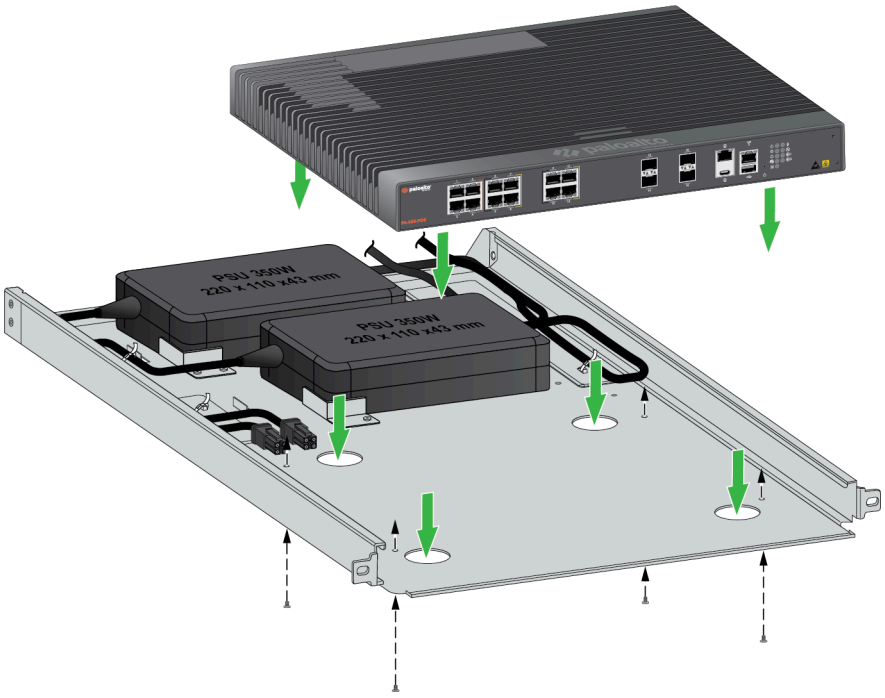
PAN-1RU-4POST-RACK-11 (PA-550 and PA-560)

1. Align the four rubber feet of the device to the mounting tray, then secure it using four M3 x 6mm flathead screws.

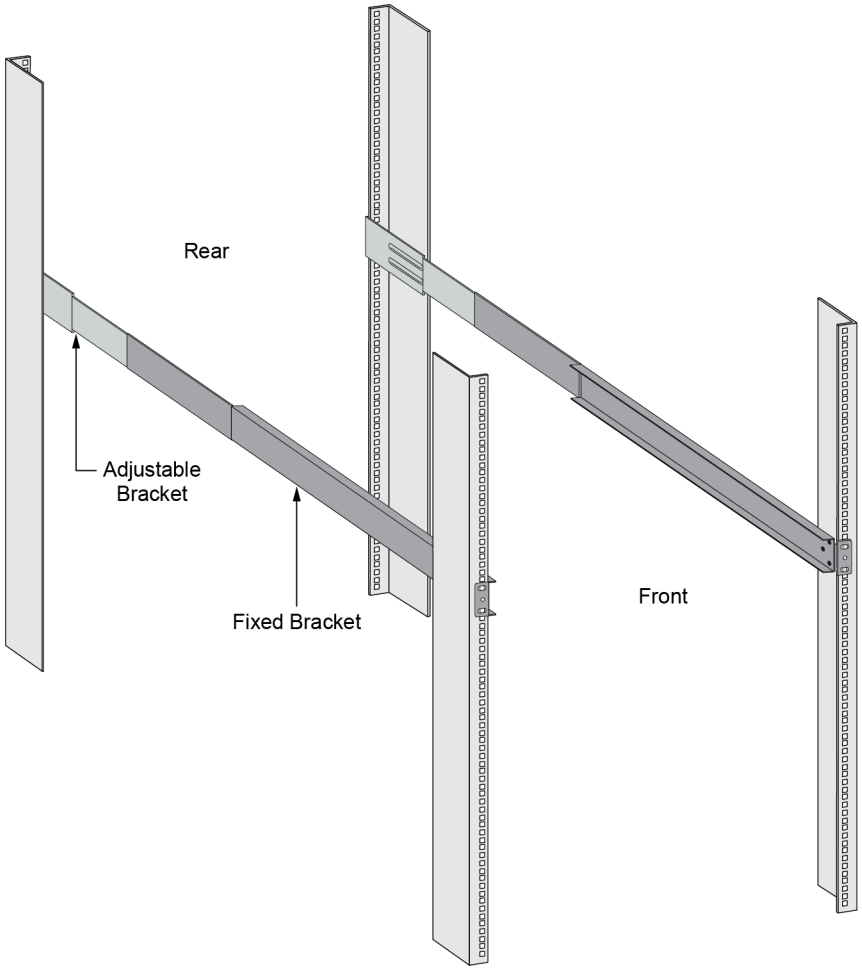


PAN-1RU-4POST-RACK-12

1. Align the four rubber feet of the device to the mounting tray, then secure it using four M3 x 6mm flathead screws.

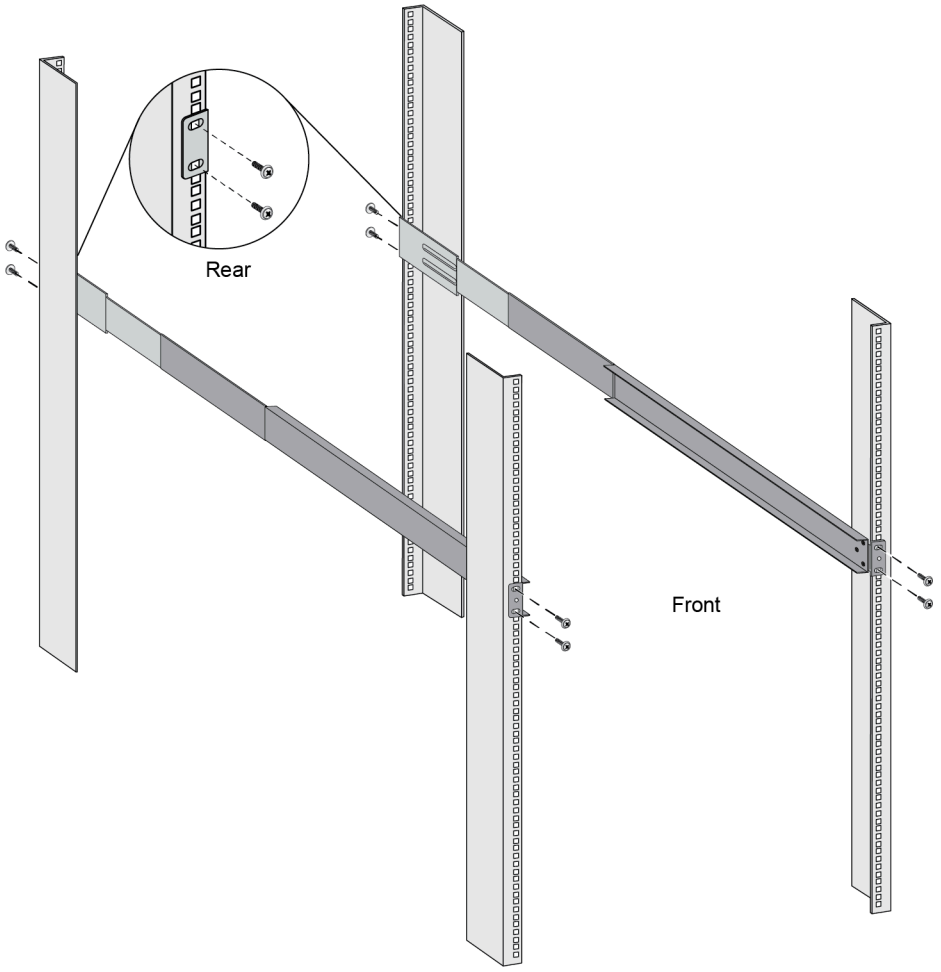


STEP 5 | Slide one of the adjustable mounting brackets into one of the fixed mounting brackets to create a mounting rail. Repeat for the second mounting rail. The adjustable and fixed brackets are the same for the left and right side.



STEP 6 | Align the bottom edge of the mounting rails to the bottom of the space reserved for your firewall. Align the slotted holes in the adjustable mounting bracket to the holes on the rear of the equipment frame.

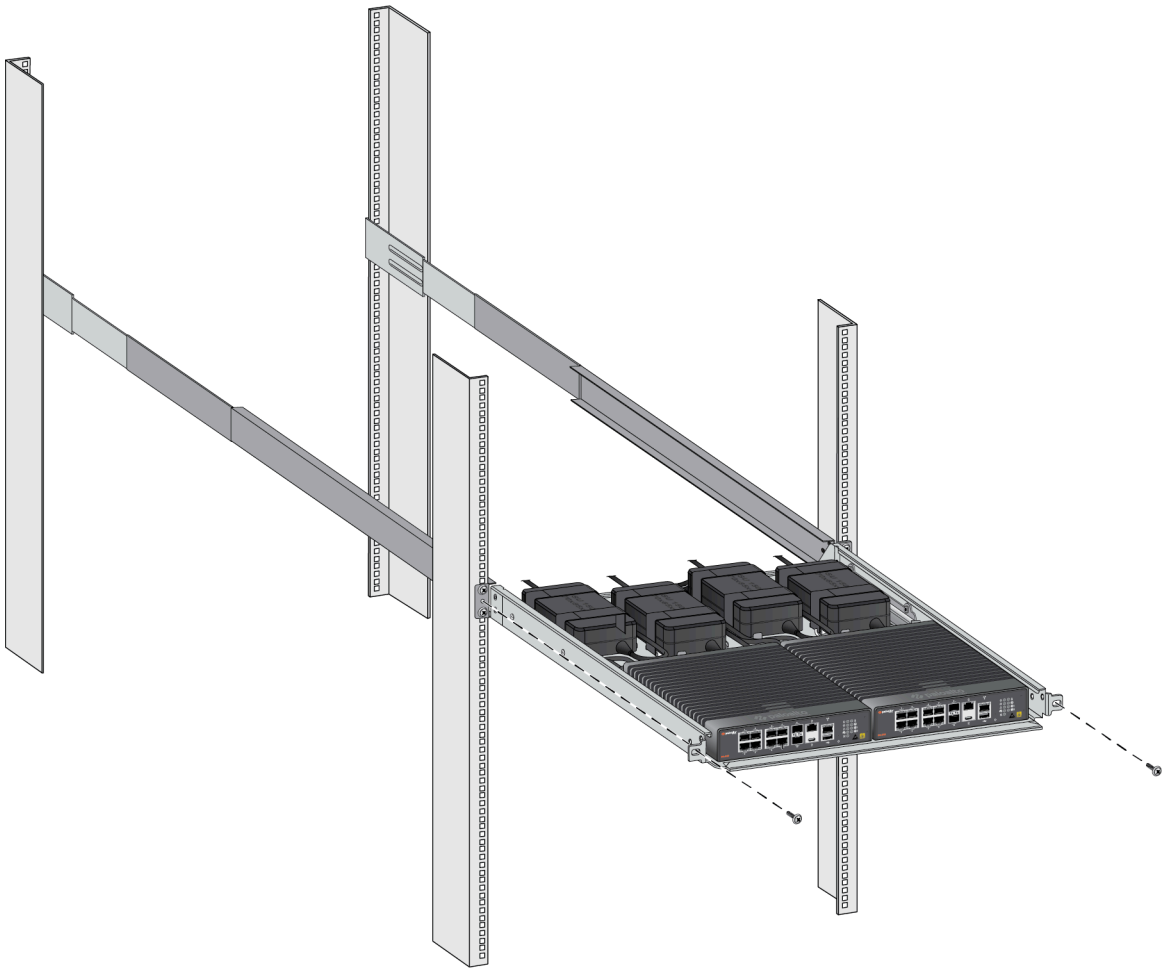
STEP 7 | Secure the rails to the equipment frame with mounting screws (not provided) compatible with your equipment frame. Tighten the screws to their recommended torque value.



STEP 8 | Slide the mounting tray into the rails previously fixed to the equipment rack. Stop when the front flange on the mounting tray is flush with the front of the rail.

STEP 9 | Align the slotted hole in the mounting tray to the hole in the equipment frame. Secure the mounting tray to the equipment frame on both sides using one screw each (not provided). The screws must be compatible with your equipment frame.

PAN-1RU-4POST-RACK-11



PAN-1RU-4POST-RACK-12

STEP 10 | Proceed to Connect Power to the PA-500 Series Firewall.

Set Up a Connection to the PA-500 Series Firewall

On first startup, the PA-500 Series firewall boots into Zero Touch Provisioning (ZTP) mode by default. ZTP mode allows you to automate the provisioning process of a new firewall that is added to a Panorama™ management server. To learn more about ZTP, see ZTP Overview. You can also bring the PA-500 Series firewall online in standard mode. See the instructions below to learn how to boot in ZTP or standard mode.

If you have already booted up the firewall and selected the wrong mode, you must perform a factory reset or private-data-reset before continuing.

- Reset the Firewall to Factory Default Settings *describes how to do a factory reset.*
- *To use the private-data-reset command, you must access the firewall CLI and enter the command* ***request system private-data-reset****. This command will remove all logs and restore the default configuration.*

Before you can successfully add a ZTP firewall to Panorama, you must ensure that a Dynamic Host Configuration Protocol (DHCP) server is deployed on the network. A DHCP server is required to successfully onboard a ZTP firewall to Panorama. The ZTP firewall is unable to connect to the Palo Alto Networks ZTP service to facilitate onboarding without a DHCP server.

ZTP mode is disabled if FIPS-CC mode is enabled. If the firewall boots with FIPS-CC mode enabled, the firewall will automatically boot in standard mode.

STEP 1 | Use an RJ-45 Ethernet cable to connect the device to the correct port. The port(s) connected will depend on which mode you intend the firewall to run in.

- (Standard mode) Connect the Ethernet cable from the MGT port on the firewall to the RJ-45 port of your network switch.
- (ZTP mode) Connect the Ethernet cable from the ZTP port (Ethernet port 1) on the firewall to your network switch.

STEP 2 | Confirm that the connection to the MGT port or Ethernet port 1 has an active network switch.

An active switch allows the firewall to trigger a "link up" state on the port you connected to for your desired boot mode.

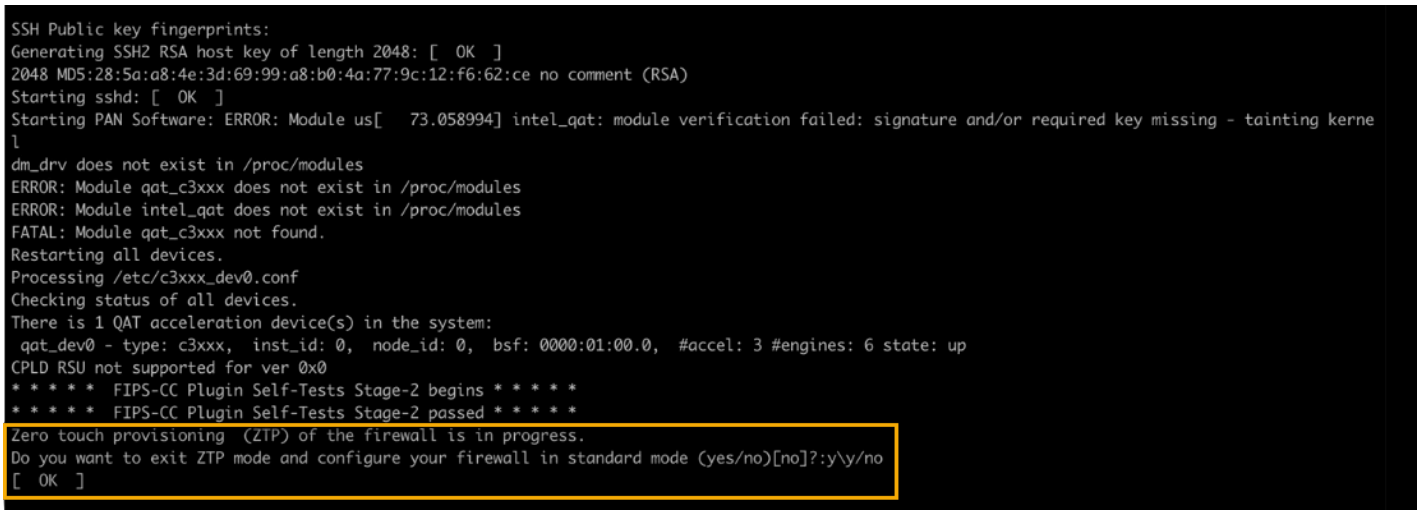
STEP 3 | (Standard mode only) If you intend to boot the firewall in standard mode, you will need access to the firewall CLI to respond to a prompt during bootup. Connect a console cable from the firewall console port to your computer. Once the firewall is powered on, use a terminal emulator such as PuTTY to access the CLI. See Access the CLI for more information.

STEP 4 | Power on the firewall. See Connect Power to the PA-500 Series Firewall to learn how to connect power to the firewall.

- (Standard mode) Using your terminal emulator, watch for the following CLI prompt as the firewall boots:

```
Do you want to exit ZTP mode and configure your firewall in
 standard mode (yes/no)[no]?
```

Enter **yes**. The system will then ask you to confirm. Enter **yes** again to boot in standard mode.



> *If you miss the above CLI prompt, you can also change your boot mode using the web interface. Go to the firewall login screen at any point before or during the startup process. A prompt will ask if you wish to continue booting in ZTP mode or if you would like to switch to standard mode. Select **Standard Mode** and the firewall will begin rebooting in standard mode.*

- (ZTP mode) Stand by as the firewall boots up.

STEP 5 | Set up the firewall manually if using standard mode. If using ZTP mode, the device group and template configuration defined on the Panorama management server are automatically pushed to the firewall by the ZTP service.

- (Standard mode) Change the IP address on your computer to an address in the 192.168.1.0/24 network, such as 192.168.1.2. From a web browser, go to https://192.168.1.1. When prompted, log in to the web interface using the default username and password (admin/admin).
- (ZTP mode) Follow the instructions provided by your Panorama administrator to register your ZTP firewall. You will have to enter the serial number (12-digit number identified as S/N) and claim key (8-digit number). The claim key is required to add a ZTP firewall to the Panorama management server. These numbers are stickers attached to the back of the device.

Connect Power to the PA-500 Series Firewall

The following procedure describes how to connect power to a PA-500 Series firewall.

To avoid injury to yourself or damage to your Palo Alto Networks® hardware or the data that resides on the hardware, read the Safety Warnings.

Learn how to Set Up a Connection to the PA-500 Series Firewall based on your desired boot mode prior to powering on the firewall for the first time.

STEP 1 | Make sure that your AC power source is powered off.

STEP 2 | Remove the screw from the ground point on the back of the firewall.

STEP 3 | Crimp a 14AWG ground cable to a ring lug (ground cable not included), place the ring lug over the screw, then replace the screw to attach the cable to the firewall. Torque the screw to 25 in-lbs and then connect the other end of the cable to earth ground.

STEP 4 | Connect the power adapter to the first power input on the back of the firewall.

PA-520 and PA-540

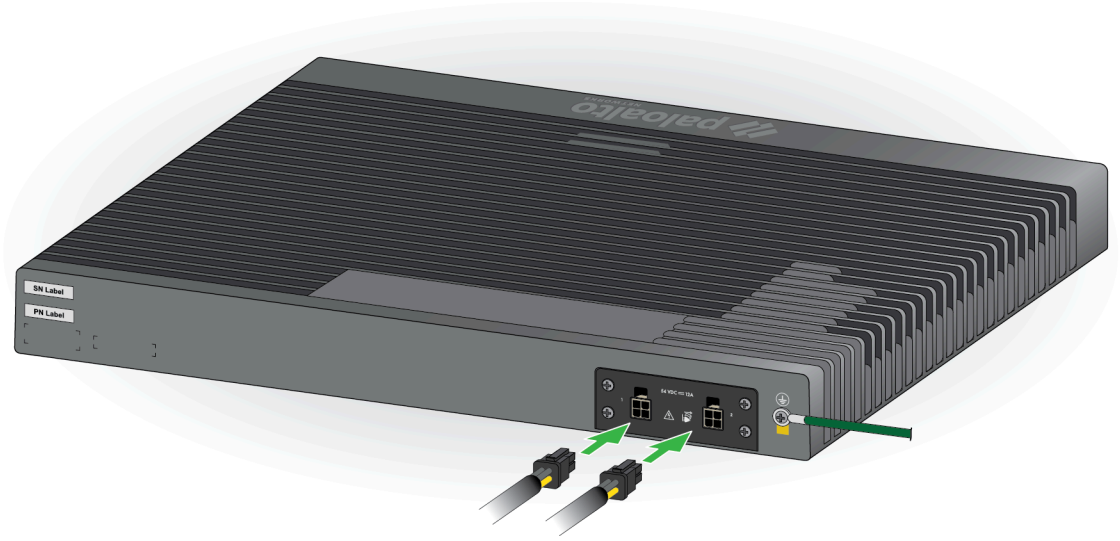
Plug the DC connector from the power adapter into the port on the firewall and tighten the connector nut to secure the cable to the firewall.

PA-550

Plug the DC connector from the power adapter into the port on the firewall and tighten the connector nut to secure the cable to the firewall.

PA-545-POE and PA-555-POE

Plug the DC connector from the power adapter into the port on the firewall and secure the input to the firewall.



PA-560

STEP 5 | Plug the AC connector from the power adapter into your AC power source.

STEP 6 | Power on your AC power source. The green power LED on the firewall indicates when the firewall is powered on.

STEP 7 | (Optional) Connect the DC connector from a second power adapter (purchased separately) into the second power port and plug the AC connector into an AC power source.

Before powering on the firewall, ensure that you have connected your Ethernet cables in accordance to the mode you wish to boot the firewall in (standard mode or Zero Touch Provisioning mode) as specified in Set Up a Connection to the PA-500 Series Firewall.

PA-500 Series Firewall Maintenance

Use the following topics to service the PA-500 Series firewall hardware.

- PA-500 Series Firewall LED Definitions
- Replace a PA-500 Series Firewall Power Supply

PA-500 Series Firewall LED Definitions

The following table describes how to interpret the status LEDs on the PA-500 Series firewalls. Not all PA-500 Series firewalls have all of the LED indicators.

LED	Description
Front Panel LEDs	
	Power • Green—The firewall is powered on. • Yellow—One or more power rails have encountered an issue. • Off—The firewall is not powered on or an error has 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. • Red—The firewall failed to boot.
	Alarm • Red—A hardware component failed, such as a power adapter failure, a firewall failure that caused an HA failover, a drive failure, or hardware is overheating and the temperature is above the high temperature threshold.

LED	Description
	• Off—The firewall is operating normally.
	**Controller** • Green—The device is connected to Panorama. • Blue—The device is connected to a SDWAN controller or SCM. • Blinking yellow—The device is attempting to connect to the controller. • Solid yellow—The device is unable to connect to a controller. • Off—The device is not cloud managed.
	**High Availability (HA)** • Green—The firewall is the active peer in an active/passive configuration. • Yellow—The firewall is the passive peer in an active/passive configuration. • Off—High availability (HA) is not operational on this firewall.  *In an active/active configuration, the HA LED only indicates HA status for the local firewall and has two possible states (green or off); it does not indicate HA connectivity of the peer. Green indicates that the firewall is either active-primary or active-secondary and off indicates that the firewall is in any other state (for example, non-functional or suspended).*
	**Temperature** • Yellow—The firewall temperature is outside tolerance levels. • Off—The firewall temperature is within normal levels.
	**Service** This LED is disabled by default but can be enabled by a remote administrator to illuminate the device for a local operator. To enable the LED, use the following CLI command: `admin@PA-540> set system setting service-led enable yes` • Off—The LED is disabled. • Blue—A device locator beacon enabled by the administrator.

LED	Description
	**PSU1 and PSU2** • Green—The PSU is powered with the correct voltage. • Yellow—The PSU is powered with the incorrect voltage. • Off—The PSU is not present.
RJ-45 port LEDs	**Link LED** • Off—There is no link • Solid yellow—10Mbps/100Mbps • Solid green—1Gbps/2.5Gbps **Activity LED** Blinking green—The link is up and there is network activity. Solid green—The link is up but there is no network activity. Off—There is no network activity.
SFP/SFP+ LEDs	**Link LED** • Off—There is no link • Solid yellow—1Gbps • Solid green—10Gbps **Activity LED** Blinking green—The link is up and there is network activity. Solid green—The link is up but there is no network activity. Off—There is no network activity.

Replace a PA-500 Series Firewall Power Supply

The PA-500 Series firewalls can operate on one power adapter. All of the PA-500 Series firewalls support the connection of a second power adapter for power redundancy. If two power adapters are installed and one fails, you can replace the failed power adapter without interruption.

To avoid injury to yourself or damage to your Palo Alto Networks® hardware or the data that resides on the hardware, read the Safety Warnings.

STEP 1 | Unplug the failed power adapter from the AC power source and then disconnect the cable plugged into the firewall.

STEP 2 | Connect the DC connector from the new power adapter to the first power input port on the firewall and ensure that it is secure.

STEP 3 | Plug the AC connector from the power adapter into an AC power source.

PA-500 Series Firewall Specifications

The following topics describe the PA-500 Series firewall hardware specifications. For feature, capacity, and performance information, refer to the datasheet.

PA-500 Series Firewall Physical Specifications

The following table describes PA-500 Series firewall physical specifications.

Specification	Value
Rack units and dimensions	**PA-520 and PA-540** • Height x Width x Depth—1.74 in x 8 in x 10.4 in (44.2 mm x 203.2 mm x 264.16 mm) • Rack units—1U **PA-550 and PA-560** • Height x Width x Depth— 1.74 in x 13 in x 12.1 in (44.2 mm x 330.2 mm x 307.3 mm) • Rack units—1U **PA-545-POE and PA-555-POE** • Height x Width x Depth— 1.75 inch x 16.1 inch x 12.6 inch (44.5 mm x 408.9 mm x 320.04 mm) • Rack units—1U
Weight	**PA-520 and PA-540** • Firewall weight—5.8 lbs (2.6 kg) • Shipping weight—8.6lbs (3.9 kg) **PA-550 and PA-560** • Firewall weight—11.2 lbs (5.1 kg) • Shipping weight—15.6 lbs (7.1 kg) **PA-545-POE and PA-555-POE** • Firewall weight—13.5 lbs (6.1 kg) • Shipping weight—19.8 lbs (8.9 kg)

PA-500 Series Firewall Electrical Specifications

The following table describes PA-500 Series firewall electrical specifications.

Specification	Value
Power adapter	The PA-500 Series firewalls operate on DC power that is provided by the external power adapter (provided). The PA-500 Series firewalls can operate on one power adapter or you can install a second power adapter for load sharing and power redundancy.
Input voltage	**PA-520, PA-540, PA-550, and PA-560** • Power adapter (AC side)—100-240V AC 50-60Hz • The power adapter converts the AC power to 12VDC to provide power to the firewall. **PA-545-POE and PA-555-POE** • Power adapter (AC side)—100-240V AC 50-60Hz • The power adapter converts the AC power to 54VDC to provide power to the firewall.
Maximum power consumption	**PA-520 and PA-540**—30W **PA-545-POE**—336W **PA-550**—57W **PA-555-POE**—503W **PA-560**—106W
Maximum current consumption	**PA-520**—4A@12VDC **PA-540**—4A@12VDC **PA-545-POE**—6A@54VDC **PA-550**—5A@12VDC **PA-555-POE**—9A@54VDC **PA-560**—8A@12VDC
Power over Ethernet (PoE)	**PA-545-POE** • Supported on ports 9, 10, 11, and 12 • Maximum power reserved per port—90W • Total PoE budget allowed (across all ports) —181W **PA-555-POE**

Specification	Value
	• Supported on ports 5, 6, 7, 8, 9, 10, 11, and 12 • Maximum power reserved per port—90W • Total PoE budget allowed (across all ports) —332W

PA-500 Series Firewall Environmental Specifications

The following table describes PA-500 Series firewall environmental specifications.

Specification	Value
Operating temperature range	• 32°F to 104°F (0° to 40°C)
Non-operating temperature	• -4°F to 158°F (-20° to 70°C)
Humidity tolerance	10% to 90% non-condensing
Airflow	All PA-500 Series firewalls (except for the PA-560) use passive cooling and do not contain fans. The PA-560 features two fans for active cooling.
Maximum BTUs/hour	**PA-520 and PA-540**—102/hour **PA-545-POE**—1145/hour **PA-550**—195/hour **PA-555-POE**—1715/hour **PA-560**—361/hour
Electromagnetic Interference (EMI)	FCC Class A, CE Class A, VCCI Class A
Acoustic noise	**PA-520, PA-540, PA-550, PA-545-POE, and PA-555-POE**—Emits no sound. **PA-560**—Under full load, the PA-560 (which has fans), can reach a noise level of up to 62dBA.
Maximum operating altitude	10,000ft (3,048m)

PA-500 Series Firewall Miscellaneous Specifications

The following table describes PA-500 Series firewall miscellaneous specifications.

Specification	Value
Storage capacity	**PA-520, PA-540, PA-545-POE, PA-550, and PA-555-POE**—120 GB **PA-560**—240 GB
Mean time between failures (MTBF)	29 years