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

Palo Alto Networks, Inc.
www.paloaltonetworks.com

© 2024-2026 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

February 4, 2026

Table of Contents

Before You Begin 5

Compliance 6

Parts List and Required Tools 11

PA-500 Series Firewall Overview 13

PA-500 Series Firewall Components 14

PA-500 Series Firewall Installation 35

Install the PA-500 Series Firewall on a Wall 36

Install the PA-500 Series Firewall in an Equipment Rack 40

Set Up a Connection to the PA-500 Series Firewall 64

Connect Power to the PA-500 Series Firewall 66

Install Antennas on the PA-520-5G Firewall 70

Insert or Replace a SIM Card in a PA-500 Series 5G Firewall 71

PA-500 Series Firewall Maintenance 73

PA-500 Series Firewall LED Definitions 74

Replace a PA-500 Series Firewall Power Supply 78

Insert or Replace a SIM Card in a PA-500 Series 5G Firewall 79

PA-500 Series Firewall Specifications 81

PA-500 Series Firewall Physical Specifications 82

PA-500 Series Firewall Electrical Specifications 84

PA-500 Series Firewall Environmental Specifications 86

PA-500 Series Firewall Antenna Specifications 87

PA-500 Series Firewall Miscellaneous Specifications 88

 ©2026 Palo Alto Networks, Inc.

 ©2026 Palo Alto Networks, Inc.

Before You Begin

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

- Compliance
- Parts List and Required Tools

Compliance

- Safety Warnings
- Safety Warnings (French)
- Regulatory 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.
- Use grounded and shielded Ethernet cables (when applicable) to ensure agency compliance with electromagnetic compliance (EMC) regulations.
- 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.

• 	Caution: Shock hazard Disconnect all power cords (AC or DC) from the power inputs to fully de-energize the hardware.

- Do not connect or disconnect energized DC wires to the power supply.
- The DC system must be earthed at a single (central) location.
- The DC supply source must be located within the same premises as the firewall.
- The DC battery return wiring on the firewall must be connected as an isolated DC (DC-I) return.
- 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.
- 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.

 ©2026 Palo Alto Networks, Inc.

- Do not disconnect the firewall in the earthed circuit conductor between the DC source and the point of connection of the earthing electrode conductor.
- 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.
- 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.
- 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.
- A suitably-rated DC mains disconnect device must be provided as part of the building installation.

Safety Warnings (French)

- **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.
- **French Translation:** Des câbles Ethernet blindés reliés à la terre doivent être utilisés pour garantir la conformité de l'organisme aux émissions électromagnétiques (CEM).
- **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.
- 

  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.
- Ne raccordez ni débranchez de câbles c.c. sous tension à la source d'alimentation.
- Le système c.c. doit être mis à la terre à un seul emplacement (central).
- La source d'alimentation c.c. doit se trouver dans les mêmes locaux que ce pare-feu.
- Le câblage de retour de batterie c.c. sur le pare-feu doit être raccordé en tant que retour c.c. isolé (CC-I).
- 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.

 ©2026 Palo Alto Networks, Inc.

- 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.
- 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.
- 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.
- 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.
- 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.
- Un interrupteur d'isolement suffisant doit être fourni pendant l'installation du bâtiment.

Regulatory 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.
  - (PA-520, PA-540, PA-545-POE, PA-550, PA-555-POE, and PA-560 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

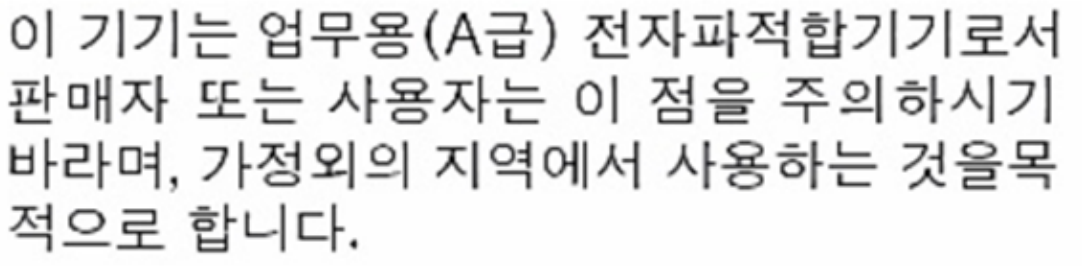
    Translation: This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take corrective actions.
  - (PA-501, PA-505, and PA-510 VCCI Class B requirements)

    この装置は、クラスB機器です。この装置は、住宅環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
    取扱説明書に従って正しい取り扱いをして下さい。 VCCI－B

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

 ©2026 Palo Alto Networks, Inc.

- **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.

 ©2026 Palo Alto Networks, Inc.

- **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.

 ©2026 Palo Alto Networks, Inc.

Parts List and Required Tools

The following tables list the items that are shipped with the PA-500 Series firewall.

Table 1: Parts List — PA-501, PA-505, and PA-510

Quantity	Item
1	PA-500 Series firewall
1	Ethernet cable
1	PA-510 only Micro USB cable
1	AC/DC power adapter
1	Power cord

Table 2: Parts List — PA-520, PA-540, PA-545-POE, PA-550, PA-555-POE, and PA-560

Quantity	Item
1	PA-500 Series firewall
1	Ethernet cable
1	USB-C to USB-C cable
1	AC/DC power adapter
1	Power cord
1	Single-hole ground lug

Table 3: Parts List — PA-520-5G

Quantity	Item
1	PA-520-5G firewall
1	Ethernet cable
1	USB-C to USB-C cable
1	AC/DC power adapter (PAN-PWR-66W-12V-AC-A)

 ©2026 Palo Alto Networks, Inc.

Quantity	Item
1	Power cord
1	Single-hole ground lug
4	5G antennas (omni-directional, 4G/5G, SMA-M)
1	SIM card tweezer tool
1	Ground lug mounting screw (Pan Head Torx-T10, M3×0.5, 5mm)

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

 ©2026 Palo Alto Networks, Inc.

PA-500 Series Firewall Overview

The Palo Alto Networks® PA-500 Series Next-Generation firewalls include the PA-501,PA-505, PA-510, PA-520, PA-520-5G, 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, 5G cellular connectivity for select models, and active/passive and active/active high availability (HA). All PA-500 Series firewalls (except the PA-505) 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
- **PAN-OS 12.1.3** — PA-505 and PA-510
- **PAN-OS 12.1.4-h2** — PA-501
- **PAN-OS 12.1.10** — PA-520-5G
- PA-500 Series Firewall Components

PA-500 Series Firewall Components

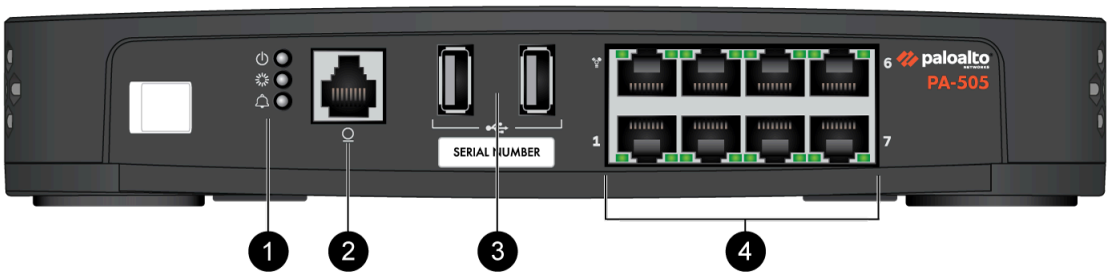
Refer to the following sections to view the front and back panel components of the PA-500 Series firewalls.

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

- PA-501 and PA-505
- PA-510
- PA-520 and PA-540
- PA-520-5G
- PA-550 and PA-560
- PA-545-POE and PA-555-POE

PA-501 and PA-505

The following image shows the front panel of the PA-501 and PA-505, which have the same front panel components (PA-505 pictured). The table describes each front panel component.



Item	Component	Description
1	LED Status Indicators	Three LEDs that indicate the status of the firewall hardware components (see PA-500 Series Firewall LED Definitions).
2	Console Port	Use this port to connect a management computer to the firewall using a 9-pin serial to RJ-45 cable and terminal emulation software. The console connection provides access to firewall boot messages, the Maintenance Recovery Tool

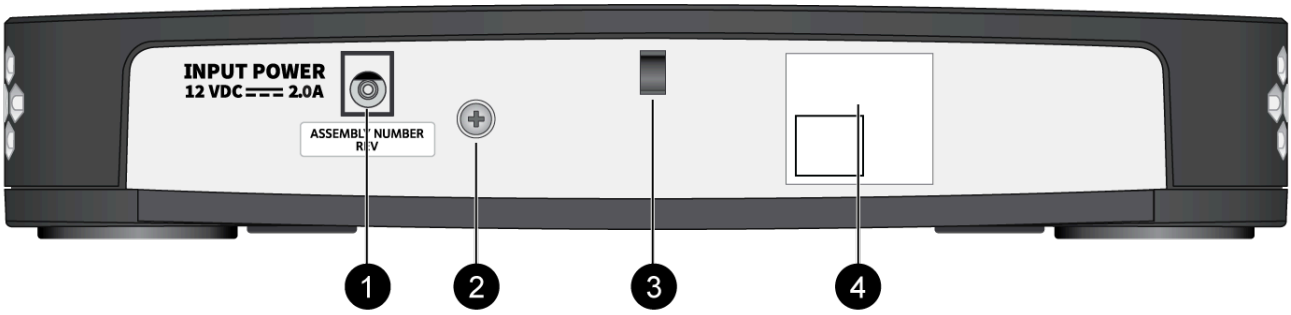
 ©2026 Palo Alto Networks, Inc.

Item	Component	Description
		(MRT), and the command line interface (CLI). *If your management computer does not have a serial port, use a USB-to-serial converter.* Use the following settings to configure your terminal emulation software to connect to the console port: • Data rate: 9600 • Data bits: 8 • Parity: none • Stop bits: 1 • Flow control: None
3	USB Ports	Two USB ports for debugging and administration only. Use one of the two ports 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.
4	RJ-45 Ports	**Management Port** One Ethernet10/100/1000Mbps port (the top-left port) that is used 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. **Ethernet Ports**

 ©2026 Palo Alto Networks, Inc.

Item	Component	Description
		Seven RJ-4510/100/1000Mbps ports for network traffic.You can set the link speed and duplex mode or choose autonegotiate.

The following image shows the back panel of the PA-501 and PA-505, which have the same back panel components (PA-505 pictured). The table describes each back panel component.

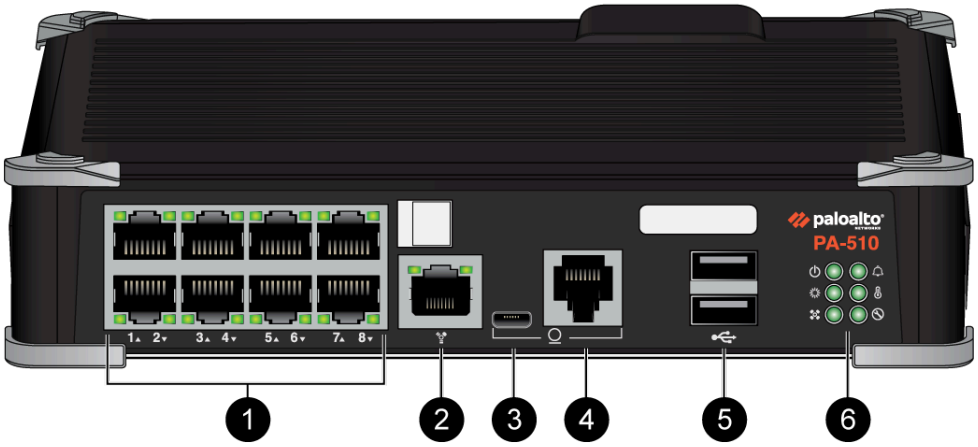


Item	Component	Description
1	Power Adapter Input	Use the power input to connect power to the firewall. The PA-505 ships with one 25W power adapter.
2	Ground Stud	Use the single post ground stud to connect the firewall to earth ground (ground cable not included).
3	Power Cord Retainer	Use the power cord retainer to secure the power cord.
4	QR Code	Scan the QR code to access product and ZTP onboarding information.

PA-510

The following image shows the front panel of the PA-510. The table describes each front panel component.

 ©2026 Palo Alto Networks, Inc.



Item	Component	Description
1	Ethernet ports	Eight RJ-45 10/100/1000Mbps ports for network traffic. You can set the link speed and duplex mode or choose auto-negotiate.
2	Management port	Use this Ethernet 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.
3	CONSOLE port (Micro USB)	Use this port to connect a management computer to the firewall using a standard Type-A USB-to-micro USB cable. The console connection provides access to firewall boot messages, the Maintenance Recovery Tool (MRT), and the command line interface (CLI). Refer to Micro USB Console Port for more information and to download the Windows driver or to learn how to

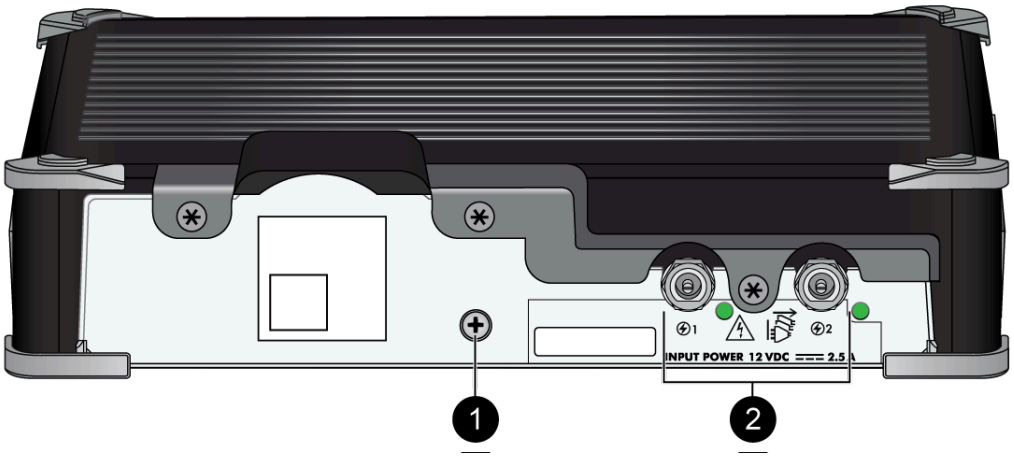
 ©2026 Palo Alto Networks, Inc.

Item	Component	Description
		connect from a Mac or Linux computer.
4	CONSOLE port (RJ-45)	Use this port to connect a management computer to the firewall using a 9-pin serial to RJ-45 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). *If your management computer does not have a serial port, use a USB-to-serial converter.* Use the following settings to configure your terminal emulation software to connect to the console port: • Data rate: 9600 • Data bits: 8 • Parity: none • Stop bits: 1 • Flow control: None
5	USB ports	Two USB ports for debugging and administration only. Use one of these ports 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	LED status indicators	Six LEDs that indicate the status of the firewall

 ©2026 Palo Alto Networks, Inc.

Item	Component	Description
		hardware components (see PA-500 Series Firewall LED Definitions).

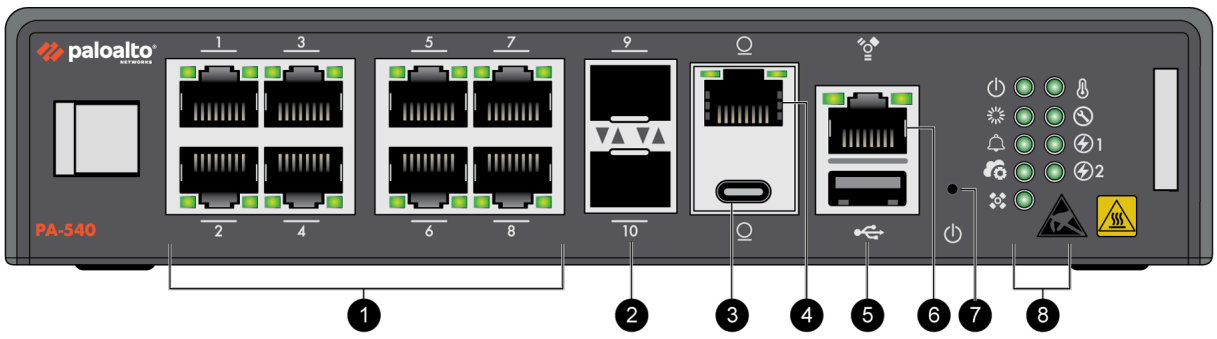
The following image shows the back panel of the PA-510. The table describes each back panel component.



Item	Component	Description
1	Ground stud	Use the single post ground stud to connect the firewall to earth ground (ground cable not included).
2	Power adapter inputs	Use the power inputs to connect power to the firewall. A second adapter can be used for redundancy.

PA-520 and PA-540

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.



 ©2026 Palo Alto Networks, Inc.

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 (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).
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

©2026 Palo Alto Networks, Inc.

Item	Component	Description
		• 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 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 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.

 ©2026 Palo Alto Networks, Inc.



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).

PA-520-5G

The following image shows the front panel of the PA-520-5G. The table describes each front panel component.

Item	Component	Description
1	5G Antenna Connector (TX3/RX3)	SMA antenna connector for connecting an external 5G antenna to the firewall. *The 5G antennas also support GPS and GLONASS (GNSS) for location services. No separate GPS antenna is required.*
2	RJ-45 Ports	Eight copper RJ-45 10Mbps/100Mbps/1Gbps ports for network traffic.

 ©2026 Palo Alto Networks, Inc.

Item	Component	Description
		Port 1 is a Zero Touch Provisioning (ZTP) port. The ZTP port can be used to automatically provision the firewall. ZTP is also supported on Cellular 1/1; whichever interface establishes connectivity first is used for bootstrapping. *Ports 3 and 4 are fail-open ports. They can be configured to provide a pass-through connection despite power or operating system failure.*
3	LED Status Indicators	Ten LEDs that indicate the status of the firewall hardware components and four LEDs that indicate cellular connection strength. (see PA-500 Series Firewall LED Definitions).
4	SFP Ports	Two SFP 1Gbps ports for network traffic.
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

 ©2026 Palo Alto Networks, Inc.

Item	Component	Description
		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	Management Port	Use this RJ-45 10/100/1000 Mbps 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.
7	USB Port	One USB-C port used for debugging and administration only. Use it to bootstrap the firewall or perform self-service enhanced factory reset (EFR). Bootstrapping enables you to provision the firewall with a specific PAN-OS configuration and then license it and make it operational on your network. EFR provides remediation of a compromised or potentially compromised firewall to initiate a complete cleanup of the device.
8	Reset Button	A pin press reset button that can be used to gracefully shut down the firewall.

 ©2026 Palo Alto Networks, Inc.

Item	Component	Description
9	5G Antenna Connector (TX4/RX4)	SMA antenna connector for connecting an external 5G antenna to the firewall.
10	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-520-5G. The table describes each back panel component.

Item	Component	Description
1	5G Antenna Connector (TX2/RX2)	SMA antenna connector for connecting an external 5G antenna to the firewall.
2	Power Adapter Inputs	Two DC 12V power inputs (PS1 and PS2). One power supply is required; a second can be used for redundancy. The two inputs do not support load sharing.
3	5G Antenna Connector (TX1/RX1)	SMA antenna connector for connecting an external 5G antenna to the firewall.

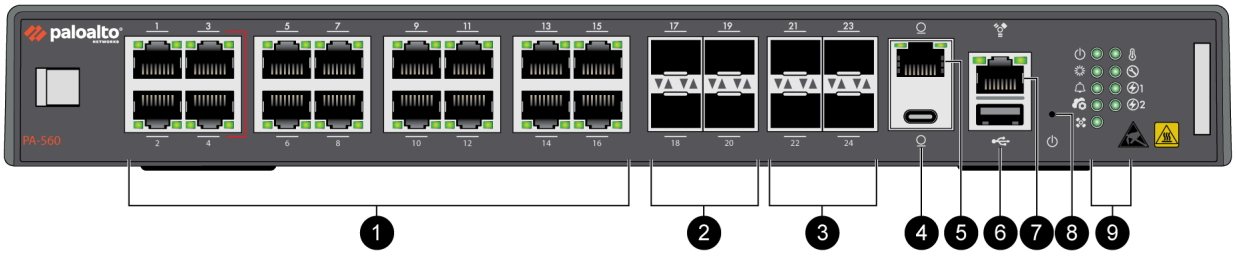
The following image shows the side panel of the PA-520-5G after the SIM cover has been removed. The table describes each side panel component.

Item	Component	Description
1	SIM Slots	Two nano SIM card slots (SIM 1 and SIM 2). The firewall supports Active/Standby SIM selection. The firewall also supports an embedded SIM (eUICC).
2	Micro USB-C Port	This port is reserved for internal use and is not available for configuration.

PA-550 and PA-560

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.

 ©2026 Palo Alto Networks, Inc.



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. *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**

 ©2026 Palo Alto Networks, Inc.

Item	Component	Description
		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. 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

 ©2026 Palo Alto Networks, Inc.

Item	Component	Description
		• 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 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).

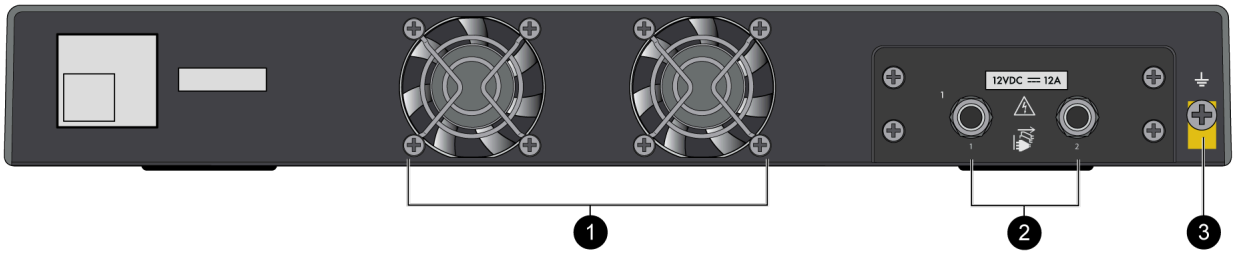
The following image shows the back panel of the PA-550. The table describes each back panel component.



 ©2026 Palo Alto Networks, Inc.

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).

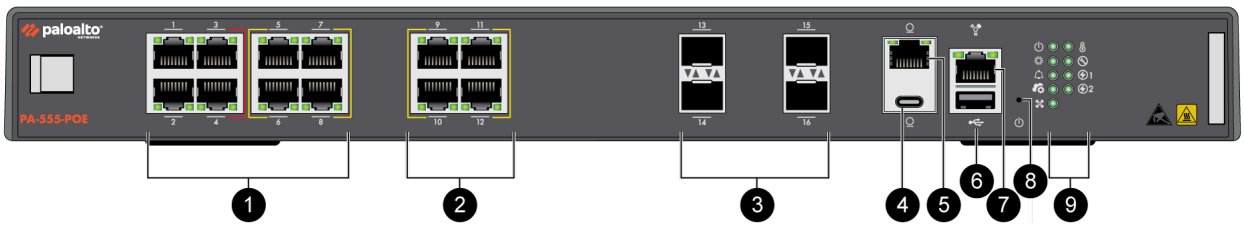
The following image shows the back panel of the PA-560. The table describes each back panel component.



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

PA-545-POE and PA-555-POE

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.



 ©2026 Palo Alto Networks, Inc.

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.* *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**

 ©2026 Palo Alto Networks, Inc.

Item	Component	Description
		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** 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:

©2026 Palo Alto Networks, Inc.

Item	Component	Description
		• 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 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 back panel of the PA-545-POE and PA-555-POE, which have similar back panel components. The table describes each back panel component.



 ©2026 Palo Alto Networks, Inc.

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).

 ©2026 Palo Alto Networks, Inc.

 ©2026 Palo Alto Networks, Inc.

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 on a Wall
- 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 Antennas on the PA-520-5G Firewall
- Insert or Replace a SIM Card in a PA-500 Series 5G Firewall

Install the PA-500 Series Firewall on a Wall

The PA-501, PA-505, PA-520-5G, and PA-510 firewalls can be installed on a drywood or plywood wall using the wall mount as described in the following procedure.

STEP 1 | Mark the locations on the wall that line up with the wall mount holes on the bottom of the firewall.

For the PA-501, PA-520-5G, and PA-505, mark four wall mount hole locations.

For the PA-510, mark three wall mount hole locations.

Ensure there are no building services (water, gas, or wiring) behind the wall where you intend to install the firewall.

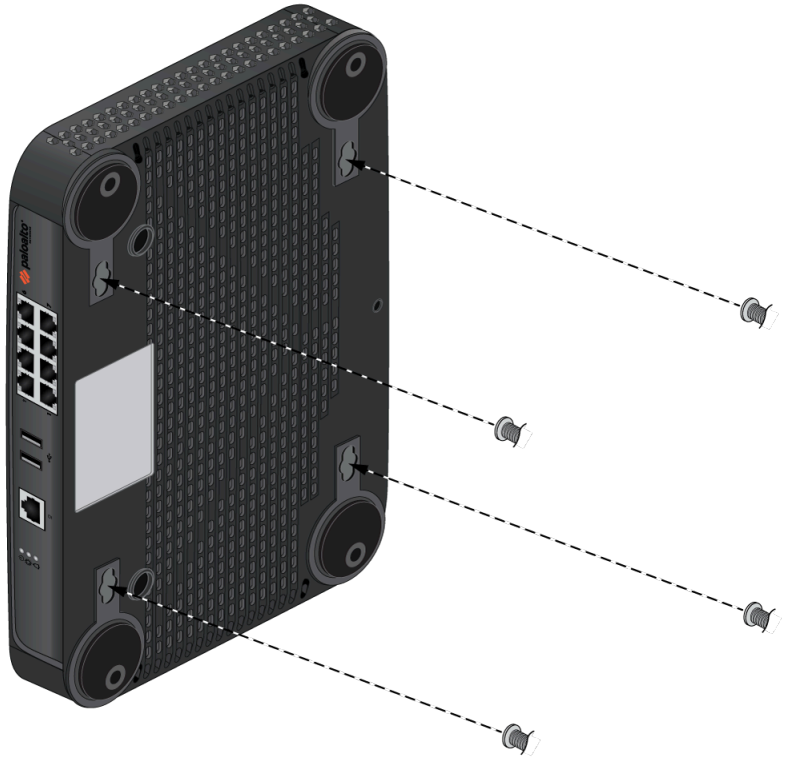
STEP 2 | Use a #1 Phillips-head screwdriver to install the appropriate screws into each of the three or four marked locations:

- **Drywall**—Press a drywall anchor slightly into the center of a mark. Then use your screwdriver to apply pressure while turning the anchor clockwise until the surface of the anchor is flush with the wall. After the drywall anchor is secure, install a 1.25” anchor screw into the anchor until the bottom of the screw head protrudes 1/4” (.6cm) from the wall. Repeat this step for the other screw locations unless either is located over wood, in which case, use a .75” wood screw instead of a drywall anchor and screw.
- **Plywood wall**—Use your screwdriver to insert a .75” wood screw into the center of each mark that is located over wood until the bottom of the screw heads protrude 1/4” (.6cm) from the wall.

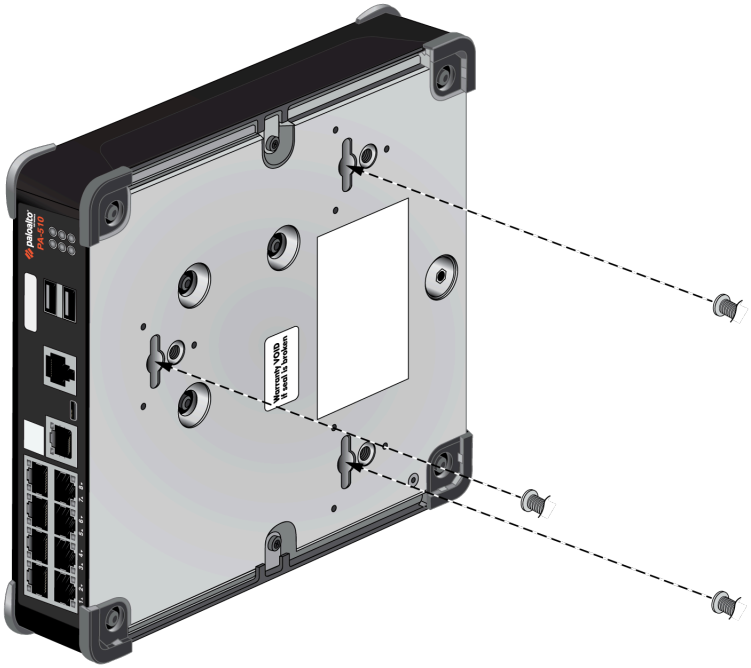
 ©2026 Palo Alto Networks, Inc.

STEP 3 | Align the holes on the bottom of the firewall with the screws on the wall and hang the firewall on the screws. Make sure the firewall is securely connected to each of the screws before you let go.

(PA-501, PA-520-5G, and PA-505)



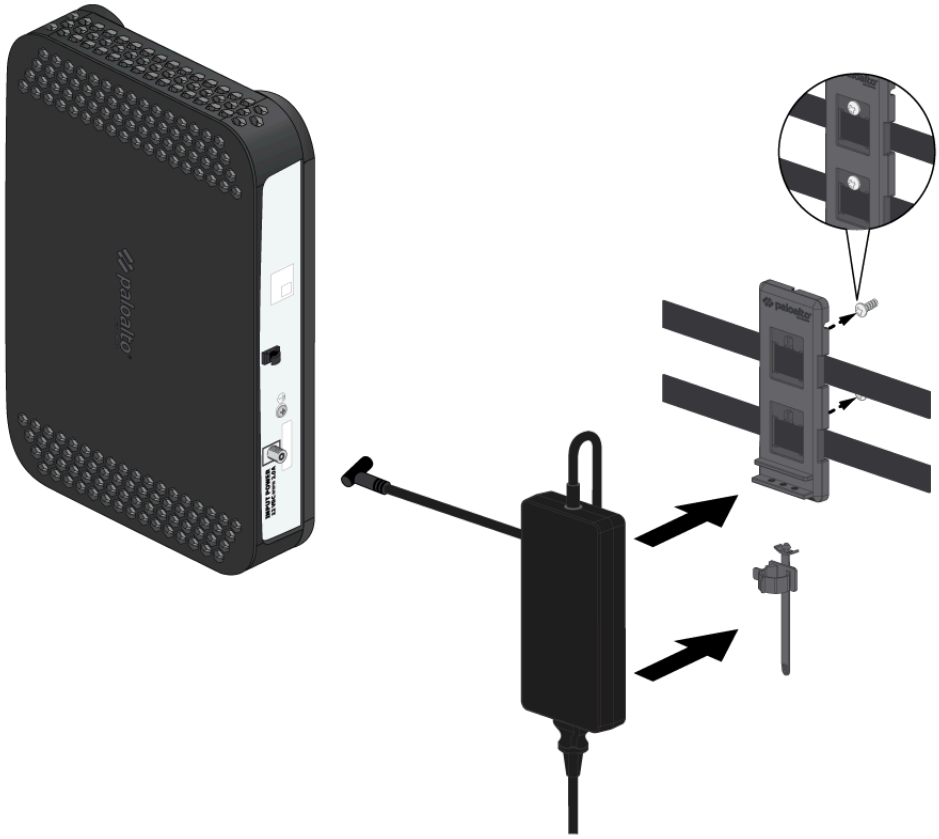
(PA-510)



 ©2026 Palo Alto Networks, Inc.

STEP 4 | Install the power adapter in the power adapter wall-mount bracket.

PA-501, PA-520-5G, and PA-505 — Install the power adapter in the power adapter wall-mount bracket using the Velcro straps and cable tie. Make sure to align the cable tie with the notches in the bracket to prevent the power cord from falling out. Next, loop the two Velcro straps through the side openings on the wall mount and over the power adapter. Lastly, loop the Velcro straps back over the top of the power adapter to secure it into place.



PA-510 — Install the power adapter in the power adapter wall-mount bracket using the Velcro straps and cable tie. Make sure to align the cable tie with the notches in the bracket to prevent the power cord from falling out. Next, loop the two Velcro straps through the side openings on the wall mount and over the power adapter. Lastly, loop the Velcro straps back over the top of the power adapter to secure it into place.

Connect the second power adapter through a different circuit breaker to provide power redundancy and allow for electrical circuit maintenance.

 ©2026 Palo Alto Networks, Inc.

STEP 5 | After you secure the power adapter to the bracket, mount the bracket next to the firewall using wood or drywall screws as appropriate.

(PA-501, PA-520-5G, and PA-505)



STEP 6 | (PA-510 firewall only) You can install an optional second power adapter next to the first power adapter.

 ©2026 Palo Alto Networks, Inc.

Install the PA-500 Series Firewall in an Equipment Rack

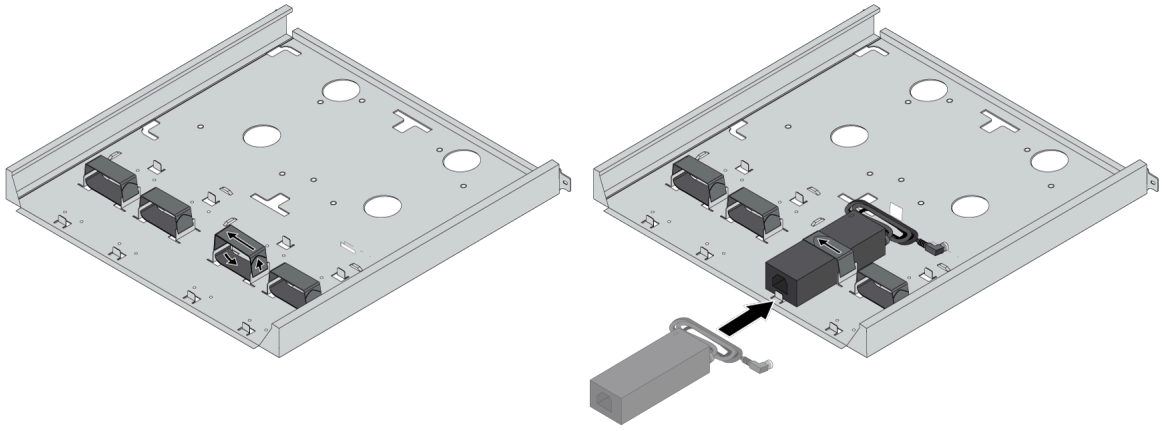
There are different rack mount SKUs that enable you to install a PA-500 Series firewall in a four-post 19" rack. The rack mount SKU used and the number of firewalls you can install depends on which PA-500 Series firewall you are installing.

- **PA-501 and PA-505**—One firewall and one power adapter can be installed in the PAN-1RU-4POST-RACK-10.
- **PA-510**—Up to two firewalls (with up to two power adapters each) can be installed in the PAN-1RU-4POST-RACK-10.
- **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.
- **PA-520-5G** — One firewall can be installed in the PAN-1RU-4POST-RACK-16 (four-post rack) or the PAN-2RU-2POST-RACK-17 (two-post rack).
- PAN-1RU-4POST-RACK-10
- PAN-1RU-4POST-RACK-11
- PAN-1RU-4POST-RACK-12
- PAN-1RU-4POST-RACK-16
- PAN-2RU-2POST-RACK-17

PAN-1RU-4POST-RACK-10

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

1. For each power adapter being installed (for a maximum of two for the PA-510), feed one Velcro strap through the opening at the dedicated power adapter locations on the mounting tray.

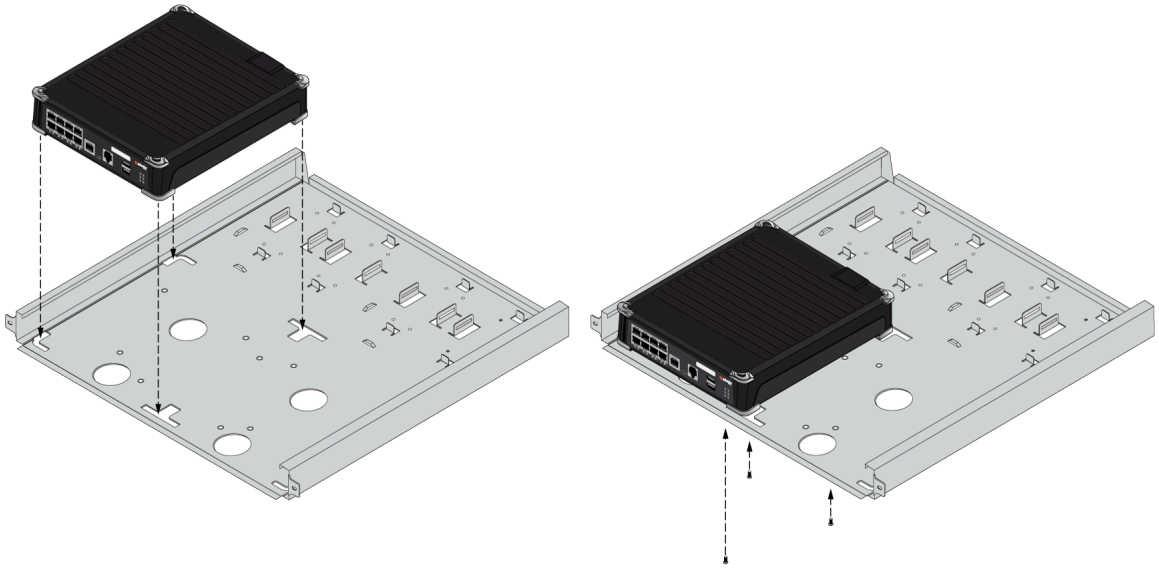


2. Place each power adapter into its designated location, then wrap each Velcro strap over the top of the adapter so that the adapter is fixed in place.

 ©2026 Palo Alto Networks, Inc.

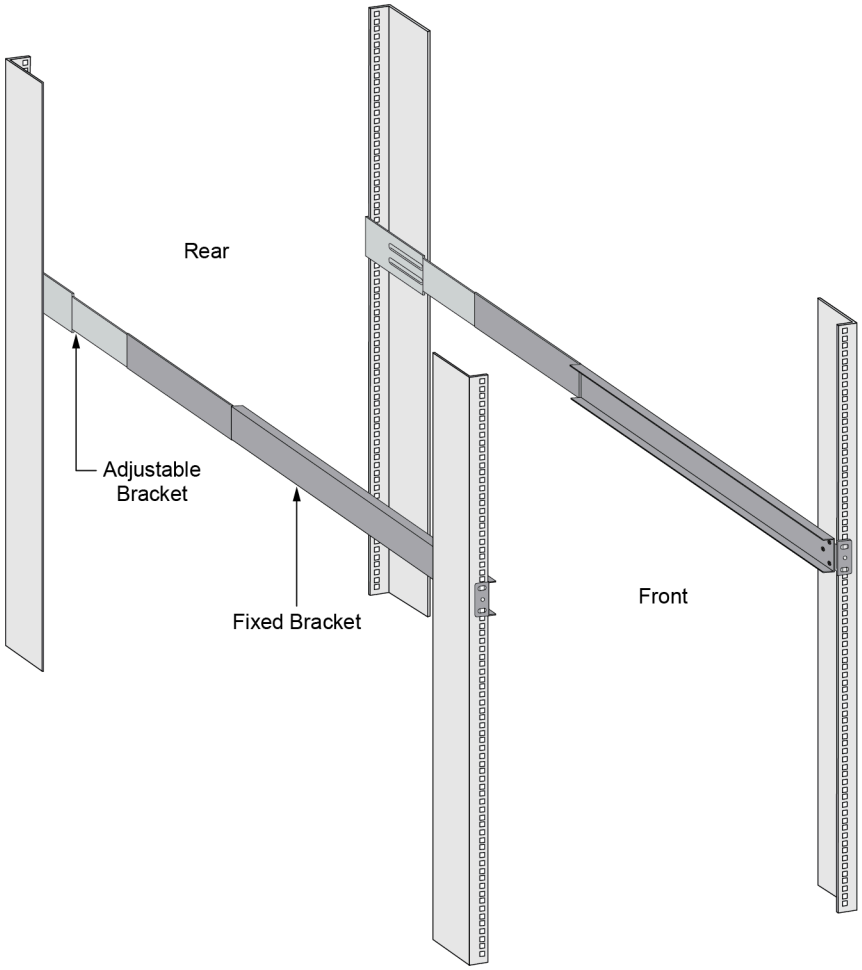
STEP 2 | Install the firewall in the mounting tray.

1. Align the four rubber feet of each device to the mounting tray, then secure it using three #6-32 x 3/16" long flathead screws.



 ©2026 Palo Alto Networks, Inc.

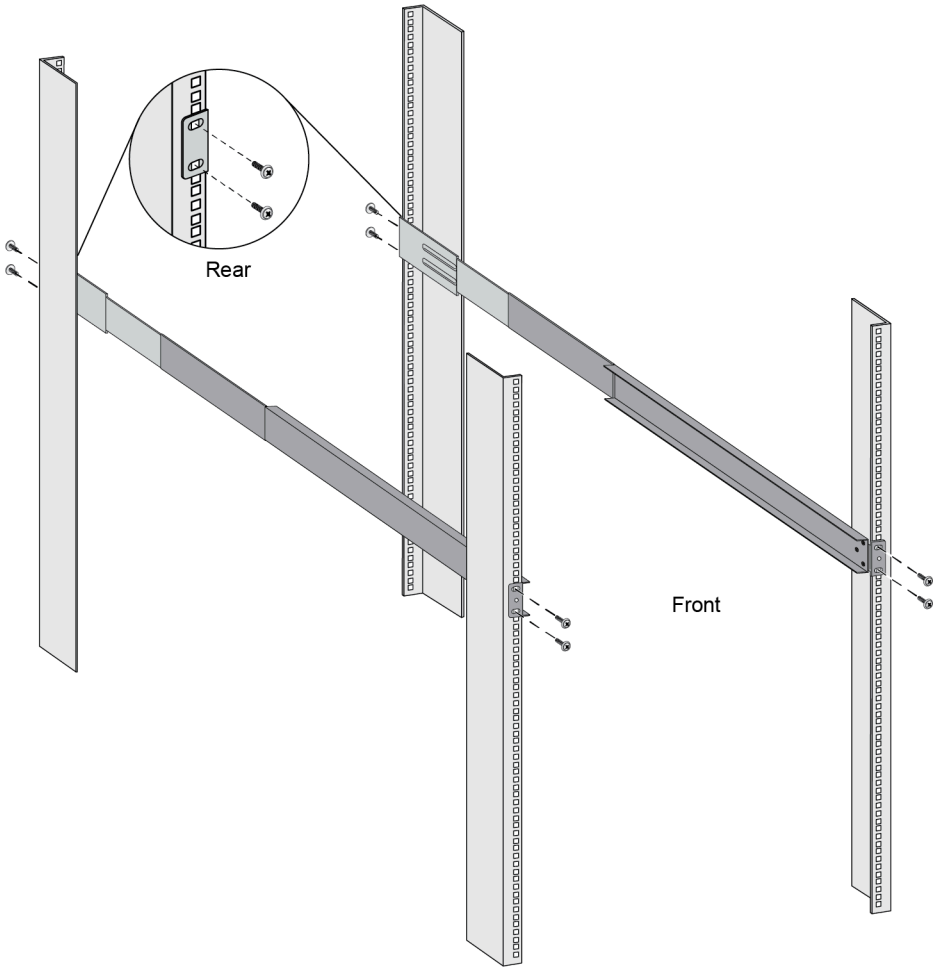
STEP 3 | Slide one of the adjustable mounting brackets into one of the fixed mounting brackets to create a mounting rail. Repeat for the second mounting rail. The adjustable and fixed brackets are the same for the left and right side.



STEP 4 | 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.

 ©2026 Palo Alto Networks, Inc.

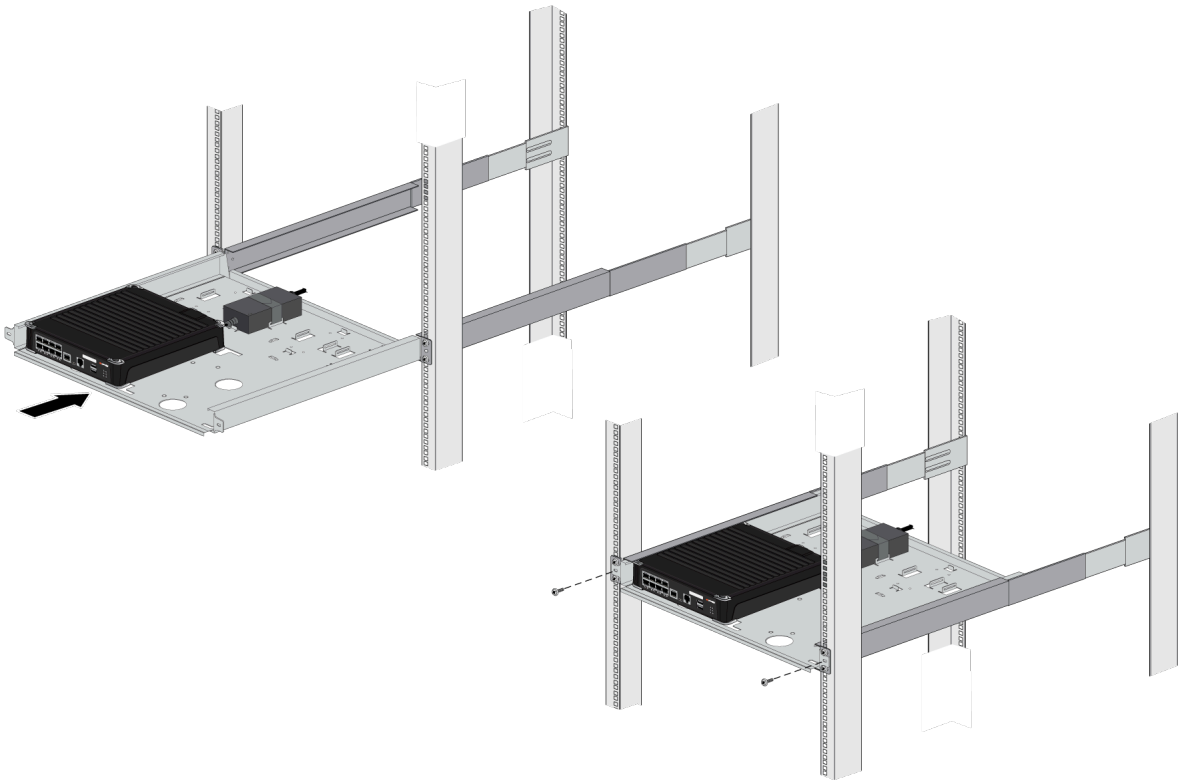
STEP 5 | Secure the rails to the equipment frame with mounting screws (not provided) compatible with your equipment frame. Tighten the screws to their recommended torque value.



STEP 6 | 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.

 ©2026 Palo Alto Networks, Inc.

STEP 7 | 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.



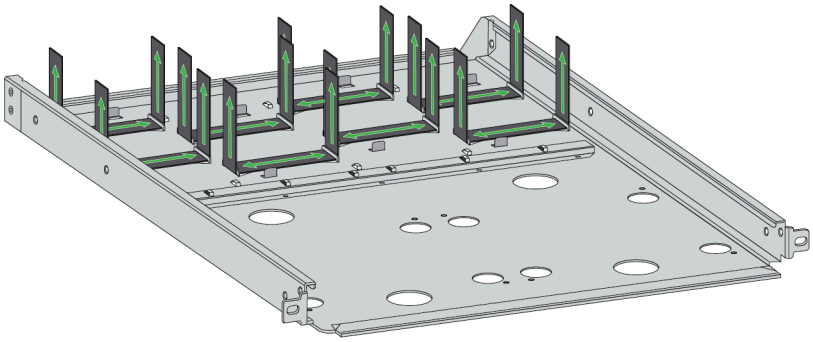
STEP 8 | Proceed to Connect Power to the PA-500 Series Firewall.

 ©2026 Palo Alto Networks, Inc.

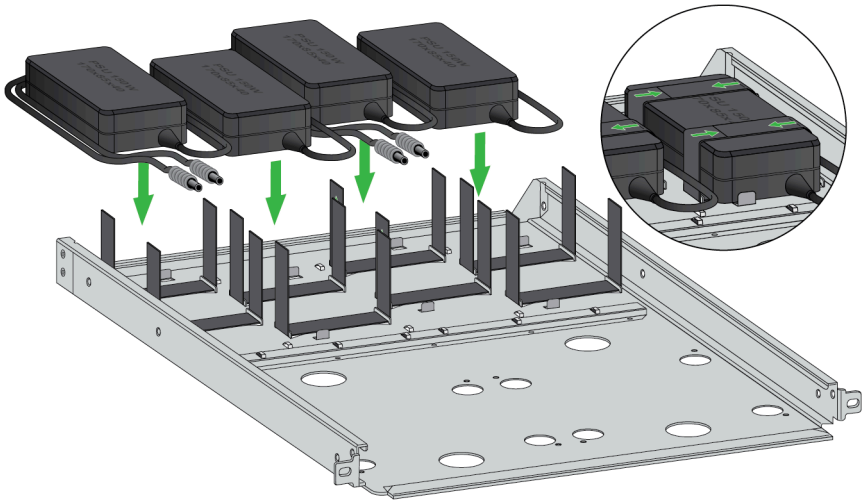
PAN-1RU-4POST-RACK-11

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

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.



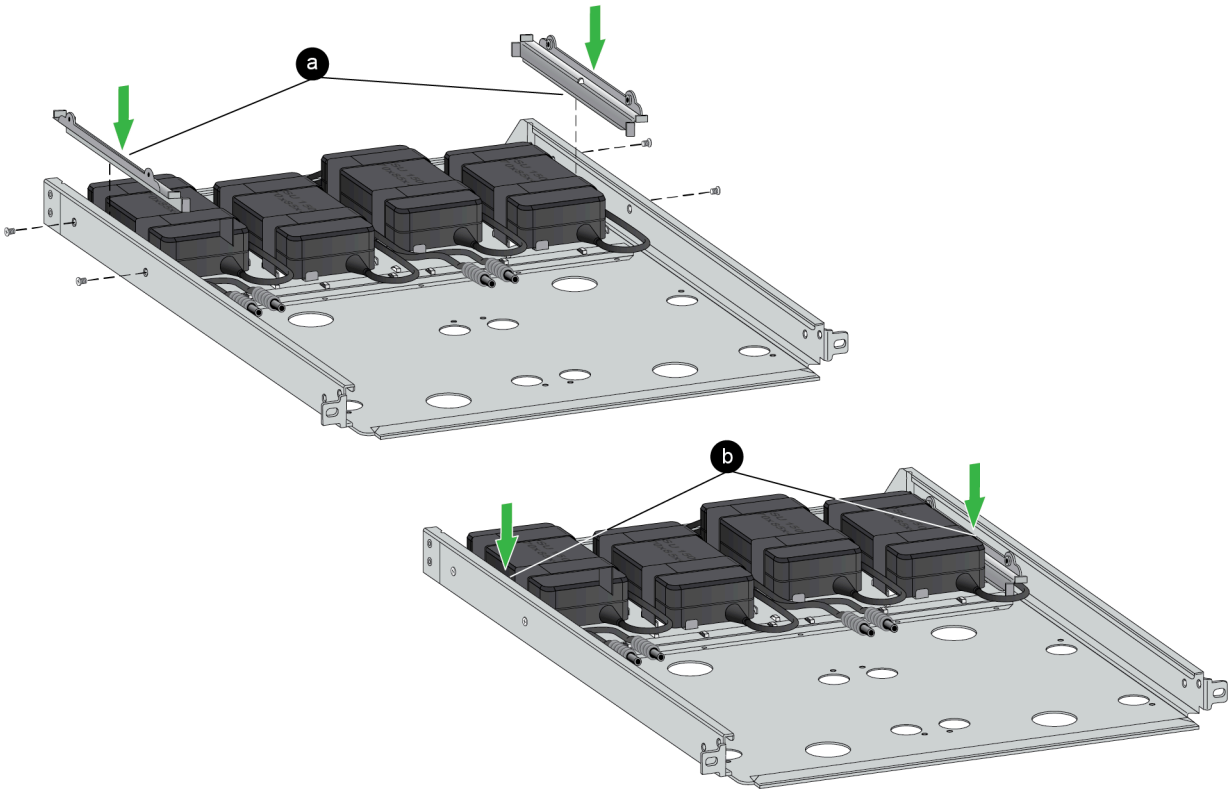
2. Place each power adapter into its designated location, then wrap both Velcro straps over the top of the adapter so that the adapter is fixed in place.



 ©2026 Palo Alto Networks, Inc.

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

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.

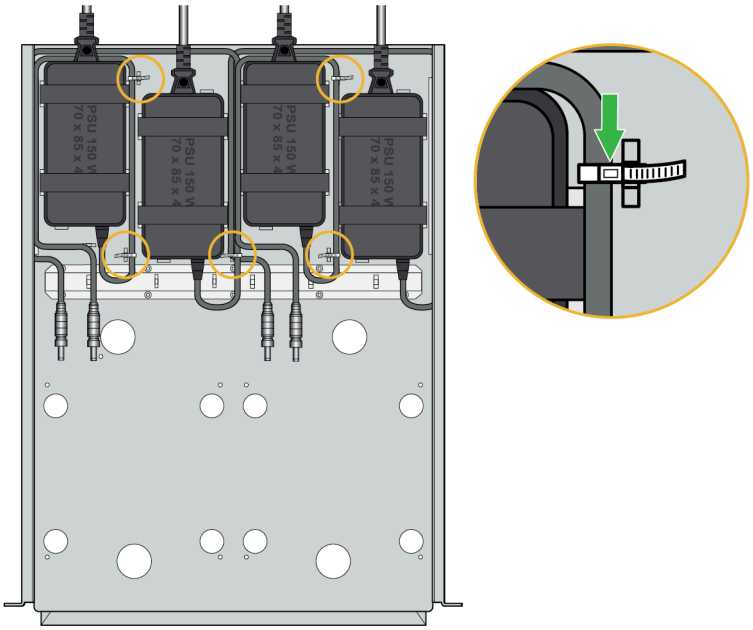


2. Using the following images as references, guide the remaining length of the power cables along the mounting tray. Thread the provided cable ties through the lances and cutouts in

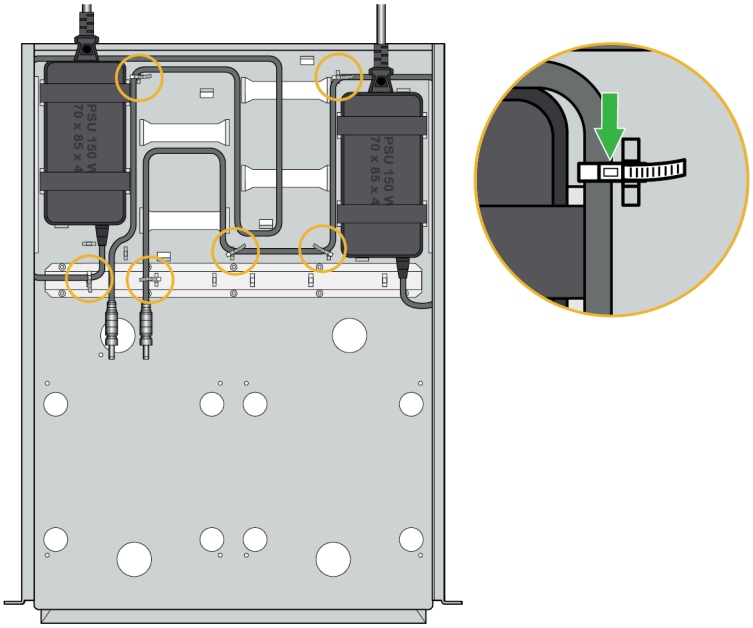
 ©2026 Palo Alto Networks, Inc.

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



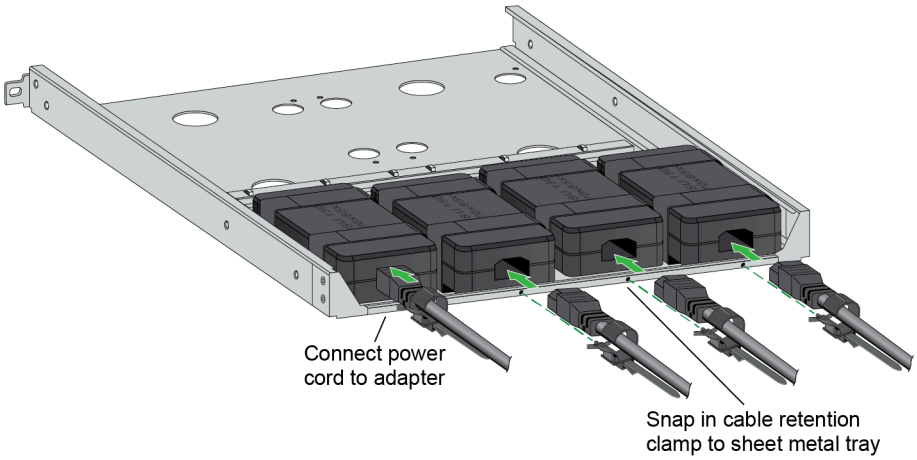
PA-550 and PA-560



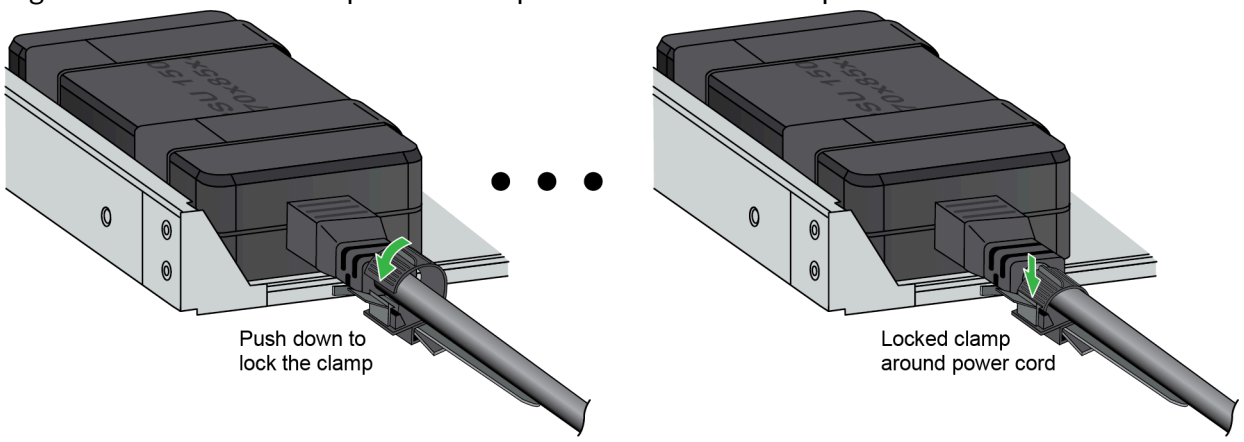
 ©2026 Palo Alto Networks, Inc.

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

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.

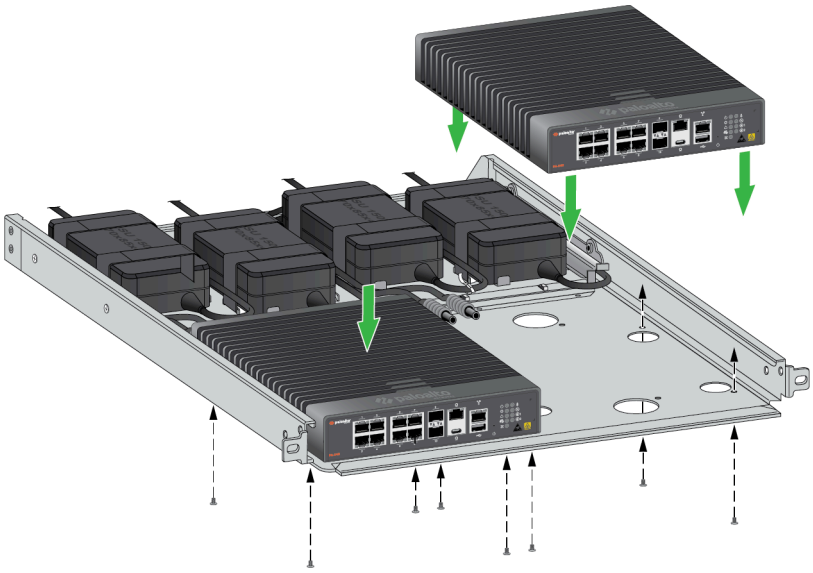


 ©2026 Palo Alto Networks, Inc.

STEP 4 | Install the firewall in the mounting tray.

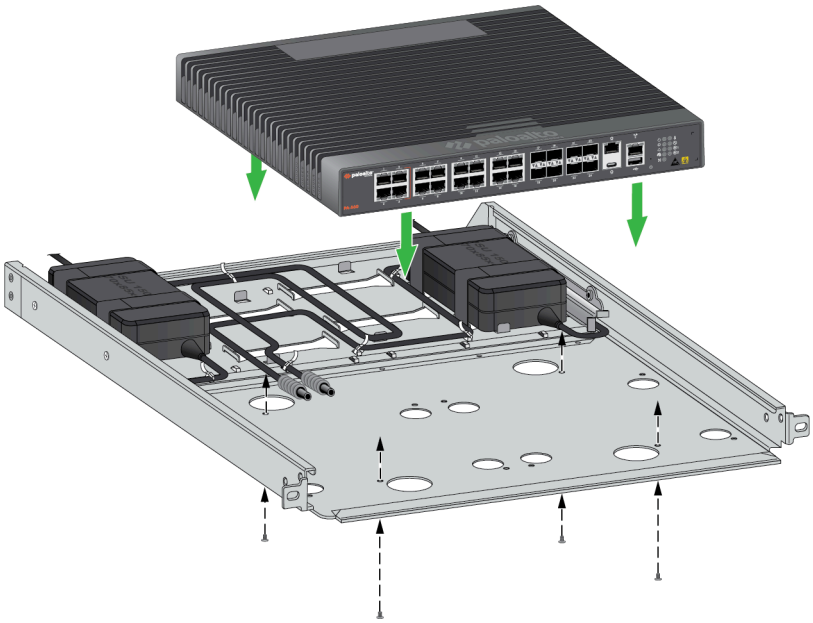
PA-520 and PA-540

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.



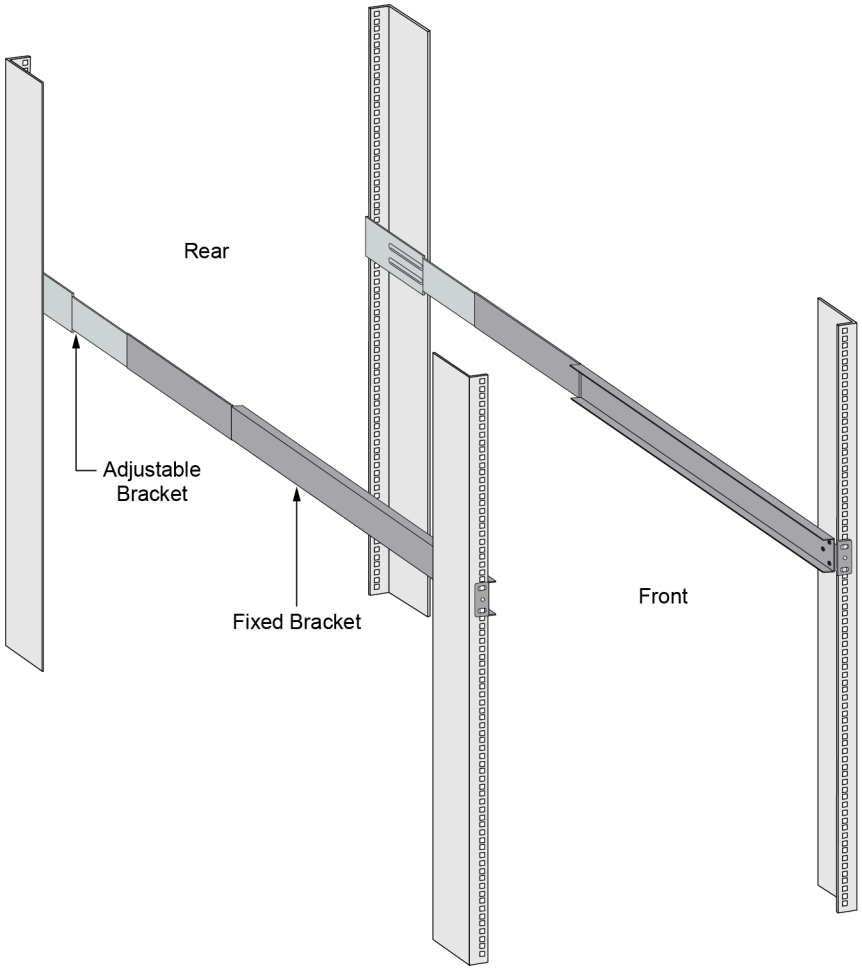
PA-550 and PA-560

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



 ©2026 Palo Alto Networks, Inc.

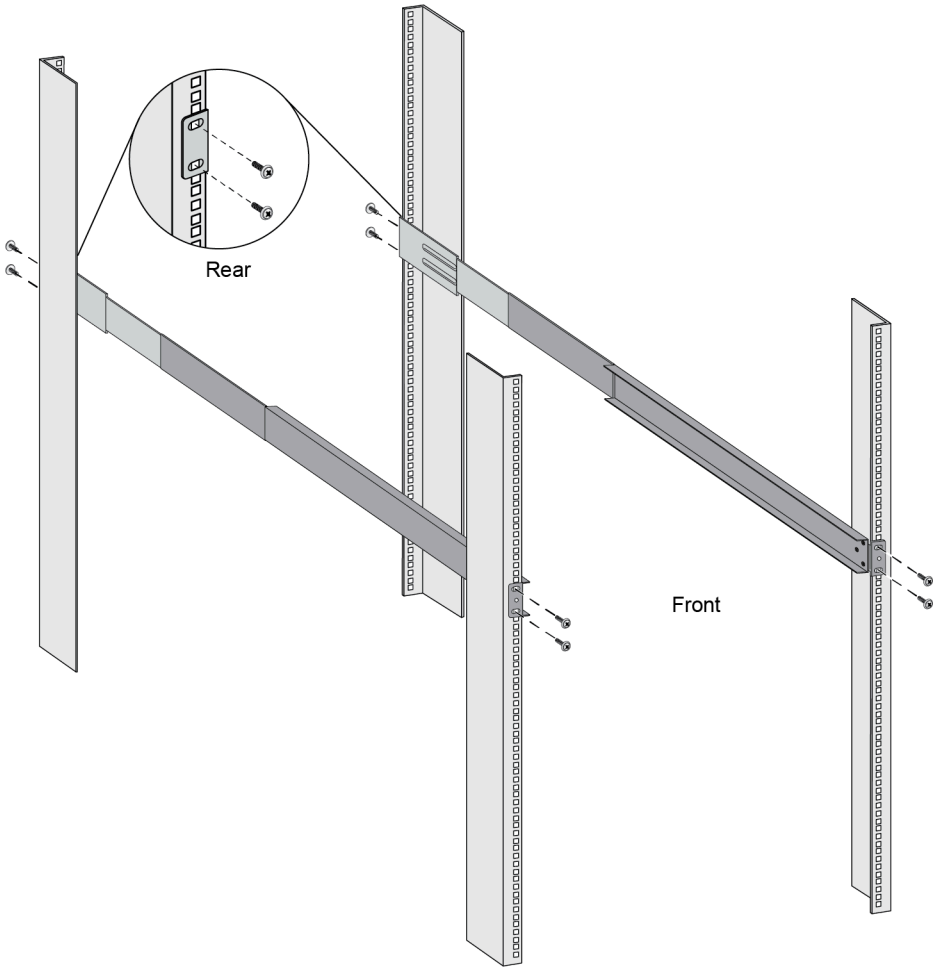
STEP 5 | Slide one of the adjustable mounting brackets into one of the fixed mounting brackets to create a mounting rail. Repeat for the second mounting rail. The adjustable and fixed brackets are the same for the left and right side.



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.

 ©2026 Palo Alto Networks, Inc.

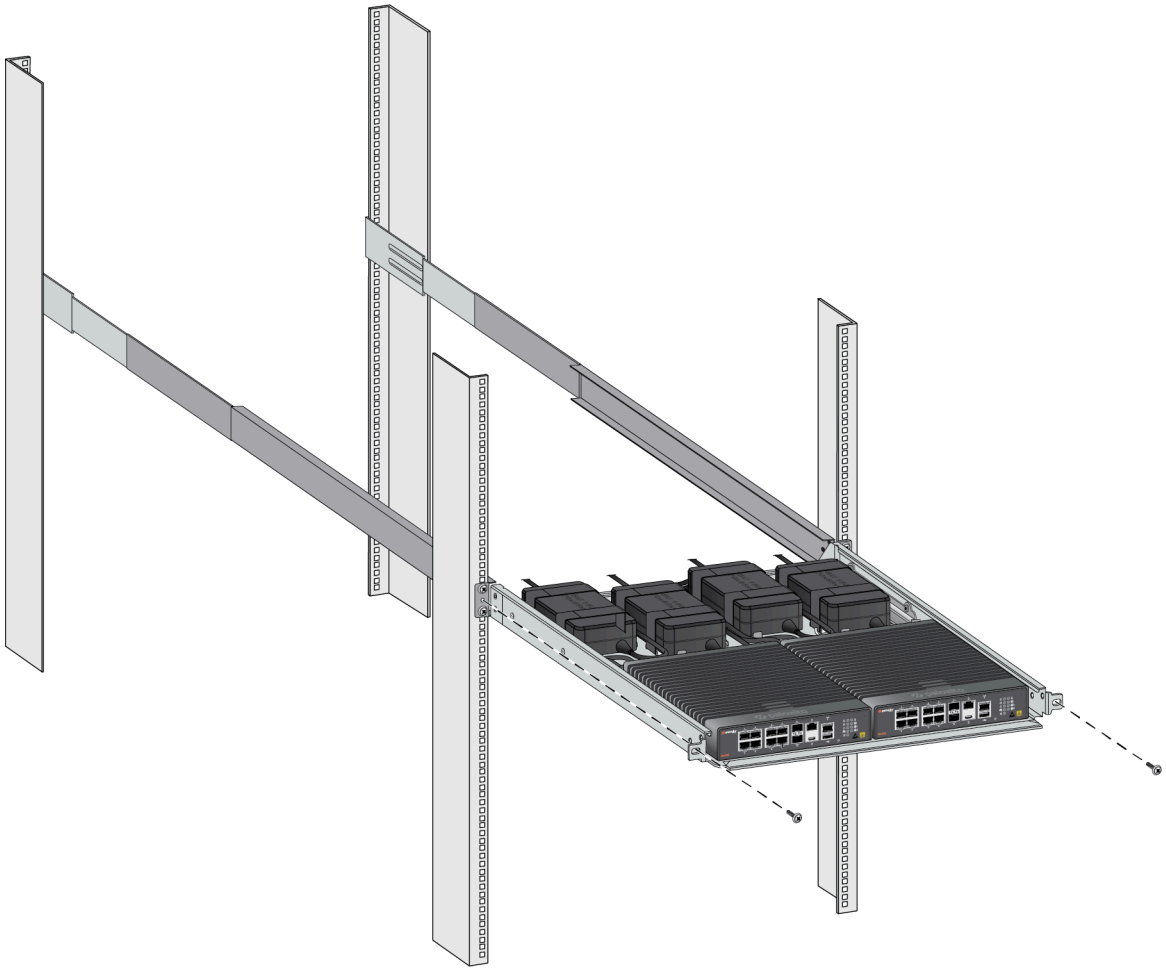
STEP 7 | Secure the rails to the equipment frame with mounting screws (not provided) compatible with your equipment frame. Tighten the screws to their recommended torque value.



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.

 ©2026 Palo Alto Networks, Inc.

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.



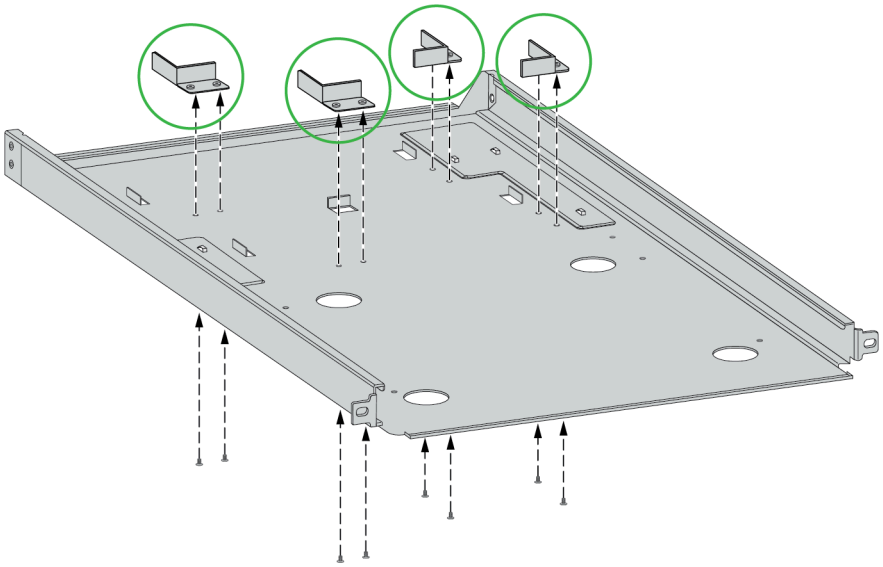
STEP 10 | Proceed to Connect Power to the PA-500 Series Firewall.

 ©2026 Palo Alto Networks, Inc.

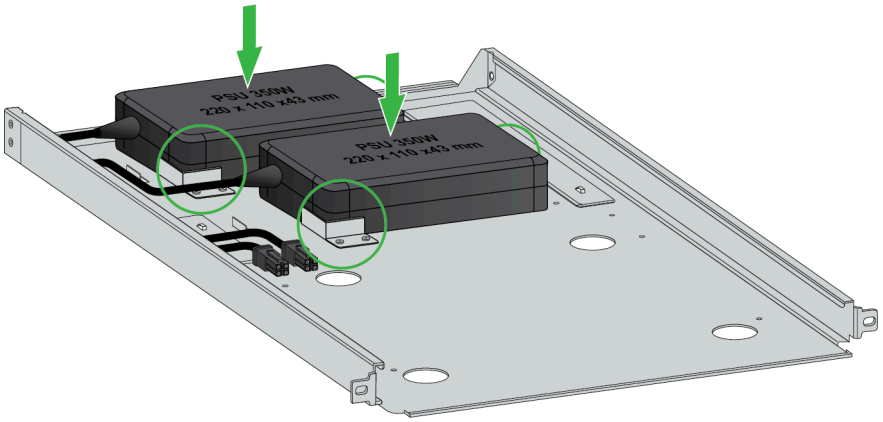
PAN-1RU-4POST-RACK-12

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

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.

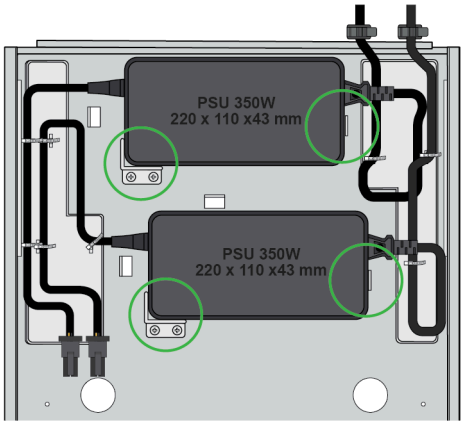


2. Place each power adapter into the location between the two installed stoppers.

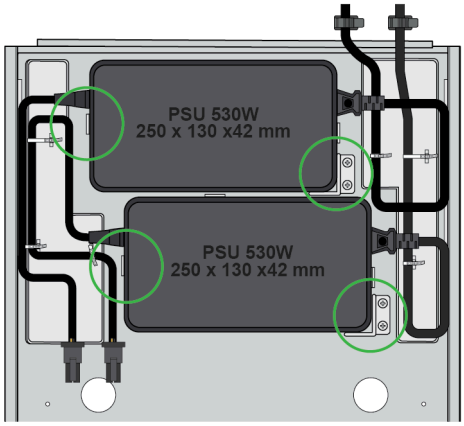


350W Power Adapter

 ©2026 Palo Alto Networks, Inc.



530W Power Adapter



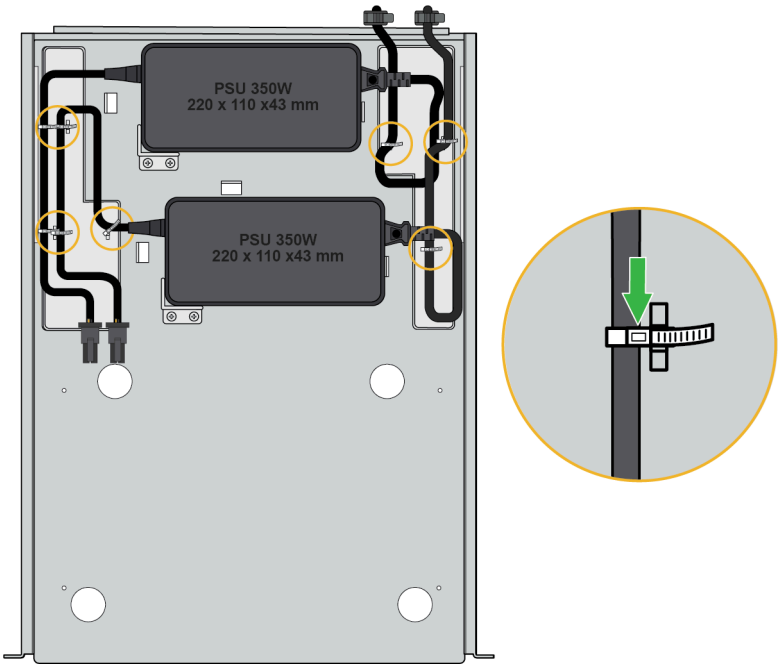
STEP 2 | Route the power cables through paths on the mounting tray.

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

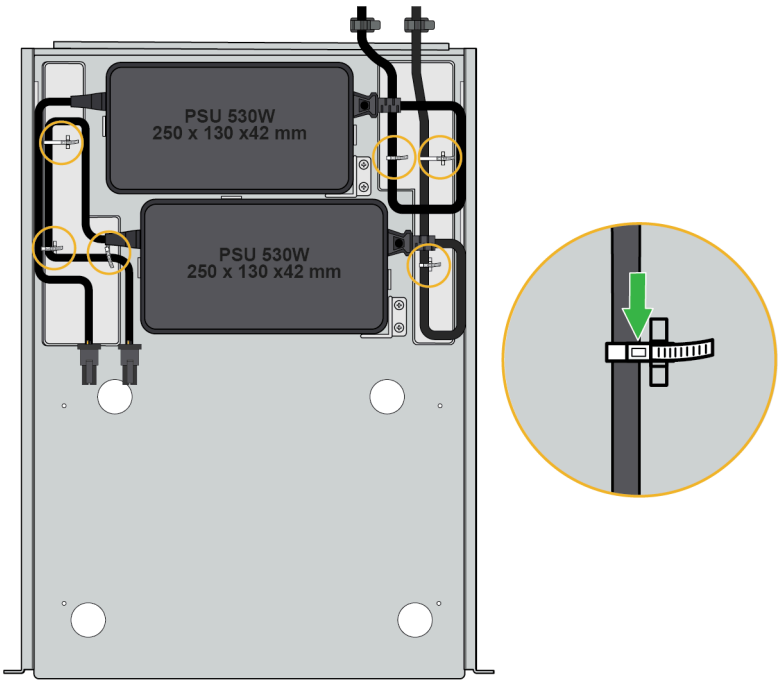
 ©2026 Palo Alto Networks, Inc.

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

350W Power Adapter



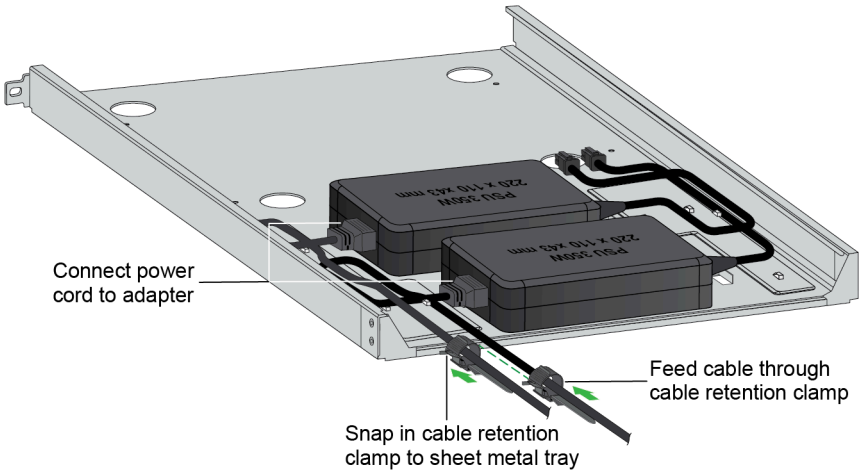
530W Power Adapter



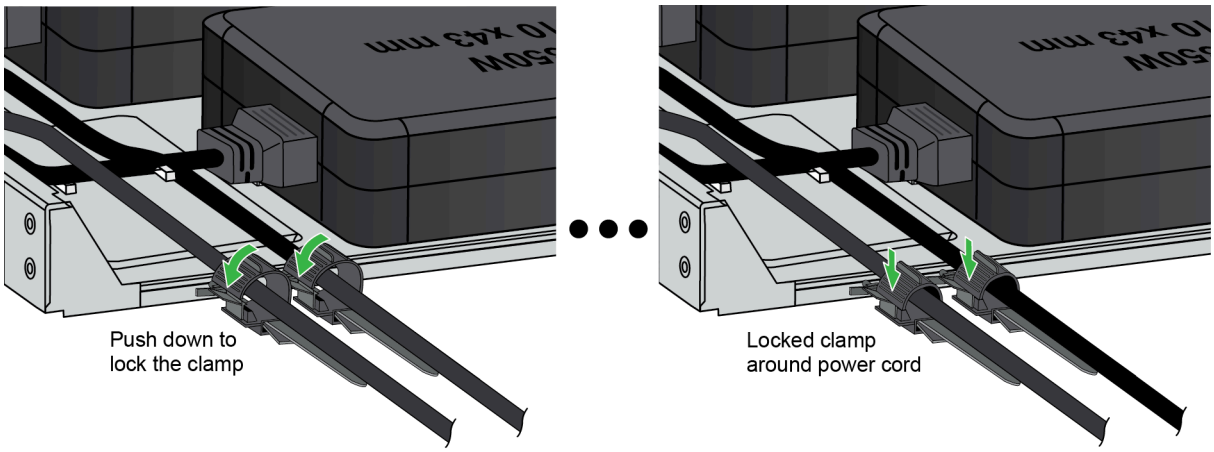
 ©2026 Palo Alto Networks, Inc.

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

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.



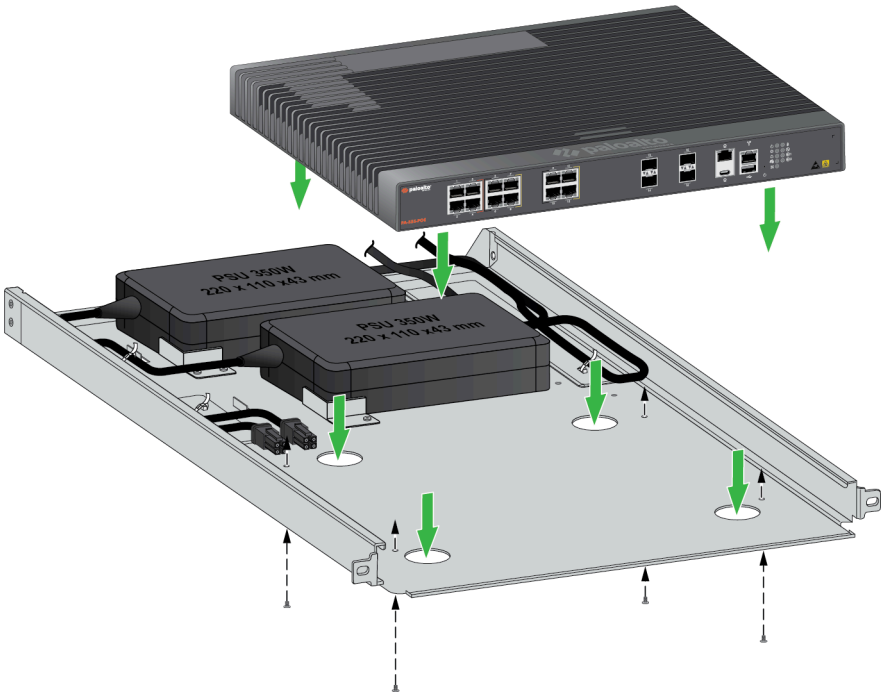
3. Tighten the retention clamp so that the power cord is locked in place.



 ©2026 Palo Alto Networks, Inc.

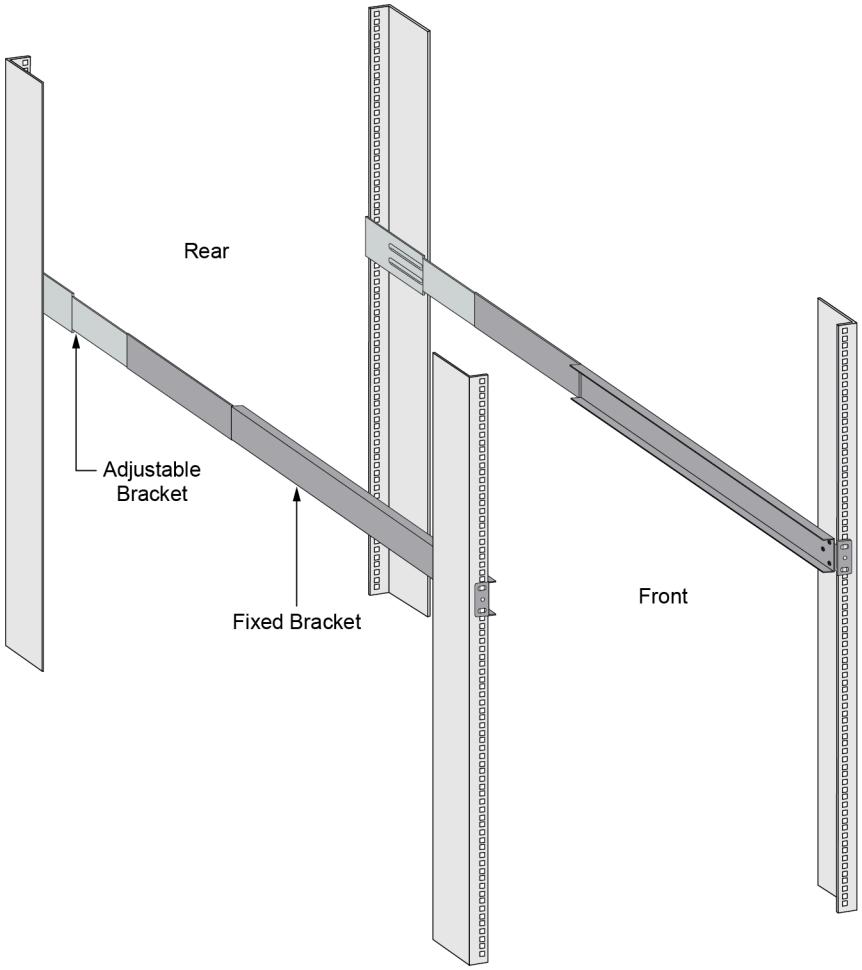
STEP 4 | Install the firewall in the mounting tray.

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



 ©2026 Palo Alto Networks, Inc.

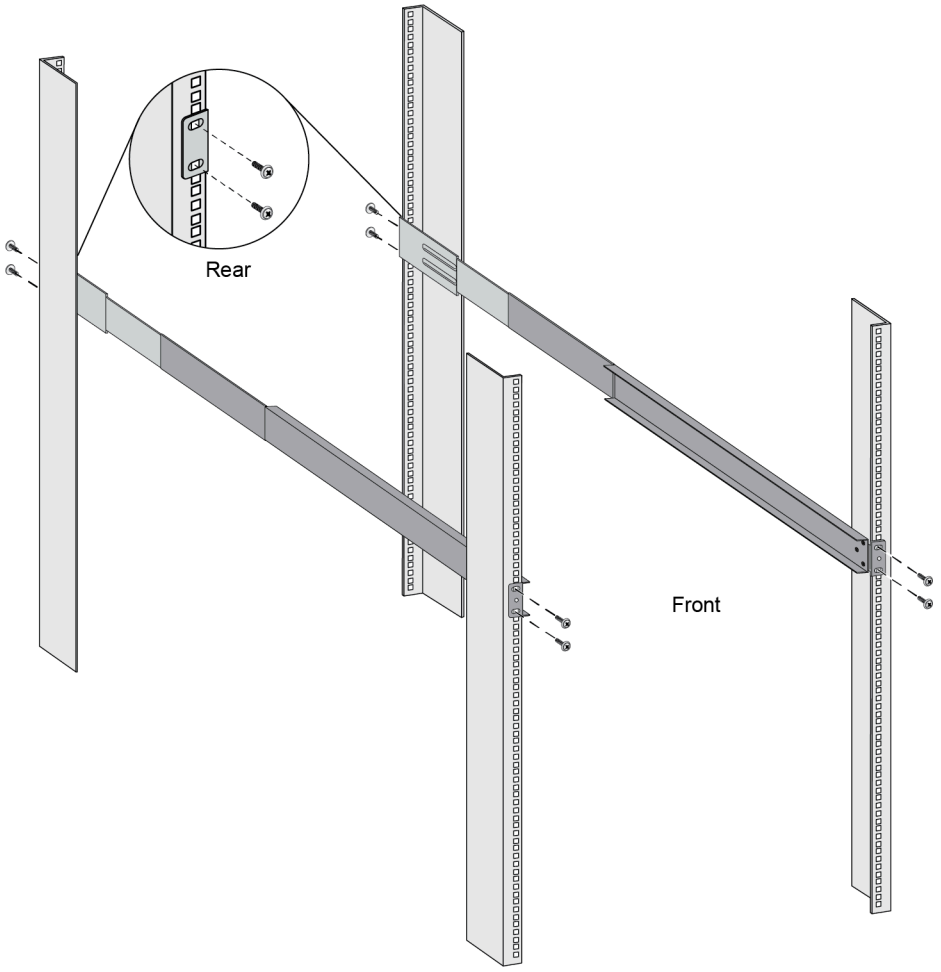
STEP 5 | Slide one of the adjustable mounting brackets into one of the fixed mounting brackets to create a mounting rail. Repeat for the second mounting rail. The adjustable and fixed brackets are the same for the left and right side.



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.

 ©2026 Palo Alto Networks, Inc.

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.

 ©2026 Palo Alto Networks, Inc.

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.



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

PAN-1RU-4POST-RACK-16

The PA-520-5G firewall can be mounted in a 4-post equipment rack using the PAN-1RU-4POST-RACK-16.

Table 4: Parts List – PAN-1RU-4POST-RACK-16

Quantity	Item
1	4-post rack mount tray
1	Fixed rail
1	Adjustable rail
2	Phillips pan head screw — M4 × 8mm

 ©2026 Palo Alto Networks, Inc.

Quantity	Item
30	Torx flat head screw (T10) — M3 × 5mm
16	Adhesive cable tie mount
28	Locking cable tie
4	Power cord retainer
8	Velcro strap
4	RF cable assembly — R/A SMA to N-type, 450mm L
4	RF cable assembly — ST SMA to N-type, IP67, 93mm L
2	Dual LTE/5G cable mount bracket
4	Single LTE/5G cable mount bracket
1	Power cord routing cover, right
1	Power cord routing cover, left

STEP 1 | Verify that the equipment rack has enough space to accommodate the firewall and has 1RU of space both above and below it.

STEP 2 | Align the four holes on the bottom of the firewall with the designated location in the mounting tray. Seat the firewall and use four M3 Torx flat head screws to secure it in place.

STEP 3 | Place up to two power adapters in the designated locations on the mounting tray. Loop the provided Velcro straps through the cutouts in the mounting tray, using two straps per power adapter.

STEP 4 | Connect your cables and antenna connectors to the device and route them through the mounting tray in order to minimize slack.

A total of six antenna cable brackets are included — four single cable brackets and two dual cable brackets. Install each bracket using two M3 screws through the holes in the mounting tray. After guiding the antenna cables through the brackets, secure each cable in place using the included lock washer and nut.

STEP 5 | Wrap cable ties through the small cutouts in the tray to secure the cables in place.

STEP 6 | Install the two provided power cord routing covers on the right and left sides of the tray. Use two M3 screws for each side (four total).

STEP 7 | Apply cable retention clamps over the power cords by slotting them into the tray.

STEP 8 | Slide the adjustable rail into the fixed rail to create a mounting rail. Repeat for the second mounting rail. The adjustable and fixed rails are the same for the left and right side.

 ©2026 Palo Alto Networks, Inc.

STEP 9 | 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 rail to the holes on the rear of the equipment frame.

STEP 10 | 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 11 | Slide the firewall (seated securely in the mounting tray) into the equipment rack.

- *Make sure that you do not block any of the airflow vents on the firewall.*

STEP 12 | Secure the mounting tray to the equipment rack using compatible screws.

- *After installation, you should inspect the hardware on a regular basis in order to account for dust, debris, and any other obstructions that may affect the firewall's airflow.*
- *Do not place any items or obstructions directly above or below the firewall within the 1RU of free space.*

PAN-2RU-2POST-RACK-17

The PA-520-5G firewall can be mounted in a 2-post equipment rack using the PAN-2RU-2POST-RACK-17.

Table 5: Parts List – PAN-2RU-2POST-RACK-17

Quantity	Item
1	2-post rack mount tray
8	Phillips pan head screw — M4 × 8mm
8	Torx flat head screw (T10) — M3 × 5mm
16	Locking cable tie
2	Power cord retainer
4	Velcro strap
4	RF cable assembly — R/A SMA to N-type, 450mm L

STEP 1 | Verify that the equipment rack has enough space to accommodate the firewall and has 1RU of space both above and below it.

STEP 2 | Using a Flathead screwdriver, remove the six screws (three on each side) securing the metal stiffener to the top of the rack tray. Remove the stiffener.

 ©2026 Palo Alto Networks, Inc.

STEP 3 | Align the four holes on the bottom of the firewall with the designated location in the mounting tray. Seat the firewall and use four M3 Torx flat head screws to secure it in place.

STEP 4 | Place up to two power adapters in the designated location beside the firewall. Loop the provided Velcro straps through the cutouts in the mounting tray, using two straps per power adapter. Use cord retainers to secure the power cables in place.

STEP 5 | Install the stiffener back over the device and secure it using three M3 screws on each side (6 total).

STEP 6 | Connect your cables and antenna connectors to the device and route them through the mounting tray in order to minimize slack.

STEP 7 | Wrap cable ties through the small cutouts in the tray to secure the cables in place.

STEP 8 | Slide the firewall (seated securely in the mounting tray) into the equipment rack.

- *Make sure that you do not block any of the airflow vents on the firewall.*

STEP 9 | Secure the mounting tray to the equipment rack using compatible screws.

- *After installation, you should inspect the hardware on a regular basis in order to account for dust, debris, and any other obstructions that may affect the firewall's airflow.*
- *Do not place any items or obstructions directly above or below the firewall within the 1RU of free space.*

 ©2026 Palo Alto Networks, Inc.

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.
- (ZTP mode — PA-520-5G) ZTP is also supported on Cellular 1/1. Whichever interface (Ethernet 1/1 or Cellular 1/1) establishes connectivity first is used for bootstrapping.

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.

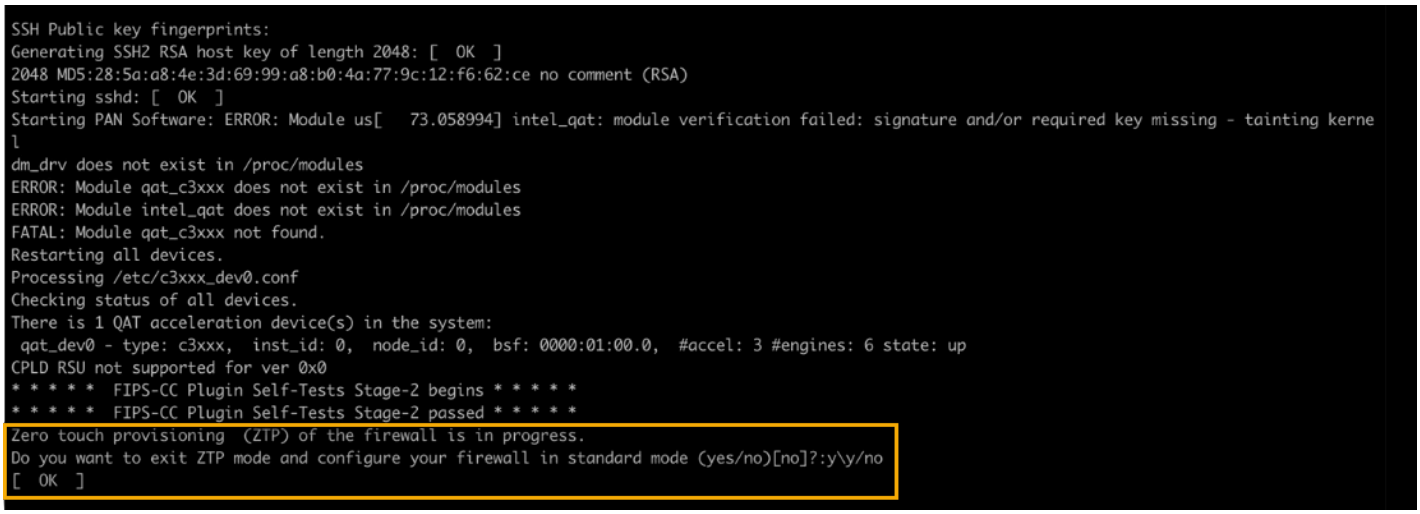
 ©2026 Palo Alto Networks, Inc.

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.

 ©2026 Palo Alto Networks, Inc.

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 firewall. See PA-500 Series Firewall Components to locate the ground point.

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.

 ©2026 Palo Alto Networks, Inc.

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

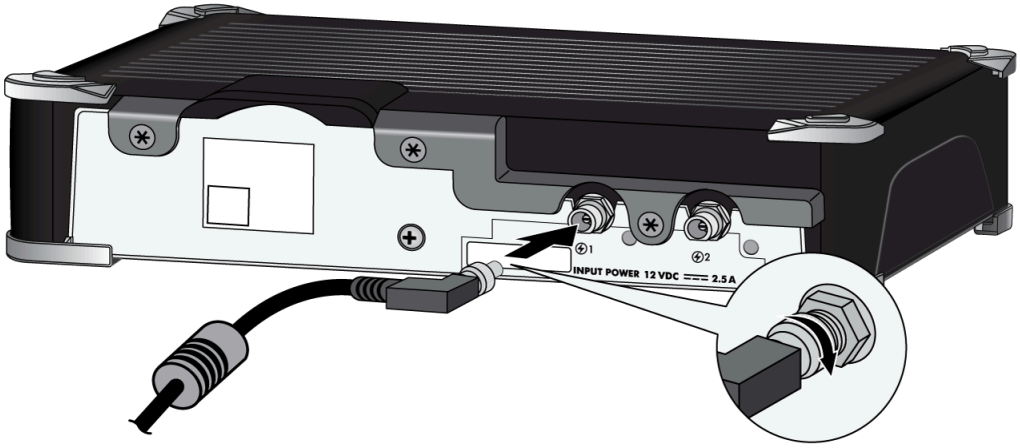
PA-501 and PA-505

Insert the DC connector from the power adapter into the port on the back of the firewall. Snap the DC connector cable to the cord retainer.



PA-510

Connect the power adapter connector into the left port on the back of the firewall. Tighten the connector nut to secure the cable to 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.

 ©2026 Palo Alto Networks, Inc.

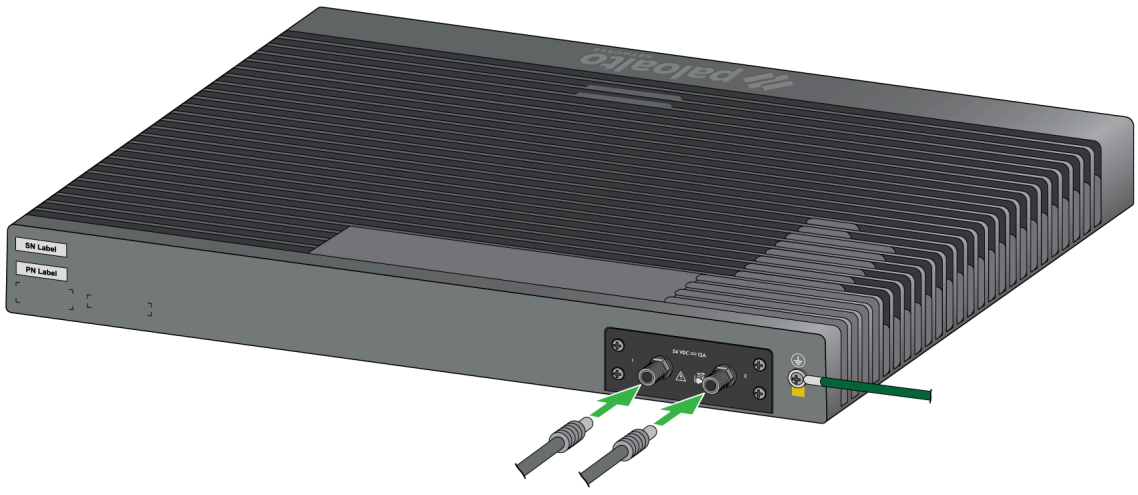


PA-520-5G

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

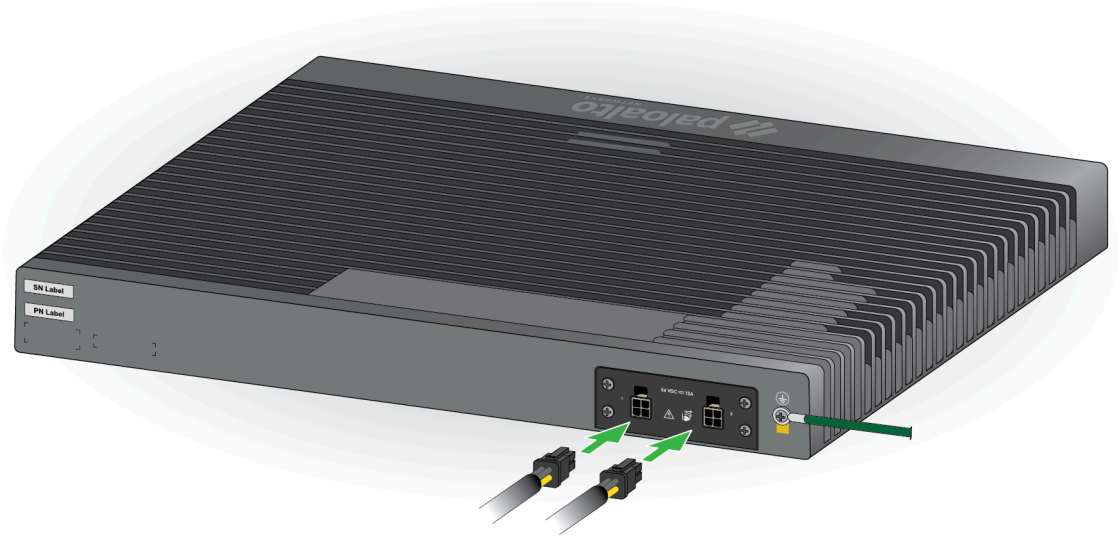
Plug the DC connector from the power adapter into the port on the firewall and tighten the connector nut to secure the cable to the firewall.



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.

 ©2026 Palo Alto Networks, Inc.



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.

 ©2026 Palo Alto Networks, Inc.

Install Antennas on the PA-520-5G Firewall

The PA-520-5G firewall has four SMA antenna connectors for 5G cellular connectivity. Two connectors (TX3/RX3 and TX4/RX4) are located on the front panel and two connectors (TX2/RX2 and TX1/RX1) are located on the rear panel. The four connectors support 4×4 MIMO antenna configurations.

Before installing the firewall, it is recommended that you conduct a cellular location assessment of the installation site to receive the best signal strength before installing the device.

The 5G antennas also support GPS and GLONASS (GNSS) for location services using L1 and L5 frequencies. No separate GPS antenna is required.

STEP 1 | Locate the two SMA antenna connectors (TX3/RX3 and TX4/RX4) on the front panel of the PA-520-5G firewall.

STEP 2 | Thread an antenna onto each front-panel SMA connector and tighten finger-tight. Do not overtighten.

STEP 3 | Locate the two SMA antenna connectors (TX2/RX2 and TX1/RX1) on the rear panel of the PA-520-5G firewall.

STEP 4 | Thread an antenna onto each rear-panel SMA connector and tighten finger-tight. Do not overtighten.

STEP 5 | Adjust the antenna orientation to receive the optimal signal strength in your environment.

Check the signal strength of the firewall by viewing the Cellular LED (see PA-500 Series Firewall LED Definitions) or by checking the Firewall Web Interface.

Ensure that power cables do not cross over the antennas as this can cause signal quality distortion and antenna performance degradation.

 ©2026 Palo Alto Networks, Inc.

Insert or Replace a SIM Card in a PA-500 Series 5G Firewall

The PA-520-5G firewall has two nano SIM card slots (SIM 1 and SIM 2) on its side panel. The firewall supports Active/Standby SIM selection, where one SIM card is active at a time and the other operates as a standby.

Use only nano SIM cards. Inserting an incorrectly sized SIM card can damage the SIM card slot.

STEP 1 | Power off the PA-520-5G firewall before inserting or removing SIM cards.

STEP 2 | Locate the SIM cover on the side panel of the PA-520-5G firewall. Unfasten the two screws using a Philips head screwdriver, then remove the SIM cover.

STEP 3 | (If replacing a SIM card) Remove the present SIM by gently pushing it inward using a tweezer tool. Release the tweezer and pull out the SIM.

STEP 4 | Insert the new nano SIM card into SIM slot 1 (SIM 1) with the gold contacts facing down and the notched corner aligned with the slot. Push the SIM card in until it clicks into place.

The SIM may get damaged if you attempt to insert it into the slot by the wrong end.

SIM 1 is the primary SIM slot by default. If you intend to use only one SIM, it is recommended to use SIM 1 as the primary slot. If you want to use SIM 2 as the primary slot, you must manually configure SIM 2 as the primary SIM slot using the Web Interface.

STEP 5 | (Optional) Insert a second nano SIM card into SIM slot 2 (SIM 2) for Active/Standby redundancy.

STEP 6 | Place the SIM cover back onto the device and refasten the two screws.

STEP 7 | Power on the PA-520-5G firewall.

 ©2026 Palo Alto Networks, Inc.

 ©2026 Palo Alto Networks, Inc.

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
- Insert or Replace a SIM Card in a PA-500 Series 5G Firewall

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.

 ©2026 Palo Alto Networks, Inc.

LED	Description
	• Off—The firewall is operating normally.
	**Controller** *This LED is reserved for a future release on certain PA-500 Series firewalls.* PA-520-5G firewall only • 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.

 ©2026 Palo Alto Networks, Inc.

LED	Description
	• Blue—A device locator beacon enabled by the administrator.
	**Power Supply 1 and 2** • Green—The PSU is powered with the correct voltage. • Yellow—The PSU is powered with the incorrect voltage. • Off—The PSU is not present.
5G	**5G** PA-520-5G firewall only • Blue—5G network connected. • Green—4G/3G network connected. • Red—Modem error, no SIM detected, or no signal. • Off—No modem detected.
	**Cellular Signal Strength (4-bar LED)** PA-520-5G firewall only Blue—5G Green—4G • 4 bars—Excellent signal strength. • 3 bars—Good signal strength. • 2 bars—Fair signal strength. • 1 bar—Poor signal strength. • Off—No service.
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

 ©2026 Palo Alto Networks, Inc.

LED	Description
	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.

 ©2026 Palo Alto Networks, Inc.

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 except for the PA-501 and PA-505 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.

 ©2026 Palo Alto Networks, Inc.

Insert or Replace a SIM Card in a PA-500 Series 5G Firewall

The PA-520-5G firewall has two nano SIM card slots (SIM 1 and SIM 2) on its side panel. The firewall supports Active/Standby SIM selection, where one SIM card is active at a time and the other operates as a standby.

Use only nano SIM cards. Inserting an incorrectly sized SIM card can damage the SIM card slot.

STEP 1 | Power off the PA-520-5G firewall before inserting or removing SIM cards.

STEP 2 | Locate the SIM cover on the side panel of the PA-520-5G firewall. Unfasten the two screws using a Philips head screwdriver, then remove the SIM cover.

STEP 3 | (If replacing a SIM card) Remove the present SIM by gently pushing it inward using a tweezer tool. Release the tweezer and pull out the SIM.

STEP 4 | Insert the new nano SIM card into SIM slot 1 (SIM 1) with the gold contacts facing down and the notched corner aligned with the slot. Push the SIM card in until it clicks into place.

The SIM may get damaged if you attempt to insert it into the slot by the wrong end.

SIM 1 is the primary SIM slot by default. If you intend to use only one SIM, it is recommended to use SIM 1 as the primary slot. If you want to use SIM 2 as the primary slot, you must manually configure SIM 2 as the primary SIM slot using the Web Interface.

STEP 5 | (Optional) Insert a second nano SIM card into SIM slot 2 (SIM 2) for Active/Standby redundancy.

STEP 6 | Place the SIM cover back onto the device and refasten the two screws.

STEP 7 | Power on the PA-520-5G firewall.

 ©2026 Palo Alto Networks, Inc.

 ©2026 Palo Alto Networks, Inc.

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
- PA-500 Series Firewall Electrical Specifications
- PA-500 Series Firewall Environmental Specifications
- PA-500 Series Firewall Antenna Specifications
- PA-500 Series Firewall Miscellaneous Specifications

PA-500 Series Firewall Physical Specifications

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

Specification	Value
Rack units and dimensions	**PA-501 and PA-505** • Height x Width x Depth—1.63 in x 9.53 in x 6.42 in (43.9 mm x 242.06 mm x 163 mm) • Rack units—1U **PA-510** • Height x Width x Depth—1.74 in x 8.07 in x 8.83 in (44.2 mm x 205 mm x 224.3 mm) • Rack units—1U **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-520-5G** • Height x Width x Depth—1.67 in x 7.95 in x 7.91 in (42.5 mm x 202 mm x 201 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-501 and PA-505** • Firewall weight—3.0 lbs (1.36 kg) • Shipping weight—6.0 lbs (2.72 kg) **PA-510** • Firewall weight—5.0 lbs (2.27 kg) • Shipping weight—7.8 lbs (3.54 kg) **PA-520 and PA-540**

©2026 Palo Alto Networks, Inc.

Specification	Value
	• Firewall weight—5.8 lbs (2.6 kg) • Shipping weight—8.6lbs (3.9 kg) **PA-520-5G** • Firewall weight—4.8 lbs (2.18 kg) • Shipping weight—7.0 lbs (3.18 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)

 ©2026 Palo Alto Networks, Inc.

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-501 and PA-505 firewalls operate on a single power adapter. The PA-510, PA-520, PA-540, PA-550, and PA-560 can operate on one power adapter or you can install a second power adapter for load sharing and power redundancy. The PA-520-5G firewall operates on DC power that is provided by the external power adapter (provided). The firewall can operate on one power adapter or you can install a second power adapter for power redundancy. The two power inputs do not support load sharing.
Input voltage	**PA-501, PA-505, PA-510, PA-520, PA-520-5G, 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-501 and PA-505**—23W **PA-510**—34.3W **PA-520 and PA-540**—30W **PA-520-5G**—36W **PA-545-POE**—336W **PA-550**—57W **PA-555-POE**—503W **PA-560**—106W
Maximum current consumption	**PA-510**—2.5A@12VDC **PA-520**—4A@12VDC **PA-540**—4A@12VDC

©2026 Palo Alto Networks, Inc.

Specification	Value
	PA-520-5G—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** • 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

©2026 Palo Alto Networks, Inc.

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-501 and PA-505**—78/hour **PA-510**—117/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)	**PA-501, PA-505, and PA-510**—FCC Class B, CE Class B, and VCCI Class B **PA-520, PA-540, PA-545-POE, PA-550, PA-555-POE, and PA-560**—FCC Class A, CE Class A, and VCCI Class A
Acoustic noise	**PA-501, PA-505, PA-510, PA-520, PA-520-5G, 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)

©2026 Palo Alto Networks, Inc.

PA-500 Series Firewall Antenna Specifications

The following table describes the PA-520-5G firewall included antenna specifications.

Specification	Value
Antenna	**PAN-PA-5G-ANTENNA** • Four 5G multi-band antennas (4x4 MIMO, omni-directional)
Supported radio frequency (RF) bands	**FR1 (sub-6GHz):** n1, n2, n3, n5, n7, n8, n12, n20, n25, n26, n28, n29, n38, n40, n41, n48, n66, n71, n75, n76, n77, n78, n79, n106 **FDD LTE:** B1, B2, B3, B4, B5, B7, B8, B12, B13, B14, B17, B18, B19, B20, B25, B26, B28, B29, B30, B32, B66, B71, B106 **TDD LTE:** B34, B38, B39, B40, B41, B42, B43, B46, B48 **3G FDD (DC-HSPA+):** B1, B2, B4, B5, B6, B8, B19
Frequency range	615MHz–5925MHz
Peak gain	5 dBi
Voltage standing wave ratio (VSWR)	< 3:1
Nominal RF port impedance	50Ω
Antenna power handling	1W
Antenna ports	SMA-F connectors
Carrier certification	AT&T, Verizon, T-Mobile, NTT DoCoMo, and Telstra

©2026 Palo Alto Networks, Inc.

PA-500 Series Firewall Miscellaneous Specifications

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

Specification	Value
Storage capacity	**PA-501, PA-505, PA-520-5G, and PA-510**—128 GB **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

©2026 Palo Alto Networks, Inc.