paloalto TECHDOCS

PA-3500 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

November 14, 2025

Table of Contents

Before You Begin

Read the following topics before you install or service the PA-3500 Series firewall.

- Safety and Compliance
- Parts List and Required Tools

Safety and Compliance

Read the Safety Warnings prior to installing the PA-3500 Series firewall hardware. This section also lists compliance and regulatory statements that apply to the firewall.

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).
- At least two people are recommended for unpacking, handling, and relocating the heavier firewalls.
- Do not connect a supply voltage that exceeds the input range of the firewall or appliance. For details on the electrical range, refer to electrical specifications in the hardware reference for your firewall or appliance.

  French Translation: Veillez à ce que la tension d'alimentation ne dépasse pas la plage d'entrée du pare-feu ou du dispositif. Pour plus d'informations sur la mesure électrique, consulter la rubrique des caractéristiques électriques dans la documentation de votre matériel de pare-feu ou votre dispositif.

	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 are the PA-3500 Series firewall hardware compliance statements:

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

  The above product conforms with Low Voltage Directive 2014/35/EU and complies with the requirements relating to electrical equipment designed for use within certain voltage limits.
- **Federal Communications Commission (FCC) statement for a Class A digital device or peripheral**—This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide

reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment to an outlet on a circuit that is different from the one to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

- **ICES (Canadian Department Compliance Statement)**—This Class A digital apparatus complies with Canadian ICES-003.

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

  Risk of explosion if battery is replaced by an incorrect type. Dispose of used battery according to local regulations.
- **VCCI**—This section provides the compliance statement for the Voluntary Control Council for Interference by Information Technology Equipment (VCCI), which governs radio frequency emissions in Japan.

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

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

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

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-3500 Series firewall.

Table 1: Parts List — PA-3500 Series

Quantity	Item
1	PA-3500 Series Firewall
1	Rack mount kit • **PA-3510 and PA-3520**—PAN-PA-1RU-RACK-KIT • **PA-3530 and PA-3540**—PAN-PA-2RU-RACK4
2	(AC power supplies only) AC power cord
1	CAT6 Ethernet cable
1	USB-C cable
1	Desiccant

The following tools are either required or recommended when installing the PA-3500 Series firewall hardware.

- (Optional) Mechanical lift – for lifting and moving the firewall
- ESD wrist strap
- Equipment rack screws
- #1 and #2 Phillips-head torque driver

PA-3500 Series Firewall Overview

The PA-3500 Series Next-Generation firewalls are high performance appliances designed for large branch, enterprise, and data center environments. The following models make up the PA-3500 Series:

- PA-3510
- PA-3520
- PA-3530
- PA-3540

The PA-3500 Series firewalls provide flexibility in performance and redundancy to adapt to your deployment requirements. These models can use either AC or DC power and come with a 960GB SSD for local storage. Dedicated computing and hardware resources ensure predictable performance in networking, zero trust security, threat performance, and management functions. These firewalls also feature a Trusted Platform Module (TPM) 2.0 for PAN-OS key storage and security.

First Supported PAN-OS® Software Release: PAN-OS 12.2.2

The PA-3500 Series Firewall Components topic describes the hardware components of the PA-3500 Series firewalls.

PA-3500 Series Firewall Components

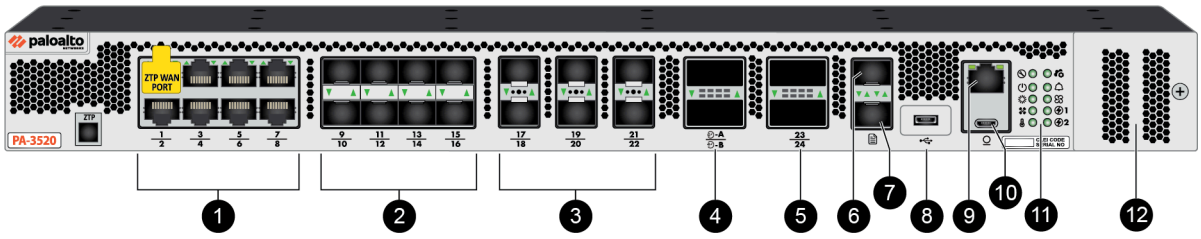
Refer to the following sections to view the front, back, and top panel components of the PA-3500 Series firewalls.

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

- PA-3510 and PA-3520
- PA-3530 and PA-3540

PA-3510 and PA-3520

The following image shows the front panel of the PA-3510 and PA-3520 firewalls (PA-3520 pictured) and the table describes each front panel component.



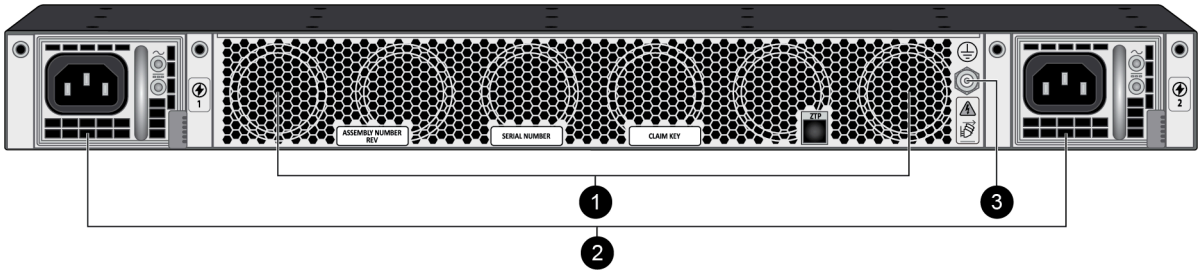
Item	Component	Description
1	Copper RJ-45 Ports	Eight 1Gbps/2.5Gbps/5Gbps/10Gbps RJ-45 ports. Port 1 is used for Zero Touch Provisioning (ZTP).
2	SFP/SFP+ Ports	Eight 1Gbps/10Gbps SFP/SFP+ ports.
3	SFP28 Ports	Six 25Gbps SFP28 ports.
4	HSCI Ports	Two HSCI ports that offer 100Gbps connectivity and are used to connect two firewalls in a high availability (HA) configuration as follows: • In an active/passive configuration, this port is for HA2 (data link). • In an active/active configuration, you can configure this port for HA2 and HA3. HA3 is used for packet forwarding for asymmetrically routed sessions that require Layer 7 inspection for App-ID and Content-ID.

Item	Component	Description
		The HSCI ports must be connected directly between the two firewalls in the HA configuration (without a switch or router between them). *The HSCI ports are not recommended for long-distance links (½ mile/1 km and above) regardless of the optical transceiver's rated capabilities. For long-distance links, use the data ports.* *Do not assign an IP address to the HSCI port. The port carries raw Layer 1 traffic that is not routable or switchable and does not support IP addressing. Assigning an IP address to the HSCI port causes the firewall to enter a permanent suspended state.* *For high-throughput deployments, do not use a 1Gbps copper interface for HA2. Use the HSCI port or a 10Gbps/40Gbps fiber interface to ensure sufficient bandwidth for HA data synchronization.* *When you configure path monitoring, do not use your HA peer's data interface IP address as the monitored destination. Using the peer's IP address causes the firewall to incorrectly detect a path failure and trigger an unnecessary failover.*
5	QSFP28 Ports	Two 40Gbps/100Gbps QSFP28 ports.
6	Management Port	One 1Gbps/10Gbps SFP+ Management port used to access the management web interface and perform administrative tasks. The firewall uses this port for management services, such as retrieving licenses and updating threat and application signatures.
7	Logging Port	One 1Gbps/10Gbps SFP+ logging port that can be used as a log interface. You must Configure Log Forwarding to forward logs from the port to one or more log collectors. *You can use any port on the firewall as a log interface.*

Item	Component	Description
8	USB-C 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.
9	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: 115,200 • Data bits: 8 • Parity: None • Stop bits: 1 • Flow control: None
10	Console port (USB-C)	Use this port to connect a management computer to the firewall using a standard Type-C USB cable. The console connection provides access to firewall boot messages, the Maintenance Recovery Tool (MRT), and the command line interface (CLI).
11	LED Indicators	Ten LEDs that indicate the status of various hardware components. For details on the LEDs, see PA-3500 Series Firewall LED Definitions.
12	SSD Cover	Secures the device's SSD, which contains PAN-OS system files, system logs, and network traffic logs.

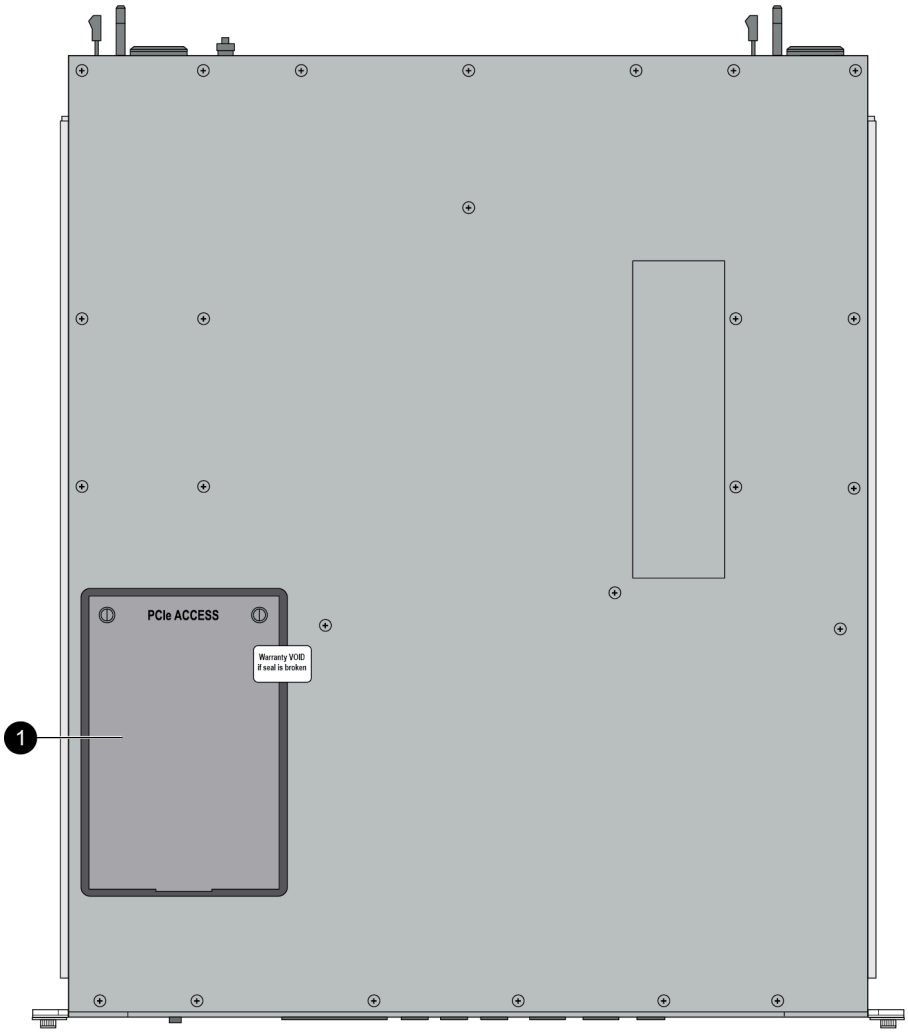
The following image shows the back panel of the PA-3510 and PA-3520 firewalls (PA-3520 pictured) and the table describes each back panel component.

The back panel of the firewall should remain accessible to ensure ease of replacing a power supply or fan assembly.



Item	Component	Description
1	Fans	Six dual-rotor fans that provide the appliance with cooling and ventilation. The fans are not field replaceable. *The firewall is designed to continue operating even if one fan rotor has failed.*
2	Power Supplies	Two power supplies that provide AC or DC power to the firewall. The power supplies are numbered 1 through 2 from left to right. Connect AC power or DC power to the firewall. *You cannot mix AC and DC power supplies. You must use two of the same type of power supply.*
3	Ground Stud	A stud used to ground the appliance to earth ground.

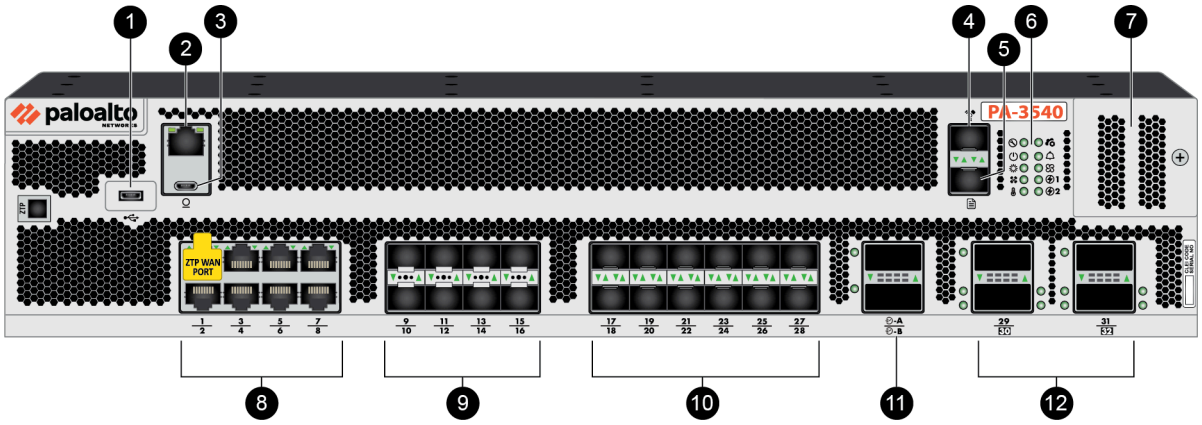
The following image shows the top panel of the PA-3500 Series firewalls and the table describes each top panel component.



Item	Component	Description
1	PCI Slot Access Hatch	Reserved for a future release.

PA-3530 and PA-3540

The following image shows the front panel of the PA-3530 and PA-3540 firewalls (PA-3540 pictured) and the table describes each front panel component.



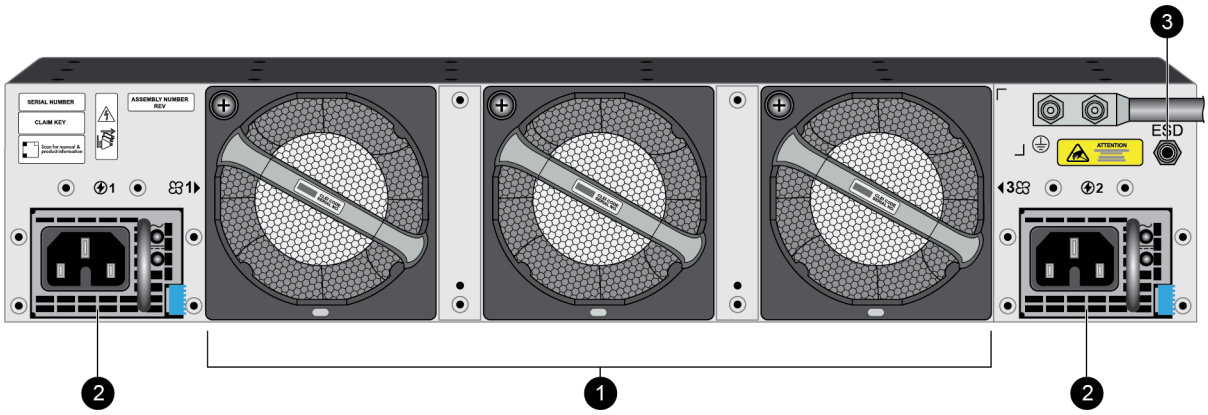
Item	Component	Description
1	USB-C Port	One USB-C port used for debugging and administration only. Use it to bootstrap the firewall or perform self-service enhanced factory reset (EFR). • Bootstrapping enables you to provision the firewall with a specific PAN-OS configuration and then license it and make it operational on your network. • EFR provides remediation of a compromised or potentially compromised firewall to initiate a complete cleanup of the device.
2	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: 115,200 • Data bits: 8 • Parity: None • Stop bits: 1 • Flow control: None
3	Console port (USB-C)	Use this port to connect a management computer to the firewall using a standard Type-C USB cable.

Item	Component	Description
		The console connection provides access to firewall boot messages, the Maintenance Recovery Tool (MRT), and the command line interface (CLI).
4	Management Port	One 1Gbps/10Gbps SFP+ Management port used to access the management web interface and perform administrative tasks. The firewall uses this port for management services, such as retrieving licenses and updating threat and application signatures.
5	Logging Port	One 1Gbps/10Gbps SFP+ logging port that can be used as a log interface. You must Configure Log Forwarding to forward logs from the port to one or more log collectors. *You can use any port on the firewall as a log interface.*
6	LED Indicators	Ten LEDs that indicate the status of various hardware components. For details on the LEDs, see PA-3500 Series Firewall LED Definitions.
7	SSD Cover	Secures the device's SSD, which contains PAN-OS system files, system logs, and network traffic logs.
8	Copper RJ-45 Ports	Eight 1Gbps/2.5Gbps/5Gbps/10Gbps RJ-45 ports. Port 1 is used for Zero Touch Provisioning (ZTP).
9	SFP28 Ports	Eight 25Gbps SFP28 ports.
10	SFP/SFP+ Ports	Twelve 1Gbps/10Gbps SFP/SFP+ ports.
11	HSCI Ports	Two HSCI ports that offer 100Gbps connectivity and are used to connect two firewalls in a high availability (HA) configuration as follows: • In an active/passive configuration, this port is for HA2 (data link). • In an active/active configuration, you can configure this port for HA2 and HA3. HA3 is used for packet forwarding for asymmetrically routed sessions that require Layer 7 inspection for App-ID and Content-ID.

Item	Component	Description
		The HSCI ports must be connected directly between the two firewalls in the HA configuration (without a switch or router between them). *The HSCI ports are not recommended for long-distance links (½ mile/1 km and above) regardless of the optical transceiver's rated capabilities. For long-distance links, use the data ports.* *Do not assign an IP address to the HSCI port. The port carries raw Layer 1 traffic that is not routable or switchable and does not support IP addressing. Assigning an IP address to the HSCI port causes the firewall to enter a permanent suspended state.* *For high-throughput deployments, do not use a 1Gbps copper interface for HA2. Use the HSCI port or a 10Gbps/40Gbps fiber interface to ensure sufficient bandwidth for HA data synchronization.* *When you configure path monitoring, do not use your HA peer's data interface IP address as the monitored destination. Using the peer's IP address causes the firewall to incorrectly detect a path failure and trigger an unnecessary failover.*
12	QSFP28 Ports	Four 40Gbps/100Gbps QSFP28 ports. Ports 30 and 32 support breakout into four 10Gbps/25Gbps interfaces each: port 30 breaks out into ports 33–36 and port 32 breaks out into ports 35–38. Ports 29 and 31 do not support breakout.

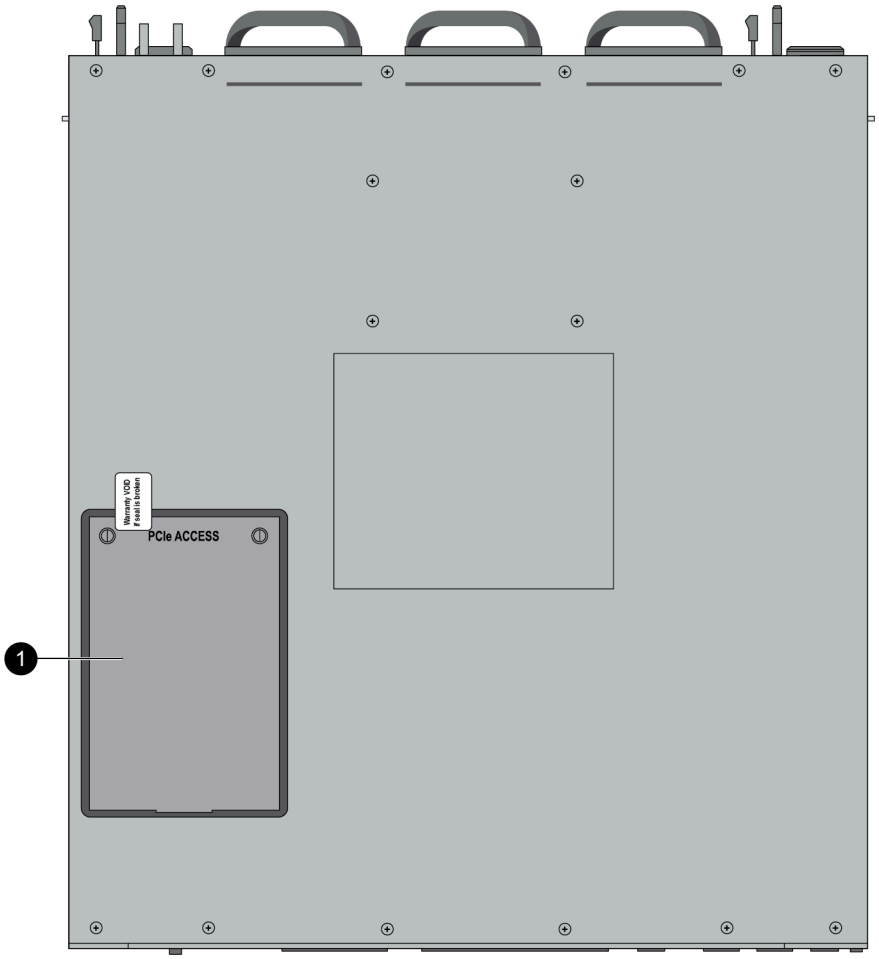
The following image shows the back panel of the PA-3530 and PA-3540 firewalls (PA-3540 pictured) and the table describes each back panel component.

The back panel of the firewall should remain accessible to ensure ease of replacing a power supply or fan assembly.



Item	Component	Description
1	Fan Assemblies	Three dual-rotor fan assemblies (for a total of six fans) that provide the appliance with cooling and ventilation. Each fan assembly can be individually replaced. The fan assemblies are numbered 1 through 3 from left to right. For information on replacing or installing a fan assembly, see Replace a PA-3500 Series Firewall Fan Assembly. *The firewall is designed to continue operating even if one fan rotor has failed.*
2	Power Supplies	Two power supplies that provide AC or DC power to the firewall. The power supplies are numbered 1 through 2 from left to right. Connect AC power or DC power to the firewall. *You cannot mix AC and DC power supplies. You must use two of the same type of power supply.*
3	Ground Stud	A stud used to ground the appliance to earth ground.

The following image shows the top panel of the PA-3500 Series firewalls and the table describes each top panel component.



Item	Component	Description
1	PCI Slot Access Hatch	Reserved for a future release.

PA-3500 Series Firewall Installation

The following topics cover how to install and set up the PA-3500 Series firewall hardware.

Install the PA-3500 Series Firewall in an Equipment Rack

The following procedure describes how to install the PA-3500 Series firewalls in a 19" four-post equipment rack.

Ensure that you have the correct rack kit equipment for your firewall.

- The PA-3510 and PA-3520 use the PAN-PA-1RU-RACK-KIT
- The PA-3530 and PA-3540 use the PAN-PA-2RU-RACK4

The back panel of the firewall should remain accessible to ensure ease of replacing a power supply or fan assembly.

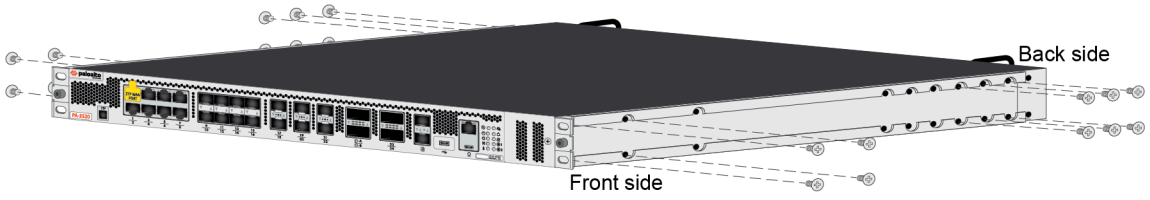
Read the following safety information before you proceed with the equipment rack installation:

- **Elevated ambient operating temperature** — If the PA-3500 Series firewall is installed in a closed or multi-unit rack assembly, the ambient operating temperature of the rack environment may be greater than the ambient room temperature. Verify that the ambient temperature of the rack assembly does not exceed the maximum rated ambient temperature requirements listed in the PA-3500 Series Firewall Environmental Specifications.
- **Reduced airflow** — Ensure that the airflow required for safe operation is not compromised by the rack installation.
- **Mechanical loading** — Ensure that the rack-mounted firewall does not cause hazardous conditions due to uneven mechanical loading.
- **Circuit overloading** — Ensure that the circuit that supplies power to the firewall is sufficiently rated to avoid circuit overloading or excess load on supply wiring. See PA-3500 Series Firewall Electrical Specifications.
- **Reliable earthing** — Maintain reliable earthing of rack-mounted equipment. Pay special attention to power connections other than direct connections to the branch circuit (such as use of power strips or extension cords) to ensure that the firewall does not exceed power ratings for connected hardware.
- PA-3510 and PA-3520
- PA-3530 and PA-3540

PA-3510 and PA-3520

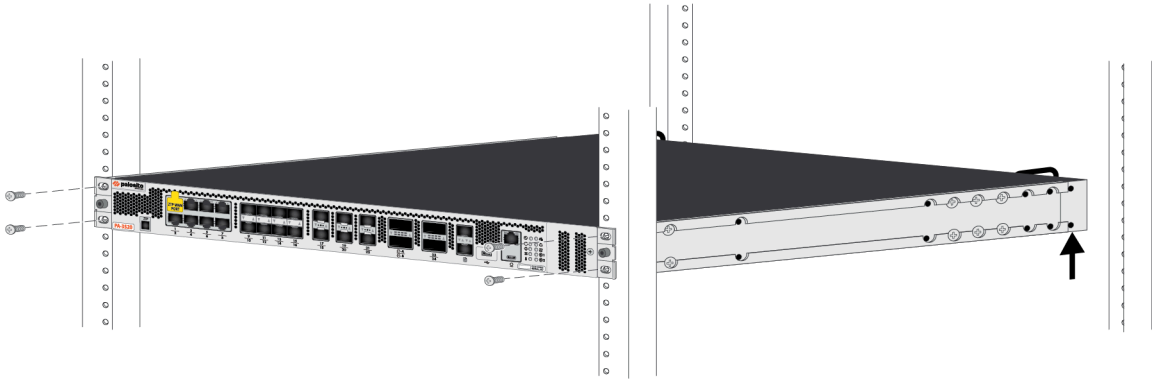
STEP 1 | Attach one fixed rack mount bracket to each side of the firewall.

- Use four #6-32 × 3/16" screws for the front screw holes in each bracket (8 total).
- Use six #6-32 × 3/16" screws for the back screw holes in each bracket (12 total).

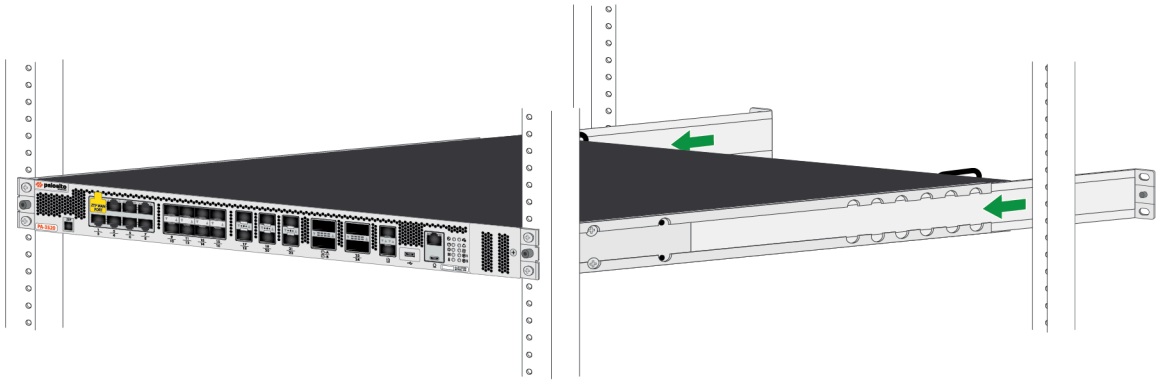


STEP 2 | With help from another person, hold the firewall in the rack and secure the fixed rack mount brackets to the front rack-posts using the appropriate screws for your rack.

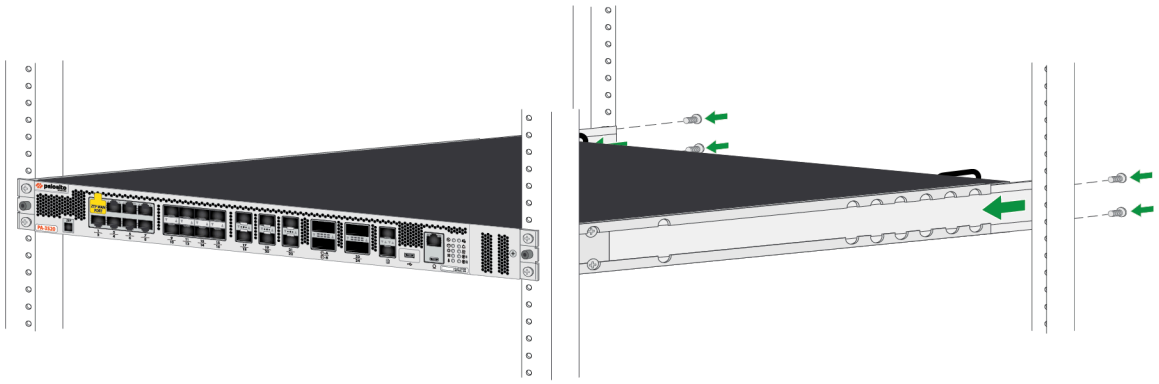
Use two screws for each bracket (4 total).



STEP 3 | Slide one adjustable rack mount bracket into each of the two previously installed fixed rack mount brackets.



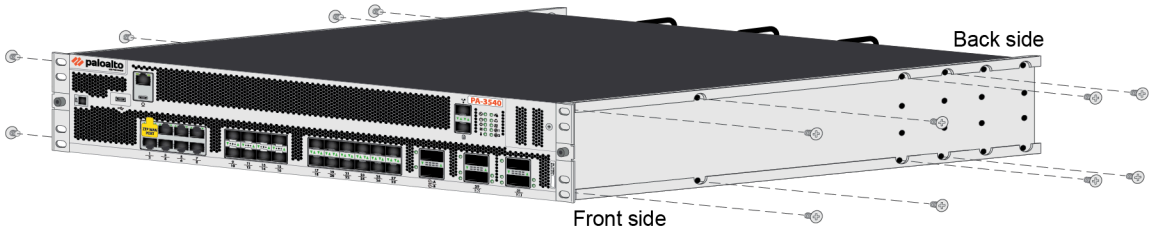
STEP 4 | Secure the two adjustable rack mount brackets to the back rack-posts using two screws for each bracket.



PA-3530 and PA-3540

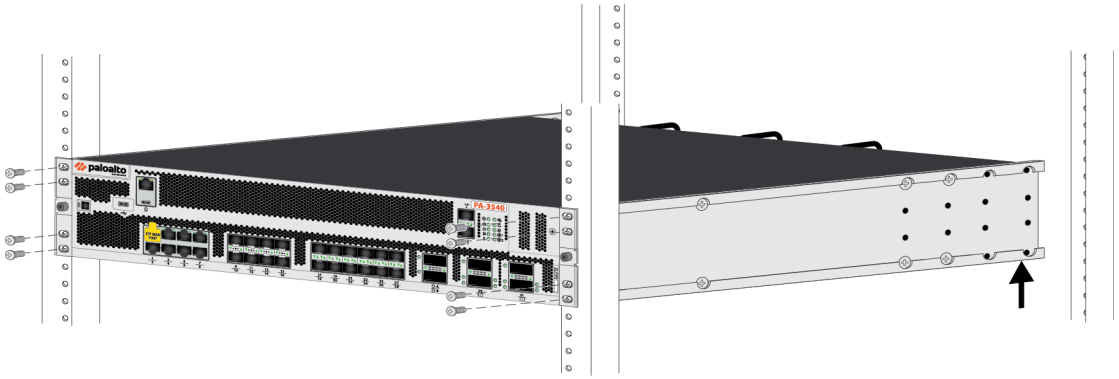
STEP 1 | Attach one fixed rack mount bracket to each side of the firewall.

- Use four #8-32 x 5/16" screws for the front screw holes in each bracket (8 total).
- Use four #6-32 x 5/16" screws for the back screw holes in each bracket (8 total).

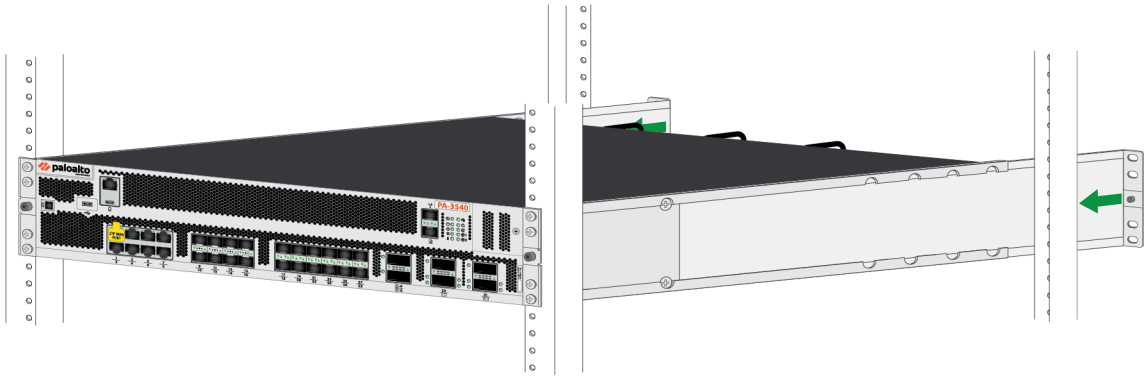


STEP 2 | With help from another person, hold the firewall in the rack and secure the fixed rack mount brackets to the front rack-posts using the appropriate screws for your rack.

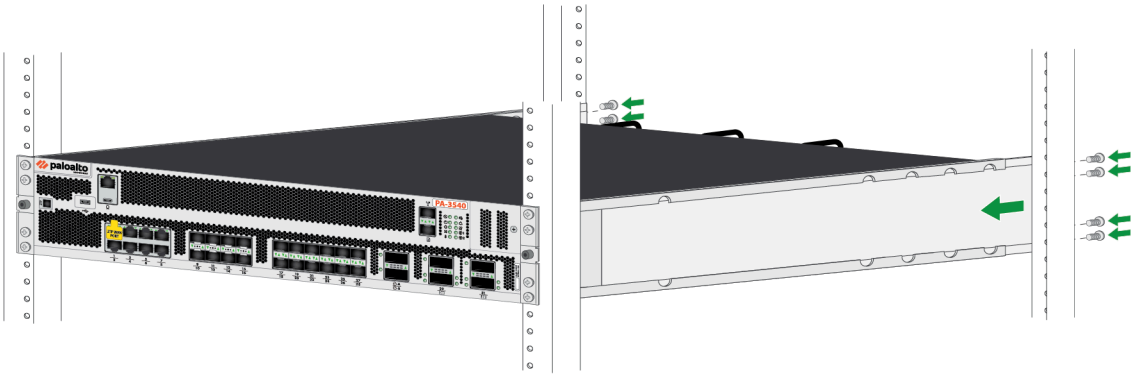
Use four screws for each bracket (8 total).



STEP 3 | Slide one adjustable rack mount bracket into each of the two previously installed fixed rack mount brackets.



STEP 4 | Secure the two adjustable rack mount brackets to the back rack-posts using two screws for each bracket.



Connect AC Power to the PA-3500 Series Firewall

The following procedure describes how to connect AC power to a PA-3500 Series firewall with AC power supplies.

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

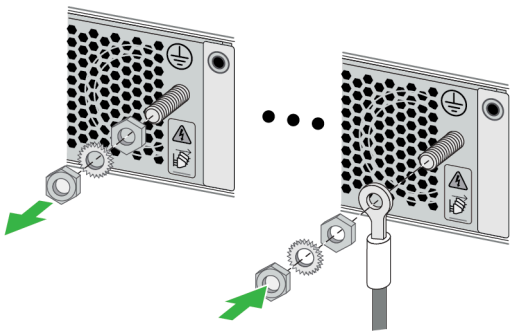
To avoid injury to yourself or damage to your Palo Alto Networks® hardware or the data that resides on the hardware, read the Safety Warnings.

STEP 1 | Ensure that your power source(s) are powered off.

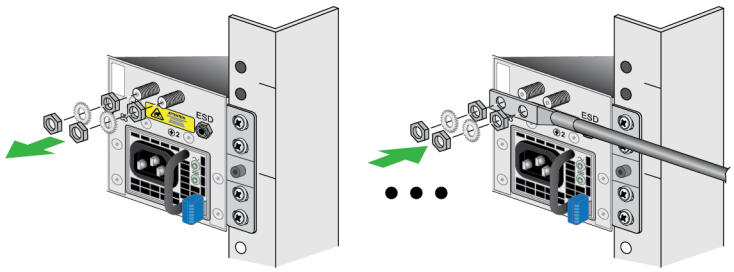
STEP 2 | Remove the nut and star washer from the ground stud(s) on the back of the firewall.

STEP 3 | Crimp a 14AWG ground cable to a ring lug (cable and lug not included) and then attach the ring lug to the ground stud on the firewall. Replace the star washers and nuts, then connect the other end of the cable to earth ground.

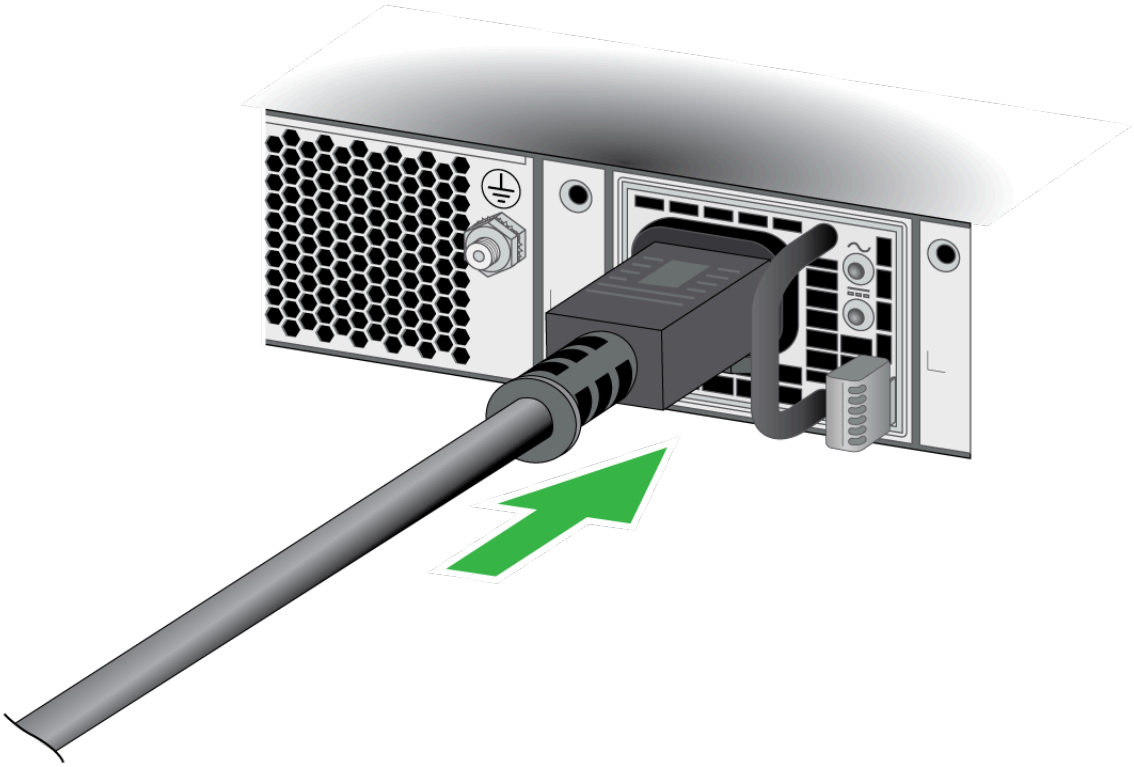
PA-3510 and PA-3520



PA-3530 and PA-3540



STEP 4 | Connect the AC power cord to the power supplies



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 Firewall.

STEP 5 | Connect the other end of the power cords to an AC power source. After the power supply is connected, the power supply powers on, the input and output LEDs on the power supply turn green, and the power LED on the front of the firewall turns green.

Connect the second power cord through a different circuit breaker to provide power redundancy and to allow for electrical circuit maintenance. The blank in the second power supply slot must be removed prior to installing the second power supply.

Connect DC Power to the PA-3500 Series Firewall

The following procedure describes how to connect DC power to a PA-3500 Series firewall with DC power supplies.

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

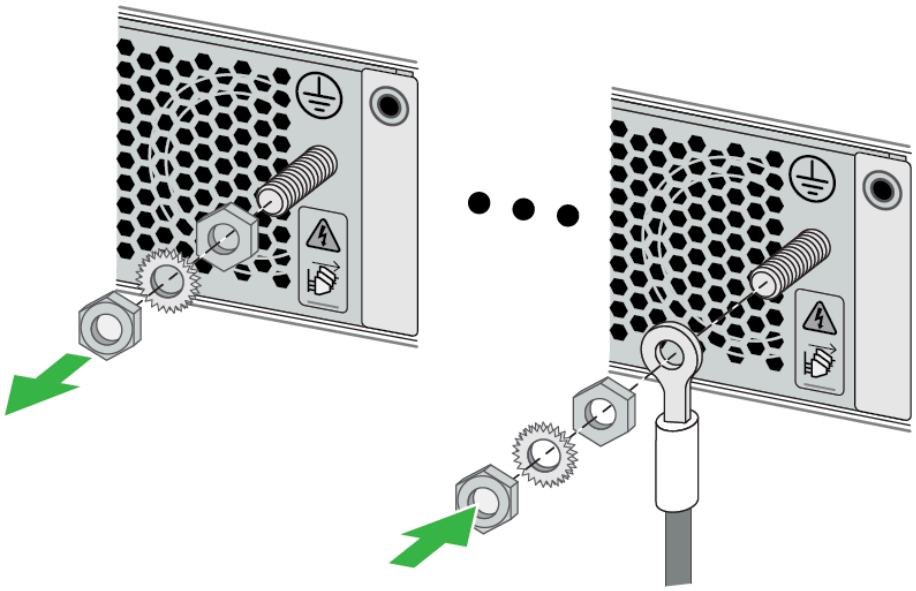
To avoid injury to yourself or damage to your Palo Alto Networks® hardware or the data that resides on the hardware, read the Safety Warnings.

STEP 1 | Ensure that your power source(s) are powered off.

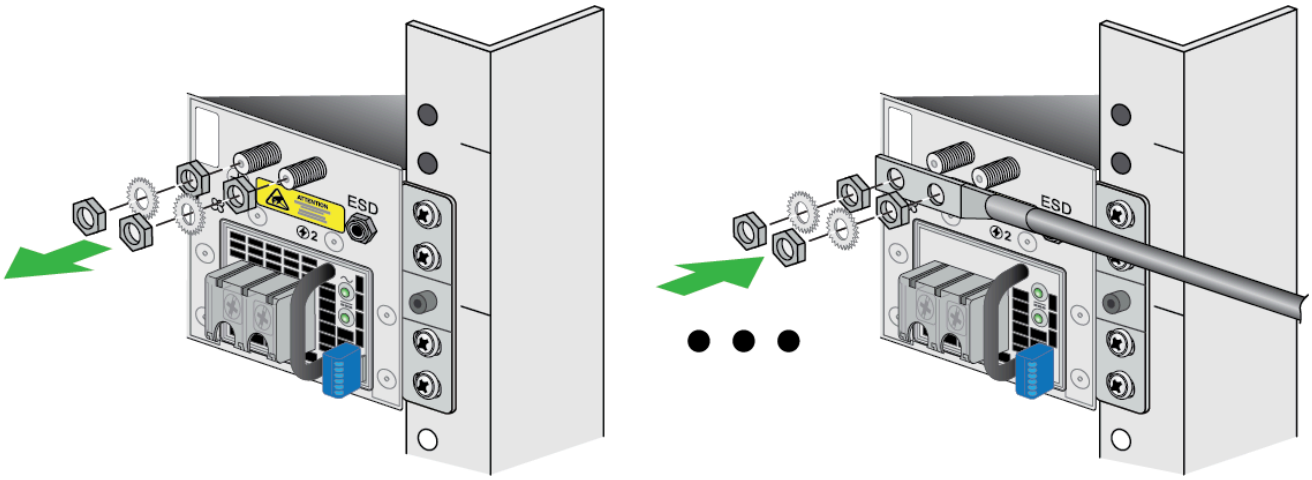
STEP 2 | Remove the nut and star washer from the ground stud(s) on the back of the firewall.

STEP 3 | Crimp a 14AWG ground cable to a ring lug (cable and lug not included) and then attach the ring lug to the ground stud on the firewall. Replace the star washers and nuts, then connect the other end of the cable to earth ground.

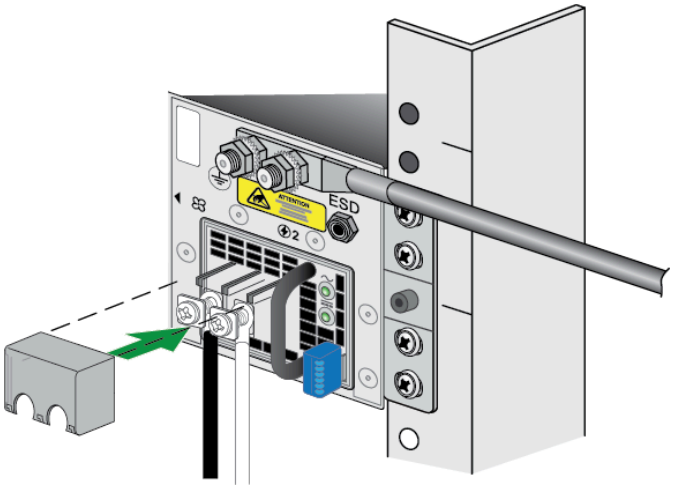
PA-3510 and PA-3520



PA-3530 and PA-3540



STEP 4 | Remove the connector cover from the power supply. Connect the positive and negative cable ends to the respective polarity slots in the power supply, then re-install the connector cover. Repeat this for each power supply.



STEP 5 | Connect the opposite end of the positive and negative cables to a 60A circuit breaker, then secure the power cords to the power inlets using the velcro straps. Repeat this for the second power supply, ensuring that each power supply is connected to its own 60A power circuit breaker. This ensures power redundancy and allows for planned electrical circuit maintenance.

STEP 6 | After each DC cable is securely connected, turn on the power source and the appliance will power on.

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 Firewall.

Set Up a Connection to the Firewall

On first startup, the PA-3500 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-3500 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 the appropriate 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 SFP transceiver and cable from the MGT port on the firewall to the port on 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.

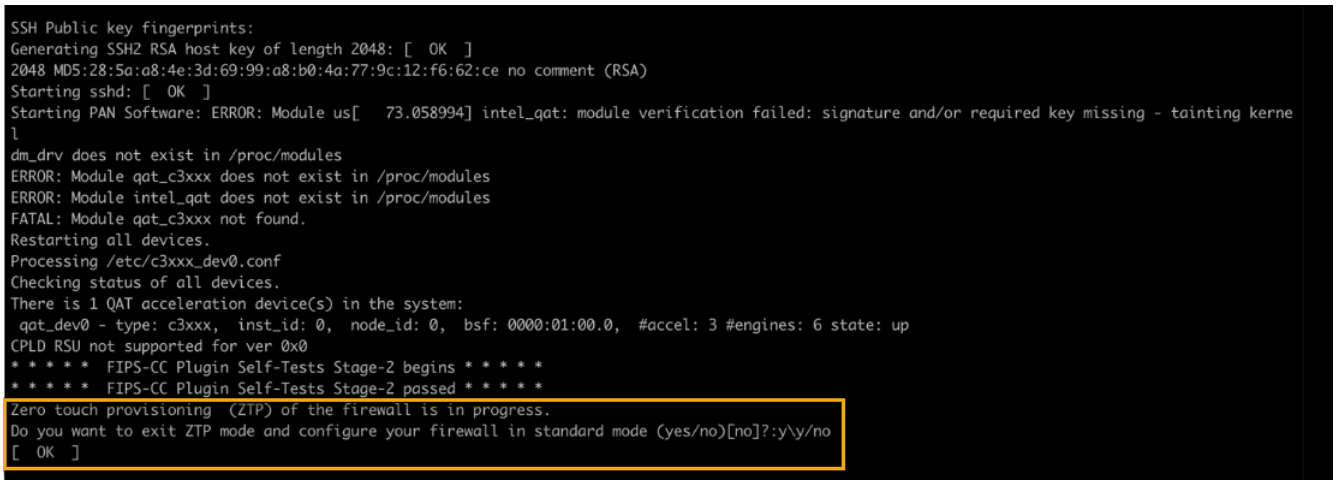
STEP 3 | (Standard mode only) If you intend to boot the firewall in standard mode, you will need access to the firewall CLI to respond to a prompt during bootup. Connect a console cable from the firewall to your computer. Once the firewall is powered on, use a terminal emulator such as PuTTY to access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

STEP 4 | Power on the firewall after installing AC or DC power supplies.

- (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.

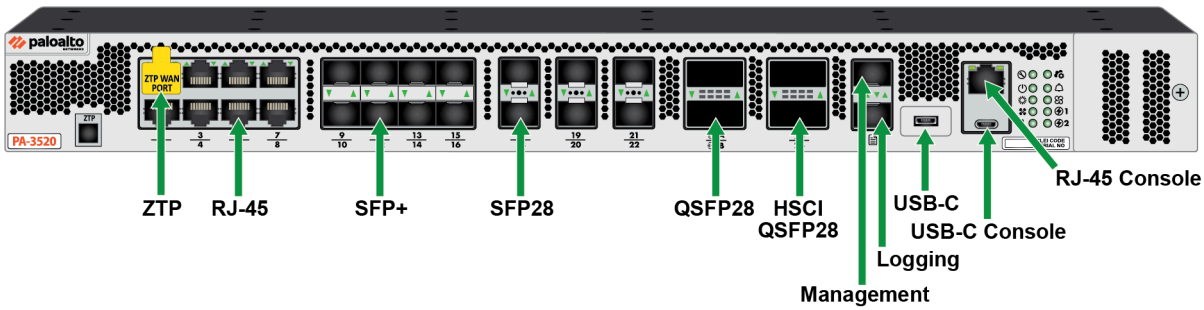
STEP 5 | Set up the firewall manually if using standard mode. If using ZTP mode, the device group and template configuration defined on the Panorama management server are automatically pushed to the firewall by the ZTP service.

- (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.

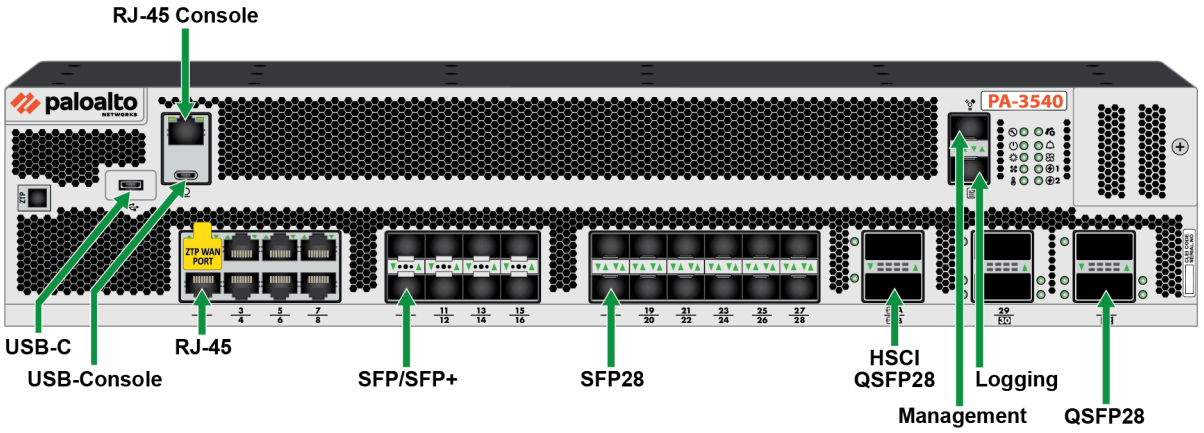
Connect Cables to the PA-3500 Series Firewall

After you connect AC or DC power to the firewall, connect your management computer to the management port on the firewall so you can begin the initial configuration. You can optionally connect your management computer to the console port, which provides a serial connection to the firewall and enables you to view the bootup messages and manage the firewall using the command line interface (CLI).

The following image shows the PA-3510 and PA-3520 cable connections.



The next image shows the PA-3530 and PA-3540 firewall cable connections.

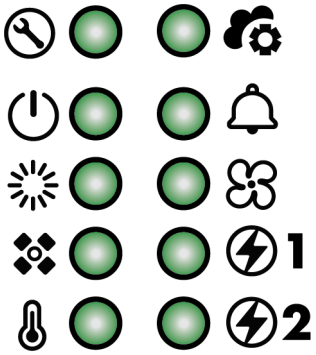


PA-3500 Series Firewall Maintenance

The following topics describes how to interpret LED information and replace field-serviceable components on a PA-3500 Series firewall.

PA-3500 Series Firewall LED Definitions

The following table describes how to interpret the status LEDs on a PA-3500 Series firewall.



LED	Description
Front Panel LEDs	
	**Service** • **Blue**—The firewall is instructed by the CLI or Web Interface to enable this LED. • **Off**—The LED has not been enabled.
	**Power** • **Green**—The firewall is powered on. • **Yellow**—The firewall has encountered a hardware failure. • **Off**—The firewall is not powered on.
	**Status** • **Green**—The firewall configuration is loaded. • **Yellow**—The firewall is booting.
	**High Availability** • **Green**—The firewall is the active HA peer. • **Yellow**—The firewall is the passive HA peer. • **Off**—The firewall is not configured for HA.
	**Temperature** • **Green**—The firewall temperature is normal. • **Yellow**—The firewall temperature is outside tolerance levels.

LED	Description
	See the PA-3500 Series Firewall Environmental Specifications for the operating temperature range.
	**Controller** • **Green**—The firewall is connected to Panorama. • **Blue**—The firewall is connected to SCM or a SDWAN controller. • **Yellow (Blinking)**—The firewall is trying to connect to a controller. • **Yellow (Solid)**—The firewall encountered a connectivity error. • **Off**—The firewall is not attempting to connect to a controller.
	**Alarm** • **Red**—A hardware failure, such as a power supply failure, a firewall failure that caused an HA failover, a drive failure, or the hardware overheated and exceeded the high temperature threshold. • **Off**—The firewall is operating normally.
	**Fans** • **Green**—All fans are operating normally. • **Yellow**—A fan has failed.
	**Power Supplies** • **Green**—The power supplies are functioning normally. • **Red**—One of the power supplies is not working. • **Off**—Power supplies are not installed  *When facing the back of the firewall, **1** is the left power supply and **2** is the right power supply.*
Port LEDs	
RJ-45	These ports have one green LED each. • **Solid Green**—The firewall network link is up. • **Blinking Green**—The firewall is processing network activity.
SFP, SFP+, SFP28, QSFP+, and QSFP28	The color of each LED differs based on the port speed. Refer to the descriptions on the PA-3500 Series Firewall Components for the supported speeds on each port. 1G—Yellow

LED	Description
	10G—Green 25G—Green & Blue 40G—Yellow 100G—Blue • **Solid Color**—The firewall network link is up. • **Blinking Color**—The firewall is processing network activity.

Replace a PA-3500 Series Firewall Power Supply

The following instructions describe how to replace a power supply in a PA-3500 Series firewall.

STEP 1 | Put the provided ESD wrist strap on your wrist ensuring that the metal contact is touching your skin. Then attach (snap) one end of the ground cable to the wrist strap and remove the alligator clip from the banana clip on the other end of the ESD grounding cable. Plug the banana clip end into one of the ESD ports located on the back of the appliance before handling ESD sensitive hardware. For details on the ESD port location, see PA-3500 Series Firewall Components.

STEP 2 | Locate the failed power supply by viewing the system logs or by viewing the LED on the front of the power supply. A red LED indicates a failed power supply.

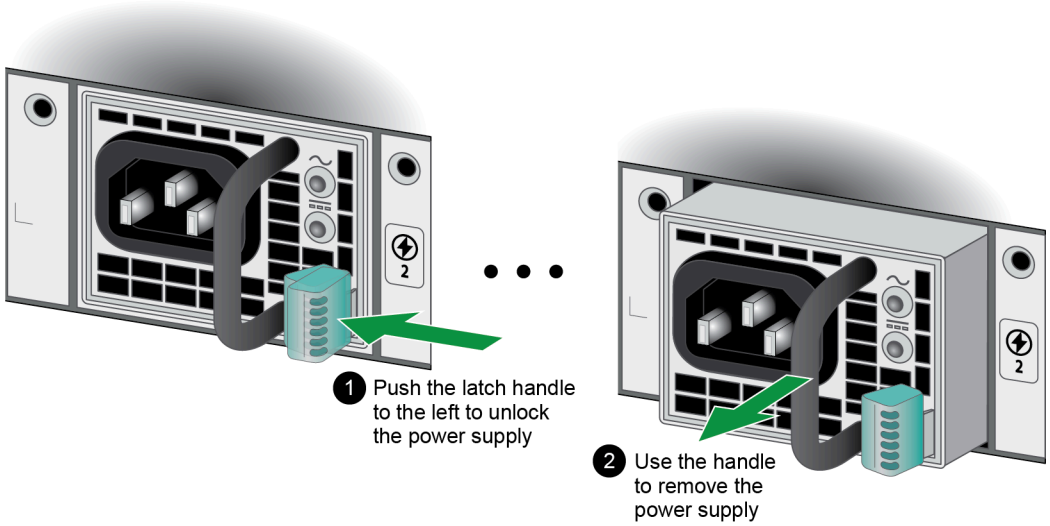
Alternatively, you can use the CLI command ***`show system environmentals`*** *to identify the failed power supply.*

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

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

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

STEP 4 | Facing the rear side of the appliance, push the power supply latch handle to the left to disengage the latch from the appliance. With the latch still pushed to the left, pull out the power supply.



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

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

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

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

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

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

Replace a PA-3500 Series Firewall Fan Assembly

The PA-3530 and PA-3540 firewalls have three dual-rotor fan assemblies on their back panel, making six individual fans. When all six fans are functioning as expected, the fan LED glows green. If any fan fails, the fan LED glows yellow.

If an individual fan fails, then the firewall software automatically determines how to manage the system temperature, whether through adjusting the speeds of the other fans or shutting down the firewall.

You can hot swap a fan assembly, but you must complete Steps 5 and 6 of the following procedure within 120 seconds to avoid downtime.

STEP 1 | Put the provided ESD wrist strap on your wrist ensuring that the metal contact is touching your skin. Then attach (snap) one end of the ground cable to the wrist strap and remove the alligator clip from the banana clip on the other end of the ESD grounding cable. Plug the banana clip end into the ESD port located on the rear of the appliance before handling ESD sensitive hardware. For details on the ESD port location, see PA-3530 and PA-3540.

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

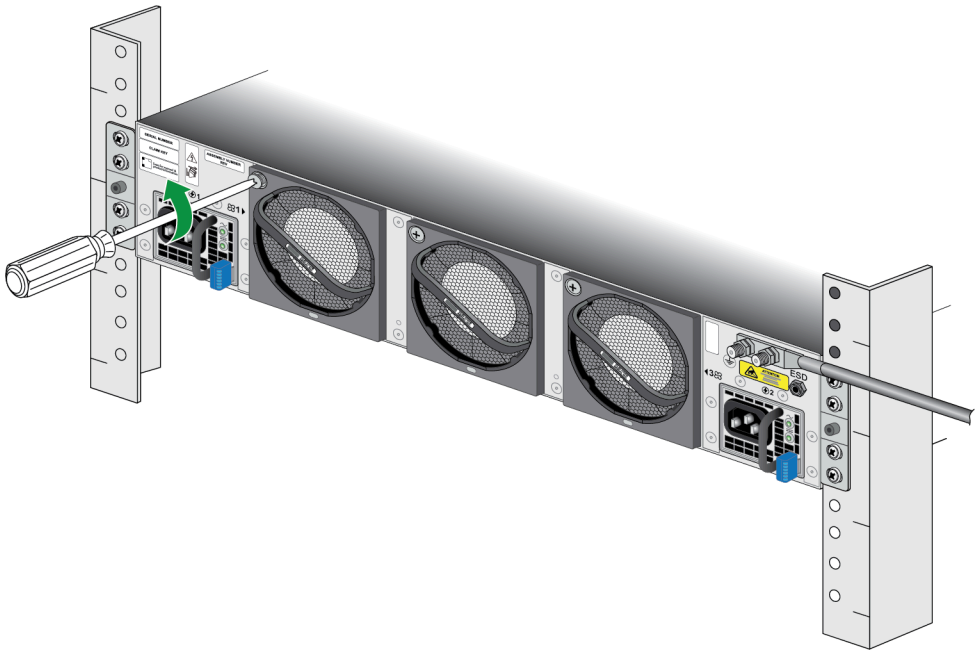
STEP 2 | Remove the replacement fan assembly from the packaging and have it ready.

STEP 3 | Identify the fan assembly with the failed fan(s) by using the following CLI command:

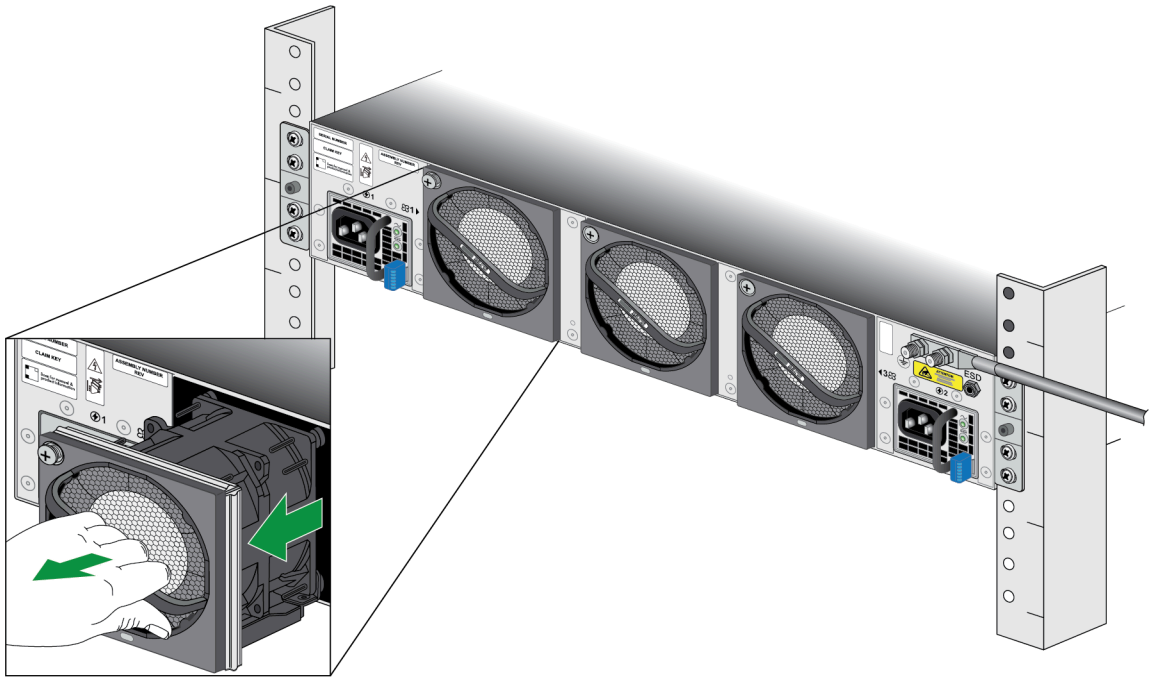
```
admin@PA-3540> show system environmentals fan-tray
```

The fan assemblies are numbered 1 through 3 from left to right.

STEP 4 | Loosen the captive screw holding the fan assembly in place.



STEP 5 | While gripping the fan assembly handle, gently pull the fan assembly out of its slot.



STEP 6 | Install the replacement fan by sliding it into the vacant fan slot. Tighten the captive screw by turning it clockwise until it is secure. Ensure that the fan assembly is secure by gently pulling on the handle.

STEP 7 | Verify that the new fan assembly is operational by noting the status of the fan LED on the front panel. The fan LED shows green if all fans are working as expected. You can also view the status of the fan assemblies by entering the following command:

```
admin@PA-3540> show system environmentals fan-tray
```

To view the status of each fan in an assembly, run the following command:

```
admin@PA-3540> show system environmentals fans
```


Replace a PA-3500 Series Firewall System Drive

The PA-3500 Series firewalls uses a single solid-state drive (SSD) to store the PAN-OS system files, system logs, and network traffic logs. The drive is embedded into a module that slides in and out of the front panel of the firewall.

The replacement drives ship with a factory default PAN-OS image with the default configuration. After you install the new drive, you will need to obtain a backup configuration that you saved from the failed firewall to restore your configuration.

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.

The following procedure describes how to replace a failed system drive.

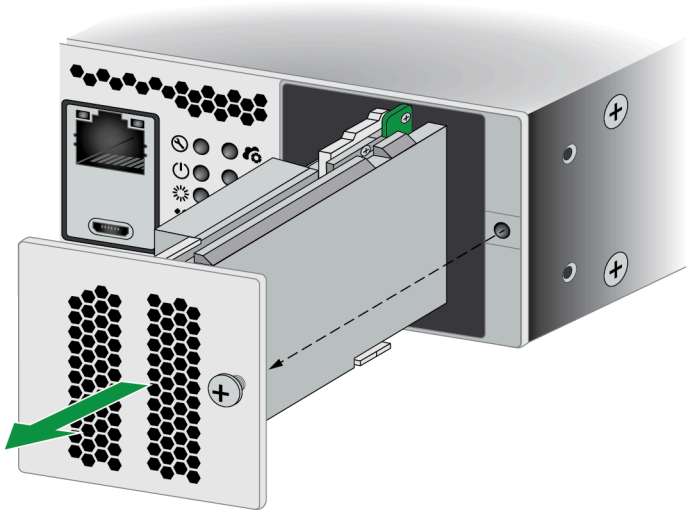
STEP 1 | Confirm that a drive has failed by issuing the following command:

```
admin@PA-3540> show system disk details
```

STEP 2 | Disconnect power from the firewall, then remove the power cords.

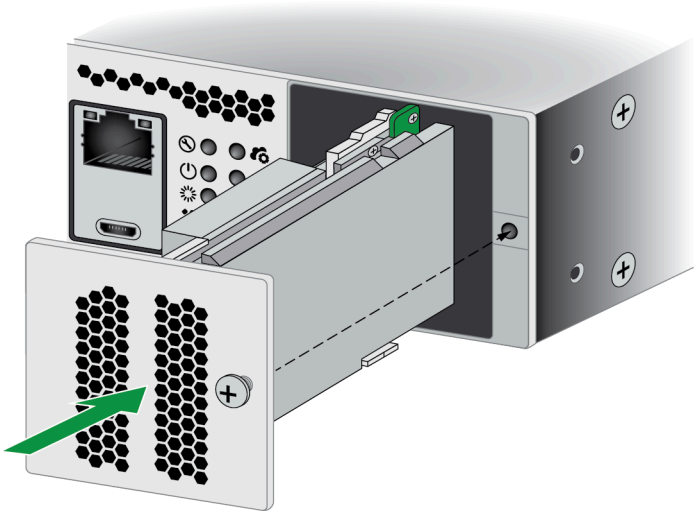
STEP 3 | Unscrew the captive screw on the system drive cover on the front side of the firewall. See PA-3500 Series Firewall Components for help locating the system drive cover.

STEP 4 | Pull the SSD module out of the firewall.



STEP 5 | Remove the replacement drive from the packaging, determine the drive model, and place it on an antistatic surface.

STEP 6 | Slide the replacement SSD module onto the rails and gently push it into the firewall. Re-fasten the captive screw until the module is secure in the appliance.



STEP 7 | After powering on the firewall, verify that the system drives are functioning properly by running the following command:

```
admin@PA-3540> show system disk details
```


PA-3500 Series Firewall Specifications

The following topics describe the PA-3500 Series firewall hardware specifications. For feature, capacity, and performance information, refer to the PA-3500 Series datasheet.

PA-3500 Series Firewall Physical Specifications

The following table describes PA-3500 Series firewall physical specifications.

Specification	Value
Rack units and dimensions	**PA-3510 and PA-3520** • Rack units—1RU • Dimensions—Height: 1.7" (4.32cm); Width: 17.3" (43.94cm); Depth: 20.85" (52.96cm) **PA-3530 and PA-3540** • Rack units—2RU • Dimensions—Height: 3.4" (8.64cm); Width: 17.3" (43.94cm); Depth: 18.7" (47.5cm)
Weight	**PA-3510 and PA-3520**—24.2 lbs (11 kg) **PA-3530 and PA-3540**—36 lbs (16.3 kg)

PA-3500 Series Firewall Electrical Specifications

The following table describes the PA-3500 Series firewall electrical specifications. To learn about the power cords compatible with the PA-3500 Series firewalls, see PA-3500 Series Firewall Power Cord Types.

Specification	Value
Power Supplies	**All PA-3500 Series firewalls** • PAN-PWR-1200W-AC-A • PAN-PWR-1200W-DC-A The PA-3500 Series firewalls support up to two load sharing AC or DC power supplies.
Input voltage	**All PA-3500 Series firewalls** • AC Power Supplies—100 to 120VAC (50-60Hz); 200 to 240VAC (50-60Hz) • DC Power Supplies—-48 to -60 VDC

Power Consumption	**PA-3510 and PA-3520**
	• Maximum—770W
	• Average
	  • 209 VAC input — 402 W
	  • 120 VAC input — 400 W
	  • 48 VDC input — 400 W
	PA-3530 and PA-3540
	• Maximum—1066 W
	• Average
	  • 208 VAC input — 643 W
	  • 120 VAC input — 708 W
	  • 48 VDC input — 854 W

Maximum Current Consumption	**PA-3510 and PA-3520** • AC power supplies—9.33A@120VAC, 4.67@240VAC • DC power supplies—30A@-60 VDC **PA-3530 and PA-3540** • AC power supplies—12A@120VAC, 7A@240VAC

Specification	Value
	• DC power supplies—30A@-60 VDC

PA-3500 Series Firewall Power Cord Types

The following table lists the power cords supported by the PA-3500 Series firewalls.

SKU Number	Description
PAN-PWR-CORD-C15-US	AC power cord with IEC-60320 C15 and NEMA 5-15P cord ends, 3m
PAN-PWR-CORD-C15-EU	AC power cord with IEC-60320 C15 and CEE 7/7 SCHUKO cord ends, 3m
PAN-PWR-CORD-C15-UK	AC power cord with IEC-60320 C15 and BS 1363 UK13 cord ends, 3m
PAN-PWR-CORD-C15-JP	AC power cord with IEC-60320 C15 and JISC8303 cord ends, 3m
PAN-PWR-CORD-C15-TW	AC power cord with IEC-60320 C15 and CNS 10917-3 cord ends, 3m
PAN-PWR-CORD-C15-AU	AC power cord with IEC-60320 C15 and AS/NZS 4417 cord ends, 3m
PAN-PWR-CORD-C15-SUI	AC power cord with IEC-60320 C15 and SEV 1011 cord ends, 3m
PAN-PWR-CORD-C15-CN	AC power cord with IEC-60320 C15 and GB 2099.1 cord ends, 3m
PAN-PWR-CORD-C15-BR	AC power cord with IEC-60320 C15 and NBR 14136 cord ends, 3m
PAN-PWR-CORD-C15-IN	AC power cord with IEC-60320 C15 and Type M cord ends, 3m

PA-3500 Series Firewall Environmental Specifications

The following table describes PA-3500 Series firewall environmental specifications.

Specification	Value
Operating temperature range	0° to 40°C (32° to 104°F)
Storage temperature range	-20° to 70°C (-4°F to 158°F)
Humidity	10% to 90% non-condensing
Appliance airflow	Front to back
Electromagnetic Interference (EMI)	FCC Class A, CE Class A, VCCI Class A
Acoustic noise	**PA-3530 and PA-3540**—72.9 dBA
Maximum operating altitude	10,000ft (3,048m)

