

PA-5500 Series Hardware Reference

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

© 2024-2025 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

August 19, 2025

Table of Contents

Before You Begin.....	5
Safety and Compliance.....	6
Safety Warnings.....	6
Compliance Statements.....	8
Tamper Proof Statement.....	8
Third-Party Component Support.....	9
Parts List and Required Tools.....	10
PA-5500 Series Firewall Overview.....	13
PA-5500 Series Firewall Front Panel.....	14
PA-5500 Series Firewall Back Panel.....	19
PA-5500 Series Firewall Top Panel.....	21
PA-5500 Series Firewall Installation.....	23
Install the PA-5500 Series Firewall in an Equipment Rack.....	24
Connect Power to the PA-5500 Series Firewall.....	27
Set Up a Connection to the Firewall.....	31
Connect Cables to the PA-5500 Series Firewall.....	33
PA-5500 Series Firewall Maintenance.....	35
PA-5500 Series Firewall LED Definitions.....	36
Replace a PA-5500 Series Firewall Power Supply.....	39
Replace a PA-5500 Series Firewall Fan Assembly.....	41
Replace a PA-5500 Series Firewall System Drive.....	44
PA-5500 Series Firewall Specifications.....	47
PA-5500 Series Firewall Physical Specifications.....	48
PA-5500 Series Firewall Electrical Specifications.....	49
PA-5500 Series Firewall Power Cord Types.....	50
PA-5500 Series Firewall Environmental Specifications.....	51

Before You Begin

Read the following topics before you install or service the PA-5500 Series firewall.

- [Safety and Compliance](#)
- [Parts List and Required Tools](#)

Safety and Compliance

Read the Safety Warnings prior to installing the PA-5500 Series firewall hardware. This section also lists compliance and regulatory statements that apply to the firewall.

- [Safety Warnings](#)
- [Compliance Statements](#)
- [Tamper Proof Statement](#)
- [Third-Party Component Support](#)

Safety Warnings

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



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

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


French Translation: Lorsque vous installez ou que vous intervenez sur un composant matériel de pare-feu ou de dispositif Palo Alto Networks qui présente des circuits exposés, veuillez 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.

- | | |
|---|--|
|  | <p>Caution: Shock hazard</p> <p>Disconnect all power cords (AC or DC) from the power inputs to fully de-energize the hardware.</p> <p>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.</p> |
|---|--|
- 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



For centralized DC (battery bank) power connection, the product is intended to be installed only in Restricted Access Areas (such as dedicated equipment rooms or equipment closets) in accordance with Sections 110.26(F) and 110.27 of the U.S. National Electrical Code (NEC), ANSI/NFPA 70 (2023), and Section 12-200 in the Canadian Electrical Code C22.2 No. 1 (2023).

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-5500 Series firewall.

Table 1: Parts List — PA-5500 AC

Quantity	Item	SKU
1	PA-5500 Series Firewall	
1	Rack mount kit	PAN-PA-3RU-RACK-A
4	AC power supplies	PAN-PA-5500-PWR-2700-AC
4	AC power cables	PAN-PWR-C19-US-120V
5	Fan assemblies	PAN-PA-FAN-2RU-A
1	CAT6 cable	
2	SFP cables	
1	USB cable	
1	3.84TB RAID1 SSD pair	PAN-PA-5500-SSD-3.84TB-PAIR

Table 2: Parts List — PA-5500 DC

Quantity	Item	SKU
1	PA-5500 Series Firewall	
1	Rack mount kit	PAN-PA-3RU-RACK-A
4	DC power supplies	PAN-PA-5500-PWR-2000-DC
4	DC power cables	PAN-PWR-DC-CBL-C
5	Fan assemblies	PAN-PA-FAN-2RU-A
1	CAT6 cable	
2	SFP cables	
1	USB cable	
1	3.84TB RAID1 SSD pair	PAN-PA-5500-SSD-3.84TB-PAIR

The following tools are either required or recommended when installing the PA-5500 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-5500 Series Firewall Overview

The PA-5500 Series Next-Generation firewalls are high performance appliances designed for large enterprise environments, data centers, and internet gateway deployments. The following models make up the PA-5500 Series:

- PA-5540
- PA-5550
- PA-5560
- PA-5570
- PA-5580

The PA-5500 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 3.84TB RAID1 SSD pair. Dedicated computing and hardware resources ensure predictable performance in networking, security, signature matching, and management functions.

First Supported PAN-OS® Software Release: PAN-OS 12.1.2

The following topics describe the hardware components of the PA-5500 Series firewalls:

- [PA-5500 Series Firewall Front Panel](#)
- [PA-5500 Series Firewall Back Panel](#)
- [PA-5500 Series Firewall Top Panel](#)

PA-5500 Series Firewall Front Panel

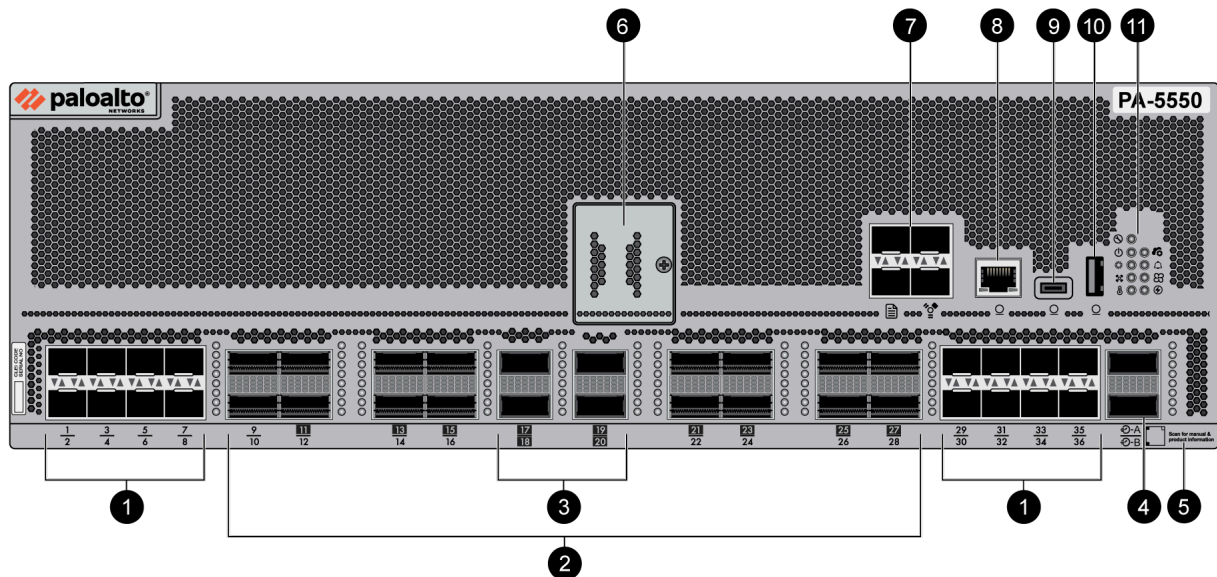
View the front panel components of your PA-5500 Series firewalls.

- [PA-5540 and PA-5550](#)
- [PA-5560, PA-5570, and PA-5580](#)




To review the specifications of supported Palo Alto Networks® interfaces and transceivers, refer to the [datasheet](#).

The following image shows the front panel of the PA-5540 and PA-5550 firewalls (PA-5550 pictured) and the table describes each front panel component.

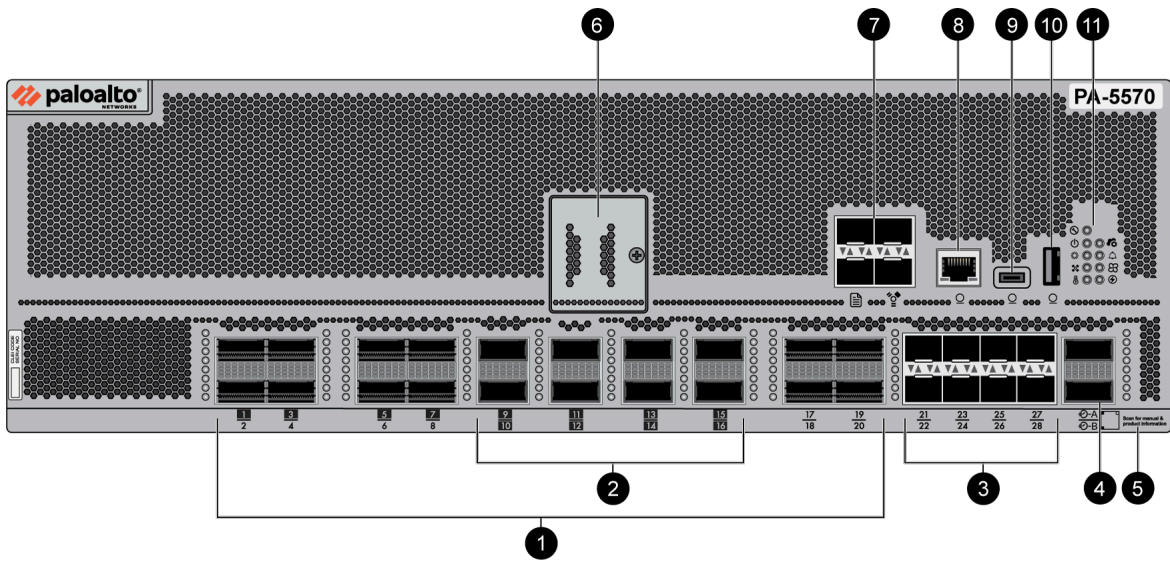


Item	Component	Description
1	SFP28 Ports	Sixteen 10Gbps/25Gbps SFP28 ports.
2	QSFP28 Ports	Sixteen 40Gbps/100Gbps QSFP28 ports. The port numbers with a black background indicate that the port can be broken out into four interfaces.
3	QSFP-DD Ports	Four 40/100Gbps/400Gbps QSFP-DD ports. The port numbers with a black background indicate that the port can be broken out into four interfaces.
4	HSCI Ports	Each HSCI port offers 100Gbps or 400Gbps connectivity and is used to create an Inter Firewall Link (IFL). An IFL is required to establish NGFW clustering , which carries configuration and state messages and data plane traffic.


Item	Component	Description
5	QR Code	A QR code that can be scanned with a mobile device to access product documentation.
6	Drive Cover	Secures the device's drive pair, which contains PAN-OS system files, system logs, and network traffic logs.
7	Management and Logging Ports	<p>Management Ports</p> <p>Two 1Gbps/10Gbps SFP+ Management ports 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.</p> <p>Logging Ports</p> <p>Two SFP+ logging ports that offer 10Gbps connectivity each and are used as log interfaces. You must Configure Log Forwarding to forward logs from the log ports to one or more log collectors. If the log interface is not configured, the management interface is used to forward logs instead.</p>
8	Console Port (RJ-45)	<p>Use this port to connect a management computer to the firewall using a 9-pin serial-to-RJ-45 cable and terminal emulation software.</p> <p>The console connection provides access to firewall boot messages, the Maintenance Recovery Tool (MRT), and the command line interface (CLI).</p> <p> <i>If your management computer does not have a serial port, use a USB-to-serial converter.</i></p> <p>Use the following settings to configure your terminal emulation software to connect to the console port:</p> <ul style="list-style-type: none"> • Data rate: 115,200 • Data bits: 8 • Parity: None • Stop bits: 1 • Flow control: None
9	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).
10	USB Port	A USB port that accepts a USB flash drive with a bootstrap bundle (PAN-OS configuration). Bootstrapping speeds up the process of configuring and licensing the firewall to make it operational on the network with or without internet access.
11	LED Indicators	Nine LEDs that indicate the status of various hardware components. For details on the LEDs, see PA-5500 Series Firewall LED Definitions .

The following image shows the front panel of the PA-5560, PA-5570, and PA-5580 firewalls (PA-5570 pictured) and the table describes each front panel component.




Item	Component	Description
1	QSFP28 Ports	Twelve 40Gbps/100Gbps QSFP28 ports. The port numbers with a black background indicate that the port can be broken out into four interfaces.
2	QSFP-DD Ports	Eight 40/100/400Gbps QSFP-DD ports. The port numbers with a black background indicate that the port can be broken out into four interfaces.
3	SFP28 Ports	Eight 10Gbps/25Gbps SFP28 ports.

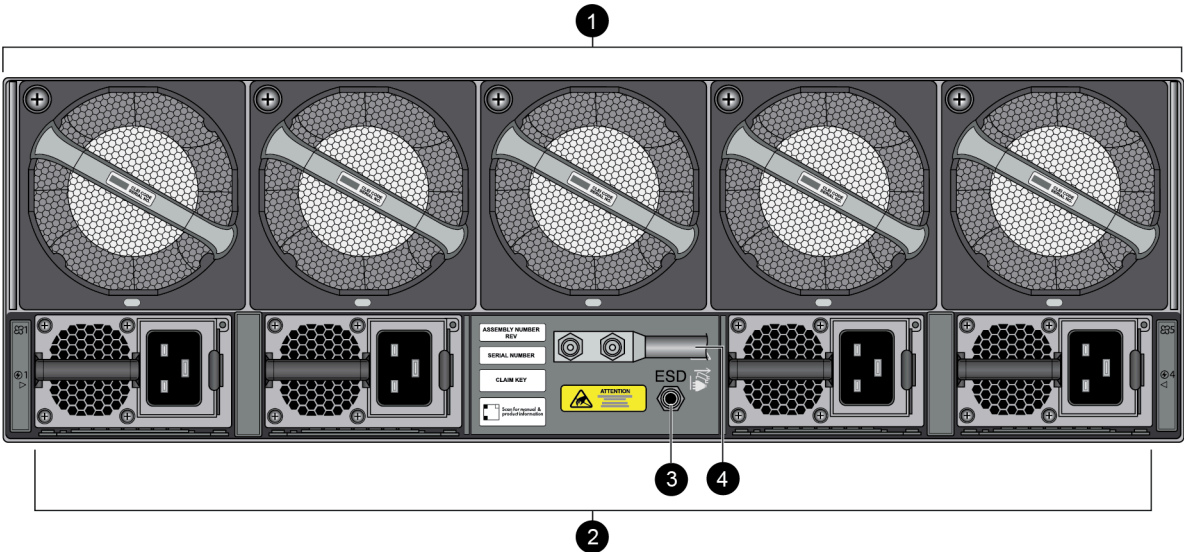
Item	Component	Description
4	HSCI Ports	Each HSCI port offers 100Gbps or 400Gbps connectivity and is used to create an Inter Firewall Link (IFL). An IFL is required to establish NGFW clustering , which carries configuration and state messages and data plane traffic.
5	QR Code	A QR code that can be scanned with a mobile device to access product documentation.
6	Drive Cover	Secures the device's drive pair, which contains PAN-OS system files, system logs, and network traffic logs.
7	Management and Logging Ports	<p>Management Ports</p> <p>Two 1Gbps/10Gbps SFP+ Management ports 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.</p> <p>Logging Ports</p> <p>Two SFP+ logging ports that offer 10Gbps connectivity each and are used as log interfaces. You must Configure Log Forwarding to forward logs from the log ports to one or more log collectors. If the log interface is not configured, the management interface is used to forward logs instead.</p>
8	Console Port (RJ-45)	<p>Use this port to connect a management computer to the firewall using a 9-pin serial-to-RJ-45 cable and terminal emulation software.</p> <p>The console connection provides access to firewall boot messages, the Maintenance Recovery Tool (MRT), and the command line interface (CLI).</p> <p> <i>If your management computer does not have a serial port, use a USB-to-serial converter.</i></p> <p>Use the following settings to configure your terminal emulation software to connect to the console port:</p> <ul style="list-style-type: none"> • Data rate: 115,200 • Data bits: 8 • Parity: None • Stop bits: 1 • Flow control: None

Item	Component	Description
9	Console port (USB-C)	<p>Use this port to connect a management computer to the firewall using a standard Type-C USB cable.</p> <p>The console connection provides access to firewall boot messages, the Maintenance Recovery Tool (MRT), and the command line interface (CLI).</p> <p>Refer to the Micro USB Console Port page for more information and to download the Windows driver or to learn how to connect from a Mac or Linux computer.</p>
10	USB Port	<p>A USB port that accepts a USB flash drive with a bootstrap bundle (PAN-OS configuration).</p> <p>Bootstrapping speeds up the process of configuring and licensing the firewall to make it operational on the network with or without internet access.</p>
11	LED Indicators	<p>Nine LEDs that indicate the status of various hardware components. For details on the LEDs, see PA-5500 Series Firewall LED Definitions.</p>

PA-5500 Series Firewall Back Panel

The following image shows the back panel of the PA-5500 Series firewalls and the table describes each front panel component.

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

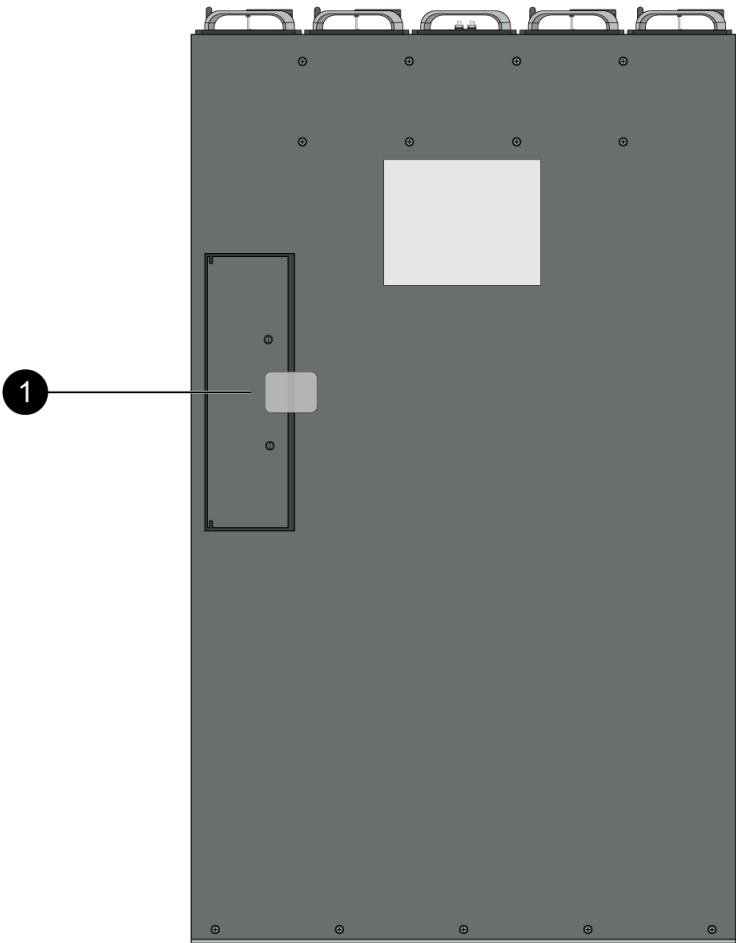


Item	Component	Description
1	Fan Assemblies	<p>Five dual-rotor fan assemblies (for a total of ten fans) that provide the appliance with cooling and ventilation. Each fan assembly can be individually replaced.</p> <p>The fan assemblies are numbered 1 through 5 from left to right.</p> <p>For information on replacing or installing a fan, see Replace a PA-5500 Series Firewall Fan Assembly.</p>
2	Power Supplies	<p>Four power supplies that provide AC or DC power to the appliance. The number of power supplies required for operation and the number eligible for redundancy depend on whether the power supplies are high line, low line, or DC.</p> <p>The power supplies are numbered 1 through 4 from left to right.</p> <p>For information on connecting power to the appliance, see Connect Power to the PA-5500 Series Firewall.</p>

Item	Component	Description
3	QR Code	A QR code that can be scanned with a mobile device to access product documentation.
4	Electrostatic Discharge (ESD) port	Provides a grounding point that you use when removing or installing appliance components. Secure the provided wrist strap end of the ESD strap around your wrist and plug the other end into the ESD port.
5	Ground Studs	Two studs used to ground the appliance to earth ground.

PA-5500 Series Firewall Top Panel

The following image shows the top panel of the PA-5500 Series firewalls and the table describes each top panel component.



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

PA-5500 Series Firewall Installation

The following topics cover how to install and set up the PA-5500 Series firewall hardware.

- [Install the PA-5500 Series Firewall in an Equipment Rack](#)
- [Connect Power to the PA-5500 Series Firewall](#)
- [Set Up a Connection to the Firewall](#)
- [Connect Cables to the PA-5500 Series Firewall](#)

Install the PA-5500 Series Firewall in an Equipment Rack

The following procedure describes how to install the PA-5540, PA-5550, PA-5560, PA-5570, and PA-5580 firewalls in a 19" four-post equipment rack using the provided four-post rack kit (PAN-PA-3RU-RACK-A). This kit is designed to provide additional support for the back of the firewall.

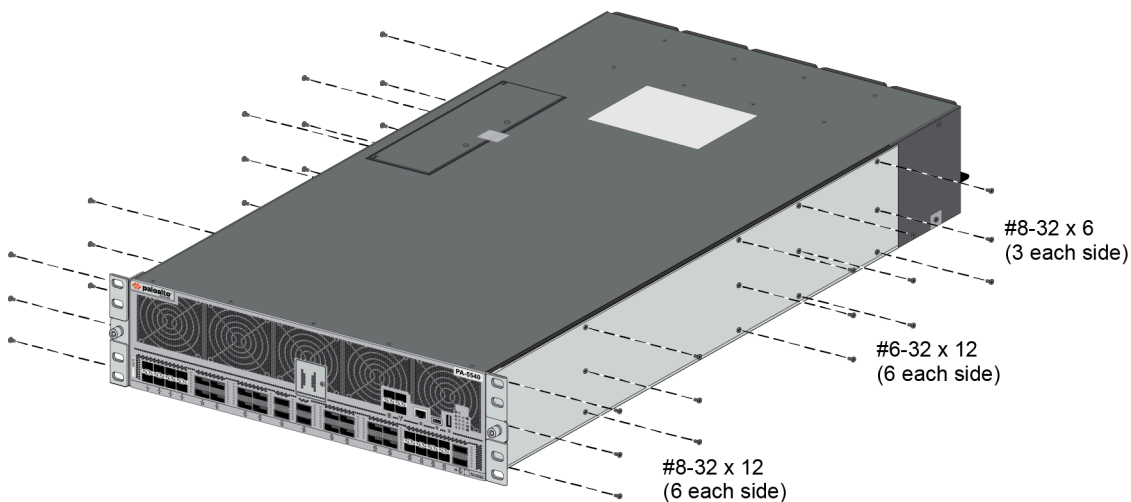


The back panel of the firewall should remain accessible to ensure ease of replacing a power supply or fan assembly.

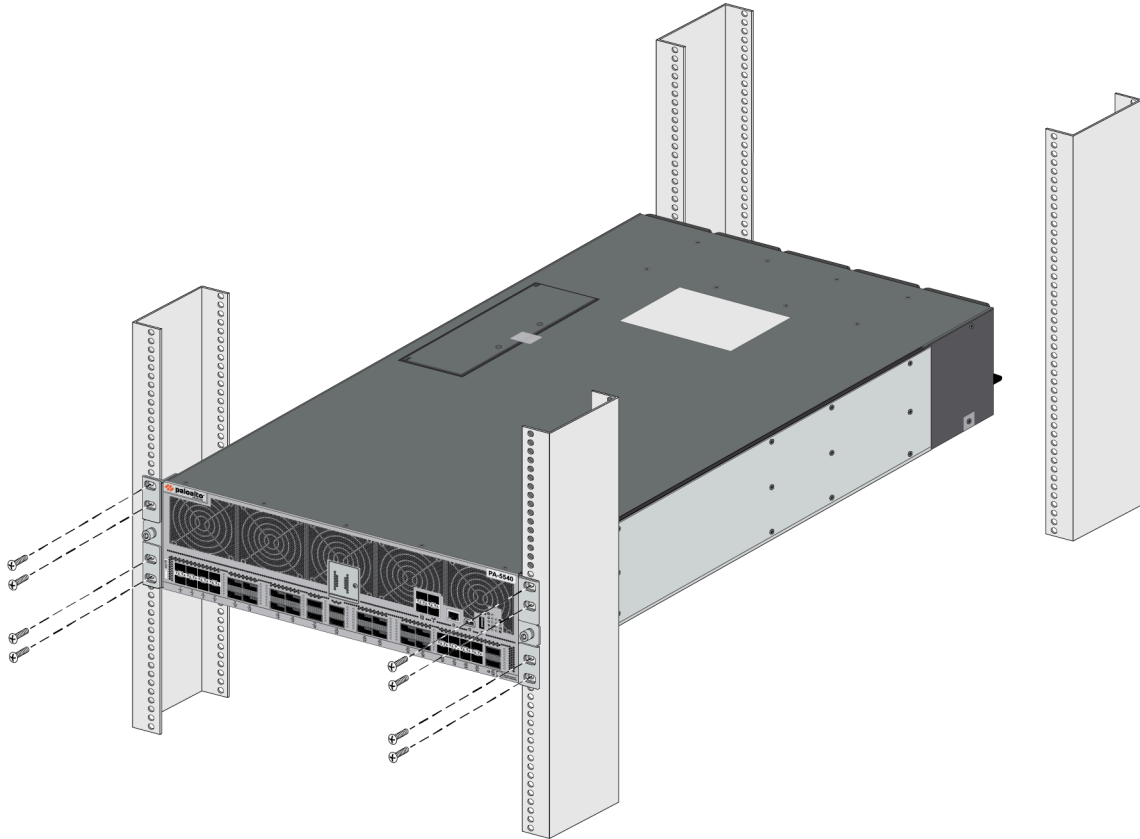
Read the following safety information before you proceed with the equipment rack installation:

- **Elevated ambient operating temperature** — If the PA-5500 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-5500 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-5500 Series Firewall Electrical Specifications](#).
- **Reliable earthing** — Maintain reliable earthing of rack-mounted equipment. Pay special attention to power connections other than direct connections to the branch circuit (such as use of power strips or extension cords) to ensure that the firewall does not exceed power ratings for connected hardware.

STEP 1 | Attach one fixed rack mount bracket to each side of the firewall. Use twelve #8-32 x 5/16" screws for the front six screw holes in each bracket. Use twelve #6-32 x 5/16" screws for the middle six screw holes in each bracket. Finally, use six #6-32 x 5/16" screws for the back screw holes in each bracket. Torque each screw to 15 in-lbs.

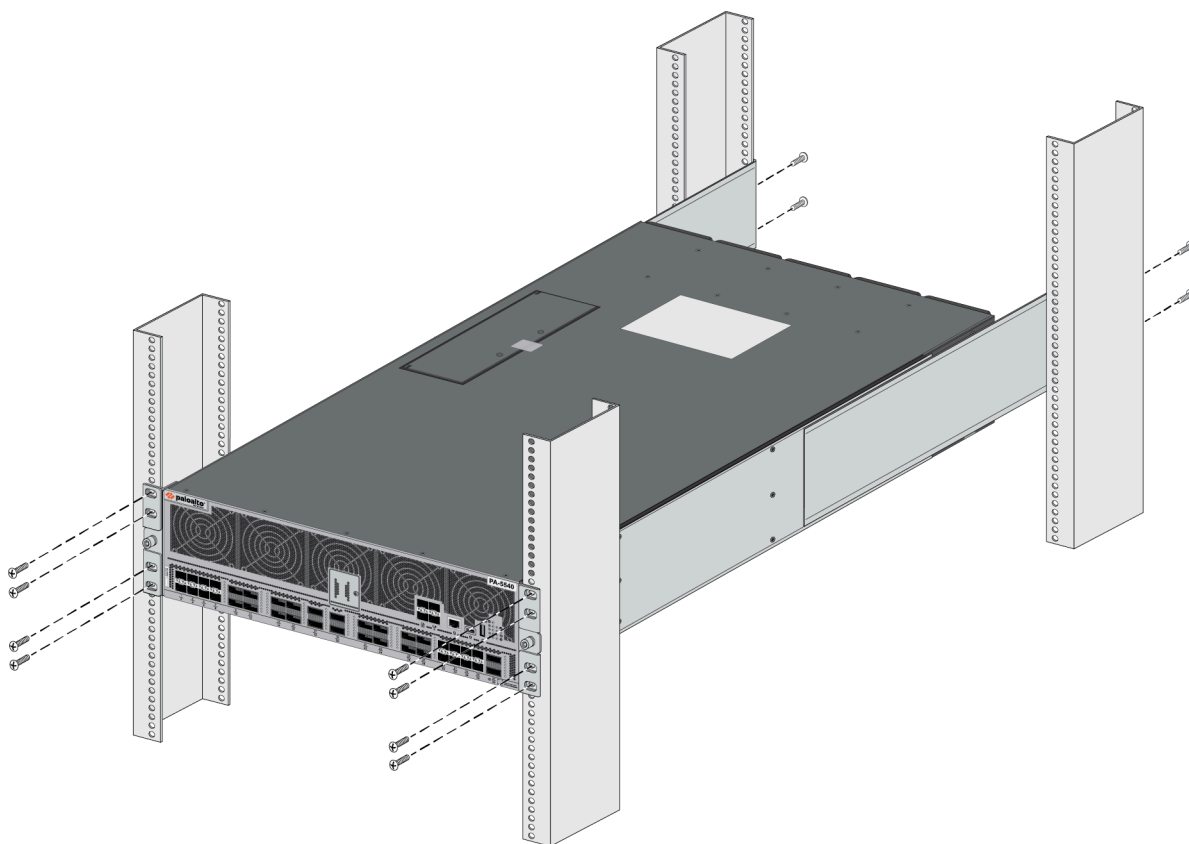


- STEP 2 |** With help from another person, hold the firewall in the rack and secure the fixed rack mount brackets to the front rack-posts using four screws for each bracket. Use the appropriate screws (#10-32 x 3/4" or #12-24 x 1/2") for your rack and torque each screw to 25 in-lbs. Use the provided cage nuts to secure the screws if the rack has square holes.



- STEP 3 |** Slide one adjustable rack mount bracket into each of the two previously installed fixed rack mount bracket. Secure the two adjustable rack mount brackets to the back rack-posts using

two screws for each bracket (#10-32 x 3/4" or #12-24 x 1/2" screws) and torque each screw to 25 in-lbs.



Connect Power to the PA-5500 Series Firewall

The following procedure describes how to connect power to a PA-5540, PA-5550, PA-5560, PA-5570, and PA-5580 firewall with either AC or DC power supplies installed.

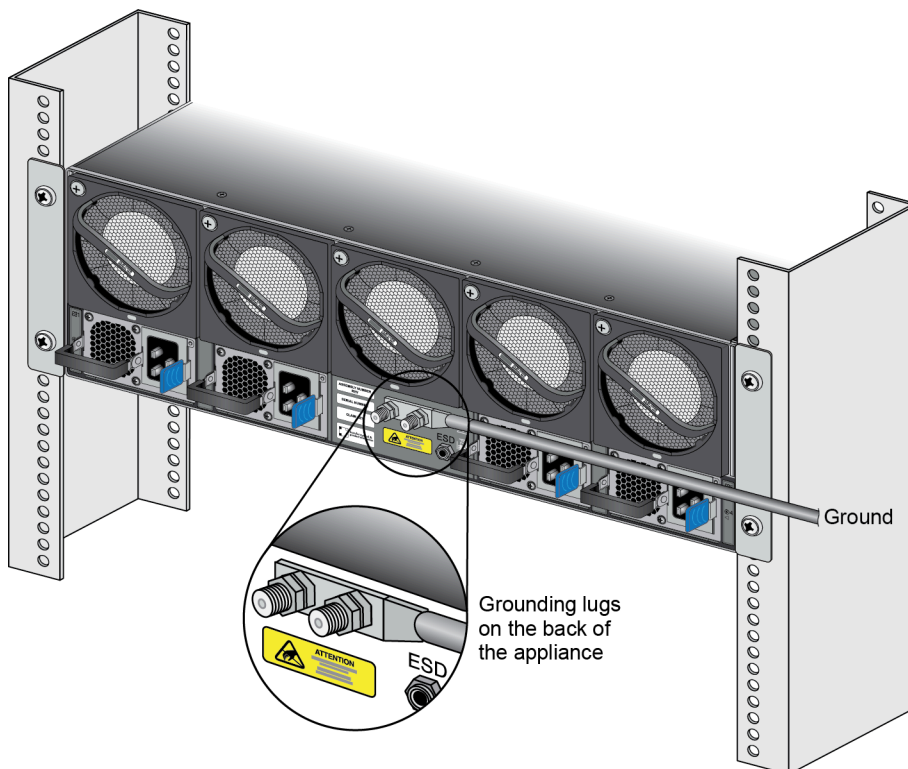
The AC and DC power supplies support two ranges of voltages: low line (110VAC) and high line (240VAC). The input voltage range determines the number of power supplies needed for the appliance. An appliance with low line input voltage requires a minimum of three power supplies while an appliance with high line input voltage requires a minimum of two power supplies. Any additional installed power supplies provided redundancy.

STEP 1 | Read the [Safety Warnings](#).

STEP 2 | Put the provided ESD wrist strap on your wrist ensuring that the metal contact is touching your skin. Then attach (snap) one end of the ground cable to the wrist strap and remove the alligator clip from the banana clip on the other end of the ESD grounding cable. Plug the banana clip end into the ESD port located on the back of the appliance before handling ESD sensitive hardware. For details on the ESD port location, see [PA-5500 Series Firewall Back Panel](#).

STEP 3 | Ensure that your power source(s) are powered off.

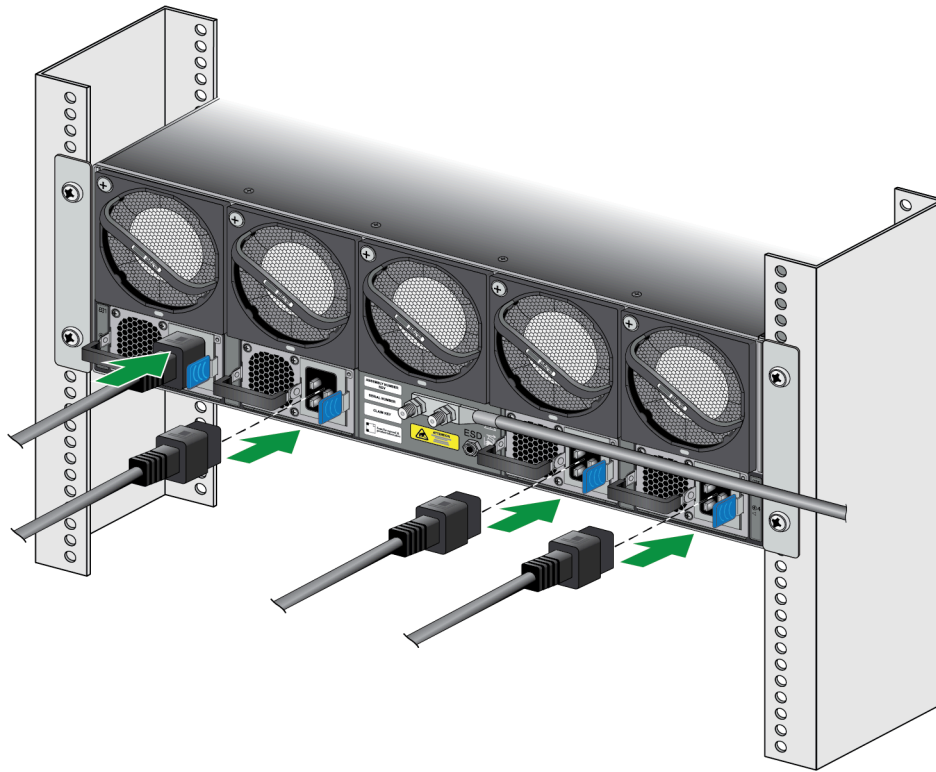
STEP 4 | Remove the nuts from one of the ground studs located on the back of the appliance.



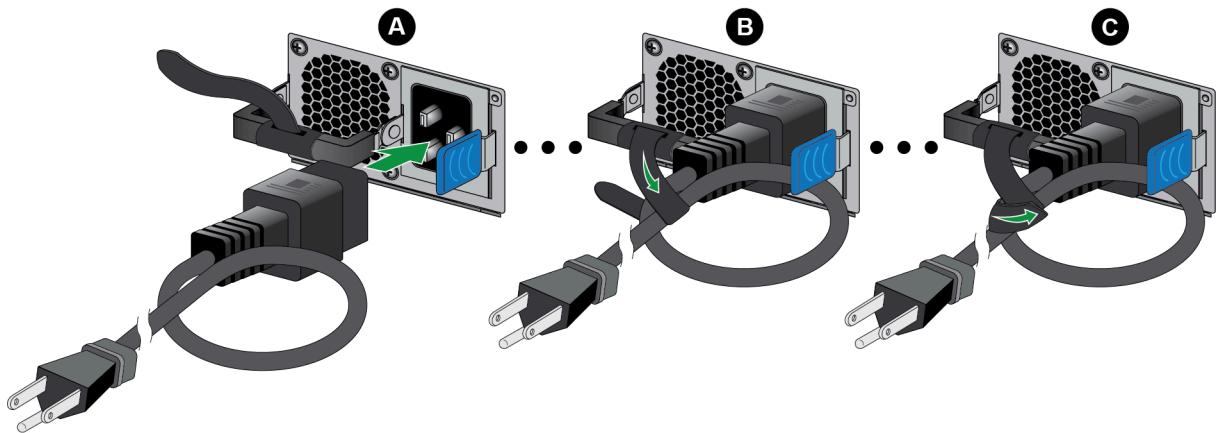
STEP 5 | Crimp a 6-AWG wire to the provided grounding lug and connect the other end to your earth ground point.

- STEP 6 |** Connect the lug connector to the ground stud on the appliance using the provided nuts and torque the nut to 50 in-lbs. Be careful not to strip the nut and lug stud.
- STEP 7 |** Slide the AC or DC power supplies into the power supply slot(s).
- STEP 8 |** (DC Power Supplies only) Connect each DC power supply to a ground connection.
- STEP 9 |** Connect the power supplies to a power source based on whether your power supplies are AC or DC.
- (AC Power Supplies)
1. Connect the first two power supplies to a 120VAC 15-amp circuit breaker or 240VAC 20-amp circuit breaker using the provided power cords and then connect the second

two power supplies to a second, independent 120VAC 15-amp circuit breaker or 240VAC 20-amp circuit breaker.

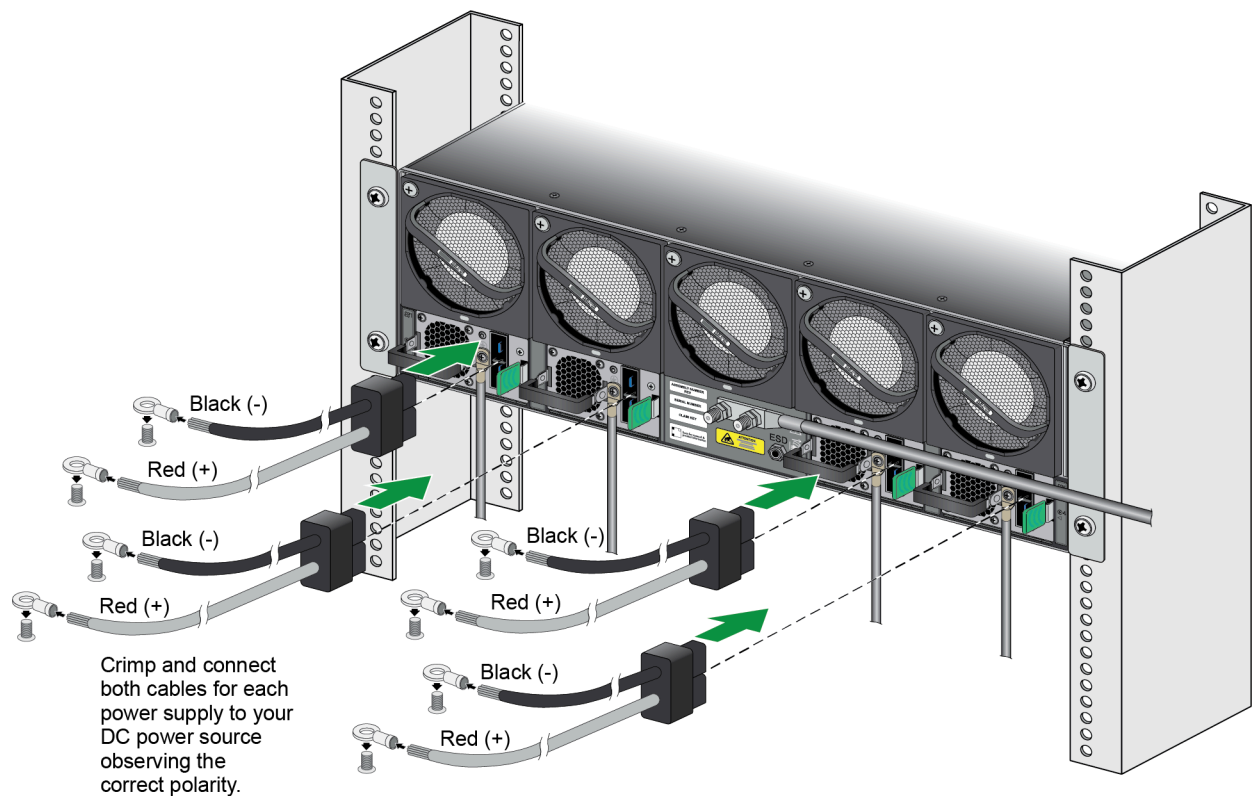


2. Secure the power cords to the power inlets using the velcro straps.



(DC Power Supplies)

1. Connect the positive and negative cable ends into the respective polarity slots in the connector, then plug the connector end into the slot in the power supply. Repeat this for each power supply.



2. 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 each of the four power supplies, 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.



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

STEP 10 | After each AC or 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-5500 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-5500 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. See [Connect Power to the PA-5500 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.

```
SSH Public key fingerprints:
Generating SSH2 RSA host key of length 2048: [ OK ]
2048 MD5:28:5a:a8:4e:3d:69:99:a8:b0:4a:77:9c:12:f6:62:ce no comment (RSA)
Starting sshd: [ OK ]
Starting PAN Software: ERROR: Module us[ 73.058994] intel_qat: module verification failed: signature and/or required key missing - tainting kernel
dm_drv does not exist in /proc/modules
ERROR: Module qat_c3xxx does not exist in /proc/modules
ERROR: Module intel_qat does not exist in /proc/modules
FATAL: Module qat_c3xxx not found.
Restarting all devices.
Processing /etc/c3xxx_dev0.conf
Checking status of all devices.
There is 1 QAT acceleration device(s) in the system:
qat_dev0 - type: c3xxx, inst_id: 0, node_id: 0, bsf: 0000:01:00.0, #accel: 3 #engines: 6 state: up
CPLD RSU not supported for ver 0x0
***** FIPS-CC Plugin Self-Tests Stage-2 begins *****
***** FIPS-CC Plugin Self-Tests Stage-2 passed *****
Zero touch provisioning (ZTP) of the firewall is in progress.
Do you want to exit ZTP mode and configure your firewall in standard mode (yes/no)[no]?y\y/no
[ OK ]
```



*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.

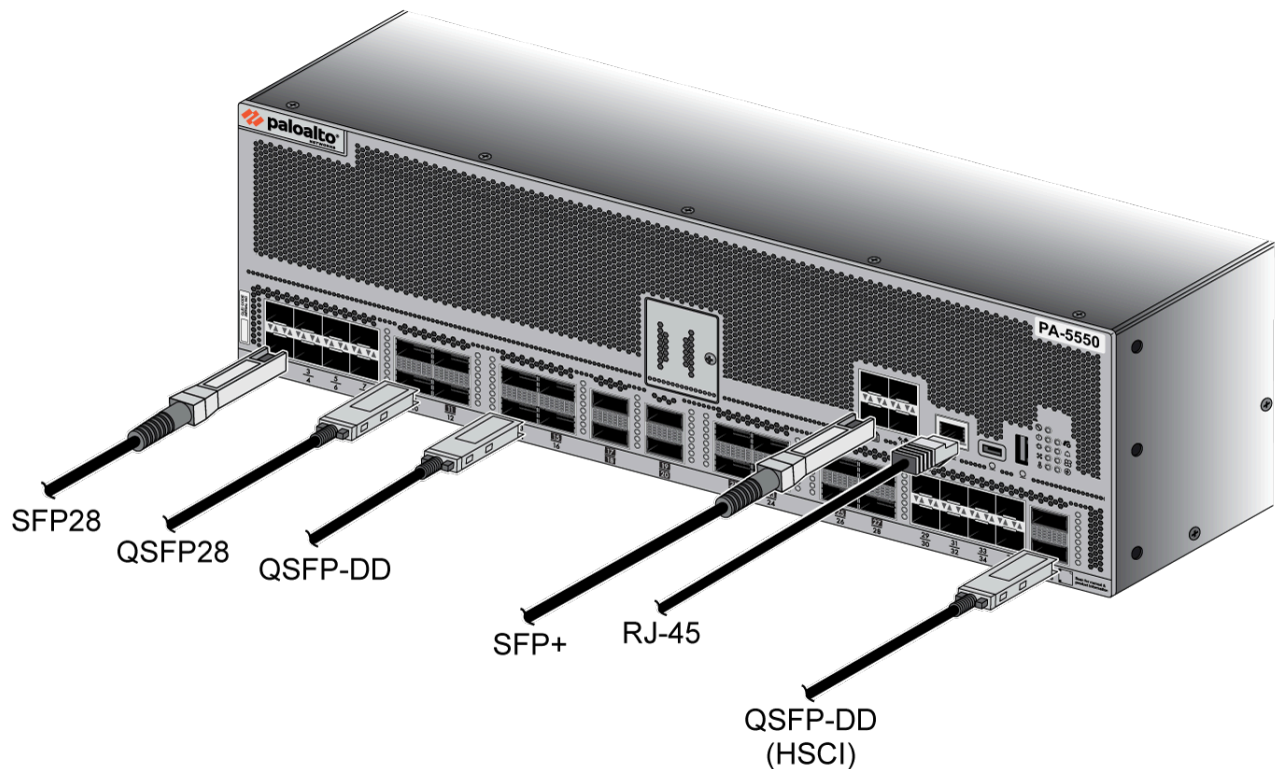
STEP 5 | Set up the firewall manually if using standard mode. If using ZTP mode, the device group and template configuration defined on the Panorama management server are automatically pushed to the firewall by the ZTP service.

- (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.

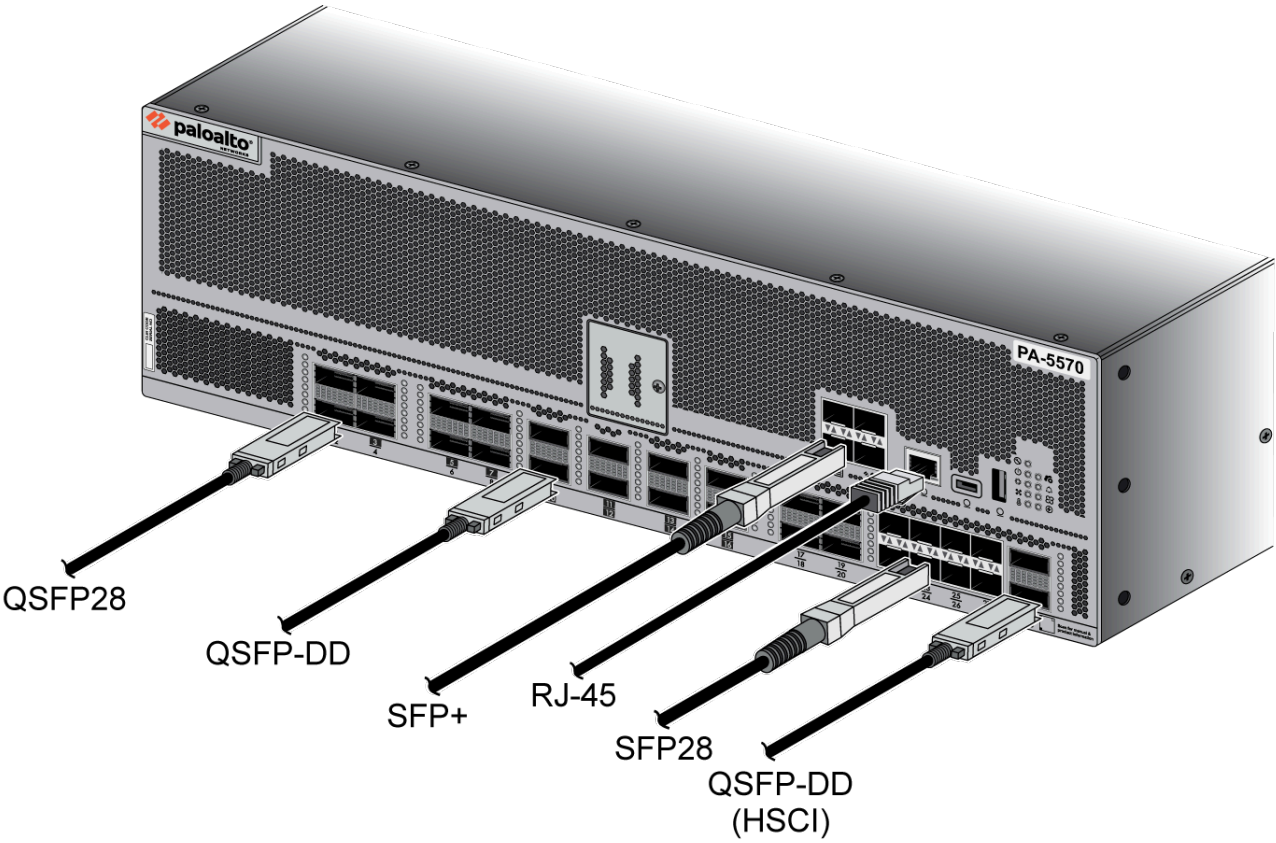
Connect Cables to the PA-5500 Series Firewall

After you [Connect Power to the PA-5500 Series 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-5540 and PA-5550 cable connections.



The next image shows the PA-5560, PA-5570, and PA-5580 firewall cable connections.



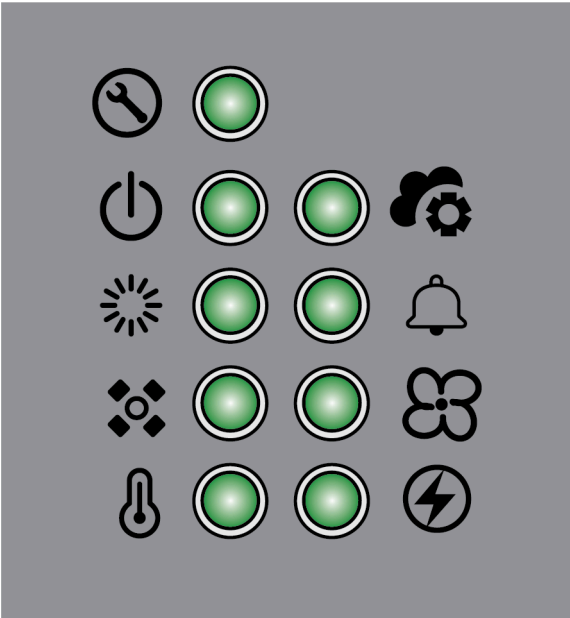
PA-5500 Series Firewall Maintenance





The following topics describes how to interpret LED information and replace field-serviceable components on a PA-5500 Series firewall.






- [PA-5500 Series Firewall LED Definitions](#)
- [Replace a PA-5500 Series Firewall Power Supply](#)
- [Replace a PA-5500 Series Firewall Fan Assembly](#)
- [Replace a PA-5500 Series Firewall System Drive](#)

PA-5500 Series Firewall LED Definitions

The following table describes how to interpret the status LEDs on a PA-5500 Series firewall.



LED	Description
Front Panel LEDs	
	Service <ul style="list-style-type: none">• Blue—The firewall is instructed by the CLI or Web Interface to enable this LED.• Off—The LED has not been enabled.
	Power <ul style="list-style-type: none">• Green—The firewall is powered on.• Yellow—The firewall has encountered a hardware failure.• Off—The firewall is not powered on.
	Status <ul style="list-style-type: none">• Green—The firewall is operating normally.• Yellow—The firewall is booting.
	NGFW Clustering <p>The LED behavior for this functionality is not implemented yet.</p>

LED	Description
	Temperature <ul style="list-style-type: none"> Green—The firewall temperature is normal. Yellow—The firewall temperature is outside tolerance levels. <p>See the PA-5500 Series Firewall Environmental Specifications for the operating temperature range.</p>
	Controller <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> Green—All fans are operating normally. Yellow—A fan has failed.
	Power Supplies <ul style="list-style-type: none"> Green—The power supplies are functioning normally. Red—One of the power supplies is not working. Off—Power supplies are not installed
Port LEDs	
RJ-45	<p>These ports have one green LED each.</p> <ul style="list-style-type: none"> Solid Green—The firewall network link is up. Blinking Green—The firewall is processing network activity.
QSFP-DD	<p>The LEDs are illuminated based on breakout status. Breaking out the port to 100Gbps causes all LEDs to glow blue. If the port is not broken out, the LEDs glow purple for 400Gbps.</p>

LED	Description
SFP28 and QSFP28	<p>The SFP28 ports have two LEDs each. The QSFP28 ports have one or four corresponding LEDs each depending on if the ports are broken out or not. The color of the LED differs based on the port speed. Refer to the descriptions on the PA-5500 Series Firewall Front Panel for the supported speeds on each port.</p> <p>10G—Green</p> <p>25G—Green & Blue</p> <p>40G—Yellow</p> <p>100G—Blue</p> <p>400G—Purple</p> <ul style="list-style-type: none">• Solid Color—The firewall network link is up.• Blinking Color—The firewall is processing network activity.

Replace a PA-5500 Series Firewall Power Supply

The following instructions describe how to replace a power supply in a PA-5500 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-5500 Series Firewall Back Panel](#).

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.



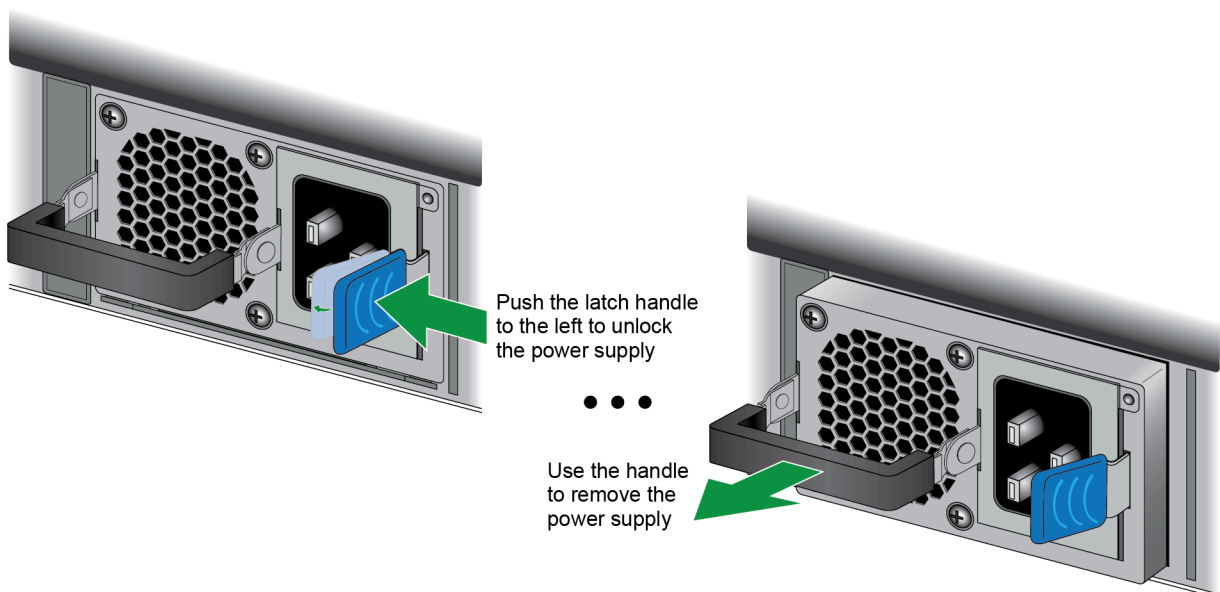
*Alternatively, you can use the CLI command **show system environmentals** to identify the failed power supply.*

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 on the metal handle to slide the power supply out.



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

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

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

(AC 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-5500 Series Firewall Fan Assembly

The PA-5500 Series firewalls have five dual-rotor fan assemblies on the rear side, making ten individual fans. When all ten 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-5500 Series Firewall Back Panel](#).



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.

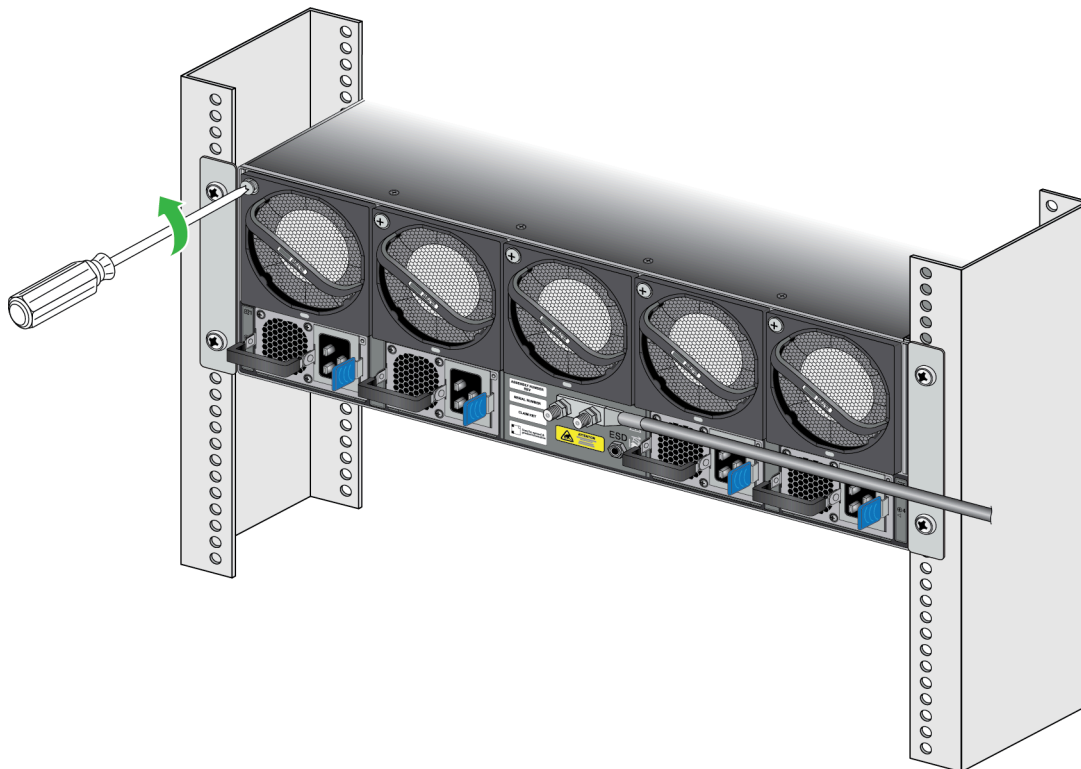
STEP 3 | Identify the fan assembly with the failed fan(s) by using the following CLI command:

```
admin@PA-5540> show system environmentals fan-tray
```

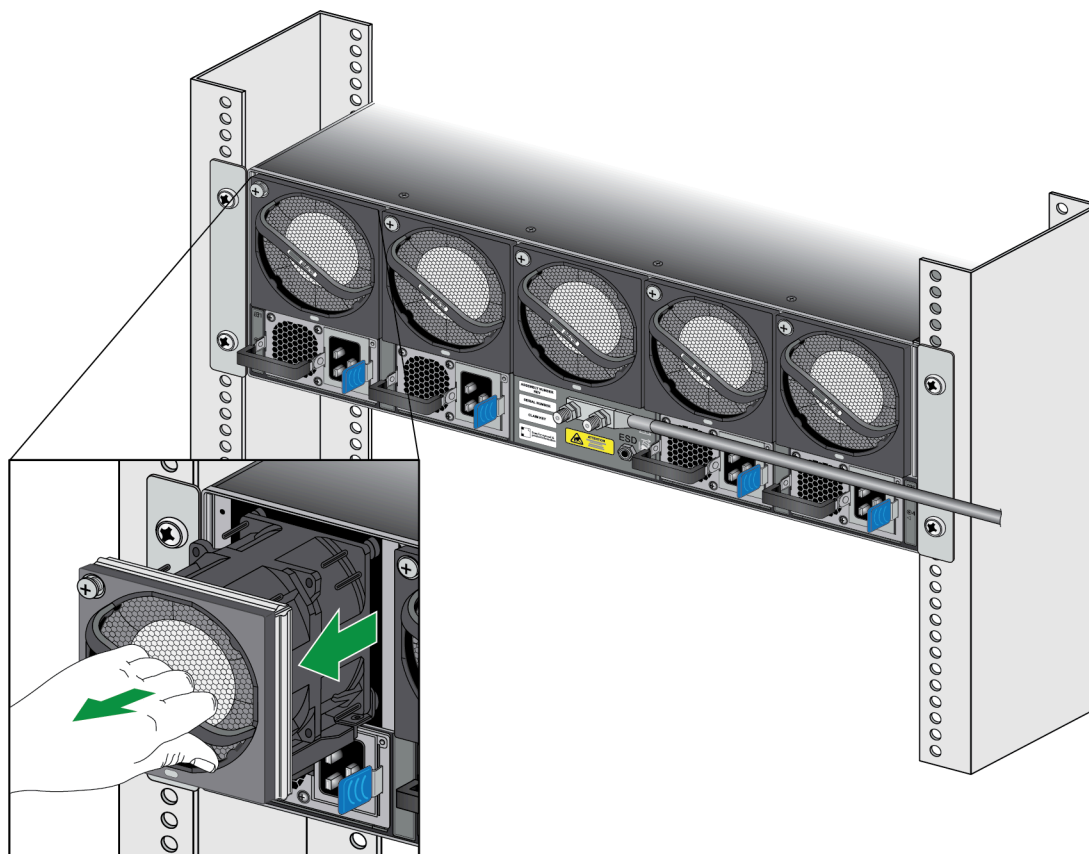


The fan assemblies are numbered 1 through 5 from left to right.

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-5540> show system environmentals fan-tray
```

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

```
admin@PA-5540> show system environmentals fans
```

Replace a PA-5500 Series Firewall System Drive

The PA-5500 Series firewalls use a pair of solid-state drives (SSDs) to store the PAN-OS system files, system logs, and network traffic logs. Both drives are embedded into a module that slides in and out of the [front panel](#) of the firewall. The second drive in the pair provides redundancy.



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:

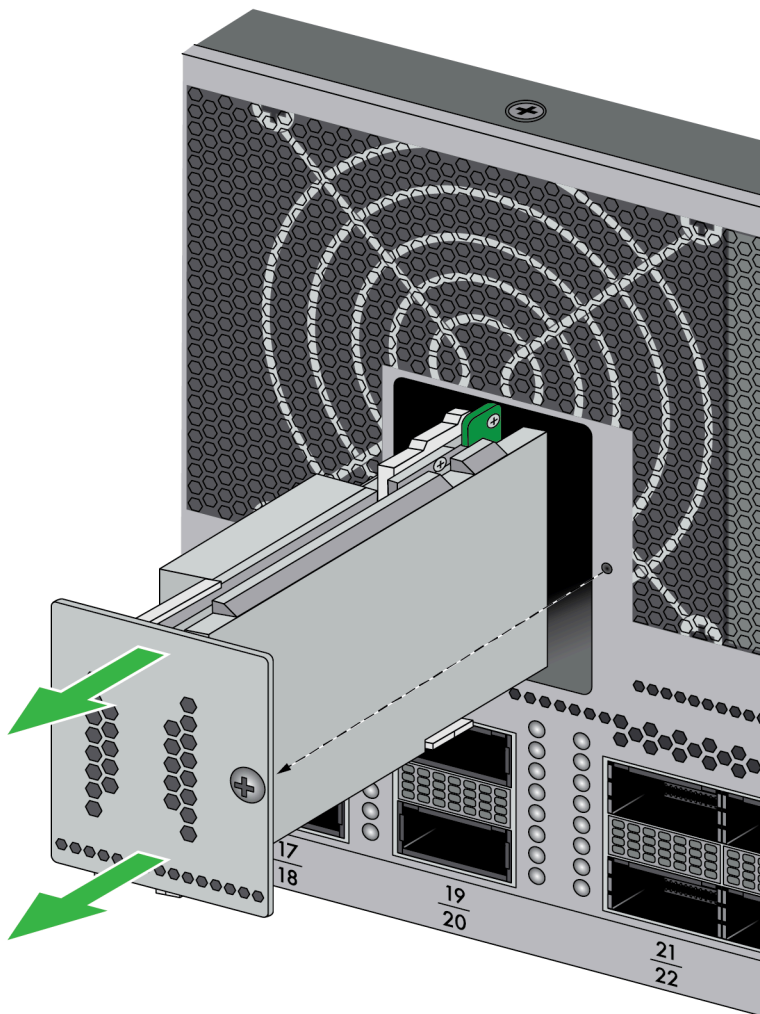
```
admin@PA-5540> show system raid detail
```

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

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

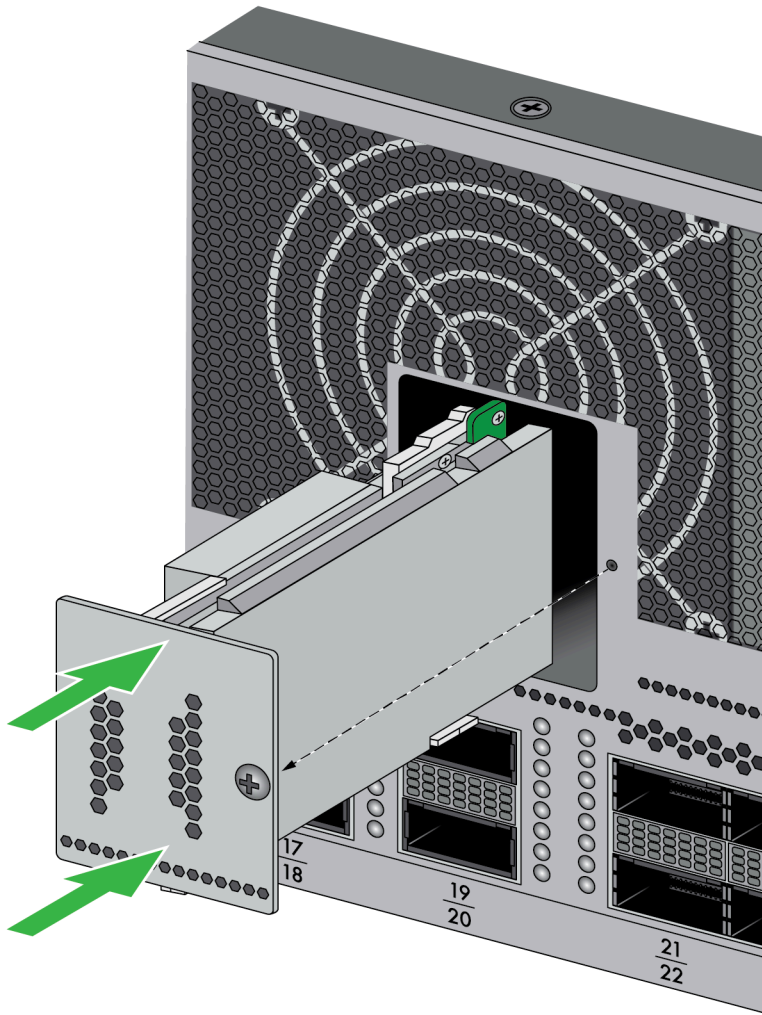
STEP 3 | Unscrew the captive screw on the system drive cover on the front side of the firewall. See [PA-5500 Series Firewall Front Panel](#) for help locating the system drive cover.

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-5540> show system raid detail
```

PA-5500 Series Firewall Specifications

The following topics describe the PA-5500 Series firewall hardware specifications. For feature, capacity, and performance information, refer to the PA-5500 Series datasheet.

- [PA-5500 Series Firewall Physical Specifications](#)
- [PA-5500 Series Firewall Electrical Specifications](#)
- [PA-5500 Series Firewall Environmental Specifications](#)

PA-5500 Series Firewall Physical Specifications

The following table describes PA-5500 Series firewall physical specifications.

Specification	Value
Rack units and dimensions	All PA-5500 Series firewalls <ul style="list-style-type: none">• Rack units—3RU• Dimensions—Height: 5.2" (13.21cm); Width: 17.3" (43.94cm); Depth: 29.8" (75.69cm)
Weight	PA-5540 and PA-5550 —78.2 lbs (35.47 kg) PA-5560, PA-5570, and PA-5580 —79 lbs (35.83 kg)

PA-5500 Series Firewall Electrical Specifications

The following table describes the PA-5500 Series firewall electrical specifications. To learn about the power cords compatible with the PA-5500 Series firewalls, see [PA-5500 Series Firewall Power Cord Types](#).

Specification	Value
Power Supplies	<p>All PA-5500 Series firewalls</p> <ul style="list-style-type: none"> PAN-PA-5500-PWR-2700-AC PAN-PA-5500-PWR-2700-DC <p>The PA-5500 Series firewalls support up to four load sharing AC or DC power supplies. The configuration of required and redundant power supplies depends on whether the power supplies support high line or low line voltages.</p> <p>The supported high line voltage is 240VAC and the supported low line voltage is 110VAC.</p> <ul style="list-style-type: none"> If the power supplies use high line voltage, two power supplies are required and two power supplies can be used for redundancy. If the power supplies use low line voltage, three power supplies are required and one power supply can be used for redundancy.
Input voltage	<p>All PA-5500 Series firewalls</p> <ul style="list-style-type: none"> AC power supplies—220VAC DC power supplies— 50VDC
Power Consumption	<p>All PA-5500 Series firewalls</p> <ul style="list-style-type: none"> Maximum—2306 W Average—2200 W
Maximum Current Consumption	<p>All PA-5500 Series firewalls</p> <ul style="list-style-type: none"> AC power supplies—10.5A@220VAC DC power supplies—46.117A@50V
Maximum Inrush Current	<p>All PA-5500 Series firewalls</p>

Specification	Value
	<ul style="list-style-type: none"> 20.274A@50V

PA-5500 Series Firewall Power Cord Types

The following table lists the power cords supported by the PA-5500 Series firewalls.

SKU Number	Description
PAN-PWR-C19-AUS	AC power cord with IEC-60320 C19 and AS/NZS 4417 cord ends, 3m
PAN-PWR-C19-EU	AC power cord with IEC-60320 C19 and CEE 7/7 SCHUKO cord ends, 3m
PAN-PWR-C19-JP	AC power cord with IEC-60320 C19 and NEMA L6-20P cord ends, 3m
PAN-PWR-C19-TW	AC power cord with IEC-60320 C19 and CNS 10917-3 cord ends, 3m
PAN-PWR-C19-UK	AC power cord with IEC-60320 C19 and BS 1363 UK13 cord ends, 3m
PAN-PWR-C19-BR	Power Cord, Brazil, 16A, 250V, NBR14136 (IEC 60906-1) to IEC-60320-C19, 10-FT, Brazilian INMETRO certified
PAN-PWR-C19-C14	Power Cord, North America, 15A, 250V, IEC C19 to IEC C14, 10ft
PAN-PWR-C19-US-120V	Power Cord, North America, 15A, 125V, C19 to NEMA 5-15P, 10ft
PAN-PWR-C19-JP-120V	Power Cord, Japan, 15A, 125V, JISC8303 to C19, 10ft, PSE Certified

PA-5500 Series Firewall Environmental Specifications

The following table describes PA-5500 Series firewall environmental specifications.

Specification	Value
Operating temperature range	0° to 50°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-5540 and PA-5550 <ul style="list-style-type: none">• With AC power supplies—79.11dBA• With DC power supplies—78.46dBA PA-5560, PA-5570, and PA-5580 <ul style="list-style-type: none">• With AC power supplies—80.57dBA• With DC power supplies—75.65dBA
Maximum operating altitude	10,000ft (3,048m)

