paloalto TECHDOCS

PA-1500 Series Next-Gen Firewall Hardware Reference

docs.paloaltonetworks.com

Contact Information

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

About the Documentation

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

Copyright

Last Revised

July 17, 2026

Table of Contents

Before You Begin

Before you install your PA-1500 Series firewall, review the following information:

- Compliance
- Parts List and Required Tools

Compliance

Safety Warnings

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

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

- When installing or servicing a Palo Alto Networks firewall or appliance hardware component that has exposed circuits, ensure that you wear an electrostatic discharge (ESD) strap. Before handling the component, make sure the metal contact on the wrist strap is touching your skin and that the other end of the strap is connected to earth ground.
- Use grounded and shielded Ethernet cables (when applicable) to ensure agency compliance with electromagnetic compliance (EMC) regulations.
- Fiber SFP transceivers emit invisible infrared lasers that can cause significant retinal damage if they make contact with your eyes. As a best practice, power off the device when installing or replacing an SFP module. If handling an SFP module while the device is operating, apply dust caps to the end of the transceiver or make sure to keep it pointed away from your eyes.
- Do not connect a supply voltage that exceeds the input range of the firewall or appliance. For details on the electrical range, refer to electrical specifications in the hardware reference for your firewall or appliance.
- 

  Caution: Shock hazard

  Disconnect all power cords (AC or DC) from the power inputs to fully de-energize the hardware.
- Do not connect or disconnect energized DC wires to the power supply.
- The DC supply source must be located within the same premises as the firewall.
- 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.
- Install all firewalls that use DC power in restricted access areas only. A restricted access area is where access is granted only to craft (service) personnel using a special tool, lock and key, or other means of security, and that is controlled by the authority responsible for the location.

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

Safety Warnings (French)

- **French Translation:** Lorsque vous installez ou que vous intervenez sur un composant matériel de pare-feu ou de dispositif Palo Alto Networks qui présente des circuits exposés, veillez à porter un bracelet antistatique. Avant de manipuler le composant, vérifiez que le contact métallique du bracelet antistatique est en contact avec votre peau et que l'autre extrémité du bracelet est raccordée à la terre.
- **French Translation:** Des câbles Ethernet blindés reliés à la terre doivent être utilisés pour garantir la conformité de l'organisme aux émissions électromagnétiques (CEM).
- **French Translation:** Veillez à ce que la tension d'alimentation ne dépasse pas la plage d'entrée du pare-feu ou du dispositif. Pour plus d'informations sur la mesure électrique, consulter la rubrique des caractéristiques électriques dans la documentation de votre matériel de pare-feu ou votre dispositif.
- 

  French Translation: (Tous les appareils Palo Alto Networks avec au moins deux sources d'alimentation) Débranchez tous les cordons d'alimentation (c.a. ou c.c.) des entrées d'alimentation et mettez le matériel hors tension.
- Ne raccordez ni débranchez de câbles c.c. sous tension à la source d'alimentation.
- La source d'alimentation c.c. doit se trouver dans les mêmes locaux que ce pare-feu.
- 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.
- Tous les pare-feux utilisant une alimentation c.c. sont conçus pour être installés dans des zones à accès limité uniquement. Une zone à accès limité correspond à une zone dans laquelle l'accès n'est autorisé au personnel (de service) qu'à l'aide d'un outil spécial, cadenas ou clé, ou autre dispositif de sécurité, et qui est contrôlée par l'autorité responsable du site.
- Installez le câble de mise à la terre c.c. du pare-feu comme indiqué dans la procédure de raccordement à l'alimentation pour le pare-feu que vous installez. Utilisez le câble American wire gauge (AWG) indiqué et serrez les écrous au couple indiqué dans la procédure d'installation de votre pare-feu.

Certifications

- **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.

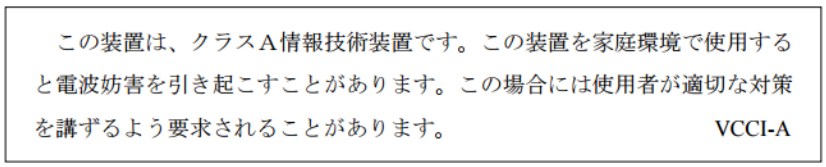
- **CE (European Union (EU) Electromagnetic Compatibility Directive)**—This device is herewith confirmed to comply with the requirements set out in the Council Directive on the Approximation of the Laws of the Member States relating to Electromagnetic Compatibility Directive (2014/30/EU).

  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)**

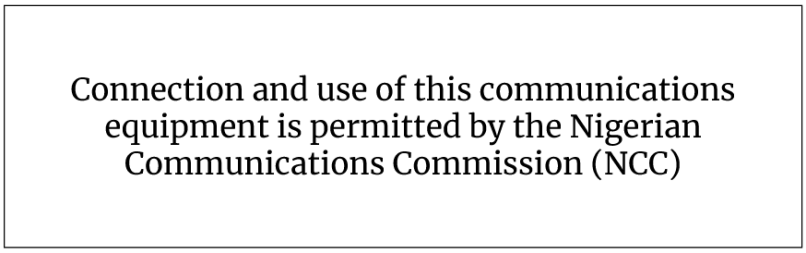
  Risk of explosion if battery is replaced by an incorrect type. Dispose of used battery according to local regulations.
- **VCCI**—This section provides the compliance statement for the Voluntary Control Council for Interference by Information Technology Equipment (VCCI), which governs radio frequency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

- **NCC (Nigerian Communications Commission)**



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-1500 Series firewall.

Table 1: Parts List – PA-1510-POE, PA-1520-POE, and PA-1530-POE

Quantity	Item
1	Ethernet cable, CAT6, white, 7 ft
1 (PA-1510-POE and PA-1520-POE) 2 (PA-1530-POE)	AC power cord, North America, 13A/125V
1	USB-C to USB-C cable
1	Rack mounting kit (PAN-PA-1RU-RACK-KIT)

The following table lists the items that are included in the PAN-PA-1RU-RACK-KIT.

Table 2: Parts List – PAN-PA-1RU-RACK-KIT

Quantity	Item
2	Fixed bracket
2	Adjustable bracket
20	Phillips head screw — #6-32 × 3/16", zinc-plated steel, Nylok

The following tools are either required or recommended when installing the PA-1500 Series firewall hardware.

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

PA-1500 Series Firewall Overview

The Palo Alto Networks® PA-1500 Series Next-Generation firewalls are designed for distributed enterprise branches. The following models make up the PA-1500 Series:

- PA-1510-POE
- PA-1520-POE
- PA-1530-POE

The PA-1500 Series firewalls provide flexibility in performance and redundancy to adapt to your deployment requirements. These models feature high port density with Multi-Gig copper ports (1G, 5G, and 10G) and fiber ports (10G SFP+ and 25G SFP28), and support Power over Ethernet on up to 16 ports at a maximum of 90W per port. The PA-1500 Series supports both AC and DC power with 1+1 redundant power supplies, and includes fail-to-wire capability for uninterrupted connectivity. These firewalls also feature a Trusted Platform Module (TPM) 2.0 for PAN-OS key storage and security, and local SSD storage for on-box logging. The PA-1500 Series provides next-generation security features to help you secure your organization through advanced visibility and control of applications, users, and content.

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

The following topic describes the hardware components of the PA-1500 Series firewalls:

- PA-1500 Series Firewall Components

PA-1500 Series Firewall Components

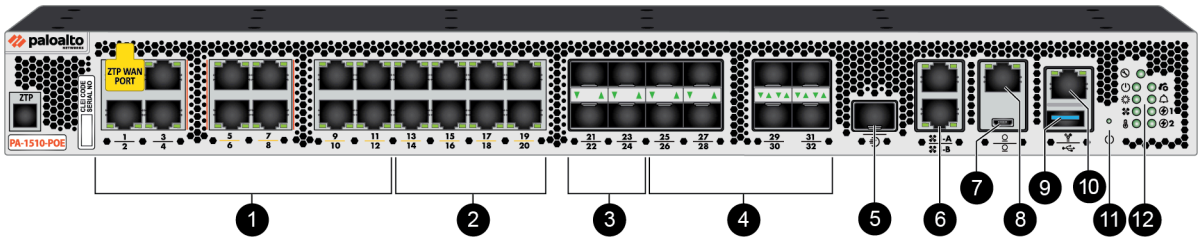
Refer to the following sections to view the front and back panel components of the PA-1500 Series firewalls.

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

- PA-1510-POE Components
- PA-1520-POE Components
- PA-1530-POE Components

PA-1510-POE Components

The following image shows the front panel of the PA-1510-POE and the table describes each front panel component.



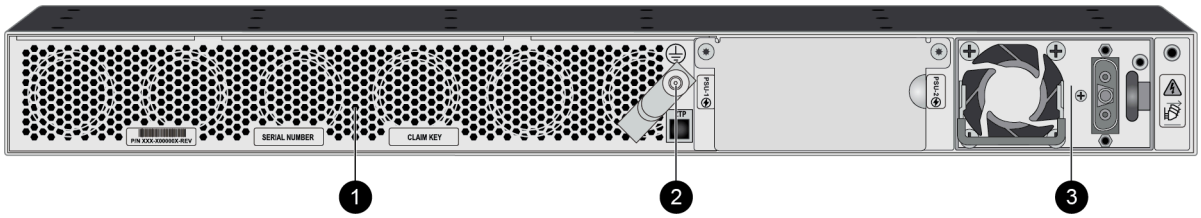
Item	Component	Description
1	RJ-45 Ports	Twelve 1Gbps copper RJ-45 ports. Port 1 is used for Zero Touch Provisioning (ZTP). *Ports 5 through 20 are PoE (Power over Ethernet) ports that can each transfer up to 90W of power to a connected device. The maximum PoE budget is 485W. Refer to the PA-1500 Series Firewall Electrical Specifications for more information about the PoE ports.* *Ports 3-4 and 5-6 are fail-open pairs. They can be configured to provide a pass-through connection despite power or operating system failure.*
2	RJ-45 Ports	Eight 5Gbps copper RJ-45 ports.
3	SFP Ports	Four 1Gbps fiber SFP ports.

Item	Component	Description
4	SFP+ Ports	Eight 10Gbps fiber SFP+ ports.
5	HSCI Port	One SFP+/SFP (10Gbps/1Gbps) port. Use this port to connect two PA-1500 Series 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. *The HSCI ports must be connected directly between the two firewalls in the HA configuration (without a switch or router between them). When directly connecting the HSCI ports between two PA-1500 Series firewalls that are physically located near each other, Palo Alto Networks recommends that you use a passive SFP+ cable.* *For installations where the two firewalls are not near each other and you cannot use a passive SFP+ cable, use a standard SFP+ transceiver and the appropriate cable length.* *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.*

Item	Component	Description
6	HA1-A and HA1-B ports	Two 1Gbps RJ-45 ports for high availability (HA) control. *If the firewall dataplane restarts due to a failure or manual restart, the HA1-B link will also restart. If this occurs and the HA1-A link is not connected and configured, then a split brain condition occurs. Therefore, we recommend that you connect and configure the HA1-A ports and the HA1-B ports to provide redundancy and to avoid split brain issues.*
7	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).
8	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
9	USB-A Port	One USB-A 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.

Item	Component	Description
		• EFR provides remediation of a compromised or potentially compromised firewall to initiate a complete cleanup of the device.
10	Management Port	One 1Gbps RJ-45 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.
11	Reset Button	A button that reboots the appliance.
12	LED Indicators	Nine LEDs that indicate the status of various hardware components. For details on the LEDs, see PA-1500 Series Firewall LED Definitions.

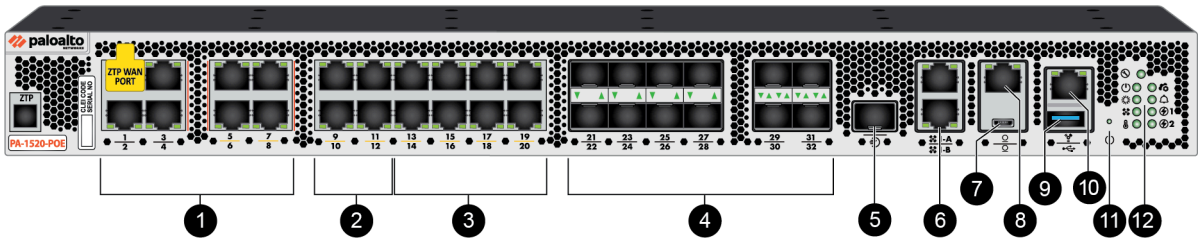
The following image shows the back panel of the PA-1510-POE and the table describes each back panel component.



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	Ground Stud	A stud used to ground the appliance to earth ground.
3	Power Supplies	One power supply that provides AC or DC power to the appliance.

PA-1520-POE Components

The following image shows the front panel of the PA-1520-POE and the table describes each front panel component.

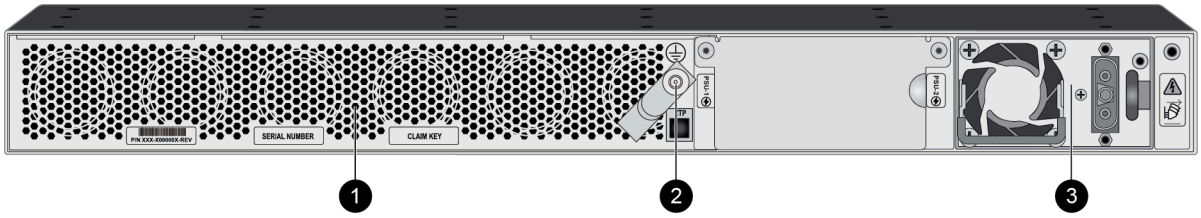


Item	Component	Description
1	RJ-45 Ports	Eight 1Gbps copper RJ-45 ports. Port 1 is used for Zero Touch Provisioning (ZTP). *Ports 5 through 20 are PoE (Power over Ethernet) ports that can each transfer up to 90W of power to a connected device. The maximum PoE budget is 545W. Refer to the PA-1500 Series Firewall Electrical Specifications for more information about the PoE ports.* *Ports 3-4 and 5-6 are fail-open pairs. They can be configured to provide a pass-through connection despite power or operating system failure.*
2	RJ-45 Ports	Eight 5Gbps copper RJ-45 ports.
3	RJ-45 Ports	Four 10Gbps copper RJ-45 ports.
4	SFP+ Ports	Twelve 10Gbps fiber SFP+ ports.
5	HSCI Port	One SFP28/SFP+/SFP (25Gbps/10Gbps/1Gbps) port. Use this port to connect two PA-1500 Series 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). When directly connecting the HSCI ports between two PA-1500 Series firewalls that are physically located near each other, Palo Alto Networks recommends that you use a passive SFP+ cable. *For installations where the two firewalls are not near each other and you cannot use a passive SFP+ cable, use a standard SFP+ transceiver and the appropriate cable length.* *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.*
6	HA1-A and HA1-B ports	Two 1Gbps RJ-45 ports for high availability (HA) control. *If the firewall dataplane restarts due to a failure or manual restart, the HA1-B link will also restart. If this occurs and the HA1-A link is not connected and configured, then a split brain condition occurs. Therefore, we recommend that you connect and configure the HA1-A ports and the HA1-B ports to provide redundancy and to avoid split brain issues.*
7	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).
8	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
9	USB-A Port	One USB-A 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.
10	Management Port	One 1Gbps RJ-45 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.
11	Reset Button	A button that reboots the appliance.
12	LED Indicators	Nine LEDs that indicate the status of various hardware components. For details on the LEDs, see PA-1500 Series Firewall LED Definitions.

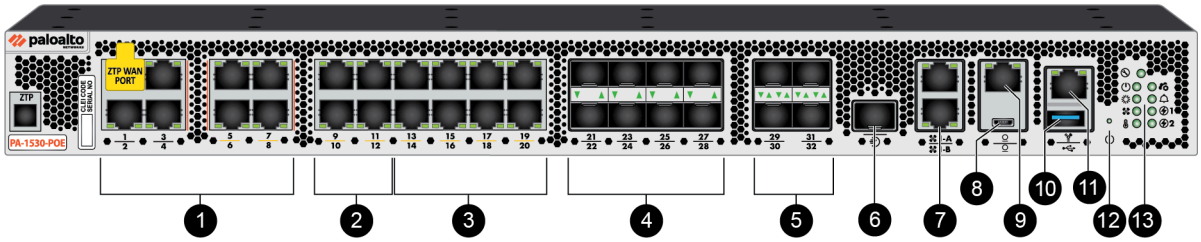
The following image shows the back panel of the PA-1520-POE and the table describes each back panel component.



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	Ground Stud	A stud used to ground the appliance to earth ground.
3	Power Supplies	One power supply that provides AC or DC power to the appliance.

PA-1530-POE Components

The following image shows the front panel of the PA-1530-POE and the table describes each front panel component.



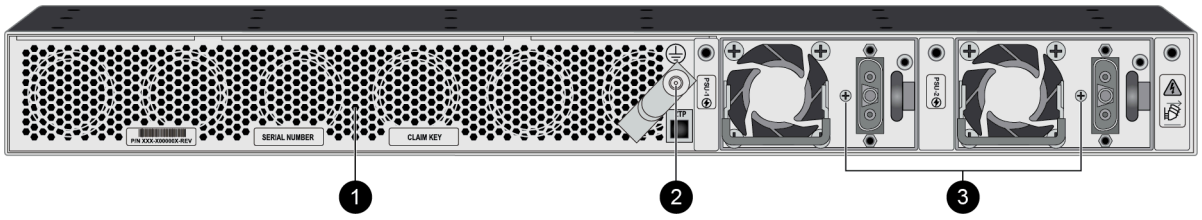
Item	Component	Description
1	RJ-45 Ports	Eight 1Gbps copper RJ-45 ports. Port 1 is used for Zero Touch Provisioning (ZTP). *Ports 5 through 20 are PoE (Power over Ethernet) ports that can each transfer up to 90W of power to a connected device. The maximum PoE budget is 724W. Refer to the PA-1500 Series Firewall Electrical Specifications for more information about the PoE ports.*

Item	Component	Description
		Ports 3-4 and 5-6 are fail-open pairs. They can be configured to provide a pass-through connection despite power or operating system failure.
2	RJ-45 Ports	Four 5Gbps copper RJ-45 ports.
3	RJ-45 Ports	Eight 10Gbps copper RJ-45 ports.
4	SFP+ Ports	Eight 10Gbps fiber SFP+ ports.
5	SFP28 Ports	Four 25Gbps fiber SFP28 ports.
6	HSCI Port	One SFP28/SFP+/SFP (25Gbps/10Gbps/1Gbps) port. Use this port to connect two PA-1500 Series 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. *The HSCI ports must be connected directly between the two firewalls in the HA configuration (without a switch or router between them). When directly connecting the HSCI ports between two PA-1500 Series firewalls that are physically located near each other, Palo Alto Networks recommends that you use a passive SFP+ cable.* *For installations where the two firewalls are not near each other and you cannot use a passive SFP+ cable, use a standard SFP+ transceiver and the appropriate cable length.*

Item	Component	Description
		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.*
7	HA1-A and HA1-B ports	Two 1Gbps RJ-45 ports for high availability (HA) control. *If the firewall dataplane restarts due to a failure or manual restart, the HA1-B link will also restart. If this occurs and the HA1-A link is not connected and configured, then a split brain condition occurs. Therefore, we recommend that you connect and configure the HA1-A ports and the HA1-B ports to provide redundancy and to avoid split brain issues.*
8	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).
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.*

Item	Component	Description
		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	USB-A Port	One USB-A 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.
11	Management Port	One 1Gbps RJ-45 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.
12	Reset Button	A button that reboots the appliance.
13	LED Indicators	Nine LEDs that indicate the status of various hardware components. For details on the LEDs, see PA-1500 Series Firewall LED Definitions.

The following image shows the back panel of the PA-1530-POE and the table describes each back panel component.



Item	Component	Description
1	Fans	Six dual-rotor fans that provide the appliance with cooling and ventilation. The fans are not field replaceable.

Item	Component	Description
		The firewall is designed to continue operating even if one fan rotor has failed.
2	Ground Stud	A stud used to ground the appliance to earth ground.
3	Power Supplies	Two power supplies that provide AC or DC power to the appliance. The power supplies are numbered 1 through 2 from left to right.

PA-1500 Series Firewall Installation

The following topics cover how to install and set up the PA-1500 Series firewall hardware.

- Install the PA-1500 Series Firewall in an Equipment Rack
- Connect AC Power to the PA-1500 Series Firewall
- Connect DC Power to the PA-1500 Series Firewall
- Set Up a Connection to the Firewall
- Connect Cables to the PA-1500 Series Firewall

Install the PA-1500 Series Firewall in an Equipment Rack

The following procedure describes how to install the PA-1510-POE, PA-1520-POE, and PA-1530-POE firewalls in a 19" four-post equipment rack using the provided four-post rack kit (PAN-PA-1RU-RACK-KIT).

Table 3: Parts List – PAN-PA-1RU-RACK-KIT

Quantity	Item
2	Fixed bracket
2	Adjustable bracket
20	Phillips head screw — #6-32 × 3/16", zinc-plated steel, Nylok

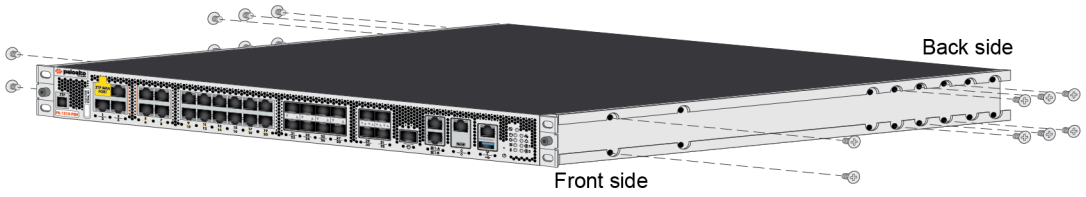
The back panel of the firewall should remain accessible to ensure ease of replacing a power supply.

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

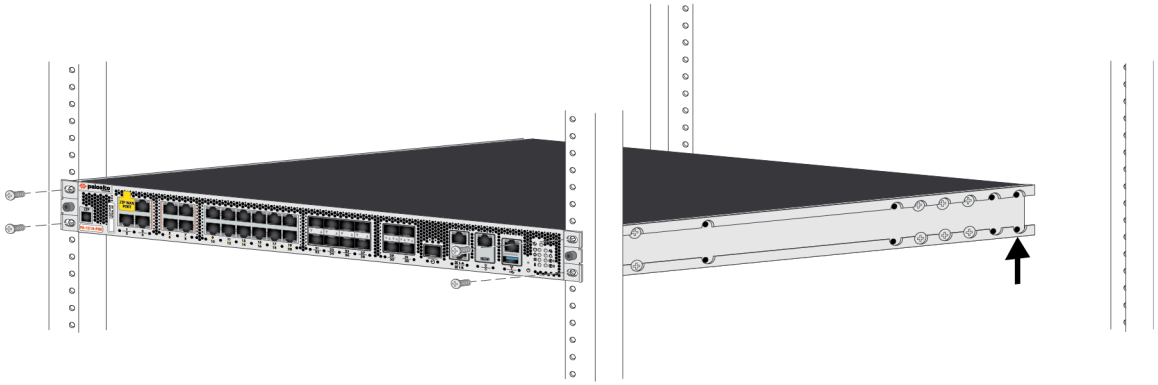
- **Elevated ambient operating temperature** — If the PA-1500 Series firewall is installed in a closed or multi-unit rack assembly, the ambient operating temperature of the rack environment may be greater than the ambient room temperature. Verify that the ambient temperature of the rack assembly does not exceed the maximum rated ambient temperature requirements listed in the PA-1500 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-1500 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

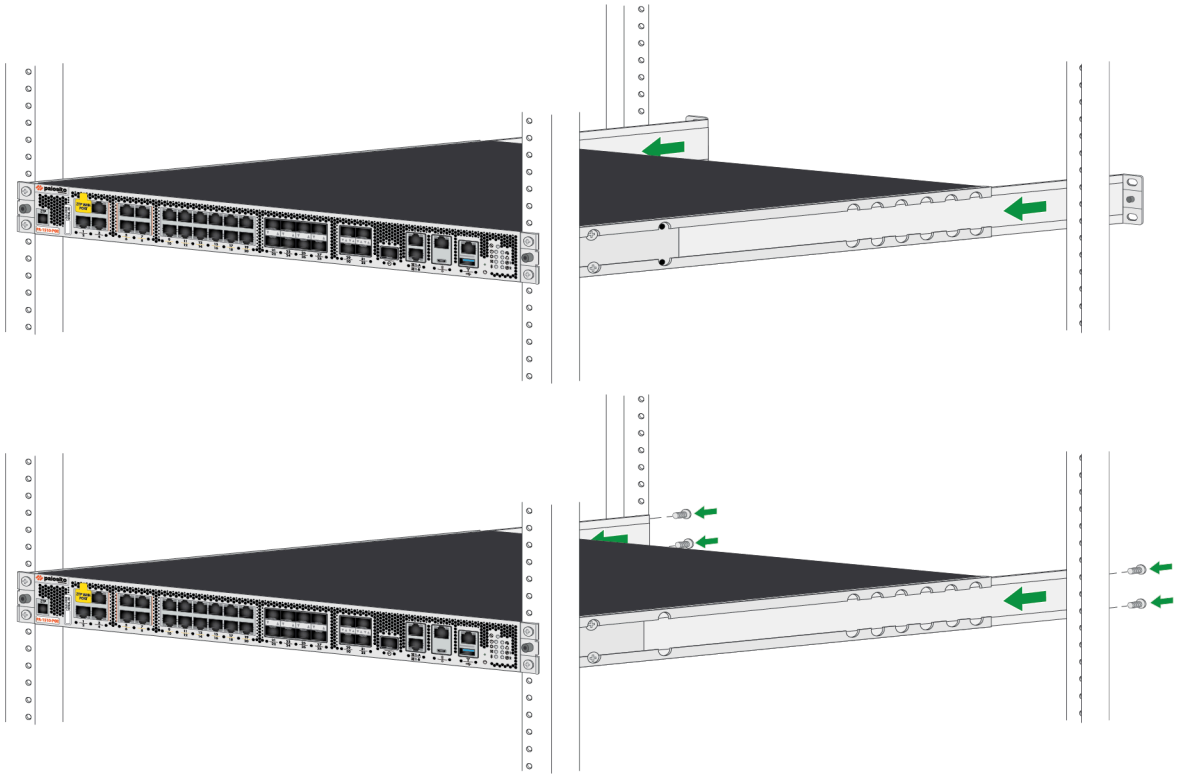
- Use four #6-32 × 3/16" screws for the front screw holes in each bracket (8 total).
- Use six #6-32 × 3/16" screws for the back screw holes in each bracket (12 total).



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 two screws for each bracket. Use the appropriate screws for your rack.



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



Connect AC Power to the PA-1500 Series Firewall

The following procedure describes how to connect AC power to a PA-1500 Series firewall with AC power supplies.

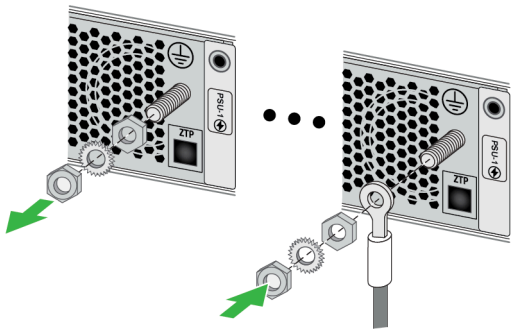
Learn how to Set Up a Connection to the Firewall based on your desired boot mode prior to powering on the firewall for the first time.

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

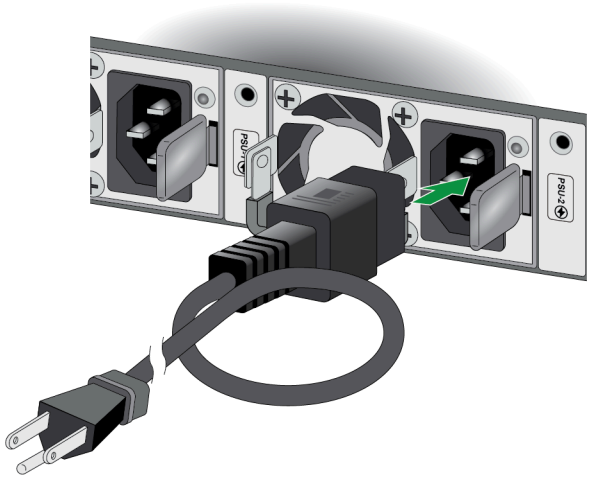
STEP 1 | Ensure that your power source(s) are powered off.

STEP 2 | Remove the nut and star washer from the ground stud 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 washer and nut, then connect the other end of the cable to earth ground.



STEP 4 | Connect the AC power cord to the input on the PSU.



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 | (PA-1530-POE only) Repeat the previous step for the second power supply.

STEP 6 | Connect the other end of the power cord 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 DC Power to the PA-1500 Series Firewall

The following procedure describes how to connect DC power to a PA-1500 Series firewall with DC power supplies.

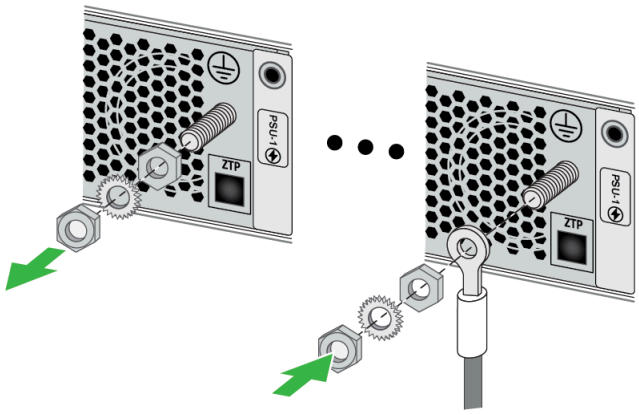
Learn how to Set Up a Connection to the Firewall based on your desired boot mode prior to powering on the firewall for the first time.

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

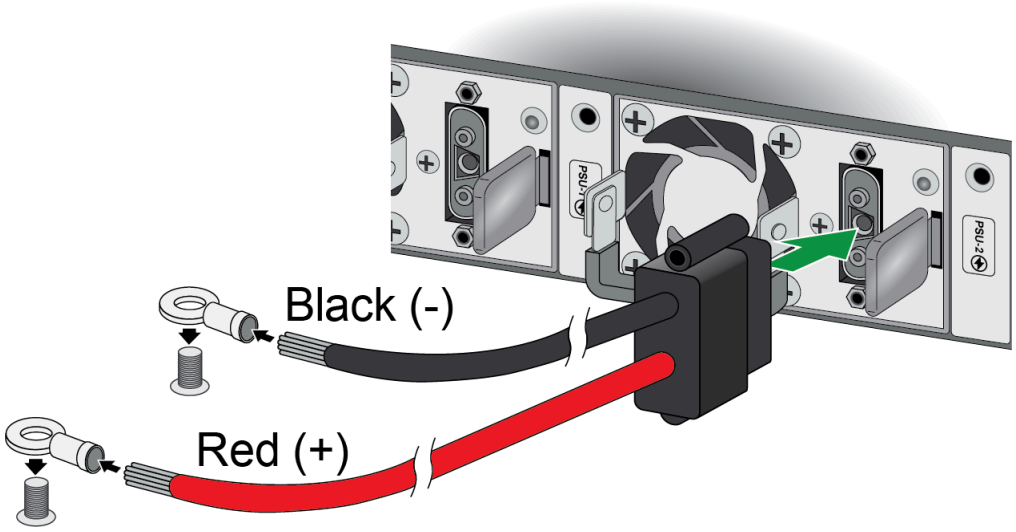
STEP 1 | Ensure that your power source(s) are powered off.

STEP 2 | Remove the nut and star washer from the ground stud 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 washer and nut, then connect the other end of the cable to earth ground.



STEP 4 | 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.



STEP 5 | Connect the opposite end of the positive and negative cables to a 60A circuit breaker.

> *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 6 | (PA-1530-POE only) Repeat steps 4 and 5 for a second power supply.

STEP 7 | Turn on the DC power source. After 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.

Set Up a Connection to the Firewall

On first startup, the PA-1500 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-1500 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.

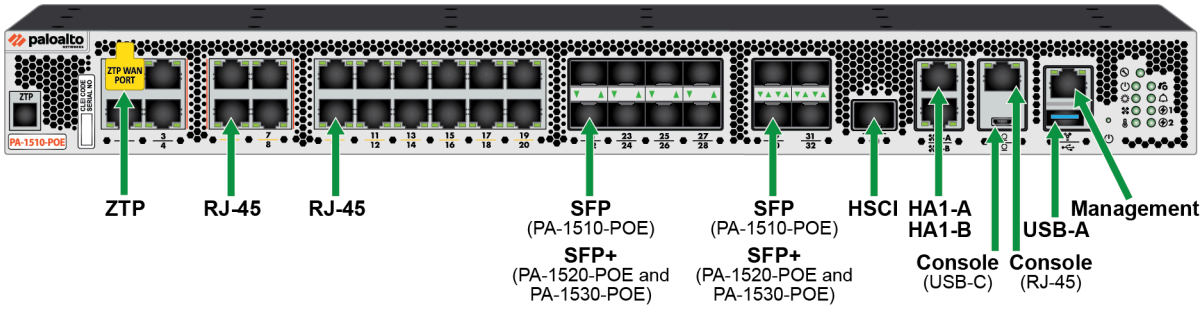
STEP 5 | Set up the firewall manually if using standard mode. If using ZTP mode, the device group and template configuration defined on the Panorama management server are automatically pushed to the firewall by the ZTP service.

- (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-1500 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 an overview of the cable connections. For specific details about port speeds, numbering, and variations between models, refer to the PA-1500 Series Firewall Components.



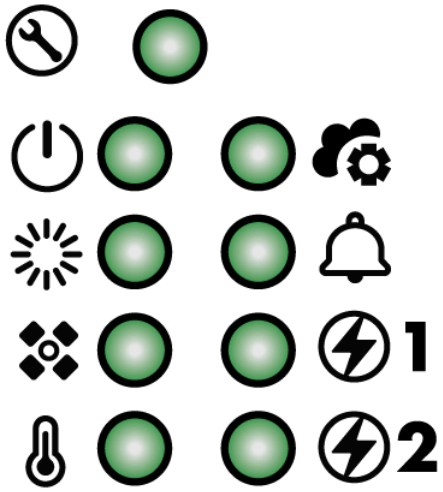
PA-1500 Series Firewall Maintenance

The following topics describe how to maintain the PA-1500 Series firewall:

- PA-1500 Series Firewall LED Definitions
- Replace a PA-1500 Series Firewall Power Supply

PA-1500 Series Firewall LED Definitions

The following table describes how to interpret the status LEDs on a PA-1500 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**—One or more power rails are not functioning normally, or the push-button power off was performed. • **Off**—The firewall is not powered on.
	**Status** • **Green**—The firewall is operating normally. • **Yellow**—The firewall is booting. • **Red**—The firewall failed to complete a secure boot.
	**High Availability**

LED	Description
	• **Green**—High availability is configured and the firewall is in the active HA state. • **Yellow**—High availability is configured and the firewall is in the standby HA state. • **Off**—High availability is not configured.
	**Temperature** • **Green**—The firewall temperature is normal. • **Yellow**—The firewall temperature is outside tolerance levels. See the PA-1500 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, a fan failure, or the hardware overheated and exceeded the high temperature threshold. • **Off**—The firewall is operating normally.
	**Power Supplies** • **Green**—The power supply is present and supplying correct voltage. • **Yellow**—The power supply is present but supplying incorrect voltage. • **Off**—The power supply is 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 two LEDs each.

LED	Description
	Left LED (Link/Speed) • **Green**—The link speed is 1 Gbps or higher. • **Yellow**—The link speed is 10 or 100 Mbps. • **Off**—No link. **Right LED (Activity)** • **Blinking Green**—The firewall is processing network activity. • **Off**—No network activity.
SFP, SFP+, and SFP28	These ports have one LED each. The color indicates the link speed. 1G—Yellow 10G—Green 25G—Light Blue • **Solid Color**—The firewall network link is up. • **Blinking Color**—The firewall is processing network activity. • **Off**—No link.

Replace a PA-1500 Series Firewall Power Supply

The following instructions describe how to replace an AC or DC power supply in a PA-1500 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.

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

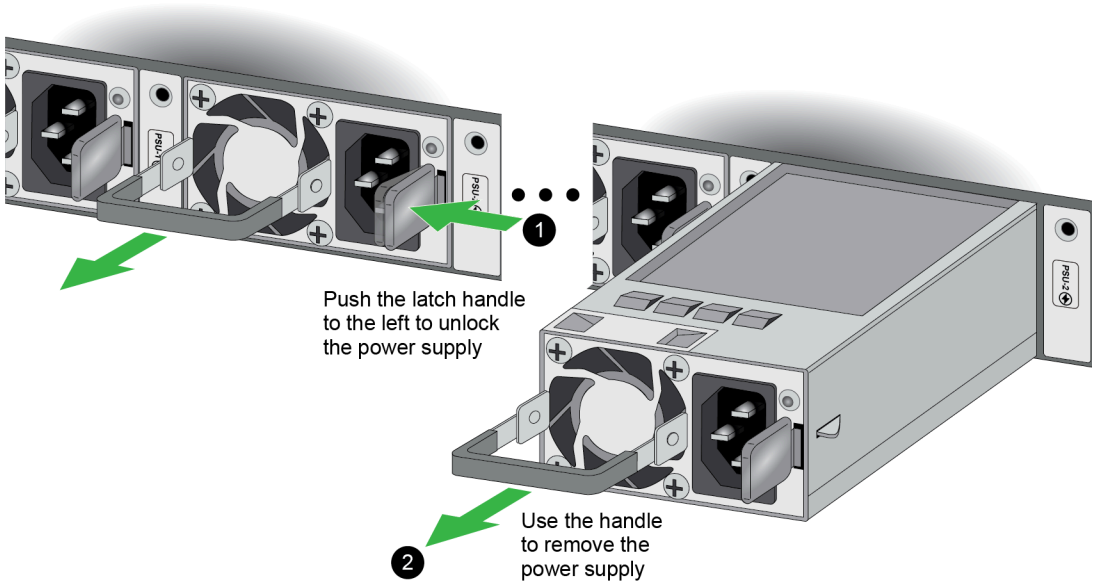
> *Alternatively, you can use the CLI command* ***`show system environmentals`*** *to identify the failed power supply.*

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. 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. Once the power supply powers on, the input and output LEDs on the power supply turn green. Similarly, the power LED and the power supply LED (1 or 2) on the front of the firewall turn green.

PA-1500 Series Firewall Specifications

The following topics describe the specifications of the PA-1500 Series firewall:

PA-1500 Series Firewall Physical Specifications

The following table describes PA-1500 Series firewall physical specifications.

Specification	Value
Rack units and dimensions	**PA-1510-POE, PA-1520-POE, and PA-1530-POE** • Height x Width x Depth—1.70 in x 17.3 in x 18.4 in (43.2 mm x 440.4 mm x 468.3 mm) • Rack units—1 RU
Weight	**PA-1510-POE and PA-1520-POE** • Firewall weight—20.1 lbs (9.1 kg) **PA-1530-POE** • Firewall weight—21.9 lbs (9.9 kg)

PA-1500 Series Firewall Electrical Specifications

The following table describes PA-1500 Series firewall electrical specifications.

Specification	Value
Power Supplies	**All PA-1500 Series firewalls** • PAN-PWR-1200W-54V-AC-A • PAN-PWR-1200W-54V-DC-A
Maximum power consumption	**PA-1510-POE**—890 W **PA-1520-POE**—956 W **PA-1530-POE**—1132 W
Power over Ethernet (PoE)	Supported on ports Ethernet Ports 5 through 20 on all models. Maximum power reserved per port—90 W **Total PoE budget (across all ports)** • **PA-1510-POE**—485 W • **PA-1520-POE**—545 W • **PA-1530-POE**—724 W

PA-1500 Series Firewall Power Cord Types

The following table lists the power cords supported by the PA-1500 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

SKU Number	Description
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

PA-1500 Series Firewall Environmental Specifications

The following table describes PA-1500 Series firewall environmental specifications.

Specification	Value
Operating temperature range	**PA-1510-POE, PA-1520-POE, and PA-1530-POE**—32°F to 104°F (0°C to 40°C)
Airflow	The PA-1500 Series firewalls use active cooling. Airflow is front-to-rear.
Maximum BTUs/hour	• **PA-1510-POE**—3036.8 BTU/hr • **PA-1520-POE**—3262.0 BTU/hr • **PA-1530-POE**—3862.5 BTU/hr
Maximum operating altitude	9,843 ft (3,000 m)

PA-1500 Series Firewall Miscellaneous Specifications

The following table describes PA-1500 Series firewall miscellaneous specifications.

Specification	Value
Storage capacity	**PA-1510-POE and PA-1520-POE**—480 GB SSD **PA-1530-POE**—960 GB SSD
Mean time between failures (MTBF)	**PA-1510-POE, PA-1520-POE, and PA-1530-POE**—211,260 hours (24 years) at 40°C