paloalto TECHDOCS

PA-3400 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

August 22, 2024

Table of Contents

Before You Begin

Read the following topics before you install or service a Palo Alto Networks® next-generation firewall or appliance.**The following topics apply to all Palo Alto Networks firewalls and appliances except where noted.**

Upgrade/Downgrade Considerations for Firewalls and Appliances

The following table lists all hardware features that have upgrade or downgrade impact. Make sure you understand all upgrade/downgrade considerations before you upgrade or downgrade from the specified version of PAN-OS.

Feature	Release	Upgrade Considerations	Downgrade Considerations
PA-7000 Log Forwarding Card (LFC)	10.0	If you are using an LFC with a PA-7000 Series Firewall, when you upgrade to PAN-OS 10.0, you must configure the management plane or dataplane interface for the service route because the LFC ports do not support the requirements for the service route. We recommend using the dataplane interface for the Data Services service route.	n/a
Upgrading a PA-7000 Series Firewall with a first generation switch management card (PA-7050-SMC or PA-7080-SMC)	PAN-OS 8.0 and later	Before upgrading the firewall, run the following CLI command to check the flash drive's status: **`debug system disk-smart-info disk-1`**. If the value for attribute ID #232, **Available_Reservd_Space 0x0000**, is greater than 20, then proceed with the upgrade. If the value is less than 20, then contact support for assistance.	Before downgrading the firewall, run the following CLI command to check the flash drive's status: **`debug system disk-smart-info disk-1`**. If the value for attribute ID #232, **Available_Reservd_Space 0x0000**, is greater than 20, then proceed with the downgrade. If the value is less than 20, then contact support for assistance.

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.

(PA-7000 Series firewalls only) PA-7000 Series firewalls are modular systems and therefore do not include a warranty label on the firewall.

Third-Party Component Support

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

Product 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.

The following safety warnings apply to all Palo Alto Networks firewalls and appliances, unless a specific hardware model is specified.

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

  French Translation: Lorsque vous installez ou que vous intervenez sur un composant matériel de pare-feu ou de dispositif Palo Alto Networks qui présente des circuits exposés, veillez à porter un bracelet antistatique. Avant de manipuler le composant, vérifiez que le contact métallique du bracelet antistatique est en contact avec votre peau et que l'autre extrémité du bracelet est raccordée à la terre.
- Use grounded and shielded Ethernet cables (when applicable) to ensure agency compliance with electromagnetic compliance (EMC) regulations.

  French Translation: Des câbles Ethernet blindés reliés à la terre doivent être utilisés pour garantir la conformité de l'organisme aux émissions électromagnétiques (CEM).
- At least two people are recommended for unpacking, handling, and relocating the heavier firewalls.
- Do not connect a supply voltage that exceeds the input range of the firewall or appliance. For details on the electrical range, refer to electrical specifications in the hardware reference for your firewall or appliance.

  French Translation: Veillez à ce que la tension d'alimentation ne dépasse pas la plage d'entrée du pare-feu ou du dispositif. Pour plus d'informations sur la mesure électrique, consulter la rubrique des caractéristiques électriques dans la documentation de votre matériel de pare-feu ou votre dispositif.
- (Devices with serviceable batteries only) Do not replace a battery with an incorrect battery type; doing so can cause the replacement battery to explode. Dispose of used batteries according to local regulations.

  French Translation: Ne remplacez pas la batterie par une batterie de type non adapté, cette dernière risquerait d'exploser. Mettez au rebut les batteries usagées conformément aux instructions.
- I/O ports are intended for intra-building connections only and not intended for OSP (Outside Plant) connections or any network connections subject to external voltage surge events.

- (PA-410R, PA-410R-5G, PA-450R-5G, and PA-450R firewalls only) Do not open, connect, or disconnect power when an explosive atmosphere is present or while the power source is energized.

• 	(All Palo Alto Networks appliances with two or more power supplies) Caution: Shock hazard Disconnect all power cords (AC or DC) from the power inputs to fully de-energize the hardware. **French Translation:** (Tous les appareils Palo Alto Networks avec au moins deux sources d'alimentation) Débranchez tous les cordons d'alimentation (c.a. ou c.c.) des entrées d'alimentation et mettez le matériel hors tension.
• 	(PA-450R and PA-450R-5G firewalls only) Caution: Hot surface Hardware components are hot and can cause burnt hands and fingers. Wait at least one-half hour after switching power off to handle the hardware.
• 	(PA-7000 Series firewalls only) Caution: High touch current Connect to earth before connecting to the power supply. Ensure that the protective earthing conductor is connected to the provided ground lug on the rear side of the firewall.
• 	(PA-7000 Series firewalls only) When removing a fan tray from a PA-7000 Series firewall, first pull the fan tray out about 1 inch (2.5cm) and then wait a minimum of 10 seconds before extracting the entire fan tray. This allows the fans to stop spinning and helps you avoid serious injury when removing the fan tray. You can replace a fan tray while the firewall is powered on but you must replace it within 45 seconds and you can only replace one fan tray at a time to prevent the thermal protection circuit from shutting down the firewall. **French Translation:** (Pare-feu PA-7000 uniquement) Lors du retrait d'un tiroir de ventilation d'un pare-

	feu PA-7000, retirez tout d'abord le tiroir sur 2,5 cm, puis patientez au moins 10 secondes avant de retirer complètement le tiroir de ventilation. Cela permet aux ventilateurs d'arrêter de tourner et permet d'éviter des blessures graves lors du retrait du tiroir. Vous pouvez remplacer un tiroir de ventilation lors de la mise sous tension du pare-feu. Toutefois, vous devez le faire dans les 45 secondes et vous ne pouvez remplacer qu'un tiroir à la fois, sinon le circuit de protection thermique arrêtera le pare-feu.

The following applies only to Palo Alto Networks firewalls that support a direct current (DC) power source:

French Translation: Les instructions suivantes s'appliquent uniquement aux pare-feux de Palo Alto Networks prenant en charge une source d'alimentation en courant continu (c.c.):

- 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.

PA-3400 Series Firewall Overview

The Palo Alto Networks® PA-3400 Series next-generation firewalls are designed for data center and internet gateway deployments. This series is comprised of the PA-3410, PA-3420, PA-3430, and PA-3440 firewalls. These models provide flexibility in performance and redundancy to help you meet your deployment requirements. Some features include UEFI secure boot support, power redundancy, Multi-Gig ports, and a TPM module for PAN-OS key storage and security. All models in this series provide next-generation security features to help you secure your organization through advanced visibility and control of applications, users, and content.

First Supported Software Release: PAN-OS® 10.2

The following topics describe the hardware features of PA-3400 Series firewalls. To view or compare performance and capacity information, refer to the Product Selection tool.

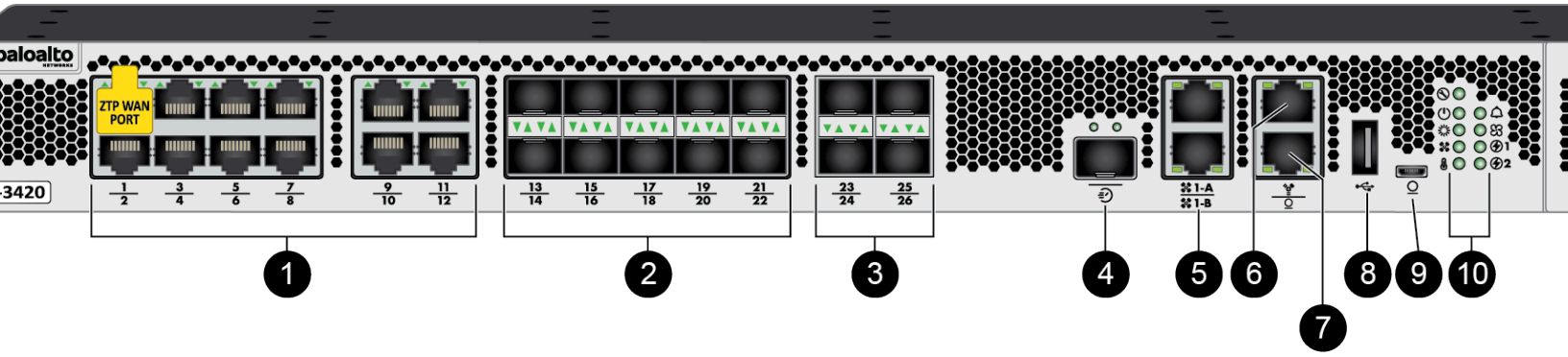
PA-3400 Series Front Panel

View the front panel components of your PA-3400 Series firewall.

- PA-3410 and PA-3420
- PA-3430 and PA-3440

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-3410 and PA-3420 firewalls and the table describes each front panel component.



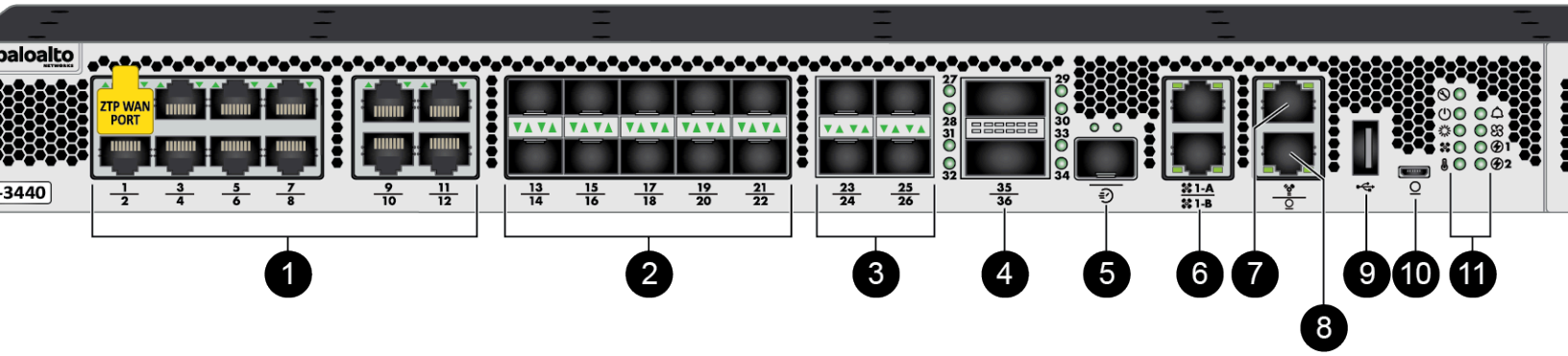
Item	Component	Description
1	Ethernet ports 1 through 12	Twelve RJ-45 10Mbps/100Mbps/1Gbps/2.5Gbps/5Gbps/10Gbps ports for network traffic. Port 1 is a Zero Touch Provisioning (ZTP) port. The ZTP port can be used to automate the on-boarding of new firewalls to a Panorama management server. To use the ZTP port, read how to boot the firewall in ZTP mode.
2	SFP ports 13 through 22	Ports 13 through 22 are SFP (1Gbps) or SFP+ (10Gbps) based on the installed transceiver. *The SFP ports can be remapped as HA-1 ports via PAN-OS or Panorama. These remapped HA-1 ports offer high availability connectivity over a longer distance than what is permitted by the HA1-A and HA1-B ports listed below.*

Item	Component	Description
3	SFP28 ports 23 through 26	Four SFP28 (25Gbps) ports that also support 1G SFP and 10G SFP+ modules. These ports support RS-FEC. *The FEC setting of the remote endpoint must be set to RS-514 or RS-528 per the IEEE standards to ensure that the link remains up.*
4	HSCI port	One SFP+ (10Gbps) port (supports both SFP and SFP+ transceivers or cables). Use this port to connect two PA-3400 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-3400 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.*
5	HA1-A and HA1-B ports	Two RJ-45 10Mbps/100Mbps/1000Mbps ports for high availability (HA) control.
6	MGT port	Use this Ethernet 10Mbps/100Mbps/1000Mbps port to access the management web interface and perform administrative tasks. The firewall also uses this port for management services, such

Item	Component	Description
		as retrieving licenses and updating threat and application signatures. *The management interface cannot be configured as a HA port.*
7	CONSOLE port (RJ-45)	Use this port to connect a management computer to the firewall using a 9-pin serial-to-RJ-45 cable and terminal emulation software. The console connection provides access to firewall boot messages, the Maintenance Recovery Tool (MRT), and the command line interface (CLI). *If your management computer does not have a serial port, use a USB-to-serial converter.* Use the following settings to configure your terminal emulation software to connect to the console port: • Data rate: 9600 • Data bits: 8 • Parity: None • Stop bits: 1 • Flow control: None
8	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.
9	CONSOLE port (Micro USB)	Use this port to connect a management computer to the firewall using a standard Type-A USB-to-micro USB cable. The console connection provides access to firewall boot messages, the Maintenance Recovery Tool (MRT), and the command line interface (CLI).
10	LED status indicators	Eight LEDs that indicate the status of the firewall hardware components (see Interpret the PA-3400 Series Status LEDs).

Item	Component	Description
11	System Drive Cover	Secures the device SSD.

The following image shows the front panel of the PA-3430 and PA-3440 firewalls and the table describes each front panel component.



Item	Component	Description
1	Ethernet ports 1 through 12	Twelve RJ-45 10Mbps/100Mbps/1Gbps/2.5Gbps/5Gbps/10Gbps ports for network traffic. Port 1 is a Zero Touch Provisioning (ZTP) port. The ZTP port can be used to automate the on-boarding of new firewalls to a Panorama management server. To use the ZTP port, read how to boot the firewall in ZTP mode.
2	SFP ports 13 through 22	Ports 13 through 22 are SFP (1Gbps) or SFP+ (10Gbps) based on the installed transceiver. *The SFP ports can be remapped as HA-1 ports via PAN-OS or Panorama. These remapped HA-1 ports offer high availability connectivity over a longer distance than what is permitted by the HA1-A and HA1-B ports listed below.*
3	SFP28 ports 23 through 26	Four SFP28 (25Gbps) ports that also support 1G SFP and 10G SFP+ modules. These ports support RS-FEC.

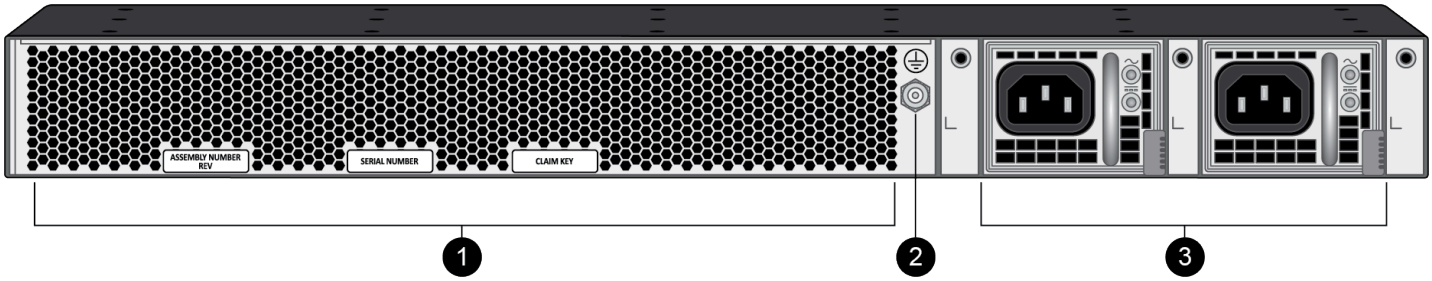
Item	Component	Description
		The FEC setting of the remote endpoint must be set to RS-514 or RS-528 per the IEEE standards to ensure that the link remains up.
4	QSFP28 ports 27 through 36	Two form-factor pluggable (QSFP+/QSFP28) 40Gbps/100Gbps Ethernet ports. These ports support RS-FEC. Each interface supports breakout mode to create four 10Gbps or four 25Gbps ports each. • Ports 27, 28, 29, and 30 break out from port 35 • Ports 31, 32, 33, and 34 break out from port 36 *The FEC setting of the remote endpoint must be set to RS-514 or RS-528 per the IEEE standards to ensure that the link remains up.* *RS-FEC is enabled for most transceiver modules. The exceptions are LR4, AOC v2, and BiDi transceivers.*
5	HSCI port	One SFP+ (10Gbps) port (supports only an SFP+ transceiver or passive SFP+ cable). Use this port to connect two PA-3400 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-3400 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.*
6	HA1-A and HA1-B ports	Two RJ-45 10Mbps/100Mbps/1000Mbps ports for high availability (HA) control.
7	MGT port	Use this Ethernet 10Mbps/100Mbps/1000Mbps port to access the management web interface and perform administrative tasks. The firewall also uses this port for management services, such as retrieving licenses and updating threat and application signatures. *The management interface cannot be configured as a HA port.*
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: 9600 • Data bits: 8

Item	Component	Description
		• Parity: None • Stop bits: 1 • Flow control: None
9	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.
10	CONSOLE port (Micro USB)	Use this port to connect a management computer to the firewall using a standard Type-A USB-to-micro USB cable. The console connection provides access to firewall boot messages, the Maintenance Recovery Tool (MRT), and the command line interface (CLI).
11	LED status indicators	Nine LEDs that indicate the status of the firewall hardware components (see Interpret the PA-3400 Series Status LEDs).
12	System Drive Cover	Secures the device SSD.

PA-3400 Series Back Panel

The following image shows the back panel of the PA-3400 Series firewall and the table describes each back-panel component. The PA-3410, PA-3420, PA-3430, and PA-3440 back-panel components are identical.



Item	Component	Description
1	Fan assemblies	Provides ventilation and cooling for the firewall. *The fans are not field replaceable.*
2	Ground stud	Use the single post ground stud to connect the firewall to earth ground (ground cable not included).
3	PS1 and PS2	Use the power supply inputs to connect AC or DC power to the firewall. The second power supply is for redundancy. When facing the back of the firewall, PS1 is on the right and PS2 is on the left.

Install the PA-3400 Series Firewall in an Equipment Rack

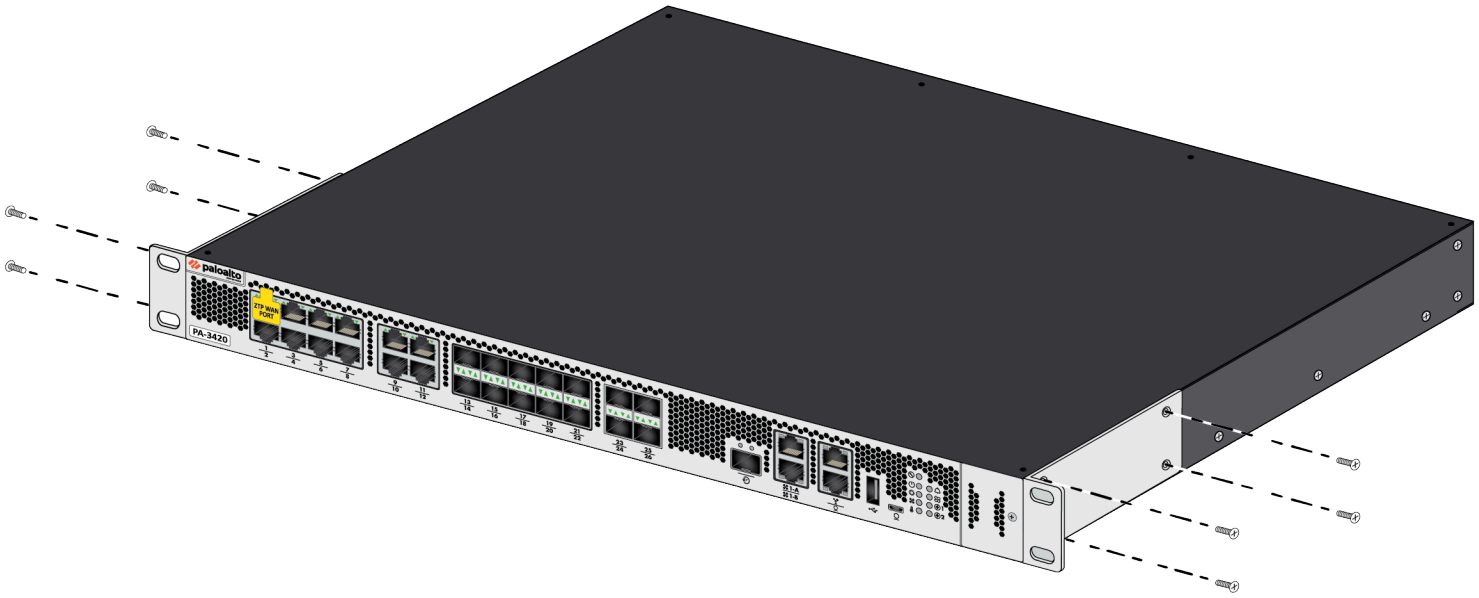
The PA-3400 Series next-generation firewall ships with rack-mount brackets for installation in a four-post 19” equipment rack.

- Install the PA-3400 Series Firewall Using the Four-Post Rack Kit

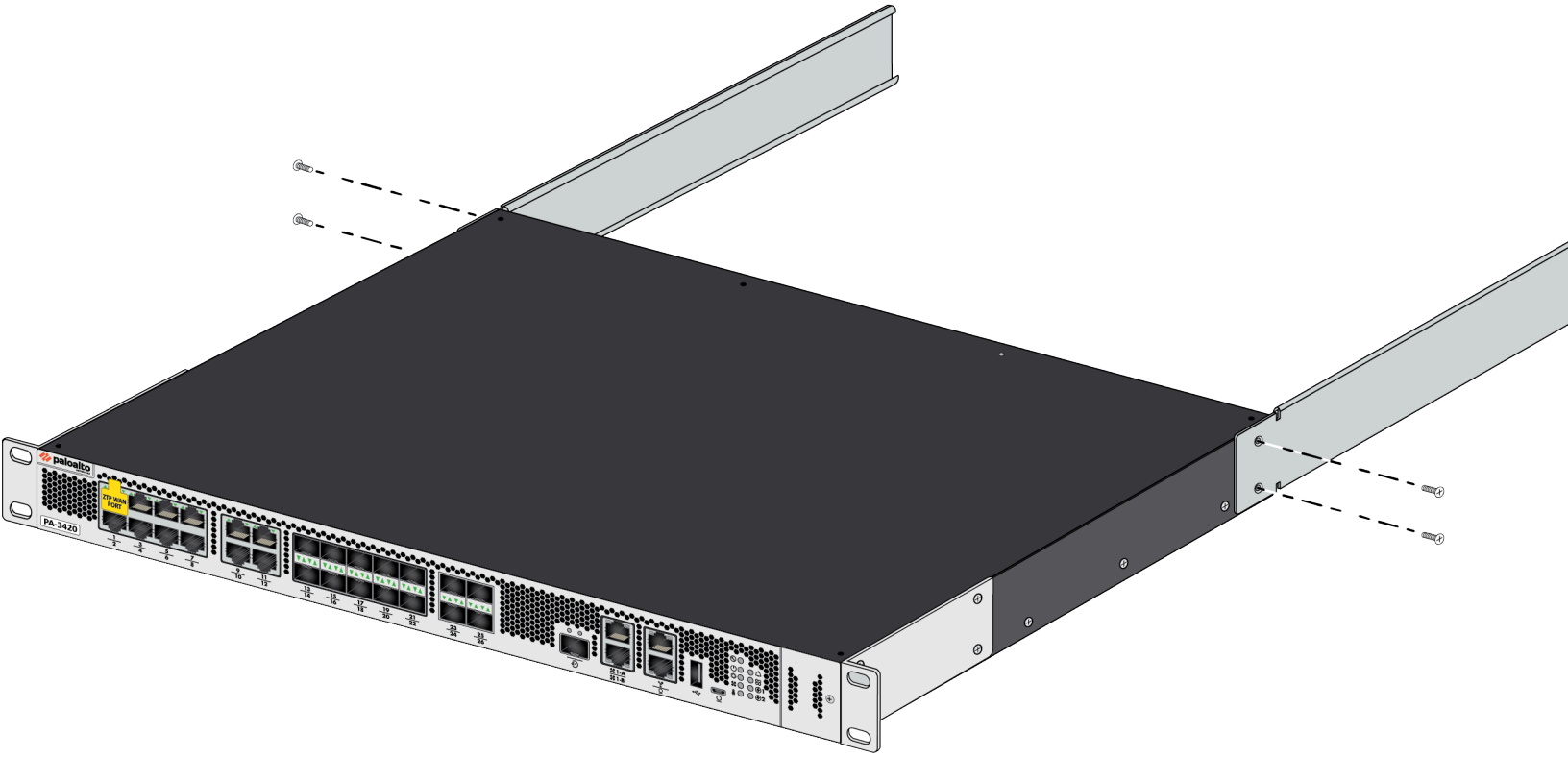
Install the PA-3400 Series Firewall Using the Four-Post Rack Kit

The following procedure describes how to install the PA-3400 Series firewall in a 19” four-post equipment rack using the four-post rack kit (PAN-PA-3400-RACK4).

STEP 1 | Attach one rack-mount bracket to each side of the firewall in the front-mount position using four #6-32 x 5/16” screws for each bracket and torque to 9 in-lbs.

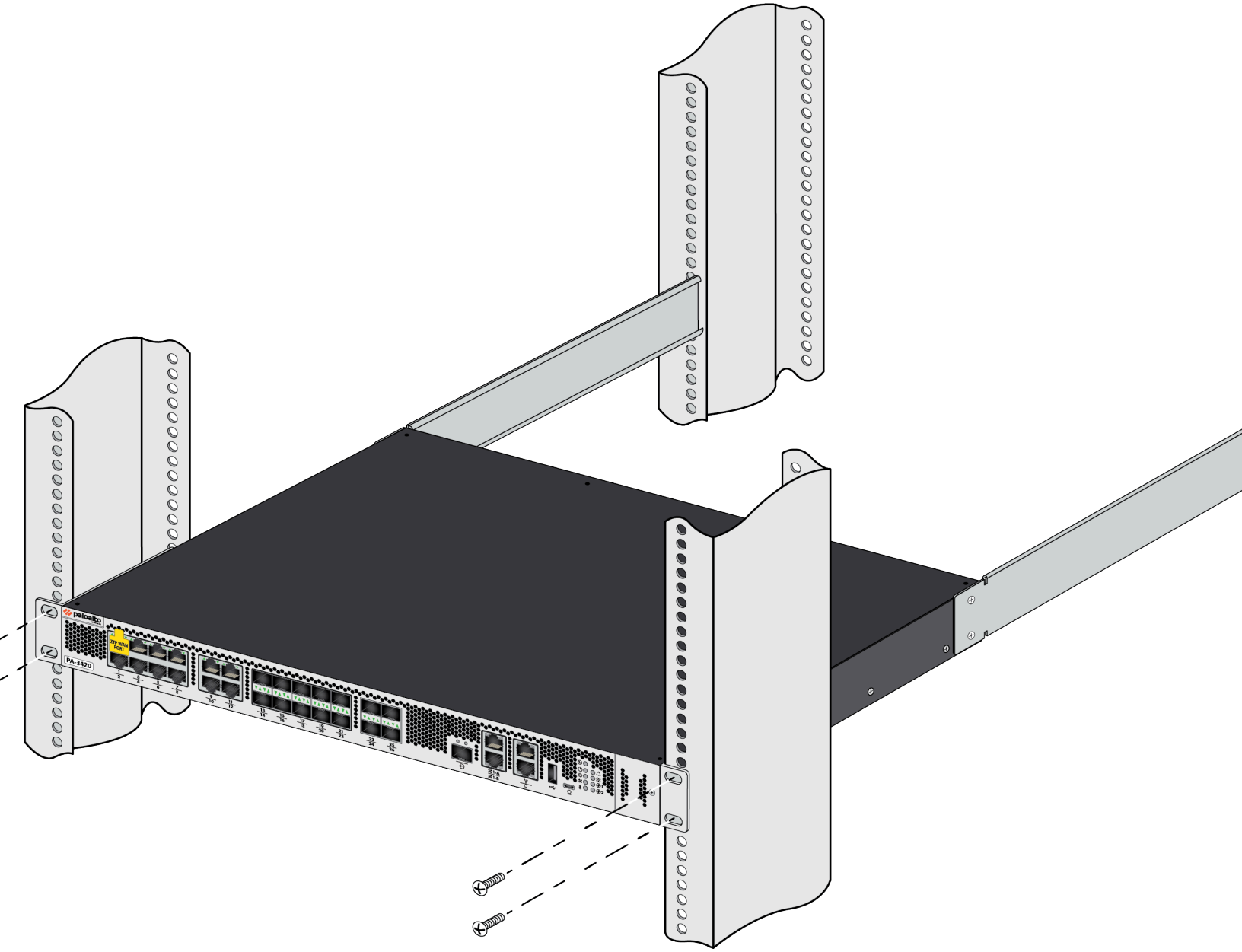


STEP 2 | Attach one rack-mount rail to each side of the firewall using two #6-32 x 5/16” screws for each rail and torque to 9 in-lbs.

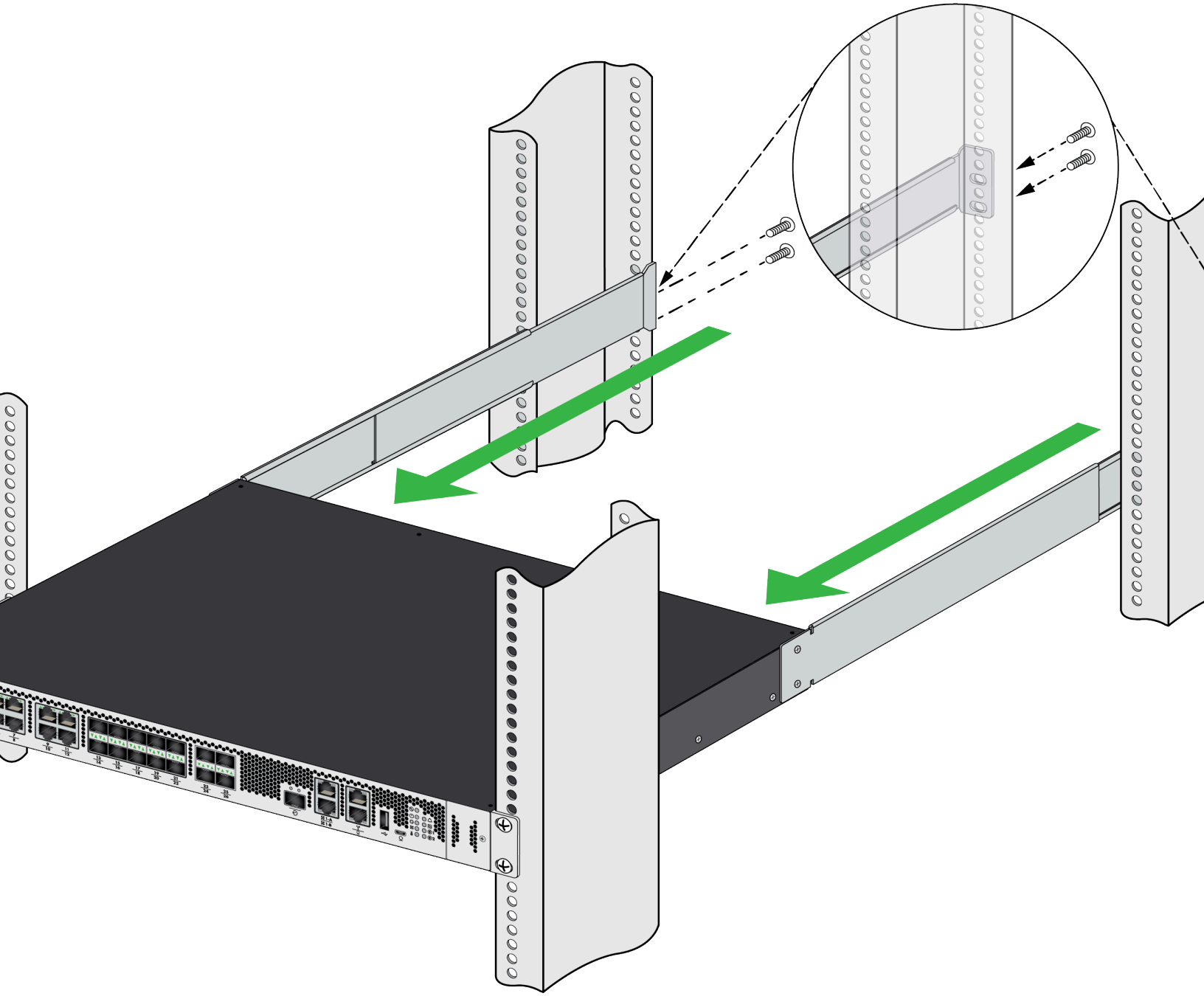


STEP 3 | With help from another person, hold the firewall in the rack and secure the front rack-mount brackets to the front rack-posts using two screws for each bracket. Use the appropriate

screws (#10-32 x 3/4” or #12-24 x 1/2”) for your rack and torque to 25 in-lbs. Use cage nuts to secure the screws if the rack has square holes.



STEP 4 | Slide one back rack-mount bracket into each of the two previously installed side rack-mount rails and secure the brackets to the back rack-posts using the appropriate screws for your rack (#10-32 x 3/4” or #12-24 x 1/2”) and torque to 25 in-lbs.



Connect Power to a PA-3400 Series Firewall

PA-3400 Series firewalls have two AC or DC power supplies (the second power supply is for redundancy). Before you connect power, read the PA-3400 Series Electrical Specifications.

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.

You cannot use a combination of AC and DC power supplies to power the same device.

- Connect AC Power to a PA-3400 Series Firewall
- Connect DC Power to a PA-3400 Series Firewall

Set Up a Connection to the Firewall

On first startup, the PA-3400 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-3400 Series firewall online in standard mode. See the instructions below to learn how to boot in ZTP or standard mode.

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

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

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

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

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

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

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

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

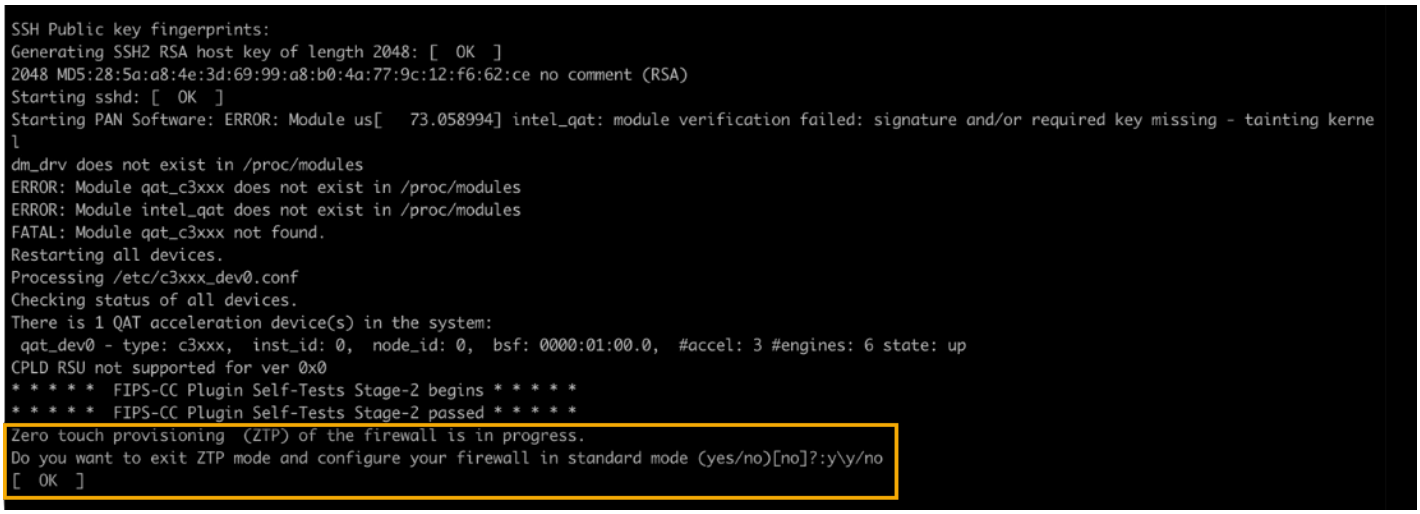
STEP 3 | (Standard mode only) If you intend to boot the firewall in standard mode, you will need access to the firewall CLI to respond to a prompt during bootup. Connect a console cable from the PA-3400 Series firewall to your computer. Once the firewall is powered on, use a terminal emulator such as PuTTY to access the CLI. See Access the CLI for more information.

STEP 4 | Power on the firewall. See Connect Power to a PA-3400 Series Firewall to learn how to connect power to the firewall.

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

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

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



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

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

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

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

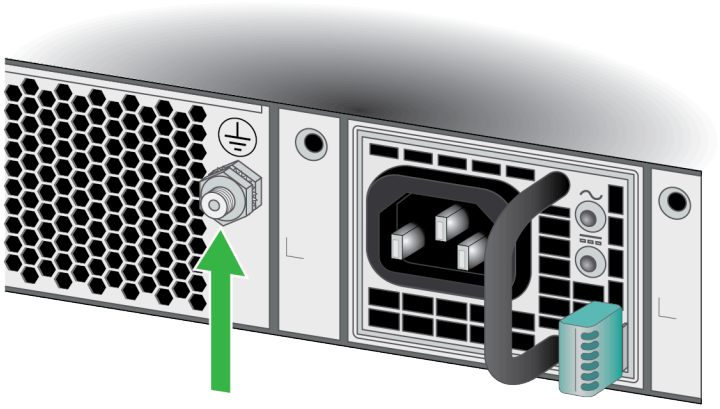
Connect AC Power to a PA-3400 Series Firewall

The following procedure describes how to connect AC power to a PA-3400 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 | Remove the nut and star washer from the ground stud on the back of the firewall.

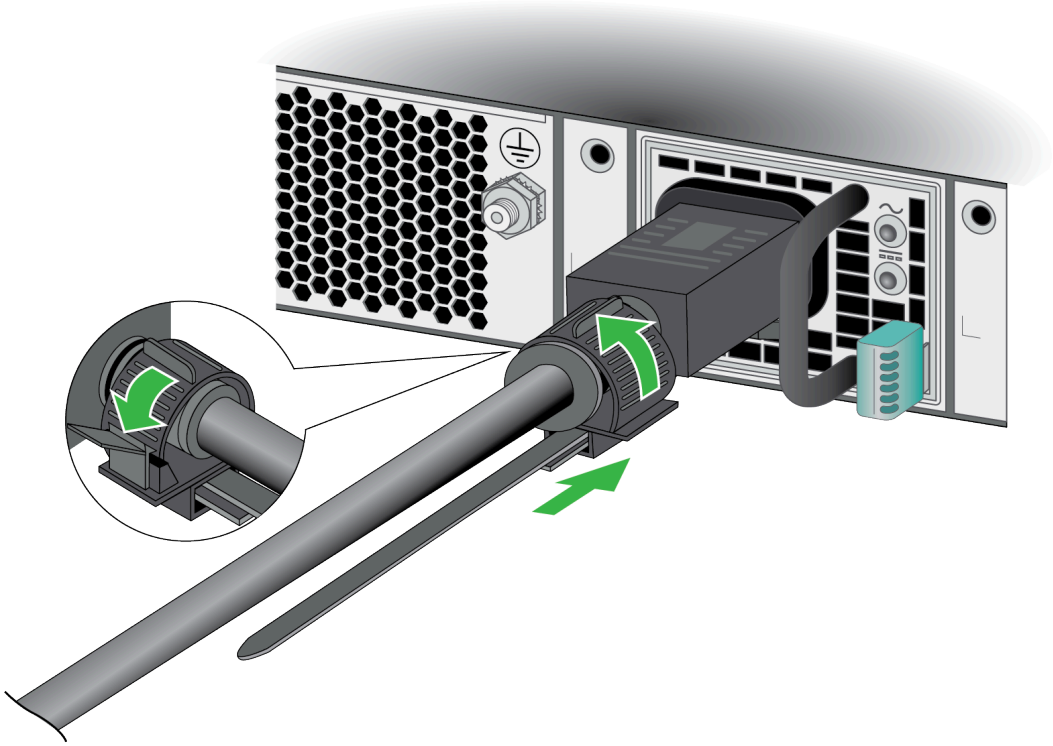


STEP 2 | Crimp a 14AWG ground cable to a ring lug (cable and lug not included) and then attach the ring lug to the ground stud on the firewall. Replace the star washers and nuts and torque to 25 in-lbs. Connect the other end of the cable to earth ground.

STEP 3 | Connect the AC power cord to the power input on the back of the firewall.

STEP 4 | Secure the power cords to the power supplies using the provided cord retainer.

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



STEP 5 | Connect the other end of the power cords to an AC power source. After the power supply is connected, the power supply powers on, the input and output LEDs on the power supply turn green, and the PWR LED and the power supply LED (PWR 1 or PWR 2) on the front of the firewall turns green.

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

Connect DC Power to a PA-3400 Series Firewall

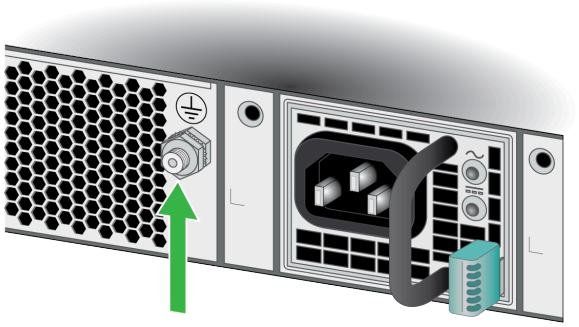
The following procedure describes how to connect DC power to a PA-3400 Series firewall with DC power supplies.

You must swap the AC power supplies with DC power supplies prior to performing this procedure.

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 | Remove the nut and star washer from the ground stud on the back of the firewall.



STEP 2 | Crimp a 14AWG ground cable to a ring lug (cable and lug not included) and then attach the ring lug to the ground stud on the firewall. Replace the star washers and nuts and torque to 25 in-lbs. Connect the other end of the cable to earth ground.

Power off the DC power sources that you will connect to the power supplies before you continue to the next step.

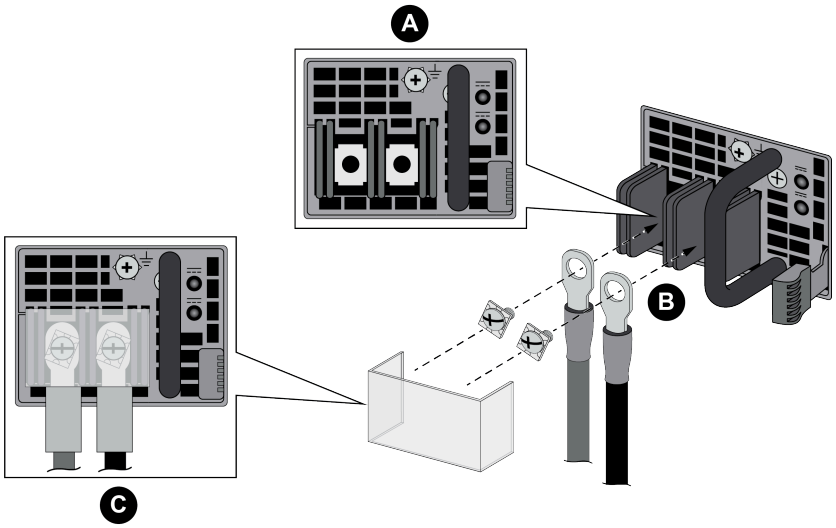
STEP 3 | Attach the DC power cables (not included) from the DC power source to the DC power supplies on the back of the firewall.

1. Remove the plastic DC power input cover from each of the two DC power supplies and then remove the positive and negative terminal screws.
2. Crimp ring lugs to the ends of the positive and negative DC cables. These lugs are used to connect the DC cables to the DC inputs on the firewall.
3. Use the DC terminal screws to connect a positive DC power cable to the positive terminal on the first DC power supply and then connect a negative DC power cable to

the negative terminal. Repeat this step for the second DC power supply using separate positive and negative cables.

4. Replace the plastic covers over each DC power input.
5. Connect the two positive and two negative DC power cables to your power sources and ensure that you observe the correct polarity (positive to positive and negative to negative).

Connect the second set of power cables through a different DC circuit to provide power redundancy and to allow for electrical circuit maintenance.



STEP 4 | After all DC power cables are securely connected, power on the DC power sources. The power supplies powers on, the input and output LEDs on the power supplies turn green, and the PWR LED and the power supply LEDs (PWR 1 and PWR 2) on the front of the firewall turns green.

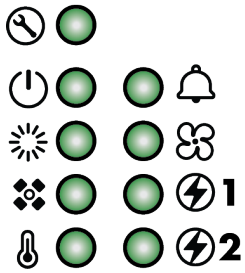
Service the PA-3400 Series Firewall

The following topics describe how to interpret the PA-3400 Series firewall status LEDs and how to replace the serviceable components.

- Interpret the PA-3400 Series Status LEDs
- Replace a PA-3400 Series Power Supply
- Replace a PA-3400 Series Drive

Interpret the PA-3400 Series Status LEDs

The following table describes how to interpret the status LEDs on a PA-3400 Series firewall.



LED	Description
Front Panel LEDs	
	Service • **Off**—The firewall is operating normally. • **Blue**—The firewall is instructed by the CLI or Web Interface to enable this LED.
	Power • **Green**—The firewall is powered on. • **Off**—The firewall is not powered on or an error occurred with the internal power system (for example, power is not within tolerance levels).
	Status • **Green**—The firewall is operating normally. • **Yellow**—The firewall is booting.
	High Availability • **Green**—The firewall is the active peer in an active/passive configuration. • **Yellow**—The firewall is the passive peer in an active/passive configuration. • **Off**—High availability (HA) is not operational on this firewall.

LED	Description
	In an active/active configuration, the HA LED only indicates HA status for the local firewall and has two possible states (green or off); it does not indicate HA connectivity of the peer. Green indicates that the firewall is either active-primary or active-secondary and off indicates that the firewall is in any other state (For example, non-functional or suspended).
	**Temperature** • **Green**—The firewall temperature is normal. • **Yellow**—The firewall temperature is outside tolerance levels. See the PA-3400 Series Environmental Specifications for the operating temperature range.
	**Alarm** • **Red**—A hardware failure, such as a power supply failure, a firewall failure that caused an HA failover, a drive failure, or the hardware overheated and exceeded the high temperature threshold. • **Off**—The firewall is operating normally.
	**Fans** • **Green**—The fan tray and all fans are operating normally. • **Red**—A fan failed. If one of the three fans fail, the firewall will continue to operate but if two fans fail, the firewall will shut down.
	**Power Supplies 1 and 2** When facing the back of the firewall, power supply 1 (PS1) is on the right and power supply 2 (PS2) is on the left. • **Green**—The power supply is operating normally. • **Red**—The power supply is present but is not working.
Ethernet Port LEDs	
RJ-45	These ports have two green LEDs each. • **Solid Green**—The firewall network link is up. • **Blinking Green**—The firewall is processing network activity.
SFP, SFP+, SFP28, QSFP+ and QSFP28 LEDs	The SFP, SFP+ and SFP28 ports have two LEDs each; the LED illuminated depends on the transceiver that is installed. The QSFP+ and QSFP28 ports have four LEDs each.

LED	Description
	On the SFP/SFP+/SFP28 ports, the left LED glows yellow when a 1G transceiver is connected and the right LED glows green when a 10G transceiver is connected. When operating at 25G speed, the right LED glows teal. *On the QSFP28 ports, the LEDs are illuminated based on breakout status. Breaking out the port to 10G causes all LEDs to glow green. Breaking out the port to 25G causes all LEDs to glow teal.* *If the port is not broken out, the LEDs glow yellow for 40G and blue for 100G.* The color of the LED differs based on the port speed. 1G—Yellow 10G—Green 25G—Teal 40G—Yellow 100G—Blue • **Solid Color**—The firewall network link is up. • **Blinking Color**—The firewall is processing network activity. *There is a slight difference in the shade of green used by the LEDs of Ports 1-22 and the LEDs of Ports 23-36.*
Back Panel LEDs	

Power supply LEDs	The top LED provides status of the power input and the bottom LED provides status of the power supply output.
	• **Input LED (Top)**
	  • **Solid green**—Input voltage operating within the normal specified range.
	  • **Blinking green**—Overvoltage or undervoltage warning.
	  • **Off**—Exceeded the overvoltage or undervoltage threshold or no input power.

LED	Description

	• **Output LED (Bottom)**
	  • **Solid green**—Main output and standby output enabled; no power supply warnings or faults.
	  • **Blinking green**—Standby output enabled with no power supply warning or fault detected.
	  • **Blinking yellow**—Power supply warning detected.
	  • **Solid yellow**—Power supply fault detected.

Fan tray LED	• **Green**—All fans are operating normally. • **Red**—A fan has failed.

Replace a PA-3400 Series Power Supply

PA-3400 Series firewalls have two AC or DC power supplies (the second power supply is for redundancy). If one power supply fails, you can replace it without service interruption as described in the following procedure.

- Replace a PA-3400 Series Power Supply

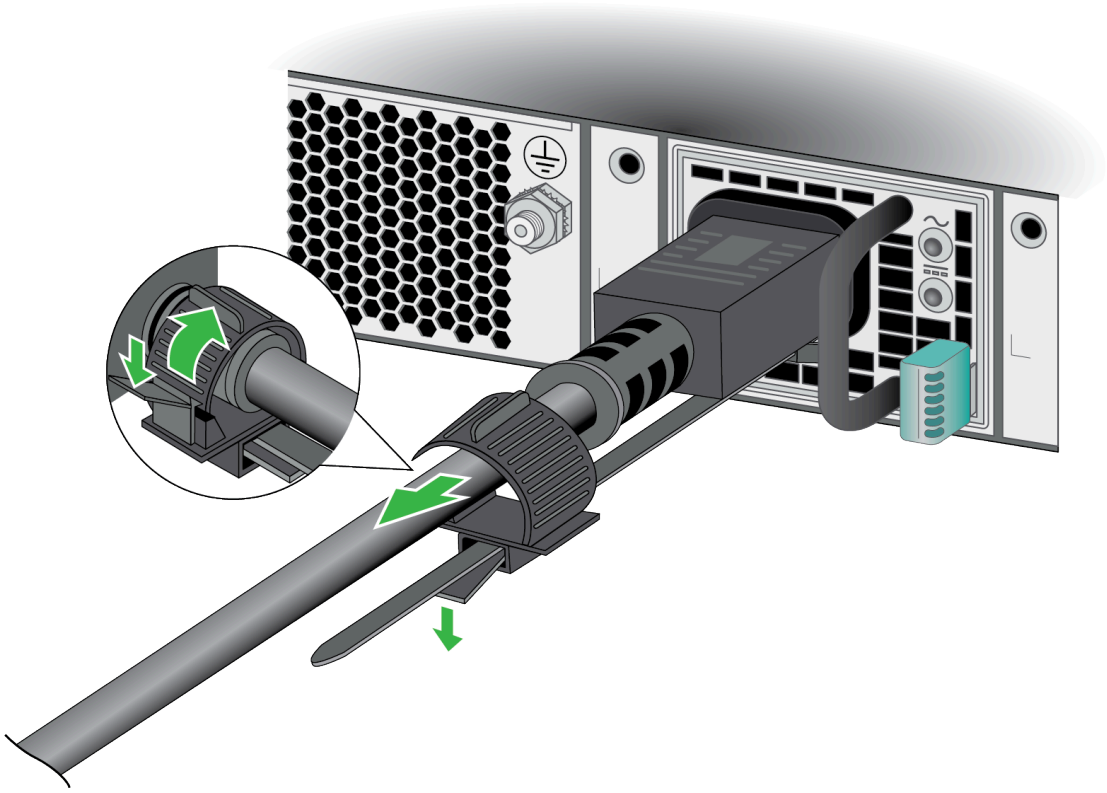
Replace a PA-3400 Series Power Supply

The following procedure describes how to replace a PA-3400 Series power supply.

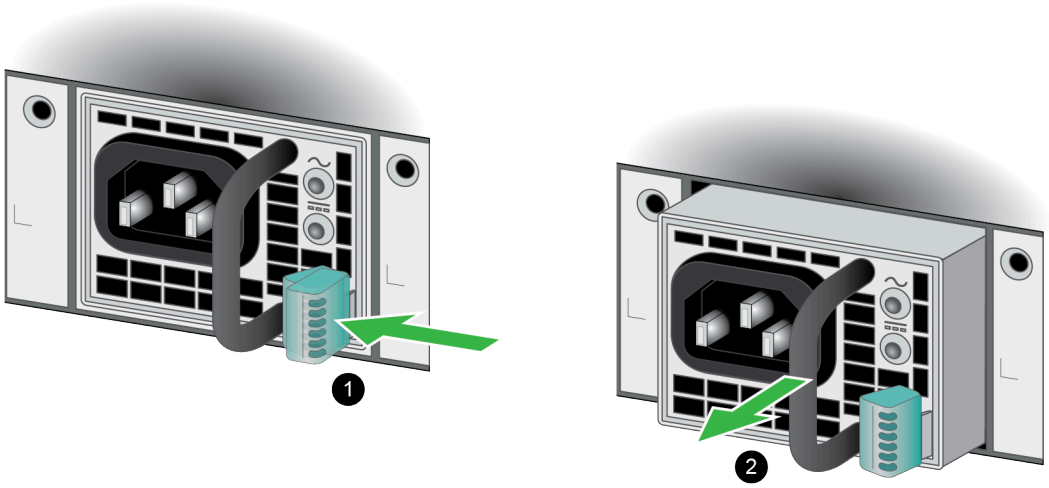
To avoid injury to yourself or damage to your Palo Alto Networks® hardware or the data that resides on the hardware, read the Product Safety Warnings.

STEP 1 | Identify the failed power supply by viewing the **System** logs or by viewing the power supply status LEDs described in Interpret the PA-3400 Series Status LEDs.

STEP 2 | Remove the cord retainer that secures the power cord to the failed power supply and disconnect the power cord from the firewall.



STEP 3 | Grasp the handle on the failed power supply and then simultaneously press the release lever to the left and pull the power supply outward to remove it.



STEP 4 | Remove the replacement power supply from the packaging and slide it into the empty power supply slot. Push the power supply all the way in until the release lever clicks and secures the power supply.

STEP 5 | Connect the AC or DC power cable(s) to the power supply input and secure it to the power supply using the cord retainer. Once the power supply powers on, the input and output LEDs on the power supply turn green. Similarly, the PWR LED and the power supply LED (PWR 1 or PWR 2) on the front of the firewall turn green.

Replace a PA-3400 Series Drive

The PA-3400 Series firewalls use a single solid-state drive (SSD) to store the PAN-OS system files, system logs, and network traffic logs. If this drive fails, you must replace it to restore functionality to the firewall.

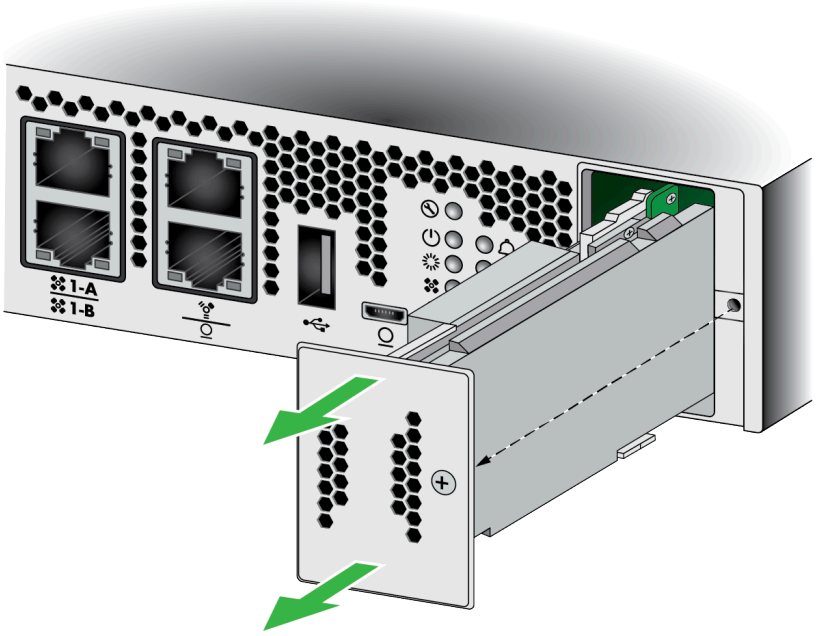
The replacement drive ships with a factory default PAN-OS image with the default configuration. After you install the new drive, you will need to obtain a backup configuration that you saved from the failed firewall to restore your configuration.

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

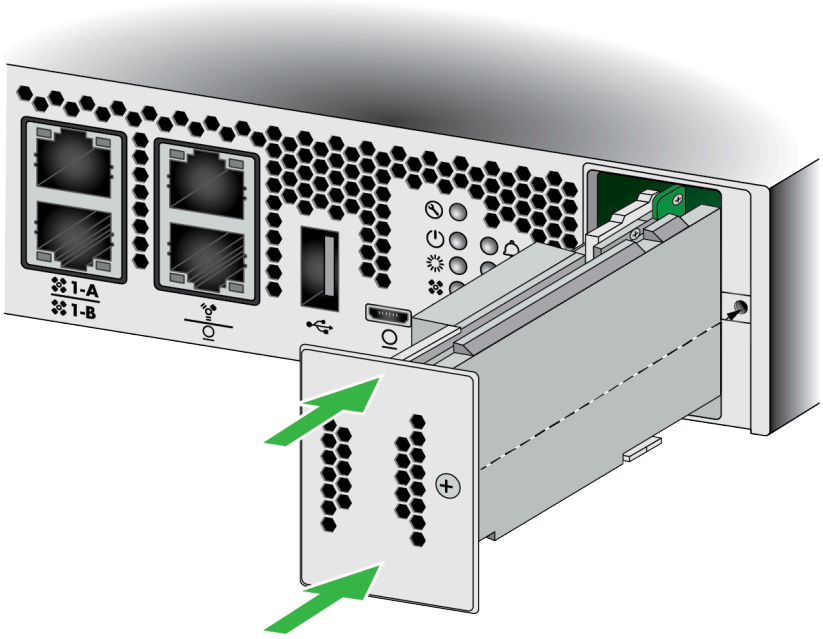
STEP 1 | Disconnect power from the firewall, then remove the power cable(s).

STEP 2 | Unscrew the captive screw on the system drive cover on the front side of the firewall. See PA-3400 Series Front Panel for help locating the system drive cover.

STEP 3 | Pull the SSD module out of the firewall.



STEP 4 | Slide the replacement SSD module onto the rails and gently push it into the firewall.



STEP 5 | Power on the firewall and connect a standard RJ-45 Ethernet cable from the RJ-45 port on your computer to the MGT port on the firewall.

STEP 6 | Change the IP address on your computer to an address in the 192.168.1.0/24 network, such as 192.168.1.2.

STEP 7 | From a web browser, go to https://192.168.1.1 and, when prompted, log in to the web interface using the default username and password (admin/admin).

STEP 8 | Configure management access and restore the firewall configuration.

For information on how to upgrade or downgrade PAN-OS, see the New Features Guide for the PAN-OS version that your firewall is running. The New Features Guides are located on the Technical Documentation portal.

PA-3400 Series Firewall Specifications

The following topics describe the PA-3400 Series firewall hardware specifications. For feature, capacity, and performance information, refer to the PA-3400 Series datasheet.

PA-3400 Series Physical Specifications

The following table describes PA-3400 Series firewall physical specifications.

Specification	Value
Rack units and dimensions	**Rack units**—1RU **Dimensions**—1.7” H x 14.23” D x 17.12” W (4.32 cm H x 36.14 cm D x 43.49 cm W) *The depth dimension includes hardware that protrudes from the back of the firewall.*
Weight	• **Firewall weight**—15.5 lbs (7.03 kg) • **Shipping weight**—25 lbs (11.34 kg)

PA-3400 Series Electrical Specifications

The following table describes PA-3400 Series firewall electrical specifications. The electrical specifications are the same for all models in the series.

Specification	Value
Power Supplies	Two load sharing 450W AC or DC power supplies. If one power supply fails, the second power supply provides full redundancy.
Input voltage	• **AC power supplies—**100 to 240VAC (50-60Hz) • **DC power supplies—**-48 to -60VDC
Power consumption	**PA-3410** • Maximum—170W • Average—133W **PA-3420** • Maximum—178W • Average—145W **PA-3430** • Maximum—185W • Average—150W **PA-3440** • Maximum—192W • Average—155W
Maximum current consumption	**AC power supplies—**2A@100VAC, 0.83A@240VAC **DC power supplies—**3.9A@-48VDC
Maximum inrush current	**AC power supplies—**25A

PA-3400 Series Environmental Specifications

The following table describes PA-3400 Series firewall environmental specifications.

Specification	Value
Operating temperature range	32°F to 104°F (0°C to 40°C)
Non-operating temperature	-4°F to 158°F (-20°C to 70°C)
Humidity tolerance (non-condensing)	**Operating and non-operating relative humidity**—10% to 90%
Airflow	Front-to-back
Maximum BTU/hr	819BTU/hr
Electromagnetic Interference (EMI)	FCC Class A, CE Class A, VCCI Class A
Acoustic noise	• **Average**—51 dB(A) • **Maximum**—65 dB(A)
Maximum operating altitude	10,000ft (3,048m)

PA-3400 Series Miscellaneous Specifications

The following table describes PA-3400 Series firewall miscellaneous specifications.

Specification	Value
Storage capacity	One 480GB SSD for system files and log storage.
Mean time between failures (MTBF)	22 years

PA-3400 Series Firewall Hardware Compliance Statements

Palo Alto Networks obtains regulatory compliance certifications to comply with the laws and regulations in each country where there are requirements applicable to our products. Our products meet standards for product safety and electromagnetic compatibility when used for their intended purpose.

To view compliance statements for the PA-3400 Series firewalls, see PA-3400 Series Firewall Compliance Statements.

PA-3400 Series Firewall Compliance Statements

The following are the PA-3400 Series firewall hardware compliance statements:

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

  The above product conforms with Low Voltage Directive 2014/35/EU and complies with the requirements relating to electrical equipment designed for use within certain voltage limits.
- **Federal Communications Commission (FCC) statement for a Class A digital device or peripheral**—This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
  - Reorient or relocate the receiving antenna.
  - Increase the separation between the equipment and receiver.
  - Connect the equipment to an outlet on a circuit that is different from the one to which the receiver is connected.
  - Consult the dealer or an experienced radio/TV technician for help.
- **ICES (Canadian Department Compliance Statement)**—This Class A digital apparatus complies with Canadian ICES-003.

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

  Risk of explosion if battery is replaced by an incorrect type. Dispose of used battery according to local regulations.

- **VCCI**—This section provides the compliance statement for the Voluntary Control Council for Interference by Information Technology Equipment (VCCI), which governs radio frequency emissions in Japan.

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

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

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

- **NBTC** (PA-3430 only) —This section provides the compliance statement for the National Broadcasting and Telecommunication Commission (NBTC), which governs radio frequency emissions in Thailand.

  เครื่องโทรคมนาคมและอุปกรณ์นี้มีความสอดคล้องตามมาตรฐานหรือข้อกำหนดทางเทคนิคของ กสทช
  (This telecommunication equipment conforms to the technical standards or requirements of NBTC.)

