paloalto TECHDOCS

PA-5400 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

Palo Alto Networks, Inc.
www.paloaltonetworks.com

© 2020-2026 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

March 6, 2026

Table of Contents

Before You Begin 5

Upgrade/Downgrade Considerations for Firewalls and Appliances 6
Tamper Proof Statement 7
Third-Party Component Support 8
Product Safety Warnings 9

PA-5400 Series Firewall Overview 13

PA-5400 Series Front and Back Panel Descriptions 14
PA-5400 Series Front Panel 14
PA-5400 Series Back Panel 17
PA-5450 Front and Back Panel Descriptions 20
PA-5450 Front Panel 20
PA-5450 Back Panel 21

PA-5400 Series Firewall Module and Interface Card Information 25

PA-5400 Series Firewall Base Card (BC) 26
PA-5400 BC-A 26
PA-5400 Series Firewall Management Processor Card (MPC) 27
PA-5400 MPC-A 27
PA-5400 Series Firewall Networking Card (NC) 33
PA-5400 NC-A 33
PA-5400 Series Firewall Data Processor Card (DPC) 37
PA-5400 DPC-A 37

PA-5400 Series Firewall Installation 41

PA-5400 Series Firewall Equipment Rack Installation 42
PA-5400 Series Firewall Rack Install Safety Information 42
Install the PA-5400 Series Firewall in an Equipment Rack 42
Install the PA-5450 Firewall in an Equipment Rack 45
Install the Mandatory PA-5400 Series Firewall Front Slot Cards 52
Install a PA-5400 Series Firewall Management Processor Card (MPC) 52
Install a PA-5400 Series Firewall Networking Card (NC) 53
Configure Session Distribution on a PA-5400 Series Firewall 55
Install a PA-5400 Series Firewall Data Processor Card (DPC) 55
Set Up a Connection to the Firewall 57
Connect Power to a PA-5400 Series Firewall 59
Connect AC or DC Power to a PA-5400 Series Firewall 59
Connect AC or DC Power to a PA-5450 Firewall 63
View PA-5400 Series Firewall Power Statistics 67

 ©2026 Palo Alto Networks, Inc.

Connect Cables to a PA-5400 Series Firewall....70
Verify the PA-5450 Firewall NC Configuration....72

Service the PA-5400 Series Firewall Hardware....75

Interpret the PA-5400 Series LEDs....76
Identify PA-5400 Series Port Activity and Link LEDs....80
Replace a PA-5400 Series Firewall AC or DC Power Supply....81
Interpret the PA-5400 Series Firewall Power Supply LEDs....81
Replace a PA-5400 Series Firewall AC or DC Power Supply....83
Replace a PA-5450 AC or DC Power Supply....84
Replace a PA-5400 Series Base Card (BC)....86
Replace a PA-5450 Base Card (BC)....86
Replace a PA-5400 Series Firewall Fan Assembly....88
Replace a PA-5400 Series Fan Assembly....88
Replace a PA-5450 Fan Assembly....90
Replace a PA-5400 Series Firewall Front Slot Card....93
Replace a PA-5400 Series Management Processor Card (MPC)....93
Replace a PA-5400 Series Networking Card (NC)....95
Replace a PA-5400 Series Data Processor Card (DPC)....98
PA-5450 Front Slot and Card States....99
PA-5450 Logical Card Slots....100
Replace a PA-5450 Front Slot Card in a High Availability (HA) Configuration....104
Install an MPC Logging Drive....107
Replace a System Drive....108
Replace a System Drive in a PA-5400 Series Firewall....108
Replace a System Drive in a PA-5450 MPC....111

PA-5400 Series Firewall Specifications....117

PA-5400 Series Firewall Physical Specifications....118
PA-5400 Series Firewall Electrical Specifications....120
PA-5450 Firewall Component Electrical Specifications....121
PA-5400 Series Firewall Power Cord Types....122
PA-5400 Series Firewall Environmental Specifications....124

PA-5400 Series Firewall Hardware Compliance Statements....125

PA-5400 Series Firewall Compliance Statements....126

 ©2026 Palo Alto Networks, Inc.

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
- Tamper Proof Statement
- Third-Party Component Support
- Product Safety Warnings

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.

 ©2026 Palo Alto Networks, Inc.

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.

 ©2026 Palo Alto Networks, Inc.

Third-Party Component Support

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

©2026 Palo Alto Networks, Inc.

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.

 ©2026 Palo Alto Networks, Inc.

- (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-

 ©2026 Palo Alto Networks, Inc.

	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.

 ©2026 Palo Alto Networks, Inc.

- Do not disconnect the firewall in the earthed circuit conductor between the DC source and the point of connection of the earthing electrode conductor.

  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.

 ©2026 Palo Alto Networks, Inc.

PA-5400 Series Firewall Overview

The PA-5400 Series firewalls (PA-5410, PA-5420, PA-5430, PA-5440, PA-5445, and PA-5450) are high performance appliances designed for large enterprise environments, data centers, and internet gateway deployments.

The PA-5410, PA-5420, PA-5430, PA-5440, and PA-5445 firewalls provide flexibility in performance and redundancy to adapt to your deployment requirements. Dedicated computing and hardware resources ensure predictable performance in networking, security, signature matching, and management functions.

The PA-5450 is a modular appliance that utilizes Networking Cards (NCs) and Data Processor Cards (DPCs) to scale network interfaces and data processing power as needed. In the PA-5450, you can install up to two NCs and four to five DPCs depending on your front slot configuration. These firewalls also feature a replaceable Base Card (BC) that interfaces with the signal connectors of the seven front slots, power supplies, and fan connections. Integrated with the BC is the Management Processor Card (MPC) that provides two logging ports, two management ports, and two HA1 ports for high availability deployments.

All PA-5400 Series firewalls can run on either AC or DC power and leverage redundancy. They also feature Multi-Gig ports, UEFI secure boot support, and a TPM module for PAN-OS key storage and security.

First Supported PAN-OS® Software Release:

- **PAN-OS 10.1.0**—PA-5450
- **PAN-OS 10.2.0**—PA-5410, PA-5420, and PA-5430
- **PAN-OS 11.0.0**—PA-5440
- **PAN-OS 11.1.0**—PA-5445

The following topics describe the hardware features of PA-5400 Series firewalls.

- PA-5400 Series Front and Back Panel Descriptions (PA-5410, PA-5420, PA-5430, PA-5440, and PA-5445)
- PA-5450 Front and Back Panel Descriptions

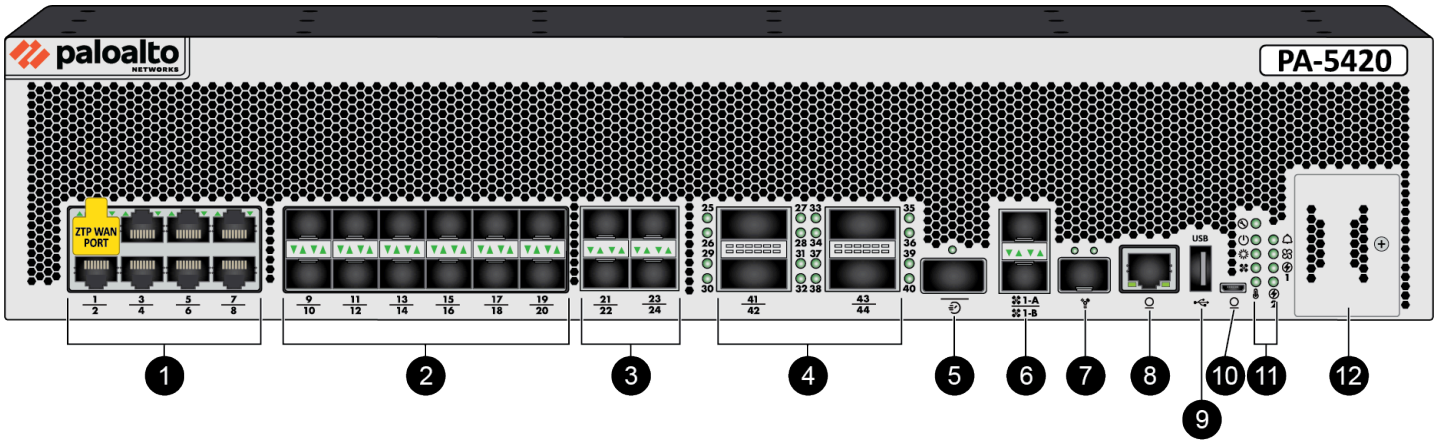
PA-5400 Series Front and Back Panel Descriptions

- PA-5400 Series Front Panel
- PA-5400 Series Back Panel

PA-5400 Series Front Panel

The following image shows the front panel of the PA-5410, PA-5420, PA-5430, PA-5440, and PA-5445 firewalls. The table describes each front panel component.

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



Item	Component	Description
1	Ethernet ports 1 through 8	Eight 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 9 through 20	Ports 9 through 20 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.*

©2026 Palo Alto Networks, Inc.

Item	Component	Description
3	SFP28 ports 21 through 24	Four SFP28 (25Gbps) ports that also support 1Gbps/SFP and 10Gbps/SFP+ modules. *The FEC setting of the remote endpoint must be set to RS-FEC to ensure that the link remains up.*
4	QSFP28 ports 25 through 44	Four form-factor pluggable (QSFP+/QSFP28) 40Gbps/100Gbps Ethernet ports. Each interface supports breakout mode to create four 10Gbps or four 25Gbps ports each. • Ports 25, 26, 27, and 28 break out from port 41 • Ports 29, 30, 31, and 32 break out from port 42 • Ports 33, 34, 35, and 36 break out from port 43 • Ports 37, 38, 39, and 40 break out from port 44 Refer to Interpret the PA-5400 Series LEDs to view the LED behavior of these ports. *Setting the interface speed to **auto** defaults the ports to breakout mode. Manually setting the interface speed allows you to use each individual port.*
5	HSCI port	One 40Gbps port that can be used to connect two PA-5400 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.

©2026 Palo Alto Networks, Inc.

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-5400 Series firewalls that are physically located near each other, Palo Alto Networks recommends that you use an active or passive QSFP+ cable. *For installations where the two firewalls are not near each other and you cannot use an active or passive QSFP+ cable, use a standard QSFP+ transceiver and the appropriate cable length.*
6	HA1-A and HA1-B ports	Two SFP+ 1Gbps/10Gbps 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	MGT port	Use this SFP+ 1Gbps/10Gbps 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 port supports copper and fiber SFP/SFP+ transceivers for 1G connectivity. For 10G connectivity, the management port only supports fiber SFP/SFP + transceivers.* *The Management port cannot be used to configure HA1 or HA1 backup. You must use the dedicated HA1-A and HA1-B ports.*
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.

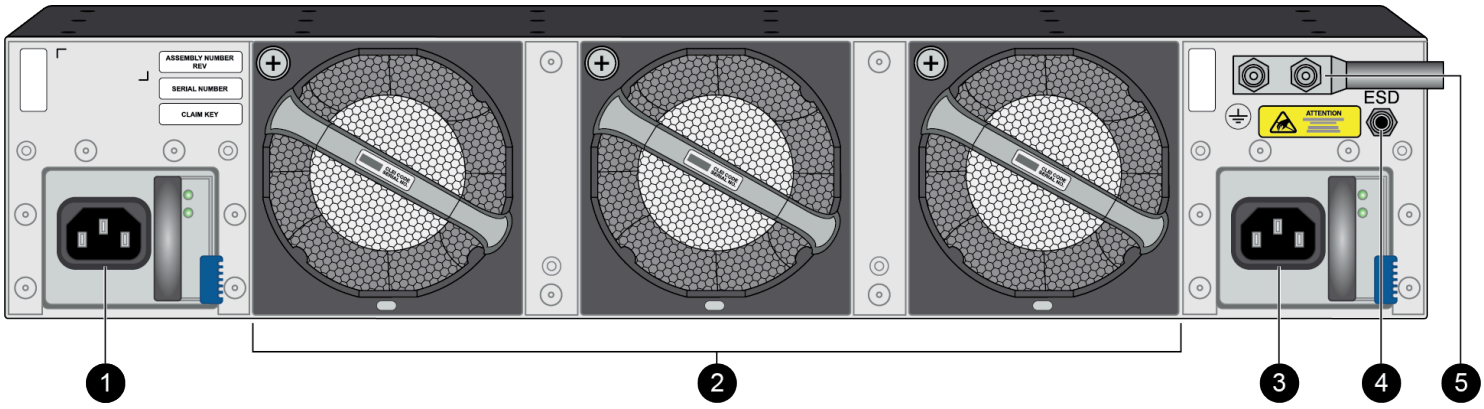
©2026 Palo Alto Networks, Inc.

Item	Component	Description
		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
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). Refer to the Micro USB Console Port page for more information and to download the Windows driver or to learn how to connect from a Mac or Linux computer.
11	LED status indicators	Eight LEDs that indicate the status of the firewall hardware components (see Interpret the PA-5400 Series LEDs).
12	System Drive Module	Secures the device SSDs.

PA-5400 Series Back Panel

The following image shows the back panel of the PA-5410, PA-5420, PA-5430, PA-5440, and PA-5445 firewalls. The table describes each back panel component.

©2026 Palo Alto Networks, Inc.



Item	Component	Description
1	Power Supply (PWR1)	Provide AC or DC power to the appliance. A minimum of one power supply is required, while an additional power supply can be installed to help load share and provide redundancy. *The AC power supplies have C14 inlets and support power cords with C13 connectors.* For information on connecting power to the appliance, see Connect Power to a PA-5400 Series Firewall.
2	Fan Assemblies	Provide the appliance with cooling and ventilation. There are three dual-rotor fan assemblies that can be individually replaced. For information on replacing or installing a fan, see Replace a PA-5400 Series Fan Assembly.
3	Power Supply (PWR2)	Provide AC or DC power to the appliance. A minimum of one power supply is required, while an additional power supply can be installed to help load share and provide redundancy. *The AC power supplies have C14 inlets and support power cords with C13 connectors.* For information on connecting power to the appliance, see Connect Power to a PA-5400 Series Firewall.
4	Electrostatic Discharge (ESD) port	Provides a grounding point that you use when removing or installing appliance components. Secure the provided wrist strap end of the ESD strap around your wrist and plug the other end into the ESD port.

©2026 Palo Alto Networks, Inc.

Item	Component	Description
5	Ground stud	Two-post stud used to ground the appliance to earth ground. Use the provided 6 AWG four#post ground lug to connect a grounded cable to the four#post stud.

©2026 Palo Alto Networks, Inc.

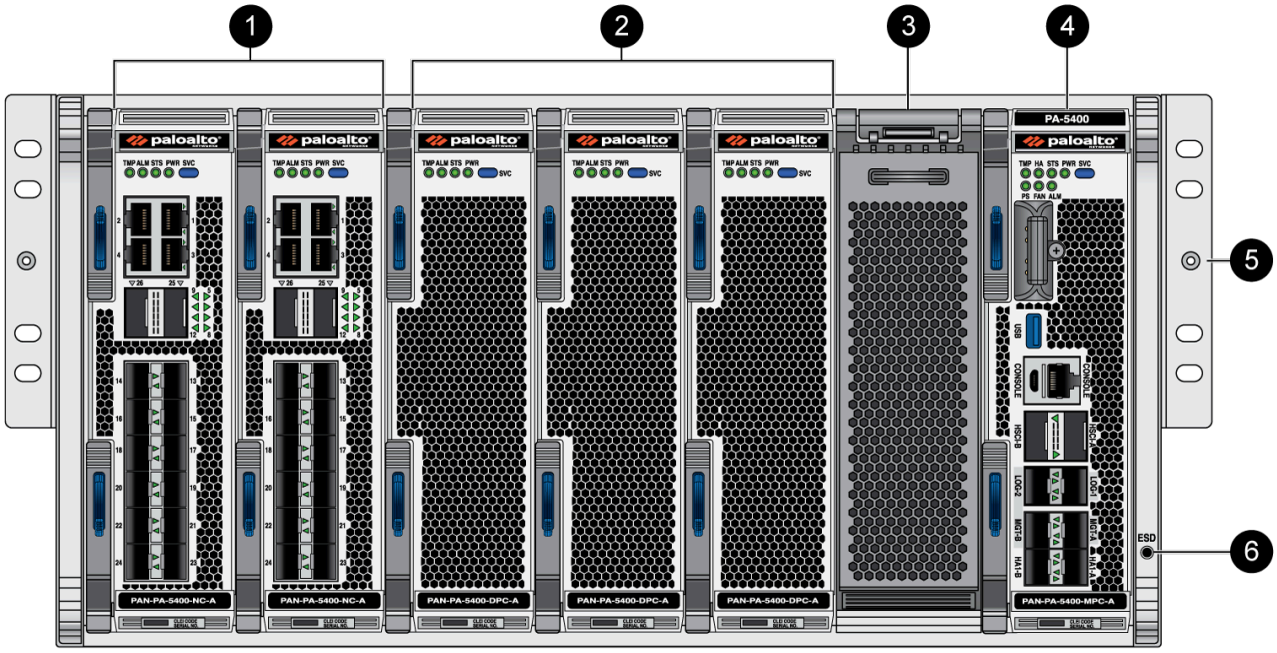
PA-5450 Front and Back Panel Descriptions

- PA-5450 Front Panel
- PA-5450 Back Panel

PA-5450 Front Panel

The following image shows the front panel of the PA-5450 firewall and the table describes each front panel component.

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



Item	Component	Description
1	Networking Cards (NC)	Provides network connectivity. An NC must be installed in slot 1. A second, optional NC can be installed in slot 2 as shown in the image. For more information, see PA-5400 Series Firewall Networking Card (NC).
2	Data Processor Cards (DPC)	Provides processing power to the appliance. Up to five DPCs can be installed in the appliance in slots 2 through 6. If a second NC is installed in slot 2, then up to four DPCs can be installed in the appliance instead.

©2026 Palo Alto Networks, Inc.

Item	Component	Description
		For more information, see PA-5400 Series Firewall Data Processor Card (DPC)
3	Blank Panel	Serves as a cover for empty slots in order to help the appliance maintain system air flow.
4	Management Processor Card (MPC)	Provides management, logging, and high availability capabilities. The MPC is a mandatory front card that is installed in slot 7. For more information, see PA-5400 Series Firewall Management Processor Card (MPC).
5	Front Mounting Flange	The two front mounting flanges are fastened to an equipment rack when mounting the firewall.
6	Electrostatic Discharge (ESD) port	Provides a grounding point that you use when removing or installing appliance components. Secure the provided wrist strap end of the ESD strap around your wrist and plug the other end into the ESD port.

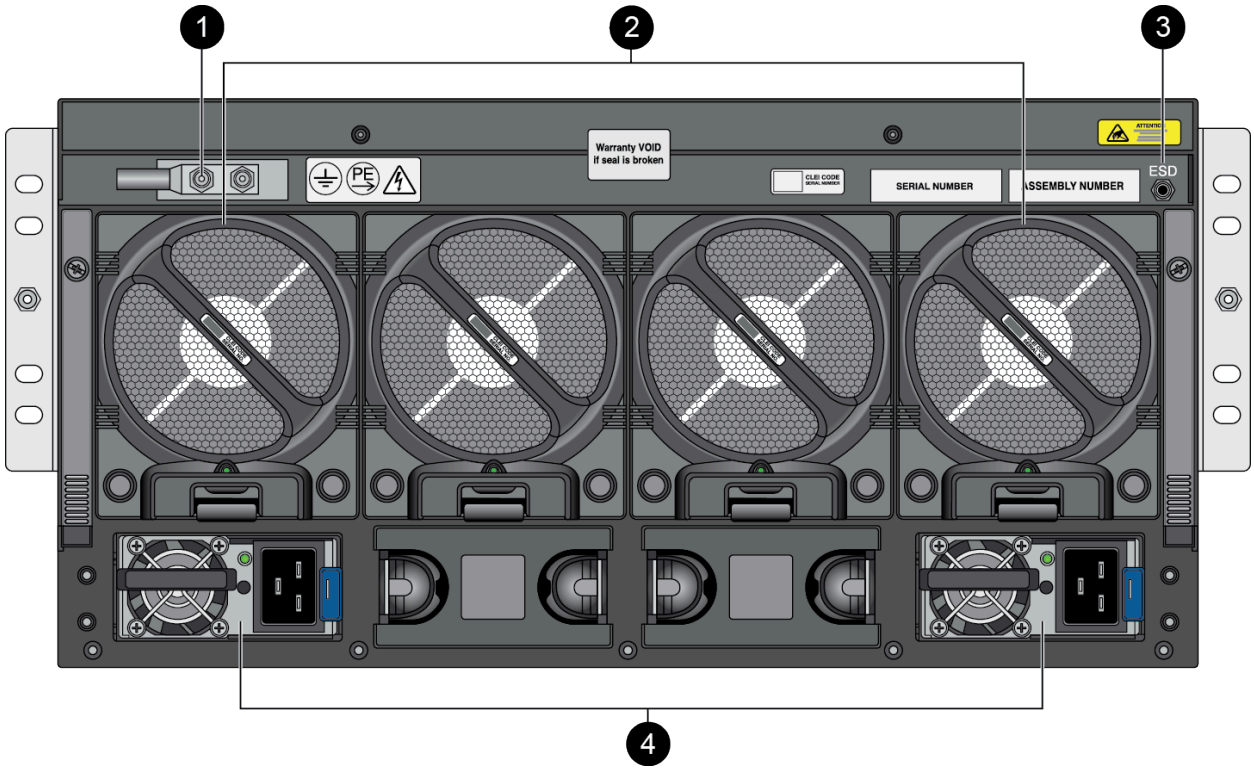
To view system firmware versions, use the following CLI command:

```
admin@PA-5400> show chassis firmware
```

PA-5450 Back Panel

The following image shows the back panel of the PA-5450 firewall (with two AC power supplies installed) and the table describes each back panel component.

©2026 Palo Alto Networks, Inc.



Item	Component	Description
1	Ground stud	Two-post stud used to ground the appliance to earth ground. Use the provided 6 AWG two#post ground lug to connect a grounded cable (not included) to the two#post stud.
2	Fan Assemblies	Provide the appliance with cooling and ventilation. There are four dual-rotor fan assemblies that can be individually replaced. While facing the rear of the firewall, the fan assemblies are labeled 1, 2, 3, and 4 from left to right. For information on replacing or installing a fan, see Replace a PA-5450 Fan Assembly.
3	Electrostatic Discharge (ESD) port	Provides a grounding point that you use when removing or installing appliance components. Secure the provided wrist strap end of the ESD strap around your wrist and plug the other end into the ESD port.
4	Power Supplies	Provide AC or DC power to the appliance. A minimum of two power supplies is required, while additional power supplies can be used to provide redundancy. *The AC power supplies support power cords with C19 connectors.*

©2026 Palo Alto Networks, Inc.

Item	Component	Description
		For information on connecting power to the appliance, see Connect Power to a PA-5400 Series Firewall.



To view system firmware versions, use the following CLI command:

```
admin@PA-5400> show chassis firmware
```


©2026 Palo Alto Networks, Inc.

 ©2026 Palo Alto Networks, Inc.

PA-5400 Series Firewall Module and Interface Card Information

The PA-5450 is a modular system that requires a Base Card (BC) and a Management Processor Card (MPC) to operate. The BC is an internal baseboard that provides connections to the front card slots, power supplies, and fan assemblies. The two types of front slot cards, Networking Cards (NC) and Data Processing Cards (DPC), are interfaced with the BC on the front of the appliance. A minimum of one NC and one DPC are required for the system to run. Due to the seven front slot arrangement, you can install up to two NCs and four DPCs or one NC and five DPCs. For details on installing front slot cards, see Install the Mandatory PA-5400 Series Firewall Front Slot Cards.



This chapter only covers the PA-5450. The PA-5450 is a modular firewall that makes use of interface cards for dedicated processing capabilities. The PA-5410, PA-5420, PA-5430, PA-5440, and PA-5445 do not have any interface cards.

The NC and DPC are hot-swappable while the BC and MPC are not.

See the following topics for more information on the PA-5450 firewall's modules.

- PA-5400 Series Firewall Base Card (BC)
- PA-5400 Series Firewall Management Processor Card (MPC)
- PA-5400 Series Firewall Networking Card (NC)
- PA-5400 Series Firewall Data Processor Card (DPC)

PA-5400 Series Firewall Base Card (BC)

The PA-5400 Series Base Card (BC) serves as the link between all static and modular components of the PA-5450 firewall. It functions as a control plane ethernet switch, a data plane traffic manager, and first packet processor subsystem. The BC interfaces with the seven front slots and the rear fan slots via signal connectors. It also uses three power bus bars to conduct currents from the power distribution board.

The BC can only be removed from the system after removing the fan assemblies first.

The following BC comes installed by default in a PA-5450 firewall:

- PA-5400 BC-A

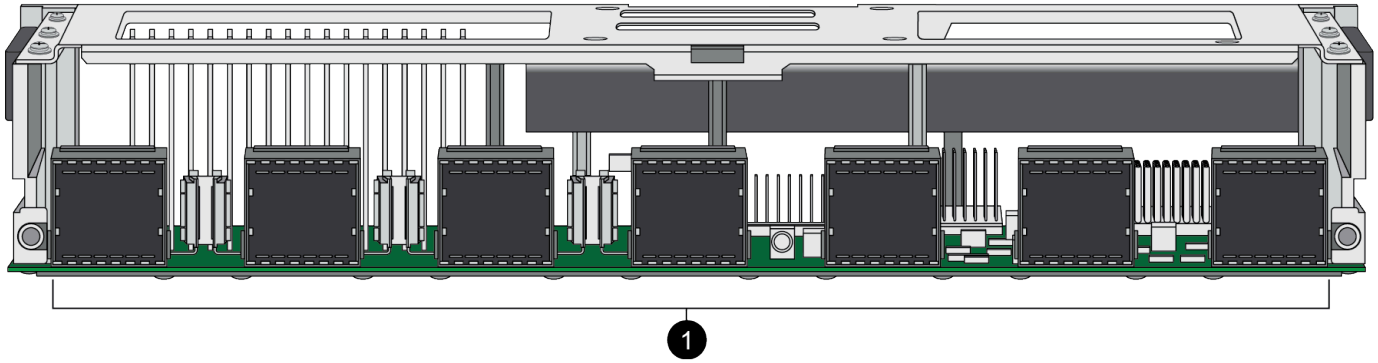
PA-5400 BC-A

The PA-5400 BC-A comes installed in a PA-5450 firewall. Use the following topic to learn about the PA-5400 BC-A component descriptions.

- PA-5400 BC-A Component Descriptions

PA-5400 BC-A Component Descriptions

The following image shows the PA-5400 BC-A and the table below describes each labeled component.



Item	Component	Description
1	Seven front signal connectors	72-differential-pair ortho-direct signal connectors that interface with the NC, DPC, and MPC slots.

©2026 Palo Alto Networks, Inc.

PA-5400 Series Firewall Management Processor Card (MPC)

The PA-5400 Series firewall Management Processor Card (MPC) is a mandatory interface for the PA-5450 that connects to the PA-5400 Series Firewall Base Card (BC). The MPC enables management, logging, and high availability functions via SFP+ ports and features two system drives and one logging drive.

The following MPC is available for PA-5450 firewall:

- PA-5400 MPC-A

PA-5400 MPC-A

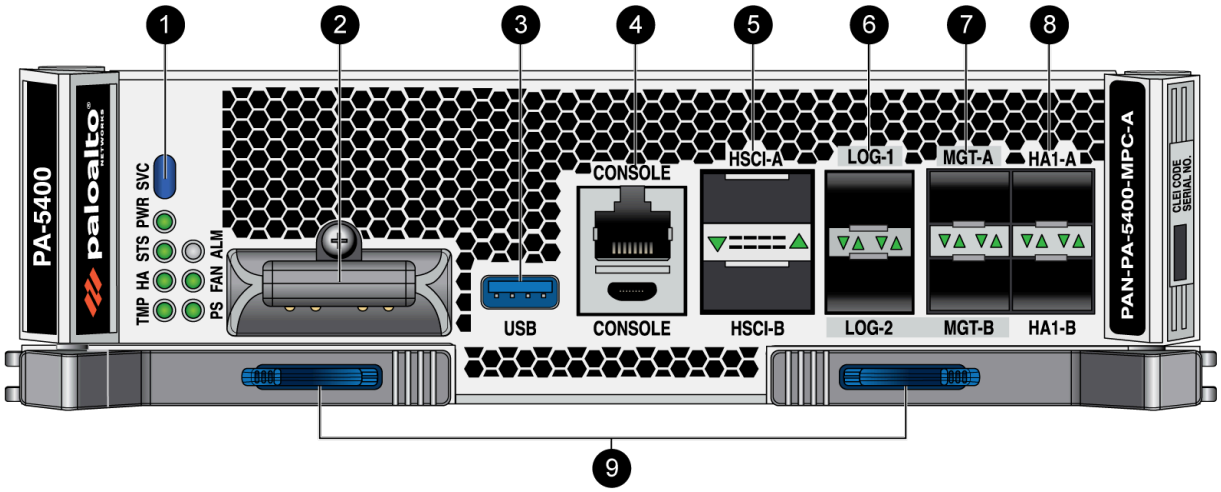
Use the following topics to learn about the PA-5400 MPC-A component descriptions and LED meanings.

- PA-5400 MPC-A Component Descriptions
- Interpret the PA-5400 MPC-A LEDs

PA-5400 MPC-A Component Descriptions

The following image shows the PA-5400 MPC-A and the table below describes each labeled component.

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



Item	Component	Description
1	LED Indicators	Eight LEDs that indicate the status of various hardware components. For details on the LEDs, see Interpret the PA-5400 MPC-A LEDs

©2026 Palo Alto Networks, Inc.

Item	Component	Description
2	Logging Drive Cover	Secures the logging drive in the MPC. By default, the MPC does not have a logging drive installed. For information about installing a logging drive, see Install an MPC Logging Drive.
3	USB Port	One USB port that accepts a USB flash drive that contains a bootstrap bundle (PAN-OS configuration) that enables you to bootstrap the firewall. Bootstrapping enables you to provision the firewall with a specific configuration, license it, and make it operational on the network.
4	RJ-45 Console Port and Micro USB Console Port	**RJ-45 Console Port** Use the console port to connect a management computer to the firewall using a 9-pin serial-to-RJ-45 cable and terminal emulation software. **Micro USB Console Port** Use the console port to connect a management computer to the firewall using a standard Type-A USB-to-micro USB cable and terminal emulation software. The console connection provides access to firewall boot messages, the Maintenance Recovery Tool (MRT), and the command line interface (CLI). *If your management computer does not have a serial port, use a USB-to-serial converter.*
5	HSCI-A and HSCI-B (High Speed Chassis Interconnect) Ports	Quad-SFP+ (QSFP+/QSFP28) interfaces used to connect two PA-5400 Series firewalls for a high availability (HA) configuration. Each port offers 80GE (two 40Gbps links) or 200GE (two 100Gbps links) connectivity and is used for HA2 data link in an active/passive configuration. When in active/active mode, the port is also used for HA3 packet forwarding for asymmetrically routed sessions that require Layer 7 inspection for App-ID™ and Content#ID™. In a typical installation, HSCI-A on the first firewall connects directly to HSCI-A on the second firewall and HSCI-B on the first firewall connects to HSCI-B on the second firewall. The purpose of HSCI-B is to increase the bandwidth for HA2/HA3 processing. This provides full 80-200Gbps transfer rates. In software, both ports (HSCI-A and HSCI-B) are treated as one HA interface. The HSCI ports are not routable and must be connected directly to each other, not through a switch. Palo Alto

©2026 Palo Alto Networks, Inc.

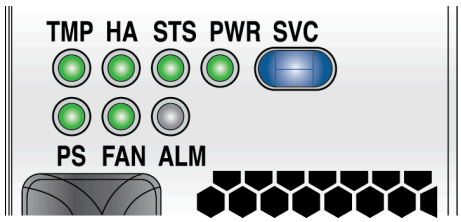
Item	Component	Description
		Networks recommends using an active or passive QSFP+ cable to connect the two HSCI ports. You can configure HA2 (data link) on the HSCI ports or on NC data ports. When configuring on dataplane ports, you must ensure that both the HA2 and HA2-Backup links are configured on dataplane interfaces. HA2-Backup cannot be configured on the HSCI ports. *For installations where the two firewalls are not near each other and you cannot use an active or passive QSFP+ cable, use a standard QSFP+ transceiver and the appropriate cable length.*
6	Logging Ports	Two SFP/SFP+ logging ports that offer 1/10GE connectivity and are used as log interfaces. LOG-1 and LOG-2 are bundled as a single logical interface called **bond1**. Bond1 uses LACP (link aggregation control protocol) as IEEE 802.3ad. Set the **Mode** for LACP status queries to **Active** and the **Transmission Rate** for LACP query and response exchanges to **Slow**. You must Configure Log Forwarding to forward logs from the log interface to one or more log collectors. If the log interface is not configured, the management interface is used to forward logs instead. *LOG-1 and LOG-2 only support fiber SFP/SFP + transceivers. Copper SFP/SFP+ transceivers are not supported.*
7	Management Ports	Two SFP/SFP+ management ports providing 1/10GE connectivity that are used to access the management interface. MGT-A (active) and MGT-B (backup) are bundled as a single logical interface called **bond0**. The two bonded ports provide redundancy, which enables the management interface to remain active if one interface goes down. LACP is not enabled on Bond0. The management interface is used for log forwarding by default if you have not configured a log interface. *The Management ports cannot be used to configure HA1 or HA1 backup. You must use the dedicated HA1-A and HA1-B ports.*

©2026 Palo Alto Networks, Inc.

Item	Component	Description
		When using bond0 with a switch, the switch should be configured with either a dynamic LAG setting or no LAG setting. Configuring the switch to use a static LAG setting causes the switch to lose connectivity. To manage the firewall, change your management computer IP address to 192.168.1.2, connect an SFP+ cable from your computer to one of the MGT ports and browse to https:// 192.168.1.1. The default login name is admin and the default password is admin. *MGT-A and MGT-B support copper and fiber SFP/SFP+ transceivers for 1G connectivity. For 10G connectivity, MGT-A and MGT-B only support fiber SFP/SFP+ transceivers.*
8	HA1 Ports	Two SFP/SFP+ ports providing 1/10GE connectivity for high availability (HA) control and synchronization. Connect this port directly from the HA1-A port on the first firewall in an HA pair to the HA1-A port on the second firewall in the pair, or connect these two ports to each other through a switch or router. The HA1-B port, when connected to the HA1-B port on a second firewall, is used for a backup connection. View the HA Ports on Palo Alto Networks Firewalls for more information.
9	Ejector Tabs	Push tabs that are used to Replace a PA-5400 Series Management Processor Card (MPC).

Interpret the PA-5400 MPC-A LEDs

Use the following information to learn how to interpret the LED dashboard located on the PA-5400 Management Processor Card (MPC-A).



The following table describes the functions and states of the MPC LED dashboard.

 ©2026 Palo Alto Networks, Inc.

LED	State	Description
TMP (Temperature)	Green	The card temperature is normal.
	Yellow	The card temperature is outside the temperature tolerance.
HA (High Availability)	Green	The firewall is in an active HA state.
	Yellow	The firewall is in a passive HA state.
	Off	The firewall is not part of an HA configuration.
STS (STATUS)	Green	The card is operating normally.
	Yellow	The card is booting up.
PWR	Green	The card is powered on.
	Off	The card is powered off.
PS (Power Supplies)	Green	All power supplies are operating normally.
	Red	A power supply has encountered a failure.
FAN (Fan Assemblies)	Green	All fans are operating normally.
	Red	A fan has encountered a failure.
ALM (Alarm)	Red	The card hardware failed.
	Off	The card is operating normally.

SVC (Service)	Allows a remote administrator to illuminate the SVC LED on a specific front-slot card so an on-site technician can locate the card.
	Enter the following command to view the status of the SVC LED on all cards that have this LED:
	`admin@PA-5450> show system service-led status`
	`Service LED`
	`Slot  Description  Status`
	`s1  PA-5400-NC-A  On`
	`s2  empty  Off`
	`s3  PA-5400-DPC-A  On`
	`s4  empty  Off`
	`s5  empty  Off`
	`s6  empty  Off`
	`s7  PA-5400-MPC-A  On`	

©2026 Palo Alto Networks, Inc.

<table>
<tr><th>LED</th><th>State</th><th>Description</th></tr>
<tr><td>SVC (Continued)</td><td colspan="2">Enter the following command to view the status for a card in a specific slot:
<code>admin@PA-5450> show system service-led status slot s3</code>
Enter the following command to enable all SVC LEDs:
<code>admin@PA-5450>set system setting service-led enable yes</code>
Enter the following command to disable the SVC LED:
<code>admin@PA-5450> set system setting service-led enable no</code>
Enter the following command to enable the SVC LED on the card in a specific slot:
<code>admin@PA-5450> set system setting service-led enable slot s3 yes</code></td></tr>
<tr><td></td><td>Off</td><td>LED is off.</td></tr>
<tr><td></td><td>On</td><td>LED is solid blue.</td></tr>
</table>

©2026 Palo Alto Networks, Inc.

PA-5400 Series Firewall Networking Card (NC)

Networking Cards (NCs) provide network connectivity for a PA-5450 firewall. To scale performance and capacity, you can install up to two NCs in a PA-5450 firewall.

When viewing the NCs from the web interface, the NCs are organized by slot and you click the icon to the left of the slot number to show the NC ports. The port numbering designation is Ethernet, followed by slot/port such as ethernet<slot>/<port>, where slot is the physical slot the card is installed in and the port is the interface port number. For example, the first Ethernet port on an NC installed in slot 1 shows ethernet1/1 and port 2 shows ethernet1/2. The first port on an NC installed in slot 2 shows ethernet2/1 and port 2 shows ethernet2/2. For information on installing the NC, see Install a PA-5400 Series Firewall Networking Card (NC).

On the PA-5450 firewall, you can install NCs in slots 1 and 2, but a minimum of one NC is required for the firewall to process network traffic. If installing in both slots, the maximum number of Data Processor Cards (DPCs) you can install is four. See PA-5400 Series Firewall Data Processor Card (DPC) for more information.

See Identify PA-5400 Series Port Activity and Link LEDs to learn how to interpret the NC port LEDs.

The PA-5450 firewall makes use of paired Logical Card Slots in order to direct processing power from a Data Processing Card (DPC) to a corresponding NC.

The following NC can be installed in a PA-5400 Series firewall:

- PA-5400 NC-A

PA-5400 NC-A

The PA-5400 NC-A provides up to 100Gbps Ethernet connectivity. Use the following topics to learn about descriptions of the NC components and how to interpret the LEDs.

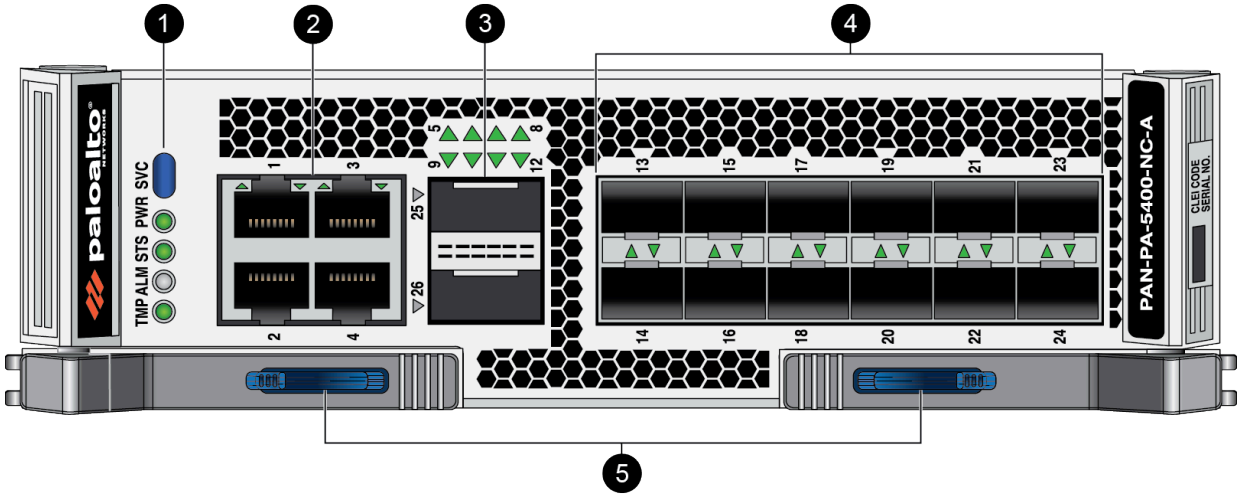
- PA-5400 NC-A Component Descriptions
- Interpret the PA-5400 NC-A LEDs

PA-5400 NC-A Component Descriptions

The following image shows the PA-5400 NC-A and the table describes each labeled component.

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

 ©2026 Palo Alto Networks, Inc.

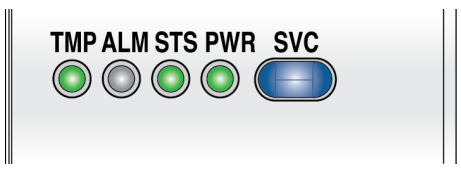


Item	Component	Description
1	LED Indicators	Five LEDs that indicate the status of various hardware components. For details on the LEDs, see Interpret the PA-5400 NC-A LEDs
2	Ethernet Ports	Four 1Gbps/10Gbps BaseT RJ45 Ethernet ports.
3	QSFP Ports	Two form-factor pluggable (QSFP+/QSFP28) 40GE/100GE Ethernet ports. Each interface supports breakout mode to create four 10GE or four 25GE ports each.
4	SFP/SFP+ Ports	Twelve 1GE/10GE SFP+ ports.
5	Ejector Tabs	Push tabs that are used to Replace a PA-5400 Series Networking Card (NC).

Interfaces on two separate NCs can be configured as aggregate interfaces.

Interpret the PA-5400 NC-A LEDs

Use the following information to learn how to interpret the LED dashboard and port LEDs on the PA-5400 Networking Card (NC-A)



The following table describes the functions and states of the NC-A LED dashboard.

 ©2026 Palo Alto Networks, Inc.

<table>
<tr><th>LED</th><th>State</th><th>Description</th></tr>
<tr><td rowspan="2">TMP
(Temperature)</td><td>Green</td><td>The card temperature is normal.</td></tr>
<tr><td>Yellow</td><td>The card temperature is outside the temperature tolerance.</td></tr>
<tr><td rowspan="2">ALM
(Alarm)</td><td>Red</td><td>The card hardware failed.</td></tr>
<tr><td>Off</td><td>The card is operating normally.</td></tr>
<tr><td rowspan="2">STS
(STATUS)</td><td>Green</td><td>The card is operating normally.</td></tr>
<tr><td>Yellow</td><td>The card is booting up.</td></tr>
<tr><td rowspan="2">PWR</td><td>Green</td><td>The card is powered on.</td></tr>
<tr><td>Off</td><td>The card is powered off.</td></tr>
<tr><td>SVC
(Service)</td><td colspan="2">Allows a remote administrator to illuminate the SVC LED on a specific front-slot card so an on-site technician can locate the card.
Enter the following command to view the status of the SVC LED on all cards that have this LED:
<pre>admin@PA-5450> show system service-led status
Service LED
Slot   Description   Status
s1   PA-5400-NC-A   On
s2   empty   Off
s3   PA-5400-DPC-A   On
s4   empty   Off
s5   empty   Off
s6   empty   Off
s7   PA-5400-MPC-A   On</pre></td></tr>
<tr><td>SVC
(Continued)</td><td colspan="2">Enter the following command to view the status for a card in a specific slot:
<pre>admin@PA-5450> show system service-led status slot s3</pre>Enter the following command to enable all SVC LEDs:
<pre>admin@PA-5450>set system setting service-led enable yes</pre>Enter the following command to disable the SVC LED:
<pre>admin@PA-5450> set system setting service-led enable no</pre></td></tr>
</table>

©2026 Palo Alto Networks, Inc.

LED	State	Description
	Enter the following command to enable the SVC LED on the card in a specific slot: `admin@PA-5450> set system setting service-led enable slot s3 yes`	
	Off	LED is off.
	On	LED is solid blue.

The following table describes functions and states of the SFP+ port LEDs.

LED	Description
Left	The LED shows green if there is a network link.
Right	Blinks green or stays green if there is network activity.

The following table describes functions and states of the QSFP28 port LEDs. The LEDs are tri-color and the color indicates link and the current port speed.

Interface Speed	Green LED	Blue LED	Yellow LED
10Gbps	On	Off	Off
25Gbps	On	On	Off
40Gbps	Off	Off	On
100Gbps	Off	On	Off

©2026 Palo Alto Networks, Inc.

PA-5400 Series Firewall Data Processor Card (DPC)

The PA-5400 Series Data Processor Card (DPC) is a front slot card that improves the processing capacity of the PA-5450 firewall. You can install up to four or five DPCs depending on your scaling needs and slot configuration. A DPC can be installed in slots 2 through 6; however, slot 2 may also be used for the installation of a Networking Card (NC). See PA-5400 Series Firewall Networking Card (NC) for more information.

The PA-5450 firewall makes use of paired Logical Card Slots in order to direct processing power from a DPC to a corresponding Networking Card (NC). Certain commands issued to the NC affect or are affected by the status of its corresponding DPC.

Because the DPC has no front ports or interfaces, you must change the firewall's session distribution policy from the default.

*It is recommended that you change the session distribution policy to **session-load** when installing the DPC.*

The following DPCs can be installed in a PA-5450 firewall:

- PA-5400 DPC-A

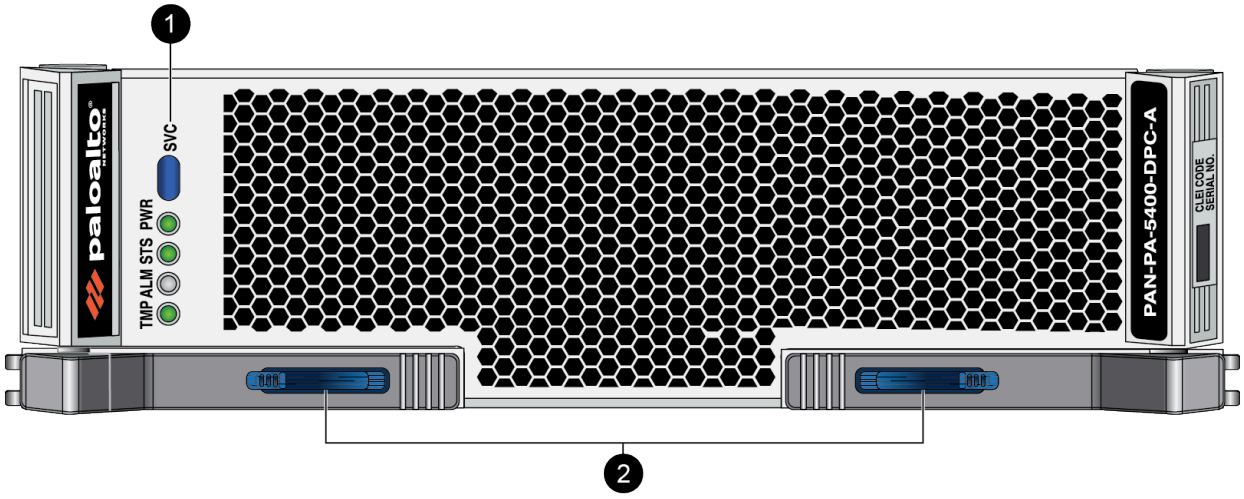
PA-5400 DPC-A

The PA-5400 DPC-A improves session capacity and performance through additional data plane instances. Use the following topics to learn about requirements, descriptions of the DPC components, and how to interpret the LEDs.

- PA-5400 DPC-A Component Descriptions
- Interpret the PA-5400 Series DPC-A LEDs

PA-5400 DPC-A Component Descriptions

The following image shows the PA-5400 DPC-A and the table describes each labeled component.

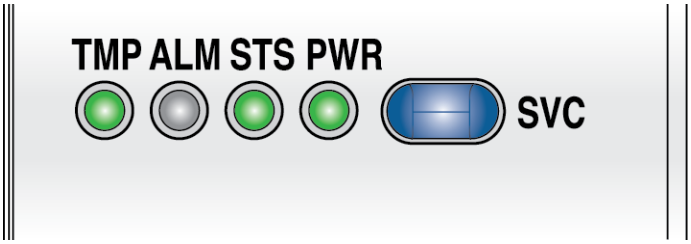


 ©2026 Palo Alto Networks, Inc.

Item	Component	Description
1	LED Indicators	Five LEDs that indicate the status of various hardware components. For details on the LEDs, see Interpret the PA-5400 Series DPC-A LEDs
2	Ejector Tabs	Push tabs that are used to Replace a PA-5400 Series Data Processor Card (DPC).

Interpret the PA-5400 Series DPC-A LEDs

Use the following information to learn how to interpret the LED dashboard and port LEDs on the PA-5400 Series Firewall Data Processing Card (DPC).



The following table describes the functions and states of the DPC LED dashboard.

LED	State	Description
TMP (Temperature)	Green	The card temperature is normal.
	Yellow	The card temperature is outside the temperature tolerance.
ALM (Alarm)	Red	The card hardware failed.
	Off	The card is operating normally.
STS (STATUS)	Green	The card is operating normally.
	Yellow	The card is booting up.
PWR	Green	The card is powered on.
	Off	The card is powered off.
SVC (Service)	Allows a remote administrator to illuminate the SVC LED on a specific front-slot card so an on-site technician can locate the card. Enter the following command to view the status of the SVC LED on all cards that have this LED: `admin@PA-5450> show system service-led status`	

©2026 Palo Alto Networks, Inc.

<table>
<tr><th>LED</th><th>State</th><th>Description</th></tr>
<tr><td></td><td colspan="2">

```
Service LED
Slot    Description       Status
s1      PA-5400-NC-A      On
s2      empty             Off
s3      PA-5400-DPC-A     On
s4      empty             Off
s5      empty             Off
s6      empty             Off
s7      PA-5400-MPC-A     On
```

</td></tr>
<tr><td>SVC (Continued)</td><td colspan="2">Enter the following command to view the status for a card in a specific slot:

admin@PA-5450> show system service-led status slot s3

Enter the following command to enable all SVC LEDs:

admin@PA-5450>set system setting service-led enable yes

Enter the following command to disable the SVC LED:

admin@PA-5450> set system setting service-led enable no

Enter the following command to enable the SVC LED on the card in a specific slot:

admin@PA-5450> set system setting service-led enable slot s3 yes</td></tr>
<tr><td></td><td>Off</td><td>LED is off.</td></tr>
<tr><td></td><td>On</td><td>LED is solid blue.</td></tr>
</table>

©2026 Palo Alto Networks, Inc.

©2026 Palo Alto Networks, Inc.

PA-5400 Series Firewall Installation

The PA-5400 Series firewalls ship with racking equipment and cables that enable you to install the firewall in your deployment environment.

The PA-5450 in particular is a modular system that requires you to install several components, such as network cards, during the installation process. Due to the weight of the firewalls, we recommend that you first install the firewall appliance into the rack and then install the front slot cards. After the firewall is installed in the rack (with all components installed), connect power, verify that the front slot cards are functioning, and then connect network and management cables.

A PA-5450 with front slot cards, fan assemblies, and power supplies installed should not be moved or shipped. Moving or shipping the firewall after assembly will void the product warranty. The PA-5450 firewall and its modules should be shipped in separate boxes.

Read Before You Begin before starting the installation.

- PA-5400 Series Firewall Equipment Rack Installation
- Install the Mandatory PA-5400 Series Firewall Front Slot Cards (PA-5450 only)
- Set Up a Connection to the Firewall
- Connect Power to a PA-5400 Series Firewall
- Verify the PA-5450 Firewall NC Configuration (PA-5450 only)
- Connect Cables to a PA-5400 Series Firewall

PA-5400 Series Firewall Equipment Rack Installation

PA-5400 Series firewalls are designed for installation in a standard 19-inch equipment rack. Before you install the hardware, read PA-5400 Series Firewall Rack Install Safety Information.

- Install the PA-5400 Series Firewall in an Equipment Rack (PA-5410, PA-5420, PA-5430, PA-5440, and PA-5445)
- Install the PA-5450 Firewall in an Equipment Rack

PA-5400 Series Firewall Rack Install Safety Information

Read the following information before you proceed with a PA-5400 Series Firewall Equipment Rack Installation.

- Elevated ambient operating temperature—If the PA-5400 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 PA-5400 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-5400 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.

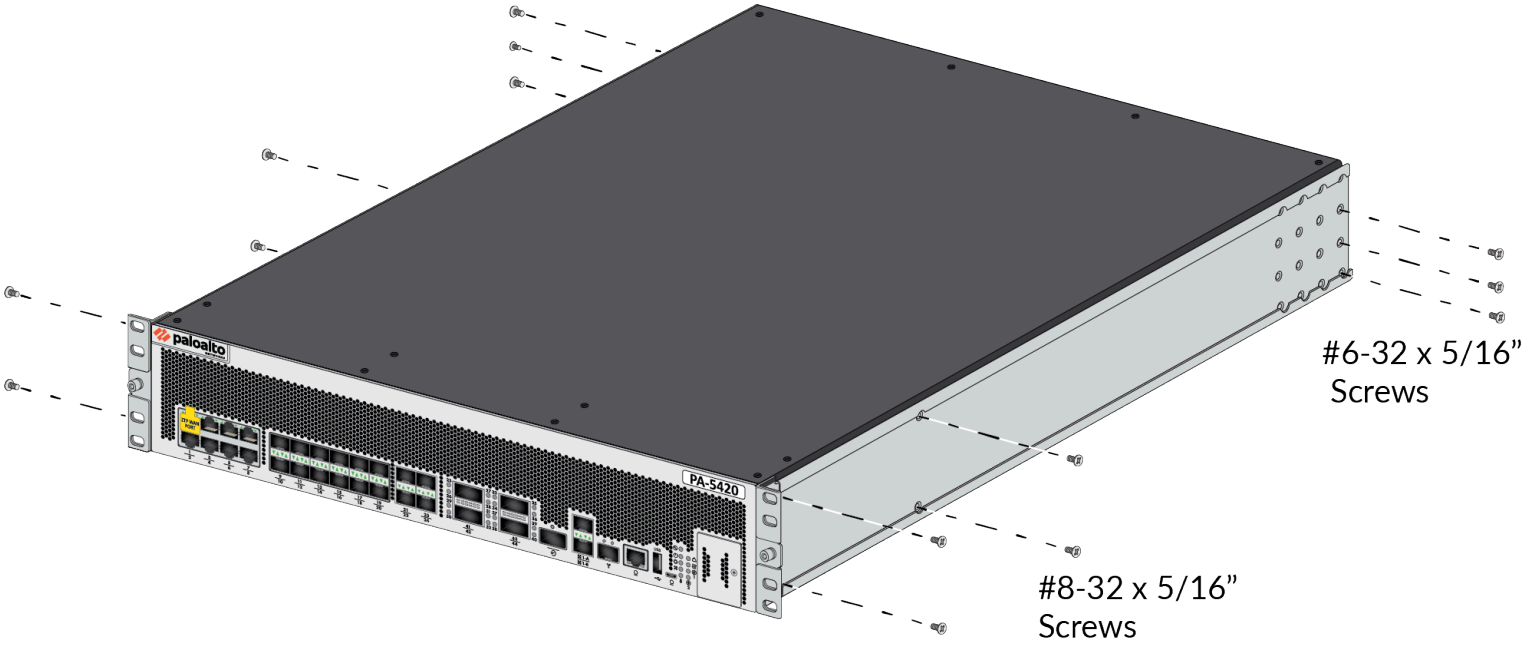
Install the PA-5400 Series Firewall in an Equipment Rack

The following procedure describes how to install the PA-5410, PA-5420, PA-5430, PA-5440, and PA-5445 firewalls in a 19” four-post equipment rack using the provided four-post rack kit (PAN-PA-2RU-RACK4). This kit is designed to provide additional support for the back of the firewall.

STEP 1 | Read PA-5400 Series Firewall Rack Install Safety Information.

©2026 Palo Alto Networks, Inc.

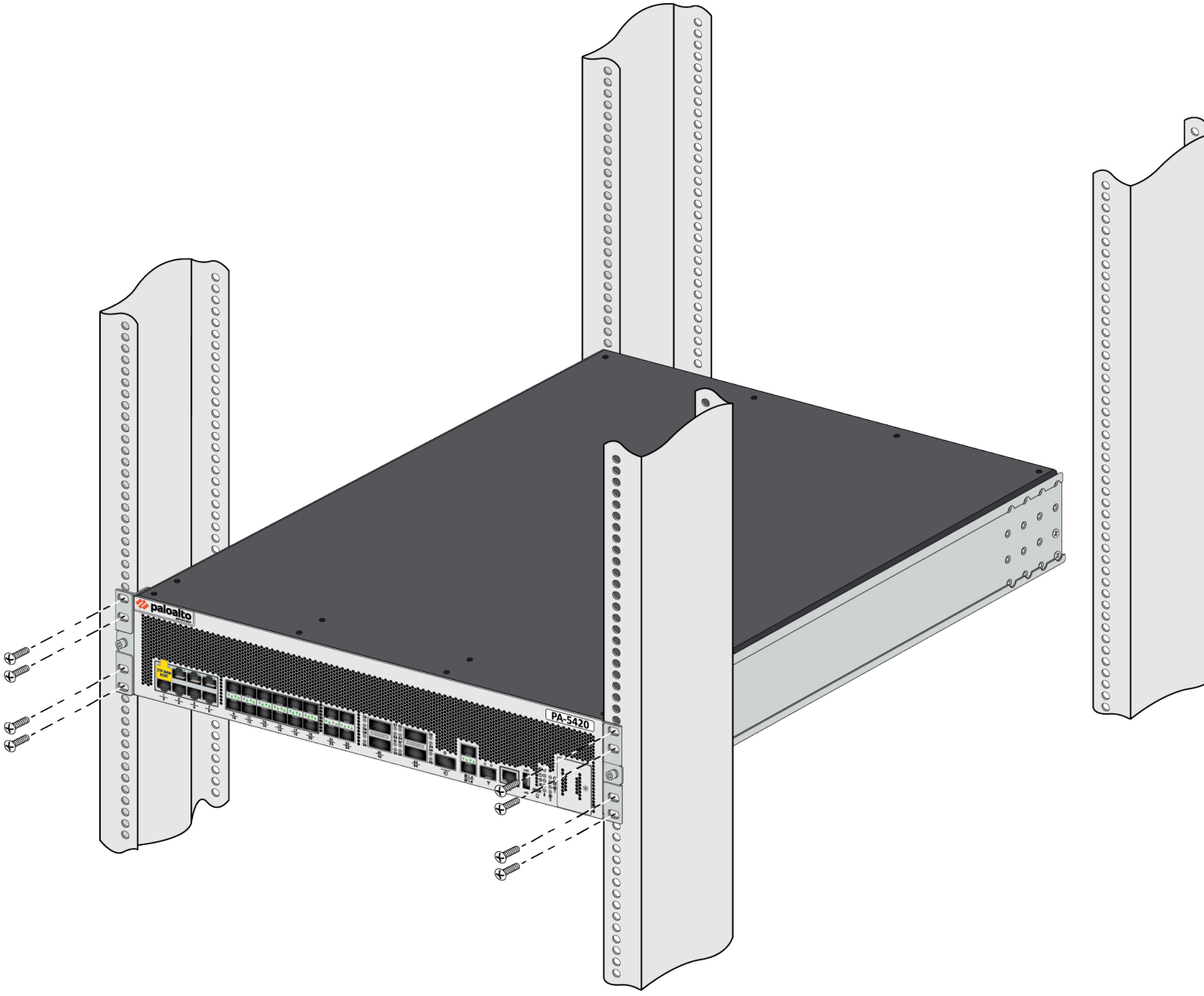
STEP 2 | Attach one fixed rack mount bracket to each side of the firewall. Use four #8-32 x 5/16” screws for the front four screw holes in each bracket and three #6-32 x 5/16” screws for the back three screw holes and torque each screw to 15 in-lbs.



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

©2026 Palo Alto Networks, Inc.

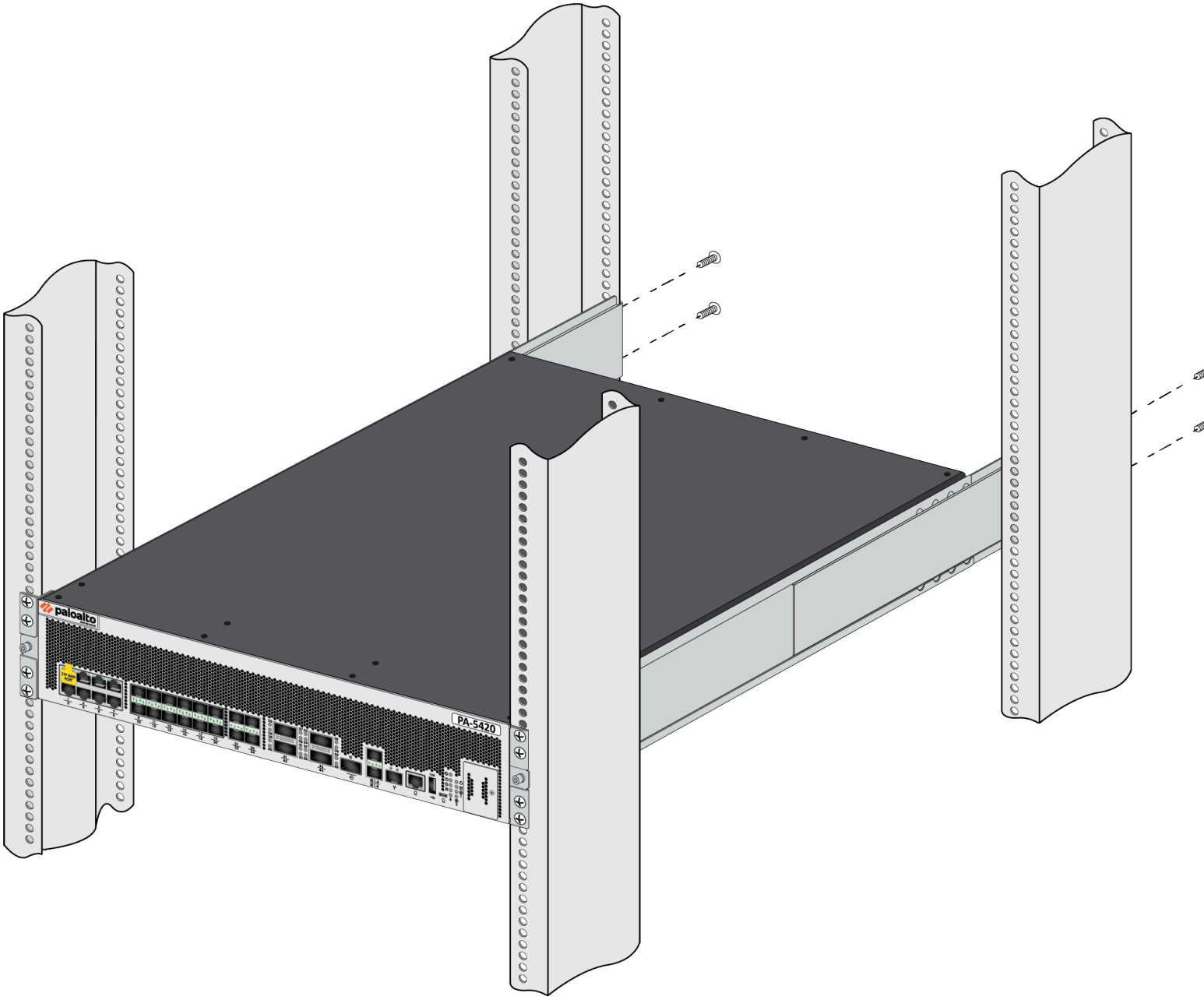
screws (#10-32 x 3/4” or #12-24 x 1/2”) for your rack and torque each screw to 25 in-lbs. Use the provided cage nuts to secure the screws if the rack has square holes.



STEP 4 | Slide one adjustable rack mount bracket into each of the two previously installed fixed rack mount bracket. Secure the two adjustable rack mount brackets to the back rack-posts using

 ©2026 Palo Alto Networks, Inc.

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



Install the PA-5450 Firewall in an Equipment Rack

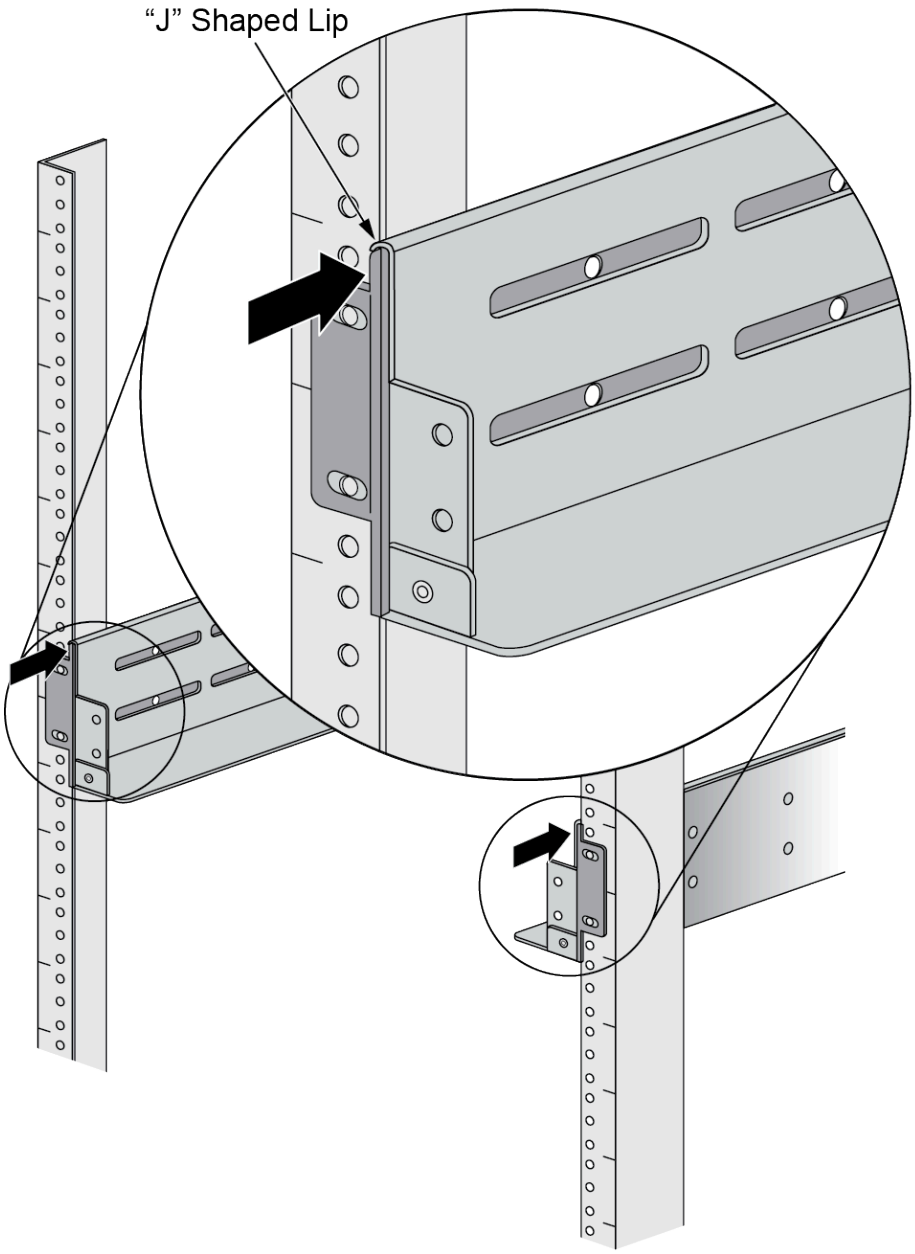
The following procedures describe how to install the PA-5450 firewall in an equipment rack.

The PA-5450 appliance and the front slot cards (MPC, NC, and DPC) ship in separate boxes and it is recommended that you install the cards after you rack-mount the appliance. This will prevent any damage to the cards that could occur during rack mounting and will reduce the weight of the appliance. To further reduce the weight, remove the fan trays and power supplies. The PA-5450 requires 5 RU (rack units) of rack space. Unless specified, screws are not provided.

 ©2026 Palo Alto Networks, Inc.

STEP 1 | Read PA-5400 Series Firewall Rack Install Safety Information.

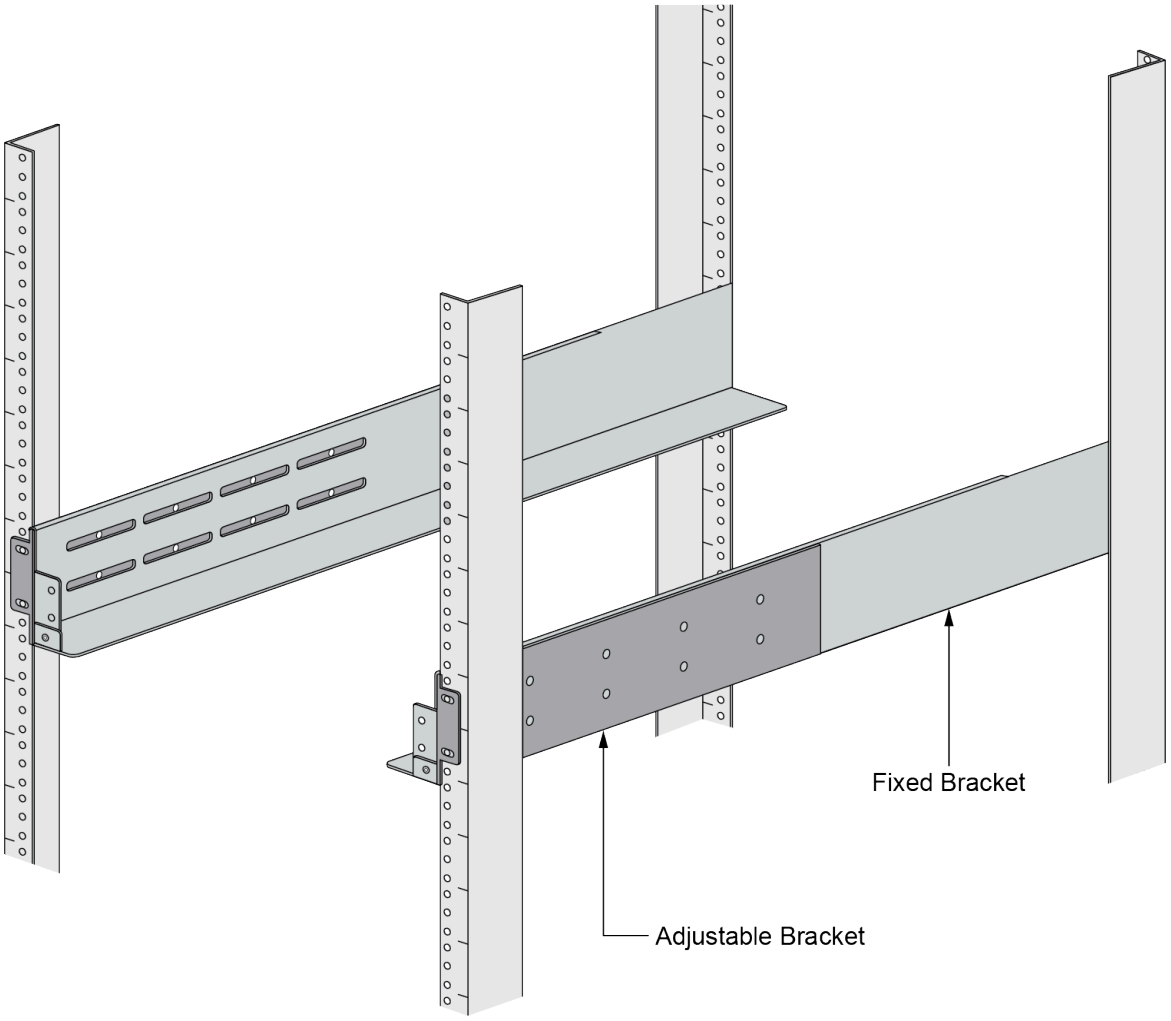
STEP 2 | Slide one of the adjustable mounting brackets into the “J” shaped lip on the top edge of one of the fixed mounting brackets. Repeat with the second adjustable and fixed mounting brackets.



STEP 3 | Position the bottom edges of the fixed and adjustable brackets to the bottom of the 5 RU rack space reserved for the PA-5450. Align the slotted holes of the fixed mounting bracket

 ©2026 Palo Alto Networks, Inc.

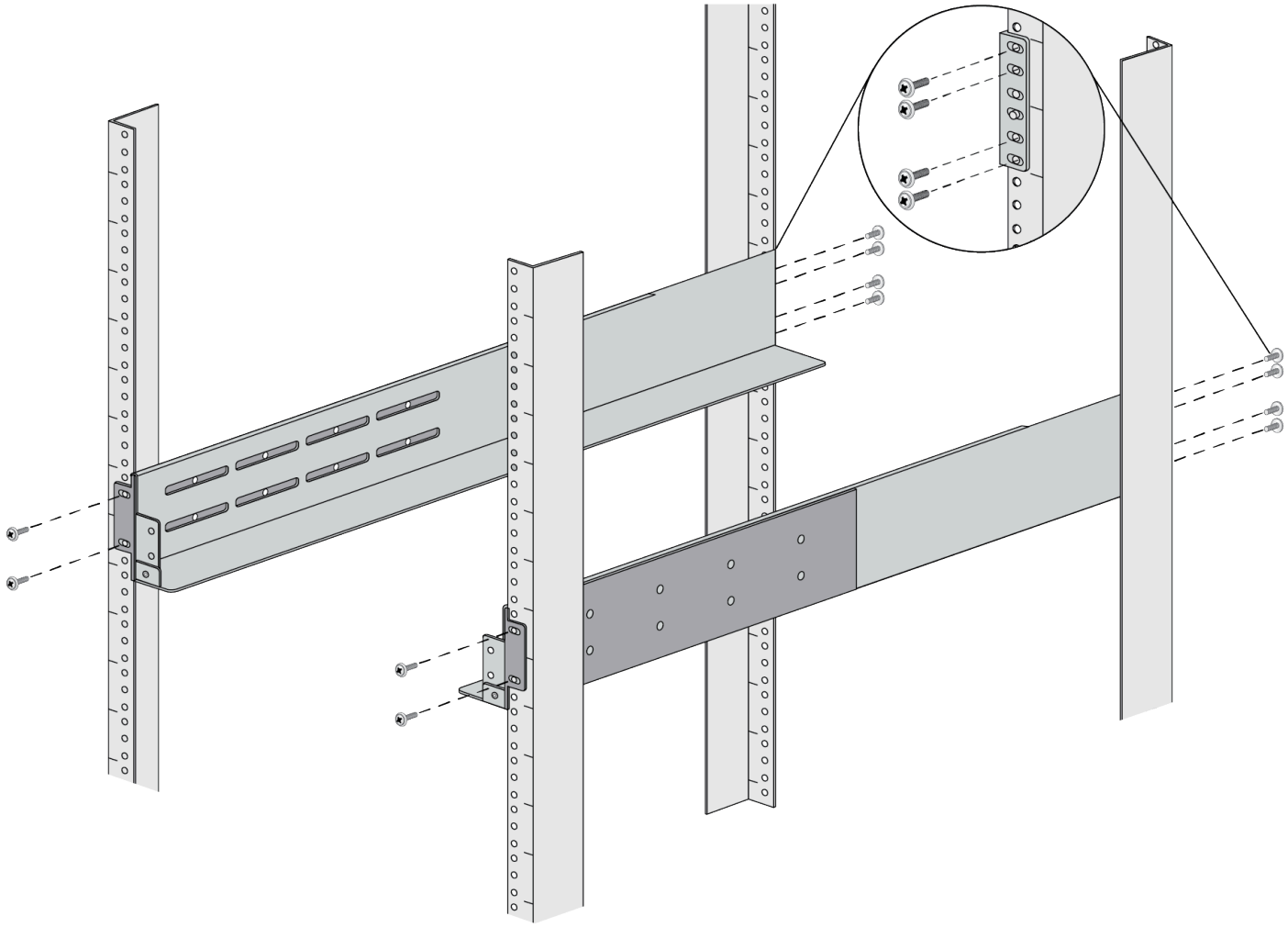
to the holes on the front side of the equipment frame being used. Similarly, align the slotted holes in the adjustable mounting bracket to the holes on the rear of the equipment frame.



©2026 Palo Alto Networks, Inc.

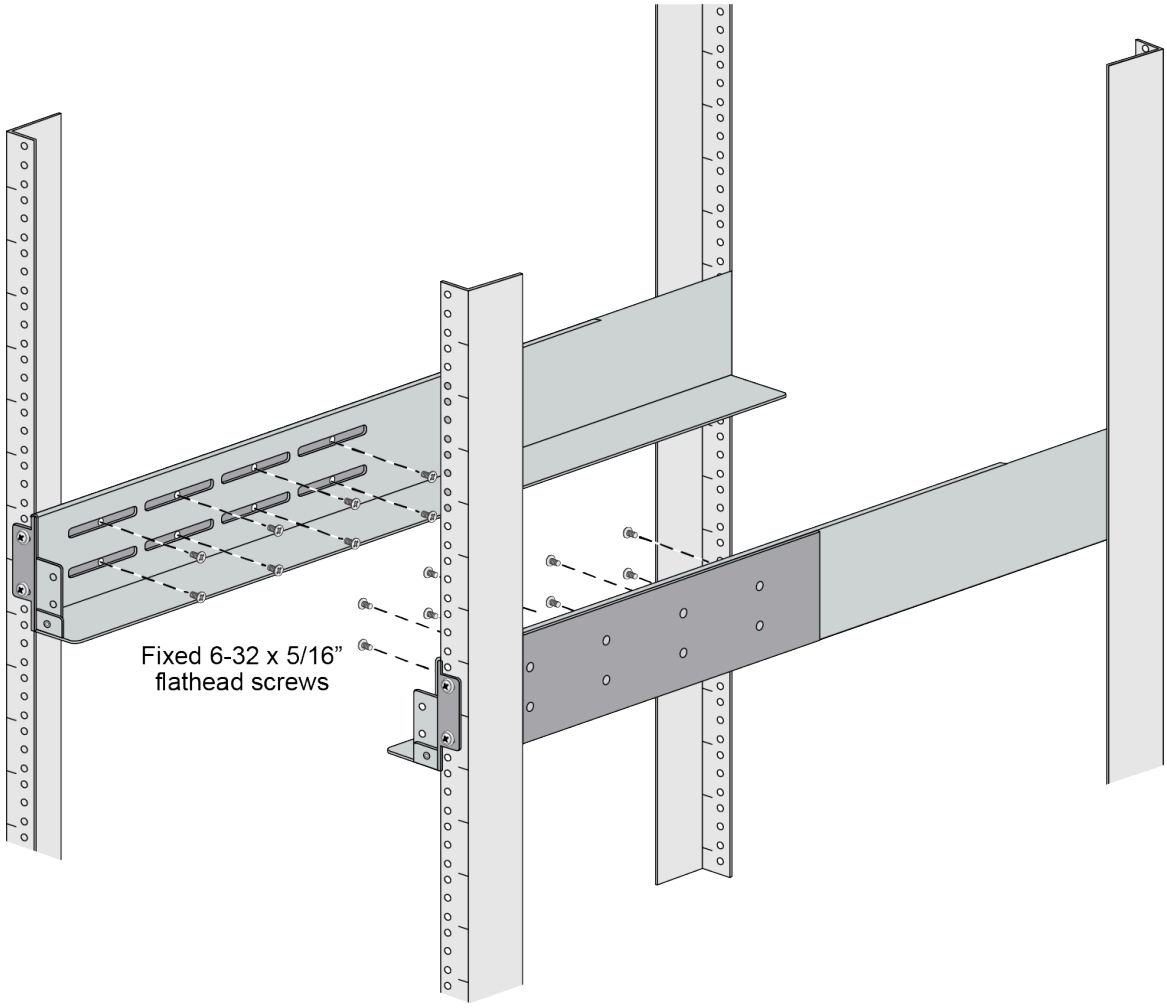
STEP 4 | Adjust the brackets to fit the depth of the equipment frame, then secure the brackets to the equipment frame with mounting screws (not provided) compatible with your equipment frame. Tighten the screws to their recommended torque value.

The mounting brackets are designed for equipment frames that are up to 32” deep (81.3 cm).



©2026 Palo Alto Networks, Inc.

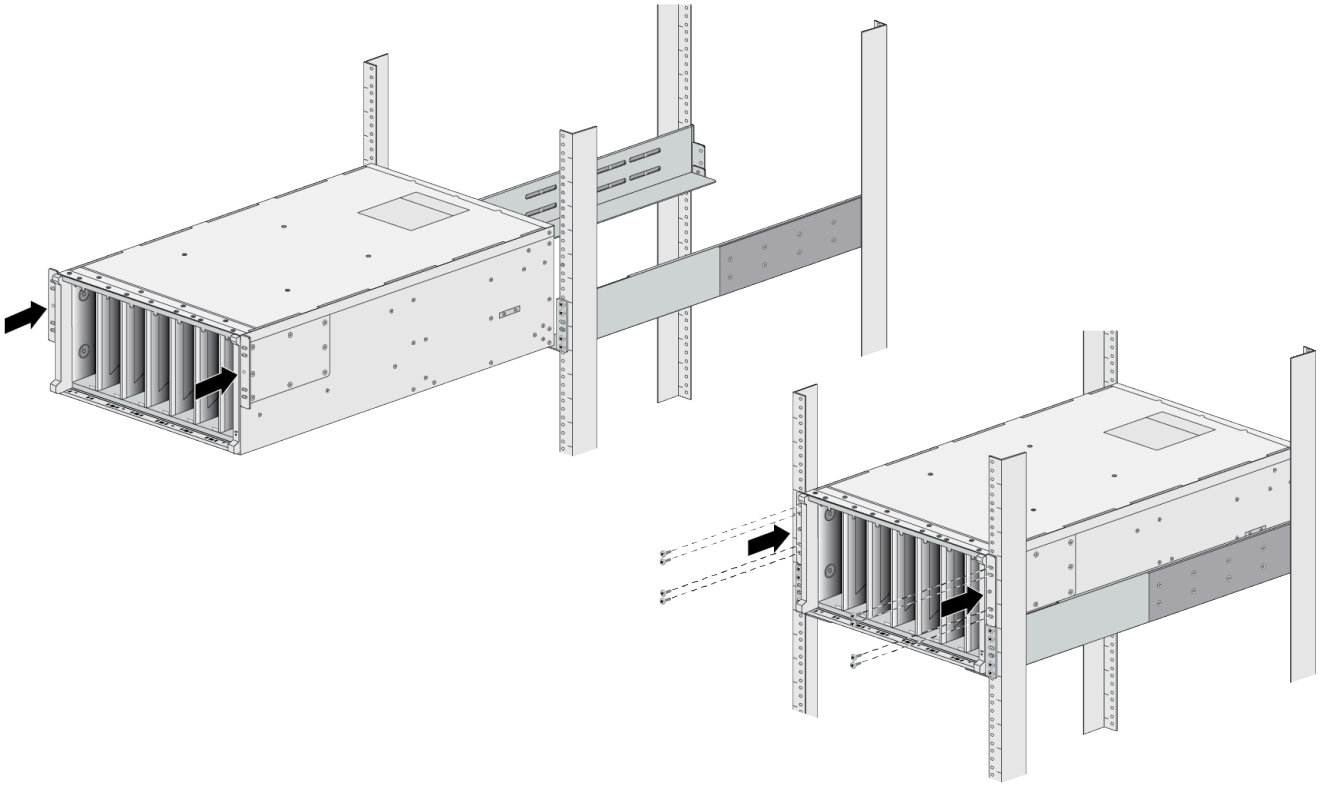
STEP 5 | Use the provided 6-32 x 5/16 flathead screws to secure the adjustable bracket to the fixed bracket. A minimum of 6 screws are required for each side.



STEP 6 | Slide the PA-5450 on the brackets that were previously mounted to the equipment frame until the front mounting flanges of the PA-5450 are flush against the mounting surface of the equipment frame.

©2026 Palo Alto Networks, Inc.

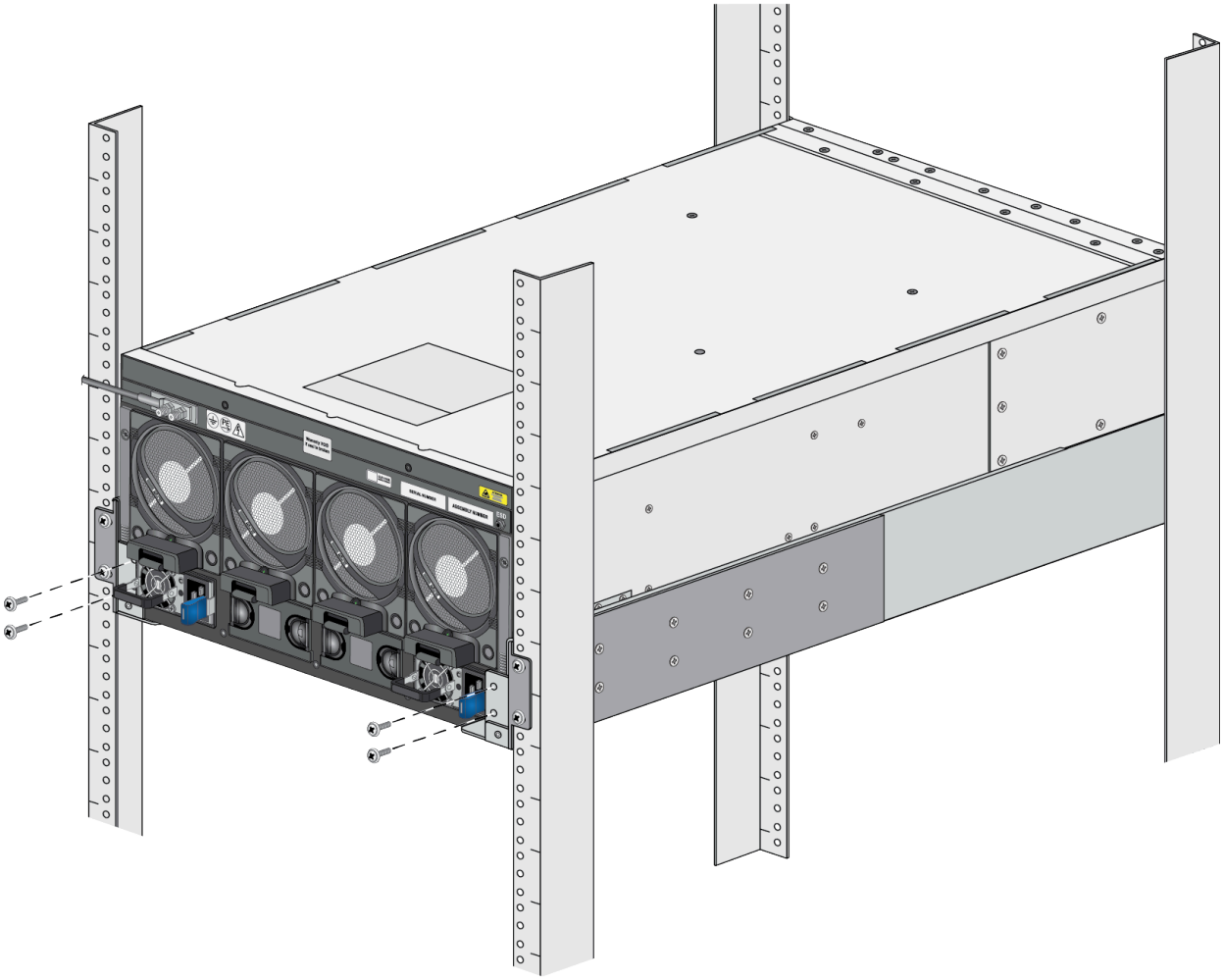
STEP 7 | Secure the PA-5450 to the equipment frame on both sides using 8 screws each (not provided). The screws must be compatible with your equipment frame.



©2026 Palo Alto Networks, Inc.

STEP 8 | Use the provided 8-32 x 3/8” Phillips panhead screws to secure the back side of the PA-5450 to the previously mounted brackets.

You may need to loosen the PA-5450 support bracket screws to align the holes in the support bracket to the threaded holes in the PA-5450 appliance. If adjustment is needed, only loosen the screws on one side at a time.



©2026 Palo Alto Networks, Inc.

Install the Mandatory PA-5400 Series Firewall Front Slot Cards

The PA-5450 firewalls require a minimum of three cards that you install in the front slots of the appliance. These cards are shipped separately from the firewall and include the following: The Management Processor Card (MPC) provides management connectivity to the appliance and HA connectivity; the Networking Card (NC) enables the firewall to process network traffic; and the Data Processor Card (DPC) handles data-plane processing.

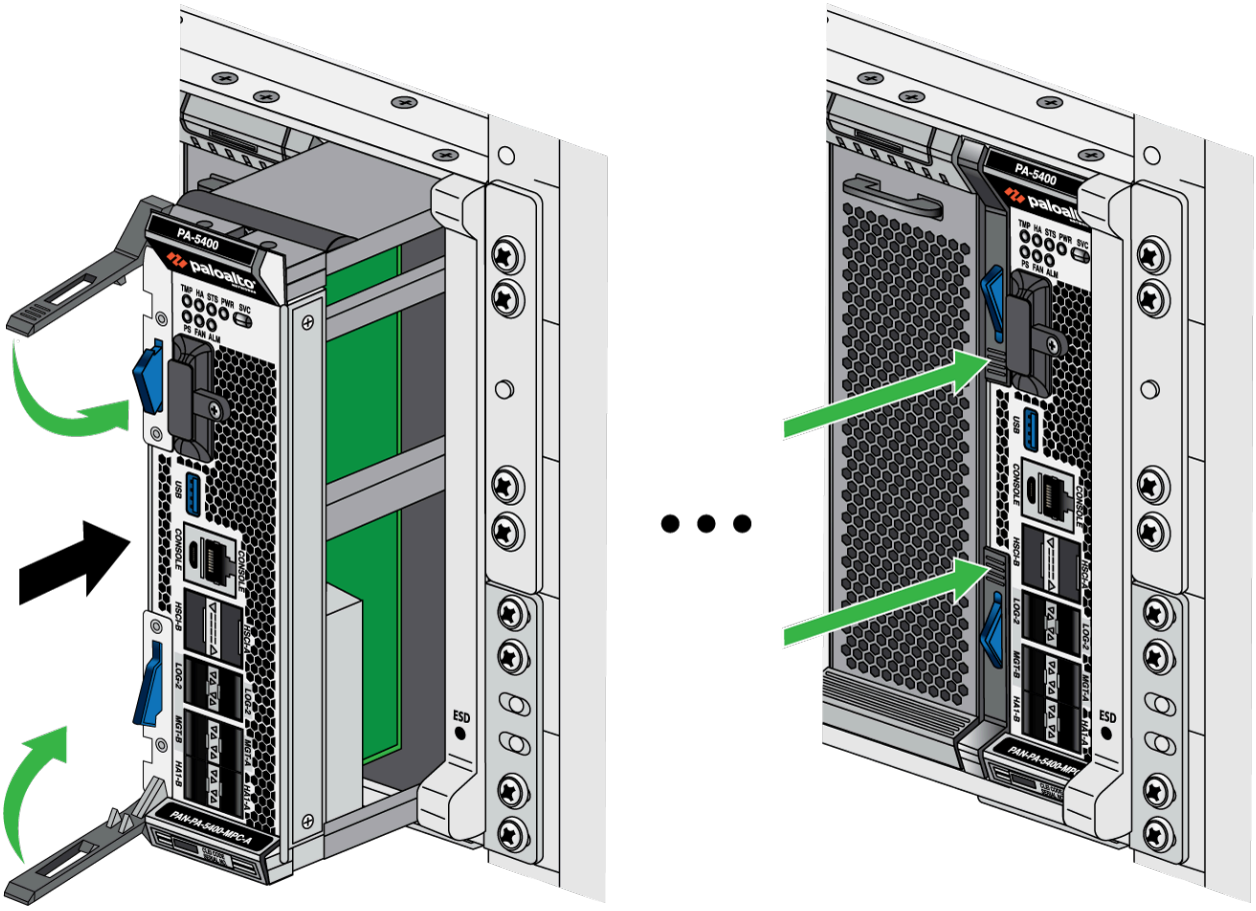
- Install a PA-5400 Series Firewall Management Processor Card (MPC)
- Install a PA-5400 Series Firewall Networking Card (NC)
- Install a PA-5400 Series Firewall Data Processor Card (DPC)

Install a PA-5400 Series Firewall Management Processor Card (MPC)

STEP 1 | Attach the provided ESD strap to your wrist and plug the other end in to the ESD port location on the front of the appliance. See PA-5450 Front Panel for the location of the ESD port.

©2026 Palo Alto Networks, Inc.

STEP 2 | Remove the MPC from the antistatic bag. Push the top and bottom ejector tabs towards each other to allow the ejector levers to rotate into an open position.



STEP 3 | Rotate the card and align it with the front of the appliance so that the Palo Alto Networks logo is readable at the top of the card. Gently push the MPC into slot 7 until the card reaches the end of the slot.

STEP 4 | Push on both ejector handles until they lock the card into place.

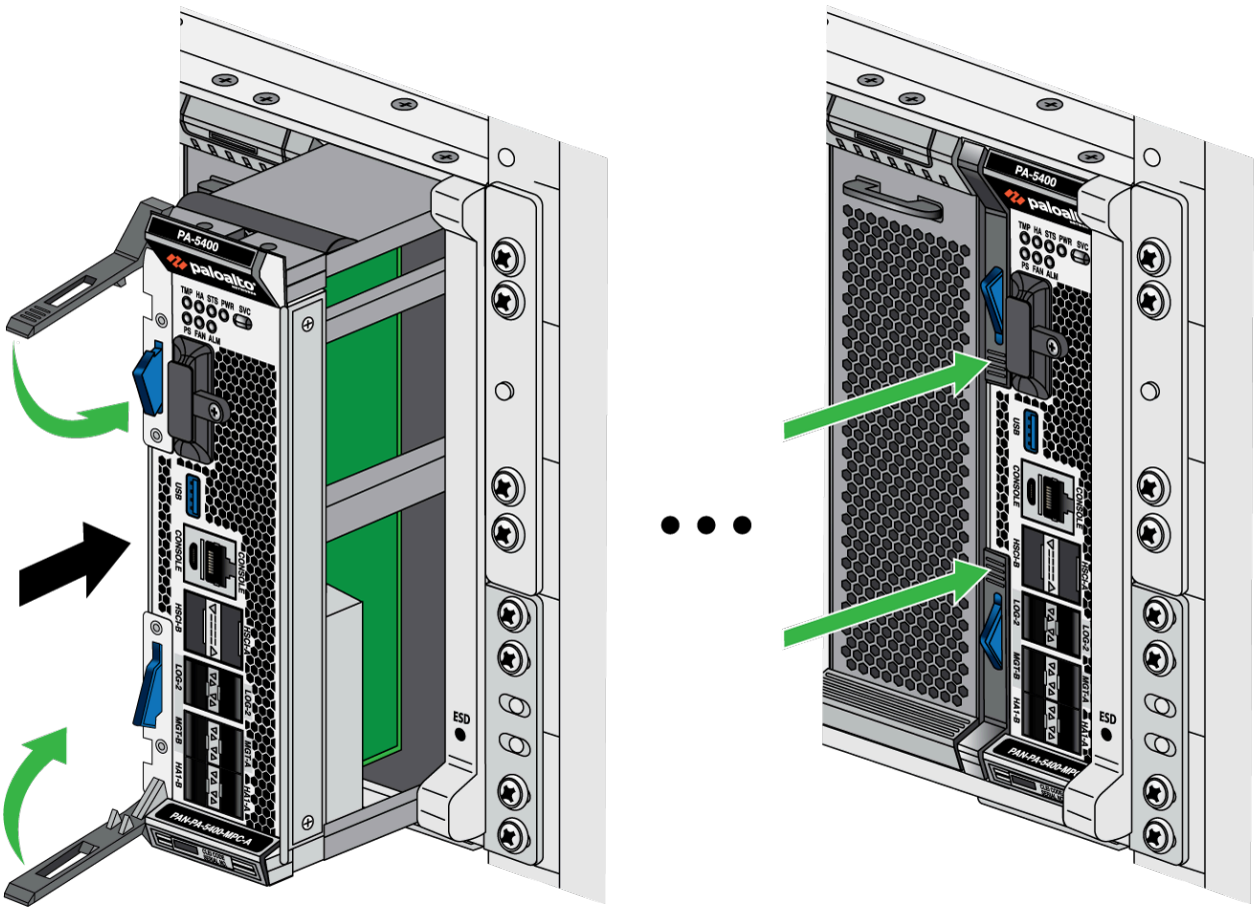
Install a PA-5400 Series Firewall Networking Card (NC)

STEP 1 | Attach the provided ESD strap to your wrist and plug the other end in to the ESD port location on the front of the appliance. See PA-5450 Front Panel for the location of the ESD port.

 ©2026 Palo Alto Networks, Inc.

STEP 2 | Remove the NC from the antistatic bag. Push the top and bottom ejector tabs towards each other to allow the ejector levers to rotate into an open position.

The image below shows a Management Processor Card (MPC); however, the procedure to install the NC is the same.



STEP 3 | Rotate the card and align it with the front of the appliance so that the Palo Alto Networks logo is readable at the top of the card. Gently push the NC into slot 1 until the card reaches the end of the slot.

The PA-5450 firewall makes use of paired Logical Card Slots in order to direct processing power from a Data Processing Card (DPC) to a corresponding NC. When installing a DPC, you must install it in the correct slot to pair with the NC.

STEP 4 | Push on both ejector handles until they lock the card into place.

STEP 5 | (Optional) Repeat Steps 3 through 5 in slot 2 if you wish to install a second NC.

STEP 6 | (If you have unused front slots) Install a blank panel into each unused card slot to help the appliance maintain system air flow. Ensure that the bottom “teeth” of the blank panel fit into the notches on the bottom of the slot. Rotate the blank panel upwards until it snaps at the top of the slot.

©2026 Palo Alto Networks, Inc.

Configure Session Distribution on a PA-5400 Series Firewall

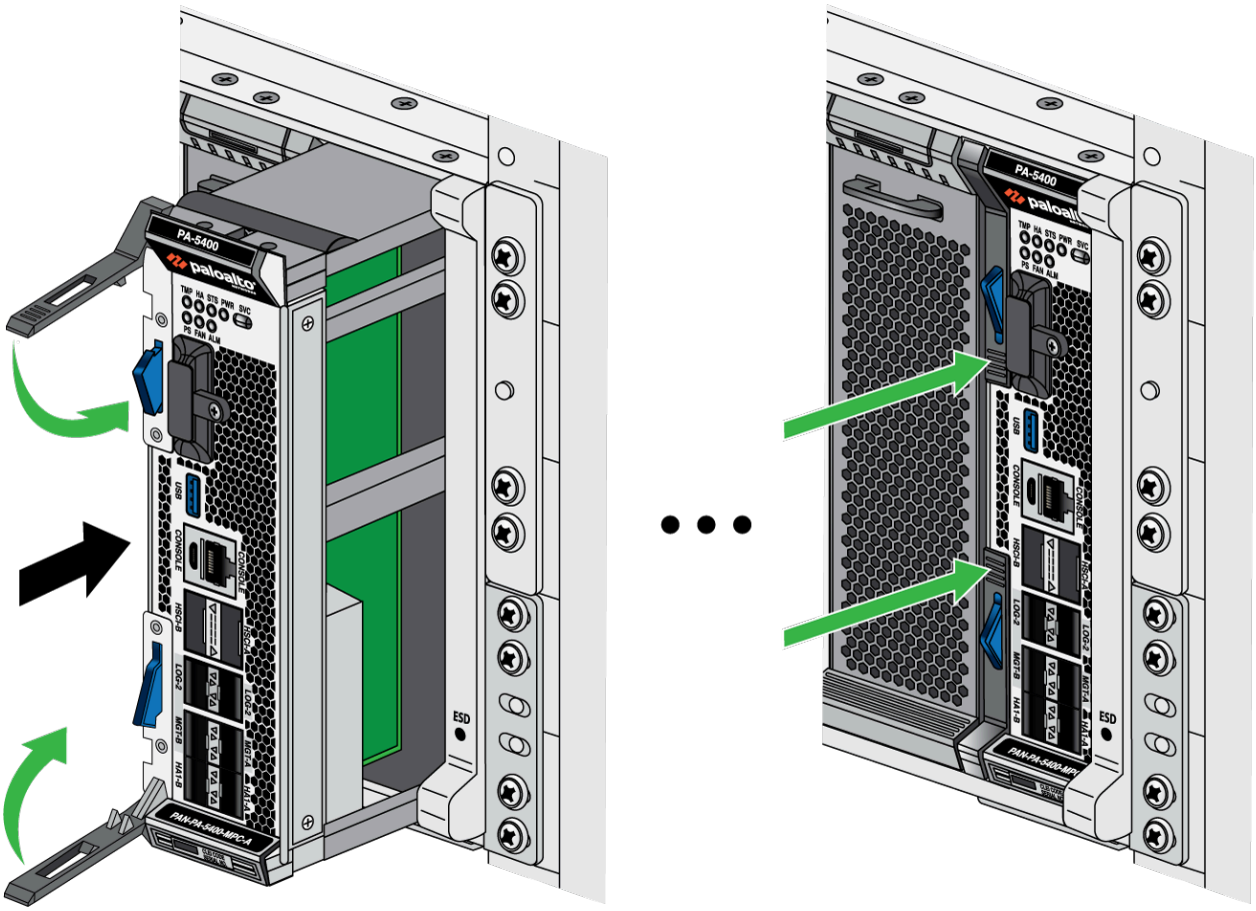
After the firewall is installed and powered on, you can review the available session distribution policies to determine if it makes sense for you to change the default policy to better fit your environment. For details, refer to Session Distribution Policies in the PAN-OS Networking Administrator's Guide.

Install a PA-5400 Series Firewall Data Processor Card (DPC)

STEP 1 | Attach the provided ESD strap to your wrist and plug the other end in to the ESD port location on the front of the appliance. See PA-5450 Front Panel for the location of the ESD port.

STEP 2 | Remove the NC from the antistatic bag. Push the top and bottom ejector tabs towards each other to allow the ejector levers to rotate into an open position.

The image below shows a Management Processor Card (MPC); however, the procedure to install the DPC is the same.



 ©2026 Palo Alto Networks, Inc.

STEP 3 | Rotate the card and align it with the front of the appliance so that the Palo Alto Networks logo is readable at the top of the card. Gently push the DPC into slot 3 until the card reaches the end of the slot.

> *The PA-5450 firewall makes use of paired Logical Card Slots in order to direct processing power from a DPC to a corresponding Networking Card (NC). When installing a DPC, you must install it in the correct slot to pair with the NC.*

STEP 4 | Push on both ejector handles until they lock the card into place.

STEP 5 | (Optional) Repeat Steps 3 through 5 if you wish to install additional DPCs. You may install a DPC into slots 2, 4, 5, and 6.

> *Slot 2 is the only slot that can either house a DPC or a second NC.*

STEP 6 | (If you have unused front slots) Install a blank panel into each unused card slot to help the appliance maintain system air flow. Ensure that the bottom “teeth” of the blank panel fit into the notches on the bottom of the slot. Rotate the blank panel upwards until it snaps at the top of the slot.

©2026 Palo Alto Networks, Inc.

Set Up a Connection to the Firewall

On first startup, the PA-5400 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-5400 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 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 PA-5450 Management Processor Card (MPC) to your computer. Once the firewall is powered on, use a terminal emulator such as PuTTY to access the CLI. See Access the CLI for more information.

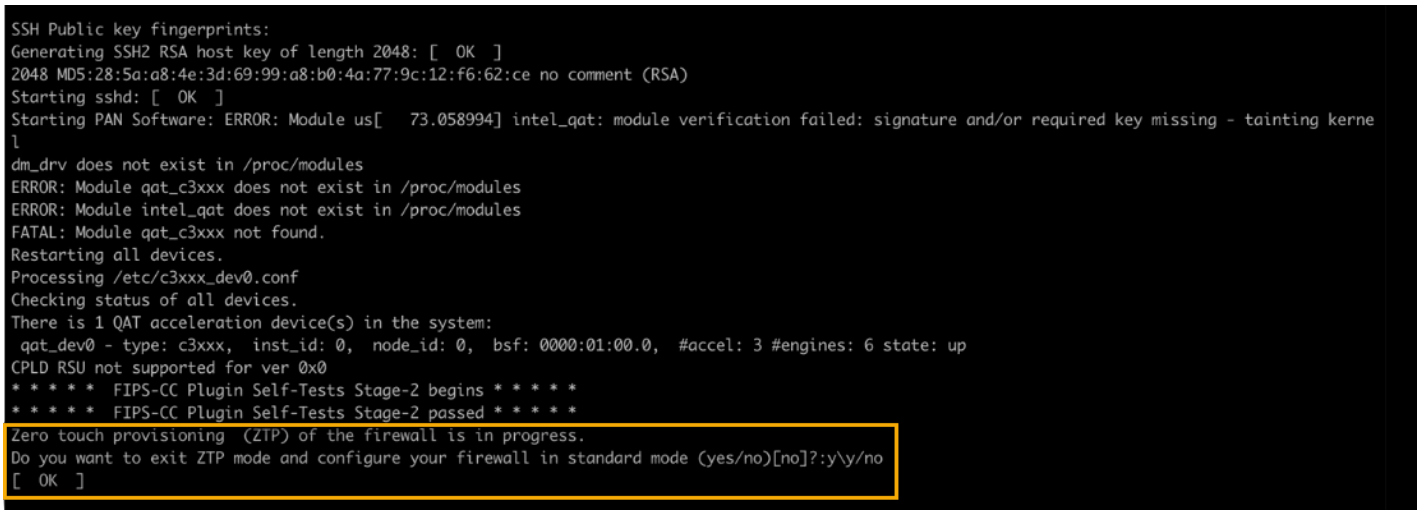
 ©2026 Palo Alto Networks, Inc.

STEP 4 | Power on the firewall. See Connect Power to a PA-5400 Series Firewall to learn how to connect power to the firewall.

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

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

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



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

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

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

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

 ©2026 Palo Alto Networks, Inc.

Connect Power to a PA-5400 Series Firewall

The following topics describe how to connect power to a PA-5400 Series firewall. After you power on the firewall, you can View PA-5400 Series Firewall Power Statistics.

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.

- Connect AC or DC Power to a PA-5400 Series Firewall (PA-5410, PA-5420, PA-5430, PA-5440, and PA-5445)
- Connect AC or DC Power to a PA-5450 Firewall

Connect AC or DC Power to a PA-5400 Series Firewall

The following procedure describes how to connect power to a PA-5410, PA-5420, PA-5430, PA-5440, and PA-5445 firewall with either AC or DC power supplies installed. The AC power supplies support 100 to 240VAC power input and the DC power supplies support 48 to 60VDC power input.

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.

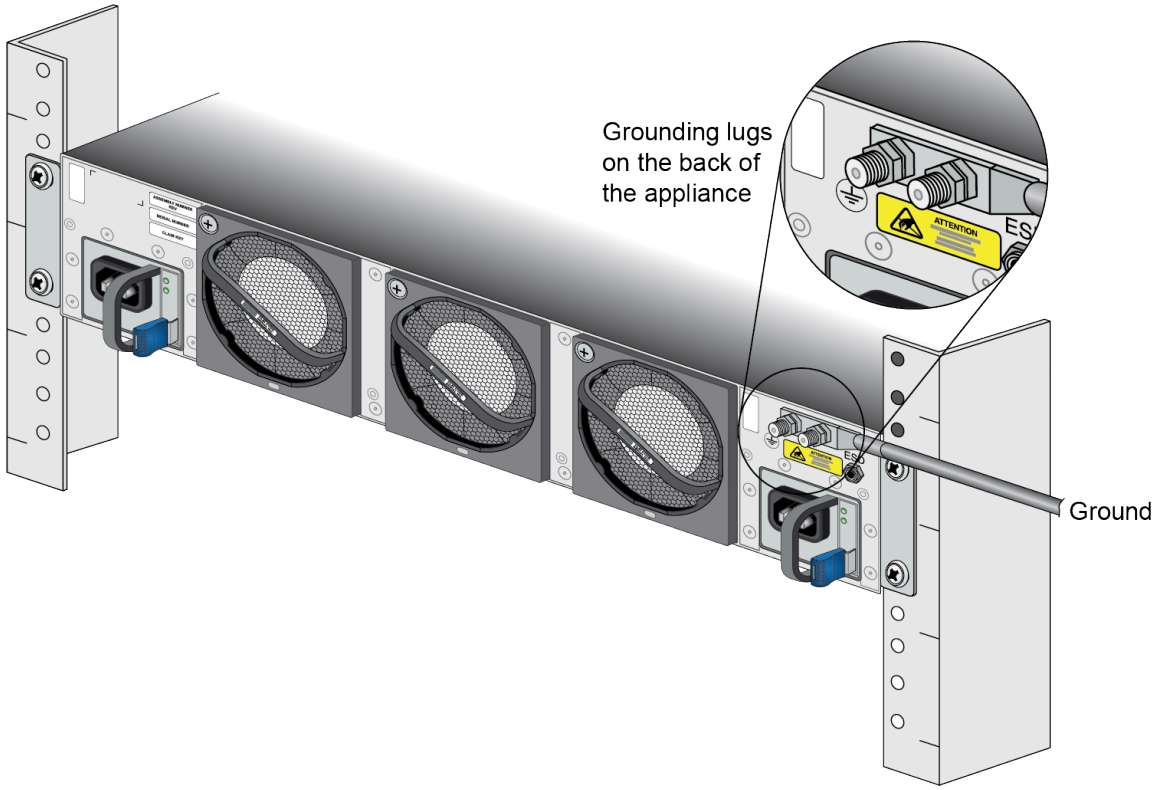
STEP 1 | Read Product Safety Warnings.

STEP 2 | Put the provided ESD wrist strap on your wrist ensuring that the metal contact is touching your skin. Then attach (snap) one end of the ground cable to the wrist strap and remove the alligator clip from the banana clip on the other end of the ESD grounding cable. Plug the banana clip end into one of the ESD ports located on the back of the appliance before handling ESD sensitive hardware. For details on the ESD port location, see PA-5400 Series Back Panel.

STEP 3 | For DC deployments, ensure that your DC power feed is powered off.

©2026 Palo Alto Networks, Inc.

STEP 4 | Remove the four nuts from the ground studs located on the back of the appliance on the upper left side.



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

The crimp tool is not included with the appliance. It is recommended that you use a Panduit CT-3001/ST crimp tool for this procedure. Refer to the manufacturer's specifications for more information.

STEP 6 | Connect the two-post lug connector to the two-post ground studs on the appliance using the provided nuts and torque each nut to 50 in-lbs. Be careful not to strip the nuts and lug studs.

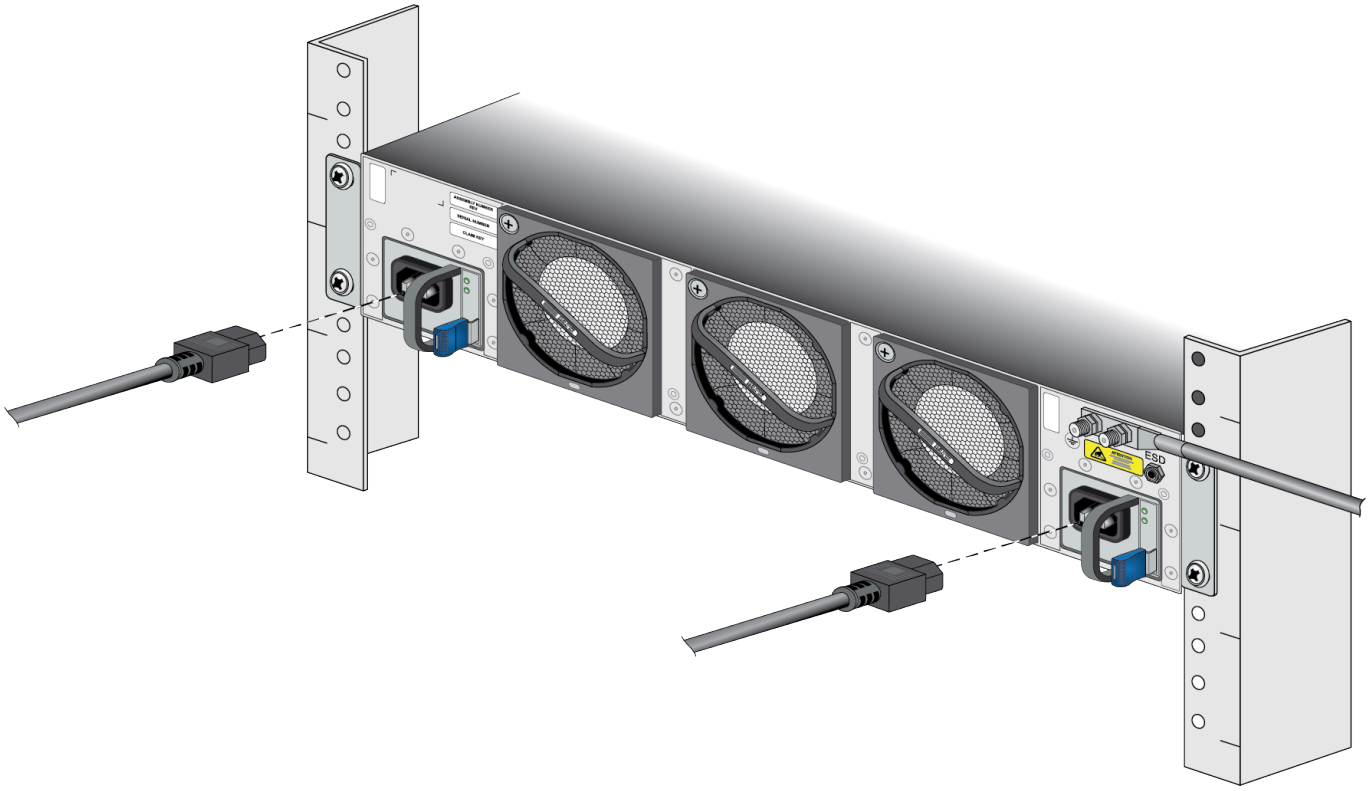
STEP 7 | Connect the power supply to a power source based on whether your power supplies are AC or DC.

(AC Power Supplies only)

1. Connect the first two power supplies to a 120VAC 15-amp circuit breaker or 240VAC 20-amp circuit breaker using the provided power cords and then connect the second two

©2026 Palo Alto Networks, Inc.

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



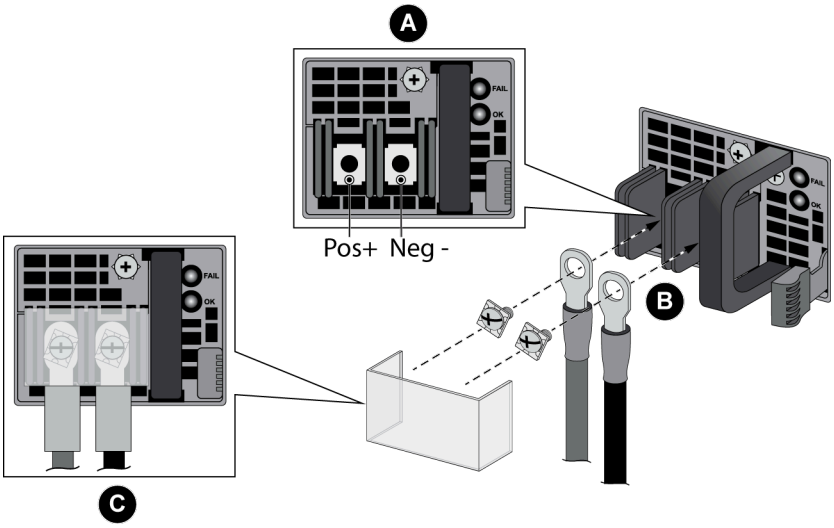
(DC Power Supplies only)

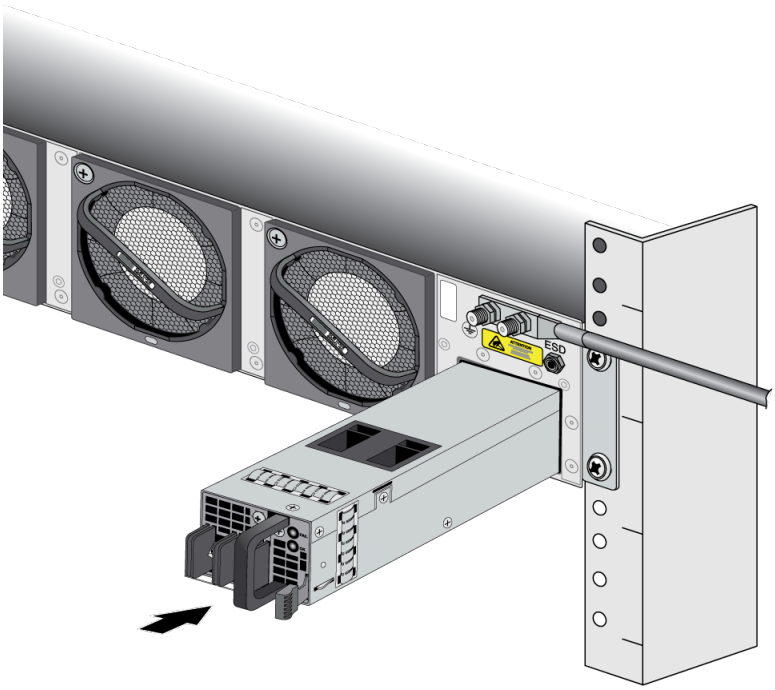
1. Remove the plastic DC power input cover from each of the two DC power supplies and then remove the positive and negative terminal screws.
2. Crimp ring lugs to the ends of the DC cables. These lugs are used to connect the DC cables to the DC inputs on the firewall.
3. Use the DC terminal screws to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

©2026 Palo Alto Networks, Inc.

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 source, ensuring that you observe the correct polarity (positive to positive and negative to negative).

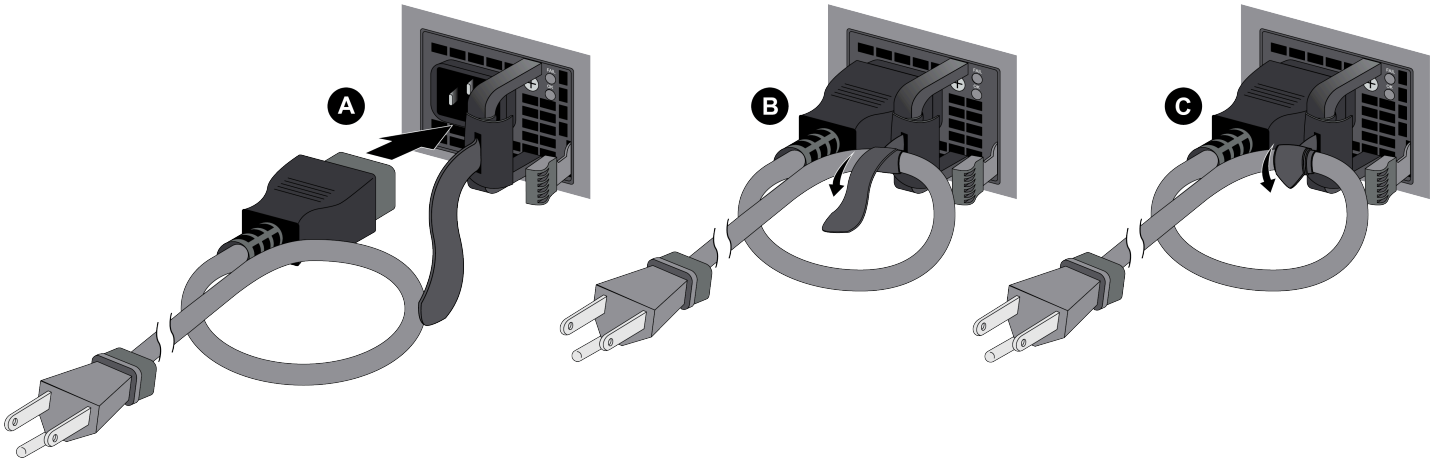




©2026 Palo Alto Networks, Inc.

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

STEP 8 | Secure the power cords to the power inlets using the velcro straps.



STEP 9 | After each AC or DC cable is securely connected, turn on the power source and the appliance will power on.

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

Connect AC or DC Power to a PA-5450 Firewall

The following procedure describes how to connect power to a PA-5450 firewall with either AC or DC power supplies installed. The AC power supplies support 100 to 240VAC power input and the DC power supplies support 48 to 60VDC power input. For details on power requirements, see Determine PA-5450 Firewall Power Configuration Requirements.

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.

STEP 1 | Read Determine PA-5450 Firewall Power Configuration Requirements to ensure that you understand the available power options and that you provide enough power to the firewall based on your configuration.

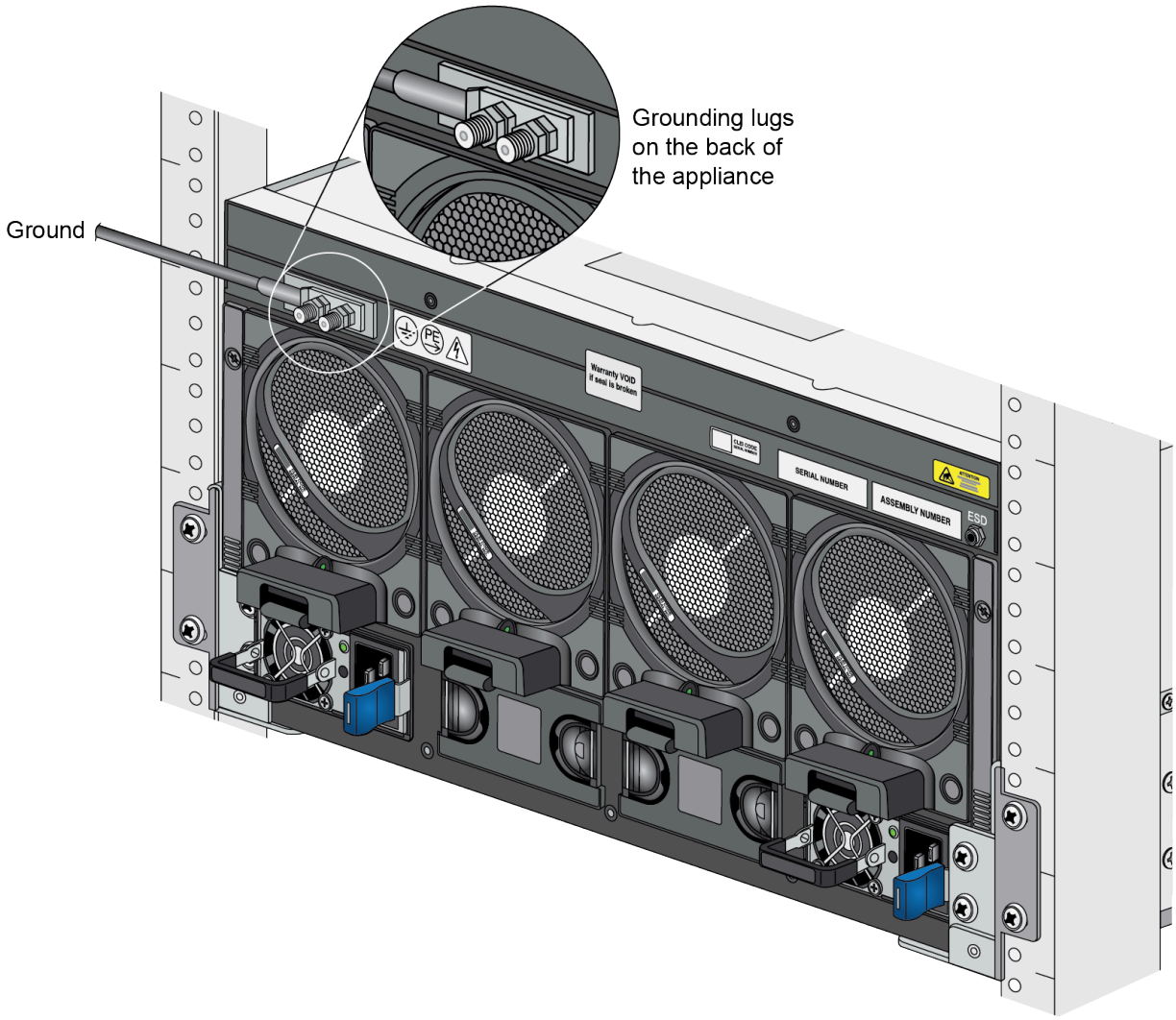
STEP 2 | Read Product Safety Warnings.

STEP 3 | Put the provided ESD wrist strap on your wrist ensuring that the metal contact is touching your skin. Then attach (snap) one end of the ground cable to the wrist strap and remove the alligator clip from the banana clip on the other end of the ESD grounding cable. Plug the banana clip end into one of the ESD ports located on the back of the appliance before handling ESD sensitive hardware. For details on the ESD port location, see PA-5450 Back Panel.

 ©2026 Palo Alto Networks, Inc.

STEP 4 | For DC deployments, ensure that your DC power feed is powered off.

STEP 5 | Remove the four nuts from the ground studs located on the back of the appliance on the upper left side.



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

The crimp tool is not included with the appliance. It is recommended that you use a Panduit CT-3001/ST crimp tool for this procedure. Refer to the manufacturer's specifications for more information.

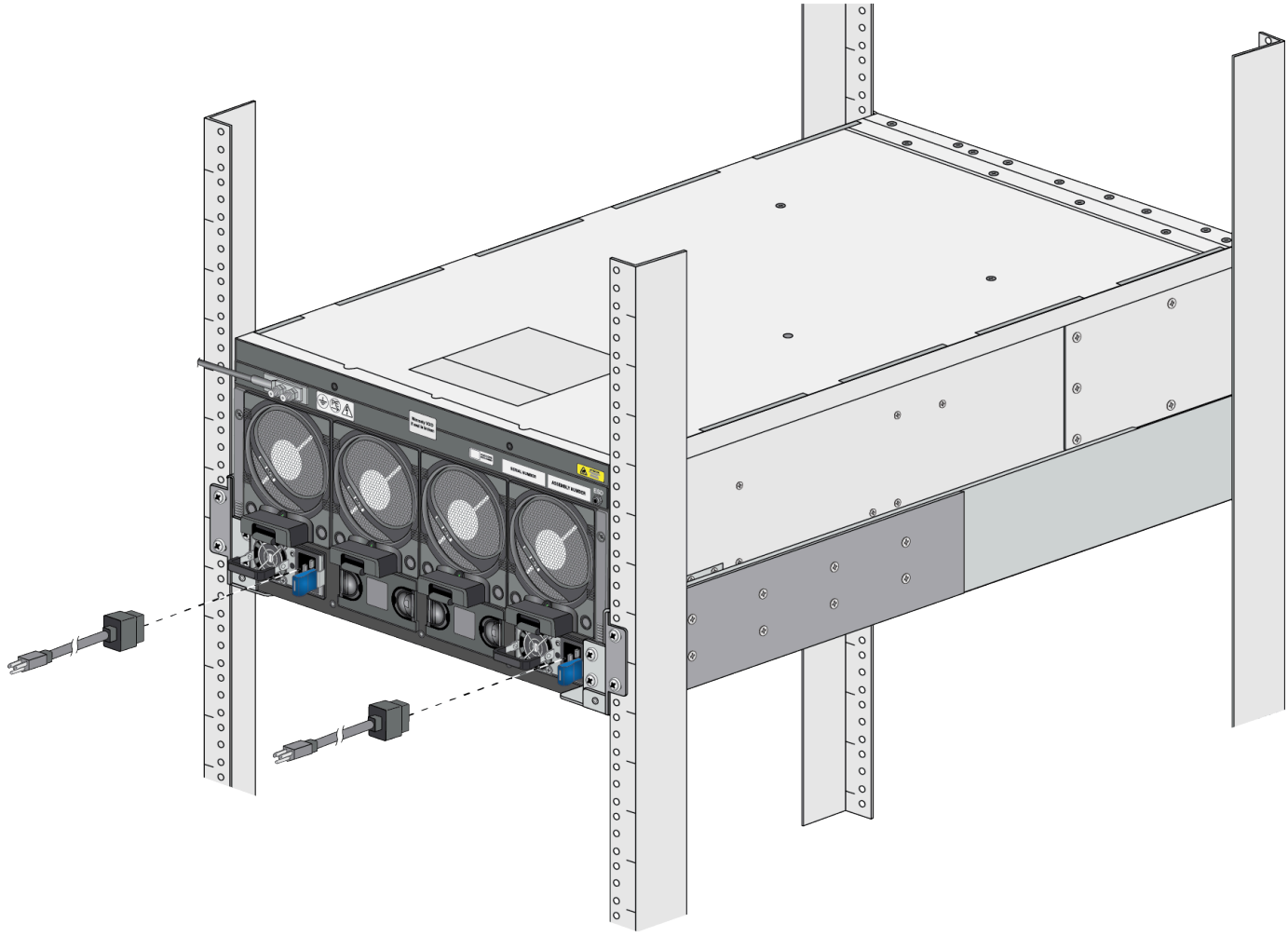
STEP 7 | Connect the two-post lug connector to the two-post ground studs on the appliance using the provided nuts and torque each nut to 50 in-lbs. Be careful not to strip the nuts and lug studs.

©2026 Palo Alto Networks, Inc.

STEP 8 | Connect the power supply to a power source based on whether your power supplies are AC or DC.

(AC Power Supplies only)

1. Connect the first two power supplies to a 120VAC 15-amp circuit breaker or 240VAC 20-amp circuit breaker using the provided power cords and then connect the second two power supplies to a second, independent 120VAC 15-amp circuit breaker or 240VAC 20-amp circuit breaker.



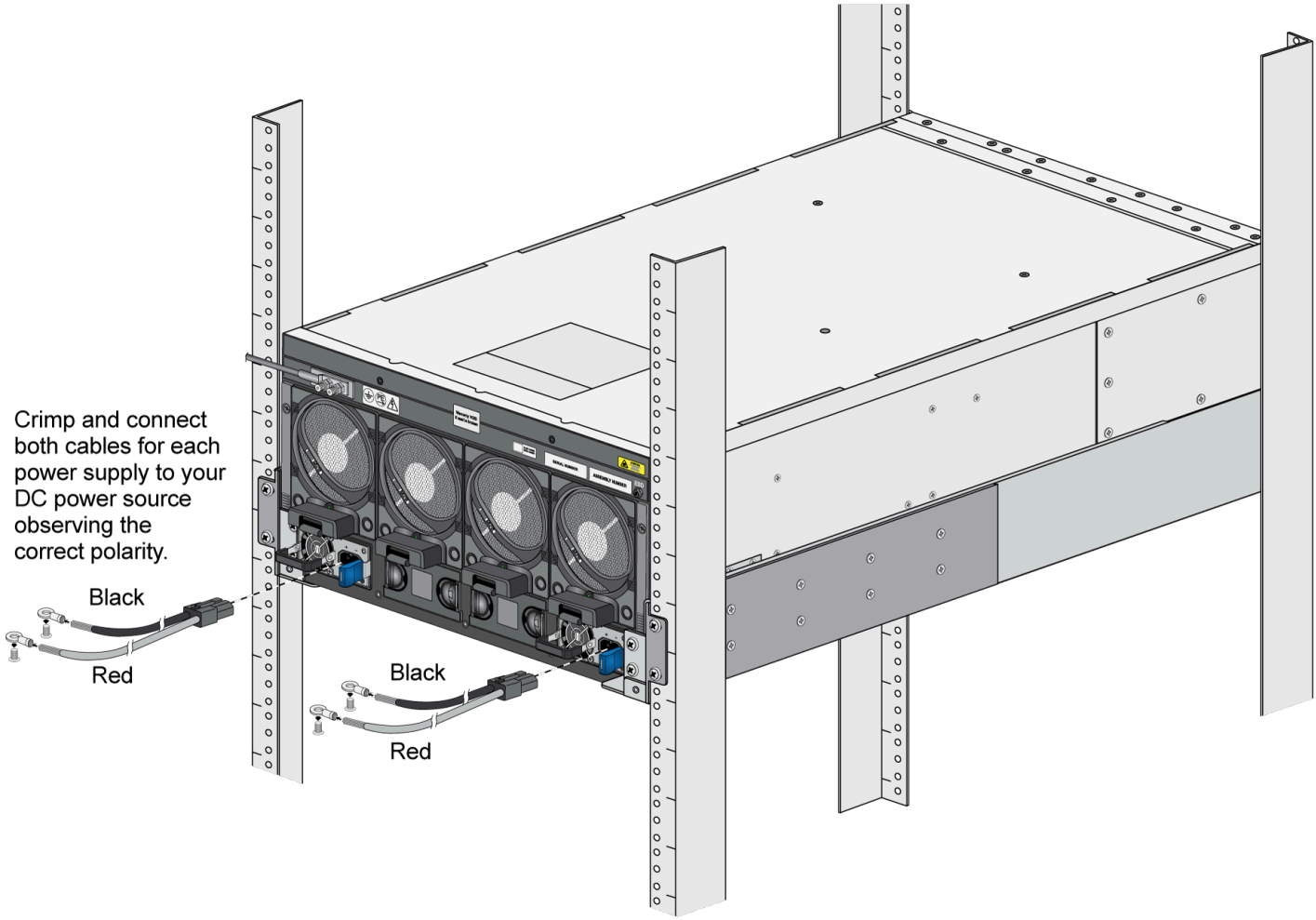
2. Secure the power cords to the power inlets using the power cord retainer clips.

(DC Power Supplies only)

1. Prepare the DC power cable by crimping the bare wire ends of the cables using lugs (not included) designed for your DC power source. Each cable dongle has one red wire and one black wire. Connect the red wire to the DC negative (-48VDC) terminal of your DC power source. Connect the black wire to the DC positive (RTN) terminal of your DC power source. Do this for each of the four power supplies, ensuring that the first two power supplies on the left are connected to one power circuit breaker and the second pair on the right is

 ©2026 Palo Alto Networks, Inc.

connected to a different circuit breaker. This ensures power redundancy and allows for planned electrical circuit maintenance.



2. Connect the other ends of the DC cables to the front of the DC power supplies by pushing the plastic connector into the DC power supply until it clicks into place. Ensure that you connect each pair of power supplies to a different circuit breaker.

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

STEP 9 | Confirm that all front slot cards are properly inserted.

STEP 10 | After each AC or DC cable is securely connected, turn on the power source and the appliance will power on.

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

©2026 Palo Alto Networks, Inc.

Determine PA-5450 Firewall Power Configuration Requirements

At least one active AC or DC power supply is required to operate a PA-5400 Series firewall. Factors that can change your power requirements are the number of Networking Cards (NCs) and Data Processor Cards (DPCs) used and your power redundancy requirement.

To determine the number of active power supplies required to operate the appliance, refer to PA-5400 Series Power Supply Chart and locate your model and power input type and then locate the column that coincides with the number of installed DPCs. Each power supply requirement in the table accounts for the installation of 1 or 2 NCs. To provide full redundancy, install double the minimum number of power supplies specified in the table. A fully redundant power configuration means that half of the installed power supplies can fail and the appliance and installed NCs and DPCs will still function.

Table 1: PA-5450 Power Supply Chart

Model and Power Input	Front Cards Installed and Active Power Supplies Required				
	1 DPC	2 DPCs	3 DPCs	4 DPCs	5 DPCs
PA-5450 Firewall 110/120VAC	2	2	3	3	3
PA-5450 Firewall 240VAC or -48VDC	1	1	2	2	2

All power supply requirements in the table above account for 1 or 2 NCs being installed in the appliance.

You can find power information for PA-5450 hardware components in PA-5450 Firewall Component Electrical Specifications. To view power statistics on an active PA-5450, see View PA-5400 Series Firewall Power Statistics.

After you determine the power requirements for your firewall, see Connect Power to a PA-5400 Series Firewall and select the topic for your model and power type.

View PA-5400 Series Firewall Power Statistics

Use the following information to learn how to view active power statistics on a PA-5400 Series firewall to help you ensure power redundancy and to plan for growth. You can view the amount of power that each power supply is producing as well as the power rating for each hardware component.

This information will also help you Determine PA-5450 Firewall Power Configuration Requirements.

*The power numbers provided by the **`show chassis power`** command represent power calculated by the firewall power management software and does not represent the exact measured power. The difference allows margin for thermal conditions and component aging factors. This CLI output helps you know how much power is required to prevent the appliance from overloading under extreme conditions.*

©2026 Palo Alto Networks, Inc.

STEP 1 | Using a terminal emulator, such as PuTTY, launch an SSH session to the firewall.

Run the following command:

```
admin@PA-5450> show chassis power
```

STEP 2 | View the output for information on the status of each component and the current power rating.

For example, the following table shows the CLI output (in table format) from a PA-5450 with three power supplies installed. The output shows each front slot (1 to 7), the installed power supplies and fan trays, the status of each component, the rated power consumption for each component, and the amount of power produced by each power supply. The power supplies are labeled PS1 to PS4.

Example Power Output from a PA-5450 Firewall

Slot	Component	Card Status	Power (w)
Base Card	PA-5400-BC-A	Up	195
1	PA-5400-NC-A	Up	100
2	PA-5400-NC-A	Up	100
3	empty		
4	PA-5400-DPC-A	Up	335
5	empty		
6	empty		
7	PA-5400-MPC-A	Up	152
FANTRAY 1	PA-5450-FAN	Present	193
FANTRAY 2	PA-5450-FAN	Present	193
FANTRAY 3	PA-5450-FAN	Present	193

 ©2026 Palo Alto Networks, Inc.

Slot	Component	Card Status	Power (w)
FANTRAY 4	PA-5450-FAN	Present	193
PS1	PAN-PWR-2200W-AC	OK	2200 (+)
PS2	PAN-PWR-2200W-AC	OK	2200 (+)
PS3	empty	empty	
PS4	PAN-PWR-2200W-AC	OK	2200 (+)
	Provided: Used: Remaining		6600 1654 4946

As indicated in the last row of the table, the three 2200 watt power supplies provide 6600 watts and the installed hardware components (BC, MPC, DPC, NCs, and fans) use 1654 watts. If you subtract 1654 from 6600, there are 4946 watts of power remaining.

©2026 Palo Alto Networks, Inc.

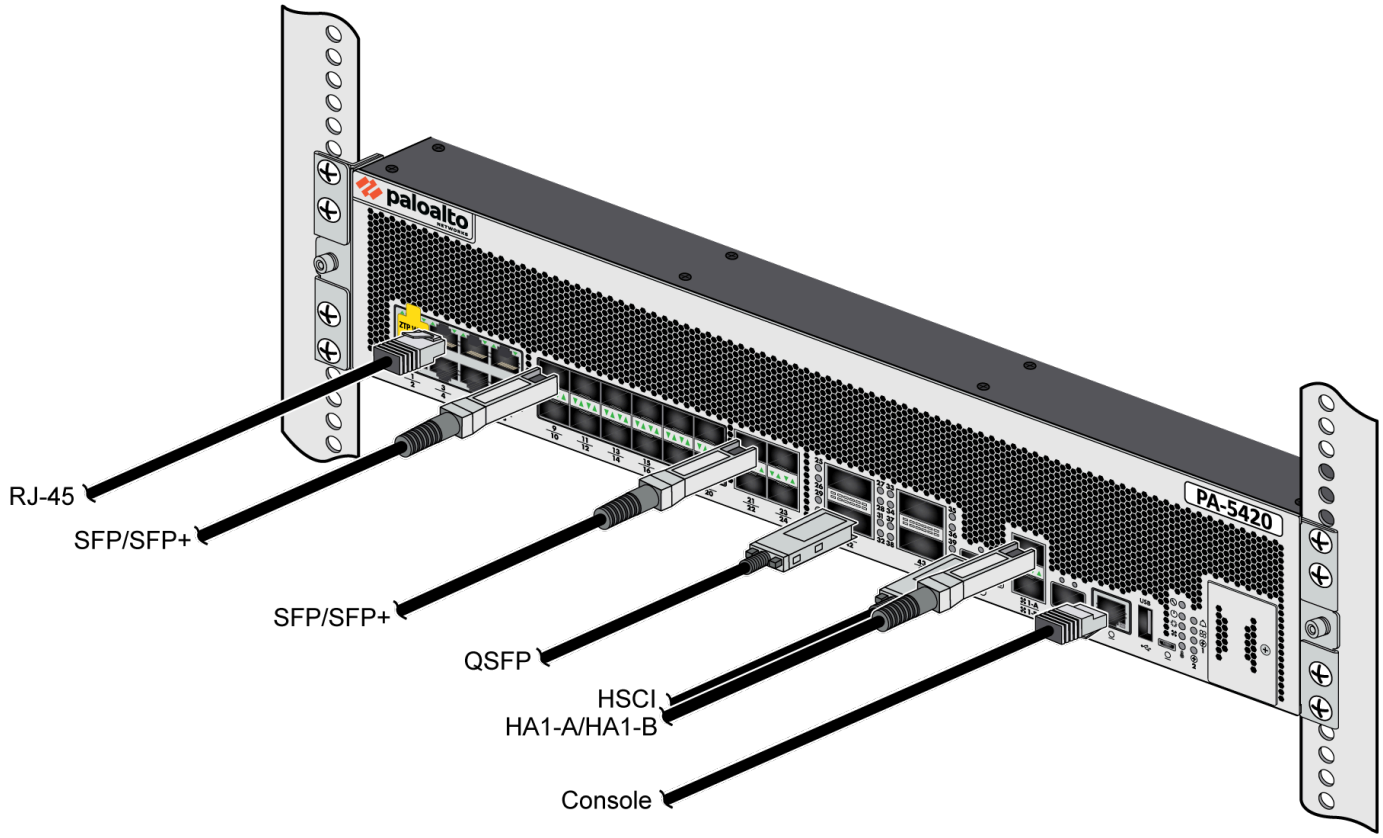
Connect Cables to a PA-5400 Series Firewall

After you Connect Power to a PA-5400 Series Firewall, connect your management computer to the management port (MGT) 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).

In PA-5410, PA-5420, PA-5430, PA-5440, and PA-5445 firewalls, the MGT and console ports are located on the front panel of the device. In the PA-5450 firewall, both the MGT and console ports are located on the Management Processor Card (MPC). You then configure the ethernet ports on the front of the device or on the Networking Card (NC) depending on which PA-5400 Series firewall you have. Finally, you connect these ports to your switch or router.

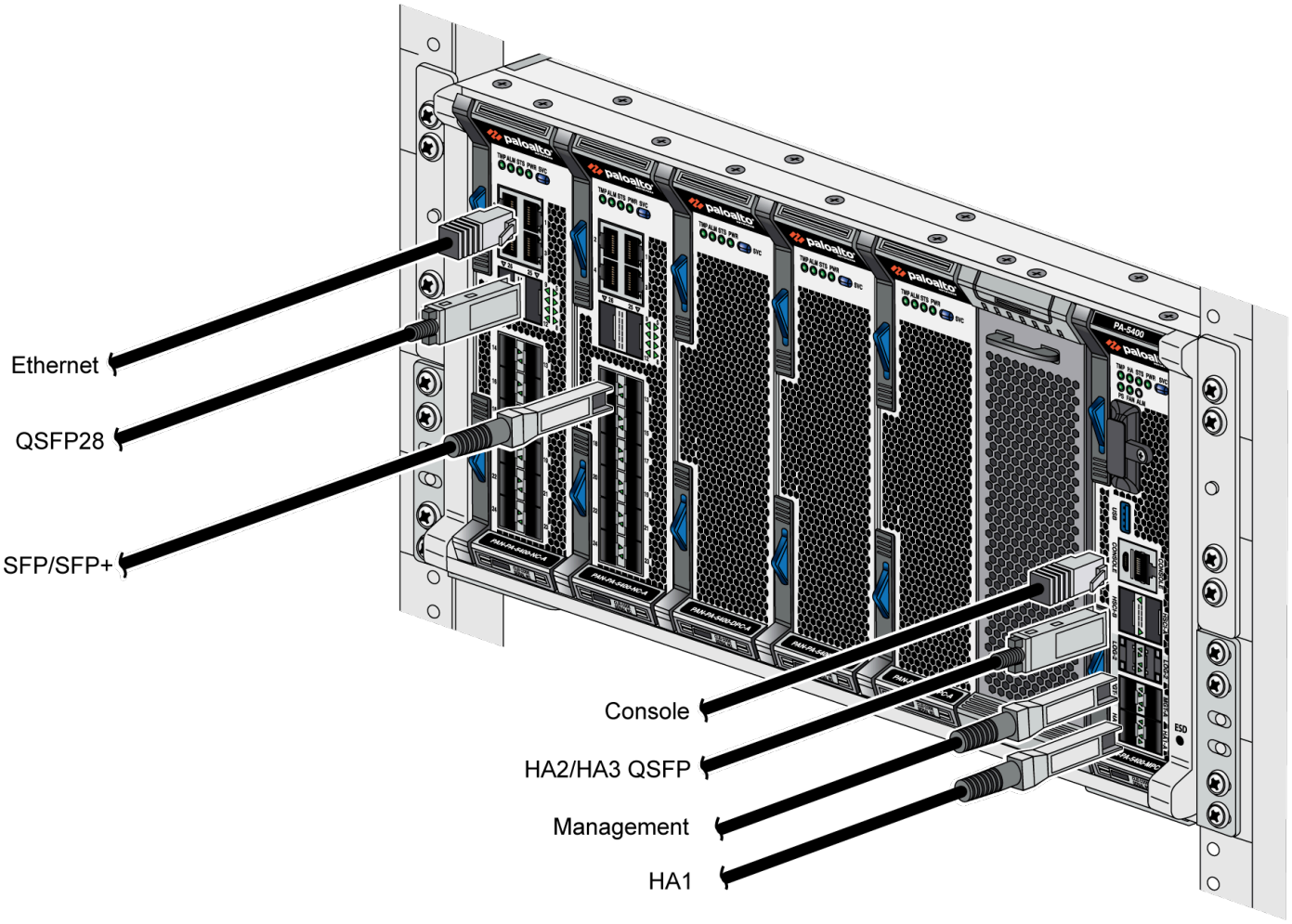
If you install two matching firewalls in a high availability configuration, you will also connect HA cables between the two appliances (see HA Links and Backup Links).

The following image shows the PA-5410, PA-5420, PA-5430, PA-5440, and PA-5445 cable connections.



The next image shows the PA-5450 firewall cable connections.

©2026 Palo Alto Networks, Inc.



 ©2026 Palo Alto Networks, Inc.

Verify the PA-5450 Firewall NC Configuration

When you first set up a PA-5450, both NC slots are ready to use. If you are working with a firewall that is already deployed, you should check slot status before adding a new NC to ensure that the NC slot is ready. If the firewall is in a high availability (HA) configuration, a newly installed NC stays in a disabled state until a matching NC is installed. After you install a matching NC in the same slot number in the HA peer firewall, you must enable the NCs.

The following commands describe how to view NC status and how to change the state of an NC.

The PA-5450 firewall makes use of paired Logical Card Slots in order to direct processing power from a Data Processing Card (DPC) to a corresponding NC. Certain commands issued to the NC affect or are affected by the status of its corresponding DPC.

To view NC status, run the following command:

```
admin@PA-5450> show chassis status slot <slot-number>
```

For example, to view the status of slot 2 run the following command:

```
admin@PA-5450> show chassis status slot s2
```

If an NC slot is ready to use, the status shows `empty`. When you insert an NC, the system updates the status of the slot.

After you successfully install an NC, the status shows `CardStatus Up` and `Config Status Success`.

You can power down a slot and the slot will stay in the down state until you power it on. Use the following commands to change the slot status:

To power on an NC slot:

```
admin@PA-5450> request chassis admin-power-on slot <slot-number>
```

To power off an NC slot:

```
admin@PA-5450> request chassis admin-power-off slot <slot-number>
```

To temporarily power down a slot:

```
admin@PA-5450> request chassis power-off slot <slot-number>
```

In an HA configuration, you must install the same number and model of NCs in each appliance and the slot numbers must match. After you install the NCs in each appliance, the firewall keeps them in a disabled state until you enable them. This allows the firewall to start HA monitoring on both NCs.

Use the following command to bring up a pair of NCs in an HA configuration:

 ©2026 Palo Alto Networks, Inc.

```
admin@PA-5450> request chassis power-on slot <slot-number> target ha-
pair
```

For example, to enable NCs installed in slot 2 of both appliances, run the following command:

```
admin@PA-5450> request chassis power-on slot s2 target ha-pair
```

For information on installing NCs, see Install a PA-5400 Series Firewall Networking Card (NC).

©2026 Palo Alto Networks, Inc.

©2026 Palo Alto Networks, Inc.

Service the PA-5400 Series Firewall Hardware

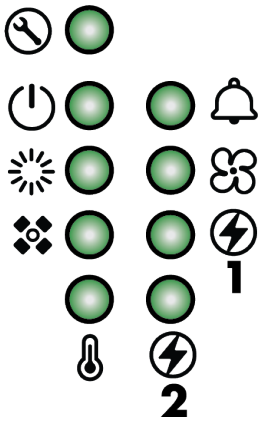
The following topics describes how to interpret LED information and replace field-serviceable components on a PA-5400 Series firewall. For an overview of the hardware components, see PA-5400 Series Firewall Overview.

- Interpret the PA-5400 Series LEDs
- Identify PA-5400 Series Port Activity and Link LEDs
- Replace a PA-5400 Series Firewall AC or DC Power Supply
- Replace a PA-5400 Series Base Card (BC) (PA-5450 only)
- Replace a PA-5400 Series Firewall Fan Assembly
- Replace a PA-5400 Series Firewall Front Slot Card (PA-5450 only)
- Install an MPC Logging Drive (PA-5450 only)
- Replace a System Drive

Interpret the PA-5400 Series LEDs

The following table describes how to interpret the status LEDs on a PA-5410, PA-5420, PA-5430, PA-5440, and PA-5445 firewall.

The PA-5450 LEDs are located on the interface cards. For more information, see PA-5400 Series Firewall Module and Interface Card Information.



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. • **Off**—The firewall is not powered on.
	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.

 ©2026 Palo Alto Networks, Inc.

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-5400 Series Firewall 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**—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 (PWR 1) is on the left and power supply 2 (PWR 2) is on the right. • **Green**—The power supply is functioning normally. • **Red**—The power supply is present but is not working. • **Off**—The power supply is not installed
Ethernet Port LEDs	
RJ-45	These ports have one green LED each. • **Solid Green**—The firewall network link is up. • **Blinking Green**—The firewall is processing network activity.

©2026 Palo Alto Networks, Inc.

LED	Description
SFP+, HA1-A and HA-1B, and Management port	These ports have two LEDs each. The color of the LED differs based on the port speed. 1G—Yellow 10G—Green
SFP28 and QSFP28	The SFP28 ports have two LEDs each. The QSFP28 ports have one or four corresponding LEDs each depending on if the ports are broken out or not. The color of the LED differs based on the port speed. 1G—Yellow 10G—Green 25G—Green & Blue 40G—Yellow 100G—Blue • **Solid Color**—The firewall network link is up. • **Blinking Color**—The firewall is processing network activity.
Back Panel LEDs	

Power supply LEDs
In AC power supplies, the input LED indicates the status of the AC input power and the output LED indicates the DC output that powers the firewall. In DC power supplies, the input and output are both DC.
	The AC and DC power supplies have a FAIL and an OK LED. The LED behavior varies based on which power supply model you have.
	Power Supply (with black handle)
	• FAIL
	  • Off—The power supply is operating normally.
	  • Solid Yellow—The power supply failed. This can also indicate a fan failure or overheating condition.
	  • Blinking Yellow—The power supply is outside of tolerance levels.
	• OK
	  • Solid Green—The power supply is operating normally.
	  • Blinking Green—The power input is present but the power supply is disabled by the system.
	  • Off—No power input or the power supply failed.
	Power Supply (with red handle)

 ©2026 Palo Alto Networks, Inc.

LED	Description

	• FAIL (Bottom/DC LED)
	  • Solid Green—The power supply is operating normally.
	  • Solid Yellow—The power supply failed. This can also indicate a fan failure or overheating condition.
	  • Blinking Yellow & Green (Alternating at 2:1 ratio)—The power supply is at high temperature.
	• OK (Top/AC LED)
	  • Solid Green—The power supply is operating normally.
	  • Blinking Yellow—The power input is present but the power supply is disabled by the system.
	  • Off—No power input or the power supply failed.

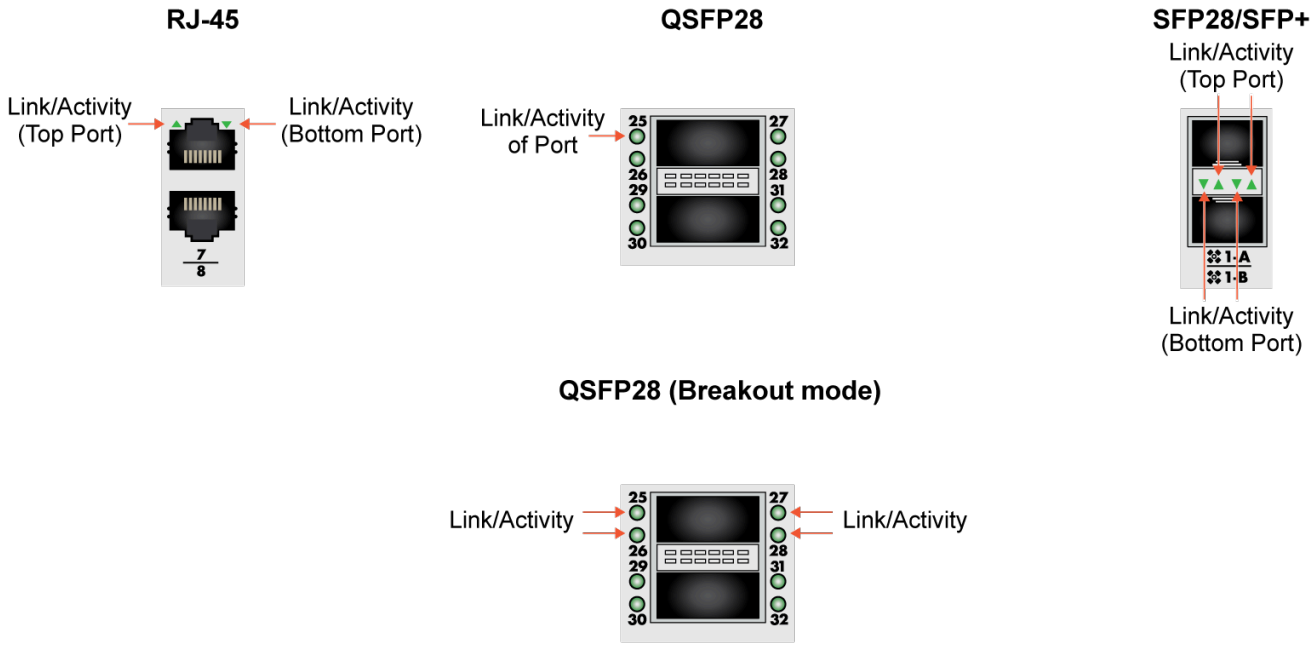
Fan Assembly LED	• **Green**—The fan trays and all fans are operating normally. • **Red**—A fan in the fan tray failed (see Replace a PA-5400 Series Firewall Fan Assembly).

 ©2026 Palo Alto Networks, Inc.

Identify PA-5400 Series Port Activity and Link LEDs

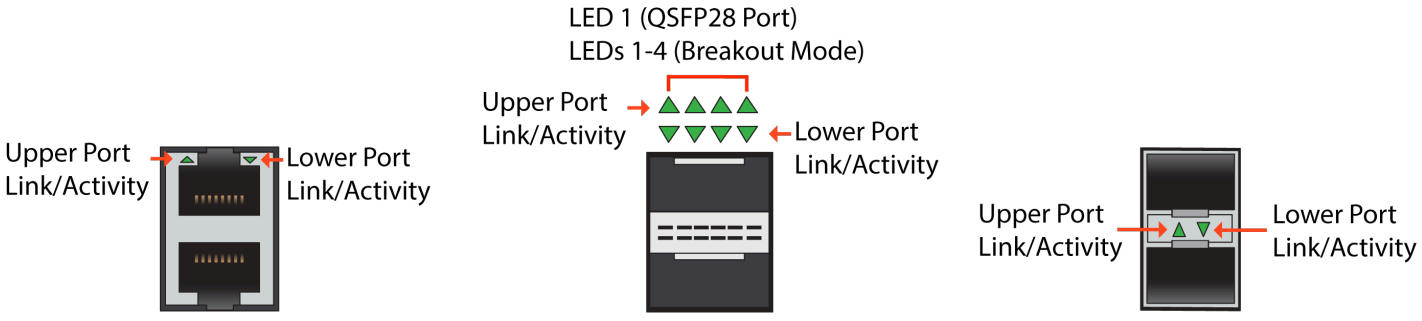
The following image shows how to identify the activity and link LEDs of the port types available on the PA-5400 Series firewalls (PA-5410, PA-5420, PA-5430, PA-5440, and PA-5445) or the PA-5450 NCs (Networking Cards). For details on the functions and states of the LEDS, see Interpret the PA-5400 Series LEDs if you have a PA-5410, PA-5420, PA-5430, PA-5440, or PA-5445. See Interpret the PA-5400 NC-A LEDs if you have a PA-5450 NC.

PA-5410, PA-5420, PA-5430, PA-5440, and PA-5445 port LEDs



In the QSFP28 ports pictured above, LEDs 25 through 28 are mapped to port 41, LEDs 29 through 32 are mapped to port 42, LEDs 33 through 36 are mapped to port 43, and LEDs 37 through 40 are mapped to port 44. Refer to the PA-5400 Series Front Panel for more information.

PA-5450 NC port LEDs



©2026 Palo Alto Networks, Inc.

Replace a PA-5400 Series Firewall AC or DC Power Supply

The following topics describe how to interpret the power supply LEDs and how to replace a PA-5400 Series firewall power supply.

- Interpret the PA-5400 Series Firewall Power Supply LEDs
- Replace a PA-5400 Series Firewall AC or DC Power Supply (PA-5410, PA-5420, PA-5430, PA-5440, and PA-5445)
- Replace a PA-5450 AC or DC Power Supply

Interpret the PA-5400 Series Firewall Power Supply LEDs

Use the two following tables to learn how to interpret the LEDs on a PA-5400 Series firewall (PA-5410, PA-5420, PA-5430, PA-5440, and PA-5445) AC or DC power supply. The table you refer to depends on the color of the handle of your power supply.

Both the AC and DC power supplies have two LEDS — FAIL and OK.

Power Supply (Black Handle)	
FAIL	• Off—The power supply is operating normally. • Solid yellow—The power supply failed. This can also indicate a fan failure or overheating condition. • Blinking yellow—The power supply is outside of tolerance levels.
OK	• Solid green—The power supply is operating normally. • Blinking green—The power input is present but the power supply is disabled by the system. • Off—No power input or the power supply failed.

Power Supply (Red Handle)	
FAIL (Bottom/DC LED)	• Solid green—The power supply is operating normally.

©2026 Palo Alto Networks, Inc.

	• Solid yellow—The power supply failed. This can also indicate a fan failure or overheating condition. • Blinking yellow and green (Alternating at 2:1 ratio)—The power supply is at high temperature.
OK(Top/AC LED)	• Solid green—The power supply is operating normally. • Blinking yellow—The power input is present but the power supply is disabled by the system. • Off—No power input or the power supply failed.

The PA-5450 has one power supply for AC power and one for DC power. Use the two following tables to learn how to interpret the single LED on a PA-5450 AC and DC power supply.

AC Power Supply	
Solid Green	Power output is on.
Blinking Green (0.5Hz)	Standby mode. AC power is present but only at 12VSB (Volts Standby).
Blinking Green (2Hz)	Power supply is in redundant state or in sleep mode.
Solid Yellow	Power supply critical failure.
Off	No AC power or AC power cord is unplugged.

DC Power Supply	
Solid Green	Power output is on.
Blinking Green (0.5Hz)	Standby mode. DC power is present but only at 12VSB (Volts Standby).
Blinking Green (1Hz)	Power supply warning such as high temperature, high current, or slow fan.
Blinking Green (2Hz)	Power supply is in standby state.
Solid Yellow	Power supply critical failure.

©2026 Palo Alto Networks, Inc.

Off	No DC power.

Replace a PA-5400 Series Firewall AC or DC Power Supply

The following instructions describe how to replace a power supply in a PA-5410, PA-5420, PA-5430, PA-5440, and PA-5445 firewall.

STEP 1 | Put the provided ESD wrist strap on your wrist ensuring that the metal contact is touching your skin. Then attach (snap) one end of the ground cable to the wrist strap and remove the alligator clip from the banana clip on the other end of the ESD grounding cable. Plug the banana clip end into one of the ESD ports located on the back of the appliance before handling ESD sensitive hardware. For details on the ESD port location, see PA-5400 Series Back Panel.

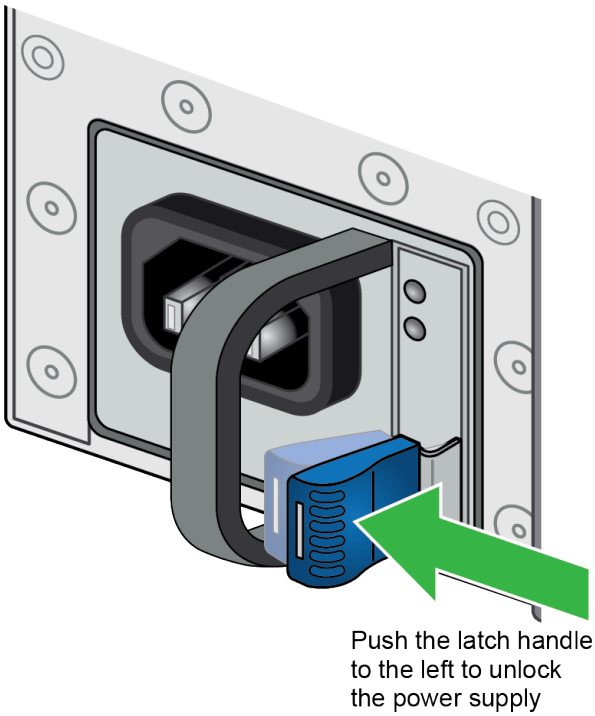
STEP 2 | Locate the failed power supply by viewing the system logs or by viewing the LED on the front of the power supply. A red LED indicates a failed power supply. For details on the power supply LEDs, see Interpret the PA-5400 Series Firewall Power Supply LEDs.

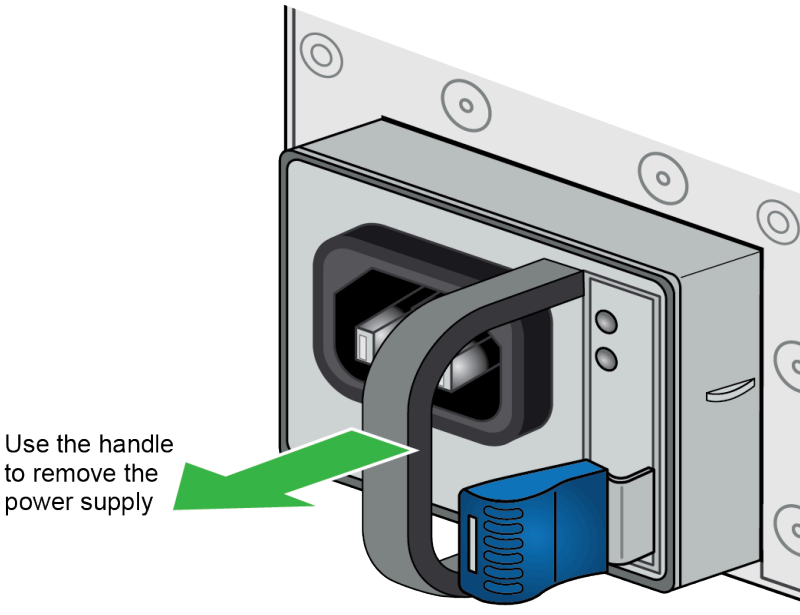
STEP 3 | Shut off power to the failed power supply.

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

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

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





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

 ©2026 Palo Alto Networks, Inc.

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

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

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

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

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

Replace a PA-5450 AC or DC Power Supply

STEP 1 | Put the provided ESD wrist strap on your wrist ensuring that the metal contact is touching your skin. Then attach (snap) one end of the ground cable to the wrist strap and remove the alligator clip from the banana clip on the other end of the ESD grounding cable. Plug the banana clip end into one of the ESD ports located on the back of the appliance before handling ESD sensitive hardware. For details on the ESD port location, see PA-5450 Back Panel.

STEP 2 | Locate the failed power supply by viewing the system logs or by viewing the LED on the front of the power supply. A red LED indicates a failed power supply. For details on the power supply LEDs, see Interpret the PA-5400 Series Firewall Power Supply LEDs.

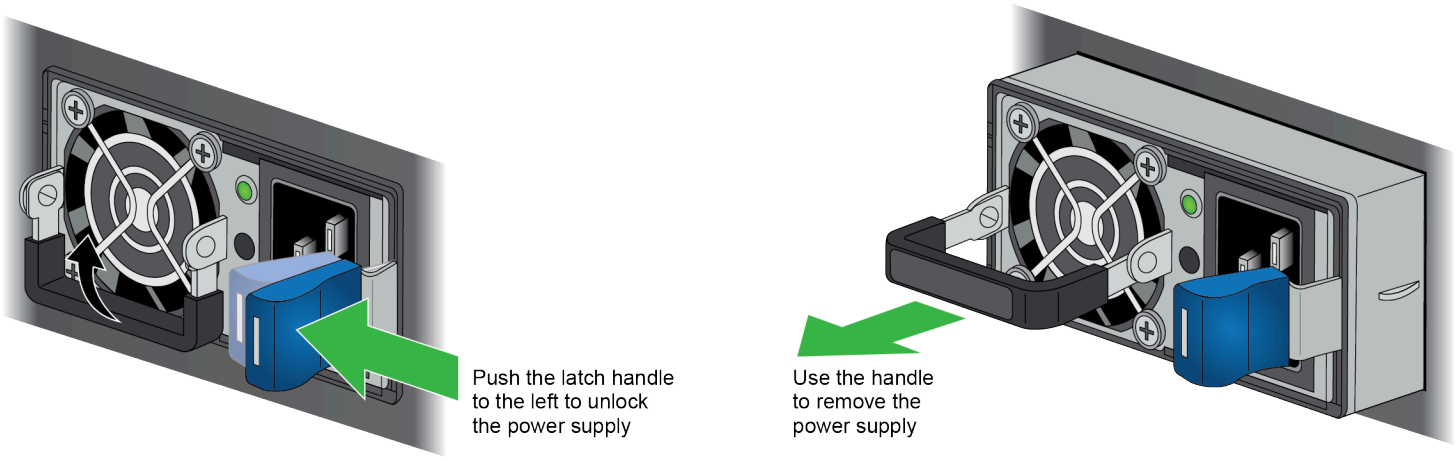
STEP 3 | Shut off power to the failed power supply.

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

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

 ©2026 Palo Alto Networks, Inc.

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



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

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

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

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

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

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

©2026 Palo Alto Networks, Inc.

Replace a PA-5400 Series Base Card (BC)

The PA-5400 Series Base Card (BC) is not hot-swappable. In the case of a failure, you must power off the appliance and disconnect all power sources before removing the BC.

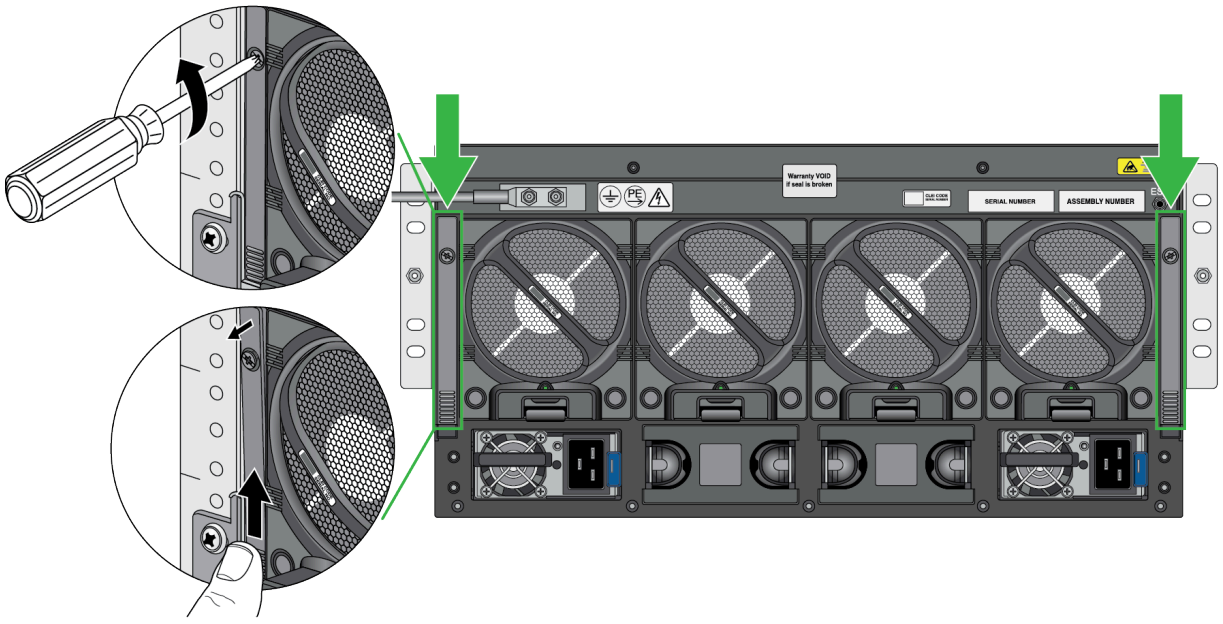
- Replace a PA-5450 Base Card (BC)

Replace a PA-5450 Base Card (BC)

STEP 1 | Put the provided ESD wrist strap on your wrist ensuring that the metal contact is touching your skin. Then attach (snap) one end of the ground cable to the wrist strap and remove the alligator clip from the banana clip on the other end of the ESD grounding cable. Plug the banana clip end into one of the ESD ports located on the back of the appliance before handling ESD sensitive hardware. For details on the ESD port location, see PA-5450 Back Panel.

STEP 2 | Ensure that the PA-5450 is powered off and that the fans are not still spinning.

STEP 3 | Loosen the two screws on the fan drawer ejector handles (one on either side). Place your thumbs on the bottom of the ejector handles and push until the ejector handles swing outward.

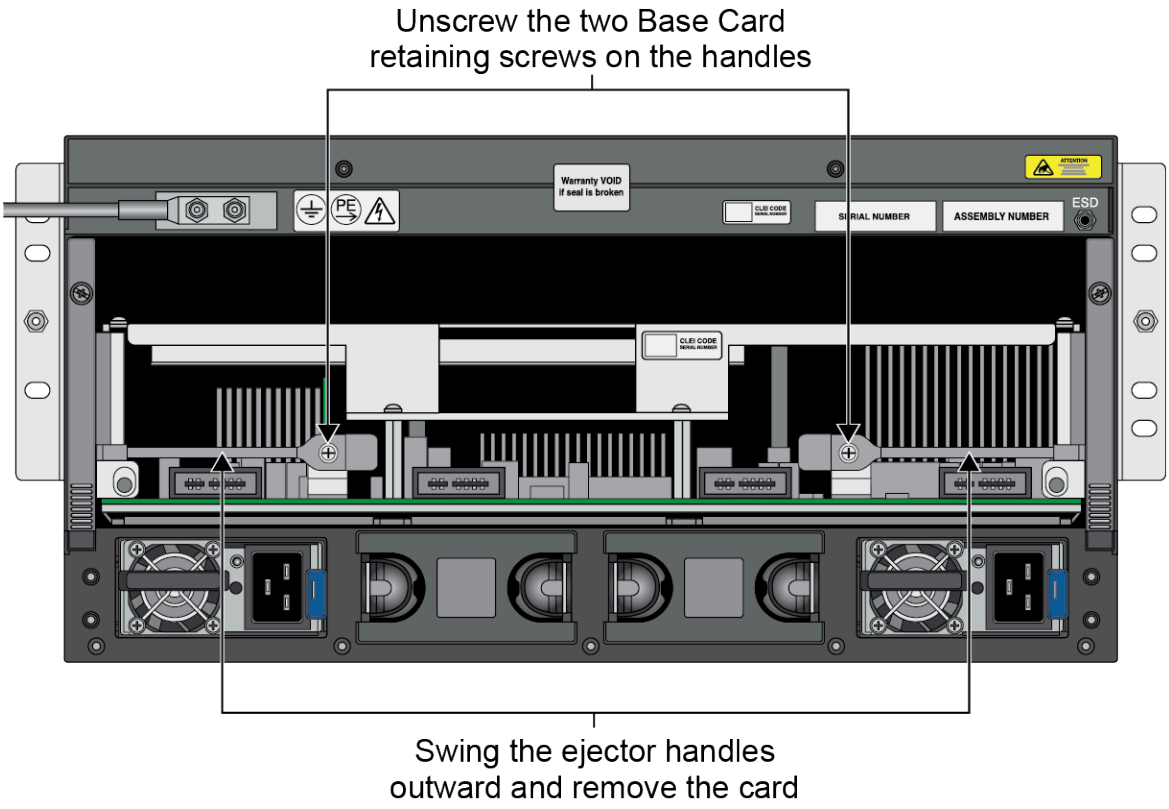


STEP 4 | Grip the top of the two ejector handles and pull them outward until both handles stop. Gently pull the fan drawer out of the appliance.

STEP 5 | Using a No. 2 Phillips head screwdriver, unscrew both Base Card (BC) retaining screws.

©2026 Palo Alto Networks, Inc.

STEP 6 | Grab both BC ejector handles and swing the handles outward at the same time. Gently pull the BC outward from inside the appliance.



Support the BC with one hand while pulling it out from the appliance.

STEP 7 | With the ejector handles on the replacement BC pointing outwards, slide the replacement BC into the appliance.

STEP 8 | Close the BC ejector handles and fasten both of the BC retaining screws.

STEP 9 | Re-install the fan drawer by locking its ejector handles into their previous positions and then tightening the two screws on the ejector handles.

©2026 Palo Alto Networks, Inc.

Replace a PA-5400 Series Firewall Fan Assembly

The following topics describe how to replace a PA-5400 Series firewall fan tray.

- Replace a PA-5400 Series Fan Assembly
- Replace a PA-5450 Fan Assembly

Replace a PA-5400 Series Fan Assembly

The PA-5410, PA-5420, PA-5430, PA-5440, and PA-5445 have three dual-rotor, single fan assemblies on its rear side. Each single fan assembly can be individually removed and replaced. When all fans are functioning as expected, the fan LED glows green. If a fan fails, the fan LED glows red. If this occurs, replace the faulty fan assembly immediately to avoid service interruption.

You can replace a failed fan assembly while the firewall is powered on; however, there is a time limit of 15 seconds starting when the fan assembly is removed to replace it before the thermal protection circuit automatically powers down the 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 the ESD port located on the rear of the appliance before handling ESD sensitive hardware. For details on the ESD port location, see PA-5400 Series Back Panel.

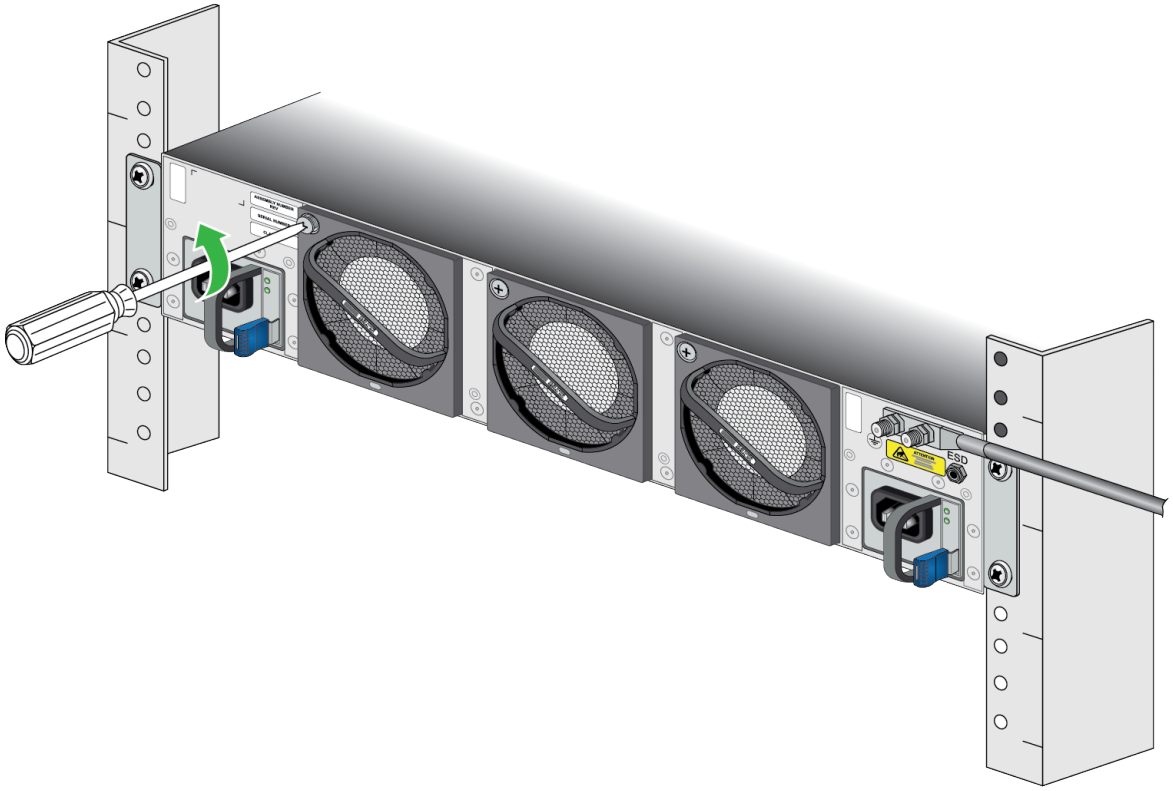
When removing a fan assembly, first pull the fan assembly out about 1 inch (2.5cm) and wait 10 seconds. This allows enough time for the working fans to stop spinning.

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

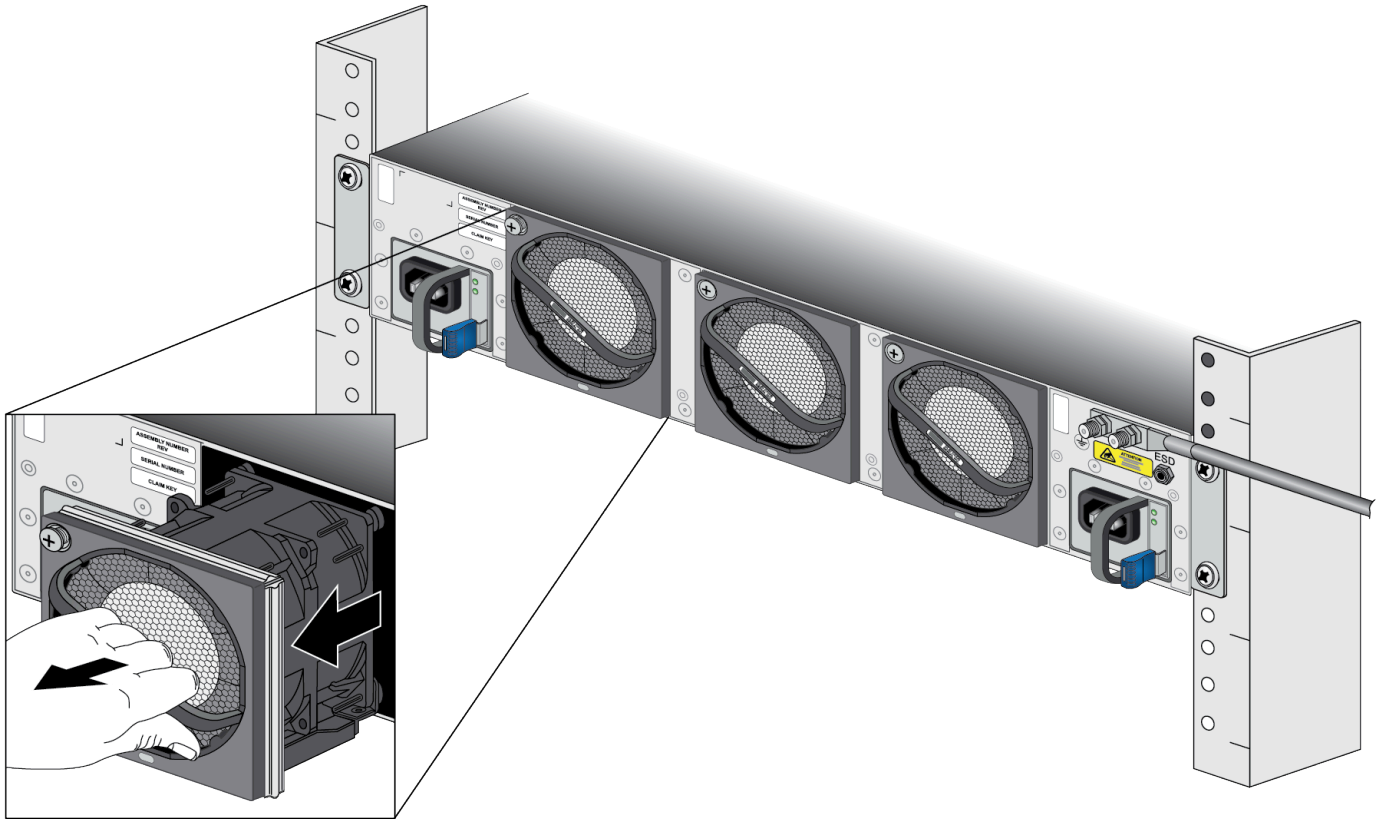
STEP 3 | Identify the failed fan assembly by checking the fault LEDs of each fan. In the event of a failure, the LED on the fan assembly will be red.

 ©2026 Palo Alto Networks, Inc.

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



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



©2026 Palo Alto Networks, Inc.

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

STEP 7 | Verify that the new fan assembly is operational by noting the status of the fan LED on the front panel. You can also view the status of the fan trays by entering the following command:

```
admin@PA-5420> show system environmentals fan-tray
```

To view the status of each fan on a fan assembly, run the following command:

```
admin@PA-5420> show system environmentals fans
```

Replace a PA-5450 Fan Assembly

The PA-5450 has four dual-rotor, single fan assemblies on its rear side. While facing the rear of the firewall, the fan assemblies are labeled 1, 2, 3, and 4 from left to right. Each single fan assembly can be individually removed and replaced. When a fan is functioning as expected, the fan LED on the MPC glows green. If a fan fails, the fan LED glows red. If this occurs, replace the fan immediately to avoid service interruption.

You can replace a failed fan assembly while the firewall is powered on; however, there is a time limit of 120 seconds starting when the fan assembly is removed to replace it before the thermal protection circuit automatically powers down the 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 the ESD port located on the rear of the appliance before handling ESD sensitive hardware. For details on the ESD port location, see PA-5450 Back Panel.

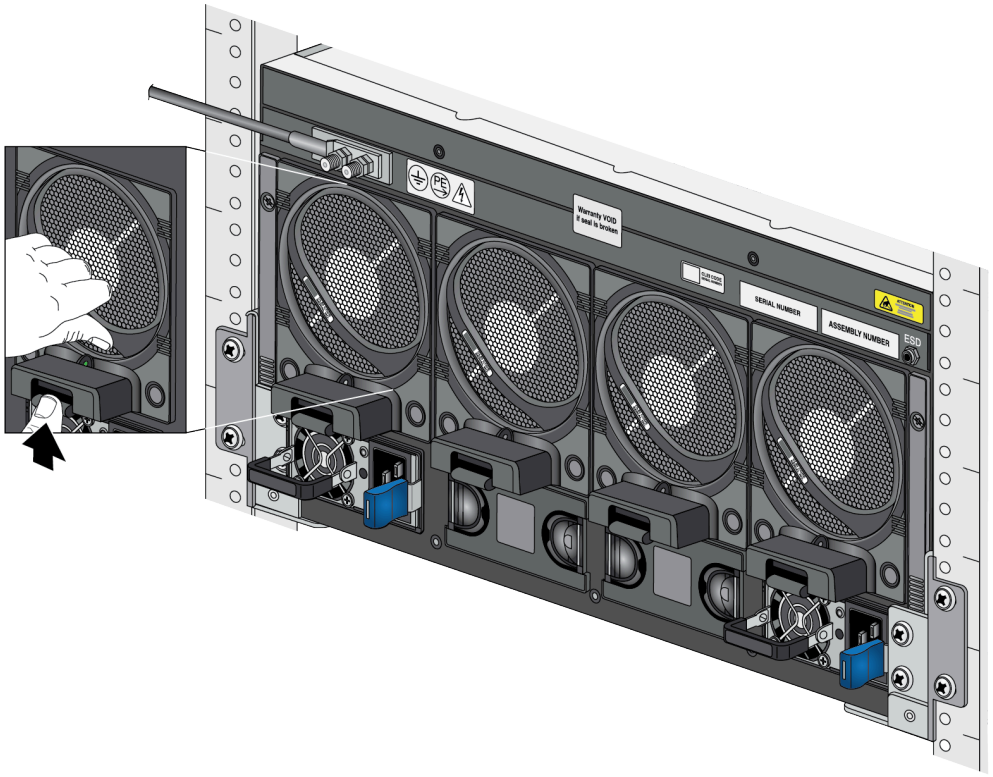
When removing a fan assembly, first pull the fan assembly out about 1 inch (2.5cm) and wait 10 seconds. This allows enough time for the working fans to stop spinning.

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

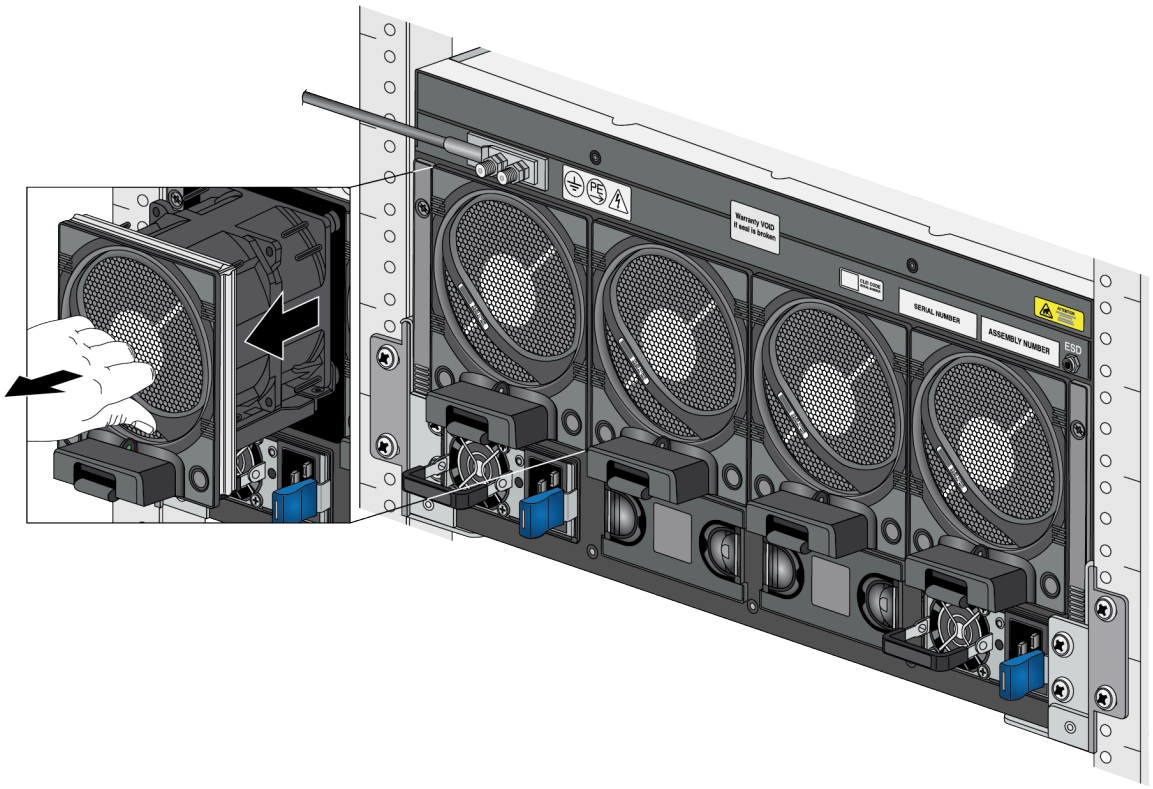
STEP 3 | Identify the failed fan assembly by checking the fault LEDs of each fan. In the event of a failure, the LED on the fan assembly will be red.

 ©2026 Palo Alto Networks, Inc.

STEP 4 | Place your thumb under the thumb tab located on the bottom of the fan assembly. Gripping the fan assembly handle with your fingers, push up on the thumb tab.



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



©2026 Palo Alto Networks, Inc.

STEP 6 | Install the replacement fan by sliding it into the vacant fan slot, ensuring that the thumb tab is on the bottom.

STEP 7 | Verify that the new fan assembly is operational by noting the status of the fan LED on the MPC. You can also view the status of the fan assemblies by entering the following command:

```
admin@PA-5450> show system environmentals fan-tray
```

To view the status of each fan on a fan assembly, run the following command:

```
admin@PA-5450> show system environmentals fans
```

 ©2026 Palo Alto Networks, Inc.

Replace a PA-5400 Series Firewall Front Slot Card

The PA-5450 is the only PA-5400 Series firewall that requires one Management Processor Card, at least one Networking Card (NC), and at least one Data Processor Card (DPC). The procedures to replace all of the front slot cards in a PA-5450 firewall are identical.

- Replace a PA-5400 Series Management Processor Card (MPC)
- Replace a PA-5400 Series Networking Card (NC)
- Replace a PA-5400 Series Data Processor Card (DPC)
- PA-5450 Front Slot and Card States
- PA-5450 Logical Card Slots
- Replace a PA-5450 Front Slot Card in a High Availability (HA) Configuration

Replace a PA-5400 Series Management Processor Card (MPC)

Learn how to replace a MPC.

- Replace a PA-5450 Management Processor Card (MPC)

Replace a PA-5450 Management Processor Card (MPC)

The replacement MPC ships with a factory default configuration and version of PAN-OS. You may need to upgrade or downgrade the PAN-OS version to your preferred version and you will need to restore the firewall configuration from a backup. Alternatively, you may swap out the boot drive from the original MPC if the drive is not the cause of the card failure.

To learn how to create a backup of your PAN-OS configuration, see Save and Export Firewall Configurations.

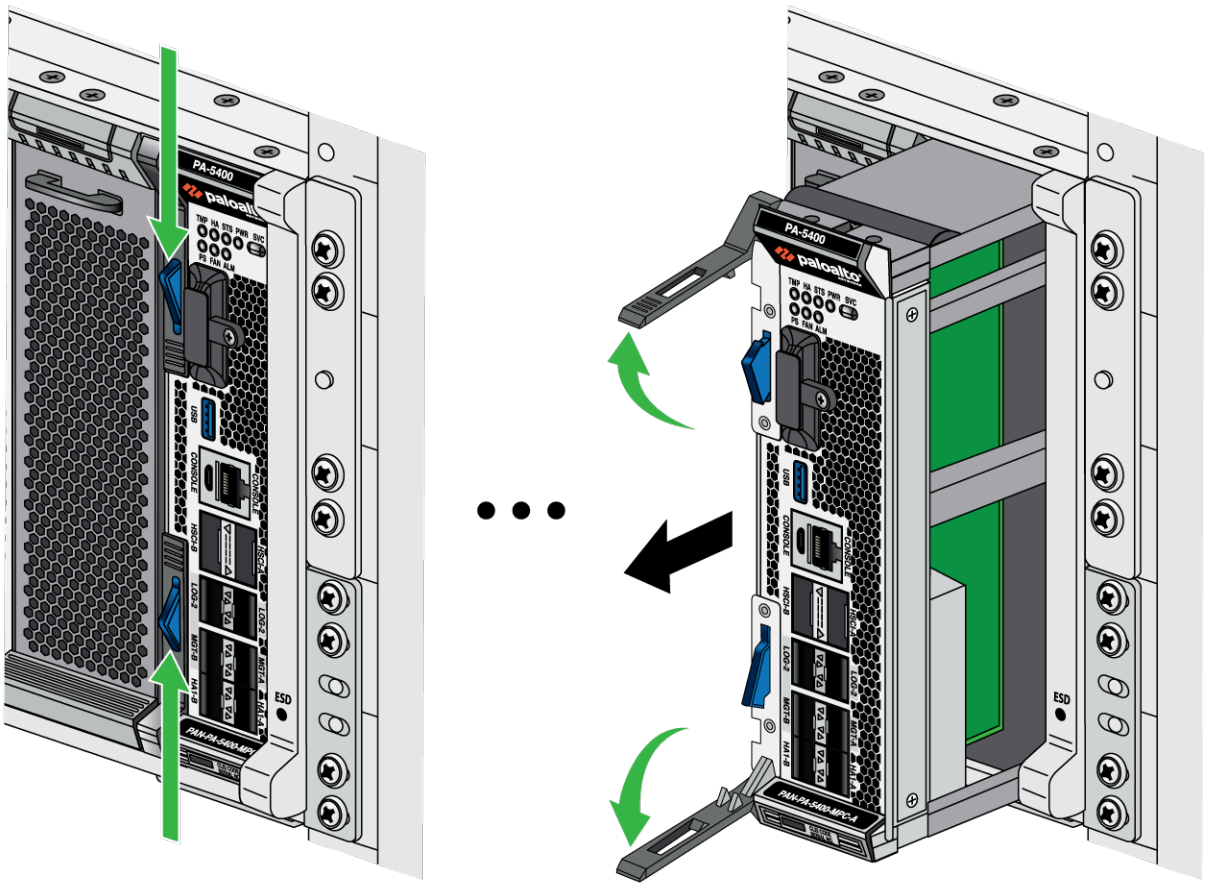
STEP 1 | Put the provided ESD wrist strap on your wrist ensuring that the metal contact is touching your skin. Then attach (snap) one end of the ground cable to the wrist strap and remove the alligator clip from the banana clip on the other end of the ESD grounding cable. Plug the banana clip end into one of the ESD ports located on the front of the appliance before handling ESD sensitive hardware. For details on the ESD port location, see PA-5450 Front Panel.

STEP 2 | Ensure that the PA-5450 is powered off and that the fans are not still spinning.

STEP 3 | Push the front tabs on the MPC towards the center, prompting a click. This will cause ejector handles on the front of the card to rotate outward and unlock the card.

©2026 Palo Alto Networks, Inc.

STEP 4 | Grip the front ejector handles and gently pull the card out of its slot.



STEP 5 | With your replacement MPC in hand, rotate the card and align it with the front of the appliance so that the Palo Alto Networks logo is readable at the top of the card.

STEP 6 | Gently push the replacement MPC into slot 7 until the card reaches the end of the slot. Push on both ejector handles until they lock the card into place.

> *Before booting the firewall in the following step, read* Set Up a Connection to the Firewall *to 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). The firewall will boot in ZTP mode if no action is taken.*

STEP 7 | Boot the appliance with the new MPC installed. When prompted, log in and reset the firewall to factory default settings.

STEP 8 | After the reset operation is complete, take the necessary steps outlined in Set Up a Connection to the Firewall to determine your boot mode.

STEP 9 | Restore your previous device configuration.

- (ZTP mode) Stand by as the device group and template configurations are pushed to the firewall from Panorama.
- (Standard mode) Login and load your preferred version and configuration of PAN-OS.

©2026 Palo Alto Networks, Inc.

Replace a PA-5400 Series Networking Card (NC)

If a Networking Card (NC) fails, the card will reboot and attempt to recover. If the card does not recover, it will change to a down state. If there is only one functioning NC in the appliance and the NC fails after three recovery attempts, the firewall will reboot to attempt to recover the card.

You do not have to power off the firewall to install or remove NCs unless the device is in FIPS-CC mode. If the device is in FIPS-CC mode, you must power off the firewall before adding or replacing an NC, otherwise the device will boot into maintenance mode.

The following topics describe how to replace an NC and provides details on checking the card slot status as well as how to troubleshoot an NC.

- Replace a PA-5450 Networking Card (NC)
- PA-5400 Series Firewall Networking Card (NC) Troubleshooting Commands

Replace a PA-5450 Networking Card (NC)

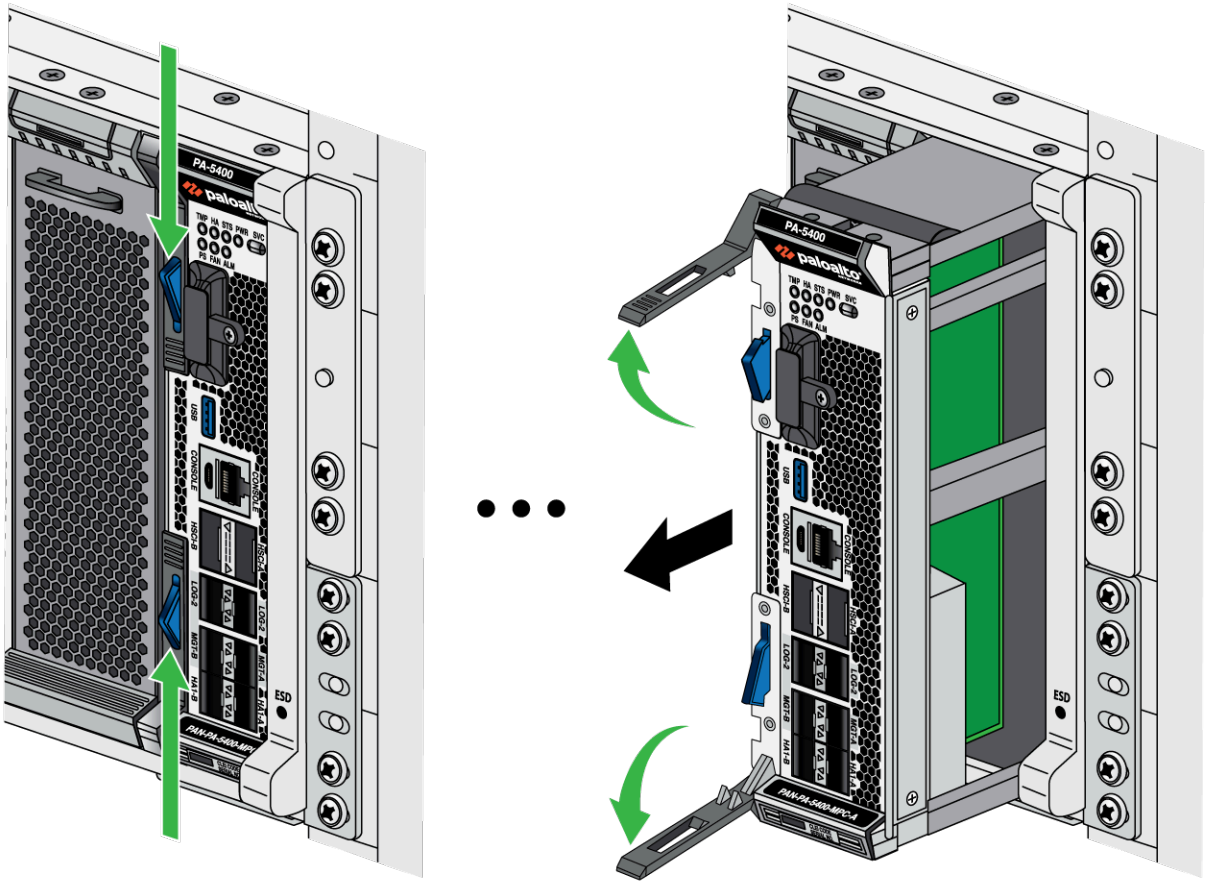
STEP 1 | Put the provided ESD wrist strap on your wrist ensuring that the metal contact is touching your skin. Then attach (snap) one end of the ground cable to the wrist strap and remove the alligator clip from the banana clip on the other end of the ESD grounding cable. Plug the banana clip end into one of the ESD ports located on the front of the appliance before handling ESD sensitive hardware. For details on the ESD port location, see PA-5450 Front Panel.

STEP 2 | Push the front tabs on the NC towards the center, prompting a click. This will cause ejector handles on the front of the card to rotate outward and unlock the card.

 ©2026 Palo Alto Networks, Inc.

STEP 3 | Grip the front ejector handles and gently pull the card out of its slot.

The below image shows a Management Processor Card (MPC); however, the procedure to remove the NC is the same.



STEP 4 | With your replacement NC in hand, rotate the card and align it with the front of the appliance so that the Palo Alto Networks logo is readable at the top of the card.

STEP 5 | Gently push the replacement NC into slot 1 or 2 until the card reaches the end of the slot. Push on both ejector handles until they lock the card into place.

PA-5400 Series Firewall Networking Card (NC) Troubleshooting Commands

The following table describes common commands that you can use to troubleshoot NC issues on a PA-5400 Series firewall.

The PA-5450 firewall makes use of paired Logical Card Slots in order to direct processing power from a Data Processing Card (DPC) to a corresponding NC. Certain commands issued to the NC affect or are affected by the status of its corresponding DPC.

 ©2026 Palo Alto Networks, Inc.

Purpose	Command

Show NC slot status.	Run the following to view all of the slots:
	`admin@PA-5450> show chassis status`
	To view the status of one slot run:
	`admin@PA-5450> show chassis status slot <slot-number>`
	For example, to check the status of slot 1, run:
	`admin@PA-5450> show chassis status slot s1`

Temporarily power on and off an NC slot.
This command gracefully powers off a slot and ends current sessions. You can use this command to remove an NC.
	To power off a slot:
	`admin@PA-5450> request chassis power-off slot <slot-number>`
	To power on a slot:
	`admin@PA-5450> request chassis power-on slot <slot-number>`

Power off an NC slot. When running this command, the NC slot stays powered off, even after a reboot.	`admin@PA-5450> request chassis admin-power-off slot <slot-number>`
Enable a slot so the NC can pass traffic.	`admin@PA-5450> request chassis enable slot <slot-number>`
Enable new NCs on both firewalls in an HA configuration.	In an HA configuration, you must install the same number and model of NCs in each firewall and the slot numbers must match. For example, after installing two NCs (one in each firewall), the firewall keeps them in a disabled state until you enable them. This allows the firewall to start HA monitoring on each NC at the same time. To enable NCs after inserting them into the same slot numbers on each firewall in an HA configuration, run the following command:

 ©2026 Palo Alto Networks, Inc.

Purpose	Command

	`admin@PA-5450> request chassis power-on slot <slot-number> target ha-pair`
	
	For example, to enable NCs installed in slot 2 of both firewalls, run the following command:
	
	`admin@PA-5450> request chassis power-on slot 2 target ha-pair`
	
	You can use the `ha-pair` option in an HA configuration for many of the slot control commands.

Replace a PA-5400 Series Data Processor Card (DPC)

Learn how to replace a DPC.

- Replace a PA-5450 Data Processor Card (DPC)

Replace a PA-5450 Data Processor Card (DPC)

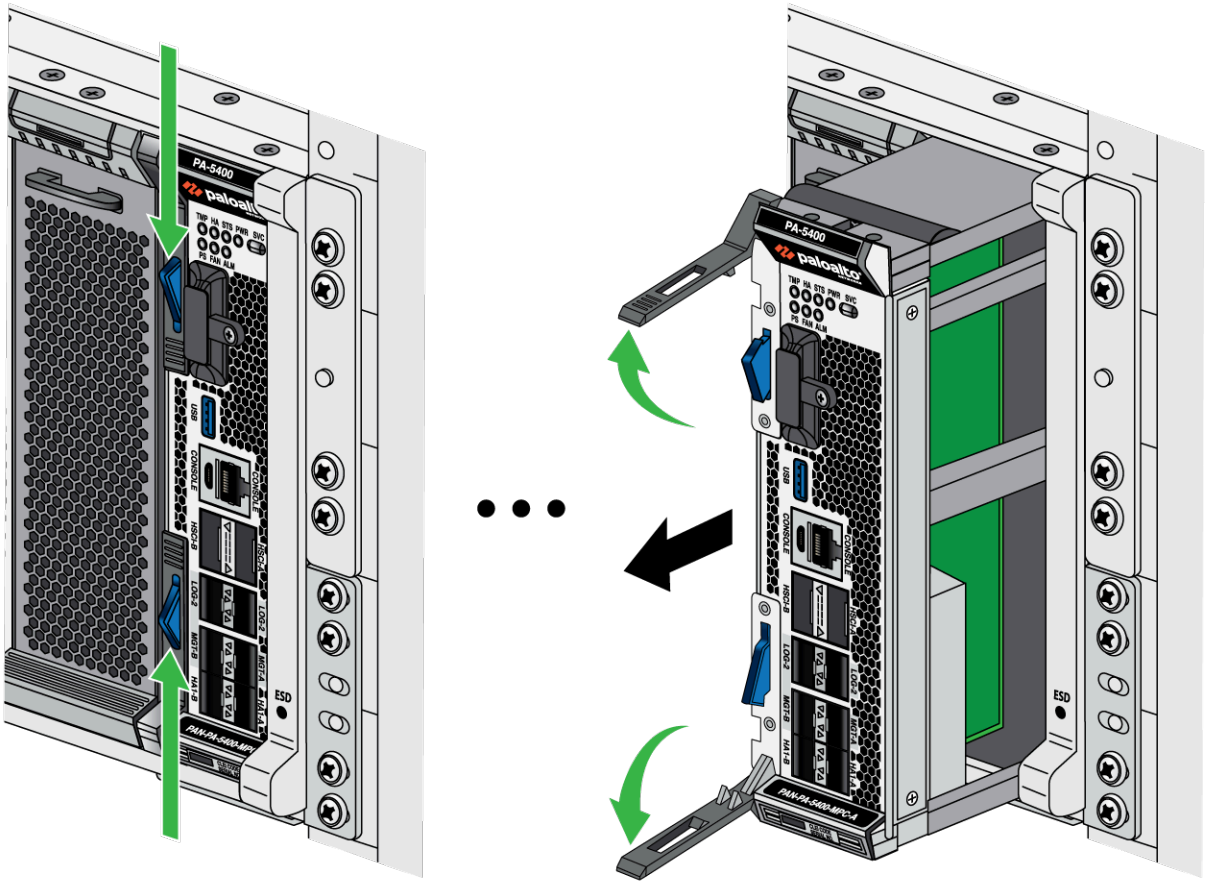
STEP 1 | Put the provided ESD wrist strap on your wrist ensuring that the metal contact is touching your skin. Then attach (snap) one end of the ground cable to the wrist strap and remove the alligator clip from the banana clip on the other end of the ESD grounding cable. Plug the banana clip end into one of the ESD ports located on the front of the appliance before handling ESD sensitive hardware. For details on the ESD port location, see PA-5450 Front Panel.

STEP 2 | Push the front tabs on the DPC towards the center, prompting a click. This will cause ejector handles on the front of the card to rotate outward and unlock the card.

 ©2026 Palo Alto Networks, Inc.

STEP 3 | Grip the front ejector handles and gently pull the card out of its slot.

The below image shows a Management Processor Card (MPC); however, the procedure to install the DPC is the same.



STEP 4 | With your replacement DPC in hand, rotate the card and align it with the front of the appliance so that the Palo Alto Networks logo is readable at the top of the card.

STEP 5 | Gently push the replacement DPC into slot 2, 3, 4 ,5 or 6 until the card reaches the end of the slot. Push on both ejector handles until they lock the card into place.

STEP 6 | (Optional) To restore LACP functionality after replacing the DPC, either reboot the firewall or restart the DPC using the following command:

```
request chassis restart slot <>
```

PA-5450 Front Slot and Card States

You can view the slot and card status information on a PA-5450 Series firewall using the web interface or the command line interface (CLI). From the web interface, select **Network** > **Interfaces** to view the status of each slot. From the CLI operational mode, run the following command:

 ©2026 Palo Alto Networks, Inc.

```
admin@PA-5450> show chassis status slot <slot-number>
```

For example, to show the status of slot 1, run the following command:

```
admin@PA-5450> show chassis status slot s1
```

For information on troubleshooting card slots and changing slot states, see PA-5400 Series Firewall Networking Card (NC) Troubleshooting Commands.

State	Description
Empty	The slot is empty and is ready to use.
Up	The card is powered on and has a valid software configuration.
Disabled	(HA only) The slot is not enabled. In a high availability (HA) configuration, the NC slots stay in a disabled state until you enable the slot. This is by design, so you can install new NCs without causing a failover. After you insert matching NCs in both firewalls, you then bring up both cards simultaneously.
HA-Disabled	(HA only) After you enable a slot, this status appears until both slots are ready. This also occurs if the peer does not have a matching card in the same slot number or the card in the peer is not ready.
Stopping	The card is preparing for removal.
Starting	The card is in the process of powering on and the software is initiating.
PowerOff	The card is powered down and ready for removal.
AdminPowerOff	An administrator powered down the slot and it will not be available until you power it back on. If there is a slot that you want ignored in an HA configuration HA, put it in this state.
Failure	The card has failed and needs to be replaced.
Unsupported	The card is not a supported type for this slot.

PA-5450 Logical Card Slots

The PA-5450 firewall requires the use of logical card slots in order to direct processing power from the Data Processing Card (PA-5400 DPC-A) to the Networking Card (PA-5400 NC-A). For

 ©2026 Palo Alto Networks, Inc.

this to occur, an NC in Slot 1 of the appliance is logically paired to a DPC in Slot 3. Similarly, an NC in Slot 2 of the appliance is logically paired to a DPC in Slot 4. Logical pairing of the NC and DPC allows the appliance to process exception packets and other data that the NC does not process alone.

If you install a DPC in Slot 2 of the appliance, then there is no logical pairing with Slot 4.

See the following table of possible CLI commands that are used to restart, power on, or power off a card.

For more information on card states, see PA-5450 Front Slot and Card States.

CLI Command	Result

`request chassis admin-power-on slot <>`
 	
`request chassis admin-power-on slot <> target ha-pair`
	Power on a card in the selected slot.

`request chassis admin-power-off slot <> now <>`
 	
`request chassis admin-power-off slot <> target ha-pair now <>`
	Power off a card in the selected slot and keep it powered off across reboots until manually powered back on.

`request chassis power-on slot <>`
 	
`request chassis power-on slot <> target ha-pair`
	Power on a card in the selected slot.

`request chassis power-off slot <> now <>`
 	
`request chassis power-off slot <> target ha-pair now <>`
	Power off a card in the selected slot until the next reboot.

`request chassis restart slot <>`	Restart a card in the selected slot.

©2026 Palo Alto Networks, Inc.

CLI Command	Result
`request chassis restart slot <> target ha-pair`	

`request chassis enable slot <>`
 	
`request chassis enable slot <> target -ha-pair`
	Enable a card in the selected slot.

The status of one card in a logical pair can have an impact on the status of the other card in the pair. The firewall will consult the logically paired card during different operations. For example, when a DPC is brought into a `Power-Off` state, its corresponding NC will also be powered off. System logs can be used to troubleshoot any status errors encountered by a logical pair. See the following table of possible outcomes that occur as a result of the status of a card or logically paired slot. The third column of the table gives examples of critical system logs that are received in response to certain outcomes.

Operation	Possible Outcomes	Critical System Log Examples
Powering on an NC	• If the logically paired DPC is already in the `Up` state, then the operation to power on the DPC is skipped. Verify if the NC is powered on. • If the logically paired DPC is in one of the following states: `empty`, `failureCard`, `unsupportedCard`, `powerNotOK`, or `coolingNotOK`, then the CLI prints a failure and does not power on the NC. Verify that the CLI received a critical system log. See the Critical System Log Examples column. • If the logically paired DPC is in the `adminPoweredDown` state and you are trying to use the **`admin-power-on`** or **`power-on`** commands, the CLI prints a failure and does not power on the NC. • Powering on the NC powers on the paired DPC if the paired DPC is NOT in one of the following states: `adminPoweredDown`, `empty`,	`2021/04/12 14:06:34 critical hw slot-po 0 Attempting to power down Slot 1 because the Logically Paired DPC is in a PowerOff state.`

©2026 Palo Alto Networks, Inc.

Operation	Possible Outcomes	Critical System Log Examples
	`failureCard`, `unsupportedCard`, `powerNotOK`, or `coolingNotOK`.	
Powering off an NC	• The state of the logically paired DPC is not affected when the NC fails or goes down.	
Powering on a DPC	• Using the **`admin-power-on`** or **`power-on`** commands will only power on the DPC. • There is no effect on the state of the logically paired NC when the DPC powers on. See the system log in the Critical System Log Examples column.	`2021/04/12 14:03:48 criti cal hw slot-po 0 The Logically paired Sl ot 1 might be in a PowerO ff state. Power it on usi ng Slot 1 specific CLI.`
Powering down a DPC	• Using the **`admin-power-off`** or **`power-off`** commands on the DPC will power off the logically paired NC before powering off the DPC. See the system log in the Critical System Log Examples column.	`2021/04/12 13:56:10 criti cal hw slot-po 0 Attempting to power do wn Slot 1 because the Log ically Paired Slot 3 went from an Up state to a St opping state.`
Restarting an NC	• When the logically paired DPC is in the `Up` or `Disabled` state: 1. The firewall first powers off the NC. 2. The firewall then verifies if the DPC is still in the `Up` or `Disabled` state. 3. Lastly, the firewall powers on the NC. • When the logically paired DPC is in the `power-off` state: 1. The firewall first powers off the NC. 2. The firewall powers on the logically paired DPC. 3. The firewall then powers on the NC. • When the logically paired DPC is in one of the following states: `empty`, `failureCard`, `unsupportedCard`, `powerNotOK`, or `coolingNotOK`,	

 ©2026 Palo Alto Networks, Inc.

Operation	Possible Outcomes	Critical System Log Examples
	the NC cannot be powered on after a restart.	

Replace a PA-5450 Front Slot Card in a High Availability (HA) Configuration

When High Availability (HA) is configured on the firewall, you must take additional steps to remove and install a Networking Card (NC) or Data Processing Card (DPC). Although it is possible to hot-swap the front slot cards, following the procedure outlined below will prevent slot or device failures in a live HA deployment.

In an HA configuration, you must install the NCs and DPCs in each chassis in corresponding slots. For example, after installing two NCs (one in each firewall), the firewall keeps them in a disabled state until you enable them. This allows the firewall to start HA monitoring on each NC at the same time.

- **To insert a new pair of NCs or DPCs into an HA pair:**
  1. Insert a card into the same numbered slot in both devices.
  2. Verify that the cards are powered on by issuing the following command:

     ```
     show chassis status
     ```

  3. If the slot is in the `Admin-power-down` state, then issue the following command on both devices to power on the slots:

     ```
     request chassis admin-power-on slot <slot-number> target
      local-device
     ```

  4. Change the distribution policy mode on each device:

     ```
     set session distribution-policy session-load
     ```

  5. Confirm that both devices are in the correct state with the following commands:

     ```
     show chassis status
     ```

     ```
     show session distribution policy
     ```

     ```
     show high-availability all
     ```

  6. Issue the following command to allow traffic to flow through the slot on both devices:

     ```
     request
     chassis enable slot <slot-number> target ha-pair
     ```

 ©2026 Palo Alto Networks, Inc.

- **To remove a pair of NCs or DPCs from an HA pair:**
  1. Disable HA on the HA pair.
  2. On the device whose front slot card you want to remove, issue the following command where X is the slot and Y is the amount of time to allow the slot to power down gracefully:

     ```
     request chassis admin-power-off slot X Y
     ```

  3. Once both slots are powered off, remove the cards from both devices.
  4. Issue the following command after the slots are removed to make sure future slots will power up when they are added:

     ```
     request chassis admin-power-on slot X
     ```

- **If a slot fails in a running HA pair, it will take the device that sees the failure into a Non-Functional or Tentative state. To bring the two devices back up:**
  1. On the device whose front slot card you want to remove, issue the following command where X is the slot. The down device should move into a functional state.

     ```
     request chassis admin-power-off slot X
     ```

     ```
     Executing this command will power off the given slot. Do you
      want to continue? (y or n)
     ```

  2. Remove the failed card from its slot.
  3. Prepare to return the failed card. The non-failed card on the other device can be left in an `AdminPowerOff` state until you receive a replacement card.

©2026 Palo Alto Networks, Inc.

- **To install a replacement of the failed card:**
  1. When you receive the replacement NC or DPC, insert it into the device that needs the replacement card. Ensure that the slot it is inserted into corresponds to the slot of the functioning card in the paired device.
  2. Verify that the card is powered on by issuing the following command:

     ```
     show chassis status
     ```

  3. If the slot is in the `Admin-power-down` state, then issue the following command on both devices to power on the slots:

     ```
     request chassis admin-power-on slot <slot-number> target
      local-device
     ```

  4. Change the distribution policy mode:

     ```
     set session distribution-policy session-load
     ```

  5. Confirm that both devices are in the correct state with the following commands:

     ```
     show chassis status
     ```

     ```
     show session distribution policy
     ```

     ```
     show high-availability all
     ```

  6. Once the slot moves into a `Disable` state, issue the following command and the slot will allow traffic to start flowing to the slot:

     ```
     request chassis enable slot <slot-number>
     ```

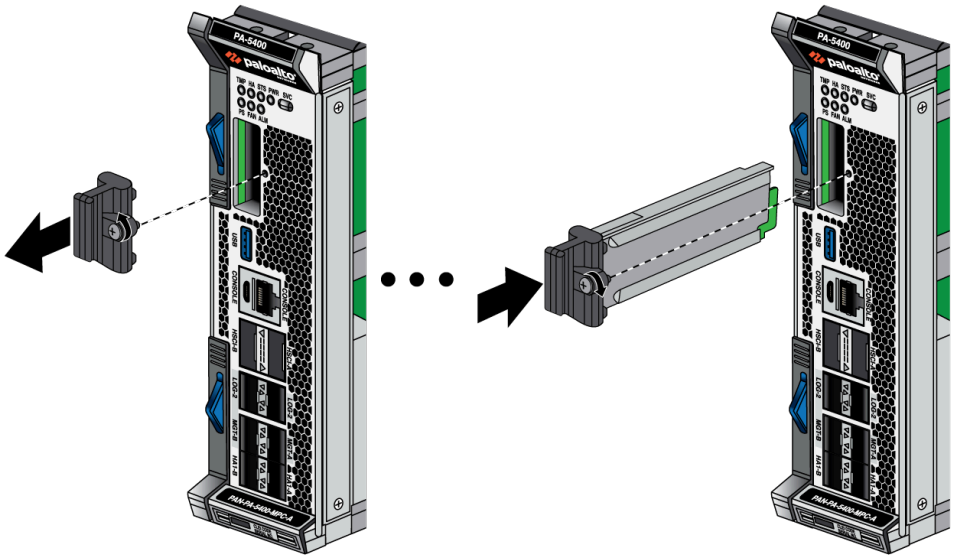

©2026 Palo Alto Networks, Inc.

Install an MPC Logging Drive

STEP 1 | Attach an ESD strap to your wrist and plug the other end in to the ESD port location on the front of the appliance. See PA-5450 Front Panel for the location of the ESD port.

STEP 2 | Loosen the retaining screw on the logging drive blank cover while gently pulling on the pull tab. Proceed until the logging drive blank cover can be pulled out from the MPC faceplate.

STEP 3 | Insert the logging drive into the opening in the MPC faceplate. Align the retainer screw with the threaded hole in the MPC faceplate.



STEP 4 | Once the logging drive is fully seated, tighten the retainer screw to 4 in-lbs.

Exceeding a torque of 4.5 in-lbs will damage the equipment.

STEP 5 | Reboot the firewall. After rebooting, the firewall recognizes the newly added logging drive.

STEP 6 | Use a terminal emulator such as PuTTY to add the logging drive to the system. Enter the following CLI command:

```
admin@PA-5400> request system disk add nvme0n1
```

Executing this command will delete all data on the drive being added.

STEP 7 | Enable the newly added logging drive by entering the following CLI command:

```
admin@PA-5400> request logdb-migrate logging-drive start
```

The firewall automatically reboots after enabling the new logging drive.

 ©2026 Palo Alto Networks, Inc.

Replace a System Drive

The following topics describe how to replace the Solid State Drive (SSD) containing the files of the PA-5400 Series firewalls. The system drive is located in the front panel of the PA-5410, PA-5420, PA-5430, PA-5440, and PA-5445 firewalls, while the PA-5450 system drive is located in the Management Processor Card (MPC).

- Replace a System Drive in a PA-5400 Series Firewall
- Replace a System Drive in a PA-5450 MPC

Replace a System Drive in a PA-5400 Series Firewall

The PA-5410, PA-5420, PA-5430, PA-5440, and PA-5445 firewalls use a pair of solid-state drives (SSDs) to store the PAN-OS system files, system logs, and network traffic logs. If one of these drives fail, you must replace the entire SSD module, which houses both drives, to restore functionality to the firewall.

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

The SSD module is not hot-swappable.

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.

The following procedure describes how to replace the SSD module.

STEP 1 | Determine if a drive has failed.

When the system drives are functioning normally, all system drive partitions show both drives with the status `clean`. If a system drive fails, the `Overall System Drives RAID status` shows `degraded`, one or more failed partition array shows `clean`, `degraded`, and one of the drives will be missing (Sys1 or Sys2). In this example, the output from the `show system raid detail` command, the panlogs partition shows the status `clean`, `degraded`, and drive `Sys1` is missing from the panlogs array; together, these indicate that Sys1 has encountered a failure.

```
admin@PA-5420> show system raid detail

Overall System Drives RAID status           degraded
------------------------------------------------------------------------------
Drive status
   Disk id Sys1                             Present
 (MICRON_M510DC_MT)
   Disk id Sys2                             Present
 (MICRON_M510DC_MT)
------------------------------------------------------------------------------
Partition status
```

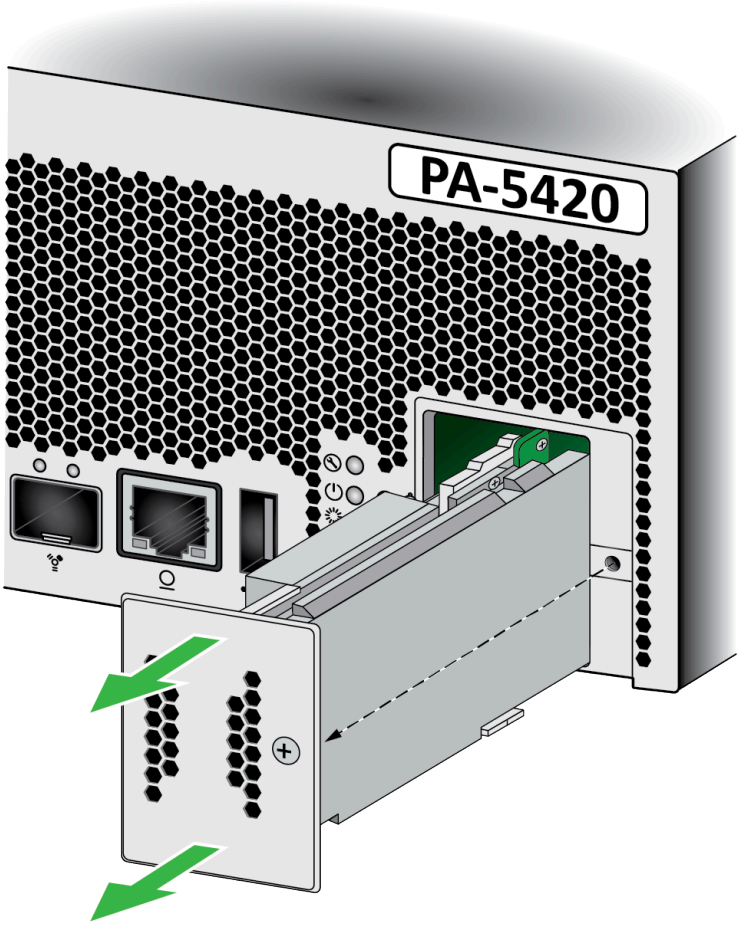
 ©2026 Palo Alto Networks, Inc.

```
panlogs                                          clean, degraded
   Drive id Sys2                                 active sync
maint                                            clean
   Drive id Sys1                                 active sync
   Drive id Sys2                                 active sync
sysroot0                                         clean
   Drive id Sys1                                 active sync
   Drive id Sys2                                 active sync
sysroot1                                         clean
   Drive id Sys1                                 active sync
   Drive id Sys2                                 active sync
pancfg                                           clean
   Drive id Sys1                                 active sync
   Drive id Sys2                                 active sync
panrepo                                          clean
   Drive id Sys1                                 active sync
   Drive id Sys2                                 active sync
swap                                             clean
   Drive id Sys1                                 active sync
   Drive id Sys2                                 active sync
```

STEP 2 | Unscrew the captive screw on the system drive module cover on the front side of the firewall.

 ©2026 Palo Alto Networks, Inc.

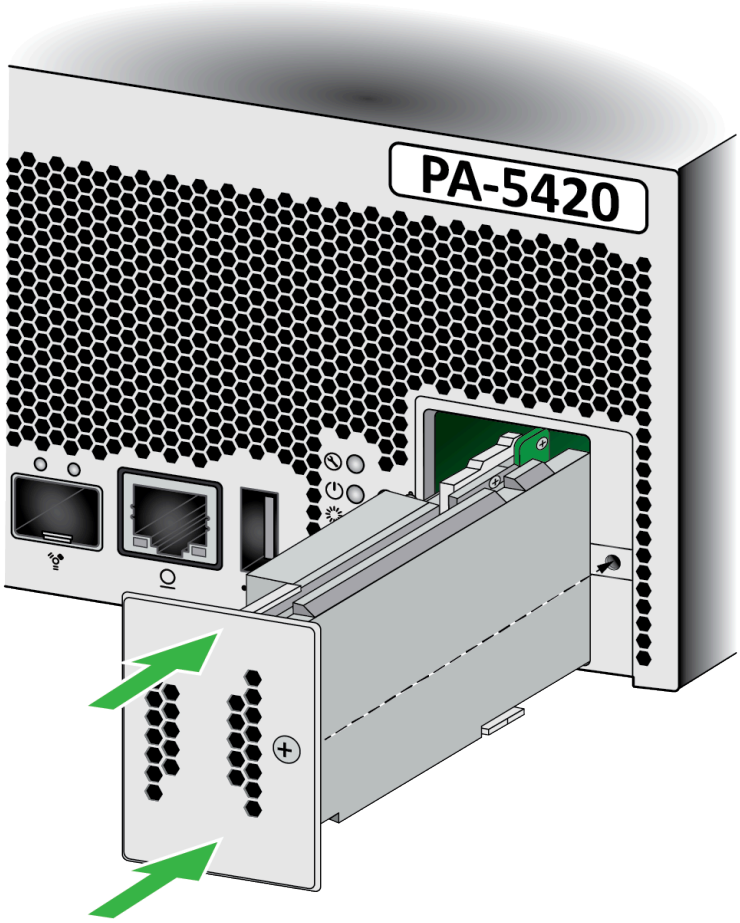
STEP 3 | Pull the SSD module out of the firewall.



STEP 4 | Remove the replacement SSD module from the packaging and place it on an antistatic surface.

 ©2026 Palo Alto Networks, Inc.

STEP 5 | Slide the replacement SSD module onto the rails and gently push it into the firewall. Re-fasten the captive screw until the module is secure in the appliance.



STEP 6 | View the RAID status until you see that the `Overall System Drives RAID status` shows `Good`, all partitions show `clean`, and both drives show `active sync`. To view RAID status, run the following command: `show system raid detail`

Do not reboot the firewall until all partitions are ready; otherwise, the system drives may become out of sync and the firewall will not boot.

STEP 7 | Restore your firewall configuration or perform initial configuration.

Replace a System Drive in a PA-5450 MPC

STEP 1 | Identify the failed drive and determine the drive model using the **`show system raid detail`** CLI command.

When the system drives are functioning normally, all system drive partitions show both drives with the status `clean`. If a system drive fails, the `Overall System Drives RAID status` shows `degraded`, one or more failed partition array shows `clean`, `degraded`, and one of the drives will be missing (Sys1 or Sys2).In this example, the output from the `show system raid detail` command shows that the drive model is `MICRON_M510DC_MT`, the panlogs

 ©2026 Palo Alto Networks, Inc.

partition shows the status `clean, degraded`, and drive `Sys1` is missing from the panlogs array; together, these indicate that you need to replace the Sys1 drive.

```
admin@PA-5450> show system raid detail

Overall System Drives RAID status           degraded
-------------------------------------------------------------------------------
Drive status
   Disk id Sys1                             Present
 (MICRON_M510DC_MT)
   Disk id Sys2                             Present
 (MICRON_M510DC_MT)
-------------------------------------------------------------------------------
Partition status

panlogs                                     clean, degraded
   Drive id Sys2                            active sync
maint                                       clean
   Drive id Sys1                            active sync
   Drive id Sys2                            active sync
sysroot0                                    clean
   Drive id Sys1                            active sync
   Drive id Sys2                            active sync
sysroot1                                    clean
   Drive id Sys1                            active sync
   Drive id Sys2                            active sync
pancfg                                      clean
   Drive id Sys1                            active sync
   Drive id Sys2                            active sync
panrepo                                     clean
   Drive id Sys1                            active sync
   Drive id Sys2                            active sync
swap                                        clean
   Drive id Sys1                            active sync
   Drive id Sys2                            active sync
```

When viewing the drives so that the labels are readable, Sys1 is the top drive and Sys2 is the bottom drive.

STEP 2 | Remove the failed drive from the RAID 1 array. In this example, run the following command to remove drive `Sys1` from the array:

```
admin@PA-5450> request system raid remove sys1
```

STEP 3 | Confirm that the failed drive is removed from all partitions. In the following output of the `show system raid detail`, you see that `drive id Sys1` is now missing from all partitions.

```
admin@PA-5450> show system raid detail

Overall System Drives RAID status              degraded
```

 ©2026 Palo Alto Networks, Inc.

```
--------------------------------------------------------------------------------
Drive status
   Disk id Sys1                                  Present
 (MICRON_M510DC_MT)
   Disk id Sys2                                  Present
 (MICRON_M510DC_MT)
--------------------------------------------------------------------------------
Partition status

panlogs                                          clean, degraded
   Drive id Sys2                                 active sync
maint                                            clean, degraded
   Drive id Sys2                                 active sync
sysroot0                                         clean, degraded
   Drive id Sys2                                 active sync
sysroot1                                         clean, degraded
   Drive id Sys2                                 active sync
pancfg                                           clean, degraded
   Drive id Sys2                                 active sync
panrepo                                          clean, degraded
   Drive id Sys2                                 active sync
swap                                             clean, degraded
   Drive id Sys2                                 active sync
```

STEP 4 | Ensure that you have access to an ESD work surface for placement of the Management Processor Card (MPC).

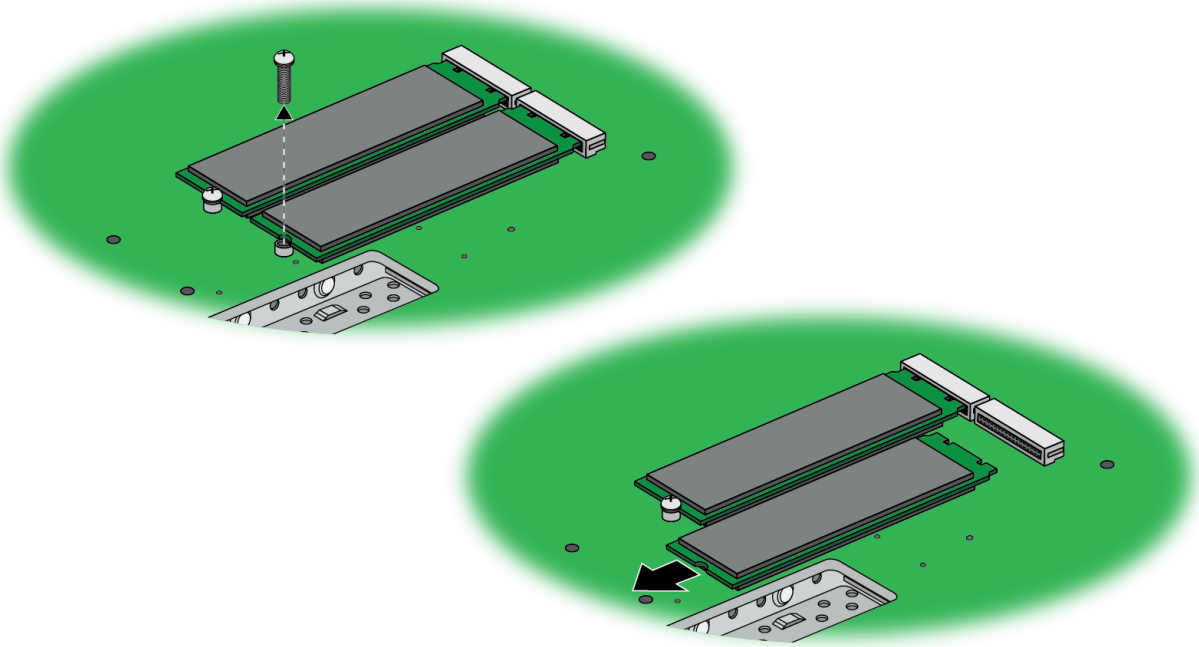
STEP 5 | Put the provided ESD wrist strap on your wrist ensuring that the metal contact is touching your skin. Then attach (snap) one end of the ground cable to the wrist strap and remove the alligator clip from the banana clip on the other end of the ESD grounding cable. Plug the banana clip end into one of the ESD ports located on the back of the appliance before handling ESD sensitive hardware. For details on the ESD port location, see PA-5450 Back Panel.

STEP 6 | Remove the MPC from card slot 7 of the appliance. See Replace a PA-5400 Series Management Processor Card (MPC) for details on removing the MPC.

STEP 7 | Place the MPC on an ESD work surface. Detach your wrist strap's ground cable from the ESD port on the appliance and securely attach the alligator clip to the new ESD surface.

 ©2026 Palo Alto Networks, Inc.

STEP 8 | Flip the MPC over and locate the two SSDs on the bottom surface of the card. Remove the retention screw for the SSD you intend to replace.



The plastic standoff becomes loose after the retention screw is removed. Do not lose the standoff as it is needed when installing the new SSD.

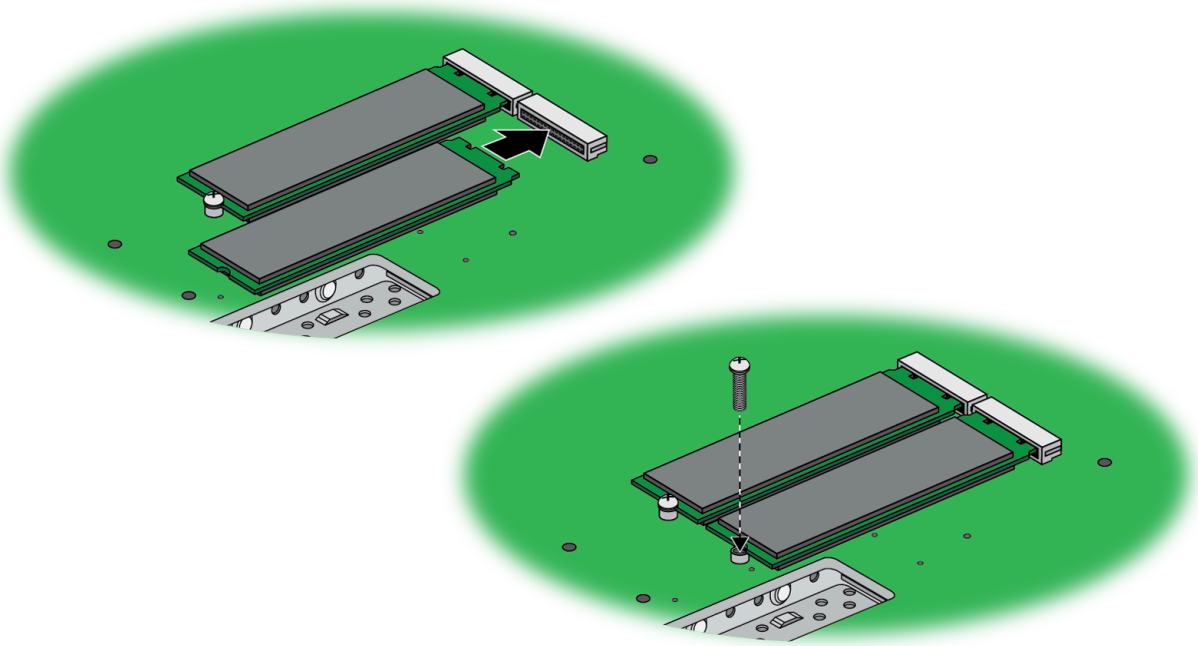
STEP 9 | Gently pull the SSD away from its mating connector. Place the old SSD to the side.

STEP 10 | Slide the new SSD into the vacant mating connector. Ensure that the SSD aligns with the plastic standoff on the MPC.

©2026 Palo Alto Networks, Inc.

STEP 11 | Fasten the retention screw back into place at a torque of 4 in-lbs.

Exceeding a torque of 4 in-lbs will damage the equipment.



STEP 12 | Before re-installing the MPC, plug the banana clip end of your ESD wrist strap into one of the ESD ports located on the back of the appliance.

STEP 13 | Slide the MPC back into slot 7. See Install a PA-5400 Series Firewall Management Processor Card (MPC) for more information.

 ©2026 Palo Alto Networks, Inc.

 ©2026 Palo Alto Networks, Inc.

PA-5400 Series Firewall Specifications

The following topics provide appliance and component specifications for the PA-5400 Series firewalls. View the datasheet for information on features, performance, and capacity numbers.

- PA-5400 Series Firewall Physical Specifications
- PA-5400 Series Firewall Electrical Specifications
- PA-5400 Series Firewall Environmental Specifications

PA-5400 Series Firewall Physical Specifications

The following table describes PA-5400 Series firewall physical specifications.

Specification	Value
Height	**PA-5410, PA-5420, PA-5430, PA-5440, and PA-5445 firewalls**—3.44 inches (8.74 cm) **PA-5450 firewall**—8.75 inches (22.23 cm)
Depth	**PA-5410, PA-5420, PA-5430, PA-5440, and PA-5445 firewalls**— 22.5 inches (57.15 cm) **PA-5450 firewall**—30 inches (76.2 cm).
Width	**PA-5410, PA-5420, PA-5430, PA-5440, and PA-5445 firewalls**—17.34 inches (44.04 cm) **PA-5450 firewall**—17.4 inches (44.2 cm).
Appliance weight	**PA-5410, PA-5420, PA-5430, PA-5440, and PA-5445 firewalls** • Appliance—35 lbs (15.88 kg) **PA-5450 firewall** • Appliance—97 lbs (44 kg) • Appliance with Base Card (BC) and fan tray installed—108 lbs (49 kg)
Appliance component weights	**PA-5410, PA-5420, PA-5430, PA-5440, and PA-5445 Components** • Fan tray—1.4 lbs (0.64 kg) • Power Supply (AC)—3.15 lbs (1.43 kg) • Power Supply (DC)—3.15 lbs (1.43 kg) **PA-5450 Components** • Base Card (BC)—10 lbs (4.5 kg) • Management Processor Card (MPC)—4 lbs (1.8 kg) • Networking Card (NC)—4 lbs (1.8 kg) • Data Processor Card (DPC)—5 lbs (2.3 kg) • Fan tray—1 lbs (.5 kg) • Power Supply (AC)—2 lbs (.9 kg) • Power Supply (DC)—2 lbs (.9 kg)

©2026 Palo Alto Networks, Inc.

Specification	Value
Rack mount size	**PA-5410, PA-5420, PA-5430, PA-5440, and PA-5445 firewalls**—2U **PA-5450 firewall**—5U
Power supply configurations	**PA-5410, PA-5420, PA-5430, PA-5440, and PA-5445 firewalls**—Two AC or DC power supplies. The AC and DC power supplies are hot-swappable. **PA-5450 firewall**—Four AC or DC power supplies. The AC and DC power supplies are hot-swappable.

©2026 Palo Alto Networks, Inc.

PA-5400 Series Firewall Electrical Specifications

The following table describes the PA-5400 Series firewall electrical specifications. To learn about the module and component electrical specifications of the PA-5450, see the PA-5450 Firewall Component Electrical Specifications. To learn about the power cords compatible with the PA-5400 Series firewalls, see PA-5400 Series Firewall Power Cord Types.

Specification	Value

Power Supplies	**PA-5410, PA-5420, PA-5430, PA-5440, and PA-5445**
	• Two load sharing 1,200W AC or DC power supplies. If one power supply fails, the second power supply provides full redundancy.
	  • PAN-PWR-1200W-AC
	  • PAN-PWR-1200W-DC
	PA-5450
	• Up to four 2,200W AC or DC power supplies; two power supplies are required at minimum.
	  • PAN-PWR-2200W-AC
	  • PAN-PWR-2200W-DC

Input voltage	**PA-5410, PA-5420, PA-5430, PA-5440, and PA-5445** • **AC power supplies**—100 to 240VAC (50-60Hz) • **DC power supplies**— -48 to -60VDC **PA-5450** • **AC power supplies**—100 to 120VAC and 200 to 240VAC (50-60Hz) • **DC power supplies**— -48 to -60VDC
Power Consumption	**PA-5410, PA-5420, PA-5430, PA-5440, and PA-5445** • Maximum—760W • Average—630W **PA-5450** • Varies based on your hardware configuration. Learn how to view the

©2026 Palo Alto Networks, Inc.

Specification	Value
	PA-5450 firewall power statistics to gauge power consumption.
Maximum Current Consumption	**PA-5410, PA-5420, PA-5430, PA-5440, and PA-5445** • **AC power supplies**—7A@100VAC, 3A@240VAC • **DC power supplies**— 15A@-48 VDC, 12A@-60VDC **PA-5450** • **AC power supplies**—14A@100-120VAC; 12.5A@200-240VAC • **DC power supplies**— 52A@-48 to -60VDC
Maximum Inrush Current	**PA-5410, PA-5420, PA-5430, PA-5440, and PA-5445** • **AC power supplies**—25A@230VAC; 50A@120VAC • **DC power supplies**—200A@72VDC **PA-5450** • **AC power supplies**—17.5A@230VAC; 35A@120VAC • **DC power supplies**—50A@72VDC

PA-5450 Firewall Component Electrical Specifications

This table describes PA-5450 power supply output and rated power consumption for the hardware components. For power configuration planning for the PA-5450, see Determine PA-5450 Firewall Power Configuration Requirements.

Component SKU Number	Power Specification (Power Produced (+) or Rated Consumption (-))	Notes
PAN-PA-5400-BC-A	-230 Watts	
PAN-PA-5400-MPC-A	-180 Watts	Includes power allocation for optics
PAN-PA-5400-DPC-A	-400 Watts	

©2026 Palo Alto Networks, Inc.

Component SKU Number	Power Specification (Power Produced (+) or Rated Consumption (-))	Notes
PAN-PA-5400-NC-A	-120 Watts	Includes power allocation for optics
PAN-PA-5450-FAN	-230 Watts	
PAN-PWR-2200W-AC	• Input Voltage—100-240VAC (50-60 Hz), Single phase • Output Power—+2200 Watts @ 200VAC or +1200 Watts @ 100VAC	
PAN-PWR-2200W-DC	• Input Voltage— -48 to -60VDC • Output Power— +2200 Watts	

PA-5400 Series Firewall Power Cord Types

The PA-5400 Series firewalls ship with two AC or two DC power cords by default.

The following table lists the PA-5410, PA-5420, PA-5430, PA-5440, and PA-5445 firewall power cords.

SKU Number	Description
PAN-PWR-CORD-US	Power cord for North America with IEC-60320 C13 and NEMA 5-15P cord ends, 10A, 125V max, 6ft
PAN-PWR-C13-C14	Power Cord for PDU with IEC-60320 C13 and IEC-60320 C14 cord ends, 15A, 250V max, 10ft
PAN-PWR-CORD-AUS	Power Cord, Australia, 10A, 250V, IEC-60320 C13 and AS/NZS 4417 cord ends, 6ft
PAN-PWR-CORD-EU	Power Cord, Europe, 10A, 250V, IEC-60320 C13 and CEE 7/7 SCHUKO cord ends, 6ft
PAN-PWR-CORD-JP-15	Power Cord, Japan, 15A, 125V, IEC-60320 C13 and JISC8303 cord ends, 6ft
PAN-PWR-CORD-JP-250V-15A	Power Cord, Japan, 15A, 250V, IEC-60320 C13 and NEMA L6-20P cord ends, 8ft, PSE Certified
PAN-PWR-CORD-SUI	Power Cord, Switzerland, 10A, 250V, IEC-60320 C13 and SEV1011 cord ends, 6ft

©2026 Palo Alto Networks, Inc.

SKU Number	Description
PAN-PWR-CORD-TW-15	Power Cord, Taiwan, 15A, 125V, IEC-60320 C13 and CNS 10917 cord ends, 6ft
PAN-PWR-CORD-UK	Power Cord, United Kingdom, 10A, 250V, IEC-60320 C13 and BS 1363 UK13 cord ends, 6ft

The following table lists the PA-5450 firewall power cords.

SKU Number	Description
PAN-PWR-C19-AUS	AC power cord with IEC-60320 C19 and AS/NZS 4417 cord ends, 3m
PAN-PWR-C19-EU	AC power cord with IEC-60320 C19 and CEE 7/7 SCHUKO cord ends, 3m
PAN-PWR-C19-JP	AC power cord with IEC-60320 C19 and NEMA L6-20P cord ends, 3m
PAN-PWR-C19-TW	AC power cord with IEC-60320 C19 and CNS 10917-3 cord ends, 3m
PAN-PWR-C19-UK	AC power cord with IEC-60320 C19 and BS 1363 UK13 cord ends, 3m
PAN-PWR-C19-US	AC power cord with IEC-60320 C19 and NEMA 6-20P cord ends, 3m
PAN-PWR-C19-US-L	AC power cord with IEC-60320 C19 and locking NEMA L6-20P cord ends, 3 m
PAN-PWR-C19-BR	Power Cord, Brazil, 16A, 250V, NBR14136 (IEC 60906-1) to IEC-60320-C19, 10-FT, Brazilian INMETRO certified
PAN-PWR-C19-C20	Power Cord, North America, 20A, 250V, IEC C19 to IEC C20, 10ft
PAN-PWR-C19-C14	Power Cord, North America, 15A, 250V, IEC C19 to IEC C14, 10ft
PAN-PWR-C19-US-120V	Power Cord, North America, 15A, 125V, C19 to NEMA 5-15P, 10ft
PAN-PWR-C19-JP-120V	Power Cord, Japan, 15A, 125V, JISC8303 to C19, 10ft, PSE Certified

©2026 Palo Alto Networks, Inc.

PA-5400 Series Firewall Environmental Specifications

The following table describes PA-5400 Series firewall environmental specifications.

Specification	Value
Operating temperature range	**PA-5410, PA-5420, PA-5430, PA-5440, and PA-5445** • 0° to 55°C (32° to 131°F) **PA-5450** • 0° to 50° C (32° to 122°F)
Storage temperature range	-20° to 70°C (-4°F to 158°F)
Humidity	10% to 90% non-condensing
Appliance airflow	Front to back
Electromagnetic Interference (EMI)	FCC Class A, CE Class A, VCCI Class A
Acoustic noise	**PA-5410, PA-5420, PA-5430, PA-5440, and PA-5445** • With AC PSUs — 69.0dBA • With DC PSUs — 66.6dBA **PA-5450** • With AC PSUs — 78.3dBA • With DC PSUs — 75.9dBA
Maximum operating altitude	10,000ft (3,048m)

©2026 Palo Alto Networks, Inc.

PA-5400 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-5400 Series firewalls, see PA-5400 Series Firewall Compliance Statements.

PA-5400 Series Firewall Compliance Statements

The following are the PA-5400 Series firewall hardware statements:

- **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.

- **NEBS Requirements**

  The following lists the Network Equipment Building System (NEBS) requirements for PA-5400 Series firewalls.

  - The firewall is intended to be installed in a Network Telecommunication Facility (Central Office) as part of a Common Bonding Network (CBN) or Isolated Bonding Network (IBN). Bare conductors must be coated with an appropriate antioxidant compound before crimp connections are made. All unplated connectors, braided strap, and bus bars must be brought to a bright finish and then coated with an antioxidant before they are connected.
  - Fastening hardware must be compatible with the materials being joined and must preclude loosening, deterioration, and electrochemical corrosion of the hardware and the joined materials.
  - The firewall is suitable for connection to the Central Office or Customer Premise Equipment (CPE).
  - The DC battery return wiring on the firewall must be connected as an isolated DC return (DC-I).

  The intra-building ports (RJ-45 Ethernet ports, AUX ports, HA ports, and the MGT port) of the equipment or subassembly are suitable for connection to only intra-building or unexposed wiring or cabling. The intra-building port(s) of the equipment or subassembly must not be metallically connected to interfaces that connect to the Outside Plant (OSP) or its wiring. These interfaces are designed for use as intra-building interfaces only (Type 2 or Type 4 ports as described in GR-1089-CORE, Issue 6) and require isolation from the exposed OSP cabling. The addition of primary protectors is not sufficient protection to connect these interfaces metallically to OSP wiring.

  The firewall must be connected to an external Special Protection Device (SPD) when installed and connected to commercial AC power.

©2026 Palo Alto Networks, Inc.

- **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.

 ©2026 Palo Alto Networks, Inc.

 ©2026 Palo Alto Networks, Inc.