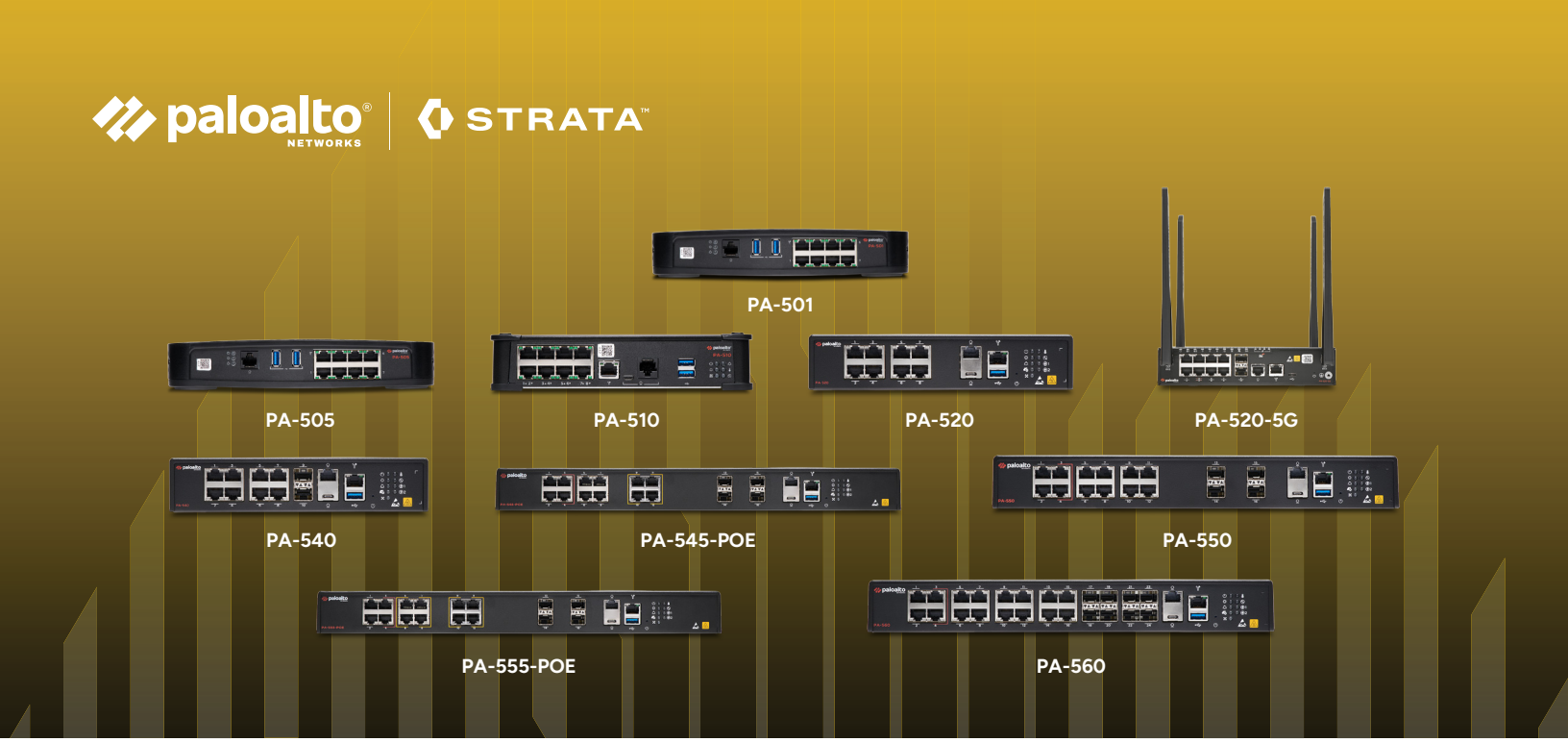


PA-500 Series Quantum-Optimized NGFWs

Palo Alto Networks PA-500 Series Quantum-Optimized NGFWs comprise the PA-501, PA-505, PA-510, PA-520, PA-520-5G, PA-540, PA-545-POE, PA-550, PA-555-POE, and PA-560 models. This series brings ML-Powered NGFW capabilities to distributed enterprise branch offices, retail locations, and midsize organizations.

PAN-OS®, the operating system of the PA-500 Series NGFWs, runs all Palo Alto Networks NGFWs. PAN-OS natively classifies all traffic—including applications, threats, and content—that runs your organization and then ties that traffic to the user regardless of location or device type. This traffic serves as the basis of your security policies, resulting in an improved security posture and reduced incident response time. PAN-OS embeds AI in the firewall core to provide inline signatureless attack prevention for file-based attacks while identifying and immediately stopping never-before-seen phishing attempts.

Post-Quantum Cryptography Optimizations

PA-500 Series is a post-quantum cryptography (PQC)-ready device that helps you achieve quantum-safe security in hardware and software with PAN-OS 12.1. PA-500 Series NGFWs support:

- **PQC for PQC SSL/TLS decryption, PQC VPN site-to-site, PQC SSL/TLS Cipher Translation Proxy, and PQC SSL/TLS Service Profile** for management access to the firewall.
- **PQC algorithms**, including NIST standards, like ML-KEM, ML-DSA, and SLH-DSA, as well as prestandard PQCs, like Classic McEliece, BIKE, HQC, Frodo-KEM, and NTRU-Prime.

For more information, see Support for Post-Quantum Features in TechDocs.

Prevention of Malicious Activity Concealed in Encrypted Traffic

PA-500 Series NGFWs provide the ability to:

- **Inspect and apply the policy** to SSL/TLS-encrypted traffic (both inbound and outbound), traffic that uses SSLv3, TLSv1.1, TLSv1.2, and TLSv1.3, as well as application protocols SMTP, WebSocket, gRPC, HTTP/1.0, HTTP/1.1, and HTTP/2.D.
- **Decrypt and inspect SSL/TLS sessions** with the classic key exchange algorithms RSA, ECDHE, DHE, and post-quantum key exchange standards ML-KEM, HQC, as well as experimental BIKE and Frodo-KEM.
- **Gather metrics on TLS traffic**, such as the amount of encrypted traffic, SSL/TLS versions, and ciphers.
- **Support suites**, such as classic key exchanges RSA, ECDHE, and DHE, as well as post-quantum key exchanges ML-KEM and HQC—without needing decryption—bringing added visibility to cryptographic information from all SSL/TLS sessions that pass-through the firewall.
- **Enable control over using legacy TLS protocols**, insecure and deprecated ciphers, and misconfigured certificates, including a mismatched Server Name Indication (SNI) to certificate Common Name (CN), to mitigate risks.
- **Facilitate easy decryption deployment** and use enhanced built-in logs to troubleshoot issues across both client-side and server-side sessions independently for a seamless troubleshooting experience, whether it's missing intermediate certificates or pinned certificates.
- **Enable or disable decryption flexibly**—based on the URL category, source and destination zone, address, user, user group, device, and port—for privacy and regulatory compliance purposes.

In addition, this feature provides Decrypt Mirror, which enables you to create a copy of decrypted traffic from the firewall and send it to traffic collection tools for forensics, historical purposes, or data loss prevention (DLP).

Read the *Decryption: Why, Where and How* whitepaper to learn about decryption to prevent threats and secure your business.

Highlights

- **High-performance enterprise branch NGFW series**.
- **Powered by Precision AI®**, a groundbreaking AI-driven engine that analyzes and prevents threats in real time.
- **High port density** with up to 24 copper and fiber optic interfaces.
- **Up to 330W Power over Ethernet (PoE) support**.
- **IEEE 802.3bt support** with a maximum of 90W of power per PoE port.
- **Zero touch provisioning (ZTP)** to simplify deployment.
- **Active/active and active/passive modes** to support high availability.
- **A single-pass architecture** to deliver predictable performance with security services.
- **Managed with Strata™ Cloud Manager**, the industry's first AI-powered unified management and operations solution for network security.
- **Leader in the 2025 Gartner® Magic Quadrant™** for Hybrid Mesh Firewalls.
- **Leader in The Forrester® Wave:** Enterprise Firewall Solutions, Q4 2024.

Application Identification and Categorization with Full Layer 7 Inspection

App-ID™ identifies and categorizes all applications, on all ports, all the time, with full Layer 7 inspection, supporting the following capabilities:

- Uses advanced techniques, such as protocol decoding, heuristics, and signature matching, to accurately identify applications across the network, regardless of the port, protocol, or encryption methods used. The optional App-ID Cloud Engine (ACE) service provides on-demand App-IDs for SaaS applications.
- Provides a comprehensive understanding of the risks and values associated with various applications, which aids in informed decision-making about network security policies.
- Allows for the effective enforcement of security policies tailored to specific applications, by centralizing the identification and control of applications at the firewall level.
- Identifies and manages evasive or custom applications that typically bypass traditional security measures.
- Continuously updates its application identifications, ensuring it stays effective against the latest application trends and tactics.
- Uses cutting-edge AI techniques to enhance precision in identifying and categorizing AI-powered applications. These techniques ensure that the most advanced and dynamic applications are accurately recognized and appropriately managed within the network.

For more information, see the *App-ID* tech brief.

User Security Enforcement

PA-500 Series NGFWs enforce security for users at any location, on any device, while adapting policies based on their activity. They include the ability to:

- **Enable visibility, security policies, reporting, and forensics** based on users, groups, and IP addresses.
- **Apply consistent policies** regardless of users' locations (office, home, travel, etc.) and devices. Such devices include iOS and Android mobile devices; macOS, Windows, and Linux desktops and laptops; Citrix and Microsoft VDI; and terminal servers.
- **Leverage IP geolocation** to automatically enforce security policies based on geographic location, enabling you to reduce the attack surface, meet compliance requirements, and control application access by blocking traffic to and from specific countries or regions.
- **Consistently authenticate and authorize your users**, regardless of location and where user identity is stored (cloud, on-premises directories, or both), to move quickly toward a zero trust security posture with Cloud Identity Engine—a cloud-based architecture for identity-based security.
- **Secure all applications with passwordless authentication**, whether on-premises, SaaS, or hybrid.
- **Provide dynamic security actions** based on user behavior to restrict suspicious or malicious users by defining Cloud Dynamic User Groups (CDUGs) on the firewall to take risk-based, time-bound security actions without waiting to apply changes to user directories.
- **Prevent corporate credentials** from both leaking to third-party websites and reusing stolen credentials by enabling multifactor authentication (MFA) at the network layer for any application without changes.

- **Easily integrate with a wide range of repositories** to work with user information, including wireless LAN controllers, VPNs, directory servers, and security information and event management (SIEM) tools.
- **Automate policy recommendations** that save time and reduce the chance of human error.

For more information, see the *Cloud Identity Engine* solution brief.

Single-Pass Architecture

PA-500 Series NGFWs process packets by using a single-pass architecture, enabling the NGFWs to:

- Perform networking, policy lookup, application and decoding, and signature matching—for all threats and content—in a single pass, reducing the amount of processing overhead required to perform multiple functions in one security device.
- Avoid introducing latency by scanning traffic for all signatures in a single pass, using stream-based, uniform signature matching.
- Produce consistent and predictable performance when security subscriptions are enabled.

For more information, see the *Single-Pass Architecture* whitepaper.

AI-Powered Unified Management and Operations with Strata Cloud Manager

Manage your PA-500 Series NGFWs with Strata Cloud Manager, which enables you to:

- **Gain complete visibility across your network security estate:** Achieve real-time, comprehensive visibility of your entire network security landscape, including all users, applications, devices, and the most critical threats that need attention through a unified interface.
- **Enable simple and consistent network security lifecycle management:** Oversee configuration and policy management across all enforcement points, including SASE, hardware and software firewalls, as well as all security services to ensure consistency and reduce operational overhead.
- **Strengthen security posture in real time:** Leverage AI-powered analysis to detect, resolve, and optimize policy anomalies like shadow and redundant policies and overly permissive or unused rules. Improve your security posture with integrated best practice recommendations and maintain compliance with industry and InfoSec standards.
- **Proactively resolve network disruptions and enhance user experience:** Predict, diagnose, and resolve network health issues—such as user experience problems, capacity bottlenecks, CVE vulnerabilities, service connection issues, and 130 other categories of issues—up to 90 days in advance to ensure smooth operations.
- **Resolve issues fast with instant knowledge at your fingertips:** Strata Copilot™, our AI-powered assistant, features a natural language interface so you can quickly find, understand, and address security and operational challenges before they escalate. Plus, with its streamlined case creation capabilities, you get rapid support when you need it most.

For more information, see the *Strata Cloud Manager* datasheet.

Layer 2 Switching

Select PA-500 Series NGFW models add a Layer 2 switching function on top of the existing security and SD-WAN capabilities. These models are PA-545-POE, PA-550, PA-555-POE, and PA-560.

Layer 2 switching removes operational complexities by helping you consolidate all endpoints on the NGFW, giving you visibility into the intra-VLAN traffic that flows through the NGFW. You can microsegment this traffic and inspect it up to Layer 7 for enhanced security.

Best-in-Class Cloud-Delivered Security Services Powered by Precision AI

PA-500 Series NGFWs provide best-in-class security with Cloud-Delivered Security Services (CDSS). At the heart of our CDSS is Precision AI. Unlike traditional reactive tools, Precision AI empowers your defenses with proactive threat detection, inline prevention, and automated response—stopping the most evasive, never-before-seen attacks before they cause damage. Backed by threat intelligence from our over 75,000 customers globally, our cloud-delivered services continuously learn, adapt, and evolve. Integrated seamlessly with our NGFW and SASE platforms, CDSS delivers unified protection across web, DNS, email, applications, and more—no matter where your users or data reside.

Whether you're navigating hybrid work, embracing cloud transformation, or defending against sophisticated adversaries, CDSS gives you the visibility, automation, and confidence to stay ahead.

Advanced Threat Prevention

Advanced Threat Prevention is the first intrusion prevention system (IPS) that stops zero-day command-and-control (C2) attacks and unknown exploits inline. In addition to traditional IPS capabilities, it delivers industry-leading protection against known and unknown threats.

For more information, see the *Advanced Threat Prevention* datasheet.

Advanced WildFire

Advanced WildFire® is the industry's largest cloud-based malware prevention engine. It protects organizations from highly evasive threats by using patented ML detection engines, enabling automated protections across networks, cloud, and customer application endpoints.

For more information, see the *Advanced WildFire* datasheet.

Advanced URL Filtering

Advanced URL Filtering analyzes URL strings and web content in real time and classifies them into benign or malicious categories, which teams can build into NGFW policies to control web traffic. It protects against phishing, malware, ransomware, C2 communications, and evasive web-based attacks.

For more information, see the *Advanced URL Filtering* datasheet.

Advanced DNS Security

Advanced DNS Security delivers real-time protection that instantly blocks sophisticated DNS request and response-based threats—including DNS hijacking, domain generation algorithms (DGA), DNS tunneling, and C2 callbacks. It uses inline, AI-powered detection models to analyze every DNS request and response in real time. These models enable precise identification of never-before-seen malicious domains, DNS tunneling, C2 activity, and network-level DNS hijacking. This powerful first line of defense identifies and stops threats at the DNS layer—whether they originate outside or inside the network.

For more information, see the *Advanced DNS Security* datasheet.

Advanced IP Defense

Advanced IP Defense combines real-time IP intelligence with direct-to-IP detection to stop threats that bypass traditional DNS-based and URL-based security controls. Advanced IP Defense implements zero trust DNS to block direct-to-IP C2 connections and exfiltration attempts by correlating outbound traffic with DNS history. Advanced IP Defense uses Precision AI IP intelligence to identify attacker infrastructure in real time using full-lifecycle telemetry.

For more information, see the *Advanced IP Defense* datasheet.

Device Security

Secure your entire attack surface with a unified, AI-first solution that provides comprehensive protection and monitoring. It discovers all connected devices and then identifies and mitigates hidden risks that would otherwise remain invisible or elusive to even the most seasoned InfoSec professionals.

For more information, see the *Device Security* solution brief.

SaaS Security

SaaS Security delivers broad visibility and real-time control over all SaaS applications, including GenAI apps. Moreover, SaaS Security provides robust data protection by monitoring and securing the unapproved movement and storage of sensitive data across various SaaS platforms.

For more information, see the *SaaS Security* solution brief.

AI Access Security

AI Access Security™ empowers organizations to monitor the adoption and usage of sanctioned and unsanctioned GenAI apps. It proactively prevents sensitive data leakage and provides continuous risk monitoring so organizations can safely adopt and use third-party GenAI tools.

For more information, see the *AI Access Security* datasheet.

Advanced SD-WAN

Easily adopt SD-WAN by simply enabling it on your existing firewalls with integrated security. Get an exceptional end-user experience and ensure SLAs by using SD-WAN path measurements and application steering capabilities to intelligently direct applications to the best performing paths.

For more information, refer to the SD-WAN documentation in TechDocs.

Table 1. PA-500 Series NGFWs Performance and Capacities										
	PA-501	PA-505	PA-510	PA-520	PA-520-5G	PA-540	PA-545-POE	PA-550	PA-555-POE	PA-560
Firewall throughput (appmix)*	0.8 Gbps	1.2 Gbps	1.8 Gbps	2.8 Gbps	2.6 Gbps	3.8 Gbps	5.0 Gbps	6.5 Gbps	7.5 Gbps	8.5 Gbps
Threat Prevention throughput (appmix)†	0.5 Gbps	0.8 Gbps	1.2 Gbps	1.8 Gbps	1.6 Gbps	2.2 Gbps	3.0 Gbps	4.5 Gbps	5.0 Gbps	6.0 Gbps
IPsec VPN throughput‡	0.24 Gbps	0.4 Gbps	0.8 Gbps	1.5 Gbps	1.4 Gbps	2.0 Gbps	3.0 Gbps	4.0 Gbps	4.5 Gbps	5.5 Gbps
Max concurrent sessions§	30K	64K	98K	148K	148K	248K	298K	398K	448K	598K
New sessions per second‖	5K	10K	15K	25K	25K	50K	55K	70K	75K	100K
Virtual systems (base/max)#	—	—	—	—	1/2	1/2	1/2	1/5	1/5	1/5

Note: Results were measured on PAN-OS 12.2.

* Firewall throughput is measured with App-ID and logging enabled by using appmix transactions.

† Threat Prevention throughput is measured with App-ID, IPS, antivirus, antispyware, WildFire, file blocking, and logging enabled using appmix transactions.

‡ IPsec VPN throughput is measured with 64 KB HTTP transactions and logging enabled.

§ Maximum concurrent sessions are measured by using HTTP transactions.

‖ New sessions per second is measured with application override by using 1 byte HTTP transactions.

Adding virtual systems over the base quantity requires a separately purchased license.

Table 2. PA-500 Series Networking Features
Interface Modes
L2 mode (not available on MC-LAG aggregate interfaces), L3 mode, tap, and virtual wire (transparent mode).
Routing
The advanced routing engine is the only routing engine supported.
OSPFv2/v3 and MP-BGP with graceful restart, RIP, and static routing.
Policy-based forwarding.
DHCPv4 server and DHCPv4 relay.
Multicast: PIM-SM, PIM-SSM, IGMPv2, and v3.
Bidirectional Forwarding Detection (BFD) and multihop BFD.
Advanced SD-WAN
Path quality measurement (jitter, packet loss, and latency).
Bandwidth monitoring.
Key exchange: Manual key, IKEv1, and IKEv2 (pre-shared key and certificate-based authentication).
Post-quantum PPK.
Multi-VR and LR support over the SD-WAN overlay.
Prisma® Access Hub (hybrid SASE).
Autonomous Digital Experience Management (ADEM) for NGFW support.
Layer 2 Switching
Supported platforms: PA-545-POE, PA-550, PA-555-POE, and PA-560.
Minimum PAN-OS version: 12.2.2.
Layer 2 switching function on all data ports of the device.
Transport traffic of multiple VLANs over a single physical link with VLAN trunking.
Microsegment and inspect (up to Layer 7) Intra-VLAN traffic.

Table 2. PA-500 Series Networking Features (continued)
Layer 2 Switching
Ensure loop-free topologies for Layer 2 domains with Multiple Spanning Tree Protocol.
Prevent unknown unicast, multicast, and broadcast storms in Layer 2 domains.
IPv6
IPv6 inspection in L2, L3, tap, and virtual wire mode (transparent mode).
Support for dual-stack and IPv6-only networks.
Features: IPv6 geolocalization, OSPFv3, MP-BGP, NAT64, and NPTv6.
DHCPv6 client with prefix delegation (PD) support. Stateless address autoconfiguration (SLAAC) server support.
IPsec and SSL VPN
Key exchange: Manual key, IKEv1, and IKEv2 (pre-shared key and certificate-based authentication).
Encryption: 3DES, AES (128-bit, 192-bit, and 256-bit).
Authentication: MD5, SHA-1, SHA-256, SHA-384, and SHA-512.
GlobalProtect® Large Scale VPN for simplified configuration and management.*
Secure remote access over IPsec and SSL VPN tunnels using GlobalProtect gateway and portals including PQC.*
VLANs
802.1Q VLAN tags per device or per interface: 4,094/4,094.
Aggregate interfaces (802.3ad) and LACP.

* Requires a GlobalProtect license.

Table 3. PA-500 Series Hardware Specifications
I/O
PA-501, PA-505: 1G RJ45 (7)
PA-510, PA-520: 1G RJ45 (8)
PA-520-5G: Embedded 5G cellular module, 1G RJ45 (8), 1G SFP (2)
PA-540: 1G RJ45 (8), 1G SFP (2)
PA-545-POE: 1G RJ45 (6), 1G RJ45 bypass (2), 1G/2.5G (4)/PoE, 1G SFP (4)
PA-550: 1G RJ45 (10), 1G RJ45 bypass (2),1G SFP (2), 1G/10G SFP/SFP+ (2)
PA-555-POE: 1G RJ45 (2), 1G RJ45 bypass (2), 1G RJ45 (4)/PoE, 1G/2.5G (4)/PoE, 1G SFP (2), 1G/10G SFP/SFP+ (2)
PA-560: 1G RJ45 (14), 1G RJ45 bypass (2), 1G SFP (4), 1G/10G SFP/SFP+ (4)
Management I/O
PA-501, PA-505: 10/100/1000 out-of-band management port (1), USB port (2), and RJ45 console port (1)
PA-510: 10/100/1000 out-of-band management port (1), USB port (2), RJ45 console port (1), and Micro USB console port (1)
PA-520, PA-520-5G, PA-540, PA-545-POE, PA-550, PA-555-POE, PA-560: 10/100/1000 out-of-band management port (1), USB port (1), RJ45 console port (1), and USB-C console port (1)
Storage Capacity
PA-501, PA-505, PA-510: 128 GB
PA-520, PA-520-5G, PA-540, PA-545-POE, PA-550, PA-555-POE: 120 GB
PA-560: 240 GB
Trusted Platform Module (TPM)
Integrated with TPM for secure boot, hardware root of trust, and securing system secrets.

Table 3. PA-500 Series Hardware Specifications (continued)	
Power Over Ethernet	
PA-545-POE total PoE budget: 181W, PoE ports (4), maximum loading on a single port: 90W **PA-555-POE total PoE budget:** 330W, PoE ports (8), maximum loading on a single port: 90W	
Power Consumption	
Model	**Max Power Consumption**
PA-501, PA-505	23W
PA-510	34.3W
PA-520, PA-540	30W
PA-520-5G	36W
PA-545-POE*	336W (with 181W PoE output)
PA-550	57W
PA-555-POE*	503W (with 332W PoE output)
PA-560	106W
Max BTU/hr	
PA-501, PA-505: 78	
PA-510: 117	
PA-520, PA-540: 102	
PA-520-5G: TBD	
PA-545-POE: 1145 (with 181W PoE output)	
PA-550: 195	
PA-555-POE: 1715 (with 332W PoE output)	
PA-560: 361	
Input Voltage (Input Frequency)	
100–240 VAC (50-60 Hz)	
Maximum Current Consumption	
PA-501, PA-505: 2 A @ 12 VDC	
PA-510: 2.5 A @ 12 VDC	
PA-520, PA-520-5G, PA-540: 4 A @ 12 VDC	
PA-545-POE: 6 A @ 54 VDC	
PA-550: 5 A @ 12 VDC	
PA-555-POE: 9 A @ 54 VDC	
PA-560: 8 A @ 12 VDC	

* With one or more provided AC adapters.

Table 3. PA-500 Series Hardware Specifications (continued)
Dimensions
PA-501, PA-505: 1.63" H x 6.42" D x 9.53" W
PA-510: 1.74" H x 8.83" D x 8.07" W
PA-520, PA-540: 1.74" H x 10.4" D x 8" W
PA-520-5G: 1.74" H x 8.6" D x 8" W
PA-550, PA-560: 1.74" H x 12.1" D x 13" W
PA-545-POE, PA-555-POE: 1.75" H x 12.6" D x 16.1" W
Weight (Standalone Device and As Shipped)
PA-501, PA-505: 3.1 lbs/5.9 lbs
PA-510: 5.0 lbs/7.8 lbs
PA-520, PA-540: 5.8 lbs/8 lbs
PA-520-5G: 4.8 lbs
PA-545-POE: 13.5 lbs/19.8 lbs
PA-550: 11.2 lbs/15.6 lbs
PA-555-POE: 13.5 lbs/20.2 lbs
PA-560: 11.2 lbs/15.6 lbs
Safety
cTUVus and CB
EMI
PA-501, PA-505, PA-510: FCC Class B, CE Class B, and VCCI Class B
PA-520, PA-540, PA-545-POE, PA-550, PA-555-POE, PA-560: FCC Class A, CE Class A, and VCCI Class A
PA-520-5G: TBD
Certifications
See our Compliance page.
Environment
Operating temperature: 32°F to 104°F, 0°C to 40°C
Nonoperating temperature: -4°F to 158°F, -20°C to 70°C
Passive cooling: PA-501, PA-505, PA-510, PA-520, PA-520-5G, PA-540, PA-545-POE, PA-550, and PA-555-POE
Active cooling: PA-560

PA-500 Series Ordering Information

Table 4 lists key SKUs for the PA-500 Series. For detailed information about the complete SKU list, including LAB bundles, spares, software subscriptions, and support, work with your Palo Alto Networks account team and NextWave Partners.

Table 4. PA-500 Series Ordering Information

	Accessory	Short Description	Model(s)
Power Adapters*	PAN-PWR-25W-AC	25W spare power adapter	PA-501, PA-505
	PAN-PWR-40W-12V-AC	40W spare power adapter	PA-510
	PAN-PWR-66W-12V-AC-A	66W spare power adapter	PA-520, PA-520-5G, PA-540
	PAN-PWR-150W-12V-AC-A†	150W spare power adapter	PA-550, PA-560
	PAN-PWR-350W-54V-AC-A	350W spare power adapter	PA-545-POE
	PAN-PWR-550W-54V-AC-A	550W spare power adapter	PA-555-POE
Accessory Kit	PAN-PA-505-ACC	Replacement accessory kit for PA-505 or PA-501. The kit is included in the system (25W AC power adapter, US power cord, Ethernet cable).	PA-501, PA-505
	PAN-PA-510-ACC	Replacement accessory kit for PA-510. The kit is included in the system (40W AC power adapter, US power cord, Micro USB console cable, Ethernet cable).	PA-510
	PAN-PA-500-SML-ACC	Replacement accessory kit for PA-520, PA-520-5G, and PA-540. The kit is included in the system (66W AC power adapter, US power cord, Ground Lug, USB-C console cable, Ethernet cable).	PA-520, PA-520-5G, PA-540
	PAN-PA-500-MED-ACC	Replacement accessory kit for PA-550, PA-560, compatible with PA-520, PA-520-5G, and PA-540. The kit is included in the system (150W AC power adapter, US power cord, Ground Lug, USB-C console cable, Ethernet cable).	PA-520, PA-540, PA-550, PA-560
	PAN-PA-545-POE-ACC	Replacement accessory kit for PA-545-POE. The kit is included in the system (350W AC power adapter, US power cord, Ground Lug, USB-C console cable, Ethernet cable).	PA-545-POE
	PAN-PA-555-POE-ACC	Replacement accessory kit for PA-555-POE. The kit is included in the system (530W AC power adapter, US power cord, Ground Lug, USB-C console cable, Ethernet cable).	PA-555-POE
	PAN-1RU-4POST-RACK-10	1RU 4-Post Rack Mount for: 1x PA-501 and one power adapter 1x PA-505 and one power adapter 2x PA-510 and two power adapters	PA-501, PA-505, PA-510
	PAN-1RU-4POST-RACK-11	1RU 4-Post Rack Mount for: 2x PA-520s and four power adapters 2x PA-540s and four power adapters 1x PA-550 and two power adapters 1x PA-560 and two power adapters	PA-520 PA-540 PA-550 PA-560
	PAN-1RU-4POST-RACK-12	1RU 4-Post Rack Mount for: 1x PA-545-POE and two power adapters, 1x PA-555-POE and two power adapters	PA-545-POE, PA-555-POE
	PAN-1RU-4POST-RACK-16	1RU 4-Post Rack Mount for: 1x PA-520-5G and two power adapters (includes the antenna cables for rack mount).	PA-520-5G

• One power adapter ships with each firewall. A second redundant power adapter is available as an optional accessory for platforms that support dual power adapters.

† Also compatible with PA-520, PA-520-5G, and PA-540.

Table 4. PA-500 Series Ordering Information (continued)			
	Accessory	**Short Description**	**Model(s)**
5G Cellular	PAN-PA-5G-ANTENNA	5G Direct Mount SMA Spare Antenna SMA male connector. Compatible with PA-520-5G, PA-415-5G (quantity one).	PA-520-5G
	PAN-PA-5G-ANTENNA-SET	5G Direct Mount SMA Spare Antenna SMA male connector. Compatible with PA-520-5G, PA-415-5G (quantity four).	
	PAN-PA-5G-ANT-4X4-5M-SMAM	5G Remote Mount SMA Antenna. 4x4 SMA Male connectors with 5-meter cable. Compatible with PA-520-5G, PA-415-5G, and PA-455-5G.	
	PAN-PA-RFADPT-NM-SMAF	RF Adapter N-Male to SMA-Female (quantity one).	

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

© 2026 Palo Alto Networks, Inc. A list of our trademarks in the United States and other jurisdictions can be found at https://www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

strata_ds_pa-500-series_082026