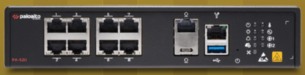
PA-505

PA-510



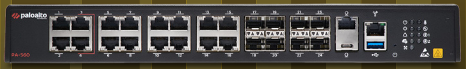
PA-520

PA-540

PA-545-POE

PA-550

PA-555-POE



PA-560

PA-500 Series

Palo Alto Networks PA-500 Series Next-Generation Firewalls (NGFWs) comprise the PA-505, PA-510, PA-520, 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 businesses.

The controlling element of the PA-500 Series NGFWs is PAN-OS®, the same software that runs all Palo Alto Networks NGFWs. PAN-OS natively classifies all traffic, inclusive of applications, threats, and content, and then ties that traffic to the user regardless of location or device type. The application, content, and user—the elements that run your business—serve as the basis of your security policies, resulting in an improved security posture and reduced incident response time. PAN-OS embeds machine learning (ML) in the core of the firewall to provide inline signatureless attack prevention for file-based attacks while identifying and immediately stopping never-before-seen phishing attempts.

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 interfaces.
- Up to 330W Power over Ethernet (PoE) support.
- IEEE 802.3bt support with a maximum of 90W of power per PoE port.
- Simplifies deployment with Zero Touch Provisioning (ZTP).
- Supports high availability with active/active and active/passive modes.
- Built with 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 Firewall.
- 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 even the most advanced and dynamic applications are accurately recognized and appropriately managed within the network.

For more information, see our 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 and 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 both corporate credentials from leaking to third-party websites and the reuse of 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 our Cloud Identity Engine solution brief.

Unique Approach to Packet Processing

PA-500 Series NGFWs process packets by using a single-pass architecture. Using this approach, the NGFWs are able to:

- Perform networking, policy lookup, application and decoding, and signature matching—for all threats and content—in a single pass. This significantly reduces 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 (see table 1).

Post-Quantum Cryptography Ready

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

- Post-quantum cryptography (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.

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.
- 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 such suites 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 let you 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.

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:** Manage 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:** With 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.

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 even the most evasive, never-before-seen attacks before they cause damage. Backed by threat intelligence from our over 70,000 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 powered by Precision AI gives you the visibility, automation, and confidence to stay ahead.

Advanced Threat Prevention

Analyze up to 673 million new sessions daily and proactively block 28.2 billion threats in real time—including zero-day exploits, malware, command-and-control (C2) traffic, and evasive techniques—to deliver cutting-edge security at unprecedented scale.

Advanced WildFire

Proactively stop up to 450,000 new threats every day with the industry's most powerful malware prevention engines. Advanced WildFire® identifies and blocks a wide range of advanced threats, including zero-day malware, ransomware, remote access Trojans (RATs), weaponized documents, and other evasive attack techniques—before they impact your organization.

Advanced URL Filtering

Safeguard web access by blocking up to 151 million threats inline every day, while analyzing 3.8 billion new URLs daily. Advanced URL Filtering protects against phishing, malware, ransomware, C2 communications, and evasive web-based attacks.

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 analyzes over 1.1 billion new domains daily and identifies up to 7.7 million newly malicious domains, preventing more than 2 billion threats inline. This powerful first line of defense identifies and stops threats at the DNS layer—whether they originate from outside or within the network.

Device Security

Secure every connected device with a solution tailored to the industry (including manufacturing, retail, healthcare, high tech, and general enterprise), and achieve a 90% device discovery rate within 48 hours—providing prioritized vulnerability and risk assessments. Also, identify anomalies, get least-privileged access control security policy recommendations, and virtually patch vulnerabilities all in one single NetSec platform.

SaaS Security

Discover and control all SaaS consumption with visibility into over 75,000 SaaS apps and DLP controls for more than 150 SaaS apps. Prevent SaaS misconfigurations with posture management for over 117 SaaS apps, as well as SaaS inline tenancy control for 39 apps.

AI Access Security

Enable the safe use of GenAI with real-time visibility into GenAI apps, user access controls, data protection, and continuous risk monitoring. AI Access Security™ provides an industry-leading catalog of over 2,500 GenAI apps, including over 15 GenAI-specific application attributes to accurately identify and mitigate risk. It includes posture management for more than 13 GenAI apps and SaaS inline tenancy control for 11 apps.

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 steer applications to the best performing paths.

PA-500 Series Specifications

Table 1. PA-500 Series NGFWs Performance and Capacities

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

Note: Results were measured on PAN-OS 12.1.

[*] 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, DNS Security, file blocking, and logging enabled, utilizing appmix transactions..

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

[§] Maximum concurrent sessions are measured using HTTP transactions.

[‖] New sessions per second is measured with application override, 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, tap, and virtual wire (transparent mode).
Routing
OSPFv2/v3 and MP-BGP with graceful restart, RIP, and static routing.
Policy-based forwarding.
PPPoE and DHCP clients are supported for dynamic address assignment for both IPv4 and IPv6.
DHCPv4 server.
Multicast: PIM-SM, PIM-SSM, IGMPv2, and v3.
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.
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.

Table 2. PA-500 Series Networking Features (continued)
IPsec and SSL VPN
Key exchange: Manual key, IKEv1, and IKEv2 (pre-shared key and certificate-based authentication).
Encryption: 3DES and AES (128-bit, 192-bit, and 256-bit).
Authentication: MD5, SHA-1, SHA-256, SHA-384, and SHA-512.
Secure access over IPsec and SSL VPN tunnels using GlobalProtect® gateway and portals.*
VLANs
802.1Q VLAN tags per device/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-505: 1G RJ45 (7) PA-510: 1G RJ45 (8) PA-520: 1G RJ45 (8) PA-540: 1G RJ45 (8), 1G SFP (2) PA-545-POE: 1G RJ45 (8), 1G/2.5G (4)/PoE, 1G SFP (4) PA-550: 1G RJ45 (12), 1G SFP (2), 1G/10G SFP/SFP+ (2) PA-555-POE: 1G RJ45 (4), 1G RJ45 (4)/PoE, 1G/2.5G (4)/PoE, 1G SFP (2), 1G/10G SFP/SFP+ (2) PA-560: 1G RJ45 (16), 1G SFP (4), 1G/10G SFP/SFP+ (4)	
Management I/O	
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-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-505, PA-510: 128 GB PA-520, 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.	
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-505	23W
PA-510	34.3W
PA-520 or PA-540	30W
PA-545-POE*	336W (with 181W PoE output)
PA-550	57W
PA-555-POE*	503W (with 332W PoE output)
PA-560	106W

* With one or more provided AC adapters.

Table 3. PA-500 Series Hardware Specifications (continued)
Max BTU/hr
PA-505: 78 PA-510: 117 PA-520 or PA-540: 102 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)
Max Current Consumption
PA-505: 2 A @ 12 VDC PA-510: 2.5 A @ 12 VDC PA-520 or 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
Dimensions
PA-505: 1.63” H x 6.42” D x 9.53” W (43.9 mm H x 163 mm D x 242 mm W) PA-510: 1.74” H x 8.83” D x 8.07” W (43.9 mm H x 224 mm D x 205 mm W) PA-520 or PA-540: 1.74” H x 10.4” D x 8” W (43.9 mm H x 265 mm D x 203 mm W) PA-550 or PA-560: 1.74” H x 12.1” D x 13” W (43.9 mm H x 37 mm D x 330 mm W) PA-545-POE or PA-555-POE: 1.75” H x 12.6” D x 16.1” W (43.9 mm H x 314 mm D x 409 mm W)
Weight (Standalone Device/As Shipped)
PA-505: 3.1 lbs/5.9 lbs PA-510: 5.0 lbs/7.8 lbs PA-520 or PA-540: 5.8 lbs/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, CB
EMI
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
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-505, PA-510, PA-520, PA-540, PA-545-POE, PA-550, and PA-555-POE Active cooling: PA-560

Table 4. PA-500 Series Ordering Information

Accessory	Short Description	Models
PAN-PWR-25W-AC	25W spare power adapter	PA-505
PAN-PWR-50W-AC*	50W spare power adapter*	PA-510
PAN-PWR-150W-12V-AC-A	150W spare power adapter	PA-520, PA-540, PA-550, and 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
PAN-PA-400-RACKTRAY*	1RU 4-post rack mount for: two PA-510s and four power adapters	PA-510
PAN-1RU-4POST-RACK-11	1RU 4-post rack mount for: One PA-560 and two power adapters, One PA-550 and two power adapters, Two PA-540s and four power adapters, Two PA-520s and four power adapters.	PA-520, PA-540, PA-550, and PA-560
PAN-1RU-4POST-RACK-12	1RU 4-post rack mount for: One PA-555-POE and two power adapters, One PA-545-POE and two power adapters	PA-545-POE and PA-555-POE

* Need to be separately quoted.

paloalto NETWORKS

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