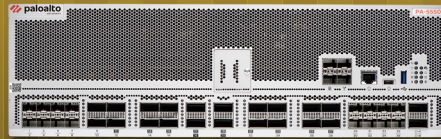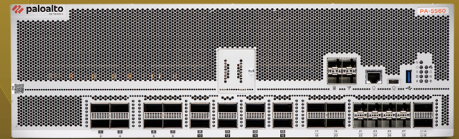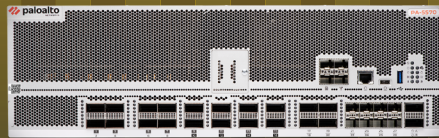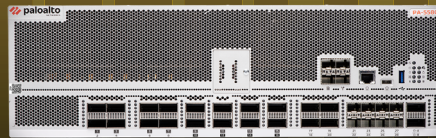PA-5540 PA-5550 PA-5560
PA-5570 PA-5580

PA-5500 Series

Palo Alto Networks PA-5500 Series Quantum Optimized Next-Generation Firewalls (NGFWs)—comprising the PA-5540, PA-5550, PA-5560, PA-5570, and PA-5580—are ideal for high-speed data center, internet gateway, and service provider deployments. This series provides visibility into and secures all traffic, including post-quantum encrypted traffic.

The operating system of the PA-5500 Series is PAN-OS®, the same software that runs all Palo Alto Networks NGFWs. PAN-OS natively classifies all traffic—including applications, threats, and content—and then ties that traffic to the user regardless of location or device type. The applications, content, and users 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

- The world's first quantum-optimized NGFW.

- Built with FE-400 ASIC for high throughput and low latency for data centers.

- Powered by Precision AI®, a groundbreaking AI-driven engine that analyzes and prevents threats in real time.

- Built with a single-pass architecture to deliver predictable performance.

- Delivers Palo Alto Networks 5G-Native Security with 5G identifier-based visibility and enforcement capabilities.

- Offers high availability with NGFW clustering.

- 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.

Post-Quantum Cryptography Optimizations

PA-5500 Series is a post-quantum cryptography-ready NGFW that helps you achieve quantum-safe security in hardware and software with PAN-OS 12.1. PA-5500 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 experimental PQCs, like Classic McEliece, BIKE, HQC, Frodo-KEM, and NTRU-Prime.

- A newly introduced PCIe slot for the future addition of post-quantum capabilities.

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

Prevention of Malicious Activity Concealed in Encrypted Traffic

PA-5500 Series NGFWs provide the ability to:

- Inspect and apply policies 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 classical key exchange algorithms RSA, ECDHE, DHE, and post-quantum key exchange standards ML-KEM, HQC, as well as experimental BIKE and Frodo-KEM.

- Let you enable or disable decryption flexibly—based on URL category, source and destination zone, address, user, user group, device, and port—for privacy and regulatory compliance purposes.

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

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.

- Allows for the effective enforcement of security policies tailored to specific applications, by centralizing the identification and control of applications at the firewall level.

- 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 the App-ID tech brief.

User Security Enforcement

PA-5500 Series NGFWs enforce security for users at any location, on any device, while adapting policies based on their activity. They include the ability to:

- **Unify identity and policy enforcement:** Bridge on-premises and cloud identity stores to enforce consistent user-based policies everywhere via the Cloud Identity Engine, and block malicious traffic sources automatically by using IP geolocation.
- **Automate dynamic risk control:** Apply dynamic security actions based on user behavior and risk scores using Cloud Dynamic User Groups (CDUGs)—without depending on directory updates. Also, leverage automated policy recommendations to save time and reduce human error when restricting suspicious activity.
- **Secure credentials:** Prevent credential theft and abuse by enforcing multifactor authentication (MFA) at the network layer for any application, including legacy and non-web apps, without requiring application changes.

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

Unique Approach to Packet Processing

PA-5500 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).

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

AI-Powered Unified Management and Operations with Strata Cloud Manager

Manage your PA-5500 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.

For more information, see the Strata Cloud Manager solution brief.

Combined NGFW Clustering and High Availability Elements

NGFW clustering optimizes resource usage and increases throughput while maintaining a highly redundant and resilient solution. This solution enables efficient horizontal scaling for highly available networks.

See the Migrating to NGFW Clustering whitepaper for more information.

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

PA-5500 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

Palo Alto Networks Advanced Threat Prevention is the industry's first intrusion prevention system (IPS) that stops zero-day command-and-control (C2) attacks and unknown exploits completely 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

Palo Alto Networks 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 can be built into NGFW policies for control of 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 from outside or inside the network.

For more information, see the Advanced DNS Security datasheet.

Device Security

Palo Alto Networks Device Security delivers a unified, AI-first solution that provides comprehensive protection and monitoring across your entire attack surface. 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

Palo Alto Networks SaaS Security delivers broad visibility and real-time control over all SaaS applications, including GenAI apps. Moreover, it 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 steer applications to the best performing paths.

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

Table 1. Performance and Capacities of PA-5500 Series Quantum Optimized NGFWs					
	PA-5540	PA-5550	PA-5560	PA-5570	PA-5580
Firewall throughput (appmix)*	150 Gbps	175 Gbps	240 Gbps	300 Gbps	375 Gbps
Threat Prevention throughput (appmix)†	90 Gbps	120 Gbps	180 Gbps	240 Gbps	300 Gbps
IPsec VPN throughput‡	80 Gbps	100 Gbps	125 Gbps	150 Gbps	170 Gbps
Max concurrent sessions§	39M	49M	74M	89M	99M
New sessions per second‖	1.33M	1.67M	2.5M	3M	3.3M
Virtual systems (base/max)#	25/225	25/225	25/225	25/225	25/225

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, 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 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. NGFW Cluster A/A supports a maximum of 25 Virtual Systems.

Table 2. PA-5500 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.
Point-to-Point Protocol over Ethernet (PPPoE) and DHCP client are supported for dynamic address assignment for both IPv4 and IPv6.
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.
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 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 access over IPsec and SSL VPN tunnels using GlobalProtect gateway and portals.[†]
VLANs
802.1Q VLAN tags per device or per interface: 4,094/4,094.
Aggregate interfaces (802.3ad) and LACP.
Network Address Translation
NAT modes (IPv4): static IP, dynamic IP, dynamic IP, and port (port address translation).
NAT64 and NPTv6.
Additional NAT features: Dynamic IP reservation, tunable dynamic IP, and port oversubscription.
High Availability and Clustering
NGFW clustering with active/active. HA active/passive.[‡]
NGFW clustering maintains a dual-active data plane with a single control plane, support for MC-LAG (Aggregate Ethernet interfaces with members on both systems).
Mobile Network Infrastructure[§]
5G security.

[*] Not supported with NGFW clustering.

[†] Requires a GlobalProtect license.

[‡] Future release.

[§] For additional information, refer to our ML-Powered NGFWs for 5G datasheet.

Table 3. PA-5500 Series Hardware Specifications
I/O
PA-5540/PA-5550: 10G/25G SFP28 (16), 40G/100G QSFP28 (16), and 100G/400G QSFP-DD (4) PA-5560/PA-5570/PA-5580: 10G/25G SFP28 (8), 40G/100G QSFP28 (12), and 100G/400G QSFP-DD (8)
Management I/O
Out-of-band management: 1G/10G SFP+ (2) Console: RJ-45 console port (1) Console: USB-C Bootstrap: USB 3.2 Gen1 Type A HSCI: 100G/400G QSFP-DD (2) Log: 10G SFP+ (2)
Storage Capacity
Optional 3.84 TB RAID1 SSD pair for system and log storage supported as cold swap.
Power Supply (Avg/Max Power Consumption)
2,100 W/3,100 W
Max BTU/hr
1638
Power Supplies
2+2 redundant for 220 V and DC 3+1 redundant for 110 V
Input Voltage
AC: 100–240 VAC (50–60 Hz) DC: -40 VDC to -60 VDC
Power Supply Output
AC: 2,700 W/power supply with 220 V or 1,200 W/power supply with 110 V DC: 2,200 W/power supply
Max Current Consumption
AC: 20.3 A @ 110 VAC and 9.3 A @ 240 VAC DC: 43.7 A @ 54 VDC
Max Inrush Current
AC: 50 A @ 230 VAC and 50 A @ 120 VAC DC: 25 A @ 54 VDC
Mean Time Between Failure (MTBF)
PA-5540/PA-5550: 8.1 years PA-5560/PA-5570/PA-5580: 6.3 years
Rack Mount Dimensions
3U, 19" standard rack (5.2" H x 29.8" D x 17.3" W) with power supply inserted.
Weight (Standalone Device/As Shipped)
70 lbs/116 lbs (includes accessory kit, rack kit, packaging, and pallet).
Safety
cTUVus, CB
EMI
FCC Class A, CE Class A, VCCI Class A

Table 3. PA-5500 Series Hardware Specifications (continued)
Certifications
See our Compliance page.
Environment
Operating temperature: 32°F to 122°F, 0°C to 50°C **Nonoperating temperature:** -4°F to 158°F, -20°C to 70°C **Humidity tolerance:** 10%–90% **Maximum altitude:** 10,000 ft/3,048 m **Airflow:** Front to back (port side to power supply side)

Table 4 lists key SKUs for the PA-5500 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 Channel partners.

Table 4. PA-5500 Series Ordering Information	
Part Number	**Details**
PAN-PA-5540-AC PAN-PA-5550-AC PAN-PA-5560-AC PAN-PA-5570-AC PAN-PA-5580-AC	Includes: 4x PAN-PA-5500-PWR-2700-AC 5x PAN-PA-FAN-2RU-A 1x PAN-PA-5500-ACC-A accessory kit 1x PAN-PA-3RU-RACK-A 2x PAN-SFP-CG 1x PAN-PA-5500-SSD-3.84TB-PAIR
PAN-PA-5540-DC PAN-PA-5550-DC PAN-PA-5560-DC PAN-PA-5570-DC PAN-PA-5580-DC	Includes: 4x PAN-PA-5500-PWR-2000-DC 5x PAN-PA-FAN-2RU-A 1x PAN-PA-5500-ACC-B accessory kit 1x PAN-PA-3RU-RACK-A 2x PAN-SFP-CG 1x PAN-PA-5500-SSD-3.84TB-PAIR
PAN-PA-5500-SSD-3.84TB-PAIR	Spare replacement drive.
PAN-PA-5500-ACC-A	Spare accessory kit includes a 4x PAN-PWR-C19-US-120V cable, 1x USB cable, and 1x Cat6 cable.
PAN-PA-5500-ACC-B	Spare accessory kit includes a 4x PAN-PWR-DC-CBL-C cable, 1x USB cable, and 1x Cat6 cable.