

PA-1510-POE



PA-1520-POE



PA-1530-POE

PA-1500 Series Quantum-Optimized NGFWs

Palo Alto Networks PA-1500 Series Quantum-Optimized NGFWs comprise the PA-1510-POE, PA-1520-POE, and PA-1530-POE. This series targets smaller campuses and larger distributed enterprise branch offices. It provides complete visibility into and secures all traffic across your network, including post-quantum encrypted traffic.

PAN-OS®, the operating system of the PA-1500 Series, 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. This traffic serves as the basis of your security policies, resulting in an improved security posture and reduced incident response time. Our 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-1500 Series is a post-quantum cryptography (PQC)-ready device that helps you achieve quantum-safe security in hardware and software with PAN-OS 12.2. PA-1500 Series NGFWs support:

- **PQC** for PQC TLS decryption, PQC VPN site-to-site, PQC-Classical TLS Cipher Translation Proxy, and PQC TLS Service Profile for Management Access to the firewall. Also, PQC GlobalProtect® for end-user remote access VPN.
- **PQC algorithms,** including NIST standards, like ML-KEM, ML-DSA, and SLH-DSA, as well as emerging and experimental PQCs like Classic McEliece, BIKE, HQC, Frodo-KEM, and NTRU-Prime. Support also for hybrid post-quantum classical and pure PQC algorithms.

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

Prevention of Malicious Activity Concealed in Encrypted Traffic

PA-1500 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, HTTP/2, and QUIC/HTTP3.
- **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.
- **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 organization.

Key Highlights

- **The world's first quantum-optimized NGFW:** Engineered to secure post-quantum encrypted traffic and protect long-life data against future decryption threats.
- **Powered by Precision AI®,** a groundbreaking AI-driven engine that analyzes and prevents threats in real time.
- **Built with a single-pass architecture:** Conducts networking, policy enforcement, decryption, and threat inspection in a single pass to deliver predictable performance under heavy loads.
- **Delivers Palo Alto Networks 5G-Native Security:** Features 5G identifier-based visibility, traffic correlation, and security enforcement capabilities.
- **Offers high availability:** Provides active/active and active/passive HA to ensure resilient, uninterrupted uptime.
- **Zero touch provisioning (ZTP)** to simplify deployment of large numbers of firewalls.
- **Managed with Strata™ Cloud Manager:** The industry's first AI-powered unified management and operations solution for network security.
- **16 integrated enhanced Power over Ethernet (PoE++; 90W) ports** with up to a 724W maximum power budget.
- **Built-in Layer 2 switching** with enterprise authentication capabilities.

Application Identification and Categorization with Full Layer 7 Inspection

App-ID™ identifies and categorizes 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 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-1500 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.

Single-Pass Architecture

PA-1500 Series NGFWs process packets by using a single-pass architecture, enabling the NGFWs to:

- Perform networking, policy lookup, application decoding, and signature matching—for all threats and content—in a single pass. This approach 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.

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

AI-Powered Unified Management and Operations with Strata Cloud Manager

Manage your PA-1500 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:** Use 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* datasheet.

Layer 2 Switching

The PA-1500 Series NGFW models add a Layer 2 switching function on top of the existing security and SD-WAN capabilities. 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-1500 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 applications, DNS, email, IP infrastructure, web, 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 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. It 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 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 steer applications to the best performing paths.

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

PA-1500 Series Specifications

Table 1. Performance and Capacities of PA-1500 Series Quantum-Optimized NGFWs			
	PA-1510-POE	PA-1520-POE	PA-1530-POE
Firewall throughput (appmix)*	15 Gbps	25 Gbps	35 Gbps
Threat Prevention throughput (appmix)†	9 Gbps	18 Gbps	27 Gbps
IPsec VPN throughput‡	7 Gbps	14 Gbps	18 Gbps
Max. concurrent sessions§	1,095,000	1,495,000	1,750,000
New sessions per second‖	140,000	180,000	220,000
Virtual systems (base/max)#	1/6	1/11	1/11

Note: Results were measured on PAN-OS 12.2.

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

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

Table 2. PA-1500 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 (ARE) is the only supported routing engine. 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 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.

Table 2. PA-1500 Series Networking Features (continued)
Layer 2 Switching
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.
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, NPTv6, DNSv6, IPv6 Multicast Routing, BGP IPv4 NLRI over IPv6 Next-hop.
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 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, and port (port address translation).
NAT64 and NPTv6.
Additional NAT features: Dynamic IP reservation, tunable dynamic IP, and port oversubscription.
High Availability
Modes: Active/active and active/passive Failure detection: Path monitoring, interface monitoring.†
Mobile Network Infrastructure‡
5G Security.

* Requires a GlobalProtect license.

† Future release.

‡ For more information, see the *ML-Powered NGFWs for 5G* datasheet.

Table 3. PA-1500 Series Hardware Specifications
I/O
PA-1510-POE: 10/100/1000 Cu (12), 1G/2.5G/5G Cu (8), 1G SFP (4), 1G/10G SFP+ (8)
PA-1520-POE: 10/100/1000 Cu (8), 1G/2.5G/5G Cu (8), 1G/2.5G/5/10G Cu (4), 1/10G SFP+ (8), 10G/25G SFP28 (4)
PA-1530-POE: 10/100/1000 Cu (8), 1G/2.5G/5G Cu (4), 1G/2.5G/5/10G Cu (8), 1/10G SFP+ (8), 10G/25G SFP28 (4)
Power over Ethernet (PoE)
Available on ports 5–20:
PA-1510-POE: 485W total, 90W max per port
PA-1520-POE: 545W total, 90W max per port
PA-1530-POE: 724W total, 90W max per port
Management I/O
Out-of-band management: 10/100/1000 Cu (1)
Console: RJ-45 console port (1)
Console: USB-C (1)
Bootstrap: USB 3.2 Gen1 Type A (1)
HA: 10/100/1000 Cu (2)
HSCI: PA-1510-POE: 10G SFP+ (1), PA-1520-POE, PA-1530-POE: 25G SFP28 (1)
Storage Capacity
PA-1510-POE, PA-1520-POE: 480 GB
PA-1530-POE: 960 GB
Power Supply (Avg/Max Power Consumption)
PA-1510-POE: 845W (max power with 485W PoE)
PA-1520-POE: 910W (max power with 545W PoE)
PA-1530-POE: 1107W (max power with 724W PoE)
Max BTU/hr
1057.8 BTU/hr (max system power dissipation of 310W)
Power Supplies
PA-1510-POE, PA-1520-POE: AC 1200W power supply (1); optional for purchase 2nd AC 1200W power supply
PA-1530-POE: AC 1200W power supply (2)
Optional FRUs: AC 1200W power supply; DC 1200W power supply **Note:** In a two-power-supply setup, power supplies must be the same type: AC/AC or DC/DC.
Input Voltage
AC: 100–240 VAC (50–60 Hz)
DC: -48 VDC to -60 VDC

Table 3. PA-1500 Series Hardware Specifications (continued)
Power Supply Output
AC: 1,200W/power supply with 220V or 1,200W/power supply with 110V
DC: 1,200W/power supply with 48V
Max Current Consumption
PA-1510-POE: 7.7 A @ 110 VAC and 3.5 A @ 240 VAC; 17.6 A @ 48 VDC (with 485W PoE)
PA-1520-POE: 8.3 A @ 110 VAC and 3.8 A @ 240 VAC; 19 A @ 48 VDC (with 545W PoE
PA-1530-POE: 10.1 A @ 110 VAC and 4.6 A @ 240 VAC; 23.1 A @ 48 VDC (with 724W PoE)
Max Inrush Current
AC: 30 A @ 230 VAC and 50 A @ 120 VAC
DC: 30 A @ 48 VDC
Mean Time Between Failure (MTBF) 25C
PA-1510-POE: 34 years
PA-1520-POE: 27 years
PA-1530-POE: 31 years
Rack Mount Dimensions
1U, 19" standard rack (1.70" H x 19.68" D x 17.34" W) with power supply inserted
Weight (Standalone Device and As Shipped)
PA-1510-POE, PA-1520-POE: 19.8 lbs (with one power supply inserted)
PA-1530-POE: 21.5 lbs (with two power supplies inserted)
22 lbs/23 lbs (includes accessory kit, rack kit, and packaging)
Safety
cMETus and CB
EMI
FCC Class A, CE Class A, and VCCI Class A
Certifications
See the 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
Humidity tolerance: 10%–90%
Maximum altitude: 10,000 ft/3,048 m
Airflow: Front to back (port side to power supply side)

PA-1500 Series Ordering Information

The following table lists key SKUs for the PA-1500 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-1500 Series

Part Number	Details
PAN-PA-1510-POE, PAN-PA-1520-POE	The package includes: 1x PA-1510-POE or PA-1520-POE firewall 1x PAN-PWR-1200W-54V-AC-A 1x C13 US power cord 1x PAN-PA-1RU-RACK-KIT 1x Ethernet cable 1x USB-C console cable
PAN-PA-1530-POE	The package includes: 1x PA-1530-POE firewall 2x PAN-PWR-1200W-54V-AC-A 2x C13 US power cords 1x PAN-PA-1RU-RACK-KIT 1x Ethernet cable 1x USB-C console cable
PAN-PA-1RU-RACK-KIT	1x RU four-post rack kit. Included with the system. Compatible with all PA-1500 Series platforms.
PAN-PWR-1200W-54V-AC-A*	1200W spare AC power supply. 1x included with PA-1510-POE, PA-1520-POE 2x included with PA-1530-POE
PAN-PWR-1200W-54V-DC-A*	1200W spare DC power supply. Compatible with all PA-1500 Series platforms.
PAN-PWR-DC-DSUB-3W3-CBL-2M	DC power cable. Compatible with PAN-PWR-1200W-54V-DC-A.
PAN-PA-1500-ACC	Replacement accessory kit for PA-1500 Series firewalls. Includes an Ethernet cable, US power cord, and replacement shipping materials.

* In a two-power-supply setup, power supplies must be the same type: AC/AC or DC/DC

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

© 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-1500-series-quantum-optimized-ngfws_091126