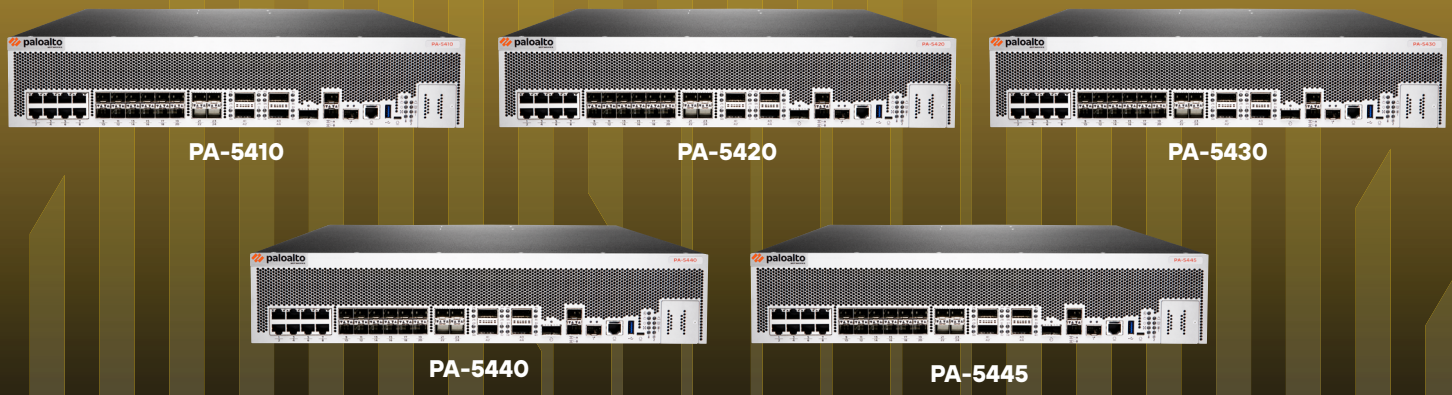


PA-5400 Series

Palo Alto Networks PA-5400 Series ML-Powered Next-Generation Firewalls—comprising the PA-5445, PA-5440, PA-5430, PA-5420, and PA-5410—are ideal for high-speed data center, internet gateway, and service provider deployments. The PA-5400 Series appliances secure all traffic, including encrypted traffic.

The world's first ML-Powered Next-Generation Firewall enables you to prevent unknown threats, see, and secure everything—including the internet of things (IoT)—and reduce errors with automatic policy recommendations.

Highlights

- World's first ML-Powered NGFW.
- Powered by Precision AI®, a groundbreaking AI-driven engine that analyzes and prevents threats in real time.
- Leader in the 2025 Gartner® Magic Quadrant™ for Hybrid Mesh Firewall.
- Leader in The Forrester® Wave™: Enterprise Firewall Solutions, Q4 2024.
- Delivers 5G-Native Security built to safeguard service provider and enterprise 5G transformation and multi-access edge computing (MEC).
- Extends visibility and security to all devices, including unmanaged IoT devices, without the need to deploy additional sensors.
- Supports high availability with active/active and active/passive modes.
- Built with a single-pass architecture to deliver predictable performance with security services.
- Supports centralized administration with Panorama® network security management.
- Native web proxy support in NGFW to simplify and consolidate management of firewall and proxy functionalities.
- Managed with Strata™ Cloud Manager, the industry's first AI-powered unified management and operations solution for network security.

The controlling element of the PA-5400 Series 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 applications, content, and users—the elements that run your business—serve as the basis of your security policies, resulting in an improved security posture and reduced incident response times. PAN-OS embeds machine learning (ML) 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

The PA-5400 Series is a post-quantum cryptography (PQC)-ready NGFW that helps you achieve quantum-safe security in hardware and software with PAN-OS 12.1. PA-5400 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 experimental 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-5400 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 solution brief.

User Security Enforcement

PA-5400 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 nonweb apps, without requiring application changes.

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

Unique Approach to Packet Processing

PA-5400 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 solution brief.

AI-Powered Unified Management and Operations with Strata Cloud Manager

Manage your PA-5400 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 datasheet.

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.

Native Web Proxy Support for the Next-Generation Firewall

- Consolidates the firewall and proxy into a single platform while managing capabilities through a centralized management platform to build policies.
- Through PAC files, supports the explicit proxy, which:
  - Can help with no-default route architectures in on-premises proxy deployments.
  - Supports authentication with Kerberos and SAML.
- Supports and simplifies the transparent proxy setup without needing WCCP or authentication.
- Web proxy on the PA-5400 series supports up to 250K sessions and 100K unique IP addresses.

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

PA-5400 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.

PA-5400 Series Specifications

Table 1. PA-5400 Series Performance and Capacities					
	PA-5410	PA-5420	PA-5430	PA-5440	PA-5445
Firewall throughput (appmix)*	52 Gbps	70 Gbps	80 Gbps	85 Gbps	90 Gbps
Threat Prevention throughput (appmix)†	35 Gbps	50 Gbps	60 Gbps	70 Gbps	76 Gbps
IPsec VPN throughput‡	20 Gbps	28 Gbps	42 Gbps	58 Gbps	64 Gbps
Max concurrent sessions§	5M	7M	9M	20M	48M
New sessions per second‖	270,000	370,000	380,000	390,000	449,000
Virtual systems (base/max)#	10/20	15/65	25/125	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, by using appmix transactions.

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

§ Max 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 base quantity requires a separately purchased license.

Table 2. PA-5400 Series Networking Features
Interface Modes
L2, L3, tap, virtual wire (transparent mode)
Routing
OSPFv2/v3 with graceful restart, BGP with graceful restart, RIP, static routing
Policy-based forwarding
Point-to-Point Protocol over Ethernet (PPPoE) and DHCP supported for dynamic address assignment
Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, and v3
Bidirectional Forwarding Detection (BFD)
SD-WAN
Path quality measurement (jitter, packet loss, latency)
Initial path selection (PBF)
Key exchange: manual key, IKEv1, and IKEv2 (pre-shared key, certificate-based authentication)
IPv6
L2, L3, tap, virtual wire (transparent mode)
Features: App-ID, User-ID™, Content-ID™, WildFire, and SSL Decryption
SLAAC

Table 2. PA-5400 Series Networking Features (continued)
IPsec and SSL VPN
Key exchange: manual key, IKEv1, and IKEv2 (pre-shared key, certificate-based authentication)
Encryption: 3des, AES (128-bit, 192-bit, 256-bit)
Authentication: MD5, SHA-1, SHA-256, SHA-384, 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/per interface: 4,094/4,094
Aggregate interfaces (802.3ad), LACP
Network Address Translation
NAT modes (IPv4): static IP, Dynamic IP, Dynamic IP and Port (port address translation)
NAT64, NPTv6
Additional NAT features: Dynamic IP reservation, tunable Dynamic IP and Port oversubscription
High Availability
Modes: active/active, active/passive, HA clustering
Failure detection: path monitoring, interface monitoring
Mobile Network Infrastructure†
5G Security
GTP Security
SCTP Security

* Requires a GlobalProtect license.

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

Table 3. PA-5400 Series Hardware Specifications
1/O
1G/2.5G/5G/10G (8), 1G/10G SFP/SFP+ (12), 1G/10G/25G SFP/SFP+/SFP28 (4), 40G/100G QSFP+/QSFP28 (4)
Management I/O
1G/10G SFP/SFP+ out-of-band management port (1)
1G/10G SFP/SFP+ high availability (2), 40G QSFP+ high availability (1)
RJ-45 console port (1), Micro USB
Storage Capacity
480 GB SSD pair, system storage
Trusted Platform Module (TPM)
Integrated with TPM for secure boot, hardware root of trust, and securing system secrets.
Power Supply (Avg/Max Power Consumption)
630/760 W
Max BTU/hr
1638

Table 3. PA-5400 Series Hardware Specifications (continued)
Power Supplies (Base/Max)
1:1 fully redundant (2/2)
AC Input Voltage (Input Hz)
100–240 VAC (50–60 Hz)
AC Power Supply Output
1,200 watts/power supply
Max Current Consumption
AC: 7 A @ 100 VAC, 3 A @ 240 VAC
DC: 15 A @ -48 VDC, 12 A @ -60 VDC
Max Inrush Current
AC: 50 A @ 230 VAC, 50 A @ 120 VAC
DC: 200 A @ 72 VDC
Mean Time Between Failure (MTBF)
22 years
Rack Mount Dimensions
2U, 19" standard rack (3.45" H x 22.5" D x 17.34" W)
Weight (Standalone Device/As Shipped)
35.2 lbs/48.8 lbs
Safety
cTUVus, CB
EMI
FCC Class A, CE Class A, VCCI Class A
Certifications
See paloaltonetworks.com/company/certifications.html
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% to 90%
Maximum altitude: 10,000 ft/3,048 m
Airflow: front to back

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-5400-series_041426