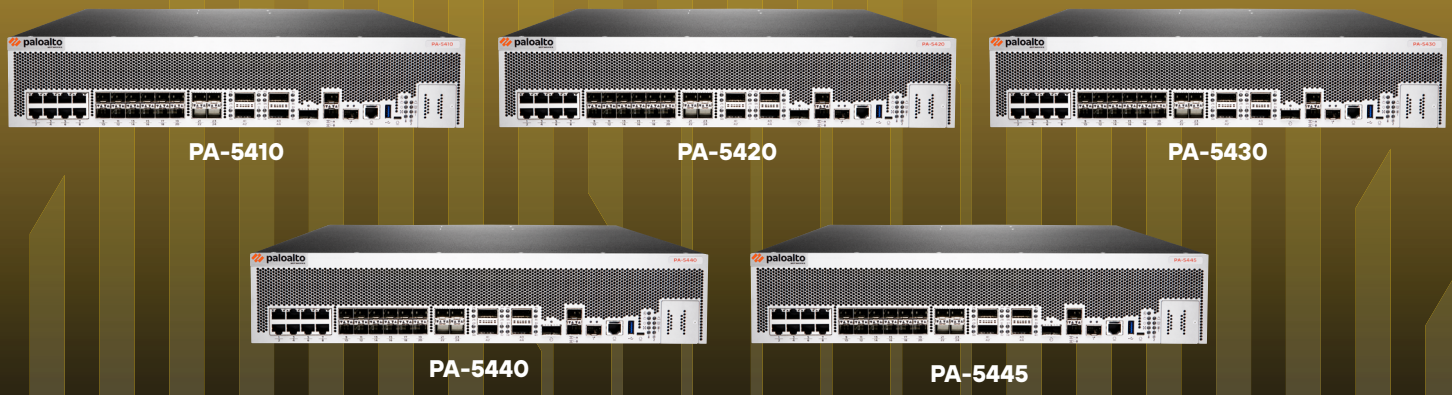

PA-5400 Series

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.

Highlights

- World's first ML-Powered NGFW
- Eleven-time Leader in the Gartner Magic Quadrant for Network Firewalls
- Leader in The Forrester Wave: Enterprise Firewalls, Q4 2022
- 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
- Delivers 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
- Maximizes security investments and prevents business disruptions with Strata™ Cloud Manager

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.

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 application, content, and user—in other words, the elements that run your business—then serve as the basis of your security policies, resulting in improved security posture and reduced incident response time.

Key Security and Connectivity Features

ML-Powered Next-Generation Firewall

- 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.
- Leverages cloud-based ML processes to push zero-delay signatures and instructions back to the NGFW.
- Uses behavioral analysis to detect IoT devices and make policy recommendations; cloud-delivered and natively integrated service on the NGFW.
- Automates policy recommendations that save time and reduce the chance of human error.

Identifies and Categorizes All Applications, on All Ports, All the Time, with Full Layer 7 Inspection

- Identifies the applications traversing your network irrespective of port, protocol, evasive techniques, or encryption (SSL/TLS). In addition, it automatically discovers and controls new applications to keep pace with the SaaS explosion with SaaS Security subscription.
- Uses the application, not the port, as the basis for all your safe enablement policy decisions: allow, deny, schedule, inspect, and apply traffic-shaping.
- Offers the ability to create custom App-ID™ tags for proprietary applications or request App-ID development for new applications from Palo Alto Networks.
- Identifies all payload data within the application (e.g., files and data patterns) to block malicious files and thwart data exfiltration attempts.
- Creates standard and customized application usage reports, including software-as-a-service (SaaS) reports that provide insight into all sanctioned and unsanctioned SaaS traffic on your network.
- Enables safe migration of legacy Layer 4 rule sets to App-ID-based rules with built-in Policy Optimizer, giving you a rule set that is more secure and easier to manage.

Check out the App-ID tech brief for more information.

Enforces Security for Users at Any Location, on Any Device, While Adapting Policy Based on User Activity

- Enables visibility, security policies, reporting, and forensics based on users and groups—not just IP addresses.
- Easily integrates with a wide range of repositories to leverage user information: wireless LAN controllers, VPNs, directory servers, SIEMs, proxies, and more.
- Allows you to define Dynamic User Groups (DUGs) on the firewall to take time-bound security actions without waiting for changes to be applied to user directories.
- Applies consistent policies irrespective of users' locations (office, home, travel, etc.) and devices (iOS and Android mobile devices; macOS, Windows, and Linux desktops and laptops; Citrix and Microsoft VDI; and terminal servers).

- Prevents corporate credentials from leaking to third-party websites and prevents reuse of stolen credentials by enabling multifactor authentication (MFA) at the network layer for any application without any application changes.
- Provides dynamic security actions based on user behavior to restrict suspicious or malicious users.
- Consistently authenticates and authorizes your users, regardless of location and where user identity stores live, to move quickly toward a Zero Trust security posture with Cloud Identity Engine—an entirely new cloud-based architecture for identity-based security.

Check out the Cloud Identity Engine solution brief for more information.

Prevents Malicious Activity Concealed in Encrypted Traffic

- Inspects and applies policy to SSL/TLS-encrypted traffic, both inbound and outbound, including for traffic that uses TLSv1.3 and HTTP/2.
- Offers rich visibility into TLS traffic, such as amount of encrypted traffic, SSL/TLS versions, cipher suites, and more, without decrypting.
- Enables control over use of legacy TLS protocols, insecure ciphers, and misconfigured certificates to mitigate risks.
- Facilitates easy deployment of decryption and lets you use built-in logs to troubleshoot issues, such as applications with pinned certificates.
- Lets 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.
- Allows you to create a copy of decrypted traffic from the firewall (i.e., decryption mirroring) and send it to traffic collection tools for forensics, historical purposes, or data loss prevention (DLP).
- Allows you to intelligently forward all traffic (decrypted TLS, undecrypted TLS, and non-TLS) to third-party security tools with network packet broker and optimize your network performance and reduce operating expenses.

Refer to this decryption whitepaper to learn where, when, and how to decrypt to prevent threats and secure your business.

Offers AI-Powered Unified Management and Operations with Strata Cloud Manager

Prevent network disruptions: Forecast deployment health and proactively identify capacity bottlenecks up to seven days in advance with predictive analytics to proactively prevent operational disruptions.

Strengthen security in real time: AI-powered analysis of policies and real-time compliance checks against industry and Palo Alto Networks best practices.

Enable simple and consistent network security management and ops: Manage configuration and security policies across all form factors, including SASE, hardware and software firewalls, and all security services to ensure consistency and reduce operational overhead.

Native Web Proxy Support for the Next-Generation Firewall

- Ability to consolidate firewall and proxy into a single platform while managing capabilities through a centralized management platform to build policies.
- Ability to support explicit proxy through PAC files and also transparent proxy.
- Explicit proxy can help with no-default route architectures with on-premises proxy deployments.
- Explicit proxy supports authentication with Kerberos and SAML.
- Transparent proxy setup is simplified without the need for WCCP or authentication.

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

The typical enterprise's attack surface has grown significantly with the mass adoption of hybrid work, cloud, internet of things (IoT), and software as a service (SaaS). Furthermore, the threat landscape is rapidly intensifying due to easily being able to access and use hacker-friendly tools and resources in their campaigns. Traditional network security solutions and approaches are no longer effective. With Palo Alto Networks Cloud-Delivered Security Services, customers can benefit from best-in-class, real-time security to help them protect all users, devices, and data in their network, regardless of location.

Palo Alto Networks security services use the power of Precision AI™ inline to stay ahead of threat actors and stop new and never-before-seen threats in real time. Through shared threat intelligence across over 70,000 customers worldwide, they have insights into emerging threats and can act proactively. Finally, seamless integration with NGFW and SASE eliminates security gaps and offers customers a single pane of glass to view and manage their security.

Services include:

- **Advanced Threat Prevention**: Stop known and unknown exploits, malware, spyware, and command-and-control (C2) threats, including 60% more injection attacks and 48% more highly evasive C2 traffic than traditional IPS solutions with industry-first zero-day attack prevention.
- **Advanced WildFire®**: Ensure safe access to files with the industry's largest malware prevention engine, stopping up to 22% more unknown malware and turning detection into prevention 180X faster than competitors.
- **Advanced URL Filtering**: Ensure safe access to the web and prevent 40% more threats in real time than traditional filtering databases with industry-first prevention of known and unknown phishing attacks, stopping up to 88% of malicious URLs at least 48 hours before competitors.
- **Advanced DNS Security**: Protect your DNS traffic and stop advanced DNS-layer threats, including DNS hijacking, all in real time with 2X more DNS-layer threat coverage than competitors.
- **Next-Generation CASB**: Discover and control all SaaS consumption in your network with visibility into 60K+ SaaS apps and protect your data with 28+ API integrations.
- **IoT Security**: Secure your blind spots and protect every connected device unique to your vertical with the industry's most comprehensive Zero Trust solution for IoT devices, discovering 90% of devices within 48 hours.

Delivers a Unique Approach to Packet Processing with Single-Pass Architecture

- Performs 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.
- Avoids introducing latency by scanning traffic for all signatures in a single pass, using stream-based, uniform signature matching.
- Enables consistent and predictable performance when security subscriptions are enabled. (In table 1, "Threat Prevention throughput" is measured with multiple subscriptions enabled.)

Enables SD-WAN Functionality

- Allows you to easily adopt SD-WAN by simply enabling it on your existing firewalls.
- Enables you to safely implement SD-WAN, which is natively integrated with our industry-leading security.
- Delivers an exceptional end-user experience by minimizing latency, jitter, and packet loss.

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 11.2.

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

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

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

§ Max concurrent sessions are measured utilizing HTTP transactions.

‖ New sessions per second is measured with application override, utilizing 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
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*

* Requires GlobalProtect license.

Table 2: PA-5400 Series Networking Features (continued)
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

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

Table 3: PA-5400 Series Hardware Specifications
I/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
Power Supply (Avg/Max Power Consumption)
630/760 W
Max BTU/hr
1638
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

Table 3: PA-5400 Series Hardware Specifications (continued)
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

strata_ds_pa-5400-series_071624