PA-3410

PA-3420

PA-3430

PA-3440

PA-3400 Series

Palo Alto Networks PA-3400 Series ML-Powered NGFWs—comprising the PA-3440, PA-3430, PA-3420, and PA-3410—target high-speed internet gateway deployments. The PA-3400 Series appliances secure all 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
- Extends visibility and security to all devices, including unmanaged IoT devices, without the need to deploy additional sensors
- Native web proxy support in NGFW to simplify and consolidate management of firewall and proxy functionalities
- Supports high availability with active/active and active/passive modes
- Delivers predictable performance with security services
- Simplifies deployment of large numbers of firewalls with Zero Touch Provisioning (ZTP)
- Supports centralized administration with Panorama network security management
- Maximizes security investments and prevents business disruptions with AIOps

The world's first ML-Powered Next-Generation Firewall (NGFW) 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-3400 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 (TLS/SSL). 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, Linux desktops, 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 TLS/SSL-encrypted traffic, both inbound and outbound, including for traffic that uses TLS 1.3 and HTTP/2.
- Offers rich visibility into TLS traffic, such as amount of encrypted traffic, TLS/SSL 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 Centralized Management and Visibility

- Benefits from centralized management, configuration, and visibility for multiple distributed Palo Alto Networks NGFWs (irrespective of location or scale) through Panorama network security management in one unified user interface.
- Streamlines configuration sharing through Panorama with templates and device groups and scales log collection as logging needs increase.
- Enables users, through the Application Command Center (ACC), to obtain deep visibility and comprehensive insights into network traffic and threats.

Maximize Your Security Investment and Prevent Business Disruption with AIOps

- AIOps for NGFW delivers continuous best practice recommendations customized to your unique deployment to strengthen your security posture and get the most out of your security investment.
- Intelligently predicts firewall health, performance, and capacity problems based on ML powered by advanced telemetry data. It also provides actionable insights to resolve the predicted disruptions.

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.

Detects and Prevents Advanced Threats with Cloud-Delivered Security Services

Today's sophisticated cyberattacks can spawn 45,000 variants in 30 minutes using multiple threat vectors and advanced techniques to deliver malicious payloads. Traditional siloed security causes challenges for organizations by introducing security gaps, increasing overhead for security teams, and hindering business productivity with inconsistent access and visibility.

Seamlessly integrated with our industry-leading NGFWs, our Cloud-Delivered Security Services use the network effect of 80,000 customers to instantly coordinate intelligence and protect against all threats across all vectors. Eliminate coverage gaps across your locations and take advantage of best-in-class security delivered consistently in a platform to stay safe from even the most advanced and evasive threats.

Services include:

- **Advanced Threat Prevention**: Stop known exploits, malware, spyware, and command-and-control (C2) threats, while utilizing industry-first prevention of zero-day attacks—prevent 60% more unknown injection attacks and 48% more highly evasive command-and-control traffic than traditional IPS solutions.

- **Advanced WildFire**: Ensure files are safe by automatically preventing known, unknown, and highly evasive malware 60X faster with the industry's largest threat intelligence and malware prevention engine.
- **Advanced URL Filtering**: Ensure safe access to the internet and prevent 40% more web-based attacks with the industry's first real-time prevention of known and unknown threats, stopping 88% of malicious URLs at least 48 hours before other vendors.
- **DNS Security**: Gain 40% more threat coverage and stop 85% of malware that abuses DNS for command and control and data theft without requiring changes to your infrastructure.
- **Enterprise DLP**: Minimize risk of a data breach, stop out-of-policy data transfers, and enable compliance consistently across your enterprise, with 2X greater coverage of any cloud-delivered enterprise DLP.
- **SaaS Security**: Stay ahead of the SaaS explosion with the industry's only Next-Generation CASB to automatically see and secure all apps across all protocols.
- **IoT Security**: Safeguard every "thing" and implement Zero Trust device security 20X faster, with the industry's smartest security for smart devices.

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-3400 Series Performance and Capacities

	PA-3410	PA-3420	PA-3430	PA-3440
Firewall throughput (HTTP/appmix)*	14.1/11.0 Gbps	20.8/16.9 Gbps	25.5/20.5 Gbps	30.2/24 Gbps
Threat Prevention throughput (HTTP/appmix)†	5.1/5.6 Gbps	7.6/8.7 Gbps	9.2/10.5 Gbps	11.0/12.8 Gbps
IPsec VPN throughput‡	6.8 Gbps	9.9 Gbps	12.2 Gbps	14.5 Gbps
Max concurrent sessions§	1.4M	2M	2.5M	3M
New sessions per second||	145,000	205,000	240,000	268,000
Virtual systems (base/max)¶	1/11	1/11	1/11	1/11

Note: Results were measured on PAN-OS 11.0.

* Firewall throughput is measured with App-ID and logging enabled, utilizing 64 KB HTTP/appmix transactions.

† Threat Prevention throughput is measured with App-ID, IPS, antivirus, antispyware, WildFire, DNS Security, file blocking, and logging enabled, utilizing 64 KB HTTP/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-3400 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)
Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, and v3
Bidirectional Forwarding Detection (BFD)
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† (PA-3440 and PA-3430)
5G Security
GTP Security
SCTP Security

* Requires GlobalProtect License.

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

Table 3: PA-3400 Series Hardware Specifications
I/O
PA-3410: 1G/2.5G/5G/10G (12), 1G/10G SFP/SFP+ (10), 25G SFP28 (4)
PA-3420: 1G/2.5G/5G/10G (12), 1G/10G SFP/SFP+ (10), 25G SFP28 (4)
PA-3430: 1G/2.5G/5G/10G (12), 1G/10G SFP/SFP+ (10), 25G SFP28 (4), 40G/100G QSFP/QSFP28 (2)
PA-3440: 1G/2.5G/5G/10G (12), 1G/10G SFP/SFP+ (10), 25G SFP28 (4), 40G/100G QSFP/QSFP28 (2)
Management I/O
100/1000 out-of-band management port (1) 100/1000 high availability (2), 10G SFP+ high availability (1) RJ-45 console port (1), Micro USB (1)
Storage Capacity
480 GB SSD

Table 3: PA-3400 Series Hardware Specifications (continued)
Power Supply (Avg/Max Power Consumption)
Redundant 450-watt AC (133W/190W)
Max BTU/hr
650
Input Voltage Frequency
AC: 100–240 VAC (50–60Hz)
Max Current Consumption
AC: 1.9 A @ 100 VAC, 0.8 A @ 240 VAC
Mean Time Between Failure (MTBF)
22 years
Rack Mount Dimensions
1U, 19" standard rack 14.15" x 17.15" x 1.70"
Weight (Standalone Device/As Shipped)
15.5 lbs / 25 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 104°F, 0°C to 40°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