paloalto NETWORKS | STRATA™

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
- Supports centralized administration with Panorama network security management
- Maximizes security investments and prevents business disruptions with Strata™ Cloud Manager

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, 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 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 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.

Detects and Prevents Advanced Threats with Cloud-Delivered Security Services

The traditional approach of using siloed security tools causes challenges for organizations, including security gaps, increased overhead for security teams, and disruptions in business productivity. Seamlessly integrated with our industry-leading NGFWs, our Cloud-Delivered Security Services share threat intelligence across 65,000 customers to prevent known and unknown threats across all threat vectors in real time. Eliminate security gaps in your entire network and take advantage of inline AI-powered security services that provide real-time protection everywhere.

Services include:

- **Advanced Threat Prevention**: Stop known and unknown exploits and command-and-control (C2) attacks with inline AI-powered detections, stopping 60% more zero-day 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 180X faster than competitors 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 sites at least 48 hours before other vendors.
- **DNS Security**: Gain 68% 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 (appmix)*	14 Gbps	19 Gbps	29 Gbps	35 Gbps
Threat Prevention throughput (appmix)†	7.5 Gbps	10 Gbps	15 Gbps	20 Gbps
IPsec VPN throughput‡	6.6 Gbps	9.9 Gbps	12 Gbps	14.5 Gbps
Max concurrent sessions§	1.4M	2.2M	2.5M	3M
New sessions per second‖	145,000	220,000	240,000	268,000
Virtual systems (base/max)¶	1/11	1/11	1/11	1/11

Note: Results were measured on PAN-OS 11.1.

* 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, DNS Security, 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-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

* Requires GlobalProtect license.

Table 2: PA-3400 Series Networking Features (continued)
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

† 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
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

Table 3: PA-3400 Series Hardware Specifications (continued)
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

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

strata_ds_pa-3400-series_022124

Premium Support

Maintaining your security infrastructure is a mission-critical task. Our Customer Support and Maintenance programs are designed to ensure that traffic flows smoothly and securely across your network. When problems arise, our dedicated Support Services team will quickly and proficiently resolve any questions or challenges.

As an industry leader, our comprehensive set of Support Services underscores our commitment to the ongoing success of your Palo Alto Networks infrastructure. With business-critical Customer Support options, 24/7 availability, and a global network of support centers and parts-replacement depots, organizations of all sizes and complexities around the world can rely on Palo Alto Networks Customer Support Services for fast and dependable service.

Benefits

- Improved system availability with continual software enhancements and outstanding responsiveness.
- Increased uptime and expedited issue resolution with Palo Alto Networks specialists augmenting your internal technical resources.
- Optimized security architecture to reduce and prevent security events.
- Improved operational efficiency.
- Enhance your investment in your internal IT resources with access to technical support by phone and online.

Premium Support: Service Overview

The Palo Alto Networks Premium Support offering enhances your in-house resources with technical experts available to support your Palo Alto Networks security infrastructure. This support level also gives you access to Security Assurance to assist when security incidents occur and you need to augment your staff with security experts.

Premium Support is ideal for organizations that want to work directly with Palo Alto Networks to address their support needs with 24/7, year-round assistance as well as keep up to date with the latest upgrades and updates.

Features

Premium Support provides access to:

- **Feature releases and software updates:** Stay current with the latest features and software updates.
- **Subscription services updates:** To ensure your Palo Alto Networks deployment stays up to date, you can configure devices to automatically download App-ID technology, URL Filtering, DNS Security, Threat Prevention, and WildFire service updates. Alternatively, these updates can be downloaded and manually applied.
- **Security Assurance:** In the event you detect suspicious activity in your network, Security Assurance gives you access to our security experts with unique threat intelligence tools and practices for your Palo Alto Networks footprint. Our team will help orient initial investigations, facilitate the collection of logs and indicators of compromise (IoCs), while expediting hand-off to your preferred incident response (IR) vendor. See our End User Support Agreement for the latest details.
- **Direct access to product experts:** Interact with a support engineer trained to quickly understand and resolve your unique challenges.
- **Premium Support availability:** Enjoy 24/7 support for issues of all severities with Platinum senior engineers available around the clock to assist.
- **Online Customer Support Portal:** A feature-rich platform provides access to product documentation, problem resolution databases, peer-to-peer interaction, and support case management.

Table 1: Palo Alto Networks Support Offering Summary

Support Comparison	Premium	Platinum*
1. Technical Support		
Telephone Support	24/7	24/7
Call Response Time		
Severity 1: Critical Product is down, and customer production environment is critically affected. No workaround available yet.	< 1 hour	< 15 minutes
Severity 2: High Product is impaired, and customer production is up but impacted. No workaround available yet.	2 hours	< 30 minutes
Severity 3: Medium A product function has failed; customer production is not affected. Support is aware of the issue, and a workaround is available.	4 hours	< 2 hours
Severity 4: Low Noncritical issue. Does not impact customer business. Feature, information, documentation, how-to, and enhancement requests from customer.	8 hours	< 4 hours
Support Specialist Type	Support Engineer	Senior Engineer
RMA (NBD included, 4-hour service optional)	**NBD | 4 Hr.**	**NBD | 4 Hr.**

Table 1: Palo Alto Networks Support Offering Summary (continued)		
Support Comparison	**Premium**	**Platinum***
2. Security Assurance Incident Support		
Assisted security investigations	•†	•
Advanced log and IoC analysis	•†	•
Next steps recommendations	•†	•
3. Expert Assistance		
Prescheduled event support	–	•
On-site assistance for critical issues (after remote troubleshooting)	–	•
Failure analysis (HW)	–	•

* Investment minimum required.

† Other restrictions may apply. Please see our EUSA for details.

- **Case management:** Submit, update, check status, and manage support cases for all your supported Palo Alto Networks products via the online Customer Support Portal.
- **Documentation and FAQ:** Access product manuals, technical guides, software release notes, and frequently asked questions (FAQ) to streamline operations and incident resolution.
- **Next-business-day delivery for parts and hardware replacement:** Get fast turnaround for hardware replacement. Note: The Next-Business-Day Delivery Service is subject to certain limitations. Please see the Return Materials Authorization (RMA) Process Policy for details.
- **(Optional) 4-hour RMA service for parts and hardware replacement:** For an additional fee, hardware replacement services can be upgraded to a 4-hour shipment for a rapid RMA turnaround. 4-Hour Premium Support RMA is an optional upgrade to Premium Support for customers and data centers requiring mission-critical response times that are located within a specified range of a Palo Alto Networks service location. With the optional upgrade to 4-Hour Premium or 4-Hour Partner Premium Support, Palo Alto Networks will make commercially reasonable best efforts to deliver replacement component hardware to you within four hours from issuance of an RMA, 24/7, year-round.

Customer Support Services Program

Palo Alto Networks provides you with a range of several customer support and maintenance options designed to meet the unique needs of your business:

- Standard Support (US only)
- Premium Support
- Platinum Support
- Focused Services
- On-Site Spares Hardware Program

Whichever support and maintenance plan you choose, you will experience our commitment to delivering the highest level of customer service. The goal of our program is to minimize business disruption, maximize protection, and increase the value of your investment.

Partner Enabled Premium Support

In addition to Standard or Premium Support delivered directly by Palo Alto Networks, you may choose a technical support offering from a Palo Alto Networks Authorized Support Center (ASC). ASC-designated partners provide Level 1 and 2 support with the added value of local language, multivendor, or customized support that complements Palo Alto Networks offerings.

When you choose support from an ASC, Palo Alto Networks will provide the partner with Partner Enabled Premium Support to enable them to better support you. This gives the ASC advanced support, 24/7, year-round coverage, and next-business-day shipment or 4-hour advanced replacement services.

More Information

To learn more about Palo Alto Networks Support offerings, visit paloaltonetworks.com/support or contact your local account manager. For product information, visit https://www.paloaltonetworks.com/products/products-a-z.

Why Palo Alto Networks?

Palo Alto Networks is committed to your success in preventing successful cyberattacks. Our award-winning services organization gives you timely access to technical experts and online resources to ensure your business is protected. We take our responsibility for your success seriously and continuously strive to deliver an exceptional customer experience. Our entire services organization and Authorized Support Centers are there to ensure maximum uptime and streamlined operations.

2015–2021: Palo Alto Networks, Inc. has been recognized by J.D. Power for seven consecutive years for providing "An Outstanding Customer Service Experience" for its Assisted Technical Support.

2015–2021: TSIA certification recognizes that Palo Alto Networks meets the highest industry support standards and has achieved Global Rated Outstanding Assisted Support for a seventh consecutive year.

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

parent_ds_premium-support_071823