



PA-440



PA-450



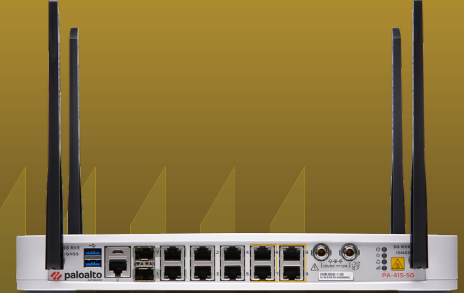
PA-460



PA-455



PA-410



PA-415-5G



PA-455-5G



PA-445



PA-415

PA-400 Series

The Palo Alto Networks PA-400 Series Next-Generation Firewalls (NGFWs) comprise the PA-410, PA-415, PA-415-5G, PA-440, PA-445, PA-450, PA-455, PA-455-5G, and PA-460. They bring ML-Powered NGFW capabilities to distributed enterprise branch offices, retail locations, and midsized businesses.

The world's first ML-Powered NGFW 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.
- Spans a range of performance needs for the distributed enterprise with a broad lineup.
- Offers security in a desktop form factor.
- Supports high availability with active/active and active/passive modes.
- Built with a single-pass architecture to deliver predictable performance with security services.
- Features silent, fanless design with optional redundant power supply for branch and home offices.
- Simplifies the deployment of large numbers of firewalls with optional Zero Touch Provisioning (ZTP).
- Supports centralized administration with Panorama® network security management.
- 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-400 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-400 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-400 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-400 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-400 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-400 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-400 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.

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

PA-400 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.

Integrated 5G Cellular Modem

The integrated 5G Next-Generation Firewall is expanding the entry-level appliance portfolio to include the PA-415-5G, with integrated 5G cellular modem. With this new appliance, enterprise and remote branches can ensure optimal uptime with 5G leveraged as a backup WAN transport for business-critical applications. In addition, other mobile businesses that require cellular as their primary WAN can simply deploy this appliance and ensure rapid deployment without the hassle of adding additional appliances to leverage 5G.

Supported radio frequency (RF) bands:

- **5G NR Sub-6GHz (FR1):** n2, n3, n5, n66, n71, n77, n78, n79
- **LTE:** B1, B2, B3, B4, B5, B7, B8, B12, B13, B14, B17, B18, B19, B20, B25, B26, B28, B29, B30, B32, B34, B38, B39, B40, B41, B42, B46, B48, B66, B71
- **3G:** B1, B2, B4, B5, B6, B8, B9, B19

Table 1. PA-400 Series Performance and Capacities

	PA-410	PA-415	PA-415-5G	PA-440	PA-445	PA-450	PA-455	PA-455-5G	PA-460
Firewall throughput (appmix)*	1.4 Gbps	1.5 Gbps	1.5 Gbps	2.4 Gbps	2.7 Gbps	3.3 Gbps	3.6 Gbps	3.2 Gbps	4.2 Gbps
Threat Prevention throughput (appmix)†	0.8 Gbps	0.8 Gbps	0.8 Gbps	1.2 Gbps	1.25 Gbps	2.1 Gbps	2.3 Gbps	1.8 Gbps	3.0 Gbps
IPsec VPN throughput‡	0.5 Gbps	0.5 Gbps	0.5 Gbps	1.1 Gbps	1.1 Gbps	1.7 Gbps	1.8 Gbps	1.6 Gbps	2.3 Gbps
Max concurrent sessions§	64,000	64,000	64,000	200,000	200,000	300,000	300,000	300,000	400,000
New sessions per second¶	11,000	11,000	11,400	34,000	34,000	48,000	56,000	48,000	67,000
Virtual systems (base/max)#	1/1	1/1	1/1	1/2	1/2	1/5	1/5	1/5	1/5

Notes: Results were measured on PAN-OS 12.1. Adding Virtual Systems requires a separate license.

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

† Threat Prevention throughput is measured with App-ID, IPS, antivirus, antispysware, WildFire, DNS Security, file blocking, and logging enabled, 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, using 1 byte HTTP transactions.

Adding virtual systems over base quantity requires a separately purchased license and a minimum of PAN-OS 11.0 and 11.1 for PA-415-5G and PA-455. PA-455-5G needs 11.2 for VSYS.

Table 2. PA-400 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
SD-WAN
Path quality measurement (jitter, packet loss, latency)
Initial path selection (PBF)
Dynamic path change
IPv6
L2, L3, tap, virtual wire (transparent mode)
Features: App-ID, User-ID, Content-ID, WildFire, and SSL decryption
SLAAC
IPsec 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
VLANs
802.1Q VLAN tags per device/per interface: 4,094/4,094
Aggregate interfaces (802.3ad), LACP

Table 3. PA-400 Series Hardware Specifications

I/O		
PA-410: 1G RJ45 (7) PA-440, PA-450, PA-460: 1G RJ45 (8) PA-415, PA-445: 1G SFP/RJ45 combo (1), 1G RJ45 (4), 1G RJ45/PoE (4) PA-415-5G: Embedded 5G cellular module, 1G SFP/RJ45 combo (1), 1G RJ45 (4), 1G RJ45/PoE (4) PA-455: 1G SFP/RJ45 combo (2), 1G RJ45 (2), 1G RJ45/PoE (4) PA-455-5G: Embedded 5G cellular module, 1G SFP/RJ45 combo (2), 1G RJ45 (6), 1G RJ45 PoE (4)		
Management I/O		
PA-410: 10/100/1000 out-of-band management port (1), RJ45 console port (1), USB port (2) PA-415, PA-415-5G, PA-445: SFP/RJ45 (1 GB) combo management port (1), RJ45 console port (1), USB port (2) Micro USB console port (1) PA-440, PA-450, PA-455, PA-460: 10/100/1000 out-of-band management port (1), RJ45 console port (1), USB port (2), Micro USB console port (1) PA-455-5G: SFP/RJ45 (1 GB) combo management port (1), RJ45 console port (1), USB port (1)		
Storage Capacity		
PA-410: 64 GB eMMC PA-415, PA-415-5G, PA-440, PA-445, PA-450, PA-455, PA-455-5G, PA-460: 128 GB eMMC		
Trusted Platform Module (TPM)		
Integrated with TPM for secure boot, hardware root of trust, and securing system secrets.		
Power Over Ethernet (PoE)		
PA-415, PA-415-5G, PA-445, PA-455, PA-455-5G PoE 1G RJ45 ports (4) Total PoE Budget: 91 W Maximum loading on a single port: 60 W		
Power Supply		
	Average Power Consumption	Max Power Consumption
PA-410	17 W	23 W
PA-415 or PA-415-5G*	133 W (with 91W PoE output)	142 W (with 91 W PoE output)
PA-440	28.9 W	34.3 W
PA-450 or PA-460	32.6 W	41.3 W
PA-445*	140 W (with 91 W PoE output)	146 W (with 91 W PoE output)
PA-455*	125.2 W (with 91 W PoE output)	143.4 W (with 91 W PoE output)
PA-455-5G*	195 W (with 151 W PoE output)	212 W (with 151 W PoE output)

* With the provided AC adapter(s)

Table 3. PA-400 Series Hardware Specifications (continued)

Max BTU/hr
PA-410: 78 PA-415, PA-440, PA-445: 117 PA-450, PA-460: 141 PA-415-5G: 150 PA-455: 205 PA-455-5G: 655
Input Voltage (Input Frequency)
100-240 VAC (50-60 Hz)
Max Current Consumption
PA-410: 1.5 A @ 12 VDC PA-415, PA-440, PA-445: 2.9 A @ 12 VDC PA-450, PA-460: 3.4 A @ 12 VDC PA-415-5G: 3.7 A @ 12 VDC PA-455: 5 A @ 12 VDC PA-455-5G: 3.6 A @ 54 VDC
Max Inrush Current
PA-410: 2.1 A PA-415, PA-440, PA-445: 3.3 A PA-450, PA-460: 4.2 A PA-415-5G: 3.5 A PA-455: 4.4 A PA-455-5G: 5.2 A @ 54 VDC input
Dimensions
PA-410: 1.63" H x 6.42" D x 9.53" W PA-415: 1.73" H x 9" D x 13" W PA-445: 1.66" H x 8.87" D x 13" W PA-440, PA-450, PA-460: 1.74" H x 8.83" D x 8.07" W PA-415-5G: 1.73" H x 9" D x 13" W PA-455: 1.7" H x 9.4" D x 15.4" W PA-455-5G: 1RU H x 283 mm D x 303 mm W
Weight (Standalone Device/As Shipped)
PA-410: 3.1 lbs/5.9 lbs PA-415: 7.85 lbs/12.2 lbs PA-445: 8.7 lbs/12.6 lbs PA-440, PA-450/PA-460: 5.0 lbs/7.8 lbs PA-415-5G: 7.85 lbs PA-455: 9.8 lbs/14.1 lbs PA-455-5G: 9 lbs/TBD
Safety
cTUVus, CB
EMI
FCC Class B, CE Class B, VCCI Class B
Certifications
See paloaltonetworks.com/legal-notices/trust-center/compliance
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 Passive cooling



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-400-series_022326