PA-410R-5G

PA-410R

PA-450R-5G

PA-450R

PA-400R Series

The Palo Alto Networks PA-400R Series consists of ruggedized ML-Powered Next-Generation Firewalls (NGFWs) that bring next-generation capabilities to industrial applications in harsh environments.

The PA-400R Series ruggedized appliances secure industrial and defense networks in a range of harsh environments, such as utility substations, power plants, manufacturing plants, oil and gas facilities, building management systems, and healthcare networks.

Highlights

- World's first ruggedized ML-Powered NGFW

- Eleven-time Leader in the Gartner Magic Quadrant for Network Firewalls

- Leader in The Forrester Wave: Enterprise Firewalls, Q4 2022

- Extended operating range for temperature

- Certified to IEC 61850-3 and IEEE 1613 environmental and testing standards for vibration, temperature, and immunity to electromagnetic interference

- Supports high availability with active/active and active/passive modes

- Deliver predictable performance with security services

- Features silent, fanless design with no moving parts

- Simplifies deployment of large numbers of firewalls with optional Zero Touch Provisioning (ZTP)

- Supports centralized administration with Panorama® centralized management and Strata™ Cloud Manager

- Maximizes security investments and prevents business disruptions with Strata Cloud Manager

The controlling element of the PA-400R 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.

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 internet of things (IoT) devices and make policy recommendations; is a 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 rules based on App-ID with Policy Optimizer built in, 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 User Devices Anywhere While Adapting Policies 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.
- Offers rich visibility into TLS traffic, such as the 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, for example, 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 a 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.

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.

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, IoT, and SaaS. Furthermore, the threat landscape is rapidly intensifying due to the ability to easily 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.

Integrated 5G Cellular Modem

The integrated 5G Next-Generation Firewall is expanding the entry-level appliance portfolio to include the PA-450R-5G and the PA-410R-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.

Table 1: PA-400R Series Performance and Capabilities				
	PA-410R	**PA-410R-5G**	**PA-450R**	**PA-450R-5G**
Firewall throughput (appmix)[*]	1.4 Gbps	1.4 Gbps	3.2 Gbps	3.2 Gbps
Threat Prevention throughput (appmix)[†]	650 Mbps	650 Mbps	1.7 Gbps	1.7 Gbps
IPsec VPN throughput[‡]	650 Mbps	650 Mbps	1.7 Gbps	1.7 Gbps
Max sessions	64,000	64,000	200,000	200,000
New sessions per second[§]	11,400	11,400	48,000	48,000
Virtual systems (base/max)[‖]	1/2	1/2	1/2	1/2
Compliance rating	IP65	IP65	IP40	IP40

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, DNS Security, file blocking, and logging enabled, utilizing appmix transactions.

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

[§] 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 and at minimum PAN-OS 11.1.

Table 2: PA-400R Series Networking Features
Interface Modes
L2, L3, tap, virtual wire (transparent mode)
Routing
OSPF v2/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, ICMP v1, v2, and v3
SD-WAN
Path quality management (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

Table 2: PA-400R Series Networking Features (continued)
IPsec VPN
Key exchange: manual key, IKEv1, and IKEv2 (preshared key, certificate-based authentication)
Encryption: 3des, AES (128-bit, 192-bit, 256-bit)
Authentication: MD5, SHA-1, SHA-256, SHA-384, SHA-512
PQC VPN
VLANs
802.1Q VLAN tags per device/per interface: 4,094/4,094
Aggregate interfaces (802.3ad), LACP

Table 3: PA-400R Series Hardware Specifications	
I/O	
PA-410R: 1G RJ45 (4), 1G SFP (2)	
PA-410R-5G: Integrated 5G (DSSS – Dual SIM Single Standby), 1G RJ45 (4), 1G SFP (2)	
PA-450R: 1G RJ45 (6), 1G SFP/RJ45 combo (2)	
PA-450R-5G: Integrated 5G (DSSS – Dual SIM Single Standby), 1G RJ45 (6), 1G SFP/RJ45 combo (2)	
Management I/O	
PA-410R, PA-410R-5G: Management Console Port – RJ45 (1), USB Port for bootstrapping (1), 1G Management Port (1)	
PA-450R, PA-450R-5G: Management Console Port – RJ45 (1), USB Port for bootstrapping (1) , 1G Management Port (1), micro USB Console Port (1)	
Storage Capacity	
PA-410R, PA-410R-5G, PA-450R, and PA-450R-5G: 128 GB	
Trusted Platform Module (TPM)	
Integrated with TPM for secure boot, hardware root of trust, and securing system secrets.	
Power Supply (Max Power Consumption)	
PA-410R	28.9 W
PA-410R-5G	28.9 W
PA-450R	39.4 W
PA-450R-5G	39.4 W
Max BTU/hr	
PA-450R and PA-450R-5G: 136 BTU/hr	
PA-410R and PA-410R-5G: 129 BTU/hr	
Input Voltage (Input Frequency)	
12 V–48 VDC	
Max Current Consumption	
5A @ 12 VDC	
Max Inrush Current	
5A	
Dimensions	
PA-410R: 96 mm H x 270 mm W x 208 mm D	
PA-410R-5G 105: mm H x 270 mm W x 208 mm D	
PA-450R: 44.4 mm H x 390 mm W x 238 mm D – 1RU	
PA-450R-5g: 44.4 mm H x 390 mm W x 253 D	

Table 3: PA-400R Series Hardware Specifications (continued)
Weight (Standalone Device/As Shipped)
PA-410R: 9/12.3 lbs
PA-410R-5G: 9/12.8 lbs
PA-450R: 10/14.5 lbs
PA-450R-5G: 10/14.5 lbs
Safety
UL 62368-1:2014, CSA C22.2 No. 62368-1:14, IEC/EN 62368-1: 2014, IEC 62368-1: 2018
EMI
FCC Class A, CE Class A, VCCI Class A
Certifications
See paloaltonetworks.com/legal-notices/trust-center/compliance
Environment
Operating temperature: -40℃ to 70℃
Nonoperating temperature: -40℃ to 70℃
Passive cooling