PA-410R-5G

PA-415-5G

PA-450R-5G

PA-455-5G

NGFW Series with Integrated 5G

Secure 5G Connectivity with Built-In Zero Trust Enforcement

Traditional cellular routers in private mobile networks offer basic connectivity but often lack the advanced security and visibility necessary for implementing Zero Trust principles and microsegmentation. Palo Alto Networks Next-Generation Firewalls (NGFWs) with integrated 5G modems—comprising the PA-410R-5G, PA-415-5G, PA-450R-5G, and PA-455-5G—address these challenges.

Our ruggedized ML-powered NGFWs are built for harsh environments, such as utility substations, power plants, manufacturing plants, and oil and gas facilities. They provide comprehensive network segmentation through security zones and application-level policies, as well as support dual SIM configurations for resilient and secure uplinks, ensuring continuous connectivity.

With built-in capabilities, including our operational technology (OT) security and Advanced Threat Prevention, these firewalls offer full visibility and control over all connected devices, enabling secure, segmented access even in the most demanding environments.

Enterprise and remote branches can enable secure, segmented, and policy-driven access for industrial and remote environments—without compromising performance or uptime—and 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 NGFW and ensure rapid deployment without the hassle of adding an additional cellular router for 5G access. PA-410R-5G, PA-415-5G, PA-450R-5G, and PA-455-5G bring ML-powered NGFW capabilities to distributed enterprise branch offices, retail locations, and midsize businesses.

Highlights

- World's first NGFW that has an integrated 5G cellular modem with a Global Positioning System (GPS) and Global Navigation Satellite System (GNSS) powered by Precision AI®.
- Spans a range of performance needs for the distributed enterprise with a broad lineup.
- Offers security in a desktop form factor with multiple mounting options, including a DIN rail, wall mount, rackmount, and desktop.
- Delivers predictable performance with security services.
- Features a silent, fanless design with an optional redundant power supply for branch and home offices.
- Simplifies deployment of large numbers of firewalls with optional Zero Touch Provisioning (ZTP) over both cellular and Ethernet uplinks.
- Supports centralized administration with Panorama® network security management.
- Maximizes security investments and prevents business disruptions with Strata™ Cloud Manager.

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

Key Security and Connectivity Features

Next-Generation Firewalls Powered by Precision AI

- 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 regardless of port, protocol, evasive techniques, or encryption (SSL/TLS). To keep pace with the SaaS explosion, it automatically discovers and controls new applications 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 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 built-in Policy Optimizer, giving you a more secure and easier-to-manage rule set.

See 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, including wireless LAN controllers, VPNs, directory servers, security information and event management (SIEM), and proxies.
- Enables 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 regardless of user 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; prevents the 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 are located, to move quickly toward a zero trust security posture with Cloud Identity Engine—a cloud-based architecture for identity-based security.

See 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 traffic that uses TLSv1.3 and HTTP/2.
- 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 the 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 the URL category, source and destination zone, address, user, user group, device, and port for privacy and regulatory compliance purposes.
- Enables 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, optimize your network performance, and reduce operating expenses.

Read the Decryption: Why, Where and How whitepaper to learn how it helps you prevent threats and secure your organization.

Offers Centralized Management and Visibility

- Provides centralized management, configuration, and visibility for multiple distributed NGFWs (regardless 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. The PA-410R-5G, PA-415-5G, PA-450R-5G, and PA-455-5G models export session logs to Panorama and Strata Cloud Manager. The PA-410R-5G, PA-415-5G, PA-450R-5G, and PA-455-5G models also support on-box session logging.
- 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 prevent operational disruptions.
- **Strengthen security in real time:** Get 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 operations:** 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 because of 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 our Cloud-Delivered Security Services (CDSS),

you can benefit from best-in-class, real-time security to help you protect all users, devices, and data in your network, regardless of location.

Our 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 the shared threat intelligence of our more than 80,000 customers worldwide, you gain insights into emerging threats and can act proactively. Finally, seamless integration with NGFWs and SASE eliminates security gaps and offers your organization a single pane of glass to view and manage your security.

Our 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 cloud access security broker (CASB):** Discover and control all SaaS consumption in your network with visibility into over 60,000 SaaS apps and protect your data with more than 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.

Plus, we've been named eleven times as a leader in the Gartner® Magic Quadrant™ for Network Firewalls. We've also been recognized as a leader in The Forrester Wave™: Enterprise Firewall Solutions, Q4 2024.

Delivers a Unique Approach to Packet Processing with a 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 on Cellular Interface

- 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. NGFW Performance and Capacities				
	PA-410R-5G	PA-415-5G	PA-450R-5G	PA-455-5G
Firewall throughput (appmix)*	1.4 Gbps	1.5 Gbps	3.2 Gbps	3.2 Gbps (preliminary)
Threat Prevention throughput (appmix)†	0.8 Gbps	0.8 Gbps	1.7 Gbps	1.8 Gbps (preliminary)
IPsec VPN throughput‡	0.65 Gbps	0.65 Gbps	1.7 Gbps	650 Mbps (preliminary)
Max. concurrent sessions§	64,000	64,000	200,000	300,000
New sessions per second‖	11,000	11,400	48,000	48,000
Virtual systems (base/max)#	1/1	1/1	1/2	1/5

Note: Results were measured on PAN-OS 11.2. 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, antispyware, WildFire, 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 using HTTP transactions.

‖ New sessions per second are measured with application override, using 1 byte HTTP transactions.

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

Table 2. NGFW Networking Features
Interface Modes
Layer 2, Layer 3, tap, and virtual wire (transparent mode)
Routing
OSPFv2/v3 with graceful restart, BGP with graceful restart, RIP, and static routing
Policy-based forwarding
PPPoE and DHCP supported for dynamic address assignment
Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, and v3
SD-WAN
Path quality measurement (jitter, packet loss, and latency)
Initial path selection (policy-based forwarding [PBF])
Dynamic path change
IPv6
Layer 2, Layer 3, tap, and virtual wire (transparent mode)
Features: App-ID, User-ID™, Content-ID™, WildFire, and SSL decryption
Stateless address autoconfiguration (SLAAC)
IPsec VPN
Key exchange: Manual key, IKEv1, and IKEv2 (pre-shared key and certificate-based authentication)
Encryption: 3des, AES (128-bit, 192-bit, and 256-bit)
Authentication: MD5, SHA-1, SHA-256, SHA-384, and SHA-512
VLANs
802.1Q VLAN tags per device/per interface: 4,094/4,094
Aggregate interfaces (802.3ad), LACP

Table 3. NGFW Antenna Specifications			
Antennas			
Model	**Antenna**	**Description**	**Included**
PA-415-5G	PAN-PA-5G-ANTENNA	Direct mount (4x)	Yes
PA-455-5G	PAN-ANT-DM-5G-SMA	4x4 MIMO w/ 5M Cable SMA-M	Order separately
PA-410R-5G	PAN-1RU-RGD-C-ANT	Direct mount (4x)	Yes
PA-450R-5G	PAN-1RU-RGD-C-ANT	Direct mount (4x)	Yes
Note: Rack mount kits for third-party remote antennas are available.			
Supported Radio Frequency (RF) Bands			
PA-415-5G	5GNR FR1	n1, n2, n3, n5, n7, n8, n12, n20, n25, n28, n38, n40, n41, n48, n66, n71, n77, n78, n79	
	4G 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, B43, B46, B48, B66, B71	
	WCDMA 3G	B1, B2, B4, B5, B6, B8, B9, B19	
PA-455-5G **PA-410R-5G** **PA-450R-5G**	5GNR FR1	n1, n2, n3, n4, n5, n7, n8, n12, n13, n14, n17, n18, n19, n20, n25, n26, n28, n30, n39, n40, n41, n48, n66, n71, n77, n78, n79	
	4G LTE	B1, B2, B3 , B4, B5, B7, B8, B12, B13, B14, B17, B18, B19, B20, B25, B26, B28, B30, B34, B38, B39, B40, B41, B42, B43, B46, B48, B66, B71	
	WCDMA 3G	B1, B2, B4, B5, B8, B19	

Table 4. NGFW Cellular Industry Certification				
Antennas				
	PA-415-5G	**PA-455-5G**	**PA-410R-5G**	**PA-450R-5G**
PTCRB	✓	✓	✓	✓
GCF	✓	—	✓	✓

Table 5. Cellular NGFW Hardware Specifications

I/O

PA-410R-5G: Integrated 5G (Dual SIM Single Standby [DSSS]), 1G RJ45 (4), and 1G SFP (2)

PA-415-5G: Integrated 5G (DSSS), 1G SFP/RJ45 combo (1), 1G RJ45 (4), and 1G RJ45/PoE (4)

PA-450R-5G: Integrated 5G (DSSS), 1G RJ45 (6), and 1G SFP/RJ45 combo (2)

PA-455-5G: Integrated 5G (DSSS), 1G SFP/RJ45 combo (2), 1G RJ45 (6), and 1G RJ45 Power over Ethernet (PoE) (4)

Management I/O

PA-410R-5G: Management console port—RJ45 (1), USB port for bootstrapping (1), and 1G management port (1)

PA-415-5G: SFP/RJ45 (1 GB) combo management port (1), RJ45 console port (1), USB port (2), and Micro USB console port (1)

PA-450R-5G: Management console port—RJ45 (1), USB port for bootstrapping (1), 1G management port (1), and Micro USB console port (1)

PA-455-5G: SFP/RJ45 (1 GB) combo management port (1), RJ45 console port (1), and USB port (1)

Log: 1G/10G SFP+ (2)

Storage Capacity

PA-410R-5G, PA-415-5G, PA-450R-5G, and PA-455-5G: 128 GB eMMC

Trusted Platform Module (TPM)

Integrated with TPM for secure boot, hardware root of trust, and securing system secrets

Power over Ethernet

PA-415-5G
PoE 1G RJ45 ports (4)
Total PoE Budget: 91 W
Maximum loading on a single port: 60 W

PA-455-5G
PoE 1G RJ45 ports (4)
Total PoE Budget: 151 W
Maximum loading on a single port: 60 W

Power Supply

	Average Power Consumption	Maximum Power Consumption
PA-410R-5G	18 W	28.9 W
PA-415-5G (with the provided AC adapters)	133 W (with 91 W PoE output)	142 W (with 91 W PoE output)
PA-450R-5G	27 W	39.4 W
PA-455-5G (with the provided AC adapters)	195 W (with 151 W PoE output)	212 W (with 151 W PoE output)

Max BTU/hr

PA-410R-5G: 129

PA-415-5G: 150

PA-450R-5G: 136

PA-455-5G: 655

Input Voltage (Input Frequency)

PA-415-5G and PA-455-5G: 100–240 VAC (50–60 Hz)

PA-410R-5G and PA-450R-5G: 12 V–48 VDC

Max Current Consumption

PA-410R-5G: 2.4A@12VDC

PA-450R-5G: 6A@ 12VDC

PA-415-5G: 11.3A@ 12VDC

PA-455-5G: 3.6A@ 54VAC

Table 5. Cellular NGFW Hardware Specifications (continued)
Max Inrush Current
PA-410R-5G and PA-450R-5G: 5 A
PA-415-5G: 3.5 A
PA-455-5G: 5.2 A
Dimensions
PA-410R-5G H: 8.07", W: 10.63", D: 3.66" (H: 20.5 cm, W: 27 cm, D: 9.3 cm)
PA-415-5G: 1RU H: 1.73", W: 13", D: 9" (H: 4.40 cm, W: 33.02 cm, D: 22.86 cm)
PA-450R-5G: 1RU H: 1.73", W: 15.35", D: 9.71" (H: 4.39 cm, W: 38.99 cm, D: 24.66 cm)
PA-455-5G: 1RU H: 1.77", W: 11.81", D: 11.02" (H: 4.5 cm, W: 30 cm, Depth: 28 cm)
Weight (Standalone Device/as Shipped)
PA-410R-5G: 9/12.8 lbs (4.08 / 5.81 kg)
PA-415-5G: 7.85/11.7 lbs (3.65 / 5.31 kg)
PA-450R-5G: 10/14.5 lbs (4.5 / 6.6 kg)
PA-455-5G: 10.75 /17.25 lbs (4.88 / 7.82 kg)
Safety
PA-410R-5G, PA-415-5G, PA-450R-5G, and PA-455-5G: UL 62368-1:2014, CSA C22.2 No. 62368-1:14, IEC/EN 62368-1: 2014, IEC 62368-1: 2018
EMC/EMI
PA-410R-5G, PA-415-5G, PA-450R-5G, and PA-455-5G: FCC Class A, VCCI Class A, AS/NZS CISPR 32 Class A, EN 300 386, EN 55032/CISPR 32 Class A, and EN 55035/CISPR 35
PA-410R-5G and PA-450R-5G: IEEE 1613 and IEC 61850-3 (power substation standards)
Certifications
See the Palo Alto Networks Compliance page.
Environment
PA-415-5G and PA-455-5G: Operating temperature: 32°F to 104°F and 0°C to 40°C Nonoperating temperature: -4°F to 158°F and -20°C to 70°C Passive cooling
PA-410R-5G and PA-450R-5G: Operating temperature: -40°F to 158°F and -40°C to 70°C Nonoperating temperature: -40°F to 158°F and -40°C to 70°C Passive cooling IEEE 1613 and IEC 61850-3 (Power Substation standards)
PA-410R-5G IP65 ingress rating MIL-STD-810H (Military Standard) Method 514.8C Category 4 - Random Vibration: Common Carrier (Operational, 10 Hz–500 Hz, and 1.08 Grms Method 514.8C Category 4 - Random Vibration: Composite Wheeled Vehicle (Unpackaged, Non-Operational, 5 to 500 Hz, and 2.24 Grms) Method 516.8 Procedure I: Functional Shock (Terminal Peak Sawtooth Pulse, Operational 40 G, and 11 ms) Method 516.8 Procedure V: Crash Hazard Shock (Terminal Peak Sawtooth Pulse, Operational, 75 G, and 6 ms) Method 516.8, Procedure VI: Bench Handling (Unpackaged, Non-Operational, and 100 mm [4 inches] drops)

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

© 2025 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_ngfw-series-with-integrated-5g_070825