

PA-50R Series Ruggedized, 5G-Enabled NGFWs

Protect Critical Infrastructure with Quantum-Optimized, ML-Powered NGFWs

Agencies and organizations with field-deployed OT assets are upgrading access networks to support new AI-led digital transformation, and are turning to cellular to connect more assets and intelligent edge devices. Yet securing this critical infrastructure has become more difficult and more urgent now with AI-driven attacks across an expanding surface of assets and devices.

Address these challenges with Palo Alto Networks PA-50R Series of ruggedized, quantum-optimized NGFWs with integrated 5G and LTE technology. These NGFWs comprise models PA-52R-5G, PA-54R-POE, PA-54R-POE-D-5G, and PA-56R-POE-5G.

Our ruggedized ML-Powered NGFWs are built to protect critical infrastructure in harsh field environments, such as utility substations, power plants, outside cabinets, and oil and gas facilities. These compact hardware appliances deliver our industry-leading cybersecurity by natively consolidating WAN (5G and LTE, fiber optics, and copper), routing, switching, SD-WAN, and NGFW capabilities into a single platform. This hyperconverged architecture provides remote field locations with secure, policy-driven access for industrial environments without sacrificing performance or network uptime.

Equipped with Advanced Threat Prevention and App-ID™ for operational technology (OT) and IT protocols, these firewalls offer visibility and granular control over all connected edge devices. Through zone-based network segmentation and application-level policies, organizations can easily enforce secure, isolated access across the most demanding physical environments.

For continuous connectivity, integrated dual-SIM configurations ensure highly resilient, active/active, secure uplinks. Whether using 5G as a primary WAN transport or as a reliable backup for business-critical applications, the platform simplifies the edge footprint and guarantees rapid deployment without the hassle of managing separate hardware devices.

Security-First Networking with NGFWs

To streamline edge hardware protection, we created a dedicated platform to secure critical infrastructure—integrating full routing, high-density switching, and Power over Ethernet (PoE) into a single ruggedized NGFW.

Hyper-Converged Edge

Our next-generation ruggedized 5G PA-50R firewall portfolio converges the hardware stack into a single, cohesive, industrial-grade solution. Built from the ground up to address the rigid operational mandates of the field practitioner, this platform natively converges premier multigigabit NGFW capabilities, advanced routing, high-density switching, and enhanced PoE delivery into a singular, fanless appliance.

High-Density Integrated Switching and High-Power PoE

Designed for connectability, the PA-50R family supports 8–16 physical Gigabit Ethernet ports. Selected models also support high-power PoE+ (up to 802.3bt PoE++ Type 4, delivering up to 90W on a single port) backed by a generous total hardware system power budget of up to 225W. Field crews can power high-draw remote equipment—such as pan-tilt-zoom (PTZ) surveillance cameras or industrial IoT sensors—from the firewall box by using a single Ethernet run, fully eliminating external power bricks.

Industrial Environmental Hardening

The NGFWs are built with a fanless, silent convection-cooled metal housing with no moving parts to prevent failure from dust, salt, moisture, or oil infiltration. The hardware is structurally hardened to endure extreme operating temperatures from -40°C to 70°C, heavy mechanical vibration, and intense electromagnetic interference (EMI).

AI-Driven Cybersecurity

As a leader in IT and OT cybersecurity, we provide unmatched visibility into connected assets and microsegmentation that supports a zero trust security framework for historically unshielded OT assets.

Frontier Virtual Patching and Threat Prevention

With new capabilities from Palo Alto Networks, the platform shields unpatchable or end-of-life industrial assets from exploitation with updated Frontier Virtual Patching. When cloud-connected, the platform integrates with a global telemetry ecosystem of over 75,000 active enterprise tenants to deliver automated protections up to 60x faster than traditional signature updates.

Precision AI Security Edge

Traditional edge security relies on rudimentary port blocking and IP address filtering, which is incapable of detecting horizontal pivots or payload manipulation. Our ruggedized edge platform extends the power of enterprise-grade, machine learning-driven security to the far edge of the network through the following capabilities.

Full-Featured Layer 7 App-ID Awareness

Provides industry-leading Layer 7 security with App-ID, which natively decodes, classifies, and controls traffic across hundreds of proprietary industrial and SCADA protocols, including Modbus, DNP3, IEC-104, Siemens S7, PROFINET, BACnet, and EtherNet/IP. Security rules are written by using human-readable application and device contexts rather than static, easily spoofed ports.

Granular Contextual Microsegmentation

Stops device-to-device lateral pivots within flat Layer 2 legacy industrial networks without requiring disruptive network topology rearchitecting. The platform delivers dual traffic-steering mechanisms tailored to any field environment:

- **Proxy ARP:** Explicitly handles legacy brownfield OT environments using hard-coded static IP addresses, safely diverting intra-VLAN traffic through the firewall engine for Layer 7 policy enforcement.
- **DHCP server response overwrite:** Intercepts dynamic addressing requests and applies a highly tailored netmask over all 32 bits (/32) of an IP address, converting the network into an isolated "subnet of one" where all communication must clear security checks.

Frictionless Secure Remote Access via Prisma Browser

Eliminates the security risk of always-on, poorly managed legacy VPN tunnels for third-party machine vendors and operational staff with the secure Prisma® Browser™. The platform enables direct, browser-native privileged remote access supporting secure RDP, SSH, and VNC terminal sessions with embedded just-in-time session controls, detailed administrative audit logs, full video recording, and a built-in enterprise password vault.

Operational Simplicity from Edge to Core

To ensure this advanced protection stays effortless for lean teams, we embed secure zero touch provisioning (ZTP) alongside highly resilient, multicarrier network uptime.

Zero Touch Provisioning at Scale

ZTP streamlines massive field rollouts by fully eliminating the need for trained IT or cybersecurity specialists on-site during installation. Nontechnical field crews can simply mount the physical appliance, connect the network lines, and power it up. The device automatically establishes a secure handshake over cellular or Ethernet with the central management portal via a quick serial or QR-code registration, securely drawing down its full verified configuration and security profiles within minutes.

Active/Active Resilient SD-WAN Delivers Uptime Reliability

This integrated SD-WAN capability provides active/active and active/standby WAN connectivity across high-performance multiband 5G and LTE cellular, copper, fiber optic, or optionally, satellite links. The platform treats routing as an embedded capability of the security fabric, executing a comprehensive software routing stack, including industry-standard OSPFv2/v3, multiprotocol BGP with graceful restart, RIP, and policy-based forwarding. It supports multicarrier active/active load balancing and seamless dynamic failover across diverse paths, ensuring continuous connectivity for business-critical data.

Uncompromising Infrastructure Resilience

With an optional active/passive high availability configuration, persistent PoE technology guarantees that power delivery to downstream life-safety or surveillance gear remains uninterrupted during firewall reloads or operational upgrades.

Unified Management Fabric

This management fabric provides a single point of truth across the entire enterprise security posture. The platform is managed via Strata™ Cloud Manager—the industry's first AI-powered unified operations solution—or on-premises via Panorama® for restricted, air-gapped enclaves. Administrators write a single security policy and push it seamlessly across all physical rugged devices, virtual software instances, and cloud SASE layers.

Certificate Lifecycle Automation

Certificate lifecycle automation integrates the deployment and configuration process to include automated PKI certificate lifecycle management with our optional Next-Generation Trust Security (NGTS) platform, eliminating manual certificate tracking overhead at scale.

Physical and Digital Monitoring Convergence

This level of monitoring features up to six ruggedized digital input/output (I/O) dry contacts, enabling the platform to act as a physical field sensor. It immediately binds real-world physical alerts (such as cabinet enclosure doors opening, flooding alarms, or local power line flips) to the centralized digital monitoring console for instant visibility and automated incident response workflows.

Deployment Flexibility and Sovereignty

The platform recognizes that critical infrastructure and defense enclaves operate under unique sovereignty, regulatory compliance, and connectivity constraints. Consequently, the architecture supports two operational modes.

Cloud-Connected Mode

Cloud-connected mode unlocks the maximum capabilities of our network security with Precision AI®. Deployed via Strata Cloud Manager, it uses predictive analytics and AIOps to forecast system and deployment health, proactively flagging potential link brownouts or capacity bottlenecks up to seven days in advance. Telemetry data flows securely to long-term cloud repositories so it can generate audit-ready, compliance-validated reporting mapped to NERC CIP, TSA Security Directives, NIS2, and NIST frameworks.

On-Premises and Sovereign Air-Gapped Mode

The air-gapped mode was built for high-consequence isolated environments where zero data or telemetry is permitted to leave the physical perimeter. Deployed via on-premises Panorama appliances, all threat signatures, protocol decoders, and PAN-OS® software packages are staged manually via secure data-diode architectures or offline media updates. All transaction logs and event contexts are collected and analyzed inside local logging enclaves, ensuring total data sovereignty and strict compliance without introducing external cloud requirements.

PA-50R Series Specifications

Table 1. Performance and Capacities of PA-50R Series Quantum-Optimized NGFWs				
	PA-52R-5G	PA-54R-POE-5G	PA-54R-POE-D-5G	PA-56R-POE-5G
Firewall throughput (appmix)*	2.0	3.0	3.0	4.0
Threat prevention throughput (appmix)†	1.0	1.6	1.6	2.4
IPsec VPN throughput‡	0.8	1.2	1.2	1.9
Max. concurrent sessions§	64,000	200,000	200,000	200,000
New sessions per second‖	2,000	5,000	5,000	5,000
Virtual systems (base/max)#	1/2	1/5	1/5	1/5

Note: Results were measured on PAN-OS 12.2.

* 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.

§ Maximum 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 the base quantity requires a separately purchased license.

Table 2. Cellular Interfaces		
Radio Frequencies		
PA-52R-5G (RedCap)	5GNR-FR1	n1, n2, n3, n5, n7, n8, n12, n13, n14, n18, n20, n25, n26, n28, n30, n34, n38, n39, n40, n41, n42, n43, n48, n66, n70, 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, B34, B38, B39, B40, B41, B42, B43, B48, B66, B70, B71, B106
	WCDMA 3G	Not supported
PA-56R-POE-5G PA-54R-POE-D-5G	5GNR-FR1	n1, n2, n3, n5, n7, n8, n12, n13, n14, n18, n20, n25, n26, n28, n29, n30, n38, n40, n41, n48, n66, n70, n71, n75, 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, B106
	WCDMA 3G	B1, B2, B4, B5, B6, B8, B9, B19
Industry Certifications		
	PTCRB	GCF
PA-52R-5G	Yes	Yes
PA-56R-POE-5G	Yes	Yes
PA-54R-POE-D-5G	Yes	Yes
Antenna Details		
	Type	Frequency
PA-52R-5G	2x1 MIMO	615–960 MHz/ 1,500–1,600 MHz/ 1,710–2,690 MHz/ 3,300–3,700 MHz
PA-56R-POE-5G	4x4 MIMO	
PA-54R-POE-D-5G	4x4 MIMO	

Table 3. PA-50R Series Networking Features
Interface Modes
L2, L3, tap, and virtual wire (transparent mode).
Routing
OSPFv2/v3 and MP-BGP with graceful restart, RIP, and static routing. Policy-based forwarding. PPPoE and DHCP clients are supported for dynamic address assignment for both IPv4 and IPv6. DHCP clients are supported for dynamic address assignment for IPv4. Multicast: PIM-SM, PIM-SSM, IGMP v2, v3, and v6.
Advanced SD-WAN
Path quality measurement (jitter, packet loss, and latency). Initial path selection (PBF). Bandwidth monitoring with dynamic path change. Key exchange: Manual key, IKEv1,* and IKEv2 (pre-shared key and certificate-based auth). Post-quantum PPK. Multi-VR and LR support over the SD-WAN overlay. Prisma Access Hub (hybrid SASE). Autonomous Digital Experience Management (ADEM) for NGFW support.
Layer 2 Switching
Layer 2 switching function on all data ports of the device. Transport traffic of multiple VLANs over a single physical link with VLAN trunking. Microsegment and inspect (up to Layer 7) intra-VLAN traffic. Ensure loop free topologies for Layer 2 domains with Multiple Spanning Tree Protocol. Prevent unknown unicast, multicast, and broadcast storms in Layer 2 domains.
IPv6
IPv6 inspection in L2, L3, tap, and virtual wire mode (transparent mode). Support for dual-stack and IPv6-only networks. Features: IPv6 geolocalization, OSPFv3, MP-BGP, NAT64, and NPTv6. DHCPv6 client with prefix delegation (PD) support. Stateless address autoconfiguration (SLAAC) server support. Features: App-ID, User-ID™, Content-ID™, WildFire, and SSL decryption.
IPsec and SSL 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. Post-quantum cypher (PQC) VPN. Secure access over IPsec and SSL VPN tunnels using GlobalProtect® gateway and portals.†
VLANs
802.1Q VLAN tags per device or per interface: 4,094/4,094. Aggregate interfaces (802.3ad) and LACP.
High Availability and Clustering
NGFW clustering with active/active. HA active/passive.
Mobile Network Infrastructure‡
Palo Alto Networks 5G-Native Security.

* Not supported with NGFW clustering.

† Requires a GlobalProtect license.

‡ For more information, see the ML-Powered NGFWs for 5G datasheet.

Table 4. PA-50R Series Hardware Specifications					
I/O	**Cellular**	**RJ-45**	**SFP**	**VIMS***	**Digital I/O**
PA-52R-5G	Dual SIM, Single Modem (RedCap)	8 x 1G	2 x 1G	Yes	N/A
PA-54R-POE	N/A	12 x 1G	2 x 1G	Yes*	6
PA-54R-POE-D-5G	Dual SIM, Dual Modem	12 x 1G	2 x 1G	Yes*	6
PA-56R-POE-5G	Dual SIM, Single Modem	16 x 1G	2 x 1G	N/A	6
Management I/O					
PA-52R-5G: Console: RJ-45 (1) Bootstrap: USB 3.0 Management: 1 Gb (1)					
PA-54R-POE, PA-54R-POE-D-5G, PA-56R-POE-5G Out-of-band management: 1G/10G SFP+ (2) Console: RJ-45 console port (1), USB-C Bootstrap: USB 3.2 Gen1 Type A Log: 10G SFP+ (2)					
		Storage Capacity		**Trusted Platform Module (TPM)**	
PA-52R-5G, PA-54R-POE, PA-54R-POE-D-5G, PA-56R-POE-5G		128 Gb		TPM 2.0	
	Max/Average Power Consumption			**Maximum Current Consumption**	
PA-52R-5G	40.0/25.0W			3.0A @ 12 VDC	
PA-54R-POE	225.1/29.7W			18.0A @ 12 VDC	
PA-54R-POE-D-5G	225.1/38.7W			18.0A @ 12 VDC	
PA-56R-POE-5G	225.1/35.9W			18.0A @ 12 VDC	
Input Voltage					
PA-52R-5G, PA-54R-POE, PA-54R-POE-D-5G, PA-56R-POE-5G: DC: 12V to 48 VDC AC (optional): 100–240 VAC (50–60 Hz)					
Mean Time Between Failure (MTBF)					
PA-52R-5G: 350,000 hrs @ 25°C					
PA-54R-POE, PA-54R-POE-D-5G, PA-56R-POE-5G: 300,000 hrs @ 25°C					
Mount Options and Dimensions					
PA-52R-5G: 1.7 H x 8.0 W x 8.0 D (inches) 1RU (side-by-side mounting optional) DIN rail mount (optional)					
PA-54R-POE, PA-54R-POE-D-5G: 5.8 H x 7.2 W x 5.5 D (inches) 3RU, 19" standard rack					
PA-56R-POE-5G: 3.4 H x 16.5 W x 5.7 D (inches) 2RU, 19" standard rack with power supply inserted					

Table 4. PA-50R Series Hardware Specifications (continued)
Weight (product/shipping)
PA-52R-5G: 5.5/7.0 lbs
PA-54R-POE, PA-54R-POE-D-5G: 7.5/10.3 lbs
PA-56R-POE-5G: 9.8/12.5 lbs
Safety
UL 62368-1/CSA C22.2 No. 62368-1: 25 IEC/EN 62368-1: 2014 IEC 62368-1: 2018 IEC 62368-1: 2023 cTUVus and CB
EMI
FCC Class A, CE Class A, and VCCI Class A
Certifications
Certification: IP-40 For more informationSee our Compliance page.
Max BTUs/Hr
PA-52R-5G†: 136.5 BTUs/Hr
PA-54R-POE, PA-54R-POE-D-5G, PA-56R-POE-5G: 767.7 BTUs/Hr
Environment
PA-52R-5G†, PA-54R-POE, PA-54R-POE-D-5G, PA-56R-POE-5G: Operating temperature: -40°C to 70°C Nonoperating temperature: -40°C to 70°C Passive cooling Humidity tolerance: 10%–90% Maximum altitude: 10,000 ft or 3,048 m Airflow: Front to back (port side to power supply side)

* Vehicle Ignition Management System (VIMS); in a future release with auto power supply unit (APSU).

† At 70°C, the PA-52R-5G requires 240 linear feet per minute (LFM) of external airflow.

Critical Infrastructure Security Series Ordering Information

Table 5. PA-52R-5G Series	
Part Number	**Details**
PAN-PA-52R-2-POST-RACK-MOUNT	PA-52R 2 post rack mount kit
PAN-PA-52R-4-POST-RACK-MOUNT	PA-52R 4 post rack mount kit
PAN-PA-52R-ACC	Replacement accessory kit for PA-52R. The accessory kit is included in the system.
PAN-PA-52R-BOX-SET	PA-52R shipping boxes with packaging: Quantity 5
PAN-PA-52R-DIN-CLIP	PA-52R-5G DIN CLIP
PAN-PA-52R-PKG-SET	PA-52R shipping boxes with packaging
PAN-PA-52R-WALL-MOUNT	PA-52R wall mount kit
PAN-PA-FIPS-KIT-52R	FIPS hardware kit for PA-52R
PAN-PA-5G-ANT-2X2-5M-SMAM	Remote antenna for PA-52R-5G
PAN-PWR-66W-12V-AC-R	66W power adapter for PA-52R

Table 6. PA-54R-POE and PA-54R-POE-D-5G Series	
Part Number	**Details**
PAN-PA-54R-2-POST-RACK-MOUNT	PA-54R, PA-54R-5G 2 post rack mount tray
PAN-PA-54R-WALL-MNT	PA-54R, PA-54R-5G wall mount
PAN-PA-PWR-R-AM-DC	Vehicle power supply for the PA-54R
PAN-PA-PWR-R-HV-DC	High-voltage power supply for PA-54R and PA-56R
PAN-PA-PWR-R-LV-DC	Low voltage (12–48 VDC): PA-54R and PA-56R
PAN-PWR-530W-54V-AC-B	AC power adapter for PA-54R and PA-56R

Table 7. PA-56R-POE-5G Series	
Part Number	**Details**
PAN-PA-56R-2-POST-RACK-MOUNT	PA-56R 2-post rack mount kit
PAN-PA-56R-ACC-LRG	Replacement accessory kit for PA-56R. The accessory kit is included in the system.
PAN-PA-56R-BOX-SET-LRG	PA-56R shipping boxes with packaging: Quantity 5
PAN-PA-56R-PKG-SET-LRG	PA-56R shipping boxes with packaging
PAN-PA-56R-WALL-MNT	PA-56R wall mount kit
PAN-PA-PWR-R-AM-DC	Vehicle power supply for PA-54R and PA-56R
PAN-PA-PWR-R-HV-DC	High-voltage power supply for PA-54R and PA-56R
PAN-PA-PWR-R-LV-DC	Low voltage (12–48 VDC): PA-54R and PA-56R
PAN-PWR-530W-54V-AC-B	AC power adapter for PA-54R and PA-56R

Forward-Looking Statements

This datasheet contains forward-looking statements that involve risks, uncertainties and assumptions, including, without limitation, statements regarding the benefits, impact, or performance or potential benefits, impact, or performance of our products and technologies or future products and technologies. These forward-looking statements are not guarantees of future performance, and a significant number of factors can cause actual results to differ materially from statements made in this datasheet. We identify certain important risks and uncertainties that could affect our results and performance in our most recent Annual Report on Form 10-K, our most recent Quarterly Report on Form 10-Q, and our other filings with the US Securities and Exchange Commission from time-to-time, each of which are available on our website at investors.paloaltonetworks.com and on the SEC's website at www.sec.gov. All forward-looking statements in this datasheet are based on information available to us as of the date hereof, and we do not assume any obligation to update the forward-looking statements provided to reflect events that occur or circumstances that exist after the date on which they were made.

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-50r-series-ruggedized-5g-enabled-ngfws_091726