STRATA™
BY PALO ALTO NETWORKS

PA-220R

Highlights

- 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.
- Dual DC power (12–48V).
- High availability firewall configuration (active/active and active/passive).
- Fanless design with no moving parts.
- Flexible I/O with support for both copper and optical via SFP ports.
- Flexible mounting options, including DIN rail, rack, and wall mount.
- Simplified remote site deployment via USB-based bootstrapping.

Palo Alto Networks PA-220R is a ruggedized ML-Powered Next-Generation Firewall that brings next-generation capabilities to industrial applications in harsh environments.

PA-220R

The PA-220R ruggedized appliance secures 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.

The controlling element of the PA-220R is PAN-OS®, which 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

Classifies all applications, on all ports, all the time

- Employs App-IDs for industrial protocols and applications, such as Modbus, DNP3, IEC 60870-5-104, Siemens S7, OSIsoft PI®, and more.
- Identifies the application, regardless of port, SSL/SSH encryption, or evasive technique employed.
- Uses the application, not the port, as the basis for all your safe enablement policy decisions: allow, deny, schedule, inspect, and apply traffic-shaping.
- Categorizes unidentified applications for policy control, threat forensics, or App-ID™ technology development.
- Provides full visibility into the details of all TLS-encrypted connections and stops threats hidden in encrypted traffic, including traffic that uses TLS 1.3 and HTTP/2 protocols.

Enforces security policies for any user, at any location

- Deploys consistent policies to local and remote users running on the Windows®, macOS®, Linux, Android®, or Apple iOS platforms.
- Enables agentless integration with Microsoft Active Directory® and Terminal Services, LDAP, Novell eDirectory™, and Citrix.
- Easily integrates your firewall policies with 802.1X wireless, proxies, network access control, and any other source of user identity information.

Extends native protection across all attack vectors with cloud-delivered security subscriptions

- **Threat Prevention**—inspects all traffic to automatically block known vulnerabilities, malware, vulnerability exploits, spyware, command and control (C2), and custom intrusion prevention system (IPS) signatures.
- **WildFire® malware prevention**—protects against unknown file-based threats, delivering automated prevention in seconds for most new threats across networks, endpoints, and clouds.
- **URL Filtering**—prevents access to malicious sites and protects users against web-based threats.
- **DNS Security**—detects and blocks known and unknown threats over DNS while predictive analytics disrupt attacks using DNS for C2 or data theft.
- **IoT Security**—discovers all unmanaged devices in your network, identifies risks and vulnerabilities, and automates enforcement policies for your Next-Generation Firewall using a new Device-ID™ policy construct.

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, natively integrated with our industry-leading security.
- Delivers an exceptional end user experience by minimizing latency, jitter, and packet loss.

Table 1: PA-220R Performance and Capacities[1]

Firewall throughput (HTTP/appmix)[2]	575/540 Mbps
Threat Prevention throughput (HTTP/appmix)[3]	275/320 Mbps
IPsec VPN throughput[4]	540 Mbps
Max sessions	64,000
New sessions per second[5]	4,300

1. Results were measured on PAN-OS 10.0.
2. Firewall throughput is measured with App-ID and logging enabled, using 64 KB HTTP/appmix transactions.
3. Threat Prevention throughput is measured with App-ID, IPS, antivirus, anti-spyware, WildFire, file blocking, and logging enabled, utilizing 64 KB HTTP/appmix transactions.
4. IPsec VPN throughput is measured with 64 KB HTTP transactions and logging enabled.
5. New sessions per second is measured with application-override utilizing 1 byte HTTP transactions.

The PA-220R supports a wide range of networking features that enable you to more easily integrate our security features into your existing network.

Table 2: PA-220R 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

Table 2: PA-220R Networking Features (continued)
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
802.1 Q VLAN tags per device/per interface: 4,094/4,094
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
High Availability
Modes: active/active, active/passive
Failure detection: path monitoring, interface monitoring
Industrial Protocols and Applications
paloaltonetworks.com/resources/whitepapers/app-ids-industrial-control-systems-scada-networks
Zero Touch Provisioning (ZTP)
Available with -ZTP SKUs (PA-220R-ZTP)
Requires Panorama 9.1.3 or higher

Table 3: PA-220R Hardware Specifications
I/O
10/100/1000 (6), SFP (2)
Management I/O
10/100/1000 out-of-band management port (1) RJ-45 console port (1) USB port (1) Micro USB console port (1)
Storage Capacity
32 GB EMMC

Table 3: PA-220R Hardware Specifications (continued)
Power Supply (Avg/Max Power Consumption)
Optional: dual redundant DC power feeds (13 W/16 W)
Max BTU/hr
55
Input Voltage (Input Frequency)
12–48 VDC 1.4 A
Max Current Consumption
Firewall – 1.4 A @ 12 VDC Max inrush current 4.9 A @ 12 VDC
Dimensions
2.0” H x 8.66” D x 9.25” W Flexible mounting options, including DIN rail, rack, and wall mount
Weight (Standalone Device/As Shipped)
4.5 lbs / 6.0 lbs
Safety
cTUVus, CB
EMI
FCC Class A, CE Class A, VCCI Class A
Certifications
IEC 61850-3 and IEEE 1613 environmental and testing standards. For more certifications, see paloaltonetworks.com/company/certifications.html.
Environment
Operating temperature: -40° to 158° F, -40° to 70° C Non-operating temperature: -40° to 167° F, -40° to 75° C Passive cooling

To learn more about the features and associated capacities of the PA-220R, please visit paloaltonetworks.com/network-security/next-generation-firewall/pa-220r.

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

pa-220r-ds-071020