PA-220R

Palo Alto Networks PA-220R ruggedized appliance brings next-generation capabilities to industrial applications in harsh environments.

Key Security 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.

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.

Prevents known and unknown threats

- Blocks a range of known general and ICS-specific threats—including exploits, malware, and spyware—across all ports, regardless of common evasion tactics employed.
- Limits the unauthorized transfer of files and sensitive data.
- Identifies unknown malware, analyzes it based on hundreds of malicious behaviors, and then automatically creates and delivers protection.

PA-220R

The PA-220R is a ruggedized next-generation firewall that 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.

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 (12–24V).
- 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 boot-strapping.

Performance and Capacities	PA-220R
Firewall throughput (HTTP/appmix)[1]	500/560 Mbps
Threat Prevention throughput (HTTP/appmix)[2]	150/260 Mbps
IPsec VPN throughput[3]	100 Mbps
Max sessions	64,000
New sessions per second[4]	4,200

1. Firewall throughput is measured with App-ID and logging enabled, using 64 KB HTTP/appmix transactions

2. Threat Prevention throughput is measured with App-ID, IPS, antivirus, anti-spyware, WildFire, file blocking, and logging enabled, utilizing 64 KB HTTP/appmix transactions

3. IPsec VPN throughput is measured with 64 KB HTTP transactions

4. 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.

Hardware Specifications

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
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
802.1 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
https://www.paloaltonetworks.com/resources/whitepapers/app-ids-industrial-control-systems-scada-networks

Networking Features

I/O
(6) 10/100/1000, (2) SFP
Management I/O
(1) 10/100/1000 out-of-band management port, (1) RJ-45 console port, (1) USB port, (1) Micro USB console port
Storage Capacity
32 GB EMMC
Power Supply (Avg/Max Power Consumption)
Dual DC power feeds (13 W/16 W)
Max BTU/hr
55
Input Voltage (Input Frequency)
12–24VDC 1.25A
Max Current Consumption
Firewall – 1.25A @ 12VDC Max inrush current 4.9A @ 12VDC
Rack Mount (Dimensions)
2.0” H x 8.66” D x 9.25” W Flexible mounting options including DIN rail, rack and wall mount
Weight (Stand-Alone Device/As Shipped)
4.5 lbs / 6.0 lbs
Safety
TUV CB report and TUV NRTL
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: https://www.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 www.paloaltonetworks.com/products.

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-020119