Corporate Armor For more information, please call 877.449.0458, or email us at Sales@CorporateArmor.com.

Shop Now

PA-220

Palo Alto Networks PA-220 brings next-generation firewall capabilities to distributed enterprise branch offices, retail locations and midsized businesses.

Key Security Features:

Classifies all applications, on all ports, all the time

- Identifies the application, regardless of port, encryption (SSL or SSH), or evasive technique employed
- Uses the application, not the port, as the basis for all of your safe enablement policy decisions: allow, deny, schedule, inspect and apply traffic-shaping
- Categorizes unidentified applications for policy control, threat forensics or App-ID™ application identification technology development

Enforces security policies for any user, at any location

- Deploys consistent policies to local and remote users running on the Windows®, Mac® OS X®, 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, NAC solutions, and any other source of user identity information

Prevents known and unknown threats

- Blocks a range of known threats, including exploits, malware and spyware, across all ports, regardless of common threat-evasion tactics employed
- Limits the unauthorized transfer of files and sensitive data, and safely enables non-work-related web surfing
- Identifies unknown malware, analyzes it based on hundreds of malicious behaviors, and then automatically creates and delivers protection

PA-220

The controlling element of the Palo Alto Networks® PA-220 is PAN-OS® security operating system, 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 business elements that run your business – are then used as the basis of your security policies, resulting in an improved security posture and a reduction in incident response time.

Highlights

- High availability with active/active and active/passive modes
- Redundant power input for increased reliability
- Fan-less design
- Simplified deployments of large numbers of firewalls through USB

Performance and Capacities[1]	PA-220
Firewall throughput (App-ID enabled)[2, 4]	500 Mbps
Threat prevention throughput[3, 4]	150 Mbps
IPsec VPN throughput[2, 4]	100 Mbps
New sessions per second[5]	4,200
Max sessions	64,000

[1] Performance and capacities are measured under ideal testing running PAN-OS 8.0

[2] Firewall and IPsec VPN throughput are measured with App-ID and User-ID features enabled

[3] Threat prevention throughput is measured with App-ID, User-ID, IPS, Antivirus and Anti-Spyware features enabled

[4] Throughput is measured with 64Kb HTTP transactions

[5] New sessions per second is measured with 4Kb HTTP transactions

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

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
Bidirectional Forwarding Detection (BFD)
IPv6
L2, L3, Tap, Virtual wire (transparent mode)
Features: App-ID, User-ID™, Content-ID™, WildFire™ and SSL
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
802.1q VLAN tags per device/per interface: 4,094/4,094
Network Address Translation (NAT)
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

Hardware Specifications

I/O
(8) 10/100/1000
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
32GB SSD
Power Supply (Avg/Max Power Consumption)
Dual redundant 40W (21W/25W)
Max BTU/hr
102 BTU
Input Voltage (Input Frequency)
100-240VAC (50-60Hz)
Max Current Consumption
Firewall—1.75A @ 12VDC Power supply (AC side)—0.5A @ 100VAC, 0.2A @ 240VAC
Dimensions
1.62”H X 6.29”D X 8.07”W
Weight (Stand-Alone Device/As Shipped)
3.0 lbs / 5.4 lbs
Safety
cCSAus, CB
EMI
FCC Class B, CE Class B, VCCI Class B
Certifications
See: https://www.paloaltonetworks.com/company/certifications.html
Environment
Operating temperature: 32° to 104° F, 0° to 40° C Non-operating temperature: -4° to 158° F, -20° to 70° C Passive cooling

To view additional information about the features and associated capacities of the PA-220, please visit www.paloaltonetworks.com/products.

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

© 2017 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at http://www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

pa-220-ds-021317