

# PA-220

Palo Alto Networks® PA-220 brings next-generation firewall capabilities to distributed enterprise branch offices, retail locations and midsize 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™ 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®, 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 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 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 PA-220 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 – 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	PA-220
Firewall throughput (App-ID enabled) <sup>1,3</sup>	500 Mbps
Threat Prevention throughput <sup>2,3</sup>	150 Mbps
IPsec VPN throughput <sup>1,3</sup>	100 Mbps
New sessions per second <sup>4</sup>	4,200
Max sessions	64,000

1. Firewall and IPsec VPN throughput are measured with App-ID and User-ID features enabled

2. Threat Prevention throughput is measured with App-ID, User-ID, IPS, antivirus and anti-spyware features enabled

3. Throughput is measured with 64KB HTTP transactions

4. 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

<b>Interface Modes</b>
L2, L3, tap, virtual wire (transparent mode)
<b>Routing</b>
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
<b>IPv6</b>
L2, L3, tap, virtual wire (transparent mode)
Features: App-ID, User-ID, Content-ID, WildFire and SSL decryption SLAAC
<b>IPsec VPN</b>
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
<b>VLANs</b>
802.1Q VLAN tags per device/per interface: 4,094/4,094
<b>Network Address Translation</b>
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
<b>High Availability</b>
Modes: active/active, active/passive
Failure detection: path monitoring, interface monitoring

## Hardware Specifications

<b>I/O</b>
(8) 10/100/1000
<b>Management I/O</b>
(1) 10/100/1000 out-of-band management port
(1) RJ-45 console port
(1) USB port
(1) Micro USB console port
<b>Storage Capacity</b>
32GB eMMC
<b>Power Supply (Avg/Max Power Consumption)</b>
Dual redundant 40 W (21 W / 25 W)
<b>Max BTU/hr</b>
102
<b>Input Voltage (Input Frequency)</b>
100–240VAC (50–60Hz)
<b>Max Current Consumption</b>
Firewall: 1.75A @ 12VDC
Power supply (AC side): 0.5A @ 100VAC, 0.2A @ 240VAC
<b>Dimensions</b>
1.62" H x 6.29" D x 8.07" W
<b>Weight (Stand-Alone Device/As Shipped)</b>
3.0 lbs / 5.4 lbs
<b>Safety</b>
cCSAus, CB
<b>EMI</b>
FCC Class B, CE Class B, VCCI Class B
<b>Certifications</b>
See <a href="https://www.paloaltonetworks.com/company/certifications.html">https://www.paloaltonetworks.com/company/certifications.html</a>
<b>Environment</b>
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](http://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](http://www.paloaltonetworks.com)

© 2018 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies. pa-220-ds-041018