STRATA™
BY PALO ALTO NETWORKS

PA-220

Palo Alto Networks PA-220 brings ML-Powered Next-Generation Firewall capabilities to distributed enterprise branch offices, retail locations, and midsize businesses.

Highlights

- World's first ML-Powered NGFW
- Eight-time Leader in the Gartner Magic Quadrant® for Network Firewalls
- Leader in The Forrester Wave™: Enterprise Firewalls, Q3 2020
- Highest Security Effectiveness score in the 2019 NSS Labs NGFW Test Report, with 100% of evasions blocked
- Extends visibility and security to all devices, including unmanaged IoT devices, without the need to deploy additional sensors
- Supports high availability with active/active and active/passive modes
- Delivers predictable performance with security services
- Features a silent, fanless design with an optional redundant power supply for branch and home offices
- Simplifies deployment of large numbers of firewalls with optional Zero Touch Provisioning (ZTP)

PA-220

The world's first ML-Powered NGFW enables you to prevent unknown threats, see and secure everything—including IoT—and reduce errors with automatic policy recommendations.

The controlling element of the PA-220 is PAN-OS®, the same software that runs all Palo Alto Networks Next-Generation Firewalls. PAN-OS 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 times.

Key Security and Connectivity Features

ML-Powered Next Generation Firewall

- Embeds machine learning (ML) in the core of the firewall to provide inline signatureless attack prevention for file-based attacks while identifying and immediately stopping never-before-seen phishing attempts.
- Leverages cloud-based ML processes to push zero-delay signatures and instructions back to the NGFW.
- Uses behavioral analysis to detect internet of things (IoT) devices and make policy recommendations; cloud-delivered and natively integrated service on the NGFW.
- Automates policy recommendations that save time and reduce the chance of human error.

Identifies and categorizes all applications, on all ports, all the time, with full Layer 7 inspection

- Identifies the applications traversing your network irrespective of port, protocol, evasive techniques, or encryption (TLS/SSL).
- Uses the application, not the port, as the basis for all your safe enablement policy decisions: allow, deny, schedule, inspect, and apply traffic-shaping.
- Offers the ability to create custom App-IDs for proprietary applications or request App-ID development for new applications from Palo Alto Networks.
- Identifies all payload data within the application, such as files and data patterns, to block malicious files and thwart data exfiltration attempts.
- Creates standard and customized application usage reports, including software-as-a-service (SaaS) reports that provide insight into all SaaS traffic—sanctioned and unsanctioned—on your network.
- Enables safe migration of legacy Layer 4 rule sets to App-ID-based rules with built-in Policy Optimizer, giving you a rule set that is more secure and easier to manage.

Enforces security for users at any location, on any device, while adapting policy in response to user activity

- Enables visibility, security policies, reporting, and forensics based on users and groups—not just IP addresses.
- Easily integrates with a wide range of repositories to leverage user information: wireless LAN controllers, VPNs, directory servers, SIEMs, proxies, and more.
- Allows you to define Dynamic User Groups (DUGs) on the firewall to take time-bound security actions without waiting for changes to be applied to user directories.
- Applies consistent policies irrespective of users' locations (office, home, travel, etc.) and devices (iOS and Android® mobile devices, macOS®, Windows®, Linux desktops, laptops; Citrix and Microsoft VDI and Terminal Servers).
- Prevents corporate credentials from leaking to third-party websites, and prevents reuse of stolen credentials by enabling multi-factor authentication (MFA) at the network layer for any application, without any application changes.
- Provides dynamic security actions based on user behavior to restrict suspicious or malicious users.

Prevents malicious activity concealed in encrypted traffic

- Inspects and applies policy to TLS/SSL-encrypted traffic, both inbound and outbound, including for traffic that uses TLS 1.3 and HTTP/2.
- Offers rich visibility into TLS traffic, such as amount of encrypted traffic, TLS/SSL versions, cipher suites, and more, without decrypting.
- Enables control over use of legacy TLS protocols, insecure ciphers, and incorrectly configured certs to mitigate risks.
- Facilitates easy deployment of decryption and lets you use built-in logs to troubleshoot issues, such as applications with pinned certs.
- Lets you enable or disable decryption flexibly based on URL category and source and destination zone, address, user, user group, device, and port, for privacy and regulatory compliance purposes.
- Allows you to create a copy of decrypted traffic from the firewall (i.e., decryption mirroring) and send it to traffic collection tools for forensics, historical purposes, or data loss prevention (DLP).

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**—unifies inline machine learning protection with robust cloud-based analysis to instantly prevent new threats in real time as well as discover and remediate evasive threats faster than ever.
- **URL Filtering**—prevents access to malicious sites and protects users against web-based threats, including credential phishing attacks.
- **DNS Security**—detects and blocks known and unknown threats over DNS (including data exfiltration via DNS tunneling), prevents attackers from bypassing security measures, and eliminates the need for independent tools or changes to DNS routing.
- **IoT Security**—discovers all unmanaged devices in your network quickly and accurately with ML, without the need to deploy additional sensors. Identifies risks and vulnerabilities, prevents known and unknown threats, provides risk-based policy recommendations, and automates enforcement.

Delivers a unique approach to packet processing with Single-Pass Architecture

- Performs networking, policy lookup, application and decoding, and signature matching—for any and all threats and content—in a single pass. This significantly reduces the amount of processing overhead required to perform multiple functions in one security device.
- Enables consistent and predictable performance when security subscriptions are enabled.
- Avoids introducing latency by scanning traffic for all signatures in a single pass, using stream-based, uniform signature matching.

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

Table 1: PA-220 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-220 supports a wide range of networking features that enable you to more easily integrate our security features into your existing network.

Table 2: PA-220 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

Table 2: PA-220 Networking Features (continued)
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
802.1Q 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
Zero Touch Provisioning (ZTP)
Available with -ZTP SKUs (PA-220-ZTP)
Requires Panorama 9.1.3 or higher

Table 3: PA-220 Hardware Specifications
I/O
10/100/1000 (8)
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
Power Supply (Avg/Max Power Consumption)
Optional: dual redundant 40 W (21 W / 25 W)
102
Input Voltage (Input Frequency)
100–240 VAC (50–60Hz)
Max Current Consumption
Firewall: 1.75 A @ 12 VDC Power supply (AC side): 1.5A

Table 3: PA-220 Hardware Specifications (continued)
Dimensions
1.62” H x 6.29” D x 8.07” W
Weight (Standalone Device/As Shipped)
3.0 lbs / 5.4 lbs
Safety
cTUVus, CB
EMI
FCC Class B, CE Class B, VCCI Class B
Certifications
See 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 learn more about the features and associated capacities of the PA-220, please visit paloaltonetworks.com/network-security/next-generation-firewall/pa-220.

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-220-ds-092920