



**Firewalls.com**  
Find It At [Firewalls.com](https://www.firewalls.com)

VISIT



## 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
- Simplifies deployment of large numbers of firewalls with optional Zero Touch Provisioning (ZTP)

# PA-3200 Series

Palo Alto Networks PA-3200 Series ML-Powered NGFWs—comprising the PA-3260, PA-3250, and PA-3220—target high-speed internet gateway deployments. PA-3200 Series appliances secure all traffic, including encrypted traffic, using dedicated processing and memory for networking, security, threat prevention, and management.



PA-3260



PA-3250



PA-3220

The controlling element of the PA-3200 Series 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 time.

## 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-3200 Series Performance and Capacities**

	PA-3260	PA-3250	PA-3220
Firewall throughput (HTTP/appmix)*	8.3/9.2 Gbps	5.6/6.2 Gbps	4.5/5.0 Gbps
Threat Prevention throughput (HTTP/appmix)†	4.1/5.0 Gbps	2.7/3.4 Gbps	2.2/2.8 Gbps
IPsec VPN throughput‡	5.0 Gbps	3.2 Gbps	2.8 Gbps
Max sessions	3M	2M	1M
New sessions per second§	105,000	73,000	57,000
Virtual systems (base/max)	1/6	1/6	1/6

Note: Results were measured on PAN-OS 10.0.

\* Firewall throughput is measured with App-ID and logging enabled, utilizing 64 KB HTTP/appmix transactions.

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

‡ IPsec VPN throughput is measured with 64 KB HTTP transactions and logging enabled.

§ New sessions per second is measured with application-override, utilizing 1 byte HTTP transactions.

|| Adding virtual systems over base quantity requires a separately purchased license.

**Table 2: PA-3200 Series 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
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

**Table 2: PA-3200 Series Networking Features (cont.)**

VLANs
802.1Q VLAN tags per device/per interface: 4,094/4,094
Aggregate interfaces (802.3ad), LACP
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, HA clustering
Failure detection: path monitoring, interface monitoring
Zero Touch Provisioning (ZTP)
Available with -ZTP SKUs (PA-3260-ZTP, PA-3250-ZTP, PA-3220-ZTP)
Requires Panorama 9.1.3 or higher

**Table 3: PA-3200 Series Hardware Specifications**

I/O
PA-3260: 10/100/1000 (12), 1G/10G SFP/SFP+ (8), 40G QSFP+ (4)
PA-3250: 10/100/1000 (12), 1G/10G SFP/SFP+ (8)
PA-3220: 10/100/1000 (12), 1G SFP (4), 1G/10G SFP/SFP+ (4)
Management I/O
10/100/1000 out-of-band management port (1), 10/100/1000 high availability (2), 10G SFP+ high availability (1), RJ-45 console port (1), Micro USB (1)
Storage Capacity
240 GB SSD
Power Supply (Avg/Max Power Consumption)
Redundant 650-watt AC or DC (180/240)
Max BTU/hr
819
Input Voltage (Input Frequency)
AC: 100–240 VAC (50/60Hz)
DC: -48 V @ 4.7 A, -60 V @ 3.8 A
Max Current Consumption
AC: 2.3 A @ 100 VAC, 1.0 A @ 240 VAC
DC: -48 V @ 4.7 A, -60 V @ 3.8 A
Mean Time Between Failure (MTBF)
14 years

**Table 3: PA-3200 Series Hardware Specs. (cont.)**

Rack Mount Dimensions
2U, 19" standard rack (3.5" H x 20.53" D x 17.34" W)
Weight (Standalone Device/As Shipped)
29 lbs / 41.5 lbs
Safety
cTUVus, CB
EMI
FCC Class A, CE Class A, VCCI Class A
Certifications
See <a href="https://paloaltonetworks.com/company/certifications.html">paloaltonetworks.com/company/certifications.html</a>
Environment
Operating temperature: 32° to 122° F, 0° to 50° C
Non-operating temperature: -4° to 158° F, -20° to 70° C
Humidity tolerance: 10% to 90%
Maximum altitude: 10,000 ft / 3,048 m
Airflow: front to back

To view additional information about the features and associated capacities of the PA-3200 Series, please visit [paloaltonetworks.com/network-security/next-generation-firewall/pa-3200-series](https://paloaltonetworks.com/network-security/next-generation-firewall/pa-3200-series).

**View More Datasheets**