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.

Highlights

- World's first ML-Powered NGFW
- Eleven-time Leader in the Gartner Magic Quadrant for Network Firewalls
- Leader in The Forrester Wave: Enterprise Firewalls, Q4 2022
- Delivers 5G-Native Security built to safeguard service provider and enterprise 5G transformation and multi-access edge computing (MEC)
- 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
- Supports centralized administration with Panorama network security management
- Maximizes security investments and prevents business disruptions with Strata™ Cloud Manager

The controlling element of the PA-3200 Series is PAN-OS®, the same software that runs all Palo Alto Networks Next-Generation Firewalls (NGFWs). 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 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). In addition, it automatically discovers and controls new applications to keep pace with the SaaS explosion with SaaS Security subscription.
- 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-ID™ tags for proprietary applications or request App-ID development for new applications from Palo Alto Networks.
- Identifies all payload data within the application (e.g., 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 sanctioned and unsanctioned SaaS traffic 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.

Check out the App-ID tech brief for more information.

Enforces Security for Users at Any Location, on Any Device, While Adapting Policy Based on 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, and Linux desktops and 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 multifactor 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.
- Consistently authenticates and authorizes your users, regardless of location and where user identity stores live, to move quickly toward a Zero Trust security posture with Cloud Identity Engine—an entirely new cloud-based architecture for identity-based security.

Check out the Cloud Identity Engine solution brief for more information.

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 misconfigured certificates to mitigate risks.
- Facilitates easy deployment of decryption and lets you use built-in logs to troubleshoot issues, such as applications with pinned certificates.
- Lets you enable or disable decryption flexibly based on URL category, 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).
- Allows you to intelligently forward all traffic (decrypted TLS, undecrypted TLS, and non-TLS) to third-party security tools with network packet broker and optimize your network performance and reduce operating expenses.

Refer to this decryption whitepaper to learn where, when, and how to decrypt to prevent threats and secure your business.

Offers AI-Powered Unified Management and Operations with Strata Cloud Manager

- **Prevent network disruptions**: Forecast deployment health and proactively identify capacity bottlenecks up to seven days in advance with predictive analytics to proactively prevent operational disruptions.
- **Strengthen security in real time**: AI-powered analysis of policies and real-time compliance checks against industry and Palo Alto Networks best practices.
- **Enable simple and consistent network security management and ops**: Manage configuration and security policies across all form factors, including SASE, hardware and software firewalls, and all security services to ensure consistency and reduce operational overhead.

Detects and Prevents Advanced Threats with Cloud-Delivered Security Services

The traditional approach of using siloed security tools causes challenges for organizations, including security gaps, increased overhead for security teams, and disruptions in business productivity. Seamlessly integrated with our industry-leading NGFWs, our Cloud-Delivered Security Services share threat intelligence across 65,000 customers in order to prevent known and unknown threats across all threat vectors in real time. Eliminate security gaps in your entire network and take advantage of inline AI-powered security services that provide real-time protection everywhere.

Services include:

- **Advanced Threat Prevention**: Stop known and unknown exploits and command-and-control (C2) attacks with inline AI-powered detections, stopping 60% more zero-day injection attacks and 48% more highly evasive command-and-control traffic than traditional IPS solutions.
- **Advanced WildFire®**: Ensure files are safe by automatically preventing known, unknown, and highly evasive malware 180X faster than competitors with the industry's largest threat intelligence and malware prevention engine.
- **Advanced URL Filtering**: Ensure safe access to the internet and prevent 40% more web-based attacks with the industry's first real-time prevention of known and unknown threats, stopping 88% of malicious sites at least 48 hours before other vendors.
- **DNS Security**: Gain 68% more threat coverage and stop 85% of malware that abuses DNS for command and control and data theft without requiring changes to your infrastructure.
- **Enterprise DLP**: Minimize risk of a data breach, stop out-of-policy data transfers, and enable compliance consistently across your enterprise, with 2X greater coverage of any cloud-delivered enterprise DLP.
- **SaaS Security**: Stay ahead of the SaaS explosion with the industry's only Next-Generation CASB to automatically see and secure all apps across all protocols.
- **IoT Security**: Safeguard every "thing" and implement Zero Trust device security 20X faster, with the industry's smartest security for smart devices.

Delivers a Unique Approach to Packet Processing with Single-Pass Architecture

- Performs networking, policy lookup, application and decoding, and signature matching—for 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.
- Avoids introducing latency by scanning traffic for all signatures in a single pass, using stream-based, uniform signature matching.
- Enables consistent and predictable performance when security subscriptions are enabled. (In table 1, "Threat Prevention throughput" is measured with multiple subscriptions enabled.)

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-3220	PA-3250	PA-3260
Firewall throughput (appmix)*	4 Gbps	5 Gbps	7.5 Gbps
Threat Prevention throughput (appmix)†	2.2 Gbps	2.5 Gbps	4 Gbps
IPsec VPN throughput‡	2.4 Gbps	2.6 Gbps	4.4 Gbps
Max concurrent sessions§	1M	2M	2.2M
New sessions per second‖	46,000	58,000	84,000
Virtual systems (base/max)#	1/6	1/6	1/6

Note: Results were measured on PAN-OS 11.1.

* Firewall throughput is measured with App-ID and logging enabled, utilizing appmix transactions.

† Threat Prevention throughput is measured with App-ID, IPS, antivirus, antispyware, WildFire, DNS Security, file blocking, and logging enabled, utilizing appmix transactions.

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

§ Max concurrent sessions are measured utilizing HTTP transactions.

‖ 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 and SSL 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
GlobalProtect Large Scale VPN for simplified configuration and management*
Secure access over IPsec and SSL VPN tunnels using GlobalProtect gateway and portals*
VLANs
802.1Q VLAN tags per device/per interface: 4,094/4,094
Aggregate interfaces (802.3ad), LACP

Table 2: PA-3200 Series Networking Features (continued)
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

* Requires GlobalProtect license.

Table 3: PA-3200 Series Hardware Specifications
I/O
PA-3220: 10/100/1000 (12), 1G SFP (4), 1G/10G SFP/SFP+ (4)
PA-3250: 10/100/1000 (12), 1G/10G SFP/SFP+ (8)
PA-3260: 10/100/1000 (12), 1G/10G SFP/SFP+ (8), 40G QSFP+ (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 (195/240)
Max BTU/hr
819
Input Voltage (Input Frequency)
AC: 100–240 VAC (50–60Hz)
DC: -48V to -60V
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
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

Table 3: PA-3200 Series Hardware Specifications (continued)
EMI
FCC Class A, CE Class A, VCCI Class A
Certifications
See paloaltonetworks.com/company/certifications.html
Environment
Operating temperature: 32°F to 122°F, 0°C to 50°C
Nonoperating temperature: -4°F to 158°F, -20°C to 70°C
Humidity tolerance: 10% to 90%
Maximum altitude: 10,000 ft / 3,048 m
Airflow: front to back

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

strata_ds_pa-3200-series_012524