PA-3200 SERIES

Palo Alto Networks PA-3200 Series next-generation firewalls—comprising the PA-3260, PA-3250, and PA-3220—are targeted at 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.

Key Security Features

Classifies all applications, on all ports, all the time

- Identifies the application, regardless of port, SSL/SSH encryption, or evasive technique employed.
- Uses the application, not the port, as the basis for all 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 Windows®, 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, 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-3260

PA-3250

PA-3220

The controlling element of the PA-3200 Series 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—then serve as the basis of your security policies, resulting in improved security posture and reduced incident response time.

Performance and Capacities	PA-3260	PA-3250	PA-3220
Firewall throughput (HTTP/appmix)[1]	8.4/10 Gbps	6/7 Gbps	4.6/4.6 Gbps
Threat Prevention throughput (HTTP/appmix)[2]	3.9/4.7 Gbps	2.6/3.1 Gbps	2.2/2.6 Gbps
IPsec VPN throughput[3]	4.8 Gbps	3.2 Gbps	2.5 Gbps
Max sessions	3,000,000	2,000,000	1,000,000
New sessions per second[4]	118,000	84,000	57,000
Virtual systems (base/max)[5]	1/6	1/6	1/6

1. Firewall throughput is measured with App-ID and logging enabled using 64 KB HTTP/appmix transactions
2. Threat Prevention throughput is measured with App-ID, IPS, antivirus, anti-spyware, WildFire, and logging enabled, utilizing 64 KB HTTP/appmix transactions
3. IPsec VPN throughput is measured with 64 KB HTTP transactions
4. New sessions per second measured with application-override utilizing 1 byte HTTP transactions
5. Adding virtual systems over base quantity requires a separately purchased license

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 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
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
Failure detection: path monitoring, interface monitoring

To view additional information about the features and associated capacities of the PA-3200 Series, please visit www.paloaltonetworks.com/products.

Hardware Specifications

I/O
PA-3260: (12) 10/100/1000, (8) 1G/10G SFP/SFP+, (4) 40G QSFP+
PA-3250: (12) 10/100/1000, (8) 1G/10G SFP/SFP+
PA-3220: (12) 10/100/1000, (4) 1G SFP, (4) 1G/10G SFP/SFP+
Management I/O
(1) 10/100/1000 out-of-band management port, (2) 10/100/1000 high availability, (1) 10G SFP+ high availability, (1) RJ-45 console port, (1) Micro USB
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: 100–240VAC (50–60 Hz)
DC: -48V @ 4.7A, -60V @ 3.8A
Max Current Consumption
AC: 2.3A @ 100VAC, 1.0A @ 240VAC
DC:-48V @ 4.7A, -60V @ 3.8A
Rack Mountable (Dimensions)
2U, 19” standard rack (3.5” H x 20.53” D x 17.34” W)
Weight (Stand-Alone Device/As Shipped)
29 lbs / 41.5 lbs
Safety
TUV CB report and TUV NRTL
EMI
FCC Class A, CE Class A, VCCI Class A
Certifications
See https://www.paloaltonetworks.com/company/certifications.html
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: 10,000ft / 3,048m
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