

PA-5200 Series

Palo Alto Networks PA-5200 Series ML-Powered NGFWs—the PA-5280, PA-5260, PA-5250, and PA-5220—are ideal for high-speed data center, internet gateway, and service provider deployments. The PA-5200 Series delivers up to 64 Gbps of throughput, using dedicated processing and memory, for the key functional areas of networking, security, threat prevention, and management.



PA-5260

The controlling element of the PA-5200 ML-Powered Next-Generation Firewalls (NGFW) 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.

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.
- Provides full visibility into the details of all TLS-encrypted connections and stops threats hidden in encrypted traffic, including traffic that uses TLS 1.3 and HTTP/2 protocols.

Enforces security policies for any user, anywhere

- Deploys consistent policies to local and remote users running on the 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.

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**—protects against unknown file-based threats, delivering automated prevention in seconds for most new threats across networks, endpoints, and clouds.
- **URL Filtering**—prevents access to malicious sites and protects users against web-based threats.
- **DNS Security**—detects and blocks known and unknown threats over DNS while predictive analytics disrupt attacks using DNS for C2 or data theft.
- **IoT Security**—discovers all unmanaged devices in your network, identifies risks and vulnerabilities, and automates enforcement policies for your ML-Powered NGFW using a new Device-ID™ policy construct.

Table 1: PA-5200 Series Performance and Capacities¹

	PA-5280	PA-5260	PA-5250	PA-5220
Firewall throughput (HTTP/appmix) ²	56/64 Gbps	56/64 Gbps	38/40 Gbps	15.6/20 Gbps
Threat Prevention throughput (HTTP/appmix) ³	26/31.5 Gbps	26/31.5 Gbps	17/21 Gbps	7.2/8.9 Gbps
IPsec VPN throughput ⁴	27 Gbps	27 Gbps	18 Gbps	10 Gbps
Max sessions	64M	32M	8M	4M
New sessions per second ⁵	450,000	450,000	297,000	133,000
Virtual systems (base/max) ⁶	25/225	25/225	25/125	10/20

1. Results were measured on PAN-OS 9.1.

2. Firewall throughput is measured with App-ID and logging enabled, utilizing 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.

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

Table 2: PA-5200 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) and DHCP supported for dynamic address assignment
Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, and v3
Bidirectional Forwarding Detection (BFD)

Table 2: PA-5200 Series Networking Features (continued)

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

Table 2: PA-5200 Series Networking Features (continued)

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
GlobalProtect large-scale VPN for simplified configuration and management
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
Mobile Network Infrastructure
GTP Security
SCTP Security

Table 3: PA-5200 Series Hardware Specifications

I/O
PA-5280 / PA-5260 / PA-5250: 100/1000/10G Cu (4), 1G/10G SFP/ SFP+ (16), 40G/100G QSFP28 (4)
PA-5220: 100/1000/10G Cu (4), 1G/10G SFP/SFP+ (16), 40G QSFP+ (4)
Management I/O
PA-5280 / PA-5260 / PA-5250: 10/100/1000 (2), 40G/100G QSFP28 HA (1), 10/100/1000 out-of-band management (1), RJ45 console port (1)
PA-5220: 10/100/1000 (2), 40G QSFP+ HA (1), 10/100/1000 out-of-band management (1), RJ45 console port (1)

Table 3: PA-5200 Series Hardware Specs. (cont.)

Storage Capacity
240 GB SSD, RAID1, system storage 2 TB HDD, RAID1, log storage
Power Supply (Avg/Max Power Consumption)
571/685 W
Max BTU/hr
2,340
Power Supplies (Base/Max)
1:1 fully redundant (2/2)
AC Input Voltage (Input Hz)
100–240 VAC (50–60 Hz)
AC Power Supply Output
1,200 watts/power supply
Max Current Consumption
AC: 8.5 A @ 100 VAC, 3.6 A @ 240 VAC DC: 19 A @ -40 VDC, 12.7 A @ -60 VDC
Max Inrush Current
AC: 50 A @ 230 VAC, 50 A @ 120 VAC DC: 200 A @ 72 VDC
DC: 200 A @ 72 VDC
9.23 years
Rack Mount (Dimensions)
3U, 19" standard rack 5.25" H x 20.5" D x 17.25" W
Weight (Standalone Device/As Shipped)
46 lbs / 62 lbs
Safety
cCSAus, CB IEC 60950-1
EMI
FCC Class A, CE Class A, VCCI Class A
Certifications
See https://www.paloaltonetworks.com/services/education/certification
Environment
Operating temperature: 32° to 122° F, 0° to 50° C Non-operating temperature: -4° to 158° F, -20° to 70° C