

PA-500

The PA-500 is a next-generation firewall that delivers unprecedented visibility and control over applications, users and content on enterprise networks.

APPLICATION IDENTIFICATION:

- Identifies and controls applications irrespective of port, protocol, encryption (SSL or SSH) or evasive tactic employed.
- Enables positive enforcement application usage policies: allow, deny, schedule, inspect, apply traffic shaping.
- Graphical visibility tools enable simple and intuitive view into application traffic.

USER IDENTIFICATION:

- Policy-based visibility and control over who is using the applications through seamless integration with Active Directory, LDAP, and eDirectory.
- Identifies Citrix, Microsoft Terminal Services and XenWorks users, enabling visibility and control over their respective application usage.
- Control non-Windows hosts via web-based authentication.

CONTENT IDENTIFICATION:

- Block viruses, spyware, and vulnerability exploits, limit unauthorized transfer of files and sensitive data such as CC# or SSN, and control non-work related web surfing.
- Single pass software architecture enables multi-gigabit throughput with low latency while scanning content.



PA-500

The Palo Alto Networks™ PA-500 is targeted at high speed Internet gateway deployments for enterprise branch offices and medium size businesses. The PA-500 manages network traffic flows using dedicated computing resources for networking, security, threat prevention and management.

A high speed backplane smoothes the pathway between processors and the separation of data and control plane ensures that management access is always available, irrespective of the traffic load. The controlling element of the PA-500 Series next-generation firewalls is PAN-OS™, a security-specific operating system that tightly integrates three unique identification technologies: App-ID™, User-ID and Content-ID, with key firewall, networking and management features.

KEY PERFORMANCE SPECIFICATIONS ¹	PA-500
Firewall throughput	250 Mbps
Threat prevention throughput	100 Mbps
IPSec VPN throughput	50 Mbps
New sessions per second	7,500
Max sessions	64,000
IPSec VPN tunnels/tunnel interfaces	250
SSL VPN users	100
Virtual routers	3
Virtual systems	Not supported
Security Zones	20
Max number of policies	1,000

¹ Performance and capacity listed above are based on systems running PAN-OS 4.0 and are measured under ideal testing conditions.

Additional PA-500 Features and Specifications

HARDWARE SPECIFICATIONS

I/O	(8) 10/100/1000
Management I/O	(1) 10/100/1000 out-of-band management port, (1) RJ-45 console port
Power supply (Avg/max power consumption)	180W (10W/75W)
Input voltage (Input frequency)	100-240Vac (50-60Hz)
Max current consumption	1A@100Vac
Mean time between failure (MTBF)	10.16 years
Max inrush current	110A@230Vac; 51A@115Vac
Rack mountable (Dimensions)	1U, 19" standard rack (1.75"H x 10"D x 17"W)
Weight (Stand alone device/As shipped)	8lbs/13lbs
Safety	UL, CUL, CB
EMI	FCC Class A, CE Class A, VCCI Class A, TUV

ENVIRONMENT

Operating temperature	32° to 122° F, 0° to 50° C
Non-operating temperature	-4° to 158° F, -20° to 70° C

NETWORKING**PA-500**

• Interface Modes	L2, L3, Tap, Virtual Wire (transparent mode)
Routing	
• Modes	OSPF, RIP, BGP, Static
• Forwarding table size (entries per device/per VR)	1,250 / 1,250
• Policy-based forwarding	Supported
• Point-to-Point Protocol over Ethernet (PPPoE)	Supported
High Availability	
• Modes	Active/Active Active/Passive
• Failure Detection	Path Monitoring, Interface Monitoring
NAT/PAT	
• Max NAT rules	125
• Max NAT rules (DIPP)	125
• Dynamic IP and port pool	254
• Dynamic IP pool	16,234
• NAT Modes	1:1 NAT, n:n NAT, m:n NAT
• PAT- Unique destination IPs per source port and IP	1
VLANs	
• 802.1q VLAN tags per device	4,094
• 802.1q VLAN tags per physical interface	4,094
• Max interfaces	250
• Aggregate Interfaces (802.3ad)	Not Supported
Virtual Wire	
• Max virtual wires (VW)	4
• Physical interfaces mapped to VWs	Supported
Address Assignment	
• Captive Portal for Management Interface	Supported
• DHCP server/DHCP relay	up to 3 servers
• Max Addresses	64,000
IPv6	
• Modes	L2, L3, Tap, Virtual Wire (transparent mode)
• Services	App-ID, User-ID, Content-ID and SSL Decryption
L2 Forwarding	
• ARP table size/device	500
• IPv6 neighbor table size	500
• MAC table size/device	500

SECURITY

FIREWALL

- Policy-based control over applications, users and content
- Fragmented packet protection
- Reconnaissance scan protection
- Denial of Service (DoS)/Distributed Denial of Services (DDoS) protection
- Decryption: SSL (inbound and outbound), SSH

USER INTEGRATION (USER-ID)

- Active Directory, LDAP, eDirectory, Citrix and Microsoft Terminal Services, Xenworks, XML API

IPSEC VPN (SITE-TO-SITE)

- Key Exchange: Manual key, IKE v1
- Encryption: 3DES, AES (128-bit, 192-bit, 256-bit)
- Authentication: SHA1, MD5

DATA FILTERING

- Control unauthorized data transfer (data patterns and file types)
- Drive-by download protection

MANAGEMENT, REPORTING, VISIBILITY TOOLS

- Integrated web interface, CLI or central management (Panorama)
- Syslog, SNMPv2 and SNMPv3
- XML-based REST API
- Graphical summary of applications, URL categories, threats and data (ACC)
- View, filter, export traffic, threat, URL, and data filtering logs
- Fully customizable reporting

NETCONNECT SSL VPN (REMOTE ACCESS)

- Transport: IPSec with SSL fall-back
- Authentication: LDAP, SecurID, or local DB
- Client OS: Macintosh, Windows XP, Windows Vista (32 and 64 bit), Windows 7 (32 and 64 bit)

THREAT PREVENTION (SUBSCRIPTION REQUIRED)

- Application, operating system vulnerability exploit protection
- Stream-based protection against viruses (including those embedded in HTML, Javascript, PDF and compressed), spyware, worms

QUALITY OF SERVICE (QOS)

- Policy-based traffic shaping by application, user, source, destination, interface, IPSec VPN tunnel and more
- 8 traffic classes with guaranteed, maximum and priority bandwidth parameters
- Real-time bandwidth monitor
- Per policy diffserv marking

GLOBALPROTECT

- GlobalProtect Gateway
- GlobalProtect Portal
- Client OS: Windows XP, Windows Vista (32/64 bit), Windows 7 (32 bit)

URL FILTERING (SUBSCRIPTION REQUIRED)

- 76-category, 20M URL on-box database
- Dynamic URL filtering (1M URL cache on device)
- Custom block pages and URL categories

ORDERING INFORMATION

PA-500

Platform

PAN-PA-500

For additional information on the PA-500 next-generation firewall feature set, please visit www.paloaltonetworks.com/literature.