

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 more than 800 applications irrespective of port, protocol, SSL encryption 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.
- Identifies Citrix and Microsoft Terminal Services 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. Interface density for the PA-500 includes (8) 10/100/1000 traffic interfaces and a dedicated out-of-band management interface.

The controlling element of the PA-500 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	PA-500
Firewall throughput	250 Mbps
Threat prevention throughput	100 Mbps
IPSec VPN throughput	50 Mbps
IPSec VPN tunnels/tunnel interfaces	250
SSL VPN Users	100
New sessions per second	7,500
Max sessions	64,000

For a complete description of the PA-500 next-generation firewall feature set, please visit www.paloaltonetworks.com/literature.

Additional PA-500 Specifications

APP-ID

- Identifies and controls more than 800 applications
- SSL decryption via forward or reverse proxy
- Customize application properties
- Custom HTTP applications

FIREWALL

- Policy-based control by application, application category, subcategory, technology, risk factor or characteristic
- Policy-based control by user, group or IP address
- Maximum number of policies: 1,000
- Reconnaissance scan protection
- Denial of Service (DoS) protection
- Fragmented packet protection

DATA FILTERING

- Detect and block social security numbers, credit card numbers, custom data patterns
- Block files by type

THREAT PREVENTION (SUBSCRIPTION REQUIRED)

- Block viruses, spyware, worms and vulnerability exploits

IPSEC VPN (SITE-TO-SITE)

- Manual Key, IKE v1
- 3DES, AES (128-bit, 192-bit, 256-bit) encryption
- SHA1, MD5 authentication

SSL VPN (REMOTE ACCESS)

- IPSec transport with SSL fall-back
- Enforce unique policies for SSL VPN traffic
- Enable/disable split tunneling to control client access

NETWORKING

- Tap mode, virtual wire, layer 2, layer 3, mixed L2/L3
- IPv6 application visibility and control via Content-ID (Virtual wire mode only)
- IPv6 full content inspection via Content-ID (Virtual wire mode only)
- 802.1Q VLAN tagging (layer 2, layer 3)
- Network address translation (NAT)
- OSPF and RIPv2
- DHCP server/ DHCP relay (up to 3 servers)
- Virtual routers: 2
- Security zones: 20

URL FILTERING (SUBSCRIPTION REQUIRED)

- 76-category on-box customizable database
- Customizable allow and block lists
- Customizable block pages

QUALITY OF SERVICE (QOS)

- Policy-based traffic shaping (guaranteed, maximum and priority) by application, user, source, destination, interface, IPSec VPN tunnel and more
- Per policy diffserv marking

HIGH AVAILABILITY

- Active/Passive
- Configuration and session synchronization
- Interface and IP tracking
- Link and path failure monitoring

MANAGEMENT TOOLS

- Integrated web interface
- Command line interface (CLI)
- Centralized management (Panorama)
- Role-based administration
- Shared policies (Panorama)
- Syslog & SNMPv2
- Customizable administrator login banner
- XML-based REST API

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 (40W/75W)
Input voltage (Input frequency)	100-240Vac (50-60Hz)
Max input current	110A@230Vac; 1A@115Vac
Rack mountable (Dimensions)	1U, 19" standard rack (1.75"H x 10"D x 17"W)
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

ORDERING INFORMATION**PA-500**

Platform	PAN-PA-500
Annual threat prevention subscription	PAN-PA-500-TP
Annual URL filtering subscription	PAN-PA-500-URL2

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



Palo Alto Networks
 232 E. Java Drive
 Sunnyvale, CA. 94089
 Sales 866.207.0077
www.paloaltonetworks.com

Copyright © 2009, Palo Alto Networks, Inc. All rights reserved. Palo Alto Networks, the Palo Alto Networks Logo, PAN-OS, App-ID and Panorama are trademarks of Palo Alto Networks, Inc. All specifications are subject to change without notice. Palo Alto Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Palo Alto Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. PAN-OS 3.0, June 2009.

840-000009-00A