

PA-5000 Series

The PA-5000 Series 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-5060



PA-5050



PA-5020

The Palo Alto Networks™ PA-5000 Series is comprised of three high performance platforms, the PA-5020, the PA-5050 and the PA-5060, all of which are targeted at high speed Internet gateway and datacenter deployments. The PA-5000 Series manages multi-Gbps traffic flows using dedicated processing and memory for networking, security, threat prevention and management.

A 20 Gbps backplane smoothes the pathway between dedicated processors, and the physical separation of data and control plane ensures that management access is always available, irrespective of the traffic load.

The controlling element of the PA-5000 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-5060	PA-5050	PA-5020
Firewall throughput	20 Gbps	10 Gbps	5 Gbps
Threat prevention throughput	10 Gbps	5 Gbps	2 Gbps
IPSec VPN throughput	4 Gbps	4 Gbps	2 Gbps
Max sessions	4,000,000	2,000,000	1,000,000
New sessions per second	120,000	120,000	120,000
IPSec VPN tunnels/tunnel interfaces	8,000	4,000	2,000
SSL VPN Users	20,000	10,000	5,000
Virtual routers	225	125	20
Virtual systems (base/max ²)	25/225	25/125	10/20
Security zones	900	500	80
Max number of policies	40,000	20,000	10,000

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

² Adding virtual systems to the base quantity requires a separately purchased license.

HARDWARE SPECIFICATIONS**PA-5060/PA-5050****PA-5020**

I/O	(12)10/100/1000, (8) Gigabit SFP, (4) 10 Gigabit SFP+	(12)10/100/1000, (8) Gigabit SFP
Management I/O	(2)10/100/1000 High Availability, (1) 10/100/1000 out-of-band management, (1) Console Port	
Power supply (Avg/max power consumption)	PA-5060: Redundant 450W AC (330W/415W) PA-5050: Redundant 450W AC (270W/340W)	Redundant 450W AC (270W/340W)
Input voltage (Input frequency)		100-240Vac (50-60Hz)
Max current consumption		8A@100Vac
Max inrush current		80A@230Vac; 40A@120Vac
Rack mountable (dimensions)		2U, 19" standard rack (3.5"H x 16.5"D x 17.5"W)
Weight (Stand alone device/As shipped)		41lbs/55lbs
Safety		UL, CUL, CB
EMI		FCC Class A, CE Class A, VCCI Class A

ENVIRONMENT

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

NETWORKING**PA-5060****PA-5050****PA-5020**

	PA-5060	PA-5050	PA-5020
<ul style="list-style-type: none"> Interface Modes 	L2, L3, Tap, Virtual Wire (transparent mode)	L2, L3, Tap, Virtual Wire (transparent mode)	L2, L3, Tap, Virtual Wire (transparent mode)
Routing			
<ul style="list-style-type: none"> Modes Forwarding table size (entries per device/per VR) Policy-based forwarding Point-to-Point Protocol over Ethernet (PPPoE) Jumbo frames 	OSPF, RIP, BGP, Static 64,000 / 64,000 Supported Supported Supported, 9210 bytes max frame size	OSPF, RIP, BGP, Static 64,000 / 64,000 Supported Supported Supported, 9210 bytes max frame size	OSPF, RIP, BGP, Static 64,000 / 64,000 Supported Supported Supported, 9210 bytes max frame size
High availability			
<ul style="list-style-type: none"> Modes Failure detection 	Active/Active Active/Passive Path Monitoring, Interface Monitoring	Active/Active Active/Passive Path Monitoring, Interface Monitoring	Active/Active Active/Passive Path Monitoring, Interface Monitoring
NAT/PAT			
<ul style="list-style-type: none"> Max NAT rules Max NAT rules (DIPP) Dynamic IP and port pool Dynamic IP pool NAT Modes DIPP- Unique destination IPs per source port and IP 	8,000 450 254 16,234 1:1 NAT, n:n NAT, m:n NAT 8	4,000 250 254 16,234 1:1 NAT, n:n NAT, m:n NAT 8	1,000 200 254 16,234 1:1 NAT, n:n NAT, m:n NAT 8
VLANs			
<ul style="list-style-type: none"> 802.1q VLAN tags per device/ per interface Max interfaces Aggregate Interfaces (802.3ad) 	4,094/ 4,094 4,096 Supported	4,094/ 4,094 4,096 Supported	4,094/ 4,094 2,048 Supported
Virtual Wire			
<ul style="list-style-type: none"> Max virtual wires Physical interfaces mapped to VWs 	12 Supported	12 Supported	12 Supported
Address Assignment			
<ul style="list-style-type: none"> Captive Portal for Management Interface DHCP server/DHCP relay Max Addresses 	Supported up to 3 servers 64,000	Supported up to 3 servers 64,000	Supported up to 3 servers 64,000
IPv6			
<ul style="list-style-type: none"> Modes Services 	L2, L3, Tap, Virtual Wire (transparent mode) App-ID, User-ID, Content-ID and SSL Decryption	L2, L3, Tap, Virtual Wire (transparent mode) App-ID, User-ID, Content-ID and SSL Decryption	L2, L3, Tap, Virtual Wire (transparent mode) App-ID, User-ID, Content-ID and SSL Decryption
L2 Forwarding			
<ul style="list-style-type: none"> ARP table size/device IPv6 neighbor table size MAC table size/device 	32,000 5,000 32,000	32,000 5,000 32,000	20,000 2,000 20,000

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 and SNMPv2
- 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-5060****PA-5050****PA-5020**

Platform
Solid State Disk Drives (120 GB)
Solid State Disk Drives (240 GB)
AC Power Supply
DC Power Supply
DC Fan Tray
Fan Filter

PAN-PA-5060
PAN-PA-5000-SSD-120
PAN-PA-5000-SSD-240
PAN-PA-5000-PWR-AC
PAN-PA-5000-PWR-DC
PAN-PA-5000-FAN
PAN-PA-5000-FLTR

PAN-PA-5050
PAN-PA-5000-SSD-120
PAN-PA-5000-SSD-240
PAN-PA-5000-PWR-AC
PAN-PA-5000-PWR-DC
PAN-PA-5000-FAN
PAN-PA-5000-FLTR

PAN-PA-5020
PAN-PA-5000-SSD-120
PAN-PA-5000-SSD-240
PAN-PA-5000-PWR-AC
PAN-PA-5000-PWR-DC
PAN-PA-5000-FAN
PAN-PA-5000-FLTR

For additional information on the PA-5000 Series software features, please visit www.paloaltonetworks.com/literature.



3300 Olcott Street
Santa Clara, CA 95054
Main: +1.408.573.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087
www.paloaltonetworks.com

Copyright ©2011, 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_SS_PA5000_051811