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:

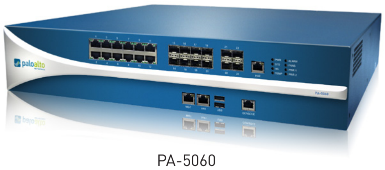
- Identifies and controls applications irrespective of port, protocol, encryption (SSL or SSH) or evasive tactic employed.
- Enables positive enforcement application usage policies: allow, deny, schedule, inspect, apply traffic shaping.
- Graphical visibility tools enable simple and intuitive view into 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	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*)	25/225*	25/125*	10/20*
Security zones	900	500	80
Max number of policies	40,000	20,000	10,000

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

NETWORKING	PA-5060	PA-5050	PA-5020
Deployment			
• Modes	L2, L3, Tap, Virtual Wire (transparent mode)	L2, L3, Tap, Virtual Wire (transparent mode)	L2, L3, Tap, Virtual Wire (transparent mode)
Routing			
• Modes	OSPF, RIP, BGP, Static	OSPF, RIP, BGP, Static	OSPF, RIP, BGP, Static
• Forwarding table size (entries per device/per VR)	64,000 / 64,000	64,000 / 64,000	64,000 / 64,000
• Policy-based forwarding	Supported	Supported	Supported
• Point-to-Point Protocol over Ethernet (PPPoE)	Supported	Supported	Supported
• Jumbo frames	Supported	Supported	Supported
NAT/PAT			
• Max NAT rules	8,000	4,000	1,000
• Max NAT rules (DIPP)	450	250	200
• Dynamic IP and port pool	254	254	254
• Dynamic IP pool	16,234	16,234	16,234
• NAT Modes	1:1 NAT, n:n NAT, m:n NAT	1:1 NAT, n:n NAT, m:n NAT	1:1 NAT, n:n NAT, m:n NAT
• PAT- Unique destination IPs per source port and IP	8	8	8
VLANs			
• 802.1q VLAN tags per device/ per interface	4,094/ 4,094	4,094/ 4,094	4,094/ 4,094
• Max interfaces	4,096	4,096	2,048
• Aggregate Interfaces (802.3ad)	Supported	Supported	Supported
Virtual Wire			
• Max virtual wires:	12	12	12
• Physical interfaces mapped to VWs	Supported	Supported	Supported
Address Assignment			
• Captive Portal for Management Interface	Supported	Supported	Supported
• DHCP server/DHCP relay	up to 3 servers	up to 3 servers	up to 3 servers
• Max Addresses: 64,000	64,000	64,000	64,000
L2 Forwarding			
• ARP table size/device	32,000	32,000	20,000
• IPv6 neighbor table size	5,000	5,000	2,000
• MAC table size/device	32,000	32,000	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
- Custom URL cache database (from 180M URL database)
- Custom block pages and URL categories

HARDWARE SPECIFICATIONS	PA-5060/PA-5050	PA-5020
Platform	(12) 10/100/1000 + (8) Gigabit SFP (4), 10 Gigabit SFP+	(12)10/100/1000 + (8) Gigabit SFP
Power supply (Avg/max power consumption)	Redundant 450W AC (175W/200W)	
Input voltage (Input frequency)	100-240Vac (50-60Hz)	
Max input current	50A@230Vac; 30A@120Vac	
Safety	UL, CUL, CB	
EMI	FCC Class A, CE Class A, VCCI Class A, TUV	
Rack mountable (dimensions)	2U, 19" standard rack (3.5"H x 16.5"D x 17.5"W)	

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-5060	PA-5050	PA-5020
Platform	PAN-PA-5060	PAN-PA-5050	PAN-PA-5020
Solid State Disk Drives (120 GB)	PAN-PA-5000-SSD-120	PAN-PA-5000-SSD-120	PAN-PA-5000-SSD-120
Solid State Disk Drives (240 GB)	PAN-PA-5000-SSD-240	PAN-PA-5000-SSD-240	PAN-PA-5000-SSD-240
AC Power Supply	PAN-PA-5000-PWR-AC	PAN-PA-5000-PWR-AC	PAN-PA-5000-PWR-AC
DC Power Supply	PAN-PA-5000-PWR-DC	PAN-PA-5000-PWR-DC	PAN-PA-5000-PWR-
DCFan Tray	PAN-PA-5000-FAN	PAN-PA-5000-FAN	PAN-PA-5000-FAN
Fan Filter	PAN-PA-5000-FLTR	PAN-PA-5000-FLTR	PAN-PA-5000-FLTR

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

paloalto NETWORKS

Palo Alto Networks
232 E. Java Drive
Sunnyvale, CA. 94089
Sales 866.320.4788
408.738.7700
www.paloaltonetworks.com