PA-4000 Series

The PA-4000 Series is a next generation firewall that delivers unprecedented visibility and control over applications, users and content on enterprise networks.

APPLICATION IDENTIFICATION:

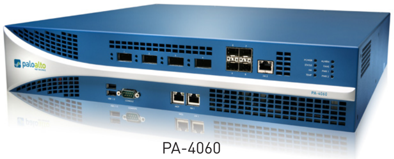
- Identifies more than 800 applications irrespective of port, protocol, SSL encryption or evasive tactic employed.
- Enables positive enforcement application usage policies: allow, deny, schedule, inspect, apply traffic shaping.
- Graphical visibility tools enable simple and intuitive view into application 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-4060

PA-4050

PA-4020

The Palo Alto Networks™ PA-4000 Series is comprised of three high performance platforms, the PA-4020, the PA-4050 and the PA-4060, all of which are targeted at high speed Internet gateway and datacenter deployments. The PA-4000 Series manages multi-Gbps traffic flows using dedicated processing and memory for networking, security, threat prevention and management.

A 10 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 PA-4050 and PA-4020 each have 24 traffic interfaces while the PA-4060 supports 10 Gbps interfaces. All of the PA-4000 Series platforms have dedicated high availability and out-of-band management interfaces.

The controlling element of the PA-4000 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-4020	PA-4050	PA-4060
Firewall throughput	2 Gbps	10 Gbps	10 Gbps
Threat prevention throughput	2 Gbps	5 Gbps	5 Gbps
IPSec VPN throughput	1 Gbps	2 Gbps	2 Gbps
IPSec VPN tunnels/interfaces	2,000	4,000	4,000
SSL VPN concurrent users	5,000	10,000	10,000
New sessions per second	60,000	60,000	60,000
Max sessions	500,000	2,000,000	2,000,000

For a complete description of the PA-4000 Series next-generation firewall feature set, please visit www.paloaltonetworks.com/literature.

Additional PA-4000 Series 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 characterisitic
- Policy-based control by user, group or IP address
- Maximum number of policies: 10,000 (PA-4020), 20,000 (PA-4050, PA-4060)
- Reconnaissance scan protection
- Denial of Service 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 visibilty 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)
- 802.3ad link aggregation
- Virtual routers: 20 (PA-4020), 125 (PA-4050, PA-4060)
- Virtual systems: 10 (PA-4020), 25 (PA-4050, PA-4060)
- Security zones: 80 (PA-4020), 500 (PA-4050, PA-4060)

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 adminstration
- Shared policies (Panorama)
- Syslog & SNMPv2
- Customizable administrator login banner
- XML-based REST API

HARDWARE SPECIFICATIONS

I/O	(16) 10/100/1000 + (8) Gigabit SFP (PA-4050, PA-4020), (4) 10 Gigabit XFP + (4) Gigabit SFP (PA-4060)
Management I/O	(2) 10/100/1000 high availability, (1) 10/100/1000 out-of-band management, (1) DB9 console port
Power supply (Avg/max power consumption)	Redundant 400W AC (175W/200W)
Input voltage (Input frequency)	100-240Vac (50-60Hz)
Max input current	50A@230Vac; 30A@120Vac
Rack mountable (dimensions)	2U, 19" standard rack (3.5"H x 16.5"D x 17.5"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-4060	PA-4050	PA-4020
Platform	PAN-PA-4060	PAN-PA-4050	PAN-PA-4020
Annual threat prevention subscription	PAN-PA-4060-TP	PAN-PA-4050-TP	PAN-PA-4020-TP
Annual URL filtering subscription	PAN-PA-4060-URL2	PAN-PA-4050-URL2	PAN-PA-4020-URL2
VSYS upgrade (10 additional)	---	---	PAN-PA-4020-VSYS-10
VSYS upgrade (50 additional)	PAN-PA-4060-VSYS-50	PAN-PA-4050-VSYS-50	---
VSYS upgrade (100 additional)	PAN-PA-4060-VSYS-100	PAN-PA-4050-VSYS-100	---

For additional information on the PA-4000 Series software features, please visit www.paloaltonetworks.com/literature.

paloalto NETWORKS

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