

# 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 VISIBILITY AND CONTROL:

- Uniquely identifies over 700 applications irrespective of port, protocol, SSL encryption or evasive tactic employed
- Graphical tools enable simple and intuitive view into application, user and content activity
- Policy control by application, category, subcategory, behavioral characteristic, source/destination, URL category, or schedule

#### USER VISIBILITY AND CONTROL:

- View application traffic by users and groups via seamless integration with Active Directory
- Tie security policies to users and groups as opposed to IP address

#### CONTENT VISIBILITY AND CONTROL:

- Detect and block viruses, spyware, and vulnerability exploits, limit unauthorized file transfers and control non-desirable web surfing



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 networking, IPsec VPN connectivity, 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/tunnel interfaces	2,000	4,000	4,000
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 feature set, please visit [www.paloaltonetworks.com/literature](http://www.paloaltonetworks.com/literature).

## Additional PA-4000 Series Specifications

**APP-ID**

- Identifies and controls more than 700 applications
- SSL decryption via forward or reverse proxy

**FIREWALL**

- Policy by application, application category, subcategory, technology, risk factor or characteristic
- Policy by user, group or IP address
- Maximum number of policies: 10,000 (PA-4020), 20,000 (PA-4050, PA-4060)
- Per policy diffserv marking
- Block files by type: bat, cab, dll, doc, encrypted doc, docx, ppt, encrypted ppt, pptx, xls, encrypted xls, xlsx, rar, encrypted rar, zip, encrypted zip, exe, gzip, hta, mdb, mdi, ocx, pdf, pgg, pif, pl, reg, sh, tar, text/html, tif, wsk, zcompressed
- Data filtering: Social Security Numbers, Credit Card Numbers, Custom Data Patterns
- Denial of Service protection
- Fragmented packet protection
- Reconnaissance scan protection

**THREAT PREVENTION (SUBSCRIPTION REQUIRED)**

- Block viruses, spyware, network worms and vulnerability exploits

**URL FILTERING (SUBSCRIPTION REQUIRED)**

- 76-category on-box database
- Customizable allow and block lists
- Customizable block page

**IPSEC VPN**

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

**NETWORKING**

- Tap Mode, Virtual Wire, layer 2, layer 3
- 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: 10 (PA-4020), 25 (PA-4050, PA-4060)
- Virtual systems: 10 (PA-4020), 25 (PA-4050, PA-4060)
- Security zones: 20 (PA-4020), 50 (PA-4050, PA-4060)

**HIGH AVAILABILITY**

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

**MANAGEMENT**

- Role-based administration
- Centralized management (Panorama)
- Shared policies (Panorama)
- Command Line Interface (CLI)
- Integrated web interface
- Syslog
- SNMPv2

**HARDWARE SPECIFICATIONS**

I/O

Management I/O

Power supply

Power consumption (avg./max)

Rack mountable

Safety

EMI

(16) 10/100/1000 + (8) Gigabit SFP (PA-4020, PA-4050)

(4) 10 Gigabit XFP + (4) Gigabit SFP (PA-4060)

(2) 10/100/1000 high availability, (1) DB9 console port,

(1) 10/100/1000 out of band management

Redundant 400W AC power

175W/200W

2U, 19" standard rack

UL, CUL, CB

FCC Class A, CE Class A, VCCI Class A, TUV

**ENVIRONMENT**

Operating temperature

Non-operating temperature

32° to 122° F, 0° to 50° C

-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](http://www.paloaltonetworks.com/literature).



**Palo Alto Networks**

232 E. Java Drive

Sunnyvale, CA. 94089

Sales 866.207.0077

[www.paloaltonetworks.com](http://www.paloaltonetworks.com)

Copyright ©2008, 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.

840-000003-00A