# 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.

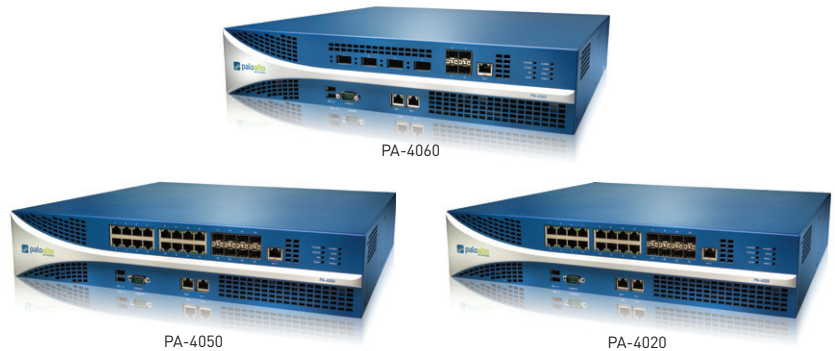PA-4060

PA-4050

PA-4020

**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, modern malware, 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.

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 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.

| PERFORMANCE AND CAPACITIES[1] | PA-4060 | PA-4050 | PA-4020 |
|---|---|---|---|
| Firewall throughput (App-ID enabled) | 10 Gbps | 10 Gbps | 2 Gbps |
| Threat prevention throughput | 5 Gbps | 5 Gbps | 2 Gbps |
| IPSec VPN throughput | 2 Gbps | 2 Gbps | 1 Gbps |
| New sessions per second | 60,000 | 60,000 | 60,000 |
| Max sessions | 2,00,000 | 2,000,000 | 5,00,000 |
| IPSec VPN tunnels/tunnel interfaces | 4,000 | 4,000 | 2,000 |
| SSL VPN Users | 10,000 | 10,000 | 5,000 |
| SSL decrypt sessions | 23,000 | 23,000 | 7,500 |
| SSL Inbound Certificates | 300 | 300 | 25 |
| Virtual routers | 125 | 125 | 20 |
| Virtual systems (base/max[2]) | 25/125 | 25/125 | 10/20 |
| Security zones | 500 | 500 | 80 |
| Max number of policies | 20,000 | 20,000 | 10,000 |
| Address Objects | 40,000 | 40,000 | 10,000 |
| Fully Qualified Domain Names (FQDN) | 2,000 | 2,000 | 2,000 |

[1] Performance and capacities are measured under ideal testing conditions using HTTP traffic and PAN-OS 4.1.

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

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

paloalto
NETWORKS

the network security company™

## HARDWARE SPECIFICATIONS

### I/O

- PA-4060: (4) 10 Gigabit XFP, (4) Gigabit SFP
- PA-4050, PA-4020: (16) 10/100/1000, (8) Gigabit SFP

### 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 CURRENT CONSUMPTION

- 2.5A@100VAC

### MEAN TIME BETWEEN FAILURE (MTBF)

- 7.18 years

### MAX INRUSH CURRENT

- 50A@230VAC; 30A@120VAC

### DIMENSIONS

- 2U, 19" standard rack (3.5"H x 16.5"D x 17.5"W)

### WEIGHT (STAND ALONE DEVICE/AS SHIPPED)

- 33lbs/40lbs

### 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

### INTERFACE MODES

- L2, L3, Tap, Virtual Wire (transparent mode): Supported

### ROUTING

- Modes: OSPF, RIP, BGP, Static
- Forwarding table size (entries per device/per VR): 20,000/20,000 (PA-4060, PA-4050), 10,000/10,000 (PA-4020)
- Policy-based forwarding: Supported
- Point-to-Point Protocol over Ethernet (PPPoE): Supported
- Jumbo frames: Supported, 9210 bytes max frame size
- Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, and v3

### HIGH AVAILABILITY

- Modes: Active/Active, Active/Passive
- Failure detection: Path Monitoring, Interface Monitoring

### NAT/PAT

- Max NAT rules: 4,000 (PA-4060, PA-4050), 1,000 (PA-4020)
- Max NAT rules (DIPP): 250 (PA-4060, PA-4050), 200 (PA-4020)
- Dynamic IP and port pool: 254
- Dynamic IP pool: 16,234
- NAT Modes: 1:1 NAT, n:n NAT, m:n NAT
- DIPP oversubscription (Unique destination IPs per source port and IP): 8 (PA-4060, PA-4050), 4 (PA-4020)

### VLANS

- 802.1q VLAN tags per device/per interface: 4,094/4,094
- Max interfaces: 4,096 (PA-4060, PA-4050), 2,048 (PA-4020)
- Aggregate Interfaces (802.3ad): Supported

### VIRTUAL WIRE

- Max virtual wires (vwire): 12
- Physical interfaces mapped to VWs: Supported

### ADDRESS ASSIGNMENT

- Address assignment for device: DHCP Client/PPPoE/Static
- Address assignment for users: DHCP Server/DHCP Relay/Static

### IPV6

- Modes: L2, L3, Tap, Virtual Wire (transparent mode)
- Services: App-ID, Content-ID and SSL Decryption

### L2 FORWARDING

- ARP table size/device: 20,000 (PA-4060, PA-4050), 10,000 (PA-4020)
- IPv6 neighbor table size: 5,000 (PA-4060, PA-4050), 2,000 (PA-4020)
- MAC table size/device: 22,000 (PA-4060, PA-4050), 10,000 (PA-4020)

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

## 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: MD5, SHA1, SHA-256, SHA-384, SHA-512

### GLOBALPROTECT (REMOTE ACCESS)

- GlobalProtect Gateway
- GlobalProtect Portal
- Transport: IPSec with SSL fall-back
- Authentication: LDAP, RADIUS, SecurID, Kerberos, local user database
- Client OS: Mac OS X 10.6, 10.7 (32/64 bit), Windows XP, Windows Vista (32/64 bit), Windows 7 (32/64 bit)
- Third Party Client Support: Apple iOS

### FILE AND DATA FILTERING

- Control unauthorized data transfer (data patterns and file types)
- Drive-by download protection
- Predefined signatures for SSN and Credit Card numbers
- Unique file types identified: 59

### MANAGEMENT, REPORTING, VISIBILITY TOOLS

- Integrated web interface, CLI or central management (Panorama)
- Syslog, SNMP v2/v3
- 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

### 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

### WILDFIRE

- Identify and analyze targeted and unknown malware
- Automated analysis of unknown files for malicious behaviors
- Forensic analysis and protection for newly discovered malware

### 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
- Physical interfaces supported for QoS: 12 (PA-4050, PA-4020), 6 (PA-4060)

### 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

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

| ORDERING INFORMATION | PA-4060 | PA-4050 | PA-4020 |
| --- | --- | --- | --- |
| Platform | PAN-PA-4060 | PAN-PA-4050 | PAN-PA-4020 |

**paloalto** NETWORKS

the network security company™

**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**