PA-4000 Series

Key PA-4000 Series next-generation firewall features:

CLASSIFY ALL APPLICATIONS, ON ALL PORTS, ALL THE TIME WITH APP-ID™.

- Identify the application, regardless of port, encryption (SSL or SSH) or evasive technique employed.
- Use the application, not the port, as the basis for all safe enablement policy decisions: allow, deny, schedule, inspect, apply traffic shaping.
- Categorize unidentified applications for policy control, threat forensics, custom App-ID creation, or packet capture for App-ID development.

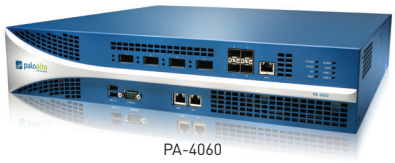
EXTEND SAFE APPLICATION ENABLEMENT POLICIES TO ANY USER, AT ANY LOCATION, WITH USER-ID™ AND GLOBALPROTECT™.

- Agentless integration with Active Directory, LDAP, eDirectory Citrix and Microsoft Terminal Services.
- Integrate with NAC, 802.1X wireless and other non-standard user repositories with an XML API.
- Deploy consistent policies to local and remote users running Microsoft Windows, Mac OS X, Linux, Android or iOS platforms.

PROTECT AGAINST ALL THREATS—BOTH KNOWN AND UNKNOWN—WITH CONTENT-IDT™ AND WILDFIRE™.

- Block a range of known threats including exploits, malware and spyware, across all ports, regardless of common threat evasion tactics employed.
- Limit unauthorized transfer of files and sensitive data, and control non-work-related web surfing.
- Identify unknown malware, analyze for more than 100 malicious behaviors, automatically create and deliver a signature in the next available update.

paloalto NETWORKS
the network security company™


PA-4060


PA-4050


PA-4020

The Palo Alto Networks™ PA-4000 Series is comprised of three high performance platforms, the PA-4060, the PA-4050 and the PA-4020, all of which are targeted at high speed datacenter and Internet gateway deployments. The PA-4000 Series delivers up to 10 Gbps of throughput using dedicated processing and memory for the key functional areas of networking, security, threat prevention and management.

The high speed backplane is physically divided into separate data and control planes, thereby ensuring that management access is always available, irrespective of the traffic load. The controlling element of the PA-4000 Series is PAN-OS™, a security-specific operating system that allows organizations to safely enable applications using App-ID, User-ID, Content-ID, GlobalProtect, and WildFire.

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	2,000,000	2,000,000	500,000
IPSec VPN tunnels/tunnel interfaces	4,000	4,000	2,000
GlobalProtect (SSL VPN) concurrent 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/max2)	25/125	25/125	10/20
Security zones	500	500	80
Max. number of policies	20,000	20,000	10,000

[1] Performance and capacities are measured under ideal testing conditions using PAN-OS 5.0.

[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.

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

STORAGE CAPACITY

- 160GB HDD

POWER SUPPLY (AVG/MAX POWER CONSUMPTION)

- Redundant 400W AC (175W/200W)

MAX BTU/HR

- 682

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

RACK MOUNTABLE (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, TUV

CERTIFICATIONS

- FIPS 140 Level 2, Common Criteria EAL2, ICSA, UCAPL

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)

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
- Point-to-Point Protocol over Ethernet (PPPoE)
- Jumbo frames: 9,210 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

ADDRESS ASSIGNMENT

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

IPV6

- L2, L3, tap, virtual wire (transparent mode)
- Features: App-ID, User-ID, Content-ID, WildFire and SSL decryption

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)

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)
- NAT64

VIRTUAL WIRE

- Max virtual wires: 2,048 (PA-4060, PA-4050), 1,024 (PA-4020)
- Interface types mapped to virtual wires: physical and subinterfaces

L2 FORWARDING

- ARP table size/device: 20,000 (PA-4060, PA-4050), 10,000 (PA-4020)
- MAC 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)

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

WILDFIRE

- Identify and analyze targeted and unknown files for more than 100 malicious behaviors
- Generate and automatically deliver protection for newly discovered malware via signature updates
- Signature update delivery in less than 1 hour, integrated logging/reporting; access to WildFire API for programmatic submission of up to 100 samples per day and up to 1,000 report queries by file hash per day (Subscription Required)

FILE AND DATA FILTERING

- File transfer: Bi-directional control over more than 60 unique file types
- Data transfer: Bi-directional control over unauthorized transfer of CC# and SSN
- Drive-by download protection

USER INTEGRATION (USER-ID)

- Microsoft Active Directory, Novell eDirectory, Sun One and other LDAP-based directories
- Microsoft Windows Server 2003/2008/2008r2, Microsoft Exchange Server 2003/2007/2010
- Microsoft Terminal Services, Citrix XenApp
- XML API to facilitate integration with non-standard user repositories

IPSEC VPN (SITE-TO-SITE)

- Key Exchange: Manual key, IKE v1
- Encryption: 3DES, AES (128-bit, 192-bit, 256-bit)
- Authentication: MD5, SHA-1, SHA-256, SHA-384, SHA-512
- Dynamic VPN tunnel creation (GlobalProtect)

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

URL FILTERING (SUBSCRIPTION REQUIRED)

- Pre-defined and custom URL categories
- Device cache for most recently accessed URLs
- URL category as part of match criteria for security policies
- Browse time information

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

SSL VPN/REMOTE ACCESS (GLOBALPROTECT)

- GlobalProtect Gateway
- GlobalProtect Portal
- Transport: IPSec with SSL fall-back
- Authentication: LDAP, SecurID, or local DB
- Client OS: Mac OS X 10.6, 10.7 (32/64 bit), 10.8 (32/64 bit), Windows XP, Windows Vista (32/64 bit), Windows 7 (32/64 bit)
- Third party client support: Apple iOS, Android 4.0 and greater, VPNC IPSec for Linux

MANAGEMENT, REPORTING, VISIBILITY TOOLS

- Integrated web interface, CLI or central management (Panorama)
- Multi-language user interface
- Syslog, SNMP v2/v3
- XML-based REST API
- Graphical summary of applications, URL categories, threats and data (ACC)
- View, filter and export traffic, threat, WildFire, URL, and data filtering logs
- Fully customizable reporting

For additional Information on the PA-4000 Series next-generation firewall feature set, please visit www.paloaltonetworks.com/literature.

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