PA-4000 Series

Key Security 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.
- Easily integrate firewall policies with NAC, 802.1X wireless, Proxies and NAC solutions.
- 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-ID™ 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 it based on more than 100 malicious behaviors, then automatically create and deliver protection in the next content update.

PA-4060

PA-4050

PA-4020

The Palo Alto Networks® PA-4000 Series is comprised of three enterprise security 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 controlling element of the PA-4000 Series is PAN-OS™, a security-specific operating system that natively classifies all traffic, inclusive of applications, threats and content, then ties that traffic to the user, regardless of location or device type. The application, content, and user—in other words, the business elements that run your business—are then used as the basis of your security policies, resulting in an improved security posture and a reduction in incident response time.

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
Virtual systems (base/max[2])	25/125	25/125	10/20

[1] Performance and capacities are measured under ideal testing conditions using PAN-OS 6.0.
[2] Adding virtual systems to the base quantity requires a separately purchased license.

To view additional information on the PA-4000 Series security features and associated capacities, please visit **www.paloaltonetworks.com/products**

paloalto NETWORKS®
the network security company™

The PA-4000 Series supports a wide range of networking features that allows you to more easily integrate our security features into your existing network.

Networking Features

INTERFACE MODES
- L2, L3, Tap, Virtual wire (transparent mode)

ROUTING
- OSPFv2/v3, BGP with graceful restart, RIP, static routing
- Policy-based forwarding
- Point-to-Point Protocol over Ethernet (PPPoE)
- Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, and v3

IPV6
- L2, L3, tap, virtual wire (transparent mode)
- Features: App-ID, User-ID, Content-ID, WildFire and SSL decryption

IPSEC VPN
- Key Exchange: Manual key, IKE v1 (Pre-shared key, certificate-based authentication)
- Encryption: 3DES, AES (128-bit, 192-bit, 256-bit)
- Authentication: MD5, SHA-1, SHA-256, SHA-384, SHA-512

VLANS
- 802.1q VLAN tags per device/per interface: 4,094/4,094
- Aggregate interfaces (802.3ad)

NETWORK ADDRESS TRANSLATION (NAT)
- NAT modes (IPv4): Static IP, dynamic IP, dynamic IP and port (port address translation)
- NAT64
- Additional NAT features: Dynamic IP reservation, dynamic IP and port oversubscription

HIGH AVAILABILITY
- Active/Passive with no session synchronization
- Failure detection: Path monitoring, Interface monitoring

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

To view additional information on the PA-4000 security features and associated capacities, please visit **www.paloaltonetworks.com/products**

paloalto NETWORKS®

the network security company™

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com