

# PA-5000 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 250 malicious behaviors, then automatically create and deliver protection in the next content update.



The Palo Alto Networks® PA-5000 Series is comprised of the PA-5060, the PA-5050 and the PA-5020, all of which are targeted at high speed datacenter and Internet gateway deployments. The PA-5000 Series delivers up to 20 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-5000 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 <sup>1</sup>	PA-5060	PA-5050	PA-5020
Firewall throughput (App-ID enabled)	20 Gbps	10 Gbps	5 Gbps
Threat prevention throughput	10 Gbps	5 Gbps	2 Gbps
IPSec VPN throughput	4 Gbps	4 Gbps	2 Gbps
Max sessions	4,000,000	2,000,000	1,000,000
New sessions per second	120,000	120,000	120,000
Virtual systems (base/max <sup>2</sup> )	25/225	25/125	10/20

<sup>1</sup> Performance and capacities are measured under ideal testing conditions using PAN-OS 6.0.

<sup>2</sup> Adding virtual systems to the base quantity requires a separately purchased license.

To view additional information on the PA-5000 Series security features and associated capacities, please visit [www.paloaltonetworks.com/products](http://www.paloaltonetworks.com/products)

The PA-5000 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
- SLAAC

### 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), LACP

### 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

- Modes: Active/Active, Active/Passive
- Failure detection: path monitoring, interface monitoring

## Hardware Specifications

### I/O

- **PA-5060 | PA-5050** - (12) 10/100/1000, (8) gigabit SFP, (4) 10 gigabit SFP+
- **PA-5020** - (12) 10/100/1000, (8) gigabit SFP

### MANAGEMENT I/O

- (2) 10/100/1000 high availability, (1) 10/100/1000 out-of-band management, (1) RJ45 console port

### STORAGE OPTIONS

- Single or dual solid state disk drives

### STORAGE CAPACITY

- 120GB, 240GB SSD, RAID 1

### POWER SUPPLY (AVG/MAX POWER CONSUMPTION)

- **PA-5060** - Redundant 450W AC (330W/415W)
- **PA-5050 | PA-5020** - Redundant 450W AC (270W/340W)

### MAX BTU/HR

- **PA-5060** - 1,416
- **PA-5050 | PA-5020** - 1,160

### INPUT VOLTAGE (INPUT FREQUENCY)

- 100-240VAC (50-60Hz); -40 to -72 VDC

### MAX CURRENT CONSUMPTION

- 8A@100VAC, 14A@48VDC

### MAX INRUSH CURRENT

- 80A@230VAC; 40A@120VAC; 40A@48VDC

### MEAN TIME BETWEEN FAILURE (MTBF)

- 6.5 years

### RACK MOUNTABLE (DIMENSIONS)

- 2U, 19" standard rack (3.5"H x 21"D x 17.5"W)

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

- 41lbs/55lbs

### SAFETY

- CB, CSA

### EMI

- FCC Class A, CE Class A, VCCI Class A

### CERTIFICATIONS

See: <https://www.paloaltonetworks.com/company/certifications.html>

### 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-5000 Series features and associated capacities, please visit [www.paloaltonetworks.com/products](http://www.paloaltonetworks.com/products)



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

Copyright ©2015, 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. PAN\_SS\_PA5000\_052215