Request a Quote

Corporate Armor For more information, please call **877.449.0458**, or email us at **Sales@CorporateArmor.com**.

PA-2000 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 230 malicious behaviors, then automatically create and deliver protection in the next content update.

PA-2050

PA-2020

The Palo Alto Networks® PA-2000 Series is comprised of the PA-2050 and the PA-2020, both of which are targeted at high speed Internet gateway deployments. The PA-2000 Series manages network traffic flows using dedicated processing and memory for networking, security, threat prevention and management.

The controlling element of the PA-2000 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-2050	PA-2020
Firewall throughput (App-ID enabled)	1 Gbps	500 Mbps
Threat prevention throughput	500 Mbps	200 Mbps
IPSec VPN throughput	300 Mbps	200 Mbps
New sessions per second	15,000	15,000
Max sessions	250,000	125,000
Virtual systems (base/max[2])	1/6	1/6

[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-2000 Series security features and associated capacities, please visit **www.paloaltonetworks.com/products**

paloalto NETWORKS®

The PA-2000 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)

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-2050 - (16) 10/100/1000, (4) SFP optical gigabit
PA-2020 - (12) 10/100/1000, (2) SFP optical gigabit

MANAGEMENT I/O
• (1) 10/100/1000 out-of-band management port, (1) RJ-45 console port

STORAGE CAPACITY
• 160GB HDD

POWER SUPPLY (AVG/MAX POWER CONSUMPTION)
• 250W (105W/120W)

MAX BTU/HR
• 409

INPUT VOLTAGE (INPUT FREQUENCY)
• 100-240VAC (50-60Hz)

MAX CURRENT CONSUMPTION
• 1.5A@100VAC

MEAN TIME BETWEEN FAILURE (MTBF)
• 7.3 years

MAX INRUSH CURRENT
• 70A@230VAC; 35A@115VAC

RACK MOUNTABLE (DIMENSIONS)
• 1U, 19" standard rack (1.75"H x 17"D x 17"W)

WEIGHT (STAND ALONE DEVICE/AS SHIPPED)
• 15lbs/20lbs

SAFETY
• UL, CUL, CB

EMI
• FCC Class A, CE Class A, VCCI Class A, TUV

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-2000 Series features and associated capacities, please visit **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