

PA-2000 Series

The PA-2000 Series is a next-generation firewall that delivers unprecedented visibility and control over applications, users and content on enterprise networks.

APPLICATION IDENTIFICATION:

- Identifies more than 950 applications irrespective of port, protocol, SSL encryption 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 and Microsoft Terminal Services users, enabling visibility and control over their respective application usage.
- Control non-Windows hosts via web-based authentication.

CONTENT IDENTIFICATION:

- Block viruses, spyware, 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.



PA-2020



PA-2050

The Palo Alto Networks™ PA-2000 Series is comprised of two high performance platforms, the PA-2020 and the PA-2050, 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.

A high speed backplane smoothes the pathway between dedicated processors, and the separation of data and control plane ensures that management access is always available, irrespective of the traffic load. Interface density for the PA-2020 and the PA-2050 is unmatched with up to 20 traffic interfaces and dedicated out-of-band management interfaces.

The controlling element of the PA-2000 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, VPN and management features.

KEY PERFORMANCE SPECIFICATIONS	PA-2020	PA-2050
Firewall throughput	500 Mbps	1 Gbps
Threat prevention throughput	200 Mbps	500 Mbps
IPSec VPN throughput	200 Mbps	300 Mbps
IPSec VPN tunnels/interfaces	1,000	2,000
SSL VPN concurrent users	500	1,000
New sessions per second	15,000	15,000
Max sessions	125,000	250,000

For a complete description of the PA-2000 Series feature set, please visit www.paloaltonetworks.com/literature.

Additional PA-2000 Series Specifications and Features

APP-ID

- Identifies and controls more than 950 applications
- SSL decryption (inbound and outbound)
- Customize application properties
- Custom HTTP and SSL applications

FIREWALL

- Policy-based control by application, application category, subcategory, technology, risk factor or characteristic
- Application function control
- Fragmented packet protection
- Reconnaissance scan protection
- Denial of Service (DoS)/Distributed Denial of Services (DDoS) protection
- Maximum number of policies: (PA-2020) 2,500 (PA-2050) 5,000

USER-ID

- Visibility and control by user, group and IP address
- Active Directory, LDAP, eDirectory, Citrix and Microsoft Terminal Services
- XML API (external user repository integration)
- WMI and NetBios polling
- Maximum concurrent user/IP mappings: 64,000

DATA FILTERING

- Control unauthorized data transfer (social security numbers, credit card numbers, custom data patterns)
- Control unauthorized transfer of more than 50 file types

URL FILTERING (SUBSCRIPTION REQUIRED)

- 76-category, 20M URL on-box database
- Custom 1M URL cache database (from 180M URL database)
- Custom block pages and URL categories

IPSEC VPN (SITE-TO-SITE)

- Manual key, IKE v1
- 3DES, AES (128-bit, 192-bit, 256-bit) encryption
- SHA1, MD5 authentication

SSL VPN (REMOTE ACCESS)

- IPsec transport with SSL fall-back
- Enforce unique policies for SSL VPN traffic
- Enable/disable split tunneling to control client access
- LDAP, SecurID, or local DB authentication
- Client OS: Windows XP, Windows Vista (32 and 64 bit), Windows 7 (32 and 64 bit)

HIGH AVAILABILITY

- Active/Passive failover
- Configuration and session synchronization
- Heartbeat checking
- Link and path failure monitoring

NETWORKING

- Dynamic routing (BGP, OSPF and RIPv2)
- Tap mode, virtual wire, layer 2, layer 3
- Network address translation (NAT)
 - Source and destination address translation
 - Dynamic IP and port pool: 254
 - Dynamic IP pool: 16,234
- DHCP server/ DHCP relay: Up to 3 servers
- 802.1Q VLANs: 4,094
- Policy-based forwarding
- Point-to-Point Protocol over Ethernet (PPPoE)
- IPv6 application visibility, control and full content inspection (Virtual wire mode only)
- Virtual routers: 10
- Security zones: 40
- Virtual systems (base/max): 1/6*

THREAT PREVENTION (SUBSCRIPTION REQUIRED)

- Detect and block application vulnerability exploits (IPS)
- Stream-based protection against viruses, spyware and worms
- HTML/Javascript virus protection
- Inspect compressed files that use the Deflate algorithm (Zip, Gzip, etc)
- Custom vulnerability and spyware phone home signatures
- Content updates: daily (malware), weekly (vulnerability signatures), emergency (all)

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

MANAGEMENT TOOLS

- Integrated web interface
- Command line interface (CLI)
- Role-based administration
- Syslog and SNMPv2
- Customizable administrator login banner
- XML-based REST API
- Centralized management (Panorama)
- Centrally manage PAN-OS and content updates (Panorama)
- Shared policies (Panorama)

VISIBILITY AND REPORTING TOOLS

- Graphical summary of applications, URL categories, threats and data (ACC)
- View, filter, export traffic, threat, URL, and data filtering logs
- Fully customizable reporting
- Trace session tool

* Adding virtual systems to the base quantity requires a separately purchased license.

HARDWARE SPECIFICATIONS**PA-2050****PA-2020**

I/O	(16) 10/100/1000 + (4) SFP optical gigabit (PA-2050)	(12) 10/100/1000 + (2) SFP optical gigabit (PA-2020)
Management I/O	(1) 10/100/1000 out-of-band management port, (1) RJ-45 console port	
Power supply (Avg/max power consumption)	175W/200W (105W/120W)	
Input voltage (Input frequency)	100-240Vac (50-60Hz)	
Power factor	0.65 to 0.70 (PA-2050, PA-2020)	
Max input current	70A@230Vac; 35A@115Vac	
Rack mountable (Dimensions)	1U, 19" standard rack (1.75"H x 17"D x 17"W)	
Safety	UL, CUL, CB	
EMI	FCC Class A, CE Class A, VCCI Class A, TUV	
MTBF	7.3 years (PA-2050, PA-2020)	

ENVIRONMENT

Operating temperature	32° to 122° F, 0° to 50° C
Non-operating temperature	-4° to 158° F, -20° to 70° C

ORDERING INFORMATION**PA-2050****PA-2020**

Platform	PAN-PA-2050	PAN-PA-2020
Annual threat prevention subscription	PAN-PA-2050-TP	PAN-PA-2020-TP
Annual URL filtering subscription	PAN-PA-2050-URL2	PAN-PA-2020-URL2
Virtual systems	PAN-PA-2050-VSYS-5	PAN-PA-2020-VSYS-5

For additional information on the PA-2000 Series software features, please visit www.paloaltonetworks.com/literature.



Palo Alto Networks
 232 E. Java Drive
 Sunnyvale, CA. 94089
 Sales 866.320.4788
 408.738.7700
www.paloaltonetworks.com

Copyright ©2010, 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-OS 3.1, March 2010.

840-000003-00B