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.

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.

APPLICATION IDENTIFICATION:
- Identifies more than 800 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.
- 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.

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.

paloalto NETWORKS

Additional PA-2000 Series Specifications

APP-ID

- Identifies and controls more than 800 applications
- SSL decryption via forward or reverse proxy
- Customize application properties
- Custom HTTP applications

FIREWALL

- Policy-based control by application, application category, subcategory, technology, risk factor or characterisitic
- Policy-based control by user, group or IP address
- Maximum number of policies: 2,500 (PA-2020), 5,000 (PA-2050)
- Reconnaissance scan protection
- Denial of Service (DoS) protection
- Fragmented packet protection

DATA FILTERING

- Detect and block social security numbers, credit card numbers, custom data patterns
- Block files by type

THREAT PREVENTION (SUBSCRIPTION REQUIRED)

- Block viruses, spyware, worms and vulnerability exploits

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

NETWORKING

- Tap mode, virtual wire, layer 2, layer 3, mixed L2/L3
- IPv6 application visibilty and control via Content-ID (Virtual wire mode only)
- IPv6 full content inspection via Content-ID (Virtual wire mode only)
- 802.1Q VLAN tagging (layer 2, layer 3)
- Network address translation (NAT)
- OSPF and RIPv2
- DHCP server/ DHCP relay (up to 3 servers)
- Virtual routers: 3 (PA-2020), 5 (PA-2050)
- Security zones: 20
- Virtual systems: 5 (optional license required)

URL FILTERING (SUBSCRIPTION REQUIRED)

- 76-category on-box customizable database
- Customizable allow and block lists
- Customizable block pages

QUALITY OF SERVICE (QOS)

- Policy-based traffic shaping (guaranteed, maximum and priority) by application, user, source, destination, interface, IPSec VPN tunnel and more
- Per policy diffserv marking

HIGH AVAILABILITY

- Active/Passive
- Configuration and session synchronization
- Interface and IP tracking
- Link and path failure monitoring

MANAGEMENT TOOLS

- Integrated web interface
- Command line interface (CLI)
- Centralized management (Panorama)
- Role-based adminstration
- Shared policies (Panorama)
- Syslog & SNMPv2
- Customizable administrator login banner
- XML-based REST API

HARDWARE SPECIFICATIONS

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)
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

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 866.207.0077
www.paloaltonetworks.com