PA-200

The PA-200 is a next-generation firewall that delivers unprecedented visibility and control over applications, users and content on enterprise networks.

APPLICATION IDENTIFICATION:

- Identifies and controls applications irrespective of port, protocol, encryption (SSL or SSH) 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:

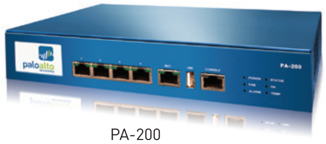
- Policy-based visibility and control over who is using the applications through seamless integration with Active Directory, LDAP, and eDirectory.
- Identifies Citrix, Microsoft Terminal Services and XenWorks users, enabling visibility and control over their respective application usage.
- Control non-Windows hosts via web-based authentication.

CONTENT IDENTIFICATION:

- Block viruses, spyware, modern malware, 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 predictable throughput performance with low latency while scanning content.

paloalto NETWORKS

the network security company™



PA-200

The Palo Alto Networks™ PA-200 is targeted at high speed Internet gateway deployments within distributed enterprise branch offices. The PA-200 manages network traffic flows using dedicated computing resources for networking, security, threat prevention and management.

A high speed dual core CPU provides separation of data and control plane and ensures that management access is always available, irrespective of the traffic load. The controlling element of the PA-200 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 and management features.

PERFORMANCE AND CAPACITIES[1]	PA-200
Firewall throughput (App-ID enabled)	100 Mbps
Threat prevention throughput	50 Mbps
IPSec VPN throughput	50 Mbps
New sessions per second	1,000
Max sessions	64,000
IPSec VPN tunnels/tunnel interfaces	25
SSL VPN users	25
SSL decrypt sessions	1,000
SSL inbound certificates	25
Virtual routers	3
Security Zones	10
Max number of policies	250
Address objects	2,500
Fully Qualified Domain Names (FQDN)	2,000

[1] Performance and capacities are measured under ideal testing conditions using HTTP traffic and PAN-OS 4.1.

For a complete description of the PA-200 Series next-generation firewall feature set, please visit www.paloaltonetworks.com/literature.

HARDWARE SPECIFICATIONS

I/O

- (4) 10/100/1000

MANAGEMENT I/O

- (1) 10/100 out-of-band management port, (1) RJ-45 console port

POWER SUPPLY (AVG/MAX POWER CONSUMPTION)

- 40W (20W/30W)

INPUT VOLTAGE (INPUT FREQUENCY)

- 100-240VAC (50-60Hz)

MAX CURRENT CONSUMPTION

- 1.3A@100VAC

DIMENSIONS

- 1.75"H x 7"D x 9.25"W

WEIGHT (STAND ALONE DEVICE/AS SHIPPED)

- 2.8lbs/5.0lbs

SAFETY

- UL, CUL, CB, TUV

EMI

- FCC Class B, CE Class B, VCCI Class B

ENVIRONMENT

- Operating temperature: 32° to 104° F, 0° to 40° C
- Non-operating temperature: -4° to 158° F, -20° to 70° C

NETWORKING

INTERFACE MODES

- L2, L3, Tap, Virtual Wire (transparent mode): Supported

ROUTING

- Modes: OSPF, RIP, BGP, Static
- Forwarding table size (entries per device/per VR): 1,000/1,000
- Policy-based forwarding: Supported
- Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, and v3

HIGH AVAILABILITY

- Modes: Active/Passive with no session synchronization
- Failure detection: Path Monitoring, Interface Monitoring

NAT/PAT

- Max NAT rules: 125
- Max NAT rules (DIPP): 125
- Dynamic IP and port pool: 254
- Dynamic IP pool: 16,234
- NAT Modes: 1:1 NAT, n:n NAT, m:n NAT
- DIPP oversubscription (Unique destination IPs per source port and IP): 1

VLANS

- 802.1q VLAN tags per device/per interface: 4,094/4,094
- Max interfaces: 100

VIRTUAL WIRE

- Max virtual wires (vwire): 2
- Physical interfaces mapped to VWs: Supported

ADDRESS ASSIGNMENT

- Address assignment for device: DHCP Client/PPPoE/Static
- Address assignment for users: DHCP Server/DHCP Relay/Static

IPV6

- Modes: L2, L3, Tap, Virtual Wire (transparent mode)
- Services: App-ID, Content-ID and SSL Decryption

L2 FORWARDING

- ARP table size/device: 500
- IPv6 neighbor table size: 500
- MAC table size/device: 500

For a complete description of the PA-200 Series next-generation firewall feature set, please visit www.paloaltonetworks.com/literature.

SECURITY

FIREWALL

- Policy-based control over applications, users and content
- Fragmented packet protection
- Reconnaissance scan protection
- Denial of Service (DoS)/Distributed Denial of Services (DDoS) protection
- Decryption: SSL (inbound and outbound), SSH

USER INTEGRATION (USER-ID)

- Active Directory, LDAP, eDirectory, Citrix and Microsoft Terminal Services, Xenworks, XML API

IPSEC VPN (SITE-TO-SITE)

- Key Exchange: Manual key, IKE v1
- Encryption: 3DES, AES (128-bit, 192-bit, 256-bit)
- Authentication: MD5, SHA1, SHA-256, SHA-384, SHA-512

GLOBALPROTECT (REMOTE ACCESS)

- GlobalProtect Gateway
- GlobalProtect Portal
- Transport: IPSec with SSL fall-back
- Authentication: LDAP, RADIUS, SecurID, Kerberos, local user database
- Client OS: Mac OS X 10.6, 10.7 (32/64 bit), Windows XP, Windows Vista (32/64 bit), Windows 7 (32/64 bit)
- Third Party Client Support: Apple iOS

FILE AND DATA FILTERING

- Control unauthorized data transfer (data patterns and file types)
- Drive-by download protection
- Predefined signatures for SSN and Credit Card numbers
- Unique file types identified: 59

MANAGEMENT, REPORTING, VISIBILITY TOOLS

- Integrated web interface, CLI or central management (Panorama)
- Syslog, SNMP v2/v3
- XML-based REST API
- Graphical summary of applications, URL categories, threats and data (ACC)
- View, filter, export traffic, threat, URL, and data filtering logs
- Fully customizable reporting

THREAT PREVENTION (SUBSCRIPTION REQUIRED)

- Application, operating system vulnerability exploit protection
- Stream-based protection against viruses (including those embedded in HTML, Javascript, PDF and compressed), spyware, worms

WILDFIRE

- Identify and analyze targeted and unknown malware
- Automated analysis of unknown files for malicious behaviors
- Forensic analysis and protection for newly discovered malware

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
- Physical interfaces supported for QoS: 4

URL FILTERING (SUBSCRIPTION REQUIRED)

- 76-category, 20M URL on-box database
- Dynamic URL filtering (1M URL cache on device)
- Custom block pages and URL categories

For a complete description of the PA-200 Series next-generation firewall feature set, please visit www.paloaltonetworks.com/literature.

ORDERING INFORMATION	PA-200
Platform	PAN-PA-200

paloalto NETWORKS
the network security company™

3300 Olcott Street
Santa Clara, CA 95054

Main: +1.408.573.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com