PA-200

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 100 malicious behaviors, then automatically create and deliver protection in the next content update.

PA-200

The Palo Alto Networks® PA-200 is an enterprise security platform for distributed enterprise branch offices and medium sized businesses.

The controlling element of the PA-200 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-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

[1]Performance and capacities are measured under ideal testing conditions using PAN-OS 6.0.

To view additional information on the PA-200 security features and associated capacities, please visit **www.paloaltonetworks.com/products**

paloalto NETWORKS®

the network security company™

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

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
- Max interfaces: 100

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

- Active/Passive with no session synchronization
- Failure detection: Path monitoring, interface monitoring

Hardware Specifications

I/O

- (4) 10/100/1000

MANAGEMENT I/O

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

STORAGE CAPACITY

- 16GB SSD

POWER SUPPLY (AVG/MAX POWER CONSUMPTION)

- 40W (20W/30W)

MAX BTU/HR

- 102 BTU

INPUT VOLTAGE (INPUT FREQUENCY)

- 100-240VAC (50-60Hz)

MAX CURRENT CONSUMPTION

- 3.3A@100VAC

MEAN TIME BETWEEN FAILURE (MTBF)

- 13 years

DIMENSIONS (STAND ALONE DEVICE/AS SHIPPED)

- 1.75”H x 7”D x 9.25”W

WEIGHT

- 2.8lbs /5.0lbs Shipping

SAFETY

- UL, CUL, CB

EMI

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

CERTIFICATIONS

- ICSA, UCAPL

ENVIRONMENT

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

The PA-200 supports a wide range of networking features that allows you to more easily integrate our security features into your existing network. To view additional information on the PA-200 security features and associated capacities, please visit **www.paloaltonetworks.com/products**

paloalto NETWORKS®
the network security company™

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

PAN_SS_PA200_122713

PA-500

The PA-500 is a next generation firewall that delivers unprecedented visibility and control over applications, users and content on enterprise networks.

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.

PA-500

The Palo Alto Networks™ PA-500 is targeted at high speed Internet gateway deployments for enterprise branch offices and medium size businesses. The PA-500 manages network traffic flows using dedicated computing resources for networking, security, threat prevention and management.

A high speed backplane smoothes the pathway between 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-500 includes (8) 10/100/1000 traffic interfaces and a dedicated out-of-band management interface.

The controlling element of the PA-500 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.

KEy PERFORmANCE SPECIFICATIONS	PA-500
Firewall throughput	250 Mbps
Threat prevention throughput	100 Mbps
IPSec VPN throughput	50 Mbps
IPSec VPN tunnels/tunnel interfaces	250
SSL VPN Uers	100
New sessions per second	7,500
Max sessions	64,000

For a complete description of the PA-500 next-generation firewall feature set, please visit www.paloaltonetworks.com/literature.

paloalto NETWORKS

Additional PA-500 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 characteristic
- Policy-based control by user, group or IP address
- Maximum number of policies 1,000
- 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 visibility 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 PIPv2
- DHCP server/DHCP relay (up to 3 servers)
- Virtual routers 2
- Security zones 20

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 administration
- Shared policies (Panorama)
- Syslog & SNMPv2
- Customizable administrator login banner
- XML-based REST API

HARDWARE SPECIFICATIONS

I/O	(8) 10/100/1000
Management I/O	(1)10/100/1000 out-of-band management port, (1) RJ-45 console port
Power supply (Avg/max power consumption)	180W (110W/75W)
Input voltage (Input frequency)	100-240Vac (50-60Hz)
Max Input current	(110Ara230Vac, (51Ara115Vac
Rack mountable (Dimensions)	1U, 19" standard rack (1.75"H x 10"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-500
Platform	PAN-PA-500
Annual threat prevention subscription	PAN-PA-500-TP
Annual URL filtering subscription	PAN-PA-500-URL2

For additional information on the PA-500 next-generation firewall feature set, please visit www.paloaltonetworks.com/literature

Palo Alto Networks
232 E. Java Drive
Sunnyvale, CA. 94089
Sales 866.207.0077
www.paloaltonetworks.com

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 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.

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.

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 characteristic
- 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 visibility 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 PIPv2
- 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 administration
- 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	70Ara230Vac, 35Ara115Vac
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, 00 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

840-000003-00B

PA-4000 Series

The PA-4000 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 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.

PA-4060

PA-4050

PA-4020

The Palo Alto Networks™ PA-4000 Series is comprised of three high performance platforms, the PA-4020, the PA-4050 and the PA-4060, all of which are targeted at high speed Internet gateway and datacenter deployments. The PA-4000 Series manages multi-Gbps traffic flows using dedicated processing and memory for networking, security, threat prevention and management.

A 10 Gbps backplane smoothes the pathway between dedicated processors, and the physical separation of data and control plane ensures that management access is always available, irrespective of the traffic load. The PA-4050 and PA-4020 each have 24 traffic interfaces while the PA-4060 supports 10 Gbps interfaces. All of the PA-4000 Series platforms have dedicated high availability and out-of-band management interfaces.

The controlling element of the PA-4000 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 and management features.

KEy PERFORmANCE SPECIFICATIONS	PA-4020	PA-4050	PA-4060
Firewall throughput	2 Gbps	10 Gbps	10 Gbps
Threat prevention throughput	2 Gbps	5 Gbps	5 Gbps
IPSec VPN throughput	1 Gbps	2 Gbps	2 Gbps
IPSec VPN tunnels/interfaces	2,000	4,000	4,000
SSL VPN concurrent users	5,000	10,000	10,000
New sessions per second	60,000	60,000	60,000
Max sessions	500,000	2,000,000	2,000,000

For a complete description of the PA-4000 Series next-generation firewall feature set, please visit www.paloaltonetworks.com/literature.

paloalto NETWORKS

Additional PA-4000 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 characteristic
- Policy-based control by user, group or IP address
- Maximum number of policies 10,000 (PA-4020), 20,000 (PA-4050, PA-4060)
- Reconnaissance scan protection
- Denial of Service 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, virtualwire, layer 2, layer 3, mixed L2/L3
- IPv6 application visibility and control via Content-ID (Virtualwire 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)
- 802.3ad link aggregation
- Virtual routers 20 (PA-4020), 125 (PA-4050, PA-4060)
- Virtual systems 10 (PA-4020), 25 (PA-4050, PA-4060)
- Security zones 80 (PA-4020), 500 (PA-4050, PA-4060)

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 administration
- Shared policies (Panorama)
- Syslog & SNMPv2
- Customizable administrator login banner
- XML-based REST API

HARDWARE SPECIFICATIONS

I/O	(16) 10/100/1000 + (8) Gigabit SFP (PA-4050, PA-4020), (4) 10 Gigabit XFP + (4) Gigabit SFP (PA-4060)
Management I/O	(2) 10/100/1000 high availability, (1) 10/100/1000 out-of-band management, (1) DB9 console port
Power supply (Avg/max power consumption)	Redundant 400W AC (175W/200W)
Input voltage (Input frequency)	100-240Vac (50-60Hz)
Max input current	50A@230Vac, 30A@120Vac
Rack mountable (dimensions)	2U, 19" standard rack (3.5"H x 16.5"D x 17.5"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-4060	PA-4050	PA-4020
Platform	PAN-PA-4060	PAN-PA-4050	PAN-PA-4020
Annual threat prevention subscription	PAN-PA-4060-TP	PAN-PA-4050-TP	PAN-PA-4020-TP
Annual URL filtering subscription	PAN-PA-4060-URL2	PAN-PA-4050-URL2	PAN-PA-4020-URL2
VSYS upgrade (10 additional)			PAN-PA-4020-VSYS-10
VSYS upgrade (50 additional)	PAN-PA-4060-VSYS-50	PAN-PA-4050-VSYS-50	
VSYS upgrade (100 additional)	PAN-PA-4060-VSYS-100	PAN-PA-4050-VSYS-100	

For additional information on the PA-4000 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

PA-5000 Series

The PA-5000 Series 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, 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-5060

PA-5050

PA-5020

The Palo Alto Networks™ PA-5000 Series is comprised of three high performance platforms, the PA-5020, the PA-5050 and the PA-5060, all of which are targeted at high speed Internet gateway and datacenter deployments. The PA-5000 Series manages multi-Gbps traffic flows using dedicated processing and memory for networking, security, threat prevention and management.

A 20 Gbps backplane smoothes the pathway between dedicated processors, and the physical separation of data and control plane ensures that management access is always available, irrespective of the traffic load.

The controlling element of the PA-5000 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 and management features.

KEY PERFORMANCE SPECIFICATIONS	PA-5060	PA-5050	PA-5020
Firewall throughput	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
IPSec VPN tunnels/tunnel interfaces	8,000	4,000	2,000
SSL VPN Users	20,000	10,000	5,000
Virtual routers	225	125	20
Virtual systems (base/max*)	25/225*	25/125*	10/20*
Security zones	900	500	80
Max number of policies	40,000	20,000	10,000

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

paloalto NETWORKS

NETWORKING	PA-5060	PA-5050	PA-5020
• Modes	L2, L3, Tap, Virtual Wire (transparent mode)	L2, L3, Tap, Virtual Wire (transparent mode)	L2, L3, Tap, Virtual Wire (transparent mode)
• Forwarding table size (entries per device/per VR)	64,000 / 64,000	64,000 / 64,000	64,000 / 64,000
• Policy-based forwarding	Supported	Supported	Supported
• Point-to-Point Protocol over Ethernet (PPPoE)	Supported	Supported	Supported
• Jumbo frames	Supported	Supported	Supported
• Max NAT rules (DIPP)	450	250	200
• Dynamic IP and port pool	254	254	254
• Dynamic IP pool	16,234	16,234	16,234
• NAT Modes	1:1 NAT, n:n NAT, m:n NAT	1:1 NAT, n:n NAT, m:n NAT	1:1 NAT, n:n NAT, m:n NAT
• PAT- Unique destination IPs per source port and IP	8	8	8
• Max interfaces	4,096	4,096	2,048
• Aggregate Interfaces (802.3ad)	Supported	Supported	Supported
• Physical interfaces mapped to VWs	Supported	Supported	Supported
• DHCP server/DHCP relay	up to 3 servers	up to 3 servers	up to 3 servers
• Max Addresses: 64,000	64,000	64,000	64,000
• IPv6 neighbor table size	5,000	5,000	2,000
• MAC table size/device	32,000	32,000	20,000

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: SHA1, MD5

DATA FILTERING

- Control unauthorized data transfer (data patterns and file types)
- Drive-by download protection

MANAGEMENT, REPORTING, VISIBILITY TOOLS

- Integrated web interface, CLI or central management (Panorama)
- Syslog and SNMPv2
- 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

NETCONNECT SSL VPN (REMOTE ACCESS)

- Transport: IPSec with SSL fall-back
- Authentication: LDAP, SecurID, or local DB
- Client OS: Macintosh, Windows XP, Windows Vista (32 and 64 bit), Windows 7 (32 and 64 bit)

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

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

GLOBALPROTECT

- GlobalProtect Gateway
- GlobalProtect Portal
- Client OS: Windows XP, Windows Vista (32/64 bit), Windows 7 (32 bit)

URL FILTERING (SUBSCRIPTION REQUIRED)

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

HARDWARE SPECIFICATIONS	PA-5060/PA-5050	PA-5020
Platform	(12) 10/100/1000 + (8) Gigabit SFP (4), 10 Gigabit SFP+	(12)10/100/1000 + (8) Gigabit SFP
Power supply (Avg/max power consumption)	Redundant 450W AC (175W/200W)	
Input voltage (Input frequency)	100-240Vac (50-60Hz)	
Max input current	50A@230Vac; 30A@120Vac	
Safety	UL, CUL, CB	
EMI	FCC Class A, CE Class A, VCCI Class A, TUV	
Rack mountable (dimensions)	2U, 19" standard rack (3.5"H x 16.5"D x 17.5"W)	
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-5060	PA-5050	PA-5020
Platform	PAN-PA-5060	PAN-PA-5050	PAN-PA-5020
Solid State Disk Drives (120 GB)	PAN-PA-5000-SSD-120	PAN-PA-5000-SSD-120	PAN-PA-5000-SSD-120
Solid State Disk Drives (240 GB)	PAN-PA-5000-SSD-240	PAN-PA-5000-SSD-240	PAN-PA-5000-SSD-240
AC Power Supply	PAN-PA-5000-PWR-AC	PAN-PA-5000-PWR-AC	PAN-PA-5000-PWR-AC
DC Power Supply	PAN-PA-5000-PWR-DC	PAN-PA-5000-PWR-DC	PAN-PA-5000-PWR-
DCFan Tray	PAN-PA-5000-FAN	PAN-PA-5000-FAN	PAN-PA-5000-FAN
Fan Filter	PAN-PA-5000-FLTR	PAN-PA-5000-FLTR	PAN-PA-5000-FLTR

For additional information on the PA-5000 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

Services.

PA-7050

PA-7050

The Palo Alto Networks® PA-7050 is designed to protect datacenters and high-speed networks with firewall throughput of up to 120 Gbps and full threat prevention at speeds of up to 100 Gbps. The PA-7050 is a modular chassis, allowing you to scale performance and capacity by adding up to six network processing cards as your requirements change; yet it is a single system, making it as easy to manage as all of our other appliances.

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 Mac OS X, Linux, Android or iOS platforms.

- Deploy consistent policies to local and remote users running Microsoft Windows,

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 100 malicious behaviors, then automatically create and deliver protection in the next content up

PERFORMANCE AND CAPACITIES [1]	PA-7050 SYSTEM	PA-7000-20G-NPC
Firewall throughput (App-ID enabled)	120 Gbps	20 Gbps
Threat prevention throughput (DSRI Enabled [2])	100 Gbps	16 Gbps
Threat prevention throughput	60 Gbps	10 Gbps
IPSec VPN throughput	24 Gbps	4 Gbps
Max sessions	24,000,000	4,000,000
New sessions per second	720,000	120,000
Virtual systems (base/max [3])	25/225	N/A

[1]

DELIVERING LINEAR SCALABILITY AND PERFORMANCE

The PA-7050 achieves predictable datacenter level protection and performance by applying more than 400 function-specific processors distributed across the following chassis subsystems:

- Network Processing Card (NPC): Each NPC delivers 20 Gbps of firewall performance using multi-core security optimized processors, along with dedicated high-speed networking and content inspection processors. Up to six NPCs, each with 24 traffic interfaces are supported in the PA-7050.
- **Switch Management Card (SMC):** The SMC is comprised of three elements that are key to delivering predictable datacenter protection and performance: the First Packet Processor, the 1.2 Tbps switch fabric and the management subsystem.
  - **First Packet Processor (FPP):** The FPP utilizes dedicated processing to apply intelligence to the incoming traffic, directing it to the appropriate processing resource to maximize throughput efficiency.
  - **High Speed Switch Fabric:** The 1.2 Tbps switch fabric means that each NPC has access to approximately 100 Gbps of traffic capacity, ensuring that performance and capacity will scale in a linear manner as NPCs are added to the PA-7050.
  - **Management Subsystem:** Unified point of contact for managing all aspects of the PA-7050.
- **Log Processing Card (LPC):** The LPC uses multi-core processors and 2TB of RAID 1 storage to offload the logging related activities without impacting the processing required for other management related tasks. The LPC allows you to generate on-system queries and reports from the most recent logs collected or forward them to a syslog server for archiving or additional analysis.

The PA-7050 delivers performance and scalability by intelligently applying all available networking and security processing power to application layer traffic classification and threat protection tasks. Orchestrating this ballet of session management tasks is the First Packet Processor which constantly tracks the shared pool of processing and I/O resources across all of the NPCs. When the FPP determines that additional processing resources are available, traffic is intelligently directed across the high-speed switch fabric to that location, even if it resides on a separate NPC. The FPP is the key to delivering linear scalability to the PA-7050, working in conjunction with each of the network processors on the NPCs to utilize all of the available computing resources as a single, cohesive system. This means that as NPCs are added, no traffic engineering changes are required in order to utilize the added capacity.

The controlling element of the PA-7050 is PAN-OS™, a securityspecific 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—the 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. All traffic classification, content inspection, policy lookup and execution are performed in a single pass. The single pass software architecture, when combined with the processing power of the PA-7050, ensures that you achieve predictable throughput.

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

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

The PA-7050 supports a wide range of networking features that allows you to more easily integrate our security features into your existing network. To view additional information on the PA-7050 security features and associated capacities, please visit **www.paloaltonetworks.com/products**

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

PAN_SS_PA7050_022614