PA-7000 Series

Key Security Features:

CLASSIFY ALL APPLICATIONS, ON ALL PORTS, ALL THE TIME.

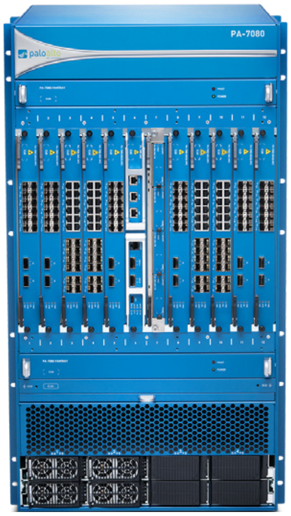
- Identify the application, regardless of port, encryption (SSL or SSH), or evasive technique employed.
- Use the application, not the port, as the basis for all of your safe enablement policy decisions: allow, deny, schedule, inspect, and apply traffic shaping.
- Categorize unidentified applications for policy control, threat forensics or App-ID™ development.

ENFORCE SECURITY POLICIES FOR ANY USER, AT ANY LOCATION.

- Deploy consistent policies to local and remote users running Windows®, Mac® OS X®, Linux®, Android®, or iOS platforms.
- Agentless integration with Microsoft® Active Directory® and Terminal Services, LDAP, Novell® eDirectory™ and Citrix®.
- Easily integrate your firewall policies with NAC, 802.1X wireless, proxies, and NAC solutions.

PREVENT KNOWN AND UNKNOWN THREATS.

- Block a range of known threats, including exploits, malware, and spyware, across all ports, regardless of common threat evasion tactics employed.
- Limit the unauthorized transfer of files and sensitive data, and control non-work-related Web surfing.
- Identify unknown malware, analyze it based on hundreds of malicious behaviors, and then automatically create and deliver protection



PA-7080

PA-7050

Redefining high-performance network security, the PA-7000 Series offers the perfect blend of power, intelligence and simplicity. Power derived from a proven architecture that blends ultra-efficient software with nearly 700 function-specific processers for networking, security, content inspection and management. Intelligence that maximizes security processing resource utilization and automatically scales as new computing power becomes available. Simplicity defined by a single system approach to management and licensing.

PERFORMANCE AND CAPACITIES[1]	PA-7080 SYSTEM	PA-7050 SYSTEM	PA-7000 NPC
Firewall throughput (App-ID enabled)	200 Gbps	120 Gbps	20 Gbps
Threat prevention throughput (DSRI Enabled[2])	160 Gbps	100 Gbps	16 Gbps
Threat prevention throughput	100 Gbps	60 Gbps	10 Gbps
IPSec VPN throughput	80 Gbps	48 Gbps	8 Gbps
Max sessions	40,000,000	24,000,000	4,000,000
New sessions per second	1,200,000	720,000	120,000
Virtual systems (base/max[3])	25/225*	25/225*	–

[1] Performance and capacities are measured under ideal testing conditions using PAN-OS® 7.0.

[2] Disable Server Response Inspection (DSRI).

[3] Adding virtual systems to the base quantity requires a separately purchased license.

THE PA-7000 SERIES ARCHITECTURE

The PA-7000 Series is powered by a scalable architecture for the express purpose of applying the appropriate type and volume of processing power to the key functional tasks of networking, security, content inspection and management. The PA-7000 Series chassis intelligently distributes the computational processing demands of networking, security, threat prevention and management across three subsystems, each with massive amounts of computing power and dedicated memory.

- **Network Processing Card (NPC):** The NPC is dedicated to executing all security-related tasks including networking, traffic classification and threat prevention. Each NPC has up to 67 processing cores, all focused on the singular task of protecting your network at up to 20 Gbps per NPC. Scaling throughput and capacity to the maximum 200 Gbps on the PA-7080 or 120 Gbps on the PA-7050 is as easy as adding a new NPC and allowing the system to determine the best use of the newly added processing power. Addressing the increasing demand for higher density 10 Gig and 40 Gig connectivity, as well as the more common 10 Gbps and 1 Gbps interface alternatives, two NPC options are available and can be used interchangeably.
- **Switch Management Card (SMC):** Acting as the control center of the PA-7000 Series, the SMC intelligently oversees all traffic, and executes all management functions, using a combination of three elements: the First Packet Processor, a high-speed backplane, and the management subsystem.
  - First Packet Processor (FPP) is the key to maximizing performance and delivering linear scalability to the PA-7000 Series. The FPP constantly tracks the shared pool of available processing and I/O resources across all NPCs, intelligently directing inbound traffic to any underutilized processing. This means that as NPCs are added to increase performance and capacity, no traffic management changes are required, nor is it necessary to re-cable or reconfigure your PA-7000 Series.
  - High-speed backplane operating at 1.2 Tbps means that each of the network processing cards has access to approximately 100 Gbps of traffic capacity, ensuring that performance and capacity will scale in a linear manner as your requirements increase.
  - Management subsystem acts as a dedicated point of contact for controlling all aspects of the PA-7000 Series.
- **Log Processing Card (LPC):** The LPC is a dedicated subsystem designed to perform the critical task of managing the high volume of logs generated by the PA-7000 Series. The LPC is unique to the PA-7000 Series and uses two high-speed, multicore processors and 2 TB of RAID 1 storage to offload the logging-related activities without impacting the processing required for other management or traffic processing-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-7000 Series is managed as a single, unified system, which enables you to easily direct all of the available resources to the singular task of protecting your data. The controlling element of the PA-7000 Series is an ultra-efficient, single-pass classification engine that analyzes all traffic traversing the appliance to immediately determine three critical elements that become the heart of your security policy; the application identity regardless of port, the content, malicious or otherwise, and the user identity.

The benefits of determining the application, content, and user in a single pass, and basing your security policy on those business relevant elements, are threefold. The first is an improvement in your security posture introduced by more directly mapping your security policies to key business initiatives while reducing the administrative overhead associated with security policies. The third benefit is a reduction in latency brought on by the elimination of the redundant scanning and look-up tasks commonly found in alternative offerings. To help further simplify administrative effort, annual support and subscription fees for the PA-7000 Series are system-wide, which means that no matter how many NPCs are installed, the annual fees are constant, providing you with a predictable, annual cost structure.

The PA-7000 Series supports a wide range of networking features that allow 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

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	PA-7000 NPC	PA-7080 FULL SYSTEM	PA-7050 FULL SYSTEM
NPC Option 1:	(2) QSFP+, (12) SFP+	(20) QSFP+, (120) SFP+	(12) QSFP +, (72) SFP+
NPC Option 2:	(12) 10/100/1000, (8) SFP, (4) SFP+	(120) 10/100/1000, (80) SFP, (40) SFP+	(72) 10/100/1000, (48) SFP, (24) SFP+
Management I/O	-	(2) 10/100/1000,(2) QSFP+ high availability, (1) 10/100/1000 out-of-band management, (1) RJ45 console port	
Storage options	-	80 GB SSD System Drive, 4x1 TB HDD on Log Processing Card	
Storage capacity	-	2 TB RAID1	
AC power supplies (system avg/max power consumption)	-	4x2500W AC (2400W / 2700)	
Max BTU/hr	-	20,132	10,236
Input voltage (input frequency)	-	200-240VAC (50-60Hz); -40 to -72VDC	
Max current consumption	-	12A@220VAC; 60A@-40VDC	
Max inrush current	-	200A	
Mean time between failure (MTBF)	Configuration dependent; contact your Palo Alto Networks representative for MTBF details.		
Rack mountable (dimensions)	-	19U, 19" standard rack (32.22"H x 19"W x 24.66"D)	9U, 19" standard rack (15.75"H x 19"W x 24"D)
Weight (stand-alone device /as shipped)	-	299.3lbs AC / 298.3lbs DC	187.4lbs AC / 185lbs DC
Safety	-	cTUVus,CB	
EMI	-	FCC Class A, CE Class A, VCCI Class A	
Certifications	-	NEBS Level 3	
ENVIRONMENT			
Operating temperature	-	32° to 122° F, 0° to 50° C	
Non-operating temperature	-	-4° to 158° F, -20° to 70° C	

paloalto NETWORKS®

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