PA-7000 Series

Palo Alto Networks PA-7000 Series ML-Powered Next-Generation Firewalls enable enterprise-scale organizations and service providers to deploy security in high-performance environments, such as large data centers and high-bandwidth network perimeters. Designed to handle growing throughput needs for application-, user-, and device-generated data, these systems offer amazing performance, prevention capabilities to stop the most advanced cyberattacks, and high-throughput decryption to stop threats hiding under the veil of encryption. Built to maximize security-processing resource utilization and automatically scale as new computing power becomes available, the PA-7000 Series offers simplicity defined by a single-system approach to management and licensing.

Key Security Features

Classifies all applications, on all ports, all the time

- Identifies the application, regardless of port, SSL/SSH encryption, or evasive technique employed.
- Uses the application, not the port, as the basis for all your safe enablement policy decisions.
- Categorizes unidentified applications for policy control, threat forensics, or App-ID™ technology development.
- Provides full visibility into the details of all TLS-encrypted connections and stops threats hidden in encrypted traffic, including traffic that uses TLS 1.3 and HTTP/2 protocols.

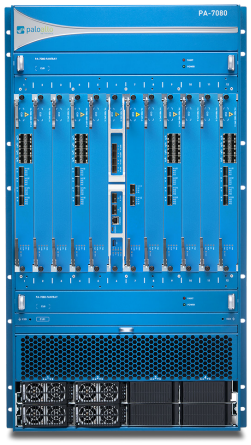
Enforces security policies for any user, at any location

- Deploys consistent policies to Windows®, macOS®, Linux, Android®, or Apple iOS platforms.
- Enables agentless integration with Microsoft Active Directory® and Terminal Services, LDAP, Novell eDirectory™, and Citrix.
- Easily integrates your firewall policies with 802.1X wireless, proxies, network access control, and any other source of user identity information.

Extends native protection across all attack vectors with cloud-delivered security subscriptions

- **Threat Prevention**—inspects all traffic to automatically block known vulnerabilities, malware, vulnerability exploits, spyware, command and control (C2), and custom intrusion prevention system (IPS) signatures.
- **WildFire® malware prevention**—protects against unknown file-based threats, delivering automated prevention in seconds for most new threats across networks, endpoints, and clouds.
- **URL Filtering**—prevents access to malicious sites and protects users against web-based threats.
- **DNS Security**—detects and blocks known and unknown threats over DNS while predictive analytics disrupt attacks using DNS for C2 or data theft.
- **IoT Security**—discovers all unmanaged devices in your network, identifies risks and vulnerabilities, and automates enforcement policies for your ML-Powered NGFW using a new Device-ID™ policy construct.

PA-7050



PA-7080

PA-7000 Series Architecture

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

Table 1: PA-7000 Series Performance and Capacities[1]

	PA-7080[2]	PA-7050[2]	PA-7000 DPC-A	PA-7000 NPC-100G	PA-7000 NPC-XM
Firewall throughput (HTTP/appmix)[3]	644/700 Gbps	390/416 Gbps	77/86 Gbps	59/66 Gbps	17.6/20.0 Gbps
Threat Prevention throughput (DSRI enabled)[4]	650 Gbps	396 Gbps	71.2 Gbps	55.7 Gbps	16.7 Gbps
Threat Prevention throughput (HTTP/appmix)[5]	362/430 Gbps	210/258 Gbps	41/49 Gbps	29/37 Gbps	9.3/12.5 Gbps
IPsec VPN throughput[6]	328 Gbps	200 Gbps	36 Gbps	28 Gbps	9 Gbps
Max sessions	416M	245M	43M	32M	8M
New sessions per second[7]	6M	4M	925,000	623,000	208,000
Virtual systems (base/max)[8]	25/225	25/225	–	–	–

1. Results were measured on PAN-OS 10.0.
2. Results in this column were derived from an optimum combination of DPC-A and NPC-100G cards populated in all available slots.
3. Throughput is measured with App-ID and logging enabled, with 64 KB HTTP/appmix transactions.
4. Disable Server Response Inspection (DSRI) throughput is measured with App-ID, IPS, antivirus, anti-spyware, WildFire, file blocking, and logging enabled, utilizing 64 KB HTTP transactions.
5. Threat Prevention throughput measured with App-ID, IPS, antivirus, anti-spyware, WildFire, and logging enabled, utilizing 64 KB HTTP/appmix transactions.
6. IPsec VPN throughput is measured with 64 KB HTTP transactions and logging enabled.
7. New sessions per second is measured with application override, utilizing 1 byte HTTP transactions.
8. The base system includes 25 virtual systems at no cost, and up to 200 additional licenses may be purchased. The maximum number of virtual systems supported is 225.

Network Processing Card

The Network Processing Card (NPC) is dedicated to executing all packet-processing tasks, including networking, traffic classification, and threat prevention. Each NPC has 64 (first generation: two 32-core CPUs) or 144 (second generation: three 48-core CPUs) processing cores with offload processing, all focused on protecting your network at up to 66 Gbps per NPC.

To address growing demand for higher capacity 40 Gbps and 100 Gbps connectivity, as well as the more common 10 Gbps interface alternatives, three NPC options are available—the first-generation NPC-20GXM and NPC-20GQXM, and the second-generation 100G-NPC—that can be used interchangeably with the first-generation Switch Management Card.

Data Processing Card

The Data Processing Card (DPC-A) maximizes security processing by packing 192 processing cores (second generation: four 48-core CPUs) on a single card capable of protecting your network at up to 86 Gbps per DPC-A. The DPC-A leverages the design of the second-generation NPC-100G, adding a fourth compute complex and an additional offload processor in place of Ethernet I/O.

Scaling throughput to the maximum 700 Gbps on the PA-7080, or 416 Gbps on the PA-7050, is as easy as adding a new DPC-A or NPC and allowing the system to determine the best use of the new processing power.

The DPC-A can be used with the first- or second-generation Switch Management Cards.

Switch Management Card

Acting as the control center of the PA-7000 Series, the Switch Management Card (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- and second-generation SMCs are available, with the second generation offering significant improvements in the functionality of all three elements.

First Packet Processor

The key to maximizing performance and delivering linear scalability to the PA-7000 Series, the First Packet Processor (FPP) constantly tracks the shared pool of available processing and I/O resources across all NPCs and DPCs, intelligently directing inbound traffic to underutilized processors. As processing cards 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

Each processing card has access to more than 100 Gbps of non-blocking traffic capacity with a high-speed backplane. The Management subsystem acts as a dedicated point of contact for controlling all aspects of the PA-7000 Series.

Management Subsystem

This subsystem acts as a dedicated point of contact for controlling all aspects of the PA-7000 Series.

Dedicated Logging Card

The Logging Card, an integral part of every system, utilizes a dual CPU design, creating a dedicated subsystem to manage the high volume of logs the PA-7000 Series generates. Two log cards are available: a first-generation Log Processing Card (LPC) and a second-generation Log Forwarding Card (LFC). The LPC uses up to 4 TB of RAID1 storage to offload logging-related activities, enabling you to run queries and reports from the most recent logs collected. The LFC is a high-performance card dedicated to exporting log messages. Both allow you to forward logs to Panorama™ network security management, Cortex™ Data Lake, and Syslog for offline analysis. The LPC supports mixed configurations of all processing cards while the LFC is optimized for use with the second-generation SMC-B, 100G-NPC, and DPC-A.

The PA-7000 Series is managed as a single, unified system, enabling you to easily direct all available resources to protect your data. The controlling element of the PA-7000 Series is PAN-OS®, which natively classifies all traffic, inclusive of applications, threats, and content, and then ties that traffic to the user regardless of location or device type. The application, content, and user—in other words, the elements that run your business—then serve as the basis of your security policies, resulting in improved security posture, reduced incident response time, and lower administrative overhead associated with keeping security policies current in a highly dynamic environment.

Table 2: PA-7000 Series Hardware Specifications

	PA-7000 NPC	PA-7080 Full System	PA-7050 Full System
100G-NPC (PA-7000-100G-NPC-A)	SFP/SFP+ (8), QSFP+/QSFP28 (4)	SFP/SFP+ (80), QSFP+/QSFP28 (40)	(48) SFP/SFP+. (24) QSFP+/QSFP28
20G-NPC XM Option 1: (PA-7000-20GQXM-NPC)	QSFP+ (2), SFP+ (12)	QSFP+ (20), SFP+ (120)	(12) QSFP +, (72) SFP+
20G-NPC XM Option 2: (PA-7000-20GXM-NPC)	10/100/1000 (12), SFP (8), SFP+ (4)	10/100/1000 (120), SFP (80), SFP+ (40)	(72) 10/100/1000, (48) SFP, (24) SFP+
Management I/O (second generation)	–	SFP MGT (2), SFP HA1 (2), HSCI HA2/HA3 QSFP+/QSFP28 (2), RJ45 serial console (1), Micro USB serial console (1)	
Management I/O (first generation)	–	10/100/1000 (2), QSFP+ high availability (2), 10/100/1000 out-of-band management (1), RJ45 console port (1)	

Table 2: PA-7000 Series Hardware Specifications (continued)			
	PA-7000 NPC	PA-7080 Full System	PA-7050 Full System
Storage capacity (second generation)	–	240 GB SSD system drive, RAID1 (2)	
Storage options (first generation)	–	120 GB SSD system drive (1), 1 TB default or 2 TB optional HDD on LPC, RAID1 (4)	
AC input voltage	–	100–240 VAC (50–60 Hz)	100–240 VAC (50–60 Hz)
Rated input current	–	65-27A	27-12A
AC power supply output	–	2500 W @ 240 VAC 1200 W @ 120 VAC	2500 W @ 240 VAC 1200 W @ 120 VAC
DC input voltage	–	-40 to -60 VDC	-40 to -60 VDC
Rated input current	–	135A	60A
DC power output	–	2500 W / power supply	2500 W / power supply
Max current / power supply	–	12 A @ 240 VAC In 75 A @ >40 VDC In	16 A @ 180 VAC In 75 A @ 37.5 VDC In
Power supplies (base/max)	–	4/8	4/4
Max inrush current / power supply	–	30 AAC / 100 ADC peak	50 AAC / 75 ADC peak
Mean time between failure (MTBF)	Configuration dependent; contact your Palo Alto Networks representative for MTBF details.		
Max BTU/hr	–	20,132	10,236
Rack mount (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 (standalone device/ as shipped)	–	299.3 lbs. AC / 298.3 lbs. DC	187.4 lbs. AC / 185 lbs. 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	

To view additional information about the features and associated capacities of the PA-7000 Series, please visit paloaltonetworks.com/network-security/next-generation-firewall/pa-7000-series.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com