PA-7000 SERIES

Palo Alto Networks PA-7000 Series 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.

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.

Prevents known and unknown threats

- Blocks a range of known threats—including exploits, malware, spyware, and command and control—across all ports.
- Limits the unauthorized transfer of files and sensitive data, and safely enables non-work-related web surfing.
- Identifies unknown malware, analyzes it based on hundreds of malicious behaviors, and then automatically creates and delivers protection.

PA-7050
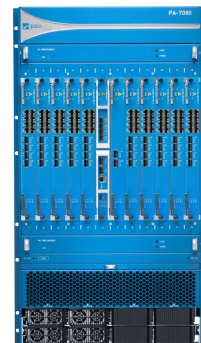
PA-7080

Performance and Capacities	PA-7080	PA-7050	PA-7000 NPC-100G	PA-7000 NPC-XM
Firewall throughput (HTTP/appmix)[1]	630/720 Gbps	380/430 Gbps	63/72 Gbps	19/20 Gbps
Threat Prevention throughput (DSRI enabled)[2]	610 Gbps	366 Gbps	61 Gbps	18 Gbps
Threat Prevention throughput (HTTP/appmix)[3]	294/350 Gbps	176/210 Gbps	29/35 Gbps	9/12 Gbps
IPsec VPN throughput[4]	240 Gbps	144 Gbps	24 Gbps	8 Gbps
Max sessions	320M	192M	32M	8M
New sessions per second[5]	4.8M	2.9M	480,000	100,000
Virtual systems (base/max)[6]	25/225*	25/225*	–	–

1. Throughput is measured with App-ID and logging enabled, with 64 KB HTTP/appmix transactions
2. 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
3. Threat Prevention throughput measured with App-ID, IPS, antivirus, anti-spyware, WildFire, and logging enabled, utilizing 64 KB HTTP/appmix transactions
4. IPsec VPN throughput is measured with 64 KB HTTP transactions
5. New sessions per second is measured with application override, utilizing 1 byte HTTP transactions
6. Adding virtual systems to the base quantity requires a separately purchased license

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.

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 between 64 (first generation) and 144 (second generation) processing cores, all focused on protecting your network at up to 72 Gbps per NPC. Scaling the throughput to the maximum 720 Gbps on the PA-7080, or 430 Gbps on the PA-7050, is as easy as adding a new NPC and allowing the system to determine the best use of the new processing power. 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 NPC-100G—that can be used interchangeably with the first-generation Switch Management Card.

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 back-plane, and the management subsystem. First- and second-generation SMCs are available, with the second generation offering significant improvements in the following three areas of functionality:

- 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 processors. 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 means each NPC has access to more than 100 Gbps of non-blocking traffic capacity. With dedicated capacity for each NPC slot, performance scales in a linear manner. As your requirements increase, you can add NPCs, increasing aggregate system capacity without backplane contention.

- Management 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 RAID 1 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, Logging Service, and Syslog for offline analysis. The LPC supports mixed configurations of NPC-20G and NPC-100G while the LFC is optimized for use with the second-generation SMC and NPC-100G.

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.

To help further simplify administrative effort, annual support and subscription fees for the PA-7000 Series are system-wide. Annual fees are constant no matter how many NPCs are installed, providing a predictable cost structure.

Hardware Features

Hardware Specifications	PA-7000 NPC	PA-7080 Full System	PA-7050 Full System
NPC-100G (PA-7000-100G-NPC-A)	(8) SFP/SFP+ (4) QSFP+ /QSFP28	(80) SFP/SFP+ (40) QSFP+/QSFP28	(48) SFP/SFP+. (24) QSFP+/QSFP28
NPC-20G XM Option 1[1]: (PA-7000-20GQXM-NPC)	(2) QSFP+, (12) SFP+	(20) QSFP+, (120) SFP+	(12) QSFP +, (72) SFP+
NPC-20G XM Option 2[1]: (PA-7000-20GXM-NPC)	12x10/100/ 1000, (8) SFP, (4) SFP+	(120) 10/100/1000, (80) SFP, (40) SFP+	(72) 10/100/1000, (48) SFP, (24) SFP+
Management I/O (second generation)	–	(2) SFP MGT, (2) SFP HA1, (2) HSCI HA2/HA3 QSFP+/QSFP28 (1) RJ45 serial console, (1) micro-USB serial console	
Management I/O (first generation)	–	(2) 10/100/1000, (2) QSFP+ high availability, (1) 10/100/1000 out-of-band management, (1) RJ45 console port	
Storage capacity (second generation)	–	(2) 240 GB SSD System Drive, RAID1	
Storage options (first generation)	–	(1) 80 GB SSD System Drive, (4) 1 TB default or (4) 2 TB optional HDD on Log Processing Card, RAID	
AC input voltage (input Hz)	–	90–305VAC (47–66 Hz)	90–264VAC (47–63 Hz)
AC power supply output	–	2500 W @ 240VAC 1200 W @ 120VAC	2500 W @ 240VAC 1200 W @ 120VAC
DC input voltage	–	-36 to -75VDC	-40 to -72VDC
DC power output	–	2500 W / power supply	2500 W / power supply
Max current / power supply	–	12ADC @ 240VAC In 75ADC @ >40VDC In	16A @ 180VAC In 75A @ 37.5VDC In
Power supplies (base/max)	–	4/8	4/4
Max inrush current / power supply	–	30AAC / 100ADC peak	50AAC / 75ADC 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 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)	–	299.3 lbs. AC / 298.3 lbs. DC	187.4 lbs AC / 185 lbs DC
Safety	–	cTUVus, cCSAus, 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	

The PA-7000 Series supports a wide range of networking features that enable you to more easily integrate our security features into your existing network.

Networking Features

Interface Modes	VLANs
L2, L3, tap, virtual wire (transparent mode)	802.1Q VLAN tags per device/per interface: 4,094/4,094
Routing	Aggregate interfaces (802.3ad), LACP
OSPFv2/v3 with graceful restart, BGP with graceful restart, RIP, static routing	**Network Address Translation**
Policy-based forwarding	NAT modes (IPv4): static IP, dynamic IP, dynamic IP and port (port address translation)
Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, and v3	NAT64, NPTv6
Bidirectional Forwarding Detection (BFD)	Additional NAT features: dynamic IP reservation, tunable dynamic IP and port oversubscription
IPv6	**High Availability**
L2, L3, tap, virtual wire (transparent mode)	Modes: active/active, active/passive
Features: App-ID, User-ID, Content-ID, WildFire, and SSL decryption	Failure detection: path monitoring, interface monitoring
IPsec VPN	
Key exchange: manual key, IKEv1, and IKEv2 (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	
GlobalProtect large-scale VPN (LSVPN) for simplified configuration and management	

To learn more about the security features and associated capacities of the PA-7000 Series, please visit www.paloaltonetworks.com/products.