STRATA™
BY PALO ALTO NETWORKS

Highlights

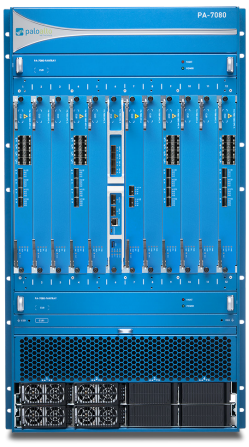
- World's first ML-Powered NGFW
- Nine-time Leader in the Gartner Magic Quadrant® for Network Firewalls
- Leader in The Forrester Wave™: Enterprise Firewalls, Q3 2020
- Highest Security Effectiveness score in the 2019 NSS Labs NGFW Test Report, with 100% of evasions blocked
- Operates on a unified and scalable architecture
- Delivers 5G-native security built to safeguard service provider and enterprise 5G transformation
- Extends visibility and security to all devices, including unmanaged IoT devices, without the need to deploy additional sensors
- Supports high availability with active/active and active/passive modes
- Delivers predictable performance with security services

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.

The controlling element of the PA-7000 Series is PAN-OS®, the same software that runs all Palo Alto Networks Next-Generation Firewalls. PAN-OS 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.

PA-7050



PA-7080

Key Security and Connectivity Features

ML-Powered Next-Generation Firewall

- Embeds machine learning (ML) in the core of the firewall to provide inline signatureless attack prevention for file-based attacks while identifying and immediately stopping never-before-seen phishing attempts.
- Leverages cloud-based ML processes to push zero-delay signatures and instructions back to the NGFW.
- Uses behavioral analysis to detect internet of things (IoT) devices and make policy recommendations; cloud-delivered and natively integrated service on the NGFW.
- Automates policy recommendations that save time and reduce the chance of human error.

Identifies and categorizes all applications, on all ports, all the time, with full Layer 7 inspection

- Identifies the applications traversing your network irrespective of port, protocol, evasive techniques, or encryption (TLS/SSL).
- Uses the application, not the port, as the basis for all your safe enablement policy decisions: allow, deny, schedule, inspect, and apply traffic-shaping.
- Offers the ability to create custom App-IDs for proprietary applications or request App-ID development for new applications from Palo Alto Networks.
- Identifies all payload data within the application, such as files and data patterns, to block malicious files and thwart data exfiltration attempts.
- Creates standard and customized application usage reports, including software-as-a-service (SaaS) reports that provide insight into all SaaS traffic—sanctioned and unsanctioned—on your network.
- Enables safe migration of legacy Layer 4 rule sets to App-ID-based rules with built-in Policy Optimizer, giving you a rule set that is more secure and easier to manage.

Enforces security for users at any location, on any device, while adapting policy in response to user activity

- Enables visibility, security policies, reporting, and forensics based on users and groups—not just IP addresses.
- Easily integrates with a wide range of repositories to leverage user information: wireless LAN controllers, VPNs, directory servers, SIEMs, proxies, and more.
- Allows you to define Dynamic User Groups (DUGs) on the firewall to take time-bound security actions without waiting for changes to be applied to user directories.
- Applies consistent policies irrespective of users' locations (office, home, travel, etc.) and devices (iOS and Android® mobile devices, macOS®, Windows®, Linux desktops, laptops; Citrix and Microsoft VDI and Terminal Servers).
- Prevents corporate credentials from leaking to third-party websites, and prevents reuse of stolen credentials by enabling multi-factor authentication (MFA) at the network layer for any application, without any application changes.
- Provides dynamic security actions based on user behavior to restrict suspicious or malicious users.

Prevents malicious activity concealed in encrypted traffic

- Inspects and applies policy to TLS/SSL-encrypted traffic, both inbound and outbound, including for traffic that uses TLS 1.3 and HTTP/2.
- Offers rich visibility into TLS traffic, such as amount of encrypted traffic, TLS/SSL versions, cipher suites, and more, without decrypting.
- Enables control over use of legacy TLS protocols, insecure ciphers, and incorrectly configured certs to mitigate risks.
- Facilitates easy deployment of decryption and lets you use built-in logs to troubleshoot issues, such as applications with pinned certs.
- Lets you enable or disable decryption flexibly based on URL category and source and destination zone, address, user, user group, device, and port, for privacy and regulatory compliance purposes.
- Allows you to create a copy of decrypted traffic from the firewall (i.e., decryption mirroring) and send it to traffic collection tools for forensics, historical purposes, or data loss prevention (DLP).

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**—unifies inline machine learning protection with robust cloud-based analysis to instantly prevent new threats in real time as well as discover and remediate evasive threats faster than ever.
- **URL Filtering**—prevents access to malicious sites and protects users against web-based threats, including credential phishing attacks.
- **DNS Security**—detects and blocks known and unknown threats over DNS (including data exfiltration via DNS tunneling), prevents attackers from bypassing security measures, and eliminates the need for independent tools or changes to DNS routing.
- **IoT Security**—discovers all unmanaged devices in your network quickly and accurately with ML, without the need to deploy additional sensors. Identifies risks and vulnerabilities, prevents known and unknown threats, provides risk-based policy recommendations, and automates enforcement.

Delivers a unique approach to packet processing with Single-Pass Architecture

- Performs networking, policy lookup, application and decoding, and signature matching—for any and all threats and content—in a single pass. This significantly reduces the amount of processing overhead required to perform multiple functions in one security device.
- Enables consistent and predictable performance when security subscriptions are enabled.
- Avoids introducing latency by scanning traffic for all signatures in a single pass, using stream-based, uniform signature matching.

Enables SD-WAN functionality

- Allows you to easily adopt SD-WAN by simply enabling it on your existing firewalls.
- Enables you to safely implement SD-WAN, which is natively integrated with our industry-leading security.
- Delivers an exceptional end user experience by minimizing latency, jitter, and packet loss.

Table 1: PA-7000 Series Performance and Capacities

	PA-7080*	PA-7050*	PA-7000 DPC-A	PA-7000-100G-NPC-A	PA-7000-20G(Q)XM-NPC
Firewall throughput (HTTP/appmix)†	644/700 Gbps	390/416 Gbps	77/86 Gbps	59/66 Gbps	17.6/20.0 Gbps
Threat Prevention throughput (DSRI enabled)‡	650 Gbps	396 Gbps	71.2 Gbps	55.7 Gbps	16.7 Gbps
Threat Prevention throughput (HTTP/appmix)§	362/430 Gbps	210/258 Gbps	41/49 Gbps	29/37 Gbps	9.3/12.5 Gbps
IPsec VPN throughput‖	328 Gbps	200 Gbps	36 Gbps	28 Gbps	9 Gbps
Max sessions	416M	245M	43M	32M	8M
New sessions per second**	6M	4M	925,000	623,000	208,000
Virtual systems (base/max)††	25/225	25/225	–	–	–

Note: Results were measured on PAN-OS 10.0.

* Results in this column were derived from an optimum combination of PA-7000-DPC-A and PA-7000-100G-NPC-A cards populated in all available slots.

† Throughput is measured with App-ID and logging enabled, with 64 KB HTTP/appmix transactions.

‡ 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.

§ Threat Prevention throughput measured with App-ID, IPS, antivirus, anti-spyware, WildFire, and logging enabled, utilizing 64 KB HTTP/appmix transactions.

‖ IPsec VPN throughput is measured with 64 KB HTTP transactions and logging enabled.

** New sessions per second is measured with application override, utilizing 1 byte HTTP transactions.

†† 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.

PA-7000 Series Architecture

The PA-7000 Series is powered by a scalable architecture for the purposes of applying the appropriate type and volume of processing power to the key functional tasks of networking, security, and management. The PA-7000 Series is managed as a single, unified system, enabling you to easily direct all available resources to protect your data. The PA-7000 Series chassis intelligently distributes processing demands across three subsystems, each with massive amounts of computing power and dedicated memory: the processing card(s), the System Management Card, and the Dedicated Logging Card.

Processing Card

The PA-7080 offers 10 slots for processing cards while the PA-7050 offers six. Processing cards are available as Network Processing Cards (NPCs), which support both networking functions and data processing, or Data Processing Cards (DPCs), which maximize data processing performance. For network connectivity, the PA-7000 series requires at least one NPC.

Network Processing Card

The NPC is dedicated to executing all packet-processing tasks, including networking, traffic classification, and threat prevention. The first-generation NPCs (PA-7000-20GXM-NPC and PA-7000-20GQXM-NPC) each have 64 processing cores (two 32-core CPUs) with offload processing. The PA-7000-20GXM-NPC offers 1G and 10G connectivity options, while the PA-7000-20GQXM-NPC offers 1G, 10G, and 40G connectivity options. The second-generation 100G-NPC (PA-7000-100G-NPC-A) more than doubles the processing capacity with 144 processing cores (three 48-core CPUs) with offload processing, all focused on protecting your network at up to 66 Gbps per NPC. The PA-7000-100G-NPC-A offers 100G, 40G, 10G, and 1G connectivity options.

Data Processing Card

The DPC-A (PA-7000-DPC-A) maximizes security processing by packing 192 processing cores (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 100G-NPC, adding a fourth compute complex and an additional offload processor in place of Ethernet I/O.

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 (FPP), a high-speed backplane, and the management subsystem. The first-generation SMC (PA-7000-SMC) supports mixed configuration of the first-generation NPCs, the second-generation 100G-NPC, and the DPC-A. The second-generation SMC-B (PA-7000-SMC-B) supports the second-generation 100G-NPC and the DPC-A while offering significant improvements in the functionality of all three elements as detailed in the following.

First Packet Processor

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 and DPCs, intelligently directing inbound traffic to the appropriate data processor based on the configured policy. As processing cards are added to increase performance and capacity, the FPP automatically detects and utilizes new resources added to the system, meaning no traffic management changes are required, nor is it necessary to re-cable or reconfigure your PA-7000 Series. 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 100G-NPC and allowing the FPP to determine the best use of the new processing power.

High-Speed Backplane

Each processing card has access to more than 100 Gbps of non-blocking traffic capacity with a high-speed backplane.

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 multi-core CPU design, creating a dedicated subsystem to manage the high volume of logs the PA-7000 Series generates. Two logging cards are available: a first-generation Log Processing Card (PA-7000-LPC) and a second-generation Log Forwarding Card (PA-7000-LFC-A). The LPC uses up to 4 TB of RAID1 storage to offload logging-related activities, enabling the ability to run queries and reports from the most recent logs collected. The LFC-A is a high-performance card dedicated to exporting log messages. Both these cards enable forwarding of 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-A is optimized for use with the second-generation SMC-B, 100G-NPC, and DPC-A.

Table 2: PA-7000 Series Networking Features
Interface Modes
L2, L3, tap, virtual wire (transparent mode)
Routing
OSPFv2/v3 with graceful restart, BGP with graceful restart, RIP, static routing
Policy-based forwarding
Point-to-point protocol over Ethernet (PPPoE) and DHCP supported for dynamic address assignment
Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, and v3
Bidirectional Forwarding Detection (BFD)
SD-WAN
Path quality measurement (jitter, packet loss, latency)
Initial path selection (PBF)
Dynamic path change
IPv6
L2, L3, tap, virtual wire (transparent mode)
Features: App-ID, User-ID, Content-ID, WildFire, and SSL Decryption
SLAAC
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 for simplified configuration and management
VLANs
802.1Q VLAN tags per device/per interface: 4,094/4,094
Aggregate interfaces (802.3ad) intra-card and/or inter-card, and LACP
Network Address Translation
NAT modes (IPv4): static IP, dynamic IP, dynamic IP and port (port address translation)
NAT64, NPTv6
Additional NAT features: dynamic IP reservation, tunable dynamic IP and port oversubscription
High Availability
Modes: active/active, active/passive, HA clustering
Failure detection: path monitoring, interface monitoring
Mobile Network Infrastructure*
GTP Security
SCTP Security

* For additional information, refer to our ML-Powered NGFWs for 5G datasheet.

Table 3: PA-7000 Series Hardware Specifications			
	PA-7000 NPC	PA-7080 Full System	PA-7050 Full System
PA-7000-100G-NPC-A	SFP/SFP+ (8), QSFP+/QSFP28 (4)	SFP/SFP+ (80), QSFP+/QSFP28 (40)	(48) SFP/SFP+. (24) QSFP+/QSFP28
PA-7000-20GQXM-NPC	QSFP+ (2), SFP+ (12)	QSFP+ (20), SFP+ (120)	(12) QSFP +, (72) SFP+
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+
PA-7050-SMC-B PA-7080-SMC-B	–	SFP MGT (2), SFP HA1 (2), HSCI HA2/HA3 QSFP+/QSFP28 (2), RJ45 serial console (1), Micro USB serial console (1)	
PA-7050-SMC PA-7080-SMC	–	10/100/1000 (2), QSFP+ high availability (2), 10/100/1000 out-of-band management (1), RJ45 console port (1)	
PA-7000-LFC-A	–	480 GB SSD, system drive RAID1 (2 x 240 GB)	
PA-7000-LPC	–	480 GB SSD system drive (1), 2 TB RAID1 (2 x 1 TB + 2 x 1 TB) default or 4 TB RAID1 (2 x 2 TB + 2 x 2 TB) optional HDD	
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