paloalto® | **STRATA**™
NETWORKS | 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 and multi-access edge computing (MEC)

- 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-5450

The Palo Alto Networks PA-5450 ML-Powered Next-Generation Firewall (NGFW) platform is designed for hyperscale data center, internet edge, and campus segmentation deployments. Delivering incredible performance—120 Gbps with security services enabled—it is based on a scalable, modular design that enables you to increase performance as your needs increase. The PA-5450 offers simplicity defined by a single-system approach to management and licensing.

PA-5450

The world's first ML-Powered NGFW enables you to prevent unknown threats, see and secure everything—including the Internet of Things (IoT)—and reduce errors with automatic policy recommendations. The controlling element of the PA-5450 is PAN-OS®, the same software that runs all Palo Alto Networks NGFWs. 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 and reduced incident response time.

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 IoT devices and make policy recommendations as part of a 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-ID™ tags for proprietary applications or request App-ID development for new applications from Palo Alto Networks.
- Identifies all payload data (e.g., files and data patterns) within an application to block malicious files and thwart exfiltration attempts.
- Creates standard and customized application usage reports, including software-as-a-service (SaaS) reports that provide insight into all sanctioned and unsanctioned SaaS traffic 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 based on 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 misconfigured certificates to mitigate risks.
- Facilitates easy deployment of decryption and lets you use built-in logs to troubleshoot issues, such as applications with pinned certificates.
- Lets you enable or disable decryption flexibly based on URL category, source and destination zone, address, user, user group, device, and port, for privacy and 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).

Offers centralized management and visibility

- Benefits from centralized management, configuration, and visibility for multiple distributed Palo Alto Networks NGFWs (irrespective of location or scale) through Panorama™ network security management, in one unified user interface.
- Streamlines configuration sharing through Panorama with templates and device groups, and scales log collection as logging needs increase.
- Enables users, through the Application Command Center (ACC), to obtain deep visibility and comprehensive insights into network traffic and threats.

Detect and Prevent Advanced Threats

Today, cyberattacks have increased in volume and sophistication, scaling to 45,000 variants within 30 minutes, using multiple threat vectors or advanced techniques to deliver malicious

payloads within your enterprise. Traditional siloed security solutions cause challenges for organizations trying to protect their users, devices and applications. They introduce security gaps and increase management overhead for security teams, and hinder business productivity with inconsistent access and visibility. Seamlessly integrated with the industry-leading Next-Generation Firewall platform, our Cloud-Delivered Security Services use the network effect of 80,000 customers to instantly coordinate intelligence and provide protections for all threats across all threat vectors. Eliminate coverage gaps across all enterprise locations and take advantage of best-in-class security delivered consistently in a platform, so you can be safe from even the most advanced and evasive threats.

- **Threat Prevention**—goes beyond a traditional intrusion prevention system (IPS) to prevent all known threats across all traffic in a single pass without sacrificing performance.
- **Advanced URL Filtering**—provides best-in-class web protection while maximizing operational efficiency with the industry's first real-time web protection engine and industry-leading phishing protection.
- **WildFire®**—ensures files are safe with automatic detection and prevention of unknown malware, powered by industry-leading cloud-based analysis and crowdsourced intelligence from more than 42,000 customers.
- **DNS Security**—harnesses the power of ML to detect as well as prevent threats over DNS in real time and empowers security personnel with the intelligence and context to craft policies and respond to threats quickly and effectively.
- **IoT Security**—provides the industry's most comprehensive IoT security solution, delivering ML-powered visibility, prevention, and enforcement in a single platform.
- **Enterprise DLP**—offers the industry's first cloud-delivered enterprise DLP that consistently protects sensitive data across networks, clouds, and users.
- **SaaS Security**—delivers integrated SaaS security that lets you see and secure new SaaS applications, protect data, and prevent zero-day threats at the lowest total cost of ownership (TCO).

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.

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

- Performs networking, policy lookup, application and decoding, and signature matching—for 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.
- Avoids introducing latency by scanning traffic for all signatures in a single pass, using stream-based, uniform signature matching.
- Enables consistent and predictable performance when security subscriptions are enabled. (In Table 1, "Threat Prevention throughput" is measured with multiple subscriptions enabled.) PA-5450 Architecture

PA-5450 Architecture

The PA-5450 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 device is managed as a single unified system, enabling you to easily direct all available resources to protect your data. The PA-5450 intelligently distributes processing demands across three subsystems, each with massive amounts of computing power and dedicated memory: the Networking Cards (NC), the Data Processing Cards (DPC), and the Management Processing Card (MPC).

The PA-5450 offers a total of six slots for NCs and DPCs.

Table 1: PA-5450 Performance and Capacities		
	PA-5450 Configured System*	**Single PA-5400-DPC-A**
Firewall throughput (HTTP/appmix)***	200/200 Gbps	72/68 Gbps
Threat Prevention throughput (HTTP/appmix)†	125/150 Gbps	31/37 Gbps
IPsec VPN throughput‡	95 Gbps**	19 Gbps
Max sessions	100M	20M
New sessions per second§	4M	830,000
Virtual systems (base/max)‖	25/225	—

* All tests performed with 2 Networking Cards + 4 Data Processing Cards populated, unless otherwise noted

** This test performed with 1 Networking Card + 5 Data Processing Cards populated

*** Firewall throughput is measured with App-ID and logging enabled, utilizing 64 KB HTTP/appmix transactions.

† Threat Prevention throughput is measured with App-ID, IPS, antivirus, anti-spyware, WildFire, file blocking, 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.

‖ Adding virtual systems over base quantity requires a separately purchased license.

Networking Cards

For network connectivity, the PA-5450 requires at least one NC (PA-5400-NC-A). A second NC requires a minimum of two DPCs installed in the system. A maximum of two NCs can be installed. NCs are dedicated to executing packet ingress and egress tasks.

Each PA-5400-NC-A offers multiple connectivity ports as listed in Table 3: 100/1000/10G Cu (4), 1G/10G SFP/SFP+ (12), and 40G/100G QSFP28 (2).

Data Processing Cards

For packet and security processing, the PA-5450 uses DPCs (PA-5400-DPC-A), with a minimum of one DPC and up to five DPCs that can be placed in the six slots.

Management Processing Card

The MPC subsystem (PAN-PA-5400-MPC-A) acts as a dedicated point of contact for controlling all aspects of the PA-5450.

Table 2: PA-5450 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

Table 2: PA-5450 Networking Features (cont.)
VLANs
802.1Q VLAN tags per device/per interface: 4,094/4,094
Aggregate interfaces (802.3ad), 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-5450 Hardware Specifications
PA-5400-NC-A Networking I/O
100/1000/10G Cu (4), 1G/10G SFP/ SFP+ (12), 40G/100G QSFP28 (2); minimum 1 NC and maximum 2 NCs per system; 2 NCs require 2 or more DPCs installed
PAN-PA-5400-MPC-A Management I/O
10/100/1000 (2), 40G/100G QSFP28 HA (2), 10/100/1000 out-of-band management (2), RJ45 console port (1), USB console port (1)
Storage Capacity
480 GB SSD, RAID1, system storage 4 TB SSD, log storage (optional)
Max BTU/hr
8,828
Power Supplies (Base/Max)
2/4
AC Input Voltage (Input Frequency)
100−120 VAC & 200−240 VAC (50−60 Hz)
AC Power Supply Output
2,200 watts/power supply
Max Current Consumption
AC: 100−120 VAC, ~14 A max. per input 200−240 VAC, ~12.5 A max. per input
DC: 48−60 VDC, 52 A max. per input

Table 3: PA-5450 Hardware Specifications (cont.)
Max Inrush Current
AC: 35 A @ 230 VAC, 35 A @ 120 VAC
DC: 50 A @ 72 VDC
Rack Mount (Dimensions)
5U, 19" standard rack 8.75" H x 30.25" D x 17.38" W
Maximum Time Between Failure (MTBF)
Configuration dependent; contact your Palo Alto Networks representative for MTBF details.
Safety
cTUVus, CB
EMI
FCC Class A, CE Class A, VCCI Class A, KCC Class A, BSMI Class A
Certifications
See paloaltonetworks.com/company/certifications.html
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-5450, please visit paloaltonetworks.com/network-security/next-generation-firewall/pa-5450.