# PA-800 Series

Palo Alto Networks PA-800 Series ML-Powered NGFWs, comprising the PA-850 and PA-820, are designed to provide secure connectivity for organizations' branch offices as well as midsize businesses.


PA-850

## Highlights

- World's first ML-Powered NGFW
- Ten-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
- 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
- Simplifies deployment of large numbers of firewalls with optional Zero Touch Provisioning (ZTP)
- Supports centralized administration with Panorama™ network security management

The controlling element of the PA-800 Series is PAN-OS®, the same software that runs all Palo Alto Networks Next-Generation Firewalls (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 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).
- Automatically discovers and controls new applications to keep pace with the SaaS explosion with SaaS Security subscription.
- 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 within the application (e.g., 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 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.
- Check out the App-ID tech brief for more information.

### 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.
- Consistently authenticates and authorizes your users, regardless of location and where user identity stores live, to quickly move towards a Zero Trust security posture with Cloud Identity Engine—an entirely new cloud-based architecture for identity-based security. Check out the Cloud Identity Engine solution brief for more information.

## 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 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).
- Allows you to intelligently forward all traffic (decrypted TLS, non-decrypted TLS, and non-TLS) to third-party security tools with Network Packet Broker, optimize your network performance and reduce operating expenses.
- Refer to this decryption white paper to learn where, when and how to decrypt to prevent threats and secure your business.

## 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.

## Maximize Your Security Investment and Prevent Business Disruption with AIOps

- AIOps for NGFW delivers continuous best practice recommendations customized to your unique deployment to strengthen your security posture and get the most out of your security investment.
- Intelligently predicts firewall health, performance and capacity problems based on ML powered by advanced telemetry data. It also provides actionable insights to resolve the predicted disruptions.

## Detects and Prevents Advanced Threats with Cloud-Delivered Security Services

Today's sophisticated cyberattacks can spawn 45,000 variants in 30 minutes using multiple threat vectors and advanced techniques to deliver malicious payloads. Traditional siloed security causes challenges for organizations by introducing security gaps, increasing overhead for security teams, and hindering business productivity with inconsistent access and visibility.

Seamlessly integrated with our industry-leading NGFWs, our Cloud-Delivered Security Services use the network effect of 80,000 customers to instantly coordinate intelligence and protect against all threats across all vectors. Eliminate coverage gaps across your locations and take advantage of best-in-class security delivered consistently in a platform to stay safe from even the most advanced and evasive threats. Services include:

- **Advanced Threat Prevention:** Stop known exploits, malware, malicious URLs, spyware, and command and control (C2) with 96% prevention of web-based Cobalt Strike C2 and 48% more unknown C2 detected than the industry's leading intrusion prevention (IPS) solution.
- **WildFire® malware prevention:** Ensure files are safe by automatically detecting and preventing unknown malware 180X faster with industry's largest threat intelligence and malware prevention engine.
- **Advanced URL Filtering:** Enable safe access to the internet, with the industry's first real-time prevention of known and unknown websites, stopping 76% of malicious URLs 24 hours before other vendors.
- **DNS Security:** Gain 40% more DNS attack coverage and disrupt the 80% of attacks that use DNS for command and control and data theft without requiring any changes to your infrastructure.
- **Enterprise DLP:** Minimize risk of a data breach, stop out-of-policy data transfers, and enable compliance consistently across your enterprise, with 2X greater coverage of any cloud-delivered enterprise DLP.
- **SaaS Security:** Stay ahead of the SaaS explosion with the industry's only Next-Generation CASB to

automatically see and secure all apps across all protocols.

- **IoT Security:** Safeguard every "thing" and implement Zero Trust device security 20X faster, with the industry's smartest security for smart devices.

## 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.)

## 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-800 Series Performance and Capacities***

| | PA-850 | PA-820 |
|---|---|---|
| Firewall throughput (HTTP/appmix)† | 2.0/2.0 Gbps | 1.6/1.5 Gbps |
| Threat Prevention throughput (HTTP/appmix)‡ | 1.0/1.0 Gbps | 790/840 Mbps |
| IPsec VPN throughput§ | 1.8 Gbps | 1.4 Gbps |
| Max sessions | 192,000 | 128,000 |
| New sessions per second|| | 13,100 | 8,100 |

* Results were measured on PAN-OS 10.2.

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

‡ Threat Prevention throughput is measured with App-ID, IPS, antivirus, antispyware, WildFire, DNS Security, 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.

PA-800 Series ML-Powered NGFWs support a wide range of networking features that enable you to more easily integrate our security features into your existing network.

| Table 2: PA-800 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) |
| Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, and v3 |
| **SD-WAN** |
| Path quality measurement (jitter, packet loss, latency) |
| Initial path selection (PBF) |
| Dynamic path change |

| Table 2: PA-800 Series Networking Features (continued) |
|---|
| **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 |
| **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 |
| Failure detection: path monitoring, interface monitoring |
| **Zero Touch Provisioning (ZTP)** |
| Available with -ZTP SKUs (PA-220-ZTP) |
| Requires Panorama 9.1.3 or higher |

| Table 3: PA-800 Series Hardware Specifications |
|---|
| **I/O** |
| PA-850: 10/100/1000 (4), Gigabit SFP (8) or<br>PA-850: 10/100/1000 (4), Gigabit SFP (4), 10 Gigabit SFP+ (4)<br>PA-820: 10/100/1000 (4), Gigabit SFP (8) |
| **Management I/O** |
| 10/100/1000 out-of-band management port (1)<br>10/100/1000 high availability (2)<br>RJ-45 console port (1)<br>USB port (1)<br>Micro USB console port (1) |
| **Storage Capacity** |
| 240 GB SSD |
| **Power Supply** |
| PA-850: AC 450 W power supplies (2); one is redundant<br>PA-820: Fixed AC 200 W power supply (1) |
| **Power Consumption** |
| Maximum: PA-850: 240 W; PA-820: 120 W<br>Average: PA-850: 64 W; PA-820: 41 W |
| **Max BTU/hr** |
| 256 |
| **Input Voltage (Input Frequency)** |
| 100–240 VAC (50–60 Hz) |

| Table 3: PA-800 Series Hardware Specifications (continued) |
|---|
| **Max Current Consumption** |
| PA-850: 2.0 A @ 100 VAC, 1.0 A @ 240 VAC<br>PA-820: 1.0 A @ 100 VAC, 0.5 A @ 240 VAC |
| **Max Inrush Current** |
| PA-850: 1.0 A @ 230 VAC, 1.84 A @ 120 VAC<br>PA-820: 0.4 A @ 230 VAC, 0.96 A @ 120 VAC |
| **Rack Mount (Dimensions)** |
| PA-850: 1U, 19" standard rack (1.75" H x 14.5" D x 17.125" W<br>PA-820: 1U, 19" standard rack (1.75" H x 14" D x 17.125" W) |
| **Weight (Standalone Device/As Shipped)** |
| PA-850: 13.5 lbs / 21.5 lbs<br>PA-820: 11 lbs / 18 lbs |
| **Safety** |
| cTUVus, CB |
| **EMI** |
| FCC Class A, CE Class A, VCCI Class A |
| **Certifications** |
| See paloaltonetworks.com/company/certifications.html |
| **Environment** |
| Operating temperature: 32° to 104° F, 0° to 40° C<br>Non-operating temperature: -4° to 158° F, -20° to 70° C |
| **Airflow** |
| Front to back |

To learn more about the features and associated capacities of the PA-800 Series, please visit paloaltonetworks.com/network-security/next-generation-firewall/pa-800-series.

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