

# PA-800 Series

Die ML-gestützten NGFWs der PA-800 Series von Palo Alto Networks mit den Modellen PA-850 und PA-820 wurden zum Schutz von Zweigniederlassungen und mittelständischen Unternehmen entwickelt.



PA-850

Die ML-gestützten Next-Generation Firewalls (NGFW) der PA-800 Series werden über PAN-OS® gesteuert, das den gesamten Datenverkehr, einschließlich Anwendungen, Bedrohungen und Inhalten, nativ klassifiziert und dann diesen Datenverkehr unabhängig von Standort oder Gerätetyp dem jeweiligen Benutzer zuordnet. Die Anwendung, der Inhalt und der Benutzer – d. h. die für Ihre Betriebsabläufe wesentlichen Ressourcen – werden anschließend als Basis für Ihre Sicherheitsleitlinien genutzt, um den Sicherheitsstatus zu erhöhen und die Reaktionszeiten bei Zwischenfällen zu reduzieren.

# Wichtige Sicherheits- und Konnektivitätsfunktionen

## Permanente Klassifizierung aller Anwendungen auf allen Ports

- Identifizierung der Anwendung unabhängig vom Port, von der Verschlüsselung (SSL oder SSH) oder der eingesetzten Umgehungsmethode.
- Nutzung der Anwendung anstelle des Ports als Grundlage für alle Entscheidungen bezüglich Sicherheitsleitlinien, wie beispielsweise Zulassen, Ablehnen, Terminieren, Untersuchen und das Anwenden von Traffic-Shaping.
- Kategorisierung nicht identifizierter Anwendungen zur Richtlinienkontrolle, für forensische Untersuchungen oder App-ID™-Entwicklungen.
- Vollständige Einsicht in die Details aller TLS-verschlüsselten Verbindungen und Abwehr von Bedrohungen, die in verschlüsseltem Datenverkehr versteckt sind, auch in Datenverkehr, der die Protokolle TLS 1.3 und HTTP/2 verwendet.

## Umsetzung von Sicherheitsrichtlinien für alle Benutzer unabhängig von ihrem Standort

- Stellt konsistente Richtlinien für lokale und Remotebenutzer auf Windows®, macOS®, Linux-, Android®- oder Apple iOS-Plattformen bereit.
- Integration ohne Agent in Microsoft Active Directory® und Terminal Services, LDAP, Novell eDirectory™ und Citrix.
- Ermöglicht die einfache Integration Ihrer Firewallrichtlinien mit 802.1X-Wireless-Systemen, Proxys, NAC-Lösungen und sonstigen Einrichtungen zur Benutzerauthentifizierung

## Erweitert den nativen Schutz auf alle Angriffsvektoren mit cloudbasierten Securityabonnements

- **Threat Prevention** – überprüft den gesamten Datenverkehr, um bekannte Schwachstellen, Malware, Schwachstellen-Exploits, Spyware, Command-and-Control (C2) und benutzerdefinierte Intrusion Prevention System-(IPS-)Signaturen automatisch zu blockieren.
- **WildFire®-Malwareprävention** – schützt vor unbekanntem dateibasierten Bedrohungen und bietet in Sekundenschnelle eine automatische Abwehr der meisten neuen Bedrohungen über Netzwerke, Endpunkte und Clouds hinweg.
- **URL-Filterung** – verhindert den Zugriff auf schädliche Websites und schützt Benutzer vor webbasierten Bedrohungen.
- **DNS Security** – erkennt und blockiert bekannte und unbekanntes Bedrohungen über DNS, während die prädiktive Analyse Angriffe unterbindet, die DNS für C2 oder Datendiebstahl verwenden.
- **IoT Security** – entdeckt alle nicht verwalteten Geräte in Ihrem Netzwerk, identifiziert Risiken und Schwachstellen und automatisiert die Durchsetzung von Richtlinien für Ihre ML-gestützte NGFW mithilfe des neuen Richtlinienkonstrukts Device-ID™.

## Ermöglicht SD-WAN-Funktionalität

- Übernehmen Sie SD-WAN ganz einfach, indem Sie es auf Ihren vorhandenen Firewalls aktivieren.
- Ermöglicht Ihnen die sichere Implementierung von SD-WAN, nativ integriert mit unserer branchenführenden Sicherheit.
- Bietet ein erstklassiges Benutzererlebnis durch Minimierung von Latenzen, Jitter und Paketverlusten.

**Tabelle 1: Leistung und Kapazitäten der PA-800 Series<sup>1</sup>**

	PA-850	PA-820
Firewalldurchsatz (HTTP/Appmix) <sup>2</sup>	2,1/2,1 Gbit/s	1,8/1,6 Gbit/s
Threat Prevention-Durchsatz (HTTP/Appmix) <sup>3</sup>	1,0/1,2 Gbit/s	850/900 Mbit/s
IPsec-VPN-Durchsatz <sup>4</sup>	1,6 Gbit/s	1,3 Gbit/s
Neue Sitzungen pro Sekunde <sup>5</sup>	13.000	8.600
Max. Sitzungen	192.000	128.000

1. Ergebnisse wurden auf PAN-OS 10.0 gemessen.  
 2. Firewalldurchsatz gemessen mit aktivierter App-ID und Protokollierung bei 64-KB-HTTP/Appmix-Transaktionen.  
 3. Threat Prevention-Durchsatz gemessen mit aktivierter App-ID, IPS, Antivirus, Antispyware, WildFire, Dateiblockade und Protokollierung unter Verwendung von 64-KB-HTTP/Appmix-Transaktionen.  
 4. IPsec-VPN-Durchsatz gemessen mit 64-KB-HTTP-Transaktionen und Protokollierung.  
 5. Neue Sitzungen pro Sekunde gemessen mit Überschreibung der App-ID unter Verwendung von 1-Byte-HTTP-Transaktionen.

Die ML-gestützten NGFWs der PA-800 Series unterstützen eine Vielzahl von Netzwerkfunktionen, mit denen Sie unsere Sicherheitsfunktionen noch einfacher in Ihr bestehendes Netzwerk integrieren können.

**Tabelle 2: Netzwerkfunktionen der PA-800 Series**

Schnittstellenmodi
L2, L3, TAP, Virtual Wire (Transparent-Modus)
Routing
OSPFv2/v3 mit Graceful Restart, BGP mit Graceful Restart, RIP, statisches Routing
Policy-Based Forwarding (PBF)
Point-to-Point Protocol Over Ethernet (PPPoE)
Multicast: PIM-SM, PIM-SSM, IGMP v1, v2 und v3
SD-WAN
Messung der Pfadqualität (Jitter, Paketverlust, Latenz)
Auswahl des Anfangspfads (PBF)
Dynamische Pfadänderung
IPv6
L2, L3, TAP, Virtual Wire (Transparent-Modus)
Funktionen: App-ID, User-ID, Content-ID, WildFire und SSL-Entschlüsselung
SLAAC
IPsec VPN
Schlüsselaustausch: manueller Schlüssel, IKEv1 und IKEv2 (Pre-shared Key, zertifikatbasierte Authentifizierung)
Verschlüsselung: 3DES, AES (128 Bit, 192 Bit, 256 Bit)
Authentifizierung: MD5, SHA-1, SHA-256, SHA-384, SHA-512

**Tabelle 2: Netzwerkfunktionen der PA-800 Series (Forts.)**

VLANs
802.1Q VLAN-Tags pro Gerät und Schnittstelle: 4.094/4.094
Aggregat-Schnittstelle (802.3ad), LACP
Network Address Translation
NAT-Modi (IPv4): statische IP, dynamische IP, dynamische IP und Port (Port Address Translation)
NAT64, NPTv6
Zusätzliche NAT-Funktionen: dynamische IP-Reservierung, anpassbare Überbelegung dynamischer IP-Adressen und Ports
High Availability (hohe Verfügbarkeit, HA)
Modi: aktiv/aktiv, aktiv/passiv
Fehlererkennung: Pfadüberwachung, Schnittstellenüberwachung
Zero Touch Provisioning (ZTP)
Erhältlich mit -ZTP SKUs (PA-850-ZTP, PA-820-ZTP) Erfordert Panorama 9.1.3 oder höher

**Tabelle 3: Hardwarespezifikationen der PA-800 Series**

I/O
PA-850: 10/100/1000 (4), Gigabit-SFP (8) oder PA-850: 10/100/1000 (4), Gigabit-SFP (4), 10-Gigabit-SFP+ (4) PA-820: 10/100/1000 (4), Gigabit-SFP (8)
Management-E/A
10/100/1000 Out-of-Band-Managementport (1) 10/100/1000 hohe Verfügbarkeit (2) Konsolenport RJ-45 (1) USB-Port (1) Micro-USB-Konsolenport (1)
Speicherkapazität
240 GB SSD
Stromversorgung
PA-850: 450-W-Wechselstromversorgungen (2); davon eine redundant PA-820: Feste 200-W-Wechselstromversorgung (1)
Stromverbrauch
Maximum: PA-850: 240 W; PA-820: 120 W Durchschnitt: PA-850: 64 W; PA-820: 41 W

**Tabelle 3: Hardwarespezifikationen der PA-800 Series (Forts.)**

Max. BTU/h
256
Eingangsspannung (Eingangsfrequenz)
100–240 V AC (50/60 Hz)
Max. Stromverbrauch
PA-850: 2,0 A bei 100 V AC, 1,0 A bei 240 V AC PA-820: 1,0 A bei 100 V AC, 0,5 A bei 240 V AC
Max. Einschaltstrom
PA-850: 1,0 A bei 230 V AC, 1,84 A bei 120 V AC PA-820: 0,4 A bei 230 V AC, 0,96 A bei 120 V AC
Im Rack montierbar (Abmessungen)
PA-850: 1 Einheit, 19"-Standard-Rack (4,45 cm H x 36,83 cm T x 43,5 cm B) PA-820: 1 Einheit, 19"-Standard-Rack (4,45 cm H x 36,83 cm T x 43,5 cm B)
Gewicht (Stand-alone-Gerät/wie geliefert)
PA-850: 6,12 kg/9,75 kg PA-820: 4,99 kg/8,16 kg
Sicherheit
cTUVus, CB
EMV
FCC-Klasse A, CE-Klasse A, VCCI-Klasse A
Zertifizierungen
Siehe <a href="https://paloaltonetworks.com/company/certifications.html">paloaltonetworks.com/company/certifications.html</a>
Umgebung
Betriebstemperatur: 0 bis 40 °C (32 bis 104 °F) Temperatur bei Nichtbetrieb: -20 bis 70 °C (-4 bis 158 °F)
Luftstrom
Von vorne nach hinten

Um mehr über die Funktionen und die damit verbundenen Kapazitäten der PA-800 Series zu erfahren, besuchen Sie [paloaltonetworks.com/network-security/next-generation-firewall/pa-800-series](https://paloaltonetworks.com/network-security/next-generation-firewall/pa-800-series).