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 Niederlassungen und mittelständischen Unternehmen entwickelt.

PA-850

Highlights

- Die erste ML-gestützte NGFW
- Neunmaliger Leader im Gartner Magic Quadrant® für Netzwerkfirewalls
- Leader im Bericht „The Forrester Wave™: Enterprise Firewalls, Q3 2020“
- Höchste Effektivitätsbewertung im „NGFW Test Report 2019“ von NSS Labs mit zu 100 Prozent blockierten Umgehungsversuchen
- Weitet Transparenz und Sicherheit ohne zusätzliche Sensoren auf sämtliche Geräte im Netzwerk aus, auch auf nicht verwaltete IoT-Geräte
- Unterstützt Hochverfügbarkeit mit Aktiv/Aktiv- und Aktiv/Passiv-Modus
- Bietet vorhersehbare Leistung mit Sicherheitsservices
- Vereinfacht die Bereitstellung einer großen Anzahl von Firewalls mit optionalem Zero Touch Provisioning (ZTP)
- Unterstützt die zentralisierte Verwaltung mit Panorama™-Netzwerksicherheitsmanagement

Die PA-800 Series nutzt das Betriebssystem PAN-OS®, wie alle Next-Generation Firewalls (NGFWs) von Palo Alto Networks. PAN-OS klassifiziert nativ den gesamten Netzwerkverkehr (einschließlich aller Anwendungsdaten, Bedrohungen und legitimen Inhalte) und ordnet die einzelnen Pakete dann unabhängig vom Standort oder Gerätetyp einem Benutzer zu. In Abhängigkeit von den Anwendungen, Inhalten und Benutzern (also den Faktoren, die für Ihr Geschäft relevant sind) wird dann entschieden, welche Sicherheitsrichtlinien anzuwenden sind. Das stärkt die Sicherheit und beschleunigt effektive Reaktionen auf Sicherheitsvorfälle.

Wichtige Sicherheits- und Konnektivitätsfunktionen

ML-gestützte Next-Generation Firewall

- Integriert maschinelles Lernen (ML) in den Kern der Firewall, um eine signaturlose Inlineabwehr dateibasierter Angriffe zu bieten und bisher unbekannte Phishingversuche zu erkennen und sofort zu stoppen.
- Nutzt cloudbasierte ML-Prozesse, um verzögerungsfrei Signaturen und Anweisungen zurück an die NGFW zu senden.
- Nutzt Verhaltensanalysen, um Geräte im Internet der Dinge (Internet of Things, IoT) zu erkennen und Richtlinienempfehlungen abzugeben; in der Cloud bereitgestellter und nativ integrierter Service auf der NGFW.
- Automatisiert Richtlinienempfehlungen, um Zeit zu sparen und das Risiko von Bedienfehlern zu reduzieren.

Identifizierung und Klassifizierung aller Anwendungen auf allen Ports – jederzeit und mit vollständiger Layer-7-Prüfung

- Identifiziert die Anwendungen, die Daten durch Ihr Netzwerk senden, unabhängig von Port, Protokoll, Umgehungstechniken oder Verschlüsselung (TLS/SSL).
- Ermöglicht die Definition und Implementierung von Sicherheitsrichtlinien, die sich auf spezifische Anwendungen (statt auf Ports) beziehen (zulassen, ablehnen, planen, untersuchen, Datenverkehrsregeln anwenden).
- Bietet die Möglichkeit, benutzerdefinierte App-ID™-Kennzeichnungen für eigene Anwendungen zu erstellen oder die App-ID-Entwicklung für neue Anwendungen bei Palo Alto Networks anzufordern.
- Identifiziert alle Nutzdaten innerhalb der Anwendung (wie Dateien und Datenmuster), um bösartige Dateien zu blockieren und Datenausschleusungen zu verhindern.
- Erstellt standardmäßige und angepasste Anwendungsnutzungsberichte, einschließlich Berichten zu Software-as-a-Service (SaaS), die einen Einblick in den gesamten genehmigten und nicht genehmigten SaaS-Datenverkehr in Ihrem Netzwerk geben.
- Ermöglicht die sichere Migration älterer Layer-4-Regelsätze zu App-ID-basierten Regeln mit integriertem Policy Optimizer. Damit erhalten Sie einen Regelsatz, der sicherer und einfacher zu verwalten ist.

Orts- und geräteunabhängige Durchsetzung von Sicherheitsmaßnahmen und Anpassung von Richtlinien anhand von Benutzeraktivitäten

- Ermöglicht Transparenz, Sicherheitsrichtlinien, Berichte und Forensik auf der Grundlage von Benutzern und Gruppen – nicht nur von IP-Adressen.
- Lässt sich leicht in eine Vielzahl von Repositorys integrieren, um Benutzerinformationen zu nutzen: WLAN-Controller, VPNs, Verzeichnisserver, SIEMs, Proxys und mehr.
- Ermöglicht das Definieren dynamischer Benutzergruppen in der Firewall, um zeitgebundene Sicherheitsmaßnahmen umzusetzen, ohne die Aktualisierung von Benutzerverzeichnissen abwarten zu müssen.
- Wendet konsistente Richtlinien an, unabhängig von den Standorten der Benutzer (Büro, zu Hause, unterwegs usw.) und ihren Geräten (iOS- und Android®-Mobilgeräte; macOS®-, Windows®-, Linux-Desktops, -Laptops; Citrix- und Microsoft VDI- und Terminal-Server).
- Verhindert, dass Anmeldedaten des Unternehmens auf Websites von Dritten gelangen, und verhindert die Nutzung gestohlener Anmeldedaten, indem die Multi-Faktor-Authentifizierung (MFA) auf der Netzwerkebene für jede Anwendung aktiviert wird, ohne dass die Anwendung geändert werden muss.
- Auf der Grundlage des Benutzerverhaltens werden dynamisch Sicherheitsmaßnahmen umgesetzt, um verdächtige oder böswillige Benutzer zu blockieren.

Schutz vor bösartigen Aktivitäten, die sich in verschlüsseltem Datenverkehr verbergen

- Untersucht ein- und ausgehenden TLS/SSL-verschlüsselten Datenverkehr, einschließlich des Datenverkehrs, der TLS 1.3 und HTTP/2 verwendet, und wendet die Richtlinien darauf an.
- Bietet umfassende Einblicke in den TLS-Verkehr, wie den Umfang des verschlüsselten Datenverkehrs, TLS/SSL-Versionen, Ciphersuites und mehr, ohne ihn zu entschlüsseln.
- Ermöglicht es, die Verwendung von veralteten TLS-Protokollen, unsicheren Ciphersuites und falsch konfigurierten Zertifikaten zu verhindern, um Risiken zu minimieren.
- Erleichtert die Bereitstellung der Entschlüsselung und ermöglicht die Verwendung integrierter Protokolle zur Fehlerbehebung, etwa bei Anwendungen mit Zertifikat-Pinning.
- Ermöglicht das flexible Aktivieren oder Deaktivieren der Entschlüsselung basierend auf URL-Kategorie und Quell- und Zielzone, Adresse, Benutzer, Benutzergruppe, Gerät und Port, um den Datenschutz und die Einhaltung regulatorischer Vorschriften zu wahren.
- Ermöglicht es, eine Kopie des entschlüsselten Datenverkehrs von der Firewall zu erstellen (d. h. Entschlüsselungsspiegelung) und diese an Tools zur Datenverkehrserfassung für Forensik, Verlaufsprotokollierung oder Data Loss Prevention (DLP) zu senden.

Zentralisierte Verwaltung und Transparenz

- Nutzt die zentrale Verwaltung, Konfiguration und Transparenz für mehrere verteilte NGFWs von Palo Alto Networks (unabhängig von Standort oder Umfang) durch das Panorama™-Netzwerksicherheitsmanagement an einer einheitlichen Benutzeroberfläche.

- Vereinfacht die gemeinsame Nutzung von Konfigurationen über Panorama mit Vorlagen und Gerätegruppen und skaliert die Protokollerfassung je nach Bedarf.
- Bietet Benutzern über das Application Command Center (ACC) detaillierte Transparenz und umfassende Einblicke in Netzwerkverkehr und -bedrohungen.

Erkennung und Abwehr komplexer Bedrohungen mit Cloud-Delivered Security Services

Moderne ausgeklügelte Cyberattacken können innerhalb von 30 Minuten auf bis zu 45.000 Varianten anwachsen. Dabei werden mehrere Bedrohungsvektoren und raffinierte Techniken eingesetzt, um Schadcode einzuschleusen. Herkömmliche Punktlösungen verursachen Sicherheitslücken in Unternehmen, erhöhen den Arbeitsaufwand von Sicherheitsteams und beeinträchtigen die Produktivität durch inkonsistenten Zugriff und unzureichende Transparenz.

Unsere Cloud-Delivered Security Services dagegen können nahtlos in unsere branchenführenden NGFWs integriert werden und nutzen unser Netzwerk aus 80.000 Kunden, um Threat Intelligence sofort zu koordinieren und Schutz vor allen Bedrohungen und Bedrohungsvektoren zu bieten. Schließen Sie Sicherheitslücken an allen Ihren Standorten und nutzen Sie die Vorteile erstklassiger Sicherheit, die konsistent über eine zentrale Plattform bereitgestellt wird, um auch vor den komplexesten und am besten getarnten Bedrohungen geschützt zu sein. Diese Dienste werden geboten:

- **Threat Prevention** – bietet mehr Sicherheit als ein herkömmliches IPS (Intrusion Prevention System), da alle bekannten Bedrohungen für den gesamten Datenverkehr in einem Durchlauf (Single Pass) abgewehrt werden, ohne dass die Leistung leidet.
- **Advanced URL Filtering** – sorgt für erstklassigen Schutz vor webbasierten Bedrohungen und eine Steigerung der betrieblichen Effizienz dank branchenweit erster Echtzeit-Präventionslösung für Webangriffe und branchenführender Phishingabwehr.
- **WildFire®** – schützt Dateien durch die automatische Erkennung und Abwehr unbekannter Malware mit branchenführenden cloudbasierten Analysen und Threat Intelligence von mehr als 42.000 Kunden.
- **DNS Security** – nutzt ML, um Bedrohungen über das DNS in Echtzeit zu erkennen und abzuwehren. Sicherheitsteams erhalten so die Kontextinformationen, die sie zur Ausarbeitung von Richtlinien und zur schnellen und wirkungsvollen Abwehr von Bedrohungen benötigen.
- **IoT Security** – bietet die umfassendste IoT-Sicherheitslösung der Branche für einen detaillierten Überblick, eine effektive Abwehr und eine zuverlässige Richtliniendurchsetzung – alles auf einer einzigen ML-gestützten Plattform.
- **Enterprise DLP** – ist die branchenweit erste cloudbasierte DLP-Lösung für Unternehmen, die sensible Daten über alle Netzwerke, Clouds und Benutzer hinweg konsistent schützt.
- **SaaS Security** – stellt integrierte SaaS-Sicherheitsfunktionen bereit, mit denen Sie neue SaaS-Anwendungen erkennen und sichern, Daten schützen und Zero-Day-Bedrohungen abwehren können – und das zu den niedrigsten Gesamtbetriebskosten.

Einzigartiger Ansatz für die Paketverarbeitung mit Single-Pass-Architektur

- Führt Netzwerkfunktionen, Richtliniensuche, -anwendung und -dekodierung sowie Signaturabgleich für alle Bedrohungen und Inhalte in einem einzigen Durchgang durch. So wird der Verarbeitungsaufwand für die Ausführung mehrerer Funktionen in einem einzelnen Sicherheitssystem erheblich reduziert.
- Vermeidet Latenzzeiten, indem der Datenverkehr in einem einzigen Durchgang mit einem streambasierten, einheitlichen Signaturabgleich anhand aller Signaturen überprüft wird.
- Ermöglicht eine konsistente und vorhersehbare Leistung, wenn Security Subscriptions aktiviert sind. (Der Threat-Prevention-Durchsatz in Tabelle 1 basiert auf mehreren aktivierten Abonnements.)

SD-WAN-Funktionalität

- Ermöglicht Ihnen die Einführung von SD-WAN, indem Sie es ganz einfach 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*

	PA-850	PA-820
Firewalldurchsatz (HTTP/Appmix)†	2,2/2,1 Gbit/s	1,8/1,7 Gbit/s
Threat-Prevention-Durchsatz (HTTP/Appmix)‡	1,0/1,2 Gbit/s	870/900 Mbit/s
IPsec-VPN-Durchsatz§	1,7 Gbit/s	1,4 Gbit/s
Neue Sitzungen pro Sekunde‖	13.100	8.100
Max. Anz. Sitzungen	192.000	128.000

* Ergebnisse wurden auf PAN-OS 10.1 gemessen.

† Der Firewalldurchsatz wurde bei aktivierter App-ID und Protokollierung unter Verwendung von 64-KB-HTTP/Appmix-Transaktionen gemessen.

‡ Der Threat-Prevention-Durchsatz wurde unter Verwendung von 64-KB-HTTP/Appmix-Transaktionen gemessen. App-ID, IPS, Antivirus- und Anti-Spyware-Funktionen, WildFire, DNS Security, die Dateiblockade und die Protokollierung waren aktiviert.

§ Der IPsec-VPN-Durchsatz wurde bei aktivierter Protokollierung unter Verwendung von 64-KB-HTTP-Transaktionen gemessen.

‖ Die Anzahl der neuen Sitzungen pro Sekunde wurde mit Application Override und 1-Byte-HTTP-Transaktionen gemessen.

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 (transparenter Modus)
Routing
OSPFv2/v3 mit ordnungsgemäßem Neustart, BGP mit ordnungsgemäßem Neustart, RIP, statisches Routing
Policy-Based Forwarding (richtlinienbasierte Weiterleitung, PBF)
Point-To-Point Protocol Over Ethernet (Punkt-zu-Punkt-Protokoll über Ethernet, PPPoE)
Multicast: PIM-SM, PIM-SSM, IGMP v1, v2 und v3

SD-WAN
Messung der Pfadqualität (Jitter, Paketverlust, Latenz)
Auswahl des Ursprungspfades (PBF)
Dynamische Pfadänderung
IPv6
L2, L3, Tap, Virtual Wire (transparenter Modus) Funktionen: App-ID, User-ID, Content-ID, WildFire und SSL-Entschlüsselung
SLAAC
IPsec VPN
Schlüsselaustausch: manuelle Schlüssel, IKEv1 und IKEv2 (vorab ausgetauschte Schlüssel, zertifikatsbasierte Authentifizierung)
Verschlüsselung: 3DES, AES (128-Bit, 192-Bit, 256-Bit)
Authentifizierung: MD5, SHA-1, SHA-256, SHA-384, SHA-512
VLANs
802.1Q-VLAN-Tags pro Gerät/pro Schnittstelle: 4.094/4.094
Aggregatschnittstellen (802.3ad), LACP

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

Netzwerkadressübersetzung
NAT-Modi (IPv4): statische IP-Adresse, dynamische IP-Adresse, dynamische IP-Adresse und Port (Portadressübersetzung)
NAT64, NPTv6
Zusätzliche NAT-Funktionen: dynamische IP-Adressenreservierung, anpassbare Überbelegung dynamischer IP-Adressen und Ports
Hochverfügbarkeit
Modi: aktiv/aktiv, aktiv/passiv
Fehlererkennung: Pfadüberwachung, Schnittstellenüberwachung
Zero Touch Provisioning (ZTP)
Erhältlich bei SKUs mit „ZTP“ in der Bezeichnung (PA-850-ZTP, PA-820-ZTP) Erfordert Panorama 9.1.3 oder höher

Tabelle 3: Hardwarespezifikationen der PA-800 Series

E/A
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 Hochverfügbarkeit (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
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

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

Platzbedarf im Rack (Abmessungen)
PA-850: 1U, 19-Zoll-Standard-Rack (4,45 cm H x 36,83 cm T x 43,5 cm B) PA-820: 1U, 19-Zoll-Standard-Rack (4,45 cm H x 35,56 cm T x 43,5 cm B)
Gewicht (Netto-/Versandgewicht)
PA-850: 6,12 kg/9,75 kg PA-820: 4,99 kg/8,16 kg
Sicherheitsstandards
cTUVus, CB
EMI
FCC-Klasse A, CE-Klasse A, VCCI-Klasse A
Zertifizierungen
Siehe paloaltonetworks.com/company/certifications.html
Umgebungsbedingungen
Betriebstemperatur: 0 °C bis 40 °C Temperatur bei Nichtbetrieb: -20 °C bis 70 °C
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.

paloalto NETWORKS

Oval Tower, De Entrée 99–197
1101 HE Amsterdam, Niederlande

Telefon: +31 20 888 1883
Vertrieb: +800 7239771
Support: +31 20 808 4600

www.paloaltonetworks.de