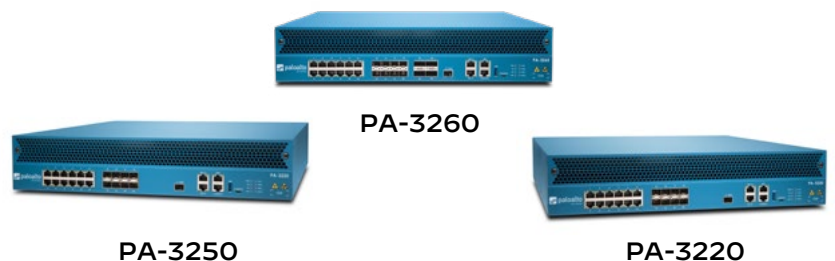


## Highlights

- Die erste ML-gestützte NGFW
- Achtmaliger 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)

# PA-3200 Series

Die PA-3200 Series von Palo Alto Networks – bestehend aus PA-3260, PA-3250 und PA-3220 – sind ML-gestützte NGFWs, die für den Einsatz mit Internetgateways in Hochgeschwindigkeitsumgebungen ausgelegt sind. Die PA-3200 Series-Modelle schützen den gesamten Datenverkehr, einschließlich verschlüsselter Daten, mithilfe dedizierter Verarbeitungs- und Speicherkomponenten, die für die Netzwerkverbindung, Sicherheit, Gefahrenabwehr und Verwaltung sorgen.



Die PA-3200 Series nutzt das Betriebssystem PAN-OS®, wie alle Next-Generation Firewalls 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 unbekanntes 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 (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.

### Identifiziert und kategorisiert alle 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-IDs 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.

### Bietet Sicherheit für Benutzer an jedem Ort und auf jedem Gerät und passt Richtlinien anhand von Benutzeraktivitäten an

- 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 Repositories integrieren, um Benutzerinformationen zu nutzen: WLAN-Controller, VPNs, Verzeichnisse, 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 dynamische Sicherheitsmaßnahmen umgesetzt, um verdächtige oder böswillige Benutzer zu blockieren.

### Verhindert bösartige 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.

### Erweitert den nativen Schutz auf alle Angriffsvektoren mit cloudbasierten Security Subscriptions

- **Threat Prevention** – überprüft den gesamten Datenverkehr, um bekannte Schwachstellen, Malware, Schwachstellenexploits, Spyware, Command-and-Control (C2) und benutzerdefinierte Intrusion Prevention System-(IPS-)Signaturen automatisch zu blockieren.
- **WildFire®-Malwareabwehr** – vereint Inlineschutz durch maschinelles Lernen mit zuverlässigen cloudbasierten Analysen, um neue Bedrohungen in Echtzeit abzuwehren und Umgehungsversuche schneller als je zuvor zu erkennen und zu verhindern.
- **URL Filtering** – verhindert den Zugriff auf bösartige Websites und schützt Benutzer vor webbasierten Bedrohungen, einschließlich Phishing nach Anmeldedaten.
- **DNS Security** – erkennt und blockiert bekannte und unbekannte Bedrohungen über DNS (einschließlich Ausschleusung von Daten über DNS-Tunneling). Damit können Sie verhindern, dass Angreifer die Sicherheitsmaßnahmen umgehen, benötigen keine separaten Tools und müssen auch keine Änderungen am DNS-Routing vornehmen.
- **IoT Security** – erkennt alle nicht verwalteten Geräte in Ihrem Netzwerk schnell und genau mit ML, ohne dass zusätzliche Sensoren eingesetzt werden müssen. Identifiziert Risiken und Schwachstellen, wehrt bekannte und unbekannte Bedrohungen ab, gibt risikobasierte Richtlinienempfehlungen und automatisiert die Durchsetzung.

## Einziger 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.
- Ermöglicht eine konsistente und vorhersehbare Leistung, wenn Security Subscriptions aktiviert sind.
- Vermeidet Latenzzeiten, indem der Datenverkehr in einem einzigen Durchgang mit einem streambasierten, einheitlichen Signaturabgleich anhand aller Signaturen überprüft wird.

## Ermöglicht 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-3200 Series**

	PA-3260	PA-3250	PA-3220
Firewalldurchsatz (HTTP/Appmix)*	8,3/9,2 Gbit/s	5,6/6,2 Gbit/s	4,5/5,0 Gbit/s
Threat-Prevention-Durchsatz (HTTP/Appmix)†	4,5/5,0 Gbit/s	2,7/3,4 Gbit/s	2,2/2,8 Gbit/s
IPsec-VPN-Durchsatz‡	5,0 Gbit/s	3,2 Gbit/s	2,8 Gbit/s
Max. Anz. Sitzungen	3 Mio.	2 Mio.	1 Mio.
Neue Sitzungen pro Sekunde§	105.000	73.000	57.000
Virtuelle Systeme (Basis/max.)	1/6	1/6	1/6

Hinweis: Ergebnisse wurden auf PAN-OS 10.0 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, 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.

|| Für zusätzliche virtuelle Systeme über die Basismenge hinaus muss eine separate Lizenz erworben werden.

**Tabelle 2: Netzwerkfunktionen der PA-3200 Series**

Schnittstellenmodi
L2, L3, Tap, Virtual Wire (transparenter Modus)
Routing
OSPFv2/v3 mit ordnungsgemäßem Neustart, BGP mit ordnungsgemäßem Neustart, RIP, statisches Routing
Richtlinienbasierte Weiterleitung
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 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

**Tabelle 2: Netzwerkfunktionen der PA-3200 Series (Forts.)**

VLANs
802.1Q-VLAN-Tags pro Gerät/pro Schnittstelle: 4.094/4.094
Aggregatschnittstellen (802.3ad), LACP
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, HA-Clustering
Fehlererkennung: Pfadüberwachung, Schnittstellenüberwachung
Zero Touch Provisioning (ZTP)
Erhältlich bei SKUs mit „ZTP“ in der Bezeichnung (PA-3260-ZTP, PA-3250-ZTP, PA-3220-ZTP)
Erfordert Panorama 9.1.3 oder höher

**Tabelle 3: Hardwarespezifikationen der PA-3200 Series**

E/A
PA-3260: 10/100/1000 (12), 1G/10G-SFP/SFP+ (8), 40G-QSFP+ (4)
PA-3250: 10/100/1000 (12), 1G/10G-SFP/SFP+ (8)
PA-3220: 10/100/1000 (12), 1G-SFP (4), 1G/10G-SFP/SFP+ (4)
Management – E/A
10/100/1000 Out-of-Band-Managementport (1), 10/100/1000 High Availability (2), 10G-SFP+ -HA (1), RJ-45 Konsolenport (1), Micro USB (1)
Speicherkapazität
240 GB SSD
Stromversorgung (Durchschn./max. Stromverbrauch)
Redundanter 650-W-Gleich- oder Wechselstrom (180/240)
Max. BTU/h
819
Eingangsspannung (Eingangsfrequenz)
AC: 100–240 V AC (50/60Hz)
DC: -48 V bei 4,7 A, -60 V bei 3,8 A
Max. Stromverbrauch
AC: 2,3 A bei 100 VAC, 1,0 A bei 240 VAC
DC: -48 V bei 4,7 A, -60 V bei 3,8 A
Mittlere Betriebsdauer zwischen Ausfällen (MTBF)
14 Jahre

**Tabelle 3: Hardwarespezifikationen der PA-3200 Series (Forts.)**

Platzbedarf im Rack (Abmessungen)
2U, 19-Zoll-Standardrack (8,89 cm H x 52,15 cm T x 44,04 cm B)
Gewicht (Netto-/Versandgewicht)
13,15 kg/18,82 kg
Sicherheitsstandards
cTUVus, CB
EMI
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>
Umgebungsbedingungen
Betriebstemperatur: 0 ° bis 50 °C
Temperatur bei Nichtbetrieb: -20 °C bis 70 °C
Feuchtetoleranz: 10 bis 90 %
Max. Einsatzhöhe: 3.048 m
Luftstrom: von vorne nach hinten

Um mehr über die Funktionen und die damit verbundenen Kapazitäten der PA-3200 Series zu erfahren, besuchen Sie [paloaltonetworks.com/network-security/next-generation-firewall/pa-3200-series](https://paloaltonetworks.com/network-security/next-generation-firewall/pa-3200-series).