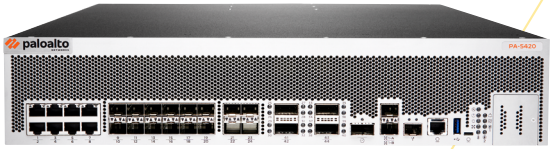
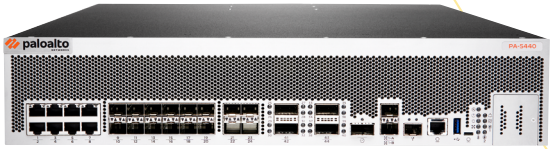
PA-5410



PA-5420

PA-5430



PA-5440

# PA-5400 Series

Die ML-gestützten Next-Generation Firewalls der PA-5400 Series von Palo Alto Networks mit den Modellen PA-5430, PA-5420 und PA-5410 eignen sich perfekt für Rechenzentren, Internetgateways und Bereitstellungen von Serviceanbietern in Hochgeschwindigkeitsumgebungen und bieten effektiven Schutz für den gesamten Datenverkehr, einschließlich verschlüsselter Daten.

## Highlights

- Die erste ML-gestützte NGFW
- Elfmaliger Leader im Gartner Magic Quadrant für Netzwerkfirewalls
- Leader im Bericht „The Forrester Wave: Enterprise Firewalls“, Q4 2022
- Bietet 5G-native Sicherheit für die 5G-Transformation von Serviceanbietern und Unternehmen sowie für Multi-Access Edge Computing (MEC)
- 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 Sicherheitsdiensten
- Unterstützt die zentralisierte Verwaltung mit Panorama-Netzwerksicherheitsmanagement
- Nutzt AIOps zur vollen Ausnutzung von Sicherheitsinvestitionen und zur Vermeidung von Geschäftsunterbrechungen

Mit der ersten ML-gestützten Next-Generation Firewall können Sie bisher unbekannte Bedrohungen abwehren. Sie profitieren von umfassenden Einblicken in und durchgehendem Schutz für Ihre gesamte IT-Umgebung – inklusive IoT-Geräten – und vermeiden Bedienfehler mit automatisierten Richtlinienempfehlungen.

Die PA-5400 Series nutzt das Betriebssystem PAN-OS, wie alle NGFWs von Palo Alto Networks. PAN-OS klassifiziert nativ den gesamten Netzwerkverkehr (einschließlich aller Anwendungsdaten, Bedrohungen und legitimen Inhalte) und ordnet die einzelnen Pakete anschließend 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 datei-basierter 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 IoT-Geräte 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 und Verschlüsselung (TLS/SSL). und bietet automatische Erkennung und Kontrolle neuer Anwendungen mit dem SaaS Security-Sicherheitsabonnement, um die stetig steigende Anzahl der SaaS-Apps im Griff zu behalten.
- 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.

Weitere Informationen finden Sie in der Lösungsbeschreibung zu App-ID.

## 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 Sicherheits-maßnahmen 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- und Linux-Desktops bzw. -Laptops; Citrix- und Microsoft-VDI sowie Terminal-Server).
- Verhindert, dass Anmeldedaten des Unternehmens auf Websites von Dritten gelangen, und unterbindet die Nutzung gestohlener Anmeldedaten durch die konsequente Aktivierung der Multifaktor-Authentifizierung (MFA) auf der Netzwerkebene für jede Anwendung, ohne dass die Anwendungen geändert werden müssen.
- Setzt Sicherheitsmaßnahmen dynamisch auf der Grundlage des Benutzerverhaltens um, um verdächtige oder böswillige Benutzer zu blockieren.
- Bietet konsistente, standortunabhängige Authentifizierungs- und Autorisierungsprozesse für sämtliche Benutzer und beliebige Identitätsspeicher, um die Umstellung auf Zero Trust voranzutreiben – mit der Cloud Identity Engine, einer brandneuen cloudgestützten Architektur für die identitätsbasierte Sicherheit.

Näheres erfahren Sie in der Lösungsübersicht zur Cloud Identity Engine.

## Schutz vor bösartigen Aktivitäten, die in verschlüsseltem Datenverkehr verborgen sind

- 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, 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 (Entschlüsselungsspiegelung) und diese an Tools zur Datenverkehrserfassung für Forensik, Verlaufsprotokollierung oder Data Loss Prevention (DLP) zu senden.
- Unterstützt die intelligente Weiterleitung des Datenverkehrs (ob TLS oder nicht, entschlüsselt oder verschlüsselt) an Drittanbietertools mit einem Network Packet Broker sowie die Optimierung der Netzwerkleistung und Reduzierung der Betriebskosten.

Lesen Sie unser Whitepaper zum Thema Entschlüsselung, um zu erfahren, wo, wann und wie Sie eingehenden Datenverkehr entschlüsseln sollten, um Ihr Unternehmen vor verschlüsselten Bedrohungen zu schützen.

## Zentralisierte Verwaltung und Transparenz

- Unterstützt 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.

## Turbo für Sicherheitsinvestitionen und weniger Geschäftsunterbrechungen mit AIOps

- AIOps for NGFW bietet kontinuierliche, an den Kunden angepasste Best-Practice-Empfehlungen, damit Sie Ihren Sicherheitsstatus stärken und Ihre Sicherheitsinvestitionen voll ausschöpfen können.
- Es nutzt ML-Funktionen und aussagekräftige Telemetriedaten, um intelligente Prognosen zu Status, Leistung und Kapazität der Firewalls sowie zu potenziellen Problemen zu bieten. Außerdem stellt es praxistaugliche Einblicke zur Behebung dieser Probleme bereit.

## Erkennung und Abwehr komplexer Bedrohungen mit Cloud-Delivered Security Services

Moderne ausgeklügelte Cyberattacken können innerhalb von 30 Minuten bis zu 45.000 Schadcodevarianten generieren und diese mithilfe mehrerer Bedrohungsvektoren und raffinierter Techniken in die Zielumgebung einschleusen. 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 all 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:

- **Advanced Threat Prevention**: Stoppen Sie bekannte Exploits, Malware, Spyware und C2-Aktivitäten mit unserer branchenweit einzigartigen Prävention von Zero-Day-Angriffen, um 60 % mehr unbekannte Injection-Angriffe und 48 % mehr gut getarnte Command-and-Control-Kommunikation zu blockieren als herkömmliche IPS-Lösungen.
- **Advanced WildFire**: Schützen Sie Ihre Dateien mit der branchenweit größten Engine für Threat Intelligence und Malwareschutz, die bekannte, unbekannte und gut getarnte Malware automatisch und bis zu 60-mal schneller stoppt.
- **Advanced URL Filtering**: Nutzen Sie die branchenweit einzigartige Lösung, die den Zugriff auf bekannte und unbekannte gefährliche Websites in Echtzeit blockiert, 88 % der schädlichen URLs 48 Stunden vor anderen Anbietern stoppt und so 40 % mehr webbasierte Angriffe vereitelt und für sicheren Internetzugang sorgt.
- **DNS Security**: Diese Lösung erkennt 40 % mehr Bedrohungen und vereitelt 85 % der Malwareangriffe, bei denen die Angreifer DNS als Command-and-Control-Kanal und für den Datendiebstahl nutzen – ganz ohne Änderungen an der Infrastruktur.

- **Enterprise DLP**: Minimieren Sie das Risiko eines Datenlecks, stoppen Sie nicht richtlinienkonforme Datentransfers und sorgen Sie unternehmensweit für Compliance. All das gelingt dank einer doppelt so breiten DLP-Abdeckung wie bei jeder anderen cloudbasierten DLP-Lösung der Enterprise-Klasse.
- **SaaS Security**: Mit dem branchenweit ersten Next-Generation CASB halten Sie mit der explosionsartig steigenden SaaS-Nutzung Schritt, denn dieser erkennt und sichert alle Apps (unabhängig vom genutzten Protokoll) automatisch.
- **IoT Security**: Schützen Sie alle Geräte aus dem Internet der Dinge und implementieren Sie Zero-Trust-Gerätesicherheit mit den intelligentesten Sicherheitsmaßnahmen für Smart Devices 20-mal schneller.

## 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 Subscriptions.)

## 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.

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

**Tabelle 1: Leistung und Kapazitäten der PA-5400 Series**

| | PA-5410 | PA-5420 | PA-5430 | PA-5440 |
|---|---|---|---|---|
| Firewalldurchsatz (HTTP/Appmix)* | 52,4/43,5 Gbit/s | 68,0/56,0 Gbit/s | 79,0/61,0 Gbit/s | 93,5/72,0 Gbit/s |
| Threat-Prevention-Durchsatz (HTTP/Appmix)† | 26,0/26,7 Gbit/s | 33,0/32,0 Gbit/s | 43,0/40,0 Gbit/s | 61,5/52,0 Gbit/s |
| IPsec-VPN-Durchsatz‡ | 21 Gbit/s | 28,7 Gbit/s | 42 Gbit/s | 58 Gbit/s |
| Max. Anz. Sitzungen | 3,6 Mio. | 5 Mio. | 7,2 Mio. | 12 Mio. |
| Neue Sitzungen pro Sekunde§ | 270.000 | 370.000 | 380.000 | 390.000 |
| Virtuelle Systeme (Basis/max.)‖ | 10/20 | 15/65 | 25/125 | 25/225 |

Hinweis: Ergebnisse wurden auf PAN-OS 11.0 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.

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

| Tabelle 2: Netzwerkfunktionen der PA-5400 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) |
| Unterstützung von Point-to-Point Protocol Over Ethernet (Punkt-zu-Punkt-Protokoll über Ethernet, PPPoE) und DHCP für die dynamische Adresszuweisung |
| Multicast: PIM-SM, PIM-SSM, IGMP v1, v2 und v3 |
| Bidirectional Forwarding Detection (BFD) |

| Tabelle 2: Netzwerkfunktionen der PA-5400 Series (Fortsetzung) |
|---|
| **SD-WAN** |
| Messung der Pfadqualität (Jitter, Paketverlust, Latenz) |
| Auswahl des Ursprungspfades (PBF) |
| Schlüsselaustausch: manuelle Schlüssel, IKEv1 und IKEv2 (vorab ausgetauschte Schlüssel, zertifikatsbasierte Authentifizierung) |
| **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 |
| **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 |
| **Mobile Netzwerkinfrastruktur*** |
| 5G-Sicherheit |
| 5G-MEC-Sicherheit (Multi-Access Edge Computing) |
| GTP-Sicherheit |
| SCTP-Sicherheit |

* Weitere Informationen finden Sie in unserem Datenblatt zu ML-gestützten NGFWs für 5G.

| Tabelle 3: Hardwarespezifikationen der PA-5400 Series |
|---|
| **E/A** |
| 1G/2,5G/5G/10G (8), 1G/10G-SFP/SFP+ (12), 1G/10G/25G-SFP/SFP+/SFP28 (4), 40G/100G-QSFP+/QSFP28 (4) |
| **Management E/A** |
| 1G SFP Out-of-Band-Managementport (1),<br>1G SFP Hochverfügbarkeit (2), 40G QSFP+ Hochverfügbarkeit (1),<br>Konsolenport RJ-45 (1), Micro-USB |
| **Speicherkapazität** |
| 480-GB-SSD-Paar, Systemspeicher |
| **Stromversorgung (durchschn./max. Stromverbrauch)** |
| 630/760 W |

| Tabelle 3: Hardwarespezifikationen der PA-5400 Series (Fortsetzung) |
|---|
| **Max. BTU/h** |
| 1.638 |
| **Stromversorgung (Basis/max.)** |
| 1:1 vollständig redundant (2/2) |
| **Wechselstromeingangsspannung (Eingangsfrequenz)** |
| 100–240 V AC (50–60 Hz) |
| **Wechselstromausgangsspannung** |
| 1.200 W/Stromversorgung |
| **Max. Stromverbrauch** |
| Wechselstrom: 7 A bei 100 V AC, 3 A bei 240 V AC |
| Gleichstrom: 15 A bei -48 V DC; 12 A bei -60 V DC |
| **Max. Einschaltstrom** |
| Wechselstrom: 50 A bei 230 V AC; 50 A bei 120 V AC |
| Gleichstrom: 200 A bei 72 V DC |
| **Mittlere Betriebsdauer zwischen Ausfällen (MTBF)** |
| 22 Jahre |
| **Platzbedarf im Rack (Abmessungen)** |
| 2U, 19-Zoll-Standard-Rack (H: 8,8 cm x T: 57,2 cm x B: 44 cm) |
| **Gewicht (Netto-/Versandgewicht)** |
| 16 kg/22,1 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 50 °C |
| Lagertemperatur: -20 °C bis 70 °C |
| Luftfeuchtigkeitstoleranz: 10 % bis 90 % |
| Max. Einsatzhöhe: 3.048 m |
| Luftstrom: von vorne nach hinten |

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