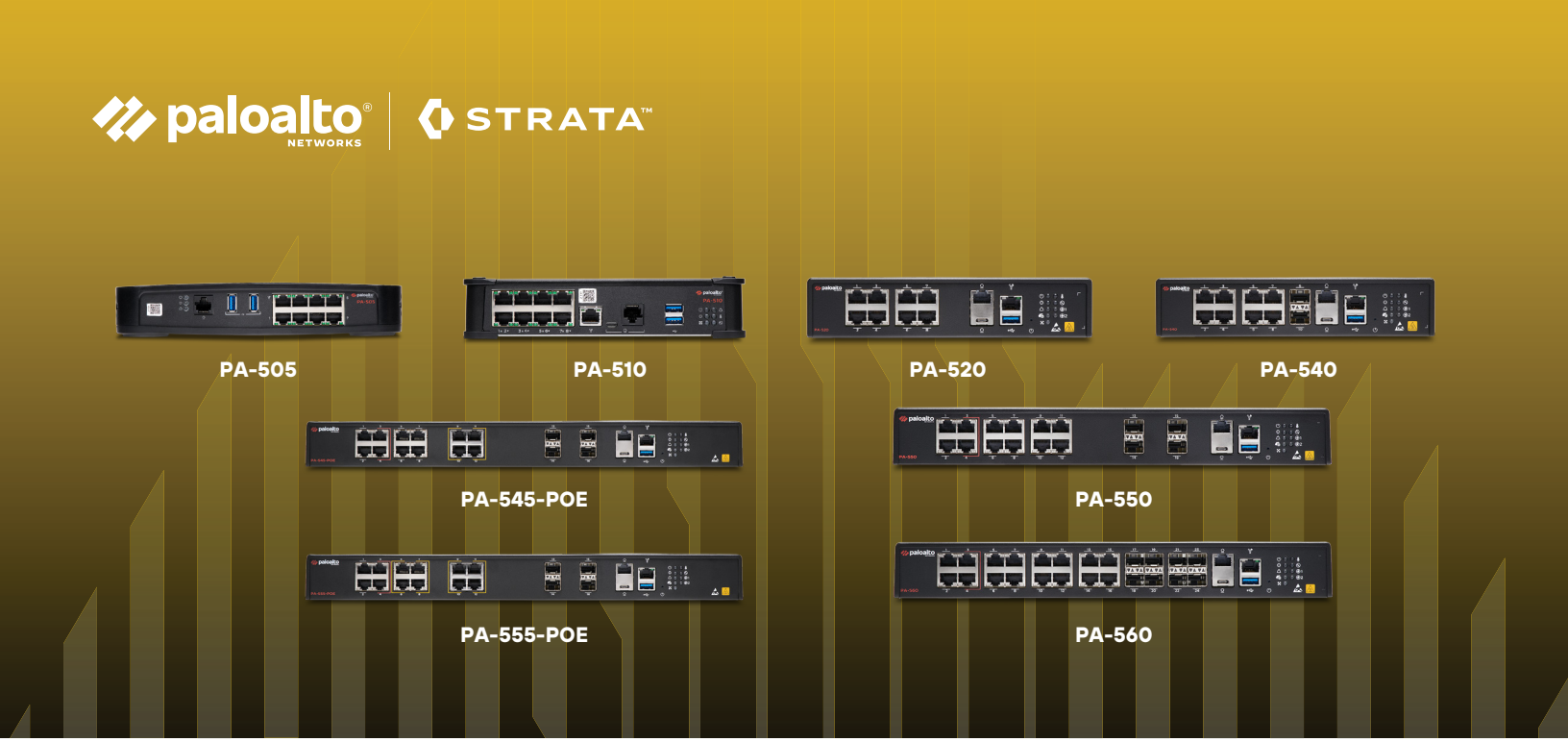

PA-500 Series

Die Next-Generation Firewalls (NGFWs) der PA-500 Series von Palo Alto Networks umfassen die Modelle PA-505, PA-510, PA-520, PA-540, PA-545-POE, PA-550, PA-555-POE und PA-560. Diese Serie bringt ML-gestützte NGFW-Funktionen in verteilte Unternehmensniederlassungen, Einzelhandelsstandorte und mittelständische Unternehmen.

Die PA-500 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 dann unabhängig vom Standort oder Gerätetyp einem Benutzer zu. In Abhängigkeit von den Anwendungen, Inhalten und Benutzern (den Faktoren, die für Ihr Geschäft relevant sind) wird entschieden, welche Sicherheitsrichtlinien anzuwenden sind. Das stärkt die Sicherheit und verkürzt die zur effektiven Reaktion auf Sicherheitsvorfälle erforderliche Zeit. PAN-OS integriert maschinelles Lernen (ML) in den Kern der Firewall, um eine signaturlose Inline-Abwehr dateibasierter Angriffe zu bieten und bisher unbekannte Phishingversuche zu erkennen und sofort zu stoppen.

Highlights

- Leistungsstarke NGFW-Serie für Unternehmensniederlassungen.
- Unterstützt durch Precision AI®, eine bahnbrechende KI-gesteuerte Engine, die Bedrohungen in Echtzeit analysiert und abwehrt.
- Hohe Portdichte mit bis zu 24 Kupfer- und Glasfaserschnittstellen.
- Bis zu 330 W Power over Ethernet (PoE)-Unterstützung.
- IEEE 802.3bt-Unterstützung mit maximal 90 W Leistung pro PoE-Port.
- Vereinfacht Bereitstellung mit Zero-Touch-Provisionierung (ZTP)
- Unterstützt Hochverfügbarkeit mit Aktiv/Aktiv- und Aktiv/Passiv-Modus
- Entwickelt mit Single-Pass-Architektur für vorhersehbare Leistung bei Sicherheitsservices.
- Verwaltet mit Strata™ Cloud Manager, der branchenweit ersten KI-gestützten Lösung für einheitliche Management- und Betriebsprozesse für Netzwerksicherheit.
- Leader im Gartner® „Magic Quadrant™ for Network Firewalls“ 2025.
- Leader im Bericht „The Forrester Wave™: Enterprise Firewall Solutions, Q4 2024.

Anwendungsidentifizierung und -kategorisierung mit vollständiger Layer-7-Prüfung

App-ID™ identifiziert und kategorisiert alle Anwendungen auf allen Ports jederzeit mit vollständiger Layer-7-Prüfung und unterstützt die folgenden Funktionen:

- Nutzt erweiterte Techniken wie Protokolldekodierung, Heuristik und Signaturabgleich, um Anwendungen im gesamten Netzwerk unabhängig vom verwendeten Port, Protokoll oder den verwendeten Verschlüsselungsmethoden genau zu identifizieren. Der optionale App-ID Cloud Engine (ACE)-Dienst bietet On-Demand-App-IDs für SaaS-Anwendungen.
- Vermittelt ein umfassendes Verständnis der mit verschiedenen Anwendungen verbundenen Risiken und Werte, was zu fundierten Entscheidungen über Netzwerksicherheitsrichtlinien beiträgt.
- Ermöglicht die effektive Durchsetzung von Sicherheitsrichtlinien, die auf bestimmte Anwendungen zugeschnitten sind, indem die Identifizierung und Kontrolle von Anwendungen auf Firewall-Ebene zentralisiert wird.
- Identifiziert und verwaltet getarnte oder benutzerdefinierte Anwendungen, die herkömmliche Sicherheitsmaßnahmen normalerweise umgehen.
- Aktualisiert kontinuierlich seine Anwendungsidentifikationen und stellt so sicher, dass es den neuesten Anwendungstrends und -taktiken standhält.
- Verwendet modernste KI-Techniken, um die Präzision bei der Identifizierung und Kategorisierung KI-gestützter Anwendungen zu verbessern. Diese Techniken stellen sicher, dass selbst die fortschrittlichsten und dynamischsten Anwendungen im Netzwerk genau erkannt und entsprechend gehandhabt werden.

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

Durchsetzung der Benutzersicherheit

NGFWs der PA-500 Series gewährleisten die Sicherheit der Benutzer an jedem Ort und auf jedem Gerät und passen die Richtlinien an ihre Aktivitäten an. Dazu gehören folgende Fähigkeiten:

- Unterstützen von Transparenz, Sicherheitsrichtlinien, Berichten und Forensik auf der Grundlage von Benutzern, Gruppen und IP-Adressen.
- Anwenden einheitlicher Richtlinien, unabhängig vom Standort (Büro, Zuhause, unterwegs usw.) und Geräte der Benutzer. Zu diesen Geräten gehören mobile iOS- und Android-Geräte, Desktop und Laptops mit macOS, Windows und Linux, Citrix und Microsoft VDI sowie Terminalserver.
- Nutzen der IP-Geolokalisierung, um Sicherheitsrichtlinien basierend auf dem geografischen Standort automatisch durchzusetzen. Sie können die Angriffsfläche reduzieren, Compliance-Anforderungen erfüllen und den Anwendungszugriff kontrollieren, indem Sie den Datenverkehr von und zu bestimmten Ländern oder Regionen blockieren.
- Konsistentes, standortunabhängiges Authentifizieren und Autorisieren für Ihre Benutzer, unabhängig vom Standort oder Speicherort des Identitätsspeichers (Cloud- und lokale Verzeichnisse oder beides), um die Umstellung auf Zero Trust voranzutreiben – mit der Cloud Identity Engine, einer cloudgestützten Architektur für die identitätsbasierte Sicherheit.
- Sichern aller Anwendungen mit passwortloser Authentifizierung, egal ob lokal, als SaaS oder hybrid.
- Bereitstellen dynamischer Sicherheitsmaßnahmen basierend auf dem Benutzerverhalten, um verdächtige oder böswillige Benutzer einzuschränken, indem Sie Cloud Dynamic User Groups (CDUGs) auf der Firewall definieren, um risikobasierte, zeitgebundene Sicherheitsmaßnahmen zu ergreifen, ohne auf die Anwendung von Änderungen an Benutzerverzeichnissen warten zu müssen.
- Verhindern, dass sowohl Anmeldedaten des Unternehmens auf Websites von Dritten gelangen als auch gestohlene Anmeldedaten erneut genutzt werden, indem die Multi-Faktor-Authentifizierung (MFA) auf der Netzwerkebene für jede Anwendung ohne Änderungen aktiviert wird.

- Einfaches Integrieren in eine Vielzahl von Repositories zur Arbeit mit Benutzerinformationen, einschließlich Wireless-LAN-Controllern, VPNs, Verzeichnisservern und SIEM-Tools (Security Information and Event Management).
- Automatisieren von Richtlinienempfehlungen, um Zeit zu sparen und das Risiko von Bedienfehlern zu reduzieren.

Weitere Informationen finden Sie in der Lösungsübersicht zur Cloud Identity Engine.

Einzigartiger Ansatz zur Paketverarbeitung

NGFWs der PA-500 Series verarbeiten Pakete mithilfe einer Single-Pass-Architektur. Mit diesem Ansatz können die NGFWs folgende Aufgaben ausführen:

- Durchführen von Netzwerkfunktionen, Richtliniensuche, -anwendung und -dekodierung sowie Signaturabgleich für alle Bedrohungen und Inhalte in einem einzigen Durchgang. So wird der Verarbeitungsaufwand für die Ausführung mehrerer Funktionen in einem einzelnen Sicherheitssystem erheblich reduziert.
- Vermeiden von Latenzzeiten, indem der Datenverkehr in einem einzigen Durchgang mit einem streambasierten, einheitlichen Signaturabgleich anhand aller Signaturen überprüft wird.
- Ermöglichen einer konsistenten und vorhersehbaren Leistung, wenn Sicherheitsabonnements aktiviert sind (siehe Tabelle 1).

Bereit für Post-Quanten-Kryptographie

Die PA-500 Series ist ein für die Post-Quanten-Kryptografie geeignetes Gerät, das Ihnen hilft, mit PAN-OS 12.1 quantensichere Sicherheit in Hardware und Software zu erreichen. NGFWs der PA-500 Series unterstützen:

- Post-Quanten-Kryptografie (PQC) für PQC SSL/TLS-Entschlüsselung, PQC VPN Site-to-Site, PQC SSL/TLS Cipher Translation Proxy und PQC SSL/TLS-Serviceprofil für den Managementzugriff auf die Firewall.
- PQC-Algorithmen, einschließlich NIST-Standards wie ML-KEM, ML-DSA und SLH-DSA, sowie vorstandardisierte PQCs wie Classic McEliece, BIKE, HQC, Frodo-KEM und NTRU-Prime.

Schutz vor bösartigen Aktivitäten, die in verschlüsseltem Datenverkehr verborgen sind

NGFWs der PA-500 Series bieten folgende Möglichkeiten:

- Überprüfen und Anwenden der Richtlinien auf SSL/TLS-verschlüsselten Datenverkehr (sowohl eingehend als auch ausgehend), auf Datenverkehr, der SSLv3, TLSv1.1, TLSv1.2 und TLSv1.3 verwendet, sowie auf die Anwendungsprotokolle SMTP, WebSocket, gRPC, HTTP/1.0, HTTP/1.1 und HTTP/2.
- Entschlüsseln und Prüfen der SSL/TLS-Sitzungen mit den klassischen Schlüsselaustauschalgorithmen RSA, ECDHE, DHE und den Post-Quanten-Schlüsselaustauschstandards ML-KEM, HQC sowie den experimentellen Standards BIKE und Frodo-KEM.
- Erfassen von Kennzahlen zum TLS-Verkehr, beispielsweise die Menge des verschlüsselten Datenverkehrs, SSL/TLS-Versionen und Chiffren.
- Unterstützen solcher Suites wie den klassischen Schlüsselaustauschalgorithmen RSA, ECDHE und DHE sowie der Post-Quanten-Schlüsselaustausch ML-KEM und HQC – ohne dass eine Entschlüsselung erforderlich ist. Ermöglicht so zusätzliche Transparenz der kryptografischen Informationen aus allen SSL/TLS-Sitzungen, die die Firewall passieren.
- Aktivieren der Kontrolle über die Verwendung älterer TLS-Protokolle, unsicherer und veralteter Chiffren und falsch konfigurierter Zertifikate, einschließlich einer nicht übereinstimmenden Server Name Indication (SNI) zum Common Name (CN) des Zertifikats, um Risiken zu minimieren.

- Erleichtern der einfachen Bereitstellung einer Entschlüsselung. Sie können erweiterte integrierte Protokolle zur unabhängigen Behebung von Problemen in client- und serverseitigen Sitzungen nutzen, um eine nahtlose Fehlerbehebung zu gewährleisten, unabhängig davon, ob Zwischenzertifikate oder fixierte Zertifikate fehlen.
- Flexibles Aktivieren oder Deaktivieren der Entschlüsselung basierend auf URL-Kategorie, Quell- und Zielzone, Adresse, Benutzer, Benutzergruppe, Gerät und Port, um den Datenschutz und die Vorschrifteneinhaltung zu wahren.

Zusätzlich bietet diese Funktion Entschlüsselungsspiegelung, womit Sie eine Kopie des entschlüsselten Datenverkehrs von der Firewall erstellen und diese an Tools zur Datenverkehrserfassung für Forensik, Verlaufsprotokollierung oder Data Loss Prevention (DLP) senden können.

Lesen Sie das Whitepaper „Verschlüsselung: Warum, wo, wie?“, um mehr über die Entschlüsselung zu erfahren, mit der Sie Bedrohungen vorbeugen und Ihr Unternehmen schützen können.

Einheitliche KI-gestützte Management- und Betriebsprozesse mit Strata Cloud Manager

Verwalten Sie Ihre NGFWs der PA-500 Series mit Strata Cloud Manager, der Ihnen Folgendes ermöglicht:

- **Vollständige Transparenz für Ihre gesamte Netzwerksicherheit Erzielen** Sie über eine einheitliche Schnittstelle umfassende Echtzeittransparenz für Ihre gesamte Netzwerksicherheitslandschaft, einschließlich aller Benutzer, Anwendungen, Geräte und der wichtigsten Bedrohungen, die Ihre Aufmerksamkeit erfordern.
- **Komfortables und konsistentes Management des Netzwerksicherheitslebenszyklus Sicherheitsteams können Konfigurationen und Sicherheitsrichtlinien auf allen Sicherheitspunkten,** einschließlich SASE, Hardware- und Softwarefirewalls, sowie allen Sicherheitsservices verwalten – für eine größere Konsistenz und einen geringeren Aufwand.
- **Stärkung des Sicherheitsniveaus in Echtzeit Nutzen Sie KI-gestützte Analysen,** um Richtlinienanomalien zu erkennen, zu beheben und zu optimieren, wie z. B. Schatten- und redundante Richtlinien und zu freizügige oder ungenutzte Regeln. Verbessern Sie Ihre Sicherheitslage durch integrierte Best-Practice-Empfehlungen und sorgen Sie für die Compliance mit Branchen- und InfoSec-Standards.
- **Proaktive Behebung von Netzwerkunterbrechungen und Verbesserung der Benutzerfreundlichkeit Prognostizieren,** diagnostizieren und beheben Sie Netzwerkprobleme – z. B. Beeinträchtigungen der Benutzererfahrung, Kapazitätsengpässe, CVE-Sicherheitslücken, Probleme mit Dienstverbindungen und 130 weitere Problemkategorien – bis zu 90 Tage im Voraus, um einen reibungslosen Betrieb zu gewährleisten.
- **Schnelle Problemlösungen mit sofortigem Know-how stets griffbereit:** Mit Strata Copilot™, unserem KI-gestützten Assistenten mit einer Schnittstelle für natürliche Sprache, können Sie Sicherheits- und Betriebsprobleme schnell erkennen, verstehen und beheben, bevor sie eskalieren. Außerdem erhalten Sie durch die optimierte Erstellung von Fällen schnelle Unterstützung, wenn Sie sie am dringendsten benötigen.

Branchenführende cloudbasierte Sicherheitsservices, powered by Precision AI®

NGFWs der PA-500 Series bieten branchenführende Sicherheit mit cloudbasierten Sicherheitsservices (CDSS). Das Herzstück unserer CDSS ist Precision AI. Im Gegensatz zu herkömmlichen reaktiven Tools stärkt Precision AI Ihre Abwehr durch proaktive Bedrohungserkennung, Inline-Schutz und automatisierte Abwehr und stoppt so selbst die am besten getarnten, noch nie dagewesenen Angriffe, bevor sie Schaden anrichten. Gestützt auf Threat Intelligence unserer über 70.000 Kunden weltweit lernen unsere Cloud-Dienste kontinuierlich dazu, passen sich an und entwickeln sich weiter. CDSS ist nahtlos in unsere NGFW- und SASE-Plattformen integriert und bietet einheitlichen Schutz für Web, DNS, E-Mail, Anwendungen und mehr – unabhängig davon, wo sich Ihre Benutzer oder Daten befinden.

Ganz gleich, ob Sie hybride Arbeit bewältigen, die Cloud-Transformation vorantreiben oder sich gegen hochentwickelte Gegner verteidigen: CDSS mit Precision AI bietet Ihnen die Transparenz, Automatisierung und Sicherheit, die Sie brauchen, um die Nase vorn zu behalten.

Advanced Threat Prevention

Analysieren Sie täglich bis zu 673 Millionen neue Sitzungen und blockieren Sie proaktiv 28,2 Milliarden Bedrohungen in Echtzeit, darunter Zero-Day-Exploits, Malware, Command-and-Control-Verkehr (C2) und getarnte Techniken, um modernste Sicherheit in beispiellosem Ausmaß zu bieten.

Advanced WildFire

Stoppen Sie proaktiv täglich bis zu 450.000 neue Bedrohungen mit den leistungsstärksten Malwareschutz-Engines der Branche. Advanced WildFire® identifiziert und blockiert eine große Bandbreite fortgeschrittener Bedrohungen, darunter Zero-Day-Malware, Ransomware, Remote Access Trojans (RATs), manipulierte Dokumente und andere Techniken für getarnte Angriffe – bevor diese Ihr Unternehmen beeinträchtigen.

Advanced URL Filtering

Schützen Sie den Webzugriff, indem Sie täglich bis zu 151 Millionen Bedrohungen blockieren und gleichzeitig täglich 3,8 Milliarden neue URLs analysieren. Advanced URL Filtering schützt vor Phishing, Malware, Ransomware, C2-Kommunikation und getarnten webbasierten Angriffen.

Advanced DNS Security

Advanced DNS Security bietet Echtzeitschutz, der komplexe Bedrohungen auf Basis von DNS-Anfragen und -Antworten sofort blockiert – darunter DNS-Hijacking, Domain Generation Algorithms (DGA), DNS-Tunneling und C2-Callbacks. Es analysiert täglich über 1,1 Milliarden neue Domains und identifiziert bis zu 7,7 Millionen neue bösartige Domains, wodurch mehr als 2 Milliarden Bedrohungen inline verhindert werden. Diese leistungsstarke erste Verteidigungslinie identifiziert und stoppt Bedrohungen auf der DNS-Ebene – unabhängig davon, ob sie von außerhalb oder innerhalb des Netzwerks stammen.

Gerätesicherheit

Sichern Sie jedes angeschlossene Gerät mit einer auf die Branche (einschließlich Fertigung, Einzelhandel, Gesundheitswesen, Hightech und Unternehmen im Allgemeinen) zugeschnittenen Lösung und erreichen Sie innerhalb von 48 Stunden eine Geräteerkennungsrate von 90 % – durch priorisierte Schwachstellen- und Risikobewertungen. Identifizieren Sie außerdem Anomalien, erhalten Sie Empfehlungen für Sicherheitsrichtlinien zur Zugriffskontrolle mit den geringsten Berechtigungen und beheben Sie praktisch alle Schwachstellen – alles auf einer einzigen NetSec-Plattform.

SaaS Security

Entdecken und kontrollieren Sie den gesamten SaaS-Verbrauch mit Einblick in über 75.000 SaaS-Apps und DLP-Kontrollen für mehr als 150 SaaS-Apps. Verhindern Sie SaaS-Fehlkonfigurationen mit Management des Sicherheitsniveaus für über 117 SaaS-Apps sowie SaaS-Inline-Tenancy-Control für 39 Apps.

AI Access Security

Ermöglichen Sie die sichere Nutzung von GenAI mit Echtzeit-Einblick in GenAI-Apps, Benutzerzugriffskontrollen, Datenschutz und kontinuierlicher Risikoüberwachung. AI Access Security™ bietet einen branchenführenden Katalog mit über 2.500 GenAI-Apps, darunter über 15 GenAI-spezifische Anwendungsattribute zur genauen Identifizierung und Minderung von Risiken. Es umfasst Management des Sicherheitsniveaus für mehr als 13 GenAI-Apps und SaaS-Inline-Tenancy-Control für 11 Apps.

Advanced SD-WAN

Integrieren Sie SD-WAN, indem Sie es in Ihren bestehenden Firewalls mit integrierter Sicherheit aktivieren. Sorgen Sie für eine außergewöhnliche Endbenutzererfahrung und gewährleisten Sie SLAs, indem Sie SD-WAN-Pfadmessungen und Anwendungssteuerungsfunktionen nutzen, um Anwendungen intelligent auf die leistungsstärksten Pfade zu lenken.

Spezifikationen der PA-500 Series

Tabelle 1: Leistung und Kapazitäten der NGFWs der PA-500 Series								
	PA-505	**PA-510**	**PA-520**	**PA-540**	**PA-545-POE**	**PA-550**	**PA-555-POE**	**PA-560**
Firewalldurchsatz (Appmix)*	1,2 Gbit/s	1,8 Gbit/s	2,8 Gbit/s	3,8 Gbit/s	5,0 Gbit/s	6,5 Gbit/s	7,5 Gbit/s	8,5 Gbit/s
Threat-Prevention-Durchsatz (Appmix)†	0,8 Gbit/s	1,2 Gbit/s	1,8 Gbit/s	2,2 Gbit/s	3,0 Gbit/s	4,5 Gbit/s	5,0 Gbit/s	6,0 Gbit/s
IPsec-VPN-Durchsatz‡	0,4 Gbit/s	0,8 Gbit/s	1,5 Gbit/s	2,0 Gbit/s	3,0 Gbit/s	4,0 Gbit/s	4,5 Gbit/s	5,5 Gbit/s
Max. Anzahl simultaner Sitzungen§	64.000	98.000	148.000	248.000	298.000	398.000	448.000	598.000
Neue Sitzungen pro Sekunde‖	10.000	15.000	25.000	50.000	55.000	70.000	75.000	100.000
Virtuelle Systeme (Basis/max.)#	—	—	—	1/2	1/2	1/5	1/5	1/5

Hinweis: Ergebnisse wurden auf PAN-OS 12.1 gemessen.

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

† Der Threat-Prevention-Durchsatz wurde unter Verwendung von 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 max. Anzahl simultaner Sitzungen wurde unter Verwendung von 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-500 Series
Schnittstellenmodi
L2-Modus (nicht verfügbar auf MC-LAG-Aggregatschnittstellen), L3, Tap- und Virtual Wire-Modus (transparenter Modus).
Routing
OSPFv2/v3 und MP-BGP mit ordnungsgemäßem Neustart, RIP und statischem Routing.
Richtlinienbasierte Weiterleitung.
PPPoE- und DHCP-Clients werden für die dynamische Adresszuweisung sowohl für IPv4 als auch für IPv6 unterstützt.
DHCPv4-Server.
Multicast: PIM-SM, PIM-SSM, IGMPv2 und v3.
Advanced SD-WAN
Messung der Pfadqualität (Jitter, Paketverlust und Latenz)
Bandbreitenüberwachung.
Schlüsselaustausch: manueller Schlüssel, IKEv1 und IKEv2 (vorinstallierter Schlüssel (PSK), zertifizierungsbasierte Authentifizierung).
Post-Quanten-PPK.
Multi-VR- und -LR-Unterstützung über das SD-WAN Overlay.
Prisma® Access Hub (hybrides SASE).
Autonomous Digital Experience Management (ADEM) für NGFW-Unterstützung
IPv6
IPv6-Prüfung im L2-, L3-, Tap- und Virtual Wire-Modus (transparenter Modus).
Unterstützung für Dual-Stack- und reine IPv6-Netzwerke.
Funktionen: IPv6-Geolokalisierung, OSPFv3, MP-BGP, NAT64 und NPTv6.
DHCPv6-Client mit Präfixdelegation (PD)-Unterstützung. Unterstützung für Stateless Address Autoconfiguration (SLAAC)-Server.

Tabelle 2: Netzwerkfunktionen der PA-500 Series (Fortsetzung)
IPsec und SSL-VPN
Schlüsselaustausch: manueller Schlüssel, IKEv1 und IKEv2 (vorinstallierter Schlüssel (PSK), zertifizierungsbasierte Authentifizierung).
Verschlüsselung: 3DES und AES (128-Bit, 192-Bit und 256-Bit).
Authentifizierung: MD5, SHA-1, SHA-256, SHA-384 und SHA-512.
Sicherer Zugang über IPsec und SSL-VPN-Tunnel mit GlobalProtect® Gateway und Portalen.*
VLANs
802.1Q-VLAN-Tags pro Gerät/pro Schnittstelle: 4.094/4.094.
Aggregatschnittstellen (802.3ad), LACP

* Erfordert eine GlobalProtect-Lizenz.

Tabelle 3: Hardwarespezifikationen der PA-500 Series
EIN- UND AUSGABE
PA-505: 1G-RJ45 (7) PA-510: 1G-RJ45 (8) PA-520: 1G-RJ45 (8) PA-540: 1G RJ45 (8), 1G SFP (2) PA-545-POE: 1G RJ45 (8), 1G/2,5G (4)/PoE, 1G SFP (4) PA-550: 1G RJ45 (12), 1G SFP (2), 1G/10G SFP/SFP+ (2) PA-555-POE: 1G RJ45 (4), 1G RJ45 (4)/PoE, 1G/2,5G (4)/PoE, 1G SFP (2), 1G/10G SFP/SFP+ (2) PA-560: 1G RJ45 (16), 1G SFP (4), 1G/10G SFP/SFP+ (4)
Managementein- und -ausgabe
PA-505: 10/100/1000 Out-of-Band-Managementport (1), USB-Port (2) und RJ45-Konsolenport (1) PA-510: 10/100/1000 Out-of-Band-Managementport (1), USB-Port (2), RJ45-Konsolenport (1) und Micro-USB-Konsolenport (1) PA-520, PA-540, PA-545-POE, PA-550, PA-555-POE, PA-560: 10/100/1000 Out-of-Band-Managementport (1), USB-Port (1), RJ45-Konsolenport (1) und Micro-USB-Konsolenport (1)
Speicherkapazität
PA-505, PA-510: 128 GB PA-520, PA-540, PA-545-POE, PA-550, PA-555-POE: 120 GB PA-560: 240 GB
Trusted Platform Module (TPM)
Integriert mit TPM für sicheren Start, Hardware-Root of Trust und Sicherung von System-Secrets.
Power Over Ethernet
PA-545-POE PoE-Kapazität insgesamt: 181 W, PoE-Ports (4), maximale Last pro Port: 90 W PA-555-POE PoE-Kapazität insgesamt: 330 W, PoE-Ports (8), maximale Last pro Port: 90 W
Stromverbrauch

Modell	Max. Stromverbrauch
PA-505	23 W
PA-510	34,3 W
PA-520 oder PA-540	30 W
PA-545-POE*	336 W (mit 181 W PoE-Ausgang)
PA-550	57 W
PA-555-POE*	503 W (mit 332 W PoE-Ausgang)
PA-560	106 W

* Mit einem oder mehreren mitgelieferten Netzteilen.

Tabelle 3: Hardwarespezifikationen der PA-500 Series (Fortsetzung)
Max. BTU/h
PA-505: 78 PA-510: 117 PA-520 oder PA-540: 102 PA-545-POE: 1.145 (mit 181 W PoE-Ausgang) PA-550: 195 PA-555-POE: 1.715 (mit 332 W PoE-Ausgang) PA-560: 361
Eingangsspannung (Eingangsfrequenz)
100-240 V AC (50-60 Hz)
Max. Stromverbrauch
PA-505: 2 A bei 12 V DC PA-510: 2,5 A bei 12 V DC PA-520 oder PA-540: 4 A bei 12 V DC PA-545-POE: 6 A bei 54 V DC PA-550: 5 A bei 12 V DC PA-555-POE: 9 A bei 54 VDC PA-560: 8 A bei 12 V DC
Abmessungen
PA-505: 43,9 mm H x 163 mm T x 242 mm B PA-510: 43,9 mm H x 224 mm T x 205 mm B PA-520 oder PA-540: 43,9 mm H x 265 mm T x 203 mm B PA-550 oder PA-560: 43,9 mm H x 37 mm T x 330 mm B PA-545-POE oder PA-555-POE: 43.9 mm H x 314 mm T x 409 mm B
Gewicht (Netto-/Versandgewicht)
PA-505: 1,4 kg/2,7 kg PA-510: 2,3 kg/3,5 kg PA-520 oder PA-540: 2,63 kg/3,62 kg PA-545-POE: 6,12 kg/8,98 kg PA-550: 5,08 kg/7,08 kg PA-555-POE: 6,12 kg/9,16 kg PA-560: 5,08 kg/7,08 kg
Sicherheitsstandards
cTUVus, CB
EMI
PA-505, PA-510: FCC-Klasse B, CE-Klasse B und VCCI-Klasse B PA-520, PA-540, PA-545-POE, PA-550, PA-555-POE, PA-560: FCC-Klasse A, CE-Klasse A und VCCI-Klasse A
Zertifizierungen
Siehe unsere Compliance-Seite.
Umgebungsbedingungen
Betriebstemperatur: 0 °C bis 40 °C Temperatur bei Nichtbetrieb: -20 °C bis 70 °C Passive Kühlung: PA-505, PA-510, PA-520, PA-540, PA-545-POE, PA-550 und PA-555-POE Aktive Kühlung: PA-560

Tabelle 4: Bestellinformationen zur PA-500 Series		
Zubehör	**Kurzbeschreibung**	**Modelle**
PAN-PWR-25W-AC	25 W Ersatznetzteil	PA-505
PAN-PWR-50W-AC*	50 W Ersatznetzteil*	PA-510
PAN-PWR-150W-12V-AC-A	150 W Ersatznetzteil	PA-520, PA-540, PA-550 und PA-560:
PAN-PWR-350W-54V-AC-A	350 W Ersatznetzteil	PA-545-POE
PAN-PWR-550W-54V-AC-A	550 W Ersatznetzteil	PA-555-POE
PAN-PA-400-RACKTRAY*	1HE 4-Pfosten-Rackmontage für: zwei PA-510s und vier Netzteile	PA-510
PAN-1RU-4POST-RACK-11	1HE 4-Pfosten-Rackmontage für: ein PA-560 und zwei Netzteile, ein PA-550 und zwei Netzteile, zwei PA-540s und vier Netzteile, zwei PA-520s und vier Netzteile.	PA-520, PA-540, PA-550 und PA-560:
PAN-1RU-4POST-RACK-12	1HE 4-Pfosten-Rackmontage für: ein PA-555-POE und zwei Netzteile, ein PA-545-POE und zwei Netzteile	PA-545-POE und PA-555-POE

* Muss separat angegeben werden.

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

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

www.paloaltonetworks.de

strata_ds_pa-500-series_090825