STRATA™
BY PALO ALTO NETWORKS

PA-5200 Series

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

PA-5260

Die ML-gestützten NGFWs der PA-5200 Series von Palo Alto Networks – die PA-5280, PA-5260, PA-5250 und PA-5220 – sind ideal für den Einsatz in Hochgeschwindigkeitsdatenzentren, Internetgateways und bei Serviceanbietern. Die PA-5200 Series stellt durch dedizierte Verarbeitung und Speicherung einen Durchsatz von bis zu 64 Gbit/s für die wesentlichen Funktionsbereiche Netzwerk, Sicherheit, Bedrohungsschutz und -management bereit.

Mit der ersten ML-gestützten NGFW können Sie bisher unbekannte Bedrohungen abwehren, profitieren von umfassenden Einblicken in und durchgehenden Schutz für ihre gesamte IT-Umgebung – inklusive Geräte im Internet der Dinge (IoT) – und vermeiden Bedienfehler mit automatisierten Richtlinienempfehlungen. Die PA-5200 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 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.

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 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.

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.

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.
- 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: PA-5200 Series – Leistung und Kapazitäten

	PA-5280	PA-5260	PA-5250	PA-5220
Firewalldurchsatz (HTTP/Appmix)*	58/65 Gbit/s	58/65 Gbit/s	38/37 Gbit/s	16/18 Gbit/s
Threat-Prevention-Durchsatz (HTTP/Appmix)†	29/36 Gbit/s	29/36 Gbit/s	19,5/24 Gbit/s	8,2/10 Gbit/s
IPsec-VPN-Durchsatz‡	28 Gbit/s	28 Gbit/s	19 Gbit/s	11 Gbit/s
Max. Anz. Sitzungen	65 Mio.	32 Mio.	8 Mio.	4 Mio.
Neue Sitzungen pro Sekunde§	600.000	600.000	382.000	180.000
Virtuelle Systeme (Basis/max.)||	25/225	25/225	25/125	10/20

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: PA-5200 Series – Netzwerkfunktionen

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

Tabelle 2: Netzwerkfunktionen der PA-5200 Series (Forts.)

Verschlüsselung: 3DES, AES (128-Bit, 192-Bit, 256-Bit)
Authentifizierung: MD5, SHA-1, SHA-256, SHA-384, SHA-512
Mit GlobalProtect geschütztes LSVPN (Large-scale-VPN) für einfachere Konfiguration und Verwaltung
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
GTP-Sicherheit
SCTP-Sicherheit

Tabelle 3: PA-5200 Series – Hardwarespezifikationen
E/A
PA-5280/PA-5260/PA-5250: 100/1000/10G-Cu (4), 1G/10G-SFP/SFP+ (16), 40G/100G-QSFP28 (4) PA-5220: 100/1000/10G-Cu (4), 1G/10G-SFP/SFP+ (16), 40G-QSFP+ (4)
Management – E/A
PA-5280/PA-5260/PA-5250: 10/100/1000 (2), 40G/100G-QSFP28-HA (1), 10/100/1000 Out-of-Band-Management (1), Konsolenport RJ45 (1) PA-5220: 10/100/1000 (2), 40G-QSFP+-HA (1), 10/100/1000 Out-of-Band-Management (1), Konsolenport RJ45 (1)
Speicherkapazität
240-GB-SSD, RAID1, Systemspeicher 2-TB-HDDs, RAID1, Logspeicher
Stromversorgung (Durchschn./max. Stromverbrauch)
571/685 W
Max. BTU/h
2.340
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
AC: 8,5 A bei 100 V AC; 3,6 A bei 240 V AC DC: 19 A bei -40 V DC; 12,7 A bei -60 V DC

Tabelle 3: Hardwarespezifikationen der PA-5200 Series (Forts.)
Max. Einschaltstrom
AC: 50 A bei 230 V AC; 50 A bei 120 V AC DC: 200 A bei 72 V DC
DC: 200 A bei 72 V DC
9,23 Jahre
Platzbedarf im Rack (Abmessungen)
3U, 19-Zoll-Standardrack H: 13,34 cm x T: 52,07 cm x B: 43,82 cm
Gewicht (Netto-/Versandgewicht)
21/28 kg
Sicherheitsstandards
cTUVus, CB
EMI
FCC-Klasse A, CE-Klasse A, VCCI-Klasse A
Zertifizierungen
Siehe paloaltonetworks.com/company/certifications.html
Umgebungsbedingungen
Betriebstemperatur: 0 ° bis 50 °C Temperatur bei Nichtbetrieb: -20 °C bis 70 °C

Um mehr über die Funktionen und die damit verbundenen Kapazitäten der PA-5200 Series zu erfahren, besuchen Sie paloaltonetworks.com/network-security/next-generation-firewall/pa-5200-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