PA-460

PA-450

PA-440

PA-445

PA-410

PA-415

PA-400 Series

Die PA-400 Series von Palo Alto Networks, die die Next-Generation Firewalls PA-410, PA-415, PA-440, PA-445, PA-450 und PA-460 umfasst, bietet ML-gestützte Funktionen einer NGFW für verteilte Unternehmensniederlassungen, Einzelhandelsstandorte und mittelgroße Unternehmen.

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.

Highlights

- Weltweit erste ML-gestützte NGFW
- Elfmaliger Leader im Gartner Magic Quadrant für Netzwerkfirewalls
- Leader im Bericht „The Forrester Wave: Enterprise Firewalls“, Q4 2022
- Breite Palette von Produkten für eine Vielzahl von Leistungsanforderungen für Unternehmen mit zahlreichen Standorten
- Bietet Sicherheit in einem Desktopform-faktor
- Unterstützt Hochverfügbarkeit mit Aktiv/Aktiv- und Aktiv/Passiv-Modus
- Bietet vorhersehbare Leistung mit Sicherheitsservices
- Geräuscharmes, lüfterloses Design mit optionaler redundanter Stromversorgung für Niederlassungen und Homeoffice
- Vereinfacht die Bereitstellung einer großen Anzahl von Firewalls mit optionalem Zero Touch Provisioning (ZTP)
- Unterstützt die zentralisierte Verwaltung mit Panorama-Netzwerksicherheits-management
- Nutzt AIOps zur vollen Ausnutzung von Sicherheitsinvestitionen und zur Vermeidung von Geschäftsunterbrechungen

Die PA-400 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 verkürzt die zur effektiven Reaktion auf Sicherheitsvorfälle erforderliche Zeit.

Wichtige Sicherheits- und Konnektivitätsfunktionen

ML-gestützte Next-Generation Firewall

- 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.
- Nutzt cloudbasierte ML-Prozesse, um Signaturen und Anweisungen verzögerungsfrei zurück an die NGFW zu senden.
- Nutzt Verhaltensanalysen, um IoT-Geräte zu erkennen und Richtlinienempfehlungen abzugeben – als Teil eines in der Cloud bereitgestellten und nativ integrierten Services 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 der SaaS Security Subscription, um die stetig steigende Anzahl der SaaS-Apps im Griff zu behalten.
- Ermöglicht die Definition und Durchsetzung von Sicherheitsrichtlinien (durch das Gestatten, Verbieten, Planen, Analysieren oder Steuern von Datenverkehr) für spezifische Anwendungen (anstelle von Ports).
- 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 einer Anwendung (wie Dateien und Datenmuster), um bösartige Dateien zu blockieren und Ausschleusungen 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 aufgrund 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- 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.
- Implementiert Sicherheitsmaßnahmen dynamisch auf der Grundlage des Benutzerverhaltens, 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 von 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. Mit PA-410, PA-415, PA-440, PA-445, PA-450 und PA-460 können Sitzungsprotokolle in Panorama und Cortex Data Lake exportiert werden. PA-415, PA-440, PA-445, PA-450 und PA-460 unterstützen außerdem die Protokollierung von Sitzungen in der Box.
- 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 werden praxistaugliche Einblicke zur Behebung dieser Probleme bereitgestellt.

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. Gleichzeitig verursachen herkömmliche Punktlösungen Sicherheitslücken in Unternehmen, erhöhen den Arbeitsaufwand von Sicherheitsteams und beeinträchtigen die Produktivität durch inkonsistenten Zugriff und unzureichende Transparenz.

Unsere Cloud-Delivered Security Services (CDSS) 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 über jeden Bedrohungsvektor 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.

- **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 sogar gut getarnte Malware automatisch und bis zu 60-mal schneller erkennt und 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 blockiert 85 % der Malware, die DNS als Command-and-Control-Kanal und für den Datendiebstahl nutzt. Dazu sind keine Infrastrukturänderungen erforderlich.
- **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 einzigartigen 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.

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.

Einzigartiger Ansatz für die Paketverarbeitung mit Single-Pass-Architektur

- Führt Netzwerkfunktionen, Richtliniensuche und -anwendung, 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.)

Tabelle 1: Leistung und Kapazitäten der PA-400 Series

	PA-410	PA-415	PA-440	PA-445	PA-450	PA-460
Firewalldurchsatz (HTTP/Appmix)*	1,59/1,1	1,65/1,2 Gbit/s	2,8/2,2 Gbit/s	2,8/2,2 Gbit/s	3,5/2,9 Gbit/s	5,1/4,4 Gbit/s
Threat-Prevention-Durchsatz (HTTP/Appmix)†	0,6/0,68 Gbit/s	0,6/0,69 Gbit/s	1,0/1,0 Gbit/s	1,0/1,0 Gbit/s	1,4/1,6 Gbit/s	2,1/2,4 Gbit/s
IPsec-VPN-Durchsatz‡	0,92 Gbit/s	0,92 Gbit/s	1,6 Gbit/s	1,6 Gbit/s	2,2 Gbit/s	3,0 Gbit/s
Max. Anz. Sitzungen	64.000	64.000	200.000	200.000	300.000	400.000
Neue Sitzungen pro Sekunde§	12.000	12.000	37.500	37.500	51.000	73.000
Virtuelle Systeme (Basis/max.)‖	1/1	1/1	1/2	1/2	1/5	1/5

Hinweis: Ergebnisse wurden auf PAN-OS 11.0 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, 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. Zudem ist PAN-OS 11.0 oder höher erforderlich.

Tabelle 2: Netzwerkfunktionen der PA-400 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

Tabelle 2: Netzwerkfunktionen der PA-400 Series (Fortsetzung)
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

Tabelle 3: Hardwarespezifikationen der PA-400 Series
E/A
PA-410: RJ45 (7) PA-440, PA-450, PA-460: RJ45 (8) PA-415, PA-445: 1G-SFP/RJ45 Combo (1), RJ45 (4), RJ45/PoE (4)
Management E/A
PA-410: 10/100/1.000 Out-of-Band-Managementport (1), RJ45-Konsolenport (1), USB-Port (2) PA-415, PA-445-SFP/RJ45(1 GB) Combo-Managementport (1), RJ45-Konsolenport (1), USB-Port (2), Micro-USB-Konsolenport (1) PA-440, PA-450, PA-460: 10/100/1.000 Out-of-Band-Managementport (1), RJ45-Konsolenport (1), USB-Port (2), Micro-USB-Konsolenport (1)
Power Over Ethernet (PoE)
PA-415, PA-445 PoE-RJ45-Ports (4) PoE-Leistungskapazität insgesamt: 91 W Max. Last pro Port: 60 W
Speicherkapazität
PA-410: 64 GB eMMC PA-415, PA-440, PA-445, PA-450, PA-460: 128 GB eMMC
Stromversorgung (durchschn./max. Stromverbrauch)
PA-415, PA-445: 150 W PA-415, PA-440, PA-445: 29/34 W PA-450, PA-460: 33/41 W
Max. BTU/h
PA-410: 78 PA-415, PA-440, PA-445: 117 PA-450, PA-460: 141
Eingangsspannung (Eingangsfrequenz)
100–240 V AC (50–60 Hz)
Max. Stromverbrauch
PA-410: 1,5 A bei 12 V DC PA-415, PA-440, PA-445: 2,9 A bei 12 V DC PA-450, PA-460: 3,4 A bei 12 V DC
Max. Einschaltstrom
PA-410: 2,1 A PA-415, PA-440, PA-445: 3,3 A PA-450, PA-460: 4,2 A
Abmessungen
PA-410: H: 4,14 cm × T: 16,31 cm × B: 24,21 cm PA-415: H: 4,4 cm × T: 33 cm × B: 22,87 cm PA-445: H: 4,22 cm × T: 33 cm × B: 22,53 cm PA-440, PA-450, PA-460: H: 4,42 cm × T: 22,43 cm × B: 20,50 cm

Tabelle 3: Hardwarespezifikationen der PA-400 Series (Fortsetzung)
Gewicht (Netto-/Versandgewicht)
PA-410: 1,4 kg/2,7 kg PA-415: 3,56 kg/5,53 kg PA-445: 3,95 kg/5,72 kg PA-440, PA-450, PA-460: 2,3 kg/3,5 kg
Sicherheitsstandards
cTUVus, CB
EMI
FCC-Klasse B, CE-Klasse B, VCCI-Klasse B
Zertifizierungen
Siehe paloaltonetworks.com/company/certifications.html
Umgebungsbedingungen
Betriebstemperatur: 0 °C bis 40 °C Temperatur bei Nichtbetrieb: -20 °C bis 70 °C Passive Kühlung

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