



PA-1410



PA-1420

PA-1400 Series

Die ML-gestützten NGFWs der PA-1400 Series von Palo Alto Networks mit den Modellen PA-1420 und PA-1410 wurden zum Schutz von Filialen und mittelständischen Unternehmen entwickelt.

Die PA-1400 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.

Highlights

- Weltweit erste ML-gestützte NGFW
- Elfmaliger Leader im Gartner Magic Quadrant für Netzwerkfirewalls
- Leader im Bericht „The Forrester Wave: Enterprise Firewalls“, Q4 2022
- Bietet vorhersehbare Leistung mit Sicherheitsdiensten
- Vereinfacht die Bereitstellung einer großen Anzahl von Firewalls mit optionalem Zero Touch Provisioning (ZTP)
- Native Unterstützung für Webproxys in der NGFW vereinfacht und konsolidiert das Management von Firewall- und Proxyfunktionen
- Unterstützt die zentralisierte Verwaltung mit Panorama-Netzwerksicherheitsmanagement
- 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
- Nutzt AIOps zur vollen Ausnutzung von Sicherheitsinvestitionen und zur Vermeidung von Geschäftsunterbrechungen

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 verzögerungsfrei Signaturen und Anweisungen zurück an die NGFW zu senden.
- Nutzt Verhaltensanalysen, um Geräte im Internet der Dinge (Internet of Things, IoT) zu erkennen und Richtlinienempfehlungen zu geben; ist ein 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 oder Verschlüsselung (TLS/SSL).
- Erkennt und verwaltet neue Anwendungen im Rahmen der SaaS Security Subscription automatisch, um die stetig steigende Anzahl der SaaS-Anwendungen 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 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 [App-ID-Lösungsbeschreibung](#).

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 Repositories 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.
- 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 Drittanbieter-Tools 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-Netzwerk-sicherheitsmanagement 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

- Bietet kontinuierliche, an den Kunden angepasste Best-Practice-Empfehlungen, damit Sie Ihren Sicherheitsstatus stärken und Ihre Sicherheitsinvestitionen voll ausschöpfen können.
- Nutzt ML-Funktionen und aussagekräftige Telemetriedaten, um intelligente Prognosen zu Status, Leistung und Kapazität der Firewalls sowie zu potenziellen Problemen zu bieten.
- Stellt praxistaugliche Einblicke zur Behebung dieser Probleme bereit.

Native Unterstützung für Webproxys durch die Next-Generation Firewall

- Ermöglicht die Konsolidierung von Firewall und Proxy in einer Plattform sowie das Management von Firewall- und Proxyfunktionen und -richtlinien über eine zentralisierte Plattform
- Unterstützt explizite Proxys mithilfe von PAC-Dateien und auch transparente Proxys
- Unterstützt Architekturen ohne Standardpfade und mit On-Premises-Proxybereitstellung für explizite Proxys. Explizite Proxys unterstützen die Authentifizierung mit Kerberos und SAML.
- Vereinfacht die Einrichtung transparenter Proxys, da weder WCCP noch Authentifizierung erforderlich sind.

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 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. 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 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 DNS-Angriffe und vereitelt 80 % der Angriffe, bei denen die Angreifer DNS als Command-and-Control-Kanal und für den Datendiebstahl nutzen. 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 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.

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.
- 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.

Tabelle 1: Leistung und Kapazitäten der PA-1400 Series

	PA-1410	PA-1420
Firewalldurchsatz (HTTP/Appmix)*	8,9/6,8 Gbit/s	9,9/9,5 Gbit/s
Threat-Prevention-Durchsatz (HTTP/Appmix)†	3,3/3,2 Gbit/s	5,0/4,8 Gbit/s
IPsec-VPN-Durchsatz‡	4,6 Gbit/s	6,5 Gbit/s
Max. Anz. Sitzungen	945.000	1.400.000
Neue Sitzungen pro Sekunde§	100.000	140.000
Virtuelle Systeme (Basis/max.)	1/6	1/6

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.

Die ML-gestützten NGFWs der PA-1400 Series unterstützen eine Vielzahl von Netzwerkfunktionen, mit denen Sie unsere Sicherheitsfunktionen noch einfacher in Ihr bestehendes Netzwerk integrieren können.

Tabelle 2: Netzwerkfunktionen der PA-1400 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)
Pfad dynamisch ändern

Tabelle 2: Netzwerkfunktionen der PA-1400 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
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
Fehlererkennung: Pfadüberwachung, Schnittstellenüberwachung
Zero Touch Provisioning (ZTP)
Erfordert Panorama 9.1.3 oder höher zur Verwaltung von NGFW der PA-1400 Series mit PAN-OS 11.0 oder höher

Tabelle 3: Hardwarespezifikationen der PA-1400 Series

E/A
PA-1410 10/100/1000 (8), 1G/2,5G/5G-/PoE (4), 1G-SFP (6), 1G/10G-SFP/SFP+ (4)
PA-1420 10/100/1000 (4), 1G/2,5G/5G (4), 1G/2,5G/5G-/PoE (4), 1G-SFP (2), 1G/10G-SFP/SFP+ (8)
Management E/A
10/100/1000 Out-of-Band-Managementport (1)
HSCI 10 Gigabit Hochverfügbarkeit (1)
Konsolenport RJ-45 (1)
USB-Port (1)
Micro-USB-Konsolenport (1)
Power Over Ethernet (PoE)
PoE-Leistungskapazität für PA-1410/PA-1420 insgesamt: 151 W, Max. Last pro Port: 90 W
Speicherkapazität
PA-1410: 120-GB-SSD
PA-1420: 240-GB-SSD
Stromversorgung (durchschn./max. Stromverbrauch)
450-W-Wechselstrom-Netzteil (1); ein zweites 450-W-Wechselstrom-Netzteil kann dazugekauft werden
Stromversorgung (durchschn./max. Stromverbrauch)*
PA-1410: 250 W/290 W
PA-1420: 260 W/300 W

* Stromverbrauch schließt 150 W PoE-Last ein

Tabelle 3: Hardwarespezifikationen der PA-1400 Series (Fortsetzung)	
Mittlere Betriebsdauer zwischen Ausfällen (MTBF)	
24 Jahre	
Eingangsspannung (Eingangsfrequenz)	
100–240 V AC (50–60 Hz)	
Platzbedarf im Rack (Abmessungen)	
PA-1410, PA-1420: 1U, 19-Zoll-Standardrack (H: 4,32 cm x T: 35,95 cm x B: 43,56 cm)	
Gewicht (Netto-/Versandgewicht)	
PA-1410, PA-1420: 7,0 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 40 °C auf 3.000 m	
Lagertemperatur: -20 °C bis 70 °C	
Luftstrom	
Von vorne nach hinten	