STRATA™
BY PALO ALTO NETWORKS

PA-220

Palo Alto Networks PA-220 ist eine auf maschinelles Lernen gestützte Next-Generation Firewall für Zweigniederlassungen, Einzelhandelsfilialen und mittelständische Unternehmen.

Highlights

- High Availability (hohe Verfügbarkeit, HA) durch Aktiv/Aktiv- und Aktiv/Passiv-Modi
- Redundante Stromversorgung, um die Zuverlässigkeit zu erhöhen
- Ohne Lüfter
- Vereinfachte Bereitstellung zahlreicher Firewalls über USB

PA-220

Die Steuerung der PA-220 erfolgt über das Betriebssystem PAN-OS®, das jeglichen Datenverkehr, einschließlich Anwendungen, Bedrohungen und Inhalte, nativ klassifiziert und den Datenverkehr unabhängig von Standort und Gerätetyp einem Benutzer zuordnet. Anwendungen, Inhalte und Benutzer – die grundlegenden Faktoren Ihrer Geschäftsprozesse – werden somit als Basis für Ihre Sicherheitsrichtlinien herangezogen. Dies erhöht die Sicherheit und verkürzt die Reaktionszeit bei Störfällen.

Die wichtigsten Sicherheits- und Konnektivitätsfunktionen

Permanente Klassifizierung aller Anwendungen auf allen Ports

- Identifiziert die Anwendung unabhängig vom Port, von der Verschlüsselung (SSL oder SSH) oder der eingesetzten Umgehungsmethode.
- Nutzt die Anwendung anstelle des Ports als Grundlage für alle Sicherheitsentscheidungen wie das Zulassen, Ablehnen, Terminieren, Untersuchen und das Anwenden von Traffic-Shaping.
- Kategorisiert nicht identifizierte Anwendungen und unterstützt so Richtlinienkontrolle, die forensische Untersuchung von Bedrohungen sowie App-ID™-Entwicklung.
- Bietet einen vollständigen Einblick in die Details aller TLS-verschlüsselten Verbindungen und stoppt Bedrohungen, die in verschlüsseltem Datenverkehr versteckt sind, einschließlich Datenverkehr, der die Protokolle TLS 1.3 und HTTP/2 verwendet.

Umsetzung von Sicherheitsrichtlinien für alle Benutzer, unabhängig von ihrem Standort

- Bereitstellung konsistenter Richtlinien für lokale und Remotebenutzer auf Windows®-, macOS®-, Linux-, Android®- oder Apple iOS-Plattformen.
- Ermöglicht agentenlose Integration mit Microsoft Active Directory® sowie Terminal Services, LDAP, Novell eDirectory™ und Citrix.
- Ermöglicht die einfache Integration Ihrer Firewallrichtlinien mit 802.1X-Wireless-Systemen, Proxys, NAC-Lösungen und sonstigen Einrichtungen zur Benutzerauthentifizierung.

Erweitert mit cloudbasierten Sicherheitsabonnements den nativen Schutz auf alle Angriffsvektoren.

- **Threat Prevention** — untersucht den gesamten Datenverkehr, um bekannte Schwachstellen, Malware, ausgenutzte Sicherheitslücken, Spyware, Command-and-Control (C2) und benutzerdefinierte Intrusion Prevention System-(IPS-) Signaturen automatisch zu blockieren.
- **WildFire®** Malwareschutz — schützt vor unbekannten dateibasierten Bedrohungen und sorgt in Sekundenschnelle für automatische Abwehr der meisten neuen Bedrohungen in Netzwerken, an Endpunkten und in Clouds.
- **URL Filtering** — verhindert den Zugriff auf bösartige Websites und schützt Benutzer vor webbasierten Bedrohungen.
- **DNS-Sicherheit** — erkennt und blockiert bekannte und unbekannte DNS nutzende Bedrohungen, während die prädiktive Analyse Angriffe vereitelt, die DNS für C2 oder Datendiebstahl nutzen.
- **IoT-Sicherheit** — erkennt alle nicht verwalteten Geräte in Ihrem Netzwerk, identifiziert Risiken und Schwachstellen und automatisiert die Durchsetzung von Richtlinien für Ihre auf maschinelles Lernen gestützte NGFW mithilfe eines neuen Device-IDTM-Richtlinienkonstrukts.

Ermöglicht SD-WAN-Funktion

- Ermöglicht die einfache SD-WAN-Integration durch problemlose Aktivierung in Ihren bestehenden Firewalls.
- Ermöglicht das sichere Implementieren von SD-WAN, das nativ in unser branchenführendes Sicherheitssystem integriert ist.
- Bietet dank Minimierung von Latenz, Jitter und Paketverlust ein einzigartiges Endnutzererlebnis.

Tabelle 1: Leistung und Kapazitäten der PA-220[1]

Firewalldurchsatz (HTTP/Appmix)[2]	575/540 Mbit/s
Threat Prevention-Durchsatz (HTTP/Appmix)[3]	275/320 Mbit/s
IPsec-VPN-Durchsatz[4]	540 Mbit/s
Max. Anzahl an Sitzungen	64.000
Neue Sitzungen pro Sekunde[5]	4.300

1. Die Ergebnisse wurden mit PAN-OS 10.0 ermittelt.
2. Die Messung des Firewalldurchsatzes erfolgte mit aktivierter App-ID und Protokollierung bei 64-KB-HTTP/Appmix-Transaktionen.
3. Die Messung des Threat Prevention-Durchsatzes erfolgte mit aktivierten Systemen für App-ID, IPS, Antivirensoftware, Anti-Spyware, WildFire, Datei-Blockade und Protokollierung bei 64-KB-HTTP/Appmix-Transaktionen.
4. Die Messung des IPsec-VPN-Durchsatzes erfolgte mit aktivierter Protokollierung bei 64-KB HTTP-Transaktionen.
5. Die Messung der neuen Sitzungen pro Sekunde erfolgte mit Application Override bei 1 Byte HTTP-Transaktionen.

Die PA-220 unterstützt eine Vielzahl von Netzwerkfunktionen, mit denen Sie unsere Sicherheitsfunktionen noch einfacher in Ihr bestehendes Netzwerk integrieren können.

Tabelle 2: Netzwerkfunktionen der PA-220

Schnittstellenmodi
L2, L3, TAP, Virtual Wire (Transparent-Modus)
Routing
OSPFv2/v3 mit Graceful Restart, BGP mit Graceful Restart, RIP, statisches Routing
Policy-Based Forwarding (PBF)
Point-To-Point Protocol over Ethernet (PPPoE)
Multicast: PIM-SM, PIM-SSM, IGMP v1, v2 und v3
SD-WAN
Messung der Pfadqualität (Jitter, Paketverlust, Latenz)
Auswahl des ersten Pfads (PBF)
Dynamischer Pfadwechsel
IPv6
L2, L3, TAP, Virtual Wire (Transparent-Modus)
Funktionen: App-ID, User-ID, Content-ID, WildFire und SSL-Entschlüsselung
SLAAC
IPSec VPN
Schlüsselaustausch: manueller Schlüssel, IKEv1 und IKEv2 (vorinstallierter Schlüssel [PSK], zertifizierungsbasierte Authentifizierung)
Verschlüsselung: 3DES, AES (128 Bit, 192 Bit, 256 Bit)
Authentifizierung: MD5, SHA-1, SHA-256, SHA-384, SHA-512

Tabelle 2: Netzwerkfunktionen der PA-220 (Fortsetzung)
VLANs
802.1Q VLAN-Tags pro Gerät/pro Schnittstelle: 4.094/4.094
Network Address Translation (Netzwerkadressenübersetzung, NAT)
NAT-Modi (IPv4): statische IP-Adresse, dynamische IP-Adresse, dynamische IP-Adresse und Port (Portadressenübersetzung))
NAT64, NPTv6
Zusätzliche NAT-Funktionen: dynamische IP-Reservierung, anpassbare Überbelegung dynamischer IP-Adressen und Ports
High Availability (hohe Verfügbarkeit, HA)
Modi: aktiv/aktiv, aktiv/passiv
Fehlererkennung: Pfadüberwachung, Schnittstellenüberwachung
Automatisierte Bereitstellung (Zero Touch Provisioning, ZTP)
Verfügbar mit -ZTP-Artikelnummern (PA-220-ZTP)
Erfordert Panorama 9.1.3 oder höher

Tabelle 3: Hardwarespezifikationen der PA-220
I/O
10/100/1000 (8)
Management-I/O
10/100/1000 Out-of-Band-Management-Port (1), Konsolen-Port RJ-45 (1) USB-Port (1) Micro-USB-Konsolenport (1)
Speicherkapazität
32 GB eMMC
Stromversorgung (durchschn./max. Stromverbrauch)
Optional: 2 x 40 W redundant (21 W/25 W)

Tabelle 3: Hardwarespezifikationen der PA-220 (Fortsetzung)
Max. BTU/h
102
Eingangsspannung (Eingangsfrequenz)
100–240 V AC (50–60 Hz)
Max. Stromverbrauch
Firewall: 1,75 A bei 12-V-DC-Stromversorgung (AC-Seite): 1,5 A
Abmessungen
4,11 cm H x 15,98 cm T x 20,50 cm B
Gewicht (nur Gerät/wie geliefert)
1,36 kg/2,45 kg
Sicherheit
cTUVus, CB
EMI
FCC-Klasse B, CE-Klasse B, VCCI-Klasse B
Zertifizierungen
Siehe paloaltonetworks.com/company/certifications.html
Umgebung
Betriebstemperatur: 0 bis 40 °C Temperatur bei Nichtbetrieb -20 bis 70 °C Passive Kühlung

Weitere Informationen zu den Funktionen und den entsprechenden Leistungsmerkmalen der PA-220 finden Sie unter paloaltonetworks.com/network-security/next-generation-firewall/PA-220.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Zentrale: +1 408 75 34 000
Vertrieb: +1 866 32 04 788
Support: +1 866 898 9087

www.paloaltonetworks.com