STRATA™
BY PALO ALTO NETWORKS

PA-220R

Palo Alto Networks PA-220R ist als robuste ML-gestützte Next-Generation Firewall für den industriellen Einsatz in anspruchsvollen Umgebungen ausgelegt.

Highlights

- Erweiterter Betriebstemperaturbereich
- Zertifiziert nach IEC 61850-3 und IEEE 1613, den Standards für Umweltverhalten und Testanforderungen für Vibration, Temperatur und Störsicherheit gegen elektromagnetische Einflüsse.
- Doppelte Gleichstromversorgung (12–48 V)
- High-Availability-Firewall-Konfiguration (aktiv/aktiv und aktiv/passiv)
- Ohne Lüfter und ohne bewegliche Teile
- Flexibler E/A für sowohl Kupfer- als auch Glasfaseranschluss über SFP-Ports
- Flexible Montageoptionen, einschließlich DIN-Schiene, Rack und Wandmontage
- Einfacher Einsatz am Remotestandort über USB-basiertes Bootstrapping

PA-220R

Die robuste PA-220R schützt Industrie- und Verteidigungsnetzwerke in diversen anspruchsvollen Umgebungen. Hierzu zählen Umspannwerke, Kraftwerke, Fertigungsanlagen, Öl- und Gasanlagen, Gebäudemanagementsysteme und Netzwerke im Gesundheitswesen.

Die PA-220R wird über PAN-OS® gesteuert, das den gesamten Datenverkehr, einschließlich Anwendungen, Bedrohungen und Inhalten, nativ klassifiziert und dann diesen Datenverkehr unabhängig von Standort oder Gerätetyp dem jeweiligen Benutzer zuordnet. Die Anwendung, der Inhalt und der Benutzer – d. h. die für Ihre Betriebsabläufe wesentlichen Ressourcen – werden anschließend als Basis für Ihre Sicherheitsleitlinien genutzt, um den Sicherheitsstatus zu erhöhen und die Reaktionszeiten bei Zwischenfällen zu reduzieren.

Wichtige Sicherheits- und Konnektivitätsfunktionen

Permanente Klassifizierung aller Anwendungen auf allen Ports

- Verwendet App-IDs für Industrieprotokolle und -anwendungen, wie z. B. Modbus, DNP3, IEC 60870-5-104, Siemens S7 und OSIsoft PI®
- Identifizierung der Anwendung unabhängig vom Port, von der Verschlüsselung (SSL oder SSH) oder der eingesetzten Umgehungsmethode
- Nutzung der Anwendung anstelle des Ports als Grundlage für alle Ihre Entscheidungen bezüglich Sicherheitsleitlinien, wie beispielsweise Zulassen, Ablehnen, Terminieren, Untersuchen und das Anwenden von Traffic-Shaping.
- Kategorisierung nicht identifizierter Anwendungen zur Richtlinienkontrolle, für forensische Untersuchungen oder App-ID™-Entwicklungen.
- Vollständige Einsicht in die Details aller TLS-verschlüsselten Verbindungen und Abwehr von Bedrohungen, die in verschlüsseltem Datenverkehr versteckt sind, auch in Datenverkehr, der die Protokolle TLS 1.3 und HTTP/2 verwendet.

Umsetzung von Sicherheitsrichtlinien für alle Benutzer unabhängig von ihrem Standort

- Stellt konsistente Richtlinien für lokale und Remotebenutzer auf Windows®-, macOS®-, Linux-, Android®- oder Apple iOS-Plattformen bereit.
- Integration ohne Agent in Microsoft Active Directory® und 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 den nativen Schutz auf alle Angriffsvektoren mit cloudbasierten Securityabonnements

- **Threat Prevention** – überprüft den gesamten Datenverkehr, um bekannte Schwachstellen, Malware, Schwachstellen-Exploits, Spyware, Command-and-Control (C2) und benutzerdefinierte Intrusion Prevention System-(IPS-)Signaturen automatisch zu blockieren.
- **WildFire®-Malwareprävention** – schützt vor unbekannten dateibasierten Bedrohungen und bietet in Sekundenschnelle eine automatische Abwehr der meisten neuen Bedrohungen über Netzwerke, Endpunkte und Clouds hinweg.
- **URL-Filterung** – verhindert den Zugriff auf schädliche Websites und schützt Benutzer vor webbasierten Bedrohungen.
- **DNS Security** – erkennt und blockiert bekannte und unbekannte Bedrohungen über DNS, während die prädiktive Analyse Angriffe unterbindet, die DNS für C2 oder Datendiebstahl verwenden.
- **IoT Security** – entdeckt alle nicht verwalteten Geräte in Ihrem Netzwerk, identifiziert Risiken und Schwachstellen und automatisiert die Durchsetzung von Richtlinien für Ihre Next-Generation Firewall mithilfe des neuen Richtlinienkonstrukts Device-ID™.

Ermöglicht SD-WAN-Funktionalität

- Ermöglicht Ihnen die Übernahme von SD-WAN, indem Sie es ganz einfach auf Ihren vorhandenen Firewalls aktivieren.
- Erlaubt 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-220R[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. Sitzungen	64.000
Neue Sitzungen pro Sekunde[5]	4.300

1. Ergebnisse wurden auf PAN-OS 10.0 gemessen.
2. Firewalldurchsatz gemessen mit aktivierter App-ID und Protokollierung bei 64-KB-HTTP/Appmix-Transaktionen.
3. Threat Prevention-Durchsatz gemessen mit aktivierter App-ID, IPS, Antivirus, Antispyware, WildFire, Dateiblockade und Protokollierung unter Verwendung von 64-KB-HTTP/Appmix-Transaktionen.
4. IPsec-VPN-Durchsatz gemessen mit 64-KB-HTTP-Transaktionen und Protokollierung.
5. Neue Sitzungen pro Sekunde gemessen mit Überschreibung der App-ID unter Verwendung von 1-Byte-HTTP-Transaktionen.

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

Tabelle 2: Netzwerkfunktionen der PA-220R

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)
Multicase: PIM-SM, PIM-SSM, IGMP v1, v2 und v3
SD-WAN
Messung der Pfadqualität (Jitter, Paketverlust, Latenz)
Auswahl des Anfangspfads (PBF)
Dynamische Pfadänderung
IPv6
L2, L3, TAP, Virtual Wire (Transparent-Modus)
Funktionen: App-ID, User-ID, Content-ID, WildFire und SSL-Entschlüsselung
SLAAC

Tabelle 2: Netzwerkfunktionen der PA-220R (Forts.)
IPSec VPN
Schlüsselaustausch: manueller Schlüssel, IKEv1 und IKEv2 (Pre-shared Key, zertifikatbasierte 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
Network Address Translation
NAT-Modi (IPv4): statische IP, dynamische IP, dynamische IP und Port (Port Address Translation)
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
Industrieprotokolle und -anwendungen
paloaltonetworks.com/resources/whitepapers/app-ids-industrial-control-systems-scada-networks
Zero Touch Provisioning (ZTP)
Erhältlich mit -ZTP SKUs (PA-220R-ZTP)
Erfordert Panorama 9.1.3 oder höher

Tabelle 3: Hardwarespezifikationen der PA-220R
I/O
10/100/1000 (6), SFP (2)
Management-E/A
10/100/1000 Out-of-Band-Managementport (1) Konsolenport RJ-45 (1) USB-Port (1) Micro-USB-Konsolenport (1)
Speicherkapazität
32 GB EMMC

Tabelle 3: Hardwarespezifikationen der PA-220R (Forts.)
Stromversorgung (Durchschn./max. Stromverbrauch)
Optional: zwei redundante Gleichstromversorgungen (13 W/16 W)
Max. BTU/h
55
Eingangsspannung (Eingangsfrequenz)
12–48 V DC 1,4 A
Max. Stromverbrauch
Firewall – 1,4 A bei 12 V DC Max. Einschaltstrom 4,9 A bei 12 V DC
Abmessungen
5,08 cm H x 22,00 cm T x 23,50 cm B Flexible Montageoptionen, einschließlich DIN-Schiene, Rack und Wandmontage
Gewicht (Stand-alone-Gerät/wie geliefert)
2 kg/2,72 kg
Sicherheit
cTUVus, CB
EMV
FCC-Klasse A, CE-Klasse A, VCCI-Klasse A
Zertifizierungen
Umwelt- und Teststandards IEC 61850-3 und IEEE 1613 Weitere Zertifizierungen finden Sie unter paloaltonetworks.com/company/certifications.html.
Umgebung
Betriebstemperatur: -40 bis 70 °C (-40 bis 158 °F) Temperatur bei Nichtbetrieb: -40 bis 75 °C (-40 bis 167 °F) Passive Kühlung

Um mehr über die Funktionen und die damit verbundenen Kapazitäten der PA-220R zu erfahren, besuchen Sie paloaltonetworks.com/network-security/next-generation-firewall/pa-220r.

paloalto NETWORKS

Oval Tower, De Entrée 99–197
Santa Clara, CA 95054

Zentrale: +1 408 75 34 000
Vertrieb: +1 866 32 04 788
Support: +1 866 89 89 087

www.paloaltonetworks.de