

PA-7000 Series

Die Palo Alto Networks PA-7000 Series der auf maschinelles Lernen gestützten Next-Generation Firewalls ermöglicht es Unternehmen und Serviceprovidern, hochleistungsfähige Umgebungen wie große Rechenzentren und Netzwerkperimeter mit hoher Bandbreite zu schützen. Die Systeme wurden entwickelt, um den steigenden Durchsatzbedarf anwendungs-, benutzer- und gerätegenerierter Daten abzudecken. Sie bieten eine hohe Performance, Schutzfunktionen gegen ausgeklügelte Cyberangriffe sowie Entschlüsselungsfunktionen mit hohem Durchsatz zum Aufhalten von verschlüsselten Bedrohungen. Die PA-7000 Series wurde konzipiert, um die Nutzung der Ressourcen für Sicherheitsprozesse zu maximieren und automatisch zu skalieren, sobald neue Rechenleistung verfügbar ist. Das einheitliche System für Verwaltung und Lizenzierung bietet eine einfache Handhabung.

Die wichtigsten Sicherheitsfunktionen

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 Ihre Sicherheitsentscheidungen.
- 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 Windows®, macOS®, Linux-, Android®- und 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

- **Abwehr von Bedrohungen** — 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 unbekanntem 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 unbekanntes 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-ID™-Richtlinienkonstrukts.



PA-7050



PA-7080

Architektur der PA-7000 Series

Technische Basis der PA-7000 Series ist eine skalierbare Architektur, die dazu dient, Art und Menge der Rechenleistung den wichtigsten funktionellen Aufgaben, nämlich Netzwerkbetrieb, -sicherheit und -management, zuzuordnen. Das Chassis der PA-7000 Series verteilt die Verarbeitungsanforderungen intelligent auf drei Subsysteme, von denen jedes über hohe Mengen an Rechenleistung und dediziertem Speicher verfügt.

Tabelle 1: Leistung und Kapazitäten der PA-7000 Series¹

	PA-7080 ²	PA-7050 ²	PA-7000 DPC-A	PA-7000 NPC-100G	PA-7000 NPC-XM
Firewalldurchsatz (HTTP/Appmix) ³	644/700 Gbit/s	390/416 Gbit/s	77/86 Gbit/s	59/66 Gbit/s	17,6/20,0 Gbit/s
Threat Prevention-Durchsatz (DSRI aktiviert) ⁴	650 Gbit/s	396 Gbit/s	71,2 Gbit/s	55,7 Gbit/s	16,7 Gbit/s
Threat Prevention-Durchsatz (HTTP/Appmix) ⁵	362/430 Gbit/s	210/258 Gbit/s	41/49 Gbit/s	29/37 Gbit/s	9,3/12,5 Gbit/s
IPsec-VPN-Durchsatz ⁶	328 Gbit/s	200 Gbit/s	36 Gbit/s	28 Gbit/s	9 Gbit/s
Max. Anzahl an Sitzungen	416 Mio.	245 Mio.	43 Mio.	32 Mio.	8 Mio.
Neue Sitzungen pro Sekunde ⁷	6 Mio.	4 Mio.	925.000	623.000	208.000
Virtuelle Systeme (Basis/max.) ⁸	25/225	25/225	–	–	–

1. Die Ergebnisse wurden mit PAN-OS 10.0 ermittelt.
 2. Die Ergebnisse in dieser Spalte wurden aus einer optimalen Kombination von DPC-A- und NPC-100G-Karten in allen verfügbaren Steckplätzen abgeleitet.
 3. Die Messung des Durchsatzes erfolgte mit aktivierter App-ID und Protokollierung bei 64-KB-HTTP/Appmix-Transaktionen.
 4. Der Durchsatz der Disable Server Response Inspection (Überprüfung der Serverantwort deaktivieren, DSRI) wurde mit aktivierten Systemen für App-ID, IPS, Antivirensoftware, Anti-Spyware, WildFire, Datei-Blockade und Protokollierung bei 64-KB-HTTP-Transaktionen gemessen.
 5. Die Messung des Threat Prevention-Durchsatzes erfolgte mit aktivierten Systemen für App-ID, IPS, Antivirensoftware, Anti-Spyware, WildFire und Protokollierung bei 64-KB-HTTP/Appmix-Transaktionen.
 6. Die Messung des IPsec-VPN-Durchsatzes erfolgte mit aktivierter Protokollierung bei 64-KB-HTTP-Transaktionen.
 7. Die Messung der neuen Sitzungen pro Sekunde erfolgte mit Application Override bei 1-Byte-HTTP-Transaktionen.
 8. Das Basissystem beinhaltet 25 kostenlose virtuelle Systeme. Bis zu 200 zusätzliche Lizenzen können erworben werden. Maximal werden 225 virtuelle Systeme unterstützt.

Network Processing Card

Die Network Processing Card (NPC) ist für die Ausführung aller Aufgaben der Paketverarbeitung zuständig, einschließlich Networking, Klassifizierung des Datenverkehrs und Bedrohungsabwehr. Jede NPC hat 64 (erste Generation: zwei 32-Kern-CPU) bis 144 (zweite Generation: drei 48-Kern-CPU) Verarbeitungskerne, die alle darauf ausgerichtet sind, mit bis zu 66 Gbit/s pro NPC Ihr Netzwerk zu schützen.

Um dem wachsenden Bedarf an Hochleistungskonnektivität mit 40 Gbit/s und 100 Gbit/s sowie den gängigeren 10 Gbit/s-Schnittstellen gerecht zu werden, stehen drei NPC-Optionen zur Verfügung – die NPC-20GX und NPC-20GX der ersten Generation sowie die NPC-100G der zweiten Generation – die austauschbar mit der Switch Management Card (Switch Management-Karte, SMC) der ersten Generation verwendet werden können.

Data Processing Card (Datenverarbeitungskarte, DPC)

Die Data Processing Card (DPC-A) zeichnet sich durch 192 Verarbeitungskerne (zweite Generation: vier 48-Kern-CPU) auf einer einzigen Karte aus, ist in der Lage, Ihr Netzwerk mit bis zu 86 Gbit/s pro DPC-A zu schützen, und sorgt so für maximale Sicherheit. Die DPC-A basiert auf dem Design der NPC-100G der zweiten Generation und nutzt zusätzlich einen vierten Rechenkomplex und einen weiteren Offload-Prozessor anstelle von Ethernet-E/A.

Den Durchsatz auf maximale 700 Gbit/s bei der PA-7080 bzw. 416 Gbit/s bei der PA-7050 zu skalieren, ist ebenso einfach wie das Hinzufügen einer neuen DPC-A oder NPC. Dabei bestimmt das System selbst, wie es das Plus an Rechenleistung optimal nutzt.

Die DPC-A kann mit Switch Management Cards der ersten oder zweiten Generation verwendet werden.

Switch Management Card (Switch Management-Karte, SMC)

Als Kontrollzentrum der PA-7000 Series überwacht die Switch Management Card (SMC) den gesamten Datenverkehr und führt alle Managementfunktionen mit einer Kombination aus drei Komponenten durch: dem First Packet Processor, einer Hochgeschwindigkeits-Backplane und dem Managementsubsystem. SMCs der ersten und zweiten Generation stehen zur Verfügung. Dabei bietet die zweite Generation deutliche Verbesserungen bei allen drei Komponenten.

First Packet Processor

Der First Packet Processor (FPP) trägt entscheidend zur Leistungsmaximierung und zur linearen Skalierbarkeit der PA-7000 Series bei und überwacht fortlaufend den gemeinsamen Pool der verfügbaren Verarbeitungs- und I/O-Ressourcen auf allen NPCs und DPCs. Dabei wird der eingehende Datenverkehr intelligent an

nicht ausgelastete Prozessoren weitergeleitet. Kommen weitere Verarbeitungskarten zur Leistungs- und Kapazitätssteigerung hinzu, hat das keinen Einfluss auf die Verwaltung des Datenverkehrs. Auch eine Neuverkabelung oder Neukonfiguration Ihrer PA-7000 Series ist nicht notwendig.

Hochgeschwindigkeits-Backplane

Dank einer Hochgeschwindigkeits-Backplane hat jede Verarbeitungskarte Zugriff auf über 100 Gbit/s blockierungsfreie Datenverkehrskapazität. Das Management-Subsystem fungiert als Kontaktstelle zur Steuerung aller Komponenten der PA-7000 Series.

Management-Subsystem

Dieses Subsystem fungiert als Kontaktstelle zur Steuerung aller Komponenten der PA-7000 Series.

Dedizierte Logging Card (Protokollierungskarte)

Die Logging Card, ein wesentlicher Bestandteil jedes Systems, verwendet ein Dual-CPU-Design und erstellt ein dediziertes Subsystem zur Verwaltung der großen Menge an Protokolldateien, die die PA-7000 Series erzeugt. Es stehen zwei Logging Cards zur Verfügung: eine Log Processing Card (Protokollverarbeitungskarte, LPC) der ersten Generation und eine Log Forwarding Card (Protokollweiterleitungskarte, LFC) der zweiten Generation. Die LPC nutzt bis zu 4 TB RAID1-Speicher, um Protokollierungsaktivitäten zu verlagern. So bietet sie Ihnen die Möglichkeit, aus den zuletzt gesammelten Protokolldateien Abfragen und Berichte zu erstellen. Die LFC ist eine hochleistungsfähige Karte und für den Export von Protokollmeldungen zuständig. Mit beiden Karten können Protokolle zur Offline-Analyse an das Panorama™-Netzwerksicherheitsmanagement, an den Cortex™ Data Lake und an Syslog weitergeleitet werden. Die LPC unterstützt gemischte Konfigurationen aller Verarbeitungskarten, während die LFC zur Verwendung mit den SMC-B, 100G-NPC und DPC-A der zweiten Generation optimiert ist.

Die PA-7000 Series wird als ein einzelnes, einheitliches System verwaltet, wodurch Sie alle verfügbaren Ressourcen zum Schutz Ihrer Daten einfach managen können. Gesteuert wird die PA-7000 Series vom Betriebssystem PAN-OS®, das den gesamten Datenverkehr, also auch Anwendungen, Bedrohungen und Inhalte, zunächst nativ klassifiziert und danach mit dem Benutzer verknüpft, und zwar unabhängig davon, wo sich dieser aufhält und welchen Gerätetyp er verwendet. Anwendungen, Inhalte und Benutzer – die grundlegenden Faktoren Ihrer Geschäftsprozesse – werden somit als Basis für Ihre Sicherheitsrichtlinien herangezogen. Dies erhöht die Sicherheit, verkürzt die Reaktionszeit bei Störfällen und verringert den Verwaltungsaufwand, der mit dem ständigen Aktualisieren der Sicherheitsrichtlinien in einem hochdynamischen Umfeld einhergeht.

Tabelle 2: Hardwarespezifikationen der PA-7000 Series

	PA-7000 NPC	Vollständiges System PA-7080	Vollständiges System PA-7050
100G-NPC (PA-7000-100G-NPC-A)	SFP/SFP+ (8), QSFP+/QSFP28 (4)	SFP/SFP+ (80), QSFP+/QSFP28 (40)	(48) SFP/SFP+. (24) QSFP+/QSFP28
20G-NPC XM, Option 1: (PA-7000-20GX-NPC)	QSFP+ (2), SFP+ (12)	QSFP+ (20), SFP+ (120)	(12) QSFP+, (72) SFP+
20G-NPC XM, Option 2: (PA-7000-20GX-NPC)	10/100/1000 (12), SFP (8), SFP+ (4)	10/100/1000 (120), SFP (80), SFP+ (40)	(72) 10/100/1000, (48) SFP, (24) SFP+
Management-I/O (zweite Generation)	–	SFP MGT, (2) SFP HA1, (2) HSCI HA2/HA3 QSFP+/QSFP28 SFP MGT (2), SFP HA1 (2), HSCI HA2/HA3 QSFP+/QSFP28 (2), RJ45 seriell Konsole (1), serielle Konsole Micro-USB	
Management-I/O (erste Generation)	–	10/100/1000 (2), QSFP+ High Availability (hohe Verfügbarkeit, HA) (2), 10/100/1000 Out-of-Band-Management (1), Konsolen-Port RJ-45 (1)	

Tabelle 2: Hardwarespezifikationen der PA-7000 Series (Fortsetzung)

	PA-7000 NPC	Vollständiges System PA-7080	Vollständiges System PA-7050
Speicherkapazität (zweite Generation)	–	240-GB-SSD-Systemlaufwerk, RAID1 (2)	
Speicheroptionen (erste Generation)	–	120-GB-SSD-Systemlaufwerk (1), 1-TB- (Standard) oder 2-TB- (optional) HDD-Festplatte auf LPC, RAID1 (4)	
Eingangsspannung AC	–	100–240 V AC (50–60 Hz)	100–240 V AC (50–60 Hz)
Nenneingangsstrom	–	65–27 A	27–12 A
Stromversorgung AC-Ausgang	–	2500 W bei 240 V AC 1200 W bei 120 V AC	2500 W bei 240 V AC 1200 W bei 120 V AC
Eingangsspannung DC	–	-40 bis -60 V DC	-40 bis -60 V DC
Nenneingangsstrom	–	135 A	60 A
Stromversorgung DC-Ausgang	–	2500 W / Stromversorgung	2500 W / Stromversorgung
Max. Strom / Stromversorgung	–	12 A bei 240 V AC Eingang 75 A bei > 40 V DC Eingang	16 A bei 180 V AC Eingang 75 A bei 37,5 V DCEingang
Stromversorgungen (Basis/max.)	–	4/8	4/4
Max. Einschaltstrom / Stromversorgung	–	30 A AC / 100 A DC Spitzenstrom	50 A AC / 75 A DC Spitzenstrom
Mean Time Between Failures (mittlere Betriebsdauer zwischen Ausfällen, MTBF)	Abhängig von der Konfiguration. Wenden Sie sich für weitere Informationen zur MTBF an Ihren Ansprechpartner bei Palo Alto Networks.		
Max. BTU/h	–	20.132	10.236
Im Rack montierbar (Abmessungen)	–	19 Einheiten, 48,26-cm-Standard-Rack (81,84 cm H x 48,26 cm B x 62,64 cm T)	9 Einheiten, 48,26-cm-Standardrack (40 cm H x 48,26 cm B x 60,96 cm T)
Gewicht (nur Gerät/wie geliefert)	–	135,76 kg AC / 135,31 kg DC	85 kg AC / 83,91 kg DC
Sicherheit	–	cTUVus, CB	
EMI	–	FCC-Klasse A, CE-Klasse A, VCCI-Klasse A	
Zertifizierungen	–	NEBS Level 3	
Umgebung			
Betriebstemperatur	–	0 ° bis 50 °C	
Temperatur bei Nichtbetrieb	–	-20 ° bis 70 °C	

Weitere Informationen zu den Funktionen und den entsprechenden Leistungsmerkmalen der PA-7000 Series finden Sie unter paloaltonetworks.com/network-security/next-generation-firewall/pa-7000-series.