

Übersicht über die technischen Daten und Merkmale der Palo Alto Networks Platform

Leistung und Kapazitäten ¹	PA-7080 ³	PA-7050 ³	PA-5280	PA-5260	PA-5250	PA-5220
Firewall-Durchsatz (App-ID, Appmix)	720 Gbit/s	430 Gbit/s	67 Gbit/s	67 Gbit/s	40 Gbit/s	20 Gbit/s
Threat-Prevention-Durchsatz (Appmix)	350 Gbit/s	210 Gbit/s	33 Gbit/s	33 Gbit/s	23 Gbit/s	9 Gbit/s
IPSec-VPN-Durchsatz	240 Gbit/s	144 Gbit/s	24 Gbit/s	24 Gbit/s	16 Gbit/s	8 Gbit/s
Neue Sitzungen pro Sekunde	4.800.000	2.900.000	390.000	390.000	284.000	150.000
Max. Anzahl an Sitzungen	320.000.000	192.000.000	64.000.000	32.000.000	8.000.000	4.000.000
Virtuelle Systeme (Basis/max. ²)	25/225	25/225	25/225	25/225	25/125	10/20
Hardwarespezifikationen	PA-7080	PA-7050	PA-5280	PA-5260	PA-5250	PA-5220
Unterstützte Schnittstellen NPC-Option 1 ⁴	Bis zu (120) 10/100/1000, (80) SFP/SFP+, (40) QSFP+/QSFP28	Bis zu (72) 10/100/1000, (48) SFP/SFP+, (24) QSFP+/QSFP28	(4) 100/1000/10G Cu, (16) 1G/10G SFP/SFP+, (4) 40G/100G QSFP28			(4) 100/1000/10G Cu, (16) 1G/10G SFP/SFP+, (4) 40G QSFP+
Management-E/A	(2) SFP/SFP+ MGT, (2) SFP/SFP+ HA1, (2) HSCI HA2/HA3 QSFP+/QSFP28, (1) serielle Konsole RJ-45, (1) serielle Konsole Micro-USB		(2) 10/100/1000 Cu, (1) 10/100/1000 Out-of-Band-Management, (1) RJ-45-Konsole			(1) 40G QSFP+ HA
Größe	19 Einheiten, 48,26 cm Standard-Rack	9 Einheiten, 48,26 cm Standard-Rack mit optionalem PAN-AIRDUCT Kit	3 Einheiten, 48,26 cm Standard-Rack			(1) 40G QSFP+ HA
Stromversorgung	4 x 2.500 W AC (2.400 W / 2.700 W) erweiterbar bis 8	4 x 2.500 W AC (2.400 W / 2.700 W)	2 x 1.200 W AC oder DC (1:1 vollständig redundant)			
Redundante Stromversorgung	Ja		Ja			
Festplattenlaufwerke	(2) 240 GB SSD-Systemlaufwerk, RAID1		System: 240 GB SSD, RAID1; Protokoll: 2 TB HDD, RAID1			
Hot-Swap-fähige Lüfter	Ja		Ja			

Leistung und Kapazitäten ¹	PA-3260	PA-3250	PA-3220
Firewall-Durchsatz (App-ID, Appmix)	10 Gbit/s	7 Gbit/s	4,6 Gbit/s
Threat-Prevention-Durchsatz (Appmix)	4,7 Gbit/s	3,1 Gbit/s	2,6 Gbit/s
IPSec-VPN-Durchsatz	4,8 Gbit/s	3,2 Gbit/s	2,5 Gbit/s
Neue Sitzungen pro Sekunde	118.000	84.000	57.000
Max. Anzahl an Sitzungen	3.000.000	2.000.000	1.000.000
Virtuelle Systeme (Basis/max. ²)	1/6	1/6	1/6
Hardwarespezifikationen	PA-3260	PA-3250	PA-3220
Unterstützte Schnittstellen ⁴	(12) 10/100/1000, (8) 1G/10G SFP/SFP+, (4) 40G QSFP+	(12) 10/100/1000, (8) 1G/10G SFP/SFP+	(12) 10/100/1000, (4) 1G SFP, (4) 1G/10G SFP/SFP+
Management-E/A	(1) 10/100/1000 Out-of-Band Management Port, (2) 10/100/1000 High Availability, (1) 10G SFP+ High Availability, (1) Konsolen-Port RJ-45, (1) Micro USB		
Größe	2 Einheiten, Standard-Rack 48,26 cm (8,89 cm H x 52,15 cm T x 44,04 cm B)		
Stromversorgung	650 W AC oder DC (180/240)		
Redundante Stromversorgung	Ja		
Festplattenlaufwerke	240 GB SSD		
Hot-Swap-fähige Lüfter	Ja		

Übersicht über die technischen Daten und Merkmale der Palo Alto Networks Platform

Leistung und Kapazitäten ¹	PA-850	PA-820	PA-220	PA-220/R
Firewall-Durchsatz (App-ID, Appmix)	2 Gbit/s	1 Gbit/s	560 Mbit/s	560 Mbit/s
Threat-Prevention-Durchsatz (Appmix)	1 Gbit/s	790 Mbit/s	260 Mbit/s	260 Mbit/s
IPSec-VPN-Durchsatz	500 Mbit/s	400 Mbit/s	100 Mbit/s	100 Mbit/s
Neue Sitzungen pro Sekunde	13.000	8.300	4.200	4.200
Max. Anzahl an Sitzungen	192.000	128.000	64.000	64.000
Virtuelle Systeme (Basis)	1	1	1	1
Hardwarespezifikationen	PA-850	PA-820	PA-220	PA-220/R
Unterstützte Schnittstellen ⁴	(4) 10/100/1000, (4) SFP, (4) 10 SFP+	(4) 10/100/1000, (8) SFP	(8) 10/100/1000	(6) 10/100/1000 und 2 SFP
Management-E/A	(1) 10/100/1000 Out-of-Band-Management, (2) 10/100/1000 High Availability, RJ-45-Konsole, (1) USB, (1) Micro-USB-Konsole		(1) 10/100/1000 Out-of-Band-Management, (1) RJ-45-Konsole, (1) USB, (1) Micro-USB-Konsole	(1) 10/100/1000 Out-of-Band-Management, (1) RJ-45-Konsole, (1) USB, (1) Micro-USB-Konsole
Größe	1 Einheit, 48,26 cm Standard-Rack		4,11 cm H x 15,98 cm T x 20,50 cm B	5,08 cm H x 22,00 cm T x 23,50 cm B
Stromversorgung	2 x 500 W AC; 1 davon redundant		200 W	2 x 40 W redundant
Keine Stromversorgung	Ja		Nein	Keine
Redundante Stromversorgung	Ja		Nein	Keine
Festplattenlaufwerke	240 GB SSD		32 GB EMMC	32 GB EMMC
Hot-Swap-fähige Lüfter	Nein		Nein	Nein

Leistung und Kapazitäten ¹	VM-50/VM-50 Lite	VM-100/VM-200	VM-300/VM-1000-HV	VM-500	VM-700
Firewall-Durchsatz (App-ID)	200 Mbit/s	2 Gbit/s	4 Gbit/s	8 Gbit/s	16 Gbit/s
Threat-Prevention-Durchsatz	100 Mbit/s	1 Gbit/s	2 Gbit/s	4 Gbit/s	8 Gbit/s
IPSec-VPN-Durchsatz	100 Mbit/s	1 Gbit/s	1,8 Gbit/s	4 Gbit/s	6 Gbit/s
Neue Sitzungen pro Sekunde ¹	3.000	15.000	30.000	60.000	120.000
Unterstützte CPUs	2 ⁶	2	2, 4	2, 4, 8	2, 4, 8, 16
Dezidiertes Speicher (mindestens)	4,0 ⁸ /4,5 GB	6,5 GB	9 GB	16 GB	56 GB
Dezidierte Festplattenkapazität (mindestens)	32 GB ⁷	60 GB	60 GB	60 GB	60 GB

Von VM-Series unterstützte Umgebungen	VM-50/VM-50 Lite	VM-100/VM-200	VM-300/VM-1000-HV	VM-500	VM-700
Private Cloud					
1. VMware NSX Manager 6.3/6.4.1 oder später	Nein	Ja	Ja	Ja	Nein
2. Cisco ACI 2.3/3.0/3.1/3.2	Ja	Ja	Ja	Ja	Ja
3. Openstack Mirantis 8.0 mit Contrail 3.2; OpenStack Newton 10	Ja	Ja	Ja	Ja	Ja
4. Nutanix AOS 5.1.5/5.5.4 oder später/5.9/5.10;	Ja	Ja	Ja	Ja	Ja
Hypervisor					
1. VMware ESXi 6.0/6.5/6.7	Ja	Ja	Ja	Ja	Ja
2. KVM auf CentOS/RHEL 7.0/7.1/7.2/7.5 und Ubuntu 14.04/16.04 LTS	Ja	Ja	Ja	Ja	Ja
3. Microsoft Hyper-V (Windows 2016 mit Hyper-V-Rolle oder Hyper-V 2016)	Ja	Ja	Ja	Ja	Ja
Public Cloud					
1. Amazon Web Services (AWS)	Nein	BYOL oder VM-Series ELA	PAYG (VM-300), BYOL oder VM-Series ELA	BYOL oder VM-Series ELA	BYOL oder VM-Series ELA
2. Microsoft Azure	Nein	BYOL oder VM-Series ELA	PAYG (VM-300), BYOL oder VM-Series ELA	BYOL oder VM-Series ELA	BYOL oder VM-Series ELA
3. Google Cloud Platform (GCP)	Nein	BYOL oder VM-Series ELA	PAYG (VM-300), BYOL oder VM-Series ELA	BYOL oder VM-Series ELA	BYOL oder VM-Series ELA
4. Oracle Cloud	Nein	BYOL oder VM-Series ELA	BYOL oder VM-Series ELA	BYOL oder VM-Series ELA	BYOL oder VM-Series ELA
5. Alibaba Cloud	Nein	BYOL oder VM-Series ELA	BYOL oder VM-Series ELA	BYOL oder VM-Series ELA	BYOL oder VM-Series ELA

(1) Die Leistung von VM-Series ist abhängig von der zugrundeliegenden Virtualisierungsinfrastruktur (Hypervisor/Cloud). Ausführliche Leistungs- und Testdaten können den jeweiligen Datenblättern entnommen werden. (2) Für zusätzliche virtuelle Systeme muss eine separate Lizenz erworben werden. (3) Neue Sitzungen pro Sekunde und Max. Sitzungskapazität für PA-7000 Series mit 100G-NPCs. (4) Glasfaser-/Kupfer-Transceiver sind separat erhältlich. (6) CPU-Überbelegung wird unterstützt mit bis zu fünf Instanzen einer Zwei-CPU-Konfiguration. (7) Beim ersten Startvorgang sind 60 GB erforderlich. Nach Aktivierung der Lizenz benötigt VM-Series 32 GB. (8) Wird nur mit VM-50 Lite unterstützt.

April 2019 (PAN-OS 9.0) Diese Übersicht über die technischen Daten und Merkmale ist nur für Vergleichszwecke bestimmt. Aktuelle Informationen sind den jeweiligen Produktdatenblättern zu entnehmen.

Übersicht über die technischen Daten und Merkmale der Palo Alto Networks Platform

Wichtige Merkmale	Bei allen Modellen unterstützt
Next-Generation Firewall	
Umfassende Transparenz und granulare Kontrolle für Tausende von Anwendungen; Möglichkeit zur Erstellung benutzerdefinierter Anwendungen; Möglichkeit zur richtlinienbasierten Verwaltung von unbekanntem Datenverkehr	✓
Benutzeridentifikation und -kontrolle: VPNs, WLAN-Controller, Captive Portal, Proxys, Active Directory, eDirectory, Exchange, Terminal Services, Syslog-Parsing, XML-API	✓
Granulare SSL-Entschlüsselung und -Überprüfung (ein- und ausgehend); richtlinienbasierte SSH-Kontrolle (ein- und ausgehend)	✓
Netzwerkverbindung: dynamisches Routing (RIP, OSPF, BGP, Multiprotocol BGP), DHCP, DNS, NAT, Route Redistribution, ECMP, LLDP, BFD, Überprüfung Tunnelinhalt	✓
QoS: richtlinienbasierte Datenverkehrsformung (Priorität, garantiert, maximal) pro Anwendung, pro Benutzer, pro Tunnel, basierend auf DSCP-Klassifizierung	✓
Virtuelle Systeme: logische, separat verwaltete Firewall-Instanzen innerhalb einer physischen Firewall, wobei der Datenverkehr jedes virtuellen Systems separat behandelt wird	✓
Zonenbasierte Netzwerksegmentierung und Zonensicherheit; DoS-Schutz vor Überflutung mit neuen Sitzungen	✓
Threat Prevention (Abonnement erforderlich)	
Automatisch durchgesetzte Inline-Malware-Sicherheit über nutzlastbasierte Signaturen; tägliche Aktualisierung	✓
Schwachstellenbasierter Schutz vor Exploits und Umgehungsmethoden auf Netzwerk- und Anwendungsebene, einschließlich Port-Scans, Pufferüberläufen, Paketfragmentierung und Verschleierung	✓
Verhinderung von Datenexfiltration oder sekundärer Malware-Nutzlasten durch Command-and-Control(C2)-Aktivitäten; Identifikation von infizierten Hosts durch DNS-Sinkholing	✓
URL-Filterung (Abonnement erforderlich)	
Automatische Prävention von webbasierten Angriffen, einschließlich Phishing-Links in E-Mails, Phishing-Websites, HTTP-basiertes C2 und Seiten mit Exploit-Kits	✓
Möglichkeit zur Unterbindung laufender Credential-Phishing-Aktivitäten	✓
Benutzerdefinierte URL-Kategorien, Alerts und Benachrichtigungsseiten	✓
WildFire Malware Prevention (Abonnement erforderlich)	
Erkennung von Zero-Day-Malware und -Exploits mit kombinierten, komplementären Analyseverfahren	✓
Automatisierte Prävention innerhalb von fünf Minuten für alle Netzwerke, Endpunkte und Clouds	✓
Sicherheitsdaten aus einer Community von mehr als 29.000 Mitgliedern	✓
AutoFocus Threat Intelligence (Abonnement erforderlich)	
Kontextualisierung und Klassifizierung von Angriffen, einschließlich Malware-Familie, Angreifer und Kampagne, zur Beschleunigung von Gegenmaßnahmen	✓
Umfassende, global korrelierte Bedrohungsdaten von WildFire	✓
Bedrohungsdaten von Drittanbietern für automatisierte Sicherheit	✓
DNS-Sicherheit (Abonnement erforderlich)	
Automatische Prävention von zig Millionen bössartiger Domains, die mit Echtzeit-Analysen und kontinuierlich wachsenden globalen Bedrohungsdaten identifiziert werden	✓
Schnelle Erkennung von Command-and-Control oder Datendiebstahl durch DNS-Tunneling mit Analysen auf der Grundlage von maschinellem Lernen	✓
Automatisierung dynamischer Gegenmaßnahmen zur Ermittlung infizierter Systeme und schnellen richtlinienbasierten Reaktion	✓
Datei- und Datenfilterung	
Bidirektionale Kontrolle über unbefugte Bewegungen von Dateitypen, Sozialversicherungs- und Kreditkartendaten sowie individuelle Dateimuster	✓
GlobalProtect Netzwerksicherheit für Endpunkte (Abonnement erforderlich)	
Remote-Access-VPN (SSL, IPsec, ohne Client); mobile Threat Prevention und Richtliniendurchsetzung je nach App, Benutzer, Inhalt, Gerät und Gerätestatus	✓
BYOD: App-Level-VPN zur Wahrung der Privatsphäre der Benutzer	✓
Panorama-Netzwerksicherheitsmanagement (zum Verwalten mehrerer Firewalls Abonnement erforderlich)	
Intuitive Richtlinienkontrolle mit Anwendungen, Benutzern, Bedrohungen, erweitertem Malware-Schutz, URLs, Dateitypen und Datenmustern in der gleichen Richtlinie	✓
Praktische Erkenntnisse über Datenverkehr und Bedrohungen mit dem Application Command Center (ACC); individuell anpassbare Reporting-Funktionen	✓
Aggregierte Protokolle und Funktionen zur Korrelation von Ereignissen	✓
Konsistente, skalierbare Verwaltung von bis zu 30.000 Geräten und sämtlichen Firewalls der VM-Series; rollenbasierte Zugriffskontrolle; logische und hierarchische Gerätegruppen; Vorlagen	✓
GUI, CLI, XML-basierte REST API	✓