Palo Alto Networks Platform Specifications and Features Summary

Table 1: Firewall Performance and Capacities[1]

Performance and Capacities[1]	PA-7080[3]	PA-7050[3]	PA-5280	PA-5260	PA-5250	PA-5220
Firewall throughput (App-ID, appmix)	700 Gbps	360 Gbps	56 Gbps	56 Gbps	40 Gbps	20 Gbps
Threat Prevention throughput (appmix)	350 Gbps	198 Gbps	31.5 Gbps	31.5 Gbps	21 Gbps	8.9 Gbps
IPsec VPN throughput	280 Gbps	168 Gbps	27 Gbps	27 Gbps	18 Gbps	10 Gbps
New sessions per second	4,800,000	2,900,000	390,000	390,000	284,000	150,000
Maximum sessions	320,000,000	192,000,000	64,000,000	32,000,000	8,000,000	4,000,000
Virtual systems (base/max[2])	25/225	25/225	25/225	25/225	25/125	10/20
Hardware Specifications	**PA-7080**	**PA-7050**	**PA-5280**	**PA-5260**	**PA-5250**	**PA-5220**
Interfaces supported NPC option 14	10/100/1000 (up to 120), SFP/ SFP+ (up to 80), QSFP+/QSFP28 (up to 40)	10/100/1000 (up to 72), SFP/ SFP+ (up to 48), QSFP+/QSFP28 (up to 24)	100/1000/10G Cu (4), 1G/10G SFP/SFP+ (16), 40G/100G QSFP28 (4)			100/1000/10G Cu (4), 1G/10G SFP/SFP+ (16), 40G QSFP+ (4)
Management I/O	SFP/SFP+ MGT (2), SFP/SFP+ HA1 (2), HSCI HA2/HA3 QSFP+/QSFP28 (2), RJ45 serial console (1), Micro USB serial console (1)		10/100/1000 Cu (2), 10/100/1000 out-of-band management (1), RJ45 console (1)			
			40G/100G QSFP28 HA (1)			(1) 40G QSFP+ HA
Size	19U, 19” standard rack	9U, 19” standard rack or 14U, 19” standard rack with optional PAN-AIRDUCT kit	3U, 19” standard rack			
Power supply	2500 W AC (2400 W / 2700 W) (4; expandable to 8)	2500 W AC (2400 W / 2700 W) (4)	1200 W AC or DC (1:1 fully redundant) (2)			
Redundant power supply	Yes		Yes			
Disk drives	240 GB SSD system drive, RAID1 (2)		System: 240 GB SSD, RAID1 | Log: 2 TB HDD, RAID1			
Hot-swappable fans	Yes		Yes			

Performance and Capacities[1]	PA-3260	PA-3250	PA-3220
Firewall throughput (App-ID, appmix)	10 Gbps	6.6 Gbps	5 Gbps
Threat Prevention throughput (appmix)	4.4 Gbps	3 Gbps	2.4 Gbps
IPsec VPN throughput	4.8 Gbps	3.2 Gbps	2.7 Gbps
New sessions per second	118,000	84,000	57,000
Maximum sessions	3,000,000	2,000,000	1,000,000
Virtual systems (base/max[2])	1/6	1/6	1/6
Hardware Specifications	**PA-3260**	**PA-3250**	**PA-3220**
Interfaces supported[4]	10/100/1000 (12), 1G/10G SFP/SFP+ (8), 40G QSFP+ (4)	10/100/1000 (12), 1G/10G SFP/SFP+ (8)	10/100/1000 (12), 1G SFP (4), 1G/10G SFP/SFP+ (4)
Management I/O	(1) 10/100/1000 out-of-band management port, (2) 10/100/1000 high availability, (1) 10G SFP+ high availability, (1) RJ-45 console port, (1) Micro USB		
Size	2U, 19” standard rack (3.5” H x 20.53” D x 17.34” W)		
Power supply	650 W AC or DC (180/240)		
Redundant power supply	Yes		
Disk drives	240 GB SSD		
Hot-swappable fans	Yes		

Table 1: Firewall Performance and Capacities[1] (continued)

	PA-850	PA-820	PA-220	PA-220R
Firewall throughput (App-ID, appmix)	2 Gbps	1.6 Gbps	580 Mbps	580 Mbps
Threat Prevention throughput (appmix)	1 Gbps	800 Mbps	280 Mbps	280 Mbps
IPsec VPN throughput	1.6 Gbps	1.2 Gbps	500 Mbps	500 Mbps
New sessions per second	13,000	8,300	4,200	4,200
Maximum sessions	192,000	128,000	64,000	64,000
Virtual systems (base)	1	1	1	1
Hardware Specifications	**PA-850**	**PA-820**	**PA-220**	**PA-220R**
Interfaces supported[4]	10/100/1000 (4), SFP (4), 10 SFP+ (4)	10/100/1000 (4), SFP (8)	10/100/1000 (8)	10/100/1000 (6), SFP (2)
Management I/O	10/100/1000 out-of-band management (1), 10/100/1000 high availability (2), RJ-45 console (1), USB (1), Micro USB console (1)		10/100/1000 out-of-band management (1), RJ-45 console (1), USB (1), Micro USB console (1)	10/100/1000 out-of-band management (1), RJ-45 console (1), USB (1), Micro USB console (1)
Size	1U, 19” standard rack		1.62” H x 6.29” D x 8.07” W	2.0” H x 8.66” D x 9.25” W
Power supply	500 W AC (2; one is redundant)	200 W	Dual redundant 40 W	None
Redundant power supply	Yes	No	Yes (optional)	None
Disk drives	240 GB SSD		32 GB EMMC	32 GB EMMC
Hot-swappable fans	No		No	No

Performance and Capacities[1]	VM-50/VM-50 Lite	VM-100/VM-200	VM-300/VM-1000-HV	VM-500	VM-700
Firewall throughput (App-ID)	200 Mbps	2 Gbps	4 Gbps	8 Gbps	16 Gbps
Threat Prevention throughput	100 Mbps	1 Gbps	2 Gbps	4 Gbps	8 Gbps
IPsec VPN throughput	100 Mbps	1 Gbps	1.8 Gbps	4 Gbps	6 Gbps
New sessions per second[1]	3,000	15,000	30,000	60,000	120,000
CPUs supported	2[6]	2	2, 4	2, 4, 8	2, 4, 8, 16
Dedicated memory (minimum)	4.08/4.5 GB	6.5 GB	9 GB	16 GB	56 GB
Dedicated disk drive capacity (minimum)	32 GB[7]	60 GB	60 GB	60 GB	60 GB

VM-Series Supported Environments	VM-50/VM-50 Lite	VM-100/VM-200	VM-300/VM-1000-HV	VM-500	VM-700
Private Cloud					
1. VMware NSX-V	No	Yes	Yes	Yes	No
2. VMware NSX-T	No	Yes	Yes	Yes	Yes
3. Cisco ACI	Yes	Yes	Yes	Yes	Yes
4. OpenStack	Yes	Yes	Yes	Yes	Yes
5. Nutanix AOS	Yes	Yes	Yes	Yes	Yes
Hypervisor					
1. VMware ESXi	Yes	Yes	Yes	Yes	Yes
2. KVM on CentOS/RHEL and Ubuntu LTS	Yes	Yes	Yes	Yes	Yes
3. Microsoft Hyper-V	Yes	Yes	Yes	Yes	Yes
Public Cloud					
1. Amazon Web Services (AWS)	No	BYOL[9] or VM-Series ELA	PAYG[10] (VM-300), BYOL or VM-Series ELA	BYOL or VM-Series ELA	BYOL or VM-Series ELA
2. Microsoft Azure	No	BYOL or VM-Series ELA	PAYG (VM-300), BYOL or VM-Series ELA	BYOL or VM-Series ELA	BYOL or VM-Series ELA
3. Google Cloud Platform (GCP)	No	BYOL or VM-Series ELA	PAYG (VM-300), BYOL or VM-Series ELA	BYOL or VM-Series ELA	BYOL or VM-Series ELA
4. Oracle Cloud	No	BYOL or VM-Series ELA	BYOL or VM-Series ELA	BYOL or VM-Series ELA	BYOL or VM-Series ELA
5. Alibaba Cloud	No	BYOL or VM-Series ELA	BYOL or VM-Series ELA	BYOL or VM-Series ELA	BYOL or VM-Series ELA

(1) VM-Series performance will vary based on underlying virtualization infrastructure (hypervisor/cloud). Refer to the individual datasheets for detailed performance and testing information. (2) Adding virtual systems to the base quantity requires a separately purchased license. (3) New sessions per second and max session capacity for PA-7000 Series specified with 100G-NPCs. (4) Optical/Copper transceivers are sold separately. (6) CPU oversubscription supported with up to five instances running on a two-CPU configuration. (7) 60 GB required at initial boot. VM-Series will use 32 GB after license activation. (8) Supported with VM-50 Lite model only. (9) “Bring your own license” deployment option. (10) “Pay as you go” deployment option.

Table 2: Key Features

Next-Generation Firewall	Supported Across All Models
Deep visibility and granular control for thousands of applications; ability to create custom applications; ability to manage unknown traffic based on policy	✓
User identification and control: VPNs, WLAN controllers, captive portal, proxies, Active Directory, eDirectory, Exchange, Terminal Services, syslog parsing, XML API	✓
Granular SSL decryption and inspection (inbound and outbound); per-policy SSH control (inbound and outbound)	✓
Networking: dynamic routing (RIP, OSPF, BGP, multiprotocol BGP), DHCP, DNS, NAT, route redistribution, ECMP, LLDP, BFD, tunnel content inspection	✓
QoS: policy-based traffic shaping (priority, guaranteed, maximum) per application, per user, per tunnel, based on DSCP classification	✓
Virtual systems: logical, separately managed firewall instances within a single physical firewall, with each virtual system's traffic kept separate	✓
Zone-based network segmentation and zone protection; DoS protection against flooding of new sessions	✓
Threat Prevention (subscription required)	
In-line malware prevention automatically enforced through payload-based signatures, updated daily	✓
Vulnerability-based protections against exploits and evasive techniques on network and application layers, including port scans, buffer overflows, packet fragmentation, and obfuscation	✓
Command-and-control (C2) activity stopped from exfiltrating data or delivering secondary malware payloads; infected hosts identified through DNS sinkholing	✓
URL Filtering (subscription required)	
Automatic prevention of web-based attacks, including phishing links in emails, phishing sites, HTTP-based C2, and pages that carry exploit kits	✓
Ability to stop in-process credential phishing	✓
Custom URL categories, alerts, and notification pages	✓
WildFire malware prevention (subscription required)	
Detection of zero-day malware and exploits with layered, complementary analysis techniques	✓
Automated prevention in as few as five minutes across networks, endpoints, and clouds	✓
Community-based data for protection, including more than 30,000 subscribers	✓
AutoFocus threat intelligence (subscription required)	
Contextualization and classification of attacks, including malware family, adversary, and campaign, to speed triage and response efforts	✓
Rich, globally correlated threat analysis sourced from WildFire	✓
Third-party threat intelligence for automated prevention	✓
DNS Security (subscription required)	
Automatically prevent tens of millions of malicious domains identified with realtime analysis and continuously growing global threat intelligence	✓
Quickly detect C2 or data theft employing DNS tunneling with machine learning-powered analysis	✓
Automate dynamic response to find infected machines and quickly respond in policy	✓
File and data filtering	
Bidirectional control over the unauthorized transfer of file types and Social Security numbers, credit card numbers, and custom data patterns	✓
GlobalProtect network security for endpoints (subscription required)	
Remote access VPN (SSL, IPsec, clientless); mobile threat prevention and policy enforcement based on apps, users, content, device, and device state	✓
BYOD: app-level VPN for user privacy	✓
Panorama network security management (subscription required for managing multiple firewalls)	
Intuitive policy control with applications, users, threats, advanced malware prevention, URLs, file types, and data patterns all in the same policy	✓
Actionable insight into traffic and threats with Application Command Center (ACC); fully customizable reporting	✓
Aggregated logging and event correlation	✓
Consistent scalable management of up to 30,000 hardware and all VM-Series firewalls; role-based access control; logical and hierarchical device groups; and templates	✓
GUI, CLI, XML-based REST API	✓