Palo Alto Networks ML-Powered Next-Generation Firewall Specifications and Features Summary

Table 1: Firewall Performance and Capacities[A]							
Performance and Capacities	**PA-7080[B]**	**PA-7050[B]**	**PA-5450[C]**	**PA-5280**	**PA-5260**	**PA-5250**	**PA-5220**
Firewall throughput (App-ID, appmix)	687 Gbps	416 Gbps	200 Gbps	60 Gbps	60 Gbps	37 Gbps	17 Gbps
Threat Prevention throughput (appmix)	405 Gbps	243 Gbps	148 Gbps	33.8 Gbps	33.8 Gbps	23 Gbps	9.7 Gbps
IPsec VPN throughput	334 Gbps	200 Gbps	79 Gbps[D]	28 Gbps	28 Gbps	19 Gbps	9.7 Gbps
New sessions per second	6,000,000	4,000,000	3,500,000[D]	586,000	586,000	392,000	166,000
Maximum sessions	416,000,000	245,000,000	100,000,000[D]	64,000,000	32,000,000	8,000,000	4,000,000
Virtual systems (base/max[E])	25/225			25/225			10/20
Hardware Specifications	**PA-7080**	**PA-7050**	**PA-5450**	**PA-5280**	**PA-5260**	**PA-5250**	**PA-5220**
Interfaces supported[F]	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 (up to 8), 1G/10G SFP/ SFP+ (up to 24), 40G/100G QSFP28 (up to 4)	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)		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 (33.22" H x 24.66" D x 17.5" W)	9U, 19" standard rack (15.75" H x 23.75" D x 17.5" W) or 14U, 19" standard rack with optional PAN-AIRDUCT kit (24.5" H x 23.75" D x 17.5" W)	5U, 19" standard rack (8.75" H x 30.25" D x 17.38" W)	3U, 19" standard rack (5.25" H x 20.5" D x 17.25" W)			
Power supply	2500 W AC (2400 W/2700 W) (4; expandable to 8)	2500 W AC (2400 W/2700 W) (4)	2,200 W AC or DC (2 expandable to 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: 480 GB SSD, RAID1 | Log: 4 TB SSD (optional)	System: 240 GB SSD, RAID1 | Log: 2 TB HDD, RAID1			
Hot-swappable fans	Yes			Yes			
Performance and Capacities	**PA-3260**			**PA-3250**		**PA-3220**	
Firewall throughput (App-ID, appmix)	8.7 Gbps			5.8 Gbps		4.8 Gbps	
Threat Prevention throughput (appmix)	4.7 Gbps			3.1 Gbps		2.6 Gbps	
IPsec VPN throughput	4.7 Gbps			2.9 Gbps		2.6 Gbps	
New sessions per second	94,400			63,700		52,800	
Maximum sessions	2,200,000			2,000,000		1,000,000	
Virtual systems (base/max[D])	1/6						
Hardware Specifications	**PA-3260**			**PA-3250**		**PA-3220**	
Interfaces supported[f]	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	10/100/1000 out-of-band management port (1), 10/100/1000 high availability (2), 10G SFP+ high availability (1), RJ-45 console port (1), Micro USB (1)						
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 (continued)							
Performance and Capacities	**PA-850**	**PA-820**	**PA-460**	**PA-450**	**PA-440**	**PA-220**	**PA-220R**
Firewall throughput (App-ID, appmix)	2.1 Gbps	1.7 Gbps	4.7 Gbps	3.2 Gbps	2.4 Gbps	560 Mbps	560 Mbps
Threat Prevention throughput (appmix)	1.2 Gbps	900 Mbps	2.6 Gbps	1.7 Gbps	1.3 Gbps	300 Mbps	300 Mbps
IPsec VPN throughput	1.7 Gbps	1.4 Gbps	3.1 Gbps	2.2 Gbps	1.6 Gbps	570 Mbps	570 Mbps
New sessions per second	13,100	8,100	74,000	52,000	39,000	4,200	4,200
Maximum sessions	192,000	128,000	400,000	300,000	200,000	64,000	
Virtual systems (base)	1	1			1		
Hardware Specifications	**PA-850**	**PA-820**	**PA-460**	**PA-450**	**PA-440**	**PA-220**	**PA-220R**
Interfaces supported[F]	10/100/1000 (4), 1G SFP (4), 1G/10G SFP/SFP+ (4)	10/100/1000 (4), 1G 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)				
Size	1U, 19" standard rack (1.75" H x 14.5" D x 17.125" W)	1U, 19" standard rack (1.75" H x 14" D x 17.125" W)	1.74" H x 8.83" D x 8.07" W			1.62" H x 6.29" D x 8.07" W	2.0" H x 8.66" D x 9.25" W
Power supply	450 W AC (2; one is redundant)	200 W	Dual redundant 50 W			Dual redundant 40 W	None
Redundant power supply	Yes	No	Yes (optional)				None
Disk drives	240 GB SSD		128 GB eMMC			32 GB EMMC	32 GB EMMC
Hot-swappable fans	No		Fanless				
Performance and Capacities	**CN-Series**	**VM-50/VM-50 Lite**	**VM-100/VM-200**	**VM-300/VM-1000-HV**		**VM-500**	**VM-700**
Firewall throughput (App-ID)	500 Mbps	200 Mbps	2 Gbps	4 Gbps		8 Gbps	16 Gbps
Threat Prevention throughput	250 Mbps	100 Mbps	1 Gbps	2 Gbps		4 Gbps	8 Gbps
IPsec VPN throughput	N/A	100 Mbps	1 Gbps	1.8 Gbps		4 Gbps	6 Gbps
New sessions per second[A]	N/A	3,000	15,000	30,000		60,000	120,000
Max Sessions	20,000	64,000/50,000	250,000	819,200		2,000,000	10,000,000
CPUs supported	2 (CN-MGMT) + 1 (CN-NGFW)	2[G]	2	2, 4		2, 4, 8	2, 4, 8, 16
Dedicated memory (minimum)	2 GB (CN-MGMT) + 2 GB (CN-NGFW)	4.08/4.5 GB	6.5 GB	9 GB		16 GB	56 GB
Dedicated disk drive capacity (minimum)	50 GB	32 GB[H]	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				No
2. VMware NSX-T	—	No	Yes				
3. Cisco ACI	—		Yes				
4. OpenStack	—		Yes				
5. Nutanix AOS	—		Yes				
Hypervisor							
1. VMware ESXi	—		Yes				
2. KVM on CentOS/RHEL and Ubuntu LTS	—		Yes				
3. Microsoft Hyper-V	—		Yes				
Public Cloud							
1. Amazon Web Services (AWS)	—	No	BYOL[I] or VM-Series ELA	PAYG[J] (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

(A) VM-Series performance will vary based on underlying virtualization infrastructure (hypervisor/cloud). Refer to the individual datasheets for detailed performance and testing information. (B) Each result in this column is for an optimum combination of PA-7000-DPC-A and PA-7000-100G-NPC-A cards populated in all available slots. (C) All tests performed with 2 Networking Cards + 4 Data Processing Cards populated, unless otherwise noted. (D) This test performed with 1 Networking Card + 5 Data Processing Cards populated. (E) Adding virtual systems to the base quantity requires a separately purchased license. (F) Optical/Copper transceivers are sold separately. (G) CPU oversubscription supported with up to 5 instances running on a 2-CPU configuration. (H) 60 GB required at initial boot. VM-Series will use 32 GB after license activation. (I) "Bring your own license" deployment option. (J) "Pay as you go" deployment option.

paloalto NETWORKS

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 TLS/SSL decryption and inspection (inbound and outbound); includes support for TLS 1.3 and HTTP/2 protocols	✓
Networking: dynamic routing (RIP, OSPF, BGP, multiprotocol BGP), DHCP, DNS, NAT, route redistribution, ECMP, LLDP, 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)	
Inline 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	✓
IoT Security (subscription required)	
Accurate identification and classification of all devices on a network, including never-before-seen devices	✓
Device security via ML-based anomaly detection, vulnerability assessment, risk-based policy recommendations, and enforcement with the Device-ID policy construct (Device-based policy enforcement not available on the VM-50, VM-50 Lite, or CN-Series)	✓
No additional infrastructure required to enable on Next-Generation Firewalls	✓
WildFire malware prevention (subscription required)	
Detection of zero-day malware and exploits with layered, complementary analysis techniques	✓
Automated prevention in seconds for most threats 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)	
Automatic prevention of tens of millions of malicious domains identified with real-time analysis and continuously growing global threat intelligence	✓
Quick detection of C2 or data theft employing DNS tunneling with machine-learning-powered analysis	✓
Automated 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	✓

paloalto NETWORKS