Platform Specifications and Features Summary

Performance and Capacities[1]	PA-7080 System[4]	PA-7050 System[4]	PA-5060	PA-5050	PA-5020
Firewall throughput (App-ID enabled)	200 Gbps	120 Gbps	20 Gbps	10 Gbps	5 Gbps
Threat prevention throughput	100 Gbps	60 Gbps	10 Gbps	5 Gbps	2 Gbps
IPSec VPN throughput	80 Gbps	48 Gbps	4 Gbps	4 Gbps	2 Gbps
New sessions per second	1,200,000	720,000	120,000	120,000	120,000
Max sessions[2]	40,000,000/80,000,000	24,000,000/48,000,000	4,000,000	2,000,000	1,000,000
Virtual systems (base/max[3])	25/225	25/225	25/225	25/125	10/20
Hardware Specifications	**PA-7080 System[4]**	**PA-7050 System[4]**	**PA-5060**	**PA-5050**	**PA-5020**
Interfaces supported NPC option 1[4]	Up to (20) QSFP+, (120) SFP+	Up to (12) QSFP+, (72) SFP+	(12) 10/100/1000, (8) SFP, (4) 10 SFP+		(12) 10/100/1000, (8) SFP
Interfaces supported NPC option 2[4]	Up to (120) 10/100/1000, (80) SFP, (40) SFP+	Up to (72) 10/100/1000, (48) SFP, (24) SFP+			
Management I/O	(2) 10/100/1000, (2) QSFP+ high availability, (1) 10/100/1000 out-of-band management, (1) RJ45 console		(2) 10/100/1000 high availability, (1) 10/100/1000 out-of-band management, (1) RJ45 console		
Rack mountable?	19U, 19" standard rack	9U, 19" standard rack or 14U, 19" standard rack with optional Airduct kit	2U, 19" standard rack		
Power supply	4x2500W AC (2400W / 2700) expandable to 8	4x2500W AC (2400W / 2700W)	Redundant 450W AC or DC		
Redundant power supply?	Yes		Yes		
Disk drives	2TB RAID1		120GB or 240GB SSD, RAID Optional		
Hot swap fans	Yes		Yes		

Performance and Capacities[1]	PA-3060	PA-3050	PA-3020	PA-500	PA-200
Firewall throughput (App-ID enabled)	4 Gbps	4 Gbps	2 Gbps	250 Mbps	100 Mbps
Threat prevention throughput	2 Gbps	2 Gbps	1 Gbps	100 Mbps	50 Mbps
IPSec VPN throughput	500 Mbps	500 Mbps	500 Mbps	50 Mbps	50 Mbps
New sessions per second	50,000	50,000	50,000	7,500	1,000
Max sessions	500,000	500,000	250,000	64,000	64,000
Virtual systems (base/max[2])	1/6	1/6	1/6	N/A	N/A
Hardware Specifications	**PA-3060**	**PA-3050**	**PA-3020**	**PA-500**	**PA-200**
Interfaces supported[3]	(8) 10/100/1000, (8) SFP, (2) 10 SFP+	(12) 10/100/1000, (8) SFP		(8) 10/100/1000	(4) 10/100/1000
Management I/O	(1) 10/100/1000 out-of-band management,(2) 10/100/1000 high availability, (1) RJ-45 console			(1) 10/100/1000 out-of-band management, (1) RJ-45 console port	
Rack mountable?	1.5U, 19" standard rack	1U, 19" standard rack		1U, 19" standard rack	1.75" H x 7"D x 9.25"
Power supply	Redundant 400W AC	250W AC		180W	40W
Redundant power supply?	Yes	No		No	No
Disk drives	120GB SSD			160GB	16GB SSD
Hot swap fans	No			No	No

Performance and Capacities[5]	VM-1000-HV	VM-300	VM-200	VM-100
Firewall throughput (App-ID enabled)	1 Gbps	1 Gbps		
Threat prevention throughput	600 Mbps	600 Mbps		
IPSec VPN throughput	250 Mbps	250 Mbps		
New sessions per second	8,000	8,000		
Max sessions	250,000	250,000	100,000	50,000
Virtualization Specifications	**VM-1000-HV**	**VM-300**	**VM-200**	**VM-100**
HyperVisor	• VMware ESXi 5.5/6.0, NSX Manager 6.0/6.1/6.2 (Required for NSX integrated solution) • VMware ESXi 5.1/5.5/6.0 (Stand alone) • KVM on CentOS/RHEL 6.5 and Ubuntu 12.04 LTS • Citrix Xen Server on SDX 10.1 • Amazon AWS • Microsoft Azure with Azure Resource Manager (ARM)	• VMware ESXi 5.1/5.5/6.0 (Stand alone) • KVM on CentOS/RHEL 6.5 and Ubuntu 12.04 LTS • Citrix Xen Server on SDX 10.1 • Amazon AWS • Microsoft Azure with Azure Resource Manager (ARM)		
Network drivers	• VMware ESXi: VMXNet 3 • Citrix NetScaler SDX: Igbvf version 2.0.4, Ixgbevf version 2.7.12 • KVM: virtIO, e1000, SR-IOV and PCI passthrough for Intel 82576 based 1G NIC, Intel 82599 based 10G NIC, Broadcom 57112 and 578xx based 10G NIC • Amazon Web Services: proprietary; SR-IOV Enhanced Networking (ixgbevf) on supported instance types • Microsoft Azure and Hyper-V: proprietary			
Dedicated CPU cores	2, 4 or 8			
Dedicated Memory (Minimum)	4GB			
Dedicated Disk drive capacity (Min/Max)	40GB/2TB			

(1) Performance and capacities are measured under ideal testing conditions with App-ID enabled and PAN-OS 7.1. (2) Max session capacity for NPCs with standard memory/extended memory (XM). (3) Adding virtual systems to the base quantity requires a separately purchased license. (4) QSFP, SFP, SFP+ and XFP transceivers are sold separately. PAN-OS 7.1 is required for NPC Option 1-XM and Option 2-XM. (5) VM-Series performance and capacities are measured under ideal testing conditions with App-ID enabled and PAN-OS 7.1 using 4 CPU cores.

Platform Specifications and Features Summary

Key Features	Supported Across All Platforms
Firewall	
Applications identified (App-IDs)	2,160+
Customizable App-IDs	✓
Policy-based control by user, group or IP address, application, application category, subcategory, technology, risk factor or characteristic	✓
Scheduled policies	✓
Per policy SSL decryption & inspection (inbound and outbound)/Per policy SSH control (inbound and outbound)	✓
IPSec VPN (site-to-site) and SSL VPN (GlobalProtect)	✓
User control: Active Directory, LDAP, eDirectory, Exchange, Citrix and Microsoft Terminal Services, XML API (User-ID)	✓
Threat Prevention (Subscription Required)	
Stream-based protection against viruses (including those embedded in HTML, Javascript, PDF and compressed), spyware, worms	✓
Drive-by download protection	✓
Behavioral botnet detection	✓
Modern Malware Protection (WildFire Subscription Required)	
Dynamic analysis and detection of unknown malware within PE, PDF, Java, Android APK, Adobe Flash, all Microsoft Office file types and webpages.	✓
Automated signature generation and delivery for discovered malware	✓
Inline control of malware infection and command/control traffic	✓
URL Filtering (Subscription Required)	
On-box customizable URL filtering database	✓
Customizable categories, allow, block lists and block pages	✓
Safe search (Google, Bing, Yahoo)	✓
File and Data Filtering	
Bidirectional control over the unauthorized transfer of more than 60 file types	✓
Bidirectional control over the transfer of Social Security Numbers, Credit Card Numbers, custom data patterns	✓
QoS	
Policy-based traffic shaping (priority, guaranteed, maximum) per application, per user, per tunnel and more	✓
Policy-based diffserv marking	✓
VPN Connectivity	
GlobalProtect (IPSec/SSL VPN)	✓
IPSec VPN (Site-to-Site)	✓
Mobile Security (GlobalProtect Mobile Security Manager, Gateway & App subscription or licenses required)	
Monitor and report device state for policy enforcement, such as jailbroken devices	✓
Manage device settings, configure key device functions, detect Android malware	✓
Deliver mobile threat prevention and policy enforcement based on apps, users, content, device and device state	
Networking	
Dynamic routing (BGP, OSPF, RIP)	✓
Tap mode, virtual wire, layer 2, and layer 3	✓
802.1Q VLAN tagging (layer 2, layer 3)	✓
Network address translation (NAT)	✓
DHCP server/ DHCP relay (up to 3 servers)	✓
IPv6 L2, L3, tap, virtual wire (transparent mode), App-ID, User-ID, Content-ID, WildFire and SSL decryption	✓
Multicast	✓
High Availability	
Active/Active, Active/Passive	✓ **(PA-200 and VM-Series support HA Lite only)**
Configuration and session synchronization	✓
Interface and IP tracking	✓
Link and path failure monitoring	✓
Management and Visibility Tools	
Integrated web interface, CLI and centralized management (Panorama)	✓
Graphical summary of applications, URL categories, threats and data (ACC)	✓
View, filter, export traffic, threat, URL, and data filtering logs	✓
Syslog and SNMPv2/v3	✓
XML-based REST API	✓
Automation features that facilitate dynamic policy updates (Dynamic Object Groups VM-monitoring)	✓
Fully customizable reporting	✓
Shared policies and objects (Panorama)	✓
Role-based administration (Individual Device or Panorama)	✓