PA-7050

Key Security Features:

CLASSIFY ALL APPLICATIONS, ON ALL PORTS, ALL THE TIME WITH APP-ID™.

- Identify the application, regardless of port, encryption (SSL or SSH) or evasive technique employed.
- Use the application, not the port, as the basis for all safe enablement policy decisions: allow, deny, schedule, inspect, apply traffic shaping.
- Categorize unidentified applications for policy control, threat forensics, custom App-ID creation, or packet capture for App-ID development.

EXTEND SAFE APPLICATION ENABLEMENT POLICIES TO ANY USER, AT ANY LOCATION, WITH USER-ID™ AND GLOBALPROTECT™.

- Agentless integration with Active Directory, LDAP, eDirectory Citrix and Microsoft Terminal Services.
- Easily integrate firewall policies with NAC, 802.1X wireless, Proxies and NAC solutions.
- Deploy consistent policies to local and remote users running Microsoft Windows, Mac OS X, Linux, Android or iOS platforms.

PROTECT AGAINST ALL THREATS—BOTH KNOWN AND UNKNOWN—WITH CONTENT-ID™ AND WILDFIRE™.

- Block a range of known threats including exploits, malware and spyware, across all ports, regardless of common threat evasion tactics employed.
- Limit unauthorized transfer of files and sensitive data, and control non work-related web surfing.
- Identify unknown malware, analyze it based on more than 100 malicious behaviors, then automatically create and deliver protection in the next content update.

PA-7050

The Palo Alto Networks® PA-7050 is designed to protect datacenters and high-speed networks with firewall throughput of up to 120 Gbps and full threat prevention at speeds of up to 100 Gbps. The PA-7050 is a modular chassis, allowing you to scale performance and capacity by adding up to six network processing cards as your requirements change; yet it is a single system, making it as easy to manage as all of our other appliances.

PERFORMANCE AND CAPACITIES[1]	PA-7050 SYSTEM	PA-7000-20G-NPC
Firewall throughput (App-ID enabled)	120 Gbps	20 Gbps
Threat prevention throughput (DSRI Enabled[2])	100 Gbps	16 Gbps
Threat prevention throughput	60 Gbps	10 Gbps
IPSec VPN throughput	24 Gbps	4 Gbps
Max sessions	24,000,000	4,000,000
New sessions per second	720,000	120,000
Virtual systems (base/max[3])	25/225	N/A

[1] Performance and capacities are measured under ideal testing conditions using PAN-OS 6.0.
[2] DSRI = Disable Server Response Inspection.
[3] Adding virtual systems to the base quantity requires a separately purchased license.

paloalto NETWORKS®
the network security company™

DELIVERING LINEAR SCALABILITY AND PERFORMANCE

The PA-7050 achieves predictable datacenter level protection and performance by applying more than 400 function-specific processors distributed across the following chassis subsystems:

- Network Processing Card (NPC): Each NPC delivers 20 Gbps of firewall performance using multi-core security optimized processors, along with dedicated high-speed networking and content inspection processors. Up to six NPCs, each with 24 traffic interfaces are supported in the PA-7050.
- **Switch Management Card (SMC):** The SMC is comprised of three elements that are key to delivering predictable datacenter protection and performance: the First Packet Processor, the 1.2 Tbps switch fabric and the management subsystem.
    - **First Packet Processor (FPP):** The FPP utilizes dedicated processing to apply intelligence to the incoming traffic, directing it to the appropriate processing resource to maximize throughput efficiency.
    - **High Speed Switch Fabric:** The 1.2 Tbps switch fabric means that each NPC has access to approximately 100 Gbps of traffic capacity, ensuring that performance and capacity will scale in a linear manner as NPCs are added to the PA-7050.
    - **Management Subsystem:** Unified point of contact for managing all aspects of the PA-7050.
- **Log Processing Card (LPC):** The LPC uses multi-core processors and 2TB of RAID 1 storage to offload the logging related activities without impacting the processing required for other management related tasks. The LPC allows you to generate on-system queries and reports from the most recent logs collected or forward them to a syslog server for archiving or additional analysis.

The PA-7050 delivers performance and scalability by intelligently applying all available networking and security processing power to application layer traffic classification and threat protection tasks. Orchestrating this ballet of session management tasks is the First Packet Processor which constantly tracks the shared pool of processing and I/O resources across all of the NPCs. When the FPP determines that additional processing resources are available, traffic is intelligently directed across the high-speed switch fabric to that location, even if it resides on a separate NPC. The FPP is the key to delivering linear scalability to the PA-7050, working in conjunction with each of the network processors on the NPCs to utilize all of the available computing resources as a single, cohesive system. This means that as NPCs are added, no traffic engineering changes are required in order to utilize the added capacity.

The controlling element of the PA-7050 is PAN-OS™, a security-specific operating system that natively classifies all traffic, inclusive of applications, threats and content, then ties that traffic to the user, regardless of location or device type. The application, content, and user—the elements that run your business—are then used as the basis of your security policies, resulting in an improved security posture and a reduction in incident response time. All traffic classification, content inspection, policy lookup and execution are performed in a single pass. The single pass software architecture, when combined with the processing power of the PA-7050, ensures that you achieve predictable throughput.

Networking Features

INTERFACE MODES

- L2, L3, Tap, Virtual wire (transparent mode)

ROUTING

- OSPFv2/v3, BGP with graceful restart, RIP, static routing
- Policy-based forwarding
- Point-to-Point Protocol over Ethernet (PPPoE)
- Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, and v3

IPV6

- L2, L3, tap, virtual wire (transparent mode)
- Features: App-ID, User-ID, Content-ID, WildFire and SSL decryption

IPSEC VPN

- Key Exchange: Manual key, IKE v1 (Pre-shared key, certificate-based authentication)
- Encryption: 3DES, AES (128-bit, 192-bit, 256-bit)
- Authentication: MD5, SHA-1, SHA-256, SHA-384, SHA-512

VLANS

- 802.1q VLAN tags per device/per interface: 4,094/4,094
- Aggregate interfaces (802.3ad)

NETWORK ADDRESS TRANSLATION (NAT)

- NAT modes (IPv4): static IP, dynamic IP, dynamic IP and port (port address translation)
- NAT64
- Additional NAT features: Dynamic IP reservation, dynamic IP and port oversubscription

HIGH AVAILABILITY

- Modes: Active/Active, Active/Passive
- Failure detection: Path monitoring, interface monitoring

The PA-7050 supports a wide range of networking features that allows you to more easily integrate our security features into your existing network.

Hardware Specifications

I/O

PA-7050 System - (72) 10/100/1000, (48) Gigabit SFP, (24) 10 Gigabit SFP+
PA-7050 NPC - (12) 10/100/1000, (8) Gigabit SFP, (4) 10 Gigabit SFP+
(Each PA-7050 supports up to six NPCs)

MANAGEMENT I/O

- ((2) 10/100/1000+(2) 40Gbps high availability, (1) 10/100/1000 out-of-band management, (1) RJ45 console port

STORAGE OPTIONS

- 80GB SSD System Drive + 4x1TB HDD on Log Processing Card

STORAGE CAPACITY

- 2TB RAID1

AC POWER SUPPLIES (SYTEM AVG/MAX POWER CONSUMPTION)

- 4x2500W AC (2400W / 2700W)

MAX BTU/HR

9,213

INPUT VOLTAGE (INPUT FREQUENCY)

- 200-240VAC (50-60Hz)

MAX CURRENT CONSUMPTION

- 12A@240VAC

MAX INRUSH CURRENT

- 200A

RACK MOUNTABLE (DIMENSIONS)

- 15.75"H x 19"W x 24"D

WEIGHT (STAND ALONE DEVICE/AS SHIPPED)

- 184Lbs

SAFETY

- UL, CUL, CB

EMI

- FCC Class A, CE Class A, VCCI Class A

CERTIFICATIONS

- NEBS Level 3 (pending)

ENVIRONMENT

- Operating temperature: 32 to 122 F, 0 to 50 C
- Non-operating temperature: -4 to 158 F, -20 to 70 C

To view additional information on the PA-7050 security features and associated capacities, please visit **www.paloaltonetworks.com/products.**

paloalto NETWORKS®
the network security company™

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com