VM-Series

Key VM-Series next-generation firewall features:

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

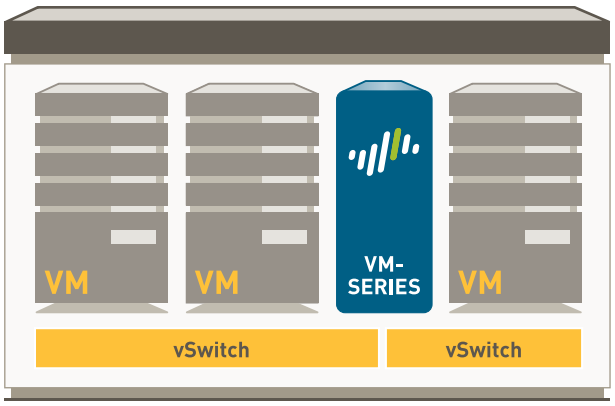
- Identify the application, regardless of port, encryption (SSL or SSH) or evasive technique employed.
- Use the application, not the port, as the basis for all safe enablement policy decisions: allow, deny, schedule, inspect, apply traffic shaping.
- Categorize unidentified applications for policy control,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

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.
- Integrate with NAC, wireless, and other non-standard user repositories with an XML API.
- Deploy consistent policies to users running Microsoft Windows, Mac OS X, Linux, Android or iOS platforms, regardless of location.

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 for more than 100 malicious behaviors, automatically create and deliver protection in the next available update.



VM-Series Virtual Firewall

The Palo Alto Networks™ VM-Series extends secure application enablement into virtualized environments while addressing key virtualization security challenges: tracking security policies to virtual machine movement with dynamic address objects and integration with orchestration systems using a powerful XML management API.

The VM-Series is comprised of three high performance models, the VM-100, VM-200, and the VM-300, all of which use a single pass software architecture to minimize latency in datacenter environments. The management and data plane are separated so that users can assign dedicated CPUs to each as a means of ensuring that management access is always available, irrespective of traffic loads. The controlling element of the VM-Series is PAN-OS™, a security-specific operating system that allows organizations to safely enable applications using App-ID, User-ID, Content-ID, GlobalProtect, and WildFire.

GENERAL CAPACITIES[1]	VM-300	VM-200	VM-100
Max sessions	250,000	100,000	50,000
IPSec VPN tunnels/tunnel interfaces	2,000	500	25
GlobalProtect (SSL VPN) concurrent users	500	200	25
SSL decrypt sessions	1024	1024	1024
SSL inbound certificates	25	25	25
Virtual routers	3	3	3
Security zones	40	20	10
Max number of policies	5,000	2,000	250
Address objects	10,000	4,000	2,500
PERFORMANCE[1]			
Firewall throughput (App-ID Enabled)		1 Gbps	
Threat prevention throughput		600 Mbps	
IPSec VPN throughput		250 Mbps	
New sessions per second		8,000	

[1] Performance and capacities are measured under ideal testing conditions using PAN-OS 5.0 and 4 CPU cores.

paloalto NETWORKS
the network security company™

VIRTUALIZATION SPECIFICATIONS	VM-300 VM-200 VM-100
HyperVisor	VMware ESXi 4.1 and ESXi 5.0
Network driver	VMXNet3
CPU cores	2, 4 or 8
Memory (Minimum)	4GB
Disk drive capacity (Min/Max)	40GB/2TB

NETWORKING

INTERFACE MODES

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

ROUTING

- Modes: OSPF, RIP, BGP, Static
- Forwarding table size (entries per device/per VR): 5000/5000 (VM-300), 1,250/1,250 (VM-200), 1000/1000 (VM-100)
- Policy-based forwarding
- Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, and v3

HIGH AVAILABILITY

- Modes: Active/Passive with no session synchronization
- Failure detection: Path monitoring, Interface monitoring

ADDRESS ASSIGNMENT

- Address assignment for device: DHCP Client/PPPoE/Static
- Address assignment for users: DHCP Server/DHCP Relay/Static

IPV6

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

VLANS

- 802.1q VLAN tags per device/per interface: 4,094/4,094
- Max interfaces: 2,000 (VM-300), 500 (VM-200), 100 (VM-100)

NAT/PAT

- Max NAT rules: 1,000 (VM-300), 1,000 (VM-200), 125 (VM-100)
- Max NAT rules (DIPP): 200 (VM-300), 200 (VM-200), 125 (VM-100)
- Dynamic IP and port pool: 254
- Dynamic IP pool: 32,000
- NAT Modes: 1:1 NAT, n:n NAT, m:n NAT
- DIPP oversubscription (Unique destination IPs per source port and IP): 2 (VM-300), 1 (VM-200), 1 (VM-100)
- NAT64

VIRTUAL WIRE

- Max virtual wires: 1,000 (VM-300), 250 (VM-200), 50 (VM-100)
- Interface types mapped to virtual wires: physical and subinterfaces

L2 FORWARDING

- ARP table size/device: 2,500 (VM-300), 500 (VM-200), 500 (VM-100)
- MAC table size/device: 2,500 (VM-300), 500 (VM-200), 500 (VM-100)
- IPv6 neighbor table size: 1,000 (VM-300), 500 (VM-200), 500 (VM-100)

SECURITY

FIREWALL

- Policy-based control over applications, users and content
- Fragmented packet protection
- Reconnaissance scan protection
- Denial of Service (DoS)/Distributed Denial of Services (DDoS) protection
- Decryption: SSL (inbound and outbound), SSH

WILDFIRE

- Identify and analyze targeted and unknown files for more than 100 malicious behaviors
- Generate and automatically deliver protection for newly discovered malware via signature updates
- Signature update delivery in less than 1 hour, integrated logging/reporting; access to WildFire API for programmatic submission of up to 100 samples per day and up to 1,000 report queries by file hash per day (Subscription Required)

FILE AND DATA FILTERING

- File transfer: Bi-directional control over more than 60 unique file types
- Data transfer: Bi-directional control over unauthorized transfer of CC# and SSN
- Drive-by download protection

USER INTEGRATION (USER-ID)

- Microsoft Active Directory, Novell eDirectory, Sun One and other LDAP-based directories
- Microsoft Windows Server 2003/2008/2008r2, Microsoft Exchange Server 2003/2007/2010
- Microsoft Terminal Services, Citrix XenApp
- XML API to facilitate integration with non-standard user repositories

IPSEC VPN (SITE-TO-SITE)

- Key Exchange: Manual key, IKE v1
- Encryption: 3DES, AES (128-bit, 192-bit, 256-bit)
- Authentication: MD5, SHA-1, SHA-256, SHA-384, SHA-512
- Dynamic VPN tunnel creation (GlobalProtect)

THREAT PREVENTION (SUBSCRIPTION REQUIRED)

- Application, operating system vulnerability exploit protection
- Stream-based protection against viruses (including those embedded in HTML, Javascript, PDF and compressed), spyware, worms

URL FILTERING (SUBSCRIPTION REQUIRED)

- Pre-defined and custom URL categories
- Device cache for most recently accessed URLs
- URL category as part of match criteria for security policies
- Browse time information

QUALITY OF SERVICE (QOS)

- Policy-based traffic shaping by application, user, source, destination, interface, IPSec VPN tunnel and more
- 8 traffic classes with guaranteed, maximum and priority bandwidth parameters
- Real-time bandwidth monitor
- Per policy diffserv marking
- Physical interfaces supported for QoS: 6 (VM-300, VM-200), 4(VM-100)

SSL VPN/REMOTE ACCESS (GLOBALPROTECT)

- GlobalProtect Gateway
- GlobalProtect Portal
- Transport: IPSec with SSL fall-back
- Authentication: LDAP, SecurID, or local DB
- Client OS: Mac OS X 10.6, 10.7 (32/64 bit), 10.8 (32/64 bit), Windows XP, Windows Vista (32/64 bit), Windows 7 (32/64 bit)
- Third party client support: Apple iOS, Android 4.0 and greater, VPNC IPSec for Linux

MANAGEMENT, REPORTING, VISIBILITY TOOLS

- Integrated web interface, CLI or central management (Panorama)
- Multi-language user interface
- Syslog, Netflow v9 and SNMP v2/v3
- XML-based REST API
- Graphical summary of applications, URL categories, threats and data (ACC)
- View, filter and export traffic, threat, WildFire, URL, and data filtering logs
- Fully customizable reporting

For a complete description of the VM-Series next-generation firewall feature set, please visit www.paloaltonetworks.com/literature.

paloalto NETWORKS
the network security company™

3300 Olcott Street
Santa Clara, CA 95054

Main: +1.408.573.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com