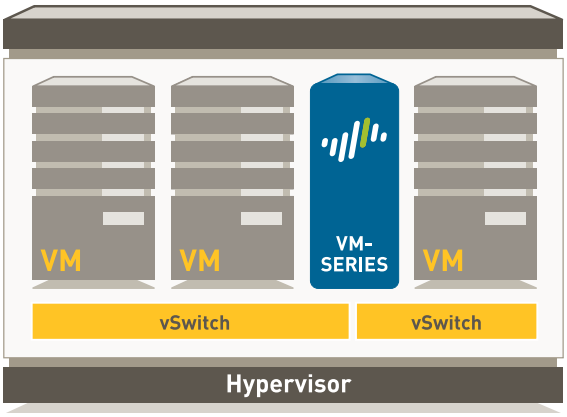
VM-Series

The VM-Series delivers comprehensive visibility, control and safe application enablement for virtualized and cloud environments.

- Identify, segment and safely enable applications regardless of port, encryption (SSL or SSH) or evasive technique employed.
- Address risk and compliance mandates with protection against known and unknown threats including exploits, viruses, spyware, malware and advanced persistent threats (APTs).
- Create dynamic security policies with virtualization and business context.
- Reduce errors in security configuration through context sharing between virtualization and security environments.



As your organization embraces virtualization and cloud initiatives, security is a critical consideration. Security must deliver the appropriate levels of visibility, safe application enablement and threat protection necessary without compromising agility. Unfortunately, traditional network security solutions can be slow to deploy and provision in virtualized and cloud environments and are often implemented with limited feature sets.

The VM-Series extends safe application enablement to virtualized and cloud environments using the same PAN-OS™ feature set that is available in physical security appliances. The core of the VM-Series is the next-generation firewall which 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—in other words, the business elements that run the business—are then used as the basis of an organization's security policies, resulting in an improved security posture and a reduction in incident response time.

The VM-Series is based on a Single Pass software architecture to minimize latency. Operations such as application identification and decoding and signature matching for all threats and content, networking functions, and policy lookup, are executed once to optimize performance. The management and data plane are separated, with dedicated CPUs assigned to each plane to ensure that management access is always available, irrespective of traffic loads.

The VM-Series allows you to apply next-generation security policies to virtualized and cloud computing environments at the same speed that the virtualized applications are built up and taken down.

- **Automated, transparent deployment and provisioning:** In order to support the agile characteristics of virtualization and cloud, security provisioning must be automated. Tight integration with VMware NSX enables the VM-Series security services to be automatically deployed and transparently inserted to inspect VM to VM traffic. In addition, the VM-Series supports a flexible REST-based API, which allows you to integrate with 3rd party cloud orchestration solutions such as OpenStack and CloudStack. This enables the VM-Series to be deployed and configured in lock step with virtualized workloads.
- **Policy creation with dynamic context:** In a virtualized and cloud environment where virtual machines often change functions and can move from server to server, building security policies based on static IP addresses alone can have limited value. Dynamic Address Groups allows you to create policies using tags as an identifier for virtual machines instead of a static object definition. Multiple tags representing virtual machine attributes such as IP address and operating system can be resolved within a Dynamic Address Group, allowing you to easily apply policies to virtual machines as they are created or travel across the network.
- **Automated VM monitoring:** Security policies must be able to monitor and keep up with changes in virtual machine attributes. The VM Monitoring capabilities on the VM-Series provide agent and agentless options to poll VMware environments (ESXi or vCenter) for virtual machine inventory and changes. Virtual machine attributes are collected as tags and can then be used in Dynamic Address Groups to keep track of virtual machine changes.
- **Centralized management:** Security appliances in a virtual and cloud environment should be managed in the same consistent manner as physical security appliances. The VM-Series can be managed using Panorama to ensure consistent enforcement of policies across physical, virtual and cloud environments. Rich centralized logging and reporting capabilities provide visibility into virtualized applications, users and content.

Deployment Flexibility

The VM-Series can be deployed in a variety of deployment use cases:

VM-Series for ESXi servers (standalone)

The VM-Series on ESXi servers is ideal in virtualized and cloud networks for East-West traffic inspection, specifically to safely enable application traffic between VMs residing on the same virtualized server.

The VM-Series on ESXi servers resides as a guest VM and requires virtual networking configuration to place the VM-Series in the path of traffic. This provides flexibility to select the appropriate VM-Series deployment mode on each virtualized server depending on organizational needs.

VM-Series for VMware NSX

In order for organizations to build a cloud environment with optimized capacity utilization and operational efficiencies, security challenges must be addressed. Visibility into communications between virtualized applications of different trust levels residing on the same physical server is needed, along with comprehensive protection against threats that can propagate from VM to VM. Dynamic security policies are needed to keep pace with virtualized application changes. In addition, security provisioning and corresponding networking changes to place traffic in the path of security must be automated.

The Palo Alto Networks integration with VMware NSX addresses these challenges. The solution components include VM-1000-HV, Panorama the centralized management platform for physical and virtual security appliances and VMware NSX network virtualization platform. As part of this integration, a VM-1000-HV is deployed on every ESXi server, and the appropriate application traffic is automatically steered to it for inspection by VMware NSX. In addition, rich security policies on applications, virtual machine "containers" and content can be defined on Panorama with dynamic context on VMs shared by VMware NSX. This allows organizations to accelerate the deployment of business critical applications, increase visibility and protection against advanced threats, and maintain consistent security for all data center traffic.

Please see the VMware NSX solution brief for more information on this integration.

VM-Series for Citrix SDX

Many organizations are building next-generation data centers that must support an IT-as-a-service cloud delivery model. In this cloud delivery model, a comprehensive set of services must be available to enhance the availability, security and performance of applications. Citrix NetScaler SDX is an open, multi-services platform that supports NetScaler application delivery controller (ADC) services, and best-in-class network and security services.

VM-Series on Citrix NetScaler SDX enables security and ADC capabilities to be consolidated on a single platform. This addresses the independent application needs for business units, owners and SP customers in a multi-tenant deployment. The combination of VM-Series on Citrix NetScaler SDX also provides a complete, validated, security and ADC solution for Citrix XenApp and XenDesktop deployments.

Please see the Citrix SDX solution brief for more information on this integration.

GENERAL CAPACITIES[1]	VM-1000-HV	VM-300	VM-200	VM-100
Max sessions	250,000	250,000	100,000	50,000
IPSec VPN tunnels/tunnel interfaces	2,000	2,000	500	25
GlobalProtect (SSL VPN) concurrent users	500	500	200	25
SSL decrypt sessions	12,500	1,024	1,024	1,024
SSL inbound certificates	1,000	25	25	25
Virtual routers	3	3	3	3
Security zones	40	40	20	10
Max number of policies	10,000	5,000	2,000	250
Address objects	10,000	10,000	4,000	2,500
Max IP addresses registered per system	100,000	1,000	1,000	1,000

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 6.0 and 4 CPU cores.

VIRTUALIZATION SPECIFICATIONS

HYPERVISOR

VM-1000-HV:

- VMware NSX Manager 6.0 with VMware ESXi 5.5
- VMware ESXi 4.1, ESXi 5.0, ESXi 5.5
- Citrix NetScaler SDX 11500 and 17550 Series

VM-300 | VM-200 | VM-100:

- VMware ESXi 4.1, ESXi 5.0, ESXi 5.5
- Citrix NetScaler SDX 11500 and 17550 Series

NETWORK DRIVER

- VMware ESXi - VMXNet 3
- Citrix NetScaler SDX – Igbvf version 2.0.4, Ixgbevf – version 2.7.12

CPU CORES

2, 4 or 8

MEMORY (MINIMUM)

4GB

DISK DRIVE CAPACITY (MIN/MAX)

40GB/2TB

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

Networking Features

INTERFACE MODES

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

ROUTING

- Modes: OSPF, RIP, BGP, Static
- 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

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)

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

To view additional information on the VM-Series 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