VM-SERIES ON LINUX KVM

Kernel-based Virtual Machine (KVM) is a leading open source hypervisor that service providers and enterprises alike use to build and deploy cloud computing environments. Linux KVM, in conjunction with OpenStack®, represents a complete open source software-based offering that combines the cost reduction of cloud computing with the benefits of open source.

VM-Series on KVM Use Cases

Palo Alto Networks VM-Series virtualized next-generation firewalls give you the flexibility to deploy next-generation security and advanced threat prevention across your KVM-based private, public, and hybrid cloud environments. The VM-Series enables you to:

- Identify and control traffic traversing your KVM-based cloud environment, limit application access based on users, and block known and unknown threats.
- Automate security policy updates so that they keep pace with changes to your private, public, and hybrid clouds.
- Manage virtual and physical appliances using Panorama, and automate security with a rich set of RESTful APIs.

Organizations are expanding their virtualization and cloud initiatives in a variety of ways, with security remaining a priority. Increased use dictates an effort for streamlined security workflows and an eye toward cloud-centric architectures that are scalable and resilient.

Today, more workloads reside in on-premises private clouds than ever, and use of the public cloud is increasing dramatically, leading to multi-cloud environments and increased demand for capacity. Examples include security deployed as a virtual network function—a cost-effective alternative to securing branch offices and data center/private cloud workloads—as well as an uptick in multi-tenant virtualized environments. Security automation workflows have streamlined virtualized security deployments, but they can still be complex and involve many steps. Security, traditionally viewed as a bottleneck that slows deployment, must more readily support the move toward cloud-centric architecture.

Palo Alto Networks VM-Series on KVM addresses these key challenges with the same next-generation firewall and advanced threat prevention features available on our physical appliances. All traffic is natively analyzed in a single pass to identify the application, content, and user. These identifiers become integral components of your security policy, allowing you to tightly control access to your cloud resources and isolate your mission-critical applications, protecting them from known and unknown threats.

The VM-Series on KVM enables you to protect your data residing in OpenStack- and KVM-based virtualized environments from cyberthreats. Panorama™ network security management, combined with native automation features, allows you to streamline policy management in a way that minimizes the policy lag time that may occur as virtual machines are added, moved, or removed.

Virtualized Next-Generation Security at High Performance and Scale

VM-Series virtualized next-generation firewalls are optimized to deliver App-ID™ technology-enabled throughput at industry-leading rates ranging from 200 Mbps to 16 Gbps across five models, which include:

- **VM-50**—engineered to consume minimal resources and support CPU oversubscription yet deliver up to 200 Mbps of App-ID-enabled firewall performance for customer scenarios from virtual branch offices and customer-premise equipment to high-density, multi-tenant environments.
- **VM-100 and VM-300**—optimized to deliver 2 Gbps and 4 Gbps of App-ID-enabled throughput, respectively, for hybrid cloud, segmentation, and internet gateway use cases.
- **VM-500 and VM-700**—able to deliver 8 Gbps to 16 Gbps of App-ID-enabled firewall throughput, respectively, and deployable as NFV security components in fully virtualized data center and service provider environments.

The Data Plane Development Kit, managed by The Linux Foundation, has been integrated into the VM-Series on KVM for enhanced packet processing performance on x86 infrastructure. Network I/O options, such as PCI passthrough and single-root I/O virtualization (SR-IOV), are supported for enhanced performance.

Applying Next-Generation Security to Virtualized Environments

The VM-Series virtualized next-generation firewall is based upon the same full-stack traffic classification engine as our physical firewalls. The VM-Series natively classifies all traffic, inclusive of applications, threats, and content, and then ties that traffic to the user. The application, content, and user—the elements that run your business—form the basis of your virtualized security policies, resulting in improved security posture and reduced incident response time.

Isolate Mission-Critical Applications and Data Using Zero Trust Principles

Security best practices dictate that your mission-critical applications and data should be isolated in secure segments using the Zero Trust principle—never trust, always verify—at each segmentation point. The VM-Series can be deployed throughout your virtualized environment, residing as a gateway within your virtual network or between the VMs running in different tiers, thereby protecting east-west traffic by exerting control based on application and user identity.

Block Lateral Movement of Cyberthreats

Today's cyberthreats will commonly compromise an individual workstation or user and then move across the network, looking for a target. Within your virtual network, cyberthreats will rapidly move laterally (east-west) from VM to VM, placing your mission-critical applications and data at risk. Exerting application-level control using Zero Trust in between VMs will reduce the threat footprint while applying policies to block both known and unknown threats.

Automated Deployment and Provisioning

You can use a rich set of APIs to integrate with external orchestration and management tools, collecting information related to workload changes, which you can then use to dynamically drive policy updates via VM Monitoring and Dynamic Address Groups (DAGs).

RESTful APIs

A flexible, REST-based API allows you to integrate with third-party or custom cloud orchestration offerings. This enables the VM-Series to be deployed and configured in lockstep with virtualized workloads.

Virtual Machine Monitoring

Security policies must be able to monitor and keep up with changes in virtualization environments, including VM attributes and the addition or removal of VMs. VM Monitoring automatically polls your virtualization environments for VM inventory and changes, collecting this data in the form of tags that can then be used in DAGs to keep policies up to date.

Dynamic Address Groups

As your VMs change functions or move from server to server, building security policies based on static data, such as IP address, delivers limited value and can contain outdated information. DAGs allows you to create policies using tags (from VM Monitoring) as identifiers for VMs instead of a static object definition. Multiple tags representing VM attributes, such as IP address and operating system, can be resolved within a DAG, allowing you to easily apply policies to VMs as they are created or travel across the network, without administrative intervention.

Bootstrapping

In addition to XML template-based bootstrapping for KVM-based virtual environments, VM-Series firewall in OpenStack environments support "config-drive" for sharing metadata. With these bootstrapping approaches, a VM-Series firewall can be modified at deployment time, effectively delivering a customized firewall during the initial provisioning process.

Centrally Manage Virtualized and Physical Firewalls

Panorama enables you to manage your VM-Series deployments along with your physical security appliances, ensuring policy consistency and cohesion. Rich, centralized logging and reporting capabilities provide visibility into virtualized applications, users, and content.

VM-Series on KVM Use Cases

Perimeter Gateway

If your organization is establishing a build-your-own-cloud environment, the VM-Series on KVM allows you to apply all Palo Alto Networks Next-Generation Firewall and advanced threat prevention features to the traffic traversing your cloud perimeter.

In this use case, you can deploy the VM-Series on KVM as your gateway firewall, enable the applications you want, and inspect them for known and unknown threats, regardless of port. Access to the virtualized workloads is controlled based on the user identity, adding yet another level of protection. As new workloads are added or modified, VM-Series automation features, APIs, and an optional OpenStack plugin allow you to dynamically update security policies, ensuring they keep pace with your respective cloud changes.

Service Provider Customer Offerings

Service providers commonly use KVM and OpenStack to efficiently, cost-effectively scale their cloud service offerings for customers. The open source nature of the offering lends itself to highly customized and differentiated services, such as virtualized CPE deployments and SD-WAN, as well as high-capacity, virtualized, network-based security services for large enterprise customers. Combined with the next-generation firewall and automation features in the VM-Series, service providers can build highly profitable cloud service offerings.

Flexible Licensing Options

The VM-Series on KVM supports several licensing options, including perpetual bundles and enterprise license agreements. Perpetual bundle options allow you to choose any one VM-Series model, along with its associated subscriptions and support. A VM-Series Enterprise License Agreement (ELA) takes a forecast of your VM-Series firewall consumption over a one- or three-year period, and purchase price is based on that projected usage. Included in each VM-Series ELA is a VM-Series firewall license, subscriptions for Threat Prevention, URL Filtering, WildFire® malware prevention service, GlobalProtect™ Gateway, and unlimited Panorama VM licenses and support. The VM-Series ELA allows you to use a single license authorization code across all virtual environments supported by the VM-Series and is ideally suited for customers with large-scale, expanding virtual environments, who want to be able to deploy VM-Series next-generation firewalls and associated subscriptions wherever needed. The VM-Series ELA simplifies the purchasing process, providing a simplified, predictable cost structure by establishing a single start and end date for all VM-Series licenses and subscriptions.

Performance and Capacities	VM-50 (0.4 Core)	VM-100/ VM-200 (2 Cores)	VM-300/ VM-1000-HV (4 Cores)	VM-500 (8 Cores)	VM-700 (16 Cores)
With SR-IOV/PCI passthrough of I/O enabled					
Firewall throughput (App-ID enabled)[1]	200 Mbps	2 Gbps	4 Gbps	8 Gbps	16 Gbps
Threat Prevention throughput[2]	100 Mbps	1 Gbps	2 Gbps	4 Gbps	8 Gbps
IPsec VPN throughput[1]	100 Mbps	1 Gbps	1.8 Gbps	4 Gbps	6 Gbps
New sessions per second[3]	3,000	15,000	30,000	60,000	120,000
With open virtual switch OVS-DPDK					
Firewall throughput (App-ID enabled)[1]	100 Mbps	1 Gbps	2 Gbps	4 Gbps	8 Gbps
Threat Prevention throughput[2]	50 Mbps	500 Mbps	1 Gbps	2 Gbps	4 Gbps
New sessions per second[3]	1,000	8,000	15,000	30,000	60,000
Capacities					
Max sessions	64,000	250,000	800,000	2,000,000	10,000,000
Max security policies	250	1,500	10,000	10,000	20,000
Max routes	5,000	10,000	20,000	64,000	200,000
IPsec tunnels	250	1,000	2,000	4,000	8,000

1. Firewall and IPsec VPN throughput are measured with App-ID and User-ID features enabled, using 64 KB HTTP transactions.
2. Threat Prevention throughput is measured with App-ID, User-ID, IPS, antivirus, and anti-spyware features enabled, using 64 KB HTTP transactions.
3. New sessions per second is measured with application-override utilizing 1 byte HTTP transactions.

Performance and Capacities Summary

In virtualized and cloud environments, many factors, such as type of CPU, hypervisor version, numbers of cores assigned, memory, and network I/O options, can impact your performance. We recommend additional testing within your environment to ensure your performance and capacity requirements are met.

VM-Series Specifications and Features

The following tables list all supported specifications, resource requirements, and networking features of VM-Series on KVM.

Virtualization Specifications	
Image formats supported	QCOW2
Hypervisors supported	KVM on CentOS Red Hat Enterprise Linux (RHEL) KVM on Ubuntu
Network I/O options	• Virtio • Paravirtual drivers (Intel e1000) • PCI passthrough • SR-IOV
Bootstrap support	• XML template-based bootstrap in KVM environments • "Config-drive" with nova boot in OpenStack
OpenStack distributions supported*	• Mirantis OpenStack v8.0 • Red Hat OpenStack Platform 5,7, and 10
Other KVM based platforms/hypervisors supported	• Cisco Enterprise Network Compute System (ENCS) • Nutanix AHV

*Refer to product documentation for up-to-date information on supported versions.

System Requirements	VM-50 (0.4 Core)	VM-100/ VM-200 (2 Cores)	VM-300/ VM-1000-HV (4 Cores)	VM-500 (8 Cores)	VM-700 (16 Cores)
CPU configurations supported	2[1]	2	2 and 4	2, 4, and 8	2, 4, 8 and 16
Memory (minimum)	4.5 GB	6.5 GB	9 GB	16 GB	56 GB
Disk drive capacity (min/max)	32 GB[2] / 2 TB	60 GB / 2 TB	60 GB / 2 TB	60 GB / 2 TB	60 GB / 2 TB

1. CPU oversubscription is supported with up to five instances running on a 2 CPU core configuration.
2. 60 GB drive capacity is needed on initial boot. VM-Series instance will use 32GB after license activation.

Networking Features	
Interface Modes	**VLANs**
• L2, L3, tap, and virtual wire (transparent mode)	• 802.1Q VLAN tags per device/per interface: 4,094/4,094 • Max interfaces: ◦ 4,096 (VM-500/VM-700) ◦ 2,048 (VM-100/VM-300) ◦ 512 (VM-50)
Routing	**Network Address Translation**
• Modes: OSPF, RIP, BGP, and Static • Policy-based forwarding • Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, and v3	• 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	**IPv6**
• Modes: active/passive with session synchronization • Failure detection: path monitoring, interface monitoring	• L2, L3, tap, and virtual wire (transparent mode) • Features: App-ID, User-ID, Content-ID, WildFire, and SSL decryption

Summary

The VM-Series on KVM enables service provider and other organizations to protect their cloud environments with full next-generation firewall and threat prevention services. Traffic flowing into your KVM-based cloud is identified based on the application, and then inspected for known and unknown cyberthreats. Automation features and centralized management with Panorama ensure that security policy can keep pace with any contextual changes in your cloud environment.

To learn more about VM-Series security features and associated capacities, please visit www.paloaltonetworks.com/products.

3000 Tannery Way
Santa Clara, CA 95054

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

www.paloaltonetworks.com