VM-SERIES

Next-Generation Firewall Security and Advanced Threat Prevention for Your Cloud Computing Deployment

As your organization embraces virtualization and cloud initiatives, your networking, security and virtualization teams have two options when it comes to protecting the resident mission-critical applications and data from modern cyber threats. The first alternative is to ignore security altogether, not because it is unnecessary, but because security policy deployment cannot keep pace with the rate of virtualization changes, oftentimes lagging weeks behind.

- Supports a wide range of hypervisor and orchestration environments including: VMware NSX, ESXi, vCloud Air, Citrix Netscaler SDX, Amazon Web Services and KVM with optional support for the OpenStack plugin.
- Identify and control applications within your virtualized environments, limit access based on users, and prevent known and unknown threats.
- Isolate and segment mission-critical applications and data using Zero Trust principles.
- Streamline policy deployment so that security keeps pace with the rate of change within your private, public or hybrid cloud.

The second alternative is to implement traditional security technologies that are port-bound, which means they lack the ability to identify and control applications, and they are ineffective at blocking today's modern attacks. Neither of these alternatives addresses the critical requirements you need to protect your virtualized environments. To be successful, organizations need a cloud security solution that:

- Controls applications within your cloud, based on the application identity, not the ports and protocols it uses.
- Stops malware from gaining access to, and moving laterally (east-west) within your cloud.
- Determines who should be allowed to use the applications, and grants access based on user needs and credentials.
- Simplifies management and minimizes the security policy lag as VMs are added, removed or moved within the cloud environment.

The Palo Alto Networks® VM-Series combines next-generation firewall security and advanced threat prevention to protect your virtualized environments from advanced cyber threats. Panorama centralized management, combined with a rich set of APIs can be used to integrate with external orchestration and management tools collecting information related to workload changes, which can then be used to dynamically drive policy updates. The result is a reduction in the security lag that may occur as your VMs change.

Applying next-generation security to virtualized environments

The VM-Series natively analyzes all traffic in a single pass to determine the application identity, the content within, and the user identity. These are then used as integral components of your security policy, resulting in an improved security posture and a reduction in 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 Zero Trust (never trust, always verify) principles at each segmentation point. The VM-Series can be deployed in your cloud environment, allowing you to protect east-west traffic between VMs at the application level.

Block lateral movement of cyber threats

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

Automated, transparent deployment and provisioning

A rich set of APIs can be used to integrate with external orchestration and management tools collecting information related to workload changes, which can then be used to dynamically drive policy updates via Dynamic Address Groups and VM Monitoring.

- **RESTful APIs:** A flexible, REST-based API allows you to integrate with third-party or custom cloud orchestration solutions. 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. Virtual Machine Monitoring (VM Monitoring) automatically polls your virtualization environments for virtual machine inventory and changes, collecting this data in the form of tags that can then be used in Dynamic Address Groups to keep policies up to date.
- **Dynamic Address Groups:** As your virtual machines are added, removed or change, building security policies based on static data, such as IP address, delivers limited value. Dynamic Address Groups allow you to create policies using tags [from VM Monitoring] 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.

Centrally manage virtualized and physical form factor firewalls

Panorama™ network security management enables you to manage your VM-Series deployments, along with your physical security appliances, thereby ensuring policy consistency and cohesiveness. 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 hypervisor and orchestration environments.

VM-Series for VMware NSX

The VM-Series for NSX is a tightly integrated solution that ties together: the VM-Series next-generation firewall, Panorama for centralized management, and VMware® NSX™ to deliver on the promise of a software-defined data center. As new virtual workloads are deployed, NSX Manager simultaneously installs a VM-Series next-generation firewall on each ESXi™ server. Once deployed on the ESXI server, safe application enablement policies that identify, control, and protect your virtualized applications and data can be deployed to each VM-Series in an automated manner by Panorama. NSX will then begin steering select application traffic to the VM-Series for more granular application-level security. As new workloads are added, removed or moved, NSX feeds those attribute changes to Panorama where they are translated into dynamic security policy updates to the virtual and perimeter gateway firewalls. The VM-Series for NSX supports virtual wire network interface mode, which requires minimal network configuration and simplifies network integration.

VM-Series for VMware ESXi (Stand-alone):

The VM-Series on ESXi servers is ideal for networks where the virtual form factor may simplify deployment and provide more flexibility. Common deployment scenarios include:

- Private or public cloud computing environments where virtualization is prevalent
- Environments where physical space is restricted and at a premium
- Remote locations where shipping hardware is not practical

The VM-Series for ESXi allows you to deploy safe application enablement policies that identify, control, and protect your virtualized applications and data. Panorama centralized management, and a rich set of APIs, can be used to integrate with external orchestration and management tools to collect information related to workload changes, which can then be used to dynamically drive policy updates via Dynamic Address Groups and VM Monitoring. A range of interface types, including L2, L3 and virtual wire, allow you to deploy the VM-Series for ESXi in a different interface mode for each virtualized server, depending on your needs.

VM-Series for VMware vCloud Air:

The VM-Series for vCloud® Air allows you to protect your VMware-based public cloud with the same safe application enablement policies that are used to protect your ESXi-based private cloud. Common use cases include:

- **Perimeter gateway:** In this use case, the VM-Series is deployed as your gateway firewall, securing your vCloud Air environment based on application, regardless of port and protocol, while preventing known and unknown threats and controlling access based on user identity.
- **Hybrid cloud security:** In this use case, the VM-Series is configured to establish a secure, standards-based IPsec connection between your private, VMware-based cloud and your vCloud Air-based public cloud. Access to the vCloud Air environment can then be controlled based on application and user identity.

- **Network segmentation:** Protect east-west traffic between subnets and application tiers using the application and the user identity as the basis for your security policies.

  Panorama centralized management, and a rich set of APIs can be used to integrate with external orchestration and management tools to collect information related to workload changes, which can then be used to dynamically drive policy updates via Dynamic Address Groups and VM Monitoring. The VM-Series for vCloud Air supports L3 network interface mode.

VM-Series for Citrix SDX

The VM-Series on Citrix® NetScaler SDX™ enables security and application delivery controller (ADC) capabilities to be consolidated on a single platform, delivering a comprehensive set of cloud-based services to enhance the availability, security and performance of applications. This integrated solution addresses the independent application needs for business units, owners and service provider customers in a multi-tenant deployment. In addition, this combined offering provides a complete, validated, security and ADC solution for XenApp® and XenDesktop® deployments. Please see the VM-Series for Citrix SDX solution brief for more information on this integration.

VM-Series for Amazon Web Services

The VM-Series for Amazon Web Services (AWS) enables you to protect public cloud deployments with our next-generation firewall and advanced threat prevention capabilities. Available as an Amazon Machine Interface (AMI), the VM-Series can be deployed as an EC2 instance to protect traffic flowing into and across your VPC. Panorama centralized management, and a rich set of APIs, can be used to integrate with external orchestration and management tools to collect information related to workload changes, which can then be used to dynamically drive policy updates via Dynamic Address Groups and VM Monitoring. Please see the VM-Series for AWS solution brief for more information on this integration.

VM-Series for KVM

The VM-Series for Kernel Virtual Machine (KVM) will allow service providers and enterprises alike to add next-generation firewall and advanced threat prevention capabilities to their Linux-based virtualization and cloud-based initiatives. KVM is a popular open-source hypervisor that will enable service providers and enterprises to deploy and manage the VM-Series across a range of Linux® operating systems, including CentOS/RHEL and Ubuntu®. In addition to the rich set of automation features and APIs within the VM-Series, the VM-Series for KVM can be managed using Panorama, along with the optional support for the OpenStack® plugin. Please see the VM-Series for KVM solution brief for more information on this integration.

Performance and Capacities [1]	VM-1000HV	VM-300	VM-200	VM-100
Firewall throughput (App-ID™ enabled)	1 Gbps			
Threat prevention throughput	600 Mbps			
IPsec VPN throughput	250 Mbps			
Max sessions per second	250,000	250,000	100,000	50,000

[1] Performance and capacities are measured under ideal testing conditions using PAN-OS® 7.0 and 4 CPU cores.

System Requirements	All VM-Series
CPU cores	2, 4 or 8
Memory (Min/Max)	4GB/5GB

Virtualization Specifications

Hypervisor Support

VM-1000HV

- 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)
- Citrix NetScaler SDX 11500, 17550 and 22000 Series
- KVM: CentOS/RHEL 6.5, Ubuntu Server 12.04 LTS, Open vSwitch: 1.9.3 LTS
- Amazon Web Services

VM-300 | VM-200 | VM-100

- VMware ESXi 5.1/5.5/6.0
- Citrix NetScaler SDX 11500 and 17550 Series
- KVM: CentOS/RHEL 6.5, Ubuntu Server 12.04 LTS, Open vSwitch: 1.9.3 LTS
- Amazon Web Services

Network Drivers

All VM-Series

- 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 supported on Intel 82576 based 1G NIC, Intel 82599 based 10G NIC, Broadcom 57112 and 578xx based 10G NIC
- **Amazon Web Services:** proprietary

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

pan-ds-vm-series-110215