VM-SERIES NEXT-GENERATION FIREWALL

Virtualization and cloud technologies are driving a data center transformation that melds on-premises resources with both private and public cloud resources. The VM-Series securely enables this transformation with the same next-generation firewall and advanced threat prevention features that protect your physical network.

The VM-Series Virtualized Next-Generation Firewall

- Delivers complete next-generation firewall security and advanced threat prevention to private, public and hybrid cloud computing environments.
- Supports a wide range of hypervisor and orchestration environments, including: VMware NSX, ESXi, vCloud Air, Microsoft Azure and Hyper-V Citrix NetScaler SDX, Amazon Web Services and KVM with optional support for the OpenStack plugin.
- Identifies and controls applications within your virtualized environments, limits access based on users, and prevents known and unknown threats.
- Enforces segmentation of applications and data to strengthen security and maintain compliance.
- Streamlines policy updates so that security keeps pace with the rate of change within your private, public or hybrid cloud.

Cloud Security Challenges: Public, Private and Hybrid

The benefits of implementing cloud technologies include greater agility, scalability, and an ability to be more responsive to your business. The benefits are well-known, but so too are the security challenges, which are no different from those you face within your on-premises data center. These challenges include a lack of application visibility and control, an inability to prevent cyberattacks, and cumbersome policy update processes that induce delays between workload deployment and security policy updates. To be successful, organizations need a cloud security solution that:

- Identifies and controls application workloads, regardless of the port it may use.
- Controls who should be allowed to use the applications, and grants access based on need and credentials.
- Extends security policy consistency from the network to the cloud to the remote device.
- Stops malware from gaining access to, and moving laterally (east-west) within the cloud.
- Simplifies management and minimizes the security policy lag as virtual workloads change.

The VM-Series supports the same next-generation firewall and advanced threat prevention features that are available in our security appliances, enabling you to protect your applications and data from the network to the cloud.

Are Native Security Features Sufficient?

Each of the public and private cloud environments provides users with basic security features that are typically port- and IP address-based. These features will help you protect your cloud deployment; however, they are looking at traffic from a ports-only perspective and cannot identify and control it at the application level. This only provides a base level of security to reduce your attack surface; it does not protect against external or lateral threats. As your cloud becomes an extension of your data center, advanced security features, such as those available from a next-generation firewall, should become a requirement.

The VM-Series: Protect Any Cloud

The VM-Series enables you to move toward a more agile data center that better supports your business and a cloud-first development methodology. Using the VM-Series in your cloud protects the resident applications and data with the same security posture that you may have established on your physical network with Palo Alto Networks® appliance-based firewalls.

The VM-Series natively analyzes all traffic in a single pass to determine the application identity, the content, and the user identity. These are key components in defining your security posture and management efforts, including visibility, policy control, reporting and incident investigation.

Application Visibility for Better Security Decisions

The VM-Series provides you with application visibility across all ports, which means you have far more relevant information about your Azure environment, which, in turn, means you can make more informed policy decisions.

Exert Greater Control with Whitelisting Policies

With the VM-Series, you can extend your firewall access control policies to the application level, forcing them to operate on specific ports, while leveraging the "deny all else" premise that a firewall is based on to block all others. The level of control becomes critically important as you deploy more of your data center assets in the public cloud.

User-Based Policies Improve Security Posture

Integration with a wide range of user repositories, such as Microsoft® Active Directory®, LDAP and Microsoft Exchange, introduces the user identity as a policy element, complementing application whitelisting with an added access control component. User-based policies mean you can grant access to critical applications and data based on user credentials and respective need. When deployed in conjunction with GlobalProtect™, the VM-Series for Azure enables you to extend your corporate security policies to mobile devices and users, regardless of their location.

Prevent Advanced Attacks at the Application Level

Attacks, much like many applications, are capable of using any port, rendering traditional prevention mechanisms ineffective. The VM-Series for Azure enables you to use the Threat Prevention and WildFire™ services to apply application-specific threat prevention policies that block exploits, malware, and previously unknown threats (APTs) from infecting your cloud.

Segmentation for Data Security and Compliance

Today's cyberthreats commonly compromise an individual workstation or user and then move laterally across your physical or virtualized network, placing your mission-critical applications and data at risk. Using security zones and whitelisting policies enables you to segment applications communicating across different subnets for tighter security and regulatory compliance. Enabling the Threat Prevention and WildFire services to complement your segmentation policies will block both known and unknown threats and stop them from moving laterally from workload to workload.

Centralized Management Delivers Policy Consistency

Panorama™ enables you to manage your VM-Series deployments across multiple cloud 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.

Automated Security Policy Updates to Support Cloud-First Initiatives

The VM-Series includes native management features that enable you to integrate security with your cloud-first development projects. A fully documented XML API and Dynamic Address Groups allow the VM-Series to consume external data in the form of tags that can be used to dynamically update your security policies as workloads are updated or change. The end result is that new applications can be deployed with baked-in security and automation.

Deployment Flexibility

The VM-Series can be deployed in a variety of hypervisor and orchestration environments. All of the security features described within this document are supported across each of the hypervisor environments.

VM-Series for VMware NSX

The VM-Series for VMware® 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. VM-Series for NSX supports multi-tenancy, along with multiple security policy sets and zones. NSX enables you to deploy the VM-Series in conjunction with any new workloads, thereby ensuring security keeps pace with the business. Changes to workloads are fed to Panorama and converted to tags, which are then used to dynamically drive policy updates.

The VM-Series for NSX supports open-vm-tools and virtual wire network interface mode, which requires minimal network configuration and simplifies network integration. Learn more about the **VM-Series for NSX**.

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 enables you to deploy safe application enablement policies that identify, control and protect your virtualized applications and data. The VM-Series for ESXi supports open-vm-tools along with a range of interface types, including L2, L3 and virtual wire. The interface types allow you to deploy the VM-Series for ESXi in a different interface mode for each virtualized server, depending on your needs. Learn more about the **VM-Series for ESXi**.

VM-Series for Microsoft Hyper-V

The VM-Series for Microsoft Hyper-V brings safe application enablement and advanced threat prevention capabilities to protect Microsoft Hyper-V based virtual infrastructure in private cloud environments. VM-Series for Microsoft Hyper-V includes support for Linux® integration services package for better integration with the hypervisor and visibility of virtual machine attributes. VM-Series can be deployed in different interface modes, including TAP, Layer 2, Layer 3 and virtual wire, depending on your needs.

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 multitenant deployment. In addition, this combined offering provides a complete, validated, security and ADC solution for Citrix XenApp® and XenDesktop® deployments. Learn more about the **VM-Series for Citrix**.

VM-Series for KVM

The VM-Series for Kernel-based 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®. Learn more about the **VM-Series for KVM**.

VM-Series for Amazon Web Services

The VM-Series for Amazon Web Services (AWS) enables you to protect your AWS deployment with our next-generation firewall and advanced threat prevention capabilities. Learn more about the **VM-Series for AWS**.

VM-Series for Azure

The VM-Series for Azure securely enables you to extend your applications built on the Microsoft stack (Windows Server, SQL Server, .NET Framework) into the public cloud. Learn more about the **VM-Series for Azure**.

VM-Series for VMware vCloud Air

The VM-Series for vCloud Air enables 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. Learn more about the **VM-Series for vCloud Air**.

VM-Series Specifications and Capacities

Virtualization specifications	
Hypervisors supported	**VM-1000-HV** • 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) • Microsoft Windows Server 2012 R2 with Hyper-V role • Microsoft Hyper-V Server 2012 R2 • Citrix NetScaler SDX 11500 and 17550 Series • KVM: CentOS/RHEL 6.5 & 7.0, Ubuntu Server 12.04 LTS & 14.04.02 LTS, Open vSwitch: 1.9.3 LTS • Amazon Web Services **VM-300 | VM-200 | VM-100** • VMware ESXi 5.1/5.5/6.0 • Microsoft Windows Server 2012 R2 with Hyper-V role • Microsoft Hyper-V Server 2012 R2 • Citrix NetScaler SDX 11500 and 17550 Series • KVM: CentOS/RHEL 6.5 & 7.0, Ubuntu Server 12.04 LTS & 14.04.02 LTS, Open vSwitch: 1.9.3 LTS • Amazon Web Services • Microsoft Azure
Network drivers	**All VM-Series** • VM-Series • VMware ESXi: VMXNet 3 • Microsoft Hyper-V Network Adaptor • Citrix NetScaler SDX: Igbvf version 2.0.4, Ixgbevf version 2.7.12 • KVM: virtIO, e1000, SR-IOV and PCI pass-through supported on Intel 82576-based 1G NIC, Intel 82599- based 10G NIC, Broadcom 57112 and 578xx-based 10G NIC • Amazon Web Services: proprietary • Microsoft Azure: proprietary

VM-Series Specifications and Capacities

Performance and capacities1	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	250,000	250,000	100,000	50,000
New sessions per second	8,000			

1 Performance and capacities are measured under ideal testing conditions using PAN-OS® 7.1 and 4 CPU cores.

System requirements	All VM-Series
CPU Cores	2, 4 or 8
Memory (Minimum)	4 GB
Disk drive capacity (Min/Max)	40 GB / 2 TB