VM-SERIES NEXT-GENERATION FIREWALL

Organizations worldwide are expanding their cloud and virtualization initiatives beyond traditional data center and public cloud deployments. New initiatives include security as an NFV component or as a more complete multi-tenancy solution.

The VM-Series Virtualized Next-Generation Firewall

Supports a wide range of cloud and virtualization environments including: VMware® NSX™, ESXi™, vCloud® Air™, Citrix® Netscaler® SDX™, Microsoft® Azure® and Hyper-V®, Amazon® Web Services and KVM with optional support for the OpenStack® plugin.

- Identify and control applications within your cloud or virtualized environment, limit access based on users, and prevent known and unknown threats.
- Isolate and segment mission-critical applications and data using Zero Trust principles.
- Streamline workflow automation to ensure that security keeps pace with the rate of change within your cloud.
- Centrally manage polices across both physical and virtualized firewalls to ensure a consistent security posture.

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 than those you face within your on-premise 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, allowing you to protect your applications and data from the network to the cloud.

Introducing the VM-Series

To help customers address the diverse cloud and virtualization use cases and the growing need for greater performance, the VM-Series has been optimized and expanded to deliver industry-leading performance of up to 16Gbps of App-ID enabled firewall throughput across five models. Customers can protect their cloud and virtualization initiatives with a security feature set that mirrors those protecting their physical networks and delivers a consistent security posture from the network to the cloud. The VM-Series models include:

- The **new** VM-50 is optimized to consume minimal resources yet deliver up to 200Mbps of App-ID enabled firewall performance for customer scenarios that range from virtual branch office/customer premise equipment (CPE) to high-density, multi-tenancy environments.
- The VM-100 and VM-300 have been optimized to deliver **2x and 4x of their existing** performance with 2Gbps and 4Gbps of App-ID enabled firewall performance for hybrid cloud, segmentation, and internet gateway use cases.
- The **new** VM-500 and VM-700 deliver an industry-leading 10Gbps to 16Gbps of App-ID enabled firewall performance respectively and can be deployed as NFV security components in fully virtualized data center and service provider environments.

The breadth of options and increased performance allow you to protect your applications and data with a consistent security posture from the network to the cloud.

The VM-Series: Protect Any Cloud

The VM-Series enables you to move toward a cloud-first deployment model that better supports your business. 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.

The VM-Series natively analyzes all traffic in a single pass to determine the application identity, the content and the user identity. The application, content within, and the user are used as core elements of your security policy and are also used for visibility, 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.

Segmentation/Whitelisting for Security and Compliance

Today's cyberthreats commonly compromise an individual workstation or user and then move laterally across your network, placing your mission-critical applications and data, regardless of location, at risk. Using segmentation and whitelisting policies allows you to control applications communicating across different subnets for tighter security and regulatory compliance. Enabling the Threat Prevention and WildFire™ cloud-based threat analysis service to complement your segmentation policies will block both known and unknown threats and stop them from moving laterally from workload to workload.

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™ network security for endpoints, 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 allows you to use Threat Prevention and WildFire to apply application-specific threat prevention policies that block exploits, malware and previously unknown threats (APTs) from infecting your cloud.

Centralized Management Delivers Policy Consistency

Panorama™ network security management 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.

Automate Security Deployment and Policy Updates

The VM-Series includes several management features that enable you to integrate security into your cloud-first development projects.

- Bootstrapping automatically provisions a firewall with a working configuration complete with licenses and subscriptions, and then auto-registers itself with Panorama.
- To automate policy updates as workloads change, a fully documented XML API and Dynamic Address Groups allow the VM-Series to consume external data in the form of tags that can drive policy updates dynamically.

As new applications and workloads are deployed, next-generation security can be deployed simultaneously in an automated manner, ensuring security keeps pace with the business.

Cloud-Centric Scalability and Availability

In any cloud or virtualization environment, scalability and availability requirements must be addressed using either a traditional data center approach or a cloud-centric approach. A cloud-centric approach leverages the existing cloud infrastructure services to address scalability and availability requirements. Utilizing existing application gateways and load balancer services on both AWS® and Azure allows the VM-Series to support both scalability and availability requirements necessary to support business critical applications.

Deployment Flexibility

The VM-Series can be deployed in a variety of cloud and virtualization 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 and VMware NSX to deliver on the promise of a software-defined data center. Learn more about the **VM-Series for NSX**.

VM-Series for VMware ESXi

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 environments where physical space is restricted and remote locations where shipping hardware is not practical. Learn more about the **VM-Series for ESXi**.

VM-Series for Microsoft Hyper-V

The VM-Series for Hyper-V securely enables applications deployed within your data center using Hyper-V. Learn more about the **VM-Series for Hyper-V**.

VM-Series for Microsoft 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 Amazon Web Services

The VM-Series on 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 on AWS**.

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. Learn more about the **VM-Series VM-Series for Citrix SDX**.

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 (CentOS/RHEL and Ubuntu®) virtualization and cloud-based initiatives. Learn more about the **VM-Series for KVM**.

VM-Series for VMware vCloud Air

The VM-Series for vCloud Air allows you to protect your VMware-based public cloud with the same secure application enablement policies that are used to protect your ESXi-based private cloud. Learn more about the VM-Series for **vCloud Air**.

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