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 offering.

The VM-Series Virtualized Next-Generation Firewall

Supports a wide range of cloud and virtualization environments, including VMware® NSX® and ESXi™, vCloud® Air™, Citrix® NetScaler® SDX™, Microsoft® Azure® and Hyper-V®, Amazon® Web Services, Google® Cloud 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 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, your organization needs cloud security that:

- Identifies and controls application workloads regardless of port.
- Controls who is 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 accessing and moving laterally, or 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 available in our hardware appliances, allowing you to protect your applications and data from the network to the cloud.

Introducing the VM-Series

To help customers address multiple clouds and the growing need for greater performance, the VM-Series has been optimized and expanded to deliver industry-leading performance of up to 16 Gbps 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 across all clouds and locations. The VM-Series models 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 office/customer-premises 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 an industry-leading 8 Gbps to 16 Gbps 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. These form 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, meaning you have far more relevant information about your cloud 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 Threat Prevention and WildFire® cloud-delivered malware analysis service to complement your segmentation policies will block both known and unknown threats, and stop them from moving laterally from workload to workload.

Improved Security Posture With User-Based Policies

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 enables you to extend your corporate security policies to mobile devices and users, regardless of their location.

Advanced Attacks Prevented at the Application Level

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

Mobile Network Infrastructure Security

The VM-Series supports a comprehensive set of software features designed specifically for mobile network operators. The SCTP Security and GTP Security features, available on all VM-Series models, provide comprehensive protection from attacks and signaling floods on RAN and roaming interfaces as well as significantly enhance application-layer protection and visibility across all mobile network peering points.

Consistent Policy Through Centralized Management

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 cohesion. Rich, centralized logging and reporting capabilities provide visibility into virtualized applications, users and content.

Container Protection Within GKE

The VM-Series on GCP protects containers running in Google Kubernetes® Engine with the same visibility and threat prevention capabilities that can be used to protect business-critical workloads on GCP. Container visibility empowers security operations teams to make informed security decisions and respond more quickly to potential incidents. Threat Prevention, WildFire and URL Filtering policies can be used to protect Kubernetes clusters from known and unknown threats. Panorama enables you to automate policy updates as Kubernetes services are added or removed, ensuring security keeps pace with your ever-changing GKE environment.

Automated 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 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.
- Build and operate secure cloud deployments with integration into native cloud services, such as Amazon Lambda and Azure, functions and automation tools, such as Ansible® and Terraform®, and many more.

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 takes advantage of the existing cloud infrastructure services to address scalability and availability requirements. Utilizing existing application gateways and load balancer services on AWS® and Azure allows the VM-Series to support 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 on VMware NSX

The VM-Series on NSX is a tightly integrated offering that ties together the VM-Series virtualized next-generation firewall, Panorama and VMware NSX to deliver on the promise of a software-defined data center. Learn more about the **VM-Series on NSX**.

VM-Series on 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 on ESXi**.

VM-Series on Microsoft Hyper-V

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

VM-Series on Microsoft Azure

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

VM-Series on Amazon Web Services

The VM-Series on 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 on Citrix NetScaler SDX

The VM-Series on Citrix NetScaler SDX enables security and application delivery controller capabilities to be consolidated on a single platform, including a comprehensive set of cloud-delivered services to enhance the availability, security and performance of applications. Learn more about the **VM-Series on Citrix SDX**.

VM-Series on Kernel Virtual Machine

The VM-Series on KVM will allow service providers and enterprises alike to add next-generation firewall and advanced threat prevention capabilities to their Linux-based (e.g., CentOS/RHEL and Ubuntu®) virtualization and cloud-based initiatives. Learn more about the **VM-Series on KVM**.

VM-Series on VMware vCloud Air

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

VM-Series on Google CloudPlatform

The VM-Series on Google Cloud Platform allows you to embed the VM-Series into your application development process to protect your applications and data while limiting business disruption. Learn more about the **VM-Series on Google Cloud Platform**.

VM-Series on Cisco ACI

The VM-Series on Cisco® ACI® enables automated insertion of Palo Alto Networks NGFW within an ACI deployment. Build dynamic security policies that are based on ACI attributes, such as Endpoint Groups, to achieve comprehensive protection. Learn more about the **VM-Series on Cisco ACI.**

VM-Series on OpenStack

The VM-Series on OpenStack® enables automated firewall service insertion within Mirantis® OpenStack deployments. The HEAT templates for the VM-Series user Juniper® Contrail® as the networking service and monitor OpenStack telemetry to auto-scale security. Learn more about the **VM-Series on OpenStack**.

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

© 2018 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at https://www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.