PRISMA
BY PALO ALTO NETWORKS

VM-Series Virtualized Next-Generation Firewall

VM-Series Virtualized Next-Generation Firewall

Protect applications and data deployed across a wide range of public cloud, virtualization, and NFV environments.

- Identify and control applications, grant access based on users, and prevent known and unknown threats.
- Segment mission-critical applications and data using Zero Trust principles to improve security posture and achieve compliance.
- Centrally manage policies across both physical and virtualized firewalls to ensure consistent security posture.
- Streamline workflow automation to ensure that security keeps pace with the rate of change in your cloud.

Organizations worldwide are executing digital transformation initiatives that are resulting in faster, more efficient network architectures that incorporate multiple public clouds, on-premises virtualized data centers, and, in some cases, security as a network functions virtualization (NFV) component.

The benefits of cloud, virtualization, and NFV technologies are well-known, and the risks of data loss and associated business disruption remain significant challenges. To protect your virtualized applications, workloads, and data, your organization needs cloud security that:

- Uses the application identity to enable segmentation and whitelisting.
- Controls resource access based on need and user identity.
- Prevents malware from gaining access and moving laterally from workload to workload.
- Simplifies management and can be fully automated to minimize friction as well as security policy lag as virtual workloads change.

Palo Alto Networks VM-Series Virtualized Next-Generation Firewalls support the same next-generation security and advanced threat prevention features available in our hardware firewalls, allowing you to protect your applications and data from the network to the cloud.

The VM-Series: Protect Any Cloud

Organizations are quickly adopting multi-cloud architectures as a means of distributing risk and taking advantage of the core competencies of different cloud vendors. To ensure your applications and data are protected across public clouds, virtualized data centers, and NFV deployments, the VM-Series has been designed to deliver up to 16 Gbps of App-ID-enabled firewall performance across five models:

- **VM-50/VM-50 Lite—**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 performance, respectively, for hybrid cloud, segmentation, and internet gateway use cases.
- **VM-500 and VM-700—**able to deliver an industry-leading 8 Gbps and 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.

Key VM-Series Features and Capabilities

The VM-Series protects your applications and data with next-generation security features that deliver superior visibility, precise control, and threat prevention at the application level. Automation features and centralized management allow you to embed security in your application development process, ensuring security can keep pace with the speed of the cloud.

- **Application visibility for informed security decisions:** The VM-Series provides application visibility across all ports, meaning you have far more relevant information about your cloud environment to help you make rapid, informed policy decisions.
- **Segment/Whitelist applications 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 at risk wherever they are. Using segmentation and whitelisting policies allows you to control applications communicating across different subnets to block lateral threat movement and achieve regulatory compliance.
- **Prevent advanced attacks within allowed application flows:** Attacks, much like many applications, can use any port, rendering traditional prevention mechanisms ineffective. The VM-Series allows you to use Palo Alto Networks Threat Prevention, DNS Security, and WildFire® to apply application-specific policies that block exploits, prevent malware, and stop previously unknown threats from infecting your cloud.
- **Control application access with user-based policies:** Integration with a wide range of user repositories—such as Microsoft Exchange, Active Directory®, and LDAP—complements application whitelisting with user identity as an added policy element that controls access to applications and data. When deployed in conjunction with Palo Alto Networks GlobalProtect™ for network security at the endpoint, the VM-Series enables you to extend your corporate security policies to mobile devices and users, regardless of their locations.
- **Policy consistency through centralized management:** Panorama™ provides centralized network security management for your VM-Series firewalls across multiple cloud 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.
- **Container protection for managed Kubernetes environments:** The VM-Series protects containers running in Google Kubernetes® Engine and Azure® Kubernetes Service with the same visibility and threat prevention capabilities that can protect business-critical workloads on GCP® and Microsoft Azure. 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 managed Kubernetes environments.
- **Automated security deployment and policy updates:** The VM-Series includes several management features that enable you to integrate security into your application development workflows.
    - Use bootstrapping to automatically provision a VM-Series firewall with a working configuration, complete with licenses, subscriptions, and connectivity to Panorama for centralized management.
    - Automate policy updates as workloads change, using a fully documented API and Dynamic Address Groups to allow the VM-Series to consume external data in the form of tags that can drive policy updates dynamically.
    - Use native cloud provider templates and services along with third-party tools—such as Terraform® and Ansible®—to fully automate VM-Series deployments and security policy updates.
- **Cloud-native scalability and availability:** In virtualization or cloud environments, scalability and availability requirements can be addressed using a traditional two-device approach or a cloud-native approach. In public cloud environments, we recommended using cloud services—such as application gateways, load balancers, and automation—to address scalability and availability.

Deployment Flexibility

To learn more about the public cloud and virtualization environments supported by the VM-Series, see the following resources:

Public Cloud

- VM-Series on Microsoft Azure/AzureStack
- VM-Series on Amazon Web Services
- VM-Series on Google Cloud Platform/GKE
- VM-Series on Oracle Cloud
- VM-Series on Alibaba Cloud
- VM-Series on VMware vCloud Air

Hybrid Cloud

- VM-Series on VMware Cloud (VMC) on AWS

Virtualized Data Center/Private Cloud

- VM-Series on VMware NSX for vSphere
- VM-Series on VMware ESXi
- VM-Series on Cisco ACI
- VM-Series on Microsoft Hyper-V
- VM-Series on KVM/Nutanix/OpenStack

PRISMA™
BY PALO ALTO NETWORKS

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

vm-series-summary-specsheet-ds-072919