VM-Series Virtual Next-Generation Firewalls

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.

Highlights

Protect applications and data deployed across a wide range of public, private, hybrid cloud, 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 virtual firewalls to ensure consistent security posture.
- Streamline workflow automation to ensure that security keeps pace with the rate of change in your cloud.

Overview

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 virtualized applications, workloads, and data, organizations need cloud security that:

- Uses the application identity to enable segmentation and allow specific access
- 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 and security policy lag as virtual workloads change

Palo Alto Networks VM-Series Virtual Next-Generation Firewalls deliver the same advanced security and threat prevention features as Palo Alto Networks hardware firewalls, providing comprehensive protection for applications and data from on-premises networks to the cloud. With Cloud-Delivered Security Services (CDSS) available, the VM-Series offers unmatched efficacy across a wide range of services, including Advanced Threat Prevention, Advanced WildFire®, Advanced DNS Security, and Advanced URL Filtering. This makes the VM-Series invaluable for organizations seeking to protect against today's advanced threats with the industry's most advanced software firewalls.

Protect Any Cloud

Organizations are quickly adopting public, private, and hybrid cloud architectures as a means of distributing risk and taking advantage of the core competencies of different cloud resources. To ensure your applications and data are protected across public clouds, virtualized data centers, and NFV deployments, the VM-Series virtual firewall has been designed to deliver industry-leading threat prevention capabilities at both the application and network layers across different vCPU configurations.

The VM-Series offers a flexible and unique consumption model, Software NGFW Credits, which allows you to match your virtual firewall performance, security services, and management requirements to the needs of your cloud infrastructure.

- Elastic throughput performance is achieved on the fly from 2 vCPUs to 64 vCPUs simply by adjusting the vCPUs requirements based on credits applied. Capacity is scaled to your exact virtual environment needs by choosing an appropriate memory profile.
- Cloud-Delivered Security Services are quickly applied, á la carte, specifically delivering targeted Zero Trust security, protecting your growing business.
- Apply credits to centralized VM Panorama® management and log collection or Strata™ Cloud Manager (SCM) for delivering consistent policy management and operational efficiency across your on-premises and multicloud deployments.

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 clouds, meaning you have far more relevant information about your cloud environment to help you make rapid, informed policy decisions.

"Segment/Allow" 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 granular security 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, similar to applications, can use any port, rendering traditional prevention mechanisms ineffective. The VM-Series allows native integration with our Cloud-Delivered Security Services, including core services for Advanced Threat Prevention, Advanced DNS Security, Advanced WildFire, and Advanced URL Filtering; as well as advanced security Enterprise DLP, IoT Security, and more. Applying application-specific policies affords your security team the ability to block exploits, prevent malware, and stop known and unknown threats from infecting your cloud applications.

Control application access with Zero Trust policies

Integration with a wide range of user repositories—such as Microsoft Exchange, Active Directory, and LDAP—complements applications with user identity as an added policy element in controlling 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 Zero Trust security policies to mobile devices and users, regardless of their locations.

Policy consistency through centralized management

Panorama or Strata™ Cloud Manager 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.

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 Panorama plugins to have your policies dynamically adjust based on tags in your public cloud environments.
- 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.
- 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.
- Security policy automation with VM ephemeral IP address mapping to Dynamic Address Groups based on application tag assignment.

Size and Scale Security Based on Immediate Needs—in Minutes

Match software firewalls and security services with the speed and flexibility needed for rapidly changing cloud requirements. Maximize the ROI on security investments with the industry's most flexible way to adopt software NGFWs and security services. Discover unmatched flexibility with easy scaling and sizing of VM-Series virtual NGFWs, Cloud-Delivered Security Services, and VM Panorama for management and log collection, or Strata Cloud Manager as the cloud-delivered management solution.

Three simple steps let you choose and deploy the right firewalls and security services you need at any given time:

1. Procure Software NGFW Credits.
2. Allocate or reallocate credits across different deployments to activate your choice of security products and your choice of security services in just minutes.
3. Manage and monitor credits via the Palo Alto Networks customer support portal.

As needs change over time, Software NGFW Credits can be reallocated to new and other firewall solutions without having to go through additional procurement cycles.

Deployment Flexibility

VM-Series virtual firewalls can be deployed on a variety of cloud and virtual networking security use cases.

Public Clouds

Public cloud security is the shared responsibility model where the CSP is responsible for security "of the cloud," and the customer is responsible for security "in the cloud." Virtual firewalls constantly address public cloud security requirements for operating systems, platforms, access, control, data, and more. Provide protection from known and unknown threats to meet security obligations in a cloud service provider's shared responsibility model, and maintain internal, industry, and government compliance. A platform approach with the VM-Series and public cloud architectures simplifies management and provides security scale at the speed of business. To leverage the VM-Series in public clouds, please look to the following major public cloud providers:

- Amazon Web Services
- Google Cloud
- Microsoft Azure
- Oracle Cloud
- Alibaba Cloud

Private Clouds and Virtual Data Centers

Virtual firewalls solve key security use cases and challenges in private cloud environments. Virtual firewalls, deployed strategically throughout a virtualized, private cloud environment, create trust zones based on an organization's risk profile and tolerance level. Critical applications are placed in their own trust zones, with Threat Prevention services turned on to inspect traffic to and from applications. Sensitive data subject to compliance standards is enclosed in other segmentation or microsegmentation zones to protect against lateral movement and enforce security measures required for compliance.

Hypervisors

- VMware ESXi
- KVM
- Nutanix AHV
- Microsoft Hyper-V
- OpenStack

Software-Defined Networking Solutions

- VMware NSX (NSX for vSphere and NSX-T)
- Cisco ACI
- Nutanix Flow

Hybrid and Multicloud

Virtual firewalls deployed in multicloud and hybrid environments can all still be managed from the same console. This lets security teams deliver the same best-in-class security capabilities to each environment and extend a uniform policy model across the entire ecosystem to ensure consistency and complete visibility that simplifies your overall security posture.

Cloud Migration

Lift-and-shift of traditional applications, migrating them to the cloud, and securing them on-premises to any cloud.

Cloud-Native Workload

Secure born-in-the-cloud SaaS services that are developed, deployed, and operated in the cloud.

Software-Defined Branches

Virtual firewalls can be deployed on existing servers in branch locations, typically called universal customer premise equipment (uCPE), avoiding the need for additional hardware. This allows security teams to create a single security policy to enforce required segmentation and intrusion prevention to protect the security of data as required by any applicable regulatory compliance requirements. The organization can centrally manage its distributed branch security, using the same management console that controls security for its data center, private cloud, and public cloud networks.

Secure SD-WAN

Virtual firewalls can be used to build a hub-and-spoke SD-WAN deployment between branch locations, the core data center, public cloud environments, and SaaS applications. For small or regional deployments, virtual NGFWs can run SD-WAN in a mesh architecture, connecting to each other without the need for a hub.

Protecting Critical Infrastructure

- Rugged Network Components from Siemens for Harsh Environments with a Built-in Security Platform with VM-Series & Siemens RUGGEDCOM Multi-Service Platform
- Secure Operational Technology (OT) Networks and Enhance the Resilience of Network Communications Between Substations, Control Centers, and Renewable Energy Plants with VM-Series & SEL Computing Platforms

- Purpose-Built Critical Infrastructure Networking Platform with VM-Series Virtual Next-Generation Firewall & iS5 Communications RAPTOR
- Seamless Protection at the Edge: Virtualized Cybersecurity with Zero Downtime with VM-Series & Stratus ztC Edge

Mobile 5G Network Security

Virtual firewalls with 5G-native security help organizations safeguard their networks, customers, and clouds, and extend Zero Trust to their 5G environments. 5G-native security supports all key mobile infrastructure environments—including on-premises, virtual, and containerized—across public and private telco clouds, and multi-access edge compute (MEC) environments with machine learning (ML)-powered NGFWs.

Virtual Desktop Infrastructure Security

Virtual firewalls deployed at the edge of the VDI environment ensure that virtual desktops are properly segmented and traffic is inspected appropriately.

Unique Networks Security Technical Partner Use Cases

- Unprecedented Performance and Efficiency Gains for Next-Generation Firewalls with VM-Series & NVIDIA BlueField-2 DPU
- Improve Network Security by Deploying High-Performance Virtual Firewalls Quickly and Easily with VM-Series & Megaport Virtual Edge (MVE)
- Auto-Scale Multi-Cloud Security and Simplify Provisioning to Meet Real-Time Demand with VM-Series & Alkira Cloud Services Exchange
- Transform On-Premises Firewalls to Virtual VM-Series Instances with Speed, Simplicity, and Savings with VM-Series & Corsa Security Orchestrator
- Partner-Qualified Products with Which VM-Series Virtual Firewalls Interoperate with VM-Series & Aryaka SmartSecure Hosted VM Firewall Service

Compatibility, Capacity, and Performance

See VM-Series Hypervisor Support for the full list of the supported public clouds and hypervisors.

See Partner Interoperability for the list of supported third-party platforms.

For full capacity specifications, visit Compare VM-Series Performance Details.

Performance varies across different hypervisors and cloud environments. Refer to environment-specific datasheets for associated performance. For full performance specifications, visit Compare VM-Series Performance Details.

For more information about the capacities of the VM-Series firewall models, see the Palo Alto Networks Next-Generation Firewalls comparison tool.

Resources

- Get started with a free trial of our VM-Series Virtual Next-Generation Firewalls on AWS, Azure, ESXi, or KVM.
- Join the Virtual Ultimate Test Drive to get hands-on experience with the VM-Series Virtual Next-Generation Firewalls. This customized virtual workshop is designed to enhance understanding and cater to every experience level.
- Check out the Software Firewalls Credit Estimator to calculate the number of NGFW Credits needed for specific security requirements.
- Explore the Software Firewall Selector to discover the optimal security solution for your cloud-based or virtual environment.

About This Datasheet

The information provided with this paper that concerns technical or professional subject matter is for general awareness only, may be subject to change, and does not constitute legal or professional advice, nor warranty of fitness for a particular purpose or compliance with applicable laws.

paloalto 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

strata_ds_vm-series-virtual-next-generation-firewalls_082124