VM-Series Virtual 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 virtual firewalls to ensure consistent security posture.
- Streamline workflow automation to ensure that security keeps pace with the rate of change in your cloud.

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.

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 allow listing.
- 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 Virtual 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 virtual firewall has been designed to deliver industry leading throughputs at the application and network layers across different vCPU configurations.

VM-Series offers the industry's most 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 32 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 delivering consistent policy management and operational efficiency across your on-premises and multi-cloud 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 ports, 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 allow listing 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 native integration with our cloud-delivered subscription services, such as 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 allow listing 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 Google Cloud 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.

Intelligent Traffic Offload Service for Service Providers

In service provider networks and hyperscale data centers, roughly 80% of traffic consists of traffic that cannot or will not benefit from security inspection. Deploying enough large firewalls to secure these enormous networks without sacrificing performance can make security costs prohibitive.

The Intelligent Traffic Offload Service eliminates these tradeoffs. The service integrates with smart network interface cards (Smart NICs) to offload traffic that does not benefit from security inspection to the Smart NIC, reducing CAPEX by up to 150%.

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.

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 your 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 and CN-Series container NGFWs, cloud-delivered Security Services, and VM Panorama for management and log collection.

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-as-a-platform solutions without having to go through additional procurement cycles.

Deployment Flexibility

VM-Series virtual firewalls can be deployed on a variety of public clouds and hypervisors:

- **Public Clouds**
  - » Amazon Web Services
  - » Google Cloud
  - » Microsoft Azure
  - » Oracle Cloud
  - » Alibaba Cloud
- **Hypervisors**
  - » VMware ESXi
  - » KVM
  - » Nutanix AHV
  - » Microsoft Hyper-V
- **Software-Defined Networking Solutions**
  - » VMware NSX (NSX for vSphere and NSX-T)
  - » Cisco ACI
  - » Nutanix Flow

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.

Table 1: VM-Series Capacity Details by Memory Allocation					
Memory (min)	**5.5 GB**	**6.5 GB**	**9 GB**	**16 GB**	**56 GB**
Sessions	64,000	250,000	819,200	2,000,000	10,000,000
Security Rules	250	1,500	10,000	10,000	20,000
Dynamic IP Addresses	2,500	5,000	10,000	32,000	100,000
Security Zones	15	40	40	200	200
IPsec VPN Tunnels	250	1,000	2,000	4,000	8,000
SSL VPN Tunnels	40	100	400	1,200	2,500

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

Table 2: VM-Series Throughput by vCPU					
VM-Series vCPUs configured	**4 vCPU**	**5 vCPU**	**8 vCPU**	**16 vCPU**	**22 vCPU**
APP-ID throughput	6Gbps	6Gbps	12Gbps	19Gbps	28Gbps
Threat Prevention throughput	3Gbps	4Gbps	6Gbps	13Gbps	15Gbps

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

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

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