STRATA™
BY PALO ALTO NETWORKS

VM-Series on Azure

- Complements native Azure security with application enablement policies that prevent threats and data loss.
- Allows you to transparently embed security in the application development process through automation and centralized management.
- Enables scale-out and high availability through integration with Azure Application Gateway and Azure Load Balancer.
- Cost-effectively protects large scale deployments with a Transit VNet architecture.

VM-Series on Microsoft Azure

Palo Alto Networks VM-Series Virtual Next-Generation Firewalls protect your Microsoft Azure® workloads with next-generation security features that allow you to confidently and quickly migrate your business-critical applications to the cloud. Azure Resource Manager (ARM) templates and third-party automation tools allow you to embed the VM-Series in your application development lifecycle to prevent data loss and business disruption.

Microsoft Azure migration initiatives are rapidly transforming data centers into hybrid clouds, yet the risks of data loss and business disruption jeopardize adoption. The VM-Series on Azure solves these challenges, enabling you to:

- Protect your Azure workloads through unmatched application visibility and precise control.
- Prevent threats from moving laterally between workloads and stop data exfiltration.
- Eliminate security-induced application development bottlenecks with automation and centralized management.

Azure Network Security Groups or VM-Series?

Organizations are migrating their enterprise applications onto Azure for many reasons, including business agility and a desire to reduce data center footprints. Security best practices dictate that your public cloud security posture should be as strong as your data center security approach: understand your threat exposure through application visibility, use policies to reduce your attack surface area, and prevent threats and data exfiltration within allowed traffic.

Native Azure security features perform port-based filtering to control access to the Azure resources deployed. They are unable to use the application identity to control traffic nor can they prevent threats within the content allowed. The VM-Series complements Azure Network Security Groups and Azure Firewall security controls by reducing your attack surface through enabling applications regardless of port, preventing threats, and stopping data exfiltration.

The VM-Series on Azure allows you to embrace a prevention-based approach to protecting your applications and data on Azure. Automation and centralized management features enable you to embed next-generation security in your Azure application workflow so security can keep pace with development.

- **Complete visibility improves security decisions**. Understanding the applications in use on your network, including those that may be encrypted, helps you make informed security policy decisions.
- **Segmentation and application whitelisting aid data security and compliance**. Using application whitelisting to enforce a positive security model reduces your attack surface. Whitelisting policies also allow you to segment applications that communicate across subnets and between virtual networks (VNets) to stop lateral threat movement and meet compliance requirements.
- **User-based policies improve security posture**. Integration with on-premises user repositories, such as Microsoft Exchange, Active Directory®, and LDAP, lets you grant access to critical applications and data based on user credentials and needs. For example, your developer group can have full access to the developer VNet while only IT administrators have RDP/SSH access to the production VNet. When deployed in conjunction with Palo Alto Networks GlobalProtect™ network security for endpoints, the VM-Series on Azure can extend your corporate security policies to mobile devices and users regardless of their location.
- **Applications and data are protected from known and unknown threats**. Attacks, like many applications, can use any port, rendering traditional prevention mechanisms ineffective. Enabling Palo Alto Networks Threat Prevention, DNS Security, and WildFire® malware prevention service as segmentation policy elements will protect you against exploits, malware, and previously unknown threats from both inbound and lateral movement perspectives.
- **Multiple defenses block data exfiltration and unauthorized file transfers**. A combination of application enablement, Threat Prevention, and DNS Security features can prevent data exfiltration. File transfers can be controlled by looking inside files, not only at file extensions, to determine whether transfer actions should be allowed. Command and control, associated data theft, and executable files found in drive-by downloads or secondary payloads can also be blocked. Data filtering features can detect and control the flow of confidential data patterns, such as credit card and Social Security numbers, in addition to custom patterns.

Centralized Management Delivers Policy Consistency

Panorama™ network security management provides centralized administration for your VM-Series firewalls across multiple cloud deployments alongside your physical appliances, ensuring consistent and cohesive policy. Rich, centralized logging and reporting capabilities provide deep visibility into virtualized applications, users, and content.

Panorama comprises Panorama Manager and the Log Collector, allowing you to centrally manage your VM-Series firewalls in a distributed manner. Panorama Manager and the Log Collector can be deployed on Azure or on-premises using VM-Series dedicated appliances. Alternatively, you can deploy both Panorama components on Azure, or in a hybrid scenario, with Panorama Manager deployed on-premises and the Log Collector deployed on Azure. You can also use Panorama in conjunction with Cortex™ Data Lake.

Automation to Support App Dev Workflows

The VM-Series on Azure includes management and automation features that enable you to embed security in your application development workflow:

- Bootstrapping can automatically provision a VM-Series with a working configuration, complete with licenses and subscriptions, and then auto-register with Panorama.

- A fully documented XML API, Dynamic Address Groups, and External Dynamic Lists allow you to automate VM-Series configuration changes and consume external data to dynamically drive security policy updates.
- Action-Oriented Log Forwarding lets you drive actions based on observed incidents in the logs. In conjunction with Azure ARM Templates or third-party tools, you can deploy next-generation security at the speed of the cloud.

Automated Policy Updates with a Tag-Based Policy Model

The VM-Series leverages the native tags from Azure in the formulation of network security policies. By basing policies on native Azure infrastructure tags, rather than static attributes such as port or IP address, VM-Series policies can dynamically update as new workloads are created, moved, or deprecated.

Automating Deployments with Terraform and Ansible

If your organization uses multiple public and private cloud platforms, or you want to embed VM-Series deployments in your application development processes, you can deploy and configure the VM-Series using third-party tool sets, such as Terraform® and Ansible®. The combination of these tools and VM-Series automation features enables you to deploy and configure heterogeneous environments at scale with great agility.

Active Health Monitoring with Application Insights

You can send VM-Series metrics to Azure Application Insights as a means of monitoring the capacity, health status, and availability of your firewall, along with other resources in your Azure deployment. VM-Series metrics can be used to trigger actions such as webhooks or Azure Functions when Application Insights detects that a metric has exceeded a user-defined threshold. Internal metrics that can be sent to Application Insights include:

- Session utilization %
- Total active sessions
- Dataplane CPU utilization %
- Dataplane packet buffer utilization %
- SSL proxy utilization %
- GlobalProtect active tunnels
- GlobalProtect tunnel utilization %

VM-Series on Azure High Availability

Network infrastructure best practices dictate that you ensure your business-critical applications achieve maximum uptime, using high availability regardless of their deployment location. The VM-Series on Azure supports either a traditional two-device, active/passive approach or a more cloud-centric approach.

Active/Passive High Availability

If you're executing a "lift and shift" data center migration to Azure, you may want to use a two-device, active/passive approach to high availability. In this scenario, two VM-Series firewalls are deployed on Azure using Availability Sets within a resource group. Both VM-Series firewalls will be configured with secondary, floating IP addresses that can be moved programmatically to the passive firewall in the event of a failure.

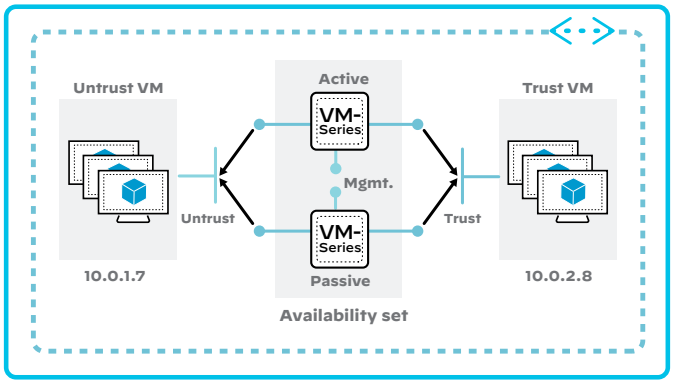

Figure 1: VM-Series active/passive high availability on Azure

Cloud Native High Availability

For an Azure deployment taking a cloud native approach, you can use a "load balancer sandwich" to achieve both high availability and managed scale. In this scenario, an Application Gateway acts as the external load balancer, distributing traffic across multiple VM-Series firewalls within an Availability Set while also front-ending the web application and serving as an internet gateway. After inspection by the VM-Series, traffic is routed to the Azure Load Balancer acting as the internal load balancer, which distributes traffic to the web applications. If a VM-Series or other element fails, the load balancers will reroute traffic to its destination automatically.

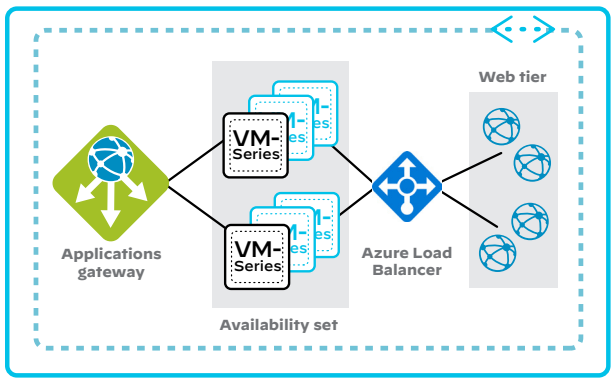

Figure 2: High availability and managed scale on Azure with a "load balancer sandwich"

Scaling the VM-Series on Azure

Scalability on Azure can be defined and addressed in two ways. To protect large or rapidly growing Azure deployments that may consist of many subscriptions or resource groups, organizations are taking a shared services approach by using a Transit VNet architecture. In deployments where inbound web application traffic may fluctuate rapidly, auto scaling can be used to dynamically deploy or remove resources as traffic patterns increase and decrease. The VM-Series can be deployed in both scalability scenarios.

Transit VNet with the VM-Series

A Transit VNet centralizes security into a shared services hub, allowing you to provide cost-effective, secure connectivity from your Azure deployment to your data center, outbound to the web, or for VNet-to-VNet communications. In a hub-and-spoke architecture, each spoke will "subscribe" to and transit the hub for secure connectivity. New spokes can be quickly be added to the hub, allowing your development team to work at the speed of the cloud. A VM-Series can be deployed within an individual spoke to address the need for secure inbound or outbound connectivity (directly to App1 or App2).

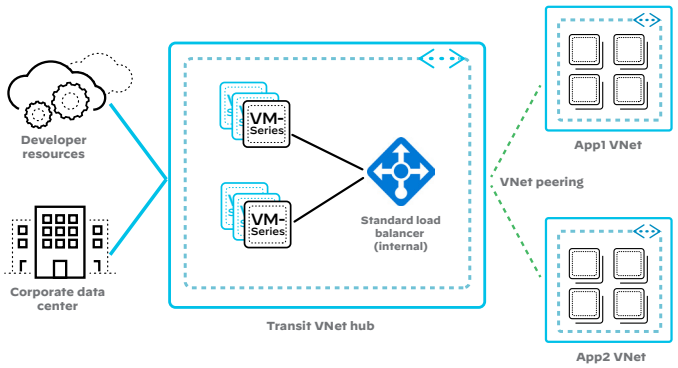

Figure 3: Using a Transit VNet architecture to cost effectively protect many VNets

Auto Scaling the VM-Series

In deployment scenarios where inbound web traffic may fluctuate dramatically, auto scaling can automatically deploy and remove new resources, including the VM-Series firewall, resulting in a cost-effective, efficient use of your Azure resources.

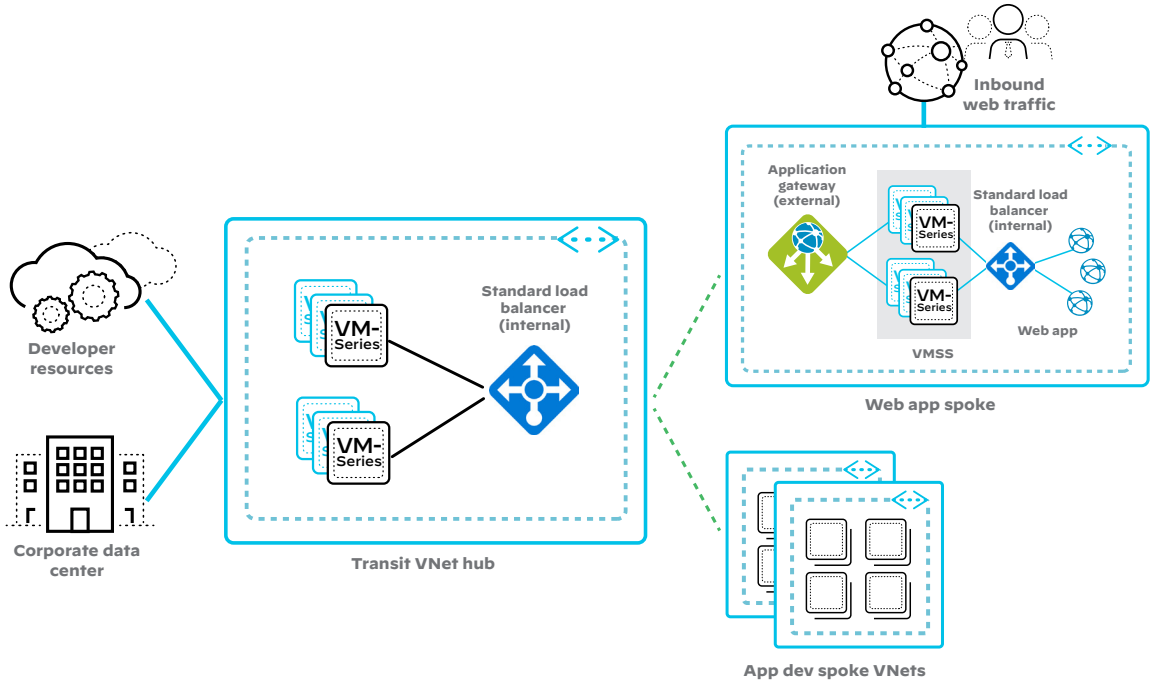

Figure 4: Auto scaling the VM-Series on Azure within a Transit VNet

Deployed as a spoke in a Transit VNet architecture, auto scaling uses Azure Application Gateways, Load Balancing, and Application Insights to automatically deploy new VM-Series firewalls within Virtual Machine Scale Sets (VMSSs) based on a user-defined traffic metric, such as maximum number of sessions.

VM-Series on Azure Use Cases

The VM-Series can be deployed on Azure to address several different use cases.

Hybrid Cloud: Securely Enable App Dev and Test

Securely migrate application development and testing to Azure through a hybrid deployment that integrates your existing development environment with Azure via a secure connection. This allows your development and testing teams to get started while maintaining a strong security posture. Deployed on Azure, the VM-Series can act as an IPsec virtual private network (VPN) termination point to enable secure communications to and from Azure. You can also layer application control and Threat Prevention policies atop the IPsec VPN tunnel or Azure Express Route as added security elements.

Segmentation Gateway: Separation for Security and Compliance

High-profile breaches have shown that cybercriminals are adept at hiding in plain sight, bypassing perimeter controls, and moving at will across networks, physical or virtualized. An Azure VNet provides an isolation and security boundary for your workloads. The VM-Series can augment that separation through application-level segmentation policies to control traffic between VNets and across subnets. With application-level policies, you have greater control over application traffic moving laterally, and you can apply Threat Prevention policies to block their movement.

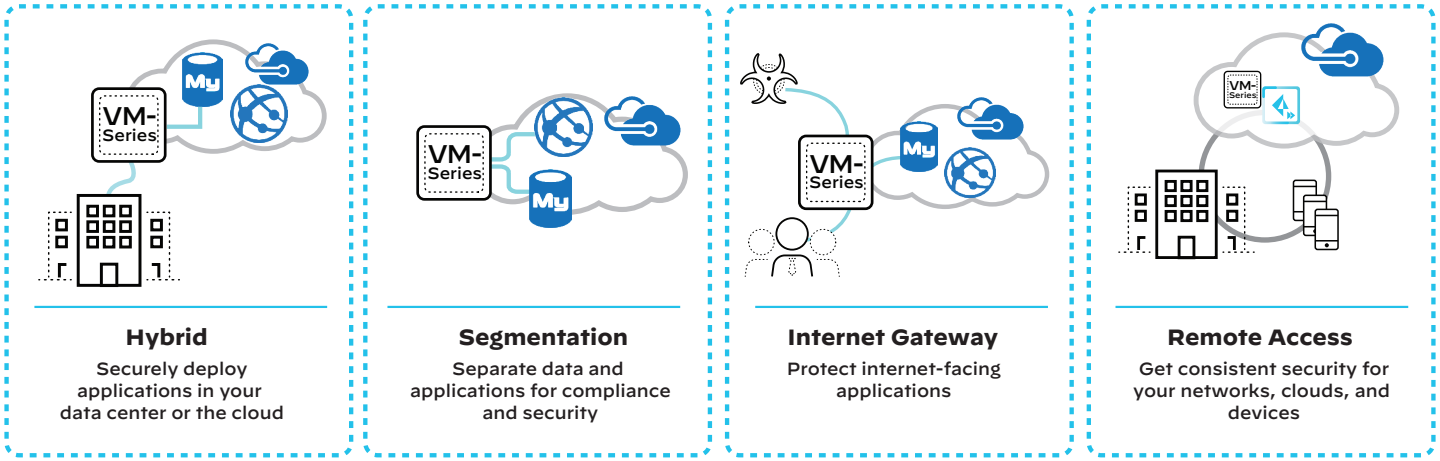

Figure 5: VM-Series on Azure use cases

Internet Gateway: Protect Production Workloads

You can use the VM-Series on Azure as an internet gateway to protect web-facing applications from known and unknown threats. Additionally, you can enable direct access to web-based developer resources, tools, and software updates, thereby minimizing the traffic that flows back to corporate and out to the web.

Remote Access: Extend Security to Users and Devices

GlobalProtect enables you to extend perimeter security to your remote users and mobile devices wherever they are. GlobalProtect establishes a secure connection to protect users from internet threats and enforces application-based access control policies. Whether accessing the internet, the data center, or SaaS applications, users will enjoy the full protection of the VM-Series.

VM-Series on Azure for Government

The VM-Series can be deployed directly from the Azure Government Marketplace to support each of the scenarios described, using any of the licensing options.

Licensing and Deployment

The VM-Series on Azure supports several licensing options, including pay-as-you-go (PAYG) licensing via the Azure Marketplace as well as a bring-your-own-license (BYOL) model. We also offer a VM-Series BYOL enterprise license agreement (ELA).

PAYG

Use your Azure Management Console to purchase and deploy VM-Series hourly subscription bundles directly from the Azure Marketplace.

- **Bundle 1 contents**: Base VM license, Threat Prevention (inclusive of IPS, AV, malware prevention) subscription, and Premium Support (in written and spoken English only).
- **Bundle 2 contents**: Base VM license, Threat Prevention (inclusive of IPS, AV, malware prevention), DNS Security, WildFire, URL Filtering, and GlobalProtect subscriptions, with Premium Support (in written and spoken English only).

BYOL

Purchase your VM-Series license through normal Palo Alto Networks channels, and then deploy the VM-Series using the Azure Management Console and the license authorization code you received.

VM-Series BYOL ELA

For large-scale deployments on Azure or across multiple virtualization environments, the VM-Series BYOL ELA allows you to forecast, and purchase upfront, the VM-Series firewalls to be deployed over a one- or three-year period. The VM-Series BYOL ELA gives you a single license authorization code to use for the life of the term, providing predictable security spend and simplifying the licensing process by establishing a single start and end date for all VM-Series licenses and subscriptions. Each VM-Series BYOL ELA includes a VM-Series firewall, Threat Prevention, DNS Security, URL Filtering, WildFire, and GlobalProtect Gateway, plus unlimited Panorama virtual machine licenses and Premium Support (in written and spoken English only).

Performance and Capacities

For information on VM-Series performance and capacities on Azure VM sizes, please visit our technical documentation.

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