VM-Series on Alibaba Cloud

VM-Series on Alibaba Cloud

- Complements native Alibaba Cloud security with application visibility, precise control, and segmentation.

- Prevents threats and data loss within allowed application flows.

- Enables policies to be updated at the speed of the cloud through automation.

- Ensures policy consistency with centralized management in Panorama.

Introduction

Organizations are using Alibaba Cloud infrastructure to accelerate their business expansion into mainland China and across Asia. Potentially slowing these initiatives are the risks of data loss and business disruption. The VM-Series on Alibaba Cloud solves these challenges, enabling you to:

- Protect your workloads deployed on Alibaba Cloud 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.

Palo Alto Networks VM-Series Virtualized Next-Generation Firewalls protect your workloads with next-generation security features that allow you to confidently and quickly migrate your business-critical applications to the cloud. Templates and third-party tools allow you to embed the VM-Series into your application development lifecycle to prevent data loss and business disruption.

Native Alibaba Cloud Security or VM-Series?

Security best practices dictate that your public cloud security posture should mimic your data center security approach: understand your threat exposure through application visibility, use policies to reduce the attack surface area, and then prevent threats and data exfiltration within the allowed traffic. Native Alibaba Cloud security functions enable you to establish a baseline of protection and control, but today's attackers are adept at hiding in plain sight to accomplish their goals. The VM-Series complements native Alibaba Cloud security by reducing your attack surface through enabling applications, preventing threats, and stopping data exfiltration.

VM-Series on Alibaba Cloud

The VM-Series allows you to embrace a prevention-based approach to your applications and data on Alibaba Cloud.

- **Complete visibility improves security decisions.** Understanding which applications are 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 by allowing specific applications that align to your organization's needs. Whitelisting policies also allow you to segment applications that communicate across subnets and between Alibaba Cloud's Virtual Private Cloud (VPC) 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 need. For example, your developer group can have full access to the developer replace with VPC while only IT administrators have RDP/SSH access to the production ECS. When deployed in conjunction with Palo Alto Networks GlobalProtect™ for network security on endpoints, the VM-Series on Alibaba Cloud 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 Threat Prevention and WildFire®, Palo Alto Networks 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.** Data exfiltration can be prevented using a combination of application enablement and Threat Prevention. File transfers can be controlled by looking inside files, not only at their 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 for Policy Consistency

Panorama™ enables you to centrally manage 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.

Automation to Support App Dev Workflows

The VM-Series on Alibaba Cloud includes management and automation features that enable you to embed security into your application development workflow. A fully documented API, Dynamic Address Groups, and External Dynamic Lists allow you to consume external data to dynamically drive security policy updates. Bootstrapping is not supported in this release.

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 toolsets, 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.

VM-Series on Alibaba Cloud Use Cases

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

Hybrid Cloud: Securely Enable App Dev and Test

Securely migrate application development and testing to Alibaba Cloud through a hybrid deployment that integrates your existing development environment with Alibaba Cloud via a secure connection. This allows your development and testing teams to get started while maintaining a strong security posture. Deployed on Alibaba Cloud, the VM-Series can act as an IPsec virtual private network (VPN) termination point to enable secure communications to and from Alibaba Cloud.
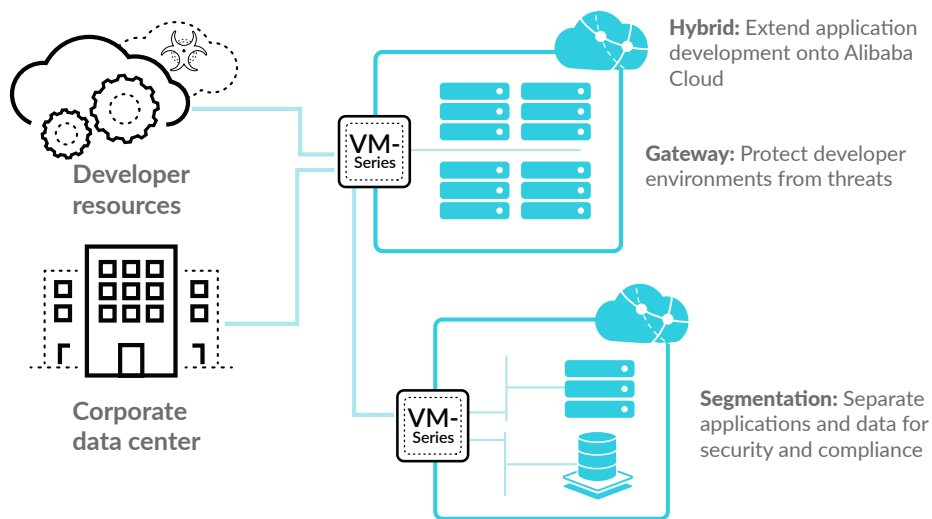

Figure 1: VM-Series on Alibaba Cloud use cases

Internet Gateway: Protect Production Workloads

As your Alibaba Cloud deployment expands to include public-facing workloads, you can use the VM-Series 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.

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 Alibaba Cloud VPC 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 ECSs 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. If traffic is flowing between ECSs in different regions across the internet, you can enable encryption for added protection.

Licensing and Deployment

The VM-Series firewall on Alibaba Cloud is deployed using the PAN-OS® 8.1.3 VM-Series KVM base image licensed through either the bring-your-own-license model or a VM-Series Enterprise Licensing Agreement (ELA).

- **Bring your own license:** Purchase Bundle 1 or 2 through your normal Palo Alto Networks channels, and then deploy the bundle using the license authorization code delivered to you via email.

  Bundle 1 contents: VM-300 firewall license, Threat Prevention (inclusive of IPS, AV, malware prevention) subscription, and Premium Support (written and spoken English only).

  Bundle 2 contents: VM-300 firewall license, Threat Prevention (inclusive of IPS, AV, malware prevention), WildFire, URL Filtering, and GlobalProtect subscriptions, with Premium Support (written and spoken English only).

- **VM-Series ELA:** For large-scale and/or multi-cloud deployments or across multiple virtualization environments, the VM-Series ELA allows you to forecast, and purchase upfront, VM-Series firewalls to be deployed over a one- or three-year period. The VM-Series 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 with a single start and end date for all VM-Series licenses and subscriptions. Each VM-Series ELA includes a VM-Series firewall, subscriptions for Threat Prevention, URL Filtering, WildFire, and GlobalProtect Gateway, plus unlimited Panorama virtual machine licenses and Premium Support (written and spoken English only).

Performance and Capacities

Model[1]	VM-50/ VM-50 Lite[2]	VM-100/ VM-200	VM-300/ VM-1000-HV	VM-500	VM-700
Alibaba Cloud instance size tested (recommended)[2]	N/A				
Firewall throughput (App-ID enabled)	N/A				
Threat Prevention throughput	N/A		Performance testing is in progress		
IPsec VPN throughput	N/A				
All instance sizes supported	N/A				
New sessions per second	N/A				
Max sessions	N/A				
System Requirements					
Cores supported (min/max)	N/A	0.4/2	2/4	2/8	2/16
Memory (min)	N/A	6.5 GB	9 GB	16 GB	56 GB
Disk drive capacity (min)	N/A	32 GB	60 GB	60 GB	60 GB
Recommended instance sizes[3]	N/A	ecs.g5.xlarge	ecs.g5.xlarge	ecs.g5.2xlarge	ecs.g5.4xlarge
Licensing options	N/A	BYOL or VM-Series ELA	BYOL or VM-Series ELA	BYOL or VM-Series ELA	BYOL or VM-Series ELA

1. VM-Series on Alibaba Cloud uses the VM-Series on KVM base image (PAN-OS 8.1.3 and above)
2. The VM-50 and VM-50 Lite are not supported on Alibaba Cloud
3. Refers to recommended Alibaba Cloud instance based on CPU cores, memory, and pricing

---

PRISMA
BY PALO ALTO NETWORKS