STRATA™
BY PALO ALTO NETWORKS

## VM-Series on AWS

- Complements native AWS 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 security to scale dynamically yet independently of your workloads through integration with AWS Auto Scaling and Elastic Load Balancing.
- Cost-effectively protects deployments with many VPCs through a transit VPC architecture.

# VM-Series on AWS

Palo Alto Networks VM-Series Virtual Next-Generation Firewalls protect your Amazon Web Services (AWS®) workloads with next-generation security features that allow you to confidently and quickly migrate your business-critical applications to the cloud. AWS CloudFormation 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.

As AWS becomes the dominant deployment platform for your business-critical applications, protecting the increased public cloud footprint from threats, data loss, and business disruption remains challenging. The VM-Series on AWS solves these challenges, enabling you to:

- Protect your AWS 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.

## AWS Security Groups or VM-Series?

Organizations are migrating their enterprise applications on AWS for many reasons, including business agility and a desire to reduce data center footprints. In nearly all cases, the AWS deployment is connected to the corporate network, making the AWS resources network-accessible by users—and possibly attackers. Security best practices dictate that your public cloud security posture should mimic your data center security approach: understand your threat exposure through application visibility; usepolicies to reduce the attack surface area; and then prevent threats and data exfiltration within the allowed traffic.

AWS Security Groups perform port-based filtering to control access to the AWS resources deployed, and they must be enabled for the cloud deployment to be operational. The VM-Series complements AWS Security Groups port-based controls by reducing your attack surface through application enablement, preventing threats, and stopping data exfiltration.

## VM-Series on AWS

The VM-Series allows you to embrace a prevention-based approach to protecting your applications and data on AWS. Automation and centralized management features enable you to embed next-generation security in your AWS application workflow, enabling security to 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 Allow Listing Aid Data Security and Compliance

Using application allow listing to enforce a positive security model reduces your attack surface by allowing specific applications that align to your organization's needs (e.g., allow SharePoint® documents for all, but limit SharePoint administration access to the IT group). Allow listing policies also allow you to segment applications that communicate across subnets and between virtual private networks (VPCs) 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 VPC while only IT administrators have RDP/SSH access to the production VPC. When deployed in conjunction with Palo Alto Networks GlobalProtect™ network security at the endpoint, the VM-Series on AWS can extend your corporate security policies to mobile devices and users regardless of their location.

### Applications and Data 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 with Threat Prevention and DNS Security features. 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 Delivers Policy Consistency

Panorama™ provides centralized network security management 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 AWS or on-premises using M-Series dedicated appliances. Alternatively, you can deploy both Panorama components on AWS or in a hybrid scenario, with Panorama Manager deployed on-premises and the Log Collector deployed on AWS. You can also use Panorama in conjunction with Cortex™ Data Lake.

## Automation to Support App Dev Workflows

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

- Bootstrapping allows you to create a working VM-Series configuration, complete with licenses and subscriptions, that can be deployed in an automated, scalable manner.
- A fully documented 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.
- Custom AMI support enables you to use the AWS Marketplace VM-Series image to create a customized AMI for use as the standard firewall image. To ensure encryption-at-rest policy compliance is maintained, you can deploy the VM-Series from an encrypted volume using AWS Key Management Service (KMS).

## Automated Policy Updates with Tag-Based Policy Model

VM-Series leverages the native tags from AWS in the formulation of network security policies. By basing policies on native AWS 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 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.

## Active Health Monitoring with AWS CloudWatch

VM-Series firewalls on AWS can send custom metrics to AWS CloudWatch. Metrics sent from VM-Series to AWS CloudWatch include:

- Session utilization %
- Total active sessions
- Dataplane CPU utilization %
- Dataplane packet buffer utilization %
- SSL proxy utilization %
- GlobalProtect active tunnels
- GlobalProtect tunnel utilization %
- Throughout (Kbps)
- Connection per Second
- Packets per Second

You can use these metrics to monitor the capacity and health status, and get deeper visibility into the usage and performance of your individual VM-Series deployed in your AWS environment. Additionally, you can use these metrics to get an aggregated view of performance of all your VM-Series firewalls in your autoscaling deployments, and then use it as a means to initiate autoscaling events.

## Integration with Amazon GuardDuty and AWS Security Hub

Amazon GuardDuty® and Security Hub both provide visibility into potentially malicious activity within your AWS deployment. Integration with the VM-Series allows you to send malicious IP address information to the VM-Series and automatically update a security policy to block malicious traffic.

## VM-Series on AWS High Availability

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

### Active/Passive High Availability

On AWS, the VM-Series supports high availability using two VM-Series firewalls deployed in an active/passive configuration within a single AWS Availability Zone. If a failure occurs, the AWS Elastic Network Interface (ENI) from the active VM-Series firewall is programmatically moved to the passive VM-Series firewall using AWS API calls.

### Cloud Native High Availability

High availability can also be achieved on AWS with a more cloud native approach that uses AWS load balancing for scale-out capacity and geographic high availability. In this scenario, an external load balancer is used to distribute traffic across multiple VM-Series firewalls deployed in separate Availability Zones. After inspection by the VM-Series, traffic is routed to an internal load balancer that distributes traffic to the web applications. If a VM-Series or other element fails, the load balancers can reroute traffic to its destination automatically.

## Scaling the VM-Series on AWS

There are two ways in which customers can view and address scalability on AWS. To protect large or rapidly growing AWS deployments that may consist of many VPCs, organizations are taking a shared services approach by using a transit VPC or transit gateway with the VM-Series. In deployments where inbound web application traffic may fluctuate rapidly,

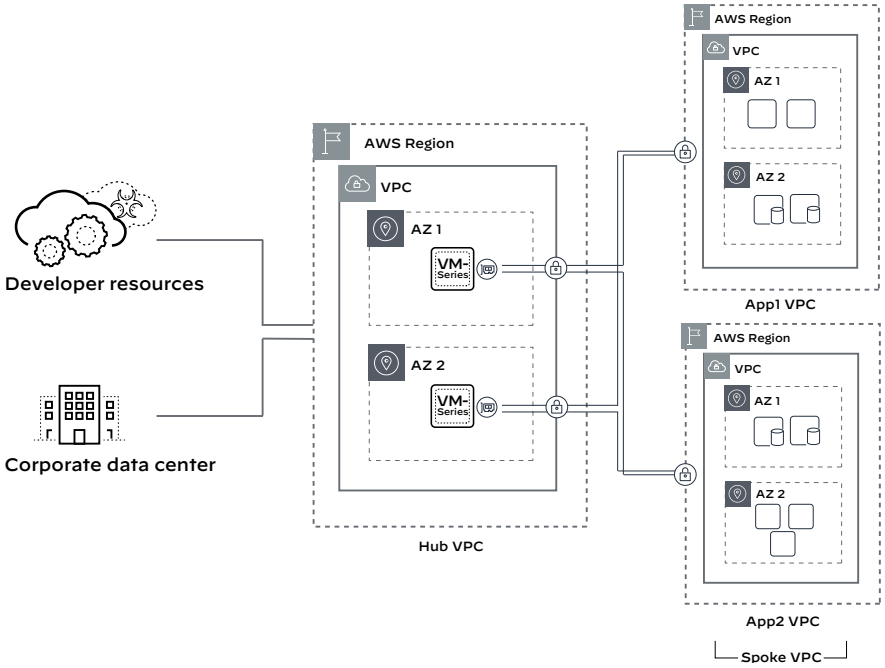


**Figure 1:** Transit VPC with the VM-Series

AWS Auto Scaling and Elastic Load Balancing 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.

In a hub-and-spoke architecture, each spoke VPC will "subscribe" to and transit the hub for secure connectivity. New spoke VPCs can be quickly 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).

## Auto Scaling the VM-Series

In deployment scenarios where inbound web traffic may fluctuate dramatically, AWS Auto Scaling can automatically deploy and remove new resources, including the VM-Series firewall, resulting in a cost-effective, efficient use of your AWS resources. Auto Scaling uses a hub-and-spoke architecture for flexibility. The hub houses the external network or application load balancer while the spokes house the internal network load balancer. User-defined metrics collected by CloudWatch are used to automatically initiate a scaling event to deploy new resources, including VM-Series firewalls. You can logically separate the hub and spokes using an AWS PrivateLink to meet your governance model needs.

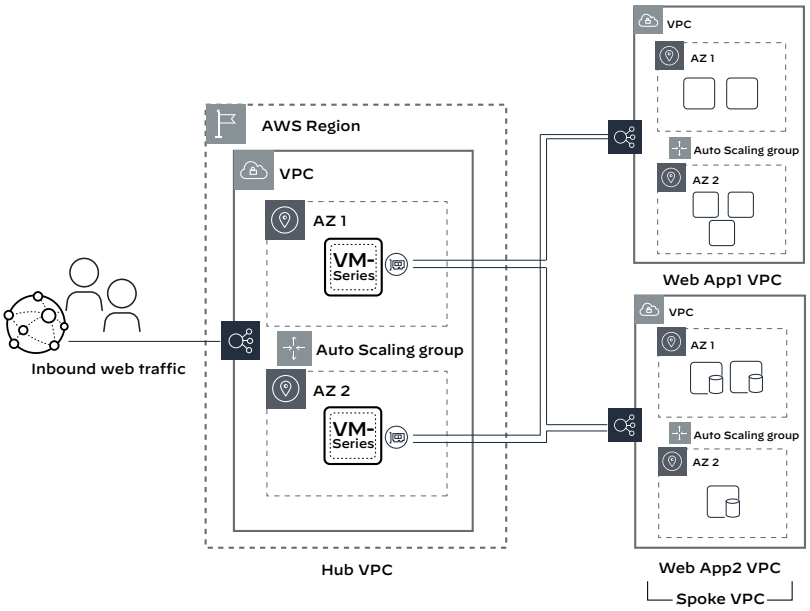


**Figure 2:** Auto Scaling with the VM-Series on AWS

# VM-Series on AWS Use Cases

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

## Internet Gateway: Protect Production Workloads

As your AWS 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.

## Hybrid Cloud: Securely Enable App Dev and Test

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

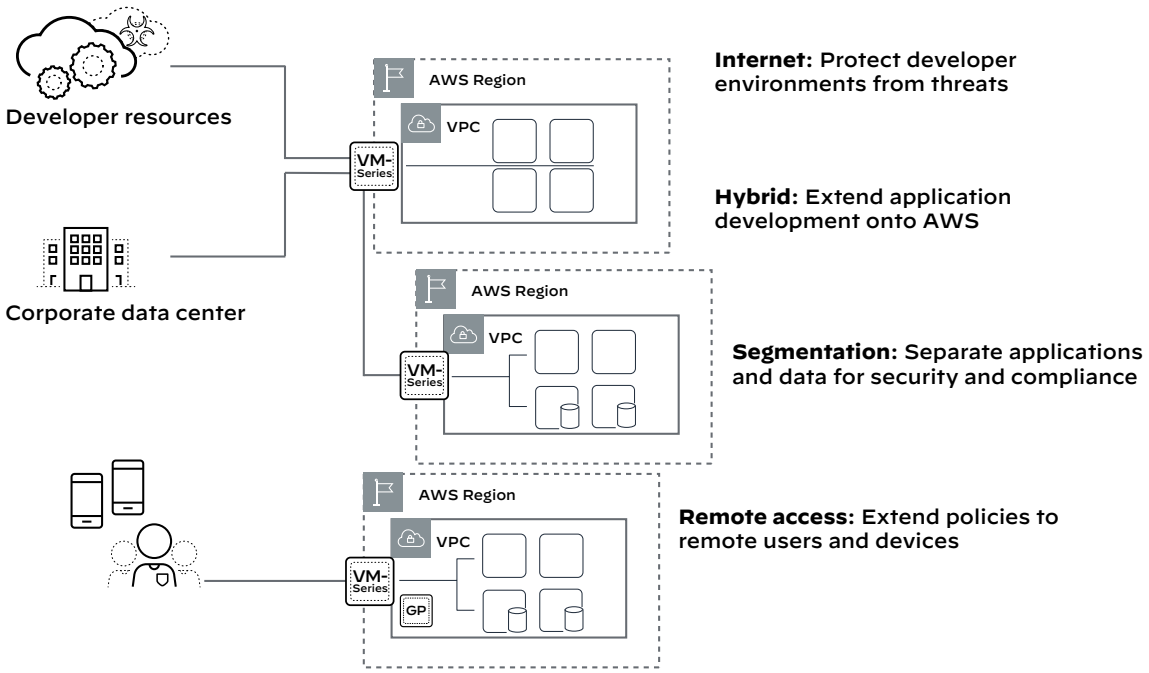


**Figure 3:** VM-Series on AWS use cases

## 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 AWS 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 VPCs 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.

## Remote Access: Extend Security to Users and Devices

GlobalProtect will enable 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.

## VM-Series on AWS GovCloud

VM-Series virtual firewalls can be deployed directly from the AWS GovCloud Marketplace to support each of the scenarios described, using any of the licensing options.

## VM-Series on AWS Outposts

VM-Series virtual firewalls can be deployed on AWS Outposts racks at your on-premises location directly from AWS marketplace. With VM-Series on your Outpost rack, you can have consistent security and policy management in your AWS Outpost subnets and your AWS Cloud subnets to protect your workloads against known and unknown threats.

## Licensing and Deployment

The VM-Series on AWS supports several licensing options, including pay-as-you-go (PAYG) licensing via the AWS Marketplace and bring your own license (BYOL):

- **Bring your own license (BYOL)**: You can purchase your VM-Series license Basic, Bundle 1, or Bundle 2 through normal Palo Alto Networks channels, and then deploy the VM-Series with your AWS Management Console using the license authorization code you received.
- **Pay-as-you-go (PAYG)**: Use your AWS Management Console to purchase and deploy hourly or annual VM-Series subscription bundles directly from the AWS Marketplace:
  - » **Bundle 1 contents**: Base VM license, Threat Prevention (inclusive of IPS, AV, malware prevention) subscription, and Premium Support (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 (written and spoken English only).

With the PAYG license bundles, the firewall is pre-licensed and ready for use as soon as you deploy it; you do not receive an auth code. When you stop or terminate the firewall from your AWS Management console, PAYG licenses are suspended or terminated.

For large-scale deployments, the VM-Series ELA allows you to forecast, and purchase upfront, VM-Series firewalls to be deployed over a one- or three-year period. Two types of VM-ELA are available:

- **BYOL ELA**: 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, subscriptions for Threat Prevention, DNS Security, URL Filtering, WildFire, and GlobalProtect Gateway, plus unlimited Panorama virtual machine licenses and Premium Support (written and spoken English only).
- **PAYG ELA**: The VM-Series PAYG ELA is ideally suited for customers with large-scale and expanding virtual firewall deployments in AWS. Available for only AWS deployments, the PAYG ELA does not provide license portability for other platforms. The PAYG ELA includes Bundle 2 subscriptions: Threat Prevention, URL Filtering, WildFire, GlobalProtect Gateway and DNS Security. Premium Support (written and spoken English only) is also included.

## Performance and Capacities

For a complete listing of all VM-Series features and capacities, please visit paloaltonetworks.com/comparefirewalls.

Please refer to the latest information on VM-Series performance on AWS instances here.

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