Secure AWS Servers and Kubernetes with the VM-Series

Challenges

As enterprises move to the cloud, they must:

- Secure both their physical and cloud infrastructure.
- Achieve scalable, easy-to-use, uniform security across clouds.
- Support their IT security teams in charting unfamiliar territory.

Solution

VM-Series firewalls bring industry-leading security to the cloud, so enterprises can:

- Configure and manage security across multiple VPCs from one place.
- Deploy once and scale endlessly with AWS Auto Scaling deployment templates.
- Provide consistent cloud security for various business units.
- Secure inbound traffic to Kubernetes® clusters and public-facing workloads.

Benefits

VM-Series AWS Auto Scaling deployment templates allow for a central point of security, safely enabling enterprises to:

- Provide additional compute on demand.
- Bring up multiple uniform VM-Series instances with minimized security fragmentation.
- Respond swiftly to new cloud infrastructure requests from DevOps without compromising security.

Product Overview

To protect large enterprise AWS® deployments, organizations can take a shared services approach by using AWS Auto Scaling deployment templates. These deployments may consist of various accounts; and multiple virtual private clouds (VPCs), security, and auto-scaling are applied using a secure VPC concept. The security VPC can be applied to protect inbound web traffic. Auto-scaling can be used to dynamically deploy or remove resources as traffic patterns fluctuate. This architecture can increase agility by allowing network security administrators to manage the security VPC while DevOps manages the application VPCs.

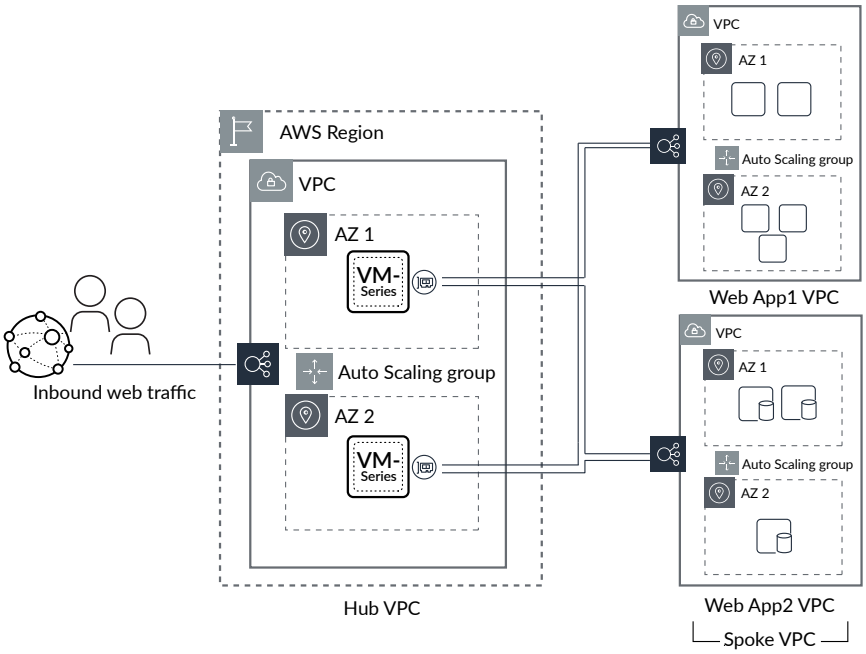

Figure 1: AWS Auto Scaling architecture with the VM-Series

Firewall Template

The firewall template uses the VM-Series Virtualized Next-Generation Firewall as a network security gateway for inbound requests. The firewall template deploys a Load Balancer and Auto Scaling group (ASG) for the VM-Series, providing centrally managed security to multiple web applications using the VM-Series as an inbound security gateway.

Application Template

Provided strictly on a proof of concept basis, the application template allows you to test-drive VM-Series auto-scaling in AWS. The application template provides multiple load balancer combinations using the application load balancer (ALB) or the network load balancer (NLB). When an ALB fronts the application workloads, the template connects the firewall VPC to the application VPC using VPC peering. When an NLB fronts the application workloads, the template can use AWS Private Link to join the firewall and application VPCs.

Active Health Monitoring with AWS CloudWatch

VM-Series firewalls on AWS can send internal metrics to AWS CloudWatch as a means of initiating Auto Scaling events. Metrics from PAN-OS® that can be sent 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 %

CloudWatch can also use these metrics to monitor the capacity, health status, and availability of your VM-Series and other resources deployed in your AWS environment.

Support for Kubernetes Clusters

Palo Alto Networks provides templates to help you deploy an Elastic Kubernetes Service (EKS) cluster in an AWS VPC. The Panorama plugin for Amazon EKS secures inbound traffic to Kubernetes clusters and provides outbound monitoring for traffic exiting the cluster. The solution works in conjunction with AWS ASGs. However, auto-scaling the VM-Series firewalls with the EKS deployment isn't supported at this time.

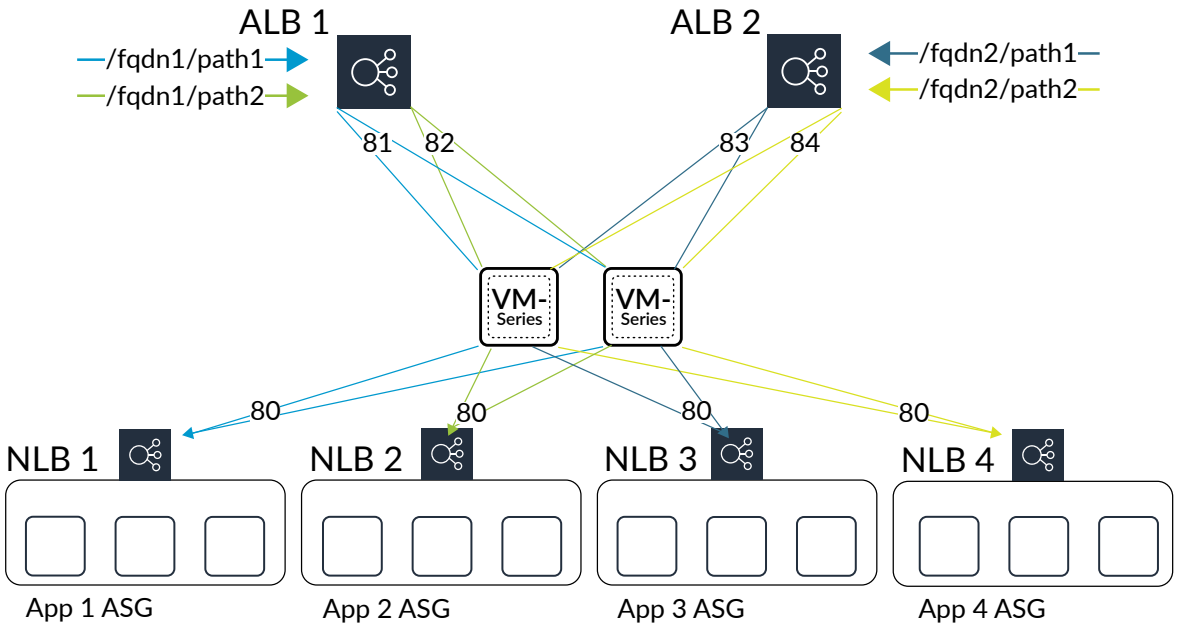

Figure 2: Load balancers in a hub-and-spoke architecture

Elastic Security: Fulfill DevOps Requests Without Sacrificing Security

The security VPC model allows flexibility while reinforcing essential security measures. By delivering security from a security VPC, you can launch infrastructure efficiently without compromising security. Panorama™ network security management provides further simplicity by enabling you to configure your VM-Series auto scale groups from a single location. Using the "deploy once, scale many" concept enables developers to meet their continuous integration/continuous delivery (CI/CD) objectives and gives IT Security the ability to scale security automatically as needed.

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 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 (DAGs), and External Dynamic Lists (EDLs) allow you to automate VM-Series configuration changes and consume external data to drive security policy updates dynamically. Action-Oriented Log Forwarding lets you drive actions based on observed incidents in the logs. In conjunction with AWS ARM templates or third-party tools, you can deploy next-generation security at the speed of the cloud.

Summary

The VM-Series auto scale templates in GitHub® can deliver centralized security and connectivity for your large-scale server and Kubernetes deployments. Palo Alto Networks Next-Generation Firewalls provide effective segmentation by ensuring appropriate application and user access to every segment, along with inspection for all content. They also provide the ability to support a flexible set of deployment modes and networking features.

Next Steps

To learn more about VM-Series cloud security solutions, visit us online or contact your Palo Alto Networks representative.

PRISMA™
BY PALO ALTO 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

secure-aws-servers-and-kubernetes-with-the-vm-series-b-121019