Securing Workloads in GCP 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 GCP autoscaling deployment templates.
- Provide consistent cloud security for various business units.
- Secure inbound traffic to Kubernetes® clusters and public-facing workloads.

Benefits

VM-Series GCP autoscaling 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 GCP™ deployments, organizations can take a shared services approach by using GCP autoscaling deployment templates. These deployments may consist of various VPC networks and multiple service projects. Security and autoscaling are applied using a secure host project concept. The secure host project is applied to protect inbound web traffic. Autoscaling 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 host project security, while DevOps manages the application service projects.

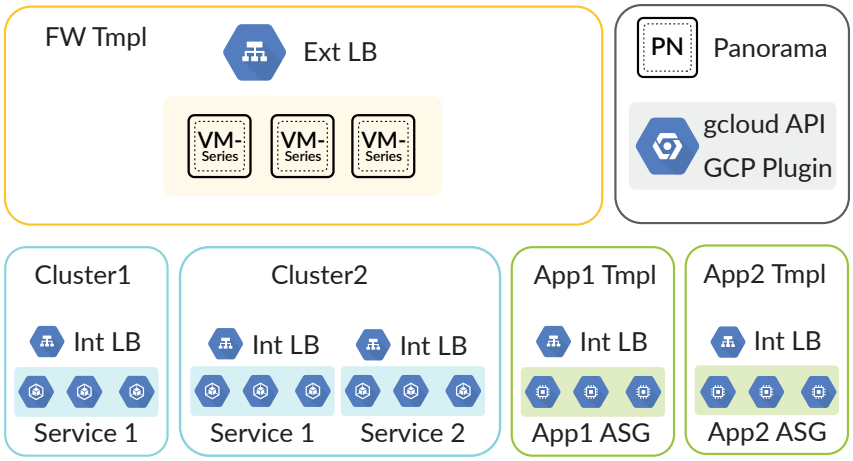

Figure 1: Inbound autoscaling architecture with the VM-Series

Details

Firewall Template

The Firewall template allows the VM-Series Virtualized Next-Generation FIrewall to be used as an edge security gateway to protect web applications and public-facing workloads. The template deploys an Application Gateway, Network Load Balancer, and a Managed Instanced Group for autoscaling the VM-Series firewalls. Secure VPC networks and applications in service projects with the click of a button.

Application Template

The application template is provided strictly on a proof-of-concept basis to allow you to test-drive VM-Series autoscaling in GCP. The application template provides

multiple load balancer combinations using either the application load balancer or the network load balancer. When an application load balancer fronts the application workloads. It also provides a managed instance group for autoscaling the sample applications deployed via the template. All service projects consume the same VPC-Trust and subnet-trust that reside south of the firewalls.

Active Health Monitoring with GCP Stackdriver

VM-Series firewalls on GCP can send internal metrics to GCP Stackdriver® as a means of initiating scaling events. Metrics from PAN-OS® that can be sent to GCP Stackdriver include:

- Session utilization %
- Total active sessions
- Dataplane CPU utilization %
- Dataplane packet buffer utilization %

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

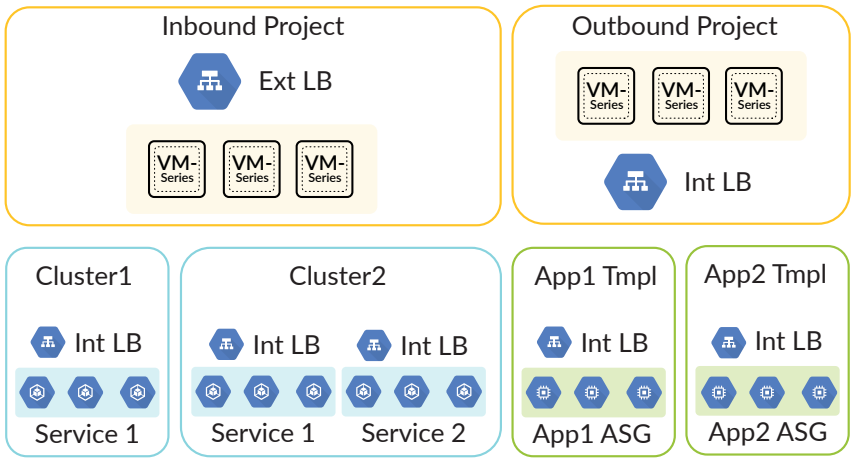

Figure 2: Load balancers in a hub-and-spoke architecture

Zero Trust: Improve Defense Against Cyberthreats and Prevent Data Exfiltration

Conventional security models operate on the outdated assumption that everything on the inside of an organization's network can be trusted. Zero Trust, rooted in the principle of "never trust, always verify," is designed to address lateral threat movement within the network by leveraging microsegmentation and granular perimeters enforcement. You can deploy the VM-Series in a managed instance group within a secure VPC network. You define movement or access based on who the user is and the defined appropriate interaction. A Zero Trust host project will provide security by serving as a security gateway for east-west and outbound traffic. In the current phase, you must create a Zero Trust host project manually, but an automation template will be available in the future.

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 host project, you will be able to launch infrastructure efficiently without compromising security. Panorama™ network security management provides further simplicity by enabling you to configure your VM-Series managed instance groups from a single location. By 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 when needed.

Automation to Support App Dev Workflows

The VM-Series on GCP 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 GCP templates or third-party tools, you can deploy next-generation security at the speed of the cloud.

Summary

The VM-Series GCP templates in GitHub® can deliver centralized security and connectivity for your large-scale server and public-facing deployments. Palo Alto Networks virtual 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

securing-workloads-in-gcp-with-the-vm-series-b-010620