

# ***Set Up the VM-Series Firewall on Google Cloud Platform***

---

## Contact Information

Corporate Headquarters:

Palo Alto Networks

3000 Tannery Way

Santa Clara, CA 95054

[www.paloaltonetworks.com/company/contact-support](http://www.paloaltonetworks.com/company/contact-support)

## About the Documentation

- To ensure you are viewing the most current version of this document, or to access related documentation, visit the Technical Documentation portal: [docs.paloaltonetworks.com](http://docs.paloaltonetworks.com).
- To search for a specific topic, go to our search page: [docs.paloaltonetworks.com/search.html](http://docs.paloaltonetworks.com/search.html).
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at [documentation@paloaltonetworks.com](mailto:documentation@paloaltonetworks.com).

## Copyright

Palo Alto Networks, Inc.

[www.paloaltonetworks.com](http://www.paloaltonetworks.com)

© 2019-2020 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at [www.paloaltonetworks.com/company/trademarks.html](http://www.paloaltonetworks.com/company/trademarks.html). All other marks mentioned herein may be trademarks of their respective companies.

## Last Revised

February 10, 2020

---

# Table of Contents

Set Up the VM-Series Firewall on Google Cloud Platform.....	4
About the VM-Series Firewall on Google Cloud Platform.....	5
Google Cloud Platform and the VM-Series Firewall.....	5
Minimum System Requirements for the VM-Series Firewall.....	5
Prepare to Set Up VM-Series Firewalls on Google Public Cloud.....	7
General Requirements.....	7
Install the Panorama Plugin for GCP.....	8
GCP Deployment Planning.....	8
Supported Deployments on Google Cloud Platform.....	14
Internet Gateway.....	14
Segmentation Gateway.....	14
Hybrid IPsec VPN.....	15
Deploy the VM-Series Firewall from Google Cloud Platform Marketplace.....	16
Management Interface Swap for Google Cloud Platform Load Balancing.....	19
Use the VM-Series Firewall CLI to Swap the Management Interface.....	20
Use Custom Templates or the gcloud CLI to Deploy the VM-Series Firewall.....	22
Enable VM Monitoring to Track VM Changes on GCP.....	23
Use Dynamic Address Groups to Secure Instances Within the VPC.....	25
Enable Google Stackdriver Monitoring on the VM Series Firewall.....	27
Google Stackdriver Permissions.....	27
Enable Google Stackdriver.....	27
VM Monitoring with the Panorama Plugin for GCP.....	29
Configure VM Monitoring with the Panorama Plugin for GCP.....	29
Auto Scaling the VM-Series Firewall on Google Cloud Platform.....	35
Auto Scaling Components for Google Cloud Platform.....	35
Deploy GCP Auto Scaling Templates.....	43

---

# Set Up the VM-Series Firewall on Google Cloud Platform

You can deploy a VM-Series firewall on a Google Compute Engine instance on the Google Cloud Platform.

- [About the VM-Series Firewall on Google Cloud Platform](#)
- [Prepare to Set Up the VM-Series Firewall on Google Public Cloud](#)
- [Supported Deployments on Google Cloud Platform](#)
- [Deploy the VM-Series Firewall from Google Cloud Platform Marketplace](#)
- [Use Custom Templates or the gcloud CLI to Deploy the VM-Series Firewall](#)
- [Enable VM Monitoring to Track VM Changes on Google Cloud Platform](#)
- [Use Dynamic Address Groups to Secure Instances Within the VPC](#)
- [Enable Google Stackdriver Monitoring on the VM Series Firewall](#)
- [VM Monitoring with the Panorama Plugin for GCP](#)
- [Auto Scaling the VM-Series Firewall on Google Cloud Platform](#)

# About the VM-Series Firewall on Google Cloud Platform

VM-Series firewalls bring next-generation firewall features to the Google® Cloud Platform (GCP™).

To maximize performance, VM-Series firewalls on GCP support the Data Plane Development Kit (DPDK) libraries, which provide fast packet processing and improve network performance based on specific combinations of VM-Series firewall licenses and Google Cloud Platform virtual machine (VM) sizes.

- [Google Cloud Platform and the VM-Series Firewall](#)
- [Minimum System Requirements for the VM-Series Firewall](#)

## Google Cloud Platform and the VM-Series Firewall

The VM-Series firewall integration with GCP allows you to deploy the VM-Series firewall as a virtual machine (VM) running on a Google Compute Engine instance. This process is simplified when you [Deploy the VM-Series Firewall from Google Cloud Platform Marketplace](#).

After you deploy the VM-Series firewall, you can manually configure the following optional services:

- [Enable Google Stackdriver Monitoring on the VM Series Firewall](#)—From the firewall, push PAN-OS metrics to the Google Stackdriver service.
- [Enable VM Monitoring to Track VM Changes on Google Cloud Platform](#)—Set up a VM information source that monitors the specific GCP zone containing your instances. The monitored VM metadata can include predefined GCP properties (such as the project ID) and user-defined properties (such as labels and network tags).

## Minimum System Requirements for the VM-Series Firewall

You must choose a [VM-Series Firewall License for Public Clouds](#) and a license method: bring-your-own-license (BYOL) or pay-as-you-go (PAYG). To deploy a VM-Series firewall on a Google Compute Engine instance, you must choose a machine type that supports the [VM-Series System Requirements](#) for your license.

Refer to the table below for the minimum recommended predefined [standard machine types](#) for each license. You can choose a higher performing machine type or you can create your own [custom machine type](#) if the resource requirements are compatible with your VM-Series firewall license.

A single Google Compute Engine instance supports up to eight [network interfaces](#). If you want to configure eight interfaces, choose n1-standard-8 or a larger machine type.

Capacity	BYOL	Bundles 1 and 2		Recommended Predefined Machine Type
		PAYG	Marketplace	
VM-100 Firewall	✓			n1-standard-4
VM-200 Firewall	✓			
VM-300 Firewall	✓	✓	✓	

Capacity	BYOL	Bundles 1 and 2		Recommended Predefined Machine Type
		PAYG	Marketplace	
VM-1000-HV Firewall	✓			
VM-500 Firewall	✓			n1-standard-8
VM-700 Firewall	✓			n1-standard-16

---

# Prepare to Set Up VM-Series Firewalls on Google Public Cloud

The process to [Deploy the VM-Series Firewall from Google Cloud Platform Marketplace](#) requires preparation tasks.

If you are deploying using the Google Marketplace, you must create your project networks and subnetworks, and plan networks and IP address assignments for the VM-Series firewall interfaces in advance. During the deployment, you must choose from existing networks and subnetworks.

Refer to the following topics when planning your deployment:

- [General Requirements](#)
- [Install the Panorama Plugin for GCP](#)
- [GCP Deployment Planning](#)

## General Requirements

The components in this checklist are common to deploying a VM-Series firewall that you manage directly or with Panorama. Additional requirements apply for Panorama plugin for services such as Stackdriver monitoring, VM monitoring, auto scaling or securing Kubernetes deployments.

Always consult the Compatibility Matrix for Panorama plugin information for [public clouds](#). This release requires the following software:

- **GCP account**—You must have a GCP user account with a linked email address and you must know the username and password for that email address.
- **Google Cloud SDK**—If you have not done so, [install](#) Google Cloud SDK, which includes [Google Cloud APIs](#), [gcloud](#) and other command line tools. You can use the command line interface to deploy the firewall template and other templates.
- **VM-Series firewalls on GCP**—VM-Series firewalls running a PAN-OS version available from the Google Marketplace.
  - Firewalls must meet the [Minimum System Requirements for the VM-Series Firewall](#).
  - You must [license](#) a VM-Series firewall to obtain a serial number. A serial number is required to add a VM-Series firewall as a Panorama managed device.
  - VM-Series firewalls that you want to manage from Panorama must be deployed in Google Cloud Platform using a Palo Alto Networks image from the Google Marketplace.
- **Panorama running in Management mode**—A Panorama physical or virtual appliance running a PAN-OS version that is the same or later than the managed firewalls. Virtual instances do not need to be deployed in GCP.

If you intend to configure features such as monitoring, or manage VMs deployed in GCP, your PAN-OS and [VM-Series plugin](#) versions must meet the requirements to support the Panorama plugin for GCP, as detailed in the Compatibility Matrix table for [Public Clouds](#).

In addition, Panorama must have network access to the VPCs in which the VMs you want to manage or secure are deployed.

- **Panorama plugin for GCP version 2.0.0**—The GCP plugin manages the interactions required to license, bootstrap and configure VM-Series firewalls. The plugin uses Panorama templates, template stacks, and device groups to program NAT rules that direct traffic to managed VM-Series firewalls.

See [Install the Panorama Plugin for GCP](#).

---

## Install the Panorama Plugin for GCP

Install the plugin version that supports the GCP features you want to configure, as detailed in the Compatibility Matrix table for [Public Clouds](#).



*You cannot upgrade the Panorama Plugin for GCP from version 1.0.0 to version 2.0.0.*

**STEP 1 | Check the PAN-OS version**—On Panorama, ensure that your PAN-OS version meets the requirements to support GCP auto scaling.

**STEP 2 | Check the VM-Series plugin.**

If the VM-Series plugin is installed, the version is listed on the Dashboard.

- **Initial installation**—Because the VM-Series plugin is optional on Panorama, the first time you [install](#) you must download the VM-Series plugin from [support.paloaltonetworks.com](https://support.paloaltonetworks.com), then go to **Panorama > Device Deployment > Plugins** to **Upload** and **Install**.
- **Upgrade**—To upgrade, go to **Panorama > Device Deployment > Plugins** and click **Check Now**. Install a version that meets the requirements in the Compatibility Matrix table for [Public Clouds](#).

After the installation you can see the plugin in the Panorama dashboard **General Information** list. In the Panorama context, view the Google Cloud Platform in the list of plugins and you see the **Setup**, **Monitoring Definition**, and **AutoScaling** topics.

**STEP 3 | Install the Panorama plugin for GCP**—Select **Panorama > Plugins**, and type **gcp** in the search bar. **Install** the plugin version that supports the features you want to configure.

## GCP Deployment Planning

Review these requirements to ensure that you have proper accounts and permissions before you use the Google Marketplace to deploy the firewall on a Google Compute Engine (GCE) instance.

- [General Accounts and Permissions](#)
- [Available Google Resources](#)
- [Google Authentication Methods](#)
- [SSH Key Pair](#)

### General Accounts and Permissions

- ❑ You, and any users you allow, must have the following minimal [roles](#) or equivalent [Identity and Access Management \(IAM\)](#) permissions to connect to the VM-Series firewall:
  - ❑ **Compute Viewer**—Enables you to get and list compute engine resources without being able to read the data stored on those resources.
  - ❑ **Storage Object Viewer**—Enables you to bootstrap using a Google storage bucket in the same project.



*Users in your organization might have [IAM permissions](#) or predefined [roles](#) that are more permissive than required. Ensure that you appropriately restrict VM-Series firewall access.*

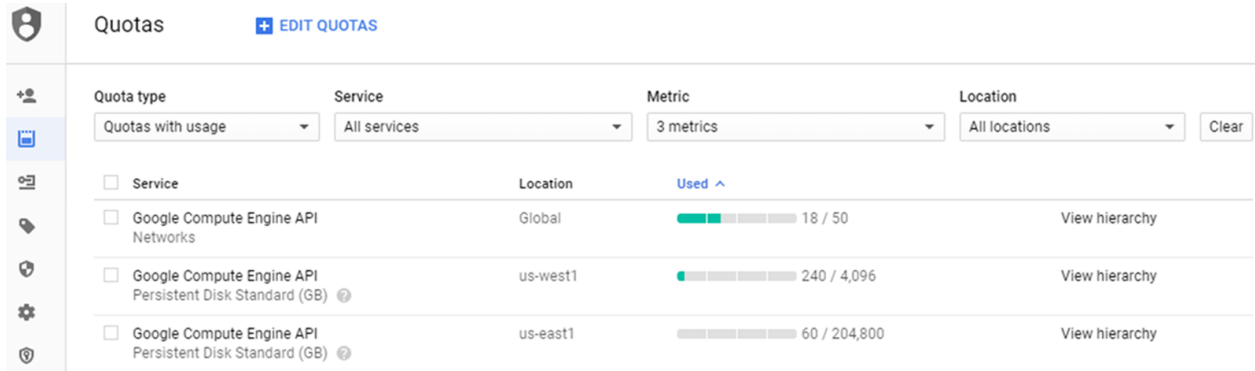
You can also restrict access with service accounts, as described in [Google Authentication Methods](#).

- ❑ **Monitoring Metric Writer**—Required for [Stackdriver](#).



## Available Google Resources

Your project must have sufficient resources to deploy the VM-Series firewall as a Google Compute Engine instance. If you are deploying a GCP [Marketplace](#) solution, determine whether the solution deploys other VMs in addition to the firewall. In the Google Cloud Console, select **IAM & admin** > **Quotas** to review the resource quotas for your project and the networks and disk space consumed. If you are running out of resources you can ask Google to allocate more for your organization.



Quota type	Service	Metric	Location	
Quotas with usage	All services	3 metrics	All locations	Clear
<input type="checkbox"/> Service		Location	Used ^	
<input type="checkbox"/> Google Compute Engine API Networks		Global	18 / 50	<a href="#">View hierarchy</a>
<input type="checkbox"/> Google Compute Engine API Persistent Disk Standard (GB)		us-west1	240 / 4,096	<a href="#">View hierarchy</a>
<input type="checkbox"/> Google Compute Engine API Persistent Disk Standard (GB)		us-east1	60 / 204,800	<a href="#">View hierarchy</a>

## Google Authentication Methods

GCP supports multiple ways to [connect to an instance](#). You can authenticate with a service account or an SSH key pair.

- **Service Accounts**—[Service Accounts](#) apply to applications or VMs—not to end users. They are commonly used to control access when you use programs or scripts, or when you access the firewall from the [gcloud](#) command line. If you are using Google [Service Accounts](#) to authenticate [instances](#) or applications, you must know the email address for the account(s). Refer to [Creating and Managing Service Account Keys](#).

Using a service account is necessary if you want to connect to the VM-Series firewall from outside the project. For example, if you want to enable a physical next generation firewall to monitor your VM-Series firewall, you must save the VM-Series firewall service account information to a JSON file. In the physical firewall, you upload the file when you configure the connection.

- **SSH Keys**—If you deploy the VM-Series firewall from the [Marketplace](#), you must supply one Open SSH key in RSA format for the Google Compute Engine instance metadata.



*The VM-Series firewall only accepts one key at deployment.*

At deployment time, you paste the public key into the Marketplace deployment, as described in [SSH Key Pair](#). After deployment you use the private key to SSH in to the firewall to configure the administrator account. To add users, see [Manage Firewall Administrators](#).

You can authenticate in several ways:

- **Use the default service account for your project**—If you are using the Google Cloud Platform (GCP™) Console, then you logged in with your email address and can access a GCE instance based on whatever permissions or roles the project administrator assigned to your account.

Every Google Compute Engine instance created with the Google Cloud Console or the [gcloud](#) command line tool has a default service account with the name in email address format:

```
<project-number>-compute@developer.gserviceaccount.com
```

To see the service account name for the firewall instance, view the instance details and scroll to the bottom (refer to the [Compute Engine default service account](#)).

---

The default service account can manage authentication to VMs in the same project as a VM-Series firewall. [Access scopes](#) allow the firewall to initiate API calls to VMs in the Google Cloud project.

- **Create service accounts for instances**—A project can have many service accounts, and you can assign specific roles to a service account, which in turn can be assigned to user
- **Use IAM permissions and the Google APIs**—If you use the Google SDK APIs and [gcloud](#), then you must call the APIs to authenticate.
  - You typically use the Google SDK when you want to manage the firewall from a command line or you want to run a script to configure the firewall.
  - You need to access the Google APIs if a virtual machine you connect to has a custom image with applications that require Google APIs.

## SSH Key Pair

When you deploy the VM-Series firewall from the Google Marketplace you need an SSH key pair to authenticate with the VM-Series firewall.



*Create the key pair according to your key generator documentation. Do not edit the public key file. Editing risks introducing illegal characters.*

The VM-Series firewall manages authentication differently than GCE instances. After deployment, you first log in with the **admin** user. The VM-series firewall default user name is accepted only once. After a successful login you set an administrator username and password for the VM-Series web interface (see [Deploy the VM-Series Firewall from Google Cloud Platform Marketplace](#)).

The Google Marketplace deployment interface **SSH key** field displays the following placeholder:

```
admin:ssh-rsa your-SSH-key
```

**admin** is the VM-Series firewall Administrator user name required to log in to the firewall for the first time. You add the **admin:** prefix into the Marketplace field when you [deploy the VM-Series firewall](#).

You cannot log in to the VM-Series firewall if you do not supply the entire public key, or your key has illegal characters when you paste the key into the Marketplace **SSH key** field. When you SSH in to the VM-Series firewall for the first time, the public key is transferred to the firewall.

If the public key is corrupted, you must delete the deployment and start over. Any networks and subnetworks remain, but the firewall rules must be recreated.

**STEP 1 |** Create an SSH key pair and store the SSH Key pair in the default location for your operating system mentioned in [Locating an SSH key](#).

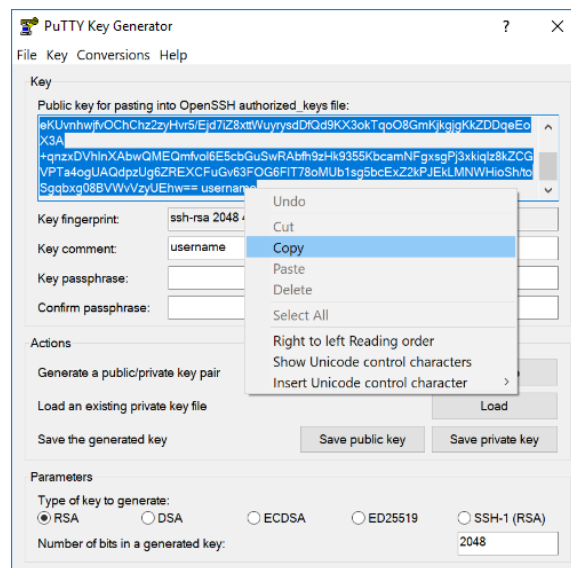
- **Linux or MacOS**—Use `ssh-keygen` to create the key pair in your `.ssh` directory.
- **Windows**—Use PuTTYgen to create the key pair.

The content of the **Key comment** field does not matter to the VM-Series firewall; you can accept the default (the key creation date) or enter a comment that helps you remember the name of the key pair. Use the **Save private key** button to store the private key in your `.ssh` directory.

**STEP 2 |** Select the full public key.

- **Linux or MacOS**—Open your public key in a text editor and copy the public key.
- **Windows**—You must use the PuTTY Key Generator to view the public key. Launch PuTTYgen, click **Load**, and browse to private key you saved in your `.ssh` directory.

In PuTTYgen, scroll down to ensure you select the entire key, right click, and choose Copy.



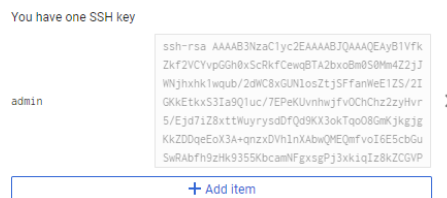
**STEP 3** | Enter the public key in the SSH key field as detailed below.

1. In the Marketplace **SSH key** field, delete the placeholder text, and type:  
**admin:**  
Make sure there are no extra spaces following the colon.
2. Insert the cursor after **admin:** and choose **Paste as plain text**. The key must be on a single line, as shown below.

SSH key ⓘ  
admin:ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEAyB1VfkZkf2VCYvpGGh0xS

**STEP 4** | Check the key.

After the deployment, and before you attempt to log in to the firewall, view the management instance and check the key for linefeeds or extra spaces:



If the key looks right you are finished.

**STEP 5** | (optional) If something is wrong you must replace the key.

1. Click the **X** to delete the key, then click **+ Add item**.
2. Type in **admin:** (no spaces) and copy and paste in the key again.
3. Click **Save** to deploy the updated deployment.
4. Re-check the key.

## Virtual Private Cloud (VPC) Network Planning

Make a plan for [VPC networks](#) (referred to as *networks*), subnetworks (also called *subnets*), and Google firewall rules. You must create networks and subnetworks before you start [Deploy the VM-Series Firewall from Google Cloud Platform Marketplace](#).



*The Marketplace deployment page displays only networks and subnetworks that exist when you start the deployment. If a network is missing, you must exit the deployment, create the network, and start over.*

- ❑ **VPC networks**—You must create a custom network specifically for each VM-Series network interface.
  - ❑ See [VM-Series Firewall Licenses for Public Clouds](#) to determine the number of network interfaces needed based on your VM-Series firewall license. At a minimum, set up the three VPC networks and subnets required to launch the VM-Series firewall.
  - ❑ A GCP [project](#) has a default network with preset configurations and firewall rules; you can delete the default network, if unused.
  - ❑ By default, there are up to five networks in a project. Your GCP administrator can request additional networks for your project.
  - ❑ To connect to the management interface you must create a GCP firewall rule that allows access. You can do this during the deployment if you choose **Enable GCP Firewall rule for connections to Management interface** then supply a CIDR block for **Source IP in GCP Firewall rule for connections to Management Interface**.



*Be sure your networks include all instances you want to secure.*

- ❑ **Subnetworks**—A compute engine instance can support up to eight Layer 3 interfaces on a single instance. The Management, Trust, and Untrust interfaces consume three interfaces and you can create up to five additional dataplane interfaces. Typically the dataplane interfaces represent application networks.
- ❑ **IP address**—You supply [IP address](#) ranges when you create interface subnetworks, and you have the option to enable an external address when you deploy a subnetwork.
  - When you create a network subnet, you must specify an IP address range. This range is used for your internal network, so it cannot overlap with other subnets.
  - During deployment, you can choose to enable an external IP address when you create a network interface. By default, you are given an [ephemeral](#) IP address. You cannot supply a reserved static IP address during the deployment, but you can promote the [ephemeral](#) address to a static IP address after you complete the deployment process (see [Promoting an ephemeral external IP address](#)).

## Network Interface Planning

When you deploy from [Google Cloud Platform Marketplace](#), the default VM-Series firewall deployment has three interfaces: the Management plane interface and the Untrust and Trust dataplane interfaces. You can define additional dataplane instances, depending on the available compute resources on your VM; see [VM-Series Firewall Licenses for Public Clouds](#).

During the deployment you have the opportunity to name these interfaces.

### Interface Order

When you deploy with [Marketplace](#), the order of the network interfaces is predefined. The Management interface maps to eth0, Untrust to eth1, and Trust to eth2. Marketplace uses this order because mapping the Management interface to eth0 and the Untrusted interface to eth1 is a requirement if you need to [Swap the Management Interface](#) for load balancing.

### Management Interface

The first network interface you add is mapped to eth0 on the firewall and includes the option to enable IP forwarding. You use this network interface to manage the VM-Series firewall. Typically, this interface has an external IP address.



*An external IP address is only required if a dataplane interface is attached to the public subnet. At creation time, you can receive an ephemeral IP address and later promote it to a static IP address after you complete the deployment (refer to [Promoting an ephemeral external IP address](#)).*

### Dataplane Interfaces (Untrust, Trust)

When you deploy from Marketplace, the order in which you add interfaces is predetermined.

- You configure the Untrust interface after the Management interface. This order means that the untrusted interface is mapped to eth1. The Untrust interfaces are typically attached to the public subnet, and have an external IP address.



*An external IP address is only required if a dataplane interface is attached to the public subnet. At creation time, you can receive an ephemeral IP address, then promote it to a static IP address, as discussed in [Promoting an ephemeral external IP address](#).*

- The Trust interface follows the Untrust interface, and it is mapped to eth2. The Trust network often does not have an external IP address. You can add any additional dataplane interfaces after the Trust interface.

### Additional Dataplane Interfaces

Plan interfaces for applications you must secure, such as web servers, databases, and other applications in your network. You can create up to five additional dataplane interfaces in addition to the three required to launch your firewall. Ensure that the applications you want to secure are in networks that connect to the VM-Series firewall.

# Supported Deployments on Google Cloud Platform

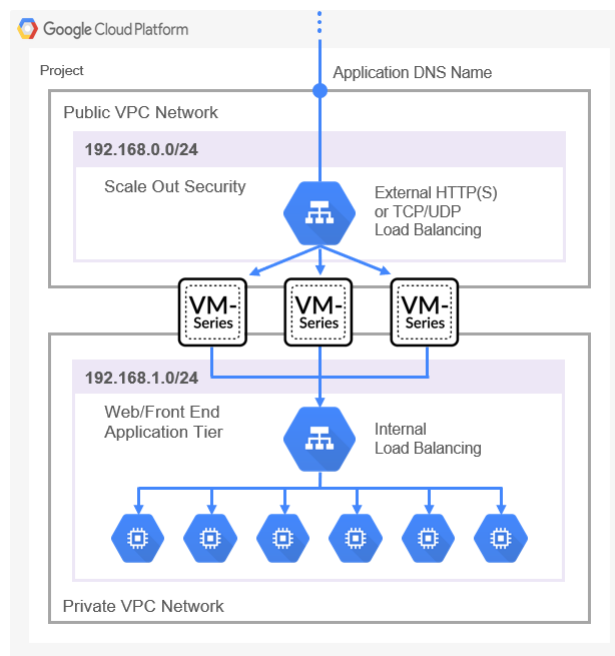
You can deploy the VM-Series firewall on a Google® Compute Engine instance in a network in your [virtual private cloud \(VPC\)](#). The deployment types are:

- [Internet Gateway](#)
- [Segmentation Gateway](#)
- [Hybrid IPsec VPN](#)

## Internet Gateway

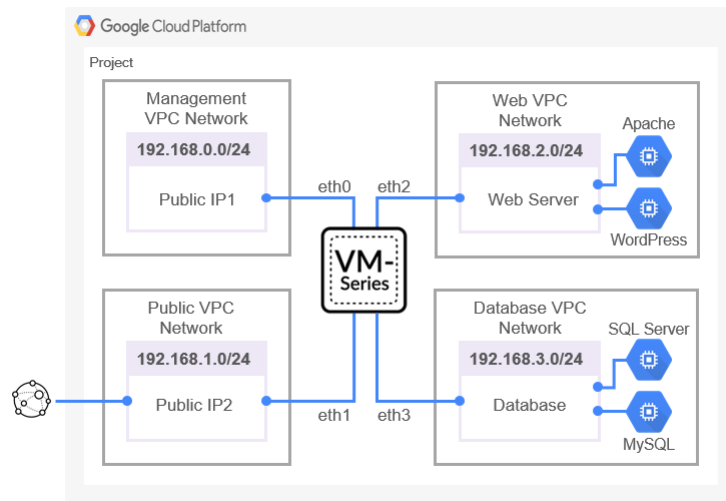
The VM-Series firewall secures North/South traffic to and from the internet to protect applications from known and unknown threats. A Google project can have up to five VPC networks. For a typical example of an internet gateway, refer to the Google [configuration examples](#).

In public cloud environments, it is a common practice to use a scale-out architecture (see the figure below) rather than larger, higher performing VMs. This architecture (sometimes called a *sandwich* deployment) avoids a single point of failure and enables you to add or remove firewalls as needed.



## Segmentation Gateway

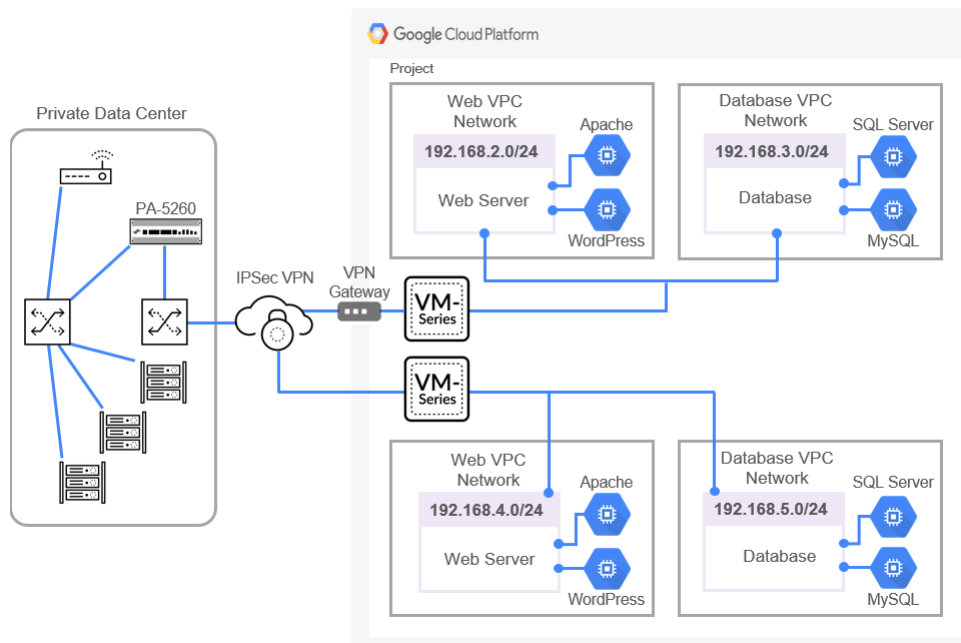
A segmentation gateway secures East/West traffic between virtual private clouds (VPCs) to ensure data protection compliance and application access. The following figure shows a firewall securing both North/South and East/West traffic.



## Hybrid IPsec VPN

The VM-Series firewall serves as an IPsec VPN termination point, which enables secure communications to and from applications hosted on Google Cloud Platform (GCP).

The deployment in the figure below shows a site-to-site VPN from an on-premises network to a VM-Series firewall deployed on GCP and an IPsec connection from an on-premises network to a Google Cloud VPN gateway.



---

# Deploy the VM-Series Firewall from Google Cloud Platform Marketplace

You can use Google® Cloud Platform [Marketplace](#) to deploy the VM-Series firewall on a VM-300 capacity license. The licensed images available from Cloud are:

- [VM-Series Next-Generation Firewall Bundle 1](#)
- [VM-Series Next-Generation Firewall Bundle 2](#)
- [VM-Series Next-Generation Firewall \(BYOL\)](#)

See [Deploy the VM-Series Firewall from Google Cloud Platform Marketplace](#) for more about these license options.

The [Marketplace](#) deploys an instance of the VM-Series firewall with a minimum of one management interface and two dataplane interfaces (Trust and Untrust). You can add additional dataplane interfaces for up to five Google Compute Engine instances in your virtual private cloud (VPC).

Before you deploy the VM-Series firewall, you must create or choose a project in your organization and create any networks and subnets that will connect to the firewall, as described in [VPC Network Planning](#) and [Network Interface Planning](#).

You cannot attach multiple network interfaces to the same VPC network. Every interface you create must have a dedicated network with at least one subnet. Ensure that your networks include any additional dataplane instances you create.

**STEP 1 |** Locate the VM-Series firewall listing in the [Marketplace](#).

1. Log in to the Google Cloud Console.
2. From the Products and Services menu, select **Marketplace**.
3. Search for **VM-Series**.
4. Select one of the VM-Series firewall licensing options.

**STEP 2 |** Click **Launch on Compute Engine**.

**STEP 3 |** Name the instance and choose resources.

1. Enter the **Deployment Name** (this name is displayed in the Deployment Manager). The name must be unique and cannot conflict with any other deployment in the project.
2. Select a Zone. See [Regions and Zones](#) for a list of supported zones.
3. Select a **Machine Type** based on the [VM-Series System Requirements](#) for your license and the [Minimum System Requirements for the VM-Series Firewall on Google Cloud Platform](#).

**STEP 4 |** Specify instance metadata. The options **Bootstrap Bucket** and **Interface Swap** affect the initial configuration the first time the VM-Series firewall boots.

1. **Bootstrap Bucket (Optional)**—If you plan to use a bootstrap file, enter the name of a storage bucket with the bootstrap configuration described in [Minimum System Requirements for the VM-Series Firewall on Google Cloud Platforms](#).
2. **Interface Swap (Optional)**—Swap the Management interface (eth0) and the first dataplane interface (eth1) at deployment time. Interface swap is only necessary when you deploy the VM-Series firewall behind Google Cloud Platform HTTP(S) Load Balancing. For details, see [Management Interface Swap for Google Cloud Platform Load Balancing](#).



- 
3. **SSH key**—Paste in the public key from an SSH key pair. Follow the instructions for your OS in [SSH Key Pair](#), to create, copy, and paste the key. Windows users must view the key in PuTTY, copy from the user interface, and paste into Marketplace deployment.



*If the key is not formatted properly, the VM-Series firewall does not allow you to log in. You must delete the deployment and start over.*

4. Click **More** to reveal additional metadata options. The options **blockProjectKeys**, and **enableSerialConsole** are properties of the instance; you can change these metadata values after a successful deployment.
  - **blockProjectKeys** (Optional)—If you [Block Project Keys](#), you can use only the public SSH key you supply to access the instance.
  - **enableSerialConsole** (Optional)—[Interacting with the Serial Console](#) enables you to monitor instance creation and perform interactive debugging tasks.

#### STEP 5 | Configure the boot disk.

1. **Boot disk type**—Select from SSD Persistent disk or Standard Persistent Disk. See [Storage Options](#).
2. Enter the **Boot disk size**—60GB is the minimum size. You can edit the disk size later but you must stop the VM to do so.

#### STEP 6 | Configure the management interface.

1. **Management VPC Network name**—Choose an existing network
2. **Management Subnet name**—Choose an existing subnet.
3. **Enable External IP for Management interface** (Optional)—If you enable this option, you can use the IP address assigned to the VM-Series firewall management interface to use SSH to access the VM-Series firewall web interface.
4. **Enable GCP Firewall rule for connections to Management interface** (Optional)—This option automatically creates a GCP firewall Allow rule for an external source IP address that you supply.
5. **Source IP in GCP Firewall rule for connections to Management Interface**—If you **Enable GCP Firewall rule for connections to Management interface**, enter a source IP address or a CIDR block.
  - Do not use 0.0.0.0/0. Supply an IP address or a CIDR block that corresponds to your dedicated management IP addresses or network. Do not make the source network range larger than necessary.
  - Verify the address to ensure that you do not lock yourself out.

#### STEP 7 | Configure the Untrust dataplane interface.

1. **Untrust VPC Network name**—Choose an existing network.
2. **Untrust Subnet name**—Choose an existing subnet.
3. **Enable External IP for Untrust**—Enable GCP to provide an [ephemeral](#) IP address to act as the external IP address.

#### STEP 8 | Configure the Trust dataplane interface.

1. **Trust VPC Network name**—Choose an existing network.
2. **Trust Subnet name**—Choose an [existing network](#).
3. **Enable External IP for Trust**—Enable GCP to provide an [ephemeral](#) IP address to act as the external IP address.

#### STEP 9 | Configure additional interfaces. You must enter the number of dataplane interfaces you want to add; the default is 0 (none). The deployment page always displays fields for five additional dataplanes numbered 4 through 8.

1. **Additional Dataplane interfaces**—Enter the number of additional dataplane instances.



*If this number is 0 (default), dataplane numbers 4 through 8 are ignored even if you fill out the interface fields. If, for example, you specify 2 and then fill out information for three interfaces, only the first two are created.*

2. **Additional Dataplane # VPC name**—Choose an existing network.
3. **Dataplane # Subnet name**—Choose a subnet that exists.
4. **Enable External IP for dataplane # interface**—Enable GCP to provide an [ephemeral](#) IP address to act as the external IP address.

**STEP 10 | Deploy** the instance.

**STEP 11 | Use [Google Cloud Deployment Manager](#)** to view and manage your deployment.

**STEP 12 | Use the CLI** to change the administrator password on the firewall.

1. Log in to the VM-Series firewall from the command line. In your SSH tool, connect to the External IP for the management interface, and specify the path to your private key.

Windows users: Use PuTTY to connect to the VM-Series firewall and issue command line instructions. To specify the path to the private key, select **Connection > SSH > Auth**. In **Private key file for authentication**: click **Browse** to select your private key.

2. Enter configuration mode:

```
VMfirewall> configure
```

3. Enter the following command:

```
VMfirewall# set mgt-config users admin password
```

4. Enter and confirm a new password for the administrator.

5. Commit your new password:

```
VMfirewall# commit
```

6. Return to command mode:

```
VMfirewall# exit
```

7. (Optional) If you used a bootstrap file for interface swap, use the following command to view the interface mapping:

```
VMfirewall> debug show vm-series interfaces all
```

**STEP 13 | Access the VM-Series firewall web interface.**

1. In a browser, create a secure (https) connection to the IP address for the management interface.

If you get a network error, check to see that you have a GCP firewall rule that allows the connection.

2. When prompted, enter the username (admin) and the administrator password you specified from the CLI.

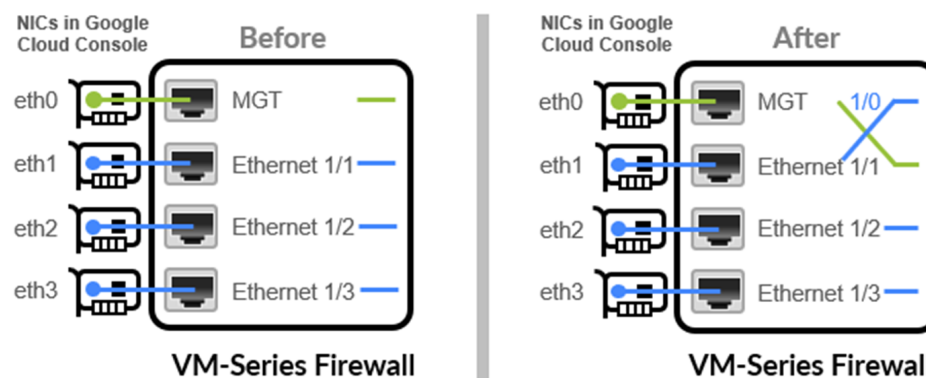
3. (Optional) If you bootstrapped, then [Verify Bootstrap Completion](#).

If you see problems, search the log information on the VM-Series firewall. Choose **Monitor > System** and, in the manual search field, enter **description contains 'bootstrap'** and look for a message in the results that indicates that the bootstrap was successful.

After you log in to the firewall, you can add administrators and create interfaces, zones, NAT rules, and policy rules, just as you would on a physical firewall.

# Management Interface Swap for Google Cloud Platform Load Balancing


Because internal load balancing can send traffic only to the primary interface of the next hop load-balanced Google Compute Engine instance, the VM-Series firewall must be able to use eth0 for dataplane traffic.



The firewall can receive dataplane traffic on eth0 if the VM-Series firewall is behind the Google Cloud Platform internal load balancing interface.

- The VM-Series firewalls secure traffic outbound directly to the internet without requiring a VPN link or a Direct Connect link back to the corporate network.
- The VM-Series firewall secures an internet-facing application when there is exactly one back-end server, such as a web server, for each firewall. The VM-Series firewalls and web servers can scale linearly, in pairs, behind the Google internal load balancing address.

To allow the firewall to send and receive dataplane traffic on eth0 instead of eth1, you must swap the mapping of the internal load balancing network interface within the firewall so that eth0 maps to ethernet 1/1, and eth1 maps to the MGT interface on the firewall.

 *Swap the management interface mapping before you configure the firewall and define policy rules.*

Swapping how the interfaces are mapped allows Google Cloud Platform to distribute and route traffic to healthy instances of the VM-Series firewall located in the same or different zones.

## Swap the Management Interface

You can swap the interfaces when you [Deploy the VM-Series Firewall from Google Cloud Platform Marketplace](#), or you can configure the firewall after it is created.

### At Creation

When you deploy the VM-Series firewall, you can enable interface swap in two ways.

- **Google Cloud Console** — In the Create Instance form, enter a key-value pair in the **Metadata** field, where **mgmt-interface-swap** is the key, and **enable** is the value.
- **Bootstrap File** — Create a bootstrap file that includes the **mgmt-interface-swap** operational command in the bootstrap configuration, as described in [Bootstrap the VM-Series Firewall on Google Cloud Platform](#). In the Create Instance form, enter a key-value pair in the **Metadata** field to enable the bootstrap option.

## After Deployment

Log in to the firewall, and [Use the VM-Series Firewall CLI to Swap the Management Interface](#). In operational mode, issue the following command:

```
set system setting mgmt-interface-swap enable yes
```



*If you configured the VM-Series firewall before swapping, check whether any IP address changes for eth0 and eth1 impact policy rules.*

*From the Google Cloud Console you cannot confirm whether you have swapped eth0 and eth1. After swapping, you must remember that load balancing is on eth0 and the firewall management interface is eth1 so that you can properly configure Google Cloud Platform load balancing, and create security policy rules to secure load balancing to one or more VM-Series firewalls.*

## Use the VM-Series Firewall CLI to Swap the Management Interface



*This task is only required if your architecture places the VM-Series firewall behind the GCP internal load balancer.*

If you did not specify metadata to swap the management interface (MGT) with the dataplane interface when you deployed the firewall, you can use the CLI to enable the firewall to receive dataplane traffic on the primary interface.

### STEP 1 | Deploy the VM-Series Firewall from Google Cloud Platform Marketplace.



*Before you proceed, verify that the firewall has a minimum of two network interfaces (eth0 and eth1). If you launch the firewall with only one interface, the interface swap command causes the firewall to boot into maintenance mode.*

**STEP 2 |** On the Google Cloud Console, view the VM instance details to verify the network interface IP addresses of the eth1 interface and verify that any security rules allow connections (HTTPS and SSH) to the new management interface (eth1).

**STEP 3 |** Log in to the VM-Series firewall CLI and enter the following command:

```
set system setting mgmt-interface-swap enable yes
```

You can view the default mapping from the command line interface. The output is similar to this:

```
> debug show vm-series interfaces all
Interface_name  Base-OS_port
mgt             eth0
Ethernet1/1     eth1
Ethernet1/2     eth2
```

**STEP 4 |** Confirm that you want to swap the interface (use the eth1 dataplane interface as the management interface).

**STEP 5 |** Reboot the firewall for the swap to take effect:

```
request restart system
```

---

**STEP 6** | Verify that the interfaces have been swapped:

```
debug show vm-series interfaces all
```

---

# Use Custom Templates or the gcloud CLI to Deploy the VM-Series Firewall

The official VM-Series images published on Google Cloud Platform Marketplace are available in the **paloaltonetworksgcp-public** project. You need to know the secure path to these images if you want to call them from the **gcloud** command line, or refer to them in a template you have written or adapted.

- BYOL: `vmseries-byol-<version>`
- PAYG Bundle 1: `vmseries-bundle1-<version>`
- PAYG Bundle 2: `vmseries-bundle2-<version>`

Use the **gcloud** CLI to find the current image names and project:

```
gcloud compute images list --project paloaltonetworksgcp-public  
--no-standard-images
```

NAME	PROJECT	FAMILY	DEPRECATED	STATUS
vmseries-bundle1-810	paloaltonetworksgcp-public			READY
vmseries-bundle2-810	paloaltonetworksgcp-public			READY
vmseries-byol-810	paloaltonetworksgcp-public			READY

Add the **--uri** flag to see the image paths:

```
gcloud compute images list --project paloaltonetworksgcp-public  
--no-standard-images --uri
```

```
https://www.googleapis.com/compute/v1/projects/paloaltonetworksgcp-public/  
global/images/vmseries-bundle1-810  
https://www.googleapis.com/compute/v1/projects/paloaltonetworksgcp-public/  
global/images/vmseries-bundle2-810  
https://www.googleapis.com/compute/v1/projects/paloaltonetworksgcp-public/  
global/images/vmseries-byol-810
```

For an example, download the **gcp-two-tier** template from <https://github.com/PaloAltoNetworks>.

This template separates the image name (which includes the PAN-OS version) from the URL path. In `two-tier-template.py` the *image* variable expects the image name; for example: `vmseries-byol-810`. `vm-series-template.py` uses the values of `COMPUTE_URL_BASE` and `sourceImage` to build the path.

---

# Enable VM Monitoring to Track VM Changes on GCP

You can enable any firewall that runs PAN-OS 9.0 (virtual or physical) to monitor application workloads deployed on Google Compute Engine instances. In this procedure you manually log in to the firewall to enable VM monitoring. If you want to use the Panorama plugin for GCP to configure VM Monitoring, see [Configure VM Monitoring with the Panorama Plugin for GCP](#).

VM Monitoring enables you to monitor a predefined set of metadata elements or attributes on the VM-Series firewall. In the [PAN-OS 9.0 Administrator's Guide](#), see [Attributes Monitored on Virtual Machines in Cloud Platforms](#).

With an awareness of virtual machine adds, moves, and deletes within a Google VPC, you can create Security policy rules that automatically adapt to changes in your application environment. As you deploy or move virtual machines, the firewall collects attributes (or metadata elements). You can use this metadata for policy matching and to define Dynamic Address Groups (see [Use Dynamic Address Groups to Secure Instances Within the VPC](#)).

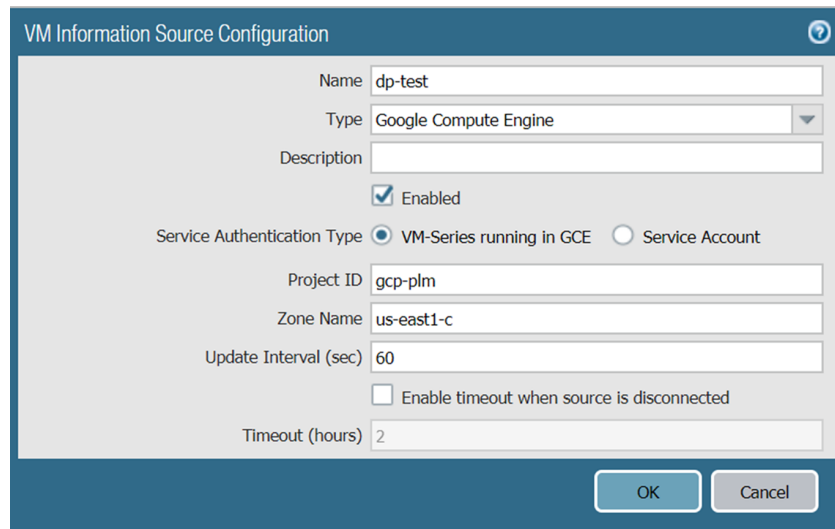
You can configure up to ten VM information sources on each firewall or on each virtual system on a firewall capable of multiple virtual systems. Information sources can also be pushed using Panorama templates.

To perform VM monitoring, you must have the IAM role Monitoring Metric Writer.

**STEP 1** | Log in to your deployed firewall.

**STEP 2** | Enable VM Monitoring.

1. Select **Device > VM Information Sources**.
2. **Add** a VM information source and enter the following information:
  - Specify a **Name** to identify the instance that you want to monitor.
  - Select the Google Compute Engine **Type**.
  - Select **Enabled**.
  - Choose the **Service Authentication Type**.
    - If you choose **VM-Series running in GCE**, you are authenticating with the default service account generated when an instance is created. This is part of the instance metadata.
    - If you want to monitor from a firewall outside the current project, choose **Service Account**. You must upload the [service account](#) credentials in JSON format. See [Creating and Managing Service Account Keys](#).
  - (**Optional**) Modify the **Update interval** to a value between 5-600 seconds. By default the firewall polls every 5 seconds. The API calls are queued and retrieved every 60 seconds—an update takes up to 60 seconds plus the configured polling interval.



VM Information Source Configuration

Name: dp-test

Type: Google Compute Engine

Description:

☒ Enabled

Service Authentication Type: ☒ VM-Series running in GCE ☐ Service Account

Project ID: gcp-plm

Zone Name: us-east1-c

Update Interval (sec): 60

☐ Enable timeout when source is disconnected

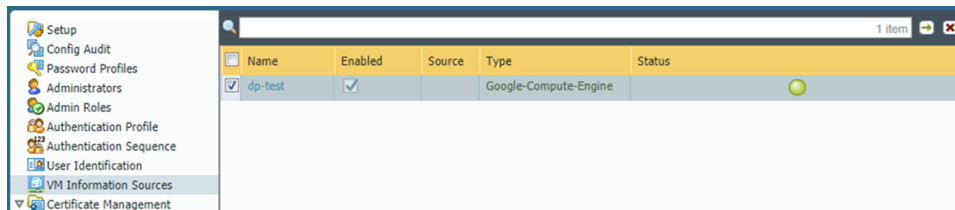
Timeout (hours): 2

OK Cancel

- (Optional) To change the number of hours before timeout, check **Enable timeout when the source is disconnected** and enter the Timeout (in hours) before the connection to the monitored source is closed (range is 2 to 10; default is 2).

If the firewall cannot access the host and the specified limit is reached, the firewall closes the connection to the source.

- Click **OK** and **Commit** your changes.



Name	Enabled	Source	Type	Status
dp-test	<input checked="" type="checkbox"/>		Google-Compute-Engine	<span style="color: green;">●</span>

### STEP 3 | Verify the connection status.

If the connection status is pending or disconnected, verify that the source is operational and that the firewall is able to access the source. If you use a port other than the Management (MGT) port for communicating with the monitored source, then you must change the service route (select **Device > Setup > Services**, click **Service Route Configuration**, and modify the **Source Interface** for the **VM Monitor** service).



---

# Use Dynamic Address Groups to Secure Instances Within the VPC

In a dynamic environment such as the Google® Cloud Platform (GCP™), where you launch new instances on demand, the administrative overhead in managing Security policy can be cumbersome. Using [use dynamic address groups in policy](#) enables agility and prevents disruption in services or gaps in protection.

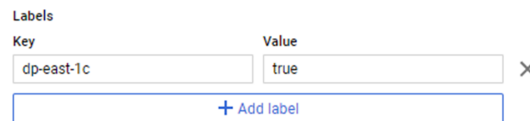
This workflow assumes that you have deployed the VM-Series firewall, configured some applications on instances, and enabled Google Stackdriver monitoring.

**STEP 1 |** Configure the firewall to monitor the VPC.

**STEP 2 |** Label instances in the VPC.

A label is a name-value pair. You can label resources from the Google Cloud Console, from Google API calls, or from the Google Cloud Shell. In this task we are labeling instances; however, labels can be applied to many resources, as described in [Labeling Resources](#).

You can also add labels from the Instance browser.

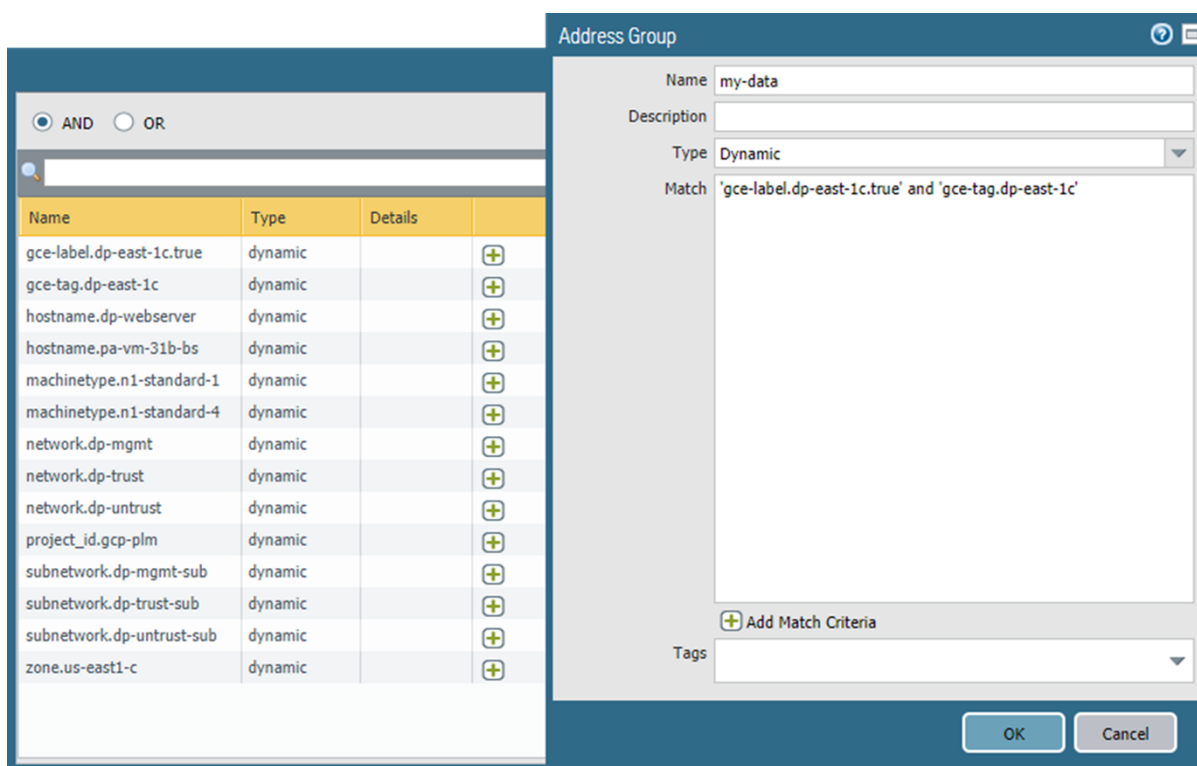


The screenshot shows a 'Labels' section with two input fields: 'Key' containing 'dp-east-1c' and 'Value' containing 'true'. To the right of the 'Value' field is a close button (X). Below these fields is a button labeled '+ Add label'.

The labels you create support your strategy for differentiating your resources in ways that are useful to your Security policy.

**STEP 3 |** Create a dynamic address group on the firewall.

1. Select **Objects > Address Groups**.
2. **Add** a dynamic address group and specify a **Name** and a **Description**.
3. Set **Type** to **Dynamic**.
4. Define the match criteria.
  1. **Add Match Criteria** and select the **And** operator.
  2. Select the attributes to filter for or to match against.



5. Click **OK**.
6. Click **Commit**.

#### STEP 4 | Use the dynamic address group in a Security policy rule.

Create a rule to allow internet access to any web server that belongs to the dynamic address group called my-data.

1. Select **Policies > Security**.
2. **Add** a rule and a **Name** for the rule and verify that the **Rule Type** is **universal**.
3. In the **Source** tab, add trust as the **Source Zone**.
4. In the Source Address section, **Add** your new my-data group.
5. In the **Destination** tab, add untrust as the **Destination Zone**.
6. In the **Service/URL Category** tab, verify that the service is set to **application-default**.
7. In the **Actions** tab, set the **Action** to Allow.
8. In the Profile Settings, set the **Profile Type** to **Profiles** and then attach the default profiles for Antivirus, Anti-Spyware, and Vulnerability Protection.
9. Click **OK**.
10. Click **Commit**.

#### STEP 5 | Verify that members of the dynamic address group are populated on the firewall.

Policy will be enforced for all IP addresses that belong to this address group and that are displayed here.

1. Select **Policies > Security** and select the rule.
2. Select **Inspect** from the drop-down. You can also verify that the match criteria is accurate.
3. Click **more** to verify that the list of registered IP addresses is displayed.

---

# Enable Google Stackdriver Monitoring on the VM Series Firewall

A VM-Series firewall on a Google® Compute Engine instance can publish custom PAN-OS metrics to Google Stackdriver. These metrics allow you to assess performance and usage patterns so that you can manage your firewall resources accordingly.

- [Google Stackdriver Permissions](#)
- [Enable Google Stackdriver](#)

## Google Stackdriver Permissions

Authentication requirements vary based on whether you can use the default service account to authenticate or need to use Google APIs to authenticate.

You can authenticate in two ways:

- **Use the default service account for the VM-Series firewall instance**—If you are using the Google Cloud Platform (GCP™) Console, then you logged in with your email address and can access the instance based on whatever permissions or roles the project administrator assigned to your account.
- **Use IAM permissions and the Google APIs**—If you use the Google SDK APIs and [gcloud](#), then you must call the APIs to authenticate. You typically use the Google SDK when you want to manage the firewall from a command line or you want to run a script to configure the firewall.

Every Google Compute Engine instance created with the Google Cloud Console or the `gcloud` command line tool has a default service account with the name in email address format:

```
<project-number>-compute@developer.gserviceaccount.com
```

To see the service account name for the firewall instance, view the instance details and scroll to the bottom (refer to the [Compute Engine default service account](#)).

The default service account can manage authentication for monitoring VMs in the same project as a VM-Series firewall.

- [Access scopes](#) allow the firewall to initiate API calls to monitor VMs in a Google Cloud project.
- You don't need to access the Google APIs unless one of the monitored virtual machines has a custom image with applications that require Google APIs.

If you want to set up monitoring from a physical firewall or from a VM-Series firewall in a different project, you must use the Google APIs to authenticate. There are two prerequisites:


- Google APIs must be installed. See [Install the Panorama Plugin for GCP](#).
- Your account must have the roles Monitoring Metric Writer and Stackdriver Account Viewer.

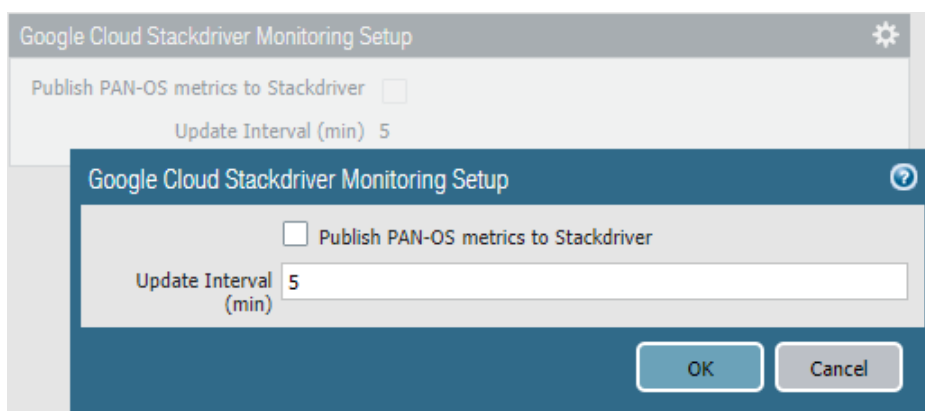
## Enable Google Stackdriver

For a description of the PAN-OS metrics that you can publish to Google Stackdriver, see [Custom PAN-OS Metrics Published for Monitoring](#).

**STEP 1** | Push PAN-OS metrics from a VM-Series firewall on a Google Compute Engine instance to Stackdriver.

1. Log in to the web interface on the VM-Series firewall.

2. Select **Device > VM-Series**. Under Google Cloud Stackdriver Monitoring Setup, click the Edit cog .
1. Check **Publish PAN-OS metrics to Stackdriver**.



2. Set the **Update Interval** (range is 1 - 60 minutes; default is 5). This is the frequency at which the firewall publishes the metrics to Stackdriver.
3. Click **OK**.
3. **Commit** your changes.

Wait until the firewall starts to publish metrics to Stackdriver before you configure alarms for PAN-OS metrics.

#### STEP 2 | Verify that you can see the metrics on Stackdriver.

1. In the Google Cloud Console, select **Products and Services > Monitoring**.
2. In Stackdriver, choose **Resources > Metrics Explorer**.
3. In the Find resource type and metric section, enter **custom** in the search field to filter the PAN-OS metrics.

#### STEP 3 | Configure alerts and actions for PAN-OS metrics on Stackdriver. See Monitoring [Quickstart for Google Compute Engine](#) and Stackdriver [Introduction to Alerting](#).

---

# VM Monitoring with the Panorama Plugin for GCP

The Panorama plugin for Google Cloud Platform (GCP) enables you to create a VM monitoring configuration that authenticates with a GCP project and monitors VM-Series firewalls and other VMs deployed within it. Once you establish a connection to your project, the plugin can retrieve tags from GCP. Tags can be predefined attributes, user-defined labels for VMs, and user-defined network tags (see [Review and Create Tags](#)).

The Panorama plugin for GCP retrieves the internal and external IP addresses from running VMs, and periodically retrieves IP-to-tag mappings from VMs in connected GCP VPCs. You can use tags to organize VMs into dynamic address groups, and then reference your tags in Security policy rules that allow or deny traffic to specific VM IP addresses. To consistently enforce Security policy, you can then push rules to your VM-Series firewalls.

- [Configure VM Monitoring with the Panorama Plugin for GCP](#)

## Configure VM Monitoring with the Panorama Plugin for GCP

This topic describes the steps to prepare your GCP assets for VM monitoring, reviews the Panorama elements that must be in place, and describes how to configure VM Monitoring in the Google Cloud Platform plugin on Panorama.

- [Configure GCP Assets for VM Monitoring](#)
- [Configure VM Monitoring with the Panorama Plugin for GCP](#)
  - [Prepare Panorama to Configure VM Monitoring](#)
  - [Install the Google Cloud Platform Plugin on Panorama](#)
  - [Set Up VM Monitoring](#)

## *Configure GCP Assets for VM Monitoring*

This topic assumes you followed the instructions in [Set Up the VM-Series Firewall on Google Cloud Platform](#) when you deployed PAN-OS VMs.

### **Review IAM Roles**

Ensure that you have the following minimum permissions for VM Monitoring tasks:

- Create a [service account](#) for your project: Project [owner](#) or [editor](#).

Service account creation cannot be automated. If you do not have permission to create a service account you can ask an administrator to create it and assign an appropriate role to you.
- View your service account: read-only.
- View PAN-OS VMs deployed from the Google Marketplace: [Compute viewer](#).
- Assign a user-defined tag to an instance: Project [owner](#), [editor](#) or [Instance Admin](#).

### **Create a Service Account**

Before you use the GCP plugin on Panorama to configure VM Monitoring, you must create a [service account](#) that grants permissions to access your GCP project, VM-Series firewalls deployed within it, any other VMs that you want Panorama to manage, and related networks and subnetworks. The GCP plugin for Panorama retrieves [pre-defined attributes](#) for Google assets, [user defined VM labels](#), and [user-defined network tags](#).

---

Every project has a [default](#) service account that was automatically created when the project was created. If you create a separate service account for VM Monitoring you have greater control users and their roles. You can have up to 100 service accounts per project.

**STEP 1 |** In the Google Cloud Platform console, select the project you want to monitor.

**STEP 2 |** Select **IAM & Admin > Service accounts** and choose **Create Service Account**.

Enter the service account name and description, and click **Create**.

**STEP 3 |** Choose a role and select an appropriate access level.

You can create multiple roles.

**STEP 4 |** Grant specific users permission to access this service account. Select users from the **Permissions** column on the right to give them permission to access the roles in the previous step.

**STEP 5 |** (Optional) Create a key to authenticate with the Google Cloud CLI to access VM-Series firewalls, networks, and other VMs associated with this service account.

The JSON format for the generated key is as follows:

```
{
  "type": "service_account",
  "project_id": "gcp-xxx",
  "private_key_id": "252e1e7a2e9c84b5d4dbb6195b1de074594b6499",
  "private_key": "-----BEGIN PRIVATE KEY-----
\nMIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDAd0i+RMKCtrsO
\n4KHnzTAPrgoBjRgpjyNcvQmdUqHr\n-----END PRIVATE KEY-----\n",
  "client_email": "dlp-vm-monit-svc-acct@gcp-xxx.iam.gserviceaccount.com",
  "client_id": "108932514695821539229",
  "auth_uri": "https://accounts.google.com/o/oauth2/auth",
  "token_uri": "https://oauth2.googleapis.com/token",
  "auth_provider_x509_cert_url": "https://www.googleapis.com/oauth2/v1/certs",
  "client_x509_cert_url": "https://www.googleapis.com/robot/v1/metadata/x509/dlp-vm-monit-svc-acct%40gcp-xxx.iam.gserviceaccount.com"
}
```

The key is downloaded automatically. Be sure to store it in a secure location.

## Review and Create Tags

In this topic “tag” is a general term for predefined [attributes](#), user-defined [labels](#), and user-defined network [tags](#).

- Predefined tags ([attributes](#)) are automatically created for Google VMs. When you configure VM Monitoring you can choose to monitor all 8 of the predefined attributes, or you can create a customized list of attributes to monitor.
- You can define your own tags for VM [labels](#) and network [tags](#).

Tag VMs and networks so that you can identify and group them so that you can structure rules to enforce Security policy. You can tag any VM deployed in your Google project—for example, a VM-Series firewall, a web server, an application server, or a load balancer.

- Tags must be associated with a VM. This also applies to networks and subnetworks.
- If there are multiple IP addresses associated with an instance (for example if you tagged the VM-Series firewall trust and untrust interfaces), Panorama generates multiple sets of tag information.

---

## Predefined Attributes

The Google Cloud Platform plugin for Panorama retrieves the following predefined tags from any managed VM.

- **Project ID**—For example: google.project-id.myProjectId.

To find your project information in the Google console, select your project, then select **IAM & Admin > Settings**.

- **Service account**—Your [service account](#) in the form of an email address. For example: google.svc-accnt.sa-name@project-id.iam.gserviceaccount.com.

To find your [Service account](#), view the VM instance details.

- **VPC name**—The name of the [VPC](#) network for a managed VM. For example: google.vpc-name.myvnet.
- **Subnet name**—The name of a [subnet](#) you created for a managed VM interface. For example, for the VM-Series firewall untrust interface, the name of the subnet you created for the untrust interface: google.subnet-name-untrust.web.
- **OS SKU**—The operating system you chose when you deployed the managed VM. For example: google.os-sku.centos-7.



*This attribute is not supported if the VM uses a custom image.*

- **Google zone**—The [zone](#) you selected when you deployed the VM. For example: google.zone.us-east1-c.
- **Google region**—The [region](#) containing the zone you selected. For example: google.region.us-east1.
- **Instance group name**—For example: google.instance-group.myInstanceGroup. To view or create an [instance group](#) in the Google console, select **Compute Engine > Instance Group**.

## User-defined Labels

Panorama uses up to 16 user-defined labels. If you have more than 16 labels, Panorama sorts your user-defined labels alphabetically and uses the first 16 tags.

Review the Google [requirements](#) for label key-value pairs: Keys have a minimum length of 1 character and a maximum length of 63 characters, and cannot be empty. Values can be empty, and have a maximum length of 63 characters.

To create or view labels in the GCP console, go to **Compute Engine > VM Instances** and select **Show Info Panel**. Select one or more VMs and in the **Info Panel**, select **Labels**. Click **+Add a label**, add a key and value, and click **Save**.

## User-defined Network Tags

Panorama uses up to 8 user-defined network tags. If you have more than 8 tags, Panorama sorts your user-defined labels alphabetically and uses the first 8 tags.

Note that Google [limits](#) network tags as follows:

- Maximum 63 characters per tag.
- You can use lowercase letters, numbers, and dashes; a tag must start with a lowercase letter, and end with a number or a lowercase letter.

To create or view network tags in the GCP console, go to **Compute Engine > VM Instances** and select an instance. **Edit** the instance, and scroll down to **Network Tags**, enter tags (separated by commas), and **Save**. See [Configuring Network Tags](#).

## Configure VM Monitoring with the Panorama Plugin for GCP

After you [tag your GCP assets](#) and create a [service account](#), make your assets available to Panorama so you can set up VM monitoring.

---

## Prepare Panorama to Configure VM Monitoring

Follow these steps to enable Panorama to manage and monitor your GCP assets. Any VM deployed in GCP can be a managed device in Panorama.

**STEP 1** | In Panorama, add the VM-Series firewalls and other VMs associated with your GCP project as [managed devices](#).

**STEP 2** | [Add a Device Group](#) and assign managed devices to it. A Device Group is a group of firewalls or virtual systems that you want to manage as a group.



*A VM can be a member of only one Device Group  
. Plan your Device Groups carefully.*

**STEP 3** | [Add a template](#). Name the template and accept the default VPC.

**STEP 4** | [Add a template stack](#). **Add** the stack, **Add** the template you just created, and select your devices.

**STEP 5** | Commit the changes.

## Install the Google Cloud Platform Plugin on Panorama

**STEP 1** | Download the `gcp-2.0.0` plugin image from the [Google Cloud Platform Plugin Beta](#) site.



*You must be a member of the Palo Alto Networks Live community to download the image.  
Contact if you have questions.*

**STEP 2** | Select **Panorama > Plugins**, click **Upload**, and browse to select the plugin image. When the download is complete, click **OK**.

If your Panorama appliances are in a high availability configuration, you must manually install the same version of the Google plugin on both Panorama peers.



*Configure the Google plugin on the active Panorama peer only. On commit, the configuration syncs to the passive Panorama peer. Only the active Panorama peer polls Google VMs you have configured for VM Monitoring.*

## Set Up VM Monitoring

**STEP 1** | Log in to the Panorama web interface and select **Panorama > Google Cloud Platform**.

**STEP 2** | Set up VM monitoring.

1. Configure general settings.

1. Select **Panorama > Google Cloud Platform > Setup > General**. To edit the settings, click the gear.

- Check **Enable Monitoring** to permit VM monitoring on all projects for which you configure a service account.
- Enter the **Monitoring Interval** in seconds. This is the length of time between tag retrieval events.

2. **Add** a notify group. A notify group is a list of Device Groups to which Panorama pushes IP-address-to-tag mappings and updates.



*A project can have only one notify group.*



1. Select **Panorama > Google Cloud Platform > Setup > Notify Groups** and click **Add**.
2. Enter a **Name** to identify the group of firewalls to which Panorama pushes the VM information (IP address-to-tag mappings) it retrieves.
3. Select the **Device Groups** to which Panorama will push the VM information (IP address-to-tag mappings) retrieved from your project. The VM-Series firewalls use the update to determine the current member list for [Dynamic Address Groups](#) referenced in Security policy.



*Plan your Device Groups carefully.*

4. Select predefined or custom tags.
  - **Select All 8 Predefined Tags**—Choose this option to select all predefined attributes (tags).
  - **Custom Tags**—Choose this option to create tag lists for predefined attributes, user-defined labels, and user-defined network tags.
5.
  - Make sure to include all relevant Device Groups in a single notify group.
  - If you want to deregister the tags that Panorama has pushed to a firewall included in a notify group, you must delete the monitoring definition.
  - To register tags to all virtual systems on a firewall enabled for multiple virtual systems, you must add each virtual system to a separate Device Group on Panorama and assign the Device Groups to the notify group. Panorama will register tags to only one virtual system, if you assign all the virtual systems to one Device Group.
3. **Add** a GCP Service Account Credential.
  - Name the service account credential.
  - (Optional) Enter a description of the service account.
  - **Browse** to upload the JSON file generated when you [created the service account](#).



*You can only use a service account once. Do not create multiple credentials from a single JSON file.*

### STEP 3 | Create a **Monitoring Definition**.

A monitoring definition consists of the service account credential for your project and a notify group. All the networking assets in your project are monitored, and the tags retrieved are pushed to the Device Groups you list in your monitoring definition. When you add a new monitoring definition, it is enabled by default.



*A project can have only one monitoring definition, and a monitoring definition can include only one notify group.*

1. Select **Panorama > Google Cloud Platform > Monitoring Definition** and click **Add**.
2. **Name** the monitoring definition.
3. Enter an optional **Description** for the project and assets you are monitoring.
4. Select the **Service Account** credential you created in the previous step.
5. Select a **Notify Group**.
6. **Enable** monitoring for the elements associated with this service account.

### STEP 4 | **Commit** the changes on Panorama.

Verify that the status for the Monitoring Definition displays as Success. If it fails, verify that you entered the project ID accurately and provided the correct keys and IDs for the service.

---

**STEP 5** | Verify that you can view the VM information on Panorama, and define the match criteria for Dynamic Address Groups.



*On HA failover, the newly active Panorama attempts to reconnect to Google Cloud Platform and retrieve tags for all monitoring definitions. If there is an error with reconnecting even one monitoring definition, Panorama generates a system log message:*

```
Unable to process subscriptions after HA switch-over; user-  
intervention required.
```

*If you see this error, fix the issue in Panorama. For example remove an invalid subscription or provide valid credentials, and commit your changes to enable Panorama to reconnect and retrieve the tags for all monitoring definitions. Even when Panorama is disconnected from Google Cloud Platform, the firewalls have the list of all tags that had been retrieved before failover, and can continue to enforce policy on that list of IP addresses. When you delete a monitoring definition, Panorama removes all tags associated with registered VMs. As a best practice, configure action-oriented [log forwarding to an HTTPS destination](#) from Panorama so that you can take immediate action.*

---

# Auto Scaling the VM-Series Firewall on Google Cloud Platform

The Panorama plugin for Google Cloud Platform (GCP) version 2.0.0 assists you in deploying the VM-Series firewall in GCP and enables Panorama to manage VM-Series firewalls securing VM monitoring or auto scaling deployments in GCP. Using Panorama for centralized policy and firewall management increases operational efficiency in managing and maintaining a distributed network of firewalls.

With Panorama maintaining your GCP [managed instance groups](#) you can create application enablement policies that protect and control the network.

This topic focuses on an auto scaling use case that requires Google [shared VPC](#) technology to create a common [VPC](#) network composed of a host project containing shared VPC networks and the VM-Series firewalls, and a service project containing a sample application deployment. Palo Alto networks supplies templates to help you deploy the VM-Series firewalls in the host project and deploy the sample application in the service project.

[BYOL and PAYG](#) licenses can be used for the VM-Series firewalls. During licensing, VM-Series firewall instances talk directly to the Palo Alto Networks license server.

If you choose BYOL your deployment can deactivate license instances in response to a scale-down event. When a VM-Series firewall is automatically removed, Panorama detects the firewall status and automatically deregisters the firewall.

- [Auto Scaling Components for Google Cloud Platform](#)
- [Deploy GCP Auto Scaling Templates](#)

## Auto Scaling Components for Google Cloud Platform

- [Auto Scaling Requirements](#)
- [Prepare to Deploy the Auto Scaling Templates](#)

### *Auto Scaling Requirements*

- ❑ **General Requirements**—Ensure your environment meets the basic [Requirements](#).
- ❑ **Panorama Plugin for GCP**—If you have not done so, [Install the Panorama Plugin for GCP](#).
- ❑ **Palo Alto Networks Auto Scale templates version 1.0**—Palo Alto Networks provides the templates to deploy VM-Series firewall instances in the host project and configure and deploy a sample application in a service project. See [About the Auto Scaling Templates](#) for more about the templates.

Download the templates from [GitHub](#). The zip file contains separate zip files for the firewall and application templates.

### *Prepare to Deploy the Auto Scaling Templates*

The auto scaling deployment on GCP requires a [shared VPC](#) with host and service projects that use a common [VPC](#) network. In this topology, the host project contains the networks and VM-Series firewalls that secure traffic to your applications, which are deployed in the service project.

Complete the following tasks before you deploy the auto scaling templates.

- [Prepare a Host Project and Required Service Accounts](#)
- [Configure the Panorama Plugin for Auto Scaling](#)
- [Prepare a VM-Series Firewall Bootstrap Package for Auto Scaling](#)

---

## Prepare a Host Project and Required Service Accounts

You need a host project and a service project to form the shared VPC topology that supports the firewall and application templates. You can create a new host project or prepare an existing project to act as your host.

To [set up the Shared VPC](#) an organization administrator must grant the host project administrator the Shared VPC Admin role. The Shared VPC Admin can [enable](#) a project to act as a host, and grant the Service Project Admin role to the service project administrator. Review the GCP documentation on [Administrators and IAM](#) roles.

**STEP 1 |** In the GCP console, create a GCP project to act as the host. If you want to use an existing project, skip to the next step.

To create a new project, select your organization or **No organization**, click **New Project** and fill in your project information. Note, this is your only chance to **EDIT** the project ID.



*The Google Cloud SDK must be [installed](#) and configured so that you can authenticate with your host project from the CLI. You will use the command line interface to deploy the firewall template and the application template, and to attach the service project to the host project.*

**STEP 2 |** Enable APIs and services required for auto scaling. The required APIs are:

- ☐ Cloud Pub/Sub API
- ☐ Cloud Deployment Manager API
- ☐ Cloud Storage API
- ☐ Compute Engine API
- ☐ Google Compute Engine Instance Group Manager API
- ☐ Google Compute Engine Instance Group Updater API
- ☐ Google Compute Engine Instance Groups API
- ☐ Kubernetes Engine API
- ☐ Stackdriver API
- ☐ Stackdriver Logging API
- ☐ Stackdriver Monitoring API

You can enable APIs from the [GCP console](#) or the [GCP CLI](#).

### Enable APIs from the GCP console

1. Select the host project, and from the Navigation menu, select **APIs & Services**.
2. Search for and view each required API.
3. **ENABLE** any APIs that do not display the “API enabled” status.

### Enable APIs from the CLI

1. In the CLI, view your configuration to ensure that you are in the correct project.

```
gcloud config list
```

If not, set the project as follows:

```
gcloud config set project <project-name>
```

2. Issue the following commands to enable the required APIs.

```
gcloud services enable pubsub.googleapis.com
gcloud services enable deploymentmanager.googleapis.com
gcloud services enable storage-component.googleapis.com
gcloud services enable compute.googleapis.com
gcloud services enable replicapool.googleapis.com
gcloud services enable replicapoolupdater.googleapis.com
gcloud services enable resourceviews.googleapis.com
gcloud services enable container.googleapis.com
gcloud services enable stackdriver.googleapis.com
gcloud services enable logging.googleapis.com
gcloud services enable monitoring.googleapis.com
```

3. Confirm that the required APIs are enabled.

```
gcloud services list --enabled
```

**STEP 3 |** Create a service account for deploying the VM-Series firewall, and assign the IAM roles required for auto scaling.

When you configure the firewall templates you add the email address for this service account to the VM-Series firewall .yaml file. Within the host project, the template uses credentials from this service account to create a host VPC with subnets, deploy VM-Series firewalls in the VPC, configure Stackdriver custom metrics, create a Pub/Sub topic, and more.

1. In the GCP console select **IAM & Admin > Service accounts** and select **+CREATE SERVICE ACCOUNT**.

Fill in the service account details and click **CREATE**.

2. Give the service account permission to auto-scale resources in this project.

Add the following roles:

- ☐ Compute Engine > Compute Admin
- ☐ Compute Engine > Compute Network User
- ☐ Pub/Sub > Admin
- ☐ Deployment Manager > Deployment Manager Editor
- ☐ Monitoring > Monitoring Metric Writer
- ☐ Stackdriver > Stackdriver Accounts Editor
- ☐ Storage > Storage Admin

### Service account permissions (optional)

Grant this service account access to GCP-AutoScale-KK so that it has permission to complete specific actions on the resources in your project. [Learn more](#)

Role Compute Admin	✕
Full control of all Compute Engine resources.	
Role Compute Network User	✕
Access to use Compute Engine networking resources.	
Role Editor	✕
Edit access to all resources.	
Role Pub/Sub Admin	✕
Full access to topics, subscriptions, and snapshots.	

[+ ADD ANOTHER ROLE](#)

[CONTINUE](#) [CANCEL](#)

**Continue** when you are finished adding roles.

- Click **+CREATE KEY** to create a key for the host service account.
  - (Optional) Add email addresses to grant other users or administrators access to this service account.
  - Click JSON to download the private key in JSON form.
  - Store the key in a safe location. You will need this key when you [Deploy GCP Auto Scaling Templates](#).
- Click **DONE**.

**STEP 4 |** Create a service account that a Panorama administrator can use to interact with this host project.

- In the GCP console select **IAM & Admin > Service accounts** and select **+CREATE SERVICE ACCOUNT**.
- Fill in the service account details and click **CREATE**.
- Give the service account the following roles:

- ☐ Compute Engine > Compute Viewer
- ☐ Pub/Sub > Admin

Click **CONTINUE**.

- Download the private key in JSON form, and store it in a safe location. You need this key when you [Configure the Panorama Plugin for Auto Scaling](#).

**STEP 5 |** (optional) In the CLI, ensure you can communicate with your new host project.

- In the CLI, set your project to the host project you just created.

```
gcloud set project <your-autoscale-host-project-name>
```
- Create a configuration for auto scaling. Your new configuration is automatically activated unless you disable activation.

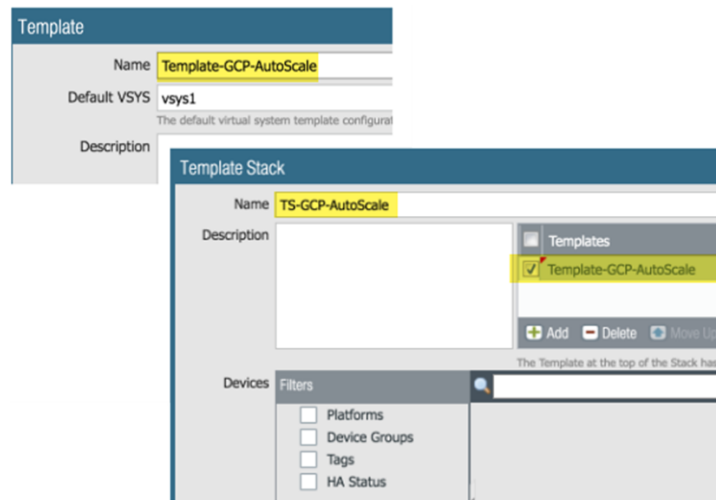
```
gcloud config configurations create CONFIGURATION_NAMEgcloud config list
```

### Configure the Panorama Plugin for Auto Scaling

In Panorama, create assets to support the auto scaling firewall deployment.

**STEP 1** | Create a Device Group to hold the VM-Series firewalls you create with the firewall template. In this example, DG-GCP-AutoScale-Firewalls.

**STEP 2** | Create a [template](#), and a [template stack](#) that includes the template, and commit the changes.



**STEP 3** | Select the template stack and add a virtual router. You must create the virtual router in the template stack to ensure that the static routes the firewall template creates are added to the virtual router.



**STEP 4** | In the template, create the ethernet1/1 (Untrust) Layer 3 interface.

Enable **DHCP Client** and **Automatically create default route pointing to default gateway provided by server** (enabled by default)

Ethernet Interface		Ethernet Interface	
Slot	Slot 1	Slot	Slot 1
Interface Name	ethernet1/1	Interface Name	ethernet1/1
Comment		Comment	
Interface Type	Layer3	Interface Type	Layer3
Netflow Profile	None	Netflow Profile	None
Config IPv4 IPv6 A		Config IPv4 IPv6 Advanced	
<b>Assign Interface To</b> Virtual Router: None Virtual System: vsys1 Security Zone: Untrust		Type: <input type="radio"/> Static <input type="radio"/> PPPoE <input checked="" type="radio"/> DHCP Client <input checked="" type="checkbox"/> Enable <input checked="" type="checkbox"/> Automatically create default route pointing to default gateway <input type="checkbox"/> Send Hostname: system-hostname Default Route Metric: 10	

**STEP 5 |** In the template, create the ethernet1/2 (Trust) Layer 3 interface.

Enable **DHCP Client** and disable **Automatically create default route pointing to default gateway provided by server**.

Ethernet Interface		Ethernet Interface	
Slot	Slot 1	Slot	Slot 1
Interface Name	ethernet1/2	Interface Name	ethernet1/2
Comment		Comment	
Interface Type	Layer3	Interface Type	Layer3
Netflow Profile	None	Netflow Profile	None
Config IPv4 IPv6 A		Config IPv4 IPv6 Advanced	
<b>Assign Interface To</b> Virtual Router: None Virtual System: vsys1 Security Zone: Trust		Type: <input type="radio"/> Static <input type="radio"/> PPPoE <input checked="" type="radio"/> DHCP Client <input checked="" type="checkbox"/> Enable <input type="checkbox"/> Automatically create default route pointing to default gateway <input type="checkbox"/> Send Hostname: system-hostname Default Route Metric: 10	

**STEP 6 |** Return to your template stack and the virtual router you created earlier. Place the untrust and trust interfaces (ethernet1/1 and ethernet1/2) in the virtual router.

Virtual Router - VR1	
Router Settings	Name: VR1
Static Routes	
Redistribution Profile	
RIP	
OSPF	
General ECMP	
<input checked="" type="checkbox"/> Interfaces <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> ethernet1/1</li> <li><input checked="" type="checkbox"/> ethernet1/2</li> </ul>	

**STEP 7 |** Add a security policy that allows web-browsing traffic from untrust to trust.



Context

Panorama

Device Group

DG-GCP-AutoScale-Firewal

Security

Pre Rules

Post Rules

Default Rules

NAT

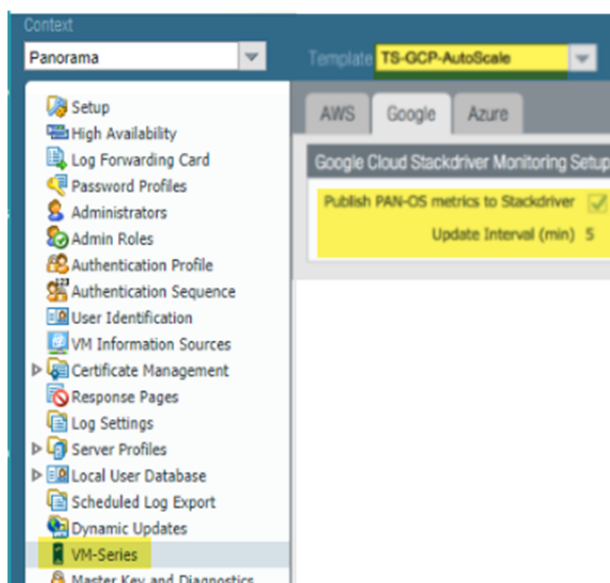
Pre Rules

					Source			Destination						
	Name	Location	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	
	allow-untrust-trust	DG-GCP-AutoScal...	none	universal	any	Untrust	any	any	any	Trust	any	web-browsing	application-d...	Allow

## STEP 8 | Configure Stackdriver for your auto scaling deployment.

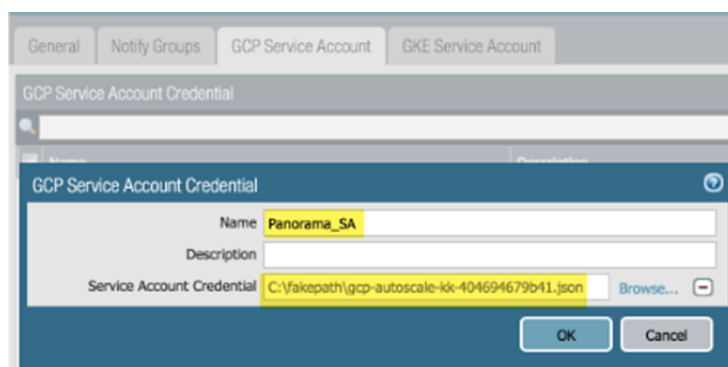
Stackdriver requires the VM-Series plugin—see [Install the Panorama Plugin for GCP](#) for instructions on viewing and installing the plugin.

1. In the **Device** context, select the template stack you created earlier from the Template drop menu.
2. Select **Device > VM-Series > Google** and click the Edit cog (⚙️). Enable **Publish PAN-OS metrics to Stackdriver**.



## STEP 9 | Set up the GCP service account for the host project.

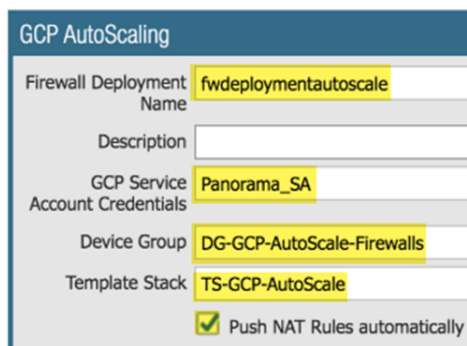
1. In the Panorama context, expand Google Cloud Platform, select **Setup**, and click **Add**.
2. Supply a name and description for the host service account you created in Step 3.
3. Upload the JSON credentials file you created in Step 3.c.



## STEP 10 | Set up auto scaling on the Panorama plugin for GCP.

1. In the Panorama context, expand Google Cloud Platform, select AutoScaling, and click **Add**.
2. Supply the Firewall Deployment Name and an optional description for the deployment.

- For the GCP Service Account Credential, supply the GCP service account name from Step 10.




The screenshot shows the 'GCP AutoScaling' configuration page. The fields are as follows:

Field	Value
Firewall Deployment Name	fwdeploymentautoscale
Description	
GCP Service Account Credentials	Panorama_SA
Device Group	DG-GCP-AutoScale-Firewalls
Template Stack	TS-GCP-AutoScale
Push NAT Rules automatically	<input checked="" type="checkbox"/>

#### STEP 11 | Obtain a Licensing API key.

You need a Licensing API key so Panorama can license and de-license managed assets.

 Only a Super User can view the Enable link and generate this key. See [How to Enable, Regenerate, Extend the Licensing API Key](#).

- On [support.paloaltonetworks.com](https://support.paloaltonetworks.com) go to **Assets > Licensing API** and click **Enable**. The key is displayed.

#### Licensing API Key

This license API key provides user license API calls. To enable this

Key : 986a2d53dcf

- Select the key and copy it.
- From the CLI, SSH in to Panorama and issue the following command, replacing <key> with the API key you copied from the support portal:

```
request license api-key set key <key>
API Key is successfully set
```

#### STEP 12 | Commit your changes.

##### Prepare a VM-Series Firewall Bootstrap Package for Auto Scaling

The firewall templates include a sample `init-cfg.txt` file. You must customize this file for your deployment.

**STEP 1** | Set up a [Google storage bucket](#) with the folders required to [Bootstrap the VM-Series Firewall on Google Cloud Platform](#). You can use an existing bootstrap package or create a new bootstrap package, for these folders.

**STEP 2** | Edit the values in the `init-cfg.txt` file to customize the file for your environment.

The firewall templates include a sample `init-cfg.txt` file.

Parameter	Value	Comment
type	dhcp-client	

Parameter	Value	Comment
op-command-modes	mgmt-interface-swap	Required in this Beta release.
hostname	<pa-vm>	Optional name you assigned when you prepared the <a href="#">host project</a> . Only required if a specific host is necessary, and dhcp-send-hostname is no.
vm-auth-key	<vmauthkey>	A key that Panorama must validate before adding a firewall as a managed device. See <a href="#">Generate the VM Auth Key On Panorama</a> .
panorama-server	<panorama-ip>	The IP address of the Panorama management device you configured in <a href="#">Configure the Panorama Plugin for Auto Scaling</a> .
tplname	<tmplstk-name>	The template stack you created in <a href="#">Configure the Panorama Plugin for Auto Scaling</a> .
dgname	<dg-name>	The name of the Device Group you created in the Panorama Plugin for GCP.
dns-primary	8.8.8.8	Your primary DNS.
dns-secondary	208.67.222.222	Your secondary DNS.
dhcp-send-hostname	yes	Leave as is.
dhcp-send-client-id	yes	Leave as is.
dhcp-accept-server-hostname	yes	Leave as is.
dhcp-accept-server-domain	yes	Leave as is.

**STEP 3** | Upload your edited `init-cfg.txt` file to the `/config` folder in your bootstrap package.

**STEP 4** | If you are using BYOL, create a text file named `authcodes` (no extension), add your auth code, and upload the file to the `/license` folder.

## Deploy GCP Auto Scaling Templates

- [About the Auto Scaling Templates](#)
- [Deploy the Firewall Template](#)
- [Prepare a Service Project](#)
- [Configure the Shared VPC](#)
- [Deploy the Application Template](#)
- [Onboard a New Application](#)

---

## About the Auto Scaling Templates

Download the Palo Alto Networks auto scaling templates from <https://github.com/PaloAltoNetworks/GCP-AutoScaling>. The zip file contains separate zips for firewall and application templates. Each zip is a template directory containing several files, but you only need to edit the YAML files.

- [Firewall Template](#)
- [Application Template](#)



### Firewall Template

The firewall directory files create VM-Series firewalls and other deployment resources. They create new networks and the familiar subnetworks for the VM-Series firewall: management, untrust, and trust. They also deploy a Cloud Pub/Sub messaging service to relay information from GCP to the Panorama plugin for GCP. With this infrastructure in place, the plugin can leverage dynamic address groups to apply security policy on inbound traffic routed to services running on GCP, and use auto scale metrics to deploy VM-Series firewalls to meet increased demand for application workload resources or to eliminate firewalls that are no longer needed.

To configure your load balancer, edit the .yaml file for an external application load balancer (ALB) or network load balancer (NLB).

- **ALB** (HTTP External Load Balancer)

To customize an ALB, edit `vm-series-fw-alb.yaml`.

HTTP external load balancer is a proxy-based load balancer that performs SNAT and DNAT on the inbound traffic from Internet. The HTTP load balancer is designed to support only the 80, 8080 and 443 TCP ports.

To support multiple applications using HTTP load balancer in load balancer sandwich architecture, we can use the GCP HTTP load balancer `urlMap` and `namedPort` to map different URLs to different ports in the load balancer. In turn, the VM-Series firewall can translate the ports to different applications, each represented by one internal load balancer per application.

- **NLB** (TCP Load Balancer)

To customize an NLB, edit `vm-series-fw-nlb.yaml`.

TCP load balancer is a non-proxy based load balancer, which means it doesn't perform NATing on inbound traffic from the Internet.

TCP load balancer in GCP allows adding multiple frontend IP addresses with an arbitrary port, making it possible to support multiple applications.

Another advantage of TCP load balancer is that the original client IP address is preserved, which is desirable for some applications.

### Application Template

The application directory provide a sample application. You configure the internal load balancer (ILB) to enable your application servers to subscribe to the Pub/Sub service and communicate with your VM-Series firewalls and the GCP plugin on Panorama.

To customize the application template, edit `apps.yaml`.

## Deploy the Firewall Template

Edit the [Firewall Template](#) from the host project.

**STEP 1** | Edit the `vm-series-fw-nlb.yaml` or `vm-series-fw-alb.yaml` environment variables to reflect your cloud environment.

This sample is for the NLB.

```
properties:
  region: us-east1
  zones:
  - us-east1-b
  # Do not modify the lb-type field.
  lb-type: nlb
  cloud-nat: yes
  forwarding-rule-port: 80
  ssl-certificate-url: 'https://www.googleapis.com/compute/v1/projects/wli-autoscale/global/sslCertificates/wilson4-crt'
```

```
# Only one app is allowed
urlPath-namedPort-maps:
- appName: appl
```

```
# ssh key PUBLIC - optional
```

Before entering the private SSH key, review [SSH Key Pair](#). The autoscaling firewall template requires you to enter the value in single quotes and prepend the key with `admin:` followed by a space. This is the same convention used for the Google Marketplace template, as detailed in [SSH Key Pair](#). For example:

```
sshkey: 'admin: ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQDe0gJHd8okxPGWXsmdTdcZBJNI6ONT/NSz6INs2CNtKW
tr+MDh5W79Hn3mlV3I4k2nqkdy3+nEZLbMtlYgt3
+jSwtiR53yGHVpkoziVnJqQ9YXixirTZYNAnzWPlF6eA4XN9XF6Fnga88GsMWcy2Lv04oB5xlC
wpXDSygpaoGv4ITb9s2P4Laer3voR1SaoQumDfzadcXzzJE+9lm01
+KjTeYItjDjnHWY9r1kIAGi4WIRdM4KruQMCS5lXpT4UlwVC+K56rI+pnk5K6/Zqg3XMJP13PD
oTKXL8t0SRnOKaKV73NR5KnfpsNfwGxG8aQtEkeMC2IxX+6WOnRf/N4K3
yourname@apt1.paloaltonetworks.local'
```

```
bootstrap-bucket: bootstrap-autoscale
```

```
image: vmseries-byol-814
machine-type: n1-standard-4
```

For the service-account, supply the email address for the [host project](#) service account you created earlier ([step 3](#)).

```
service-account: sa-pan@gcp-autoscale-kk.iam.gserviceaccount.com
```

The `fw-instance-tag` value will be the managed instance group name in the deployment.

```
fw-instance-tag: vm-series-fw
```

Choose one metric for auto scaling. Possible values are: `panSessionActive`, `panSessionUtilization`, `DataPlaneCPUUtilizationPct`, `DataPlanePacketBufferUtilization`, or `panSessionUtilization`.

```
metric: custom.googleapis.com/VMSeries/panSessionActive
max-size: 2
min-size: 1
target-type: GAUGE
util-target: 100
```

```
# Greenfield deployment
mgmt-network-cidr: 172.22.2.0/24
untrust-network-cidr: 172.22.1.0/24
trust-network-cidr: 172.22.3.0/24
mgmt-network-access-source-range:
- 199.167.54.229/32
- 199.167.52.5/32
mgmt-network-access-ports:
- 22
- 443
```

## STEP 2 | Deploy the firewall template.

```
gcloud deployment-manager deployments create <firewall-deployment-name>  
--config vm-series-fw-nlb.yaml --automatic-rollback-on-error
```

Take note of the outputs the CLI prints after the deployment: The subnet names, the deployment name, and the Panorama Pub/Sub topic name. You need these values to configure the Shared VPC and for the application template deployment.

The firewall deployment name must be configured in the Panorama plugin for GCP auto scaling definition.

Parameter	Value	Comment
region	us-central1	<a href="https://cloud.google.com/compute/docs/regions-zones">https://cloud.google.com/compute/docs/regions-zones</a>
zones	zones- us-central1-a	If applicable, list multiple zones as follows:  zones- us-central1-a- us-central1-b- us-central1-c- us-central1-f
lb-type	nlb	Do not modify the lb-type field
cloud-nat	yes	Leave as is
forwarding-rule-port	80	
ssl-certificate-url	'https://www.googleapis.com/compute/v1/projects/wli-autoscale/global/sslCertificates/wilson4-crt'	
ssh key public		optional

Parameter	Value	Comment
sshkey	sshkey: 'admin: ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAQEA +zMI9TzqQPPTYMR2Im/ R/Jfg39PcvXr+q +es9IAeu3uhDys/<truncated>/ HT943xaWQhna2yCWPLdFI10HivhyL dphillips'	Review <a href="#">SSH Key Pair</a> . Enter the value in <code>sshkey</code> : followed by a space. This is the same convention used for the Google Marketplace template, as detailed in <a href="#">SSH Key Pair</a> .
bootstrap-bucket	bootstrap-autoscale	
image	vm-series-byol-814	The BYOL image currently available from the Google marketplace.  If you are using PAYG or another license model,
machine-type	n1-standard-4	n1-standard-4 is default for BYOL.
service-account	sa-pan@gcp-autoscale-kk.iam.gserviceaccount.com	
fw-instance-tag	vm-series-fw	
metric	custom.googleapis.com/VMSeries/ panSessionActive	You can choose only one auto scaling metric.  Possible values: panSessionActive panSessionUtilization DataPlaneCPUUtilizationPct DataPlanePacketBufferUtilization panSessionUtilization
max-size	2	
min-size	1	
target-type	GAUGE	
util-target	100	

## Prepare a Service Project

Create a separate service project, or choose an existing project, for your application.

To learn more about host and service projects in a shared VPC, see the [Shared VPC Overview](#), and review the [Administrators and IAM](#) roles. A host project administrator must have the proper role to [set up the Shared VPC](#), make the application project a service project for the host project. See the instructions in [Provisioning Shared VPC](#).

Create a service account for deploying an application and assign the IAM roles required for auto scaling.

1. In the GCP console select **IAM & Admin** > **Service accounts** and select **+CREATE SERVICE ACCOUNT**.

Fill in the service account details and **CREATE**.

2. Give the service account permissions to auto scale resources in this project.

Add the following roles:

- ☐ Compute Engine > Compute Admin
- ☐ Compute Engine > Compute Network User
- ☐ Project > Editor
- ☐ Pub/Sub > Admin

**Continue** when you are finished.

3. (Optional) Add email addresses to grant users or administrators access to this application.
4. Download a JSON file with a private key.  
Click **+CREATE KEY**, select JSON, click **CREATE**, and store the key in a secure location.
5. Click **DONE**.

## Configure the Shared VPC

After the firewall template is deployed in the host project, configure the service project that supports your applications. An administrator with Shared VPC credentials performs these tasks from the host project. To understand more about the host project and service projects in the context of shared VPC, see the [Shared VPC Overview](#).

**STEP 1** | Create a shared VPC using the Trust VPC created when you deployed the firewall template.

Set up Shared VPC for the host (firewall) project:

```
gcloud compute shared-vpc enable HOST_PROJECT_ID
```

**STEP 2** | Make the application project a service project for the host project.

Add the service account email (<project number>@cloudservices.gserviceaccount.com) from Service/application project administrator as a member in host project with below role:

- Compute Admin
- Compute Network User
- Pub/Sub Admin

**STEP 3** | Attach the service/application project to the host project.

```
gcloud compute shared-vpc associated-projects add SERVICE_PROJECT_ID --host-project HOST_PROJECT_ID
```

Additional options are available to share only specific subnets, rather than all subnets in the host project.

## Deploy the Application Template

The Service project administrator deploys the [Application Template](#) from the service project.

**STEP 1** | Create a separate application project (service project) to deploy the application.

**STEP 2** | Prepare the `apps.yaml` file.



```
properties:
  host-project: gcp-autoscale-host
  fw-deployment-name: fw-template-9
  region: us-east1
  zones:
    - us-east1-b
    - us-east1-c
```

**STEP 3** | Deploy a new application with the application template and define a label for the named port.

```
gcloud deployment-manager deployments create <your-template>--config
apps.yaml --labels named-port=82--automatic-rollback-on-error
```

## *Onboard a New Application*

To secure an application you have deployed using an external load balancer and an autoscaled VM-Series firewall deployment, follow these steps. For every application you must supply the application name, the named ports, and the path.

**STEP 1** | Prepare new named port and URL path to be added to the HTTP external load balancer created when you [deployed the firewall template](#).

**STEP 2** | Update all instance groups named-ports with an additional service name and port values for app2 and app3.

```
gcloud compute instance-groups set-named-ports
fw-template2-fw-igm-us-east1-b
--zone us-east1-b
--named-ports=app1:80,app2:81,app3:82

gcloud compute instance-groups set-named-ports
fw-template2-fw-igm-us-east1-c
--zone us-east1-c
--named-ports=app1:80,app2:81,app3:82
```

**STEP 3** | Create a new http-health-check.

```
gcloud compute backend-services create fw-template2-backend-app3
--protocol="HTTP"
--port-name=app3
--http-health-checks=fw-template2-healthcheck-app3
--load-balancing-scheme="EXTERNAL"
--global
```

**STEP 4** | Create a new backend service with the port-name created earlier on the HTTP external load balancer.

```
gcloud compute backend-services create fw-template2-backend-app3
--protocol="HTTP" --port-name=app3
--http-health-checks=fw-template2-healthcheck-app3 --load-balancing-
scheme="EXTERNAL"
--global
```

Check to see if it is visible.

```
gcloud compute backend-services list
```

**STEP 5** | Edit url-maps and add new path rule. For example:

```
- paths:
  - /app3
  - /app3/*service:
    https://www.googleapis.com/compute/v1/projects/stellar-cumulus-95806/global/backendServices/fw-template2-backend-app3
```

```
gcloud compute url-maps edit fw-template2-ext-loadbalancer
```

**STEP 6** | To secure this application with the VM-Series firewall, manually trigger the pub/sub message through the gcloud CLI. This sends a message to the topic created in the firewall template.

```
gcloud pubsub topics publish <template-path>/fw-template-4-gcp-autoscale-host-panorama-apps-deployment
--attribute ilb-ip=172.22.3.6,app-deployment-name=fw-template-4-app1,
  ilb-port=80,named-port=80,fw-deployment-name=fw-template-4,
  host-project=gcp-autoscale-host,type=ADD-APP
--message "ADD-APP"
```



After you onboard an application you can view it in the Panorama plugin for GCP. Select Panorama > Google Cloud Platform > Autoscaling > Show Status. The Details column displays if you have deployed an application. Click the Status link. NAT Rule Programmed is True if a NAT rule exists, and Protected is True when an application has successfully onboarded.

**STEP 7** | To update application attributes, such as ilb-ip, ilb-port, or named-port, issue the pubsub command:

```
gcloud pubsub topics publish <template-path>/fw-template-4-gcp-autoscale-host-panorama-apps-deployment
--attribute ilb-ip=172.22.3.7,app-deployment-name=<your-app>,
  ilb-port=81,named-port=80,w-deployment-name=fw-template-4,
  fhost-project=gcp-autoscale-host,type=UPDATE-APP
--message "UPDATE-APP"
```

**STEP 8** | To stop securing the application, issue the following command:

```
gcloud pubsub topics publish <template-path>/fw-template-3-vmseries-dev-242318-panorama-apps-deployment
--attribute ilb-ip=172.22.3.20,app-deployment-name=fw-templ-3-app-1,
  ilb-port=80,named-port=80,fw-deployment-name=<your-deployment>,
  type=DEL-APP
--message "DEL-APP"
```