FortiOS - GCP Cookbook

Version 6.2

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET COOKBOOK
http://cookbook.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdocs@fortinet.com

June 28, 2019
FortiOS 6.2 GCP Cookbook
01-620-543925-20190628

TABLE OF CONTENTS

About FortiGate-VM for GCP **4**
Machine type support 4
Models 5
Licensing 6
Order types 6
Creating a support account 7
Registering and downloading licenses 7
Deploying FortiGate-VM on Google Cloud Marketplace **9**
Initial deployment 9
Registering and downloading your license 11
Connecting to the FortiGate-VM 12
Deploying FortiGate-VM on Google Cloud Compute Engine **14**
Obtaining the deployment image 14
Uploading the FortiGate deployment image to Google Cloud 14
Creating the FortiGate deployment image 15
Deploying the FortiGate-VM instance 17
Connecting to the FortiGate-VM 21
Configuring Google Cloud firewall rules 26
Configuring the second NIC on the FortiGate-VM 28
Deploying FortiGate-VM using Google Cloud SDK **30**
Using the Google Cloud SDK to deploy FortiGate-VM 30
Bootstrapping FortiGate at initial boot-up 33
High availability for FortiGate-VM on GCP **35**
Deploying FortiGate-VM HA on GCP in one zone 36
Deploying FortiGate HA using the GCP GUI 37
Deploying FortiGate HA using the Google Cloud command interface 43
Deploying FortiGate-VM HA on GCP between multiple zones 45
Security Fabric Connector Integration with GCP **50**
Configuring GCP SDN Connector on FortiGate for GCP 50
GCP Kubernetes (GKE) Fabric connector 52
Checking metadata API access 52
Creating a GCP service account 54
Creating an Address 55
Creating a firewall policy 57
Troubleshooting GCP SDN Connector 58
Deploying auto scaling on GCP **60**
Change log **63**

About FortiGate-VM for GCP

By combining stateful inspection with a comprehensive suite of powerful security features, FortiGate Next Generation Firewall technology delivers complete content and network protection. This solution is available for deployment on Google Cloud Platform (GCP).

There are several ways to deploy FortiGate-VM on GCP:

Deployment method	Description
Google Cloud Marketplace	The FortiGate-VM listed on Google Cloud marketplace deployment currently supports one-arm mode (one network interface) only. See Deploying FortiGate-VM on Google Cloud Marketplace on page 9.
Google Cloud Compute Engine	Deploy a FortiGate-VM instance on Google Cloud Compute Engine from the custom image without using the Google Cloud Platform marketplace. See Deploying FortiGate-VM on Google Cloud Compute Engine on page 14. You must deploy FortiGate in this method when: • FortiGate is required to be deployed inline across multiple networks and multiple network interfaces must be assigned to the instance. The FortiGate marketplace launcher does not support assigning multiple network interfaces to a FortiGate instance. (This will be supported in the future). Google Cloud also does not allow changing the number of network interfaces after deploying VM instances. • You do not want to use the Google marketplace launcher. For example, you may want to use this deployment method if your organization does not allow you to browse marketplace websites in its IT policy.
Google Cloud SDK	Deploy a FortiGate-VM (BYOL) instance by using the Google Cloud SDK on your local PC. This is a method of deploying FortiGate-VM on GCP outside of the marketplace product listing and without creating an instance on the Google Cloud Compute Portal. This method also allows assigning multiple network interfaces to the VM instance. See Deploying FortiGate-VM using Google Cloud SDK on page 30.

Machine type support

FortiGate for GCP can be deployed as VM instances. Supported machine types may change without notice. Currently FortiGate supports standard machine types, high-memory machine types, and high-CPU machine types with minimum 1 vCPU and 3.75 GB of RAM and maximum 96 vCPUs and 624 GB of RAM in the predefined machine type lineup. You can also customize the combination of vCPU and RAM sizes within this range. See here for more details on predefined machine types.

Latest supported machine types can be seen under machine type selection if you try to launch FortiGate from the marketplace listing or Compute Engine portal.

Models

FortiGate-VM is available with different CPU and RAM sizes and can be deployed on various private and public cloud platforms. The following table shows the models conventionally available to order, also known as bring your own license (BYOL) models. See Order types on page 6.

Model name	vCPU	
	Minimum	Maximum
FG-VM01 or 01v	1	1
FG-VM02 or 02v	1	2
FG-VM04 or 04v	1	4
FG-VM08 or 08v	1	8
FG-VM16 or 16v	1	16
FG-VM32 or 32v	1	32
FG-VMUL or ULv	1	Unlimited

The v-series does not support VDOM by default. To run VDOM on v-models, you must purchase additional VDOM licenses. You can add and stack VDOMs up to the maximum supported number after initial deployment.

Generally there are RAM size restrictions to FortiGate BYOL licenses. However, these restrictions are not applicable to GCP deployments. Any RAM size with certain CPU models are allowed. Licenses are based on the number of CPUs only.

Previously, platform-specific models such as FortiGate for GCP with a GCP-specific orderable menu existed. However, the common model is now applicable to all supported platforms.

For information about each model's order information, capacity limits, and adding VDOM, see the FortiGate-VM datasheet.

The primary requirement for the provisioning of a virtual FortiGate may be the number of interfaces it can accommodate rather than its processing capabilities. In some cloud environments, the options with a high number of interfaces tend to have high numbers of vCPUs.

The licensing for FortiGate-VM does not restrict whether the FortiGate can work on a VM instance in a public cloud that uses more vCPUs than the license allows. The number of vCPUs indicated by the license does not restrict the FortiGate

from working, regardless of how many vCPUs are included in the virtual instance. However, only the licensed number of vCPUs process traffic and management. The rest of the vCPUs are unused.

License	1 vCPU	2 vCPU	4 vCPU	8 vCPU	16 vCPU	32 vCPU
FGT-VM08	OK	OK	OK	OK	8 vCPUs used for traffic and management. The rest are not used.	8 vCPUs used for traffic and management. The rest are not used.

You can provision a VM instance based on the number of interfaces you need and license the FortiGate-VM for only the processors you need.

Licensing

You must have a license to deploy FortiGate for GCP. The following sections provide information on licensing FortiGate for GCP:

- Order types on page 6
- Creating a support account on page 7
- Registering and downloading licenses on page 7

Order types

On GCP, there are usually two order types: bring your own license (BYOL) and pay as you go (PAYG).

BYOL is perpetual licensing as opposed to PAYG, which is an hourly subscription available with marketplace-listed products. BYOL licenses are available for purchase from resellers or your distributors, and prices are listed in the publicly available price list which is updated quarterly. BYOL licensing provides the same ordering practice across all private and public clouds, no matter what the platform is. You must activate a license for the first time you access the instance from the GUI or CLI before you can start using various features.

PAYG has no licenses. FortiGate becomes available for use immediately after the instance is created. Term-based prices (hourly or annually) are mentioned in the marketplace product page.

In both BYOL and PAYG, cloud vendors charge separately for resource consumption on computing instances, storage, and so on, without use of software running on top of it (in this case FortiGate).

For BYOL, you typically order a combination of products and services including support entitlement. PAYG includes support, for which you must contact Fortinet Support with your customer information.

To purchase PAYG, all you need to do is subscribe to the product on the marketplace. However, you must contact Fortinet Support with your customer information to obtain support entitlement. See Creating a support account on page 7.

PAYG FortiGate instances do not support the use of virtual domains (VDOMs). If you plan to use VDOMs, deploy BYOL instances instead.

Creating a support account

FortiGate for GCP supports both PAYG and BYOL licensing models. See Order types on page 6.

To make use of Fortinet technical support and ensure products function properly, you must complete certain steps to activate your entitlement. Our support team can identify your registration in the system thereafter.

First, if you do not have a Fortinet account, you can create one at Customer Service & Support.

Registering and downloading licenses

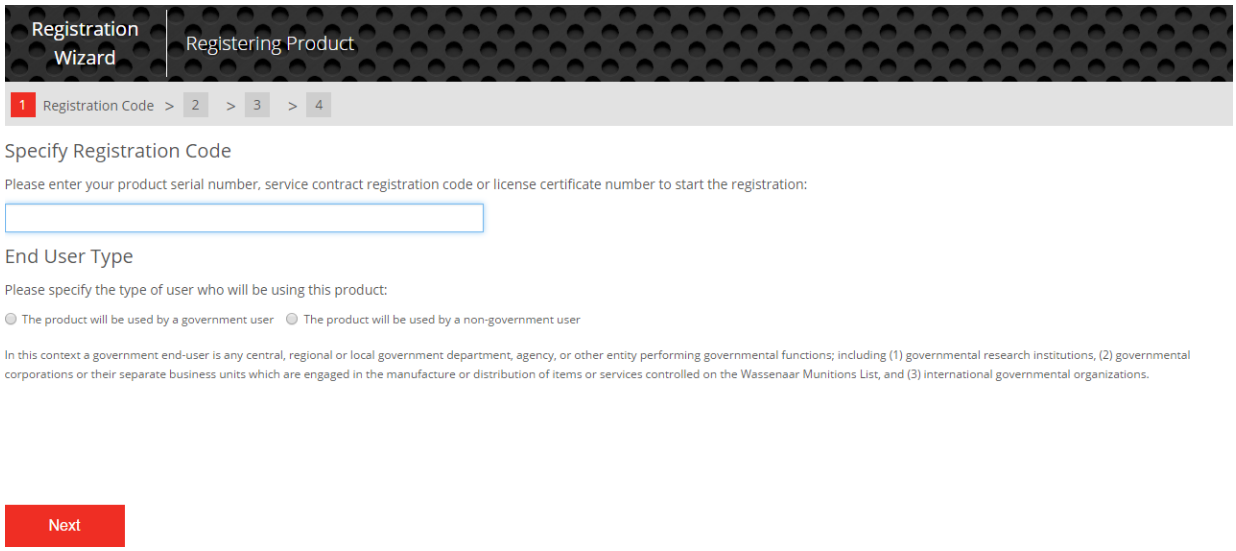
You must register and download licenses for the FortiGate-VM instance, based on the order type:

BYOL

You must obtain a license to activate the FortiGate. If you have not activated the license, you will see the license upload screen when you log into the FortiGate and cannot proceed to configure the FortiGate.

Licenses for the BYOL licensing model can be obtained through any Fortinet partner. After you purchase a license or obtain an evaluation license (60-day term), you will receive a PDF with an activation code.

1. Go to Customer Service & Support and create a new account or log in with an existing account.
2. Go to *Asset* > *Register/Renew* to start the registration process.
3. In the *Specify Registration Code* field, enter your license activation code, then select *Next* to continue registering the product.

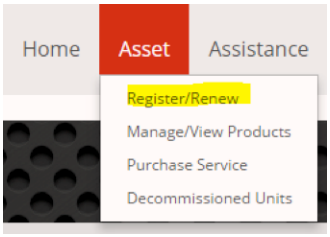


4. Enter your details in the other fields as required.
5. At the end of the registration process, download the license (.lic) file to your computer. You will upload this license later to activate the FortiGate-VM.

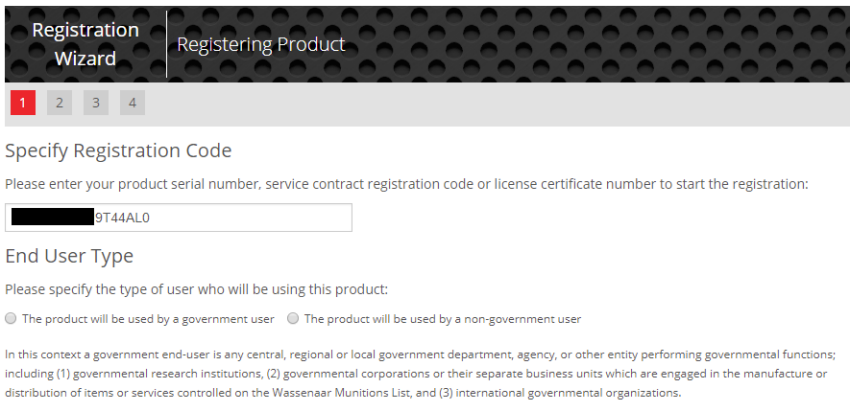
   After registering a license, Fortinet servers may take up to 30 minutes to fully recognize the new license. When you upload the license (.lic) file to activate the FortiGate-VM, if you get an error that the license is invalid, wait 30 minutes and try again.

PAYG

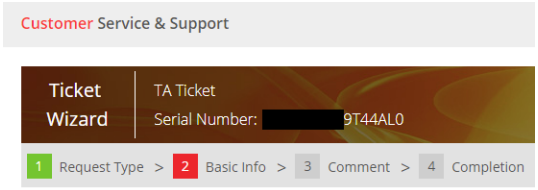
1. Deploy and boot the FortiGate PAYG VM and log into the FortiGate GUI management console.
2. From the Dashboard, copy the VM's serial number.
3. Go to Customer Service & Support and create a new account or log in with an existing account.
4. Go to *Asset* > *Register/Renew* to start the registration process.



5. In the *Specify Registration Code* field, enter the serial number, and select *Next* to continue registering the product. Enter your details in the other fields.



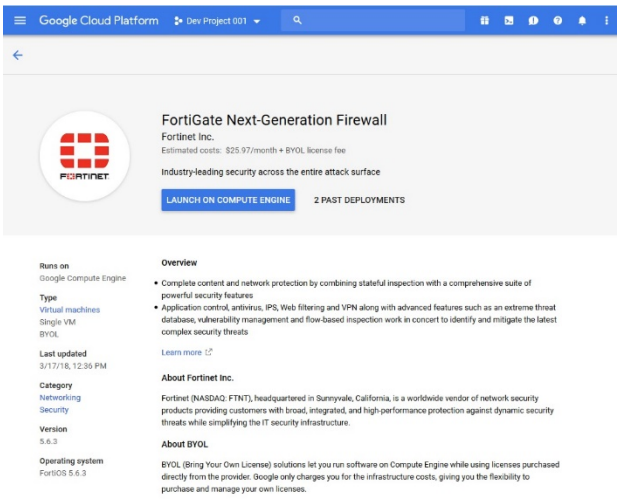
6. After completing registration, contact Fortinet Customer Support and provide your FortiGate instance's serial number and the email address associated with your Fortinet account.



Deploying FortiGate-VM on Google Cloud Marketplace

Initial deployment

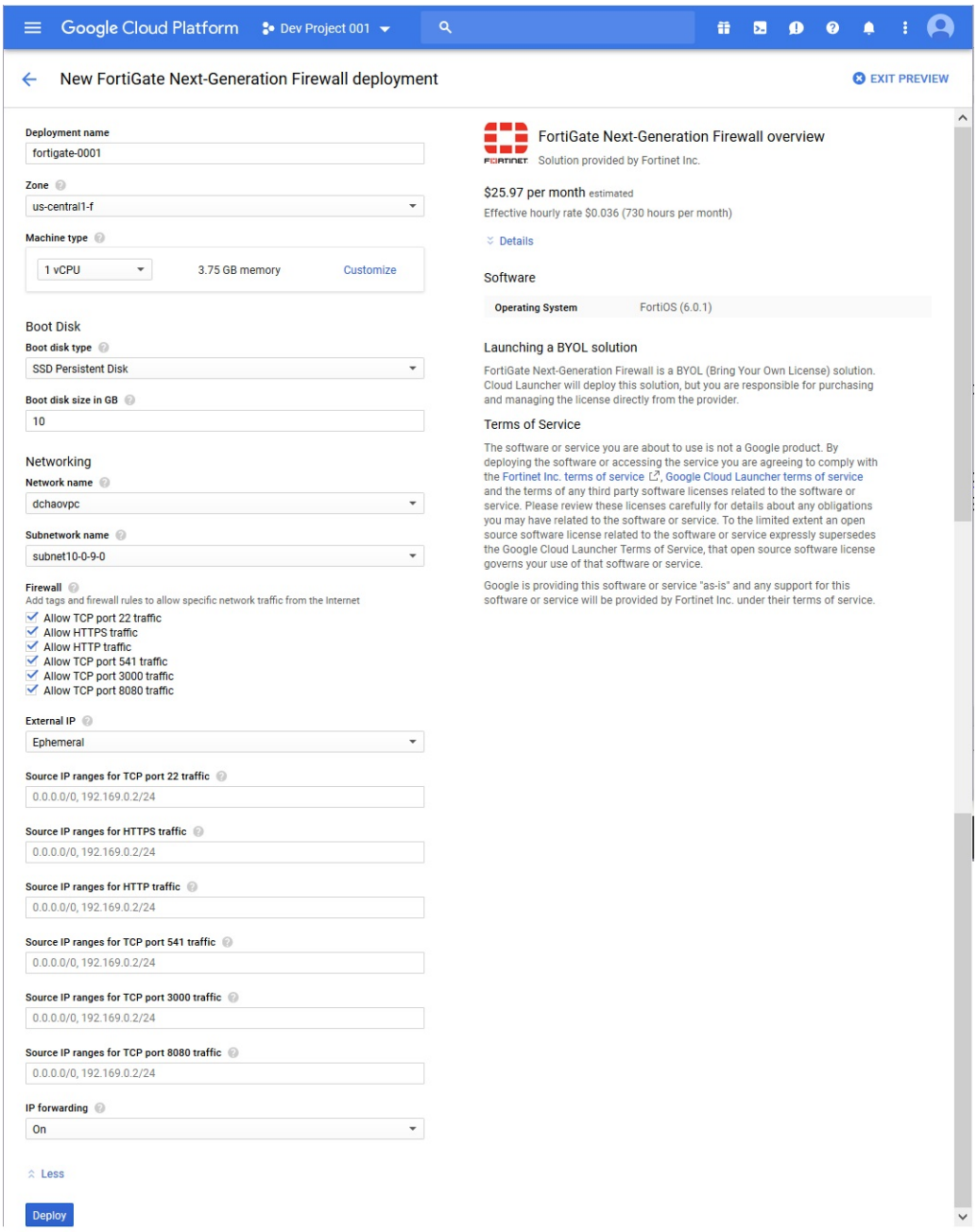
1. In the Google Cloud marketplace Cloud Launcher, find FortiGate Next-Generation Firewall.



This deployment method assigns only one network interface to the VM instance. With this deployment method, you cannot change the number of network interfaces after VM deployment. To assign multiple network interfaces, perform a manual deployment. See Deploying FortiGate-VM on Google Cloud Compute Engine on page 14 or Deploying FortiGate-VM using Google Cloud SDK on page 30.

2. Click *LAUNCH ON COMPUTE ENGINE*.

3. Configure the variables as required:

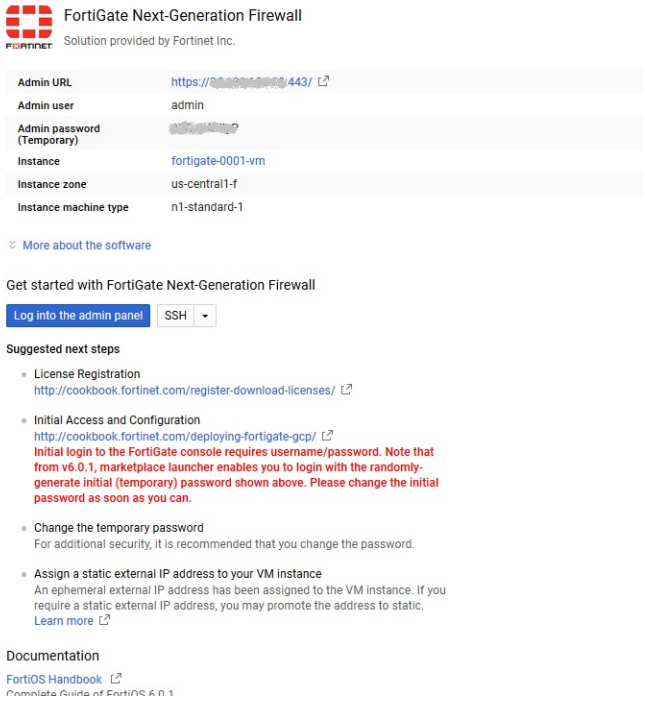


Deployment name	Enter the FortiGate-VM name to appear in the Compute Engine portal.
Zone	Choose the zone to deploy the FortiGate to.
Machine type	Choose the instance type required.
Boot disk type	Choose the desired boot disk type.
Boot disk size in GB	Leave as-is at 10 GB.

Network name	Select the network located in the selected zone.
Subnetwork name	Select the subnet where the FortiGate resides. Currently a one-arm setup in one subnet is supported on the Cloud Launcher solution.
Firewall	Leave all selected as shown, or allow at least HTTPS if the strictest security is allowed in your network as the first setup. Change firewall settings as needed later on. These are the open ports allowed in Google Cloud to protect incoming access to the FortiGate instance over the Internet and are not part of FortiGate firewall features.
External IP	Select *Ephemeral*. You will need to access the FortiGate management GUI via this public IP address.

Leave the other options as shown.

4. Click *Deploy*. When deployment is done, the screen appears as below.



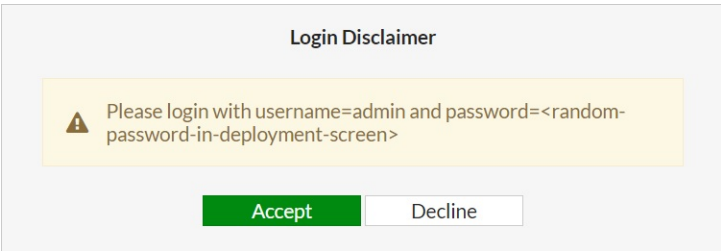
Registering and downloading your license

Follow the instructions detailed in BYOL on page 7, then continue to Connecting to the FortiGate-VM on page 12.

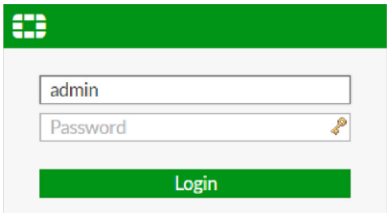
Connecting to the FortiGate-VM

To connect to the FortiGate-VM, you need your login credentials and the FortiGate-VM's public DNS address. From the previous step, there is a temporary admin password automatically generated on the Google Cloud.

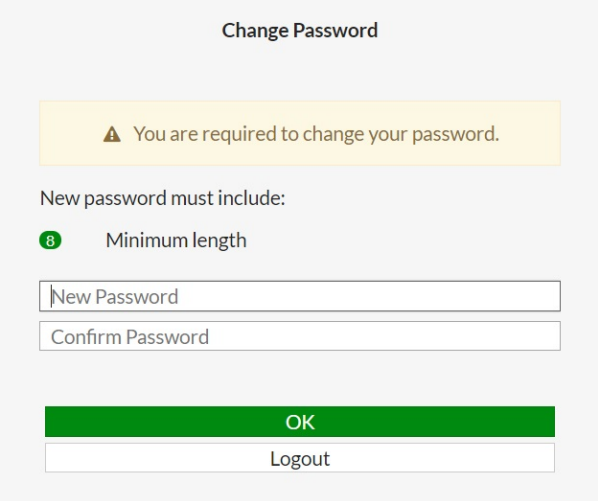
1. Connect to the FortiGate using your browser. You will see a certificate error message from your browser, which is normal because browsers do not recognize the default self-signed FortiGate certificate. Proceed past this error.
2. If accessing the FortiGate for the first time via the GUI (HTTPS, port 443) or SSH (port 22), you will see the disclaimer below. Note this appears when deploying FortiOS 6.0.2 or later. Click *Accept*.



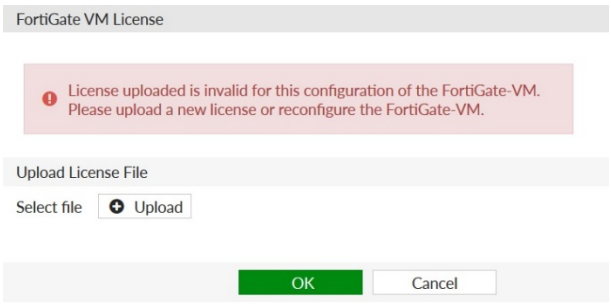
3. Log into the FortiGate-VM with the username *admin* and the supplied temporary password.



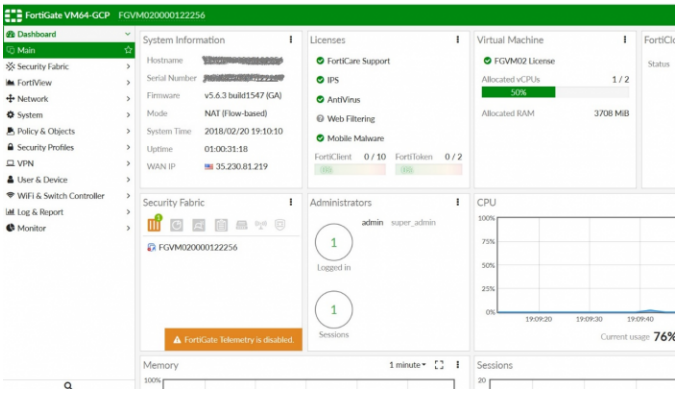
4. You are required to change the password. Change the password.



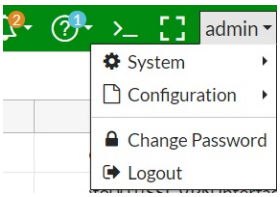
5. After logging in successfully, upload your license (.lic) file to activate the FortiGate-VM. The FortiGate-VM automatically restarts. After it restarts, wait about 30 minutes until the license is fully registered at Fortinet, then log in again.



6. After you log in, you see the FortiGate dashboard. The information in the dashboard varies depending on the instance type.



7. If deploying a version of FortiOS older than 6.0.2, you are encouraged to change the initial password as soon as possible after the initial launch, or to regularly change the password for all versions. Click *admin* in the top-right corner to change the password.



Deploying FortiGate-VM on Google Cloud Compute Engine

Obtaining the deployment image

1. Go to the Fortinet support site and log in.
2. Go to *Download* > *VM Images*.
3. Under *Select Product*, select *FortiGate*.
4. Under *Select Platform*, select *Google*.
5. Download the deployment package file. The deployment package file is named “FGT_VM64_GCP-vX-buildXXXX-FORTINET.out.gcp.tar.gz”, where vX is the major version number and XXXX is the build number.

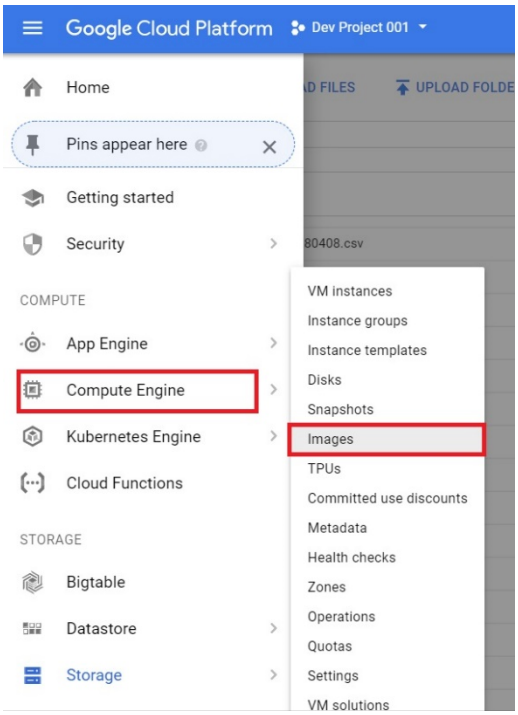
This deployment method is only applicable for BYOL. The PAYG deployment file will be ready at a later time.

Uploading the FortiGate deployment image to Google Cloud

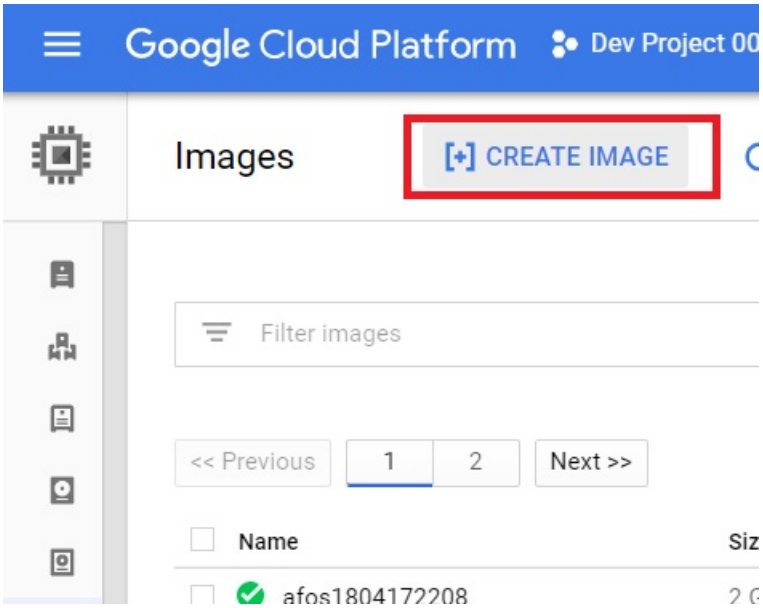
1. Log into Google Cloud.
2. Go to *Storage* > *Browser*.
3. Create a new bucket or go to an existing bucket.
4. Upload the newly downloaded deployment file.

Creating the FortiGate deployment image

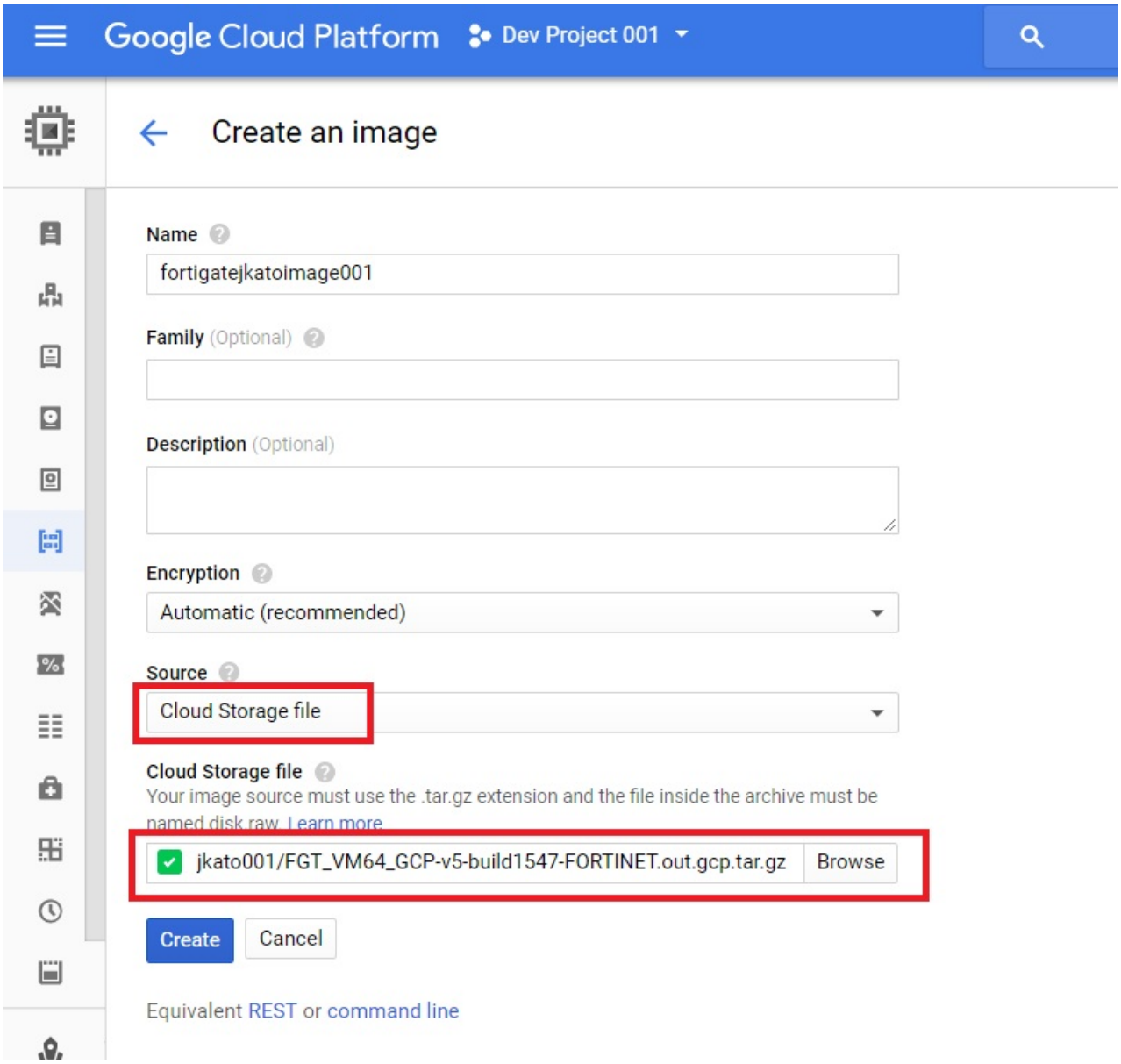
1. Go to *Compute Engine* > *Images*.



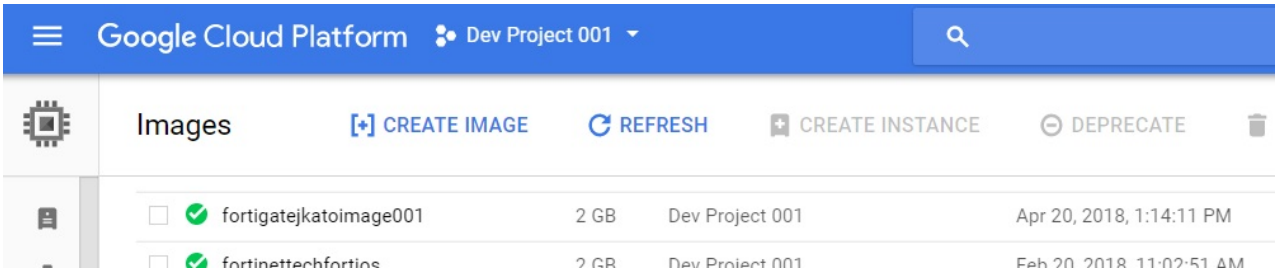
2. Click *CREATE IMAGE*.



3. On the *Create an image* page, enter the desired name. Under *Source*, select *Cloud Storage file*, then browse to the location of the deployment image file. Click *Create*.

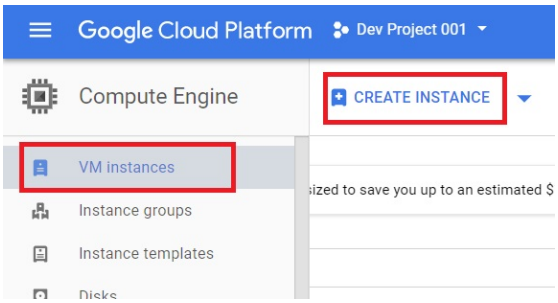


The image is listed on the *Images* pane.

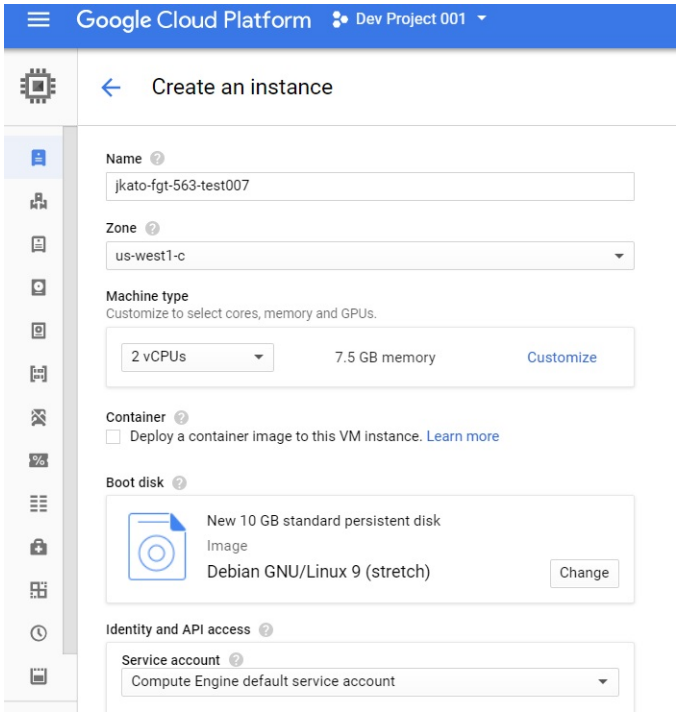


Deploying the FortiGate-VM instance

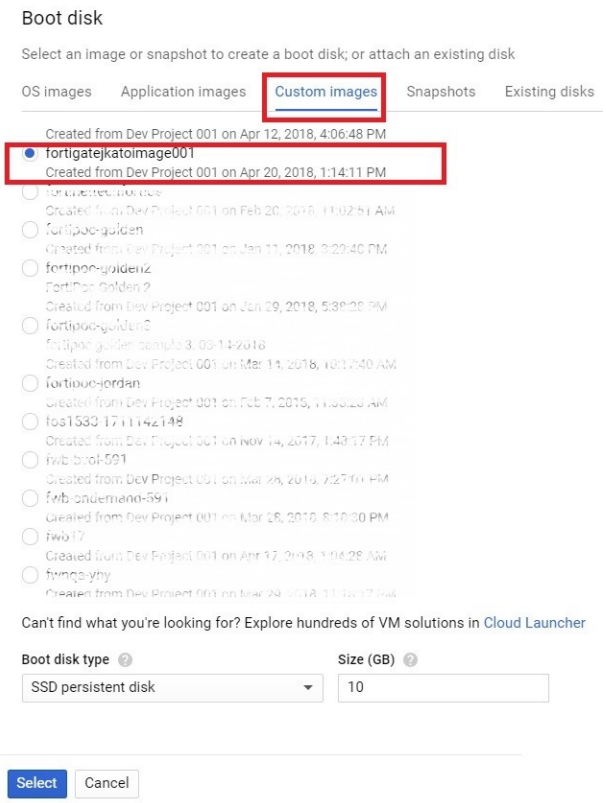
1. Go to *Compute Engine* > *VM Instances*. Click *CREATE INSTANCE*.



2. Configure the instance:
   a. In the *Name* field, enter the desired name. Select the desired zone and machine type.



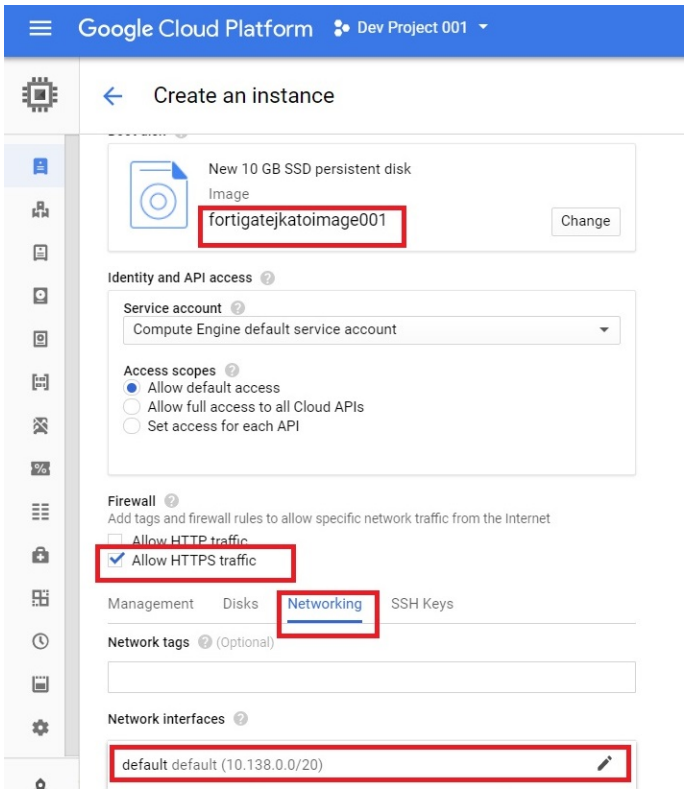
   b. Under *Boot disk*, click *Change*.
   c. On the *Custom images* tab, select the newly created image. Change the boot disk type as needed, and enter 10 for the *Size*. Click *Select*.



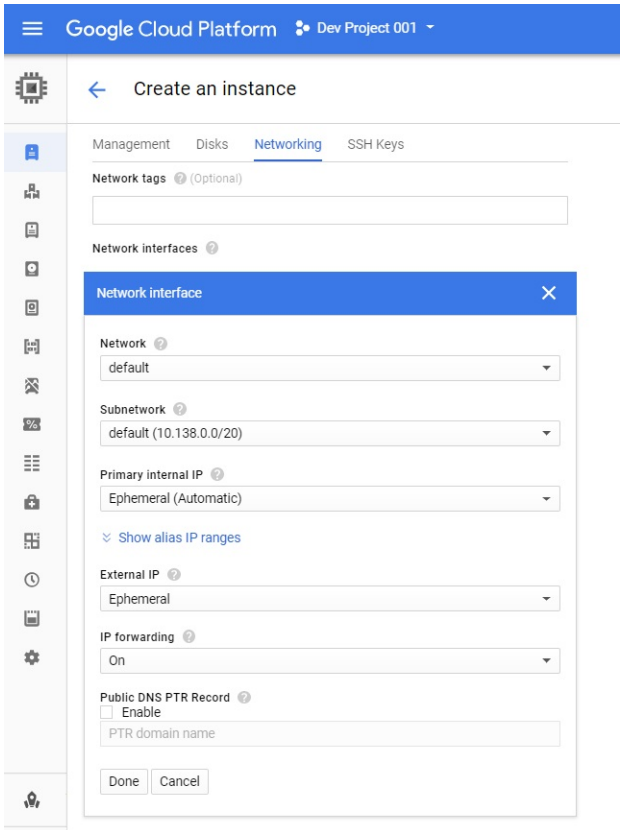
d. Ensure the new image is selected.

e. Select *Allow HTTPS* traffic. You will access the FortiGate management console using HTTPS. If you allocate multiple network interfaces to the FortiGate, this is nullified at this stage. You can configure this later. See Configuring Google Cloud firewall rules on page 26.

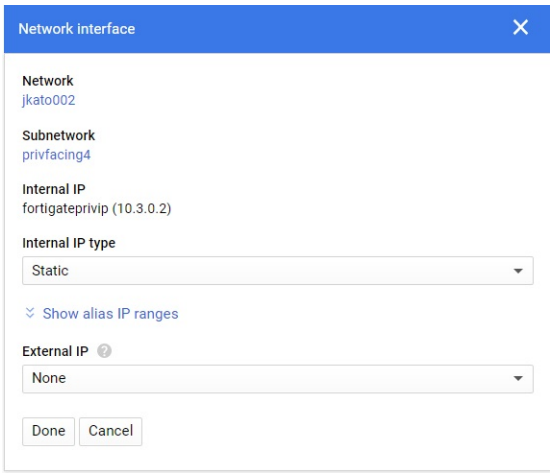
f. Click *Networking*. Here you want to specify multiple network interfaces. One is located on the public-facing side of the Internet, the other facing a protected private network.



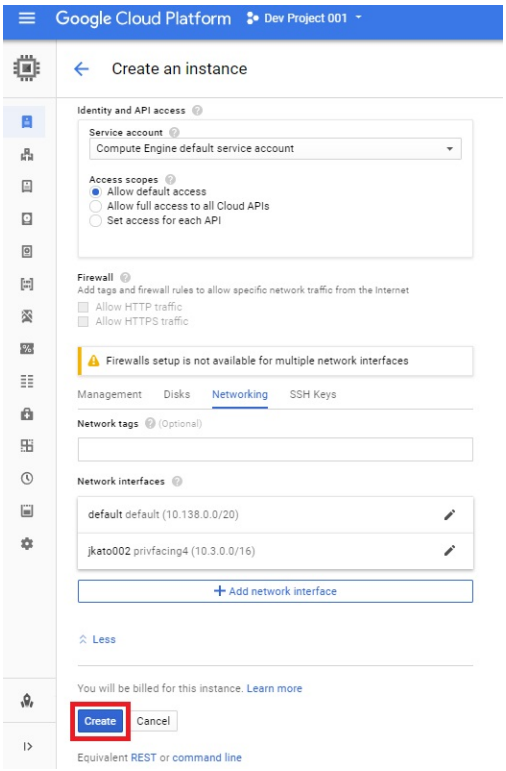
g. Edit the first network interface. Preferably assign a static IP address. Under *IP Forwarding*, select *On*. Configure other items as needed and click *Done*.



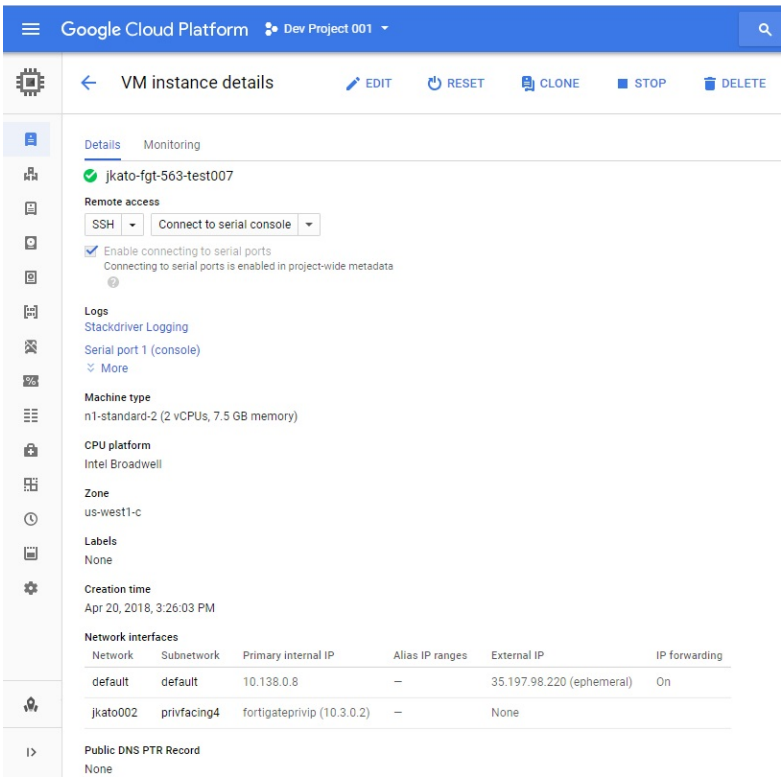
h. Click *Add network interface* to add the second interface for the private subnet. If you click *Network* there will be the list of preconfigured networks. Choose the one located in the same region as you chose to deploy the instance. Under *External IP*, select *None*.



3. After configuring all elements, click *Create*.



After 15-30 minutes, the instance should be up and running.

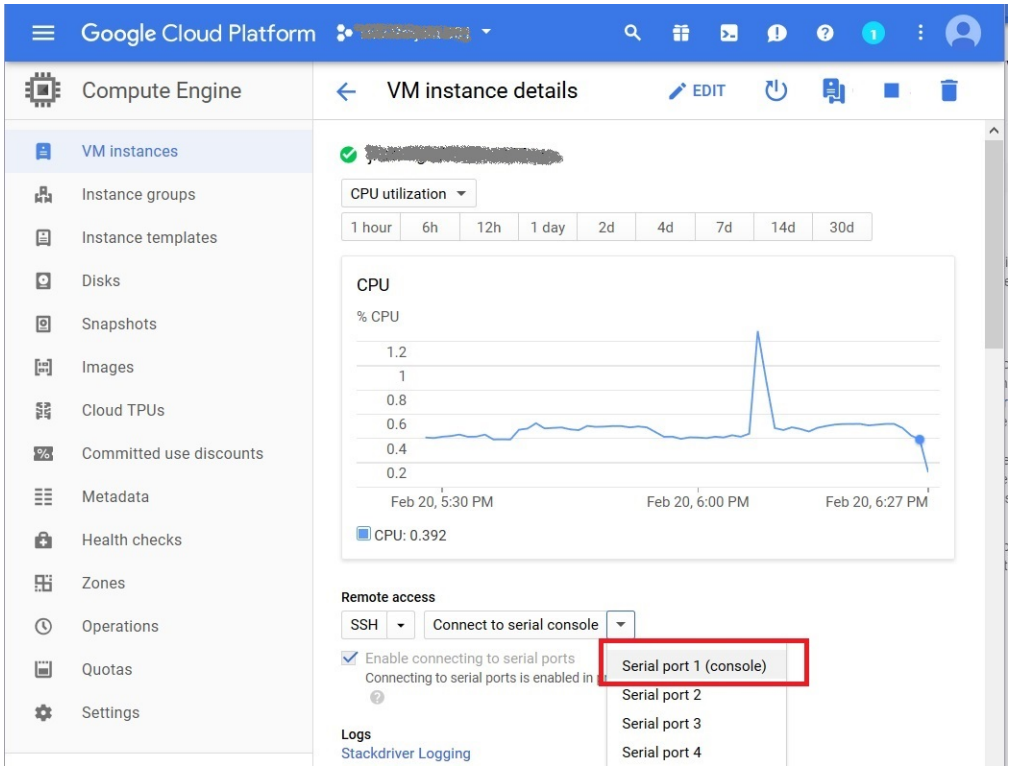


Connecting to the FortiGate-VM

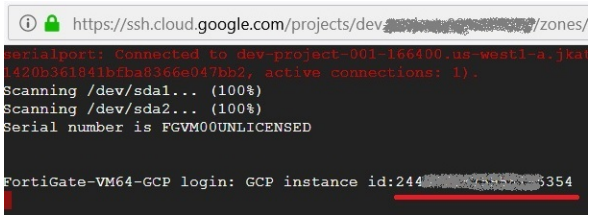
To connect to the FortiGate-VM, you need your login credentials and its public DNS address.

The default username is admin and the default password is the GCP instance ID, which is represented as a number that can be found after locating the instance in the GCP Compute Engine console.

1. Choose the instance from the list of instances on the *VM Instances* page.
2. There are two methods to obtain the instance ID. Do one of the following:
   a. Open *Serial port 1 (console)* as seen below.

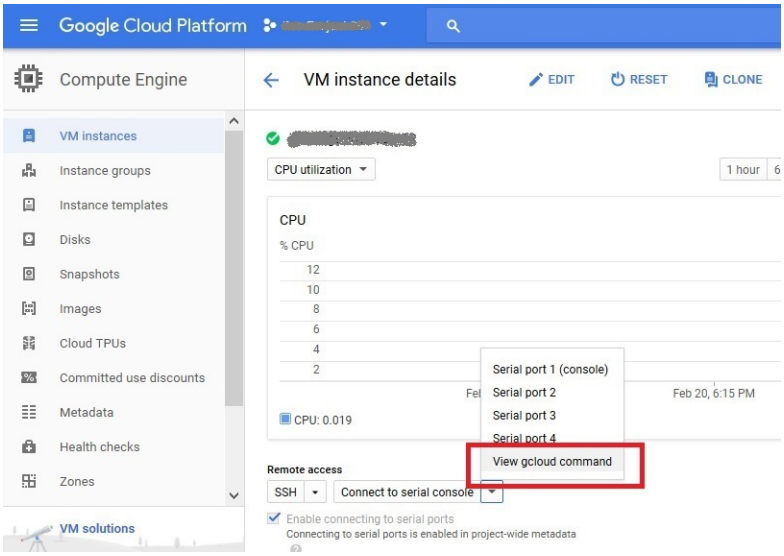


The first time you access the serial console, you will find the instance ID, represented as a number. This is the login password.



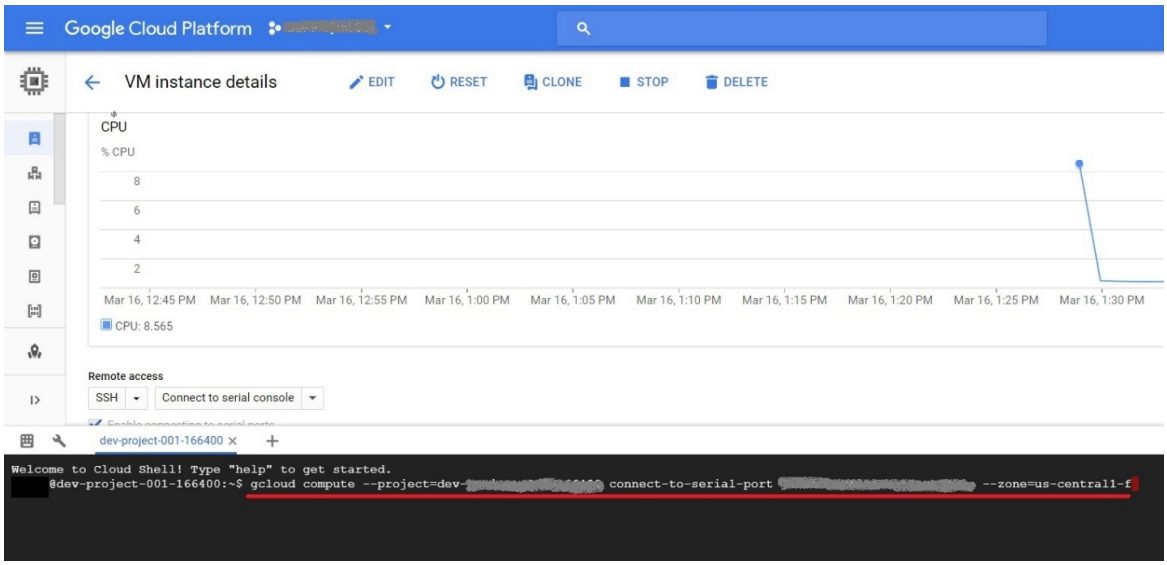
b. Do the following:

i. Select *View gcloud command* on the *VM instance details*.

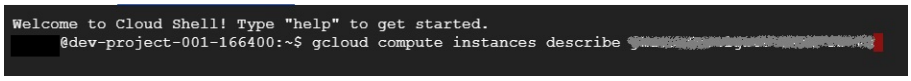


ii. Click *RUN IN CLOUD SHELL*.

iii. By default, a command is shown as underlined below. Delete the command underlined below.

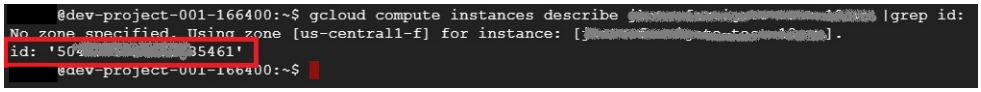


iv. Enter the following command: `gcloud compute instances describe <instance_name>`.

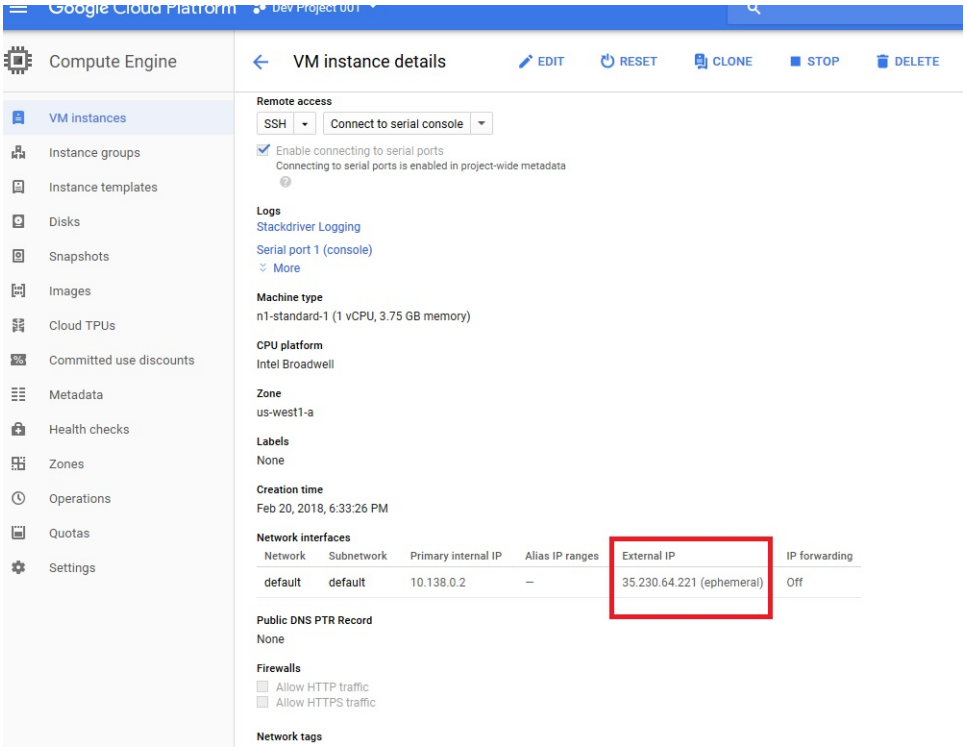


v. You will see a line starting with `id: '<number>'`. This is the FortiGate initial login password.

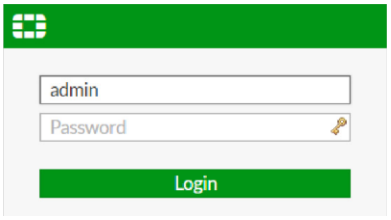
You can also enter `gcloud compute instances describe <instance_name> | grep id:` This number is the login password.



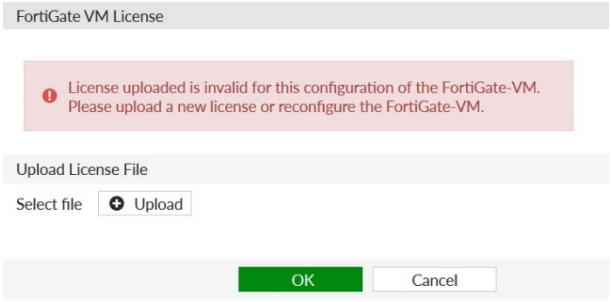
3. Open an HTTPS session using the FortiGate-VM's public DNS address in your browser (https://<public_DNS>). You can find the FortiGate-VM's public IP address on the *VM instance details* page.



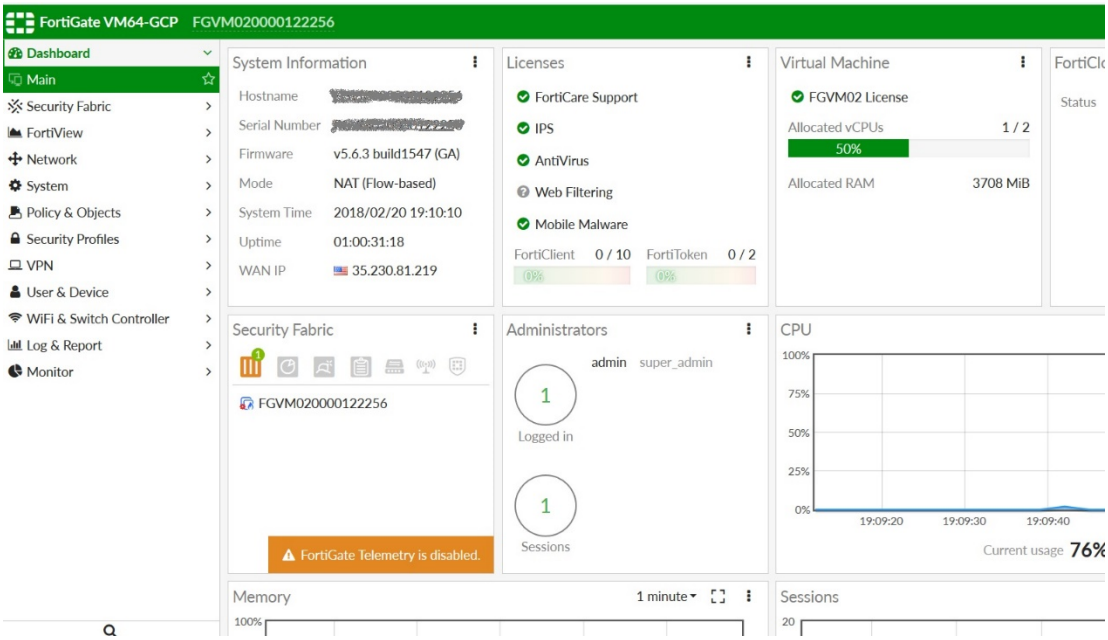
4. Access the FortiGate in your browser.



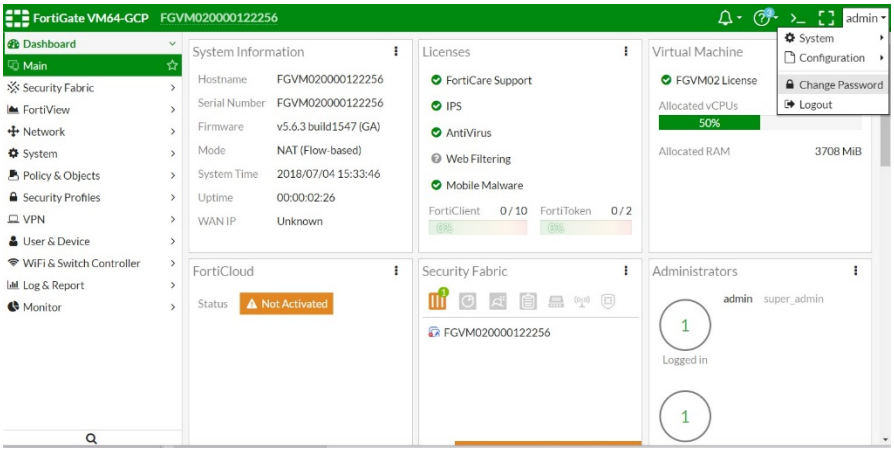
5. You will see a certificate error message from the browser. This is expected since browsers do not recognize the default self-signed FortiGate certificate. Proceed past the error message.
6. Log into the FortiGate-VM with the username admin and the password.
7. Upload your license (.lic) file to activate the FortiGate-VM. The FortiGate-VM automatically restarts. After it restarts, wait about 30 minutes until the license is fully registered at Fortinet, and log in again.



You now see the FortiOS dashboard. The information in the main dashboard varies depending on the instance type.



You are encouraged to change the initial password at the top right corner of the FortiGate management GUI.

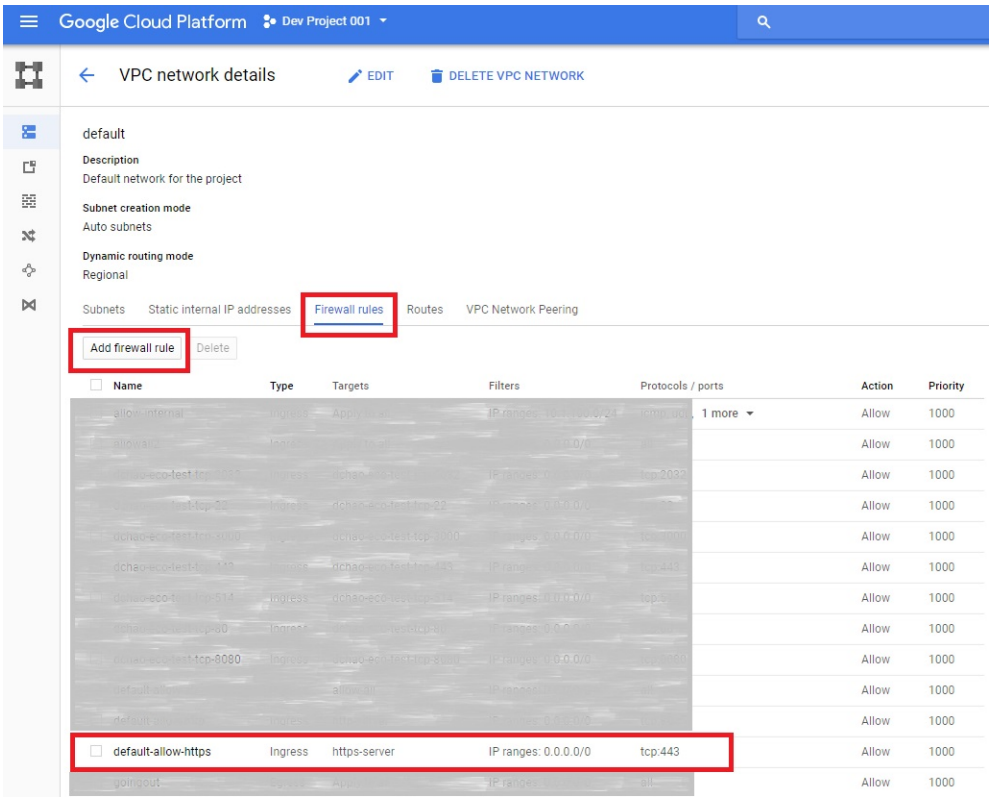


Configuring Google Cloud firewall rules

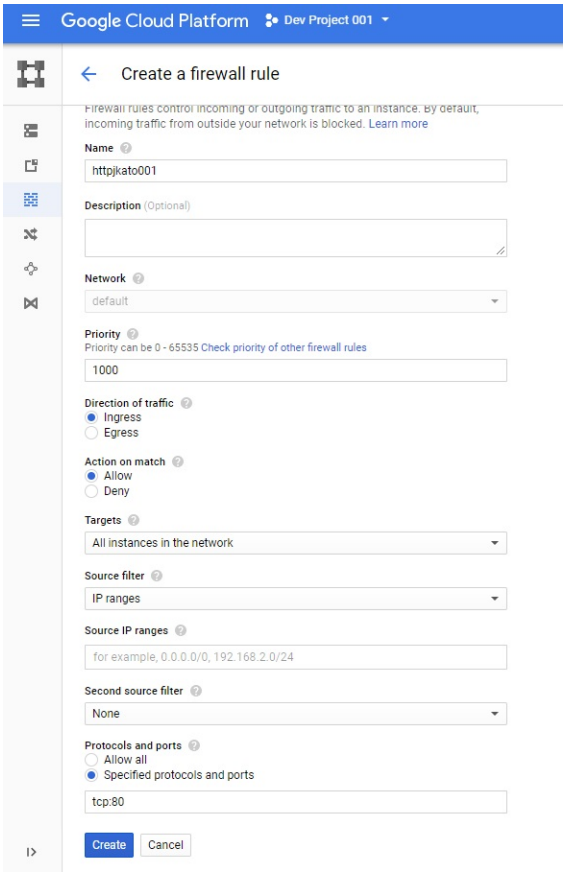
You must open incoming port(s) to access FortiGate over the Internet.

HTTPS is the first port that is needed. Other ports are optional depending on what features are enabled. See *FortiGate open ports* in *FortiOS Ports and Protocols*.

1. Go to the VPC where the public-facing subnet belongs for the FortiGate.



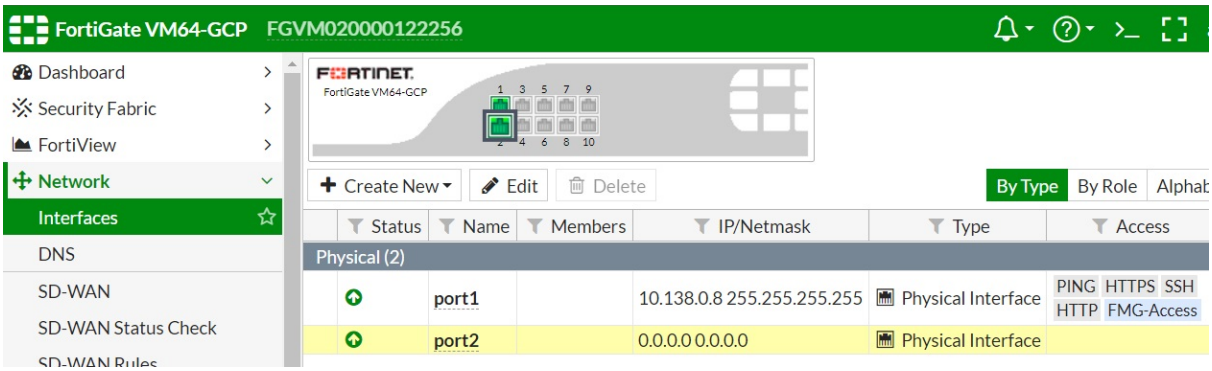
2. Select *Firewall rule*, then *Add firewall rule* if the required port is not open.



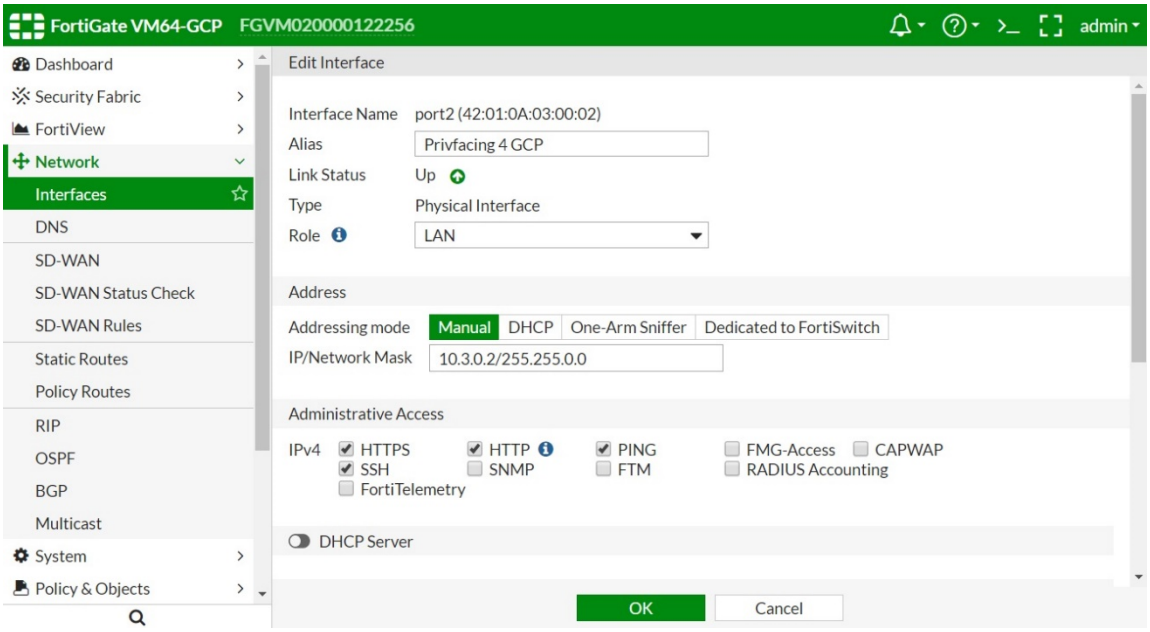
Configuring the second NIC on the FortiGate-VM

After logging into the FortiGate management GUI, you must manually configure the second NIC. Otherwise, the configuration is empty.

1. Go to *Network* > *Interfaces*. port2's IP address/netmask is shown as *0.0.0.0 0.0.0.0*.



2. Edit port2. Enter the IP address and netmask. Configure other elements as needed, then click *OK*.



Deploying FortiGate-VM using Google Cloud SDK

You can deploy FortiGate-VM (BYOL) by using the Google Cloud SDK on your local PC. This is a method of deploying FortiGate-VM on GCP outside of the marketplace product listing and without creating an instance on the Google Cloud Compute Portal.

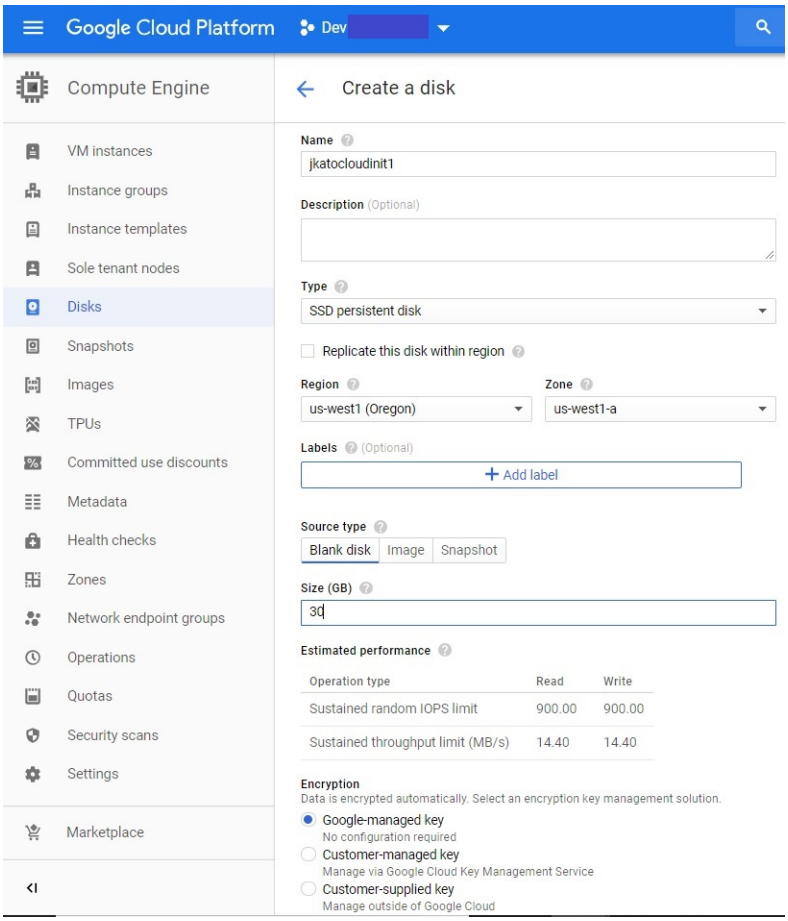
For details, see Cloud SDK.

This deployment method is only applicable for BYOL. The PAYG deployment file will be ready at a later time.

Using the Google Cloud SDK to deploy FortiGate-VM

The following example assumes that the Google Cloud SDK is installed on a Linux machine.

1. Log into your GCP environment: `$sudo gcloud auth login`
2. Select your Google Cloud account and enter your credentials. Then, the default project will be specified.
3. In Compute Engine, go to *Disks* and create a blank disk for the FortiGate-VM log disk. You will attach this disk to the FortiGate at the time of deployment.



You can also create a disk using Google Cloud. To create a disk, run the following command:

```
gcloud compute --project="project name" disks create "your disk name" --zone="your zone" --type="your disk type" --size="your disk size"
```

For example, if used with the example in the screenshot, the command looks as follows:

```
sudo gcloud compute --project="project name" disks create jkatocloudinit1 --zone=us-west1-a --type=pd-ssd --size=30GB
```

4. The command to deploy a FortiGate-VM requires the following values. Check the following for your GCP environment:
   a. `VM name`: desired VM name.
   b. `network name1`: Name for the public-facing network.
   c. `subnet name1`: Subnet name for the public-facing network.
   d. `network name2`: Name for the internal protected network.
   e. `subnet name2`: Subnet name for the Internet network.
   f. `no-address` will not allocate an ephemeral/external IP address on the interface.
   g. `project name`: Project where you will deploy the VM instance. You must have access to the project.
   h. `image name`: The FortiGate image where you will deploy the VM from. For details on how to obtain this image, see Obtaining the deployment image on page 14.
   i. `--can-ip-forward`: Should be specified for IP Forwarding=ON.
   j. `machine type`: Enter the machine type, such as `n1-highcpu-2`.
   k. `zone name`: Enter the zone name, such as `us-west-1a`. Note that this is a zone within a region.

l. `disk name`: A blank disk name for the second disk. FortiGate-VM requires an additional disk for logging.

m. `device name`: Enter a device name.

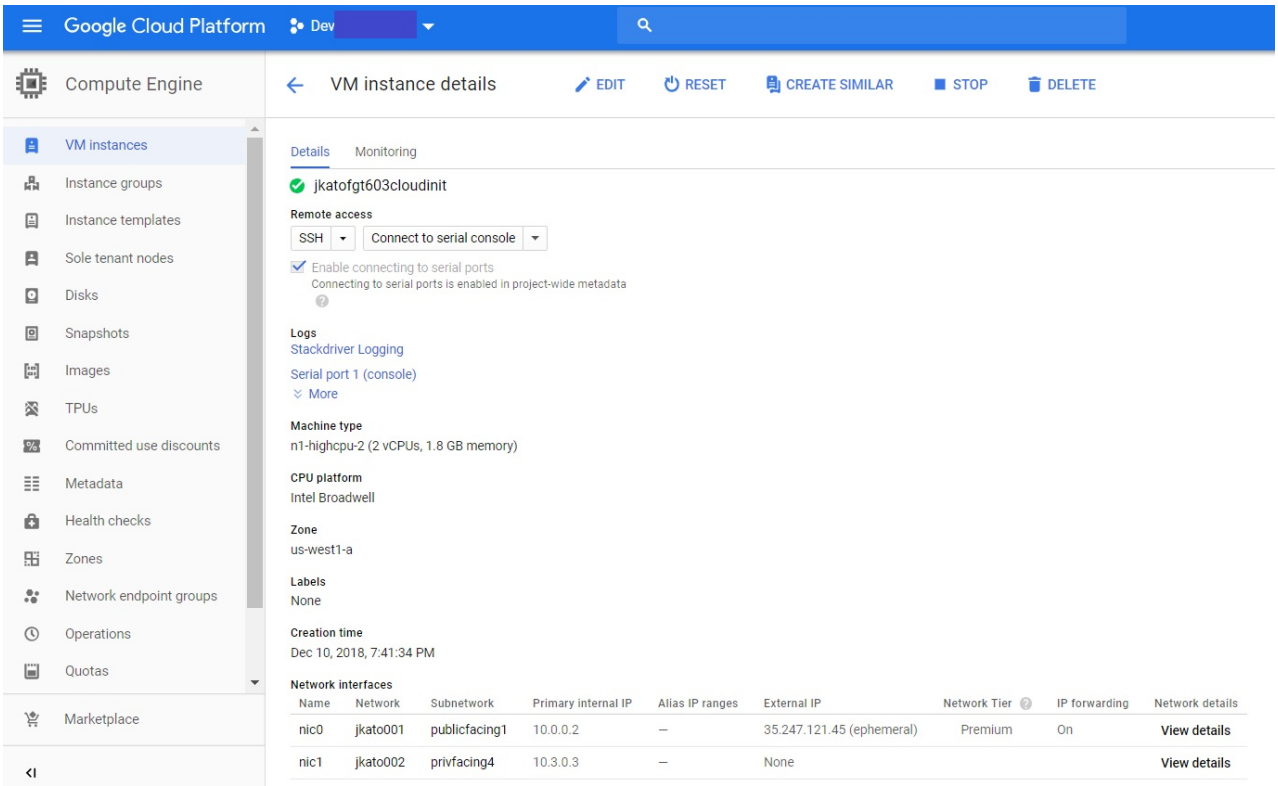
5. The command to deploy a FortiGate-VM is as follows. This example creates a VM with two network interfaces:

```
$gcloud compute instances create <VM name> --network-interface network=<network
      name1>,subnet=<subnet name1> --network-interface network=<network
      name2>,subnet=<subnet name2>,no-address --project <project name> --image <image name>
      --can-ip-forward --machine-type
```

In this example, let's run the following command to create the FortiGate-VM instance with name jkatofgt603cloudinit:

```
$sudo gcloud compute instances create jkatofgt603cloudinit --network-interface
      network=jkato001,subnet=publicfacing1 --network-interface
      network=jkato002,subnet=privfacing4 --project "project name" --image jkato-fgt-603-
      10162018-001 --can-ip-forward --machine-type n1-highcpu-2" --zone us-west1-a --
      disk=name=jkatocloudinit1,device-name=jkatodevicecloudinit1,mode=rw,boot=no
```

6. Go to the Google Cloud Compute Engine and find the new VM instance.



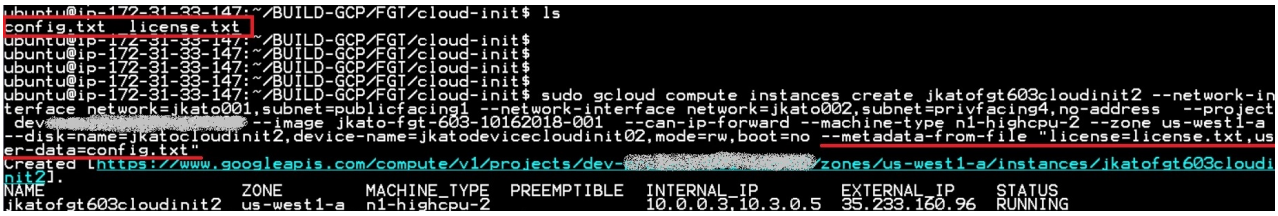
7. Connect to the FortiGate-VM instance. See Connecting to the FortiGate-VM on page 21.

Bootstrapping FortiGate at initial boot-up

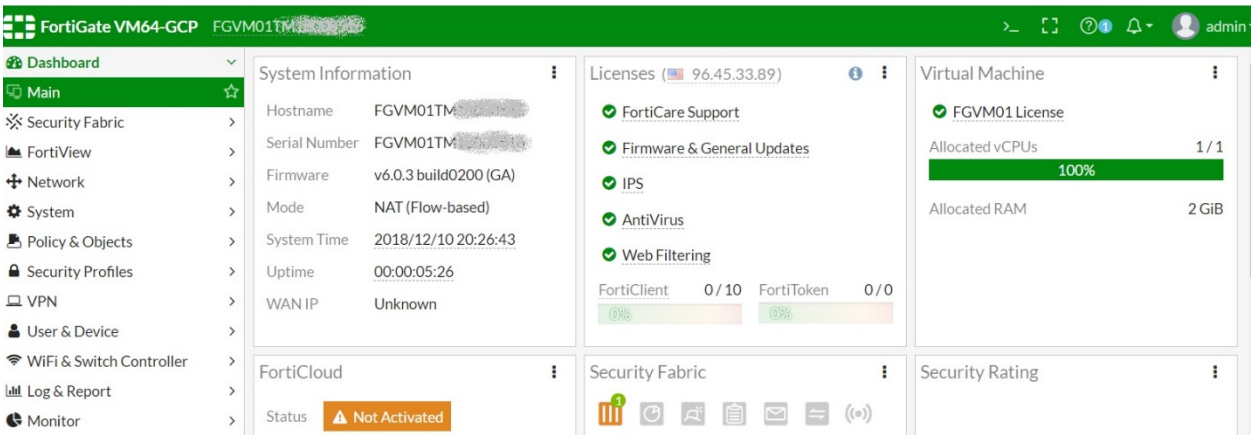
This section explains how to add bootstrapping of FortiGate CLI commands and a BYOL license at the time of initial boot-up as part of Google Cloud commands.

1. Create a text file that contains FortiGate CLI commands. In this example, let's save the file as config.txt. CRLF must be present. Therefore it is recommended to use a text editor that includes CRLF automatically. In this example, we will use the following CLI commands:
   ```
   config system global
      set timezone 03
   end
   ```
   This example sets the timezone as GMT-9 Alaska. You can replace these lines with your own set of CLI commands.
2. You can download a license file from Customer Service & Support after registering your product code. Save the license file as a .txt file. FortiGate-VM license content resembles the following:

3. Upload the config.txt and license files onto the Linux machine were you will run the Google Cloud SDK commands. Place the files in the same directory.
4. Run the command as described in Using the Google Cloud SDK to deploy FortiGate-VM on page 30, adding the following:
   ```
   --metadata-from-file "license=<license text file>,user-data=<FortiGate CLI text file>". In
         this example, it will be --metadata-from-file "license=license.txt,user-
         data=config.txt".
   ```



5. After deployment, log into the FortiGate by accessing https://<IP_address> in your browser. The system displays the dashboard instead of a license upload window, since the license is already activated.



To see how bootstrapping went, check if the command was successfully run. Open the CLI console and enter `diag debug cloudinit show`.

If the cloud-init was run successfully, the CLI shows `Finish running script` with no errors. If you see an error with this `diagnose` command, resolve it and try again by checking the license and config.txt files. Ensure that the text file contains CRLF.

6. Check the timezone by running `config system global` and `get` commands.

```
Connected

FGVM01TM18000516 #
FGVM01TM18000516 #
FGVM01TM18000516 # diag debug cloudinit show
 >> Checking metadata source gcp
 >> Run config script
 >> Finish running script
 >> FGVM01TM18000516 $  config system global
 >> FGVM01TM18000516 (global) $  set timezone 03
 >> FGVM01TM18000516 (global) $  end
```

The timezone was changed to Alaska as expected, meaning that the bootstrapping CLI command was successful. This assumes that you used the default FortiGate CLI command in step 1. If you modified the command, test it accordingly.

High availability for FortiGate-VM on GCP

Deploying FortiGate-VM HA on GCP in one zone

FortiGate-VM for Google Cloud Marketplace supports using the FortiGate Clustering Protocol (FGCP) in unicast form to provide an active-passive clustering solution for deployments in GCP. This feature shares a majority of the functionality, including configuration and session synchronization, that FGCP on FortiGate hardware provides with key changes to support GCP software-defined networking (SDN).

This solution works with two FortiGate instances configured as a primary and secondary pair, and requires that you deploy each instance with four network interfaces, within the same availability zone. These FortiGate instances act as a single logical instance and share interface IP addressing.

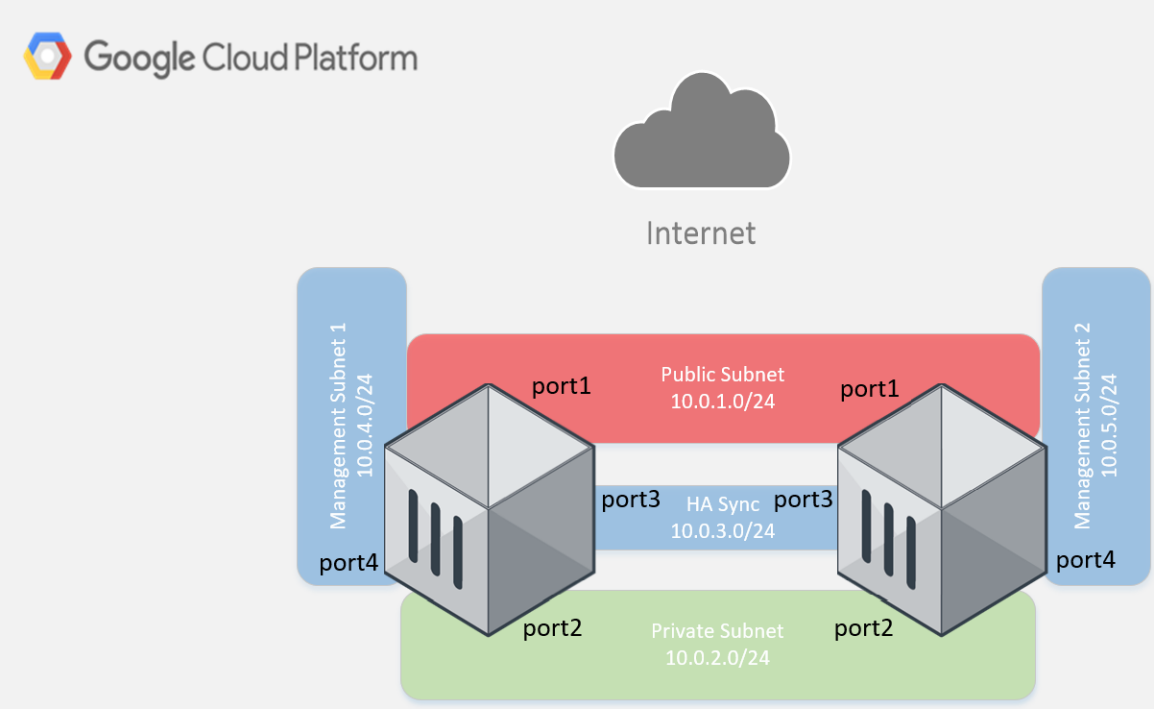
The main benefits of this solution are:

- Fast and stateful failover of FortiOS and GCP SDN without external automation/services
- Automatic GCP SDN updates to route targets and IP addresses
- Native FortiOS session synchronization of firewall, IPsec/SSL VPN, and voice over IP sessions
- Native FortiOS configuration synchronization
- Ease of use as the cluster is treated as a single logical FortiGate

You can configure FortiGate high availability on GCP using one of the following methods:

- Using the GCP GUI console. See Deploying FortiGate HA using the GCP GUI on page 37.
- Using the Google Cloud command interface. See Deploying FortiGate HA using the Google Cloud command interface on page 43.

For information on FGCP, see the FortiOS documentation.



Deploying FortiGate HA using the GCP GUI

Obtaining the deployment image

1. Go to the Fortinet support site and log in.
2. Go to *Download* > *VM Images*.
3. Under *Select Product*, select *FortiGate*.
4. Under *Select Platform*, select *Google*.
5. Select the desired firmware version.
6. Download the package file for a new deployment of FortiGate on GCP. The deployment package file is named “FGT_VM64_GCP-vX-buildXXXX-FORTINET.out.gcp.tar.gz”, where vX is the major version number and XXXX is the build number.

This deployment method is only applicable for BYOL. The PAYG deployment file will be ready at a later time.

Uploading the FortiGate deployment image to GCP

1. Log into GCP.
2. Go to *Storage* > *Browser*.
3. Create a new bucket.
4. Upload the newly downloaded deployment file.

Creating the FortiGate deployment image

1. Go to *Compute Engine* > *Images*.
2. Click *CREATE IMAGE*.
3. On the *Create an image* page, enter the desired name. Under *Source*, select *Cloud Storage file*, then browse to the location of the deployment image file. Click *Create*. The image is listed on the *Images* pane. It may take a few minutes for your image to complete and become available.

Creating VPC networks

This deployment requires four networks which you must create prior to deploying the FortiGates. The networks are as follows:

Network	Description
unprotected-network	Treated as unsafe and directly attached to the Internet.
protected-network	Commonly referred to as LAN in traditional physical network architectures.

Network	Description
ha-sync-network	All HA functionality, such as session and configuration synchronization, communicates with this network.
mgmt-network	Out of band management network.

Additionally, you must set up the route tables and GCP firewall rules necessary to allow traffic flow through the FortiGates. The route tables and firewall rules are separate separate from those that are configured on the FortiGates. Name the GCP route tables and firewall rules according to associated network and functionality.

1. In the GCP console, go to *VPC Networks*, then click *CREATE VPC NETWORK*.
2. In the *Name* field, enter the desired name.
3. From the *Region* dropdown list, select the region appropriate for your deployment. All four networks must be in the same region.
4. From the *IP address range* field, enter the first network's subnet in CIDR format, such as 10.0.1.0/24.
5. Leave all other settings as-is, then click *Create*.
6. Repeat steps 1-5 to create the remaining three networks in your VPC.

Creating VPC firewall rules

GCP firewall rules are stateful, meaning that you only need to create one rule for the originating traffic. However, you may have traffic originate from both the Internet and your GCP resources. This requires you to create both an egress and ingress rule for each VPC network.

To create ingress rules:

1. In the GCP console, go to *VPC networks* > *Firewall Rules*. Click *Create Firewall Rule*.
2. In the *Name* field, enter the desired name.
3. From the *Network* dropdown list, select the desired network to associate with this firewall rule.
4. For *Direction of Traffic*, select *Ingress*.
5. For *Action on match*, select *Allow*.
6. From the *Targets* dropdown list, select *All instances in the network*.
7. In the *Source IP ranges* field, enter 0.0.0.0/0.
8. For *Protocols and ports*, click *Allow all*, then click *Create*.
9. Repeat steps 1-8 for the remaining three networks in your VPC.

To create egress rules:

1. In the GCP console, go to *VPC networks* > *Firewall Rules*. Click *Create Firewall Rule*.
2. In the *Name* field, enter the desired name.
3. From the *Network* dropdown list, select the desired network to associate with this firewall rule.
4. For *Direction of Traffic*, select *Egress*.
5. For *Action on match*, select *Allow*.
6. From the *Targets* dropdown list, select *All instances in the network*.
7. In the *Source IP ranges* field, enter 0.0.0.0/0.

8. For *Protocols and ports*, click *Allow all*, then click *Create*.
9. Repeat steps 1-8 for the remaining three networks in your VPC.

Now you have a total of eight GCP firewall rules.

Deploying the primary FortiGate-VM instance

1. Go to *Compute Engine* > *VM Instances*. Click *CREATE INSTANCE*.
2. Configure the instance settings:
   a. In the *Name* field, enter the desired name.
   b. From the *Region* dropdown list, select the region where you created your VPC networks in Creating VPC networks on page 37.
   c. From the *Zone* dropdown list, select a zone within the chosen region. You must deploy both FortiGates in the same region and zone.
   d. From the *Machine type* dropdown list, select the number of vCPUs for this instance. This should match the FortiGate license and be a minimum of four vcPUs so that the instance supports four vNICs.
   e. Under *Boot disk*, click *Change*.
   f. On the *Custom images* tab, select the newly created image. Click *Select*.
   g. Click to expand *Management, security, disks, networking, sole tenancy*, then click *Networking*.
   h. Configure the unprotected network:
      i. Click the edit icon for the interface already created for the instance.
      ii. From the *Network* dropdown list, select the unprotected network. Your subnet is automatically populated.
      iii. From the *External IP* dropdown list, select *Create IP address*.
      iv. In the *Name* field, enter a name for the IP address, then click *RESERVE*.
      v. From the *IP Forwarding* dropdown list, select *On*.
      vi. Click *Done*.
   i. Configure the protected network:
      i. Click *Add network interface*.
      ii. From the *Network* dropdown list, select the protected network.
      iii. From the *External IP* dropdown list, select *None*.
      iv. Click *Done*.
   j. Configure the HA network:
      i. Click *Add network interface*.
      ii. From the *Network* dropdown list, select the HA network.
      iii. From the *External IP* dropdown list, select *None*.
      iv. Click *Done*.
   k. Configure the management network:
      i. Click *Add network interface*.
      ii. From the *Network* dropdown list, select the management network.
      iii. From the *External IP* dropdown list, select *Ephemeral*.
      iv. Click *Done*.

You cannot add interfaces to an instance after creating it. If you create the instance with an improper interface configuration, you must destroy the instance and recreate it with the proper interface configuration.

3. After configuring all elements, click *Create*.

Deploying the secondary FortiGate-VM instance

1. Go to *Compute Engine* > *VM Instances*. Click *CREATE INSTANCE*.
2. Configure the instance settings:
   a. In the *Name* field, enter the desired name.
   b. From the *Region* dropdown list, select the region where you created your VPC networks in Creating VPC networks on page 37.
   c. From the *Zone* dropdown list, select a zone within the chosen region. You must deploy both FortiGates in the same region and zone.
   d. From the *Machine type* dropdown list, select the number of vCPUs for this instance. This should match the FortiGate license and be a minimum of four vcPUs so that the instance supports four vNICs.
   e. Under *Boot disk*, click *Change*.
   f. On the *Custom images* tab, select the newly created image. Click *Select*.
   g. Click to expand *Management, security, disks, networking, sole tenancy*, then click *Networking*.
   h. Configure the unprotected network:
      i. Click the edit icon for the interface already created for the instance.
      ii. From the *Network* dropdown list, select the unprotected network. Your subnet is automatically populated.
      iii. From the *External IP* dropdown list, select *Ephemeral*. This IP address will be removed later, but is necessary to log into the FortiGate and upload the license prior to HA configuration.
      iv. From the *IP Forwarding* dropdown list, select *On*.
      v. Click *Done*.
   i. Configure the protected network:
      i. Click *Add network interface*.
      ii. From the *Network* dropdown list, select the protected network.
      iii. From the *External IP* dropdown list, select *None*.
      iv. Click *Done*.
   j. Configure the HA network:
      i. Click *Add network interface*.
      ii. From the *Network* dropdown list, select the HA network.
      iii. From the *External IP* dropdown list, select *None*.
      iv. Click *Done*.
   k. Configure the management network:
      i. Click *Add network interface*.
      ii. From the *Network* dropdown list, select the management network.
      iii. From the *External IP* dropdown list, select *Ephemeral*.
      iv. Click *Done*.

You cannot add interfaces to an instance after creating it. If you create the instance with an improper interface configuration, you must destroy the instance and recreate it with the proper interface configuration.

3. After configuring all elements, click *Create*.

Creating a GCP route table

When you created your VPC networks, GCP automatically created several route tables. You must create one additional route table, which will allow the protected network to use the FortiGates as the default gateway.

1. In the GCP console, click the primary FortiGate's instance details and note the IP address assigned to the protected network interface, nic1 if you followed the order of interface creation previously covered in this guide.

Network interfaces

Name	Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP	Network Tier	IP forwarding	Network details
nic0	unprotected-network	unprotected-subnet	fgt1-port1 (10.0.1.11)	–	fgt-ha-vip (35.247.116.241)	Premium	On	View details
nic1	protected-network	protected-subnet	10.0.2.13	–	None			View details
nic2	ha-sync-network	ha-sync-subnet	10.0.3.11	–	None			View details
nic3	mgmt-network	mgmt-subnet	10.0.4.2	–	fgt1-mgmt (35.185.242.37)	Premium		View details

2. Go to *VPC Networks* > *Routes*, then click *CREATE ROUTE*.
3. In the *Name* field, enter the route table name.
4. From the *Network* dropdown list, select the protected network.
5. In the *Destination* field, enter 0.0.0.0/0.
6. In the *Priority* field, enter 10. You can set this to any number less than 1000, which is the default priority for the GCP default route table. This ensures you route all traffic from the protected network through the FortiGate before leaving the VPC.
7. From the *Next hop* dropdown list, select *Specify an IP address*.
8. In the *Next hop IP address* field, enter the IP address of the FortiGate interface assigned to the protected network. In this example, the IP address is 10.0.2.13, but your IP address may be different.
9. Click *Create*.

Uploading the license and configuring network interfaces

1. Go to *Compute Engine* > *VM instances*.
2. Note the external IP addresses assigned to each FortiGate's unprotected network interface.
3. Click the name of each instance and note the instance ID.
4. Configure the primary FortiGate:
   a. Open a web browser window for the primary FortiGate. Go to http://<FortiGate external IP address>.
   b. Log in with admin as the username and the FortiGate instance ID as the password.
   c. FortiOS prompts you to change the admin password immediately. Change the password as required.
   d. Log back into the FortiGate using the admin username and the newly changed password.
   e. Click Upload to install the license. Upload the license. The FortiGate reboots automatically.
   f. Once the reboot is complete, FortiOS redirects you to the dashboard. Go to Network > Interfaces.

g. FortiGate port2, port3, and port4 show no IP addresses. Edit port2:
   i. Under *Address*, ensure that *Manual* is selected under *Addressing Mode*.
   ii. In the *IP/Network Mask* field, enter the IP address that GCP assigned to nic1 with a netmask of 255.255.255.255. While the 255.255.255.255 netmask may seem different from what you would expect in a typical network, it works in GCP due to the SDN capabilities of the GCP VPC.
   iii. Click *OK*.

h. Repeat step 10 for port3 and port4. Port3's IP address is the same as nic2 in GCP, while port4's IP address is the same as nic3 in GCP.

5. Repeat steps 4-11 for the secondary FortiGate.

Setting up FortiGate HA

1. Go to *Compute Engine* > *VM Instances*.
2. Note the external IP addresses assigned to nic0 on each FortiGate.
3. Connect to the primary FortiGate's external IP address using SSH, then enter the following commands:

```
config system ha
   set group-name <choose a group name for the cluster>
   set mode a-p
   set hbdev "port3" 100
   set session-pickup enable
   set session-pickup-connectionless enable
   set ha-mgmt-status enable
config ha-mgmt-interfaces
   edit 1
      set interface "port4"
      set gateway <ip address of MGMT network intrinsic router>
   next
   end
      set override disable
      set priority 255
      set unicast-hb enable
      set unicast-hb-peerip <ip address of HA interface of secondary FortiGate>
      set unicast-hb-netmask <netmask of HA sync network>
end
```

4. Connect to the secondary FortiGate's external IP address using SSH, then enter the following commands:

```
config system ha
   set group-name <enter the same group name you entered in the primary FortiGate>
   set mode a-p
   set hbdev "port3" 100
   set session-pickup enable
   set session-pickup-connectionless enable
   set ha-mgmt-status enable
config ha-mgmt-interfaces
   edit 1
      set interface "port4"
      set gateway <ip address of MGMT network intrinsic router>
   next
   end
      set override disable
      set priority 255
      set unicast-hb enable
      set unicast-hb-peerip <ip address of HA interface of primary FortiGate>
      set unicast-hb-netmask <netmask of HA sync network>
```

```
end
```

5. In the GCP console, go to *VPC network* > *Routes*.
6. Note the name of the default route table created in Creating a GCP route table on page 41.
7. Go to *Compute Engine* > *VM Instances*.
8. Note the primary FortiGate's external IP address.

Setting up a GCP Fabric connector on the primary FortiGate

Lastly, you must configure a GCP Fabric connector on the primary FortiGate. Follow the instructions in Security Fabric Connector Integration with GCP on page 50.

Deploying FortiGate HA using the Google Cloud command interface

This deployment consists of the following steps:

1. Checking the prerequisites on page 43
2. Deploying the FortiGate-VM on page 44

Checking the prerequisites

To deploy and configure the FortiGate-VM as an A-P HA solution, you need the following items:

- Google Cloud command interface. Note that in this example, you will deploy two FortiGate-VMs using Google Cloud. For more information about how to deploy FortiGate-VM using Google Cloud, see Deploying FortiGate-VM using Google Cloud SDK on page 30.
- Availability to accommodate the required GCP resources:
  - Four networks/subnets
    - Ensure that the two FortiGates have connectivity to each other on each network.
    - Appropriate ingress/egress firewall rules for relevant networks (same as a single FortiGate-VM deployment). For detail on open ports that the FortiGate requires, see FortiGate Open Ports.
  - Three public (external) IP addresses:
    - One for traffic to/through the active (primary) FortiGate. At the event of failover, this IP address will move from the primary FortiGate to the secondary. This must be a static external IP. It should be reserved/created before creating FortiGate instances, or promote an ephemeral IP to a static one after deployment. See Reserving a Static External IP Address.
    - Two for management access to each FortiGate. They can be ephemeral IP address, but static ones are highly recommended. See IP Addresses.
  - All internal IP addresses must be static, not DHCP. You should change ephemeral IP addresses to static ones after deployment. See Reserving a Static Internal IP Address.
  - Two FortiGate-VM instances:
    - The two nodes must be deployed in the same region/zone.
    - Each FortiGate-VM must have at least four network interfaces.
    - Each FortiGate-VM should have a log disk attached. Log disks should be created before deploying FortiGate instances. This is the same requirement as when deploying a single FortiGate-VM.
    - Machine types that support at least four network interfaces. See Creating Instances with Multiple Network Interfaces.
    - Two valid FortiGate-VM BYOL licenses. See Licensing on page 6.

- Configuration of SDN Connector with GCP is required. See Security Fabric Connector Integration with GCP on page 50.

Deploying the FortiGate-VM

This deployment method is only applicable for BYOL. The PAYG deployment file will be ready at a later time.

1. Prepare your GCP environment by meeting the prerequisites. Ensure that you have at least four networks.
2. Run the following Google Cloud commands:
   a. Create a disk for each FortiGate as described in step 3 of Using the Google Cloud SDK to deploy FortiGate-VM on page 30. Replace the disk names, zones, and sizes as required.

```
PS C:\Users\jkato> gcloud compute --project=dev-[redacted] disks create jkato-logdisk1 --zone=us-west2-b --type=
pd-standard --size=30GB
WARNING: You have selected a disk size of under [200GB]. This may result in poor I/O performance. For more information,
see: https://developers.google.com/compute/docs/disks#performance.
Created [https://www.googleapis.com/compute/v1/projects/dev-[redacted]/zones/us-west2-b/disks/jkato-logdisk1].
NAME           ZONE        SIZE_GB  TYPE         STATUS
jkato-logdisk1  us-west2-b  30       pd-standard  READY

New disks are unformatted. You must format and mount a disk before it
can be used. You can find instructions on how to do this at:

https://cloud.google.com/compute/docs/disks/add-persistent-disk#formatting

PS C:\Users\jkato>
PS C:\Users\jkato>
PS C:\Users\jkato> gcloud compute --project=dev-[redacted] disks create jkato-logdisk2 --zone=us-west2-b --type=
pd-standard --size=30GB
WARNING: You have selected a disk size of under [200GB]. This may result in poor I/O performance. For more information,
see: https://developers.google.com/compute/docs/disks#performance.
Created [https://www.googleapis.com/compute/v1/projects/dev-[redacted]/zones/us-west2-b/disks/jkato-logdisk2].
NAME           ZONE        SIZE_GB  TYPE         STATUS
jkato-logdisk2  us-west2-b  30       pd-standard  READY

New disks are unformatted. You must format and mount a disk before it
can be used. You can find instructions on how to do this at:

https://cloud.google.com/compute/docs/disks/add-persistent-disk#formatting
```

   b. Create a static external IP address.
   c. Create the two FortiGate-VM instances. Run the Google Cloud command twice to deploy FortiGate-VM instances. In this example, internal static IP addresses are not assigned at the time of deployment. You must assign the static ones to each network interface on each internal network after deployment.

      For details about Google Cloud commands to deploy a FortiGate instance, see Deploying FortiGate-VM using Google Cloud SDK on page 30.

      To deploy the primary FortiGate, run the following command:

```
gcloud compute instances create fortigate1 --network-interface
      network=default,subnet=default,address=your-public-IP-name
      network=vpc2,subnet=internal,no-address --network-interface
      network=vpc3,subnet=subnet3,no-address --network-interface --network-interface
      network=vpc4,subnet=subnet4 --project "your-project" --image your-fortigate-image
      --can-ip-forward --machine-type n1-standard-8 --zone "us-central1-a" --metadata-
      from-file "license=licenseA.txt,user-data=master.txt" --disk=name=your-
      logdisk1,device-name=your-device1,mode=rw,boot=no
```

      To deploy the secondary FortiGate, run the following command:

```
gcloud compute instances create fortigate2 --network-interface
      network=default,subnet=default ----network-interface
      network=vpc2,subnet=internal,no-address network-interface
      network=vpc3,subnet=subnet3,no-address --network-interface
      network=vpc4,subnet=subnet4 --project "your-project" --image your-fortigate-image
      --can-ip-forward --machine-type n1-standard-8 --zone "us-central1-a" --metadata-
```

```
from-file "license=licenseB.txt,user-data=slave.txt" --disk=name=your-
logdisk2,device-name=your-device2,mode=rw,boot=no
```

Replace the VM host names, network names, external (public) IP address name, project name, machine type, zone name, license file name (licenseA.txt, licenseB.txt), FortiGate config file name (primary.txt, secondary.txt), disk names, and device names, with your own.

You can upload a BYOL license on the management GUI later if you do not have licenses at the time of deployment.

In this example, four networks are being used for the following purposes:

Default network (subnet default)	External Internet-facing network. This uses port1 on the FortiGate.
VPC2 (subnet internal)	Internal network where protected VMs are located. This uses port2 on the FortiGate.
VPC3 (subnet 3)	A subnet dedicated to the heartbeat between two FortiGates. This uses port3 on the FortiGate.
VPC4 (subnet 4)	A subnet dedicated to management access to the two FortiGates. This uses port4 on the FortiGate.

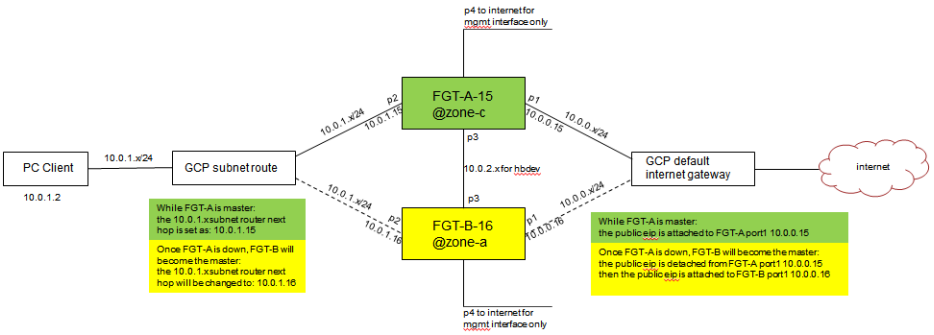
3. After deploying the two FortiGates, connect to each FortiGate management console. Do the following:
   a. Configure the network interfaces, ports 2, 3, and 4 by entering IP addresses and subnets. By default, only port1 is configured. For port4, configure administrative access. You may want to allow HTTPS and SSH.
   b. Shut down the FortiGate-VMs. Allow access to Google Cloud API. See Checking metadata API access on page 52.

Deploying FortiGate-VM HA on GCP between multiple zones

This guide provides a sample deployment of active-passive FortiGate-VM high availability (HA) on GCP between multiple zones:

1. Check the prerequisites before deployment.
2. Create FortiGate A in one zone as the primary FortiGate, using metadata that has the ha-master configuration.
3. Create FortiGate B in another zone as the secondary FortiGate, using metadata that has the ha-slave configuration.
4. Create an Ubuntu PC which can access the Internet via FortiGate HA.
5. Shut down FortiGate A. FortiGate B becomes the primary FortiGate and handles the traffic, and the public external IP address attaches to FortiGate B.
6. Run a diagnose command to see what happened to the route and public external IP address during the failover procedure.

The following depicts the network topology for this sample deployment:



To check the prerequisites:

- Ensure that four VPC networks have been created.
- Ensure that routes have been created for each network.
- Create firewall rules for each network.
- It is suggested to reserve three external IP addresses for convenience.

To create FortiGate A in one zone as the primary FortiGate, using metadata that has the ha-master configuration:

In this example, FortiGate A is created in zone c.

1. Run the following commands in GCP:

```
gcloud beta compute --project=dev-project-001-166400 instances create fgt-a --zone=us-
      central1-c --machine-type=n1-standard-4 --network-tier=PREMIUM --can-ip-forward --
      maintenance-policy=MIGRATE --service-account=966517025500-
      compute@developer.gserviceaccount.com --scopes=https://www.googleapis.com/auth/cloud-
      platform --image=ond-0804 --image-project=dev-project-001-166400 --boot-disk-type=pd-
      standard --boot-disk-device-name=fgt-0804 --network-interface subnet=hapvc-
      port1external,private-network-ip=10.0.0.15,address=104.154.241.0 --network-interface
      subnet=hapvc-port2internal,private-network-ip=10.0.1.15,no-address --network-
      interface subnet=hapvc-port3heartbeat,private-network-ip=10.0.2.15,no-address --
      network-interface subnet=hapvc-port4mgmt,private-network-
      ip=10.0.3.15,address=104.154.25.116 --metadata-from-file user-
      data=/home/gcloud/config/master.conf
```

2. Run the following commands in FortiOS:

```
config system ha
   set group-id 21
   set group-name "cluster1"
   set mode a-p
   set hbdev "port3" 50
   set session-pickup enable
   set session-pickup-connectionless enable
   set ha-mgmt-status enable
   config ha-mgmt-interfaces
      edit 1
         set interface "port4"
         set gateway 10.0.3.1
      next
   end
   set override enable
   set priority 200
   set unicast-hb enable
```

```
   set unicast-hb-peerip 10.0.2.16
   set unicast-hb-netmask 255.255.255.0
end
config system sdn-connector
   edit "gcp_conn"
      set type gcp
      set ha-status enable
      config external-ip
         edit "reserve-fgthapublic"
         next
      end
      config route
         edit "route-internal"
         next
      end
         set use-metadata-iam disable
      set gcp-project "..."
      set service-account "..."
      set private-key "..."
   next
end
```

To create FortiGate B in another zone as the secondary FortiGate, using metadata that has the ha-slave configuration:

In this example, FortiGate B is created in zone a.

1. Run the following commands in GCP:

```
gcloud beta compute --project=dev-project-001-166400 instances create fgt-b --zone=us-
      central1-a --machine-type=n1-standard-4 --network-tier=PREMIUM --can-ip-forward --
      maintenance-policy=MIGRATE --service-account=966517025500-
      compute@developer.gserviceaccount.com --scopes=https://www.googleapis.com/auth/cloud-
      platform --image=ond-0804 --image-project=dev-project-001-166400 --boot-disk-type=pd-
      standard --boot-disk-device-name=fgt-0804 --network-interface subnet=hapvc-
      port1external,private-network-ip=10.0.0.16,no-address --network-interface
      subnet=hapvc-port2internal,private-network-ip=10.0.1.16,no-address --network-
      interface subnet=hapvc-port3heartbeat,private-network-ip=10.0.2.16,no-address --
      network-interface subnet=hapvc-port4mgmt,private-network-
      ip=10.0.3.16,address=35.226.235.236 --metadata-from-file user-
      data=/home/gcloud/config/slave.conf
```

2. Run the following commands in FortiOS:

```
config system ha
   set group-id 21
   set group-name "cluster1"
   set mode a-p
   set hbdev "port3" 50
   set session-pickup enable
   set session-pickup-connectionless enable
   set ha-mgmt-status enable
   config ha-mgmt-interfaces
      edit 1
         set interface "port4"
         set gateway 10.0.3.1
      next
   end
   set override enable
   set priority 200
```

```
    set unicast-hb enable
    set unicast-hb-peerip 10.0.2.15
    set unicast-hb-netmask 255.255.255.0
end
```

To create an Ubuntu PC that can access the Internet via FortiGate HA:

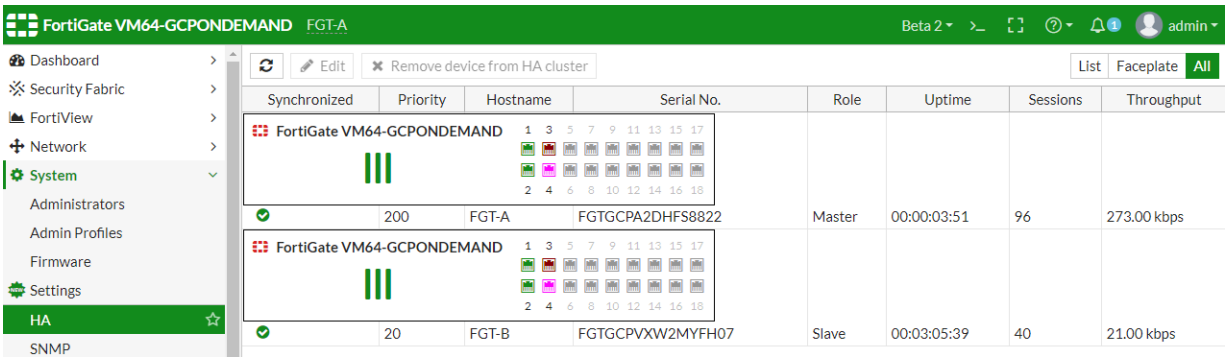
Run the following commands in GCP:

```
gcloud beta compute --project=dev-project-001-166400 instances create fgt-b --zone=us-
    central1-a --machine-type=n1-standard-4 --network-tier=PREMIUM --can-ip-forward --
    maintenance-policy=MIGRATE --service-account=966517025500-
    compute@developer.gserviceaccount.com --scopes=https://www.googleapis.com/auth/cloud-
    platform --image=ond-0804 --image-project=dev-project-001-166400 --boot-disk-type=pd-
    standard --boot-disk-device-name=fgt-0804 --network-interface subnet=hapvc-
    port1external,private-network-ip=10.0.0.16,no-address --network-interface subnet=hapvc-
    port2internal,private-network-ip=10.0.1.16,no-address --network-interface subnet=hapvc-
    port3heartbeat,private-network-ip=10.0.2.16,no-address --network-interface subnet=hapvc-
    port4mgmt,private-network-ip=10.0.3.16,address=35.226.235.236 --metadata-from-file user-
    data=/home/gcloud/config/slave.conf
```

To test FortiGate-VM HA:

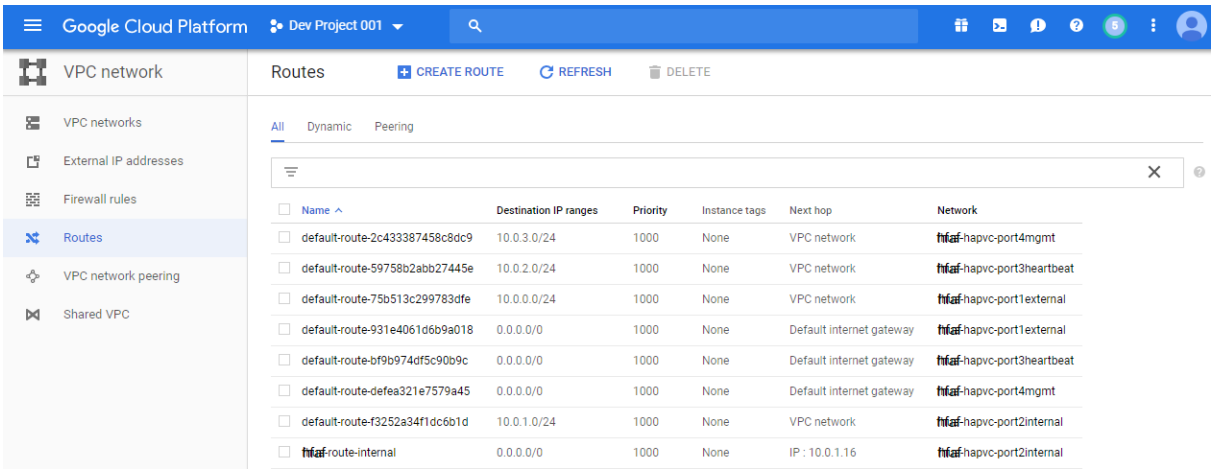
1. Ensure that the HA status is in-sync and that the public external IP address (104.154.241.0 in this example) is attached to the primary FortiGate:

```
FGT-A # get sys ha status
HA Health Status: OK
Model: FortiGate-VM64-GCPONDEMAND
Mode: HA A-P
Group: 21
Debug: 0
Cluster Uptime: 0 days 3:7:1
Cluster state change time: 2019-01-16 17:17:11
Master selected using:
   <2019/01/16 17:17:11> FGTGCPA2DHFS8822 is selected as the master because it has the
        largest value of override priority.
   <2019/01/16 17:17:11> FGTGCPA2DHFS8822 is selected as the master because it's the only
        member in the cluster.
ses_pickup: enable, ses_pickup_delay=disable
override: enable
unicast_hb: peerip=10.0.2.16, myip=10.0.2.15, hasync_port='port3'
Configuration Status:
   FGTGCPA2DHFS8822(updated 4 seconds ago): in-sync
   FGTGCPVXW2MYFH07(updated 3 seconds ago): in-sync
```



2. Log into the PC.

3. Verify that the PC can access the Internet via FortiGate A, since FortiGate A is the primary FortiGate. Verify that the route-internal route gateway is set as 10.0.1.15, the FortiGate A IP address.
4. Shut down FortiGate A.
5. Verify that FortiGate B is now the primary FortiGate.
6. Using an API call, ensure that the route-internal route was removed and replaced with a new one, which has set the gateway as 10.0.1.16, the FortiGate B IP address.



7. Verify that the public IP address has detached from FortiGate A and is attached to FortiGate B.
8. Log into the PC.
9. Verify that the PC can access the Internet via FortiGate B, since FortiGate B is now the primary FortiGate.

To run diagnose commands:

After FortiGate A is shut down and FortiGate B becomes the new primary FortiGate, run the following diagnose command to see what happened to the route and public external IP address during the failover procedure:

```
FGT-B # d deb app gcpd -1
```

The following shows the procedure of removing the old route (route-internal) and replacing it with a new route:

```
failover route: route-internal (destRange: 0.0.0.0/0, nextHop: 10.0.1.15)
move next hop from 10.0.1.15 to 10.0.1.16
remove route route-internal on next hop 10.0.1.15
create route route-internal on next hop 10.0.1.16
gcpd api post data: { "name": "route-internal", "network":
      "https://www.googleapis.com/compute/v1/projects/dev-project-001-
      166400/global/networks/hapvc-port2internal", "destRange": "0.0.0.0/0", "nextHopIp":
      "10.0.1.16", "priority": "1000" }
route route-internal is updated to next hop 10.0.1.16 successfully.
```

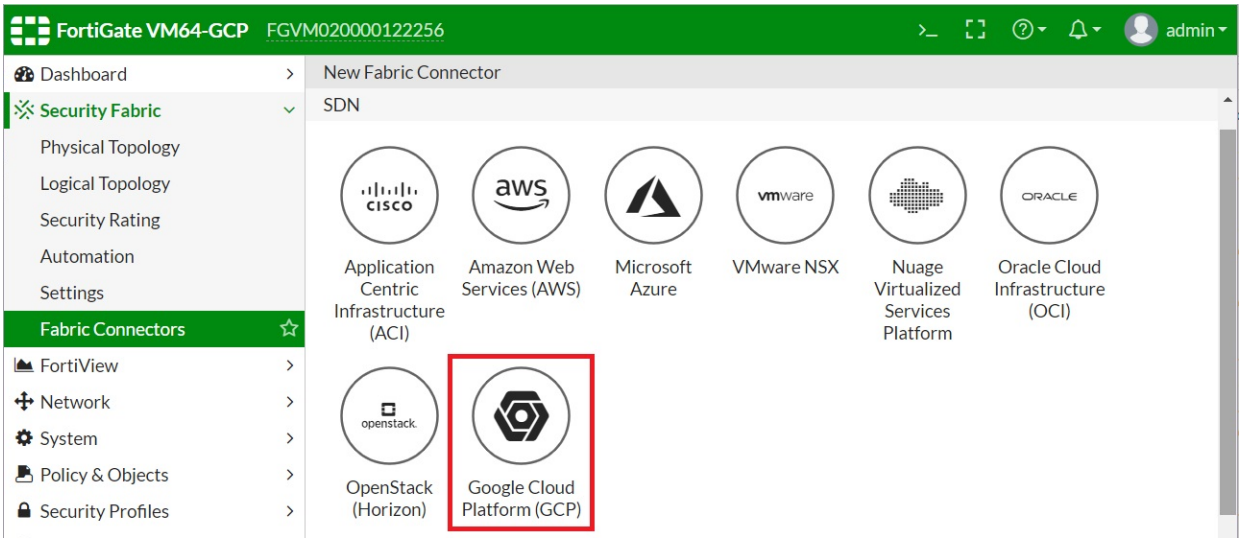
The following shows the procedure of attaching a public external IP address to the new primary FortiGate B:

```
eip: reserve-fgthapublic(104.154.241.0)
eip reserve-fgthapublic(104.154.241.0) is attached in remote instance: us-central1-c/fgt-a,
      should be moved to local
get instance nic: nic0, 10.0.0.15, hapvc-port1external, accessConfig(external-nat), eip
      (104.154.241.0)
nic0 of instance fgt-a is using eip 104.154.241.0
remove eip 104.154.241.0 from instance fgt-a(nic0).
attach eip 104.154.241.0 to instance fgt-b(nic0).
gcpd api post data: { "name": "external-nat", "natIP": "104.154.241.0"}
eip reserve-fgthapublic(104.154.241.0) is attached to local successfully.
```

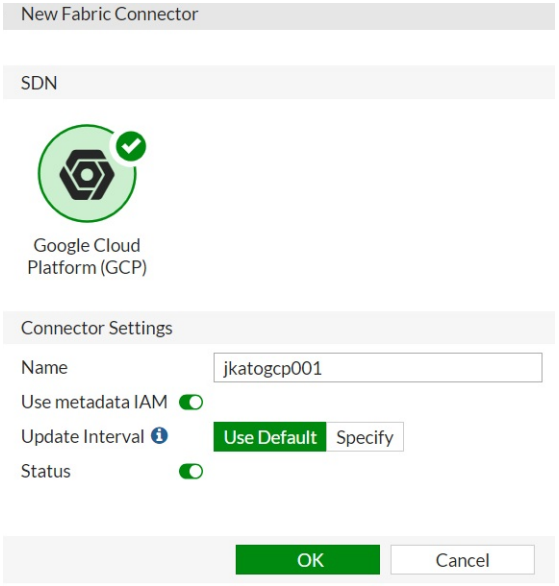
Security Fabric Connector Integration with GCP

Configuring GCP SDN Connector on FortiGate for GCP

1. In FortiOS, go to *Security Fabric* > *Fabric Connectors*.
2. Click *Create New*, and select *Google Cloud Platform (GCP)*.

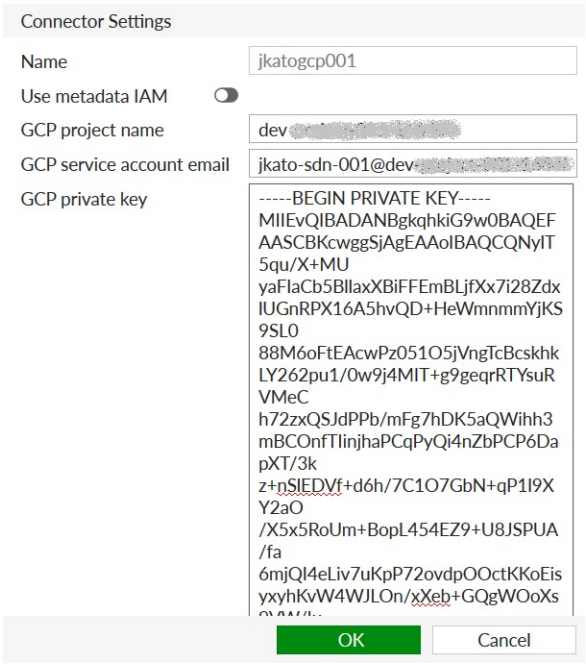


Note you can create only one SDN Connector per connector type. For example, you can create one entry for GCP.

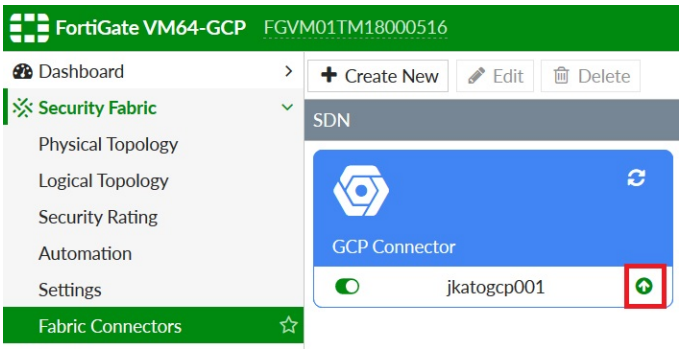


3. Configure the connector as follows:
   a. *Name*: Enter the desired connector name.
   b. *Use metadata IAM*: The Google platform requires a certain authentication level to call APIs from the FortiGate.
      i. If you enable *Use metadata IAM*, ensure that the FortiGate has API access on Google Compute Engine. For details, see Checking metadata API access on page 52.
      ii. If you do not enable *Use metadata IAM*, you must specify your own service account.

      The *Use metadata IAM* option is only available to FortiGate-VMs running on GCP. FortiGates running outside of GCP (including physical FortiGate units and FortiGate-VMs running on other cloud platforms) have a configuration that is equivalent to disabling this option.
   c. *GCP project name*: Enter the name of the GCP project. The VMs whose IP addresses you want to populate should be running within this project.
   d. *GCP service account email*: Enter the email address associated with the service account that will call APIs to the GCP project specified above.
   e. *GCP private key*: Enter the private key statement as shown in the text box. For details, see Creating a GCP service account on page 54.
   f. *Update interval*: the default value is 60 seconds. You can enter a value between 1 and 3600 seconds.
   g. *Status*: Green means that the connector is enabled. You can disable it at any time by toggling the switch.



Once the connector is successfully configured, a green indicator appears at the bottom right corner. If the indicator is red, the connector is not working. See Troubleshooting GCP SDN Connector on page 58.



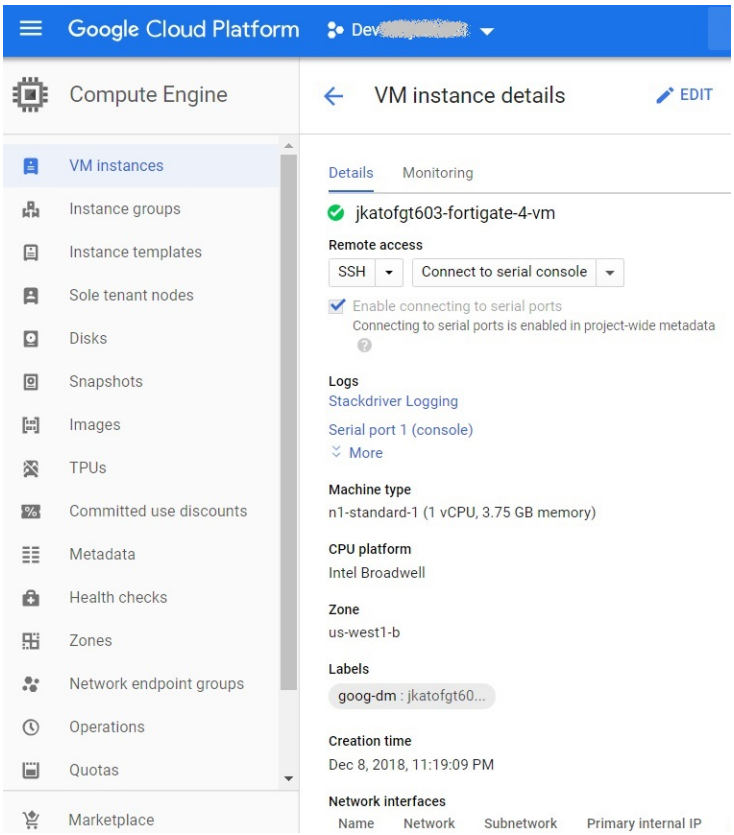
GCP Kubernetes (GKE) Fabric connector

GCP Fabric connectors support dynamic address groups based on GCP Kubernetes Engine (GKE) filters. See the *FortiOS Cookbook*.

Checking metadata API access

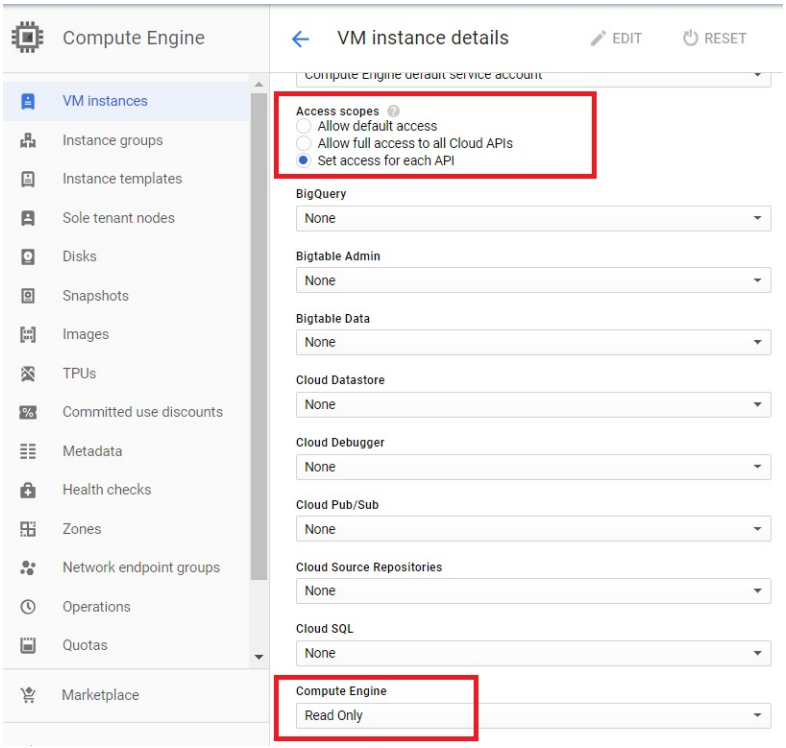
To populate dynamic objects, the FortiGate-VM must have API access to required resources on the Google Cloud Compute Engine.

1. On the GCP Compute Engine, go to the FortiGate-VM.



2. Scroll down to *Cloud API Access Scopes* and check the Compute Engine configuration. If Compute Engine is configured as disabled, you must enable it:
   a. Stop the VM.
   b. Once the VM is completely stopped, click *Edit*.

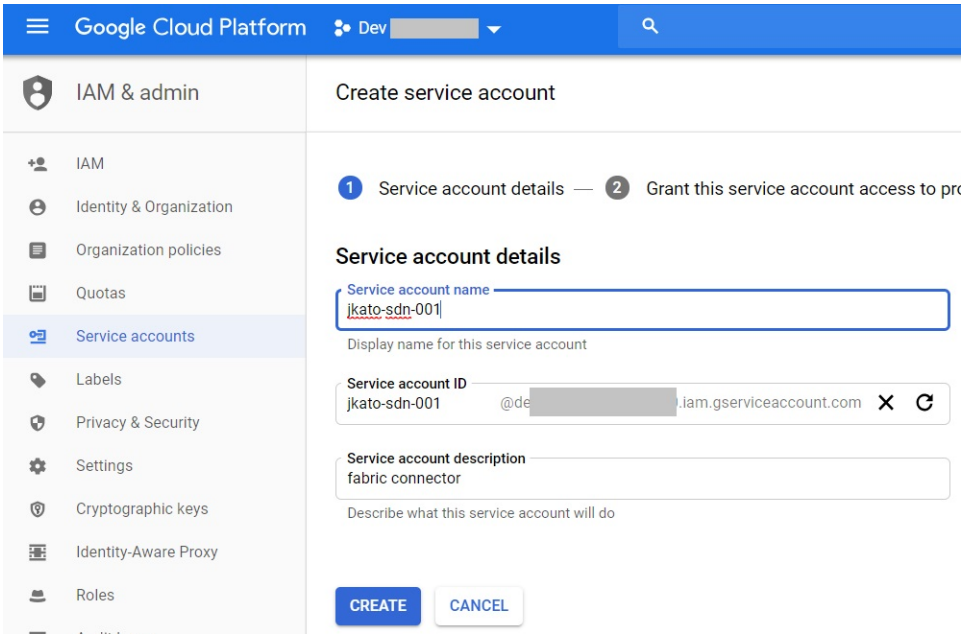
c. From the *Compute Engine* dropdown list, select *Read Only* or a higher access level.



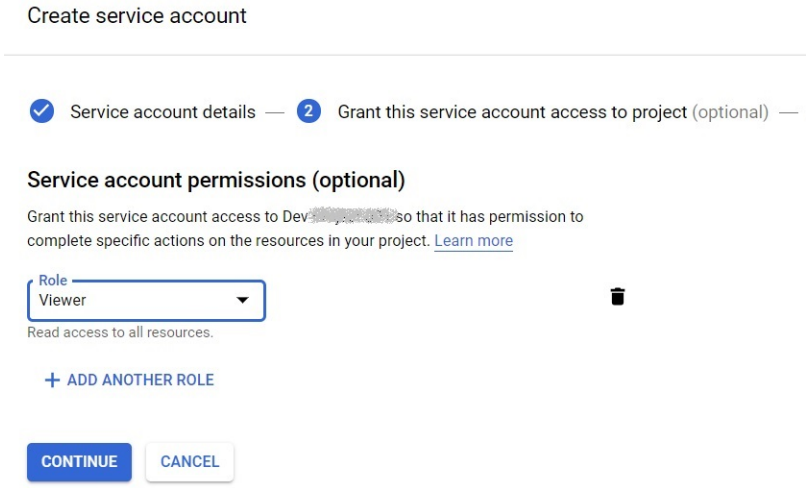
d. Save the change, then restart the VM.

Creating a GCP service account

1. Log into the GCP Compute Portal.

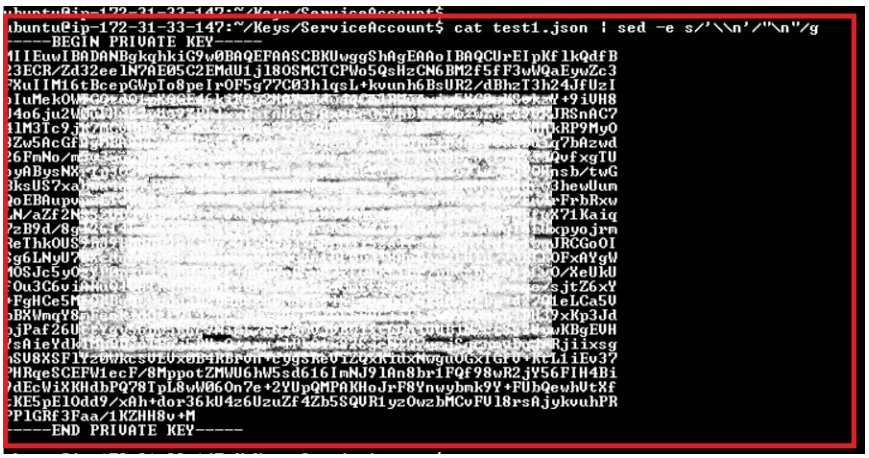


2. Go to *IAM & admin* > *Service accounts*.
3. Create a service account.
   a. Name the account, then click *CREATE*.



   b. From the *Role* dropdown list, select *Viewer*, then click *CONTINUE*.
   c. (Optional) Configure user access.
4. Create the service account key. This example describes creating a private key in JSON format.
5. Once created, the key automatically downloads to your PC. Click *Done*.
6. Use a text editor to open the downloaded key. Find the line "`"private_key": "-----BEGIN PRIVATE KEY-----\n.....`" This line contains line breaks with "`\n`". Therefore, copying and pasting the line into the FortiOS GUI will not work.
7. Remove "`\n`" using a tool or command of your choice. For example, the Linux command shown below removes "`\n`". In this example, output.json is the downloaded key file which includes line breaks:

```
$cat <output.json> | sed -e s/'\\n'/"\n"/g
```



8. Copy and paste the key content into the FortiOS GUI.

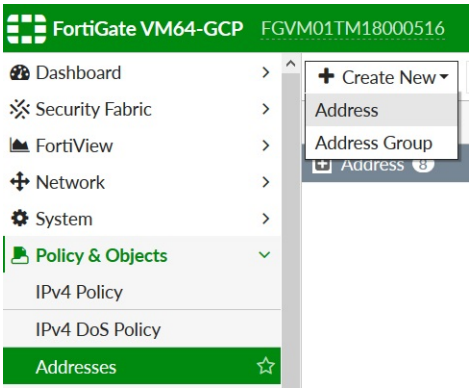
Creating an Address

Creating an Address consists of the following:

- Creating an “Address”, which will be used as an address group or single address to be used for source/destination of firewall policies. The Address is based on IP addresses.
- The Address contains IP addresses of GCP instances that are currently running.
- When changes occur on the instances, the SDN Connector populates and updates the changes automatically based on the specified filtering condition so administrators do not need to reconfigure the Address’s content manually
- Appropriate firewall policies using the Address are applied to the instances that are members of it.

The following describes creating an Address using the FortiOS GUI. If you are familiar with the FortiOS CLI, you an also create an Address using the CLI.

1. In FortiOS, go to *Policy & Objects* > *Addresses*. Click *Create New*, then select *Address*.

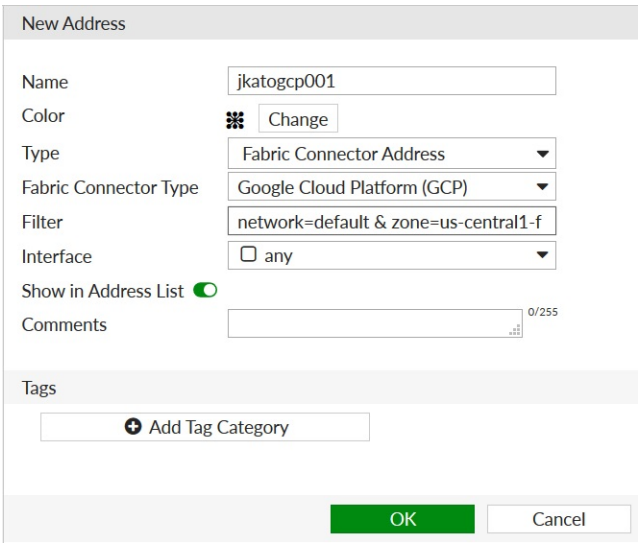


2. Configure the Address:
   a. *Name*: Enter the desired name.
   b. *Type*: Select *Fabric Connector Address*.
   c. *Fabric Connector Type*: Select *Google Cloud Platform (GCP)*.
   d. *Filter*: This means the SDN Connector automatically populates and updates only instances belonging to the specified VPN that match this filtering condition. Currently GCP supports the following filters:
      i. `id=<instance id>` : This matches an VM instance ID.
      ii. `name=<instance name>` : This matches a VM instance name.
      iii. `zone=<gcp zones>` : This matches a zone name.
      iv. `network=<gcp network name>` : This matches a network name.
      v. `subnet=<gcp subnet name>` : This matches a subnet name.
      vi. `tag=<gcp network tags>` : This matches a network tag.
      vii. `label.<gcp label key>=<gcp label value>` : This matches a free form GCP label key and its value.

      In the example, the filter is set as `'network=default & zone=us-central-1f'`. This configuration populates all IP addresses that belong to the default network in the zone us-central-1f.

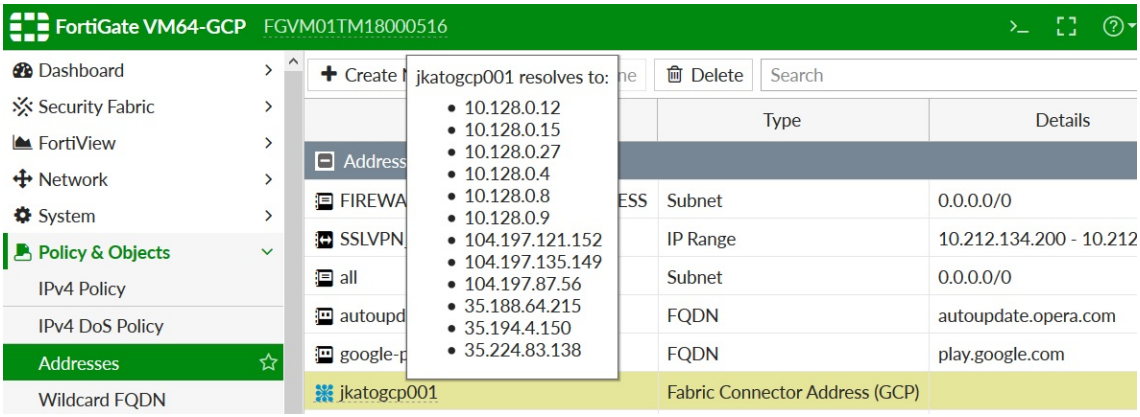
      You can set filtering conditions using multiple entries with AND ("&") or OR ("|"). When both AND and OR are specified, AND is interpreted first, then OR.

      Note that wildcards (such as the asterisk) are not allowed in filter values.



e. Click *OK*.

The Address has been created. Wait for a few minutes before the setting takes effect. You will know that the Address is in effect when the exclamation mark disappears from the Address entry. When you hover over the Address, you can see the list of populated IP addresses.



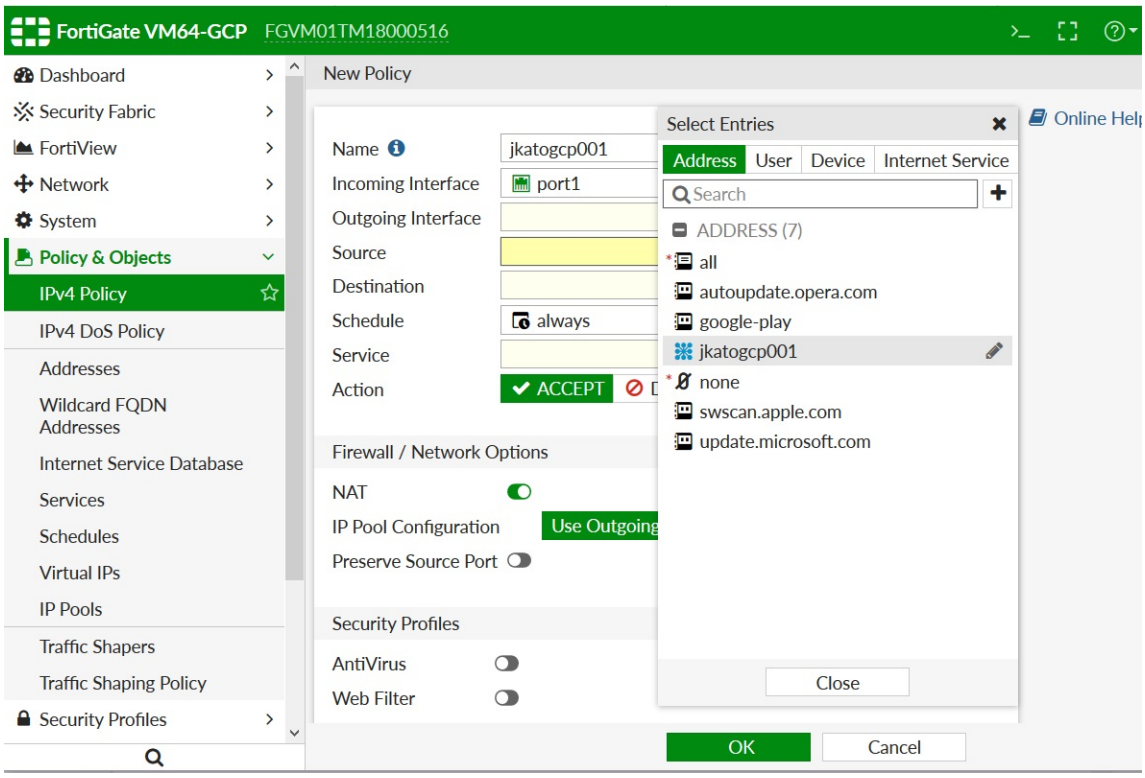
If the exclamation mark does not disappear, check the Address settings.

Creating a firewall policy

Finally, you can use this Address to configure a firewall policy as a source or destination. The following operation is not SDN Connector-specific but shows a general way of creating a firewall policy in FortiOS.

You can use the GUI or CLI to create the firewall policy. The example below shows a firewall policy where the newly created Address is specified as the source or destination.

Go to *Policy & Objects* > *IPv4 Policy*, and create a firewall policy. Specify the created Address as a source or destination.



Troubleshooting GCP SDN Connector

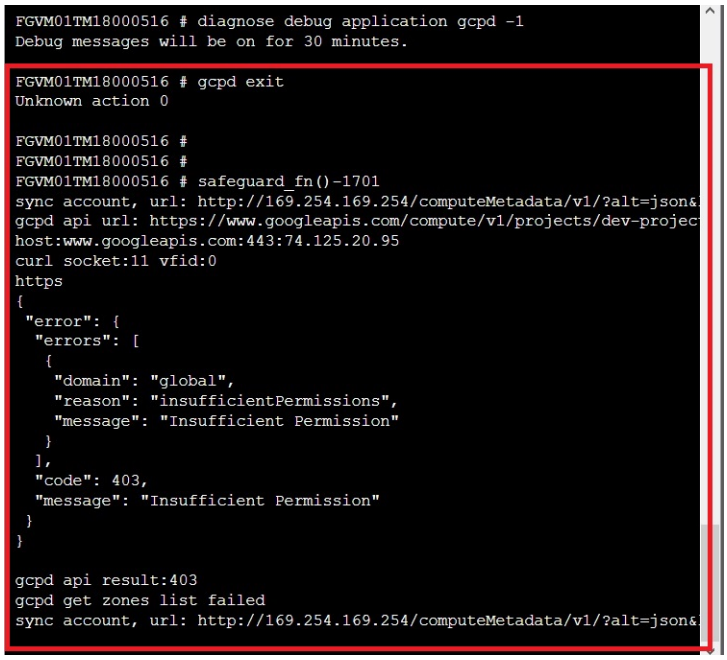
You can check if API calls are made successfully by running the following commands in the CLI:

```
diagnose debug enable
diagnose debug application gcpd -1
```

```
FGVM01TM18000516 # diagnose debug enable

FGVM01TM18000516 # diagnose debug application gcpd -1
Debug messages will be on for 30 minutes.
```

Wait a few minutes for the output. If the SDN connector was configured successfully, the API status shows `200` in communicating with the Google Cloud API server as shown below. The host looks different depending on where you run the FortiGate instance (on or outside of GCP).

```
FGVM01TM18000517 (global) # diag debug enable

FGVM01TM18000517 (global) # diagnose debug application gcpd -1
Debug messages will be on for 30 minutes.

FGVM01TM18000517 (global) #
FGVM01TM18000517 (global) # gcpd api url: https://www.googleapis.com/compute/v
host:www.googleapis.com:443:172.217.8.170
gcpd api result:200
host:www.googleapis.com:443:172.217.8.170
gcpd get instance list successfully
gcpd checking firewall address object jkatogcp001, vd 0
```



If the CLI shows a failure, check the following and see if any required configuration is missing or incorrect:

- If using metadata IAM, can the FortiGate-VM access the API on Google Cloud Compute Engine?
- If the service account is specified:
  - Is the project name correct?
  - Is the service account email address correct?
  - Is the service account key correct?
  - Does the service account have the appropriate role/permissions?

Deploying auto scaling on GCP

This recipe provides instructions for deploying auto scaling on GCP. This recipe consists of the following steps:

1. Create an instance template with the GCP console.
2. Create an instance group with the GCP console.
3. Set the first FortiGate-VM in the auto scaling group (ASG) as the primary member.
4. Scale out a new FortiGate-VM and set it as the secondary member.
5. Run `diagnose` commands.

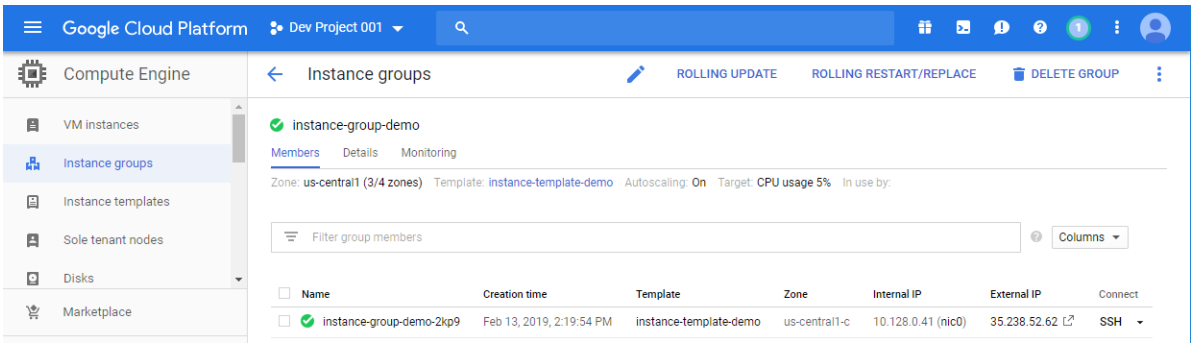
To create an instance template with the GCP console:

1. On the GCP console, go to *Instance templates*, then click *CREATE INSTANCE TEMPLATE*.
2. In the *Name* field, enter the desired instance template name.
3. From the *Machine type* dropdown list, select the desired machine type.
4. Under *Boot disk*, select the FortiGate-VM image.
5. Under *Firewall*, enable *Allow HTTP traffic* and *Allow HTTPS traffic*.
6. Click *Create*.
7. Go to *Instance templates* and check that the instance template has been created.

To create an instance group with the GCP console:

1. Go to *Instance groups*, then click *CREATE INSTANCE GROUP*.
2. Configure the instance group:
   a. In the *Name* field, enter the desired instance group name.
   b. From the *Instance template* dropdown list, select the instance template created earlier.
   c. From the *Autoscaling* dropdown list, select *On*.
   d. From the *Autoscaling policy* dropdown list, select *CPU usage*.
   e. In the *Target CPU usage* field, enter the target CPU usage. This is treated as a percentage. For example, if 60% CPU usage is the target, enter 60.
   f. In the *Minimum number of instances* field, enter the minimum number of instances desired for this instance group. For this example, enter 1.
   g. In the *Maximum number of instances* field, enter the maximum number of instances desired for this instance group.
   h. In the *Cool down period* field, enter the number of seconds that the autoscaler should wait after a VM has started before collecting information from it. This accounts for the amount of time that it can take for a VM to initialize, during which the collected usage is not reliable for auto scaling. The default cool down period is 60 seconds.
3. Click *Create*.
4. Go to *Instance groups* and check that the instance group has been created.
5. After a few minutes, click the group to check that an instance was launched automatically, since the minimum number of instances is set as 1. In this example, the first FortiGate-VM instance has been launched and is called

"instance-group-demo-2kp9".

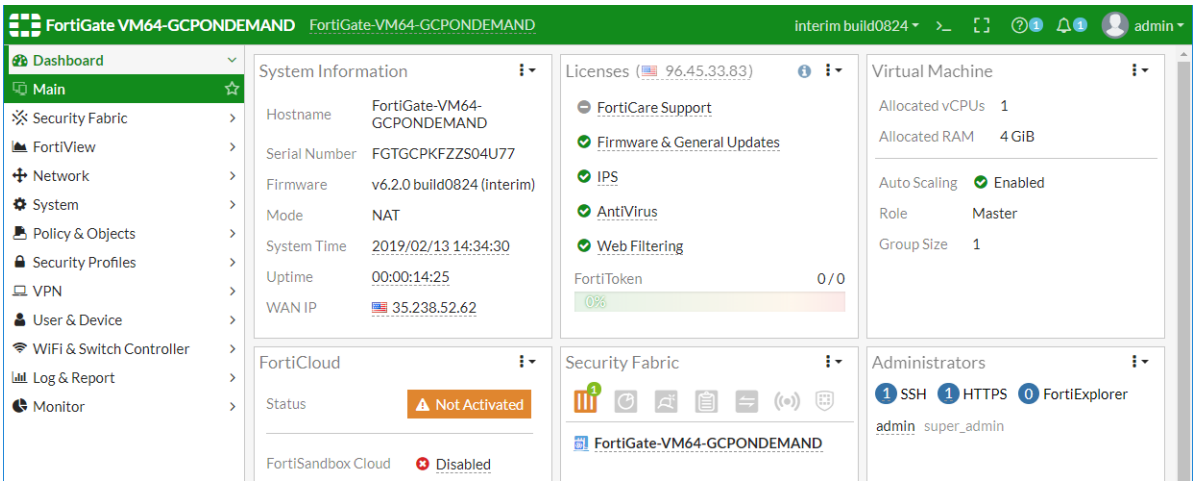


To set the first FortiGate-VM in the ASG as the primary member:

1. Log into FortiOS on the FortiGate-VM using the username "admin" and the instance ID as the password.
2. Run the following commands to enable auto scaling and set this FortiGate-VM as the primary member:

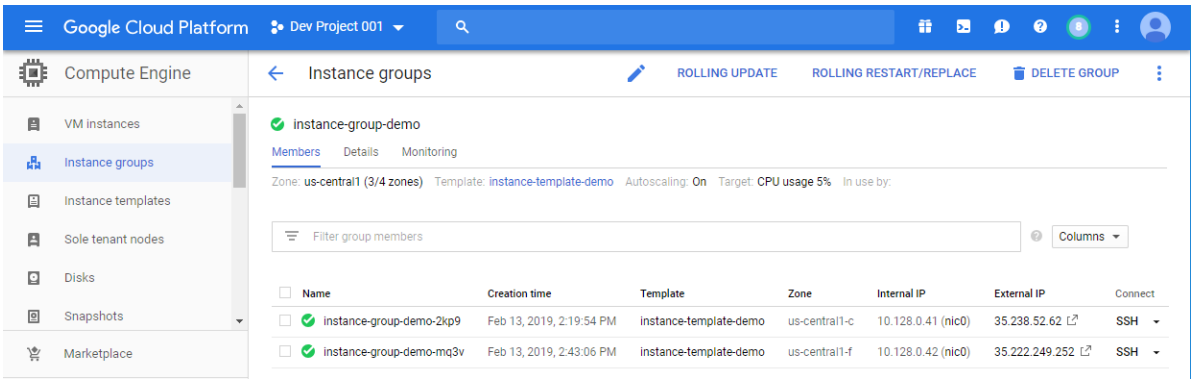
```
config system auto-scale
   set status enable
   set role master
   set sync-interface "port1"
   set psksecret xxxxxx
end
```

3. Log into the FortiOS GUI. Check the *Dashboard* > *Virtual Machine* widget to ensure that auto scaling is enabled and that this FortiGate-VM's *Role* is *Master*.



To scale out a new FortiGate-VM and set it as the secondary member:

1. Generate traffic on the FortiGate-VM to ensure that the CPU rate is higher than the instance group target CPU usage. For testing purposes, you can also lower the target CPU usage.
2. Go to *Instance groups* to verify that the instance group scaled out a new FortiGate-VM. In this example, the second FortiGate-VM instance is named "instance-group-demo-mq3v".



3. Log into FortiOS on the new FortiGate-VM using the username "admin" and the instance ID as the password.
4. Run the following commands to enable auto scaling, set this FortiGate-VM as the secondary member, and configure the primary FortiGate's IP address (using the primary FortiGate's private IP address). Ensure that the configuration can be synced only from the primary to the secondary FortiGate:

```
config system auto-scale
   set status enable
   set role slave
   set sync-interface "port1"
   set master-ip 10.128.0.41
   set psksecret xxxxxx
end
```

After a few minutes, the secondary FortiGate is synced with the primary FortiGate. The secondary FortiGate can synchronize the FortiGate configuration from the primary FortiGate.

To run `diagnose` commands:

Run the `diag deb app hasync -1` command to check if the secondary FortiGate is synced with the primary FortiGate. The output should resemble the following:

```
FortiGate-VM64-GCPON~AND # diag deb app hasync -1
slave's configuration is not in sync with master's, sequence:0
slave's configuration is not in sync with master's, sequence:1
slave's configuration is not in sync with master's, sequence:2
slave's configuration is not in sync with master's, sequence:3
slave's configuration is not in sync with master's, sequence:4
slave starts to sync with master
logout all admin users
```

Change log

Date	Change Description
2019-03-28	Initial release.
2019-06-28	Added GCP Kubernetes (GKE) Fabric connector on page 52.