



FortiOS - GCP Administration Guide

Version 6.4

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



August 30, 2021

FortiOS 6.4 GCP Administration Guide

01-640-619463-20210830

TABLE OF CONTENTS

About FortiGate-VM for GCP	5
Machine type support	5
Upgrading or downgrading a GCP instance to another machine type	6
Models	7
Licensing	8
Order types	8
Creating a support account	10
Migrating a FortiGate-VM instance between license types	11
Deploying FortiGate-VM on Google Cloud Marketplace	12
Initially deploying the FortiGate-VM	12
Deployment variables	21
Registering and downloading your license	21
Connecting to the FortiGate-VM	21
Deploying FortiGate-VM on Google Cloud Compute Engine	24
Obtaining the deployment image	24
Uploading the FortiGate deployment image to Google Cloud	24
Creating the FortiGate deployment image	25
Deploying the FortiGate-VM instance	27
Connecting to the FortiGate-VM	31
Configuring Google Cloud firewall rules	36
Configuring the second NIC on the FortiGate-VM	38
Deploying FortiGate-VM using Google Cloud SDK	40
Using the Google Cloud SDK to deploy FortiGate-VM	40
Bootstrapping FortiGate at initial bootup	43
Deploying FortiGate-VM using Terraform	45
High availability for FortiGate-VM on GCP	46
Deploying FortiGate-VM HA on GCP in one zone	46
Deploying FortiGate HA using the GCP GUI	47
Deploying FortiGate HA using the Google Cloud command interface	54
Deploying FortiGate-VM HA on GCP between multiple zones	57
SDN connector integration with GCP	63
Configuring GCP SDN Connector using service account	63
Custom role permission guideline	63
API calls	64
Multiple GCP projects in a single SDN connector	64
GCP Kubernetes (GKE) SDN connector	69
Configuring GCP SDN connector using metadata IAM	69
Creating a GCP service account	73
Troubleshooting GCP SDN Connector	78

Pipelined automation using Google Cloud function	79
Deploying auto scaling on GCP	80
Requirements	80
Account permissions	80
Region requirements	80
Deployment	81
Quotas	82
Terraform variables	83
Deployment information	85
Verify the deployment	86
Verify the instance group	88
Cluster monitoring	89
Adding instances to the protected subnet	90
Destroying the cluster	94
Troubleshooting	95
Debugging cloud-init	95
How to reset the elected primary FortiGate	96
Appendix	96
FortiGate Autoscale for GCP features	96
Architectural diagram	98
VPN for FortiGate-VM on GCP	99
Site-to-site IPsec VPNs between HA VPN on GCP	99
Packet mirroring	100
Creating VPC networks	100
Launching the FortiGate-VM instance	101
Creating an unmanaged instance group and load balancer	102
Configuring bidirectional VPC peering	103
Creating the packet mirroring policy	103
Verifying the configuration	104
Change log	105

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	See Deploying FortiGate-VM on Google Cloud Marketplace on page 12 .
Google Cloud Compute Engine	<p>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 24. You must deploy FortiGate in this method when:</p> <ul style="list-style-type: none">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. (A future release may support this). 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	<p>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 40.</p>

Machine type support

You can deploy FortiGate for GCP 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.

FortiOS 6.4.3 and later versions support hot-adding vCPU and RAM. However, GCP may not support this. See [Changing the machine type of a VM instance](#).

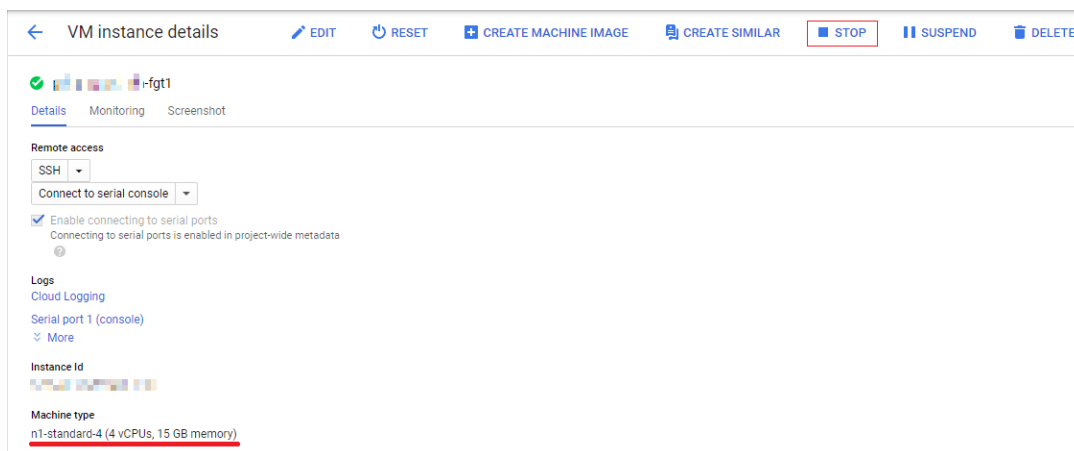
Upgrading or downgrading a GCP instance to another machine type

With FortiGate-VM BYOL instances, you must source appropriate licenses to support the change in machine types for FortiGate-VM BYOL instances and add the licenses manually. You may have to add a new license to correspond to the new processor core count. See [How to upgrade FortiGate VM license](#).

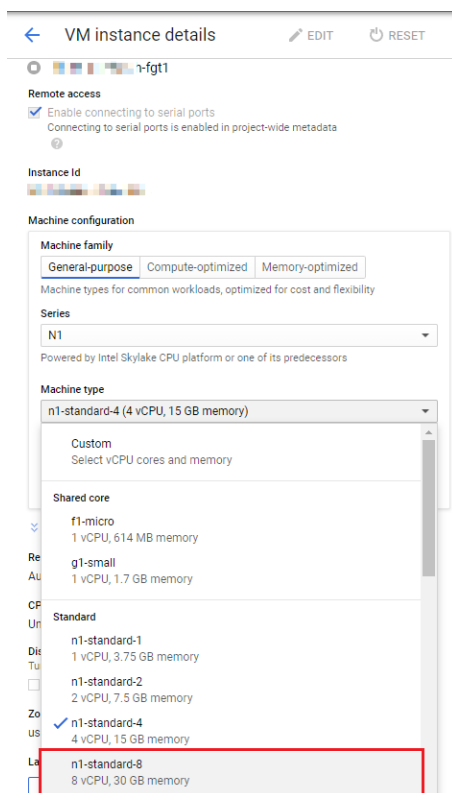
Editing the instance configuration does not allow you to add or delete network interfaces.

To upgrade or downgrade a GCP instance to another machine type:

1. Go to *Compute Engine > Instances*.
2. Select the desired instance.
3. On the *VM instance details* page, click *STOP* to shut down the VM. In this example, the original machine type is n1-standard-4.



4. Once the VM is powered off, click *EDIT* on the VM instance details page.
5. From the *Series* and *Machine type* dropdown lists, select the desired new series and machine type. This example upgrades the VM instance from n1-standard-4 to n1-standard-8.



6. Click **Save**.
7. Select the VM and click **START/RESUME**.

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 8.

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



The v-series and s-series do not support virtual domains (VDMs) by default. To add VDMs, you must separately purchase perpetual VDOM addition licenses. You can add and stack VDMs 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 8](#)
- [Creating a support account on page 10](#)
- [Migrating a FortiGate-VM instance between license types on page 11](#)

Order types

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

BYOL offers perpetual (normal series and v-series) and annual subscription (s-series, available starting Q4 2019) 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.

With a PAYG subscription, the FortiGate-VM 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. New s-series SKUs contain the VM base and service bundle entitlements for easier ordering. 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 10](#).



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

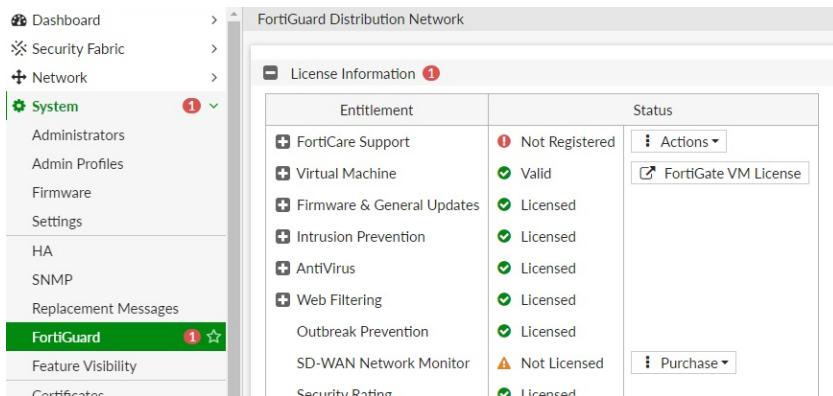


PAYG and BYOL licensing and payment models are not interchangeable. For example, once you spin up a FortiGate-VM PAYG instance, you cannot inject a BYOL license on the same VM. Likewise, you cannot convert a FortiGate-VM BYOL instance to PAYG.

When using a FortiGate-VM on-demand instance prior to version 6.4.2, the FortiOS GUI may display expiry dates for FortiGuard services. However, these expiries are automatically extended for as long as the on-demand instance's lifespan. You do not need to be concerned about the expiry of FortiGuard services. For example, the following screenshot shows 2038/01/02.

Entitlement	Status
FortiCare Support	Not Supported
Firmware & General Updates	Licensed - expires on 2038/01/02
Application Control Signatures	Version 16.00975
Device & OS Identification	Version 1.00110
Internet Service Database Definitions	Version 7.01212
Intrusion Prevention	Licensed - expires on 2038/01/02
IPS Definitions	Version 16.00975
IPS Engine	Version 5.00021

FortiOS 6.4.2 and later versions do not display dates.



Creating a support account

FortiGate for GCP supports both PAYG and BYOL licensing models. See [Order types on page 8](#).

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](#).

BYOL

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

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

To activate a BYOL license:

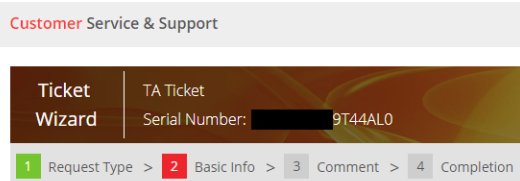
1. Go to [Customer Service & Support](#) and create a new account or log in with an existing account.
2. Go to *Asset > Register/Activate* to start the registration process.
3. In the *Registration* page, enter your license activation code, then select *Next* to continue registering the product.
4. If you register the S-series subscription model, the site prompts you to select one of the following:
 - a. Click *Register* to newly register the code to acquire a new serial number with a new license file.
 - b. Click *Renew* to renew and extend the licensed period on top of the existing serial number, so that all features on the VM node continue working uninterrupted upon license renewal.
5. At the end of the registration process, download the license (.lic) file to your computer. You 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

To activate a PAYG license:

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/Activate* to start the registration process.
5. In the *Registration* page, 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.



Migrating a FortiGate-VM instance between license types

When deploying a FortiGate-VM on public cloud, you determine the license type (PAYG or BYOL) during deployment. The license type is fixed for the VM's lifetime. The image that you use to deploy the FortiGate-VM on the public cloud marketplace predetermines the license type.

Migrating a FortiGate-VM instance from one license type to another requires a new deployment. You cannot simply switch license types on the same VM instance. However, you can migrate the configuration between two VMs running as different license types. There are also FortiOS feature differences between PAYG and BYOL license types. For example, a FortiGate-VM PAYG instance is packaged with Unified Threat Management protection and does not support VDOMs, whereas a FortiGate-VM BYOL instance supports greater protection levels and features depending on its contract.

To migrate FortiOS configuration to a FortiGate-VM of another license type:

1. Connect to the FortiOS GUI or CLI and back up the configuration. See [Configuration backups](#).
2. Deploy a new FortiGate-VM instance with the desired license type. If deploying a BYOL instance, you must purchase a new license from a Fortinet reseller. You can apply the license after deployment via the FortiOS GUI or bootstrap the license and configuration during initial bootup using custom data as described in [Bootstrapping FortiGate at initial bootup on page 43](#).
3. Restore the configuration on the FortiGate-VM instance that you deployed in step 2. As with the license, you can inject the configuration during initial bootup. Alternatively, you can restore the configuration in the FortiOS GUI as described in [Configuration backups](#).
4. If you deployed a PAYG instance in step 2, register the license. To receive support for a PAYG license, you must register the license as described in [Creating a support account on page 10](#).

Deploying FortiGate-VM on Google Cloud Marketplace

Initially deploying the FortiGate-VM

To perform initial deployment of the FortiGate-VM:

1. In the Google Cloud marketplace Cloud Launcher, find FortiGate Next-Generation Firewall. Select bring-your-own-license or pay-as-you-go according to your needs.

2. Click *LAUNCH*.

3. Configure the variables as required:

New FortiGate Next-Generation Firewall (BYOL) deployment

Deployment name *
fortigate-deployment-example

Zone
us-central1-f

Machine type

Machine family

GENERAL-PURPOSE

COMPUTE-OPTIMIZED

Machine types for common workloads, optimized for cost and flexibility

Series

N2

Powered by Intel Cascade Lake and Ice Lake CPU platforms

Machine type

n2-standard-4 (4 vCPU, 16 GB memory)



vCPU

4

Memory

16 GB

Boot Disk

Boot disk type *

SSD Persistent Disk

Boot disk size in GB *

10

Log Disk

☒ Enable log disk

Log disk type

SSD Persistent Disk

Log disk size in GB

30

See [Deployment variables](#) for descriptions of the deployment variables:

4. Add more networks and network interfaces if desired:
 - a. Under *Network interfaces*, click *ADD NETWORK INTERFACE*.
 - b. Select the desired network and subnetwork, then click *DONE*.

Networking

Network interfaces

unprotected-public unprotected-public-subnet (10.0.1.0/24)	▼
protected-private protected-private-subnet (10.0.2.0/24)	▼

Network interface ^

☒ Networks in this project

☐ Networks shared with me (from host project: shared-vpc-project-301520)

Network

ha-sync ▼ ?

Subnetwork

ha-sync-subnet ▼ ?

External IP

None ▼ ?

CANCEL

DONE

ADD NETWORK INTERFACE

Networking

Network interfaces

unprotected-public unprotected-public-subnet (10.0.1.0/24)	▼
protected-private protected-private-subnet (10.0.2.0/24)	▼
ha-sync ha-sync-subnet (10.0.3.0/24)	▼
ha-mgmt ha-mgmt-subnet (10.0.4.0/24)	▼
ADD NETWORK INTERFACE	

Firewall

Add tags and firewall rules to allow specific network traffic from the Internet



Creating certain firewall rules may expose your instance to the Internet. Please check if the rules you are creating are aligned with your security preferences. [Learn more](#)

☒ Allow TCP port 22 traffic

Source IP ranges for TCP port 22 traffic



☒ Allow HTTPS traffic

Source IP ranges for HTTPS traffic



☒ Allow HTTP traffic

Source IP ranges for HTTP traffic



☒ Allow TCP port 541 traffic

Source IP ranges for TCP port 541 traffic



☒ Allow TCP port 3000 traffic

Source IP ranges for TCP port 3000 traffic



☒ Allow TCP port 8080 traffic

Source IP ranges for TCP port 8080 traffic





In this example, the HA-Sync and HA-Mgmt networks were added to NIC 3 and NIC 4 respectively to illustrate the support of multiple networks. If you are not configuring high availability, you can select other networks for any NIC on the FortiGate deployment.



Google Cloud instances support a maximum of eight interfaces, based on the selected VM type.

5. Click *Deploy*. When deployment is done, the following screen appears.



FortiGate Next-Generation Firewall (BYOL)

Solution provided by Fortinet Inc.

Admin URL	https:// /
Admin user	admin
Admin password (Temporary)	
Instance	fortigate-deployment-example-vm
Instance zone	us-central1-f
Instance machine type	n2-standard-4

▼ MORE ABOUT THE SOFTWARE

Get started with FortiGate Next-Generation Firewall (BYOL)

[LOG INTO THE ADMIN PANEL](#) [SSH](#)

Suggested next steps

- **License Registration**
[Registering and Downloading Your License](#)
- **Initial Access and Configuration**
[Deploying FortiGate-VM on GCP Cloud Launcher](#)
- **Change the temporary password**
For additional security, it is recommended that you change the password.

Documentation

- [Administration Guide](#)
How to deploy and configure FortiGate 7.2 on Google Cloud
- [Protecting Docker Environments](#)
Docker/container environment protection while inspecting application traffic
- [Set-up Tutorial Video](#)
Quick overview on how to deploy FortiGate
- [Secure SD-WAN Architecture](#)
FortiGate Secure SD-WAN on Google Cloud Reference Architecture
- [Data Sheet](#)
Datasheet of FortiGate-VM on GCP

Support

Fortinet FortiCare Support Services give you global support on a per-product basis. By subscribing to these services, you'll receive a timely response to any technical issue as well as complete visibility on ticket resolution progress. All FortiCare Support Services include firmware upgrades, access to the support portal and associated technical

Deployment variables

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	Select the network located in the selected zone.
Subnetwork	Select the subnetwork where the FortiGate resides.
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 <i>Ephemeral</i> . You must access the FortiOS GUI via this public IP address.
Enable log disk	Enable the log disk.
Log disk type	Select the desired log disk type.
Log disk size in GB	Select the desired log disk size or leave as-is at 30 GB.
Delete log disk when instance is deleted	If enabled, the log disk is removed once you delete the FortiGate-VM instance. To retain the log disk after FortiGate-VM instance deletion, leave this disabled.
Image Version	Select the FortiGate version. The latest version is the default.

Registering and downloading your license

Follow the instructions detailed in [BYOL on page 10](#), then continue to [Connecting to the FortiGate-VM on page 21](#).

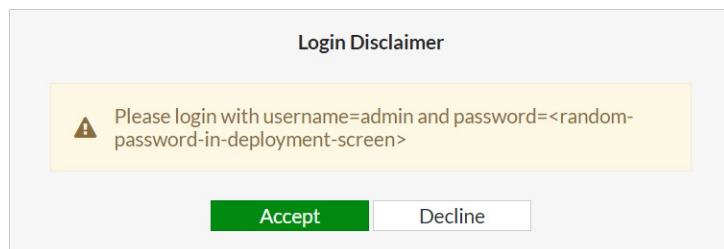
Connecting to the FortiGate-VM

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 that Google Cloud automatically generates.

To connect to the FortiGate-VM:

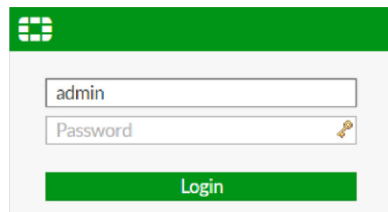
1. Connect to the FortiGate using your browser. Your browser displays a certificate error message, which is normal because browsers do not recognize the default self-signed FortiGate certificate. Proceed past this error.

2. If accessing the FortiGate for the first time via the GUI (HTTPS, port 443) or SSH (port 22), you see the following disclaimer. Click *Accept*.



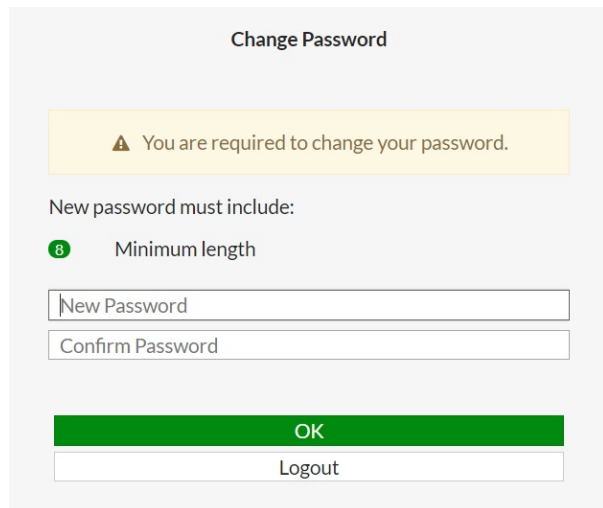
The screenshot shows a 'Login Disclaimer' window. At the top, it says 'Login Disclaimer'. Below that is a yellow box with a warning icon and the text: 'Please login with username=admin and password=<random-password-in-deployment-screen>'. At the bottom, there are two buttons: 'Accept' (green) and 'Decline' (white).

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



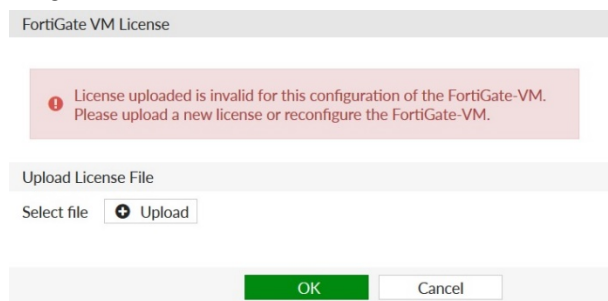
The screenshot shows the login interface. At the top is a green header with the FortiGate logo. Below it are two input fields: 'admin' for the username and 'Password' for the password. There is a key icon next to the password field. At the bottom is a green 'Login' button.

4. Change the password.



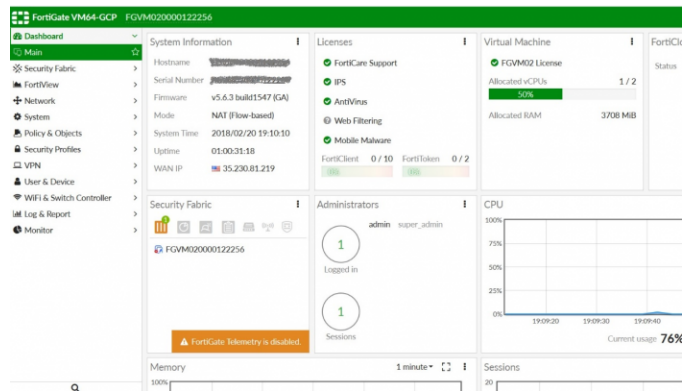
The screenshot shows the 'Change Password' screen. At the top is a yellow box with a warning icon and the text: 'You are required to change your password.' Below that, it says 'New password must include:'. There is a green circle with the number '8' and the text 'Minimum length'. Below that are two input fields: 'New Password' and 'Confirm Password'. At the bottom are two buttons: 'OK' (green) and 'Logout' (white).

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.



The screenshot shows the 'FortiGate VM License' screen. At the top is a header 'FortiGate VM License'. Below that is a red box with a warning icon and the text: 'License uploaded is invalid for this configuration of the FortiGate-VM. Please upload a new license or reconfigure the FortiGate-VM.' Below that is a section 'Upload License File' with a 'Select file' button and an 'Upload' button. At the bottom are two buttons: 'OK' (green) and 'Cancel' (white).

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



Deploying FortiGate-VM on Google Cloud Compute Engine

Obtaining the deployment image

To obtain 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.



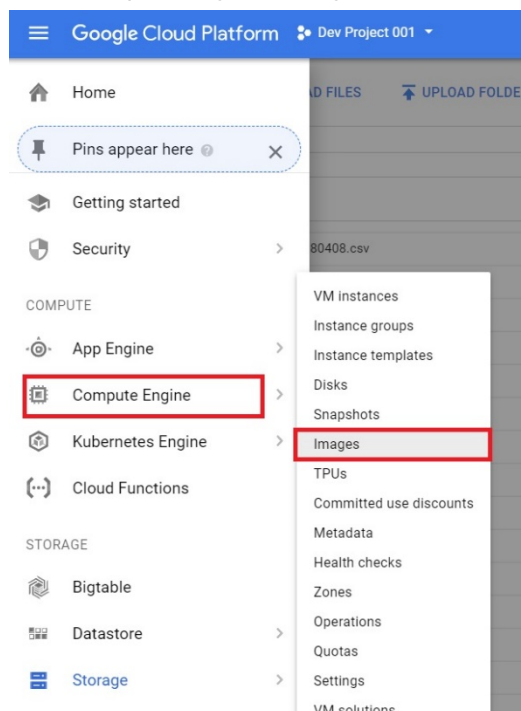
This deployment method is only applicable for BYOL. The PAYG deployment file will be ready at a later time.

Uploading the FortiGate deployment image to Google Cloud

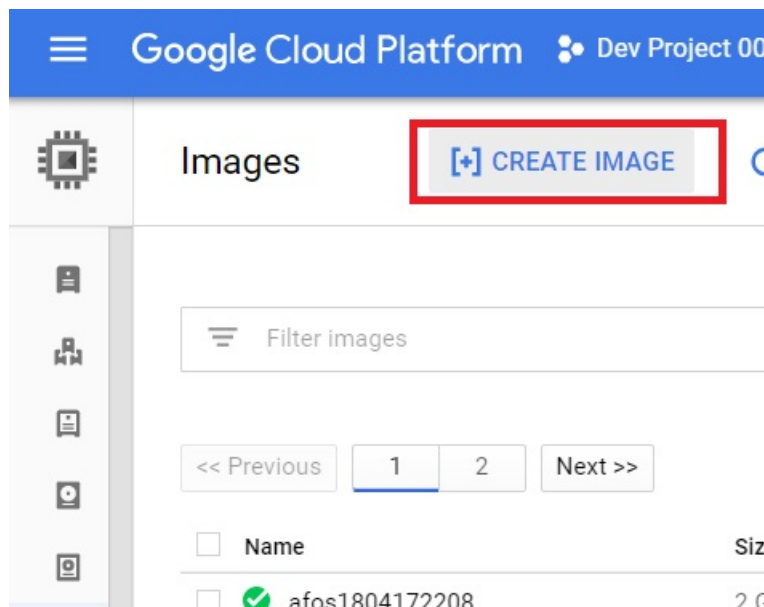
1. Log into Google Cloud.
2. Go to *Storage > Browser*.
3. Create a new bucket or go to an existing bucket.
4. Upload the newly downloaded deployment file.

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*.

Google Cloud Platform Dev Project 001

Create an image

Name ?

fortigatejkatoimage001

Family (Optional) ?

Description (Optional)

Encryption ?

Automatic (recommended)

Source ?

Cloud Storage file

Cloud Storage file ?

Your image source must use the .tar.gz extension and the file inside the archive must be named disk.raw. [Learn more](#)

☒ jkato001/FGT_VM64_GCP-v5-build1547-FORTINET.out.gcp.tar.gz

Equivalent [REST](#) or [command line](#)

The image is listed on the *Images* pane.

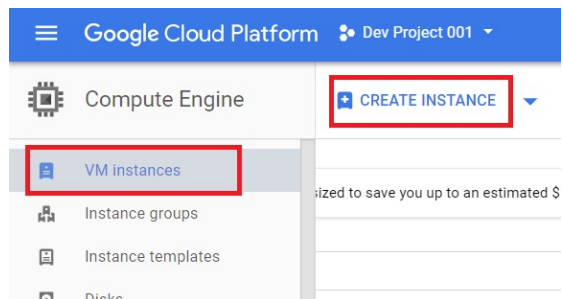
Google Cloud Platform Dev Project 001

Images [+ CREATE IMAGE](#) [REFRESH](#) [+ CREATE INSTANCE](#) [DEPRECATE](#) [DELETE](#)

<input type="checkbox"/>	<input checked="" type="checkbox"/>	fortigatejkatoimage001	2 GB	Dev Project 001	Apr 20, 2018, 1:14:11 PM
<input type="checkbox"/>	<input checked="" type="checkbox"/>	fortinettechfortios	2 GB	Dev Project 001	Feb 20, 2018, 11:02:51 AM

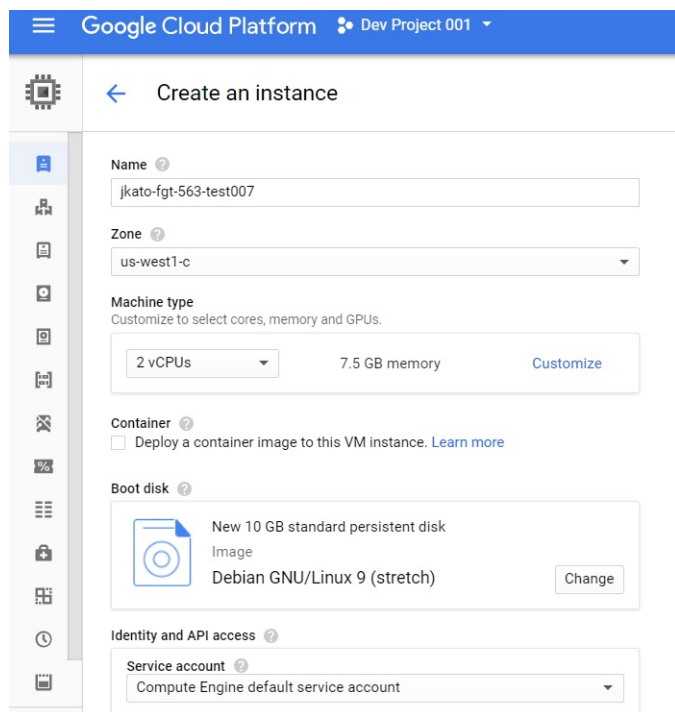
Deploying the FortiGate-VM instance

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*.

Boot disk

Select an image or snapshot to create a boot disk; or attach an existing disk

OS images Application images **Custom images** Snapshots Existing disks

Created from Dev Project 001 on Apr 12, 2018, 4:06:48 PM

- ☒ **fortigatejkatolimage001**
Created from Dev Project 001 on Apr 20, 2018, 1:14:11 PM
- ☐ fortigatejkatolimage002
Created from Dev Project 001 on Feb 20, 2018, 11:02:51 AM
- ☐ fortipoc-golden
Created from Dev Project 001 on Jan 11, 2018, 9:29:40 PM
- ☐ fortipoc-golden2
FortiPoc Golden 2
Created from Dev Project 001 on Jan 29, 2018, 5:38:28 PM
- ☐ fortipoc-golden3
fortipoc-golden-sample3-09-14-2018
Created from Dev Project 001 on Mar 14, 2018, 10:17:40 AM
- ☐ fortipoc-jordan
Created from Dev Project 001 on Feb 7, 2018, 11:00:20 AM
- ☐ fos1530-1711142148
Created from Dev Project 001 on Nov 14, 2017, 1:48:17 PM
- ☐ fw6-brot-591
Created from Dev Project 001 on Mar 28, 2018, 7:27:01 PM
- ☐ fw6-brodermann-591
Created from Dev Project 001 on Mar 28, 2018, 6:10:30 PM
- ☐ fw617
Created from Dev Project 001 on Apr 17, 2018, 1:04:28 AM
- ☐ fw6ga-yhy
Created from Dev Project 001 on Mar 29, 2018, 11:10:17 PM

Can't find what you're looking for? Explore hundreds of VM solutions in [Cloud Launcher](#)

Boot disk type [?] Size (GB) [?]

SSD persistent disk 10

Select Cancel

- 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 36](#).
- 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.

Google Cloud Platform Dev Project 001

← Create an instance

New 10 GB SSD persistent disk
Image
fortigatejkatimage001 Change

Identity and API access

Service account
Compute Engine default service account

Access scopes
☒ Allow default access
☐ Allow full access to all Cloud APIs
☐ Set access for each API

Firewall
Add tags and firewall rules to allow specific network traffic from the Internet
☐ Allow HTTP traffic
☒ Allow HTTPS traffic

Management Disks **Networking** SSH Keys

Network tags (Optional)

Network interfaces

default default (10.138.0.0/20)

- 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*.

Google Cloud Platform Dev Project 001

← Create an instance

Management Disks **Networking** SSH Keys

Network tags (Optional)

Network interfaces

Network interface

Network
default

Subnetwork
default (10.138.0.0/20)

Primary internal IP
Ephemeral (Automatic)

Show alias IP ranges

External IP
Ephemeral

IP forwarding
On

Public DNS PTR Record
☒ Enable
 PTR domain name

Done Cancel

- 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*.

Network interface [X]

Network
jkato002

Subnetwork
privfacing4

Internal IP
fortigateprivip (10.3.0.2)

Internal IP type
Static

[Show alias IP ranges](#)

External IP ⓘ
None

Done Cancel

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

Google Cloud Platform Dev Project 001

← Create an instance

Identity and API access ⓘ

Service account ⓘ
Compute Engine default service account

Access scopes ⓘ
☒ Allow default access
☐ Allow full access to all Cloud APIs
☐ Set access for each API

Firewall ⓘ
 Add tags and firewall rules to allow specific network traffic from the Internet
☐ Allow HTTP traffic
☐ Allow HTTPS traffic

Firewalls setup is not available for multiple network interfaces

Management Disks **Networking** SSH Keys

Network tags ⓘ (Optional)

Network interfaces ⓘ

default default (10.138.0.0/20)	✎
jkato002 privfacing4 (10.3.0.0/16)	✎

[+ Add network interface](#)

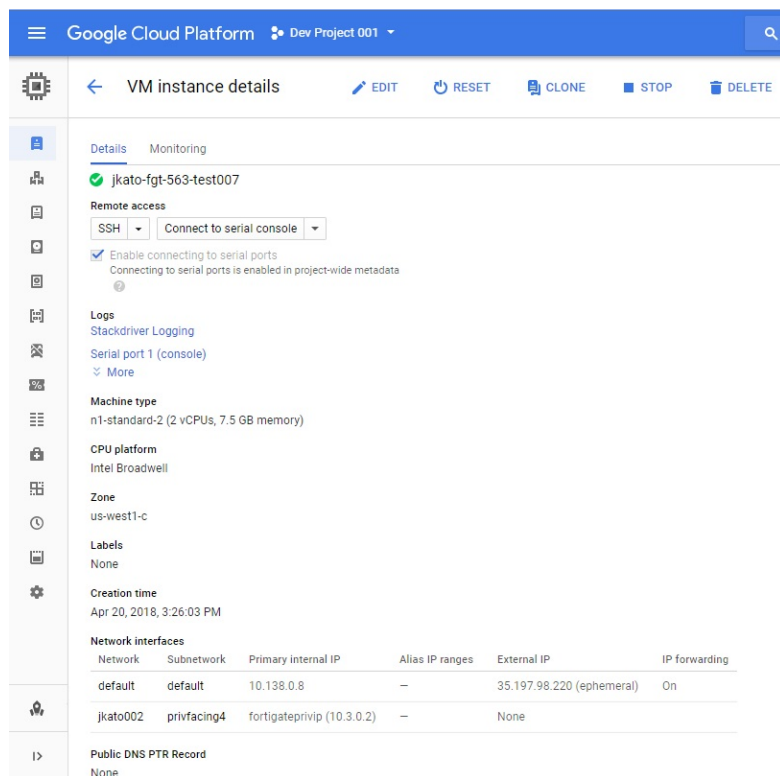
[Less](#)

You will be billed for this instance. [Learn more](#)

Create Cancel

Equivalent REST or command line

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



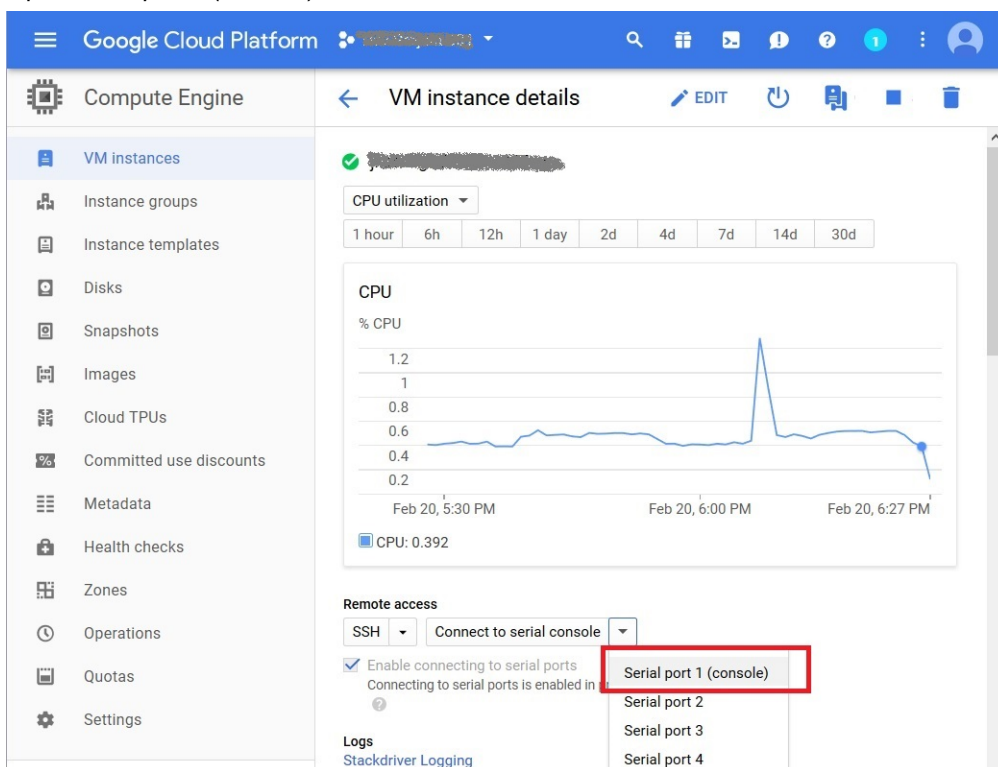
Connecting to the FortiGate-VM

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

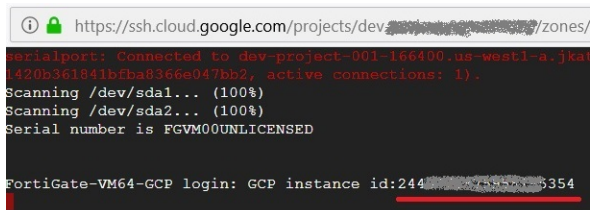
To connect to the FortiGate-VM:

1. Choose the instance from the list of instances on the *VM Instances* page.
2. Depending on how you provisioned the instance, you must use the instance ID or the `fortigate_user_password` as the password. The instance ID is represented as a number that can be found after locating the instance in the GCP Compute Engine console.
 - a. There are two methods to obtain the instance ID. To use the instance ID as the password, do one of the following:

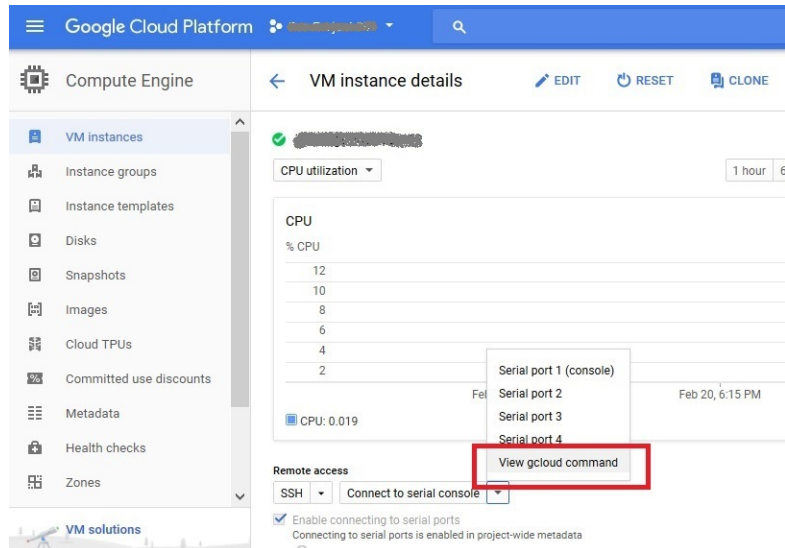
- i. Open *Serial port 1 (console)* as seen.



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



ii. Do the following:

i. Select *View gcloud command* on the VM instance details.ii. Click *RUN IN CLOUD SHELL*.

gcloud command line

This is the gcloud command line with the parameters you have selected.

```
gcloud compute --project=dev-XXXXXXXXXX connect-to-serial-port XXXXXXXXXX --zone=us-centra
11-f
```

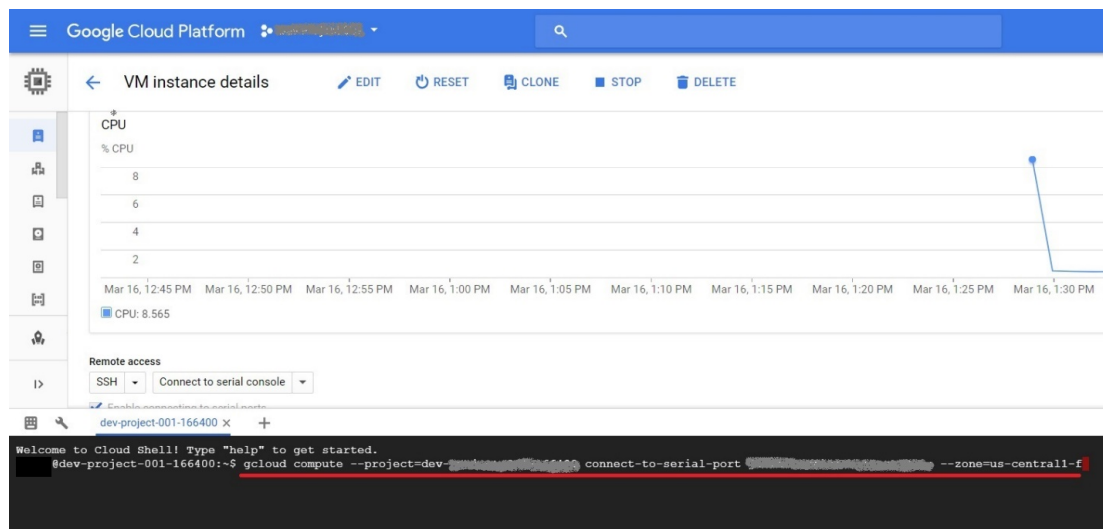
☒ Line wrapping

[gcloud reference](#)

CLOSE

RUN IN CLOUD SHELL

iii. By default, a command is shown as underlined in the following example. Delete the command shown underlined.



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

```
Welcome to Cloud Shell! Type "help" to get started.
@dev-project-001-166400:~$ gcloud compute instances describe <instance_name>
```

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

```
dev-project-001-166400 x
creationTimestamp: '2018-03-16T13:27:55.300-07:00'
deletionProtection: false
disks:
- autoDelete: true
  boot: true
  deviceName: <device_name>-tmpl-boot-disk
  index: 0
  interface: SCSI
  kind: compute#attachedDisk
  licenses:
  - https://www.googleapis.com/compute/v1/projects/fortigcp-.../global/licenses/fortigate
  mode: READ_WRITE
  source: https://www.googleapis.com/compute/v1/projects/dev-.../zones/us-central1-f/disks/<disk_name>
  type: <disk_type>
  id: '504...5461'
kind: ComputeInstance
labelFingerprint: <label_fingerprint>
machineType: https://www.googleapis.com/compute/v1/projects/dev-.../zones/us-central1-f/machineTypes/n1-standard-2
metadata:
  fingerprint: <fingerprint>
  items:
  - key: ssh-keys
    value: |
```

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

```
@dev-project-001-166400:~$ gcloud compute instances describe <instance_name> | grep id:
No zone specified. Using zone [us-central1-f] for instance: [<instance_name>].
id: '504...5461'
@dev-project-001-166400:~$
```

- b. To use the `fortigate_user_password` as the password, go to the *VM instance details* page and find the `fortigate_user_password` under *Custom metadata*.

Google Cloud Platform Terraform	
Compute Engine	VM instance details EDIT RESET
VM instances	On host maintenance Migrate VM instance (recommended)
Instance groups	Automatic restart On (recommended)
Instance templates	Custom metadata
	fortigate_user_password PD5gHY*D

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.

Google Cloud Platform VM instance details

Remote access: SSH, Connect to serial console

Enable connecting to serial ports: Connecting to serial ports is enabled in project-wide metadata

Logs: Stackdriver Logging, Serial port 1 (console), More

Machine type: n1-standard-1 (1 vCPU, 3.75 GB memory)

CPU platform: Intel Broadwell

Zone: us-west1-a

Labels: None

Creation time: Feb 20, 2018, 6:33:26 PM

Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP	IP forwarding
default	default	10.138.0.2	—	35.230.64.221 (ephemeral)	Off

Public DNS PTR Record: None

Firewalls: Allow HTTP traffic, Allow HTTPS traffic

Network tags

4. Access the FortiGate in your browser.

admin

Password

Login

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 (the instance ID or fortigate_user_password, depending on how you provisioned this instance).
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.

FortiGate VM License

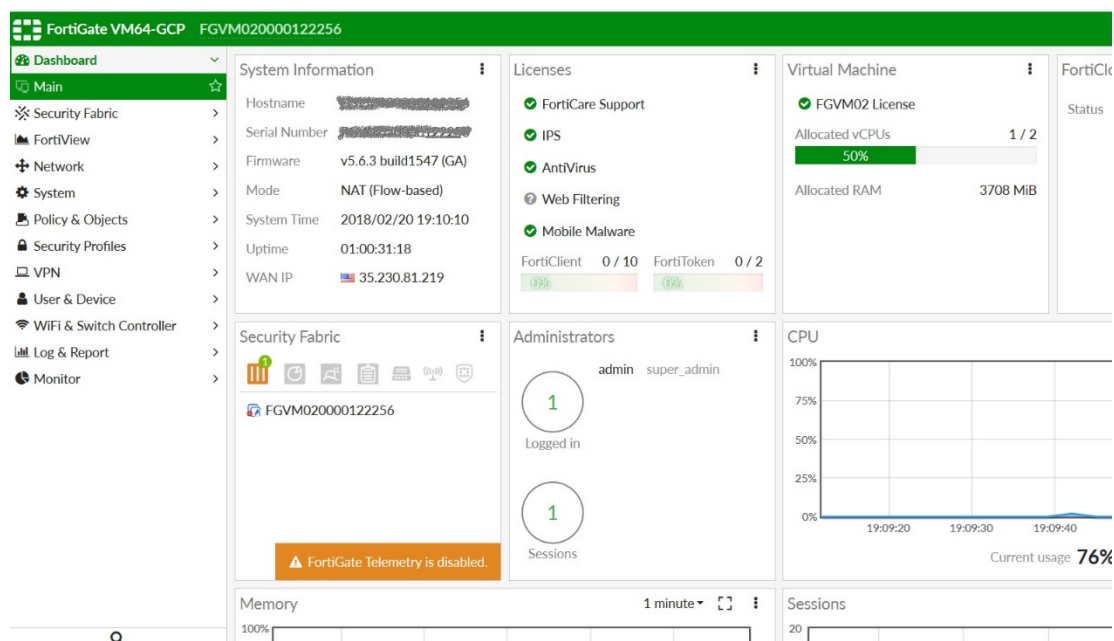
License uploaded is invalid for this configuration of the FortiGate-VM. Please upload a new license or reconfigure the FortiGate-VM.

Upload License File

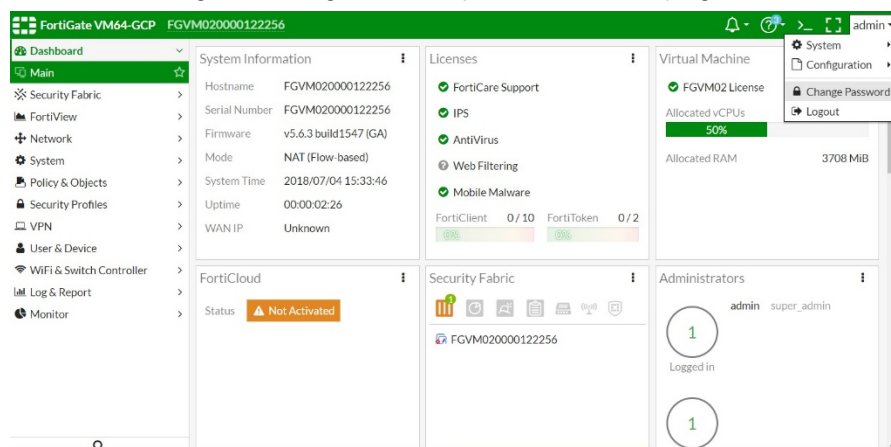
Select file Upload

OK Cancel

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.

The screenshot shows the Google Cloud Platform console for the 'Dev Project 001'. The 'VPC network details' page for the 'default' VPC is displayed. The 'Firewall rules' tab is selected, and the 'Add firewall rule' button is highlighted with a red box. Below the button, a table lists existing firewall rules. The 'default-allow-https' rule is highlighted with a red box.

Name	Type	Targets	Filters	Protocols / ports	Action	Priority
allow-internal	Ingress	App Engine	IP ranges: 10.0.0.0/24	tcp:80, 443	Allow	1000
allow-icmp	Ingress	all VMs	IP ranges: 0.0.0.0/0	icmp	Allow	1000
dchao-eco-test-tcp-2032	Ingress	dchao-eco-test-tcp-2032	IP ranges: 0.0.0.0/0	tcp:2032	Allow	1000
dchao-eco-test-tcp-22	Ingress	dchao-eco-test-tcp-22	IP ranges: 0.0.0.0/0	tcp:22	Allow	1000
dchao-eco-test-tcp-2000	Ingress	dchao-eco-test-tcp-2000	IP ranges: 0.0.0.0/0	tcp:2000	Allow	1000
dchao-eco-test-tcp-443	Ingress	dchao-eco-test-tcp-443	IP ranges: 0.0.0.0/0	tcp:443	Allow	1000
dchao-eco-test-tcp-514	Ingress	dchao-eco-test-tcp-514	IP ranges: 0.0.0.0/0	tcp:514	Allow	1000
dchao-eco-test-tcp-80	Ingress	dchao-eco-test-tcp-80	IP ranges: 0.0.0.0/0	tcp:80	Allow	1000
dchao-eco-test-tcp-8080	Ingress	dchao-eco-test-tcp-8080	IP ranges: 0.0.0.0/0	tcp:8080	Allow	1000
default-allow-ssh	Ingress	all VMs	IP ranges: 0.0.0.0/0	tcp:22	Allow	1000
default-allow-https	Ingress	https-server	IP ranges: 0.0.0.0/0	tcp:443	Allow	1000
google-cloud-internal	Ingress	all VMs	IP ranges: 0.0.0.0/0	tcp:80, 443	Allow	1000

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

Google Cloud Platform Dev Project 001

Create a firewall rule

Firewall rules control incoming or outgoing traffic to an instance. By default, incoming traffic from outside your network is blocked. [Learn more](#)

Name

Description (Optional)

Network

Priority Priority can be 0 - 65535 [Check priority of other firewall rules](#)

Direction of traffic ☒ Ingress ☐ Egress

Action on match ☒ Allow ☐ Deny

Targets

Source filter

Source IP ranges

Second source filter

Protocols and ports ☒ Allow all ☒ Specified protocols and ports

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*.

FortiGate VM64-GCP FGVM020000122256

Dashboard Security Fabric FortiView **Network** Interfaces DNS SD-WAN SD-WAN Status Check SD-WAN Rules

FortiGate VM64-GCP

+ Create New Edit Delete

Status	Name	Members	IP/Netmask	Type	Access
Physical (2)					
	port1		10.138.0.8 255.255.255.255	Physical Interface	PING HTTPS SSH HTTP FMG-Access
	port2		0.0.0.0 0.0.0.0	Physical Interface	

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

The screenshot displays the FortiGate VM64-GCP web interface. The top header bar is green and contains the text 'FortiGate VM64-GCP FGVM020000122256' along with a bell icon, a question mark icon, a back arrow, a forward arrow, and a user profile icon labeled 'admin'. On the left side, there is a navigation menu with the following items: Dashboard, Security Fabric, FortiView, Network (highlighted in green), Interfaces (highlighted in green), DNS, SD-WAN, SD-WAN Status Check, SD-WAN Rules, Static Routes, Policy Routes, RIP, OSPF, BGP, Multicast, System, and Policy & Objects. The main content area is titled 'Edit Interface' and shows the configuration for 'port2 (42:01:0A:03:00:02)'. The configuration includes: Interface Name: port2 (42:01:0A:03:00:02), Alias: Privfacing 4 GCP, Link Status: Up (with a green up arrow icon), Type: Physical Interface, Role: LAN (with a dropdown arrow), Addressing mode: Manual (selected), DHCP, One-Arm Sniffer, and Dedicated to FortiSwitch, IP/Network Mask: 10.3.0.2/255.255.0.0. Under the 'Administrative Access' section, there are checkboxes for IPv4: HTTPS (checked), SSH (checked), HTTP (checked), SNMP (unchecked), PING (checked), FTM (unchecked), FMG-Access (unchecked), CAPWAP (unchecked), RADIUS Accounting (unchecked), and FortiTelemetry (unchecked). At the bottom of the configuration area, there is a 'DHCP Server' toggle switch which is currently turned off. At the very bottom of the interface, there are two buttons: 'OK' (green) and 'Cancel' (white).

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.

Google Cloud Platform Dev

Compute Engine

Create a disk

Name ?
jkatocloudinit1

Description (Optional)

Type ?
SSD persistent disk

☐ Replicate this disk within region ?

Region ? **Zone** ?
us-west1 (Oregon) us-west1-a

Labels ? (Optional)
 + Add label

Source type ?
Blank disk | Image | Snapshot

Size (GB) ?
30

Estimated performance ?

Operation type	Read	Write
Sustained random IOPS limit	900.00	900.00
Sustained throughput limit (MB/s)	14.40	14.40

Encryption
Data is encrypted automatically. Select an encryption key management solution.

- ☒ **Google-managed key**
No configuration required
- ☐ **Customer-managed key**
Manage via Google Cloud Key Management Service
- ☐ **Customer-supplied key**
Manage outside of Google Cloud

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 24](#).
 - 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 `jkatoft603cloudinit`:

```
$sudo gcloud compute instances create jkatoft603cloudinit --network-interface network=jkato001,subnet=publicfacing1 --network-interface network=jkato002,subnet=privfacing4 --project "project name" --image jkato-ft-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
```

```
ubuntu@ip-172-31-38-147:~/BUILD-GCP/Fgt/cloud-init$ sudo gcloud compute instances create jkatoft603cloudinit --network-interface network=jkato001,subnet=publicfacing1 --network-interface network=jkato002,subnet=privfacing4,no-address --project dev --image jkato-ft-603-10162018-001 --can-ip-forward --machine-type n1-highcpu-2 --zone us-west1-a --disk=name=jkatocloudinit1,device-name=jkatodevicecloudinit01,mode=rw,boot=no
Created [https://www.googleapis.com/compute/v1/projects/dev/zones/us-west1-a/instances/jkatoft603cloudinit].
NAME                                ZONE          MACHINE_TYPE  PREEMPTIBLE  INTERNAL_IP  EXTERNAL_IP  STATUS
jkatoft603cloudinit                us-west1-a    n1-highcpu-2               10.0.0.2,10.3.0.3  35.247.121.45  RUNNING
```

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

The screenshot shows the Google Cloud Platform console. On the left is a navigation menu with options like Compute Engine, VM instances, Instance groups, Instance templates, Sole tenant nodes, Disks, Snapshots, Images, TPUs, Committed use discounts, Metadata, Health checks, Zones, Network endpoint groups, Operations, Quotas, and Marketplace. The main area displays the 'VM instance details' for 'jkatoft603cloudinit'. It includes tabs for 'Details' and 'Monitoring'. Under 'Details', there are sections for 'Remote access' (SSH, Connect to serial console), 'Logs' (Stackdriver Logging, Serial port 1 (console)), 'Machine type' (n1-highcpu-2), 'CPU platform' (Intel Broadwell), 'Zone' (us-west1-a), 'Labels' (None), 'Creation time' (Dec 10, 2018, 7:41:34 PM), and 'Network interfaces'. A table lists the network interfaces:

Name	Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP	Network Tier	IP forwarding	Network details
nic0	jkato001	publicfacing1	10.0.0.2	—	35.247.121.45 (ephemeral)	Premium	On	View details
nic1	jkato002	privfacing4	10.3.0.3	—	None			View details

7. Connect to the FortiGate-VM instance. See [Connecting to the FortiGate-VM on page 31](#).

Bootstrapping FortiGate at initial bootup

This section explains how to add bootstrapping of FortiOS CLI commands and a BYOL license at the time of initial bootup as part of Google Cloud commands.

To bootstrap FortiGate at initial bootup:

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:

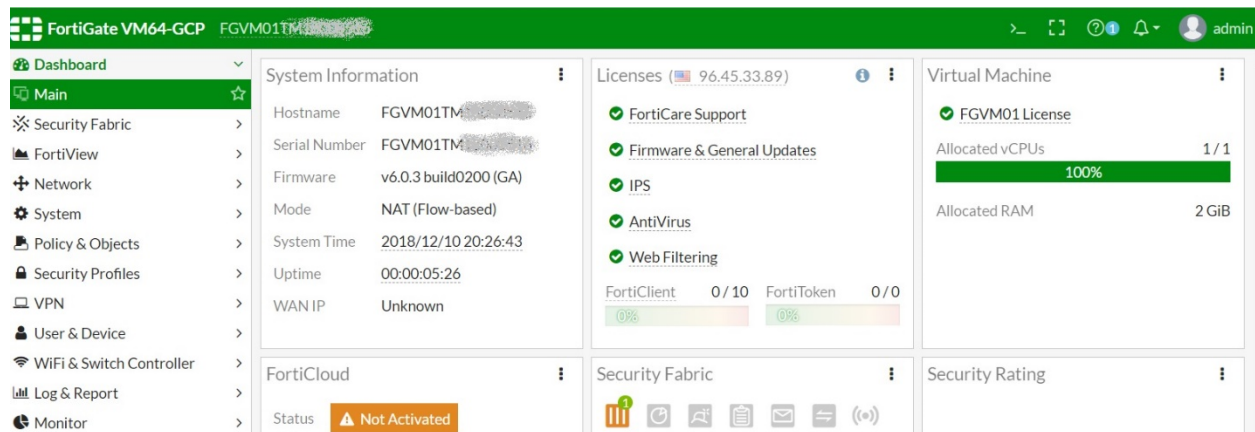
```
-----BEGIN FGT VM LICENSE-----
QAAABUiztrwjdUjEe/8C5dNvOm1w70ZMXPTG7vm2KKwYvL4++qL0gED6/q
SQSPkwpTF1XjAURGtGyX1VvaTpXGQAA1pwrFdJnS6TJ6dVT7KID8ncufaa3bCw
s8XpmLivzje4//+C9nqh4FN/KyDweIEPtMaNsoCm0B8rU8HQIDKX+rgeCs3QZ5
ELStRrX11/oQgTB/gorG67ZdybXvzPwVwJYDS5AsI+QK8BHJ+xGhLjhkzBZ4ezU
Hd01HCSm7MKEYV5KauU43sZ9XESTxqPEInah3yXgYTD24pnV683G4EHCkAdGyMTP
QqDqBMKcT5aei0ooGVAOX8D62C5Zjh+1+tkdpR5YHoVYZHU95hBCNjB8oJbMnk7
NogYuadQEH28MDtpvzXnb24mW1FDQMjTjySQCtwzJzmm8nvSBo7xNq/iNtS2QnFB
-----END FGT VM LICENSE-----
```

3. Upload the config.txt and license files onto the Linux machine where 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 40](#), 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".
```

```
ubuntu@ip-172-31-33-147:~/BUILD-GCP/FGT/cloud-init$ ls
config.txt license.txt
ubuntu@ip-172-31-33-147:~/BUILD-GCP/FGT/cloud-init$
ubuntu@ip-172-31-33-147:~/BUILD-GCP/FGT/cloud-init$
ubuntu@ip-172-31-33-147:~/BUILD-GCP/FGT/cloud-init$
ubuntu@ip-172-31-33-147:~/BUILD-GCP/FGT/cloud-init$ sudo gcloud compute instances create jkatofgt603cloudinit2 --network-in
terface network=jkato001,subnet=publicfacing1 --network-interface network=jkato002,subnet=privfacing4,no-address --project
dev --image jkato-fgt-603-10162018-001 --can-ip-forward --machine-type n1-highcpu-2 --zone us-west1-a
--disk=name=jkatocloudinit2,device-name=jkato-devicecloudinit02,mode=rw,boot=no --metadata-from-file "license=license.txt,us
er-data=config.txt"
Created [https://www.googleapis.com/compute/v1/projects/dev-1/zones/us-west1-a/instances/jkatofgt603cloudi
nit2].
NAME                                ZONE          MACHINE_TYPE  PREEMPTIBLE  INTERNAL_IP  EXTERNAL_IP  STATUS
jkatoft603cloudinit2               us-west1-a    n1-highcpu-2                10.0.0.3     10.3.0.5     35.233.160.96  RUNNING
```

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.

Deploying FortiGate-VM using Terraform

See the following:

- [Single FortiGate-VM deployment](#)
- [Active-passive HA cluster deployment](#)

High availability for FortiGate-VM on GCP

The following summarizes minimum sufficient roles for active-passive HA deployments:

- Compute Instance Admin (v1)
- Compute Network Admin

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 (A-P) HA 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.

When deploying a FortiGate-VM HA cluster, choose a VM type that supports four or more network interfaces for each FortiGate-VM instance, as GCP does not allow adding network interfaces after you deploy the VMs. You can attach multiple network interfaces only when creating the VM instance on GCP.

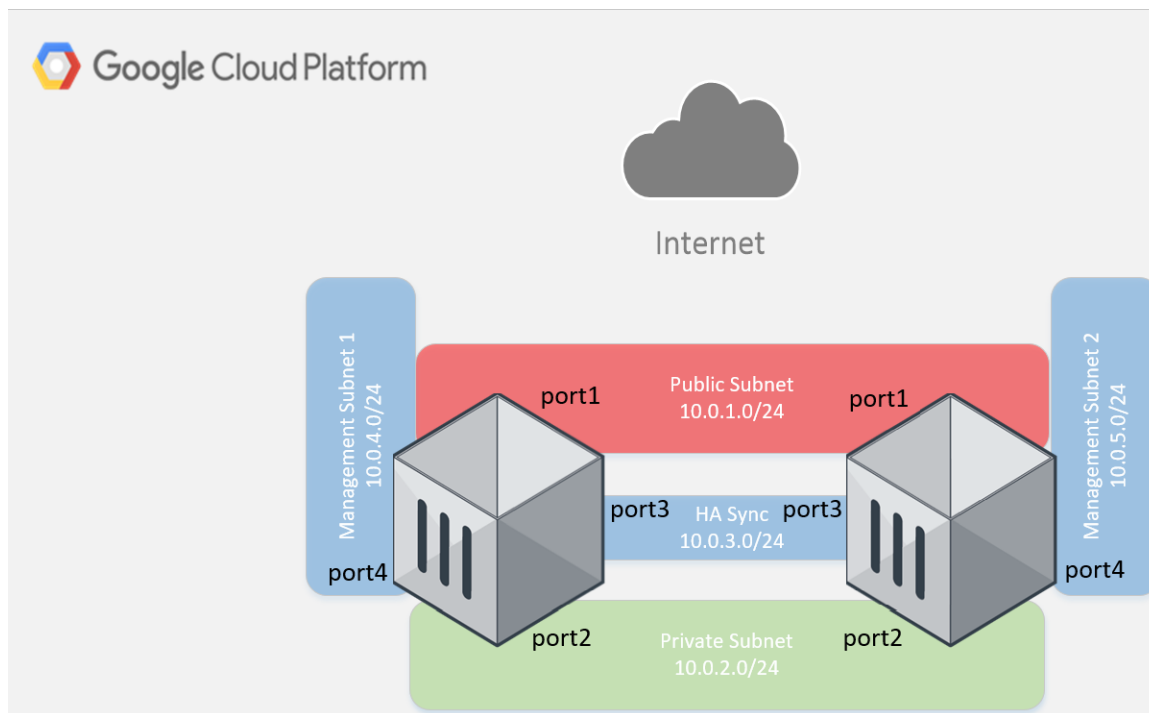
Two FortiGate-VM instances must be the same machine type.

The main benefits of this solution are:

- Fast and stateful failover of FortiOS without external automation/services
- Automatic 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 deploy FortiGate-VM instances on GCP using one of the following methods and configure A-P HA:

- Using the GCP GUI console. See [Deploying FortiGate HA using the GCP GUI on page 47](#).
- Using the Google Cloud command interface. See [Deploying FortiGate HA using the Google Cloud command interface on page 54](#).
- Using Marketplace deployments. See [Deploying FortiGate-VM on Google Cloud Marketplace on page 12](#).
- Using Terraform deployments. See [Deploying FortiGate-VM using Terraform on page 45](#).



Deploying FortiGate HA using the GCP GUI



When configuring the route's next hop policy, select *Specify an IP address* in the *Next hop* dropdown list. This is the only option that allows HA to function.

Obtaining the deployment image

This section describes manual image deployment. You can also use other deployment alternatives, as described in [Deploying FortiGate-VM HA on GCP in one zone on page 46](#).

To obtain 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 only applies for BYOL deployments. The PAYG deployment file is unavailable for download in the above site. For PAYG, configure HA after deploying two FortiGate-VM instances on the GCP marketplace.

Deciding and configuring required VPC and networks is highly encouraged before you launch FortiGate-VM instances that you plan to form an HA cluster with. For details about GCP networks, see [Creating VPC networks on page 48](#).

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:

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.
ha-sync-network	All HA functionality, such as session and configuration synchronization, communicates with this network.
mgmt-network	Out of band management network. For A-P HA to properly manage IP addresses and route tables, the HA cluster must have a public IP address assigned to the HA mgmt interface. Without this configuration, failover does not complete successfully and results in failure of the cluster.

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 from those that you configure on the FortiGates. Name the GCP route tables and firewall rules according to the associated network and functionality.

To create VPC networks:

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 48](#).
 - 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. For A-P HA to properly manage IP addresses and route tables, the HA cluster must have a public IP address assigned to the HA mgmt interface. Without this configuration, failover does not complete successfully and results in failure of the cluster:
 - 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 48](#).
 - 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.

To create a GCP route table:

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. Depending on how you provisioned the instance, you must use the instance ID or the `fortigate_user_password` (found in the GCP management console under *VM instance details*) as the password. The instance ID is represented as a number that can be found after locating the instance in the GCP Compute Engine console. Click the name of each instance and note the instance ID or the `fortigate_user_password`.
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 or `fortigate_user_password` 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

To set 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
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
```

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 51](#).
7. Go to *Compute Engine > VM Instances*.
8. Note the primary FortiGate's external IP address.

Deploying FortiGate HA using the Google Cloud command interface



When configuring the route's next hop policy, select *Specify an IP address* in the *Next hop* dropdown list. This is the only option that allows HA to function.

This deployment consists of the following steps:

1. [Checking the prerequisites on page 54](#)
2. [Deploying the FortiGate-VM on page 55](#)

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 40](#).
- 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 8](#).
- You must configure an SDN connector with GCP on the primary FortiGate:

```
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
```

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 40](#). Replace the disk names, zones, and sizes as required.

```

PS C:\Users\jkato> gcloud compute --project=dev-... 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-.../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-... 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-.../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 40](#).

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.

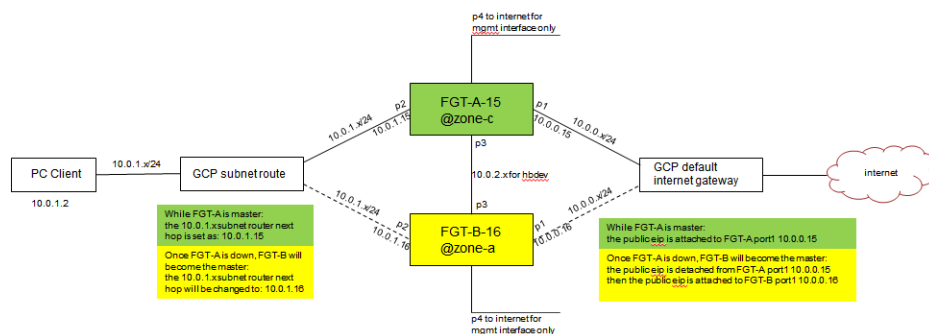
3. After deploying the two FortiGates, connect to each FortiGate management console. Do the following:
 - a. Configure the network interfaces, ports 2, 3, and 4 by entering IP addresses and subnets. By default, only port1 is configured. For port4, configure administrative access. You may want to allow HTTPS and SSH.
 - b. Shut down the FortiGate-VMs. Allow access to Google Cloud API. See [Configuring GCP SDN connector using metadata IAM on page 69](#).

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. Configure a VDOM exception.
7. 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:



IPsec VPN phase 1 configuration does not synchronize between primary and secondary FortiGates across zones. Phase 2 configuration does synchronize.

To check the prerequisites:

- Ensure that you have created four VPC networks.
- Ensure that you have created routes for each network.
- Create firewall rules for each network.
- Reserving three external IP addresses is suggested for convenience.

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

This example creates FortiGate A 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 userdata=/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:

This example creates FortiGate B in zone a.

1. Run the following commands in GCP:

```

gcloud beta compute --project=dev-project-001-166400 instances create fgt-b --zone=us-
centrall1-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-portlexternal,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-
centrall1-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
```

Synchronized	Priority	Hostname	Serial No.	Role	Uptime	Sessions	Throughput
✓	200	FGT-A	FGTGCPA2DHFS8822	Master	00:00:03:51	96	273.00 kbps
✓	20	FGT-B	FGTGCPVXW2MYFH07	Slave	00:03:05:39	40	21.00 kbps

2. Log in to 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.

Name	Destination IP ranges	Priority	Instance tags	Next hop	Network
default-route-2c43387458c8dc9	10.0.3.0/24	1000	None	VPC network	hapvc-port4mgmt
default-route-59758b2abb27445e	10.0.2.0/24	1000	None	VPC network	hapvc-port3heartbeat
default-route-75b513c299783dfe	10.0.0.0/24	1000	None	VPC network	hapvc-port1external
default-route-931e4061d6b9a018	0.0.0.0/0	1000	None	Default internet gateway	hapvc-port1external
default-route-bf9b974df5c90b9c	0.0.0.0/0	1000	None	Default internet gateway	hapvc-port3heartbeat
default-route-defea321e7579a45	0.0.0.0/0	1000	None	Default internet gateway	hapvc-port4mgmt
default-route-f3252a34f1dc6b1d	10.0.1.0/24	1000	None	VPC network	hapvc-port2internal
route-internal	0.0.0.0/0	1000	None	IP : 10.0.1.16	hapvc-port2internal

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 configure a VDOM exception:

You must configure a VDOM exception to prevent interface synchronization between the two FortiGates. FortiOS 6.4.1 and later versions support the following commands. FortiOS 6.4.0 does not support these commands.

```
config system vdom-exception
edit 1
set object system.interface
next
edit 2
set object router.static
next
edit 3
set object firewall.vip
next
end
```

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 # diagnose debug application 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-centrall-c/fgt-a,
    should be moved to local
get instance nic: nic0, 10.0.0.15, hapvc-portlexternal, 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.
```

SDN connector integration with GCP

This guide describes configuring GCP SDN connector on FortiGate-VM for GCP.

The following summarizes minimum sufficient roles for this deployment:

- Compute Viewer
- Kubernetes Engine Viewer

You can also configure pipelined automation. See [Pipelined automation using Google Cloud function on page 79](#).

Configuring GCP SDN Connector using service account

See the *FortiOS Administration Guide*.

Custom role permission guideline

The following provides the least privileged guideline for a custom role when using a GCP SDN connector with a service account for high availability (HA):

- compute.addresses.get
- compute.addresses.use
- compute.instances.addAccessConfig
- compute.instances.deleteAccessConfig
- compute.instances.get
- compute.instances.list
- compute.instances.updateNetworkInterface
- compute.networks.updatePolicy
- compute.networks.useExternalIp
- compute.subnetworks.use
- compute.subnetworks.useExternalIp
- compute.routes.create
- compute.routes.delete
- compute.routes.get
- compute.routes.list



This list is a guideline and focuses on the operation of HA between two FortiGate-VMs in a single zone and multizone deployment only. It allows for moving a single public IP address from the primary FortiGate to the secondary and updating the referenced GCP routing table in the FortiOS SDN connector configuration. Your custom role Identity and Access Management (IAM) permissions vary depending on your environment.



The predefined compute admin role includes the aforementioned IAM permissions. See [IAM permissions reference](#).

API calls

The SDN connector uses API calls to GCP API endpoints respective to its function. You can review the methods, calls, and error codes by using the following diagnostics commands:

Command	Description
<code>diagnose debug reset</code>	Clears filters or previous diagnostic configuration in the console or SSH session.
<code>diagnose debug console timestamp enable</code>	Enables timestamp of console output messages.
<code>diagnose debug enable</code>	Enables diagnostic output to the console.
<code>diagnose debug application gcpd -1</code>	Selects the GCP daemon or SDN connector.



For information about creating a GCP SDN connector, see [GCP SDN connector using service account](#).

The following are references for running a VM with a service account:

- [Creating and enabling service accounts for instances](#)
- [Permissions required for this task](#)

Multiple GCP projects in a single SDN connector

An option is added to specify multiple projects under a single GCP SDN connector. Previously, only one project was allowed per SDN connector, which limits the total projects to the number of SDN connectors (256). This enhancement also allows dynamic firewall address filters to filter on a project. FortiOS 6.4.7 and later versions support this feature.

In this example, a GCP SDN connector (gcp_conn) is configured with two projects. The first project, dev-project-001-166400, is configured using the simple format. The second project, dev-project-002, is configured using the advanced format.

To configure a GCP connector with multiple projects in the GUI:

1. Go to *Security Fabric > External Connectors* and click *Create New*.
2. Select *Google Cloud Platform (GCP)* and enter a name for the connector.

3. Configure the first project:
 - a. For *Projects*, select *Simple*.
 - b. Enter the project name, service account email, and private key.

New External Connector

Public SDN

Google Cloud Platform (GCP)

Connector Settings

Name:

Status: ☒ Enabled ☐ Disabled

Update interval: ☒ Use Default ☐ Specify

GCP Connector

Projects: **Simple** Advanced

Name:

Service account email: 50/127

Private key:

-----BEGIN PRIVATE KEY-----
[Blurred Private Key Content]
-----END PRIVATE KEY-----

OK Cancel

Public SDN Connector Setup Guides

- [Amazon Web Services](#)
- [Google Cloud Platform](#)
- [Microsoft Azure](#)
- [Oracle Cloud Infrastructure](#)

Private SDN Connector Setup Guides

- [Cisco Application Centric Infrastructure](#)
- [Nuage Virtualized Services Platform](#)
- [OpenStack Connector](#)
- [VMware NSX](#)

Documentation

- [Online Help](#)
- [Video Tutorials](#)

4. Configure the second project:

- a. For *Projects*, select *Advanced* (the projects are now displayed in a table) and click *Create New*.

The *Add GCP Project* pane opens.

- b. Enter a name.
- c. Optionally, click the + to enter zones. If no zones are selected, the SDN connector will include all zones. The *us-central1-a* zone is used in this example.

- d. Click *OK*.
5. Click *OK* to save the SDN connector.
6. Create a dynamic firewall address for the first project:
 - a. Go to *Policy & Objects > Addresses* and click *Create New > Address*.
 - b. Enter the following:

Name	project1_addresses
Type	Dynamic

Sub Type	Fabric Connector Address
SDN Connector	gcp_conn
Filter	<p>Add a filter for the project, <i>Project=dev-project-001-166400</i>.</p> <p>In this example, there are several instances for the first project, so add a filter for the ID, <i>Id=6266132824476267466</i>.</p> <p>Change the logic operator to <i>and</i>.</p>

The screenshot shows the 'New Address' configuration window. The 'Category' is set to 'Address'. The 'Name' is 'project1_addresses'. The 'Type' is 'Dynamic'. The 'Sub Type' is 'Fabric Connector Address'. The 'SDN Connector' is 'gcp_conn'. The 'SDN address type' is 'Private'. The 'Filter' is configured with two conditions: 'Project=dev-project-001-166400' and 'Id=6266132824476267466', connected by an 'and' operator. The 'Interface' is set to 'any'. The 'Comments' field is empty. The right sidebar shows the 'FortiGate' configuration tree with 'Dynamic Address' selected.

c. Click **OK**.

7. Create a dynamic firewall address for the second project:

a. Click **Create New > Address**.

b. Enter the following:

Name	project2_addresses
Type	Dynamic
Sub Type	Fabric Connector Address
SDN Connector	gcp_conn
Filter	Add a filter for the project, <i>Project=dev-project-002</i> .

c. Click **OK**.

The addresses have been created. Wait for a few minutes before the settings take effect.

8. Verify that the address resolve to the correct addresses. Hover over the address in the table to view the list of populated IP addresses.

To configure a GCP connector with multiple projects in the CLI:

1. Configure the SDN connector:

```
config system sdn-connector
  edit "gcp_conn"
    set status enable
    set type gcp
    config gcp-project-list
```

```

        edit "dev-project-001-166400"
        next
        edit "dev-project-002"
        set gcp-zone-list "us-central1-a"
        next
    end
    set service-account "xxxxxxxxxxxx-compute@developer.gserviceaccount.com"
    set private-key *****
    set update-interval 30
next
end

```

2. Create a dynamic firewall address for project one:

```

config firewall address
    edit "project1_addresses"
        set type dynamic
        set sdn "gcp_conn"
        set filter "Project=dev-project-001-166400 & Id=6266132824476267466"
    next
end

```

The dynamic firewall address IP is resolved by the SDN connector:

```

config firewall address
    edit "project1_addresses"
        show
        config firewall address
            edit "project1_addresses"
                set uuid 38efbd88-fb08-51eb-8e6d-9b78a2a9bf49
                set type dynamic
                set sdn "gcp_conn"
                set filter "Project=dev-project-001-166400 &
Id=6266132824476267466"
            config list
                edit "172.16.16.3"
                next
                edit "172.16.24.3"
                next
                edit "172.16.8.4"
                next
            end
        next
    end
next
end

```

3. Create a dynamic firewall address for project two:

```

config firewall address
    edit "project2_addresses"
        set type dynamic
        set sdn "gcp_conn"
        set filter "Project=dev-project-002"
        set sdn-addr-type all
    end
end

```



```

    next
end

```

The dynamic firewall address IP is resolved by the SDN connector:

```

config firewall address
    edit "project2_addresses"
        show
        config firewall address
            edit "project2_addresses"
                set uuid 5ca9b2ba-fb08-51eb-57c0-12701b3d33c1
                set type dynamic
                set sdn "gcp_conn"
                set filter "Project=dev-project-002"
                set sdn-addr-type all
            config list
                edit "10.128.0.2"
                next
                edit "34.66.35.241"
                next
            end
        next
    end
end
next
end

```

GCP Kubernetes (GKE) SDN connector

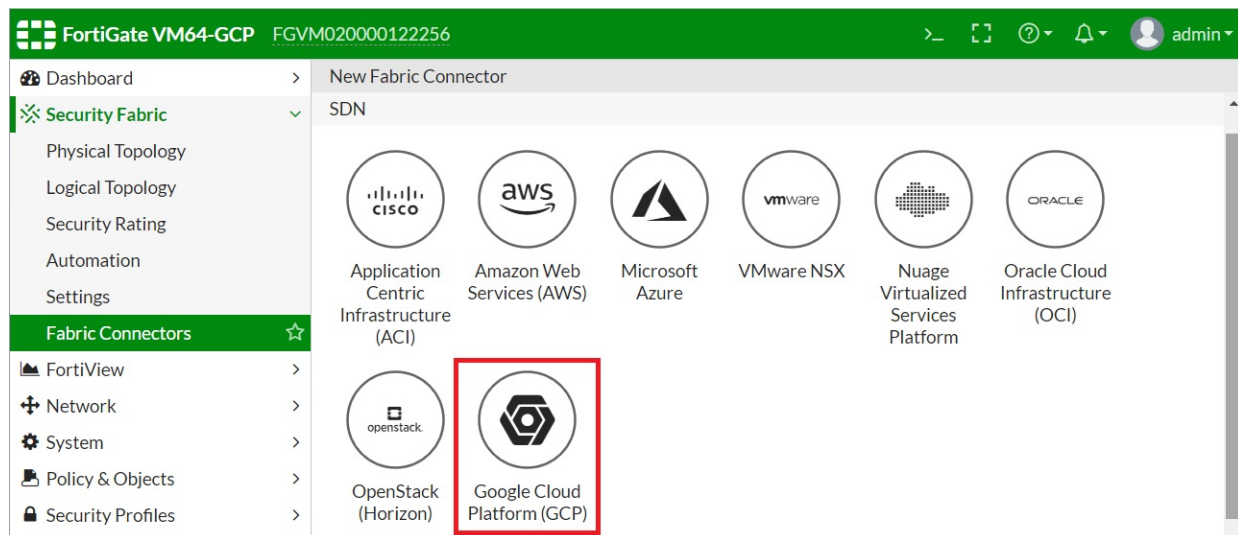
GCP SDN connectors support dynamic address groups based on GCP Kubernetes Engine (GKE) filters. See the [FortiOS Administration Guide](#).

Configuring GCP SDN connector using metadata IAM

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

To configure GCP SDN connector using metadata IAM:


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.

New Fabric Connector

SDN

 Google Cloud Platform (GCP)

Connector Settings

Name

Use metadata IAM ☒

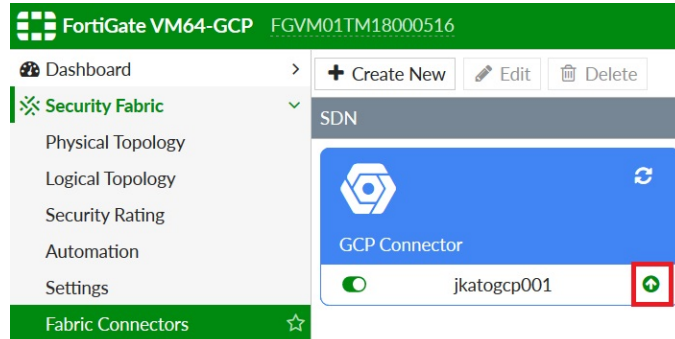
Update Interval ⓘ Use Default Specify

Status ☒

OK Cancel

3. Configure the connector as follows:
 - a. **Name:** Enter the desired connector name.
 - b. Enable *Use metadata IAM*. The Google platform requires a certain authentication level to call APIs from the FortiGate. See [To check metadata API access: on page 73](#). 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. **Update interval:** the default value is 60 seconds. You can enter a value between 1 and 3600 seconds.
 - d. **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 78](#).



4. Create a dynamic firewall address for the configured GCP SDN connector:
 - a. Go to *Policy & Objects > Addresses*. Click *Create New*, then select *Address*.
 - a. Configure the Address:
 - i. *Name*: Enter the desired name.
 - ii. *Type*: Select *Fabric Connector Address*.
 - iii. *Fabric Connector Type*: Select *Google Cloud Platform (GCP)*.
 - iv. *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.

New Address

Name

jkatogcp001

Color

Change

Type

Fabric Connector Address

Fabric Connector Type

Google Cloud Platform (GCP)

Filter

network=default & zone=us-central1-f

Interface

☐ any

Show in Address List

☒

Comments

Tags

Add Tag Category

OK

Cancel

v. 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.

FortiGate VM64-GCP FGVM01TM18000516

Dashboard

Security Fabric

FortiView

Network

System

Policy & Objects

IPv4 Policy

IPv4 DoS Policy

Addresses

Wildcard FQDN

Create

Address

FIREWALL

SSLVPN

all

autoupdate

google-p

jkatogcp001

jkatogcp001 resolves to:

- 10.128.0.12
- 10.128.0.15
- 10.128.0.27
- 10.128.0.4
- 10.128.0.8
- 10.128.0.9
- 104.197.121.152
- 104.197.135.149
- 104.197.87.56
- 35.188.64.215
- 35.194.4.150
- 35.224.83.138

Delete

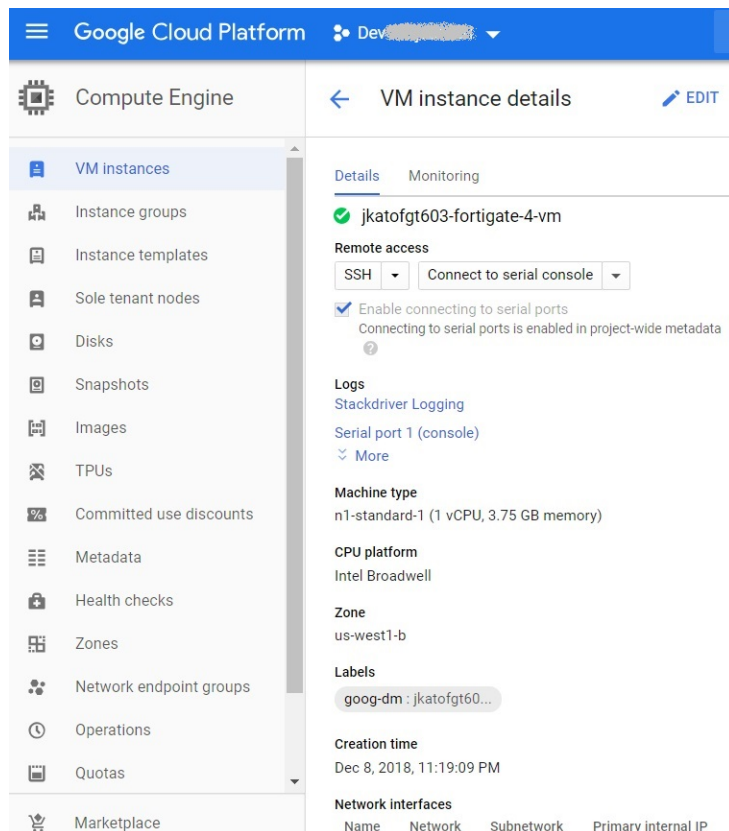
Search

Type	Details
Subnet	0.0.0.0/0
IP Range	10.212.134.200 - 10.212
Subnet	0.0.0.0/0
FQDN	autoupdate.opera.com
FQDN	play.google.com
Fabric Connector Address (GCP)	

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

To check metadata API access:

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 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/Write access*.
 - d. Save the change, then restart the VM.

Creating a GCP service account

This topic describes how to create a GCP service account and an API key pair, and provides guidelines on how to edit the private key for use in FortiOS. If you enabled metadata Identity and Access Management (IAM) in [Configuring GCP SDN Connector using service account on page 63](#), you do not need to create a service account.

To create a GCP service account:

1. Log into the GCP Compute Portal.
2. Go to *IAM & admin > Service accounts*.

3. Create a service account:
 - a. Select *Create a service account*.
 - b. Name the account.
 - c. Click *CREATE* and *CONTINUE*.

Create service account

1

Service account details

Service account name

example-service-account

Display name for this service account

Service account ID *

example-service-account

X ↺

Email address: example-service-account@dev-project-001-166400.iam.gserviceaccount.com

Service account description

example-service-account

Describe what this service account will do

CREATE AND CONTINUE

2

Grant this service account access to project (optional)

3

Grant users access to this service account (optional)

DONE

CANCEL

- d. From the *Role* dropdown list, select the desired role, then click *CONTINUE* or *DONE*.

Create service account

✓ Service account details

2 Grant this service account access to project (optional)

Grant this service account access to Dev Project 001 so that it has permission to complete specific actions on the resources in your project. [Learn more](#)

Role

fgt-ha-role

fgt-ha-role

Condition

[Add condition](#)

+ ADD ANOTHER ROLE

CONTINUE

3 Grant users access to this service account (optional)

DONE

CANCEL



This example selects a custom role for high availability (HA). You can select the viewer role or another role if the FortiGate is on-premise or you do not need to configure HA.

- e. If you are configuring the service account for use in an SDN connector for HA or for running the VM, select the correct IAM role with the needed permissions.



For guidelines on the IAM role permissions for HA, see [Configuring GCP SDN Connector using service account on page 63](#).

For information about configuring a GCP IAM service account, see [Creating and managing service accounts](#).

- f. (Optional) Configure user access.

To create the service account key:

1. Edit the service account by selecting its email address.
2. On the **Keys** tab, click **ADD KEY**.

The screenshot shows the Google Cloud IAM & Admin console. On the left, the 'Service Accounts' menu item is selected. The main panel displays the 'Keys' tab for the 'example-service-account'. A warning message states: 'Service account keys could pose a security risk if compromised. We recommend...' followed by instructions to add a new key pair or upload a public key certificate. Below this, there are links to 'organization policies' and 'Learn more about setting organization policies for service accounts'. An 'ADD KEY' button is visible, with a dropdown menu showing 'Create new key' and 'Upload existing key'. A table header for 'Key creation date' and 'Key expiration date' is also shown.

3. Select to import your existing key or generate another. If you create a new key, you can select a JSON formatted key or a P12, which includes the private and public keys. Once created, the key automatically downloads to your PC.

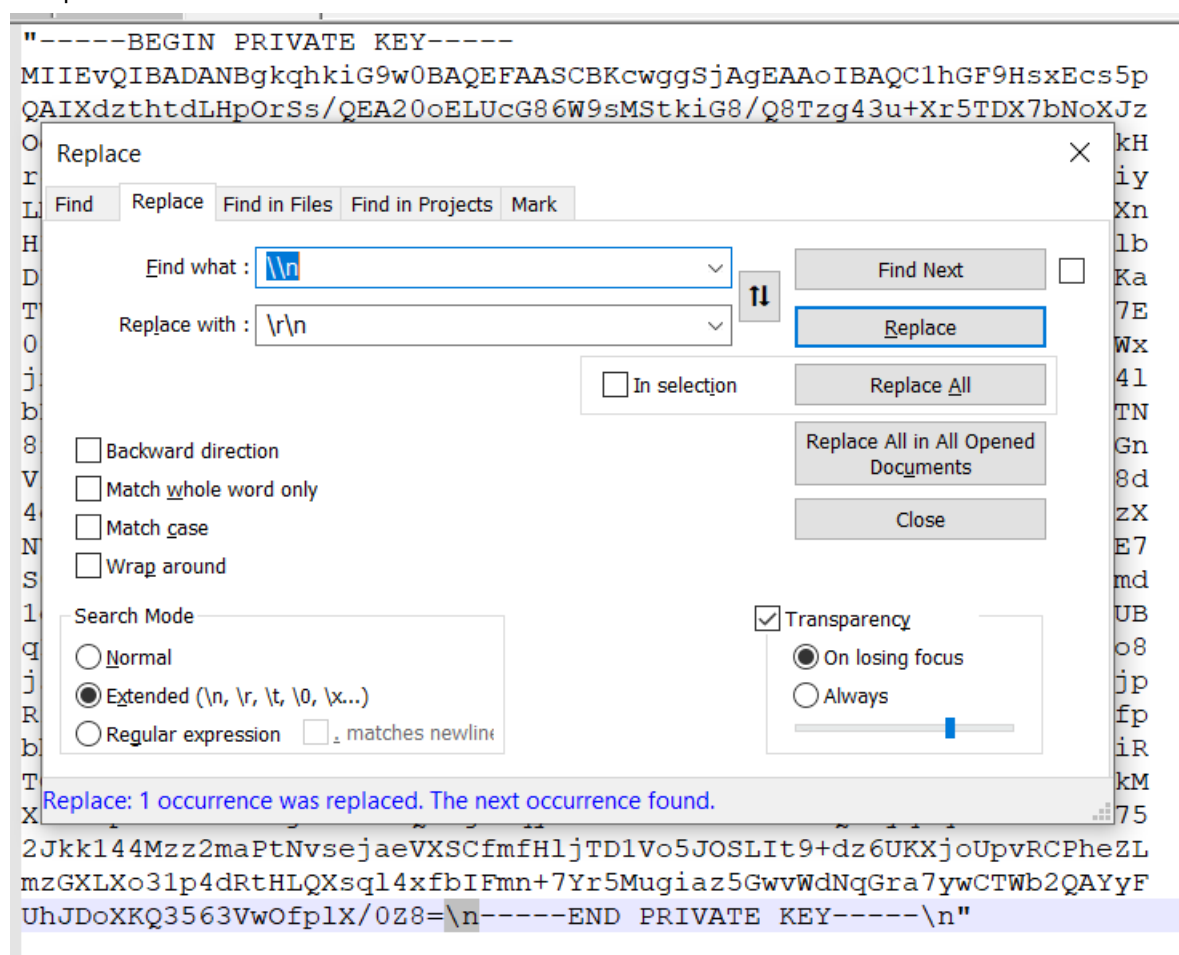


For information about creating service account keys, see [Create and manage service account keys](#).

To edit the private key:

1. Use a text editor to open the downloaded key.
2. Find the line `"private_key": "-----BEGIN PRIVATE KEY-----\n....."`
3. Edit the key between `"-----BEGIN PRIVATE KEY-----"` and `"-----END PRIVATE KEY-----"`.
4. Remove `"\n"` using a tool or command of your choice, for example by using the Find and Replace function in

Notepad++.



This replaces "\n" with the actual return line, rendering a correctly formatted private key.

5. Copy and paste the key content into the FortiOS GUI or CLI.

```
FortiWiFi-60E (gcp-connector-test) # set private-key "-----BEGIN PRIVATE KEY-----
> MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBAcwggSjAgEAAoIBAQC1hGF9HsxEcs5p
> QATYd+th+dlU=O=Ca (GF400+FLU+006WQ+M0+L+00 (00T==40+LY=FTDY75N+Y Jz
> Oe .:H
> rE .y
> LM (n
> HF .b
> DF (a
> TV 'E
> 0E lx
> j> lI
> bF 'N
> 8r in
> V/ }d
> 4e :X
> NV :7
> S0 id
> 1e JB
> qF }8
> jE |p
> Rf i'p
> bt .R
> TC :M
> Xz '5
> 2L :L
> mZ0ALX0S |p40K0H0QASq14X101F0007 / 11 0mug1aZ00WV0m0q01 a/ yw01m0ZQA1 yF
> UhJDoXKQ3563VwOfp1X/0Z8=
> -----END PRIVATE KEY-----
> "
```

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. 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/v1/
host:www.googleapis.com:443:172.217.8.170
gcpd api result:200
nost:www.googleapis.com:443:172.217.8.170
gcpd get instance list successfully
gcpd checking firewall address object jkatogcp001, vd 0
```

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

FGVM01TM18000516 # gcpd exit
Unknown action 0

FGVM01TM18000516 #
FGVM01TM18000516 #
FGVM01TM18000516 # safeguard_fn()-1701
sync account, url: http://169.254.169.254/computeMetadata/v1/?alt=json&
gcpd api url: https://www.googleapis.com/compute/v1/projects/dev-project
host:www.googleapis.com:443:74.125.20.95
curl socket:11 vfid:0
https
{
  "error": {
    "errors": [
      {
        "domain": "global",
        "reason": "insufficientPermissions",
        "message": "Insufficient Permission"
      }
    ],
    "code": 403,
    "message": "Insufficient Permission"
  }
}

gcpd api result:403
gcpd get zones list failed
sync account, url: http://169.254.169.254/computeMetadata/v1/?alt=json&
```

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?

Pipelined automation using Google Cloud function

See [GitHub](#).

Deploying auto scaling on GCP

You can deploy FortiGate virtual machines (VMs) to support Auto Scaling on Google Cloud Platform (GCP).

Multiple FortiGate-VM instances can form an Auto Scaling group (ASG) to provide highly efficient clustering at times of high workloads. FortiGate-VM instances will be scaled out automatically according to predefined workload levels. Auto Scaling is achieved by using FortiGate-native high availability (HA) features such as `config-sync`, which synchronizes operating system (OS) configurations across multiple FortiGate-VM instances at the time of scale-out events.

FortiGate Autoscale for GCP is available with FortiOS 6.2.3 for On-Demand (PAYG) instances.

The standard deployment contains the following:

- A highly available architecture that spans two Availability Zones (AZs).
- A virtual private cloud (VPC) configured with public and private subnets.
- Cloud NAT.
- An external facing network load balancer.
- An internal facing network load balancer.
- Cloud Functions, which runs Fortinet-provided scripts for running Auto Scaling. Functions are used to handle cluster creation and failover management
- A Firestore database which stores Autoscaling configuration such as primary and secondary IP addresses. Firestore is a nosql database hosted on Google Cloud Platform.
- A managed instance group and an instance template.

Requirements

Installing and configuring FortiGate Autoscale for GCP requires knowledge of the following:

- Configuring a FortiGate using the Command Line Interface (CLI)
- Google Cloud Platform (GCP)
- Terraform 0.12

It is expected that FortiGate Autoscale for GCP will be deployed by DevOps engineers or advanced system administrators who are familiar with the above.

Account permissions

The default Compute service account should have sufficient Identity and Access Management (IAM) permissions to deploy the cluster using Terraform. For details, refer to the Google Cloud article [Access Control for Organizations using IAM](#).

Region requirements

To deploy FortiGate Autoscale for GCP, the region must support the following:

- Firestore
- Google Bucket Storage
- Cloud Functions
- Managed Instance Groups
- Cloud NAT

Deployment

The easiest way to deploy FortiGate Autoscale for GCP is with Terraform.

This deployment was tested with:

- Terraform 0.12
- Terraform Google Provider 2.20.1
- Terraform Google Provider Beta 2.20.1

To deploy FortiGate Autoscale for GCP:

1. Log into your GCP account.
2. If you haven't already done so, create an authentication token. The default Compute service account should have sufficient permissions. For details refer to the Google Cloud article [Getting Started](#).
3. Install Terraform. For installation details, refer to the HashiCorp article [Install Terraform](#).
4. Clone the repository.
5. Change into the new directory and do one of the following:
 - Run the following commands:

```
npm install
npm run setup
```

- Visit the FortiGate Autoscale for GCP [GitHub project release page](#) and download the latest `gcp.zip` from the releases tab; create a folder named `dist` and place the `gcp.zip` file in that directory.
6. The following files and folders should be present:

```
.
├── assets
│   └── configset
│       ├── baseconfig
│       ├── httproutingpolicy
│       ├── httpsroutingpolicy
│       ├── internalelbweb
│       ├── port2config
│       ├── setuptgwvpn
│       └── storelogtofaz
├── cloud-function-package.json
├── dist
│   └── gcp.zip
├── index.ts
├── main.tf
├── package.json
└── package-lock.json
```

```
└─ README.md
└─ tsconfig.json
└─ tslint.json
└─ vars.tf
```

7. Open the `vars.tf` file and add values to the following variables:

- `project`: your Google Project ID
- `service_account`: the service account that will be used to call Cloud Function
- `auth_key`: the name (and path) of your GCP authentication key. The default is `account.json`. Specify the path if the key is not in the current directory.

The above can also be done from the command line using the syntax:

```
terraform plan -var "<var_name>=<value>"
```

8. Customize other variables such as `cpu_utilization`, `cool_down_period`, etc. as needed. For variable descriptions, refer to the section "Terraform variables" on the next page.

9. Initialize the providers and modules:

```
terraform init
```

10. Verify the plan:

```
terraform plan
```

11. Confirm and apply the plan:

```
terraform apply
```

Output will be similar to the following. A randomly generated five (5) letter suffix is added to all resources and can be used to help identify your cluster resources.

```
InstanceTemplate = fortigateautoscale-instance-template-cehpm
LoadBalance_instances = []
LoadBalancer_Ip_Address = xxx.xxx.xxx.xxx
Notes = The Firestore Database must be deleted separately
Trigger_URL = https://us-central1-
*****.cloudfunctions.net/fortigateautoscale-cehpm
google_compute_region_instance_group_manager = fortigateautoscale-fortigate-
autoscale-cehpm
```

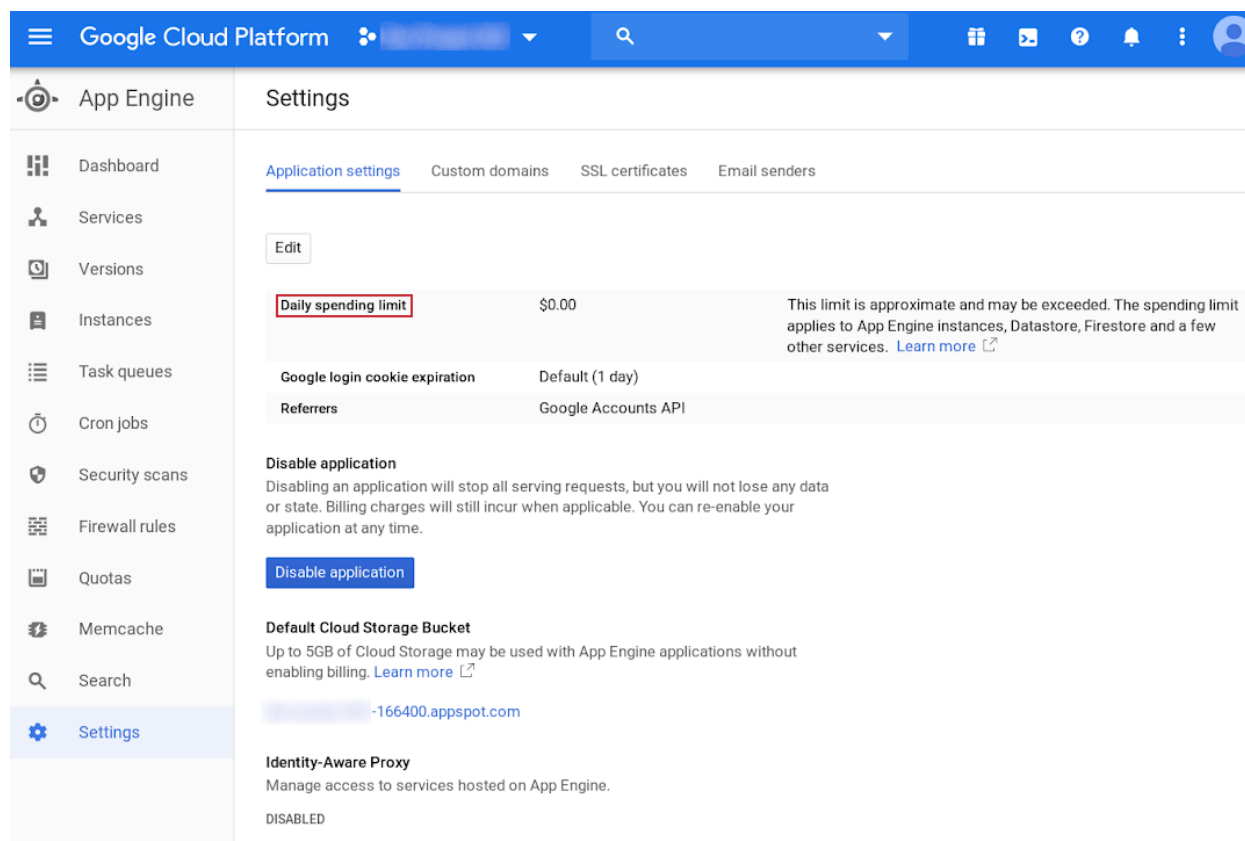


As part of the deployment, Terraform will adjust the value of `fgt_secondary_ip` within the `baseconfig` file located in `assets/configset/`. The value should be the IP address of the external load balancer. For details on Load Balancing in GCP, refer to the Google Cloud article [Network Load Balancing Concepts](#).

Quotas

FortiGate Autoscale for GCP makes heavy use of Firestore to store cluster information. Quota information for Firestore can be found under *App Engine > Quotas*. For details on Firestore quotas, refer to the Google Cloud article [Quotas and limits](#).

Daily spending limits can be adjusted under the *Settings* tab of *App Engine*:





Firestore pricing is at: <https://cloud.google.com/firestore/pricing>.

Terraform variables

Following are variables listed in the `vars.tf` file. They can be changed to suit the needs of your cluster.

Resource	Default	Description
project	Requires input	The project under which you will deploy the instance group. For details on managing projects, refer to the Google Cloud article Creating and Managing Projects .
auth_key	Requires input	The file name of the authentication key you are using to connect to GCP. For details on creating the key, refer to the Adding credentials section of the HashiCorp article "Getting Started with the Google Provider".
service_account	Requires input	The service account that will be used to call Cloud Functions. This allows Cloud Functions to be restricted to authorized calls.
region	us-central1	GCP region
zone	us-central1-c	GCP zone
nodejs_version	nodejs10	Version of Node.js to use in Cloud Functions.

Resource	Default	Description
max_replicas	3	Maximum number of FortiGate-VM instances in the instance group. For details on scaling configurations, refer to the Google Cloud article Instance groups .
min_replicas	2	Minimum number of FortiGate-VM instances in the instance group.
cpu_utilization	0.5	Target CPU usage for the cluster to achieve. Instances will scale out or scale in to meet this target.  Autoscaling is based on CPU utilization. Autoscaling using custom metrics is not supported.
cluster_name	FortigateAutoScale	Name of the cluster to be used across objects (buckets, VPC, etc.)
bucket_name	fortigateautoscale	Name of the Blob Storage bucket.
fortigate_image	projects/fortigcp-project-001/global/images/fortinet-fgtondemand-623-20191223-001-w-license	The source image for the Instance Group to use. The default image is FortiOS 6.2.3.
instance	n1-standard-1	The instance Family type to be used by the scaling configuration.
vpc_cidr	172.16.0.0/16	The Classless Inter-Domain Routing (CIDR) block for the FortiGate Autoscale VPC, divided into two /21 subnets.
public_subnet	172.16.0.0/21	Public subnet used by the FortiGate cluster.
protected_subnet	172.16.8.0/21	Private subnet for VMs behind the FortiGate cluster.
firewall_allowed_range	0.0.0.0/0	The GCP firewall range to allow.  <ul style="list-style-type: none"> The default is to allow all. If you use the GCP firewall policy to block incoming traffic, you will need to allow the load balancer to perform health checks and send data. For details on the IP addresses that will need access, refer to the <i>Probe IP ranges and firewall rules</i> section of the Google Cloud article Health checks.
target_size	2	Target size of the Autoscale cluster. For details, refer to the Google Cloud article Autoscaling groups of instances .

Resource	Default	Description
SCRIPT_TIMEOUT	500	Timeout (in seconds) of a Cloud Functions invocation.
MASTER_ELECTION_TIMEOUT	400	The maximum time (in seconds) to wait for a primary election to complete. This variable should be less than the total script timeout (SCRIPT_TIMEOUT).
FORTIGATE_ADMIN_PORT	8443	A port number for FortiGate-VM administration. Do not use the FortiGate reserved ports 443, 541, 514, or 703. Minimum is 1. Maximum is 65535. was: The admin port for the FortiGate Autoscale Cluster
HEARTBEAT_INTERVAL	25	The length of time (in seconds) that a FortiGate-VM waits between sending heartbeat requests to the function.
HEART_BEAT_DELAY_ALLOWANCE	10	Allowed variance (in seconds) before a heartbeat is considered out-of-sync and heartbeat loss is increased.
HEART_BEAT_LOSS_COUNT	10	Number of consecutively lost heartbeats. When the Heartbeat loss count has been reached, the FortiGate-VM is deemed unhealthy and failover activities will commence.

Variables can be referenced from the command line using:

```
terraform plan -var "<var name>=<value>"
```

Deployment information

Terraform will deploy the following resources:

- A VPC with two subnets split over two zones. More can be chosen if the region supports it.
- A Cloud NAT for egress traffic in the protected subnet
- An [Instance group](#)
- An [Instance template](#)
- A [Regional Autoscaler](#) (auto scaling policy)
- A [Google Storage bucket](#)
 - A template uploaded to the bucket at `assets/configset/baseconfig`
- A [Google Compute Function](#) with an [HTTP trigger](#)
- Two [GCP Firewall Rules](#): *Allow all*, and *Allow only internal connections*
- An [external-facing TCP network load balancer](#)
- An internal load balancer



Additionally, a [Firestore](#) collection will be created by the function. It is not created during the Terraform deployment phase.

Verify the deployment

1. Log in to the GCP console and navigate to *Firestore*.
2. Navigate to the *FortiGateMasterElection* table.
3. Make note of the primary FortiGate-VM IP address and ensure the *voteState* is *done*. See below for an example:

fortigateautoscale-fortigateautoscale-mmlo	FORTIGATEMASTERELECTION
+ ADD DOCUMENT	+ START COLLECTION
FORTIANALYZER	+ ADD FIELD
FORTIGATEAUTOSCALE	<div> <div>▼ masterRecord</div> <div> InstanceId: "7723829953355373558" </div> <div> MasterIP: "172.16.0.3" </div> <div> SubnetId: "null" </div> <div> VoteState: "done" </div> <div> VpcId: "empty" </div> <div> voteEndTime: 1575577057464 </div> </div>
<div> <div>⋮</div> <div>FORTIGATEMASTERELECTION</div> <div>></div> </div>	
LIFECYCLEITEM	
SETTINGS	

4. Navigate to the *FortiGateAutoscale* table and confirm that instances have been added to the cluster. Following is an example of a healthy cluster:

fortigateautoscale-fortigateautoscale-rnmlo 	FORTIGATEAUTOSCALE 
+ ADD DOCUMENT	+ START COLLECTION
FORTIANALYZER	+ ADD FIELD
⋮ FORTIGATEAUTOSCALE >	<div>▼ 5075870911861937758</div> <div> healthy: true heartBeatInterval: 25 heartBeatLossCount: "0" inSync: true instanceId: "5075870911861937758" ip: "172.16.0.7" masterIp: "172.16.0.3" nextHeartBeatTime: 1575580740272 syncState: "in-sync" </div>
FORTIGATEMASTERELECTION	<div>▼ 7244177209853008860</div> <div> healthy: true heartBeatInterval: 25 heartBeatLossCount: "0" inSync: true instanceId: "7244177209853008860" ip: "172.16.0.4" masterIp: "172.16.0.3" nextHeartBeatTime: 1575580747567 syncState: "in-sync" </div>
LIFECYCLEITEM	<div>▼ 7723829953355373558</div> <div> healthy: true heartBeatInterval: 25 heartBeatLossCount: "0" inSync: true instanceId: "7723829953355373558" ip: "172.16.0.3" masterIp: "172.16.0.3" nextHeartBeatTime: 1575580745865 syncState: "in-sync" </div>
SETTINGS	



The *masterIp* field displays the IP address of the primary FortiGate-VM.
When an instance is removed from a cluster its record will not be deleted.

Verify the instance group

1. Log in to the primary FortiGate-VM instance using the public IP address from step 3 of "Verify the deployment" on page 86. The default admin port is 8443 and the default username/password is *admin/<instance-id>*.
2. Cluster information is displayed on the main dashboard:

Virtual Machine

Allocated vCPUs 2

Allocated RAM 4 GiB

Auto Scaling ✔ Enabled

Role Master

Group Size 2

3. VPN status is under *Monitor > Ipsec Monitor*, which shows the current connections between the FortiGates in the cluster.

Refresh	Reset Statistics	Bring Up	Bring Down	Locate on VPN Map			
Name	Type	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
__autoscale_m_p1_0	Custom	172.16.0.4		27.74 kB <div></div>	13.85 kB <div></div>	__autoscale_m_p1	__autoscale_m_p2
__autoscale_m_p1_1	Custom	172.16.0.5		25.88 kB <div></div>	13.07 kB <div></div>	__autoscale_m_p1	__autoscale_m_p2
__autoscale_m_p1_2	Custom	172.16.0.7		17.66 kB <div></div>	7.61 kB <div></div>	__autoscale_m_p1	__autoscale_m_p2

4. Additional settings can be found in the *Firestore* collection under *SETTINGS*. See below for an example:

fortigateautoscale-fortigateautoscale-rnmlo	SETTINGS
+ ADD DOCUMENT	+ START COLLECTION
+ ADD FIELD FORTIANALYZER FORTIGATEAUTOSCALE FORTIGATEMASTERELECTION LIFECYCLEITEM SETTINGS	+ ADD FIELD ▼ asset-storage-key-prefix description: "Asset storage key prefix." editable: false jsonEncoded: false settingValue: "empty" ▼ asset-storage-name description: "Asset storage name." editable: false jsonEncoded: false settingValue: "fortigate-autoscale-rnmlo" ▼ autoscale-handler-url description: "The FortiGate Autoscale handler UR..." editable: false jsonEncoded: false settingValue: "https://us-central1-..." ▼ byol-scaling-group-name description: "The name of the BYOL auto scaling ..." editable: false jsonEncoded: false settingValue: "fortigateautoscale-rnmlo"

Cluster monitoring

Various cluster metrics are displayed in the GCP console under *Compute > Instance Groups > YOUR-FORTIGATE-AUTOSCALE_CLUSTER > Monitor*.

From here you can see the scale in and scale out actions that have been performed, as well as cluster health data.



Use [Operations \(formerly Stackdriver\)](#) for additional logging information, including scaling of the Function.

Adding instances to the protected subnet

When the deployment has completed, an Instance group can be created and VMs can be added to the protected subnet, behind the internal load balancer.

In GCP, NICs must reside in separate VPCs. In this deployment, the FortiGate will have two NICs: one in the exposed public subnet / VPC; the other in the protected subnet / VPC. By default, the protected subnet will be called *fortigateautoscale-protected-subnet-CLUSTER-SUFFIX*.

The default FortiGate configuration located under `/assets/configset/baseconfig` specifies a VIP on port 80 and a VIP on port 443 with a policy that points to an internal load balancer.



In FortiOS 6.2.3 any VIPs created on the primary instance will not sync to the secondary instances. Any VIP you wish to add must be added as part of the baseconfig.

The following illustrates adding a basic unmanaged Instance group into the protected subnet and internal load balancer.

1. Create the VM, ensuring that it resides within the proper region, VPC and subnet:

← Create an instance

To create a VM instance, select one of the options:

- New VM instance**
Create a single VM instance from scratch
- New VM instance from template**
Create a single VM instance from an existing template
- Marketplace**
Deploy a ready-to-go solution onto a VM instance

Name ⓘ
Name is permanent
protected-instance

Region ⓘ
Region is permanent
us-central1 (Iowa)

Zone ⓘ
Zone is permanent
us-central1-a

Machine configuration ⓘ

Machine family
General-purpose Memory-optimized
Machine types for common workloads, optimized for cost and flexibility

Series
N1
Powered by Intel Skylake CPU platform or one of its predecessors

Machine type
n1-standard-1 (1 vCPU, 3.75 GB memory)

	vCPU	Memory
	1	3.75 GB

⌵ CPU platform and GPU

Container ⓘ
☐ Deploy a container image to this VM instance. [Learn more](#)

Boot disk ⓘ

New 10 GB standard persistent disk
Image
CentOS 7 Change

Identity and API access ⓘ

Service account ⓘ
Compute Engine default service account

Access scopes ⓘ
☒ Allow default access
☐ Allow full access to all Cloud APIs
☐ Set access for each API

Firewall ⓘ
Add tags and firewall rules to allow specific network traffic from the Internet
☐ Allow HTTP traffic
☐ Allow HTTPS traffic

Management Security Disks **Networking** Sole Tenancy

Network tags ⓘ (Optional)

Hostname ?
Set a custom hostname for this instance or leave it default. Choice is permanent

protected-instance.c.dev-project-001-166400.internal

Network interfaces ?
Network interface is permanent

Network Interface

Network ?
fortigateautoscale-protected-vpc-kcjjg

Subnetwork ?
fortigateautoscale-protected-subnet-kcjjg (172.16.8.0/24)

Primary internal IP ?
Ephemeral (Automatic)

⌵ Show alias IP ranges

External IP ?
None

IP forwarding ?
Off

Done Cancel

+ Add network interface

⌵ Less

You will be billed for this instance. [Compute Engine pricing](#)

Create Cancel

Equivalent [REST](#) or [command line](#)


FortiOS GCP Administration Guide

Fortinet Technologies Inc.

2. Create an Instance group:


← Create an instance group

To create an instance group, select one of the options:



New managed instance group

Create a group of identical VM instances from an existing template. Manage VM instances as a single entity.



New unmanaged instance group

Create a group of unique VM instances without using a template. Add and remove VM instances manually.

Organize VM instances in a group to manage them together. [Instance groups](#)

Name ⓘ
Name is permanent

protected-instance-group

Description (Optional)

Location

Region ⓘ
Region is permanent

us-central1 (Iowa)

Zone ⓘ
Zone is permanent

us-central1-a

Specify port name mapping (Optional)

Network ⓘ

fortigateautoscale-protected-vpc-kcjjg

Subnetwork ⓘ

fortigateautoscale-protected-subnet-kcjjg (172.16.8.0/24)

VM instances

protected-instance

No available instances

You will be billed for VM instances in this group. [Compute Engine pricing](#)

Create Cancel

Equivalent [REST](#) or [command line](#)

3. Under *Network services > Load balancing* choose the *Internal load balancer*, select *Backend configuration* and add the new Instance group.

Destroying the cluster

The easiest way to destroy an autoscale cluster is to use Terraform.

1. From your GCP directory, enter the following and confirm the resources are the ones you wish to destroy.

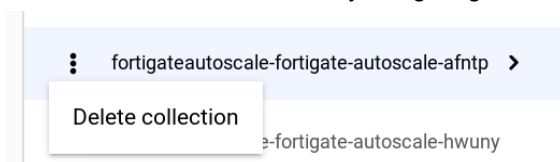
```
terraform destroy
```

If you have VMs in the protected subnet you will need to manually remove these VMs before destroying the cluster.

2. Output should appear as follows after the cluster has been destroyed:

```
Destroy complete! Resources: 20 destroyed.
```

3. Erase the Firestore database by navigating to *Firestore*. Hover over the root collection and select *Delete collection*.



4. Enter the collection name to proceed.

Delete this collection?

! Doing so will permanently delete the data at this collection path, including all nested documents and collections.

Collection path
/fortigateautoscale-fortigate-autoscale-afntp

Confirm you want to delete this collection by typing its ID: **fortigateautoscale-fortigate-autoscale-afntp**

Collection ID *

CANCEL DELETE

Troubleshooting

Debugging cloud-init

Retrieving the `cloud-init` log can be useful when issues are occurring at boot up. To retrieve the log, log in to the FortiGate-VM and type the following into the CLI:

```
diag debug cloudinit show
```

Output will look similar to the following:

```
>> Checking metadata source gcp
>> GCP processing json format user-data
>> GCP trying to get config script from: https://us-central1-
*****.cloudfunctions.net/fortigateautoscale-rnmlo
>> GCP download config script successfully
>> Run config script
>> Finish running script
>> FortiGate-VM64-GCPON~AND $ config system dns
>> FortiGate-VM64-GCPON~AND (dns) $ unset primary
>> FortiGate-VM64-GCPON~AND (dns) $ unset secondary
>> FortiGate-VM64-GCPON~AND (dns) $ end
>> FortiGate-VM64-GCPON~AND $ config system auto-scale
>> FortiGate-VM64-GCPON~AND (auto-scale) $ set status enable
```

```
>> FortiGate-VM64-GCPON~AND (auto-scale) $ set sync-interface "port1"
>> FortiGate-VM64-GCPON~AND (auto-scale) $ set hb-interval 25
>> FortiGate-VM64-GCPON~AND (auto-scale) $ set role slave
>> FortiGate-VM64-GCPON~AND (auto-scale) $ set master-ip xxx.xxx.xxx.xxx
>> FortiGate-VM64-GCPON~AND (auto-scale) $ set callback-url https://us-central1-
*****.cloudfunctions.net/fortigateautoscale-rnmlo
>> FortiGate-VM64-GCPON~AND (auto-scale) $ set psksecret *****
>> FortiGate-VM64-GCPON~AND (auto-scale) $ end
```

How to reset the elected primary FortiGate

To reset the elected primary FortiGate, navigate to *FireStore > FortiGateMasterElection* and delete the only item. A new primary FortiGate will be elected and a new record will be created as a result.

For details on locating *FireStore > FortiGateMasterElection*, refer to the section "Verify the deployment" on page 86.

Appendix

FortiGate Autoscale for GCP features



Major components

- *The Instance group*. The Instance group contains one to many FortiGate-VMs (PAYG licensing model). This Instance group will dynamically scale out or scale in based on `cpu_utilization`.
- The *configset* folder contains files that are loaded as the initial configuration for a new FortiGate-VM instance.
 - *baseconfig* is the base configuration. This file can be modified as needed to meet your network requirements. Placeholders such as {SYNC_INTERFACE} are explained in the section "Configset placeholders" below.
- *Tables in Firestore*. These tables are required to store information such as health check monitoring, primary election, state transitions, etc. These records should not be modified unless required for troubleshooting purposes.

Configset placeholders

When the FortiGate-VM requests the configuration from the Auto Scaling function, the placeholders in the table below will be replaced with associated environment variables stored in Cloud Functions.

Placeholder	Type	Description
{SYNC_INTERFACE}	Text	The interface for FortiGate-VMs to synchronize information. All characters must be lowercase.
{CALLBACK_URL}	URL	The Cloud Functions URL to interact with the Auto Scaling handler script. Automatically generated during the Terraform deployment.

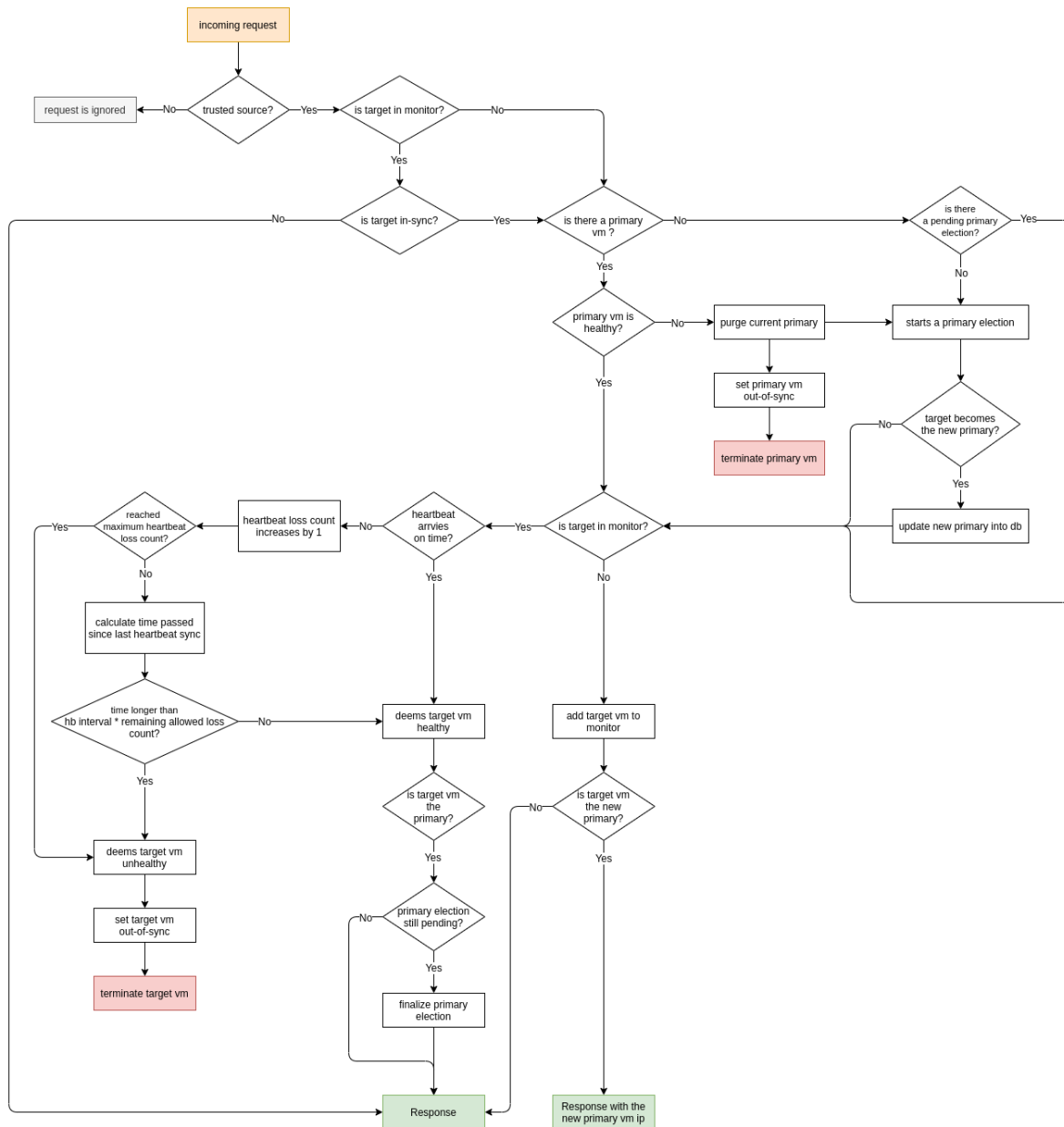
Placeholder	Type	Description
{PSK_SECRET}	Text	The Pre-Shared key used in FortiOS. Randomly generated during the Terraform deployment.
		 Changes to the PSK secret after FortiGate Autoscale for GCP has been deployed are not reflected here. For new instances to be spawned with the changed PSK secret, this environment variable will need to be manually updated.
{ADMIN_PORT}	Number	A port number specified for administration login. A positive integer such as 443 etc. Default value: 8443.
		 Changes to the admin port after deployment are not reflected here. For new instances to be spawned with the changed admin port, this environment variable will need to be updated.

Architectural diagram

Election of the primary instance

FortiGate Autoscale

with heartbeat response & failover management



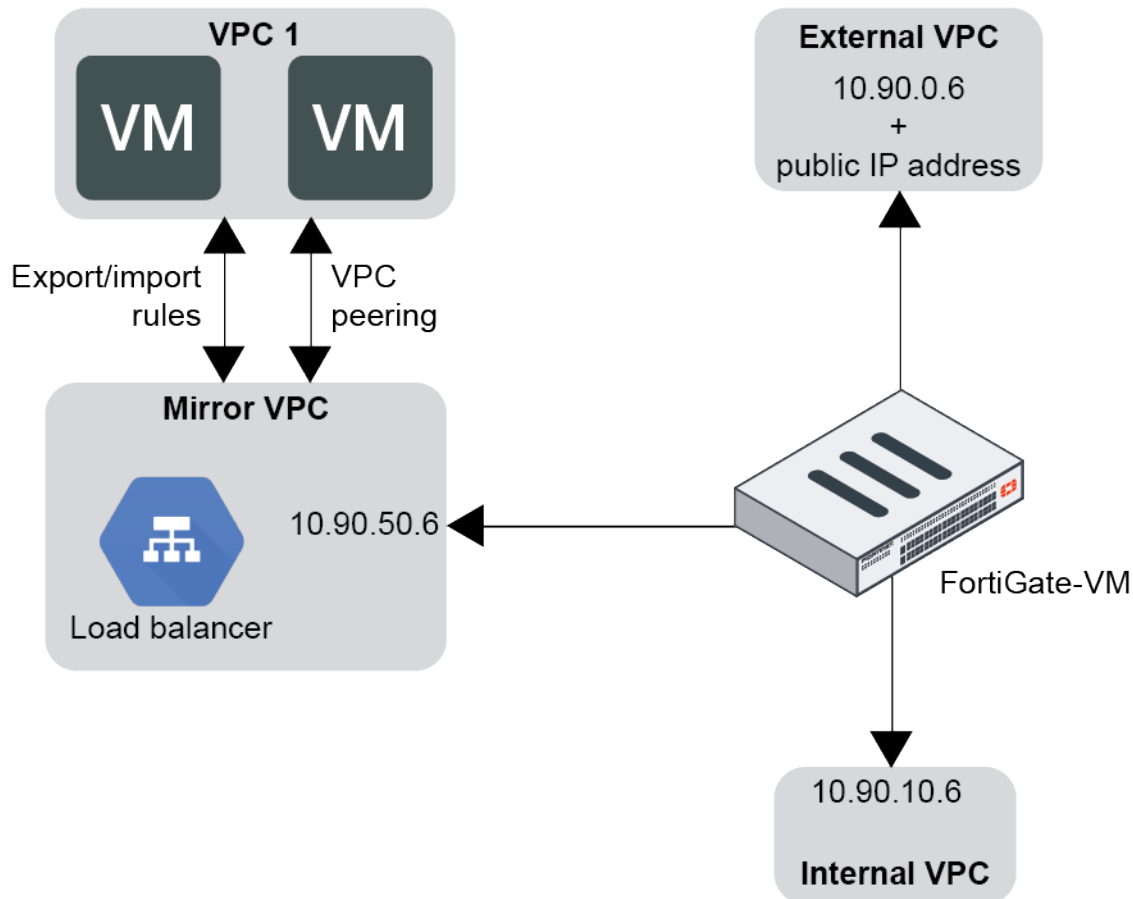
VPN for FortiGate-VM on GCP

Site-to-site IPsec VPNs between HA VPN on GCP

See [Google Cloud HA VPN interoperability guide for FortiGate](#).

Packet mirroring

You can use GCP's packet mirroring feature to capture all ingress and egress traffic and packet data, such as payloads and headers. As packet mirroring exports all traffic, not only the traffic between sampling periods, you may find it useful when monitoring and analyzing your security status. This configuration mirrors the traffic from a network interface or subnet in the specified VPC and sends it to the internal load balancer, which is specified as the destination in the packet mirroring policy. The following shows the topology for this configuration:



Creating VPC networks

This configuration requires three VPCs for the FortiGate: external, internal, and mirroring. It also requires a fourth VPC where you deploy the VM instances whose traffic will be mirrored. This guide refers to the fourth VPC as "VPC 1".

To create the VPC networks:

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.
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*.

[←](#) VPC network details
 [EDIT](#)
[DELETE VPC NETWORK](#)

packetmirroring-vpc1

Subnet creation mode
Custom subnets

Dynamic routing mode ?
☒ **Regional**
 Cloud Routers will learn routes only in the region in which they were created
☐ **Global**
 Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router

DNS server policy (Optional)
 No server policy

[Save](#) [Cancel](#)

[Subnets](#)
[Static internal IP addresses](#)
[Firewall rules](#)
[Routes](#)
[VPC Network Peering](#)
[Private service connection](#)

[Add subnet](#)
[Flow logs](#)

<input type="checkbox"/> Name ^	Region	IP address ranges	Gateway	Private Google access	Flow logs ?
<input type="checkbox"/> packetmirroring-vpc1-subnet1	us-west1	10.90.100.0/24	10.90.100.1	Off	Off

Reserved subnets for internal HTTP(S) load balancers ?

<input type="checkbox"/> Name	Region ^	IP address ranges	Gateway	Role
No matching results				

6. Repeat steps 1-5 to create the remaining three VPCs.
7. Go to *Compute Engine > Virtual machines > VM instances*. Deploy two VMs to VPC 1.

Launching the FortiGate-VM instance

Launch the FortiGate-VM instance from the marketplace as [Initially deploying the FortiGate-VM on page 12](#) describes. Ensure that you configure the FortiGate-VM with the network interfaces for the internal, external, and mirroring VPCs that you created in [Creating VPC networks on page 100](#).

VM instance details [EDIT](#) [RESET](#) [+ CREATE MACHINE IMAGE](#) [LEARN](#)

byol-fgt1

[Details](#) [Monitoring](#) [Screenshot](#)

Remote access

SSH [Connect to serial console](#)

☒ Enable connecting to serial ports
Connecting to serial ports is enabled in project-wide metadata

Logs

[Cloud Logging](#)

[Serial port 1 \(console\)](#)

[More](#)

Instance Id

Machine type

n1-standard-4 (4 vCPUs, 15 GB memory)

This instance is underutilized. You can save an estimated \$46 per month by switching to the machine type: custom (2 vCPUs, 5 GB memory). [Learn more](#) [Dismiss](#) [Resize](#)

Reservation

Automatically choose

In use by

[packetmirror-instance-group1](#)

CPU platform

Intel Broadwell

Display device

Turn on a display device if you want to use screen capturing and recording tools.

☐ Turn on display device

Zone

us-west1-a

Labels

None

Creation time

Dec 4, 2020, 10:35:19 AM

Network interfaces

Name	Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP	Network Tier	IP forwarding	Network details
nic0	vpc-ext	vpc-ext-subnet	10.90.0.6	—	34.82.224.172 (ephemeral)	Premium	On	View details
nic1	vpc-int	vpc-int-subnet	10.90.10.6	—	None			View details
nic2	vpc-mirror	vpc-mirror-subnet	10.90.50.6	—	None			View details

Creating an unmanaged instance group and load balancer

To create an unmanaged instance group:

1. Go to *Compute Engine > Instance groups > New unmanaged instance group*.
2. From the *Region* and *Zone* dropdown lists, select the same region and zone that the mirrored recipient, in this case the FortiGate-VM, is in.
3. From the *Network* dropdown list, select the FortiGate-VM external VPC network.
4. From the *Subnetwork* dropdown list, select the subnet in the external VPC where the FortiGate-VM interface is.
5. From the *VM instances* dropdown list, select the FortiGate-VM.
6. Click *Create*.

To create a health check:

1. Go to *Compute Engine > Instance groups > Health checks*.
2. From the *Protocol* dropdown list, select *TCP*.

3. In the *Port* field, enter 22.
4. In the *Check interval* and *Timeout* fields, enter 5.



The health check fails unless you add a firewall rule to allow the following IP address ranges: 130.211.0.0/22 and 35.191.0.0/16.

To create an internal load balancer for the packet mirroring policy:

1. Go to *NETWORKING > Network services > Load balancing > Create load balancer*.
2. Under *TCP Load Balancing*, click *Start configuration*.
3. Under *Internet facing or internal only*, select *Only between my VMs*.
4. Under *Multiple regions or single region*, select *Single region only*.
5. Click *Continue*.
6. Complete backend configuration:
 - a. From the *Region* dropdown list, select the same region as the FortiGate-VM and instance group.
 - b. From the *Network* dropdown list, select the mirror VPC.
 - c. From the *Health check* dropdown list, select the health check that you created.
7. Complete frontend configuration:
 - a. From the *Subnetwork* dropdown list, select the mirror subnet.
 - b. Under *Advanced options*, select *Enable this load balancer for packet mirroring*.
 - c. Click *Done*.
8. Click *Create*.

Configuring bidirectional VPC peering

To configure bidirectional VPC peering:

1. Go to *VPC network > VPC network peering*.
2. Click *CREATE CONNECTION*, then *Continue*.
3. From the *Your VPC network* dropdown list, select the mirror VPC.
4. From the *VPC network name* dropdown list, select VPC 1.
5. Select all *Import* and *Export* options.
6. Click *CREATE*.
7. Repeat steps 2-6, this time selecting VPC 1 in the *Your VPC network* dropdown list and the mirror VPC in the *VPC network name* dropdown list. This allows bidirectional traffic flow.

Creating the packet mirroring policy

This policy mirrors the contents of VPC 1 and reflects them on the mirror VPC.

To create the packet mirroring policy:

1. Go to *VPC network > Packet mirroring > CREATE POLICY*.
2. From the *Region* dropdown list, select the same region selected for previous resources.
3. Under *Policy enforcement*, select *Enabled*. Click *CONTINUE*.
4. Select the VPC network:
 - a. Select *Mirrored source and collector destination are in separate, peered VPC networks*.
 - b. From the *Mirrored source VPC network* dropdown list, select VPC 1.
 - c. From the *Collector destination VPC network* dropdown list, select the mirror VPC. Click *CONTINUE*.
5. Click *Select one or more subnetworks*.
6. From the dropdown list, select VPC 1. Click *CONTINUE*.
7. The collector destination must be a GCP load balancer. From the *Collector destination* dropdown list, select the frontend name of the load balancer that you created in [To create an internal load balancer for the packet mirroring policy: on page 103](#). Click *CONTINUE*.
8. Select *Mirror all traffic*. Alternatively, you can monitor traffic between specific instances using instance tags.

Verifying the configuration

To verify the configuration:

1. On one of the VMs in VPC 1, ping the other VM. In this example, the VM IP addresses are 10.138.0.8 and 10.138.0.9. The following shows successful communication between the VMs:

```

$ ping 10.138.0.8
PING 10.138.0.8 (10.138.0.8) 56(84) bytes of data:
64 bytes from 10.138.0.8: icmp_seq=1 ttl=64 time=1.48 ms
64 bytes from 10.138.0.8: icmp_seq=2 ttl=64 time=0.371 ms
64 bytes from 10.138.0.8: icmp_seq=3 ttl=64 time=0.382 ms
64 bytes from 10.138.0.8: icmp_seq=4 ttl=64 time=0.377 ms
^C
--- 10.138.0.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 42ms
rtt min/avg/max/mdev = 0.371/0.653/1.484/0.480 ms

```

2. If the packet mirroring configuration was successful, the packets are visible to the FortiGate. In FortiOS, run the `diagnose sniffer packet port3 'host <VM 1 IP address> and host <VM 2 IP address>' 4 0 3` command. Port3 is the FortiGate interface that is sitting in the mirror VPC. The output should look as follows:

```

# FortiGate #1 fgt $ diagnose sniffer packet port3 'host 10.138.0.8 and host 10.138.0.9' 4 0 3
interfaces=[port3]
filters=[host 10.138.0.8 and host 10.138.0.9]
pcap_lookupnet: port3: no IPv4 address assigned
6.783470 port3 -- 10.138.0.9 -> 10.138.0.8: icmp: echo request
6.783623 port3 -- 10.138.0.9 -> 10.138.0.8: icmp: echo request
6.784078 port3 -- 10.138.0.8 -> 10.138.0.9: icmp: echo reply
6.784310 port3 -- 10.138.0.8 -> 10.138.0.9: icmp: echo reply
7.784492 port3 -- 10.138.0.9 -> 10.138.0.8: icmp: echo request
7.784519 port3 -- 10.138.0.9 -> 10.138.0.8: icmp: echo request
7.784673 port3 -- 10.138.0.8 -> 10.138.0.9: icmp: echo reply
7.784687 port3 -- 10.138.0.8 -> 10.138.0.9: icmp: echo reply
8.797265 port3 -- 10.138.0.9 -> 10.138.0.8: icmp: echo request
8.797290 port3 -- 10.138.0.9 -> 10.138.0.8: icmp: echo request
8.797485 port3 -- 10.138.0.8 -> 10.138.0.9: icmp: echo reply
8.797494 port3 -- 10.138.0.8 -> 10.138.0.9: icmp: echo reply
9.821224 port3 -- 10.138.0.9 -> 10.138.0.8: icmp: echo request
9.821246 port3 -- 10.138.0.9 -> 10.138.0.8: icmp: echo request
9.821393 port3 -- 10.138.0.8 -> 10.138.0.9: icmp: echo reply
9.821494 port3 -- 10.138.0.8 -> 10.138.0.9: icmp: echo reply

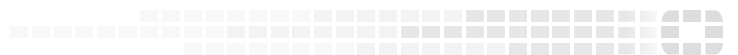
```

Change log

Date	Change Description
2020-03-31	Initial release.
2020-05-05	Updated Registering and downloading licenses.
2020-05-13	Added Migrating a FortiGate-VM instance between license types on page 11. Updated Order types on page 8.
2020-05-15	Updated Order types on page 8.
2020-06-26	Updated Deploying FortiGate-VM HA on GCP in one zone on page 46.
2020-07-06	Added Deploying FortiGate-VM using Terraform on page 45.
2020-07-09	Added To configure a VDOM exception: on page 61.
2020-10-06	Updated Creating VPC networks on page 48 and Deploying the primary FortiGate-VM instance on page 49.
2020-10-09	Updated Deploying auto scaling on GCP on page 80.
2020-12-08	Updated Order types on page 8.
2020-12-11	Updated Creating a support account on page 10.
2021-01-13	Added Packet mirroring on page 100.
2021-02-18	Updated SDN connector integration with GCP on page 63.
2021-03-22	Added Upgrading or downgrading a GCP instance to another machine type on page 6.
2021-04-12	Updated Initially deploying the FortiGate-VM on page 12.
2021-08-30	Added Multiple GCP projects in a single SDN connector on page 64.



FORTINET®



Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.