Deploying on Google Cloud

FortiProxy 7.2

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

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

FORTINET BLOG
https://blog.fortinet.com

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

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

May 1, 2023
FortiProxy 7.2 Deploying on Google Cloud
45-720-842808-20230501

TABLE OF CONTENTS

Change Log

Date	Change Description
2022-09-19	Initial release.
2023-05-01	Updated Obtaining the deployment image on page 6.

Deploying FortiProxy-VM on Google Cloud Compute Engine

This guide describes deploying FortiProxy-VM on Google Cloud Compute Engine. This deployment consists of the following steps:

1. Obtaining the deployment image on page 6
2. Uploading the FortiProxy deployment image to Google Cloud on page 7
3. Creating the FortiProxy deployment image on page 8
4. Deploying the FortiProxy-VM instance on page 10
5. Connecting to the FortiProxy-VM on page 13
6. Configuring Google Cloud firewall rules on page 17
7. Configuring the second NIC on the FortiProxy-VM on page 19
8. Configuring static routing in FortiProxy-VM on page 20

Obtaining the deployment image

To obtain the deployment image:

1. Go to the Fortinet support site and log in.
2. Go to *Support* > *Firmware Download*.
3. From the *Select Product* dropdown list, select *FortiProxy*.
4. Click the *Download* tab and browse to the required version.
5. Download the deployment package file by clicking *HTTPS* at the end of the row. The deployment package file is named *FPX_KVM_GCP-vX00-buildXXXX-FORTINET.out.gcp.tar.gz*, where vX00 is the major version number and XXXX is the build number.

This deployment method only applies for BYOL.

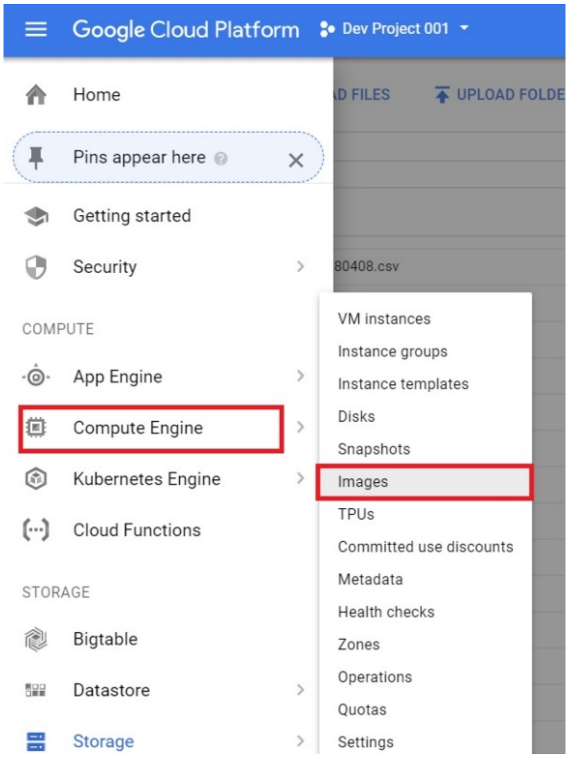
Uploading the FortiProxy deployment image to Google Cloud

To upload the FortiProxy deployment image to Google Cloud:

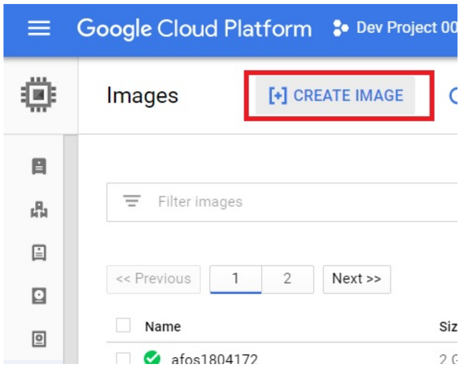
1. Log into Google Cloud.
2. Go to *Cloud Storage* > *Browser*.
3. Create a new bucket or go to an existing bucket.
4. Upload the newly downloaded deployment file.

Creating the FortiProxy deployment image

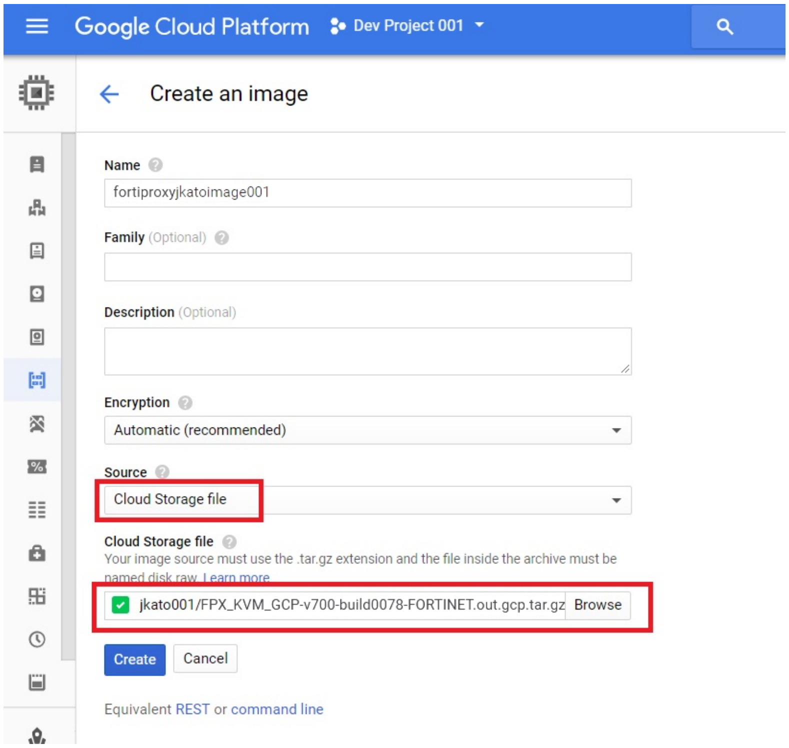
1. Go to *Compute Engine* > *Images*.



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*.



Name
fortiproxyjkatoimage001

Family (Optional)

Description (Optional)

Encryption
Automatic (recommended)

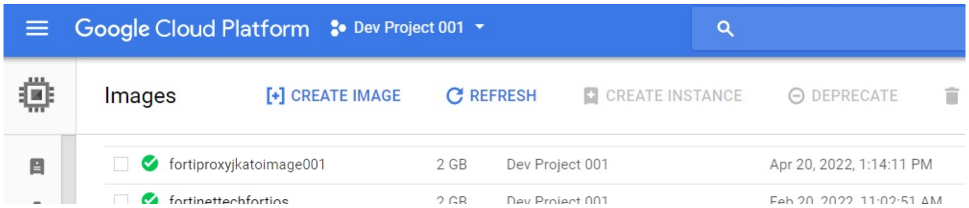
Source
Cloud Storage file

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/FPX_KVM_GCP-v700-build0078-FORTINET.out.gcp.tar.gz

Equivalent REST or command line

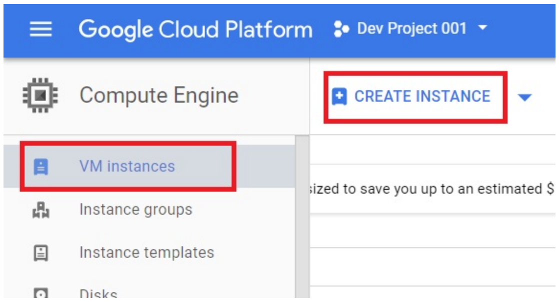
The image is listed on the *Images* pane.



fortiproxyjkatoimage001	2 GB	Dev Project 001	Apr 20, 2022, 1:14:11 PM
fortinettechfortios	2 GB	Dev Project 001	Feb 20, 2022, 11:02:51 AM

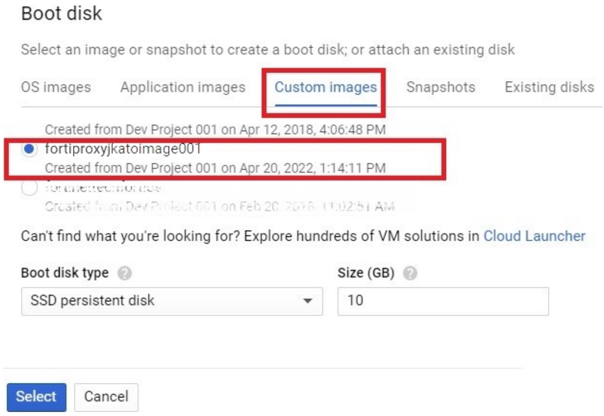
Deploying the FortiProxy-VM instance

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



ized to save you up to an estimated $

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.
   d. Change the boot disk type as needed, enter *10* for the *Size*, then click *Select*.



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

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

● fortiproxyjkatoimage001
Created from Dev Project 001 on Apr 20, 2022, 1:14:11 PM

○
Created from Dev Project 001 on Feb 20, 2018, 11:02:51 AM

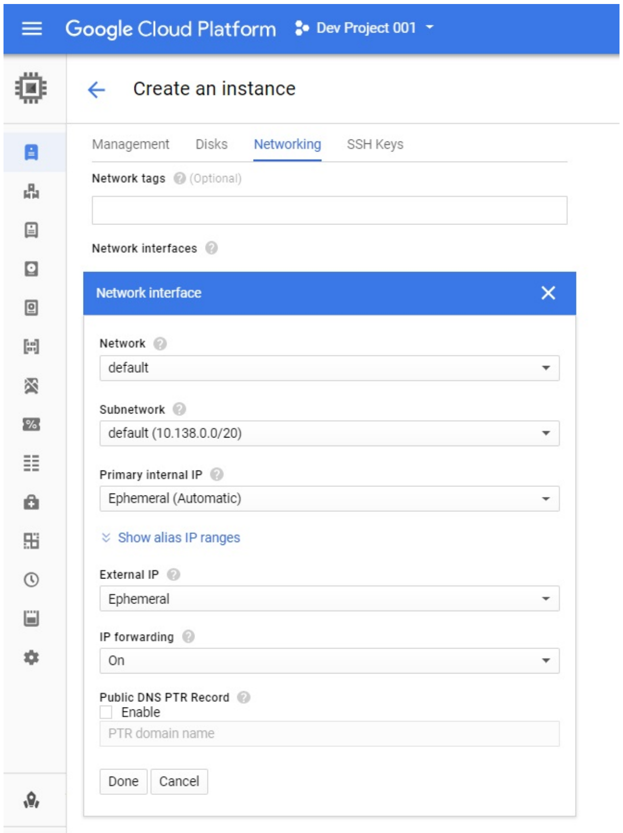
Can't find what you're looking for? Explore hundreds of VM solutions in Cloud Launcher

Boot disk type: SSD persistent disk

Size (GB): 10

   e. Ensure the new image is selected then select *Allow HTTPS* traffic.

      You will access the FortiProxy management console using HTTPS. If you allocate multiple network interfaces to the FortiProxy, this is nullified at this stage. You can configure this later. See Configuring Google Cloud firewall rules on page 17.
   f. Click *Networking*. Two network interfaces will be specified, one on the public-facing side of the internet and the other facing a protected private network.
   g. Edit the first network interface. Assign a static IP address and under *IP Forwarding* select *On*. Configure other items as needed and click *Done*.



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

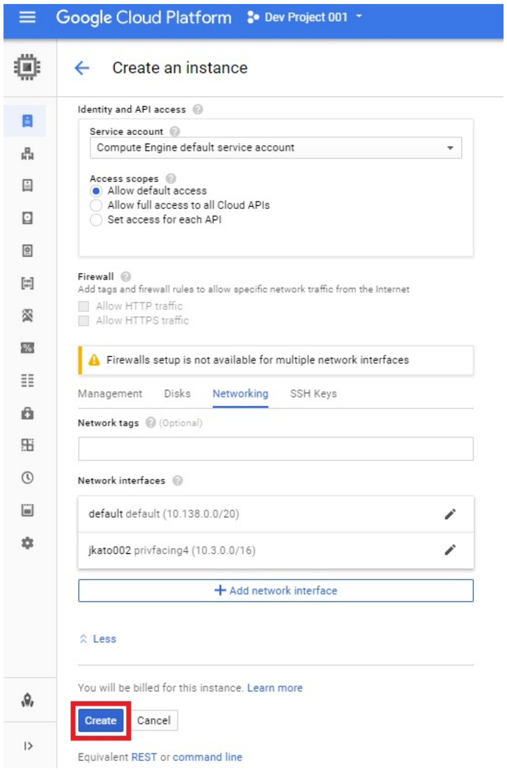
Public DNS PTR Record

□ Enable

PTR domain name

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 and under *External IP* select *None*.

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



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

Network tags (Optional)

Network interfaces
- default default (10.138.0.0/20)
- jkato002 privfacing4 (10.3.0.0/16)

You will be billed for this instance. Learn more

Equivalent REST or command line

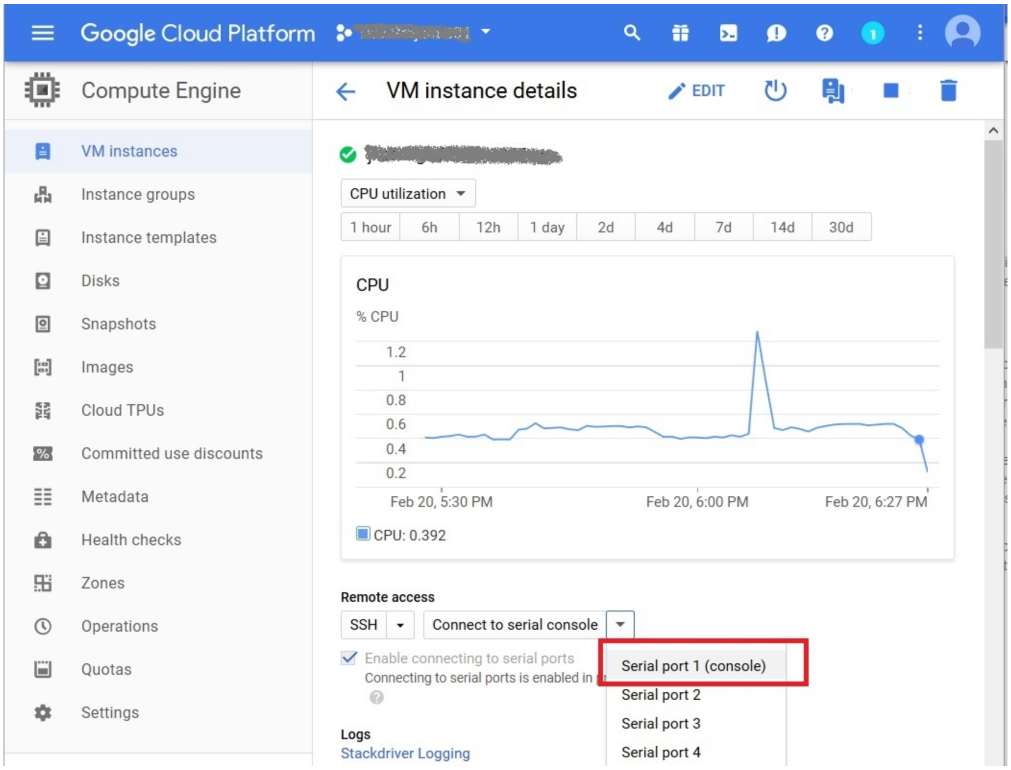
After 15 to 30 minutes, the instance should be up and running.

Connecting to the FortiProxy-VM

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

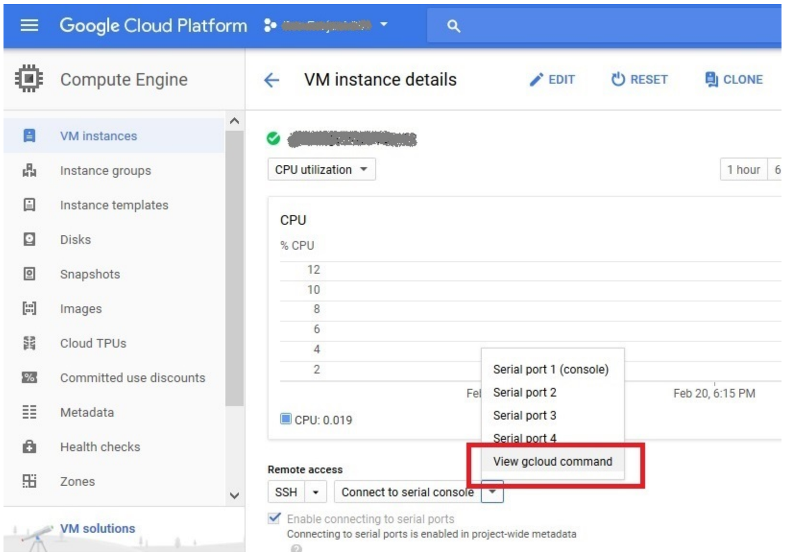
To connect to the FortiProxy-VM:

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 FortiProxy_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.

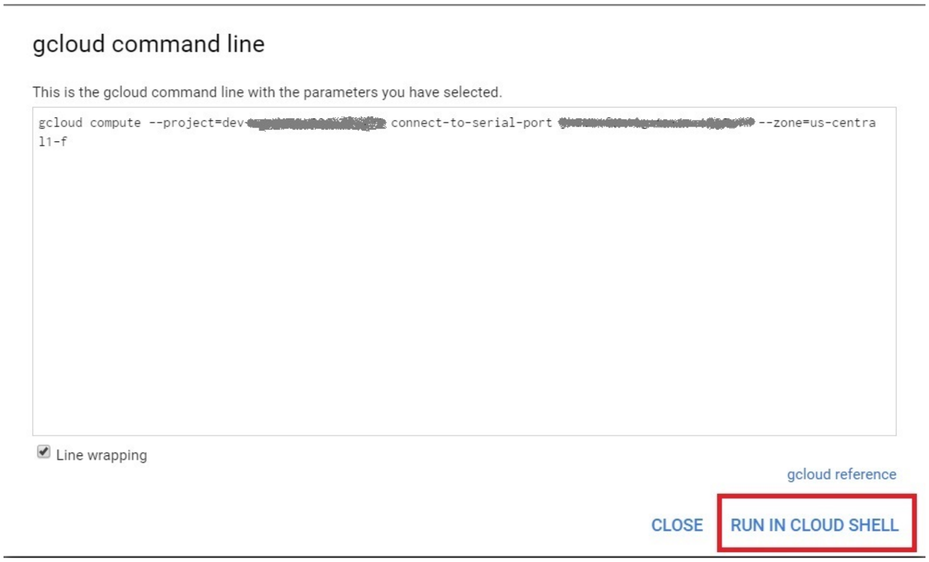


The first time you access the serial console, you will find the instance ID, represented as a number. This is the login password.

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



iii. Click *RUN IN CLOUD SHELL*.



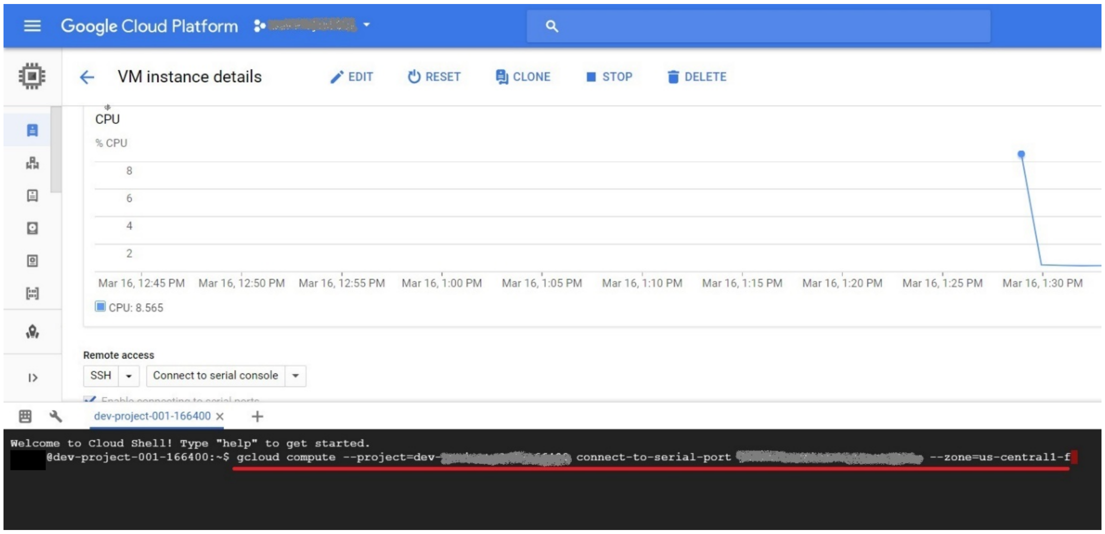
gcloud command line

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

```
gcloud compute --project=dev[redacted] connect-to-serial-port [redacted] --zone=us-centra
l1-f
```

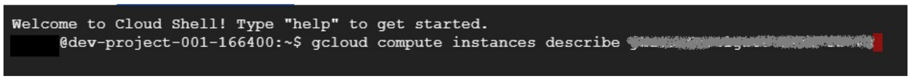
☑ Line wrapping

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



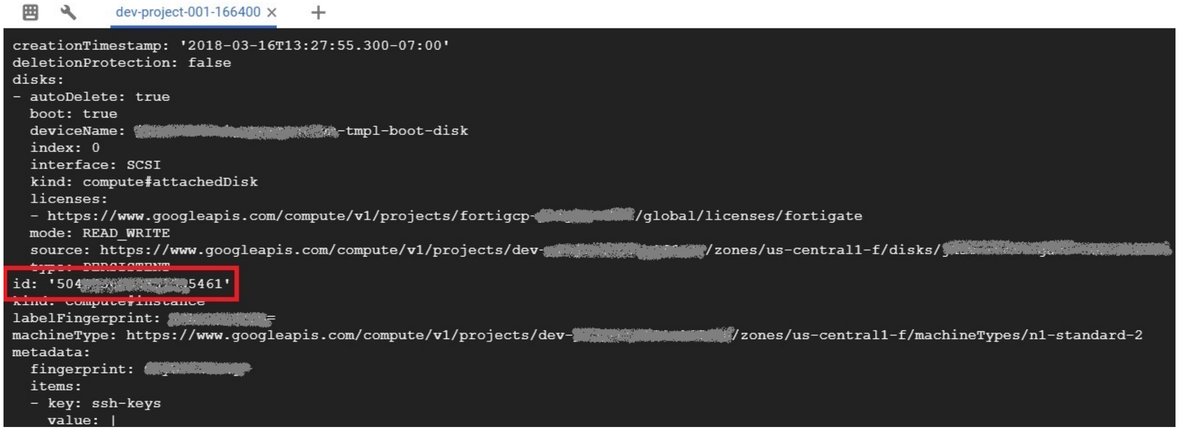
```
Welcome to Cloud Shell! Type "help" to get started.
[redacted]@dev-project-001-166400:~$ gcloud compute --project=dev-[redacted] connect-to-serial-port [redacted] --zone=us-central1-f
```

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



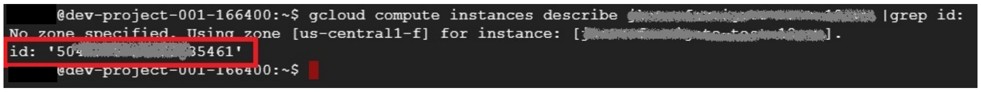
```
Welcome to Cloud Shell! Type "help" to get started.
[redacted]@dev-project-001-166400:~$ gcloud compute instances describe [redacted]
```

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



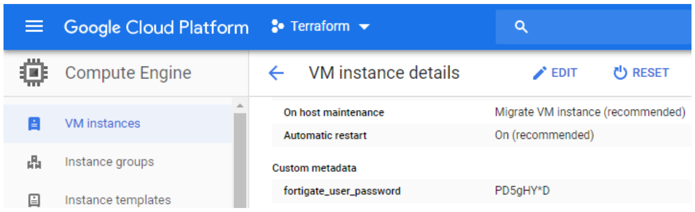
```
creationTimestamp: '2018-03-16T13:27:55.300-07:00'
deletionProtection: false
disks:
- autoDelete: true
  boot: true
  deviceName: [redacted]-tmpl-boot-disk
  index: 0
  interface: SCSI
  kind: compute#attachedDisk
  licenses:
  - https://www.googleapis.com/compute/v1/projects/fortigcp-[redacted]/global/licenses/fortigate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

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



```
[redacted]@dev-project-001-166400:~$ gcloud compute instances describe [redacted] |grep id:
No zone specified. Using zone [us-central1-f] for instance: [[redacted]].
id: '504[redacted]35461'
[redacted]@dev-project-001-166400:~$
```

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

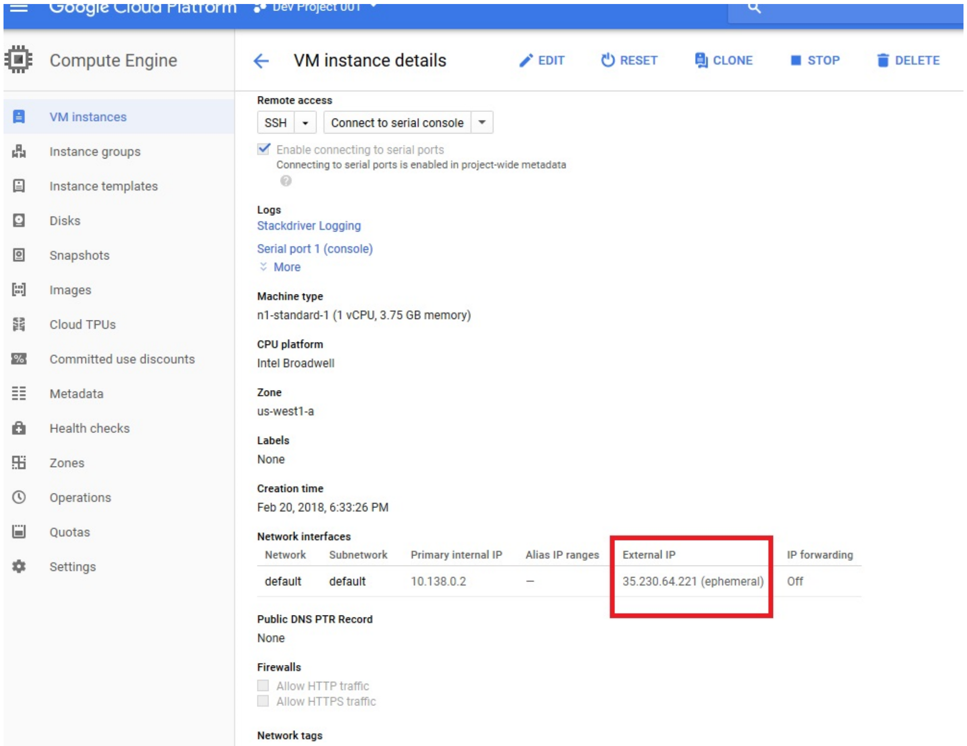


On host maintenance	Migrate VM instance (recommended)
Automatic restart	On (recommended)

Custom metadata

fortigate_user_password	PD5gHY*D

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



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 interfaces

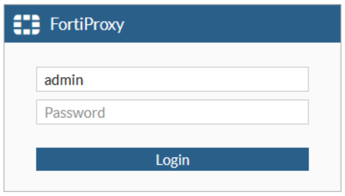
Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP	IP forwarding
default	default	10.138.0.2	–	35.230.64.221 (ephemeral)	Off

Public DNS PTR Record
None

Firewalls
□ Allow HTTP traffic
□ Allow HTTPS traffic

Network tags

4. Access the FortiProxy in your browser.



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

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

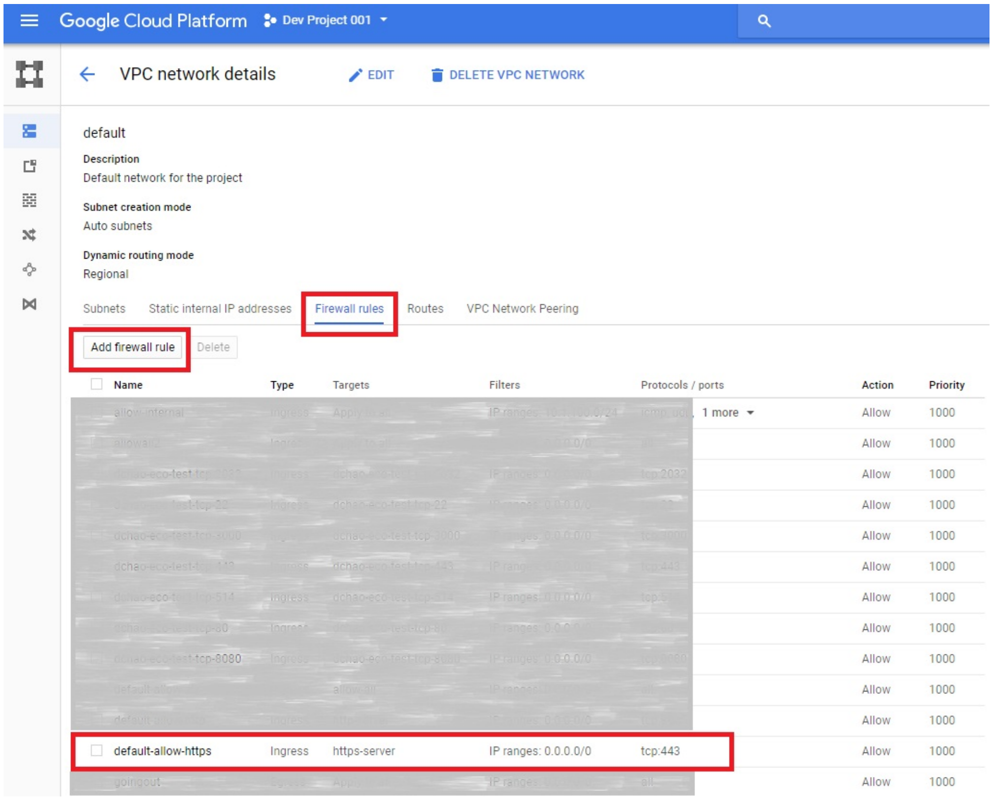
   You are encouraged to change the initial password at the top right corner of the FortiProxy GUI.

Configuring Google Cloud firewall rules

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

HTTPS is the first port that is needed. Other ports are optional depending on what features are enabled. See *FortiProxy Ports* for a list of incoming and outgoing ports.

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



default

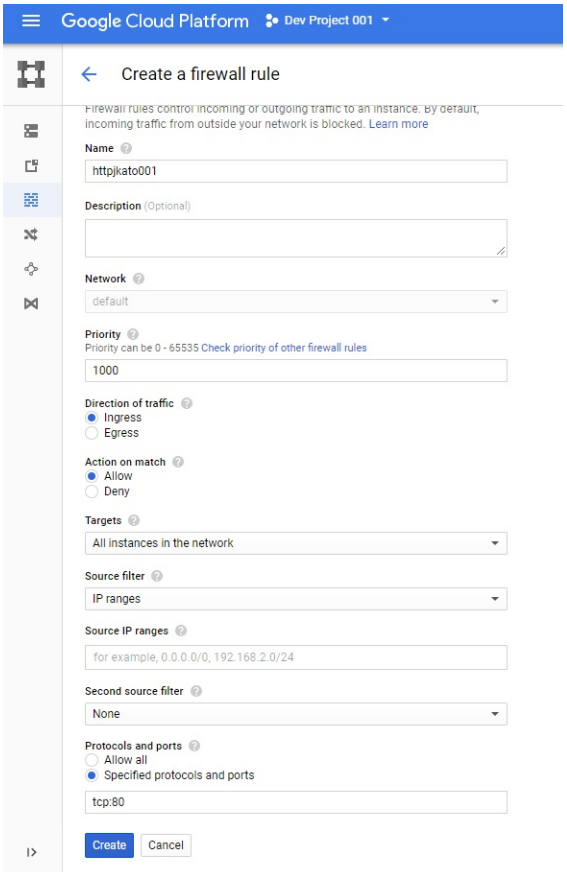
Description
Default network for the project

Subnet creation mode
Auto subnets

Dynamic routing mode
Regional

□ Name	Type	Targets	Filters	Protocols / ports	Action	Priority
[redacted]	[redacted]	[redacted]	[redacted]	[redacted] 1 more ▾	Allow	1000
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Allow	1000
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Allow	1000
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Allow	1000
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Allow	1000
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Allow	1000
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Allow	1000
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Allow	1000
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Allow	1000
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Allow	1000
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Allow	1000
□ default-allow-https	Ingress	https-server	IP ranges: 0.0.0.0/0	tcp:443	Allow	1000
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Allow	1000

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



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
httpjkato001

Description (Optional)

Network
default

Priority
Priority can be 0 - 65535 Check priority of other firewall rules
1000

Direction of traffic
● Ingress
○ Egress

Action on match
● Allow
○ Deny

Targets
All instances in the network

Source filter
IP ranges

Source IP ranges
for example, 0.0.0.0/0, 192.168.2.0/24

Second source filter
None

Protocols and ports
○ Allow all
● Specified protocols and ports

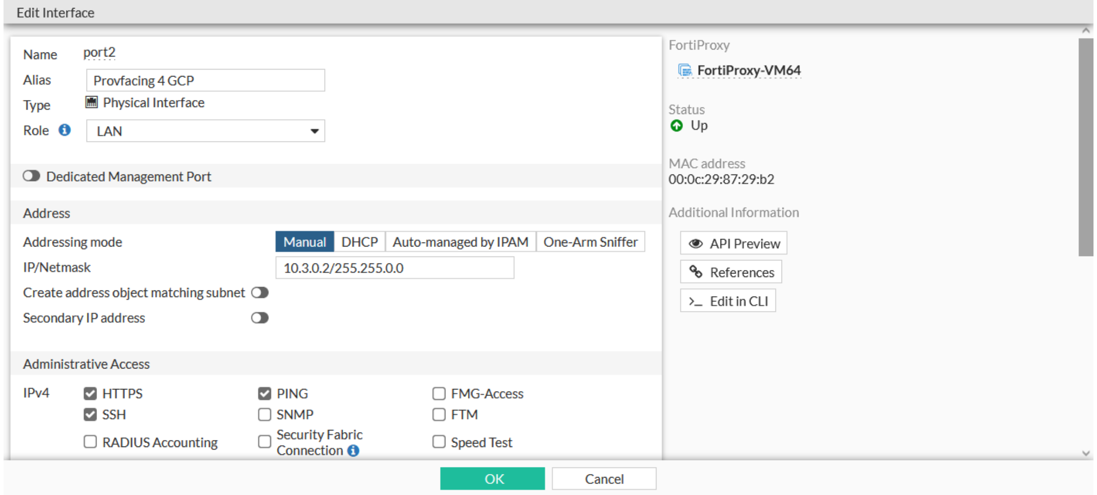
tcp:80

Configuring the second NIC on the FortiProxy-VM

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

To configure the second NIC on the FortiProxy-VM:

1. Go to *Network > Interfaces*. port2's IP address/netmask is shown as *0.0.0.0 0.0.0*.
2. Edit port2 and enter the IP address and netmask.



Edit Interface

Name port2
Alias Provfacing 4 GCP
Type Physical Interface
Role LAN

Dedicated Management Port

Address
Addressing mode: Manual | DHCP | Auto-managed by IPAM | One-Arm Sniffer
IP/Netmask 10.3.0.2/255.255.0.0
Create address object matching subnet
Secondary IP address

Administrative Access
IPv4
☑ HTTPS ☑ PING □ FMG-Access
☑ SSH □ SNMP □ FTM
□ RADIUS Accounting □ Security Fabric Connection □ Speed Test

FortiProxy
FortiProxy-VM64
Status
Up
MAC address
00:0c:29:87:29:b2
Additional Information

3. Configure the remaining settings as required, then click *OK*.

Configuring static routing in FortiProxy-VM

By default, Google Compute virtual machine (VM) instances' network configuration use single host (/32 net mask) subnets regardless of the subnet CIDR configuration. The internal IP address and routes are assigned to the VM using the dynamic host configuration protocol (DHCP), but in some cases, you may need to configure addresses and routing statically in FortiProxy. This guide describes configuring static IP addresses and routing for such requirements.

You can affect the way that subnets work on a per-VM basis during VM deployment using the `MULTI_IP_SUBNET` guest operating system feature, which is described at the end of this guide. As some Fortinet templates use this feature, confirm whether your deployment uses `MULTI_IP_SUBNET` or the standard networking scheme before continuing.

Configuring static network settings

Assigning a static internal IP address in GCP

By default, GCP assigns a VM instance an ephemeral internal IP address every time it is started. Before you configure a static IP address in FortiProxy, ensure that Google Compute will always use the same IP address.

To assign a static internal IP address in GCP:

1. Open VM instance details for the FortiProxy.
2. Click *Edit*.
3. Under *Network interfaces*, click the pencil icon to edit a desired network interface's properties.
4. From the *Internal IP type* dropdown list, select *Static*. This reserves the currently used internal IP address. This option is only available for instances that are currently running. You can assign a custom internal IP address for a stopped instance by changing its NIC properties.
5. Enter a name for the reserved internal IP address.
6. Repeat steps 3-6 for all required network interfaces.

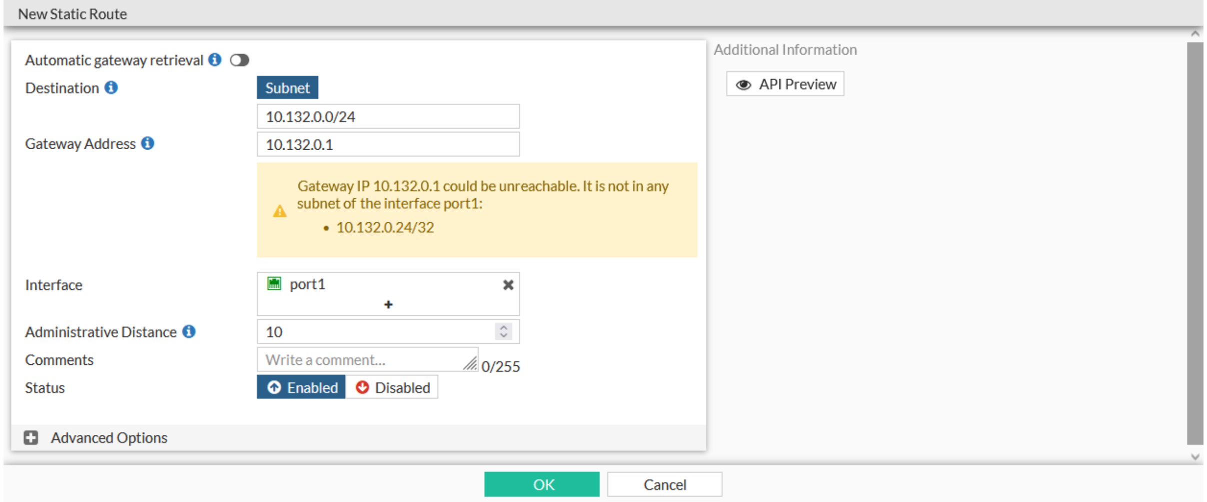
Configuring static addressing in FortiProxy

You must following the proper order of actions as documented. Changing interface settings before configuring routing results in loss of communication with the FortiProxy, which you can recover using CLI commands over a serial console.

To configure static addressing in FortiProxy:

1. Log in to the FortiProxy GUI.
2. Go to *Network* > *Static Routes*.

3. Configure a route to the first IP address in the subnet with a netmask of 255.255.255.255:
   a. Click *Create New*.
   b. In the *Destination* field, enter the required subnet.
   c. For *Gateway Address*, select *Specify* and enter *0.0.0.0*.
   d. From the *Interface* dropdown list, select the required interface.
   e. Click *OK*.
4. Configure a route to the local subnet CIDR:
   a. Click *Create New*.
   b. In the *Destination* field, enter the required subnet.
   c. For *Gateway Address*, enter the first IP address in the subnet. In this example, it is 10.132.0.1. The FortiProxy GUI displays a warning that the gateway IP address is unreachable through the interface. You can disregard this error, as the first configured route mitigates it.
   d. From the *Interface* dropdown list, select the desired interface.
   e. Click *OK*.



New Static Route

Automatic gateway retrieval

Destination: Subnet 10.132.0.0/24

Gateway Address: 10.132.0.1

Gateway IP 10.132.0.1 could be unreachable. It is not in any subnet of the interface port1:
- 10.132.0.24/32

Interface: port1

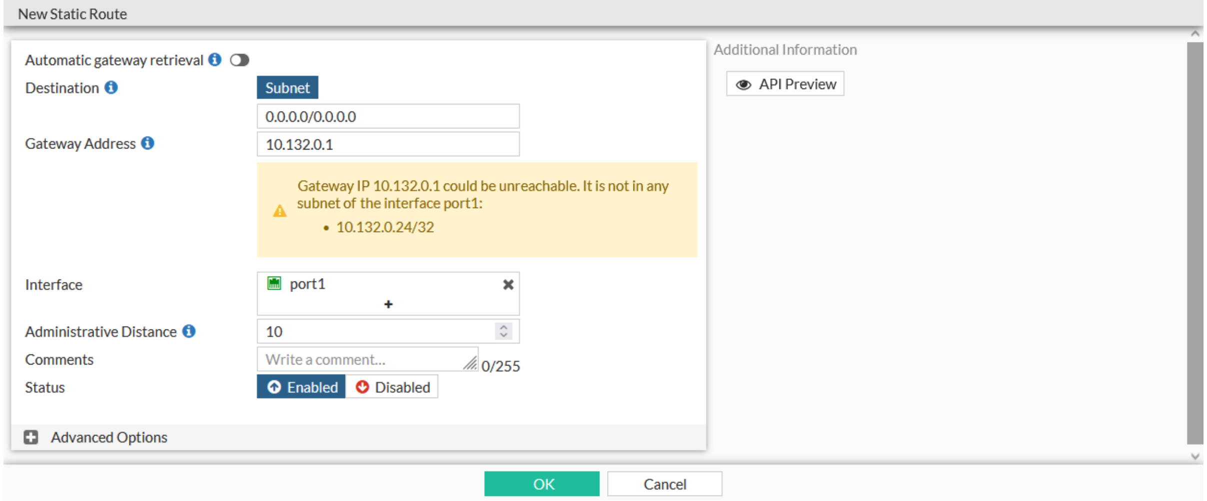
Administrative Distance: 10

Comments: Write a comment... 0/255

Status: Enabled Disabled

5. If you are configuring the port1 interface, which FortiProxy typically uses for egress traffic to the Internet, metadata service, and the Google API, you must configure a default route using gateway settings:
   a. Click *Create New*.
   b. In the *Destination* field, enter 0.0.0.0/0.0.0.0.
   c. For *Gateway Address*, enter the same IP address configured as the gateway address for the route to the local subnet CIDR. In this example, it is 10.132.0.1.
   d. From the *Interface* dropdown list, select *port1*.

   e. Click *OK*.



New Static Route

Automatic gateway retrieval ○

Destination: Subnet

0.0.0.0/0.0.0.0

Gateway Address: 10.132.0.1

⚠ Gateway IP 10.132.0.1 could be unreachable. It is not in any subnet of the interface port1:

- 10.132.0.24/32

Interface: port1

Administrative Distance: 10

Comments: Write a comment... 0/255

Status: Enabled Disabled

6. Go to *Network > Interfaces*.
7. Double-click the required interface.
8. Under *Addressing mode*, select *Manual*. FortiProxy automatically populates the proper IP address with a 255.255.255.255 netmask.
9. Click *OK*.

Load balancer routes

If your FortiProxy is accepting connections via a load balancer (LB), you must additionally configure routes to the health probes' IP ranges on each interface receiving traffic. This prevents the reverse path forwarding check from blocking the health probes. The IP ranges are different for different LB types. Google documents the ranges. For the internal LB, the ranges are 35.191.0.0/16 and 130.211.0.0/22.

The 0.0.0.0/0 route on the external interface covers the ranges that the external network LB uses.

MULTI_IP_SUBNET scheme

`MULTI_IP_SUBNET` is a guest operating system feature flag, which you can enable when creating the VM by using the command line, a deployment manager template, or Terraform. The following shows the commands:

```
gcloud compute instances create …
```

```
--guest-os-features MULTI_IP_SUBNET
```

The following shows the deployment manager template:

```
- type: compute.v1.instance
  properties:
    disks:
    - boot: true
```

```
guestOsFeatures:
- type: MULTI_IP_SUBNET
```

You can verify that the instance was created using this option by clicking Equivalent REST at the bottom of the VM Instance details page or describing the instance using gcloud commands.

The `MULTI_IP_SUBNET` scheme simplifies configuring routing in FortiProxys. It uses the subnet configuration known from on-premise networks, where the interface IP address is configured with the subnet's full netmask, instead of 255.255.255.255. Static route configuration in FortiProxy is necessary only for the CIDRs not directly connected to the firewall.

FORTINET®

www.fortinet.com