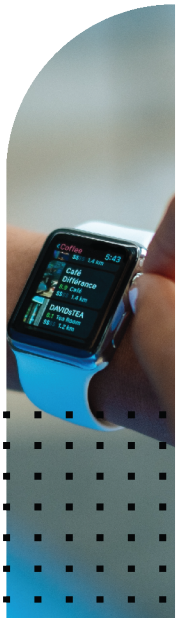
GCP Deployment Guide

FortiDeceptor 5.2.0



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

FORTINET VIDEO LIBRARY
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

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

December 8, 2023
FortiDeceptor 5.2.0 GCP Deployment Guide
00-520-809409-20231207

TABLE OF CONTENTS

Change Log

Date	Change Description
2023-03-15	Initial release.
2023-10-16	Updated Configuring FortiDeceptor Manager and GCP Client on page 19.
2023-12-04	Updated Configure client on page 20.

About FortiDeceptor VM on GCP

FortiDeceptorVM is a 64-bit virtual appliance version of FortiDeceptor. It is deployed in a virtual machine environment. Once the virtual appliance is deployed and set up, you can manage FortiDeceptor VM via its GUI in a web browser on your management computer.

This document provides information about deploying a FortiDeceptor VM in the Google Cloud Platform (GCP). This includes how to configure the virtual hardware settings of the virtual appliance. This guide presumes that the reader has a thorough understanding of virtualization servers.

This document does not cover configuration and operation of the virtual appliance after it has been successfully installedand started. For that information, see the FortiDeceptor Administration Guide in the Fortinet Document Library.

Licensing

Fortinet offers the FortiDeceptor in a stackable license model. This model allows you to expand your VM solution as your environment expands. For information on purchasing a FortiDeceptor license, contact your Fortinet Authorized Reseller, or visit https://www.fortinet.com/how_to_buy/.

When configuring your FortiDeceptor, ensure that you configure hardware settings as outlined in the following table and consider future expansion. Contact your Fortinet Authorized Reseller for more information.

Technical Specification	Details
GCP Support	e2-medium for 2 nics n1-standard-8 v2 for 6 nics
Virtual CPUs (min / max)	4/ Unlimited*
Virtual Network Interfaces	2-6
Virtual Memory (min / max)	8GB / Unlimited**
Virtual Storage (min / max)	HDD 50GB / 16TB***

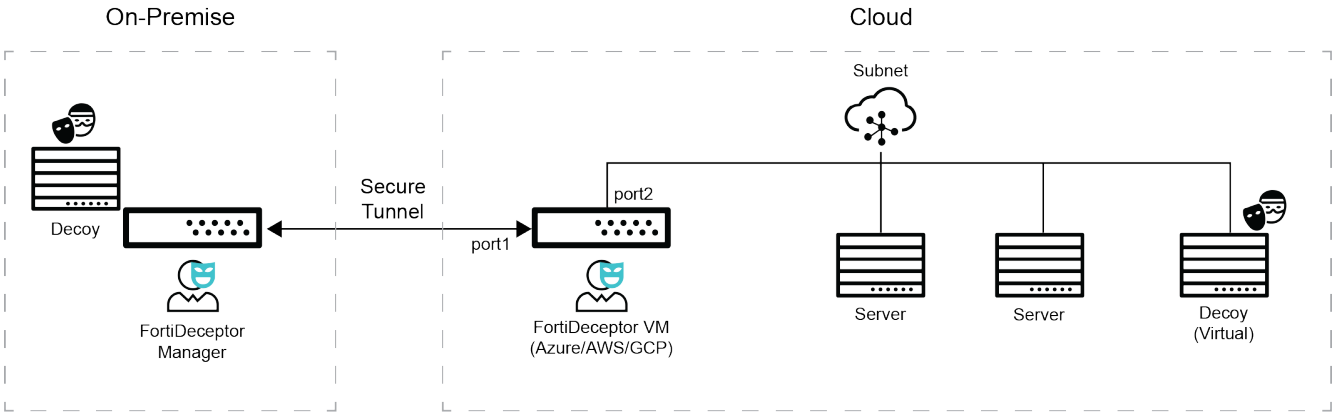
For more information, see the FortiDeceptor product data sheet available on the Fortinet web site, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiDeceptor.pdf.

After placing an order for FortiDeceptor, a license registration code is sent to the email address used in the order form. Use the license registration code provided to register the FortiDeceptor with Customer Service & Support at https://support.fortinet.com.

Upon registration, you can download the license file. You will need this file to activate your FortiDeceptor. You can configure basic network settings from the CLI to complete the deployment. Once the license file is uploaded and validated, the CLI and GUI will be fully functional.

FortiDeceptor Cloud topology

The cloud appliance is deployed over the public infrastructure but uses a different method for decoy deployment. This new method requires less HW requirements for the cloud appliance itself.



The cloud decoy deployment method is as folows:

- The cloud appliance will be deployed over the cloud infrastructure.
- An on-premise FortiDeceptor Manager will manage the cloud appliance over a propriety network tunnel.
- The propriety network tunnel allows managing the cloud appliance and decoy deployment provisioning over layer2 tunnel communication over layer3.
- The cloud appliance network interfaces will hold IP addresses in the cloud segment. Each IP address represents a network decoy.
- The network decoy will run on the on-premise FortiDeceptor Manager and use the same IP address as the cloud appliance network interfaces.
- The cloud IP address will tunnel over Layer2 to the IP address on the on-premise FortiDeceptor Manager.
- The idea is to run a light appliance in the cloud while running the actual network decoys inside the on-premise FortiDeceptor Manager in a sandbox mode. The cloud network is isolated from the rest of the decoys, the on-premise networks.

While the cloud appliance uses different hardware requirements, the on-premise FortiDeceptor Manager HW requirements that should serve the cloud appliance decoys is the same concept as today.

Deploying FortiDeceptor on GCP

To deploy FortiDeceptor on Google the Cloud Platform, first you will create and upload a FortiDeceptor image file. Next you will create a VPC network and subnets, and then configure a firewall policy to access FortiDeceptor. Lastly, you will create a FortiDeceptor instance and add it to a new deployment network.

To deploy FortiDeceptor on Google Cloud Platform:

1. Prepare the FortiDeceptor image.
2. Create a bucket and upload the image file.
3. Create an image with the image file.
4. Create VPC networks.
5. Create firewall policies.
6. Create a FortiDeceptor instance.
7. Check the FortiDeceptor output.

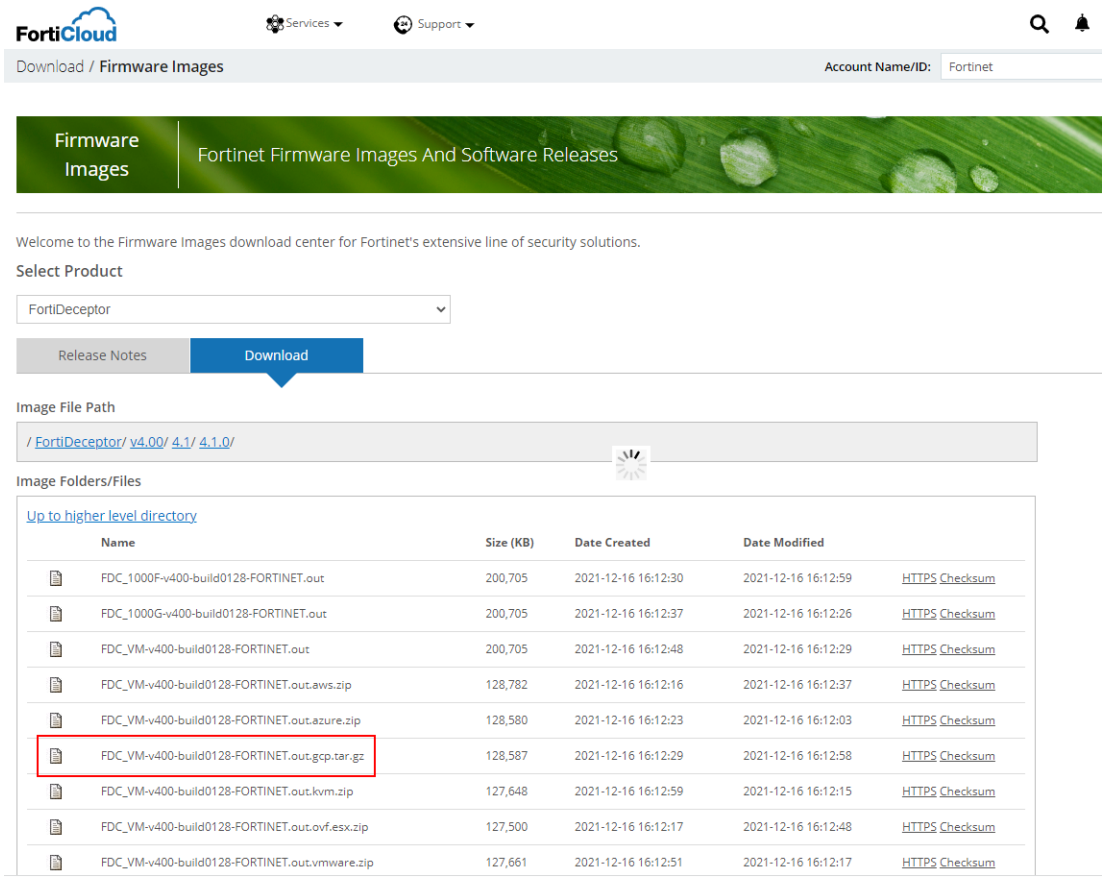
Prepare the FortiDeceptor image for GCP

Download the image archive file for Google Cloud Platform from FortiCloud.

To download the FortiDeceptor image:

1. Log in to FortiCloud.
2. In the banner, click *Support* > *Downloads* > *Firmware Download*. The *Download/Firmware Images* page opens.
3. From the *Select Product* dropdown, click *FortiDeceptor*.
4. Click the *Download* tab.
5. In the *Image File Path* section, click the image folder until you reach the image page.

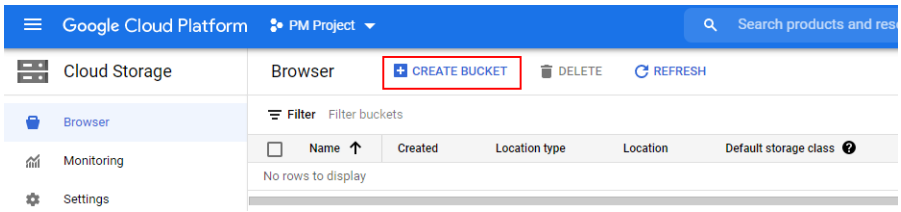
6. Click *FDC_VM-vx.x.x-buildxxxx-FORTINET.out.gcp.tar.gz* to save the file to your device.



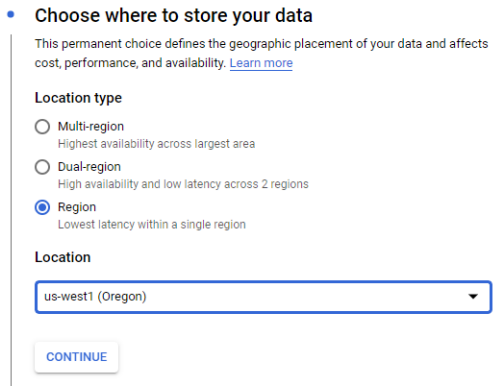
Create a bucket and upload the image file

To create a bucket and upload the image file:

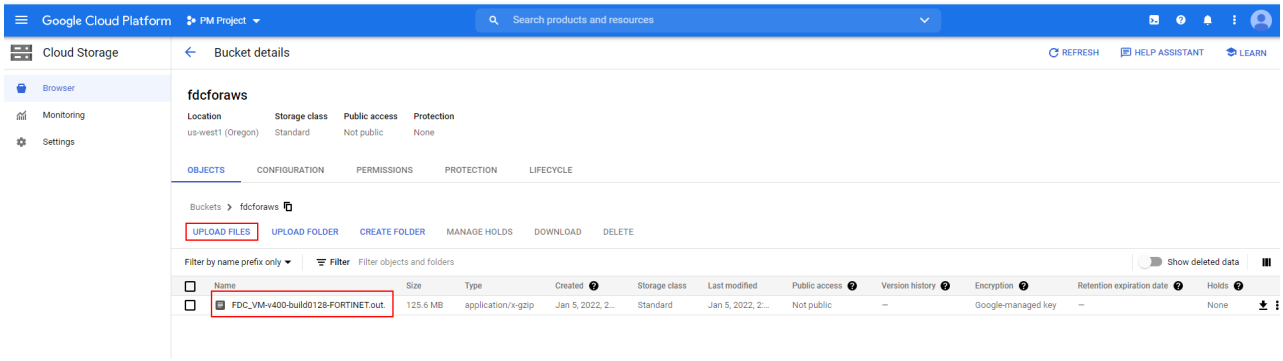
1. Log in to your Google Cloud account.
2. Go to *Storage* > *Cloud Storage* and click *Create bucket*. The *Create Bucket* page opens.



3. In the *Name your bucket* field, enter a name for the bucket.
4. Click *Choose where to store your data*. Under *Location type*, click *Region* and select an option from the *Location* dropdown.



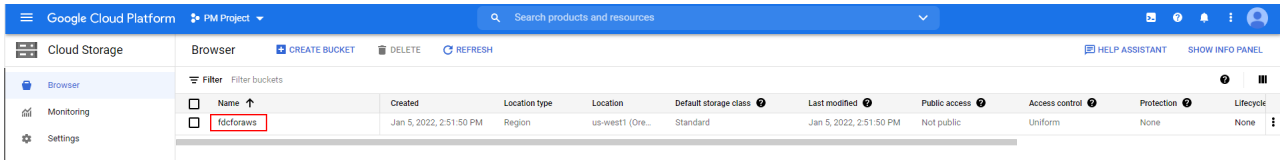
5. Click *Create*. The *Bucket Details* window opens.
6. In the *Objects* tab, click *Upload Files* and upload the image file you downloaded from FortiCloud. See Prepare the FortiDeceptor image for GCP on page 7.



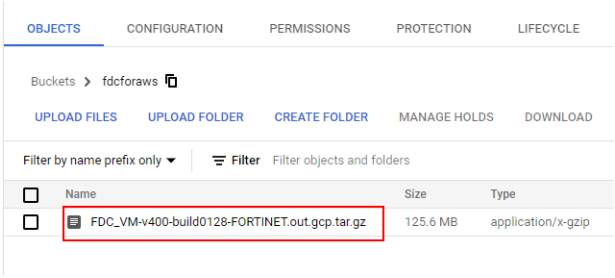
Create an image with the image file

To create an image with an image file:

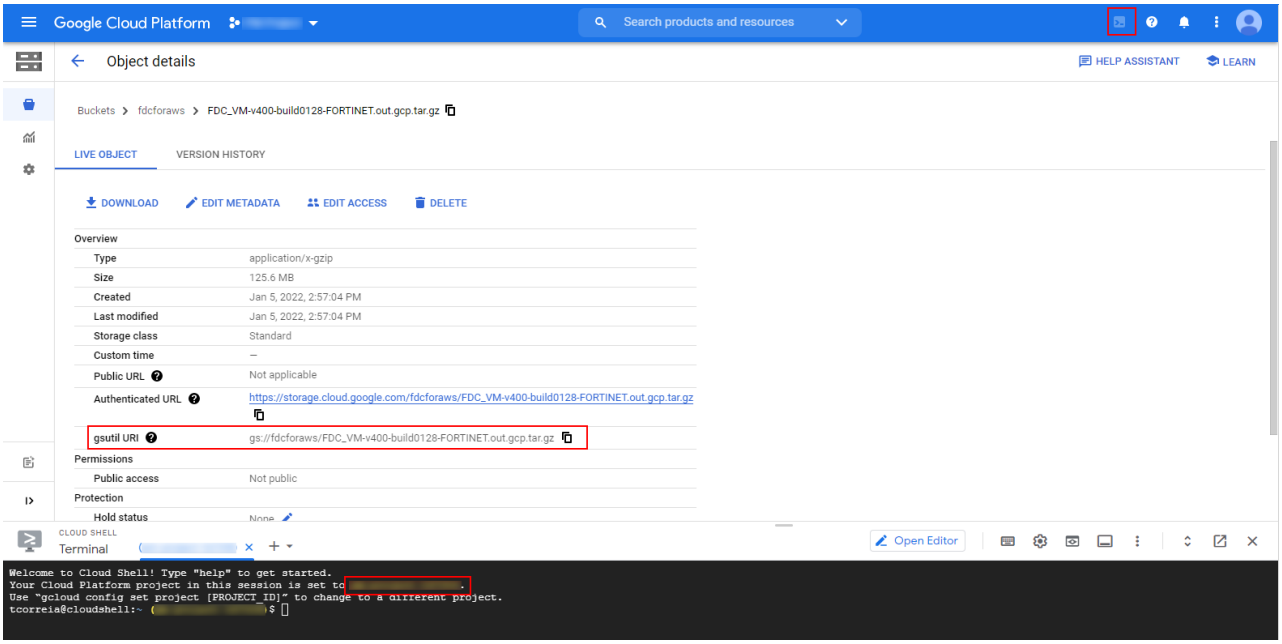
1. In the Google Cloud platform, go to *storage* > *Cloud Storage* > *Browser*.
2. Open the bucket you created. See, Create a bucket and upload the image file on page 8.



3. Click the *xxx.gcp.tar.gz* image you uploaded to the bucket. The *Object details* page opens.

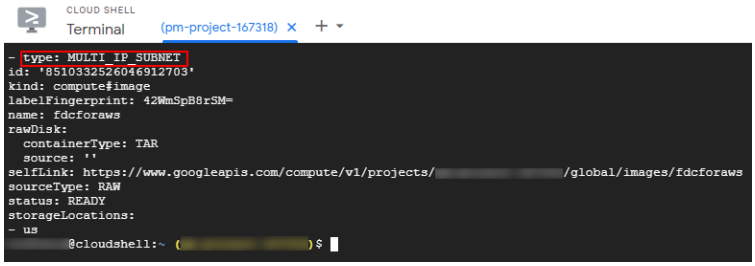


4. Click the *Activate Cloud Shell* icon to prepare the image.
   a. Click to copy the gsutil URI.
   b. Ensure `Your Cloud Platform project in this sessions is set to` the correct project.



5. To prepare the image, run the following command:
   `gcloud compute images create <image_name> --source-uri <gsutil_URI> --guest-os-features MULTI_IP_SUBNET`
   - `<image_name>` is the name of the new image.
   - `<gsutil_URI>` is the *gsutil URI* you copied in the previous step.

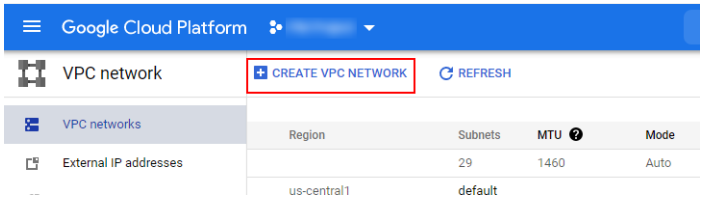
6. To verify the image is ready, run the following command:
   `gcloud compute images describe <image_name>`
   Ensure the image `type` supports `MULTI_IP_SUBNET`.



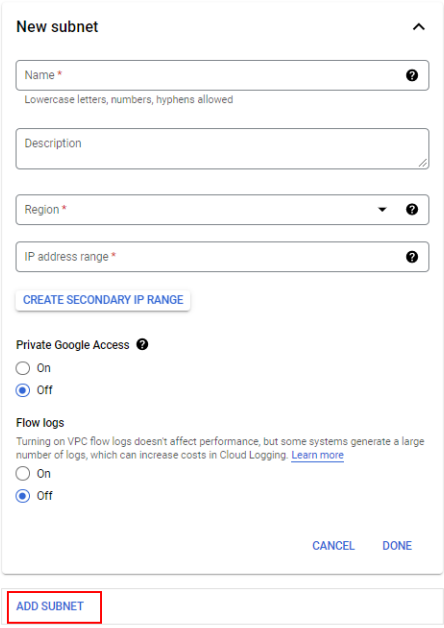
Create VPC networks

To create a new VPC network:

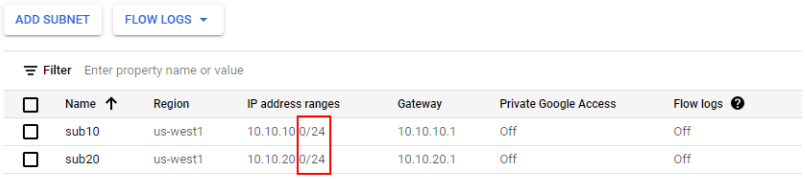
1. In Google Cloud, go to *VPC network* > *VPC networks*.
2. In the banner, click *Create VPC Network*. The *VPC network details* page opens.



3. Create several subnets in the VPC for FortiDeceptor management and deployment.
   - You may need to deploy decoys on some FortiDeceptor ports.
   - Ensure the ports are in the same subnet with the endpoints.



4. After the VPC is created, open it to verify the netmask in the *IP address ranges* column is correct.



Create a firewall policy

To access FortiDeceptor, you need to enable HTTPS (port 443) in a firewall. To manage the FortiDeceptor cloud appliances, you need to enable port 8443.

To set up lure services with decoys, enable the relevant ports between the endpoints and the FortiDeceptor ports.

Example:

To enable SSH service on a decoy, create a firewall to enable port 22 in the subnet and attach this firewall to both the endpoint and the FortiDeceptor port.

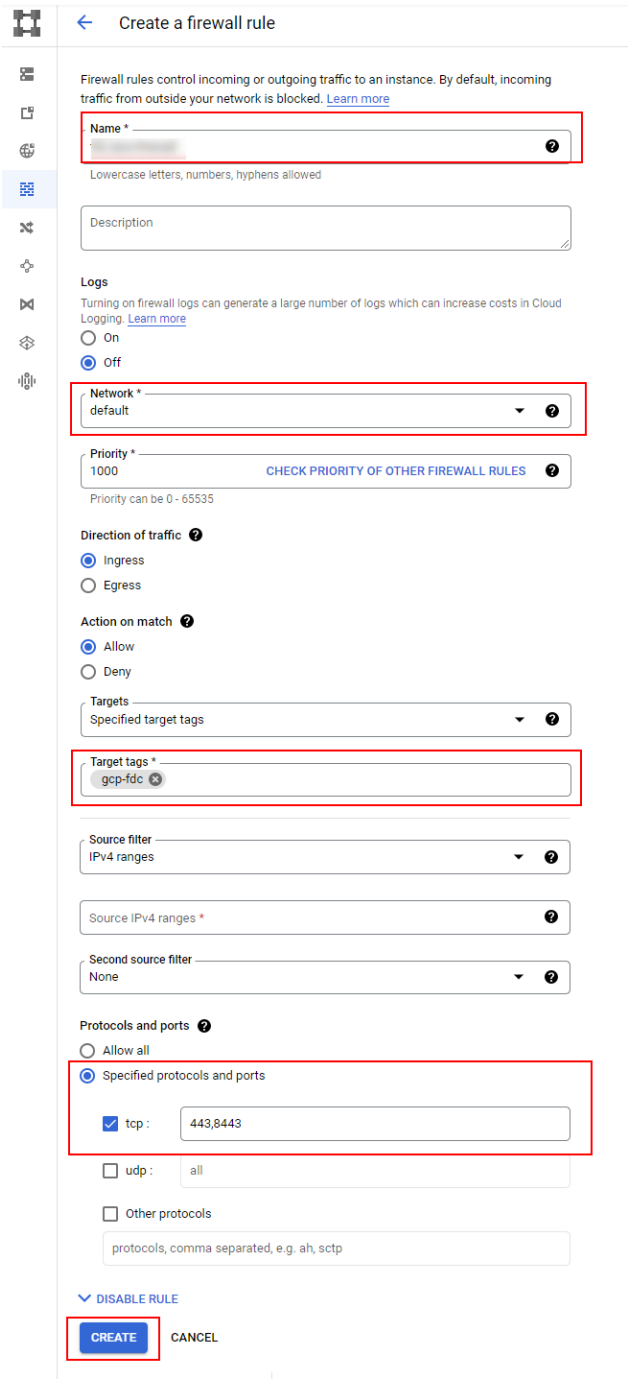
You will use target tags to create the FortiDeceptor instance and attach it to the network. When this is complete, the newly created firewall will go into effect.

To create a firewall policy in Google Cloud:

1. Go to *VPC Network* > *Firewall*.
2. In the toolbar, click *Create Firewall Rule*. The *Create a firewall rule* page opens.

3. Configure the following settings and then click *Create*.

Name	Enter a name for the firewall rule.
Network	Set to *default*.
Target Tags	Enter a new tag, for example *gcp-fdc*.
Protocols and ports	1. Enable *Specified protocols and ports*. 2. Select *tcp* and enter the port number. • To enable for HTTPS enter 443. • To manage the cloud 8443.



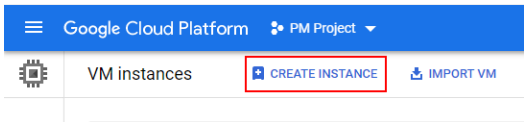
Create a FortiDeceptor instance

Use the prepared image as the boot disk to create cloud FortiDeceptor and configure the interfaces.

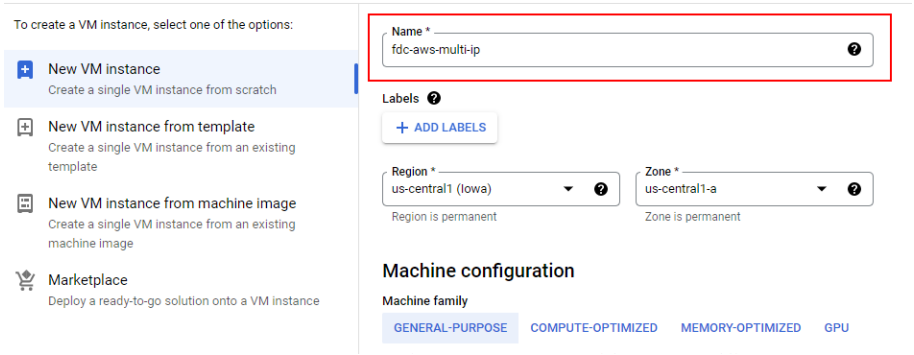
Creating a VM instance

To create a VM instance in Google Cloud:

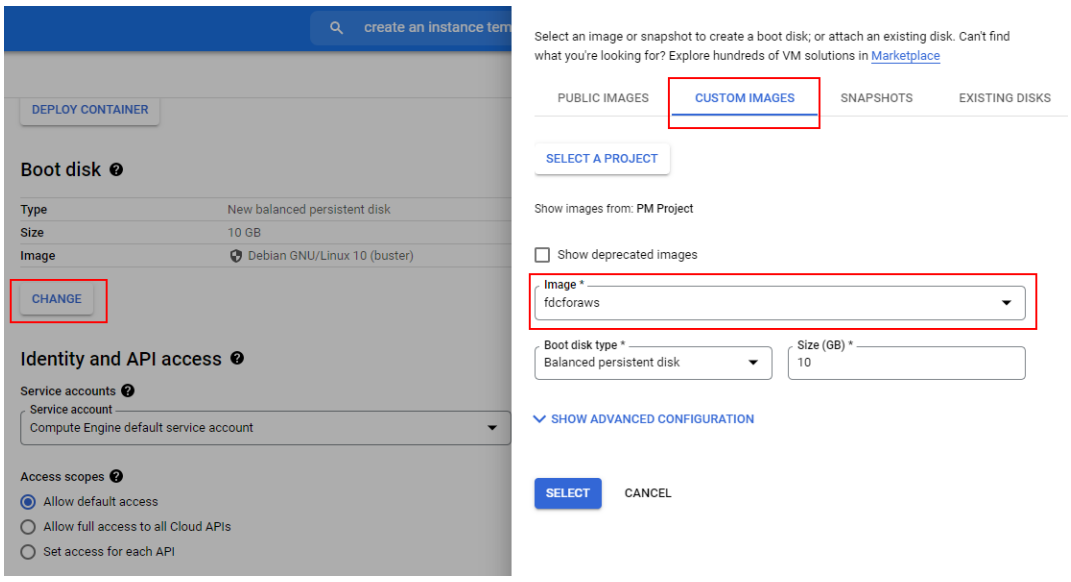
1. In the Google Cloud, go to *Virtual Machines* > *VM Instances*.
2. In the toolbar, click *Create Instance*. The *Create an instance* page opens.



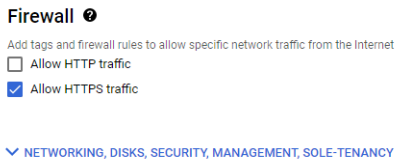
3. Enter a name for the instance.



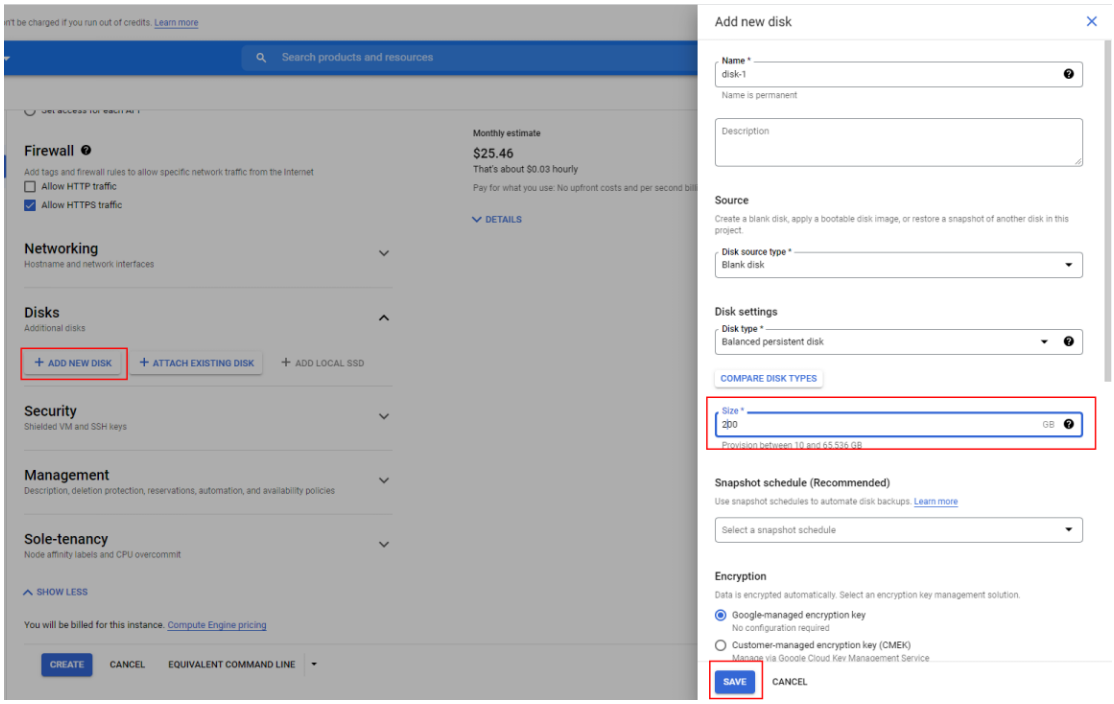
4. Change the boot disk.
   a. Scroll down to the *Book disk* section, and click the *Change* button. The *Book disk* pane opens.
   b. Click the *Custom Images* tab.
   c. Click *Select a Project* and select the image you prepared in the Google Cloud console. See Create an image with the image file on page 9.
   d. Click *Select*.



5. Scroll down to *Firewall*, select *All HTTPS* traffic.



6. Click *Networking, Disks, Management, Sole-Tenancy* and add a new disk and set up the network.
   a. Under *Disks*, click *Add New Disk*. The *Add New Disk* pane opens.
   b. From the *Size* dropdown, set the size to *50GB* or more and click *Save*.



7. Add the interfaces.

Adding a deployment network

You must configure a minimum of two ports and maximum of six ports. You will also add some secondary IPs to the ports. Later, when you deploy decoys, you will assign these IPs to the decoys.

The number of virtual network interfaces scales with the number of vCPUs with a minimum of two and a maximum of eight.

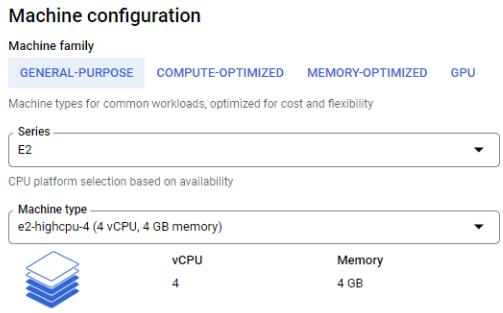
Use the following table to determine how many network interfaces can be attached to an instance:

Number of vCPU	Number of vNICs
2 or less	2
2 to 8	2 to 8
8 or more	8

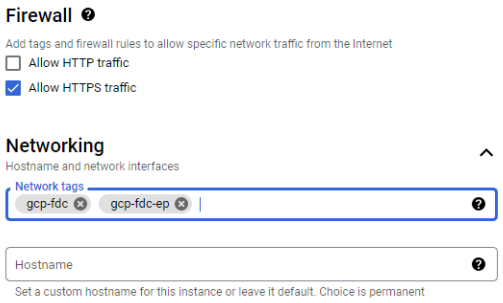
For more information, see Creating instances with multiple network interfaces.

To add a deployment network:

1. Select a machine type based on how many networks you need to deploy.
   a. Go to the *Create an instance* page in the Google Cloud console.
   b. Click *New VM instance* and enter a name for the instance.
   c. In the *Machine configuration* area, click the *Machine type* dropdown and select the machine type.



2. Configure the firewalls with networks.
   a. In the *Firewall* section, select *Allow HTTPS traffic*. This allows you to access FortiDeceptor with a web browser.
   b. Click *Networking, Disks, Management, Sole-Tenancy*
   c. In the *Networking* section, in the *Network tags* area, enter the network tags.
      - A firewall in the default network attaches to tag (such as *gcp-fdc*) opens 8443 on port1.
      - A firewall attached to tag (such as *gcp-fdc-ep*) opens all ports between port2/3/4/5/6 and the endpoints.



For more information about firewalls and networks, see Create VPC networks on page 11 and Create a firewall policy on page 12.

The firewall *fcp-fdc-ep*" should be crated in the same VPC of each FortiDeceptor port.

---

3. In the *Network Interfaces* area, click *Add Network Interface*, make the following configurations:

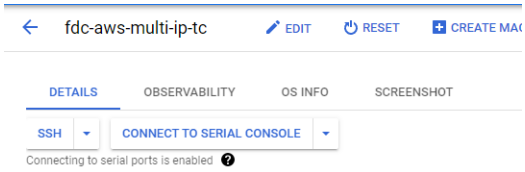
Network	Select the VPC you created for port2
Subnetwork	Select the proper subnet within the VPC region.
Subnet range	Enter the secondary IPs.
External IP	None

4. Click *Create*.

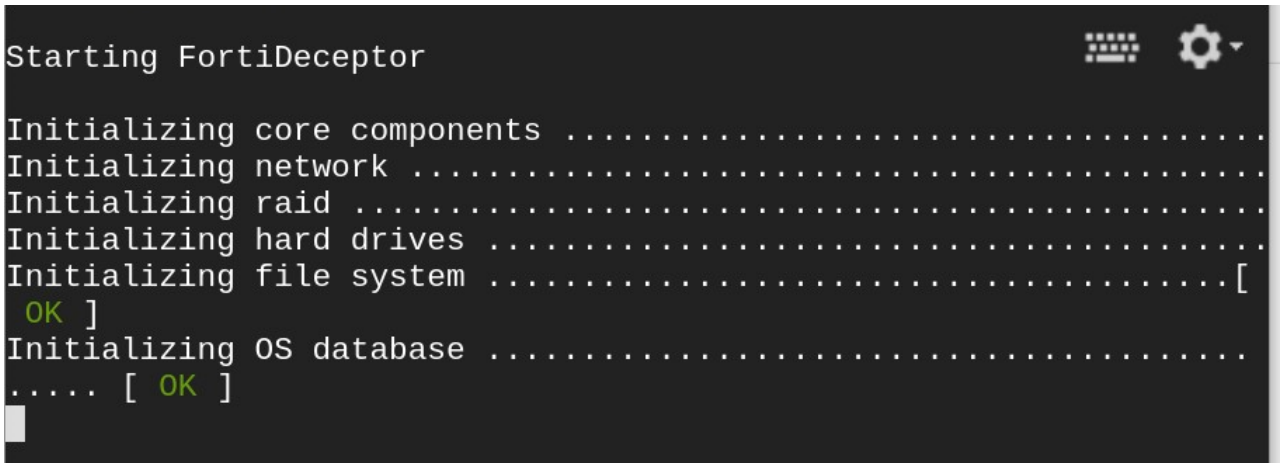
Check the FortiDeceptor output

To check the VM image output:

1. In the Google Cloud Console, go to the *VM instances* page.
2. Click the instance you want to connect to.
3. Under *Remote Access*, select *SSH* and click *Connect to Serial Console*.



The response should look like this:



The FortiDeceptor on Google Cloud Platform can automatically get the port1 IP, which is assigned by Google Cloud network. The license should be generated based on this IP.

Configuring FortiDeceptor Manager and GCP Client

After FortiDeceptor is deployed, get the appliance authorization key and configure FortiDeceptor Manager. After FortiDeceptor is configured, you can deploy the decoys and endpoints.

We recommend setting up a security policy and trusted host to ensure the FortiDeceptor is running in a safe environment.

To configure FortiDeceptor:

1. Get the authentication key.
2. Configure client on page 20.
3. Configure FortiDeceptor manager.
4. Deploy the decoys.
5. Deploy the endpoints.

Get the authentication key

Access the GCP client via the public IP to upload a valid license and get the authentication key for deployment.

To get the authentication key:

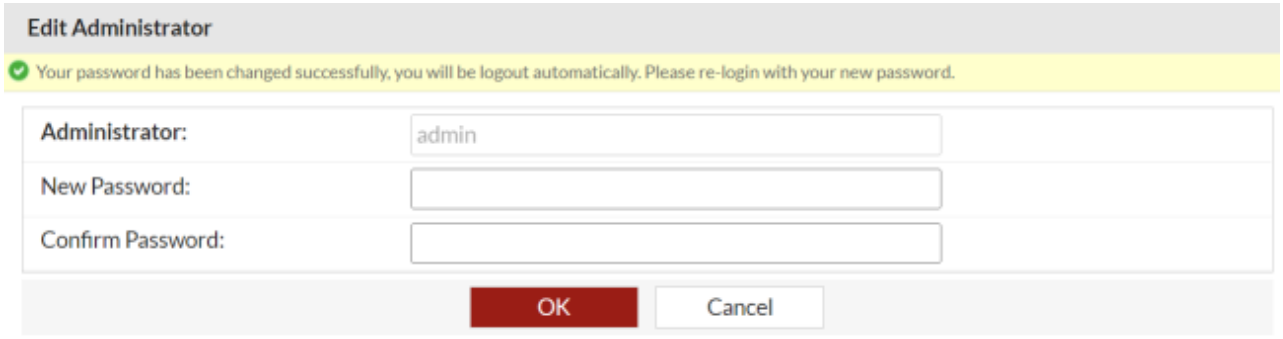
1. Log in to the GCP client via the public IP.
2. Upload the FortiDeceptor license.
   a. Go to *Dashboard* > *System Information* widget.
   b. In the *Firmware License* field, click *Upload License*.
3. Change the password.
   a. In the top-right of the page, click the Account menu (*Admin*), then click *Change Password*.
   b. Complete the fields In the *Edit Administrator* page and click *OK*.
4. Get the authorization key.
   a. Go to *Dashboard* > *System Information* widget.
   b. In the *Appliance Auth Key* field and record authorization key.

Alternatively, you can get the authorization key with the CLI command `cm -p`.

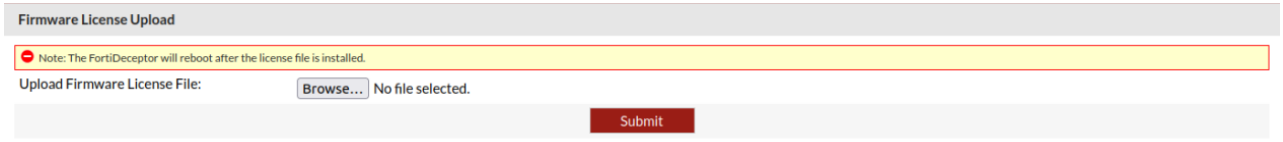
Configure client

To configure the GCP client:

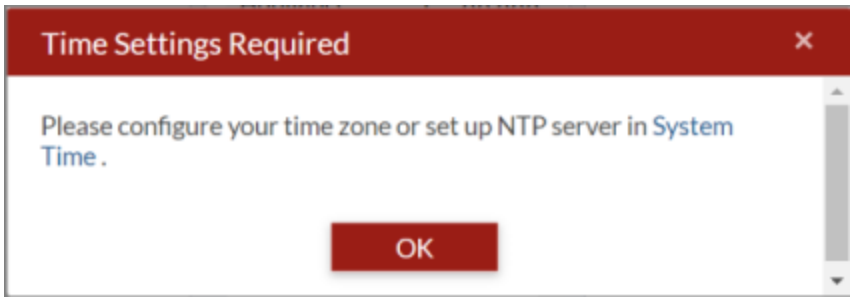
1. Log in to the Azure client with the public IP address. By default, the *admin* user account has no password.
2. After the instance reboots, you are prompted to change the password and log in again.



3. After logging in, the FortiDeceptor instance prompts you to upload the license file. Click *Choose File* to navigate to the file and click *Submit*. After the file submitted, FortiDeceptor will reboot.

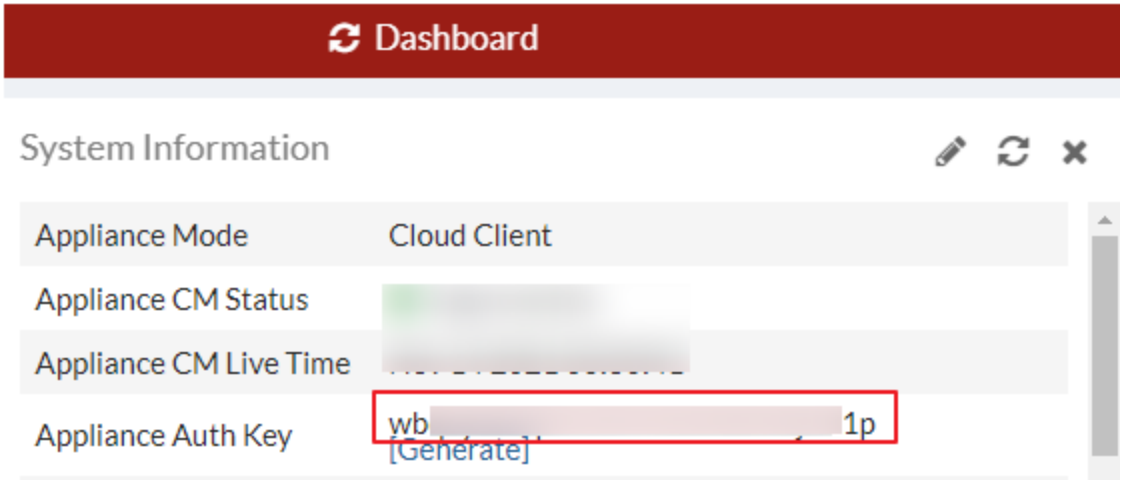


4. After you log in, you are prompted to configure the timezone and time.

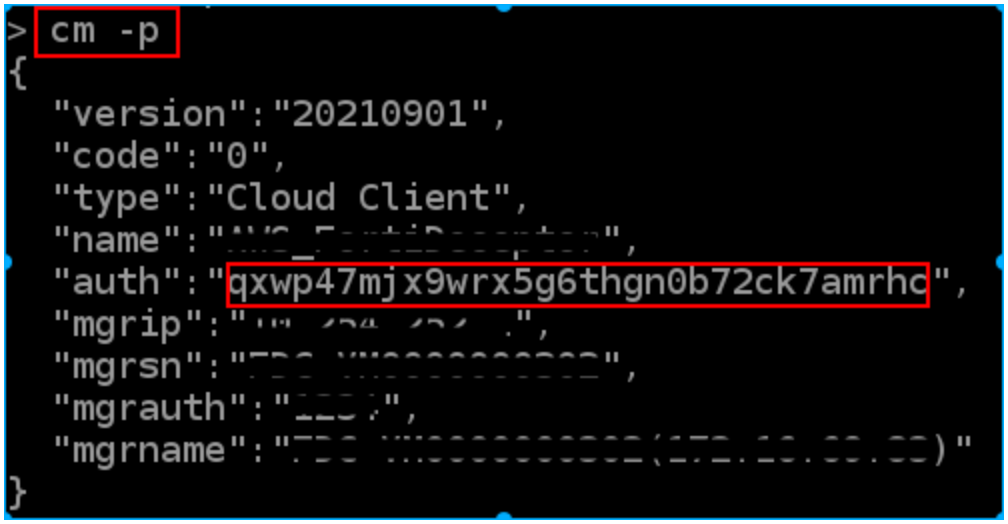


5. In the banner, click your username and select *Change Password*, then change the password.
6. Change the Host Name.
   a. Go to *Dashboard* > *System information* > *Host Name* and click *Change*. The *Edit Host Name* field opens.
   b. In the *New Name* field, enter a the new Host Name.

7. Get the appliance key with the GUI or CLI.
   - GUI: Go to *Dashboard* > *System Information* widget and locate the *Appliance Auth Key*.



   - CLI: `cm -p`



Configure FortiDeceptor Manager

Use the authorizing key you generated in the previous section to add GCP FortiDeceptor as a cloud appliance. After the appliance is added, configure the deployment network.

Adding and deleting a cloud appliances

To add the GCP FortiDeceptor as a cloud appliance:

1. In FortiDeceptor, go to *Central Management* > *Appliances*.
2. Click *Add Cloud Appliance*. The *Add Cloud Appliance* dialog opens.

3. Configure the following settings:

Appliance IP	Enter the cloud client's public IP address.
Auth Key	Enter Appliance Authorization Key. See, Get the authentication key on page 19.

4. Click *Test*. You should see the message, *Successfully communicated with the cloud appliance*.
5. Click *Add* to add this cloud appliance.

Delete the previous client and add the client with new public IP once the public IP is changed.

To delete a cloud appliances:

1. Go to *Central Management* > *Appliances*.
2. In the *Action* column, click the *Trash* icon.

Configuring the deployment network

To configure the deployment network:

1. Go to *Deception* > *Deployment Network*.
2. Click *Add New Vlan/Subnet*. The *Add New Vlan/Subnet* dialog opens.
3. Configure the network settings and click *Save*.

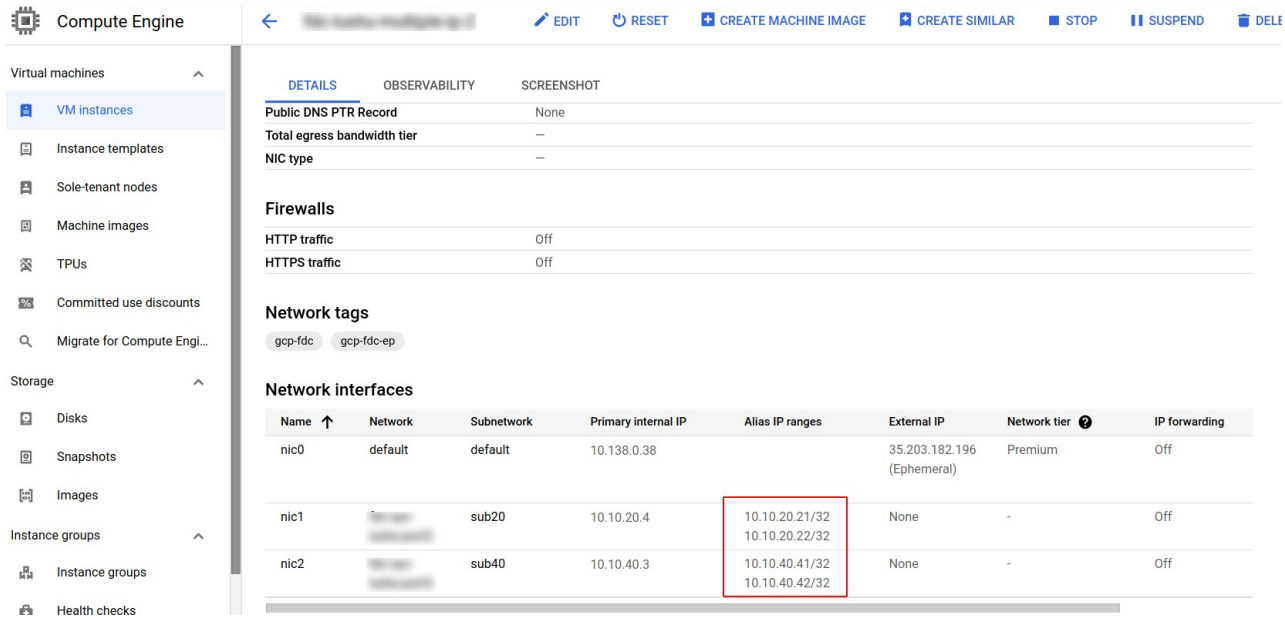
Deploy decoys

To deploy the decoys:

1. In the GCP Cloud FortiDeceptor, get the MAC address of the cloud FortiDeceptor ports with the CLI command `show`.

```
> show
Configured parameters:
        Port 1  IPv4 IP: 10.138.0.38/20         MAC: 42:01:0A:8A:00:26
        Port 2  IPv4 IP: 192.168.1.99/24        MAC: 42:01:0A:0A:14:04
        Port 3  IPv4 IP: 192.168.2.99/24        MAC: 42:01:0A:0A:28:03
        IPv4 Default Gateway: 10.138.0.1
>
```

2. In Google Cloud Console go to *Virtual Machines* > *VM Instances* and select the VM. In the *Details* tab, under *Network Interfaces*, record the IPs in the *Alias IP ranges* column. See, Create a FortiDeceptor instance on page 14.

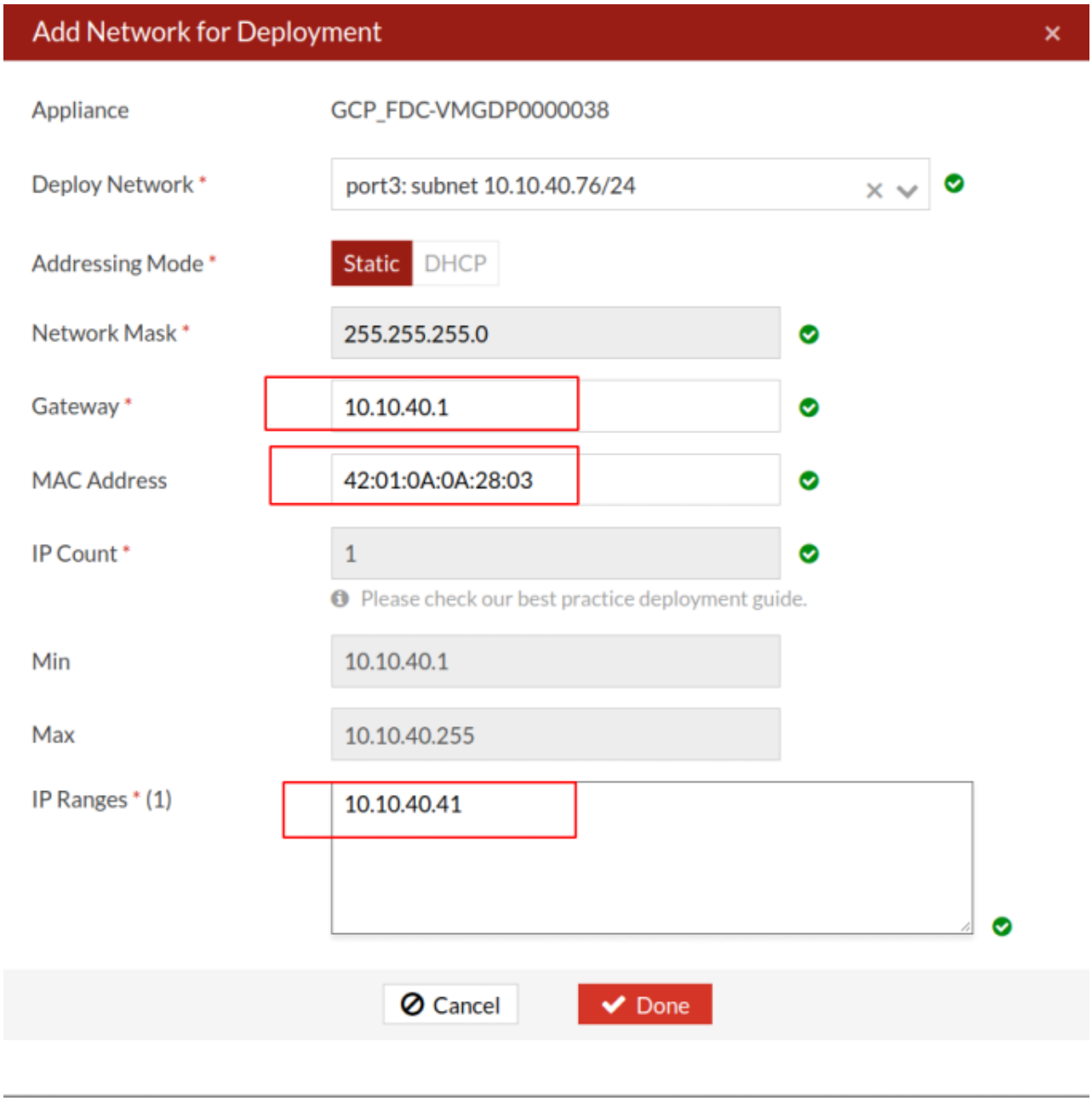


3. Set up the decoy networks.
4. Click *Done*.

To set up the decoy networks in FortiDeceptor:

1. Go to *Deception* > *Deployment Wizard*.
2. Complete Step 1 *Template* and step 2 *Configuration*. For more information, see Deploy Decoy VMs with the Deployment Wizard.
   - Enter the Gateway address from the Vlan you created when you configured the deployment network. See, Configure FortiDeceptor Manager on page 21.

- Enter the MAC address you copied in Step 1 of To deploy the decoys: on page 22



Deploy endpoints

To deploy the endpoints:

1. In the Google Cloud Console, go to the *VM instances* page.
2. Open the FortiDeceptor instance.

3. Under network interfaces, configure the endpoints so they are on the subnets as FortiDeceptor.
4. Attack the decoys through the endpoints.

www.fortinet.com