IBM Cloud Administration Guide

FortiOS 8.0

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

April 21, 2026
FortiOS 8.0 IBM Cloud Administration Guide
01-80-1054274-20260421

TABLE OF CONTENTS

About FortiGate for IBM Cloud

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 IBM Cloud.

In addition to advanced features such as an extreme threat database, vulnerability management, and flow-based inspection, features including application control, firewall, antivirus, IPS, web filter, and VPN work in concert to identify and mitigate the latest complex security threats.

Highlights of FortiGate for IBM Cloud include the following:

- Delivers complete content and network protection by combining stateful inspection with a comprehensive suite of powerful security features.
- IPS technology protects against current and emerging network-level threats. In addition to signature-based threat detection, IPS performs anomaly-based detection, which alerts users to any traffic that matches attack behavior profiles.
- Docker application control signatures protect your container environments from newly emerged security threats. See FortiGate-VM on a Docker Environment.

> ⚠ When deploying Fortinet products on a cloud platform, it is critical to understand that you are responsible for all costs incurred from the resources you use. This includes but is not limited to the following: CPU, memory, storage volumes, snapshots, data transfers, and network bandwidth.
>
> Once your deployment is live, services may automatically generate temporary files, system logs, or additional volumes and snapshots. These can consume disk space and lead to unexpected charges.
>
> To avoid surprise costs, it is your responsibility to do the following:
>
> - Regularly check which services and features are active in your cloud environment.
> - Monitor disk usage and be aware of what triggers new volume or snapshot creation.
> - Set appropriate usage limits, quotas, and budget alerts.
> - Configure disk space threshold alarms and act promptly when notified.
> - Each cloud provider has different tools for managing and monitoring these settings. Refer to IBM Cloud documentation to configure alerts, budgets, and usage controls appropriately.

Instance type support

You can deploy FortiGate-VM on IBM Cloud for Gen1 and Gen2 spaces by importing the FortiGate-VM deployment file as a custom image to your object storage bucket and creating an instance from it. A minimum 2 GB of RAM is required.

Having at least 4 GB of RAM for proper FortiGate-VM operation is recommended, especially if unified threat management, zero trust network access, or proxy is enabled.

There is no specific preference on supported instance types.

Supported instances on IBM Cloud for new deployments may change without notice.

Region support

FortiGate-VM is available for purchase in all the regions or datacenters that IBM Cloud covers.

Models

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

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-VM16/016v/016s	1	16
FG-VM32/032v/032s	1	32
FG-VMUL/ULv/ULs	1	Unlimited

With the changes in the FortiGuard extended IPS database introduced in FortiOS 7.4.0, some workloads that depend on the extended IPS database must have the underlying VM resized to 8 vCPU or more to continue using the extended IPS database.

See Support full extended IPS database for FortiGate VMs with eight cores or more.

For information about changing the instance type on an existing VM, see How to change the instance type of your On Demand instances.

For more information about IBM Compute instances, see Compute.

The v-series and s-series do not support virtual domains (VDOMs) by default. To add VDOMs, you must separately purchase perpetual VDOM addition licenses. You can add and stack VDOMs up to the maximum supported number after initial deployment.

Any RAM size with certain CPU models are allowed. Licenses are based on the number of CPUs only.

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

Licensing

You must have a license to deploy FortiGate for IBM Cloud.

Order types

On general public clouds, there are usually two order types: bring your own license (BYOL) and on-demand.

FortiGate-VM deployable on IBM Cloud supports only BYOL.

BYOL offers perpetual (normal series and v-series) and annual subscription (s-series) licensing as opposed to on-demand, which is a term-based subscription available with marketplace-listed products. BYOL licenses are available for purchase from resellers or your distributors, and the publicly available price list, which Fortinet updates quarterly, lists prices. 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.

In both BYOL and on-demand, 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 the FortiGate-VM).

For BYOL, you typically order a combination of products and services including support entitlement. S-series SKUs contain the VM base and service bundle entitlements for easier ordering.

Creating a support account

FortiGate for IBM Cloud supports only the bring your own license (BYOL) licensing model. See Order types on page 6.

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

First, if you do not have a Fortinet account, you can create one.

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. If you do not have a partner, contact your nearest Fortinet sales office for assistance in purchasing a license.

After you purchase a license or obtain an evaluation license, you receive a PDF with an activation code.

FortiOS 7.2.1 introduces a new permanent trial license, which requires a FortiCare account. This trial license has limited features and capacity. The trial license only applies to BYOL deployments for FortiGate-VM on IBM Cloud. See VM license for details.

FortiOS 7.2.0 supports the older evaluation license, which has a 15-day term.

To register the BYOL license:

1. Go to Fortinet 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. In the *Specify Registration Code field*, enter your license activation code and select *Next* to continue registering the product. Enter your details in the other fields.
3. 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

Deploying FortiGate-VM on IBM Cloud

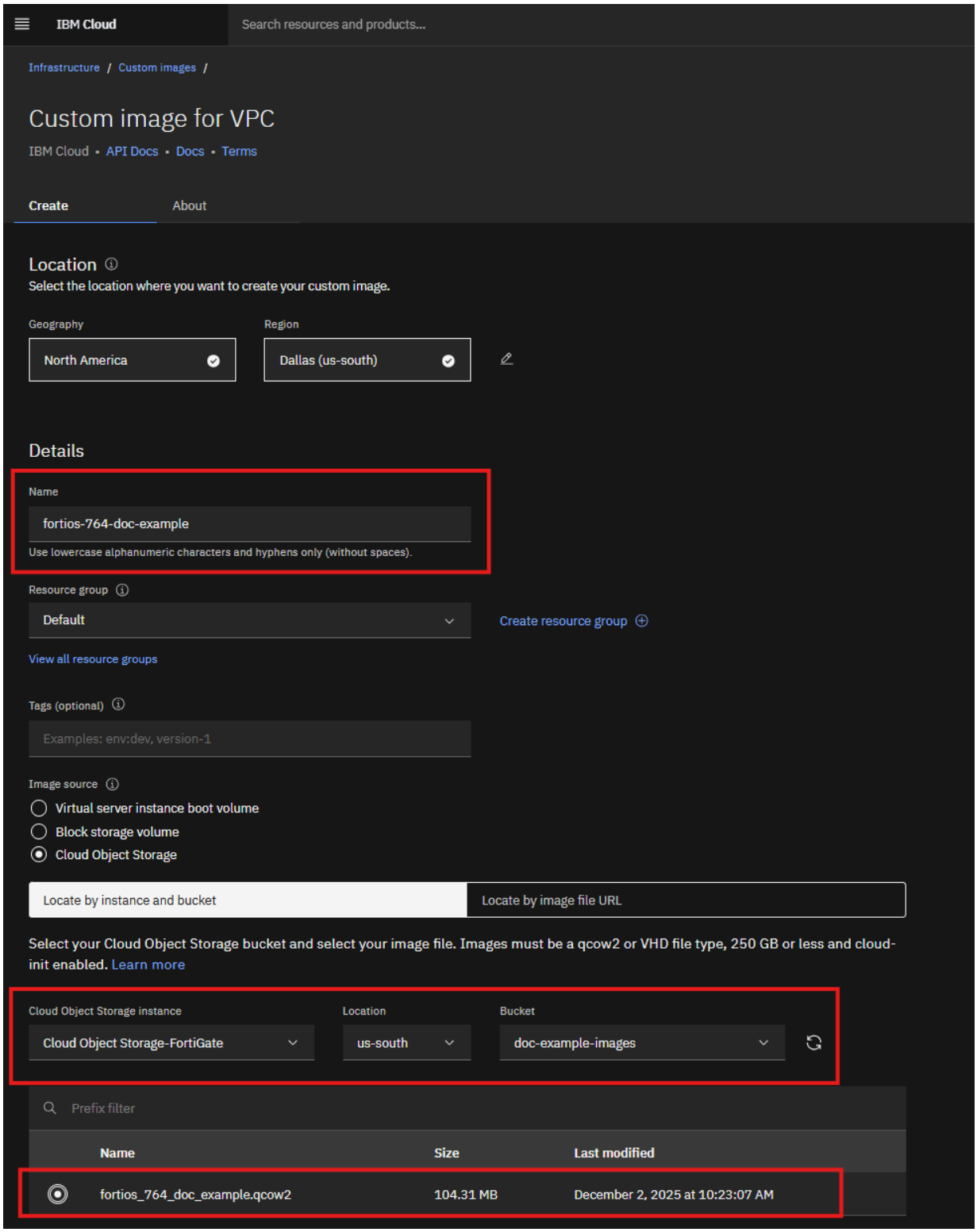
The following topics provide overviews of deploying FortiGate-VM bring your own license (BYOL) for IBM Cloud:

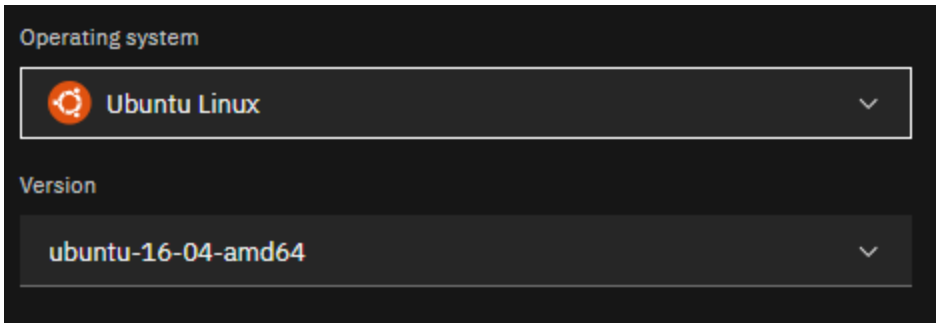
IBM Cloud Console VPC Gen2

FortiOS supports deploying FortiGate-VM bring your own license (BYOL) for IBM Cloud. IBM Cloud users can purchase and deploy FortiGate-VMs. The following describes the steps that you take to create and access a FortiGate-VM BYOL instance in IBM Cloud.

To deploy FortiGate-VM on IBM Cloud using the GUI:

1. Obtain the .qcow2 image file:
   a. Log in to the Fortinet Support site.
   b. Go to *Support* > *Downloads* > *Firmware Download*.
   c. On the *Download* tab, go to *v7.00* > *8.0*, then to the latest 8.0 patch.
   d. Download the FortiGate-VM deployment file (FGT_VM64_IBM-v8.0.X.X-buildXXXX-FORTINET.out.kvm.zip).
   e. Extract the zip file to get a .qcow2 file.
2. Log in to the IBM Cloud portal.
3. Prepare an object storage bucket on the IBM Cloud VPC.
4. Upload the .qcow2 image file.
5. Import the custom image:
   a. Go to *VPC Infrastructure (Gen 2)* > *Compute* > *Custom images*.
   b. Click *Import custom image*.
   c. Import the custom image. You must enter a name and select a region. Select the .qcow2 image file uploaded earlier, and select Ubuntu 16.04 for the operating system.


IBM Cloud
Search resources and products...
Infrastructure / Custom images /
Custom image for VPC
IBM Cloud • API Docs • Docs • Terms
Create
About
Location
Select the location where you want to create your custom image.
Geography
North America
Region
Dallas (us-south)
Details
Name
fortios-764-doc-example
Use lowercase alphanumeric characters and hyphens only (without spaces).
Resource group
Default
Create resource group
View all resource groups
Tags (optional)
Examples: env:dev, version-1
Image source
Virtual server instance boot volume
Block storage volume
Cloud Object Storage
Locate by instance and bucket
Locate by image file URL
Select your Cloud Object Storage bucket and select your image file. Images must be a qcow2 or VHD file type, 250 GB or less and cloud-init enabled. Learn more
Cloud Object Storage instance
Cloud Object Storage-FortiGate
Location
us-south
Bucket
doc-example-images
Prefix filter
Name
Size
Last modified
fortios_764_doc_example.qcow2
104.31 MB
December 2, 2025 at 10:23:07 AM

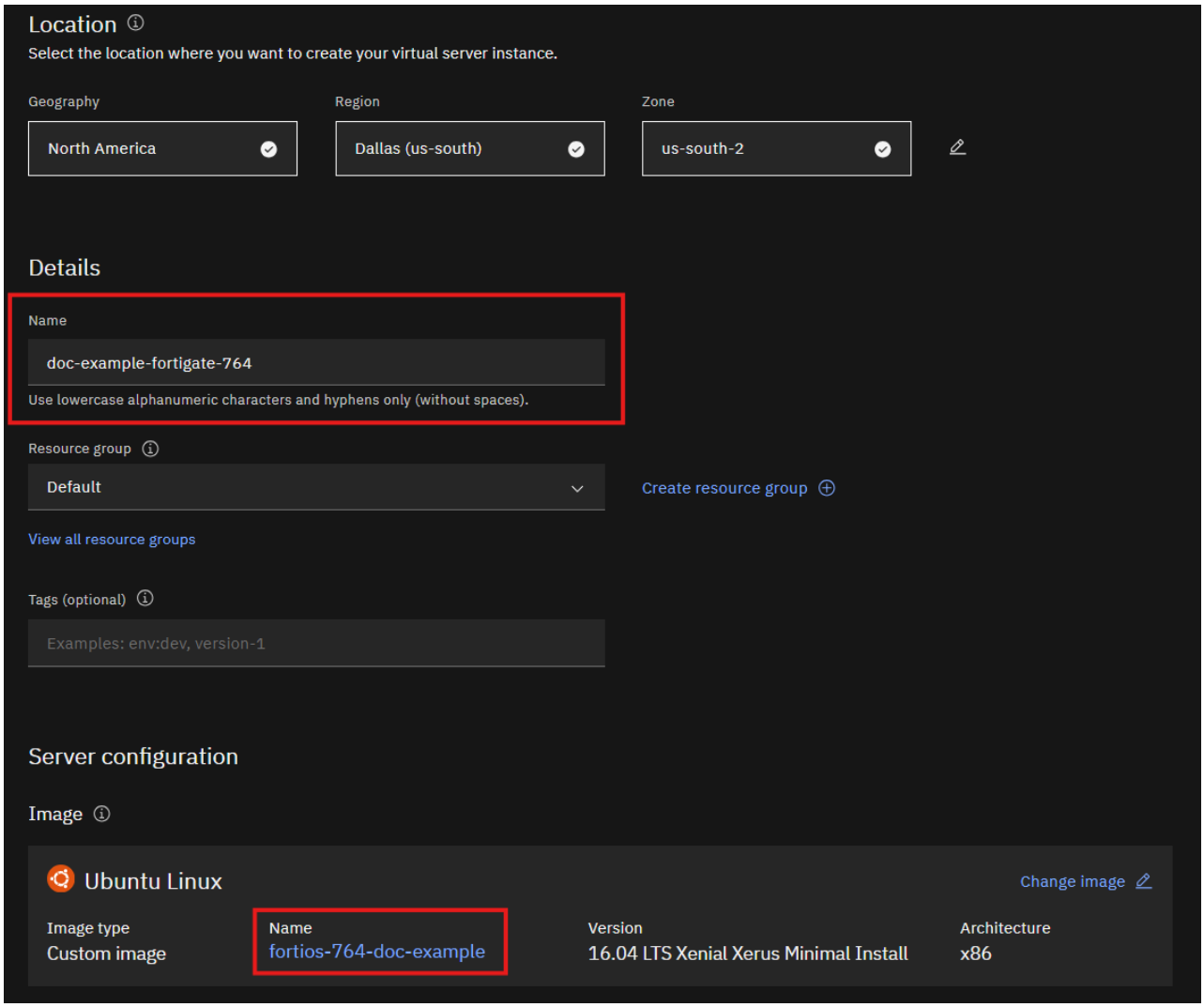


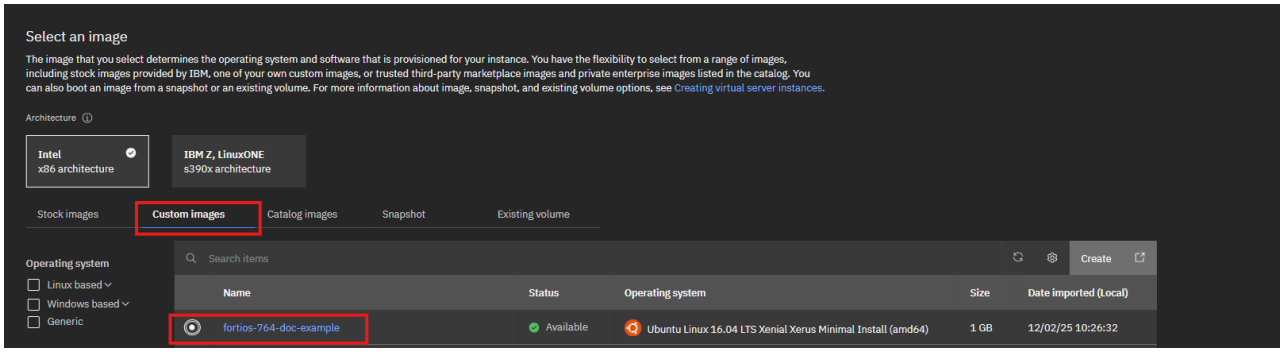
6. Create a new instance based on the custom image. Enter a name, select the VPC, location, custom image imported earlier, profile, SSH key, and user data. User data can be from the IBM Cloud bucket, `config-url/license-url`, or directly inputted in the form of a config, license, or MIME file. See the following example:

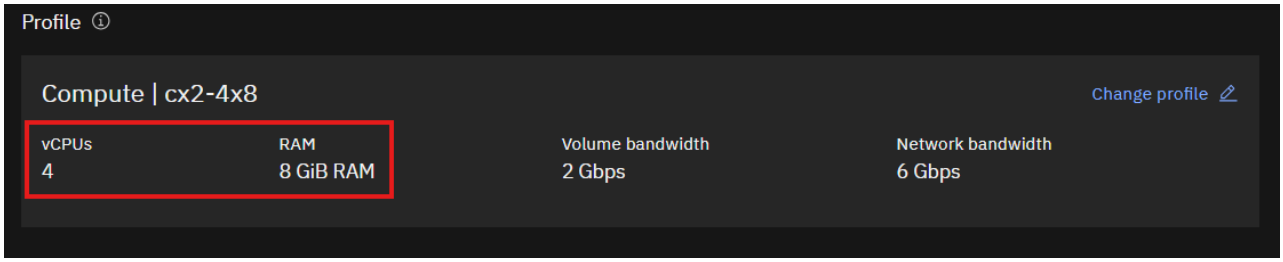
```
{
"bucket" : "lzou-bucket1",
"region" : "eu-gb",
"license" : "FGVM16TM19000211.lic",
"config" : "config.txt",
"apikey": "{{omitted}}"
}
```

The following example includes the license-url and config-url:

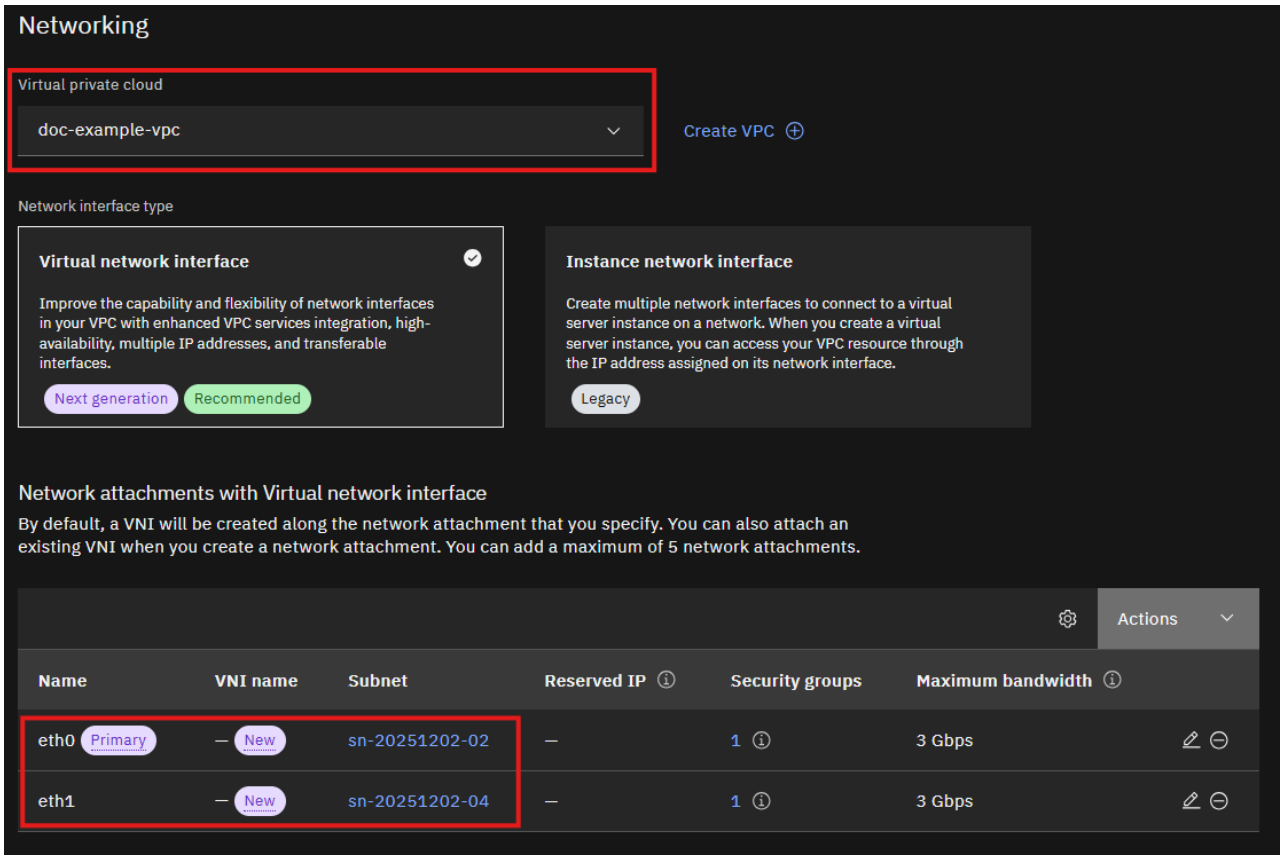
```
{
"license-url" : "http://ec2-54-151-72-112.us-west-
1.compute.amazonaws.com/FGVM16TM19000211.lic",
"config-url" : "http://ec2-54-151-72-112.us-west-1.compute.amazonaws.com/config.txt" }
}
```


Location
Select the location where you want to create your virtual server instance.
Geography
North America
Region
Dallas (us-south)
Zone
us-south-2
Details
Name
doc-example-fortigate-764
Use lowercase alphanumeric characters and hyphens only (without spaces).
Resource group
Default
Create resource group
View all resource groups
Tags (optional)
Examples: env:dev, version-1
Server configuration
Image
Ubuntu Linux
Change image
Image type
Custom image
Name
fortios-764-doc-example
Version
16.04 LTS Xenial Xerus Minimal Install
Architecture
x86


Select an image
The image that you select determines the operating system and software that is provisioned for your instance. You have the flexibility to select from a range of images, including stock images provided by IBM, one of your own custom images, or trusted third-party marketplace images and private enterprise images listed in the catalog. You can also boot an image from a snapshot or an existing volume. For more information about image, snapshot, and existing volume options, see Creating virtual server instances.
Architecture
Intel
x86 architecture
IBM Z, LinuxONE
s390x architecture
Stock images
Custom images
Catalog images
Snapshot
Existing volume
Operating system
Linux based
Windows based
Generic
Search items
Create
Name
Status
Operating system
Size
Date imported (Local)
fortios-764-doc-example
Available
Ubuntu Linux 16.04 LTS Xenial Xerus Minimal Install (amd64)
1 GB
12/02/25 10:26:32


Profile
Compute | cx2-4x8
Change profile
vCPUs
4
RAM
8 GiB RAM
Volume bandwidth
2 Gbps
Network bandwidth
6 Gbps

The instance profile selected will affect the number of VNIs that can be attached to the FortiGate, selecting 4 vCPU profiles will allow for more VNIs.



7. Attach a floating IP address to the instance NIC.

   In 8.0 and later versions, the FortiGate-VM supports virtual network interfaces. This interface type is selected by default.

8. In a browser, go to the IP address to connect to the FortiOS GUI and confirm that the instance is running.

To verify the FortiGates using the CLI:

```
ibmcloud # diagnose debug cloudinit show
    >> Checking metadata source ibm
    >> Found nocloud drive /dev/vdb
    >> Successfully mounted nocloud drive
    >> Setting password to instance id
    >> Provisioning ssh key
    >> Cloudinit curl header:
    >> Cloudinit trying to get license from:
https://thomasbucket2.s3.amazonaws.com/FGVM08TM123456.lic
    >> Cloudinit download license successfully
    >> Cloudinit trying to get config script from:
https://thomasbucket2.s3.amazonaws.com/config2.txt
    >> Cloudinit download config script successfully
```

```
    >> Found metadata source: ibm
    >> Trying to install vmlicense ...
    >> Run config script
    >> Finish running script
    >> FGVM08TM123456 $  config system global
    >> FGVM08TM123456 (global) $  set hostname ibmcloud
    >> FGVM08TM123456 (global) $  end
get system status
Version: FortiGate-VM64-IBM v7.6.4,build3596 GA
Virus-DB: 1.00000(2018-04-09 18:07)
Extended DB: 1.00000(2018-04-09 18:07)
Extreme DB: 1.00000(2018-04-09 18:07)
IPS-DB: 6.00741(2015-12-01 02:30)
IPS-ETDB: 6.00741(2015-12-01 02:30)
APP-DB: 6.00741(2015-12-01 02:30)
INDUSTRIAL-DB: 6.00741(2015-12-01 02:30)
Serial-Number: FGVM08TM123456
IPS Malicious URL Database: 1.00001(2015-01-01 01:01)
License Status: Valid
License Expiration Date: 2021-05-15
VM Resources: 4 CPU/8 allowed, 8,192 MB RAM
Log hard disk: Not available
Hostname: ibmcloud
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: standalone
Branch point: 1705
Release Version Information: interim
FortiOS x86-64: Yes
System time: Tue Mar  19 15:14:00 2024
```

IBM Cloud Catalog - Single FortiGate

FortiOS supports deploying FortiGate-VM bring your own license (BYOL) for IBM Cloud. IBM Cloud users can purchase and deploy FortiGate-VMs. The following describes the steps on how to use the IBM Marketplace product to deploy a FortiGate-VM in a single VM deployment.

Prerequisites:

- A VPC
- Two subnets
- An SSH key
- A FortiOS BYOL licenses

Terraform deploys the following components:

- A FortiGate BYOL instance with two NICs, one in each subnet
- A Floating Public IP address attached to the FortiGate
- A Logging disk

Privileges

This list is a guideline and not an exhaustive list. Please review your environment and add or remove privileges as needed to fit your environment.

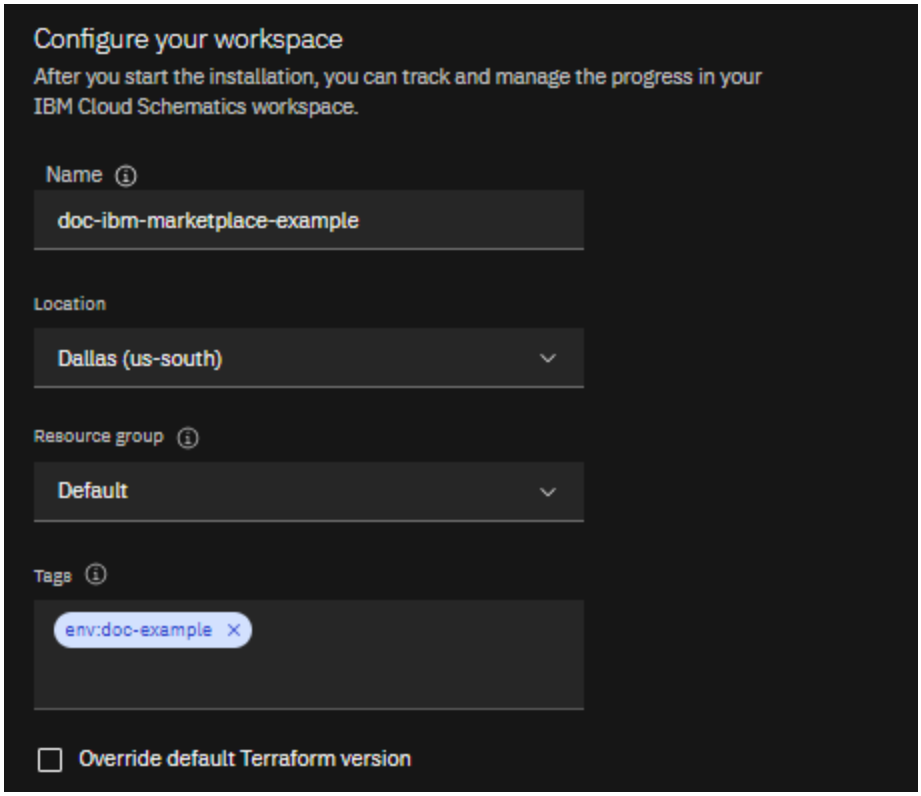
IBM Cloud Service	Actions (create / read / list / attach / etc.)
VPC (Networking)	Read existing VPCs, subnets (get / list). Attach network interfaces to subnets. Manage public IPs (allocate/attach).
Compute / Instances	Create VM instance. *Specify image (BYOL image). Attach NICs, disks. Manage instance lifecycle (start / stop / delete).
Block Storage / Volume	Provision / create volume. Attach to VM. Delete afterwards.
SSH Key resource	List / read SSH keys. If creating them (but in this case, it's preexisting), then ssh_keys.create would be needed.
IAM roles / resource group	Read resource group. Possibly manage tags / resource group.
General read / list permissions	Read images. Read region / zones / quotas. Read resource limits / service status.

Marketplace product

To deploy FortiGate-VM on IBM Cloud marketplace:

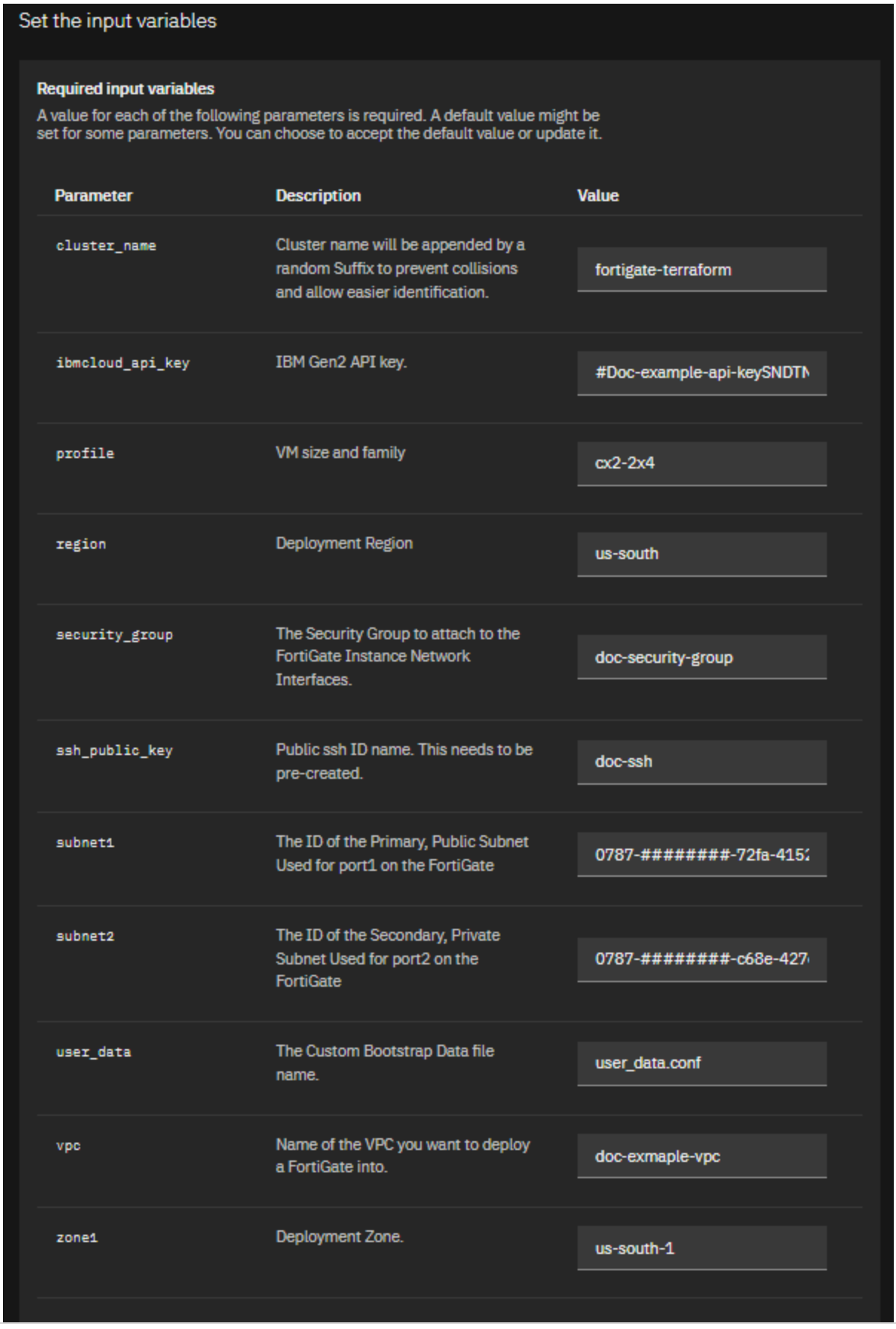
1. Login into IBM Cloud (https://cloud.ibm.com/) and then access the Catalog (https://cloud.ibm.com/catalog)
2. Search for or use this link to deploy FortiGate-VM from the IBM Catalog: Fortinet FortiGate Next-Generation Firewall - Single VM.
3. In the *Configure your workspace*, configure the *Name*, *Location*, *Resource group*, and *Tags* to fit your environment.

Leave *Override default Terraform version* unchecked.



4. Set the input Variables section:

Variable	Description
`cluster_name`	Set as desired. This example leaves it as the default.
`ibmcloud_api_key`	Enter your API key.
`profile`	The instance type used in the deployment.
`region`	Set as desired. This example leaves it as the default.
`security_group`	Enter your desired security group.
`ssh_public_key`	Enter your SSH key that is configured in your account on IBM Cloud.
`subnet1`	Enter the public subnet ID of the subnet in the VPC that the FortiGate-VM will be deployed into.
`subnet2`	Enter the private subnet ID of the subnet in the VPC that the FortiGate-VM will be deployed into.
`user_data`	Configure to load your desired user configuration.
`vpc`	Enter the name of the VPC that the FortiGate-VM will be deployed into.
`zone1`	Enter the zone in the region that the FortiGate-VM will be deployed into.



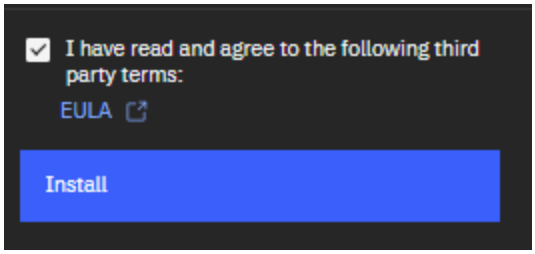
Set the input variables

Required input variables

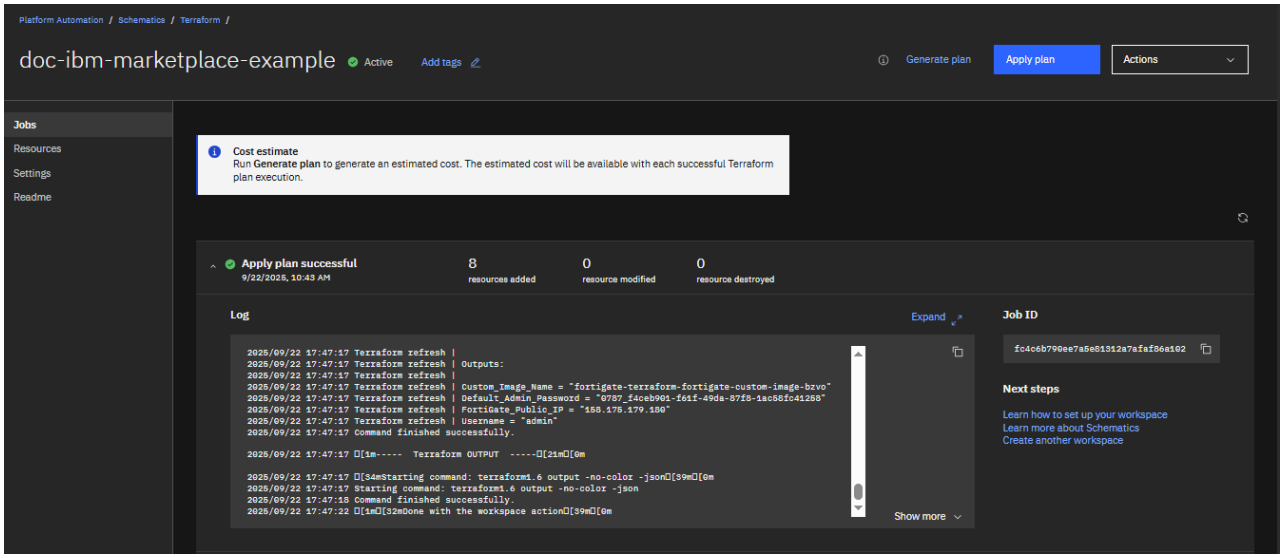
A value for each of the following parameters is required. A default value might be set for some parameters. You can choose to accept the default value or update it.

Parameter	Description	Value
cluster_name	Cluster name will be appended by a random Suffix to prevent collisions and allow easier identification.	fortigate-terraform
ibmcloud_api_key	IBM Gen2 API key.	#Doc-example-api-keySNDTN
profile	VM size and family	cx2-2x4
region	Deployment Region	us-south
security_group	The Security Group to attach to the FortiGate Instance Network Interfaces.	doc-security-group
ssh_public_key	Public ssh ID name. This needs to be pre-created.	doc-ssh
subnet1	The ID of the Primary, Public Subnet Used for port1 on the FortiGate	0787-########-72fa-415
subnet2	The ID of the Secondary, Private Subnet Used for port2 on the FortiGate	0787-########-c68e-427
user_data	The Custom Bootstrap Data file name.	user_data.conf
vpc	Name of the VPC you want to deploy a FortiGate into.	doc-exmaple-vpc
zone1	Deployment Zone.	us-south-1

5. Read and Accept the EULA then click install.



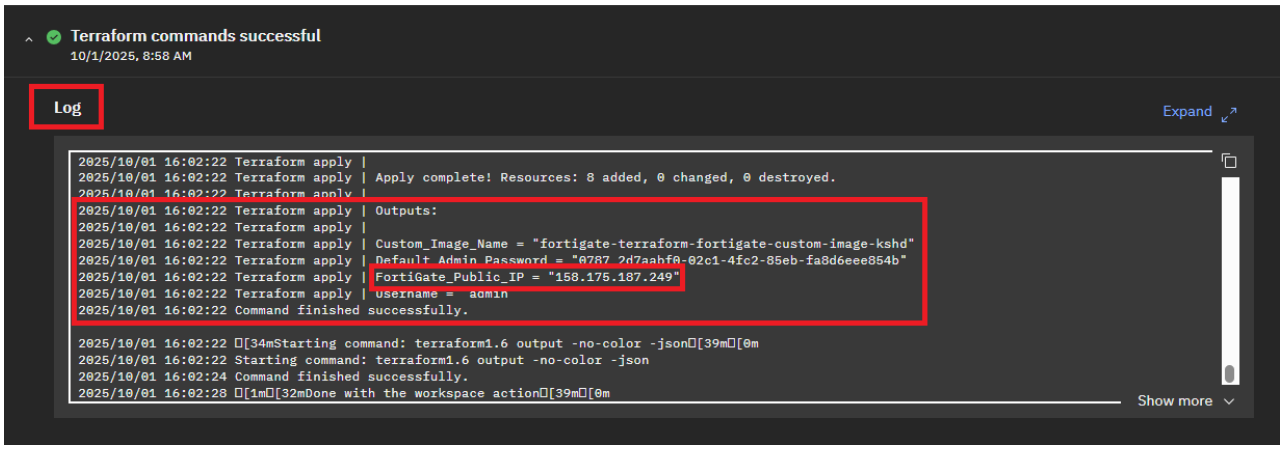
6. Follow the workspace progress until the deployment is complete and successful.



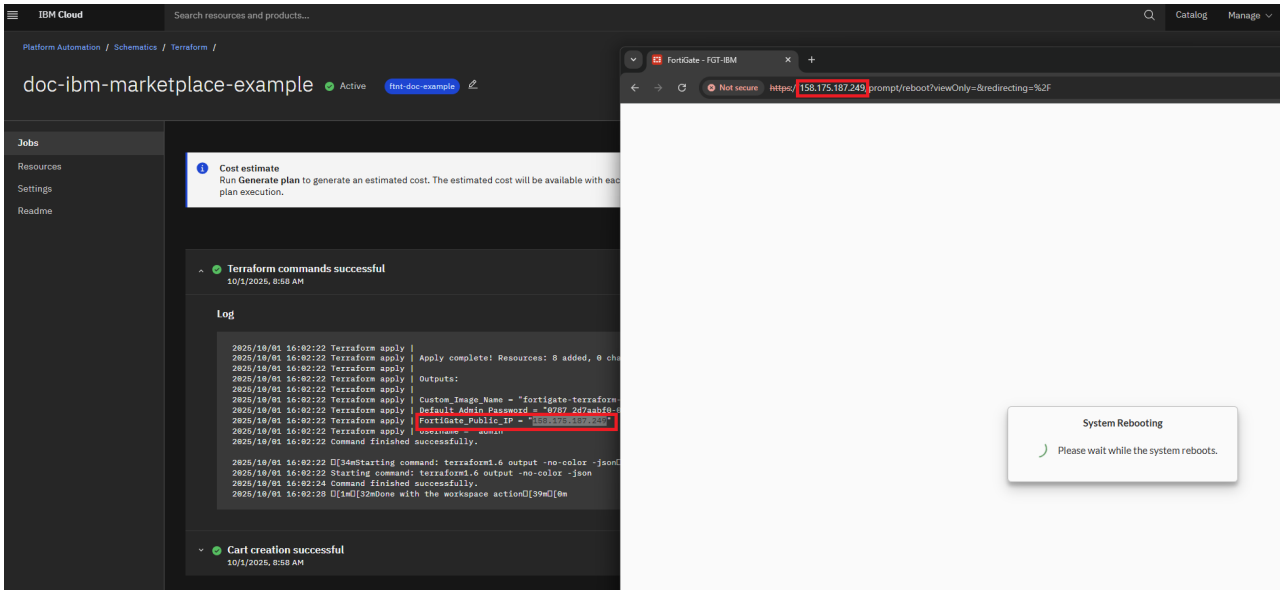
Validating the deployment

To access the FortiGate-VM:

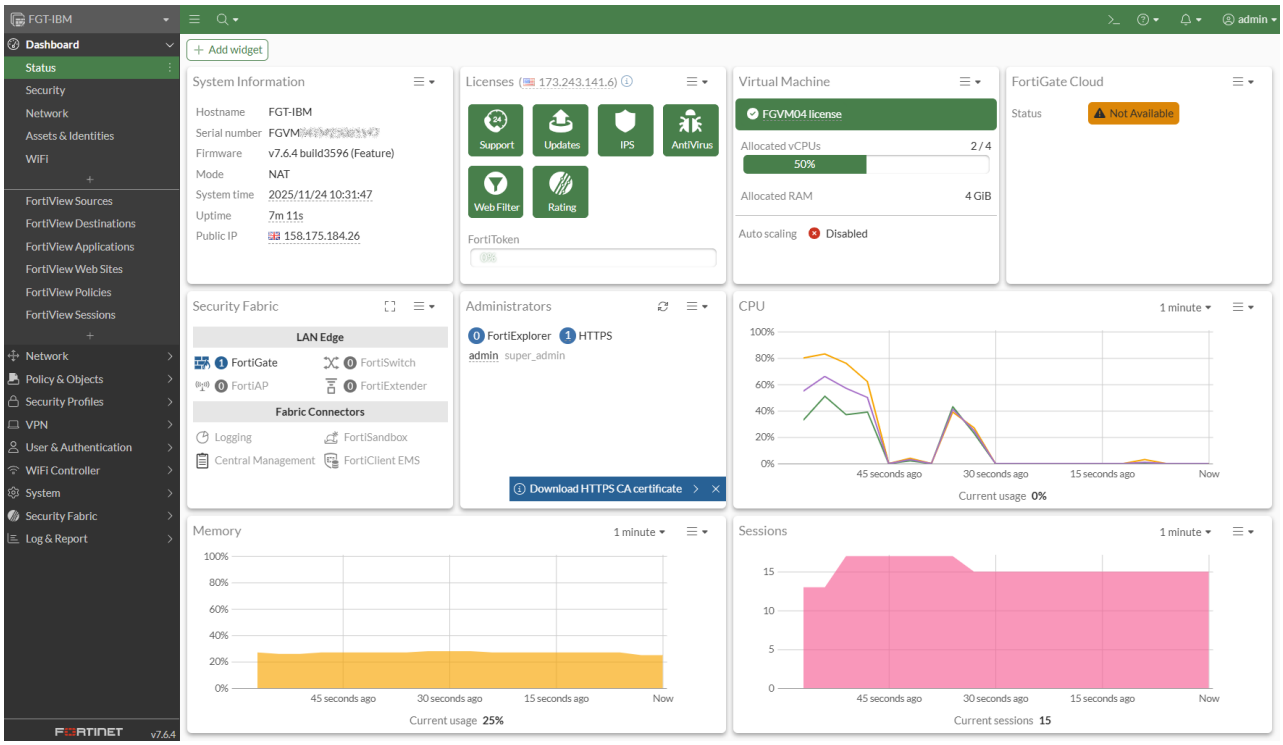
1. After the deployment completes successfully you can connect to the FortiGate-VM using the information found in the logs of the workspace schematics.
2. In the log section scroll to the bottom and review the information contained in the outputs of the Terraform run.



3. Use the public IP address to access and license the FortiGate-VM.
4. Use the admin username and the default admin password provided in the outputs.
5. Login and license the FortiGate-VM and allow time for the FortiGate-VM to reboot.



6. Log in again to view the FortiGate-VM dashboard.

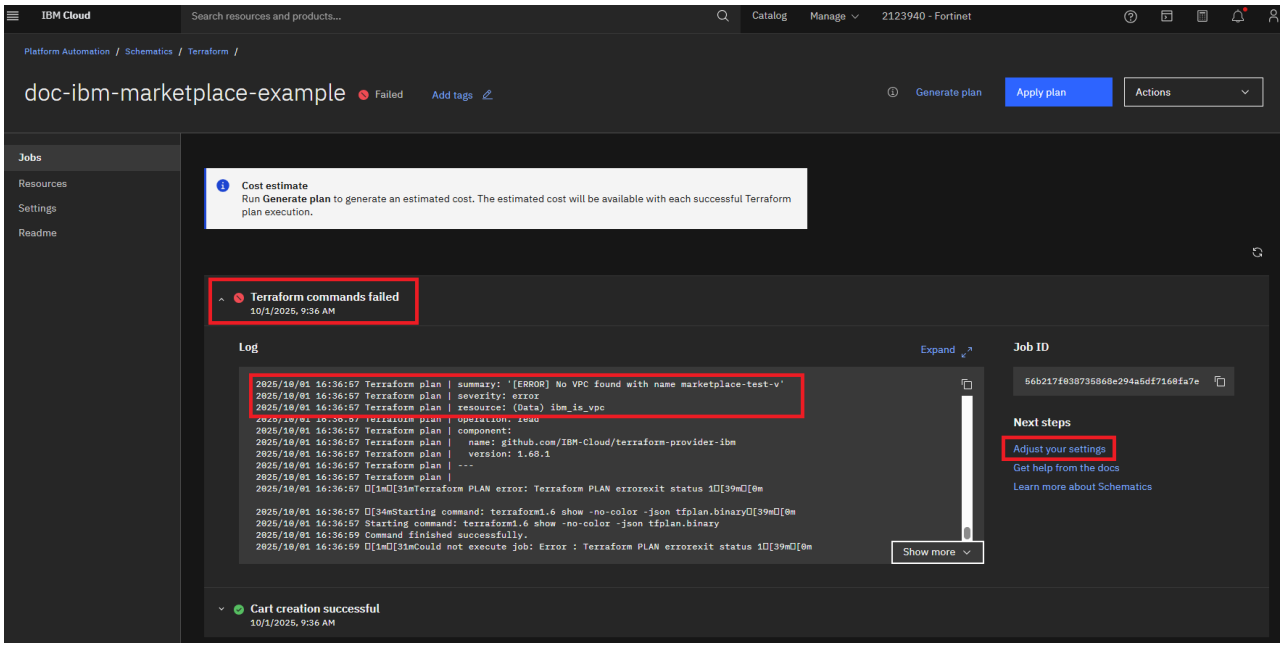


Troubleshooting

> ⚠ The IBM Cloud Schematics (webform) values must match the resources in your IBM VPC environment exactly. The results of mismatching values can result in licensing issues, FortiGate management issues, and HA instability. If the format of the values is accepted but the value itself is incorrect this will not be caught by terraform, IBM schematics, or FortiGate-VM.
>
> For example, if the HA management network is 10.242.3.0/24 and the webform value is 10.242.6.10, this format is correct but the value is incorrect and causes issues in management and licensing as HTTPS traffic is not routed correctly as well as HA cluster formation and communication.

1. When troubleshooting access issues review the assigned or used security group inbound rules and confirm that your public IP address is allowed to access.
2. When FortiGate-VM fails to license confirm that the security group is not restricting access to directregistration.fortinet.com.
3. When troubleshooting Terraform deployment issues it is suggested to review the output of the schematics workspace. The error will be from Terraform stating the issue with the specific field and value that was used in that field.

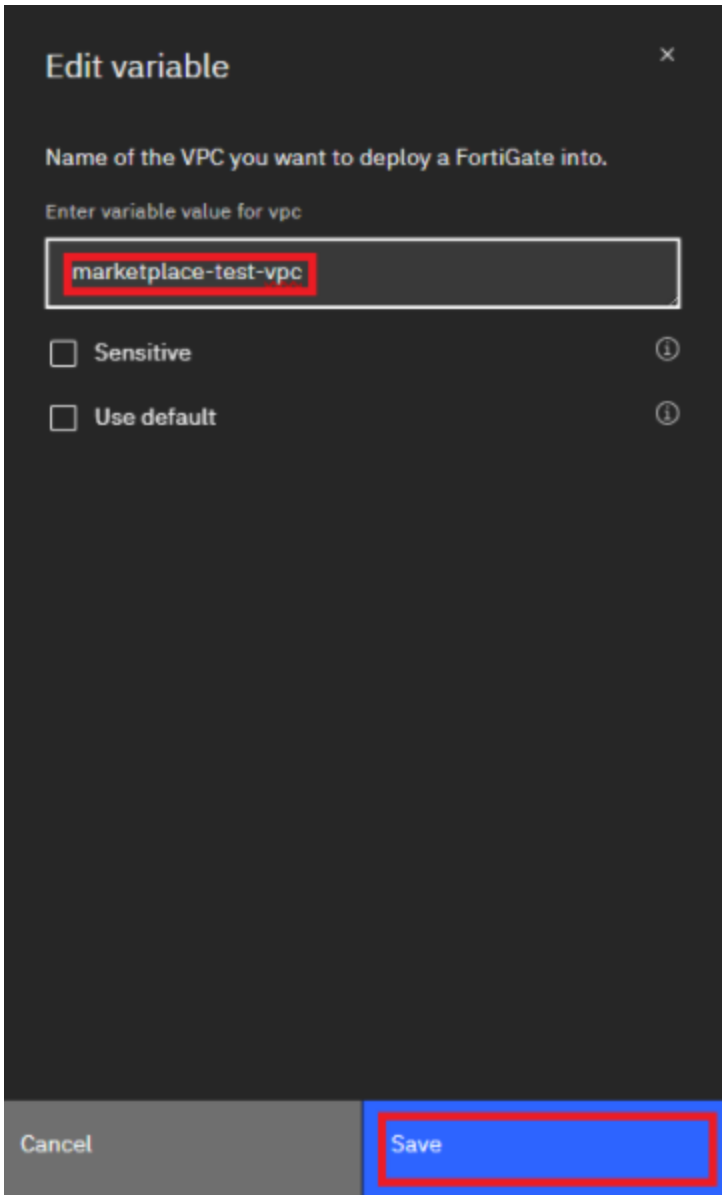
   Example of misspelled VPC name:



a. Select *Adjust your settings*.

b. Then select the variable that has the issue, in this example the VPC name is incorrect.

c. Select the vertical three dots and then select *Edit* to change the value of variable.


Edit variable
Name of the VPC you want to deploy a FortiGate into.
Enter variable value for vpc
marketplace-test-vpc
Sensitive
Use default
Cancel
Save

HA for FortiGate-VM on IBM Cloud

The following topics provide overviews of high availability (HA) configuration when using FortiGate-VM for IBM Cloud:

Deploying FortiGate-VM A-P HA on IBM VPC Cloud (BYOL)

IBM VPC Cloud users can deploy their BYOL FortiGate-VMs in unicast high availability (HA). The HA failover automatically triggers routing changes and floating IP address reassignment on the IBM Cloud via API.

Example

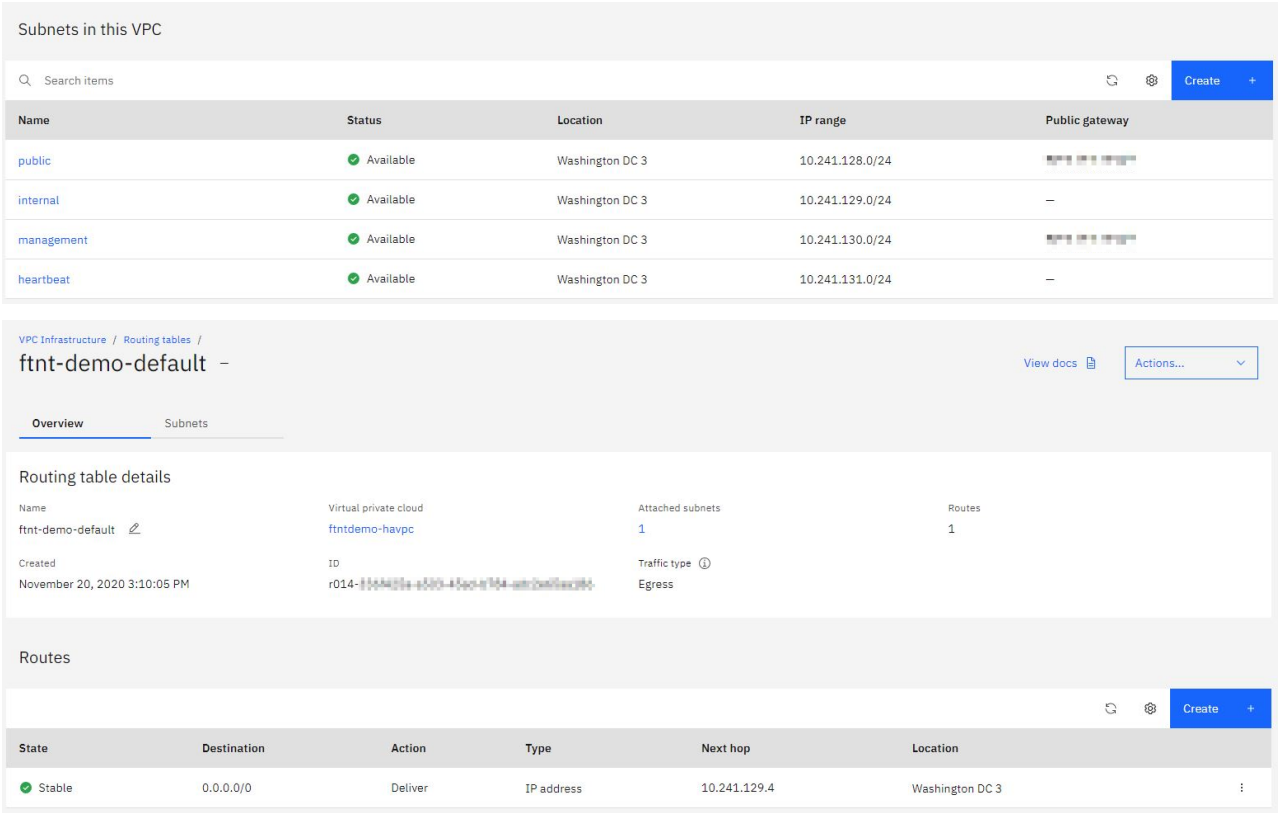
In the following example, the administrator has an Ubuntu client that an IBM FortiGate in HA active-passive (A-P) mode protects. The administrator uses a virtual IP address (VIP) to access Ubuntu and the web, and has traffic inspected for EICAR.

When you shut down the primary device to simulate a failover event, the floating IP address (FIP) and route fail over. After the failover, the administrator can use the VIP to access Ubuntu and the web, and have traffic inspected for EICAR, through the secondary FortiGate.

The following example configures the IBM Virtual PC device and the primary and secondary FortiGates.

To configure the IBM VPC:

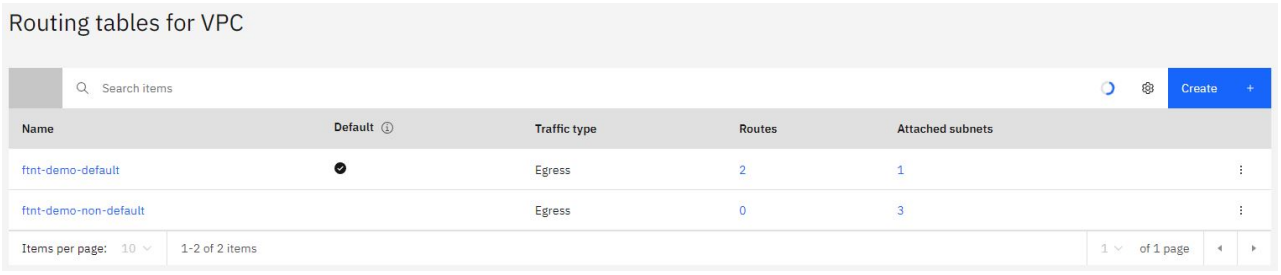
1. Configure the subnets and attach the public gateway:
   a. Configure four subnets:
      - *Public*
      - *Internal*
      - *Management*
      - *Heartbeat*
   b. Ensure a *Public Gateway* is attached to the *Public* subnet



2. Configure two route tables:

Route table	Description
Internal	• Must be the IBM default route table for the VPC. • Has a route for all traffic to the primary FortiGate internal subnet IP address. • Applies to the internal subnet. If you have not deployed FortiGate, return to this step after deployment.
Open	1. Can have no routes, and you can apply it to the *Public*, *Management*, and *Heartbeat* subnets.

You cannot use non-default route tables for the internal subnet's route table failover in IBM VPC.



3. Configure the floating IP.

> IBM Cloud does not currently support multiple FIPs for a single instance. Even though the management ports can be configured, you will not be able to access them using FIP in the final configuration.
>
> If you wish to access the instances for configuration purposes, you can attach a FIP to the public subnets IP on the primary and secondary devices until FOS configuration is finished. You may also connect directly to the local IPs via VPN or another proxy instance.

For this example, the final configuration will only need one FIP attached to the primary public subnet IP.

To configure the FortiGate:

1. Configure the primary and secondary device's static IP addresses.
   a. Configure the primary FortiGate's static IPs for all ports according to IBM Cloud's delegated internal IPs.

```
config system interface
   edit "port1"
      set vdom "root"
      set ip 10.241.128.4 255.255.255.0
      set allowaccess ping https ssh snmp http telnet fgfm radius-acct probe-response fabric
          ftm
      set type physical
      set snmp-index 1
      next
      edit "port2"
      set vdom "root"
      set ip 10.241.129.4 255.255.255.0
      set allowaccess ping https ssh snmp http telnet fgfm radius-acct probe-response fabric
          ftm
      set type physical
      set snmp-index 2
      next
      edit "port3"
      set ip 10.241.131.4 255.255.255.0
      set allowaccess ping https ssh snmp http telnet fgfm radius-acct probe-response fabric
          ftm
      set type physical
      set snmp-index 3
      next
      edit "port4"
      set ip 10.241.130.4 255.255.255.0
      set allowaccess ping https ssh snmp http telnet fgfm radius-acct probe-response fabric
          ftm
```

```
      set type physical
      set snmp-index 4
   next
end
```

b. Configure the secondary FortiGate's static IPs for all ports according to IBM Cloud's delegated internal IPs.

```
config system interface
   edit "port1"
      set vdom "root"
      set ip 10.241.128.5 255.255.255.0
      set allowaccess ping https ssh snmp http telnet fgfm radius-acct probe-response fabric
          ftm
      set type physical
      set snmp-index 1
      next
      edit "port2"
      set vdom "root"
      set ip 10.241.129.5 255.255.255.0
      set allowaccess ping https ssh snmp http telnet fgfm radius-acct probe-response fabric
          ftm
      set type physical
      set snmp-index 2
      next
      edit "port3"
      set ip 10.241.131.5 255.255.255.0
      set allowaccess ping https ssh snmp http telnet fgfm radius-acct probe-response fabric
          ftm
      set type physical
      set snmp-index 3
      next
      edit "port4"
      set ip 10.241.130.5 255.255.255.0
      set allowaccess ping https ssh snmp http telnet fgfm radius-acct probe-response fabric
          ftm
      set type physical
      set snmp-index 4
   next
end
```

2. Configure the HA.

a. Configure the `group-name`, `mode`, `password`, and set `hbdev` port to the heartbeat port.

b. Configure `ha-mgmt-interfaces` and `unicast-hb-peerip` with the FortiGate's heartbeat port IP.

```
config system ha
   set group-name "Test"
   set mode a-p
set password xxxxxxxx
   set hbdev "port3" 100
   set ha-mgmt-status enable
   config ha-mgmt-interfaces
      edit 1
         set interface "port4"
         set gateway 10.241.130.1
      next
   end
   set override enable
   set priority 255
   set unicast-hb enable
```

```
   set unicast-hb-peerip 10.241.131.5
end
```

c. Configure the secondary FortiGate's HA settings.

```
config system ha
   set group-name "Test"
   set mode a-p
   set password xxxxxxxx
   set hbdev "port3" 100
   set ha-mgmt-status enable
   config ha-mgmt-interfaces
      edit 1
         set interface "port4"
         set gateway 10.241.130.1
      next
   end
   set override enable
   set priority 0
   set unicast-hb enable
   set unicast-hb-peerip 10.241.131.4
end
```

d. Verify the primary and secondary FortiGate's can see each other, and the configuration can be synced.

```
# get system ha status
HA Health Status: OK
Model: FortiGate-VM64-IBM
Mode: HA A-P
Group: 0
Debug: 0
Cluster Uptime: 1 days 3:15:48
Cluster state change time: 2020-11-24 15:35:01
Primary selected using:
   <2020/11/24 15:35:01> FGVM08TM20000007 is selected as the primary because it has the
         largest value of override priority.
ses_pickup: disable
override: enable
unicast_hb: peerip=10.241.131.5, myip=10.241.131.4, hasync_port='port3'
Configuration Status:
   FGVM08TM20000007(updated 1 seconds ago): in-sync
   FGVM08TM20000006(updated 2 seconds ago): in-sync
System Usage stats:
   FGVM08TM20000007(updated 1 seconds ago):
      sessions=4, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=4%
   FGVM08TM20000006(updated 2 seconds ago):
      sessions=0, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=4%
HBDEV stats:
FGVM08TM20000007(updated 1 seconds ago):
      port3: physical/10000full, up, rx-bytes/packets/dropped/errors=15646281/45910/0/0,
            tx=21807567/45445/0/0
   FGVM08TM20000006(updated 2 seconds ago):
      port3: physical/10000full, up, rx-bytes/packets/dropped/errors=25485511/54398/0/0,
            tx=22502231/143827/0/0
Primary     : FGVM08TM20000007, FGVM08TM20000007, HA cluster index = 0
Secondary   : FGVM08TM20000006, FGVM08TM20000006, HA cluster index = 1
number of vcluster: 1
vcluster 1: work 10.241.131.4
Primary: FGVM08TM20000007, HA operating index = 0
Secondary: FGVM08TM20000006, HA operating index = 1
```

3. Configure the static route for the primary FortiGate to sync with the secondary FortiGate.
   The gateway is your public subnet's first address, which in this case is `10.241.128.1`
   ```
   config router static
      edit 1
         set gateway 10.241.128.1
         set device "port1"
      next
   end
   ```
4. Configure the `vdom-exception` and `firewall vip`.
   a. Configure the `vdom-exception` on the primary FortiGate to automatically with the secondary FortiGate.
   b. Configure the firewall VIP on the primary and secondary devices. Make sure to set the `extip` to the IP of the individual FortiGate's public subnet IP, and the mapped IP to the Ubuntu client's internal subnet IP.

      Primary FortiGate configuration:

      ```
      config system vdom-exception
         edit 1
            set object firewall.vip
         next
      end
      config firewall vip
         edit "to internal ubuntu"
            set extip 10.241.128.4
            set mappedip "10.241.129.6"
            set extintf "port1"
            set portforward enable
            set extport 8822
            set mappedport 22
         next
      end
      ```

      Secondary FortiGate configuration:

      ```
      config firewall vip
         edit "to internal ubuntu"
            set extip 10.241.128.5
            set mappedip "10.241.129.6"
            set extintf "port1"
            set portforward enable
            set extport 8822
            set mappedport 22
         next
      end
      ```

   c. Configure a VIP in policy for the internal Ubuntu client, and a policy for the internal subnet to reach the internet. This firewall policy will also apply antivirus inspection for HTTP requests. This will be synced from the primary to the secondary device.
      ```
      config firewall policy
         edit 1
            set name "toVIP"
            set srcintf "port1"
            set dstintf "port2"
            set srcaddr "all"
            set dstaddr "to internal ubuntu"
            set action accept
            set schedule "always"
            set service "ALL"
      ```

```
            set logtraffic all
            set nat enable
        next
        edit 2
            set name "main"
            set srcintf "port2"
            set dstintf "port1"
            set srcaddr "all"
            set dstaddr "all"
            set action accept
            set schedule "always"
            set service "ALL"
            set utm-status enable
            set ssl-ssh-profile "certificate-inspection"
            set av-profile "default"
            set logtraffic all
            set nat enable
        next
    end
```

5. Configure the connector on the primary FortiGate to sync with the secondary FortiGate.

```
config system sdn-connector
   edit "1"
      set type ibm
      set ha-status enable
      set api-key xxxxxxxx
      set ibm-region us-east
   next
end
```

6. Ensure that the IBM Cloud SDN connector is up.
   a. Go to *Security Fabric > External Connectors*.
   b. Verify that the *IBM Cloud Connector* is *Up*.

To test the configuration:

1. Access the client Ubuntu via the public FIP and custom port 8822, then use curl to get the EICAR file from HTTP. FortiGate should block the file.

```
root@mail:/home/kvm/scripts# ssh ubuntu@52.117.123.241 -p 8822
ubuntu@52.117.123.241's password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-1026-kvm x86_64)
... omitted ...
ubuntu@thomas-ha-ubuntu:~$ curl http://www.eicar.org/download/eicar.com
<!DOCTYPE html>
... omitted ...
<p>You are not permitted to download the file "eicar.com" because it is infected with the virus
      "EICAR_TEST_FILE".</p>
```

2. Trigger the failover by shutting down primary FortiGate. Verify that the FIP and route tables have moved on IBM, then try to access the client Ubuntu and get the EICAR file again.

```
root@mail:/home/kvm/scripts# ssh ubuntu@53.111.222.333-p 8822
ubuntu@52.111.222.333's password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-1026-kvm x86_64)
... omitted ...
ubuntu@thomas-ha-ubuntu:~$ curl http://www.eicar.org/download/eicar.com
<!DOCTYPE html>
... omitted ...
```

```
<p>You are not permitted to download the file "eicar.com" because it is infected with the virus
      "EICAR_TEST_FILE".</p>
```

3. If the failover is unsuccessful, you can debug the secondary FortiGate in the IBM VPC. Note that even though there are some reported fails, the failover is successful.

```
token size: 1163
token expiration: 1606264324
parsing instance 0888_f8e568dc-5cd7-48eb-b319-8858a3ab5a2b
ibmd HA successfully got fip for hb peer
parsing instance 0888_7b49bafc-db71-4d10-bc05-d009ddb95e4b
ibmd HA found hb host/peer info
in collect rtbl
ibmd HA found rtbl on hb peer ip
ibmd http request response: 204
ibmd HA deleted rtbl r019-167d7dff-86ge-4104-be7d-6efdceb29154
ibmd HA deleted rtbl r019-167d7dff-86ge-4104-be7d-6efdceb29154
ibmd http request response: 201
{"id":"r014-b8771cd6-1669-45c6-80f7-7cd22cd369eb","href":"https://us-
      east.iaas.cloud.ibm.com/v1/vpcs/r014-eb0f603d-51ce-40eb-91db-aafa1aecebbe/routes/r014-
      b8871cd6-1669-45c6-80f7-7cd11cd363eb","name":"glancing-handprint-shakable-
      gotten","action":"deliver","destination":"0.0.0.0/0","next_hop":
      {"address":"10.241.129.5"},"lifecycle_state":"stable","created_at":"2020-11-
      24T23:32:12Z","zone":{"name":"us-east-3","href":"https://us-
      east.iaas.cloud.ibm.com/v1/regions/us-east/zones/us-east-3"}}
ibmd HA created rtbl
ibmd HA created rtbl
HA state: primary
ibmd sdn connector is getting token
token size: 1163
token expiration: 1606234327
parsing instance 0888_e8e564dc-5cd7-47eb-b319-8858a3ab5a2b
ibmd HA failed to parse fip list
ibmd HA failed to get fip for hb peer
parsing instance 0888_7b90bafc-db71-4d20-cd04-d009ddb95e4b
ibmd HA found hb host/peer info
in collect rtbl
ibmd HA failed to find hb fip
ibmd HA failed to move fip
```

Deploying FortiGate-VM A-A HA load balancer sandwich

FortiOS supports deploying FortiGate-VM bring your own license (BYOL) for IBM Cloud. IBM Cloud users can purchase and deploy FortiGate-VMs. The following describes the steps that you take to create and access FortiGate-VM BYOL in active-active (A-A) state in IBM Cloud.

This scenario uses the following load balancers (LB):

- External LB, which sends traffic from the Internet to the FortiGate-VMs
- Internal load balancer, which sends internal traffic to the FortiGate-VMs.

The following lists the steps to configure this deployment:

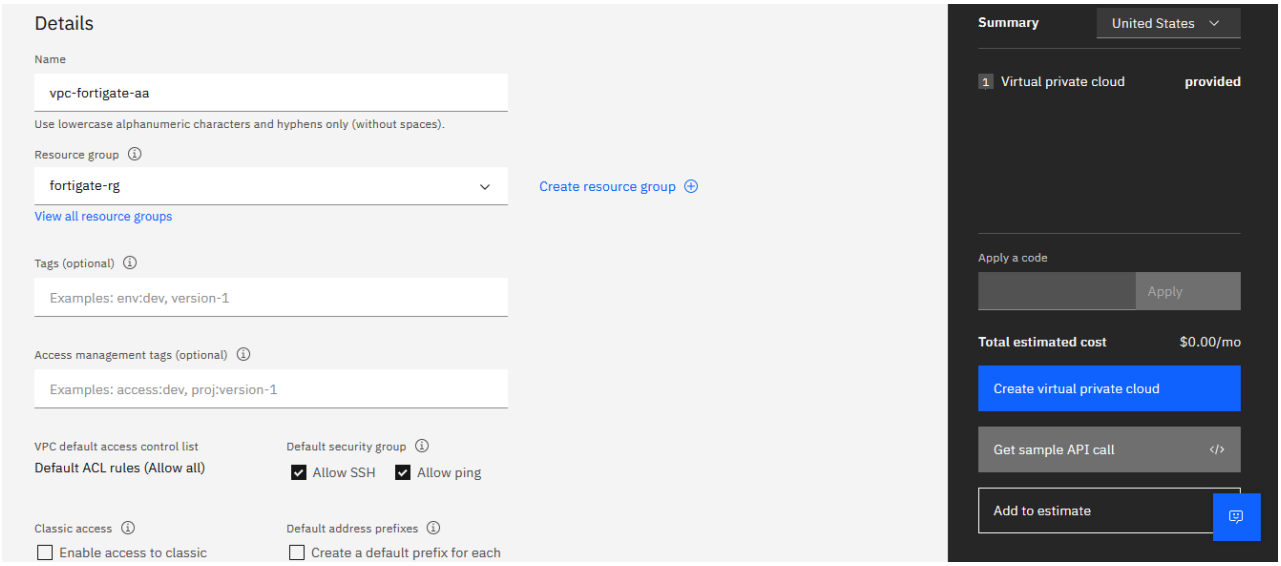
1. Create a new virtual private cloud (VPC). See To create a new VPC: on page 30.
2. Deploy the FortiGate-VMs. See To deploy the FortiGate-VMs: on page 31.
3. Allow IP address spoofing. See To allow IP address spoofing: on page 31.
4. Configure access for the FortiGate-VMs. See To configure access for the FortiGate-VM: on page 31.
5. Access the FortiGate-VMs. See To access the FortiGate-VMs: on page 32.
6. Create a network load balancer (NLB). See To create NLBs: on page 34.
7. Create and change route tables. See To create and change route tables: on page 36.
8. (Optional) Create an Ubuntu instance in the workload subnet for testing. See (Optional) To create an Ubuntu instance in workload subnet for testing: on page 37.
9. Test the FortiGate-VMs. See To test the FortiGate-VMs: on page 37.

To create a new VPC:

1. Go to *VPC Infrastructure* > *Network* > *VPCs*.
2. Select the *Geography* and *Region*.
3. Enter a name.
4. Click *Create*.
5. Deselect *Create a default prefix for each zone*.

   Deselecting *Create a default prefix for each zone* is recommended so you can have more control on the subnets that you are creating.

6. Click *Create virtual private cloud*.



7. Configure the subnet:
   a. Click the subnet that you created.
   b. Go to the *Address prefixes* tab.
   c. Click *Create*.
   d. Set your *IP Range* and *Location*.
   e. Click *Create*.
8. Go to the *Overview* tab.

9. You must create at least two subnets for the FortiGate-VM: one external (public) and one internal. This example also creates an optional subnet to add a virtual machine for testing purposes. Scroll to *Subnets in this VPC session* and click *Create*. Configure the following subnets:
   a. Configure the external (public) subnet:
      i. Ensure to select the desired VPC.
      ii. Set the IP address range for the subnet.
      iii. Enable the *Public gateway* attach.
      iv. Configure other fields as desired. In this example, the external subnet is named *external*.
      v. Click *Create subnet*.
   b. Configure the internal subnet:
      i. Click *Create* in the *Subnets* page.
      ii. Ensure to select the desired VPC.
      iii. Set the IP address range for the subnet.
      iv. Leave *Public gateway* unselected.
      v. Configure other fields as desired. In this example, the internal subnet is named *internal*.
      vi. Click *Create subnet*.
   c. (Optional) Repeat the steps for the internal subnet to create the workload subnet. This example names this subnet *workload*.

To deploy the FortiGate-VMs:

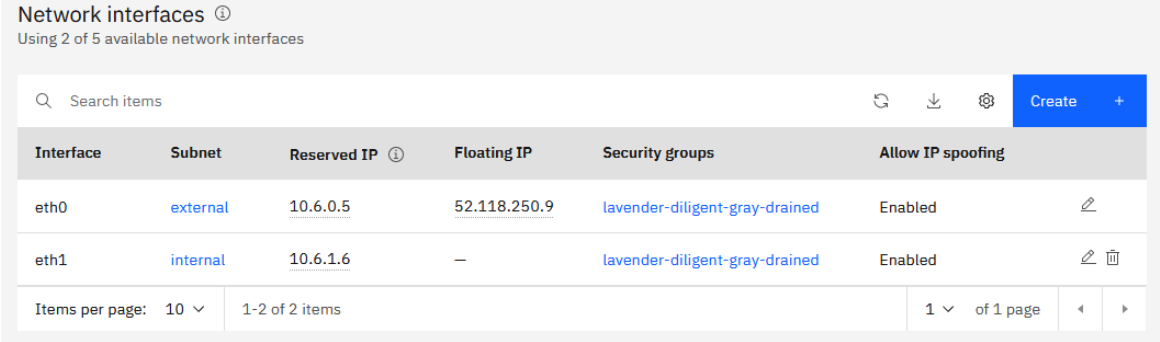
See Deploying FortiGate-VM on IBM Cloud on page 8.

To allow IP address spoofing:

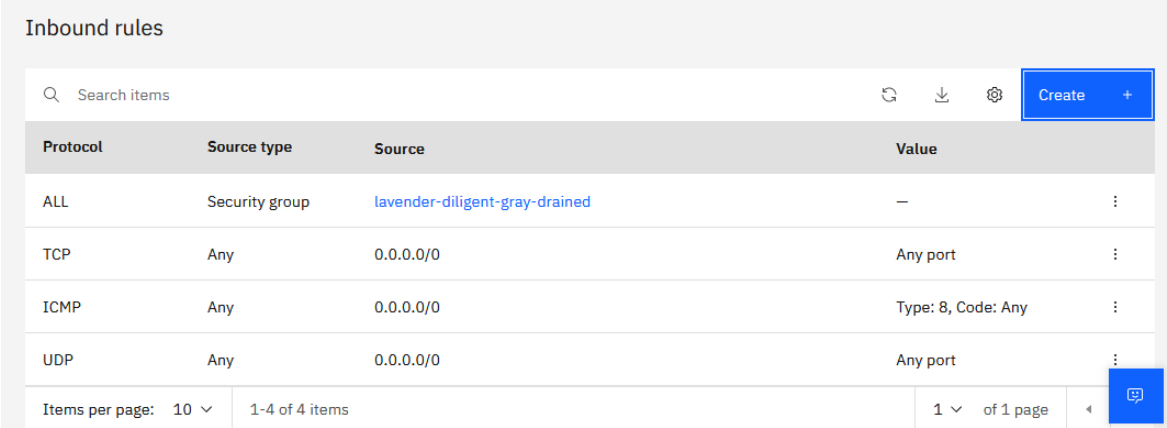
1. In *VPC Infrastructure*, go to and select the FortiGate port1.
2. Under *Network interfaces*, select and edit eth0/port1 or the interface used in the public/external subnet.
3. Enable *Allow IP spoofing*.
4. Click *Save*.

To configure access for the FortiGate-VM:

1. Go to *VPC Infrastructure* > *Compute* > *Virtual server instances*.
2. Select FortiGate 01 (fgtaa-01).
3. Scroll to *Network interfaces* and edit *eth0*.
4. In *Floating IP address*, select *Reserve a new floating IP*.
5. Click *Save*.
6. Copy the generated *Floating IP* and note it for later.
7. Click the associated security group.



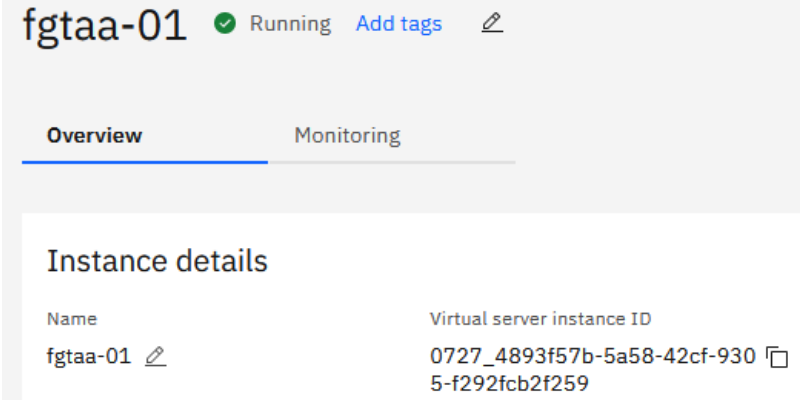
8. Go to the *Rules* tab and edit the existing rule or create a new rule allowing all TCP and UDP traffic.



9. Repeat steps 1-6 for FortiGate 02 (fgtaa-02).

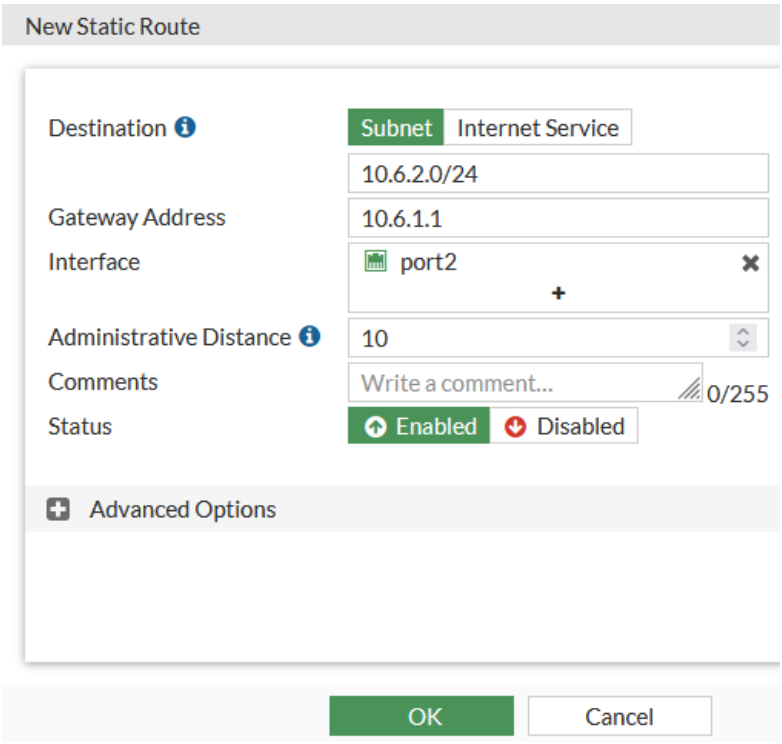
To access the FortiGate-VMs:

1. Log in to FortiGate 01:
   a. Using your browser, access FortiGate 01 with the floating IP address that you created: https://<Floating IP address>.
   b. Ignore certificate issues.
   c. Click *Accept* on *Login Disclaimer*.
   d. Log in using the following credentials:
      i. For the username, enter admin.
      ii. For the password, enter the virtual server instance ID. You can find this value in IBM Cloud.



e. Change the default password and log in.

2. If you did not license the FortiGate-VM during deployment with user data, you must do so now. FortiGate reboots after you insert the license. Log in again.
3. If you created an optional subnet to the workload, you must create a route to access it. Create the route:
   a. Go to *Network > Static Routes*.
   b. Click *Create New*
   c. In the *Destination* field, select *Subnet*, then enter the workload subnet.
   d. In the *Gateway Address* field, enter the port2 subnet first valid IP address.
   e. Click *OK*.



4. Open the FortiOS CLI and run the following commands to enable system probe-response:

```
config system probe-response
   set mode http-probe
end
config sys interface
   edit port1
```

```
        set allowaccess ping https ssh http fgfm probe-response
    next
    edit port2
        set allowaccess ping https ssh http fgfm probe-response
end
```

5. Repeat steps 1-6 for FortiGate 02.

> You can use FortiManager or the autoscale feature on FortiOS to sync config between the VMs. This example uses the autoscale feature. It does not enable autoscaling and only syncs the config.

6. Note the FortiGate 01 port2 address.
7. On FortiGate 01, open the CLI and enter the following:

```
config system auto-scale
    set status enable
    set role primary
    set sync-interface "port2"
    set psksecret "averystrongpassword"
end
```

8. On FortiGate 02, open the CLI and enter the following:

```
config system auto-scale
    set status enable
    set role secondary
    set sync-interface "port2"
    set primary-ip FGT_01_PORT2_IP
    set psksecret "averystrongpassword"
end
```

9. Execute the following command to check the autoscale sync status of both FortiGates. If both FortiGates are not visible in the output, log out, wait a couple of minutes, and log in again: `diagnose sys ha autoscale-peers`

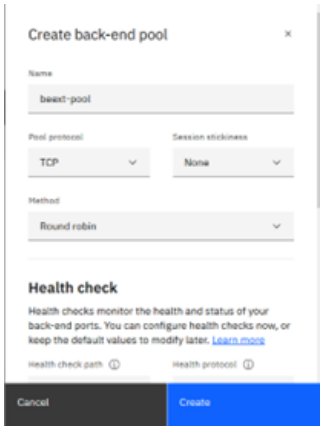
```
FGVM04T[redacted] # diagnose sys  ha autoscale-peers
Serial#: FGVM04T[redacted]
VMID:    0727_c29cd09a-6b4f-4aef-a526-1f042a6e06
Role:    secondary
IP:      10.6.1.5

Serial#: FGVM04T[redacted]
VMID:    0727_4893f57b-5a58-42cf-9305-f292fcb2f2
Role:    primary
IP:      10.6.1.6
```

To create NLBs:

1. You must create one LB for external traffic and another for internal traffic:
   a. Go to *VPC Infrastructure > Network > Load balancers*. Click *Create+*.
   b. Choose *Network load balancer*.

c. Configure the region, name, and VPC as desired. This example names the LB *external-nlb*.
d. Leave the type as public.
e. In *Subnet*, select the external subnet that you created.
f. Create a backend pool:
   i. In *Back-end pools*, click *Create pool*.
   ii. Enter a name. This example names the LB *beext-pool*.
   iii. Click *Create*.



g. Attach the external subnet to the backend line:
   i. In the backend line created, click *Attach server*.
   ii. Select the external subnet.
   iii. Select both FortiGates and in the *Server port* field, enter 8008.
   iv. Click *Attach*.
h. Create a listener:
   i. Under *Front-end listeners*, click *Create listener*.
   ii. Select the back-end pool that you created.
   iii. If desired, you can choose to redirect only one port or a port range. These ports are forwarded to FortiGate external interfaces. Click *Create*.
i. Ensure that the security group used allows all desired traffic.
j. Click *Create load balancer*.

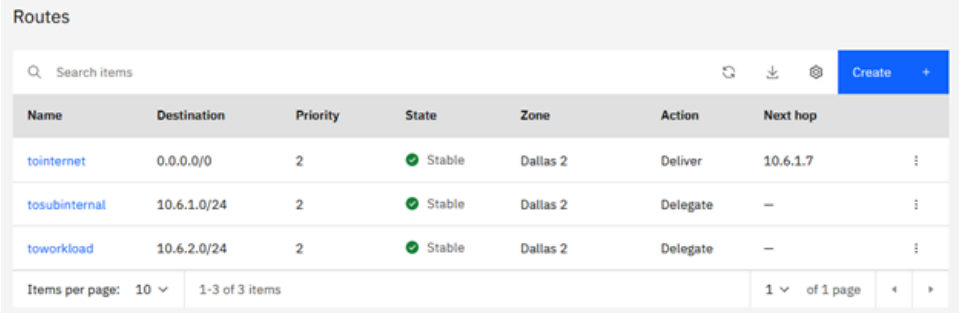
2. Create the internal load balancer:
   a. Go to *VPC Infrastructure > Network > Load balancers*. Click *Create+*.
   b. Choose *Network load balancer*.
   c. Configure the region, name, and VPC as desired. This example names the LB *internal-nlb*.
   d. For *Type*, select *Private*.
   e. Enable *Routing mode*.
   f. In *Subnet*, select the internal subnet that you created.
   g. Create a backend pool:
      i. In *Back-end pools*, click *Create pool*.
      ii. Enter a name. This example names the LB *beint-pool*.
      iii. Click *Create*.
   h. Attach the external subnet to the backend line:

   i. In the backend line created, click *Attach server*.
   ii. Select the internal subnet.
   iii. Select both FortiGates and in the *Server port* field, enter 8008.
   iv. Click *Attach*.
  i. Create a listener:
   i. Under *Front-end listeners*, click *Create listener*.
   ii. Select the backend pool that you created.
  j. Ensure that the security group used allows all desired traffic.
  k. Click *Create load balancer*.
3. Wait for both LB statuses to change to *Active*.
4. When their statuses show as *Active*, click them and copy their IP addresses. The internal LB shows two IP addresses. Only copy the first IP address.

To create and change route tables:

You must change route tables to the newly created LB.

1. Create a route table:
   a. Go to *VPC Infrastructure > Network > Routing tables*.
   b. Select your VPC and click *Create+*.
   c. Name the table as desired. This example names the table *rtb-external*.
   d. Leave all the fields at their default values and click *Create routing table*.
2. In the newly created route table, click its number of attached subnets.
3. Click *Attach+*, select the external subnet, and click *Attach*.
4. Return to the routing table list and click the other route table with the *VPC default* tag.
5. Configure a route for the external subnet:
   a. Scroll to *Routes* and click *Create+*.
   b. Name the route as desired. This example names the route *tointernet*.
   c. In the *Destination CIDR* field, enter 0.0.0.0/0.
   d. For *Action*, select *Deliver*.
   e. In the *Next hop* field, enter the internal LB IP address.
   f. Save.
6. Configure a route for the internal subnet:
   a. Click *Create+* under *Routes*.
   b. Name the route as desired. This example names the route *tointernal*.
   c. In the *Destination CIDR* field, enter 10.6.1.0/24. This is your internal subnet CIDR.
   d. For *Action*, select *Delegate*.
   e. Save.
7. Configure a route for the optional workload subnet:
   a. Click *Create+* under *Routes*.
   b. Name the route as desired. This example names the route *toworkload*.
   c. In the *Destination CIDR* field, enter 10.6.2.0/24. This is your workload subnet CIDR.
   d. For *Action*, select *Delegate*.
   e. Save.



(Optional) To create an Ubuntu instance in workload subnet for testing:

1. Go to *VPC Infrastructure* > *Compute* > *Virtual server instances*.
2. Click *Create*.
3. Configure the Ubuntu instance:
   a. Configure *Region*, *Zone*, and *Name* as desired. This example names the Ubuntu instance *ubuntu-testing-01*.
   b. Under *Image and profile*, click *Change image*.
   c. Search for and select *Ubuntu*, and save.
   d. Choose the desired profile.
   e. Choose or create an SSH key.
   f. Under *Networking*, select the VPC previously created.
   g. Edit *Network interfaces on eth0* and select the workload subnet.
4. Click *Create virtual server*.

To test the FortiGate-VMs:

1. As your FortiGate-VMs are under the external LB, access the FortiGate by entering the external LB public IP address and the FortiGate HTTPS port.
2. Create a virtual IP object (VIP). This example redirects port 2222 to port 22 (SSH). Complete the configuration as fits your environment and remember that you have to set this port in the external LB to forward the traffic.
3. Go to *Policy & Objects* > *Firewall Policy* and click *Create New*.
4. Configure as follows:
   a. For *Type*, select *Standard*.
   b. From the *Incoming Interface* dropdown list, select *port1*.
   c. From the *Outgoing Interface* dropdown list, select *port2*.
   d. For *Source*, select *all*.
   e. For *Destination*, select the VIP that you created.
   f. For *Service*, select *SSH*.
   g. For *Action*, select *Accept*.
   h. Configure other fields as desired.
5. Test the access. You should have access to your Ubuntu instance.

IBM Cloud Catalog - HA Active Passive - One Zone

FortiOS supports deploying FortiGate-VM bring your own license (BYOL) for IBM Cloud. IBM Cloud users can purchase and deploy FortiGate-VMs. The following describes the steps on how to deploy an Active-Passive (A-P) HA cluster in a single zone. This template makes use of the FortiGate IBM Cloud Connector to failover in the event of a VM shutdown. After the active VM is back up, it will take over as active once again.

Prerequisites:

- A VPC
- Four subnets in a single zone:
  - A public subnet with a public gateway attached
  - An HA management subnet also with a public gateway attached
- An SSH key
- Two FortiOS BYOL licenses

Terraform deploys the following components:

- Two FortiGate BYOL instances with four NICs each, one in each subnet.
- Three floating Public IP addresses: one attached to the Primary FortiGate on Port1, which will failover, and the other two attached to the HA management port (Port4) of each FortiGate.
- One log disk per FortiGate.
- A basic bootstrap configuration with HA support.

Privileges

This list is a guideline and not an exhaustive list. Please review your environment and add or remove privileges as needed to fit your environment.

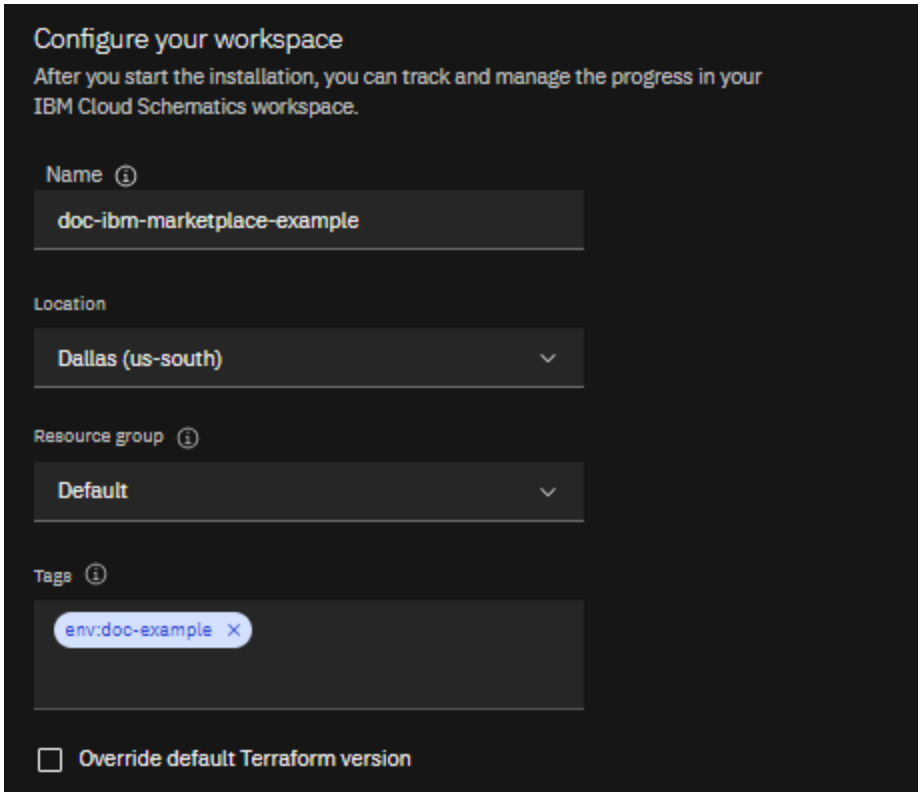
IBM Cloud Service	Actions (create / read / list / attach / etc.)
VPC (Networking)	Read existing VPCs, subnets (get / list). Attach network interfaces to subnets. Manage public IPs (allocate/attach).
Compute / Instances	Create VM instance. *Specify image (BYOL image). Attach NICs, disks. Manage instance lifecycle (start / stop / delete).
Block Storage / Volume	Provision / create volume.

IBM Cloud Service	Actions (create / read / list / attach / etc.)
	Attach to VM. Delete afterwards.
SSH Key resource	List / read SSH keys. If creating them (but in this case, it's preexisting), then ssh_keys.create would be needed.
IAM roles / resource group	Read resource group. Possibly manage tags / resource group.
General read / list permissions	Read images. Read region / zones / quotas. Read resource limits / service status.

Marketplace product

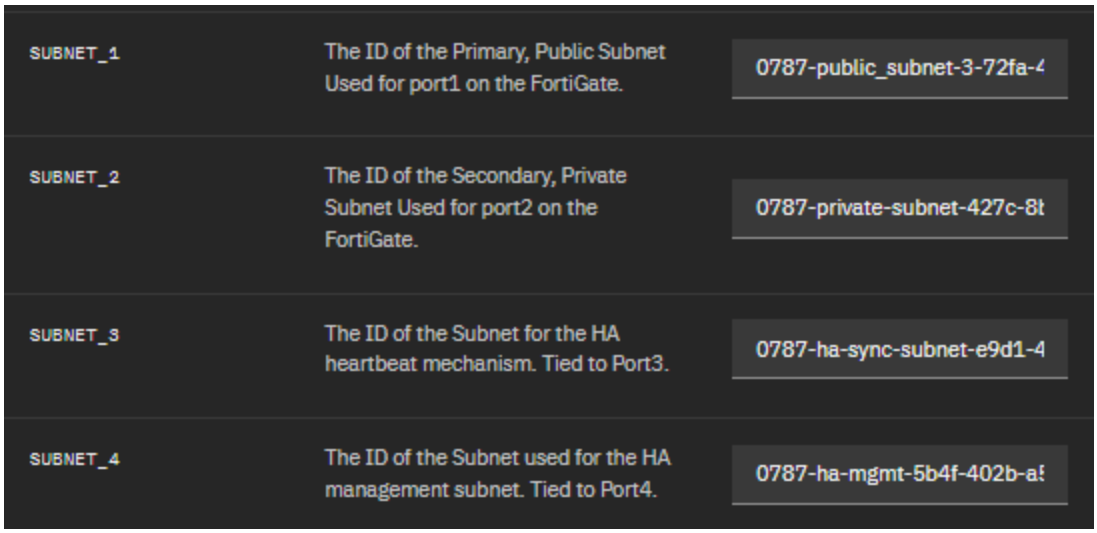
To deploy FortiGate-VM on IBM Cloud marketplace:

1. Login into IBM Cloud (https://cloud.ibm.com/) and then access the Catalog (https://cloud.ibm.com/catalog)
2. Search for or use this link to deploy FortiGate-VM from the IBM Catalog: Fortinet FortiGate Next-Generation Firewall - A/P HA.
3. In the *Configure your workspace*, configure the *Name*, *Location*, *Resource group*, and *Tags* to fit your environment.
   Leave *Override default Terraform version* unchecked.



4. Set the input Variables section:

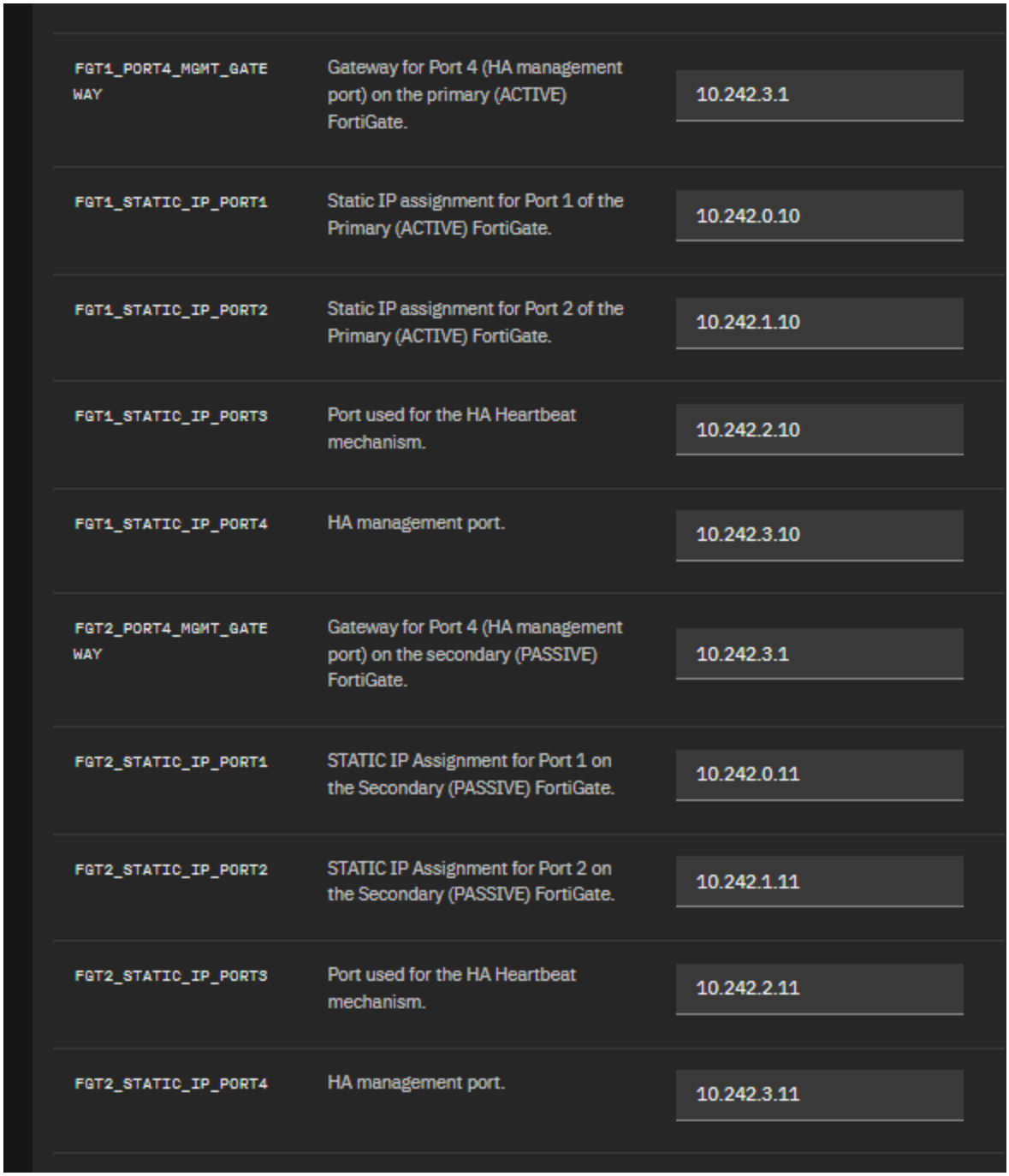
Variable	Description
cluster_name	Set as desired. This example leaves it as the default.
ibmcloud_api_key	Enter your API key.
profile	The instance type used in the deployment.
region	Set as desired. This example leaves it as the default.
security_group	Enter your desired security group.
ssh_public_key	Enter your SSH key that is configured in your account on IBM Cloud.
subnet1	Enter the public subnet ID of the subnet in the VPC that the FortiGate-VM will be deployed into.
subnet2	Enter the private subnet ID of the subnet in the VPC that the FortiGate-VM will be deployed into.
subnet3	Enter the ha-sync subnet ID of the subnet in the VPC that the FortiGate-VM will be deployed into.
subnet4	Enter the ha-mgmt subnet ID of the subnet in the VPC that the FortiGate-VM will be deployed into.
user_data	Configure to load your desired user configuration.
vpc	Enter the name of the VPC that the FortiGate-VM will be deployed into.
zone1	Enter the zone in the region that the FortiGate-VM will be deployed into.



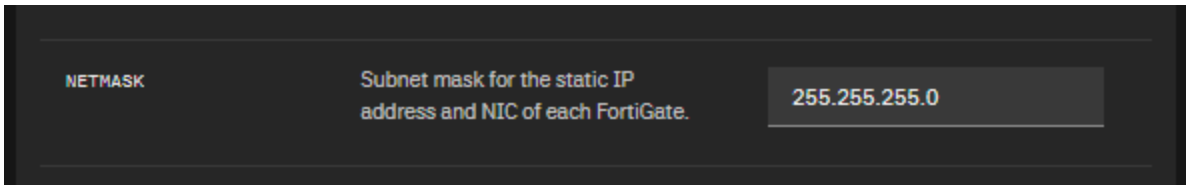
In addition to the above list of inputs, the following must also be configured:

- FGT1_PORT4_MGMT_GATEWAY
- FGT1_STATIC_IP_PORT1
- FGT1_STATIC_IP_PORT2
- FGT1_STATIC_IP_PORT3

- FGT1_STATIC_IP_PORT4
- FGT2_PORT4_MGMT_GATEWAY
- FGT2_STATIC_IP_PORT1
- FGT2_STATIC_IP_PORT2
- FGT2_STATIC_IP_PORT3
- FGT2_STATIC_IP_PORT4
- NETMASK

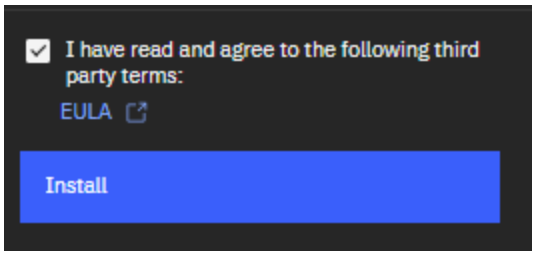


FGT1_PORT4_MGMT_GATEWAY	Gateway for Port 4 (HA management port) on the primary (ACTIVE) FortiGate.	10.242.3.1
FGT1_STATIC_IP_PORT1	Static IP assignment for Port 1 of the Primary (ACTIVE) FortiGate.	10.242.0.10
FGT1_STATIC_IP_PORT2	Static IP assignment for Port 2 of the Primary (ACTIVE) FortiGate.	10.242.1.10
FGT1_STATIC_IP_PORT3	Port used for the HA Heartbeat mechanism.	10.242.2.10
FGT1_STATIC_IP_PORT4	HA management port.	10.242.3.10
FGT2_PORT4_MGMT_GATEWAY	Gateway for Port 4 (HA management port) on the secondary (PASSIVE) FortiGate.	10.242.3.1
FGT2_STATIC_IP_PORT1	STATIC IP Assignment for Port 1 on the Secondary (PASSIVE) FortiGate.	10.242.0.11
FGT2_STATIC_IP_PORT2	STATIC IP Assignment for Port 2 on the Secondary (PASSIVE) FortiGate.	10.242.1.11
FGT2_STATIC_IP_PORT3	Port used for the HA Heartbeat mechanism.	10.242.2.11
FGT2_STATIC_IP_PORT4	HA management port.	10.242.3.11

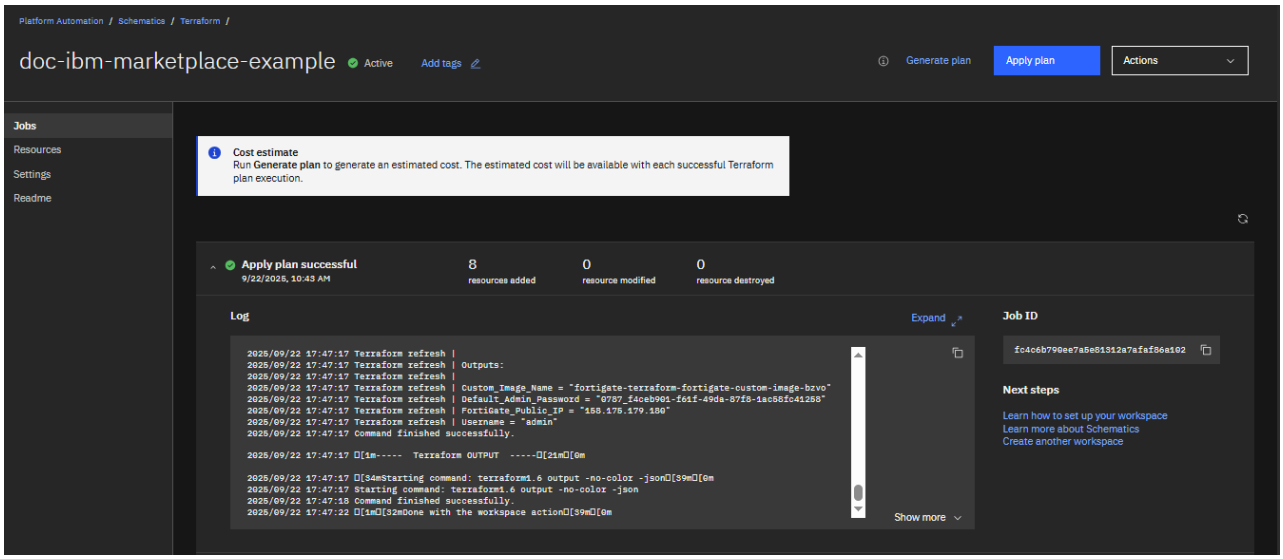


These values are gained from the network configuration of the subnets created in your VPC. This example uses a netmask of 255.255.255.0 and 10.242.0.0/16 address space. 10.242.3.1 is the value for each FortiGate-VM HA Management gateway as both FortiGate-VM's are deployed into the same zone.

5. Read and Accept the EULA then click install.



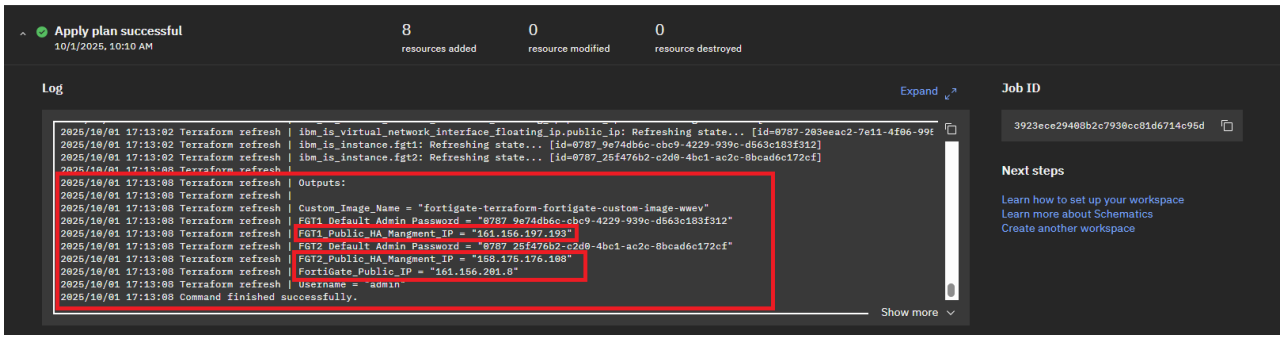
6. Follow the workspace progress until the deployment is complete and successful.



Validating the deployment

To access the FortiGate-VM:

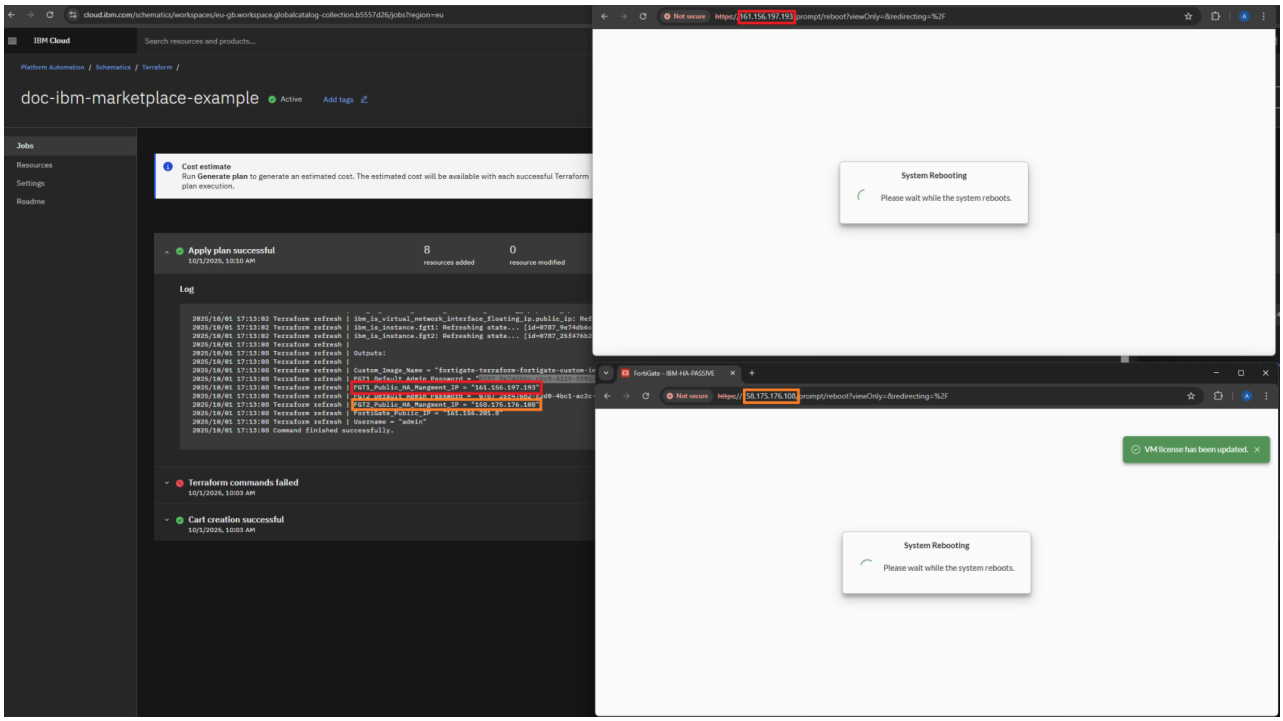
1. After the deployment completes successfully you can connect to the FortiGate-VMs using the information found in the logs of the workspace schematics. There will be a HA management interface public for the Primary or Active and the secondary FortiGate-VM's.
2. In the log section scroll to the bottom and review the information contained in the outputs of the Terraform run.



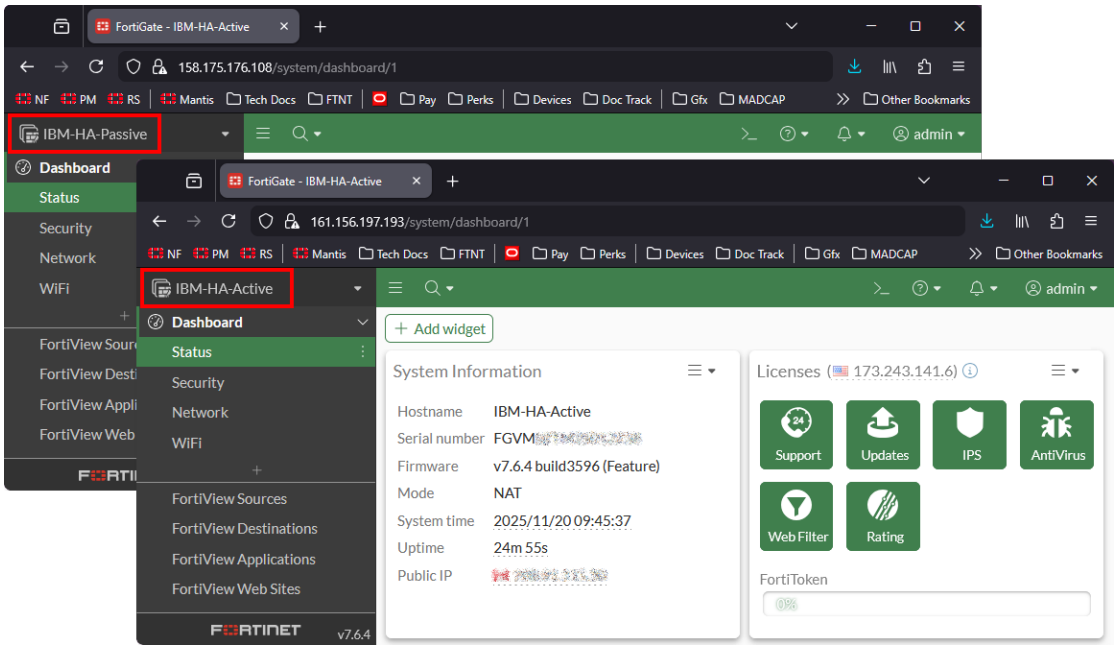
3. Use the public IP address to access and license both the FortiGate-VM. The Fortiget_public_ip value states the IP address that will move between the FortiGates on Failover.
4. Use the admin username and the default admin password provided in the outputs for both FortiGate-VMs.

> If the secondary FortiGate-VM default or temporary password does not work after you have changed the Admin password on the Primary or active FortiGate-VM, use the new password set on Primary FortiGate-VM.

5. Login and license each of the FortiGate-VMs and allow time for the FortiGate-VM to reboot.



6. As well as allow time for the HA cluster to sync configuration fully after rebooting. Log in again to view the FortiGate-VM dashboard.

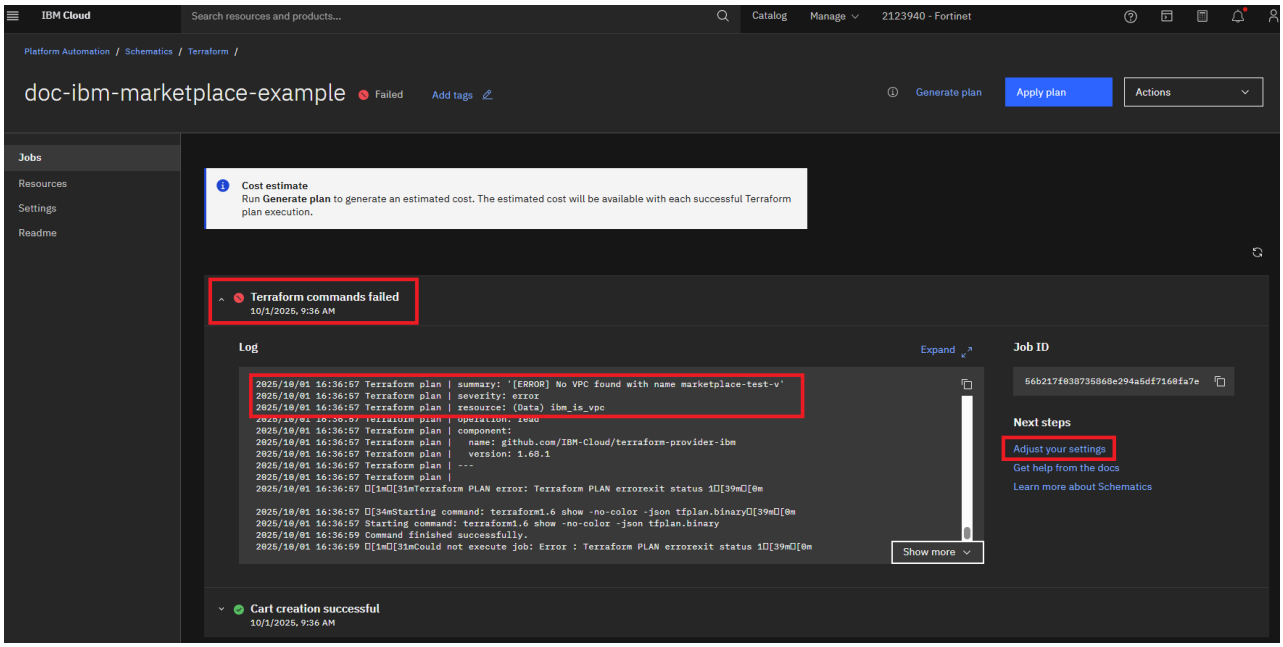


Troubleshooting

> ⚠ The IBM Cloud Schematics (webform) values must match the resources in your IBM VPC environment exactly. The results of mismatching values can result in licensing issues, FortiGate management issues, and HA instability. If the format of the values is accepted but the value itself is incorrect this will not be caught by terraform, IBM schematics, or FortiGate-VM.
>
> For example, if the HA management network is 10.242.3.0/24 and the webform value is 10.242.6.10, this format is correct but the value is incorrect and causes issues in management and licensing as HTTPS traffic is not routed correctly as well as HA cluster formation and communication.

1. When troubleshooting access issues review the assigned or used security group inbound rules and confirm that your public IP address is allowed to access.
2. When FortiGate-VM fails to license confirm that the security group is not restricting access to directregistration.fortinet.com.
3. When troubleshooting Terraform deployment issues it is suggested to review the output of the schematics workspace. The error will be from Terraform stating the issue with the specific field and value that was used in that field.

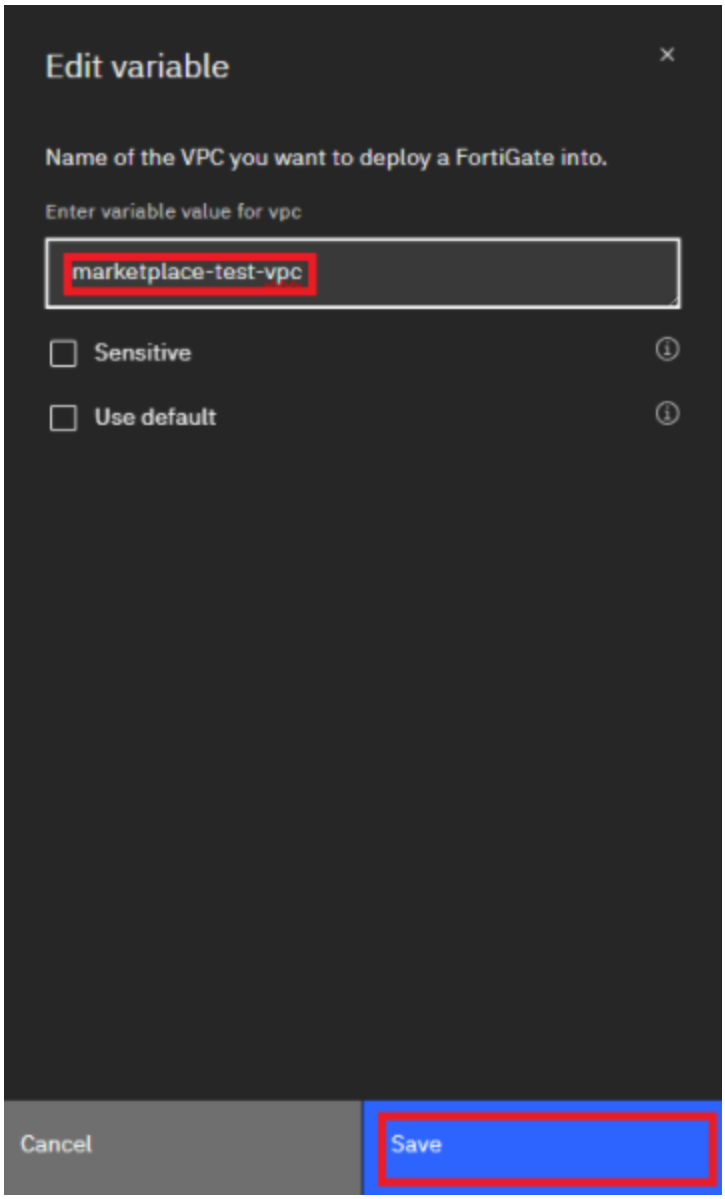
   Example of misspelled VPC name:



a. Select *Adjust your settings*.

b. Then select the variable that has the issue, in this example the VPC name is incorrect.

c. Select the vertical three dots and then select *Edit* to change the value of variable.



IBM Cloud Catalog - HA Active Passive - Two Zones

FortiOS supports deploying FortiGate-VM bring your own license (BYOL) for IBM Cloud. IBM Cloud users can purchase and deploy FortiGate-VMs. The following describes the steps on how to deploy an Active-Passive (A-P) HA cluster in two zones. This template makes use of the FortiGate IBM Cloud Connector to failover in the event of a VM disruption. After the active VM is back up, it will take over as active once again.

Prerequisites:

- A VPC
- Four subnets in each zone (eight total subnets):
  - Two public subnets with a public gateway attached, one in each zone
  - Two HA management subnets with a public gateway attached, one in each zone
- An SSH key
- Two FortiOS BYOL licenses

Terraform deploys the following components:

- Two FortiGate BYOL instances with four NICs each, one in each subnet in each zone.
- Two floating Public IP addresses: one attached to the HA management port of each FortiGate.
- Public Address Range and PAR specific routing table.
- One log disk per FortiGate.
- A basic bootstrap configuration with HA support.

Privileges

This list is a guideline and not an exhaustive list. Please review your environment and add or remove privileges as needed to fit your environment.

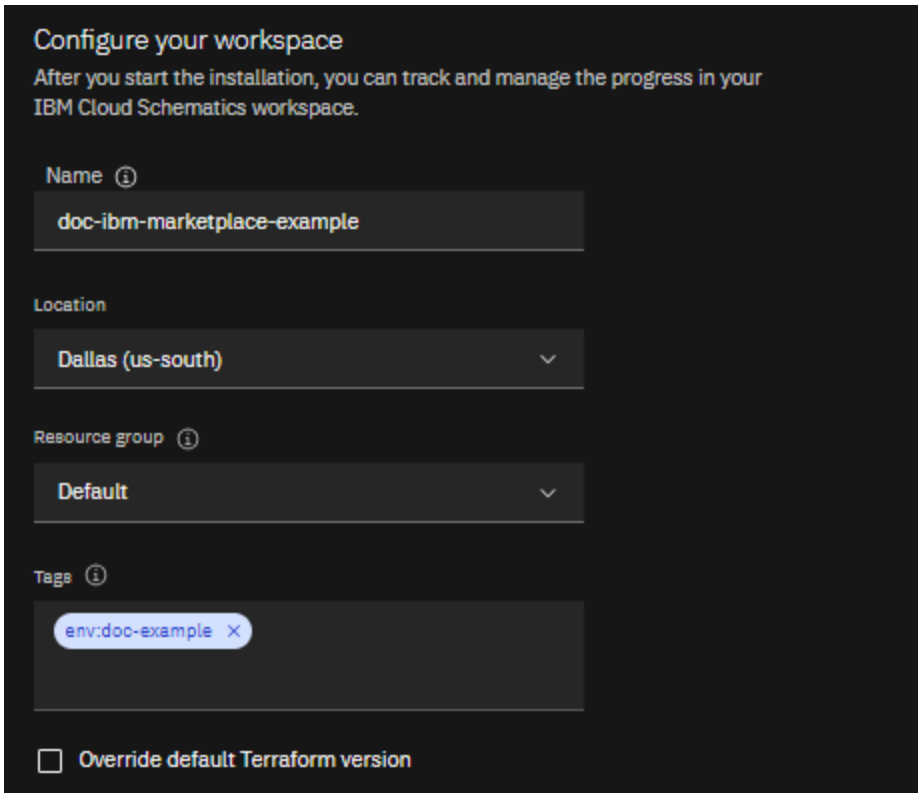
IBM Cloud Service	Actions (create / read / list / attach / etc.)
VPC (Networking)	Read existing VPCs, subnets (get / list). Attach network interfaces to subnets. Manage public IPs (allocate/attach).
Compute / Instances	Create VM instance. *Specify image (BYOL image). Attach NICs, disks. Manage instance lifecycle (start / stop / delete).
Block Storage / Volume	Provision / create volume. Attach to VM. Delete afterwards.
SSH Key resource	List / read SSH keys. If creating them (but in this case, it's preexisting), then ssh_keys.create would be needed.
IAM roles / resource group	Read resource group. Possibly manage tags / resource group.
General read / list permissions	Read images. Read region / zones / quotas. Read resource limits / service status.

IBM Cloud Service	Actions (create / read / list / attach / etc.)
Public Address Range	Read / Create / delete / bind and unbind

Marketplace product

To deploy FortiGate-VM on IBM Cloud marketplace:

1. Login into IBM Cloud (https://cloud.ibm.com/) and then access the Catalog (https://cloud.ibm.com/catalog)
2. Search for or use this link to deploy FortiGate-VM from the IBM Catalog: Fortinet FortiGate Next-Generation Firewall - HA Cross Zone.
3. In the *Configure your workspace*, configure the *Name*, *Location*, *Resource group*, and *Tags* to fit your environment.
   Leave *Override default Terraform version* unchecked.



4. Set the input Variables section:

Variable	Description
`cluster_name`	Set as desired. This example leaves it as the default.
`ibmcloud_api_key`	Enter your API key.
`profile`	The instance type used in the deployment.

Variable	Description
region	Set as desired. This example leaves it as the default.
security_group	Enter your desired security group.
ssh_public_key	Enter your SSH key that is configured in your account on IBM Cloud.
subnet1_zone1	Enter the public subnet ID of the subnet in the VPC that the FortiGate-VM will be deployed into.
subnet2_zone1	Enter the private subnet ID of the subnet in the VPC that the FortiGate-VM will be deployed into.
subnet3_zone1	Enter the ha-sync subnet ID of the subnet in the VPC that the FortiGate-VM will be deployed into.
subnet4_zone1	Enter the ha-mgmt subnet ID of the subnet in the VPC that the FortiGate-VM will be deployed into.
subnet1_zone2	Enter the public subnet ID of the subnet in the VPC that the FortiGate-VM will be deployed into.
subnet2_zone2	Enter the private subnet ID of the subnet in the VPC that the FortiGate-VM will be deployed into.
subnet3_zone2	Enter the ha-sync subnet ID of the subnet in the VPC that the FortiGate-VM will be deployed into.
subnet4_zone2	Enter the ha-mgmt subnet ID of the subnet in the VPC that the FortiGate-VM will be deployed into.
user_data	Configure to load your desired user configuration.
vpc	Enter the name of the VPC that the FortiGate-VM will be deployed into.
zone1	Enter the zone in the region that the Active FortiGate-VM will be deployed into.
Zone2	Enter the zone in the region that the Passive FortiGate-VM will be deployed into.

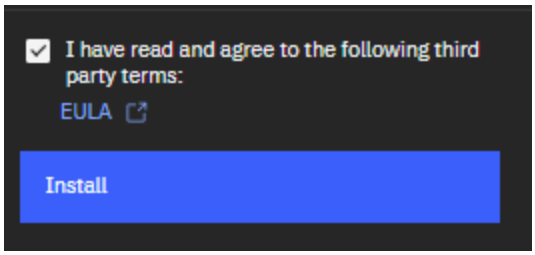
In addition to the above list of inputs, the following must also be configured:

- FGT1_PORT4_MGMT_GATEWAY
- FGT1_STATIC_IP_PORT1
- FGT1_STATIC_IP_PORT2
- FGT1_STATIC_IP_PORT3
- FGT1_STATIC_IP_PORT4
- FGT2_PORT4_MGMT_GATEWAY
- FGT2_STATIC_IP_PORT1
- FGT2_STATIC_IP_PORT2
- FGT2_STATIC_IP_PORT3
- FGT2_STATIC_IP_PORT4
- NETMASK

FGT1_PORT4_MGMT_GATEWAY	Gateway for Port 4 (HA management port) on the primary (ACTIVE) FortiGate.	string	10.242.3.1
FGT1_STATIC_IP_PORT1	Static IP assignment for Port 1 of the Primary (ACTIVE) FortiGate.	string	10.242.0.10
FGT1_STATIC_IP_PORT2	Static IP assignment for Port 2 of the Primary (ACTIVE) FortiGate.	string	10.242.1.10
FGT1_STATIC_IP_PORT3	Port used for the HA Heartbeat mechanism.	string	10.242.2.10
FGT1_STATIC_IP_PORT4	HA management port.	string	10.242.3.10
FGT2_PORT4_MGMT_GATEWAY	Gateway for Port 4 (HA management port) on the secondary (PASSIVE) FortiGate.	string	10.242.67.1
FGT2_STATIC_IP_PORT1	STATIC IP Assignment for Port 1 on the Secondary (PASSIVE) FortiGate.	string	10.242.64.10
FGT2_STATIC_IP_PORT2	STATIC IP Assignment for Port 2 on the Secondary (PASSIVE) FortiGate.	string	10.242.65.10
FGT2_STATIC_IP_PORT3	Port used for the HA Heartbeat mechanism.	string	10.242.66.10
FGT2_STATIC_IP_PORT4	HA management port.	string	10.242.67.10

These values are gained from the network configuration of the subnets created in your VPC. This example uses a netmask of 255.255.255.0 and 10.242.0.0/16 address space. 10.242.3.1 is the value for zone1 FortiGate-VM HA Management gateway and 10.242.67.1 for zone2 FortiGate-VM HA Management gateway.

5. Read and Accept the EULA then click install.



6. Follow the workspace progress until the deployment is complete and successful.

Validating the deployment

This validation example uses a webserver deployed in the private subnet in each zone. As the primary FortiGate-VM experiences a disruption(shutdown or restart in this example), the second FortiGate starts to process network traffic and the webserver in the second zone will be used.

After the deployment has created the Public Address Range, you can send traffic to one of the Public Addresses with in the range. For this example, **169.45.12.24** was selected.

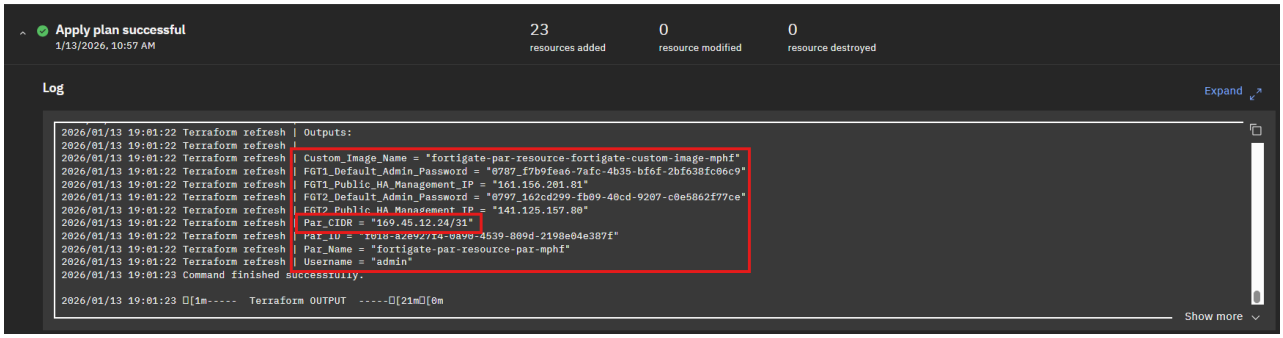
Review the PAR configuration

1. Log into the IBM Console
2. Navigate to *Network > Routing Tables > fortigate-par-resource-par-rtb-mphf*

3. The internal IP from the public subnet in zone1 should be under the *next hop* column. In this example it is 10.242.0.10.

Access the FortiGate-VM

1. After the deployment completes successfully you can connect to the FortiGate-VMs using the management port information found in the logs of the workspace schematics. There will be a HA management interface public for the Primary or Active and the secondary FortiGate-VM's.
2. In the log section scroll to the bottom and review the information contained in the outputs of the Terraform run.



Use the public IP address listed in FGT#_Public_HA_Management_IP for the respective FortiGate to access and license both FortiGate-VMs.

3. Use the admin username and the default admin password provided in the outputs for both FortiGate-VMs.

> If the secondary FortiGate-VM default or temporary password does not work after you have changed the Admin password on the Primary or active FortiGate-VM, use the new password set on Primary FortiGate-VM.

4. Login and license each of the FortiGate-VMs and allow time for the FortiGate-VM to reboot.
5. Also allow time for the HA cluster to sync configuration fully after rebooting. Log in again to view the FortiGate-VM dashboard.

Configure a Virtual IP and Firewall Policy

1. Edit and paste the following VIP configuration into the Active FortiGate:

```
config firewall vip
    edit "IBM_VIP_To_Internal_Server"
        set extip "169.45.12.24"
        set mappedip "10.242.1.7"
        set extintf "port1"
```

```
   next
end
```

Where `extip` is an IP from the Public Address Range and `mappedip` is the internal IP of Webserver1 in Zone1.

2. Edit and paste the following Firewall configuration into the Active FortiGate:

```
config firewall policy
    edit 1
        set name "tovip"
        set srcintf "port1"
        set dstintf "port2"
        set action accept
        set srcaddr "all"
        set dstaddr "IBM_VIP_To_Internal_Server"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set av-profile "default"
        set nat enable
    next
end
```

3. Edit and paste the following VDOM exception configuration into the Active FortiGate:

```
config system vdom-exception
    edit 0
        set object firewall.vip
    next
end
```

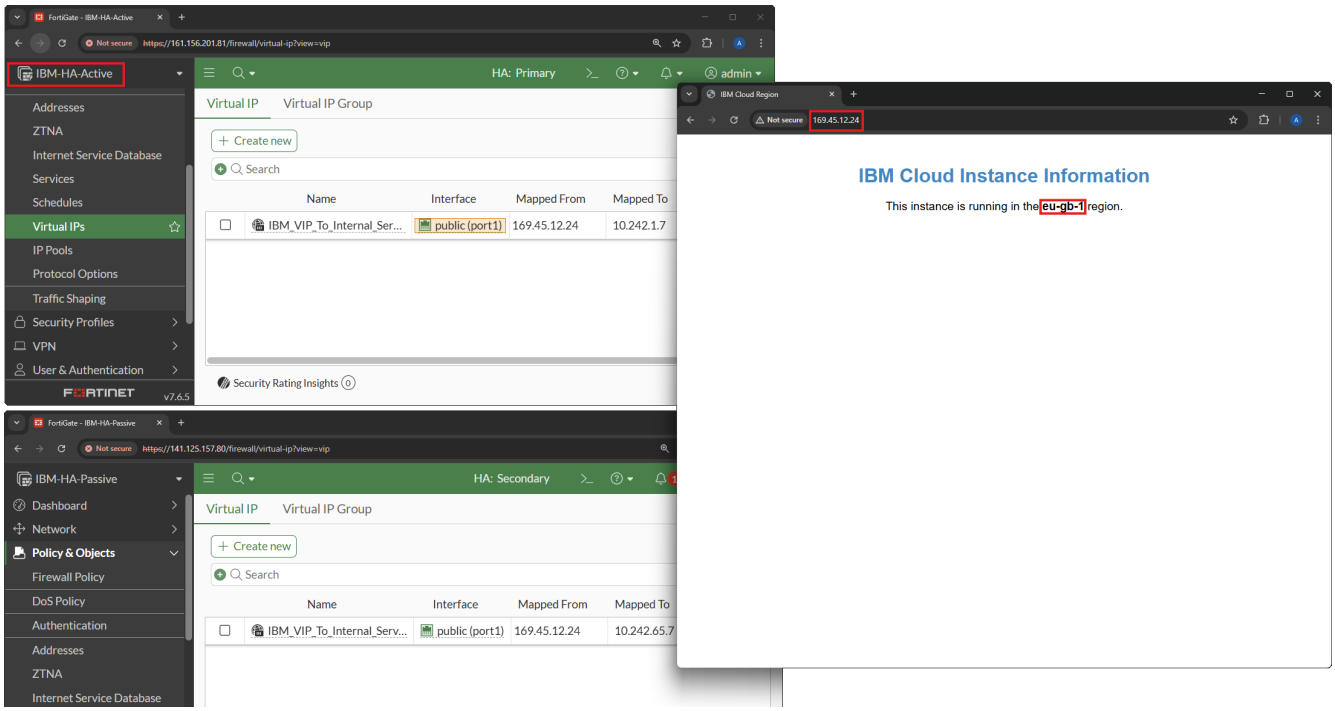
Note that this will prevent the HA configuration sync from pushing the incorrect VIP internal IP of the webserver in Zone2.

4. Edit and paste the following VIP configuration into the Passive FortiGate:

```
config firewall vip
    edit "IBM_VIP_To_Internal_Server"
        set extip "169.45.12.24"
        set mappedip "10.242.65.7"
        set extintf "port1"
    next
end
```

Where `extip` is an IP from the Public Address Range and `mappedip` is the internal IP of Webserver2 in Zone2.

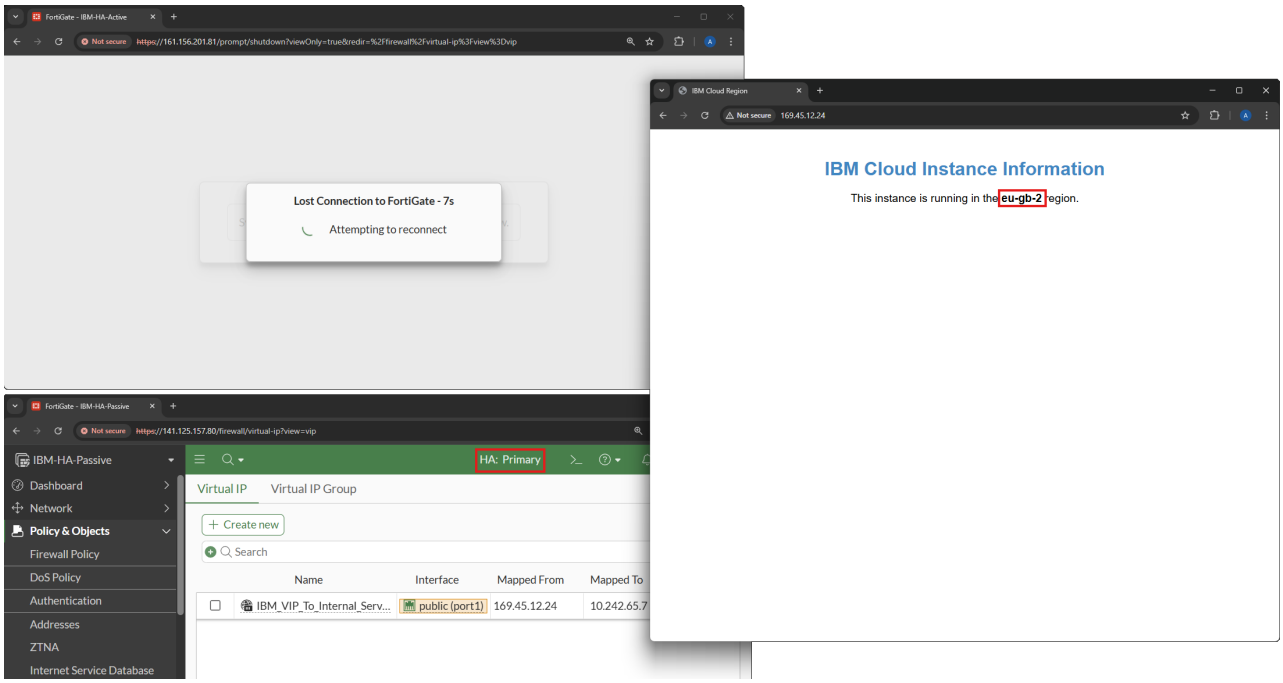
The Public Address Range public IP should now be forwarding traffic to the internal webserver in subnet2_zone1.



Validating Failover

1. Restart or shutdown the active FortiGate-VM in Zone1.
2. Review the PAR configuration – it should now state the internal IP of the FortiGate-VM in Zone2.

3. The Passive FortiGate will have assumed role of Primary.
4. Refresh the webpage displaying the webserver in Zone1, this should now be pointing to Zone2 webserver over the same PAR Public IP.

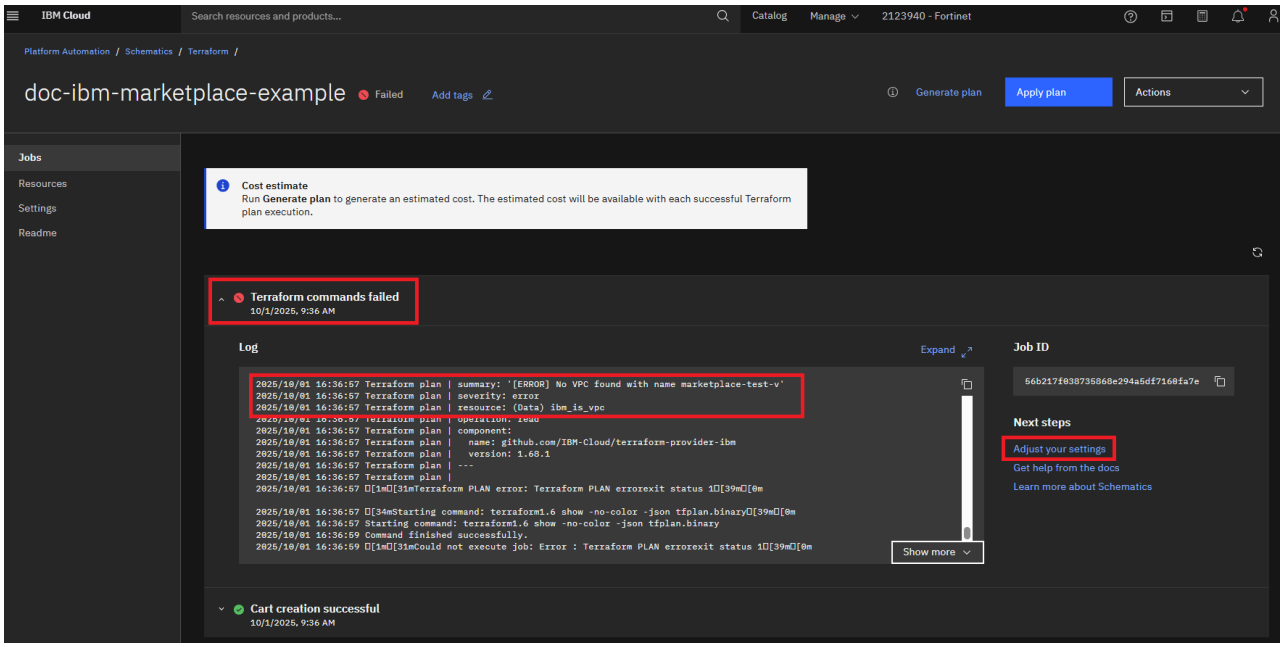


Troubleshooting

> ⚠ The IBM Cloud Schematics (webform) values must match the resources in your IBM VPC environment exactly. The results of mismatching values can result in licensing issues, FortiGate management issues, and HA instability. If the format of the values is accepted but the value itself is incorrect this will not be caught by terraform, IBM schematics, or FortiGate-VM.
>
> For example, if the HA management network is 10.242.3.0/24 and the webform value is 10.242.6.10, this format is correct but the value is incorrect and causes issues in management and licensing as HTTPS traffic is not routed correctly as well as HA cluster formation and communication.

1. When troubleshooting access issues review the assigned or used security group inbound rules and confirm that your public IP address is allowed to access.
2. When FortiGate-VM fails to license confirm that the security group is not restricting access to directregistration.fortinet.com.
3. When troubleshooting Terraform deployment issues it is suggested to review the output of the schematics workspace. The error will be from Terraform stating the issue with the specific field and value that was used in that field.

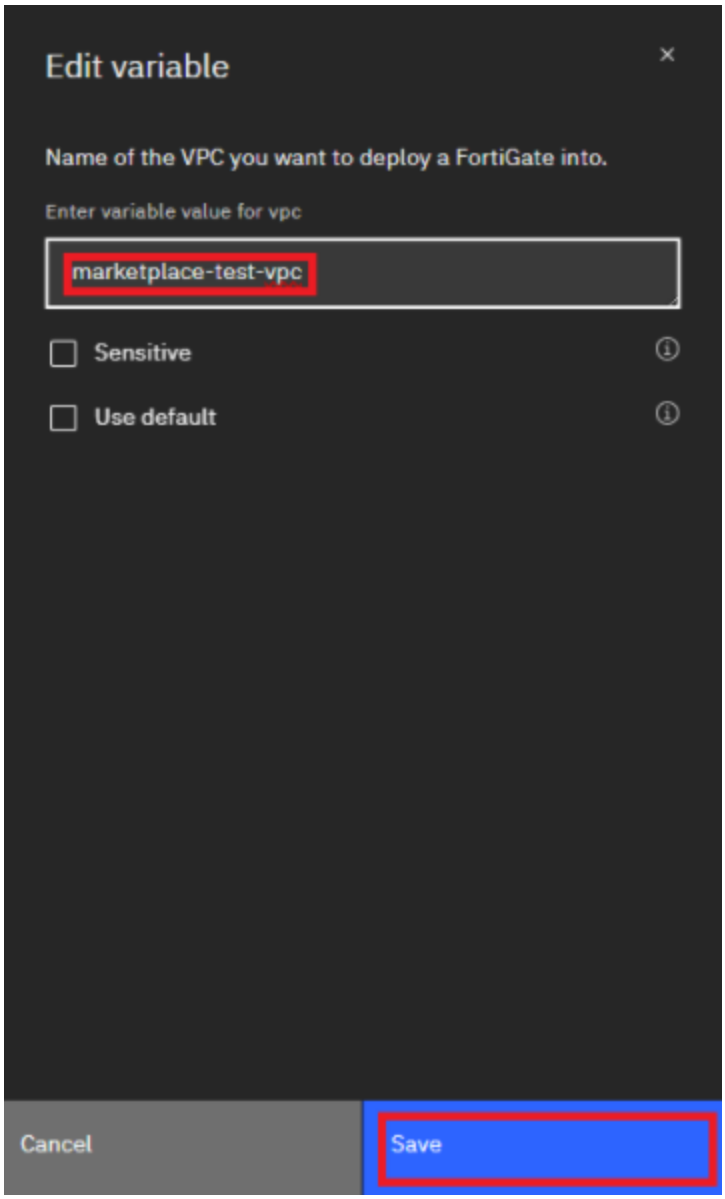
   Example of misspelled VPC name:



a. Select *Adjust your settings*.

b. Then select the variable that has the issue, in this example the VPC name is incorrect.

c. Select the vertical three dots and then select *Edit* to change the value of variable.


Edit variable
Name of the VPC you want to deploy a FortiGate into.
Enter variable value for vpc
marketplace-test-vpc
Sensitive
Use default
Cancel
Save

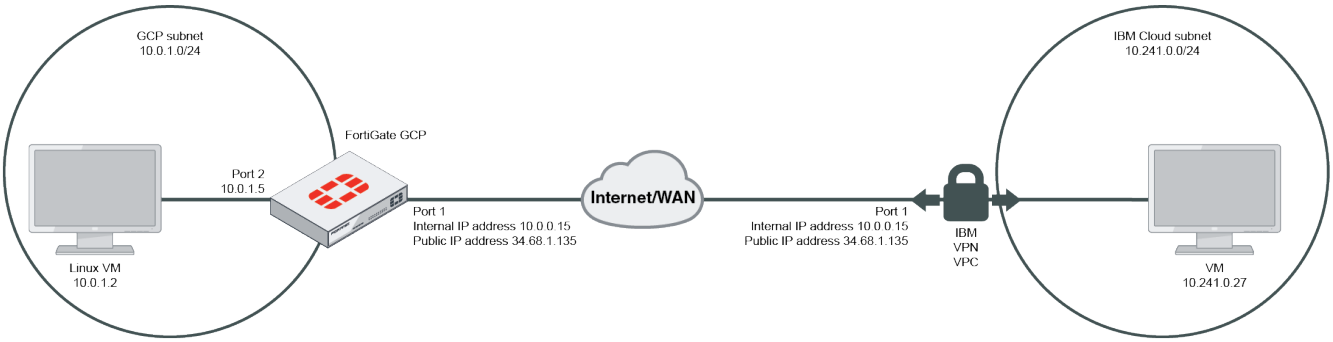
SDN Connector integration with IBM Cloud

See the FortiOS Administration Guide.

VPN for FortiGate-VM on IBM Cloud

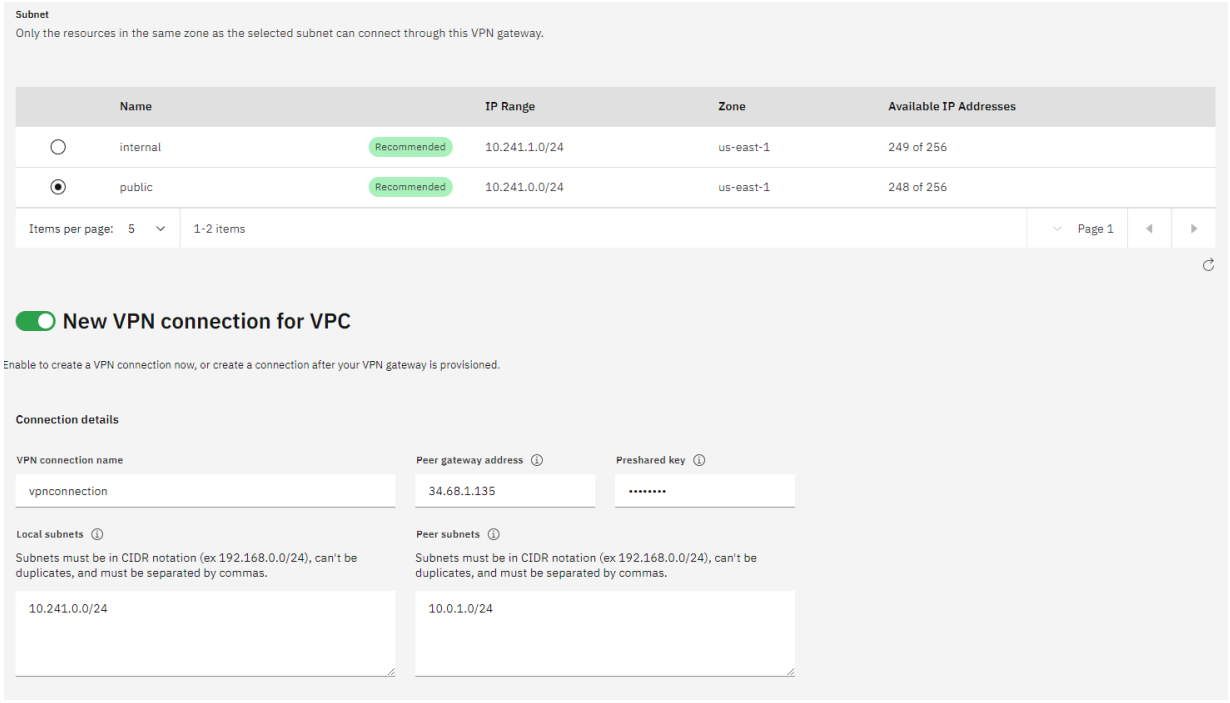
Connecting a FortiGate to an IBM Cloud VPC VPN

This example provides sample configuration of a site-to-site VPN connection from a FortiGate-VM deployed on Google Cloud Platform (GCP) to an IBM Cloud VPC VPN. Since IBM Cloud VPN requires a peer gateway IP address, it cannot be dialed up to and requires a public IP address from the FortiGate. Therefore, this example uses GCP as the secondary site. The secondary site can be at other locations, such as AWS, Azure, or your corporate network. Replace with your desired environment. The following shows the topology for this example:



To create the VPN gateway on IBM Cloud:

1. In the IBM Cloud management console, create a gateway. In the *VPN gateway name* field, enter the desired name.
2. From the *Virtual private cloud* dropdown list, select the desired VPC.
3. (Optional) From the *Resource group* dropdown list, select the desired group.
4. Under *Region*, select the desired region.
5. Under *Subnet*, select the public subnet.
6. Enable *New VPN connection for VPC*, then configure the VPN connection:
   a. In the *VPN connection name* field, enter the desired name.
   b. In the *Peer gateway address* field, enter the FortiGate public gateway IP address. In this example, the FortiGate is deployed on GCP, and its public gateway IP address is 34.68.1.135.
   c. In the *Preshared key* field, enter the desired key.
   d. Under *Local subnets*, enter the IBM Cloud internal subnet. In this example, it is 10.241.0.0/24.
   e. Under *Peer subnets*, enter the secondary site internal subnet. In this example, the GCP internal subnet is 10.0.1.0/24.



f. Keep the *Dead peer detection* fields at their default values: *Action: Restart*, *Interval (sec): 2*, and *Timeout (sec): 10*.

g. Select *New IKE policy*:

i. In the *Name* field, enter the desired name.

ii. (Optional) From the *Resource group* dropdown list, select the desired group.

iii. Under *Region*, select the desired region.

iv. From the *IKE Version* dropdown list, select *1*.

v. From the *Authentication* dropdown list, select *sha1*.

vi. From the *Encryption* dropdown list, select *aes128*.

vii. From the *DH Group* dropdown list, select *5*.

viii. In the *Key Lifetime* field, enter *86400*.

ix. Click *Create IKE policy*.

h. Select *New IPsec policy*:

i. In the *Name* field, enter the desired name.

ii. (Optional) From the *Resource group* dropdown list, select the desired group.

iii. Under *Region*, select the desired region.

iv. From the *Authentication* dropdown list, select *sha1*.

v. From the *Encryption* dropdown list, select *aes128*.

vi. From the *DH Group* dropdown list, select *5*.

vii. In the *Key Lifetime* field, enter *43200*.

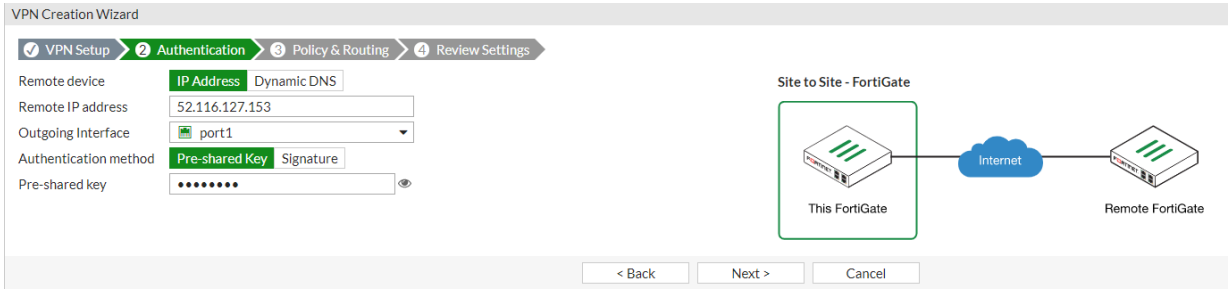
viii. Click *Create IPsec policy*.

To create the VPN connection in FortiOS:

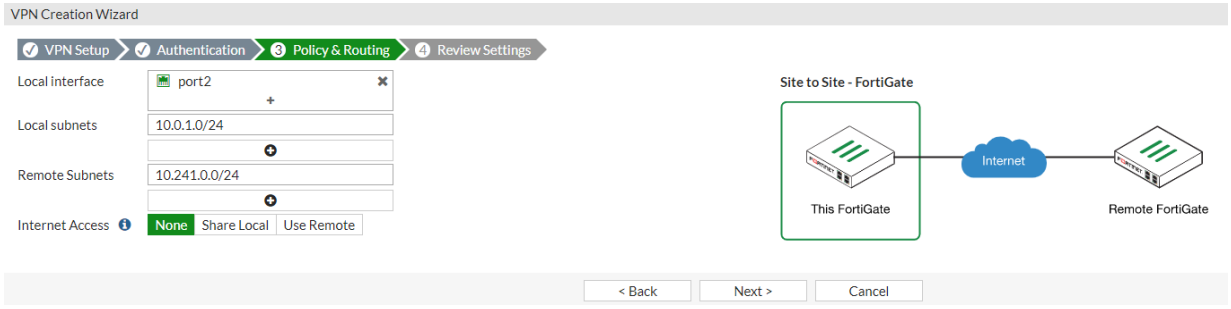
1. In FortiOS on the local FortiGate, go to *VPN* > *VPN Wizard*.
2. On the *VPN Setup* tab, configure the following:

a. In the *Name* field, enter the desired name.
b. For *Template type*, select *Site to Site*.
c. For *NAT Configuration*, select *No NAT between sites*.
d. For *Remote device type*, select *FortiGate*.

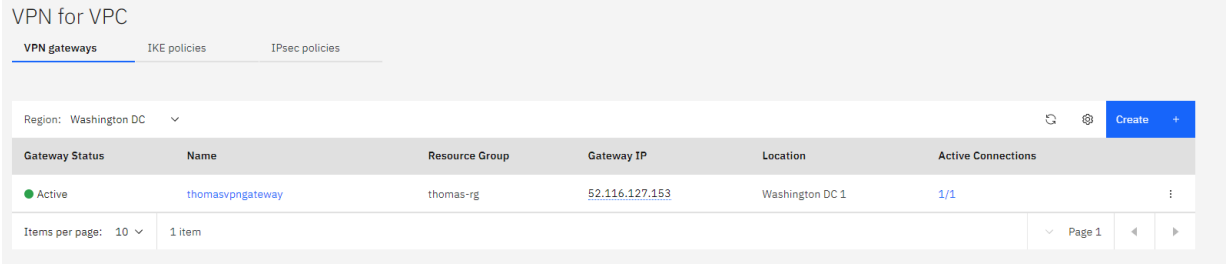
3. On the *Authentication* tab, configure the following:
   a. For *Remote device*, select *IP Address*.
   b. In the *Remote IP address* field, enter the IBM Cloud VPN gateway IP address. In this example, it is 52.116.127.153.
   c. For *Outgoing Interface*, allow FortiOS to automatically configure as port1.
   d. For *Authentication Method*, select *Pre-shared Key*.
   e. In the *Pre-shared Key* field, enter the desired key. Click *Next*.

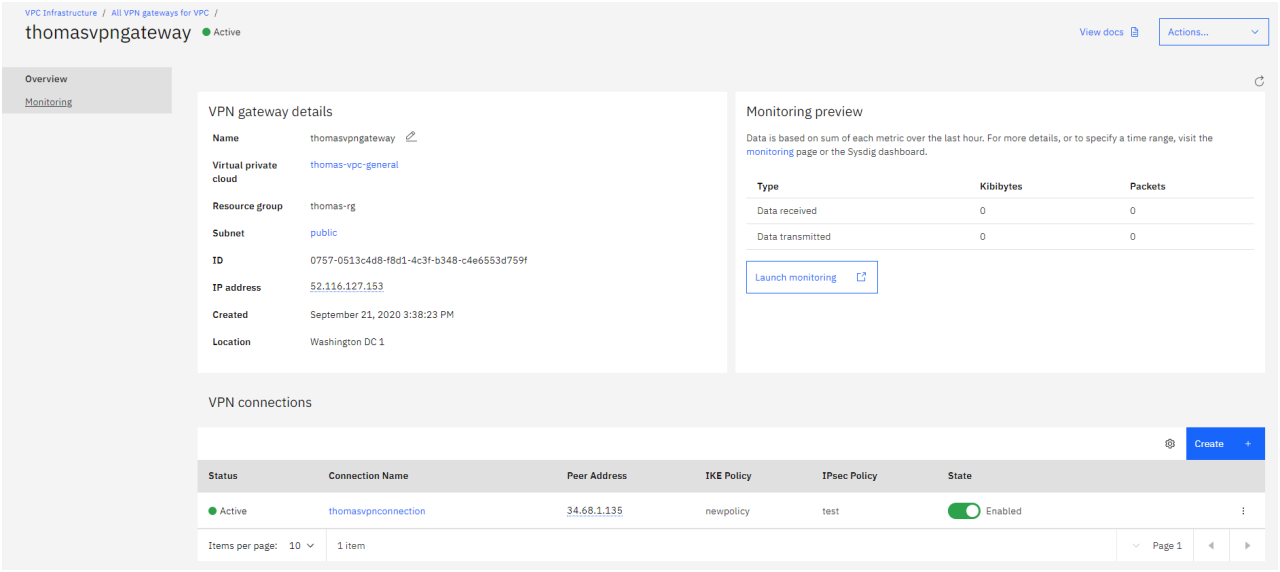


4. On the *Policy & Routing* tab, configure the following:
   a. For *Local interface*, select *port2*, the GCP internal network port.
   b. In the *Local subnets* field, enter the GCP internal subnet, *10.0.1.0/24*.
   c. In the *Remote Subnets* field, enter the IBM Cloud remote subnet. In this example, it is 10.241.0.0/24.
   d. For *Internet Access*, select *None*.

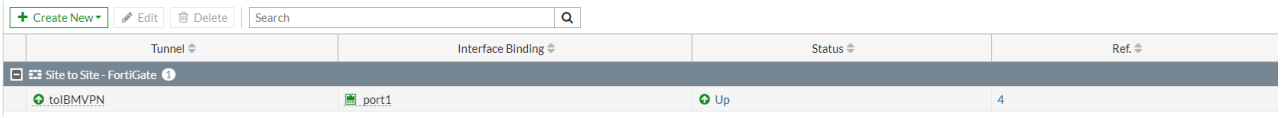


5. Proceed to create the VPN connection. After configuration, the VPN should automatically come up, and traffic can transverse. In the IBM Cloud console, you should see that the VPN gateway status is active and up.





FortiOS also shows that the VPN connection is up.



A GCP Linux client can ping a machine on the IBM Cloud VPC subnet.

```
root@thomas-script-ubuntu-internal:~# ifconfig
ens4: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1460
        inet 10.0.1.2  netmask 255.255.255.255  broadcast 0.0.0.0
        inet6 fe80::4001:aff:fe00:102  prefixlen 64  scopeid 0x20<link>
        ether 42:01:0a:00:01:02  txqueuelen 1000  (Ethernet)
        RX packets 4837  bytes 9646082 (9.6 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4473  bytes 450838 (450.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 122  bytes 10686 (10.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 122  bytes 10686 (10.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@thomas-script-ubuntu-internal:~# ping 10.241.0.27
PING 10.241.0.27 (10.241.0.27) 56(84) bytes of data.
64 bytes from 10.241.0.27: icmp_seq=1 ttl=253 time=37.2 ms
64 bytes from 10.241.0.27: icmp_seq=2 ttl=253 time=35.4 ms
^C
--- 10.241.0.27 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 35.483/36.386/37.289/0.903 ms
```

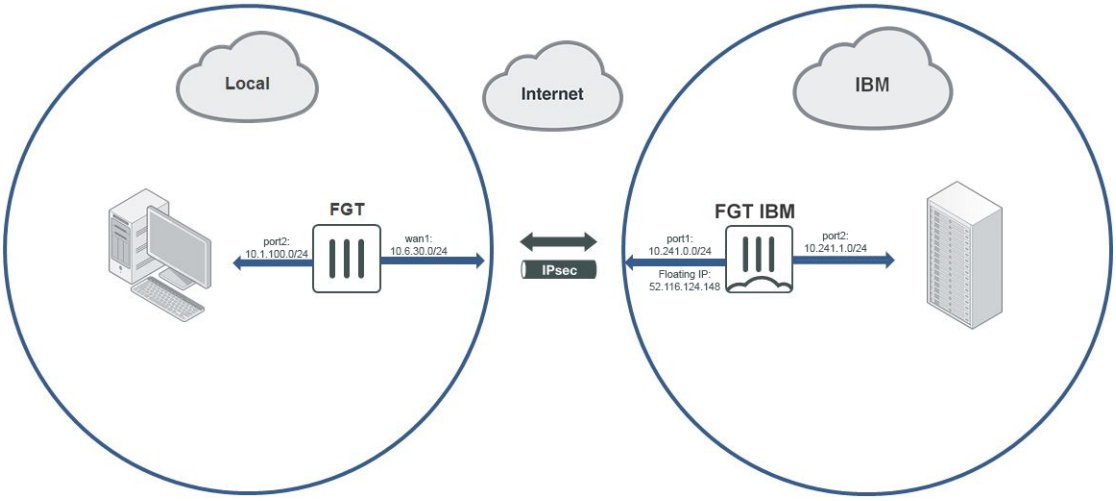
The following shows sniffer traffic.

```
SCRIPT-MASTER # diagnose sniffer packet any 'icmp' 4
interfaces=[any]
filters=[icmp]
11.688528 port2 in 10.0.1.2 -> 10.241.0.27: icmp: echo request
11.688578 toIBMVPN out 10.0.1.2 -> 10.241.0.27: icmp: echo request
11.723878 toIBMVPN in 10.241.0.27 -> 10.0.1.2: icmp: echo reply
11.723905 port2 out 10.241.0.27 -> 10.0.1.2: icmp: echo reply
```

Connecting a local FortiGate to an IBM Cloud FortiGate via site-to-site VPN

This guide provides sample configuration of a site-to-site VPN connection from a local FortiGate to an IBM FortiGate via site-to-site IPsec VPN with static routing. You can access resources that are protected behind a FortiGate on IBM from your local environment by using a site-to-site VPN.

The following depicts the network topology for this sample deployment:



The following prerequisites must be met for this configuration:

- A FortiGate located on (Gen 2) IBM Cloud Virtual Servers for VPC with some resources behind it. In this example, the IBM FortiGate has port1 connected to WAN and port2 connected to local LAN.
- An on-premise FortiGate. For your local environment, determine if your FortiGate has a publicly accessible IP address or if it is behind NAT. In this example, the on-premise FortiGate is behind NAT.

This configuration consists of the following steps:

1. Create a VPN on the local FortiGate to the IBM FortiGate.
2. Create a VPN on the IBM FortiGate to the local FortiGate.
3. Establish a connection between the FortiGates.

To create a VPN on the local FortiGate to the IBM FortiGate:

1. In FortiOS on the local FortiGate, go to *VPN* > *VPN Wizard*.
2. On the *VPN Setup* tab, configure the following:
   a. In the *Name* field, enter the desired name.
   b. For *Template Type*, select *Site to Site*.
   c. For *Remote Device Type*, select *FortiGate*.
   d. For *NAT Configuration*, select the appropriate option. In this example, since the local FortiGate is behind NAT, *This site is behind NAT* is selected. Click *Next*. For non-dialup situations where the local FortiGate has an external IP address, select *No NAT between sites*.

3. On the *Authentication* tab, configure the following:
   a. For *Remote Device*, select *IP Address*.
   b. In the *IP Address* field, enter the IBM FortiGate's floating IP address. In this example, it is 52.116.124.148.
   c. For *Outgoing Interface*, allow FortiOS to detect the interface via routing lookup.
   d. For *Authentication Method*, select *Pre-shared Key*.
   e. In the *Pre-shared Key* field, enter the desired key. Click *Next*.
4. On the *Policy & Routing* tab, configure the following:
   a. For *Local Interface*, select the desired local interface. In this example, port2 is selected. The *Local Subnets* field should autopopulate.
   b. In the *Remote Subnets* field, enter the remote subnet on the other side of the IBM FortiGate. In this example, it is 10.241.1.0/24.
   c. For *Internet Access*, select *None*.
5. Click *Create*. The VPN Wizard creates the following:
   - Firewall addresses for local and remote subnets
   - Firewall address groups containing the above firewall addresses
   - phase-1 and phase-2 interfaces
   - Static route and blackhole route
   - Two firewall policies: one for traffic to the tunnel interface and one for traffic from the tunnel interface

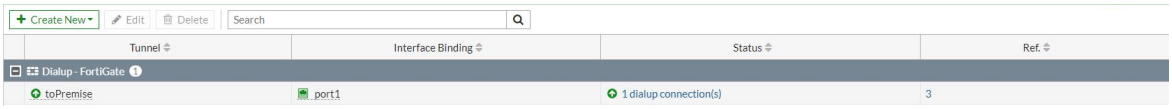
To create a VPN on the IBM FortiGate to the local FortiGate:

1. In FortiOS on the IBM FortiGate, go to *VPN > VPN Wizard*.
2. On the *VPN Setup* tab, configure the following:
   a. In the *Name* field, enter the desired name.
   b. For *Template Type*, select *Site to Site*.
   c. For *Remote Device Type*, select *FortiGate*.
   d. For *NAT Configuration*, select *This site is behind NAT*. This is the correct configuration since the IBM FortiGate has an floating IP address. Click *Next*.
3. On the *Authentication* tab, configure the following:
   a. For *Incoming Interface*, select the WAN-facing incoming interface. In this example, it is port1.
   b. For *Authentication Method*, select *Pre-shared Key*.
   c. In the *Pre-shared Key* field, enter the same key configured on the local FortiGate. Click *Next*.
4. On the *Policy & Routing* tab, configure the following:
   a. For *Local Interface*, select the desired local interface. In this example, port2 is selected. The *Local Subnets* field should then autopopulate.
   b. In the *Remote Subnets* field, enter the remote subnet on the other side of the local FortiGate. In this example, it is 10.1.100.0/24.
   c. For *Internet Access*, select *None*.
5. Click *Create*. The VPN Wizard creates the following:
   - Firewall addresses for local and remote subnets
   - Firewall address groups containing the above firewall addresses
   - phase-1 and phase-2 interfaces
   - Static route and blackhole route

- Two firewall policies: one for traffic to the tunnel interface and one for traffic from the tunnel interface

To establish a connection between the FortiGates:

1. The tunnels are down until you initiate a connection from the local FortiGate to the IBM FortiGate. In FortiOS on the local FortiGate, go to *Dashboard > Network* and click IPsec to expand the widget.
2. Right-click the phase-2 interface, and select *Bring Up > All Phase 2 Selectors*.
3. In FortiOS on the IBM FortiGate, go to *VPN > IPsec Tunnels* and verify that the connection is up.



The floating IP address can be considered as one to one to the FortiGate's IP address, even though the port IP address may be an internal IP address.

Change log

Date	Change description
2026-04-21	Initial release.

www.fortinet.com