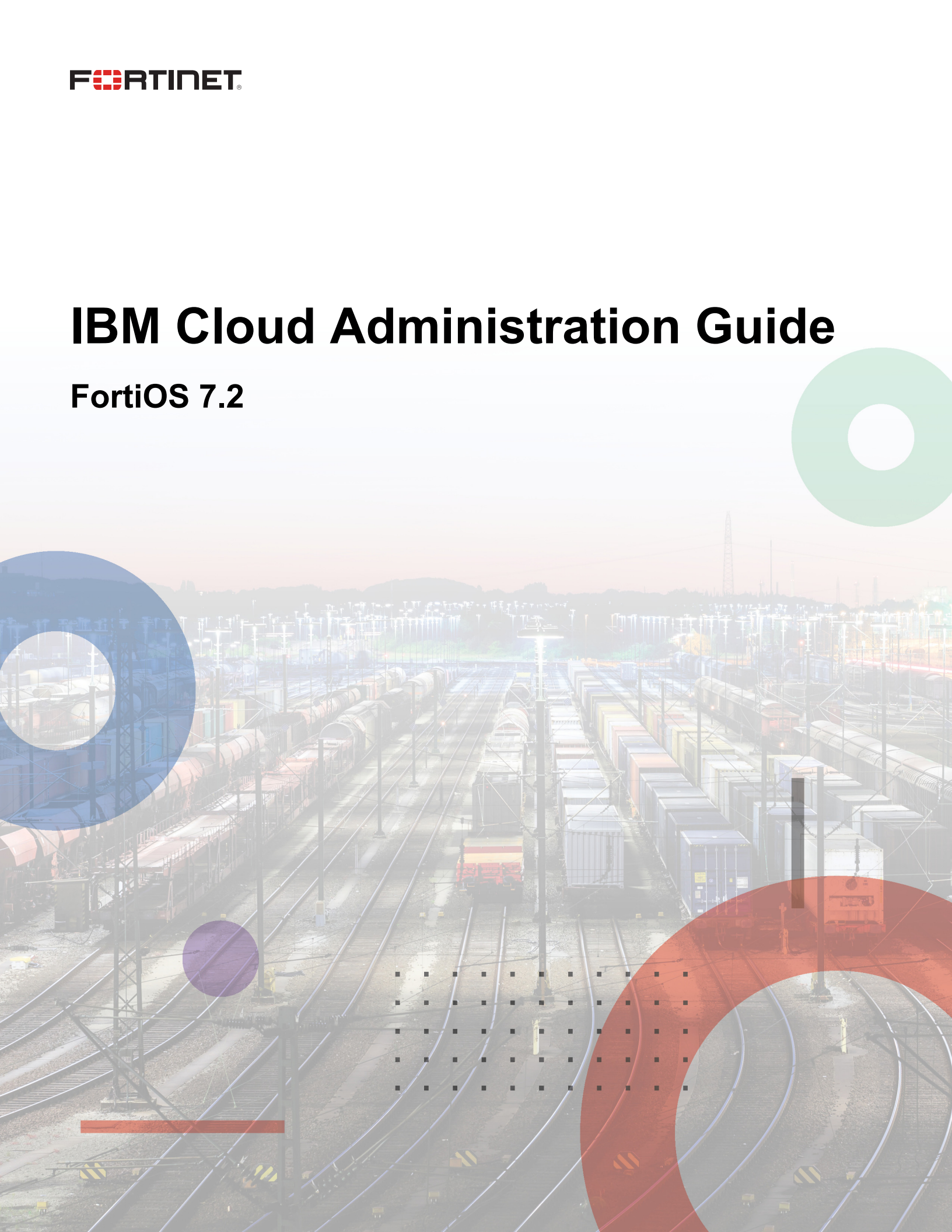


IBM Cloud Administration Guide

FortiOS 7.2



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



March 20, 2024

FortiOS 7.2 IBM Cloud Administration Guide

01-720-792266-20240320

TABLE OF CONTENTS

About FortiGate for IBM Cloud	4
Instance type support	4
Region support	4
Models	5
Licensing	5
Order types	5
Creating a support account	6
Deploying FortiGate-VM on IBM Cloud	7
HA for FortiGate-VM on IBM Cloud	12
Deploying FortiGate-VM A-P HA on IBM VPC Cloud (BYOL)	12
Example	12
SDN Connector integration with IBM Cloud	20
VPN for FortiGate-VM on IBM Cloud	21
Connecting a FortiGate to an IBM Cloud VPC VPN	21
Connecting a local FortiGate to an IBM Cloud FortiGate via site-to-site VPN	25
Change log	28

About FortiGate for IBM Cloud

By combining stateful inspection with a comprehensive suite of powerful security features, FortiGate next generation firewall (NGFW) 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.



FortiGate-VM for IBM Cloud only supports standalone node deployment.

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](#).

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.

Currently there is no specific preference on supported instance types.

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

Region support

FortiGate-VM is available for purchase in all the regions/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 BYOL models. See [Order types on page 5](#).

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 7.2.5, 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 (VDMs) by default. To add VDMs, you must separately purchase perpetual VDOM addition licenses. You can add and stack VDMs up to the maximum supported number after initial deployment.

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 VDMs, 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 5](#).

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


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 *Download > VM Images*.
 - c. From the *Select Platform* dropdown list, select *IBM VPC Cloud*.
 - d. Download the FortiGate-VM deployment file (FGT_VM64_IBM-v7.2.X.F-buildXXXX-FORTINET.out).
 - 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 IBM 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.

VPC Infrastructure / All custom images for VPC



Gen 2 compute

This custom image will be created for use with generation 2 compute resources. It cannot be used with generation 1 instances.

[Switch to Gen 1 compute](#)

Import custom image

Name

fortios1705

Resource group

The resource group can't be changed after the custom image is created

[Learn about resource groups](#)

Default

[View all resource groups](#)

Tags

Examples: env:dev, version-1

Region

Dallas

Frankfurt

London

Washington DC

Select your Cloud Object Storage bucket and select your image file below. [How to upload to Cloud Object Storage.](#)

Images must be a qcow2 file type, 100GB or less and cloud-init enabled.

Cloud Object Storage instances	Location	Bucket
thomasobjectstore	us-east	thomasbucket

Prefix filter

Name	Size	Last Modified
fortios.qcow2	58.63 MB	July 9, 2020 12:23:19 PM

Items per page: 10 1 item Page 1

Operating system

CentOS
7.x - Minimal Install

Debian GNU/Lin...
debian-8-amd64

Red Hat Enterpr...
7.x - Minimal Install

Ubuntu Linux
ubuntu-16-04-amd64

Windows Server
windows-2012-amd

Summary United States

1 Image \$0.01

0.06 GB

Apply a code

Apply

Total monthly cost* \$0.01
estimated

Import custom image

Get sample API call

Add to estimate

Need help?
[Contact IBM Cloud Sales](#)
[View docs](#)

Terms
[Virtual Server](#)
[Virtual Private Cloud](#)
[Block Storage](#)

FEEDBACK

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 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" }
}
```

IBM Cloud

QCatalogDocsSupportManage🔗📅✍️🔔👤

New virtual server for VPC

Name

fosinstance

Virtual private cloud

thomas-vpc-general

Resource group

The resource group can't be changed after the virtual server instance is created
[Learn about resource groups](#)

Default

[View all resource groups](#)

Tags ⓘ

Examples: env:dev, version-1

Location

Washington DC ✓
Washington DC 1

Image

CentOS
7.x - Minimal Install

Red Hat Enterprise Linux
7.x - Minimal Install

Windows Server
2016 Standard Editi

Catalog image
[Select catalog image](#)

Debian GNU/Linux
9.x Stretch/Stable - Minimal Install

Ubuntu Linux
18.04 LTS Bionic Be

fortios1705 ✓
[Change image](#)

Popular profilesAll profiles

Balanced
Best for common cloud workloads

8 vCPUs

32 GB RAM

16 Gbps

Compute ✓
Best for workloads with intensive CPU demands

2 vCPUs

4 GB RAM

4 Gbps

Memory
Best for memory intensive workloads

2 vCPUs

16 GB RAM

4 Gbps

SSH keys

thomas-myfirstkeypair

New key +

User data (optional) ⓘ

Paste user data

Import user data ⬇

Boot volume

VolumeSizeMaxThroughputEncryptionAuto

SummaryUnited States

1 Virtual server instance\$0.09/hr

2 vCPUs
4 GB RAM
4 Gbps
Custom image

Boot volume\$0.02/hr

100 GB

Network interfaceprovided

Apply a code

Apply

Subtotal\$78.04

Sustained usage discount ⓘ-\$6.58

Total monthly cost*\$71.46
estimated

Create virtual server instance

Get sample API call</>

Add to estimate

Need help?
[Contact IBM Cloud Sales](#)
[View docs](#)

Terms
[Virtual Server](#)
[Virtual Private Cloud](#)
[Block Storage](#)

FEEDBACK

7. Attach a floating IP address to the instance NIC.
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://thomasgabucket2.s3.amazonaws.com/FGVM08TM20004028.lic
>> Cloudinit download license successfully
>> Cloudinit trying to get config script from:
    https://thomasgabucket2.s3.amazonaws.com/config2.txt
>> Cloudinit download config script successfully
>> Found metadata source: ibm
>> Trying to install vmlicense ...
>> Run config script
>> Finish running script
>> FGVM08TM20004028 $ config system global
>> FGVM08TM20004028 (global) $ set hostname ibmcloud
>> FGVM08TM20004028 (global) $ end

get system status
Version: FortiGate-VM64-IBM v7.2.0,buildXXXX,200708 (interim)
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: FGVM08TM20004028
IPS Malicious URL Database: 1.00001(2015-01-01 01:01)
License Status: Valid
License Expiration Date: 2021-05-15
VM Resources: 2 CPU/8 allowed, 3689 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: Thu Jul 9 15:14:00 2020
```

HA for FortiGate-VM on IBM Cloud

The following topic provides an overview of High Availability (HA) configuration when using FortiGate-VM for IBM Cloud:

- [Deploying FortiGate-VM A-P HA on IBM VPC Cloud \(BYOL\) on page 12](#)

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 mode is protecting. The administrator uses a virtual IP address (VIP) to access Ubuntu, the web, and has traffic inspected for EICAR.

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

In the following example you will configure 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. Make sure a *Public Gateway* is attached to the *Public* subnet

Subnets in this VPC				
Q Search items				
Name	Status	Location	IP range	Public gateway
public	Available	Washington DC 3	10.241.128.0/24	
internal	Available	Washington DC 3	10.241.129.0/24	—
management	Available	Washington DC 3	10.241.130.0/24	
heartbeat	Available	Washington DC 3	10.241.131.0/24	—

VPC Infrastructure / Routing tables / **ftnt-demo-default** - [View docs](#) [Actions...](#)

Overview Subnets

Routing table details

Name	Virtual private cloud	Attached subnets	Routes
ftnt-demo-default	ftntdemo-havpc	1	1
Created	ID	Traffic type	
November 20, 2020 3:10:05 PM	r014-8554855-8550-8550-8554-8550-8550	Egress	

Routes

State	Destination	Action	Type	Next hop	Location
Stable	0.0.0.0/0	Deliver	IP address	10.241.129.4	Washington DC 3

2. Configure two route tables:

- Internal:** This route table:
 - Needs to be the IBM default route table for the VPC.
 - Has a route for all traffic to the internal subnet IP of the primary FortiGate.
 - Applies to the internal subnet.

If you have not deployed FortiGate, return to this step after deployment.

- Open:** This route table can have no routes, and can be applied to the *Public*, *Management*, and *Heartbeat* subnets.



Non-default route tables cannot be used for the internal subnet's route table failover in IBM VPC at this time.

Routing tables for VPC

Search items

Name	Default	Traffic type	Routes	Attached subnets
ftnt-demo-default	Default	Egress	2	1
ftnt-demo-non-default		Egress	0	3

Items per page: 10 1-2 of 2 items 1 of 1 page

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.

Network interfaces ⓘ						
Interface	Subnet name	Private IP	Floating IP	Security groups	Allow IP spoofing	
eth0	public	10.241.128.4		turkey-unaware-harmonize-versus	Enabled	
eth1	internal	10.241.129.4	—	turkey-unaware-harmonize-versus	Enabled	
eth2	heartbeat	10.241.131.4	—	turkey-unaware-harmonize-versus	Enabled	
eth3	management	10.241.130.4	—	turkey-unaware-harmonize-versus	Enabled	

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 xxxxxxxxx
    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 xxxxxxxxx
    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

```

```

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.

- Configure the vdom-exception on the primary FortiGate to automatically with the secondary FortiGate.
- 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
  next
end

```

```

        set nat enable
    next
end

```

5. Configure the SDN 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 the 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-aafalaecebbe/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
```

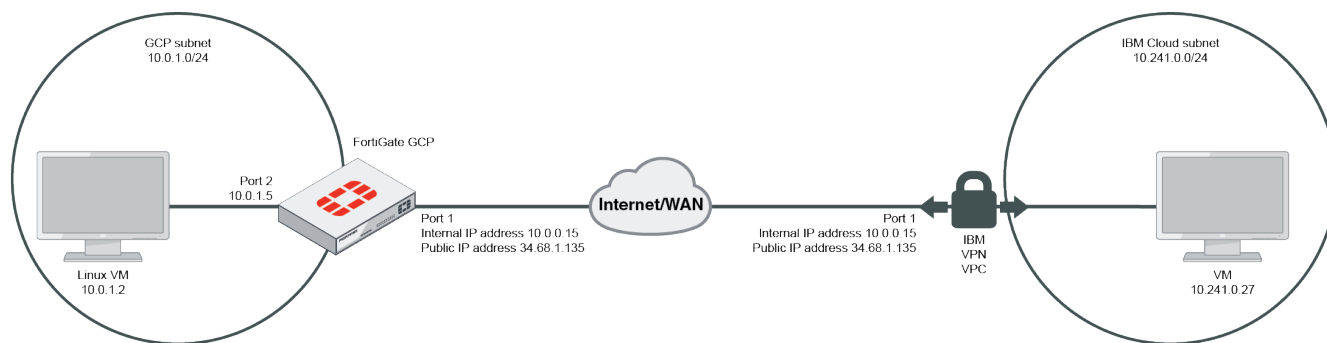
SDN Connector integration with IBM Cloud

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.

Subnet
Only the resources in the same zone as the selected subnet can connect through this VPN gateway.

	Name		IP Range	Zone	Available IP Addresses
<input type="radio"/>	internal	Recommended	10.241.1.0/24	us-east-1	249 of 256
<input checked="" type="radio"/>	public	Recommended	10.241.0.0/24	us-east-1	248 of 256

Items per page: 5 1-2 items Page 1

New VPN connection for VPC

Enable to create a VPN connection now, or create a connection after your VPN gateway is provisioned.

Connection details

VPN connection name: vpnconnection

Peer gateway address: 34.68.1.135

Preshared key:

Local subnets: 10.241.0.0/24

Peer subnets: 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 > IPsec 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*.

VPN Creation Wizard

1 VPN Setup 2 Authentication 3 Policy & Routing 4 Review Settings

Remote device: **IP Address** Dynamic DNS

Remote IP address: 52.116.127.153

Outgoing Interface: port1

Authentication method: **Pre-shared Key** Signature

Pre-shared key: [masked]

Site to Site - FortiGate

This FortiGate --- Internet --- Remote FortiGate

< Back Next > Cancel

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*.

VPN Creation Wizard

1 VPN Setup 2 Authentication 3 Policy & Routing 4 Review Settings

Local interface: port2

Local subnets: 10.0.1.0/24

Remote Subnets: 10.241.0.0/24

Internet Access: **None** Share Local Use Remote

Site to Site - FortiGate

This FortiGate --- Internet --- Remote FortiGate

< Back Next > Cancel

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.

VPN for VPC

VPN gateways IKE policies IPsec policies

Region: Washington DC

Gateway Status	Name	Resource Group	Gateway IP	Location	Active Connections
Active	thomasvpngateway	thomas-rg	52.116.127.153	Washington DC 1	1/1

Items per page: 10 1 item Page 1

VPC Infrastructure / All VPN gateways for VPC / **thomasvpngateway** Active View docs Actions...

Overview
Monitoring

VPN gateway details

Name: [thomasvpngateway](#)

Virtual private cloud: [thomas-vpc-general](#)

Resource group: [thomas-rg](#)

Subnet: [public](#)

ID: 0757-0513c4d8-f8d1-4c3f-b348-c4e6553d759f

IP address: [52.116.127.153](#)

Created: September 21, 2020 3:38:23 PM

Location: Washington DC 1

Monitoring preview

Data is based on sum of each metric over the last hour. For more details, or to specify a time range, visit the [monitoring](#) page or the Sysdig dashboard.

Type	Kibibytes	Packets
Data received	0	0
Data transmitted	0	0

[Launch monitoring](#)

VPN connections Create

Status	Connection Name	Peer Address	IKE Policy	IPsec Policy	State
Active	thomasvpnconnection	34.68.1.135	newpolicy	test	Enabled

Items per page: 10 1 item Page 1

FortiOS also shows that the VPN connection is up.

+ Create New	Edit	Delete	<input type="text" value="Search"/>	<input type="button" value="Q"/>
Tunnel	Interface Binding	Status	Ref	
Site to Site - FortiGate				
toIBMVPN	port1	Up	4	

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
```

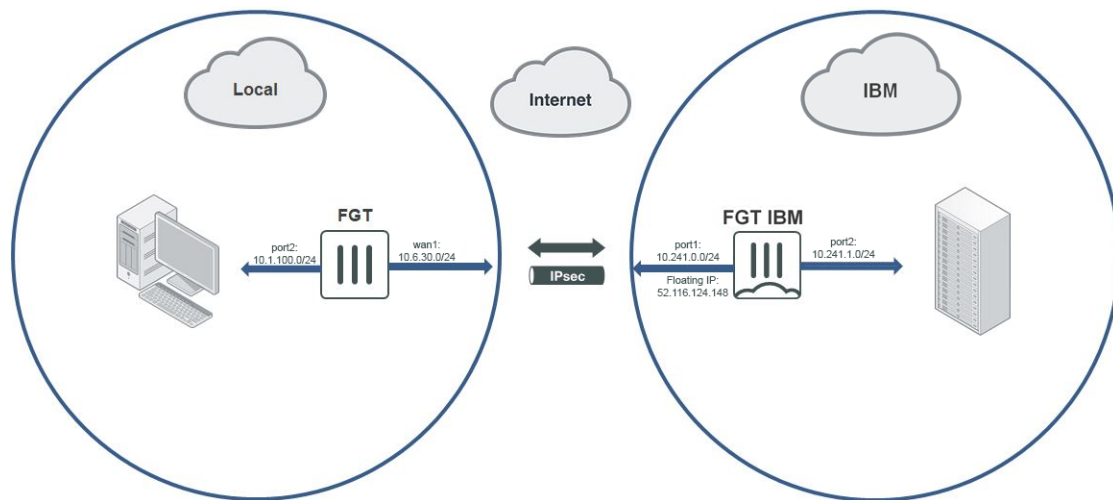
The following shows sniffer traffic.

```
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 > IPsec 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 IPsec 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 > IPsec 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 IPsec 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.

+ Create New Edit Delete Search Q			
Tunnel	Interface Binding	Status	Ref.
[-] Dialup - FortiGate ⓘ			
toPremise	port1	1 dialup connection(s)	3



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
2022-03-31	Initial release.
2022-08-04	Updated Creating a support account on page 6 .
2023-10-18	Updated Models on page 5 .
2024-03-20	Updated Deploying FortiGate-VM on IBM Cloud on page 7 .



www.fortinet.com

Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.