FortiOS - IBM Cloud Cookbook

Version 6.4

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

February 17, 2021
FortiOS 6.4 IBM Cloud Cookbook
01-640-652433-20210217

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**
SDN Connector integration with IBM Cloud **12**
VPN for FortiGate-VM on IBM Cloud **13**
Connecting a FortiGate to an IBM Cloud VPC VPN 13
Connecting a local FortiGate to an IBM Cloud FortiGate via site-to-site VPN 17
Change log **20**

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. FortiOS 6.4.2 and later versions support IBM Cloud deployment.

Support for active-passive high availability (HA) using two FortiGate nodes is planned for future releases.

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.
- New 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

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: 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 is updated 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. New s-series SKUs contain the VM base and service bundle entitlements for easier ordering. PAYG includes support, for which you must contact Fortinet Support with your customer information.

Creating a support account

FortiGate for IBM Cloud supports only the 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.

BYOL

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

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

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

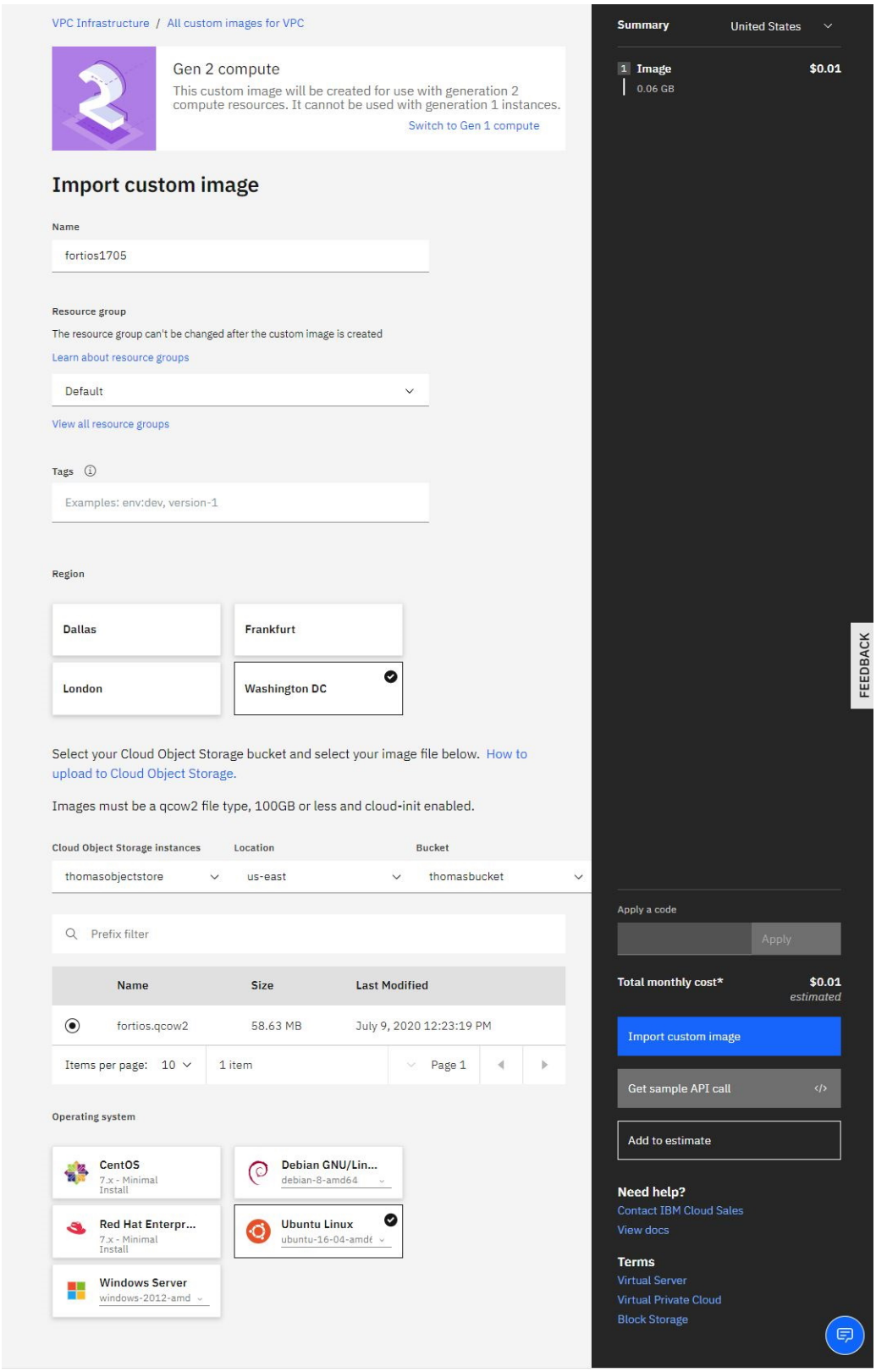
Deploying FortiGate-VM on IBM Cloud

FortiOS 6.4.2 adds support for deploying FortiGate-VM BYOL for the IBM Cloud platform. IBM Cloud platform 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 the 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-v6-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 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.

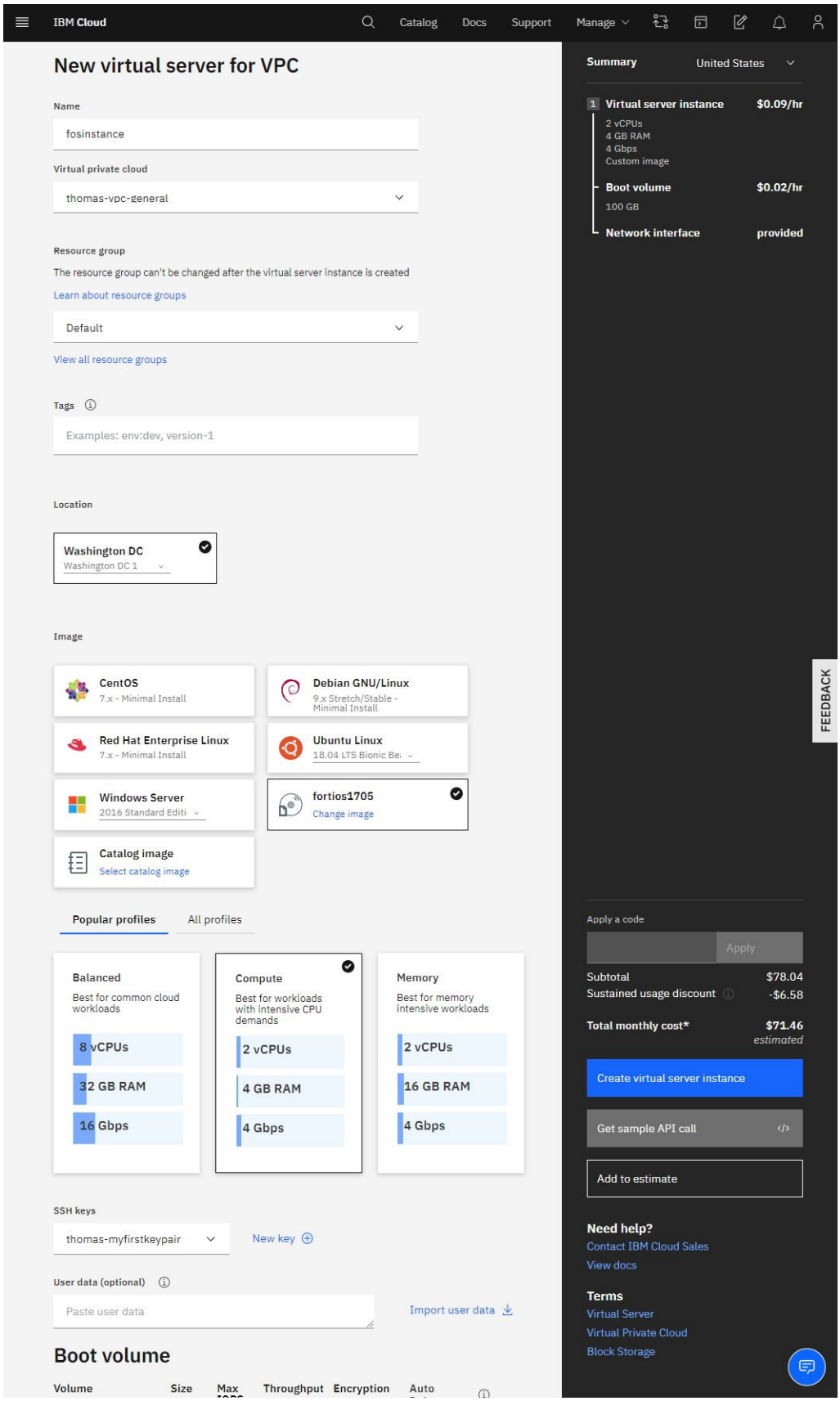


6. Create a new instance based on the custom image. Enter a name, select the VPC, location, custom image imported earlier, profile, SSH key, and user data. User data can be from the IBM bucket, config-url/license-url, or directly inputted in the form of a config, license, or MIME file. See the following 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
Catalog
Docs
Support
Manage
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
Debian GNU/Linux
9.x Stretch/Stable - Minimal Install
Red Hat Enterprise Linux
7.x - Minimal Install
Ubuntu Linux
18.04 LTS Bionic Be
Windows Server
2016 Standard Editi
fortios1705
Change image
Catalog image
Select catalog image
Popular profiles
All 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
Volume
Size
Max
Throughput
Encryption
Auto
Summary
United 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 interface
provided
FEEDBACK
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

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 FortiGate-VMs 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://thomasqabucket2.s3.amazonaws.com/FGVM08TM20004028.lic
   >> Cloudinit download license successfully
   >> Cloudinit trying to get config script from:
        https://thomasqabucket2.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 v6.4.0,build1705,200708 (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
```

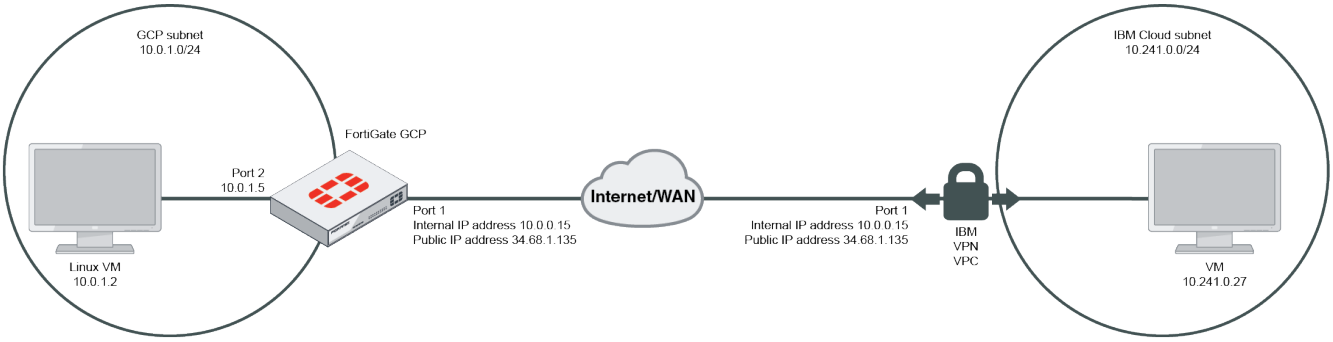
SDN Connector integration with IBM Cloud

See the *FortiOS Administration Guide*.

VPN for FortiGate-VM on IBM Cloud

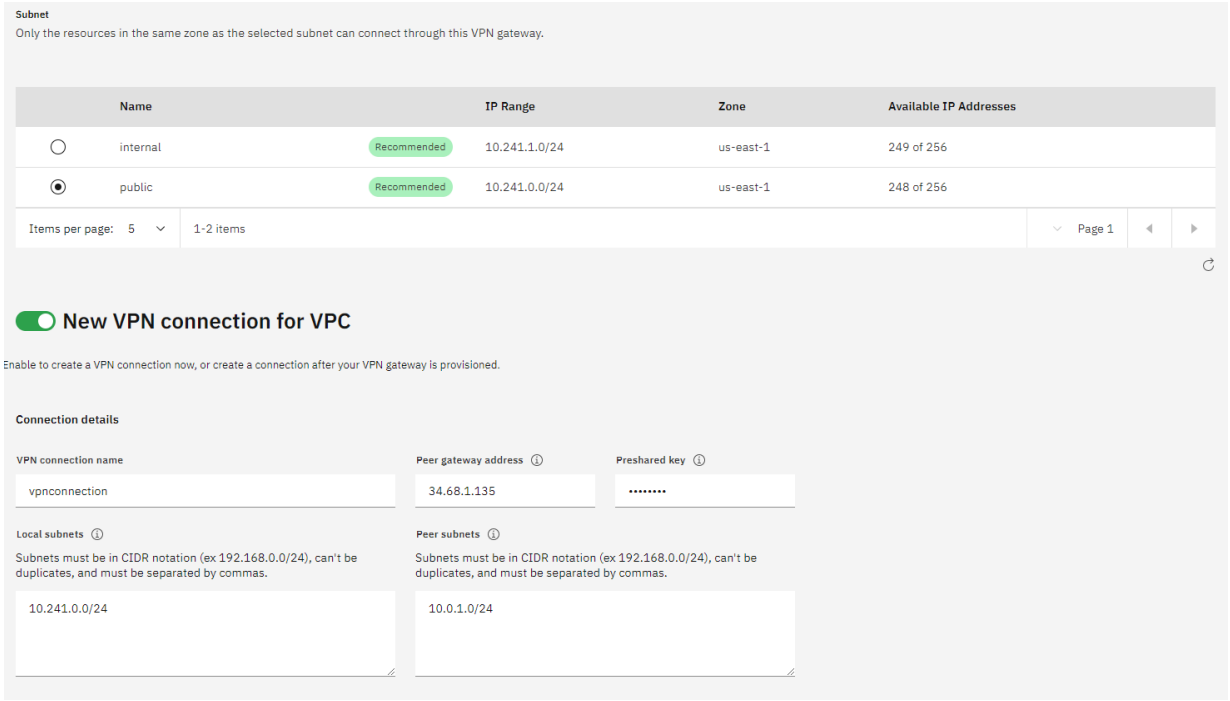
Connecting a FortiGate to an IBM Cloud VPC VPN

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*.

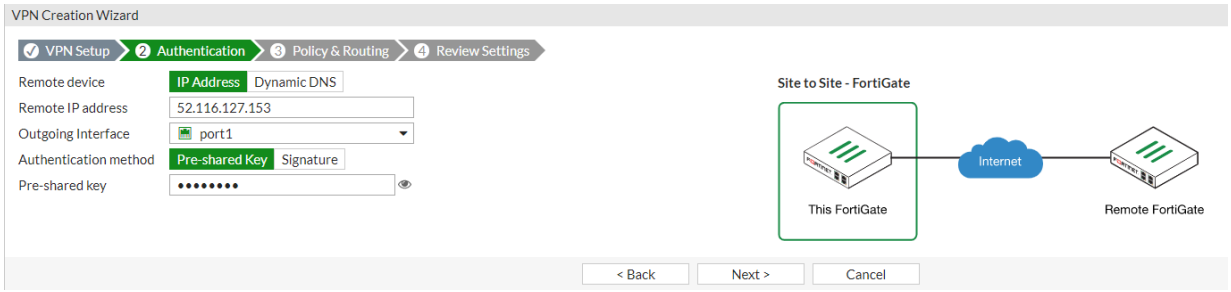
vi. From the *DH Group* dropdown list, select *5*.

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

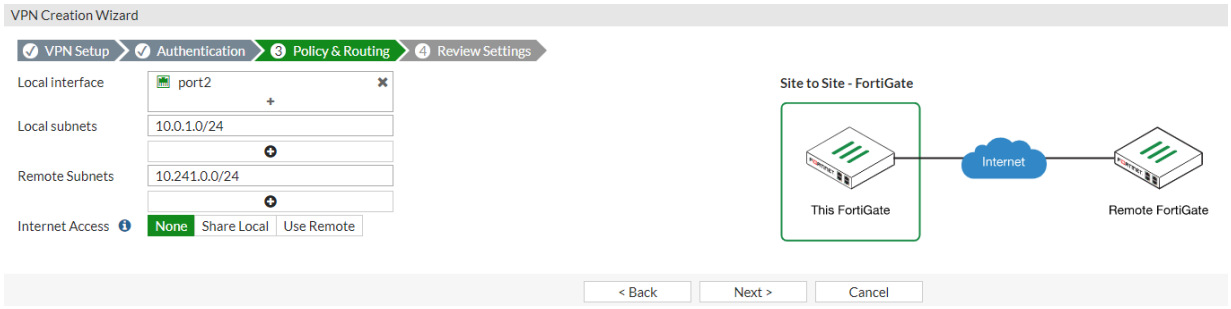
viii. Click *Create IPsec policy*.

To create the VPN connection in FortiOS:

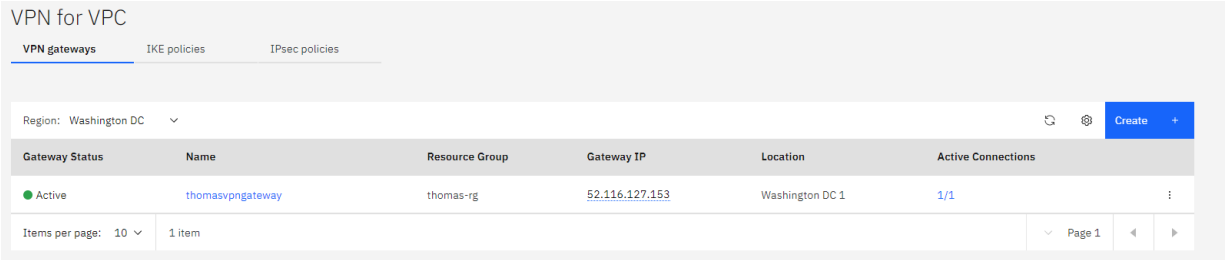
1. In FortiOS on the local FortiGate, go to *VPN* > *IPsec Wizard.*
2. On the *VPN Setup* tab, configure the following:
   a. In the *Name* field, enter the desired name.
   b. For *Template type*, select *Site to Site*.
   c. For *NAT Configuration*, select *No NAT between sites*.
   d. For *Remote 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*.

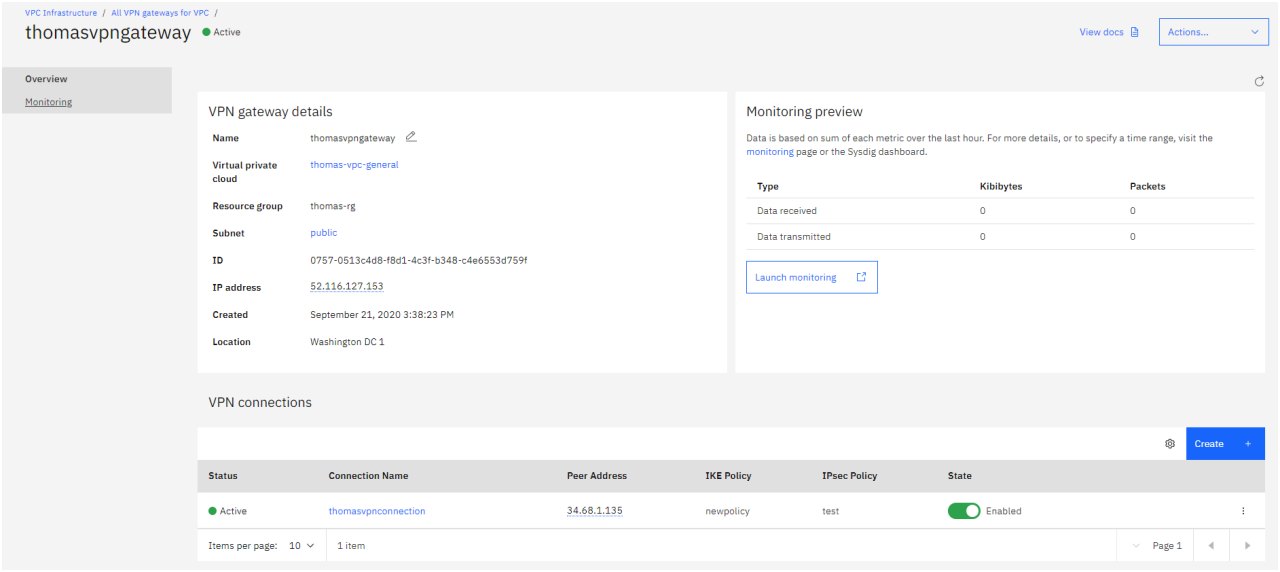


4. On the *Policy & Routing* tab, configure the following:
   a. For *Local interface*, select *port2*, the GCP internal network port.
   b. In the *Local subnets* field, enter the GCP internal subnet, *10.0.1.0/24*.
   c. In the *Remote Subnets* field, enter the IBM Cloud remote subnet. In this example,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

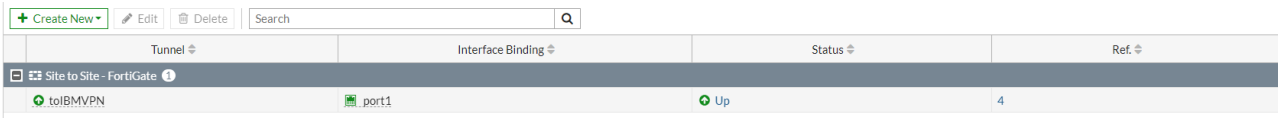


5. Proceed to create the VPN connection. After configuration, the VPN should automatically come up, and traffic can transverse. In the IBM Cloud console, you should see that the VPN gateway status is active and up.





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
```

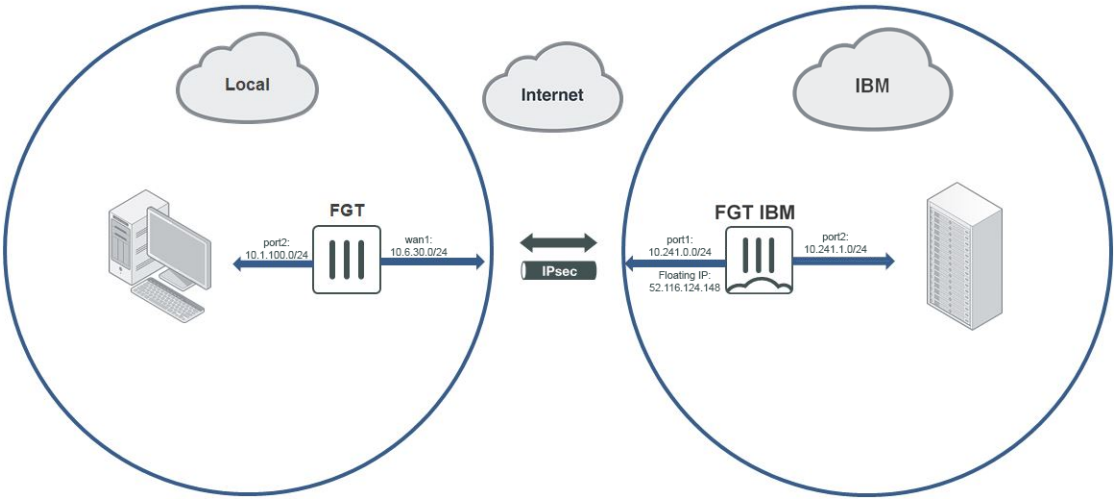
The following shows sniffer traffic.

```
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* > *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

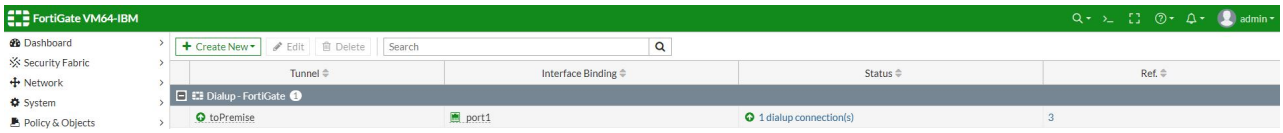
To create a VPN on the IBM FortiGate to the local FortiGate:

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.



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
2020-07-30	Initial release.
2020-08-04	Added SDN Connector integration with IBM Cloud on page 12.
2020-08-27	Added Connecting a local FortiGate to an IBM Cloud FortiGate via site-to-site VPN on page 17.
2020-10-01	Added Connecting a FortiGate to an IBM Cloud VPC VPN on page 13.
2021-02-17	Updated SDN Connector integration with IBM Cloud on page 12.

Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.