

OCI 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



August 04, 2022

FortiOS 7.2 OCI Administration Guide

01-720-793023-20220804

TABLE OF CONTENTS

About FortiGate-VM for OCI	5
Instance type support	5
Specialty and previous generation	6
Flexible SKUs	6
Models	6
Licensing	8
Order types	8
Creating a support account	8
Migrating a FortiGate-VM instance between license types	10
Single FortiGate-VM deployment	11
Deploying FortiGate-VM in paravirtualized or emulated mode	11
Creating a virtual cloud network (VCN) and public-facing subnets	11
Creating a security list	12
Creating a route table for the internal network	12
Creating an internal network subnet	13
Creating a FortiGate-VM instance	13
Attaching storage to the FortiGate-VM	22
Accessing the FortiGate-VM	22
Creating the second VNIC	24
Configuring the second VNIC on the FortiGate-VM	26
Enabling jumbo frame on the second VNIC	26
Changing the protected network's default route	28
Deploying a native mode FortiGate-VM on OCI	28
Deploying FortiGate-VM via the marketplace	30
Deploying FortiGate-VM using compute shapes that use Mellanox network cards	31
HA for FortiGate-VM on OCI	34
Deploying FortiGate-VM HA on OCI within one AD	34
FortiGate active-passive HA	34
Deploying and configuring FortiGate active-passive HA	34
Checking the prerequisites	35
Reviewing the network topology	36
Creating a VCN for same-AD HA topology	37
Deploying the FortiGate-VM	40
Configuring the OCI HA interfaces	41
Initial Fabric connector configuration	45
Using a custom certificate	45
Configuring active-passive HA	48
Troubleshooting	49
Deploying FortiGate-VM HA on OCI between multiple ADs	51
Checking the prerequisites	52
Reviewing the network topology	53
Configuring the OCI VCN	54
Deploying the FortiGate-VM	54
Configuring active-passive HA	54
Checking the HA status and function	57

Deploying FortiGate-VM HA on OCI between multiple ADs using a regional VCN	60
Checking the prerequisites	61
Reviewing the network topology	61
Creating a VCN for multiple-AD HA topology	62
Deploying the FortiGate-VM	65
Configuring the OCI HA interfaces	66
Initial Fabric connector configuration	70
Configuring active-passive HA	70
Troubleshooting	71
Deploying FortiGate-VM using Terraform in the CLI	72
Using Terraform to deploy a single FortiGate-VM	72
Bootstrapping the FortiGate-VM at initial bootup	74
SDN connector integration with OCI	77
Certificate-based SDN connector user privileges	77
Troubleshooting OCI SDN connector	77
Configuring an OCI SDN connector using IAM roles	78
Oracle Kubernetes (OKE) SDN connector	80
Change log	81

About FortiGate-VM for OCI

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 Oracle Cloud Infrastructure (OCI).

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 OCI supports active/passive high availability (HA) configuration with FortiGate-native unicast HA synchronization between the primary and secondary nodes. When the FortiGate-VM detects a failure, the passive firewall instance becomes active and uses OCI API calls to configure its interfaces/ports.

Highlights of FortiGate-VM for OCI 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 for OCI as a virtual machine (VM). Supported instances may change without notice. For up-to-date information on each instance type, see the following:

- Bring your own license (BYOL):
 - [FortiGate Next-Gen Firewall \(BYOL\)](#)
- Pay-as-you-go:
 - [FortiGate Next-Gen Firewall \(2 cores\)](#)
 - [FortiGate Next-Gen Firewall \(4 cores\)](#)
 - [FortiGate Next-Gen Firewall \(8 cores\)](#)
 - [FortiGate Next-Gen Firewall \(24 cores\)](#)

For licensing information, see [Order types on page 8](#).

FortiOS supports hot-adding OCPU and RAM. However, OCI may not support this. See [Changing the Shape of an Instance](#).

The following shows supported instance shapes for FortiGate on OCI:

Specialty and previous generation

Instance shape	OCPU	Max NIC	Recommended BYOL license
VM.Standard2.1	1	2	VM-02/02V/02S
VM.Standard2.2	2	2	VM-04/04V/04S
VM.Standard2.4	4	4	VM-08/08V/08S
VM.Standard2.8	8	8	VM-16/16V/16S
VM.Standard2.16	16	16	VM-UL/ULV/ULS
VM.Standard2.24	24	24	VM-UL/ULV/ULS

Flexible SKUs

AMD

Instance shape	OCPU	Memory (RAM) in GB
VM.Standard.E3.Flex	1-64	1-1024 GB
VM.Standard.E4.Flex	1-64	1-1024 GB

Intel

Instance shape	OCPU	Memory (RAM) in GB
VM.Standard.3.Flex	1-32	1-512 GB

Ampere

FortiOS 7.2.4 and later versions support the following instance types:

Instance shape	OCPU	Memory (RAM) in GB
VM.Standard.A1.Flex	1-64	1-1024 GB

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 (BYOL) models. See [Order types on page 8](#).



1 OCPU is typically equivalent to 2 vCPU as mentioned in the [Oracle Cloud Infrastructure Compute Classic FAQ](#).

Model name	vCPU	
	Minimum	Maximum
FG-VM02/02v/02s	1	2
FG-VM04/04v/04s	1	4
FG-VM08/08v/08s	1	8
FG-VM16/16v/16s	1	16
FG-VM32/32v/32s	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 [Changing the Shape of an Instance](#).

For more information about OCI Compute instance shapes, see [Compute Shapes](#).



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

Generally there are RAM size restrictions to FortiGate BYOL licenses. However, these restrictions are not applicable to OCI deployments. Any RAM size with certain CPU models are allowed. Licenses are based on the number of CPUs only.

Previously, platform-specific models such as FortiGate for OCI with an OCI-specific orderable menu existed. However, the common model is now applicable to all supported platforms.

For information about each model's order information, capacity limits, and adding VDM, see the [FortiGate-VM datasheet](#).

The primary requirement for the provisioning of a virtual FortiGate may be the number of interfaces it can accommodate rather than its processing capabilities. In some cloud environments, the options with a high number of interfaces tend to have high numbers of vCPUs.

The licensing for FortiGate-VM does not restrict whether the FortiGate can work on a VM instance in a public cloud that uses more vCPUs than the license allows. The number of vCPUs indicated by the license does not restrict the FortiGate from working, regardless of how many vCPUs are included in the virtual instance. However, only the licensed number of vCPUs process traffic and management. The rest of the vCPUs are unused.

The following shows an example for FGT-VM08:

License	2 vCPU	4 vCPU	8 vCPU	16 vCPU	32 vCPU
FGT-VM08	OK	OK	OK	The FortiGate-VM uses eight vCPUs for traffic and management. It does not use the rest.	The FortiGate-VM uses eight vCPUs for traffic and management. It does not use the rest.

You can provision a VM instance based on the number of interfaces you need and license the FortiGate-VM for only the processors you need.

Licensing

You must have a license to deploy FortiGate-VM for OCI. The following sections provide information on licensing FortiGate-VM for OCI:

Order types

OCI supports bring-your-own-license (BYOL) and pay-as-you-go (PAYG) licensing.

BYOL offers perpetual (normal series and v-series) and annual subscription (s-series) licensing as opposed to PAYG, which is an hourly 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.



PAYG FortiGate instances do not support the use of virtual domains (VDOM). If you plan to use VDOMs, deploy BYOL instances instead.



PAYG and BYOL licensing and payment models are not interchangeable. For example, once you spin up a FortiGate-VM PAYG instance, you cannot inject a BYOL license on the same VM. Likewise, you cannot convert a FortiGate-VM BYOL instance to PAYG.

Creating a support account

FortiGate-VM for OCI supports bring your own license (BYOL) and pay-as-you-go (PAYG) licensing models.

For BYOL, you typically order a combination of products and services, including support entitlement. PAYG includes support, for which you must contact Fortinet Support with your customer information.

You must create a FortiCare support account and obtain a license to activate the product through the FortiCare support portal. If you have not activated the license, you see the license upload screen when logging into the FortiGate-VM and cannot proceed to configure the FortiGate-VM.

BYOL

You can obtain licenses for the BYOL licensing model through any Fortinet partner. 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 OCI. See [VM license](#) for details.

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

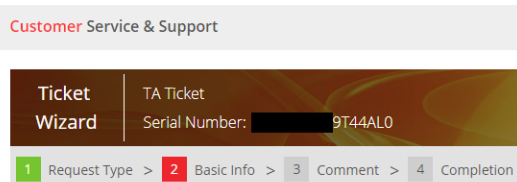
To register and download a license:

1. Go to [Customer Service & Support](#) and create a new account or log in with an existing account.
2. Click *Register Now* to start the registration process.
3. In the *Registration Code* field, enter your license activation code, then select *Next* to continue registering the product.
4. If you register the S-series subscription model, the site prompts you to select one of the following:
 - a. Click *Register* to newly register the code to acquire a new serial number with a new license file.
 - b. Click *Renew* to renew and extend the licensed period on top of the existing serial number, so that all features on the VM node continue working uninterrupted upon license renewal.
5. 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.

PAYG

To activate a PAYG license:

1. Deploy and boot the FortiGate PAYG VM and log into the FortiGate GUI management console.
2. From the Dashboard, copy the VM's serial number.
3. Go to [Customer Service & Support](#) and create a new account or log in with an existing account.
4. Click *Register Now* to start the registration process.
5. In the *Registration Code* field, enter your license activation code, then select *Next* to continue registering the product.
6. After completing registration, contact [Fortinet Customer Support](#) and provide your FortiGate instance's serial number and the email address associated with your Fortinet account.



Migrating a FortiGate-VM instance between license types

When deploying a FortiGate-VM on public cloud, you determine the license type (pay as you go (PAYG) or bring your own license (BYOL)) during deployment. The license type is fixed for the VM's lifetime. The image that you use to deploy the FortiGate-VM on the public cloud marketplace predetermines the license type.

Migrating a FortiGate-VM instance from one license type to another requires a new deployment. You cannot simply switch license types on the same VM instance. However, you can migrate the configuration between two VMs running as different license types. There are also FortiOS feature differences between PAYG and BYOL license types. For example, a FortiGate-VM PAYG instance is packaged with Unified Threat Management protection and does not support virtual domains, whereas a FortiGate-VM BYOL instance supports greater protection levels and features depending on its contract.

To migrate FortiOS configuration to a FortiGate-VM of another license type:

1. Connect to the FortiOS GUI or CLI and back up the configuration. See [Configuration backups](#).
2. Deploy a new FortiGate-VM instance with the desired license type. If deploying a BYOL instance, you must purchase a new license from a Fortinet reseller. You can apply the license after deployment via the FortiOS GUI or bootstrap the license and configuration during initial bootup using custom data as [\(Optional\) Bootstrapping FortiGate-VM on the OCI GUI at initial bootup on page 20](#) describes.
3. Restore the configuration on the FortiGate-VM instance that you deployed in step 2. As with the license, you can inject the configuration during initial bootup. Alternatively, you can restore the configuration in the FortiOS GUI as described in [Configuration backups](#).
4. If you deployed a PAYG instance in step 2, register the license. To receive support for a PAYG license, you must register the license as described in [Creating a support account on page 8](#).

Single FortiGate-VM deployment

Deploying FortiGate-VM in paravirtualized or emulated mode

Creating a virtual cloud network (VCN) and public-facing subnets

To create a VCN and public-facing subnets:

1. In OCI, go to *Networking > Virtual Cloud Networks*, and click *Create Virtual Cloud Network*.
2. In the *NAME* field, enter the VCN name. Then, select *CREATE VIRTUAL CLOUD NETWORK PLUS RELATED RESOURCES*. This allows you to create the Internet gateway, routing table, and subnet all together using Oracle default settings. If you intend to create each resource separately by specifying your own inputs, click *CREATE VIRTUAL CLOUD NETWORK ONLY*. This example uses the first choice.

The screenshot displays the 'Create Virtual Cloud Network' wizard in the OCI console. The 'CREATE IN COMPARTMENT' dropdown is set to 'Project001'. The 'NAME' field contains 'jkato002'. The 'CREATE VIRTUAL CLOUD NETWORK PLUS RELATED RESOURCES' radio button is selected. Below this, a summary section titled 'Create Virtual Cloud Network' shows the following details: DNS Resolution is enabled (checkbox checked), Name is 'jkato002 Project001', CIDR is '10.0.0.0/16', DNS Label is 'jkato002project', and DNS Domain Name is 'jkato002project.oraclevcn.com'. The next section, 'Create Internet Gateway', shows the Name as 'Internet Gateway'. The 'Update Default Route Table' section shows the Add Route Rule as '0.0.0.0/0 - Internet Gateway'. The final section, 'Create Subnet', shows the Name as 'Public Subnet www1:US-ASHBURN-AD-1', Security List as 'Default Security List', DHCP Options as 'Default DHCP Options', CIDR as '10.0.0.0/24; 10.0.0.0 - 10.0.0.255 (256 IP addresses)', Route Table as 'Default Route Table', and DNS Label as 'Auto-generated'.

3. Click *Create Virtual Cloud Network* at the bottom of the screen. This configures the related resources. There are three subnets, each of which will belong to an AD. They can be defined as public-facing networks (connecting to the Internet). In this example, (1) is 10.0.x.x/24. You can access

the FortiGate over the Internet once it is deployed via HTTPS through the GUI management screen or via SSH.

Creating a security list

To create a security list:

1. Click *Default Security List* for the 10.0.0.0/24 subnet, which you defined as the network's public side. By default, port 22 is allowed.
2. Click *Edit all Rules* > *Add Rule*. Manually add a rule to allow TCP port 443.

Allow Rules for Ingress

Oracle recommends adding an ingress rule to receive Path MTU Discovery fragmentation messages. Without it, you may experience connectivity issues for traffic going outside the VCN. For more information, see [Handling Connection](#).

<input type="checkbox"/>	SOURCE CIDR 0.0.0.0/0	IP PROTOCOL TCP	SOURCE PORT RANGE (OPTIONAL) All	DESTINATION PORT RANGE (OPTIONAL) 22
STATELESS (more information)	Allows TCP traffic for ports: 22 SSH Remote Login Protocol			
<input type="checkbox"/>	SOURCE CIDR 0.0.0.0/0	IP PROTOCOL ICMP	TYPE AND CODE (OPTIONAL) 3, 4	
STATELESS (more information)	Allows ICMP traffic for: 3, 4 Destination Unreachable: Fragmentation Needed and Don't Fragment was Set			
<input type="checkbox"/>	SOURCE CIDR 10.0.0.0/16	IP PROTOCOL ICMP	TYPE AND CODE (OPTIONAL) 3	
STATELESS (more information)	Allows ICMP traffic for: 3 Destination Unreachable			
<input type="checkbox"/>	SOURCE CIDR 0.0.0.0/0	IP PROTOCOL TCP	SOURCE PORT RANGE (OPTIONAL) All	DESTINATION PORT RANGE (OPTIONAL) 443
STATELESS (more information)	Specified IP addresses: 0.0.0.0-255.255.255.255 (4,294,967,296 IP addresses) Allows TCP traffic for ports: 443 HTTPS			

[+ Add Rule](#)

For a full list of ports that you must allow for the FortiGate-VM instance, see [FortiGate open ports](#). For example, for Heartbeat sync ports, you must have the following included in the security list:

Ingress Rules

Add Ingress Rules							
	Stateless	Source	IP Protocol	Source Port Range	Destination Port Range	Type and Code	Allows
<input type="checkbox"/>	Yes	0.0.0.0/0	UDP	All	730		UDP traffic for ports: 730
<input type="checkbox"/>	Yes	0.0.0.0/0	TCP	All	703		TCP traffic for ports: 703
<input type="checkbox"/>	Yes	0.0.0.0/0	UDP	All	703		UDP traffic for ports: 703

3. Click *Save Security List Rules*.

Creating a route table for the internal network

To create a route table for the internal network:

1. Let's change the default gateway for the protected network and point it to the FortiGate-VM's second network interface. Go to *Route Tables* > *Create Route Table*.

- For all destinations, choose *Internet Gateway* for now. You will change the configuration later. Click *Create Route Table*. A new route table has been created.

Creating an internal network subnet

To create an internal network subnet:

- Create an internal protected network, where VMs will be placed under the FortiGate-VM's protection. Click *Create Subnet*.
- Create the internal protected network in the AD where the FortiGate-VM is located. Choose the appropriate domain in use, then enter the internal subnet. The route table must be the one created earlier for the internal network. Under *SUBNET ACCESS*, select *PRIVATE SUBNET*. You can select any security list as desired. In the example, a security list that allows all protocols for any source and destination was selected. You must create the security list prior to this configuration.

Create Subnet [help](#) [cancel](#)

If the Route Table, DHCP Options, or Security Lists are in a different Compartment than the Subnet, [click here](#) to enable Compartment selection for those resources.

NAME (OPTIONAL)

AVAILABILITY DOMAIN

CIDR BLOCK

Source IP addresses: 10.0.4.0-10.0.4.255 (256 IP addresses)

ROUTE TABLE

SUBNET ACCESS
☒ PRIVATE SUBNET
 Prohibit public IP addresses for instances in this Subnet
☐ PUBLIC SUBNET
 Allow public IP addresses for instances in this Subnet

DNS RESOLUTION
☒ USE DNS HOSTNAMES IN THIS SUBNET
 Allows assignment of DNS hostname when launching an Instance

DNS LABEL

DNS DOMAIN NAME (READ-ONLY)

DHCP OPTIONS

Security Lists
☒ Internal network security list

TAGS
 Tagging is a metadata system that allows you to organize and track resources within your tenancy. Tags are composed of keys and values which can be attached to resources. [Learn more about tagging](#)

TAG NAME/SPACE	TAG KEY	VALUE
None (apply a free-form tag)		

[Create](#)

Creating a FortiGate-VM instance

There are two methods of creating the FortiGate-VM instance. Select one of the following methods:

- The first method consists of obtaining the deployment image file, importing the file into the OCI portal, then launching the FortiGate-VM instance. See [Creating an instance by importing an image file on page 14](#).
- The second method consists of pointing to an available FortiGate-VM image on OCI instead of importing one. See [Creating an instance by selecting an OCI partner image on page 17](#).

You can also add bootstrapping of FortiGate CLI commands and a BYOL license at the time of initial bootup as part of instance creation, as described in [\(Optional\) Bootstrapping FortiGate-VM on the OCI GUI at initial bootup on page 20](#). This step is optional and can be included as part of either creation method.

Once you have completed using either method to create a FortiGate-VM, continue to [Attaching storage to the FortiGate-VM on page 22](#).

Creating an instance by importing an image file

To create a FortiGate-VM instance by importing an image file, follow these steps:

To obtain the deployment image file and place it in your bucket:

1. Obtain the deployment image file:
 - a. Go to [Customer Service & Support](#). Go to *Download > VM Images* in the top menu.
 - b. In the *Select Product* dropdown list, select *FortiGate*.
 - c. In the *Select Platform* dropdown list, select *Oracle*.
 - d. Obtain the *FGT_VM64_OPC-vX-buildXXXX-FORTINET.out.OpenXen.zip* file. XXXX is the build number. Ensure that the file name includes OpenXen.
 - e. After downloading, unzip the file. You will find the *forties.qcow2* file, which is needed to deploy the FortiGate-VM on OCI.
2. In OCI, go to *Object Storage*, then click *Create Bucket* to create a standard storage bucket.
3. Configure the standard storage bucket as shown:

Create Bucket [help](#) [cancel](#)

Specify the storage tier for this bucket. Storage tier for a bucket can only be specified during creation.

BUCKET NAME

STORAGE TIER
☒ STANDARD
☐ ARCHIVE

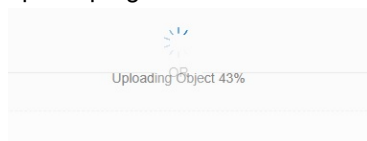
TAGS
 Tagging is a metadata system that allows you to organize and track resources within your tenancy. Tags are composed of keys and values which can be attached to resources.
[Learn more about tagging](#)

TAG NAMESPACE	TAG KEY	VALUE
None (apply a free-form tag)	<input type="text"/>	<input type="text"/>

[+](#)

[Create Bucket](#)

4. Select the bucket, then click *Upload Object* to upload the deployment image file *forties.qcow2*. The dialog shows the upload progress.



5. Once uploaded, the following screen appears. Click *Create Pre-Authenticated Requests*.

Search Objects by prefix

Details
Edit
Download
Create Pre-Authenticated Request
Delete

Create Pre-Authenticated Request

NAME
pre-Auth-FGT-deploy

PRE-AUTHENTICATED REQUEST TARGET
☐ BUCKET
☒ OBJECT
fortios.qcow2

ACCESS TYPE
☒ PERMIT READS ON THE OBJECT
☐ PERMIT WRITES TO THE OBJECT
☐ PERMIT READS TO AND WRITES FROM THE OBJECT

EXPIRATION DATE/TIME
2018-02-02 20:13 GMT

Create Pre-Authenticated Request

6. Note down this URL. Further steps require it.

Pre-Authenticated Request Details

NAME
pre-Auth-FGT-deploy

PRE-AUTHENTICATED REQUEST URL
https://objectstorage.us-phoenix-1.oraclecloud.com/p/Pi6mVtK434eShZD62IPbv6zH96AAeS0DXK8hUpR-Ex4/n/fortinet/b-Bucket001/o/fortios.qcow2

Copy
Copy this URL for your records. It will not be shown again.

Close

To import the image:

1. Go to *Compute > Custom Images*. Click *Import Image*.
2. In the *Import Image* dialog, complete the fields. In the *OBJECT STORAGE URL* field, enter the URL link obtained earlier and place it in your bucket.

3. Under *IMAGE TYPE*, select *QCOW2*.
4. Under *LAUNCH MODE*, select *PARAVIRTUALIZED MODE* or *EMULATED MODE*.
5. You have now imported the image. Wait until the *IMPORTING...* status changes to *AVAILABLE*.

To create the FortiGate-VM instance:

1. From the newly imported image, click *Create Instance*.
2. Configure the parameters:
 - a. In the *Name your instance* field, enter the desired name to identify the instance by.
 - b. Under *Select an availability domain for your instance*, select the desired domain.
 - c. Under *Choose instance type*, select *Virtual Machine*.
 - d. Under *Choose instance shape*, select one of the supported instance shapes. Currently, FortiGate-VM supports the Standard1 and Standard2 instance families.
 - e. In the *Virtual cloud network* field, select a network to launch the instance.
 - f. In the *Subnet* field, select a subnet on the Internet-facing side of the network.
 - g. Click *Show Advanced Options*.
 - h. On the *Management* tab, if you want to add bootstrapping of FortiGate CLI commands and a BYOL license, follow the instructions in [\(Optional\) Bootstrapping FortiGate-VM on the OCI GUI at initial bootup on page 20](#), then copy and paste all of the text content (CLI commands and license) under *User Data*. Modify the text as needed.
 - i. On the *Networking* tab, in the *Private IP address* field, specify a static IP address within the selected subnet.
 - j. Ensure *Assign public IP address* is selected so you can access the FortiGate-VM over the Internet. You can disable this once you have configured everything as desired.
 - k. In the *Hostname* field, enter the desired name.
3. Click *Create*. Wait until the *PROVISIONING...* status changes to *RUNNING*. You can also check the FortiGate's public IP address in this screen once it becomes available.

The screenshot shows the Oracle Cloud Infrastructure (OCI) console interface for an instance named 'jkato-fgt603-dev005'. The instance is in the 'PROVISIONING...' state, indicated by an orange square icon. The console displays the following information:

- Instance Information:**
 - Availability Domain: wwwl-US-ASHBURN-AD-1
 - Fault Domain: FAULT-DOMAIN-3
 - Region: iad
 - Shape: VM.Standard2.1
 - Virtual Cloud Network:
 - Maintenance Reboot: -
- Primary VNIC Information:**
 - Private IP Address: -
 - Public IP Address: Unavailable
- Image:** FGT-OCI-test001
- OCID:** ...d8ffwq [Show Copy](#)
- Launched:** Fri, 11 Jan 2019 20:25:25 GMT
- Compartment:** fortinetoraclecloud1 (root)
- Launch Mode:** PARAVIRTUALIZED
- Internal FQDN:** Unavailable
- Subnet:**

A note at the bottom states: "This instance's traffic is controlled by its firewall rules in addition to the associated [Subnet's](#) Security Lists."

At this stage, FortiGate deployment is not complete. You also need to add a storage volume as a system log disk and attach it to the FortiGate instance. If you want FortiGate to run inline across two or multiple subnets, you will also need to add one or more virtual network interfaces and attach them to the FortiGate instance.

Creating an instance by selecting an OCI partner image


This section describes an alternative method of deploying a single FortiGate-VM instance. OCI's partner image catalog lists FortiGate deployment images. You can create the instance by pointing to an available image instead of importing one yourself.

To create an instance by selecting an OCI partner image:

1. In OCI, click *Create Instance*.
2. Name the instance as desired.
3. Under *Choose an operating system or image source*, click *Change Image Source*.
4. In the *Browse All Images* window, go to the *Partner Images* tab. Select the FortiGate app, then select an image/build from the *Image build* dropdown list. Select the checkbox at the bottom of the window to confirm that you have read and agree to the terms of use, then click *Select Image*.
5. Configure the parameters as follows:
 - a. Under *Choose instance shape*, select one of the supported instance shapes.
 - b. Under *Configure boot volume* and *Add SSH key*, keep the default values.

c. Under *Configure networking*, configure the options as required.

Choose an operating system or image source




Fortinet FortiGate-VM Next-Generation Firewall (NGFW) for OCI
Comprehensive Security in One, Simplified Solution

Change Image Source

Choose instance type

Virtual Machine

A virtual machine is an independent computing environment that runs on top of physical bare metal hardware.



Bare Metal Machine

A bare metal compute instance gives you dedicated physical server access for highest performance and strong isolation.

Choose instance shape

VM.Standard2.1
1 Core OCPU, 15 GB Memory

Change Shape

Configure boot volume

Default boot volume size: 46.6 GB

☐ Custom boot volume size (in GB)

☐ Choose a key from Key Management to encrypt this volume

Add SSH key

☒ Choose SSH key file ☐ Paste SSH keys

Choose SSH key file (.pub) from your computer

Drop files here

Choose Files

Configure networking

Virtual cloud network compartment

fortinetoracled1 (root)/DevelopmentEngineering

Virtual cloud network

jkato001-vcn

Subnet compartment

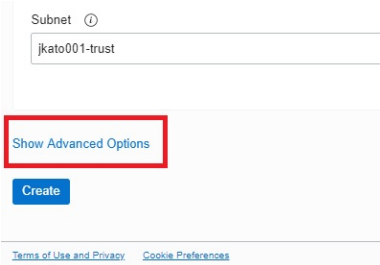
fortinetoracled1 (root)/DevelopmentEngineering

Subnet ⓘ

jkato001-trust

Show Advanced Options

Create

d. Click *Show Advanced Options*.


Subnet ⓘ

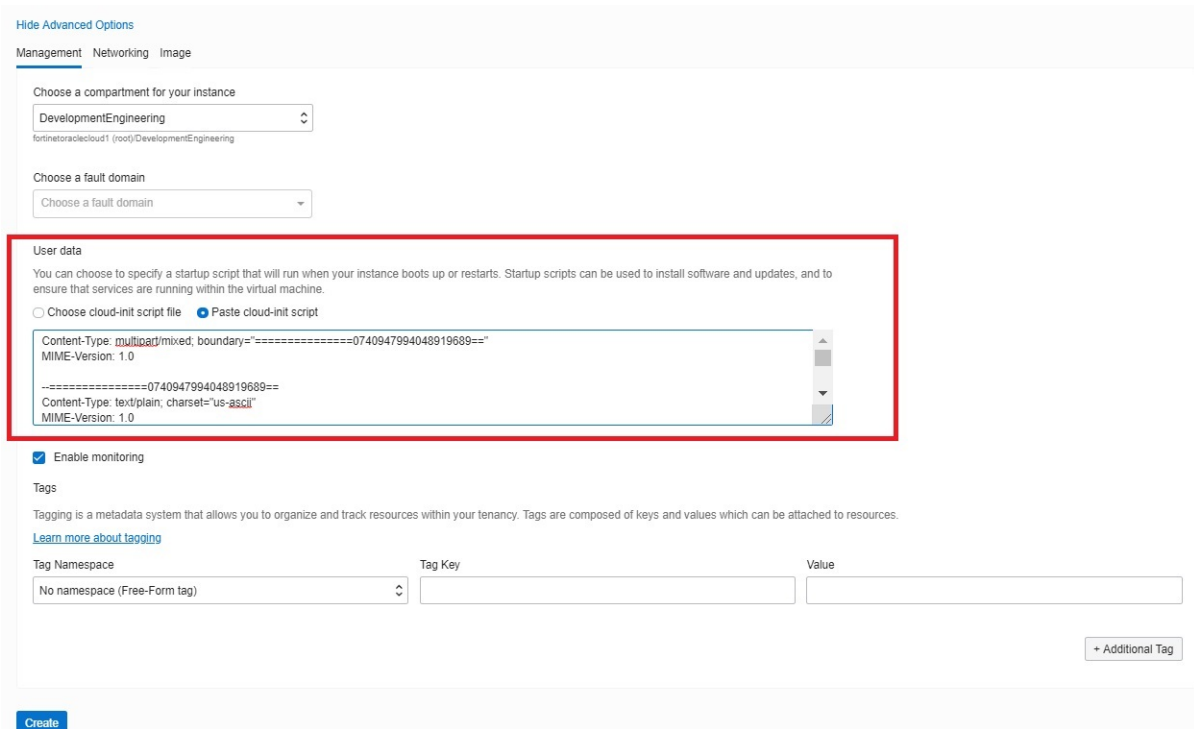
jkato001-trust

Show Advanced Options

Create

[Terms of Use and Privacy](#) [Cookie Preferences](#)

- e. On the *Management* tab, if you want to add bootstrapping of FortiGate CLI commands and a BYOL license, follow the instructions in [\(Optional\) Bootstrapping FortiGate-VM on the OCI GUI at initial bootup on page 20](#), then copy and paste all of the text content (CLI commands and license) under *User Data*. Modify the text as needed.



Hide Advanced Options

Management Networking Image

Choose a compartment for your instance

DevelopmentEngineering

fortinetoracled1 (root)/DevelopmentEngineering

Choose a fault domain

Choose a fault domain

User data

You can choose to specify a startup script that will run when your instance boots up or restarts. Startup scripts can be used to install software and updates, and to ensure that services are running within the virtual machine.

☐ Choose cloud-init script file ☒ Paste cloud-init script

Content-Type: multipart/mixed; boundary="=====0740947994048919689=="

MIME-Version: 1.0

-----0740947994048919689==

Content-Type: text/plain; charset="us-ascii"

MIME-Version: 1.0

☒ Enable monitoring

Tags

Tagging is a metadata system that allows you to organize and track resources within your tenancy. Tags are composed of keys and values which can be attached to resources.

[Learn more about tagging](#)

Tag Namespace	Tag Key	Value
No namespace (Free-Form tag)		

+ Additional Tag

Create

- f. On the *Networking* tab, ensure that *Assign public IP address* is enabled.

Subnet ⓘ

jkato001-untrust

Hide Advanced Options

Management Networking Image

Private IP address (Optional)

☒ Assign public IP address

Hostname (Optional)

Create


- 6.** Click *Create*. This deploys the FortiGate-VM instance.

MENU

ORACLE
Cloud Infrastructure

us-ashburn-1

[Compute](#) » [Instances](#) » Instance Details



jkato-fgt603-dev005

Create Custom Image
Start
Stop
Reboot
Terminate
Apply Tag(s)
Create Instance Configuration

Instance Information

Tags

Instance Information

Availability Domain:	www-US-ASHBURN-AD-1	Image:	Published Image: FortiGate-VM 6.0.3 for OCI Emulated Mode
Fault Domain:	FAULT-DOMAIN-2	OCID:	...torvq Show Copy
Region:	iad	Launched:	Wed, 02 Jan 2019 21:05:49 GMT
Shape:	VM.Standard2.1	Compartment:	ocid1-compartment-xxxxxx
Virtual Cloud Network:		Launch Mode:	EMULATED
Maintenance Reboot:	-		

Primary VNIC Information

Private IP Address:	-	Internal FQDN:	Unavailable
Public IP Address:	Unavailable	Subnet:	

This Instance's traffic is controlled by its firewall rules in addition to the associated [Subnet's Security Lists](#).

(Optional) Bootstrapping FortiGate-VM on the OCI GUI at initial bootup

This section explains how to add bootstrapping of FortiGate CLI commands and a bring your own license at the time of initial bootup as part of instance creation on the OCI GUI console.

To bootstrap a FortiGate-VM on the OCI GUI at initial bootup:

1. Refer to sample text content available on [GitHub](#). This content is in MIME format.
2. This example uses the following CLI commands:

```
config system global
    set timezone 03
end
```

This example CLI sets the timezone as GMT-9 Alaska. You can replace these lines with your own set of CLI commands.

3. Download a FortiGate-VM license file from [Customer Service & Support](#) after registering your product code. In the sample text found in step 1, find the following lines:

```

20 -----BEGIN FGT VM LICENSE-----
21 Replace with your own
22 -----END FGT VM LICENSE-----

```

Replace these lines with the license file content. FortiGate-VM license content resembles the following:

```

-----BEGIN FGT VM LICENSE-----
QAAAABUjZtrwrJdUjEe/8C5dWnOvmY1w70ZNXPTG7vm2KKuYvL4++qL0gED6/q
SQSPkwpTfIXjAuRgtGyX1VvaTpXgQAA1pwrFdJnS6TWJ6dVT7K1D8ncuFaa3bCw
s8XpmlivzjE4//+C9nqh4fN/KyDweWEIptDMaIsoCmBB0rU8HQIDkX+rgeCs3QZ5
ELStRrX11/oXqTB/gorG67ZdybXwVzPwVwJYDS5AsI+QK8BHJ+XghLjHkzBZ4ezU
Hd01HCsm7MXEYV5Kau43sZ9XESTxqPEInah3yXgYtd24pnV683G4EHCKAdGyMTP
QqDqBMKcTSaei0ooGVAOX8D62C5Zjh+r1+tkdpR5YhoVYZHJ95hBCNjBbroJbMnK7
NogYuadQEH28MDtpvzXnb24mW1fDQMTJysQwCtwzJzmnBny5Bo7XNg/1rTs2QnFB
-----END FGT VM LICENSE-----

```

You copy and paste this content into the OCI GUI during instance creation in *Advanced Options > Management > User data*. See steps 2h in [To create the FortiGate-VM instance: on page 16](#) or 5e in [Creating an instance by selecting an OCI partner image on page 17](#).

Hide Advanced Options

Management Networking Image

Choose a compartment for your instance

DevelopmentEngineering

fortinetoracledcloud1 (root)/DevelopmentEngineering

Choose a fault domain

Choose a fault domain

User data

You can choose to specify a startup script that will run when your instance boots up or restarts. Startup scripts can be used to install software and updates, and to ensure that services are running within the virtual machine.

☐ Choose cloud-init script file ☒ Paste cloud-init script

Content-Type: multipart/mixed; boundary="-----0740947994048919689=="

MIME-Version: 1.0

-----0740947994048919689==

Content-Type: text/plain; charset="us-ascii"

MIME-Version: 1.0

☒ Enable monitoring

Tags

Tagging is a metadata system that allows you to organize and track resources within your tenancy. Tags are composed of keys and values which can be attached to resources.

[Learn more about tagging](#)

Tag Namespace	Tag Key	Value
No namespace (Free-Form tag)		

+ Additional Tag

Create

Attaching storage to the FortiGate-VM

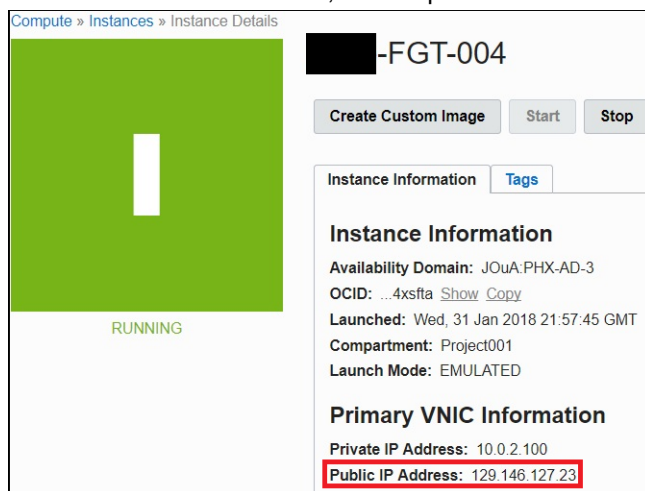
To attach storage to the FortiGate-VM:

1. Go to *Storage > Block Volumes > Create Block Volume*.
2. Enter a unique name, choose the availability domain, then specify the size to around 50 GB. Click *Create Block Volume*. This provisions the volume.
3. Once provisioned, return to the FortiGate-VM instance. Click *Attach Block Volume*.
4. Under *Choose how you want to attach your block volume*, select *EMULATED*.
5. After attaching the block volume, ensure you reboot the FortiGate-VM instance.

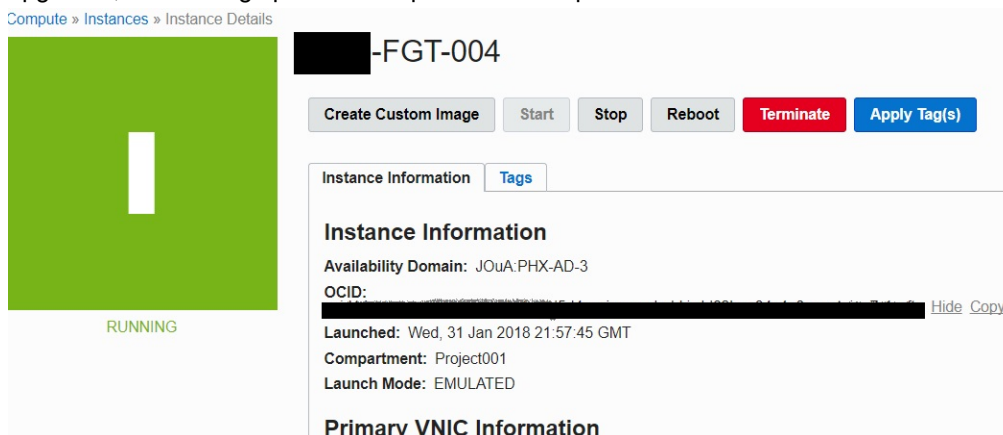
Accessing the FortiGate-VM

To access the FortiGate-VM:

1. In the FortiGate-VM instance, find the public IP address. Your IP address will differ from the example.



2. In a browser, go to https://<public_IP_address>. The default username is “admin” for new installations. For upgrades, the existing opc user is kept. The default password is the OCID. You can find the OCID as shown:



3. Once logged in, FortiOS prompts for a license file. You can obtain licenses through any Fortinet partner. If you do not have a partner, contact Fortinet 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. Go to [Customer Service & Support](#) and

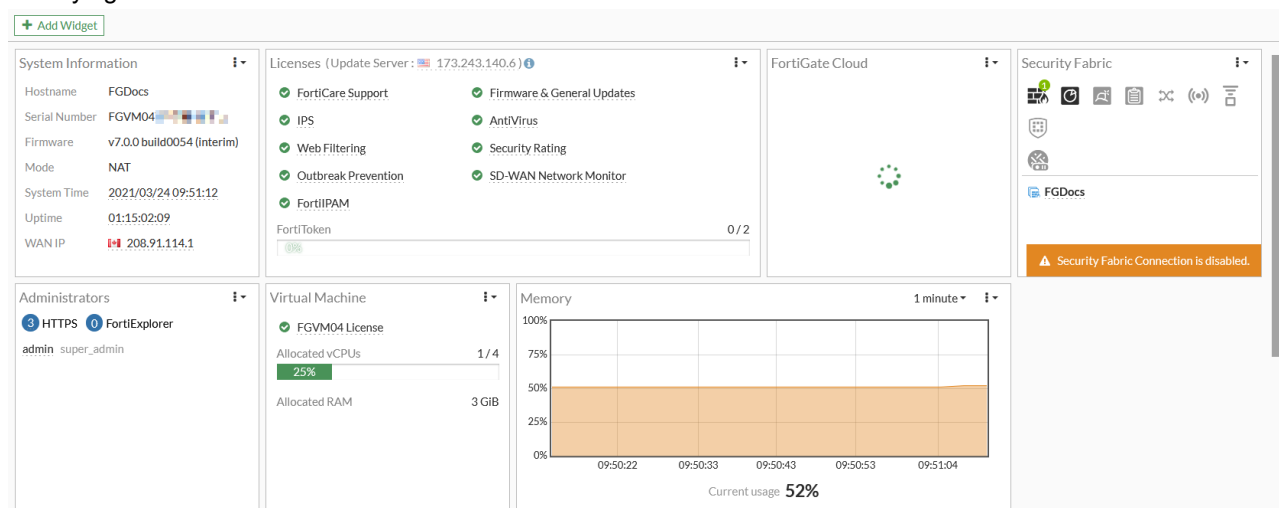
create a new account or log in with an existing account.



If you added a license by following the instructions in [\(Optional\) Bootstrapping FortiGate-VM on the OCI GUI at initial bootup on page 20](#), the system displays the dashboard instead of a license upload window, since the license is already activated.

- Go to **Asset > Register Now** to start the registration process. In the **Registration Code** field, enter your license activation code and select **Next** to continue registering the product. Enter your details in the other fields.

- At the end of the registration process, download the license (.lic) file to your computer. You upload this license to activate the FortiGate.
- After registering a license, Fortinet servers may take 30-45 minutes to fully recognize the new license. When you upload the license (.lic) file to activate the FortiGate, if you get an error that the license is invalid, wait 30 minutes and try again. You should now be able to see the FortiGate GUI console.



- If you followed the instructions in [\(Optional\) Bootstrapping FortiGate-VM on the OCI GUI at initial bootup on page 20](#), check if the command succeeded. Open the CLI console and enter `diag debug cloudinit show`. If the cloud-init succeeded, the CLI shows `Finish running script` with no errors.

8. Check the timezone by running `config system global and get` commands.

```
security-rating-run-on-schedule: enable
send-pmtu-icmp      : enable
snat-route-change   : disable
special-file-23-support: disable
ssd-trim-freq        : weekly
--More--            : 1
ssd-trim-min         : Random
ssd-trim-weekday     : sunday
ssh-kex-sha1         : enable
ssl-min-proto-version: TLSv1-2
ssl-static-key-ciphers: enable
sslvpn-cipher-hardware-acceleration: enable
sslvpn-kxp-hardware-acceleration: enable
sslvpn-plugin-version-check: enable
strict-dirty-session-check: enable
strong-crypto        : enable
switch-controller    : disable
switch-controller-reserved-network: 169.254.0.0 255.255.0.0
sys-perf-log-interval: 5
tcp-halfclose-timer  : 120
tcp-halfopen-timer   : 10
tcp-option           : enable
tcp-timewait-timer   : 1
timezone            : (GMT-9:00) Alaska
traffic-priority      : tos
```

The timezone changed to Alaska as expected, meaning that the bootstrapping CLI command succeeded.

Creating the second VNIC

To create the second VNIC:

1. In the FortiGate-VM instance, click *Attached VNICs > Create VNIC*.
2. Create the virtual network interface by specifying the name, VNC, and internal subnet created earlier. Ensure that *Skip Source/Destination Check* is selected. Enter an IP address and click *Create VNIC*. You now have the second network interface attached to the FortiGate-VM.

Create VNIC [cancel](#)

VNIC Information

If the Virtual Cloud Network, or Subnet is in a different Compartment than the VNIC, [click here](#) to enable Compartment selection for those resources.

NAME (Optional)
[redacted]-vnic2

VIRTUAL CLOUD NETWORK
[redacted]002

SUBNET
[redacted]-protected-network2

☒ Skip Source/Destination Check

The source/destination check causes this VNIC to drop any network traffic whose source or destination is not this VNIC. Only check the checkbox if you want this VNIC to skip the check and forward that traffic (for example, to perform Network Address Translation).

Primary IP Information

PRIVATE IP ADDRESS (Optional)
10.0.5.100

Must be within 10.0.5.2 to 10.0.5.254. Cannot be in current use.

☐ Assign public IP address (cannot create public IP addresses in a private Subnet)

HOSTNAME (Optional)
To specify a hostname, select a Subnet that has DNS services enabled

No spaces. Only letters, numbers, and hyphens. 63 characters max.

FULLY QUALIFIED DOMAIN NAME (Read-only)
To specify a hostname, select a Subnet that has DNS services enabled

Create VNIC

Attached VNICS

Create VNIC			
 ATTACHED	[redacted]-FGT-004 (Primary VNIC) OCID: ...3f43fa Show Copy Attached: Wed, 31 Jan 2018 21:57:50 GMT Compartment: Project001	Private IP Address: 10.0.2.100 Fully Qualified Domain Name: jkato-igt-004... Show Copy Public IP Address: 129.146.127.23	Subnet: Public Subnet jOwa-PHX-AD-3 Skip Source/Destination Check: No MAC Address: 00:00:17:01:FF:06 VLAN Tag: 15
 ATTACHED	[redacted]-vnic2 OCID: ...muyayq Show Copy Attached: Thu, 08 Feb 2018 03:40:18 GMT Compartment: Project001	Private IP Address: 10.0.5.100 Fully Qualified Domain Name: <i>Unavailable</i> Public IP Address:	Subnet: [redacted]-protected-network2 Skip Source/Destination Check: Yes MAC Address: 00:00:17:01:E6:57 VLAN Tag: 16

Networking » Virtual Cloud Networks » Virtual Cloud Network Details » Route Tables » Route Table Details

protected-network2

RT
AVAILABLE

Route Table Information
OCID: ...r4alta [Show](#) [Copy](#)
Created: Thu, 08 Feb 2018 03:40:18 GMT

Route Rules
[Edit Route Rules](#)

Edit Route Rules [help](#) [cancel](#)

Important: For a route rule that targets a Private IP, you must first enable "Skip Source/Destination Check" on the VNIC that the Private IP is assigned to.

DESTINATION CIDR BLOCK: 0.0.0.0/0

TARGET TYPE: Private IP

TARGET SELECTION: 10.0.5.100 [OCID: ...6ddudq](#) [×](#)

Save [+ Another Route Rule](#)

Resources
[Route Rules \(1\)](#)

Route Rules
[Edit Route Rules](#)

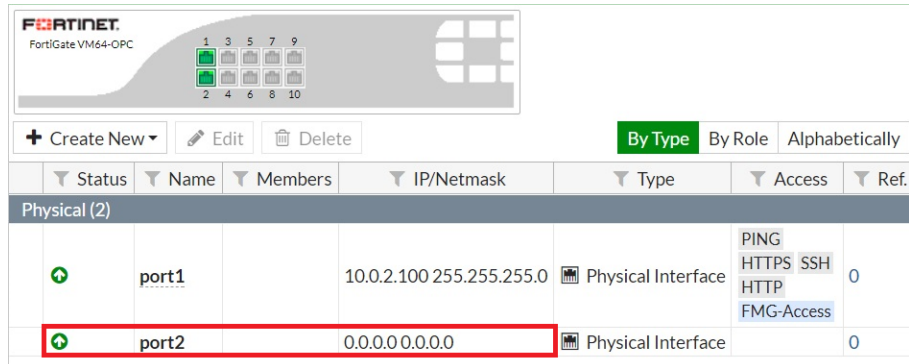
Destination CIDR Block: 0.0.0.0/0

Target Type: Internet Gateway
Target: [Internet Gateway jkato002](#) ...hwm2tq [Show](#) [Copy](#)

Configuring the second VNIC on the FortiGate-VM

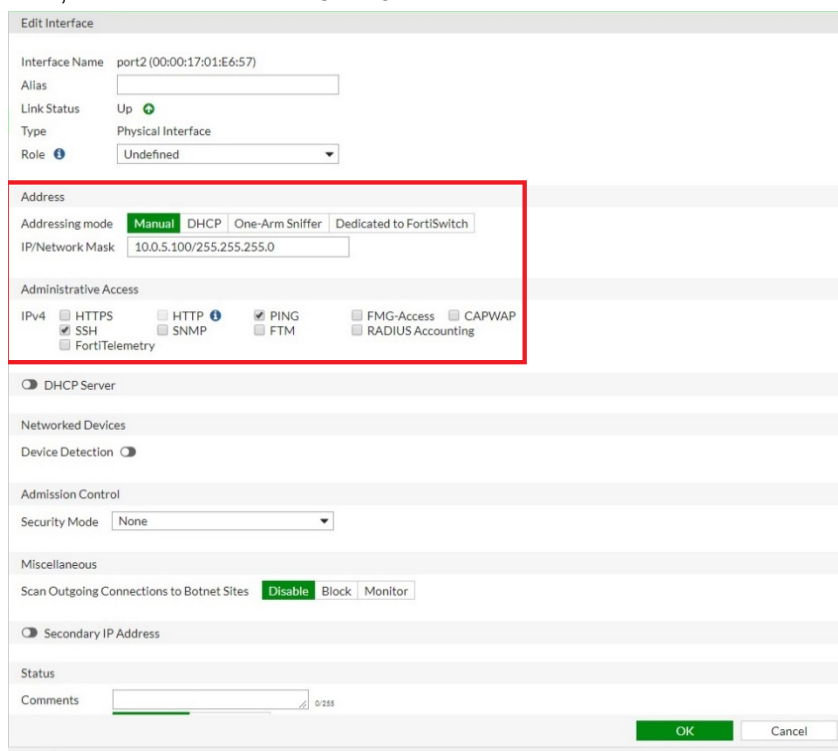
To configure the second VNIC on the FortiGate-VM:

1. After attaching the second VNIC to the FortiGate-VM, ensure you reboot, then log into the FortiGate-VM. Log into the GUI console and go to *Network > Interfaces*. You now see two ports, but the second port is not configured with an IP address. Manually configure the same IP address specified on OCI.



Status	Name	Members	IP/Netmask	Type	Access	Ref.
Physical (2)						
	port1		10.0.2.100 255.255.255.0	Physical Interface	PING HTTPS SSH HTTP FMG-Access	0
	port2		0.0.0.0 0.0.0.0	Physical Interface		0

2. Select port2, then click *Edit*. Manually enter the IP address and netmask. Allow administrative access to PING, SSH, and so on as desired. Click *OK*.



Interface Name: port2 (00:00:17:01:E6:57)

Alias:

Link Status: Up

Type: Physical Interface

Role:

Address

Addressing mode: **Manual** DHCP One-Arm Sniffer Dedicated to FortiSwitch

IP/Network Mask:

Administrative Access

IPv4: ☐ HTTPS ☐ HTTP ☒ PING ☐ FMG-Access ☐ CAPWAP

☒ SSH ☐ SNMP ☐ FTM ☐ RADIUS Accounting

☐ FortiTelemetry

☐ DHCP Server

Networked Devices

Device Detection: ☐

Admission Control

Security Mode:

Miscellaneous

Scan Outgoing Connections to Botnet Sites: **Disable** Block Monitor

☐ Secondary IP Address

Status

Comments:

OK Cancel

You now have two network interfaces configured.

Enabling jumbo frame on the second VNIC

By default, the first virtual network interface (VNIC) port1 is enabled for jumbo frame. You must configure the same on the newly added VNIC port2. For jumbo frame support, refer to [Technical Note: MTU size and Jumbo frames support on](#)

FortiGate devices.

If you look at the VNIC information in the CLI, MTU is set to 9000 by default.

```
FGVM3200000103038 # diagnose hardware deviceinfo nic port1
Name:      port1
Driver:    e1000
Version:   7.3.21-k8-NAPI
FW version: N/A
Bus:       0000:00:03.0
Hwaddr:    00:00:17:02:5a:77
Permanent Hwaddr:00:00:17:02:5a:77
State:     up
Link:      up
Mtu:       9000
Supported: auto 10half 10full 100half 100full 1000full
Advertised: auto 10half 10full 100half 100full 1000full
Speed:     1000full
Auto:      enabled
Rx packets: 1181791
Rx bytes:   476054799
Rx compressed: 0
Rx dropped: 0
Rx errors:  0
  Rx Length err: 0
  Rx Buf overflow: 0
  Rx Crc err: 0
  Rx Frame err: 0
  Rx Fifo overrun: 0
  Rx Missed packets: 0
Tx packets: 1244011
Tx bytes:   151802125
```

After adding the second VNIC in the previous step, it is not set with the jumbo frame by default. As you can see, the MTU is set to 1500.

```
FGVM320000103038 # diagnose hardware deviceinfo nic port2
Name:      port2
Driver:    e1000
Version:   7.3.21-k8-NAPI
FW version: N/A
Bus:       0000:00:05.0
Hwaddr:    00:00:17:02:4c:ee
Permanent Hwaddr:00:00:17:02:4c:ee
State:     up
Link:      up
Mtu:       1500
Supported: auto 10half 10full 100half 100full 1000full
Advertised: auto 10half 10full 100half 100full 1000full
Speed:     1000full
Auto:      enabled
Rx packets: 0
Rx bytes:   0
Rx compressed: 0
Rx dropped: 0
Rx errors:  0
  Rx Length err: 0
  Rx Buf overflow: 0
  Rx Crc err: 0
  Rx Frame err: 0
  Rx Fifo overrun: 0
  Rx Missed packets: 0
Tx packets: 1
Tx bytes:   42
Tx compressed: 0
Tx dropped: 0
Tx errors:  0
```

Run the following CLI commands to change the MTU size on port2. See [Interface MTU packet size](#).

```
config system interface
  edit port2
    set mtu-override enable
    set mtu 9000
```

end

Check if the MTU changed as expected.

```
FGVM320000103038 # diagnose hardware deviceinfo nic port2
Name:      port2
Driver:    e1000
Version:   7.3.21-k8-NAPI
FW version: N/A
Bus:       0000:00:05.0
Hwaddr:    00:00:17:02:4c:ee
Permanent Hwaddr:00:00:17:02:4c:ee
State:     up
Link:      up
Mtu:       9000
Supported: auto 10half 10full 100half 100full 1000full
Advertised: auto 10half 10full 100half 100full 1000full
Speed:     1000full
Auto:      enabled
```

Changing the protected network's default route

Once you have created the VNIC with the private IP address, it is available for you to select it as the default gateway in the route table configuration. Go to the route tables and edit the route rules for the internal network subnet. For all destinations, select *Private IP* as the *Target Type*, and enter the FortiGate-VM's second VNIC's private IP address.

Deploying a native mode FortiGate-VM on OCI

This guide demonstrates how to launch a native mode FortiGate-VM on OCI. This deployment consists of the following steps:

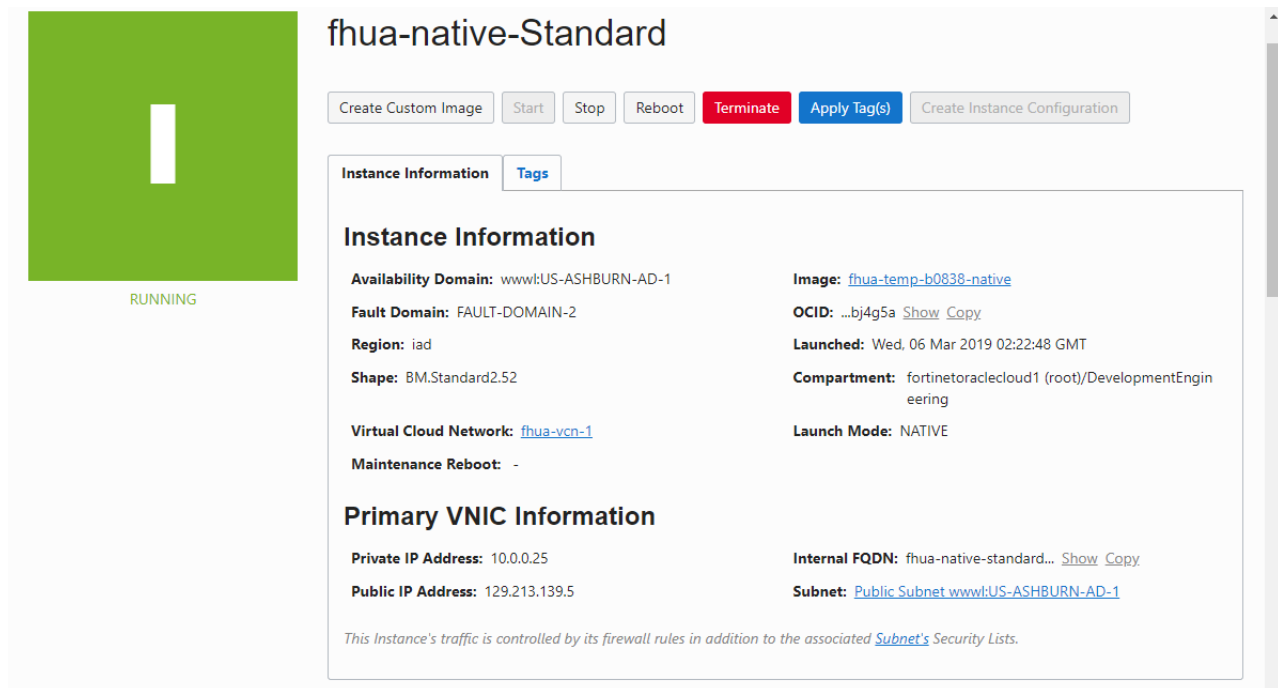
1. [Create a native mode FGT-VM64-OPC custom image.](#)
2. [Create a FGT-VM64-OPC instance with the native mode custom image.](#)
3. [Attach a hard disk to the FGT-VM64-OPC with Internet Small Computer Systems Interface \(iSCSI\) mode.](#)
4. [Run diagnose commands.](#)

To create a native mode FortiGate-VM custom image:

1. Obtain the deployment image file and upload the forties.qcow2 file to OCI object storage as [To obtain the deployment image file and place it in your bucket: on page 14](#) describes. Obtain the file URL path.
2. Import the image:
 - a. Go to *Compute > Custom Images*. Click *Import Image*.
 - b. In the *Import Image* dialog, complete the fields. In the *OBJECT STORAGE URL* field, enter the URL link obtained in step 1.
 - c. Under *OPERATING SYSTEM*, select *Linux*.
 - d. Under *IMAGE TYPE*, select *QCOW2*.
 - e. Under *LAUNCH MODE*, select *NATIVE MODE*.
 - f. Click *Import Image*. After some time, the FortiGate for OCI custom image becomes available on OCI.

To create a FortiGate-VM instance with the native mode custom image:

1. Log into the OCI web portal. Go to *Compute > Instances > Create Instance*.
2. Configure the FortiGate-VM instance:
 - a. In the *Name your instance* field, enter the desired name for your FortiGate-VM instance.
 - b. Select an availability domain for your instance.
 - c. Under *Choose an operating system or image source*, select the image source as the image created in the previous step.
 - d. Under *Choose instance type*, select *Virtual Machine* or *Bare Metal Machine*.
 - e. Under *Choose instance shape*, select *Change Shape* and select the instance shape.
 - f. Under *Configure networking*, select your virtual cloud network and subnet.
 - g. Leave the *Configure boot volume* options at their default values. You can also add an SSH key file if desired.
3. Click *Create*. After a few minutes, the instance is ready and running. You can access the FortiGate-VM with your SSH key or using the username "admin" and the OCID as the password.
4. Go to the *Instance Information* tab for the FortiGate-VM. Verify that the instance's *Launch Mode* displays as *NATIVE*.



The screenshot shows the OCI Instance Information page for an instance named 'fhua-native-Standard'. The instance is in a 'RUNNING' state, indicated by a green square icon. The page includes a navigation bar with buttons: 'Create Custom Image', 'Start', 'Stop', 'Reboot', 'Terminate', 'Apply Tag(s)', and 'Create Instance Configuration'. Below the navigation bar, there are two tabs: 'Instance Information' (selected) and 'Tags'. The 'Instance Information' section displays the following details:

- Availability Domain:** wwwk-US-ASHBURN-AD-1
- Fault Domain:** FAULT-DOMAIN-2
- Region:** iad
- Shape:** BM.Standard2.52
- Virtual Cloud Network:** fhua-vcn-1
- Maintenance Reboot:** -
- Image:** fhua-temp-b0838-native
- OCID:** ...bj4g5a [Show Copy](#)
- Launched:** Wed, 06 Mar 2019 02:22:48 GMT
- Compartment:** fortinetoracled1 (root)/DevelopmentEngineering
- Launch Mode:** NATIVE

The **Primary VNIC Information** section shows:

- Private IP Address:** 10.0.0.25
- Public IP Address:** 129.213.139.5
- Internal FQDN:** fhua-native-standard... [Show Copy](#)
- Subnet:** [Public Subnet wwwk-US-ASHBURN-AD-1](#)

A note at the bottom states: 'This Instance's traffic is controlled by its firewall rules in addition to the associated [Subnet's](#) Security Lists.'

To attach a hard disk to the FortiGate-VM with iSCSI mode:

1. From the navigation bar, click *Attach Block Volume*.
2. Under *Choose how you want to attach your block volume*, select *iSCSI*.
3. Leave *ACCESS* at the default value, *READ/WRITE*.
4. Configure other options as desired.
5. Click *Attach*. After a few minutes, the *Instance Information* page shows that the block volume was attached.
6. Under *Attached Block Volumes*, go to the block volume entry, and click *iSCSI Commands & Information*. You can find this iSCSI's IP address and IQN here.
7. Log into the FortiGate and run the following commands to configure the iSCSI hard disk:


```
config system iscsi
  edit "Demo-iSCSI-HD"
```

```

set ip 169.254.2.4 set iqn "iqn.2015-12.com.oracleiaas:debf5040-260a-4a28-a00e-
dal72baa6698"
next
end

```

8. Run the `diagnose hardware deviceinfo disk` command to ensure that the second hard drive (50.0 GiB) is attached. The output should look like the following:

```

Disk SYSTEM(boot) 46.6GiB type: ISCSI [IET Controller] dev: /dev/sda
  partition 123.0MiB, 62.0MiB free mounted: Y label: dev: /dev/sda1(boot) start: 2048
  partition 1.7GiB, 1.7GiB free mounted: Y label: dev: /dev/sda2(boot) start: 264192
  partition ref: 3 127.0MiB, 86.0MiB free mounted: N label: dev: /dev/sda3 start:
    3932160
Disk Virtual-Disk ref: 32 50.0GiB type: ISCSI [IET Controller] dev: /dev/sdc
  partition ref: 33 49.2GiB, 48.9GiB free mounted: N label: LOGUSEDX6FFE3A65 dev:
    /dev/sdc1 start: 2048
Total available disks: 2 Max SSD disks: 8 Available storage disks: 1

```

To run diagnose commands:

1. Run the following commands to configure the iSCSI disk:

```

config system iscsi
  edit "i1"
    set ip class_ip
    set iqn string
  next
end

```

2. Run the `execute iscsi logout <iscsi-disk-name>` command to disconnect the iSCSI disk.
3. Run the `execute iscsi login <iscsi-disk-name>` command to connect the iSCSI disk.

Deploying FortiGate-VM via the marketplace

To deploy FortiGate-VM via the marketplace:

1. Go to *Compute > Instances*. Click *Create Instance*.
2. Enter the desired instance name.
3. For *Choose an operating system or image source*, click *Change Image Source*, then *Partner Images > FortiGate Next Gen Firewall (BYOL)*.
4. Select the desired instance shape. If this instance will be part of a high availability topology, select a shape with at least four OCPU.
5. Select the desired VCN and subnet, then click *Create*.



A newly created FortiGate-VM only has one VNIC. To configure a second VNIC, see [Creating the second VNIC on page 24](#) and [Configuring the second VNIC on the FortiGate-VM on page 26](#).

Deploying FortiGate-VM using compute shapes that use Mellanox network cards

You can deploy FortiGate-VMs that are paravirtualized with SR-IOV and DPDK/vNP on OCI shapes that use Mellanox network cards.

To deploy the VM using a Mellanox card:

1. Create an instance using a compute shape that supports the Mellanox network card, such as VM.Standard.E3.Flex.
2. In the OCI console, verify the instance has SR-IOV enabled:

```
# oci compute instance get --instance-id <instance ID>
{
  "data": {
    ...
    "launch-mode": "PARAVIRTUALIZED",
    "launch-options": {
      "boot-volume-type": "PARAVIRTUALIZED",
      "firmware": "BIOS",
      "is-consistent-volume-naming-enabled": false,
      "is-pv-encryption-in-transit-enabled": false,
      "network-type": "VFIO",
      "remote-data-volume-type": "PARAVIRTUALIZED"
    },
    ...
  },
  ...
}
```

The network type is `VFIO` (as opposed to `PARAVIRTUALIZED`), which means that SR-IOV is enabled.

3. In FortiOS, verify that the boot succeeds and check instance details:

```
# get system status
Version: FortiGate-VM64-OPC v6.4.3,buidl1776,201013 (interim)
...
Serial-Number: FGVMLTM20000xxx
IPS Malicious URL Database: 2.00798(2020-10-15 09:20)
License Status: Valid
License Expiration Date: 2021-07-01
VM Resources: 2 CPU, 16085 MB RAM
VM Instance ID: ocid1.instance.oc1.iad.xxxxxxxx
...
```

4. Check the NIC driver to ensure that it is `mlx5_core`:

```
# diagnose hardware deviceinfo nic port1
Name:          port1
Driver:        mlx5_core
...
```

5. Enable DPDK:

```
config dpdk global
  set status enable
  set interface port2 port1
end
```

6. Reboot the FortiGate.

7. Verify the drivers are now net_mlx5 to signify they are DPDK enabled:

```
# diagnose hardware deviceinfo nic port1
Name:          port1
Driver:        net_mlx5
...
```

8. Verify that DPDK was initiated successfully:

```
# diagnose dpdk log show early-init
-----
DPDK early initialization starts at 2020-10-16 00:37:36(UTC)
-----
Content of early configuration file:
status=1
multiqueue=0
sleep-on-idle=0
elasticbuffer=0
per-session-accounting=1
hugepage-percentage=30
nr_hugepages=2412
interfaces=port1 port2
cpus=0 1
rxcpus=0 1
vnpcpus=0 1
ipscpus=0 1
txcpus=0 1
Parse config file success!

Check CPU definitions 'cpus'
Check CPU definitions 'rxcpus'
Check CPU definitions 'ipscpus'
Check CPU definitions 'vnpcpus'
Check CPU definitions 'txcpus'
Check CPUs success!

Huge page allocation done

Ports enabled for DPDK:
port1
port2
Port name to device name mapping:
port1: eth0
port2: eth1
port3: eth2
port4: eth3
...

Start enabling DPDK kernel driver for port 'port1'...
Getting PCI device info for eth0...
reading pci dev /sys/class/net/eth0
link path: ../../devices/pci0000:00/0000:00:03.0/net/eth0
Device info of eth0:
dev_name: eth0
macaddr: 00:00:17:02:3c:d9
pci_vendor: 0x15b3
pci_device: 0x101a
```



```
pci_id: 0000:00:03.0
pci_domain: 0
pci_bus: 0
pci_devid: 3
pci_function: 0
guid: n/a
Device eth0 is mlx5_core name changed to slv0
Creating DPDK kernel driver for device eth0...
Add VNP dev: eth0 PCI: 0000:00:03.0, Succeeded
DPDK kernel driver for eth0 successfully created
DPDK kernel driver enabled for port 'port1' (device name 'eth0')

Start enabling DPDK kernel driver for port 'port2'...
Getting PCI device info for eth1...
reading pci dev /sys/class/net/eth1
link path: ../../devices/pci0000:00/0000:00:05.0/net/eth1
Device info of eth1:
  dev_name: eth1
  macaddr: 02:00:17:02:bd:df
  pci_vendor: 0x15b3
  pci_device: 0x101a
  pci_id: 0000:00:05.0
  pci_domain: 0
  pci_bus: 0
  pci_devid: 5
  pci_function: 0
  guid: n/a
Device eth1 is mlx5_core name changed to slv1
Creating DPDK kernel driver for device eth1...
Add VNP dev: eth1 PCI: 0000:00:05.0, Succeeded
DPDK kernel driver for eth1 successfully created
DPDK kernel driver enabled for port 'port2' (device name 'eth1')
Bind ports success!

Make UIO nodes success!

DPDK sanity test passed
```

9. Send traffic through the FortiGate and verify the statistics to ensure packets actually pass through DPDK:

```
# diagnose dpdk statistics show engine
# diagnose dpdk statistics show port
# diagnose dpdk statistics show vnp
# diagnose dpdk statistics show memory
```

HA for FortiGate-VM on OCI

Deploying FortiGate-VM HA on OCI within one AD

FortiGate active-passive HA

You can configure FortiGate's native active-passive high availability (HA) feature (without using an OCI supplementary mechanism such as a load balancer) with two FortiGate-VM instances: one acting as the primary node and the other as the secondary node, both located in the same availability domain. This guide refers to the primary and secondary nodes as FortiGate A and FortiGate B, respectively. This is called "unicast HA" and is specific to cloud environments, including OCI, to comply to their network restrictions in comparison to an equivalent feature that physical FortiGates provided. The FortiGate-VMs run heartbeats between dedicated ports and synchronize operating system configurations. When the primary node fails, the secondary node takes over as the primary node so endpoints continue to communicate with external resources over the FortiGate-VM. The FortiGates also synchronize sessions at the time of failover.

Using the latest version of FortiGate-VM is always recommended.

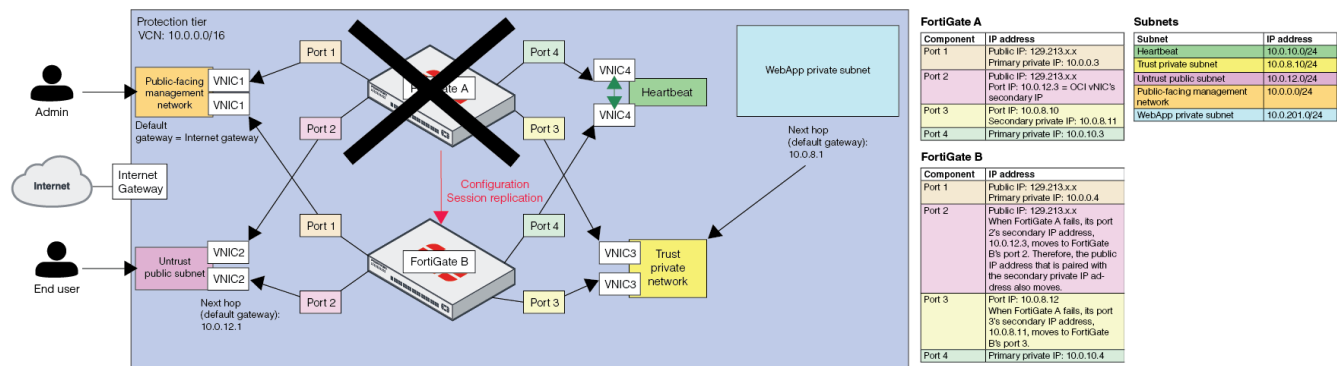


When deploying a FortiGate-VM HA cluster, choose a compute VM shape that supports four or more vNICs for each FortiGate-VM instance.

Two FortiGate-VM instances must be the same compute VM shape.

Deploying and configuring FortiGate active-passive HA

For this HA deployment, you can manually configure two FortiGate-VM instances after deployment on OCI using CLI commands or run Terraform scripts. Terraform scripts for FortiOS Your deployment will have different IP addresses than in the diagram.



Unlike other public clouds, on OCI, you must configure port 1 as the management interface. The other ports are interchangeable. Locating each port in a different subnet is considered best practice. DNS must work with port 1 to resolve OCI's API endpoint URLs at the time of HA failover.



You must configure primary private IP addresses, even where the diagram does not mention them. Although not required for HA purposes, you must do this to comply with general networking requirements.

Checking the prerequisites

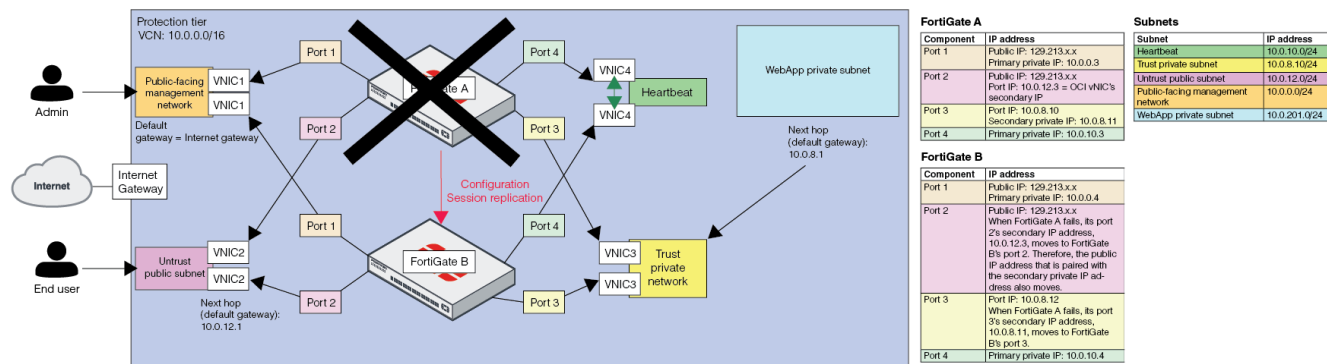
To deploy and configure the FortiGate-VM as an active-passive high availability solution, you need the following items:

- OCI account to operate in OCI compute portal
- Availability to accommodate required OCI resources
 - See [Service Limits](#).
 - VCN with five subnets
 - Three public IP addresses
 - One for traffic to/through the active (primary) FortiGate-VM
 - Two for management access to each FortiGate-VM
 - All IP addresses must be static, not DHCP.
- Two FortiGate-VM instances
 - You must deploy the two nodes in the same availability domain and under the same VCN.
 - Each FortiGate-VM must have at least four network interfaces. See [Compute Shapes](#).
- Two valid FortiGate-VM bring your own license licenses. See [Licensing on page 8](#).
- The following summarizes minimum sufficient IAM roles for this deployment:
 - Allow dynamic-group <group_name> to read compartments in tenancy
 - Allow dynamic-group <group_name> to read instances in tenancy
 - Allow dynamic-group <group_name> to read vnic-attachments in tenancy
 - Allow dynamic-group <group_name> to read subnets in tenancy
 - Allow dynamic-group <group_name> to manage private-ips in tenancy
 - Allow dynamic-group <group_name> to manage public-ips in tenancy
 - Allow dynamic-group <group_name> to manage route-tables in tenancy
 - To define simpler roles, use the following:
 - Allow dynamic-group <group_name> to read compartments in tenancy
 - Allow dynamic-group <group_name> to read instances in tenancy
 - Allow dynamic-group <group_name> to manage virtual-network-family in tenancy



Actual role configurations may differ depending on your environments. Check with your company's public cloud administrators for more details.

Reviewing the network topology



A recommended installation requires four network interfaces per FortiGate-VM node. In addition to inbound and outbound data interfaces, the configuration uses two interfaces for internal operations: management and heartbeat. Ensure you choose OCI VM instance sizes that can equip four network interfaces.

The table describes the usage of each port. Port1 and 2 are on public (or untrusted) subnets, and public IP addresses are allocated to them.

Port	Description
Port 1	Dedicated management interface. In case of heartbeat failure, the passive firewall needs a dedicated port through which to communicate with OCI to issue failover-related commands. This port is always available, regardless of node status (active/passive), except when a node is down. DNS must work with port 1 to resolve OCI's API endpoint URLs at the time of HA failover.
Port 2	External data interface on the public network-facing side. A public IP address for the protected server is associated with the active node's private IP address. FortiGate performs NAT for inbound traffic and outbound traffic.
Port 3	Internal data traffic interface on the protected/trusted network-facing side.
Port 4	Heartbeat between two FortiGate nodes. This is unicast communication. This heartbeat interface has its dedicated "hbdev" VDOM and cannot be used for any other purpose.

You must configure port 1 as the management interface. The other ports are interchangeable. The best practice is to locate each port in a different subnet.



You must configure primary private IP addresses, even where not mentioned in the diagram. Although not required for HA purposes, you must do this to comply with general networking requirements.

Creating a VCN for same-AD HA topology

To create a VCN and public-facing subnets:

1. In OCI, go to *Networking > Virtual Cloud Networks*, and click *Create Virtual Cloud Network*.
2. In the *NAME* field, enter the virtual cloud network (VCN) name. Then, select *CREATE VIRTUAL CLOUD NETWORK PLUS RELATED RESOURCES*. This allows you to create the Internet gateway, routing table, and subnet all together using Oracle default settings. If you intend to create each resource separately by specifying your own inputs, click *CREATE VIRTUAL CLOUD NETWORK ONLY*. This example uses the first choice.

Create Virtual Cloud Network [help](#) [cancel](#)

NAME

fgtvm

CREATE IN COMPARTMENT

DevelopmentEngineering

fortinetoracledcloud1 (root)/DevelopmentEngineering

☐ CREATE VIRTUAL CLOUD NETWORK ONLY
Creates a Virtual Cloud Network only. You'll still need to set up at least one Subnet, Gateway, and Route Rule to have a working Virtual Cloud Network.

☒ CREATE VIRTUAL CLOUD NETWORK PLUS RELATED RESOURCES
Automatically sets up a Virtual Cloud Network with access to the internet. You can set up firewall rules and Security Lists to control ingress and egress traffic to your instances. All related resources will be created in the same Compartment as the VCN.

Create Virtual Cloud Network

DNS RESOLUTION

☒ USE DNS HOSTNAMES IN THIS VCN
Required for instance hostname assignment if you plan to use VCN DNS or a third-party DNS. This choice cannot be changed after the VCN is created. [Learn more](#)

Name: fgtvm

CIDR: 10.0.0.0/16

DNS Label: fgtvm

DNS Domain Name: fgtvm.oraclevcn.com

Create Internet Gateway

Name: Internet Gateway

Update Default Route Table

Add Route Rule: 0.0.0.0/0 - Internet Gateway

Create Subnet

Name: Public Subnet www:CA-TORONTO-1-AD-1

Security List: Default Security List

DHCP Options: Default DHCP Options

CIDR: 10.0.0.0/24; 10.0.0.0 - 10.0.0.255 (256 IP Addresses)

Route Table: Default Route Table

DNS Label: Auto-generated

3. Click *Create Virtual Cloud Network* at the bottom of the screen, then click *Close*. This configures the related resources.
4. Create the other subnets:
 - a. Go to *Networking > Virtual Cloud Networks*. Click the name of the previously created VCN, then click *Create Subnet*.
 - b. For *Subnet Type*, select *Regional*.
 - c. For *Subnet Access*, select *Private* or *Public Subnet* as desired. The screenshot shows the configuration for the public subnet.

Create Subnet [help](#) [cancel](#)

If the Route Table, DHCP Options, or Security Lists are in a different Compartment than the Subnet, enable Compartment selection for those resources: [Click here](#)

NAME

Untrust Public

SUBNET TYPE

☒ REGIONAL (RECOMMENDED)
Instances in the subnet can be created in any availability domain in the region. Useful for high availability.

☐ AVAILABILITY DOMAIN-SPECIFIC
Instances in the subnet can only be created in one availability domain in the region.

CIDR BLOCK

10.0.12.0/24

Specified IP addresses: 10.0.12.0-10.0.12.255 (256 IP addresses)

ROUTE TABLE

Default Route Table for fgtvm

SUBNET ACCESS

☐ PRIVATE SUBNET
Prohibit public IP addresses for Instances in this Subnet

☒ PUBLIC SUBNET
Allow public IP addresses for Instances in this Subnet

DNS RESOLUTION

☒ USE DNS HOSTNAMES IN THIS SUBNET ⓘ
Allows assignment of DNS hostname when launching an Instance

DNS LABEL

UntrustPublic

Only letters and numbers, starting with a letter. 15 characters max.

DNS DOMAIN NAME READ-ONLY

<dns-label>.fgtvm.oraclecn.com

DHCP OPTIONS

Select DHCP Options

Security Lists

SECURITY LIST

Default Security List for fgtvm

+ Additional Security List

TAGS

Tagging is a metadata system that allows you to organize and track resources within your tenancy. Tags are composed of keys and values that can be attached to resources.

[Learn more about tagging](#)

TAG NAMESPACE	TAG KEY	VALUE
None (add a free-form tag)		
+ Additional Tag		

Create Subnet Cancel

Create Subnet
[help](#)
[cancel](#)

If the Route Table, DHCP Options, or Security Lists are in a different Compartment than the Subnet, enable Compartment selection for those resources: [Click here](#)

NAME

SUBNET TYPE

☒ REGIONAL (RECOMMENDED)
Instances in the subnet can be created in any availability domain in the region. Useful for high availability.

☐ AVAILABILITY DOMAIN-SPECIFIC
Instances in the subnet can only be created in one availability domain in the region.

CIDR BLOCK

Specified IP addresses: 10.0.8.0-10.0.8.255 (256 IP addresses)

ROUTE TABLE

SUBNET ACCESS

☒ PRIVATE SUBNET
Prohibit public IP addresses for Instances in this Subnet

☐ PUBLIC SUBNET
Allow public IP addresses for Instances in this Subnet

DNS RESOLUTION

☒ USE DNS HOSTNAMES IN THIS SUBNET ⓘ
Allows assignment of DNS hostname when launching an Instance

DNS LABEL

Only letters and numbers, starting with a letter. 15 characters max.

DNS DOMAIN NAME READ-ONLY

DHCP OPTIONS

Security Lists

SECURITY LIST

+ Additional Security List

TAGS

Tagging is a metadata system that allows you to organize and track resources within your tenancy. Tags are composed of keys and values that can be attached to resources.
[Learn more about tagging](#)

TAG NAMESPACE	TAG KEY	VALUE
None (add a free-form tag)	<input type="text"/>	<input type="text"/>
+ Additional Tag		

Create Subnet
Cancel

- d. Repeat to create a minimum of four subnets for HA setup. The following shows an example of the minimum requirement:

Subnets in DevelopmentEngineering Compartment

Create Subnet				
Name	State	CIDR Block	Subnet Access	Created
heartbeat	Available	10.0.10.0/24	Private (Regional)	Mon, Sep 16, 2019, 5:50:53 PM UTC
trust-private	Available	10.0.8.0/24	Private (Regional)	Mon, Sep 16, 2019, 5:44:59 PM UTC
Untrust-Public	Available	10.0.12.0/24	Public (Regional)	Mon, Sep 16, 2019, 5:39:47 PM UTC
Public Subnet www1-CA-TORONTO-1-AD-1	Available	10.0.0.0/24	Public (www1-CA-TORONTO-1-AD-1)	Mon, Sep 16, 2019, 4:59:05 PM UTC

Showing 4 items < Page 1 >

Deploying the FortiGate-VM

To deploy the FortiGate-VM:

1. Set up the OCI virtual cloud network (VCN) environment. See [Creating a VCN for same-AD HA topology on page 37](#).
2. Deploy FortiGate-VMs in the environment for an active-passive configuration. See [Creating a FortiGate-VM instance on page 13](#). To deploy FortiGate-VM from the marketplace, see [Deploying FortiGate-VM via the marketplace on page 30](#).
3. Configure extra VNICs for the FortiGate-VM. Ensure there are at least four network interfaces configured for each instance. See [Checking the prerequisites on page 35](#). To create an extra VNIC, see [Creating the second VNIC on page 24](#). To configure the extra VNIC, see [Configuring the second VNIC on the FortiGate-VM on page 26](#).
4. Update route rules to point to the internal/trust private IP address on the active FortiGate. Creating a separate route table for the internal/trust subnet is recommended:
 - a. Go to *Networking > Virtual Cloud Networks > <VCN used> > Route Tables*, then click *Create Route Table*.
 - b. Specify the route table to point to the internal/trust private IP address on the active FortiGate:

Create Route Table [help](#) [cancel](#)

NAME

CREATE IN COMPARTMENT

fortinetoracled1 (root)/DevelopmentEngineering

Route Rules

Important: For a route rule that targets a Private IP, you must first enable "Skip Source/Destination Check" on the VNIC that the Private IP is assigned to.

TARGET TYPE

DESTINATION

DESTINATION CIDR BLOCK

Specified IP addresses: 0.0.0.0-255.255.255.255 (4,294,967,296 IP addresses)

COMPARTMENT

fortinetoracled1 (root)/DevelopmentEngineering

TARGET SELECTION

OCID: ...6oph7a

+ Additional Route Rule

- c. Go to *Networking > Virtual Cloud Networks > <VCN used>*. Edit the desired subnet.
- d. Under *Route Table*, update the configuration to the newly created route table.

Configuring the OCI HA interfaces

OCI recommends leaving VM NIC interfaces set to DHCP. This is to avoid potential misaligned configurations. However, when configuring an NVA, you may need to ignore this recommendation. When doing so, ensure that the IP addresses correspond with those intended, so that to the extent required, the configurations match.

In the case of HA, the FortiGate-VMs must have the correct IP address information statically configured to provide proper failover between the two devices.



OCI API calls enable the failover mentioned above through the OCI Fabric connector, but only for IP addresses configured as secondary in the OCI VNIC configuration.

Also, OCI API calls, if initiated from within a VCN, must be made by a primary interface with a public address with DNS properly configured. Thus, the network configuration for OCI HA is unique and specific.



You may lose connection to the instance during interface IP address and route configuration. Therefore, performing this configuration via the console is recommended.

Primary FortiGate

port1

The primary VNIC associated with the FortiGate NVA must have a primary IP address with a corresponding public IP address, and so needs to be configured in a public subnet. This is used as a management interface and also the interface from which API calls are made. You assign this in the HA configuration). See this interface's OCI configuration, then the corresponding FortiGate-VM configuration.

 fgtvminstance-1 (Primary VNIC) OCID: ... Attached: Mon, 16 Sep 2019 18:51:44 UTC Compartment: DevelopmentEngineering	Private IP Address: 10.0.0.3 Fully Qualified Domain Name: fgtvminstance-1... Public IP Address: 132.145.108.199	Subnet: Public Subnet www:CA-TORONTO-1-AD-1 Skip Source/Destination Check: No MAC Address: 02:00:17:00:71:6A VLAN Tag: 2999 Network Security Groups: None Edit
--	---	---

```
config system interface
  edit "port1"
    set vdom "root"
    set ip 10.0.0.3 255.255.255.0
    set allowaccess ping https ssh http fgfm
    set description "management"
    set mtu-override enable
    set mtu 9000
  next
end
```

port2

Beyond port1 (also the primary VNIC), interface order is arbitrary and you can rearrange it. This example assumes port2 to be a public/WAN-facing interface. The following FortiGate configuration does not use the primary IP address for its interface IP address. Instead, the configuration uses the non-primary private IP address, as shown. This is because the

primary IP address is not relocatable to the secondary FortiGate in the event of HA failover. In this example, the FortiGate uses a single secondary IP address with an associated public IP address. In the case of a failover, the secondary IP address and associated public IP address are migrated from the active to the passive FortiGate. Therefore, if the setup uses any extra non-primary private IP addresses in the setup, you must explicitly reference these IP addresses in the interface configuration by enabling secondary IP addresses.

Assign Private IP Address			
	Private IP Address: 10.0.12.4 (Primary IP) Private IP OCID: ...6qizfa Show Copy Private IP Assigned: Mon, 16 Sep 2019 19:03:29 UTC	Fully Qualified Domain Name: Unavailable Public IP Address: 132.145.110.187 (Ephemeral) Public IP OCID: ...arnsxa Show Copy	...
	Private IP Address: 10.0.12.3 Private IP OCID: ...44jhxq Show Copy Private IP Assigned: Mon, 16 Sep 2019 19:30:21 UTC	Fully Qualified Domain Name: Unavailable Public IP Address: 132.145.107.54 (Reserved) Public IP OCID: ...5eme3q Show Copy	...
	Private IP Address: 10.0.12.5 Private IP OCID: ...k7rv6q Show Copy Private IP Assigned: Mon, 16 Sep 2019 21:10:28 UTC	Fully Qualified Domain Name: Unavailable Public IP Address: 132.145.107.42 (Reserved) Public IP OCID: ...xhdoua Show Copy	...

```
config system interface
edit "port2"
set vdom "root"
set ip 10.0.12.3 255.255.255.0
set allowaccess ping https ssh fgfm
set description "untrust"
set secondary-IP enable
set mtu-override enable
set mtu 9000
config secondaryip
edit 1
set ip 10.0.12.5 255.255.255.0
set allowaccess ping https ssh fgfm
next
end
next
end
```

port3

This example configures port3 as the internal port, which the configuration uses to connect to internal resources on local subnets, peered VCNs, and so on. However, as aforementioned, FortiGate does not use the primary IP address. You must still attach the VNIC to the instance with the primary IP address. However, the configuration is synced from the primary FortiGate.

Assign Private IP Address			
	Private IP Address: 10.0.8.3 (Primary IP) Private IP OCID: ...dpo53a Show Copy Private IP Assigned: Mon, 16 Sep 2019 19:38:41 UTC	Fully Qualified Domain Name: Unavailable Public Address: (Not Assigned)	...
	Private IP Address: 10.0.8.10 Private IP OCID: ...6oph7a Show Copy Private IP Assigned: Mon, 16 Sep 2019 19:42:57 UTC	Fully Qualified Domain Name: Unavailable Public Address: (Not Assigned)	...

```
config system interface
edit "port3"
set vdom "root"
set ip 10.0.8.10 255.255.255.0
set allowaccess ping https ssh fgfm
set description "trusted"
set mtu-override enable
set mtu 9000
next
```

end

Enabling *Skip Source/Destination Check* for the VNIC is recommended.

port4

This example uses port4 as the HA interface for heartbeat and configuration synchronization. As such, it only needs a single private IP address.

Assign Private IP Address	
 Private IP Address: 10.0.10.3 (Primary IP) Private IP OCID: mg67ha Show Copy Private IP Assigned: Mon, 16 Sep 2019 19:54:14 UTC	Fully Qualified Domain Name: Unavailable Public IP Address: (Not Assigned)

```
config system interface
  edit "port4"
    set vdom "root"
    set ip 10.0.10.3 255.255.255.0
    set allowaccess ping https ssh fgfm
    set description "heartbeat"
    set mtu-override enable
    set mtu 9000
  next
end
```

Additional configuration

For any unconnected subnets or networks, the FortiGate needs a route assigned to know how to get to them. Typically, you connect these via the internal designated interface. In this case, this is port3. Therefore, a route with a next hop or gateway of the first IP address of the subnet to which port3 belongs is necessary. This can be a specific host route or summary route of some sort.

See the following, where a summary route is configured for 10.0.0.0/16. If this route is not added, the FortiGate communicates with any unconnected routes through the default (0.0.0.0/0) route, which typically should be out the WAN interface (port2 in this example). Since all interfaces are being configured statically and you are not configuring a default route through DHCP, you must also add this default route. If you do not set a destination, FortiOS assumes the default route of 0.0.0.0/0. Therefore, the 2 configuration is the default route.

```
config router static
  edit 2
    set gateway 10.0.12.1
    set device "port2"
  next
  edit 3
    set dst 10.0.0.0 255.0.0.0
    set gateway 10.0.8.1
    set device "port3"
  next
end
```

Secondary FortiGate

For the secondary FortiGate, you do not need to configure port2 or port3, as these configurations should sync from the primary FortiGate.

port1

The primary VNIC associated with the FortiGate NVA must have a primary IP address with a corresponding public IP address, and so must be configured in a public subnet. This is used as a management interface and also the interface from which API calls are made. You assign this in the HA configuration). See this interface's OCI configuration, then the corresponding FortiGate-VM configuration.

Assign Private IP Address	
 Private IP Address: 10.0.0.4 (Primary IP) Private IP OCID: ...cggya Show Copy Private IP Assigned: Mon, 16 Sep 2019 20:05:52 UTC	Fully Qualified Domain Name: fgtvminstance-2- Show Copy Public IP Address: 132.145.109.8 (Ephemeral) Public IP OCID: ...hoshva Show Copy

```
config system interface
  edit "port1"
    set vdom "root"
    set ip 10.0.0.4 255.255.255.0
    set allowaccess ping https ssh http fgfm
    set description "management"
    set mtu-override enable
    set mtu 9000
  next
end
```

port2

You must attach the VNIC to the instance with the primary IP address. However, the FortiGate syncs the configuration from the primary unit.

 Private IP Address: 10.0.12.2 (Primary IP) Private IP OCID: ...m3e62q Show Copy Private IP Assigned: Mon, 16 Sep 2019 20:10:45 UTC	Fully Qualified Domain Name: Unavailable Public IP Address: (Not Assigned)
---	---

port3

You must attach the VNIC to the instance with the primary IP address. However, the FortiGate syncs the configuration from the primary unit.

 Private IP Address: 10.0.8.2 (Primary IP) Private IP OCID: ...lrebzq Show Copy Private IP Assigned: Mon, 16 Sep 2019 20:18:37 UTC	Fully Qualified Domain Name: Unavailable Public IP Address: (Not Assigned)
--	---

port4

This example uses port4 as the HA interface for heartbeat and configuration synchronization. As such, it only needs a single private IP address.

Assign Private IP Address	
 Private IP Address: 10.0.10.4 (Primary IP) Private IP OCID: ...iwp32q Show Copy Private IP Assigned: Mon, 16 Sep 2019 20:20:44 UTC	Fully Qualified Domain Name: Unavailable Public IP Address: (Not Assigned)

```
config system interface
  edit "port4"
    set vdom "root"
```

```
set ip 10.0.10.4 255.255.255.0
set allowaccess ping https ssh fgfm
set description "heartbeat"
next
end
```

Initial Fabric connector configuration

You must configure a Fabric connector in FortiOS. Calling APIs to OCI during HA failover requires this step.

Follow the steps in [Certificate-based SDN connector user privileges on page 77](#). Ensure you can successfully call APIs to OCI by referring to [Troubleshooting OCI SDN connector on page 77](#).

You must ensure that HA status is enabled for the Fabric connector:

```
config system sdn-connector
edit "oci"
set type oci
set ha-status enable
next
end
```

You must then configure A-P HA settings by using CLI commands on the GUI or via SSH.

Using a custom certificate

OCI requires a mechanism to append a certain signature/credential in making API requests. Currently FortiGate uses a certificate to do so. You must specify a certificate on the FortiGate for OCI when configuring A-P HA. The certificate calls APIs to OCI. In the previous deployment step, you used a built-in FortiGate certificate called "Fortinet_Factory".

For greater security, OCI recommends rotating the security element periodically. You may want to change the default certificate after some time, or if you have multiple sets of A-P HA clusters, you may want to use a different certificate for each cluster initially.

This section explains how to replace the certificate. This example uses a self-signed certificate that you created for your organization outside of the FortiGate. For details about the certificates that OCI requires, see [Request Signatures](#).

You need three files:

- Certificate file (for use on the FortiGate)
- Key file (for use on the FortiGate)
- PEM file (for use on OCI)

The signing algorithm must be RSA SHA-256. In this example, you have used an RSA-2048-bit key to create a certificate.

To use a custom certificate:

1. Import your custom certificate to the primary FortiGate. There is no need to do the same on the secondary unit, as A-P HA enables a feature called configuration synchronization, where the certificate is automatically applied to the secondary unit with the FortiOS configuration:
 - a. Log into the primary FortiGate and go to *System > Certificates*. The list of available FortiGate certificates displays.
 - b. Have a pair of the certificate and key files ready on the PC.


- c. Click *Import > Local Certificate*. In the *Import Certificate* panel, for *Type*, select *Certificate*.
- d. Upload the pair of certificate and key files. In this example, the file names are *apache-selfsigned.crt* and *apache-selfsigned.key*, respectively. Enter the password if any, and name the certificate as desired. Click *OK*.

Import Certificate

Type	Local Certificate	PKCS #12 Certificate	Certificate
Certificate file	+ apache-selfsigned.crt		
Key file	+ apache-selfsigned.key		
Password	<input type="password"/>		
Certificate Name	new-cert1		

- e. The certificate displays on the screen. Double-click to show certificate detail.

Certificate Detail Information



new-cert1 (CA)

Serial Number: E5:04:FE:F5:89:E1:35:D4

Subject Information	
Common Name (CN)	localhost
Organization (O)	JKATO, Inc.
Organization Unit (OU)	IT
Locality (L)	Burnaby
State (ST)	BC
Country/Region (C)	CA
Email Address	jkato@fortinet.com
Issuer	
Common Name (CN)	localhost
Organization (O)	JKATO, Inc.
Organization Unit (OU)	IT

2. Edit the OCI SDN connector created earlier. You can do this via the GUI or the CLI.

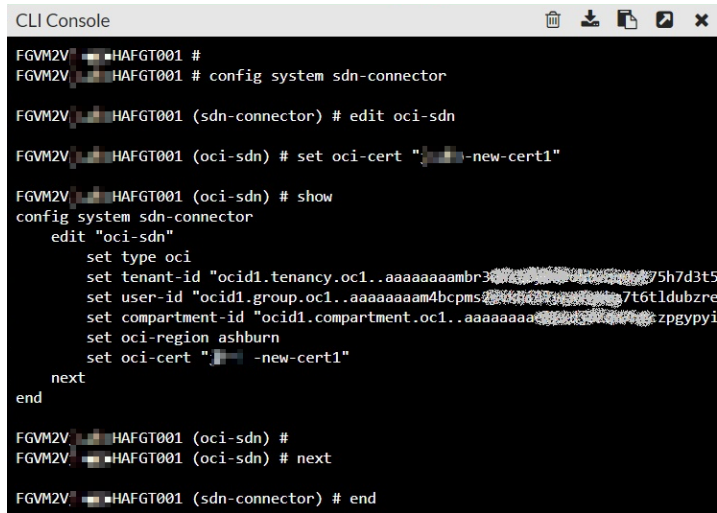
- a. To edit the SDN connector via the GUI, do the following:
 - i. Go to *Security Fabric > External Connectors*.
 - ii. Select the Fabric connector, then click *Edit*.
 - iii. From the *Certificate* dropdown list, select the newly created certificate.
 - iv. Click *OK*.
- b. To edit the Fabric connector via the CLI, do the following:
 - i. Open the CLI console in the FortiGate-VM management console.
 - ii. Enter CLI commands as follows to point to the new certificate. The `show` command shows what is currently configured. `next` and `end` save the configuration and returns to the original indentation with which you started. Replace `oci-sdn` with the name you configured for your Fabric connector, and enter the desired certificate name. The example certificate name is `jkato-new-cert1`.

```
config system sdn-connector
edit oci-sdn
```

```

    set oci-cert "your_certificate_name"
  next
end

```



```

CLI Console
FGVM2V HAFGT001 #
FGVM2V HAFGT001 # config system sdn-connector

FGVM2V HAFGT001 (sdn-connector) # edit oci-sdn

FGVM2V HAFGT001 (oci-sdn) # set oci-cert "new-cert1"

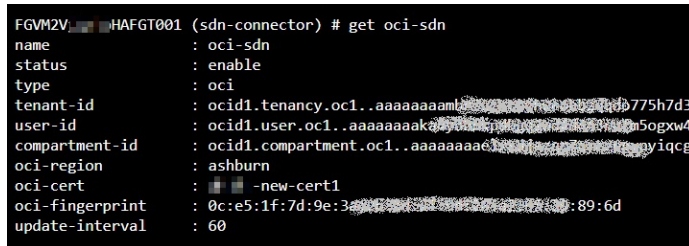
FGVM2V HAFGT001 (oci-sdn) # show
config system sdn-connector
edit "oci-sdn"
set type oci
set tenant-id "ocid1.tenancy.oc1..aaaaaaaambr3...75h7d3t5
set user-id "ocid1.group.oc1..aaaaaaaam4bcps...7t6tldubzre
set compartment-id "ocid1.compartment.oc1..aaaaaaaam...zpgypy1
set oci-region ashburn
set oci-cert "new-cert1"
next
end

FGVM2V HAFGT001 (oci-sdn) #
FGVM2V HAFGT001 (oci-sdn) # next

FGVM2V HAFGT001 (sdn-connector) # end

```

You can see the configuration by running `get OCI_connector_name`.

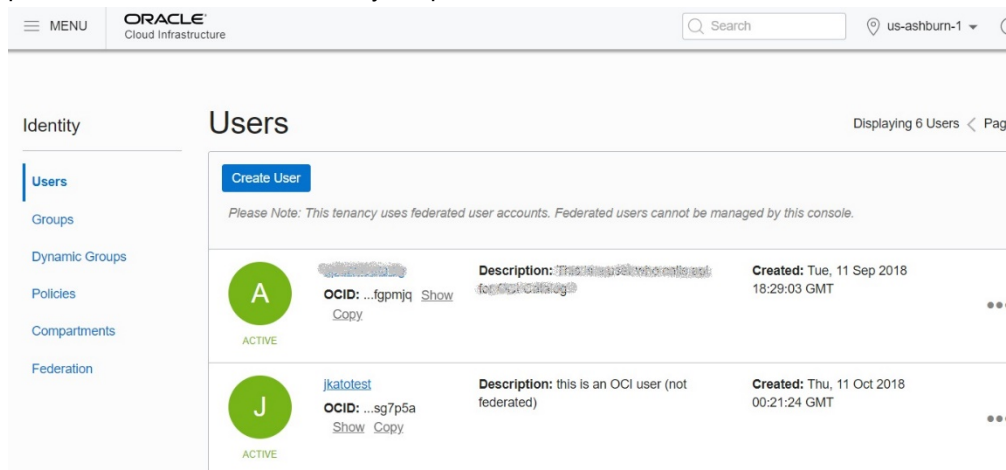


```

FGVM2V HAFGT001 (sdn-connector) # get oci-sdn
name          : oci-sdn
status        : enable
type          : oci
tenant-id     : ocid1.tenancy.oc1..aaaaaaaambr3...75h7d3t5
user-id       : ocid1.user.oc1..aaaaaaaam4bcps...7t6tldubzre
compartment-id : ocid1.compartment.oc1..aaaaaaaam...zpgypy1
oci-region    : ashburn
oci-cert      : new-cert1
oci-fingerprint : 0c:e5:1f:7d:9e:3...:89:6d
update-interval : 60

```

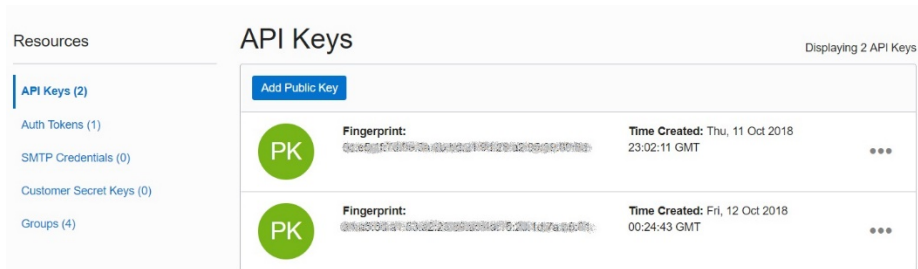
- Next, you must add a new fingerprint for the user based on the new certificate's PEM. Log into the OCI compute portal and locate the user, which you specified with *user-id* above.



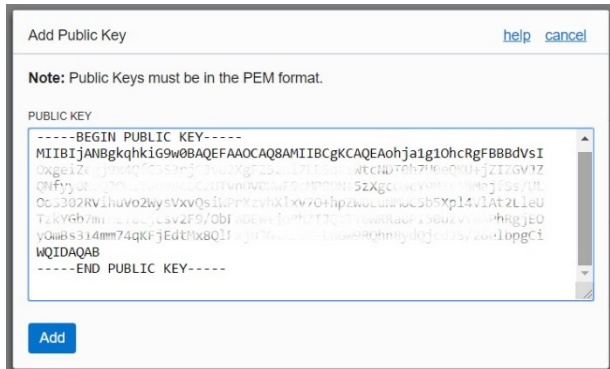
The screenshot shows the Oracle Cloud Infrastructure (OCI) Identity console. The left sidebar contains a menu with options: Identity, Users, Groups, Dynamic Groups, Policies, Compartments, and Federation. The main area is titled 'Users' and shows a list of users. A 'Create User' button is at the top. A note states: 'Please Note: This tenancy uses federated user accounts. Federated users cannot be managed by this console.' The list displays two users:

User	OCID	Description	Created
A	...fgpmjq	This is a user (not federated)	Tue, 11 Sep 2018 18:29:03 GMT
J	...sg7p5a	this is an OCI user (not federated)	Thu, 11 Oct 2018 00:21:24 GMT

- a. Select the user and go to API Keys. Click *Add Public Key*.



- b. Copy and paste the content of the PEM key. Click *Add*.



You should see that a new fingerprint has been added. You can also see the fingerprint in the CLI by running the `get OCI_connector_name` command.

```
FGVM2V... HAFGT001 (sdn-connector) # get oci-sdn
name          : oci-sdn
status        : enable
type          : oci
tenant-id     : ocid1.tenancy.oc1..aaaaaaaa...775h7d3t
user-id       : ocid1.user.oc1..aaaaaaaak...5ogxw4f
compartment-id : ocid1.compartment.oc1..aaaaaaa6...pyicgk
oci-region    : ashburn
oci-cert      : -new-cert1
oci-fingerprint : 0c:e5:1f:7d:9e:3...:89:6d
update-interval : 60
```

4. Check if you can successfully make API calls by referring to [Troubleshooting OCI SDN connector on page 77](#).

Configuring active-passive HA

This step shows you how to configure A-P HA settings by using CLI commands on the GUI or via SSH.

In the commands, note the following:

- Port4 is the hbdev port used for heartbeat connection.
- For the management interface, you must use port 1, as OCI allows only port 1 for metadata access.
- When setting priority on FortiGate B, set the priority to 100 (lower than FortiGate A's priority level). The node with the lower priority level is determined as the secondary node.
- When setting the unicast heartbeat peer IP address (the last command), this is the IP address on the peer, which in the example is FortiGate B, which has port4 IP address 10.0.10.4 in the example. When setting FortiGate B's configuration, specify FortiGate A's port4 IP address, which is 10.0.10.3.

The following is the primary FortiGate configuration:

```
config system ha
set group-id 30
```



```
set group-name "ha-cluster"
set mode a-p
set hbdev "port4" 50
set session-pickup enable
set session-pickup-connectionless enable
set ha-mgmt-status enable
config ha-mgmt-interfaces
  edit 1
    set interface "port1"
    set gateway 10.0.0.1
  next
end
set override disable
set priority 200
set unicast-hb enable
set unicast-hb-peerip 10.0.10.4
end
```

Once configuration is complete, exit the CLI or SSH session.

The following is the secondary FortiGate configuration:

```
config system ha
  set group-id 30
  set group-name "ha-cluster"
  set mode a-p
  set hbdev "port4" 50
  set session-pickup enable
  set session-pickup-connectionless enable
  set ha-mgmt-status enable
  config ha-mgmt-interfaces
    edit 1
      set interface "port1"
      set gateway 10.0.0.1
    next
  end
  set override disable
  set priority 100
  set unicast-hb enable
  set unicast-hb-peerip 10.0.10.3
end
```

Troubleshooting

To validate your HA configuration sync you can issue:

```
diagnose sys ha checksum show
```

OCI components in FortiOS come with their own daemon, including debug output. This can be invoked with:

```
diagnose debug application ocid -99
```

You can display diagnose commands with:

```
diagnose test application ocid -1
1. show HA stats
2. SDN api test
3. HA api test
4. filter list test
```

```
99. restart
```

You can verify that the following `diagnose` command works for the `ocid` daemon:

On FortiGate A:

```
diag test application ocid 1
ocid stats:
master: 1
```

On FortiGate B:

```
diag test application ocid 1
ocid stats:
master: 0
```

`SDN api test` is practical to see whether your `sdn-connector` configuration can successfully authenticate and issue commands to OCI Management.

Running `HA api test` on production environments is not recommended. This may lead your cluster to a mixed state. Use it only to see whether `ocid` daemon successfully sends failover commands to OCI Management.

If you have performed any modifications to your CLI configuration, restart your `ocid` daemon by running the following commands:

```
diag test application ocid 99
ocid start
```

By default, all configuration between firewalls is synchronized. Since some settings, especially NAT, are node-specific, you may want to disable synchronization.

```
config system ha
    set sync-config disable
end
```

During a successful HA failover event, the secondary FortiGate-VM takes over the private IP address from the active unit to the passive unit. The following shows the sample debug output in this scenario:

```
FGVM8VTM19000449 # diag debug enable
FGVM8VTM19000449 # diag debug application ocid -1
Debug messages will be on for 30 minutes.
FGVM8VTM19000449 # HA event
Become HA master
ocid collect vnics info for instance fgtvminstance-2
vnic id(1/4): ocidl.vnic.oc1.ca-toronto-
1.ab2g6ljraiheu5bqvq5riy4rsngg2lm6z766glghhlneqjld3gcpquuhlv5a
vnic id(2/4): ocidl.vnic.oc1.ca-toronto-
1.ab2g6ljrhxf63fvlacjnyl6del3vzo42g5cjyvlczvosxuc5dtn4zqrnwds
vnic id(3/4): ocidl.vnic.oc1.ca-toronto-
1.ab2g6ljr3hmbq675vbgjbuwn2aywjhonqmw5slxjitwy4pyw3fipa2wzwpq
vnic id(4/4): ocidl.vnic.oc1.ca-toronto-
1.ab2g6ljruyxpzi4db2tjet45gix3qauwwgnvf3pbsjcvbd337rgr7ygyy4ka
ocid fail over private ip: 10.0.12.3
private ip 10.0.12.3 is attached in remote instance
attaching private ip 10.0.12.3 to local vnic (ocidl.vnic.oc1.ca-toronto-
1.ab2g6ljraiheu5bqvq5riy4rsngg2lm6z766glghhlneqjld3gcpquuhlv5a)
updating private ip with data: {"vnicId": "ocidl.vnic.oc1.ca-toronto-
1.ab2g6ljraiheu5bqvq5riy4rsngg2lm6z766glghhlneqjld3gcpquuhlv5a"}
moving private ip 10.0.12.3 to local successfully
ocid fail over private ip: 10.0.12.5
private ip 10.0.12.5 is attached in remote instance
```

```

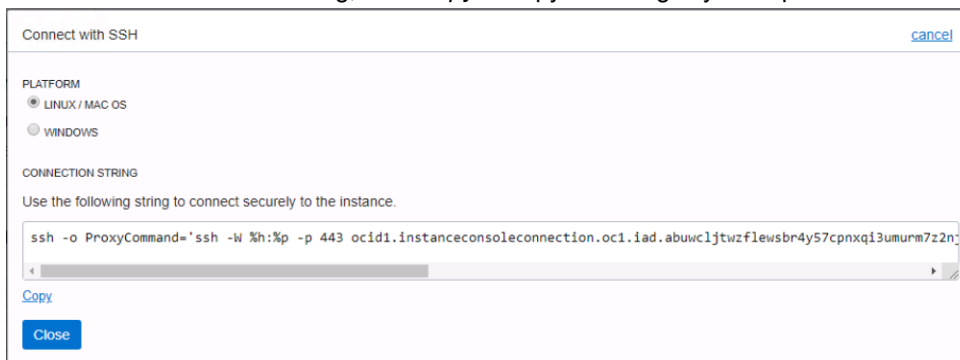
attaching private ip 10.0.12.5 to local vnic (ocidl.vnic.oc1.ca-toronto-
1.ab2g61jraiheu5bqvq55riy4rsngg2lm6z766glghhlneqjld3gcpquuhlv5a)
updating private ip with data: {"vnicId": "ocidl.vnic.oc1.ca-toronto-
1.ab2g61jraiheu5bqvq55riy4rsngg2lm6z766glghhlneqjld3gcpquuhlv5a"}
moving private ip 10.0.12.5 to local successfully
ocid fail over private ip: 10.0.8.10
private ip 10.0.8.10 is attached in remote instance
attaching private ip 10.0.8.10 to local vnic (ocidl.vnic.oc1.ca-toronto-
1.ab2g61jr3hmbq675vbqjbuwn2aywjhonqmb5slxjity4pyw3fipa2wzwpq)
updating private ip with data: {"vnicId": "ocidl.vnic.oc1.ca-toronto-
1.ab2g61jr3hmbq675vbqjbuwn2aywjhonqmb5slxjity4pyw3fipa2wzwpq"}
moving private ip 10.0.8.10 to local successfully

```

To access FortiOS via the console:

If the instance is malfunctioning, you can attempt access to the instance via the console for troubleshooting.

1. Create the console connection for an instance:
 - a. In the OCI console, go to *Core Infrastructure > Compute > Instances*. Select the desired instance name.
 - b. Go to *Resources > Console Connections*. Click *Create Console Connection*.
 - c. Specify the public key (.pub) portion for the SSH key. You can browse to a public key file on your computer or paste your public key into the text field. Then, click *Create Console Connection*. When the console connection has been created and is available, the status changes to *ACTIVE*.
2. Connect to FortiOS via the console using OpenSSH on macOS or Linux:
 - a. Click the *Actions* icon, then click *Connect with SSH*.
 - b. In the *Connect with SSH* dialog, click *Copy* to copy the string to your clipboard.



- c. Use the string to connect to the FortiGate-VM instance. Ensure that you specify the correct SSH key and use `-i`:


```
ssh -i id_rsa -o ProxyCommand='ssh -i id_rsa -W %h:%p -p 443 ....'
```

Deploying FortiGate-VM HA on OCI between multiple ADs

When deploying FortiGate-VM active-passive HA on OCI between multiple ADs, the following differs from when deploying within one AD:

- You do not need to allocate a secondary private IP address for the OCI NIC because a private IP address cannot be moved across ADs.
- During failover, the public IP address detaches from the old primary FortiGate NIC and attaches to the new primary FortiGate NIC.

- Route next hop updates to point to the new primary FortiGate NIC's primary private IP address.
- System interfaces, static route configurations, and sessions do not sync between FortiGates when deployed between multiple ADs. They do sync when deploying within one AD.

This guide refers to the primary FortiGate in AD 1 as "FGT-A-AD1" and the secondary FortiGate, located in AD2, as "FGT-B-AD2".



IPsec VPN phase 1 configuration does not synchronize between primary and secondary FortiGates across ADs. Phase 2 configuration does synchronize.

Checking the prerequisites

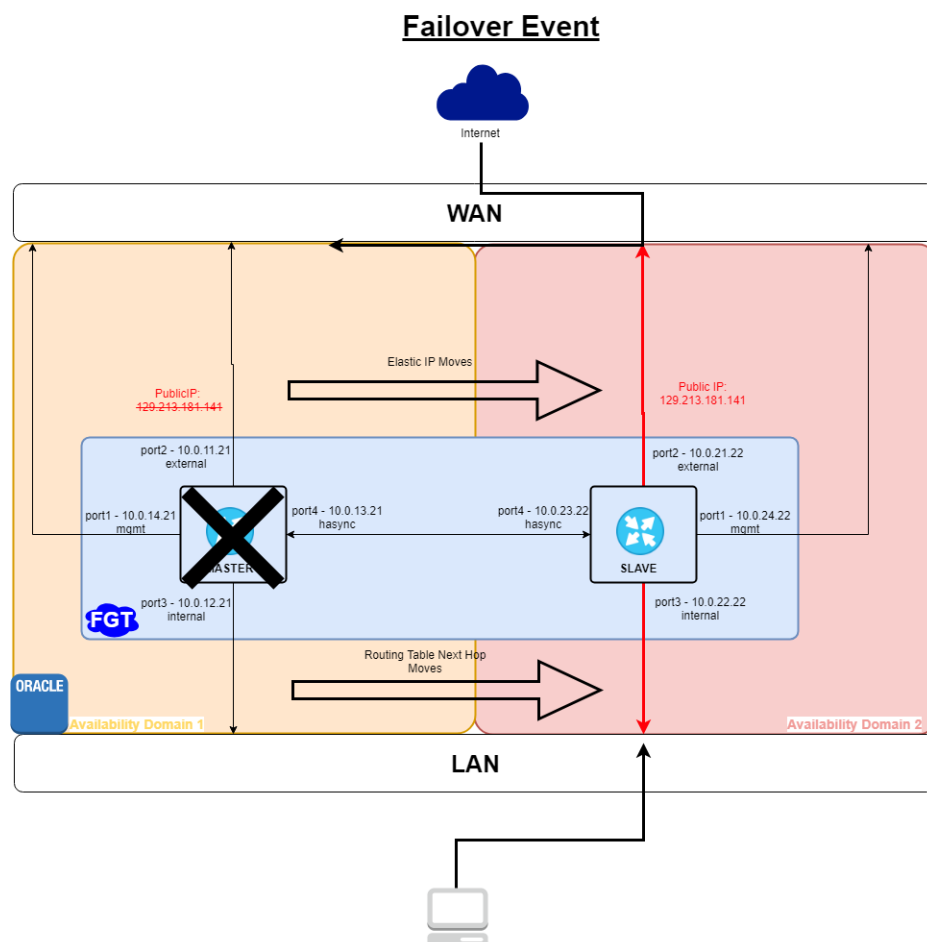
To deploy and configure the FortiGate-VM as an A-P HA solution, you need the following items:

- OCI account to operate in OCI compute portal
- Availability to accommodate required OCI resources
 - See [Service Limits](#).
 - VCN with eight subnets located in two different ADs for management, external, internal, and heartbeat purposes.
 - Three public IP addresses
 - All IP addresses must be static, not DHCP.
 - Two FortiGate-VM instances
- Two valid FortiGate-VM BYOL licenses. See [Licensing on page 8](#)
- The following summarizes minimum sufficient IAM roles for this deployment:
 - Allow dynamic-group <group_name> to read compartments in tenancy
 - Allow dynamic-group <group_name> to read instances in tenancy
 - Allow dynamic-group <group_name> to read vnic-attachments in tenancy
 - Allow dynamic-group <group_name> to read subnets in tenancy
 - Allow dynamic-group <group_name> to manage private-ips in tenancy
 - Allow dynamic-group <group_name> to manage public-ips in tenancy
 - Allow dynamic-group <group_name> to manage route-tables in tenancy
 - To define simpler roles, use the following:
 - Allow dynamic-group <group_name> to read compartments in tenancy
 - Allow dynamic-group <group_name> to read instances in tenancy
 - Allow dynamic-group <group_name> to manage virtual-network-family in tenancy



Actual role configurations may differ depending on your environments. Check with your company's public cloud administrators for more details.

Reviewing the network topology



The following table describes the IP address assignments for FGT-A-AD1:

Port	OCI primary IP address	Subnet
Port 1	10.0.14.21	10.0.14.0/24 EIP1
Port 2	10.0.11.21	10.0.11.0/24 EIP3
Port 3	10.0.12.21	10.0.12.0/24
Port 4	10.0.13.21	10.0.13.0/24

The following table describes the IP address assignments for FGT-B-AD2:

Port	OCI primary IP address	Subnet
Port 1	10.0.24.22	10.0.24.0/24 EIP1
Port 2	10.0.21.22	10.0.21.0/24 EIP3
Port 3	10.0.22.22	10.0.22.0/24

Port	OCI primary IP address	Subnet
Port 4	10.0.23.22	10.0.23.0/24

Configuring the OCI VCN

To configure the OCI VCN:

1. In the OCI console, go to *Networking > Virtual Cloud Networks > Subnets*.
2. Ensure that the VCN contains the following eight subnets (four in AD1 and four in AD2):

AD1 subnet	AD2 subnet	Purpose
net11-external	net21-external	External data traffic on the public network-facing side.
net12-internal	net22-internal	Internal data traffic on the protected/trusted network-facing side.
net13-heartbeat	net23-heartbeat	Heartbeat between two FortiGate nodes. This is unicast communication.
net14-mgmt	net24-mgmt	Dedicated management interface use.

3. Go to *Route Tables*.
4. Configure an internal routing table, setting the default gateway as FGT-A-AD1 NIC2's primary IP address (10.0.12.21). You can create this routing table after configuring NIC2 on FGT-A-AD1. Two subnets, net12-internal and net22-internal, use this routing table.
5. Configure an external routing table, setting the default gateway as this VCN's Internet gateway. The remaining six subnets use this routing table.

Deploying the FortiGate-VM

1. Prepare your OCI environment as detailed in [Configuring the OCI VCN on page 54](#) if you do not have one yet.
2. To take advantage of A-P HA, you need four VNICs (port1 to port4) on each FortiGate-VM that constitutes an A-P HA cluster. Configure all required network interfaces (OCI VNICs and FortiGate-VM network interface configuration) that support A-P HA. You must choose an OCI instance type that supports at least four VNICs.
3. Ensure you configure the security list on each subnet for egress and ingress interfaces appropriately. It is particularly important that the management interfaces have egress Internet access for API calls to the OCI metadata server.
4. Ensure that you attached four NICs to each FortiGate and that you assigned the static private IP address.

Configuring active-passive HA

This step shows you how to configure A-P HA settings by using CLI commands on the GUI or via SSH. If using SSH, the FortiGate may lose connection due to routing table changes, so configuring HA via the GUI is recommended.

To configure the HA interfaces on FGT-A-AD1:

```
config system interface
  edit "port1"
    set mode static
    set ip 10.0.14.21 255.255.255.0
    set allowaccess ping https ssh snmp http
  next
  edit "port2"
    set ip 10.0.11.21 255.255.255.0
    set allowaccess ping https ssh snmp http
  next
  edit "port3"
    set ip 10.0.12.21 255.255.255.0
    set allowaccess ping https ssh snmp http
  next
  edit "port4"
    set ip 10.0.13.21 255.255.255.0
    set allowaccess ping https ssh snmp http
  next
end
```

To configure the HA interfaces on FGT-B-AD2:

```
config system interface
  edit "port1"
    set mode static
    set ip 10.0.24.22 255.255.255.0
    set allowaccess ping https ssh snmp http
  next
  edit "port2"
    set ip 10.0.21.22 255.255.255.0
    set allowaccess ping https ssh snmp http
  next
  edit "port3"
    set ip 10.0.22.22 255.255.255.0
    set allowaccess ping https ssh snmp http
  next
  edit "port4"
    set ip 10.0.23.22 255.255.255.0
    set allowaccess ping https ssh snmp http
  next
end
```

To configure the routing tables on FGT-A-AD1:

```
config router static
  edit 1
    set gateway 10.0.11.1
    set device "port2"
  next
  edit 2
    set dst 10.0.22.0 255.255.255.0
    set gateway 10.0.12.1
    set device "port3"
  next
end
```

To configure the routing tables on FGT-B-AD2:

```
config router static
  edit 1
    set gateway 10.0.21.1
    set device "port2"
  next
  edit 2
    set dst 10.0.12.0 255.255.255.0
    set gateway 10.0.22.1
    set device "port3"
  next
end
```

To configure the OCI Fabric connector on FGT-A-AD1 and FGT-B-AD2:

```
config system sdn-connector
  edit "FGT-OCI-SDN"
    set type oci
    set use-metadata-iam disable
    set ha-status enable
    set tenant-id
      "ocidl.tenancy.oc1..aaaaaaaambr3uzztoyhweohbzqqdo775h7d3t54zpmzkgp4b2cf35vs55ck3a"
    set user-id
      "ocidl.user.oc1..aaaaaaaakgeja4xkdvgfcsfyctpj5gxwjlogq4iv3l673wsaljbfluegzh3q"
    set compartment-id
      "ocidl.tenancy.oc1..aaaaaaaambr3uzztoyhweohbzqqdo775h7d3t54zpmzkgp4b2cf35vs55ck3a"
    set oci-region "us-ashburn-1"
    set oci-cert "Fortinet_Factory"
  next
end
```



The Fabric connector settings are the same on both FortiGates. Ensure that you imported the oci-cert public key as an OCI user API key. You can print the certificate public key in the FortiOS CLI with the `diagnose oci pubkey` command.

To configure the firewall policy on FGT-A-AD1 and FGT-B-AD2:

```
config firewall policy
  edit 1
    set srcintf "port3"
    set dstintf "port2"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set nat enable
  next
end
```

To configure HA settings on FGT-A-AD1:

```
config system ha
  set group-name "ha-cross-ad"
```



```

set mode a-p
set hbdev "port4" 50
set ha-mgmt-status enable
config ha-mgmt-interfaces
  edit 1
    set interface "port1"
    set gateway 10.0.14.1
  next
end
set unicast-hb enable
set unicast-hb-peerip 10.0.23.22
end

```

To configure HA settings on FGT-B-AD2:

You must set the FGT-B HA priority to a value lower than FGT-A's priority level. The node with the lower priority level is determined as the secondary node.

```

config system ha
  set group-name "ha-cross-ad"
  set mode a-p
  set hbdev "port4" 50
  set ha-mgmt-status enable
  config ha-mgmt-interfaces
    edit 1
      set interface "port1"
      set gateway 10.0.24.1
    next
  end
  set priority 64
  set unicast-hb enable
  set unicast-hb-peerip 10.0.13.21
end

```

Checking the HA status and function

To check the HA status and function:

1. In FortiOS on the primary FortiGate, go to *System > HA*. Check that the HA status is synchronized.

<div> </div> <div>List Faceplate All</div>							
Synchronized	Priority	Hostname	Serial No.	Role	Uptime	Sessions	Throughput
<div> </div>	128	FGT-A-AD1	FGVM32	Master	00:18:22:27	46	230.00 kbps
<div> </div>	64	FGT-B-AD2	FGVM32	Slave	00:17:36:55	7	15.00 kbps

2. Create one PC in the internal subnet located in AD1, and another PC in the internal subnet located in AD2. Verify that both PCs can access the Internet via FGT-A-AD1, the current primary node.
3. Shut down FGT-A-AD1.
4. Verify that FGT-B-AD2 becomes the primary FortiGate.
5. Use an API call to verify that the internal routing table's next hop changed from FGT-A-AD1's internal NIC address (10.0.12.21) to FGT-B-AD2's internal NIC address (10.0.22.22) and that the EIP address attached to FGT-A-AD1's

external NIC reattached to FGT-B-AD2's external NIC. You can also use the following diagnose command:

```
FGT-B-AD2 # d deb app ocid -1
Debug messages will be on for 30 minutes.
```

```
FGT-B-AD2 # d deb en
```

```
FGT-B-AD2 # HA event
Become HA master mode 2
Getting oci meta-token
ocid api url: https://auth.us-ashburn-1.oraclecloud.com/v1/x509
ocid collect public ip from OCI
ocid api url: https://iaas.us-ashburn-1.oraclecloud.com/20160918/publicIps?compartmentId=ocid1.tenancy.oc1..aaaaaaaambr3u
zztoyhweohbzqqdo775h7d3t54zpmz4b2cf35vs55ck3a&scope=REGION&lifetime=RESERVED&limit=1000
ocid collect vnics info for instance FGT-B
ocid api url: https://iaas.us-ashburn-1.oraclecloud.com/20160918/vnicAttachments?compartmentId=ocid1.tenancy.oc1..aaaaaaaambr3u
zztoyhweohbzqqdo775h7d3t54zpmz4b2cf35vs55ck3a&instanceId=ocid1.instance.oc1.iad.abuwcljsdd24ejpo2pvzdtoltfvuil4ss6w2md7k6gc66xzt222546ygc71a
vnic id(1/4):
ocid1.vnic.oc1.iad.abuwcljs76qzu6gmevtzpv12xpaih3cq6atcvyxbvywezp2rwhdlk6xfhvza
ocid api url: https://iaas.us-ashburn-1.oraclecloud.com/20160918/privateIps?vnicId=ocid1.vnic.oc1.iad.abuwcljs76qzu6gmevtzpv12xpaih3cq6atcvyxbvywezp2rwhdlk6xfhvza
vnic id(2/4):
ocid1.vnic.oc1.iad.abuwcljsdka5z6qukwhaeemg5uxn4zqiaksp3gqyezdisxcvveczcy2di5a
ocid api url: https://iaas.us-ashburn-1.oraclecloud.com/20160918/privateIps?vnicId=ocid1.vnic.oc1.iad.abuwcljsdka5z6qukwhaeemg5uxn4zqiaksp3gqyezdisxcvveczcy2di5a
vnic id(3/4):
ocid1.vnic.oc1.iad.abuwcljsoict6e4i3rr4vzl25ogims22b26khe2kroywwdre5ybuvmxqjswq
ocid api url: https://iaas.us-ashburn-1.oraclecloud.com/20160918/privateIps?vnicId=ocid1.vnic.oc1.iad.abuwcljsoict6e4i3rr4vzl25ogims22b26khe2kroywwdre5ybuvmxqjswq
vnic id(4/4):
ocid1.vnic.oc1.iad.abuwcljs72l3az24q4ellxxde7533bcvz6tebfdzzmi2henh4acwrpl5kjbq
ocid api url: https://iaas.us-ashburn-1.oraclecloud.com/20160918/privateIps?vnicId=ocid1.vnic.oc1.iad.abuwcljs72l3az24q4ellxxde7533bcvz6tebfdzzmi2henh4acwrpl5kjbq
instance: FGT-B
    vnic: 10.0.24.22 (129.213.188.144)
    vnic: 10.0.21.22
    vnic: 10.0.22.22
    vnic: 10.0.23.22
ocid api url: https://iaas.us-ashburn-1.oraclecloud.com/20160918/subnets/ocid1.subnet.oc1.iad.aaaaaaaaz5htioi34gbwpm4ib6t54lhdsmlp6gpygo4joy2zqhtc4jzswq
ocid api url: https://iaas.us-ashburn-
```

```

1.oraclecloud.com/20160918/subnets?compartmentId=ocidl.tenancy.oc1..aaaaaaaambr3uzz
toyhweohbzqqdo775h7d3t54zpmz4b2cf35vs55ck3a&vcnId=ocidl.vcn.oc1.iad.aaaaaaa5dfd4
ud7pceb5uykemraiddojlgk3qsibvm2sectfvmpeuta73ha
ocid api url: https://iaas.us-ashburn-
1.oraclecloud.com/20160918/privateIps?ipAddress=10.0.13.21&subnetId=ocidl.subnet.oc
1.iad.aaaaaaaajjdbd62mq2kqfy7ncjada5i4pvnfyuwrwqri763illanlyh3y3a
ocid api url: https://iaas.us-ashburn-
1.oraclecloud.com/20160918/privateIps?ipAddress=10.0.13.21&subnetId=ocidl.subnet.oc
1.iad.aaaaaaaaz5htioi34gbwpm4ib6t54lhdsmwlp6gppygo4joy2zqhtc4jzswq
ocid api url: https://iaas.us-ashburn-
1.oraclecloud.com/20160918/privateIps?ipAddress=10.0.13.21&subnetId=ocidl.subnet.oc
1.iad.aaaaaaaagypiubrrowu4cy3khyo23uxqcnrftdizqzmbdwp2qoxediub2q
ocid api url: https://iaas.us-ashburn-
1.oraclecloud.com/20160918/privateIps?ipAddress=10.0.13.21&subnetId=ocidl.subnet.oc
1.iad.aaaaaaaalk3n5o74urfjbg5q77owicsahhc34fjdsmlyq5r7auuzpbhknj7a
ocid api url: https://iaas.us-ashburn-
1.oraclecloud.com/20160918/privateIps?ipAddress=10.0.13.21&subnetId=ocidl.subnet.oc
1.iad.aaaaaaaep4y5zoaotwpjlyrxtvucrkhappytdw2ktw5kwplykg2h57ya
ocid api url: https://iaas.us-ashburn-
1.oraclecloud.com/20160918/privateIps?ipAddress=10.0.13.21&subnetId=ocidl.subnet.oc
1.iad.aaaaaaaafn3wl6kuh5fbaqsggfezgxkhqagduo2lxw6my5wb4hrywd7s73fq
ocid found peer heart beat ip 10.0.13.21 in subnet net13-heartbeat
ocid api url: https://iaas.us-ashburn-
1.oraclecloud.com/20160918/vnicAttachments?compartmentId=ocidl.tenancy.oc1..aaaaaaa
ambr3uzztoyhweohbzqqdo775h7d3t54zpmz4b2cf35vs55ck3a&vnicId=ocidl.vnic.oc1.iad.abu
wcljqtujnevzbifkcvv6c4itt3xmrn6gr57qps2v2w7ccwfrijrdmkhq
ocid collect vnics info for peer instance
ocid api url: https://iaas.us-ashburn-
1.oraclecloud.com/20160918/vnicAttachments?compartmentId=ocidl.tenancy.oc1..aaaaaaa
ambr3uzztoyhweohbzqqdo775h7d3t54zpmz4b2cf35vs55ck3a&instanceId=ocidl.instance.oc1
.iad.abuwcljt5zkznwtdirurbeghpheuh5ktcizg2srdn6segjebphejscoj2y6la
vnic id(1/4):
ocidl.vnic.oc1.iad.abuwcljqtujnevzbifkcvv6c4itt3xmrn6gr57qps2v2w7ccwfrijrdmkhq
ocid api url: https://iaas.us-ashburn-
1.oraclecloud.com/20160918/privateIps?vnicId=ocidl.vnic.oc1.iad.abuwcljqtujnevzbif
kcvv6c4itt3xmrn6gr57qps2v2w7ccwfrijrdmkhq
vnic id(2/4):
ocidl.vnic.oc1.iad.abuwcljt5aj42rcy6yrpmfmhem7wiboiargdlvdfnsg5jkkqc426gukhavdq
ocid api url: https://iaas.us-ashburn-
1.oraclecloud.com/20160918/privateIps?vnicId=ocidl.vnic.oc1.iad.abuwcljt5aj42rcy6yr
pmfmhem7wiboiargdlvdfnsg5jkkqc426gukhavdq
vnic id(3/4):
ocidl.vnic.oc1.iad.abuwcljtzdqf5rhpvcbhzm7gxgvmzu5xm34eo6kiaxtea5l5f4qwhskw6nbq
ocid api url: https://iaas.us-ashburn-
1.oraclecloud.com/20160918/privateIps?vnicId=ocidl.vnic.oc1.iad.abuwcljtzdqf5rhpvcb
hzm7gxgvmzu5xm34eo6kiaxtea5l5f4qwhskw6nbq
vnic id(4/4):
ocidl.vnic.oc1.iad.abuwcljtpw6tkr3jevqd52b3sg4f5rkzqoyd4zegimdqkqa4ualwe5cnat4q

```

```

ocid api url: https://iaas.us-ashburn-
1.oraclecloud.com/20160918/privateIps?vnicId=ocid1.vnic.oc1.iad.abuwcljtpw6tkr3jevq
d52b3sg4f5rkzqoyd4zegimdqkqa4ualwe5cnat4q
instance:
  vnic: 10.0.14.21(129.213.181.141)
  vnic: 10.0.11.21(129.213.191.163)
  vnic: 10.0.12.21
  vnic: 10.0.13.21
checking ip: 10.0.21.22 in port2
ocid failover public ip 129.213.191.163 from 10.0.11.21 to 10.0.21.22
ocid updating public ip 129.213.191.163 with data: {"privateIpId":
"ocid1.privateip.oc1.iad.abuwcljsgvcf5narv2qgmbc5djv43qci6heja3lxxamtch24qhp5vzizwbs
na"}
ocid api url: https://iaas.us-ashburn-
1.oraclecloud.com/20160918/publicIps/ocid1.publicip.oc1.iad.aaaaaaaucxuvfvi2tyl222
ib4mcluori5fofovq2lqkows7eikwhaaijdnq
ocid assigned public ip 129.213.191.163 to private ip 10.0.21.22 successfully
checking ip: 10.0.22.22 in port3
ocid collect route table info from vcn
ocid1.vcn.oc1.iad.aaaaaaa5dfd4ud7pceb5uykemraiddojlgk3qsibvm2sectfvmpeuta73ha
ocid api url: https://iaas.us-ashburn-
1.oraclecloud.com/20160918/routeTables?compartmentId=ocid1.tenancy.oc1..aaaaaaaambr
3uzztoyhweohbzqqdo775h7d3t54zpmz4b2cf35vs55ck3a&vcnId=ocid1.vcn.oc1.iad.aaaaaaa5
dfd4ud7pceb5uykemraiddojlgk3qsibvm2sectfvmpeuta73ha
route table: rtb-internal
  rule: 0.0.0.0/0, next hop: 10.0.12.21
ocid update next hop from 10.0.12.21 to 10.0.22.22 in route table rtb-internal
ocid updating route table rtb-internal with data: {"routeRules": [{"destination":
"0.0.0.0/0", "destinationType": "CIDR_BLOCK", "networkEntityId":
"ocid1.privateip.oc1.iad.abuwcljstkyb7gvv5lyrf3ugb4mqbmmugijl6zpcbtr2cht4tsggqlq6e4
fq"}]}}
ocid api url: https://iaas.us-ashburn-
1.oraclecloud.com/20160918/routeTables/ocid1.routetable.oc1.iad.aaaaaaaapxqqkjznvkv
qvhcbghotxzfy7umjgg4jtg7z6o2s5dcmjsmmmta
ocid update route table rtb-internal successfully
HA event

```

6. Log into both PCs created in step 2. Verify that each PC can access the Internet via FGT-B-AD2, the new primary node.

Deploying FortiGate-VM HA on OCI between multiple ADs using a regional VCN

This deployment process consists of the following steps:

Checking the prerequisites

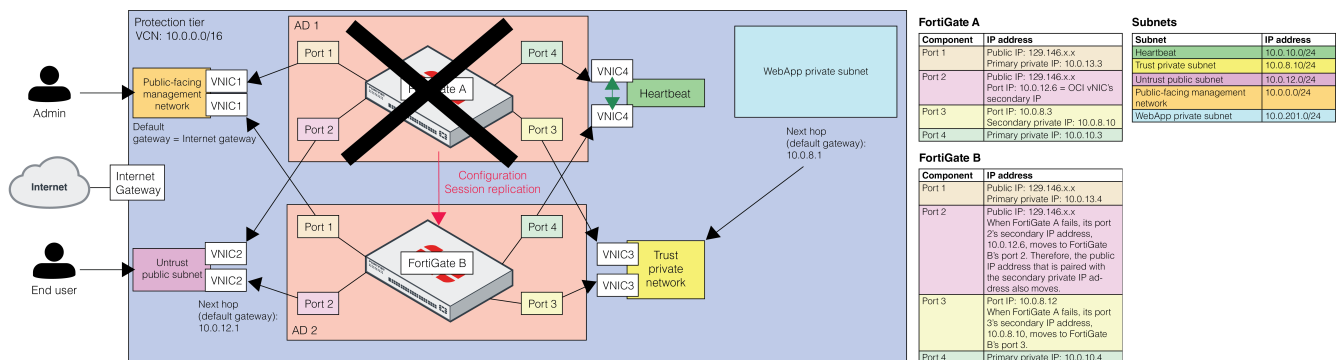
To deploy and configure the FortiGate-VM as an A-P HA solution, you need the following items:

- OCI account to operate in OCI compute portal
- Availability to accommodate required OCI resources
 - See [Service Limits](#).
 - VCN with five subnets
 - Three public IP addresses
 - One for traffic to/through the active (primary) FortiGate-VM
 - Two for management access to each FortiGate-VM
 - All IP addresses must be static, not DHCP.
 - Two FortiGate-VM instances
 - You must deploy the two nodes in different ADs and under the same VCN.
 - Each FortiGate-VM must have at least four network interfaces. See [Compute Shapes](#).
- Two valid FortiGate-VM BYOL licenses. See [Licensing on page 8](#).
- The following summarizes minimum sufficient IAM roles for this deployment:
 - Allow dynamic-group <group_name> to read compartments in tenancy
 - Allow dynamic-group <group_name> to read instances in tenancy
 - Allow dynamic-group <group_name> to read vnic-attachments in tenancy
 - Allow dynamic-group <group_name> to read subnets in tenancy
 - Allow dynamic-group <group_name> to manage private-ips in tenancy
 - Allow dynamic-group <group_name> to manage public-ips in tenancy
 - Allow dynamic-group <group_name> to manage route-tables in tenancy
 - To define simpler roles, use the following:
 - Allow dynamic-group <group_name> to read compartments in tenancy
 - Allow dynamic-group <group_name> to read instances in tenancy
 - Allow dynamic-group <group_name> to manage virtual-network-family in tenancy



Actual role configurations may differ depending on your environments. Check with your company's public cloud administrators for more details.

Reviewing the network topology



A recommended installation requires four network interfaces per FortiGate-VM node. In addition to inbound and outbound data interfaces, two interfaces are used for internal operations: management and heartbeat. Ensure you choose OCI VM instance sizes that can equip four network interfaces.

The table describes the usage of each port. Port1 and 2 are on public (or untrusted) subnets, and public IP addresses are allocated to them.

Port	Description
Port 1	Dedicated management interface. In case of heartbeat failure, the passive firewall needs a dedicated port through which to communicate with OCI to issue failover-related commands. This port is always available, regardless of node status (active/passive), except when a node is down.
Port 2	External data interface on the public network-facing side. A public IP address for the protected server is associated with the active node's private IP address. FortiGate performs NAT for inbound traffic and outbound traffic.
Port 3	Internal data traffic interface on the protected/trusted network-facing side.
Port 4	Heartbeat between two FortiGate nodes. This is unicast communication. This heartbeat interface has its dedicated "hbdev" VDOM and cannot be used for any other purpose.

You must configure port 1 as the management interface. The other ports are interchangeable. The best practice is to locate each port in a different subnet.



You must configure primary private IP addresses, even where not mentioned in the diagram. Although not required for HA purposes, you must do this to comply with general networking requirements.

Creating a VCN for multiple-AD HA topology

To create a VCN and public-facing subnets:

1. In OCI, go to *Networking > Virtual Cloud Networks*, and click *Create Virtual Cloud Network*.
2. In the *NAME* field, enter the VCN name. Then, select *CREATE VIRTUAL CLOUD NETWORK PLUS RELATED RESOURCES*. This allows you to create the Internet gateway, routing table, and subnet all together using Oracle default settings. If you intend to create each resource separately by specifying your own inputs, click *CREATE VIRTUAL CLOUD NETWORK ONLY*. This example uses the first choice.

Create Virtual Cloud Network [help](#) [cancel](#)

NAME
fgtvm

CREATE IN COMPARTMENT
DevelopmentEngineering
fortinetoracled1 (root)/DevelopmentEngineering

☐ CREATE VIRTUAL CLOUD NETWORK ONLY
Creates a Virtual Cloud Network only. You'll still need to set up at least one Subnet, Gateway, and Route Rule to have a working Virtual Cloud Network.

☒ CREATE VIRTUAL CLOUD NETWORK PLUS RELATED RESOURCES
Automatically sets up a Virtual Cloud Network with access to the internet. You can set up firewall rules and Security Lists to control ingress and egress traffic to your Instances. All related resources will be created in the same Compartment as the VCN.

Create Virtual Cloud Network

DNS RESOLUTION
☒ USE DNS HOSTNAMES IN THIS VCN
Required for instance hostname assignment if you plan to use VCN DNS or a third-party DNS. This choice cannot be changed after the VCN is created. [Learn more](#)

Name: fgtvm
CIDR: 10.0.0.0/16
DNS Label: fgtvm
DNS Domain Name: fgtvm.oraclevcn.com

Create Internet Gateway

Name: Internet Gateway

Update Default Route Table

Add Route Rule: 0.0.0.0/0 - Internet Gateway

Create Subnet

Name: Public Subnet www/CA-TORONTO-1-AD-1
Security List: Default Security List
DHCP Options: Default DHCP Options
CIDR: 10.0.0.0/24; 10.0.0.0 - 10.0.0.255 (256 IP Addresses)
Route Table: Default Route Table
DNS Label: Auto-generated

3. Click *Create Virtual Cloud Network* at the bottom of the screen, then click *Close*. This configures the related resources.
4. Create the other subnets:
 - a. Go to *Networking > Virtual Cloud Networks*. Click the name of the previously created VCN, then click *Create Subnet*.
 - b. For *Subnet Type*, select *Regional*.
 - c. For *Subnet Access*, select *Private* or *Public Subnet* as desired. The screenshot shows the configuration for the public subnet.

Create Subnet
[help](#)
[cancel](#)

If the Route Table, DHCP Options, or Security Lists are in a different Compartment than the Subnet, enable Compartment selection for those resources: [Click here](#)

NAME

SUBNET TYPE

☒ REGIONAL (RECOMMENDED)
Instances in the subnet can be created in any availability domain in the region. Useful for high availability.

☐ AVAILABILITY DOMAIN-SPECIFIC
Instances in the subnet can only be created in one availability domain in the region.

CIDR BLOCK

Specified IP addresses: 10.0.12.0-10.0.12.255 (256 IP addresses)

ROUTE TABLE

SUBNET ACCESS

☐ PRIVATE SUBNET
Prohibit public IP addresses for Instances in this Subnet

☒ PUBLIC SUBNET
Allow public IP addresses for Instances in this Subnet

DNS RESOLUTION

☒ USE DNS HOSTNAMES IN THIS SUBNET ⓘ
Allows assignment of DNS hostname when launching an Instance

DNS LABEL

Only letters and numbers, starting with a letter. 15 characters max.

DNS DOMAIN NAME READ-ONLY

DHCP OPTIONS

Security Lists

SECURITY LIST

+ Additional Security List

TAGS

Tagging is a metadata system that allows you to organize and track resources within your tenancy. Tags are composed of keys and values that can be attached to resources.

[Learn more about tagging](#)

TAG NAMESPACE	TAG KEY	VALUE
None (add a free-form tag)		
+ Additional Tag		

Create Subnet
Cancel

- d. Repeat to create a minimum of four subnets for HA setup. The following shows an example of the minimum requirement:

Subnets in DevelopmentEngineering Compartment


Create Subnet				
Name	State	CIDR Block	Subnet Access	Created
heartbeat	Available	10.0.10.0/24	Private (Regional)	Mon, Sep 16, 2019, 5:50:53 PM UTC
trust-private	Available	10.0.8.0/24	Private (Regional)	Mon, Sep 16, 2019, 5:44:59 PM UTC
Untrust-Public	Available	10.0.12.0/24	Public (Regional)	Mon, Sep 16, 2019, 5:39:47 PM UTC
Public Subnet wwwt-CA-TORONTO-1-AD-1	Available	10.0.0.0/24	Public (wwwt-CA-TORONTO-1-AD-1)	Mon, Sep 16, 2019, 4:59:05 PM UTC

Showing 4 items < Page 1 >

Deploying the FortiGate-VM

1. Set up the OCI VCN environment. See [Creating a VCN for multiple-AD HA topology on page 62](#).
2. Deploy FortiGate-VMs in the environment for an active-passive configuration. See [Creating a FortiGate-VM instance on page 13](#). To deploy FortiGate-VM from the marketplace, see [Deploying FortiGate-VM via the marketplace on page 30](#). You must select different ADs when creating the Compute instances:

Choose an operating system or image source ⓘ



FortiGate Next-Gen Firewall (4 cores)
 Comprehensive Security in One, Simplified Solution
 Software Price \$0.49 per hour per OCPU. Your actual costs depends on various factors. ⓘ

Change Image Source

[Hide Shape](#) [Network](#) [Storage Options](#)

Availability Domain

AD 1
 wwwt-PHX-AD-1 ✓

AD 2
 wwwt-PHX-AD-2


AD 3
 wwwt-PHX-AD-3

Instance Type

Virtual Machine
 A virtual machine is an independent computing environment that runs on top of physical bare metal hardware. ✓

Bare Metal Machine
 A bare metal compute instance gives you dedicated physical server access for highest performance and strong isolation.

Choose an operating system or image source ⓘ



FortiGate Next-Gen Firewall (4 cores)
 Comprehensive Security in One, Simplified Solution
 Software Price \$0.49 per hour per OCPU. Your actual costs depends on various factors. ⓘ

Change Image Source



[Hide Shape](#) [Network](#) [Storage Options](#)

Availability Domain

AD 1
 wwwt-PHX-AD-1

AD 2
 wwwt-PHX-AD-2 ✓

AD 3
 wwwt-PHX-AD-3

 RUNNING	fgt-b OCID: ...6aguya Show Copy	Shape: VM.Standard2.4	Region: phx Availability Domain: wwwt-PHX-AD-2 Fault Domain: FAULT-DOMAIN-3
 RUNNING	fgt-a OCID: ...kkgnja Show Copy	Shape: VM.Standard2.4	Region: phx Availability Domain: wwwt-PHX-AD-1 Fault Domain: FAULT-DOMAIN-2

3. Configure extra VNICs for the FortiGate-VM. You must ensure there are at least four network interfaces configured for each instance. See [Checking the prerequisites on page 35](#). To create an extra VNIC, see [Creating the second VNIC on page 24](#). To configure the extra VNIC, see [Configuring the second VNIC on the FortiGate-VM on page 26](#).

4. Update route rules to point to the internal/trust private IP address on the active FortiGate. It is recommended to create a separate route table for the internal/trust subnet:
 - a. Go to *Networking > Virtual Cloud Networks > <VCN used> > Route Tables*, then click *Create Route Table*.
 - b. Specify the route table to point to the internal/trust private IP address on the active FortiGate:

Create Route Table [help](#) [cancel](#)

NAME
internal-route

CREATE IN COMPARTMENT
DevelopmentEngineering
fortinetoracled1 (root)/DevelopmentEngineering

Route Rules

Important: For a route rule that targets a Private IP, you must first enable "Skip Source/Destination Check" on the VNIC that the Private IP is assigned to.

TARGET TYPE
Private IP

DESTINATION
CIDR Block

DESTINATION CIDR BLOCK
0.0.0.0/0
Specified IP addresses: 0.0.0.0-255.255.255.255 (4,294,967,296 IP addresses)

COMPARTMENT
DevelopmentEngineering
fortinetoracled1 (root)/DevelopmentEngineering

TARGET SELECTION
10.0.8.10
OCID: ...6oph7a

+ Additional Route Rule

- c. Go to *Networking > Virtual Cloud Networks > <VCN used>*. Edit the desired subnet.
- d. Under *Route Table*, update the configuration to the newly created route table.

Configuring the OCI HA interfaces

OCI recommends leaving VM NIC interfaces set to DHCP. This is to avoid potential misaligned configurations. However, when configuring an NVA, you may need to ignore this recommendation. When doing so, ensure that the IP addresses correspond with those intended, so that to the extent required, the configurations match.

In the case of HA, it is necessary that the FortiGate-VMs have the correct IP information statically configured in order to provide proper failover between the two devices.



OCI API calls enable the failover mentioned above through the OCI Fabric connector, but only for IP addresses configured as secondary in the OCI VNIC configuration.

Also, OCI API calls, if initiated from within a VCN, must be made by a primary interface with a public address. Thus, the network configuration for OCI HA will be unique and very specific.



You may lose connection to the instance during interface IP address and route configuration. It is therefore recommended to perform this configuration via the console.

Primary FortiGate

port1

The primary VNIC associated with the FortiGate NVA must have a primary IP address with a corresponding public IP address configured in a public subnet. This will be used as a management interface and also the interface from which API calls are made (this will be assigned in the HA configuration). See this interface's OCI configuration, then the corresponding FortiGate-VM configuration.



Private IP Address: 10.0.13.3 (Primary IP)
Private IP OCID: ...3egzva [Show](#) [Copy](#)
Private IP Assigned: Fri, 11 Oct 2019 20:37:11 UTC

Fully Qualified Domain Name: fgt-a... [Show](#) [Copy](#)
Public IP Address: 129.146.66.249 (Ephemeral)
Public IP OCID: ...nyvnha [Show](#) [Copy](#)

```
config system interface
  edit "port1"
    set vdom "root"
    set ip 10.0.13.3 255.255.255.0
    set allowaccess ping https ssh http fgfm
    set description "management"
    set mtu-override enable
    set mtu 9000
  next
end
```

port2

In this example, port2 is assumed to be a public/WAN-facing interface. The following FortiGate configuration does not use the primary IP address for its interface IP address. Instead, it uses the non-primary private IP address, as shown. This is because the primary IP address is not relocatable to the secondary FortiGate in the event of HA failover. In this example, the FortiGate uses only a single secondary IP address with an associated public IP address. In the case of a failover, the secondary IP address and associated public IP address are migrated from the active to the passive FortiGate. Therefore, if any extra non-primary private IP addresses are used in the setup, these IP addresses must be referenced explicitly in the interface configuration by enabling secondary IP addresses.

Assign Private IP Address



Private IP Address: 10.0.12.3 (Primary IP)
Private IP OCID: ...wkbkeq [Show](#) [Copy](#)
Private IP Assigned: Fri, 11 Oct 2019 20:40:14 UTC

Fully Qualified Domain Name: Unavailable
Public IP Address: (Not Assigned)



Private IP Address: 10.0.12.5
Private IP OCID: ...hyzpq [Show](#) [Copy](#)
Private IP Assigned: Fri, 11 Oct 2019 21:35:12 UTC

Fully Qualified Domain Name: Unavailable
Public IP Address: 129.146.156.171 (Reserved)
Public IP OCID: ...aqo3a [Show](#) [Copy](#)



Private IP Address: 10.0.12.6
Private IP OCID: ...2jughq [Show](#) [Copy](#)
Private IP Assigned: Fri, 11 Oct 2019 21:35:55 UTC

Fully Qualified Domain Name: Unavailable
Public IP Address: 129.146.89.204 (Reserved)
Public IP OCID: ...bxoipq [Show](#) [Copy](#)

```
config system interface
  edit "port2"
    set vdom "root"
    set ip 10.0.12.5 255.255.255.0
    set allowaccess ping https ssh fgfm
    set description "untrust"
    set secondary-IP enable
    set mtu-override enable
    set mtu 9000
```

```

config secondaryip
  edit 1
    set ip 10.0.12.6 255.255.255.0
    set allowaccess ping https ssh fgfm
  next
end
next
end

```

port3

This example configures port3 as the internal port, which is used to connect to internal resources on local subnets, peered VCNs, and so on. However, as mentioned earlier, FortiGate does not use the primary IP address.

	Private IP Address: 10.0.8.3 (<i>Primary IP</i>) Private IP OCID: ...nmaduq Show Copy Private IP Assigned: Fri, 11 Oct 2019 21:41:11 UTC	Fully Qualified Domain Name: Unavailable Public IP Address: (<i>Not Assigned</i>)
	Private IP Address: 10.0.8.10 Private IP OCID: ...h3qj2a Show Copy Private IP Assigned: Fri, 11 Oct 2019 21:44:12 UTC	Fully Qualified Domain Name: Unavailable Public IP Address: (<i>Not Assigned</i>)

```

config system interface
  edit "port3"
    set vdom "root"
    set ip 10.0.8.10 255.255.255.0
    set allowaccess ping https ssh fgfm
    set description "trusted"
    set mtu-override enable
    set mtu 9000
  next
end

```

port4

This example uses port4 as the HA interface for heartbeat and configuration synchronization. As such, it only needs a single private IP address.

	Private IP Address: 10.0.10.3 (<i>Primary IP</i>) Private IP OCID: ...shocsa Show Copy Private IP Assigned: Fri, 11 Oct 2019 20:41:39 UTC	Fully Qualified Domain Name: Unavailable Public IP Address: (<i>Not Assigned</i>)
---	--	--

```

config system interface
  edit "port4"
    set vdom "root"
    set ip 10.0.10.3 255.255.255.0
    set allowaccess ping https ssh fgfm
    set description "heartbeat"
    set mtu-override enable
    set mtu 9000
  next
end

```

Secondary FortiGate

For the secondary FortiGate, you do not need to configure port2 or port3, as these configurations should sync from the primary FortiGate.

port1

The primary VNIC associated with the FortiGate NVA must have a primary IP address with a corresponding public IP address, and so needs to be configured in a public subnet. This will be used as a management interface and also the interface from which API calls are made (this will be assigned in the HA configuration).



Private IP Address: 10.0.13.4 (Primary IP)
 Private IP OCID: ...bsa3sa [Show](#) [Copy](#)
 Private IP Assigned: Fri, 11 Oct 2019 20:43:30 UTC

Fully Qualified Domain Name: fgt-b... [Show](#) [Copy](#)
 Public IP Address: 129.146.128.51 (Ephemeral)
 Public IP OCID: ...7pptvq [Show](#) [Copy](#)

```
config system interface
  edit "port1"
    set vdom "root"
    set ip 10.0.13.4 255.255.255.0
    set allowaccess ping https ssh http fgfm
    set description "management"
    set mtu-override enable
    set mtu 9000
  next
end
```

port2

You must attach the VNIC to the instance with the primary IP address. However, the FortiGate syncs the configuration from the primary unit.



Private IP Address: 10.0.12.4 (Primary IP)
 Private IP OCID: ...u2r5aa [Show](#) [Copy](#)
 Private IP Assigned: Fri, 11 Oct 2019 20:47:17 UTC

Fully Qualified Domain Name: Unavailable
 Public IP Address: (Not Assigned)

port3

You must attach the VNIC to the instance with the primary IP address. However, the FortiGate syncs the configuration from the primary unit.



Private IP Address: 10.0.8.12 (Primary IP)
 Private IP OCID: ...x3zdqa [Show](#) [Copy](#)
 Private IP Assigned: Fri, 11 Oct 2019 20:48:16 UTC

Fully Qualified Domain Name: Unavailable
 Public IP Address: (Not Assigned)

port4

This example uses port4 as the HA interface for heartbeat and configuration synchronization. As such, it only needs a single private IP address.



Private IP Address: 10.0.10.4 (Primary IP)
 Private IP OCID: ...vrmgpq [Show](#) [Copy](#)
 Private IP Assigned: Fri, 11 Oct 2019 20:48:52 UTC

Fully Qualified Domain Name: Unavailable
 Public IP Address: (Not Assigned)

```
config system interface
```

```

edit "port4"
    set vdom "root"
    set ip 10.0.10.4 255.255.255.0
    set allowaccess ping https ssh fgfm
    set description "heartbeat"
next
end

```

Initial Fabric connector configuration

First, you must configure a Fabric connector in FortiOS. Calling APIs to OCI during HA failover requires this step.

Follow the steps in [Configuring an OCI SDN connector using IAM roles on page 78](#). Ensure you can successfully call APIs to OCI by referring to [Troubleshooting OCI SDN connector on page 77](#).

You must ensure that HA status is enabled for the Fabric connector:

```

config system sdn-connector
    edit "oci"
        set type oci
        set ha-status enable
    next
end

```

You must then configure A-P HA settings by using CLI commands on the GUI or via SSH.

Configuring active-passive HA

This step shows you how to configure A-P HA settings by using CLI commands on the GUI or via SSH. Note the following:

In the commands, note the following:

- Port4 is the hbdev port used for heartbeat connection.
- For the management interface, you must use port 1, as OCI allows only port 1 for metadata access.
- When setting priority on FortiGate B, set the priority to 100 (lower than FortiGate A's priority level). The node with the lower priority level is determined as the secondary node.
- When setting the unicast heartbeat peer IP address (the last command), this is the IP address on the peer, which in the example is FortiGate B, which has port4 IP address 10.0.10.4 in the example. When setting FortiGate B's configuration, specify FortiGate A's port4 IP address, which is 10.0.10.3.

The following is the primary FortiGate configuration:

```

config system ha
    set group-id 30
    set group-name "ha-cluster"
    set mode a-p
    set hbdev "port4" 50
    set session-pickup enable
    set session-pickup-connectionless enable
    set ha-mgmt-status enable
    config ha-mgmt-interfaces
        edit 1
            set interface "port1"
            set gateway 10.0.13.1
        next
    end
end

```

```
end
set override disable
set priority 200
set unicast-hb enable
set unicast-hb-peerip 10.0.10.4
end
```

Once configuration is complete, exit the CLI or SSH session.

The following is the secondary FortiGate configuration:

```
config system ha
  set group-id 30
  set group-name "ha-cluster"
  set mode a-p
  set hbdev "port4" 50
  set session-pickup enable
  set session-pickup-connectionless enable
  set ha-mgmt-status enable
  config ha-mgmt-interfaces
    edit 1
      set interface "port1"
      set gateway 10.0.13.1
    next
  end
  set override disable
  set priority 100
  set unicast-hb enable
  set unicast-hb-peerip 10.0.10.3
end
```

Troubleshooting

See [Troubleshooting on page 49](#).

Deploying FortiGate-VM using Terraform in the CLI

Using Terraform to deploy a single FortiGate-VM

You can deploy FortiGate-VM using Terraform. In this example, OCI is a Terraform provider, and FortiGate is a Terraform consumer. For details about Terraform, see [Introduction to Terraform](#).

Before using Terraform to deploy a FortiGate-VM, ensure the following prerequisites are met:

1. See [Getting Started with the Terraform Provider](#).
2. Prepare a PEM key file for the user to authenticate themselves with the OCI platform.
3. Upload the FortiGate-VM image to OCI where you plan to deploy the FortiGate-VM. See [To obtain the deployment image file and place it in your bucket: on page 14](#).

The following lists the steps for deploying a FortiGate-VM using Terraform:

1. Prepare Terraform deployment files. There is a sample set of Terraform files available on [GitHub](#). Clone or download the files in the [Single-VM-BareMinimum-BYOL directory](#). This creates a new VCN.
2. Select your OS with the Terraform applications. See [Terraform Downloads](#).
3. Edit the Terraform variables and config files to suit your environment:
 - a. Change the OCI variables in the terraform.tfvars file. You must know the OCIDs of your tenant, compartment, user, and AD. If using Windows, you do not need to specify the C: drive in paths.
 - b. Change the resource names in the block.tf, compute.tf, network.tf, and variables.tf files. You can modify resources including the following:
 - i. FortiGate-VM hostname
 - ii. VCN name
 - iii. Network interface, subnet, volume names
 - iv. Security list settings. Ensure you open port 443 to allow access to the FortiGate-VM.
 - v. Disk size for the second drive. By default, this is 50 GB.
 - vi. Network CIDRs
4. Run Terraform:
 - a. Run `terraform.exe init` to initialize the Terraform environment.

```
PS C:\Users\jkato\tmp4> .\terraform.exe init
Initializing provider plugins...
- Checking for available provider plugins on https://releases.hashicorp.com...
- Downloading plugin for provider "template" (1.0.0)...
- Downloading plugin for provider "oci" (3.11.0)...

The following providers do not have any version constraints in configuration,
so the latest version was installed.

To prevent automatic upgrades to new major versions that may contain breaking
changes, it is recommended to add version = "..." constraints to the
corresponding provider blocks in configuration, with the constraint strings
suggested below.

* provider.template: version = "~> 1.0"

Terraform has been successfully initialized!

You may now begin working with Terraform. Try running "terraform plan" to see
any changes that are required for your infrastructure. All Terraform commands
should now work.

If you ever set or change modules or backend configuration for Terraform,
rerun this command to reinitialize your working directory. If you forget, other
commands will detect it and remind you to do so if necessary.
```


b. Run `terraform.exe plan`.

```
PS C:\Users\jkato\tmp4> .\terraform.exe plan
Refreshing Terraform state in-memory prior to plan...
The refreshed state will be used to calculate this plan, but will not be
persisted to local or remote state storage.

data.template_file.userdata_lic: Refreshing state...
data.oci_identity_availability_domains.ads: Refreshing state...

-----

An execution plan has been generated and is shown below.
Resource actions are indicated with the following symbols:
  + create
  <= read (data resources)

Terraform will perform the following actions:

<= data.oci_core_boot_volume_attachments.block_attach
   id:
   availability_domain:                               <computed>
                                                    "www1:US-ASHBURN-AD-1"
```

Check the output for newly creating resources. You can add "-out" and an output file to check the output in the file.

c. Run `terraform.exe apply`.

```
PS C:\Users\jkato\tmp4> .\terraform.exe apply
data.template_file.userdata_lic: Refreshing state...
data.oci_identity_availability_domains.ads: Refreshing state...

An execution plan has been generated and is shown below.
Resource actions are indicated with the following symbols:
  + create
  <= read (data resources)

Terraform will perform the following actions:

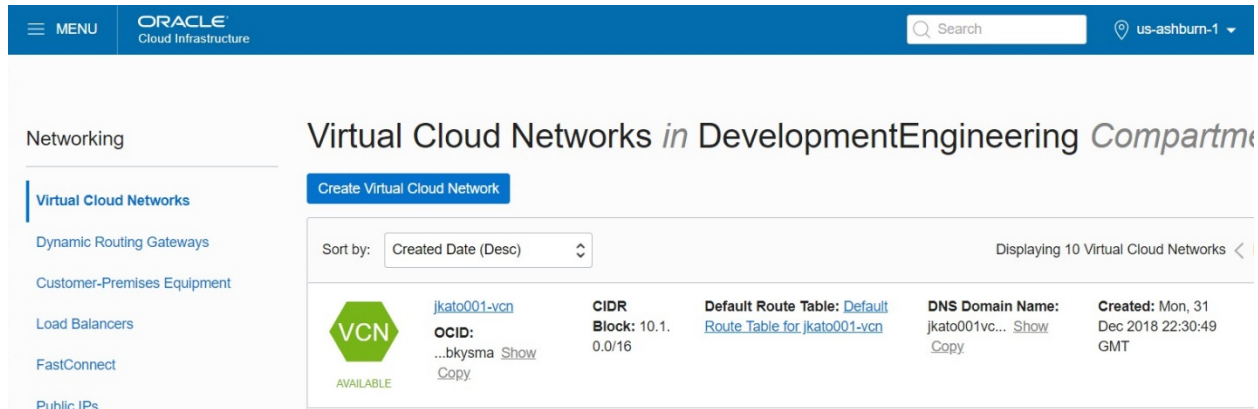
<= data.oci_core_boot_volume_attachments.block_attach
   id:
   availability_domain:                               <computed>
                                                    "www1:US-ASHBURN-AD-1"
```

At the Enter a value prompt, enter `yes` to continue. Wait about ten minutes for the command to end.

```
scope:      "" => <computed>
state:      "" => <computed>
time_created: "" => <computed>
oci_core_public_ip.untrust_public_ip: Creation complete after 1s (ID: ocid1.publicip.oc1.iad.abuwc1...jtl...
5661: 2a2730b9a122rwm7p2uim4q)
oci_core_volume_attachment.vm_volume_attach: Creation complete after 24s (ID: ocid1.volumeattachment.oc1.iad.abuwc1...
cguamocaf4abtpu9d39v3v76776u1g8c4gzq)
Apply complete! Resources: 19 added, 0 changed, 0 destroyed.
```

5. In the OCI console, go to the newly created resources. The FortiGate-VM instances and VCN have been created.

The screenshot shows the Oracle Cloud Infrastructure (OCI) console interface. The top navigation bar includes the Oracle logo, 'Cloud Infrastructure', a search bar, and a location dropdown set to 'us-ashburn-1'. The main content area is titled 'Instances in Development' and shows a list of instances. A sidebar on the left contains navigation links for 'Compute', 'Instances', 'Instance Configurations', 'Instance Pools', 'Custom Images', 'Boot Volumes', and 'Boot Volume Backups'. The 'Instances' link is selected. The instance list table has columns for Name, OCID, Shape, Region, Availability Domain, Fault Domain, and Created. The instance 'jkato003-vm' is listed with OCID '...x5emq', Shape 'VM.Stan dard1.4', Region 'iad', Availability Domain 'www1:US-ASHBURN-AD-1', Fault Domain 'FAULT-DOMAIN-1', and Created 'Mon, 31 Dec 2018 22:30:53 GMT'. The instance status is 'RUNNING'. A 'Create Instance' button is visible above the table. The table also shows 'Displaying 22 Instances'.



6. Connect to the FortiGate-VMs. See [Accessing the FortiGate-VM on page 22](#).

Bootstrapping the FortiGate-VM at initial bootup

This section explains how to add bootstrapping of FortiGate CLI commands and a BYOL license at the time of initial bootup as part of a Terraform deployment.

To bootstrap the FortiGate-VM at initial bootup:

1. Create a text file that contains FortiGate CLI commands. This example saves the file as config.txt. This example uses the following CLI commands:

```
config system global
  set timezone 03
end
```

The config text file is in MIME format and looks like the following:

```
Content-Type: multipart/mixed; boundary=="==OCI=="
MIME-Version: 1.0
--==OCI==
Content-Type: text/x-shellscript; charset="us-ascii"
MIME-Version: 1.0
config system global
set timezone 03
end
--==OCI==
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="license"
${license_file}
--==OCI==
```

You can find the example file on [GitHub](#).

This example CLI sets the timezone as GMT-9 Alaska. You can replace these lines with your own set of CLI commands.

2. Download a FortiGate-VM license file from [Customer Service & Support](#) after registering your product code. Save the license file as a .txt file. FortiGate-VM license content resembles the following:

```

-----BEGIN FGT VM LICENSE-----
QAAAAABUjZtrwrJdUjEe/8C5dVnOmVw1w70ZWPPTG7vm2KKwVvL4++qL0gED6/q
SQSPkwpTFIXjAwRGtGyX1VvaTpXgGQAA1pwrFdJnS6TWJ6dVT7KiD8ncufaa3bCw
s8XpmlLvzjE4//+C9nqh4FN/KyDweMEIptDMaNsOCmBBBrU8HQIDkX+rgeCs3QZ5
ELStRrX11/oXqT8/gorG67ZdybXvzPwVwVJYDS5AsI+QK8BHJ+XgHLjHkzBZ4ezU
Hd01HCsm7MXEYV5KauU43s29XESTxqPEInah3yXgYtd24pnV683G4EHCAdgyHTP
QqDqBMKcT5aei0ooGVAX8D62C5Zjh+1+tkdpR5YHoVY2HU95hBCNj8roJbMnk7
NogYuaDQeh28MDtpvzXnb24m1f0QMTJysQcTvwJzmn8nySBo7xNg/iT52QnFB
-----END FGT VM LICENSE-----

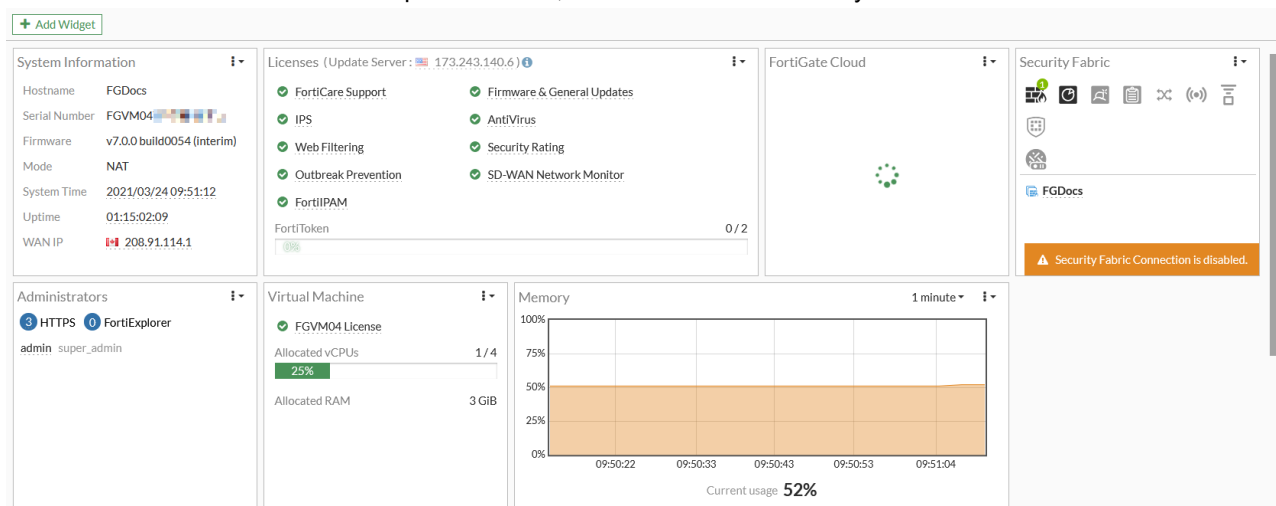
```

- Upload the config.txt and license.txt files under the directory on your local PC where you also run Terraform. Point to the correct paths in variables.tf, the Terraform variables file. On Windows, you do not need to specify the C: drive in paths.
- Uncomment the following lines in the compute.tf file:

```

32 // Required for bootstrapping / cloud-init
33 // Comment out the following if you use the feature.
34 metadata {
35   user_data = "${base64encode(data.template_file.userdata_lic.rendered)}"
36 }
and
99 // Comment out the following if you use bootstrapping / cloud-init
100 data "template_file" "userdata_lic" {
101   template = "${file(var.bootstrap)}"
102   vars {
103     license_file = "${file("${var.license}")}"
104   }
105 }

```
- Run Terraform as described in [Using Terraform to deploy a single FortiGate-VM on page 72](#).
- After deployment, log into the FortiGate by accessing https://<IP_address> in your browser. The system displays the dashboard instead of a license upload window, since the license is already activated.



To see how bootstrapping went, check if the command was successfully run. Open the CLI console and enter `diag debug cloudinit show`.

If the cloud-init was run successfully, the CLI shows `Finish running script` with no errors.

7. Check the timezone by running `config system global and get` commands.

```
security-rating-run-on-schedule: enable
send-pmtu-icmp      : enable
snat-route-change   : disable
special-file-23-support: disable
ssd-trim-freq        : weekly
--More--            : 1
ssd-trim-hour        : 1
ssd-trim-min         : Random
ssd-trim-weekday     : sunday
ssh-kex-sha1         : enable
ssl-min-proto-version: TLSv1-2
ssl-static-key-ciphers: enable
sslvpn-cipher-hardware-acceleration: enable
sslvpn-kxp-hardware-acceleration: enable
sslvpn-plugin-version-check: enable
strict-dirty-session-check: enable
strong-crypto        : enable
switch-controller    : disable
switch-controller-reserved-network: 169.254.0.0 255.255.0.0
sys-perf-log-interval: 5
tcp-halfclose-timer  : 120
tcp-halfopen-timer   : 10
tcp-option           : enable
tcp-timewait-timer   : 1
timezone             : (GMT-9:00) Alaska
traffic-priority      : tos
```

The timezone was changed to Alaska as expected, meaning that the bootstrapping CLI command was successful.

SDN connector integration with OCI

You can configure SDN connector integration with OCI in one of the following ways:

- Using certificates from the FortiGate-VM to OCI over TCP/IP. This is the more common method of configuring the integration. See [Certificate-based SDN connector user privileges on page 77](#).
- Using an IAM role provided by and configurable in the OCI environment. See [Configuring an OCI SDN connector using IAM roles on page 78](#).

Certificate-based SDN connector user privileges

See the [FortiOS Administration Guide](#).

When configuring a certificate-based OCI SDN connector in FortiOS, you must enter the OCID of an OCI user who belongs to the administrator group. The user should be added in a dedicated group. The following policy summarizes minimum sufficient privileges for this user:

- Allow dynamic-group <group_name> to read compartments in tenancy
- Allow dynamic-group <group_name> to read instances in tenancy
- Allow dynamic-group <group_name> to read vnic-attachments in tenancy
- Allow dynamic-group <group_name> to read private-ips in tenancy
- Allow dynamic-group <group_name> to read public-ips in tenancy
- Allow group <group_name> to manage private-ips in tenancy
- Allow group <group_name> to manage public-ips in tenancy
- Allow group <group_name> to manage vnics in tenancy

Troubleshooting OCI SDN connector

You can check if API calls are made successfully by running `diagnose test application ocid 1`. The following shows an example of a successful configuration:

```
FGVM2VjkatoHAFGT001 # diag test application ocid 1
[{"availabilityDomain":"www1:US-ASHBURN-AD-1","compa
api call succeeded.
```

The following shows an example of a failed configuration:

```
FGVM2VjkatoHAFGT001 # diag test application ocid 1
api call failed, rc 401
```

Check the following to see if you made other unexpected changes:

- Tenant ID
- User ID
- Compartment ID

- Does the specified OCI user belong to the Administrator group on the OCI portal?
- Does the fingerprint on the OCI portal match the one that the specified user has on the FortiGate-VM? If you change the certificate, its corresponding fingerprint must be updated or added to the OCI user on the OCI portal. In the earlier example, the fingerprint on the OCI portal and the SDN connector settings match.

API Keys

Add Public Key



Fingerprint: a7:5f:77:53:3e:01:13:03:00:03:fa:bc:a4:6a

```
FGVM2VjkatoHAFGT001 (sdn-connector) # get oci-sdn
name           : oci-sdn
status          : enable
type            : oci
tenant-id       : ocid1.tenancy.oc1..aaaaaaaah...5h7d3t
user-id         : ocid1.user.oc1..aaaaaaaah...mtdiql
compartment-id  : ocid1.compartment.oc1..aaaaaaaac...iqcgk
oci-region      : ashburn
oci-cert         : Fortinet Factory
oci-fingerprint : a7:5f:77:53:3e:01:13:03:00:03:fa:bc:a4:6a
update-interval : 60
```

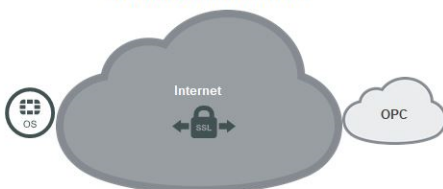
- Does the OCI security list on the Internet-facing subnet allow proper outgoing access from the FortiGate?

Configuring an OCI SDN connector using IAM roles

This guide provides a sample configuration of an OCI SDN connector using IAM roles instead of traditional authentication. Traditional authentication uses certificates from the FortiGate-VM to OCI over TCP/IP. Instead, this configuration uses the IAM role provided by and configurable in the OCI environment for authentication. The IAM role includes permissions that you can give to the instance, so that FortiOS can implicitly access metadata information and communicate to the SDN connector on its own private internal network without further authentication.

The following shows the topology when using traditional authentication versus IAM roles:

Traditional Method



Using IAM Role



The following prerequisites must be met for this configuration:

- FortiGate located on OCI
- Correct administrative permissions as an administrator on OCI over the FortiGate instance and the environment
- The following summarizes minimum sufficient IAM roles for this deployment:
 - Allow dynamic-group <group_name> to read compartments in tenancy
 - Allow dynamic-group <group_name> to read instances in tenancy
 - Allow dynamic-group <group_name> to read vnic-attachments in tenancy
 - Allow dynamic-group <group_name> to read private-ips in tenancy
 - Allow dynamic-group <group_name> to read public-ips in tenancy
 - Allow dynamic-group <group_name> to manage private-ips in tenancy
 - Allow dynamic-group <group_name> to manage public-ips in tenancy
 - Allow dynamic-group <group_name> to manage vnics in tenancy

You can use resource tags to further control the API calls, as follows:

- Allow dynamic-group <group_name> to manage private-ips in tenancy
- Allow dynamic-group <group_name> to manage public-ips in tenancy where any { target.resource.tag.<namespace>.<tag key>= 'value' }
- Allow dynamic-group <group_name> to manage vnics in tenancy where any { target.resource.tag.<namespace>.<tag key>= 'value' }



Actual role configurations may differ depending on your environments. Check with your company's public cloud administrators for more details.

To configure an OCI SDN connector using IAM roles, complete the following steps:

1. [Configure an IAM role on OCI.](#)
2. [Configure an SDN connector in .](#)
3. [Perform testing to ensure that the SDN connector is connected to .](#)

To configure an IAM role on OCI:

1. In OCI, go to *Compute > Instances*, and select the desired FortiGate-VM instance.
2. On the *Instance Details* page, note the instance's OCID. In this example, the OCID is `ocid1.instance.oc1.iad.abuwcljthhvs7djktxkljr2pzjelkcj4pgozd46bnpcpt5pxcaj56mkurhq`.
3. Open the OPC menu and go to *Identity > Dynamic Groups*. Create a dynamic group with rules that allow instances that match the FortiGate-VM's instance ID. Use the syntax "ALL {instance.id = 'instanceID'}" when creating the rule. In this example, the configured rule is "ALL {instance.id = 'ocid1.instance.oc1.iad.abuwcljthhvs7djktxkljr2pzjelkcj4pgozd46bnpcpt5pxcaj56mkurhq'}". If you have multiple instances to include in the dynamic group, create multiple rules for this dynamic group.
4. Go to *Identity > Policies*. Create a policy that allows the dynamic group to manage the environment. This allows the instance referenced in the dynamic group to query metadata and move resources around if the SDN connector is used for HA. In the *STATEMENT* field, use the syntax "Allow dynamic-group <group-name> to manage all-resources in TENANCY".

To configure an SDN connector in FortiOS:

To configure an SDN connector in the FortiOS GUI, do the following:

1. In FortiOS, go to *Security Fabric > Fabric Connectors*.
2. Click *Create New > Oracle Cloud Infrastructure (OCI)*.

3. Enable *Use metadata IAM*.
4. In the *Tenant ID* field, enter the FortiGate-VM's tenant ID.
5. In the *Compartment ID* field, enter the compartment's tenant ID. This may be the same as the tenant ID depending on your configuration.
6. Configure the other SDN connector settings as required.
7. In *Security Fabric > Fabric Connectors*, ensure that the OCI connector has been created and is enabled and connected.

To configure an SDN connector using the FortiOS CLI, run the following commands:

```
config system sdn-connector
  edit "oci-sdn-connector"
    set status enable
    set type oci
    set ha-status disable
    set tenant-id "<tenant ID>"
    set user-id ''
    set compartment-id "<compartment ID>"
    set oci-region phoenix
    set oci-cert ''
    set use-metadata-iam enable
    set update-interval 60
  next
end
```

To perform testing:

To ensure the SDN connector is connected to OCI, run the `diagnose sys sdn status` command. The output should display that the SDN connector has a connected status.

You can run the `diagnose debug application ocid -1` and `diagnose test application ocid` commands for further debugging.



If you have security concerns about the policy allowing the dynamic group access to the entire environment, follow the concept of least privileges detailed in the [OPC documentation](#). For example, if you are not using the SDN connector for failover and instead are using it for querying, you can assign the dynamic group read-only permissions.

Oracle Kubernetes (OKE) SDN connector

OCI SDN connectors support dynamic address groups based on Oracle Kubernetes (OKE) filters. See the [FortiOS Administration Guide](#).

Change log

Date	Change Description
2022-03-31	Initial release.
2022-08-04	Updated Creating a support account on page 8 .



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.