

FortiOS - VMware ESXi Administration Guide

Version 6.4

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<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>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



October 06, 2021

FortiOS 6.4 VMware ESXi Administration Guide

01-640-619610-20211006

TABLE OF CONTENTS

| | |
|---|-----------|
| About FortiGate-VM on VMware ESXi | 5 |
| FortiGate-VM models and licensing | 5 |
| FortiGate-VM evaluation license | 6 |
| FortiGate-VM virtual licenses and resources | 7 |
| Public compared to private clouds | 7 |
| Preparing for deployment | 8 |
| Virtual environment | 8 |
| Management software | 8 |
| Connectivity | 8 |
| Configuring resources | 8 |
| Registering the FortiGate-VM | 9 |
| Downloading the FortiGate-VM deployment package | 10 |
| Deployment package contents | 10 |
| Compatibility for VM hardware versions | 11 |
| Deployment | 12 |
| Deploying the FortiGate-VM | 12 |
| Initial settings | 12 |
| Configuring port 1 | 13 |
| Connecting to the FortiGate-VM GUI | 14 |
| Uploading the FortiGate-VM license | 14 |
| Validating the FortiGate-VM license with FortiManager | 15 |
| Testing connectivity | 17 |
| Configuring your FortiGate-VM | 18 |
| Transparent mode | 18 |
| High availability | 18 |
| Cloud-init using config drive | 21 |
| FortiGate-VM license file | 21 |
| FortiGate configuration script | 22 |
| Creating the config drive ISO | 22 |
| Verifying the results | 27 |
| ESXi cloud init reference | 29 |
| SDN connector integration with VMware ESXi | 31 |
| Optimizing FortiGate-VM performance | 32 |
| SR-IOV | 32 |
| Interrupt affinity | 34 |
| Packet-distribution affinity | 36 |
| TSO and LRO | 36 |
| Hyperthreading | 37 |
| Multiqueue support | 37 |

| | |
|--|-----------|
| vMotion in a VMware ESXi environment | 39 |
| Setting up FortiGate-VM HA for a VMware vMotion environment | 42 |
| Enhancing FortiGate-VM Performance with DPDK and vNP offloading | 47 |
| Enabling DPDK+vNP offloading using the FortiOS CLI | 47 |
| DPDK global settings | 48 |
| DPDK CPU settings | 50 |
| DPDK diagnostic commands | 51 |
| Change log | 56 |

About FortiGate-VM on VMware ESXi

FortiGate-VMs allow you to mitigate blind spots by implementing critical security controls within your virtual infrastructure. They also allow you to rapidly provision security infrastructure whenever and wherever it is needed. FortiGate-VMs feature all the security and networking services common to hardware-based FortiGate appliances. You can deploy a mix of FortiGate hardware and VMs, operating together and managed from a common centralized management platform.

This document describes how to deploy a FortiGate-VM in a VMware ESXi environment.

FortiGate-VM models and licensing

FortiGate-VM offers perpetual licensing (normal series and V-series) and annual subscription licensing (S-series). The differences are as follows:

| | Normal series | V-series | S-series |
|---|---|----------|---|
| Licensing term | VM base is perpetual. You must separately contract support services on an annual basis. | | Single annually contracted SKU that contains VM base and a FortiCare service bundle. |
| Support services | Each VM base type is associated with over a dozen SKUs. See the pricelist for details. | | Four support service bundle types: <ul style="list-style-type: none">• Only FortiCare• UTM• Enterprise• 360 protection |
| License level | SKUs are based on the number of virtual CPUs (vCPU) (1, 2, 4, 8, 16, 32, or unlimited). The RAM/memory restriction no longer applies for FortiOS 6.2.2 and later versions. FortiOS 6.2.1 and earlier versions have RAM/memory restrictions. | | |
| vCPU number upgrade during contracted term | Not supported. | | Supported. You can also upgrade the support service bundle. For details about upgrading, contact a Fortinet sales correspondent. |
| vCPU number downgrade during contracted term | Not supported. | | |

| | Normal series | V-series | S-series |
|--------------------------------------|---|---|----------|
| Virtual domain (VDOM) support | By default, each CPU level supports up to a certain number of VDOMs. See the FortiGate-VM datasheet for the default limits. | By default, all CPU levels do not support adding VDOMs. | |

After you submit an order for a FortiGate-VM, Fortinet sends a license registration code to the email address that you entered on the order form. Use this code to register the FortiGate-VM with Customer Service & Support, and then download the license file. After you upload the license to the FortiGate-VM and validate it, your FortiGate-VM is fully functional.

FortiGate-VM evaluation license

The FortiGate-VM includes a limited 15-day evaluation license that supports:

- 1 CPU maximum
- 2 GB memory maximum
- Low encryption only (no HTTPS administrative access)
- Security protection:
 - With the built-in signatures that the evaluation license includes, you can use the following features:
 - IPS
 - AntiVirus
 - Industrial DB
 - The following features do not have built-in signatures:
 - Security rating
 - Antispam
 - Web Filter
- Features related to FortiGuard access are not available. Go to *System > FortiGuard* in FortiOS for details.
- VDOM:
 - You can enable split-task VDOM in the CLI.
 - You cannot enable multi-VDOM.

Note the following:

- Attempting to upgrade the FortiGate firmware locks the GUI until you upload a full license.
- The evaluation license does not include technical support. The trial period begins the first time that you start the FortiGate-VM.
- After the trial license expires, functionality is disabled until you upload a full license file.
- Features available in the evaluation state may change without prior notice.

FortiGate-VM virtual licenses and resources

The primary requirement for provisioning a FortiGate-VM 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.

FortiGate-VM licensing 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 that the license indicates does not restrict the FortiGate from working, regardless of how many vCPUs the virtual instance includes. However, only the licensed number of vCPUs process traffic and management tasks. The FortiGate-VM does not use the rest of the vCPUs.

| License | 1 vCPU | 2 vCPU | 4 vCPU | 8 vCPU | 16 vCPU | 32 vCPU |
|----------|--------|--------|--------|--------|---|---|
| FGT-VM08 | OK | OK | OK | OK | The FortiGate-VM uses 8 vCPUs for traffic and management and does not use the rest. | The FortiGate-VM uses 8 vCPUs for traffic and management and 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.

Public compared to private clouds

The behavior differs between private and public clouds:

- Private clouds (ESXi/KVM/Xen/Hyper-V): Both licensed vCPUs and RAM are affected. FortiOS 6.4 does not have licensed RAM size restrictions. However, the minimum recommended RAM size is 2 GB for all versions.
- Public clouds (AWS/Azure/GCP/OCI/Aliyun): Only licensed vCPU is affected.

For example, you can activate FG-VM02 on a FGT-VM with 4vCPUs with 16 GB of RAM, running on a private VM platform. Only 2 vCPU and 4 GB of RAM, as licensed, is consumable.

Likewise, you can activate FG-VM02 on a FGT-VM c5.2xlarge EC2 instance with 8 vCPUs running on AWS. Only 2 vCPU is consumable, and there is no limit on the RAM size. You can refer to licenses for public clouds as bring your own license.

Preparing for deployment

This documentation assumes that before deploying the FortiGate-VM on the VMware ESXi virtual platform, you have addressed the following requirements:

Virtual environment

You have installed the VMware ESXi software on a physical server with sufficient resources to support the FortiGate-VM and all other VMs deployed on the platform.

If you configure the FortiGate-VM to operate in transparent mode, or include it in a FortiGate clustering protocol (FGCP) high availability (HA) cluster, configure any virtual switches to support the FortiGate-VM's operation before you create the FortiGate-VM. See [Transparent mode on page 18](#) or [High availability on page 18](#).

Management software

The VMware ESXi management software, vSphere, is installed on a computer with network access to the VMware ESXi server.

| Platform | Management software |
|---------------------------|-------------------------|
| Open VMware ESXi | Virtual Machine Manager |
| Citrix VMware ESXi Server | VMware ESXiCenter |

Connectivity

The FortiGate-VM requires an Internet connection to contact FortiGuard to validate its license. If the FortiGate-VM is in a closed environment, it must be able to connect to a FortiManager to validate the FortiGate-VM license. See [Validating the FortiGate-VM license with FortiManager on page 15](#).

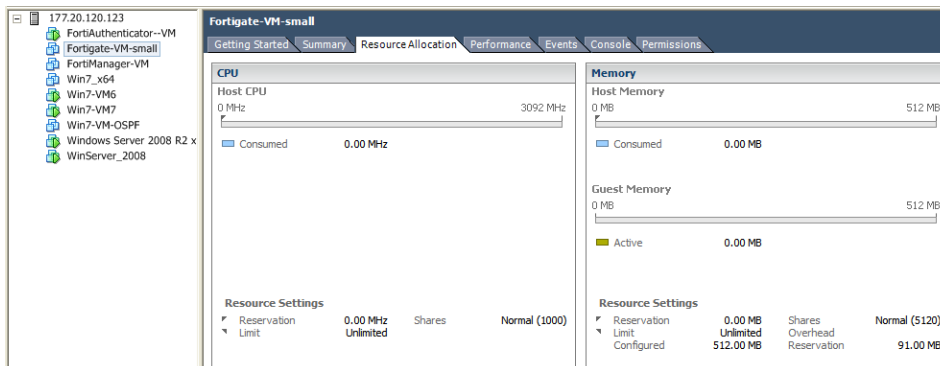
Configuring resources

Before you start the FortiGate-VM for the first time, ensure that you have configured the following resources as the FortiGate-VM license specifies:

- Disk sizes
- CPUs

- RAM
- Network settings

To configure the resources for a FortiGate-VM deployed on VMware ESXi, use the vSphere client.

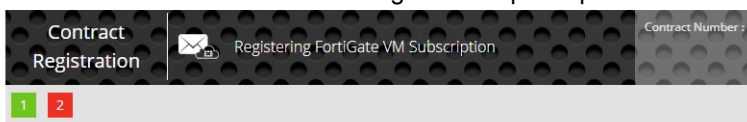


Registering the FortiGate-VM

Registering the FortiGate-VM with [Customer Service & Support](#) allows you to obtain the FortiGate-VM license file.

To register the FortiGate-VM:

1. Log in to the [Customer Service & Support site](#) using a support account, or select *Sign Up* to create an account.
2. In the main page, under *Asset*, select *Register/Activate*.
3. In the *Registration* page, enter the registration code that you received via email, and select *Register* to access the registration form.
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.



Registration Confirmation

You wish to Register or Renew Fortinet product FortiGate VM Subscription with the license number [redacted]. We find you have existing FortiGate VM Subscription license under this account, therefore you have two options to proceed: Click Register to register a new license. A new serial number will be created. Or, Click Renew if you want to apply contract to an existing product. System will extend product expiration.



5. Complete and submit the registration form.
6. In the registration acknowledgment page, click the *License File Download* link.
7. Save the license file (.lic) to your local computer. See [Uploading the FortiGate-VM license on page 14](#) or [Validating the FortiGate-VM license with FortiManager on page 15](#) for information about uploading the license file to your FortiGate-VM via the GUI.

Downloading the FortiGate-VM deployment package

FortiGate-VM deployment packages are found on the [Customer Service & Support](#) site. In the *Download* drop-down menu, select *VM Images* to access the available VM deployment packages.

1. In the *Select Product* drop-down menu, select *FortiGate*.
2. In the *Select Platform* drop-down menu, select *VMware ESXi*.
3. Select the FortiOS version you want to download.
There are two files available for download: the file required to upgrade from an earlier version and the file required for a new deployment.
4. Click the *Download* button and save the file.

For more information, see the [FortiGate datasheet](#).



You can also download the following resources for the firmware version:

- FortiOS Release Notes
- FORTINET-FORTIGATE MIB file
- FSSO images
- SSL VPN client

Deployment package contents

You must create a 32 GB log disk.

For supported VMware hardware versions, see [Compatibility for VM hardware versions on page 11](#).

The FortiGate-VM deployment package contains the following components:

| Component | Description |
|--|--|
| fortios.vmdk | FortiGate-VM system hard disk in VMDK format. |
| datadrive.vmdk | FortiGate-VM log disk in VMDK format. |
| Open Virtualization Format (OVF) template files | |
| FortiGate-VM64.ovf | OVF template based on Intel e1000 NIC driver. |
| FortiGate-VM64.hw04.ovf | OVF template file for older (v3.5) VMware ESX server. This file will be deprecated in future releases. |
| FortiGate-VMxx.hw07_vmxnet2.ovf | OVF template file for VMware vmxnet2 driver. |
| FortiGate-VMxx.hw07_vmxnet3.ovf | OVF template file for VMware vmxnet3 driver. |
| FortiGate-VM64.hw13.ovf | OVF template file for VMware ESXi 6.5 and later versions. |
| FortiGate-VM64.hw14.ovf | OVF template file for VMware ESXi 6.7 and later versions. |
| FortiGate-VM64.vapp.ovf | OVF template file for VMware vSphere, vCenter, and vCloud. |



Use the VMXNET3 interface (FortiGate-VMxx.hw07_vmxnet3.ovf template) if the FortiGate-VM will distribute workload to multiple processor cores.

Compatibility for VM hardware versions

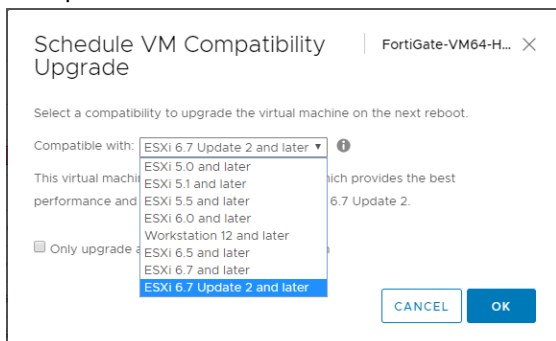
FortiGate-VM supports ESXi 5.5 and later versions. Using corresponding hardware versions 10 and later is highly recommended, as [Virtual machine hardware versions](#) mentions.

To check the FortiGate-VM ESXi compatibility, go to the [VMware Marketplace listing](#).

Upgrading hardware versions incrementally with only one delta at a time is recommended. For example, upgrading from 10 to 11, 11 to 12, 12 to 13, then 13 to 14 is recommended, although directly upgrading from 10 to 14 generally has no issues.

To upgrade hardware versions:

1. Log in to vSphere Client.
2. Right-click the FortiGate-VM in the left *Hosts and Clusters* window.
3. Go to *Compatibility > Schedule VM Compatibility Upgrade*, then click **YES**.
4. A dropdown list shows all the available VM hardware versions. Select the desired compatibility, then click **OK**.



5. Reboot the FortiGate-VM.

Deployment

Before you deploy a FortiGate-VM, ensure that you have met the requirements described in [Preparing for deployment on page 8](#) and that the correct deployment package is extracted to a folder on the local computer (see [Downloading the FortiGate-VM deployment package on page 10](#)).

After you deploy a FortiGate-VM and upload a full license to replace the default evaluation license, you can power on the FortiGate-VM and test connectivity.

Deploying the FortiGate-VM

Use the vSphere client to deploy the FortiGate OVF template and create the FortiGate-VM on the VMware ESXi server.

To create the FortiGate-VM:

1. Deploy the FortiGate OVF template as described in the [VMware documentation](#). Ensure that you select the correct vSphere version in the dropdown list on the right.
2. After deployment, configure the FortiGate-VM. See [Initial settings on page 12](#).

Disk format options

| Option | Description |
|-------------------------------------|--|
| Thick Provision Lazy Zeroed | Allocates the disk space statically (no other volumes can take the space), but does not write zeros to the blocks until the first write takes place to that block during runtime (which includes a full disk format). |
| Thick Provision Eager Zeroed | Allocates the disk space statically (no other volumes can take the space), and writes zeros to all blocks. |
| Thin Provision | Allocates the disk space only when a write occurs to a block, but the total volume size is reported by VMFS to the OS. Other volumes can take the remaining space. This allows you to float space between your servers, and expand your storage when your size monitoring indicates there is a problem. Note that once a Thin Provisioned block is allocated, it remains on the volume regardless of whether you have deleted data, etc. |

Initial settings

After you deploy a FortiGate-VM on the VMware ESXi server, perform the following tasks:

- Connect the FortiGate-VM to the network so that it can process network traffic and maintain license validity.
- Connect to FortiGate-VM GUI via a web browser for easier administration.

- Ensure that the full license file is uploaded to the FortiGate-VM.
- If you are in a closed environment, enable validation of the FortiGate-VM license against a FortiManager on your network.

Network configuration

The first time you start the FortiGate-VM, you will have access only through the console window of your VMware ESXi server environment. After you configure one FortiGate network interface with an IP address and administrative access, you can access the FortiGate-VM GUI.

Configuring port 1

VM platform or hypervisor management environments include a guest console window. On the FortiGate-VM, this provides access to the FortiGate console, equivalent to the console port on a hardware FortiGate unit. Before you can access the GUI, you must configure FortiGate-VM port1 with an IP address and administrative access.

To configure the port1 IP address:

1. In your hypervisor manager, start the FortiGate-VM and access the console window. You may need to press *Enter* to see a login prompt.
2. At the FortiGate-VM login prompt enter the username `admin`. By default there is no password. Press *Enter*.
3. Using CLI commands, configure the port1 IP address and netmask:

```
config system interface
  edit port1
    set mode static
    set ip 192.168.0.100 255.255.255.0
  next
end
```

4. To configure the default gateway, enter the following CLI commands:

```
config router static
  edit 1
    set device port1
    set gateway <class_ip>
  next
end
```



You must configure the default gateway with an IPv4 address. FortiGate-VM needs to access the Internet to contact the FortiGuard Distribution Network (FDN) to validate its license.

5. To configure your DNS servers, enter the following CLI commands:

```
config system dns
  set primary <Primary DNS server>
  set secondary <Secondary DNS server>
end
```



The default DNS servers are `208.91.112.53` and `208.91.112.52`.

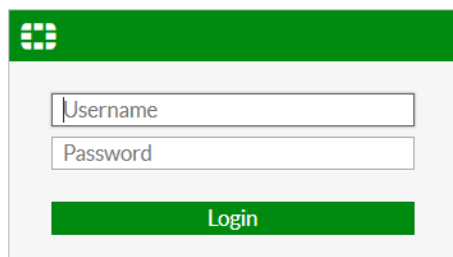
Connecting to the FortiGate-VM GUI

You connect to the FortiGate-VM GUI via a web browser by entering the IP address assigned to the port 1 interface (see [Configuring port 1 on page 13](#)) in the browser location field. You must enable HTTP and/or HTTPS access and administrative access on the interface to ensure that you can connect to the GUI. If you only enabled HTTPS access, enter "https://" before the IP address.



When you use HTTP rather than HTTPS to access the GUI, certain web browsers may display a warning that the connection is not private.

On the FortiGate-VM GUI login screen, enter the default username "admin" and then select *Login*. FortiOS does not assign a default password to the admin user.



Fortinet recommends that you configure a password for the admin user as soon as you log in to the FortiGate-VM GUI for the first time.

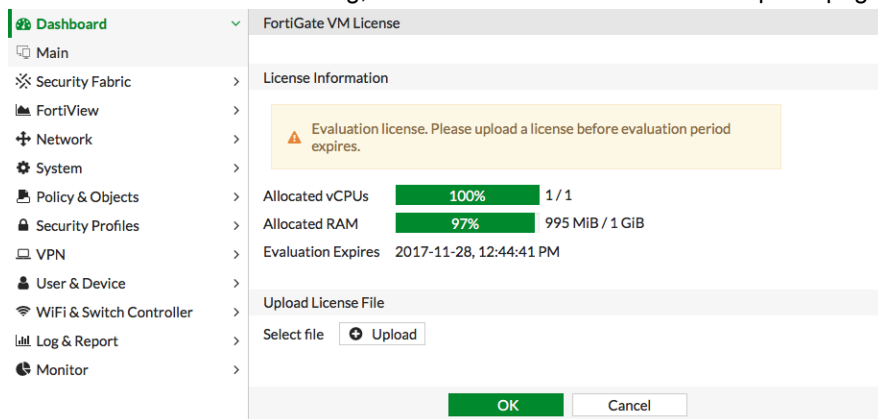
Uploading the FortiGate-VM license

Every Fortinet VM includes a 15-day trial license. During this time the FortiGate-VM operates in evaluation mode. Before using the FortiGate-VM, you must enter the license file that you downloaded from [Customer Service & Support](#) upon registration.

To upload the FortiGate-VM license file via the GUI:

1. Do one of the following to access the license upload window:
 - In *Dashboard > Status* window, in the *Virtual Machine* widget, click the *FGVMEV* (FortiGate-VM Evaluation) *License* icon. This reveals a menu of selections to take you directly to the *FortiGate VM License* window or to the *FortiGuard Details* window.
 - Go to *System > FortiGuard*. In the *License Information* section, go to the *Virtual Machine* row and click *FortiGate VM License*.

2. In the *Evaluation License* dialog, select *Enter License*. The license upload page opens.



3. Select *Upload* and locate the license file (.lic) on your computer.

4. Select *OK* to upload the license file.

5. Refresh the browser to log in.

6. Enter `admin` in the Name field and select *Login*.

The VM registration status appears as valid in the License Information widget after the license is validated by the FortiGuard Distribution Network (FDN) or FortiManager for closed networks.



Modern browsers can have an issue with allowing connecting to a FortiGate if the encryption on the device is too low. If this happens, use an FTP/TFTP server to apply the license.

To upload the FortiGate-VM license file via the CLI:

You can also upload the license file using the following CLI command:

```
execute restore vmlicense {ftp | tftp} <filename string> <ftp server>[:ftp port]
```

Example:

The following is an example output when using a TFTP server to install a license:

```
execute restore vmlicense tftp license.lic 10.0.1.2
This operation will overwrite the current VM license!Do you want to continue? (y/n)y
Please wait...Connect to tftp server 10.0.1.2 ...
Get VM license from tftp server OK.
VM license install succeeded.
Rebooting firewall.
```



This command automatically reboots the firewall without giving you a chance to back out or delay the reboot.

Validating the FortiGate-VM license with FortiManager

You can validate your FortiGate-VM license with some FortiManager models. To determine whether your FortiManager has the VM activation feature, see the [FortiManager datasheet's Features section](#).

To validate your FortiGate-VM with your FortiManager:

1. To configure your FortiManager as a closed network, enter the following CLI command on your FortiManager:

```
config fmupdate publicnetwork
  set status disable
end
```

2. To configure FortiGate-VM to use FortiManager as its override server, enter the following CLI commands on your FortiGate-VM:

```
config system central-management
  set mode normal
  set type fortimanager
  set fmg <FortiManager IPv4 address>
  config server-list
    edit 1
      set server-type update
      set server-address <FortiManager IPv4 address>
    end
  end
  set fmg-source-ip <Source IPv4 address when connecting to the FortiManager>
  set include-default-servers disable
  set vdom <Enter the VDOM name to use when communicating with the FortiManager>
end
```

3. Load the FortiGate-VM license file in the GUI:

- a. Go to *System > Dashboard > Status*.
- b. In the *License Information* widget, in the *Registration Status* field, select *Update*.
- c. Browse for the `.lic` license file and select *OK*.

4. To activate the FortiGate-VM license, enter the `execute update-now` command on your FortiGate-VM.

5. To check the FortiGate-VM license status, enter the following CLI commands on your FortiGate-VM:

```
get system status
Version: Fortigate-VM v5.0,build0099,120910 (Interim)
Virus-DB: 15.00361(2011-08-24 17:17)
Extended DB: 15.00000(2011-08-24 17:09)
Extreme DB: 14.00000(2011-08-24 17:10)
IPS-DB: 3.00224(2011-10-28 16:39)
FortiClient application signature package: 1.456(2012-01-17 18:27)
Serial-Number: FGVM02Q105060000
License Status: Valid
BIOS version: 04000002
Log hard disk: Available
Hostname: Fortigate-VM
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: standalone
Distribution: International
Branch point: 511
Release Version Information: MR3 Patch 4
System time: Wed Jan 18 11:24:34 2012
```

```
diagnose hardware sysinfo vm full
  UUID: 564db33a29519f6b1025bf8539a41e92
  valid: 1
```



```

status: 1
code: 200 (If the license is a duplicate, code 401 displays)
warn: 0
copy: 0
received: 45438
warning: 0
recv: 201201201918
dup:
    
```

Licensing timeout

In closed environments without Internet access, you must license the FortiGate-VM offline using a FortiManager as a license server. If the FortiGate-VM cannot validate its license within the 30-day license timeout period, the FortiGate discards all packets, effectively ceasing operation as a firewall.

The license status goes through some changes before it times out:

| Status | Description |
|----------------|---|
| Valid | The FortiGate can connect and validate against a FortiManager or FDS. |
| Warning | The FortiGate cannot connect and validate against a FortiManager or FDS. A check is made against how many days the Warning status has been continuous. If the number is less than 30 days, the status does not change. |
| Invalid | The FortiGate cannot connect and validate against a FortiManager or FDS. A check is made against how many days the Warning status has been continuous. If the number is 30 days or more, the status changes to Invalid. The firewall ceases to function properly. |



There is only a single log entry after the FortiGate-VM cannot access the license server for the license expiration period. When you search the logs for the reason that the FortiGate is offline, there is not a long error log list that draws attention to the issue. There is only one entry.

Testing connectivity

You can now power on your FortiGate-VM.

Use one of the following methods to power on the FortiGate-VM:

- Select the FortiGate-VM in the inventory list, and select *Power on the virtual machine* in the *Getting Started* tab.
- In the inventory list, right-click the FortiGate-VM, and select *Power > Power On*.
- Select FortiGate-VM, and click the *Power On* button on the toolbar.

The PING utility is the usual method to test connectivity to other devices. For this, you need the console on the FortiGate-VM. Select the *Console* tab to access the FortiGate-VM console. To enter text, click in the console window. This captures the mouse pointer; however, as the FortiGate-VM console is text-only, the pointer is not visible. To release the pointer, press Ctrl+Alt.



In FortiOS, the command for the PING utility is `execute ping` followed by the IP address you want to connect to.

Before you configure the FortiGate-VM for use in production, ensure that connections between it and all required resources can be established.

- If the FortiGate-VM will provide firewall protection between your network and the internet, verify that it can connect to your Internet access point and to resources on the Internet.
- If the FortiGate-VM is part of a Fortinet Security Fabric, verify that it can connect to all devices in the Fabric.
- Verify that each node on your network can connect to the FortiGate-VM.

Configuring your FortiGate-VM

For information about configuring and operating the FortiGate-VM after successful deployment and startup on the hypervisor, see the [FortiOS Administration Guide](#).

Transparent mode

If you want to configure the FortiGate-VM to operate in transparent mode, you must configure the VMware ESXi server's virtual switches to operate in promiscuous mode to allow traffic that is not addressed to the FortiGate-VM to pass through it.

To configure virtual switches to support FortiGate-VM transparent mode:

1. In the vSphere client, select your VMware server, and then select the *Configuration* tab.
2. In *Hardware*, select *Networking*.
3. Select *Properties* of vSwitch0.
4. In the *Properties* window, select *vSwitch*, and then select *Edit*.
5. Select the *Security* tab, set *Promiscuous Mode* to *Accept*, and then select *OK*.
6. Select *Close*.
7. Repeat steps 3 to 6 for other virtual switches that the FortiGate-VM uses.

High availability

FortiGate-VM HA supports having two VMs in an HA cluster on the same physical platform or different platforms. The primary consideration is that all interfaces involved can communicate efficiently over TCP/IP connection sessions.

Heartbeat

There are two options for setting up the HA heartbeat: unicast and broadcast. Broadcast is the default HA heartbeat configuration. However, the broadcast configuration may not be ideal for FortiGate-VM because it may require special settings on the host. In most cases, the unicast configuration is preferable.

Differences between the unicast and broadcast heartbeat setups are:

- The unicast method does not change the FortiGate-VM interface MAC addresses to virtual MAC addresses.
- Unicast HA only supports two FortiGate-VMs.
- Unicast HA heartbeat interfaces must be connected to the same network and you must add IP addresses to these interfaces.

Unicast

You can configure the unicast settings in the FortiOS CLI:

```
config system ha
  set unicast-hb {enable/disable}
  set unicast-hb-peerip {Peer heartbeat interface IP address}
end
```

| Setting | Description |
|-------------------|---|
| unicast-hb | Enable or disable default unicast HA heartbeat. |
| unicast-hb-peerip | IP address of the HA heartbeat interface of the other FortiGate-VM in the HA cluster. |

Broadcast

Broadcast HA heartbeat packets are non-TCP packets that use Ethertype values 0x8890, 0x8891, and 0x8890. These packets use automatically assigned link-local IPv4 addresses in the 169.254.0.x range for HA heartbeat interface IP addresses.

For FortiGate-VMs to support a broadcast HA heartbeat configuration, you must configure the virtual switches that connect heartbeat interfaces to operate in promiscuous mode and support MAC address spoofing.

In addition, you must configure the VM platform to allow MAC address spoofing for the FortiGate-VM data interfaces. This is required because in broadcast mode, the FGCP applies virtual MAC addresses to FortiGate data interfaces, and these virtual MAC addresses mean that matching interfaces of the FortiGate-VM instances in the cluster have the same virtual MAC addresses.

To configure a virtual switch that connects heartbeat interfaces:

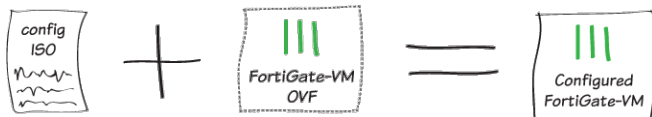
1. In the vSphere client, select your VMware server, and then select the *Configuration* tab.
2. In *Hardware*, select *Networking*.
3. Select the virtual switch *Properties*.
4. In the *Properties* window, select *vSwitch*, and then select *Edit*.
5. Select the *Security* tab, set *Promiscuous Mode* to *Accept*, and then select *OK*.
6. Select *Close*.

You must also configure the virtual switches connected to other FortiGate-VM interfaces to allow MAC address changes and accept forged transmits. This is required because the FGCP sets virtual MAC addresses for all FortiGate-VM interfaces and the same interfaces on the different FortiGate-VM instances in the cluster will have the same virtual MAC addresses.

To configure a virtual switch that connects FortiGate-VM interfaces:

1. In the vSphere client, select your VMware server, and then select the *Configuration* tab.
2. In *Hardware*, select *Networking*.
3. Select *Properties* of the virtual switch.
4. Set *MAC Address Changes* to *Accept*.
5. Set *Forged Transmits* to *Accept*.

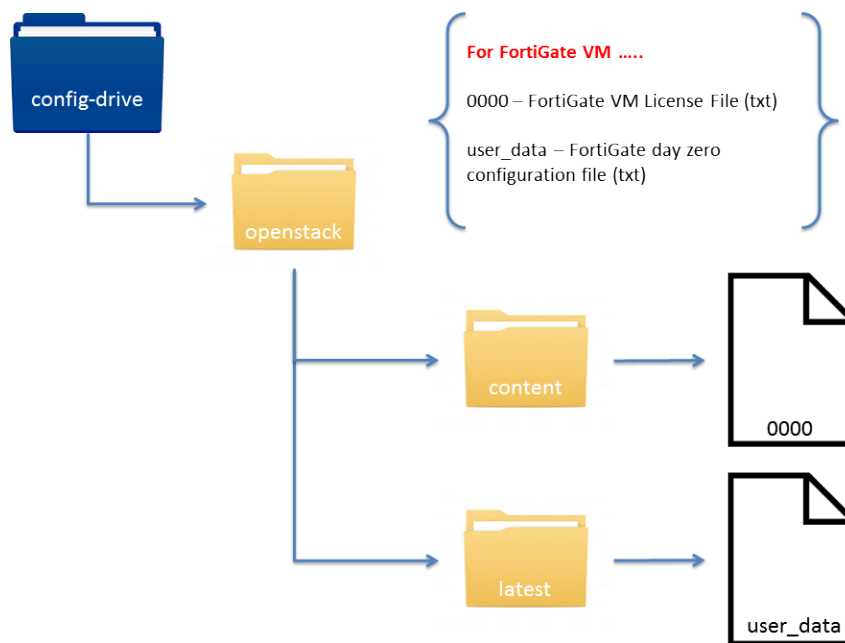
Cloud-init using config drive



This section describes how to bootstrap a FortiGate-VM in VMware vCenter using config drive. If you find yourself deploying VMs on VMware vCenter or standalone ESX and are looking for a way to preconfigure the FortiGate-VM so that it boots with a predetermined configuration, and a valid license you have found the right recipe

Make sure to verify the config drive functionality available for your FortiGate-VM version in the release notes. FortiGate-VM 5.4.1 and above support version 2 of the config-drive capabilities. [Cloud-Init config drive](#) was initially created for OpenStack and other cloud environments and is a capability available on the FortiGate-VM even when booting within a VMware vCenter or standalone ESX environment. *Config drive* also allows the administrator to pass both day zero configuration scripts and FGT-VM licenses to the FortiGate on initial boot.

To pass a *config drive* to the FGT-VM, first you must create a directory structure, and place the license file and configuration script file in the appropriate places. Here is the directory structure you will need:



For more information on the directory structure, see [ESXi cloud init reference](#) on page 29.

FortiGate-VM license file

The contents of the FGT-VM license file go into the `0000` file. Generally one would cat the license file and redirect the output into the `config-drive/openstack/content/0000` file.

```
fgt-user@ubuntu: /var/tmp$
```

```
fgt-user@ubuntu:/var/tmp$ cat config-drive/openstack/content/0000
-----BEGIN FGT VM LICENSE-----
#-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-#
#-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-#
#-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-#
-----END FGT VM LICENSE-----
fgt-user@ubuntu:/var/tmp$
```

FortiGate configuration script

The configuration script for a FortiGate-VM uses standard FortiOS CLI syntax.

Here is a simple example, where the hostname is `Example-Day0` and `port1` is configured to use DHCP to get an IP address:

```
cat config-drive/openstack/latest/user_data
#Example FGT Day0 Configuration
config system global
set hostname Example-Day0
end

config system interface
edit port1
set mode dhcp
set allowaccess https ssh ping
end
fgt-user@ubuntu:/var/tmp$
```

Creating the config drive ISO

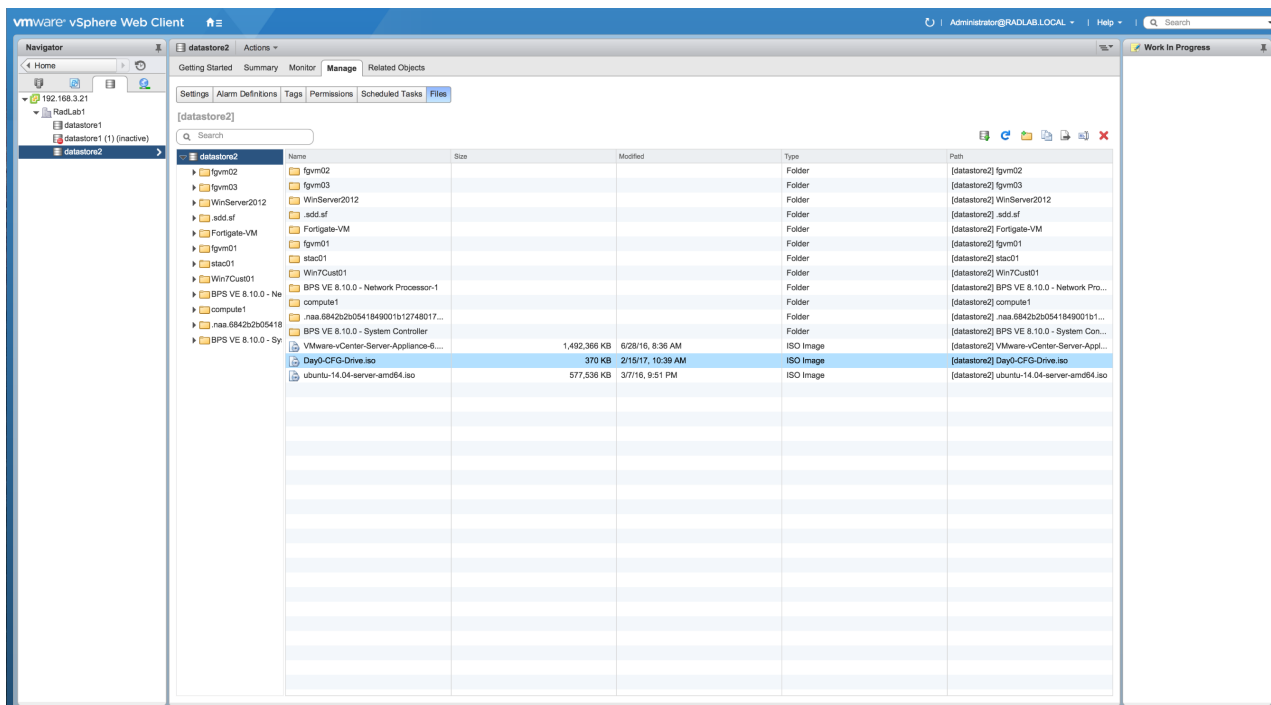
To create the config drive ISO:

1. Create the config-drive ISO using a utility such as **xorriso** (other utilities can also be used to create ISOs, such as **mkisofs**). Using **xorriso**, this example refers to the config-drive directory created above with the relevant license file and configuration script. Here is an example of creating a config-drive ISO on an Ubuntu host:

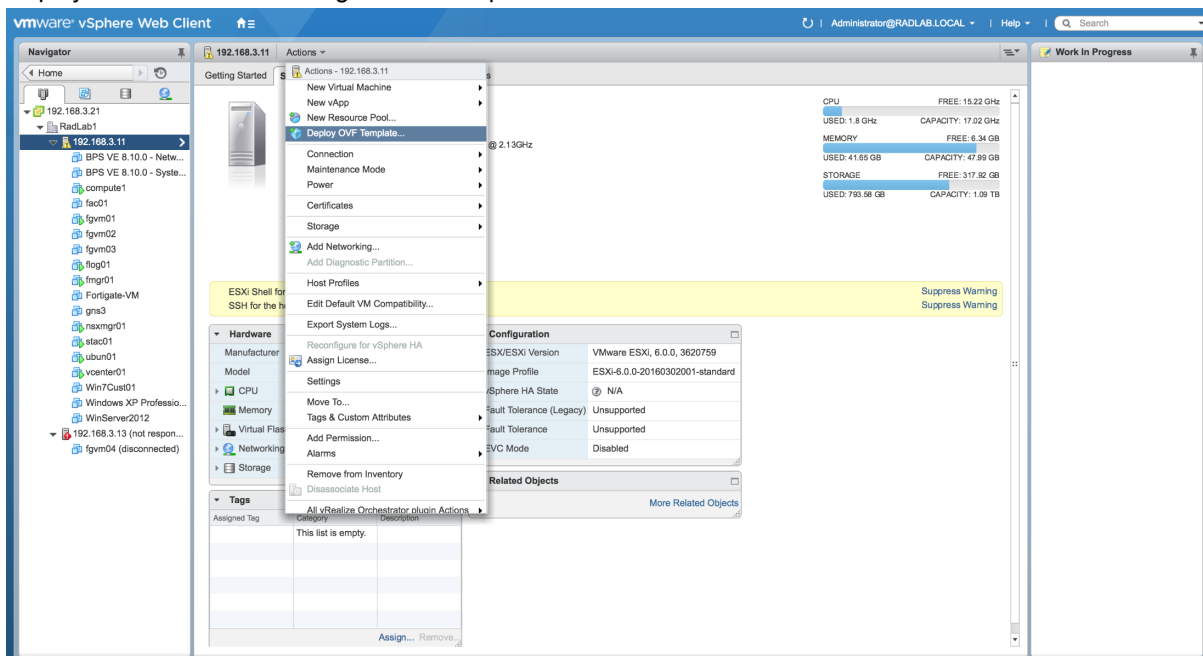
```
xorriso -as mkisofs -V config-2 -o Day0-CFG-Drive.iso config-drive/
xorriso 1.3.2 : RockRidge filesystem manipulator, libburnia project.
Drive current: -outdev 'stdio:Day0-CFG-Drive.iso'
Media current: stdio file, overwriteable
Media status : is blank
Media summary: 0 sessions, 0 data blocks, 0 data, 14.3g free
xorriso : WARNING : -volid text does not comply to ISO 9660 / ECMA 119 rules
Added to ISO image: directory '/'='/var/tmp/config-drive'
xorriso : UPDATE : 5 files added in 1 seconds
xorriso : UPDATE : 5 files added in 1 seconds
ISO image produced: 185 sectors
Written to medium : 185 sectors at LBA 0
Writing to 'stdio:Day0-CFG-Drive.iso' completed successfully.
```

```
ls -l Day0-CFG-Drive.iso
-rw-rw-r-- 1 fgt-user fgt-user 378880 Feb 15 13:32 Day0-CFG-Drive.iso
```

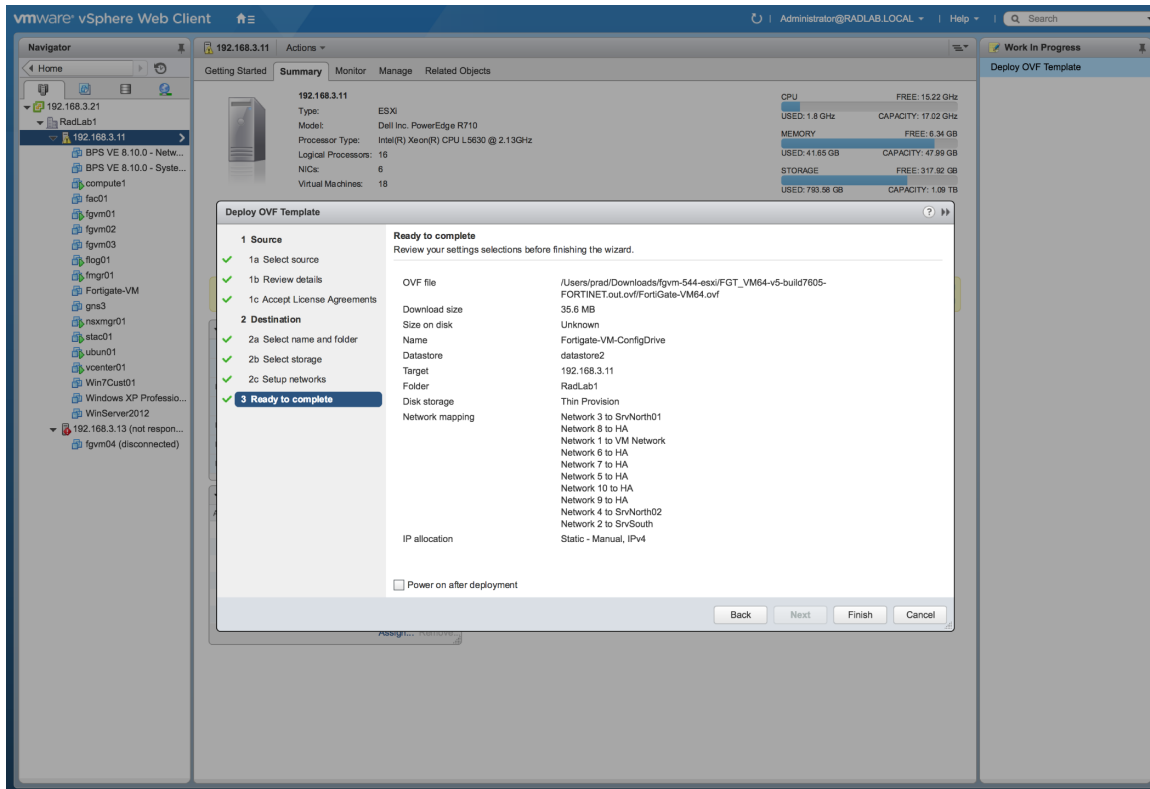
- Now that the configuration drive has been created, place the ISO on the data store so that it can be used with FortiGate-VMs.



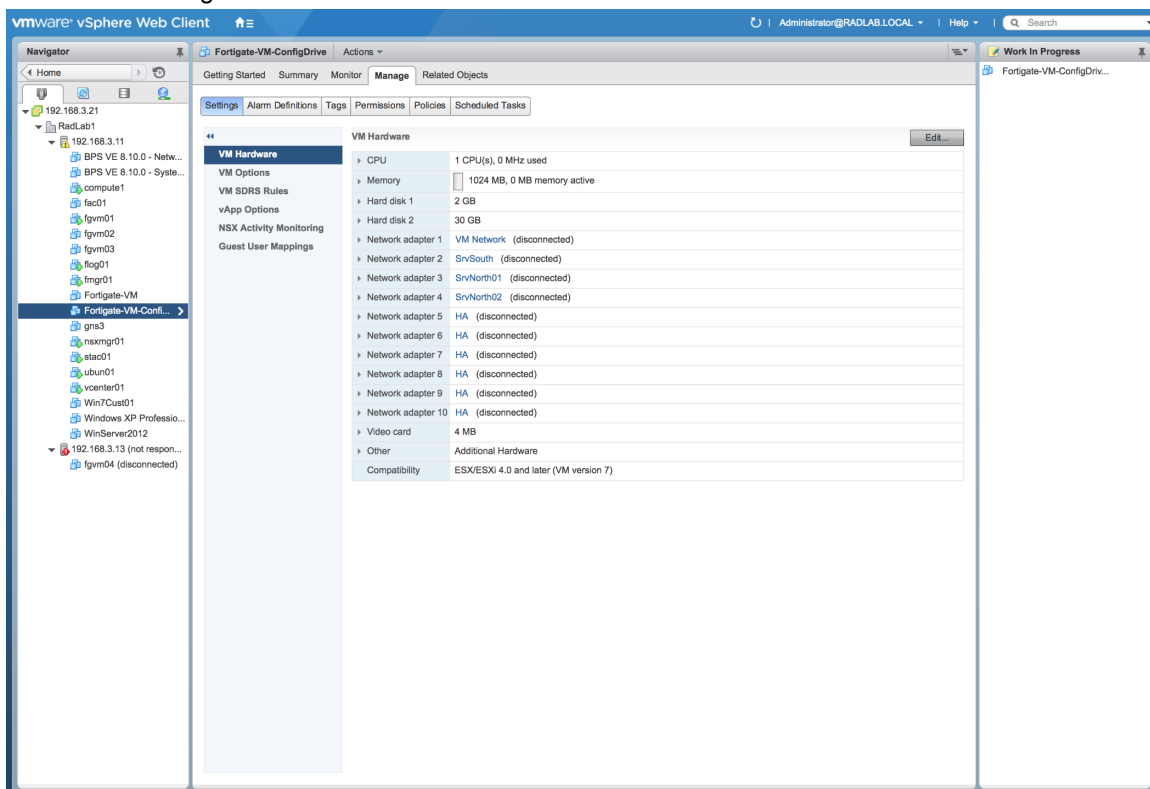
- Deploy the FortiGate-VM using an OVF template.



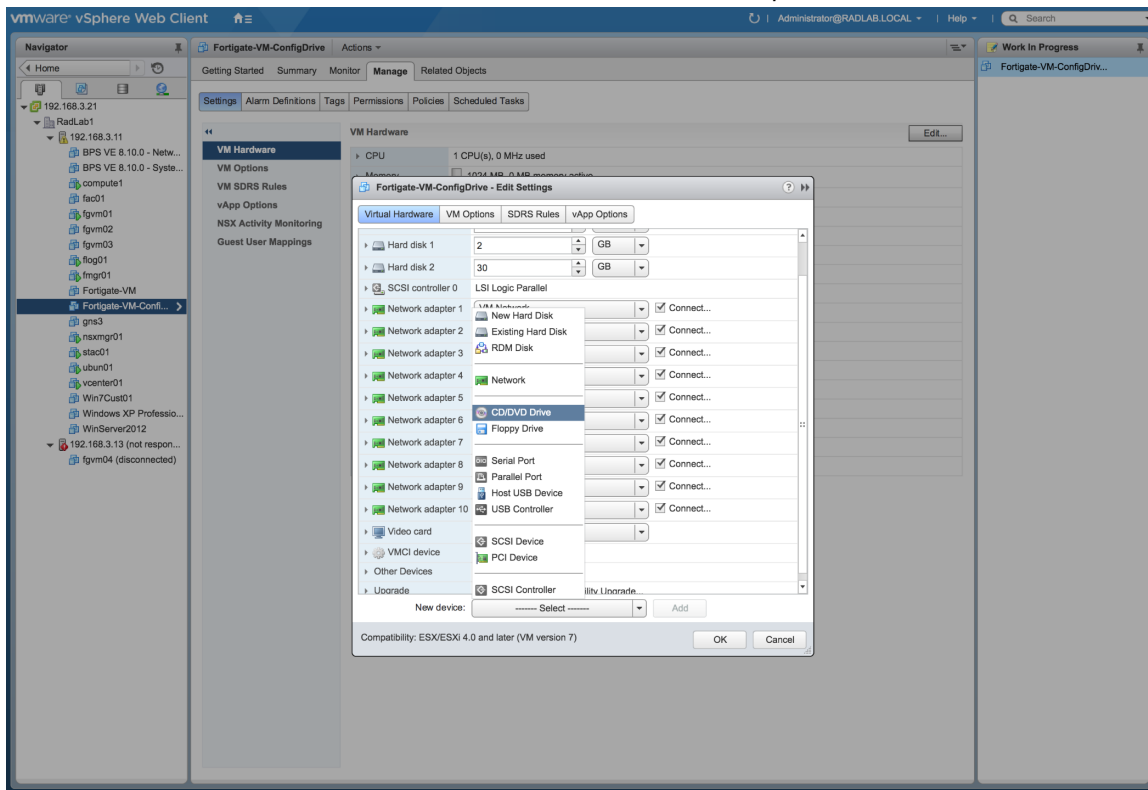
- Accept the EULA, define your storage policy along with the virtual disk format, and pick the network configuration. Once you reach the end of the OVF template deployment make sure to deselect *Power on after deployment*. This is so we can attach our config-drive ISO as a *cdrom* device before initial boot.



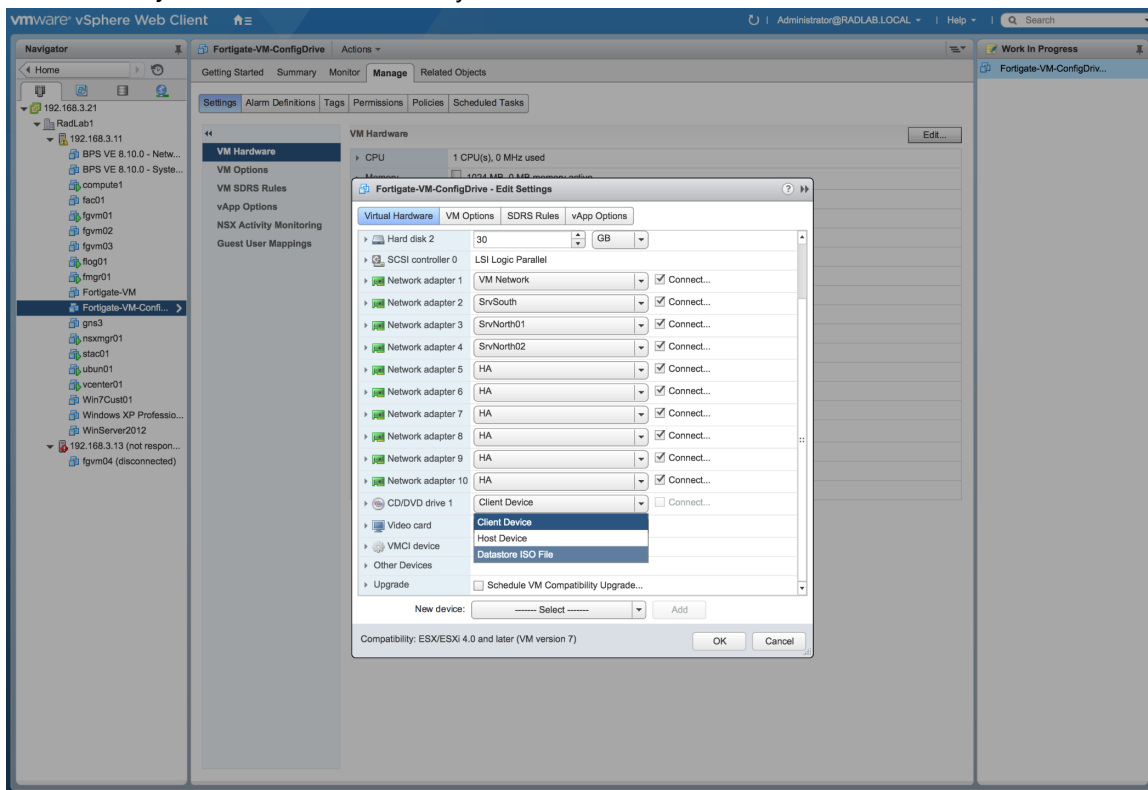
5. Edit the VM settings.



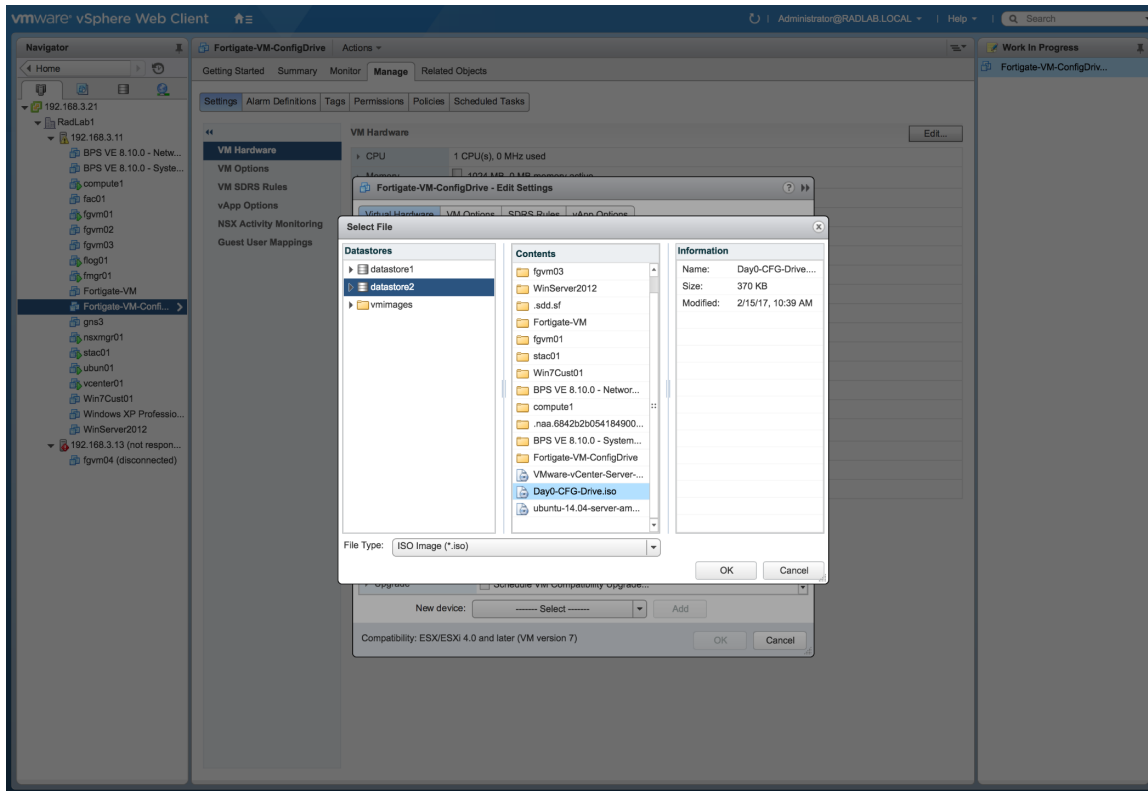
6. Add a new device: *CD/DVD drive* and make sure to select *Connect at power on*.



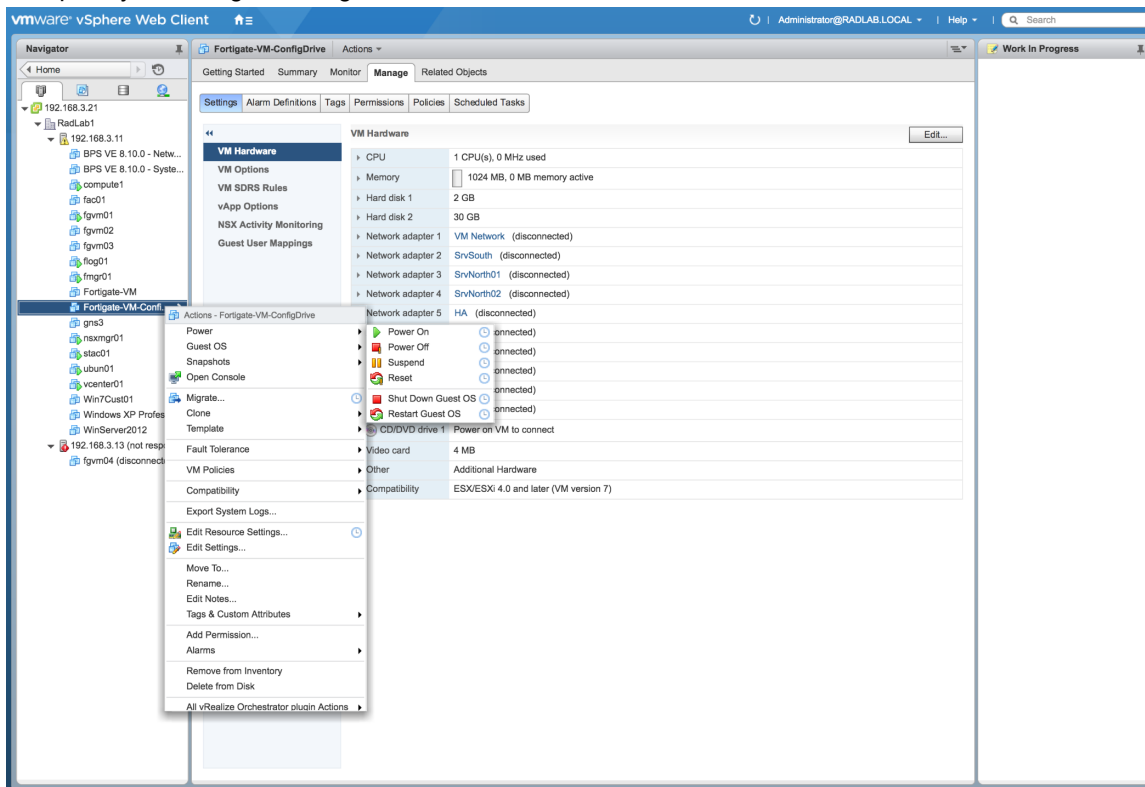
7. Attach the *Day0-CFG-Drive.iso* ISO that you created earlier.



Cloud-init using config drive



8. Complete your changes, then go to the VM to boot it.

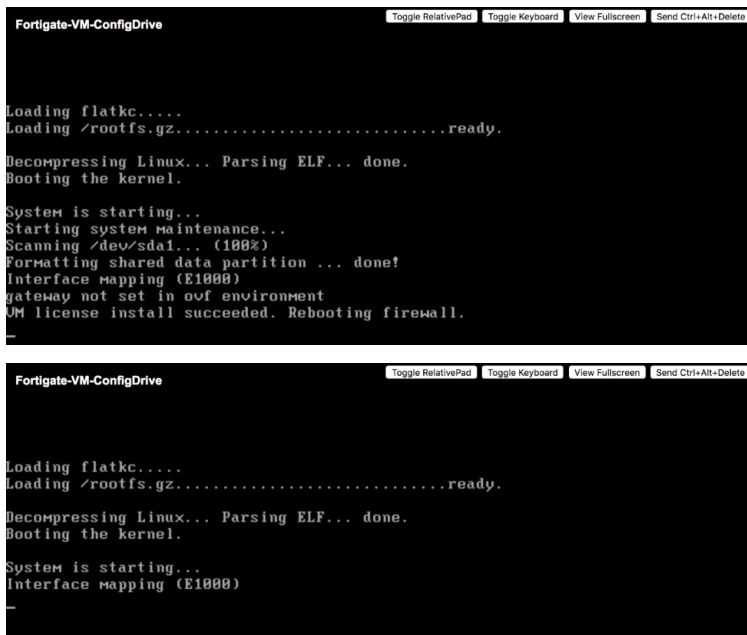


Verifying the results

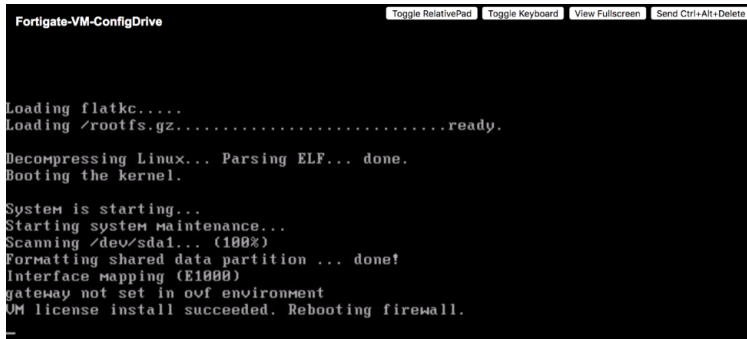
Boot the FortiGate-VM and open the console to verify that the VM is booting and utilizing the license file and day zero configuration file that was provided.

To verify the results:

1. Power on the VM.



2. Go to the *Console*. Verify that you see the VM *license install succeeded* message and the subsequent reboot.



3. Upon completion of the boot sequence, you can verify that the FGT-VM hostname has changed to *Example-Day0*. Also verify that the license file has been verified and the license registration status has changed to *VALID*.

```
FortiGate-VM-ConfigDrive
Loading flatk....
Loading /rootfs.gz.....ready.
Decompressing Linux... Parsing ELF... done.
Booting the kernel.
System is starting...
Interface mapping (E1000)
Example-Day0 login: admin
Password:
Welcome !
Example-Day0 # *ATTENTION*: Admin sessions removed because license registration
status changed to 'VALID'
Example-Day0 #
Example-Day0 login: _
```

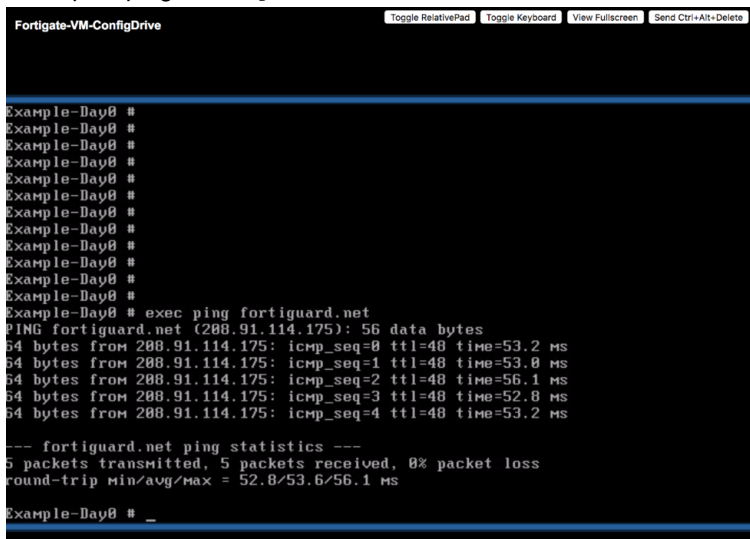
4. After logging in, use the `get system status` command to verify that the license is valid.

```
FortiGate-VM-ConfigDrive
Version: FortiGate-UM64 v5.4.4,build7605,170208 (GA)
Virus-DB: 1.00123(2015-12-11 13:10)
Extended DB: 1.00000(2012-10-17 15:46)
IPS-DB: 6.00741(2015-12-01 02:30)
IPS-ETDB: 0.00000(2001-01-01 00:00)
Serial-Number: FGUM020000064003
IPS Malicious URL Database: 1.00001(2015-01-01 01:01)
Botnet DB: 1.00000(2012-05-28 22:51)
License Status: Valid
BIOS version: 04000002
Log hard disk: Need format
Hostname: Example-Day0
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: standalone
Branch point: 1117
Release Version Information: GA
FortiOS x86-64: Yes
System time: Wed Feb 15 10:46:05 2017
Example-Day0 # _
```

5. Use the `get system interface physical` to verify that port1 (configured in DHCP mode), has received an IP from the DHCP server.

```
FortiGate-VM-ConfigDrive
Example-Day0 # get sys int physical
== [onboard]
  ==[port1]
    mode: dhcp
    ip: 192.168.3.201 255.255.255.0
    ipv6: ::0
    status: up
    speed: 1000Mbps (Duplex: full)
  ==[port2]
    mode: static
    ip: 0.0.0.0 0.0.0.0
    ipv6: ::0
    status: up
    speed: 1000Mbps (Duplex: full)
  ==[port3]
    mode: static
    ip: 0.0.0.0 0.0.0.0
    ipv6: ::0
    status: up
    speed: 1000Mbps (Duplex: full)
  ==[port4]
    mode: static
    ip: 0.0.0.0 0.0.0.0
    ipv6: ::0
--More-- _
```

6. Attempt to ping `fortiguard.com` to confirm that the FortiGate-VM can contact Fortinet for licensing and updates.



ESXi cloud init reference

For ESXi the utility `xorriso` is used on a Linux host to create the ISO used to boot the VM. The following describes the directory structure used to create the ISO.

After the ISO is created, you must upload it to your datastore of choice and attach it to the FortiGate-VM after deploying the OVF but before booting it up for the first time.

```
ls -lR config-drive/
config-drive/:
total 4
drwxrwxr-x 4 fgt-user fgt-user 4096 Feb 8 16:59 openstack
```

```
config-drive/openstack:
total 8
drwxrwxr-x 2 fgt-user fgt-user 4096 Feb 8 17:07 content
drwxrwxr-x 2 fgt-user fgt-user 4096 Feb 8 17:06 latest
```

```
config-drive/openstack/content:
total 4
-rw-rw-r-- 1 fgt-user fgt-user 287 Feb 8 17:00 0000
```

```
config-drive/openstack/latest:
total 4
-rw-r--r-- 1 fgt-user fgt-user 172 Feb 8 17:06 user_data
```

```
cat config-drive/openstack/content/0000
-----BEGIN FGT VM LICENSE---
#-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED- REDACTED-#
#-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED- REDACTED-#
#-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-#
-----END FGT VM LICENSE---
```

```
cat config-drive/openstack/latest/user_data
```

```
#Example FGT Day0 Configuration

config system global
set hostname Example-Day0
end
config system interface
edit port1
set mode dhcp
set allowaccess https ssh ping end

xorriso -as mkisofs -V config-2 -o Day0-CFG-Drive.iso config-drive/
xorriso 1.3.2 : RockRidge filesystem manipulator, libburnia project.

Drive current: -outdev 'stdio:Day0-CFG-Drive.iso' Media current: stdio file, overwriteable
Media status : is blank
Media summary: 0 sessions, 0 data blocks, 0 data, 14.3g free
xorriso : WARNING : -volid text does not comply to ISO 9660 / ECMA 119 rules Added to ISO
image:
directory '/'='/var/tmp/config-drive'
xorriso : UPDATE : 5 files added in 1 seconds xorriso : UPDATE : 5 files added in 1 seconds
ISO
image produced: 185 sectors
Written to medium : 185 sectors at LBA 0
Writing to 'stdio:Day0-CFG-Drive.iso' completed successfully.

ls -l Day0-CFG-Drive.iso
-rw-rw-r-- 1 fgt-user fgt-user 378880 Feb 15 13:32 Day0-CFG-Drive.iso
```

SDN connector integration with VMware ESXi

See the *FortiOS Administration Guide*.

Optimizing FortiGate-VM performance

This section describes FortiGate-VM and VMware ESXi performance optimization techniques that can improve your FortiGate-VM performance by optimizing the hardware and the VMware ESXi host environment for FortiGate-VM's network- and CPU-intensive performance requirements.

Additionally, the port4 interface MTU is set to be compatible with the OpenStack 10 environment, which has an MTU of 1446 by default. (In the user_data file, the MTU of port4 is set to 1400.) Using the same MTU setting as the OpenStack 10 environment enables the HA heartbeat interfaces to communicate effectively over the ha-sync network.

See these pages for more information on RedHat OpenStack networks and MTU values:

- [MTU for VLAN networks is by default 1496 Bytes in Red Hat OpenStack Platform 10](#)
- [Configure MTU Settings](#)

SR-IOV

FortiGate-VMs installed on VMware ESXi platforms support Single Root I/O virtualization (SR-IOV) to provide FortiGate-VMs with direct access to physical network cards. Enabling SR-IOV means that one PCIe network card or CPU can function for a FortiGate-VM as multiple separate physical devices. SR-IOV reduces latency and improves CPU efficiency by allowing network traffic to pass directly between a FortiGate-VM and a network card, bypassing VMware ESXi host software and without using virtual switching.

FortiGate-VMs benefit from SR-IOV because SR-IOV optimizes network performance and reduces latency and CPU usage. FortiGate-VMs do not use VMware ESXi features that are incompatible with SR-IOV, so you can enable SR-IOV without negatively affecting your FortiGate-VM. SR-IOV implements an I/O memory management unit (IOMMU) to differentiate between different traffic streams and apply memory and interrupt translations between the physical functions (PF) and virtual functions (VF).

Setting up SR-IOV on VMware ESXi involves creating a PF for each physical network card in the hardware platform. Then, you create VFs that allow FortiGate-VMs to communicate through the PF to the physical network card. VFs are actual PCIe hardware resources and only a limited number of VFs are available for each PF.

SR-IOV hardware compatibility

SR-IOV requires that the hardware and operating system on which your VMware ESXi host is running has BIOS, physical NIC, and network driver support for SR-IOV.

To enable SR-IOV, your VMware ESXi platform must be running on hardware that is compatible with SR-IOV and with FortiGate-VMs. FortiGate-VMs require network cards that are compatible with ixgbev or i40evf drivers. As well, the host hardware CPUs must support second level address translation (SLAT).

For optimal SR-IOV support, install the most up to date ixgbev or i40e/i40evf network drivers. Fortinet recommends i40e/i40evf drivers because they provide four TxRx queues for each VF and ixgbev only provides two TxRx queues.

Create SR-IOV virtual interfaces

Complete the following procedure to enable SR-IOV. This procedure requires restarting the VMware host and powering down the FortiGate-VM and should only be done during a maintenance window or when the network is not very busy.

For example, if you are using the VMware host client:

1. Go to *Manage > Hardware > PCI Devices* to view all of the PCI devices on the host.
2. Select the *SR-IOV capable* filter to view the PCI devices (network adapters) that are compatible with SR-IOV.
3. Select a network adapter and select *Configure SR-IOV*.
4. Enable *SR-IOV* and specify the *Number of virtual functions*.
5. Save your changes and restart the VMware host

For example, if you are using the vSphere web client:

1. Go to the host with the SR-IOV physical network adapter that you want to add virtual interfaces to.
2. In the *Networking* part of the *Manage* tab, select *Physical Adapters*.
3. Select the physical adapter for which to enable SR-IOV settings.
4. Enable *SR-IOV* and specify the *Number of virtual functions*.
5. Save your changes and restart the VMware host.

You can also use the following command from the ESXi host CLI to add virtual interfaces to one or more compatible network adapters:

```
$ esxcli system module parameters set -m <driver-name> -p "max_vfs=<virtual-interfaces>"
```

Where *<driver-name>* is the name of the network adapter driver (for example *ixgbevf* or *i40evf*) and *<virtual-interfaces>* is a comma-separated list of number of virtual interfaces to allow for each physical interface.

For example, if your VMware host includes three *i40evf* network adapters and you want to enable 6 virtual interfaces on each network adapter, enter the following:

```
$ esxcli system module parameters set -m <i40evf> -p "max_vfs=6,6,6"
```

Assign SR-IOV virtual interfaces to a FortiGate-VM

1. Power off the FortiGate-VM and open its virtual hardware settings.
2. Create or edit a network adapter and set its type to *SR-IOV passthrough*.
3. Select the physical network adapter for which you have enabled SR-IOV.
4. Optionally associate the FortiGate-VM network adapter with the port group on a standard or distributed switch.
5. To guarantee that the pass-through device can access all VM memory, in the *Memory* section select *Reserve all guest memory*.
6. Save your changes and power on the FortiGate-VM.

Set up VMware CPU affinity

Configuring CPU affinity on your FortiGate-VM further builds on the benefits of SR-IOV by enabling the FortiGate-VM to align interrupts from interfaces to specific CPUs.

By specifying a CPU affinity setting for each VM, you can restrict the assignment of VMs to a subset of the available processors in multiprocessor systems. By using this feature, you can assign each VM to processors in the specified affinity set.

Using CPU affinity, you can assign a VM to a specific processor. This assignment allows you to restrict the assignment of VMs to a specific available processor in multiprocessor systems.

For example, if you are using the vSphere web client use the following steps:

1. Power off the FortiGate-VM.
2. Edit the FortiGate-VM hardware settings and select Virtual Hardware.
3. Select CPU options.
4. In Scheduling Affinity, specify the CPUs to have affinity with the FortiGate-VM. For best results, the affinity list should include one entry for each of the FortiGate-VM's virtual CPUs.
5. Save your changes.

Interrupt affinity

In addition to enabling SR-IOV in the VM host, to fully take advantage of SR-IOV performance improvements you must configure interrupt affinity for your FortiGate-VM. Interrupt affinity (also called CPU affinity) maps FortiGate-VM interrupts to the CPUs that are assigned to your FortiGate-VM. You use a CPU affinity mask to define the CPUs that the interrupts are assigned to.

A common use of this feature is to improve your FortiGate-VM's networking performance by:

- On the VM host, add multiple host CPUs to your FortiGate-VM.
- On the VM host, configure CPU affinity to specify the CPUs that the FortiGate-VM can use.
- On the VM host, configure other VM clients on the VM host to use other CPUs.
- On the FortiGate-VM, assign network interface interrupts to a CPU affinity mask that includes the CPUs that the FortiGate-VM can use.

In this way, all available CPU interrupts for the configured host CPUs are used to process traffic on your FortiGate interfaces. This configuration could lead to improve FortiGate-VM network performance because you have dedicated VM host CPU cycles to processing your FortiGate-VM's network traffic.

You can use the following CLI command to configure interrupt affinity for your FortiGate-VM:

```
config system affinity-interrupt
  edit <index>
    set interrupt <interrupt-name>
    set affinity-cpumask <cpu-affinity-mask>
  next
end
```

Where:

- `<interrupt-name>` is the name of the interrupt to associate with a CPU affinity mask. You can view your FortiGate-VM interrupts using the `diagnose hardware sysinfo interrupts` command. Usually you associate all of the interrupts for a given interface with the same CPU affinity mask.
- `<cpu-affinity-mask>` is the CPU affinity mask for the CPUs that will process the associated interrupt.

For example, consider the following configuration:

- The port2 and port3 interfaces of a FortiGate-VM send and receive most of the traffic.
- On the VM host you have set up CPU affinity between your FortiGate-VM and four CPUs (CPU 0, 1, 2, and 3).
- SR-IOV is enabled and SR-IOV interfaces use the i40evf interface driver.

The output from the `diagnose hardware sysinfo interrupts` command shows that port2 has the following transmit and receive interrupts:

```
i40evf-port2-TxRx-0
i40evf-port2-TxRx-1
i40evf-port2-TxRx-2
i40evf-port2-TxRx-3
```

The output from the `diagnose hardware sysinfo interrupts` command shows that port3 has the following transmit and receive interrupts:

```
i40evf-port3-TxRx-0
i40evf-port3-TxRx-1
i40evf-port3-TxRx-2
i40evf-port3-TxRx-3
```

Use the following command to associate the port2 and port3 interrupts with CPU 0, 1, 2, and 3.

```
config system affinity-interrupt
  edit 1
    set interrupt "i40evf-port2-TxRx-0"
    set affinity-cpumask "0x0000000000000001"
  next
  edit 2
    set interrupt "i40evf-port2-TxRx-1"
    set affinity-cpumask "0x0000000000000002"
  next
  edit 3
    set interrupt "i40evf-port2-TxRx-2"
    set affinity-cpumask "0x0000000000000004"
  next
  edit 4
    set interrupt "i40evf-port2-TxRx-3"
    set affinity-cpumask "0x0000000000000008"
  next
  edit 1
    set interrupt "i40evf-port3-TxRx-0"
    set affinity-cpumask "0x0000000000000001"
  next
  edit 2
    set interrupt "i40evf-port3-TxRx-1"
    set affinity-cpumask "0x0000000000000002"
  next
  edit 3
    set interrupt "i40evf-port3-TxRx-2"
    set affinity-cpumask "0x0000000000000004"
  next
  edit 4
    set interrupt "i40evf-port3-TxRx-3"
    set affinity-cpumask "0x0000000000000008"
  next
end
```

Packet-distribution affinity

With SR-IOV enabled on the VM host and interrupt affinity configured on your FortiGate-VM there is one additional configuration you can add that may improve performance. Most common network interface hardware has restrictions on the number of RX/TX queues that it can process. This can result in some CPUs being much busier than others and the busy CPUs may develop extensive queues.

You can get around this potential bottleneck by configuring affinity packet redistribution to allow overloaded CPUs to redistribute packets they receive to other less busy CPUs. This may result in a more even distribution of packet processing to all available CPUs.

You configure packet redistribution for interfaces by associating an interface with an affinity CPU mask. This configuration distributes packets sent and received by that interface to the CPUs defined by the CPU affinity mask associated with the interface.

You can use the following CLI command to configure affinity packet redistribution for your FortiGate-VM:

```
config system affinity-packet-redistribution
  edit <index>
    set interface <interface-name>
    set affinity-cpumask <cpu-affinity-mask>
  next
end
```

Where:

- `<interface-name>` the name of the interface to associate with a CPU affinity mask.
- `<cpu-affinity-mask>` the CPU affinity mask for the CPUs that will process packets to and from the associated interface.

For example, you can improve the performance of the interrupt affinity example shown in the following command to allow packets sent and received by the port3 interface to be redistributed to CPUs according to the 0xE CPU affinity mask.

```
config system affinity-packet-redistribution
  edit 1
    set interface port3
    set affinity-cpumask "0xE"
  next
end
```

TSO and LRO

Enabling TCP Segmentation Offload (TSO) and Large Receive Offload (LRO) can improve FortiGate-VM performance by reducing CPU overhead for TCP/IP network operations.

TSO causes network cards to divide larger data chunks into TCP segments. If you disable TSO, the CPU performs segmentation for TCP/IP. TSO is also sometimes called Large Segment Offload (LSO) or Large Send Offload.

LRO reassembles incoming network packets into larger buffers and transfers the resulting larger but fewer packets to the network stack of the host or VM. The CPU has to process fewer packets.

Your server hardware must support TSO and LRO.

To enable TSO from the vSphere web client:

1. Open the *Manage* tab and select *Advanced System Settings*.
2. For IPv4 set `Net.UseHwTSO` to 1 to enable TSO, or to 0 to disable TSO.
3. For IPv6 set `useNet.UseHwTSO6` to 1 to enable TSO, or to 0 to disable TSO.

To enable LRO from the vSphere web client:

1. Open the *Manage* tab and select *Advanced System Settings*.
2. For IPv4 TSO, set `Net.Vmxnet2HwLRO` and `Net.Vmxnet3HwLRO` to 1 to enable LRO, or to 0 to disable LRO.
3. For IPv6 TSO, set `useNet.UseHwTSO6` to 1 to enable TSO, or to 0 to disable TSO.

Hyperthreading

Enabling hyperthreading for VMware allows a single processor core to function as two logical processors, often resulting in improved performance. If your VMware server hardware CPUs support hyperthreading you may be able to optimize FortiGate-VM performance by enabling hyperthreading (sometimes called logical processor) in the server's BIOS and in VMware.

To enable hyperthreading from the vSphere web client:

1. Open the *Configuration* tab and go to *Processors > Properties*.
2. Turn on hyperthreading.
3. Save your changes.

Multiqueue support

Multiqueue can scale network performance with the number of vCPUs. Multiqueue can also create multiple TX and RX queues. Modify the `.vmx` file or access *Advanced Settings* to enable multi-queue.

To enable multiqueue:

1. Open the `.vmx` file.
2. Add the `ethernetX.pnicFeatures = "4"` parameter.

To enable receive-side scaling (RSS) from the ESXi CLI:

```
$ vmkload_mod -u ixgbe
$ vmkload_mod ixgbe RSS="4,4,4,4,4,4"
```

For the best performance, you should also configure additional CPU threads for each ethernet/vSwitch device. This is limited by the amount of spare CPU resources available on the ESXi host.

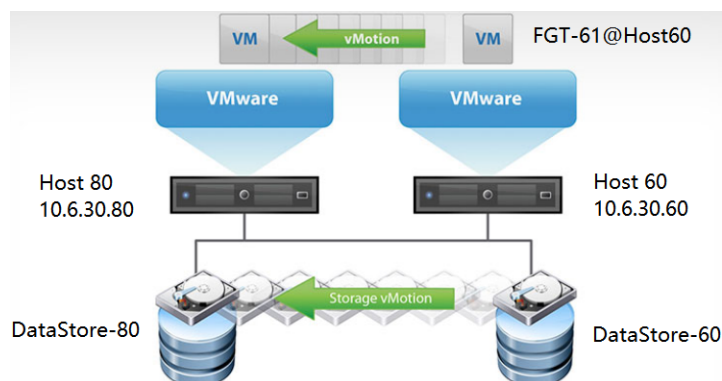
To configure additional CPU threads for each ethernet/vSwitch device:

1. Open the .vmx file.
2. Add the `ethernetX.ctxPerDev = "1"` parameter.

vMotion in a VMware ESXi environment

This guide provides sample configuration of vMotion FortiGate-VM HA in a VMware ESXi environment. This feature enables the live migration of a running FortiGate-VM from one physical server to another with zero downtime, continuous service availability, and complete transaction integrity. It also provides transparency to users.

The following depicts the network topology for this sample deployment. In this sample deployment, there are two hosts, Host 60 (10.6.30.60) and Host 80 (10.6.30.80), which are members of Cluster 1 in the DataCenter 1. The vCenter server (10.6.30.99) manages DataCenter 1.



The following prerequisites must be met for this configuration:

- The vCenter server has been set up and the data center and cluster have been created.
- Host 60 and Host 80 are part of the cluster.
- A Gigabit Ethernet network interface card with a VMkernel port enabled for vMotion exists on both ESXi hosts.
- A FortiGate-VM is set up and able to handle traffic.

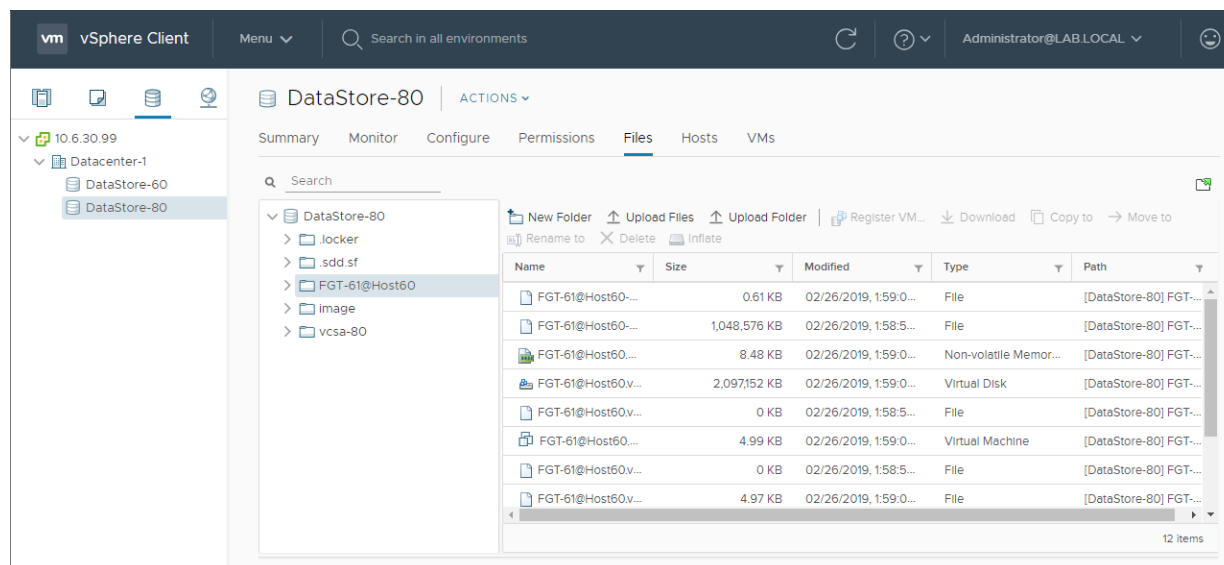
To migrate the FortiGate-VM on the vCenter web portal:

1. Log into the vCenter web portal.
2. Verify the current location of the FortiGate-VM:
 - a. Go to the FortiGate-VM.
 - b. On the *Summary* tab, check the *Host*. In this example, the host is currently Host 60 (10.6.30.60).
 - c. Go to *Storage > Files*. Check that the FortiGate-VM is located in the correct datastore. In this example, the datastore is currently Datastore 60, which is in Host 60.
3. Right-click the FortiGate-VM and select *Migrate*.
4. Configure the migration options:
 - a. For *Select a migration type*, select *Change both compute resource and storage*. Click *NEXT*.
 - b. For *Select a compute resource*, select the desired new compute resource. In this example, Host 80 (10.6.30.80) is selected. Click *NEXT*.
 - c. For *Select storage*, select the storage associated with the compute resource selected in step 5. In this example, Datastore 80 (as corresponds to Host 80) is selected. Click *NEXT*.
 - d. For *Select networks*, select the desired destination network at the compute resource selected in step 5. In this example, the source network is at Host 60, and the destination network is at Host 80. Click *NEXT*.
 - e. For *Select vMotion priority*, select *Schedule vMotion with high priority (recommended)*. Click *NEXT*.

- Before initiating the migration, open the CLI for the FortiGate-VM to check on traffic during the migration. Enter the `diag sniffer packet any 'icmp and host 8.8.8.8'` command to check if traffic is stable. If no traffic is lost during migration and the FortiGate-VM SSH session does not break, the output resembles the following:

```
FortiGate-VM64 # diag sniffer packet any 'icmp and host 8.8.8.8'
interfaces=[any]
filters=[icmp and host 8.8.8.8]
2.284655 10.1.100.22 -> 8.8.8.8: icmp: echo request
2.284704 172.16.200.61 -> 8.8.8.8: icmp: echo request
2.290014 8.8.8.8 -> 172.16.200.61: icmp: echo reply
2.290023 8.8.8.8 -> 10.1.100.22: icmp: echo reply
3.286396 10.1.100.22 -> 8.8.8.8: icmp: echo request
3.286399 172.16.200.61 -> 8.8.8.8: icmp: echo request
3.291257 8.8.8.8 -> 172.16.200.61: icmp: echo reply
3.291259 8.8.8.8 -> 10.1.100.22: icmp: echo reply
4.287616 10.1.100.22 -> 8.8.8.8: icmp: echo request
4.287620 172.16.200.61 -> 8.8.8.8: icmp: echo request
4.293134 8.8.8.8 -> 172.16.200.61: icmp: echo reply
4.293136 8.8.8.8 -> 10.1.100.22: icmp: echo reply
5.289483 10.1.100.22 -> 8.8.8.8: icmp: echo request
5.289486 172.16.200.61 -> 8.8.8.8: icmp: echo request
5.294584 8.8.8.8 -> 172.16.200.61: icmp: echo reply
5.294586 8.8.8.8 -> 10.1.100.22: icmp: echo reply
6.290972 10.1.100.22 -> 8.8.8.8: icmp: echo request
6.290976 172.16.200.61 -> 8.8.8.8: icmp: echo request
6.295467 8.8.8.8 -> 172.16.200.61: icmp: echo reply
6.295469 8.8.8.8 -> 10.1.100.22: icmp: echo reply
7.292842 10.1.100.22 -> 8.8.8.8: icmp: echo request
7.292846 172.16.200.61 -> 8.8.8.8: icmp: echo request
7.297360 8.8.8.8 -> 172.16.200.61: icmp: echo reply
7.297362 8.8.8.8 -> 10.1.100.22: icmp: echo reply
8.294735 10.1.100.22 -> 8.8.8.8: icmp: echo request
8.294742 172.16.200.61 -> 8.8.8.8: icmp: echo request
8.299282 8.8.8.8 -> 172.16.200.61: icmp: echo reply
8.299285 8.8.8.8 -> 10.1.100.22: icmp: echo reply
9.296594 10.1.100.22 -> 8.8.8.8: icmp: echo request
9.296600 172.16.200.61 -> 8.8.8.8: icmp: echo request
9.301125 8.8.8.8 -> 172.16.200.61: icmp: echo reply
9.301127 8.8.8.8 -> 10.1.100.22: icmp: echo reply
```

- Click **FINISH**. After a few seconds, the FortiGate-VM is migrated to the new compute resources, in this case Host 80.
- Log into the vCenter web portal. Go to the FortiGate-VM. On the **Summary** tab, the **Host** is now the new compute resources, in this case Host 80 (10.6.30.80).
- Go to **Storage > Files**. It shows that the FortiGate-VM is now located in a new datastore, in this example Datastore 80.



To configure the FortiGate-VM using the CLI:

```
config system interface
edit "port1"
set vdom "root"
set ip 10.6.30.61 255.255.255.0
set allowaccess ping https ssh snmp http telnet
set type physical
next
```

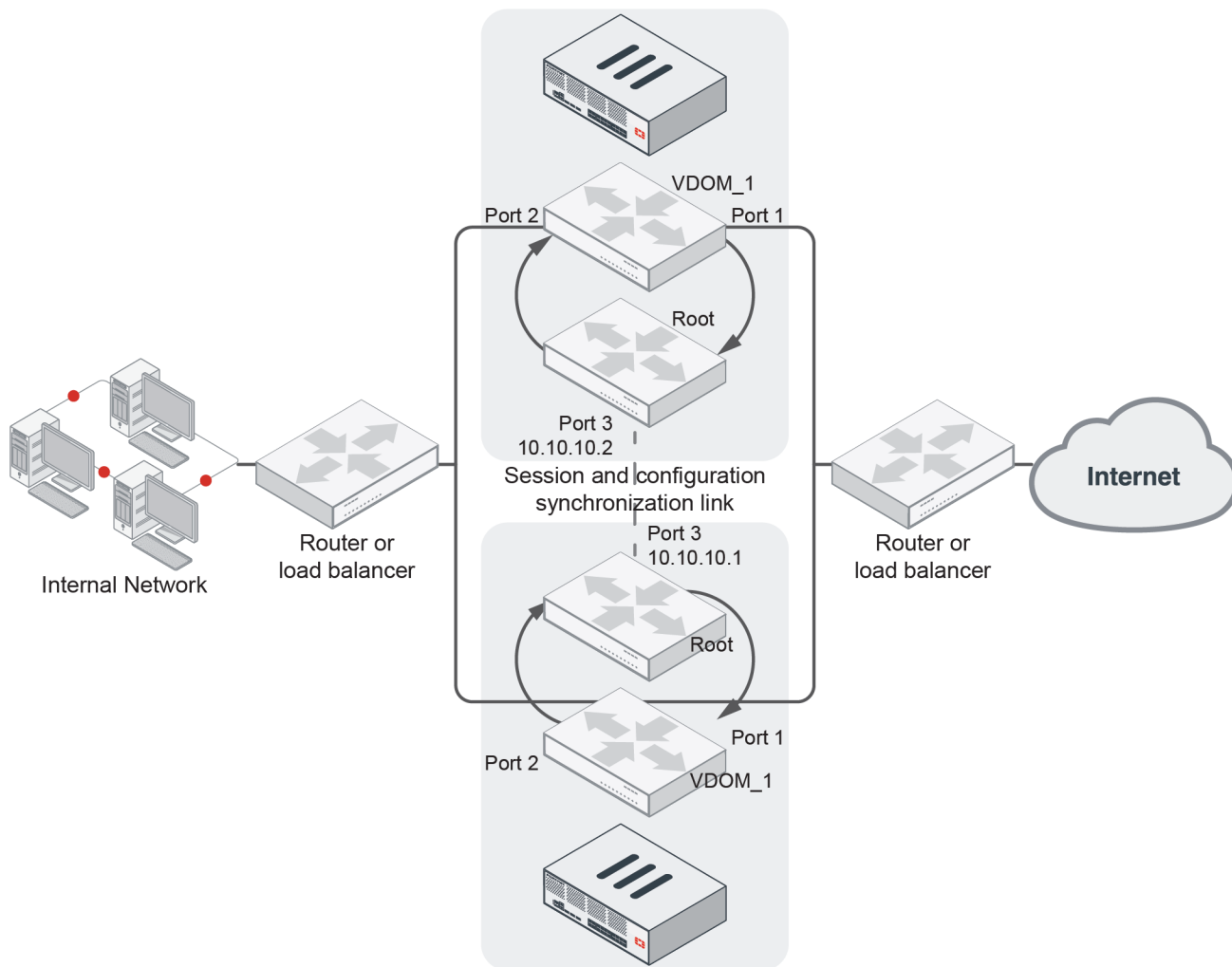


```
edit "port2"
  set vdom "root"
  set ip 10.1.100.61 255.255.255.0
  set allowaccess ping https ssh snmp http telnet
  set type physical
next
edit "port3"
  set vdom "root"
  set ip 172.16.200.61 255.255.255.0
  set allowaccess ping https ssh snmp http telnet
  set type physical
next
end
config router static
  edit 1
    set gateway 172.16.200.254
    set device "port3"
  next
end
config firewall policy
  edit 1
    set srcintf "port2"
    set dstintf "port3"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set nat enable
  next
end
```

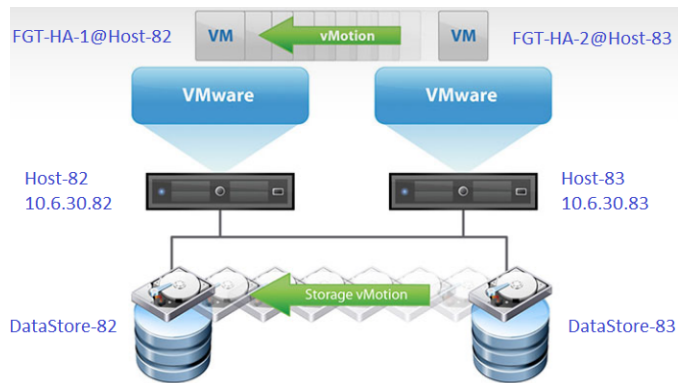
Setting up FortiGate-VM HA for a VMware vMotion environment

This guide provides sample configuration of vMotion FortiGate-VM HA in a VMware environment. VMware vMotion enables the live migration of a running FortiGate-VM from one physical server to another with zero downtime, continuous service availability, and complete transaction integrity. It also provides transparency to users.

In VM environments that do not support broadcast communication, you can set up a unicast HA heartbeat when configuring HA. Setting up a unicast HA heartbeat consists of enabling the feature and adding a peer IP address. The peer IP address is the IP address of the HA heartbeat interface of the other FortiGate-VM in the HA cluster.



The following depicts the network topology for this sample deployment. In this sample deployment, there are two hosts, Host 82 (10.6.30.82) and Host 83 (10.6.30.83), which are members of Cluster 1 in the DataCenter 1. DataCenter 1 is managed by the vCenter server (10.6.30.81).



The following prerequisites must be met for this configuration:

- The vCenter server has been set up and the data center and cluster have been created.
- Host 82 and Host 83 are part of the cluster.
- A Gigabit Ethernet network interface card with a VMkernel port enabled for vMotion exists on both ESXi hosts.
- Two FortiGate-VM nodes, FGT-HA-1@Host-82 and FGT-HA-2@Host-83 are set up and factory reset. In this example, FGT-HA-1 is the primary side on Host 82, while FGT-HA-2 is the primary side on Host 83. HA is in sync.

To set up FortiGate-VM HA for a VMware vMotion environment:

1. Log into the vSphere web client.
2. Verify the current location of FGT-HA-1:
 - a. Go to FGT-HA-1.
 - b. On the *Summary* tab, check the *Host*. In this example, the host is currently Host 82 (10.6.30.82).
3. Repeat step 2 for FGT-HA-2. For FGT-HA2, the host should be Host 83 (10.6.30.83).
4. Log into FortiOS on FGT-HA-1 and FGT-HA-2 and run the following commands in the CLI:
 - a. Run the following commands on FGT-HA-1:

```
config system interface
  edit "port3"
    set ip 192.168.40.91 255.255.255.0
    set allowaccess ping https ssh snmp http telnet
  next
  edit "port4"
    set ip 10.6.30.91 255.255.255.0
    set allowaccess ping https ssh snmp http telnet
  next
end

config system ha
  set group-name "FGT-VM-HA"
  set mode a-p
  set hbdev "port3" 50
  set session-pickup enable
  set ha-mgmt-status enable
  config ha-mgmt-interfaces
    edit 1
      set interface "port4"
```

```
        set gateway 10.6.30.254
    next
end
set unicast-hb enable
set unicast-hb-peerip 192.168.40.92
end

config router static
    edit 1
        set gateway 172.16.200.254
        set device "port1"
    next
end

config firewall policy
    edit 1
        set srcintf "port2"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end
```

b. Run the following commands on FGT-HA-2:

```
config system interface
    edit "port3"
        set ip 192.168.40.92 255.255.255.0
        set allowaccess ping https ssh snmp http telnet
    next
    edit "port4"
        set ip 10.6.30.92 255.255.255.0
        set allowaccess ping https ssh snmp http telnet
    next
end

config system ha
    set group-name "FGT-VM-HA"
    set mode a-p
    set hbdev "port3" 50
    set session-pickup enable
    set ha-mgmt-status enable
    config ha-mgmt-interfaces
        edit 1
            set interface "port4"
            set gateway 10.6.30.254
        next
    end
    set unicast-hb enable
```

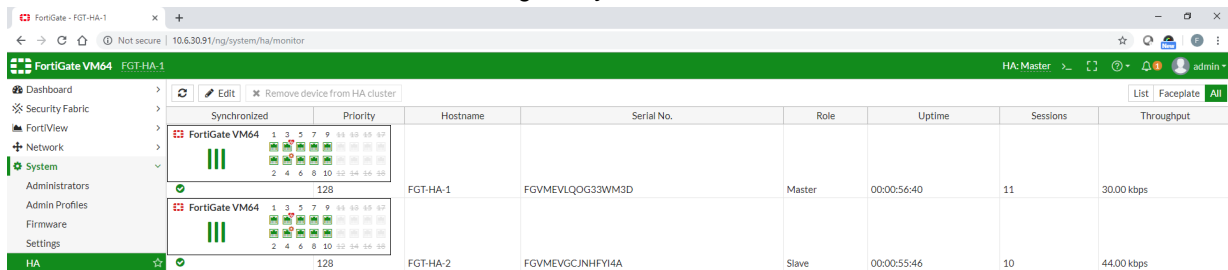
```

set unicast-hb-peerip 192.168.40.91
end

```

5. Check the HA status:

- a. To check the HA status in the GUI, in FortiOS, go to *System > HA*.



- b. To check the HA status in the CLI, run the `get system ha status` command. The output should be as follows. You should expect both FGT-HA-1 and FGT-HA-2 to have an in-sync configuration status.

```

FGT-HA-1 # get system ha status
HA Health Status: OK
Model: FortiGate-VM64
Mode: HA A-P
Group: 0
Debug: 0
Cluster Uptime: 0 days 1:35:12
Cluster state change time: 2019-05-16 14:53:05
Master selected using:
  <2019/05/16 14:53:05> FGVMEVLQOG33WM3D is selected as the master because it
  has the largest value of uptime.
  <2019/05/16 14:45:53> FGVMEVLQOG33WM3D is selected as the master because
  it's the only member in the cluster.
ses_pickup: enable, ses_pickup_delay=disable
override: disable
unicast_hb: peerip=192.168.40.92, myip=192.168.40.91, hasync_port='port3'
Configuration Status:
  FGVMEVLQOG33WM3D(updated 2 seconds ago): in-sync
  FGVMEVGCJNHFYI4A(updated 0 seconds ago): in-sync

```

- 6. Before initiating the migration, open the CLI for both FGT-HA-1 and FGT-HA-2 to check on traffic during the migration. During the migration, you can enter the `diag sniffer packet any 'icmp and host 8.8.8.8'` command to check if traffic is stable. If no traffic is lost during migration and the FortiGate-VM SSH session does not break, the output resembles the following:

```

FGT-HA-1 # diag sniffer packet any 'icmp and host 8.8.8.8'
interfaces=[any]
filters=[icmp and host 8.8.8.8]
27.103356 10.1.100.22 -> 8.8.8.8: icmp: echo request
27.103423 172.16.200.91 -> 8.8.8.8: icmp: echo request
27.108160 8.8.8.8 -> 172.16.200.91: icmp: echo reply
27.108167 8.8.8.8 -> 10.1.100.22: icmp: echo reply
28.104695 10.1.100.22 -> 8.8.8.8: icmp: echo request
28.104699 172.16.200.91 -> 8.8.8.8: icmp: echo request
28.109381 8.8.8.8 -> 172.16.200.91: icmp: echo reply
28.109385 8.8.8.8 -> 10.1.100.22: icmp: echo reply
29.105058 10.1.100.22 -> 8.8.8.8: icmp: echo request
29.105069 172.16.200.91 -> 8.8.8.8: icmp: echo request
29.109682 8.8.8.8 -> 172.16.200.91: icmp: echo reply
29.109693 8.8.8.8 -> 10.1.100.22: icmp: echo reply

```

- 7. Migrate FGT-HA-1, the primary node, from Host 82 to Host 83, then migrate it from Host 83 back to Host 82. Refer to [vMotion in a VMware ESXi environment on page 39](#) for migration details.

8. Migrate FGT-HA-2, the secondary node, from Host 83 to Host 82, then migrate it from Host 82 back to Host 83. Again, refer to [vMotion in a VMware ESXi environment on page 39](#) for migration details.

Enhancing FortiGate-VM Performance with DPDK and vNP offloading

DPDK and vNP enhance FortiGate-VM performance by offloading part of packet processing to user space while using a kernel bypass solution within the operating system. You must enable and configure DPDK with FortiOS CLI commands.

FortiOS 6.4 supports DPDK for VMware ESXi environments.

FortiOS 6.4.1 supports IPv6.

The current DPDK+vNP offloading-capable version of FortiOS only supports FortiGate instances with two or more vCPUs. Minimum required RAM sizes differ from those on regular FortiGate-VM models without offloading. It is recommended to allocate as much RAM size as the licensed limit for maximum performance, as shown. See [the 5.6 document](#) for minimum size reference. FortiOS 6.2.2 and later versions do not restrict RAM size by license. Therefore, you can allocate as much memory as desired on 6.4-based DPDK-enabled FortiGate-VMs:

| Model name | RAM size (licensed limit) |
|------------|---------------------------|
| FG-VM02(v) | No restriction |
| FG-VM04(v) | No restriction |
| FG-VM08(v) | No restriction |
| FG-VM16(v) | No restriction |
| FG-VM32(v) | No restriction |

You can enable DPDK up to 64 vCPUs.



The current build does not support encrypted traffic. Support is planned for future versions. It is recommended to disable the DPDK option using the CLI or adopt regular FortiGate-VM builds when using IPsec and SSL VPN features.



Enabling DPDK+vNP offloading may result in fewer concurrent sessions when under high load than when DPDK+vNP offloading is not enabled and the same FortiGate-VM license is used.

Enabling DPDK+vNP offloading using the FortiOS CLI

Provided that you obtained a DPDK+vNP offloading-capable FortiOS build, the following provides the configuration to enable the capability:

- [DPDK global settings on page 48](#)
- [DPDK CPU settings on page 50](#)
- [DPDK diagnostic commands on page 51](#)

FortiOS 6.2.3 and later versions support SNMP to poll DPDK-related status. For details, see the corresponding MIB file that Fortinet provides.

DPDK global settings

To enable DPDK operations for the FortiGate-VM:

1. In the FortiOS CLI, enter the following commands to enable DPDK operation:

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

2. The CLI displays the following message:

```
Status and interface changes will trigger system reboot and take effect after the
reboot.
```

```
Do you want to continue? (y/n)
```

```
Press y to reboot the device.
```



Before system reboot, you must check if other DPDK settings are configured properly. You must enable at least one network interface for DPDK. The example enables port1. You can enable other interfaces as desired. If you do not set an interface, a prompt displays and the change is discarded. See [To enable a network interface to run DPDK operation: on page 49](#).

To enable DPDK multiqueue mode:

Enabling multiqueue at network RX/TX helps DPDK better balance the workload onto multiple engines.

1. In the FortiOS CLI, enter the following commands to enable DPDK operation:

```
config dpdk global
  set multiqueue enable
end
```

2. The CLI displays the following message:

```
Multiqueue change will trigger IPS restart and will take effect after the restart.
Traffic may be interrupted briefly.
```

```
Do you want to continue? (y/n)
```

```
Press y to reboot IPS engine.
```

To set the percentage of main memory allocated to DPDK huge pages and packet buffer pool:

You can configure the amount of main memory (as a percentage) allocated to huge pages, which are dedicated to DPDK use. You can also configure the amount of main memory (as a percentage) allocated to the DPDK packet buffer pool.

Enter the following commands to set these amounts:

```
config dpdk global
  set hugepage-percentage [X]
  set mbufpool-percentage [Y]
end
```

Changing `mbufpool-percentage` requires IPS engine to restart (no reboot).



Huge page memory is mounted at system startup and remains mounted as long as the FortiGate-VM is running. Packet buffer pool memory is drawn from huge pages. Therefore, the packet buffer pool amount (Y) must not exceed the huge pages amount (X).

In practice, it is mandated that Y is lesser than or equal to X - 5 to leave 5% memory overhead for other DPDK data structures. The range of X is between 10 and 50, and the range of Y is between 5 and 45.



Setting X too high may force FortiOS to enter conserve mode. Setting X too low may result in insufficient memory for DPDK operation and failure of initialization.



During FortiOS DPDK Helper environment initialization, RTE memory zones are drawn from huge memory pages. The system tries to reserve continuous memory chunks for these memory zones with best effort. Therefore, the amount of huge page memory is slightly larger than the amount of memory that RTE memory zones use. To gain insight into how RTE memory zones reserve memory spaces, run the `diagnose dpdk statistics show memory` command.

To enable a network interface to run DPDK operation:

You must enable at least one network interface to run DPDK operation.

```
config dpdk global
  set interface "portX" "portY"
end
```



You must enable at least one network interface for DPDK. Otherwise, DPDK early initialization during system startup fails and falls back to a disabled state. In this example, if there are two network interfaces that you intend to use, you can specify `set interface port1 port2`.



Enabling DPDK is only available for physical network interfaces.

To enable DPDK monitor engine:

Enabling DPDK monitor engine is optional.

1. In the FortiOS CLI, enter the following commands to enable DPDK monitor engine:

```
config dpdk global
  set sleep-on-idle enable
end
```

2. The CLI displays the following message:

```
sleep-on-idle change will trigger IPS restart and will take effect after the restart.
Traffic may be interrupted briefly.
```

```
Do you want to continue? (y/n)
```

Press `y` to reboot IPS engine.

By default, DPDK monitor engine is disabled. When enabled, only one DPDK engine polls DPDK-enabled interfaces. When packets arrive, corresponding DPDK entries are activated. This helps when services other than firewall or IPS engine, such as antivirus, WAD, or web filter, are running and performance degradation is observed while DPDK performance statistics show that DPDK engines are not fully used. Latency may increase due to the time needed to activate the proper DPDK engines by the monitor engine.

To enable elastic buffer (temporary memory buffer):

Enabling elastic buffer is optional.

1. In the FortiOS CLI, enter the following commands to enable elastic memory buffer:

```
config dpdk global
    set elasticbuffer enable
end
```

2. The CLI displays the following message:

```
elasticbuffer change will trigger IPS restart and will take effect after the restart.
Traffic may be interrupted briefly.
Do you want to continue? (y/n)
Press y to reboot IPS engine.
```

By default, elastic buffer is disabled. When enabled, an elastic buffer takes effect to store packets in case of traffic burst. The feature helps to reduce packet drops when received packets peak under system overload by storing packets in the buffer and processing them afterward. This feature is experimental.

To enable per-session accounting:

Enabling per-session accounting is optional.

1. In the FortiOS CLI, enter the following commands to enable per session accounting:

```
config dpdk global
    set per-session-accounting enable|disable|traffic-log-only
end
```

2. The CLI displays the following message:

```
per-session-accounting change will trigger IPS restart and will take effect after the
restart. Traffic may be interrupted briefly.
Do you want to continue? (y/n)
Press y to reboot IPS engine.
```

By default, per-session accounting is configured only for traffic logs, which results in per-session accounting being enabled when you enable traffic logging in a policy.

Per-session accounting is a logging feature that allows FortiOS to report the correct bytes per packet numbers per session for sessions offloaded to a vNP process. This information appears in traffic log messages, FortiView, and `diagnose` commands. Per-session accounting can affect vNP offloading performance. You should only enable per-session accounting if you need the accounting information. A similar feature is available for [physical FortiGate NP6 processors](#).

DPDK CPU settings

On the FortiGate-VM, a DPDK engine is attached to an IPS engine, which shares the same process and is mapped to a CPU. A processing pipeline of four stages handles a packet from RX to TX:

1. DPDK RX
2. vNP
3. IPS
4. DPDK TX

You can freely determine the CPUs enabled for each pipeline stage by running the following commands:

```
config dpdk cpus
    set [X] [Y]
end
```

Here X is one of the pipeline stages: rx-cpus, vnp-cpus, ips-cpus, and tx-cpus.

Y is a string expression of CPU IDs, which contains comma-delimited individual CPU IDs or ranges of CPU IDs separated by a dash.

The example enables CPUs 0, 2, 4, 6, 7, 8, 9, 10, and 15 to run the vNP pipeline stage:

```
set vnp-cpus 0,2,4,6-10,15
```

In FortiOS 6.4.1, Y can also be a special token string `all`, which means to use all available CPUs to run that pipeline stage. The system automatically determines the number of available CPUs. `all` is the default value of each pipeline stage's CPU setting.

The example uses all available CPUs to run the IPS pipeline stage:

```
set ips-cpus all
```



You must enable at least one CPU for each pipeline stage. Otherwise, DPDK early initialization fails.

DPDK diagnostic commands

To view DPDK-related logs:

Enter the following command to view DPDK-related logs:

```
diagnose dpdk log show [log type]
```

Currently, FortiOS provides two DPDK-related logs:

| Log | Records kept |
|------------|---|
| early-init | DPDK's early initialization procedure during system startup |
| fdh | Warnings and errors met during the initialization of FortiOS DPDK helper (FDH), i.e. DPDK engines |

Ensure that you double-check whether DPDK early initialization was successful. If successful, the end of the early-init log shows the following:

```
DPDK sanity test passed
```

If the DPDK early initialization was unsuccessful, refer to [DPDK global settings on page 48](#) to see if the DPDK-related options were properly set.

The early init-log also keeps records of last-edited DPDK configuration, enabled CPUs/ports, binding/unbinding of drivers, device PCI info, and so on.

To view DPDK-related statistics:

Enter the following command to view DPDK-related statistics:

```
diagnose dpdk statistics show [stats type]
```

Currently, FortiOS provides four types of DPDK-related statistics:

- `engine`: provides per-DPDK engine statistics
- `port`: provides per-DPDK port statistics
- `vnp`: provides per-vNP engine statistics
- `memory`: provides a quick view of memory size reserved by each RTE memory zone

To reset statistics, enter the following command:

```
diagnose dpdk statistics clear all
```

This command resets engine and port statistics to zeroes, but does not affect vNP and memory statistics.

To check if traffic is properly forwarded, load-balanced, and offloaded to fast path:

A useful way to check whether traffic is properly forwarded is to check the port statistics. This shows the number of received/transmitted/dropped packets in each DPDK-enabled port.

```

-----
FortiOS DPDK Helper Port Stats
-----

```

| | Total | port2 |
|----------------------------|-------|-------|
| ----- DPDK RX Stage ----- | | |
| dpdkrx_rx_pkts: | 0 | 0 |
| ----- DPDK TX Stage ----- | | |
| dpdktx_tx_pkts: | 0 | 0 |
| dpdktx_drop_pkts: | 0 | 0 |
| dpdktx_drop_oversized_pkt: | 0 | 0 |

Checking engine statistics is helpful in understanding how traffic is load-balanced among DPDK engines at each pipeline stage.

```

-----
FortiOS DPDK Helper Engine Stats
-----
Total
CPU ID:
----- DPDK RX Stage -----
dpdkrx_rx_pkts:          2
dpdkrx_tx_pkts:          2
dpdkrx_drop_pkts:        0

----- VNP Stage -----
vnp_rx_pkts:             2
vnp_tx_pkts:             1
vnp_tx_drop_pkts:        0
vnp_to_ips_pkts:         0
vnp_to_ips_drop_pkts:    0

----- IPS Stage -----
ips_rx_pkts:             0
ips_tx_pkts:             0
ips_drop_pkts:           0
ips_rej_pkts:            0

----- DPDK TX Stage -----
dpdktx_rx_pkts:          1
dpdktx_tx_pkts:          1
dpdktx_drop_pkts:        0
dpdktx_drop_oversized_pkt: 0

CPU ID:          Engine 0      Engine 1      Engine 2      Engine 3
----- DPDK RX Stage -----
dpdkrx_rx_pkts:          2          0          0          0
dpdkrx_tx_pkts:          2          0          0          0
dpdkrx_drop_pkts:        0          0          0          0

----- VNP Stage -----
vnp_rx_pkts:             0          0          0          0
vnp_tx_pkts:             0          0          0          0
vnp_tx_drop_pkts:        0          0          0          0
vnp_to_ips_tx_pkts:      0          0          0          0
vnp_to_ips_tx_drop_pkts: 0          0          0          0

----- IPS Stage -----
ips_rx_pkts:             0          0          0          0
ips_tx_pkts:             0          0          0          0
ips_drop_pkts:           0          0          0          0
ips_rej_pkts:            0          0          0          0

----- DPDK TX Stage -----
dpdktx_rx_pkts:          0          0          0          1
dpdktx_tx_pkts:          0          0          0          1
dpdktx_drop_pkts:        0          0          0          0
dpdktx_drop_oversized_pkt: 0          0          0          0
    
```

Checking vNP statistics provides insights to how traffic is offloaded from the slow path (traversing the kernel) to the fast path (firewall and IPS operations quickly processed by the vNP engine). In particular, observe the number of session search engine (SSE) entries pushed from kernel or IPS to vNP engine, shown bolded (**ctr_sse_entries**). The number of packets going through the SSE fast path is also important and is bolded (**ctr_fw_and_ips_fpath**).

```

-----
FortiOS DPDK Helper VNP Stats
-----
CPU ID:
----- VNP Internal -----
ctr_ctx_alloc: 2
ctr_ctx_alloc_fail: 0
ctr_ctx_free: 2
ctr_to_kernel: 2
ctr_from_kernel: 1
ctr_sse: 0
ctr_sse_cmd: 0
ctr_sse_delmiss: 0
ctr_sse_msg: 0
ctr_sse_pruned: 0
ctr_fw_and_ips_fpath: 0
ctr_sse_entries: 0
err_sse_batch_size: 0
err_sse_unknown_cmd: 0
err_sse_full: 0
err_sse_tbl_alloc_fail: 0
err_sse_inv_oid: 0
err_fp_no_act: 0
drop_inv_port: 0
drop_inv_ip_cksum: 0
drop_inv_tcp_cksum: 0
drop_inv_udp_cksum: 0
drop_oversized_pkt: 0
-----
CPU ID: Engine 0 Engine 1 Engine 2 Engine 3
----- VNP Internal -----
ctr_ctx_alloc: 0 0 0 0
ctr_ctx_alloc_fail: 0 0 0 0
ctr_ctx_free: 0 0 0 0
ctr_to_kernel: 0 0 0 0
ctr_from_kernel: 0 0 0 0
ctr_sse: 0 0 0 0
ctr_sse_cmd: 0 0 0 0
ctr_sse_delmiss: 0 0 0 0
ctr_sse_msg: 0 0 0 0
ctr_sse_pruned: 0 0 0 0
ctr_fw_and_ips_fpath: 0 0 0 0
ctr_sse_entries: 0 0 0 0
err_sse_batch_size: 0 0 0 0
err_sse_unknown_cmd: 0 0 0 0
err_sse_full: 0 0 0 0
err_sse_tbl_alloc_fail: 0 0 0 0
err_sse_inv_oid: 0 0 0 0
err_fp_no_act: 0 0 0 0
drop_inv_port: 0 0 0 0
drop_inv_ip_cksum: 0 0 0 0
drop_inv_tcp_cksum: 0 0 0 0
drop_inv_udp_cksum: 0 0 0 0
drop_oversized_pkt: 0 0 0 0
-----

```

To see DPDK CPU settings, run the following commands. In this case, N is the number of CPUs that the FortiGate-VM uses.

```

show dpdk cpus
config dpdk cpus
set rx-cpus "0-N"
set vnp-cpus "0-N"
set ips-cpus "0-N"
set tx-cpus "0-N"
end

```

To view DPDK performance:

The `diagnose dpdk performance show` command provides near real-time performance of each DPDK engine, in particular, the CPU usage. The system provides the following response:

```

-----
CPU usages
-----
2018:12:10 15:17:52      rx:      Engine 0      Engine 1      Engine 2      Engine 3
2018:12:10 15:17:52      vnp:      0.0           0.0           0.0           0.0
2018:12:10 15:17:52      ips:      0.0           0.0           0.0           0.0
2018:12:10 15:17:52      tx:      0.0           0.0           0.0           0.0
2018:12:10 15:17:52      idle:    100.0        100.0        100.0        100.0
-----

2018:12:10 15:17:52      rx:      Engine 4      Engine 5      Engine 6      Engine 7
2018:12:10 15:17:52      vnp:      0.0           0.0           0.0           0.0
2018:12:10 15:17:52      ips:      0.0           0.0           0.0           0.0
2018:12:10 15:17:52      tx:      0.0           0.0           0.0           0.0
2018:12:10 15:17:52      idle:    100.0        100.0        100.0        100.0
-----

2018:12:10 15:17:52      rx:      Engine 8      Engine 9      Engine 10     Engine 11
2018:12:10 15:17:52      vnp:      0.0           0.0           0.0           0.0
2018:12:10 15:17:52      ips:      0.0           0.0           0.0           0.0
2018:12:10 15:17:52      tx:      0.0           0.0           0.0           0.0
2018:12:10 15:17:52      idle:    100.0        100.0        100.0        100.0
-----

2018:12:10 15:17:52      rx:      Engine 12     Engine 13     Engine 14     Engine 15
2018:12:10 15:17:52      vnp:      0.0           0.0           0.0           0.0
2018:12:10 15:17:52      ips:      0.0           0.0           0.0           0.0
2018:12:10 15:17:52      tx:      0.0           0.0           0.0           0.0
2018:12:10 15:17:52      idle:    100.0        100.0        100.0        100.0
-----

```

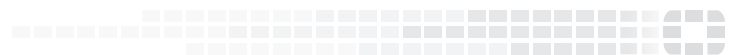
This provides better insight into how many CPUs to allocate to each pipeline stage.

Change log

| Date | Change Description |
|------------|--|
| 2020-03-31 | Initial release. |
| 2020-04-08 | Updated Public compared to private clouds on page 7. |
| 2020-04-15 | Added Compatibility for VM hardware versions on page 11. Updated Deployment package contents on page 10. |
| 2020-04-23 | Updated Deploying the FortiGate-VM on page 12. |
| 2020-04-23 | Updated FortiGate-VM evaluation license on page 6. |
| 2020-05-05 | Updated Registering the FortiGate-VM on page 9. |
| 2020-06-04 | Updated Enhancing FortiGate-VM Performance with DPDK and vNP offloading on page 47 and DPDK CPU settings on page 50. |
| 2021-02-17 | Updated SDN connector integration with VMware ESXi on page 31. |
| 2021-02-24 | Updated FortiGate-VM evaluation license on page 6. |
| 2021-10-06 | Added Setting up FortiGate-VM HA for a VMware vMotion environment on page 42. |



FORTINET[®]



Copyright© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.