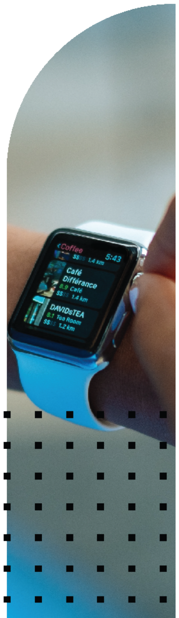
# Xen Administration Guide

## FortiOS 7.0



**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/support-and-training/training.html

**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

March 30, 2021
FortiOS 7.0 Xen Administration Guide
01-700-705051-20210330

# TABLE OF CONTENTS

# About FortiGate-VM on Xen

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 Xen environment.

## FortiGate-VM models and licensing

FortiGate-VM offers perpetual licensing (normal series and V-series) and annual subscription licensing (S-series, available starting Q4 2019). 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:<br>• Only FortiCare<br>• UTM<br>• Enterprise<br>• 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. |

| | Normal series | V-series | S-series |
|---|---|---|---|
| **vCPU number downgrade during contracted term** | Not supported. | | |
| **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 Xen virtual platform, you have addressed the following requirements:

## Virtual environment

You have installed the Xen 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.

## Management software

If you plan to use the GUI to manage the Xen server, make sure that the appropriate management software for the platform is installed:

| Platform | Management software |
|---|---|
| Open Xen | Virtual Machine Manager |
| Citrix Xen Server | XenCenter |

## 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 22.

## 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

## OpenXen

Unlike some other FortiGate-VM deployments, Open Xen does not have you configure the resources of the VM before the installation process. The configuration of the resources is done as part of the deployment.

Go to Deploying FortiGate-VM on OpenXen.

## Citrix Xen

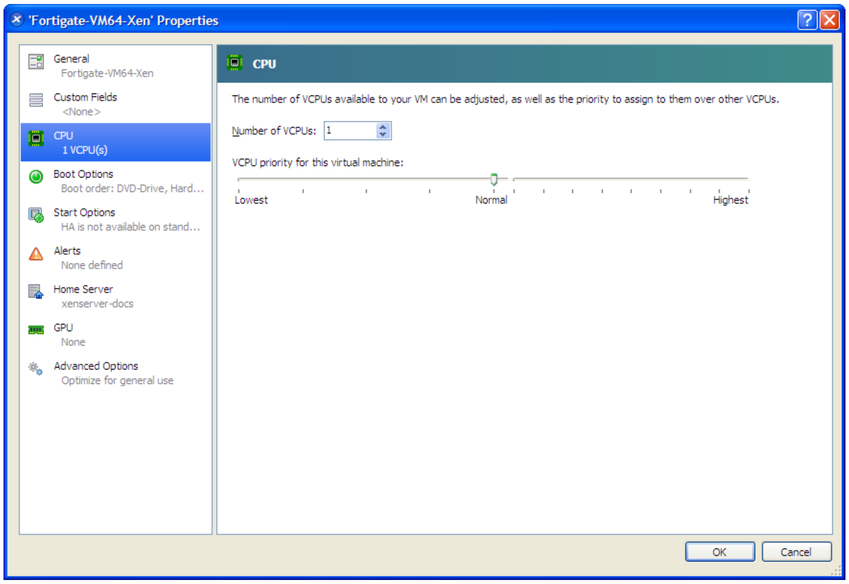
### To access VM settings:

1. Open XenCenter.
2. Select your FortiGate-VM in the left pane.
   The tabs in the right pane provide access to the virtual hardware configuration. The Console tab provides access to the FortiGate console.

## CPUs

### To configure the number of CPUs:

1. In the XenCenter left pane, right-click the FortiGate-VM and select *Properties*. The *Properties* window opens.
2. In the left pane, select *CPU*.



'Fortigate-VM64-Xen' Properties

General: Fortigate-VM64-Xen
Custom Fields: <None>
CPU: 1 VCPU(s)
Boot Options: Boot order: DVD-Drive, Hard...
Start Options: HA is not available on stand...
Alerts: None defined
Home Server: xenserver-docs
GPU: None
Advanced Options: Optimize for general use

CPU

The number of VCPUs available to your VM can be adjusted, as well as the priority to assign to them over other VCPUs.

Number of VCPUs: 1

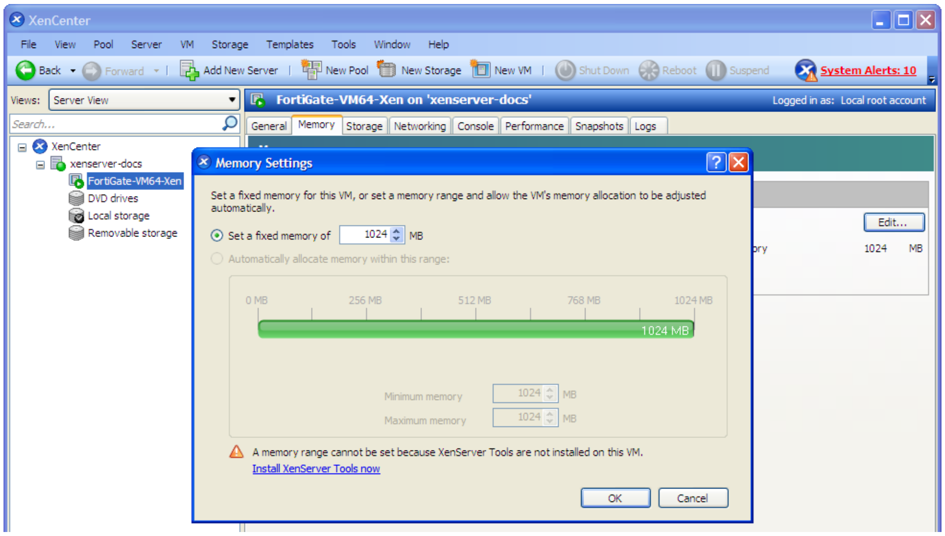
VCPU priority for this virtual machine: Normal

3. Adjust *Number of CPUs* and then select *OK*. XenCenter displays a warning if you select more CPUs than the Xen host computer contains. Such a configuration may reduce performance.

## Memory

### To configure memory:

1. In the XenCenter left pane, select the FortiGate-VM.
2. In the right pane, select the *Memory* tab.
3. Select *Edit*, modify the value in the the *Set a fixed memory of* field and select *OK*.



Memory Settings

Set a fixed memory for this VM, or set a memory range and allow the VM's memory allocation to be adjusted automatically.

● Set a fixed memory of 1024 MB

○ Automatically allocate memory within this range:

Minimum memory 1024 MB

Maximum memory 1024 MB

A memory range cannot be set because XenServer Tools are not installed on this VM.

Install XenServer Tools now

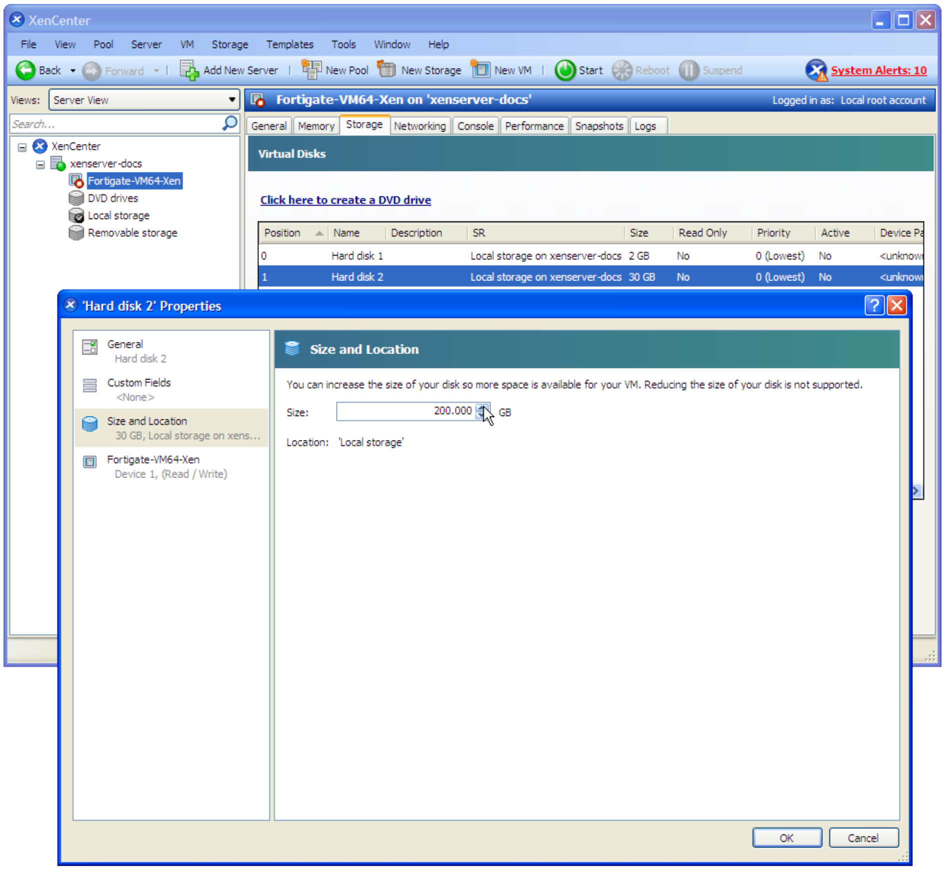
## Disk storage

By default the FortiGate-VM data disk size is 30 GB. You probably want to increase this. You must resize the disk before you start the VM for the first time.

### To resize the FortiGate data disk

1. In the XenCenter left pane, select the FortiGate-VM.
2. Select the *Storage* tab. Select *Hard disk 2* (the 30GB drive), then select *Properties*. The *‘Hard disk 2’ Properties* window opens.

3. Select *Size and Location*. Adjust *Size* and select *OK*.


XenCenter
File View Pool Server VM Storage Templates Tools Window Help
Back Forward Add New Server New Pool New Storage New VM Start Reboot Suspend
System Alerts: 10
Views: Server View
Search...
XenCenter
xenserver-docs
Fortigate-VM64-Xen
DVD drives
Local storage
Removable storage
Fortigate-VM64-Xen on 'xenserver-docs'
Logged in as: Local root account
General Memory Storage Networking Console Performance Snapshots Logs
Virtual Disks
Click here to create a DVD drive
'Hard disk 2' Properties
General
Hard disk 2
Custom Fields
<None>
Size and Location
30 GB, Local storage on xens...
Fortigate-VM64-Xen
Device 1, (Read / Write)
Size and Location
OK
Cancel

| Position | Name | Description | SR | Size | Read Only | Priority | Active | Device Pa |
|---|---|---|---|---|---|---|---|---|
| 0 | Hard disk 1 | | Local storage on xenserver-docs | 2 GB | No | 0 (Lowest) | No | <unknow |
| 1 | Hard disk 2 | | Local storage on xenserver-docs | 30 GB | No | 0 (Lowest) | No | <unknow |

You can increase the size of your disk so more space is available for your VM. Reducing the size of your disk is not supported.

Size: 200.000 GB

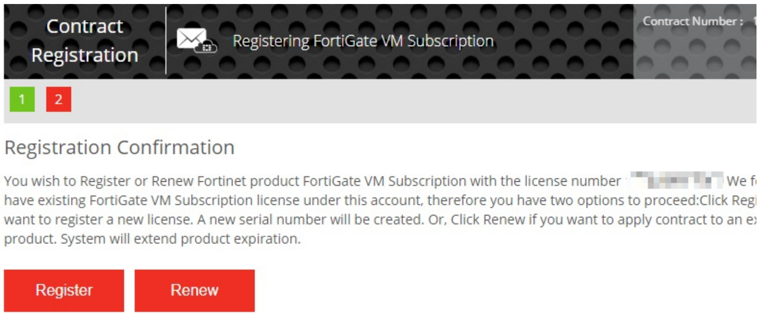
Location: 'Local storage'

## 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 f
have existing FortiGate VM Subscription license under this account, therefore you have two options to proceed:Click Regi
want to register a new license. A new serial number will be created. Or, Click Renew if you want to apply contract to an e
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 21 or Validating the FortiGate-VM license with FortiManager on page 22 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 Xen.
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

## OpenXen

The *FORTINET.out.OpenXen.zip file contains only fortios.qcow2, the FortiGate-VM system hard disk in qcow2 format. You must manually:

- Create a 32GB log disk
- Specify the virtual hardware settings

## Citrix XenServer

The *FORTINET.out.CitrixXen.zip file contains:

- fortios.vhd: the FortiGate-VM system hard disk in VHD format
- fortios.xva: binary file containing virtual hardware configuration settings
- in the ovf folder:
  - FortiGate-VM64.ovf: Open Virtualization Format (OVF) template file, containing virtual hardware settings for Xen
  - fortios.vmdk: the FortiGate-VM system hard disk in VMDK format
  - datadrive.vmdk: the FortiGate-VM log disk in VMDK format

The ovf folder and its contents is an alternative method of installation to the .xva and VHD disk image.

# Deployment

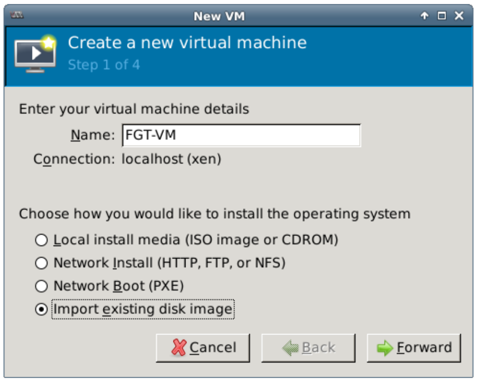
Before you deploy a FortiGate-VM, ensure that you have met the requirements described in Preparing for deployment on page 7 and that the correct deployment package is extracted to a folder on the local computer (see Downloading the FortiGate-VM deployment package on page 11).

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 on OpenXen

**To create the FortiGate-VM:**

1. Launch Virtual Machine Manager (virt-manager) on your OpenXen host server.
2. In the toolbar, select *Create a new virtual machine*.



New VM

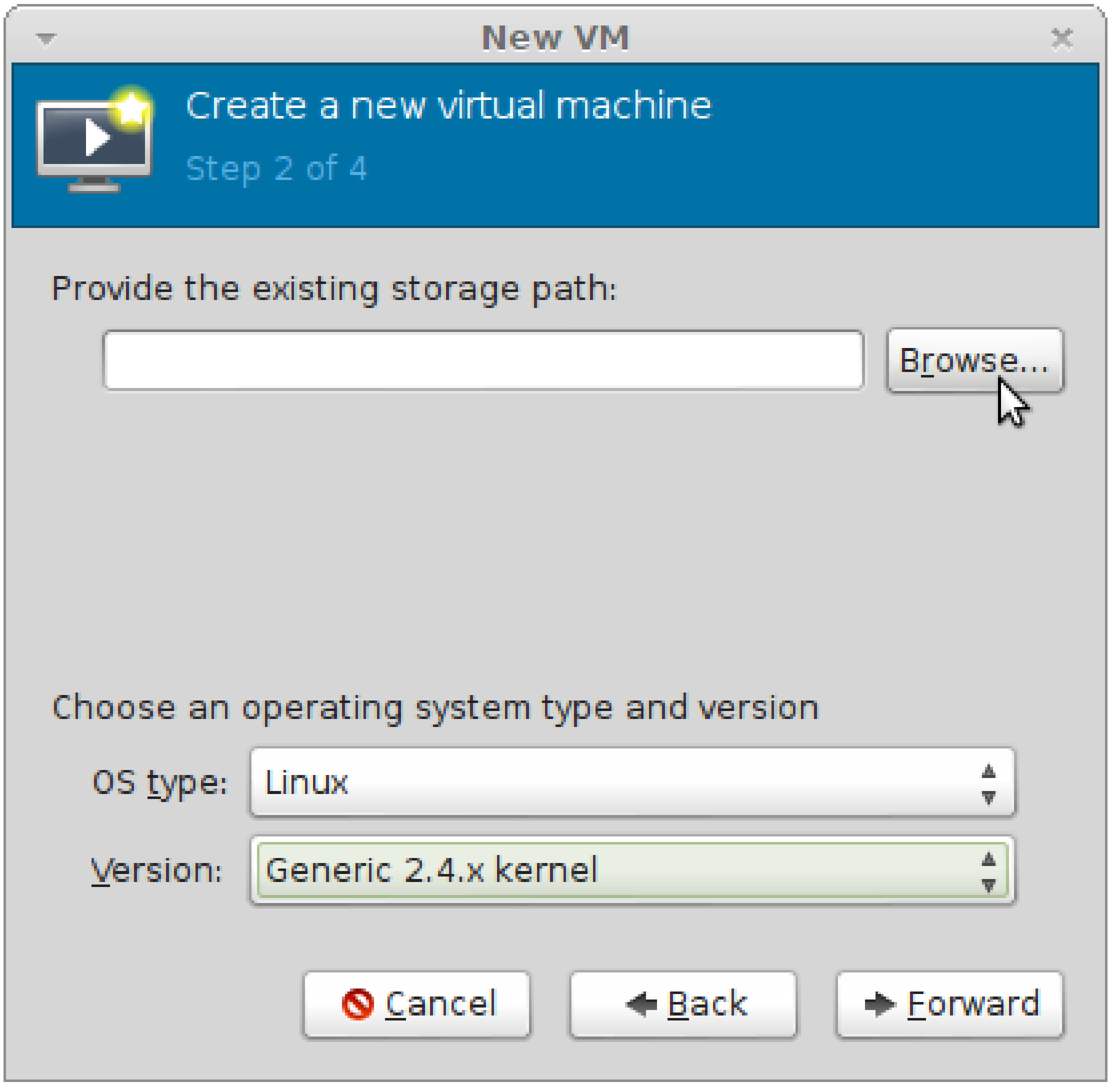
Create a new virtual machine
Step 1 of 4

Enter your virtual machine details
Name: FGT-VM
Connection: localhost (xen)

Choose how you would like to install the operating system
○ Local install media (ISO image or CDROM)
○ Network Install (HTTP, FTP, or NFS)
○ Network Boot (PXE)
● Import existing disk image

3. Enter a *Name* for the VM, FGT-VM for example.
4. Ensure that *Connection* is localhost. (This is the default.)
5. Select *Import existing disk image*.
6. Select *Forward*.

7. In *OS Type* select *Linux*.



New VM

Create a new virtual machine

Step 2 of 4

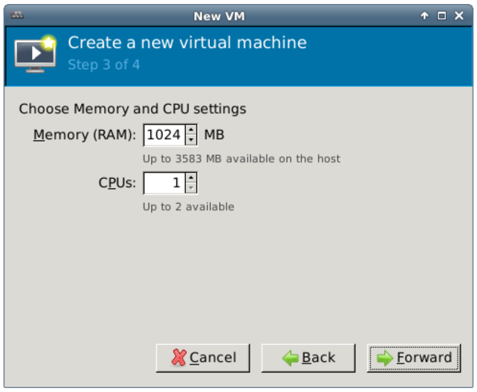
Provide the existing storage path:

Choose an operating system type and version

OS type: Linux

Version: Generic 2.4.x kernel

8. In *Version*, select *Generic 2.4.x.kernel*.
9. Select *Browse*. The *Locate or create storage volume* window opens.
10. Select *Browse Local,* and locate the fortios.qcow2 disk image file.
11. Select fortios.qcow2 and select *Choose Volume*.
12. Select *Forward*.
13. Specify the amount of memory and number of CPUs to allocate to this VM. The amounts must not exceed your license limits.



New VM

Create a new virtual machine

Step 3 of 4

Choose Memory and CPU settings

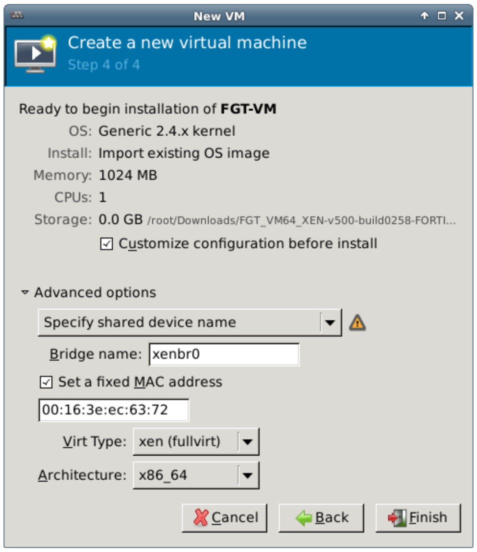
Memory (RAM): 1024 MB

Up to 3583 MB available on the host

CPUs: 1

Up to 2 available

14. Select *Forward*.
15. Select *Customize configuration before install*. This enables you to make some hardware configuration changes before VM creation is started.



New VM

Create a new virtual machine

Step 4 of 4

Ready to begin installation of **FGT-VM**

OS: Generic 2.4.x kernel

Install: Import existing OS image

Memory: 1024 MB

CPUs: 1

Storage: 0.0 GB /root/Downloads/FGT_VM64_XEN-v500-build0258-FORTI...

☑ Customize configuration before install

Advanced options

Specify shared device name

Bridge name: xenbr0

☑ Set a fixed MAC address

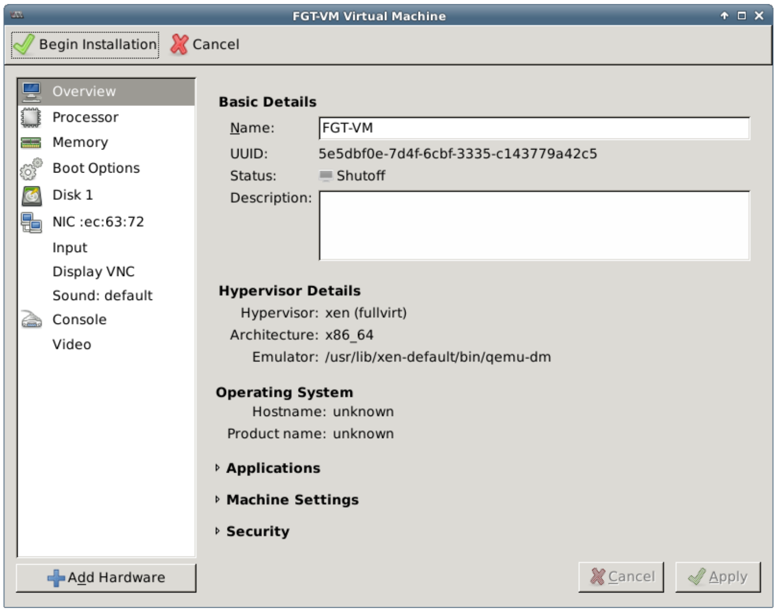
00:16:3e:ec:63:72

Virt Type: xen (fullvirt)

Architecture: x86_64

16. Expand *Advanced options*. A new VM includes one network adapter by default. Select *Specify shared device name* and enter the name of the bridge interface on the OpenXen host. Optionally, set a specific MAC address for the virtual network interface. *Virt Type* and *Architecture* are set by default and should be correct.

17. Select *Finish*. The VM hardware configuration window opens.



Basic Details
Name: FGT-VM
UUID: 5e5dbf0e-7d4f-6cbf-3335-c143779a42c5
Status: Shutoff
Description:

Hypervisor Details
Hypervisor: xen (fullvirt)
Architecture: x86_64
Emulator: /usr/lib/xen-default/bin/qemu-dm

Operating System
Hostname: unknown
Product name: unknown

You can use this window to add hardware such as network interfaces and disk drives.

18. Select *Add Hardware*. In the *Add Hardware* window select *Storage*.
19. Select *Create a disk image on the computer's harddrive* and set the size to 30GB.

If you know your environment will expand in the future, it is recommended to increase the hard disk size beyond 30GB. The VM license limit is 2TB.

20. Enter:

| | |
|---|---|
| **Device type** | Virtio disk |
| **Cache mode** | Default |
| **Storage format** | raw |

21. Select *Network* to configure the network interfaces. The *Device type* must be *Virtio*.
A new virtual machine includes one network adapter by default. You can add more through the Add Hardware window. FortiGate-VM requires four network adapters. You can configure network adapters to connect to a virtual switch or to network adapters on the host computer.
22. Select *Finish*.
23. Select *Begin Installation*. After the installation completes successfully, the VM starts and the console window opens.

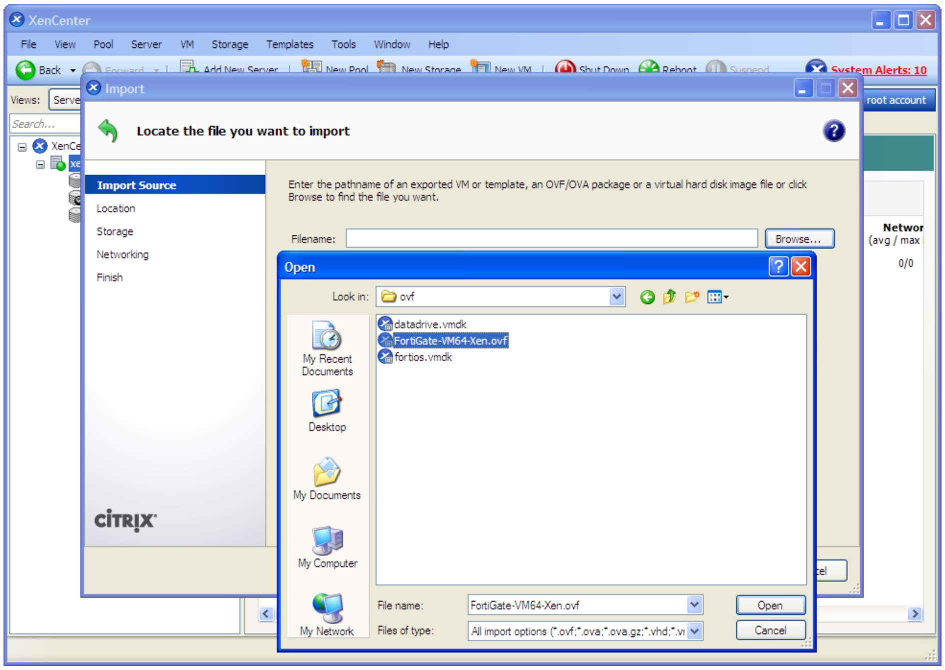
# Deploying the FortiGate-VM on Citrix Xen

**To create the FortiGate-VM from the OVF file:**

1. Launch XenCenter on your management computer. The management computer can be any computer that can run Citrix XenCenter, a Windows application.
2. If you have not already done so, select *ADD a server*. Enter your Citrix XenServer IP address and the root logon credentials required to manage that server.

   Your Citrix XenServer is added to the list in the left pane.

   The *Virtual Machine Manager* homepage opens.
3. Go to *File* > *Import*. An import dialog appears.
4. Click the *Browse* button, find the FortiGate-VM64-Xen.ovf template file, then click *Open*.

   Locate the file you want to import

   Enter the pathname of an exported VM or template, an OVF/OVA package or a virtual hard disk image file or click Browse to find the file you want.

   Filename:

   Look in: ovf

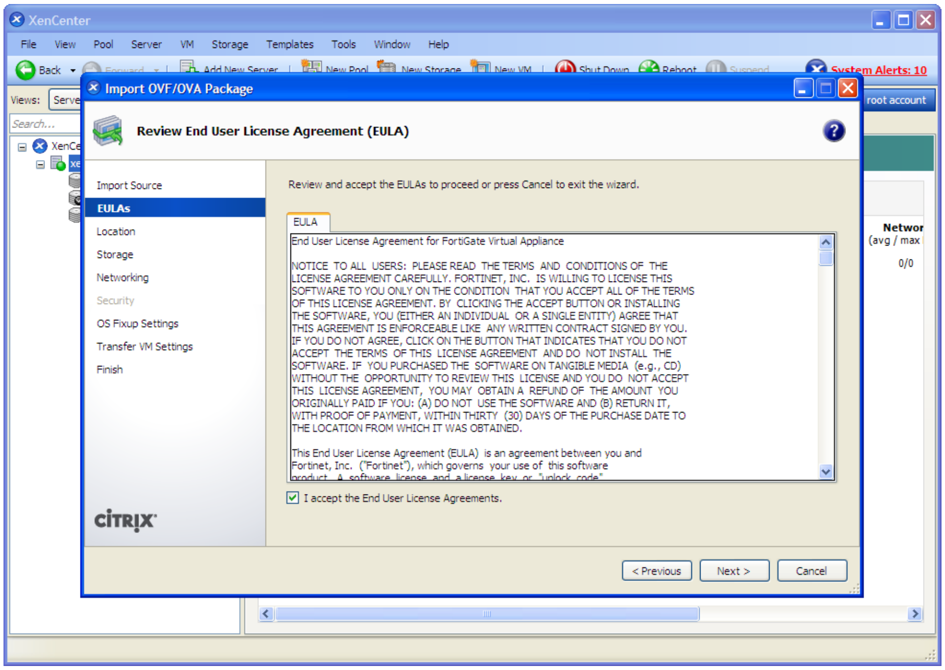
   datadrive.vmdk
   FortiGate-VM64-Xen.ovf
   fortios.vmdk

   File name: FortiGate-VM64-Xen.ovf

   Files of type: All import options (*.ovf;*.ova;*.ova.gz;*.vhd;*.vı

5. Select *Next*.

6. Accept the EULA, then select *Next*.



Import OVF/OVA Package

**Review End User License Agreement (EULA)**

Review and accept the EULAs to proceed or press Cancel to exit the wizard.

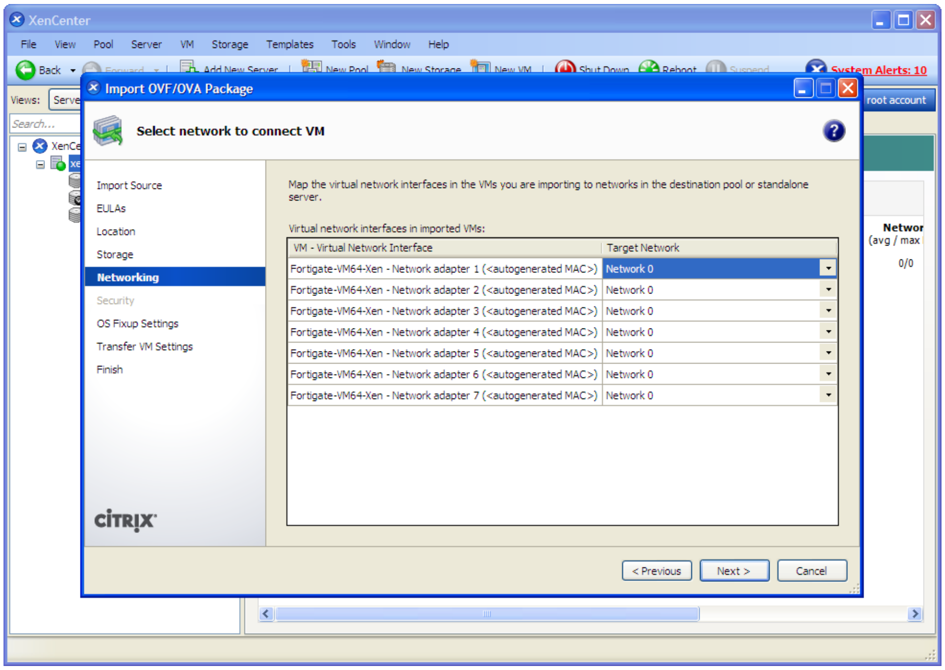
End User License Agreement for FortiGate Virtual Appliance

NOTICE TO ALL USERS: PLEASE READ THE TERMS AND CONDITIONS OF THE LICENSE AGREEMENT CAREFULLY. FORTINET, INC. IS WILLING TO LICENSE THIS SOFTWARE TO YOU ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. BY CLICKING THE ACCEPT BUTTON OR INSTALLING THE SOFTWARE, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN CONTRACT SIGNED BY YOU. IF YOU DO NOT AGREE, CLICK ON THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS LICENSE AGREEMENT AND DO NOT INSTALL THE SOFTWARE. IF YOU PURCHASED THE SOFTWARE ON TANGIBLE MEDIA (e.g., CD) WITHOUT THE OPPORTUNITY TO REVIEW THIS LICENSE AND YOU DO NOT ACCEPT THIS LICENSE AGREEMENT, YOU MAY OBTAIN A REFUND OF THE AMOUNT YOU ORIGINALLY PAID IF YOU: (A) DO NOT USE THE SOFTWARE AND (B) RETURN IT, WITH PROOF OF PAYMENT, WITHIN THIRTY (30) DAYS OF THE PURCHASE DATE TO THE LOCATION FROM WHICH IT WAS OBTAINED.

This End User License Agreement (EULA) is an agreement between you and Fortinet, Inc. ("Fortinet"), which governs your use of this software product. A software license and a license key or "unlock code"

☑ I accept the End User License Agreements.

7. Choose the pool or standalone server to host the VM, then select *Next*.
8. Select the storage location for FortiGate-VM disk drives or accept the default. Select *Next*.
9. Configure how each vNIC (virtual network adapter) in FortiGate-VM will map to each vNetwork on the Citrix XenServer, then click *Next*.



Import OVF/OVA Package

**Select network to connect VM**

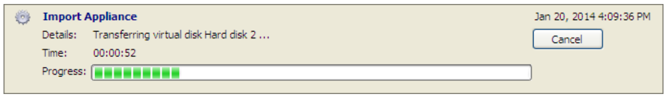
Map the virtual network interfaces in the VMs you are importing to networks in the destination pool or standalone server.

Virtual network interfaces in imported VMs:

| VM - Virtual Network Interface | Target Network |
|---|---|
| Fortigate-VM64-Xen - Network adapter 1 (<autogenerated MAC>) | Network 0 |
| Fortigate-VM64-Xen - Network adapter 2 (<autogenerated MAC>) | Network 0 |
| Fortigate-VM64-Xen - Network adapter 3 (<autogenerated MAC>) | Network 0 |
| Fortigate-VM64-Xen - Network adapter 4 (<autogenerated MAC>) | Network 0 |
| Fortigate-VM64-Xen - Network adapter 5 (<autogenerated MAC>) | Network 0 |
| Fortigate-VM64-Xen - Network adapter 6 (<autogenerated MAC>) | Network 0 |
| Fortigate-VM64-Xen - Network adapter 7 (<autogenerated MAC>) | Network 0 |

10. Click *Next* to skip OS fixup.
11. Select *Next* to use the default network settings for transferring the VM to the host.
12. Select *Finish*.

The Citrix XenServer imports the FortiGate-VM files and configures the VM as specified in the OVF template. Depending on your computer's hardware speed and resource load, and also on the file size and speed of the network connection, this might take several minutes to complete.



Import Appliance

Jan 20, 2014 4:09:36 PM

Details: Transferring virtual disk Hard disk 2 ...

Time: 00:00:52

When VM import is complete, the XenCenter left pane includes the FortiGate-VM in the list of deployed VMs for your Citrix XenServer.

# Initial settings

After you deploy a FortiGate-VM on the Xen 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 Xen 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
```

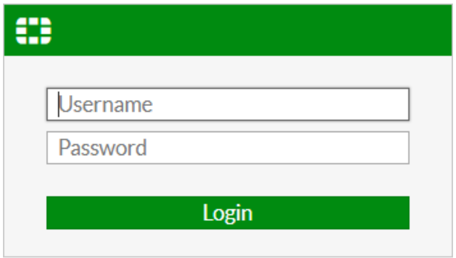
The default DNS servers are `208.91.112.53` and `208.91.112.52`.

## 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 19) 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} <filenmame 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:
   1. Go to *System* > *Dashboard* > *Status*.
   2. In the *License Information* widget, in the *Registration Status* field, select *Update*.
   3. 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

The PING utility is the usual method to test connectivity to other devices. For this, you need the console on the FortiGate-VM.

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*.

# 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.

## Promiscuous mode for broadcast HA

This section describes how to support promiscuous mode for the heartbeat interfaces of a FortiGate-VM running on XenServer to support broadcast HA heartbeat.

On XenServer, FortiGate-VM HA interfaces are directly attached to a virtual network interface (VIF). The VIF is connected to a virtual switch (xenbr) that segments network traffic between a physical network interface (PIF) and one or more VIFs. Enabling promiscuous mode as described allows all traffic crossing the PIF to become transparent across the xenbr and visible to the VIF that the FortiGate-VM HA interface is connected to.

### To enable promiscuous mode for the PIF from the XenServer host CLI:

1. Find and record the UUID of the PIF that the HA heartbeat interface is connected to by entering the following command:
   ```
   xe pif-list network-name-label=<network>
   ```
   Where `<network>` is the common name for the network as it appears in XenCenter (for example, Network 0).
2. Enter the following command to enable promiscuous mode for the PIF:
   ```
   xe pif-param-set uuid=<uuid> other-config:promiscuous="true"
   ```
   Where `<uuid>` is the UUID for the PIF.
3. Enter the following command to verify that the promiscuous option has been set:
   ```
   xe pif-param-list uuid=<uuid>
   ```
   A line similar to the following should appear in the command output to indicate that promiscuous mode is enabled:
   ```
   other-config (MRW): promiscuous: true
   ```

### To enable promiscuous mode for the VIF from the XenServer host CLI:

1. Find and record the UUID of the VIF that the HA heartbeat interface is connected to by entering the following command:
   ```
   xe vif-list vm-name-label=<vm-name>
   ```
   Where `<vm-name>` is the common name of the FortiGate-VM as it appears in XenCenter.
2. Enter the following command to enable promiscuous mode for the VIF:
   ```
   xe vif-param-set uuid=<uuid> other-config:promiscuous="true"
   ```
   Where `<uuid>` is the UUID for the PIF.
3. Enter the following command to verify that the promiscuous option has been set:
   ```
   xe vif-param-list uuid=<uuid_of_vif>
   ```
   A line similar to the following should appear in the command output to indicate that promiscuous mode is enabled:
   ```
   other-config (MRW): promiscuous: true
   ```

4. Enter the following command to verify that the promiscuous option has been set:

   ```
   xe vif-param-list uuid=<uuid_of_vif>
   ```

   A line similar to the following should appear in the command output to indicate that promiscuous mode is enabled:

   ```
   other-config (MRW): promiscuous: true
   ```

5. Enter the following commands to activate promiscuous mode for the VIF:

   ```
   xe vif-unplug uuid=<uuid_of_vif>
   xe vif-plug uuid=<uuid_of_vif>
   ```

   These commands disconnect and reconnect the VIF to the VM. When the VIF reconnects, promiscuous mode will be active. The `unplug` command takes the FortiGate-VM HA interface offline, and brings down the interface to the VM until you enter the `vif-plug` command.

   You can use `tcpdump` utility to compare traffic on the PIF and VIF to ensure that the VIF is behaving promiscuously.

# Optimizing FortiGate-VM performance

You can optimize FortiGate-VM performance by configuring interrupt-affinity and packet-distribution-affinity attributes to improve efficiency and resource utilization.

## SR-IOV

FortiGate-VMs installed on Xen 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 Xen 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 Xen 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 Xen 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 Xen host is running has BIOS, physical NIC, and network driver support for SR-IOV.

To enable SR-IOV, your Xen 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 ixgbevf 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 ixgbevf or i40e/i40evf network drivers. Fortinet recommends i40e/i40evf drivers because they provide four TxRx queues for each VF and ixgbevf only provides two TxRx queues.

### Create an SR-IOV network from XenCenter

The following procedure may require rebooting the XenServer host, so it should only be performed during a maintenance window.

From the XenCenter GUI:

1. Under the *Networking* tab select *Add Network*.
2. On the *Select Type* page, select *SR-IOV Network*.
3. Give the new network a name.

4. On the *Network Settings* page, select a NIC that supports SR-IOV.
5. Select *Finish* to build the network and select *Create SR-IOV anyway* when prompted.
6. On the *Network* tab, confirm that the new network was added. The SR-IOV column should indicate that the new network is an SR-IOV network. The column could also indicate whether you must reboot the XenServer host.
7. Restart the XenServer host if required.

## Assign an SR-IOV network to a FortiGate-VM from XenCenter

The following procedure requires shutting down and restarting the FortiGate-VM, so it should only be performed during a maintenance window.

From the XenCenter GUI:

1. From the *Networking* tab, select a FortiGate-VM that you want to assign the SR-IOV network to.
2. Shut down the FortiGate-VM.
3. Select *Add Interface* to add a new interface.
4. Set *Network* to the SR-IOV network added above and configure other network settings as required.
5. Start the FortiGate-VM.

## Create an SR-IOV network from the xe CLI

The following procedure may require rebooting the XenServer host, so it should only be performed during a maintenance window.

From the xe CLI:

1. Create the SR-IOV network with the following `network-create` command. This command also returns the UUID of the newly created network:
   ```
   xe network-create name-label=<network-name>
   ```
2. Determine the PIF UUID of the NIC on which SRIOV Network would be configured.
   ```
   xe pif-list
   ```
3. Configure the network as an SR-IOV network. The following command also returns the UUID of the newly created SR-IOV Network:
   ```
   xe network-sriov-create network-uuid=<network-uuid> pif-uuid=<physical-pif-uuid>
   ```
4. Enter the following command to determine if the XenServer host needs to be rebooted:
   ```
   xe network-sriov-param-list uuid=<SR-IOV Network_uuid>
   ```
   The output should contain a line similar to the following that indicates whether or not the XenServer host needs to be restarted:
   ```
   requires-reboot ( RO): false
   ```

## Assign an SR-IOV network to a FortiGate-VM from the xe CLI

The following procedure requires shutting down and restarting the FortiGate-VM, so it should only be performed during a maintenance window.

From the xe CLI:

1. Determine the vif mac address of the FortiGate-VM by entering the following command:
   ```
   xe vm-vif-list vm=”<fortigate-vm-instance-name>”
   ```

2. Assign the SR-IOV Network to the FortiGate-VM:

   ```
   xe vif-create device=<device-index> mac=<vf-mac-address> network-uuid=<sriov-network>
        vm-uuid=<vm-uuid>
   ```

   This command also returns the UUID of the newly created network.

# 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. The 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 set 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 mast.
- `<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
```

## Hyperthreading

Enabling hyperthreading for XenServer allows a single processor core to function as two logical processors, often resulting in improved performance. If your XenServer 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 XenServer.

### To check hyperthreading status on a XenServer host:

1. Open a local shell and log in as 'root'.
2. Run the following command to display the number of threads uses on the XenServer host
   `xl info | grep threads_per_core`
   A value greater than 1 indicates that hyperthreading is enabled on the host. A value of 1 indicates that hyperthreading is disabled on the Xen command line or not enabled on the hardware.

### To enable hyperthreading on a XenServer host:

1. Open a local shell and log in as 'root'.
2. Enter the following command:
   ```
   /opt/xensource/libexec/xen-cmdline --set-xen smt=1
   ```
3. Restart the XenServer host.

### To disable hyperthreading on a XenServer host:

1. Open a local shell and log in as 'root'.
2. Enter the following command:
   ```
   /opt/xensource/libexec/xen-cmdline --set-xen smt=0
   ```
3. Restart the XenServer host.

# Change log

| Date | Change Description |
|---|---|
| 2021-03-30 | Initial release. |
| | |
| | |
| | |
| | |

FORTINET®

www.fortinet.com

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. 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.