FortiDDoS - VM Deployment Guide

Version 6.1.0

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://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

January 15, 2021
FortiDDoS 6.1.0 VM Deployment Guide
00-610-681153-20210115

TABLE OF CONTENTS

Change Log

Date	Change Description
2021-01-06	Initial release.

Getting Started

Introduction

FortiDDoS F-series features a clean-sheet new architecture that draws on more than 10 years of FortiDDoS' DDoS mitigation experience while providing a flexible and forward-looking solution to detect and mitigate Layer 3 to Layer 7 DDoS attacks for enterprise data centers. FortiDDoS uses machine learning and behavior based methods, and monitors hundreds of thousands of networking parameters to build an adaptive baseline of normal activity. It then monitors traffic against that baseline and defends against every DDoS attack.

About this document

This document describes how to deploy a FortiDDoS virtual appliance disk image onto a virtualization server, and how to configure the virtual hardware settings of the virtual appliance. It assumes you have already successfully installed a virtualization server on the physical machine.

This document does not cover initial configuration of the virtual appliance itself, nor ongoing use and maintenance.

System requirements

Before you can install FortiDDoS VM, you must first have virtual machine (VM) environment software (a hardware abstraction layer (HAL), sometimes called a hypervisor) on your server. FortiDDoS VM is a virtual appliance that runs inside that environment.

VM environment	Tested Versions
VMware	ESXi 6.x, 7.x

For best performance, install FortiDDoS-VM on a “bare metal” hypervisor. Hypervisors that are installed as applications on top of a general purpose operating system (Windows, Mac OS X or Linux) host have fewer computing resources available due to the host OS’s own overhead.

Hardware-assisted virtualization (VT) must be enabled in the BIOS.

For installation instructions, see the documentation for your VM environment.

Hardware-assisted virtualization (VT) must be enabled in the BIOS. You must also have the VM environment client, such as VMware vSphere Client, installed on a management computer. (A management computer is a desktop or a laptop that you will use to deploy and manage your virtual machines.)

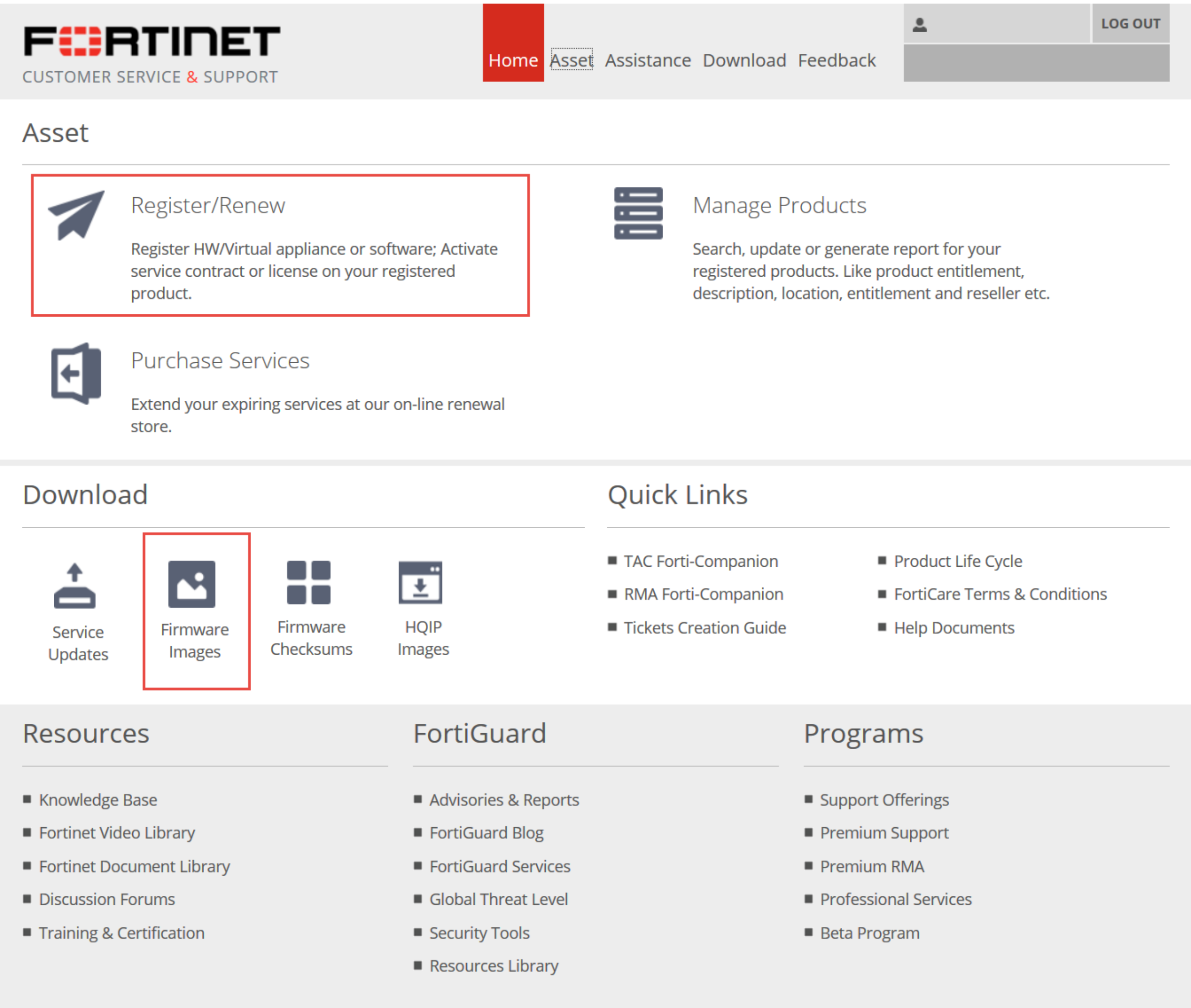
Downloading software & registering with support

When you purchase a FortiDDoS-VM, you receive an email that contains a registration number. This is used to download the software, your purchased license, and also to register your purchase with Fortinet Customer Service & Support so that your FortiDDoS-VM will be able to validate its license with Fortinet.

Many Fortinet customer services such as firmware updates, technical support, and FortiGuard services require product registration. For more information, see the Fortinet Knowledge Base article Registration Frequently Asked Questions.

Fortinet Customer Service & Support on page 6 shows the Fortinet Customer Service & Support website.

Fortinet Customer Service & Support



Asset

Register/Renew

Register HW/Virtual appliance or software; Activate service contract or license on your registered product.

Manage Products

Search, update or generate report for your registered products. Like product entitlement, description, location, entitlement and reseller etc.

Purchase Services

Extend your expiring services at our on-line renewal store.

Download

Quick Links

- TAC Forti-Companion
- RMA Forti-Companion
- Tickets Creation Guide
- Product Life Cycle
- FortiCare Terms & Conditions
- Help Documents

Resources

- Knowledge Base
- Fortinet Video Library
- Fortinet Document Library
- Discussion Forums
- Training & Certification

FortiGuard

- Advisories & Reports
- FortiGuard Blog
- FortiGuard Services
- Global Threat Level
- Security Tools
- Resources Library

Programs

- Support Offerings
- Premium Support
- Premium RMA
- Professional Services
- Beta Program

To register & download FortiDDoS-VM and your license:

1. Log into the Fortinet Customer Service & Support web site:
   https://support.fortinet.com/

2. Under Asset, click **Register/Renew**.
3. Provide the registration number that was emailed to you when you purchased the software. Registration numbers are a hyphenated string of 25 numbers and characters in groups of 5, such as: `TLH5R-NUNDP-MC6T7-0DNWA-AP45ZA`

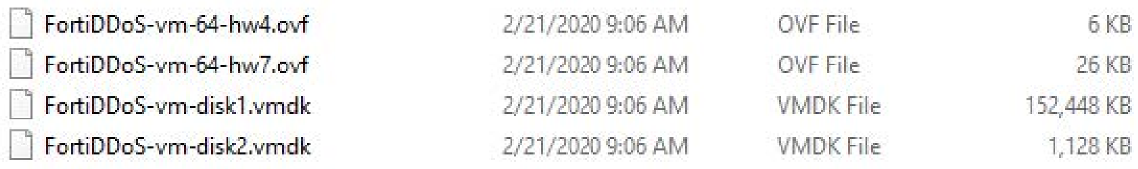
   A registration form appears.
4. Use the form to register your ownership of FortiDDoS-VM.

   After completing the form, a registration acknowledgment page appears.
5. Click the **License File Download** link.

   Your browser will download the `.lic` file that was purchased for that registration number.
6. Click the **Home** link to return to the initial page.
7. Under Download, click **Firmware Images**.
8. Click the FortiDDoS link and navigate to the version that you want to download.
9. Download the .zip file. You use the VM installation files contained in the .zip file for *new* VM installations. (The `.out` image files are for upgrades of existing installations only, and cannot be used for a new installation.)

   Files for FortiDDoS-VM have a FDD_VM filename prefix. Other prefixes indicate that the file is for hardware versions of FortiDDoS such as FortiDDoS 200F. Such other files cannot be used with FortiDDoS-VM.

10. Extract the .zip file contents to a folder. The following figure shows the contents of the package for VMware.



FortiDDoS-vm-64-hw4.ovf	2/21/2020 9:06 AM	OVF File	6 KB
FortiDDoS-vm-64-hw7.ovf	2/21/2020 9:06 AM	OVF File	26 KB
FortiDDoS-vm-disk1.vmdk	2/21/2020 9:06 AM	VMDK File	152,448 KB
FortiDDoS-vm-disk2.vmdk	2/21/2020 9:06 AM	VMDK File	1,128 KB

The FortiDDoS-vm-64-hw4.ovf file is a VMware virtual hardware version 4 image that supports ESXi 3.5. The FortiDDoS-vm-64-hw7.ovf file is a VMware virtual hardware version 7 image that supports ESXi 4.0 and above.

Refer to the VMware support site for information about VMware virtual hardware versions and ESXi versions.

VM environment	Download package
VMware	The ovf.zip download file contains multiple ovf files. The FortiDDoS-vm-64-hw4.ovf file is a VMware virtual hardware version 4 image that supports ESXi 3.5. The FortiDDoS-vm-64-hw7.ovf file is a VMware virtual hardware version 7 image that supports ESXi 4.0 and above. Refer to the VMware support site for information about VMware virtual hardware versions and ESXi versions.

Licensing

This section describes licensing. It includes the following information:

- Evaluation license
- License sizes
- License validation

Evaluation license

FortiDDoS-VM can be evaluated with a free 15-day trial license that includes all the features.

You do not need to manually upload the trial license. It is built-in. The trial period begins the first time you start FortiDDoS-VM. When the trial expires, most functionality is disabled. You must purchase a license to continue using FortiDDoS-VM.

License sizes

FortiDDoS-VM licenses are available at the following sizing levels.

FortiDDoS-VM sizes

	License/model		
	VM04	**VM08**	**VM16**
Virtual CPUs (vCPUs)	4	8	16
Virtual RAM (vRAM)	16 GB	16 GB	32 GB

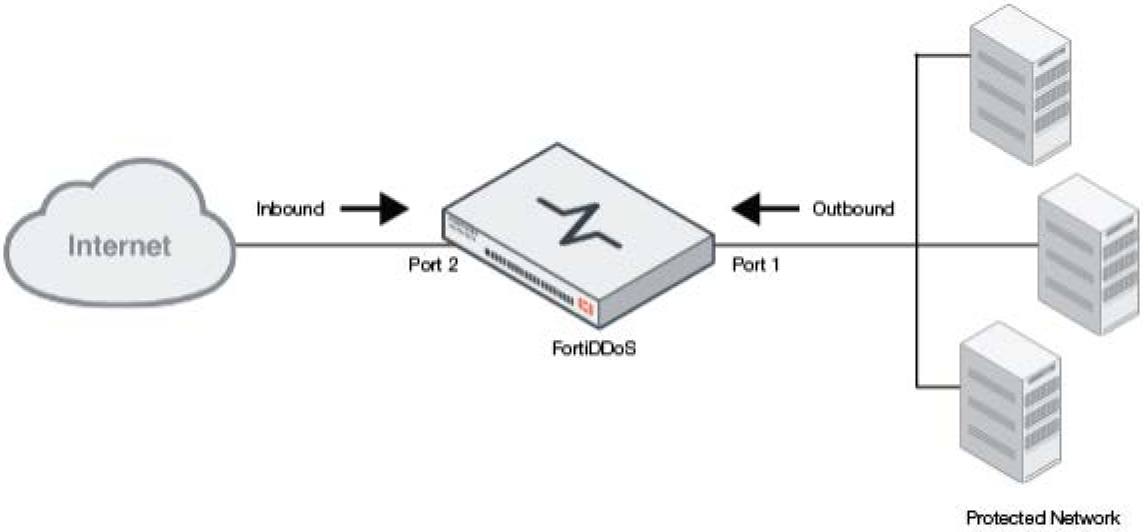
Maximum IP sessions varies by license, but also by available vRAM, just as it does for hardware models. For details, see the maximum configuration values in the FortiDDoS Handbook.

License validation

FortiDDoS-VM must periodically re-validate its license with the Fortinet Distribution Network (FDN). FortiDDoS-VM should directly connect to Fortiguard server for license validation.

Deploying FortiDDoS VM

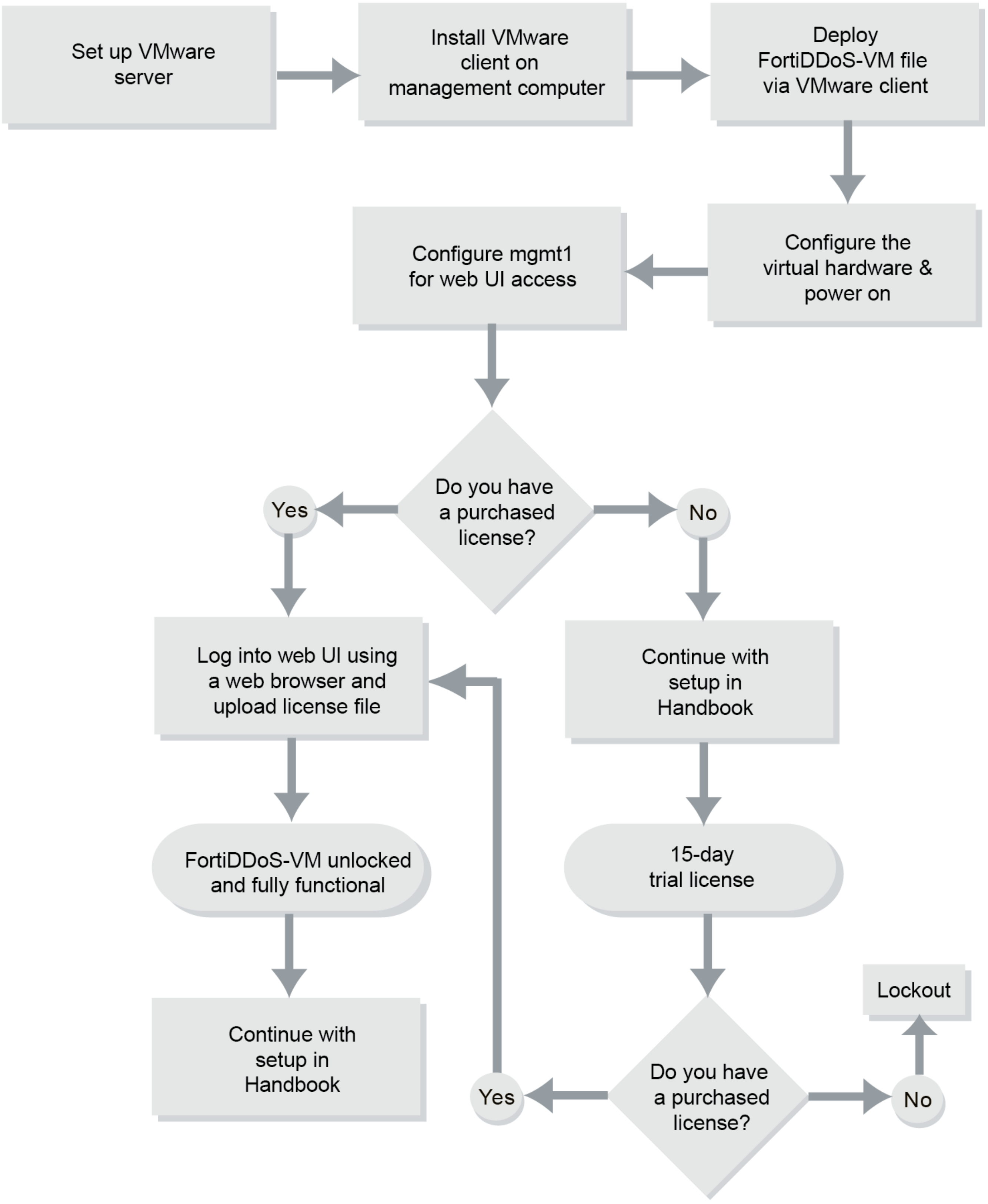
This section provides procedures for deploying the FortiDDoS VM software.



Installation overview

The diagram below gives an overview of the process for installing FortiDDoS-VM on VMware.

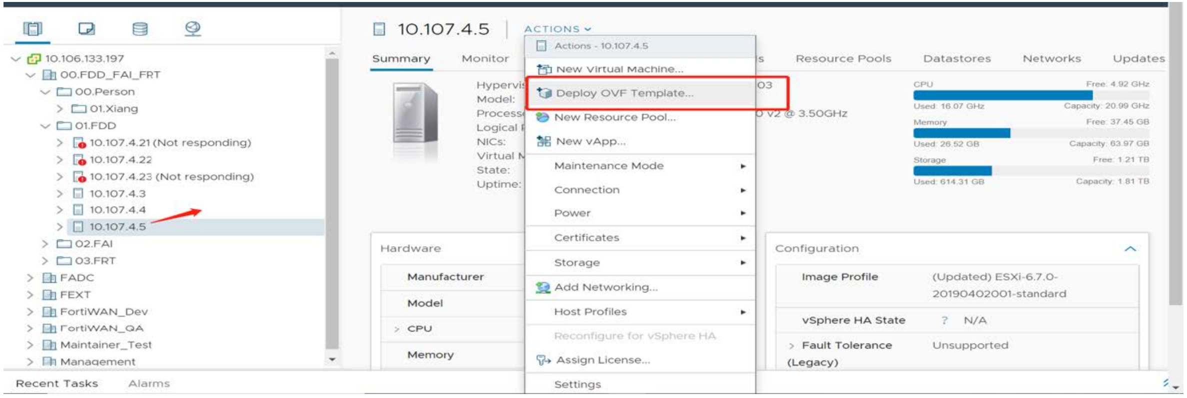
Basic steps for installing FortiDDoS-VM (VMware)


Set up VMware server
Install VMware client on management computer
Deploy FortiDDoS-VM file via VMware client
Configure the virtual hardware & power on
Configure mgmt1 for web UI access
Do you have a purchased license?
Yes
No
Log into web UI using a web browser and upload license file
FortiDDoS-VM unlocked and fully functional
Continue with setup in Handbook
Continue with setup in Handbook
15-day trial license
Do you have a purchased license?
Yes
No
Lockout

Step 1: Deploy FortiDDoS VM in ESXi

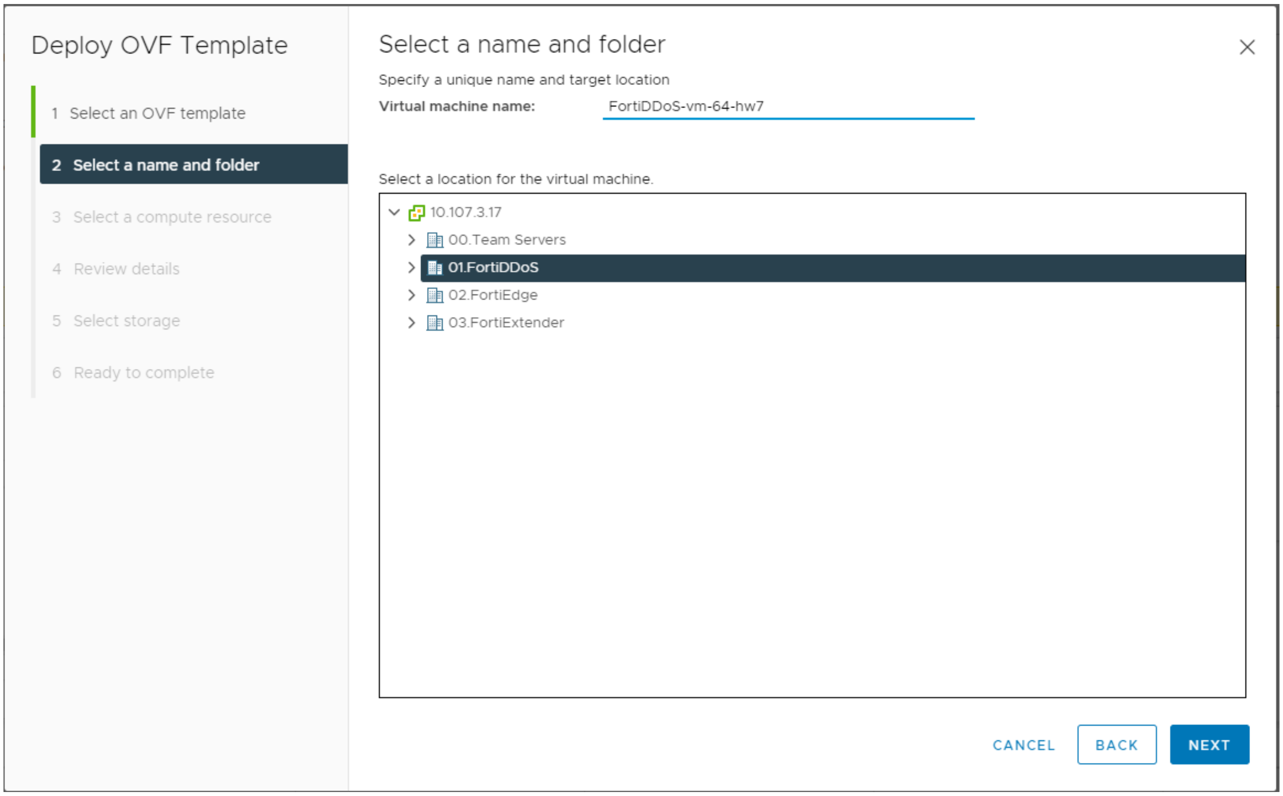
Deployment

1. Download the out.ovf.zip file and extract the file contents if you have not already done so. (Refer to Getting Started on page 5 for specific instructions.)
2. Deploy the image on your client after logging in.
3. Select the ESXi you want to deploy in. Click the **Actions** dropdown menu (or right click the ESXI) and select **Deploy OVF Template**.



4. **Select an OVF template**: Click the **Local file** option and choose the following three files from the "image-esx-64" folder:
   a. FortiDDoS-vm-65-hw7.ovf
   b. FortiDDoS-vm-disk1.vmdk
   c. FortiDDoS-vm-disk2.vmdk
   Note: Make sure you do NOT include the "FortiDDoS-vm-64-hw4.ovf" file

5. Select a name and folder: Provide a virtual machine name.



Deploy OVF Template

Select a name and folder

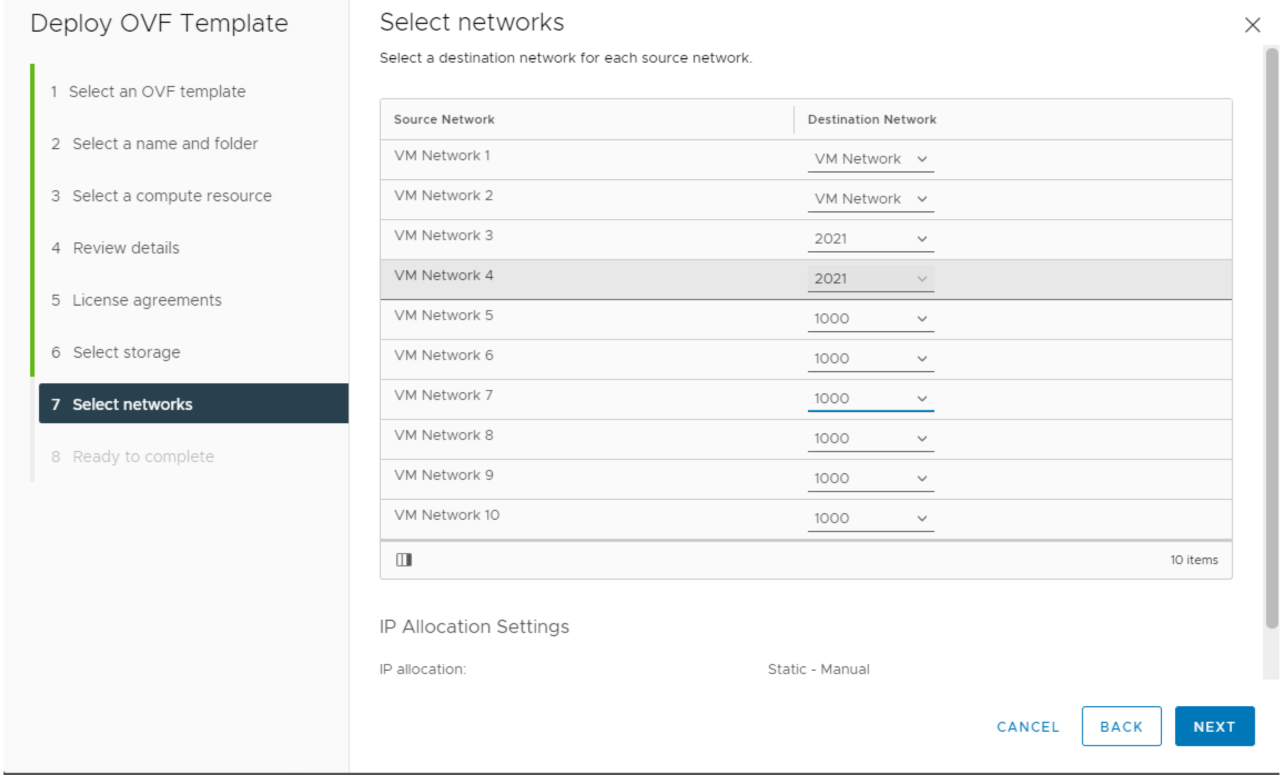
Specify a unique name and target location

Virtual machine name: FortiDDoS-vm-64-hw7

Select a location for the virtual machine.

6. **Select a compute resource:** By default the VM will be installed in your selected ESXi. Select an alternate destination if desired.
7. **Review details:** Verify the information displayed, then click Next.
8. **License agreements:** Check the box next to "I accept all license agreements" and click Next.
9. **Select storage:** Select your storage or use the default and click Next.

10. **Select networks:** Select the desired destination network. In this example we will keep the default in this step and edit it after we create the VLAN.



Select networks

Select a destination network for each source network.

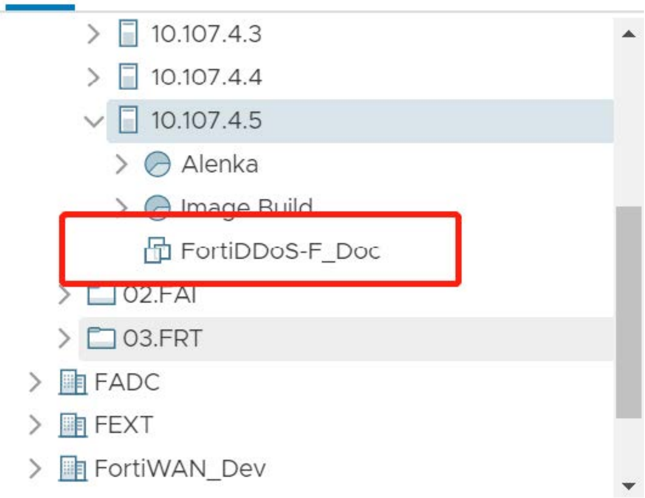
Source Network	Destination Network
VM Network 1	VM Network
VM Network 2	VM Network
VM Network 3	2021
VM Network 4	2021
VM Network 5	1000
VM Network 6	1000
VM Network 7	1000
VM Network 8	1000
VM Network 9	1000
VM Network 10	1000

10 items

IP Allocation Settings

IP allocation: Static - Manual

11. **Ready to complete:** Click Finish to deploy. You should see your new V added to the ESXi tree once complete.



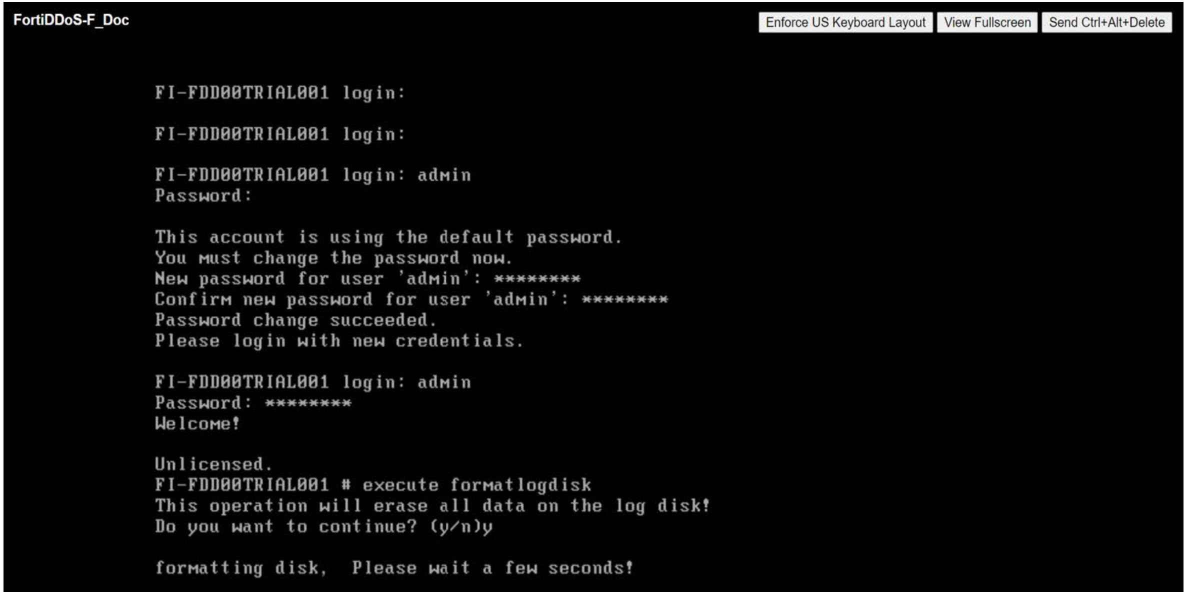
Do not power on the virtual appliance until you have completed the following steps:

- Resize the virtual disk (VMDK).
- Set the number of vCPUs.
- Set the vRAM on the virtual appliance.
- Map the virtual network adapter(s).

These settings must be configured in the VM environment, not the FortiDDoS OS.

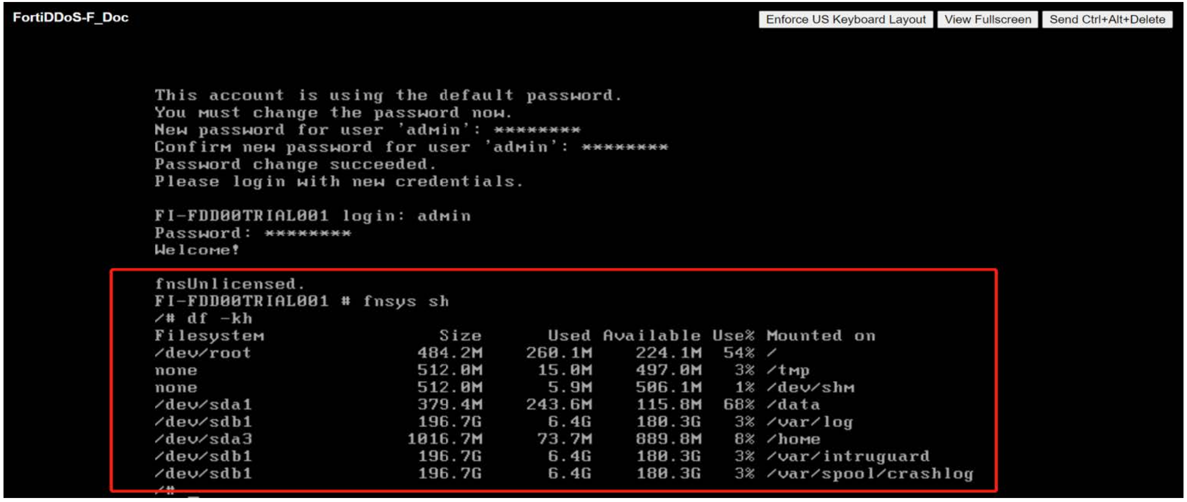
Formatting disk

1. Power up the VM once the deployment process is complete. Only 30G disk is shown after executing df -kh in shell so we need to format the disk. This process will take about 10 minutes.



```
FI-FDD00TRIAL001 login:

FI-FDD00TRIAL001 login:

FI-FDD00TRIAL001 login: admin
Password:

This account is using the default password.
You must change the password now.
New password for user 'admin': ********
Confirm new password for user 'admin': ********
Password change succeeded.
Please login with new credentials.

FI-FDD00TRIAL001 login: admin
Password: ********
Welcome!

Unlicensed.
FI-FDD00TRIAL001 # execute formatlogdisk
This operation will erase all data on the log disk!
Do you want to continue? (y/n)y

formatting disk,  Please wait a few seconds!
```

2. Once the process is complete, the disk will now be 200G.



```
This account is using the default password.
You must change the password now.
New password for user 'admin': ********
Confirm new password for user 'admin': ********
Password change succeeded.
Please login with new credentials.

FI-FDD00TRIAL001 login: admin
Password: ********
Welcome!

fnsUnlicensed.
FI-FDD00TRIAL001 # fnsys sh
/# df -kh
Filesystem                Size      Used Available Use% Mounted on
/dev/root               484.2M    260.1M    224.1M  54% /
none                    512.0M     15.0M    497.0M   3% /tmp
none                    512.0M      5.9M    506.1M   1% /dev/shm
/dev/sda1               379.4M    243.6M    115.8M  68% /data
/dev/sdb1               196.7G      6.4G    180.3G   3% /var/log
/dev/sda3              1016.7M     73.7M    889.8M   8% /home
/dev/sdb1               196.7G      6.4G    180.3G   3% /var/intruguard
/dev/sdb1               196.7G      6.4G    180.3G   3% /var/spool/crashlog
/#
```

Step 2: Configure virtual hardware settings

After deploying the FortiDDoS-VM image and before powering on the virtual appliance, configure the virtual appliance hardware settings to suit the size of your deployment.

Virtual hardware settings on page 14 summarizes the defaults that are set in the default image and provides rough guidelines to help you understand whether you need to upgrade the hardware before you power on the virtual appliance. For more precise guidance on sizing, contact your sales representative or Fortinet Technical Support.

Virtual hardware settings

Component	Default	Guidelines
Hard disk	32 GB	32 GB is insufficient for most deployments. Upgrade the hard disk before you power on the appliance. After you power on the appliance, you must reformat the FortiDDoS OS log disk with the following command: `execute formatlogdisk` This will change the size to 200 GB. Note: Before you use this command you must first upload a license file.
CPU	4 CPU	4 CPU is appropriate for a VM04 license. Upgrade to 8 or 16 CPU for VM08 and VM16 licenses, respectively.
RAM	4 GB	4 GB is the minimum. See the section on vRAM for guidelines based on expected concurrent connections.
Network interfaces	10 bridging vNICs are mapped to a port group on one virtual switch (vSwitch).	Change the mapping as required for your VM environment and network.

Configuring the number of virtual CPUs (vCPUs)

By default, the virtual appliance is configured to use 4 vCPUs. Depending on the FortiDDoS-VM license that you purchased, you can allocate 8 or16 vCPUs.

To change the number of vCPUs:

1. Use the ESXi client to connect to the server.
2. In the left pane, right-click the name of the virtual appliance, such as **FortiDDoS-VM-Doc**, then select **Edit Settings**.
3. In the list of virtual hardware, click **CPUs**.
4. In Number of virtual processors, specify the maximum number of vCPUs to allocate. Valid values range from 1 to 8.
5. Click **OK**.

Configuring the virtual RAM (vRAM) limit

To change the amount of vRAM:

1. Use the ESXi client to connect to the server.
2. In the left pane, right-click the name of the virtual appliance, such as **FortiDDoS-VM-Doc**, then select **Edit Settings**.
   The virtual appliance properties dialog appears.
3. In the list of virtual hardware on the left side of the dialog, click **Memory**.

4. In Memory Size, type the maximum number in gigabytes (GB) of the vRAM to allocate.
5. Click **OK**.

Mapping the virtual NICs (vNICs) to physical NICs

In FortiDDoS, we have 2 management ports, mgmt1 and mgmt2. In general practice mgmt1 will be used to manage the system using GUI/CLI.

mgmt2 is used for High-availability where 2 FortiDDoS mgmt2 ports share a same VLAN for HA communication.

Port 1 to Port 8 are data ports which form 4 port pairs.

Ports pairs are:

- Port 1 - Port 2
- Port 3 – Port 4
- Port 5 – Port 6
- Port 7 – Port 8

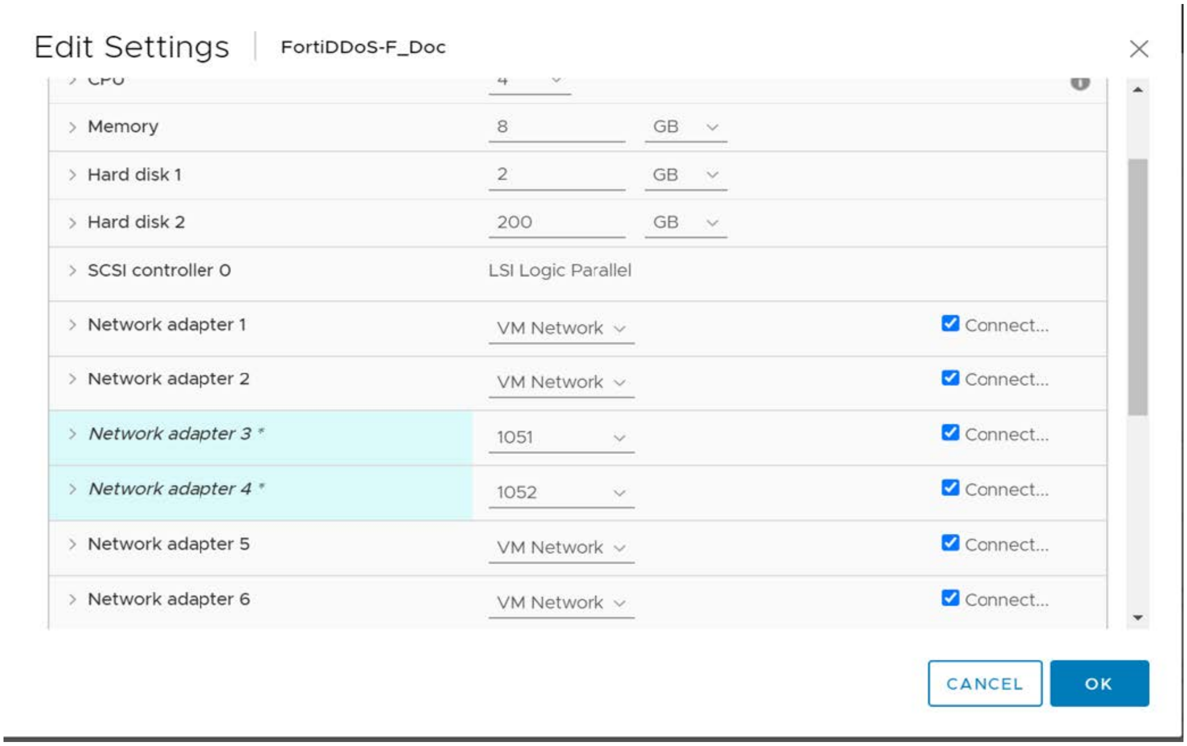
Odd numbers represent the LAN side and even numbers represent WAN side. Each Port pair that is in use should share the same VLAN which is unique to pair.

Example: Network mapping

Physical Network Adapter	Network Mapping (vSwitch Port Group)	Virtual Network Adapter for FortiDDoS-VM	FortiDDoS-VMNetwork Interface Name in Web UI/CLI
eth0	VM Network 0	Management	mgmt1
eth1	VM Network 1	HA	mgmt2
	VM Network 2	Data	port1
	VM Network 3		port2
	VM Network 4		port3
	VM Network 5		port4
	VM Network 6		port5
	VM Network 7		port6
	VM Network 8		port7
	VM Network 9		port8

To add a VM adapter:

1. Right click on **ESXi** and select **Edit Settings**.
2. Because VM Network adapter1 is mapped to VM mgmt1, set this adapter VLAN to VM Network. VM Network adapter 3 is mapped to VM port1 and VM Network adapter 4 is mapped to port2, so set Network adapter 3 to 1051 and Network adapter 4 to 1052.
   Note: ports come in pairs for input and output, so make sure you do not set an adapter to an existing pair.
3. Click **OK**.



Edit Settings | FortiDDoS-F_Doc

CPU	4		
Memory	8	GB	
Hard disk 1	2	GB	
Hard disk 2	200	GB	
SCSI controller 0	LSI Logic Parallel		
Network adapter 1	VM Network		☑ Connect...
Network adapter 2	VM Network		☑ Connect...
*Network adapter 3 **	1051		☑ Connect...
*Network adapter 4 **	1052		☑ Connect...
Network adapter 5	VM Network		☑ Connect...
Network adapter 6	VM Network		☑ Connect...

HA Configuration

Create a new VLAN for HA and mgmt2 ports of HA primary and secondary should be part of this VLAN. For more information, see the FortiDDoS Handbook.

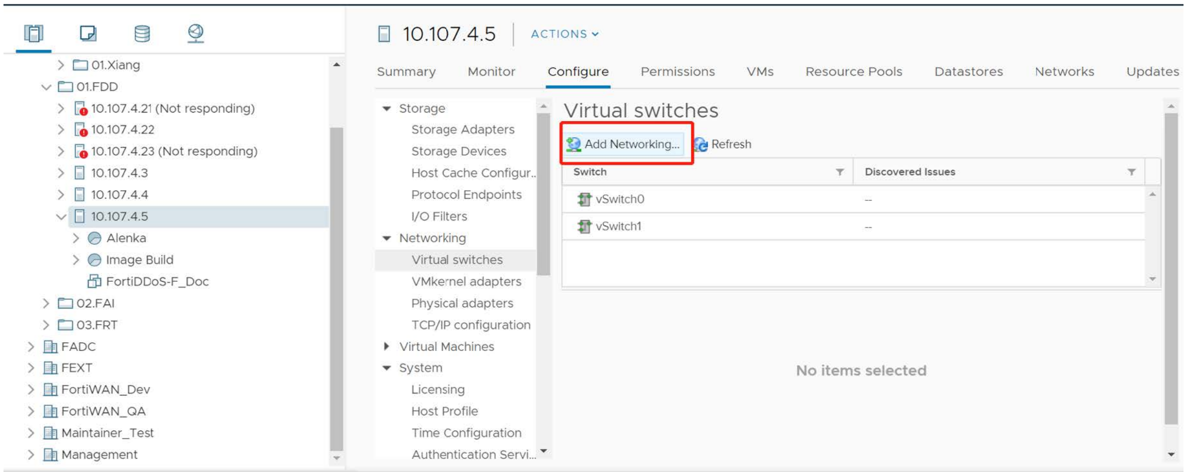
Step 3: Create VLAN

Create vswitch (optional)

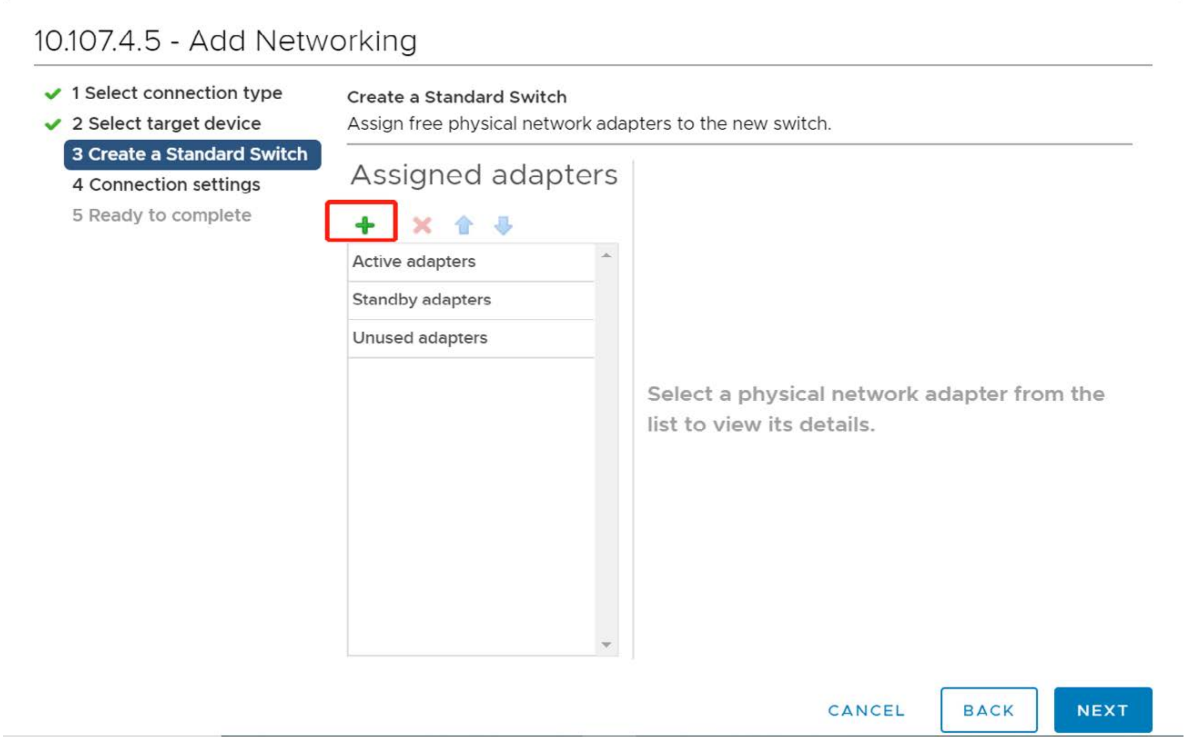
ESXi has a default vswitch named vswitch0. You can create your VLAN with the default switch or you can create your own vswitch.

If you would like to create your own vswitch, following the steps below:

1. Click **ESXi** and select the **Configure** tab. From the left menu, navigate to **Networking > Virtual switches** and click **Add Networking...**



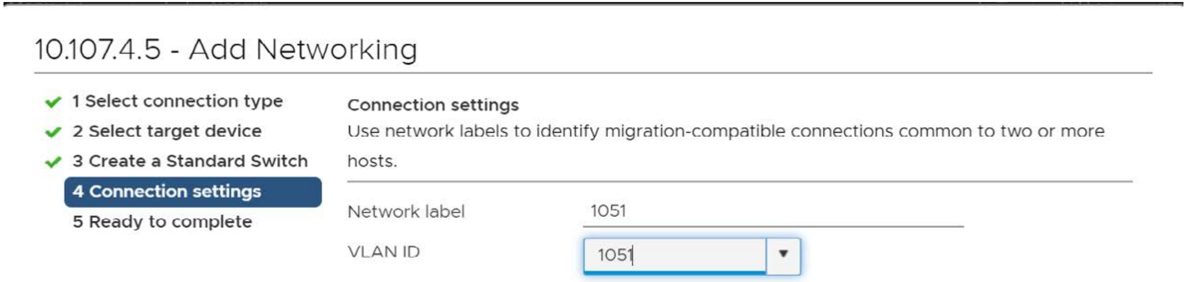
2. **Select connection type:** Select the option for "Virtual Machine Port Group for a Standard Switch".
3. **Select target device:** Select the option for "New standard switch" with 1500 MTU (Bytes).
4. **Create a standard switch:** If your client and server is not located on the same ESXi as your FortiDDoS VM, click the green plus button to bind your adapter to this vswitch. Otherwise, just click Next (which is the option we used for this demonstration). You may see a Physical Network Adapters Warning - just click OK to continue.


10.107.4.5 - Add Networking

Create a Standard Switch

Assign free physical network adapters to the new switch.

5. **Connection settings:** Create the first vlan that belongs to this vswitch.


10.107.4.5 - Add Networking

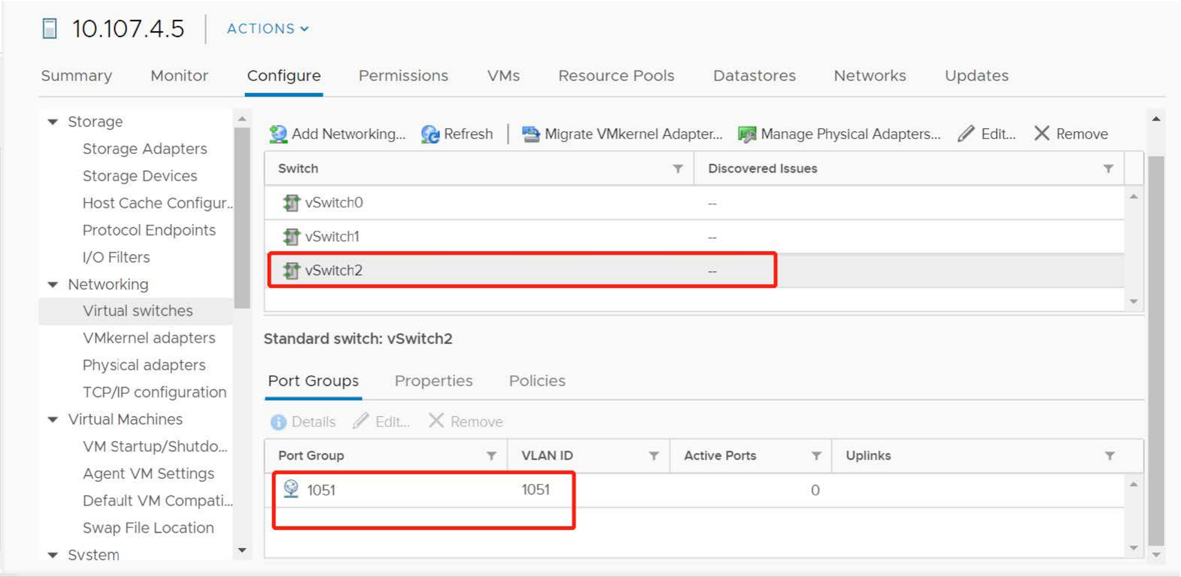
Connection settings

Use network labels to identify migration-compatible connections common to two or more hosts.

Network label 1051

VLAN ID 1051

6. **Ready to complete:** Review your settings and click **Finish**.
7. You should now see the new vswitch and its VLAN.



Switch	Discovered Issues
vSwitch0	--
vSwitch1	--
vSwitch2	--

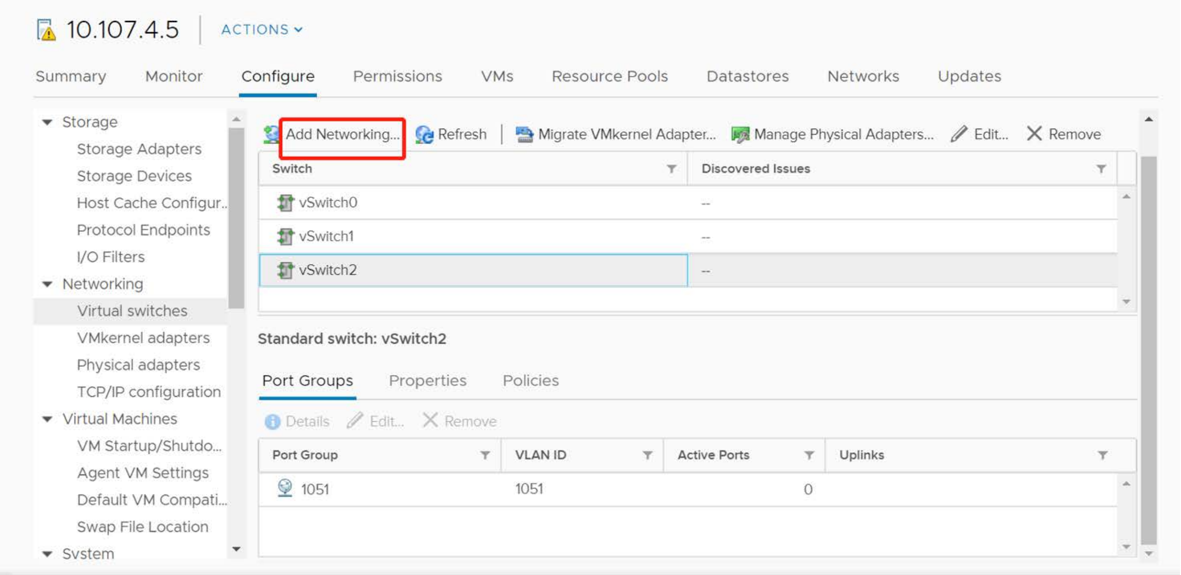
Standard switch: vSwitch2

Port Group	VLAN ID	Active Ports	Uplinks
1051	1051	0	

Create VLAN

You can add VLAN to the default vswitch vswitch0 or to the vswitch you created. In the following steps we will demonstrate with vswitch2.

1. Click **ESXi** and select the **Configure**. From the left menu, navigate to **Networking > Virtual switches**. Select the vswitch (in our case, vswitch2) from the table of switches and click **Add Networking...**.



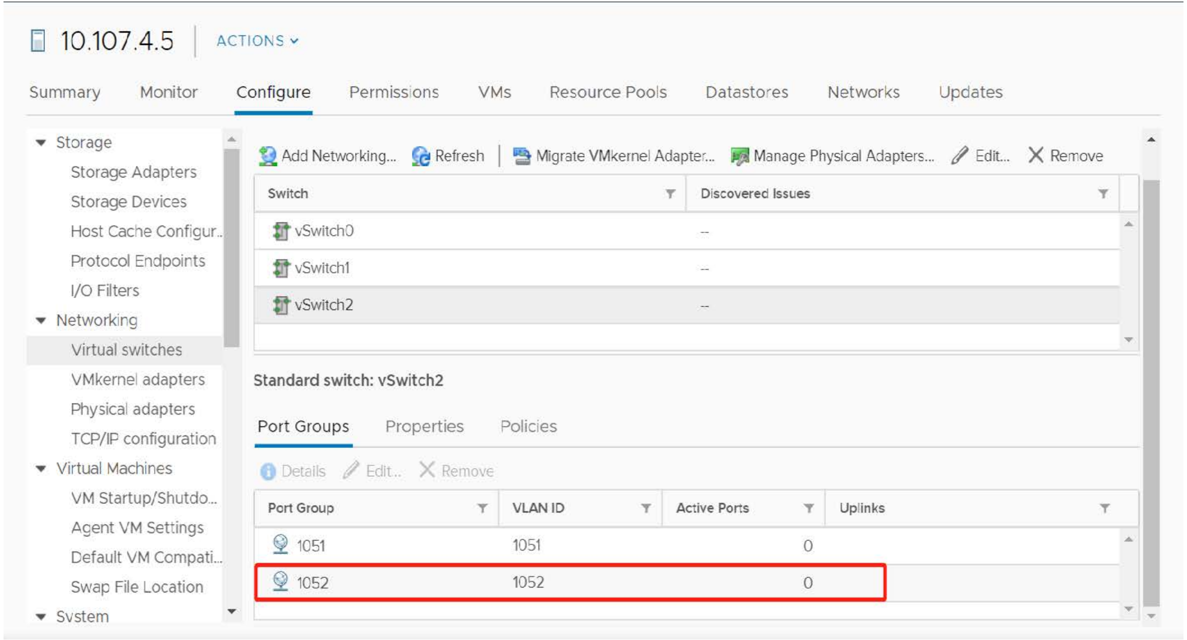
Switch	Discovered Issues
vSwitch0	--
vSwitch1	--
vSwitch2	--

Standard switch: vSwitch2

Port Group	VLAN ID	Active Ports	Uplinks
1051	1051	0	

2. **Select connection type:** Select the option for "Virtual Machine Port Group for a Standard Switch".
3. **Select target device:** Select the option for "New standard switch" with 1500 MTU (Bytes).
4. **Connection settings:** enter the Network label and VLAN ID.
5. **Ready to complete:** Review your settings and click Finish to complete the process.

6. You should now see the new VLAN you've created under the Port Groups section.



Switch	Discovered Issues
vSwitch0	--
vSwitch1	--
vSwitch2	--

Standard switch: vSwitch2

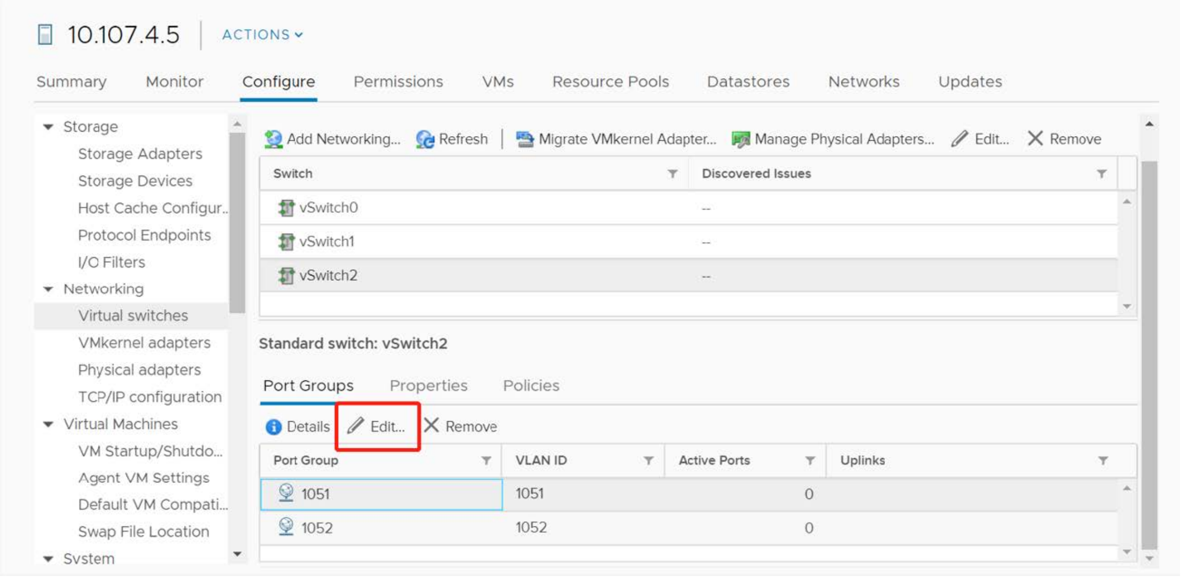
Port Group	VLAN ID	Active Ports	Uplinks
1051	1051	0	
1052	1052	0	

Enable VLAN Promiscuous mode

Enabling VLAN promiscuous mode is one of the mandatory settings for VM, so all VLANs you plan to use must be set to promiscuous mode.

Click Esxi -> Configure -> Virtual Switch -> click Switch name -> click VLAN id -> Edit

1. Click **ESXi** and select the Configure tab. From the left menu, navigate to **Networking > Virtual switches**. Select the Switch name (e.g. "vSwitch2") from the table of switches. Then, select the VLAN row (e.g. Port Group 1051, VLAN ID 1051) from the Port Groups table and click **Edit...**.

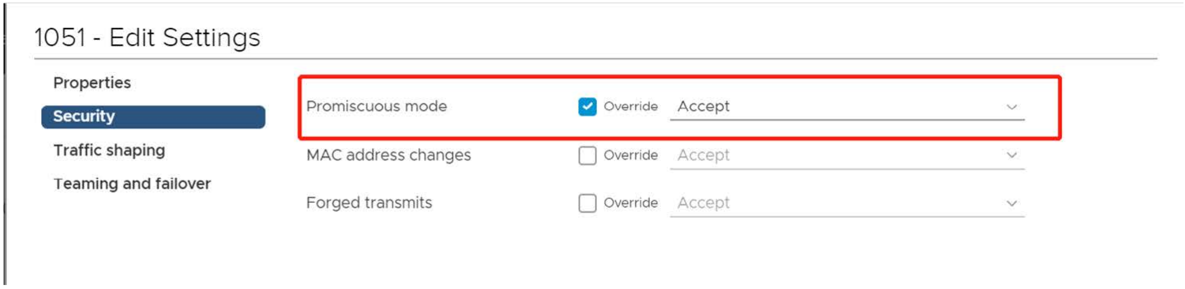


Switch	Discovered Issues
vSwitch0	--
vSwitch1	--
vSwitch2	--

Standard switch: vSwitch2

Port Group	VLAN ID	Active Ports	Uplinks
1051	1051	0	
1052	1052	0	

2. In the **Edit Settings** table, select **Security** from the left menu. Check the **Override** box next to Promiscuous mode and choose **Accept** from the dropdown menu and click **Finish**.



1051 - Edit Settings

Promiscuous mode ☑ Override Accept

MAC address changes ☐ Override Accept

Forged transmits ☐ Override Accept

Step 4: Power on the virtual appliance

After the virtual appliance software has been deployed and its virtual hardware configured, you can power on the virtual appliance.

Before you begin:

- You must have resized the disk (VMDK).
- You must have resized the CPUs and RAM, if necessary.
- You must have mapped the virtual network adapters if the defaults are not appropriate.

These settings must be configured in virtual machine environment. You do not configure them in the FortiDDoS OS.

To power on FortiDDoS-VM:

1. Use the ESXi client to connect to the server.
2. Click the name of the virtual appliance, such as **FortiDDoS-VM-Doc**.
3. Click **Power on the virtual machine**.

Step 5: Configure access to the web UI & CLI

Once it is powered on, you must log into the FortiDDoS-VM command-line interface (CLI) via the ESXi console and configure basic network settings so that you can connect to the web UI and/or CLI of the appliance through your management computer's network connection.

To configure basic network settings:

1. Log into the server.
2. Select the name of the virtual appliance, such as **FortiDDoS-VM-Doc**.
3. Click the **Console** tab to open the console of the FortiDDoS-VM virtual appliance.
4. At the login prompt, type `admin` and no password to log in.
5. Configure the management interface, static route, and DNS server so you can access the system from a secure management network. Use the following command syntax:

```
config system interface
   edit mgmt1
```

```
         set ip <address/mask>
         set allowaccess {http https ping snmp ssh telnet}
   end
   config system default-gateway
      edit 1
         set gateway <gateway_address>
   end
   config system dns
      set primary <dns_address>
      set secondary <dns_address>
   end
   config system l2-interface-pair
      edit l2-port1-port2
         set status enable
      next
      edit l2-port3-port4
         set status enable
      next
      edit l2-port5-port6
      next
      edit l2-port7-port8
      next
   end
```

where:

- `<address/mask>` is either the IP address and netmask assigned to the network interface, such as `192.168.1.99/24`; the correct IP will vary by your configuration of the vNetwork.
- `<gateway_address>}` is IP address of the next hop router for mgmt1.
- `<dns_address>` is the IP address of a DNS server

You should now be able to connect via the network from your management computer to `mgmt1` of FortiDDoS-VM using:

- a web browser for the web UI (e.g. If `mgmt1` has the IP address 192.168.1.1, go to https://192.168.1.1/).
- an SSH client for the CLI (e.g. If `mgmt1` has the IP address 192.168.1.1, connect to 192.168.1.1 on port 22).

Step 6: Upload the license file

When you purchase a license for FortiDDoS-VM, Technical Support provides a license file that you can use to convert the 15-day trial license to a permanent, paid license.

You can upload the license via a web browser connection to the web UI. No maintenance period scheduling is required: it will not interrupt traffic, nor cause the appliance to reboot.

To upload the license via the web UI:

1. On your management computer, start a web browser.
   Your computer must be connected to the same network as the hypervisor.
2. In your browser’s URL or location field, enter the IP address of mgmt1 of the virtual appliance, such as: `https://192.168.1.99/`.
3. Use the username `admin` and no password to log in.

The system presents a self-signed security certificate, which it presents to clients whenever they initiate an HTTPS connection to it.

4. Verify and accept the certificate, and acknowledge any warnings about self-signed certificates.
   The web UI opens to the dashboard.
5. To upload the license file (.lic), go to **System > FortiGuard**.

After the license has been validated, the System Information widget indicates the following:

- License row: The message: `Valid: License has been successfully authenticated with registration servers.`
- Serial Number row: A number that indicates the maximum number of vCPUs that can be allocated according to the FortiDDoS-VM software license, such as `FIVM16TM20090003` (where “VM16” indicates a limit of 16 vCPUs).

If logging is enabled, this log message will also be recorded in the event log:

```
"VM license has been updated by user admin via GUI(192.0.2.40)"
```

If the update did not succeed, on FortiDDoS, verify the following settings:

- time zone & time
- DNS settings
- network interface up/down status
- network interface IP address
- static routes

On your computer, use `nslookup` to verify that FortiGuard domain names are resolving (VM license queries are sent to `update.fortiguard.net`).

```
C:\Users\username>nslookup update.fortiguard.net
Server: google-public-dns-a.google.com
Address: 8.8.8.8

Non-authoritative answer:
Name: fds1.fortinet.com
Addresses: 209.66.81.150
209.66.81.151
208.91.112.66
Aliases: update.fortiguard.net
```

On FortiDDoS, use `execute ping` and `execute traceroute` to verify that connectivity from FortiDDoS to the Internet and FortiGuard is possible. Check the configuration of any NAT or firewall devices that exist between the FortiDDoS appliance and the FDN or FDS server override.

```
FortiDDoS # exec traceroute update.fortiguard.net
traceroute to update.fortiguard.net (209.66.81.150), 32 hops max, 84 byte packets
1 192.0.2.2 0 ms 0 ms 0 ms
2 209.87.254.221 <static-209-87-254-221.storm.ca> 4 ms 2 ms 3 ms
3 209.87.239.161 <core-2-g0-3.storm.ca> 2 ms 3 ms 3 ms
4 67.69.228.161 3 ms 4 ms 3 ms
5 64.230.164.17 <core2-ottawa23_POS13-1-0.net.bell.ca> 3 ms 5 ms 3 ms
6 64.230.99.250 <tcore4-ottawa23_0-4-2-0.net.bell.ca> 16 ms 17 ms 15 ms
7 64.230.79.222 <tcore3-montreal01_pos0-14-0-0.net.bell.ca> 14 ms 14 ms 15 ms
8 64.230.187.238 <newcore2-newyork83_so6-0-0_0> 63 ms 15 ms 14 ms
9 64.230.187.42 <bxX5-newyork83_POS9-0-0.net.bell.ca> 21 ms 64.230.187.93 <BX5-NEWYORK83_
     POS12-0-0_core.net.bell.ca> 17 ms 16 ms
```

```
10 67.69.246.78 <Abovenet_NY.net.bell.ca> 28 ms 28 ms 28 ms
11 64.125.21.86 <xe-1-3-0.cr2.lga5.us.above.net> 29 ms 29 ms 30 ms
12 64.125.27.33 <xe-0-2-0.cr2.ord2.us.above.net> 31 ms 31 ms 33 ms
13 64.125.25.6 <xe-4-1-0.cr2.sjc2.us.above.net> 82 ms 82 ms 100 ms
14 64.125.26.202 <xe-1-1-0.er2.sjc2.us.above.net> 80 ms 79 ms 82 ms
15 209.66.64.93 <209.66.64.93.t01015-01.above.net> 80 ms 80 ms 79 ms
16 209.66.81.150 <209.66.81.150.available.above.net> 83 ms 82 ms 81 ms
```

If the first connection had not succeeded, you can either wait up to 30 minutes for the next license query, or reboot.

```
execute reboot
```

If after 4 hours FortiDDoS still cannot validate its license, a warning message will be printed to the local console.

What’s next?

At this point, the FortiDDoS virtual appliance is running, and it has received a license file, but its operating system is almost entirely unconfigured. See the FortiDDoS Handbook for information on getting started with feature configuration.

Upgrading the number of VM CPUs

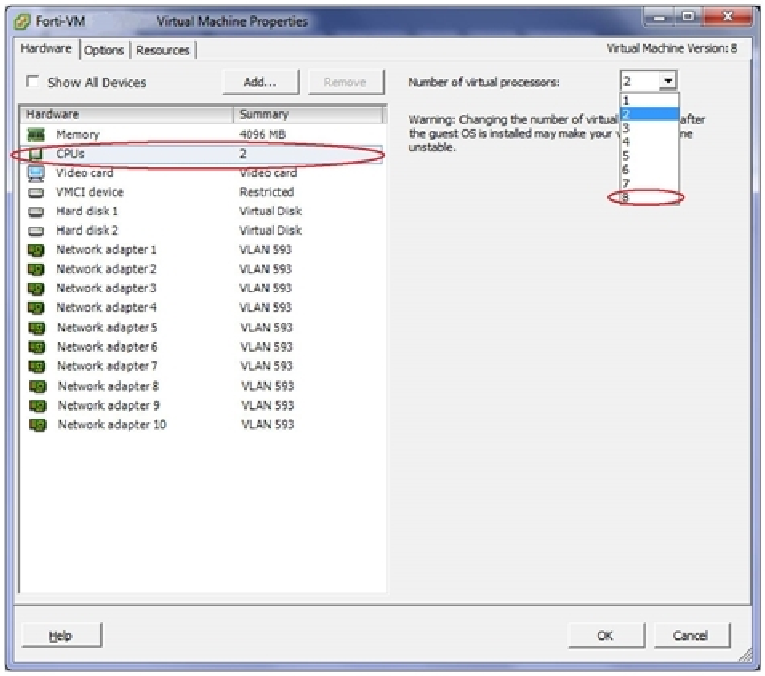
FortiDDoS-VM is licensed for either 4, 8, or 16 CPUs. If you start with one license and outgrow it, you can upgrade.

Before you begin:

- You must purchase the new license and copy the license file to your management computer.
- Be aware that you must shut down FortiDDoS and power off the virtual machine to perform the upgrade.

To allocate more vCPUs:

1. In the FortiDDoS web UI, go to System > Status > Dashboard.
2. Upload the new license. For details, see Step 6: Upload the license file.
3. In the System Information widget, click **Shut Down**.
   The virtual appliance will flush its data to its virtual disk, and prepare to be powered off. If you skip this step and immediately power off FortiDDoS-VM, you might lose buffered data.
4. On your management computer, log into the VMware server.
5. In the left pane, click the name of the virtual appliance, such as **FortiDDoS-VM-Doc**.
6. Click the **Getting Started** tab.
7. Click **Power off the virtual machine**.
8. Increase the vCPU allocation. For details, see Configuring the number of virtual CPUs (vCPUs).



Hardware	Summary
Memory	4096 MB
CPUs	2
Video card	Video card
VMCI device	Restricted
Hard disk 1	Virtual Disk
Hard disk 2	Virtual Disk
Network adapter 1	VLAN 593
Network adapter 2	VLAN 593
Network adapter 3	VLAN 593
Network adapter 4	VLAN 593
Network adapter 5	VLAN 593
Network adapter 6	VLAN 593
Network adapter 7	VLAN 593
Network adapter 8	VLAN 593
Network adapter 9	VLAN 593
Network adapter 10	VLAN 593

Number of virtual processors: 2

Warning: Changing the number of virtual after the guest OS is installed may make your v ne unstable.

9. Power on the virtual appliance again.

Upgrading the virtual hardware

By default, the FortiDDoS-VM fortidd-vm-64-hw7.ovf image uses VMware virtual hardware version 7. If you have a VMware ESXi 5.1 environment that supports virtual hardware version 9, and you want to provide version 9 feature support such as backups, you can update the virtual hardware.

For more information on virtual hardware, see:

http://kb.vmware.com/selfservice/documentLinkInt.do?micrositeID=&popup=true&languageId=&externalID=1010675

To upgrade the virtual hardware:

1. Shut down FortiDDoS-VM. To do this, you can enter the CLI command:
   ```
   execute shutdown
   ```
2. In VMware vCenter, right-click the VM and select **Power > Power Off.**
3. After it has been powered off, right-click the VM and select the option to upgrade the virtual hardware.
4. When the upgrade is complete, power on FortiDDoS-VM.