Virtual Wireless Controller Deployment Guide

2017

Release 8.3.3

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.

For assistance, contact Fortinet Customer Service and Support 24 hours a day at +1 408-542-7780, or by using one of the local contact numbers, or through the Support portal at https://support.fortinet.com/

Fortinet Customer Service and Support provide end users and channel partners with the following:

- Technical Support
- Software Updates
- Parts replacement service

Overview

About Fortinet Virtual Controllers

The Virtual Controllers are a software version of the Fortinet Appliance Controllers that are installed on an existing hardware platform provided that the platform implements a supported virtual hosting software solution.

The Virtual Controllers are built on the same System Director operating system that powers the Fortinet WLAN Controller for the enterprise delivering superior reliability, scalability and predictability for WLAN deployments. They run on the widely deployed **VMware vSphere, RHEL Kernel-based Virtual Machine (KVM)**, and **Windows based Hyper-V** virtualization platforms installed on industry-standard hardware.

When a virtual controller is purchased, the controller image can be downloaded from the Customer Support Portal and, once properly installed, can be configured just as a standard physical machine.

Advantages of Fortinet Virtual Controllers

These are some of the advantages of the Fortinet Virtual Controllers.

- Flexibility in hardware selection based on your requirements.
- Reduced cost, space requirements, and other overheads since multiple appliances can be replaced with single hardware running multiple instances of the controllers, FWLM Management; which is a web based application suite which manages controllers and access points mapped to the network to provide real-time data that enables centralized and remote monitoring of the network, and Fortinet Connect; which is a complete provisioning, management, and reporting system that provides temporary network access for guests, visitors, contractors, consultants, or customers..
- Independent and mutually exclusive instances allow administrators to use multiple virtual controllers to manage different locations or scale the deployment using the same hardware.
- Enable features provided by the virtualization software, including High Availability, failover protection, and ease of migration.
  VMWare vMotion Storage and Snapshots are supported. Hyper-V specific features (Snapshot, Failover (HA), Replication, Hot swapping) are not supported.
- Centralized control and visibility at every level of the virtual infrastructure.

Supported Hardware Configuration

The Fortinet Virtual Controller Models are available as the MC-VE series and the FWC-VM series.

MC-VE Series Virtual Controllers

This table lists the controller models available for the MC-VE Series Virtual Controllers and their corresponding requirements.

Models		MC1550-VE	MC3200-VE	MC4200-VE (1G)	MC4200-VE (10G)
Scale	AP	50	200	500	500
	Clients	1250	2500	6250	6250
vCPU		2	3	4	4
Memory		2GB	2GB	4GB	4GB
vNIC		1-2	1-2	1-4	1-2
Disk Space		2GB	2GB	2GB	2GB

FWC-VM Series Virtual Controllers

This table lists the controller models available for the new FWC-VM Series Virtual Controllers and their corresponding requirements.

Models		FWC-VM-50	FWC-VM200	FWC-VM500	FWC-VM-1000	FWC-VM-3000
Scale	AP	50	200	500	1000	3000
	Clients	1250	2500	6250	10000	30000
vCPU		4	4	8	24	48
Memory		4GB	8GB	16GB	32GB	64GB
vNIC		1-4	1-4	1-4	1-4	1-8
Disk Space		16GB (Fixed)	16GB (Fixed)	16GB (Fixed)	16GB (Fixed)	16GB (Fixed)

Fortinet Virtual Controller Deployment Modes

The MC-VE series and the FWC-VM series Virtual Controllers can be deployed in different modes.

The following list summarizes the recommended 3rd party software requirements for installing and configuring Fortinet Virtual Controllers.

Platforms	Supported	Recommended
VMWare, vSphere client	vSphere ESXi 5.5, 6.0, and 6.5	vSphere ESXi 6.5
Linux KVM	Ubuntu 16.04.2 LTS	Ubuntu 16.04.2 LTS
Hyper-V	Windows 2016	Windows 2016

Web based configuration interface has been tested with the following browsers:

- Internet Explorer versions 10 and 11 on Windows
- Firefox on Windows
- Safari on MAC OS

MC-VE Series Virtual Controllers

The MC-VE Series Virtual Controllers are tested on Dell PowerEdge R610 CPUs – Intel Xeon CPU ES620 @ 2.40 Ghz, or any equivalent h/w that has support for virtualization.

This table lists the deployment modes available in the MC-VE Series Virtual Controllers

	VMWare ESXi		Linux KVM	Windows Hyper-V
	Shared	Dedicated		
MC-VE Series	✓	✓	X	X

FWC-VM Series Virtual Controllers

The FWC-VM Series Virtual Controllers are tested on Dell PowerEdge R730 CPUs– Intel(R) Xeon(R) CPU E5-2697 v4 @ 2.30GHz. Any equivalent h/w that has support for Virtualization should work.

This table lists the deployment modes available in the FWC-VM Series Virtual Controllers.

	VMWare ESXi		Linux KVM	Windows Hyper-V
	Shared	Dedicated		
FWC-VM Series	X	✓	✓	✓

Virtual Controller Requirements

The following points are general advisories regarding Virtual Controllers.

- The number of Virtual Ports configured for the controller will vary depending on the controller's model; be sure to configure the appropriate number of ports for the model being installed.
- If you are operating more than one Fortinet Virtual Controller on a single host machine, ensure that the Virtual Interface for each Virtual Controller is configured in its own port group on the Virtual Switch. This will prevent network loops.
- Virtual Controller Ports can be configured for active-active mode or active/redundant mode.

Note: See the Fortinet WLC 8.3.2 Release Notes for limitations on the active/redundant mode.

Common Terminology

The following are some of the Networking VMware elements that will be used to configure the Fortinet Virtual Controller to operate in VMware environment:

vSwitch

This is a virtual switch, similar to a physical switch, performs functions including the Layer 2 forwarding engine, VLAN tagging, stripping, and filtering, security, checksum, and segmentation. The vSwitch links VMs to each other locally as well as to physical networks. A controller VE should connect to a vSwitch through virtual machine port groups.

Port Groups

Port groups are not VLANs. They are configuration templates for the vNIC ports on the vSwitch. Administrators can set specific QoS, security policies, and VLANs by port group. This is where you should enable promiscuous mode (and not on the vSwitch).

Promiscuous Mode (VMWare ESXi only)

Fortinet Virtual Controllers are typically deployed as an in-line device on the data path and all the packets pass through the controller. Because of this, it needs to operate in Promiscuous mode. vSphere's vSwitch and port group properties have the option to enable promiscuous mode. Again, it is highly recommended to enable this on the port group.

VM-NIC Queues Usage

The field **VM NIC Queues** in the **sh controller** command indicates the value assigned to a Controller for better performance, based on different platforms/hypervisors. This field mainly applies for the Virtual Controller Instance's deployed using VMWare and Linux KVM and **not** for Hyper-V.

For Virtual Controller models deployed using Hyper-V Platform, this field is not applicable and shows **N** for all Controller models.

For the Virtual Controller models deployed using different platforms, these are the VM NIC Queues values.

Platforms	FWC-VM-50	FWC-VM-200	FWC-VM-500	FWC-VM-1000	FWC-VM-3000
VMWare	4	4	8	8	8
Linux KVM	2	2	4	8	16
Hyper-V	N	N	N	N	N

Deploying Fortinet Virtual Controllers with VMWare ESXi

Pre-requisites

For deployment and management of the Virtual Controller, you will need to download any of these VMware suites to the workstation:

- Single ESXi server management – Use VMware vSphere Client.
- Multiple ESXi servers requires vCenter – Advance features are also tied with vCenter which needs separate licenses (vMotion, and so on).

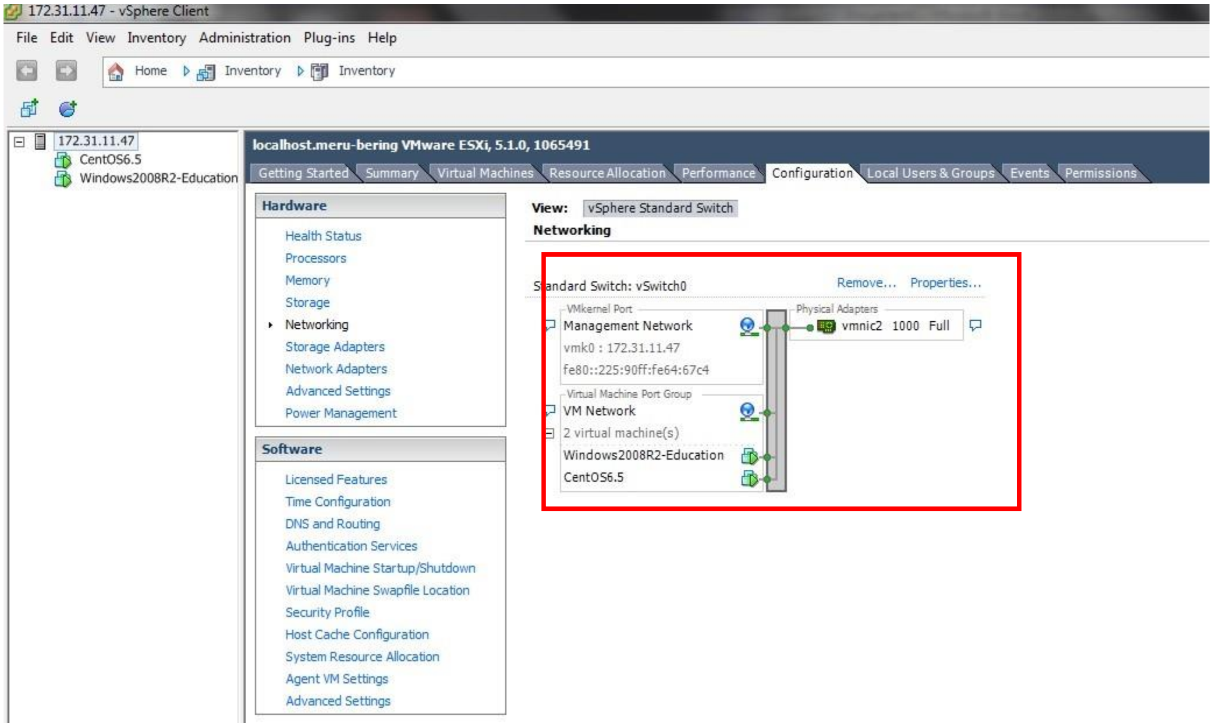
Fortinet Virtual Controllers can be deployed in these 2 modes in a VMWare setup.

Note: Fortinet recommends that you deploy the Fortinet Virtual Controllers in the dedicated mode. This mode of deployment achieves the maximum throughput for each Controller model, especially when using the APs in Tunnel mode where all the traffic will be tunneled by the APs to the controller and then to the Network.

- Dedicated Deployment: Dedicated NIC, vSwitch and vPort Group
- (MC-VE Series Only) Shared Deployment: Sharing NIC with existing vSwitch

Start the **VMware vSphere Client**, and log in to the ESXi server. Go to **Configuration** and click **Networking.**

As you can see, there are existing 2 VM running on the host, using the same vSwitch0 and same Virtual Machine port Group. The vSwitch is also used by the vKernel Port that is responsible for the ESXi management.



View: vSphere Standard Switch

Networking

Standard Switch: vSwitch0

Management Network
vmk0 : 172.31.11.47
fe80::225:90ff:fe64:67c4

VM Network
2 virtual machine(s)
Windows2008R2-Education
CentOS6.5

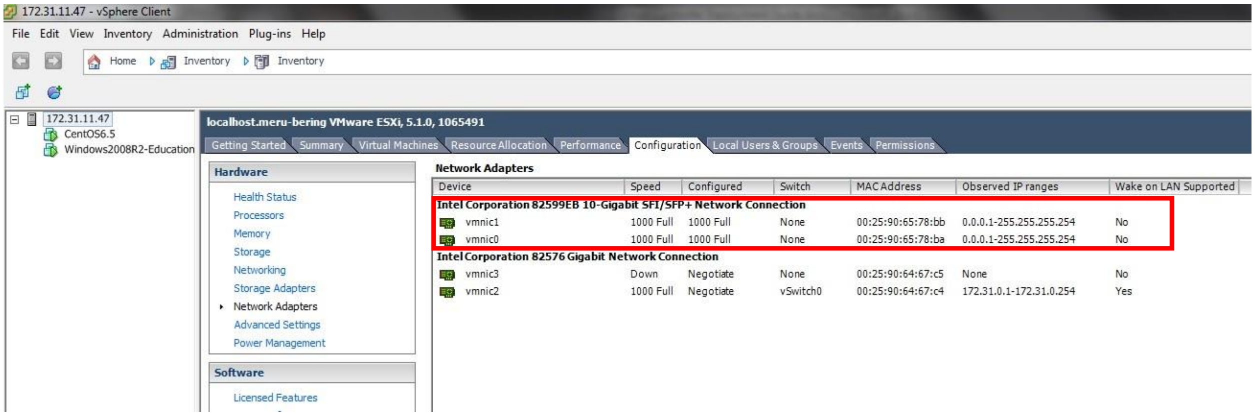
vmnic2 1000 Full

Downloading the Virtual Controller Package File

You can download the virtual controller packages from the Fortinet Customer Support website. To access the support website you need a Fortinet Customer Support account.
The file name is, *forti-x.x-xbuild-0-x86_64.ova*, where x.x-x is the release version number. For example, 8.3.2.

Configuring Dedicated Deployment

In this deployment, we will be using an added NIC card with 2 Gig Ethernet ports as shown in the **Network Adapters** wizard.

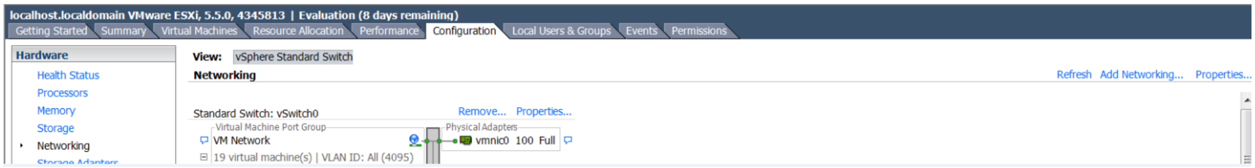


Network Adapters

Device	Speed	Configured	Switch	MAC Address	Observed IP ranges	Wake on LAN Supported
Intel Corporation 82599EB 10-Gigabit SFI/SFP+ Network Connection						
vmnic1	1000 Full	1000 Full	None	00:25:90:65:78:bb	0.0.0.1-255.255.255.254	No
vmnic0	1000 Full	1000 Full	None	00:25:90:65:78:ba	0.0.0.1-255.255.255.254	No
Intel Corporation 82576 Gigabit Network Connection						
vmnic3	Down	Negotiate	None	00:25:90:64:67:c5	None	No
vmnic2	1000 Full	Negotiate	vSwitch0	00:25:90:64:67:c4	172.31.0.1-172.31.0.254	Yes

These 2 Gig Interface are connected to a Switch that support Link Aggregation (LAG). It is assumed in this procedure that the LAG is created on the switch and has the appropriate VLAN configuration. Refer to the VLAN deployment guide for the Fortinet Controllers.

1. Create a new Virtual Switch: Go to **Networking** and click **Add Networking…**



localhost.localdomain VMware ESXi, 5.5.0, 4345813 | Evaluation (8 days remaining)

View: vSphere Standard Switch

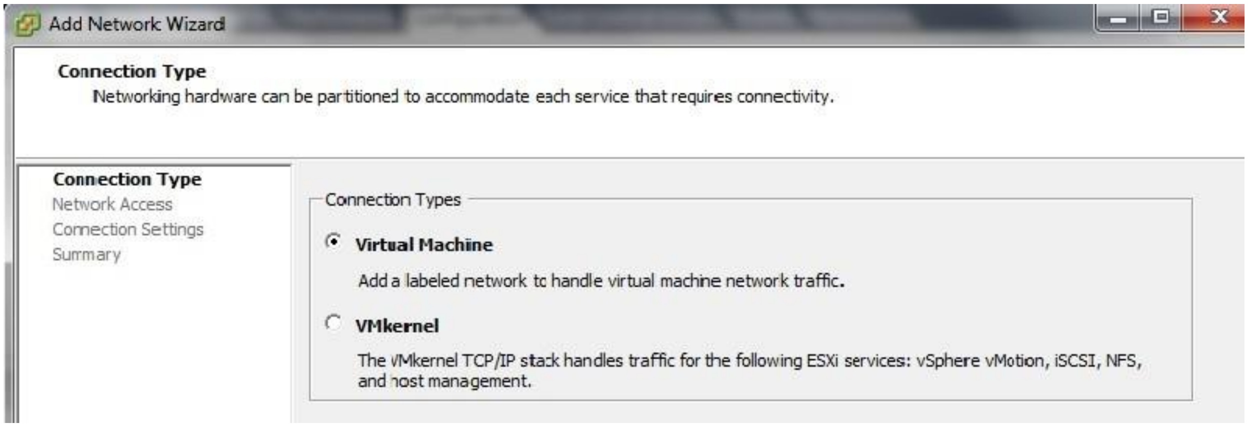
Networking

Standard Switch: vSwitch0

Virtual Machine Port Group: VM Network — 19 virtual machine(s) | VLAN ID: All (4095)

Physical Adapters: vmnic0 100 Full

2. Select **Virtual Machine** and click **Next**.



Add Network Wizard

Connection Type

Networking hardware can be partitioned to accommodate each service that requires connectivity.

Connection Types

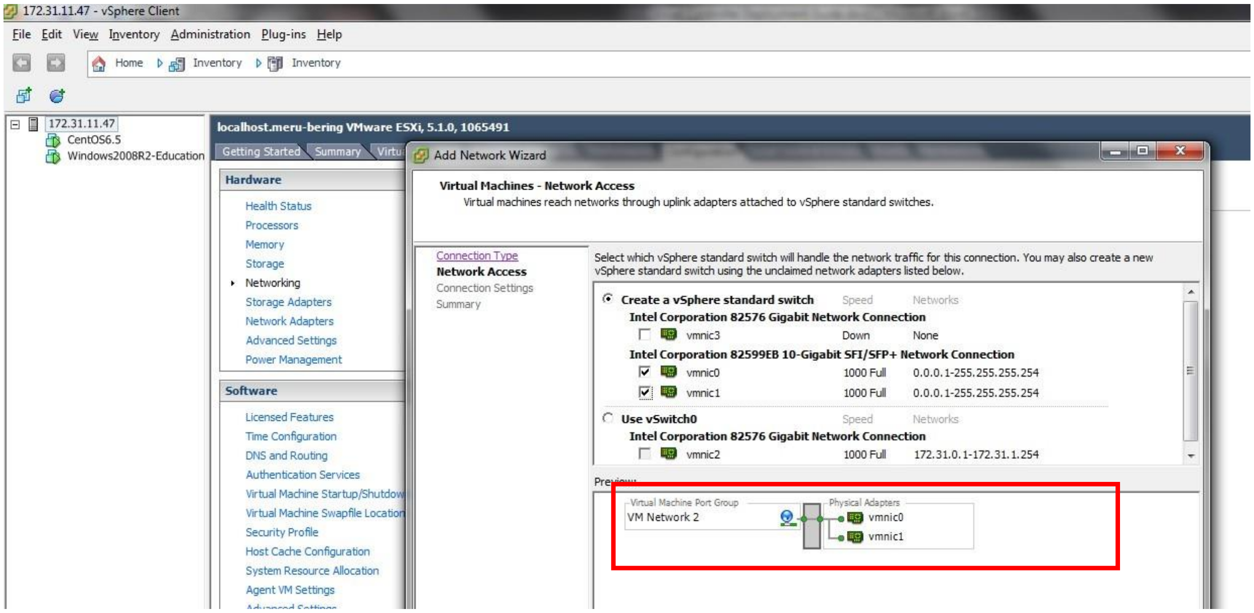
● **Virtual Machine**

Add a labeled network to handle virtual machine network traffic.

○ **VMkernel**

The VMkernel TCP/IP stack handles traffic for the following ESXi services: vSphere vMotion, iSCSI, NFS, and host management.

Create a vSwitch and assign the dedicated physical NIC. Click **Next** and provide and label for the vSwitch, for example, FWC-VM-50.



172.31.11.47 - vSphere Client

localhost.meru-bering VMware ESXi, 5.1.0, 1065491

Add Network Wizard

Virtual Machines - Network Access

Virtual machines reach networks through uplink adapters attached to vSphere standard switches.

Select which vSphere standard switch will handle the network traffic for this connection. You may also create a new vSphere standard switch using the unclaimed network adapters listed below.

● **Create a vSphere standard switch** — Speed — Networks

Intel Corporation 82576 Gigabit Network Connection

☐ vmnic3 — Down — None

Intel Corporation 82599EB 10-Gigabit SFI/SFP+ Network Connection

☑ vmnic0 — 1000 Full — 0.0.0.1-255.255.255.254

☑ vmnic1 — 1000 Full — 0.0.0.1-255.255.255.254

○ **Use vSwitch0** — Speed — Networks

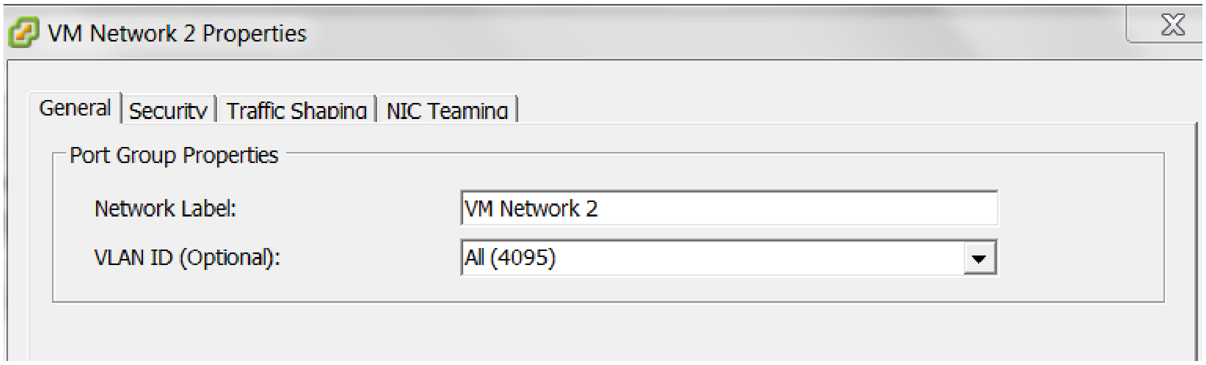
Intel Corporation 82576 Gigabit Network Connection

☐ vmnic2 — 1000 Full — 172.31.0.1-172.31.1.254

Preview:

Virtual Machine Port Group: VM Network 2 — Physical Adapters: vmnic0, vmnic1

3. For VLAN ID, select **All (4095)**, if you are using Trunk port on the switch. Click **Next** and then **Finish** to complete the vSwitch creation.

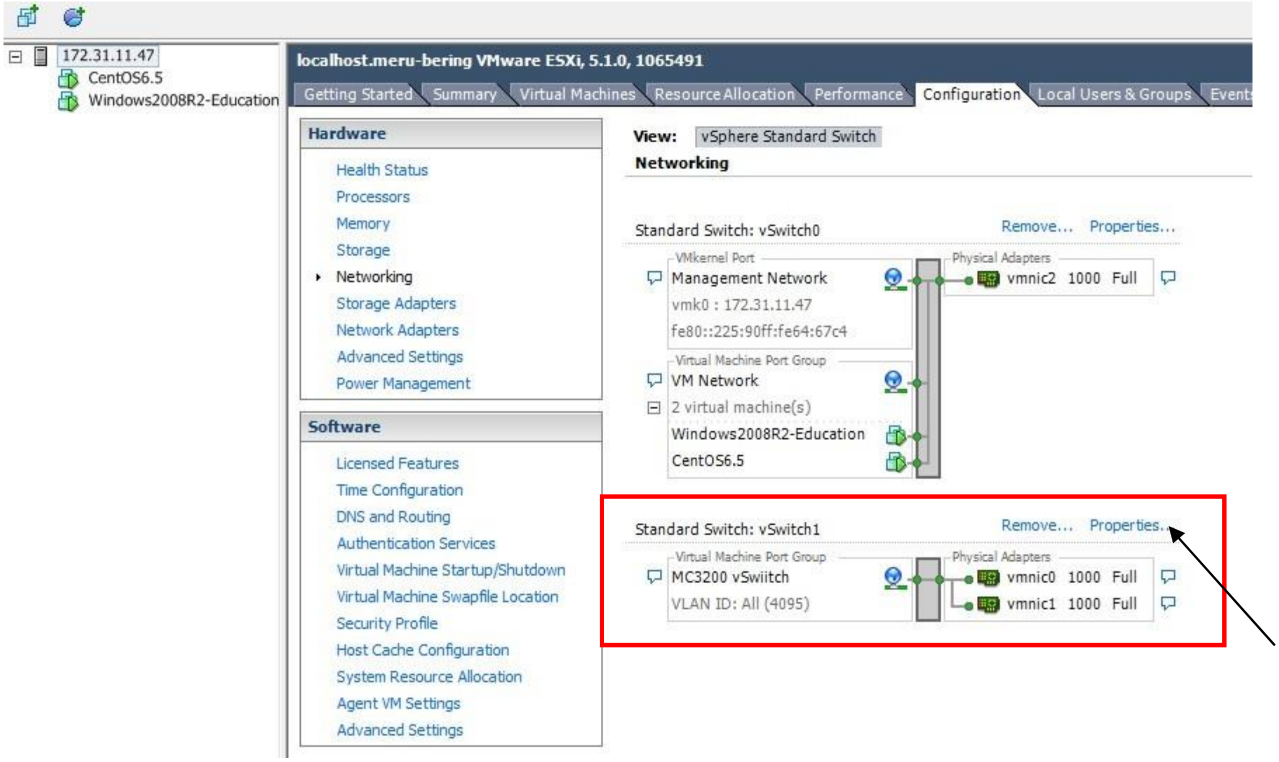


Port Group Properties

Network Label: VM Network 2

VLAN ID (Optional): All (4095)

4. The end result of adding the vSwitch will result in vSwitch 1 and a virtual machine port group named MC3200 vSwitch.



Standard Switch: vSwitch0

VMkernel Port: Management Network, vmk0 : 172.31.11.47, fe80::225:90ff:fe64:67c4

Physical Adapters: vmnic2 1000 Full

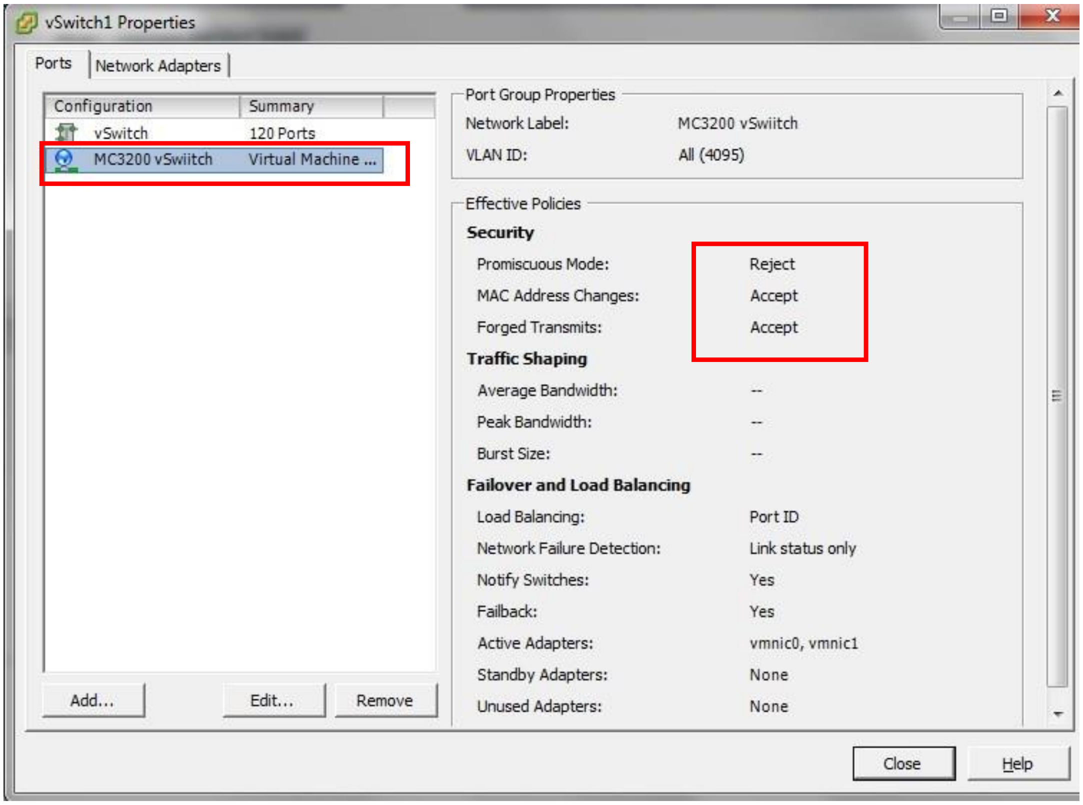
Virtual Machine Port Group: VM Network, 2 virtual machine(s), Windows2008R2-Education, CentOS6.5

Standard Switch: vSwitch1

Virtual Machine Port Group: MC3200 vSwiitch, VLAN ID: All (4095)

Physical Adapters: vmnic0 1000 Full, vmnic1 1000 Full

5. Click on vSwitch1 **Properties**, select **MC3200 vSwitch** port group and click **Edit.**



Configuration	Summary
vSwitch	120 Ports
MC3200 vSwiitch	Virtual Machine ...

Port Group Properties

Network Label: MC3200 vSwiitch

VLAN ID: All (4095)

Effective Policies

Security

Promiscuous Mode: Reject

MAC Address Changes: Accept

Forged Transmits: Accept

Traffic Shaping

Average Bandwidth: --

Peak Bandwidth: --

Burst Size: --

Failover and Load Balancing

Load Balancing: Port ID

Network Failure Detection: Link status only

Notify Switches: Yes

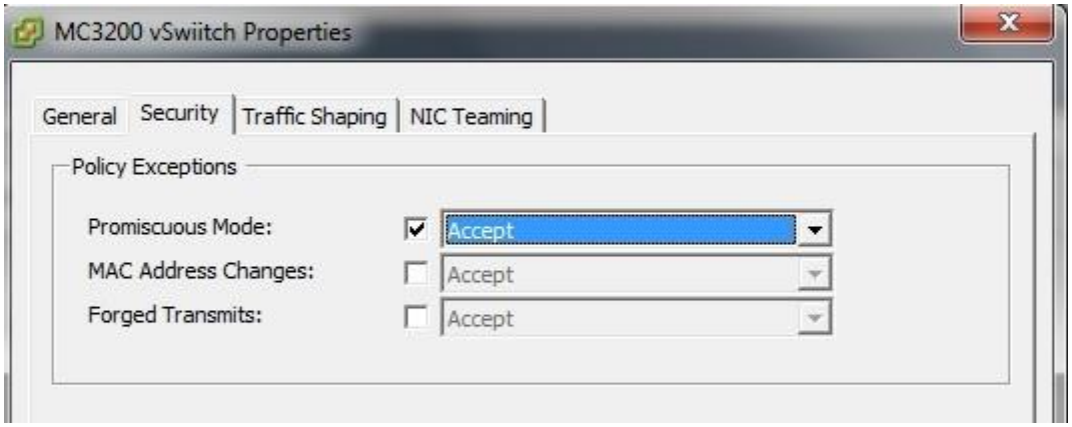
Failback: Yes

Active Adapters: vmnic0, vmnic1

Standby Adapters: None

Unused Adapters: None

6. Under the **Security** tab, select the **Promiscuous Mode** and select **Accept** from the drop menu and click **OK** to apply the changes.



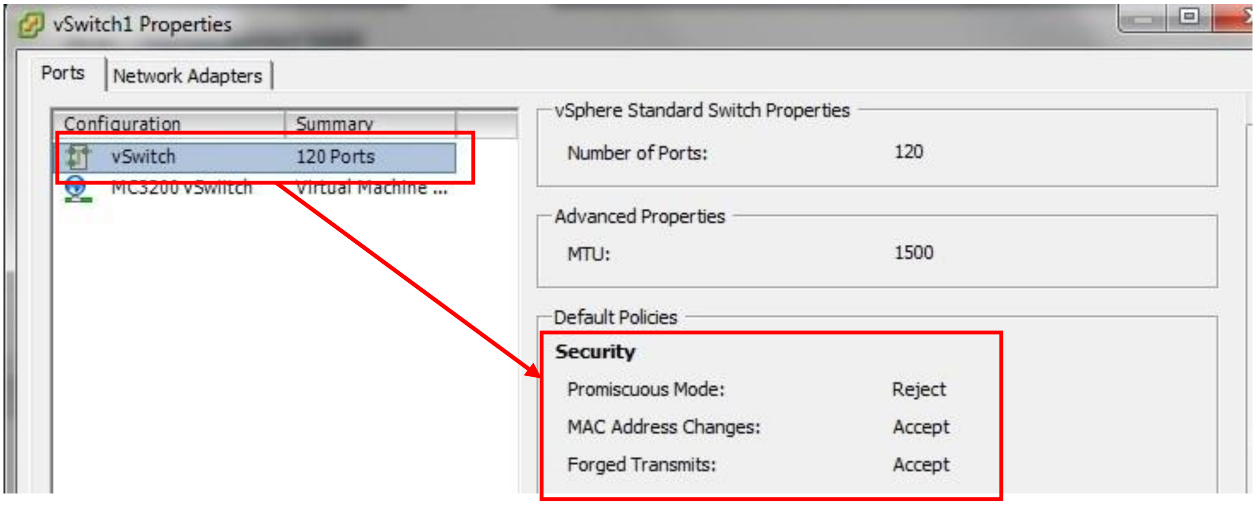
Policy Exceptions

Promiscuous Mode: ☑ Accept

MAC Address Changes: □ Accept

Forged Transmits: □ Accept

Note: The vSwitch main configuration is set to reject the Promiscuous mode, but the virtual machine port group overwrites the vSwitch configuration and operates in a Promiscuous Mode for the MC3200 vSwitch port group.



Configuration	Summary
vSwitch	120 Ports
MC3200 vSwitch	Virtual Machine ...

vSphere Standard Switch Properties

Number of Ports: 120

Advanced Properties

MTU: 1500

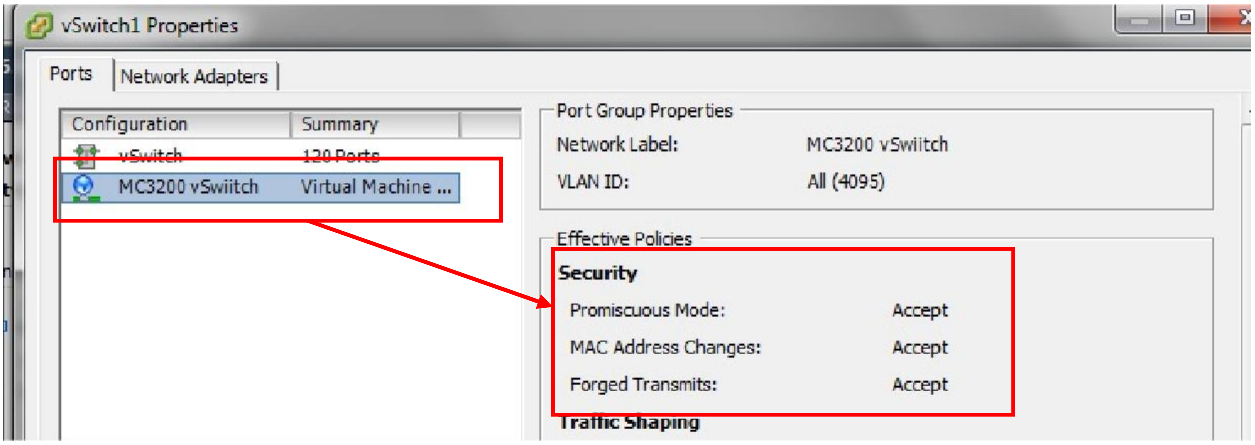
Default Policies

Security

Promiscuous Mode: Reject

MAC Address Changes: Accept

Forged Transmits: Accept



Configuration	Summary
vSwitch	120 Ports
MC3200 vSwiitch	Virtual Machine ...

Port Group Properties

Network Label: MC3200 vSwiitch

VLAN ID: All (4095)

Effective Policies

Security

Promiscuous Mode: Accept

MAC Address Changes: Accept

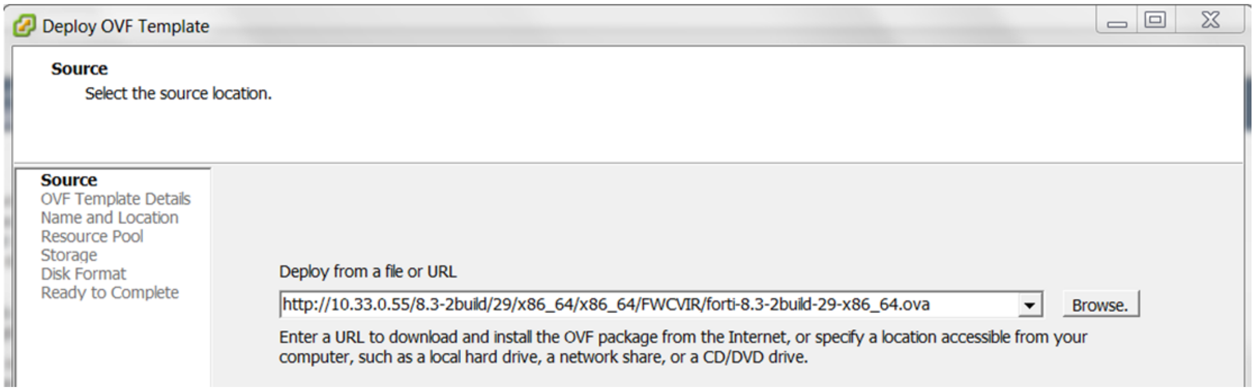
Forged Transmits: Accept

Traffic Shaping

Each vNIC has to be a part of a different Vswitch connected to different physical ports. Now that the structure is ready, start installing the OVA template into the VMware host.

Installing the Virtual Controller

1. Go to **File** and click **Deploy OVF Template…** in order to start the installation.
2. Browse to the location of the OVA template that you downloaded from Fortinet Support page and click **Next.**



Source

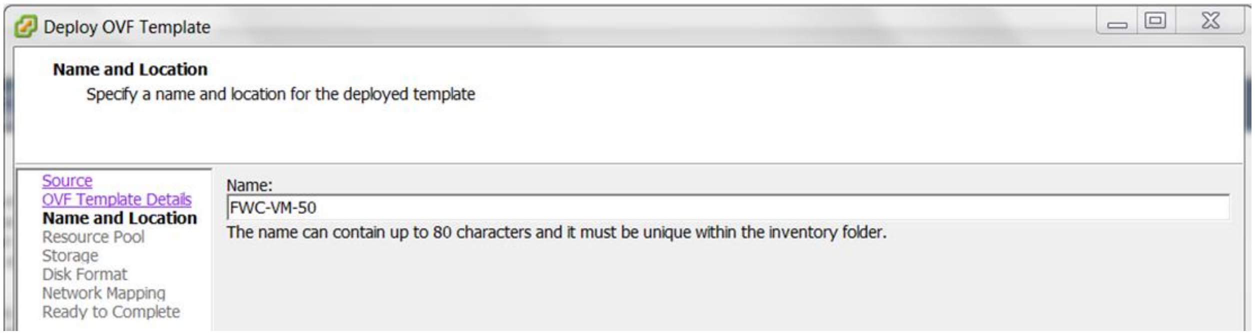
Select the source location.

Deploy from a file or URL

http://10.33.0.55/8.3-2build/29/x86_64/x86_64/FWCVIR/forti-8.3-2build-29-x86_64.ova

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

3. Click **Next** and enter a **Name** for the Virtual Controller, for example, MC3200VE-NorthCampus.



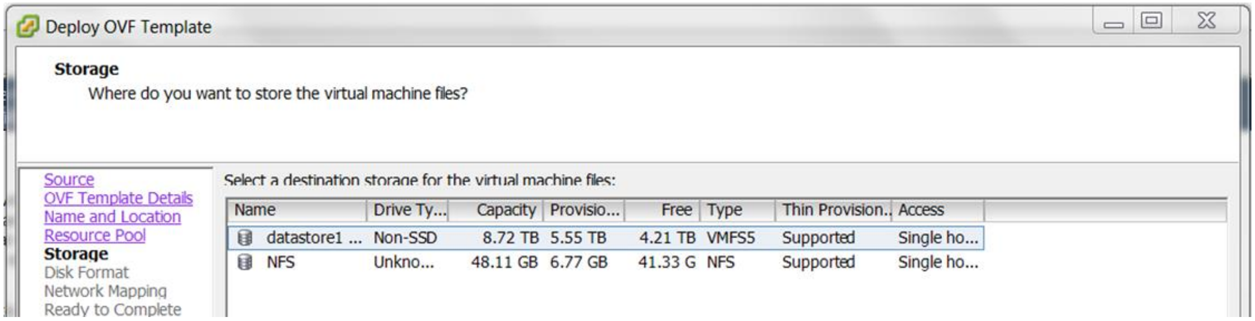
Name and Location
Specify a name and location for the deployed template

Name: FWC-VM-50

The name can contain up to 80 characters and it must be unique within the inventory folder.

4. Configure the following:

   - Resource Pool
   - Storage

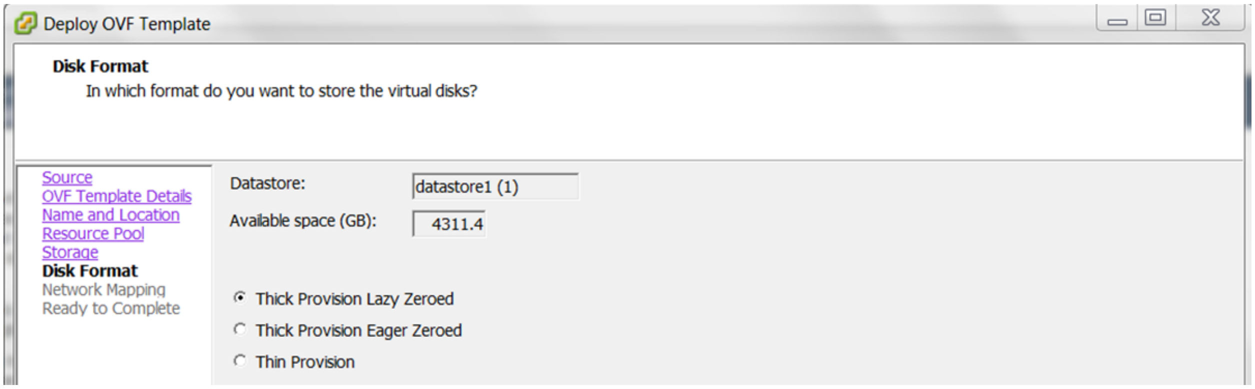


Storage
Where do you want to store the virtual machine files?

Select a destination storage for the virtual machine files:

Name	Drive Ty...	Capacity	Provisio...	Free	Type	Thin Provision..	Access
datastore1 ...	Non-SSD	8.72 TB	5.55 TB	4.21 TB	VMFS5	Supported	Single ho...
NFS	Unkno...	48.11 GB	6.77 GB	41.33 G	NFS	Supported	Single ho...

   - Disk Format, use the default for the disk format, **Thick Provisioning Lazy Zereod**.



Disk Format
In which format do you want to store the virtual disks?

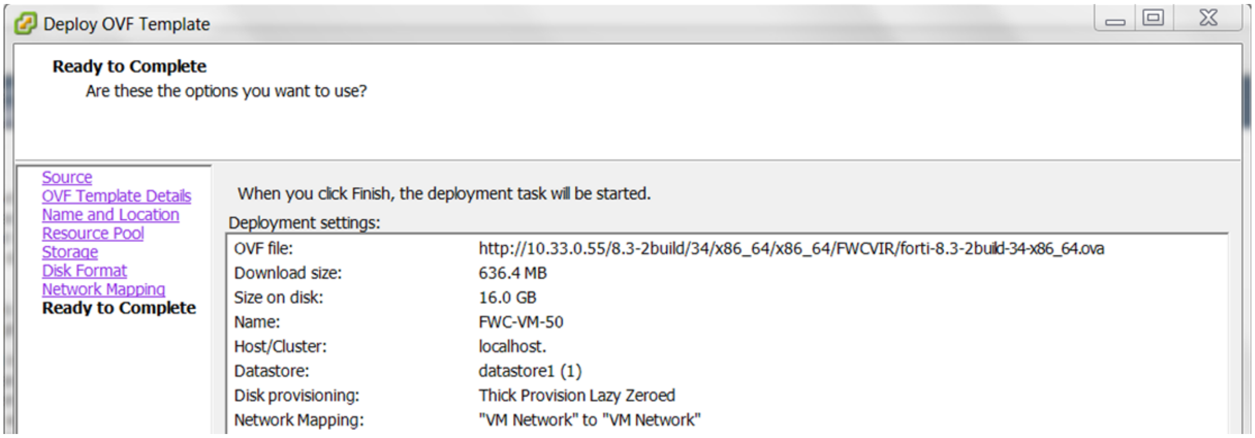
Datastore: datastore1 (1)

Available space (GB): 4311.4

● Thick Provision Lazy Zeroed
○ Thick Provision Eager Zeroed
○ Thin Provision

   - Network Mapping.

5. Click **Finish** in the **Ready to Complete** wizard**.**



Ready to Complete

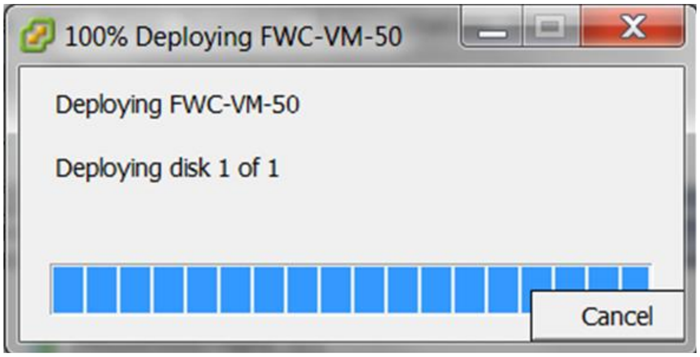
Are these the options you want to use?

When you click Finish, the deployment task will be started.

Deployment settings:

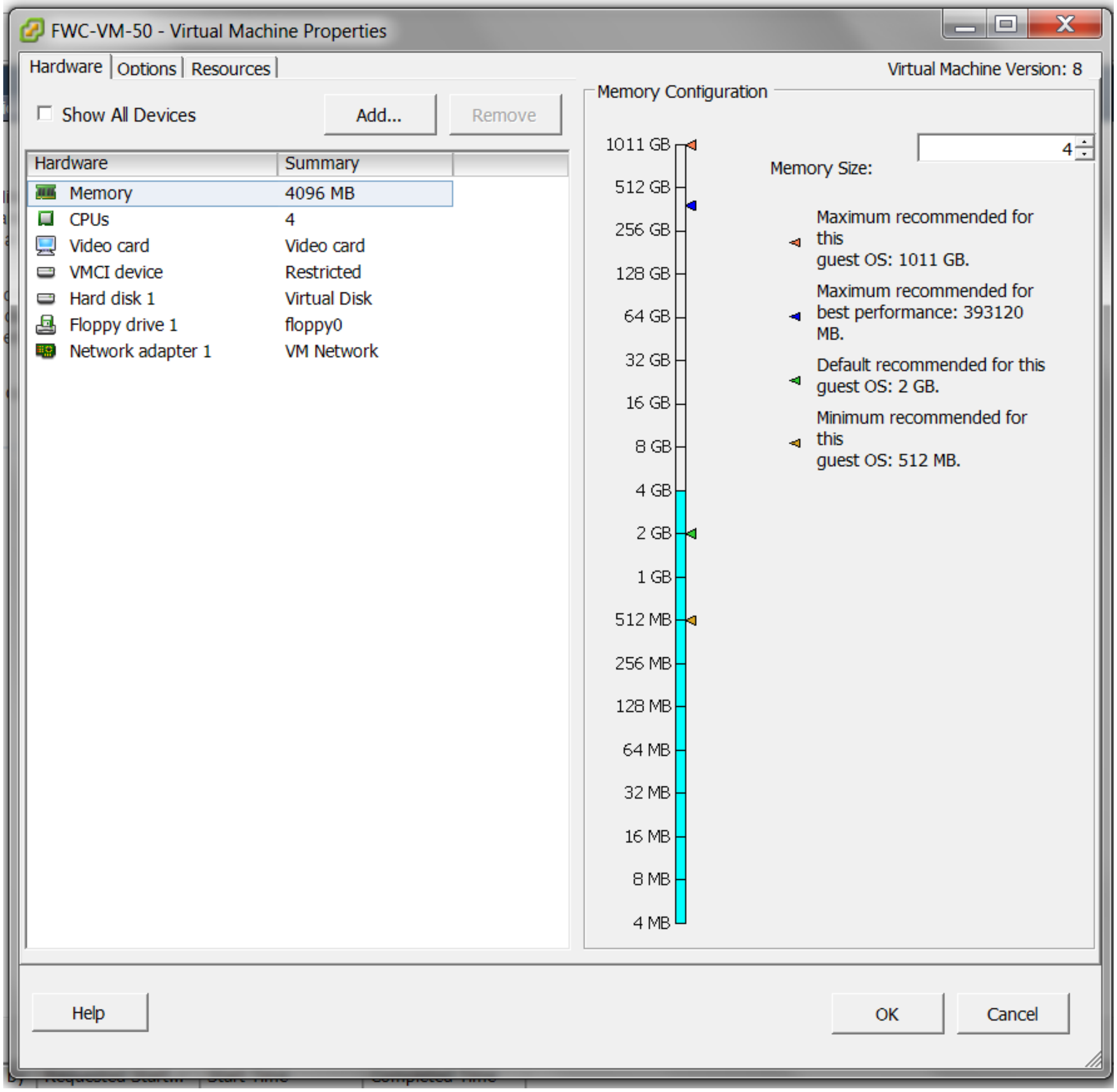
OVF file:	http://10.33.0.55/8.3-2build/34/x86_64/x86_64/FWCVIR/forti-8.3-2build-34-x86_64.ova
Download size:	636.4 MB
Size on disk:	16.0 GB
Name:	FWC-VM-50
Host/Cluster:	localhost.
Datastore:	datastore1 (1)
Disk provisioning:	Thick Provision Lazy Zeroed
Network Mapping:	"VM Network" to "VM Network"

The upload and installation of the Virtual Controller will start, the time varies according to the network bandwidth between the vSphere Client and the ESXi Host. You should get a **Completed Successfully** message at the end.



Deploying FWC-VM-50

Deploying disk 1 of 1



FWC-VM-50 - Virtual Machine Properties

Hardware | Options | Resources

Virtual Machine Version: 8

☐ Show All Devices

Hardware	Summary
Memory	4096 MB
CPUs	4
Video card	Video card
VMCI device	Restricted
Hard disk 1	Virtual Disk
Floppy drive 1	floppy0
Network adapter 1	VM Network

Memory Configuration

Memory Size: 4

Maximum recommended for this guest OS: 1011 GB.

Maximum recommended for best performance: 393120 MB.

Default recommended for this guest OS: 2 GB.

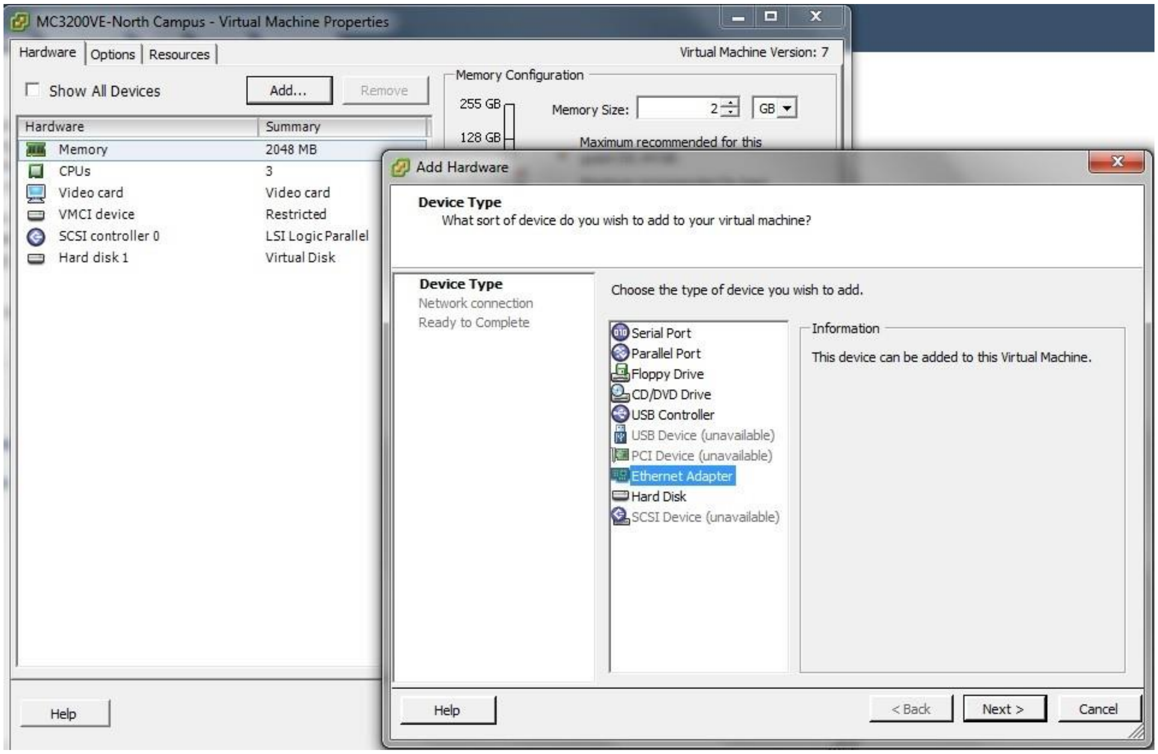
Minimum recommended for this guest OS: 512 MB.

Configuring Virtual Controller Settings

After creating the virtual controller, configure the virtual machine settings and add the needed network adapters.

1. Select the Virtual Controller created above (MC3200VE-North Campus) and click **Edit virtual machine settings** in the **Getting Started** tab.

2. Click on **Add** and select **Ethernet Adapter.**



Hardware	Summary
Memory	2048 MB
CPUs	3
Video card	Video card
VMCI device	Restricted
SCSI controller 0	LSI Logic Parallel
Hard disk 1	Virtual Disk

Device Type
What sort of device do you wish to add to your virtual machine?

Device Type
Network connection
Ready to Complete

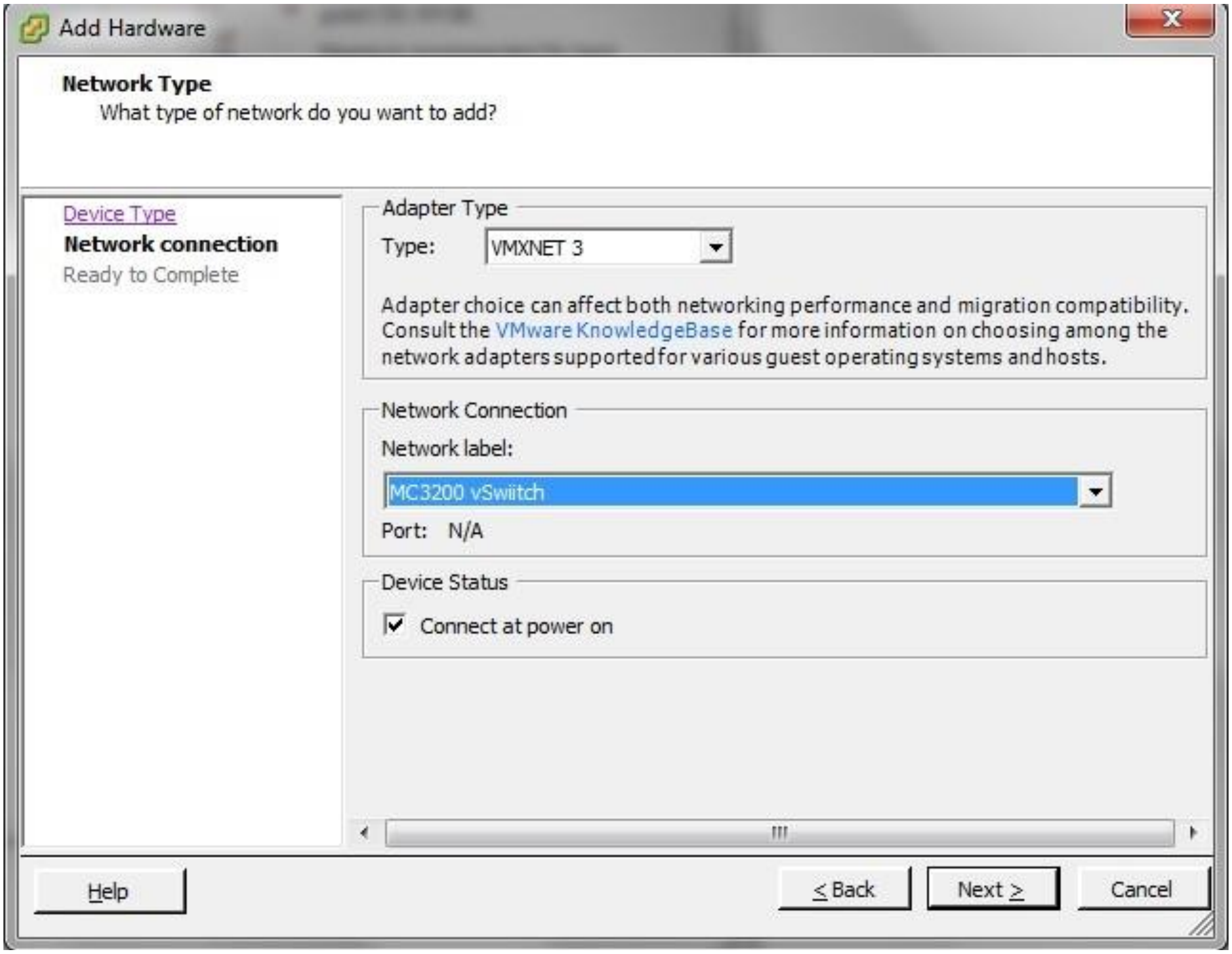
Choose the type of device you wish to add.

- Serial Port
- Parallel Port
- Floppy Drive
- CD/DVD Drive
- USB Controller
- USB Device (unavailable)
- PCI Device (unavailable)
- Ethernet Adapter
- Hard Disk
- SCSI Device (unavailable)

Information
This device can be added to this Virtual Machine.

Click **Next**, choose **VMXNET 3** and choose the **Network Connection** (port group) created above (MC3200 vSwitch) and then click **Next** and **Finish**. (Other drivers supported are E1000, VMXNET and VMXNET 2. The latest VMXNET 3 is needed to support the 10GB connection for the Virtual Controller.

3. Use 1 or more Ethernet adapters as recommended in section Supported Hardware Configuration. Adding more than 1 will cause duplicate packets, see the FortiWLC Release Notes for limitations.



Adapter Type

Type: VMXNET 3

Adapter choice can affect both networking performance and migration compatibility. Consult the VMware KnowledgeBase for more information on choosing among the network adapters supported for various guest operating systems and hosts.

Network Connection

Network label: MC3200 vSwitch

Port: N/A

Device Status

☑ Connect at power on

Configuring Shared Deployment

Note: This deployment mode applies only to the MC-VE Series Virtual Controllers.

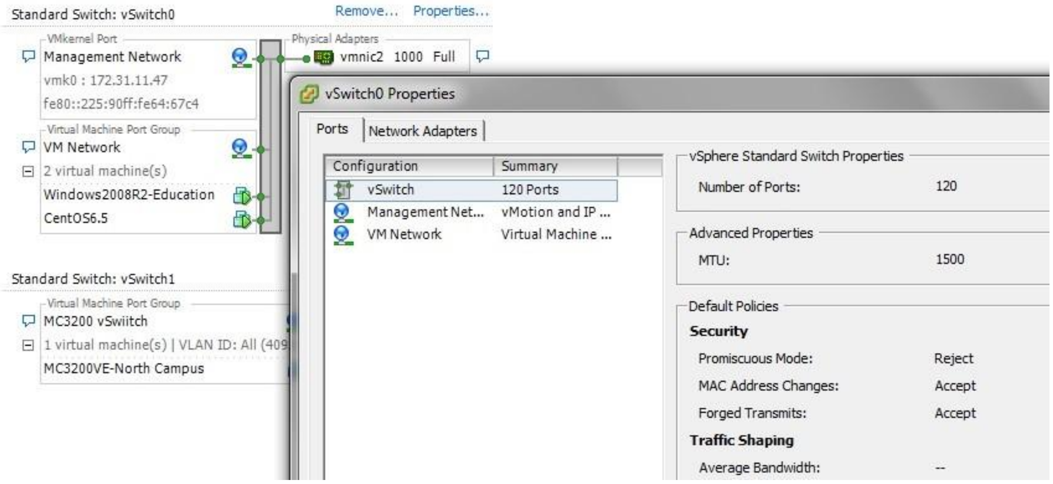
In this deployment, an existing NIC card is used where the Ethernet port is used by other VM already running on the Hypervisor.

Since the Virtual Controller requires Promiscuous Mode in order to operate, a new Virtual Machine port group is created in the vSwitch where the Virtual Controller is added.

In this example, an MC1550VE is added to vSwitch0 where a CentOS VM and a Windows 2008 Server are sharing the same Ethernet port.

Follow these steps to complete the installation

1. Login to the ESXi and go to **Networking**. Locate the vSwitch0 and click on **Properties.**



Standard Switch: vSwitch0 Remove... Properties...

VMkernel Port
Management Network
vmk0 : 172.31.11.47
fe80::225:90ff:fe64:67c4

Physical Adapters
vmnic2 1000 Full

Virtual Machine Port Group
VM Network
2 virtual machine(s)
Windows2008R2-Education
CentOS6.5

Standard Switch: vSwitch1

Virtual Machine Port Group
MC3200 vSwiitch
1 virtual machine(s) | VLAN ID: All (409
MC3200VE-North Campus

vSwitch0 Properties

Ports | Network Adapters

Configuration	Summary
vSwitch	120 Ports
Management Net...	vMotion and IP ...
VM Network	Virtual Machine ...

vSphere Standard Switch Properties

Number of Ports: 120

Advanced Properties

MTU: 1500

Default Policies

Security

Promiscuous Mode: Reject

MAC Address Changes: Accept

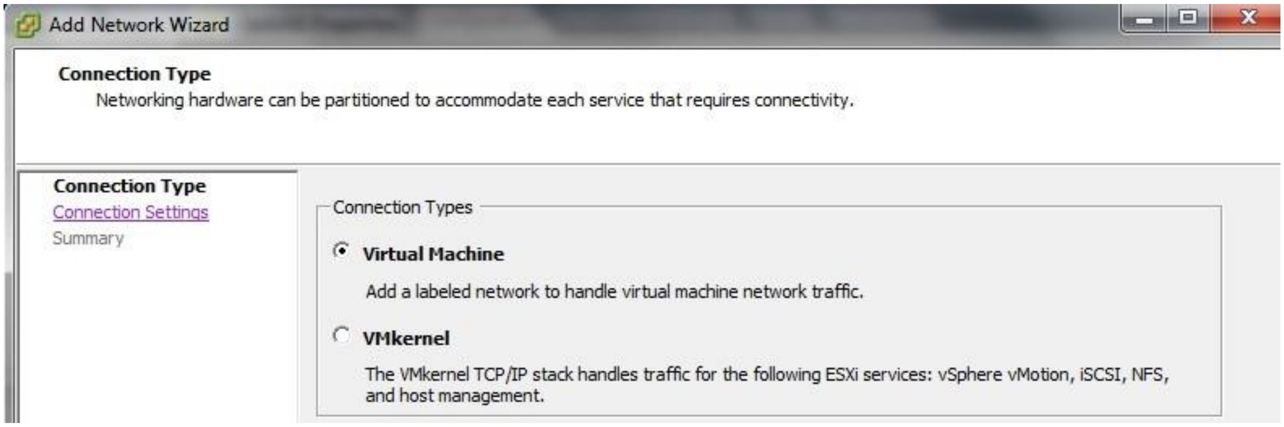
Forged Transmits: Accept

Traffic Shaping

Average Bandwidth: --

The vSwitch has the Promiscuous Mode set to **Reject**.

2. Click on **Add**, select **Virtual Machine** and click **Next**.



Add Network Wizard

Connection Type

Networking hardware can be partitioned to accommodate each service that requires connectivity.

Connection Type
Connection Settings
Summary

Connection Types

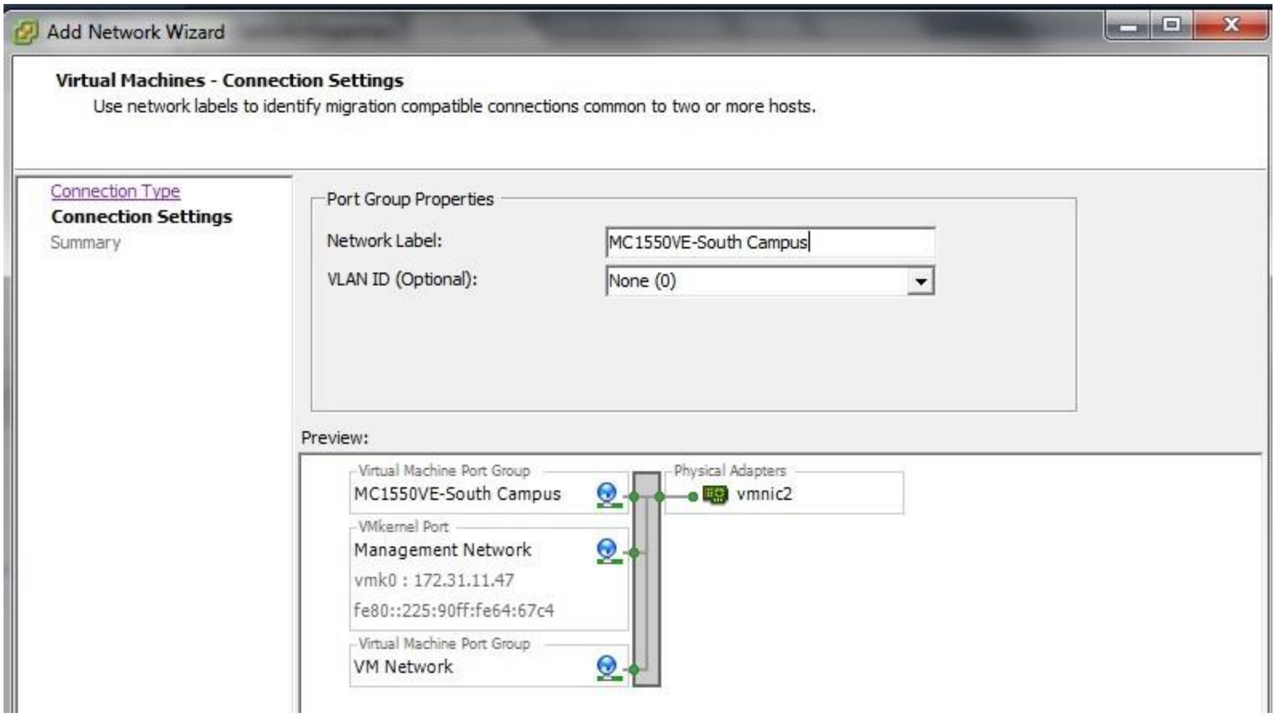
● **Virtual Machine**

Add a labeled network to handle virtual machine network traffic.

○ **VMkernel**

The VMkernel TCP/IP stack handles traffic for the following ESXi services: vSphere vMotion, iSCSI, NFS, and host management.

3. Add a **Network label** to the **Virtual Machine Port Group** (MC1550VE-South Campus), click **Next** and then **Finish.**



Add Network Wizard

Virtual Machines - Connection Settings

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

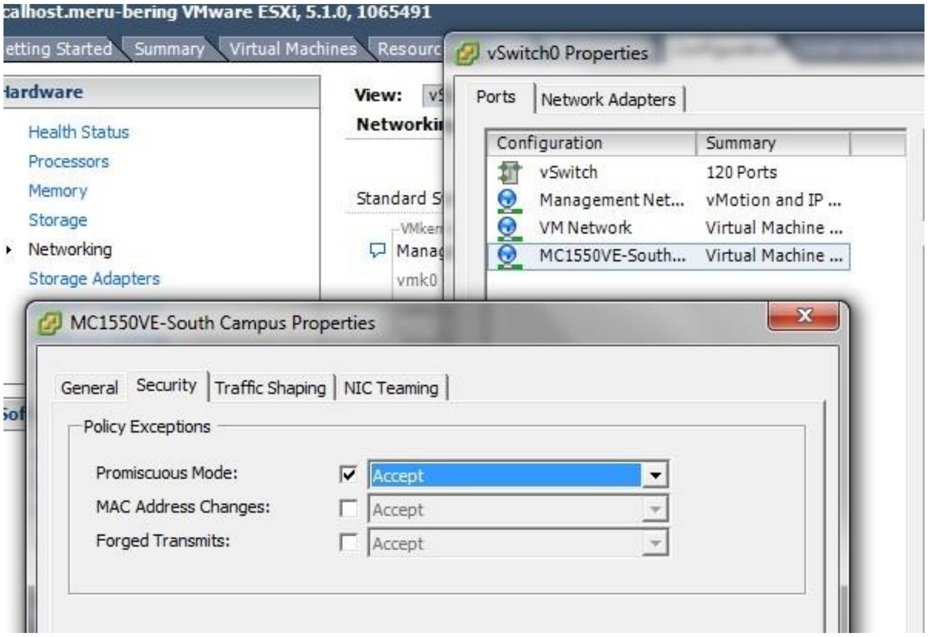
Port Group Properties

Network Label: MC1550VE-South Campus

VLAN ID (Optional): None (0)

Preview:

Select the newly created port group and **Edit** the settings. Under the **Security** tab, change the **Promiscuous Mode** to **Accept** and click **OK**.



calhost.meru-bering VMware ESXi, 5.1.0, 1065491

vSwitch0 Properties

Configuration	Summary
vSwitch	120 Ports
Management Net...	vMotion and IP ...
VM Network	Virtual Machine ...
MC1550VE-South...	Virtual Machine ...

MC1550VE-South Campus Properties

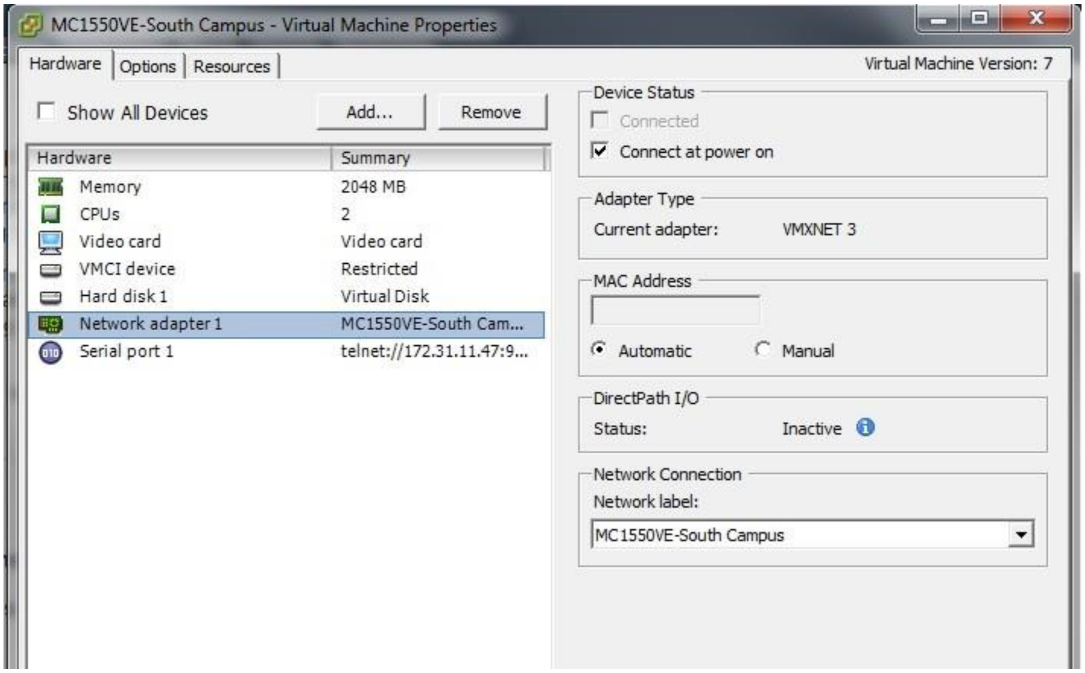
Policy Exceptions

Promiscuous Mode: ☑ Accept

MAC Address Changes: □ Accept

Forged Transmits: □ Accept

Now that the infrastructure is ready, you can install the OVA as described in the previous section. Add the **Network Adapter** and map the Virtual Controller Ethernet to the **Virtual Machine Port Group** that was created (MC1550VE-South Campus).



Virtual Machine Version: 7

□ Show All Devices

Hardware	Summary
Memory	2048 MB
CPUs	2
Video card	Video card
VMCI device	Restricted
Hard disk 1	Virtual Disk
Network adapter 1	MC1550VE-South Cam...
Serial port 1	telnet://172.31.11.47:9...

Device Status

□ Connected

☑ Connect at power on

Adapter Type

Current adapter: VMXNET 3

MAC Address

● Automatic ○ Manual

DirectPath I/O

Status: Inactive

Network Connection

Network label: MC1550VE-South Campus

Starting the Virtual Controller

Select the Controller and go to the **Console** Tab and Start the VM by clicking on the Power On button or (Ctrl+b). The Virtual Controller will start and you will see the entire startup message that you will typically found in a Hardware Controller.

The first boot might take few minutes longer to boot up if no DHCP server is available as the controller will try to get an IP address from the DHCP server. Please refer to the Controller SD documentation to complete the controller installation.

Recommended VMware ESXi Host Settings

Fortinet recommends the following VM configurations and global host settings for enhanced Controller performance.

VM Configuration Settings

- CPU affinity - In servers where the available physical cores (i.e. half of HT CPUs) are more than the required cores for Controllers, set the CPU affinity such that no two vCPUs are scheduled on the same physical core by the VMKernel.
  To set the CPU range, go to **Edit Settings ->Virtual Hardware -> CPU -> Scheduling Affinity**.
- Latency Sensitivity - Set the Latency sensitivity to **High**, to do so, go to **Edit Settings -> VM Options -> Advanced -> Latency Sensitivity**.
- Virtual NIC settings - Disable virtual interrupt coalescing, to do so, go **to Edit Settings -> Options tab -> Advanced -> Configuration Parameters** and add an entry for **ethernetX.coalescingScheme** with the value **disabled**.

Global Host Settings

- Physical NIC settings – Disable the interrupt moderation/coalescing. Run the **esxcli system module parameters set -m ixgbe -p "InterruptThrottleRate=0"** CLI command.
  This is applicable to Intel 10G with ixgbe driver, that is, chipsets Intel 82599 and is not applicable or i40en based drivers. Run the **esxcli network nic list** CLI command to find the list of drivers.
- Set the **/Net/MaxNetifTxQueueLen** global parameter to 10000 (default is 2000). Run the **esxcli system settings advanced set -o /Net/MaxNetifTxQueueLen -i=10000** CLI command.
- Set the **/Net/NetVMTxType** global parameter to 3 (applicable only for ESXi 6.5). Run the **esxcli system settings advanced set -o /Net/NetVMTxType -i=3** CLI command.
  This allocates multiple Tx world, that is, 1 per queue.

These are the parameters for different Controller models.

Parameters	FWC-VM-50	FWC-VM-200	FWC-VM-500 (10G)	FWC-VM-1000	FWC-VM-3000	FWC-VM-500-(1G)
CPU affinity	Yes	Yes	Yes	Yes	No (Applicable only if the number of physical cores on the host are more than 48.)	Yes
Latency Sensitivity	High	High	High	High	High	High
Virtual NIC settings (Disable interrupt coalescing)	Yes	Yes	Yes	Yes	No	Yes
/Net/MaxNetifTxQueueLen	1000	1000	10000	10000	10000	1000
/Net/NetVMTxType (for ESXi 6.5 and above)	1	1	3	3	3	1

Deploying Fortinet Virtual Controllers with Linux KVM

Pre-requisites

For deployment and management of the Virtual Controller on Linux KVM, install the following 3rd party software.

- Install Ubuntu v16.04 LTS server.
- Install KVM on the Ubuntu LTS server.
- Create an open Vswitch with KVM.
- Install Virtual Machine Manage (virt-manager) to create and manage guest virtual machines.

Note: To accomplish the pre-requisites refer to the respective 3rd party documentation.

Downloading the Virtual Controller Package File

You can download the virtual controller packages from the Fortinet Customer Support website. To access the support website you need a Fortinet Customer Support account.

The file name is, *forti-x.x-xbuild-0-x86_64.img.KVM.zip*, where x.x-x is the release version number. For example, 8.3.2.

Installing Linux KVM

1. Install Ubuntu 16.04.2 64-bit Desktop version.
2. Run the **apt-get install openssh-server** command to install openssh utility.

   Now, you should be able to ssh to the machine.
3. Run the **egrep -c '(vmx|svm)' /proc/cpuinfo** command to check whether the system supports Virtualization or not.

   If the output is 0, then the system does not support Virtualization. If the output is greater than 0 it means your system is set and ready to go for KVM installation.
4. Run the following commands to install openvswitch which is used for tagging and untagging the vlans created.
   - **apt-get install openvswitch openvswitch-common openvswitch-switch**
   - **/etc/init.d/openvswitch-switch start**
5. Run the following commands to create a virtual-bridge.
   - **ovs-vsctl add-br <bridge-name:(user-defined)>**
   - **ovs-vsctl port <port-name:(user-defined) <eth-intf: name of the physical Ethernet port>**
   - **ovs-vsctl set port vnet0 trunks=0,168,169**.

     In this command 168 and 169 are tagged vlans and 0 is a mandatory argument which specifies the native-vlan.
   - **dhclient <<bridge-name:(user-defined)>**
6. Run the **ovs-vsctl show** command to see the virtual switch created. This is a sample command output:

   ```
   root@automation-HP-406-G1-MT:~# ovs-vsctl show
   52690264-a2da-4a63-86e9-c8ceabf9be72
       Bridge "N164-T168-T169" (N164-T168-T169:Bridge-name)
           Port "N164-T168-T169" (N164-T168-T169:port--name)
               Interface "N164-T168-T169"
                   type: internal
           Port "enp3s0" (enp3s0:physical Ethernet port name)
               Interface "enp3s0"
          Port "vnet0"
               trunks: [0, 168, 169]
               Interface "vnet0"
   ovs_version: "2.5.0"
   ```
7. Run the **sudo apt-get install qemu-kvm libvirt-bin ubuntu-vm-builder bridge-utils** command to install KVM.

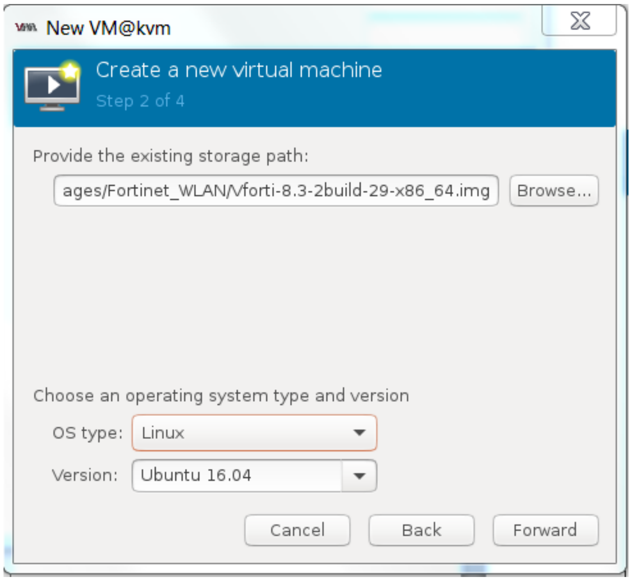
8. Run the **sudo adduser `id -username` libvirtd** command to ensure that your Ubuntu username is added to the group libvirtd.
9. Run the **sudo apt-get install virt-manager** command to install graphical user interface for KVM.
10. After the virt-manager is installed, type **virt-manager** to start the virtual manager application.
11. You can create a virtual Instance using GUI. In one of the window, you have to select **bridge interface vnet0.**
12. Create a virtual network:
    - Create a directory for storing the virtual network xml file, for example, mkdir vmswitch-xml.
    - Let the name of the xml file stored in the directory be *N164-T168-T169.xml*.
    - Contents of the xml file are as follows:

```
  <network>
 <name>N164</name>
 <forward mode='bridge'/>
 <bridge name='N164-T168-T169' />  #Created Bridge name
 <virtualport type='openvswitch'/>
 <portgroup name='N164-T168-T169'> #Created Port name
   <vlan trunk='yes'>
     <tag id='164' nativeMode='untagged'/>
     <tag id='168'/>  #tagged vlan
     <tag id='169'/> #tagged vlan
   </vlan>
 </portgroup>
</network>
```

13. Run the following commands to activate the created virtual network.
    - **virsh net-define N164-T168-T169.xml**
    - **virsh net-start N164**
14. Copy the image in the specified path and run the VM through virt-manager(GUI).
    - cd /var/lib/libvirt/images/
    - wget -c http://10.34.224.254/release/8.3-1build/11/x86_64/x86_64/FWCVIR/forti-8.3-1build-11-x86_64.img.KVM.zip *(this is a sample file)*.
    - Unzip forti-8.3-1build-11-x86_64.img.KVM.zip

Configuring the Virtual Controller

1. Open the virt-manager and select **Import Existing Disk Image**.
2. Browse to the location of the downloaded package file and specify the **OS type** as **Linux** and **Version** as **Ubuntu 16.04**.
3. Click **Forward**.



New VM@kvm

Create a new virtual machine

Step 2 of 4

Provide the existing storage path:

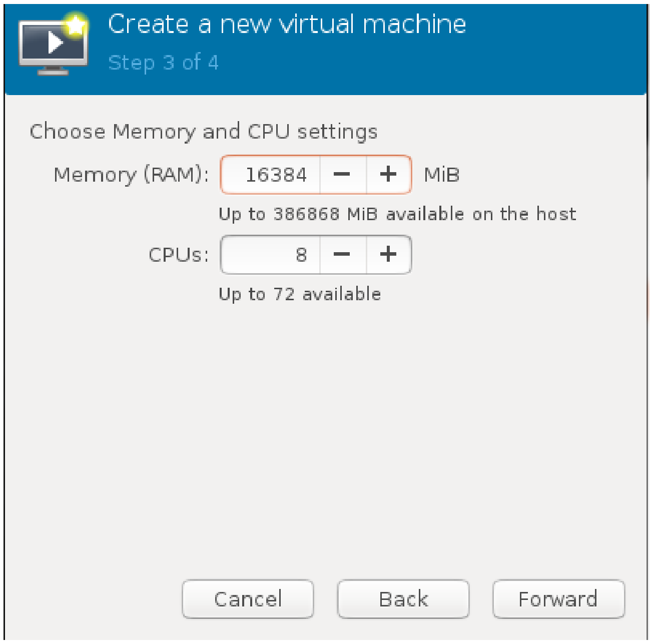
ages/Fortinet_WLAN/Vforti-8.3-2build-29-x86_64.img

Choose an operating system type and version

OS type: Linux

Version: Ubuntu 16.04

4. Specify the memory and CPU setting as per the deployed virtual controller model.



Create a new virtual machine

Step 3 of 4

Choose Memory and CPU settings

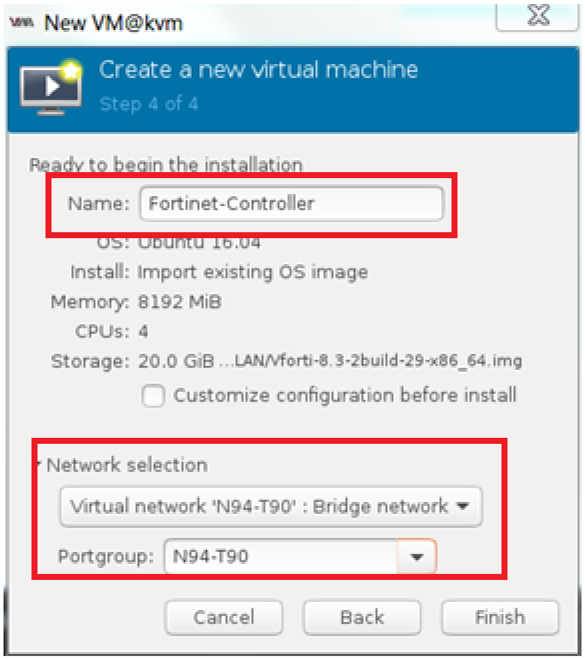
Memory (RAM): 16384 MiB

Up to 386868 MiB available on the host

CPUs: 8

Up to 72 available

5. Click **Forward**.
6. Specify the hostname, select the network adapter from the **Network Selection** drop down, and specify the **Portgroup**.



New VM@kvm

Create a new virtual machine

Step 4 of 4

Ready to begin the installation

Name: Fortinet-Controller

OS: Ubuntu 16.04

Install: Import existing OS image

Memory: 8192 MiB

CPUs: 4

Storage: 20.0 GiB ...LAN/Vforti-8.3-2build-29-x86_64.img

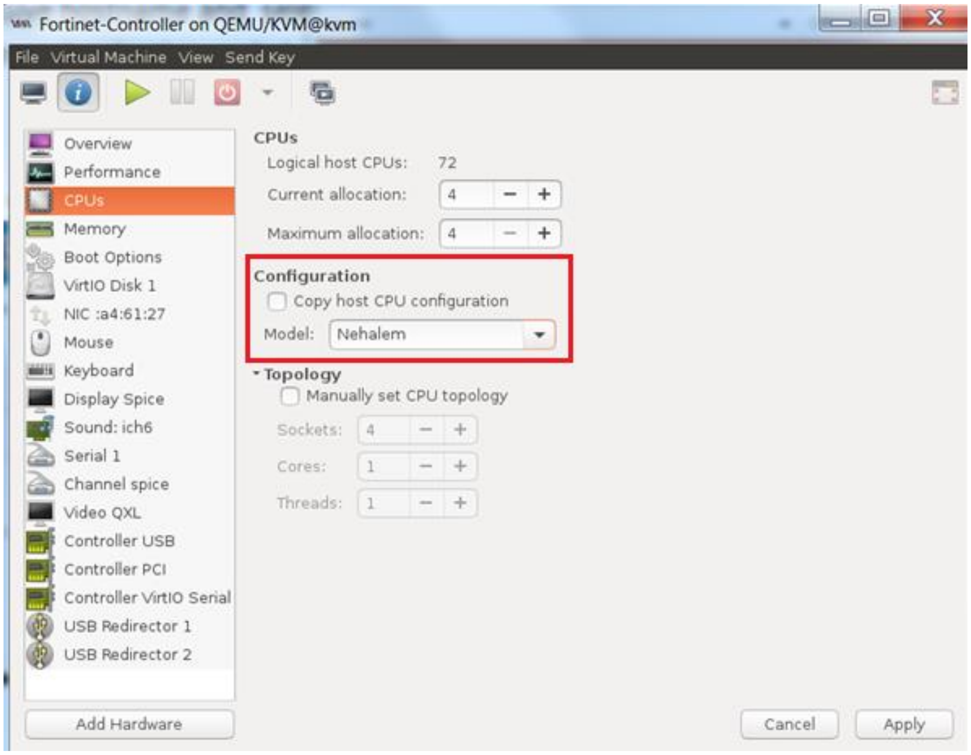
□ Customize configuration before install

Network selection

Virtual network 'N94-T90' : Bridge network

Portgroup: N94-T90

7. Click **Finish**.
8. In the **CPUs** settings, configure the **Model** as **Nehalem**. Click **Apply.**



Fortinet-Controller on QEMU/KVM@kvm

CPUs

Logical host CPUs: 72

Current allocation: 4

Maximum allocation: 4

Configuration

□ Copy host CPU configuration

Model: Nehalem

Topology

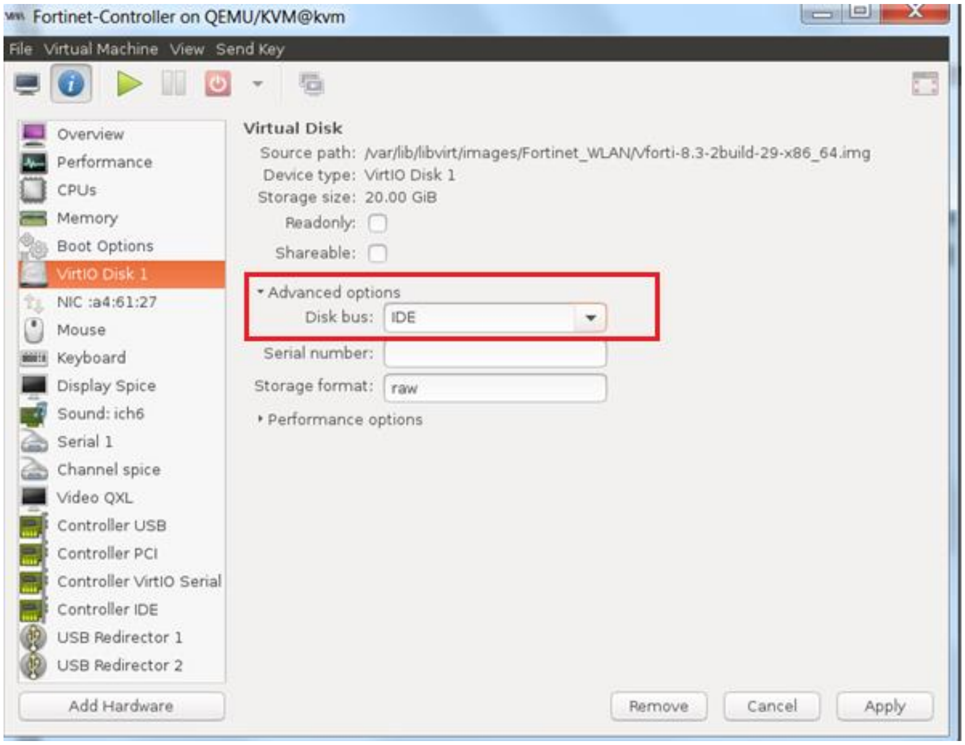
□ Manually set CPU topology

Sockets: 4

Cores: 1

Threads: 1

9. In the **VirtIO Disk1,** under **Advanced options,** select the **Disk bus** as **IDE.** Click **Apply.**



Fortinet-Controller on QEMU/KVM@kvm

Virtual Disk

Source path: /var/lib/libvirt/images/Fortinet_WLAN/forti-8.3-2build-29-x86_64.img

Device type: VirtIO Disk 1

Storage size: 20.00 GiB

Readonly: □

Shareable: □

Advanced options

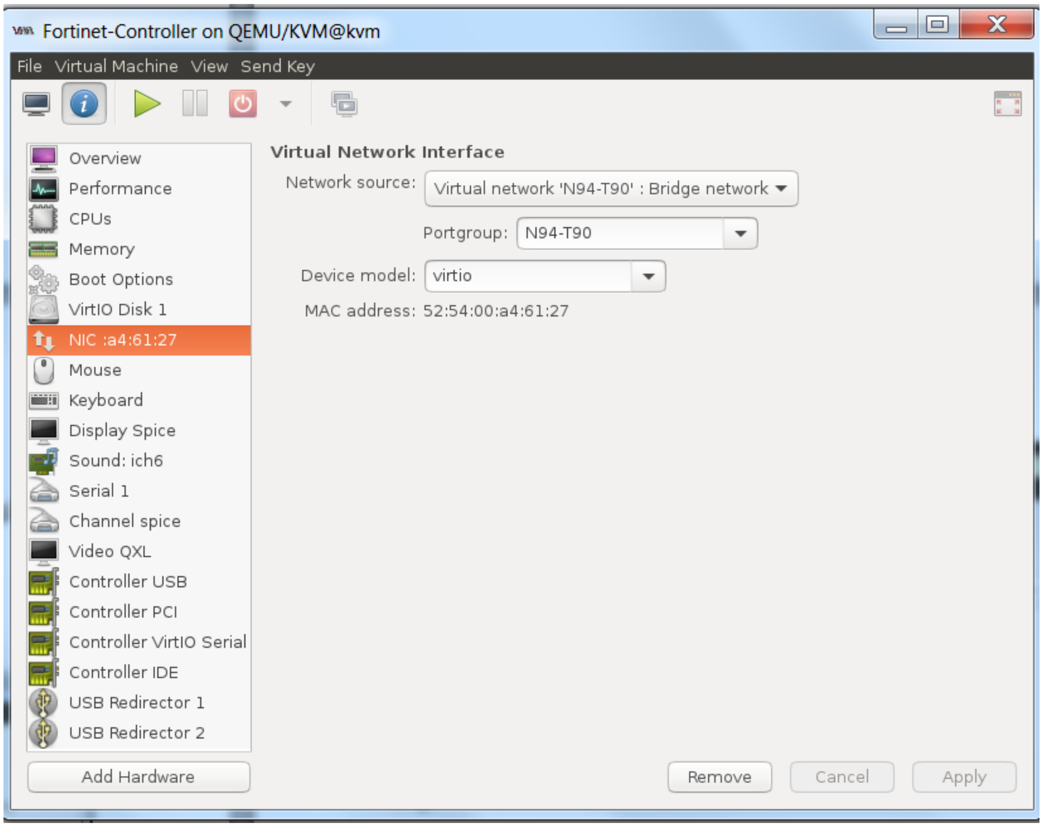
Disk bus: IDE

Serial number:

Storage format: raw

Performance options

10. In the NIC settings, specify the **Network source**, **Portgroup**, and **Device model** as **virtio**. Click **Apply.**



Fortinet-Controller on QEMU/KVM@kvm

Virtual Network Interface

Network source: Virtual network 'N94-T90' : Bridge network

Portgroup: N94-T90

Device model: virtio

MAC address: 52:54:00:a4:61:27

The Virtual Controller deployment is complete.

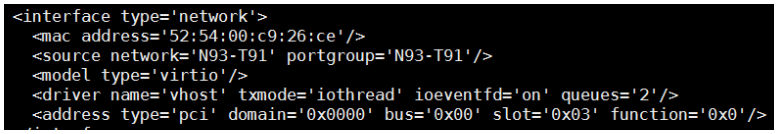
Recommended Linux KVM Host Settings

Fortinet recommends the following host settings for enhanced Controller performance.

- Disable the offload settings like GSO, GRO, TSO, and UFO for all ports. Run the **ethtool -K <eth dev> gso off lro off tso off ufo off** command.
- Set the ring descriptor size (**ethtool -G <eth dev> 4096**) to the maximum limit (4096) for all ports.
- Set **net.core.netdev_budget** to 600 and **net.core.netdev_max_backlog** to 60000.
  The commands in the above steps could be set in */etc/rc.local* so that configuration is retained on a reboot of the host. Based on the VM model, modify the guest xml file and add below line in each interface in xml file.as follows:

  - FWC-VM-50: *<driver name='vhost' txmode='iothread' ioeventfd='on' queues=’2'/>*
  - FWC-VM-200: *<driver name='vhost' txmode='iothread' ioeventfd='on' queues=’2'/>*
  - FWC-VM-500: *<driver name='vhost' txmode='iothread' ioeventfd='on' queues=‘4'/>*
  - FWC-VM-1000: *<driver name='vhost' txmode='iothread' ioeventfd='on' queues='8'/>*
  - FWC-VM-3000: *<driver queues=‘16'/>*

  This is an example of FWC-VM-200 configuration.



```
<interface type='network'>
  <mac address='52:54:00:c9:26:ce'/>
  <source network='N93-T91' portgroup='N93-T91'/>
  <model type='virtio'/>
  <driver name='vhost' txmode='iothread' ioeventfd='on' queues='2'/>
  <address type='pci' domain='0x0000' bus='0x00' slot='0x03' function='0x0'/>
```

- In servers where the available physical cores, that is, half of HT CPUs, are more than the number of vhost kernel threads, set the IRQ affinity for vhost kernel threads. For example, in 1000D each port has 8 queues, hence, there are 32 total vhost threads. Use this script to set the affinity for vhost kernel threads for 1000D VM on Dell PowerEdge R730 (for other hosts, the configuration would be different).

```
#!/bin/bash
cpids=`ps -ef | grep [v]host- | awk '{ print $2 }' | xargs`
echo $cpids
for cpid in $cpids;
do
   taskset -pc 36-71 $cpid
   echo $cpid
done
```

  This script sets the CPU affinity for vhost kernel threads from CPUs 36-71.

Parameters	**FWC-VM-50**	**FWC-VM-200**	**FWC-VM-500**	**FWC-VM-1000**	**FWC-VM-3000**
CPU affinity	Yes	Yes	Yes	Yes	No (Applicable only if the number of physical cores on the host are more than 48.)
Offload settings	Yes	Yes	Yes	Yes	Yes
Ring Descriptor size	4096	4096	4096	4096	4096
Net.core sysctl parameters	Yes	Yes	Yes	Yes	Yes
Guest Network configuration	<drivername=‘vhost’ txmode=’iothread’ ioeventfd=’on’ queues=’2’/>	<drivername=‘vhost’ txmode=’iothread’ ioeventfd=’on’ queues=’2’/>	<drivername=‘vhost’ txmode=’iothread’ ioeventfd=’on’ queues=’2’/>	<drivername=‘vhost’ txmode=’iothread’ ioeventfd=’on’ queues=’2’/>	<driver queues=’16’/>

Deploying Fortinet Virtual Controllers on Hyper-V

Note:

FWC-VM-1000 & FWC-VM-3000 are not supported on the Windows Hyper-V platform.

Pre-requisites

For deployment and management of the Virtual Controller on Hyper-V, install the following 3rd party software.

- Install Windows server 2016.
- Install the Hyper-V role.
- Create a Hyper-V Vswitch.

Note: To accomplish the pre-requisites refer to the respective 3rd party documentation.

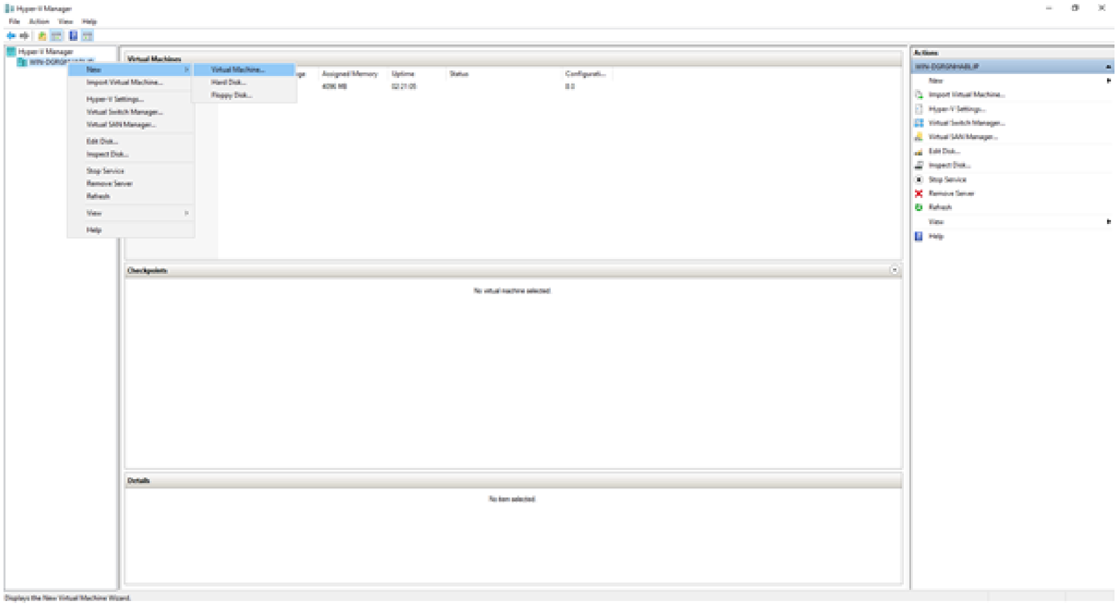
Downloading the Virtual Controller Package File

You can download the virtual controller packages from the Fortinet Customer Support website. To access the support website you need a Fortinet Customer Support account.

The file name is, *forti-x.x-xbuild-0-x86_64.vhd.hv.zip*, where x.x-x is the release version number. For example, 8.3.2.

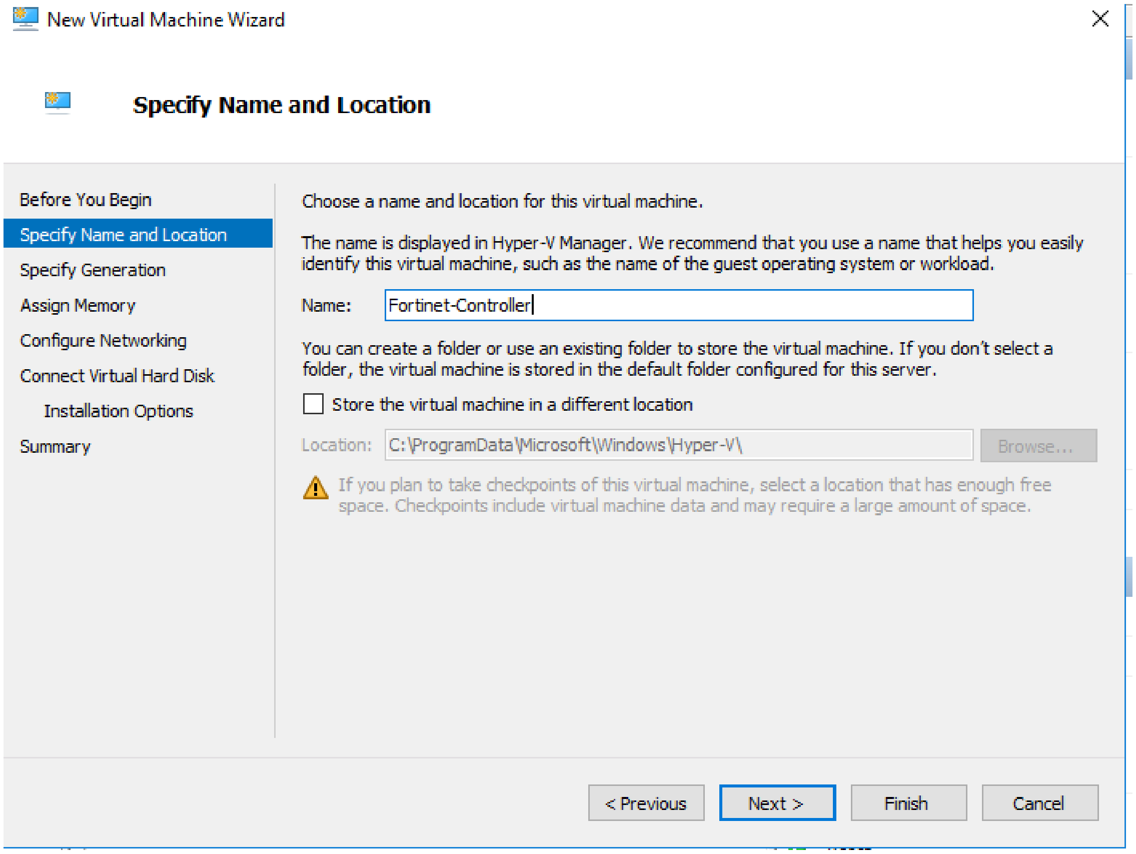
Configuring the Virtual Controller

1. Download the package file to *C:\Users\Public\Documents\Hyper-V\Virtual hard disks* and unzip it. The file should have a unique name and one file is used to create only one instance.
2. Open the HYPER-V manager and select **New > Virtual Machine.**



   The **Virtual Machine** wizard is displayed.

3. Configure the following settings in the **Virtual Machine** wizard:
   - Specify Name and Location



Choose a name and location for this virtual machine.

The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.

Name: Fortinet-Controller

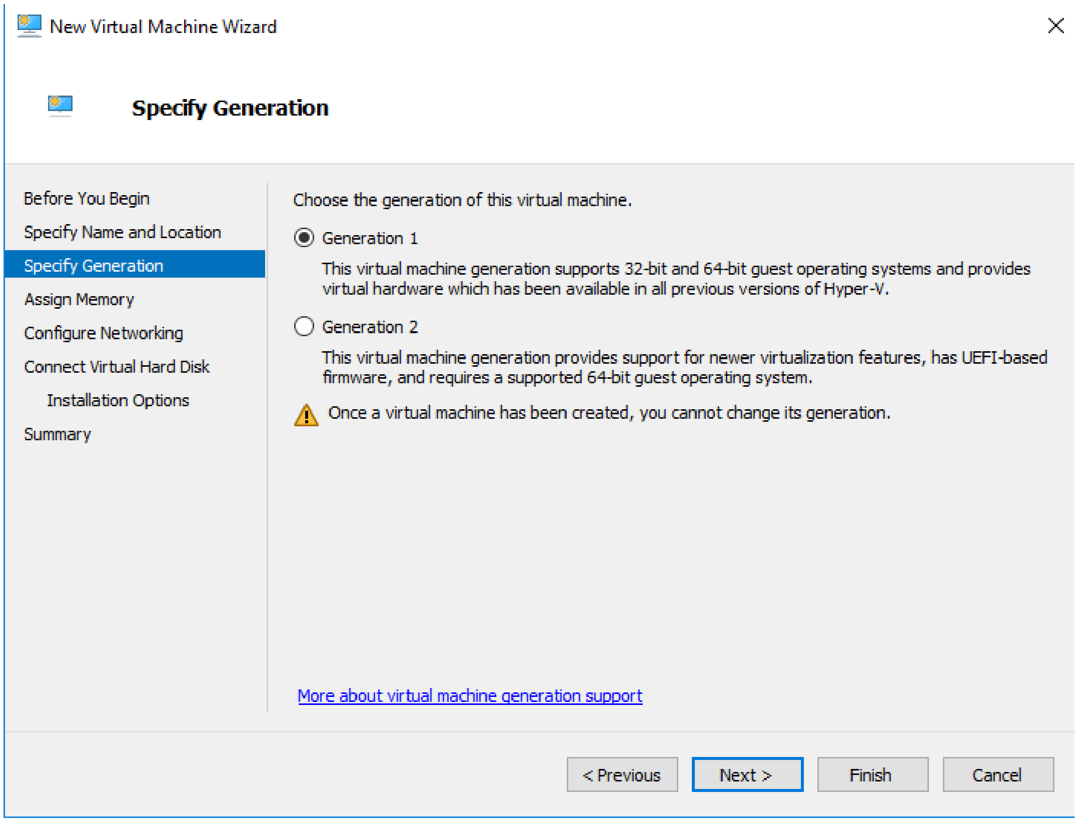
You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.

☐ Store the virtual machine in a different location

Location: C:\ProgramData\Microsoft\Windows\Hyper-V\

If you plan to take checkpoints of this virtual machine, select a location that has enough free space. Checkpoints include virtual machine data and may require a large amount of space.

- Specify Generation – Select **Generation 1**.



Choose the generation of this virtual machine.

● Generation 1

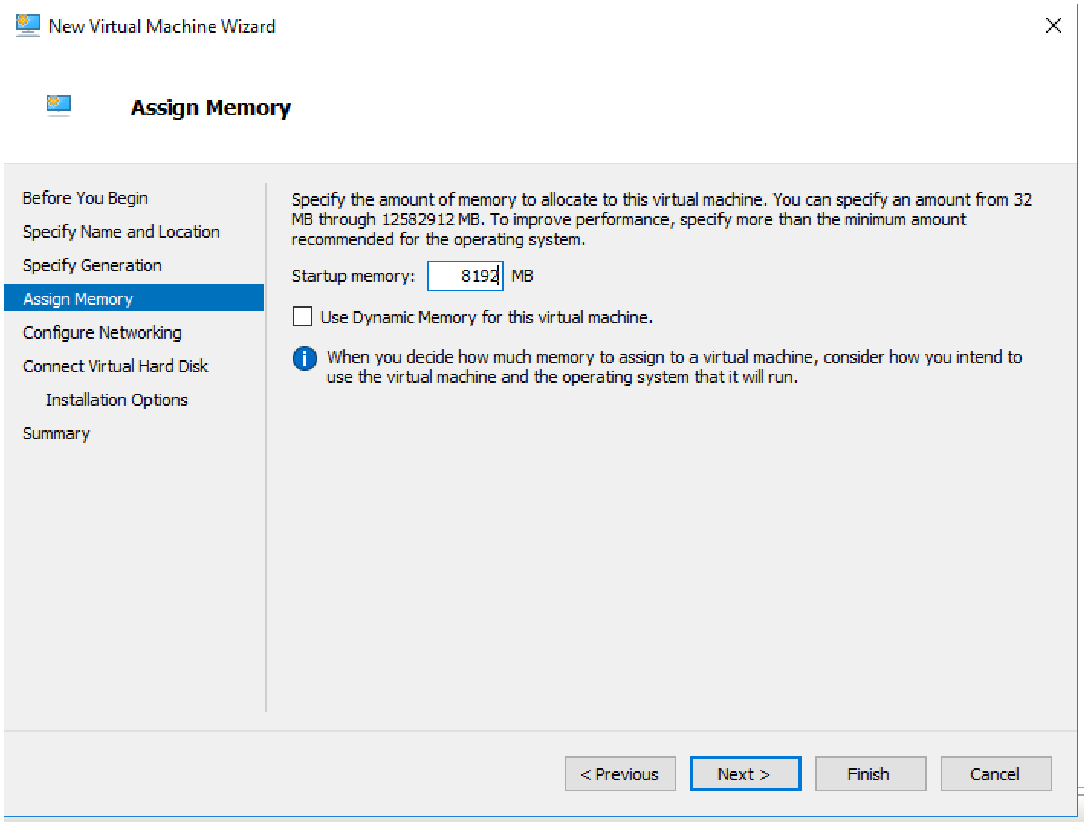
This virtual machine generation supports 32-bit and 64-bit guest operating systems and provides virtual hardware which has been available in all previous versions of Hyper-V.

○ Generation 2

This virtual machine generation provides support for newer virtualization features, has UEFI-based firmware, and requires a supported 64-bit guest operating system.

Once a virtual machine has been created, you cannot change its generation.

- Assign Memory (Supported Hardware Configuration)



New Virtual Machine Wizard

Assign Memory

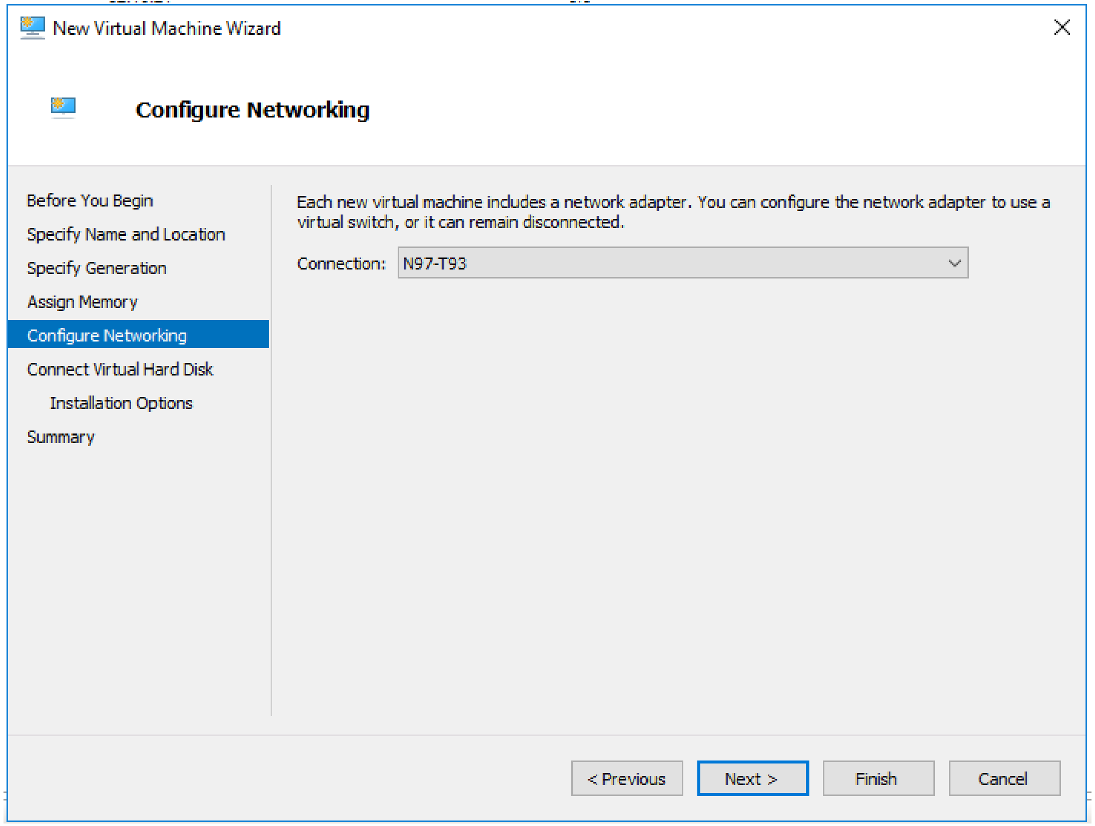
Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 32 MB through 12582912 MB. To improve performance, specify more than the minimum amount recommended for the operating system.

Startup memory: 8192 MB

☐ Use Dynamic Memory for this virtual machine.

When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run.

- Configure Networking



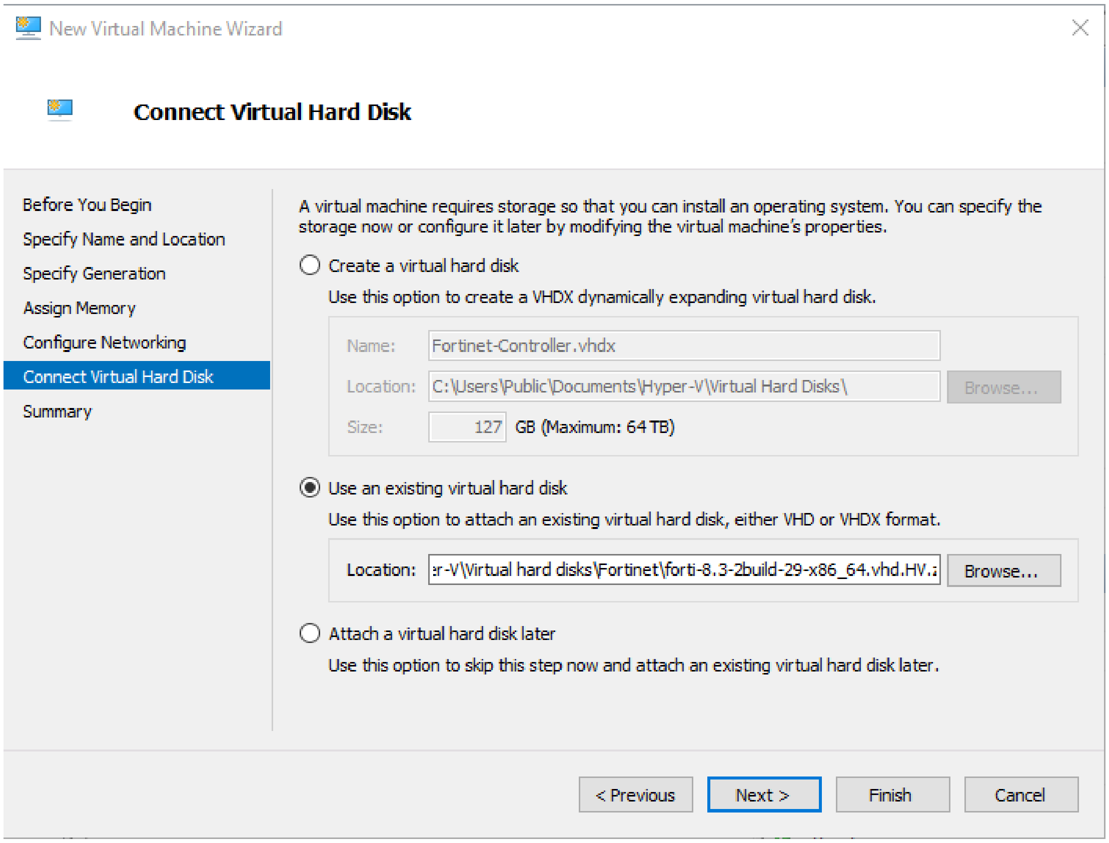
New Virtual Machine Wizard

Configure Networking

Each new virtual machine includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected.

Connection: N97-T93

- Connect Virtual Hard Disk – Select **Use an existing virtual hard disk**



A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.

○ Create a virtual hard disk

Use this option to create a VHDX dynamically expanding virtual hard disk.

Name: Fortinet-Controller.vhdx

Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\

Size: 127 GB (Maximum: 64 TB)

● Use an existing virtual hard disk

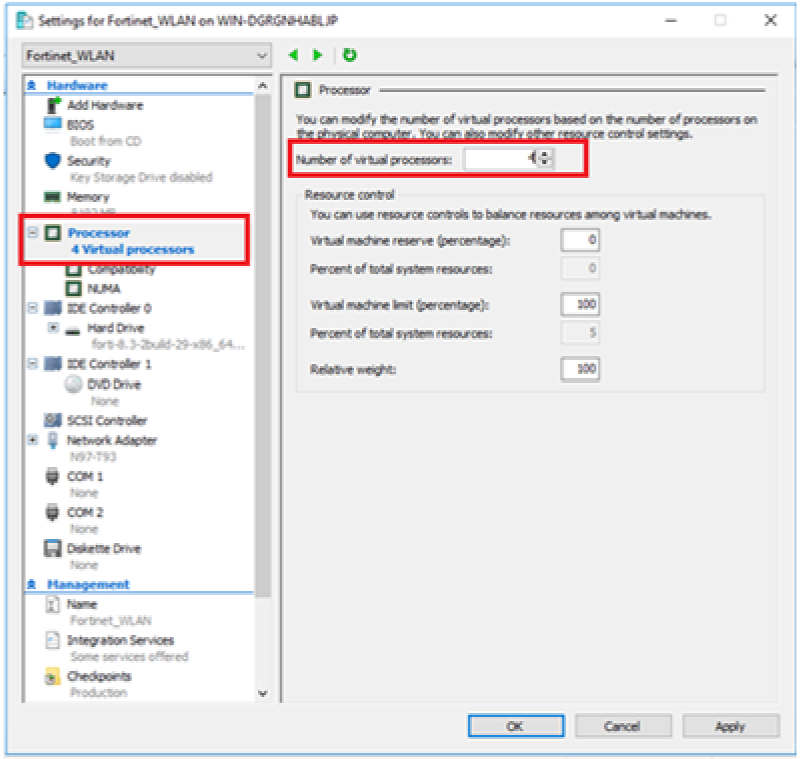
Use this option to attach an existing virtual hard disk, either VHD or VHDX format.

Location: :r-V\Virtual hard disks\Fortinet\forti-8.3-2build-29-x86_64.vhd.HV.z

○ Attach a virtual hard disk later

Use this option to skip this step now and attach an existing virtual hard disk later.

4. Click **Finish**. The virtual machine is listed.
5. Select the newly created virtual machine and double-click. The settings are displayed.
6. Specify the **Number of virtual processors** in the **Processor** settings.



You can modify the number of virtual processors based on the number of processors on the physical computer. You can also modify other resource control settings.

Number of virtual processors: 4

Resource control

You can use resource controls to balance resources among virtual machines.

Virtual machine reserve (percentage): 0

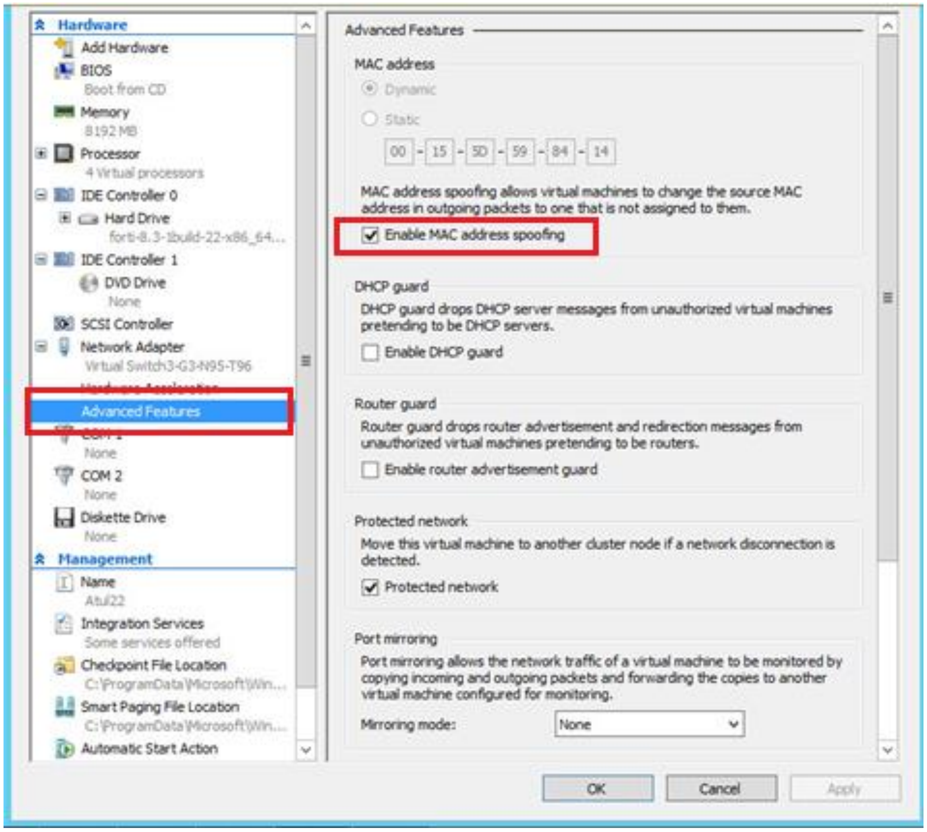
Percent of total system resources: 0

Virtual machine limit (percentage): 100

Percent of total system resources: 5

Relative weight: 100

7. Select **Enable MAC address spoofing** in the **Advanced Features** settings to establish wireless connectivity.



Advanced Features

MAC address

● Dynamic

○ Static

00 - 15 - 5D - 59 - 84 - 14

MAC address spoofing allows virtual machines to change the source MAC address in outgoing packets to one that is not assigned to them.

☑ Enable MAC address spoofing

DHCP guard

DHCP guard drops DHCP server messages from unauthorized virtual machines pretending to be DHCP servers.

□ Enable DHCP guard

Router guard

Router guard drops router advertisement and redirection messages from unauthorized virtual machines pretending to be routers.

□ Enable router advertisement guard

Protected network

Move this virtual machine to another cluster node if a network disconnection is detected.

☑ Protected network

Port mirroring

Port mirroring allows the network traffic of a virtual machine to be monitored by copying incoming and outgoing packets and forwarding the copies to another virtual machine configured for monitoring.

Mirroring mode: None

The Virtual Controller deployment is complete.

8. Run the following command in secure shell on each instance to get the configured VLAN working.
   This is a sample command:

   Set-VMNetworkAdapterVlan -Trunk -AllowedVlanIdList "96" -VMName "Forti22" -VMNetworkAdapterName "Network Adapter" -NativeVlanId 0

Recommended Hyper-V Settings

Fortinet recommends the following settings for enhanced Controller performance.

- Disable the default VMQ.
- Enable RSS on all the adapters.
- Tx and Rx buffers set to 4096.

License Management for Fortinet Virtual Controllers

This section assumes you have already received your entitlement for the Fortinet Virtual Controller you ordered. Along with the entitlement that allows you to obtain the license for your instance, you would also have received instructions on where to download the right version of the software for the model you ordered. Register your product at the Fortinet Support Portal and use the registration key and system ID to obtain a license file.

⚠ **Note:** Obtain the license only after completing the installation of the Virtual Controller. Contact the Forticare Support with the details entailed in the following sections to obtain the license.

FWC-VM Series Virtual Controllers

After completing installation of the Virtual Controller, login to the controller and run the **setup** command to generate the system-id. Perform the following steps to obtain the license.

1. Run the **setup** command on the Controller to generate the system-id, configure the hostname, and configure the static IP address of the Controller, to ensure that the IP address does not change as the system-id/license is mapped to the IP address of the Controller.
2. Save the configuration. The Controller restarts.
3. Run the **show system-id** command to obtain the system-id.
4. Share the Virtual Controller model details and system-id with the Forticare Support team.
5. Configure the Virtual Controller instance with the required resources (Supported Hardware Configuration) as per the model for which the license has been generated.
6. Install the license from the GUI (See section *Importing and installing a License*) OR from the CLI (Configuration Terminal mode => **vm-license scp://username@<Your file server IP Address>:<license filename>**)
7. Reboot the Controller to apply the changes as per the generated license.

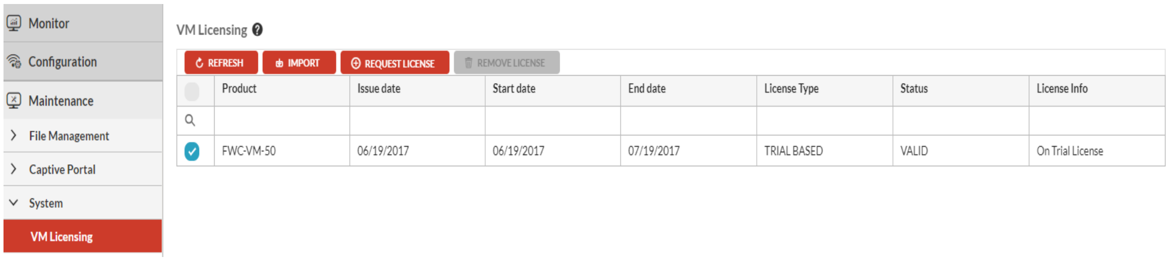
⚠ **Note:** A freshly installed system boots up as FWC-VM-50 with default license valid for 30 days.

- System-id is not get generated until you run the **setup** command on a fresh instance.
- System-id is coupled with the IP address. Hence, any change in the IP address generates a new system-id thereby failing validation of the older license. In this case, a new license is required. Changing the IP address via CLI followed by a reboot to activate the new IP address does not generate a new system-id. Hence, license validation fails and the Controller is once again the FWC-VM-50 model. Therefore, use only the **setup** command to change the Controller IP address.
- After the license is invalidated due to a change in the system-id and the controller is once again a FWC-VM-50 model, ensure that you delete the invalid license for the Controller to function properly. Else, the Controller reboots after every one hour.

Importing and Installing a License

Perform these steps to obtain the license using the GUI.

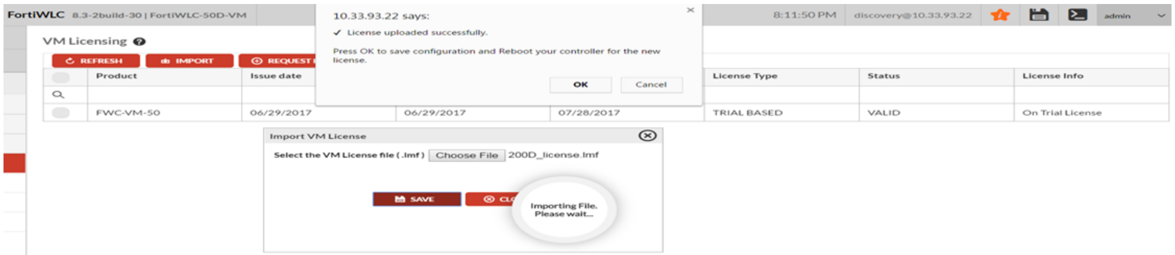
1. Navigate to **Maintenance > System > VM Licensing**
   This image displays a freshly installed system which has a default license (trial based) valid for 30 days from the license issued date.
2. In the **VM Licensing** wizard, click **Import** to add a license. By default, this page lists the license available on the system which includes details on the Virtual Controller model.



VM Licensing

Product	Issue date	Start date	End date	License Type	Status	License Info
FWC-VM-50	06/19/2017	06/19/2017	07/19/2017	TRIAL BASED	VALID	On Trial License

Browse to the license file and click **Save**.



10.33.93.22 says:

✓ License uploaded successfully.

Press OK to save configuration and Reboot your controller for the new license.

VM Licensing

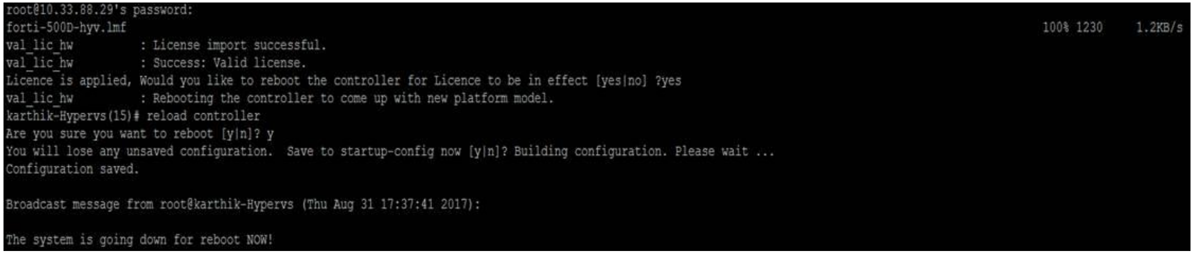
Product	Issue date			License Type	Status	License Info
FWC-VM-50	06/29/2017	06/29/2017	07/28/2017	TRIAL BASED	VALID	On Trial License

Import VM License

Select the VM License file (.lmf) 200D_license.lmf

Importing File. Please wait...

The license can be imported through the CLI as well.



```
root@10.33.88.29's password:
forti-500D-hyv.lmf                                                                                                    100% 1230     1.2KB/s
val_lic_hw          : License import successful.
val_lic_hw          : Success: Valid license.
Licence is applied, Would you like to reboot the controller for Licence to be in effect [yes|no] ?yes
val_lic_hw          : Rebooting the controller to come up with new platform model.
karthik-Hypervs(15)# reload controller
Are you sure you want to reboot [y|n]? y
You will lose any unsaved configuration.  Save to startup-config now [y|n]? Building configuration. Please wait ...
Configuration saved.

Broadcast message from root@karthik-Hypervs (Thu Aug 31 17:37:41 2017):

The system is going down for reboot NOW!
```

Note:

- The Controller reboots when you have uploaded the license file.
- The Controller does not support importing license files with spaces or brackets [()] in the filename.

License Validation

After the license is imported, validation is performed on the license parameters. If that validation succeeds and the appropriate hardware resources for the requested controller model are allocated, then the license is installed successfully. If either license validation or hardware resource validation fails, the system reverts to the default license. See section *Supported Hardware Configuration* for further details.

Once the license is installed successfully, it replaces the default license. There are two types of licenses – Trial Based and Perpetual (Never ending).

License Monitoring

The license validation happens after every one hour at regular intervals. With 30 days to go for expiry, alarms are raised on the controller. The Software License Expired alarm is generated as per the configured severity. The default severity is critical.

In a fresh installation running on a default license (FWC-VM-50) which is valid for 30 days, you get 30 additional days within which to purchase and apply for a valid license. If a valid license is not imported, at the end of additional 30 days, the Controller will reboot and the APs will go to offline state.

To delete a **perpetual** license, select the license and click **Remove License** or run the **delete vm-license** CLI command. After the license is deleted, the Controller reboots and comes up as FWC-VM-50 with the default trial based license.

Note: Deletion of trial based license is not allowed.

MC-VE Series Virtual Controllers

After completing installation of the Virtual Controller, login to the controller and run the **show system-id** command.

You will need the output of this command along with the entitlement ID to generate the license key for your Virtual controller.

The system-id parameter is computed based on the configuration gathered through the setup process in the Controller or entered using the Ez-Setup wizard. The following fields are captured through the setup process.

- Time zone
- Hostname
- IP Address of Controller's primary interface
- IP Mask of Controller's primary interface
- Gateway Address of Controller's primary interface
- Country Code
- VC model

Share the Virtual Controller model details, system-id, and the license validity period (or permanent license) with the Forticare Support team.
Any subsequent changes to the parameters above would warrant you to get a new license.

Fortinet Virtual Controller Management

Like any conventional Hardware Controller that Fortinet offers, the Virtual Controller can be managed by directly accessing the controller using the System Director Web UI or FortiWLM.

Refer to System Director Configuration Guide and Command Reference guide and other System Director for configuring and managing your Virtual Controller. The term Controller refers to Physical appliance as well as your Virtual Controller.

Fortinet Virtual Controller Upgrade

Virtual Controllers can be upgraded the same way as the hardware controllers. Download the appropriate Virtual Controller image from Fortinet Customer Support website.

Upgrading the controller can be done in the following ways:

- Using the FTP, TFTP, SCP, and SFTP protocols.
- Navigate to **Maintenance < File Management** in the FortiWLC GUI to import the downloaded package.

The following are sample commands for upgrading the Virtual Controllers using any of these protocols.

- upgrade-image tftp://10.xx.xx.xx:forti-x.x-xbuild-x-x86_64-rpm.tar both reboot
- upgrade-image sftp://build@10.xx.xxx.xxx:/home/forti-x.x-xGAbuild-88-FWC1KD-rpm.tar both reboot
- upgrade-image scp://build@10.xx.xxx.xxx:/home /forti-x.x-xGAbuild-88-FWC1KD-rpm.tar both reboot
- upgrade-image ftp://anonymous@10.xx.xx.xx:forti-x.x-xbuild-x-x86_64-rpm.tar both reboot

The **both** option upgrades the Fortinet binaries (rpm) as well as the Kernel (iso), the **apps** option upgrades only the Fortinet binaries (rpm).

After upgrade, the Virtual Controller should maintain the System-id of the system, unless there were some changes in the fields that are used to generate the system-id. See the to the Licensing section for detailed information.

The International Virtual Controller can be installed, configured, licensed and upgraded the same way.

Fortinet Virtual Controller High Availability

Virtual Controller are affordable and an easy way to achieve High Availability for your environment. These are some highlights of the Virtual Controllers High Availability deployment:

- N+1 slave for controller appliances.
- **The FWC-VM Series Virtual Controllers -** Supports HW appliances of same model, for example,1000D-VM can act as N+1 slave for 1000D-VM only.
- **The MC-VE Series Virtual Controllers** - Supports HW appliances of same model and lower, for example,MC4200-VE can act as N+1 slave for MC4200-VE, MC3200-VE, and MC1550-VE.
- When a controller slave becomes active, the slave model operates with the same capacity as that of the master controller it has taken over.

This table describes the N+1 compatibility with the MC Series as the master.

Slave	Master						
	MC1550	MC1550-VE	MC3200	MC3200-VE	MC4200	MC4200-VE	MC6000
MC1550	✓	X	X	X	X	X	X
MC3200	X	X	✓	X	X	X	X
MC4200	X	X	X	X	✓	X	X
MC6000	X	X	X	X	X	X	✓
MC1550-VE	✓	✓	X	X	X	X	X
MC3200-VE	✓	✓	✓	✓	X	X	X
MC4200-VE	✓	✓	✓	✓	✓	✓	X
FWC-50D	X	X	X	X	X	X	X
FWC-VM-50	X	X	X	X	X	X	X
FWC-200D	X	X	✓	X	X	X	X
FWC-VM-200	X	X	X	X	X	X	X
FWC-500D	X	X	X	X	✓	X	X
FWC-VM-500	X	X	X	X	X	X	X
FWC-1000D	X	X	X	X	X	X	X
FWC-VM-1000	X	X	X	X	X	X	X
FWC-3000D	X	X	X	X	X	X	X
FWC-VM-3000	X	X	X	X	X	X	X

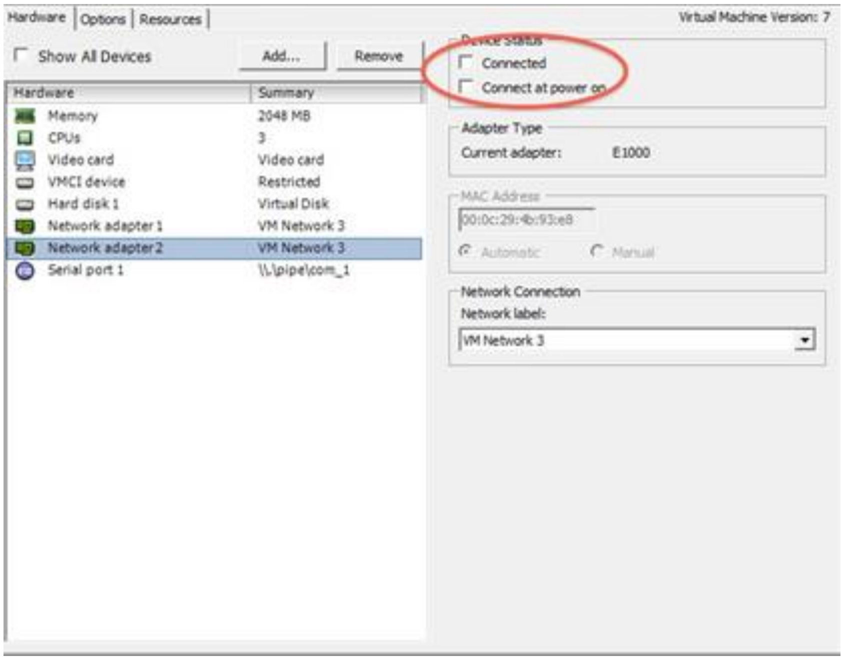
This table describes the N+1 compatibility with the FWC Series as the master.

Slave	Master									
	FWC-50D	FWC-VM-50	FWC-200D	FWC-VM-200	FWC-500D	FWC-VM-500	FWC-1000D	FWC-VM-1000	FWC-3000D	FWC-VM-3000
MC1550	X	X	X	X	X	X	X	X	X	X
MC3200	X	X	✓	X	X	X	X	X	X	X
MC4200	X	X	X	X	✓	X	X	X	X	X
MC6000	X	X	X	X	X	X	X	X	X	X
MC1550-VE	X	X	X	X	X	X	X	X	X	X
MC3200-VE	✓	X	✓	X	X	X	X	X	X	X
MC4200-VE	✓	X	✓	X	✓	X	X	X	X	X
FWC-50D	✓	X	X	X	X	X	X	X	X	X
FWC-VM-50	X	✓	X	X	X	X	X	X	X	X
FWC-200D	X	X	✓	X	X	X	X	X	X	X
FWC-VM-200	X	X	X	✓	X	X	X	X	X	X
FWC-500D	X	X	X	X	✓	X	X	X	X	X
FWC-VM-500	X	X	X	X	X	✓	X	X	X	X
FWC-1000D	X	X	X	X	X	X	✓	X	X	X
FWC-VM-1000	X	X	X	X	X	X	X	✓	X	X
FWC-3000D	X	X	X	X	X	X	X	X	✓	X
FWC-VM-3000	X	X	X	X	X	X	X	X	X	✓

Troubleshooting Tips

APs not connecting to the controller & seeing duplicate responses for pings from the controller to an outside system

The same vSwitch is being used for both vNICs, define separate vSwitches for each vNIC. Alternatively you could disable one of the vNICs in the virtual machine.
You can disable the 2nd vNIC, by un-checking the **Connected**
and **Connect at Power On** options.



Virtual Machine Version: 7

☐ Show All Devices

Hardware	Summary
Memory	2048 MB
CPUs	3
Video card	Video card
VMCI device	Restricted
Hard disk 1	Virtual Disk
Network adapter 1	VM Network 3
Network adapter 2	VM Network 3
Serial port 1	\\.\pipe\com_1

Device Status
☐ Connected
☐ Connect at power on

Adapter Type
Current adapter: E1000

MAC Address
00:0c:29:4b:93:e8
● Automatic ○ Manual

Network Connection
Network label:
VM Network 3

Clients not able to connect to the network

If you look at the station log and see “Client moved to wired side”. This is an indication that your vSwitches are not configured properly. Potentially vSwitch is not mapped to one physical vNIC or the physical resources is not bonded properly or multiple hosts are sharing the same vSwitch.

How To Capture Events leading to a Crash on Virtual Controller

1. Unlike physical controllers, virtual controllers may not generate a kernel-gather file if theycrash.
2. It should generate a file Fortinet-kernel-diag similar to Physical controller unless you encounter silent reboot which can happen to both VM and Physical controller.
3. The output for a virtual controller crash may well look like a fault onVMWare.
4. To confirm, connect a PC to the serial port of the physical host (virtual blade).
5. Map the serial port resource on the host to the VMware image.
6. Try to connect via PuTTY (same serial settings as those set for a physical host) to virtual controller.
7. You will be able to catch the reboot reason / crash log, the next time the eventoccurs.

Does Fortinet Support Mesh on Virtual Controllers?

Yes, Fortinet supports Mesh on Virtual controllers as well.

Notice

ALL INFORMATION PROVIDED IN THIS DEPLOYMENT GUIDE, INCLUDING COMMENTARY, OPINION, FORTINET NETWORKS DESIGN SPECIFICATIONS, AND OTHER DOCUMENTS (TOGETHER AND SEPARATELY, “MATERIALS”) ARE BEING PROVIDED “AS IS.” FORTINET NETWORKS MAKES NO WARRANTIES, EXPRESSED, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO MATERIALS, AND EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES OF NONINFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE.