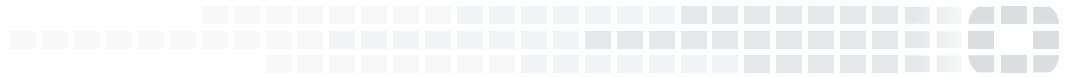




FORTINET
High Performance Network Security



FortiGate-VMX v.2 - Installation Guide

VMX Security Nodes using FortiOS v5.4



FORTIOS
5.4
VERSION

FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO GUIDE

<http://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

<http://cookbook.fortinet.com/how-to-work-with-fortinet-support/>

FORTIGATE COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING SERVICES

<http://www.fortinet.com/training>

FORTIGUARD CENTER

<http://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdocs@fortinet.com



11/9/2015

FortiGate-VMX v.2 - Installation Guide

1-540-0292458-20151006

TABLE OF CONTENTS

Change Log	5
Introduction	6
Overview	7
The Integration/Interaction Process.....	7
Terms and concepts.....	9
dvPortGroups.....	9
dvSwitch.....	9
ESXi.....	9
Host.....	9
Kernel agent.....	9
NetX.....	9
NSX.....	10
Security Node.....	10
Service Manager.....	10
vCenter Server.....	10
vCNS.....	10
vSphere.....	10
FortiGate-VMX and FortiGate-VM - similarities.....	10
FortiGate-VMX and FortiGate-VM - differences.....	11
The FortiGate-VMX Target Customer.....	12
Environmental prerequisites	13
VMware components:.....	13
VMware technologies.....	13
Other resources.....	13
Licensing	14
Getting the License.....	14
Installation of FortiGate-VMX Service Manager	16
Assumptions.....	16
Configuring ESXi Agent VM Settings.....	16
Relevant settings.....	16
How to configure them:.....	17
Registering FortiGate-VMX Service Manager.....	17
Downloading the images.....	18

Deployment Package Contents.....	19
Placing FortiGate-VMX Security Node files on the Web Server.....	19
Deploying the FortiGate-VMX Service Manager.....	19
Configuring FortiGate-VMX Service Manager.....	25
Configure FortiGate-VMX Service Manager MGMT Interface.....	25
Set MGMT port IP address.....	25
Set default gateway.....	25
Set DNS.....	25
Connecting to the FortiGate-VMX Service Manager Web UI.....	26
Uploading FortiGate-VMX Service Manager license file.....	26
VMware settings.....	26
Interface settings.....	27
Register FortiGate-VMX Service.....	29
NSX host preparation of cluster.....	31
Service Deployment.....	32
Configuring Security Groups and Re-Direction Policy.....	34
Configuring NSX Security Groups.....	34
Re-Direction Security Policy.....	35
Associating a Security Group to Re-Direction Security Policy.....	38
A Note About VMware Tools and IP Sets.....	40
IP Set Creation.....	40
Associate the IP Set with the Security Group.....	41
SpoofGuard in NSX.....	41
Enable SpoofGuard.....	41
Setting Policies.....	45
Creating and Navigating Virtual Domains (VDOMs).....	46

Change Log

Date	Change Description
2015-11-09	Initial Release.

Introduction

Just because it's in the cloud does not make it secure. The nature of virtual systems make it difficult for most of us to properly visualize what is really going on and how it really works. The analogy that a virtual system is exactly like its hardware counterpart, except that it is a computer simulation, gets most of the important ideas across but it doesn't convey everything. A single computer that spread over multiple computers across the world is a little harder to comprehend, especially when you consider that it is in multiple places at the same time. For the final step, add in the idea of a network between virtual computers that is on one computer; or the more likely scenario, multiple computers that are synthesizing a platform that hosts virtual systems as if it is one computer. With every extra layer of complexity, it gets more difficult for the mind to grasp.

Now, to make this more confusing, consider this...

If you introduce malware to the computer hosting some virtual computers, you might detect it by running AV on the OS of the host computer. If you introduce malware into one of the virtual systems hosted by that computer, antivirus software might be able to detect the malware if run on the OS of the virtual computer. What about the virtual network used to communicate between the virtual computers? This network is running within a computer, but the operating system's logic tells it a network is something separate from the OS and thus to be ignored when running scans. The tendency so far in the world of IT, is that if there is a weakness in a system, someone is going to find a way to exploit it. Therefore defenses need to be put in place.

FortiGate VMX is one of the tools in the strategy of that defense.

The following topics are included in this section:

- [Overview on page 7](#)
- [Environmental prerequisites on page 13](#)
- [Licensing on page 14](#)
- [Installation of FortiGate-VMX Service Manager on page 16](#)
- [Configuring FortiGate-VMX Service Manager on page 25](#)
- [Register FortiGate-VMX Service on page 29](#)
- [NSX host preparation of cluster on page 31](#)
- [Service Deployment on page 32](#)
- [Configuring Security Groups and Re-Direction Policy on page 34](#)
- [A Note About VMware Tools and IP Sets on page 40](#)
- [Setting Policies on page 45](#)

Overview

The FortiGate-VMX solution is intended to provide integrated protection of East/West traffic flow inside a virtual environment.

These VMware-specific solutions are engineered to integrate with either NSX or vCloud Networking and Security (vCNS) environments:

- FortiGate-VMX v2 for NSX
- FortiGate-VMX v1 for vCNS

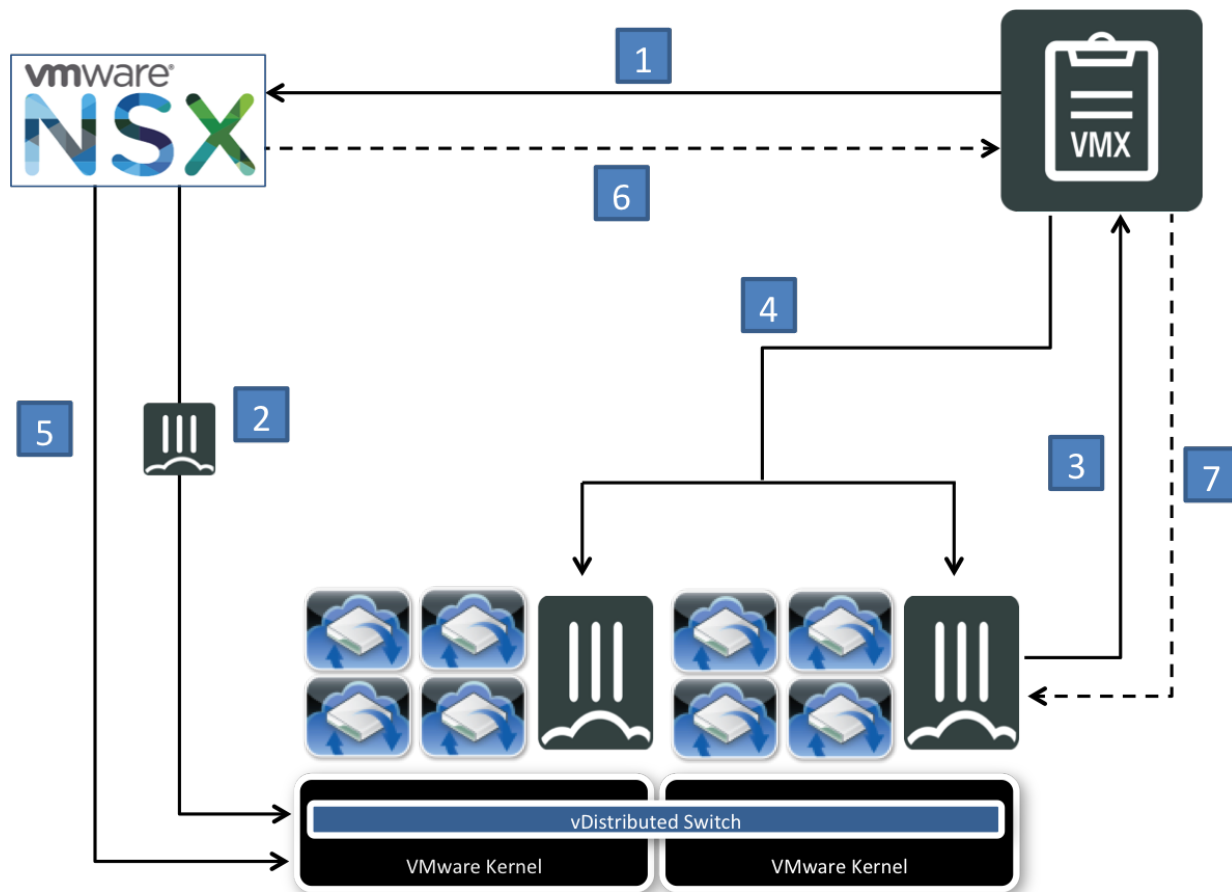
Through the close partnership VMware and Fortinet maintain, VMware-specific APIs were made available to enable the FortiGate-VMX integration. This allows for interception and policy enforcement at the hypervisor level.

Once properly configured and licensed, FortiGate-VMX Security Nodes will be automatically deployed to each ESXi host in the designated cluster(s). If a new ESXi host is introduced into a designated cluster, a FortiGate-VMX Security Node will auto-deploy and policy synchronized.

The FortiGate-VMX Security Node is not in Transparent Mode as might be assumed because there is no NAT occurring. The FortiGate-VMX Security Node only has internal interfaces. For FortiGate-VMX v1, they are conveniently named "internal" & "external". For FortiGate-VMX v2, there is an internal port pair per VDOM, so the naming convention is <VDOM name>-int & <VDOM name>-ext. FortiGate-VMX security policies are configured and applied using these interfaces.

The Integration/Interaction Process

Once everything has been properly installed, the deployment of FortiGate-VMX Security Nodes will be automatic. An overview of the deployment process is laid out as follows:



1. FortiGate-VMX Service Manager registers the Fortinet security service with NSX Manager (FortiGate-VMX):
 - The registration process uses the NetX management plane API to enable bi-directional communication between the FortiGate-VMX Service Manager and the NSX Manager.
2. Auto-deploy FortiGate-VMX to all hosts in designated cluster(s):
 - The NSX Manager collects the FortiGate-VMX image from the URL specified during registration and installs an instance of FortiGate-VMX on each ESXi host in the designated cluster(s). The image update is instantaneous and beneficial for on-demand, software-defined data center requirements.
3. FortiGate-VMX Security Node connects with FortiGate-VMX Service Manager:
 - The FortiGate-VMX Security Node initiates a connection to the FortiGate-VMX Service Manager to register and obtain its license.
4. License verification and configuration synchronization with FortiGate-VMX:
 - FortiGate-VMX Service Manager verifies the serial number and synchronizes configuration and policy.
5. Redirection policy rules updated for enablement of FortiGate-VMX security service:
 - For all objects secured in the cluster, a policy redirecting all, or specific traffic to FortiGate-VMX is ready.
6. Real-time updates of object database:
 - The NSX Manager sends real-time updates on the changes in the virtual environment to the FortiGate-VMX Service Manager.
7. FortiGate-VMX Service Manager dynamically synchronizes object database and policy to all FortiGate-VMX Security Nodes deployed in cluster.

Terms and concepts

This product, more than most, is dependent on its interaction with a third party product as well as being designed differently from most of the other virtual Fortinet products, so a short listing of terms and concepts not common to our other products is included to avoid confusion.

dvPortGroups

Distributed Port groups in VMware are similar to vLAN's traditionally used to isolate traffic in a network.

VMware's official definition of a dvPortGroup is:

A distributed port group specifies port configuration options for each member port on a vSphere distributed switch. Distributed port groups define how a connection is made to a network.

dvSwitch

A dvSwitch is a distributed Virtual Switch. In the traditional virtual environment that hosts multiple VM instances on a single host, there is one virtual switch that all the instances are "attached" to inside the host. The difference in a distributed virtual switch is that this switch can span multiple hosts.

ESXi

VMware's enterprise-class, type-1 hypervisor, used for deploying and hosting virtual computers. Because it is a type-1 hypervisor it is not a software application that is installed on top of an existing operating system. It has its own OS components and can be installed directly on the computer hardware or as its own virtual OS.

Host

In a VMware infrastructure, a host is an instance of ESXi that holds one or more VMs. These VMs can be virtual servers or virtual network devices.

Kernel agent

This is a component of the infrastructure that is situated between each virtual NIC and its associated port on the vDistributed Switch. As traffic traverses between the vNIC and the vSwitch, it is re-directed to the FortiGate-VMX Security Node instance to be processed.

NetX

An API that is available to specific Technical Alliance Partner (TAP) Elite partners. It is called the Network Extensibility API or NetX. This allows the interception of traffic between a VM's vNIC and the virtual switch it's plugged into to make policy decisions.

This API allows FortiGate-VMX to integrate into the VMware infrastructure.

NSX

NSX is VMware's network virtualization platform for the Software-defined Data Center. In NSX, virtual networks are programmed, provisioned, and managed independent of the underlying hardware. It reproduces the entire network model in software, enabling any network topology to be created and provisioned without all the physical work of having to rewire, move and connect your hardware.

Security Node

The FortiGate-VMX Security Node is the virtual FortiGate-VMX Firewall instance deployed with each host.

Service Manager

The Service Manager, or if you prefer its full name, FortiGate-VMX Service Manager, is the interface between the FortiGate-VMX Security Nodes and the VMware infrastructure. It is through the Service Manager that the Security Nodes are deployed, configured and licensed. In some ways it could be thought of as a FortiManager for VMX Security Nodes only.

vCenter Server

VMware vCenter Server is the centralized management application portion of vSphere that lets you centrally manage virtual machines and ESXi hosts. vCenter is a requirement to have enterprise features like vMotion, VMware High Availability, VMware Update Manager and VMware Distributed Resource Scheduler (DRS).

vCNS

VMware vCloud Networking and Security enable a broad range of services in a single solution, including virtual firewall, VPN, load balancing and VXLAN extended networks.

VMware has announced EOA (End of Availability) of vCNS v5.5. Support is scheduled to run through 2016.

FortiGate-VMX v1 is supported on vCNS, FortiGate-VMX v2 only supports NSX.

vSphere

VMware's cloud computing virtualization operation system.

FortiGate-VMX and FortiGate-VM - similarities

Both the FortiGate VM and VMX are security virtual appliances. In fact, they are based on the same FortiOS firmware. FortiGate-VMX v1 supports FortiOS v5.2.4 while FortiGate-VMX v2 utilizes FortiOS v5.4. Just like the FortiGate hardware appliances and FortiGate-VM virtual appliances, FortiGate-VMX includes the following advanced functions and features:

- Firewall
- Application Control
- Application Security
- Anti Virus

- Data Leak Prevention
- Email Filter
- IPS/IDS
- Web filtering
- Explicit Proxy
- FortiGuard Services

FortiGate-VMX and FortiGate-VM - differences

While a FortiGate-VMX functions in the same way as a FortiGate VM, securing and filtering traffic that goes through it, there are some differences which include:

- The FortiGate-VM is an edge security solution. It has features like VPN termination and NAT. The FortiGate-VMX security service secures traffic between vNICs of each VM and the virtual ports of the vSwitch they are connected to. FortiGate-VMX is a platform-centric security solution, with VMware NSX API integration to provide complete visibility and inspection for East-West inter-VM traffic across security clusters.
- FortiGate-VMX is designed to sit inside of the virtual infrastructure, not outside of it.
- FortiGate-VMX is a two component system encompassing a Service Manager and Security Nodes. Both are required for it to function properly.
- A FortiGate VM is a virtual appliance deployed from an OVF file either manually by the VM administrator or as part of an orchestrated event. It has the same feature set of the hardware version of a FortiGate. It is intended for a static environment. By comparison, the FortiGate VMX is part of an automated deployment process that is part of the VMware virtual environment through its use of an API.
- Once the FortiGate-VMX Service Manager is integrated into the SDDC, any time an ESXi host is added, a FortiGate-VMX instance will be auto deployed and self-register with the FortiGate-VMX Service Manager.
- The configuration of FortiGate-VMX instances is handled by the FortiGate-VMX Service Manager rather than by logging on to the instance itself to configure it. No manual configuration of the node is required.
- The licensing of FortiGate-VM relates to the number of vCPUs assigned to it. FortiGate-VMX is instance-based; 1 instance requires 1 license regardless of the resources assigned to it.
- The only available support options for FortiGate-VMX are the 24x7 UTM or 24x7 NGFW bundles.
- FortiGate-VM is an edge or perimeter security solution that supports a number of features which are not relevant in a FortiGate-VMX security environment:
 - VPN tunnels.
 - WAN optimization
 - NAT
 - Dynamic Routing
 - VDOM upgrades



While the functionality of some regular feature may not be included in the VMX version of FortiGate, the menu items may still be present in the GUI.

The FortiGate-VMX Target Customer

In trying to figure out if FortiGate-VMX is the correct security solutions for your environment, the first question to ask is what is expected of the system? If it is a solution that terminates VPNs or requires NAT for external traffic flow, then FortiGate-VM, as opposed to FortiGate-VMX, is the proper solution for that type of environment.

Once past the first question, the second question is even more basic: what is the virtualization environment that this solution will be deployed into? FortiGate-VMX is a VMware-specific solution. VMware vSphere, NSX or vCNS (for FortiGate-VMX v1) are required for proper integration. If these answers all came back as 'yes', then the FortiGate-VMX security solution is a potential fit.

Environmental prerequisites

The deployment of FortiGate-VMX requires a properly licensed VMware vSphere 5.5 or 6.0 environment as well as knowledge of how to configure and maintain the environment. Other VMware platforms such as Workstation, Fusion, Player or Server are not supported. The following environment should be set up and properly licensed in the environment:

VMware components:

- vCenter Server Standard version 5.5, Update 2 or later, v6.0
- vSphere version 5.5, Update 2 or later, v6.0
 - vSphere Enterprise Plus licenses for ESXi
- vSphere Web Client - the Windows client does not support NSX management
- NSX Manager v6.1.3 or v6.1.4



FortiGate-VMX v2 is supported in vSphere v5.5 & v6.0 environments.

VMware technologies

- vDistributed switches (standard vSwitches aren't supported – this is a VMware requirement). Only traffic going through the vDistributed switches can be secured by the FortiGate-VMX security solution.
- DRS Cluster(s) - These clusters will contain the hosts. The clusters containing the hosts must be DRS enabled for the solution to work.

Other resources

- Web server (for FortiGate-VMX Security Node deployment files) - there is no particular type or version of web server. It can be hardware based or vm-based. The requirements are that it be:
 - able to serve up files designated by a URL.
 - be accessible by the NSX Manager
- 2 configured networks
 - mgmt: management network for communication between the FortiGate-VMX Service Manager and VMware components as well as the FortiGuard Distribution Network (FDN).
 - sync: sync network for communication between the FortiGate-VMX Service Manager and all deployed FortiGate-VMX Security Nodes

Licensing

There are two Fortinet components that make up a FortiGate-VMX environment. Each has its own license scheme, but the FortiGate-VMX Security Node license(s) are 'associated' with the FortiGate-VMX Service Manager license and are made available in its license repository after validation:

1. FortiGate-VMX Service Manager
 - Licensing the Service Manager requires the installation of a license file
 - A single Service Manager can handle an almost unlimited number of FortiGate-VMX Security Nodes so only one license is required.
 - The Service Manager must be able to connect to the Internet to validate its license against the FortiGuard Network
2. FortiGate-VMX instances
 - A license is required for each FortiGate-VMX instance deployed
 - Only one FortiGate-VMX Security Node is required per ESXi Host
 - It is kept simple in that 1 Security Node requires 1 license. RAM and virtual CPUs are not used when calculating license requirements.
 - The FortiGate-VMX Security Nodes receive their license from, and validate against the FortiGate-VMX Service Manager.

The licenses for the FortiGate-VMX Security Nodes are not assigned directly to the instance by the administrator, they are applied to the FortiGate-VMX Service Manager. The Service Manager keeps track of how many licenses have been purchased and how many are available for use. The total number of instances deployed is not as relevant as how many are concurrently in operation. As instances are deployed, licenses are allocated to them and when an instance is decommissioned, licenses are returned to the pool. If a deployment is attempted when there are no licenses left in the pool, the instance will be deployed, but when it requests a license from the FortiGate-VMX Service Manager, it will be denied and the Security Node will be considered 'invalid'. This means that any VM on that host will have its traffic blocked.

The information on FortiGate-VMX License usage is located in the licensing widget so if you are planning on future deployments you can quickly see if you have enough available licenses.



While the logical limit to the number of nodes that a Service Manager can handle is theoretically unlimited, there are practical limitations that are likely to limit the number. Things like IT resources may put an upper limit on how many instances can be effectively installed and managed.

Getting the License

The procedure for retrieving the license file is essentially the same as with FortiGate-VM.

When ordering the FortiGate-VMX Service Manager and FortiGate-VMX Security Nodes, you will receive a single license registration code. After registering the license with FortiCare, you will select the "License File Download" link for the FortiGate-VMX Service Manager.

Product Information

General

Product Model: FortiGate-VMX Service Manager
Serial Number: FGTVMX0000000158
License Number: FGVMX0000101
Registration Date: 2015-09-16
Description: Daniel Tests
Partner: N/A
FortiGate VMX Instance: [FGVMXI0000000101](#)
License File: [License File Download](#)
Type: Evaluation
Expiration Date: 2016-09-15

Edit

Installation of FortiGate-VMX Service Manager

The installation of FortiGate-VMX Service Manager shares a number of the same procedures as a FortiGate VM deployment. However, there are differences due to how the FortiGate-VMX Service Manager is integrated into the VMware environment and these differences warrant separate documentation of the installation procedure apart from that of a regular FortiGate-VM in VMware.

As noted prior, the Fortinet FortiGate-VMX security solution consists of two components: FortiGate-VMX Service Manager & FortiGate-VMX Security Node. This section will focus on the installation and configuration of the FortiGate-VMX Service Manager as FortiGate-VMX Security Nodes are automatically deployed and configuration synchronization is done when communicating with the FortiGate-VMX Service Manager.

Assumptions

Because the successful installation of this product depends on a third-party technology that is responsible for its own documentation, some assumptions will have to be made in reference to the instructions and documentation for the installation.

- The installer has knowledge of the required VMware components that will be interacting with FortiGate-VMX Service Manager.
- All of the VMware components required are already installed, configured, licensed, and communicating properly.
- Distributed Virtual Switches have been properly configured to allow traffic to and from the setup.

Configuring ESXi Agent VM Settings

The Agent VM Settings must be properly set on each ESXi host which you plan to make part of the cluster. For larger environments, these values can also be configured via the NSX Manager during the Service Deployment step.

Relevant settings

Datastore

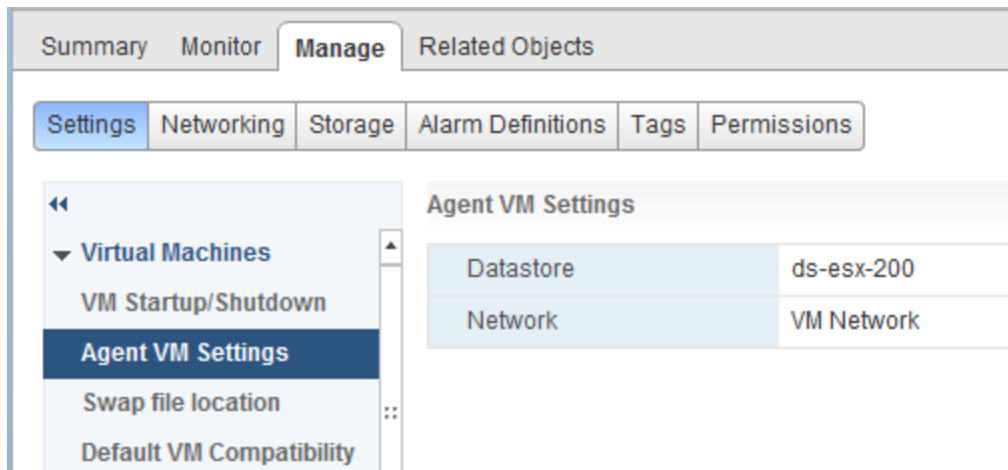
Used when deploying the FortiGate -VMX Security Node to the host. The Datastore setting is where the Service VM's files will reside. In Fortinet's case, the Service VM is a FortiGate-VMX Security Node

Network

The Network setting is for communication between the FortiGate-VMX Service Manager and FortiGate-VMX Security Node instance.

How to configure them:

1. Log into the vCenter Server with the vSphere Web Client.
2. Select the **Manage** tab for each ESXi host.
3. Under **Settings**, look for **Agent VM Settings** in the left pane.
4. Click Edit
5. Select Datastore and set the value
6. Select Network and set the value



Fortinet recommends choosing a local Datastore if one is available

Registering FortiGate-VMX Service Manager

In order to properly license FortiGate-VMX Service Manager you will need the correct license file. To obtain the license file, the FortiGate-VMX Service Manager must be registered with Fortinet Customer Service & Support.

To register the FortiGate VMX Service Manager:

1. Go to the Fortinet Customer Service & Support website at: <https://support.fortinet.com>
2. Log in to the Customer Service & Support portal
 - Use an existing support account or select Sign Up to create a new account
4. Go to the **Asset** section on the page or select the **Asset** tab at the top of the page, and choose **Register/Renew**. The **Registration Wizard** page will open.
5. The first step in the Wizard is to specify a registration code. Enter the registration code that was emailed to you in the field. select **Next**.

6. Complete filling out the fields in the wizard. There are 4 pages to the wizard.
7. After completing the wizard, a registration acknowledgment page will appear.
8. Select the **License File Download** link.
9. You will be prompted to save the license file (.lic) to your local computer.
10. Once the FortiGate-VMX Service Manager has been installed, the license file can be upload and the registration process can be completed. See "Uploading FortiGate-VMX license file" for instructions in the process.



Downloading the images

Like all FortiGate images, whether firmware for hardware appliances or virtual instances, the images for FortiGate-VMX products are found on the Fortinet Customer Service & Support site.

1. Login to the site with your credentials
2. Got to the **Download** section
3. Select **Firmware Images**
4. In the **Select Product** drop down menu, select **FortiGate**.
5. Select the **Download** tab
6. From the **Image Folders/Files** list, choose **v5.00**
7. From the resulting secondary sub-list, choose the **5.4** directory
8. From the resulting tertiary sub-list, choose the version that you wish to install. The earliest firmware version that includes FortiGate-VMX v2 is **5.4.0**
9. There are two image files that you will need.
 - The image for the FortiGate-VMX Service Manager - these files will have the prefix `FGT_VM64_SVM-v5-build`
 - The image for the FortiGate-VMX Security Node - these files will have the prefix `FGT_VM64_VMX-v5-build`

For each of these prefexes there will be two variations of file extensions; the `.out` file or the `.out.ovf.zip` file.

Below is an example of what the file links will look like:

	<code>FGT_VM64_SVM-v5-build[REDACTED]-FORTINET.out</code>
	<code>FGT_VM64_SVM-v5-build[REDACTED]-FORTINET.out.ovf.zip</code>
	<code>FGT_VM64_VMX-v5-build[REDACTED]-FORTINET.out</code>
	<code>FGT_VM64_VMX-v5-build[REDACTED]-FORTINET.out.ovf.zip</code>

The files that need to be downloaded are the deployment packages for each component. These will be the ones with the extension: `.out.ovf.zip`.



Other things that you may want to consider downloading are the checksums of the files to verify that you got a good copy and the Release Notes for the FortiGate firmware version that you downloaded.

Once you have downloaded the deployment packages, the files will need to be extracted from the zip file. There are a number of applications and utilities that will do this. Use whichever is available to you depending upon the OS of the system that you downloaded the files to.

Deployment Package Contents

FortiGate-VMX Service Manager .out.ovf.zip:

- `FortiGate-VMX-Service-Manager.ovf` - OVF template file
- `fortios.vmdk` - FortiGate-VMX Service Manager system hard disk in VMDK format
- `datadrive.vmdk` - FortiGate-VMX Service Manager log disk in VMDK format

The contents of the FortiGate VMX Service Manager package only needs to be placed in a folder, where you will remember where to find it, on the computer that you will be doing the deployment from.

FortiGate-VMX Security Node .out.ovf.zip:

- `FortiGate-VMX.ovf` - OVF template file
- `fortios.vmdk` - FortiGate-VMX system hard disk in VMDK format
- `datadrive.vmdk` - FortiGate-VMX log disk in VMDK format (not currently used)

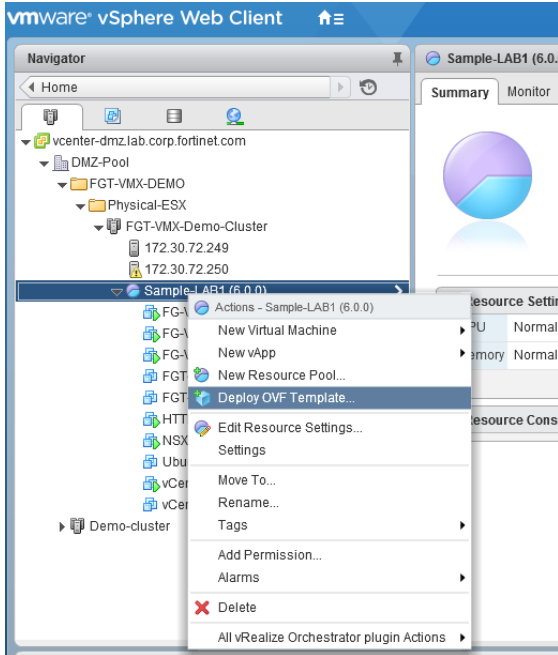
The contents of the the FortiGate-VMX Security Node package will need to be place on a webserver that can be accessed by the VMware NSX Manager for generating new instances of the security node.

Placing FortiGate-VMX Security Node files on the Web Server

There are no special requirements for the placing of the files on the web server other than making sure the access and permissions allow the downloading of the files by the use of a URL. Placing the files on the web server should be an easy step but it is an important one because deployment cannot occur if the files are not there.

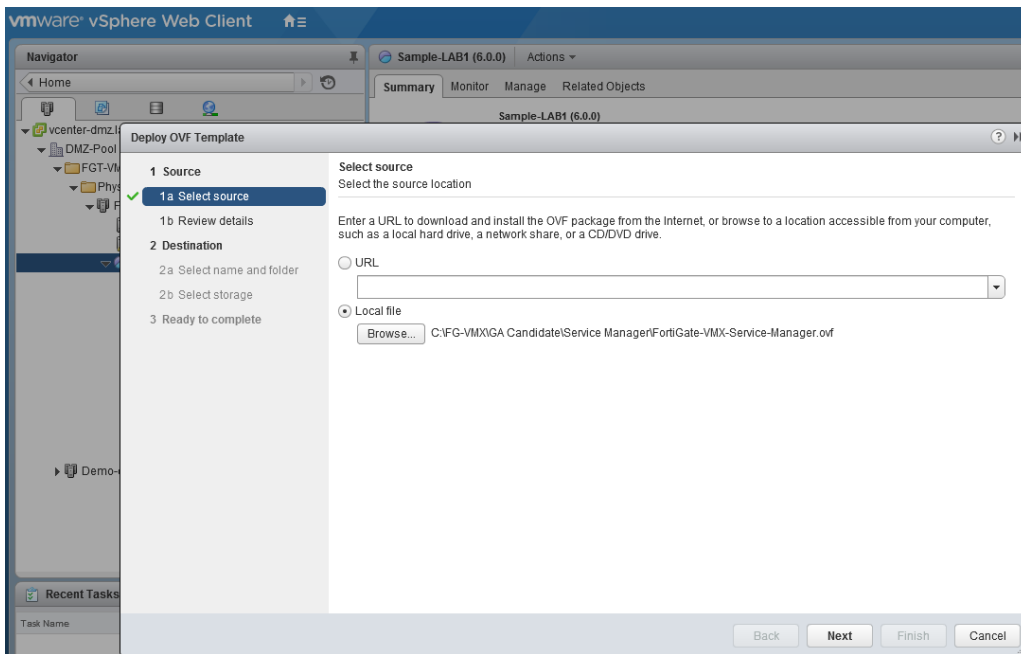
Deploying the FortiGate-VMX Service Manager

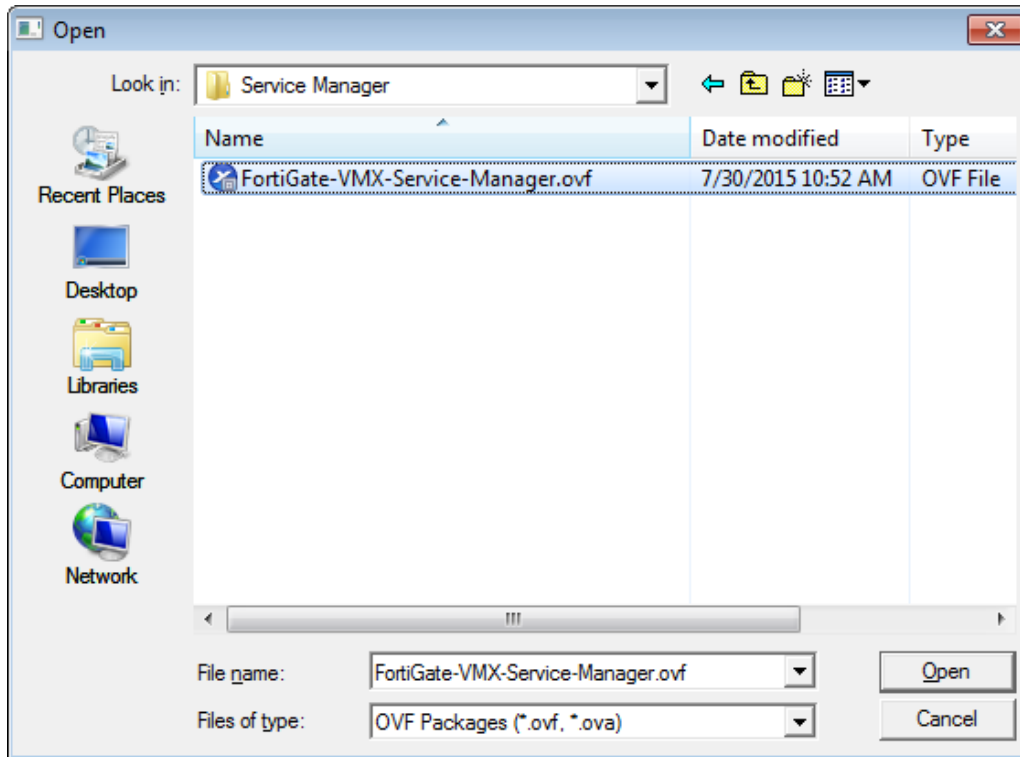
1. Using VMware's vSphere Web Client, select the virtual instance that you which to use, right-click on it to reveal the drop down menu and select **Deploy OVF Template** to open the OVF deployment wizard.



2. Select Source

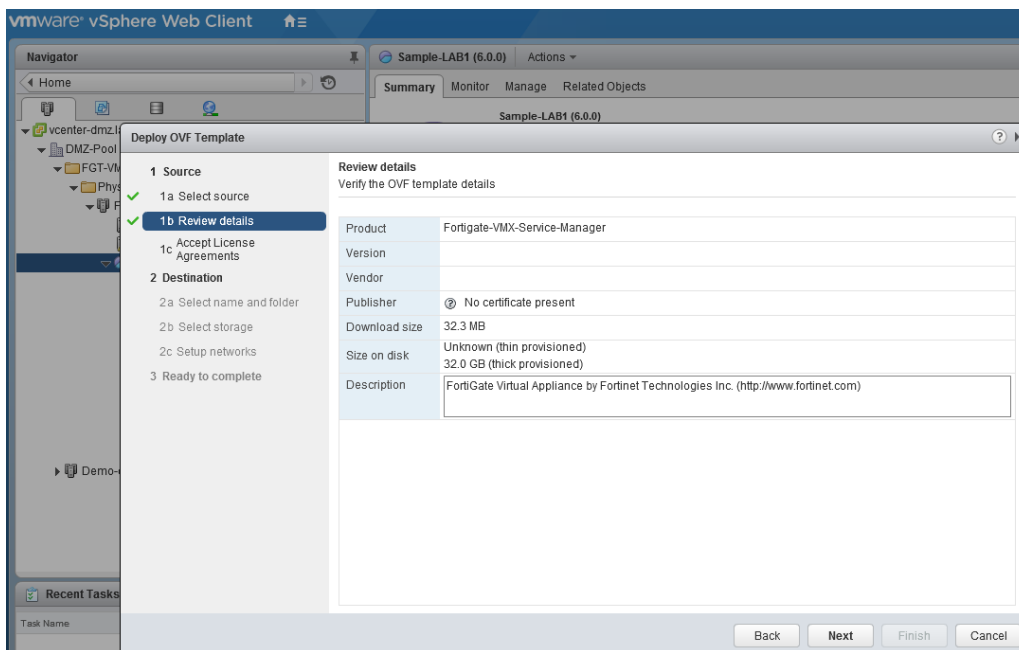
- Select **Local File** and browse to the FortiGate-VMX-Service-Manager.ovf file.
- Press **Next**.





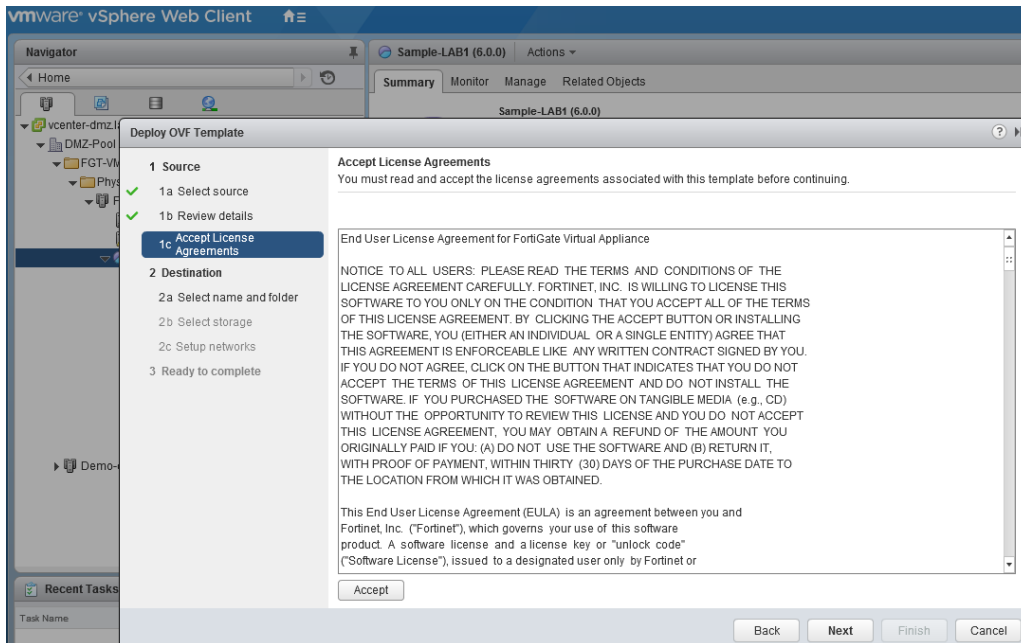
3. Review details

- Review the information about the location of the OVF file to make sure that it is correct.
- Press the **Next**.



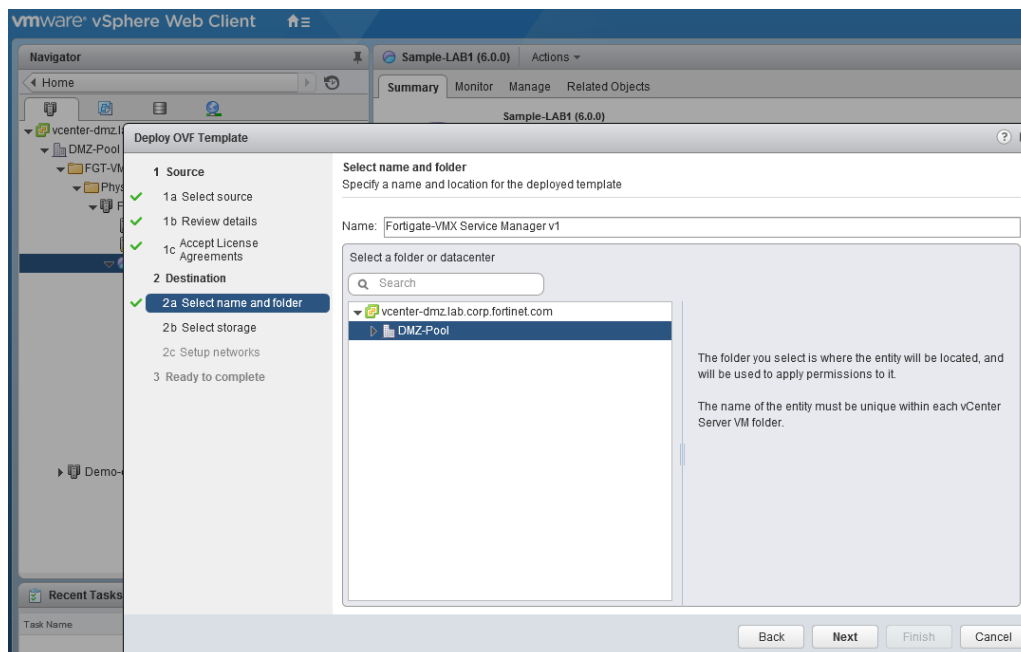
4. Accept Licence Agreements

- Read the EULA and if you accept it press **Accept**.
- Press **Next**.



5. Select name and folder

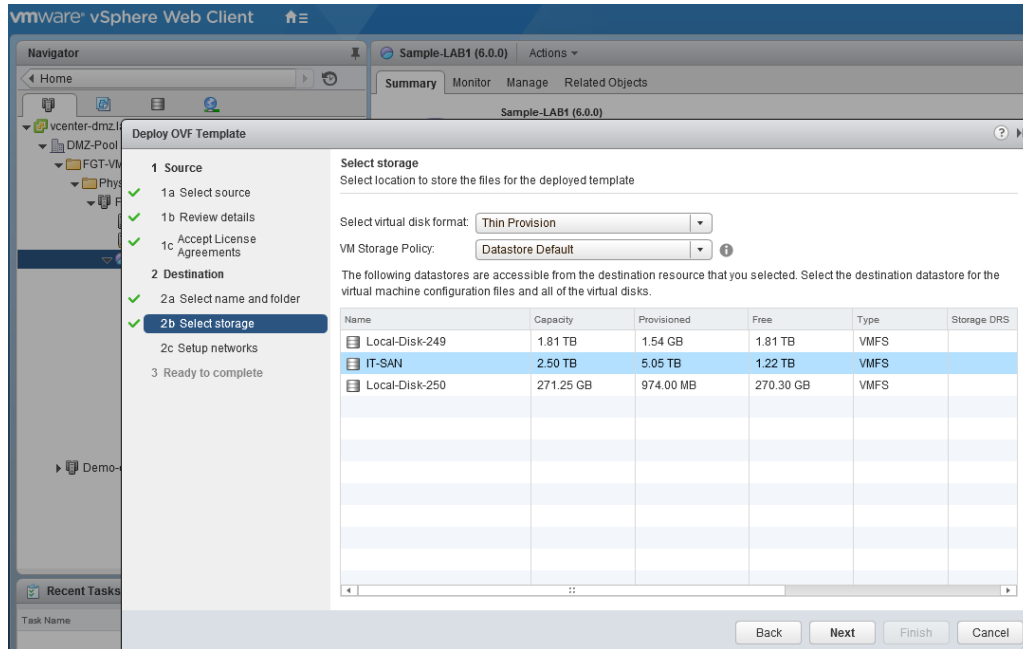
- Enter a name for the instance in the **Name** field
- Select a location for this instance to be placed.
- Press **Next**.



6. Select storage

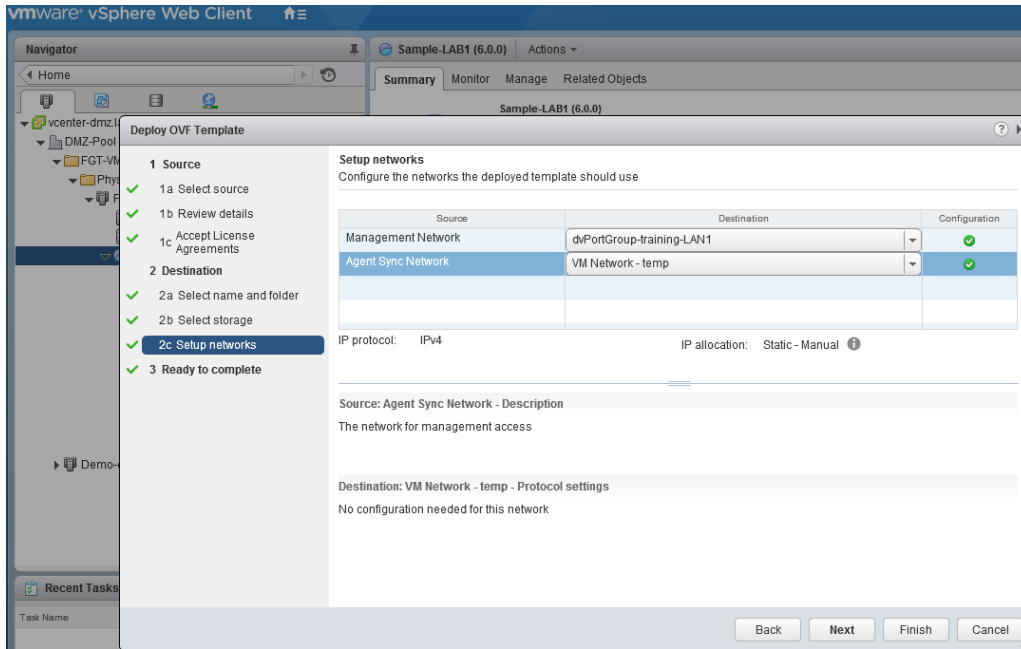
- Select the **virtual disk format** from its drop down menu.

- Select the **VM Storage policy** from its drop down menu.
- Select the destination datastore from the list of available datastores.
- Press **Next**.



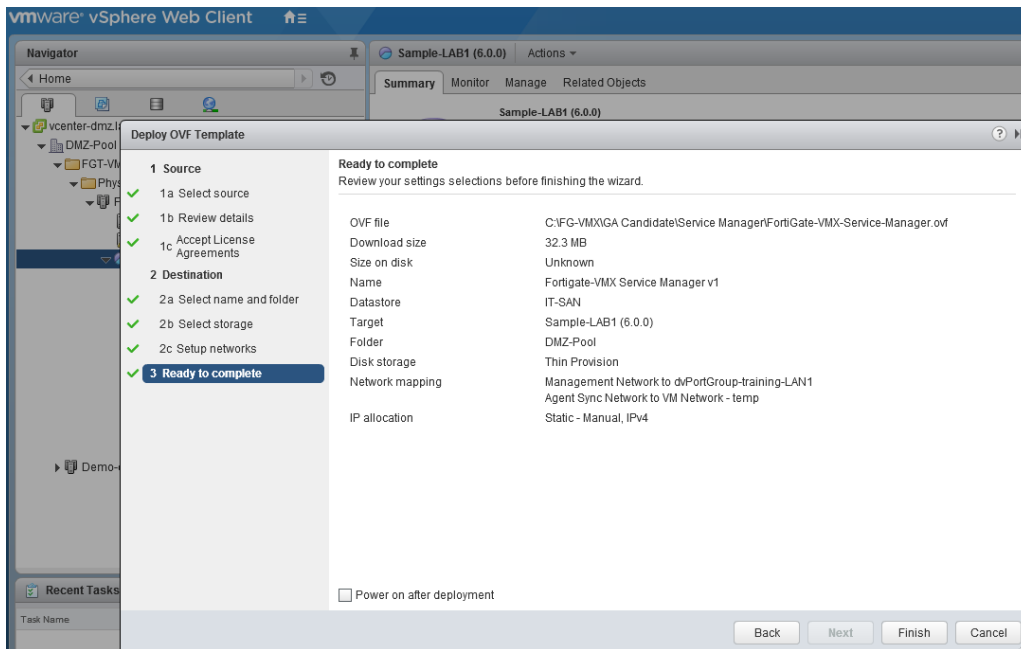
7. Setup networks

- Select a **Management Network** that the deployed template should use from the drop down menu. This will be the network that is used to communicate between the FortiGate-VMX Service Manager and the VMware components as well as connecting to the FortiGate-VMX Server Manager Web Interface or other Management communications.
- Select an **Agent Sync Network** that the deployed template should use from the drop down menu. This will be the network that will be used for all communications between the FortiGate-VMX Service Manager and FortiGate-VMX Security Node instances. It is recommended that this should be a closed network with only FortiGate-VMX components connected to it.
- Press **Next**.



8. Ready to complete

- Review the settings to make sure they are correct.
- Press **Finish**.



Configuring FortiGate-VMX Service Manager

The following steps need to be completed to establish a basic FortiGate-VMX Service Manager setup.

Configure FortiGate-VMX Service Manager MGMT Interface

Before you can connect to the FortiGate-VMX Service Manager web-based manager you must configure a network interface in the FortiGate-VMX Service Manager console. This is done by using the console feature of VMware to connect to the VM in a terminal emulator mode.

Set MGMT port IP address

Using the CLI type in the following commands:

```
config global
  config system interface
    edit mgmt
      set ip <IP address for the MGMT interface > <subnet mask>
      set allowaccess ping https ssh http
    end
```

Set default gateway

Using the CLI type in the following commands:

```
config vdom
  edit root
    config router static
      edit 0
        set device mgmt
        set gateway <IP address of gateway>
      end
```

Set DNS

Using the CLI type in the following commands:

```
config global
  config system dns
    set primary <IPv4 address of DNS server>
    set secondary <IPv4 address of DNS server>
  end
```

Once you have configured the management interface you should be able to connect through the Web-based user interface to complete the configuration.



An added reason to make sure that the network settings are properly configured is that the FortiGate-VMX Service Manager requires Internet connectivity to validate its license against FDN. A regular FortiGate-VM can validate against a FortiManager but this capability is not supported by FortiGate-VMX.

Connecting to the FortiGate-VMX Service Manager Web UI

The Graphic User Interface (GUI) of the FortiGate-VMX Service Manager is web-based so before it can be used the MGMT port must be configured with an IP address and netmask. The default gateway and DNS should also be set up.

1. Opening up a browser
2. Enter in the URL field, the IP address that was assigned to the MGMT port.
3. At the login page, enter your credentials into the **Name** and **Password** fields
4. Select **Login**



The default username on a factory fresh system will be "admin". There is no default password. Leave the field blank. As always, a password should be set up as soon as possible.

Uploading FortiGate-VMX Service Manager license file

The FortiGate-VMX license files are uploaded to the FortiGate-VMX Service Manager through the FortiGate-VMX Service Manager's GUI.

The Login page will include a setting called **Evaluation License**.

1. At Select **Enter License**
2. This will reveal the **License Upload** page
3. Select **Browse** and locate the license file (.lic) on your computer.
4. Select **OK** to upload the license file.
5. Refresh the browser to login.
6. Enter admin in the Name field and select Login. The Virtual Machine License registration status appears as Valid in the License Information widget once the license has been validated by the FortiGuard Distribution Network (FDN).

VMware settings

The Web-based interface should be familiar to anyone that has worked with FortiGates or FortiGate-VMs. The only significant difference should be that there is now a VMware setting.

1. In the FortiGate VMX Service Manager GUI, go to **Global > VMware > Settings**
2. Configure the connection to the NSX Manager
 - Use the **Hostname** field to enter the IP address of the server
 - Use the **Username** and **Password** fields to enter credentials that have sufficient privileges on the server
3. Set the location of the FortiGate-VMX Security Node
 - The **Image Location** field should contain the URL of the webserver where the FortiGate-VMX Security Node `.ovf` file is located.

FortiGate VMX-Service-Manager FGTVMX0000000158

Global | SVM Settings

Dashboard | Network | **VMware** | Settings | System | Log & Report

NSX Manager

Hostname: 172.30.70.136

Username: admin

Password: ●●●●●●

VMX

Service Name: FGTVMXv2

Image Location: http://172.30.70.138/FortiGate-VMX.

REST API

Port: 9443

Interface: mgmt

Apply

Interface settings

There are two ports on the FortiGate-VMX Service Manager. The MGMT port was configured through the CLI in order to enable access to the Web-based user interface. This section covers configuration of the 'sync' network. The 'sync' network is only used for communication between FortiGate-VMX Security Nodes and the FortiGate-VMX Service Manager.

Fortinet recommends the 'sync' network to be a closed network, only used by FortiGate-VMX components for communication. While a corporate DHCP server may be used for enabling IP addresses on FortiGate-VMX Security Nodes, the FortiGate-VMX Service Manager has those capabilities built into it. Setting a static IP address on the 'sync' interface and using the interface DHCP server is the preferred approach.

To configure the 'sync' network, log into the FortiGate-VMX Service Manager and go to **Global > Network > Interfaces**.

1. Set the **Addressing Mode** to **Manual**
2. Enable the **DHCP Server** function by checking the **Enable** box
3. Select Create New to define an address ranges scope that is large enough to handle the likely number of VMX instances that you are going to be creating. Choose an IP addressing scheme and starting point that will allow for growth beyond the number of initial FortiGate-VMX licenses acquired.

- Global
- Dashboard
- Network
- Interfaces
- DNS
- VMware
- System
- Log & Report

Edit Interface

Address

Addressing mode: **Manual** | DHCP | Dedicated to FortiAP
IP/Network Mask: 4.4.4.1/255.255.255.0

Restrict Access

Administrative Access: HTTPS PING HTTP FMG-Access
 CAPWAP SSH SNMP RADIUS Accounting

DHCP Server

Address Range

+ Create New	Edit	Delete
Starting IP	End IP	
4.4.4.21	4.4.4.54	

Netmask: 255.255.255.0

Default Gateway: **Same as Interface IP** | Specify

DNS Server: **Same as System DNS** | Same as Interface IP | Specify

[+ Advanced...](#)

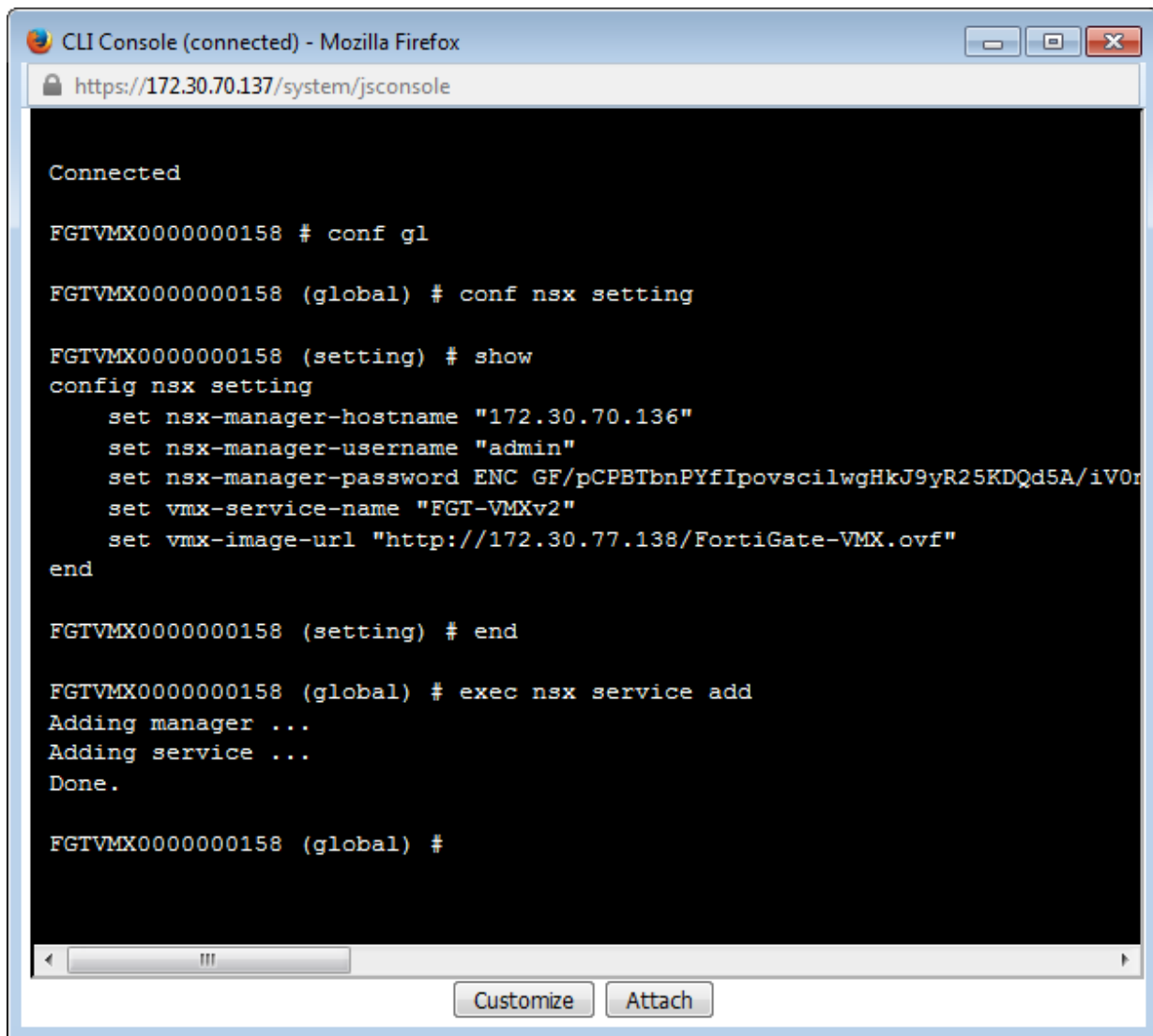
Register FortiGate-VMX Service

1. Login to FortiGate-VMX Service Manager
2. Open the **CLI Console** widget in **Global -> Dashboard**
3. Enter the following commands

```
config global
  exec nsx service add
```

The above command should result in the following output:

```
Adding manager ...
Adding service ...
Done.
```



```
CLI Console (connected) - Mozilla Firefox
https://172.30.70.137/system/jsconsole

Connected

FGTVMX0000000158 # conf gl

FGTVMX0000000158 (global) # conf nsx setting

FGTVMX0000000158 (setting) # show
config nsx setting
  set nsx-manager-hostname "172.30.70.136"
  set nsx-manager-username "admin"
  set nsx-manager-password ENC GF/pCPBTbnPYfIpovscilwgHkJ9yR25KDQd5A/iVOr
  set vmx-service-name "FGT-VMXv2"
  set vmx-image-url "http://172.30.77.138/FortiGate-VMX.ovf"
end

FGTVMX0000000158 (setting) # end

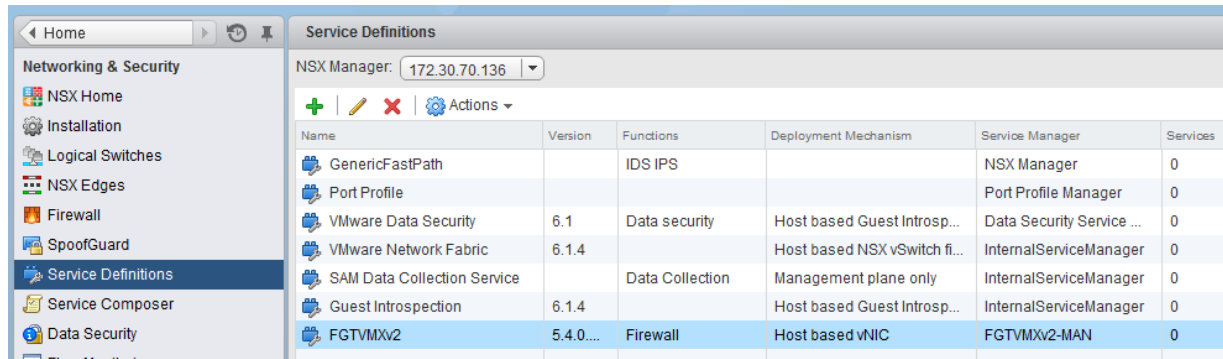
FGTVMX0000000158 (global) # exec nsx service add
Adding manager ...
Adding service ...
Done.

FGTVMX0000000158 (global) #
```

Verify service definition has been added in NSX Manager

1. Log in with the vSphere Web Client
2. Choose **Networking & Security**
3. Select **Service Definitions**

You should see the service located in the output.

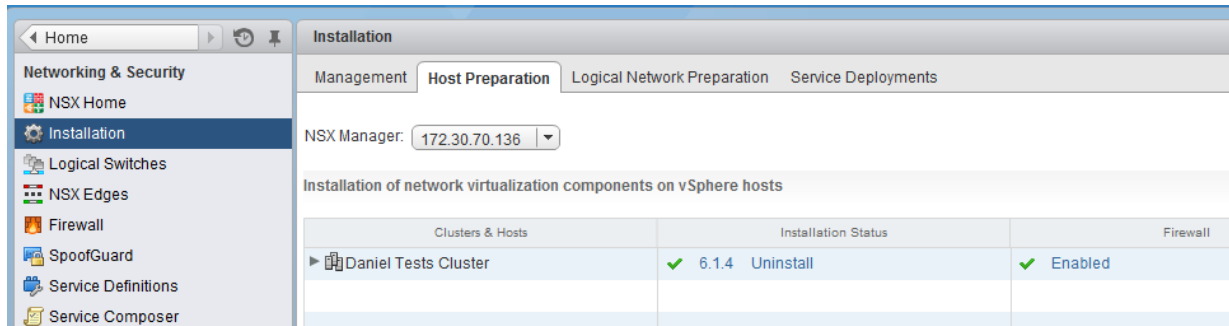


Name	Version	Functions	Deployment Mechanism	Service Manager	Services
GenericFastPath		IDS IPS		NSX Manager	0
Port Profile				Port Profile Manager	0
VMware Data Security	6.1	Data security	Host based Guest Introspection	Data Security Service Manager	0
VMware Network Fabric	6.1.4		Host based NSX vSwitch	InternalServiceManager	0
SAM Data Collection Service		Data Collection	Management plane only	InternalServiceManager	0
Guest Introspection	6.1.4		Host based Guest Introspection	InternalServiceManager	0
FGTVMX2	5.4.0...	Firewall	Host based vNIC	FGTVMX2-MAN	0

NSX host preparation of cluster

If you have not already installed NSX on the hosts of the cluster, please do so now

1. Log in with the vSphere Web Client
2. Choose **Networking & Security**
3. Select **Installation**
4. Click the **Host Preparation** tab
5. Under **Installation Status**, select **Install**



Service Deployment

1. Log in with the vSphere Web client
2. Choose **Networking & Security**
3. Select **Installation**
4. Click the **Service Deployments** tab

The screenshot shows the 'Deploy Network & Security Services' interface. On the left, a sidebar lists four steps: 1. Select services & schedule (highlighted), 2. Select clusters, 3. Select storage and Management Network, and 4. Ready to complete. The main area is titled 'Select services & schedule' and contains the instruction: 'Select one or more Network & Security services to deploy. You can also specify the schedule for deployment.' Below this is a 'Select services:' section with a table:

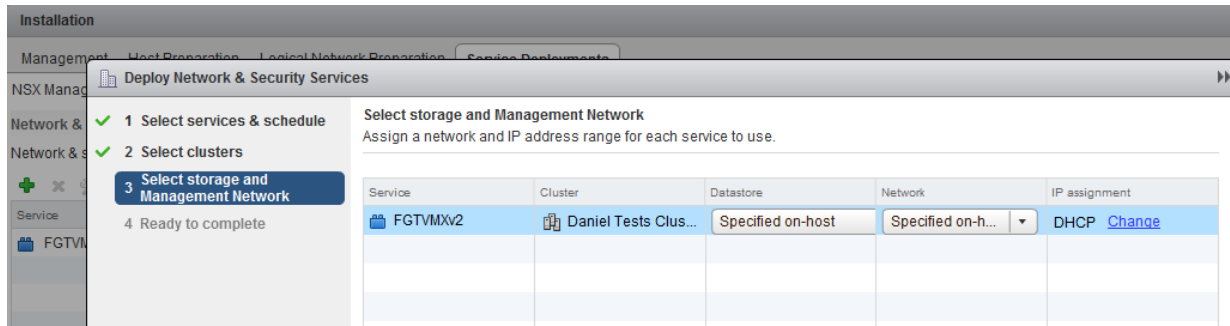
<input type="checkbox"/>	Name	Description	Category
<input type="checkbox"/>	VMware Data Security	Discovery of sensitive data at rest	
<input type="checkbox"/>	Guest Introspection	Base service for all solutions based ...	
<input checked="" type="checkbox"/>	FGTVMXv2		

5. Add a new Service Deployment, choose the name of the service you inserted and click **Next**
6. Designate the cluster upon which you wish to deploy the FortiGate-VMX security service and click **Next**

The screenshot shows the 'Deploy Network & Security Services' interface. On the left, a sidebar lists four steps: 1. Select services & schedule (marked with a green checkmark), 2. Select clusters (highlighted), 3. Select storage and Management Network, and 4. Ready to complete. The main area is titled 'Select clusters' and contains the instruction: 'Select one or more clusters on which to deploy the service(s). If service will be upgraded.' Below this is a 'Datacenter:' dropdown menu with 'QA Test DC' selected. At the bottom, there is a table:

<input checked="" type="checkbox"/>	Name
<input checked="" type="checkbox"/>	Daniel Tests Cluster

7. Datastore and Network have already been configured in the **VM Agent Settings** for each host back in an earlier step in this document



8. Click **Finish**

Configuring Security Groups and Re-Direction Policy

Configuring NSX Security Groups

Not only does NSX Manager configure re-direction rules based on Security Groups, it also enables FortiGate-VMX Service Manager to create policy based on Security Group objects.

1. Log in with the vSphere Web Client
2. Choose **Networking & Security**
3. Select **Service Composer**
4. Click the **Security Groups** tab and add or edit an existing Security Group

Define dynamic membership

Specify dynamic membership criteria that objects must meet to be part of this security group.

Membership criteria 1

Match: Any of the criteria below

Criteria Details

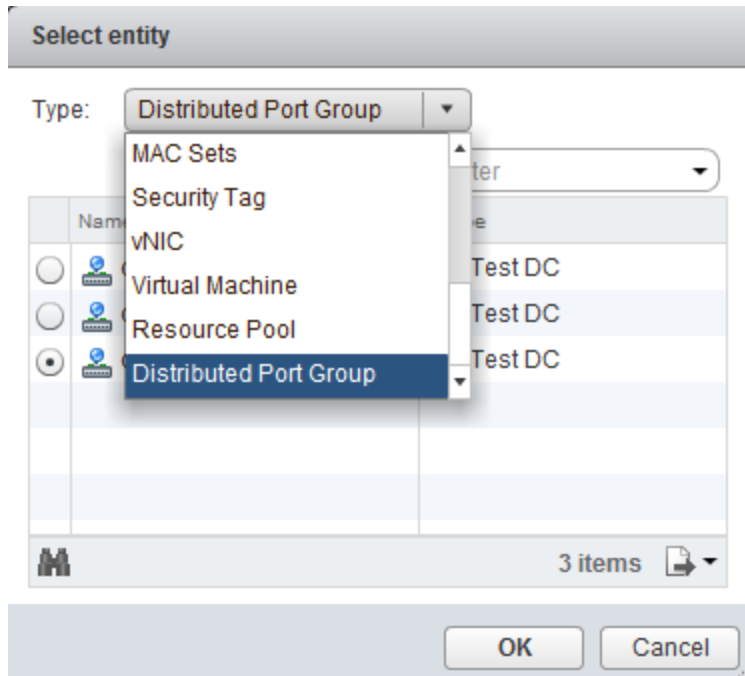
Entity	Belongs to	dvPortGroup-Server
--------	------------	--------------------

Back Next Finish Cancel

You can set up static or dynamic Security Groups. VMware entities can encompass any of 14 different options:

- Security Groups - Clusters
- Logical Switches
- Legacy Port Groups
- Networks
- vApps
- Datacenters
- IP Sets
- MAC Sets
- Security Tags

- vNICs
- Virtual Machines
- Resource Pools
- Distributed Port Groups

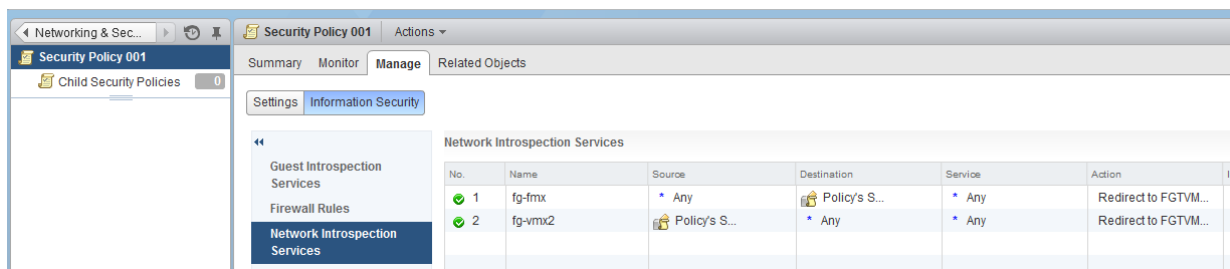
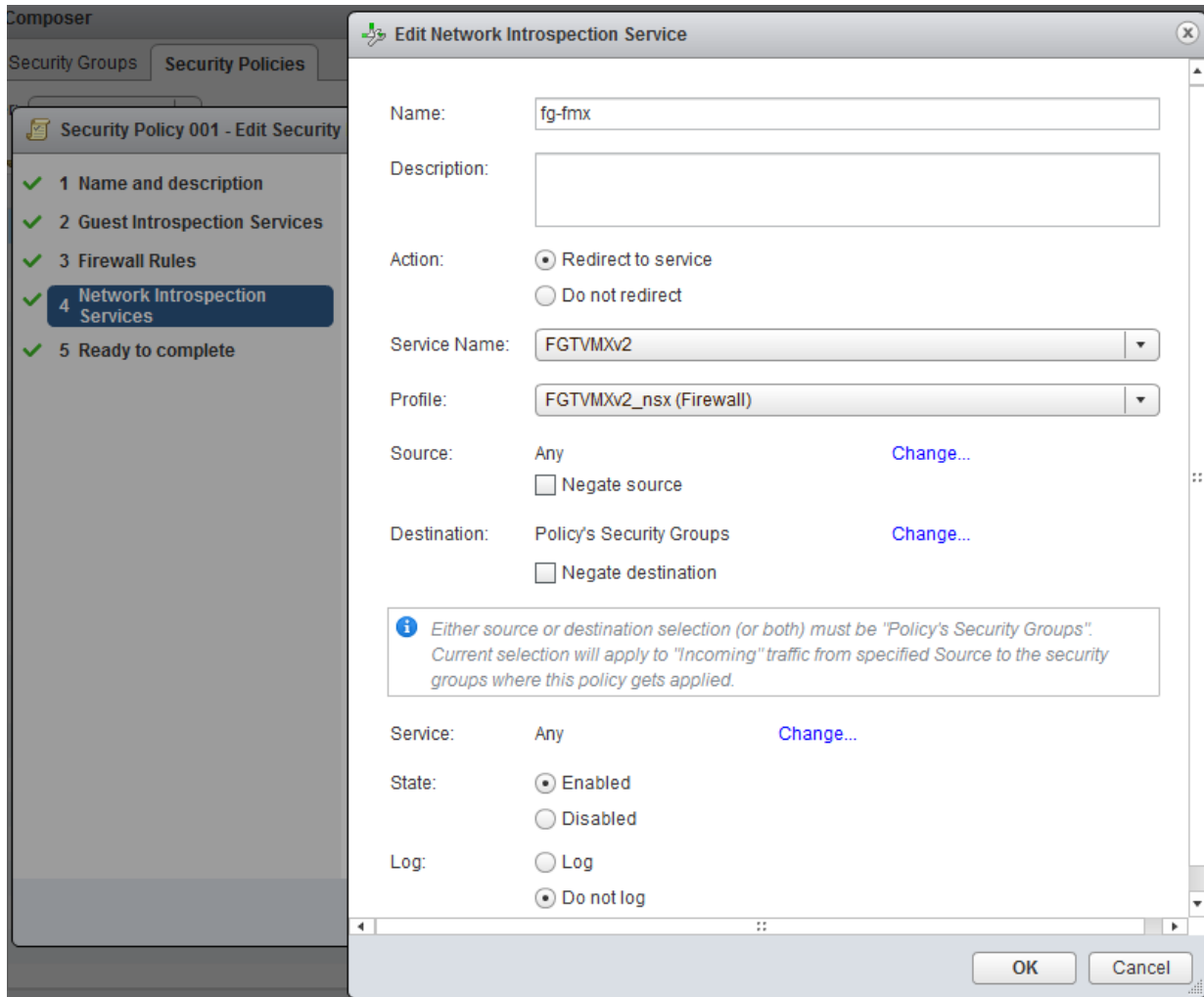


Re-Direction Security Policy

1. Log in with the vSphere Web Client
2. Choose **Networking & Security**
3. Select **Service Composer**
4. Click the **Security Policies** tab
5. Add a new security policy; give it a name and description

The screenshot shows the 'Service Composer' interface with the 'Security Policies' tab selected. A 'New Security Policy' dialog box is open, displaying a progress list on the left and configuration fields on the right. The progress list includes: 1 Name and description (selected), 2 Guest Introspection Services, 3 Firewall Rules, 4 Network Introspection Services, and 5 Ready to complete. The configuration fields include: Name (Security Policy 002), Description (empty), Inherit security policy (unchecked), and Parent policy (dropdown menu). An 'Advanced options' section is collapsed. At the bottom, there are 'Back', 'Next', 'Finish', and 'Cancel' buttons.

6. Set the **Network Introspection Service**; choosing the Service Name, Profile, source and destination (at this stage you may also choose services as well, but we generally recommend “**Any**” as the proper setting – hit **OK**, **Next** and **Finish**)



Security Policy 001

Description:

Weight: 4300

Inherits from:

Guest Introspection Services			
No.	Name	Action	Enforce

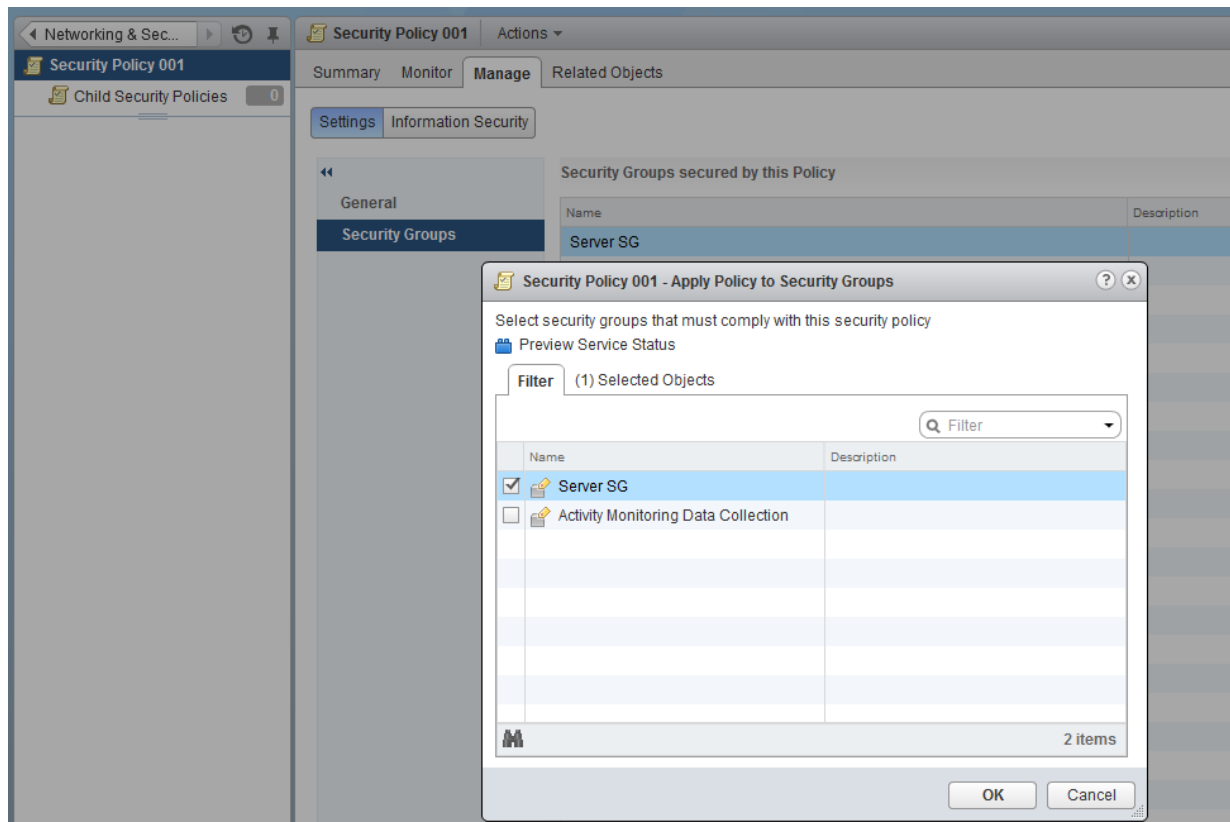
Network Introspection Services					
No.	Name	Source	Destination	Service	Action
✓ 1	fg-fmx	* Any	Policy's S...	* Any	Re...
✓ 2	fg-vmx2	Policy's S...	* Any	* Any	Re...



The Security Policy requires creation of rules for re-direction of both inbound and outbound traffic for the designated sources and destinations.

Associating a Security Group to Re-Direction Security Policy

1. Click on the Security Policy name
2. Select the **Manage** tab
3. Under **Settings**, choose **Security Groups**
4. Click **Edit** and add all Security Groups you wish to associate with this re-direction Security Policy



1. Click **OK**

A Note About VMware Tools and IP Sets

VMware Tools is generally required to be running on all VMs to be protected in this environment. This is the best and most secure method for enabling future changes to the workloads without any added steps. If it's not possible to have VMware Tools running on protected VMs, you may optionally use IP Sets.

The following are directions to be used in such circumstances.

IP Set Creation

1. Log in with vSphere Web Client
2. Choose **Networking & Security**
3. Under **Networking & Security Inventory**, select **NSX Managers**
4. Click on the **NSX Manager** under the **Objects** tab
5. Select **IP Sets**
6. Create a new IP Set; enter the name, description and IP address

Add IP Addresses [?] [x]

IP addresses grouping must be defined under the global scope or under the scope of a datacenter or a portgroup. IP address grouping defined under the global scope is visible at all datacenters and portgroups.

Scope: Global

Name: * test ip set

Description: test for re-direction

IP Addresses: * 10.1.1.36

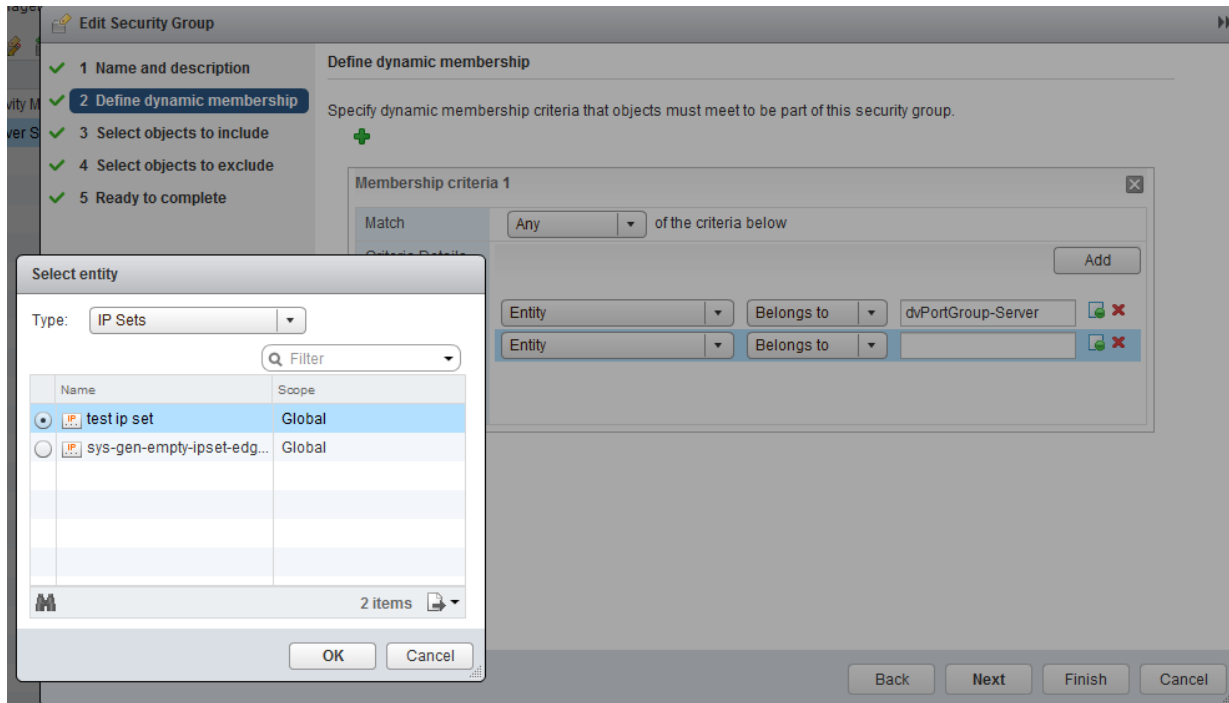
eg: 192.168.200.1, 192.168.200.1/24, 192.168.200.1-192.168.200.24

Enable inheritance to allow visibility at underlying scopes

OK Cancel

Associate the IP Set with the Security Group

1. In **Service Composer** -> **Security Groups**, edit the **Security Group**
2. Add the IP Set either through direct inclusion or dynamic membership
3. Click **Finish**



SpoofGuard in NSX

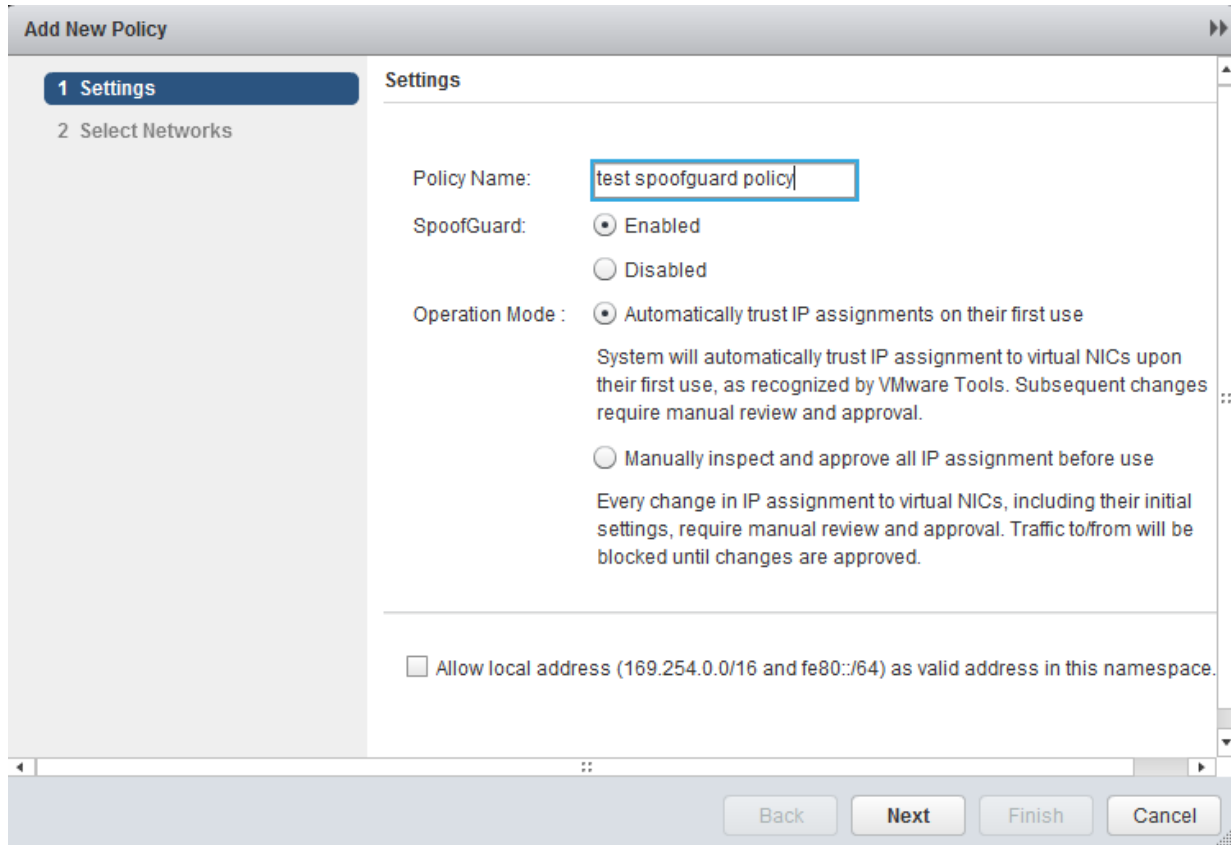
After synchronizing with the vCenter Server, NSX Manager collects the IP addresses of all vCenter guest virtual machines from VMware Tools on each virtual machine. If a virtual machine has been compromised, the IP address can be spoofed and malicious transmissions can bypass firewall policies.

You create a SpoofGuard policy for specific networks that allows you to authorize the IP addresses reported by VMware Tools and alter them if necessary to prevent spoofing. SpoofGuard inherently trusts the MAC addresses of virtual machines collected from the VMX files and vSphere SDK. Operating separately from Firewall rules, you can use SpoofGuard to block traffic determined to be spoofed.

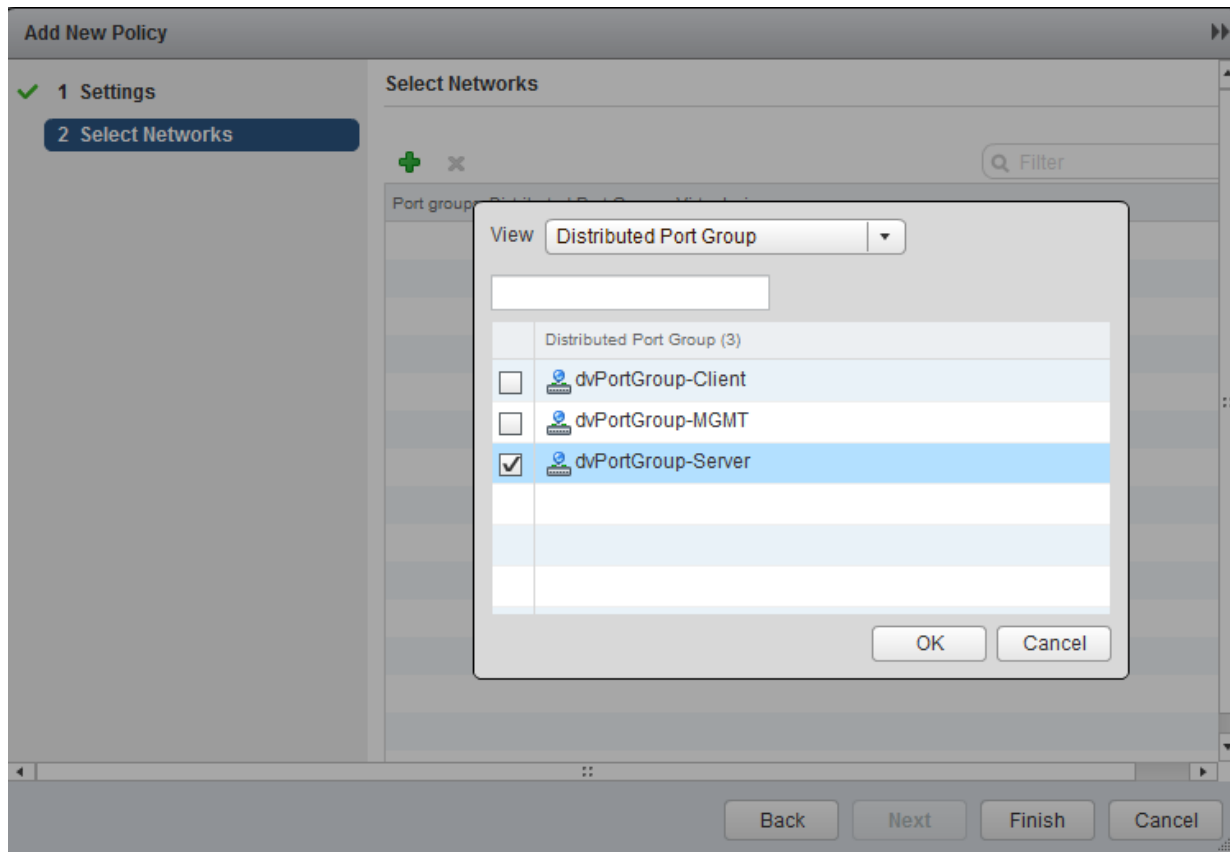
SpoofGuard supports both IPv4 and IPv6 addresses. When using IPv4, the SpoofGuard policy supports a single IP address assigned to a vNIC. IPv6 supports multiple IP addresses assigned to a vNIC. The SpoofGuard policy monitors and manages the IP addresses reported by your virtual machines in one of the following modes.

Enable SpoofGuard

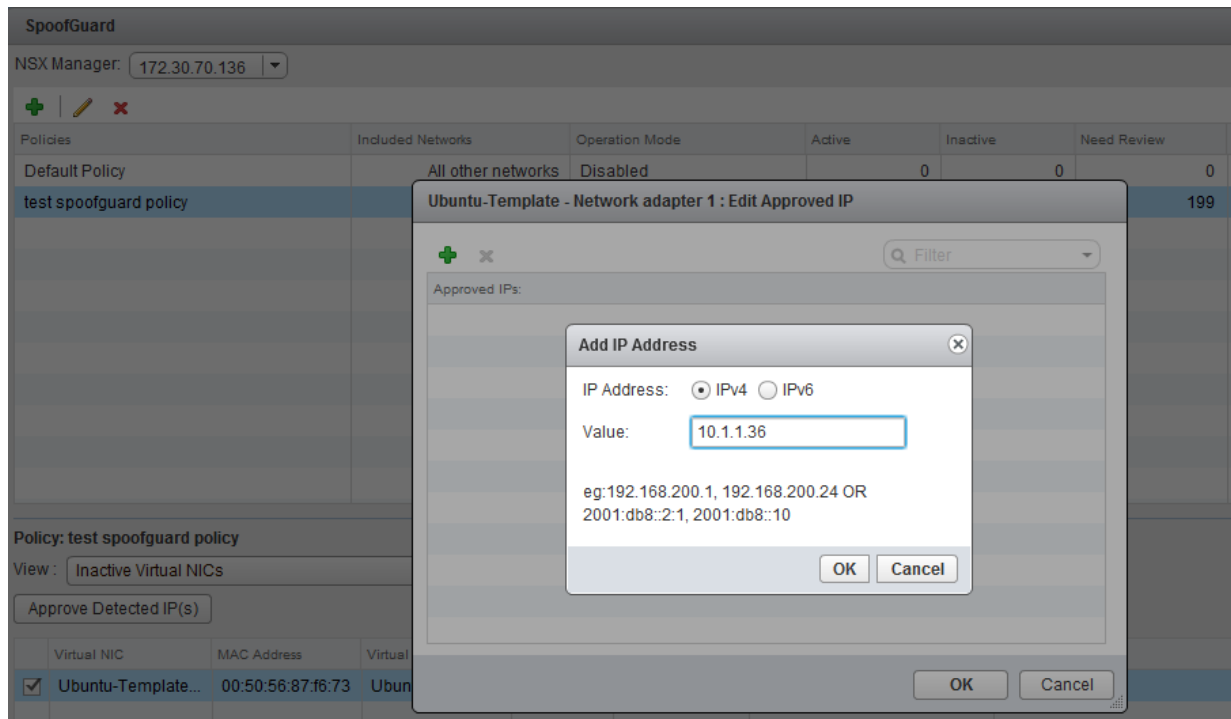
1. Login with the vSphere Web Client
2. Choose **Networking & Security**
3. Select **SpoofGuard**
4. Create or edit an existing SpoofGuard policy and enable it



5. Select the proper Network



6. Click **Finish**
7. Highlight the SpoofGuard Policy and in the lower section of screen, choose **Inactive Virtual NICs** in the View section
8. Edit the Virtual NIC IP address under **Approved IP**



Setting Policies

Setting policies in FortiGate-VMX doesn't look that much different than setting up a policy on any other FortiGate product except for a few minor differences.

The policies for the FortiGate-VMX Security Node are set up on the FortiGate-VMX Service Manager.

Go to **Virtual Domains > nsx > Policy & Objects > Policy > IPv4**.

In this version of FortiGate-VMX, we support a limited number of Virtual Domains (VDOMs). Each VDOM will have a virtual (internal) internal & external port. These interfaces are the two ends of a port pairing. As stated earlier, traffic is intercepted between the given vNIC of a VM and its port on the dvSwitch. In effect, the 'internal' port can be considered the VM itself and the 'external' port as everything else. Policy is based on NSX Security Groups as source and destination.

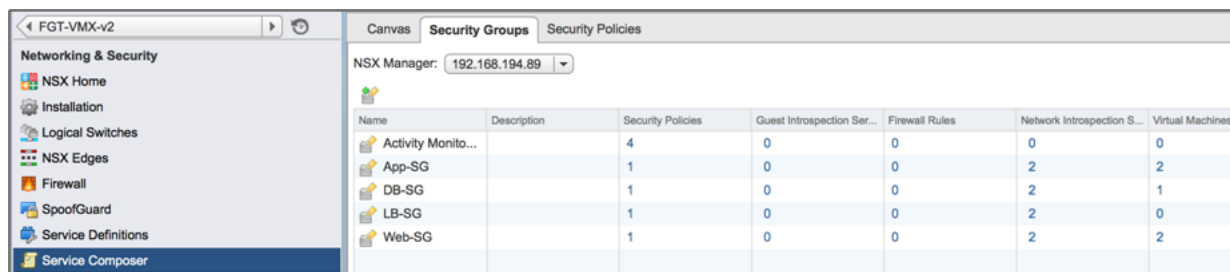
The default VDOM is "nsx" and its two virtual interfaces are "internal" and "external". For all other created VDOMs, the port pairs are named as follows:

1. <VDOM name>-int: the VM itself
2. <VDOM name>-ext: everything else

When setting up a new policy, instead of matching up physical or virtual ports, all that really needs to be done is determine whether the traffic is inbound to the VM or outbound to everything else. All other parameters involved in a policy such as Service, Action, Schedule, Security profiles etc are just like a regular FortiGate. For instructions on the detailed operation and administration of a FortiGate Firewall see the FortiOS manuals. You can either choose the [FortiOS Handbook - The Complete Guide to FortiOS](#) or one of the specific topic handbooks found at [The Fortinet Document Library - http://docs.fortinet.com](http://docs.fortinet.com).

An example of synchronized NSX Security Group objects and FortiGate-VMX Security Policy are seen below.

Dynamic Security Groups created in NSX Manager.



The screenshot shows the NSX Manager interface with a table of Security Groups. The table has columns for Name, Description, Security Policies, Guest Introspection Ser..., Firewall Rules, Network Introspection S..., and Virtual Machines. The data rows are:

Name	Description	Security Policies	Guest Introspection Ser...	Firewall Rules	Network Introspection S...	Virtual Machines
Activity Monito...		4	0	0	0	0
App-SG		1	0	0	2	2
DB-SG		1	0	0	2	1
LB-SG		1	0	0	2	0
Web-SG		1	0	0	2	2

The NSX Security Groups are synchronized with the FortiGate-VMX Service Manager creating dynamic objects in the FortiGate-VMX Service Manager to allow advanced granular security policy. As stated earlier, any change to the NSX Security Group will also alter the dynamic objects in the FortiGate-VMX Service Manager to reflect that change immediately.

Name	Type	Details
Address (34)		
Adobe Login	Wildcard FQDN	*adobelogin.com
App-SG	NSX Object	10.0.2.11 10.0.2.12
DB-SG	NSX Object	10.0.3.11
Gotomeeting	Wildcard FQDN	*gotomeeting.com
LB-SG	NSX Object	172.16.1.1 172.16.1.6
Web-SG	NSX Object	10.0.1.12 10.0.1.11
Windows update 2	Wildcard FQDN	*windowsupdate.com
adobe	Wildcard FQDN	*.adobe.com
all	Subnet	0.0.0.0/0

This is an example of a FortiGate-VMX Security Policy which utilizes the NSX Security Groups to secure a multi-tier application while doing Anti-virus scanning on incoming connections to the front-end web servers.

Seq.#	Name	From	To	Source	Destination	Schedule	Service	Action	Security Profiles	Log
1	Incoming Web Servers	external	internal	all	Web-SG	always	HTTP HTTPS	Accept	AV	UTM
2	Outgoing Web Servers	internal	external	Web-SG	App-SG LB-SG	always	HTTP HTTPS	Accept		UTM
3	Incoming App Servers	external	internal	LB-SG Web-SG	App-SG	always	HTTP HTTPS	Accept		UTM
4	Outgoing App Servers	internal	external	App-SG	DB-SG	always	MYSQL	Accept		UTM
5	Incoming DB	external	internal	App-SG	DB-SG	always	MYSQL	Accept		UTM
6	web to web out	internal	external	Web-SG	Web-SG	always	ALL_ICMP	Accept		UTM
7	web to web in	external	internal	Web-SG	Web-SG	always	ALL_ICMP	Accept		UTM

Creating and Navigating Virtual Domains (VDOMs)

Virtual Domain creation is recommended prior to registering the FortiGate-VMX security service with the NSX Manager (complementary NSX Service Profiles will also be created during the registration process). This section isn't meant to be a detailed study of VDOMs, the FortiOS Handbook does that. This is just to show the basic steps of creating a Virtual Domain (VDOM) in the FortiGate-VMX Service Manager and their navigation.

1. Login to FortiGate-VMX Service Manager
2. Navigate to **Global -> System -> VDOM**

FortiGate VMX-Service-Manager SVM2					
Global	+ Create New	Edit	Delete	Switch Management [root]	Search
Name	Operation Mode	Inspection Mode	Security Preset	Enable	
nsx	NAT	Proxy	Custom	✓	
nsx2	NAT	Flow-based	Custom	✓	
nsx3	NAT	Flow-based	Custom	✓	
root	NAT	Flow-based	Custom	✓	
test	NAT	Proxy	Custom	✓	

3. Click on + **Create New**

New Virtual Domain

Virtual Domain:

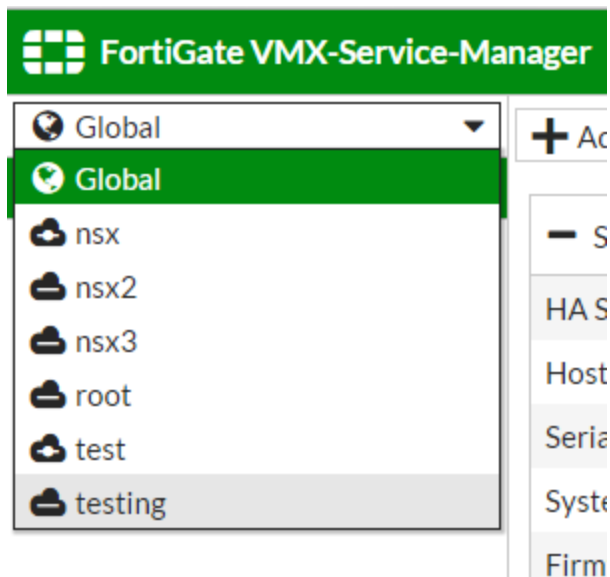
Inspection Mode:

Comments: 25/255

4. Enter values in the fields for **Virtual Domain**, **Inspection Mode** and optionally, **Comments**.

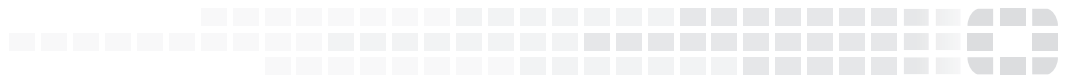
FortiGate VMX-Service-Manager SVM2								
+ Create New	Edit	Delete	Switch Management [root]	Search				
Name	Operation Mode	Inspection Mode	Security Preset	Enable	CPU	Memory	Interfaces	
nsx	NAT	Proxy	Custom	✓	0%	0%	external internal ssl.nsx (SSL VPN interface)	
nsx2	NAT	Flow-based	Custom	✓	0%	0%	nsx2-ext nsx2-int ssl.nsx2 (SSL VPN interface)	
nsx3	NAT	Flow-based	Custom	✓	0%	0%	nsx3-ext nsx3-int ssl.nsx3 (SSL VPN interface)	
root	NAT	Flow-based	Custom	✓	33%	35%	mgmt ssl.root (SSL VPN interface) sync	
test	NAT	Proxy	Custom	✓	0%	0%	ssl.test (SSL VPN interface) test-ext test-int	test
testing	NAT	Flow-based	Custom	✓	0%	0%	ssl.testing (SSL VPN interface) testing-ext testing-int	Cre...

To navigate between Global and various VDOMs, use the pull down arrow in the upper left to show all currently available VDOMs.





High Performance Network Security



Copyright© 2015 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.