



Cisco Firepower NGIPSv Quick Start Guide for VMware

Version 6.0

Published: November 10, 2015

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2015 Cisco Systems, Inc. All rights reserved.



Introduction to Cisco Firepower Virtual Appliances for VMware

Cisco packages 64-bit virtual Firepower Management Centers and virtual devices for the VMware vSphere and VMware vCloud Director hosting environments. You can deploy 64-bit Cisco Firepower Management Center Virtual and 64-bit Cisco Firepower NGIPSv managed devices to ESXi hosts using VMware vCenter or VMware vCloud Director. Virtual appliances use e1000 (1 Gbit/s) interfaces, or you can replace the default interfaces with vmxnet3 (10 Gbit/s) interfaces. You can also use VMware Tools to improve the performance and management of your virtual appliances.

Cisco Firepower Management Center Virtual can manage physical devices and Cisco ASA with FirePOWER Services (ASA FirePOWER), and physical Cisco Firepower Management Centers can manage virtual devices. However, virtual appliances do not support any of the system's hardware-based features—Cisco Firepower Management Center Virtual does not support high availability and virtual devices do not support clustering, stacking, switching, routing, and so on. For detailed information on physical Firepower System appliances, see the *Firepower 7000 and 8000 Series Installation Guide* and the *Firepower Management Center Installation Guide*.

This guide provides information about deploying, installing, and setting up virtual Firepower System appliances (Firepower NGIPSv devices and Firepower Management Center Virtual). It also assumes familiarity with the features and nomenclature of VMware products, including the vSphere Client, VMware vCloud Director web portal, and, optionally, VMware Tools.

Operating Environment Prerequisites

You can host 64-bit virtual appliances on the following hosting environments:

- VMware ESXi 5.5 (vSphere 5.5)
- VMware ESXi 5.1 (vSphere 5.1)
- VMware vCloud Director 5.1

You can also enable VMware Tools on all supported ESXi versions. For information on the full functionality of VMware Tools, see the VMware website (<http://www.vmware.com/>). For help creating a hosting environment, see the VMware ESXi documentation, including VMware vCloud Director and VMware vCenter.

Virtual appliances use Open Virtual Format (OVF) packaging. VMware Workstation, Player, Server, and Fusion do not recognize OVF packaging and are not supported. Additionally, virtual appliances are packaged as virtual machines with Version 7 of the virtual hardware.

The computer that serves as the ESXi host must meet the following requirements:

- It must have a 64-bit CPU that provides virtualization support, either Intel® Virtualization Technology (VT) or AMD Virtualization™ (AMD-V™) technology.
- Virtualization must be enabled in the BIOS settings
- To host virtual devices, the computer must have network interfaces compatible with Intel e1000 drivers (such as PRO 1000MT dual port server adapters or PRO 1000GT desktop adapters).

For more information, see the VMware website: <http://www.vmware.com/resources/guides.html>.

Each virtual appliance you create requires a certain amount of memory, CPUs, and hard disk space on the ESXi host. Do **not** decrease the default settings, as they are the minimum required to run the system software. However, to improve performance, you can increase a virtual appliance's memory and number of CPUs, depending on your available resources. The following table lists the default appliance settings.

Table 1 Default Virtual Appliance Settings

Setting	Default	Adjustable Setting?
memory	8GB	yes
virtual CPUs	4	yes, up to 8
hard disk provisioned size	40GB (NGIPSv) 250GB (Firepower Management Center Virtual)	no

Virtual Appliance Performance

It is not possible to accurately predict throughput and processing capacity for virtual appliances. A number of factors heavily influence performance, such as the:

- amount of memory and CPU capacity of the ESXi host
- number of total virtual machines running on the ESXi host
- number of sensing interfaces, network performance, and interface speed
- amount of resources assigned to each virtual appliance
- level of activity of other virtual appliances sharing the host
- complexity of policies applied to a virtual device

Note: VMware provides a number of performance measurement and resource allocation tools. Use these tools on the ESXi host while you run your virtual appliance to monitor traffic and determine throughput. If the throughput is not satisfactory, adjust the resources assigned to the virtual appliances that share the ESXi host.

You can enable VMware Tools to improve the performance and management of your virtual appliances. Alternatively, you can install tools (such as `esxtop` or VMware/third-party add-ons) on the host or in the virtualization management layer (not the guest layer) on the ESXi host to examine virtual performance. To enable VMware Tools, see the *Firepower Management Center Configuration Guide*.

Guidelines and Limitations

The following limitations exist when deploying Firepower NGIPSv for VMware:

- vMotion is not supported.
- Cloning a virtual machine is not supported.
- Restoring a virtual machine with snapshot is not supported.
- Restoring a backup is not supported.

Virtual Appliance Installation Packages for VMware

Cisco provides packaged virtual appliances for VMware ESXi host environments on its Support Site as compressed archive (.tar.gz) files. Cisco virtual appliances are packaged as virtual machines with Version 7 of the virtual hardware. Each archive contains the following files:

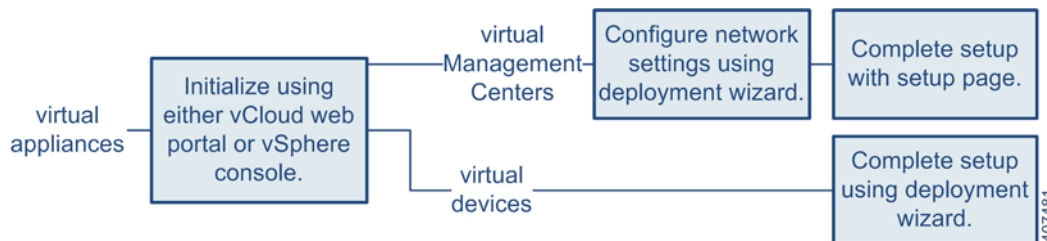
- an Open Virtual Format (.ovf) template containing -ESXi - in the file name
- an Open Virtual Format (.ovf) template containing -VI- in the file name
- a Manifest File (.mf) containing -ESXi - in the file name
- a Manifest File (.mf) containing -VI- in the file name
- the Virtual Machine Disk Format (.vmdk)

You deploy a virtual appliance with a virtual infrastructure (VI) or ESXi Open Virtual Format (OVF) template:

- When you deploy with a VI OVF template, you can configure Firepower System-required settings (such as the password for the admin account and settings that allow the appliance to communicate on your network) using the setup wizard in the deployment; you must deploy using a managing platform, either VMware vCloud Director or VMware vCenter.

VI OVF Template Deployment

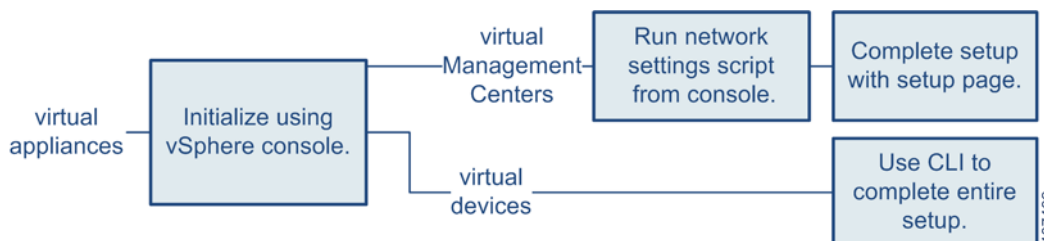
The following diagram shows the general process of setting up Firepower System virtual appliances when you deploy with a VI OVF template.



- When you deploy with an ESXi OVF template, you must configure settings after installation using the command line interface (CLI) on the VMware console of the virtual appliance; you can deploy using a managing platform (VMware vCloud Director or VMware vCenter), or you can deploy as a standalone appliance.

ESXi OVF Template Deployment

The following diagram shows the general process of setting up Firepower System virtual appliances when you deploy with a ESXi OVF template.



Obtaining the Installation Files

Before you install a Firepower System virtual appliance for VMware, obtain the correct archive file from the Support Site. Cisco recommends that you always use the most recent package available. Virtual appliance packages are usually associated with major versions of the system software (for example, 5.4 or 6.0).

To obtain virtual appliance archive files:

1. Using a web browser, navigate to the Downloads area of the Cisco Support Site (<https://software.cisco.com/download/navigator.html>).
2. Browse for software in the **Products** area, or enter a name in the **Find** field of the system software you want to install.
For example, to search for any Firepower archive files, enter **Firepower**.
3. Find the archive file that you want to download for the Firepower System virtual appliance using the following naming convention:

```
Cisco_Firepower_NGIPSv_VMware-X.X.X-xxx.tar.gz
Cisco_Firepower_Management_Center_Virtual_VMware-X.X.X-xxx.tar.gz
```

where *X.X.X-xxx* is the version and build number of the archive file you want to download.

4. Click the archive you want to download.

Note: While you are logged into the Support Site, Cisco recommends you download any available updates for virtual appliances so that after you install a virtual appliance to a major version, you can update its system software. You should always run the latest version of the system software supported by your appliance. For Cisco Firepower Management Center Virtual, you should also download any new intrusion rule and Vulnerability Database (VDB) updates.

5. Copy the archive file to a location accessible to the workstation or server that is running the vSphere Client or VMware vCloud Director web portal.

Caution: Do not transfer archive files via email; the files can become corrupted.

6. Decompress the archive file using your preferred tool and extract the installation files.

For the Cisco Firepower NGIPSv virtual device:

```
Cisco_Firepower_NGIPSv_VMware-X.X.X-xxx-disk1.vmdk
Cisco_Firepower_NGIPSv_VMware-ESXi-X.X.X-xxx.ovf
Cisco_Firepower_NGIPSv_VMware-ESXi-X.X.X-xxx.mf
Cisco_Firepower_NGIPSv_VMware-VI-X.X.X-xxx.ovf
Cisco_Firepower_NGIPSv_VMware-VI-X.X.X-xxx.mf
```

For the Cisco Firepower Management Center Virtual:

```
Cisco_Firepower_Management_Center_Virtual_VMware-X.X.X-xxx-disk1.vmdk
Cisco_Firepower_Management_Center_Virtual_VMware-ESXi-X.X.X-xxx.ovf
Cisco_Firepower_Management_Center_Virtual_VMware-ESXi-X.X.X-xxx.mf
Cisco_Firepower_Management_Center_Virtual_VMware-VI-X.X.X-xxx.ovf
Cisco_Firepower_Management_Center_Virtual_VMware-VI-X.X.X-xxx.mf
```

where *X.X.X-xxx* is the version and build number of the archive file you downloaded.

Note: Make sure you keep all the files in the same directory.

What to Do Next

- Cisco Firepower NGIPSv — continue with [Cisco Firepower NGIPSv for VMware Deployment, page 7](#) to deploy the virtual Firepower System managed device.
- Cisco Firepower Management Center Virtual — see the *Cisco Firepower Management Center Virtual Quick Start Guide for VMware* for information on how to deploy the virtual Firepower Management Center.



Cisco Firepower NGIPSv for VMware Deployment

To install a Cisco Firepower NGIPSv virtual device, you deploy an OVF (VI or ESXi) template to a managing platform (VMware vCloud Director or VMware vCenter) using a platform interface (VMware vCloud Director web portal or vSphere Client):

- If you deploy using a VI OVF template, you can configure Firepower System-required settings during installation. You must manage this virtual appliance using either VMware vCloud Director or VMware vCenter.
- If you deploy using an ESXi OVF template, you must configure Firepower System-required settings after installation. You can manage this virtual appliance using either VMware vCloud Director or VMware vCenter, or use it as a standalone appliance.

After you make sure your planned deployment meets the prerequisites (described in [Operating Environment Prerequisites, page 3](#)) and download the necessary archive files, use the VMware vCloud Director web portal or vSphere Client to install virtual appliances

You have the following installation options for installing a Cisco Firepower NGIPSv virtual device:

```
Cisco_Firepower_NGIPSv_VMware-VI-X.X.X-xxx.ovf  
Cisco_Firepower_NGIPSv_VMware-ESXi-X.X.X-xxx.ovf
```

where *x.x.x-xxx* is the version and build number of the file you want to use.

When you deploy an OVF template you provide the following information:

Table 1 VMware OVF Template

Setting	ESXi or VI	Action
Import/Deploy OVF Template	Both	Browse to the OVF templates you downloaded in the previous procedure to use.
OVF Template Details	Both	Confirm the appliance you are installing (Cisco Firepower NGIPSv) and the deployment option (VI or ESXi).
Accept EULA	VI only	Agree to accept the terms of the licenses included in the OVF template.
Name and Location	Both	Enter a unique, meaningful name for your virtual appliance and select the inventory location for your appliance.
Host / Cluster	Both	Select the host or cluster where you want to deploy the virtual appliance.
Resource Pool	Both	Manage your computing resources within a host or cluster by setting them up in a meaningful hierarchy. Virtual machines and child resource pools share the resources of the parent resource pool.
Storage	Both	Select a datastore to store all files associated with the virtual machine.
Disk Format	Both	Select the format to store the virtual disks: thick provision lazy zeroed, thick provision eager zeroed, or thin provision.
Network Mapping	Both	Select the management interface for the virtual appliance.
Properties	VI only	Customize the Virtual Machine initial configuration setup.

If you deploy with a VI OVF template, the installation process allows you to perform the entire initial setup for Cisco Firepower NGIPSv virtual devices. You can specify:

Deploy Using VMware vCloud Director

- A new password for the admin account
- Network settings that allow the appliance to communicate on your management network
- The initial detection mode
- The managing Cisco Firepower Management Center

If you deploy with an ESXi OVF template or if you choose not to configure with the setup wizard, you must perform the initial setup for virtual appliances using the VMware console; see [Cisco Firepower Virtual for VMware Setup, page 15](#) for information on performing the initial setup, including guidance on what configurations to specify.

Use one of the following options to install your virtual appliance:

- [Deploy Using VMware vCloud Director, page 8](#) describes how to deploy a Cisco Firepower NGIPSv virtual device to the VMware vCloud Director.
- [Deploy Using VMware vSphere, page 9](#) describes how to deploy a Cisco Firepower NGIPSv virtual device to the VMware vCenter.

Deploy Using VMware vCloud Director

You can use the VMware vCloud Director web portal to deploy a Cisco Firepower NGIPSv virtual device using a vApp template. To use VMware vCloud Director for deployment, you create an organization and catalog, upload an OVF package obtained from Cisco.com, and create the Cisco Firepower NGIPSv using the vApp template.


Uploading the Virtual Appliance OVF Package

You can upload OVF packages for the Cisco Firepower NGIPSv virtual device to your VMware vCloud Director organization catalog.

Before You Begin

- Create an organization and catalog to contain the vApp templates; see the *VMware vCloud Director User's Guide* for more information.
- Download an OVF template from Cisco.com; see [Obtaining the Installation Files, page 6](#).

Procedure

1. On the VMware vCloud Director web portal, select **Catalogs > Organization > vApp Templates** where *Organization* is the name of the organization that you want to contain your vApp templates.
2. On the vApp Templates media tab, click the Upload icon (.
3. In the OVF package field, enter the location of the OVF package, or click **Browse** to browse to the OVF package for the Cisco Firepower NGIPSv virtual device:
`Cisco_Firepower_NGIPSv_VMware-VI-X.X.X-xxx.ovf`
where *X.X.X-xxx* is the version and build number of the OVF package you want to upload.
4. Enter a name and optionally a description for the OVF package.
5. From the drop-down lists, select the virtual datacenter, storage profile, and catalog to contain the vApp template.
6. Click **Upload**.


What to Do Next

- Create the virtual device from the vApp template; see [Using the vApp Template, page 9](#).

Using the vApp Template

You can use a vApp template to create a Cisco Firepower NGIPSv virtual device that allows you to configure Firepower System-required settings during the installation using a setup wizard.

Procedure

1. On the VMware vCloud Director web portal, select **My Cloud > vApps**.
2. On the vApps media tab, click the Add icon () to add a vApp from the catalog.
3. Click **All Templates** on the template menu bar.
4. Select the vApp template you want to add to display a description of the Cisco Firepower NGIPSv virtual device:
`Cisco_Firepower_NGIPSv_VMware-VI-X.X.X-xxx.ovf`
where `X.X.X-xxx` is the version and build number of the archive file.
5. Read and accept the EULA.
6. Enter a name and optionally a description for the vApp.
7. On the Configure Resources screen, select the virtual datacenter, enter a system name (or use the default system name), and select the storage profile.
8. Map the networks used in the OVF template to a network in your inventory by selecting the destination for the external, management, and internal sources, and your IP allocation.
9. Optionally, on the Custom Properties screen, perform the initial setup for the appliance by entering the Firepower System-required settings on the setup wizard. If you do not perform the initial setup now, you can do it later using the instructions in [Cisco Firepower Virtual for VMware Setup, page 15](#).
10. Confirm your settings and click **Finish**.

Note: Do **not** enable the **Power on after deployment** option for a virtual device. You must map your sensing interfaces and be sure they are set to connect before powering on the appliance. For more information, see [Initializing a Virtual Appliance, page 15](#).

What to Do Next

- Determine if you need to modify the virtual appliance's hardware and memory settings, or configure interfaces; see [Post-Installation Configuration, page 11](#).

Deploy Using VMware vSphere

You can use the VMware vSphere vCenter, vSphere Client, vSphere Web Client, or vSphere Hypervisor (for standalone ESXi deployment) to deploy a Cisco Firepower NGIPSv virtual device. You can use vSphere to deploy with either a VI OVF or ESXi OVF template:

- If you deploy using a VI OVF template, the appliance must be managed by VMware vCenter or VMware vCloud Director.
- If you deploy using a ESXi OVF template, the appliance can be managed by VMware vCenter, VMware vCloud Director, or deployed to a standalone host. In either case, you must configure Firepower System-required settings after installation.

Before You Begin

- Download an OVF template from Cisco.com; see [Obtaining the Installation Files, page 6](#).

Procedure

1. Using the vSphere Client, deploy the OVF template file you downloaded earlier by clicking **File > Deploy OVF Template**.
2. From the drop-down list, select one of the OVF templates you want to deploy for the Cisco Firepower NGIPSv virtual device:

```
Cisco_Firepower_NGIPSv_VMware-VI-X.X.X-xxx.ovf  
Cisco_Firepower_NGIPSv_VMware-ESXi-X.X.X-xxx.ovf
```

where *X.X.X-xxx* is the version and build number of the archive file you downloaded.

3. View the OVF Template Details page and click **Next**.
4. If license agreements are packaged with the OVF template (VI templates only), the End User License Agreement page appears. Agree to accept the terms of the licenses and click **Next**.
5. Optionally, edit the name and select the folder location within the inventory where the Cisco Firepower NGIPSv will reside, and click **Next**.

Note: When the vSphere Client is connected directly to an ESXi host, the option to select the folder location does not appear.

6. Select the host or cluster on which you want to deploy the Cisco Firepower NGIPSv and click **Next**.
7. Navigate to, and select the resource pool where you want to run the Cisco Firepower NGIPSv and click **Next**.

Note: This page appears only if the cluster contains a resource pool.

8. Select a storage location to store the virtual machine files, and click **Next**.

On this page, you select from datastores already configured on the destination cluster or host. The virtual machine configuration file and virtual disk files are stored on the datastore. Select a datastore large enough to accommodate the virtual machine and all of its virtual disk files.

9. Select the disk format to store the virtual machine virtual disks, and click **Next**.

When you select **Thick Provisioned**, all storage is immediately allocated. When you select **Thin Provisioned**, storage is allocated on demand as data is written to the virtual disks.

10. Associate the NGIPSv management interface and the two sensing interfaces (internal and external) with a VMware network on the Network Mapping screen.

For each network specified in the OVF template, select a network by right-clicking the **Destination Networks** column in your infrastructure to set up the network mapping for each Cisco Firepower NGIPSv interface and click **Next**.

Ensure the Management interface is associated to a VM Network that is reachable from the Firepower Management Center. Non-management interfaces are configurable from the Firepower Management Center.

11. If user-configurable properties are packaged with the OVF template (VI templates only), including **Detection Mode** and **Registration** information for the managing Firepower Management Center, set the configurable properties and click **Next**.
12. Review and verify the settings on the **Ready to Complete** window.
13. Confirm your settings, then click **Finish**.

Note: Do **not** enable the **Power on after deployment** option for a virtual appliance. You must map your sensing interfaces and be sure they are set to connect before powering on the appliance. For more information, see [Initializing a Virtual Appliance, page 15](#).

14. After the installation is complete, close the status window.
15. After you complete the wizard, the vSphere Web Client processes the VM; you can see the “Initialize OVF deployment” status in the **Global Information** area **Recent Tasks** pane.

When it is finished, you see the Deploy OVF Template completion status.

The Cisco Firepower NGIPSv VM instance then appears under the specified data center in the Inventory. Booting up the new VM could take up to 30 minutes.

Note: To successfully register the Cisco Firepower NGIPSv with the Cisco Licensing Authority, the Cisco Firepower NGIPSv requires Internet access. You might need to perform additional configuration after deployment to achieve Internet access and successful license registration.

What to Do Next

- Determine if you need to modify the virtual appliance's hardware and memory settings, or configure interfaces; see [Post-Installation Configuration, page 11](#).

Post-Installation Configuration

After you deploy a virtual appliance, confirm that the virtual appliance's hardware and memory settings meet the requirements for your deployment. Do **not** decrease the default settings, as they are the minimum required to run the system software. However, to improve performance, you can increase a virtual appliance's memory and number of CPUs, depending on your available resources. The following table lists the default appliance settings.

Figure 1 Default Virtual Appliance Settings

Setting	Default	Adjustable Setting?
memory	8GB	yes
virtual CPUs	4	yes, up to 8
hard disk provisioned size	40GB (NGIPSv)	no

Verifying Virtual Machine Properties

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	Any	Any	Admin

Use the VMware Virtual Machine Properties dialog box to adjust the host resource allocation for the selected virtual machine. You can change CPU, memory, disk, and advanced CPU resources from this tab. You can also change the power-on connection setting, the MAC address, and the network connection for the virtual Ethernet adapter configuration for a virtual machine.

Procedure

1. Right-click the name of your new virtual appliance, then select **Edit Settings** from the context menu, or click **Edit virtual machine settings** from the **Getting Started** tab in the main window.
2. Make sure the **Memory**, **CPUs**, and **Hard disk 1** settings are set no lower than the defaults, as described in [Default Virtual Appliance Settings, page 11](#).

The memory setting and the number of virtual CPUs for the appliance are listed on the left side of the window. To see the hard disk **Provisioned Size**, click **Hard disk 1**.

3. Optionally, increase the memory and number of virtual CPUs by clicking the appropriate setting on the left side of the window, then making changes on the right side of the window.
4. Confirm the **Network adapter 1** settings are as follows, making changes if necessary:
 - a. Under **Device Status**, enable the **Connect at power on** check box.
 - b. Under **MAC Address**, manually set the MAC address for your virtual appliance's management interface.

Manually assign the MAC address to your virtual appliance to avoid MAC address changes or conflicts from other systems in the dynamic pool.

Additionally, for virtual Cisco Firepower Management Centers, setting the MAC address manually ensures that you will not have to re-request licenses from Cisco if you ever have to reimage the appliance.

- c. Under **Network Connection**, set the **Network label** to the name of the management network for your virtual appliance.

5. Click **OK**.

What to Do Next

- Initialize the virtual appliance; see [Initializing a Virtual Appliance, page 15](#).
- Optionally, before you power on the appliance, you can replace the default e1000 interfaces with vmxnet3 interfaces, create an additional management interface, or both; see [Adding and Configuring Interfaces, page 12](#).

Adding and Configuring Interfaces

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	NGIPSv	Any	Admin

You can replace the default e1000 (1 Gbit/s) interfaces with vmxnet3 (10 Gbit/s) interfaces by deleting all of the e1000 interfaces and replacing them with vmxnet3 interfaces.

Although you can mix interfaces in your deployment (such as, e1000 interfaces on a virtual Cisco Firepower Management Center and vmxnet3 interfaces on its managed virtual device), you cannot mix interfaces on the same appliance. **All sensing and management interfaces on the appliance must be the same, either e1000 or vmxnet3.**

To replace e1000 interfaces with vmxnet3 interfaces, use the vSphere Client to first remove the existing e1000 interfaces, add the new vmxnet3 interfaces, and then select the appropriate adapter type and network connection.

You can also add a second management interface on the same virtual Firepower Management Center to manage traffic separately on two different networks. Configure an additional virtual switch to connect the second management interface to a managed device on the second network. Use the vSphere Client to add a second management interface to your virtual appliance.

For more information about using the vSphere Client, see the VMware website (<http://vmware.com>). For more information about multiple management interfaces, see *Managing Devices in the Firepower Management Center Configuration Guide*.

Note: Make all changes to your interfaces before you turn on your appliance. To change the interfaces, you must un-register from the Firepower Management Center, power down the appliance, delete the interfaces, add the new interfaces, power on the appliance, and then re-register to the Firepower Management Center.

Configuring Virtual Device Sensing Interfaces

The sensing interfaces on a Cisco Firepower NGIPSv virtual device must have a network connection to a port on an ESXi host virtual switch that accepts promiscuous mode.

Note: Add a port group to a virtual switch to isolate promiscuous mode virtual network connections from your production traffic. For information on adding port groups and setting security attributes, see your VMware documentation.

Procedure

1. Use the vSphere Client to log into your server and click on your server's **Configuration** tab.

The **Hardware** and **Software** selection lists appear.

2. In the **Hardware** list, click **Networking**.

3. On the switch and port group where you connect the sensing interfaces of the virtual device, click **Properties**.
4. On the **Switch Properties** pop-up window, click **Edit**.
5. On the **Detailed Properties** pop-up window, select the **Security** tab.

Under **Policy Exceptions > Promiscuous Mode**, confirm that the Promiscuous Mode is set to **Accept**.

Note: To monitor VLAN traffic in your virtual environment, set the VLAN ID of the promiscuous port to 4095.

6. Save your changes.

The virtual appliance is ready to initialize.

What to Do Next

- Initialize the virtual appliance; see [Initializing a Virtual Appliance, page 15](#).



Cisco Firepower Virtual for VMware Setup

After you install a Cisco Firepower System virtual appliance, you must complete a setup process that allows the new appliance to communicate on your trusted management network. You must also change the administrator password and accept the end user license agreement (EULA).

The setup process also allows you to perform many initial administrative-level tasks, such as setting the time, registering and licensing devices, and scheduling updates. The options you choose during setup and registration determine the default interfaces, inline sets, zones, and policies that the system creates and applies.

The purpose of these initial configurations and policies is to provide an out-of-the-box experience and to help you quickly set up your deployment, not to restrict your options. Regardless of how you initially configure a virtual appliance, you can change its configuration at any time using the Cisco Firepower Management Center. In other words, choosing a detection mode or access control policy during setup, for example, does not lock you into a specific device, zone, or policy configuration.

Regardless of how you deploy, begin by powering on the appliance to initialize it. After initialization completes, log in using the VMware console and complete the setup in one of the following ways, depending on the appliance type:

Cisco Firepower NGIPSv

Cisco Firepower NGIPSv virtual appliances do not have a web interface. If you deploy with the VI OVF template, you can perform the initial setup, including registering the appliance to a Firepower Management Center, using the deployment wizard. If you deploy with the ESXi OVF template, you must use the interactive command line interface (CLI) to perform the initial setup.

Cisco Firepower Management Center Virtual

If you deploy with the VI OVF template, you can perform the network configuration using the wizard in the deployment. If you choose not to use the setup wizard or you deploy with the ESXi OVF template, configure network settings using a script. After your network is configured, complete the setup process using a computer on your management network to browse to the Cisco Firepower Management Center's web interface.

Note: If you are deploying multiple appliances, set up your Firepower NGIPSv appliances first, then their managing Firepower Management Center. The initial setup process for a device allows you to preregister it to a Firepower Management Center; the setup process for a Firepower Management Center allows you to add and license preregistered managed devices.

Initializing a Virtual Appliance

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	Any	Any	Admin

After you install a virtual appliance, initialization starts automatically when you power on the virtual appliance for the first time.

Caution: Startup time depends on a number of factors, including server resource availability. It can take up to 40 minutes for the initialization to complete. Do not interrupt the initialization or you may have to delete the appliance and begin again.

Use the following procedure to initialize a virtual appliance.

Procedure

1. Power on the appliance:
 - In the VMware vCloud Director web portal, select the **vApp** from the display, then click **Start**.
 - In the vSphere Client, right-click the name of your imported virtual appliance from the inventory list, then select **Power > Power On** from the context menu.
2. Monitor the initialization on the VMware console tab.

What to Do Next

If you used a VI OVF template and configured your Firepower System-required settings during deployment, no further configuration is required.

If you used an ESXi OVF template or you did not configure Firepower System-required settings when you deployed with the VI OVF template, continue with [Setting Up a Firepower NGIPSv Device Using the CLI, page 16](#).

Setting Up a Firepower NGIPSv Device Using the CLI

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	NGIPSv	Any	Admin

Because Firepower NGIPSv devices do not have web interfaces, you must set up a virtual device using the CLI if you deployed with an ESXi OVF template. You can also use the CLI to configure Firepower System-required settings if you deployed with a VI OVF template and did not use the setup wizard during deployment.

Note: If you deployed with a VI OVF template and used the setup wizard, your virtual device is configured and no further action is required.

When you first log into a newly configured device, you must read and accept the EULA. Then, follow the setup prompts to change the administrator password, and configure the device's network settings and detection mode.

When following the setup prompts, for multiple-choice questions, your options are listed in parentheses, such as (y/n). Defaults are listed in square brackets, such as [y]. Press Enter to confirm a choice.

Note that the CLI prompts you for much of the same setup information that a physical device's setup web page does. For more information, see the *Firepower 7000 and 8000 Series Installation Guide*.

Note: To change any of these settings for a virtual device after you complete the initial setup, you must use the CLI. For more information, see the Command Line Reference chapter in the *Firepower Management Center Configuration Guide*.

Understanding Device Network Settings

The Firepower System provides a dual stack implementation for both IPv4 and IPv6 management environments. You must set the IPv4 or IPv6 management IP address, netmask or prefix length, and default gateway. You can also specify up to three DNS servers, as well as the host name and domain for the device. Note that the host name is not reflected in the syslog until after you reboot the device.

Understanding Detection Modes

The detection mode you choose for a virtual device determines how the system initially configures the device's interfaces, and whether those interfaces belong to an inline set or security zone. The detection mode is not a setting you can change later; it is simply an option you choose during setup that helps the system tailor the device's initial configurations. In general, you should choose a detection mode based on how your device is deployed.

Passive

Choose this mode if your device is deployed passively, as an intrusion detection system (IDS). In a passive deployment, virtual devices can perform network-based file and malware detection, and Security Intelligence monitoring, as well as network discovery.

Inline

Choose this mode if your device is deployed inline, as an intrusion prevention system (IPS).

Note: Although general practice in IPS deployments is to fail open and allow non-matching traffic, inline sets on virtual devices lack bypass capability.

Access Control

Choose this mode if your device is deployed inline as part of an access control deployment, that is, if you want to perform application, user, and URL control. A device configured to perform access control usually fails closed and blocks non-matching traffic. Rules explicitly specify the traffic to pass.

In an access control deployment, you can also perform advanced malware protection, file control, Security Intelligence filtering, and network discovery.

Network Discovery

Choose this mode if your device is deployed passively, to perform host, application, and user discovery only.

The following table lists the interfaces, inline sets, and zones that the system creates depending on the detection mode you choose.

Table 1 Initial Configurations Based on Detection Mode

Detection Mode	Security Zones	Inline Sets	Interfaces
Inline	Internal and External	Default Inline Set	first pair added to Default Inline Set—one to the Internal and one to the External zone
Passive	Passive	none	first pair assigned to Passive zone
Access Control	none	none	none
Network Discovery	Passive	none	first pair assigned to Passive zone

Note that security zones are a Firepower Management Center-level configuration which the system does not create until you actually add the device to the Firepower Management Center. At that time, if the appropriate zone (Internal, External, or Passive) already exists on the Firepower Management Center, the system adds the listed interfaces to the existing zone. If the zone does not exist, the system creates it and adds the interfaces. For detailed information on interfaces, inline sets, and security zones, see the *Firepower Management Center Configuration Guide*.

Procedure

1. Open the VMware console.
2. Log into the virtual device at the VMware console using `admin` as the username and the new admin account password that you specified in the deployment setup wizard.

If you did not change the password using the wizard or you are deploying with a ESXi OVF template, use `Admin123` as the password.

The device immediately prompts you to read the EULA.

3. Read and accept the EULA.
4. Change the password for the `admin` account. This account has the Configuration CLI access level, and cannot be deleted.

Note: Cisco recommends that you use a strong password that is at least eight alphanumeric characters of mixed case and includes at least one numeric character. Avoid using words that appear in a dictionary.

- Configure network settings for the device. First configure (or disable) IPv4 management settings, then IPv6. If you manually specify network settings, you must:

- Enter IPv4 addresses, including the netmask, in dotted decimal form. For example, you could specify a netmask of 255.255.0.0.
- Enter IPv6 addresses in colon-separated hexadecimal form. For an IPv6 prefix, specify the number of bits; for example, a prefix length of 112.

The VMware console may display messages as your settings are implemented.

- Specify the detection mode based on how you deployed the device.

The VMware console may display messages as your settings are implemented. When finished, the device reminds you to register this device to a Cisco Firepower Management Center, and displays the CLI prompt.

What to Do Next

- Continue with the next section, [Registering a Virtual Device to a Cisco Firepower Management Center, page 18](#) to use the CLI to register the device to the Cisco Firepower Management Center that will manage it. You must manage devices with a Cisco Firepower Management Center. If you do not register the device now, you must log in later and register it before you can add it to a Cisco Firepower Management Center.

Registering a Virtual Device to a Cisco Firepower Management Center

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	NGIPSv	Any	Admin CLI Configuration

Because virtual devices do not have web interfaces, you must use the CLI to register a virtual device to a Cisco Firepower Management Center, which can be physical or virtual. It is easiest to register a device to its Firepower Management Center during the initial setup process, because you are already logged into the device's CLI.

To register a device, use the `configure manager add` command. A unique self-generated alphanumeric registration key is always required to register a device to a Firepower Management Center. This is a simple key that you specify, and it is not the same as a license key.

In most cases, you must provide the Firepower Management Center's IP address along with the registration key, for example:

```
configure manager add XXX.XXX.XXX.XXX my_reg_key
```

where `XXX.XXX.XXX.XXX` is the IP address of the managing Firepower Management Center and `my_reg_key` is the registration key you entered for the virtual device.

Note: When using the vSphere Client to register a virtual device to a Firepower Management Center, you must use the IP address (not the hostname) of the managing Firepower Management Center.

However, if the device and the Firepower Management Center are separated by a Network Address Translation (NAT) device, enter a unique NAT ID along with the registration key, and specify `DONTRESOLVE` instead of the IP address, for example:

```
configure manager add DONTRESOLVE my_reg_key my_nat_id
```

where `my_reg_key` is the registration key you entered for the virtual device and `my_nat_id` is the NAT ID of the NAT device.

If the device, rather than the Firepower Management Center, is behind a NAT device, enter a unique NAT ID along with the registration key, and specify the host name or IP address of the Firepower Management Center. For example:

```
configure manager add [hostname | ip address] my_reg_key my_nat_id
```

where `my_reg_key` is the registration key you entered for the virtual device and `my_nat_id` is the NAT ID of the NAT device.

Procedure

1. Log into the virtual device as a user with CLI Configuration (Administrator) privileges:
 - If you are performing the initial setup from the VMware console, you are already logged in as the `admin` user, which has the required access level.
 - Otherwise, log into the device using the VMware console, or, if you have already configured network settings for the device, SSH to the device's management IP address or host name.
2. At the prompt, register the device to a Cisco Firepower Management Center using the `configure manager add` command, which has the following syntax:

```
configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE} reg_key
[nat_id]
```

where:

- `{hostname | IPv4_address | IPv6_address | DONTRESOLVE}` specifies the IP address of the Firepower Management Center. If the Firepower Management Center is not directly addressable, use `DONTRESOLVE`.
- `reg_key` is the unique alphanumeric registration key required to register a device to the Firepower Management Center.
- `nat_id` is an optional alphanumeric string used during the registration process between the Cisco Firepower Management Center and the device. It is required if the hostname is set to `DONTRESOLVE`.

3. Log out of the appliance.

What to Do Next

- Log into its web interface and use the Device Management (**Devices > Device Management**) page to add the device if you have already set up the Firepower Management Center. For more information, see the Managing Devices chapter in the *Firepower Management Center Configuration Guide*.
- See the *Cisco Firepower Management Center Virtual Quick Start Guide for VMware* for a virtual Firepower Management Center, or see the *Cisco Firepower Management Center Installation Guide* for a physical Firepower Management Center if you have not already set up the Firepower Management Center.

Enabling VMware Tools

VMware Tools is a suite of utilities installed in the operating system of a virtual machine to enhance the performance of the virtual machine and to make possible many of the ease-of-use features of VMware products. The system supports the following plugins on all virtual appliances:

- `guestInfo`
- `powerOps`
- `timeSync`
- `vmbackup`

For more information on the supported plugins and full functionality of VMware Tools, see the VMware website (<http://www.vmware.com/>).

After you setup your virtual appliance, you can enable VMware Tools on your virtual appliances on your managed device using the command line interface (CLI).

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	NGIPSv	Any	Admin

You can log into the virtual device and enter one or more of the following commands:

- `show vmware-tools` displays whether VMware Tools are running on the system.
- `configure vmware-tools enable` enables VMware Tools on the virtual device.
- `configure vmware-tools disable` disables VMware Tools on the virtual device.

To enable VMware Tools on a virtual device:

1. At the console, log into the virtual device and, at the CLI prompt, enter the appropriate command to enable or disable VMware Tools, or display whether VMware Tools is enabled, and press **Enter**.

Next Steps

After you complete the initial setup process for a virtual appliance and verify its success, Cisco recommends that you complete various administrative tasks that make your deployment easier to manage. You should also complete any tasks you skipped during the initial setup, such as device registration and licensing. For detailed information on any of the tasks described in the following sections, as well as information on how you can begin to configure your deployment, see the *Firepower Management Center Configuration Guide*.

Individual User Accounts

After you complete the initial setup, the only user on the system is the `admin` user, which has the Administrator role and access. Users with that role have full menu and configuration access to the system, including via the shell or CLI. Cisco recommends that you limit the use of the `admin` account (and the Administrator role) for security and auditing reasons.

Creating a separate account for each person who will use the system allows your organization not only to audit actions and changes made by each user, but also to limit each person's associated user access role or roles. This is especially important on the Cisco Firepower Management Center, where you perform most of your configuration and analysis tasks. For example, an analyst needs access to event data to analyze the security of your network, but may not require access to administrative functions for the deployment.

The system includes ten predefined user roles designed for a variety of administrators and analysts. You can also create custom user roles with specialized access privileges.

Health and System Policies

By default, all appliances have an initial system policy applied. The system policy governs settings that are likely to be similar for multiple appliances in a deployment, such as mail relay host preferences and time synchronization settings. Cisco recommends that you use the Firepower Management Center to apply the same system policy to itself and all the devices it manages.

By default, the Firepower Management Center also has a health policy applied. A health policy, as part of the health monitoring feature, provides the criteria for the system continuously monitoring the performance of the appliances in your deployment. Cisco recommends that you use the Firepower Management Center to apply a health policy to all the devices it manages.

Software and Database Updates

You should update the system software on your appliances before you begin any deployment. Cisco recommends that all the appliances in your deployment run the most recent version of the Firepower System. If you are using them in your deployment, you should also install the latest intrusion rule updates, VDB, and GeoDB.

Caution: Before you update any part of the Firepower System, you must read the release notes or advisory text that accompanies the update. The release notes provide important information, including supported platforms, compatibility, prerequisites, warnings, and specific installation and uninstallation instructions.

Next Steps



Cisco Firepower Virtual Appliances for VMware Deployment Examples

Using virtual devices and virtual Cisco Firepower Management Centers allows you to deploy security solutions within your virtual environment for increased protection of both physical and virtual assets. Virtual devices and virtual Cisco Firepower Management Centers enable you to easily implement security solutions on the VMware platform. Virtual devices also make it easier to deploy and manage devices at remote sites where resources may be limited.

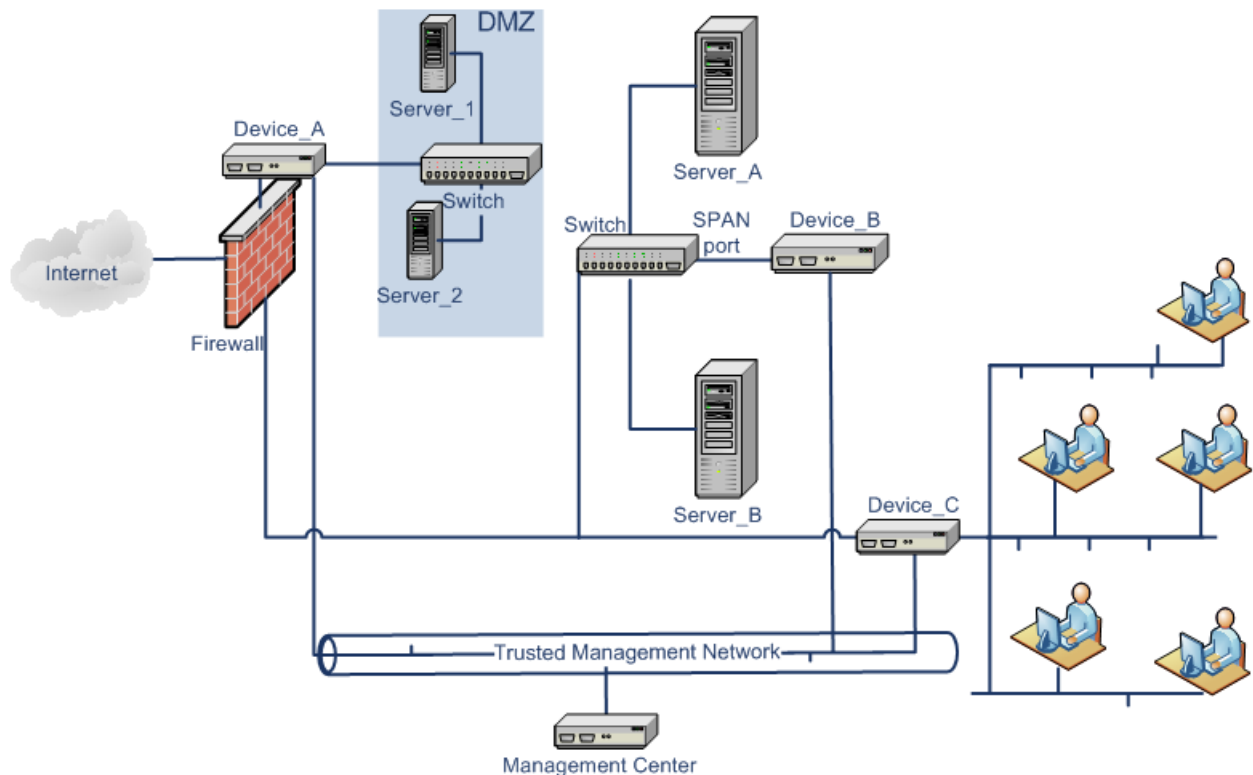
In these examples, you can use a physical or virtual Cisco Firepower Management Center to manage your physical or virtual devices. You can deploy on a IPv4 or IPv6 network. You can also configure multiple management interfaces on the Cisco Firepower Management Center to isolate and monitor two different networks, or to separate internal and event traffic on a single network. Note that virtual devices do not support multiple management interfaces.

You can configure a second management interface on your virtual Cisco Firepower Management Center to improve performance or to manage traffic separately on two different networks. Configure an additional interface and an additional virtual switch to connect the second management interface to a managed device on the second network. To add a second management interface to your virtual appliance, see VMware vSphere (<http://vmware.com>). For more information about multiple management interfaces, see Managing Devices in the *Firepower Management Center Configuration Guide*.

Caution: Cisco strongly recommends that you keep your production network traffic and your trusted management network traffic on different network segments. You must take precautions to ensure the security of the appliances and the management traffic data stream.

Typical Firepower System Deployment

In a physical appliance environment, a typical Firepower System deployment uses physical devices and a physical Cisco Firepower Management Center. The following graphic displays a sample deployment. You can deploy Device_A and Device_C in an inline configuration and Device_B in a passive configuration, as shown below.



You can configure port mirroring on most network switches to send a copy of network packets seen on one switch port (or an entire VLAN) to a network monitoring connection. Also called Switch Port Analyzer or SPAN by a major network equipment provider, port mirroring allows you to monitor network traffic. Note that Device_B monitors the traffic between Server_A and Server_B via a SPAN port on the switch between Server_A and Server_B.

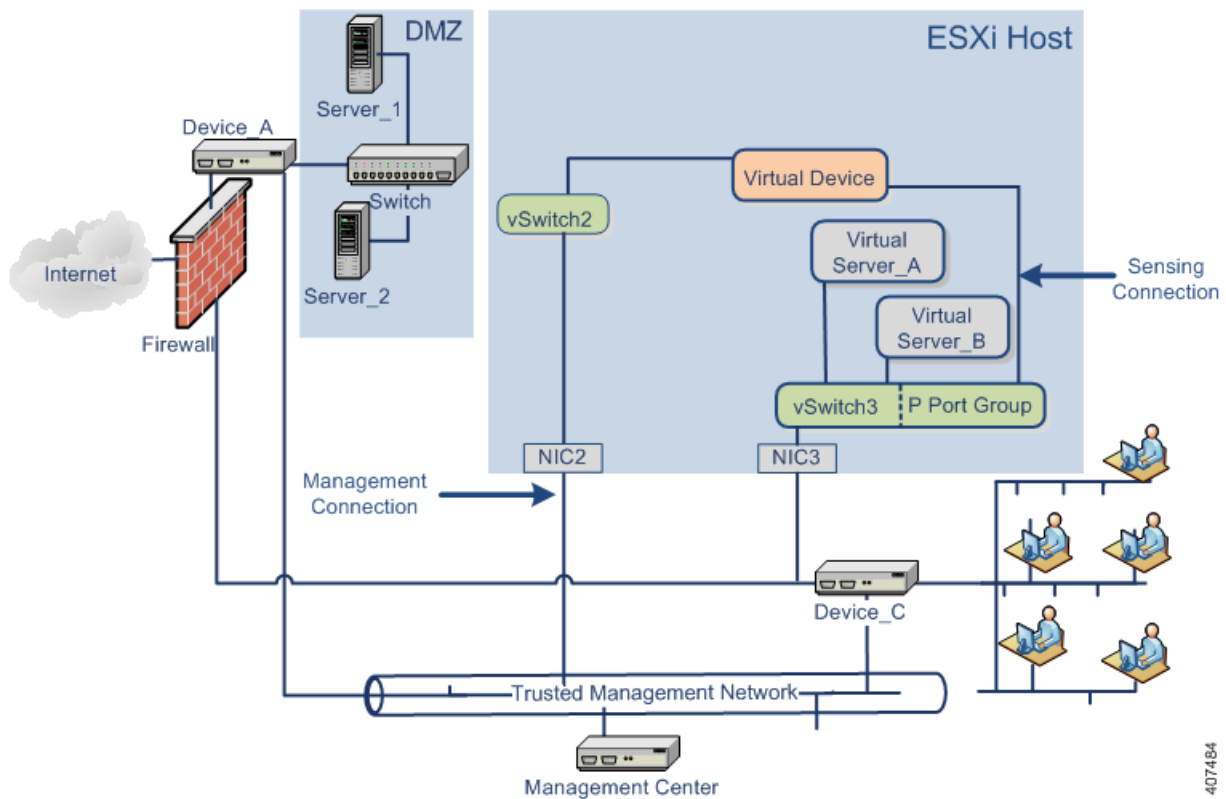
Virtual Firepower Appliance Deployments on VMware

Adding Virtualization and a Virtual Device

You can replace the physical internal servers in our [Typical Firepower System Deployment, page 23](#) by using virtual infrastructure. In the following example, you can use an ESXi host and virtualize Server_A and Server_B.

You can use a virtual device to monitor the traffic between Server_A and Server_B.

The virtual device sensing interface must connect to a switch or port group that accepts promiscuous mode traffic, as shown below.



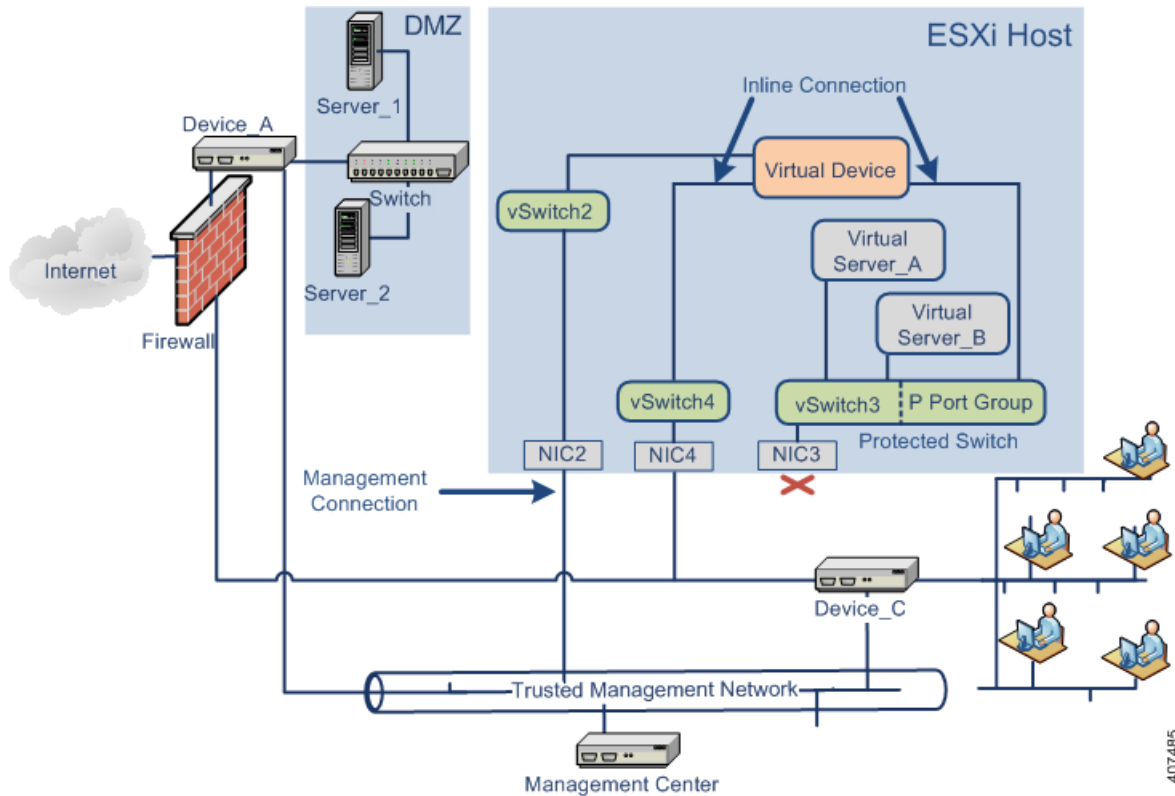
Note: To sense all traffic, allow promiscuous mode traffic on the virtual switches or port groups where the device sensing interfaces connect. See [Configuring Virtual Device Sensing Interfaces](#), page 12.

Although our example shows only one sensing interface, two sensing interfaces are available by default on your virtual device. The virtual device management interface connects to your trusted management network and your Cisco Firepower Management Center.

Using the Virtual Device for Inline Detection

You can provide a secure perimeter around virtual servers by passing traffic through your virtual device's inline interface set. This scenario builds on the [Typical Firepower System Deployment](#), page 23 and on the example shown in [Adding Virtualization and a Virtual Device](#), page 24.

First, create a protected virtual switch and connect it to your virtual servers. Then, connect the protected switch through your virtual device to the external network. For more information, see the *Firepower Management Center Configuration Guide*.



Note: To sense all traffic, allow promiscuous mode traffic on the virtual switches or port groups where the device sensing interfaces connect. See [Configuring Virtual Device Sensing Interfaces](#), page 12.

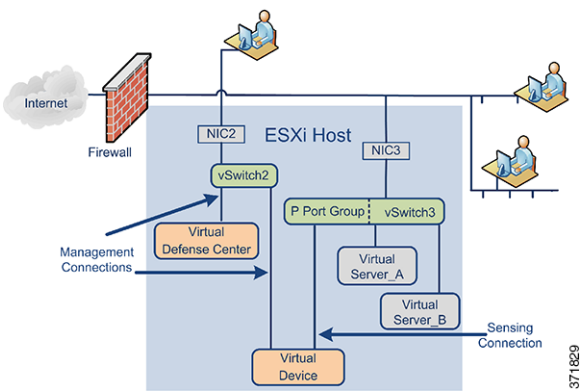
The virtual device monitors and drops any malicious traffic to Server_A and Server_B, depending on your intrusion policy.

Adding a Cisco Firepower Management Center Virtual

You can deploy a Cisco Firepower Management Center Virtual on an ESXi host and connect it to the virtual network as well as the physical network, as shown below. This scenario builds on the [Typical Firepower System Deployment](#), page 23 and on the example shown in [Using the Virtual Device for Inline Detection](#), page 25.

The connection from a Firepower Management Center Virtual through NIC2 to the trusted management network allows the Firepower Management Center Virtual to manage both physical and virtual devices.

Because Cisco virtual appliances are preconfigured with the required application software, they are ready to run when deployed on an ESXi host. This diminishes complex hardware and software compatibility issues so you can accelerate your deployment and concentrate on the benefits of a Firepower System. You can deploy virtual servers, a Firepower Management Center Virtual, and a virtual device on an ESXi host and manage the deployment from the Firepower Management Center Virtual, as shown below.



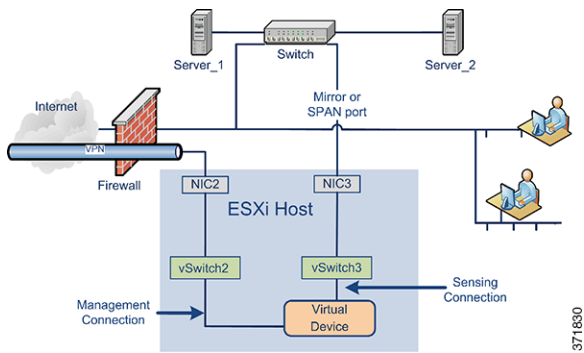
Your sensing connection on your virtual device must be allowed to monitor network traffic. The virtual switch, or the port group on that switch to which the virtual interface connects, must accept promiscuous mode traffic. This permits the virtual device to read packets intended for other machines or network devices. In the example, the P Port Group is set to accept promiscuous mode traffic. See [Configuring Virtual Device Sensing Interfaces](#), page 12.

Your virtual appliance management connections are more typical, non-promiscuous mode connections. The virtual Firepower Management Center provides command and control for the virtual device. The connection through the ESXi host's Network Interface Card (NIC2 in our example) allows you to access the virtual Firepower Management Center. See the *Cisco Firepower Management Center Virtual Quick Start Guide for VMware* and [Setting Up a Firepower NGIPSv Device Using the CLI](#), page 16 for information on setting up the Firepower Management Center Virtual and the virtual device management connections.

Using a Remote Office Deployment

A virtual device is an ideal way to monitor a remote office with limited resources. You can deploy a virtual device on an ESXi host and monitor local traffic, as shown below.

Virtual Firepower Appliance Deployments on VMware



371830

Your sensing connection on your virtual device must be allowed to monitor network traffic. To do this, the virtual switch, or port group on the switch to which the sensing interface connects, must accept promiscuous mode traffic. This permits the virtual device to read packets intended for other machines or network devices. In our example, all of vSwitch3 is set to accept promiscuous mode traffic. VSwitch3 is also connected through NIC3 to the SPAN port so that it can monitor traffic as it passes through the remote office's switch. See [Configuring Virtual Device Sensing Interfaces, page 12](#).

Your virtual device must be managed by a Firepower Management Center. The connection through the ESXi host's Network Interface Card (NIC2 in our example) allows you to access the virtual device with a remote Firepower Management Center.

When deploying devices in disparate geographic locations, you must take precautions to ensure the security of the devices and the data stream by isolating the devices from unprotected networks. You can do this by transmitting the data stream from the device over a VPN or another secure tunneling protocol. See [Setting Up a Firepower NGIPSv Device Using the CLI, page 16](#) for information on setting up the virtual device management connections.



Cisco Firepower Virtual Appliances for VMware Troubleshooting

This section provides information about the most common setup issues, as well as where to submit questions or obtain assistance.

Time Synchronization

If your health monitor indicates that the clock setup for your virtual appliance is not synchronized, check your system policy time synchronization settings. Cisco recommends that you synchronize your virtual appliances to a physical NTP server. Do not synchronize your managed devices (virtual or physical) to a Virtual Cisco Firepower Management Center. To ensure your time synchronization is set up correctly, see *Synchronizing Time* in the *Firepower Management Center Configuration Guide*. After you determine that the clock setup for your virtual appliance is correct, contact your ESXi host administrator and ensure that the server's time configuration is correct.

Performance Issues

If you are having performance issues, remember that there are several factors that affect your virtual appliance. See [Virtual Appliance Performance, page 4](#) for a list of the factors that may affect your performance. To monitor ESXi host performance, you can use your vSphere Client and the information found under the **Performance** tab.

Connectivity Issues

You can view and confirm connectivity for the management and sensing interfaces using VMware vCloud Director Web Portal and vSphere Client.

Using VMware vCloud Director Web Portal

You can use VMware vCloud Director web portal to view and confirm that the management connection and sensing interfaces are properly connected.

To confirm connectivity:

1. Select **My Cloud > VMs**, hover over the virtual appliance you want to view, and right-click.
2. On the Actions window, click **Properties**.
3. On the **Hardware** tab, view the NICs for the management and sensing interfaces to confirm connectivity.

Using vSphere Client

You can use vSphere Client to confirm that the management connection and sensing interfaces are properly connected.

Management Connection

During initial setup, it is important to ensure that network adapter connects at power on. If you do not, the initial management connection setup cannot properly complete and ends with the message:

```
ADDRCONF (NETDEV_UP): eth0: link is not ready
```

To ensure that the management connection is connected:

1. Right-click the name of the virtual appliance in the vSphere Client and select **Edit Settings**. Select **Network adapter 1** in the **Hardware** list and make sure the **Connect at power on** check box is selected.

When the initial management connection completes properly, check the `/var/log/messages` directory for this message:

```
ADDRCONF (NETDEV_CHANGE): eth0: link becomes ready
```

Sensing Interfaces

During initial setup, it is important to ensure that sensing interfaces connect at power on.

To ensure that the sensing interfaces connect at power on:

1. Right-click the name of the virtual device in the vSphere Client and select **Edit Settings**. Select **Network adapter 2** and **Network adapter 3** in the **Hardware** list. Make sure the **Connect at power on** check box is selected for each adapter in use.

You must connect your virtual device sensing interfaces to a virtual switch or virtual switch group that accepts promiscuous mode traffic. If it is not, your device can detect only broadcast traffic.

What to Do Next

- See [Configuring Virtual Device Sensing Interfaces, page 12](#) to ensure your sensing interfaces detect all exploits.

Inline Interface Configurations

You can verify that your inline interfaces are symmetrical and that traffic is flowing between them. To open the VMware console to your virtual device, use either VMware vCloud Director web portal or vSphere Client.

To ensure that the inline sensing interfaces are configured properly:

1. At the console, log in as a user with CLI Configuration (Administrator) privileges.
2. Type `expert` to display the shell prompt.
3. Enter the command: `cat /proc/sf/sfe1000.*`

A text file appears with information similar to this example:

```
SFE1000 driver for eth1 is Fast, has link, is bridging, not MAC filtering, MAC timeout 7500,
Max Latency 0.
 39625470 packets received.
      0 packets dropped by user.
 13075508 packets sent.
0 Mode 1 LB Total 0 Bit 000...
.
.
SFE1000 driver for eth2 is Fast, has link, is bridging, not MAC filtering, MAC timeout 7500,
Max Latency 0.
 13075508 packets received.
      0 packets dropped by user.
```

```
39625470 packets sent.  
0 Mode 1 LB Total 0 Bit 00
```

Note that the number of packets received on `eth1` matches those sent from `eth2` and those sent from `eth1` match those received on `eth2`.

4. Log out of the virtual device.
5. Optionally, and if direct routing to the protected domain is supported, ping the protected virtual appliance where the inline interface of the virtual device is connected.

Pings return to indicate there is connectivity through the inline interface set of the virtual device.

For Assistance

Thank you for using Cisco products.

Cisco Support

If you have any questions or require assistance with the Cisco ASA appliances, please contact Cisco Support:

- Visit the Cisco Support Site at <http://www.cisco.com/cisco/web/support/index.html>.
- Email Cisco Support at tac@cisco.com.
- Call Cisco Support at 1.408.526.7209 or 1.800.553.2447.

For Assistance