



# 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](#).

