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:

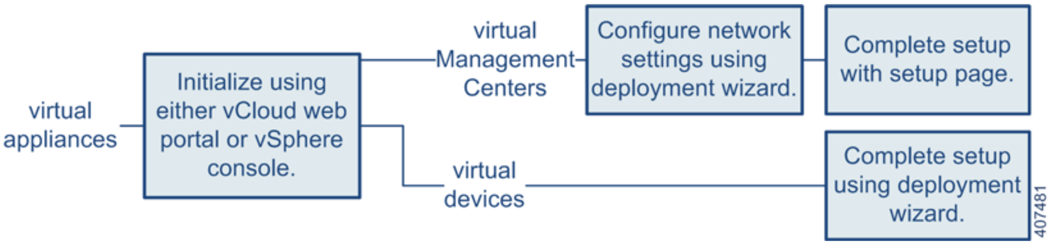
- an Open Virtual Format (`.ovf`) template containing `-ESXi-` in the file name
- an Open Virtual Format (`.ovf`) template containing `-VI-` in the file name
- a Manifest File (`.mf`) containing `-ESXi-` in the file name
- a Manifest File (`.mf`) containing `-VI-` in the file name
- the Virtual Machine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

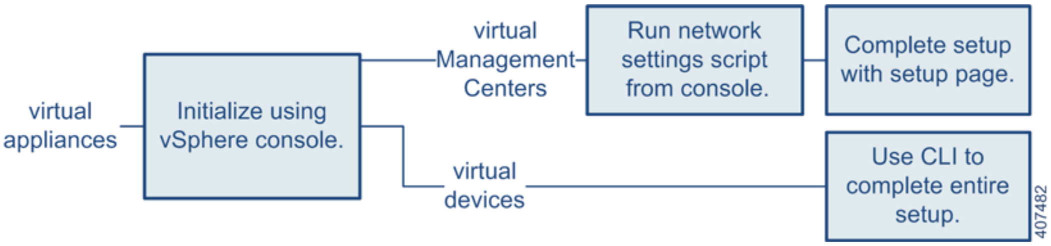
The following diagram shows the general process of setting up Firepower System virtual appliances when you deploy with a VI OVF template.


virtual appliances
Initialize using either vCloud web portal or vSphere console.
virtual Management Centers
Configure network settings using deployment wizard.
Complete setup with setup page.
virtual devices
Complete setup using deployment wizard.
407481

- 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.


virtual appliances
Initialize using vSphere console.
virtual Management Centers
Run network settings script from console.
Complete setup with setup page.
virtual devices
Use CLI to complete entire setup.
407482

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 the 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 CenterVirtual — see the *Cisco Firepower Management Center Virtual Quick Start Guide for VMware* for information on how to deploy the virtual Firepower Management Center.