Getting Started with Firepower Threat Defense Virtual and VMware

The Cisco Firepower Threat Defense Virtual (FTDv) brings Cisco's Firepower Next-Generation Firewall functionality to virtualized environments, enabling consistent security policies to follow workloads across your physical, virtual, and cloud environments, and between clouds.

This chapter describes how the Firepower Threat Defense Virtual functions within a VMware ESXi environment, including feature support, system requirements, guidelines, and limitations. This chapter also describes your options for managing the FTDv.

It's important that you understand your management options before you begin your deployment. You can manage and monitor the FTDv using the Firepower Management Center or the Firepower Device Manager. Other management options may be available.

- About Firepower Threat Defense Virtual and VMware, on page 1
- VMware Feature Support for the Firepower Threat Defense Virtual, on page 2
- How to Manage Your Firepower Device, on page 3
- System Requirements, on page 4
- Guidelines, Limitations, and Known Issues for Firepower Threat Defense Virtual and VMware, on page 7
- Plan the Interfaces, on page 10

About Firepower Threat Defense Virtual and VMware

Cisco packages 64-bit Firepower Threat Defense Virtual (FTDv) devices for VMware vSphere vCenter and ESXi hosting environments. The FTDv is distributed in an Open Virtualization Format (OVF) package available from Cisco.com. OVF is an open-source standard for packaging and distributing software applications for virtual machines (VM). An OVF package contains multiple files in a single directory.

You can deploy the FTDv to any x86 device that is capable of running VMware ESXi. In order to deploy the FTDv you should be familiar with VMware and vSphere, including vSphere networking, ESXi host setup and configuration, and virtual machine guest deployment.
## VMware Feature Support for the Firepower Threat Defense Virtual

The following table lists the VMware feature support for the Firepower Threat Defense Virtual.

**Table 1: VMware Feature Support for the FTDv**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Support (Yes/No)</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cold Clone</td>
<td>The VM is powered off during cloning.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>vMotion</td>
<td>Used for live migration of VMs.</td>
<td>Yes</td>
<td>Use shared storage. See Guidelines, Limitations, and Known Issues for Firepower Threat Defense Virtual and VMware.</td>
</tr>
<tr>
<td>Hot add</td>
<td>The VM is running during an addition.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Hot clone</td>
<td>The VM is running during cloning.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Hot removal</td>
<td>The VM is running during removal.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Snapshot</td>
<td>The VM freezes for a few seconds.</td>
<td>No</td>
<td>Risk of out-of-sync situations between the FMC and managed devices.</td>
</tr>
<tr>
<td>Suspend and resume</td>
<td>The VM is suspended, then resumed.</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>vCloud Director</td>
<td>Allows automatic deployment of VMs.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>VMware FT</td>
<td>Used for HA on VMs.</td>
<td>No</td>
<td>Use the Firepower failover feature for Firepower Threat Defense Virtual VM failovers.</td>
</tr>
<tr>
<td>VMware HA with VM heartbeats</td>
<td>Used for VM failures.</td>
<td>No</td>
<td>Use the Firepower failover feature for Firepower Threat Defense Virtual VM failovers.</td>
</tr>
<tr>
<td>VMware vSphere Standalone</td>
<td>Used to deploy VMs.</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Windows Client</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
How to Manage Your Firepower Device

You have two options to manage your Firepower Threat Defense device.

Firepower Device Manager

The Firepower Device Manager (FDM) onboard integrated manager.

FDM is a web-based configuration interface included on some Firepower Threat Defense devices. FDM lets you configure the basic features of the software that are most commonly used for small networks. It is especially designed for networks that include a single device or just a few, where you do not want to use a high-powered multiple-device manager to control a large network containing many Firepower Threat Defense devices.

Note

See the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for list of Firepower Threat Defense devices that support FDM.

Firepower Management Center

The Cisco Firepower Management Center (FMC).

If you are managing large numbers of devices, or if you want to use the more complex features and configurations that Firepower Threat Defense allows, use the FMC to configure your devices instead of the integrated FDM.

Important

You cannot use both the FDM and FMC to manage a Firepower device. Once the FDM integrated management is enabled, it won't be possible to use an FMC to manage the Firepower device, unless you disable the local management and re-configure the management to use an FMC. On the other hand, when you register the Firepower device to an FMC, the FDM onboard management service is disabled.

Caution

Right now Cisco does not have an option to migrate your FDM Firepower configuration to an FMC and vice-versa. Take this into consideration when you choose what type of management you configure for the Firepower device.
System Requirements

See the Cisco Firepower Compatibility Guide for the most current information about hypervisor support for the Firepower Threat Defense Virtual.

The specific hardware used for FTDv deployments can vary, depending on the number of instances deployed and usage requirements. Each instance of the FTDv requires a minimum resource allocation—number of memory, CPUs, and disk space—on the server.

Systems running VMware vCenter Server and ESXi instances must meet specific hardware and operating system requirements. For a list of supported platforms, see the VMware online Compatibility Guide.

Table 2: Firepower Threat Defense Virtual Appliance Resources

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of cores and memory</td>
<td><strong>Version 6.4 and later</strong></td>
</tr>
<tr>
<td></td>
<td>The FTDv deploys with adjustable vCPU and memory resources. There are three supported vCPU/memory pair values:</td>
</tr>
<tr>
<td></td>
<td>• 4vCPU/8GB (default)</td>
</tr>
<tr>
<td></td>
<td>• 8vCPU/16GB</td>
</tr>
<tr>
<td></td>
<td>• 12vCPU/24GB</td>
</tr>
<tr>
<td></td>
<td>Other vCPU/memory values can be configured; however, only the above three combinations are supported.</td>
</tr>
<tr>
<td>Note</td>
<td>To change the vCPU/memory values, you must first power off the FTDv device.</td>
</tr>
<tr>
<td>Storage</td>
<td><strong>Version 6.3 and earlier</strong></td>
</tr>
<tr>
<td></td>
<td>The FTDv deploys with fixed vCPU and memory resources. There is only one supported vCPU/memory pair value:</td>
</tr>
<tr>
<td></td>
<td>• 4vCPU/8GB</td>
</tr>
<tr>
<td></td>
<td>Other vCPU/memory values can be configured; however, only the above three combinations are supported.</td>
</tr>
<tr>
<td>Note</td>
<td>Adjustments to vCPUs and memory are not supported.</td>
</tr>
<tr>
<td></td>
<td>Based on Disk Format selection.</td>
</tr>
<tr>
<td></td>
<td>• Thin Provision disk size is 48.24GB.</td>
</tr>
</tbody>
</table>
### Setting | Value
---|---
vNICs | The FTDv supports the following virtual network adapters:

- **VMXNET3**—FTDv on VMware now defaults to vmxnet3 interfaces when you create a virtual device. Previously, the default was e1000. The vmxnet3 driver uses two management interfaces. The first two Ethernet adapters must be configured as management interfaces; one for device management/registration, one for diagnostics.

- **IXGBE**—The ixgbe driver uses two management interfaces. The first two PCI devices must be configured as management interfaces; one for device management/registration, one for diagnostics. The ixgbe driver does not support failover (HA) deployments of FTDv.

- **E1000**—When using e1000 interfaces, the FTDv management interface (br1) for the e1000 driver is a bridged interface with two MAC addresses, one for management and one for diagnostics.

  **Important** For Firepower versions earlier than 6.4, the e1000 was the default interface for FTDv on VMware. Starting with release 6.4, FTDv on VMware defaults to vmxnet3 interfaces. If your virtual device is currently using e1000 interfaces, we strongly recommend that you change your interfaces vmxnet3. See Configuring VMXNET3 Interfaces, on page 13 for more information.

- **IXGBE-VF**—The ixgbe-vf (10 Gbit/s) driver supports virtual function devices that can only be activated on kernels that support SR-IOV. SR-IOV requires the correct platform and OS support; see Support for SR-IOV for more information.

### Support for Virtualization Technology

- Virtualization Technology (VT) is a set of enhancements to newer processors that improves performance for running virtual machines. Your system should have CPUs that support either Intel VT or AMD-V extensions for hardware virtualization. Both Intel and AMD provide online processor identification utilities to help you identify CPUs and determine their capabilities.

- Many servers that include CPUs with VT support might have VT disabled by default, so you must enable VT manually. You should consult your manufacturer's documentation for instructions on how to enable VT support on your system.

**Note** If your CPUs support VT, but you do not see this option in the BIOS, contact your vendor to request a BIOS version that lets you enable VT support.
Support for SR-IOV

SR-IOV Virtual Functions require specific system resources. A server that supports SR-IOV is required in addition to an SR-IOV capable PCIe adapter. You must be aware of the following hardware considerations:

- The capabilities of SR-IOV NICs, including the number of VFs available, differ across vendors and devices. The following NICs are supported:
  - Intel Ethernet Server Adapter X520 - DA2
  - Intel Ethernet Server Adapter X540

- Not all PCIe slots support SR-IOV.

- SR-IOV-capable PCIe slots may have different capabilities.

- x86_64 multicore CPU — Intel Sandy Bridge or later (Recommended).

  **Note**
  
  We tested the FTDv on Intel's Broadwell CPU (E5-2699-v4) at 2.3GHz.

  - Cores
    - Minimum of 8 physical cores per CPU socket.
    - The 8 cores must be on a single socket.

  **Note**
  
  CPU pinning is recommended to achieve full throughput.

You should consult your manufacturer's documentation for SR-IOV support on your system. You can search the VMware online Compatibility Guide for system recommendations that include SR-IOV support.

Support for SSSE3

- Firepower Threat Defense Virtual requires support for Supplemental Streaming SIMD Extensions 3 (SSSE3 or SSE3S), an single instruction, multiple data (SIMD) instruction set created by Intel.

- Your system should have CPUs that support SSSE3, such as Intel Core 2 Duo, Intel Core i7/i5/i3, Intel Atom, AMD Bulldozer, AMD Bobcat, and later processors.

- See this reference page for more information about the SSSE3 instruction set and CPUs that support SSSE3.

Verify CPU Support

You can use the Linux command line to get information about the CPU hardware. For example, the /proc/cpuinfo file contains details about individual CPU cores. Output its contents with less or cat.

You can look at the flags section for the following values:

- vmx—Intel VT extensions
- svm—AMD-V extensions
• ssse3—SSSE3 extensions

Use `grep` to quickly see if any of these values exist in the file by running the following command:

```
egrep "vmx|svm|ssse3" /proc/cpuinfo
```

If your system supports VT or SSSE3, then you should see vmx, svm, or ssse3 in the list of flags. The following example shows output from a system with two CPUs:

```
flags : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm syscall nx lm constant_tsc pni monitor ds_cpl vmx est tm2 ssse3 cx16 xtpr lahf_lm
```

Guidelines, Limitations, and Known Issues for Firepower Threat Defense Virtual and VMware

Management Mode

• You have two options to manage your Firepower Threat Defense device:
  • The Firepower Device Manager (FDM) onboard integrated manager.

  ![Note]
  
  The FTDv on VMware supports Firepower Device Manager starting with Cisco Firepower software version 6.2.2 and later. Any FTDv on VMware running Firepower software earlier than version 6.2.2 can only be managed using the Firepower Management Center; see How to Manage Your Firepower Device, on page 3

  ![Note]
  
  When you choose Yes for Enable Local Manager, the Firewall Mode is changed to routed. This is the only supported mode when using Firepower Device Manager.

• The Firepower Management Center (FMC)

  • You must install a new image (version 6.2.2 or greater) to get Firepower Device Manager support. You cannot upgrade an existing FTDv virtual machine from an older version (earlier than 6.2.2) and then switch to Firepower Device Manager.

  • Firepower Device Manager (local manager) is enabled by default.
OVF File Guidelines

You have the following installation options for installing a Firepower Threat Defense Virtual appliance:

- Cisco_Firepower_Threat_Defense_Virtual-VI-X.X.X-xxx.ovf
- Cisco_Firepower_Threat_Defense_Virtual-ESXi-X.X.X-xxx.ovf

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

- If you deploy with a VI OVF template, the installation process allows you to perform the entire initial setup for FTDv appliance. You can specify:
  - A new password for the admin account.
  - Network settings that allow the appliance to communicate on your management network.
  - Management, either local management using Firepower Device Manager (default) or remote management using the Firepower Management Center.
  - Firewall Mode. When you choose Yes for Enable Local Manager, the Firewall Mode is changed to routed. This is the only supported mode when using Firepower Device Manager.

  **Note** You must manage this virtual appliance using VMware vCenter.

- If you deploy using an ESXi OVF template, you must configure Firepower System-required settings after installation. You manage this FTDv as a standalone appliance on ESXi; see Deploy the Firepower Threat Defense Virtual to a vSphere ESXi Host, on page 19 for more information.

vMotion Support

We recommend that you only use shared storage if you plan to use vMotion. During deployment, if you have a host cluster you can either provision storage locally (on a specific host) or on a shared host. However, if you try to vMotion the Firepower Management Center Virtual to another host, using local storage will produce an error.

INIT Respawning Error Messages Symptom

You may see the following error message on the FTDv console running on ESXi 6 and ESXi 6.5:

"INIT: Id "ftdv" respawning too fast: disabled for 5 minutes"

**Workaround**—Edit the virtual machine settings in vSphere to add a serial port while the device is powered off.

1. Right-click the virtual machine and select **Edit Settings**.
2. On the Virtual Hardware tab, select **Serial port** from the **New device** drop-down menu, and click **Add**.
   The serial port appears at the bottom of the virtual device list.
3. On the **Virtual Hardware** tab, expand **Serial port**, and select connection type **Use physical serial port**.
4. Uncheck the **Connect at power on** checkbox.
   Click **OK** to save settings.
Modify the Security Policy Settings for a vSphere Standard Switch

For a vSphere standard switch, the three elements of the Layer 2 Security policy are promiscuous mode, MAC address changes, and forged transmits. Firepower Threat Defense Virtual uses promiscuous mode to operate, and Firepower Threat Defense Virtual high availability depends on switching the MAC address between the active and the standby to operate correctly.

The default settings will block correct operation of Firepower Threat Defense Virtual. See the following required settings:

<p>| Table 3: vSphere Standard Switch Security Policy Options |
|---------------------------------|----------------|----------------|</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Required Setting</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Promiscuous Mode</td>
<td>Accept</td>
<td>You must edit the security policy for a vSphere standard switch in the vSphere Web Client and set the Promiscuous mode option to Accept. Firewalls, port scanners, intrusion detection systems and so on, need to run in promiscuous mode.</td>
</tr>
<tr>
<td>MAC Address Changes</td>
<td>Accept</td>
<td>You should verify the security policy for a vSphere standard switch in the vSphere Web Client and confirm the MAC address changes option is set to Accept.</td>
</tr>
<tr>
<td>Forged Transmits</td>
<td>Accept</td>
<td>You should verify the security policy for a vSphere standard switch in the vSphere Web Client and confirm the Forged transmits option is set to Accept.</td>
</tr>
</tbody>
</table>

Modify the Security Policy Settings for a vSphere Standard Switch

The default settings will block correct operation of FTDv.

Procedure

**Step 1**  In the vSphere Web Client, navigate to the host.
**Step 2**  On the Manage tab, click Networking, and select Virtual switches.
**Step 3**  Select a standard switch from the list and click Edit settings.
**Step 4**  Select Security and view the current settings.
**Step 5**  Accept promiscuous mode activation, MAC address changes, and forged transmits in the guest operating system of the virtual machines attached to the standard switch.
Plan the Interfaces

You can avoid reboots and configuration issues by planning the Firepower Threat Defense Virtual vNIC and interface mapping in advance of deployment. The FTDv deploys with 10 interfaces, and must be powered up at firstboot with at least 4 interfaces.

The FTDv supports the vmxnet3 (default), ixgbe, and e1000 virtual network adapters. In addition, with a properly configured system, FTDv also supports the ixgbe-vf driver for SR-IOV; see System Requirements, on page 4 for more information.

Important

FTDv on VMware now defaults to vmxnet3 interfaces when you create a virtual device. Previously, the default was e1000. If you are using e1000 interfaces, we **strongly recommend** you switch. The vmxnet3 device drivers and network processing are integrated with the ESXi hypervisor, so they use fewer resources and offer better network performance.

Step 6  
Click OK.

What to do next

- Ensure these settings are the same on all networks that are configured for management and failover (HA) interfaces on FTDv devices.
Interface Guidelines and Limitations

The following sections provide guidelines and limitations for the supported virtual network adapters used with FTDv on VMware. It’s important to keep these guidelines in mind when planning your deployment.

General Guidelines

• As previously stated, the FTDv deploys with 10 interfaces, and must be powered up at firstboot with at least 4 interfaces. You need to assign a network to AT LEAST FOUR INTERFACES.

• You do not need to use all 10 FTDv interfaces; for interfaces you do not intend to use, you can simply leave the interface disabled within the FTDv configuration.

• Keep in mind that you cannot add more virtual interfaces to the virtual machine after deployment. If you delete some interfaces and then decide you want more, you’ll have to delete the virtual machine and start over.

Default VMXNET3 Interfaces

FTDv on VMware now defaults to vmxnet3 interfaces when you create a virtual device. Previously, the default was e1000. If you are using e1000 interfaces, we strongly recommend you switch. The vmxnet3 device drivers and network processing are integrated with the ESXi hypervisor, so they use fewer resources and offer better network performance.

• The vmxnet3 driver uses two management interfaces. The first two Ethernet adapters must be configured as management interfaces; one for device management/registration, one for diagnostics.

• For vmxnet3, Cisco recommends using a host managed by VMware vCenter when using more than four vmxnet3 network interfaces. When deployed on standalone ESXi, additional network interfaces are not added to the virtual machine with sequential PCI bus addresses. When the host is managed with a VMware vCenter, the correct order can be obtained from the XML in the configuration CDROM. When the host is running standalone ESXi, the only way to determine the order of the network interfaces is to manually compare the MAC addresses seen on the FTDv to the MAC addresses seen from the VMware configuration tool.

The following table describes the concordance of Network Adapter, Source Networks and Destination Networks for FTDv for vmxnet3 and ixgbe interfaces.

<table>
<thead>
<tr>
<th>Network Adapter</th>
<th>Source Networks</th>
<th>Destination Networks</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network adapter 1</td>
<td>Management0-0</td>
<td>Management0/0</td>
<td>Management</td>
</tr>
<tr>
<td>Network adapter 2</td>
<td>Diagnostic0-0</td>
<td>Diagnostic0/0</td>
<td>Diagnostic</td>
</tr>
<tr>
<td>Network adapter 3</td>
<td>GigabitEthernet0-0</td>
<td>GigabitEthernet0/0</td>
<td>Outside data</td>
</tr>
<tr>
<td>Network adapter 4</td>
<td>GigabitEthernet0-1</td>
<td>GigabitEthernet0/1</td>
<td>Inside data</td>
</tr>
<tr>
<td>Network adapter 5</td>
<td>GigabitEthernet0-2</td>
<td>GigabitEthernet0/2</td>
<td>Data traffic (Optional)</td>
</tr>
</tbody>
</table>
Interface Guidelines and Limitations

**IXGBE Interfaces**

- The ixgbe driver uses two management interfaces. The first two PCI devices must be configured as management interfaces; one for device management/registration, one for diagnostics.

- For ixgbe, the ESXi platform requires the ixgbe NIC to support the ixgbe PCI device. In addition, the ESXi platform has specific BIOS and configuration requirements that are needed to support ixgbe PCI devices. Refer to the Intel Technical Brief for more information.

- The only ixgbe traffic interface types supported are routed and ERSPAN passive. This is due to VMware limitations with respect to MAC address filtering.

- The ixgbe driver does not support failover (HA) deployments of Firepower Threat Defense Virtual.

**E1000 Interfaces**

**Important**

FTDv on VMware now defaults to vmxnet3 interfaces when you create a virtual device. Previously, the default was e1000. If you are using e1000 interfaces, we strongly recommend you switch. The vmxnet3 device drivers and network processing are integrated with the ESXi hypervisor, so they use fewer resources and offer better network performance.

- The management interface (br1) for the e1000 driver is a bridged interface with two MAC addresses, one for management and one for diagnostics.

- If you are upgrading your FTDv to 6.4 and are using e1000 interfaces, you should replace the e1000 interfaces with either vmxnet3 or ixgbe interfaces for greater network throughput.

The following table describes the concordance of Network Adapter, Source Networks and Destination Networks for FTDv for the default e1000 interfaces.

**Table 5: Source to Destination Network Mapping—E1000 Interfaces**

<table>
<thead>
<tr>
<th>Network Adapter</th>
<th>Source Networks</th>
<th>Destination Networks</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network adapter 1</td>
<td>Management0-0</td>
<td>Diagnostic0/0</td>
<td>Management and diagnostic</td>
</tr>
<tr>
<td>Network adapter 2</td>
<td>GigabitEthernet0-0</td>
<td>GigabitEthernet0/0</td>
<td>Outside data</td>
</tr>
<tr>
<td>Network adapter 3</td>
<td>GigabitEthernet0-1</td>
<td>GigabitEthernet0/1</td>
<td>Inside date</td>
</tr>
</tbody>
</table>

---

Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide

12
**Configuring VMXNET3 Interfaces**

Starting with the 6.4 release, FTDv on VMware defaults to vmxnet3 interfaces when you create a virtual device. Previously, the default was e1000. If you are using e1000 interfaces, we strongly recommend you switch. The vmxnet3 device drivers and network processing are integrated with the ESXi hypervisor, so they use fewer resources and offer better network performance.

To change e1000 interfaces to vmxnet3, you must delete ALL interfaces and reinstall them with the vmxnet3 driver.

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

**Procedure**

**Step 1**
Power off the FTDv Virtual Machine.

To change the interfaces, you must power down the appliance.

**Step 2**
Right-click the FTDv Virtual Machine in the inventory and select Edit Settings.

**Step 3**
Select the applicable network adapters and then select Remove.

**Step 4**
Click Add to open the Add Hardware Wizard.

**Step 5**
Select Ethernet adapter and click Next.

**Step 6**
Select the vmxnet3 adapter and then choose network label.

**Step 7**
Repeat for all interfaces on the FTDv.

**What to do next**
- Power on the FTDv from the VMware console.
Adding Interfaces

You can have a total of 10 interfaces (1 management, 1 diagnostic, 8 data interfaces) when you deploy a FTDv device. For data interfaces, make sure that the **Source Networks** map to the correct **Destination Networks**, and that each data interface maps to a unique subnet or VLAN.

---

**Caution**

You cannot add more virtual interfaces to the virtual machine and then have FTDv automatically recognize them. Adding interfaces to a virtual machine requires that you completely wipe out the FTDv configuration. The only part of the configuration that remains intact is the management address and gateway settings.

---

If you need more physical-interface equivalents for a FTDv device, you basically have to start over. You can either deploy a new virtual machine, or you can use the “Add Interfaces to Firepower Threat Defense Virtual” procedure in the [Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager](#).
CHAPTER 2

Deploy the Firepower Threat Defense Virtual

This chapter describes the procedures to deploy the Firepower Threat Defense Virtual to a VMware vSphere environment, either to a vSphere vCenter or to a stand-alone ESXi host.

- About VMware Deployment, on page 15
- Deploy the Firepower Threat Defense Virtual to vSphere vCenter, on page 15
- Deploy the Firepower Threat Defense Virtual to a vSphere ESXi Host, on page 19
- Complete the Firepower Threat Defense Virtual Setup Using the CLI, on page 22

About VMware Deployment

You can deploy the Firepower Threat Defense Virtual (FTDv) to a standalone ESXi server or, if you have vSphere vCenter, you can deploy using the vSphere Client or the vSphere Web Client. To successfully deploy the FTDv you should be familiar with VMware and vSphere including vSphere networking, ESXi host setup and configuration, and virtual machine guest deployment.

FTDv for VMware is distributed using the Open Virtualization Format (OVF), which is a standard method of packaging and deploying virtual machines. VMware provides several methods to provision vSphere virtual machines. The optimal method for your environment depends on factors such as the size and type of your infrastructure and the goals that you want to achieve.

The VMware vSphere Web Client and the vSphere Client are interfaces to vCenter Server, ESXi hosts, and virtual machines. With the vSphere Web Client and the vSphere Client, you can connect remotely to vCenter Server. With the vSphere Client you can also connect directly to ESXi from any Windows system. The vSphere Web Client and the vSphere Client are the primary interfaces for managing all aspects of the vSphere environment. They also provide console access to virtual machines.

All administrative functions are available through the vSphere Web Client. A subset of those functions is available through the vSphere Client.

Deploy the Firepower Threat Defense Virtual to vSphere vCenter

Use this procedure to deploy the Firepower Threat Defense Virtual (FTDv) appliance to VMware vSphere vCenter. You can use the VMware Web Client (or vSphere Client) to deploy and configure FTDv virtual machines.
Before you begin

- You must have at least one network configured in vSphere (for management) before you deploy the FTDv.

Procedure

**Step 1**  
Log in to the vSphere Web Client (or the vSphere Client).

**Step 2**  
Using the vSphere Web Client (or the vSphere Client), deploy the OVF template file you downloaded earlier by clicking **File > Deploy OVF Template**.

The Deploy OVF Template wizard appears.

**Step 3**  
Browse your file system for the OVF template source location and click **Next**.

You want to select the Firepower Threat Defense Virtual VI OVF template:

`Cisco_Firepower_Threat_Defense_Virtual-VI-X.X.X-xxx.ovf`

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

**Step 4**  
Review the **OVF Template Details** page and verify the OVF template information (product name, version, vendor, download size, size on disk, and description) and click **Next**.

**Step 5**  
The **End User License Agreement** page appears. Review the license agreement packaged with the OVF template (VI templates only), click **Accept** to agree to the terms of the licenses and click **Next**.

**Step 6**  
On the **Name and Location** page, enter a name for this deployment and select the a location in the inventory (host or cluster) on which you want to deploy the FTDv, then click **Next**. The name must be unique within the inventory folder and can contain up to 80 characters.

The vSphere Web Client presents the organizational hierarchy of managed objects in inventory views. Inventories are the hierarchal structure used by vCenter Server or the host to organize managed objects. This hierarchy includes all of the monitored objects in vCenter Server.

**Step 7**  
Navigate to, and select the resource pool where you want to run the Firepower Threat Defense Virtual and click **Next**.

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

**Step 8**  
Select a **Deployment Configuration**. Choose one of three supported vCPU/memory values from the **Configuration** drop-down list, and click **Next**.

**Important**  
Beginning with version 6.4, the FTDv deploys with adjustable vCPU and memory resources. Prior to version 6.4, the FTDv deployed as a fixed configuration 4vCPU/8GB device; see **System Requirements**, on page 4.

**Step 9**  
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.

**Step 10**  
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. Thin provisioning can also reduce the amount of time it takes to deploy the virtual appliance.

**Step 11**

On the **Network Mapping** page, map the networks specified in the OVF template to networks in your inventory, and then select **Next**.

Ensure the Management0-0 interface is associated with a VM Network that is reachable from the Internet. Non-management interfaces are configurable from either a Firepower Management Center or from Firepower Device Manager, depending on your management mode.

**Important** FTDv on VMware now defaults to vmxnet3 interfaces when you create a virtual device. Previously, the default was e1000. If you are using e1000 interfaces, we strongly recommend you switch. The vmxnet3 device drivers and network processing are integrated with the ESXi hypervisor, so they use fewer resources and offer better network performance.

The networks may not be in alphabetical order. If it is too difficult to find your networks, you can change the networks later from the **Edit Settings** dialog box. After you deploy, right-click the FTDv instance, and choose **Edit Settings**. However that screen does not show the FTDv IDs (only Network Adapter IDs).

See the following concordance of Network Adapter, Source Networks and Destination Networks for FTDv interfaces (note these are the default vmxnet3 interfaces):

<table>
<thead>
<tr>
<th>Network Adapter</th>
<th>Source Networks</th>
<th>Destination Networks</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network adapter 1</td>
<td>Management0-0</td>
<td>Management0/0</td>
<td>Management</td>
</tr>
<tr>
<td>Network adapter 2</td>
<td>Diagnostic0-0</td>
<td>Diagnostic0/0</td>
<td>Diagnostic</td>
</tr>
<tr>
<td>Network adapter 3</td>
<td>GigabitEthernet0-0</td>
<td>GigabitEthernet0/0</td>
<td>Outside data</td>
</tr>
<tr>
<td>Network adapter 4</td>
<td>GigabitEthernet0-1</td>
<td>GigabitEthernet0/1</td>
<td>Inside date</td>
</tr>
<tr>
<td>Network adapter 5</td>
<td>GigabitEthernet0-2</td>
<td>GigabitEthernet0/2</td>
<td>Data traffic (Optional)</td>
</tr>
<tr>
<td>Network adapter 6</td>
<td>GigabitEthernet0-3</td>
<td>GigabitEthernet0/3</td>
<td>Data traffic (Optional)</td>
</tr>
<tr>
<td>Network adapter 7</td>
<td>GigabitEthernet0-4</td>
<td>GigabitEthernet0/4</td>
<td>Data traffic (Optional)</td>
</tr>
<tr>
<td>Network adapter 8</td>
<td>GigabitEthernet0-5</td>
<td>GigabitEthernet0/5</td>
<td>Data traffic (Optional)</td>
</tr>
<tr>
<td>Network adapter 9</td>
<td>GigabitEthernet0-6</td>
<td>GigabitEthernet0/6</td>
<td>Data traffic (Optional)</td>
</tr>
<tr>
<td>Network adapter 10</td>
<td>GigabitEthernet0-7</td>
<td>GigabitEthernet0/7</td>
<td>Data traffic (Optional)</td>
</tr>
</tbody>
</table>

You can have a total of 10 interfaces when you deploy the FTDv. For data interfaces, make sure that the Source Networks map to the correct Destination Networks, and that each data interface maps to a unique subnet or VLAN. You do not need to use all FTDv interfaces; for interfaces you do not intend to use, you can simply leave the interface disabled within the FTDv configuration.

**Step 12**

On the **Properties** page, set the user-configurable properties packaged with the OVF template (VI templates only):

a) **Password**
Set the password for FTDv admin access.

b) **Network**

Set the network information, including the Fully Qualified Domain Name (FQDN), DNS, search domain, and network protocol (IPv4 or IPv6).

c) **Management**

Set the management mode. Click the drop-down arrow for **Enable Local Manager** and select **Yes** to use the integrated Firepower Device Manager web-based configuration tool. Select **No** to use a Firepower Management Center to manage this device. See **How to Manage Your Firepower Device**, on page 3 for an overview of how to choose your management option.

d) **Firewall Mode**

Set the initial firewall mode. Click the drop-down arrow for **Firewall Mode** and choose one of the two supported modes, either **Routed** or **Transparent**.

If you chose **Yes** for **Enable Local Manager**, you can only select **Routed** firewall mode. You cannot configure transparent firewall mode interfaces using the local Firepower Device Manager.

e) **Registration**

If you chose **No** for **Enable Local Manager**, you need to provide the required credentials to register this device to the managing **Firepower Management Center**. Provide the following:

- **Managing Defense Center**—Enter the hostname or IP address of the FMC.
- **Registration Key**—The registration key is a user-generated one-time use key that must not exceed 37 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). You will need to remember this registration key when you add the device to the FMC.
- **NAT ID**—If the FTDv and the FMC are separated by a Network Address Translation (NAT) device, and the Firepower Management Center is behind a NAT device, enter a unique NAT ID. This is a user-generated one-time use key that must not exceed 37 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-).

f) Click **Next**.

**Step 13**

In the **Ready to Complete** section, review and verify the displayed information. To begin the deployment with these settings, click **Finish**. To make any changes, click **Back** to navigate back through the screens.

Optionally, check the **Power on after deployment** option to power on the FTDv, then click **Finish**.

After you complete the wizard, the vSphere Web Client processes the virtual machine; 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 FTDv virtual instance 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 FTDv with the Cisco Licensing Authority, the FTDv requires Internet access. You might need to perform additional configuration after deployment to achieve Internet access and successful license registration.
What to do next

Your next steps depend on what management mode you chose.

- If you chose No for Enable Local Manager, you'll use the Firepower Management Center to manage your FTDv; see Managing the Firepower Threat Defense Virtual with the Firepower Management Center, on page 25.

- If you chose Yes for Enable Local Manager, you'll use the integrated Firepower Device Manager to manage your FTDv; see Managing the Firepower Threat Defense Virtual with the Firepower Device Manager, on page 41.

See How to Manage Your Firepower Device, on page 3 for an overview of how to choose your management option.

Deploy the Firepower Threat Defense Virtual to a vSphere ESXi Host

Use this procedure to deploy the Firepower Threat Defense Virtual (FTDv) appliance on a single ESXi host. You can use the VMware Host Client (or vSphere Client) to manage single ESXi hosts and to perform administrative tasks such as basic virtualization operations, such as deploying and configuring FTDv virtual machines.

Note

It is important to know that the VMware Host Client is different from the vSphere Web Client, regardless of their similar user interfaces. You use the vSphere Web Client to connect to vCenter Server and manage multiple ESXi hosts, whereas you use the VMware Host Client to manage a single ESXi host.

For instructions of how to deploy a Firepower Threat Defense Virtual appliance to a vCenter environment, see Deploy the Firepower Threat Defense Virtual to vSphere vCenter, on page 15.

Before you begin

- You must have at least one network configured in vSphere (for management) before you deploy the FTDv.

Procedure

Step 1

Download the Firepower Threat Defense Virtual install package for VMware ESXi from Cisco.com, and save it to your local management computer:

https://www.cisco.com/go/ftd-software

A Cisco.com login and Cisco service contract are required.

Step 2

Unpack the tar file into a working directory. Do not remove any files from the directory. The following files are included:

- Cisco_Firepower_Threat_Defense_Virtual-VI-X.X.X.xx.ovf—for vCenter deployments
• Cisco_Firepower_Threat_Defense_Virtual-ESXi-X.X.X-xx.ovf—For ESXi deployments.
• Cisco_Firepower_Threat_Defense_Virtual-ESXi-X.X.X-xx.mf—Manifest file for ESXi deployments.

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

**Step 3**  
In a browser enter the ESXi target host name or IP address using the form `http://host-name/ui` or `http://host-IP-address/ui`.  
A log in screen appears.

**Step 4**  
Enter the administrator user name and password.

**Step 5**  
Click **Login** to continue.  
You are now logged in to your target ESXi host.

**Step 6**  
Right-click on **Host** in the VMware Host Client inventory and select **Create/Register VM**.  
The New Virtual Machine wizard opens.

**Step 7**  
On the **Select creation type** page of the wizard, select **Deploy a virtual machine from an OVF or OVA file** and click **Next**.

**Step 8**  
On the **Select OVF and VMDK files** page of the wizard:

a) Enter a name for your FTDv virtual machine.  
Virtual machine names can contain up to 80 characters and must be unique within each ESXi instance.

b) Click the blue pane, browse to the directory where you unpacked the FTDv tar file, and choose the ESXi OVF template and the accompanying VMDK file:

- Cisco_Firepower_Threat_Defense_Virtual-ESXi-X.X.X-xx.ovf
- Cisco_Firepower_Threat_Defense_Virtual-X.X.X-xx.vmdk

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

**Attention**  
Make sure you select the ESXi OVF.

**Step 9**  
Click **Next**.  
Your local system storage opens.

**Step 10**  
Choose a datastore from the list of accessible datastores on the **Select storage** page of the wizard.  
The datastore stores the virtual machine configuration files and all of the virtual disks. Each datastore might have a different size, speed, availability, and other properties.

**Step 11**  
Click **Next**.

**Step 12**  
Configure the **Deployment options** that come packaged with the ESXi OVF for the FTDv:

a) **Network Mapping**—Map the networks specified in the OVF template to networks in your inventory, and then select **Next**.
Ensure the Management0-0 interface is associated with a VM Network that is reachable from the Internet. Non-management interfaces are configurable from either a Firepower Management Center or from Firepower Device Manager, depending on your management mode.

**Important**  FTDv on VMware now defaults to vmxnet3 interfaces when you create a virtual device. Previously, the default was e1000. If you are using e1000 interfaces, we **strongly recommend** you switch. The vmxnet3 device drivers and network processing are integrated with the ESXi hypervisor, so they use fewer resources and offer better network performance.

The networks may not be in alphabetical order. If it is too difficult to find your networks, you can change the networks later from the **Edit Settings** dialog box. After you deploy, right-click the FTDv instance, and choose **Edit Settings**. However that screen does not show the FTDv IDs (only Network Adapter IDs).

See the following concordance of Network Adapter, Source Networks and Destination Networks for FTDv interfaces (note these are the default vmxnet3 interfaces):

**Table 7: Source to Destination Network Mapping—VMXNET3**

<table>
<thead>
<tr>
<th>Network Adapter</th>
<th>Source Networks</th>
<th>Destination Networks</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network adapter 1</td>
<td>Management0-0</td>
<td>Management0/0</td>
<td>Management</td>
</tr>
<tr>
<td>Network adapter 2</td>
<td>Diagnostic0-0</td>
<td>Diagnostic0/0</td>
<td>Diagnostic</td>
</tr>
<tr>
<td>Network adapter 3</td>
<td>GigabitEthernet0-0</td>
<td>GigabitEthernet0/0</td>
<td>Outside data</td>
</tr>
<tr>
<td>Network adapter 4</td>
<td>GigabitEthernet0-1</td>
<td>GigabitEthernet0/1</td>
<td>Inside date</td>
</tr>
<tr>
<td>Network adapter 5</td>
<td>GigabitEthernet0-2</td>
<td>GigabitEthernet0/2</td>
<td>Data traffic (Optional)</td>
</tr>
<tr>
<td>Network adapter 6</td>
<td>GigabitEthernet0-3</td>
<td>GigabitEthernet0/3</td>
<td>Data traffic (Optional)</td>
</tr>
<tr>
<td>Network adapter 7</td>
<td>GigabitEthernet0-4</td>
<td>GigabitEthernet0/4</td>
<td>Data traffic (Optional)</td>
</tr>
<tr>
<td>Network adapter 8</td>
<td>GigabitEthernet0-5</td>
<td>GigabitEthernet0/5</td>
<td>Data traffic (Optional)</td>
</tr>
<tr>
<td>Network adapter 9</td>
<td>GigabitEthernet0-6</td>
<td>GigabitEthernet0/6</td>
<td>Data traffic (Optional)</td>
</tr>
<tr>
<td>Network adapter 10</td>
<td>GigabitEthernet0-7</td>
<td>GigabitEthernet0/7</td>
<td>Data traffic (Optional)</td>
</tr>
</tbody>
</table>

You can have a total of 10 interfaces when you deploy the FTDv. For data interfaces, make sure that the Source Networks map to the correct Destination Networks, and that each data interface maps to a unique subnet or VLAN. You do not need to use all FTDv interfaces; for interfaces you do not intend to use, you can simply leave the interface disabled within the FTDv configuration.

b) **Disk provisioning**—Select the disk format to store the virtual machine virtual disks.

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. Thin provisioning can also reduce the amount of time it takes to deploy the virtual appliance.

**Step 13**  On the **Ready to complete** page of the New virtual machine wizard, review the configuration settings for the virtual machine.

a) (Optional) Click **Back** to go back and review or modify the wizard settings.

b) (Optional) Click **Cancel** to discard the creation task and close the wizard.
c) Click **Finish** to complete the creation task and close the wizard.

After you complete the wizard, the ESXi host processes the VM; you can see the deployment status in the **Recent Tasks** pane. A successful deployment shows *Completed successfully* under the **Results** column.

The new FTDv virtual machine instance then appears under the Virtual Machines inventory of the ESXi host. Booting up the new virtual machine could take up to 30 minutes.

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

---

**What to do next**

- Complete the set up of your virtual device using the CLI. This is the next step when you deploy the FTDv using the ESXi OVF template; see *Complete the Firepower Threat Defense Virtual Setup Using the CLI*, on page 22.

---

**Complete the Firepower Threat Defense Virtual Setup Using the CLI**

If you deployed with an ESXi OVF template, you must set up the FTDv using the CLI. Firepower Threat Defense Virtual appliances do not have web interfaces. 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 device configuration is required. Your next steps depend on which management mode you choose.

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 firewall 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.

**Procedure**

**Step 1** Open the VMware console.

**Step 2** At the **firepower login** prompt, log in with the default credentials of username **admin** and the password **Admin123**.

**Step 3** When the Firepower Threat Defense system boots, a setup wizard prompts you for the following information required to configure the system:

- Accept EULA
• New admin password
• IPv4 or IPv6 configuration
• IPv4 or IPv6 DHCP settings
• Management port IPv4 address and subnet mask, or IPv6 address and prefix
• System name
• Default gateway
• DNS setup
• HTTP proxy
• Management mode (local management uses Firepower Device Manager).

Step 4
Review the Setup wizard settings. Defaults or previously entered values appear in brackets. To accept previously entered values, press Enter.
The VMware console may display messages as your settings are implemented.

Step 5
Complete the system configuration as prompted.

Step 6
Verify the setup was successful when the console returns to the firepower # prompt.

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

What to do next
Your next steps depend on what management mode you chose.

• If you chose No for Enable Local Manager, you'll use the Firepower Management Center to manage your FTDv; see Managing the Firepower Threat Defense Virtual with the Firepower Management Center, on page 25.

• If you chose Yes for Enable Local Manager, you'll use the integrated Firepower Device Manager to manage your FTDv; see Managing the Firepower Threat Defense Virtual with the Firepower Device Manager, on page 41.

See How to Manage Your Firepower Device, on page 3 for an overview of how to choose your management option.
CHAPTER 3

Managing the Firepower Threat Defense Virtual with the Firepower Management Center

This chapter describes how to deploy a standalone FTDv device managed with a FMC.

Note
This document covers the latest FTDv version features; see History for Managing the Firepower Threat Defense Virtual with the Firepower Management, on page 39 for details about feature changes. If you are on an old version of software, refer to the procedures in the FMC configuration guide for your version.

- About Firepower Threat Defense Virtual with Firepower Management Center, on page 25
- Log Into the Firepower Management Center, on page 26
- Register the Device with the Firepower Management Center, on page 26
- Configure a Basic Security Policy, on page 28
- Access the Firepower Threat Defense CLI, on page 38
- History for Managing the Firepower Threat Defense Virtual with the Firepower Management, on page 39

About Firepower Threat Defense Virtual with Firepower Management Center

The Firepower Threat Defense Virtual (FTDv) is the virtualized component of the Cisco NGFW solution. The FTDv provides next-generation firewall services, including stateful firewalling, routing, VPN, Next-Generation Intrusion Prevention System (NGIPS), Application Visibility and Control (AVC), URL filtering, and Advanced Malware Protection (AMP).

You can manage the FTDv using the Firepower Management Center (FMC), a full-featured, multidevice manager on a separate server. For information about installing the FMC, see the FMC getting started guide.

The FTDv registers and communicates with the FMC on the Management interface that you allocated to the FTDv virtual machine.

For troubleshooting purposes, you can access the FTD CLI using SSH on the Management interface, or you can connect to the FTD from the Firepower CLI.
Log Into the Firepower Management Center

Use the FMC to configure and monitor the FTD.

**Before you begin**

For information on supported browsers, refer to the release notes for the version you are using (see https://www.cisco.com/go/firepower-notes).

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1 | Using a supported browser, enter the following URL.  
  **https://fmc_ip_address**  
  - **fmc_ip_address**—Identifies the IP address or host name of the FMC. |
| 2 | Enter your username and password. |
| 3 | Click **Log In**. |

Register the Device with the Firepower Management Center

**Before you begin**

Make sure the FTDv virtual machine has deployed successfully, is powered on, and has gone through its first boot procedures.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose <strong>Devices &gt; Device Management</strong>.</td>
</tr>
<tr>
<td>2</td>
<td>From the <strong>Add</strong> drop-down list, choose <strong>Add Device</strong>, and enter the following parameters.</td>
</tr>
</tbody>
</table>
• **Host**—Enter the IP address of the logical device you want to add. You can leave this field blank if you specified both the FMC IP address and a NAT ID in the FTD bootstrap configuration.

• **Display Name**—Enter the name for the logical device as you want it to display in the FMC.

• **Registration Key**—Enter the same registration key that you specified in the FTDv bootstrap configuration.

• **Domain**—Assign the device to a leaf domain if you have a multidomain environment.

• **Group**—Assign it to a device group if you are using groups.

• **Access Control Policy**—Choose an initial policy. Unless you already have a customized policy you know you need to use, choose **Create new policy**, and choose **Block all traffic**. You can change this later to allow traffic; see *Configure Access Control*, on page 36.

• **Smart Licensing**—Assign the Smart Licenses you need for the features you want to deploy: **Malware** (if you intend to use AMP malware inspection), **Threat** (if you intend to use intrusion prevention), and **URL** (if you intend to implement category-based URL filtering).
Configure a Basic Security Policy

This section describes how to configure a basic security policy with the following settings:

- **Inside and outside interfaces**—Assign a static IP address to the inside interface, and use DHCP for the outside interface.
- **DHCP server**—Use a DHCP server on the inside interface for clients.
- **Default route**—Add a default route through the outside interface.
- **NAT**—Use interface PAT on the outside interface.
- **Access control**—Allow traffic from inside to outside.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Configure Interfaces, on page 29</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Configure The DHCP Server, on page 32</td>
</tr>
<tr>
<td>Step 3</td>
<td>Add the Default Route, on page 33</td>
</tr>
<tr>
<td>Step 4</td>
<td>Configure NAT, on page 34</td>
</tr>
<tr>
<td>Step 5</td>
<td>Configure Access Control, on page 36</td>
</tr>
</tbody>
</table>
Step 6  Deploy the Configuration, on page 37

Configure Interfaces

Enable FTDv interfaces, assign them to security zones, and set the IP addresses. Typically, you must configure at least a minimum of two interfaces to have a system that passes meaningful traffic. Normally, you would have an outside interface that faces the upstream router or internet, and one or more inside interfaces for your organization’s networks. Some of these interfaces might be “demilitarized zones” (DMZs), where you place publically-accessible assets such as your web server.

A typical edge-routing situation is to obtain the outside interface address through DHCP from your ISP, while you define static addresses on the inside interfaces.

The following example configures a routed mode inside interface with a static address and a routed mode outside interface using DHCP.

Procedure

Step 1  Choose Devices > Device Management, and click the edit icon (Edit) for the device.

Step 2  Click Interfaces.

Step 3  Click the edit icon (Edit) for the interface that you want to use for inside.

The General tab appears.
Configure Interfaces

Edit Physical Interface

a) Enter a **Name** up to 48 characters in length. For example, name the interface *inside*.

b) Check the **Enabled** check box.

c) Leave the **Mode** set to *None*.

d) From the **Security Zone** drop-down list, choose an existing inside security zone or add a new one by clicking **New**.

For example, add a zone called *inside_zone*. Each interface must be assigned to a security zone and/or interface group. An interface can belong to only one security zone, but can also belong to multiple interface groups. You apply your security policy based on zones or groups. For example, you can assign the inside interface to the inside zone; and the outside interface to the outside zone. Then you can configure your access control policy to enable traffic to go from inside to outside, but not from outside to inside. Most policies only support security zones; you can use zones or interface groups in NAT policies, prefilter policies, and QoS policies.

e) Click the **IPv4** and/or **IPv6** tab.

- **IPv4**—Choose **Use Static IP** from the drop-down list, and enter an IP address and subnet mask in slash notation.

For example, enter **192.168.1.1/24**
• IPv6—Check the Autoconfiguration check box for stateless autoconfiguration.

f) Click OK.

**Step 4**

Click the edit icon (✎) for the interface that you want to use for outside.

The General tab appears.

![Edit Physical Interface](image)

- **Name**: Outside
- **Description**: None
- **Mode**: None
- **Security Zone**: Outside_zone
- **Interface ID**: GigabitEthernet0/0
- **MTU**: 1500 (64 - 9000)

a) Enter a Name up to 48 characters in length.

For example, name the interface outside.

b) Check the Enabled check box.
c) Leave the Mode set to None.
d) From the Security Zone drop-down list, choose an existing outside security zone or add a new one by clicking New.

For example, add a zone called outside_zone.
e) Click the IPv4 and/or IPv6 tab.

- **IPv4**—Choose Use DHCP, and configure the following optional parameters:
  - **Obtain default route using DHCP**—Obtains the default route from the DHCP server.
  - **DHCP route metric**—Assigns an administrative distance to the learned route, between 1 and 255. The default administrative distance for the learned routes is 1.
Configure The DHCP Server

Enable the DHCP server if you want clients to use DHCP to obtain IP addresses from the FTDv.

Procedure

Step 1  Choose Devices > Device Management, and click the edit icon ( ) for the device.
Step 2  Choose DHCP > DHCP Server.
Step 3  On the Server page, click Add, and configure the following options:

- **Interface**—Choose the interface from the drop-down list.
- **Address Pool**—Set the range of IP addresses from lowest to highest that are used by the DHCP server. The range of IP addresses must be on the same subnet as the selected interface and cannot include the IP address of the interface itself.
- **Enable DHCP Server**—Enable the DHCP server on the selected interface.

Step 4  Click OK.
Step 5  Click Save.
Add the Default Route

The default route normally points to the upstream router reachable from the outside interface. If you use DHCP for the outside interface, your device might have already received a default route. If you need to manually add the route, complete this procedure. If you received a default route from the DHCP server, it will show in the IPv4 Routes or IPv6 Routes table on the Devices > Device Management > Routing > Static Route page.

Procedure

Step 1  Choose Devices > Device Management, and click the edit icon (📝) for the device.
Step 2 Choose Routing > Static Route, click Add Route, and set the following:

- **Type**—Click the IPv4 or IPv6 radio button depending on the type of static route that you are adding.
- **Interface**—Choose the egress interface; typically the outside interface.
- **Available Network**—Choose any-ipv4 for an IPv4 default route, or any-ipv6 for an IPv6 default route.
- **Gateway** or IPv6 Gateway—Enter or choose the gateway router that is the next hop for this route. You can provide an IP address or a Networks/Hosts object.
- **Metric**—Enter the number of hops to the destination network. Valid values range from 1 to 255; the default value is 1.

Step 3 Click OK.

The route is added to the static route table.
### Configure NAT

A typical NAT rule converts internal addresses to a port on the outside interface IP address. This type of NAT rule is called *interface Port Address Translation (PAT)*.

**Procedure**

**Step 1** Choose **Devices > NAT**, and click **New Policy > Threat Defense NAT**.

**Step 2** Name the policy, select the device(s) that you want to use the policy, and click **Save**.

The policy is added the FMC. You still have to add rules to the policy.
**Step 3**  
Click **Add Rule**.  
The **Add NAT Rule** dialog box appears.

**Step 4**  
Configure the basic rule options:

- **NAT Rule**—Choose **Auto NAT Rule**.
- **Type**—Choose **Dynamic**.

**Step 5**  
On the **Interface Objects** page, add the outside zone from the **Available Interface Objects** area to the **Destination Interface Objects** area.

**Step 6**  
On the **Translation** page, configure the following options:

- **Original Source**—Click the add icon (zoek) to add a network object for all IPv4 traffic (0.0.0.0/0).
Configure Access Control

If you created a basic **Block all traffic** access control policy when you registered the FTDv with the FMC, then you need to add rules to the policy to allow traffic through the device. The following procedure adds a rule to allow traffic from the inside zone to the outside zone. If you have other zones, be sure to add rules allowing traffic to the appropriate networks.

See the FMC configuration guide to configure more advanced security settings and rules.

**Procedure**

**Step 1** Choose **Policy > Access Policy > Access Policy**, and click the edit icon (🔧) for the access control policy assigned to the FTD.

**Step 2** Click **Add Rule**, and set the following parameters:

**Step 7** Click **Save** to add the rule.

The rule is saved to the **Rules** table.

**Step 8** Click **Save** on the **NAT** page to save your changes.
• **Name**—Name this rule, for example, *inside_to_outside*.

• **Source Zones**—Select the inside zone from *Available Zones*, and click **Add to Source**.

• **Destination Zones**—Select the outside zone from *Available Zones*, and click **Add to Destination**.

Leave the other settings as is.

**Step 3**

Click **Add**.

The rule is added to the **Rules** table.

**Step 4**

Click **Save**.

---

**Deploy the Configuration**

Deploy the configuration changes to the FTDv; none of your changes are active on the device until you deploy them.

**Procedure**

**Step 1**

Click **Deploy** in the upper right.
Step 2  Select the device in the **Deploy Policies** dialog box, then click **Deploy**.

![Deploy Policies](image)

Step 3  Ensure that the deployment succeeds. Click the icon to the right of the **Deploy** button in the menu bar to see status for deployments.

![Deployment Status](image)

Access the Firepower Threat Defense CLI

You can use the FTDv CLI to change management interface parameters and for troubleshooting purposes. You can access the CLI using SSH to the Management interface, or by connecting from the VMware console.

**Procedure**

**Step 1**  (Option 1) SSH directly to the FTDv management interface IP address.

You set the management IP address when you deployed the virtual machine. Log into the FTDv with the **admin** account and the password you set during initial deployment.

**Step 2**  (Option 2) Open the VMware console and log in with the default username **admin** account and the password you set during initial deployment.
## History for Managing the Firepower Threat Defense Virtual with the Firepower Management

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC management</td>
<td>6.0</td>
<td>Initial support.</td>
</tr>
</tbody>
</table>
Managing the Firepower Threat Defense Virtual with the Firepower Device Manager

This chapter describes how to deploy a standalone FTDv device managed with FDM. To deploy a High Availability pair, see the FDM configuration guide.

- About Firepower Threat Defense Virtual with Firepower Device Manager, on page 41
- Initial Configuration, on page 42
- How to Configure the Device in Firepower Device Manager, on page 44

About Firepower Threat Defense Virtual with Firepower Device Manager

The Firepower Threat Defense Virtual (FTDv) is the virtualized component of the Cisco NGFW solution. The FTDv provides next-generation firewall services, including stateful firewalling, routing, VPN, Next-Generation Intrusion Prevention System (NGIPS), Application Visibility and Control (AVC), URL filtering, and Advanced Malware Protection (AMP).

You can manage the FTDv using the Firepower Device Manager (FDM), a web-based device setup wizard included on some Firepower Threat Defense models. FDM lets you configure the basic features of the software that are most commonly used for small networks. It is especially designed for networks that include a single device or just a few, where you do not want to use a high-powered multiple-device manager to control a large network containing many Firepower Threat Defense devices.

If you are managing large numbers of devices, or if you want to use the more complex features and configurations that Firepower Threat Defense allows, use the Firepower Management Center to configure your devices instead of the integrated Firepower Device Manager. See Managing the Firepower Threat Defense Virtual with the Firepower Management Center, on page 25 for more information.

For troubleshooting purposes, you can access the FTD CLI using SSH on the Management interface, or you can connect to the FTD from the Firepower CLI.

Default Configuration

The FTDv default configuration puts the management interface and inside interface on the same subnet. You must have Internet connectivity on the management interface in order to use Smart Licensing and to obtain updates to system databases.
Thus, the default configuration is designed so that you can connect both the Management0-0 and GigabitEthernet0-1 (inside) to the same network on the virtual switch. The default management address uses the inside IP address as the gateway. Thus, the management interface routes through the inside interface, then through the outside interface, to get to the Internet.

You also have the option of attaching Management0-0 to a different subnet than the one used for the inside interface, as long as you use a network that has access to the Internet. Ensure that you configure the management interface IP address and gateway appropriately for the network.

The FTDv must be powered up on firstboot with at least four interfaces:

- The first interface on the virtual machine is the management interface (Management0-0).
- The second interface on the virtual machine is the diagnostic interface (Diagnostic0-0).
- The third interface on the virtual machine (GigabitEthernet0-0) is the outside interface.
- The fourth interface on the virtual machine (GigabitEthernet0-1) is the inside interface.

You can add up to six more interfaces for data traffic, for a total of eight data interfaces. For additional data interfaces, make sure that the Source Networks map to the correct Destination Networks, and that each data interface maps to a unique subnet or VLAN. See Configuring VMware Interfaces.

Initial Configuration

You must complete an initial configuration to have the FTDv function correctly in your network, which includes configuring the addresses needed to insert the security appliance into your network and connect it to the Internet or other upstream router. You can do the initial configuration of the system in one of two ways:

- Using the FDM web interface (recommended). FDM runs in your web browser. You use this interface to configure, manage, and monitor the system.
- Using the Command Line Interface (CLI) setup wizard (optional). You can use the CLI setup wizard for initial configuration instead of FDM, and you can use the CLI for troubleshooting. You still use FDM to configure, manage, and monitor the system; see (Optional) Launch the Firepower Threat Defense CLI Wizard.

The following topics explain how to use these interfaces to do the initial configuration of your system.

Launch Firepower Device Manager

When you initially log into Firepower Device Manager (FDM), you are taken through the device setup wizard to complete the initial system configuration.

Procedure

Step 1

Open a browser and log into FDM. Assuming you did not go through initial configuration in the CLI, open Firepower Device Manager at https://ip-address, where the address is one of the following:

- If you are connected to an inside bridge group interface: https://192.168.1.1.
- If you are connected to the Management physical interface: https://192.168.45.45.
Step 2  Log in with the username admin, password Admin123.

Step 3  If this is the first time logging into the system, and you did not use the CLI setup wizard, you are prompted to read and accept the End User License Agreement and change the admin password. You must complete these steps to continue.

Step 4  Configure the following options for the outside and management interfaces and click Next.

Note  Your settings are deployed to the device when you click Next. The interface will be named “outside” and it will be added to the “outside_zone” security zone. Ensure that your settings are correct.

a)  **Outside Interface**—This is the data port that you connected to your gateway mode or router. You cannot select an alternative outside interface during initial device setup. The first data interface is the default outside interface.

    **Configure IPv4**—The IPv4 address for the outside interface. You can use DHCP or manually enter a static IP address, subnet mask, and gateway. You can also select Off to not configure an IPv4 address.

    **Configure IPv6**—The IPv6 address for the outside interface. You can use DHCP or manually enter a static IP address, prefix, and gateway. You can also select Off to not configure an IPv6 address.

b)  **Management Interface**

    **DNS Servers**—The DNS server for the system's management address. Enter one or more addresses of DNS servers for name resolution. The default is the OpenDNS public DNS servers. If you edit the fields and want to return to the default, click Use OpenDNS to reload the appropriate IP addresses into the fields.

    **Firewall Hostname**—The hostname for the system's management address.

    Note  When you configure the Firepower Threat Defense device using the device setup wizard, the system provides two default access rules for outbound and inbound traffic. You can go back and edit these access rules after initial setup.

Step 5  Configure the system time settings and click Next.

a)  **Time Zone**—Select the time zone for the system.

b)  **NTP Time Server**—Select whether to use the default NTP servers or to manually enter the addresses of your NTP servers. You can add multiple servers to provide backups.

Step 6  Configure the smart licenses for the system.

You must have a smart license account to obtain and apply the licenses that the system requires. Initially, you can use the 90-day evaluation license and set up smart licensing later.

To register the device now, click the link to log into your Smart Software Manager account, generate a new token, and copy the token into the edit box.

To use the evaluation license, select **Start 90 day evaluation period without registration**. To later register the device and obtain smart licenses, click the name of the device in the menu to get to the Device Dashboard, then click the link in the Smart Licenses group.

Step 7  Click Finish.

**What to do next**

- Configure the device using Firepower Device Manager; see How to Configure the Device in Firepower Device Manager, on page 44.
How to Configure the Device in Firepower Device Manager

After you complete the setup wizard, you should have a functioning device with a few basic policies in place:

• Security zones for the inside and outside interfaces.
• An access rule trusting all inside to outside traffic.
• An interface NAT rule that translates all inside to outside traffic to unique ports on the IP address of the outside interface.
• A DHCP server running on the inside interface or bridge group.

The following steps provide an overview of additional features you might want to configure. Please click the help button (?) on a page to get detailed information about each step.

Procedure

Step 1
Choose Device, then click View Configuration in the Smart License group.
Click Enable for each of the optional licenses you want to use: Threat, Malware, URL. If you registered the device during setup, you can also enable the RA VPN license desired. Read the explanation of each license if you are unsure of whether you need it.
If you have not registered, you can do so from this page. Click Request Register and follow the instructions. Please register before the evaluation license expires.
For example, an enabled Threat license should look like the following:

Figure 2: Enabled Threat License

Step 2
If you configured other interfaces, choose Device, then click View Configuration in the Interfaces group and configure each interface.
You can create a bridge group for the other interfaces, or configure separate networks, or some combination of both. Click the edit icon (✍️) for each interface to define the IP address and other settings.
The following example configures an interface to be used as a “demilitarized zone” (DMZ), where you place publically-accessible assets such as your web server. Click Save when you are finished.
Step 3

If you configured new interfaces, choose **Objects**, then select **Security Zones** from the table of contents. Edit or create new zones as appropriate. Each interface must belong to a zone, because you configure policies based on security zones, not interfaces. You cannot put the interfaces in zones when configuring them, so you must always edit the zone objects after creating new interfaces or changing the purpose of existing interfaces.

The following example shows how to create a new dmz-zone for the dmz interface.
Step 4  If you want internal clients to use DHCP to obtain an IP address from the device, choose Device > System Settings > DHCP Server, then select the DHCP Servers tab.

There is already a DHCP server configured for the inside interface, but you can edit the address pool or even delete it. If you configured other inside interfaces, it is very typical to set up a DHCP server on those interfaces. Click + to configure the server and address pool for each inside interface.

You can also fine-tune the WINS and DNS list supplied to clients on the Configuration tab. The following example shows how to set up a DHCP server on the inside2 interface with the address pool 192.168.4.50-192.168.4.240.

Figure 5: DHCP Server

Add Server

Enabled DHCP Server

Interface
inside2

Address Pool
192.168.4.50-192.168.4.240

e.g. 192.168.45.46-192.168.45.254

Step 5  Choose Device, then click View Configuration (or Create First Static Route) in the Routing group and configure a default route.

The default route normally points to the upstream or ISP router that resides off the outside interface. A default IPv4 route is for any-ipv4 (0.0.0.0/0), whereas a default IPv6 route is for any-ipv6 (:0/0). Create routes for each IP version you use. If you use DHCP to obtain an address for the outside interface, you might already have the default routes that you need.

Note  The routes you define on this page are for the data interfaces only. They do not impact the management interface. Set the management gateway on Device > System Settings > Management Interface.

The following example shows a default route for IPv4. In this example, isp-gateway is a network object that identifies the IP address of the ISP gateway (you must obtain the address from your ISP). You can create this object by clicking Create New Network at the bottom of the Gateway drop-down list.
Step 6 Choose Policies and configure the security policies for the network.

The device setup wizard enables traffic flow between the inside-zone and outside-zone, and interface NAT for all interfaces when going to the outside interface. Even if you configure new interfaces, if you add them to the inside-zone object, the access control rule automatically applies to them.

However, if you have multiple inside interfaces, you need an access control rule to allow traffic flow from inside-zone to inside-zone. If you add other security zones, you need rules to allow traffic to and from those zones. These would be your minimum changes.

In addition, you can configure other policies to provide additional services, and fine-tune NAT and access rules to get the results that your organization requires. You can configure the following policies:

- **SSL Decryption**—If you want to inspect encrypted connections (such as HTTPS) for intrusions, malware, and so forth, you must decrypt the connections. Use the SSL decryption policy to determine which connections need to be decrypted. The system re-encrypts the connection after inspecting it.

- **Identity**—If you want to correlate network activity to individual users, or control network access based on user or user group membership, use the identity policy to determine the user associated with a given source IP address.

- **Security Intelligence**—Use the Security Intelligence policy to quickly drop connections from or to blacklisted IP addresses or URLs. By blacklisting known bad sites, you do not need to account for them in your access control policy. Cisco provides regularly updated feeds of known bad addresses and URLs so that the Security Intelligence blacklist updates dynamically. Using feeds, you do not need to edit the policy to add or remove items in the blacklist.

- **NAT (Network Address Translation)**—Use the NAT policy to convert internal IP addresses to externally routeable addresses.
• **Access Control**—Use the access control policy to determine which connections are allowed on the network. You can filter by security zone, IP address, protocol, port, application, URL, user or user group. You also apply intrusion and file (malware) policies using access control rules. Use this policy to implement URL filtering.

• **Intrusion**—Use the intrusion policies to inspect for known threats. Although you apply intrusion policies using access control rules, you can edit the intrusion policies to selectively enable or disable specific intrusion rules.

The following example shows how to allow traffic between the inside-zone and dmz-zone in the access control policy. In this example, no options are set on any of the other tabs except for **Logging**, where **At End of Connection** is selected.

*Figure 7: Access Control Policy*

**Step 7** Choose **Device**, then click **View Configuration** in the **Updates** group and configure the update schedules for the system databases.

If you are using intrusion policies, set up regular updates for the Rules and VDB databases. If you use Security Intelligence feeds, set an update schedule for them. If you use geolocation in any security policies as matching criteria, set an update schedule for that database.

**Step 8** Click the **Deploy** button in the menu, then click the Deploy Now button ( ), to deploy your changes to the device.

Changes are not active on the device until you deploy them.

---

**What to do next**

For more information about managing the Firepower Threat Defense Virtual with the Firepower Device Manager, see the *Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager*, or the Firepower Device Manager online help.
Performance Tuning for VMware—Best Practices for the Firepower Threat Defense Virtual

The Firepower Threat Defense Virtual is a high-performance appliance but may require tuning of the hypervisor to achieve the best results.

This chapter describes some best practices and recommendations for facilitating the best performance of the Firepower Threat Defense Virtual in a VMware vSphere environment.

For the best performance, ESXi 6.0.0.0 or later is recommended.

**Note**

- SR-IOV Interface Provisioning, on page 49

**SR-IOV Interface Provisioning**

Single Root I/O Virtualization (SR-IOV) allows multiple VMs running a variety of guest operating systems to share a single PCIe network adapter within a host server. SR-IOV allows a VM to move data directly to and from the network adapter, bypassing the hypervisor for increased network throughput and lower server CPU burden. Recent x86 server processors include chipset enhancements, such as Intel VT-d technology, that facilitate direct memory transfers and other operations required by SR-IOV.

The SR-IOV specification defines two device types:

- **Physical Function (PF)**—Essentially a static NIC, a PF is a full PCIe device that includes SR-IOV capabilities. PFs are discovered, managed, and configured as normal PCIe devices. A single PF can provide management and configuration for a set of virtual functions (VFs).

- **Virtual Function (VF)**—Similar to a dynamic vNIC, a VF is a full or lightweight virtual PCIe device that provides at least the necessary resources for data movements. A VF is not managed directly but is derived from and managed through a PF. One or more VFs can be assigned to a VM.

VFs are capable of providing up to 10 Gbps connectivity to Firepower Threat Defense Virtual virtual machines within a virtualized operating system framework. This section explains how to configure VFs in a VMware environment.
Best Practices for SR-IOV Interfaces

Guidelines for SR-IOV Interfaces

VMware vSphere 5.1 and later releases support SR-IOV in an environment with specific configurations only. Some features of vSphere are not functional when SR-IOV is enabled.

In addition to the System Requirements for the Firepower Threat Defense Virtual and SR-IOV, you should review the Supported Configurations for Using SR-IOV in the VMware documentation for more information about requirements, supported NICs, availability of features, and upgrade requirements for VMware and SR-IOV.

This section shows various setup and configuration steps for provisioning SR-IOV interfaces on a VMware system. The information in this section was created from devices in a specific lab environment, using VMware ESXi 6.0 and vSphere Web Client, a Cisco UCS C Series server, and an Intel Ethernet Server Adapter X520 - DA2.

Limitations for SR-IOV Interfaces

When the Firepower Threat Defense Virtual is booted, be aware that SR-IOV interfaces can show up in reverse order when compared to the order presented in ESXi. This could cause interface configuration errors that result in a lack of network connectivity for a particular FTDv virtual machine.

\[Caution\]

It is important that you verify the interface mapping before you begin configuring the SR-IOV network interfaces on the FTDv. This ensures that the network interface configuration will apply to the correct physical MAC address interface on the VM host.

After the FTDv boots, you can confirm which MAC address maps to which interface. Use the `show interface` command to see detailed interface information, including the MAC address for an interface. Compare the MAC address to the results of the `show kernel ifconfig` command to confirm the correct interface assignment.

Check the ESXi Host BIOS

Before you begin

To deploy the FTDv with SR-IOV interfaces on VMware, virtualization needs to be supported and enabled. VMware provides several methods of verifying virtualization support, including their online Compatibility Guide for SR-IOV support as well as a downloadable CPU identification utility that detects whether virtualization is enabled or disabled.

You can also determine if virtualization is enabled in the BIOS by logging into the ESXi host.

Procedure

Step 1

Log in to the ESXi Shell using one of the following methods:

- If you have direct access to the host, press Alt+F2 to open the login page on the machine’s physical console.
• If you are connecting to the host remotely, use SSH or another remote console connection to start a session on the host.

Step 2
Enter a user name and password recognized by the host.

Step 3
Run the following command:

Example:
esxcfg-info|grep "\----\HV Support"

The output of the HV Support command indicates the type of hypervisor support available. These are the descriptions for the possible values:

0 - VT/AMD-V indicates that support is not available for this hardware.
1 - VT/AMD-V indicates that VT or AMD-V might be available but it is not supported for this hardware.
2 - VT/AMD-V indicates that VT or AMD-V is available but is currently not enabled in the BIOS.
3 - VT/AMD-V indicates that VT or AMD-V is enabled in the BIOS and can be used.

Example:

~ # esxcfg-info|grep "\----\HV Support"
|----HV Support...........................3

The value 3 indicates the virtualization is supported and enabled.

What to do next
• Enable SR-IOV on the host physical adapter.

Enable SR-IOV on the Host Physical Adapter

Before you can connect virtual machines to virtual functions, use the vSphere Web Client to enable SR-IOV and set the number of virtual functions on your host.

Before you begin
• Make sure you have an SR-IOV-compatible network interface card (NIC) installed; see System Requirements, on page 4.

Procedure

Step 1
In the vSphere Web Client, navigate to the ESXi host where you want to enable SR-IOV.

Step 2
On the Manage tab, click Networking and choose Physical adapters.

You can look at the SR-IOV property to see whether a physical adapter supports SR-IOV.

Step 3
Select the physical adapter and click Edit adapter settings.

Step 4
Under SR-IOV, select Enabled from the Status drop-down menu.

Step 5
In the Number of virtual functions text box, type the number of virtual functions that you want to configure for the adapter.
We recommend that you **DO NOT** use more than 1 VF per interface. Performance degradation is likely to occur if you share the physical interface with multiple virtual functions.

**Step 6**  Click OK.

**Step 7**  Restart the ESXi host.

The virtual functions become active on the NIC port represented by the physical adapter entry. They appear in the PCI Devices list in the **Settings** tab for the host.

---

**What to do next**

- Create a standard vSwitch to manage the SR-IOV functions and configurations.

### Create a vSphere Switch

Create a vSphere switch to manage the SR-IOV interfaces.

**Procedure**

1. **Step 1**  In the vSphere Web Client, navigate to the ESXi host.
2. **Step 2**  Under **Manage** select **Networking**, and then select **Virtual switches**.
3. **Step 3**  Click the **Add host networking** icon, which is the green globe icon with the plus (+) sign.
4. **Step 4**  Select a **Virtual Machine Port Group for a Standard Switch** connection type and click **Next**.
5. **Step 5**  Choose **New standard switch** and click **Next**.
6. **Step 6**  Add physical network adapters to the new standard switch.
   - Under **Assigned adapters**, click the green plus (+) sign to **Add adapters**.
   - Select the corresponding network interface for SR-IOV from the list. For example, Intel(R) 82599 10 Gigabit Dual Port Network Connection.
   - Select from the **Failover order group** drop-down menu, select from the **Active adapters**.
   - Click **OK**.
7. **Step 7**  Enter a **Network label** for the SR-IOV vSwitch and click **Next**.
8. **Step 8**  Review your selections on the **Ready to complete** page, then click **Finish**.
Upgrade of the Compatibility Level for Virtual Machines

The compatibility level determines the virtual hardware available to the virtual machine, which corresponds to the physical hardware available on the host machine. The FTDv VM needs to be at Hardware Level 10 or higher. This will expose the SR-IOV passthrough feature to the FTDv. This procedure upgrades the FTDv to the latest supported virtual hardware version immediately.

For information about virtual machine hardware versions and compatibility, see the vSphere Virtual Machine Administration documentation.

Procedure

**Step 1** Log in to the vCenter Server from the vSphere Web Client.

**Step 2** Locate the FTDv virtual machine you wish to modify.
   a) Select a datacenter, folder, cluster, resource pool, or host and click the Related Objects tab.
   b) Click Virtual Machines and select the FTDv virtual machine from the list.

What to do next

- Review the compatibility level of your virtual machine.
Step 3  Power off the selected virtual machine.
Step 4  Right-click on the FTDv and select Actions > All vCenter Actions > Compatibility > Upgrade VM Compatibility.
Step 5  Click Yes to confirm the upgrade.
Step 6  Choose the ESXi 5.5 and later option for the virtual machines compatibility.
Step 7  (Optional) Select Only upgrade after normal guest OS shutdown.

The selected virtual machine is upgraded to the corresponding hardware version for the Compatibility setting that you chose, and the new hardware version is updated in the Summary tab of the virtual machine.

What to do next

• Associate the FTDv with a virtual function through an SR-IOV passthrough network adapter.

Assign the SR-IOV NIC to the Firepower Threat Defense Virtual

To ensure that the FTDv virtual machine and the physical NIC can exchange data, you must associate the FTDv with one or more virtual functions as SR-IOV passthrough network adapters. The following procedure explains how to assign the SR-IOV NIC to the FTDv virtual machine using the vSphere Web Client.

Procedure

Step 1  Log in to the vCenter Server from the vSphere Web Client.
Step 2  Locate the FTDv virtual machine you wish to modify.
  a) Select a datacenter, folder, cluster, resource pool, or host and click the Related Objects tab.
  b) Click Virtual Machines and select the FTDv virtual machine from the list.
Step 3  On the Manage tab of the virtual machine, select Settings > VM Hardware.
Step 4  Click Edit and choose the Virtual Hardware tab.
Step 5  From the New device drop-down menu, select Network and click Add.

A New Network interface appears.

Step 6  Expand the New Network section and select an available SRIOV option.
Step 7  From the Adapter Type drop-down menu, select SR-IOV passthrough.
Step 8  From the Physical function drop-down menu, select the physical adapter that corresponds to the passthrough virtual machine adapter.
Step 9  Power on the virtual machine.

When you power on the virtual machine, the ESXi host selects a free virtual function from the physical adapter and maps it to the SR-IOV passthrough adapter. The host validates all properties of the virtual machine adapter and the underlying virtual function.