

Deploy the Firewall Threat Defense Virtual Unlimited

- Overview, on page 1
- Licensing, on page 1
- Deploy the Firewall Threat Defense Virtual Unlimited on KVM, on page 2
- Deploy the Firewall Threat Defense Virtual Unlimited on VMware, on page 8

Overview

From Secure Firewall version 10.0, Firewall Threat Defense Virtual supports a new performance tier license - Firewall Threat Defense Virtual Unlimited (FTDvU). FTDvU supports up to 64 vCPUs.

From version 10.0, you can use the FTDvU license for Firewall Threat Defense Virtual deployments on KVM and VMware.

Licensing

Firewall Threat Defense Virtual supports performance-tier licensing. From Version 10.0, a new performance tier license Firewall Threat Defense Virtual Unlimited (FTDvU) is introduced. FTDvU supports deployments with up to 64 vCPUs and 128 GB memory.

For more information about licensing and performance tiers, see the Licenses chapter in the Cisco Secure Firewall Management Center Administration Guide.

Table 1: Firewall Threat Defense Virtual Unlimited License Entitlements

Performance Tier	Device Specifications (vCPU/RAM)	RA VPN Session Limit	Supported platforms
FTDv - Unlimited (FTDvU)	32 vCPU/64 GB	20,000	KVM, VMware
FTDv - Unlimited (FTDvU)	64 vCPU/128 GB	32,000	KVM, VMware

Deploy the Firewall Threat Defense Virtual Unlimited on KVM

From Secure Firewall version 10.0, you can deploy Firewall Threat Defense Virtual Unlimited (FTDvU) on KVM.

Prerequisites

Hardware Requirements

- Cisco UCS M7, M8 servers, or later.
- x86-based processors (64 cores per socket or higher recommended).
- 100 Gigabit Ethernet NICs - Intel E810 series or NVIDIA/Mellanox ConnectX-6 card.

CPU Requirements

32/64 vCPUs

Memory (RAM)

Minimum of 64 GB RAM for FTDvU 32-core deployments

Minimum of 128 GB RAM for FTDvU 64-core deployments

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

For more details on generic system requirements, supported platforms, and hardware guidelines, see the System Requirements section in the Deploy the Firewall Threat Defense Virtual on KVM chapter.

Guidelines and Limitations

Ensure that you read the generic guidelines and limitations for deploying Firewall Threat Defense Virtual on KVM.

NUMA Optimization Guidelines for ASAvU

- Always enforce Single-NUMA placement. Cross-socket memory access introduces significant latency and throughput penalties.
- Ensure all vCPUs are pinned to a single physical NUMA node. Avoid vCPU/memory pinning across NUMA boundaries to maintain strict memory locality.

Prepare the Day-0 Configuration File

To prepare the Day-0 configuration file used during deployment, see the Prepare the Day-0 Configuration File section in the Deploy the Firewall Threat Defense Virtual on KVM chapter.

Deploy the Firewall Threat Defense Virtual Unlimited using a Deployment Script

Use a virt-install based deployment script to launch the Firewall Threat Defense Virtual Unlimited.

Be aware that you can optimize performance by selecting the best guest caching mode for your environment. The cache mode in use will affect whether data loss occurs, and the cache mode can also affect disk performance.

Each KVM guest disk interface can have one of the following cache modes specified: *writethrough*, *writeback*, *none*, *directsync*, or *unsafe*. *writethrough* provides read caching. *writeback* provides read and write caching. *directsync* bypasses the host page cache. *unsafe* may cache all content and ignore flush requests from the guest.

- A *cache=writethrough* will help reduce file corruption on KVM guest machines when the host experiences abrupt losses of power. We recommend that you use *writethrough* mode.
- However, *cache=writethrough* can also affect disk performance due to more disk I/O writes than *cache=none*.
- If you remove the cache parameter on the *--disk* option, the default is *writethrough*.
- Not specifying a cache option may also significantly reduce the time required for the VM creation. This is due to the fact that some older RAID controllers have poor disk caching capability. Hence, disabling disk caching (*cache=none*) and thus defaulting to *writethrough*, helps ensure data integrity.
- Starting with version 6.4, the Firewall Threat Defense Virtual deploys with adjustable vCPU and memory resources. Prior to version 6.4, the Firewall Threat Defense Virtual deployed as a fixed configuration 4vCPU/8GB device. See the following table for supported values for the --vcpus and --ram parameters for each Firewall Threat Defense Virtual platform size.

Table 2: Supported vCPU and Memory Parameters for virt-install

--vcpus	--ram	Firewall Threat Defense Virtual Unlimited Platform Size
32	65536 (64 GB)	32 vCPU/ 64 GB (FTDv Unlimited)
64	131072 (128 GB)	64 vCPU / 128 GB (FTDv Unlimited)

Procedure

Step 1 Create a virt-install script called “virt_install_ftdv.sh”.

The name of the Firewall Threat Defense Virtual VM must be unique across all other virtual machines (VMs) on this KVM host. The Firewall Threat Defense Virtual can support up to 10 network interfaces. This example uses four interfaces. The virtual NIC must be VirtIO.

For Version 10.0 and later, the diagnostic interface is optional. The Firewall Threat Defense Virtual can be configured with minimum three interfaces when the diagnostic interface is disabled (one management and two data interfaces). If the diagnostic interface is enabled, a minimum of four interfaces is required (one management interface, one diagnostic interface and two data interfaces).

For more information about the diagnostic interface removal starting in Firewall Threat Defense Virtual version 10.0, see the Diagnostic Interface Removal section.

The default configuration for the Firewall Threat Defense Virtual assumes that you put the management interface, diagnostic interface, and inside interface on the same subnet. The interface-to-network assignments must be ordered as follows:

- Diagnostic:ON
  - (1) Management interface (required)
  - (2) Reserved for internal use (required)
  - (3) Outside interface (required)
  - (4) Inside interface (required)
  - (5-10) Data interfaces — 3 required, up to 3 additional interfaces allowed (total of 6 data interfaces)
- Diagnostic:OFF
  - (1) Management interface (required)
  - (2) Outside interface (required)
  - (3) Inside interface (required)
  - (4-10) Data interfaces — 3 required, up to 4 additional interfaces allowed (total of 7 data interfaces)

For Secure Boot Configuration: Use *virt-install* command with specific parameters.

```
virt-install \
  --connect=qemu:///system \
  --network bridge:br1556,model=virtio\
  --network bridge:br-in,model=virtio\
  --network bridge:br-out,model=virtio\
  --name=<prefix>-vm-ftdv \
  --cpu host \
  --arch=x86_64 \
  --vcpus=32 \
  --ram=65536 \
  --os-type=linux \
  --os-variant=generic \
  --virt-type=kvm \
  --import \
  --watchdog i6300esb,action=reset \
  --disk path=<path to qcow2 file>,format=qcow2,device=disk,bus=virtio,cache=none \
  --disk path=<path to day0.iso file>,format=iso,device=cdrom,bus=sata \
  --console pty,target_type=serial \
  --serial tcp,host=127.0.0.1:<port>,mode=bind,protocol=telnet \
  --boot firmware=efi,loader_secure=yes \
  --machine q35 \
  --features smm.state=on \
  --force
```

Note Machine type must be q35 and SMM (System Management Mode) must be ON for Secure Boot.

VM Management:

Note To delete a VM, use the following command:

```
virsh undefine <vm-name> --nvram
```

Step 2 Run the virt_install script:

Note Inline traffic is not supported, as promiscuous mode can not be enabled for the SRIOV interfaces.

Example:

```
/usr/bin/virt_install_ftdv.sh

Starting install...
Creating domain...
```

A window appears displaying the console of the VM. You can see that the VM is booting. It takes a few minutes for the VM to boot. Once the VM stops booting, you can issue CLI commands from the console screen.

Important During registration of Firewall Threat Defense Virtual to the Management Center, select the **FTDvU - Unlimited** performance tier from the drop-down list to apply the FTDvU license tier.

Launch Using a Graphical User Interface (GUI)

There are a several open-source options available to manage KVM virtual machines using a GUI. The following procedure uses virt-manager, also known as Virtual Machine Manager, to launch the Firewall Threat Defense Virtual. virt-manager is a graphical tool for creating and managing guest virtual machines.

Note KVM can emulate a number of different CPU types. For your VM, you typically should select a processor type which closely matches the CPU of the host system, as it means that the host CPU features (also called CPU flags) will be available in your VMs. You should set the CPU type to **host** in which case the VM will have exactly the same CPU flags as your host system.

Procedure

Step 1 Start virt-manager **(Applications** > **System Tools** > **Virtual Machine Manager**).

You may be asked to select the hypervisor and/or enter your root password.

Step 2 Click the button in the top left corner to open the **New VM** wizard.

Step 3 Enter the virtual machine details:

a) For the operating system, select **Import existing disk image**.

This method allows you to import a disk image (containing a pre-installed, bootable operating system) to it.

b) Click **Forward** to continue.

Step 4 Load the disk image:

a) Click **Browse...** to select the image file.
b) Choose *Generic* for the **OS type**.
c) Click **Forward** to continue.

Step 5 Configure the memory and CPU options:



Important The Firewall Threat Defense Virtual supports performance-tiered licensing that provides different throughput levels and VPN connection limits based on deployment requirements.

See the following table for supported performance tiers and values for the --vcpus and --ram parameters for each Firewall Threat Defense Virtual platform.

Table 3: Supported vCPU and Memory Parameters for Virtual Machine Manager

CPUs	Firewall Threat Defense Virtual Platform Size
32	32 vCPU / 64 GB (FTDv Unlimited)
64	64 vCPU / 128 GB (FTDv Unlimited)

a) Set the **Memory (RAM)** parameter for your Firewall Threat Defense Virtual platform size.
b) Set the corresponding **CPUs** parameter for the Firewall Threat Defense Virtual platform size.
c) Click **Forward** to continue.

Step 6 Check the **Customize configuration before install** box, specify a **Name**, then click **Finish**.

Doing so opens another wizard that allows you to add, remove, and configure the virtual machine's hardware settings.

Step 7 Modify the CPU configuration:

From the left panel, select **Processor**, then select **Configuration** > **Copy host CPU configuration**.

This applies the physical host's CPU model and configuration to your VM.

Step 8 Configure the Virtual Disk:

a) From the left panel, select **Disk 1**.
b) Select **Advanced options**.
c) Set the **Disk bus** to *Virtio*.
d) Set the **Storage format** to *qcow2*.

Step 9 Configure a serial console:

a) From the left panel, select **Console**.
b) Select **Remove** to remove the default console.
c) Click **Add Hardware** to add a serial device.
d) For **Device Type**, select *TCP net console (tcp)*.
e) For **Mode**, select *Server mode (bind)*.

f) For **Host**, enter **0.0.0.0** for the IP address, then enter a unique **Port** number.
g) Check the **Use Telnet** box.
h) Configure device parameters.

Step 10 Configure a watchdog device to automatically trigger some action when the KVM guest hangs or crashes:

a) Click **Add Hardware** to add a watchdog device.
b) For **Model**, select *default*.
c) For **Action**, select *Forcefully reset the guest*.

Step 11 Configure virtual network interfaces.

Click **Add Hardware** to add an interface, then choose **macvtap** or specify a shared device name (use a bridge name).

For Version 10.0 and later, the diagnostic interface is optional. The Firewall Threat Defense Virtual can be configured with minimum three interfaces when the diagnostic interface is disabled (one management and two data interfaces). If the diagnostic interface is enabled, a minimum of four interfaces is required (one management interface, one diagnostic interface and two data interfaces).

For more information about the diagnostic interface removal starting in Firewall Threat Defense Virtual version 10.0, see the Diagnostic Interface Removal section.

- Diagnostic:ON
  - vnic0—Management interface (required)
  - vnic1—Reserved for internal use (required)
  - vnic2— Outside interface (required)
  - vnic3—Inside interface (required)
  - vnic4-vnic9—Data interfaces (optional)

  Make sure vnic0 and vnic3 are mapped to the same subnet.

- Diagnostic:OFF
  - vnic0—Management interface (required)
  - vnic1—Outside interface (required)
  - vnic2—Inside interface (required)
  - vnic3-vnic9—Data interfaces (optional)

  Make sure vnic0 and vnic2 are mapped to the same subnet.

Step 12 If deploying using a Day 0 configuration file, create a virtual CD-ROM for the ISO:

a) Click **Add Hardware**.
b) Select **Storage**.
c) Click **Select managed or other existing storage** and browse to the location of the ISO file.
d) For **Device type**, select *IDE CDROM*.

Step 13 After configuring the virtual machine's hardware, click **Apply**.

Step 14 Click **Begin installation** for virt-manager to create the virtual machine with your specified hardware settings.

Note When launching the Threat Defense Virtual in virt-manager, a graphical (SPICE) console opens by default. On some systems, this console may appear frozen or show only partial output during boot. However, the device continues to boot normally in the background.

To view the full console output, go to:

`View → Consoles → Console or Serial`

If a TCP serial console is configured, use telnet to access the console instead — output will not appear in virt-manager.

Important During registration of Firewall Threat Defense Virtual to the Management Center, select the **Threat Defense Virtual Unlimited** performance tier from the drop-down list to apply the FTDvU license tier.

Deploy the Firewall Threat Defense Virtual Unlimited on VMware

From Secure Firewall version 10.0, you can deploy Firewall Threat Defense Virtual Unlimited (FTDvU) on a VMware vSphere environment using vSphere vCenter.

Prerequisites

Hardware Requirements

- Cisco UCS M7, M8 servers, or later.
- x86-based processors (64 cores per socket or higher recommended).
- 100 Gigabit Ethernet NICs - Intel E810 series or NVIDIA/Mellanox ConnectX-6 card.

CPU Requirements

32/64 vCPUs

Memory (RAM)

Minimum of 64 GB RAM for ASAvU 32-vCPU deployments

Minimum of 128 GB RAM for FTDvU 64-core deployments

For detailed system requirements, supported platforms, and hardware guidelines, see the System Requirements section in the Deploy the Firewall Threat Defense Virtual on VMware chapter.

Guidelines and Limitations

Ensure that you read the generic guidelines and limitations for deploying Firewall Threat Defense Virtual on VMware.

NUMA Optimization Guidelines for FTDvU

- Always enforce Single-NUMA placement. Cross-socket memory access introduces significant latency and throughput penalties.
- Set "numa.autosize.vcpu.maxPerVirtualNode" to ≤ physical cores per socket. Exceeding this value forces the hypervisor to span sockets, degrading performance.

Deploy the Firewall Threat Defense Virtual Unlimited to vSphere vCenter

Use this procedure to deploy the Firewall Threat Defense Virtual Unlimited appliance to VMware vSphere vCenter. You can use the VMware Web Client (or vSphere Client) to deploy and configure the Firewall Threat Defense Virtual machines.

Before you begin

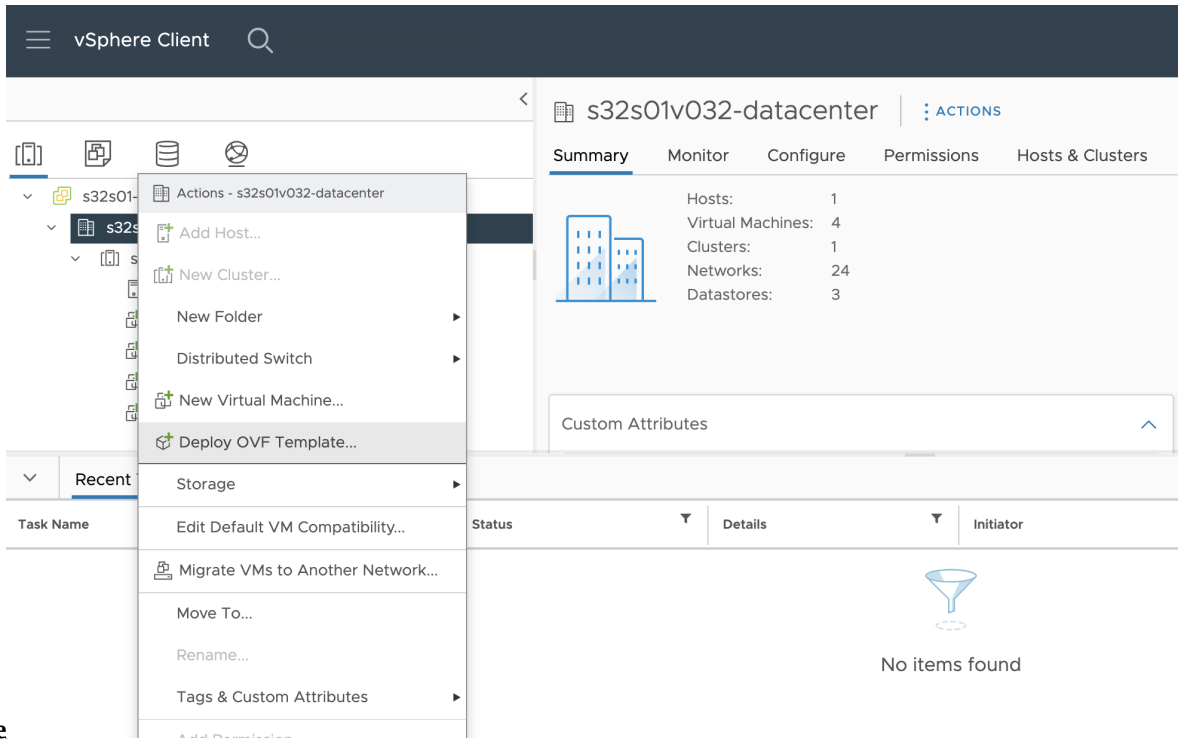
- You must have at least one network configured in vSphere (for management) before you deploy the Firewall Threat Defense Virtual Unlimited.

Procedure

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

Step 2 Download the OVF template file from this link.

Step 3 Using the vSphere Web Client (or the vSphere Client), deploy the OVF template file you downloaded earlier by clicking **File** > **Deploy OVF Template**.



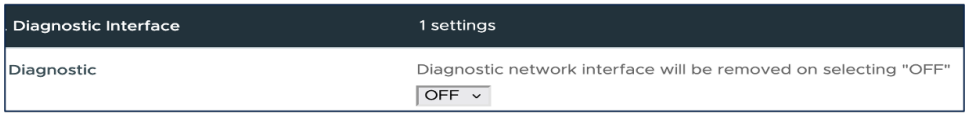
The Deploy OVF Template wizard appears.

Note For Version 10.0, in a VMware OVF template, the network interfaces are typically mapped in a static NetAdaptor.

When deploying a Threat Defense Virtual, the diagnostic interface is optional.

If the **Diagnostic** is selected as ON, then there is no change in the network interface mapping.

If the **Diagnostic** is selected as OFF, it results in a shift of network adapter assignments.



The removal of the diagnostic interface shifts the mapping of each subsequent ethernet interface down by one position and the network adapters are reassigned as follows:

Table 4: Network Interface Mapping

Diagnostic: ON	Diagnostic: OFF
Management0-0 > Management	Management0-0 -> Management
Diagnostic ------- > Diagnostic	Diagnostic ------> Ethernet0/0
Ethernet0-0 ------> Ethernet0/0	Ethernet0-0 ------> Ethernet0/1
Ethernet0-1 ------> Ethernet0/1	Ethernet0-1 ------> Ethernet0/2
Ethernet0-2 ------> Ethernet0/2	Ethernet0-2 ------> Ethernet0/3
Ethernet0-3 ------> Ethernet0/3	Ethernet0-3 ------> Ethernet0/4
Ethernet0-4 ------> Ethernet0/4	Ethernet0-4 ------> Ethernet0/5
Ethernet0-5 ------> Ethernet0/5	Ethernet0-5 ------> Ethernet0/6
Ethernet0-6 ------> Ethernet0/6	Ethernet0-6 ------> Ethernet0/7
Ethernet0-7 ------> Ethernet0/7	Ethernet0-7 ------> Ethernet0/8

Important If the diagnostic setting is specified both in the Day0 configuration file and in the VMware OVF deployment wizard, the Day0 configuration takes precedence.

For example:

If **"Diagnostic": "OFF"** is specified in the Day0 configuration file, but the diagnostic option is set to ON in the OVF deployment wizard, the diagnostic interface will be disabled.

The Day0 configuration is applied at first boot and overrides the OVF template selection.

To avoid interface mapping inconsistencies, ensure that the diagnostic setting is consistently configured in both the Day0 configuration file and the OVF wizard.

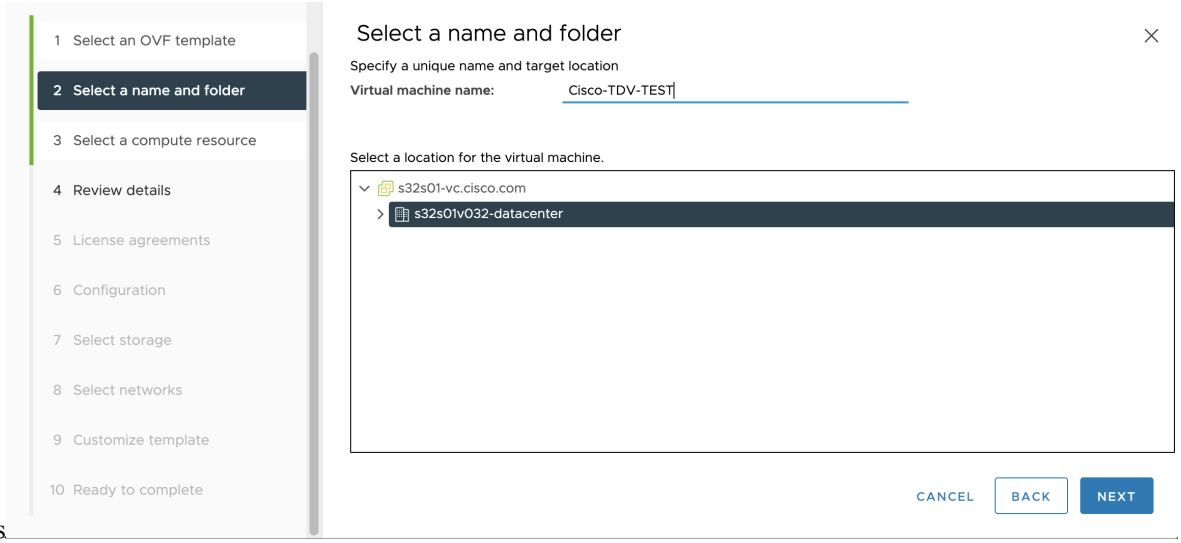
Step 4 Browse your file system for the OVF template source location and click **Next**.

Select the Firewall Threat Defense Virtual VI OVF template:

- *Cisco_Secure_Firewall_Threat_Defense_Virtual-VI-X.X.X-xxx.ovf*
- *Cisco_Secure_Firewall_Threat_Defense_Virtual-X.X.X-xxx.vmdk*
- *day0.iso*

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

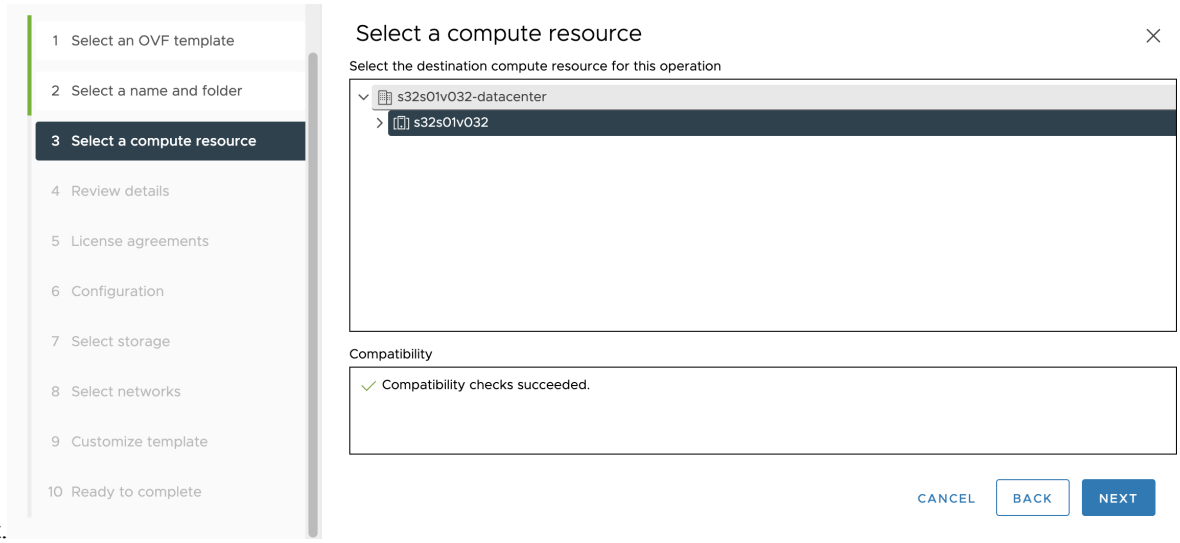
Step 5 On the **Name and Location** page, enter a name for this deployment and select the location in the inventory (host or cluster) on which you want to deploy the Firewall Threat Defense Virtual Unlimited, then click **Next**. The name must be unique within the inventory folder and can contain up to 80



characters.

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

Step 6 Navigate to, and select the resource pool where you want to run the Firewall Threat Defense Virtual and click **Next**.



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

Step 7 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 8 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 9 On the **Configuration** page, select either 32 vCPU / 64 GB or 64 vCPU / 128 GB for FTDvU from the the **Configuration** options, and click **Next**.

Important The Firewall Threat Defense Virtual deploys with adjustable vCPU and memory resources.

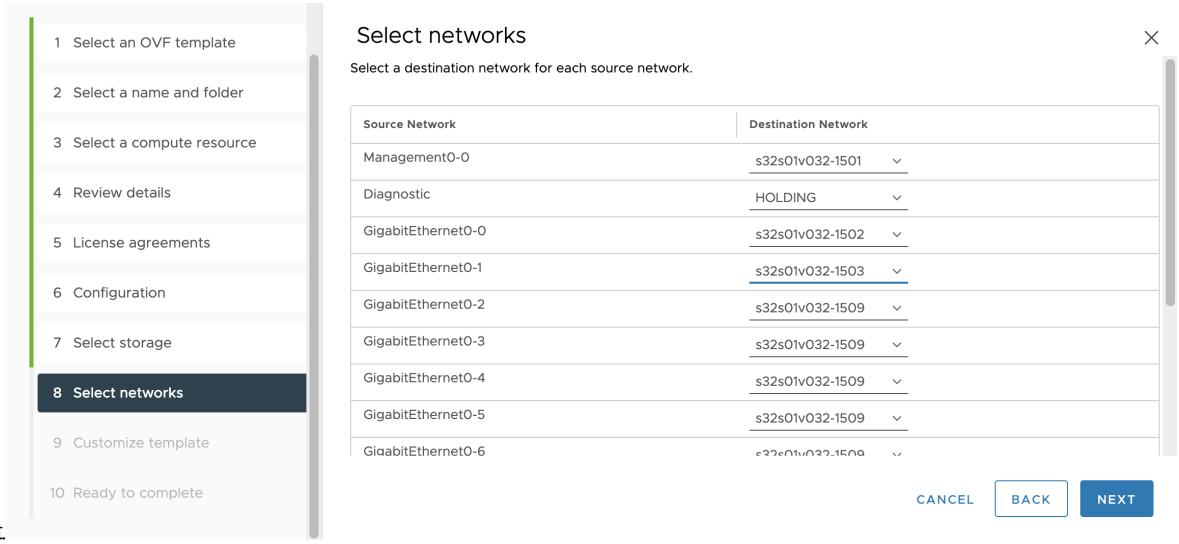
Step 10 Select a **Storage** location to store the virtual machine files.

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 11 From the **Select virtual disk format** drop-down list, choose 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 12 On the **Select networks** page, map the networks specified in the OVF template to networks in your inventory, and then click **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 the Firewall Management Center or from the Firewall Device Manager depending on your management mode.

Important Firewall Threat Defense Virtual 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 Firewall Threat Defense Virtual instance, and choose **Edit Settings**. However, that screen does not show the Firewall Threat Defense Virtual IDs (only Network Adapter IDs).

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

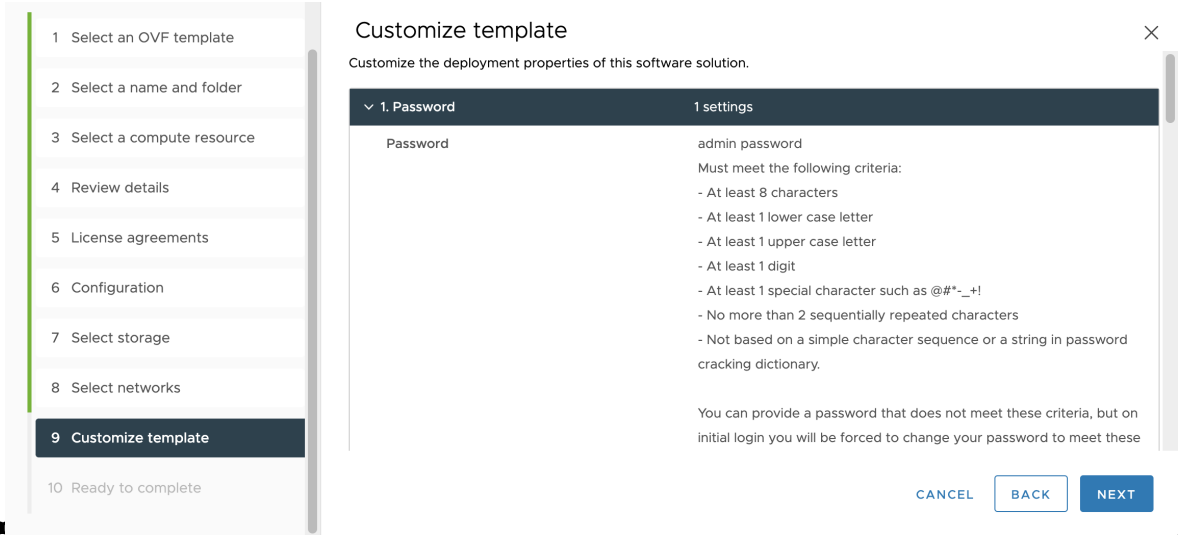
Table 5: Source to Destination Network Mapping—VMXNET3

Network Adapter	Source Networks	Destination Networks	Function
Network adapter 1	Management0-0	Management0/0	Management
Network adapter 2	Reserved for internal use.	Reserved for internal use.	Reserved for internal use.
Network adapter 3	Ethernet0-0	Ethernet0/0	Outside data
Network adapter 4	Ethernet0-1	Ethernet0/1	Inside data
Network adapter 5	Ethernet0-2	Ethernet0/2	Data traffic (Optional)
Network adapter 6	Ethernet0-3	Ethernet0/3	Data traffic (Optional)

Network Adapter	Source Networks	Destination Networks	Function
Network adapter 7	Ethernet0-4	Ethernet0/4	Data traffic (Optional)
Network adapter 8	Ethernet0-5	Ethernet0/5	Data traffic (Optional)
Network adapter 9	Ethernet0-6	Ethernet0/6	Data traffic (Optional)
Network adapter 10	Ethernet0-7	Ethernet0/7	Data traffic (Optional)

You can have a total of 10 interfaces when you deploy the Firewall Threat Defense Virtual. 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 Firewall Threat Defense Virtual interfaces; for interfaces you do not intend to use, you can simply leave the interface disabled within the Firewall Threat Defense Virtual configuration

Step 13 On the **Customize templates** properties page, set the user-configurable properties packaged with the OVF template (VI templates only):

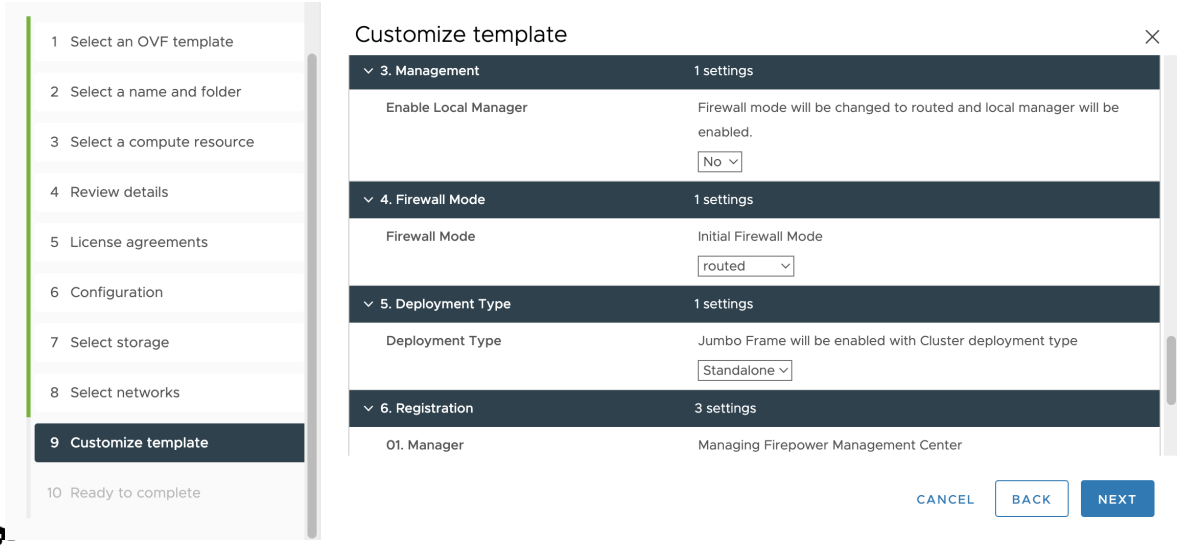


a) **Pa**

Set the password for Firewall Threat Defense Virtual 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) **Mg**

Set the management mode. Click the drop-down arrow for **Enable Local Manager** and select **Yes** to use the integrated Firewall Device Manager web-based configuration tool. Select **No** to use Firewall Management Center to manage this device.

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 Firewall Device Manager.

e) **Deployment Type**

Set the deployment type to **Standalone** or **Cluster**. Choose **Cluster** to enable jumbo-frame reservation, which is required for the cluster control link. Choose **Standalone** for a standalone or High Availability deployment. Note that if you deploy as a Standalone device, you can still use it in a cluster; however, enabling jumbo frames for clustering after deployment means you will have to restart.

f) **Registration**

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

- **Managing Defense Center**—Enter the host name or IP address of the Firewall Management Center.
- **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 Firewall Management Center.
- **NAT ID**—If the Firewall Threat Defense Virtual and the Firewall Management Center are separated by a Network Address Translation (NAT) device, and the Firewall 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 (-).

g) Click **Next**.

Step 14 On the **Ready to complete** page, 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 Firewall Threat Defense Virtual, 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 Firewall Threat Defense 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 Firewall Threat Defense Virtual with the Cisco Licensing Authority, the Firewall Threat Defense Virtual requires Internet access. You might need to perform additional configuration after deployment to achieve Internet access and successful license registration.

Important During registration of Threat Defense Virtual to the Management Center, select the **FTDvU - Unlimited** performance tier from the drop-down list to apply the FTDvU license tier.

Attach the SR-IOV interfaces

Procedure

Step 1 Power off the Firewall Threat Defense Virtual instance.

Step 2 Remove the data interfaces.

In the vSphere Client, click **Edit Settings**, and under **Virtual Hardware**, remove all data interfaces. Ensure that only the **management interface (Network adapter 1)** remains attached.

Step 3 Attach the SR-IOV interface.

Select the new network and set Adapter Type as PCI Device passthrough.

Choose the SR-IOV network (for example, sriov1).

The maximum number of supported interfaces is 10. You can attach the SR-IOV interfaces to the data interfaces based on your requirements.

Step 4 Power on the Firewall Threat Defense Virtual instance.

Click **OK** to save the configuration, then power on the Firewall Threat Defense Virtual instance.

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

Important During registration of Firewall Threat Defense Virtual to the Management Center, select the **Threat Defense Virtual Unlimited** performance tier from the drop-down list to apply the FTDvU license tier.

Deploy the Firewall Threat Defense Virtual Unlimited to a vSphere ESXi Host

Use this procedure to deploy the Firewall Threat Defense Virtual 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 Firewall Threat Defense 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.

Before you begin

- You must have at least one network configured in vSphere (for management) before you deploy the Firewall Threat Defense Virtual.
- Validate the SHA1 checksum after extracting the VMDK files from the directory.

Procedure

Step 1 Download the Firewall 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 is 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_Secure_Firewall_Threat_Defense_Virtual-VI-*X.X.X-xxx*.ovf—For vCenter deployments
- Cisco_Secure_Firewall_Threat_Defense_Virtual-ESXi-*X.X.X-xxx*.ovf—For ESXi deployments.
- Cisco_Secure_Firewall_Threat_Defense_Virtual-*X.X.X-xxx*.vmdk—VMware virtual disk file.
- Cisco_Secure_Firewall_Threat_Defense_Virtual-VI-*X.X.X-xxx*.mf—Manifest file for vCenter deployments.
- Cisco_Secure_Firewall_Threat_Defense_Virtual-ESXi-*X.X.X-xxx*.mf—Manifest file for ESXi deployments.
- day0.iso

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 format *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 Firewall Threat Defense 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 Firewall Threat Defense Virtual tar file, and choose the ESXi OVF template and the accompanying VMDK file:

Cisco_Secure_Firewall_Threat_Defense_Virtual-ESXi-*X.X.X-xxx*.ovf

Cisco_Secure_Firewall_Threat_Defense_Virtual-*X.X.X-xxx*.vmdk

day0.iso

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 Firewall Threat Defense Virtual:

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 the Firewall Management Center or from the Firewall Device Manager depending on your management mode.

Important Firewall Threat Defense Virtual 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 Firewall Threat Defense Virtual instance, and choose **Edit Settings**. However, that screen does not show the Firewall Threat Defense Virtual IDs (only Network Adapter IDs).

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

Table 6: Source to Destination Network Mapping—VMXNET3

Network Adapter	Source Networks	Destination Networks	Function
Network adapter 1	Management0-0	Management0/0	Management
Network adapter 2	Reserved for internal use.	Reserved for internal use.	Reserved for internal use.
Network adapter 3	Ethernet0-0	Ethernet0/0	Outside data
Network adapter 4	Ethernet0-1	Ethernet0/1	Inside data
Network adapter 5	Ethernet0-2	Ethernet0/2	Data traffic (Optional)
Network adapter 6	Ethernet0-3	Ethernet0/3	Data traffic (Optional)
Network adapter 7	Ethernet0-4	Ethernet0/4	Data traffic (Optional)

Network Adapter	Source Networks	Destination Networks	Function
Network adapter 8	Ethernet0-5	Ethernet0/5	Data traffic (Optional)
Network adapter 9	Ethernet0-6	Ethernet0/6	Data traffic (Optional)
Network adapter 10	Ethernet0-7	Ethernet0/7	Data traffic (Optional)

You can have a total of 10 interfaces when you deploy the Firewall Threat Defense Virtual. 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 Firewall Threat Defense Virtual interfaces; for interfaces you do not intend to use, you can simply leave the interface disabled within the Firewall Threat Defense Virtual 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 Firewall Threat Defense Virtual 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 Firewall Threat Defense Virtual with the Cisco Licensing Authority, the Firewall Threat Defense Virtual 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 Firewall Threat Defense Virtual using the ESXi OVF template.

Complete the Firewall Threat Defense Virtual Unlimited Setup Using the CLI

If you deployed with an ESXi OVF template, you must set up the Firewall Threat Defense Virtual Unlimited using the CLI. Firewall Threat Defense Virtual Unlimited appliances do not have web interfaces. You can also use the CLI to configure 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 in to 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 Firewall Threat Defense Virtual Unlimited 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 the Firewall 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 Firewall Threat Defense Virtual with the Cisco Licensing Authority, the Firewall Threat Defense Virtual requires Internet access. You might need to perform additional configuration after deployment to achieve Internet access and successful license registration.