Deploy the Threat Defense Virtual on Nutanix

This chapter describes the procedures to deploy the threat defense virtual to a Nutanix environment.

Overview

The Cisco Secure Firewall Threat Defense Virtual (formerly Firepower Threat Defense Virtual) brings Cisco's Secure 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 threat defense virtual functions in the Nutanix environment with AHV hypervisor, including feature support, system requirements, guidelines, and limitations. This chapter also describes your options for managing the threat defense virtual.

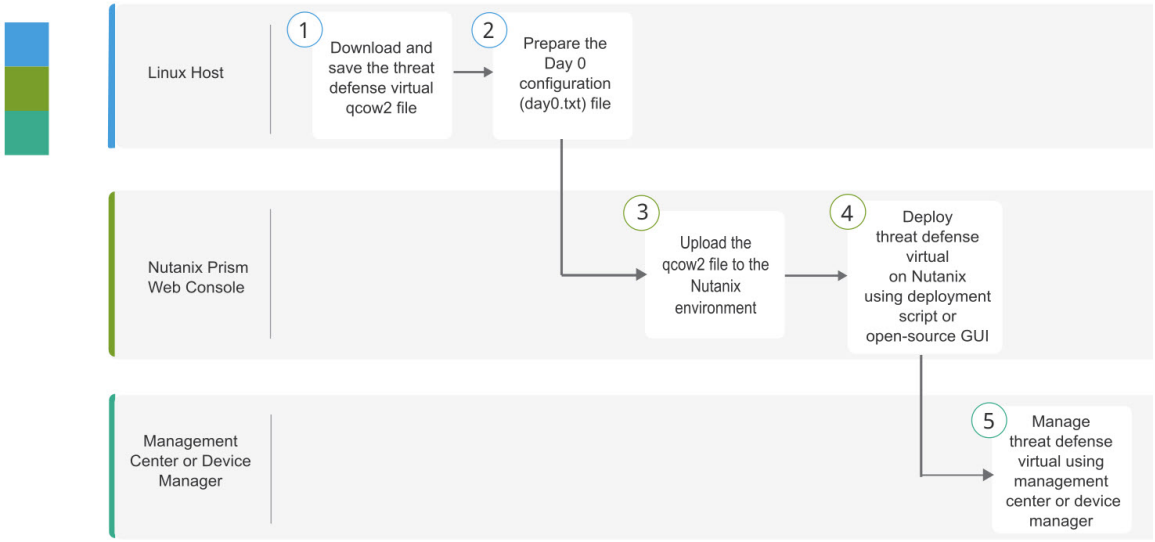
It's important that you understand your management options before you begin your deployment. You can manage and monitor the threat defense virtual using the Secure Firewall Management Center (formerly Firepower Management Center) or the Secure Firewall Device Manager (formerly Firepower Device Manager).

About Threat Defense Virtual Deployment On Nutanix

The Nutanix Enterprise Cloud Platform is a converged, scale-out compute and storage system that is built to host and store virtual machines. You can run multiple virtual machines running unmodified OS images of threat defense virtual using Nutanix AHV. Each virtual machine has private virtualized hardware: a network card, disk, graphics adapter, and so forth.

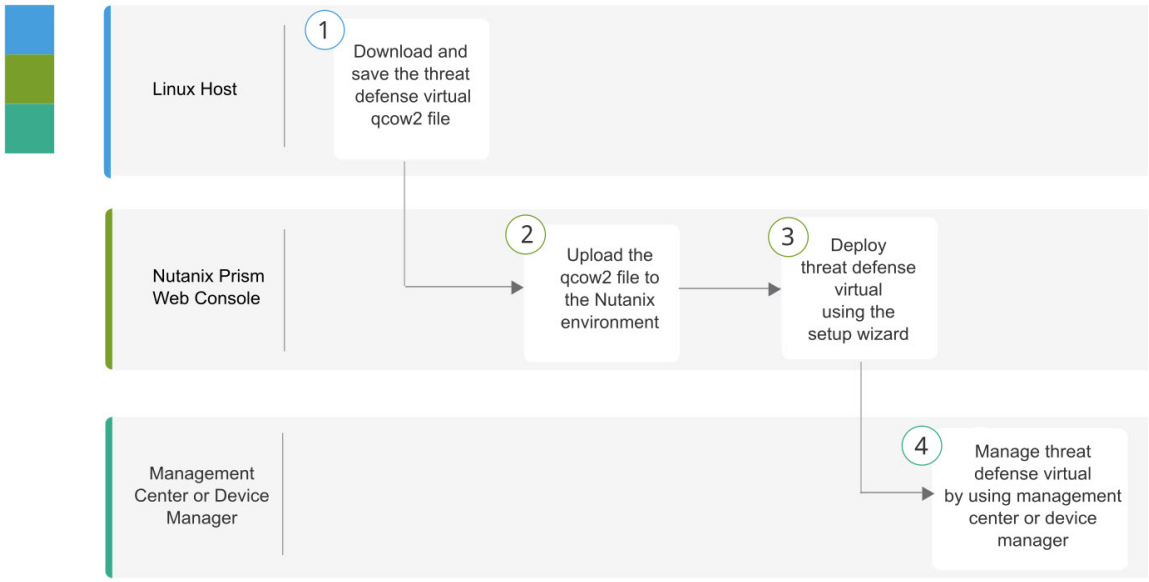
End-to-End Procedure

The following flowchart illustrates the workflow for deploying Threat Defense Virtual on Nutanix Platform with Day-0 Configuration File.



	Workspace	Steps
1	Linux Host	Deploy the Threat Defense Virtual: Download and save the threat defense virtual qcow2 file.
2	Linux Host	Upload the Threat Defense Virtual QCOW2 File to Nutanix: Upload the qcow2 file to the Nutanix environment.
3	Nutanix Prism Web Console	Prepare the Day 0 Configuration File: Prepare the Day-0 Configuration File (**Text file** > **Enter the configuration details** > **Save as day0-config.txt**.
4	Nutanix Prism Web Console	Deploy the Threat Defense Virtual: Deploy the Threat Defense Virtual on Nutanix.
5	Management Center or Device Manager	Manage Threat Defense Virtual: • Using Management Center • Using Device Manager

The following flowchart illustrates the workflow for deploying Threat Defense Virtual on Nutanix Platform without Day-0 Configuration File.



	Workspace	Steps
1	Linux Host	Deploy the Threat Defense Virtual: Download and save the threat defense virtual qcow2 file.
2	Nutanix Prism Web Console	Upload the Threat Defense Virtual QCOW2 File to Nutanix: Upload the qcow2 file to the Nutanix environment.
3	Nutanix Prism Web Console	Deploy the Threat Defense Virtual: Deploy the Threat Defense Virtual on Nutanix.
4	Management Center or Device Manager	Manage Threat Defense Virtual: • Using Management Center • Using Device Manager

System Requirements

Versions

Manager Version	Device Version
Device Manager 7.0	Threat Defense 7.0
Management Center 7.0	

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

Threat Defense Virtual Memory, vCPU, and Disk Sizing

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

Settings	Value
Performance Tiers	**Version 7.0 and later** The threat defense virtual supports performance-tiered licensing that provides different throughput levels and VPN connection limits based on deployment requirements. • FTDv5 4vCPU/8GB (100Mbps) • FTDv10 4vCPU/8GB (1Gbps) • FTDv20 4vCPU/8GB (3Gbps) • FTDv30 8vCPU/16GB (5Gbps) • FTDv50 12vCPU/24GB (10Gbps) • FTDv100 16vCPU/32GB (16Gbps) See the "Licensing the System" chapter in the*Secure Firewall Management Center Configuration* for guidelines when licensing your threat defense virtual device. **Note** To change the vCPU/memory values, you must first power off the threat defense virtual device.
Storage	50 GB (Adjustable) • Supports virtio block devices

Note The minimum number of network for the threat defense virtual are 4 data interfaces (management,diagnostic,outside and inside).

Threat Defense Virtual Licenses

- Configure all license entitlements for the security services from the management center.
- See *Licensing the System* in the Secure firewall Management Center Configuration Guide for more information about how to manage licenses.

Nutanix Components and Versions

Component	Version
Nutanix Acropolis Operating System (AOS)	5.15.5 LTS and later

Component	Version
Nutanix Cluster Check (NCC)	4.0.0.1
Nutanix AHV	20201105.12 and later
Nutanix Prism Web Console	-

Guidelines and Limitations

Supported Features

- Deployment Modes–Routed (Standalone), Routed (HA), Inline Tap, Inline, Passive, and Transparent
- Licensing–Only BYOL
- IPv6
- Threat Defense Virtual native HA
- Device Manager
- Jumbo frames
- VirtIO

Performance Optimizations

To achieve the best performance out of the threat defense virtual, you can make adjustments to the both the VM and the host. See Virtualization Tuning and Optimization on Nutanix for more information.

Receive Side Scaling—The threat defense virtual supports Receive Side Scaling (RSS), which is a technology utilized by network adapters to distribute network receive traffic to multiple processor cores. Supported on Version 7.0 and later. See Multiple RX Queues for Receive Side Scaling (RSS) for more information.

Snort

- If you are observing abnormal behavior such as Snort taking a long time to shut down, or the VM being slow in general or when a certain process is executed, collect logs from the threat defense virtual and the VM host. Collection of overall CPU usage, memory, I/O usage, and read/write speed logs will help troubleshoot the issues.
- High CPU and I/O usage is observed when Snort is shutting down. If a number of threat defense virtual instances have been created on a single host with insufficient memory and no dedicated CPU, Snort will take a long time to shut down which will result in the creation of Snort cores.

Unsupported Features

- Threat Defense Virtual on Nutanix AHV does not support hot plug of interface. Do not try to Add/Remove interface when the threat defense virtual is powered on.
- Nutanix AHV does not support SR-IOV or DPDK-OVS.

Note Nutanix AHV supports in-guest DPDK using VirtIO. For more information, refer DPDK support on AHV.

General Guidelines

- Requires two management interfaces and two data interfaces to boot. Supports a total of 10 interfaces.

Note
- The threat defense virtual default configuration puts the management interface, diagnostic interface, and inside interface on the same subnet.
- When you are modifying the network interfaces, you must turn off the threat defense virtual device.

- The default configuration for the threat defense virtual assumes that you put both the management (management and diagnostic) and inside interfaces on the **same subnet**, and the management address uses the inside address as its gateway to the Internet (going through the outside interface).
- The threat defense virtual must be powered up on firstboot with at least four interfaces. Your system will not deploy without four interfaces.
- The threat defense virtual supports a total of 10 interfaces—1 management interface, 1 diagnostic interface, and a maximum of 8 network interfaces for data traffic. The interface-to-network assignments must be ordered as follows:
  1. Management interface (required)
  2. Diagnostic interface (required)
  3. Outside interface (required)
  4. Inside interface (required)
  5. 5–10 Data interfaces (optional)

Note The minimum number of network for the threat defense virtual are 4 data interfaces.

- For the console access, terminal server is supported through telnet.
- The following are the supported vCPU and memory parameters:

CPUs	Memory	Threat Defense Virtual Platform Size
4	8 GB	4vCPU/8GB (default)
8	16 GB	8vCPU/16GB
12	24 GB	12vCPU/24GB

CPUs	Memory	Threat Defense Virtual Platform Size
16	32 GB	16vCPU/32GB

- See the following concordance of Network Adapter, Source Networks and Destination Networks for the threat defense virtual interfaces:

Network Adapter	Source Network	Destination Network	Function
vnic0*	Management0-0	Management0/0	Management
vnic1	Diagnostic	Diagnostic	Diagnostic
vnic2*	GigabitEthernet0-0	GigabitEthernet0/0	Outside
vnic3*	GigabitEthernet0-1	GigabitEthernet0/1	Inside
*Attach to the same subnet.			

Related Documentation

- Nutanix Release Notes
- Nutanix Field Installation Guide
- Hardware Support on Nutanix

How to Manage Secure Firewall Threat Defense Virtual Device

You have two options to manage your Secure Firewall Threat Defense Virtual device.

Secure Firewall device manager

The device manager is an onboard integrated manager.

The device manager is a web-based configuration interface included on some of the threat defense devices. The device manager 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 of the threat defense devices.

Note See the Cisco Secure Firewall Device Manager Configuration Guide for list of the threat defense devices that support the device manager.

Secure Firewall Management Center

If you are managing large numbers of devices, or if you want to use the more complex features and configurations that the threat defense allows, use the management center to configure your devices instead of the integrated device manager.

Important You cannot use both the device manager and the management center to manage the threat defense device. Once the device manager integrated management is enabled, it won't be possible to use the management center to manage the threat defense device, unless you disable the local management and re-configure the management to use the management center. On the other hand, when you register the threat defense device to the management center, the device manager onboard management service is disabled.

Caution Currently, Cisco does not have an option to migrate your device manager configuration to the management center and vice-versa. Take this into consideration when you choose what type of management you configure for the threat defense device.

Prerequisites for Deployment on Nutanix

- Download the Threat Defense Virtual qcow2 file from Cisco.com: https://software.cisco.com/download/navigator.html

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

- Review the Overview, on page 1 chapter.
- For Nutanix and System compatibility, seeCisco Secure Firewall Threat Defense Compatibility Guide .

How to Deploy the Threat Defense Virtual on Nutanix

Step	Task	More Information
1	Review the prerequisites.	Prerequisites for Deployment on Nutanix, on page 8
2	Upload the threat defense virtual qcow2 file to the Nutanix environment.	Upload the Threat Defense Virtual QCOW2 File to Nutanix, on page 9
3	(Optional) Prepare a Day 0 configuration file that contains the initial configuration data that gets applied at the time a virtual machine is deployed.	Prepare the Day 0 Configuration File, on page 9
4	Deploy the threat defense virtual to the Nutanix environment.	Deploy the Threat Defense Virtual, on page 11

Step	Task	More Information
5	(Optional) If you did not use a Day 0 configuration file to set up the threat defense virtual, complete the setup by logging in to the CLI.	Complete the Threat Defense Virtual Setup, on page 13

Upload the Threat Defense Virtual QCOW2 File to Nutanix

To deploy an threat defense virtual to the Nutanix environment, you must create an image from the threat defense virtual qcow2 disk file in the Prism Web Console.

Before you begin

Download the threat defense virtual qcow2 disk file from Cisco.com: https://software.cisco.com/download/navigator.html

Step 1 Log in to the Nutanix Prism Web Console.

Step 2 Click the gear icon to open the **Settings** page.

Step 3 Click **Image Configuration** from the left pane.

Step 4 Click **Upload Image**.

Step 5 Create the image.

a. Enter a name for the image.

b. From the **Image Type** drop-down list, choose **DISK**.

c. From the **Storage Container** drop-down list, choose the desired container.

d. Specify the location of the threat defense virtual qcow2 disk file.

You can either specify a URL (to import the file from a web server) or upload the file from your workstation.

e. Click **Save**.

Step 6 Wait until the new image appears in the **Image Configuration** page.

Prepare the Day 0 Configuration File

You can prepare a Day 0 configuration file before you deploy the threat defense virtual. This file is a text file that contains the initial configuration data that gets applied at the time a virtual machine is deployed.

Keep in mind that:

- If you deploy with a Day 0 configuration file, the process allows you to perform the entire initial setup for the threat defense virtual appliance.
- If you deploy without a Day 0 configuration file, you must configure System-required settings after launch; see Complete the Threat Defense Virtual Setup, on page 13 for more information.

You can specify:

- The End User License Agreement (EULA) acceptance.
- A hostname for the system.
- A new administrator password for the admin account.
- The initial firewall mode; sets the initial firewall mode, either **routed** or **transparent**.

  If you plan to manage your deployment using the local device manager, you can only enter **routed** for the firewall mode. You cannot configure transparent firewall mode interfaces using the device manager.
- The management mode; see How to Manage Secure Firewall Threat Defense Virtual Device.

  You can either set **ManageLocally** to **Yes**, or enter information for the management center fields (**FmcIp**, **FmcRegKey**, and **FmcNatId**). Leave fields empty for the management mode you are not using.
- Network settings that allow the appliance to communicate on your management network.

Step 1 Create a new text file using a text editor of your choice.

Step 2 Enter the configuration details in the text file as shown in the following sample:

Example:

```
#Firepower Threat Defense
{
    "EULA": "accept",
    "Hostname": "ftdv-production",
    "AdminPassword": "Admin123",
    "FirewallMode": "routed",
    "DNS1": "1.1.1.1",
    "DNS2": "1.1.1.2",
    "DNS3": "",
    "IPv4Mode": "manual",
    "IPv4Addr": "10.12.129.44",
    "IPv4Mask": "255.255.0.0",
    "IPv4Gw": "10.12.0.1",
    "IPv6Mode": "disabled",
    "IPv6Addr": "",
    "IPv6Mask": "",
    "IPv6Gw": "",
    "FmcIp": "",
    "FmcRegKey": "",
    "FmcNatId": "",
    "ManageLocally":"Yes"
}
```

Note The content of the Day 0 configuration file must be in JSON format. You must validate the text using a JSON validator tool.

Step 3 Save the file as "**day0-config.txt**."

Step 4 Repeat Step 1–3 to create unique default configuration files for each threat defense virtual that you want to deploy.

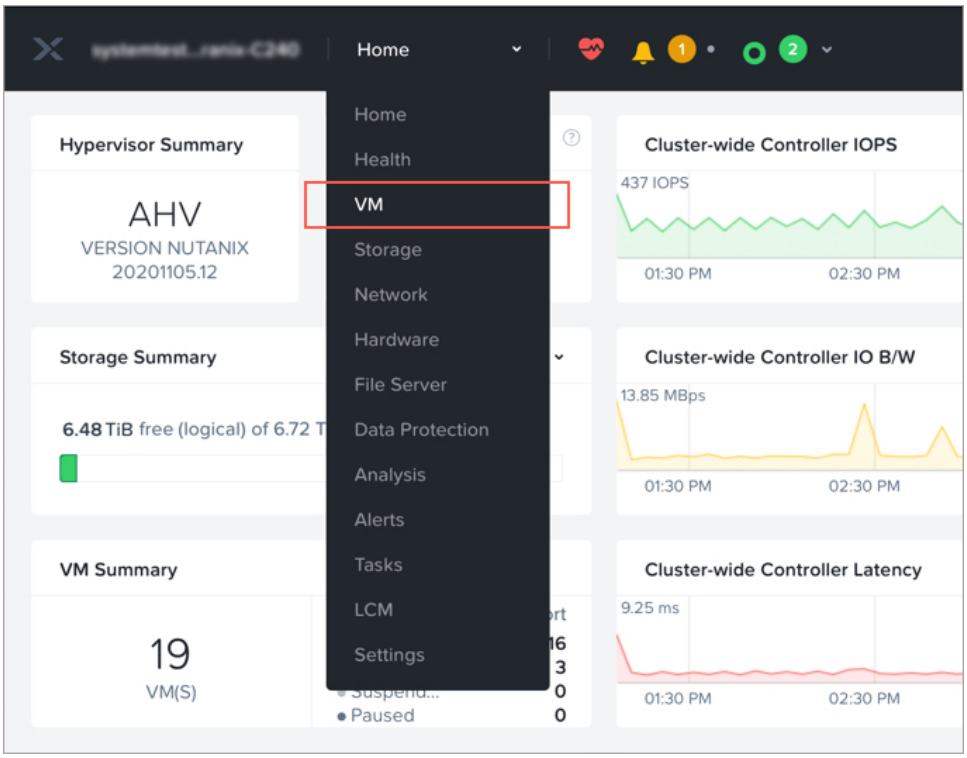
Deploy the Threat Defense Virtual

Before you begin

Ensure that the image of the threat defense virtual that you plan to deploy is appearing on the **Image Configuration** page.

Step 1 Log in to the Nutanix Prism Web Console.

Step 2 From the main menu bar, click the view drop-down list, and choose **VM**.



Step 3 On the VM Dashboard, click **Create VM**.

Step 4 Do the following:

a. Enter a name for the threat defense virtual instance.

b. Optionally enter a description for the threat defense virtual instance.

c. Select the timezone that you want the threat defense virtual instance to use.

Step 5 Enter the compute details.

a. Enter the number of virtual CPUs to allocate to the threat defense virtual instance.

b. Enter the number of cores that must be assigned to each virtual CPU.

c. Enter the amount of memory (in GB) to allocate to the threat defense virtual instance.

Step 6 Attach a disk to the threat defense virtual instance.

a. Under **Disks**, Click **Add New Disk**.

b. From the **Type** drop-down list, choose **DISK**.

c. From the **Operation** drop-down list, choose **Clone from Image Service**.

d. From the **Bus Type** drop-down list, choose **PCI** or **SCSI**.

e. From the **Image** drop-down list, choose the image that you want to use.

f. Click **Add**.

Step 7 Configure at least four virtual network interfaces.

Under **Network Adapters (NIC)**, click **Add New NIC**, select a network, and click **Add**.

Repeat this process to add more network interfaces.

The threat defense virtual on Nutanix supports a total of 10 interfaces—One management interface, one diagnostic interface, and a maximum of eight network interfaces for data traffic. The interface-to-network assignments must be ordered as follows:

- vnic0—Management interface (required)
- vnic1—Diagnostic interface (required)
- vnic2—Outside interface (required)
- vnic3—Inside interface (required)
- vnic4-9—Data interfaces (optional)

Step 8 Configure affinity policy for the threat defense virtual.

Under **VM Host Affinity** , click **Set Affinity**, select the hosts, and click **Save**.

Select more than one host to ensure that the threat defense virtual can be run even if there is a node failure.

Step 9 If you have prepared a Day 0 configuration file, do the following:

a. Select **Custom Script**.

b. Click **Upload A File**, and choose the Day 0 configuration file (**day0-config.txt**).

Note All the other custom script options are not supported in this release.

Step 10 Click **Save** to deploy the threat defense virtual. The threat defense virtual instance appears in the VM table view.

Step 11 In the VM table view, select the newly created threat defense virtual instance, and click **Power On**.

What to do next

- If you used a Day 0 configuration file to set up the threat defense virtual, your next steps depend on what management mode you chose.
  - If you chose **No** for **ManageLocally**, you'll use the management center to manage your threat defense virtual; see Managing the Secure Firewall Threat Defense Virtual with the Secure Firewall Management Center.

- If you did not use a Day 0 configuration file to set up the threat defense virtual, complete the threat defense virtual setup by logging in to the CLI. For instructions, see Complete the Threat Defense Virtual Setup, on page 13.

Complete the Threat Defense Virtual Setup

Because the threat defense virtual appliances do not have web interfaces, you must set up a virtual device using the CLI if you deployed without a Day 0 configuration file.

Step 1 Open a console to the threat defense virtual.

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

Step 3 When the threat defense virtual system boots, a setup wizard prompts you for the following information that is 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 required)

Step 4 Review the Setup wizard settings. Defaults or previously entered values appear in brackets. To accept previously entered values, press **Enter**.

Step 5 Complete the system configuration as prompted.

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

Step 7 Close the CLI.

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 management center to manage your threat defense virtual; see Managing the Secure Firewall Threat Defense Virtual with the Secure Firewall Management Center.

See How to Manage Secure Firewall Threat Defense Virtual Device for an overview of how to choose your management option.