在 Nutanix 上部署 Threat Defense Virtual

本章介绍将 threat defense virtual 部署到 Nutanix 环境的程序。

- 概述，第 1 页
- 关于 Nutanix 上的 Threat Defense Virtual 部署，第 1 页
- 端到端程序，第 2 页
- 系统要求，第 3 页
- 准则和限制，第 5 页
- 如何管理 Cisco Secure Firewall Threat Defense Virtual 设备，第 7 页
- 在 Nutanix 上部署的前提条件，第 8 页
- 如何在 Nutanix 上部署 Threat Defense Virtual，第 8 页

概述

Cisco Cisco Secure Firewall Threat Defense Virtual （之前称为 Firepower Threat Defense Virtual）将 Cisco Secure Firewall 功能带到虚拟环境，支持采用一致的安全策略来跟踪物理、虚拟和云环境以及云之间的工作负载。

本章介绍了具有 AHV 虚拟机管理程序的 Nutanix 环境中的 threat defense virtual 功能，包括功能支持、系统要求、指南和限制。 本章还介绍了管理 threat defense virtual 的选项。

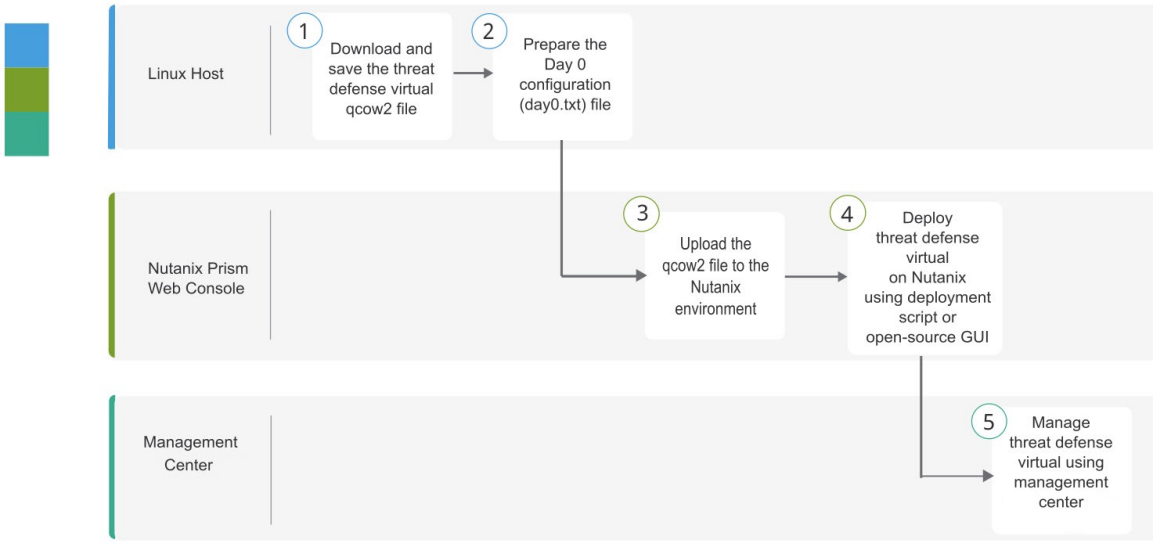
在开始部署之前，了解您的管理选项非常重要。您可以使用 Cisco Secure Firewall Management Center 来管理和监控 threat defense virtual。（之前称为 Firepower 管理中心）

关于 Nutanix 上的 Threat Defense Virtual 部署

Nutanix 企业云平台是一个融合的外向扩展计算和存储系统，用于托管和存储虚拟机。您可以运行多个虚拟机，这些虚拟机使用 Nutanix AHV 来运行未修改的 threat defense virtual OS 映像。每个虚拟机都有专用的虚拟化硬件：网卡、磁盘、图形适配器等等。

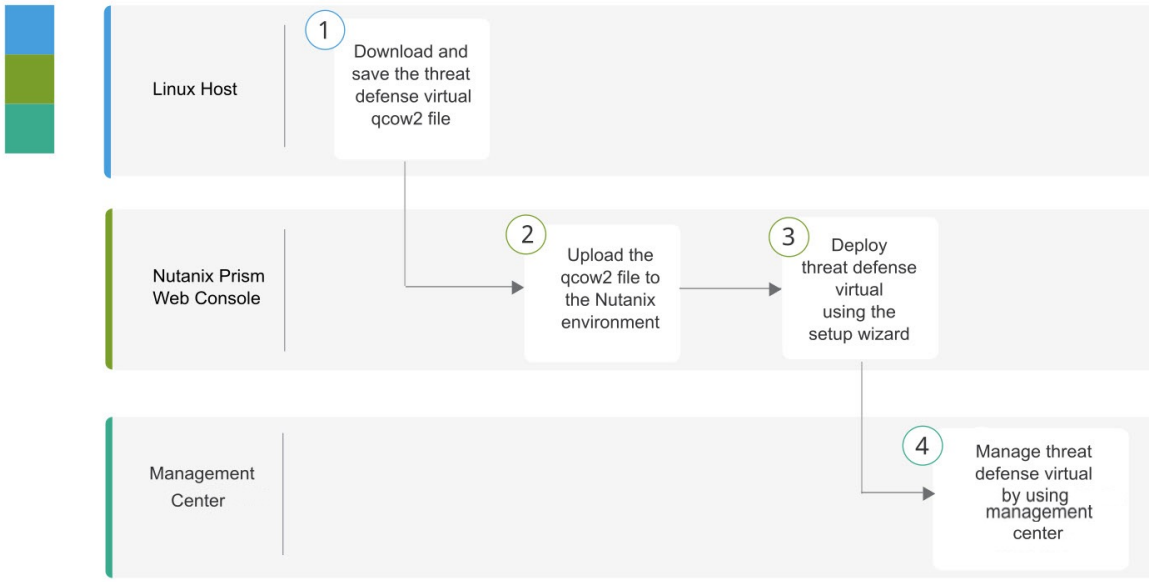
端到端程序

以下流程图说明了在使用 Day-0 配置文件的 Nutanix 平台上部署 Threat Defense Virtual 的工作流程。



	工作空间	步骤
1	Linux 主机	部署 Threat Defense Virtual：下载并保存 Threat Defense Virtual qcow2 文件。
2	Linux 主机	将 Threat Defense Virtual QCOW2 文件上传到 Nutanix：将 qcow2 文件上传到 Nutanix 环境。
3	Nutanix Prism Web 控制台	准备 Day 0 配置文件：准备 Day-0 配置文件（**文本文件 (Text file)** > **输入配置详细信息 (Enter the configuration details)** > **另存为 day0-config.txt (Save as day0-config.txt)**。
4	Nutanix Prism Web 控制台	部署 Threat Defense Virtual：在 Nutanix 上部署 Threat Defense Virtual。
5	管理中心或设备管理器	管理 Threat Defense Virtual： • 使用管理中心 • 使用设备管理器

以下流程图说明了在没有 Day-0 配置文件的情况下在 Nutanix 平台上部署 Threat Defense Virtual 的工作流程。



	工作空间	步骤
1	Linux 主机	部署 Threat Defense Virtual：下载并保存 Threat Defense Virtual qcow2 文件。
2	Nutanix Prism Web 控制台	将 Threat Defense Virtual QCOW2 文件上传到 Nutanix：将 qcow2 文件上传到 Nutanix 环境。
3	Nutanix Prism Web 控制台	部署 Threat Defense Virtual：在 Nutanix 上部署 Threat Defense Virtual。
4	管理中心或设备管理器	管理 Threat Defense Virtual： • 使用管理中心 • 使用设备管理器

系统要求

版本

管理器版本	设备版本
设备管理器 7.0	威胁防御 7.0
管理中心 7.0	

有关 threat defense virtual 支持的虚拟机管理程序的最新信息，请参阅《Cisco Secure Firewall Threat Defense 兼容性指南》。

Threat Defense Virtual 内存、vCPU 和磁盘大小估算

根据所需部署的实例数量和使用要求，threat defense virtual部署所使用的具体硬件可能会有所不同。每个 threat defense virtual 实例都需要服务器保证最小的资源配置，这包括内存数量、CPU 数和磁盘空间。

设置	值
性能级别	**7.0 及更高版本** threat defense virtual 支持性能级许可，该级别许可可基于部署要求提供不同的吞吐量级别和 VPN 连接限制。 • FTDv5 4vCPU/8GB (100Mbps) • FTDv10 4vCPU/8GB (1Gbps) • FTDv20 4vCPU/8GB (3Gbps) • FTDv30 8vCPU/16GB (5Gbps) • FTDv50 12vCPU/24GB (10Gbps) • FTDv100 16vCPU/32GB (16Gbps) 请参阅*Cisco Secure Firewall Management Center* 配置 中的“许可系统”一章，了解在许可 threat defense virtual 设备时的准则。 **注释** 要更改 vCPU/内存值，必须先关闭 threat defense virtual 设备的电源。
存储	50 GB（可调整） • 支持 virtio 块设备

注释 threat defense virtual 的最小网络数量是 4 个数据接口（管理、诊断、外部和内部）。

Threat Defense Virtual许可证

- 所有安全服务的许可证授权均在 管理中心中配置。
- 有关如何管理许可证的更多信息，请参阅《Cisco Secure firewall Management Center 配置指南》中的系统许可。

Nutanix 组件和版本

组件	版本
Nutanix Acropolis操作系统 (AOS)	5.15.5 LTS 及更高版本
Nutanix 集群检查 (NCC)	4.0.0.1
Nutanix AHV	20201105.12 及更高版本
Nutanix Prism Web 控制台	-

准则和限制

支持的功能

- 部署模式 - 路由（独立）、路由 (HA)、内联分流、内联、被动和透明
- 许可 - 仅 BYOL
- IPv6
- Threat Defense Virtual 本地 HA
- 设备管理器
- 巨型帧
- VirtIO

性能优化

为实现 threat defense virtual的最佳性能，您可以对 VM 和主机进行调整。有关详细信息，请参阅 Nutanix 上的虚拟化调整和优化。

接收端扩展 - threat defense virtual 支持接收端扩展 (RSS)，网络适配器利用这项技术将网络接收流量分发给多个处理器内核。在 7.0 及更高版本上受支持。有关详细信息，请参阅用于接收端扩展 (RSS) 的多个 RX 队列。

Snort

- 如果您观察到异常行为，例如 Snort 需要很长时间才能关闭，或者 VM 通常缓慢，或者在执行某个进程时，请从 threat defense virtual 和 VM 主机收集日志。收集总体 CPU 使用情况、内存、I/O 使用情况和读/写速度日志将有助于对问题进行故障排除。
- 当 Snort 关闭时，观察到高 CPU 和 I/O 使用率。如果在内存不足且没有专用 CPU 的单个主机上创建了大量 threat defense virtual 实例，则 Snort 将需要很长时间才能关闭，这将导致创建 Snort 核心。

不支持的功能

- Nutanix AHV 上的 Threat Defense Virtual 不支持接口热插拔。请勿在 threat defense virtual 通电时尝试添加/删除接口。
- Nutanix AHV 不支持 SR-IOV 或 DPDK-OVS。

注释 Nutanix AHV 使用 VirtIO 支持访客内 DPDK。有关详细信息，请参阅 AHV 上的 DPDK 支持。

一般准则

- 需要两个管理接口和两个数据接口来启动。支持共计 10 个接口

注释
- threat defense virtual 默认配置将管理接口、诊断接口和内部接口置于同一子网上。
- 修改网络接口时，必须关闭 threat defense virtual 设备。

- threat defense virtual 的默认配置假设您将管理接口（管理和诊断）和内部接口置于**同一子网**，并且管理地址使用内部地址作为访问互联网的网关（经过外部接口）。
- threat defense virtual 首次启动时，必须启用至少四个接口。您的系统必须要有四个接口才能部署。
- threat defense virtual 支持共计 10 个接口 - 1 个管理接口、1 个诊断接口，以及最多 8 个用于数据流量的网络接口。接口到网络分配必须遵循以下顺序：
  1. 管理接口（必需）
  2. 诊断接口（必需）
  3. 外部接口（必需）
  4. 内部接口（必需）
  5. 5-10 数据接口（可选）

注释 threat defense virtual 的最小网络数量是 4 个数据接口。

- 对于控制台访问，通过 telnet 支持终端服务器。
- 以下是支持的 vCPU 和内存参数：

CPU	内存	Threat Defense Virtual 平台规模
4	8 GB	4vCPU/8GB（默认）
8	16 GB	8vCPU/16GB
12	24 GB	12vCPU/24GB
16	32 GB	16vCPU/32GB

- 请查看 threat defense virtual 接口的以下网络适配器、源网络和目标网络的对应关系：

网络适配器	源网络	目标网络	功能
vnic0*	Management0-0	Management0/0	管理
vnic1	诊断	诊断	诊断
vnic2*	GigabitEthernet0-0	GigabitEthernet0/0	外部
vnic3*	GigabitEthernet0-1	GigabitEthernet0/1	内部
*连接到同一子网。			

相关文档

- Nutanix 发行说明
- Nutanix 现场安装指南
- Nutanix 上的硬件支持

如何管理 Cisco Secure Firewall Threat Defense Virtual 设备

您可以使用以下选项来管理 Cisco Secure Firewall Threat Defense Virtual 设备：

Cisco Secure Firewall Management Center

如果要管理大量设备或要使用 威胁防御 支持的更复杂的功能和配置，请使用 管理中心（而不是集成的 设备管理器）来配置您的设备。

重要事项 您不能同时使用 设备管理器 和 管理中心 来管理 威胁防御 设备。在启用 设备管理器 集成管理功能后，将无法使用 管理中心 来管理 威胁防御 设备，除非您禁用本地管理功能并重新配置管理功能以使用 管理中心。另一方面，当您向 威胁防御 注册 管理中心 设备时，设备管理器 载入管理服务会被禁用。

注意 目前，思科不提供将 设备管理器 配置迁移到 管理中心 的选项，反之亦然。选择为 威胁防御 设备配置的管理类型时，请考虑这一点。

在 Nutanix 上部署的前提条件

- 从 Cisco.com 下载 Threat Defense Virtual qcow2 文件：https://software.cisco.com/download/navigator.html

注释 需要 Cisco.com 登录信息和思科服务合同。

- 查看概述，第 1 页一章。
- 有关 Nutanix 和系统兼容性，请参阅《Cisco Secure Firewall Threat Defense 兼容性指南》 。

如何在 Nutanix 上部署 Threat Defense Virtual

步骤	任务	更多信息
1	查看先决条件。	在 Nutanix 上部署的前提条件，第 8 页
2	将 threat defense virtual qcow2 文件上传到 Nutanix 环境。	将 Threat Defense Virtual QCOW2 文件上传到 Nutanix，第 8 页
3	（可选）准备一个 Day 0 配置文件，其中包含了在部署虚拟机时需要应用的初始配置数据。	准备 Day 0 配置文件，第 9 页
4	将 threat defense virtual 部署到 Nutanix 环境。	部署 Threat Defense Virtual，第 11 页
5	（可选）如果未使用 Day 0 配置文件来设置 threat defense virtual，请通过登录 CLI 来完成设置。	完成 Threat Defense Virtual 设置，第 13 页

将 Threat Defense Virtual QCOW2 文件上传到 Nutanix

要将 threat defense virtual 部署到 Nutanix 环境，则必须在 Prism Web 控制台中从 threat defense virtual qcow2 磁盘文件创建映像。

开始之前

从 Cisco.com 下载 threat defense virtual qcow2 磁盘文件：https://software.cisco.com/download/navigator.html

过程

步骤 1 登录到 Nutanix Prism Web 控制台。

步骤 2 打击齿轮图标打开**设置 (Settings)** 页面。

步骤 3 点击左侧窗格中的**映像配置 (Image Configuration)**。

步骤 4 点击**上传映像 (Upload Image)**。

步骤 5 创建映像。

1. 为映像输入名称。
2. 从**映像类型 (Image Type)** 下拉列表中选择**磁盘 (DISK)**。
3. 从**存储容器 (Storage Container)** 下拉列表中选择所需的容器。
4. 指定 threat defense virtual qcow2 磁盘文件的位置。

   您可以指定 URL（以便从 Web 服务器导入文件）或从工作站上传文件。
5. 点击**保存 (Save)**。

步骤 6 请等待，直到新映像出现在**映像配置 (Image Configuration)** 页面中。

准备 Day 0 配置文件

在部署 threat defense virtual 之前，您可以准备一个 Day 0 配置文件。此文件是一个文本文件，其中包含了在部署虚拟机时需要应用的初始配置数据。

请记住：

- 如果使用 Day 0 配置文件进行部署，该过程将允许您执行 threat defense virtual 设备的整个初始设置。
- 如果您在没有 Day 0 配置文件的情况下进行部署，则必须在启动后配置系统所需的设置；有关更多信息，请参阅完成 Threat Defense Virtual 设置，第 13 页。

可以指定：

- 接受《最终用户许可协议》(EULA)。
- 系统的主机名。
- 管理员账户的新管理员密码。

- 初始防火墙模式；设置初始防火墙模式：**已路由**或**透明**。

  如果您打算使用本地 设备管理器 管理部署，可以仅为防火墙模式输入**已路由**。不能使用 设备管理器 配置透明防火墙模式接口。

- 管理模式；请参阅如何管理 Cisco Secure Firewall Threat Defense Virtual 设备。

  您可以将**本地管理**设置为**是**，或者输入 管理中心 字段（**FmcIp**、**FmcRegKey** 和 **FmcNatId**）的信息。对于您未使用的管理模式，保留字段为空。

- 使设备可以在管理网络上进行通信的网络设置。

过程

步骤 1 使用您选择的文本编辑器来创建一个新的文本文件。

步骤 2 在文本文件中输入配置详细信息，如下例所示：

示例：

```
#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"
}
```

注释

Day 0 配置文件的内容必须采用 JSON 格式。您必须使用 JSON 验证器工具来验证文本。

步骤 3 将文件另存为“**day0-config.txt**”。

步骤 4 为每个要部署的 threat defense virtual 重复步骤 1-3 以创建唯一的默认配置文件。

部署 Threat Defense Virtual

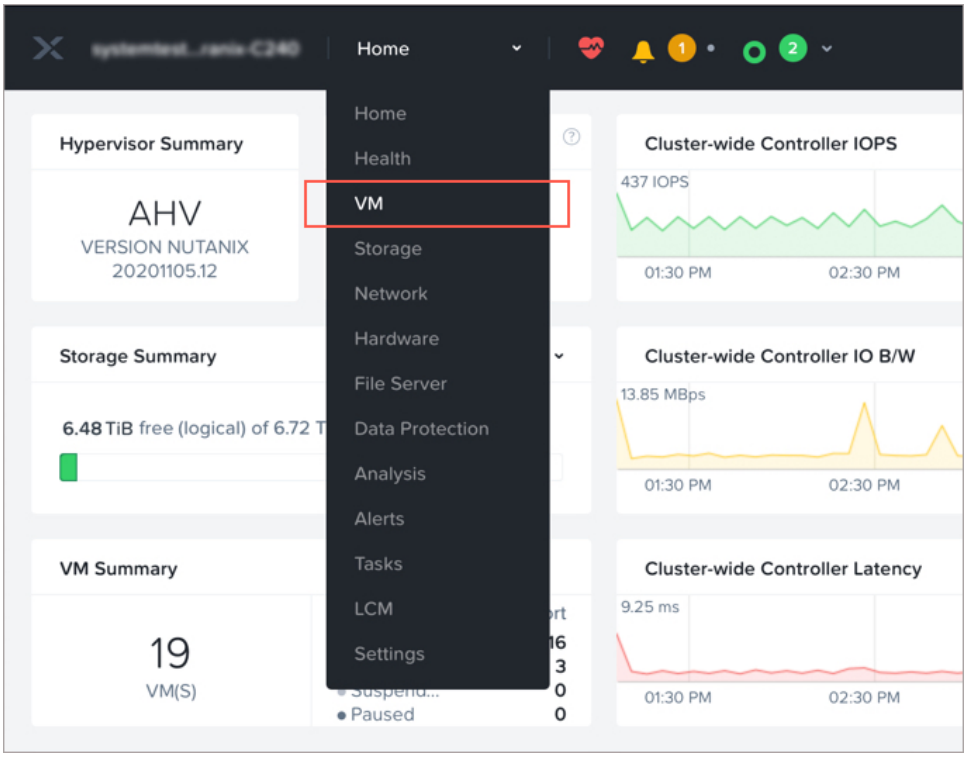
开始之前

确保您计划部署的 threat defense virtual 的映像显示在**映像配置 (Image Configuration)** 页面上。

过程

步骤 1 登录到 Nutanix Prism Web 控制台。

步骤 2 从主菜单栏中，点击视图下拉列表，然后选择 **VM**。



步骤 3 在 VM 控制面板上，点击**创建 VM (Create VM)**。

步骤 4 执行以下操作：

1. 输入 threat defense virtual 实例的名称。
2. （可选）输入 threat defense virtual 实例的说明。
3. 选择您希望 threat defense virtual 实例使用的时区。

步骤 5 输入计算详细信息。

1. 输入要分配给 threat defense virtual 实例的虚拟 CPU 数量。
2. 输入必须分配给每个虚拟 CPU 的核心数。

3. 输入要分配给 threat defense virtual 实例的内存量 (GB)。

步骤 6 将磁盘连接到 threat defense virtual 实例。

1. 在**磁盘 (Disks)**，点击**添加新磁盘 (Add New Disk)**。
2. 从**类型 (Type)** 下拉列表中选择**磁盘 (DISK)**。
3. 从**操作 (Operation)** 下拉列表中，选择**从映像服务克隆 (Clone from Image Service)**。
4. 从**总线类型 (Bus Type)** 下拉列表中，选择 **PCI** 或 **SCSI**。
5. 从**映像 (Image)** 下拉列表中，选择要使用的映像。
6. 点击**添加 (Add)**。

步骤 7 配置至少四个虚拟网络接口。

在**网络适配器 (NIC) (Network Adapters [NIC])** 下，点击**添加新 NIC (Add New NIC)**，选择网络，然后点击**添加 (Add)**。

重复此过程以便添加更多网络接口。

Nutanix 上的 threat defense virtual 支持共计 10 个接口 - 一个管理接口、一个诊断接口，以及最多八个用于数据流量的网络接口。接口到网络分配必须遵循以下顺序：

- vnic0 - 管理接口（必需）
- vnic1 - 诊断接口（必需）
- vnic2 - 外部接口（必需）
- vnic3 - 内部接口（必需）
- vnic4-9 - 数据接口（可选）

步骤 8 配置 threat defense virtual 的关联策略。

在 **VM 主机关联 (VM Host Affinity)** 下，点击**设置关联 (Set Affinity)**，选择主机，然后点击**保存 (Save)**。

选择多个主机以确保即使节点出现故障也可运行 threat defense virtual。

步骤 9 如果您已准备了 Day 0 配置文件，请执行以下操作：

1. 选择**自定义脚本 (Custom Script)**。
2. 点击**上传文件 (Upload A File)**，，然后选择 Day 0 配置文件 (**day0-config.txt**)。

注释
此版本中不支持所有其他自定义脚本选项。

步骤 10 点击**保存 (Save)** 以部署 threat defense virtual。threat defense virtual 实例会显示在 VM 表格视图中。

步骤 11 在 VM 表格视图中，选择新创建的 threat defense virtual 实例，然后点击**打开电源 (Power On)**。

下一步做什么

- 如果您使用 Day 0 配置文件来设置 threat defense virtual，则后续步骤取决于您选择的管理模式。
  - 如果为**本地管理 (ManageLocally)**选择**否 (No)**，您将使用 管理中心 管理 threat defense virtual；请参阅使用 Cisco Secure Firewall Management Center 来管理 Cisco Secure Firewall Threat Defense Virtual。
- 如果未使用 Day 0 配置文件来设置 threat defense virtual，请通过登录 CLI 来完成 threat defense virtual 设置。有关说明，请参阅完成 Threat Defense Virtual 设置，第 13 页。

完成 Threat Defense Virtual 设置

由于 threat defense virtual 设备没有 Web 界面，如果您在没有 Day 0 配置文件的情况下进行部署，必须使用 CLI 来设置虚拟设备。

过程

步骤 1 打开 threat defense virtual的控制台。

步骤 2 在 **firepower login** 提示符下，使用默认凭据（**username** *admin*，**password** *Admin123*）登录。

步骤 3 当 threat defense virtual 系统启动时，安装向导会提示您执行以下操作，并输入配置系统所需的下列信息：

- 接受 EULA
- 新管理员密码
- IPv4 或 IPv6 配置
- IPv4 或 IPv6 DHCP 设置
- 管理端口 IPv4 地址和子网掩码，或者 IPv6 地址和前缀
- 系统名称
- 默认网关
- DNS 设置
- HTTP 代理
- 管理模式（需要进行本地管理）

步骤 4 检查设置向导的设置。默认值或以前输入的值会显示在括号中。要接受之前输入的值，请按 **Enter** 键。

步骤 5 根据提示完成系统配置。

步骤 6 当控制台返回到 # 提示符时，验证设置是否成功。

步骤 7 关闭 CLI。

下一步做什么

接下来的步骤取决于您选择的管理模式。

- 如果为**启用本地管理器 (Enable Local Manager)** 选择**否 (No)**，您将使用 管理中心 管理 threat defense virtual；请参阅使用 Cisco Secure Firewall Management Center 来管理 Cisco Secure Firewall Threat Defense Virtual。

有关如何选择管理选项的概述，请参阅如何管理 Cisco Secure Firewall Threat Defense Virtual 设备。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。