# 在思科 HyperFlex 上部署 Threat Defense Virtual

本章介绍在 vCenter 服务器或独立 ESXi 主机上的思科 HyperFlex 上部署 threat defense virtual 的程序。



## 概述

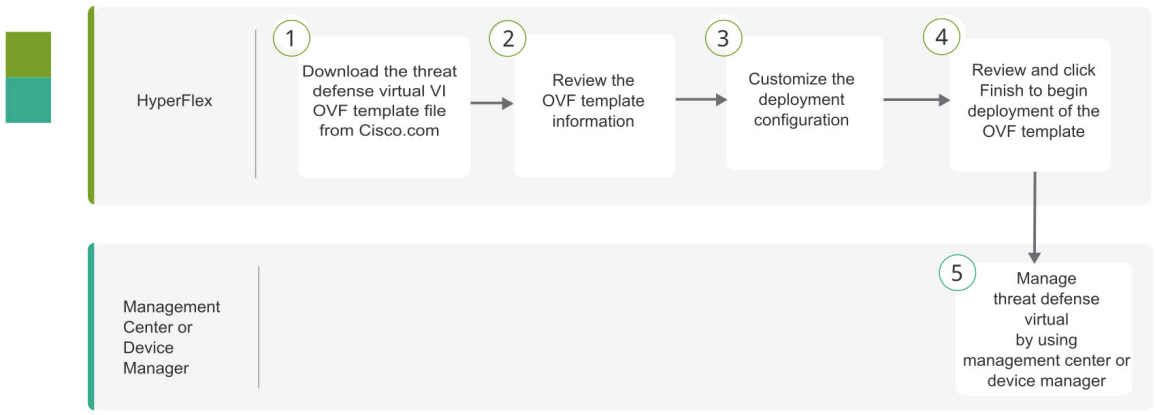
Cisco Cisco Secure Firewall Threat Defense Virtual （之前称为 Firepower Threat Defense Virtual）将 Cisco Secure Firewall 功能带到虚拟环境，支持采用一致的安全策略来跟踪物理、虚拟和云环境以及云之间的工作负载。

HyperFlex 系统可为任何应用程序和任何位置提供超融合。通过思科 Intersight 云运营平台管理的 HyperFlex 采用了思科统一计算系统 (Cisco UCS) 技术，可以在任何地方为应用程序和数据提供支持，优化从核心数据中心到边缘和公共云的运营，从而通过加速 DevOps 实践来提高灵活性。

本章介绍 threat defense virtual 如何在思科 HyperFlex 环境中工作，包括功能支持、系统要求、准则和限制。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 （以前称为 Firepower Management Center）或 Cisco Secure Firewall 设备管理器 （以前称为 Firepower Device Manager）来管理和监控 threat defense virtual。其他管理选项也可能可用。

# 端到端程序

以下流程图说明了在思科 HyperFlex 上部署 Threat Defense Virtual 的工作流程。




| | 工作空间 | 步骤 |
|---|---|---|
| 1 | Hyperflex | 部署 Threat Defense Virtual：从 Cisco.com 下载Threat Defense Virtual VI OVF 模板文件。 |
| 2 | Hyperflex | 部署 Threat Defense Virtual：查看 OVF 模板信息。 |
| 3 | Hyperflex | 部署 Threat Defense Virtual：自定义部署配置。 |
| 4 | Hyperflex | 部署 Threat Defense Virtual：查看并验证显示的信息。点击“完成”(Finish) 开始部署 OVF 模板。 |
| 5 | 管理中心或设备管理器 | 管理 Threat Defense Virtual：<br>• 使用管理中心<br>• 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、磁盘和 vCPU 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**<br>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。<br>• FTDv5 4vCPU/8GB (100Mbps)<br>• FTDv10 4vCPU/8GB (1Gbps)<br>• FTDv20 4vCPU/8GB (3Gbps)<br>• FTDv30 8vCPU/16GB (5Gbps)<br>• FTDv50 12vCPU/24GB (10Gbps)<br>• FTDv100 16vCPU/32GB (16Gbps)<br>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。<br>**注释**<br>要更改 vCPU/内存值，必须先关闭 threat defense virtual 设备的电源。 |
| 存储 | 取决于所选磁盘格式。<br>• 调配磁盘大小为 48.24 GB。 |
| vNIC | threat defense virtual 支持以下虚拟网络适配器：<br>• **VMXNET3**-在 threat defense virtual 上，如果创建虚拟设备，现默认为 VMXNET3 接口。先前，默认值为 e1000。（7.1 及更高版本）vmxnet3 驱动程序使用第一个以太网适配器进行管理。第二个适配器未使用。（7.0 及更早版本）<br>VMXNET3 驱动程序使用两个管理接口。前两个以太网适配器必须配置为管理接口：一个用于设备管理/注册，一个用于诊断。 |

### 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。

### HyperFlex HX 系列的配置和集群

| 配置 | 集群 |
|---|---|
| HX220c 融合节点 | • 闪存集群<br>• 最少 3 个节点集群（数据库、VDI、VSI） |
| HX240c 融合节点 | • 闪存集群<br>• 最少 3 个节点集群（VSI：IT/商业应用、测试/开发） |
| HX220C 和 Edge（VDI、VSI、ROBO）<br>HX240C（VDI、VSI、测试/开发 | • 混合集群<br>• 最少 3 个节点集群 |
| B200 + C240/C220 | 计算绑定应用/VDI |

HyperFlex HX 系列的部署选项：

- 混合集群
- 闪存集群
- HyperFlex 边缘
- SED 驱动器
- NVME 缓存
- GPU

有关 HyperFlex HX 云支持的管理选项，请参阅思科 HyperFlex 系统安装指南中的部署 *HyperFlex* 交换矩阵互联连接的集群部分。

### HyperFlex 组件和版本

| 组件 | 版本 |
|---|---|
| VMware vSphere/VMware ESXI | 7.0<br>有关威胁防御虚拟与 VMware vSphere/VMware ESXI 的兼容性的详细信息，请参阅威胁防御虚拟兼容性：VMware。 |

| 组件 | 版本 |
| --- | --- |
| HyperFlex 数据平台 | 4.5.1a-39020 及更高版本<br>。 |

# 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
- 巨型帧
- HyperFlex 数据中心集群（不包括扩展集群）
- HyperFlex Edge 集群
- HyperFlex 全 NVMe、全闪存和混合融合节点
- HyperFlex 纯计算节点

### 不支持的功能

与 SR-IOV 一起运行的 Threat Defense Virtual 尚未通过 HyperFlex 的认证。

注释 HyperFlex 支持 SR-IOV，但除 MLOM VIC 外还需要 PCI-e NIC。

### 一般准则

要为 HyperFlex 配置 vSwitch，可以使用 GUI 或命令行界面。在安装多个 ESX 服务器并计划编写 vSwitch 配置脚本时，这些配置非常有用。有关详细信息，请参阅《思科 HyperFlex 系统网络和外部存储管理指南》中的“配置 vSwitch”部分。

以下是 threat defense virtual 接口的网络适配器、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 |
| --- | --- | --- | --- |
| 网络适配器 1 | Management0-0 | Management0/0 | 管理 |
| 网络适配器 2 | Diagnostic0-0 | 诊断 | 诊断 |

| 网络适配器 | 源网络 | 目标网络 | 功能 |
|---|---|---|---|
| 网络适配器 3 | GigabitEthernet0-0 | GigabitEthernet0/0 | 外部 |
| 网络适配器 4 | GigabitEthernet0-1 | GigabitEthernet0/1 | 内部 |
| 网络适配器 5 | GigabitEthernet0-2 | GigabitEthernet0/2 | 数据流量（可选） |
| 网络适配器 6 | GigabitEthernet0-3 | GigabitEthernet0/3 | 数据流量（可选） |
| ...直到网络适配器 10 | | | |

### 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 HyperFlex 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。

## 修改 vSphere 标准交换机的安全策略设置

对于 vSphere 标准交换机，第 2 层安全策略的三个要素分别是混合模式、MAC 地址更改和伪传输。threat defense virtual 在混合模式下运行，并且 threat defense virtual 的高可用性依赖于主用和备用设备之间的 MAC 地址切换，从而保证正确运行。

默认设置会阻碍 threat defense virtual 的正确运行。请参见以下要求的设置：

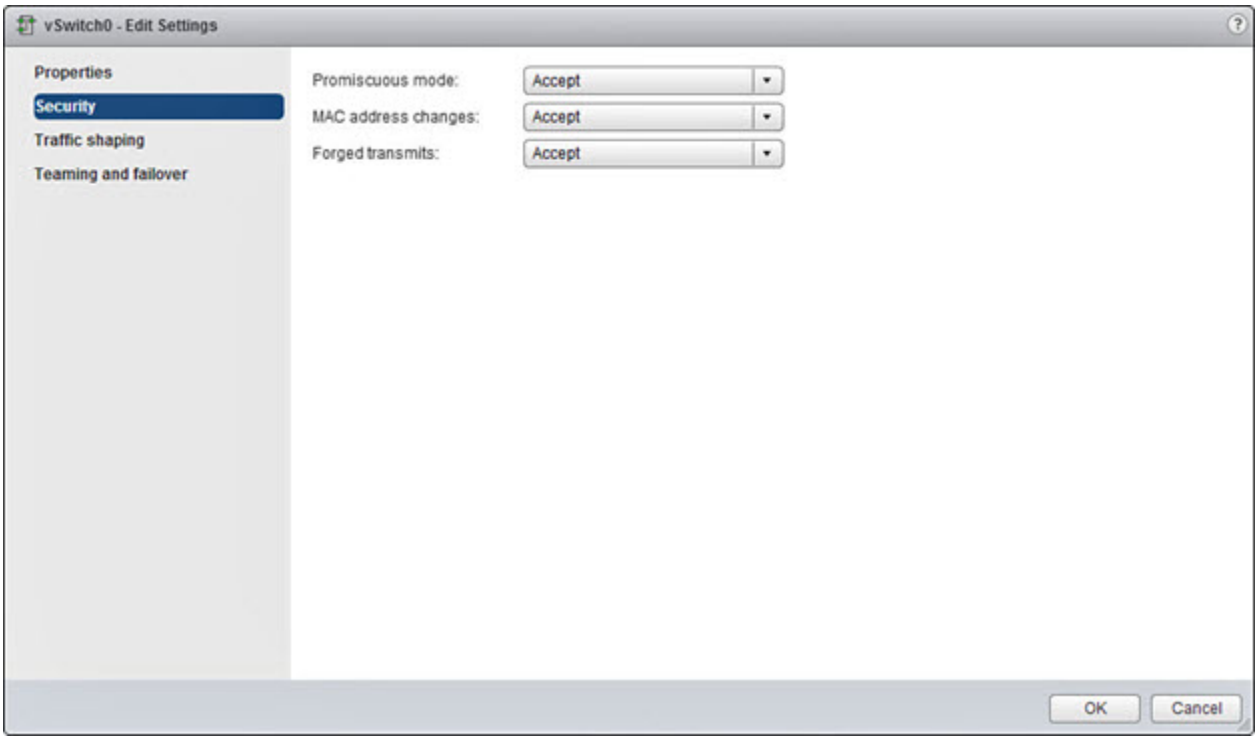
表 *1: vSphere* 标准交换机安全策略选项

| 选项 | 要求的设置 | 操作 |
| --- | --- | --- |
| 混合模式 | 接受 | 您必须在 vSphere Web 客户端中编辑 vSphere 标准交换机的安全策略，并将混合模式选项设置为“接受”。<br>防火墙、端口扫描程序、入侵检测系统等等需要在混合模式下运行。 |
| MAC 地址更改 | 接受 | 您应该在 vSphere Web 客户端中检验 vSphere 标准交换机的安全策略，确认 MAC 地址更改选项已设为“接受”。 |
| 伪传输 | 接受 | 您应该在 vSphere Web 客户端中检验 vSphere 标准交换机的安全策略，确认伪传输选项已设为“接受”。 |

使用以下程序配置 threat defense virtual 的正确操作的默认设置。

1. 在 vSphere Web 客户端中，导航至 HyperFlex 集群。
2. 在**管理**选项卡中，点击**网络**，然后选择**虚拟交换机**。
3. 从列表中选择一个标准交换机，然后点击**编辑设置**。
4. 选择**安全**，查看当前设置。
5. 在连接到标准交换机的虚拟机的访客操作系统中**接受**混合模式激活、MAC 地址更改和伪传输。

图 *1: vSwitch* 编辑设置




6. 点击**确定**。

注释 确保在为 threat defense virtual 上的管理和故障切换 (HA) 接口所配置的所有网络上，这些设置是相同的。

### 相关文档

思科 HX 数据平台的版本说明

Cisco HX 数据平台配置指南

适用于采用 VMware ESXi 的虚拟服务器基础设施的思科 HyperFlex 4.0

思科 HyperFlex 系统解决方案概述

思科 HyperFlex 系统文档规划图

# 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。

# Cisco Secure Firewall 设备管理器

设备管理器 板载集成的管理器。

设备管理器 是基于 Web 的配置界面，包含在某些 威胁防御 设备上。设备管理器可以配置小型网络最常用软件的基本功能。此产品专为包括一台或几台设备的网络而设计，在这种网络中，无需使用高功率多设备管理器来控制包含许多 威胁防御 设备的大型网络。

**注释** 有关支持 设备管理器 的 威胁防御 设备的列表，请参阅《Cisco Secure Firewall 设备管理器配置指南》。

# 概述

您可以在 VMware vCenter 服务器上将 threat defense virtual 部署到思科 HyperFlex。

要成功部署 threat defense virtual，您必须熟悉 VMware 和 vSphere，包括 vSphere 联网、ESXi 主机设置和配置，以及虚拟机访客部署。

适用于思科 HyperFlex 的 threat defense virtual 使用开放虚拟化格式 (OVF) 进行分发，这是一种打包和部署虚拟机的标准方法。VMware 提供多种调配 vSphere 虚拟机的方法。适合您环境的最佳方式取决于您基础设施的规模和类型以及您想要实现的目标。

您可以使用 VMware vSphere Web 客户端访问您的思科 HyperFlex 环境。

# 部署 Threat Defense Virtual

使用此程序将 threat defense virtual 设备部署到 vSphere vCenter 服务器上的思科 HyperFlex。

### 开始之前

- 确保您已部署思科 HyperFlex 并执行了所有安装后配置任务。有关详细信息，请参阅思科 HyperFlex 系统文档规划图。
- 在部署 threat defense virtual 之前，您必须在 vSphere 中配置至少一个网络（用于管理）。
- 从 Cisco.com 下载 threat defense virtual VI OVF 模板文件：*Cisco_Secure_Firewall_Threat_Defense_Virtual-VI-X.X.X-xxx.ovf*，其中 *X.X.X-xxx* 是版本和内部版本号。

### 过程

**步骤 1** 登录 vSphere Web 客户端。

**步骤 2** 选择要部署 threat defense virtual 的 HyperFlex 集群，然后点击**操作 (ACTIONS)** > **部署 OVF 模板 (Deploy OVF Template)**。

**步骤 3** 浏览文件系统以找到 OVF 模板源位置，然后点击**下一步 (NEXT)**。

选择 threat defense virtual VI OVF 模板：

*Cisco_Secure_Firewall_Threat_Defense_Virtual-VI-X.X.X-xxx.ovf*

其中，*X.X.X-xxx* 是已下载的存档文件的版本和内部版本号。

**步骤 4** 为 threat defense virtual 指定名称和位置，然后点击**下一步 (NEXT)**。

**步骤 5** 选择计算资源，并等待兼容性检查完成。

如果兼容性检查成功，请点击**下一步 (NEXT)**。

**步骤 6** 查看 OVF 模板信息（产品名称、版本、供应商、下载大小、磁盘上的大小和说明），然后点击**下一步 (NEXT)**。

**步骤 7** 审查并接受与 OVF 模板一起打包的许可协议（仅限 VI 模板），然后点击**下一步 (NEXT)**。

**步骤 8** 选择部署配置（vCPU/内存值），然后点击**下一步 (NEXT)**。

**步骤 9** 选择存储位置和虚拟磁盘格式，然后点击**下一步 (NEXT)**。

在此窗口中，您可以从目标 HyperFlex 集群上已配置的数据存储中选择。存储在数据存储上的虚拟机配置文件和虚拟磁盘文件。选择一个足够大的数据存储，以容纳虚拟机及其所有虚拟磁盘文件。

如果选择**密集调配 (Thick Provisioned)** 作为虚拟磁盘格式，则会立即分配所有存储。如果选择**精简调配 (Thin Provisioned)** 作为虚拟磁盘格式，则会在数据写入虚拟磁盘时将按需分配存储。精简调配还可缩短虚拟设备的部署时间。

**步骤 10** 将 OVF 模板中指定的网络映射到清单中的网络，然后点击**下一步 (NEXT)**。

确保将 Management0-0 接口关联到可以从互联网访问的 VM 网络。非管理接口可从 管理中心 或 设备管理器 配置，具体取决于您的管理模式。

网络可能没有按字母顺序排序。如果很难找到您的网络，可以稍后在**编辑设置**对话框中更改网络。在部署后，右键点击 threat defense virtual 实例，然后选择**编辑设置**。但是，该屏幕不会显示 threat defense virtual ID（仅显示网络适配器 ID）。

请查看适用于 threat defense virtual 接口的以下网络适配器、源网络和目标网络的一致性（注意这些是默认的 vmxnet3 接口）：

| 网络适配器 | 源网络 | 目标网络 | 功能 |
|---|---|---|---|
| 网络适配器 1 | Management0-0 | Management0/0 | 管理 |
| 网络适配器 2 | Diagnostic0-0 | Diagnostic0/0 | 诊断 |
| 网络适配器 3 | GigabitEthernet0-0 | GigabitEthernet0/0 | 外部数据 |
| 网络适配器 4 | GigabitEthernet0-1 | GigabitEthernet0/1 | 内部日期 |
| 网络适配器 5 | GigabitEthernet0-2 | GigabitEthernet0/2 | 数据流量（可选） |
| 网络适配器 6 | GigabitEthernet0-3 | GigabitEthernet0/3 | 数据流量（可选） |
| 网络适配器 7 | GigabitEthernet0-4 | GigabitEthernet0/4 | 数据流量（可选） |
| 网络适配器 8 | GigabitEthernet0-5 | GigabitEthernet0/5 | 数据流量（可选） |
| 网络适配器 9 | GigabitEthernet0-6 | GigabitEthernet0/6 | 数据流量（可选） |
| 网络适配器 10 | GigabitEthernet0-7 | GigabitEthernet0/7 | 数据流量（可选） |

部署 threat defense virtual 时，总共可以有 10 个接口。如果添加额外的数据接口，请确保源网络映射到正确的目标网络，而且每个数据接口都映射到一个唯一的子网或 VLAN。您无需使用 threat defense virtual 的所有接口。对于您不打算使用的接口，只需在 threat defense virtual 配置中禁用即可。

**步骤 11** 设置与 OVF 模板一起打包的用户可配置的属性：

**注释**
建议在此步骤中强制配置所有必需的自定义设置。如果未配置所有必需的自定义，则必须在部署后登录 CLI 以完成设置。有关说明，请参阅使用 CLI 完成 Threat Defense Virtual 设置，第 13 页。

a) **密码**

设置 threat defense virtual 管理员访问的密码。

b) **网络**

设置网络信息，包括完全限定的域名 (FQDN)、DNS、搜索域和网络协议（IPv4 或 IPv6）。

c) **管理**

设置管理模式。点击**启用本地管理器**的下拉箭头，然后选择**是**使用集成的基于 Web 的 设备管理器配置工具。选择**否 (No)** 以使用 管理中心 来管理此设备。

d) 防火墙模式

设定初始防火墙模式。点击**防火墙模式**的下拉箭头，然后选择两种支持的模式之一；**已路由**或**透明**。

如果对**启用本地管理器**选择**是**，则只能选择**已路由**防火墙模式。不能使用本地 设备管理器 配置透明防火墙模式接口。

e) 注册

如果对**启用本地管理器**选择**否**，则需要提供必要的凭证以将此设备注册到负责管理的 **Firepower 管理中心**。提供以下各项：

- **负责管理的防御中心** - 输入 管理中心 的主机名或 IP 地址。
- **注册密钥** - 注册密钥是由用户生成的一次性使用密钥，长度不超过 37 个字符。有效字符包括字母数字（A－Z、a－z、0－9）和连字符 (-)。当将设备添加到 管理中心时，您必须记住此注册密钥。
- **NAT ID** - 如果 threat defense virtual 和 管理中心 被网络地址转换 (NAT) 设备分隔，并且 管理中心 位于 NAT 设备后方，请输入一个唯一的 NAT ID。这是由用户生成的一次性使用密钥，长度不超过 37 个字符。有效字符包括字母数字（A－Z、a－z、0－9）和连字符 (-)。

f) 点击**下一步 (NEXT)**。

**步骤 12** 查看并验证显示的信息。要使用这些设置开始部署，点击**完成 (FINISH)**。要进行更改，点击**后退 (BACK)** 以在屏幕中向后导航。

完成该向导后，vSphere Web 客户端将处理虚拟机；您可以在**全局信息**区域的**最近任务**窗格中看到“初始化 OVF 部署”状态。

完成后，您会看到“部署 OVF 模板”完成状态。

在“清单”中的指定数据中心下会显示 threat defense virtual 虚拟实例。启动新的 VM 最多可能需要 30 分钟。

**注释**
要向思科许可颁发机构成功注册 threat defense virtual，threat defense virtual需要访问互联网。部署之后，需要执行其他配置，以实现互联网访问和成功注册许可证。

---

### 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。

**注释** 如果在部署 threat defense virtual 时未配置所有必需的自定义，则必须使用 CLI 完成设置。有关说明，请参阅使用 CLI 完成 Threat Defense Virtual 设置，第 13 页。

# 使用 CLI 完成 Threat Defense Virtual 设置

如果在部署 threat defense virtual 时未配置所有必需的自定义，则必须使用 CLI 完成设置。

过程

**步骤 1** 打开 VMware 控制台。

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

**步骤 3** 当 威胁防御系统启动时，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（本地管理使用 设备管理器）。

**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。

当实施设置时，VMware 控制台可能显示消息。

**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。

**注释**
要向思科许可颁发机构成功注册 threat defense virtual，threat defense virtual需要访问互联网。部署之后，可能需要执行其他配置，以实现互联网访问和成功注册许可证。

### 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。

# 启用巨型帧

MTU 越大，能发送的数据包就越大。加大数据包可能有利于提高网络效率。请参阅以下准则：

- 匹配流量路径上的 MTU - 我们建议您将流量路径的所有 ASAv 接口及其他设备接口的 MTU 都设置为同一值。匹配 MTU 可防止中间设备对数据包进行分片。
- 容纳巨型帧 - MTU 最大可设置为 9198 字节。ASAv 的最大值为 9000。

此程序介绍如何在以下环境中启用巨型帧：

**vSphere 7.0.1 上的 HyperFlex 集群 > VMware vSphere vSwitch> 思科 UCS 交换矩阵互联 (FI)**。

过程

**步骤 1** 更改已部署 ASAv 的 ASAv 主机的 MTU 设置。

1. 使用 vSphere Web 客户端连接到 vCenter 服务器。
2. 在 HyperFlex 主机的**高级系统设置 (Advanced System Settings)** 中，将配置参数 `Net.Vmxnet3NonTsoPacketGtMtuAllowed` 的值设置为 `1`。
3. 保存更改，然后重启主机。

有关详细信息，请参阅https://kb.vmware.com/s/article/1038578。

**步骤 2** 更改 VMware vSphere vSwitch 的 MTU 设置。

1. 使用 vSphere Web 客户端连接到 vCenter 服务器。
2. 编辑 VMware vSphere vSwitch 的属性，并将 **MTU** 的值设置为 `9000`。

**步骤 3** 更改思科 UCS 交换矩阵互联 (FI) 的 MTU 设置。

1. 登录思科 UCS 管理控制台。
2. 要编辑 QoS 系统类，请选择 **LAN** > **LAN 云 (LAN Cloud)** > **QoS 系统类 (QoS System Class)**。在**常规 (General)** 选项卡下，将 **MTU** 的值设置为 9216。
3. 要编辑 vNIC，请选择 **LAN** > **策略 (Policies)** > **root** > **子组织 (Sub-Organizations)**

   <your-hyperflex-org>**vNIC 模板** <your-vnic>。在**常规 (General)** 选项卡下，将 **MTU** 的值设置为 9000。

# 故障排除

本节提供与虚拟机上的 Hyperflex 部署相关的一些基本故障排除步骤。

### 验证您的虚拟机是否正在运行 Hyperflex

如果在采用 ESX OS 的 HyperFlex 上安装了 threat defense virtual 设备，则在 threat defense virtual 启动时，由 HX post_install 脚本创建的默认 vSphere HA 策略会导致错误消息。错误消息将显示：

“启动故障：资源不足，无法满足为 vSphere HA 配置的故障转移级别。”(Power on Failures: Insufficient resources to satisfy configured failover level for vSphere HA.)

### 解决办法

1. 在 VMware vCenter 中，转至 **HX 集群 (HX cluster)** > **配置 (Configure)** > **vSphere 可用性 (vSphere Availability)** > **编辑 VSphere HA (Edit Vsphere HA)** > **准入控制 (Admission Control)** > **定义主机故障转移容量 (Define host failover capacity)** > **覆盖计算的故障转移容量 (Override calculated failover capacity)**。
2. 更改和调整预留的故障转移 CPU 和内存容量百分比。
3. 启动 threat defense virtual VM。

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。