在 VMware 上部署 Firewall Threat Defense Virtual

本章介绍将 Firewall Threat Defense Virtual 部署到 VMware vSphere 环境（vSphere vCenter 或独立式 ESXi 主机）的步骤。

- 概述， 第 1 页
- Firewall Threat Defense Virtual的 VMware 功能支持 ， 第 2 页
- 系统要求， 第 3 页
- 准则和限制， 第 7 页
- 如何管理 Secure Firewall Threat Defense Virtual 设备， 第 13 页
- 规划接口， 第 14 页
- 关于 VMware 部署， 第 18 页
- 端到端程序， 第 19 页
- 准备 Day0 配置文件， 第 21 页
- 将 Firewall Threat Defense Virtual 部署到 vSphere vCenter， 第 23 页
- 向 vSphere ESXi 主机部署 Firewall Threat Defense Virtual， 第 31 页
- 使用 CLI 完成 Firewall Threat Defense Virtual 设置， 第 35 页
- 提高 ESXi 配置的性能， 第 36 页
- NUMA 准则， 第 36 页
- VMware 上 Threat Defense Virtual 部署的最佳实践， 第 37 页
- SR-IOV 接口调配， 第 38 页

概述

思科为 VMware vSphere vCenter 和 ESXi 托管环境打包了 64 位 Firewall Threat Defense Virtual 设备。Firewall Threat Defense Virtual 以开放虚拟化格式 (OVF) 包分发，可从 Cisco.com 下载。OVF 是用于为虚拟机 (VM) 打包和分发软件应用程序的开放源标准。一个 OVF 包在一个目录中包含多个文件。

您可以将 Firewall Threat Defense Virtual 部署到能够运行 VMware ESXi 的任何 x86 设备上。要部署 Firewall Threat Defense Virtual，您应该熟悉 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。

Firewall Threat Defense Virtual的 VMware 功能支持

下表列出了 Firewall Threat Defense Virtual的 VMware 功能支持。

表 *1: Firewall Threat Defense Virtual*的 *VMware* 功能支持

功能	说明	支持（是/否）	备注
冷克隆	VM 在克隆过程中关闭。	否	–
vMotion	用于实时迁移 VM。	是	使用共享存储。请参阅 vMotion 支持。
分布式资源调度程序 (DRS)	监控虚拟机工作负载并解决不均衡问题，识别要使用 vMotion 进行实时迁移的虚拟机。	否	不符合条件
热添加	VM 在添加过程中运行。	否	–
热克隆	VM 在克隆过程中运行。	否	–
热删除	VM 在删除过程中运行。	否	–
快照	VM 会冻结几秒钟。	否	防火墙管理中心 与托管设备之间存在不同步情况的风险。
暂停和恢复	VM 暂停，然后恢复。	是	–
vCloud Director	允许自动部署 VM。	否	–
VMware FT	用于 VM 上的 HA。	否	使用故障转移功能进行 Firewall Threat Defense Virtual VM 故障转移。
带 VM 心跳信号的 VMware HA	用于 VM 故障。	否	使用故障转移功能进行 Firewall Threat Defense Virtual VM 故障转移。
VMware vSphere 独立 Windows 客户端	用于部署 VM。	是	–
VMware vSphere Web 客户端	用于部署 VM。	是	–

系统要求

有关 Firewall 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》。

根据所需部署的实例数量和使用要求，Firewall Threat Defense Virtual部署所使用的具体硬件可能会有所不同。每个 Firewall 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 和磁盘空间。

运行 VMware vCenter 服务器和 ESXi 实例的系统必须满足特定的硬件和操作系统要求。有关支持平台的列表，请参阅 VMware 在线兼容性指南。

表 *2: Firewall Threat Defense Virtual* 设备资源要求

设置	值
性能级别	Firewall 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。 请参阅*Cisco Secure Firewall Management Center* 管理指南中的“许可”一章，了解在许可 Firewall Threat Defense Virtual 设备时的准则。 **注释** 要更改 vCPU/内存值，必须先关闭 Firewall Threat Defense Virtual 设备的电源。
存储	取决于所选磁盘格式。 • 精简调配磁盘大小为 100 GB。

设置	值
vNIC	Firewall Threat Defense Virtual 支持以下虚拟网络适配器： • **VMXNET3** - 在 VMware 上，如果创建虚拟设备，Firewall Threat Defense Virtual 现默认为 vmxnet3 接口。先前，默认值为 e1000。 对于版本 10.0 及更高版本，当禁用诊断接口时，只需要一个管理接口。当**诊断**设置为“关闭”时，以前为诊断保留的第二个接口可用作数据接口。 • **E1000** - 使用 e1000 接口时，e1000 驱动程序的 Firewall Threat Defense Virtual 管理接口 (br1) 是具有两个 MAC 地址的桥接接口：一个用于管理，一个用于诊断。 **重要事项** 对于 6.4 之前的版本，在 VMware 上，e1000 是 Firewall Threat Defense Virtual 的默认接口。从 6.4 版开始，VMware 上的 Firewall Threat Defense Virtual 默认值为 vmxnet3 接口。如果您的虚拟设备当前使用的是 e1000 接口，**强烈建议**您更改接口 vmxnet3。有关详细信息，请参阅配置 VMXNET3 接口，第 17 页。
驱动因素	Firewall Threat Defense Virtual 支持以下驱动程序： • **IXGBE** - ixgbe 驱动程序使用两个管理接口。前两个 PCI 设备必须配置为管理接口：一个用于设备管理/注册，一个保留用于内部用途。驱动程序不支持 Firewall Threat Defense Virtual 的故障转移 (HA) 部署。 • **IXGBE-VF** - ixgbe-vf (10 Gbit/s) 驱动程序支持只能在支持 SR-IOV 的内核上激活的虚拟功能设备。SR-IOV 需要正确的平台和操作系统支持；有关详细信息，请参阅“对 SR-IOV 的支持”部分。 **重要事项** 对于 VMware 上具有桥接 ixgbe-vf 接口的 Threat Defense Virtual，不支持透明模式，且在路由模式下不支持网桥组。请参阅路由和透明模式接口准则和限制。

注释

- Threat Defense Virtual 10.0.0 支持在 VMware vSphere / ESXi 8.0 平台上部署。
- 在版本 10.0.0 中，默认磁盘大小设置为 100 GB，支持的最大大小为 500 GB。有关详细信息，请参阅Threat Defense Virtual 支持动态磁盘扩展。

对虚拟化技术的支持

- 虚拟化技术(VT)是新型处理器的一套增强功能，可提高运行虚拟机的性能。您的系统应配备支持英特尔 VT 或 AMD-V 扩展的 CPU，才能实现硬件虚拟化。英特尔和 AMD 都提供在线处理器识别实用程序来帮助您识别 CPU 并确定它们的性能。
- 许多服务器虽含有支持的 VT 的 CPU，但默认状态下会禁用 VT，您必须手动启用 VT。请查阅制造商文档，了解如何在您的系统中启用 VT 支持。

注释 如果您的 CPU 支持 VT，但您在 BIOS 中没有看到此选项，请联系您的供应商，获取可让您启用 VT 支持的 BIOS 版本。

禁用超线程

我们建议您为运行 Firewall Threat Defense Virtual 的系统禁用超线程；请参阅不推荐使用超线程，第 9 页。以下处理器支持超线程，每个核心有两个线程：

- 基于 Intel Xeon 5500 处理器微架构的处理器。
- Intel Pentium 4（支持 HT）
- Intel Pentium EE 840（启用 HT）

要禁用超线程，必须先在系统的 BIOS 设置中将其禁用，然后在 vSphere 客户端中将其关闭（请注意，默认为 vSphere 启用超线程）。请参阅系统文档，以确定您的 CPU 是否支持超线程。

对 SR-IOV 的支持

SR-IOV 虚拟功能需要特定的系统资源。除支持 SR-IOV 功能的 PCIe 适配器之外，还需要支持 SR-IOV 的服务器。您必须了解以下硬件注意事项：

- 不同供应商和设备的 SR-IOV NIC 功能有所不同，包括可用的 VF 数量。支持以下 NIC：
  - Intel 以太网服务器适配器 X520 - DA2
  - Intel 以太网服务器适配器 X540
- 并非所有 PCIe 插槽都支持 SR-IOV。
- 支持 SR-IOV 的 PCIe 插槽可能具有不同的功能。
- x86_64 多核 CPU - Intel 沙桥或更高版本（推荐）。

注释 我们在 Intel 的 Broadwell CPU (E5-2699-v4) 上以 2.3Ghz 的频率对 Firewall Threat Defense Virtual 进行了测试。

- 核心

- 每个 CPU 插槽至少 8 个物理核心

注释 Firewall Threat Defense Virtual 不支持物理核心的多非一致内存访问 (NUMA) 节点和多个 CPU 插槽。

- 确保将所有已分配的物理核心分配到单个插槽。

注释 建议通过 CPU 固定来实现完整的吞吐量。

请查阅制造商的文档，以了解系统对 SR-IOV 的支持情况。可以搜索 VMware 联机兼容性指南，了解包含 SR-IOV 支持的系统建议。

对 SSSE3 的支持

- Firewall Threat Defense Virtual 要求您的系统支持英特尔命名的 Supplemental Streaming SIMD Extensions 3（SSSE3 或 SSE3S），这是一种单指令流多数据流 (SIMD) 指令集。
- 您的系统应配备支持 SSSE3 的 CPU，例如 Intel Core 2 Duo、Intel Core i7/i5/i3、Intel Atom、AMD Bulldozer、AMD Bobcat 和更高版本的处理器。
- 请参阅此参考页面，进一步了解 SSSE3 指令集和支持 SSSE3 的 CPU。

验证 CPU 支持

您可以使用 Linux 命令行获取 CPU 硬件的相关信息。例如，**/proc/cpuinfo** 文件包含每个 CPU 核心的详细信息。运行 **less** 或 **cat** 命令，可输出其中的内容。

您可以前往“flags”部分查看以下值：

- vmx - Intel VT 扩展
- svm - AMD-V 扩展
- ssse3 - SSSE3 扩展

要查看文件中是否包含这些值，请使用 **grep** 运行以下命令：

```
egrep “vmx|svm|ssse3” /proc/cpuinfo
```

如果您的系统支持 VT 或 SSSE3，您会在“flags”列表中看到 vmx、svm 或 ssse3。以下示例显示了含有两种 CPU 的系统的输出：

```
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

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
```

固件支持

- 默认情况下，使用 UEFI 模式部署 Threat Defense Virtual 实例。用户可以在部署后、启动 VM 前启用安全启动。
- ESXi 主机应能够支持 UEFI 模式。请参阅 VMware 文档中了解如何在访客虚拟机上启用 UEFI 支持。

注释 不支持将启动模式从 UEFI 更改为 BIOS。

准则和限制

Firewall Threat Defense Virtual 智能许可的性能层

Firewall Threat Defense Virtual 支持性能层许可，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。

表 *3:* 基于授权的 *Firewall Threat Defense Virtual* 许可功能限制

性能层	设备规格（核心/RAM）	速率限制	RA VPN 会话限制
FTDv5，100Mbps	4 核/8 GB	100Mbps	50
FTDv10，1Gbps	4 核/8 GB	1Gbps	250
FTDv20，3Gbps	4 核/8 GB	3 Gbps	250
FTDv30，5Gbps	8 核/16 GB	5Gbps	250
FTDv50，10Gbps	12 核/24 GB	10Gbps	750
FTDv100，16Gbps	16 核/32 GB	16Gbps	10,000
FTDvU	32 核/64 GB	不受限制	20,000
FTDvU	64 核/128 GB	不受限制	32,000

请参阅*Cisco Secure Firewall Management Center* 管理指南中的“许可”一章，了解在许可 Firewall Threat Defense Virtual 设备时的准则。

性能优化

为实现 Firewall 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，请参阅提高 ESXi 配置的性能，第 36 页、NUMA 准则，第 36 页和SR-IOV 接口调配，第 38 页。

接收端扩展 - Firewall 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。RSS 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。

集群

从版本 7.2 开始，在 VMware 上部署的 Threat Defense Virtual 实例支持集群。有关详细信息，请参阅私有云中 Threat Defense Virtual 的集群。

管理模式

- 您可以通过两种方法来管理您的 Cisco Secure Firewall Threat Defense（之前称为 Firepower Threat Defense）设备。
  - 防火墙设备管理器 板载集成的管理器。

注释 VMware 上的 Firewall Threat Defense Virtual 支持运行思科 6.2.2 及更高版本软件的 防火墙设备管理器。VMware 上任何运行 6.2.2 版之前软件的 Firewall Threat Defense Virtual 只能使用 防火墙管理中心管理；请参阅如何管理 Secure Firewall Threat Defense Virtual 设备

  - 防火墙管理中心。

- 必须安装新版映像（6.2.2 或更高版本）才能取得 防火墙设备管理器支持。不能在从较低版本（低于 6.2.2）更新现有 Firewall Threat Defense Virtual 计算机后切换至 防火墙设备管理器。
- 防火墙设备管理器 （本地管理器）默认启用。

注释 当**启用本地管理器**选项设置为**是**时，防火墙模式会变为“已路由”。这是使用 防火墙设备管理器 时唯一受支持的模式。

部署

运行版本 7.4.3 或更高版本的 Threat Defense Virtual 实例会在首次启动期间执行多项初始化任务，这会导致控制台在大约五分钟后可用。这种延迟是正常的。如果设备在首次启动后大约两分钟内关闭，重要的初始化步骤可能会中断，从而可能导致设置不完整和意外行为。

要解决此问题，必须使用新映像重新安装虚拟平台。

OVF 文件准则

安装 Firewall Threat Defense Virtual的可用选项如下：

```
Cisco_Secure_Firewall_Threat_Defense_Virtual-VI-X.X.X-xxx.ovf
Cisco_Secure_Firewall_Threat_Defense_Virtual-ESXi-X.X.X-xxx.ovf
```

其中，X.X.X-xxx 是要使用的文件的版本和内部版本号。

- 如果使用 VI OVF 模板部署，安装过程中，您可以执行 Firewall Threat Defense Virtual 设备的整个初始设置。可以指定：
  - 管理员账户的新密码。
  - 使设备可以在管理网络上进行通信的网络设置。
  - 管理模式 - 使用 防火墙设备管理器 进行本地管理（默认），或者使用 防火墙管理中心 进行远程管理。
  - 防火墙模式 - 当启用本地管理器选项设置为是时，防火墙模式会变为已路由。这是使用 防火墙设备管理器 时唯一受支持的模式。

注释 必须使用 VMware vCenter 管理此虚拟设备。

- 如果使用 ESXi OVF 模板部署，必须在安装后配置系统所需的设置。您可以将此 Firewall Threat Defense Virtual 作为 ESXi 上的独立设备管理；有关详细信息，请参阅向 vSphere ESXi 主机部署 Firewall Threat Defense Virtual，第 31 页。

无法在 vSphere 7.0.2 中保存虚拟机 (VM) 配置

如果使用的是 vSphere 7.0.2，则可能不允许保存 VM 配置。

注释 您可以按照 VMware 知识库文章中的说明解决此问题：https://kb.vmware.com/s/article/83898。

vMotion 支持

如果计划使用 vMotion，建议仅使用共享存储。在部署期间，如果有主机集群，则可以在本地（特定主机上）或在共享主机上调配存储。但是，如果您尝试使用 vMotion 将 Cisco Secure Firewall Management Center Virtual（之前称为 Firepower Management Center Virtual）迁移到另一台主机，则使用本地存储将会产生错误。

不推荐使用超线程

超线程技术允许单个物理处理器内核像两个逻辑处理器一样运行。我们建议您为运行 Firewall Threat Defense Virtual 的系统禁用超线程。Snort 进程已经最大限度地利用了 CPU 内核的处理资源。当尝试通过每个处理器推动两个 CPU 使用率线程时，性能不会有任何提高。实际上，由于超线程进程所需的开销，您可能还会看到性能下降。

INIT 重生错误消息现象

您可能会在运行 ESXi 6 或 ESXi 6.5 的 Firewall Threat Defense Virtual 控制台上看到以下错误消息：

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

解决方法 - 在设备电源关闭时，编辑 vSphere 中的虚拟机设置添加串行端口。

1. 右键点击虚拟机，然后选择**编辑设置 (Edit Settings)**。
2. 在虚拟硬件选项卡中，从**新设备**下拉菜单中选择**串行端口**，然后点击**添加**。

   虚拟设备列表的底部将会显示串行端口。
3. 在**虚拟硬件 (Virtual Hardware)** 选项卡中，展开**串行端口 (Serial port)**，并选择连接类型**使用物理串行端口 (Use physical serial port)**。
4. 取消选中**在启动时连接**复选框。

   点击**确定**保存设置。

从防火墙保护中排除虚拟机

在 vCenter Server 与 VMware NSX Manager 集成的 vSphere 环境中，分布式防火墙 (DFW) 作为 VIB 包在所有为 NSX 准备的 ESXi 主机集群的内核中运行。主机准备工作会自动激活 ESXi 主机集群上的 DFW。

Firewall Threat Defense Virtual 使用混合模式运行，并且如果需要混合模式的虚拟机受分布式防火墙保护，则这些虚拟机的性能可能会受到不利影响。VMware 建议您将需要混合模式的虚拟机排除在分布式防火墙保护之外。

1. 导航到排除列表设置。
   - 在 NSX 6.4.1 及更高版本中，导航到**网络和安全** > **安全** > **防火墙设置** > **排除列表**。
   - 在 NSX 6.4.0 中，导航到**网络和安全** > **安全** > **防火墙** > **排除列表**。
2. 点击**添加**。
3. 将要排除的虚拟机移至**所选对象**。
4. 点击**确定**。

如果虚拟机有多个 vNIC，则所有 vNIC 都不在保护范围内。如果在将虚拟机添加到排除列表后再将 vNIC 添加到虚拟机，则会在新添加的 vNIC 上自动部署防火墙。要将新 vNIC 排除在防火墙保护之外，必须将虚拟机从排除列表中移除，然后将其重新添加到排除列表中。另一种解决方法是重启（关闭电源再打开电源）虚拟机，但第一种方法的破坏性较小。

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是混合模式、MAC 地址更改和伪造传输。Firewall Threat Defense Virtual 使用混合模式运行，Firewall Threat Defense Virtual 高可用性取决于在主用设备和备用设备之间切换 MAC 地址才能正常运行。

默认设置会阻碍 Firewall Threat Defense Virtual 的正确运行。请参见以下要求的设置：

表 *4: 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”。 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”。

注释 对于 vSphere 标准交换机的 NSX-T 配置安全策略设置，我们没有任何建议，因为带有 NSX-T 的 VMware 不符合条件。

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 Firewall 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 Firewall 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。

UEFI 和安全启动限制

在 VMware 上，UEFI 固件和 UEFI 安全启动仅支持绿地（全新）部署，并且必须在首次打开虚拟机电源之前启用。

现有的棕色地带部署（包括使用传统 BIOS 模式的部署）可以升级到版本 10.0.0，而不会受到影响。不支持在部署后更改启动模式或启用 UEFI 安全启动。

升级限制和局限性

恢复升级限制

⚠

注意　不支持恢复升级。

确保在升级前进行备份。升级到 Threat Defense Virtual 10.0.0 后，您无法回滚到以前的软件版本。要返回到较早的版本，必须重新部署管理中心。

修改 vSphere 标准交换机的安全策略设置

默认设置会阻碍 Firewall Threat Defense Virtual 的正确运行。

过程

步骤 1 在 vSphere Web 客户端中，导航至主机。

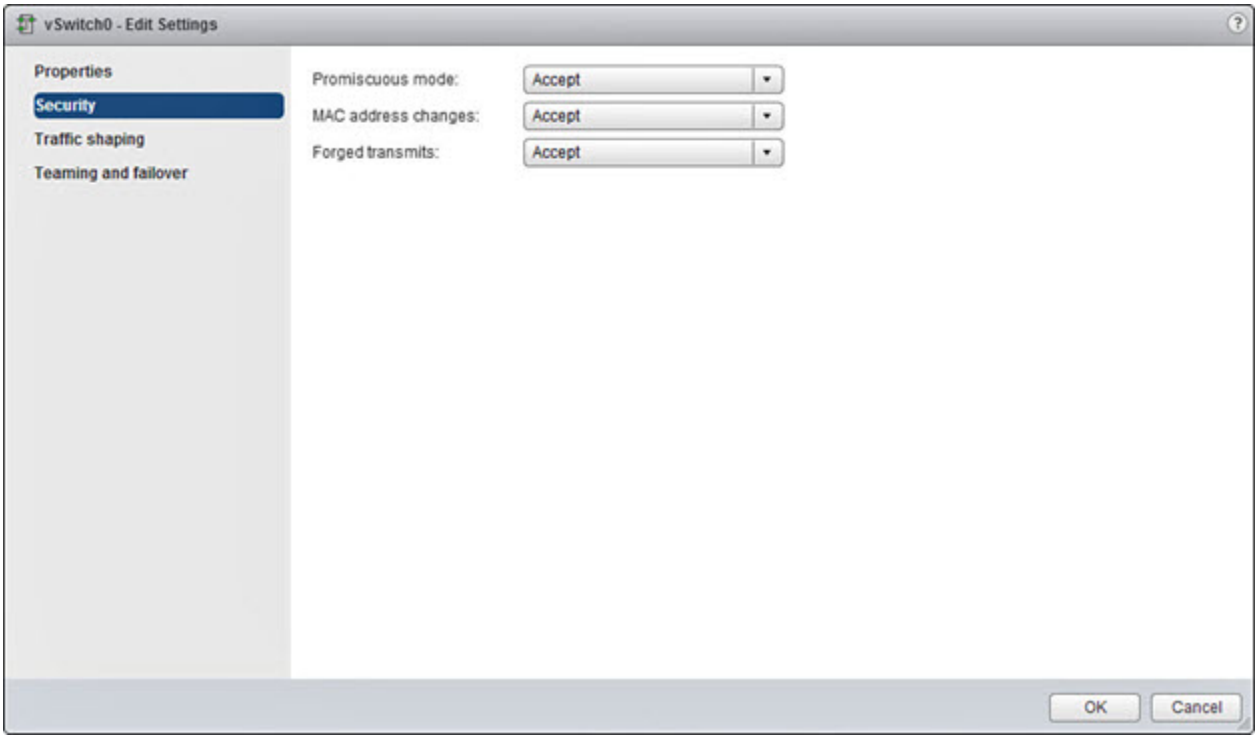
步骤 2 在**管理**选项卡中，点击**网络**，然后选择**虚拟交换机**。

步骤 3 从列表中选择一个标准交换机，然后点击**编辑设置**。

步骤 4 选择**安全**，查看当前设置。

步骤 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



步骤 6 点击确定。

下一步做什么

- 确保在为 Firewall 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。

如何管理 Secure Firewall Threat Defense Virtual 设备

您有两个选择来管理您的 Secure Firewall Threat Defense Virtual。

Secure Firewall Management Center

如果要管理大量设备或要使用 Firewall Threat Defense 支持的更复杂的功能和配置，请使用 防火墙管理中心（而不是集成的 防火墙设备管理器）来配置您的设备。有关详细信息，请参阅使用 Secure Firewall Management Center 来管理 Secure Firewall Threat Defense Virtual

重要事项 您不能同时使用 防火墙设备管理器 和 防火墙管理中心 来管理 Firewall Threat Defense 设备。在启用 防火墙设备管理器 集成管理功能后，将无法使用 防火墙管理中心 来管理 Firewall Threat Defense 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防火墙管理中心。另一方面，当您向Firewall Threat Defense 注册 防火墙管理中心 设备时，防火墙设备管理器 载入管理服务会被禁用。

注意 目前，思科不提供将 防火墙设备管理器 配置迁移到 防火墙管理中心 的选项，反之亦然。选择为 Firewall Threat Defense 设备配置的管理类型时，请考虑这一点。

Cisco Secure Firewall 设备管理器

防火墙设备管理器 是大多数 Firewall Threat Defense 设备上都包含的 Web界面。它可以配置小型网络最常用的软件基本功能。此产品专为仅包含一台或几台设备的网络而设计，在这种网络中，无需使用高性能多设备管理器来控制包含大量设备的大型网络。有关详细信息，请参阅使用 Cisco Secure Firewall 设备管理器 来管理 Secure Firewall Threat Defense Virtual

注释 有关支持的 防火墙设备管理器 设备的列表，请参阅*Cisco Secure Firewall Threat Defense* 兼容性指南。

云交付的防火墙管理中心

云交付的防火墙管理中心是一个基于云的管理平台，让您可以集中管理 Secure Firewall Threat Defense Virtual 设备。云交付的防火墙管理中心支持 Secure Firewall Threat Defense Virtual 7.0.3、7.2.0 及更高版本。有关详细信息，请参阅使用 云交付的防火墙管理中心 来管理 Secure Firewall Threat Defense Virtual。

重要事项 您不能将云交付的防火墙管理中心与 防火墙设备管理器 配合使用来管理同一台 Secure Firewall Threat Defense Virtual 设备。

规划接口

您可以在部署之前规划 Firewall Threat Defense Virtual vNIC 和接口映射，以避免重新启动和配置问题。

对于版本 7.7 及更早版本，诊断接口为必填项。所需的最小接口数量是四个（一个管理接口、一个诊断接口和两个数据接口）。

对于版本 10.0 及更高版本，诊断接口是可选的。在禁用诊断接口时，可以为防火墙 Threat Defense Virtual 配置至少三个接口（一个管理接口和两个数据接口）。如果启用了诊断接口，则至少需要四个接口（一个管理接口、一个诊断接口和两个数据接口）。

有关从 Firewall Threat Defense Virtual 版本 10.0 开始删除诊断接口的详细信息，请参阅移除诊断接口。

Firewall Threat Defense Virtual 支持 vmxnet3（默认）、ixgbe 和 e1000 虚拟网络适配器。此外，借助正确配置的系统，Firewall Threat Defense Virtual 也支持将 ixgbe-vf 驱动程序用于 SR-IOV；有关详细信息，请参阅系统要求，第 3 页。

重要事项 Firewall Threat Defense Virtual 在 VMware 上，如果创建虚拟设备，则默认为 vmxnet3 接口。先前，默认值为 e1000。如果您使用的是 e1000 接口，我们**强烈建议**您切换。vmxnet3 设备驱动器和网络处理与 ESXi 虚拟机监控程序集成，因此其使用更少的资源并提供更好的网络性能。

接口准则和限制

以下部分介绍在 VMware 上与 Firewall Threat Defense Virtual 一起使用的受支持虚拟网络适配器的准则和限制。在规划部署时，记住这些原则至关重要。

一般准则

- 从版本 10.0 开始，诊断接口是可选的。在禁用诊断接口时，可以为防火墙 Threat Defense Virtual 配置至少三个接口（一个管理接口和两个数据接口）。如果启用了诊断接口，则至少需要四个接口（一个管理接口、一个诊断接口和两个数据接口）。

- 我们建议您避免将 HOLDING 端口组用于 Firewall Threat Defense Virtual 接口。来自 vSphere 的 HOLDING 端口组导致接口连接不一致。等待端口是分配给 VLAN ID 的通用端口组。这可能会导致在辅助 Firewall Threat Defense Virtual 设备形成 HA 期间出现问题。
- 您无需使用全部 10 个 Firewall Threat Defense Virtual 接口；对于您不打算使用的接口，只需在 Firewall Threat Defense Virtual 配置中将其禁用即可。
- 请记住，在部署后，您不能将更多虚拟接口添加到虚拟机。如果在删除某些接口想要更多接口，则必须删除虚拟机并重新开始。
- 您可以选择为 防火墙管理中心 配置数据接口，而非管理接口。管理接口是数据接口管理的前提条件，因此您仍需要在初始设置中对其进行配置。请注意，在高可用性部署中，不支持从数据接口进行 防火墙管理中心 访问。有关为 防火墙管理中心 访问配置数据接口的详细信息，请参阅*Cisco Secure Firewall Threat Defense 命令参考*中的 **configure network management-data-interface** 命令。
- 在 Firewall Threat Defense Virtual 内部接口或故障切换高可用性链路中使用的 ESX 端口组的两个虚拟网卡的故障切换顺序，必须配置为一个虚拟网卡作为活动上行链路，另一个作为备用上行链路。这是两个虚拟机相互 ping 或 Threat Defense Virtual 高可用性 (HA) 链路正常运行所必需的。

默认的 VMXNET3 接口

重要事项 Firewall Threat Defense Virtual 在 VMware 上，如果创建虚拟设备，则默认为 vmxnet3 接口。先前，默认值为 e1000。如果您使用的是 e1000 接口，我们**强烈建议**您切换。vmxnet3 设备驱动器和网络处理与 ESXi 虚拟机监控程序集成，因此其使用更少的资源并提供更好的网络性能。

- 对于版本 10.0 及更高版本，当禁用诊断接口时，只需要一个管理接口。当**诊断**设置为“关闭”时，以前为诊断保留的第二个接口可用作数据接口。
- 对于 vmxnet3，思科建议在使用四个以上 vmxnet3 网络接口时使用由 VMware vCenter 管理的主机。部署在独立式 ESXi 上时，其他网络接口不会添加到具有连续 PCI 总线地址的虚拟机。通过 VMware vCenter 管理主机时，可以从配置 CDROM 的 XML 中获取正确的顺序。当主机运行独立式 ESXi 时，只能通过手动比较在 Firewall Threat Defense Virtual 上看到的 MAC 地址与从 VMware 配置工具看到的 MAC 地址，确定网络接口的顺序。

下表描述了 Firewall Threat Defense Virtual 适用于 vmxnet3 和 ixgbe 接口的网络适配器、源网络和目标网络的一致性。

表 *5:* 源网络与目标网络的映射 - *VMXNET3* 和 *IXGBE*

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	保留供内部使用。	保留供内部使用。	保留供内部使用。

网络适配器	源网络	目标网络	功能
网络适配器 3	GigabitEthernet0-0	GigabitEthernet0/0	外部数据
网络适配器 4	GigabitEthernet0-1	GigabitEthernet0/1	内部数据
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）

IXGBE 接口

- ixgbe 驱动程序使用两个管理接口。前两个 PCI 设备必须配置为管理接口：一个用于设备管理/注册，一个保留用于内部用途。
- 对于 ixgbe，ESXi 平台要求 ixgbe NIC 支持 ixgbe PCI 设备。此外，ESXi 平台还具有支持 ixgbe PCI 设备所需的特定 BIOS 和配置要求。有关详细信息，请参阅英特尔技术概要。
- 对于 ixgbe 数据接口，系统仅支持“路由”和“ERSPAN 被动”两种类型。这是由于有关 MAC 地址过滤的 VMware 限制所致。
- 驱动程序不支持 Firewall Threat Defense Virtual 的故障转移 (HA) 部署。

E1000 接口

重要事项 Firewall Threat Defense Virtual 在 VMware 上，如果创建虚拟设备，则默认为 vmxnet3 接口。先前，默认值为 e1000。如果您使用的是 e1000 接口，我们**强烈建议**您切换。vmxnet3 设备驱动器和网络处理与 ESXi 虚拟机监控程序集成，因此其使用更少的资源并提供更好的网络性能。

- 如果您将 Firewall Threat Defense Virtual 升级到 6.4 并使用 e1000 接口，则应将 e1000 接口替换为 vmxnet3 或 ixgbe 接口，以实现更大的网络吞吐量。

下表描述了 Firewall Threat Defense Virtual 适用于默认 e1000 接口的网络适配器、源网络和目标网络的一致性。

表 *6:* 源网络与目标网络的映射 - *E1000* 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	源网络	目标网络	功能
网络适配器 2	GigabitEthernet0-0	GigabitEthernet0/0	外部数据
网络适配器 3	GigabitEthernet0-1	GigabitEthernet0/1	内部数据
网络适配器 4	GigabitEthernet0-2	GigabitEthernet0/2	数据流量（必需）
网络适配器 5	GigabitEthernet0-3	GigabitEthernet0/3	数据流量（可选）
网络适配器 6	GigabitEthernet0-4	GigabitEthernet0/4	数据流量（可选）
网络适配器 7	GigabitEthernet0-5	GigabitEthernet0/5	数据流量（可选）
网络适配器 8	GigabitEthernet0-6	GigabitEthernet0/6	数据流量（可选）
网络适配器 9	GigabitEthernet0-7	GigabitEthernet0/7	数据流量（可选）
网络适配器 10	GigabitEthernet0-8	GigabitEthernet0/8	数据流量（可选）

配置 VMXNET3 接口

重要事项

- 从 6.4 版本开始，如果您使用的是 e1000 接口，我们**强烈建议**您切换到 VMXNET3 接口。VMXNET3 设备驱动器和网络处理与 ESXi 虚拟机监控程序集成，因此其使用更少的资源并提供更好的网络性能。
- 在 7.4 及更早版本上，FMCv300 仅支持 e1000 接口。

  从 7.6 版本开始，FMCv300 支持 e1000 和 VMXNET3 接口。默认情况下，在您部署 VM 时，VMware 上的管理中心虚拟默认使用 e1000 接口。我们强烈建议您切换到 VMXNET3 接口。
- 从 10.0.0 版本开始，当您部署虚拟机时，VMware 上的 Threat Defense Virtual 和管理中心虚拟默认使用 VMXNET3 接口。

要将 e1000 接口更改为 vmxnet3，必须删除所有接口，然后使用 vmxnet3 驱动程序重新安装。

虽然可以在部署中混合使用接口（例如在 防火墙管理中心 上使用 e1000 接口，在其受管虚拟设备上使用 vmxnet3 接口），但不能在同一虚拟设备中混合使用接口。虚拟设备上的所有传感接口和管理接口必须为相同类型。

过程

步骤 1 断开 Firewall Threat Defense Virtual 或 Firewall Management Center Virtual 计算机电源。

要更改接口，必须关闭设备电源。

步骤 2 右键点击清单中的 Firewall Threat Defense Virtual 或 Firewall Management Center Virtual 计算机，然后选择**编辑设置 (Edit Settings)**。

步骤 3 选择适用的网络适配器，然后选择**删除 (Remove)**。

步骤 4 点击**添加**以打开**添加硬件向导**。

步骤 5 选择**以太网适配器**，然后点击**下一步**。

步骤 6 选择 vmxnet3 适配器，然后选择网络标签。

步骤 7 对 Firewall Threat Defense Virtual 上的所有接口重复上述操作。

下一步做什么

- 从 VMware 控制台接通 Firewall Threat Defense Virtual 或 Firewall Management Center Virtual 电源。

添加接口

部署 Firewall Threat Defense Virtual 设备时，最多可以设置 10 个接口（1 个管理接口、1 个保留接口以供内部使用和 8 个数据接口）。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。

⚠

注意 您不能给虚拟机添加多个虚拟接口，然后让 Firewall Threat Defense Virtual 来自动识别它们。要给虚拟机添加接口，您需要完全清除 Firewall Threat Defense Virtual 配置。配置中唯一保留不变的部分是管理地址和网关设置。

如果您需要为 Firewall Threat Defense Virtual 设备配置更多物理接口对等体，那基本上需要重新执行该流程。您可以部署新的虚拟机，也可以使用 *Cisco Secure Firewall* 设备管理器配置指南 中的 “扫描接口更改并迁移接口”程序。

关于 VMware 部署

您可以将 Firewall Threat Defense Virtual 部署到独立的 ESXi 服务器；如果有 vSphere vCenter，则可以使用 vSphere 客户端或 vSphere Web 客户端进行部署。要成功部署 Firewall Threat Defense Virtual，您应该熟悉 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。

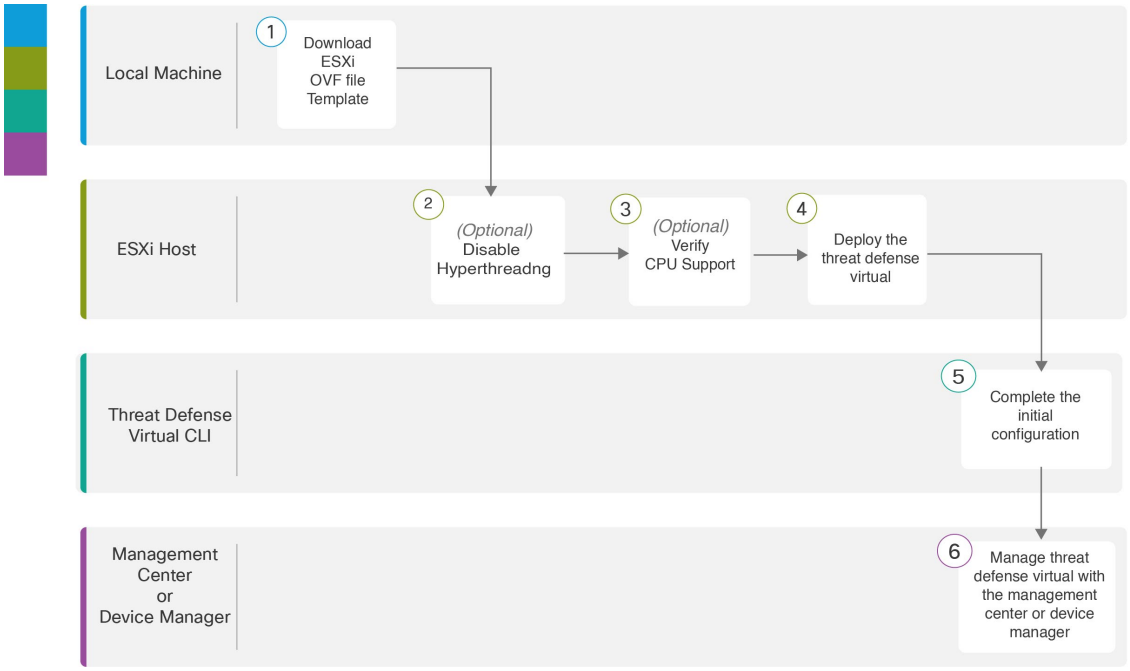
Firewall Threat Defense Virtual 对于 VMware 使用开放虚拟化格式（OVF）进行分发，这是一种打包和部署虚拟机的标准方法。VMware 提供多种调配 vSphere 虚拟机的方法。最适合您的环境的方法取决于多种因素，例如基础设施的规模和类型以及您要实现的目标等。

VMware vSphere Web 客户端和 vSphere 客户端都是连接 vCenter 服务器、ESXi 主机和虚拟机的接口。通过 vSphere Web 客户端和 vSphere 客户端，可以远程连接到 vCenter 服务器。通过 vSphere 客户端，还可以从任何 Windows 系统直接连接到 ESXi。VSphere Web 客户端和 vSphere 客户端是管理 vSphere 环境所有方面的主要界面。它们还提供虚拟机的控制台访问权限。

可通过 vSphere Web 客户端使用所有管理功能。可通过 vSphere 客户端使用其中的部分功能。

端到端程序

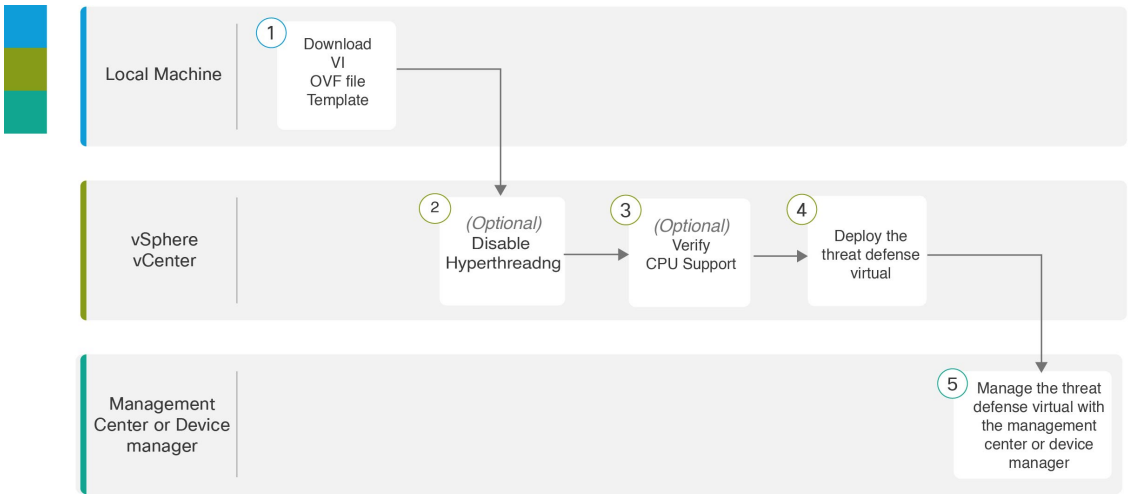
以下流程图说明了在 ESXi 主机上部署 Firewall Threat Defense Virtual 的工作流程。



	工作空间	步骤
1	本地计算机	下载 ESXi OVF 模板：从 Cisco.com 下载开放虚拟化格式 (OVF) 软件包。
2	ESXi 主机	（可选）禁用超线程：为运行 Firewall Threat Defense Virtual 的系统禁用超线程。
3	ESXi 主机	（可选）验证 CPU 支持：使用 Linux 命令行获取 CPU 硬件的相关信息。
4	ESXi 主机	部署 Threat Defense Virtual：在单个 ESXi 主机上部署 Firewall Threat Defense Virtual 设备。
5	Firewall Threat Defense Virtual CLI	完成初始配置：如果使用 ESXi OVF 模板部署，则必须使用 CLI 来设置 Firewall Threat Defense Virtual。

	工作空间	步骤
6	防火墙管理中心或防火墙设备管理器	管理 Firewall Threat Defense Virtual： • 使用 Secure Firewall Management Center 来管理 Secure Firewall Threat Defense Virtual • 使用 Cisco Secure Firewall 设备管理器 来管理 Secure Firewall Threat Defense Virtual

以下流程图说明了在 vSphere vCenter 上部署 Firewall Threat Defense Virtual 的工作流程。



	工作空间	步骤
1	本地计算机	下载 VI OVF 模板：从 Cisco.com 下载开放虚拟化格式 (OVF) 软件包。
2	vSphere vCenter	（可选）禁用超线程：为运行 Firewall Threat Defense Virtual 的系统禁用超线程。
3	vSphere vCenter	（可选）验证 CPU 支持：使用 Linux 命令行获取 CPU 硬件的相关信息。
4	vSphere vCenter	部署 Threat Defense Virtual：在单个 ESXi 主机上部署 Firewall Threat Defense Virtual 设备。
5	防火墙管理中心或防火墙设备管理器	管理 Firewall Threat Defense Virtual： • 使用 Secure Firewall Management Center 来管理 Secure Firewall Threat Defense Virtual • 使用 Cisco Secure Firewall 设备管理器 来管理 Secure Firewall Threat Defense Virtual

准备 Day0 配置文件

您可以在部署 Firewall Threat Defense 之前准备 Day0 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。此初始配置将放入您选择的工作目录中名为“day0-config”的文本文件，并写入首次启动时装载和读取的 day0.iso 文件。

重要事项 该 day0.iso 文件必须在首次启动期间可用。

如果您使用 Day0 配置文件进行部署，该过程允许您执行整个初始设置。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。
- 管理模式；请参阅如何管理 Secure Firewall Threat Defense Virtual 设备。

  您可以将**本地管理**设置为**是**，或者输入 防火墙管理中心 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。
- 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 防火墙设备管理器 管理部署，可以仅为防火墙模式输入**已路由**。不能使用 防火墙设备管理器 配置透明防火墙模式接口。
- 使设备可以在管理网络上进行通信的网络设置。
- 部署类型，您可以在其中指定是在集群模式还是独立模式下部署。

如果您在没有 Day0 配置文件的情况下部署，则必须在启动后配置系统必需设置；有关更多信息，请参阅在没有 Day 0 配置文件的情况下启动。

注释 我们在本示例中使用的是 Linux，但对于 Windows 也有类似的实用程序。

过程

步骤 1 在名为“day0-config”的文本文件中输入设备的 CLI 配置。添加网络设置和关于管理设备的信息。

示例：

```
#Secure Firewall Threat Defense
{
    "EULA": "accept",
    "Hostname": "ftdv-production",
    "AdminPassword": "r2M$9^Uk69##",
    "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": "enabled",
    "IPv6Addr": "2001:db8::a111:b221:1:abca/96",
    "IPv6Mask": "",
    "IPv6Gw": "",
    "DeploymentType": "Cluster" //This is required for Cluster node.//
    "FmcIp": "",
    "FmcRegKey": "",
    "FmcNatId": "",
    "ManageLocally":"No",
    "Diagnostic": "On/Off",
    "IfNamingConvention": "Old/New"
}
```

在Day0配置文件的**ManageLocally**中输入**Yes**以使用本地防火墙设备管理器；输入防火墙管理中心字段（**FmcIp**、**FmcRegKey** 和 **FmcNatId**）的值。对于您未使用的管理选项，将这些字段留空。

注释
对于版本 10.0 及更高版本，如果使用三个接口（无诊断接口）部署威胁防御虚拟设备，您必须在 Day0 配置文件中明确设置：**"Diagnostic": "OFF"**。

重要事项
如果同时在 Day0 配置文件和 VMware OVF 部署向导中指定了诊断设置，则以 Day0 配置为准。

例如：

如果在 Day0 配置文件中指定了 **"Diagnostic": "OFF"**，但在 OVF 部署向导中将诊断选项设置为“ON”，则诊断接口将被禁用。

Day0 配置在首次启动时应用，并覆盖 OVF 模板的选择。

为避免接口映射不一致，请确保在 Day0 配置文件和 OVF 向导中一致地配置诊断设置。

步骤 2 在目录 `Cisco_Secure_Firewall_Threat_Defense_Virtual-X.X.X-xxx` 中的以下元文件中，删除元文件 [*.mf] 或更新 **day0.iso** 的 SHA1 值：

- SHA1(Cisco_Secure_Firewall_Threat_Defense_Virtual-VI-X.X.X-xxx.ovf)= dae28a93d35841b02f18dee17b83cbf161a471ba
- SHA1(Cisco_Secure_Firewall_Threat_Defense_Virtual-X.X.X-xxx.vmdk)= 5c7f83aaa9013f601b27d891439fee52d23c59c6
- SHA1(day0.iso)= 0b77d551a9e17e8d09a0def348ffbfeb1e2f8844

运行以下命令为 **day.iso** 文件生成 SH1 值：

```
sha1sum /path/to/day0.iso | cut -d' ' -f1
```

步骤 3 重复步骤 2，为要部署 Firewall Threat Defense Virtual 时使用的每个元文件生成 SH1 值。

将 Firewall Threat Defense Virtual 部署到 vSphere vCenter

遵照此程序可将 Firewall Threat Defense Virtual 设备部署到 VMware vSphere vCenter。您可以使用 VMware Web 客户端（或 vSphere 客户端）部署和配置 Firewall Threat Defense Virtual 计算机。

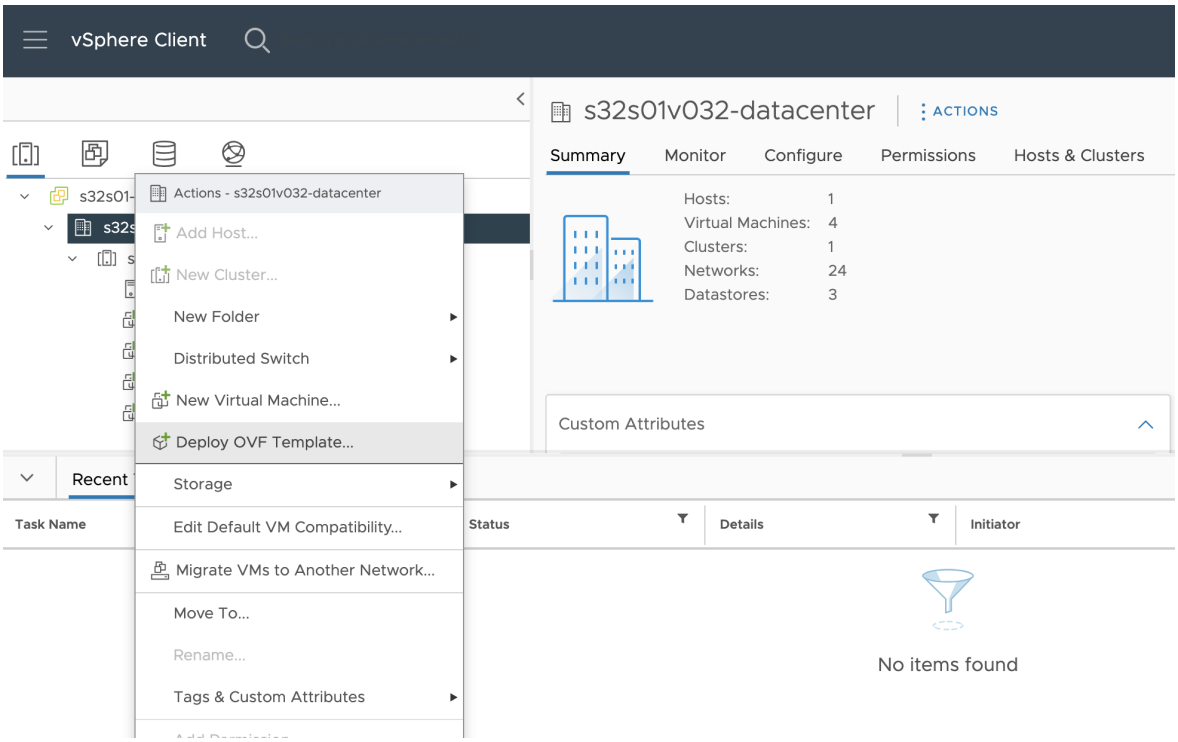
开始之前

- 在部署 Firewall Threat Defense Virtual 之前，您必须在 vSphere 中配置至少一个网络（用于管理）。

过程

步骤 1 登录到 vSphere Web 客户端（或 vSphere 客户端）。

步骤 2 点击 **文件** > **部署 OVF 模板**，使用 vSphere Web 客户端（或 vSphere 客户端）部署之前下载的 OVF 模板文件。



此时将出现“部署 OVF 模板”向导。

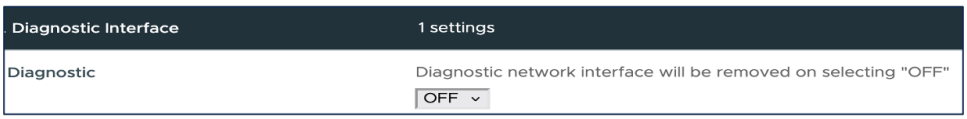
注释

对于 10.0 版，在 VMware OVF 模板中，网络接口通常映射到静态 NetAdaptor。

部署 Threat Defense Virtual 时，诊断接口为可选。

如果选择开启**诊断**，则在网络接口映射中没有更改。

如果选择关闭**诊断**，则会导致网络适配器分配发生变化。



诊断接口的删除会将每个后续以太网接口的映射向下移动一个位置，并将重新分配网络适配器，如下所示：

表 7: 网络接口映射

诊断：开启	诊断：关闭
Ethernet0-0 ------> Ethernet0/0	诊断 ------> Ethernet0/0
Ethernet0-1 ------> Ethernet0/1	Ethernet0-0 ------> Ethernet0/1
Ethernet0-2 ------> Ethernet0/2	Ethernet0-1 ------> Ethernet0/2
Ethernet0-3 ------> Ethernet0/3	Ethernet0-2 ------> Ethernet0/3
Ethernet0-4 ------> Ethernet0/4	Ethernet0-3 ------> Ethernet0/4
Ethernet0-5 ------> Ethernet0/5	Ethernet0-4 ------> Ethernet0/5
Ethernet0-6 ------> Ethernet0/6	Ethernet0-5 ------> Ethernet0/6
Ethernet0-7 ------> Ethernet0/7	Ethernet0-6 ------> Ethernet0/7
	Ethernet0-7 ------> Ethernet0/8

重要事项
如果同时在 Day0 配置文件和 VMware OVF 部署向导中指定了诊断设置，则以 Day0 配置为准。

例如：

如果在 Day0 配置文件中指定了 **"Diagnostic": "OFF"**，但在 OVF 部署向导中将诊断选项设置为“ON”，则诊断接口将被禁用。

Day0 配置在首次启动时应用，并覆盖 OVF 模板的选择。

为避免接口映射不一致，请确保在 Day0 配置文件和 OVF 向导中一致地配置诊断设置。

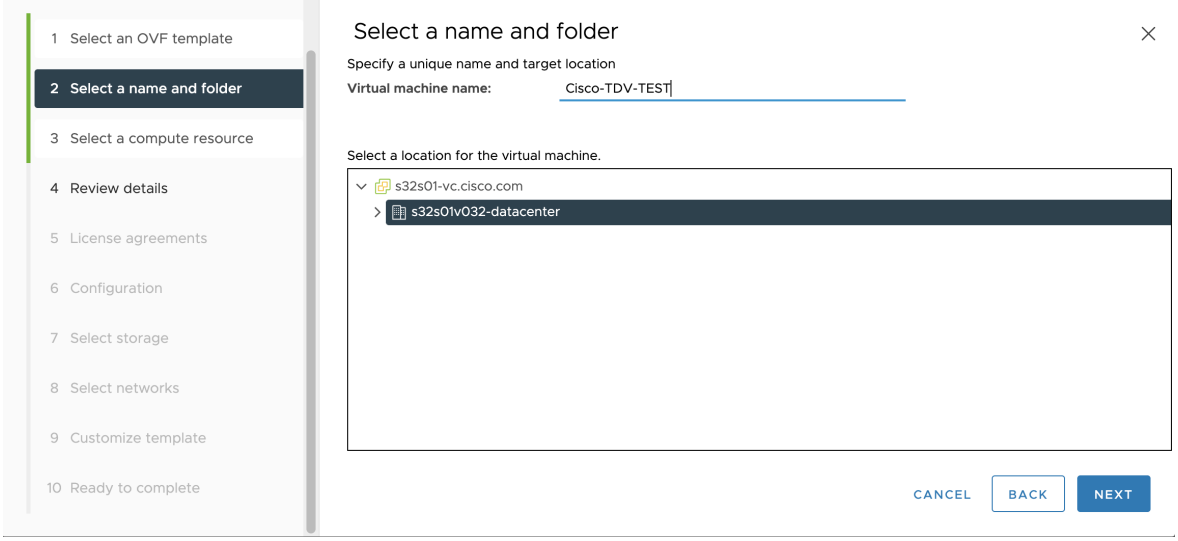
步骤 3 浏览文件系统以找到 OVF 模板源位置，然后点击**下一步**。

选择 Firewall Threat Defense Virtual VI OVF 模板：

- *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*

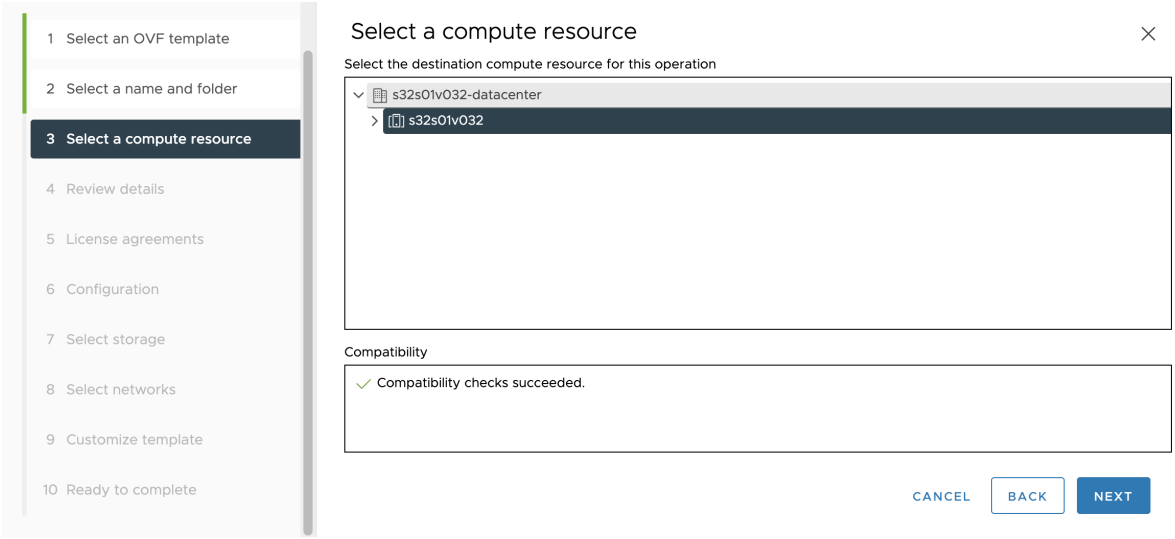
其中，*X.X.X-xxx* 是已下载的存档文件的版本和内部版本号。

步骤 4 在**名称和位置**页面，输入此部署的名称，然后在清单中选择要部署 Firewall Threat Defense Virtual 的的位置（主机或集群），然后点击**下一步**。名称在清单文件夹中必须唯一，最多可以包含 80 个字符。



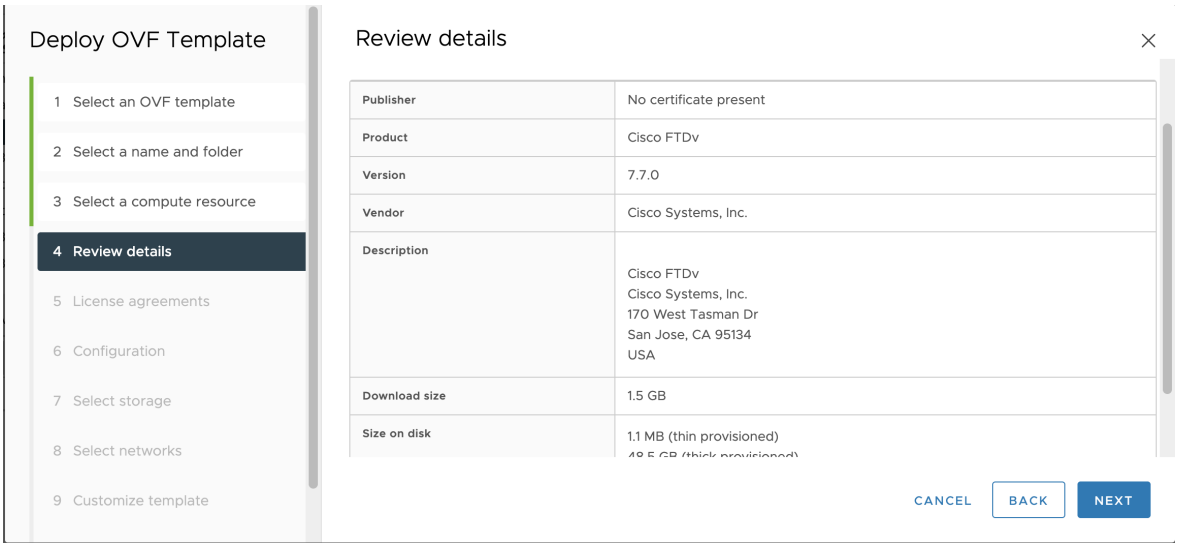
VSphere Web 客户端在清单视图中显示托管对象的组织层级。清单是 vCenter 服务器或主机用于组织托管对象的分层结构。此层次结构包括 vCenter 服务器中的所有受监控对象。

步骤 5 导航至并选择您想运行 Firewall Threat Defense Virtual的资源池，然后点击**下一步**。



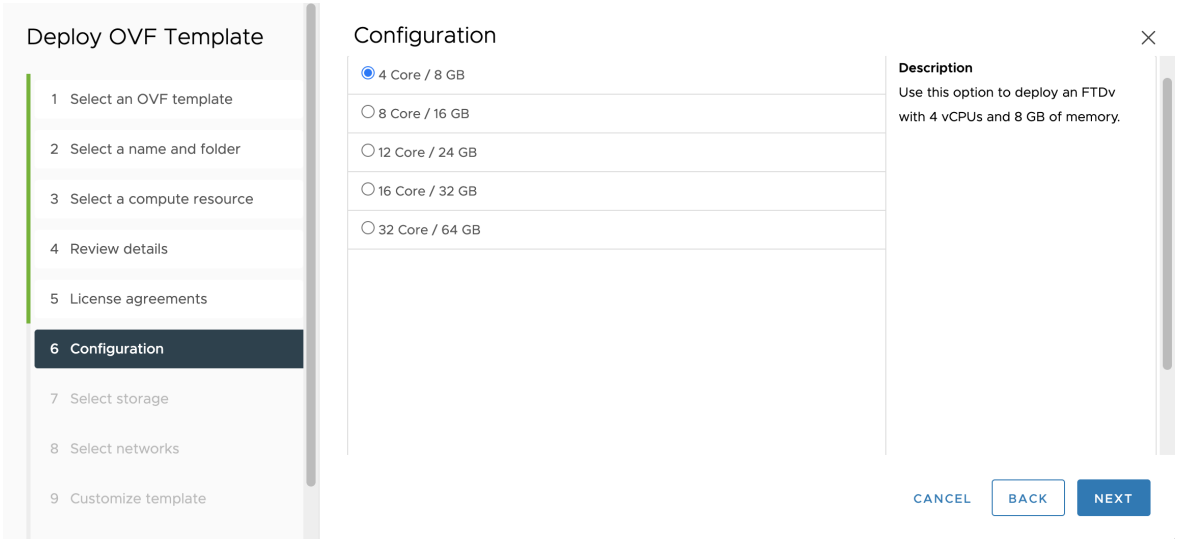
注释
仅当集群包含资源池时，系统才会显示此页面。

步骤 6 查看 **OVF 模板详细信息**页面并验证 OVF 模板信息（产品名称、版本、供应商、下载大小、磁盘大小和说明），然后点击**下一步**。



步骤 7 屏幕上随即会显示**最终用户许可协议**页面。查看随 OVF 模板提供的许可协议（仅 VI 模板），点击**接受**同意许可条款，然后点击**下一步**。

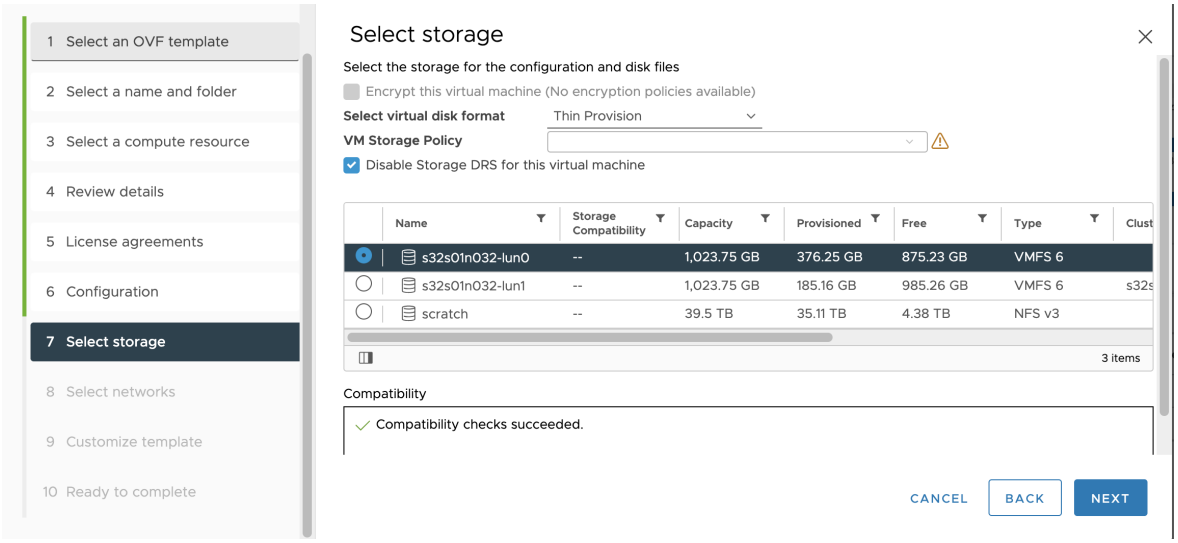
步骤 8 中 **配置** 页面，从 **配置** 选项中的受支持的 vCPU/内存值中选择一个，然后点击 **下一步**。



重要事项

部署的 Firewall Threat Defense Virtual 具有可调的 vCPU 和内存资源。

步骤 9 选择要存储虚拟机文件的 **存储** 位置。

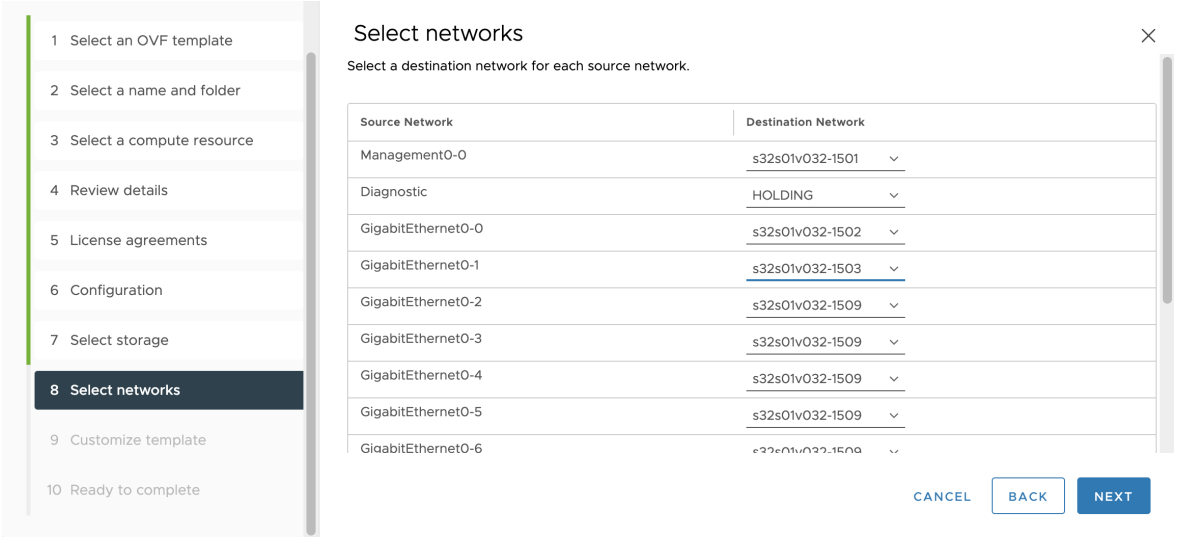


在此页面上，您可以从目标集群或主机上已配置的数据存储中选择。虚拟机配置文件和虚拟磁盘文件均存储在 Datastore 上。选择一个足够大的数据存储，以容纳虚拟机及其所有虚拟磁盘文件。

步骤 10 从 **选择虚拟磁盘格式** 下拉列表中选择 **磁盘格式** 以存储虚拟机虚拟磁盘，然后点击 **下一步**。

如果选择**密集调配 (Thick Provisioned)**，则会立即分配所有存储。如果选择**精简调配 (Thin Provisioned)**，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 11 在 **选择网络** 页面，将 OVF 模板中指定的网络映射到您清单中的网络，然后点击 **下一步**。



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 防火墙管理中心 或 防火墙设备管理器 配置，具体取决于您的管理模式。

重要事项

Firewall Threat Defense Virtual 在 VMware 上，如果创建虚拟设备，则默认为 vmxnet3 接口。先前，默认值为 e1000。如果您使用的是 e1000 接口，我们**强烈建议**您切换。vmxnet3 设备驱动器和网络处理与 ESXi 虚拟机监控程序集成，因此其使用更少的资源并提供更好的网络性能。

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 Firewall Threat Defense Virtual 实例，然后选择**编辑设置**。但是，该屏幕不会显示 Firewall Threat Defense Virtual ID（仅显示网络适配器 ID）。

请查看适用于 Firewall 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）：

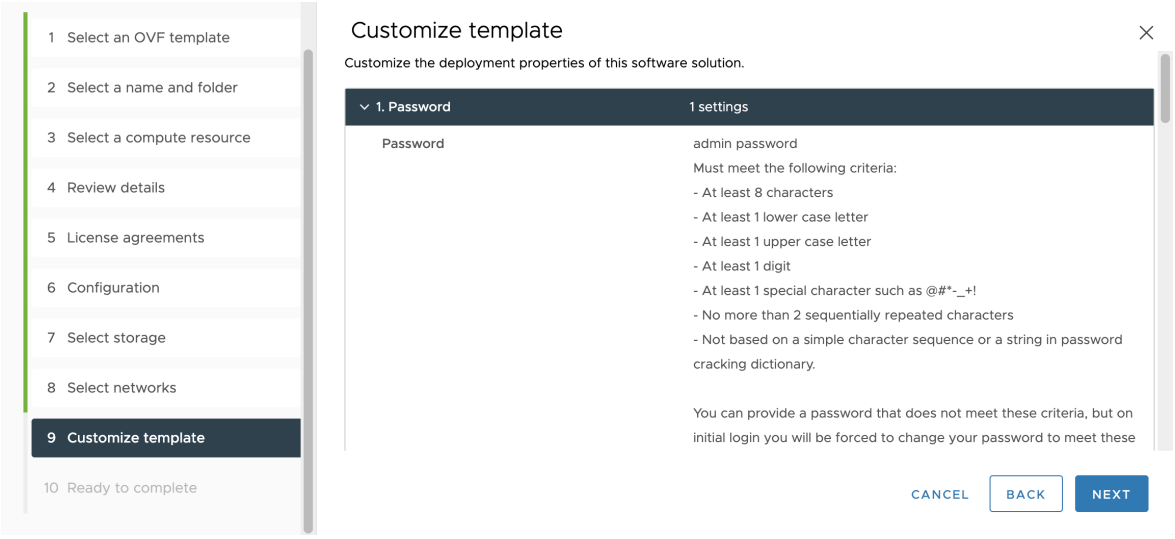
表 *8:* 源网络与目标网络的映射 - *VMXNET3*

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	保留供内部使用。	保留供内部使用。	保留供内部使用。
网络适配器 3	GigabitEthernet0-0	GigabitEthernet0/0	外部数据
网络适配器 4	GigabitEthernet0-1	GigabitEthernet0/1	内部数据
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 Firewall 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。您无需使用所有 Firewall Threat Defense Virtual 接口；对于不打算使用的接口，只需在 Firewall Threat Defense Virtual 配置中将其禁用即可。

步骤 12 在 **自定义模板** 属性页面，设定随 OVF 模板（仅 VI 模板）提供的用户可配置属性：

a) **密码**

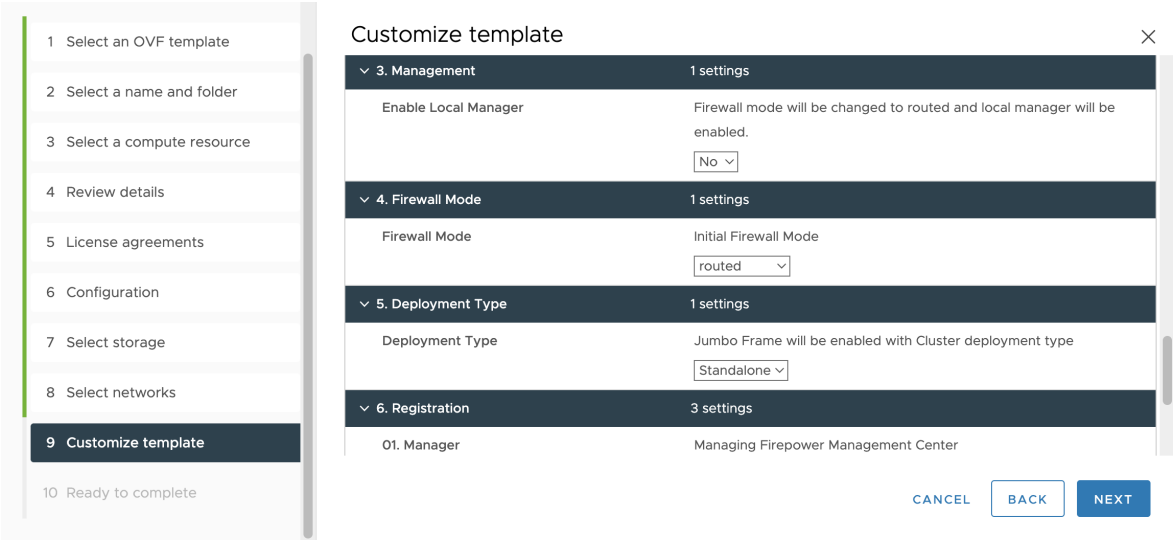


设置 Firewall Threat Defense Virtual 管理员访问的密码。

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 防火墙设备管理器配置工具。选择**否**以使用 防火墙管理中心 来管理此设备。有关如何选择管理选项的概述，请参阅如何管理 Secure Firewall Threat Defense Virtual 设备。

d) 防火墙模式

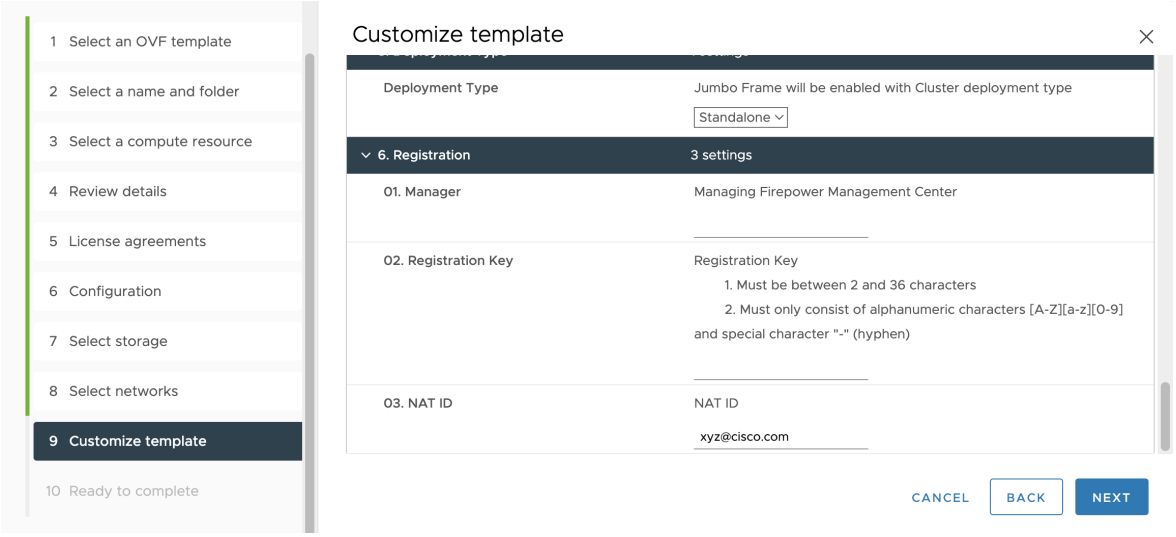
设定初始防火墙模式。点击**防火墙模式**的下拉箭头，然后选择两种支持的模式之一；**已路由**或**透明**。

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 防火墙设备管理器 配置透明防火墙模式接口。

e) 部署类型

将部署类型设置为**独立**或**集群**。依次选择**集群**以启用巨帧预留，这是集群控制链路所必需的。为独立或高可用性部署选择**独立**。请注意，如果作为独立设备部署，仍可在集群中使用；但是，在部署后为集群启用巨帧意味着必须重新启动。

f) 注册

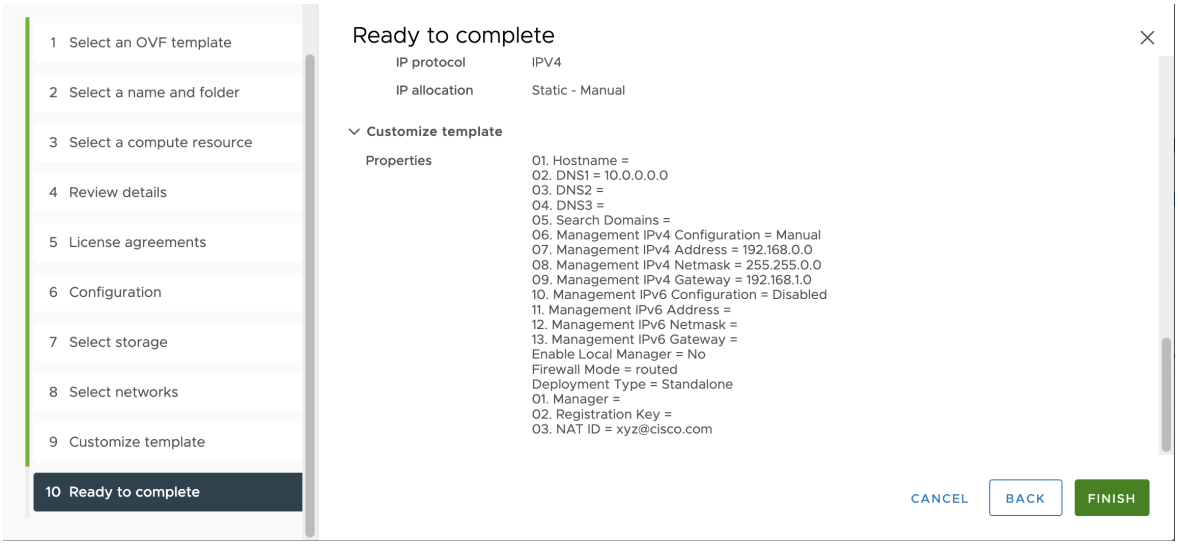


如果对**启用本地管理器**选择**否**，则需要提供必要的凭证以将此设备注册到负责管理的 Cisco Secure Firewall Management Center。提供以下各项：

- **负责管理的防御中心** - 输入 防火墙管理中心 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 (-)。当您将设备添加到 防火墙管理中心时，需要记住此注册密钥。
- **NAT ID** - 如果 Firewall Threat Defense Virtual 和 防火墙管理中心 被网络地址转换 (NAT) 设备分隔，并且 防火墙管理中心 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 (-)。

g) 点击**下一步**。

步骤 13 在 **即将完成** 页面中，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**。要进行更改，点击**后退**以在屏幕中向后导航。



或者，选中**部署后启动**选项启动 Firewall Threat Defense Virtual，然后点击**完成**。

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”(Inventory) 中的指定数据中心下会显示 Firewall Threat Defense Virtual 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 Firewall Threat Defense Virtual，Firewall 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**选择**否**，您将使用 防火墙管理中心 管理 Firewall Threat Defense Virtual；请参阅使用 Secure Firewall Management Center 来管理 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 Secure Firewall Threat Defense Virtual 设备。

向 vSphere ESXi 主机部署 Firewall Threat Defense Virtual

遵照此程序可在单个 ESXi 主机上部署 Firewall Threat Defense Virtual 设备。您可以使用 VMware 主机客户端（或 vSphere 客户端）管理单个 ESXi 主机并执行管理任务，例如基本虚拟化操作（如部署和配置 Firewall Threat Defense Virtual 计算机）。

注释 了解 VMware 主机客户端与 vSphere Web 客户端的区别很重要，尽管它们具有相似的用户界面。您可以使用 vSphere Web 客户端连接到 vCenter 服务器并管理多个 ESXi 主机，同时使用 VMware 主机客户端管理单个 ESXi 主机。

有关如何将 Firewall Threat Defense Virtual 设备部署到 vCenter 环境的说明，请参阅将 Firewall Threat Defense Virtual 部署到 vSphere vCenter，第 23 页。

开始之前

- 在部署 Firewall Threat Defense Virtual 之前，您必须在 vSphere 中配置至少一个网络（用于管理）。
- 从目录中提取 VMDK 文件后，验证 SHA1 校验和。

过程

步骤 1 从 Cisco.com 下载适用于 VMware ESXi 的 Firewall Threat Defense Virtual 安装软件包，并将其保存到本地的管理计算机。

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

需要 Cisco.com 登录信息和思科服务合同。

步骤 2 将 tar 文件解压缩到工作目录中。请勿删除该目录中的任何文件。其中包括以下文件：

- Cisco_Secure_Firewall_Threat_Defense_Virtual-VI-*X.X.X-xxx*.ovf - 适用于 vCenter 部署
- Cisco_Secure_Firewall_Threat_Defense_Virtual-ESXi-*X.X.X-xxx*.ovf - 适用于 ESXi 部署。
- Cisco_Secure_Firewall_Threat_Defense_Virtual-*X.X.X-xxx*.vmdk - VMware 虚拟磁盘文件。
- Cisco_Secure_Firewall_Threat_Defense_Virtual-VI-*X.X.X-xxx*.mf - 适用于 vCenter 部署的清单文件。
- Cisco_Secure_Firewall_Threat_Defense_Virtual-ESXi-*X.X.X-xxx*.mf - 适用于 ESXi 部署的清单文件。
- day0.iso

其中，*X.X.X-xx* 是已下载的存档文件的版本和内部版本号。

步骤 3 在浏览器中，使用 *http://host-name/ui* 或 *http://host-IP-address/ui* 格式输入 ESXi 目标主机名或 IP 地址。

登录屏幕会显示。

步骤 4 输入管理员用户名和密码。

步骤 5 点击**登录**继续。

此时您即已登录到目标 ESXi 主机。

步骤 6 右键点击 VMware 主机客户端清单中的**主机**，然后选择**创建/注册 VM**。

新的虚拟机向导将打开。

步骤 7 在向导的**选择创建类型**页面，选择**从 OVF 或 OVA 文件部署虚拟机**，然后点击**下一步**。

步骤 8 在向导的**选择 OVF 和 VMDK 文件**页面：

a) 输入您的 Firewall Threat Defense Virtual 计算机的名称。

虚拟机名称最多可包含 80 个字符，并且在每个 ESXi 实例中必须唯一。

b) 点击蓝色窗格，浏览到您将 Firewall Threat Defense Virtual tar 文件解压缩到的目录，然后选择 ESXi OVF 模板和附带的 VMDK 文件：

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

其中，*X.X.X-xx* 是已下载的存档文件的版本和内部版本号。

注意
确保选择 ESXi OVF。

步骤 9 点击**下一步**。

您的本地系统存储将打开。

步骤 10 从向导**选择存储**页面上的可访问数据存储库列表中选择一个数据存储库。

数据存储库会保存虚拟机配置文件和所有虚拟磁盘文件。每个数据存储库的大小、速度、可用性和其他属性可能有所不同。

步骤 11 点击**下一步**。

步骤 12 配置随适用于 Firewall Threat Defense Virtual 的 ESXi OVF 提供的**部署选项**：

a) **网络映射** - 将 OVF 模板中指定的网络映射到清单中的网络，然后选择**下一步**。

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 防火墙管理中心 或 防火墙设备管理器 配置，具体取决于您的管理模式。

重要事项
Firewall Threat Defense Virtual 在 VMware 上，如果创建虚拟设备，则默认为 vmxnet3 接口。先前，默认值为 e1000。如果您使用的是 e1000 接口，我们**强烈建议**您切换。vmxnet3 设备驱动器和网络处理与 ESXi 虚拟机监控程序集成，因此其使用更少的资源并提供更好的网络性能。

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 Firewall Threat Defense Virtual 实例，然后选择**编辑设置**。但是，该屏幕不会显示 Firewall Threat Defense Virtual ID（仅显示网络适配器 ID）。

请查看适用于 Firewall 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）：

表 *9:* 源网络与目标网络的映射 - *VMXNET3*

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	保留供内部使用。	保留供内部使用。	保留供内部使用。
网络适配器 3	GigabitEthernet0-0	GigabitEthernet0/0	外部数据
网络适配器 4	GigabitEthernet0-1	GigabitEthernet0/1	内部数据
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 Firewall 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。您无需使用所有 Firewall Threat Defense Virtual 接口；对于不打算使用的接口，只需在 Firewall Threat Defense Virtual 配置中将其禁用即可。

b) **磁盘调配** - 选择磁盘格式以存储虚拟机虚拟磁盘。

如果选择**密集**调配，则会立即分配所有存储。如果选择**精简**调配，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 13 在新建虚拟机向导的**即将完成**页面，查看虚拟机的配置设置。

a) （可选）点击**返回**以返回并查看或修改向导设置。
b) （可选）点击**取消**以放弃创建任务并关闭向导。
c) 点击**完成**以完成创建任务并关闭向导。

完成该向导后，ESXi 主机将处理 VM；您可以在**最近任务**窗格中看到部署状态。部署成功完成后，**结果**列下将显示成功完成。

随后 ESXi 主机的虚拟机清单下会显示新的 Firewall Threat Defense Virtual 虚拟机实例。启动新的虚拟机最多可能需要 30 分钟。

注释
要向思科许可颁发机构成功注册 Firewall Threat Defense Virtual，Firewall 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

- 使用 CLI 完成虚拟设备的设置。这是使用 ESXi OVF 模板部署 Firewall Threat Defense Virtual 时的下一步；请参阅使用 CLI 完成 Firewall Threat Defense Virtual 设置 ，第 35 页。

使用 CLI 完成 Firewall Threat Defense Virtual 设置

使用 ESXi OVF 模板部署时，必须使用 CLI 设置 Firewall Threat Defense Virtual。Firewall Threat Defense Virtual 设备没有 Web 界面。如果使用 VI OVF 模板部署并且在部署过程中没有使用设置向导，也可以使用 CLI 来配置系统所需的设置。

注释 如果使用 VI OVF 模板部署并且使用了设置向导，虚拟设备已配置，并且不需要执行其他设备配置。接下来的步骤取决于您选择的管理模式。

首次登录新配置的设备时，必须阅读并接受 EULA。然后，请按照设置提示更改管理员密码，并配置设备的网络设置和防火墙模式。

在遵循设置提示的情况下，对于多选问题，选项会列在括号内，例如(y/n)。默认值会列在方括号内，例如 [y]。按 Enter 键确认选择。

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 Firewall 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（本地管理使用 防火墙设备管理器）。

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 firepower # 提示符时，确认设置是否成功。

注释
要向思科许可颁发机构成功注册 Firewall Threat Defense Virtual，Firewall 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**选择**否**，您将使用 防火墙管理中心 管理 Firewall Threat Defense Virtual；请参阅使用 Secure Firewall Management Center 来管理 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 Secure Firewall Threat Defense Virtual 设备。

提高 ESXi 配置的性能

通过调整 ESXi 主机的 CPU 配置设置，可以提高 ESXi 环境中的 Firewall Threat Defense Virtual 性能。通过调度关联选项，可以控制虚拟机 CPU 在主机物理核心（和超线程，如果已启用超线程）范围内的分布方式。使用此功能，您可以将每个虚拟机分配到指定关联组中的处理器。

有关详细信息，请参阅以下 VMware 文档。

- 《vSphere 资源管理》的 *CPU* 资源管理一章。
- 《VMware vSphere 的性能最佳实践》。
- vSphere 客户端联机帮助。

NUMA 准则

非一致内存访问 (NUMA) 是一种共享内存架构，描述了多处理器系统中主内存模块相对于处理器的位置。如果处理器访问的内存不在自己的节点内（远程内存），则数据通过 NUMA 连接以低于本地内存的访问速率传输。

X86 服务器架构由多个插槽和每个插槽内的多个内核组成。每个 CPU 插槽及其内存和 I/O 均称为 NUMA 节点。要从内存高效读取数据包，来宾应用和关联的外围设备（例如 NIC）应位于同一个节点中。

为获得最佳 Firewall Threat Defense Virtual性能：

- Firewall Threat Defense Virtual VM 必须在单一 NUMA 节点上运行。如果部署了单个 Firewall Threat Defense Virtual 以跨 2 个插槽运行，则性能将显著下降。
- 8 核 Firewall Threat Defense Virtual 要求主机 CPU 上的每个插槽至少有 8 个内核。必须考虑服务器上运行的其他虚拟机。
- 16 核 Firewall Threat Defense Virtual 要求主机 CPU 上的每个插槽至少有 16 个内核。必须考虑服务器上运行的其他虚拟机。
- NIC 应与 Firewall Threat Defense Virtual VM 位于同一 NUMA 节点上。

注释 从版本 10.0 开始，如果用户使用 64 核部署 FTDvU，则需要配置 NUMA 设置。在 VMware 中创建 64 核心 Threat Defense Virtual 后，用户必须编辑虚拟机设置，并将 **numa.autosize.vcpu.maxPerVirtualNode** 值更新为 **64**。

有关在 ESXi 上使用 NUMA 系统的详细信息，请参阅您的 VMware ESXi 版本对应的 VMware 文档 *vSphere* 资源管理。要查看此文档和其他相关文档的最新版本，请参阅 http://www.vmware.com/support/pubs... 。

VMware 上 Threat Defense Virtual 部署的最佳实践

本节提供在 VMware ESXi 或 vCenter 环境中部署 Threat Defense Virtual 时确保最佳性能、稳定性和可预测性的最佳实践。

CPU 和 vCPU 配置

- 使用物理 CPU (pCPU) 和虚拟 CPU (vCPU) 之间的一对一映射配置虚拟机。
- 不要在部署了 Threat Defense Virtual 的 ESXi 主机上超订用 CPU 资源。
- 预留相当于分配给虚拟机的总 vCPU 容量的 CPU 资源。

  在 vSphere UI 中，导航至编辑设置 → 虚拟硬件 → CPU → 预留，输入以 MHz 为单位的值，然后点击确定。

  通过将物理 CPU 的基本时钟频率乘以已分配的 vCPU 数量来计算 CPU 预留。

  CPU 预留 = 基本时钟频率 * vCPU 数量

  例如，考虑具有以下规格的 ESXi 主机：

  - **处理器类型**： Intel(R) Xeon(R) CPU E5-2695 v4
  - **基本时钟速度**：2.10 GHz（相当于 2100 MHz）

  如果 Threat Defense Virtual 实例配置了 16 个 vCPU，则 CPU 预留计算方式如下：

  CPU 预留 = 16 vCPUs * 2100 MHz = 33,600 MHz (33.6 GHz)

- 根据需要在 ESXi 主机级别禁用超线程。

  有关详细配置和最佳实践，请参阅 VMware 官方文档。

注释 超订用主机处理资源可能会导致数据包丢失、系统错误或服务中断。

内存配置

- 为 VM 预留 100% 的已配置内存。
- 在 vSphere UI 中，导航至编辑设置 → 虚拟硬件 → 内存 → 预留，然后选择预留所有访客内存（全部锁定）。
- 避免主机内存过量使用（目标零激增和零交换）。

网络配置

- 确保 vSwitch、端口组和物理上行链路有足够的带宽，以避免网络拥塞。
- 启用 SR-IOV 或 PCI 直通可增强网络性能。
- 不建议对 Threat Defense Virtual 部署使用 e1000 网络适配器。

存储配置

- 对所有虚拟存储使用厚置备预先归零磁盘。
- 使数据存储延迟稳定在 5 毫秒以下，峰值在 10-15 毫秒以下。

延迟灵敏度设置

仅当配置了 100% CPU 和内存预留时，才将虚拟机的延迟灵敏度设定为高。

在 vSphere UI 中，导航至编辑设置 → VM 选项 → 高级 → 延迟灵敏度，选择高，然后点击确定。

注释 仅当配置了完整的 CPU 和内存预留时，才将延迟灵敏度设定为高。

SR-IOV 接口调配

单一根 I/O 虚拟化 (SR-IOV) 允许运行各种访客操作系统的多个 VM 共享主机服务器内的单个 PCIe 网络适配器。SR-IOV 允许 VM 在网络适配器中绕过虚拟机监控程序而直接移入或移出数据，从而提

高网络吞吐量及降低服务器 CPU 负担。最新的 x86 服务器处理器包括芯片组增强功能（例如 Intel VT-d 技术），它们可促进 SR-IOV 所需的直接内存传输及其他操作。

SR-IOV 规范定义了两种设备类型：

- 物理功能 (PF) - 实质上属于静态 NIC，PF 是完整的 PCIe 设备，包括 SR-IOV 功能。PF 按正常 PCIe 设备的方式进行发现、管理和配置。使用单个 PF 可为一组虚拟功能 (VF) 提供管理和配置。
- 虚拟功能 (VF) - 类似于动态 vNIC，VF 是完整或轻型虚拟 PCIe 设备，至少提供必要的数据移动资源。VF 并非直接进行管理，而是通过 PF 进行获取和管理。可以为一台 VM 分配一个或多个 VF。

VF 在虚拟化操作系统框架下，最高可以 10 Gbps 的速度连接 Firewall Threat Defense Virtual 计算机。本节介绍如何在 VMware 环境下配置 VF。

SR-IOV 接口的最佳实践

SR-IOV 接口准则

VMware vSphere 5.1 及更高版本仅在具有特定配置的环境下支持 SR-IOV。启用 SR-IOV 时，vSphere 的某些功能无法正常工作。

除了 Firewall Threat Defense Virtual 和 SR-IOV 的系统要求之外，您还应该查看 VMware 文档中的支持使用 SR-IOV 的配置，以了解有关要求、支持的 NIC、功能可用性及 VMware 和 SR-IOV 升级要求方面的详细信息。

VMware 上使用 SR-IOV 接口的 Firewall Threat Defense Virtual 支持混合接口类型。您可以将 SR-IOV 或 VMXNET3 用于管理接口，并将 SR-IOV 用于数据接口。

本节介绍在 VMware 系统上调配 SR-IOV 接口的各种设置和配置步骤。本节中的信息基于特定实验室环境中的设备创建，这些设备使用的是 VMware ESXi 6.0 和 vSphere Web 客户端、思科 UCS C 系列服务器及 Intel 以太网服务器适配器 X520 - DA2。

SR-IOV 接口的限制

启动 Firewall Threat Defense Virtual 时，请注意 SR-IOV 接口出现的顺序可能与 ESXi 中显示的顺序相反。这可能引起接口配置错误，导致特定的 Firewall Threat Defense Virtual机无网络连接。

⚠

注意 开始在 Firewall Threat Defense Virtual 上配置 SR-IOV 网络接口之前，先验证接口映射非常重要。这可确保将网络接口配置应用到 VM 主机上正确的物理 MAC 地址接口。

Firewall Threat Defense Virtual 启动后，您可以确认哪个 MAC 地址映射到哪个接口。请使用 **show interface** 命令查看详细的接口信息，包括接口的 MAC 地址。将 MAC 地址与 **show kernel ifconfig** 命令的结果进行比较以确认正确的接口分配。

注：

使用 ixgbe-vf 接口的限制

使用 ixgbe-vf 接口时，请注意以下限制：

- 禁止访客 VM 将 VF 设置为混合模式。因此，使用 ixgbe-vf 时不支持透明模式。
- 禁止访客 VM 在 VF 上设置 MAC 地址。因此，在 HA 期间不会像在其他 Firewall Threat Defense Virtual 平台上和使用其他接口类型那样传输 MAC 地址。HA 故障转移通过从主用设备向备用设备传送 IP 地址的方式运行。

注释 此限制也适用于 i40e-vf 接口。

- 思科 UCS-B 服务器不支持 ixgbe-vf vNIC。
- 在故障转移设置中，当配对的 Firewall Threat Defense Virtual（主设备）发生故障时，备用 Firewall Threat Defense Virtual 设备将接管主设备的角色，并使用备用 Firewall Threat Defense Virtual 设备的新 MAC 地址更新其接口 IP 地址。此后，Firewall Threat Defense Virtual 会向同一网络上的其他设备发送免费地址解析协议 (ARP) 更新，以通告接口 IP 地址的 MAC 地址更改。但是，由于与这些类型的接口不兼容，因此不会将免费 ARP 更新发送到用于将接口 IP 地址转换为全局 IP 地址的 NAT 或 PAT 语句中所定义的全局 IP 地址。

检查 ESXi 主机 BIOS

开始之前

要在 VMware 上部署带 SR-IOV 接口的 Firewall Threat Defense Virtual，需要支持和启用虚拟化。VMware 提供了几种验证虚拟化支持的方法，包括其在线 SR-IOV 支持兼容性指南以及可下载的 CPU 识别实用程序（检测虚拟化处于启用还是禁用状态）。

另外，您还可以通过登录到 ESXi 主机来确定是否在 BIOS 中启用了虚拟化。

过程

步骤 1 使用下列方法之一登录到 ESXi Shell：

- 如果您可以直接访问主机，请按 Alt+F2 打开计算机物理控制台的登录页面。
- 如果您正在远程连接主机，请使用 SSH 或其他远程控制台连接在主机上启动会话。

步骤 2 输入主机识别的用户名和密码。

步骤 3 运行以下命令：

```
esxcfg-info|grep "\----\HV Support"
```

- HV Support 命令的输出指示可用的虚拟机监控程序类型。有关可能值的说明如下：
- 0 - VT/AMD-V 表示该支持对于此硬件不可用。

- 1 - VT/AMD-V 表示 VT 或 AMD-V 可能可用，但此硬件不支持它们。
- 2 - VT/AMD-V 表示 VT 或 AMD-V 可用，但目前在 BIOS 中未启用。
- 3 - VT/AMD-V 表示 VT 或 AMD-V 在 BIOS 中已启用，并且可以使用。

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

值 3 表示支持并启用虚拟化。

下一步做什么

在主机物理适配器上启用 SR-IOV。

在主机物理适配器上启用 SR-IOV

在将虚拟机连接到虚拟功能之前，请使用 vSphere Web 客户端启用 SR-IOV，并设置主机上的虚拟功能数量。

开始之前

- 请确保已安装兼容 SR-IOV 的网络接口卡 (NIC)；请参阅系统要求，第 3 页。

过程

步骤 1 在 vSphere Web 客户端中，导航到要启用 SR-IOV 的 ESXi 主机。

步骤 2 在**管理**选项卡上，点击**网络**并选择**物理适配器**。

您可以查看 SR-IOV 属性，以了解物理适配器是否支持 SR-IOV。

步骤 3 选择物理适配器，然后点击**编辑适配器设置 (Edit adapter settings)**。

步骤 4 在 SR-IOV 下，从**状态 (Status)** 下拉菜单中选择**启用 (Enabled)**。

步骤 5 在**虚拟功能数量 (Number of virtual functions)** 文本框中，键入要为该适配器配置的虚拟功能数目。

注释
我们建议您对每个接口使用的 VF 数量**不要**超过 1 个。如果与多个虚拟功能共享物理接口，可能会出现性能下降。

步骤 6 点击**确定**。

步骤 7 重启 ESXi 主机。

虚拟功能在由物理适配器项表示的 NIC 端口上将变为活动状态。它们显示在主机**设置**选项卡的“PCI 设备”列表中。

在主机物理适配器上启用 SR-IOV 后，验证 ESXi 主机上的 NIC 驱动程序是否需要其他配置。

对于英特尔 E810 适配器，必须调整 `icen` 驱动程序参数以确保在 SR-IOV 部署中实现最佳性能。

要为具有 64 个 vCPU 和 128 GB 内存的 Threat Defense Virtual 部署配置 ESXi 主机，请在 ESXi 主机上使用以下命令，然后重新引导主机。

```
esxcfg-module -g icen
esxcfg-module -s 'NumQPsPerVF=16,16' icen
reboot
```

虽然 NumQPsPerVF 可设置为小于 16 的值，但建议使用 16 以获得最佳性能。

同样，对于具有 32 个 vCPU 和 64 GB 内存的 Threat Defense Virtual 部署，请将 NumQPsPerVF 设置为 8，以实现最佳性能（但如果需要，也可以使用更低的值）：

```
esxcfg-module -s 'NumQPsPerVF=8,8' icen
```

注释
务必在更改模块参数后重新引导主机。

下一步做什么

- 创建一个标准 vSwitch 来管理 SR-IOV 功能和配置。

创建 vSphere 交换机

创建一个 vSphere 交换机来管理 SR-IOV 接口。

过程

步骤 1 在 vSphere Web 客户端中，导航至 ESXi 主机。

步骤 2 在**管理**下，选择**网络**，然后选择**虚拟交换机**。

步骤 3 点击**添加主机网络 (Add host networking)**图标，即带有加号 (+) 的绿色地球仪图标。

步骤 4 选择**标准交换机的虚拟机端口组**连接类型，然后点击**下一步**。

步骤 5 选择**新建标准交换机**，然后点击**下一步**。

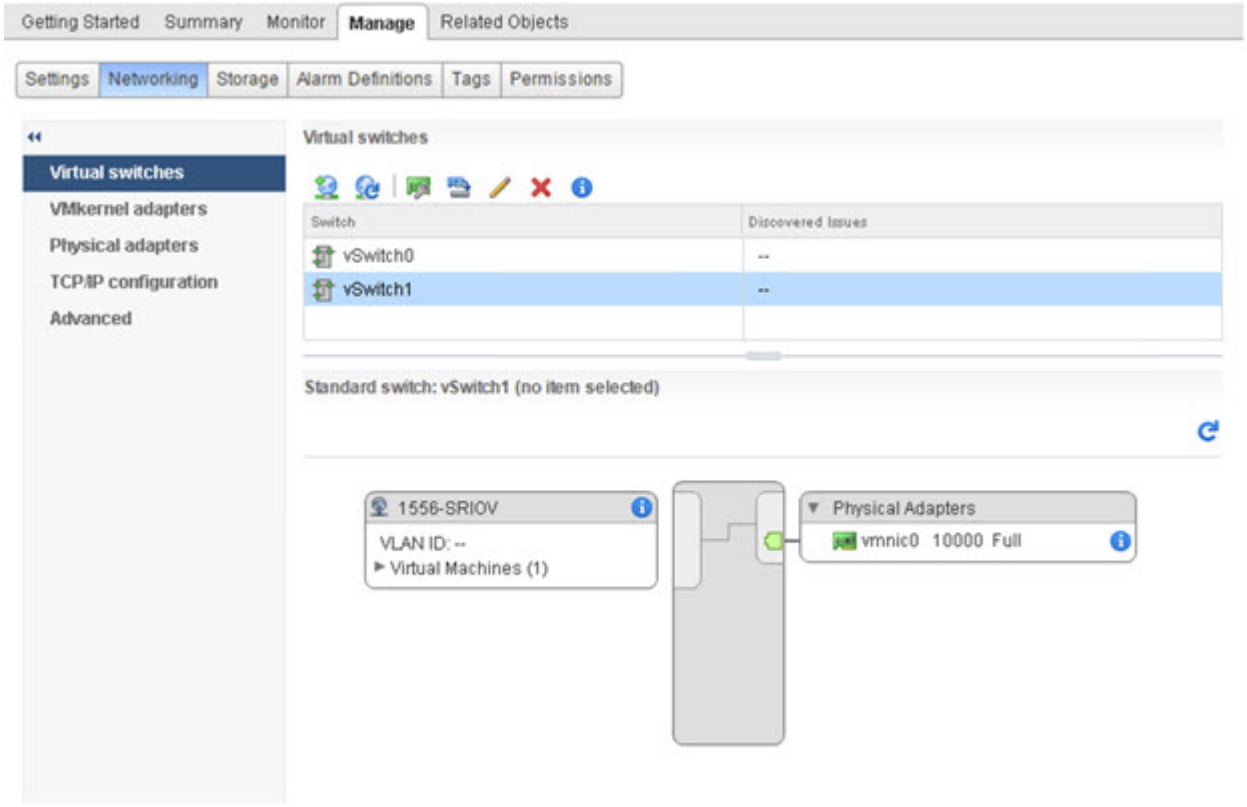
步骤 6 将物理网络适配器添加到新的标准交换机中。

a) 在分配的适配器下，点击绿色加号 (+) 以**添加适配器**。
b) 从列表中为 SR-IOV 选择相应的网络接口。例如 Intel(R) 82599 万兆位双端口网络连接。
c) 从**故障转移顺序组 (Failover order group)**下拉菜单中，选择**活动适配器 (Active adapters)**。
d) 点击**确定**。

步骤 7 为该 SR-IOV vSwitch 输入一个**网络标签**，然后点击**下一步**。

步骤 8 在**准备完成**页面上查看您的选择，然后点击**完成**。

图 2: 已连接 *SR-IOV* 接口的新 *vSwitch*



下一步做什么

- 查看虚拟机的兼容级别。

升级虚拟机的兼容级别

兼容级别决定可用于虚拟机的虚拟硬件，它们与主机上可用的物理硬件相对应。Firewall Threat Defense Virtual VM 的硬件级别需要达到 10 级或更高级别。这样才能将 SR-IOV 直通功能暴露给 Firewall Threat Defense Virtual。以下操作程序可立即将 Firewall Threat Defense Virtual 升级到最新支持的虚拟硬件版本。

有关虚拟机硬件版本和兼容性的信息，请参阅 vSphere 虚拟机管理文档。

过程

步骤 1 从 vSphere Web 客户端登录到 vCenter 服务器。

步骤 2 找到要修改的 Firewall Threat Defense Virtual 计算机。

a) 选择数据中心、文件夹、集群、资源池或主机，然后点击**相关对象 (Related Objects)** 选项卡。

b) 点击**虚拟机 (Virtual Machines)**，并从列表中选择 Firewall Threat Defense Virtual机。

步骤 3 关闭所选的虚拟机。

步骤 4 右键点击该 Firewall Threat Defense Virtual，并依次选择**操作 (Actions)** > **所有 vCenter 操作 (All vCenter Actions)** > **兼容性 (Compatibility)** > **升级 VM 兼容性 (Upgrade VM Compatibility)**。

步骤 5 点击**是**以确认升级。

步骤 6 为虚拟机兼容性选择 **ESXi 5.5 及更高版本 (ESXi 5.5 and later)**选项。

步骤 7 （可选）选择**仅在正常访客操作系统关闭后升级 (Only upgrade after normal guest OS shutdown)**。

所选虚拟机将升级为您选择的相应硬件版本的兼容性设置，并且虚拟机的**摘要**选项卡中将更新为新的硬件版本。

下一步做什么

- 通过 SR-IOV 直通网络适配器将该 Firewall Threat Defense Virtual 与虚拟功能关联。

将 SR-IOV NIC 分配给 Firewall Threat Defense Virtual

为了确保 Firewall Threat Defense Virtual机和物理 NIC 可以交换数据，您必须将 Firewall Threat Defense Virtual 与一个或多个用作 SR-IOV 直通网络适配器的虚拟功能相关联。以下操作程序说明如何使用 vSphere Web 客户端将 SR-IOV NIC 分配给 Firewall Threat Defense Virtual机。

过程

步骤 1 从 vSphere Web 客户端登录到 vCenter 服务器。

步骤 2 找到要修改的 Firewall Threat Defense Virtual计算机。

a) 选择数据中心、文件夹、集群、资源池或主机，然后点击**相关对象 (Related Objects)** 选项卡。

b) 点击**虚拟机 (Virtual Machines)**，并从列表中选择 Firewall Threat Defense Virtual机。

步骤 3 在虚拟机的**管理**选项卡上，依次选择**设置** > **VM 硬件**。

步骤 4 点击**编辑 (Edit)**，然后选择**虚拟硬件 (Virtual Hardware)** 选项卡。

步骤 5 从**新建设备**下拉菜单中，选择**网络**，然后点击**添加**。

系统将显示**新建网络 (New Network)** 界面。

注释
连接 SR-IOV 接口时，将以相反的顺序连接接口。例如，“SR-IOV 网络适配器 1”接口被检测为以太网 0/1，而“SR-IOV 网络适配器 2”接口被检测为以太网 0/0。

步骤 6 展开**新建网络 (New Network)** 部分，然后选择可用的 SRIOV 选项。

注释
不支持内联流量，因为无法为 SR-IOV 接口启用混杂模式。

步骤 7 从**适配器类型 (Adapter Type)**下拉菜单中选择 **SR-IOV 直通 (SR-IOV passthrough)**。

步骤 8 从**物理功能 (Physical function)** 下拉菜单中，选择与直通虚拟机适配器相对应的物理适配器。

步骤 9 接通虚拟机电源。

接通虚拟机电源后，ESXi 主机将从物理适配器中选择一个可用的虚拟功能，并将其映射到 SR-IOV 直通适配器。主机将验证虚拟机适配器和底层虚拟功能的所有属性。

注释 由于混杂模式限制，某些使用 SR-IOV 驱动程序的 Intel 网络适配器（例如 Intel X710 或 82599）不支持在 Firewall Threat Defense Virtual 上将 SR-IOV 接口用作被动接口。在此情况下，请使用支持此功能的网络适配器。有关英特尔网络适配器的详细信息，请参阅英特尔以太网产品。

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。

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。

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。