Firepower Threat Defense Virtual 和 VMware 入门

思科 Firepower Threat Defense Virtual（FTDv）将 Cisco Firepower 新一代防火墙功能带到虚拟环境，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 Firepower Threat Defense Virtual 如何在 VMware ESXi 环境中工作，包括功能支持、系统要求、指导原则和限制。本章还介绍了管理 FTDv 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 Firepower 管理中心 或 Firepower 设备管理器 管理和监控 FTDv。其他管理选项也可能可用。

关于 Firepower Threat Defense Virtual 和 VMware

思科为 VMware vSphere vCenter 和 ESXi 托管环境打包了 64 位 Firepower Threat Defense Virtual (FTDv) 设备。FTDv 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 FTDv 部署到能够运行 VMware ESXi 的任何 x86 设备上。要部署 FTDv，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。

Firepower Threat Defense Virtual 支持的 VMware 功能

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

表 *1:* 的 *VMware* 功能支持 *FTDv*

特性	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。请参阅适用于 Firepower Threat Defense Virtual 和 VMware 的准则、限制和已知问题。
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	FMC 与受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	针对 Firepower Threat Defense Virtual VM 故障转移使用 Firepower 故障转移功能。
带 VM 心跳信号的 VMware HA	用于 VM 故障。	否	针对 Firepower Threat Defense Virtual VM 故障转移使用 Firepower 故障转移功能。
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	–

如何管理您的 Firepower 设备

您可以通过两种方法来管理您的 Firepower 威胁防御设备。

Firepower 设备管理器

Firepower 设备管理器 (FDM) 板载集成的管理器。

FDM 是一个基于 Web 的配置界面，在部分 Firepower 威胁防御 设备上可用。您可以通过 FDM 配置最常用于小型网络的软件的基本功能。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 Firepower 威胁防御 设备的大型网络。

注释 有关支持 FDM 的 Firepower 威胁防御 设备的列表，请参阅《适用于 Firepower 设备管理器的 Cisco Firepower 威胁防御配置指南》。

Firepower 管理中心

思科 Firepower 管理中心 (FMC)。

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

重要事项 您不能同时使用 FDM 和 FMC 管理 Firepower 设备。FDM 集成管理功能启用后，将无法使用 FMC 来管理 Firepower 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 FMC。另一方面，当您向 FMC 注册 Firepower 设备时，FDM 板载管理服务会被禁用。

注意 目前，Cisco 不提供将 FDM Firepower 配置迁移到 FMC 的选项，反之亦然。选择为 Firepower 设备配置的管理类型时，请考虑这一点。

系统要求

有关 Firepower Threat Defense Virtual 支持的虚拟机管理程序的最新信息，请参阅Cisco Firepower 兼容性指南。

根据所需部署的实例数量和使用要求，FTDv部署所使用的具体硬件可能会有所不同。每个 FTDv 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: Firepower Threat Defense Virtual* 设备资源

设置	值
核心和内存数	**6.4 及更高版本** FTDv 具有可调的 vCPU 和内存资源。支持的 vCPU/内存对值有三种： • 4vCPU/8GB（默认） • 8vCPU/16GB • 12vCPU/24GB 注释 要更改 vCPU/内存值，必须先断开 FTDv 设备的电源。仅支持上述三种组合。
	6.3 及更低版本 FTDv 具有固定的 vCPU 和内存资源。支持的 vCPU/内存对值只有一个： • 4vCPU/8GB 可以配置其他 vCPU/内存值；不过，仅支持上述三种组合。 注释 不允许调整 vCPU 和内存。
存储	取决于所选磁盘格式。 • 调配磁盘大小为 48.24 GB。

设置	值
vNIC	FTDv 支持以下虚拟网络适配器： • **VMXNET3** - 在 VMware 上，如果创建虚拟设备，FTDv 现默认为 vmxnet3 接口。先前，默认值为 e1000。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。 • **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，一个用于诊断。驱动程序不支持 FTDv 的故障转移 (HA) 部署。 • **E1000** - 使用 e1000 接口时，e1000 驱动程序的 FTDv 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 Firepower 版本，在 VMware 上，e1000 是 FTDv 的默认接口。从 6.4 版开始，VMware 上的 FTDv 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 13 页。 • **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”。

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。

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 FTDv 进行了测试。

- 核心
  - 每个 CPU 插槽至少 8 个物理核心
  - 8 个核心必须位于一个插槽中。

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

- Firepower 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

要快速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
```

适用于 Firepower Threat Defense Virtual 和 VMware 的准则、限制和已知问题

管理模式

- 您可以通过两种方法来管理您的 Firepower 威胁防御设备。
  - Firepower 设备管理器 (FDM) 板载集成的管理器。

    注释 VMware 上的 FTDv 支持运行 Cisco Firepower 6.2.2 及更高版本软件的 Firepower 设备管理器。VMware 上任何运行 Firepower 6.2.2 版之前软件的 FTDv 只能使用 Firepower 管理中心管理；请参阅如何管理您的 Firepower 设备，第 2 页
  - Firepower 管理中心 (FMC)
- 必须安装新版映像（6.2.2 或更高版本）才能取得 Firepower 设备管理器支持。不能在从较低版本（低于 6.2.2）更新现有 FTDv 虚拟机后切换至 Firepower 设备管理器。
- Firepower 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 Firepower 设备管理器时唯一受支持的模式。

OVF 文件准则

安装 Firepower Threat Defense Virtual 设备时有以下安装选项：

```
Cisco_Firepower_Threat_Defense_Virtual-VI-X.X.X-xxx.ovf
Cisco_Firepower_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 FTDv 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 Firepower 设备管理器进行本地管理（默认），或者使用 Firepower 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。这是唯一支持使用 Firepower 设备管理器的模式。

  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 Firepower 系统所需的设置。您可以将此 FTDv 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 Firepower Threat Defense Virtual。

vMotion 支持

如果计划使用 vMotion，建议仅使用共享存储。在部署过程中，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 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。

INIT 重生错误消息现象

您可能会在运行 ESXi 6 或 ESXi 6.5 的 FTDv 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. 右键单击虚拟机，然后选择**编辑设置**。
2. 在虚拟硬件选项卡中，从**新建设备**下拉菜单中选择**串行端口**，然后单击**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**选项卡中，展开**串行端口**，并选择连接类型**使用物理串行端口**。
4. 取消选中**在启动时连接**复选框。

   单击**确定**保存设置。

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。Firepower Threat Defense Virtual 使用混杂模式运行，通过在主用与备用角色之间切换 MAC 地址实现高可用性，确保正常运行。

如果采用默认设置，则系统将阻止 Firepower Threat Defense Virtual 正确运行。请参见以下要求的设置：

表 *3: 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”。

修改 vSphere 标准交换机的安全策略设置

默认设置会阻碍 FTDv的正确运行。

过程

步骤 1 在 vSphere Web 客户端中，导航至主机。

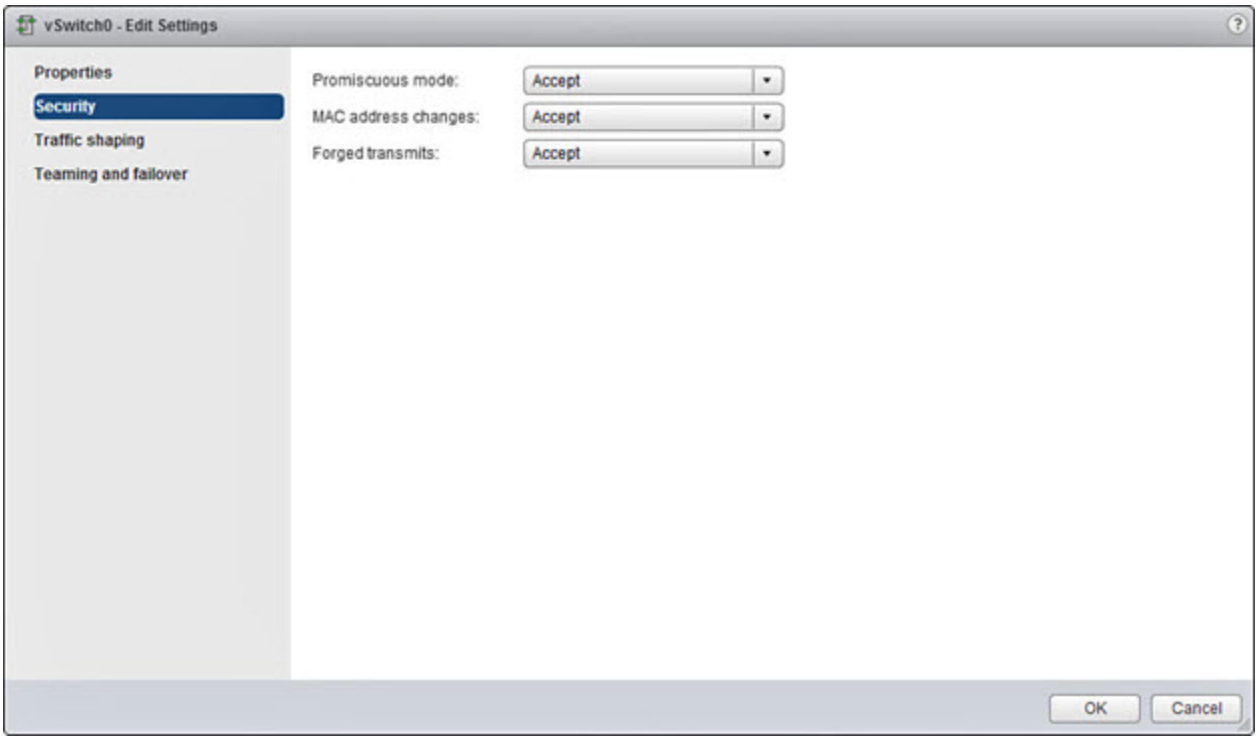
步骤 2 在**管理**选项卡中，单击**网络**，然后选择**虚拟交换机**。

步骤 3 从列表中选择一个标准交换机，然后单击**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 单击**确定**。

下一步做什么

- 确保在为 FTDv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。

规划接口

您可以在部署之前规划 Firepower Threat Defense Virtual vNIC 和接口映射，以避免重新启动和配置问题。FTDv 部署有 10 个接口，首次启动时必须通过至少 4 个接口通电。

FTDv 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，FTDv 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 FTDv 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 FTDv 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

- 如前所述，FTDv 部署有 10 个接口，首次启动时必须通过至少 4 个接口通电。您需要将网络分配给**至少四个接口**。
- 您无需使用全部 10 个 FTDv 接口；对于您不打算使用的接口，只需在 FTDv 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。

默认的 VMXNET3 接口

重要事项 FTDv 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。

- 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。
- 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 FTDv 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 FTDv 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 *4:* 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	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	源网络	目标网络	功能
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。头两个 PCI 设备必须配置为管理接口：一个用于设备管理/注册，一个用于诊断。
- 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 流量接口，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 Firepower Threat Defense Virtual 的故障转移 (HA) 部署。

E1000 接口

重要事项

FTDv 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。

- e1000 驱动程序的管理接口 (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。
- 如果您将 FTDv 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 FTDv 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 *5:* 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	Diagnostic0/0	管理与诊断
网络适配器 2	GigabitEthernet0-0	GigabitEthernet0/0	外部数据
网络适配器 3	GigabitEthernet0-1	GigabitEthernet0/1	内部日期

网络适配器	源网络	目标网络	功能
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，当您创建虚拟设备时，VMware 上的 FTDv 默认值为 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。

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不同类型的接口（例如在虚拟 Firepower 管理中心上使用 e1000 接口，在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不同类型的接口。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 FTDv 虚拟机电源。

要更改接口，必须关闭设备电源。

步骤 2 右键单击清单中的 FTDv 虚拟机，然后选择**编辑设置**。

步骤 3 选择适用的网络适配器，然后选择**删除**。

步骤 4 单击**添加**以打开**添加硬件向导**。

步骤 5 选择**以太网适配器**，然后单击**下一步**。

步骤 6 选择 vmxnet3 适配器，然后选择网络标签。

步骤 7 对 FTDv 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 FTDv 电源。

添加接口

部署 FTDv时，最多可以设置 10 个接口（1 个管理接口、1 个诊断接口和 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 FTDv 来自动识别它们。要给虚拟机添加接口，您需要完全清除 FTDv 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 FTDv 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。您既可以部署新虚拟机，也可以按《适用于 Firepower 设备管理器的 Cisco Firepower 威胁防御配置指南》“为 Firepower Threat Defense Virtual 添加接口”一节中的程序操作。