



《适用于 VMware 的 Cisco Firepower Threat Defense Virtual 入门指南》

首次发布日期: 2016 年 7 月 10 日

上次修改日期: 2020 年 5 月 29 日

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



第 1 章

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，第 1 页](#)
- [Firepower Threat Defense Virtual 支持的 VMware 功能，第 1 页](#)
- [如何管理您的 Firepower 设备，第 2 页](#)
- [系统要求，第 3 页](#)
- [适用于 Firepower Threat Defense Virtual 和 VMware 的准则、限制和已知问题，第 7 页](#)
- [规划接口，第 10 页](#)

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	<p>6.4 及更高版本</p> <p>FTDv 具有可调的 vCPU 和内存资源。支持的 vCPU/内存对值有三种：</p> <ul style="list-style-type: none"> • 4vCPU/8GB（默认） • 8vCPU/16GB • 12vCPU/24GB <p>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。</p>
	<p>6.3 及更低版本</p> <p>FTDv 具有固定的 vCPU 和内存资源。支持的 vCPU/内存对值只有一个：</p> <ul style="list-style-type: none"> • 4vCPU/8GB <p>可以配置其他 vCPU/内存值；不过，仅支持上述三种组合。</p> <p>注释 不允许调整 vCPU 和内存。</p>
存储	<p>取决于所选磁盘格式。</p> <ul style="list-style-type: none"> • 调配磁盘大小为 48.24 GB。

设置	值
vNIC	<p>FTDv 支持以下虚拟网络适配器：</p> <ul style="list-style-type: none"> • VMXNET3 - 在 VMware 上，如果创建虚拟设备，FTDv 默认认为 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。 <p>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。</p> <ul style="list-style-type: none"> • 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 VIOVF 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](#)，第 19 页。

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”。

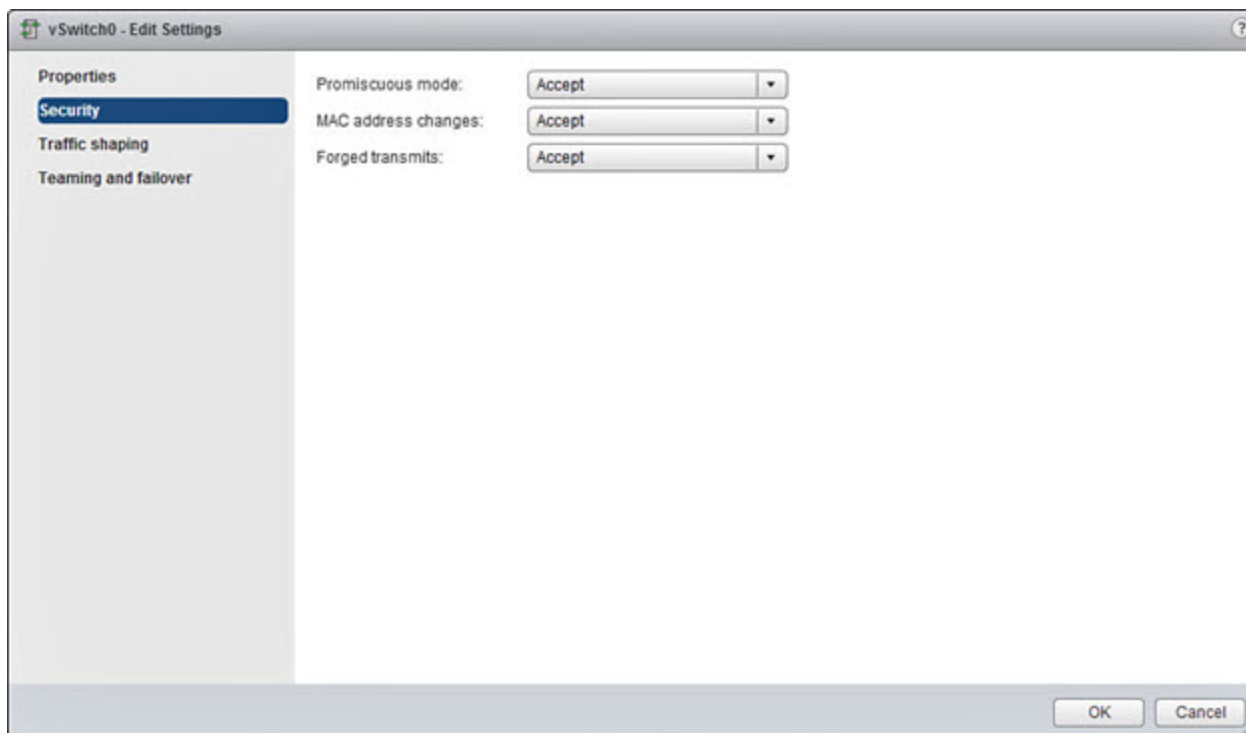
修改 vSphere 标准交换机的安全策略设置

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。



第 2 章

部署 Firepower Threat Defense Virtual

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

- [关于 VMware 部署，第 15 页](#)
- [向 vSphere vCenter 部署 Firepower Threat Defense Virtual，第 15 页](#)
- [向 vSphere ESXi 主机部署 Firepower Threat Defense Virtual，第 19 页](#)
- [使用 CLI 完成 Firepower Threat Defense Virtual 设置，第 22 页](#)

关于 VMware 部署

您可以将 Firepower Threat Defense Virtual (FTDv) 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 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。

FTDv 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。

向 vSphere vCenter 部署 Firepower Threat Defense Virtual

遵照此程序可将 Firepower Threat Defense Virtual (FTDv) 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 FTDv 虚拟机。

开始之前

- 在部署 FTDv 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** 单击文件 > 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。
- 步骤 3** 浏览文件系统以找到 OVF 模板源位置，然后单击下一步。
选择 Firepower Threat Defense Virtual VI OVF 模板：
`Cisco_Firepower_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** 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），然后单击下一步。
- 步骤 5** 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），单击接受同意许可条款，然后单击下一步。
- 步骤 6** 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 FTDv 的位置（主机或集群），然后单击下一步。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 7** 导航至想要在其中运行 Firepower Threat Defense Virtual 的资源池并将其选中，然后单击下一步。
注释 仅当集群包含资源池时，系统才会显示此页面。
- 步骤 8** 选择部署配置。从配置下拉列表中的三个受支持的 vCPU/内存值中选择一个，然后单击下一步。
重要事项 从 6.4 版开始，FTDv 具有可调的 vCPU 和内存资源。在 6.4 版之前，FTDv 具有固定配置 4VCPU/8GB 设备；请参阅[系统要求，第 3 页](#)。
- 步骤 9** 选择要存储虚拟机文件的存储位置，然后单击下一步。
在此页面上，您可以从目标集群或主机上已配置的 Datastore 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 Datastore，以容纳虚拟机及其所有虚拟磁盘文件。
- 步骤 10** 选择磁盘格式以存储虚拟机虚拟磁盘，然后单击下一步。
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 11** 在网络映射页面，将 OVF 模板中指定的网络映射到您清单中的网络，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 Firepower 管理中心或 Firepower 设备管理器配置，具体取决于您的管理模式。

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。

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，右键单击 FTDv 实例，然后选择**编辑设置**。但是，该屏幕不会显示 FTDv ID（仅显示网络适配器 ID）。

请查看适用于 FTDv 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 6: 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	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 FTDv 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 FTDv 接口；对于不打算使用的接口，只需在 FTDv 配置中将其禁用即可。

步骤 12 在属性页面，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 FTDv 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。单击**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 Firepower 设备管理器配置工具。选择否将使用 Firepower 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[如何管理您的 Firepower 设备](#)，第 2 页。

d) 防火墙模式

设定初始防火墙模式。单击**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。不能使用本地的 Firepower 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 FMC 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 (-)。当您设备添加到 FMC 时，需要记住此注册密钥。
- **NAT ID** - 如果 FTDv 和 FMC 被网络地址转换 (NAT) 设备分隔，并且 FIREPOWER 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) 单击下一步。

步骤 13 在**即将完成**部分，查看并验证显示的信息。要使用这些设置开始部署，单击**完成**。要进行更改，单击**后退**以在屏幕中向后导航。

或者，选中**部署后启动**选项启动 FTDv，然后单击**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”中的指定数据中心下会显示 FTDv 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 FTDv，FTDv 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 Firepower 管理中心管理 FTDv；请参阅[使用 Firepower 管理中心管理 Firepower Threat Defense Virtual](#)，第 25 页。

- 如果为启用本地管理器选择是，您将使用集成的 Firepower 设备管理器管理 FTDv；请参阅[使用 Firepower 设备管理器管理 Firepower Threat Defense Virtual](#)，第 41 页。

有关如何选择管理选项的概述，请参阅[如何管理您的 Firepower 设备](#)，第 2 页。

向 vSphere ESXi 主机部署 Firepower Threat Defense Virtual

遵照此程序可在单个 ESXi 主机上部署 Firepower Threat Defense Virtual (FTDv) 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 FTDv 虚拟机）。



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 Firepower Threat Defense Virtual 设备部署到 vCenter 环境的说明，请参阅[向 vSphere vCenter 部署 Firepower Threat Defense Virtual](#)，第 15 页。

开始之前

- 在部署 FTDv 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 从 Cisco.com 下载适用于 VMware ESXi 的 Firepower 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_Firepower_Threat_Defense_Virtual-VI-X.X.X-xx.ovf - 适用于 vCenter 部署
- Cisco_Firepower_Threat_Defense_Virtual-ESXi-X.X.X-xx.ovf - 适用于 ESXi 部署。
- Cisco_Firepower_Threat_Defense_Virtual-X.X.X-xx.vmdk - VMware 虚拟磁盘文件。
- Cisco_Firepower_Threat_Defense_Virtual-VI-X.X.X-xx.mf - 适用于 vCenter 部署的清单文件。
- Cisco_Firepower_Threat_Defense_Virtual-ESXi-X.X.X-xx.mf - 适用于 ESXi 部署的清单文件。

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 单击登录继续。

此时您即已登录到目标 ESXi 主机。

步骤 6 右键单击 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，然后单击下一步。

步骤 8 在向导的选择 OVF 和 VMDK 文件页面：

a) 输入您的 FTDv 虚拟机的名称。

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) 单击蓝色窗格，浏览到您将 FTDv 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_Firepower_Threat_Defense_Virtual-ESXi-X.X.X-xx.ovf`

`Cisco_Firepower_Threat_Defense_Virtual-X.X.X-xx.vmdk`

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 单击下一步。

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 单击下一步。

步骤 12 配置随适用于 FTDv 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 Firepower 管理中心或 Firepower 设备管理器配置，具体取决于您的管理模式。

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。

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，右键单击 FTDv 实例，然后选择**编辑设置**。但是，该屏幕不会显示 FTDv ID（仅显示网络适配器 ID）。

请查看适用于 FTDv 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 7: 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	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 FTDv 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 FTDv 接口；对于不打算使用的接口，只需在 FTDv 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。

- （可选）单击**返回**以返回并查看或修改向导设置。
- （可选）单击**取消**以放弃创建任务并关闭向导。
- 单击**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 FTDv 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 FTDv，FTDv 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 FTDv 时的下一步；请参阅[使用 CLI 完成 Firepower Threat Defense Virtual 设置](#)，第 22 页。

使用 CLI 完成 Firepower Threat Defense Virtual 设置

使用 ESXi OVF 模板部署时，必须使用 CLI 设置 FTDv。Firepower Threat Defense Virtual 设备没有 Web 界面。如果使用 VIOVF 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 Firepower 系统所需的设置。



注释 如果使用 VIOVF 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 Firepower 威胁防御系统启动时，安装向导会提示您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 Firepower 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 FTDv，FTDv 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 Firepower 管理中心管理 FTDv；请参阅[使用 Firepower 管理中心管理 Firepower Threat Defense Virtual](#)，第 25 页。
- 如果为启用本地管理器选择是，您将使用集成的 Firepower 设备管理器管理 FTDv；请参阅[使用 Firepower 设备管理器管理 Firepower Threat Defense Virtual](#)，第 41 页。

有关如何选择管理选项的概述，请参阅[如何管理您的 Firepower 设备](#)，第 2 页。



第 3 章

使用 Firepower 管理中心管理 Firepower Threat Defense Virtual

本章介绍如何部署使用 FMC 管理的独立式 FTDv 设备。



注释

本文档涵盖最新的 FTDv 版本功能；有关功能更改的详细信息，请参阅使用 [Firepower Management 管理 Firepower Threat Defense Virtual 的历史](#)，第 39 页。如果您使用的是旧版本的软件，请参考您的版本的《FMC 配置指南》中的步骤。

- [关于使用 Firepower 管理中心管理的 Firepower Threat Defense Virtual](#)，第 25 页
- [登录到 Firepower 管理中心](#)，第 26 页
- [向 Firepower 管理中心注册设备](#)，第 26 页
- [配置基本安全策略](#)，第 28 页
- [访问 Firepower 威胁防御 CLI](#)，第 39 页
- [使用 Firepower Management 管理 Firepower Threat Defense Virtual 的历史](#)，第 39 页

关于使用 Firepower 管理中心管理的 Firepower Threat Defense Virtual

Firepower Threat Defense Virtual (FTDv) 是思科 NGFW 解决方案的虚拟化组件。FTDv 提供各种下一代防火墙服务，包括状态防火墙、路由、下一代入侵防御系统(NGIPS)、应用可视性与可控性(AVC)、URL 过滤，以及高级恶意软件防护 (AMP)。

您可以使用 Firepower 管理中心 (FMC) 管理 FTDv，这是一个功能齐全的多设备管理器，位于单独的服务器上。有关安装 FMC 的详细信息，请参阅 [FMC 入门指南](#)。

FTDv 向您分配给 FTDv 虚拟机的管理接口上的 FMC 注册并与之通信。

要进行故障排除，您可以使用管理接口上的 SSH 访问 FTD CLI，也可以从 Firepower CLI 连接到 FTD。

登录到 Firepower 管理中心

使用 FMC 配置并监控 FTD。

开始之前

有关受支持浏览器的信息，请参阅您所用版本的发行说明（参阅<https://www.cisco.com/go/firepower-notes>）。

过程

步骤 1 使用支持的浏览器输入以下 URL。

https://fmc_ip_address

- *fmc_ip_address* - 标识 FMC 的 IP 地址或主机名。

步骤 2 输入您的用户名和密码。

步骤 3 单击 **Log In**。

向 Firepower 管理中心注册设备

开始之前

确保 FTDv 虚拟机已部署成功、已接通电源并且已首次完成其启动程序。

过程

步骤 1 选择设备 > 设备管理。

步骤 2 从添加下拉列表选择添加设备，然后输入以下参数。

Add Device ?

Host:†

Display Name:

Registration Key:*

Group:

Access Control Policy:*

Smart Licensing

Malware
 Threat
 URL Filtering

Advanced

Unique NAT ID:†

Transfer Packets

- **主机** - 输入要添加的逻辑设备的 IP 地址。如果您在 FTD 引导程序配置中指定了 FMC IP 地址和 NAT ID，则可以将此字段留空。
- **显示名称** - 输入要在 FMC 中显示的逻辑设备的名称。
- **注册密钥** - 输入您在 FTDv 引导程序配置中指定的注册密钥。
- **Domain** - 如果有多域环境，请将设备分配给分叶域。
- **Group** - 如果在使用组，则将其分配给设备组。

- **Access Control Policy** - 选择初始策略。除非已经拥有您知道自己需要使用的自定义策略，否则选择 **Create new policy**，然后选择 **Block all traffic**。之后您可以更改此设置以允许流量通过；请参阅[配置访问控制](#)，第 37 页。

- **Smart Licensing** - 为要部署的功能分配所需的智能许可证：**Malware**（如果您打算使用 AMP 恶意软件检查）、**Threat**（如果您打算使用入侵防御）、**URL**（如果您打算实施基于类别的 URL 过滤）。
- **唯一 NAT ID** - 指定您在 FTDv 启动程序配置中指定的 NAT ID。
- **Transfer Packets** - 可让设备将数据包传输至 FMC。如果在启用此选项时触发了 IPS 或 Snort 等事件，设备会将事件元数据信息和数据包数据发送到 FMC 进行检测。如果禁用此选项，只有事件信息会发送到 FMC，数据包数据不发送。

步骤 3 单击 **Register**，并确认注册成功。

如果注册成功，设备将添加到列表中。如果注册失败，您会看到一则错误消息。如果 FTDv 注册失败，请检查以下项：

- **Ping** - 访问 FTD CLI ([访问 Firepower 威胁防御 CLI](#)，第 39 页)，然后使用以下命令 ping FMC IP 地址：

```
ping system ip_address
```

 如果 ping 不成功，使用 **show network** 命令检查网络设置。如果需要更改 FTDIP 地址，使用 **configure network {ipv4 | ipv6} manual** 命令。
- **NTP** - 确保 NTP 服务器与系统 > 配置 > 时间同步页面上的 FMC 服务器设定一致。
- **注册密钥、NAT ID 和 FMCIP 地址** - 确保在两个设备上使用相同的注册密钥和 NAT ID（如有使用）。可以在 FTDv 上使用 **configure manager add** 命令设定注册密钥和 NAT ID。也可以使用此命令更改 FMCIP 地址。

配置基本安全策略

本部分介绍如何使用以下设置配置基本安全策略：

- 内部和外部接口 - 为内部接口分配静态 IP 地址，并将 DHCP 用作外部接口。
- DHCP 服务器 - 在内部接口上为客户端使用 DHCP 服务器。
- 默认路由 - 通过外部接口添加默认路由。
- NAT - 在外部接口上使用接口 PAT。
- 访问控制 - 允许流量从内部传到外部。

过程

- 步骤 1 [配置接口，第 29 页](#)
 - 步骤 2 [配置 DHCP 服务器，第 32 页](#)
 - 步骤 3 [添加默认路由，第 33 页](#)
 - 步骤 4 [配置 NAT，第 34 页](#)
 - 步骤 5 [配置访问控制，第 37 页](#)
 - 步骤 6 [部署配置，第 38 页](#)
-

配置接口

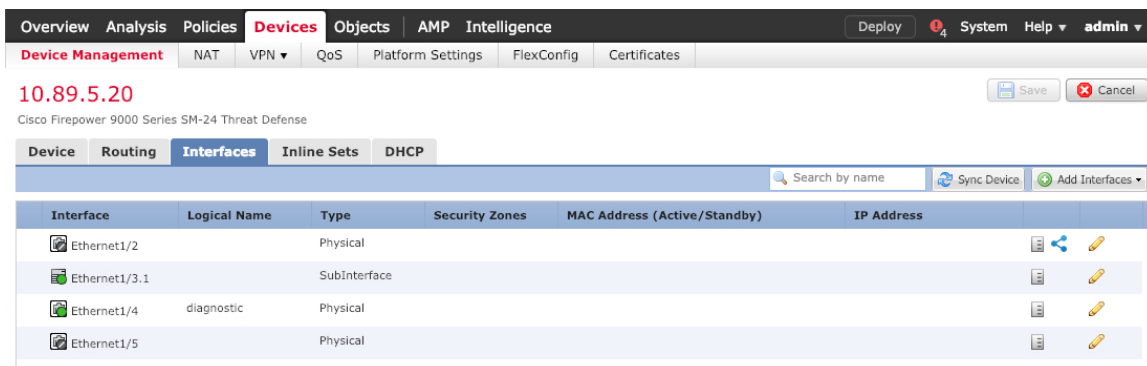
启用 FTDv 接口，为其分配安全区域并设置 IP 地址。通常，您必须至少配置两个接口才能让系统传递有意义的流量。通常，您将拥有面向上游路由器或互联网的外部接口，以及组织网络的一个或多个内部接口。其中一些接口可能是“隔离区”（DMZ），您可以在其中放置可公开访问的资产，例如 Web 服务器。


典型的边缘路由情况是通过 DHCP 从 ISP 获取外部接口地址，同时在内部接口上定义静态地址。

以下示例使用 DHCP 在接口内部配置了一个路由模式（含静态地址），并在接口外部配置了一个路由模式。

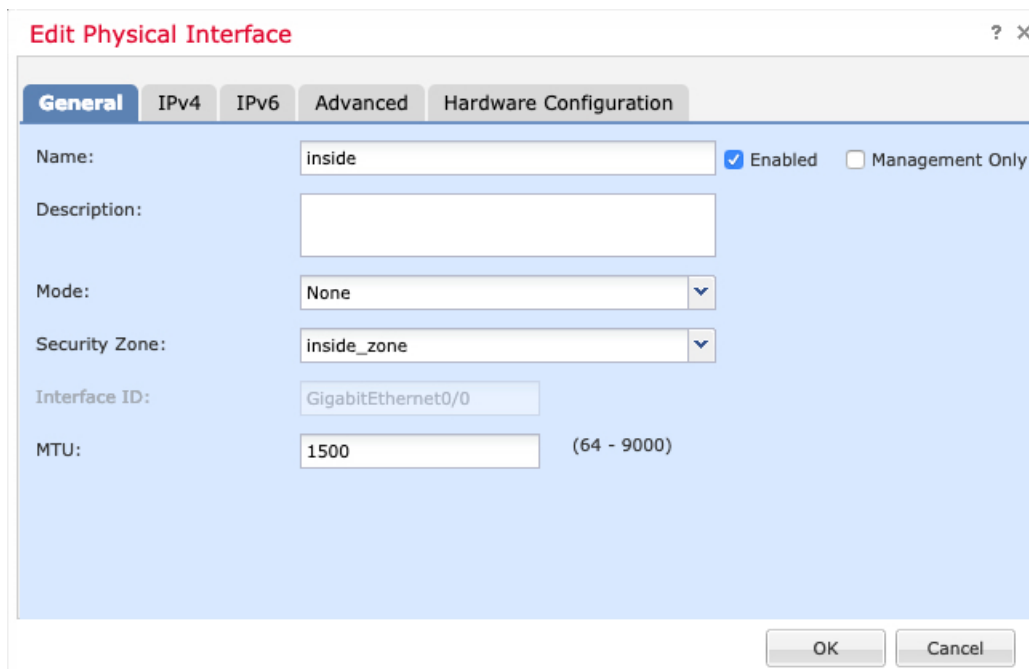
过程

- 步骤 1 选择 **Devices > Device Management**，然后单击设备的编辑（）。
- 步骤 2 单击 **Interfaces**。



步骤 3 单击要用于内部的接口的编辑（）。

General 选项卡将显示。



- 输入长度最大为 48 个字符的 **Name**。
例如，将接口命名为 **inside**。
- 选中 **Enabled** 复选框。
- 将 **Mode** 保留为 **None**。
- 从 **Security Zone** 下拉列表中选择一个现有的内部安全区域，或者单击 **New** 添加一个新的安全区域。

例如，添加一个名为 **inside_zone** 的区域。必须将每个接口分配给安全区域和/或接口组。每个接口只能属于一个安全区域，但可以同时属于多个接口组。您可以根据区域或组应用安全策略。例如，您可以将内部接口分配到内部区域，而将外部接口分配到外部区域。然后可以配置访问控制策略，允许流量从内部传到外部，但不允许从外部传入内部。大多数策略仅支持安全区域；您可以在 NAT 策略、预过滤器策略和 QoS 策略中使用区域或接口组。

e) 单击 **IPv4** 和/或 **IPv6** 选项卡。

- **IPv4** - 从下拉列表中选择 **Use Static IP**，然后以斜杠表示法输入 IP 地址和子网掩码。
例如，输入 **192.168.1.1/24**

- **IPv6** - 为无状态自动配置选中 **Autoconfiguration** 复选框。

f) 单击**确定**。

步骤 4 单击要用于外部的接口的 **编辑** (✎)。

General 选项卡将显示。

a) 输入长度最大为 48 个字符的 **Name**。

例如，将接口命名为 **outside**。

b) 选中 **Enabled** 复选框。

c) 将 **Mode** 保留为 **None**。

d) 从 **Security Zone** 下拉列表中选择 一个现有的外部安全区域，或者单击 **New** 添加一个新的安全区域。

例如，添加一个名为 **outside_zone** 的区域。

e) 单击 **IPv4** 和/或 **IPv6** 选项卡。

- **IPv4** - 选择 **Use DHCP**，然后配置以下选填参数：
 - **Obtain default route using DHCP** - 从 DHCP 服务器获取默认路由。
 - **DHCP route metric** - 分配到所获悉路由的管理距离，介于 1 和 255 之间。获悉的路由的默认管理距离为 1。

The screenshot shows the 'Edit Physical Interface' dialog box with the 'IPv4' tab selected. The 'IP Type' dropdown menu is set to 'Use DHCP'. Below it, the 'Obtain default route using DHCP' checkbox is checked. The 'DHCP route metric' is set to '1', with a range of '(1 - 255)' shown to the right.

- **IPv6** - 为无状态自动配置选中 **Autoconfiguration** 复选框。

f) 单击确定。

步骤 5 单击保存。

配置 DHCP 服务器

如果希望客户端使用 DHCP 从 FTDv 处获取 IP 地址，请启用 DHCP 服务器。

过程

步骤 1 选择 **Devices > Device Management**，然后单击设备的编辑（✎）。

步骤 2 选择 **DHCP > DHCP Server**。

步骤 3 在 **Server** 页面上单击 **Add**，然后配置以下选项：

The screenshot shows the 'Add Server' dialog box. The 'Interface*' dropdown menu is set to 'inside'. The 'Address Pool*' is set to '10.9.7.9-10.9.7.25', with a range of '(2.2.2.10-2.2.2.20)' shown to the right. The 'Enable DHCP Server' checkbox is checked. 'OK' and 'Cancel' buttons are at the bottom.

- **Interface** -- 从下拉列表中选择接口。

- **Address Pool** - DHCP 服务器使用的 IP 地址的范围（从最低到最高）。IP 地址范围必须与选定接口位于相同的子网上，且不能包括接口自身的 IP 地址。
- **Enable DHCP Server** - 在所选接口上启用 DHCP 服务器。

步骤 4 单击确定。

步骤 5 单击保存。

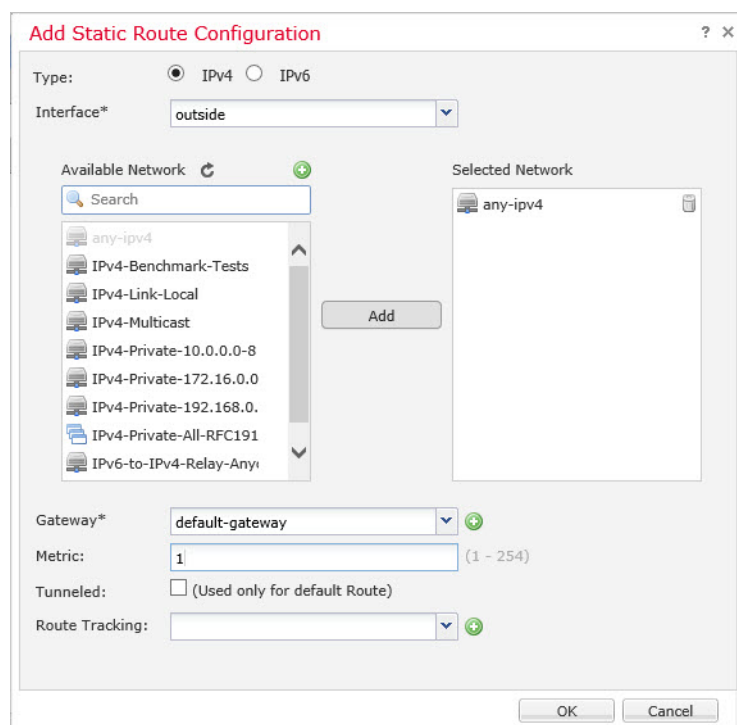
添加默认路由

默认路由由通常指向可从外部接口访问的上游路由器。如果您将 DHCP 用作外部接口，则您的设备可能已经收到了默认路由。如果需要手动添加路由，则遵照此程序执行。如果收到来自 DHCP 服务器的默认路由，其将显示在 **Devices > Device Management > Routing > Static Route** 页面上的 **IPv4 Routes** 或 **IPv6 Routes** 表中。

过程

步骤 1 选择 **Devices > Device Management**，然后单击设备的编辑（）。

步骤 2 选择 **Route > Static Route**，单击 **Add Route**，然后设置以下项：

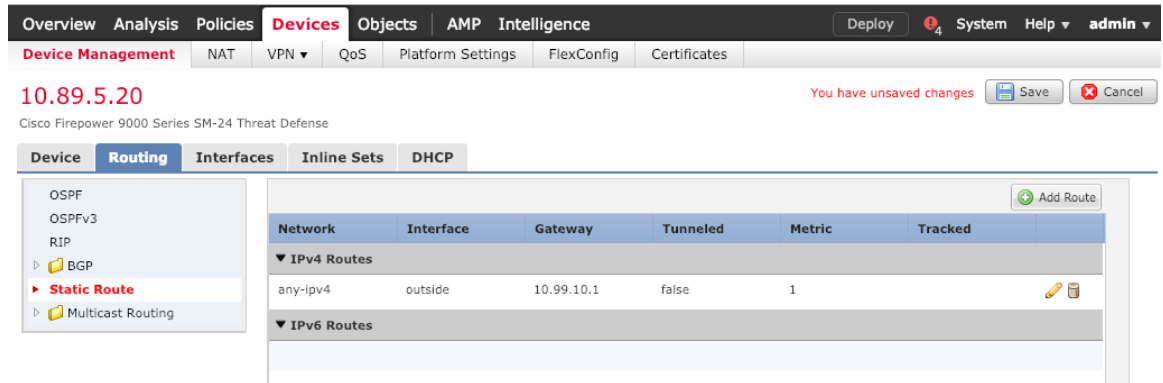


- **Type** - 根据要添加静态路由的类型，单击 **IPv4** 或 **IPv6** 单选按钮。
- **Interface** - 选择出口接口；通常是外部接口。

- 可用网络 - 为 IPv4 默认路由选择 **any-ipv4**，为 IPv6 默认路由选择 **any-ipv6**。
- **Gateway** 或 **IPv6 Gateway** - 输入或选择作为此路由的下一个跃点的网关路由器。您可以提供 IP 地址或网络/主机对象。
- **Metric** - 输入到目标网络的跃点数。有效值范围为 1 到 255；默认值为 1。

步骤 3 单击 **OK**。

路由即已添加至静态路由表。



步骤 4 单击保存。

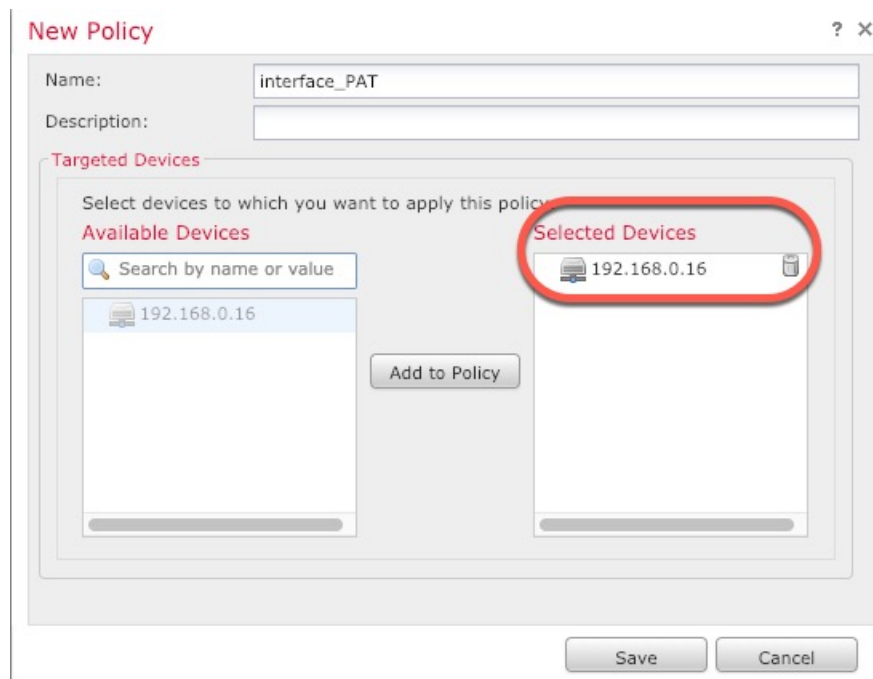
配置 NAT

典型的 NAT 规则会将内部地址转换为外部接口 IP 地址上的端口。这类 NAT 规则称为接口端口地址转换 (*PAT*)。

过程

步骤 1 选择 **Devices > NAT**，然后单击 **New Policy > Threat Defense NAT**。

步骤 2 为策略命名，选择要使用策略的设备，然后单击 **Save**。

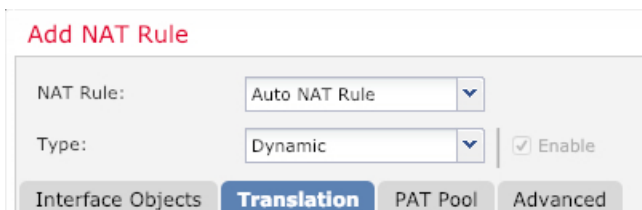


策略即已添加 FMC。您仍然需要为策略添加规则。

步骤 3 单击 **Add Rule**。

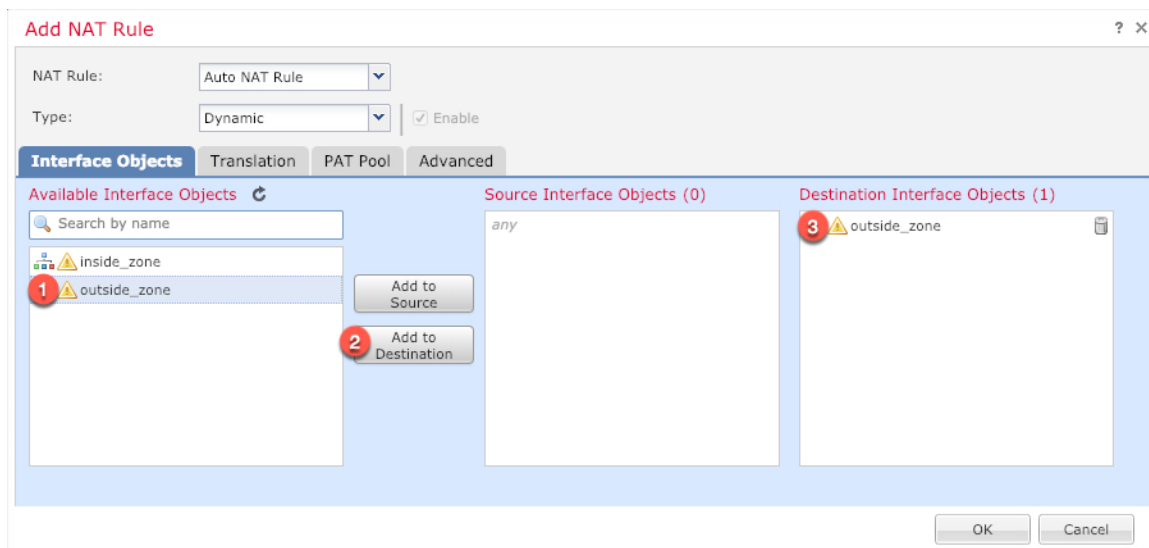
Add NAT Rule 对话框将显示。

步骤 4 配置基本规则选项：

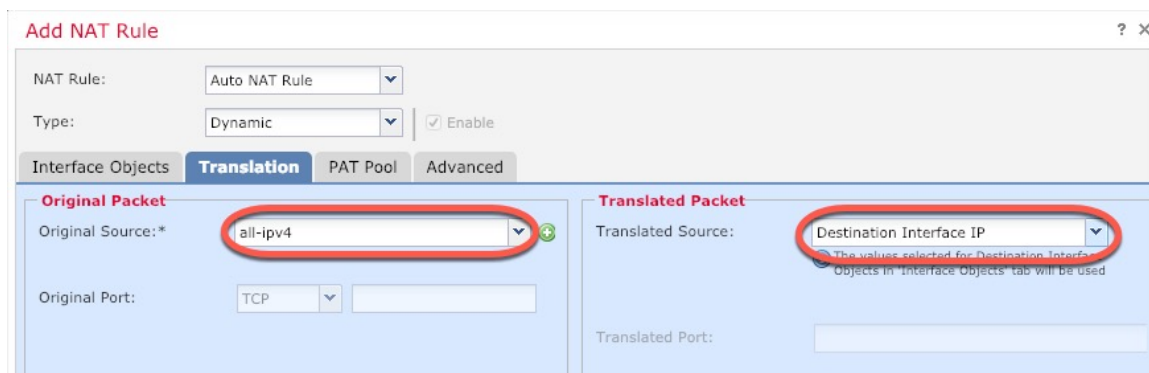


- **NAT Rule** - 选择 **Auto NAT Rule**。
- **Type** - 选择 **Dynamic**。

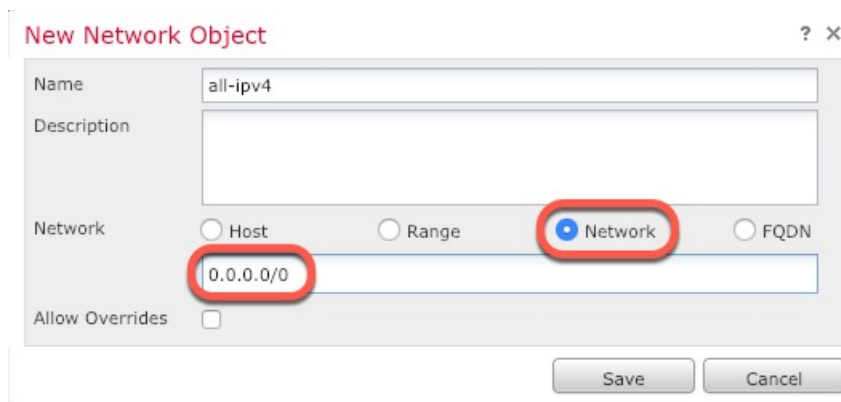
步骤 5 在 **Interface Objects** 页面，将 **Available Interface Objects** 区域中的外部区域添加到 **Destination Interface Objects** 区域。



步骤 6 在 **Translation** 页面上配置以下选项：



- 原始源 - 单击添加 (+) 为所有 IPv4 流量添加网络对象 (0.0.0.0/0)。

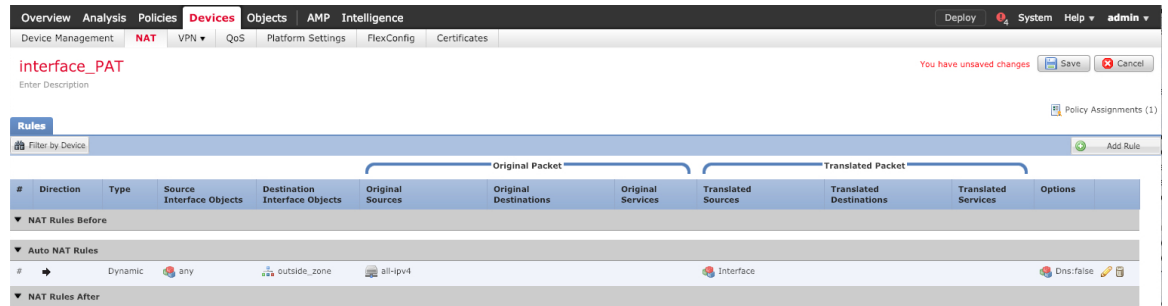


注释 您不能使用系统定义的 **any-ipv4** 对象，因为自动 NAT 规则在对象定义过程中添加 NAT，并且您无法编辑系统定义的对象。

- **Translated Source** - 选择 **Destination Interface IP**。

步骤 7 单击 **Save** 以添加规则。

规则即已保存至 **Rules** 表。



步骤 8 单击 **NAT** 页面上的 **Save** 以保存更改。

配置访问控制

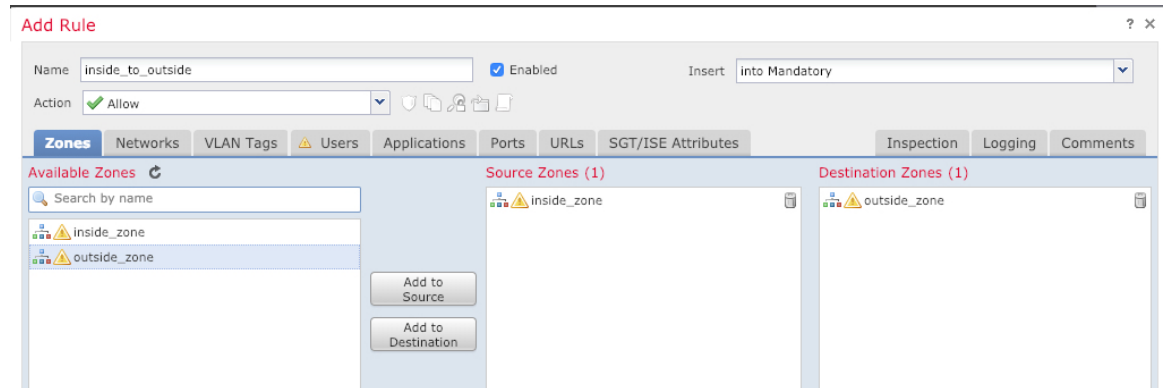
如果您在使用 FMC 注册 FTDv 时创建了基本的封锁所有流量访问控制策略，则需要向策略添加规则以允许流量通过设备。以下程序可添加规则以允许从内部区域到外部区域的流量。如有其他区域，请务必添加允许流量到适当网络的规则。

请参阅 FMC 配置指南以配置更高级的安全设置和规则。

过程

步骤 1 选择 **Policy > Access Policy > Access Policy**，然后单击分配给 FTD 的访问控制策略的编辑（✎）。

步骤 2 单击 **Add Rule** 并设置以下参数：

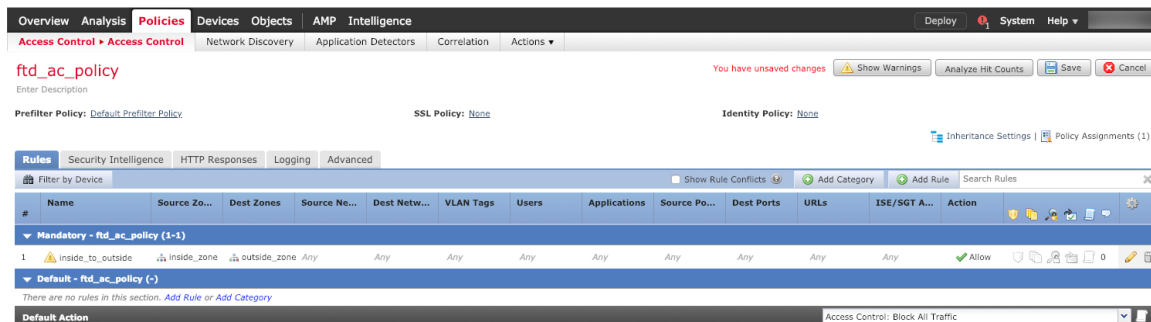


- **Name** - 为此规则命名，例如 **inside_to_outside**。
- **Source Zones** - 从 **Available Zones** 中选择内部区域，然后单击 **Add to Source**。
- **Destination Zones** - 从 **Available Zones** 中选择外部区域，然后单击 **Add to Destination**。

其他设置保留原样。

步骤 3 单击 **Add**。

规则即已添加至 **Rules** 表。



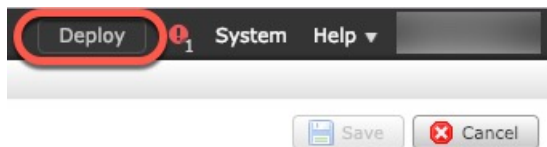
步骤 4 单击保存。

部署配置

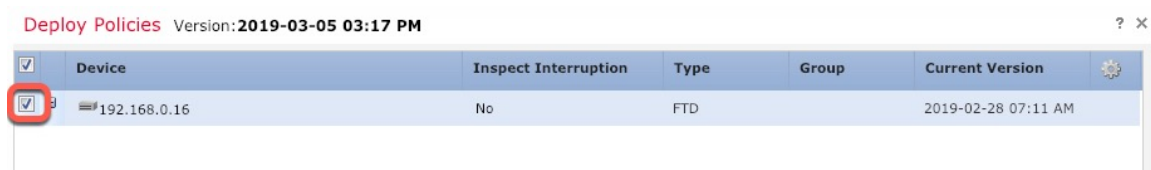
将配置更改部署到 FTDv；在部署之前，您的所有更改都不会在设备上生效。

过程

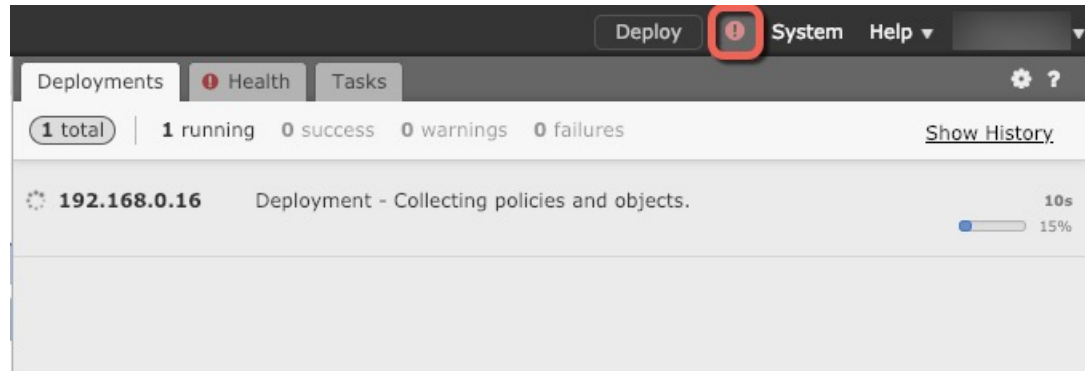
步骤 1 单击右上方的 **Deploy**。



步骤 2 选择 **Deploy Policies** 对话框中的设备，然后单击 **Deploy**。



步骤 3 确保部署成功。单击菜单栏中 **Deploy** 按钮右侧的图标可以查看部署状态。



访问 Firepower 威胁防御 CLI

您可以使用 FTDv CLI 更改管理接口参数并进行故障排除。要访问 CLI，可以使用管理接口上的 SSH，也可以从 VMware 控制台连接。

过程

步骤 1（选项 1）通过 SSH 直接连接到 FTDv 管理接口的 IP 地址。

在部署虚拟机时，您需要设置管理 IP 地址。使用 **admin** 帐户和初始部署期间设定的密码登录 FTDv。

步骤 2（选项 2）打开 VMware 控制台并使用默认用户名 **admin** 帐户和初始部署期间设定的密码登录。

使用 Firepower Management 管理 Firepower Threat Defense Virtual 的历史

功能名称	平台版本	功能信息
FMC 管理	6.0	初始支持。



第 4 章

使用 Firepower 设备管理器管理 Firepower Threat Defense Virtual

本章介绍如何部署使用 FDM 管理的独立式 FTDv 设备。要部署高可用性对，请参阅 FDM 配置指南。

- [关于使用 Firepower 设备管理器管理的 Firepower Threat Defense Virtual](#)，第 41 页
- [初始配置](#)，第 42 页
- [如何在 Firepower 设备管理器中配置设备](#)，第 44 页

关于使用 Firepower 设备管理器管理的 Firepower Threat Defense Virtual

Firepower Threat Defense Virtual (FTDv) 是思科 NGFW 解决方案的虚拟化组件。FTDv 提供各种下一代防火墙服务，包括状态防火墙、路由、下一代入侵防御系统(NGIPS)、应用可视性与可控性(AVC)、URL 过滤，以及高级恶意软件防护 (AMP)。

您可以使用 Firepower 设备管理器 (FDM) 管理 FTDv，这是部分 Firepower 威胁防御 型号中包含的基于 Web 的设备设置向导。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。

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 Firepower 管理中心（而不是集成的 Firepower 设备管理器）来配置您的设备。有关详细信息，请参阅[使用 Firepower 管理中心管理 Firepower Threat Defense Virtual](#)，第 25 页。

要进行故障排除，您可以使用管理接口上的 SSH 访问 FTD CLI，也可以从 Firepower CLI 连接到 FTD。

默认配置

FTDv 默认配置将管理接口和内部接口置于同一子网上。您的管理接口必须具有互联网连接，才能使用智能许可并获取系统数据库的更新。

因此，默认配置的设计使您可以将 Management0-0 和 GigabitEthernet0-1（内部）两个接口都连接到虚拟交换机上的同一网络。默认管理地址使用内部 IP 地址作为网关。因此，管理接口路由通过内部接口，然后通过外部接口连通互联网。

您还可以选择将 Management0-0 连接到与用于内部接口的子网不同的子网，只要使用具有互联网接入的网络即可。确保为网络正确配置管理接口 IP 地址和网关。

FTDv 首次启动时，必须启用至少四个接口：

- 虚拟机的第一个接口 (Management0-0) 是管理接口。
- 虚拟机上的第二个接口是诊断接口 (Diagnostic0-0)。
- 虚拟机的第三个接口 (GigabitEthernet0-0) 是外部接口。
- 虚拟机的第四个接口 (GigabitEthernet0-1) 是内部接口。

您还可以添加最多六个额外的数据流量接口，使数据接口的总数达到八个。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。请参阅“配置 VMware 接口”。

初始配置

您必须完成初始配置，才能使 FTDv 在网络中正常运行，其中包括配置将安全设备插入网络以及将其连接到互联网或其他上游路由器所需的地址。您可以通过以下两种方式进行系统初始配置：

- 使用 FDM Web 界面（推荐）。FDM 在您的网络浏览器中运行。使用该界面可配置、管理和监控系统。
- 使用命令行界面 (CLI) 设置向导（可选）。可以使用 CLI 设置向导（而不是 FDM）进行初始配置，并可以使用 CLI 执行故障排除。您仍然可以使用 FDM 来配置、管理和监控系统；请参阅（可选）“启动 Firepower 威胁防护 CLI 向导”。

以下主题介绍如何使用这些界面来执行系统初始配置。

启动 Firepower 设备管理器

在首次登录 Firepower 设备管理器 (FDM) 时，系统会通过设备设置向导指导您完成初始系统配置。

过程

步骤 1 打开浏览器并登录 FDM。假定您未在 CLI 中进行初始配置，请在 <https://ip-address> 中打开 Firepower 设备管理器，其中地址为以下项之一：

- 如果您连接到内部桥组界面：<https://192.168.1.1>。
- 如果连接到管理物理接口，则地址为：<https://192.168.45.45>。

步骤 2 使用用户名 **admin** 和密码 **Admin123** 登录。

步骤 3 如果是首次登录系统，而且您未使用过 CLI 安装向导，系统将提示您阅读并接受“最终用户许可协议”以及更改管理员密码。只有完成这些步骤，才能继续。

步骤 4 为外部接口和管理接口配置以下选项，然后单击下一步。

注释 单击下一步后，您的设置将部署到设备中。该接口将命名为“outside”，并添加到“outside_zone”安全区。确保您的设置正确。

a) **Outside Interface** - 即连接到网关调制解调器或路由器的数据端口。在初始设备设置期间，您不能选择其他外部接口。第一个数据接口是默认的外部接口。

配置 IPv4 (Configure IPv4) - 外部接口的 IPv4 地址。可以使用 DHCP，也可以手动输入静态 IP 地址、子网掩码和网关。另外，也可以选择关，不配置 IPv4 地址。

配置 Ipv6 - 外部接口的 Ipv6 地址可以使用 DHCP，也可以手动输入静态 IP 地址、前缀和网关。另外，也可以选择关，不配置 IPv6 地址。

b) **管理接口**

DNS 服务器 - 系统管理地址的 DNS 服务器。输入 DNS 服务器的一个或多个地址以解析名称。默认值为 OpenDNS 公共 DNS 服务器。如果您编辑字段并想要恢复默认值，请单击使用 **OpenDNS** 以重新将合适的 IP 地址载入字段。

防火墙主机名 - 系统管理地址的主机名。

注释 在使用设备设置向导配置 Firepower 威胁防御设备时，系统会为出站和入站流量提供两个默认访问规则。您可以在完成初始配置后更改这些访问规则。

步骤 5 配置系统时间设置，然后单击下一步。

a) **时区** - 选择系统时区。

b) **NTP 时间服务器** - 选择使用默认 NTP 服务器，还是手动输入 NTP 服务器的地址。可以添加多个服务器来提供备份。

步骤 6 为系统配置智能许可证。

只有具有智能许可证账户，才能获取和应用系统需要的许可证。最初，可以使用为期 90 天的评估许可证，以后再设置智能许可。

要立即注册设备，请单击链接登录您的智能软件管理器账户，生成新的令牌，并将该令牌复制到编辑框。

要使用评估许可证，请选择 **Start 90 day evaluation period without registration**。如需稍后注册设备并获取智能许可证，请单击菜单中的设备名称打开 **Device Dashboard**，然后单击 **Smart Licenses** 组中的链接。

步骤 7 单击 **Finish**。

下一步做什么

- 使用 Firepower 设备管理器配置设备；请参阅[如何在 Firepower 设备管理器中配置设备](#)，第 44 页。

如何在 Firepower 设备管理器中配置设备

完成设置向导后，您的设备应该会正常工作并部署了下列基本策略：

- 内部和外部接口的安全区域。
- 信任所有内部到外部流量的访问规则。
- 接口 NAT 规则，用于将所有内部到外部流量转换到外部接口 IP 地址上的唯一端口。
- 在内部接口或网桥组上运行的 DHCP 服务器。

以下步骤概述了可能需要配置的其他功能。请单击页面上的帮助按钮(?)，获取有关每个步骤的详细信息。

过程

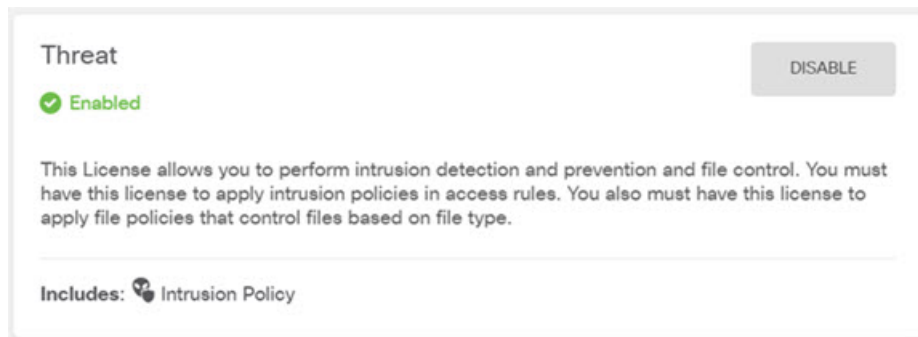
步骤 1 选择 Device，然后单击 Smart License 组中的 View Configuration。

对于您想要使用的可选许可证（威胁、恶意软件、URL），单击**启用**。如果在安装过程中注册设备，还可启用所需的 RA VPN 许可证。如果不确定是否需要使用某个许可证，请参阅该许可证的说明。

如果尚未注册，可以从该页面执行该操作。单击**Request Register**，并按照说明执行操作。请在评估版许可证到期前进行注册。

例如，以下是启用的威胁许可证：

图 2: 已启用的威胁许可证



步骤 2 如果配置了其他接口，请选择设备，然后单击接口组中的查看配置并配置每个接口。

可以为其他接口创建网桥组或配置单独的网络，或同时采用这两种方法。单击每个接口的编辑图标(🔗)，定义 IP 地址和其他设置。

以下示例将一个接口配置为“隔离区”(DMZ)，可以将可公开访问的资产（例如 Web 服务器）放在该区域中。完成后单击**保存**。

图 3: 编辑接口

Edit Physical Interface

Interface Name: dmz Status:

Description:

IPv4 Address | IPv6 Address | Advanced Options

Type: Static

IP Address and Subnet Mask: 192.168.6.1 / 24
e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

步骤 3 如果已配置新接口，请选择对象，然后从目录中选择安全区域。

根据需要编辑或创建新区域。每个接口都必须属于一个区域，因为需要根据安全区域而不是接口来配置策略。配置接口时不能将其放在区域中，因此每当创建新接口或更改现有接口的用途之后，都必须编辑区域对象。

以下示例显示如何为 DMZ 接口创建一个新的 DMZ 区域。

图 4: 安全区域对象

步骤 4 如果要让内部客户端使用 DHCP 从设备获取 IP 地址，请选择 **Device > System Settings > DHCP Server**，然后选择 **DHCP Server** 选项卡。

内部接口已配置了 DHCP 服务器，但可以编辑地址池或甚至将其删除。如果配置了其他内部接口，则在这些接口上设置 DHCP 服务器是非常典型的做法。单击 +，为每个内部接口配置服务器和地址池。

此外，您还可以在 **Configuration** 选项卡中对为客户端提供的 WINS 和 DNS 列表进行精细调整。以下示例显示如何在 inside2 接口（地址池为 192.168.4.50-192.168.4.240）上设置 DHCP 服务器。

图 5: DHCP 服务器

步骤 5 选择 **Device**，然后单击 **Routing** 组中的 **View Configuration**（或 **Create First Static Route**），配置默认路由。

默认路由通常指向位于外部接口之外的上游或 ISP 路由器。默认的 IPv4 路由适用于 any-ipv4 (0.0.0.0/0)，而默认的 IPv6 路由适用于 any-ipv6 (:::0/0)。为所使用的每个 IP 版本创建路由。如果使用 DHCP 获取外部接口的地址，则可能已经拥有所需的默认路由。

注释 此页面上定义的路由仅适用于数据接口，而不会影响管理接口。在 **设备 > 系统设置 > 管理接口** 上设置管理网关。

以下示例显示 IPv4 的默认路由。在此示例中，isp-gateway 是用于标识 ISP 网关 IP 地址的网络对象（必须从 ISP 中获取地址）。可以通过单击 **网关** 下拉菜单底部的 **创建新网络**，来创建该对象。

图 6: 默认路由

The screenshot shows the 'Add Static Route' configuration interface. It includes the following fields and options:

- Protocol:** Radio buttons for IPv4 (selected) and IPv6.
- Gateway:** A text input field containing 'isp-gateway'.
- Interface:** A text input field containing 'outside'.
- Metric:** A text input field containing '1'.
- Networks:** A dropdown menu with a '+' icon and 'any-ipv4' selected.

步骤 6 选择策略，并为网络配置安全策略。

设备安装向导设置允许内部区域与外部区域之间存在流量流动，并对所有接口上流向外部接口的流量启用网络地址转换 (NAT)。即使配置了新接口，如果将其添加到内部区域对象中，访问控制规则也将自动应用于这些接口。

但是，如果有多个内部接口，则需要一条访问控制规则来允许内部区域之间的流量。如要添加其他安全区域，则需要规则来允许这些区域之间的流量。这是您需要进行的最低限度的更改。

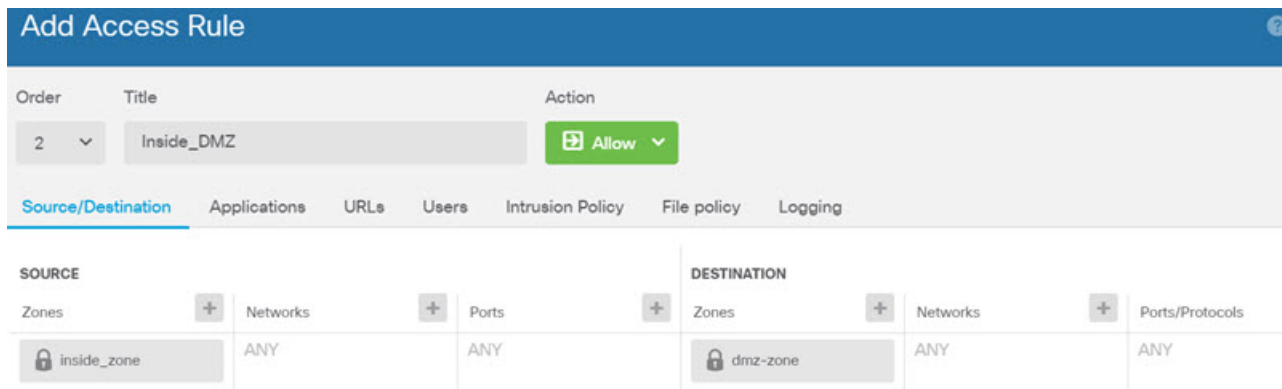
此外，您还可配置其他策略以提供附加服务，并对 NAT 和访问规则进行精细调整，以实现组织需要的结果。您可以配置以下策略：

- **SSL 解密** - 如果要检查加密连接（例如 HTTPS）是否存在入侵、恶意软件等，则必须解密连接。使用 SSL 解密策略确定需要解密的连接。系统检查连接后，会将其重新加密。
- **身份** - 如果要将网络活动与各个用户相关联，或根据用户或用户组成员身份控制网络访问，请使用身份策略确定与给定源 IP 地址关联的用户。

- **Security Intelligence** - 使用安全情报策略快速丢弃进出列入黑名单的 IP 地址或 URL 的连接。将已知恶意站点列入黑名单后，在访问控制策略中即可无需考虑这些站点。思科提供定期更新的已知恶意地址和 URL 源，可使安全情报黑名单实现动态更新。使用情报源，无需通过编辑策略来添加或删除黑名单中的项目。
- **NAT (Network Address Translation)** - 使用 NAT 策略将内部 IP 地址转换为外部可路由地址。
- **访问控制** - 使用访问控制策略确定网络上允许的连接。您可以按安全区域、IP 地址、协议、端口、应用、URL、用户或用户组进行过滤。您还可以使用访问控制规则来应用入侵策略和文件（恶意软件）策略。使用此策略实施 URL 过滤。
- **入侵** - 使用入侵策略检测已知威胁。即使使用访问控制规则应用入侵策略，也仍可以编辑入侵策略，以选择性地启用或禁用特定的入侵规则。


以下示例显示如何在访问控制策略中允许内部区域与 DMZ 区域之间的流量。在此示例中，任何其他选项卡上均未设置任何选项，日志记录除外，其中在连接结束时选项已被选中。

图 7: 访问控制策略



步骤 7 选择 **Device**，然后单击 **Updates** 组中的 **View Configuration**，为系统数据库配置更新计划。

如果使用入侵策略，请为“规则”和“VDB”数据库设置定期更新。如果使用安全情报源，请为“规则”和“VDB”数据库设置更新计划。如果在任何安全策略中使用地理位置作为匹配条件，请为“规则”和“VDB”数据库设置更新计划。

步骤 8 单击菜单中的 **Deploy** 按钮，然后单击立即部署按钮 ()，以部署对设备的更改。

只有将更改部署至设备，更改才会生效。

下一步做什么

有关使用 Firepower 设备管理器管理 Firepower Threat Defense Virtual 的详细信息，请参阅 [《适用于 Firepower 设备管理器的 Cisco Firepower 威胁防御配置指南》](#) 或 Firepower 设备管理器联机帮助。



第 5 章

VMware 的性能调整—虚拟 Firepower 威胁防御的最佳实践

Firepower Threat Defense Virtual 是一种高性能设备，但可能需要调整虚拟机监控程序才能获得最佳效果。

本章介绍 Firepower Threat Defense Virtual 在 VMware vSphere 环境中促进最佳性能的一些最佳实践和建议。



注释 为获得最佳性能，建议使用 ESXi 6.0.0.0 或更高版本。

- [SR-IOV 接口调配](#)，第 49 页

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 的速度连接威胁防御虚拟设备的虚拟机。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 Firepower 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。

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 Firepower 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 FTDv 虚拟机无网络连接。



注意 开始在 FTDv 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。

FTDv 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。

检查 ESXi 主机 BIOS

开始之前

要在 VMware 上部署带 SR-IOV 接口的 FTDv，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：

示例：

```
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 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。

示例：

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

值 3 表示受支持且已启用虚拟化。

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 **Manage** 选项卡上，单击 **Networking** 并选择 **Physical adapters**。

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，然后单击 **Edit adapter settings**。

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

步骤 5 在 **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 单击 **OK**。

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 **Settings** 选项卡的 PCI Devices 列表中。

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 **Manage** 下，选择 **Networking**，然后选择 **Virtual switches**。

步骤 3 单击 **Add host networking** 图标，即带有加号 (+) 的绿色地球仪图标。

步骤 4 选择 **Virtual Machine Port Group for a Standard Switch** 连接类型，然后单击 **Next**。

步骤 5 选择 **新建标准交换机**，然后单击 **Next**。

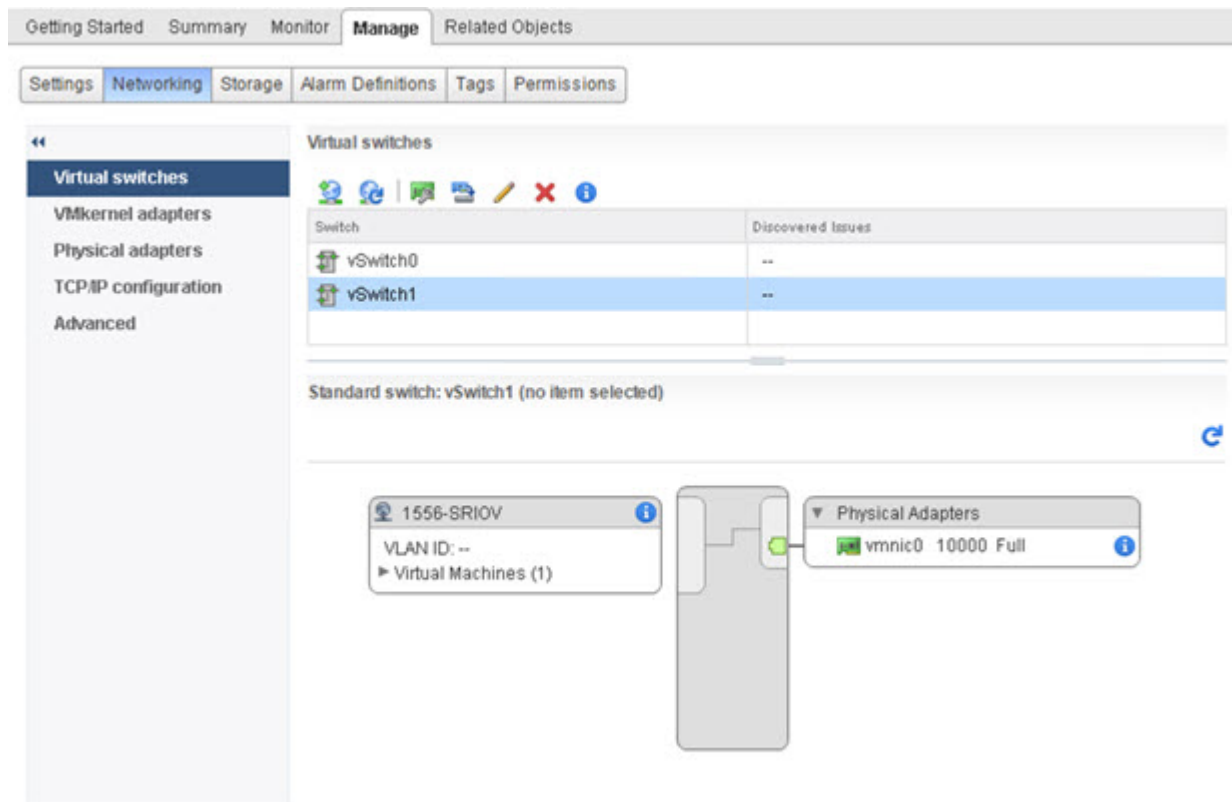
步骤 6 将物理网络适配器添加到新的标准交换机中。

- 在分配的适配器下，单击绿色加号 (+) 以添加适配器。
- 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。
- 从 **Failover order group** 下拉菜单中，选择 **Active adapters**。
- 单击 **OK**。

步骤 7 为该 SR-IOV vSwitch 输入一个网络标签，然后单击 **Next**。

步骤 8 在 **Ready to complete** 页面上查看您的选择，然后单击 **Finish**。

图 8: 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。FTDv 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 FTDv。以下操作程序可立即将 FTDv 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 FTDv 虚拟机。

- 选择数据中心、文件夹、集群、资源池或主机，然后单击 **Related Objects** 选项卡。
- 单击**虚拟机**，并从列表中选择 FTDv 虚拟机。

步骤 3 关闭所选的虚拟机。

步骤 4 右键单击该 FTDv，并依次选择 **操作 > 所有 vCenter 操作 > 兼容性 > 升级 VM 兼容性**。

步骤 5 单击 **Yes** 以确认升级。

步骤 6 为虚拟机兼容性选择 **ESXi 5.5 and later** 选项。

步骤 7 （可选）选择 **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 FTDv 与虚拟功能关联。

将 SR-IOV NIC 分配到虚拟 Firepower 威胁防御

为了确保 FTDv 虚拟机和物理 NIC 可以交换数据，您必须将 FTDv 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 FTDv 虚拟机。

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 FTDv 虚拟机。

- a) 选择数据中心、文件夹、集群、资源池或主机，然后单击 **Related Objects** 选项卡。
- b) 单击虚拟机，并从列表中选择 FTDv 虚拟机。

步骤 3 在虚拟机的 **Manage** 选项卡上，依次选择 **Settings > VM Hardware**。

步骤 4 单击 **Edit**，然后选择 **Virtual Hardware** 选项卡。

步骤 5 从 **New device** 下拉菜单中，选择 **Network**，然后单击 **Add**。

系统将显示 **New Network** 界面。

步骤 6 展开 **New Network** 部分，并选择可用的 SRIOV 选项。

步骤 7 从 **Adapter Type** 下拉菜单中选择 **SR-IOV passthrough**。

步骤 8 从 **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。

