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

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。

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 *1:* 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。

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 (-)。当您将设备添加到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。

- 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。

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。

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 1 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 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 *2:* 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。

a) （可选）单击**返回**以返回并查看或修改向导设置。

b) （可选）单击**取消**以放弃创建任务并关闭向导。

c) 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 8 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 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 Firepower 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 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。
- 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。

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。