适用于 VMware 的思科 Firepower 威胁防御虚拟部署

修订日期：2016 年 6 月 1 日

您可以使用 VMware 部署思科 Firepower 威胁防御虚拟。

Firepower 威胁防御虚拟和 VMware 的先决条件

您可以使用 VMware vSphere Web 客户端或 vSphere 独立客户端在 ESXi 上部署 Firepower 威胁防御虚拟。有关系统要求，请参阅《思科 Firepower 威胁防御兼容性》。

默认情况下，虚拟设备使用 e1000（1 千兆位/秒）接口。可以使用 vmxnet3 或 ixgbe(10 千兆位/秒）接口替换默认接口。

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 威胁防御虚拟在混合模式下运行，并且 Firepower 威胁防御虚拟的高可用性依赖于主用和备用设备之间的 MAC 地址切换，从而保证正确运行。

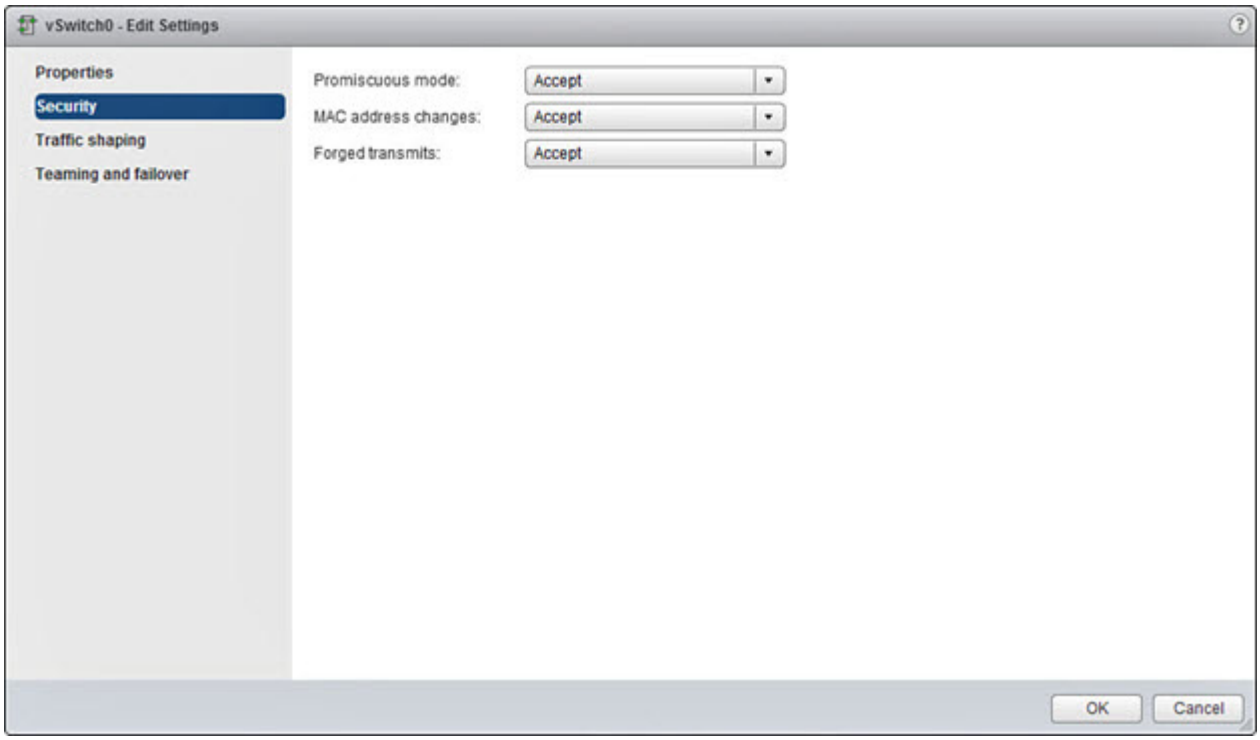
默认设置会阻碍 Firepower 威胁防御虚拟的正确运行。请参见以下要求的设置：

表 1 vSphere 标准交换机安全策略选项

选项	要求的设置	操作
混合模式 (Promiscuous mode)	接受 (Accept)	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 (Promiscuous mode)** 选项设置为**接受 (Accept)**。 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 (MAC address changes	接受 (Accept)	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 (MAC address changes)**选项已设为**接受 (Accept)**。
伪传输 (Forged transmits)	接受 (Accept)	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 (Forged transmits)** 选项已设为**接受 (Accept)**。

程序

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



6. 点击**确定 (OK)**。

后续操作

确保在为 Firepower 威胁防御虚拟传感器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。

Firepower 威胁防御虚拟和 VMware 准则

- Firepower 威胁防御虚拟**首次启动时，必须启用至少四个接口。**
- 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。
- 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 (eth0)，一个用于诊断 (eth1)。
- 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 (eth0)，一个用于诊断 (eth1)。
- 版本 6.0 仅支持两种 ixgbe 流量接口类型,即路由类型和 ERSPAN 被动类型。这是由于有关 MAC 地址过滤的 VMware 限制所致。

  注：在此版本中，ixgbe 驱动程序不支持 Firepower 威胁防御虚拟的故障切换 (HA) 部署。

- 当使用四个以上 vmxnet3 网卡时，思科建议使用由 VMware vCenter 管理的主机。部署在独立 ESXi 上时，其他网卡不会添加到具有连续 PCI 总线地址的虚拟机。请参阅添加和配置 VMware 接口（第 7 页）。
- 不支持 vMotion。
- 不支持克隆虚拟机。
- 不支持使用快照恢复虚拟机。
- 不支持恢复备份。

OVF 文件准则

安装 Firepower 威胁防御虚拟设备的安装选项如下：

```
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，安装过程将允许您执行 Firepower 威胁防御虚拟设备的整个初始设置。可以指定：
  - 管理员帐户的新密码
  - 允许设备在管理网络通信的网络设置
  - 初始防火墙模式
  - 管理思科 FirePOWER 管理中心

  注：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。您可以使用 VMware vCenter 管理此虚拟设备，或将它作为独立设备；有关详细信息，请参阅使用 CLI 设置 Firepower 威胁防御虚拟设备（第 8 页）。

部署 OVF 模板时需提供以下信息：

表 2 VMware OVF 模板

设置	ESXi 或 VI	操作
导入/部署 OVF 模板 (Import/Deploy OVF Template)	两者	浏览上一步骤中下载的 OVF 模板进行使用。
OVF 模板详细信息 (OVF Template Details)	两者	确认正在安装的设备（思科 Firepower 威胁防御虚拟）和部署选项（VI 或 ESXi）。
接受 EULA (Accept EULA)	仅 VI	同意接受 OVF 模板中包含的许可条款。
名称和位置 (Name and Location)	两者	为虚拟设备输入一个有意义的唯一名称，然后选择设备的库存库位。
主机/集群 (Host / Cluster)	两者	选择要部署虚拟设备的主机或集群。
资源池 (Resource Pool)	两者	通过建立有意义的层次结构，管理您在主机或集群内的计算资源。虚拟机和子资源池共享父资源池的资源。
存储 (Storage)	两者	存储与虚拟机关联的所有文件。

表 2 VMware OVF 模板（续）

设置	ESXi 或 VI	操作
磁盘格式化 (Disk Format)	两者	选择存储虚拟磁盘的格式：密集配置延迟归零、密集配置快速归零或精简置备。
网络映射 (Network Mapping)	两者	选择虚拟设备的管理接口。
属性 (Properties)	仅 VI	自定义虚拟机初始配置设置。

使用 VMware vSphere Web 客户端或 vSphere 虚拟机监控程序部署 Firepower 威胁防御虚拟

可以使用 VMware vSphere Web 客户端部署 Firepower 威胁防御虚拟。Web 客户端需要 vCenter。您也可以使用 vSphere 虚拟机监控程序进行独立 ESXi 部署。可以使用 vSphere 通过 VI OVF 或 ESXi OVF 模板进行部署：

- 如果使用 VI OVF 模板部署，设备必须由 VMware vCenter 管理。
- 如果使用 ESXi OVF 模板部署，设备可由 VMware vCenter 管理，或部署到独立主机。无论是哪种情况，都必须在安装后配置 Firepower 系统所需的设置。

准备工作

- 从思科支持网站的“下载”(Downloads) 区域下载 Firepower 威胁防御虚拟的存档文件 (https://software.cisco.com/download/navigator.html)。

  注：需要 Cisco.com 登录信息和思科服务合同。
- 将存档文件解压到工作目录中。不要从目录中删除任何文件。

程序

1. 使用 vSphere 客户端，点击**文件 (File) > 部署 OVF 模板 (Deploy OVF Template)** 部署您之前下载的 OVF 模板文件。
2. 从下拉列表中，选择要为 Firepower 威胁防御虚拟设备部署的任意一个 OVF 模板：

   ```
   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* 是已下载的存档文件的版本和内部版本号。
3. 查看“OVF 模板详细信息”(OVF Template Details) 页面，然后点击**下一步 (Next)**。
4. 如果许可协议封装在 OVF 模板内（仅 VI 模板），系统会显示“最终用户许可协议”(End User License Agreement) 页面。同意接受许可条款并点击**下一步 (Next)**。
5. 或者，编辑名称并选择库存中 Firepower 威胁防御虚拟所驻留的文件夹位置，然后点击**下一步 (Next)**。

   注：当 vSphere 客户端直接连接到 ESXi 主机时，不会出现选择文件夹位置的选项。
6. 选择要部署 Firepower 威胁防御虚拟的主机或集群，然后点击**下一步 (Next)**。
7. 导航至您想运行 Firepower 威胁防御虚拟的资源池并进行选择，然后点击**下一步 (Next)**。

   注：仅当集群包含资源池时，系统才会显示此页面。
8. 选择要存储虚拟机文件的存储位置，然后点击**下一步 (Next)**。

   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。

9. 选择磁盘格式以存储虚拟机虚拟磁盘，然后点击**下一步 (Next)**。

   如果选择**密集调配 (Thick Provisioned)**，将立即分配所有存储。如果选择**精简调配 (Thin Provisioned)**，则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。

10. 对于 OVF 模板中指定的每个网络，右键点击您的基础设施中的**目标网络 (Destination Networks)** 列，选中一个网络为每个 Firepower 威胁防御虚拟 接口设置网络映射，然后点击**下一步 (Next)。**

    注：Firepower 威胁防御虚拟**要求**将每个网络分配给**至少四个接口**。您的系统必须要有四个接口才能部署。

    确保将 Management0-0 接口关联到可以从 Firepower 管理中心访问的 VM 网络。非管理接口可从 Firepower 管理中心配置。

    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 (Edit Settings) 对话框中更改网络。在部署后，右键点击 Firepower 威胁防御虚拟 实例，然后选择**编辑设置 (Edit Settings)** 以访问**编辑设置 (Edit Settings)** 对话框。但是，该屏幕不会显示 Firepower 威胁防御虚拟 接口 ID（仅显示网络适配器 ID）。请查看以下源网络和目标网络索引，了解 Firepower 威胁防御虚拟接口：

源网络	目标网络	功能
Management0-0	Diagnostic0/0	诊断和管理
GigabitEthernet0-0	GigabitEthernet0/0	流量
GigabitEthernet0-1	GigabitEthernet0/1	流量
GigabitEthernet0-2	GigabitEthernet0/2	流量

    部署 Firepower 威胁防御虚拟后，您可以返回到 vSphere 客户端，从“编辑设置 (Edit Settings)”对话框中添加额外的接口。部署 Firepower 威胁防御虚拟时，总共可以有 10 个接口。有关详细信息，请参阅 vSphere 客户端 在线帮助。

    注：vSphere 客户端 要求将每个网络分配给至少四个接口。不需要使用所有 Firepower 威胁防御虚拟接口；对于您不打算使用的接口，只需在 Firepower 威胁防御虚拟配置中禁用即可。

11. 如果用户可配置属性封装在 OVF 模板（仅 VI 模板）内，则设置可配置属性，然后点击**下一步 (Next)**。

12. 查看并验证**准备完成 (Ready to Complete)** 窗口的设置。或者，选中**部署后启动 (Power on after deployment)** 选项启动 Firepower 威胁防御虚拟，然后点击**完成 (Finish)**。

    完成该向导后，vSphere Web 客户端将处理 VM；您可以在**全局信息 (Global Information)** 区域的**最近任务 (Recent Tasks)** 窗格中看到“初始化 OVF 部署 (Initialize OVF deployment)”状态。

    完成后，您会看到部署 OVF 模板 (Deploy OVF Template) 完成状态。

    然后在清单 (Inventory) 中的指定数据中心下会显示 Firepower 威胁防御虚拟 VM 实例。启动新的 VM 最多可能需要 30 分钟。

    注：要向思科许可颁发机构成功注册 Firepower 威胁防御虚拟，Firepower 威胁防御虚拟 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。

后续操作

- 确定您是否需要修改虚拟设备的硬件和内存设置；或配置接口；请参阅安装后配置（第 6 页）。
- 将您的 Firepower 威胁防御虚拟注册至 Firepower 管理中心；请参阅将 Firepower 威胁防御虚拟注册至 Firepower 管理中心（第 8 页）。

安装后配置

部署虚拟设备后，请确认虚拟设备的硬件和内存设置满足部署需求。默认设置是运行系统软件的最低要求，**不**能降低。下表列出了默认的设备设置。

表 3 虚拟设备默认设置

设置	默认	设置可调节？
memory	8GB	否
虚拟 CPU	4	否
硬盘配置大小	48.24GB	否，取决于磁盘格式选择（精简调配为 48.24GB）

验证虚拟机属性

使用 VMware 虚拟机“属性”(Properties) 对话框为选定的虚拟机调整主机资源分配。您可以从此选项卡更改 CPU、内存、磁盘和高级 CPU 资源。也可以更改适用于虚拟机的虚拟以太网适配器配置的启动连接设置、MAC 地址和网络连接。

程序

1. 右键单击新虚拟设备名称，然后从上下文菜单中选择**编辑设置 (Edit Settings)**，或从主窗口的 **入门 (Getting Started)** 选项卡中点击**编辑虚拟机设置 (Edit virtual machine settings)**。
2. 确保**内存 (Memory)**、**CPU (CPUs)** 和**硬盘 1 (Hard disk 1)** 设置为默认设置（如表 3虚拟设备默认设置（第 6 页）中所述）。

   内存设置和设备的虚拟 CPU 数量会列在窗口左侧。要查看硬盘的**调配容量 (Provisioned Size)**，请点击**硬盘 1 (Hard disk 1)**。
3. 确认**网络适配器 1 (Network adapter 1)** 设置如下，必要时执行更改：
   a. 在**设备状态 (Device Status)** 下，启用**打开电源时连接 (Connect at power on)** 复选框。
   b. 在 **MAC 地址 (MAC Address)** 下，手动设置虚拟设备管理接口的 MAC 地址。

      将 MAC 地址手动分配到虚拟设备，以避免 MAC 地址更改或动态池中的其他系统出现冲突。

      此外，对于虚拟思科 FirePOWER 管理中心，如果已重新映像虚拟设备，手动设置其 MAC 地址可确保不需要再次向思科申请许可证。
   c. 在**网络连接 (Network Connection)** 下，将**网络标签 (Network label)** 设置为虚拟设备管理网络的名称。
4. 点击**确定 (OK)**。

后续操作

- 初始化虚拟设备；请参阅初始化虚拟设备（第 7 页）。
- 或者，请在打开设备电源前用 vnxnet3 接口替换默认的 e1000 接口或创建额外的管理接口；或两者都用；请参阅添加和配置 VMware 接口（第 7 页）。

添加和配置 VMware 接口

创建虚拟机时，VMware 默认为 e1000（1 千兆位/秒）接口。完全完成虚拟机创建和 Firepower 威胁防御虚拟安装之后，可以从 e1000 接口切换到 vmxnet3（10 千兆位/秒）或 ixgbe（10 千兆位/秒）接口，以实现更高的网络吞吐量。以下准则在替换默认 e1000 接口时至关重要：

- 对于 vmxnet3，当使用四个以上的 vmxnet3 网络接口时，思科建议使用由 VMware vCenter 管理的主机。部署在独立 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 中的 XML 中获取正确的顺序。当主机运行独立的 ESXi 时，只能通过手动比较在 Firepower 威胁防御虚拟上看到的 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。
- 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 ixgbe，ESXi 平台要求 ixgbe 网络接口卡支持 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，请参阅英特尔技术简介《*如何在 VMware* ESXi* 5.1 中配置支持 Intel® 以太网融合网络适配器的虚拟功能*》。
- 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。

  注：在此版本中，ixgbe 驱动程序不支持 Firepower 威胁防御虚拟的故障切换 (HA) 部署。

您可以通过删除所有 e1000 接口并其替换为 vmxnet3 或 ixgbe 接口，替换默认的 e1000 接口。

虽然可以在部署中混合使用接口（例如在虚拟 思科 FirePOWER 管理中心上使用 e1000 接口，在其受管虚拟设备上使用 vmxnet3 接口），但不能在同一设备中混合使用接口。设备上的所有传感接口和管理接口必须为相同类型。

要更换 e1000 接口，请使用 vSphere 客户端 先删除现有 e1000 接口，添加新接口，然后选择相应的适配器类型和网络连接。

也可在同一虚拟 Firepower 管理中心中再添加一个管理接口，以分别管理两个不同网络上的流量。再配置一个虚拟交换机，以将第二个管理接口与第二个网络上的受管设备连接。使用 vSphere 客户端 将第二个管理接口添加到虚拟设备。

注： 请确保对接口进行了所有更改后，才可启动设备。要更改接口，必须先关闭设备、删除接口、添加新接口，然后启动设备。

有关使用 vSphere 客户端 的详细信息，请参阅 VMware 网站 (http://vmware.com)。有关多个管理接口的详细信息，请参阅《*Firepower 管理中心配置指南*》中的“管理设备”。

初始化虚拟设备

安装虚拟设备后，在首次启动虚拟设备时，初始化会自动启动。

注意： 启动时间取决于多种因素，包括服务器资源可用性。最多可能需要 40 分钟来完成初始化。请勿中断初始化，否则您可能需要删除设备，重新开始。

使用以下过程创建虚拟设备：

程序

1. 启动设备。在 vSphere 客户端中，右键单击从库存清单中导入的虚拟设备的名称，然后从上下文菜单中选择**电源 (Power) > 打开电源 (Power On)**。
2. 监控 VMware 控制台标签上的初始化。

后续操作

- 如果在部署期间使用了 VI OVF 模板并配置了 Firepower 系统所需的设置，则不需要进行其他配置；请参阅将 Firepower 威胁防御虚拟注册至 Firepower 管理中心（第 8 页）。
- 如果使用了 ESXi OVF 模板或在使用 VI OVF 模板部署时没有配置 Firepower 系统所需的设置，则应继续执行使用 CLI 设置 Firepower 威胁防御虚拟设备（第 8 页）。

使用 CLI 设置 Firepower 威胁防御虚拟设备

因为 Firepower 威胁防御虚拟设备没有 Web 界面，如果使用 ESXi OVF 模板部署，则必须使用 CLI 设置虚拟设备。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： 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操作。

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。

请注意，CLI 提示物理设备的设置网页的许多设置信息相同。有关详细信息，请参阅《*Firepower 系统安装指南*》。

注： 要在完成初始设置后更改虚拟设备的任何设置，必须使用 CLI。有关详细信息，请参阅《*Firepower 管理中心配置指南*》中的“命令行参考”一章。

程序

1. 打开 VMware 控制台。
2. 使用 `admin` 作为用户名和部署设置向导中指定的新管理员帐户密码，在 VMware 控制台登录虚拟设备。

   如果没有使用向导更改密码，或者正在使用 ESXi OVF 模板部署，请使用 `Admin123` 作为密码。

   设备立即提示您阅读 EULA。
3. 阅读并接受 EULA。
4. 更改 `admin` 帐户的密码。此帐户为 Configuration CLI 访问级别的帐户，无法删除。

   注：思科建议使用至少包含 8 个大小写混合的字母数字字符和至少一个数字字符的强密码。避免使用词典中的单词。
5. 根据提示完成系统配置。

   在进行设置时，VMware 控制台可能会显示消息。完成后，设备将提醒您将该设备注册至思科 FirePOWER 管理中心，并显示 CLI 提示。
6. 当控制台返回到 firepower **#** 提示符时，确认设置是否成功。

   注：要向思科许可颁发机构成功注册 Firepower 威胁防御虚拟，Firepower 威胁防御虚拟 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。

后续操作

- 将您的 Firepower 威胁防御虚拟注册至 Firepower 管理中心；请参阅将 Firepower 威胁防御虚拟注册至 Firepower 管理中心（第 8 页）。

将 Firepower 威胁防御虚拟注册至 Firepower 管理中心

因为虚拟设备没有网络界面，所以必须使用 CLI 向思科 FirePOWER 管理中心（可是物理的，也可是虚拟的）注册虚拟设备。因为在初始设置过程中已登录设备的 CLI，所以在此过程中向Firepower 管理中心注册设备最容易。

要注册设备，请使用 `configure manager add` 命令。将设备注册至 Firepower 管理中心，始终需要唯一的自身生成的字母数字注册密钥。这是由您指定的简单密钥，不同于许可密钥。

在大多数情况下，必须同时提供注册密钥以及Firepower 管理中心的 IP 地址，例如：

`configure manager add` *`XXX.XXX.XXX.XXX my_reg_key`*

其中，*`XXX.XXX.XXX.XXX`* 是管理Firepower 管理中心的 IP 地址，*`my_reg_key`* 是输入虚拟设备的注册密钥。

注： 在 ESXi 平台上，当使用 vSphere 客户端向 Firepower 管理中心注册虚拟设备时，如果设置过程中未提供 DNS 信息，则必须使用管理 Firepower 管理中心的 IP 地址（而非主机名）。

但是，如果设备和 Firepower 管理中心被网络地址转换 (NAT) 设备分隔，并且 Firepower 管理中心位于 NAT 设备的后面，则需输入唯一 NAT ID 和注册密钥，并指定 `DONTRESOLVE` 而不是 IP 地址。例如：

```
configure manager add DONTRESOLVE my_reg_key my_nat_id
```

其中， *my_reg_key* 是为虚拟设备输入的注册密钥，*my_nat_id* 是 NAT 设备的 NAT ID。

如果该设备而非 Firepower 管理中心位于 NAT 设备的后面，则需输入唯一的 NAT ID 和注册密钥，并指定 Firepower 管理中心的主机名或 IP 地址。例如：

```
configure manager add [hostname | ip address] my_reg_key my_nat_id
```

其中， *my_reg_key* 是为虚拟设备输入的注册密钥，*my_nat_id* 是 NAT 设备的 NAT ID。

程序

1. 使用 CLI 配置（管理员）权限的用户身份登录虚拟设备：
   - 如果正在通过 VMware 控制台执行初始设置，那么已经以???用户身份登录，此用户具有所需权限级别。
   - 否则，使用 VMware 控制台登录设备，或者在已配置设备的网络设置的情况下，将 SSH 用于设备的管理 IP 地址或主机名。
2. 在提示符处，使用 `configure manager add` 命令将设备注册至思科 FirePOWER 管理中心，命令的语法如下：

```
configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE} reg_key [nat_id]
```

   其中：
   - {*hostname* | *IPv4_address* | *IPv6_address* | DONTRESOLVE} 指定Firepower 管理中心的 IP 地址。如果 Firepower 管理中心不可直接寻址，则使用 `DONTRESOLVE`。
   - *reg_key* 是将设备注册到Firepower 管理中心所需的唯一字母数字注册密钥。

   注：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 Firepower 管理中心时，需要记住此注册密钥。
   - *nat_id* 是向 思科 FirePOWER 管理中心 注册设备过程中使用的可选字母数字字符串。如果主机名设置为 `DONTRESOLVE`，则需要此参数。

   注：使用 `show manager` 命令监控设备注册的状态。
3. 从设备注销。

后续操作

- 如果已设置 Firepower 管理中心，则登录其 Web 界面并使用“设备管理”(Device Management)（**设备 [Devices] > 设备管理 [Device Management]**）页面添加设备。有关详细信息，请参阅《*Firepower 管理中心配置指南*》中的“管理设备”一章。

将 Firepower 威胁防御虚拟注册至 Firepower 管理中心