使用面向 VMware 的 Firepower 设备管理器部署思科 Firepower 威胁防御虚拟设备快速入门指南

版本 6.2.2（或更高版本）

首次发布日期： 2017 年 9 月 5 日

最后更新日期： 2017 年 11 月 16 日

您可以使用面向 VMware 的 Firepower 设备管理器来部署思科 Firepower 威胁防御虚拟设备。有关具体系统要求和支持的虚拟机监控程序，请参阅思科 Firepower 兼容性指南。

在 VMware 环境下使用 Firepower 设备管理器部署 Firepower 威胁防御虚拟设备的前提条件

- 您必须为虚拟机安装新版映像（版本 6.2.2 或更高版本），才能使其支持 Firepower 设备管理器。如果您是对较早版本的现有虚拟机进行升级，则无法获得 Firepower 设备管理器支持。
- Firepower 设备管理器（本地管理器）会默认启用。

  注意： 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。
- 您也可以先使用 VMware vSphere Web 客户端或 ESXi 上的 vSphere 独立客户端来部署Firepower 威胁防御虚拟设备，再使用 Firepower 设备管理器配置虚拟机。
- 在 VMware 环境中，虚拟机默认使用 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 威胁防御虚拟设备在混合模式下运行，并且 Firepower 威胁防御虚拟设备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。

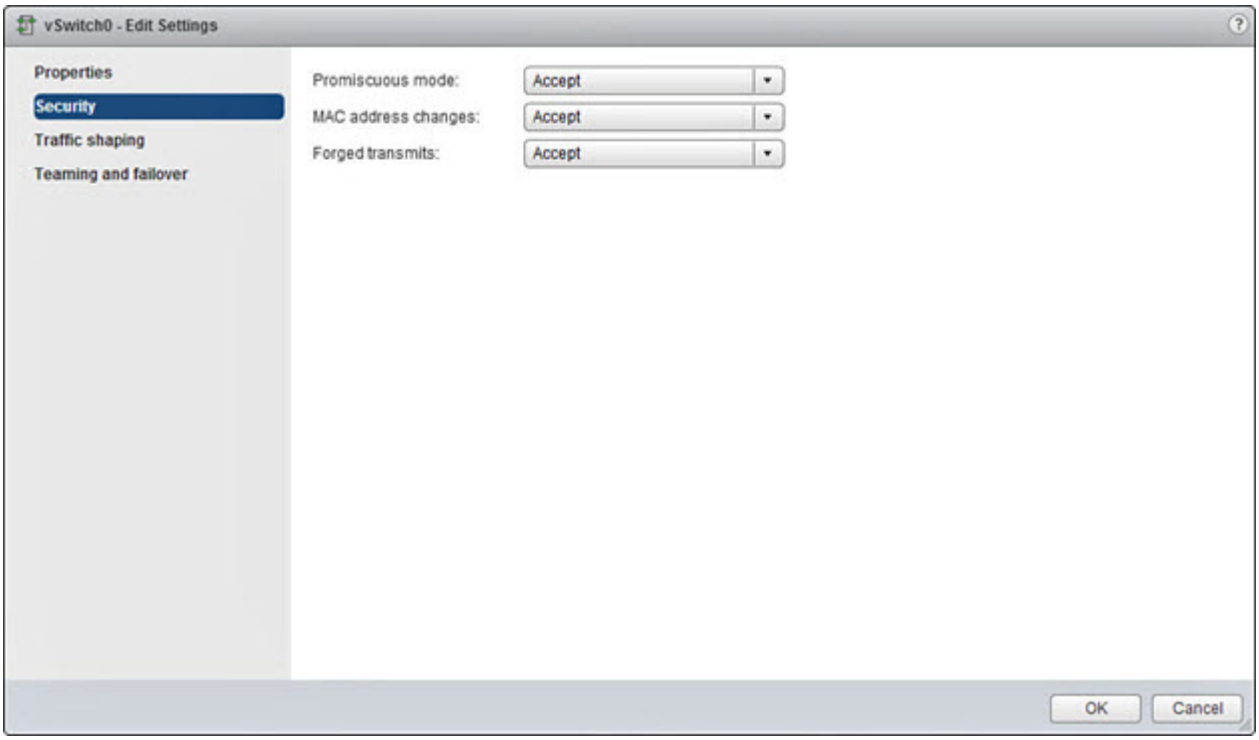
默认设置会阻碍 Firepower 威胁防御虚拟设备的正确运行。请参见以下要求的设置：

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	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**。

操作步骤

1. 在 vSphere Web 客户端中，导航至主机。
2. 在**管理**选项卡中，点击**网络**，然后选择**虚拟交换机**。
3. 从列表中选择一个标准交换机，然后点击**编辑设置**。
4. 选择**安全**，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**混合模式激活、MAC 地址更改和伪传输。



6. 点击**确定**。

后续操作

确保在为 Firepower 威胁防御虚拟设备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 威胁防御虚拟设备与 Firepower 设备管理器指南和限制

支持的网络适配器类型

Firepower 威胁防御虚拟设备支持三种虚拟网络适配器：

- **e1000** - 在 VMware 环境下创建虚拟机时，会默认使用 e1000（1 千兆位/秒）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** - 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。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。

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

默认配置

虚拟 Firepower 威胁防御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。

注意： 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。

Firepower 威胁防御虚拟设备**首次启动时，必须具有至少四个接口**：

- 虚拟机的第一个接口 (Management0-0) 是管理接口。
- 虚拟机的第二个接口 (GigabitEthernet0-0) 是外部接口。
- 虚拟机的第三个接口 (GigabitEthernet0-1) 是内部接口。
- 虚拟机的第四个接口 (GigabitEthernet0-2) 是数据接口。对于您不打算使用的接口，只需禁用即可。**请勿**删除第四个接口。

注意： 创建虚拟机时，VMware 默认为 e1000（1 千兆位/秒）接口。虚拟机创建完毕，且 Firepower 威胁防御虚拟设备充分完成安装后，您可以通过以下操作替换默认 e1000 接口，以获得更高的网络吞吐量：删除所有 e1000 接口，改为使用 vmxnet3（10 千兆位/秒）或 ixgbe（10 千兆位/秒）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（第 7 页）。

限制

- 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可用选项如下：

```
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。
  - 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。

  注意： 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，请参阅初始配置（第 9 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	双向	浏览上一步骤中下载的 OVF 模板进行使用。
OVF 模板详细信息	双向	确认正在安装的设备 （思科 Firepower 威胁防御虚拟设备）和部署选项（VI 或 ESXi）。
接受 EULA	仅 VI	同意接受 OVF 模板中包含的许可条款。
名称和位置	双向	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	双向	选择要部署虚拟设备的主机或集群。
资源池	双向	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	双向	存储与虚拟机关联的所有文件。
磁盘格式化	双向	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	双向	选择虚拟设备的管理接口。
属性	仅 VI	自定义虚拟机初始配置设置 （包括管理模式）。 **注意：**如需使用 Firepower 设备管理器管理 Firepower 威胁防御虚拟设备，请将**启用本地管理器**设置为**是**。在使用 Firepower 设备管理器时，您只能在路由模式下部署 Firepower 威胁防御虚拟设备。 有关设置 Firepower 设备管理器的详细信息，请参阅 “初始配置”，第 9 页。 **注意：**当**启用本地管理器**设置为**是**时，系统会忽略 Firepower 管理中心（远程管理器）的注册属性。

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

可以使用 VMware vSphere Web 客户端部署Firepower 威胁防御虚拟设备。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”区域下载 Firepower 威胁防御虚拟设备的存档文件 (https://software.cisco.com/download/navigator.html)。

  注意： 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。

操作步骤

1. 使用 vSphere 客户端，点击**文件 > 部署 OVF 模板**，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”页面，然后点击**下一步**。
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”页面。同意接受许可条款并点击**下一步**。
5. 或者，编辑名称并选择库存中 Firepower 威胁防御虚拟设备所驻留的文件夹位置，然后点击**下一步**。

   注意： 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 威胁防御虚拟设备的主机或集群，然后点击**下一步**。
7. 导航至并选择您想运行 Firepower 威胁防御虚拟设备的资源池，然后点击**下一步**。

   注意： 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**。

   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**。

   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。
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**列，选中一个网络，为每个 Firepower 威胁防御虚拟设备 接口设置网络映射，然后点击**下一步**。

    注意： Firepower 威胁防御虚拟设备 **要求**必须为网络分配**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”对话框中更改网络。在部署后，右键点击 Firepower 威胁防御虚拟设备 实例，然后选择**编辑设置**进入**编辑设置**对话框。但是，该屏幕不会显示 Firepower 威胁防御虚拟设备 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 威胁防御虚拟设备接口：

表 3　　源网络与目标网络的映射

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

注意： **vSphere 客户端 要求必须为网络分配至少四个接口。您无需使用 Firepower 威胁防御虚拟设备的所有接口。对于您不打算使用的接口，只需在 Firepower 威胁防御虚拟设备配置中禁用即可。**

部署 Firepower 威胁防御虚拟设备时，最多可以设置 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。有关详细信息，请参阅 vSphere 客户端 在线帮助。

注意： 如果部署 Firepower 威胁防御虚拟设备后需要添加更多接口，请参阅《*适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南*》的“为 Firepower 威胁防御虚拟设备添加接口”一节。

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**。

    注意： 要使用 Firepower 设备管理器配置 Firepower 威胁防御虚拟设备，您需要启用本地管理功能。您只能使用一种管理模式：或者使用 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。

12. 查看并验证**准备完成**窗口中的设置。或者，选中**部署后启动**选项启动 Firepower 威胁防御虚拟设备，然后点击**完成**。

    完成该向导后，vSphere Web 客户端将处理 VM；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。

    随即在“清单”中的指定数据中心下会显示 Firepower 威胁防御虚拟设备 VM 实例。启动新的 VM 最多可能需要 30 分钟。

    注意： 要向思科许可颁发机构成功注册 Firepower 威胁防御虚拟设备，Firepower 威胁防御虚拟设备需要访问互联网。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 7 页）。
- 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 11 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 4　　虚拟设备默认设置

设置	默认	设置可调节？
内存	8GB	否
虚拟 CPU	4	否
硬盘调配容量	48.24GB	否；取决于选择的磁盘格式 （精简调配为 48.24GB）

验证虚拟机属性

使用 VMware 虚拟机“属性”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。

操作步骤

1. 右键点击新虚拟设备名称，然后从上下文菜单中选择**编辑设置**，或从主窗口的**开始**选项卡中点击**编辑虚拟机设置**。
2. 确保**内存**、**CPU** 和**硬盘 1** 设置为默认设置（如表 4 虚拟设备默认设置（第 7 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**，请点击**硬盘 1**。
3. 确认**网络适配器 1** 设置如下，必要时执行更改：
   a. 在**设备状态**下，启用**打开电源时连接**复选框。
   b. 在 **MAC 地址**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**下，将**网络标签**设置为虚拟设备管理网络的名称。
4. 点击**确定**。

后续操作

- 初始化虚拟设备；请参阅启动虚拟设备（第 9 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；请参阅配置 VMware 接口（第 7 页）。

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 威胁防御虚拟设备安装之后，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。在替换默认 e1000 接口时，应谨记下列重要指导原则。

VMXNET3 接口

- 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 威胁防御虚拟设备上看到的 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。

IXGBE 接口

- 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。
- 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。
- ixgbe 驱动程序不支持 Firepower 威胁防御虚拟设备的故障切换 (HA) 部署。

替换接口

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不同类型的接口（例如在虚拟 思科 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。

要替换 e1000 接口，请使用 vSphere 客户端执行以下操作：

- 删除已有的 e1000 接口
- 添加新接口
- 选择适当的适配器类型和网络连接
- 启动虚拟设备

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。

注意： 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”。

添加接口

部署 Firepower 威胁防御虚拟设备时，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。

警告： 您无法为虚拟机添加更多虚拟接口，然后用 Firepower 设备管理器来自动识别这些接口。要为虚拟机添加接口，必须完全清除 Firepower 威胁防御虚拟设备配置。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 Firepower 威胁防御虚拟设备配置更多物理接口等效对象，则基本需要重新执行该流程。您既可以部署新虚拟机，也可以执行《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》的“为 Firepower 威胁防御虚拟设备添加接口”一节中所述的步骤。

启动虚拟设备

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。

警告： 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：

操作步骤

1. 启动设备。在 vSphere 客户端中，右键点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 > 打开电源**。
2. 监控 VMware 控制台标签上的初始化。

后续操作

- 如果您在部署时使用了 VI OVF 模板并配置了 Firepower 系统所需的设置，则无需进行其他配置。您也可以登录 Firepower 设备管理器，执行其他设备配置；有关详细信息，请参阅启动 Firepower 设备管理器（第 9 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，则应继续执行初始配置（第 9 页）。

初始配置

您必须完成初始配置，才能使 Firepower 威胁防御虚拟设备在网络中正常运行，。您可以通过以下两种方式来进行系统初始配置：

- 使用 Firepower 设备管理器 Web 界面（推荐）。

  Firepower 设备管理器在网络浏览器中运行。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）。

  您可以使用 CLI 设置向导代替 Firepower 设备管理器进行初始配置，并使用 CLI 执行故障排除。在这种情况下，您仍可使用 Firepower 设备管理器来配置、管理和监控系统；请参阅（可选）启动 Firepower 威胁防御 CLI 向导（第 10 页）。

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 设备管理器时，系统会通过设备设置向导指导您完成初始系统配置。

操作步骤

1. 在与 Firepower 威胁防御虚拟设备处于同一子网的客户端上打开浏览器。
2. 登录 Firepower 设备管理器。如果您未在 CLI 中进行初始配置，请以 **https://***ip-address* 格式输入地址（例如 **https://192.168.45.45**），打开 Firepower 设备管理器。
3. 使用用户名 **admin** 和密码 **Admin123** 登录。
4. 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。
5. 为外部接口和管理接口配置以下选项，然后点击**下一步**。

注意： 点击**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. **外部接口** - 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 - 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. **管理界面**

   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，请点击**使用 OpenDNS** 以重新将合适的 IP 地址加载到字段。

   防火墙主机名 - 系统管理地址的主机名。

注意： 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。

6. 配置系统时间设置，然后点击**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。

7. 为系统配置智能许可证。

   只有具有智能许可证帐户，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，请点击链接登录您的智能软件管理器帐户，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**开始 90 天评估期（无需注册）**。如需稍后注册设备并获取智能许可证，请点击菜单中的设备名称打开**设备控制面板**，然后点击**智能许可证**组中的链接。

8. 点击**完成**。

后续操作

使用设备设置向导完成设置后，系统会弹出一个窗口，显示后续选项。

- 如果需要将其他接口连接到了网络，请选择**配置接口**来配置各个连接的接口。
- 如果需要修改默认访问规则，请选择**配置策略**来配置和管理流量策略。

您可以选择任何一个选项，也可以直接关闭弹出窗口返回**设备控制面板**。

（可选）启动 Firepower 威胁防御 CLI 向导

如果您使用 ESXi OVF 模板部署 Firepower 威胁防御虚拟设备，则可以使用 CLI 进行设备设置。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。

注意： 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。

使用 CLI 设置系统时，可执行的配置仅限于设备的网络设置、防火墙模式和管理模式。您无法通过 CLI 会话配置策略。但是，您仍可使用 Firepower 设备管理器来配置、管理和监控系统；请参阅启动 Firepower 设备管理器（第 9 页）。

登录后，如需了解 CLI 中可用的命令，请输入 **help** 或 **?**。

操作步骤

1. 打开 VMware 控制台。
2. 在 **firepower login** 提示符下，使用默认凭据（用户名 **admin**，密码 **Admin123**）登录。
3. 当 Firepower 威胁防御系统启动时，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（需要进行本地管理）
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。
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。

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

使用 Firepower 设备管理器可配置、管理和监控系统。通过浏览器可配置的功能不能通过 CLI 配置；必须使用 Web 界面来实施安全策略。

如何在 Firepower 设备管理器中配置设备

完成设置向导后，您的设备应正常工作，并已部署下列基本策略：

- （ASA 5506-X 除外）外部和内部接口。其他数据接口则未配置。
- （仅限 ASA 5506-X。）外部接口以及包含所有其他数据接口的内部桥接组。
- 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。
- 在内部接口或桥接组上运行的 DHCP 服务器。

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

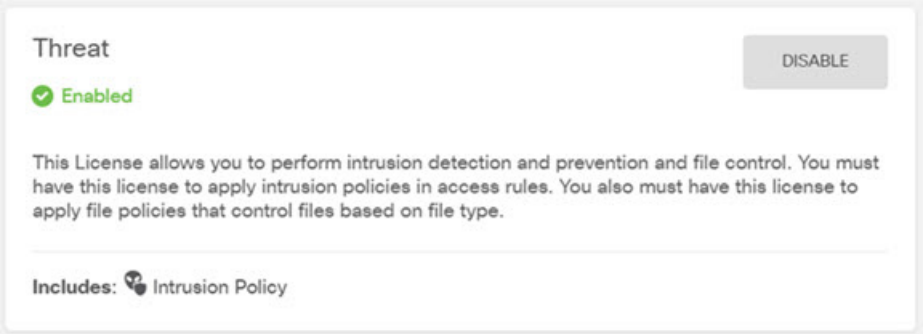
操作步骤

1. 选择**设备**，然后点击**智能许可证**组中的**查看配置**。

   对于您想要使用的可选许可证（威胁、恶意软件、URL），点击**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。点击**申请注册**，并按照指示执行操作。请在评估版许可证到期前进行注册。

   例如，如果启用了威胁许可证，则应显示如下内容：

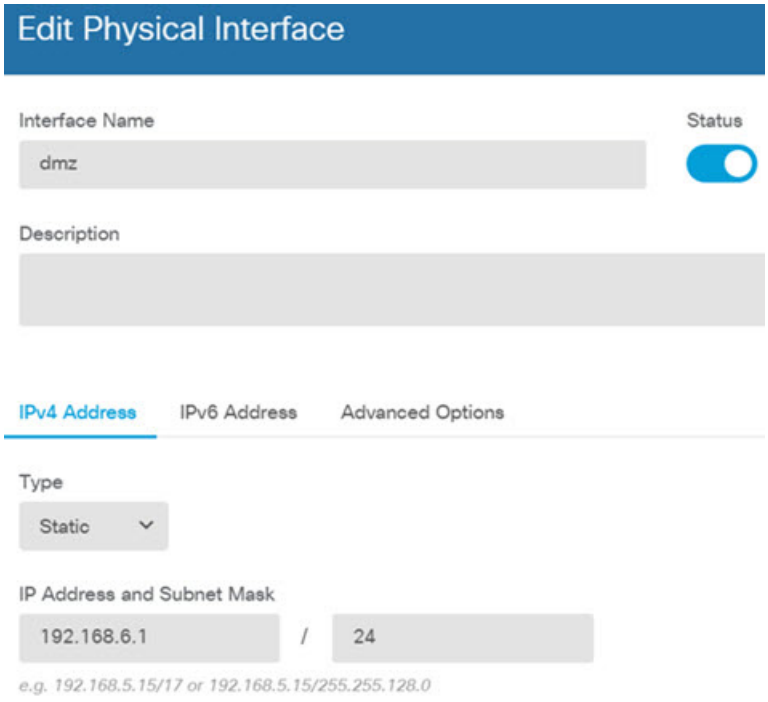


2. 如果连接了其他接口，请选择**设备**，然后点击**接口**组中的**查看配置**，配置各个连接的接口。

   由于 ASA 5506-X 预先配置了包含所有非外部数据接口的桥接组，因此不需要配置这些接口。但是，如果要拆分该桥接组，可以对其进行编辑，删除要单独处理的接口。然后，可以将这些接口配置为承载单独的网络。

   对于其他型号，可以为其他接口创建桥接组或配置单独的网络，或同时采用这两种方法。点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)，用于放置可公开访问的资产（例如 Web 服务器）。完成后点击“保存”。



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**。

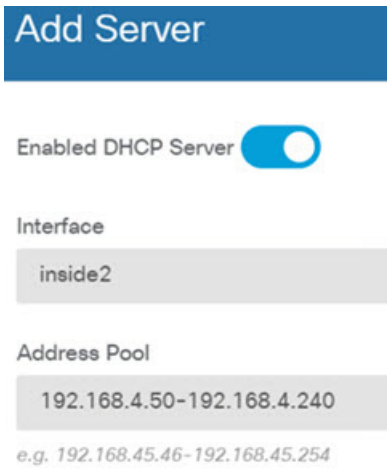
   根据需要编辑或创建新区域。每个接口都必须属于一个区域，因为需要根据安全区域而不是接口来配置策略。配置接口时不能将其放在区域中，因此每当创建新接口或更改现有接口的用途之后，都必须编辑区域对象。

   以下示例显示如何为 DMZ 接口创建一个新的 DMZ 区域。

4. 如果要让内部客户端使用 DHCP 从设备获取 IP 地址，请选择**设备** > **系统设置** > **DHCP 服务器**，然后选择 **DHCP 服务器**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。点击 +，为每个内部接口配置服务器和地址池。

   此外，您也可以在**配置**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。



5. 选择**设备**，然后点击**路由**组中的**查看配置**（或**创建第一个静态路由**），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。

注意： 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。您可以在**设备** > **系统设置** > **管理接口**下设置管理网关。

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）。可以通过点击**网关**下拉菜单底部的**创建新网络**，来创建该对象。

6. 选择**策略**，为网络配置安全策略。

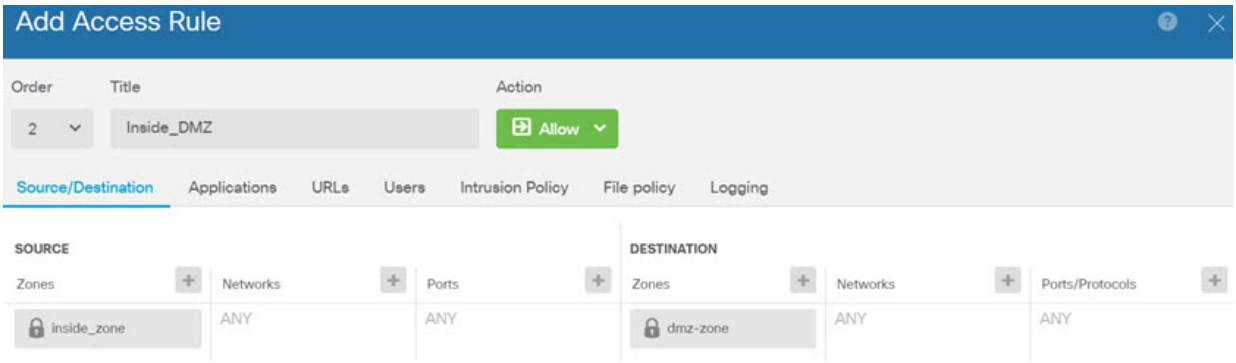
设备安装向导设置允许内部区域与外部区域之间存在流量流动，并对所有接口上流向外部接口的流量启用网络地址转换 (NAT)。即使配置了新接口，如果将其添加到内部区域对象中，访问控制规则也将自动应用于这些接口。

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。
- **安全情报** - 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。通过使用情报源，您将无需编辑策略来添加或删除黑名单中的项目。
- **NAT**（网络地址转换）- 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。使用此策略可实施 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，除**日志记录**中的**在连接结束时**选项外，任何其他选项卡上均未设置任何选项。



7. 选择**设备**，然后点击**更新**组中的**查看配置**，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。

8. 点击菜单中的**部署**按钮，然后点击“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。

后续操作

- 有关使用 Firepower 设备管理器管理 Firepower 威胁防御虚拟设备的完整信息，请参阅《*适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南*》或 Firepower 设备管理器在线帮助。

如何在 Firepower 设备管理器中配置设备