适用于 VMware 部署的思科 Firepower NGIPSv 快速入门指南

修订日期：2018 年 10 月 7 日

您可以使用 VMware 部署 适用于 VMware 的思科 Firepower NGIPSv。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。

Firepower NGIPSv 的 VMware 功能支持

下表列出了 Firepower NGIPSv 支持的 VMware 功能。

表 1　　Firepower NGIPSv 的 VMware 功能支持

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。请参阅使用 vMotion 的原则，第 5 页。
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	-
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	-

表 1　　Firepower NGIPSv 的 VMware 功能支持（续）

特性	说明	支持（是/否）	备注
带 VM 心跳信号的 VMware HA	用于 VM 故障。	否	-
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	-

Firepower NGIPSv 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 NGIPSv。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 NGIPSv 在混合模式下运行，并且 Firepower NGIPSv 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 NGIPSv 的正确运行。请参见以下要求的设置：

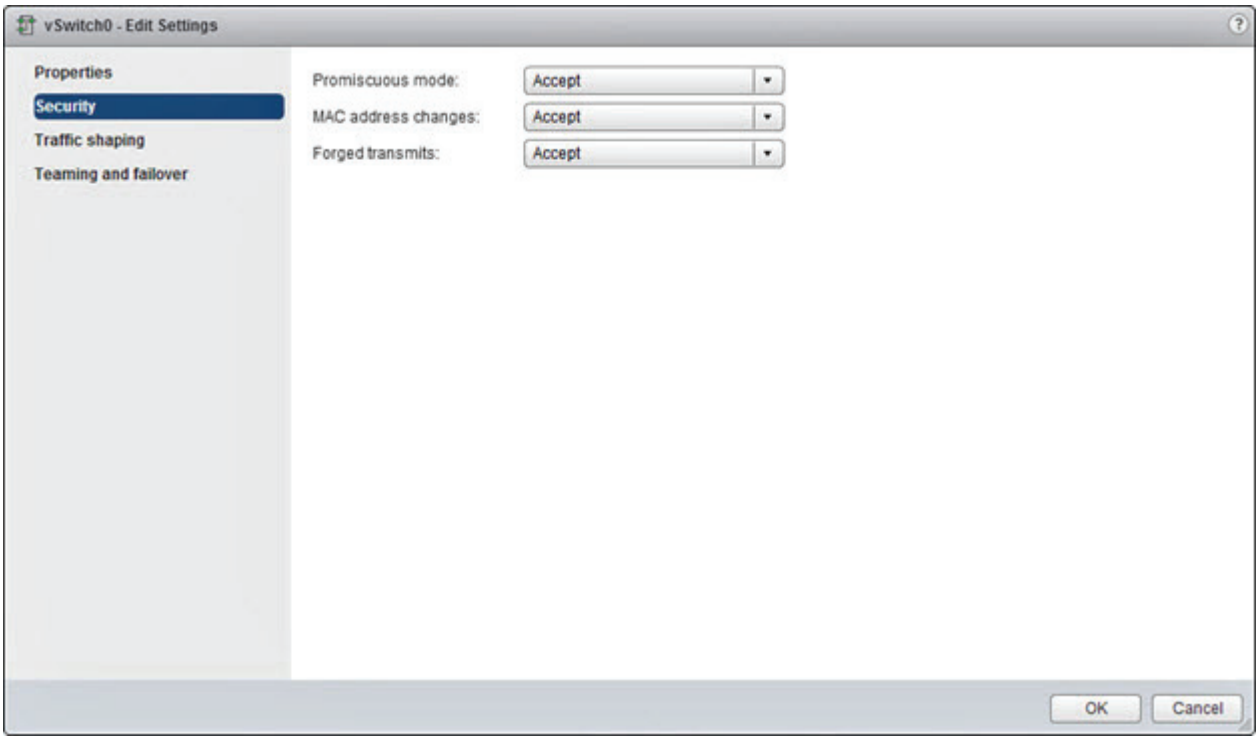
表 2　　vSphere 标准交换机安全策略选项

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 NGIPSv 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。

系统要求

根据所需部署的实例数量和使用要求，Firepower NGIPSv 部署所使用的具体硬件可能会有所不同。每个 Firepower NGIPSv 实例都需要服务器保证最小的资源配置，这包括内存数量、CUP 和磁盘空间。

下表列出了默认的设备设置。

表 3 Firepower NGIPSv 设备默认设置

设置	默认	设置可调节？
内存	4GB	是
虚拟 CPU	4	是，最多 8 个
硬盘调配容量	40GB	否，取决于所选磁盘格式
网络接口	2 个 vNIC（最少）	最多 10 个 vNIC（最多）

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。

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：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 SSSE3 的支持

- Firepower NGIPSv 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。

使用 Linux 命令行验证 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 NGIPSv 和 VMware 的准则和限制

部署适用于 VMware 的 Firepower NGIPSv 时，有以下限制：

- 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。您无法为 Firepower NGIPSv 管理的设备创建或恢复备份文件。要备份事件数据，请对管理设备的 Firepower 管理中心执行备份。

使用 vMotion 的原则

- 如果您计划使用 vMotion，我们建议您仅使用共享存储。部署 Firepower NGIPSv 期间，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 NGIPSv 移至其他主机，使用本地存储会造成错误。如果您不使用共享存储，则需关闭 VM，才能执行迁移。

INIT 重生错误消息

症状 - 可能会看到在 ESXi 6 和 ESXi 6.5 上运行的 Firepower NGIPSv 控制台显示以下错误消息：

```
"INIT: Id "ngipsv1" 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. 右键点击虚拟机，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**，然后点击**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。
5. 点击**确定**保存设置。

OVF 文件准则

安装 Firepower NGIPSv 设备的可用选项如下：

```
Cisco_Firepower_NGIPSv_VMware-VI-X.X.X-xxx.ovf
Cisco_Firepower_NGIPSv_VMware-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 NGIPSv 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
  - 检测模式
  - 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 NGIPSv，第 9 页。

部署 OVF 模板时需提供以下信息：

表 4 VMware OVF 模板

设置	ESXi 或 VI	操作
导入/部署 OVF 模板 (Import/Deploy OVF Template)	双向	浏览至您在上一步骤下载的需要使用的 OVF 模板。
OVF 模板详细信息 (OVF Template Details)	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 (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)	双向	为虚拟设备输入一个有意义的唯一名称，然后选择设备的资产位置。

表 4 VMware OVF 模板 （续）

设置	ESXi 或 VI	操作
主机/集群 (Host / Cluster)	双向	选择要部署虚拟设备的主机或集群。
资源池 (Resource Pool)	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：密集调配延迟置零、密集调配快速置零或精简调配。
网络映射 (Network Mapping)	双向	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 NGIPSv

您可以使用 VMware vSphere Web 客户端部署 Firepower NGIPSv。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 NGIPSv 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。

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 NGIPSv 部署的任意一个 OVF 模板：

   `Cisco_Firepower_NGIPSv_VMware-VI-`*`X.X.X-xxx`*`.ovf`
   `Cisco_Firepower_NGIPSv_VMware-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 NGIPSv 所驻留的文件夹位置，然后点击**下一步**。

   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 NGIPSv 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：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 模板中指定的每个源网络，右键点击基础设施中的**目标网络**列，选中一个网络，为每个 Firepower NGIPSv 接口设置网络映射，然后点击**下一步**。

    确保将管理接口关联到可以从 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，可以稍后更改网络。在部署后，右键点击 Firepower NGIPSv 实例，然后选择**编辑设置**以访问**编辑设置**对话框。但是，该屏幕不会显示 Firepower NGIPSv 接口 ID（仅显示网络适配器 ID）。

    请查看 Firepower NGIPSv 接口的以下网络适配器、源网络和目标网络的对应关系：

表 5 源网络与目标网络的映射

网络适配器	源网络	目标网络	功能
网络适配器 1	管理	Management0/0	管理
网络适配器 2	内部	GigabitEthernet0/0	内部数据
网络适配器 3	外部	GigabitEthernet0/1	外部数据

    部署 Firepower NGIPSv 后，您可以返回到 vSphere 客户端，从**编辑设置**对话框中添加额外的接口。部署 Firepower NGIPSv 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。

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**。

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 NGIPSv，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 NGIPSv 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 NGIPSv，Firepower NGIPSv 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。
- 将您的 Firepower 威胁防御虚拟设备注册至 Firepower 管理中心；请参阅将 Firepower NGIPSv 注册至 Firepower 管理中心，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是否满足部署需求（参阅系统要求，第 3 页）。默认设置是运行系统软件的最低要求，**不**能降低。

验证虚拟机属性

使用 VMware 虚拟机的“属性”对话框验证所选虚拟机的主机资源分配情况。您可以在这个选项卡中查看 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**，或在主窗口的**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 3 Firepower NGIPSv 设备默认设置，第 3 页中所述）。

   窗口左侧列出了设备的内存设置和虚拟 CPU 数量。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；请参阅初始化虚拟设备，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；请参阅添加和配置 VMware 接口，第 8 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 NGIPSv 安装之后，可以从 e1000 接口切换到 vmxnet3（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：

- 您可以通过删除所有 e1000 接口并将其替换为 vmxnet3 接口，将默认的 e1000（1 千兆位/秒）接口更改为 vmxnet3（10 千兆位/秒）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 NGIPSv 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。
- 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。**设备上的所有传感器和管理接口必须相同，可以是 e1000，也可以是 vmxnet3**。

要将 e1000 接口更改为 vmxnet3 接口，请使用 vSphere 客户端，先删除现有 e1000 接口，然后添加新的 vmxnet3 接口，最后选择相应的适配器类型和网络连接。

您也可在同一虚拟 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： 请确保在对接口进行所有更改**后**，再启动设备。要更改接口，必须先从 Firepower 管理中心取消注册，然后关闭设备，删除接口，添加新接口，再启动设备，重新注册 Firepower 管理中心。

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”一节。

初始化虚拟设备

安装虚拟设备后，在首次启动虚拟设备时，会自动启动初始化。

注意： 启动时间取决于多种因素，包括服务器资源的可用性。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并重新开始。

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；有关详细信息，请参阅将 Firepower NGIPSv 注册至 Firepower 管理中心，第 11 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，则应按照使用 CLI 设置 Firepower NGIPSv，第 9 页继续操作。

使用 CLI 设置 Firepower NGIPSv

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检测模式。

按照设置提示操作时，如遇单选问题，选项会小括号内列出，例如 `(y/n)`。默认值会在方括号内列出，例如 `[y]`。按 Enter 键确认选择。

请注意，CLI 提供的设置提示与物理设备设置页面大致相同。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。

了解设备网络设置

Firepower 系统为 IPv4 和 IPv6 管理环境提供了双堆栈实施。您必须设置 IPv4 或 IPv6 管理 IP 地址、网络掩码或前缀长度，以及默认网关。还可以指定最多三个 DNS 服务器以及设备的主机名和域。请注意，只有在重新启动设备后，主机名才会显示在系统日志中。

了解检测模式

为虚拟设备选择的检测模式确定系统最初如何配置设备的接口，以及这些接口是属于内联集，还是属于安全区域。设置之后则不可更改检测模式；检测模式是一个只能在设置期间进行选择的选项，用于帮助系统定制设备的初始配置。一般来说，应根据设备部署方式选择检测模式。

无源

如果设备以被动方式部署为一个入侵检测系统 (IDS)，则选择该模式。在被动部署过程中，虚拟设备可执行基于网络的文件与恶意软件检测、安全情报监控以及网络发现。

内联

如果以内联方式部署设备，选择此模式作为入侵防御系统 (IPS)。

注：尽管 IPS 部署中的常见做法是失效开放并允许非匹配流量通过，但虚拟设备上的内联集缺乏旁路功能。

访问控制

如果您想要执行应用、用户和 URL 控制，而将设备以内联方式部署为访问控制部署的一部分，请选择此模式。配置为执行访问控制的设备通常会不允许关闭，并且会阻止不匹配的流量。具体规则会明确指定可以通过的流量。

在访问控制部署过程中，还可以执行高级恶意软件防护、文件控制、安全情报过滤和网络发现。

网络发现

如果设备以被动方式部署为仅用于执行主机、应用和用户发现，则选择该模式。

下表列出了系统根据所选检测模式创建的接口、内联集和区域。

表 6　　基于检测模式的初始配置

检测模式	安全区域	内联集	接口
内联	内部和外部	默认内联集	添加至默认内联集的第一对接口，一个添加至内部区域，一个添加至外部区域
被动	被动	无	分配至被动区域的第一对接口
访问控制	无	无	无
网络发现	被动	无	分配至被动区域的第一对接口

请注意，安全区域为 Firepower 管理中心级配置。只有向 Firepower 管理中心添加设备后，系统才会创建安全区域。在满足此条件的情况下，如果 Firepower 管理中心上已存在相应区域（内部，外部或被动），系统会将所列接口添加到现有区域。如果区域不存在，系统会创建并添加接口。有关接口、内联集和安全区域的详细信息，请参阅《*Firepower 管理中心配置指南*》。

操作步骤

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。

   设备会提示您阅读《最终用户许可协议》(EULA)。
3. 阅读并接受 EULA。
4. 更改 `admin` 帐户的密码。此帐户为“配置 CLI”访问级别的帐户，无法删除。

   注：思科建议使用强密码，其中应至少包含 8 个大小写混合的字母数字字符和至少一个数字字符。应避免使用词典中的单词。
5. 配置设备的网络设置。首先配置（或禁用）IPv4 管理设置，然后配置 Ipv6 管理设置。如果手动指定网络设置，则必须：
   - 采用点分十进制格式输入 IPv4 地址，包括网络掩码。例如，可以指定 `255.255.0.0` 作为网络掩码。
   - 以冒号隔开的十六进制格式输入 IPv6 地址。对于 IPv6 前缀，请指定位数；例如，前缀长度为 `112`。

   当您实施设置后，VMware 控制台可能显示消息。
6. 根据设备的部署方式指定检测模式。

   当您实施设置后，VMware 控制台可能显示消息。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。

7. 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 NGIPSv，Firepower NGIPSv 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 NGIPSv 注册至 Firepower 管理中心；请参阅将 Firepower NGIPSv 注册至 Firepower 管理中心，第 11 页。

将 Firepower NGIPSv 注册至 Firepower 管理中心

因为虚拟设备没有 Web 界面，所以必须使用 CLI 向（可是物理的，也可是虚拟的）思科 Firepower 管理中心注册虚拟设备。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。要将设备注册至 Firepower 管理中心，您需要提供自己生成的唯一字母数字注册密钥。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，必须随注册密钥一起提供 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* 是您输入的虚拟设备注册密钥。

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* 是您输入的虚拟设备注册密钥，*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* 是您输入的虚拟设备注册密钥，*my_nat_id* 是 NAT 设备的 NAT ID。

操作步骤

1. 使用具有 CLI 配置（管理员）权限的用户身份登录虚拟设备：
   - 如果您正在通过 VMware 控制台执行初始设置，您应该已经以管理员用户身份登录，此用户拥有所需的权限级别。
   - 否则，请使用 VMware 控制台登录设备。或者，如果您已为设备配置网络设置，请通过 SSH 连接至设备的管理 IP 地址或主机名。
2. 在提示符处，使用 `configure manager add` 命令向思科 Firepower 管理中心注册设备，该命令使用以下语法：

```
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 管理中心无法直接寻址，请使用 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*是在 思科 Firepower 管理中心与设备之间的注册流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”（**设备** > **设备管理**）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。