适用于 VMware 的虚拟思科 Firepower 管理中心快速入门指南

版本 6.0

发布日期：2015 年 11 月 10 日

本手册中有关产品的规格和信息如有更改，恕不另行通知。本手册中的所有声明、信息和建议均准确可靠，但我们不为其提供任何明示或暗示的担保。用户必须承担使用产品的全部责任。

随附产品的软件许可和有限担保在随产品一起提供的信息包中提供，且构成本文的一部分。如果您无法找到软件许可或有限担保，请与思科代表联系以获取副本。

思科所采用的 TCP 报头压缩是加州大学伯克莱分校 (UCB) 开发的一个程序的改版，是 UCB 的 UNIX 操作系统公共域版本的一部分。保留所有权利。版权所有 © 1981，加州大学董事会。

无论在该手册中是否作出了其他担保，来自这些供应商的所有文档文件和软件都按“原样”提供且仍有可能存在缺陷。思科和上述供应商不承诺所有明示或暗示的担保，包括（但不限于）对特定用途的适销性、适用性、非侵权性以及因交易、使用或商业惯例所衍生的担保。

在任何情况下，对于任何间接、特殊、连带发生或偶发的损坏，包括（但不限于）因使用或无法使用本手册而导致的任何利润损失或数据损失或损坏，思科及其供应商概不负责，即使思科及其供应商已获知此类损坏的可能性也不例外。

本文档中使用的任何互联网协议 (IP) 地址和电话号码并非实际地址和电话号码。本文档中所含的任何示例、命令显示输出、网络拓扑图和其他图形仅供说明之用。说明性内容中用到的任何真实 IP 地址或电话号码纯属巧合，并非有意使用。

所有打印副本和软拷贝均被视为非受控副本，应以原始在线版本为最新版本。

思科在全球设有 200 多个办事处。www.cisco.com/go/offices 中列有各办事处的地址、电话和传真。

思科和思科徽标是思科和/或其附属公司在美国和其他国家/地区的商标或注册商标。要查看思科商标列表，请转至此 URL：www.cisco.com/go/trademarks。文中提及的第三方商标为其相应所有者的财产。“合作伙伴”一词的使用并不意味着思科和任何其他公司之间存在合作伙伴关系。(1110R)

适用于 VMware 的思科 Firepower 虚拟设备简介

思科封装了适用于 VMware vSphere 和 VMware vCloud Director 托管环境的 64 位虚拟 Firepower 管理中心和虚拟设备。通过 VMware vCenter 或 VMware vCloud Director，您可以将 64 位思科 Firepower 管理中心和 64 位思科 Firepower NGIPSv 受管设备部署到 ESXi 主机。虚拟设备使用 e1000 (1 Gbit/s) 接口，或者，您也可以将默认接口替换为 vmxnet3 (10 Gbit/s)。您也可以使用 VMware 工具来改善虚拟设备的性能和管理。

虚拟思科 Firepower 管理中心可管理物理设备和提供 FirePOWER 服务的思科 ASA (ASA FirePOWER)，而物理思科 Firepower 管理中心可管理虚拟设备。但是，虚拟设备不支持任何基于硬件的系统功能，虚拟思科 Firepower 管理中心不支持高可用性，虚拟设备不支持集群、堆栈、交换和路由等。有关物理 Firepower 系统设备的详细信息，请参阅《*Firepower 系统安装指南*》。

本指南提供关于部署、安装和设置虚拟 Firepower 系统设备（Firepower NGIPSv 设备和虚拟 Firepower 管理中心）的信息。同时假定读者熟悉 VMware 产品（包括 vSphere 客户端、VMware vCloud Director Web 门户或者 VMware 工具）的功能和术语定义。

操作环境先决条件

您可以将 64 位虚拟设备托管至以下托管环境：

- VMware ESXi 5.5 (vSphere 5.5)
- VMware ESXi 5.1 (vSphere 5.1)
- VMware vCloud Director 5.1

您也可以在所有受支持的 ESXi 版本上启用 VMware 工具。有关 VMware 工具全部功能的信息，请参阅 VMware 网站 (http://www.vmware.com/)。有关创建托管环境的详细信息，请参阅 VMware ESXi 文档，包括 VMware vCloud Director 和 VMware vCenter。

虚拟设备使用开放虚拟化格式 (OVF) 封装。不支持无法识别 OVF 封装的 VMware工作站、播放器、服务器和 Fusion。此外，虚拟设备被封装成带虚拟硬件 7 版本的虚拟机。

用作 ESXi 主机的计算机必须满足以下要求：

- 必须具有一个可提供虚拟化支持的 64 位 CPU，并采用英特尔虚拟化技术 (VT) 或 AMD Virtualization™ (AMD-V™) 技术。
- 必须在 BIOS 设置中启用虚拟化技术
- 必须具有与英特尔 E1000 驱动程序（如 Pro1000MT 双端口服务器适配器或 PRO1000GT 台式机适配器）兼容的网络界面，用以托管虚拟设备。

有关详细信息，请参阅 VMware 网站：http://www.vmware.com/resources/guides.html。

创建的每台虚拟设备要求 ESXi 主机具有一定数量的内存、CPU 和硬盘空间。默认设置是运行系统软件的最低要求，不能降低。但是，为了提高性能，您可以根据可用的资源来增加虚拟设备的内存和 CPU 数量。下表列出了默认的设备设置。

表 1 虚拟设备默认设置

设置	默认	设置可调节？
内存	8GB	是
虚拟 CPU 数量	4	是，最多 8 个
硬盘配置大小	40GB (NGIPSv) 250GB（虚拟 Firepower 管理中心）	否

虚拟设备性能

虚拟设备的吞吐量和处理能力无法准确预测。虚拟设备的性能在很大程度上会受到多种因素的影响，例如：

- ESXi 主机内存数量和 CPU 容量
- ESXi 主机上运行的虚拟设备总数量
- 感应接口数量、网络性能和接口速度
- 为每台虚拟设备分配的资源数量
- 共用主机的其他虚拟设备的活动水平
- 应用到虚拟设备的策略复杂度

注意： VMware 提供多种性能测量和资源分配工具。当您运行虚拟设备监控流量和确定吞吐量时，请使用 ESXi 主机上的这些工具。如果吞吐量并不理想，请调整分配至共用 ESXi 主机的虚拟设备的资源。

您也可以启用 VMware 工具来改善虚拟设备的性能和管理。此外，您也可以在主机上或 ESXi 主机上的虚拟化管理层（非访客层）中安装工具（如 `esxtop` 或 VMware 第三方插件），以检验虚拟性能。要启用 VMware 工具，请参阅*《Firepower 系统配置指南》*。

规定和限制

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。

适用于 VMware 的虚拟设备安装包

思科为支持站点上的 VMware ESXi 主机环境提供封装虚拟设备作为压缩存档 (`.tar.gz`) 文件。思科虚拟设备封装为虚拟机，带有虚拟硬件版本 7。每个存档文件包含以下文件：

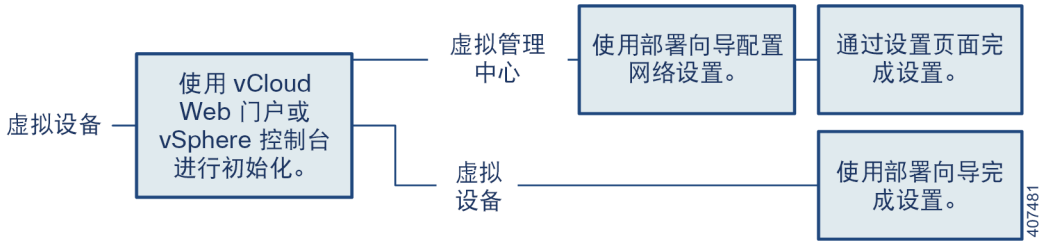
- 文件名中包含 `-ESXi-` 的开放虚拟格式 (`.ovf`) 模板
- 文件名中包含 `-VI-` 的开放虚拟格式 (`.ovf`) 模板
- 文件名中包含 `-ESXi-` 的 Manifest 文件 (`.mf`)
- 文件名中包含 `-VI-` 的 Manifest 文件 (`.mf`)
- 虚拟机磁盘格式 (`.vmdk`)

使用虚拟基础设施 (VI) 或 ESXi 开放虚拟格式 (OVF) 模板部署虚拟设备：

- 在使用 VI OVF 模板部署时，可以使用部署中的设置向导配置 Firepower 系统所需的设置（例如允许设备在网络上通信的管理员帐户的密码和设置）；您必须使用管理平台 VMware vCloud Director 或 VMware vCenter 进行部署。

VI OVF 模板部署

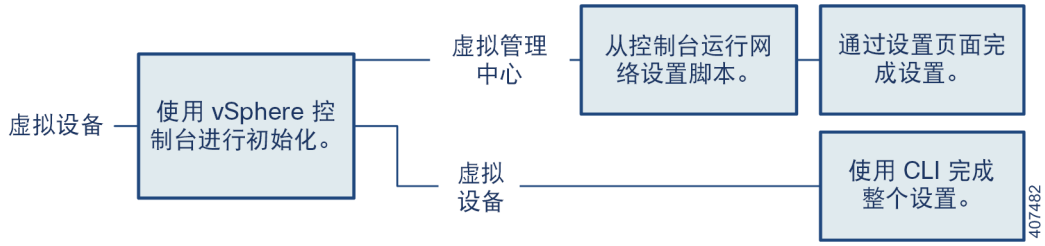
以下图表显示了在使用 VI OVF 模板部署时，设置 Firepower 系统虚拟设备的一般过程。



- 在使用 ESXi OVF 模板进行部署时，您必须在安装后使用虚拟设备的 VMware 控制台上的命令行界面 (CLI) 配置设置；您可以使用管理平台（VMware vCloud Director 或 VMware vCenter）进行部署，或作为独立设备部署。

ESXi OVF 模板部署

以下图表显示了在使用 ESXi OVF 模板部署时，设置 Firepower 系统虚拟设备的一般过程。



获取安装文件

在安装适用于 VMware 的 Firepower 系统虚拟设备前，从支持站点获取正确的存档文件。思科建议始终使用所提供的最新软件包。虚拟设备包通常与系统软件的主要版本（例如，5.4 或 6.0）关联。

要获取虚拟设备存档文件，请执行以下操作：

1. 使用 Web 浏览器，导航至思科支持网站的“下载”(Downloads) 区域 (https://software.cisco.com/download/navigator.html)。
2. 在**产品 (Products)** 区域浏览软件，或在要安装的系统软件的**查找 (Find)** 字段中输入名称。

   例如，要搜索 Firepower 存档文件，请输入 **Firepower**。
3. 使用以下命名约定，查找要为 Firepower 系统虚拟设备下载的存档文件：

   `Cisco_Firepower_NGIPSv_VMware-`*`X.X.X-xxx`*`.tar.gz`
   `Cisco_Firepower_Management_Center_Virtual_VMware-`*`X.X.X-xxx`*`.tar.gz`

   其中，*X.X.X-xxx* 是要下载的存档文件的版本和内部版本号。
4. 点击要下载的存档文件。

   注意： 在登录支持站点时，思科建议下载虚拟设备的所有可用更新，这样，在将虚拟设备到安装到主版本之后，就可以更新其系统软件。应始终运行设备支持的最新版本的系统软件。对于虚拟思科 Firepower 管理中心，您还需下载所有新的入侵规则和漏洞数据库 (VDB) 更新。

5. 将存档文件复制到运行 vSphere 客户端或 VMware vCloud Director 网络门户的工作站或服务器可访问的位置。

警告： 请勿通过邮件传输存档文件；文件可能已损坏。

6. 使用首选工具解压缩存档文件并提取安装文件。

   对于思科 Firepower NGIPSv 虚拟设备：

   ```
   Cisco_Firepower_NGIPSv_VMware-X.X.X-xxx-disk1.vmdk
   Cisco_Firepower_NGIPSv_VMware-ESXi-X.X.X-xxx.ovf
   Cisco_Firepower_NGIPSv_VMware-ESXi-X.X.X-xxx.mf
   Cisco_Firepower_NGIPSv_VMware-VI-X.X.X-xxx.ovf
   Cisco_Firepower_NGIPSv_VMware-VI-X.X.X-xxx.mf
   ```

   对于虚拟思科 Firepower 管理中心：

   ```
   Cisco_Firepower_Management_Center_Virtual_VMware-X.X.X-xxx-disk1.vmdk
   Cisco_Firepower_Management_Center_Virtual_VMware-ESXi-X.X.X-xxx.ovf
   Cisco_Firepower_Management_Center_Virtual_VMware-ESXi-X.X.X-xxx.mf
   Cisco_Firepower_Management_Center_Virtual_VMware-VI-X.X.X-xxx.ovf
   Cisco_Firepower_Management_Center_Virtual_VMware-VI-X.X.X-xxx.mf
   ```

   其中，*X.X.X-xxx* 是已下载的存档文件的版本和内部版本号。

   注意： 请确保将所有文件存放在同一目录中。

后续操作

- 思科 Firepower NGIPSv - 请参阅 *《适用于 VMware 的思科 NGIPSv 快速入门指南》* 部署虚拟 Firepower 系统受管设备。
- 虚拟思科 Firepower 管理中心 - 继续按照适用于 VMware 的虚拟思科 Firepower 管理中心部署（第 7 页）部署虚拟 Firepower 管理中心。

适用于 VMware 的虚拟思科 Firepower 管理中心部署

要安装虚拟思科 Firepower 管理中心，请使用平台界面（VMware vCloud Director Web 门户或 vSphere 客户端）将 OVF（VI 或 ESXi）模板部署到管理平台（VMware vCloud Director 或 VMware vCenter）：

- 如果使用 VI OVF 模板部署，可以在安装过程中配置 Firepower 系统所需的设置。必须使用 VMware vCloud Director 或 VMware vCenter 管理虚拟设备。
- 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。使用 VMware vCloud Director 或 VMware vCenter 可以管理该虚拟设备，或者将其用作独立设备。

在确保计划的部署满足前提条件（如操作环境先决条件（第 3 页）中所述）并下载必要的存档文件后，可使用 VMware vCloud Director 网络门户或 vSphere 客户端安装虚拟设备。

具有以下安装虚拟设备的安装选项：

- 对于虚拟思科 Firepower 管理中心：

  `Cisco_Firepower_Management_Center_Virtual_VMware-VI-`*`X.X.X-xxx`*`.ovf`
  `Cisco_Firepower_Management_Center_Virtual_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。

下表列出了部署所需的信息：

表 1 VMware OVF 模板

设置	ESXi 或 VI	操作
导入/部署 OVF 模板	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	两者	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	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	两者	选择要部署虚拟设备的主机或集群。
资源池	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	两者	选择一个 datastore 来存储与虚拟机关联的所有文件。
磁盘格式	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	两者	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。

如果使用 VI OVF 模板部署，安装过程将允许您执行虚拟思科 Firepower 管理中心的基本设置。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

如果使用 ESXi OVF 模板部署，或者选择不使用设置向导配置，必须使用 VMware 控制台执行虚拟设备的初始设置。有关执行初始设置的详细信息，包括关于要指定的配置的指导，请参阅设置思科 Firepower 管理中心虚拟设备（第 14 页）。

使用以下选项之一安装虚拟设备：

- 使用 VMware vCloud Director 进行部署（第 8 页） 说明如何将虚拟设备部署到 VMware vCloud Director。
- 使用 VMware vCloud Director 进行部署（第 8 页） 说明如何将虚拟设备部署到 VMware vCenter。

要了解网络设置，请参阅网络设置（第 16 页）。

使用 VMware vCloud Director 进行部署

您可以使用 vApp 模板，通过 VMware vCloud Director Web 门户部署虚拟 Firepower 管理中心。要使用 VMware vCloud Director 进行部署，您可以创建一个组织和目录，上传从 Cisco.com 获取的 OVF 包，并使用 vApp 模板创建虚拟 Firepower 管理中心。

上传虚拟设备 OVF 包

您可以将虚拟思科 Firepower 管理中心的 OVF 包上传至 VMware vCloud Director 组织目录。

准备工作

- 创建包含 vApp 模板的组织和目录。有关详细信息，请参阅《*VMware vCloud Director 用户指南*》。
- 从 Cisco.com 下载 OVF 模板；请参阅获取安装文件。

程序

1. 在 VMware vCloud Director Web 门户上，选择**目录 (Catalogs) >** *组织 (Organization)* **> vApp 模板 (vApp Templates)**，其中*组织 (Organization)* 是要包含 vApp 模板的组织名称。
2. 在 vApp Templates 媒体选项卡中，点击 Upload 图标 ( )。
3. 在 OVF 包字段中，输入 OVF 包的位置，或点击**浏览 (Browse)** 浏览 OVF 包。

   对于虚拟思科 Firepower 管理中心：

   ```
   Cisco_Firepower_Management_Center_Virtual_VMware-VI-X.X.X-xxx.ovf
   ```
4. 输入 OVF 包的名称，或者也可输入其描述。
5. 从下拉列表中，选择虚拟数据中心、存储配置文件和要包含 vApp 模板的目录。
6. 点击**上传 (Upload)**，将作为 vApp 模板的 OVF 包上传到目录。

OVF 包会上传到组织目录。

后续操作

- 使用 vApp 模板创建虚拟 Firepower 管理中心；请参阅使用 vApp 模板（第 9 页）。

使用 vApp 模板

您可以使用 vApp 模板创建虚拟设备，在使用设置向导安装时您将能配置 Firepower 系统所需的设置。

程序

1. 在 VMware vCloud Director Web 门户上，选择**我的云 (My Cloud) > vApps**。
2. 在 vApps 媒体选项卡中，点击 Add 图标 ( )，从此目录添加 vApp。
3. 在模板菜单栏上点击**所有模板 (All Templates)**。
4. 选择要添加以显示虚拟设备描述的 vApp 模板。

   对于虚拟思科 Firepower 管理中心：

   `Cisco_Firepower_Management_Center_Virtual_VMware-VI-`*`X.X.X-xxx`*`.ovf`

   其中，*X.X.X-xxx* 是存档文件的版本和内部版本号。
5. 阅读并接受 EULA。
6. 输入 vApp 的名称，也可以可选择地输入其描述。
7. 在“配置资源”(Configure Resources) 屏幕上，选择虚拟数据中心，输入系统名称（或使用默认系统名称），然后选择存储配置文件。
8. 通过选择外部、管理和内部源的目标，以及 IP 分配，将 OVF 模板中使用的网络映射到清单中的网络。
9. 或者，在“自定义属性”(Custom Properties) 屏幕上，通过在设置向导中输入 Firepower 系统所需的设置，进行设备的初始设置。如果现在不执行初始设置，可以按照设置思科 Firepower 管理中心虚拟设备（第 14 页）中的说明稍后执行。
10. 确认设置并点击**完成 (Finish)**。

    或者，启用虚拟 Firepower 管理中心的**部署后启动 (Power on after deployment)** 选项。如果选择稍后启动设备，请参阅初始化虚拟设备（第 13 页）。

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；参阅安装后配置（第 11 页）。

使用 VMware 进行部署 vSphere

您可以使用 VMware vSphere vCenter、vSphere 客户端、vSphere Web 客户端或 vSphere 虚拟机监控程序（用于单机 ESXi 部署），部署虚拟 Firepower 管理中心。您可以使用 vSphere，通过 VI 或 ESXi OVF 模板进行部署：

- 如果使用 VI OVF 模板部署，设备必须受 VMware vCenter 或 VMware vCloud Director 管理。
- 如果使用 ESXi OVF 模板部署，设备可由 VMware vCenter 或 VMware vCloud Director 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 Cisco.com 下载 OVF 模板；请参阅获取安装文件。

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，选择要部署的 OVF 模板：

   对于虚拟思科 Firepower 管理中心：

   `Cisco_Firepower_Management_Center_Virtual_VMware-VI-`*`X.X.X-xxx`*`.ovf`
   `Cisco_Firepower_Management_Center_Virtual_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”(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虚拟 Firepower 管理中心将位于的文件夹位置，然后点击**下一步 (Next)**。

   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. 选择要部署虚拟 Firepower 管理中心的主机或集群，然后点击**下一步 (Next)**。
7. 导航至并选择您想运行虚拟 Firepower 管理中心的资源池，然后点击**下一步 (Next)**。

   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 (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。
10. 将 Firepower 管理中心虚拟管理接口与网络映射屏幕上的 VMware 网络关联。

    右键单击您的基础设施中的**目标网络 (Destination Networks)** 列，选中一个网络以建立网络映射，然后点击**下一步 (Next)**。
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。
13. 或者，选中**部署后启动 (Power on after deployment)** 选项启动虚拟 Firepower 管理中心，然后点击**完成 (Finish)**。

    注意： 如果您选择不在部署后启动，可以稍后从 VMware 控制台执行此操作；请参阅初始化虚拟设备（第 13 页）。
14. 完成安装后，关闭状态窗口。
15. 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“库存”(Inventory) 中的指定数据中心下会显示虚拟思科 Firepower 管理中心实例。启动新的 VM 最多可能需要 30 分钟。

    注意： 为成功向思科许可授权机构注册虚拟 Firepower 管理中心，Firepower 管理中心需要互联网访问。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；参阅安装后配置（第 11 页）。

安装后配置

安装虚拟设备后，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。但是，为了提高性能，您可以根据可用的资源来增加虚拟设备的内存和 CPU 数量。下表列出了默认的设备设置。

表 1 虚拟 Firepower 管理中心的默认虚拟设备设置

设置	默认	设置可调节？
内存	8GB	是
虚拟 CPU 数量	4	是，最多 8 个
硬盘配置大小	250 GB（思科 Firepower 管理中心）	否

验证虚拟机属性

智能许可证	经典许可证	支持的设备	支持的域	访问权限
任何环境	任何环境	任何环境	任何环境	管理员

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)** 的设置不低于默认设置（如虚拟设备默认设置（第 4 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. 或者，通过点击窗口左侧的相应设置并在窗口右侧执行更改，增加内存和虚拟 CPU 的数量。
4. 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。
5. 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 13 页）。
- 或者，在启动设备之前，您可以创建一个额外的管理接口；请参阅《*适用于 VMware 的思科 Firepower NGIPSv 快速入门指南*》。

适用于 VMware 的虚拟思科 Firepower 管理中心设置

在安装思科 Firepower 系统虚拟设备后，必须完成允许新设备在可信管理网络上通信的设置过程。还必须更改管理员密码并接受最终用户许可协议 (EULA)。

在设置过程中，您可以执行多种初始管理级别的任务，例如设置时间、注册和许可设备及安排更新。设置和注册过程中所选择的选项决定系统创建并应用的默认接口、内联集、区域和策略。

这些初始配置和策略旨在提供开箱即用的用户体验，助您快速设置部署，同时不限制您的选项。无论最初如何配置虚拟设备，都可以随时使用思科 Firepower 管理中心更改其配置。例如，如果在设置过程中选择了某个检测模式或访问控制策略，不会使您锁定于特定设备、区域或策略配置。

无论如何部署，请从启动并初始化设备开始。初始化完成后，请使用 VMware 控制台登录，并根据设备类型采用以下任一方式完成设置：

思科 Firepower NGIPSv

思科 Firepower NGIPSv 虚拟设备没有网络界面。如果使用 VI OVF 模板部署，可执行初始设置，包括使用部署向导在 Firepower 管理中心上注册设备。如果使用 ESXi OVF 模板部署，必须使用交互式命令行界面 (CLI) 执行初始设置。

虚拟思科 Firepower 管理中心

如果使用 VI OVF 模板部署，可以使用向导在部署过程中进行网络配置。如果选择不使用设置向导或使用 ESXi OVF 模板部署，那么使用脚本配置网络设置。配置网络后，使用管理网络上的计算机完成设置过程，以浏览思科 Firepower 管理中心的网络界面。

注意： 如果要部署多台设备，您可以先设置 Firepower NGIPSv 设备，然后设置这些设备的管理 Firepower 管理中心。在设备初始设置流程中，您可以将设备预注册到 Firepower 管理中心；在 Firepower 管理中心的设置过程中，可添加并许可已预注册的受管设备。

初始化虚拟设备

智能许可证	经典许可证	支持的设备	支持的域	访问权限
任何环境	任何环境	任何环境	任何环境	管理员

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：

程序

1. 启动设备：
   - 在 VMware vCloud Director Web 门户中，从显示内容中选择 **vApp**，然后点击**开始 (Start)**。
   - 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

- 继续按照设置思科 Firepower 管理中心虚拟设备（第 14 页）完成设置。

设置思科 Firepower 管理中心虚拟设备

设置思科 Firepower 管理中心虚拟设备所需的步骤取决于是使用 VI OVF 模板还是 ESXi OVF 模板部署：

- 如果使用 VI OVF 模板部署并使用了设置向导，请使用配置 Firepower 系统所需的设置时设置的密码登录 Firepower 管理中心虚拟设备，然后使用 Firepower 系统设置本地设备配置、添加许可证和设备，并应用策略以监控和管理流量。有关详细信息，请参阅 *《Firepower 系统配置指南》*。
- 如果使用 ESXi OVF 模板部署，或在使用 VI OVF 模板部署时没有配置 Firepower 系统所需的设置，则设置虚拟 Firepower 管理中心分为两个步骤。初始化 Firepower 管理中心虚拟设备后，在 VMware 控制台运行脚本，这可帮助配置要在管理网络上通信的设备。然后，使用管理网络上的计算机完成设置过程，以浏览设备的网络界面。
- 如果使用 ESXi OVF 模板部署 Firepower 管理中心虚拟设备，并使用 VI OVF 模板部署所有虚拟设备，可通过单页面的设置向导同时将所有设备注册到 Firepower 管理中心。有关详细信息，请参阅初始设置页面：虚拟思科 Firepower 管理中心（第 15 页）。

自动化 Firepower 管理中心虚拟设备网络设置

智能许可证	经典许可证	支持的设备	支持的域	访问权限
任何环境	任何环境	管理中心	仅全局	管理员

新的思科 Firepower 管理中心虚拟设备初始化以后，您必须配置允许设备在管理网络上通信的设置。通过在 VMware 控制台运行脚本完成此步骤。

Firepower 系统为 IPv4 和 IPv6 管理环境提供了双堆栈实施。首先，脚本提示配置（或禁用） IPv4 管理设置，然后提示配置（或禁用） IPv6。对于 IPv6 部署，您可从本地路由器检索设置。必须提供 IPv4 或 IPv6 管理 IP 地址、网络掩码或前缀长度以及默认网关。

按照脚本提示，多选问题的选项会列在括号内，例如 `(y/n)`。默认值会列在方括号内，例如 `[y]`。按 Enter 键确认选择。

准备工作

按初始化虚拟设备（第 13 页）中所述初始化设备。

程序

1. 使用 `admin` 作为用户名，使用部署 VI OVF 模板时在设置向导中指定的管理员帐户密码，在 VMware 控制台登录 Firepower 管理中心虚拟设备。

   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。

2. 在管理员提示符下，运行以下脚本：

   ```
   sudo /usr/local/sf/bin/configure-network
   ```

3. 按脚本提示操作。首先配置（或禁用）IPv4 管理设置，然后配置 IPv6。如果手动指定网络设置，您必须：

   - 输入 IPv4 地址，包括网络掩码，采用点分十进制格式。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`。

4. 确认设置正确。

   如果输入的设置错误，您可以根据提示键入 `n`，然后按 Enter 键。然后，输入正确的信息。在进行设置时，VMware 控制台可能会显示消息。

5. 从设备注销。

后续操作

- 使用思科 Firepower 管理中心的网络界面，继续执行初始设置页面：虚拟思科 Firepower 管理中心（第 15 页）以完成设置。

初始设置页面：虚拟思科 Firepower 管理中心

智能许可证	经典许可证	支持的设备	支持的域	访问权限
任何环境	任何环境	管理中心	仅全局	管理员

对于虚拟思科 Firepower 管理中心，您必须通过登录设备的网络界面并在设置页面指定初始配置选项来完成设置流程。必须更改管理员密码，指定网络设置（若尚无指定），并接受 EULA。

在设置流程中，可注册并许可设备。注册设备之前，必须在设备上完成设置流程，并将 Firepower 管理中心添加为远程管理器，否则，注册将失败。

程序

1. 从管理网络上的计算机中，将支持的浏览器定向至 `https://`*`MC_name`*`/`，其中，*`MC_name`* 是您在上一个操作步骤中分配给 Firepower 管理中心管理接口的主机名或 IP 地址。

2. 使用 `admin` 作为用户名和使用 VI OVF 模板部署的设置向导中指定的管理员帐户密码登录。如果没有使用向导更改密码，请使用**思科**作为密码。

   系统将显示设置页面。有关完成设置的详细信息，请参阅以下各节：

   更改密码（第 16 页）

   网络设置（第 16 页）

   时间设置（第 16 页）

   重复规则更新导入（第 17 页）

   重复地理位置更新（第 17 页）

   自动备份（第 17 页）

许可证设置（第 17 页）

许可证设置（第 17 页）

最终用户许可协议（第 18 页）

3. 完成设置后，点击**应用 (Apply)**。

   Firepower 管理中心虚拟设备会根据您的选择进行配置。

4. 使用“任务状态”(Task Status) 页面（**系统 [System] > 监控 [Monitoring] > 任务状态 [Task Status]**）验证初始设置是否成功。

   此页面每隔 10 秒自动更新一次。请监控页面，直到该页面上列出的任何初始设置注册和策略应用任务的状态成为**已完成 (Completed)** 为止。如果在安装过程中配置了入侵规则或地理位置更新，您还可以监控这些任务。

现在，该思科 Firepower 管理中心可以使用了。有关配置部署的详细信息，请参阅 *《Firepower 系统配置指南》*。

后续操作

- 继续执行后续步骤（第 19 页）。

更改密码

您必须更改管理员帐户的密码。该帐户拥有管理员权限，您无法将其删除。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。

网络设置

思科 Firepower 管理中心的网络设置允许该设备在管理网络上通信。因为您已使用脚本配置网络设置，所以页面的此部分应该已预填充。

如果要更改预填充的设置，请记住 Firepower 系统提供 IPv4 和 IPv6 管理环境的双堆栈实施。您必须指定管理网络协议（**IPv4**、**IPv6** 或**两者**）。根据选择，设置页面将显示多种字段，在这些字段中必须设置 IPv4 或 IPv6 管理 IP 地址、网络掩码或前缀长度以及默认网关：

- 对于 IPv4，必须以点分十进制格式设置地址和网络掩码（例如：`255.255.0.0` 网络掩码）。
- 对于 IPv6 网络，您可以选择**使用路由器自动配置分配 IPv6 地址 (Assign the IPv6 address using router autoconfiguration)** 复选框，自动分配 IPv6 网络设置。否则，必须以冒号隔开的十六进制格式设置地址和前缀的位数（例如：前缀长度为 `112`）。

还可以指定最多三个 DNS 服务器以及设备的主机名和域。

时间设置

您可以手动或通过 NTP 服务器的网络时间协议 (NTP) 设置思科 Firepower 管理中心的时间。

还可以指定在管理员帐户的本地网络界面上使用的时区。点击当前时区，然后通过弹出窗口进行更改。

思科建议使用物理 NTP 服务器设置时间。

重复规则更新导入

随着新的漏洞为大家所知，思科漏洞研究团队 (VRT) 发布了入侵规则更新。规则更新提供全新和更新的入侵规则和预处理程序规则、现有规则的修改状态和修改的默认入侵策略设置。规则更新也可以删除规则并提供新规则类别和系统变量。

如果您计划在部署中执行入侵检测和防御，思科建议您选择**启用重复规则更新导入 (Enable Recurring Rule Update Imports)**。

可以指定**导入频率 (Import Frequency)** 并配置系统，使系统在每项规则更新后执行入侵**策略重新应用 (Policy Reapply)**。要在初始配置过程中执行规则更新，请选择**立即安装 (Install Now)**。

注意： 规则更新可能包含新的二进制文档。请确保下载和安装规则更新的流程符合安全策略。此外，规则更新内容可能很大，因此，请确保在网络使用量少的情况下导入规则。

重复地理位置更新

可以使用虚拟思科 Firepower 管理中心看关于与系统生成的事件相关的路由 IP 地址地理信息，并监控控制面板和 Context Explorer 中的地理位置统计信息。

思科 Firepower 管理中心的地理位置数据库 (GeoDB) 包含各种信息，如 IP 地址相关的互联网服务提供商 (ISP)、连接类型、代理信息和准确位置。启用定期 GeoDB 更新可确保系统使用最新的地理位置信息。如果要在部署中执行地理位置相关的分析，思科建议选择**启用每周重复的更新 (Enable Recurring Weekly Updates)**。

您可以指定 GeoDB 的每周更新频率。点击时区，然后通过弹出窗口进行更改。要在初始配置过程中下载数据库，请选择**立即安装 (Install Now)**。

注意： GeoDB 更新内容可能很大，下载后安装过程可能需要长达 45 分钟。您应在网络使用量少的情况下更新 GeoDB。

自动备份

Firepower 管理中心提供一个数据存档机制，以便在发生故障的情况下恢复配置。在初始设置过程中，您可以选择**启用自动备份 (Enable Automatic Backups)**。

启用该设置后，将创建一项定期任务，即对 Firepower 管理中心上的配置创建周备份。

许可证设置

您可许可各种功能，为贵公司创建最佳 Firepower 系统部署。您可使用 Firepower 管理中心为其本身及其管理的设备管理许可证 Firepower 系统提供的许可证类型取决于要管理的设备类型：

- 对于 Firepower、ASA FirePOWER 和 NGIPSv 设备，必须使用经典许可证。

默认情况下，您的 Firepower 管理中心可以执行域控制、主机、应用和用户发现，以及解密和检查 SSL 和 TLS 加密的流量。特定功能的经典许可证允许受管设备执行各种功能。有关许可的完整信息，请参阅 *《Firepower 系统配置指南》* 或 Firepower 管理中心中的在线帮助。

设备注册

虚拟思科 Firepower 管理中心可将任何设备（物理或虚拟），目前由 Firepower 系统支持。在初始设置过程中，可以将大多预注册设备添加到 Firepower 管理中心。但是，如果设备和 Firepower 管理中心由一台 NAT 设备隔开，您必须在设置过程完成后进行添加。

在 Firepower 管理中心注册受管设备后，如果您想要将访问控制策略自动应用于设备，请选中**应用默认访问控制策略 (Apply Default Access Control Policies)** 复选框。请注意，您无法选择 Firepower 管理中心对每台设备应用哪项策略，只能选择是否应用这些策略。应用到每个设备的策略取决于配置设备时选择的检测模式，在下表列出。

表 1 按检测模式所应用的默认访问控制策略

检测模式	默认访问控制策略
线内	默认入侵防御
被动	默认入侵防御
访问控制	默认访问控制
网络发现	默认网络发现

此情况除外，即您以前使用 Firepower 管理中心管理设备并且已更改设备的初始界面配置。在这种情况下，此新 Firepower 管理中心页面应用的策略取决于已更改（当前）的设备配置。如果配置了界面，Firepower 管理中心将应用默认入侵防御策略，否则，Firepower 管理中心将应用默认访问控制策略。

有关虚拟设备检测模式的详细信息，请参阅《*适用于 VMware 的思科 NGIPSv 快速入门指南*》；对于物理设备，请参阅《*Firepower 系统安装指南*》。

注意： 如果设备与访问控制策略不兼容，则策略应用会失败。这种不兼容有多种可能的原因，包括许可不匹配、型号限制、被动与内联问题和其他配置错误。如果初始访问控制策略应用失败，则初始网络发现策略也会应用失败。在解决导致失败的问题后，您必须手动向设备应用访问控制和网络发现策略。有关可能导致访问控制策略应用失败的问题的详细信息，请参阅 《*Firepower 系统配置指南*》。

要添加设备，请键入在设备注册时指定的**主机名 (Hostname)** 或 **IP 地址 (IP Address)**，以及**注册密钥 (Registration Key)**。请记住，这是指定的简单密钥，并不等同于许可证密钥。

然后，使用复选框将已许可功能添加至该设备。请注意，只可选择已添加到思科 Firepower 管理中心的许可证。此外，在启用其他许可证之前，无法启用特定许可证。例如，在首次启用保护之前，无法在设备上启用可控性。

由于架构和资源的限制，并非所有许可证在所有受管设备上受支持。但是，设置页面**不会**阻止您在受管设备上启用不支持的许可证。这是因为思科 Firepower 管理中心稍后才能确定设备型号。系统无法启用无效的许可证，而且尝试启用无效的许可证不会减少可用许可证的数量。

启用许可证后，点击**添加 (Add)** 保存设备的注册设置，或者添加更多设备。如果您选择了错误的选项或错误键入了设备名称，请点击**删除 (Delete)** 将其移除。然后，您可以重新添加设备。

最终用户许可协议

请仔细阅读 EULA，如果您同意遵守本协议条款，请选择复选框。确保提供的所有信息都正确无误后，请点击**应用 (Apply)**。

思科 Firepower 管理中心会根据您的选择进行配置。您将以管理员用户（具有管理员角色）身份登录网络界面。继续初始设置页面：虚拟思科 Firepower 管理中心（第 15 页）中的第 3. 步，以完成 Firepower 管理中心的初始设置。

启用 VMware 工具

VMware 工具是安装在虚拟机操作系统中的一套实用程序，可提高虚拟机的性能以及使 VMware 产品的许多简单易用的功能变成现实。该系统在所有虚拟设备上均支持以下插件：

- guestInfo
- powerOps
- timeSync
- vmbackup
- 快照

关于 VMware 工具支持的插件和全部功能的详细信息，请参阅 VMware 网站 (http://www.vmware.com/)。

在设置虚拟设备后，可以使用命令行界面 (CLI) 在受管设备的虚拟设备上，也可使用浏览器在虚拟 Firepower 管理中心上启用 VMware 工具。有关详细信息，请参阅在虚拟 Firepower 管理中心上配置 VMware 工具（第 19 页）。

在虚拟 Firepower 管理中心上配置 VMware 工具

智能许可证	经典许可证	支持的设备	支持的域	访问权限
任何环境	任何环境	虚拟管理中心	任何环境	管理员

使用网络界面，可以选择或清除 Configuration 菜单上的复选框。使用 CLI，不能在虚拟思科 Firepower 管理中心上启用 VMware 工具。

要在虚拟思科 Firepower 管理中心上启用或禁用 VMware 工具，请执行以下操作：

1. 使用 Web 浏览器，登录思科 Firepower 管理中心并选择**系统 (System) > 配置 (Configuration) > VMware 工具 (VMware Tools)**，然后选择或清除**启用 VMware 工具 (Enable VMware Tools)** 复选框并点击**保存 (Save)**。

后续步骤

在完成虚拟设备的初始设置过程并验证其成功后，思科建议您完成各种管理任务，以使部署更易于管理。此外，还应该完成在初始设置过程中跳过的所有任务，例如设备注册和许可。有关以下各节中描述的任何任务的详细信息，以及关于如何开始配置部署的信息，请参阅*《Firepower 系统配置指南》*。

单个用户帐户

完成初始设置后，系统上的唯一用户是管理员用户，此用户具备管理员角色和访问权限。具备管理员角色的用户拥有对系统菜单和配置的完整访问权限，包括通过外壳或 CLI 进行访问。思科限制使用管理员帐户（和管理员角色），以保障安全、便于审计。

为使用系统的每个人创建独立帐户，不仅可以让公司审计每个用户所做的操作和更改，还能限制每个人的相关用户访问角色。这点对于思科 Firepower 管理中心来说尤其重要，因为您要在防御中心执行大多数的配置和分析任务。例如，分析师需要访问事件数据来分析网络的安全性，但不需要访问用于部署的管理功能。

系统提供 10 个专为各种管理员和分析师设计的预定义用户角色。此外，您还可以创建具备专门访问权限的自定义用户角色。

运行状况和系统策略

默认情况下，所有设备都应用了初始系统策略。系统策略管理同一部署中多个设备的类似设置，例如邮件中继主机首选项和时间同步设置。思科建议您使用 Firepower 管理中心将同一系统策略应用到防御中心本身以及它管理的所有设备上。

默认情况下，Firepower 管理中心还应用了运行状况策略。作为运行状况监控功能的一部分，运行状况策略为系统提供了用以持续监控部署中设备的性能的标准。思科建议您使用 Firepower 管理中心将运行状况策略应用到其管理的所有设备上。

软件和数据库更新

开始任何部署之前，您应当更新设备上的系统软件。思科建议部署中的所有设备运行 Firepower 系统的最新版本。如果您正在部署中使用这些设备，还应当安装最新的入侵规则更新、VDB 和 GeoDB。

警告： 更新 Firepower 系统的任何部分之前，您必须阅读更新随附的版本说明或建议性文本。版本说明提供重要信息，包括支持的平台、兼容性、先决条件、警告以及具体安装和卸载说明。

适用于 VMware 的思科 Firepower 虚拟设备部署示例

您可以利用虚拟设备和虚拟思科 Firepower 管理中心，在虚拟环境中部署安全解决方案，从而加强对物理和虚拟资产的保护。通过虚拟设备和虚拟思科 Firepower 管理中心，您可以在 VMware 平台上轻松实施安全解决方案。此外，虚拟设备还方便您部署和管理资源可能受到限制的远程站点中的设备。

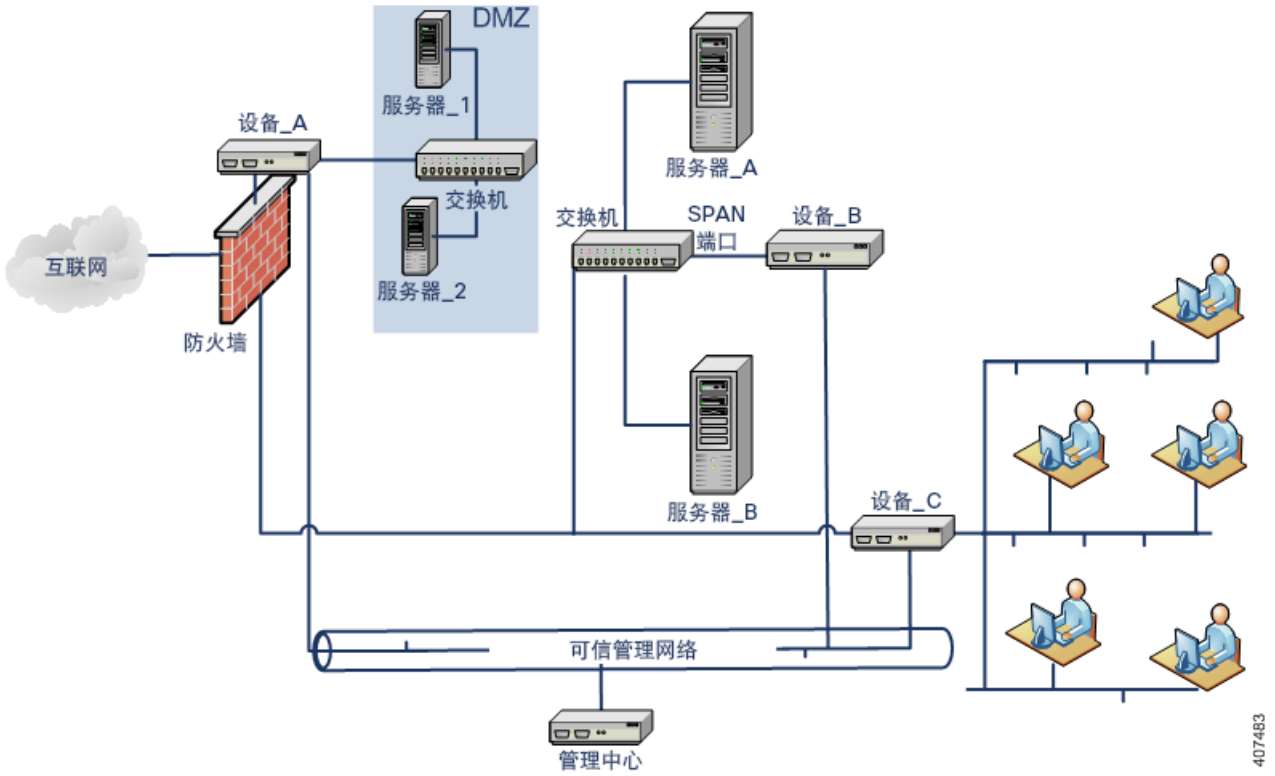
在以下示例中，可使用物理或虚拟思科 Firepower 管理中心来管理物理或虚拟设备。您可在 IPv4 或 IPv6 网络中进行部署。也可以在思科 Firepower 管理中心上配置多个管理接口，以隔离和监控两个不同的网络，或分离单一网络中的内部和事件流量。请注意，虚拟设备不支持多个管理接口。

为此，您可在虚拟思科 Firepower 管理中心上配置另外一个管理接口，以提高性能或分别管理两个不同网络中的流量。请另外再配置一个接口和一台虚拟交换机，用于将第二个管理接口连接至第二个网络中的受管设备。要给虚拟设备添加另外一个管理接口，请参阅 VMware vSphere (http://vmware.com)。有关多个管理接口的详细信息，请参阅*《Firepower 系统配置指南》*中的“管理设备”。

警告： 思科强烈建议您将生产网络流量和可信管理网络流量放于不同的网段。您必须采取预防措施来确保设备和管理流量数据流的安全。

典型 Firepower 系统部署

在物理设备环境中，典型的 Firepower 系统部署可使用物理设备和物理思科 Firepower 管理中心。下图显示的是一个部署示例。可以在内联配置中部署设备_A 和 设备_C，在被动配置中部署设备_B，如下所示。



您可在大多数网络交换机上配置端口镜像，以便将某个交换机端口（或整个 VLAN）中观测到的网络数据包复制一份发送至网络监控连接。端口镜像也被一家大型网络设备供应商称为交换机端口分析器或 SPAN，通过端口镜像您可以监控网络流量。请注意，设备_B 可通过服务器_A 和服务器_B 之间的交换机上的 SPAN 端口监控服务器_A 和服务器_B 之间的流量。

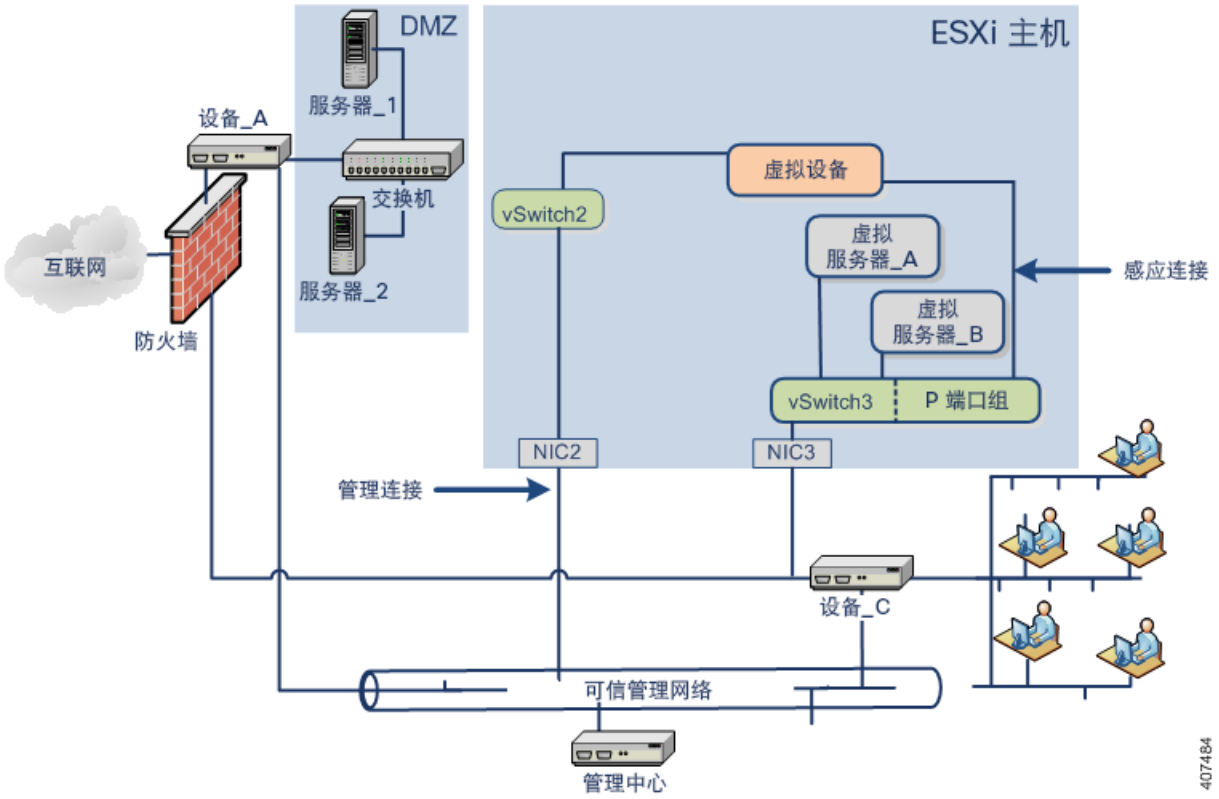
VMware 上的虚拟 Firepower 设备部署

添加虚拟化和虚拟设备

您可使用虚拟基础设施来替换典型 Firepower 系统部署（第 22 页）中所述的物理内部服务器。在以下示例中，可以使用 ESXi 主机，并将服务器_A 和服务器_B 虚拟化。

可以使用虚拟设备来监控服务器_A 和服务器_B 之间的流量。

虚拟设备感应接口必须连接至可接收混杂模式流量的交换机或端口组，如下所示。



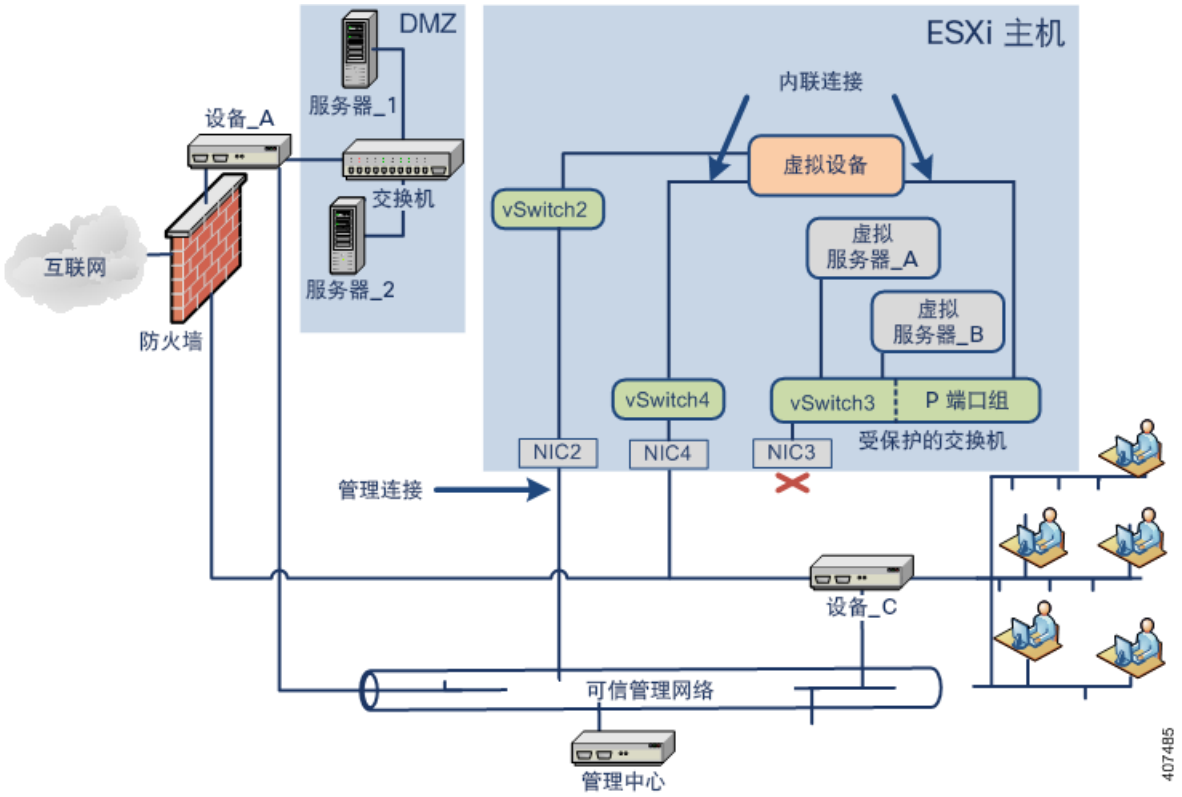
注意： 要感应所有流量，需在设备感应接口所连接的虚拟交换机或端口组允许混杂模式流量。

尽管示例仅显示了一个感应接口，但默认情况下虚拟设备配有两个感应接口。虚拟设备管理接口连接至您的可信管理网络以及思科 Firepower 管理中心。

使用虚拟设备进行内联检测

您可以使流量通过虚拟设备的内联接口组，从而在虚拟服务器周围界定一个安全边界。此场景依据典型 Firepower 系统部署（第 22 页）以及添加虚拟化和虚拟设备（第 22 页）中所示的示例建立而成。

首先，创建一台受保护的虚拟交换机，并将其连接至虚拟服务器。然后，使用虚拟设备将受保护的交换机连接至外部网络。有关详细信息，请参阅*《Firepower 系统配置指南》*。



注意： 要感应所有流量，需在设备感应接口所连接的虚拟交换机或端口组允许混杂模式流量。

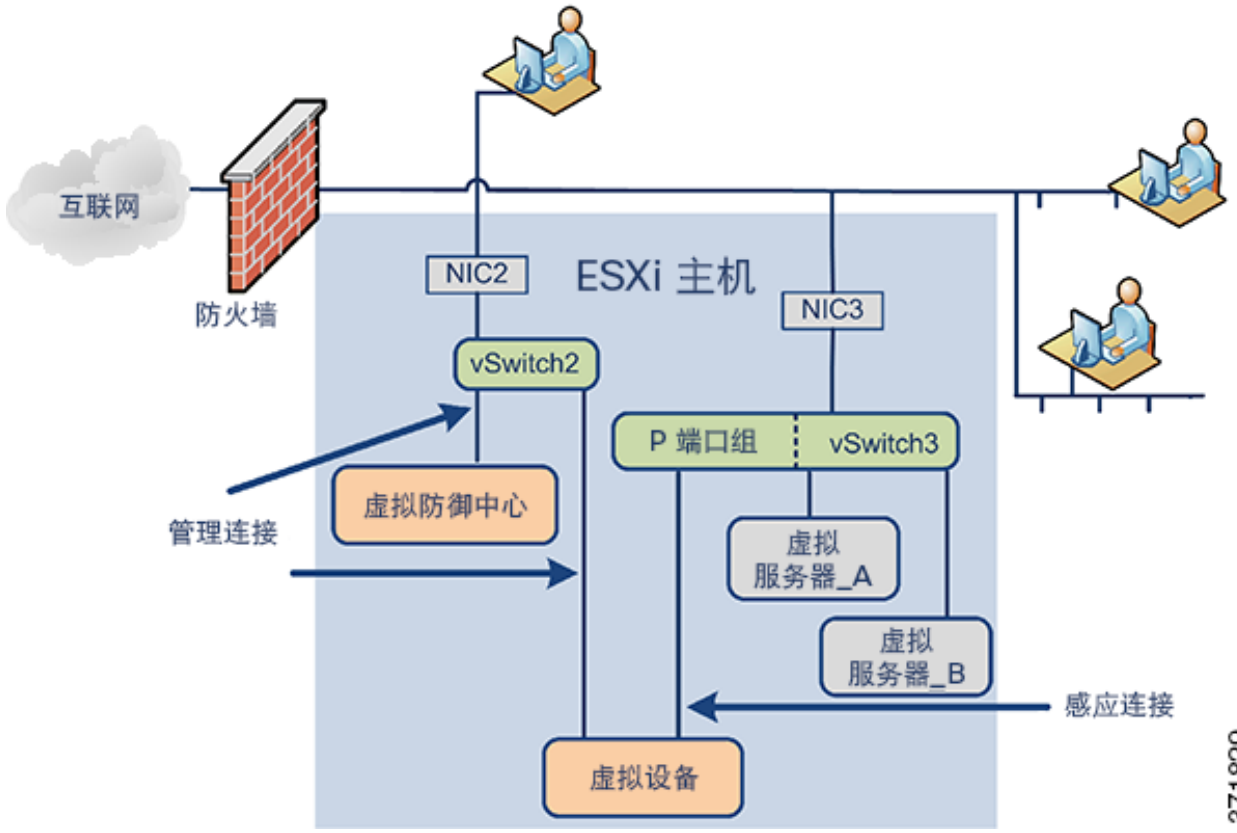
虚拟设备可按照入侵策略监控和丢弃进入服务器_A 和服务器_B 的任何恶意流量。

添加虚拟思科 Firepower 管理中心

您可以将虚拟思科 Firepower 管理中心部署在 ESXi 主机上，并将其连接至虚拟网络和物理网络，如下所示。此场景依据典型 Firepower 系统部署（第 22 页）以及使用虚拟设备进行内联检测（第 23 页）中所示的示例建立而成。

利用虚拟 Firepower 管理中心与可信管理网络之间通过 NIC2 的连接，虚拟 Firepower 管理中心能够同时管理物理和虚拟设备。

由于思科虚拟设备已随所需的应用软件进行预配置，因此，在 ESXi 主机上部署后，可随时运行。这将减少有关硬件和软件兼容性的问题，让您加快部署进程并体验 Firepower 系统的优势。您可以将虚拟服务器、虚拟 Firepower 管理中心和虚拟设备部署在 ESXi 主机上，并从虚拟 Firepower 管理中心管理部署，如下所示。

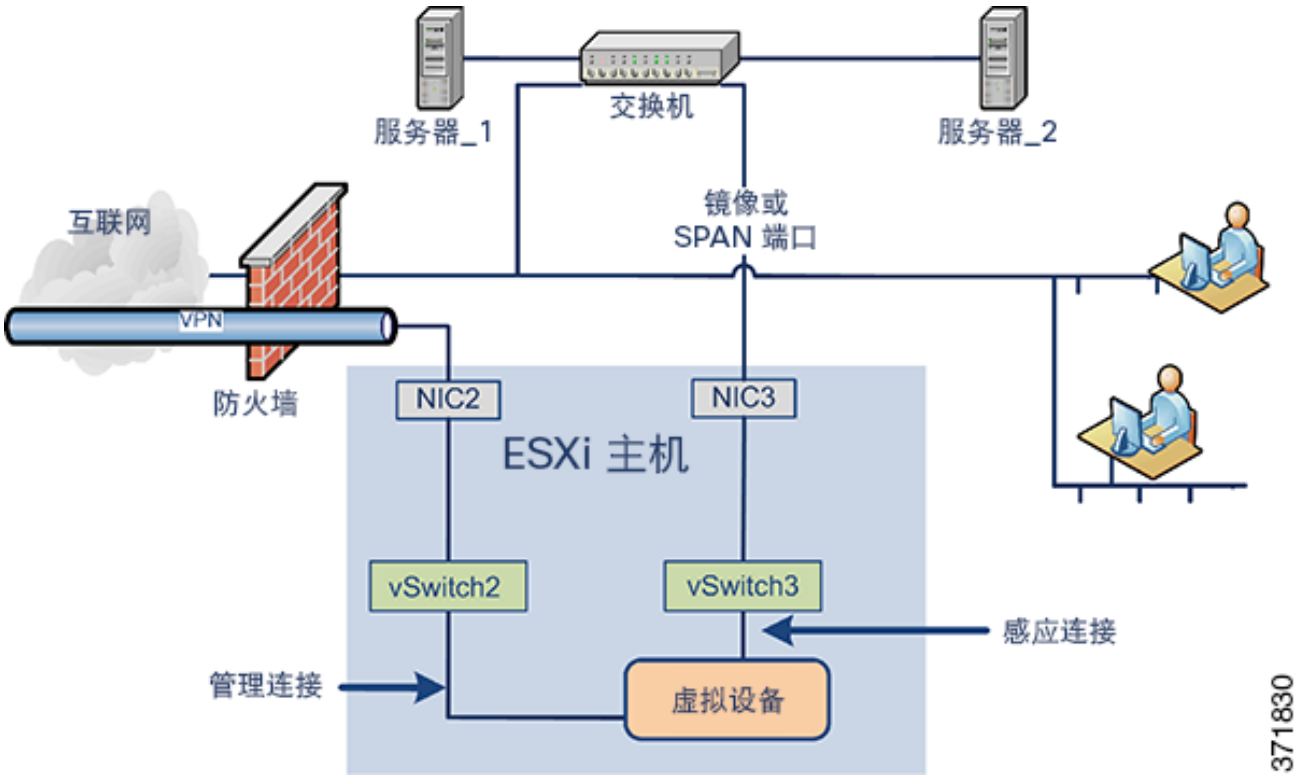


必须允许虚拟设备上的感应连接以监控网络流量。虚拟接口连接的虚拟交换机或该交换机上的端口组必须能够接收混杂模式流量。这样，虚拟设备便能读取欲发往其他计算机或网络设备的数据包。示例中，P 端口组设置为可接收混杂模式流量。

虚拟设备管理连接属于更典型的非混杂模式连接。虚拟 Firepower 管理中心可为虚拟设备提供命令和控制。利用通过 ESXi 主机的网络接口卡（示例中的 NIC2）实现的连接，您可以访问虚拟 Firepower 管理中心。有关建立虚拟 Firepower 管理中心和虚拟设备管理连接的信息，请参阅自动化 Firepower 管理中心虚拟设备网络设置（第 14 页）和*《适用于 VMware 的思科 NGIPSv 快速入门指南》*。

使用远程办公室部署

虚拟设备为在有限资源基础上监控远程办公室的一种理想方式。您可以将虚拟设备部署在 ESXi 主机上，用以监控本地流量，如下所示。



必须允许虚拟设备上的感应连接以监控网络流量。为此，感应接口连接的虚拟交换机或该交换机上的端口组必须能够接收混杂模式流量。这样，虚拟设备便能读取欲发往其他计算机或网络设备的数据包。示例中，所有 vSwitch3 均设置为可接收混合模式流量。VSwitch3 也通过 NIC3 连接至SPAN 端口，监控通过远程办公室交换机的流量。

虚拟设备必须由 Firepower 管理中心进行管理。利用通过 ESXi 主机的网络接口卡（示例中的 NIC2）实现的连接，您可以使用远程 Firepower 管理中心访问虚拟设备。

将设备部署在不同的地理位置时，必须采取预防措施，将设备与不受保护的网络隔离，来确保设备和数据流的安全。您可以通过 VPN 或其他安全隧道协议传输来自设备的数据流。

适用于 VMware 的思科 FirePOWER 虚拟设备故障排除

本部分描述有关常见设置问题的信息，以及提交问题至何处或从何处获得帮助。

时间同步

如果运行状况状况监控器显示虚拟设备时钟设置不同步，请检查系统策略时间同步设置。思科建议您将虚拟设备同步至物理 NTP 服务器。请勿将受管设备（虚拟或物理设备）同步到虚拟思科 Firepower 管理中心。为确保时间同步设置正确，请参阅*《Firepower 系统配置指南》*中的“时间同步”章节。在确定虚拟设备时钟设置正确之后，请联系 ESXi 主机管理员确保服务器时间配置正确。

性能问题

如果出现性能相关的问题，请记住，有多个因素会影响虚拟设备。有关可能会影响性能的因素列表，请参阅虚拟设备性能（第 4 页）。要监控 ESXi 主机性能，您可以利用 vSphere 客户端和**性能 (Performance)** 选项卡下的信息。

连接问题

您可以使用 VMware vCloud Director 门户网站和 vSphere 客户端，查看并确认管理和感应接口的连接。

使用 VMware vCloud Director 门户网站

您可以使用 VMware vCloud Director 门户网站，查看和确认管理连接及感应接口是否已正确连接。

要确认连接，请执行以下操作：

1. 选择**我的云 (My Cloud) > 虚拟机 (VMs)**，将鼠标停留在要查看的虚拟设备上并单击右键。
2. 在“操作”(Actions) 窗口中，点击**属性 (Properties)**。
3. 在**硬件 (Hardware)** 选项卡上，查看用于管理和感应接口的 NIC，以确认连接。

使用 vSphere 客户端

您可以使用 vSphere 客户端，查看和确认管理连接及感应接口是否已正确连接。

管理连接

在初始设置期间，必须确保网络适配器在带电时连接。否则，将无法正确完成初始管理连接设置，并显示以下信息：

```
ADDRCONF (NETDEV_UP): eth0: link is not ready
```

要确保管理连接已连接，请执行以下操作：

1. 右键单击 vSphere 客户端中虚拟设备的名称，然后选择**编辑设置 (Edit Settings)**。在**硬件 (Hardware)** 列表中，选择**网络适配器 1 (Network adapter 1)**，并确保选中**打开电源时连接 (Connect at power on)** 复选框。

   在初始管理连接完成时，检查 `/var/log/messages` 目录查看以下信息：

   ```
   ADDRCONF (NETDEV_CHANGE): eth0: link becomes ready
   ```

感应接口

在初始设置期间，必须确保感应接口在带电时连接。

为了确保感应接口在通电时连接，请执行以下操作：

1. 右键单击 vSphere 客户端中虚拟设备的名称，然后选择**编辑设置 (Edit Settings)**。在**硬件 (Hardware)** 列表中，选择**网络适配器 2 (Network adapter 2)** 和**网络适配器 3 (Network adapter 3)**。确保选中使用中的各适配器的**打开电源时连接 (Connect at power on)** 复选框。

   必须将虚拟设备感应接口连接至能接受混杂模式流量的虚拟交换机或虚拟交换机组。否则，设备只能检测广播流量。

后续操作

- 有关如何确保感应接口检测漏洞，请参阅*《适用于 VMware 的思科 NGIPSv 快速入门指南》*。

内联接口配置

您可以验证内联接口是否对称以及接口之间是否正传输流量。要打开虚拟设备的 VMware 控制台，请使用 VMware vCloud Director 门户网站或 vSphere 客户端。

为了确保内联感应接口配置正确，请执行以下操作：

1. 在控制台中，作为具有 CLI 配置（管理员）权限的用户登录。
2. 键入 `expert`，系统将显示外壳提示符。
3. 输入以下命令：`cat /proc/sf/sfe1000.*`

   系统将显示一个文本文件，含有类似以下的信息：

```
SFE1000 driver for eth1 is Fast, has link, is bridging, not MAC filtering, MAC timeout 7500,
Max Latency 0.
  39625470 packets received.
         0 packets dropped by user.
  13075508 packets sent.
0 Mode 1 LB Total 0 Bit 000...
.
.
SFE1000 driver for eth2 is Fast, has link, is bridging, not MAC filtering, MAC timeout 7500,
Max Latency 0.
  13075508 packets received.
         0 packets dropped by user.
  39625470 packets sent.
0 Mode 1 LB Total 0 Bit 00
```

请注意，`eth1` 上接收的数据包数量与从 `eth2` 发送的数据包数量匹配，且从 `eth1`发送的数据包数量与 `eth2` 上接收的数据包数量匹配。

4. 从虚拟设备注销。

5. 或者，如果支持直接路由至受保护的域，可以对虚拟设备的内联接口所连接的受保护虚拟设备进行 ping 操作。Ping 操作返回结果表明存在通过虚拟设备内联接口集连接。

获得帮助

感谢您使用思科产品。

思科支持

如果您有任何关于思科 ASA 设备的疑问或需要帮助，请通过以下方式与思科技术支持部门联系：

- 访问思科技术支持部门网站 http://www.cisco.com/cisco/web/support/index.html。
- 向思科支持部门发送邮件，邮箱为 tac@cisco.com。
- 致电思科支持部门，电话号码为 1.408.526.7209 或 1.800.553.2447。

获得帮助