FireSIGHT 虚拟安装指南

5.3.1 版本
2014 年 7 月 17 日

思科系统公司
www.cisco.com
思科在全球设有 200 多个办事处。
有关地址、电话号码和传真号码信息，
可查阅思科网站：
www.cisco.com/go/offices。

目 录

虚拟设备介绍

思科 FireSIGHT® 系统兼具行业领先的网络入侵防御系统安全性和基于检测到的应用、用户和 URL 控制网络访问的能力。

思科封装了适用于 VMware vSphere 和 VMware vCloud Director 宿主环境的 64 位虚拟防御中心® 和虚拟设备。通过 vCenter 或 vCloud Director，您可以将 64 位虚拟防御中心和 64 位虚拟受管设备部署到 ESXi 主机。防御中心为系统提供集中式管理控制台和数据存储库。无论是被动部署还是内联部署，虚拟设备均可检查虚拟或物理网络上的流量：

- 被动部署中的虚拟设备仅监控流经网络的流量。
- 被动感应接口无条件地接收所有流量，且这些接口上所接收的任何流量都不会被重新传输。
- 内联部署中的虚拟设备能够让网络免受可能影响网络上主机的可用性、完整性和保密性的攻击。可将内联设备部署为一个简单的入侵防御系统。也可以使用其他方法配置内联设备，以执行访问控制和管理网络流量。
- 内联接口无条件地接收所有流量，除非部署中的某些配置明确放弃这些流量，否则这些接口上接收的流量都不会被重新传输。

虚拟防御中心可管理物理设备、用于 X 系列的 Sourcefire 软件和具备 FirePOWER 服务的思科 ASA 防火墙 (ASA FirePOWER)；物理防御中心可管理虚拟设备。但是，虚拟设备不支持系统任何基于硬件的功能，虚拟防御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 FireSIGHT 系统设备的详细信息，请参阅 《*FireSIGHT 系统安装指南*》。

本安装指南提供关于部署、安装和设置虚拟 FireSIGHT 系统设备 （设备和防御中心）的相关信息。同时假定读者熟悉 VMware 产品 （包括 vSphere 客户端和 VMware vCloud Director 网络门户）的功能和术语定义。

以下主题将为您介绍 FireSIGHT 系统虚拟设备：

FireSIGHT 系统虚拟设备

FireSIGHT 系统*虚拟设备*可以指流量感应受管*虚拟设备*，也可以是管理型*虚拟*防御中心。有关详细信息，请参阅以下各节：

虚拟防御中心

防御中心为 FireSIGHT 系统部署提供一个集中的管理点和事件数据库。虚拟防御中心汇总并关联入侵、文件、恶意软件、发现、连接和性能数据，评估事件对特定主机的影响并用危害表现对主机进行标记。借助此功能，您可以监控设备所报告的与其他设备有关的信息，并评估和控制网络上发生的大体活动。

虚拟防御中心的主要功能包括：

- 设备、许可证和策略管理
- 表格、图形和图表中显示的事件和上下文信息
- 运行状况与性能监控
- 外部通知和警报
- 实时威胁响应的关联、危害表现及补救功能
- 自定义和基于模板的报告

虚拟受管设备

在贵公司内网段上部署的虚拟设备可监控流量以供分析。被动部署的虚拟设备可帮助您深入了解您的网络流量。在内联部署中，您可以使用虚拟设备基于多重标准来影响业务流。根据不同的型号和许可证，设备可：

- 收集有关贵公司的主机、操作系统、应用、用户、文件、网络和漏洞的详细信息
- 根据各种基于网络的标准以及其他标准（包括应用、用户、URL、IP 地址信誉和入侵或恶意软件检查结果）来阻止或允许网络流量

虚拟设备**没有**网络界面。您必须通过控制台和命令行对虚拟设备进行配置，且必须使用防御中心对其进行管理。

注意事项　您无法将虚拟设备升级或重新映像到 5.3.1 版本，但 5.3.1 版本的防御中心可管理 5.2 或 5.3 版本的虚拟设备。

了解虚拟设备功能

虚拟设备具有物理设备的诸多功能：

- 除了无法创建高可用性虚拟防御中心对之外，虚拟防御中心具有与物理防御中心相同的功能。借助 FireSIGHT 许可证，虚拟防御中心可监控 50,000 个主机和用户。
- 虚拟设备具有物理设备的流量和阻塞分析能力。但是，这些设备不能执行交换、路由、 VPN 和基于硬件、冗余和资源共享的其他功能。

了解虚拟防御中心的功能

表 1-1虚拟防御中心所支持的功能，第 1-3 页列出系统的主要功能并说明虚拟设备是否支持这些功能 （假设您正在管理支持这些功能的设备并已安装和应用了正确的许可证）。

有关虚拟设备所支持的功能和许可证摘要，请参阅 FireSIGHT 系统组件，第 1-6 页和许可虚拟设备，第 1-9 页。

请注意，虚拟防御中心可管理 2 系列、3 系列、ASA FirePOWER 和 X 系列设备。同样，2 系列和 3 系列防御中心可管理虚拟设备。与基于设备的功能 （例如：堆栈、交换和路由）相对应的防御中心栏指明了虚拟防御中心是否能够管理和配置设备以执行这些功能。例如，尽管您无法在虚拟设备上配置 VPN，但您可以使用虚拟防御中心来管理 VPN 部署中的 3 系列设备。

表 1-1　　虚拟防御中心所支持的功能

功能	虚拟防御中心
收集受管设备所报告的发现数据 （主机、应用和用户）并为贵公司建立一个网络映射	支持
查看网络流量的地理定位数据	支持
管理入侵检测和防御 (IPS) 部署	支持
管理执行安全情报过滤的设备	支持
管理执行简单的基于网络控制的设备，包括基于地理定位的过滤	支持
管理执行应用控制的设备	支持
管理执行用户控制的设备	支持
管理通过文字 URL 过滤网络流量的设备	支持
管理按类别和信誉执行 URL 过滤的设备	支持
管理按文件类型执行简单文件控制的设备	支持
管理执行基于网络的高级恶意软件防护 (AMP) 的设备	支持
从 FireAMP 部署接收基于终端的恶意软件 (FireAMP) 事件	支持

表 1-1　虚拟防御中心所支持的功能 （续）

功能	虚拟防御中心
管理基于设备及硬件的功能： • 快速路径规则 • 严格的 TCP 执行 • 可配置的旁路接口 • 侧录模式 • 交换和路由 • NAT 策略 • VPN	支持
管理基于设备的冗余和资源共享： • 设备堆叠 • 设备集群 • Sourcefire 软件 （用于 X 系列）VAP 组 • 集群堆叠	支持
构建高可用性	不支持
安装恶意软件存储包	不支持
连接至 eStreamer、主机输入或数据库客户端	支持

了解虚拟受管设备功能

表 1-2虚拟受管设备所支持的功能，第 1-4 页列出系统的主要功能并说明虚拟受管设备是否支持这些功能 （假设您已从管理防御中心中安装和应用了正确的许可证）。

请注意，尽管您可以使用运行系统 5.3.1 版本的任意型号防御中心来管理 5.2 或 5.3 版本的虚拟设备，但是，一些系统功能仍受防御中心型号的限制。例如， 2 系列 DC500 不可用于管理执行安全情报过滤的虚拟受管设备，即使这些虚拟受管设备支持该功能。有关详细信息，请参阅了解虚拟防御中心的功能，第 1-3 页。

表 1-2　虚拟受管设备所支持的功能

功能	虚拟受管设备
收集受管设备所报告的发现数据 （主机、应用和用户）并为贵公司建立一个网络映射	支持
查看网络流量的地理定位数据	支持
网络发现：主机、应用和用户	支持
入侵检测和防御 (IPS)	支持
安全情报过滤	支持
访问控制：基础网络控制	支持
访问控制：基于地理定位的过滤	支持
访问控制：应用控制	支持

表 1-2　　虚拟受管设备所支持的功能 （续）

功能	虚拟受管设备
访问控制：用户控制	支持
访问控制：文字 URL	支持
访问控制：按类别和信誉进行 URL 过滤	支持
文件控制：按文件类型	支持
基于网络的高级恶意软件防护 (AMP)	支持
自动应用旁路	支持
快速路径规则	不支持
严格的 TCP 执行	不支持
可配置的旁路接口	不支持
侧录模式	不支持
交换和路由	不支持
NAT 策略	不支持
VPN	不支持
设备堆叠	不支持
设备集群	不支持
集群堆叠	不支持
恶意软件存储包	不支持
FireSIGHT 系统特定交互式 CLI	支持
连接至 eStreamer 客户端	不支持

操作环境先决条件

您可以将 64 位虚拟设备托管至以下宿主环境：

- VMware vSphere Hypervisor 5.1
- VMware vSphere Hypervisor 5.0
- VMware vCloud Director 5.1

有关创建宿主环境的详细信息，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。 VMware 不支持无法识别 OVF 封装的工作站、播放器、服务器和 Fusion。此外，虚拟设备被封装成带虚拟硬件第 7 版的虚拟机。

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 1-3　　虚拟设备默认设置

设置	默认	设置可调节？
内存	4 GB	是，对于虚拟设备，您**必须**分配： • 最少 4 GB • 5 GB，用于基于类别和信誉的 URL 过滤 • 6 GB，用于使用大型动态源来执行安全情报过滤 • 7 GB，用于执行 URL 过滤和安全情报
虚拟 CPU	4	是，最多 8 个
硬盘配置大小	40 GB （设备） 250 GB （防御中心）	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

提示 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。

尽管思科不支持在来宾层安装工具 （包括 VMware 工具），但您可以在 ESXi 主机上安装工具（如 `esxtop` 或 VMware 第三方插件），以检验虚拟性能。但是，您只能在主机或虚拟化管理层而非来宾层中安装这些工具。

FireSIGHT 系统组件

以下各节描述虚拟防御中心和虚拟设备的一些关键功能，这些功能可提升贵公司的安全性，有助于促成可接受的使用策略以及流量管理策略。有关使用 2 系列和 3 系列设备所支持的其他功能的相关信息，请参阅 《*FireSIGHT 系统安装指南*》和 《*FireSIGHT 系统用户指南*》。

提示 虚拟设备的许多功能取决于许可证和用户角色。在必要的地方， FireSIGHT 系统文档提供了对每个功能和任务的要求。

下列主题描述 FireSIGHT 系统的一些关键功能，这些功能可提升贵公司的安全性，有助于促成可接受的使用策略以及流量管理策略：

FireSIGHT

FireSIGHT™ 是思科研发的发现和感知技术，用于收集主机、操作系统、应用、用户、文件、网络、地理位置信息和漏洞相关信息，帮助您全面了解您的网络。

通过防御中心的网络界面可查看和分析由 FireSIGHT 收集的数据。还可以基于该数据执行访问控制并修改入侵规则状态。此外，还可以根据主机的关联事件数据生成和跟踪网络上主机的危害表现。

访问控制

*访问控制*是一项基于策略的功能，允许您指定、检查和记录可经过您网络的流量。*访问控制策略*决定系统如何处理网络上的流量。您可以使用不包含*访问控制规则*的策略，以下列方式之一处理流量（采用所谓的*默认动作*）：

- 阻止所有流量进入网络
- 信任进入网络的所有流量，无需进一步检查
- 允许所有流量进入网络，并且只通过网络发现策略检查流量
- 允许所有流量进入网络，并且通过入侵和网络发现策略检查流量

您可以将访问控制规则添加至访问控制策略，从而进一步定义目标设备如何处理流量，从简单的 IP 地址匹配到涉及不同用户、应用、端口和 URL 的复杂场景。对于每个规则，都要指定规则*操作*，即是否根据入侵或文件策略信任、监控、阻止或者检查匹配的流量。

对于每项访问控制策略，您可以创建自定义 HTML 页面，当系统阻断 HTTP 请求时此页面将显示给用户。或者，您可以显示一个用户警告页面，也可以允许他们点击按钮继续前往先前请求的站点。

作为访问控制的一部分，在按访问控制规则对流量进行更深层次的分析之前，您可以使用安全情报功能拉黑特定 IP 地址，拒绝发往和来自该地址的流量。如果您的系统支持地理定位，还可以根据检测出的源和目标国家/地区和大洲过滤流量。

访问控制包括入侵检测和防御、文件控制和高级恶意软件防护。有关详细信息，请参阅接下来的章节。

入侵检测和防御

借助入侵检测和防御功能，您可以监控网络流量，以检测安全违规行为以及在内联部署中阻止或修改恶意流量

入侵防御被集成至访问控制，您可以通过访问控制将入侵策略与特定访问控制规则进行关联。如果网络流量符合某个规则中的条件，您可以使用入侵策略分析匹配流量。也可以将入侵策略与访问控制策略的默认操作进行关联。

入侵策略包含各种组件，包括：

- 检查协议头值、负载内容和某些数据包大小特征的规则
- 基于 FireSIGHT 建议的规则状态配置
- 高级设置，例如预处理器及其他检测和性能功能
- 预处理器规则，允许您为关联预处理器和预处理器选项生成事件

文件追踪、控制和恶意软件防护

为了便于识别和减轻恶意软件的影响， FireSIGHT 系统的文件控制、网络文件轨迹和高级恶意软件防护组件可以检测、跟踪、捕获、分析并选择性地阻止网络流量中的文件 （包括恶意软件文件）传输。

文件控制

通过 *文件控制*，受管设备可以检测和阻止用户通过特定应用协议上传 （发送）或下载 （接收）特定类型文件。您可在整体访问控制配置中配置文件控制；与访问控制规则相关的文件策略检查符合规则条件的网络流量。

基于网络的高级恶意软件防护 (AMP)

通过基于网络的 *高级恶意软件防护* (AMP)，系统可以检查网络流量，以发现某些类型文件中的恶意软件。可以将检测到的文件存储到硬盘，进行进一步的分析。

无论是否存储已检测到的文件，您都可以使用此文件的 SHA-256 哈希值，将文件提交至综合安全情报云，进行简单的已知文件性质查找。还可以提交文件用于 *动态分析*，产生威胁得分。您可以利用此上下文信息配置系统，以阻止或允许特定的文件。

您可在整体访问控制配置中配置恶意软件防护；与访问控制规则相关的文件策略检查符合规则条件的网络流量。

FireAMP 集成

FireAMP 是思科制定的企业级高级恶意软件分析和防护解决方案，可发现、了解和阻止高级恶意软件爆发、高级持续性威胁和针对性攻击。

如果贵公司已订用 FireAMP，个人用户可在其计算机和移动设备 （也称为 *终端*）上安装 *FireAMP Connectors*。这些轻型代理与综合安全情报云通信，该云进而与防御中心通信。

对防御中心进行配置使其连接到云之后，您可以通过防御中心网络界面查看贵公司中的终端经过扫描、检测和隔离而产生的基于终端的恶意软件事件。防御中心还基于 FireAMP 数据生成和跟踪主机上的危害表现，并显示网络文件轨迹。

请使用 *FireAMP 门户网站* (http://amp.sourcefire.com/) 来配置 FireAMP 部署。该门户网站可帮您快速识别并隔离恶意软件。在恶意软件爆发时，您可以识别并追踪其轨迹、了解其影响和了解如何顺利恢复。您也可以使用 FireAMP 创建自定义保护，基于组策略阻止特定应用的执行，并创建自定义白名单。

网络文件轨迹

网络文件轨迹功能可以用来跟踪一个文件在网络中的传输路径。系统使用 SHA-256 哈希值跟踪文件；因此，为了追踪文件，系统必须执行下列操作之一：

- 计算文件的 SHA-256 哈希值，并使用该值执行恶意软件云查找
- 通过将防御中心与贵公司的 FireAMP 订用集成来接收与该文件相关的基于终端的威胁和隔离数据

每个文件都有一个关联的轨迹图，其中包含随时间推移文件传输的视觉展示和其他文件补充信息。

应用程序编程接口

您可以使用应用程序编程接口 (API) 以不同的方式与系统交互 关于详细信息，可从技术支持站点下载附加文档。

eStreamer

通过 Event Streamer (eStreamer)，您可以将多种事件数据从思科设备流处理至定制开发的客户端应用。创建一个客户端应用之后，您可以将其连接至 eStreamer 服务器 （防御中心或受管设备），启动 eStreamer 服务，开始交换数据。

eStreamer 集成需要自定义编程，但您可以从设备中请求特定数据。例如，如果您需要在某个网络管理应用中显示网络主机数据，那么您可以编写一个程序，从防御中心检索主机重要性或安全漏洞数据，并将此信息添加至显示屏。

外部数据库访问

借助数据库访问功能，您可以通过支持 JDBC SSL 连接的第三方客户端，查询防御中心的多个数据库表。

您可以使用行业标准报告工具 （例如：Crystal Reports、 Actuate BIRT 或 JasperSoft iReport）设计和提交查询。或者，配置自定义应用来查询思科数据。例如，您可以建立一个小服务程序，用于定期报告入侵和发现事件数据或刷新警报控制面板。

主机输入

借助主机输入功能，您可以使用脚本或命令行文件从第三方源导入数据，从而添加信息至网络映射。

网络界面还提供一些主机输入功能；您可以修改操作系统或应用协议标识，启用或禁用漏洞，同时从网络映射中删除各项目，包括客户端和服务器端口。

补救措施

该系统包含一个 API，允许您创建纠正措施，从而在网络上条件违反相关性策略或合规性白名单时，防卫中心可自动启动。该功能不仅可以在您无法立即解决攻击的时候自动缓解攻击，还可以确保系统符合贵公司的安全策略。除您所创建的补救措施之外，防御中心还配备多个预定义的补救模块。

许可虚拟设备

您可以许可各种功能，为贵公司创建最佳 FireSIGHT 系统部署。必须使用防御中心来控制其自身和所管理设备的许可证。

思科建议您在防御中心的初始设置过程中添加贵公司已购买的许可证。否则，初始设置过程中注册的所有设备均会作为未许可设备添加至防御中心。初始设置流程结束后，必须逐个启用每个设备的许可证。有关详细信息，请参阅设置虚拟设备，第 4-1 页。

防御中心在购买时已包含一个 FireSIGHT 许可证。执行主机、应用和用户发现时均需该许可证。防御中心上的 FireSIGHT 许可证同时决定了使用防御中心及其受管设备时可以监控的主机和用户数量，以及进行用户控制的用户数量。对于虚拟防御中心，该限值为 50,000 个主机和用户。

如果防御中心以前运行的是 4.10.x 版本，那么您可以使用旧版 RNA 主机和 RUA 的用户许可证，而非 FireSIGHT 许可证。有关详细信息，请参阅许可证设置，第 4-9 页。

其他适用于特定型号的许可允许您的受管设备执行以下多种功能：

保护

保护许可证允许虚拟设备设备进行入侵检测和防御、文件控制和安全情报过滤。

控制

控制许可证允许虚拟设备执行用户和应用控制。尽管虚拟设备不支持控制许可证向 2 系列和 3 系列设备授予的任何基于硬件的功能（如交换或路由），但虚拟防御中心可管理物理设备上的此类功能。控制许可证需要一个保护许可证。

URL 过滤

URL 过滤许可证允许虚拟设备使用定期更新基于云的类别和信誉数据，以便根据受监控主机所请求的 URL 确定可经由网络的流量。 URL 过滤许可证需要一个保护许可证。

恶意软件

恶意软件许可证允许受管设备执行基于网络的高级恶意软件防护 (AMP)，即，检测并阻止网络传输的文件中的恶意软件。它还允许您查看跟踪网络传输文件的轨迹。恶意软件许可证需要一个保护许可证。

VPN

VPN 许可证允许您使用虚拟防御中心在 3 系列设备上的虚拟路由器之间、或从在 3 系列设备到远程设备或其他第三方 VPN 终端之间，建立安全的 VPN 隧道。 VPN 许可证需要保护和控制许可证。

由于架构和资源的限制，并非所有许可证都可应用于所有受管设备。一般而言，您无法许可设备不支持的功能；请参阅了解虚拟设备功能，第 1-3 页。下表汇总了可添加至虚拟防御中心并应用于每个设备型号的许可证。

- 设备行表示您是否可以将相应许可证应用到使用其管理防御中心的设备，包括防御中心。
- 防御中心行（适用于 FireSIGHT 之外的许可证）表示防御中心是否可以将相应许可证应用至设备（包括虚拟设备）。例如， DC500 无法将URL 过滤许可应用到虚拟设备。

例如，您可以通过虚拟防御中心使用 3 系列创建一个 VPN 部署，但是，您无法通过 DC500 使用虚拟设备来执行基于类别和信誉的 URL 过滤。请注意，不适用表示与受管设备无关并基于防御中心的许可证。

表 1-4　　不同型号所支持的许可证

型号	FireSIGHT	保护	控制	URL 过滤	恶意软件	VPN
2 系列设备： • 3D500/1000/2000 • 3D2100/2500/3500/4500 • 3D6500 • 3D9900	不适用	自动，无安全情报	否	否	否	否
3 系列设备： • 7000 系列 • 8000 系列	不适用	支持	支持	支持	支持	支持
虚拟设备	不适用	支持	支持，但不支持硬件功能	支持	支持	否
Sourcefire 软件 （用于 X 系列）	不适用	支持	支持，但不支持硬件功能	支持	支持	否
具备 FirePOWER 服务的思科 ASA 防火墙	不适用	支持	支持，但不支持硬件功能	支持	支持	否
DC500 2 系列防御中心	支持	支持，但无安全情报	支持，但无用户控制	否	否	支持
DC1000/3000 2 系列防御中心	支持	支持	支持	支持	支持	支持
DC750/1500/3500 3 系列防御中心	支持	支持	支持	支持	支持	支持
虚拟防御中心	支持	支持	支持	支持	支持	支持

有关许可证的详细信息，请参阅 《*FireSIGHT 系统用户指南*》中的“许可 FireSIGHT 系统”。

安全性、互联网接入和通信端口

为了保护防御中心的安全，应将其安装在受保护的内部网络中。虽然防御中心仅提供必要的服务和端口，但必须确保其 （或任何受管设备）不会受到防火墙外部的攻击。

如果防御中心及其受管设备位于同一个网络，可以将设备的管理接口连接到与防御中心相同的受保护内部网络。这样您就可以安全地从防御中心控制设备。

无论设备如何部署，设备内部通信必须加密。但是，您仍需采取措施，确保设备之间的通信不会出现中断、阻塞或受到篡改；例如，被分布式拒绝服务 (DDoS) 或中间人攻击。

另请注意， FireSIGHT 系统的特定功能需要互联网连接。默认情况下，所有设备配置直接连接到互联网。此外，系统要求某些端口保持打开状态，以便进行基本的设备内部通信和安全设备访问，这样，特定系统功能就可以访问正确运行所需的本地或互联网资源。

提示　除用于 X 系列的 Sourcefire 软件和具备 FirePOWER 服务的思科 ASA 防火墙外， FireSIGHT 系统设备支持代理服务器。有关详细信息，请参阅 《*FireSIGHT 系统用户指南*》。

有关详细信息，请参阅：

- 互联网访问要求，第 1-12 页
- 通信端口要求，第 1-12 页

互联网访问要求

虚拟防御中心配置为可通过默认打开的端口 443/tcp (HTTPS) 和端口 80/tcp (HTTP) 直接连接到互联网。在虚拟设备上，只要您启用了恶意软件许可证，端口 443 就处于打开状态，设备就可以提交用于动态分析的文件。有关详细信息，请参阅通信端口要求，第 1-12 页。FireSIGHT 虚拟设备支持使用代理服务器；有关详细信息，请参阅 《FireSIGHT 系统*用户指南*》。

下表描述了 FireSIGHT 系统特定功能的互联网接入需求。

表 1-5　　FireSIGHT 系统功能的互联网接入需求

功能	需要互联网接入，以.....	设备
动态分析：查询	查询综合安全情报云，了解以前提交进行动态分析的文件的威胁得分。	防御中心
动态分析：提交	提交文件至综合安全情报云进行动态分析。	受管设备
FireAMP 集成	接收来自综合安全情报云云的基于终端的 (FireAMP) 恶意软件事件。	防御中心
入侵规则、VDB 和 GeoDB 更新	直接下载或安排下载入侵规则、 GeoDB 或 VDB 更新至设备。	防御中心
基于网络的 AMP	执行恶意软件云查找。	防御中心
RSS 源控制面板构件	从外部来源，包括思科，下载 RSS 源数据。	任何设备，虚拟设备、 X 系列和 ASA FirePOWER 除外
安全情报过滤	从外部来源下载安全情报源数据，包括 FireSIGHT 系统情报源。	防御中心
系统软件更新	直接下载或安排下载系统更新至设备。	任何设备，虚拟设备、 X 系列和 ASA FirePOWER 除外
URL 过滤	下载基于云的 URL 类别和信誉数据进行访问控制，并执行未分类的 URL 查找。	防御中心
whois	请求外部主机的域名项信息。	任何设备，虚拟设备、 X 系列和 ASA FirePOWER 除外

通信端口要求

FireSIGHT 系统设备使用双向的 SSL 加密通信信道进行通信。该信道默认使用端口 8305/TCP。系统**要求**该端口保持开放状态，以便进行基本的设备内部通信。其他开放的端口允许：

- 访问设备的网络界面
- 确保设备的远程连接安全
- 系统的某些功能访问正常运行所需的本地或网络资源

一般来说，除非启用或配置相关功能，否则，功能相关的端口会保持关闭。例如，在将防御中心连接到用户代理之前，代理通信端口 (3306/tcp) 保持关闭。又例如，在启用 LOM 之前， 3 系列设备上的端口 623/udp 保持关闭。

注意事项　在了解此操作对部署的影响之前，请勿关闭已打开的端口。

例如，关闭受管设备上的出站端口 25/tcp (SMTP) 后，设备将无法发送关于单个入侵活动的邮件通知（请参阅《*FireSIGHT 系统用户指南*》）。又例如，关闭端口 443/TCP (HTTPS) 后，将禁止访问物理受管设备的网络界面，但是，设备却无法将可疑的恶意软件文件提交到综合安全情报云以进行动态分析。

请注意，系统允许您更改某些通信端口：

- 在配置系统与身份验证服务器之间的连接时，您可以指定用于 LDAP 和 RADIUS 身份验证的自定义端口；请参阅《*FireSIGHT 系统用户指南*》。
- 您可以更改管理端口 (8305/TCP)；请参阅《*FireSIGHT 系统用户指南*》。但是，思科**强烈**建议您保留默认设置。如果要更改管理端口，您必须更改部署中需要相互通信的所有设备的管理端口。
- 您可以通过端口 32137/tcp 将已升级的防御中心与综合安全情报云进行通信。但是，思科建议您切换到端口 443。该端口为 5.3 版本及更高版本全新安装的默认端口。有关详细信息，请参阅《*FireSIGHT 系统用户指南*》。

下表列出了每种设备类型所需的开放端口，以使 FireSIGHT 系统功能得到充分利用。

表 1-6　FireSIGHT 系统功能和操作的默认通信端口

端口	说明	方向	在.....上打开	以.....
22/TCP	SSH/SSL	双向	任意	允许到设备的安全远程连接。
25/TCP	SMTP	出站	任意	从设备发送邮件通知和警报。
53/TCP	DNS	出站	任意	使用 DNS。
67/UDP 68/UDP	DHCP	出站	任何设备， X 系列除外	使用 DHCP。 **注**　默认情况下，这些端口为**关闭状态**。
80/TCP	HTTP	出站	任何设备，虚拟设备、 X 系列和 ASA FirePOWER 除外	允许 RSS 源控制面板构件连接到一个远程网络服务器。
		双向	防御中心	通过 HTTP 更新自定义和第三方安全情报源。 下载 URL 类别和信誉数据（还需要端口 443）。
161/UDP	SNMP	双向	任何设备， X 系列和 ASA FirePOWER 除外	允许通过 SNMP 轮询访问设备的 MIB。
162/UDP	SNMP	出站	任意	发送 SNMP 警报至远程陷阱服务器。
389/TCP 636/TCP	LDAP	出站	任何设备，虚拟设备和 X 系列除外	与 LDAP 服务器通信以进行外部身份验证。
389/TCP 636/TCP	LDAP	出站	防御中心	获取检测到的 LDAP 用户元数据。
443/TCP	HTTPS	入站	任何设备，虚拟设备、 X 系列和 ASA FirePOWER 除外	访问设备的网络界面。

表 1-6　FireSIGHT 系统功能和操作的默认通信端口 （续）

端口	说明	方向	在.....上打开	以.....
443/TCP	HTTPS AMQP cloud comms.	双向	防御中心	获取： • 软件、入侵规则、 VDB 和 GeoDB 更新 • URL 类别和信誉数据 （还需要端口 80）。 • 综合安全情报源和其他安全的安全情报源 • 基于终端的 (FireAMP) 恶意软件事件 • 网络流量中检测到的文件的恶意软件性质 • 已提交文件的动态分析信息
			2 系列和 3 系列设备	使用设备的本地网络界面下载软件更新。
			3 系列、虚拟设备、 X 系列和 ASA FirePOWER	提交文件进行动态分析。
514/UDP	系统日志	出站	任意	向远程系统日志服务器发送警报。
623/UDP	SOL/LOM	双向	3 系列	允许使用 Serial Over LAN (SOL) 连接执行无人值守管理。
1500/TCP 2000/TCP	入站	TCP	防御中心	允许第三方客户端对数据库进行只读访问。
1812/UDP 1813/UDP	RADIUS	双向	任何设备，虚拟设备、 X 系列和 ASA FirePOWER 除外	与 RADIUS 服务器通信以进行外部身份验证和记帐。
3306/TCP	用户代理	入站	防御中心	与用户代理通信。
8302/TCP	eStreamer	双向	任何设备，虚拟设备和 X 系列除外	与 eStreamer 客户端通信。
8305/TCP	设备管理	双向	任意	在同一部署中的设备之间安全地进行通信。**要求**。
8307/TCP	主机输入客户端	双向	防御中心	与主机输入客户端通信。
32137/TCP	cloud comms.	双向	防御中心	允许升级的防御中心与综合安全情报云云进行通信。

部署虚拟设备

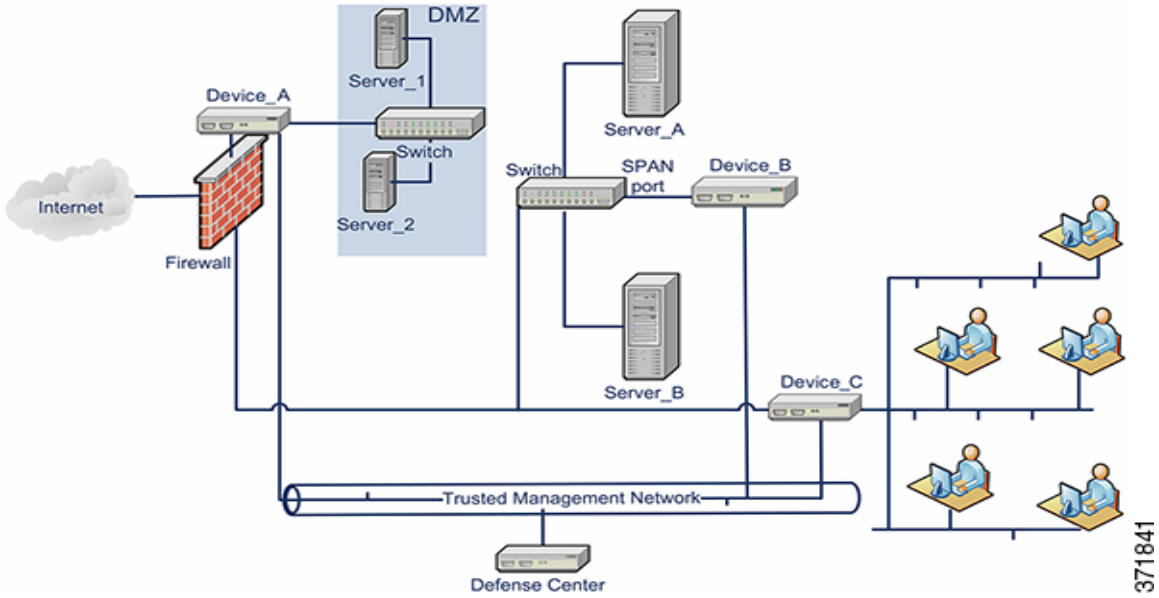
您可以利用虚拟设备和虚拟防御中心，在虚拟环境中部署安全解决方案，从而加强对物理和虚拟资产的保护。通过虚拟设备和虚拟防御中心，您可以在 VMware 平台上轻松实施安全解决方案。此外，虚拟设备还方便您部署和管理资源可能受到限制的远程站点中的设备。在以下示例中，可使用物理或虚拟防御中心来管理物理或虚拟设备。您可在 IPv4 或 IPv6 网络中进行部署。

注意事项 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。

本章提供适用于以下情况的部署示例：

典型 FireSIGHT 系统部署

在物理设备环境中，典型的 FireSIGHT 系统部署可使用物理设备和物理防御中心。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 虚拟设备部署

有关典型部署的示例，请参阅以下虚拟设备部署场景：

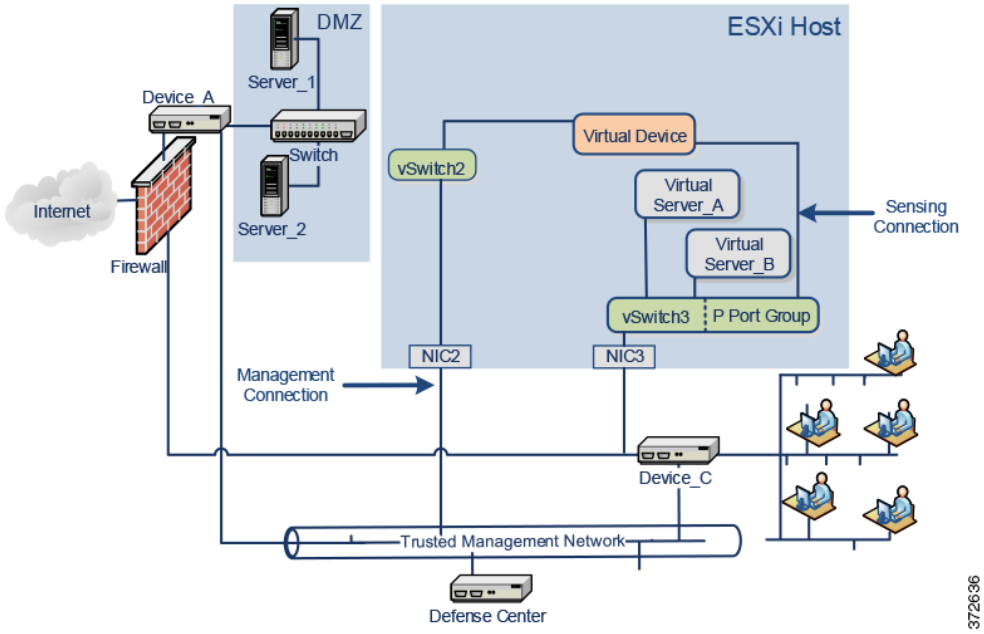
- 添加虚拟化和虚拟设备，第 2-2 页
- 使用虚拟设备进行内联检测，第 2-3 页
- 添加虚拟防御中心，第 2-4 页
- 使用远程办公室部署，第 2-6 页

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 FireSIGHT 系统部署，第 2-1 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。



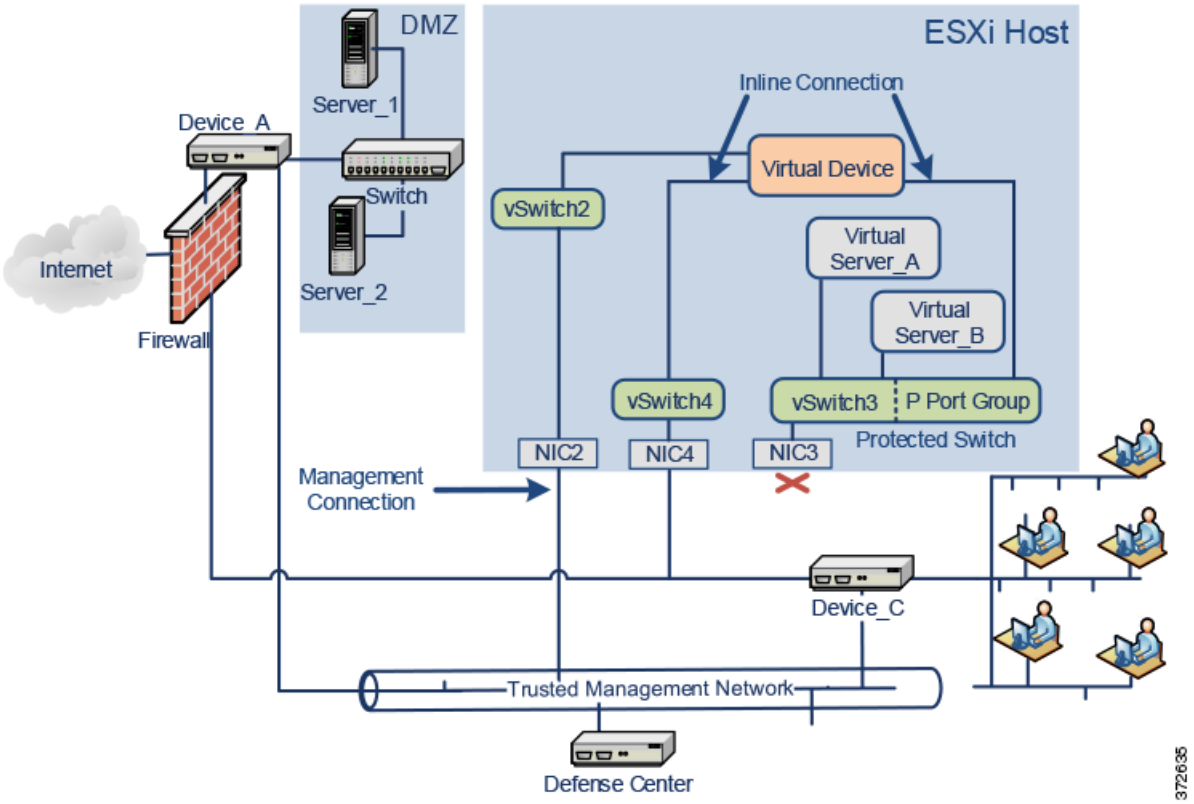
注　要感应所有流量，需在设备感应接口所连接的虚拟交换机或端口组允许混杂模式流量。请参阅配置虚拟设备接口，第 3-9 页。

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防御中心。

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 FireSIGHT 系统部署，第 2-1 页以及添加虚拟化和虚拟设备，第 2-2 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《*FireSIGHT 系统用户指南*》。



注　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。请参阅配置虚拟设备接口，第 3-9 页。

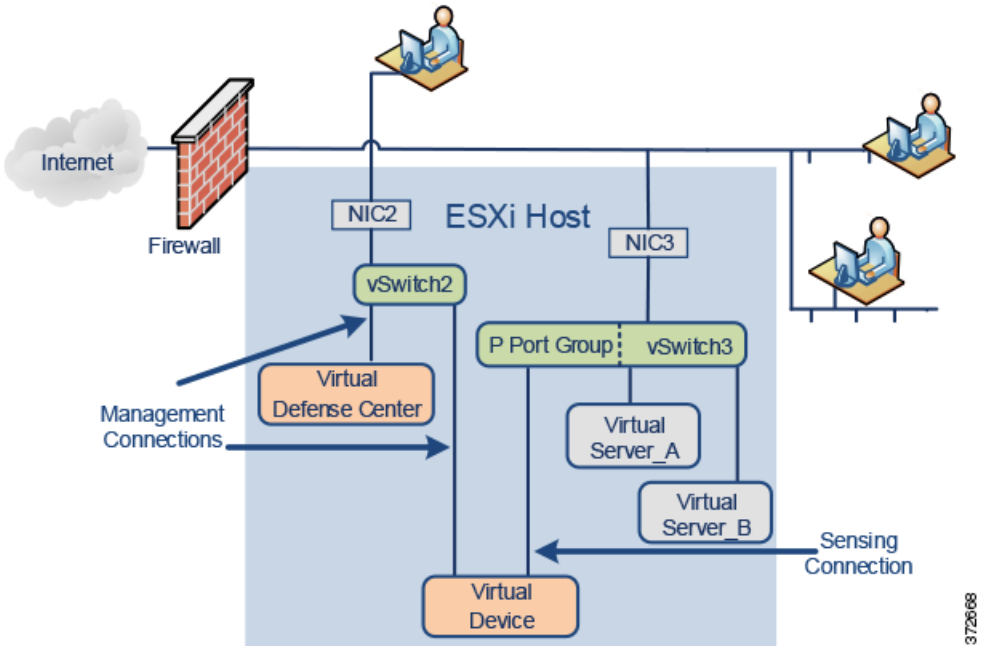
虚拟设备可按照入侵策略监控和丢弃进入服务器_A 和服务器_B 的任何恶意流量。

添加虚拟防御中心

您可以将虚拟防御中心部署在 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 FireSIGHT 系统部署，第 2-1 页以及使用虚拟设备进行内联检测，第 2-3 页中所示的示例建立而成。

利用虚拟防御中心与可信管理网络之间通过 NIC2 的连接，虚拟防御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 FireSIGHT 系统的优势。可以将虚拟服务器、虚拟防御中心和虚拟设备部署在 ESXi 主机上，并通过虚拟防御中心管理部署工作，如下所示。

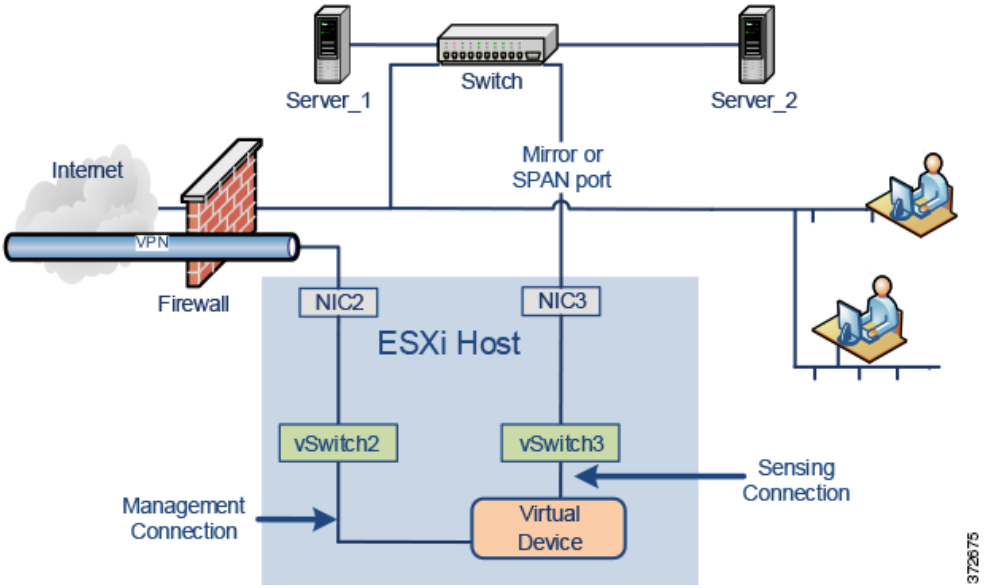


必须允许虚拟设备上的感应连接以监控网络流量。虚拟接口连接的虚拟交换机或该交换机上的端口组必须能够接收混杂模式流量。这样，虚拟设备便能读取欲发往其他计算机或网络设备的数据包。示例中， P 端口组设置为可接收混杂模式流量。请参阅配置虚拟设备接口，第 3-9 页。

虚拟设备管理连接属于更典型的非混杂模式连接。虚拟防御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，您可以访问虚拟防御中心。有关建立虚拟防御中心和虚拟设备管理连接的信息，请参阅自动化虚拟防御中心网络设置，第 4-6 页和使用 CLI 设置虚拟设备，第 4-3 页。

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。请参阅配置虚拟设备接口，第 3-9 页。

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

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。有关建立虚拟设备管理连接的信息，请参阅使用 CLI 设置虚拟设备，第 4-3 页。

安装虚拟设备

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硬件的版本为 7 的虚拟机。

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 FireSIGHT 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）。
- 必须部署到管理平台，即 VMware vCloud Director 或 VMware vCenter。
- 在使用 ESXi OVF 模板部署时，必须在安装后使用虚拟设备 VMware 控制台上的命令行界面 (CLI) 配置设置。
- 您可以部署到管理平台 （VMware vCloud Director 或 VMware vCenter），也可以部署为独立设备。

注 不支持思科虚拟设备的 VMware 快照

使用本章中的说明下载、安装和配置思科虚拟设备。有关创建虚拟主机环境的帮助，请参阅 ESXi VMware 文档。

在根据以下步骤安装和配置虚拟设备后，请按下一章所述启动以初始化并开始初始设置过程。有关卸载虚拟设备的信息，请参阅卸载虚拟设备，第 3-9 页。

要安装和部署思科虚拟设备，请执行以下操作：

步骤 1 确保计划的部署满足操作环境先决条件，第 1-5 页中所述的先决条件。

步骤 2 从支持站点获取正确的存档文件，将其复制到适当的存储介质，并解压缩；请参阅获取安装文件，第 3-2 页。

步骤 3 使用 VMware vCloud Director 网络门户或 vSphere 客户端安装虚拟设备，但是不要启动；请参阅安装虚拟设备，第 3-3 页。

步骤 4 确认并调整网络、硬件和内存设置；请参阅安装后更新重要设置，第 3-8 页。

步骤 5 确保虚拟设备上的感应接口已正确连接到 ESXi 主机虚拟交换机；请参阅配置虚拟设备接口，第 3-9 页。

获取安装文件

思科提供用于安装虚拟设备的压缩存档 (.tar.gz) 文件，一个用于防御中心，一个用于设备。每个存档文件包含以下文件：

- 文件名中包含 -ESXi- 的开放虚拟格式模板 (.ovf)
- 文件名中包含 -VI- 的开放虚拟格式模板 (.ovf)
- 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)

在安装虚拟设备前，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， 5.2 或 5.3）关联。

要获取虚拟设备存档文件，请执行以下操作：

步骤 1　请使用支持帐户的用户名和密码登录支持站点 (https://support.sourcefire.com/)。

步骤 2　点击 **Downloads**，在系统显示的页面上选择 **3D System** 选项卡，然后点击要安装的系统软件的主要版本。

例如，要下载 5.3.1 版本的存档文件，请点击 **Downloads > 3D System > 5.3**。

步骤 3　使用以下命名约定，查找要为或虚拟设备或虚拟防御中心下载的存档文件：

```
Sourcefire_3D_Device_Virtual64_VMware -  X.x.x、.tar .gz
Sourcefire_Defense_Center_Virtual64_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。

可以在页面左侧点击其中一个链接查看页面的相应部分。例如，点击 **5.3 虚拟设备**，查看 5.3.1 版本的 FireSIGHT 系统的存档文件。

步骤 4　点击要下载的存档文件。

文件开始下载。

提示　在登录支持站点时，思科建议下载虚拟设备的任何可用更新，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。对于防御中心，还应下载任何新入侵规则和漏洞数据库 (VDB) 更新。

步骤 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。

注意事项　请**勿**通过邮件传输存档文件；文件可能已损坏。

步骤 6　使用首选工具解压缩存档文件并提取安装文件。

对于虚拟设备：

```
Sourcefire_3D_Device_Virtual64_VMware-X.X.X-xxx-disk1.vmdk
Sourcefire_3D_Device_Virtual64_VMware-ESXi-X.X.X-xxx.ovf
Sourcefire_3D_Device_Virtual64_VMware-ESXi-X.X.X-xxx.mf
Sourcefire_3D_Device_Virtual64_VMware-VI-X.X.X-xxx.ovf
Sourcefire_3D_Device_Virtual64_VMware-VI-X.X.X-xxx.mf
```

对于虚拟防御中心：

```
Sourcefire_Defense_Center_Virtual64_VMware-X.X.X-xxx-disk1.vmdk
Sourcefire_Defense_Center_Virtual64_VMware-ESXi-X.X.X-xxx.ovf
Sourcefire_Defense_Center_Virtual64_VMware-ESXi-X.X.X-xxx.mf
Sourcefire_Defense_Center_Virtual64_VMware-VI-X.X.X-xxx.ovf
Sourcefire_Defense_Center_Virtual64_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。

请确保将所有文件存放在同一目录中。

步骤 7　继续安装虚拟设备以部署虚拟设备。

安装虚拟设备

要安装虚拟设备，使用平台界面 （VMware vCloud Director 网络门户或 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 FireSIGHT 系统所需的设置。必须使用 VMware vCloud Director 或 VMware vCenter 管理虚拟设备。
- 如果部署使用 ESXi OVF 模板，必须在安装后配置 FireSIGHT 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 1-5 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：

- 对于虚拟防御中心：

```
Sourcefire_Defense_Center_Virtual64_VMware-VI-X.X.X-xxx.ovf
Sourcefire_Defense_Center_Virtual64_VMware-ESXi-X.X.X-xxx.ovf
```

- 对于虚拟设备：

```
Sourcefire_3D_Device_Virtual64_VMware-VI-X.X.X-xxx.ovf
Sourcefire_3D_Device_Virtual64_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 3-1　　VMware OVF 模板

设置	操作
导入/部署 OVF 模板	浏览上一步骤中下载的 OVF 模板进行使用。
OVF 模板详细信息	确认正在安装的设备 （虚拟防御中心或虚拟设备）和部署选项 （VI 或 ESXi）。
名称和位置	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	仅对于虚拟设备，请选择要在其中部署设备的主机或集群。
磁盘格式	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	选择虚拟设备的管理接口。

如果使用 VI OVF 模板部署，安装过程允许进行虚拟防御中心的基本设置以及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
- 初始检测测模式（仅适用于虚拟设备）
- 管理防御中心（仅适用于虚拟设备）

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，请参阅设置虚拟设备，第 4-1 页。

使用以下选项之一安装虚拟设备：

- 使用 VMware vCloud Director 网络门户安装，第 3-4 页 说明如何将虚拟设备部署到 VMware vCloud Director。
- 使用 vSphere 客户端安装，第 3-6 页 说明如何将虚拟设备部署到 VMware vCenter。

要了解网络设置和检测模式，请参阅使用 CLI 设置虚拟设备，第 4-3 页和设置虚拟防御中心，第 4-6 页。

使用 VMware vCloud Director 网络门户安装

按照以下步骤，可以使用 VMware vCloud Director 网络门户部署虚拟设备：

- 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*》。
- 将 FireSIGHT 系统虚拟设备 OVF 包作为 vApp 模板上载到此目录。有关详细信息，请参阅上载虚拟设备 OVF 包，第 3-4 页。
- 使用 vApp 模板创建虚拟设备。有关详细信息，请参阅使用 vApp 模板，第 3-5 页。

上载虚拟设备 OVF 包

可以将以下 OVF 上载到 VMware vCloud Director 组织目录：

- 对于虚拟防御中心：

  `Sourcefire_Defense_Center_Virtual64_VMware-VI-X.X.X-  xxx.ovf`

- 对于虚拟设备：

  `Sourcefire_3D_Device_Virtual64_VMware-VI-X.X.X-xxx.ovf`

其中，*X.X.X-xxx* 是要上载的 OVF 包的版本和内部版本号。

要上载虚拟设备 OVF 包，请执行以下操作：

步骤 1　在 VMware vCloud Director 网络门户上，选择 **Catalogs >** *Organization* **> vApp Templates**，其中，*Organization* 是要包含 vApp 模板的组织名称。

步骤 2　在 vApp Templates 媒体选项卡中，点击 Upload 图标 ( )。

在系统显示弹出窗口时上载 OVF 包。

步骤 3　在 OVF 包字段中，输入 OVF 包的位置或点击 **Browse**，浏览 OVF 包。

- 对于虚拟防御中心：

  `Sourcefire_Defense_Center_Virtual64_VMware-VI-X.X.X-xxx.ovf`

- 对于虚拟设备：

  `Sourcefire_3D_Device_Virtual64_VMware-VI-X.X.X-xxx.ovf`

- 其中，*X.X.X-xxx* 是要上载的 OVF 包的版本和内部版本号。

步骤 4　输入 OVF 包的名称，或者也可输入其描述。

步骤 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。

步骤 6　点击 **Upload**，将作为 vApp 模板的 OVF 包上载到目录。

OVF 包会上载到企业目录。

步骤 7　继续按照使用 vApp 模板中所述从 vApp 模板创建虚拟设备。

使用 vApp 模板

在使用设置向导安装过程中，可使用 vApp 模板创建虚拟设备，这允许您配置 FireSIGHT 系统所需的设置。在向导的每个页面指定设置后，点击 **Next** 继续。为方便起见，向导的最后一个页面允许您在完成操作步骤之前确认设置。

要使用 vApp 模板创建虚拟设备，请执行以下操作：

步骤 1　在 VMware vCloud Director 网络门户上，选择 **My Cloud > vApps**。

步骤 2　在 vApps 媒体选项卡中，点击 Add 图标 ( )，从此目录添加 vApp。

系统将显示 Add vApp from Catalog 弹出窗口。

步骤 3　在模板菜单栏上点击 **All Templates**。

系统将显示可用的 vApp 模板列表。

步骤 4　选择要添加以显示虚拟设备描述的 vApp 模板。

- 对于虚拟防御中心：

  `Sourcefire_Defense_Center_Virtual64_VMware-VI-X.X.X-xxx.ovf`

- 对于虚拟设备：

  `Sourcefire_3D_Device_Virtual64_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。

系统将显示最终用户许可协议 (EULA)。

步骤 5　阅读并接受 EULA。

系统将显示此 vApp 屏幕的名称。

步骤 6　输入 vApp 的名称，也可以可选择地输入其描述。

系统将显示 Configure Resources 屏幕。

步骤 7　在 Configure Resources 屏幕上，选择虚拟数据中心，输入计算机名称 （或使用默认计算机名称），然后选择存储配置文件。

系统将显示 Network Mapping 屏幕。

步骤 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。

系统将显示 Custom Properties 屏幕。

步骤 9　或者，在 Custom Properties 屏幕，通过在设置向导中输入 FireSIGHT 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，可以按照设置虚拟设备，第 4-1 页中的说明稍后执行。

系统将显示 Ready to Complete 屏幕，该屏幕显示虚拟设备的配置。

步骤 10　确认设置并点击 **Finish**。

注　请勿启用虚拟设备的 **Power on after deployment** 选项。必须映射感应接口，并确它们在启动设备之前已设置连接。有关详细信息，请参阅初始化虚拟设备，第 4-2 页。

步骤 11　继续安装后更新重要设置，第 3-8 页中的内容。

使用 vSphere 客户端安装

可以使用 vSphere 客户端，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 FireSIGHT 系统 所需的设置。

在向导的每个页面指定设置后，点击 **Next** 继续。为方便起见，向导的最后一个页面允许您在完成操作步骤之前确认设置。

要使用 vSphere 客户端 安装虚拟设备，请执行以下操作：

步骤 1　使用 vSphere 客户端，通过点击 **File > Deploy OVF Template** 部署以前下载的 OVF 模板文件。

系统将显示 Source 屏幕，在该屏幕中，可浏览要部署的模板的下拉列表。

步骤 2　从下拉列表中，选择要部署的 OVF 模板：

- 对于虚拟防御中心：

```
Sourcefire_Defense_Center_Virtual64_VMware-VI-X.X.X-xxx.ovf
Sourcefire_Defense_Center_Virtual64_VMware-ESXi-X.X.X-xxx.ovf
```

- 对于虚拟设备：

```
Sourcefire_3D_Device_Virtual64_VMware-VI-X.X.X-xxx.ovf
Sourcefire_3D_Device_Virtual64_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。

系统将显示 OVF Template Details 屏幕。

步骤 3　确认已选择正确的虚拟机：

- 对于 ESXi OVF 模板：

  系统将显示 Name and Location 屏幕。
- 对于 VI OVF 模板：

  系统将显示 End User License Agreement (EULA) 屏幕。

  阅读并接受 EULA，然后系统将显示 Name and Location 屏幕。

步骤 4　在文本字段中键入虚拟设备的名称，然后选择要部署设备的库存库位。

系统将显示 Host/Cluster 屏幕。

步骤 5　选择要部署模板的主机和集群。

系统将显示 Specific Host 屏幕。

步骤 6　选择要部署模板的集群中的特定主机。

系统将显示 Storage 屏幕。

步骤 7　选择虚拟机的目标存储

系统将显示 Disk Format 页面。

步骤 8　从以下选项中选择要存储虚拟磁盘的格式：

- 密集配置延迟置零
- 密集配置快速归零
- 精简置备

系统将显示 Network Mapping 屏幕。

步骤 9　选择要部署模板的网络：

- 对于 ESXi OVF 模板：

  系统将显示 ESXi Finish 屏幕。
- 对于 VI OVF 模板：

  系统将显示 Properties 屏幕。

  输入 FireSIGHT 系统所需的设备设置，或稍后点击完成设置，确认设置，然后点击 **Finish**。

注　请勿启用虚拟设备的 **Power on after deployment** 选项。必须映射感应接口，并确它们在启动设备之前已设置连接。有关详细信息，请参阅初始化虚拟设备，第 4-2 页。

步骤 10　完成安装后，关闭状态窗口。

步骤 11　继续安装后更新重要设置中的内容。

安装后更新重要设置

安装虚拟设备后，必须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 3-2　　虚拟设备默认设置

设置	默认	设置可调节？
内存	4 GB	是，对于虚拟设备，您必须分配： • 最少 4 GB • 5 GB，用于添加基于类别和信誉的 URL 过滤 • 6 GB，用于使用大型动态源添加安全情报过滤 • 7 GB，用于添加 URL 过滤和安全情报
虚拟 CPU	4	是，最多 8 个
硬盘配置大小	40 GB （设备） 250 GB （防御中心）	否

以下步骤说明了如何检查和调整虚拟设备的硬件和内存设置。

要检查虚拟设备设置，请执行以下操作：

步骤 1　右键单击新虚拟设备名称，然后从上下文菜单中选择 **Edit Settings**，或从主窗口的 **Getting Started** 选项卡中点击 **Edit virtual machine settings**。

系统将显示 Virtual Machine Properties 弹出窗口，显示 Hardware 选项卡。

步骤 2　确保 **Memory**、**CPUs** 和 **Hard disk 1** 的设置不低于默认设置，如表 3-2虚拟设备默认设置，第 3-8 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 **Provisioned Size**，点击 **Hard disk 1**。

步骤 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。

步骤 4　确认 **Network adapter 1** 设置如下，必要时执行更改：

- 在 **evice Status** 下，启用 **Connect at power on** 复选框。
- 在 **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，对于虚拟防御中心，如果已重新映像虚拟设备，手动设置其 MAC 可确保不需要再次向思科申请许可证。
- 在 **Network Connection** 下，将 **Network label** 设置为虚拟设备管理网络的名称。

步骤 5　点击 **OK**。

更改保存成功。

步骤 6　下一步取决于已安装的设备类型。

- 虚拟防御中心已准备好初始化：继续设置虚拟设备，第 4-1 页中的内容。
- 虚拟设备需要一些其他配置：继续配置虚拟设备接口中的内容。

配置虚拟设备接口

虚拟设备上的接口必须具有接受混杂模式的 ESXi 主机虚拟交换机上端口的网络连接。

提示　将端口组添加到虚拟交换机，以将混杂模式虚拟网络连接与生产流量隔离。有关添加端口组和设置安全属性的信息，请参阅 VMware 文档。

要允许混杂模式，请执行以下操作：

步骤 1　使用 vSphere 客户端 登录到服务器并点击服务器的 **Configuration** 选项卡。

系统将显示 **Hardware** 和 **Software** 选择列表。

步骤 2　在 **Hardware** 列表中，点击 **Networking**。

系统将显示虚拟交换机图。

步骤 3　在连接虚拟设备的感应接口的交换机和端口组中，点击 **Properties**。

系统将显示 **Switch Properties** 弹出窗口。

步骤 4　在 **Switch Properties** 弹出窗口中，点击 **Edit**。

系统将显示 **Detailed Properties** 弹出窗口。

步骤 5　在 **Detailed Properties** 弹出窗口中，请选择 **Security** 选项卡。

在 **Policy Exceptions > Promiscuous Mode** 下，请确认 Promiscuous Mode 已设置为 **Accept**。

提示　要监控虚拟环境中的 VLAN 流量，请将混杂端口的 VLAN ID 设置为 4095。

步骤 6　保存更改。

设备已准备好初始化。

步骤 7　继续下一章，设置虚拟设备，第 4-1 页。

卸载虚拟设备

可能需要卸载或移除虚拟设备。关闭虚拟设备，然后通过将其删除而卸载。

提示　在移除虚拟设备后，请谨记将传感器连接虚拟交换机端口组返回到默认设置：**Promiscuous Mode**：**Reject**。有关详细信息，请参阅配置虚拟设备接口，第 3-9 页。

关闭虚拟设备

使用以下步骤正确关闭虚拟设备。

要关闭虚拟设备，请执行以下操作：

步骤 1　在 VMware 控制台上，以管理员（或，对于虚拟设备， CLI 配置）权限的用户身份登录。如果使用虚拟设备，键入 `expert` 显示外壳提示符。

系统将显示设备提示。

步骤 2　关闭虚拟设备：

- 在虚拟防御中心中，键入 `sudo shutdown -h now`。
- 在虚拟设备上，键入 `system shutdown`。

虚拟设备关闭。

删除虚拟设备

在虚拟设备关闭后，可以删除虚拟设备。

使用以下步骤删除在 VMware vCloud Director 上部署的虚拟设备：

要使用 VMware vCloud Director 网络门户删除虚拟设备，请执行以下操作：

步骤 1　选择 **My Cloud > vApps**，右键单击要删除 vApp，从菜单中点击 **Delete**，然后点击确认弹出窗口中的 **Yes**。

虚拟设备已卸载。

使用以下步骤删除在 VMware vCenter 上部署的虚拟设备：

要使用 vSphere 客户端 删除虚拟设备，请执行以下操作：

步骤 1　点击 vSphere 客户端上下文菜单中的设备名称，使用 Inventory 菜单点击 **Delete**，然后点击确认对话框中的 **Yes**。

虚拟设备已卸载。

设置虚拟设备

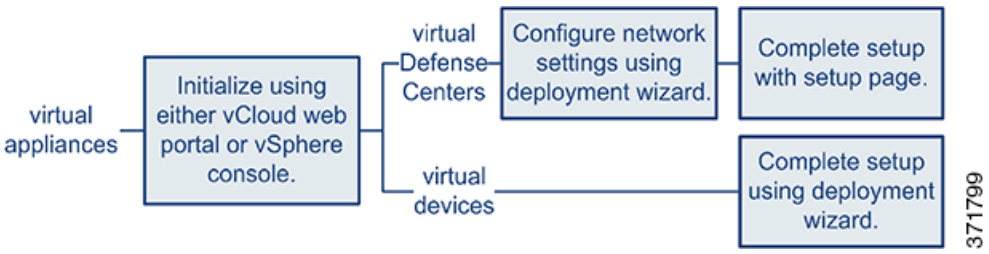
在安装虚拟设备后，必须完成允许新设备在信任的管理网络上通信的设置过程。还必须更改管理员密码并接受最终用户许可协议 (EULA)。

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。无论最初如何配置设备，都可以随时使用防御中心更改其配置。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。

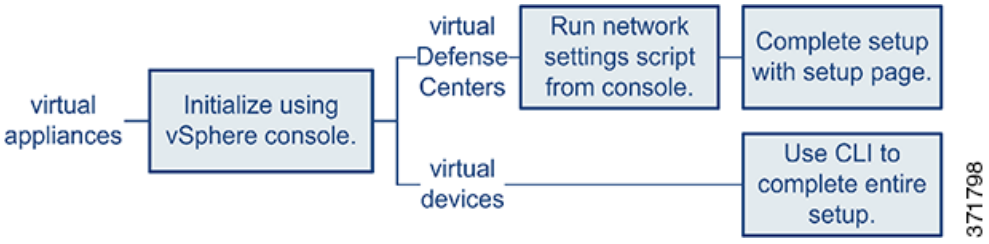
VI OVF 模板部署

以下图表显示在使用 VI OVF 模板部署时，设置虚拟防御中心和受管设备的一般过程。



ESXi OVF 模板部署

以下图表显示在使用 ESXi OVF 模板部署时，设置虚拟防御中心和受管设备的一般过程。



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：

虚拟设备

不具有网络界面的虚拟设备。如果使用 VI OVF 模板部署，可执行设备的初始设置，包括使用部署向导在防御中心上注册。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。

虚拟防御中心

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，以浏览防御中心的网络界面。

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

有关详细信息，请参阅：

- 初始化虚拟设备，第 4-2 页
- 使用 CLI 设置虚拟设备，第 4-3 页
- 设置虚拟防御中心，第 4-6 页
- 后续步骤，第 4-10 页

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。

注意事项 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：

要初始化虚拟设备，请执行以下操作:

步骤 1 启动设备：

- 在 VMware vCloud Director 网络门户，请从显示内容中选择 vApp，然后点击 **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 **Power > Power On**。

步骤 2 监控 VMware 控制台标签上的初始化。

在该过程的两个最长的部分，系统会显示消息。在过程结束后，系统将显示登录提示。

下一步取决于设备类型和部署。

如果在部署过程中使用了 VI OVF 模板并配置了 FireSIGHT 系统所需的设置：

- 对于虚拟防御中心，请继续使用设置虚拟防御中心，第 4-6 页完成设置。
- 对于虚拟设备，不需要其他配置。

如果使用了 OVF ESXi 模板或在使用 VI OVF 模板部署时没有配置 FireSIGHT 系统所需的设置：

- 对于虚拟防御中心，继续设置虚拟防御中心，第 4-6 页，以通过使用脚本配置网络设置来设置虚拟防御中心。
- 对于虚拟设备，继续使用 CLI 设置虚拟设备，第 4-3 页，以使用 CLI 设置虚拟设备。

使用 CLI 设置虚拟设备

因为虚拟设备没有网络界面，如果使用 ESXi OVF 模板部署，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 FireSIGHT 系统所需的设置。

提示 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。

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。详细信息，请参阅 《*FireSIGHT 系统安装指南*》。

提示 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 《*FireSIGHT 系统用户指南*》中的“命令行参考”一章。

了解设备的网络设置

FireSIGHT 系统提供 IPv4 和 IPv6 管理环境的双堆栈实施。必须设置 IPv4 或 IPv6 管理 IP 地址、网络掩码或前缀长度和默认网关。还可以指定多达三个 DNS 服务器，以及设备主机名和域。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。

被动

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 尽管在 IPS 部署的通常的做法是失效打开且允许不匹配的流量，但虚拟设备上的内联集缺乏旁路功能。

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的检测模式创建的接口、内联集和区域。

表 4-1　　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
网络发现	被动	无	分配给被动区域的第一对

请注意，安全区域是将设备实际添加防御中心到后，系统创建的防御中心级的配置。此时，如果防御中心上已存在合适的区域（内部，外部或被动），系统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《*FireSIGHT 系统用户指南*》。

要使用 CLI 设置虚拟设备，请执行以下操作：

访问：管理员

步骤 1　使用管理员作为用户名和部署设置向导中指定的新管理员帐户密码，登录 VMware 控制台上的虚拟设备。

如果使用向导更改密码，或者正在使用 OVF ESXi 模板部署，请使用思科作为密码。

设备立即提示您阅读 EULA。

步骤 2　阅读并接受 EULA。

步骤 3　更改管理员帐户的密码。此帐户为 Configuration CLI 访问级别的帐户，无法删除。

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。

步骤 4　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。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`。

在进行设置时， VMware 控制台可能会显示消息。

步骤 5　根据设备的部署方式指定检测模式。

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防御中心，并显示 CLI 提示。

步骤 6　要使用 CLI 将设备注册至管理设备的防御中心，请继续下一节，将虚拟设备注册至防御中心，第 4-5 页。

您必须通过防御中心管理设备。如果设备目前尚未注册，您必须稍后登录并注册设备，才可将其添加到防御中心。

将虚拟设备注册至防御中心

因为虚拟设备没有网络界面，所以必须使用 CLI 将虚拟设备注册至防御中心（可是物理的，也可是虚拟的）。因为在初始设置过程中已登录设备的 CLI，所以在此过程中向防御中心注册设备最容易。

要注册设备，请使用 `configure manager add` 命令。向防御中心注册设备，始终需要唯一的自身生成的字母数字注册密钥。这是指定的简单密钥，并不等同于许可证密钥。

在大多数情况下，必须同时提供注册密钥以及防御中心的 IP 地址，例如：

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

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

注　在使用 vSphere 客户端向防御中心注册虚拟设备时，必须使用管理防御中心的 IP 地址（而非主机名）。

但是，如果设备和防御中心被网络地址转换 (NAT) 设备分隔，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。

要将虚拟设备注册到防御中心，请执行以下操作：

访问：CLI 配置

步骤 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，那么已经以管理员用户身份登录，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。

步骤 2　在提示符处，使用 `configure manager add` 命令将设备注册至防御中心，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} 指定防御中心的 IP 地址。如果防御中心不可直接寻址，则使用 DONTRESOLVE。
- *reg_key* 是将设备注册到防御中心所需的唯一字母数字注册密钥。
- *nat_id* 是在防御中心与设备之间的注册过程中使用的可选的字母数字字符串。如果主机名设置为 DONTRESOLVE，则此项为必填项。

步骤 3　从设备注销。

步骤 4　下一步取决于是否已设置了管理防御中心以及防御中心的型号：

- 如果已设置防御中心，登录其网络界面并使用 Device Management (**Devices > Device Management**) 页面添加设备。有关详细信息，请参阅《*FireSIGHT 系统用户指南*》中的“管理设备”一章。
- 如果尚未设置防御中心，对于虚拟 防御中心，请参阅设置虚拟防御中心，第 4-6 页，对于物理防御中心，请参阅《*FireSIGHT 系统安装指南*》。

设置虚拟防御中心

设置虚拟防御中心的所需步骤取决于是使用 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 FireSIGHT 系统所需的设置时设置的密码登录虚拟防御中心，然后使用 FireSIGHT 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 《*FireSIGHT 系统用户指南*》。
- 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 FireSIGHT 系统所需的设置，设置虚拟防御中心分为两个步骤。在初始化虚拟防御中心后，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 模板部署虚拟防御中心，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防御中心。有关详细信息，请参阅初始设置页面：虚拟防御中心，第 4-7 页。

有关详细信息，请参阅：

- 自动化虚拟防御中心网络设置，第 4-6 页
- 初始设置页面：虚拟防御中心，第 4-7 页

自动化虚拟防御中心网络设置

新的虚拟防御中心初始化以后，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。

FireSIGHT 系统提供 IPv4 和 IPv6 管理环境的双堆栈实施。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 确认选择。

要使用脚本配置防御中心的网络设置，请执行以下操作：

访问：管理员

步骤 1　在初始化过程完成后，使用 `admin` 作为用户名和使用 VI OVF 模板部署时在设置向导中指定的管理员帐户密码，在 VMware 控制台登录虚拟防御中心。

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

步骤 2　在管理员提示符下，运行以下脚本：

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

步骤 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。
- 输入冒号分隔的十六进制形式的 IPv6 地址。对于 IPv6 前缀，请指定位数；例如，前缀长度为 `112`。

步骤 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。

步骤 5　从设备注销。

步骤 6　使用防御中心的网络界面，继续执行初始设置页面：虚拟防御中心，第 4-7 页以完成设置。

初始设置页面：虚拟防御中心

对于虚拟防御中心，必须通过登录防御中心的网络界面并在设置页面上指定初始配置选项完成设置过程。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，并将防御中心添加为远程管理器，否则，注册将失败。

要使用其网络界面在防御中心上完成初始设置，请执行以下操作：

访问：管理员

步骤 1　在管理网络上的计算机中，请将受支持的浏览器定向到 `https://` *`DC_name`*`/`，其中 *`DC_name`* 是分配给上一步骤中的防御中心管理界面的主机名或 IP 地址。

系统将显示登录页面。

步骤 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，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 4-8 页
- 网络设置，第 4-8 页
- 时间设置，第 4-8 页
- 重复规则更新导入，第 4-8 页
- 重复地理位置更新，第 4-8 页
- 自动备份，第 4-9 页
- 许可证设置，第 4-9 页
- 设备注册，第 4-9 页
- 最终用户许可协议，第 4-10 页

步骤 3　完成设置后，点击 **Apply**。

防御中心已根据您的选择配置。在系统显示中间页面后，您已经以管理员 用户（具有管理员角色）身份登录网络界面。

步骤 4　使用 Task Status 页面 (**System > Monitoring > 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 **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，该防御中心可以使用了。有关配置部署的详细信息，请参阅《*FireSIGHT 系统用户指南*》。

步骤 5　继续后续步骤，第 4-10 页中的内容。

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

防御中心的网络设置允许该设备在管理网络上通信。因为已经使用脚本配置网络设置，可预填页面的此部分。

如果要更改预填的设置，请记住 FireSIGHT 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 **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) 设置防御中心的时间。

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

新漏洞出现后，思科漏洞研究团队 (VRT) 将发布入侵规则更新。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 **Enable Recurring Rule Update Imports**。

可以指定**导入频率**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**。要在初始配置过程中执行规则更新，请选择 **Install Now**。

注　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

可以使用虚拟防御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。

防御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 **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 **Install Now**。

注 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

防御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 **Enable Automatic Backups**。

启用该设置后，将创建一项定期任务，即对防御中心上的配置创建周备份。

许可证设置

您可以许可各种功能，为贵公司创建最佳的 FireSIGHT 系统部署。要求防御中心上有 FireSIGHT 的许可证，以执行主机、应用和用户发现。其他型号特定的许可证允许受管设备设备执行各种功能。由于架构和资源限制，并非所有的许可证都适用于所有受管设备；请参阅了解虚拟设备功能，第 1-3 页和许可虚拟设备，第 1-9 页。

思科建议使用初始设置页面来添加公司购买的许可证。如果目前没有添加许可证，在初始设置过程中注册的所有设备会以未许可的状态添加到 防御中心；必须在初始安装过程后单独许可每个设备。

提示 如果重新创建了虚拟防御中心并将管理界面的同一 MAC 地址用作已删除的设备，可以使用旧的许可证。如果不能使用同一 MAC 地址 （例如，通过动态分配），请联系支持人员获得新许可证。

如果尚未获取许可证，请点击链接，以导航到 https://keyserver.sourcefire.com/ 并按照屏幕说明执行操作。您需要许可证秘钥 （在初始设置页面上列出）以及以前通过邮件发送给与支持合同相关的联系人的激活秘钥。

通过将其粘贴到文本框，并点击 **Submit License** 添加许可证。添加有效许可证后，页面将更新。您可以跟踪已添加的许可证。一次添加一个许可证。

设备注册

虚拟防御中心可将任何设备 （物理或虚拟），目前由 FireSIGHT 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防御中心。但是，如果设备和防御中心由一台 NAT 设备隔开，您必须在设置过程完成后进行添加。

在注册设备时，如果注册后，需要将访问控制策略应用于设备，请启用 **Apply Default Access Control Policies** 复选框。请注意，您无法选择防御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 4-2　　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
内联	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，即您以前使用防御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，此新防御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，防御中心将应用默认入侵防御策略，否则，防御中心将应用默认访问控制策略。

有关虚拟设备的检测模式的详细信息，请参阅使用 CLI 设置虚拟设备，第 4-3 页；关于物理设备，请参阅 《*FireSIGHT 系统安装指南*》。

要添加设备，请键入在设备注册时指定的 **Hostname** 或 **IP Address**，以及 **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，只可选择已添加到防御中心的许可证。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，无法在设备上启用控制。

由于架构和资源的限制，并非所有许可证都可应用于所有受管设备。然而，设置页面**不会**阻止您在受管设备上启用不支持的许可证，或者启用没有相应型号特定许可证的功能。这是因为防御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。有关详细信息，请参阅了解虚拟设备功能，第 1-3 页和许可虚拟设备，第 1-9 页。

注　如果您已启用 **Apply Default Access Control Policies**，则必须在已选择 **Inline** 或 **Passive** 检测模式的设备上启用保护许可证。此外，还必须在拥有已配置接口的任何以前受管设备上启用保护许可证。否则，默认策略 （在这些情况下需要保护）将无法应用。

启用许可证后，点击 **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 **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 **Apply**。

防御中心会根据您的选择进行配置。在系统显示中间页面后，您已经以管理员 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：虚拟防御中心，第 4-7 页中的第3步，以完成防御中心的初始设置。

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 《*FireSIGHT 系统用户指南*》。

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。这点对于防御中心来说尤其重要，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。思科建议您使用防御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，防御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。思科建议您使用防御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 FireSIGHT 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。

注意事项　更新 FireSIGHT 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。

虚拟设备部署故障排除

本章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。不可将受管设备（虚拟或物理设备）同步至虚拟防御中心。为确保时间同步设置正确，请参阅《FireSIGHT 系统*用户指南*》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 1-6 页。要监控 ESXi 主机性能，您可以利用 vSphere 客户端和 **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：

步骤 1　选择 **My Cloud > VMs**，将鼠标停留在待查看的虚拟设备上并右键单击。

系统将显示 Actions 窗口。

步骤 2　在 Actions 窗口中，点击 **Properties**。

系统将显示 Virtual Machine Properties 窗口。

步骤 3　在 **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：

步骤 1　右键单击 vSphere 客户端中虚拟设备的名称，从上下文菜单中选择 **Edit Settings**。在 **Hardware** 列表中，选择 **Network adapter 1**，并确保 **Connect at power on** 复选框已选择。

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：

步骤 1　右键单击 vSphere 客户端中虚拟设备的名称，从上下文菜单中选择 **Edit Settings**。在 **Hardware** 列表中，选择 **Network adapter 2** 和 **Network adapter 3**。确保已为使用中的各适配器选择 **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。有关如何确保感应接口能检测所有漏洞，请参阅配置虚拟设备接口，第 3-9 页。

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：

访问：CLI 配置

步骤 1　在控制台中，作为具有 CLI 配置 （管理员）权限的用户登录。

系统将显示 CLI 提示符。

步骤 2　键入 `Expert`，系统将显示外壳提示符。

步骤 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。

步骤 4　从虚拟设备注销。

步骤 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。

Sourcefire 技术支持部门

如果您有任何关于 FireSIGHT 虚拟设备或虚拟防御中心的疑问或需要帮助，请通过以下方式与 Sourcefire 技术支持部门联系：

- 访问 Sourcefire 技术支持部门网站：https://support.sourcefire.com/。
- 将问题发送至 Sourcefire 技术支持部门的邮箱：support@sourcefire.com。
- 通过电话联系 Sourcefire 技术支持部门：1.410.423.1901 或 1.800.917.4134。

思科技术支持部门

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。
- 将问题发送至思科技术支持部门的邮箱：tac@cisco.com。
- 通过电话联系思科技术支持部门：1.408.526.7209 or 1.800.553.2447。