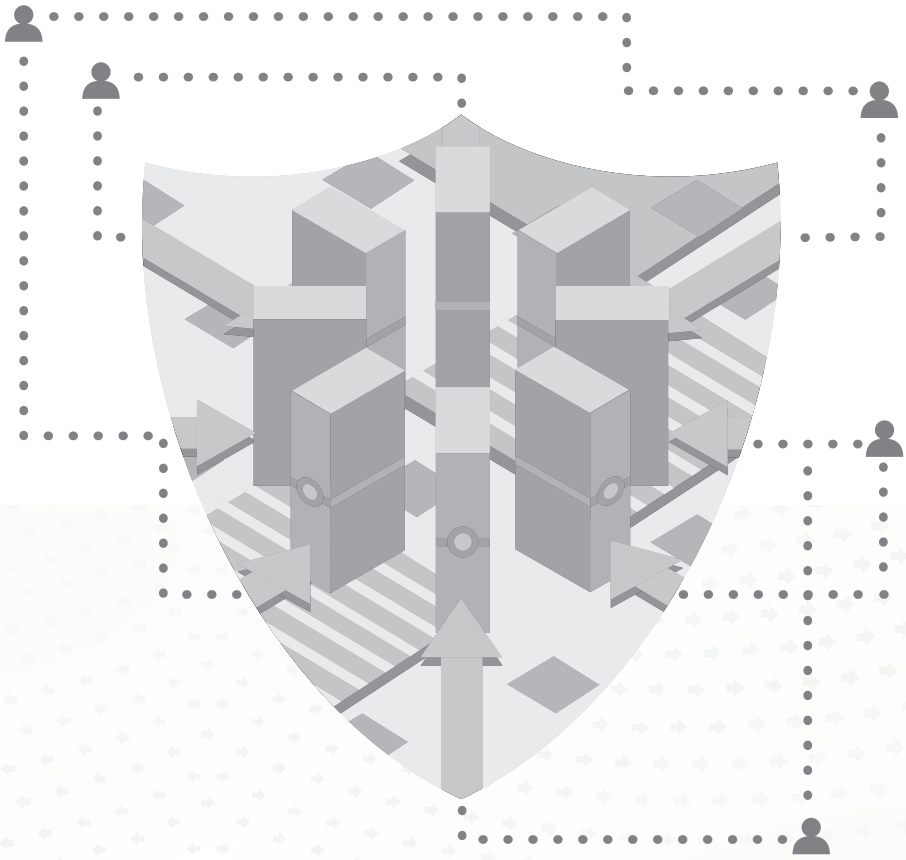
Sourcefire 3D 系统

虚拟安装指南

5.3 版本



SOURCEfire®

Sourcefire is now part of Cisco. CISCO

法律声明

免责声明

文档和文档中的任何可用信息可能包括不精确之处或排版错误。思科可能随时更改本文档。对于思科控制的任何网站、文档和/或任何产品信息的准确性或适用性，思科不做任何表示或保证。思科控制的网站、文档和所有产品信息都“按原样”提供，并且思科不承担任何及所有明示和暗示的保证，包括但不限于权利保证以及适销性和/或特定用途适用性的暗示保证。对于思科控制的网站或文档所引起或以任何与思科控制的网站或文档相关的方式产生的直接、间接、偶然、特殊、惩戒性、惩罚性或必然损害 （包括但不限于替代产品或服务的采购、数据丢失、利润损失和/或业务中断），无论是何种原因引起和/或是否基于合同、严格责任、疏忽或其他侵权行为或者任何其他责任理论，思科在任何情况下概不负责，即使思科已被告知存在此类损害的可能性也一样。由于某些州/司法管辖区不允许排除或限制必然或偶然损害责任，因此上述限制可能不适用。

2015 年 2 月 17 日 13:59

目录

目录

目录

第 1 章
虚拟设备简介

Sourcefire 3D® 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。

Sourcefire 封装了适用于 VMwareESXi 和 VMware vCloud Director 托管环境的 64 位虚拟防御中心® 和虚拟设备。防御中心为系统提供了一个集中的管理控制台和数据库资源库。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和用于 X 系列的 Sourcefire 软件，物理防御中心可以管理虚拟设备。然而，虚拟设备不支持系统基于硬件的任何系统，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 Sourcefire 设备的详细信息，请参阅 《*Sourcefire 3D 系统安装指南*》。

本安装指南提供关于部署、安装和设置虚拟 Sourcefire 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 门户网站）的功能和术语定义。

以下主题将为您介绍 Sourcefire 3D 系统虚拟设备：

Sourcefire 3D 系统虚拟设备

Sourcefire *虚拟设备*可以是流量感应受管*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 Sourcefire 3D 系统部署提供了一个集中的管理点和事件数据库。虚拟防御中心汇聚并关联入侵、文件、恶意软件、发现、连接和性能数据。借助此功能，您可以监控设备相互报告的信息，并评估和控制网络中发生的总体活动。

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
- 使用关联和补救功能进行实时威胁响应
- 报告

虚拟受管设备

被动部署的虚拟 Sourcefire 可帮助您深入了解您的网络流量。采用内联部署时，您可以使用虚拟设备基于多重标准来影响流量。

虚拟设备可以收集有关公司主机、操作系统、应用、用户、网络和漏洞的详细信息。通过其他许可的功能，虚拟设备可以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。

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止分析能力。然而，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。

Sourcefire 3D 系统简介章中的第 18 页的不同设备型号支持的功能列出了 Sourcefire 3D 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，请参阅第 20 页的 Sourcefire 3D 系统组件和第 10 页的许可 Sourcefire 虚拟设备。

操作环境先决条件

您可以在以下托管环境中托管 64 位 Sourcefire 虚拟设备：

- VMware vSphere 虚拟机监控程序 5.1
- VMware vSphere 虚拟机监控程序 5.0
- VMware vCloud Director 5.1

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。

Sourcefire 虚拟设备使用开放虚拟化格式 (OVF) 封装。 VMware 工作站、播放器、服务器和 Fusion 不识别 OVF 包装并且不受支持。此外， Sourcefire 虚拟设备被封装成带虚拟硬件第 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）兼容的网络接口，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，**不得**降低。然而，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。

默认虚拟设备设置

设置	默认	设置是否支持调整
内存	4 GB	支持，对于一台虚拟设备，您**必须**分配： • 4 GB （最低） • 5 GB，用于使用基于类别和信誉的 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	支持，最多可增至 8 个
硬盘有效容量	40 GB （设备） 250 GB (防御中心)	不支持

虚拟设备性能

无法准确预测虚拟设备吞吐量和处理能力。一些因素会在很大程度上影响性能，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，调整分配至共用 ESXi 主机的虚拟设备的资源。

尽管 Sourcefire 不支持在访客层安装工具 （包括 VMware 工具），但您可以将工具 （例如 `esxtop` 或 VMware/第三方插件）安装在 ESXi 主机上，检查虚拟性能。然而，您必须将这些工具安装在此主机或虚拟化管理层上，而不是访客层上。

许可 Sourcefire 虚拟设备

您可以许可各种功能，为贵公司创建最佳的 Sourcefire 3D 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。

Sourcefire 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，初始设置过程中所注册的所有设备均被作为未许可设备被添加至防御中心。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，请参阅第 57 页的设置虚拟设备。

购买防御中心时随附一个 FireSIGHT 许可证，执行主机、应用和用户发现时要使用该许可证。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。

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 （如切换或路由），但虚拟防御中心可管理物理设备上的此类功能。控制许可证必须包含保护许可证。

URL 过滤

URL 过滤许可证允许虚拟设备使用定期的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 过滤许可证必须包含保护许可证。

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。恶意软件许可证必须包含保护许可证。

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 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 许可证必须包含保护和控制许可证。

由于架构和资源的限制，并非所有的许可证都可被应用至所有受管设备。一般而言，您无法许可设备不支持的功能；请参阅第 8 页的了解虚拟设备功能。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。此外，空白单元格表示许可不被支持，而不适用表示与受管设备无关并基于防御中心的许可证。

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	不支持	不支持	不支持	不支持
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	不支持硬件功能	支持	支持	不支持
用于 X 系列的 Sourcefire 软件	不适用	支持	不支持硬件功能	支持	支持	不支持
DC500 2 系列防御中心	支持	无安全情报	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 《*Sourcefire 3D 系统用户指南*》中的“许可 Sourcefire 3D 系统”章节。

后续操作

有关使用 Sourcefire 3D 系统部署、安装和管理虚拟设备的详细信息，请参阅下列各章：

- 有关 Sourcefire 3D 系统的详细信息，请参阅第 13 页的 Sourcefire 3D 系统简介
- 有关将虚拟化添加至被动和内联部署的详细信息，请参阅第 38 页的部署虚拟设备
- 有关使用 VMware vCloud Director 网络门户和 vSphere 客户端进行安装的详细信息，请参阅第 44 页的安装虚拟设备
- 有关初始化和设置虚拟设备和防御中心的详细信息，请参阅第 57 页的设置虚拟设备
- 有关常见设置问题的详细信息，例如时间同步、性能问题、管理连接、感应接口和内联接口配置，请参阅第 74 页的虚拟设备部署故障排除

第 2 章
SOURCEFIRE 3D 系统简介

Sourcefire 3D® 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。 Sourcefire 设备也可以用于交换式、路由式或混合式（交换路由式）的环境中，执行网络地址转换 (NAT) 以及在 Sourcefire 受管设备的虚拟路由器之间建立安全的虚拟专用网络 (VPN) 隧道。

Sourcefire 防御中心® 为 Sourcefire 3D 系统提供了一个集中管理控制台和数据库资源库。安装于各网段上的受管设备对流量进行监控，以便进行分析。

被动部署中的设备使用交换机 SPAN、虚拟交换机或镜像端口等方式监控通过网络的流量。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。内联接口无条件地接收所有流量，并且这些接口上接收的流量都会被重新传输，除非部署中的某些配置明确放弃这些流量。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。

除了物理设备之外，您还可以部署下列基于软件的 Sourcefire 设备：

- 适用于 VMware ESXi 和 VMware VMware vCloud Director 托管环境的 64 位虚拟防御中心®
- 使用同一 VMware 环境以及在 Crossbeam 平台上托管用于 X 系列的 Sourcefire 软件的 64 位虚拟设备

本指南提供关于 Sourcefire 3D 系统特性和功能的信息。每章里的说明文本、图形和操作步骤提供了详尽的信息，帮助您导航用户界面，使系统性能得到最大程度地发挥，并提供疑难解答。

第 2 章

以下主题将介绍 Sourcefire 3D 系统，描述其主要组件，解释如何登录和注销 Sourcefire 设备，提供一些有关使用系统网络界面的基础信息，以及帮助您了解如何使用本指南：

Sourcefire 3D 系统设备

Sourcefire *设备*可以是流量感应受管*设备*，也可以是管理型*防御中心*。

物理设备是指拥有多种吞吐量和多项功能的容错专用网络设备。防御中心可用作这些设备的集中管理点，自动汇聚并关联这些设备生成的事件。每个物理设备类型都有若干*型号*；这些型号可进一步划分为*多个产品系列和子系列*。

您也可以将 64 位虚拟防御中心和设备托管至 Vmware ESXi 和 VMware vCloud Director 托管环境。虚拟防御中心可以管理物理设备，物理防御中心可以管理虚拟设备。除此以外，您可以将用于 X 系列的 Sourcefire 软件托管至 Crossbeam 平台。

Sourcefire 3D 系统的许多功能都取决于设备。有关详细信息，请参阅以下各节：

防御中心

防御中心为 Sourcefire 3D 系统部署提供了一个集中的管理点和事件数据库。防御中心（可以是物理的或虚拟的）汇聚并关联入侵、文件、恶意软件、发现、连接和性能数据，同时评估事件对特定主机的影响并用危害表现标记主机。借助此功能，您可以监控设备相互报告的信息，并评估和控制网络中发生的总体活动。

防御中心的主要功能包括：

- 设备、许可证和策略管理
- 表、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
- 外部通知和告警
- 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

对于很多物理防御中心，高可用性 （冗余）功能有助于确保运行的连续性。

受管设备

物理 Sourcefire 设备是指拥有多种吞吐量的容错专用网络设备。您还可以托管虚拟设备或用于 X 系列的 Sourcefire 软件。被动部署的设备可帮助您深入了解您的网络流量。采用内联部署时，您可以使用 Sourcefire 基于多重标准来影响流量。必须用防御中心管理 Sourcefire 设备。

根据型号和许可证，受管设备可以：

- 收集有关公司主机、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。
- 具有交换、路由、DHCP、NAT 和 VPN 功能以及可配置的旁路接口、快速路径规则和严格的 TCP 实施
- 具有集群 （冗余）功能以帮助确保运行的连续性，并且具有堆栈功能以整合多个设备的资源

了解设备系列、型号和功能

Sourcefire 3D 系统的 5.3 版本在两个系列的物理设备、虚拟设备和用于 X 系列的 Sourcefire 软件上可以提供。 Sourcefire 3D 系统的许多功能都取决于设备。有关详细信息，请参阅：

- 第 16 页的 2 系列设备
- 第 16 页的 3 系列设备
- 第 16 页的虚拟设备
- 第 16 页的用于 X 系列的 Sourcefire 软件
- 第 17 页的 5.3 版本随附设备
- 第 18 页的不同设备型号支持的功能

2 系列设备

2 系列 是 Sourcefire 物理设备的第二个系列。由于资源和架构的限制，2 系列设备只支持有限的 Sourcefire 3D 系统功能。

尽管 Sourcefire 不再提供新的 2 系列设备，但您可以将 2 系列设备和防御中心重新映像至 5.3 版本。重新映像将导致设备上的**全部**配置和事件数据丢失。有关详细信息，请参阅 《*Sourcefire 3D 系统安装指南*》。

警告！ 此外，您可以将特定的配置和事件数据从 4.10.3 版本防御中心或 3D 传感器迁移至 5.2 版本防御中心，然后升级至 5.3 版本。有关详细信息，请参阅适用于 5.2 版本的 《*Sourcefire 3D 系统迁移指南*》。

运行 5.3 版本时， 2 系列设备自动将大多数功能与保护许可证相关联：入侵检测和防御、文件控制以及基本访问控制。然而， 2 系列设备不能执行安全情报过滤、高级访问控制或高级恶意软件防护。您也无法在 2 系列设备上启用其他许可的功能。除了 3D9900 支持快速路径规则、堆栈和分路模式，2 系列设备不支持任何与 3 系列设备关联的基于硬件的功能：交换、路由、 NAT 等等。

运行 5.3 版本时， DC1000 和 DC3000 等 2 系列防御中心支持 Sourcefire 3D 系统的所有功能；DC500 更多功能被限制。

3 系列设备

3 系列是 Sourcefire 物理设备的第三个系列。所有 7000 系列和 8000 系列设备都属于 3 系列设备。 8000 系列设备功能更强大，且支持 7000 系列设备不支持的一些功能。

虚拟设备

您可以将 64 位虚拟防御中心托管至 VMware ESXi 和 VMware vCloud Director 托管环境。虚拟防御中心可以管理多达 25 个物理或虚拟设备；物理防御中心可以管理虚拟设备。

无论安装和应用了何种许可证，虚拟设备都不支持任何基于硬件的系统功能：冗余和资源共享、交换、路由等等。此外，虚拟设备没有网络界面。

用于 X 系列的 Sourcefire 软件

您可以将基于软件的用于 X 系列的 Sourcefire 软件托管至与虚拟设备具有类似功能的 Crossbeam 平台。与虚拟设备一样，用于 X 系列的 Sourcefire 软件没有网络界面。

无论安装和应用了何种许可证，用于 X 系列的 Sourcefire 软件都不支持任何基于硬件的功能，例如冗余和资源共享、堆栈、集群、交换、路由、 VPN 或 NAT。

尽管您不能使用 Sourcefire 3D 系统配置冗余，但您可以在安装用于 X 系列的 Sourcefire 软件软件包时配置冗余。有关详细信息，请参阅 《*用于 X 系列的 Sourcefire 软件安装指南*》。

5.3 版本随附设备

下表列出了 Sourcefire 随 Sourcefire 3D 系统的 5.3 版本一起交付的设备。

5.3 版本 Sourcefire 设备

型号/子系列	系列	类型
70xx 子系列： • 3D7010/7020/7030	3 系列 （7000 系列）	设备
71xx 子系列： • 3D7110/7120 • 3D7115/7125 • AMP7150	3 系列 （7000 系列）	设备
81xx 子系列： • 3D8120/8130/8140 • AMP8150	3 系列 （8000 系列）	设备
82xx 子系列： • 3D8250 • 3D8260/8270/8290	3 系列 （8000 系列）	设备
83xx 子系列： • 3D8350 • 3D8360/8370/8390	3 系列 （8000 系列）	设备
虚拟设备	不适用	设备
用于 X 系列的 Sourcefire 软件	不适用	设备
3 系列防御中心： • DC750/1500/3500	3 系列	防御中心
虚拟防御中心	不适用	防御中心

尽管 Sourcefire 不再提供新的 2 系列设备，但您可以将 2 系列设备和防御中心重新映像至 5.3 版本。重新映像将导致设备上的**全部**配置和事件数据丢失。有关详细信息，请参阅 《*Sourcefire 3D 系统安装指南*》。

此外，您可以将特定的配置和事件数据从 4.10.3 版防御中心或 3D 传感器迁移至 5.2 版防御中心，然后升级至 5.3 版。有关详细信息，请参阅适用于 5.2 版本的 《*Sourcefire 3D 系统迁移指南*》。有关获取指南和迁移脚本的详细信息，请联系 Sourcefire 技术支持部门。

不同设备型号支持的功能

Sourcefire 3D 系统的许多功能都取决于设备。下表将系统的主要功能与支持这些功能的设备一一对应 （假设您已安装并应用了正确的许可）。

相对应基于设备的功能 （例如，堆栈、交换和路由），防御中心列说明防御中心能否管理和配置设备，以执行设备的功能。例如，您可以使用 2 系列 DC1000 管理 3 系列设备上的 NAT。

不同设备型号支持的功能

功能	2 系列设备	2 系列防御中心	3 系列设备	3 系列防御中心	虚拟设备	虚拟防御中心	X 系列
网络发现：主机、应用和用户	支持	支持	支持	支持	支持	支持	支持
地理位置数据	支持	DC1000、DC3000	支持	支持	支持	支持	支持
入侵检测和防御 (IPS)	支持	支持	支持	支持	支持	支持	支持
安全情报过滤	不支持	DC1000、DC3000	支持	支持	支持	支持	支持
访问控制：基本网络控制	支持	支持	支持	支持	支持	支持	支持
访问控制：应用	不支持	支持	支持	支持	支持	支持	支持
访问控制：用户	不支持	DC1000、DC3000	支持	支持	支持	支持	支持
访问控制：文字 URL	不支持	支持	支持	支持	支持	支持	支持

不同设备型号支持的功能 （续）

功能	2 系列设备	2 系列防御中心	3 系列设备	3 系列防御中心	虚拟设备	虚拟防御中心	X 系列
访问控制：按类别和信誉进行的 URL 过滤	不支持	DC1000、DC3000	支持	支持	支持	支持	支持
文件控制：按文件类型	支持	支持	支持	支持	支持	支持	支持
基于网络的高级恶意软件防护 (AMP)	不支持	DC1000、DC3000	支持	支持	支持	支持	支持
FireAMP 集成	不适用	支持	不适用	支持	不适用	支持	不适用
快速路径规则	3D9900	支持	8000 系列	支持	不支持	支持	不支持
严格 TCP 实施	不支持	支持	支持	支持	不支持	支持	不支持
可配置旁路接口	支持	支持	硬件受限制的情况除外	支持	不支持	支持	不支持
分路模式	3D9900	支持	支持	支持	不支持	支持	不支持
交换和路由	不支持	支持	支持	支持	不支持	支持	不支持
NAT 策略	不支持	支持	支持	支持	不支持	支持	不支持
VPN	不支持	支持	支持	支持	不支持	支持	不支持
高可用性	不适用	DC1000、DC3000	不适用	DC1500、DC3500	不适用	不支持	不适用
设备堆叠	3D9900	支持	3D8140、82xx 系列、83xx 系列	支持	不支持	支持	不支持
设备集群	不支持	支持	支持	支持	不支持	支持	不支持

不同设备型号支持的功能 （续）

功能	2 系列设备	2 系列防御中心	3 系列设备	3 系列防御中心	虚拟设备	虚拟防御中心	X 系列
集群堆栈	不支持	支持	3D8140、82xx 系列、83xx 系列	支持	不支持	支持	不支持
恶意软件存储包	不支持	DC1000、DC3000	支持	支持	不支持	不支持	不支持
交互式 CLI	不支持	不支持	支持	不支持	支持	不支持	不支持

用于 X 系列的 Sourcefire 软件具备 Crossbeam 平台所特有的命令行界面，您可以在此配置冗余和/或负载平衡。有关详细信息，请参阅 《*用于 X 系列的 Sourcefire 软件安装指南*》。

Sourcefire 3D 系统组件

接下来的主题介绍 Sourcefire 3D 系统有利于公司安全的重要功能、可接受的使用策略和流量管理战略：

- 第 20 页的冗余和资源共享
- 第 21 页的网络流量管理
- 第 22 页的 FireSIGHT
- 第 22 页的访问控制
- 第 23 页的入侵检测和防御
- 第 23 页的文件跟踪、控制和恶意软件防护
- 第 24 页的应用编程接口

提示！ Sourcefire 3D 系统很多功能都取决于设备型号、许可证和用户角色。本文档包含有关每个功能要求使用哪些 Sourcefire 3D 系统许可证和设备以及哪些用户有权限完成各个操作步骤的详细信息。有关详细信息，请参阅第 29 页的文档约定 。

冗余和资源共享

可以通过 Sourcefire 3D 系统的冗余和资源共享功能确保运行的连续性并整合多个物理设备的处理资源。

防御中心高可用性

为确保运行的连续性，您可以通过防御中心*高可用性*功能指定冗余 DC1000、DC1500、 DC3000 或者 DC3500 防御中心来管理设备。事件数据从受管设备流式传输至两个防御中心；两个防御中心上都保留了某些配置元素。如果一个防御中心发生故障，您可以使用另一个防御中心继续不间断地监控网络。

设备堆栈

借助*设备堆栈*功能，您可以通过以堆栈配置的方式连接两至四台物理设备，以增加网段上检测的总流量。建立堆栈配置时，您将每个堆栈设备的资源合并至单一共享配置。

设备集群

借助*设备集群*（有时称为设备高可用性）功能，您可以在两个或多个 3 系列设备或堆栈之间建立网络功能和配置数据的冗余。集群两个或多个对等设备或堆栈可为策略应用、系统更新和注册建立单一的逻辑系统。通过设备集群，系统可以手动或自动进行故障转移。

在大多数情况下，您可以使用 Sourcefire 冗余协议 (SFRP) 实现第 3 层冗余，无需集群设备。 SFRP 允许设备作为指定的 IP 地址的冗余网关。通过网络冗余，您可以配置两台或多台设备或堆栈来提供相同的网络连接，确保网络上其他主机的连接。

用于 X 系列的 Sourcefire 软件冗余

尽管您无法使用 Sourcefire 3D 系统集群用于 X 系列的 Sourcefire 软件，但可以在安装用于 X 系列的 Sourcefire 软件文件包时配置冗余。有关详细信息，请参阅《*用于 X 系列的 Sourcefire 软件安装指南*》。

网络流量管理

通过 Sourcefire 3D 系统的网络流量管理功能，您可以将受管设备作为公司网络基础设施的一部分。可以配置 3 系列设备，使其可以用于交换式、路由式或混合式（交换路由式）环境；执行网络地址转换 (NAT)；以及构建安全的虚拟专用网络 (VPN) 隧道。

交换

您可以在第 2 层部署中配置 Sourcefire 3D 系统，使其在两个或多个网段之间提供数据包交换。在第 2 层部署中，配置受管设备上的交换接口和虚拟交换机，使其作为独立的广播域运行。虚拟交换机根据来自主机的 MAC 地址来确定发送数据包的目的地。

路由

在第 3 层部署中，您可以配置 Sourcefire 3D 系统，使其在两个或多个接口之间路由流量。在第 3 层部署中，将受管设备上的路由接口和虚拟路由器配置为可以接收和转发流量。系统根据目标 IP 地址制定数据包转发决策，以路由数据包。

路由器根据转发条件从传出接口获取目标位置，而访问控制规则指定要应用的安全策略。

配置虚拟路由器时，您可以定义静态路由器。此外，可以配置路由信息协议 (RIP) 和开放式最短路径优先 (OSPF) 动态路由协议。还可以配置静态路由与 RIP 或静态路由与 OSPF 的组合。可以为所配置的每个虚拟路由器设置 DHCP 中继。

如果在 Sourcefire 设备配置中同时使用虚拟交换机和虚拟路由器，您可以配置关联的混合接口，以桥接它们之间的流量。这些实用程序将分析流量，确定流量类型和适当的响应 （路由、交换或其他）。

NAT

在第 3 层部署中，您可以配置网络地址转换 (NAT)。从而允许从外部网络连接内部服务器，或允许内部主机或服务器连接外部应用。还可以使用 IP 地址块或使用被限制的 IP 地址块和端口转换，配置 NAT 隐藏来自外部网络的专用网络地址。

VPN

虚拟专用网络 (VPN) 是通过互联网或其他网络等公共资源，在终端之间建立安全隧道的一种网络连接。您可以配置 Sourcefire 3D 系统，在 3 系列设备的虚拟路由器之间建立安全的 VPN 隧道。

FireSIGHT

FireSIGHT™ 是 Sourcefire 研发的发现和感知技术，可以收集有关主机、操作系统、应用、用户、文件、网络、地理位置信息和漏洞的信息，以便让您全面了解网络。

您可以使用防御中心的网络界面查看和分析 FireSIGHT 收集的数据。还可以使用此数据来执行访问控制并修改入侵规则状态。此外，您还可以根据主机的关联事件数据，生成并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，可用于指定、检查和记录可以流经网络的流量。*访问控制策略*决定系统如何处理网络上的流量。您可以使用不包括*访问控制规则*的策略，通过以下任何一种方法，使用所谓的*默认操作*处理流量：

- 阻止所有流量进入网络
- 信任所有流量，所有流量无需进一步检查即可进入网络
- 允许所有流量进入网络，并只通过网络发现策略检查流量
- 允许所有流量进入网络，并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并入至访问控制策略，以进一步定义目标设备如何处理流量，包括从简单的 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，您都要指定一个规则*操作*，即是否信任、监控、阻止或检查与入侵或文件策略匹配的流量。

对于每个访问控制策略，可以创建一个自定义 HTML 页面，在系统阻止用户的 HTTP 请求时向用户显示此页面。或者，可以显示一个向用户发出警告并允许用户通过点击一个按钮继续访问初始请求站点的页面。

安全情报功能是访问控制的一部分。通过它，您可以将特定 IP 地址拉入黑名单，即在按访问控制规则对流量进行分析之前，拒绝这些地址之间的往来流量。如果系统支持地理定位，还可以根据其检测的来源和目标国家/地区与洲过滤流量。

访问控制包括入侵检测和防御、文件控制以及高级恶意软件防护。有关详细信息，请参阅后续章节。

入侵检测和防御

入侵检测和防御功能可以监控网络流量是否存在违反安全性的情况，并且在内联部署中可以阻止或更改恶意流量。

入侵防御集成于访问控制中，您可以将入侵策略与特定访问控制规则关联。如果网络流量符合规则中的条件，您就可以分析与入侵策略匹配的流量。还可以将入侵策略与访问控制策略的默认操作相关联。

入侵策略包含很多组成部分，包括：

- 检查协议报头值、负载内容和某些数据包大小特性的规则
- 基于 FireSIGHT 建议的规则状态配置
- 高级设置，例如预处理器和其他检测与性能功能
- 可以为关联预处理器和预处理器选项生成事件的预处理器规则

文件跟踪、控制和恶意软件防护

为了帮助识别和减轻恶意软件的影响， Sourcefire 3D 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 （可选地）阻止网络流量中的文件传输 （包括恶意软件文件）。

文件控制

*文件控制*允许受管设备检测并阻止用户通过特定应用协议上传 （发送）或下载（接收）特定类型的文件。您可以在全局访问控制配置中配置文件控制；与访问控制规则关联的文件策略可以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)

基于网络的*高级恶意软件防护* (AMP) 允许系统检查网络流量中某些类型的文件中是否存在恶意软件，其中包括 PDF 文件、诸多 Microsoft Office 文档和其他类型的文件。检测时，受管设备可以将这些文件存储在硬盘或恶意软件存储包中，以便

进行人工分析。无论是否存储文件，设备都可以将文件提交到 Sourcefire 云，以便进行*动态分析*。防御中心还基于以下内容分配文件性质：

- 恶意软件云查找或*动态分析*结果 （威胁分数）
- 文件*清除列表*
- 文件*自定义检测列表*

受管设备基于此信息阻止或允许文件。

您可以在全局访问控制配置过程中配置恶意软件防护；与访问控制规则关联的文件策略可以检查符合规则条件的网络流量。

FireAMP 集成

FireAMP 是 Sourcefire 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 连接器*。这些轻型代理与 Sourcefire 云通信，后者又与防御中心通信。将防御中心配置为连接至云之后，您可以使用防御中心网络界面查看由于公司终端上的扫描、检测和隔离而生成的基于终端的恶意软件事件。

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，要追踪文件，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有关文件的附加信息。

应用编程接口

您可以使用应用编程接口 (API) 以多种方式与系统交互。关于详细信息，可从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 Sourcefire 设备流式传输至自定义开发的客户端应用。创建客户端应用之后，可以将其连接到 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，但您可以向设备请求特定数据。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漏洞数据，并将此信息纳入显示范畴。

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，查询位于 Sourcefire 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 Sourcefire 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告警控制面板。

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，以增加网络映射中的信息。

该网络界面也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，使漏洞生效或无效，同时从网络映射中删除各项目，包括客户和服务器端口。

补救措施

通过该系统的一个 API，您可以创建*补救措施*，使防御中心可以在网络状况违反关联的关联策略或合规白名单时自动启动这些补救措施。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。

安全性、互联网接入和通信端口

为保护防御中心的安全，应将防御中心安装在受保护的内部网络中。虽然防御中心被配置为仅提供必要的服务和端口，但您必须确保该防御中心不会受到防火墙外部的攻击。

如果防御中心和受管设备驻留在同一网络上，可将设备上的管理接口连接到防御中心所在的受保护内部网络。这样您就可以从防御中心安全地控制设备并汇聚受管设备的网段上生成的事件数据。通过使用防御中心的过滤功能，可以分析和关联网络上的攻击数据，以评估安全策略实施情况。

然而，请注意， Sourcefire 设备被配置为直接连接到互联网。 Sourcefire 3D 系统的特定功能要求这种直接连接，其他功能支持使用代理服务器。此外，系统要求某些端口保持开放，以允许基本的设备内通信以及访问设备的网络界面。默认情况下，还会有其他多个端口保持开放，以允许系统利用附加的特性和功能。

有关详细信息，请参阅：

- 第 26 页的互联网接入要求
- 第 27 页的开放通信端口要求

互联网接入要求

默认情况下， Sourcefire 设备被配置为直接连接到互联网。 Sourcefire 3D 系统的特定功能要求这种直接连接。然而，所有此类功能都支持使用代理服务器；请参阅《*Sourcefire 3D 系统用户指南*》中的“配置网络设置”章节。

提示！ 您可以将系统软件、入侵文件、 GeoDB 和 VDB 更新手动上传至设备。

为确保操作的连续性，高可用性对中的两个防御中心必须能够访问互联网。为获取特定功能，主防御中心连接互联网，然后在同步过程中与辅助防御中心共享信息。因此，如果主防御中心出现故障，应将辅助防御中心升级为主防御中心，如《*Sourcefire 3D 系统用户指南*》中的“监控和更改高可用性状态”章节中所述。

下表描述了 Sourcefire 3D 系统的互联网访问要求。

Sourcefire 3D 系统互联网访问要求

对于.....	要求互联网访问以.....	高可用性考虑事项	代理?
RSS 源控制面板构件	从外部来源下载 RSS 源数据，包括 Sourcefire。	源数据未同步。	是
安全情报源	从外部来源下载安全情报源数据，包括 Sourcefire 情报源。	主防御中心下载源数据并与辅助防御中心共享。如果主防御中心出现故障，必须切换角色。	是
URL 过滤数据	下载基于云的 URL 类别和信誉数据以进行访问控制，查找未分类的 URL。	主防御中心下载 URL 过滤数据并与辅助防御中心共享。如果主防御中心出现故障，必须切换角色。	是
恶意软件云查找 （经 恶意软件 许可）	执行云查找，确定在网络流量中检测到的文件是否包含恶意软件。	成对的防御中心独立执行云查找，尽管文件策略已同步。	是
动态分析	将文件提交到云以进行恶意软件分析。	成对的防御中心独立在云中查询提交的文件以进行恶意软件分析，尽管文件策略已同步。	是
FireAMP 集成 （FireAMP 订用）	接收来自 Sourcefire 云的基于终端的恶意软件事件。	云连接未同步。在两个防御中心上配置连接。	是
系统、入侵规则、 GeoDB 和 VDB 更新	将入侵规则、GeoDB、VDB 或系统更新直接下载或安排直接下载至设备。	Rule、 GeoDB 和 VDB 更新已同步；系统更新未同步。所有下载更新的设备都必须能够访问互联网。	是
使用 IP 地址上下文菜单获取域名信息	获取域名信息。	任何请求域名信息的设备都必须能够访问互联网。	是

开放通信端口要求

Sourcefire 3D 系统要求端口 443 （入站）和端口 8305 （入站和出站）保持开放，以允许基本的设备内通信以及访问设备的网络界面。

默认情况下，多个其他端口保持开放，允许系统利用附加功能。下表列出了这些端口。请注意，端口 67 和端口 68 上的 DHCP 在默认情况下禁用。

Sourcefire 3D 系统开放通信端口要求

端口	说明	协议	方向	此端口开放给...
22	SSH/SSL	TCP	双向	允许安全的远程设备连接。
25	SMTP	TCP	出站	发送来自设备的邮件通知和告警。
53	DNS	TCP	出站	使用 DNS。
67、 68	DHCP	UDP	出站	使用 DHCP。**默认情况下禁用。**
80	HTTP	TCP	出站或双向	允许 RSS 源控制面板构件连接到远程网络服务器 （出站）。 添加入站访问允许防御中心通过 HTTP 更新自定义和第三方安全情报源，以及下载 URL 过滤信息。
161、 162	SNMP	UDP	双向 (161)；出站 (162)	如果已禁用 SNMP 轮询 （入站）和 SNMP 陷阱 （出站），提供访问。
389、 636	LDAP	TCP	出站	跟踪用户活动，进行身份验证。
443	HTTPS/AMQP；云查找	TCP	入站或双向	访问设备。**必需。** 添加出站访问允许防御中心下载或接收软件更新、 VDB 和 GeoDB 更新、 URL 过滤信息、安全的安全情报源和基于终端的 (FireAMP) 恶意软件事件。 通过端口 443 进行的连接还允许防御中心执行云查找，以判断在网络流量中检测到的文件是否包含恶意软件，在云中查找动态分析信息，以及跟踪文件的踪迹。 通过端口 443 进行的连接允许受管设备将文件提交到云，以进行动态分析。
514	系统日志	UDP	出站	将告警发送到远程系统日志服务器。

Sourcefire 3D 系统开放通信端口要求 （续）

端口	说明	协议	方向	此端口开放给...
623	SOL/LOM	UDP	双向	允许您使用 Serial Over LAN (SOL) 连接在3系列 设备上执行无人值守管理 (LOM)。
1500、2000	数据库访问	TCP	入站	如果外部数据库访问已启用，访问防御中心。
1812、1813	RADIUS	UDP	出站或双向	使用 RADIUS。添加入站访问可确保 RADIUS 身份验证和统计正确运行。 端口 1812 和端口 1813 是默认设置，但可以配置 RADIUS 使用其他端口；请参阅《*Sourcefire 3D 系统用户指南*》中的“配置 RADIUS 连接设置”章节。
3306	Sourcefire 用户代理	TCP	入站	允许防御中心和 Sourcefire 用户代理之间的通信。
8302	eStreamer	TCP	双向	使用 eStreamer 客户端。
8305	设备管理	TCP	双向	在防御中心和受管设备之间通信。**必需**。
8307	主机输入客户端	TCP	双向	允许防御中心和主机输入客户端之间的通信。
32137	恶意软件云查找（旧版；可选）	TCP	双向	允许防御中心执行云查找，确定在网络流量中检测到的文件是否包含恶意软件，并跟踪文件的轨迹。

文档资源

Sourcefire 3D 系统文档集包括联机帮助和 PDF 文件。您可以通过以下两种方式获取联机帮助：

- 点击每个页面上的上下文帮助链接
- 选择 **Help > Online**

联机帮助含有有关可以在网络界面上完成的任务的详细信息，包括有关用户管理、系统管理和事件分析的程序性信息和概念性信息。

文档 CD 包含以下资料的 PDF 版：

- 《*Sourcefire 3D 系统用户指南*》，其内容与联机帮助相同，但格式更便于打印
- 《*Sourcefire 3D 系统安装指南*》，包含有关安装 Sourcefire 设备的信息以及硬件规格和安全信息

- 《*Sourcefire 3D 系统虚拟安装指南*》，包含有关安装、管理虚拟设备和虚拟防御中心以及疑难解答的信息
- 《*用于 X 系列的 Sourcefire 软件安装指南*》，包含有关安装、管理用于 X 系列的 Sourcefire 软件以及疑难解答的信息
- 各种 API 指南和补充材料

可以在 Sourcefire 支持网站 (https://support.sourcefire.com/) 上访问最新版本的 PDF 文档。

文档约定

本文档包含有关每个功能要求使用哪些 Sourcefire 3D 系统许可证和设备型号以及哪些用户角色有权限完成各个操作步骤的信息。有关详细信息，请参阅以下各节：

- 第 29 页的许可约定
- 第 30 页的支持的设备和防御中心约定
- 第 30 页的访问约定

许可约定

各个章节开头的许可证声明指出了使用本节所述功能所要求使用的许可证，详情如下：

FireSIGHT

FireSIGHT 许可证包含在防御中心中，必须使用此许可证才能执行主机、应用和用户发现。防御中心上的 FireSIGHT 许可证决定了利用防御中心及其受管设备可以监控多少单独的主机和用户，以及可以对多少用户执行用户控制。

如果防御中心以前运行的是 4.10.x 版本，您可以使用旧版 RNA 主机和 RUA 用户许可证代替 FireSIGHT 许可证。

保护

保护许可证允许受管设备执行入侵检测和防御、文件控制以及安全情报过滤。

控制

控制许可证允许受管设备执行用户和应用控制。此许可证还允许设备执行交换和路由 （包括 DHCP 中继）、 NAT，以及集群设备和堆栈。控制许可证必须包含保护许可证。

URL 过滤

URL 过滤许可证允许受管设备基于受监控主机请求的 URL，使用定期更新的基于云的类别和信誉数据确定哪些流量可以流经网络。URL 过滤许可证必须包含保护许可证。

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、捕捉并阻止通过网络传输的文件中的恶意软件并提交这些文件进行动态分析。它还允许您查看用于跟踪通过网络传输的文件的轨迹。恶意软件许可证必须包含保护许可证。

VPN

VPN 许可证允许在 Sourcefire 受管设备的虚拟路由器之间建立安全的 VPN 隧道。 VPN 许可证必须包含保护和控制许可证。

由于许可的功能通常是累加的，此文档仅提供每项功能的最高要求许可证。例如，如果功能要求 FireSIGHT、保护和控制许可证，则只列出控制许可证。

许可声明中“或”语句表明要使用本部分描述的功能需要使用的特定许可证，但是使用附加许可证可以增加功能。例如，在文件策略中，有些文件规则操作要求使用保护许可证，而其他的操作则要求使用恶意软件许可证。因此，文件规则文档的许可声明会列出“保护或恶意软件。”

请注意，由于架构和资源的限制，并非所有的许可证都可被应用至所有受管设备。一般而言，您无法许可设备不支持的功能；请参阅第 18 页的不同设备型号支持的功能 。有关许可证对可以使用的功能的影响的详细信息，包括有关使用旧版 RNA 主机和 RUA 用户许可证的信息，请参阅 《*Sourcefire 3D 系统用户指南*》中的“了解许可”章节。

支持的设备和防御中心约定

每节开头的支持设备声明指出了某功能只能在指定的设备系列或型号上使用。例如，只有在3 系列 设备上才支持堆栈。如果某一节没有支持设备声明，则表明所有设备都支持该功能，或该节不适用于受管设备。

有关此版本支持的平台的详细信息，请参阅第 15 页的了解设备系列、型号和功能 。

访问约定

本文档每个操作步骤开头的“访问”声明都指出了执行此操作步骤所要求的预定用户角色。正斜杠隔开的角色表示任何列出的角色都可执行此操作步骤。下表定义了访问声明中出现的常用术语。

访问约定

访问术语	表明
访问管理员	用户必须具备访问控制管理员角色
管理员	用户必须具备管理员角色
任意	用户可以是任意角色

访问约定 （续）

访问术语	表明
任意/管理员	用户可以是任意角色，但是只有管理员角色的访问才不受限制 （例如可以查看保存为专用级别的其他用户数据）
任何安全分析师	用户可以是安全分析师角色或安全分析师 （只读）角色
数据库	用户必须具备外部数据库角色
发现管理员	用户必须具备发现管理员角色
入侵管理员	用户必须具备入侵管理员角色
维护人员	用户必须具备维护用户角色
网络管理员	用户必须具备网络管理员角色
安全分析师	用户必须具备安全分析师角色
安全审批人	用户必须具备安全审批人角色

具有自定义角色的用户可以拥有不同于预定角色的权限集。预定角色用于指示某个程序的访问要求，而具有相似权限的自定义角色也能访问。有关自定义用户角色的详细信息，请参阅 《*Sourcefire 3D 系统用户指南*》中的“管理自定义用户角色”章节。

IP 地址约定

可以使用 IPv4 无类别域际路由选择 (CIDR) 表示法和类似的 IPv6 前缀长度表示法定义 Sourcefire 3D 系统不同位置的地址块。

CIDR 表示法将网络 IP 地址与位掩码结合使用来定义指定地址块中的 IP 地址。例如，下表列出了 CIDR 表示法中的专用 IPv4 地址空间。

CIDR 表示法语法示例

CIDR 块	CIDR 块中的 IP 地址	子网掩码	IP 地址数量
10.0.0.0/8	10.0.0.0 - 10.255.255.255	255.0.0.0	16,777,216

CIDR 表示法语法示例 （续）

CIDR 块	CIDR 块中的 IP 地址	子网掩码	IP 地址数量
172.16.0.0/12	172.16.0.0 - 172.31.255.255	255.240.0.0	1,048,576
192.168.0.0/16	192.168.0.0 - 192.168.255.255	255.255.0.0	65,536

同样， IPv6 将网络 IP 地址与前缀长度结合使用来定义指定块中的 IP 地址。例如，2001:db8::/32 指定在 2001:db8:: 网络中前缀长度为 32 位的 IPv6 地址，即 2001:db8:: 至 2001:db8:ffff:ffff:ffff:ffff:ffff:ffff。

当您使用 CIDR 或前缀长度表示法指定 IP 地址块时， Sourcefire 3D 系统**只**使用掩码或前缀长度指定的网络 IP 地址部分。例如，如果您键入 10.1.2.3/8，则 Sourcefire 3D 系统使用 10.0.0.0/8。

换句话说，虽然 Sourcefire 建议您在使用 CIDR 或前缀长度表示法时采用使用位边界上网络 IP 地址的标准方法，但是 Sourcefire 3D 系统并不要求必须这么做。

登录设备

许可证： 任意

防御中心具备网络界面，您可以使用此网络界面执行管理和分析任务。物理受管设备具有受限的网络界面，您可以使用此网络界面执行初始设置以及基本的分析和配置任务。虚拟受管设备和用于 X 系列的 Sourcefire 软件不具备网络界面。您可以使用网络浏览器登录设备来访问网络界面。有关浏览器要求的信息，请参阅此版 Sourcefire 3D 系统的版本说明。

如果您是设备安装后第一个登录设备的用户，您必须使用管理员 (admin) 用户帐户登录，完成初始设置流程，详情请见 《*Sourcefire 3D 系统安装指南*》。按 《*Sourcefire 3D 系统用户指南*》中的“添加新用户帐户”章节创建其他用户帐户后，您和其他用户应当使用这些帐户登录网络界面。

重要！ 因为 Sourcefire 设备根据用户帐户审计用户活动，所以请务必确保用户使用正确的帐户登录系统。

在登录设备后，可以访问的功能受控于已授予用户帐户的权限。然而，登录设备和从设备注销的操作步骤保持不变。如果登录时公司使用 SecurID® 令牌，则将令牌附加到 SecurID PIN，并将其用作登录密码。例如，如果 PIN 为 1111，SecurID 令牌为 222222，请键入 1111222222。

警告！ 如果您多次提供不正确的凭证，您的外壳访问帐户可能会被锁定。甚至在帐户锁定后，系统会提示您再次提供凭证。如果您提供了正确的凭证但是登录被拒绝，请联系系统管理员，不要反复尝试登录。

首次在网络会话期间访问设备主页时，您可以查看在此设备最后一次登录会话的信息。您可以看到以下有关最后一次登录的信息：

- 登录星期、月份、日期和年份
- 采用 24 小时表示法的设备本地登录时间
- 最后一次用于访问设备的主机名和域名

默认情况下，会话会在 1 小时的非活动期后自动将您从设备注销，除非您已被配置为不受会话超时限制。拥有管理员角色的用户可以更改系统策略中的会话超时间隔。有关详细信息，请参阅《*Sourcefire 3D 系统用户指南*》中的“管理用户登录设置和配置用户界面设置”章节。

请注意，有些操作步骤耗时很长。此时，网络浏览器可能会显示脚本已停止响应的消息。如果发生这种情况，请务必允许脚本继续运行，直到完成为止。

要通过网络界面登录设备，请执行以下操作：

访问： 任意

1. 将浏览器定向到 `https://`*`hostname`*`/`，其中 *`hostname`* 对应设备的主机名。

   系统将显示 Login 页面。

2. 在 **Username** 和 **Password** 字段中，键入用户名和密码。用户名区分大小写。

   如果公司使用 SecurID，请将 SecurID 令牌附加到 SecurID PIN 末端，并在登录时将其用作密码。您必须在登录 Sourcefire 3D 系统之前生成 SecurID PIN。

3. 点击 **Login**。

   系统将显示默认启动页面。如果已为用户帐户选择了新主页，则系统将改为显示该页面。有关详细信息，请参阅《*Sourcefire 3D 系统用户指南*》中的“指定主页”章节。

   页面顶部的菜单和菜单选项取决于用户帐户的权限。然而，默认主页上的链接带有超出用户帐户权限范围的选项。如果点击的链接所需的权限与已授予帐户的权限不同，系统将显示以下警告消息：

   > 您正在尝试查看未经授权的页面。此活动已被记录。

   您可以从可用菜单中选择另一个选项，或者点击浏览器窗口中的 **Back**。

要通过命令行登录 3 系列或虚拟设备，请执行以下操作：

访问： CLI 基本配置

1. 在 *hostname* 打开一个到设备的 SSH 连接，其中 *hostname* 对应设备的主机名。

   系统将显示 `login as:` 命令提示符。

2. 键入用户名，然后按 Enter 键。

   系统将显示 `Password:` 提示符。

3. 键入密码，然后按 Enter 键。

   系统将显示登录横幅，后接 > 提示符。

   您可以使用命令行访问级别允许的任何命令。有关可用 CLI 命令的详细信息，请参阅 《*Sourcefire 3D 系统用户指南*》中的“命令行参考”章节。

登录设备以设置帐户

许可证： 任意

有些用户帐户可以通过外部身份验证服务器进行身份验证。如果公司允许使用 LDAP 或 RADIUS 凭证登录 Sourcefire 3D 系统，在您首次使用外部用户凭证登录设备时，设备会创建本地用户记录，将这些凭证与一系列的权限关联起来。然后，您可以修改对本地用户记录的权限，除非这些权限通过群组或列表成员身份授予，如下所示：

- 如果经外部身份验证的用户帐户的默认角色被设为特定访问角色，您可以使用外部帐户凭证登录设备，无需系统管理员设置其他配置。
- 如果帐户经外部身份验证并在默认情况下没有接收访问权限，您可以登录设备，但无法访问任何功能。然后，您 （或系统管理员）可以更改权限，以授予相应的用户功能访问权限。

如果您是外壳访问用户，系统不会在设备上为您创建本地用户帐户。外壳访问受到 LDAP 服务器的外壳访问过滤器或 PAM 登录属性集或 RADIUS 服务器上的外壳访问列表的完全控制。

外壳用户可以使用采用小写、大写或大小写字母的用户名登录。外壳登录身份验证区分大小写。 LDAP 用户名可以包含下划线 (_)、句点 (.) 和连字符 (-)，但其他字符仅支持字母数字字符。

如果登录时公司使用 SecurID 令牌，请将令牌附加到 SecurID PIN，并将其用作登录密码。例如，如果 PIN 为 `1111`， SecurID 令牌为 `222222`，请键入 `1111222222`。

重要！ 如果您无权访问网络界面，请联系系统管理员，修改帐户权限，或者以拥有管理员访问权限的用户登录，修改帐户权限。有关详细信息，请参阅 《*Sourcefire 3D 系统用户指南*》中的“修改用户权限和选项”章节。

要在设备上创建经外部身份验证的帐户，请执行以下操作：

访问： 任意

1. 将浏览器定向到 `https://hostname/`，其中 *hostname* 对应设备的主机名。

   系统将显示 Login 页面。

2. 在 **Username** 和 **Password** 字段中，键入用户名和密码。

   重要！ 如果公司使用 SecurID，请将 SecurID 令牌附加到 SecurID PIN，并在登录时将其用作密码。

3. 点击 **Login**。

   系统将页面取决于进行外部身份验证的默认访问角色：

   - 如果在身份验证对象或系统策略中选择了默认访问角色，系统将显示默认开始页面。如果已为用户帐户选择新主页，则系统将显示新主页。有关详细信息，请参阅《*Sourcefire 3D 系统用户指南*》中的“指定主页”章节。

     页面顶部的可用菜单和菜单选项取决于用户帐户权限。然而，默认主页上的链接带有超出用户帐户权限范围的选项。如果点击的链接所需的权限与已授予帐户的权限不同，系统将显示以下警告消息：

     您正在尝试查看未经授权的页面。此活动已被记录。

     您可以从可用菜单中选择另一个选项，或者点击浏览器窗口中的 **Back**。

   - 如果未选择默认访问角色，系统会再次显示 Login 页面，并显示以下错误消息：

     无法授权访问。如果依然无法访问此设备，请联系系统管理员。

   请注意，如果您使用的 RADIUS 服务器采用属性匹配作为身份验证方法，您的首次登录尝试会被拒绝，因为用户帐户已创建。您必须登录第二次。

从设备注销

许可证： 任意

当您当前不再使用网络界面时，即使只是暂时不使用网络浏览器， Sourcefire 也建议您从设备注销。注销会终止网络会话，确保他人不能通过您的凭证使用设备。

默认情况下，会话会在 1 小时的非活动期后自动将您从设备注销，除非您已被配置为不受会话超时限制。拥有管理员角色的用户可以更改系统策略中的会话超时间隔。有关详细信息，请参阅《*Sourcefire 3D 系统用户指南*》中的“管理用户登录设置和配置用户界面设置”章节。

要从设备注销，请执行以下操作：

访问： 任意

▶ 点击工具栏上的 **Logout**。

使用上下文菜单

许可证： 因功能而异

为方便起见，网络界面中的某些页面支持弹出上下文菜单，您可以将其用作快捷方式，访问 Sourcefire 3D 系统中的其他功能。菜单内容取决于您访问菜单的*热点* - 不仅是页面，还包括特定数据。

例如，事件视图、入侵事件数据包视图、控制面板和 Context Explorer 中的 *IP 地址热点*可以提供附加选项。通过右键单击热点，使用 IP 地址上下文菜单，了解与该地址关联的主机的详细信息，包括任何可用的域名和主机配置文件信息。除了在不支持安全情报过滤的 DC500 防御中心上，您还可以将单个 IP 地址添加到安全情报全局白名单或黑名单中。

又例如，事件视图和控制面板中的 *SHA-256 值热点*允许您将文件的 SHA-256 哈希值添加到清除列表或自定义检测列表中，或者查看整个哈希值以复制。请注意，DC500 防御中心也不支持此功能。

下表描述了网络界面各个页面上的上下文菜单中的可用选项。在不支持 Sourcefire 上下文菜单的页面或位置，会显示浏览器的标准上下文菜单。

访问控制策略编辑器

访问控制策略编辑器包含基于每条访问控制规则的热点。您可以使用上下文菜单插入新规则和类别；剪切、复制和粘贴规则；设置规则状态；编辑规则。

NAT 策略编辑器

NAT 策略编辑器包含基于每条 NAT 规则的热点。您可以使用上下文菜单插入新规则；剪切、复制和粘贴规则；设置规则状态；编辑规则。

入侵规则编辑器

入侵规则编辑器包含基于每条入侵规则的热点。您可以使用上下文菜单编辑规则，设置规则状态 （包括禁用规则），配置阈值和抑制选项，以及查看规则文档。

事件查看器

事件页面 （向下钻取页面和表视图）包含基于每个事件、 IP 地址和某些已检测文件的 SHA-256 哈希值的热点。对于大多数事件类型，您可以使用上下文菜单在 Context Explorer 中查看相关信息，或者向下钻取至新窗口中的事件信息。如果事件字段包含的文本太长而无法在事件视图中完全显示此文本，例如文件的 SHA-256 哈希值、漏洞描述或 URL，您可以使用上下文菜单查看完整文本。

对于捕获的文件、文件事件和恶意软件事件，您可以使用上下文菜单将文件添加至清除列表或自定义检测列表或从这些列表中移除文件，下载文件副本，或者将文件提交到云进行动态分析。

对于入侵事件，可以使用上下文菜单执行与入侵规则编辑器或入侵策略中的任务类似的任务：编辑触发规则，设置规则状态 （包括禁用规则），配置阈值和抑制选项，以及查看规则文档。

数据包视图

入侵事件数据包视图包含 IP 地址热点。请注意，数据包视图使用左键单击上下文菜单而非右键单击菜单。

控制面板

许多控制面板构件包含热点，您可以在 Context Explorer 中查看相关信息。控制面板构件也可以包含 IP 地址和 SHA-256 值热点。

Context Explorer

Context Explorer 包含基于其图表、表和图形的热点。如果想要超出 Context Explorer 允许的范围，更详细地检查图形或列表中的数据，您可向下钻取相关数据的表视图。还可以查看相关主机、用户、应用、文件和入侵规则信息。

请注意， Context Explorer 使用左键单击上下文菜单，此菜单还包含过滤选项以及 Context Explorer 独有的其他选项。有关详细信息，请参阅 《*Sourcefire 3D 系统用户指南*》中的“向下钻取 Context Explorer 数据”章节。

要访问上下文菜单，请执行以下操作：

访问： 任意

1. 在网络界面中已启用热点的页面上，将光标悬停在热点上方。

   除了在 Context Explorer 中，系统将显示右键单击打开菜单的消息。

2. 调用上下文菜单：
   - 在 Context Explorer 或数据包视图中，左键单击光标指向的设备。
   - 在所有其他热点启用的页面上，右键单击光标指向的设备。

   系统将显示弹出上下文菜单，其中包含适用于热点的选项。

3. 左键单击选项名称，选择其中一个选项。

   如果您正在使用访问控制策略编辑器或 NAT 策略编辑器，规则将被修改。否则，系统会根据您选择的选项打开一个新的浏览器窗口。

第 3 章
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。

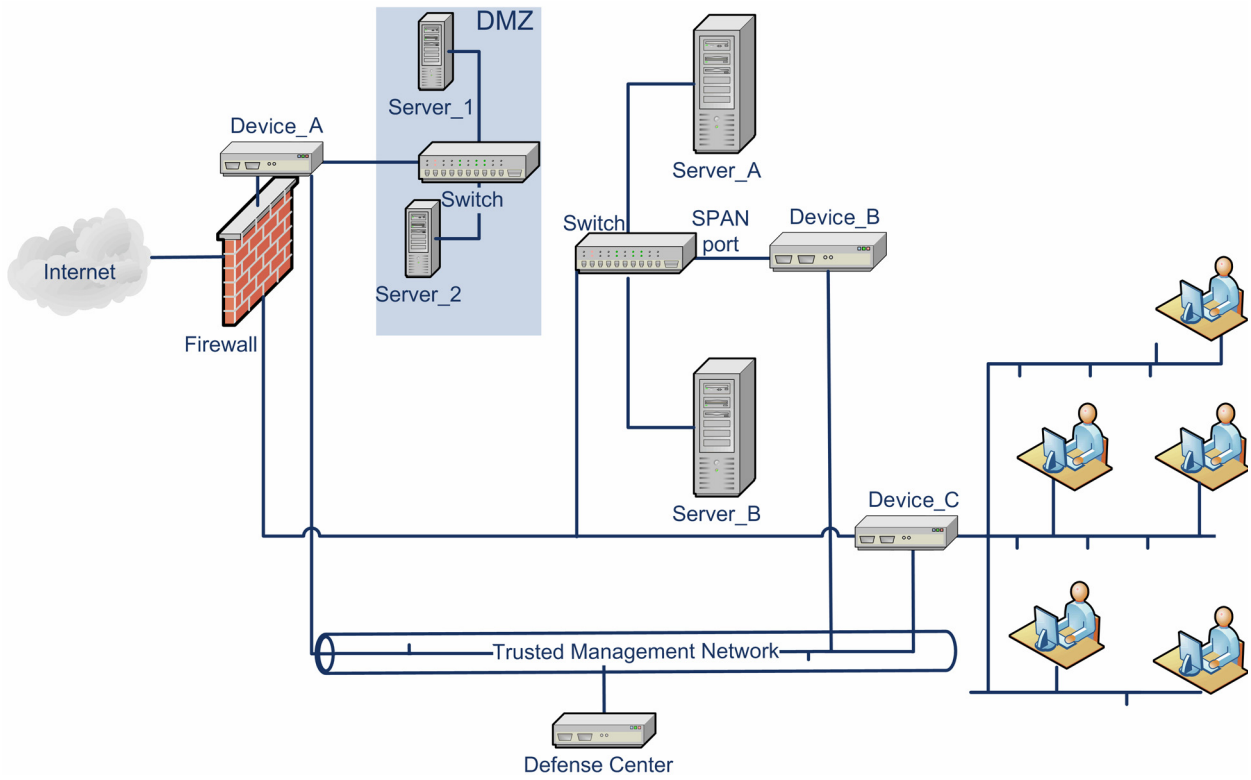
警告！ Sourcefire **强烈**建议您将生产网络流量和可信管理网络流量置于不同的网段。您必须采取预防措施来确保设备和管理流量数据流的安全。

本章提供适用于以下情况的部署示例：

- 第 39 页的典型的 Sourcefire 3D 系统部署
- 第 39 页的 VMware 虚拟设备部署

典型的 Sourcefire 3D 系统部署

在物理设备环境中，典型的 Sourcefire 3D 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。端口镜像也被某家大型网络设备供应商称为交换交端口分析器或 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：

- 第 40 页的添加虚拟化和虚拟设备
- 第 41 页的使用虚拟设备进行内联检测
- 第 41 页的添加虚拟防御中心

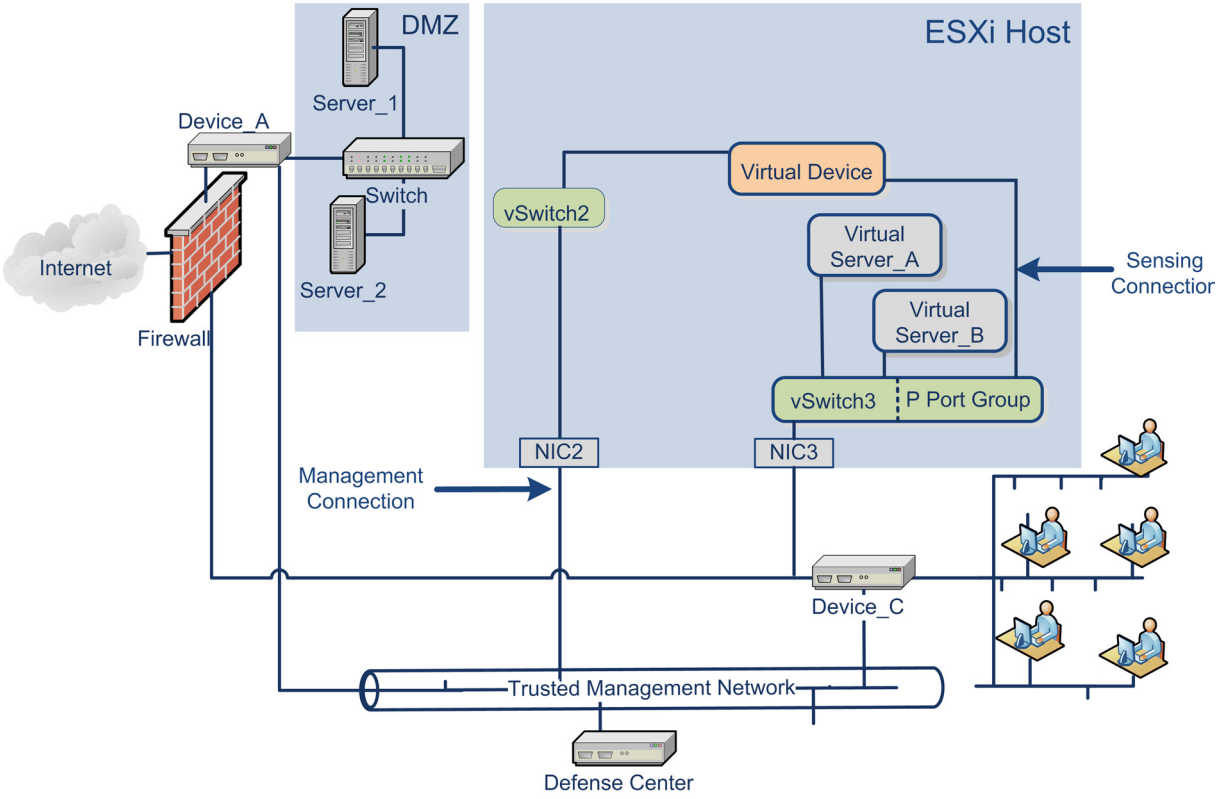
- 第 42 页的使用试部署
- 第 43 页的使用远程办公室部署

添加虚拟化和虚拟设备

您可使用虚拟基础设施来替换第 39 页的典型的 Sourcefire 3D 系统部署中所述的内部物理服务器。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。

您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。

此虚拟设备感应接口必须连接到接受混杂模式流量的交换机或端口组，如下所示。



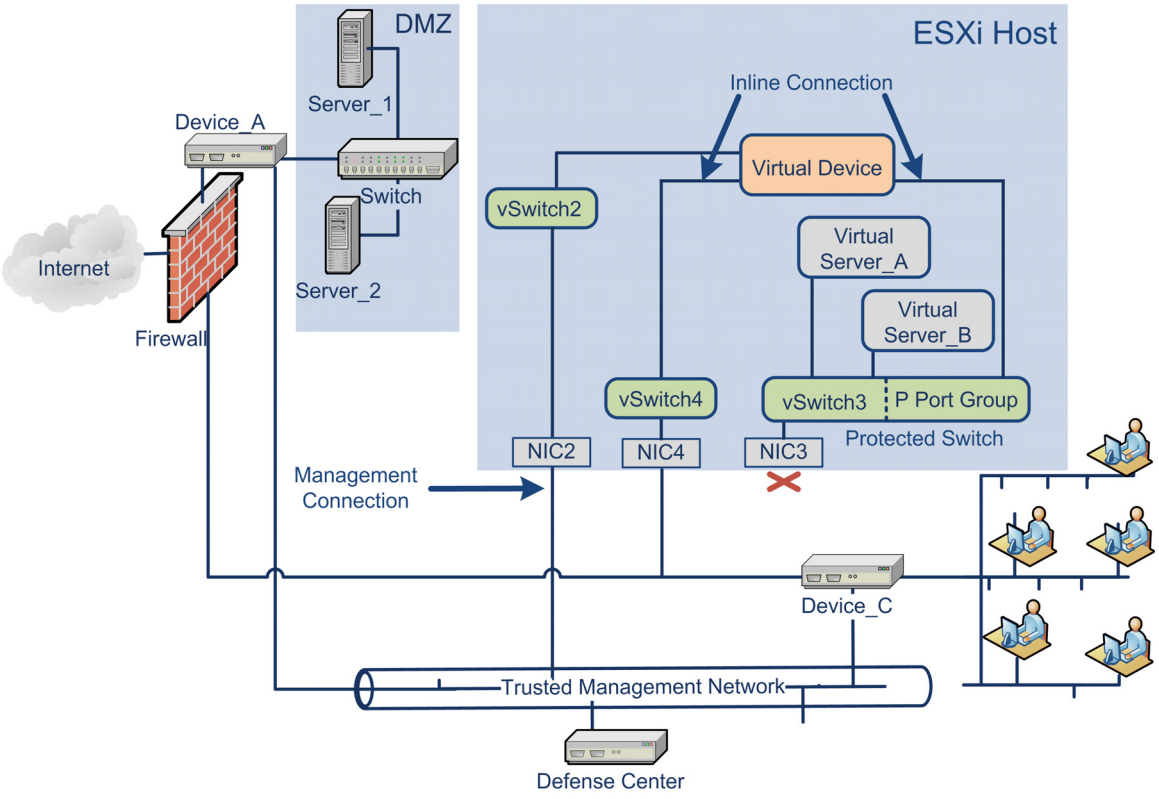
重要！ 要感应所有流量，需在设备感应接口所连接的虚拟交换机或端口组允许混杂模式流量。请参阅第 54 页的配置虚拟设备感应接口。

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确定一个安全边界。此场景依据第 39 页的典型的 Sourcefire 3D 系统部署以及第 40 页的添加虚拟化和虚拟设备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 《*Sourcefire 3D 系统用户指南*》。



重要！ 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。请参阅第 54 页的配置虚拟设备感应接口。

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。

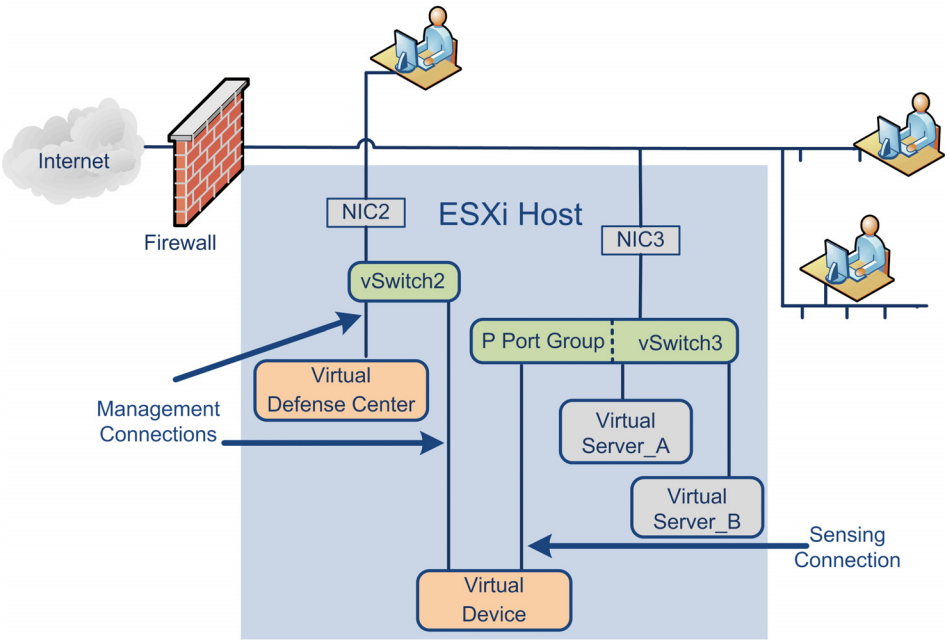
添加虚拟防御中心

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。此场景依据第 39 页的典型的 Sourcefire 3D 系统部署以及第 41 页的使用虚拟设备进行内联检测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 建立的连接，虚拟防御中心能够同时管理物理和虚拟设备。

使用试部署

由于 Sourcefire 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。这将减少复杂的硬件和软件兼容性问题，让您加快部署进程并体验 Sourcefire 3D 系统的优势。在此测试或试验中，您可以将多个虚拟服务器、一个虚拟防御中心和一个虚拟设备部署在 ESXi 主机上，并通过虚拟防御中心管理部署工作，如下所示。

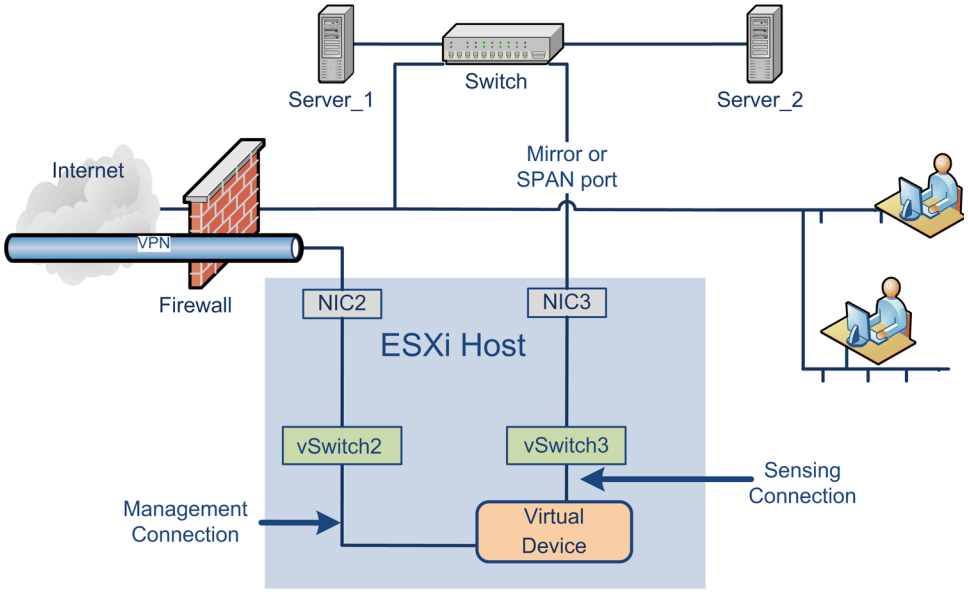


您必须允许虚拟设备上的感应连接以监控网络流量。虚拟接口连接的虚拟交换机或该交换机上的端口组必须能够接收混杂模式流量。这样，虚拟设备便能读取打算发往其他计算机或网络设备的数据包。示例中， P 端口组设置为可接收混杂模式流量。请参阅第 54 页的配置虚拟设备感应接口。

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，请参阅第 64 页的使用脚本配置虚拟防御中心网络设置和第 59 页的使用 CLI 设置虚拟设备。

使用远程办公室部署

虚拟设备是在有限的资源上监控远程办公室的一个理想方法。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。



您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，虚拟设备便能读取打算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 请参阅第 54 页的配置虚拟设备感应接口。

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，请参阅第 59 页的使用 CLI 设置虚拟设备。

第 4 章
安装虚拟设备

Sourcefire 在其支持网站上以压缩存档文件形式 (`.tar.gz`) 提供适用 VMwareESXi 主机环境的打包虚拟设备。Sourcefire 虚拟设备被打包为带有第 7 版虚拟硬件的虚拟机。

您可以通过虚拟基础设施 (VI) 或 ESXi 开放虚拟格式 (OVF) 模板部署虚拟设备：

- 使用 VI OVF 模板部署虚拟设备时，您可以使用部署中的设置向导配置 Sourcefire 所需的设置 （例如，管理员帐户密码和允许设备在网络上进行通信的设置）。

  您必须将虚拟设备部署至一个管理平台，此平台可以是 VMware vCloud Director 或 VMware vCenter。
- 使用 ESXi OVF 模板部署虚拟设备时，您必须在安装之后使用虚拟设备的 VMware 控制台上的命令行界面 (CLI) 来配置设置。

  您可以将虚拟设备部署至一个管理平台 （VMware vCloud Director 或 VMware vCenter），也可以将虚拟设备部署为一个独立设备。

重要！ Sourcefire 虚拟设备的 VMware 快照功能不受支持。

请按本章的指示下载、安装和配置 Sourcefire 虚拟设备。有关创建虚拟主机环境的帮助信息，请参阅 VMwareESXi 文档。

按照以下步骤安装和配置虚拟设备后，将虚拟设备接通电源，进行初始化并按接下来的章节开始初始设置。有关卸载虚拟设备的信息，请参阅第 55 页的卸载虚拟设备。

要安装和部署 Sourcefire 虚拟设备，请执行以下操作：

1. 确保规划的部署符合第 8 页的操作环境先决条件中描述的先决条件。
2. 从支持网站获取正确的存档文件，将这些文件复制到一个适当的存储介质，然后进行解压缩；请参阅第 45 页的获取安装文件。
3. 使用 VMware vCloud Director 网络门户或 vSphere 客户端安装虚拟设备，但不要接通电源；请参阅第 47 页的安装虚拟设备。
4. 确认和调整网络、硬件和内存设置；请参阅第 53 页的安装后更新重要设置。
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；请参阅第 54 页的配置虚拟设备感应接口。

获取安装文件

Sourcefire 提供了安装虚拟设备所需的压缩存档文件 (`.tar.gz`)：一个用于防御中心，一个用于设备。每个存档都包含下列文件：

- 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- 的清单文件 (`.mf`)
- 文件名中包含 -VI- 的清单文件 (`.mf`)
- 虚拟机磁盘格式 (`.vmdk`)

安装虚拟设备之前，请从 Sourcefire 支持网站获取正确的存档文件。Sourcefire 建议您始终使用最新的数据包。虚拟设备数据包通常与系统硬件的主版本 （例如，5.2 或 5.3）相关联。

要获取虚拟设备存档文件，请执行以下操作：

1. 使用支持帐户的用户名和密码，登录 Sourcefire 支持网站 (https://support.sourcefire.com/)。
2. 单击 **Downloads**，选择显示页面上的 **3D System** 选项卡，然后点击您想要安装的系统软件的主版本。

   例如，若要下载 5.3 版本存档文件，请点击 **Downloads > 3D System > 5.3**。
3. 使用以下命名惯例，查找要下载的虚拟设备或虚拟防御中心的存档文件：

   `Sourcefire _3D_Device_Virtual64_VMware-`*`X.X.X-xxx`*`.tar.gz`

   `Sourcefire_Defense_Center_Virtual64_VMware-`*`X.X.X-xxx`*`.tar.gz`

   其中，*X.X.X-xxx* 表示要下载的存档文件的版本和内部版本号。

   可点击页面左侧的其中一条链接查看页面的相应部分。例如，点击 **5.3 Virtual Appliances**，查看 5.3 版本的 Sourcefire 3D 系统的存档文件。

4. 点击要下载的档案。

   文件将开始下载。

   提示！ 在支持网站登录时， Sourcefire 建议您为虚拟设备下载所有可用更新，以便在将虚拟设备安装到主版本后更新系统软件。应当始终运行设备支持的最新版本的系统软件。对于防御中心，您还需下载所有新的入侵规则和漏洞数据库 (VDB) 更新。

5. 将存档文件复制至可以接入正在运行 vSphere 客户端或 VMware vCloud Director 网络门户的工作站或服务器的位置。

   警告！ 请**勿**通过邮件传输存档文件；否则，文件会被损坏。

6. 使用您偏好的工具解压缩存档文件，然后提取安装文件。

   适用于虚拟设备的文件：

   - `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`

   适用于虚拟防御中心的文件：

   - `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* 表示已下载存档文件的版本和内部版本号。

   请务必将所有文件都保存在同一目录下。

7. 接下来安装虚拟设备，以部署虚拟设备。

安装虚拟设备

要安装虚拟设备，请使用平台接口 （VMware vCloud Director 网络门户或 vSphere 客户端）将 OVF （VI 或 ESXi）模板部署至一个管理平台 （VMware vCloud Director 或 VMware vCenter）。

- 如果使用 VI OVF 模板部署虚拟设备，您可以在安装过程中配置 Sourcefire 所需的设置。必须使用 VMware vCloud Director 或 VMware vCenter 管理此虚拟设备。
- 如果使用 ESXi OVF 模板部署虚拟设备，您必须在安装之后配置 Sourcefire 所需的设置。可以使用 VMware vCloud Director 或 VMware vCenter 管理此虚拟设备，或者将其用作独立设备。

确保规划的部署符合第 8 页的操作环境先决条件中描述的先决条件并下载所需的存档文件后，请使用 VMware vCloud Director 网络门户或 vSphere 客户端安装虚拟设备。

您可以使用下列文件来安装虚拟设备：

- 适用于虚拟防御中心的文件：
  `Sourcefire_Defense_Center_Virtual64_VMware-VI-`*`X.X.X-xxx`*`.ovf`
  `Sourcefire_Defense_Center_Virtual64_VMware-ESXi-`*`X.X.X-xxx`*`.ovf`
- 适用于虚拟设备的文件：
  `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* 表示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：

VMware OVF 模板

设置	操作
导入/部署 OVF 模板	浏览至您在上一步骤下载的 OVF 模板以备使用。
OVF 模板详细信息	确认您正在安装的设备 （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具有唯一性且有意义的名称，并为设备选择库存库位。
主机/集群	选择在其上部署设备的主机或集群 （仅适用于虚拟设备）。

VMware OVF 模板 （续）

设置	操作
磁盘格式	选择存储虚拟磁盘的格式：密集配置延迟置零、密集配置快速置零或精简配置。
网络映射	为虚拟设备选择管理接口。

如果使用 VI OVF 模板部署虚拟设备，您可以在安装流程中为虚拟防御中心执行基本设置，为虚拟设备执行完整的初始设置。您可以指定：

- 管理员帐户的新密码
- 网络设置，使设备可以在管理网络上进行通信
- 初始检测模式 （仅适用于虚拟设备）
- 管理防御中心 （仅适用于虚拟设备）

如果您使用 ESXi OVF 模板部署虚拟设备或者选择不使用设置向导进行配置，则必须使用 VMware 控制台为虚拟设备执行初始设置。关于执行初始设置的详细信息，包括关于指定哪些配置的指南，请参阅第 57 页的设置虚拟设备。

请使用以下方案之一安装虚拟设备：

- 第 48 页的使用 VMware vCloud Director 网络门户安装虚拟设备说明如何将虚拟设备部署至 VMware vCloud Director。
- 第 51 页的使用 vSphere 客户端安装虚拟设备说明如何将虚拟设备部署至 VMware vCenter。

要了解网络设置和检测模式，请参阅第 59 页的使用 CLI 设置虚拟设备和第 63 页的设置虚拟防御中心。

使用 VMware vCloud Director 网络门户安装虚拟设备

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

- 创建公司和目录，以将 vApp 模板包含在内。有关详细信息，请参阅《*VMware vCloud Director 用户指南*》。
- 将 Sourcefire 3D 系统虚拟设备 OVF 文件包作为 vApp 模板上传到目录中。有关详细信息，请参阅第 49 页的上传虚拟设备 OVF 文件包。
- 使用 vApp 模板创建虚拟设备。有关详细信息，请参阅第 49 页的使用 vApp 模板。

上传虚拟设备 OVF 文件包

您可以将以下 OVF 文件包上传至 VMware vCloud Director 公司目录：

- 适用于虚拟防御中心的文件：
  `Sourcefire_Defense_Center_Virtual64_VMware-VI-X.X.X-xxx.ovf`
- 适用于虚拟设备的文件：
  `Sourcefire_3D_Device_Virtual64_VMware-VI-X.X.X-xxx.ovf`

  其中，*X.X.X-xxx* 表示要上传的 OVF 文件包的版本和内部版本号。

要上传虚拟设备 OVF 文件包，请执行以下操作：

1. 在 VMware vCloud Director 网络门户上，选择 **Catalogs >** *Organization* **> vApp Templates**，其中 *Organization* 是您想要包含 vVpp 模板的公司的名称。
2. 在 vApp Templates 媒体选项卡上，点击上传图标 ( )。

   系统将显 Upload OVF package as a vApp Template 弹出窗口。
3. 在 OVF 文件包字段中，输入 OVF 文件包的位置，或者点击 **Browse** 浏览至 OVF 文件包。
   - 适用于虚拟防御中心的文件：
     `Sourcefire_Defense_Center_Virtual64_VMware-VI-X.X.X-xxx.ovf`
   - 适用于虚拟设备的文件：
     `Sourcefire_3D_Device_Virtual64_VMware-VI-X.X.X-xxx.ovf`

     其中，*X.X.X-xxx* 表示要上传的 OVF 文件包的版本和内部版本号。
4. 输入 OVF 文件包的名称或者描述。
5. 从下拉列表中，选择虚拟数据中心、存储配置文件和包含 vApp 数据包的目录。
6. 点击 **Upload**，将 OVF 文件包作为 vApp 模板上传至目录。

   OVF 文件包上传至贵公司的目录。
7. 接下来使用 vApp 模板，以从 vApp 模板创建虚拟设备。

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可以配置 Sourcefire 所需的设置。在向导的每个页面上指定设置之后，点击 **Next** 继续。为方便起见，您可以在向导的最后页面确认设置，然后完成此步骤。

要使用 vApp 模板创建虚拟设备，请执行以下操作：

1. 在 VMware vCloud Director 网络门户上，选择 **My Cloud > vApps**。
2. 在 vApps 媒体选项卡上，点击添加图标 (➕)，从目录添加 vApp。

   系统将显示 Add vApp from Catalog 弹出窗口。
3. 点击模板菜单栏上的 **All Templates**。

   系统将显示所有可用的 vApp 模板列表。
4. 选择要添加的 vApp 模板，显示虚拟设备描述。
   - 适用于虚拟防御中心的文件：
     `Sourcefire_Defense_Center_Virtual64_VMware-VI-`*`X.X.X-xxx`*`.ovf`
   - 适用于虚拟设备的文件：
     `Sourcefire_3D_Device_Virtual64_VMware-VI-`*`X.X.X-xxx`*`.ovf`

     其中，*X.X.X-xxx* 表示存档文件的版本和内部版本号。

   系统将显示 End User License Agreement (EULA)。
5. 阅读并接受 EULA。

   系统将显示 Name this vApp 屏幕。
6. 输入 vApp 的名称或者描述。

   系统将显示 Configure Resources 屏幕。
7. 在 Configure Resources 屏幕上，选择虚拟数据库，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。
8. 选择外部、管理和内部来源的目标以及 IP 分配，将 OVF 模板中使用的网络映射至库存中的网络。

   系统将显示 Custom Properties 屏幕。
9. 或者，在 Custom Properties 屏幕上，在设置向导上输入 Sourcefire 所需的设置，对设备进行初始设置。如果现在不进行初始设置，您可以稍后按照第 57 页的设置虚拟设备中的说明来设置。

   系统将显示 Ready to Complete 屏幕，其中显示了虚拟设备的配置。
10. 确认设置，然后点击 **Finish**。

重要！ 请**勿**为虚拟设备启用 **Power on after deployment** 选项。您必须映射感应接口，并确保将这些接口设置为在接通设备电源之前连接。有关详细信息，请参阅第 58 页的初始化虚拟设备。

---

11. 继续执行第 53 页的安装后更新重要设置。

使用 vSphere 客户端安装虚拟设备

您可以使用 vSphere 客户端，通过 VI OVF 或 ESXi OVF 模板部署虚拟设备：

- 如果使用 VI OVF 模板部署虚拟设备，设备必须由 VMware vCenter 或 VMware vCloud Director 管理。
- 如果使用 ESXi OVF 模板部署虚拟设备，设备可以由 VMware vCenter 或 VMware vCloud Director 管理，或被部署至一个独立主机。无论使用哪种部署，您都必须在安装之后配置 Sourcefire 所需的设置。

在向导的每个页面上指定设置之后，点击 **Next** 继续。为方便起见，您可以在向导的最后页面确认设置，然后完成此步骤。

要使用 vSphere 客户端安装虚拟设备，请执行以下操作：

1. 使用 vSphere 客户端，点击 **File > Deploy OVF Template**，部署先前下载的 OVF 模板文件。

   系统将显示 Source 屏幕。您可以在此屏幕浏览下拉列表，然后找到要部署的模板。

2. 从下拉列表选择要部署的 OVF 模板。
   - 适用于虚拟防御中心的文件：

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

     `Sourcefire_Defense_Center_Virtual64_VMware-ESXi-`*`X.X.X-xxx`*`.ovf`
   - 适用于虚拟设备的文件：

     `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* 表示已下载存档文件的版本和内部版本号。

   系统将显示 OVF Template Details 屏幕。

3. 确认已选择正确的虚拟设备。
   - 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。系统将显示 Name and Location 屏幕。

4. 在文本字段键入虚拟设备的名称，选择在其部署设备的库存库位。

   系统将显示 Host / Cluster 屏幕。

5. 选择在其部署模板的主机或集群。

   系统将显示 Specific Host 屏幕。

6. 在想要部署模板的集群中选择特定主机。

   系统将显示 Storage 屏幕。

7. 选择虚拟机的目标存储位置。

   系统将显示 Disk Format 屏幕。

8. 从以下选项中选择想要存储虚拟磁盘的格式：
   - 密集配置延迟置零
   - 密集配置快速置零
   - 精简配置

   系统将显示 Network Mapping 屏幕。

9. 选择在其部署模板的网络。
   - 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。

     为设备输入 Sourcefire 所需的设置，或者点击浏览，稍后完成设置，确认设置，然后点击 **Finish**。

   重要！请**勿**为虚拟设备启用 **Power on after deployment** 选项。您必须映射感应接口，并确保将这些接口设置为在接通设备电源之前连接。有关详细信息，请参阅第 58 页的初始化虚拟设备。

10. 安装完成后，关闭状态窗口。
11. 继续执行安装后更新重要设置。

安装后更新重要设置

安装虚拟设备后，您必须确认虚拟设备的硬件和内存设置都符合部署要求。默认设置是运行系统软件的最低要求，**不得**降低。然而，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。

默认虚拟设备设置

设置	默认	设置是否支持调整
内存	4 GB	支持，对于一台虚拟设备，您**必须**分配： • 4 GB （最低） • 5 GB，用于添加基于类别和信誉的 URL 过滤 • 6 GB，用于添加大型动态源来执行安全情报过滤 • 7 GB，用于添加 URL 过滤和安全情报
虚拟 CPU	4	支持，最多可增至 8 个
硬盘有效容量	40 GB （设备） 250 GB (防御中心)	不支持

以下步骤说明了如何查看和调整虚拟设备的硬件和内存设置。

要查看虚拟设备设置，请执行以下操作：

1. 右键单击新虚拟设备的名称，然后从上下文菜单选择 **Edit Settings**，或者在主窗口 Getting Started 选项卡中点击 **Edit virtual machine settings**。

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

2. 确保 **Memory**、**CPU** 和 **Hard disk 1** 的设置不低于默认值，如第 53 页的默认虚拟设备设置中所述。

   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**配置容量**，请点击 **Hard disk 1**。

3. 或者，点击窗口左侧的相应设置，然后在窗口右侧做出更改，增加内存和虚拟 CPU 数量。

4. 确认 **Network adapter 1** 按如下设置，您可以根据需要做出更改：
   - 在 Device Status 下，启用 **Connect at power on** 复选框。
   - 在 Mac Address 下，手动设置虚拟设备的管理接口的 MAC 地址。

     手动向虚拟设备分配 MAC 地址，避免 MAC 地址更改或者与动态池中其他系统发生冲突。

     此外，对于虚拟防御中心，手动设置 MAC 地址可以确保在必须重新映像设备时，您无需从 Sourcefire 重新请求许可。
   - 在 Network Connection 下，将 **Network label** 设为虚拟设备管理网络的名称。
5. 点击 **OK**。

   您的更改已保存。
6. 根据刚刚安装的设备类型，选择下一步操作：
   - 虚拟防御中心可随时进行初始化；接下来执行第 57 页的设置虚拟设备。
   - 虚拟设备需要一些其他配置；接下来执行配置虚拟设备感应接口。

配置虚拟设备感应接口

虚拟设备上的感应接口与接受混杂模式的 ESXi 主机虚拟交换机上的端口之间必须有网络连接。

提示！ 将端口组添加至虚拟交换机，用以隔离混杂模式虚拟网络和生产流量。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：

1. 使用 vSphere 客户端登录服务器，点击服务器的 **Configuration** 选项卡。

   系统将显示 **Hardware** 和 **Software** 选择列表。
2. 在 **Hardware** 列表中，点击 **Networking**。

   系统将显示虚拟交换机示意图。
3. 在连接虚拟设备感应接口的交换机和端口组上，点击 **Properties**。

   系统将显示 **Switch Properties** 弹出窗口。
4. 在 **Switch Properties** 弹出窗口上，点击 **Edit**。

   系统将显示 **Detailed Properties** 弹出窗口。

5. 在 **Detailed Properties** 弹出窗口上，选择 **Security** 选项卡。

   在 **Policy Exceptions > Promiscuous Mode** 下，确认 Promiscuous Mode 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 设为 4095。

6. 保存更改。

   设备可随时进行初始化。

7. 接下来执行下一章第 57 页的设置虚拟设备。

卸载虚拟设备

您可能需要卸载或移除虚拟设备。关闭虚拟设备，然后删除，即可卸载虚拟设备。

提示！ 移除虚拟设备后，请将感应连接虚拟交换机端口组恢复至默认设置：**Promiscuous Mode**: **Reject**。有关详细信息，请参阅第 54 页的配置虚拟设备感应接口。

关闭虚拟设备

请按照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：

1. 在 VMware 控制台上，以拥有管理员 （或者，对于虚拟设备， CLI 配置）权限的用户登录。

   系统将显示设备提示符。

2. 关闭虚拟设备：

   - 在虚拟防御中心上，键入 `sudo su -`，然后再次键入密码。在根提示符上，键入 `shutdown -h now`，关闭设备。
   - 在虚拟设备上，键入 `system shutdown`。

   虚拟设备将关闭。

删除虚拟设备

在虚拟设备关闭后，您可以删除虚拟设备。

按照以下步骤删除部署在 VMware vCloud Director 上的虚拟设备：

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

- 选择 **My Cloud > vApps**，右键单击要删除的 vApp，点击菜单中的 **Delete**，然后在确认弹出窗口上点击 **Yes**。

  虚拟设备已卸载。

按照以下步骤删除部署在 VMware vCenter 上的虚拟设备：

要使用 vSphere 客户端删除虚拟设备，请执行以下操作：

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

  虚拟设备已卸载。

第 5 章
设置虚拟设备

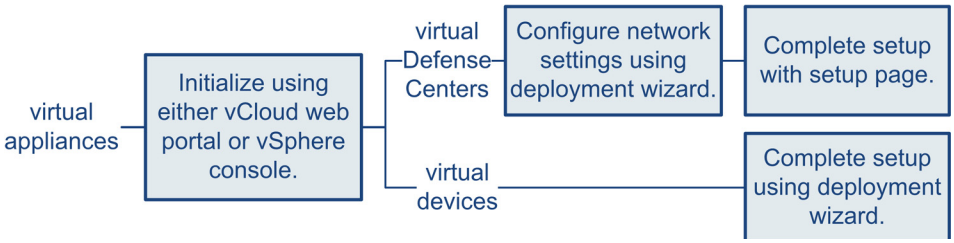
安装虚拟设备后，您必须完成设置过程，使新设备能够在可信任的管理网络上进行通信。您还必须更改管理员密码并接受最终用户许可协议 (EULA)。

在设置过程中，您可以执行多个管理层任务，例如设置时间、注册和许可设备，以及安排更新。在设置和注册过程中选择的选项决定系统将要创建和应用的默认接口、内联集、区域以及策略。

这些初始配置和策略旨在提供开箱即用体验，帮助您快速设置部署，而不会限制您的选择。无论设备初始配置如何，您都可以使用防御中心随时更改配置。换句话说，例如，若在设置过程中选择了检测模式或访问控制策略，系统不会将您锁定至特定设备、区域或策略配置。

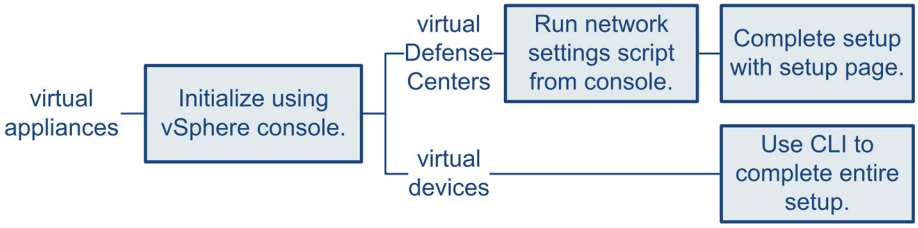
VI OVF 模板部署

下图显示了使用 VI OVF 模板部署时设置虚拟防御中心和受管设备的一般流程。



ESXi OVF 模板部署

下图显示了使用 ESXi OVF 模板部署时设置虚拟防御中心和受管设备的一般流程。



无论如何部署，首先要接通设备电源并初始化设备。初始化完成后，使用 VMware 控制台登录，并根据设备类型按以下方式之一完成设置：

虚拟设备

虚拟设备没有网络界面。如果使用 VI OVF 模板部署，您可以使用部署向导执行设备的初始设置，包括将设备注册至防御中心。如果使用 ESXi OVF 模板部署，您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，您可以使用部署向导执行网络配置。如果选择不使用设置向导或使用 ESXi OVF 模板部署，请使用脚本配置网络设置。配置网络后，请使用管理网络上的计算机浏览到防御中心的网络界面，完成设置过程。

提示！ 如果您正在部署多个设备，请首先设置设备，然后设置这些设备的管理防御中心。在设备的初始设置过程中，您可以将设备预先注册至防御中心；在防御中心的设置过程中，您可以添加和许可预注册的受管设备。

有关详细信息，请参阅：

- 第 58 页的初始化虚拟设备
- 第 59 页的使用 CLI 设置虚拟设备
- 第 63 页的设置虚拟防御中心
- 第 72 页的后续步骤

初始化虚拟设备

当您安装虚拟设备后首次启动虚拟设备时，初始化将自动开始。

警告！ 启动时间取决于许多因素，其中包括服务器资源可用性。初始化完成最多需要 40 分钟。请**勿**中断初始化，否则您将不得不删除设备，重新开始。

使用以下操作步骤初始化虚拟设备：

要初始化虚拟设备，请执行以下操作：

1. 启动设备。
   - 在 VMware vCloud Director 网络门户中，从显示屏中选择 vApp，然后点击 **Start**。
   - 在 vSphere 客户端 中，右键单击您从库存列表导入的虚拟设备的名称，然后从上下文菜单中选择 **Power > Power On**。
2. 在 VMware 控制台选项卡上监控初始化。

   在该过程最长的两个部分中，系统将显示消息。该过程结束后，系统将显示登录提示符。

按照设备类型和部署执行下一个步骤。

如果使用了 VI VOF 模板并且在部署中配置了 Sourcefire 所需的设置：

- 对于虚拟防御中心，执行第 63 页的设置虚拟防御中心，以完成设置。
- 对于虚拟设备，无需进一步配置。

如果使用了 ESXi OVF 模板或者在使用 VI OVF 模板部署时没有配置 Sourcefire 所需的设置：

- 对于虚拟防御中心，执行第 63 页的设置虚拟防御中心，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，执行第 59 页的使用 CLI 设置虚拟设备，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，所以如果使用了 ESXi OVF 模板进行部署，则必须使用 CLI 设置虚拟设备。如果使用了 VI OVF 模板进行部署，但是在部署过程中没有使用设置向导，您也可以使用 CLI 配置 Sourcefire 所需的设置。

提示！ 如果使用了 VI OVF 模板进行部署并且使用了设置向导，则虚拟设备已配置，无需进一步操作。

首次登录新配置的设备时，您必须阅读并接受 EULA。然后，按照设置提示更改管理员密码，配置设备的网络设置和检测模式。

按照设置提示操作时，对于多选问题，选项在圆括号中列出，例如 (y/n)。默认值在方括号中列出，例如 [y]。按 Enter 键，确认选择某个选项。

请注意， CLI 将提示设置信息，这些信息与物理设备的设置页面提示的信息大致相同。有关详细信息，请参阅 《*Sourcefire 3D 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，您必须使用 CLI。有关详细信息，请参阅 《*Sourcefire 3D 系统用户指南*》中的“命令行参考”章节。

了解设备网络设置

Sourcefire 3D 系统可以为 IPv4 和 IPv6 管理环境提供双堆栈实施。您必须设置 IPv4 或 IPv6 管理 IP 地址、子网掩码或前缀长度以及默认网关。您还可以指定最多三台 DNS 服务器，以及设备的主机名和域。请注意，只有重新启动设备后，主机名才会在系统日志中体现出来。

了解检测模式

您为虚拟设备选择的检测模式决定了系统如何初始配置设备的接口，以及这些接口是属于内联集还是属于安全区域。设置后，您无法更改检测模式；它只是您在设置过程中选择的一个选项，以便系统定制设备的初始配置。一般来说，您应当根据设备的部署方式选择检测模式。

被动

如果设备以被动方式部署成一个入侵检测系统 (IDS)，请选择此模式。在被动部署中，虚拟设备可以执行基于网络的文件和恶意软件检测、安全情报监控以及网络发现。

内联

如果设备以内联方式部署成一个入侵防御系统 (IPS)，请选择此模式。

重要！ 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。

网络发现

如果设备采用被动部署，仅执行主机、应用和用户发现，请选择此模式。

下表列出了系统根据您选择的检测模式而创建的接口、内联集和区域。

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	首个添加到默认内联集的对 - 一个添加到内部区域，另一个添加到外部区域
被动	被动	无	首个分配给被动区域的对
网络发现	被动	无	首个分配给被动区域的对

请注意，安全区域是防御中心级配置。直到您确实将设备添加至防御中心时，系统才会创建安全区域。此时，如果防御中心上存在适当的区域 （内部、外部或被动），系统将把已列出的接口添加至现有的区域。如果没有区域存在，系统会创建区域并添加接口。有关接口、内联集和安全区域的详细信息，请参阅 《*Sourcefire 3D 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

1. 在 VMware 控制台上，使用 `admin` 作为用户名以及您在部署设置向导中指定的新管理员帐户密码，登录虚拟设备。

   如果您没有使用部署设置向导更改密码，或者正在使用 ESXi OVF 模板进行部署，请使用 `Sourcefire` 作为密码。

   设备会立即提示您阅读 EULA。

2. 阅读并接受 EULA。

3. 更改管理员帐户密码。此帐户拥有配置 CLI 访问权限，您无法将其删除。

   Sourcefire 建议使用强密码，包含至少 8 个大小写混合的字母数字字符，其中至少有一个数字字符。避免使用出现在词典中的单词。

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。如果您手动指定网络设置，则必须：

   - 输入采用点分十进制格式的 IPv4 地址，包括子网掩码。例如，可以指定子网掩码为 255.255.0.0。
   - 输入采用冒号分隔式十六进制格式的 IPv6 地址。对于 IPv6 前缀，请指定位数；例如，前缀长度为 112 位。

   在实施您的设置时， VMware 控制台可能会显示消息。

5. 根据设备部署方式指定检测模式。

   在实施您的设置时，VMware 控制台可能会显示消息。完成后，设备将提醒您将此设备注册至防御中心并显示 CLI 提示符。

6. 要使用 CLI 将设备注册至用于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。

   您必须使用防御中心来管理设备。如果不立即注册设备，您必须稍后登录并注册设备，才能将设备添加至防御中心。

将虚拟设备注册至防御中心

因为虚拟设备没有网络界面，所以您必须使用 CLI 将虚拟设备注册至防御中心，防御中心可以是物理设备也可以是虚拟设备。在初始设置过程中将设备注册至其防御中心最容易操作，因为此时您已登录至设备的 CLI。

要注册设备，请使用 `configure manager add` 命令。将设备注册至防御中心时，始终需要一个唯一的自生成字母数字注册密钥。这是一个指定的简单密钥，与许可证密钥不同。

在大多数情况下，必须与注册密钥一起提供防御中心的 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* 是为虚拟设备输入的注册密钥。

重要！ 使用 vSphere 客户端将虚拟设备注册至防御中心时，您必须使用管理防御中心的 IP 地址 （而非主机名）。

但是，如果设备与防御中心由一台网络地址转换 (NAT) 设备分，请与注册密钥一起输入唯一的 NAT ID，并指定 `DONTRESOLVE` 而非 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。

要将设备注册至防御中心，请执行以下操作：

访问： CLI 配置

1. 以拥有 CLI 配置 （管理员）权限的用户登录虚拟设备：
   - 如果您正在从 VMware 控制台执行初始设置，说明您已作为管理员用户登录，此用户拥有所需级别的访问权限。
   - 否则，使用 VMware 控制台登录设备，或者，如果您已配置了设备的网络配置，则 SSH 至设备的管理 IP 地址或主机名。

2. 在提示符中，使用 `configure manager add` 命令将设备注册至防御中心，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} 指定了防御中心的 IP 地址。如果防御中心不可直接访问，请使用 DONTRESOLVE。
   - *reg_key* 是将设备注册至防御中心所需的唯一的字母数字注册密钥。
   - *nat_id* 是在防御中心和设备之间的注册过程中使用的可选字母数字字符串。在主机名被设为 DONTRESOLVE 时为必填项。

3. 从设备注销。
4. 根据是否已设置管理防御中心以及防御中心的型号来执行下一步操作

   - 如果已设置防御中心，请登录其网络界面，使用 Device Management (**Devices > Device Management**) 页面添加设备。有关更多信息，请参阅《*Sourcefire 3D 系统用户指南*》中的“管理设备”章节。
   - 如果未设置防御中心，请参阅第 63 页的设置虚拟防御中心了解有关设置虚拟防御中心的详细信息，或者参阅《*Sourcefire 3D 系统安装指南*》了解有关设置物理防御中心的详细信息。

设置虚拟防御中心

设置虚拟防御中心所需的步骤取决于您在部署时采用的是 VI OVF 模板还是 ESXi OVF 模板：

- 如果已采用 VI OVF 模板进行部署并已使用设置向导，请使用配置 Sourcefire 所需的设置时设定的密码登录虚拟防御中心，然后使用 Sourcefire 3D 系统设定本地设备配置，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《*Sourcefire 3D 系统用户指南*》。
- 如果已采用 ESXi OVF 模板部署或在采用 VI OVF 模板部署时未配置 Sourcefire 所需的设置，则分两步设置虚拟防御中心。初始化虚拟防御中心后，在 VMware 控制台上运行脚本，使您将设备配置成可以在管理网络上进行通信。然后，使用管理网络上的计算机浏览至设备的网络界面，完成设置过程。

提示！ 如果您采用 ESXi OVF 模板部署虚拟防御中心并采用 VI OVF 模板部署所有虚拟设备，则可以通过只含一页的设置向导将所有设备同时注册至虚拟防御中心。有关详细信息，请参阅第 65 页的初始设置页面：虚拟防御中心。

有关详细信息，请参阅：

- 第 64 页的使用脚本配置虚拟防御中心网络设置
- 第 65 页的初始设置页面：虚拟防御中心

使用脚本配置虚拟防御中心网络设置

初始化新的虚拟防御中心后，您必须配置设置，以允许设备在管理网络上进行通信。在 VMware 控制台上运行脚本，完成此步骤。

Sourcefire 3D 系统可以为 IPv4 和 IPv6 管理环境提供双堆栈实施。首先，脚本提示您配置 （或禁用） IPv4 管理设置，然后配置 （或禁用） IPv6。对于 IPv6 部署，可以从本地路由器检索设置。您必须提供 IPv4 或 IPv6 管理 IP 地址、子网掩码或前缀长度以及默认网关。

按照脚本提示操作时，对于多选问题，选项在圆括号中列出，例如 (y/n)。默认值在方括号中列出，例如 [y]。按 Enter 键，确认选择某个选项。

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

1. 初始化完成后，使用 admin 作为用户名以及通过 VI OVF 模板进行部署时在设置向导中为管理员帐户指定的密码，在 VMware 控制台登录虚拟防御中心。

   如果您没有使用设置向导更改密码，或者正在使用 ESXi OVF 模板进行部署，请使用 Sourcefire 作为密码。

2. 在管理员提示符中，键入 sudo su -切换到根用户，然后再次键入密码 （如果系统提示的话）。

3. 在根提示符中，运行以下脚本：

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

4. 按照脚本的提示操作。

   首先配置 （或禁用） IPv4 管理设置，然后配置 IPv6。如果您手动指定网络设置，则必须：

   - 输入采用点分十进制格式的 IPv4 地址，包括子网掩码。例如，可以指定子网掩码为 255.255.0.0。
   - 输入采用冒号分隔式十六进制格式的 IPv6 地址。对于 IPv6 前缀，请指定位数；例如，前缀长度为 112 位。

5. 确认设置正确无误。

   如果未正确输入设置，请在提示符中键入 n，然后按 Enter 键。然后，您可以输入正确的信息。在实施您的设置时， VMware 控制台可能会显示消息。

6. 从设备注销。

7. 执行第 65 页的初始设置页面：虚拟防御中心，以使用防御中心的网络界面完成设置。

初始设置页面：虚拟防御中心

对于虚拟防御中心，您必须登录防御中心的网络界面并在设置页面指定初始配置选项，以完成设置过程。您必须更改管理员密码，指定网络设置 （如果尚未指定），并接受 EULA。

在设置过程中，您可以注册和许可设备。注册设备之前，您必须在此设备上完成设置过程，并将防御中心作为一个远程管理器添加，否则注册将失败。

要使用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

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

   系统将显示登录页面。

2. 使用 `admin` 作为用户名和采用 VI OVF 模板部署时在设置向导中为管理员帐户指定的密码登录。如果您未使用向导更改密码，请使用 `Sourcefire` 作为密码。

   系统将显示设置页面。请参阅以下各节，了解有关完成设置的详细信息：

   - 第 66 页的更改密码
   - 第 66 页的网络设置
   - 第 67 页的时间设置
   - 第 67 页的周期性规则更新导入
   - 第 68 页的周期性地理位置更新
   - 第 68 页的自动备份
   - 第 69 页的许可设置
   - 第 70 页的设备注册
   - 第 72 页的最终用户许可协议

3. 完成后，请点击 **Apply**。

   防御中心已根据您的选择配置。出现中间页面后，请以拥有管理员权限的管理员用户身份登录到网络界面。

4. 使用 Task Status 页面 (**System > Monitoring > Task Status**) 验证初始设置是否已成功完成。

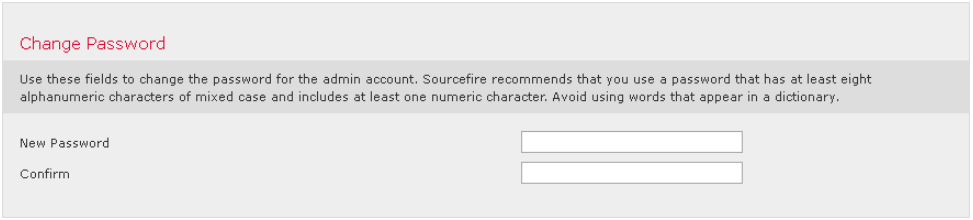
   页面每 10 秒钟自动刷新一次。在页面为任何初始设备注册和策略应用任务列出 **Completed** 状态前，保持监控此页面。在设置过程中，如果配置了入侵规则或地理位置更新，您也可以监控这些任务。

   防御中心随时可用。请参阅 《*Sourcefire 3D 系统用户指南*》，了解有关配置部署的详细信息。

5. 继续执行第 72 页的后续步骤。

更改密码

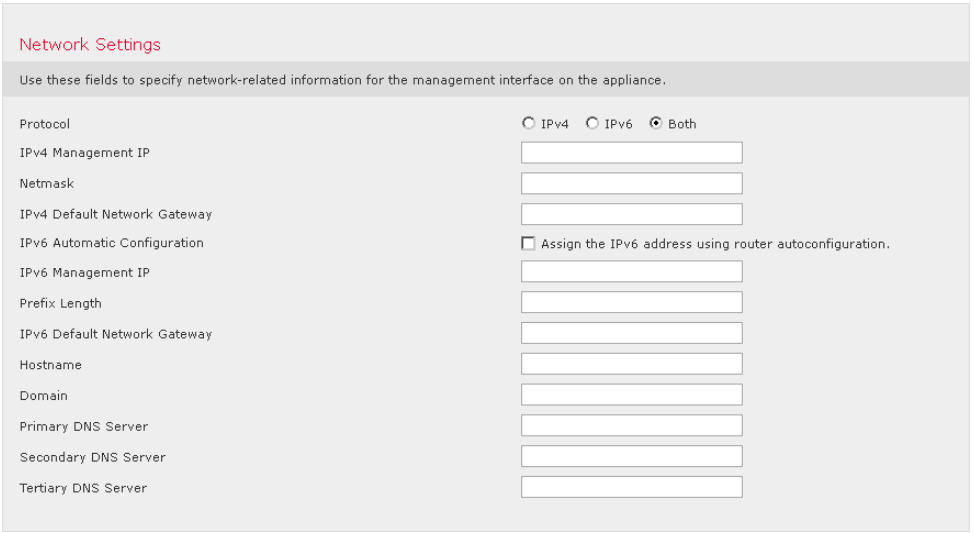
必须更改管理员帐户密码。此帐户拥有管理员权限，您无法将其删除。



Sourcefire 建议使用强密码，包含至少 8 个大小写混合的字母数字字符，其中至少有一个数字字符。避免使用出现在词典中的单词。

网络设置

防御中心的网络设置使防御中心能够在管理网络上进行通信。因为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。



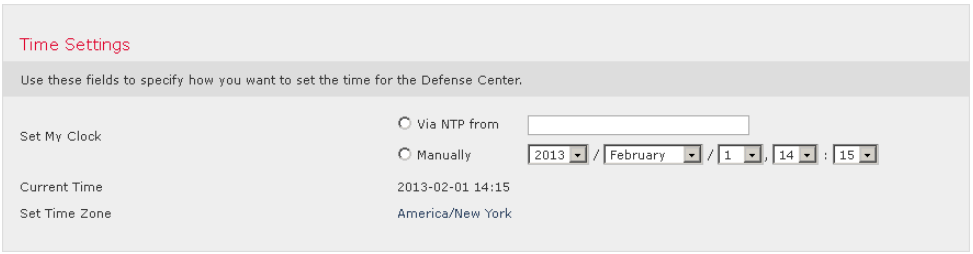
如果想更改预填充的设置，请记住， Sourcefire 3D 系统可以为 IPv4 和 IPv6 管理环境提供双堆栈实施。您必须指定管理网络协议 （**IPv4**、 **IPv6** 或**两者**）。根据您的选择，设置页面会显示不同的字段，您必须在这里设置 IPv4 或 IPv6 管理 IP 地址、子网掩码或前缀长度以及默认网关：

- 对于 IPv4，您必须设置点分十进制格式的地址和子网掩码 （例如，子网掩码为 255.255.0.0）。
- 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，您必须设置冒号分隔十六进制格式的地址和前缀中的位数 （例如：前缀长度为 112 位）。

您还可以指定最多三台 DNS 服务器，以及设备的主机名和域。

时间设置

您可以手动或通过来自 NTP 服务器的网络时间协议 (NTP) 为防御中心设置时间。



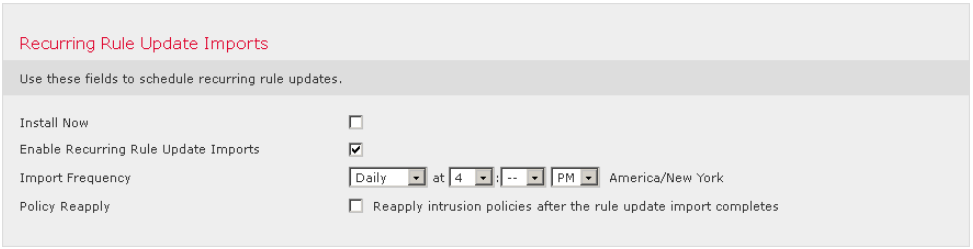
您也可以为管理员帐户指定用于本地网络界面的时区。点击当前时区，通过弹出窗口更改时区。

Sourcefire 建议您使用物理 NTP 服务器来设置时间。

周期性规则更新导入

随着新漏洞被获悉， Sourcefire 漏洞研究团队 (VRT) 会发布入侵规则更新。规则更新提供新的和已更新的入侵规则和预处理器规则、现有规则的修改后状态以及修改后的默认入侵策略设置。规则更新还可能删除规则，以及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， Sourcefire 建议您选择 **Enable Recurring Rule Update Imports**。



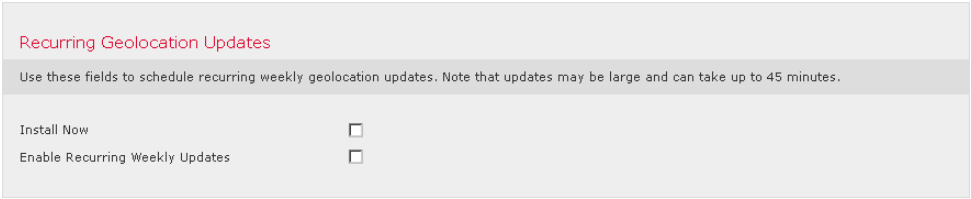
您可以指定 **Import Frequency**，以及将系统配置为在每次规则更新后执行入侵 **Policy Reapply**。要在初始配置过程中执行规则更新，请选择 **Install Now**。

重要！ 规则更新可能含有新的二进制文件。请确保下载和安装规则更新的过程符合安全策略。此外，规则更新文件可能比较大，所以，请务必在网络不繁忙的时段导入规则。

周期性地理位置更新

您可以使用防御中心查看与系统生成的事件相关的路由 IP 地址的地理信息，以及在控制面板和 Context Explorer 中监控地理位置统计信息。

防御中心的地理位置数据库 (GeoDB) 包含的信息包括 IP 地址的关联互联网服务提供商 (ISP)、连接类型、代理信息和精确位置。启用定期 GeoDB 更新可以确保系统使用最新的地理位置信息。如果您计划在部署中执行地理位置相关分析，Sourcefire 建议您选择 **Enable Recurring Weekly Updates**。



可以将 GeoDB 的更新频率指定为每周。点击时区，通过弹出窗口更改时区。要在初始配置过程中下载数据库，请选择 **Install Now**。

重要！ GeoDB 更新文件可能比较大，在下载后可能需要 45 分钟完成安装。所以请在网络不繁忙的时段更新 GeoDB。

自动备份

防御中心提供了存档数据机制，以便在发生故障时还原配置。在初始设置过程中，您可以选择 **Enable Automatic Backups**。

启用此设置可以创建定时任务，为防御中心上的配置创建每周备份。

许可设置

您可以许可各种功能，为贵公司创建最佳的 Sourcefire 3D 系统部署。防御中心上需要有 FireSIGHT 许可证，以执行主机、应用和用户发现。附加的型号特定许可证允许受管设备执行各种功能。由于架构和资源的限制，并非所有的许可证都可被应用至所有受管设备；请参阅第 8 页的了解虚拟设备功能和第 10 页的许可 Sourcefire 虚拟设备。

Sourcefire 建议您使用初始设置页面添加贵公司已购买的许可证。如果您现在不添加许可证，则在初始设置过程中注册的所有设备都将被作为未许可设备添加至防御中心；然后，您必须在初始设置过程结束后，单独许可每个设备。

提示！ 如果您重新创建了一个虚拟防御中心并使用了和已删除设备一样的 MAC 地址用于管理接口，则您可以使用旧许可。如果不能使用同一 MAC 地址 （例如，MAC 地址已被动态分配），请联系 Sourcefire 技术支持部门，获取新的许可证。

如果尚未获得许可证，请点击链接导航至 `https://keyserver.sourcefire.com/`，然后按照屏幕上的说明操作。您需要许可证密钥 （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密钥。

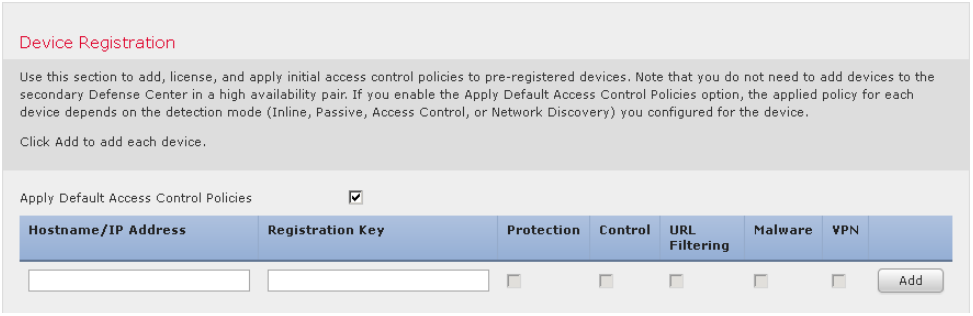
将许可证粘贴到文本框中，点击 **Submit License**，添加许可证。添加有效许可证后，页面将更新。您可以跟踪已添加的许可证。一次添加一个许可证。

Maximum 3D8250 Licenses				
Protection	Control	URL Filtering	Malware	VPN
5	5	0	0	5
Maximum Virtual Device 64bit Licenses				
Protection	Control	URL Filtering	Malware	VPN
5	5	0	5	0
Maximum Virtual DC 64bit Licenses				
FireSIGHT Host	FireSIGHT User			
50000	50000			

Type	Description	Expires
3D8250	5 Protection License(s)	Never
3D8250	5 Control License(s)	Never
3D8250	5 VPN License(s)	Never
Virtual Device 64bit	5 Malware License(s)	2013-09-16 18:58:01
Virtual Device 64bit	5 Control License(s)	Never
Virtual Device 64bit	5 Protection License(s)	Never
Virtual DC 64bit	50000 FireSIGHT Host, 50000 FireSIGHT User License(s)	Never

设备注册

虚拟防御中心可以管理 Sourcefire 3D 系统当前支持的任何物理或虚拟设备。您可以在初始设置过程中，将大部分预先注册的设备添加至防御中心。然而，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。



注册设备时，如果想将访问控制策略应用至正在注册的设备，请将 **Apply Default Access Control Policies** 复选框保持启用状态。请注意，您不能选择防御中心应用到每个设备的策略，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，如下表所列。

根据检测模式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，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。如果有已配置的接口，防御中心会应用默认的入侵防御策略，否则，防御中心应用默认的访问控制策略。

有关虚拟设备上检测模式的详细信息，请参阅第 59 页的使用 CLI 设置虚拟设备；对于物理设备，请参阅 《*Sourcefire 3D 系统安装指南*》。

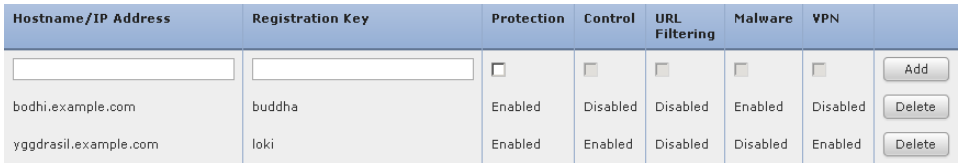
要添加设备，请键入其**Hostname**或 **IP Address**，以及在注册设备时指定的 **Registration Key**。请注意，这是一个指定的简单密钥，与许可证密钥不同。

然后，使用复选框将已许可的功能添加至设备。请注意，您只能选择已添加至防御中心的许可证。此外，有些许可证只有在您启用其他许可证之后才能被启用。例如，您只有在首次启用保护许可证后，才能在设备上启用控制许可证。

由于架构和资源的限制，并非所有的许可证都可被应用至所有受管设备。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，请参阅第 8 页的了解虚拟设备功能和第 10 页的许可 Sourcefire 虚拟设备。

重要！ 如果您启用了 **Apply Default Access Control Policies**，则必须在选择了 **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 （在这些情况下要求保护许可证）将无法应用。

启用许可后，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键入了错误的设备名称，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，如果同意遵守协议条款，请选择复选框。请确保您提供的所有信息正确无误，然后点击 **Apply**。

防御中心已根据您的选择配置。出现中间页面后，请以拥有管理员权限的管理员角色登录到网络界面。执行第 65 页的初始设置页面：虚拟防御中心中的3，以完成防御中心的初始设置。

后续步骤

完成虚拟设备的初始设置过程并验证设置成功后， Sourcefire 建议您完成管理任务，以更轻松地管理部署。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。有关以下各节描述的任何任务的详细信息，以及有关如何开始配置部署的详细信息，请参阅 《*Sourcefire 3D 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。 Sourcefire 建议您限制使用管理员帐户 （和管理员角色），以保障安全性及便于审核。

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。

系统包括 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。 Sourcefire 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。 Sourcefire 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。 Sourcefire 建议部署中的所有设备运行 Sourcefire 3D 系统的最新版本。如果您正在部署中使用它们，还应当安装最新的入侵规则更新、 VDB 和 GeoDB。

警告！ 更新 Sourcefire 3D 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。

第 6 章
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。 Sourcefire 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）同步至虚拟防御中心。为确保时间同步设置正确，请参阅《*Sourcefire 3D 系统用户指南*》中的“同步时间”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。有关可能会影响到性能的因素的列表，请参阅第 9 页的虚拟设备性能。要监控 ESXi 主机性能，您可以使用 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 网络门户和 vSphere 客户端查看并确认管理接口与感应接口的连接。

使用 VMware vCloud Director 网络门户

您可以使用 VMware vCloud Director 网络门户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 **My Cloud > VMs**，将鼠标停留在待查看的虚拟设备上，然后右键单击。

   系统将显示 Actions 窗口。

2. 在 Action 窗口中，点击 **Properties**。

   系统将显示 Virtual Machine Properties 窗口。

3. 在 Hardware 选项卡上，查看用于管理 NIC 和感应接口，以确认连接。

使用 vSphere 客户端

您可以使用 vSphere 客户端确认管理连接及感应接口是否已正确连接。

管理连接

在初始设置过程中，必须确保网络适配器在启动时连接。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：

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

在初始管理连接正常完成时，检查 /var/log/messages 目录查看以下消息：

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

感应接口

在初始设置过程中，必须确保感应接口在启动时连接。

为确保感应接口在启动时连接，请执行以下操作：

- 右键单击 vSphere 客户端中虚拟设备的名称，从出现的上下文菜单中选择 **Edit Settings**。在 Hardware 列表中，选择 **Network adapter 2** 和 **Network adapter 3**。确保使用中的各适配器的 **Connect at power on** 复选框已经选中。

您必须将虚拟设备感应接口连接至接受混杂模式流量的虚拟交换机或虚拟交换机组。否则，设备仅可检测广播流量。要确保感应接口能检测所有漏洞，请参阅第 54 页的配置虚拟设备感应接口。

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在传输流量。要打开虚拟设备的 VMware 控制台，请使用 VMware vCloud Director 网络门户或 vSphere 客户端。

要确保内联感应接口配置正确，请执行以下操作：

访问： CLI 配置

1. 在控制台中，以拥有 CLI 配置 （管理员）权限的用户身份登录。

   系统将显示 CLI 提示符。

2. 键入 `expert`，以显示外壳提示符。

3. 输入以下命令：`cat /proc/sf/sfe1000.*`

   系统将显示一个文本文件，该文件包含类似以下的信息：

```
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` 发送的数据包数量相匹配，且从 `eth1` 发送的数据包数量与 `eth2` 上接收的数据包数量相匹配。

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，您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 返回的消息表示，存在通过虚拟设备的内联接口集的连接。

获得帮助

如果您有任何关于 Sourcefire 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 支持网站，网址为：https://support.sourcefire.com/。
- 将问题发送至 Sourcefire 技术支持部门的邮箱：support@sourcefire.com。
- 致电 Sourcefire 支持部门，号码为：410.423.1901 或 1.800.917.4134。

感谢您使用 Sourcefire 产品。