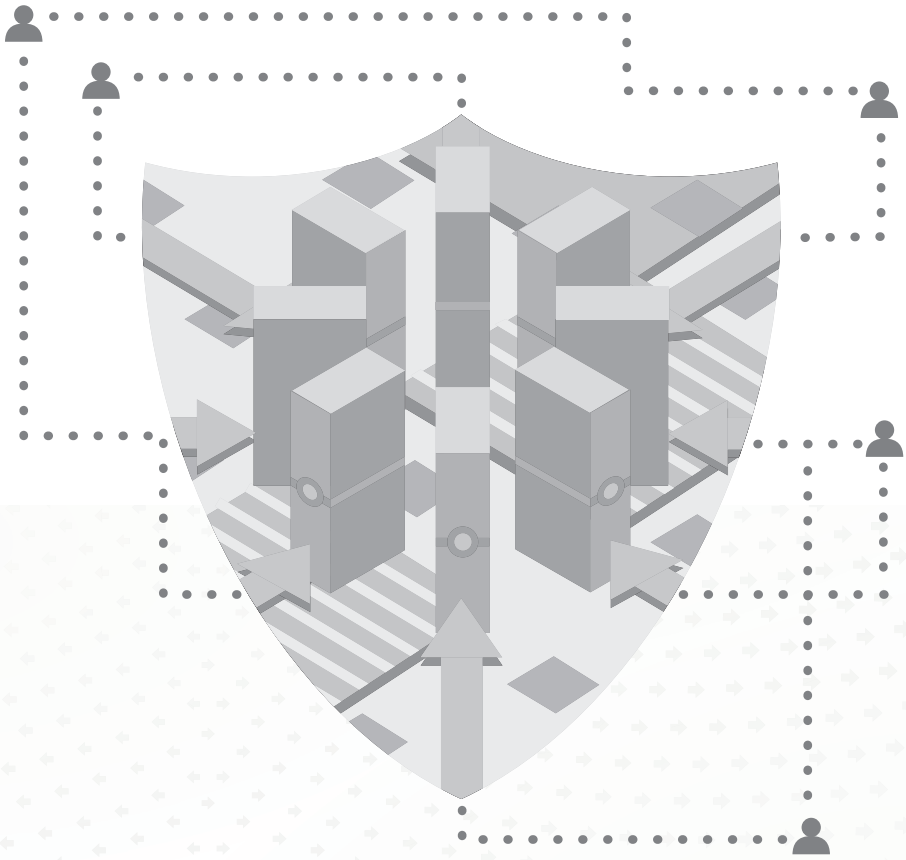
Sourcefire 3D 系统

安装指南

5.3 版本



SOURCEfire®

Sourcefire is now part of Cisco. CISCO

法律声明

免责声明

本文档及其提供的任何信息可能包括不准确之处或拼写错误。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。

2015-2-17 10:11

目录

目录

目录

目录

目录

目录

第 1 章

SOURCEFIRE 3D 系统简介

Sourcefire 3D® 系统结合了行业领先的网络入侵防护系统的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。您还可以在交换、路由或混合 （交换和路由）环境中使用 Sourcefire 设备提供服务；执行网络地址转换 (NAT)；以及在 Sourcefire 受管设备上的虚拟路由器之间，或从受管设备到远程设备或其他第三方 VPN 终端之间建立安全虚拟专用网络 (VPN) 隧道。

Sourcefire 防御中心® 为 Sourcefire 3D 系统提供了集中管理控制台和数据库资源库。网络段上安装的受管设备监控流量进行分析。

被动部署中的设备监控通过网络的流量，例如，使用交换机 SPAN、虚拟交换机或镜像端口。被动感应接口无条件地接收所有流量，并且这些接口上接收的任何流量都不会被重新传输。

可以通过内联部署中的设备保护网络免受可能影响网络上主机可用性、完整性或机密性的攻击。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。内联设备可以部署为简单的入侵防御系统。也可以使用其他方法配置内联设备来执行访问控制和管理网络流量。

本安装指南提供有关部署、安装和设置 Sourcefire 设备 （设备和防御中心）的信息。本安装指南还包含 Sourcefire 设备的硬件规格和安全与监管信息。

提示！ 您可以托管虚拟防御中心和设备，它们可以管理物理设备或被物理设备管理。但是，虚拟设备不支持任何基于硬件的系统功能：冗余、交换和路由等。有关详细信息，请参阅 《*Sourcefire 3D 系统虚拟安装指南*》。

接下来的主题介绍 Sourcefire 3D 系统并说明其主要组件：

Sourcefire 3D 系统设备

Sourcefire *设备*可以是流量感应受管*设备*或管理*防御中心*：

物理设备是提供一系列吞吐量和功能的具有容错能力的专用网络设备。防御中心用作这些设备的中心管理点并自动汇聚和关联这些设备生成的事件。每种物理设备类型都有几种*型号*；这些型号进一步分为不同的*系列*和*类别*。

许多 Sourcefire 3D 系统功能与设备相关。有关详细信息，请参阅以下各节：

防御中心

防御中心为 Sourcefire 3D 系统部署提供了集中管理点和事件数据库。防御中心（可以是物理或虚拟防御中心）汇聚和关联入侵、文件、恶意软件、发现、连接和性能数据。借助此功能，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
- 使用表、图形和图表显示事件和上下文信息
- 运行状况与性能监控
- 外部通知和警报
- 关联、危害表现以及实时威胁响应的补救措施功能
- 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连续性。

受管设备

物理 Sourcefire 设备是提供一系列吞吐量的具有容错能力的专用网络设备。您也可以托管虚拟设备。被动部署的设备有助于深入了解网络流量。采用内联部署时，可以基于多个条件使用 Sourcefire 设备影响流量。必须通过防御中心管理 Sourcefire 设备。

根据型号和许可证，受管设备：

- 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包括应用、用户、 URL、 IP 地址信誉和入侵或恶意软件检查结果的其他标准阻止或允许网络通信
- 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），有助于确保运行连续性和堆栈，整合多种设备的资源

了解设备系列、型号和功能

两个系列的物理设备以及虚拟设备上提供 5.3 版本 Sourcefire 3D 系统。许多 Sourcefire 3D 系统功能与设备相关。有关详细信息，请参阅：

- 第 11 页的2 系列设备
- 第 11 页的3 系列设备
- 第 12 页的虚拟设备
- 第 12 页的5.3 版本随附设备
- 第 13 页的按设备型号列出的支持的功能

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 系统功能集。

尽管 Sourcefire 不再发出新 2 系列设备，但您可以将 2 系列设备和防御中心重新映像到 5.3 版本。重新映像会导致设备上的**所有**配置和事件数据丢失。

警告！ 此外，您可以将特定配置和事件数据从 4.10.3 版本防御中心或 3D 感应器迁移到 5.2 版本防御中心，然后升级到 5.3 版本。有关详细信息，请参阅 5.2 版本的《*Sourcefire 3D 系统迁移指南*》。

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 系列设备都是 3 系列设备。 8000 系列设备更强大并且支持 7000 系列设备不支持的一些功能。

虚拟设备

您可以在 VMware ESX/ESXi 和 VMware vCloud Director 托管环境中托管 64 位虚拟防御中心和设备。虚拟防御中心可以管理最多 25 台物理或虚拟设备；物理防御中心可以管理虚拟设备。

无论安装和应用的许可证如何，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。有关虚拟设备的详细信息，请参阅 《*Sourcefire 3D 系统虚拟安装指南*》。

5.3 版本随附设备

下表列出了5.3 版本 的 Sourcefire 3D 系统随附的 Sourcefire 设备。

5.3 版本 Sourcefire 设备

型号 / 类别	系列	类型
70xx 系列： • 3D7010/3D7020/3D7030	3 系列 （7000 系列）	设备
71xx 系列： • 3D7110/3D7120 • 3D7115/3D7125 • AMP7150	3 系列 （7000 系列）	设备
81xx 系列： • 3D8120/3D8130/3D8140 • AMP8150	3 系列 （8000 系列）	设备
82xx 系列： • 3D8250 • 3D8260/3D8270/3D8290	3 系列 （8000 系列）	设备
83xx 系列： • 3D8350 • 3D8360/3D8370/3D8390	3 系列 （8000 系列）	设备
虚拟设备	不适用	设备
3 系列防御中心： • DC750/DC1500/DC3500	3 系列	防御中心
虚拟防御中心。	不适用	防御中心

尽管 Sourcefire 在 2 系列设备上不提供 5.3 版本，但您可以将以下 2 系列设备和防御中心重新映像到 5.3 版本：

- 3D500、 3D1000 和 3D2000
- 3D2100、 3D2500、 3D3500、 3D4500
- 3D6500
- 3D9900
- DC500、 DC1000 和 DC3000

重新映像会导致设备上的**所有**配置和事件数据丢失。有关详细信息，请参阅第 176 页的将 Sourcefire 设备恢复至出厂默认设置。

按设备型号列出的支持的功能

许多 Sourcefire 3D 系统功能与设备相关。下表将系统的主要功能和支持这些功能的设备相匹配 （假设您已安装和应用了正确的许可证）。有关这些功能和许可证的简短摘要，请参阅第 13 页的按设备型号列出的支持的功能和第 19 页的授予 Sourcefire 3D 系统许可证。

基于设备的功能 （例如堆栈、交换和路由）的防御中心列指示防御中心是否能够管理和配置设备以执行其功能。例如，您可以使用 2 系列 DC1000 来管理 3 系列设备上的 NAT。

按设备型号列出的支持的功能

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
网络发现：主机、应用和用户	是	是	是	是	是	是
地理定位数据	是	DC1000 和 DC3000	是	是	是	是
入侵检测和防御 (IPS)	是	是	是	是	是	是
安全情报过滤	否	DC1000 和 DC3000	是	是	是	是
访问控制：基本网络控制	是	是	是	是	是	是
访问控制：应用	否	是	是	是	是	是

按设备型号列出的支持的功能 （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
访问控制：用户	否	DC1000 和 DC3000	是	是	是	是
访问控制：文本 URL	否	是	是	是	是	是
访问控制：按类别和信誉执行的 URL 过滤	否	DC1000 和 DC3000	是	是	是	是
文件控件：按文件类型	是	是	是	是	是	是
基于网络的高级恶意软件防护 (AMP)	否	DC1000 和 DC3000	是	是	是	是
FireAMP 集成	不适用	是	不适用	是	不适用	是
快速路径规则	3D9900	是	8000 系列	是	否	是
严格 TCP 实施	否	是	是	是	否	是
可配置旁路接口	是	是	受硬件限制的情况除外	是	否	是
分路模式	3D9900	是	是	是	否	是
交换和路由	否	是	是	是	否	是
NAT 策略	否	是	是	是	否	是
VPN	否	是	是	是	否	是
高可用性	不适用	DC1000 和 DC3000	不适用	DC1500 和 DC3500	不适用	否
设备堆栈	3D9900	是	3D8140、82xx 系列和 83xx 系列	是	否	是
设备集群	否	是	是	是	否	是

按设备型号列出的支持的功能 （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
集群堆栈	否	是	3D8140、82xx 系列和 83xx 系列	是	否	是
恶意软件存储包	否	DC1000 和 DC3000	是	是	否	否
交互式 CLI	否	否	是	否	是	否

3 系列设备机箱名称

下一节列出了 7000 系列和 8000 系列设备及其相应的机箱硬件代码。机箱代码显示在机箱外部的监管标签上，该代码是硬件认证和安全的正式参考代码。

7000 系列机箱名称

7000 系列机箱型号表列出了在全球销售的 7000 系列型号的机箱名称。

7000 系列机箱型号

3D 设备型号	硬件机箱代码
3D7010、 3D7020 和 3D7030	CHRY-1U-AC
3D7110 和 3D7120 （铜缆）	GERY-1U-8-C-AC
3D7110 和 3D7120 （光纤）	GERY-1U-8-FM-AC
3D7115、 3D7125 和 AMP7150	GERY-1U-4C8S-AC

8000 系列机箱名称

8000 系列机箱型号表列出了在全球销售的 3 系列型号的机箱名称。

8000 系列机箱型号

3D 设备型号	硬件机箱代码
3D8120、 3D8130、 3D8140 和 AMP8150（交流电源）	CHAS-1U-AC
3D8120、 3D8130、 3D8140 和 AMP8150（直流电源）	CHAS-1U-DC
3D8120、 3D8130、 3D8140 和 AMP8150（交流或直流电源）	CHAS-1U-AC/DC
3D8250、 3D8260、 3D8270 和 3D8290（交流电源）	CHAS-2U-AC
3D8250、 3D8260、 3D8270 和 3D8290（直流电源）	CHAS-2U-DC
3D8250、 3D8260、 3D8270 和 3D8290（交流或直流电源）	CHAS-2U-AC/DC
3D8350、 3D8360、 3D8370 和 3D8390（交流或直流电源）	PG35-2U-AC/DC

Sourcefire 3D 系统组件

以下各节介绍一些有利于公司安全的 Sourcefire 3D 系统重要功能、可接受的使用策略和流量管理策略。

提示！ 很多 Sourcefire 3D 系统功能都取决于设备型号、许可证和用户角色。Sourcefire 文档根据需要概述了每个功能和任务的要求。

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和整合多个物理设备的处理资源：

- 防御中心高可用性可以指定冗余 DC1000、DC1500、DC3000 或 DC3500 防御中心以管理设备。
- 设备堆栈可以通过将二者连接到堆栈配置中的四台物理设备来增加网段上检查的流量。
- 设备集群让您能够在两个或多个 3 系列设备或堆栈之间实现网络功能和配置数据的冗余。

网络流量管理

利用 Sourcefire 3D 系统的网络流量管理功能可将 3 系列设备用作公司网络基础设施的一部分。您可以：

- 配置第 2 层部署，以在两个或多个网段之间执行数据包交换
- 配置第 3 层部署，以在两个或多个接口之间路由流量
- 执行网络地址转换 (NAT)
- 构建从受管设备到远程设备或其他第三方 VPN 终端的安全 VPN 隧道

FireSIGHT

FireSIGHT™ 是 Sourcefire 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的发现和感知技术，用以提供对网络的完整展现。

可以使用防御中心的网络界面来查看和分析 FireSIGHT 收集的数据。还可以使用此数据来帮助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，对网络上的主机生成和跟踪危害表现信息。

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。在访问控制过程中，安全情报功能可以将特定 IP 地址拉入黑名单，即拒绝这些地址之间的往来流量，再对流量进行更深入的分析。

在执行安全情报过滤后，您可以定义目标设备可以处理哪些流量以及如何处理，包括从简单的 IP 地址匹配到涉及不同用户、应用、端口和 URL 的复杂方案。您可以信任、监控或阻止流量，或者执行进一步分析，例如：

- 入侵检测和防御
- 文件控制
- 文件跟踪和基于网络的高级恶意软件防护 (AMP)

入侵检测和防御

入侵检测和防御是集成到访问控制中的基于策略的功能，可以监控网络流量以确定安全违例，并且，在内联部署中阻止或修改恶意流量。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、分析和 （可选）阻止网络流量中的文件 （包括恶意软件文件）传输。

文件控制是集成到访问控制中的基于策略的功能，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。

基于网络的高级恶意软件防护 (AMP) 允许系统检查特定类型的文件中的网络流量是否存在恶意软件。在受管设备检测到这些文件类型中的一种时，它可将文件存储到其硬盘驱动器或恶意软件存储包进行手动分析。无论设备是否存储文件，它都可以将文件提交到云进行动态分析。防御中心从 Sourcefire 云获取文件的性质。受管设备使用此信息跟踪文件，并随后阻止或允许文件通过。

FireAMP 是 Sourcefire 的基于终端的企业级 AMP 解决方案。如果公司有 FireAMP 订用，个人用户可以在计算机或移动设备 （又叫做终端）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。这样，您就可以使用防御中心查看公司中终端上的恶意软件检测和隔离，以及跟踪恶意软件的轨迹。

网络文件轨迹功能可以跟踪网络中的文件传输路径。系统使用 SHA-256 哈希值跟踪文件。每个文件都有一个关联的轨迹映射，其中包含文件随着时间推移进行的传输的直观显示以及有关该文件的其他信息。

应用编程接口

有几种方法可以使用应用编程接口 (API) 来与系统交互：

- 事件流转换器 (eStreamer) 可以将几种事件数据从 Sourcefire 设备传输至定制开发的客户端应用。
- 数据库访问功能可以在防御中心上使用支持 JDBC SSL 连接的第三方客户端查询几个数据库表。
- 主机输入功能可以使用脚本或命令行文件从第三方源导入数据，从而增加网络映射中的信息。
- 补救措施是当满足网络上的某些条件时，防御中心可以自动启动的程序。这不仅可以在您无法立即处理攻击时自动减轻攻击，还可以确保系统仍然符合组织安全策略。

授予 Sourcefire 3D 系统许可证

您可以许可各种功能，以便为贵公司创建优化的 Sourcefire 3D 系统部署。您必须使用防御中心控制自身和其所管理的设备的许可证。

Sourcefire 建议您在防御中心的初始设置期间添加公司购买的许可证。否则，您在初始设置期间注册的所有设备都将作为未授权设备添加到防御中心。在初始设置过程结束后，您必须逐一对每台设备启用许可证。有关详细信息，请参阅第 77 页的设置Sourcefire 3D 系统设备。

购买的每一台防御中心都随附有 FireSIGHT 许可证，执行主机、应用和用户发现时需要该许可证。防御中心上的 FireSIGHT 许可证还确定利用防御中心及其受管设备监控的单独的主机数目和用户数目，以及可以用于执行用户控制的用户数目。FireSIGHT 主机和用户许可证限制特定于型号，如下表所示。

FireSIGHT 限制 （按防御中心型号）

防御中心型号	FireSIGHT 主机和用户限制
DC500	1000 （无用户控制）
DC750	2000
DC1000	20,000
DC1500	50,000
DC3000	100,000
DC3500	300,000

如果防御中心之前运行的是 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。有关详细信息，请参阅第 21 页的使用旧版 RNA 主机和 RUA 用户许可证。

额外的特定于型号的许可证允许受管设备执行各种功能，如下所示：

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。它还允许设备执行交换和路由（包括 DHCP 中继）、 NAT，并且允许集群设备和堆栈。控制许可证要求具备保护许可证。

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来确定哪些流量可以流经网络。URL 过滤许可证要求具备保护许可证。

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，检测并阻止通过网络传输的文件中的恶意软件。它还允许查看其轨迹，跟踪通过网络传输的文件。恶意软件许可证要求具备保护许可证。

VPN

VPN 许可证允许在 Sourcefire 受管设备上的虚拟路由器之间或从受管设备到远程设备或其他第三方 VPN 终端之间构建安全 VPN 隧道。VPN 许可证要求具备保护和控制许可证。

由于架构和资源限制，并非所有的许可证均可应用于所有受管设备。一般而言，无法许可设备不支持的功能，请参阅第 13 页的按设备型号列出的支持的功能。

下表汇总了可以添加到防御中心和应用于每个设备型号的各种许可证。防御中心行（用于除 FireSIGHT 外的所有许可证）指示防御中心是否能够使用这些许可证管理设备。例如，您可以使用 2 系列 DC1000 创建使用3 系列 的 VPN 部署，但是，无论 DC500 管理的设备如何，您都不能使用它执行基于类别和信誉的 URL 过滤。此外，空白单元意味着许可证不受支持，而 n/a 表示与受管设备无关的基于防御中心的许可证。

按型号列出的受支持的许可证

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	是	是	是	是	是
虚拟设备	不适用	是	不支持硬件功能	是	是	否
DC500 2 系列防御中心	是	无安全情报	无用户控制	否	否	是

按型号列出的受支持的许可证 （续）

型号	FIRESIGHT	保护	控制	URL 过滤	恶意软件	VPN
DC1000/3000 2 系列防御中心	是	是	是	是	是	是
DC750/1500/3500 3 系列防御中心	是	是	是	是	是	是
虚拟防御中心。	是	是	是	是	是	是

除了表中的信息以外，请注意：

- 2 系列设备自动具有除安全情报过滤以外的保护功能。
- 虽然您可以在虚拟设备上启用控制许可证，但虚拟设备不支持此许可证授权的任何基于硬件的功能，例如，交换或路由。
- 虽然 DC500 可以管理具有保护和控制许可证的设备，但您无法执行安全情报过滤或用户控制。

有关许可的详细信息，请参阅《*Sourcefire 3D 系统用户指南*》中的“许可 Sourcefire 3D 系统”一章。

使用旧版 RNA 主机和 RUA 用户许可证

在 4.10.x 版本的 Sourcefire 3D 系统中， RNA 主机和 RUA 用户功能许可证分别确定监控的主机和用户限制。如果防御中心之前运行 4.10.x 版本，您可能可以使用旧版主机和用户许可证代替 FireSIGHT 许可证。

使用旧版许可证的 5.3 版本防御中心将 RNA 主机限制用作 FireSIGHT 主机限制，并将 RUA 用户限制用作 FireSIGHT 用户和受控访问用户限制。 FireSIGHT 主机许可证限制健康模块对于许可的限制适当发出警报。

请注意， RNA 主机和 RUA 用户限制是累积的。也就是说，您可以将每种类型的多个许可证添加到防御中心，以监控许可证允许的主机总数或用户总数。

如果以后添加 FireSIGHT 许可证，防御中心使用较高的限制。例如，DC1500 上的 FireSIGHT 许可证支持多达 50,000 台主机和用户。如果 4.10.x 版本 DC1500 上的 RNA 主机限制大于 50,000，在运行 5.3 版本的同一台防御中心上使用该旧版主机许可证会给您提供较高的限制。为方便您使用，网络界面仅显示代表更高限制的许可证。

重要！ 由于 FireSIGHT 许可证限制与防御中心的硬件能力相匹配，因此 Sourcefire **不**建议在使用旧版许可证时超过该限制。要获得指导，请与 Sourcefire 支持部门联系。

由于没有从 4.10.x 版本到 5.3 版本的更新路径，因此您必须使用 ISO 映像“恢复”防御中心。请注意，重新映像会导致设备上的**所有**配置和事件数据都丢失。您**无法**在重新映像后将此数据导入设备。有关详细信息，请参阅第 176 页的将 Sourcefire 设备恢复至出厂默认设置。

重要！ 应当仅在维护时段内重新映像设备。重新映像会将内联部署中的设备重置为非旁路配置，并中断网络上的流量，直到您重新配置旁路模式。有关详细信息，请参阅第 177 页的恢复过程中的流量。

在恢复过程中，系统会提示您删除许可证和网络设置。请保留这些设置，尽管如果您意外删除了它们，以后您还可以重新添加。请注意， 5.3 版本防御中心无法管理 4.10.x 版本设备。但是，您可以将受支持的 4.10.x 版本设备恢复并更新到最新版本。有关详细信息，请参阅第 176 页的将 Sourcefire 设备恢复至出厂默认设置。

安全、互联网访问和通信端口

为了保护防御中心，必须将防御中心安装到受保护的内部网络中。虽然防御中心配置为仅提供必需的服务和端口，但是您必须确保攻击无法从防火墙外部影响到该防御中心。

如果防御中心和受管设备位于同一个网络，您可以将设备上的管理接口连接到与防御中心相同的受保护内部网络。这使您可以安全地从防御中心控制设备并汇聚在受管设备的网段生成的事件数据。通过使用防御中心的过滤功能，您可以分析和关联通过网络发送的攻击中的数据，以评估安全策略的实施情况。

然而，请注意， Sourcefire 设备配置为直接连接到互联网。 Sourcefire 3D 系统的特定功能需要此直接连接，而其他功能支持使用代理服务器。此外，系统需要某些端口保持打开状态以进行基本的设备内部通信，以及让您能够访问设备的网络界面。默认情况下，会打开若干其他端口以允许系统利用附加功能和功能。

有关详细信息，请参阅：

- 第 22 页的互联网访问要求
- 第 24 页的打开通信端口要求

互联网访问要求

默认情况下， Sourcefire 设备配置为直接连接到互联网。 Sourcefire 3D 系统的特定功能需要此直接连接，而其他功能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”一章。

提示！ 您可以将系统软件、入侵规则、 GeoDB 和 VDB 更新手动上传到设备中。

为确保业务连续性，高可用性对中的两台防御中心均必须能够访问互联网。为获取特定功能，主要防御中心联系互联网，然后在同步过程中与辅助防御中心共享信息。因此，如果主要防御中心发生故障，您应该将辅助防御中心提升为主要防御中心，如《*Sourcefire 3D 系统用户指南*》中的“管理设备”一章所述。

下表列出了 Sourcefire 3D 系统的互联网访问要求。

Sourcefire 3D 系统互联网访问要求

为了 ...	互联网访问需要 ...	高可用性注意事项	代理？
RSS 源控制面板构件	从外部源 （包括 Sourcefire）下载 RSS 源数据。	源数据未同步。	是
安全情报源	从外部源 （包括 Sourcefire 情报源）下载安全情报源数据。	主要防御中心下载源数据并与辅助防御中心共享源数据。在主要防御中心发生故障的情况下，您必须交换角色。	是
URL 过滤数据	下载基于云的 URL 类别和信誉数据用于访问控制，并查找未归类的 URL。	主要防御中心下载 URL 过滤数据并与辅助防御中心共享该数据。在主要防御中心发生故障的情况下，您必须交换角色。	是
恶意软件云查找 （已许可恶意软件功能）	执行云查找以确定在网络流量中检测到的文件是否包含恶意软件。	尽管文件策略已同步，但是成对的防御中心仍旧独立执行云查找。	是
动态分析	将文件提交到云进行恶意软件分析。	尽管文件策略已同步，但是成对的防御中心独立向云查询提交进行恶意软件分析的文件。	是
FireAMP 集成 （FireAMP 订用）	从 Sourcefire 云接收基于终端的恶意软件事件。	云连接未同步。在两台防御中心上配置云连接。	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调度下载到设备中。	规则、 GeoDB 和 VDB 更新已同步；系统更新未同步。下载更新的所有设备必须能够访问互联网。	是
使用 IP 地址上下文菜单获取 whois 信息	获取 whois 信息。	请求 whois 信息的任何设备必须能够访问互联网。	是

打开通信端口要求

Sourcefire 3D 系统需要端口 443 （入站）和 8305 （入站和出站）保持打开状态以用于基本的设备内部通信，以及让您能够访问设备的网络界面。

默认情况下，会打开若干其他端口以允许系统利用附加功能和功能。下表列出了这些端口。请注意，默认情况下在端口 67 和 68 上禁用 DHCP。

Sourcefire 3D 系统打开通信端口要求

端口	说明	协议	方向	打开端口以 ...
22	SSH/SSL	TCP	双向	可以建立到设备的安全远程连接。
25	SMTP	TCP	出站	从设备发送邮件通知和警报。
53	DNS	TCP	出站	使用 DNS。
67 和 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；用于自动更新。 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并下载 URL 过滤信息。
161 和 162	SNMP	UDP	双向 (161)；出站 (162)	如果启用 SNMP 轮询 （入站）和 SNMP 陷阱 （出站），则提供访问。
389 和 636	LDAP	TCP	出站	跟踪用户活动和用于身份验证。
443	HTTPS/AMPQ	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、安全情报源和基于终端的 (FireAMP) 恶意软件事件。 通过端口 443 的连接还允许防御中心进行云查找，以确定在网络流量中检测到的文件是否包含恶意软件、查询云以获取动态分析信息和跟踪文件的轨迹。 通过端口 443 的连接允许受管设备将文件提交到云进行动态分析。
514	系统日志	UDP	出站	向远程系统日志服务器发送警报。

Sourcefire 3D 系统打开通信端口要求 （续）

端口	说明	协议	方向	打开端口以 ...
623	SOL/LOM	UDP	双向	可以使用 Serial Over LAN (SOL) 连接在 3 系列设备上执行无人值守管理 (LOM)。
1500 和 2000	数据库访问	TCP	入站	访问防御中心 （如果启用了外部数据库访问）。
1812 和 1813	RADIUS	UDP	出站或双向	使用 RADIUS。添加入站访问可以确保 RADIUS 身份验证和记帐功能正常工作。 端口 1812 和 1813 是默认端口，但是，您可以配置 RADIUS 改为使用其他端口。有关详细信息，请参阅 《*Sourcefire 3D 系统用户指南*》。
3306	Sourcefire 用户代理	TCP	入站	允许防御中心与 Sourcefire 用户代理之间进行通信。
8302	eStreamer	TCP	双向	使用 eStreamer 客户端。
8305	设备管理	TCP	双向	防御中心和受管设备之间进行通信。**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进行通信。
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，以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轨迹。

预配置设备

您可以在一个中心位置预配置多台设备和防御中心，以便稍后用于其他站点的部署。有关预配置设备的注意事项，请参阅第 242 页的预配置 Sourcefire 设备。

第 2 章
了解部署

可以部署 Sourcefire 3D 系统以满足每个独特网络架构的需求。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存储库。设备安装在网段上，收集流量连接用于分析。

被动部署中的设备使用交换机 SPAN、虚拟交换机或镜像端口监控网络上传输的流量，以收集与流经网络的流量性质相关的数据。内联部署中的设备可让您监控网络，以防可能影响到网络上的主机的可用性、完整性或机密性的攻击。设备可在内联、交换、路由或混合 （2 层/3 层）环境中部署。

要了解有关部署选项的详细信息，请参阅以下各节：

- 第 27 页的了解部署选项说明设计部署时需要考虑的一些因素。
- 第 27 页的了解接口说明不同接口之间的差别以及这些接口在部署中的作用。
- 第 30 页的将设备连接至网络介绍如何在部署中使用集线器、SPAN 和网络分路器。
- 第 34 页的部署选项介绍基本部署并确定该部署内的主要功能位置。
- 第 39 页的使用访问控制进行部署介绍在内联部署中使用访问控制的优势。
- 第 43 页的使用多端口受管设备说明在网络部署中如何将受管设备用于多个网络或用作虚拟路由器或虚拟交换机。
- 第 46 页的复杂的网络部署介绍高级部署方案 （例如，使用 VPN 或具有多个入口点）。

有关部署的额外信息，请参阅 《*最佳实践指南*》（可向 Sourcefire 销售部门索取）。

了解部署选项

部署决策取决于多种因素。回答下列问题有助于您了解网络易受攻击的方面以及确定入侵检测和防御需求：

- 您是否采用被动或内联接口部署受管设备？您的设备是否支持多种接口，一些是被动接口，另一些是内联接口？有关详细信息，请参阅第 27 页的了解接口。
- 您准备通过哪种方式将受管设备连接至网络？集线器？分路器？交换机上的生成端口？虚拟交换机？有关详细信息，请参阅第 30 页的将设备连接至网络。
- 您是想检测网络中的每个攻击，还是只了解穿透防火墙的攻击？网络上是否存在特定资产，例如，财务、会计、或人事记录、生产代码或其他需要特殊安全策略的敏感受保护信息？有关详细信息，请参阅第 34 页的部署选项。
- 您是否为远程员工提供 VPN 或调制解调器访问？您是否有也需要部署 IPS 的远程办公室？您是否雇用合同工或其他临时员工？他们是否仅限于访问特定网段？您是否将将您的网络与客户、供应商或业务合作伙伴等其他组织的网络集成在一起？有关详细信息，请参阅第 46 页的复杂的网络部署。

了解接口

以下各节介绍不同接口对 Sourcefire 3D 系统能力的影响。除被动和内联接口外，您还可以使用路由、交换及混合接口。有关详细信息，请参阅以下各节：

- 第 27 页的被动接口
- 第 28 页的内联接口
- 第 29 页的交换接口
- 第 29 页的路由接口
- 第 30 页的混合接口

被动接口

许可证：任意
支持的设备：任意

您可以配置被动 IPS 部署，以使用交换机 SPAN、虚拟交换机或镜像端口监控网络上传输的流量，从而允许从交换机上的其他端口复制流量。被动接口允许您在不参与网络流量传输的情况下检查网络内部的流量。如果在被动部署中配置系统，系统将不能执行某些操作，例如，阻止流量或流量整形。被动接口无条件地接收所有流量并且不会重新传输接收到的流量。

您可以将受管设备上的一个或多个物理端口配置为被动接口。有关详细信息，请参阅第 30 页的将设备连接至网络。

内联接口

许可证：任意
支持的设备：任意

您可以将两个端口绑定在一起，以透明方式在网段上配置内联 IPS 部署。内联接口允许您将设备安装在任何网络配置中，无需配置相邻网络设备。内联接口无条件地接收所有流量，然后重新传输在这些接口上接收的、除明确丢弃的流量以外的所有流量。

您可以将受管设备上的一个或多个物理端口配置为内联接口。您必须将一对内联接口分配至一个内联集，它们才能处理内联部署中的流量。

重要！如果将一个接口配置为内联接口，该接口网络模块上的相邻端口会自动成为内联接口以完成配对。

可配置旁路内联集允许您选择在硬件完全无法工作的情况下 （例如，设备断电）如何处理流量。您可以确定，连接性在一个网段上非常重要，但是，在另一个网段上，则不允许未经检查的流量通过。您可以使用可配置旁路内联集，通过以下任一方式管理网络流量：

- *旁路*：将一个接口对配置为旁路，如果设备出现故障，允许所有流量通过。流量绕过设备及设备执行的任何检查或其他处理。旁路允许未经检查的流量通过整个网段，但是可确保保持网络连接。
- *非旁路*：将一个接口对配置为非旁路，如果设备出现故障，将停止所有流量。到达故障设备的流量不会进入设备。非旁路不允许未经检测的流量通过网络，但是如果设备出现故障，网段将失去连接。在网络安全比流量丢失问题更为重要的部署情境中，请使用非旁路接口。

可将内联集配置为旁路，以确保在设备发生故障时能够继续传输流量。可将内联集配置为非旁路，以在设备发生故障时停止流量。请注意，重新映像会将处于旁路模式下的设备重置为非旁路配置并中断网络上的流量，直至您重新配置旁路模式。有关详细信息，请参阅第 177 页的恢复过程中的流量。

所有设备均包含可配置旁路接口。 8000 系列设备还可能包含具有无法配置为旁路的接口的网络模块。有关网络模块的详细信息，请参阅第 163 页的8000 系列模块。

高级选项因设备而异，可能包括分路模式、传播链路状态、透明内联模式和严格 TCP 模式。有关如何配置内联接口集的信息，请参阅 《*Sourcefire 3D 系统用户指南*》中的“配置内联集”。有关使用内联接口的详细信息，请参阅第 30 页的将设备连接至网络。

交换接口

许可证：控制
支持的设备：3 系列

可以在第 2 层部署中的受管设备上配置交换接口，以在两个或更多网络之间提供数据包交换。还可以将受管设备上的虚拟交换机配置为充当独立的广播域，从而将网络划分为多个逻辑段。虚拟交换机使用来自主机的媒体访问控制 (MAC) 地址确定数据包的发送目标。

交换接口可以是物理或逻辑配置：

- *物理交换接口*是已配置交换功能的物理接口。物理交换接口用于处理未标记的 VLAN 流量。
- *逻辑交换接口*是物理接口与 VLAN 标记之间的关联。逻辑接口用于处理带有指定 VLAN 标记的流量。

虚拟交换机可以作为独立的广播域，从而将网络划分为多个逻辑段。虚拟交换机使用来自主机的媒体访问控制 (MAC) 地址确定数据包的发送目标。配置虚拟交换机时，交换机首先通过交换机上的每个可用端口广播数据包。随着时间的推移，交换机通过带标记的返回流量了解哪些主机位于与每个端口连接的网络上。

您可以将设备配置为虚拟交换机并使用其余接口连接至想要监控的网段。要在设备上使用虚拟交换机，请创建物理交换接口，然后按照《*Sourcefire 3D 系统指南*》中有关“设置虚拟交换机”的说明进行操作。

路由接口

许可证：控制
支持的设备：3 系列

可以在第 3 层部署中的受管设备上配置路由接口，以使受管设备能够在两个或更多接口之间路由流量。要路由流量，必须为每个接口分配一个 IP 地址并将接口分配给虚拟路由器。

可以将路由接口配置为可与网关虚拟专用网络 （网关 VPN）或网络地址转换 (NAT) 配合使用。有关详细信息，请参阅第 38 页的部署网关 VPN和第 39 页的使用基于策略的 NAT 进行部署。

还可以将系统配置为根据目标地址作出数据包转发决策，并据此路由数据包。配置为路由接口的接口将接收和转发第 3 层流量。路由器将根据转发条件从传出接口获取目标，访问控制规则将指定将应用的安全策略。

路由接口可以具有物理或逻辑配置：

- *物理路由接口*是已配置路由功能的物理接口。物理路由接口用于处理未标记的 VLAN 流量。
- *逻辑交换接口*是物理接口与 VLAN 标记之间的关联。逻辑接口用于处理带有指定 VLAN 标记的流量。

要在第 3 层部署中使用路由接口，必须配置虚拟路由器并为其分配路由接口。虚拟路由器是路由第 3 层流量的一组路由接口。

您可以将设备配置为虚拟路由器，并使用其余接口连接至想要监控的网段。您还可以启用严格 TCP 实施，以实现最高的 TCP 安全性。要在设备上使用虚拟路由器，请在设备上创建物理路由接口，然后按照《*Sourcefire 3D 系统用户指南*》中有关“设置虚拟路由器”的说明进行操作。

混合接口

许可证：控制
支持的设备：3 系列

可以在受管设备上配置逻辑混合接口，以便 Sourcefire 3D 系统能够在虚拟路由器和虚拟交换机之间桥接流量。如果在虚拟交换机的接口上接收到的 IP 流量的目标地址为关联混合逻辑接口的 MAC 地址，系统会将其作为第 3 层流量处理，并会根据目标 IP 地址来路由流量或对流量作出响应。如果系统接收到任何其他流量，则将其视为第 2 层流量处理并相应地进行交换。

要创建混合接口，请首先配置虚拟交换机和虚拟路由器，然后将配置好的虚拟交换机和虚拟路由器添加到混合接口。未同时与虚拟交换机和虚拟路由器关联的混合接口不可用于路由，也不会生成流量或对流量作出响应。

可以为混合接口配置网络地址转换 (NAT) 功能，以在网络间传输流量。有关详细信息，请参阅第 39 页的使用基于策略的 NAT 进行部署。

如果要在设备上使用混合接口，请在设备上定义一个混合接口，然后按照《*Sourcefire 3D 系统用户指南*》中有关“设置混合接口”的说明进行操作。

将设备连接至网络

您可以通过多种方式将受管设备连接至网络。使用被动或内联接口配置集线器或网络分路器，或者使用被动接口配置 SPAN 端口。以下各节介绍受支持的连接方法和布线注意事项：

- 第 31 页的使用集线器
- 第 31 页的使用 SPAN 端口
- 第 31 页的使用网络分路器
- 第 31 页的在铜缆端口接口上进行内联部署布线
- 第 34 页的特殊情况

使用集线器

以太网集线器是一种确保受管设备能监控网段上所有流量的简单方法。这种类型的绝大多数集线器都采用专用于此网段主机的 IP 流量并将其广播给连接此集线器的所有设备。将接口集连接至集线器可监控网段上所有传入和传出流量。使用集线器无法保证检测引擎能监控更高流量网络上的所有数据包。，因为可能发生数据包冲突。对于低流量的简单网络，不大可能存在这个问题。在高流量网络中，使用其他方法可能会有更好的结果。请注意，如果集线器出现故障或断电，网络连接将会断开。在简单网络中，网络将会断开。

某些设备作为集线器销售，但实际上其作用和交换机一样，并且不向各端口广播每个数据包。如果将受管设备连接至集线器后却未能监控所有流量，则可能需要购买其他集线器或使用带 SPAN 端口的交换机。

使用 SPAN 端口

许多网络交换机包含 SPAN 端口，该端口可对来自一个或多个端口的流量生成镜像文件。将接口集连接至 SPAN 端口，可以监控来自所有端口的合并流量，通常包括传入和传出流量。如果网络上的适当位置已有包括此功能的交换机，那么，几乎无需在受管设备以外再花额外成本即可在多个网段部署检测。在高流量网络中，此解决方案有其局限性。如果 SPAN 端口可处理 200Mbps，并且三个镜像端口都可以处理高达 100Mbps 的流量，则 SPAN 端口可能超出限额并丢弃数据包，从而降低受管设备的有效性。

使用网络分路器

网络分路器用于被动监控流量，而不会中断网络流量或更改网络拓扑。不同带宽都有现成可用的分路器，可用于分析网段的传入和传出数据包。由于大多数分路器都只能监控一个网段，因此，如果想要监控交换机八个端口中的两个端口，这个解决方案就不适用。可以在路由器和交换机之间安装分路器并访问流向交换机的完整 IP 数据流。

根据设计，网络分路器将传入和传出流量分为两个不同的数据流，通过两种不同的电缆进行传输。受管设备提供可将对话两端重新整合的多端口选项，以使解码器、预处理器和检测引擎能够对整个流量进行评估。

在铜缆端口接口上进行内联部署布线

如果在网络上部署内联设备并且想要使用设备的旁路功能在设备出现故障时保持网络连接，必须特别注意连接的布线方式。

如果利用支持光纤旁路的接口部署设备，除了要确保连接牢固并且电缆没有扭结之外，没有什么需要注意的特殊布线问题。但是，如果用铜缆端口接口而不是光纤网络接口部署设备，必须了解所使用设备的型号，因为不同型号的设备要使用不同的网卡。请注意，某些 8000 系列网络模块不支持旁路配置。

设备中的网络接口卡 (NIC) 功能支持叫做自动媒体依赖接口交叉 (Auto-MDI-X) 的一种功能，使网络接口自动配置是使用直通还是交叉以太网电缆连接另一个网络设备。设备和旁路特性表列出了各种设备及其是作为直通还是交叉连接旁路。

设备和旁路特性

设备	出故障时自动打开为 ...
3D500、 3D1000、 3D2000	直通
7000 系列	交叉
8000 系列	交叉

对于使用直通连接旁路的受管设备，请像在网络上已经部署设备一样正常连接设备。大多数情况下，应使用一根直通电缆和一根交叉电缆将设备连接至两个终端。

直通旁路连接布线

对于使用交叉连接旁路的受管设备，请像未部署设备一样正常连接设备。这种连接在设备断电的情况下应该仍能够正常工作。大多数情况下，应使用两根直通电缆将设备连接至两个终端。

交叉旁路连接布线

硬件旁路的有效配置表列出了硬件旁路配置中哪些情况下应使用交叉电缆，哪些情况下应使用直通电缆。请注意，第 2 层端口在部署中用作直通 (MDI) 终端，第 3 层端口在部署中用作交叉(MDIX) 终端。总交叉数 （电缆和设备）应为奇数，旁路才能正常工作。

硬件旁路的有效配置

终端 1	电缆	受管设备	电缆	终端 2
MDIX	=	=	=	MDI
MDI	X	=	=	MDI
MDI	=	=	X	MDI
MDI	=	=	=	MDIX
MDIX	=	X	=	MDIX
MDI	=	X	=	MDI
MDI	X	X	X	MDI
MDIX	X	X	=	MDI

重要！在硬件旁路的有效配置表中，= 表示直通电缆或受管设备旁路连接，X 表示交叉电缆或受管设备旁路连接。

请注意，每个网络环境都可能是独一无二的，其终端具有不同的 Auto-MDI-X 支持组合。要确定安装设备使用的电缆是否正确，最简单的办法是，首先在关闭设备的情况下用一根交叉电缆和一根直通电缆将设备分别连接至两个终端。确保两个终端之间可以通信。如果它们无法通信，则表示其中一根电缆类型不正确。将其中一根（且仅一根）电缆更换为其他类型 - 直通或交叉电缆。

在内联设备断电的情况下两个终端能够成功通信之后，打开设备电源。 Auto-MDI-X 功能可确保两个终端继续通信。请注意，如果必须更换内联设备，应重复确保终端能够与断电的新设备通信的过程，以防止原始设备与更换后的设备具有不同的旁路特性。

仅在您允许网络接口自动协商的情况下， Auto-MDI-X 功能才能正常工作。如果网络环境要求关闭 Network Interfaces 页面上的 Auto Negotiate 选项，必须为内联网络接口指定正确的 MDI/MDIX 选项。有关详细信息，请参阅 《*Sourcefire 3D 系统用户指南*》中的“配置内联接口”。

特殊情况

连接 8000 系列设备

8000 系列受管设备不支持半双工网络链路；它们也不支持连接的相对端之间存在速度或双工配置上的差异。为确保稳定的网络链路，必须在连接的两端自动协商或将两端设置为相同的静态速度。

更改远程控制台

如果在 70xx 系列设备上将远程控制台从物理串行端口改为无人值守管理或者从无人值守管理改为物理串行端口，可能需要重新启动设备两次，才会显示预期的 LILO 启动提示符。

部署选项

将受管设备部署在网段上后，可以使用入侵检测系统监控流量，或者使用入侵防御系统保护网络免遭威胁侵扰。

还可以将受管设备部署为可用作虚拟交换机、虚拟路由器或网关 VPN。此外，还可以使用策略来路由流量或控制对网络流量的访问。有关详细信息，请参阅以下各节：

- 第 34 页的使用虚拟交换机进行部署
- 第 36 页的使用虚拟路由器进行部署
- 第 37 页的使用混合接口进行部署
- 第 38 页的部署网关 VPN
- 第 39 页的使用基于策略的 NAT 进行部署
- 第 39 页的使用访问控制进行部署

使用虚拟交换机进行部署

许可证：控制
支持的设备：3 系列

可以通过将内联接口配置为交换接口，在受管设备上创建*虚拟交换机*。虚拟交换机为部署提供第 2 层数据包交换。高级选项包括设置静态 MAC 地址、启用生成树协议、启用严格 TCP 实施和在域级别丢弃网桥协议数据单元 (BPDU)。有关交换接口的信息，请参阅第 29 页的交换接口。

虚拟交换机必须包含两个或更多交换接口，用以处理流量。对于每个虚拟交换机，系统仅向配置为交换接口的一组端口交换流量。例如，如果您配置具有四个交换接口的虚拟交换机，当系统通过一个端口接收流量数据包时，它只会将这些数据包广播到交换机的其余三个端口。

要将虚拟交换机配置为允许流量通过，可在物理端口上配置两个或更多交换接口，添加并配置虚拟交换机，然后将配置好的虚拟交换机分配给这些交换接口。系统会丢弃在没有对应交换接口的外部物理接口上接收到的所有流量。如果系统接收到没有 VLAN 标记的数据包，且您未为该端口配置物理交换接口，系统将丢弃该数据包。如果系统接收到 VLAN 标记的数据包，且您未配置逻辑交换接口，系统将丢弃该数据包。

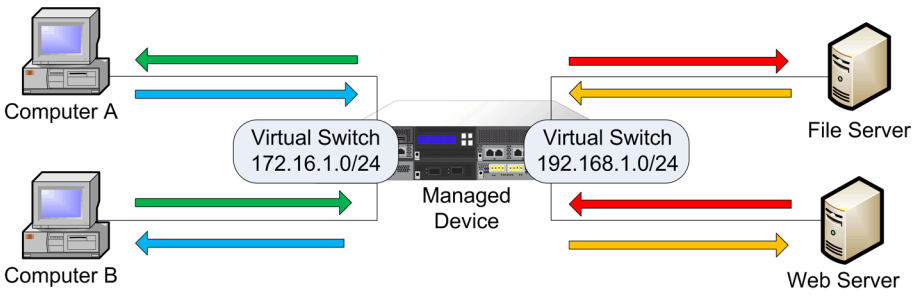
必要时可以在物理端口上定义更多逻辑交换接口，但是，必须将一个逻辑交换接口分配给虚拟交换机以用于处理流量。

虚拟交换机具有可扩展性优势。如果使用物理交换机，会受到该交换机上可用端口数量的限制。如果使用虚拟交换机代替物理交换机，则仅受制于带宽和想要实现部署的复杂程度。

请在要使用第 2 层交换机的情况下使用虚拟交换机，例如要确保工作站连接和网络分段的情况下。在员工主要使用本地网段的情况下，第 2 层交换机特别有用。对于大型部署 （例如，包含广播流量、 IP 语音或多个网络的部署），可以在部署的小型网段上使用虚拟交换机。

在同一受管设备上部署多个虚拟交换机时，可以根据每个网络的需要保持独立的安全级别。

受管设备上的虚拟交换机



在本示例中，受管设备监控来自两个独立网络 （172.16.1.0/20 和 192.168.1.0/24）的流量。虽然这两个网络由同一受管设备监控，但是虚拟交换机仅向同一网络上的计算机或服务器传输流量。流量可以通过 172.16.1.0/24 虚拟交换机从计算机 A 传输到计算机 B （用蓝色线表示），也可以通过同一虚拟交换机从计算机 B 传输到计算机 A （用绿色线表示）。同样，流量可以通过 192.168.1.0/24 虚拟交换机在文件和网络服务器之间往返传输 （用红色线和橙色线表示）。但是，流量不能在计算机与网络服务器或文件服务器之间传输，因为计算机与这些服务器不在同一个虚拟交换机上。

有关配置交换接口和虚拟交换机的详细信息，请参阅《*Sourcefire 3D 系统用户指南*》中的“设置虚拟交换机”。

使用虚拟路由器进行部署

许可证：控制
支持的设备：3 系列

可以在受管设备上创建*虚拟路由器*，用于在两个或更多网络之间路由流量，或者用于将专用网络连接至公共网络 （例如互联网）。虚拟路由器连接两个路由接口，根据目标地址为部署提供第 3 层数据包转发决策。也可以在虚拟路由器上启用严格 TCP 实施。有关路由接口的详细信息，请参阅第 29 页的路由接口。虚拟路由器必须与网关 VPN 配合使用。有关详细信息，请参阅第 38 页的部署网关 VPN。

虚拟路由器可以包含同一广播域中一个或多个独立设备的物理或逻辑路由配置。必须将每个逻辑接口与 VLAN 标记关联，才能使用该特定标记处理物理接口接收的流量。要路由流量，必须为虚拟路由器分配逻辑路由接口。

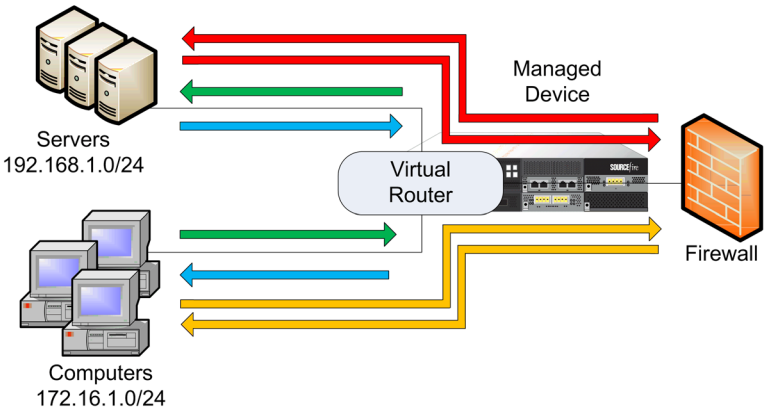
要配置虚拟路由器，请使用物理或逻辑配置设置路由接口。可以配置物理路由接口，用于处理未标记的 VLAN 流量。还可以创建逻辑路由接口，用于处理带有指定 VLAN 标记的流量。系统会丢弃在没有对应路由接口的外部物理接口上接收到的所有流量。如果系统接收到没有 VLAN 标记的数据包，且您未为该端口配置物理路由接口，系统将丢弃该数据包。如果系统接收到 VLAN 标记的数据包，且您未配置逻辑路由接口，系统将丢弃该数据包。

虚拟路由器具有可扩展性优势。如果物理路由器限制可以连接的网络数量，您可以在同一受管设备上配置多个虚拟路由器。将多个路由器放在同一设备上可降低部署的物理复杂性，使您可以从一台设备监控和管理多个路由器。

如果想使用第 3 层物理路由器在部署中的多个网络之间转发流量或者将专用网络连接至公共网络，可使用虚拟路由器。在拥有很多网络或网段而且具有不同安全要求的大型部署中，虚拟路由器尤其有用。

在受管设备上部署虚拟路由器时，可以使用一个设备相互连接多个网络以及互联网。

受管设备上的虚拟路由器



在本示例中，受管设备包含一个虚拟路由器，该路由器实现网络 172.16.1.0/20 上的计算机与网络 192.168.1.0/24 上的服务器之间的流量传输 （用蓝色线和绿色线表示）。虚拟路由器上的第三个接口允许来自每个网络的流量在防火墙之间往返传输 （分别用红色线和橙色线表示）。

有关详细信息，请参阅 《*Sourcefire 3D 系统用户指南*》中的“设置虚拟路由器”。

使用混合接口进行部署

许可证：控制
支持的设备：3 系列

可以在受管设备上创建*混合接口*，以使用虚拟交换机和虚拟路由器在第 2 层与第 3 层网络之间路由流量。这样就提供了一个接口，既可以传送交换机上的本地流量，又可以传送往返外部网络的流量。为了获得最佳效果，请在接口上配置基于策略的 NAT，在混合接口上提供网络地址转换。请参阅第 39 页的使用基于策略的 NAT 进行部署。

一个混合接口必须包含一个或多个交换接口和一个或多个路由接口。常见的部署包括两个配置为虚拟交换机的交换接口 （用于在本地网络上传输流量）和两个虚拟路由器 （用于将流量传送到专用网络或公共网络）。

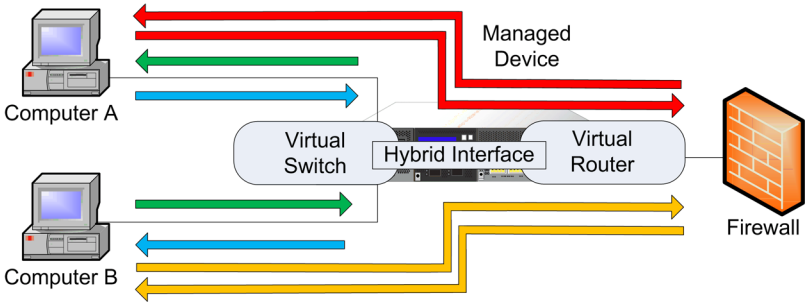
要创建混合接口，请首先配置虚拟交换机和虚拟路由器，然后将配置好的虚拟交换机和虚拟路由器添加到混合接口。未同时与虚拟交换机和虚拟路由器关联的混合接口不可用于路由，也不会生成流量或对流量作出响应。

混合接口具有紧凑性和可扩展性优势。使用一个混合接口可将第 2 层和第 3 层流量路由功能整合到一个统一接口中，从而减少部署中的物理设备数量并为流量提供一个统一的管理接口。

在同时需要第 2 层和第 3 层路由功能的情况下可使用一个混合接口。这种部署适合部署中空间和资源均有限的小型网段。

部署混合接口时，可以允许流量从本地网络传输到外部网络或公共网络 （例如互联网），这样还可以解决混合接口中虚拟交换机和虚拟路由器的各种完全性问题。

受管设备上的混合接口



在本示例中，计算机 A 和计算机 B 位于同一个网络中，并且使用受管设备上配置的第 2 层虚拟交换机进行通信 （用蓝色线和绿色线表示）。受管设备上配置的虚拟路由器提供对防火墙的第 3 层访问。混合接口整合了虚拟交换机和虚拟路由器的第 2 层和第 3 层功能，允许流量从每台计算机通过混合接口传输至防火墙 （用红色线和橙色线表示）。

有关详细信息，请参阅 《*Sourcefire 3D 系统用户指南*》中的“设置混合接口”。

部署网关 VPN

许可证：VPN
支持的设备：3 系列

可以创建*网关虚拟专用网络* （网关 VPN）连接，以在本地网关和远程网关之间建立安全隧道。网关之间的安全隧道可保护网关之间的通信。

可以配置 Sourcefire 3D 系统，使它可使用互联网协议安全 (IPSec) 协议族构在 Sourcefire 受管设备的虚拟路由器与远程设备或其他第三方 VPN 终端之间构建安全 VPN 隧道。建立 VPN 连接后，本地网关后面的主机可以通过 VPN 安全隧道连接至远程网关后面的主机。VPN 终端利用互联网密钥交换 (IKE) V1 或 V2 协议相互进行身份验证，从而为隧道创建安全关联。系统在 IPSec 身份验证报头 (AH) 模式或 IPSec 封装安全负载 (ESP) 模式下运行。AH 和 ESP 都提供身份验证，ESP 还提供加密。

网关 VPN 可以用于点对点部署、星型部署或网状网部署：

- 点对点部署以直接一对一关系相互连接两个终端。两个终端配置为对等设备，因此，其中任一设备都可启动安全连接。至少一台设备必须是支持 VPN 的受管设备。

  如果远程位置上的主机使用公共网络连接网络中的主机，可使用点对点部署保持网络安全性。
- 星型部署在集线器和多个远程终端 （叶节点）之间建立安全连接。集线器节点和各个叶节点之间的每个连接都是一个单独的 VPN 隧道。通常，集线器节点是位于总部的支持 VPN 的受管设备。叶节点位于分支机构，负责发起大部分流量。

  可使用星型部署在互联网或其他第三方网络上利用安全连接来连接组织的总部与分支机构，从而为所有员工提供对组织网络的受控访问。
- 网状网部署通过 VPN 隧道将所有终端连接在一起。这可提供冗余，以便当某个终端出现故障时，其余终端仍然能够相互通信。

  可使用网状网部署连接一组分散的分支机构，以确保即使一个或多个 VPN 隧道出现故障，流量仍然可以传输。此配置中部署的支持 VPN 的受管设备数量决定冗余级别。

有关网关 VPN 配置和部署的详细信息，请参阅 《*Sourcefire 3D 系统用户指南*》中的“网关 VPN”。

使用基于策略的 NAT 进行部署

许可证：控制
支持的设备：任意

可以使用*基于策略的网络地址转换* (NAT) 来定义指定要如何执行 NAT 的策略。策略可以针对一个接口、一台或多台设备或者整个网络。

可以配置静态 （一对一）或动态 （一对多）转换。请注意，动态转换取决于顺序，其中规则是按照顺序搜索的，直至应用第一个匹配规则。

基于策略的 NAT 通常用于以下部署：

- 隐藏专用网络地址。

  从专用网络访问公共网络时， NAT 会将专用网络地址转换为公共网络地址。具体专用网络地址对公共网络是隐藏的。
- 允许访问专用网络服务。

  公共网络访问专用网络时， NAT 会将公共地址转换为专用网络地址。公共网络可以访问特定专用网络地址。
- 重定向多个专用网络之间的流量。

  专用网络上的服务器访问连接的专用网络上的服务器时， NAT 会转换两个专用网络之间的专用地址，以确保专用地址中没有重复且流量可以在这些地址之间传输。

使用基于策略的 NAT 使得无需使用额外硬件的需求，而且可以将入侵检测或防御系统和 NAT 的配置整合到了一个用户界面中。有关详细信息，请参阅《*Sourcefire 3D 系统用户指南*》中的“使用 NAT 策略”。

使用访问控制进行部署

许可证：任意
支持的设备：任意

访问控制是一项基于策略的功能，可用于指定、检查和记录可以进出网络或在网络中传输的流量。以下节介绍访问控制如何在部署中发挥作用。有关此功能的详细信息，请参阅《*Sourcefire 3D 系统用户指南*》。

访问控制策略决定系统如何处理网络上的流量。可以将访问控制规则添加到策略中，就如何处理和记录网络流量进行更精细的控制。

不包括访问控制规则的访问控制策略使用以下默认操作之一来处理流量：

- 阻止所有流量进入网络
- 信任进入网络的所有流量，不会作进一步检查
- 允许所有流量进入网络，并且只使用网络发现策略检查流量
- 允许所有流量进入网络，并且使用入侵策略和网络发现策略检查流量

访问控制规则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 的复杂方案。对于每个规则，都要指定规则操作，即，是否根据入侵策略或文件策略信任、监控、阻止或者检查匹配的流量。

访问控制可以根据安全情报数据过滤流量，此功能允许根据源 IP 地址或目标 IP 地址指定对于每个访问控制策略可以流经网络的流量。此功能可以创建包含不允许的 IP 地址的黑名单，系统会阻止并且不检查这些地址的流量。

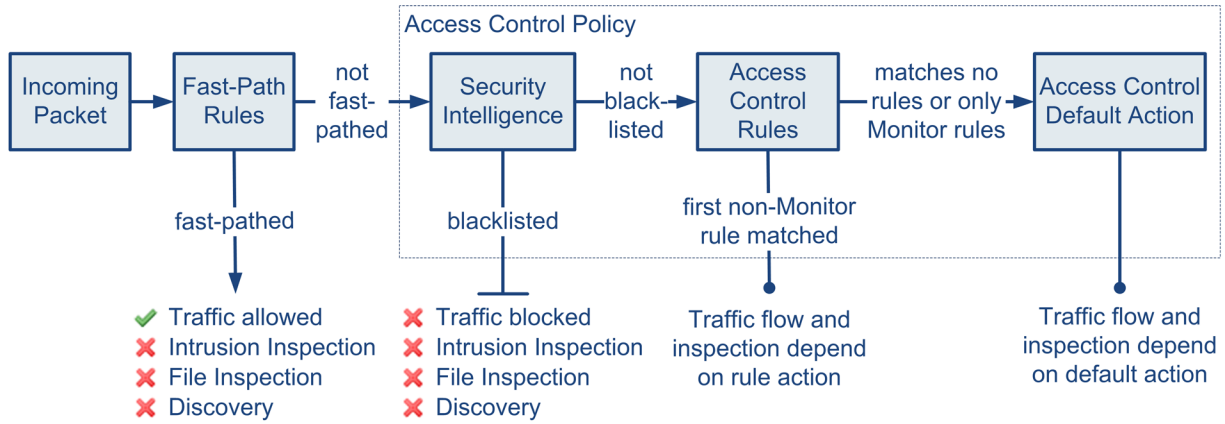
部署示例说明了常见的网段。在每个这些位置中部署受管设备具有不同的作用。以下各节提供了典型的位置建议：

- 第 40 页的在防火墙内部说明访问控制如何对通过防火墙的流量发挥作用。
- 第 41 页的在 DMZ 上说明在 DMZ 中访问控制如何保护向外服务器。
- 第 42 页的在内部网络上说明访问控制如何保护内部网络免受蓄意或意外攻击。
- 第 42 页的在核心网络上说明包含严格规则的访问控制策略可以如何保护重要资产。
- 第 43 页的在远程或移动网络上说明访问控制如何监控和保护网络免受远程位置或移动设备上的流量影响。

在防火墙内部

防火墙内部的受管设备监控防火墙允许的入站流量或由于配置错误通过防火墙的流量。常见网段包括 DMZ、内部网络、核心网络、移动接入网络和远程网络。

下图说明了通过 Sourcefire 3D 系统的流量，并提供了关于对这些流量执行的检测类型的一些详细信息。请注意，系统不检查经由快速路径传输或列入黑名单的流量。对于访问控制规则或默认操作处理的流量，流量和检查取决于规则操作。虽然为了简洁起见在图上未显示规则操作，但是对于受信任或受阻止的流量，系统也不会执行任何类型的检查。此外，默认操作也不支持文件检查。



首先按照任何快速路径规则检查传入数据包。如果匹配，该流量将经由快速路径传输。如果没有匹配项，基于安全情报的过滤功能将确定该数据包是否已被列入黑名单。如果不是，将应用任何访问控制规则。如果该数据包符合规则中的条件，流量和检查取决于规则操作。如果没有规则与该数据包匹配，流量和检查取决于默认策略操作。（监控规则属于例外，此类规则允许持续评估流量。）每个访问控制策略的默认操作管理未经由快速路径传输或未列入黑名单的流量，或与任何非监控规则匹配的流量。请注意，快速路径仅适用于 8000 系列和 3D9900 设备。

可以创建访问控制规则，就如何处理和记录网络流量进行更精细的控制。对于每个规则，请指定应用于满足特定条件的流量的操作 （信任、监控、阻止或检查）。

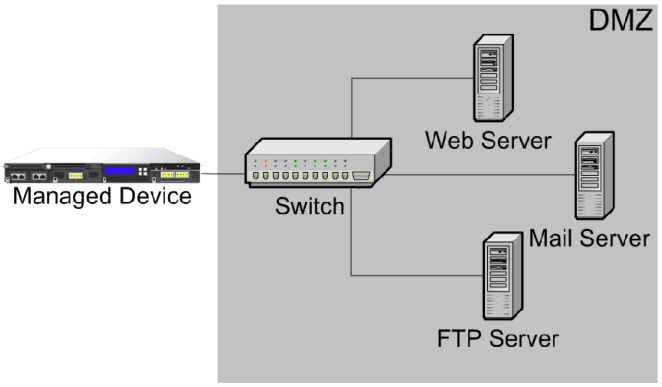
在 DMZ 上

DMZ 包含向外服务器 （例如网络、 FTP、 DNS 和邮件），可以为内部网络上的用户提供邮件中继和网络代理等服务。

DMZ 中存储的内容是静态的，对于 DMZ，更改的计划和执行需要有明确告知和提前通知。此网段上的攻击通常是传入的并且立即透明化，因为在 DMZ 中的服务器上只允许执行事先计划好的更改。此网段的有效控制访问策略严格控制对服务的访问并搜索任何新的网络事件。

DMZ 中的服务器可以包含 DMZ 可通过网络查询的数据库。像 DMZ 一样，不应出现意外的更改，但是，数据库内容比网站或其他 DMZ 服务更加敏感而且需要更好的保护。严格的入侵策略加上 DMZ 访问控制策略是有效的策略。

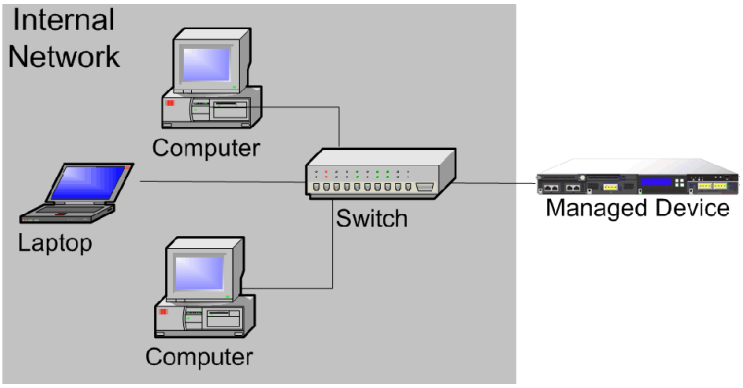
此网段上部署的受管设备可以检测 DMZ 中来自受威胁服务器的针对互联网的攻击。使用网络发现监控网络流量有助于监控这些受威胁的服务器是否出现了可能表示 DMZ 中服务器受到了攻击的变化 （例如，突然出现意料之外的服务）。



在内部网络上

恶意攻击可能来自内部网络上的计算机。这可能是故意行为 （例如，在网络上出现未知计算机），也可能是意外感染 （例如，工作笔记本电脑在外部位置感染，然后被连接至网络，从而传播了病毒）。内部网络的风险也可能是出站的 （例如，计算机向外部可疑 IP 地址发送信息）。

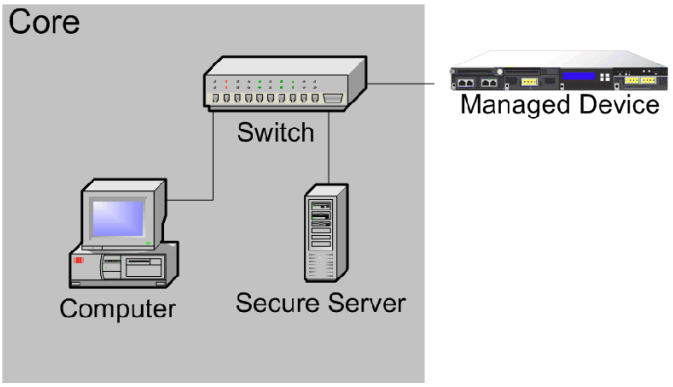
除了出站流量外，此动态网络要求所有内部流量都进行严格的访问控制策略。可以通过添加访问控制规则来严格控制用户和应用之间的流量。



在核心网络上

核心资产是指对于企业取得成功至关重要的、必须不惜一切代价进行保护的那些资产。虽然核心资产根据企业性质而异，但是，典型的核心资产通常包括财务中心和管理中心或知识产权库。如果核心资产的安全遭受侵犯，可能会对企业造成致命打击。

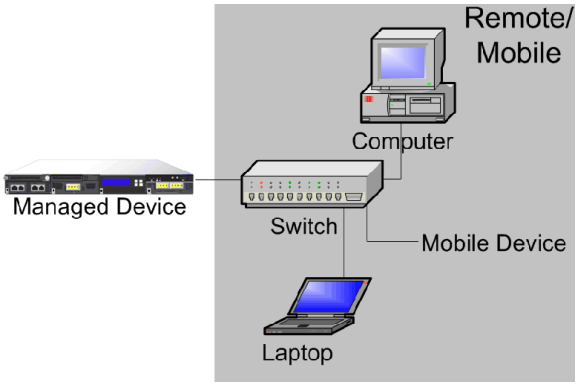
虽然此网段必须随时可用以确保企业正常运行，但是必须进行严格的限制和控制。访问控制应确保存在最高风险的网段 （例如远程网络或移动设备）无法访问这些资产。必须对此网段进行最严格的控制，对用户和应用访问执行严格的规则。



在远程或移动网络上

位于外部的远程网络通常使用虚拟专用网络 (VPN) 访问主网。移动设备越来越普遍，人们也越来越多地将个人设备用于工作用途 （例如，使用“智能手机”访问公司邮件）。

这些网络可能会快速、频繁地发生变化，属于高度动态的环境。在专用移动或远程网络中部署受管设备可以创建严格的访问控制策略来监控和管理往返未知外部资源的流量。策略可以通过严格限制用户、网络和应用如何访问核心资源来降低风险。



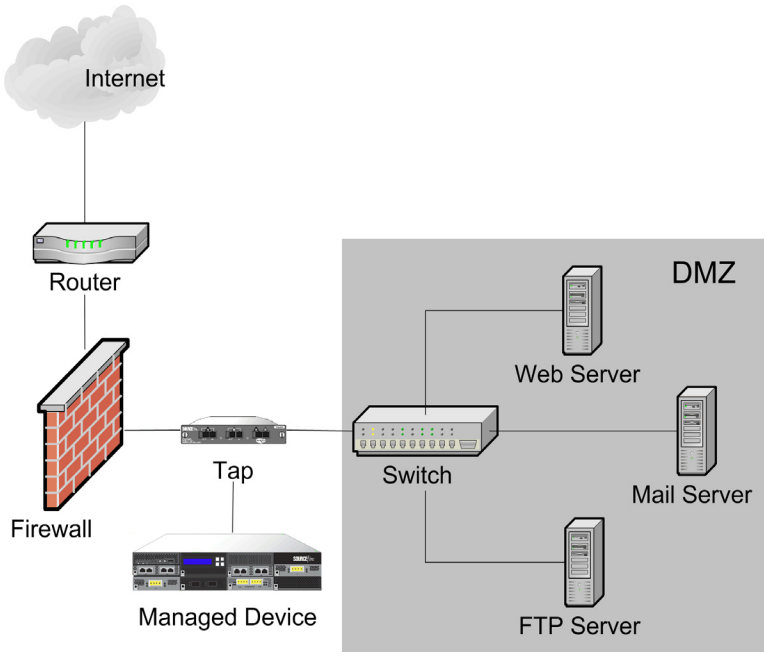
使用多端口受管设备

受管设备在其网络模块上提供多个感应端口。可以使用多端口受管设备执行以下操作：

- 重新整合来自网络分路器的独立连接
- 捕获并评估来自不同网络的流量
- 用作虚拟路由器
- 用作虚拟交换机

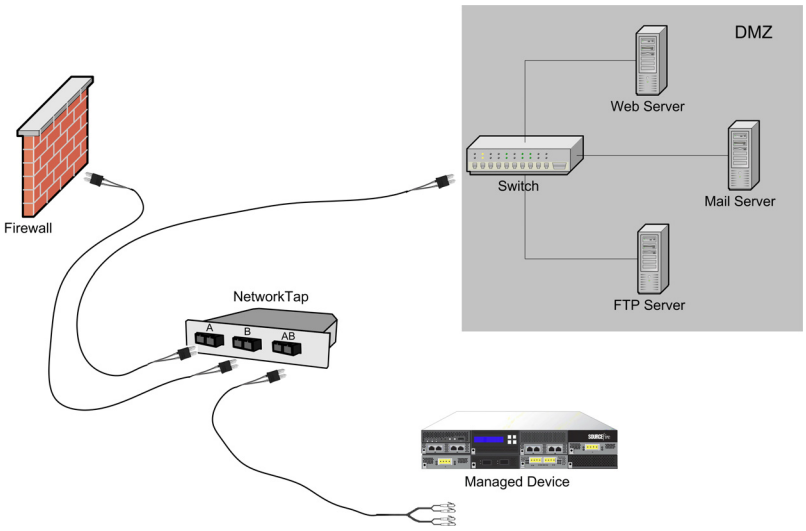
重要！ 虽然每个端口能够接收设备额定的完整吞吐量，但是受管设备上的总流量不能超过其带宽额定值，才不会出现任何数据包丢失。

部署带有网络分路器的多端口受管设备是一个很简单的过程。下图说明了如何在高流量网段上安装网络分路器。

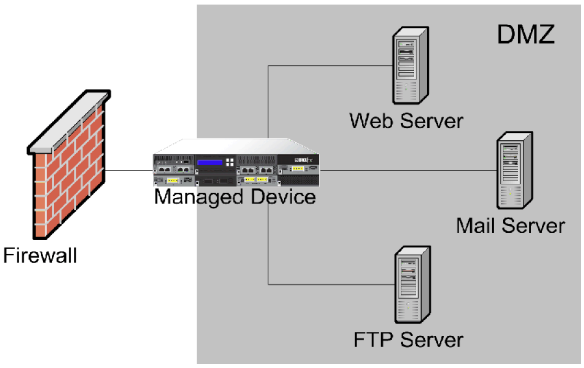


在此方案中，分路器通过单独的端口传输传入流量和传出流量。在受管设备上将多端口适配器卡连接至分路器后，受管设备就能将流量整合到一个统一的数据流中，从而可以对其进行分析。

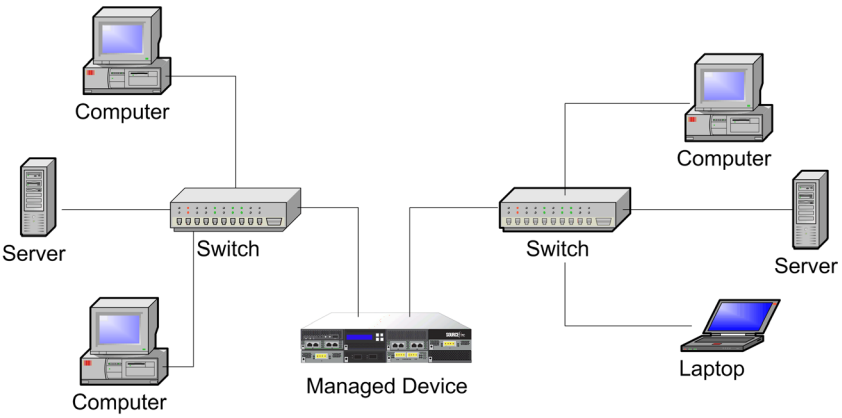
请注意，对于千兆光纤分路器，受管设备上的两组端口都用于分路器上的连接器，如下图所示。



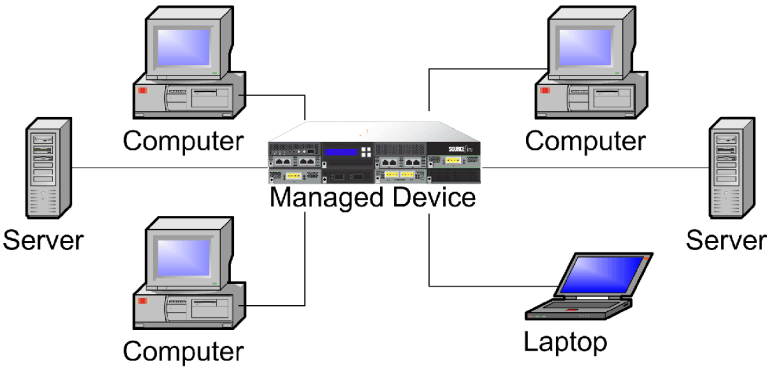
可以用虚拟交换机来代替部署中的分路器和交换机。请注意，如果用虚拟交换机代替分路器，将会失去分路器数据包传输保障。



还可以创建接口用于捕获来自单独网络的数据。下图显示了一台带有双端口适配器和两个接口的设备连接至两个网络。



除了使用一台设备监控两个网段之外，还可以使用设备的虚拟交换机功能来代替部署中的两个交换机。



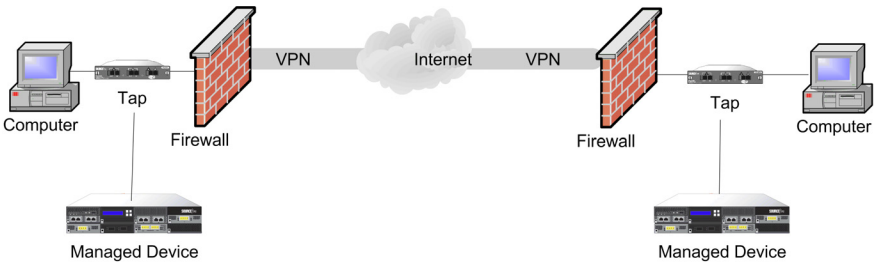
复杂的网络部署

企业网络可能需要远程访问，例如，使用 VPN 或者有多个入口点 （例如业务合作伙伴或银行连接）。以下各节讲述了这些部署涉及的一些问题：

集成 VPN

虚拟专用网络 (VPN) 使用 IP 隧道技术使互联网上的远程用户获得本地网络安全性。一般来说， VPN 解决方案会加密 IP 数据包中的数据负载。 IP 报头未加密，因此， IP 数据包可以像任何其他数据包一样通过公共网络进行传输。数据包到达其目标网络时，负载被解密，数据包被传送到正确的主机。

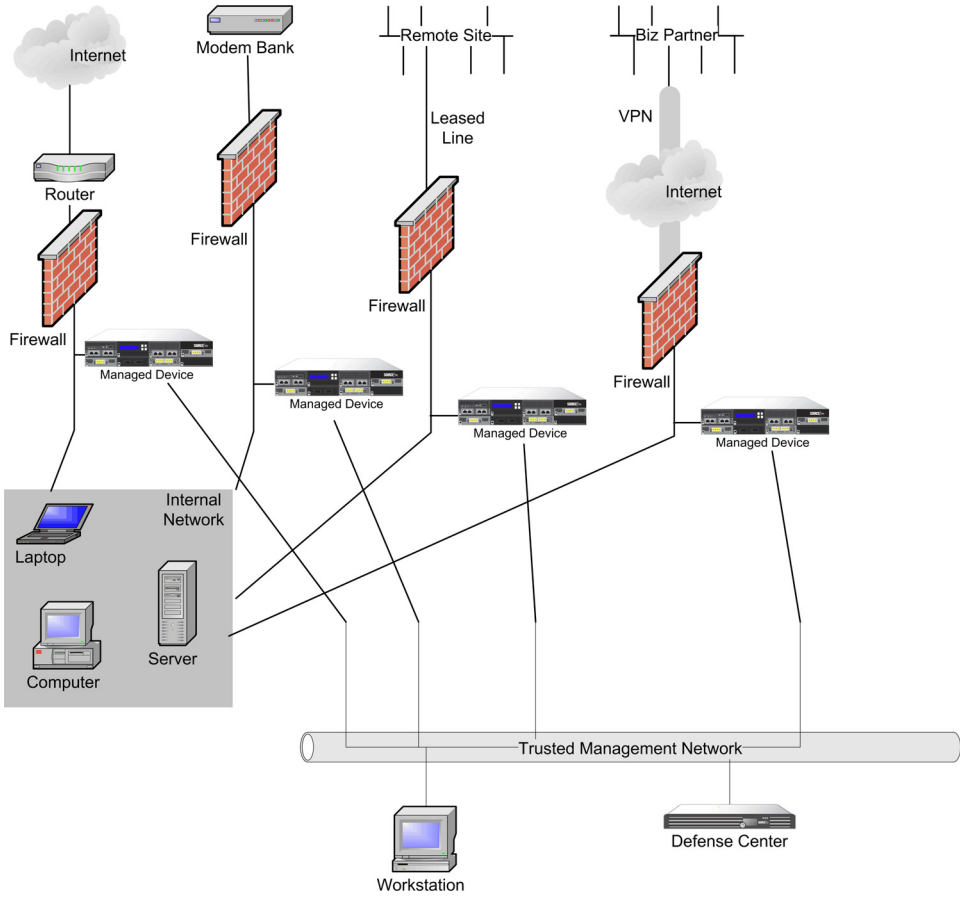
由于网络设备无法分析 VPN 数据包的加密负载，因此，将受管设备放置在 VPN 连接的终端外部可确保可以访问所有数据包信息。下图说明了可以在 VPN 环境中如何部署受管设备。



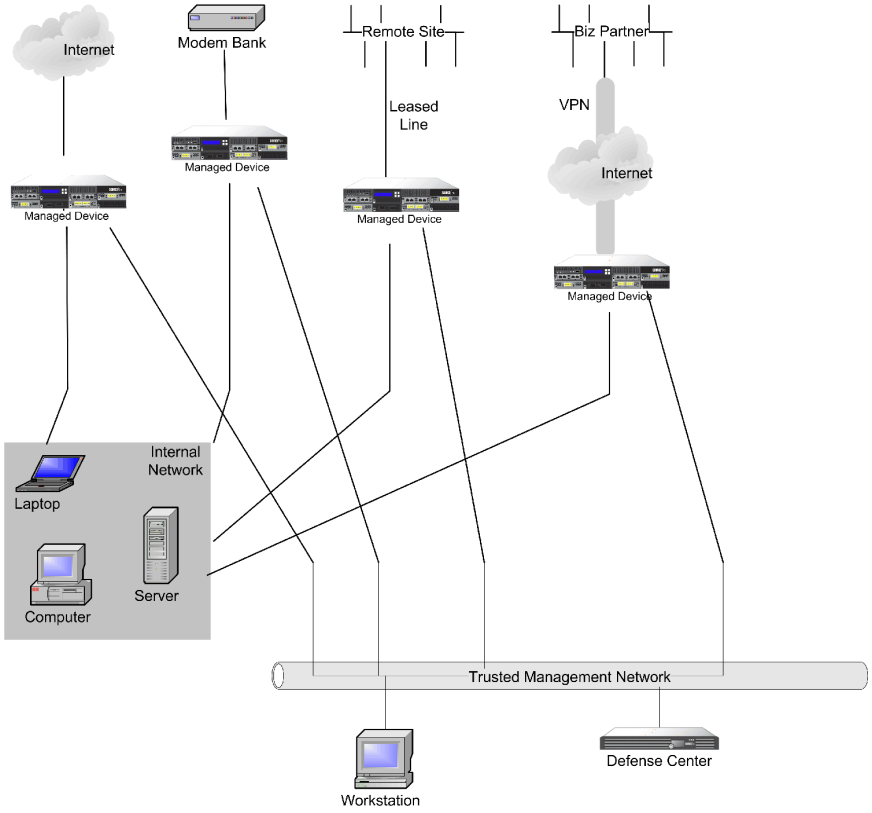
可以用受管设备代替 VPN 连接任一端的分路器。请注意，如果用受管设备代替分路器，将会失去分路器数据包传输保障。

检测其他入口点上的入侵

许多网络包括不止一个接入点。有些企业不是使用边界路由器连接至互联网，而是将互联网、调制解调器组与连接业务合作伙伴网络的直接链接结合起来使用。一般来说，应在防火墙附近（在防火墙内部和/或防火墙外部）以及对于企业数据完整性和机密性很重要的网段上部署受管设备。下图显示了可以在具有多个入口点的复杂网络上的关键位置如何安装受管设备。

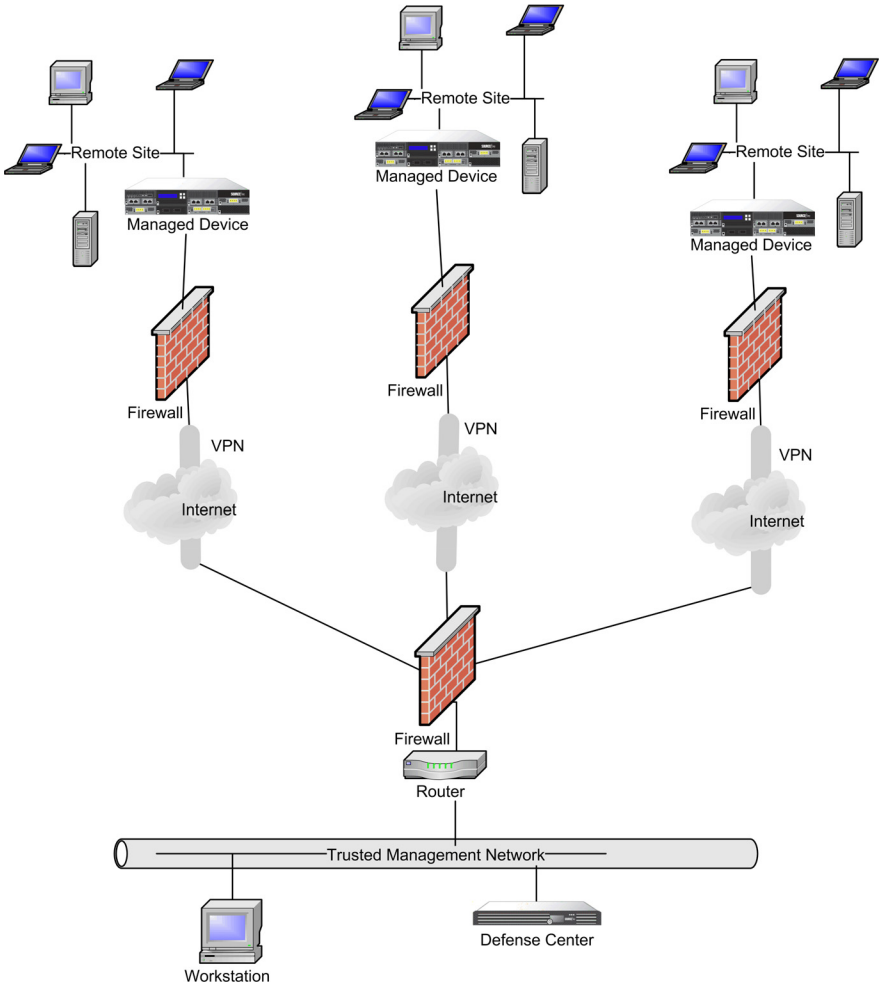


可以用网段上部署的受管设备代替防火墙和路由器。

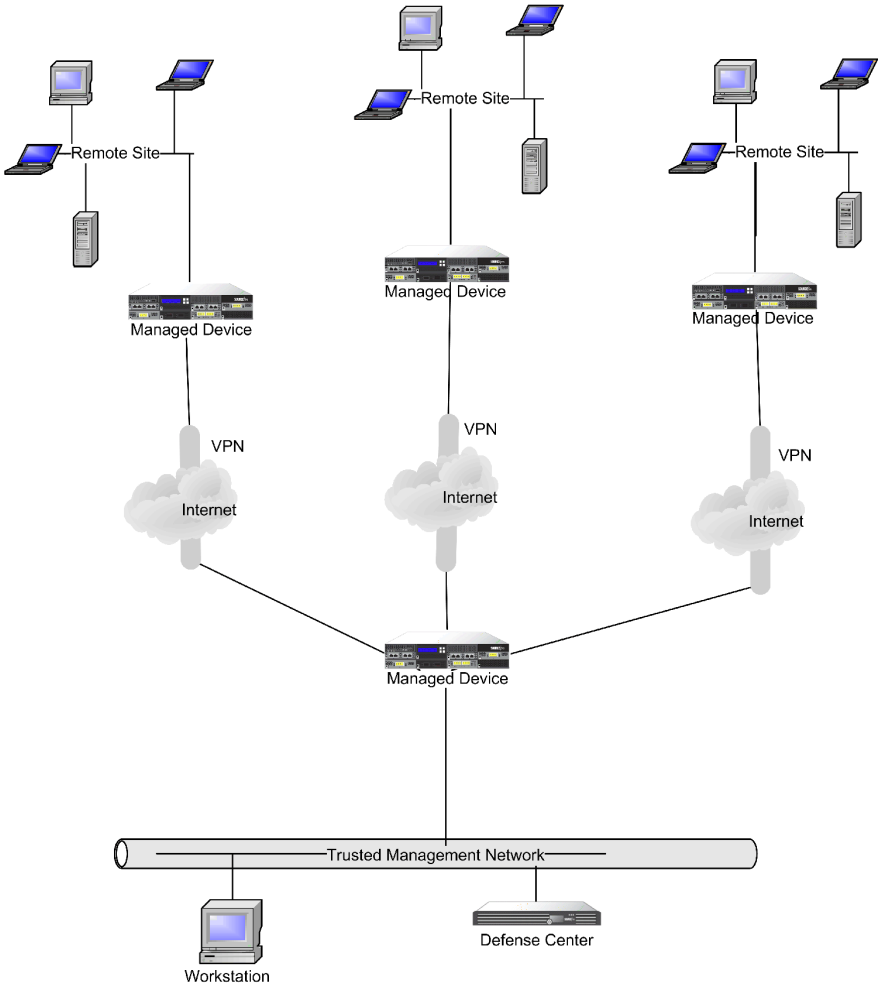


在多站点环境中进行部署

许多组织想要扩展入侵检测，使之覆盖地理位置很分散的整个企业，然后从一个位置分析所有 IPS 数据。 Sourcefire 3D 系统提供了防御中心，后者聚合和关联来自整个组织中很多位置部署的受管设备的事件，从而可以实现此功能。与在同一网络相同位置部署多个受管设备和防御中心不同，在分散的地理位置部署多个受管设备时，必须采取预防措施，确保受管设备和数据流的安全。要保护数据，必须将受管设备和防御中心与不受保护的网络隔离。为此，可以通过 VPN 或利用某些其他安全隧道协议，传输来自受管设备的数据流，如下图所示。



可以用每个网段上部署的受管设备代替防火墙和路由器。



在复杂的网络中集成受管设备

可以在比单纯的多分区网络更复杂的网络拓扑中部署受管设备。本节讲述在存在代理服务器、 NAT 设备和 VPN 的环境中部署时有关网络发现和漏洞分析的一些问题，还提供关于使用 Sourcefire 防御中心管理多个受管设备以及在多站点环境中部署和管理受管设备的信息。

与代理服务器和 NAT 集成

网络地址转换 (NAT) 设备或软件可以越过防火墙来使用，从而有效地将内部主机的 IP 地址隐藏在防火墙后面。如果受管设备部署在这些设备或软件和受监控的主机之间，系统可能无法正确识别代理或 NAT 设备后面的主机。在这种情况下，Sourcefire建议将受管设备配置在受代理或 NAT 设备保护的网段内，从而确保主机接受正确的检测。

与负载平衡方法集成

在一些网络环境中，“服务器场”配置用于为网络托管、FTP 存储站点等服务执行网络负载平衡。在负载平衡环境中， IP 地址在具有同一操作系统的两个或更多主机之间共享。在这种情况下，系统会检测操作系统的更改，但无法提供高置信度的静态操作系统识别。根据受影响主机上不同操作系统的数量，系统可能会生成大量操作系统更改事件或以较低的置信度显示静态操作系统识别。

其他检测注意事项

如果更改了正被识别的主机的 TCP/IP 堆栈，系统可能无法正确识别该主机的操作系统。在某些情况下，进行这种更改是为了提高性能。例如，鼓励运行互联网信息服务 (IIS) 网络服务器的 Windows 主机的管理员增大 TCP 窗口，以便接收更量数据，从而提高性能。在其他情况下，可通过 TCP/IP 堆栈更改对真正的操作系统进行模糊处理，以使其无法被准确识别，从而避免针对性攻击。这样做旨在应对这样一种可能的情况：攻击者对网络执行侦察扫描，识别使用特定操作系统的主机，然后利用该操作系统特有的漏洞发起针对性攻击。

第 3 章

安装 SOURCEFIRE 3D 系统设备

Sourcefire 设备可作为较大的 Sourcefire 3D 系统部署的一部分在网络上轻松安装。您在各个网段安装设备以检查流量，并根据应用的入侵策略生成入侵事件。该数据传输至防御中心，防御中心管理一台或多台设备以关联整个部署中的数据，并协调和应对安全威胁。

您可以将多台设备预配置在一个位置，以供不同的部署位置使用。有关预配置的指导，请参阅第 242 页的预配置 Sourcefire 设备。

有关安装 Sourcefire 设备的详细信息，请参阅以下各节：

附件

以下是 Sourcefire 设备随附的组件列表。打开系统和关联附件的包装，检查包装内容是否完整，如下所列：

- 一台 Sourcefire 设备
- 电源线 （随包括冗余电源的设备提供两根电源线）。
- 5e 类以太网直通电缆：一根用于防御中心；两根用于受管设备
- 一个机架安装式套件 （分别为 3D7010、 3D7020 和 3D7030 提供的托盘和机架安装式套件）

安全注意事项

在安装设备之前， Sourcefire 建议您考虑以下事项：

- Sourcefire 3D 系统设备应安装在一个可上锁的机架中，且机架应位于一个能防止未授权人员进入的安全位置。
- Sourcefire 设备只能由经过培训的合格人员进行安装、更换、管理或维修。
- 请始终将管理接口连接至可防止未授权访问的安全内部管理网络。
- 识别可访问设备的具体工作站的 IP 地址。使用设备系统策略中的访问列表限制仅某些特定主机才能访问设备。有关详细信息，请参阅 《*Sourcefire 3D 系统用户指南*》。

识别管理接口

可通过管理接口将部署中的每台设备连接至网络。这样，防御中心能够与其管理的设备通信并管理该设备。

Sourcefire 设备在不同的硬件平台上提供。在执行安装操作步骤时，请务必参考正确的设备示意图：

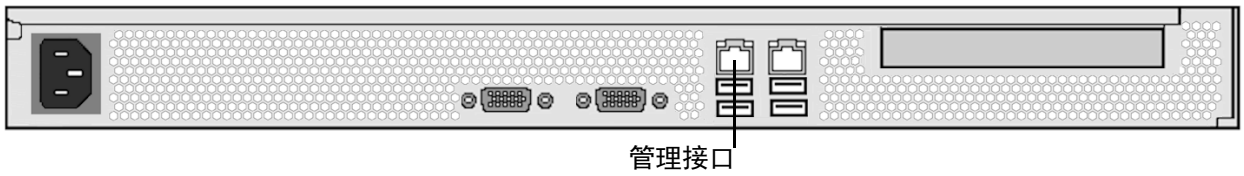
- 第 54 页的Sourcefire 防御中心 750
- 第 54 页的Sourcefire 防御中心 1500
- 第 54 页的Sourcefire 防御中心 3500
- 第 55 页的Sourcefire 7000 系列
- 第 55 页的Sourcefire 8000 系列

Sourcefire 防御中心 750

DC750 作为 1U 设备提供。

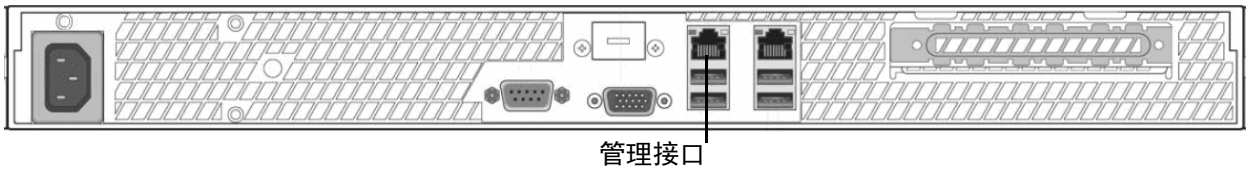
以下机箱背面示意图显示了 DC750 （第 1 版）上的管理接口的位置。

DC750 （第 1 版）



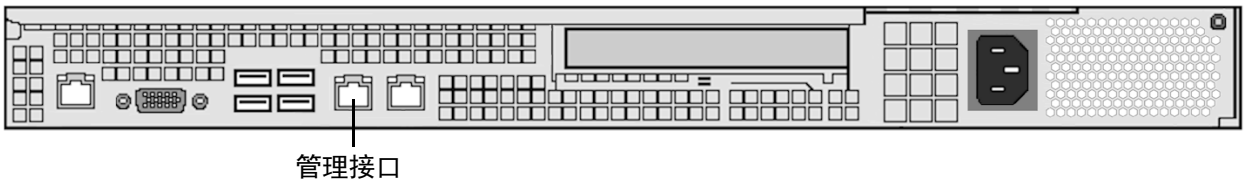
以下机箱背面示意图显示了 DC750 （第 2 版）上的管理接口的位置。

DC750 （第 2 版）



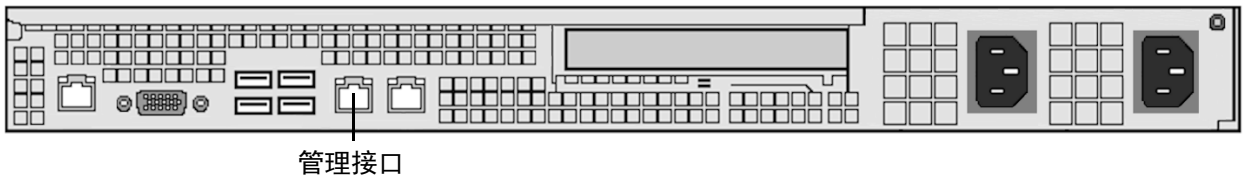
Sourcefire 防御中心 1500

DC1500 作为 1U 设备提供。以下机箱背面示意图显示了管理接口的位置。



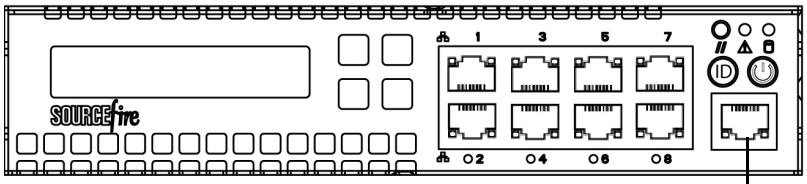
Sourcefire 防御中心 3500

DC3500 作为 1U 设备提供。以下机箱背面示意图显示了管理接口的位置。

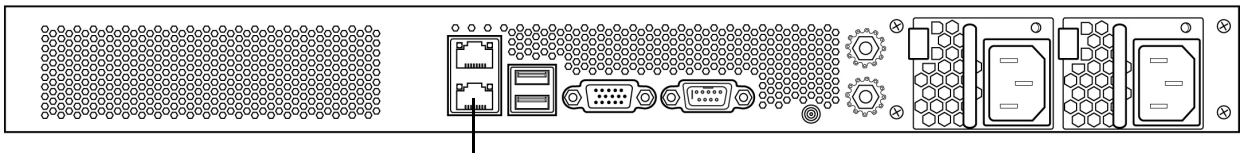


Sourcefire 7000 系列

3D7010、3D7020 和 3D7030 为 1U 设备，宽度为机箱托盘宽度的一半。以下机箱正面示意图显示了管理接口。

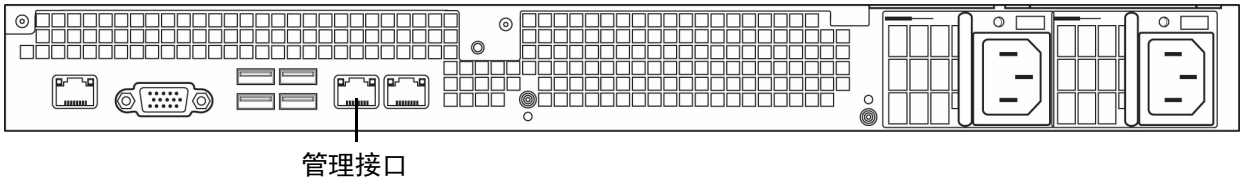


3D7110/7120、 3D7115/7125 和 AMP7150 作为 1U 设备提供。以下机箱背面示意图显示了管理接口的位置。

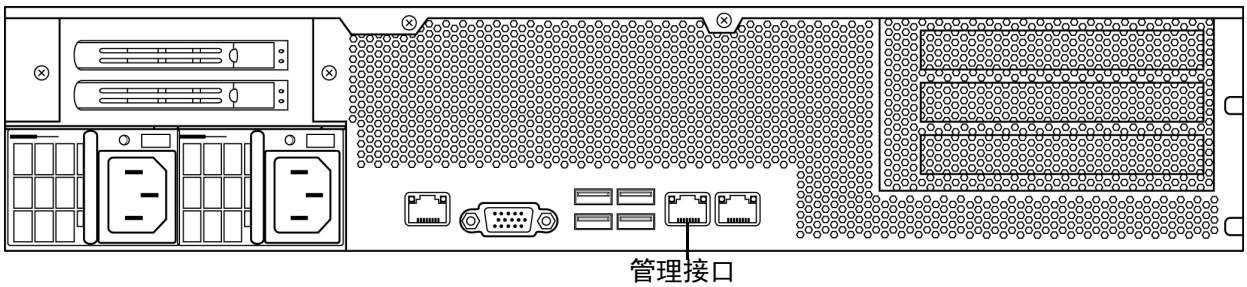


Sourcefire 8000 系列

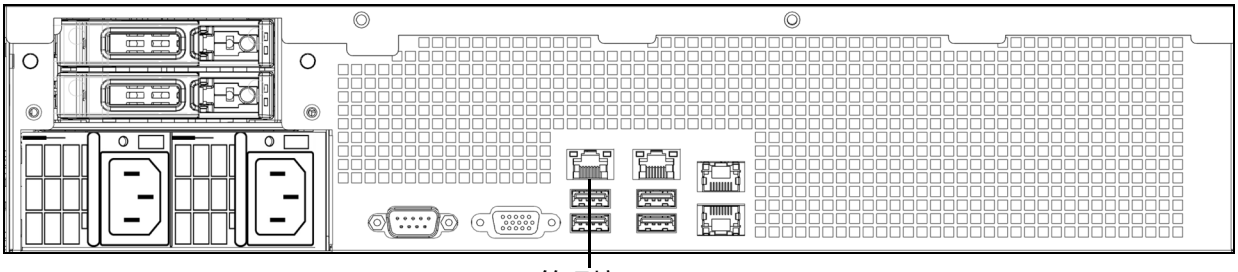
3D8120、 3D8130、 3D8140 和 AMP8150 作为 1U 设备提供。以下机箱背面示意图显示了管理接口的位置。



3D8250 作为 2U 设备提供。3D8260、3D8270 和 3D8290 作为 2U 设备提供（带一台、两台或三台辅助 2U 设备）。以下机箱背面示意图显示了每台 2U 设备的管理接口的位置。



3D8350 作为 2U 设备提供。3D8360、3D8370 和 3D8390 作为 2U 设备提供（带一台、两台或三台辅助 2U 设备）。以下机箱背面示意图显示了每台 2U 设备的管理接口的位置。



识别感应接口

受管设备使用感应接口连接至网段。每台设备可监控的网段数量取决于设备上的感应接口数和您要在网段上使用的连接类型 （被动、内联、路由或交换）。

以下各节介绍每台受管设备的感应接口。有关连接类型的信息，请参阅第 27 页的了解接口。

- 要找到 7000 系列上的感应接口，请参阅第 56 页的Sourcefire 7000 系列。
- 要定位 8000 系列上的模块插槽，请参阅第 60 页的Sourcefire 8000 系列。
- 要定位 8000 系列网络模块上的感应接口，请参阅第 61 页的8000 系列模块。

Sourcefire 7000 系列

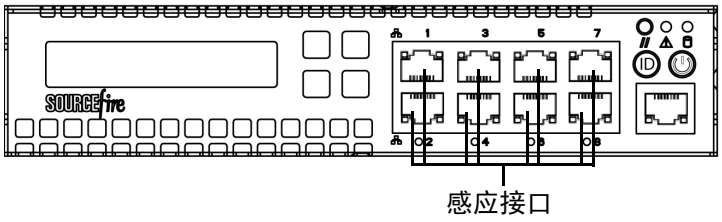
Sourcefire 7000 系列可提供以下配置：

- 带八个铜缆接口的 1U 设备 （宽度为机架托盘宽度的一半），每个接口都支持可配置旁路功能。
- 带八个铜缆接口或八个光纤接口的 1U 设备，每个接口都支持可配置旁路功能。
- 带四个铜缆接口 （支持可配置旁路功能）和八个小型可插拔 (SFP) 端口 （不支持旁路功能）的 1U 设备

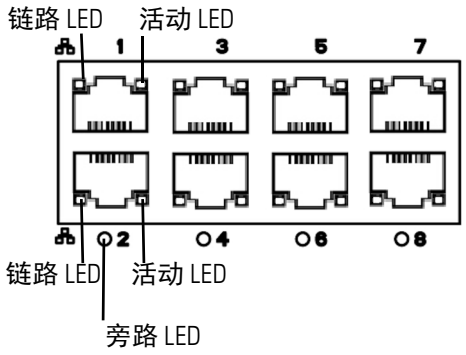
3D7010、 3D7030 和 3D7030

3D7010、 3D7020 和 3D7030 配置有八个铜缆端口感应接口，每个接口都支持可配置旁路功能。以下机箱正面示意图显示了感应接口的位置。

八端口 1000BASE-T 铜缆可配置旁路接口



您可使用这些连接以被动方式监控多达八个独立网段。您还可使用处于内联模式或支持旁路功能的内联模式的成对接口，将设备在多达四个网络上部署为入侵防御系统。

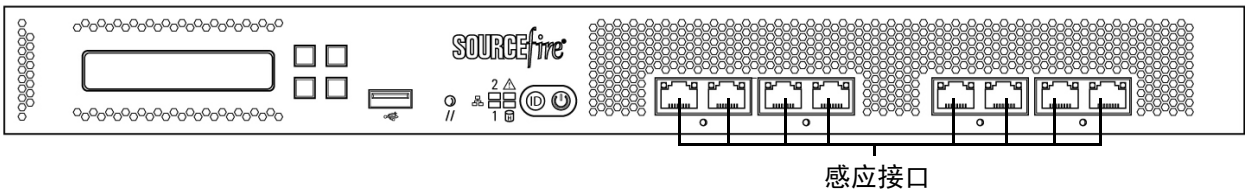


如果希望充分利用设备的自动旁路功能，您必须将两个接口 （接口 1 和 2、 3 和 4、 5 和 6、或 7 和 8）纵向连接至网段。即使设备发生故障或断电，自动旁路功能也允许流量通过。在使用电缆连接接口后，您可通过网络界面将一对接口配置为内联集，并在该内联集上启用旁路模式。

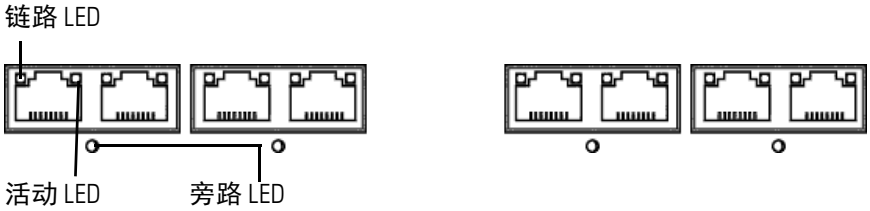
3D7110 和 3D7120

3D7110 和 3D7120 配置有八个铜缆端口感应接口或八个光纤端口感应接口，每个接口都支持可配置旁路功能。以下机箱正面示意图显示了感应接口的位置。

3D7110 和 3D7120 铜缆接口



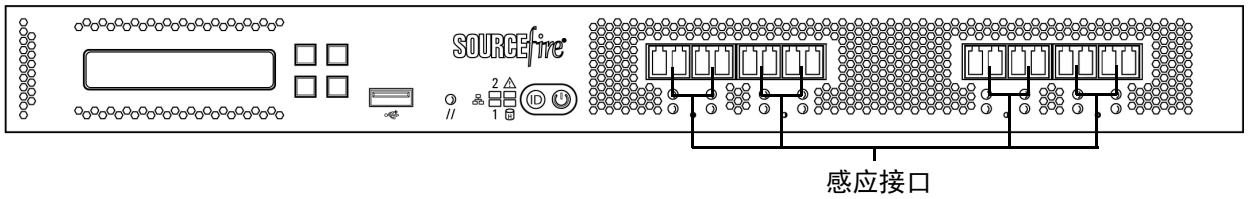
八端口 1000BASE-T 铜缆接口



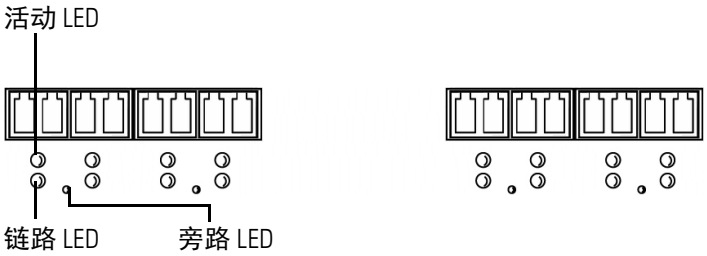
您可使用这些连接以被动方式监控多达八个独立网段。您还可使用处于内联模式或支持旁路功能的内联模式的成对接口，将设备在多达四个网络上部署为入侵防御系统。

如果希望利用设备的自动旁路功能，则必须将左侧的两个接口或右侧的两个接口连接至网段。即使设备发生故障或断电，自动旁路功能也允许流量通过。在使用电缆连接接口后，您可通过网络界面将一对接口配置为内联集，并在该内联集上启用旁路模式。

3D7110 和 3D7120 光纤接口



八端口 1000BASE-SX 光纤可配置旁路



八端口 1000BASE-SX 光纤可配置旁路配置使用 LC 类型（本地连接器）光收发器。

您可使用这些连接以被动方式监控多达八个独立网段。您还可使用处于内联模式或支持旁路功能的内联模式的成对接口，将设备在多达四个网络上部署为入侵防御系统。

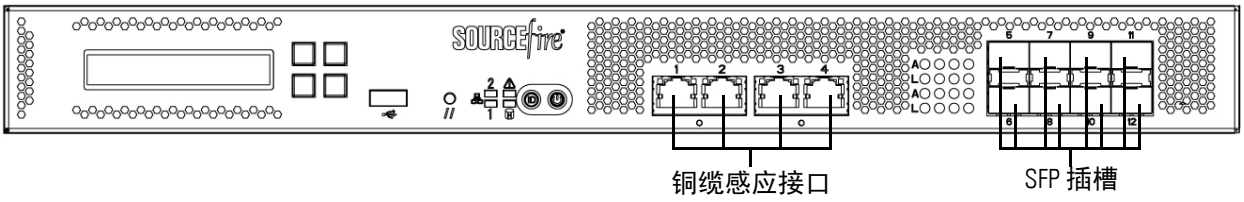
提示！ 为获得最佳性能，请连续使用接口集。如果您跳过任何接口，则可能会发生性能降级。

如果希望利用设备的自动旁路功能，则必须将左侧的两个接口或右侧的两个接口连接至网段。即使设备发生故障或断电，自动旁路功能也允许流量通过。在使用电缆连接接口后，您可通过网络界面将一对接口配置为内联集，并在该内联集上启用旁路模式。

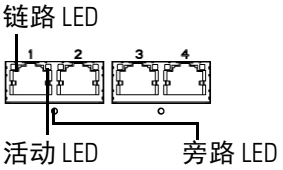
3D7115、 3D7125 和 AMP7150

3D7115、 3D7125 和 AMP7150 设备配置有四端口铜缆接口 （支持可配置旁路功能）和八个可热插拔小型可插拔 (SFP) 端口 （不支持旁路功能）。以下机箱正面示意图显示了感应接口的位置。

3D7115 和 3D7125 铜缆和 SFP 接口



四个 1000BASE-T 铜缆接口



您可使用这些铜缆接口以被动方式监控最多四个独立网段。您还可使用处于内联模式或支持旁路功能的内联模式的成对接口，将设备在最多两个网络上部署为入侵防御系统。

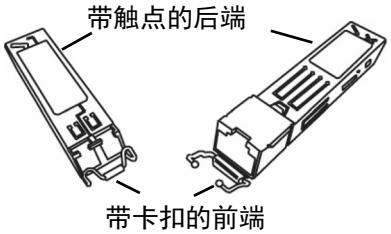
如果希望利用设备的自动旁路功能，则必须将左侧的两个接口或右侧的两个接口连接至网段。即使设备发生故障或断电，自动旁路功能也允许流量通过。在使用电缆连接接口后，您可通过网络界面将一对接口配置为内联集，并在该内联集上启用旁路模式。

SFP 接口

当您将 Sourcefire SFP 收发器安装到 SFP 插槽时，您可以被动方式监控最多八个独立网段。您还可以使用内联非旁路模式下的成对接口，在多达四个网络上将设备部署为入侵检测系统。

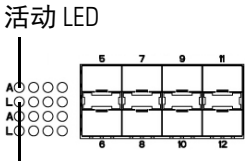
SourcefireSFP 收发器可提供 1G 铜缆、 1G 短距离光纤或 1G 长距离光纤版本，且支持热插拔功能。您可以在被动或内联配置的设备中使用铜缆或光收发器的任意组合。请注意， SFP 收发器没有旁路功能，不应用于入侵防御部署。为确保兼容性，请仅使用 Sourcefire 提供的 SFP 收发器。有关详细信息，请参阅第 231 页的在 3D7115、 3D7125 和 AMP7150 设备中使用 SFP 收发器。

样本 SFP 收发器



样本光纤　　样本铜缆

SFP 插槽



Sourcefire 8000 系列

Sourcefire 8000 系列作为 1U 设备提供，配置有 10G 网络交换机；或作为 2U 设备提供，配置有 10G 或 40G 网络交换机。此设备可以完全装配后装运，或者您也可以安装包含感应接口的网络模块 (NetMod)。

重要！ 如果您在设备的不兼容插槽中安装网络模块 （例如，将 40G 网络模块插入 3D8250 或 3D8350 上的插槽 1 和 4）或网络模块与系统不兼容，当您尝试配置该网络模块时，管理防御中心的网络界面中将显示错误或警告消息。请与 Sourcefire 支持人员联系请求协助。

以下模块包含可配置旁路感应接口：

- 四端口 1000BASE-T 铜缆接口 （支持可配置旁路功能）
- 四端口 1000BASE-SX 光纤接口 （支持可配置旁路功能）
- 双端口 10GBASE （MMSR 或 SMLR）光纤接口 （支持可配置旁路功能）
- 双端口 40GBASE-SR4 光纤接口 （支持可配置旁路功能）（仅限于 2U 设备）

以下模块包含非旁路感应接口：

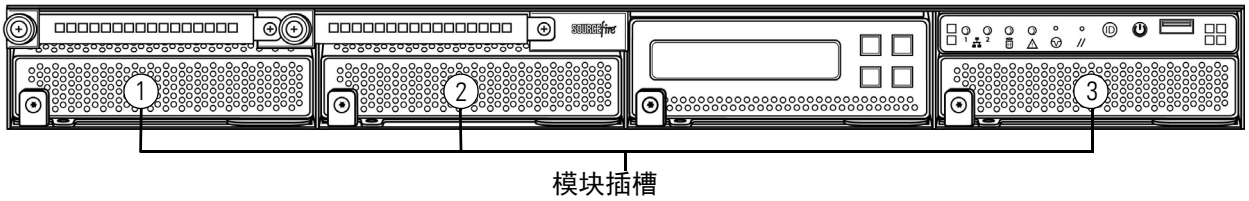
- 四端口 1000BASE-T 铜缆接口 （不支持旁路功能）
- 四端口 1000BASE-SX 光纤接口 （不支持旁路功能）
- 双端口 10GBASE （MMSR 或 SMLR）光纤接口 （不支持旁路功能）

此外，堆栈模块组合两个或更多配置相同的设备的资源。堆栈模块在 3D8140、3D8250 和 3D8350 上为可选组件；在 3D8260、 3D8270、 3D8290 和 3D8360、3D8370、 3D8390 堆栈配置中提供了堆栈模块。

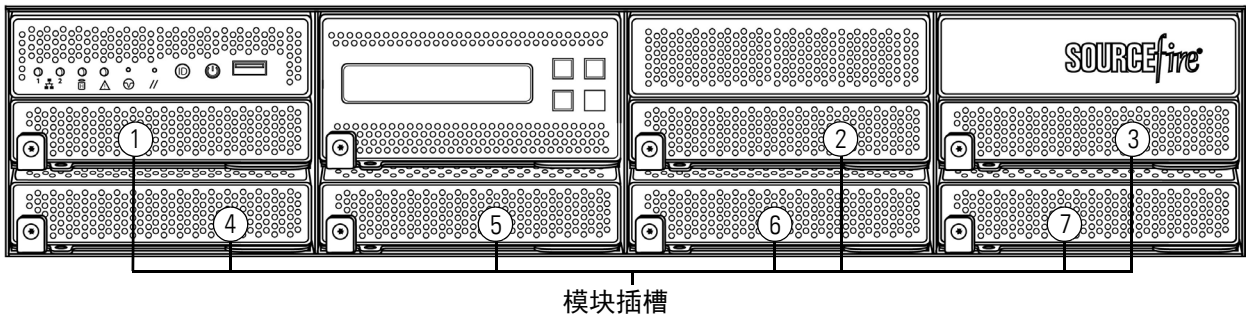
警告！ 模块**不可**热插拔。有关详细信息，请参阅第 234 页的插入或拆除 8000 系列模块。

以下机箱正面示意图显示包含感应接口的模块插槽的位置。

81xx 系列机箱前视图



82xx 系列和 83xx 系列机箱前视图



8000 系列模块

8000 系列可随以下支持可配置旁路功能的模块提供：

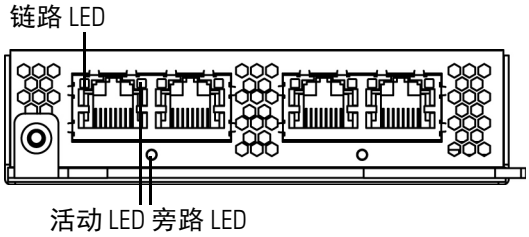
- 四端口 1000BASE-T 铜缆接口 （支持可配置旁路功能）。有关详细信息，请参阅第 62 页的四端口 1000BASE-T 铜缆可配置旁路网络模块。
- 四端口 1000BASE-SX 光纤接口 （支持可配置旁路功能）。有关详细信息，请参阅第 62 页的四端口 1000BASE-SX 光纤可配置旁路网络模块。
- 双端口 10GBASE （MMSR 或 SMLR）光纤接口 （支持可配置旁路功能）。有关详细信息，请参阅第 63 页的双端口 10GBASE （MMSR 或 SMLR）光纤可配置旁路网络模块。
- 双端口 40GBASE-SR4 光纤接口 （支持可配置旁路功能）。有关详细信息，请参阅第 63 页的双端口 40GBASE-SR4 光纤可配置旁路网络模块。

8000 系列可随以下不支持可配置旁路功能的模块提供：

- 四端口 1000BASE-T 铜缆接口 （不支持旁路功能）。有关详细信息，请参阅第 64 页的四端口 1000BASE-T 铜缆非旁路网络模块。
- 四端口 1000BASE-SX 光纤接口 （不支持旁路功能）。有关详细信息，请参阅第 64 页的四端口 1000BASE-SX 光纤非旁路网络模块。
- 四端口 10GBASE （MMSR 或 SMLR）光纤接口 （不支持旁路功能）。有关详细信息，请参阅第 65 页的四端口 10GBASE （MMSR 或 SMLR）光纤非旁路网络模块。

堆栈模块在 3D8140、 3D8250 和 3D8350 上为可选组件；在 3D8260、 3D8270、 3D8290 和 3D8360、 3D8370、 3D8390 堆栈配置中提供了堆栈模块。有关详细信息，请参阅第 65 页的8000 系列堆栈模块。

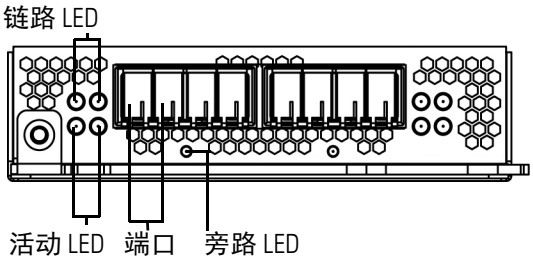
四端口 1000BASE-T 铜缆可配置旁路网络模块



您可以使用这些连接以被动方式监控多达四个独立网段。您还可以使用内联模式的或与旁路模式内联的成对接口将设备部署为最多两个网络上的入侵防御系统。

如果希望利用设备的自动旁路功能，则必须将左侧的两个接口或右侧的两个接口连接至网段。这样，即使设备发生故障或断电，也允许流量通过。您还必须通过网络界面将一对接口配置为内联集，并在该内联集上启用旁路模式。

四端口 1000BASE-SX 光纤可配置旁路网络模块



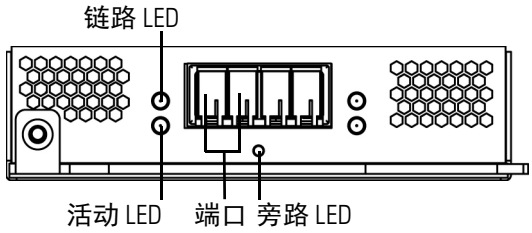
四端口 1000BASE-SX 光纤可配置旁路配置使用 LC 类型 （本地连接器）光收发器。

您可使用此配置以被动方式监控最多四个独立网段。您还可使用内联模式的或与旁路模式内联的成对接口将受管设备部署为最多两个网络上的入侵防御系统。

提示！ 为获得最佳性能，请连续使用接口集。如您跳过接口，则可能会发生性能降级。

如果希望利用设备的自动旁路功能，则必须将左侧的两个接口或右侧的两个接口连接至网段。这样，即使设备发生故障或断电，也允许流量通过。您还必须通过网络界面将一对接口配置为内联集，并在该内联集上启用旁路模式。

双端口 10GBASE （MMSR 或 SMLR）光纤可配置旁路网络模块



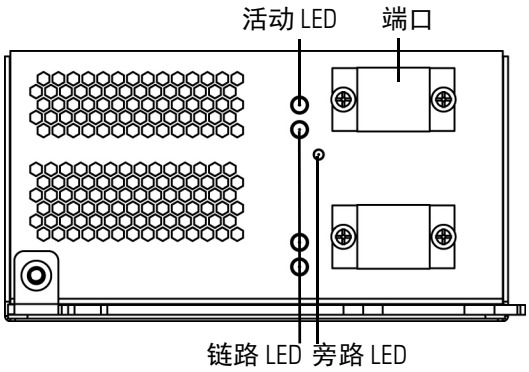
双端口 10GBASE 光纤可配置旁路配置使用 LC 类型 （本地连接器）光收发器。请注意，这些接口可以是 MMSR 或 SMLR 接口。

您可使用该配置以被动方式监控最多两个独立网段。您还可使用内联模式的或与旁路模式内联的成对接口将受管设备部署为单个网络上的入侵防御系统。

提示！ 为获得最佳性能，请连续使用接口集。如您跳过接口，则可能会发生性能降级。

如果希望利用设备的自动旁路功能，则必须将两个接口连接至网段。这样，即使设备发生故障或断电，也允许流量通过。您还必须通过网络界面将一对接口配置为内联集，并在该内联集上启用旁路模式。

双端口 40GBASE-SR4 光纤可配置旁路网络模块



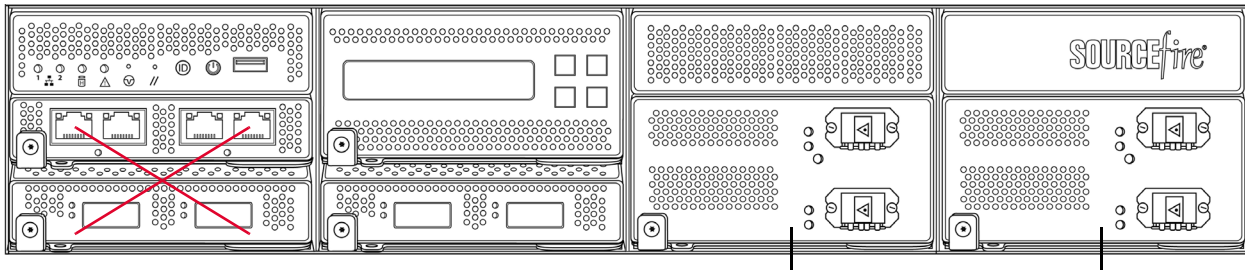
双端口 40GBASE-SR4 光纤可配置旁路配置使用 MPO （多光纤插拔式）连接器光收发器。

您只能在 3D8270、 3D8290、 3D8360、 3D8370 和 3D8390 或支持 40G 的 3D8250、3D8260 和 3D8350 中使用 40G 网络模块。如果您尝试在不支持 40G 的设备上创建 40G 接口，在其管理防御中心网络界面上的 40G 接口屏幕将显示红色。支持 40G 的 3D8250 在 LCD 面板上显示“3D 8250-40G”，支持 40G 的 3D8350 在 LCD 面板上显示“3D 8350-40G”。

您可使用该配置以被动方式监控最多两个独立网段。您还可使用内联模式的或与旁路模式内联的成对接口将设备部署为一个网络上的入侵防御系统。

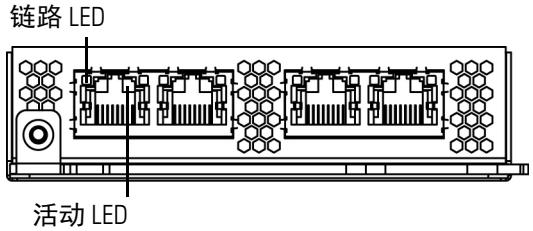
您可使用最多两个 40G 网络模块。将第一个 40G 网络模块安装在插槽 3 和 7 中，将第二个 40G 网络模块安装在插槽 2 和 6 中。在插槽 1 和 4 中不能使用 40G 网络模块。

40G 网络模块布局



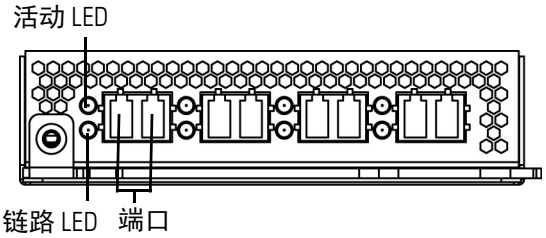
如果希望利用设备的自动旁路功能，则必须使用网络界面将一对接口配置为内联集并对该内联集启用旁路模式。

四端口 1000BASE-T 铜缆非旁路网络模块



您可以使用这些连接以被动方式监控多达四个独立网段。您还可在最多两个网段的内联配置中使用成对的接口。

四端口 1000BASE-SX 光纤非旁路网络模块

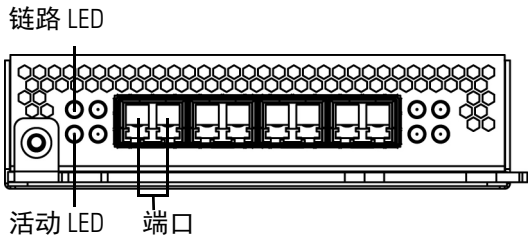


四端口 1000BASE-SX 光纤非旁路配置使用 LC 类型 （本地连接器）光收发器。

您可以使用这些连接以被动方式监控多达四个独立网段。您还可在最多两个网段的内联配置中使用成对的接口。

提示！ 为获得最佳性能，请连续使用接口集。如您跳过接口，则可能会发生性能降级。

四端口 10GBASE （MMSR 或 SMLR）光纤非旁路网络模块



四端口 10GBASE 光纤非旁路配置使用带 MMSR 或 SMLR 接口的 LC 类型 （本地连接器）光收发器。

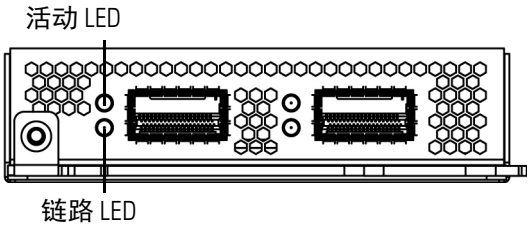
警告！ 四端口 10GBase 非旁路网络模块包含不可移除的小型可插拔 (SFP) 收发器。尝试卸下 SFP 可能损坏模块。

您可以使用这些连接以被动方式监控多达四个独立网段。您还可在最多两个网段的内联配置中使用成对的接口。

提示！ 为获得最佳性能，请连续使用接口集。如您跳过接口，则可能会发生性能降级。

8000 系列堆栈模块

堆栈模块组合两个或更多配置相同的设备的资源。堆栈模块在 3D8140、 3D8250 和 3D8350 上为可选组件；在 3D8260、3D8270、3D8290 和 3D8360、3D8370、3D8390 堆栈配置中提供了堆栈模块。



堆栈模块可供您组合两台设备的资源，使用一个作为主设备，另一个作为辅助设备。只有主设备具有感应接口。以下设备可使用堆栈模块：

- 3D8140、 3D8250 和 3D8350 可随堆栈模块一起提供。
- 3D8260 和 3D8360 分别随主设备和辅助设备中的一个堆栈模块提供。
- 3D8270 和 3D8370 随主设备中的两个堆栈模块以及两台辅助设备中每一台中的一个堆栈模块提供。
- 3D8290 和 3D8390 随主设备中的三个堆栈模块以及三台辅助设备中每一台中的一个堆栈模块提供。

有关使用堆栈设备的详细信息，请参阅使用堆栈配置中的设备。

使用堆栈配置中的设备

您可增加在网段上检查的流量数量，只需在堆栈配置中组合配置相同的设备的资源。一台设备被指定为主设备，并连接至到各网段。所有其他设备均被指定为辅助设备，用于向主设备提供额外资源。防御中心创建、编辑并管理堆栈配置。

主设备包含感应接口，以及为连接至主设备的每台辅助设备提供的一组堆栈接口。使用与连接非堆栈设备相同的方式将主设备上的感应接口连接至要监控的网段。将主设备上的堆栈接口通过堆栈电缆连接至辅助设备上的堆栈接口。每台辅助设备均通过堆栈接口直接连接至主设备。如果辅助设备包含感应接口，则将不使用这些接口。

您以在以下配置中使用堆栈设备：

- 两台 3D8140
- 最多四台 3D8250
- 3D8260 （一台支持 10G 的主设备和一台辅助设备）
- 3D8270 （一台支持 40G 的主设备和两台辅助设备）
- 3D8290 （一台支持 40G 的主设备和三台辅助设备）
- 最多四台 3D8350
- 3D8360 （一台支持 40G 的主设备和一台辅助设备）
- 3D8370 （一台支持 40G 的主设备和两台辅助设备）
- 3D8390 （一台支持 40G 的主设备和三台辅助设备）

对于 3D8260，3D8270、3D8360 和 3D8370，您可在堆栈配置中另行堆栈总计四台设备。

一台设备被指定为主设备，并作为主要角色显示在防御中心的网络界面上。堆栈配置中的所有其他设备均为辅助设备，并作为辅助角色显示在网络界面上。除了查看堆栈设备的信息，还可将组合资源用作单一实体。

使用与连接单台 3D8140、 3D8250 或 3D8350 相同的方式将主设备连接至要分析的网段。按照堆栈电缆连接图所示，将辅助设备连接至主设备。

在将设备以物理方式连接至网段和相互连接之后，请使用防御中心建立并管理堆栈。

以下各节提供有关如何连接并管理堆栈设备的详细信息：

- 第 67 页的连接 3D8140
- 第 67 页的连接 82xx 系列和 83xx 系列
- 第 71 页的使用 8000 系列堆栈电缆
- 第 71 页的管理堆栈设备

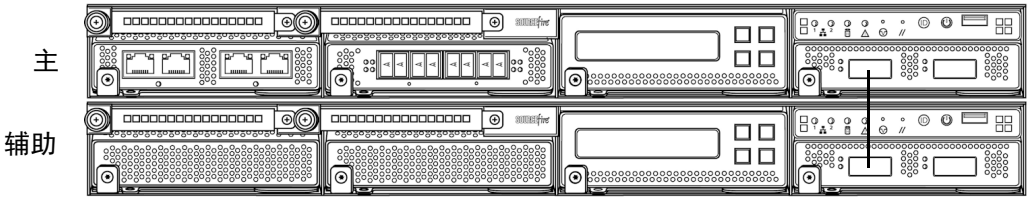
连接 3D8140

在堆栈配置中可连接两台 3D8140。您必须使用一根 8000 系列堆栈电缆在主设备与辅助设备之间创建物理连接。有关使用堆栈电缆的详细信息，请参阅第 71 页的使用 8000 系列堆栈电缆。

将设备安装在机架中，这样您就可在堆栈模块之间轻松地连接电缆。您可在主设备的上方或下方安装辅助设备。

使用与连接单台 3D8140 相同的方式将主设备连接至要分析的网段。请将辅助设备直接连接至主设备。

下图显示下方安装有辅助设备的主设备。



要连接 3D8140 辅助设备，请执行以下操作：

▶ 使用一根 8000 系列堆栈电缆将主设备的左堆栈接口连接至辅助设备的左堆栈接口，然后使用管理设备的防御中心在系统中建立堆栈设备关系。请注意，右堆栈接口未连接。请参阅第 71 页的管理堆栈设备。

连接 82xx 系列和 83xx 系列

您可连接以下任一种配置：

- 最多四台 3D8250 或四台 3D8350
- 3D8260 （一台支持 10G 的主设备和一台辅助设备）
- 3D8360 （一台支持 40G 的主设备和一台辅助设备）
- 3D8270 或 3D8370 （一台支持 40G 的主设备和两台辅助设备）
- 3D8290 或 3D8390 （一台支持 40G 的主设备和三台辅助设备）

对于 3D8260，3D8270、3D8360 和 3D8370，您可在堆栈配置中另行堆栈总计四台设备。

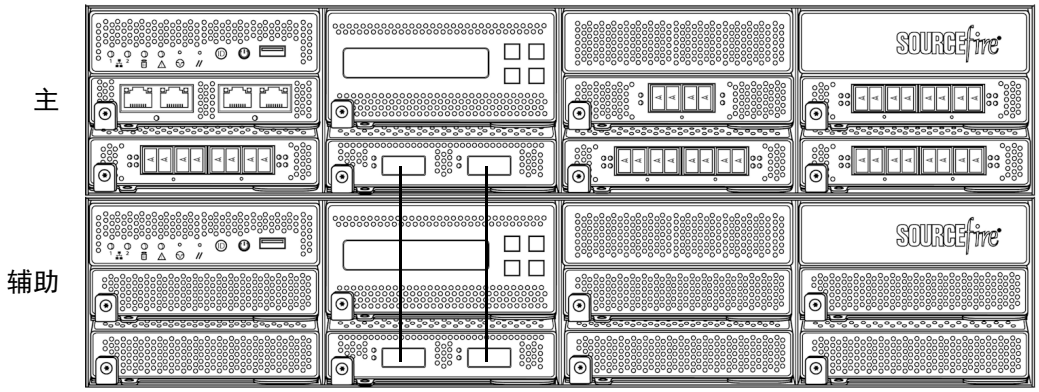
对于每台想要连接至主设备的辅助设备，必须使用两根 8000 系列堆栈电缆。有关使用堆栈电缆的详细信息，请参阅第 71 页的使用 8000 系列堆栈电缆。

将设备安装在机架中，这样您就可在堆栈模块之间轻松地连接电缆。您可在主设备的上方或下方安装辅助设备。

以与单台 3D8250 或 3D8350 设备相同的方式将主设备连接至想要分析的网段。根据配置中需要的辅助设备数量将每台辅助设备直接连接至主设备。

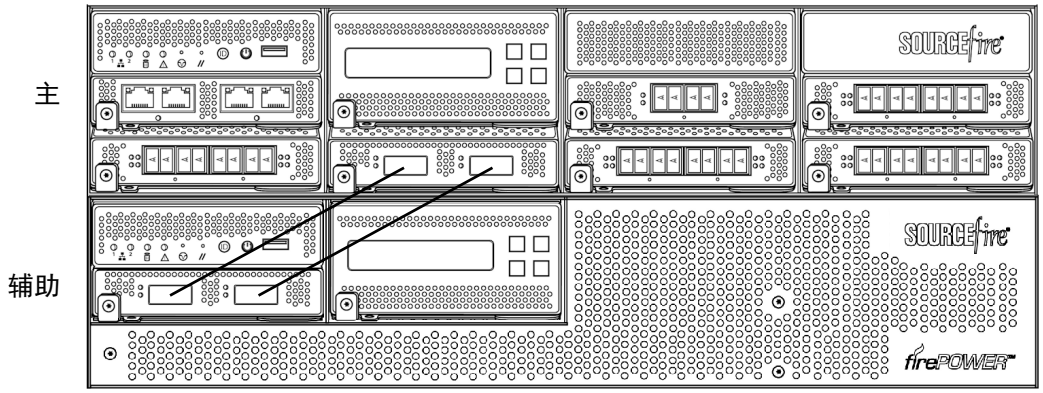
具有一台辅助设备的 3D8250 或 3D8350 主设备

以下示例显示 3D8250 或 3D8350 主设备和一台辅助设备。辅助设备安装在主设备下方。请注意，辅助设备不包含感应接口。



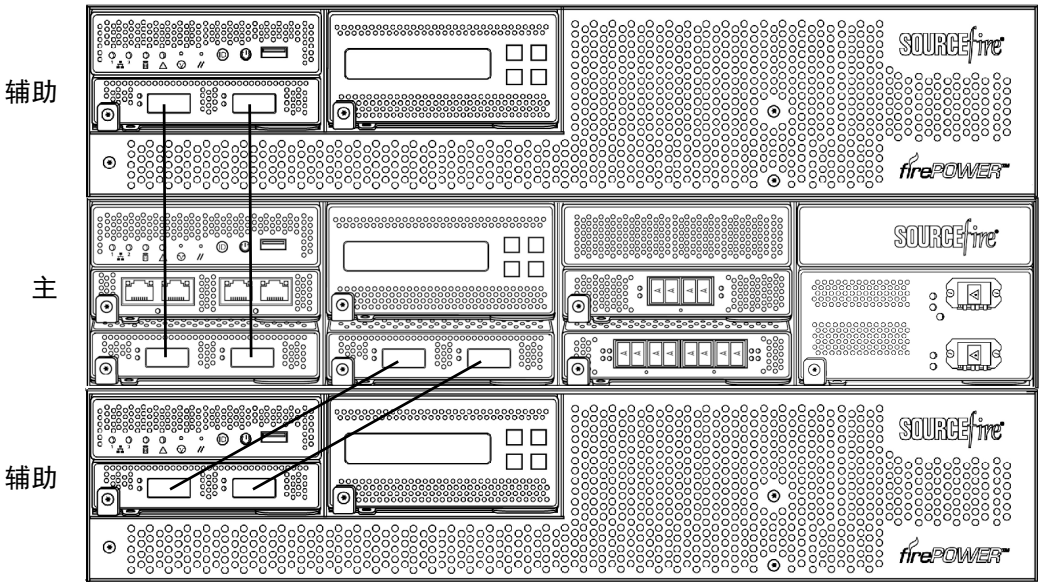
3D8260 或 3D8360 主设备以及一台辅助设备

以下示例显示了 3D8260 或 3D8360 的配置。 3D8260 包括一台支持 10G 的 3D8250 主设备和一台专用辅助设备。3D8360 包括一台支持 40G 的 3D8350 主设备和一台专用辅助设备。对于每种配置 （3D8260 或 3D8360），辅助设备均安装在主设备下方。



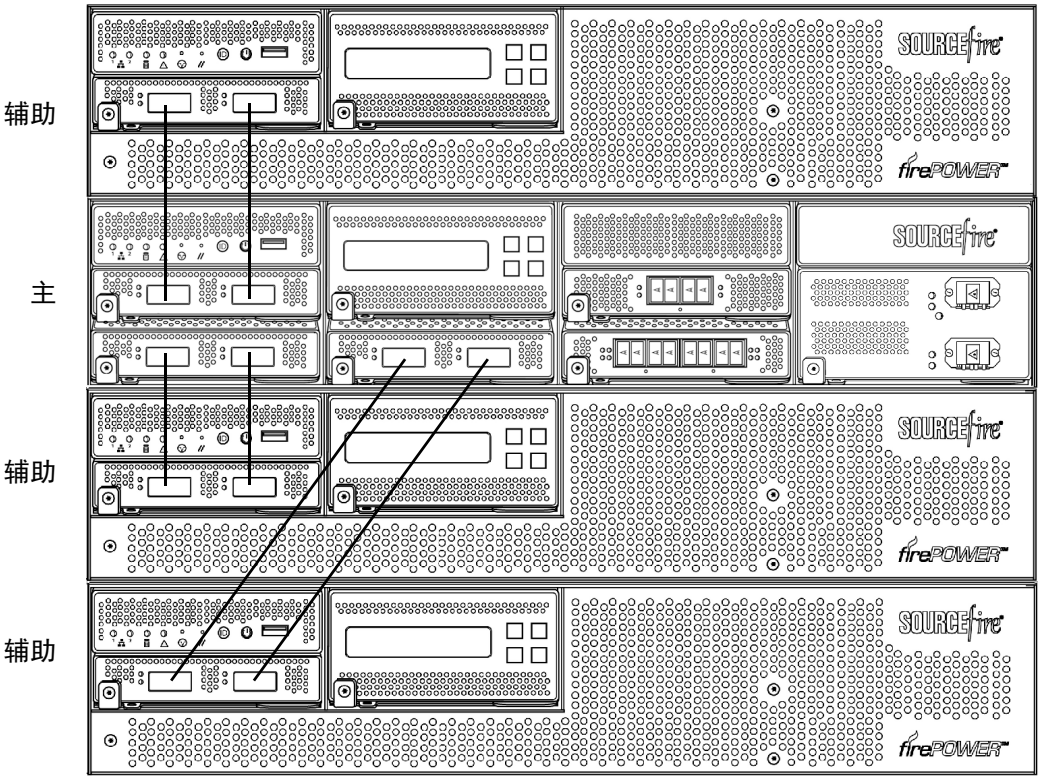
3D8270 或 3D8370 主设备 (40G) 和两台辅助设备

以下示例显示了 3D8270 或 3D8370 的配置。 3D8270 包括一台支持 40G 的 3D8250 主设备和两台专用辅助设备。3D8370 包括一台支持 40G 的 3D8350 主设备和两台专用辅助设备。对于每种配置 （3D8270 或 3D8370），一台辅助设备安装在主设备上方，另一台安装在主设备下方。



3D8290 或 3D8390 主设备 (40G) 和三台辅助设备

以下示例显示了 3D8290 或 3D8390 的配置。 3D8290 包括一台支持 40G 的 3D8250 主设备和三台专用辅助设备。3D8370 包括一台支持 40G 的 3D8350 主设备和两台专用辅助设备。对于每种配置 （3D8290 或 3D8390），一台辅助设备安装在主设备上方，两台辅助设备安装在主设备下方。

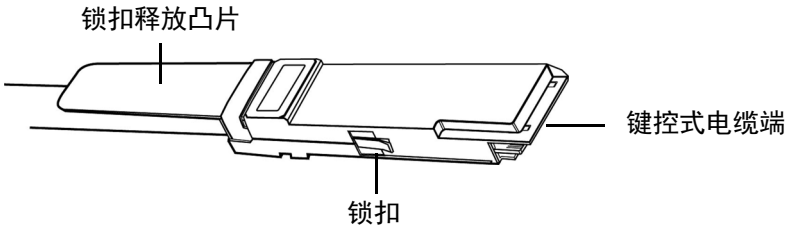


要连接 3D8250 或 3D8350 辅助设备，请执行以下操作：

1. 使用一根 8000 系列堆栈电缆将主设备上堆栈模块的左接口连接至辅助设备上堆栈模块的左接口。
2. 使用另一根 8000 系列堆栈电缆将主设备上堆栈模块的右接口连接至辅助设备上堆栈模块的右接口。
3. 对要连接的每台辅助设备重复步骤 1 和 2。
4. 使用管理设备的防御中心建立堆栈设备关系并管理其共同资源。请参阅第 71 页的管理堆栈设备。

使用 8000 系列堆栈电缆

8000 系列堆栈电缆有以相同方式键控的端部，每个端部均带锁扣，用于将电缆固定在设备中的锁扣和锁扣释放凸片。



按每种设备配置的要求使用 8000 系列堆栈电缆在主设备与每台辅助设备之间创建物理连接：

- 3D8250、 3D8260、 3D8270 和 3D8290 每条连接均需要两根电缆
- 3D8350、 3D8360、 3D8370 和 3D8390 每条连接均需要两根电缆
- 3D8140 需要一根电缆

插入或拔出堆栈电缆时不需要关闭设备电源。

警告！ 连接设备时，请仅使用 Sourcefire 8000 系列堆栈电缆。使用不受支持的电缆可能导致不可预见的错误。

在设备物理连接后，请使用防御中心管理堆栈设备。

要插入 8000 系列堆栈电缆，请执行以下操作：

▶ 要插入电缆，请按住释放凸片朝上的电缆端部头，然后将键控端部插入堆栈模块的端口，直至听到锁扣卡入到位。

要拔出 8000 系列堆栈电缆，请执行以下操作：

▶ 要拔出电缆，请拉释放凸片以释放锁扣，然后拔出电缆端部。

管理堆栈设备

防御中心建立设备之间的堆栈关系、控制主设备的接口集并管理堆栈中的组合资源。不能在堆栈设备的本地网络界面上管理接口集。

在堆栈关系已建立后，每台设备将使用单一的共享检测配置分别检查流量。如果主设备发生故障，将根据主设备的配置处理流量 （也就是说，如同堆栈关系不存在一样）。如果辅助设备发生故障，主设备将继续感知流量、生成警报并将流量从中断位置继续发送至有故障的辅助设备。

有关建立和管理堆栈设备的信息，请参阅 《*Sourcefire 3D 系统用户指南*》中的 “管理堆栈设备” 一节。

在机架中安装设备

Sourcefire 3D 系统在不同的硬件平台上提供。您可在机架中安装所有 Sourcefire 设备 （为 3D7010、 3D7020 和 3D7030 购买 1U 安装套件）。安装设备时，您必须确保自己能够访问设备的控制台。要访问控制台进行初始设置，请通过以下其中一种方式连接至 Sourcefire 设备：

键盘和显示器/KVM

您可将 USB 键盘和 VGA 显示器连接至任何 Sourcefire 设备，该设备对于连接至键盘、视频和鼠标 (KVM) 切换器的机架安装式设备很有用。

到管理接口的以太网连接

使用以下设置配置一台本地计算机，该计算机不得连接至互联网：

- IP 地址：192.168.45.2
- 子网掩码：255.255.255.0
- 默认网关：192.168.45.1

使用以太网电缆将本地计算机上的网络接口连接至设备的管理接口。要与设备交互，请使用终端仿真软件 （例如， HyperTerminal 或 Xmodem）。此软件的设置为 9600 波特、 8 个数据位、无奇偶校验、 1 个停止位和无流量控制。

请注意，物理 Sourcefire 设备的管理接口已用默认 IPv4 地址进行配置。但是，在设置过程中，您可用 IPv6 地址重新配置管理接口。

在初始设置后，可通过以下其他方式访问控制台：

串行连接/笔记本电脑

您可使用串行电缆将计算机连接至任何 Sourcefire 设备。要与设备交互，请使用上述终端仿真软件。

使用局域网串行连接执行无人值守管理

LOM 功能可供您使用局域网串行 (SOL) 连接 在 3 系列设备上执行一组有限的管理操作，包括恢复为出厂默认设置。有关详细信息，请参阅第 194 页的设置无人值守管理。

默认情况下， Sourcefire 设备会将初始化状态或 *init* 消息发送至 VGA 端口。如果要使用物理串行端口或 SOL 访问控制台，Sourcefire 建议您在完成初始设置之后，将控制台输出重定向至串行端口。有关详细信息，请参阅第 74 页的重定向控制台输出。

要安装设备，请执行以下操作：

1. 使用安装套件及其随附的说明，将设备安装在机架中。
2. 使用键盘和显示器或以太网连接连接至设备。
3. 如果您使用键盘和显示器设置设备，请立即使用以太网电缆将管理接口连接至受保护的网段。

   如果您计划通过将计算机直接连接至设备的物理管理接口来执行初始设置过程，在完成设置时，您需要将此管理接口连接至受保护的网络。
4. 对于受管设备，请使用适合接口的电缆将感应接口连接到要分析的网段：
   - 铜缆感应接口：如果设备包括铜缆感应接口，请确保使用适当的电缆将它们连接至网络；请参阅第 31 页的在铜缆端口接口上进行内联部署布线。
   - 光纤适配器卡：对于带光纤适配器卡的设备，将可选多模光缆的 LC 连接器连接至适配器卡的两个端口 （按任意顺序）。将 SC 插头插入到要分析的网段。
   - 光纤分路器：如在部署有可选光纤分路器的设备，请将可选多模光缆上的 SC 插头插入分路器上的 " 分析器 " 端口。将分路器连接到要分析的网段。
   - 铜缆分路器：如在部署有可选铜缆分路器的设备，请将分路器左侧的 A 和 B 端口连接至要分析的网段。将分路器右侧的 A 和 B 端口 （ " 分析器 " 端口）连接至适配器卡的两个铜缆端口。

   有关用于部署受管设备的选项的详细信息，请参阅第 27 页的了解部署选项。

   请注意，如果您在部署有旁路接口的设备，则是在利用设备的功能在即使设备有故障时仍保持网络连接。有关安装和延迟测试的信息，请参阅第 75 页的测试内联旁路接口安装。
5. 将电源线连接至设备并插入电源。

   如果设备有冗余电源，请将电源线连接至两个电源并将它们插入单独电源。
6. 打开设备。

   如果您在使用直接以太网连接设置设备，请确认本地计算机上网络接口和设备上管理接口的链路 LED 均已点亮。如果管理接口和网络接口 LED 不亮，请尝试使用交叉电缆。有关详细信息，请参阅第 31 页的在铜缆端口接口上进行内联部署布线。
7. 请继续下一章：第 77 页的设置Sourcefire 3D 系统设备。

重定向控制台输出

默认情况下， Sourcefire 设备会将初始化状态或 *init* 消息发送至 VGA 端口。如果将设备恢复至出厂默认值并删除其许可证和网络设置，则恢复实用程序也将控制台输出重置为 VGA。如果要使用物理串行端口或 SOL 访问控制台， Sourcefire 建议您在完成初始设置之后，将控制台输出重定向至串行端口。

要重定向控制台输出，请从设备的 Shell 运行脚本。下表列出了根据计划访问设备的方式应使用的控制台。

控制台重定向选项

选项	设置
VGA （默认值）	`tty0`
物理串行	`ttyS0`
基于 SOL 的 LOM	`ttyS0`

请注意，虽然所有 3 系列设备均支持 LOM，但 7000 系列设备不支持同时进行 LOM 和物理串行访问。但是，无论您要使用哪种方式，控制台设置均相同。

要重定向控制台输出，请执行以下操作：

访问： 管理员

1. 以具有管理员权限的帐户身份使用键盘/显示器或串行连接登录设备。密码与设备网络界面的密码相同。

   系统将显示设备提示符。

2. 在提示符处，访问设备上的 root 权限：
   - 在防御中心上，键入 `sudo su -` 并再次提供密码。
   - 在 3 系列受管设备上，键入 `expert` 以显示 Shell 提示符。然后，键入 `sudo su -` 并再次提供密码。

   系统将显示 root 提示符。

3. 通过键入以下内容设置控制台输出：

   ```
   /usr/local/sf/bin/set_console.sh -c console_value
   ```

   其中 *console_value* 代表您计划用于访问设备的方法，如以上控制台重定向选项表中所述。

4. 要实施更改，请通过键入 `reboot` 来重新启动设备。

   设备重新启动。

测试内联旁路接口安装

具有旁路接口的受管设备可维护网络连接性，即使在设备关闭或无法运行时也如此。务必确保已正确安装这些设备并量化由其安装引起的任何延迟。

重要！ 交换机的生成树发现协议将导致 30 秒流量延迟。 Sourcefire 建议在以下操作步骤期间禁用生成树。

以下操作步骤仅适用于铜缆接口，介绍如何测试内联旁路接口的安装和 ping 延迟。您需要连接至网络以运行 ping 测试并连接至受管设备控制台。

要通过内联旁路接口安装测试设备，请执行以下操作：

访问： 管理员

1. 确保已为内联旁路模式配置设备的接口集类型。

   请参阅《*Sourcefire 3D 系统用户指南*》中的“配置内联集”一章，了解有关为内联旁路模式配置接口集的说明。

2. 将交换机和防火墙上的所有接口以及设备感应接口均设置为自动协商。

   重要！ 当在设备上使用自动 MDIX 时，思科设备需要自动协商。

3. 关闭设备并断开所有网络电缆。

   重新连接设备并确保有合适的网络连接。检查从设备到交换机和防火墙的交叉与和直通连接连线说明，请参阅第 31 页的在铜缆端口接口上进行内联部署布线。

4. 在关闭设备电源的情况下，请确保您能够从防火墙通过设备 ping 到交换机。

   如果 ping 失败，请纠正网络连线。

5. 请运行连续 ping，直至您完成第 10 步。

6. 重新为设备接通电源。

7. 以具有管理员权限的帐户身份使用键盘/显示器或串行连接登录设备。密码与设备网络界面的密码相同。

   系统将显示设备提示符。

8. 通过键入 `system shutdown` 关闭设备。

   您也可使用设备的网络界面关闭设备；请参阅《*Sourcefire 3D 系统用户指南*》中的“管理设备”一章。大多数设备关闭时会发出咔嗒声。此咔嗒声是中继交换和设备进入硬件旁路模式的声音。

9. 等待 30 秒。

   确认您的 ping 流量已恢复。

10. 重新启动设备，并确认您的 ping 流量继续通过。
11. 对于支持分路器模式的设备，您可在以下一组条件下测试和记录 ping 延迟结果：
    - 设备已关闭
    - 设备已启动，应用了不包含规则的策略，内联入侵策略保护模式
    - 设备已启动，应用了不包含规则的策略，内联入侵策略分路器模式
    - 设备已启动，应用了包含已调整规则的策略，内联入侵策略保护模式

    请确保您的安装可接受延迟时间。有关解决延迟过长问题的信息，请参阅《*Sourcefire 3D 系统用户指南*》中的“配置数据包延迟阈值和了解规则延迟阈值”。

第 4 章

设置SOURCEFIRE 3D 系统设备

在部署并安装 Sourcefire 设备后，必须完成设置过程，以便新设备能够在受信任管理网络上通信。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，您还可以执行多种初始管理级别任务，例如，设置时间、注册设备和获得设备许以及调度更新。您在设置和注册过程中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体验和帮助您快速设置部署，而不是限制您的选项。无论您最初如何配置设备，在使用防御中心时您可以随时更改其配置。换句话说，例如，在设置过程中选择检测模式或访问控制策略，不会将您局限于特定设备、区域或策略配置。

有关初始设置过程中每个步骤的详细信息，请参阅以下各节：

- 第 78 页的了解设置过程概述设置过程，该过程取决于设备的型号以及您能否亲身接近设备。

  重要！ 如果您尚不熟悉设置过程， Sourcefire **强烈**建议您先阅读本节。

- 第 80 页的使用脚本配置网络设置说明如何使用脚本指定网络设置，从而使新设备能够在管理网络上通信。对于您使用键盘和显示器访问的所有防御中心，此步骤是必需的。
- 第 81 页的使用 CLI 在 3 系列设备上执行初始设置说明如何使用交互式命令行界面 (CLI) 在 3 系列设备上执行设置过程。

- 第 84 页的初始设置页面：设备说明如何使用任何设备的网络界面完成其初始设置。
- 第 89 页的初始设置页面：防御中心说明如何使用防御中心的网络界面完成其初始设置。
- 第 96 页的后续步骤包含有关您在设置 Sourcefire 3D 系统部署之后可能希望执行的设置后任务的指导。

警告！ 本章中的操作步骤说明如何在不关闭设备电源的情况下对其进行设置。但是，如果由于任何原因需要关闭电源，请按照《Sourcefire 3D *系统用户指南*》中的“管理设备”章节中的操作步骤，从 3 系列设备上的 CLI 运行 `system shutdown` 命令，或从设备的外壳（有时称为专家模式）运行 `shutdown -h now` 命令。

了解设置过程

在部署并安装新Sourcefire设备后，如本指南前几章所述，您必须完成设置过程。在开始安装之前，请确保满足下列条件。

设备型号

您必须知道要设置的设备型号。 Sourcefire *设备*为流量感知受管*设备*或管理*防御中心*：每种设备类型有若干*型号*；这些型号进一步分为多个*产品系列*。有关详细信息，请参阅第 11 页的了解设备系列、型号和功能。

访问

要设置新设备，您必须使用键盘和显示器/KVM （键盘、视频和鼠标）或到设备管理接口的直接以太网连接。在初始设置后，您可以配置串行接入的设备。有关详细信息，请参阅第 72 页的在机架中安装设备。

信息

您至少具有使设备能够在管理网络上通信所需的信息：IPv4 或 IPv6 管理 IP 地址、子网掩码或前缀长度和默认网关。

如果您知道如何部署设备，安装程序也很适合执行许多初始管理级别任务，包括注册和许可。

提示！ 如果要部署多个设备，请先设置设备，然后再设置它们的管理防御中心。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。

在完成设置后，您将使用防御中心的网络界面执行部署的大多数管理和分析任务。物理受管设备提供可用于执行基本管理任务的受限网络界面。有关详细信息，请参阅第 96 页的后续步骤。

有关如何设置各种 Sourcefire 设备的详细信息，请参阅：

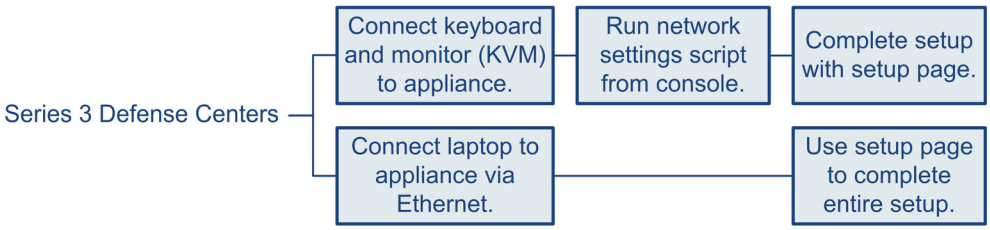
- 第 79 页的设置 3 系列防御中心
- 第 80 页的设置 3 系列设备

提示！ 如果在将设备恢复到出厂默认设置（请参阅第 176 页的将 Sourcefire 设备恢复至出厂默认设置）后对设备进行设置，并且未删除设备的许可证和网络设置，您可以使用管理网络上的计算机直接浏览到设备的网络界面执行设置。请跳至第 84 页的初始设置页面：设备或第 89 页的初始设置页面：防御中心。

设置 3 系列防御中心

支持的防御中心：3 系列

以下图表说明您在设置 3 系列防御中心时选择的选项：



要设置 3 系列防御中心，请执行以下操作：

访问：管理员

1. 如果您使用键盘和显示器，请运行帮助您配置设置的脚本以使设备能够在管理网络上通信；请参阅第 80 页的使用脚本配置网络设置。

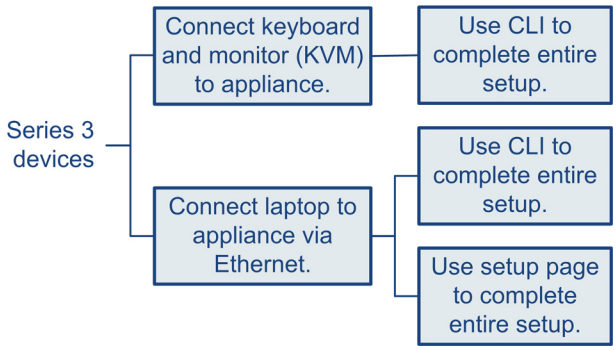
   如果您正在设置一个重新映象设备，并且在恢复过程中保留了网络设置，或者，如果您通过直接以太网连接访问设备，请跳至下一步。

2. 通过从管理网络上的计算机浏览到设备的网络界面完成设置过程：
   - 要使用其网络界面完成受管设备的设置，请参阅第 84 页的初始设置页面：设备。
   - 要使用其网络界面完成防御中心的设置，请参阅第 89 页的初始设置页面：防御中心。

设置 3 系列设备

支持的设备：3 系列

以下图表说明您在设置 3 系列设备时选择的选项：



您对 3 系列设备的访问方式决定了您如何设置该设备。您有以下选项：

- 无论如何连接到设备，您都可以使用 CLI 对设备进行设置；请参阅第 81 页的使用 CLI 在 3 系列设备上执行初始设置。
- 如果您通过直接以太网连接访问设备，您可以从本地计算机浏览到设备的网络界面；请参阅第 84 页的初始设置页面：设备。

如果您正在设置一个重新映象设备，并且在恢复过程中保留了网络设置，您可以通过 SSH 或无人值守管理 (LOM) 连接访问 CLI。您也可以从管理网络上的计算机浏览到设备的网络界面。

使用脚本配置网络设置

支持的设备：2 系列

在安装新防御中心或 2 系列设备或在重新映像期间删除其网络设置后，您必须配置设备以使其能够在管理网络上通信。请通过从控制台运行脚本执行此步骤。

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，然后再配置 IPv6。对于 IPv6 部署，您可以从本地路由器获取设置。您必须提供 IPv4 或 IPv6 管理 IP 地址、子网掩码或前缀长度和默认网关。

当遵循脚本提示操作时，多选项问题的的选项在括号内列出，例如，(y/n)。默认选项在方括号中列出，例如，[y]。按 Enter 键确认选择。

请注意，脚本提示您的设置信息与设备设置网络页面所显示的信息大多数都相同。有关详细信息，请参阅第 85 页的网络配置 （设备）和第 91 页的网络配置 （防御中心）。

要使用脚本配置网络设置，请执行以下操作：

访问：管理员

1. 在控制台上，请登录设备。

   以 admin 作为用户名，以 Sourcefire 作为密码。

2. 在管理员提示符下，输入 sudo su -，然后再次键入密码 （如果提示），切换至根用户。

3. 在根提示符下运行以下脚本：

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

4. 遵循脚本的提示。

   首先配置 （或禁用） IPv4 管理设置，然后再配置 IPv6。如果手动指定网络设置，您必须：

   - 输入点分十进制格式 IPv4 地址，包括子网掩码。例如，您可以指定子网掩码 255.255.0.0。
   - 输入以冒号分隔的十六进制形式 IPv6 地址。为 IPv6 前缀指定位数；例如，前缀长度为 112。

5. 确认设置是正确的。

   如果输入了不正确的设置，请提示符键入 n 并按 Enter 键。您可以输入正确的信息。当实施设置时，控制台可能显示消息。

6. 从设备注销。

7. 您的下一步取决于设备：

   - 要使用其网络界面完成受管设备的设置，请继续执行第 84 页的初始设置页面：设备。
   - 要使用其网络界面完成防御中心设置，请继续执行第 89 页的初始设置页面：防御中心。

使用 CLI 在 3 系列设备上执行初始设置

支持的设备：3 系列

或者，您可以使用 CLI 来配置 3 系列设备而不是使用该设备的网络界面。当您使用 CLI 首次登录新配置的设备时，您必须阅读并接受 EULA。然后，请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。最后，将设备注册至管理设备的防御中心。

当遵循设置提示操作时，选项在括号内列出，例如，(y/n)。默认选项在方括号中列出，例如，[y]。按 Enter 键确认选择。

请注意， CLI 提示您的设置信息与设备设置网络页面所显示的相同。有关这些选项的详细信息，请参阅第 84 页的初始设置页面：设备。

要使用 CLI 在 3 系列设备上完成初始设置，请执行以下操作：

访问：管理员

1. 请登录设备。以 admin 作为用户名，以 Sourcefire 作为密码。
   - 对于连接显示器和键盘的 3 系列设备，请登录控制台。
   - 如果您使用以太网线缆将计算机连接至 3 系列设备的管理接口，请通过 SSH 连接至该接口的默认 IPv4 地址：192.168.45.45。

   设备立即提示您阅读 EULA。
2. 阅读并接受 EULA。
3. 更改管理员帐户的密码。此帐户拥有管理员权限，无法删除。

   Sourcefire 建议您使用至少包含八个混合大小写的字母数字字符并至少包含一个数字字符的强密码。请避免使用词典中出现的单词。有关详细信息，请参阅第 85 页的更改密码。
4. 配置设备的网络设置。

   首先配置 （或禁用） IPv4 管理设置，然后再配置 IPv6。如果手动指定网络设置，您必须：
   - 输入点分十进制格式 IPv4 地址，包括子网掩码。例如，您可以指定子网掩码 255.255.0.0。
   - 输入以冒号分隔的十六进制形式 IPv6 地址。为 IPv6 前缀指定位数；例如，前缀长度为 112。

   有关详细信息，请参阅第 85 页的网络配置。当实施设置时，控制台可能显示消息。
5. 请选择是否允许使用 LCD 面板更改设备的网络设置。

   警告！启用此选项可能会引起安全风险。要使用 LCD 面板配置网络设置，您只需亲身接近，而无需进行身份验证。有关详细信息，请参阅第 98 页的使用 3 系列设备上的 LCD 面板。
6. 请根据设备的部署方式指定检测模式。

   有关详细信息，请参阅第 87 页的检测模式。当实施设置时，控制台可能显示消息。完成后，设备提醒您将设备注册至防御中心并显示 CLI 提示符。
7. 要使用 CLI 将设备注册至管理设备的防御中心，请继续下一部分：使用 CLI 将 3 系列设备注册至防御中心。

   您必须使用防御中心来管理设备。如果您现在不注册设备，稍后必须登录并注册设备，然后才能将其添加到防御中心。
8. 从设备注销。

使用 CLI 将 3 系列设备注册至防御中心

支持的设备：3 系列

如果您使用 CLI 配置 3 系列设备， Sourcefire 建议您在设置脚本执行结束时使用 CLI 将设备注册至防御中心。因为在初始设置过程中，您已登录设备的 CLI，因此将设备注册至防御中心更容易。

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字母数字注册密钥。这是一个指定的简单密钥，长度最多为 37 个字符，并且与许可证密钥不同。

在大多数情况下，必须与注册密钥一起提供 防御中心的主机名或 IP 地址，例如：

```
configure manager add DC.example.com my_reg_key
```

但是，如果设备与防御中心由一台 NAT 设备分开，请与注册密钥一起输入唯一的 NAT ID，并指定 DONTRESOLVE 而非主机名，例如：

```
configure manager add DONTRESOLVE my_reg_key my_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. 以具有配置 CLI 访问级别的用户身份登录设备：
   - 如果要从控制台执行初始设置，您已经以管理员用户身份登录，该用户具有需要的访问级别。
   - 否则，请通过 SSH 连接到设备的管理 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} 指定防御中心的完全限定主机名或 IP 地址。如果防御中心不可直接寻址，请使用 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，最多包含 37 个字符。
   - *nat_id* 是在防御中心与设备之间的注册过程中使用的可选字母数字字符串。如果主机名设置为 DONTRESOLVE，此字符串必填。
3. 从设备注销。

   随时可将设备添加到防御中心。

初始设置页面：设备

对于所有受管设备（除您使用 CLI 配置的 3 系列外；请参阅第 81 页的使用 CLI 在 3 系列设备上执行初始设置），您必须通过登录设备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。

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。您还可以将设备预注册至防御中心并指定检测模式；您在注册期间选择的检测模式和其他选项将决定系统创建的默认接口、内联集和区域，以及它最初应用于受管设备的策略。

要使用物理受管设备的网络界面完成其初始配置，请执行以下操作：

访问：管理员

1. 使用浏览器访问 `https://mgmt_ip/`，其中 *mgmt_ip* 是设备管理接口的 IP 地址。
   - 对于通过以太网线缆连接到计算机的设备，请使用该计算机上的浏览器访问默认管理接口 IPv4 地址：`https://192.168.45.45/`。
   - 对于已配置网络设置的设备，请使用管理网络上的计算机浏览到设备管理接口的 IP 地址。

   系统将显示登录页面。

2. 以 `admin` 作为用户名，以 `Sourcefire` 作为密码登录。

   系统将显示设置页面。有关完成设置的信息，请参阅以下各节：
   - 第 85 页的更改密码
   - 第 85 页的网络配置
   - 第 86 页的3 系列设备 LCD 面板配置
   - 第 86 页的远程管理
   - 第 87 页的时间设置
   - 第 87 页的检测模式
   - 第 89 页的自动备份
   - 第 89 页的最终用户许可协议

3. 当完成后，请点击 **Apply**。

   系统将根据您的选择配置设备。在显示中间页面后，您将作为具有管理员角色的管理员用户登录网络界面。

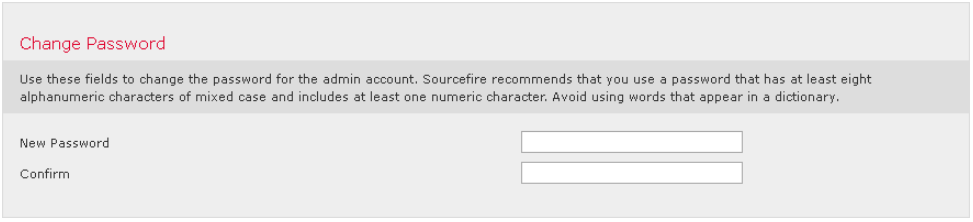
4. 从设备注销。

   随时可将设备添加到其管理防御中心。

> **重要！** 如果您使用以太网电缆直接连接到设备，请断开与计算机的连接，并将设备的管理接口连接到管理网络。任何时候如果需要访问设备的网络界面，请使用管理网络上的一台计算机上的浏览器访问您在设置过程中配置的 IP 地址或主机名。

更改密码

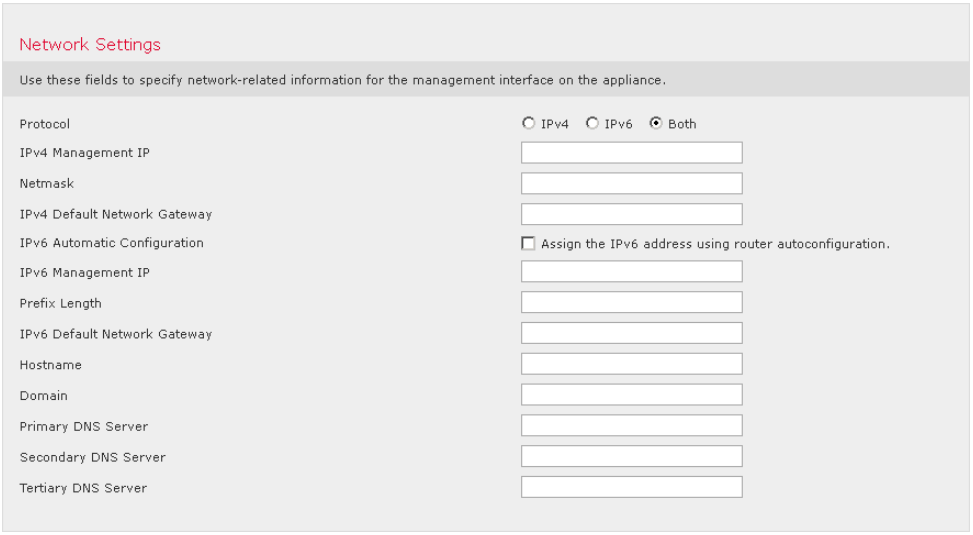
您必须更改管理员帐户的密码。此帐户拥有管理员权限，无法删除。



Sourcefire 建议您使用至少包含八个混合大小写的字母数字字符并至少包含一个数字字符的强密码。请避免使用词典中出现的单词。

网络配置

设备的网络设置使其能够在管理网络上通信。如果已配置设备的网络设置，页面的此部分可能已填充内容。



Sourcefire 3D 系统可以为 IPv4 和 IPv6 管理环境提供双堆栈实施。您必须指定管理协议 （**IPv4**、 **IPv6** 或 **Both**）。根据您的选择、设置页面将显示各种字段，您必须在其中设置 IPv4 或 IPv6 管理 IP 地址、子网掩码或前缀长度以及默认网关。

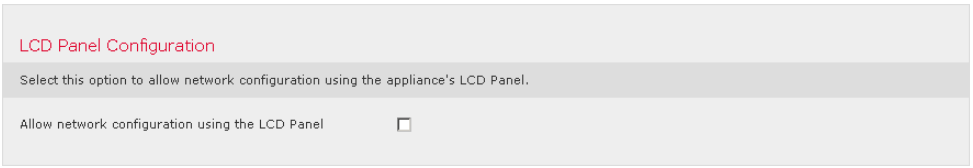
- 对于 IPv4，必须设置点分十进制形式的 IP 地址和子网掩码 （例如，子网掩码为 255.255.0.0）。
- 对于 IPv6 网络，您可以选择 **Assign the IPv6 address using router autoconfiguration** 复选框以自动分配 IPv6 网络设置。否则，您必须设置该地址 （以冒号分隔的十六进制形式）和前缀中的位数 （例如：前缀长度为 112）。

您还可以指定最多三个 DNS 服务器以及设备的主机名和域。

3 系列设备 LCD 面板配置

支持的设备：3 系列

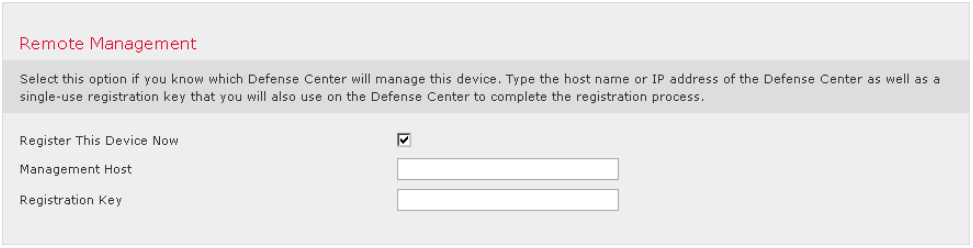
如果您配置 3 系列设备，请选择您是否允许使用 LCD 面板更改设备的网络设置。



警告！启用此选项可能会引入安全风险。要使用 LCD 面板配置网络设置，您只需亲身接近，而无需进行身份验证。有关详细信息，请参阅第 98 页的使用 3 系列设备上的 LCD 面板。

远程管理

您必须使用防御中心管理 Sourcefire 设备。在此两步式过程中，您首先配置设备上的远程管理，然后将设备添加到防御中心。为方便您使用，设置页允许您将设备预注册至管理设备的防御中心。

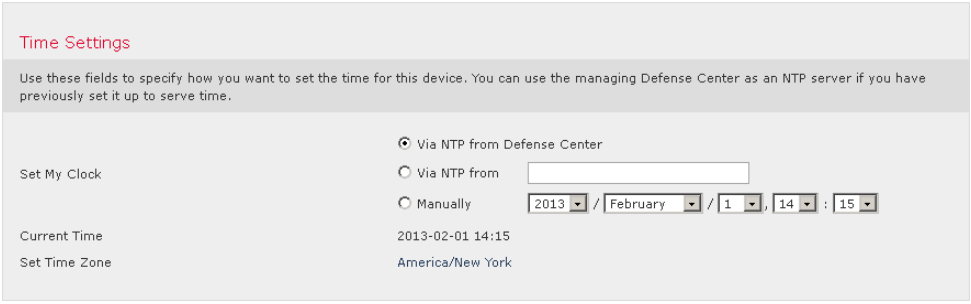


保持启用 **离开** 复选框，然后指定管理防御中心的 IP 地址或完全限定域名作为 **Management Host**。此外，键入您稍后用于将设备注册至防御中心的字母数字**注册密钥**。请注意，这是一个指定的简单密钥，长度最多为 37 个字符，并且不同于许可证密钥。

重要！ 如果设备和防御中心被网络地址转换 (NAT) 设备隔开，请延迟设备注册，直到完成初始设置。有关详细信息，请参阅 《*Sourcefire 3D 系统用户指南*》中的“管理设备”章节。

时间设置

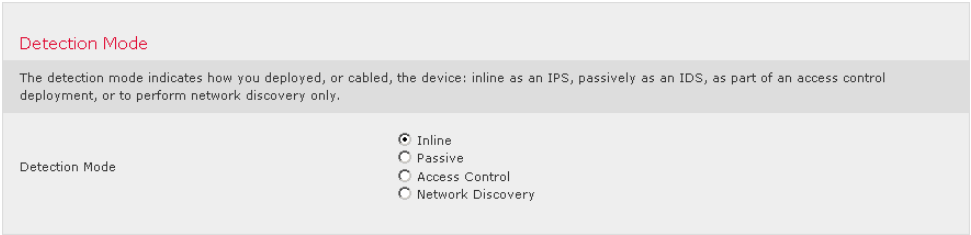
您可以手动设置设备的时间或通过网络时间协议 (NTP) 从 NTP 服务器设置时间，包括防御中心。 Sourcefire 建议您使用防御中心作为其受管设备的 NTP 服务器。



您还可以指定本地网络界面上用于管理员帐户的时区。点击当前时区以在弹出窗口中进行更改。

检测模式

您为设备选择的检测模式将决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安全区域。



检测模式不是以后可更改的设置；它是您在设置过程中选择的选项，用于帮助系统定制设备的初始配置。一般来说，应根据您的设备部署方式选择检测模式：

被动

如果您的设备以被动方式部署为入侵检测系统 (IDS)，请选择此模式。在被动部署中，您可以执行文件和恶意软件检测、安全情报监控以及网络发现。

内联

如果您的设备以内联方式部署为入侵防御系统 (IPS)，请选择此模式。 IPS 通常设置为失败*打开*并*允许*不匹配的流量通过。

在内联部署中，您还可执行基于网络的高级恶意软件防护 (AMP)、文件控制、安全情报过滤和网络发现。

虽然您可以对所有设备选择内联模式，但请记得使用以下接口的内联集不具有旁路功能：

- 8000 系列设备上的非旁路网络模块
- 71xx 系列设备上的 SFP 收发器

重要！ 重镜像会将内联部署中的设备重置为非旁路配置；这会中断网络上的流量，直到您重新配置旁路模式。有关详细信息，请参阅第 177 页的恢复过程中的流量。

访问控制

如果在访问控制部署过程中使用内联模式部署设备，请选择此模式，即，如果您要执行应用、用户和 URL 控制。配置为执行访问控制的设备通常设置为不允许*关闭*并*阻止*不匹配的流量。规则明确指定允许通过的流量。

如果您希望充分利用设备特定的基于硬件功能，也应选择此模式，这些功能包括 （依型号而定）：集群、严格 TCP 实施、快速路径规则、交换、路由、DHCP、 NAT 和 VPN。

在访问控制部署中，您还可以执行恶意软件防护、文件控制、安全情报过滤和网络发现。

网络发现

如果设备以内联方式部署，请选择此模式以仅执行主机、应用和用户发现。

下表列出了系统根据您选择的检测模式创建的接口、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	添加到默认内联集中的第一对接口 - 一个添加到内部区域，另一个添加到外部区域
被动	被动	无	分配到被动区域的第一对
访问控制	无	无	无
网络发现	被动	无	分配到被动区域的第一对

请注意，安全区域是防御中心级配置，直到您实际将设备注册至防御中心，系统才会创建该配置。在注册时，如果适当的区域（内部，外部或被动）已存在于防御中心上，注册过程会将所列接口添加到现有区域。如果区域不存在，系统会创建该区域并添加接口。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*》。

自动备份

设备提供了一种用于存档数据的机制，以便可在发生故障时存储配置和事件数据。初始设置过程中，您可以 **Enable Automatic Backups**。

启用此设置会创建一个计划任务，该任务会创建设备上的配置的每周备份。

最终用户许可协议

请仔细阅读 EULA，并且，如果您同意遵守本协议条款，请选择复选框。请确保您提供的所有信息正确，然后点击 **Apply**。系统将根据您选择的选项配置设备，您可以随时将准备添加到其管理防御中心。

初始设置页面：防御中心

对于所有防御中心，您必须通过登录防御中心的网络界面并在设置页上指定初始配置选项来完成设置过程。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。

设置过程还允许您注册并许可设备。您必须首先在设备上完成设置过程并添加防御中心作为远程管理器，然后才能注册设备，否则注册将失败。

有关详细信息，请参阅第 13 页的按设备型号列出的支持的功能和第 19 页的授予 Sourcefire 3D 系统许可证。

要在防御中心上使用其网络界面完成其初始设置，请执行以下操作：

访问：管理员

1. 使用浏览器访问 `https://mgmt_ip/`，其中，*mgmt_ip* 是防御中心管理接口的 IP 地址：
   - 对于通过以太网线缆连接到计算机的防御中心，请使用该计算机上的浏览器访问默认管理接口 IPv4 地址：`https://192.168.45.45/`。
   - 对于已配置网络设置的防御中心，请使用管理网络上的计算机浏览到防御中心管理接口的 IP 地址。

系统将显示登录页面。

2. 以 admin 作为用户名，以 Sourcefire 作为密码登录。

   系统将显示设置页面。有关完成设置的信息，请参阅以下各节：

   - 第 91 页的更改密码
   - 第 91 页的网络配置
   - 第 92 页的时间设置
   - 第 92 页的重复规则更新导入
   - 第 93 页的重复地理定位更新
   - 第 93 页的自动备份
   - 第 93 页的许可设置
   - 第 95 页的设备注册
   - 第 96 页的最终用户许可协议

3. 当完成后，请点击 **Apply**。

   系统将根据您的选择配置防御中心。在显示中间页面后，您将作为具有管理员角色的管理员用户登录网络界面。

   重要！ 如果您使用以太网电缆直接连接到设备，请断开与计算机的连接，并将防御中心的管理接口连接到管理网络。使用管理网络上的计算机上的浏览器访问您本指南中的其余操作步骤中配置的防御中心的 IP 地址或主机名。

4. 使用 Task Status 页面 (**System > Monitoring > Task Status**) 验证初始设置成功。

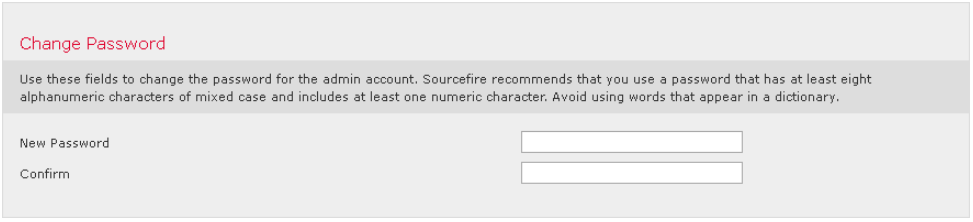
   该页面每十秒自动刷新。请监控该页面，直到其列出的初始设备注册和策略应用任务的状态均为 **Completed**。如果您在安装过程中配置了入侵规则或地理定位更新，您还可以监控这些任务。

   该防御中心已可以使用。请参阅《*Sourcefire 3D 系统用户指南*》以了解有关配置部署的详细信息。

5. 继续执行第 96 页的后续步骤。

更改密码

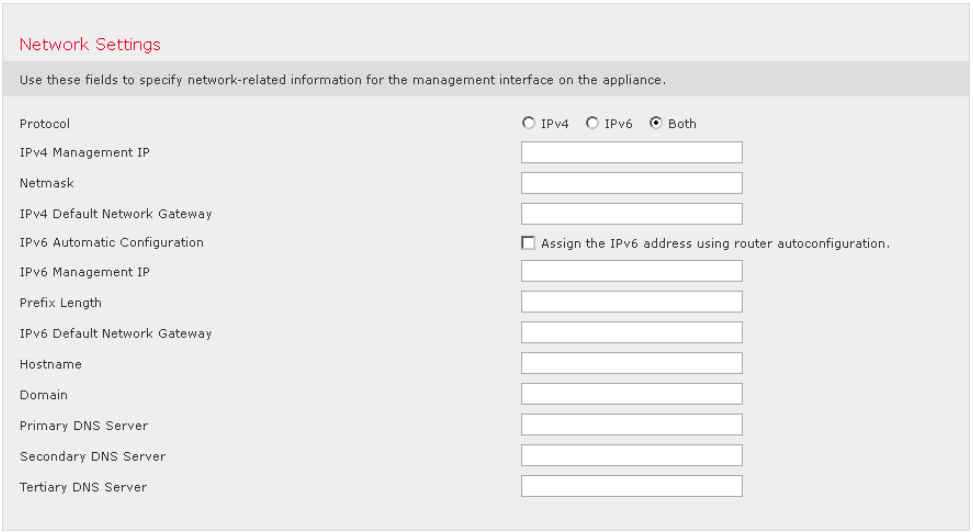
您必须更改管理员帐户的密码。此帐户拥有管理员权限，无法删除。



Sourcefire 建议您使用至少包含八个混合大小写的字母数字字符并至少包含一个数字字符的强密码。请避免使用词典中出现的单词。

网络配置

防御中心的网络设置使其能够在管理网络上通信。如果已配置网络设置，页面的此部分可能已填充内容。



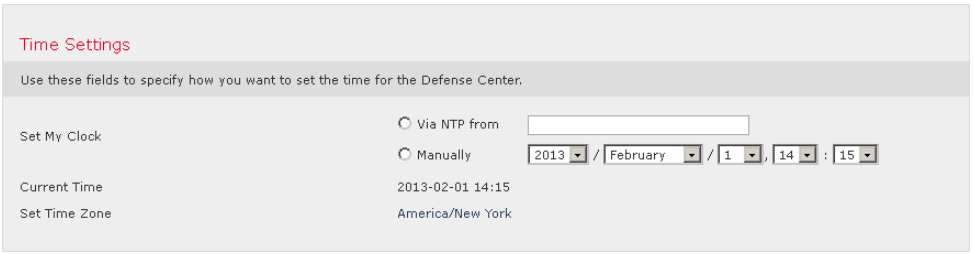
Sourcefire 3D 系统可以为 IPv4 和 IPv6 管理环境提供双堆栈实施。您必须指定管理协议 （**IPv4**、 **IPv6** 或 **Both**）。根据您的选择、设置页面将显示各种字段，您必须在其中设置 IPv4 或 IPv6 管理 IP 地址、子网掩码或前缀长度以及默认网关。

- 对于 IPv4，必须设置点分十进制形式的 IP 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** 复选框以自动分配 IPv6 网络设置。否则，您必须设置该地址（以冒号分隔的十六进制形式）和前缀中的位数 （例如：前缀长度为 112）。

您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

您可以手动设置防御中心的时间或通过网络时间协议 (NTP) 从 NTP 服务器设置时间。



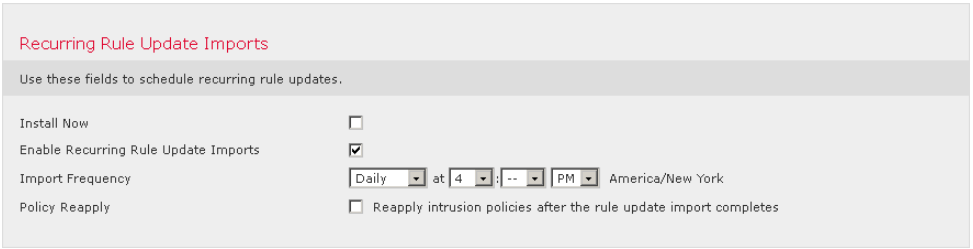
您还可以指定本地网络界面上用于管理员帐户的时区。点击当前时区以在弹出窗口中进行更改。

重复规则更新导入

许可证：保护

随着新的漏洞被发现， Sourcefire 漏洞研究团队 (VRT) 会发布入侵规则更新。规则更新为现有规则提供最新和更新的入侵规则和预处理器规则、修改的现有规则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和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 **Enable Recurring Rule Update Imports**。



您可以指定 **Import Frequency**，以及配置系统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**。

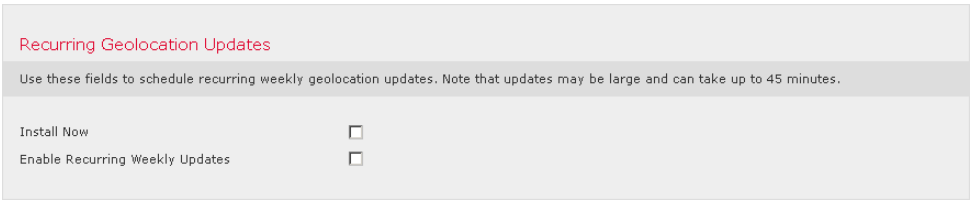
重要！ 规则更新可能包含新的二进制文件。请确保您下载并安装规则更新的过程符合您的安全策略。此外，规则更新可能很大，请确保在网络使用较少的时段导入规则。

重复地理定位更新

支持的防御中心：除 DC500 外的所有型号

您可以使用大多数防御中心查看有关与系统生成的事件相关的已路由 IP 地址的地理信息，以及监控控制面板和 Context Explorer 中的地理定位统计信息。

防御中心的地理定位数据库 (GeoDB) 包含诸如 IP 地址的关联互联网服务提供商 (ISP)、连接类型、代理信息和具体位置等信息。启用定期 GeoDB 更新以确保系统使用最新地理定位信息。如果您计划在部署中执行地理定位相关分析， Sourcefire 建议您 **Enable Recurring Weekly Updates**。



您可以指定 GeoDB 的每周更新频率。点击时区以在弹出窗口中进行更改。要在初始配置过程中下载数据库，请选择 **Install Now**。

重要！ GeoDB 更新可能比较大，在下载后可能需要 45 分钟安装。应在网络使用较少的时段更新 GeoDB。

自动备份

防御中心提供了一种用于存档数据的机制，以便可在发生故障时存储配置。初始设置过程中，您可以 **Enable Automatic Backups**。

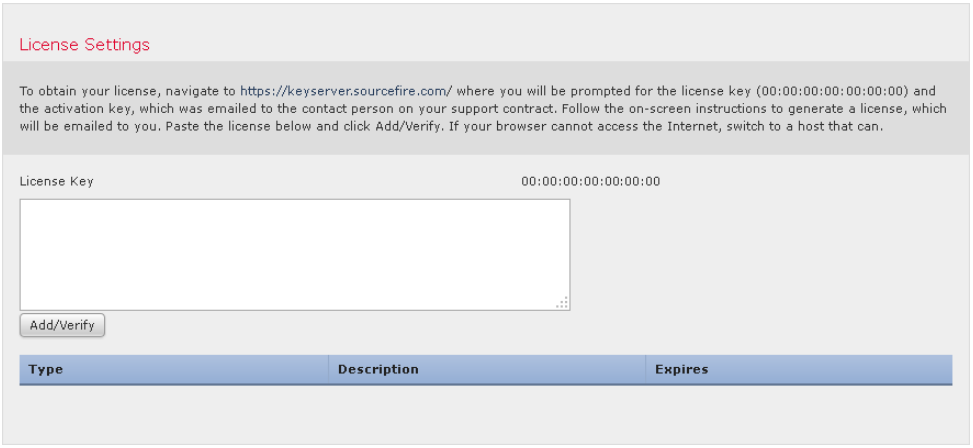
启用此设置会创建一个计划任务，该任务会创建防御中心上的配置的每周备份。

许可设置

您可以许可各种功能，以便为贵公司创建优化的 Sourcefire 3D 系统部署。执行主机、应用和用户发现需要防御中心上的 FireSIGHT 许可证。额外的特定于型号的许可证允许受管设备执行各种功能。由于架构和资源限制，并非所有的许可证均可应用于所有受管设备；请参阅第 13 页的按设备型号列出的支持的功能和第 19 页的授予 Sourcefire 3D 系统许可证。

Sourcefire 建议您使用初始设置页面添贵公司已购买的许可证。如果现在不添加许可证，您在初始设置期间注册的所有设备都将作为未授权设备添加到防御中心；在初始设置过程结束后，您必须逐个许可这些设备。请注意，如果您正在设置一个重新映象的设备，并且在恢复过程中保留了许可设置，此部分可能已填充内容。

如果您尚未获取许可证，请点击链接导航到 `https://keyserver.sourcefire.com/` 并按照屏幕说明操作。您需要您的许可证密钥 （列示在初始设置页面上），以及之前通过邮件发送给您的支持合同关联的联系人的激活密钥。



通过将许可证粘贴到文本框添加许可证，然后点击 **Add/Verify**。在添加一个有效许可证后，页面将更新，以便您可以跟踪您已添加的许可证。请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 DC1500 Licenses				
FireSIGHT Host	FireSIGHT User			
50000	50000			

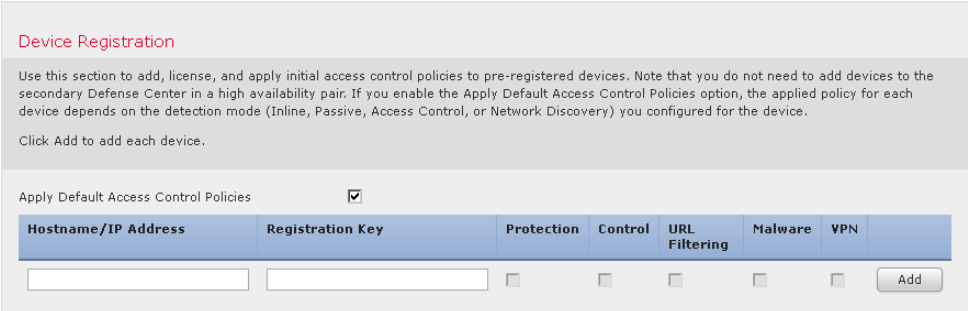
Type	Description	Expires
3D8250	5 Protection License(s)	Never
3D8250	5 Control License(s)	Never
3D8250	5 VPN License(s)	Never
Virtual Device 64bit	5 Malware License(s)	2013-09-16 18:58:01
Virtual Device 64bit	5 Control License(s)	Never
Virtual Device 64bit	5 Protection License(s)	Never
DC1500	50000 FireSIGHT Host, 50000 FireSIGHT User License(s)	Never

设备注册

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。

重要！ 您必须在设备上配置远程管理，然后才能将设备注册至防御中心。

您可以在初始设置过程中将大多数预注册的设备 （请参阅第 86 页的远程管理）添加到防御中心。但是，如果设备和防御中心被一台 NAT 设备隔开，在安装过程完成之后，必须添加该设备。



在注册设备时，如果要在注册后自动对设备应用访问控制策略，请保持启用 **Apply Default Access Control Policies** 复选框。请注意，您无法选择防御中心应用于每个设备的策略，仅可选择是否应用策略。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 （请参阅第 87 页的检测模式），如下表所列。

每个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

如果您以前使用防御中心管理设备并且更改了设备的初始接口配置，就会发生异常。在这种情况下，此新防御中心页面应用的策略取决于设备更改的 （当前）配置。如果配置了接口，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。

要添加设备，请键入其 **Hostname** 或 **IP Address** 地址，以及您在注册该设备时指定的 **Registration Key**。请记得，这是一个指定的简单密钥，长度最多为 37 个字符，并且不同于许可证密钥。

然后，使用复选框向设备将添加许可的功能。您只能选择已经添加至防御中心的许可证；请参阅第 93 页的许可设置。

由于架构和资源限制，并非所有的许可证均可应用于所有受管设备。但是，设置页**不会**禁止您在受管设备上启用不支持的许可证或启用没有特定于型号的许可证的功能。这是因为，防御中心稍后才会确定设备型号。系统无法启用无效的许可证，并且尝试启用无效的许可证不会减少可用的许可证总数。

有关许可的详细信息，包括可以使用哪些防御中心向每种设备型号应用每个许可证，请参阅第 13 页的按设备型号列出的支持的功能和第 19 页的授予 Sourcefire 3D 系统许可证。

重要！ 如果您启用 **Apply Default Access Control Policies**，您必须在选择 **Inline** 或 **Passive** 检测模式的设备上启用保护许可证。您还必须在已配置接口的先前受管设备上启用保护。否则，将无法应用默认策略 （在此情况下该策略将需要保护）。

在启用许可证之后，请点击 **Add** 保存设备的注册设置，或者，添加更多设备。

Hostname/IP Address	Registration Key	Protection	Control	URL Filtering	Malware	VPN	
							Add
bodhi.example.com	buddha	Enabled	Disabled	Disabled	Enabled	Disabled	Delete
yggdrasil.example.com	loki	Enabled	Enabled	Disabled	Disabled	Enabled	Delete

如果选择了错误的选项或键入了错误的设备名称，请点击 **Delete** 将其删除。然后您可以重新添加该设备。

最终用户许可协议

请仔细阅读 EULA，并且，如果您同意遵守本协议条款，请选择复选框。请确保您提供的所有信息正确，然后点击 **Apply**。

系统将根据您的选择配置防御中心。在显示中间页面后，您将作为具有管理员角色的管理员用户登录网络界面。请继续第 89 页的初始设置页面：防御中心中的第 3 步以完成防御中心的初始设置。

后续步骤

在完成设备的初始设置过程并验证其成功后， Sourcefire 建议您完成让您的部署更易于管理的各种管理任务。您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。有关以下各节中介绍的任何任务的详细信息以及有关如何开始配置部署的信息，请参阅 《*Sourcefire 3D 系统用户指南*》。

提示！ 如果要使用串行或 LOM/SOL 连接访问设备的控制台，应该重定向控制台输出；请参阅第 74 页的重定向控制台输出。如果要具体使用 LOM，必须启用该功能并至少启用一个 LOM 用户；请参阅第 195 页的启用 LOM 和 LOM 用户。

单个用户帐户

在完成初始设置之后，系统上的唯一用户是管理员用户，该用户具有管理员角色和访问权。该角色的用户可以访问所有菜单并具有配置访问权，包括通过外壳或 CLI 访问。 Sourcefire 建议您出于安全和审计原因限制使用管理员帐户 （和管理员角色）。

为将使用系统的每个用户创建单独的帐户，不仅使贵公司能够监控每个用户和操作和所做的更改，还能够限制每个人的关联用户访问角色或角色。在防御中心上这一点尤其重要，您将在其上执行大部分配置和分析任务。例如，分析师需要访问事件数据分析网络安全，但是，可能不需要访问部署的管理功能。

系统提供专为各种管理员和分析师设计的十个预定义用户角色。您还可以创建具有特殊访问权限的自定义用户角色。

健康和系统策略

默认情况下，所有设备均已应用初始系统策略。系统策略管理对于部署中的多个设备可能类似的设置，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相同的系统策略应用于其自身及其管理的所有设备。

默认情况下，防御中心也会应用一个健康策略。健康策略作为运行状况监控功能的一部分，为系统持续监控部署中设备的性能提供标准。 Sourcefire 建议您使用防御中心将健康策略应用于其管理的所有设备。

软件和数据库更新

在开始任何部署之前，应更新设备上的系统软件。 Sourcefire 建议在部署的所有设备上运行最新版本的 Sourcefire 3D 系统。如果要在部署中使用设备，还应安装最新的入侵规则更新、 VDB 和 GeoDB。

警告！ 在更新 Sourcefire 3D 系统的任何部分之前，**必须**阅读随更新提供的版本说明或建议文本。版本说明提供重要信息，包括支持的平台、兼容性、前提条件、警告和具体安装和卸载说明。

第 5 章
使用 3 系列设备上的 LCD 面板

3 系列设备可供您使用设备正面的 LCD 面板而不是系统的网络界面查看设备信息或配置某些设置。

LCD 面板有一个显示屏和四个多功能键，且可在多种模式下运行，这些模式显示不同的信息并允许不同配置 （取决于设备的状态）。

有关详细信息，请参阅以下各节：

- 第 99 页的了解 LCD 面板组件说明如何识别 LCD 面板的组件并显示面板的主菜单。
- 第 100 页的使用 LCD 多功能键说明如何使用 LCD 面板上的多功能键。
- 第 101 页的空闲显示模式介绍当设备空闲时， LCD 面板如何显示各种系统信息。
- 第 101 页的网络配置模式说明如何使用 LCD 面板为设备的管理接口配置网络配置：IPv4 或 IPv6 地址、子网掩码或前缀和默认网关。

  警告！ 允许使用 LCD 面板进行重新配置可能带来安全风险。您只需实际访问，而无需进行身份验证，即可使用 LCD 面板进行配置。有关详细信息，请参阅第 98 页的使用 3 系列设备上的 LCD 面板。

- 第 104 页的系统状态模式说明如何查看受监控系统的信息，例如链路状态传播、旁路状态和系统资源，以及更改 LCD 面板的亮度和对比度。

- 第 106 页的信息模式说明如何查看标识系统的信息，例如，设备的机箱序列号、 IP 地址、型号以及软件和固件版本。
- 第 107 页的错误警报模式介绍 LCD 面板如何传达错误或故障情况；例如，旁路、风扇状态或硬件警报。

重要！ 只有启动设备才能使用 LCD 面板。有关如何安全地启动或关闭设备的信息，请参阅《*Sourcefire 3D 系统用户指南*》中的“管理设备”一章。

了解 LCD 面板组件

在 3 系列设备正面的 LCD 面板具有一个显示屏和四个多功能键：

- 显示屏包含两行文本 （每行最多 17 个字符），以及多功能键映射。映射图使用符号表示您可使用相应的多功能键执行的操作。
- 多功能键可供您查看系统信息并完成基本配置任务，该等任务因 LCD 面板的模式而异。有关详细信息，请参阅第 100 页的使用 LCD 多功能键。

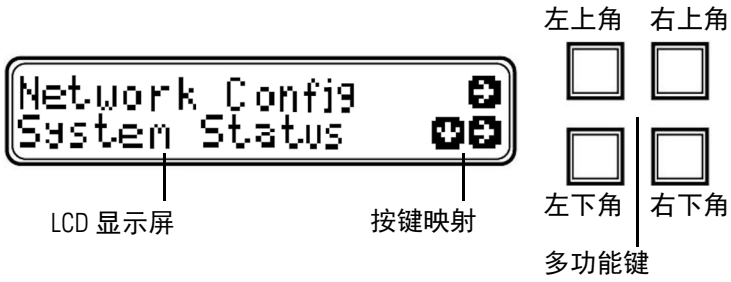
下图显示该面板的默认空闲显示模式，该模式不包括键映射。

LCD 面板，空闲显示模式

在空闲显示模式中，该面板交替显示 CPU 利用率和可用内存以及机箱序列号。您可访问网络配置、系统状态和信息模式，只需中断空闲显示模式以显示 LCD 面板的主菜单。

下图显示主菜单，其中包括对应四个多功能键 （左上角、右上角、左下角和右下角）的键映射。

LCD 面板，主菜单



要访问主菜单，请执行以下操作：

▶ 在空闲显示模式下，按任意多功能键。

系统将显示主菜单：

- 要更改设备的网络配置，请参阅第 101 页的网络配置模式。
- 要查看受监控系统的信息或调整 LCD 面板的亮度和对比度，请参阅第 104 页的系统状态模式。
- 要查看标识系统的信息，请参阅第 106 页的信息模式。

重要！ 在 LCD 面板进入空闲显示模式时按多功能键可能导致面板显示意外的菜单。

使用 LCD 多功能键

四个多功能键可供您在 3 系列设备的 LCD 面板上导航菜单和选项。当显示屏上出现按映射时，您可使用多功能键。符号在映射上显示的位置与用于执行该功能的键的功能和位置相对应。如未显示任何符号，则相应键没有功能。

提示！ 符号的功能以及键映射因 LCD 面板模式而异。如未获得期望的结果，请检查 LCD 面板的模式。

下表说明多功能键功能。

LCD 面板多功能键

符号	说明	功能
↑	向上箭头	向上滚动当前菜单选项列表。
↓	向下箭头	向下滚动当前菜单选项列表。
←	向左箭头	执行以下一种操作： • 不采取任何操作并显示 LCD 面板菜单。 • 将光标向左侧移动。 • 重新启用编辑。
→	向右箭头	执行以下一种操作： • 进入该行上显示的的菜单选项。 • 将光标向右侧移动。 • 滚动浏览后续文本。

LCD 面板多功能键 （续）

符号	说明	功能
X	取消	取消操作。
+	加	对选定数字位加一。
-	减	对选定数字位减一。
✓	复选标记	接受操作。

空闲显示模式

在系统未检测到错误的情况下， LCD 面板在 60 秒钟无活动 （您未按任何多功能键）后进入空闲显示模式。如果系统检测到错误，面板进入错误警报模式 （请参阅第 107 页的错误警报模式），直至错误解决。当您编辑网络配置或运行诊断时，空闲显示模式也将禁用。

在空闲显示模式下，该面板交替显示 （以五秒钟间隔 CPU 利用率和可用内存以及机箱序列号。

每种显示模式的示例可能如下所示：

```
CPU: 50%
FREE MEM: 1024 MB
```

或：

```
Serial Number:
3D99-101089108-BA0Z
```

在空闲显示模式下，按任何多功能键进入主菜单；请参阅第 99 页的了解 LCD 面板组件。

重要！ 在 LCD 面板进入空闲显示模式时按多功能键可能导致面板显示意外的菜单。

网络配置模式

Sourcefire 3D 系统可以为 IPv4 和 IPv6 管理环境提供双堆栈实施。在网络配置模式下，您可使用 LCD 面板为 3 系列设备的管理接口配置网络配置：IP 地址、子网掩码或前缀和默认网关。

默认情况下，已禁用使用 LCD 面板更改网络设置的功能。您可在初始设置过程中或使用设备的网络界面启用该功能。有关详细信息，请参阅第 103 页的允许使用 LCD 面板重新进行网络配置。

警告！ 启用此选项可能会引起安全风险。您只需实际访问，而无需进行身份验证，即可使用 LCD 面板进行配置。

要使用网络配置模式进行配置，请执行以下操作：

1. 在空闲显示模式下，按任何多功能键进入主菜单。

   系统将显示主菜单：

   ```
   Network Config          →
   System Status        ↓ →
   ```

2. 按顶行的向右箭头 (à) 键，以访问网络配置模式。

   LCD 面板将显示以下内容：

   ```
   IPv4                 ↓ →
   IPv6                   →
   ```

3. 按向右箭头键，以选择要配置的 IP 地址：

   - 对于 IPv4，LCD 面板可能显示以下内容：

     ```
     IPv4 set to DHCP.    ←
     Enable Manual?       →
     ```

   - 对于 IPv6，LCD 面板可能显示以下内容：

     ```
     IPv6 Disabled.       ←
     Enable Manual?       →
     ```

4. 按向右箭头键以手动配置网络：

   - 对于 IPv4，LCD 面板将显示 IPv4 地址。例如：

     ```
     IPv4 Address:      - +
     194.170.001.001    X →
     ```

   - 对于 IPv6，LCD 面板将显示空白 IPv6 地址。例如：

     ```
     IPv6 Address:      - +
     0000:0000:0000:00  X →
     ```

   面板的第一行表示您正在编辑的是 IPv4 还是 IPv6 地址。第二行显示您正在编辑的 IP 地址。光标在第一位数字下以下划线形式显示，代表您正在编辑的数位。与多功能键对应的两个符号显示在每行的右侧。

   请注意，IPv6 地址在显示屏上无法完全显示。当您编辑每一数位并将光标向右移动时，IPv6 地址向右滚动。

5. 根据需要编辑下划线光标所在的位，然后移动到 IP 地址中的下一位：
   - 要编辑数位，请按顶行上的减号 (-) 或加号 (+) 以对该数位加一或减一。
   - 要移至 IP 地址中的下一位，请按底行上的向右箭头键，以将光标移至右侧的下一位。

   当光标在第一位上时， LCD 面板在 IP 地址末尾处显示取消和向右箭头符号。当光标在任何其他位上时， LCD 面板显示向左箭头和向右箭头符号。

6. 当您完成编辑 IPv4 或 IPv6 地址时，再次按向右箭头键，可显示复选标记 (✓) 键以接受更改。

   在您按向右箭头键之前，显示屏上的功能符号可能如以下示例所示：

   ```
   IPv4 Address:      - +
   194.170.001.001    X →
   ```

   在您按向右箭头键之后，显示屏上的功能符号可能如以下示例所示：

   ```
   IPv4 Address:      X ✓
   194.170.001.001    ←
   ```

7. 按复选标记键，以接受对 IP 地址的更改。

   对于 IPv4， LCD 面板将显示以下内容：

   ```
   Subnet Mask:       - +
   000.000.000.000    X →
   ```

   对于 IPv6， LCD 面板将显示以下内容：

   ```
   Prefix:            - +
   000.000.000.000    X →
   ```

8. 按照编辑 IP 地址的方式编辑子网掩码或前缀，然后按复选标记键以接受更改。

   LCD 面板将显示以下内容：

   ```
   Default Gateway    - +
   000.000.000.000    X →
   ```

9. 按照编辑 IP 地址的方式编辑默认网关，然后按复选标记键以接受更改。

   LCD 面板将显示以下内容：

   ```
   Save?              ✓
                      X
   ```

10. 按复选标记键以保存更改。

允许使用 LCD 面板重新进行网络配置

因为这将带来安全风险，默认情况下，已禁用使用 LCD 面板更改网络设置的功能。您可在初始设置过程 （请参阅第 80 页的设置 3 系列设备）中或使用设备的网络界面启用该功能，如以下操作步骤中所述。

要允许使用设备的 LCD 面板重新进行网络配置，请执行以下操作：

访问： 管理员

1. 在完成设备的初始设置后，使用具有管理员权限的帐户登录设备的网络界面。
2. 选择 **System > Local > Configuration**。

   系统将显示 Information 页面。
3. 点击 **Network**。

   系统将显示 Network Settings 页面。
4. 在 **LCD Panel** 下，请选择 **Allow reconfiguration of network settings** 复选框。当系统显示安全警告时，请确认您要启用此选项。

   提示！ 有关此页面上其他选项的信息，请参阅 《*Sourcefire 3D 系统用户指南*》。
5. 点击 **Save**。

   Network Settings 页面已更改成功。

系统状态模式

LCD 面板的系统状态模式显示受监控系统信息，例如，链路状态传播、旁路状态和系统资源。在系统状态模式下，您还可更改 LCD 面板的亮度和对比度。

下表介绍此模式下可用的信息和选项。

系统状态模式选项

选项	说明
Resources	显示 CPU 利用率和可用内存。请注意，空闲显示模式也显示此信息。

Link State	显示当前正在使用的任何内联集的列表以及该内联集的链路状态。第一行标识内联集，第二行显示其状态 （正常或已脱扣）。例如：
	`eth2-eth3:`
	`normal`

Fail Open	显示正在使用的旁路内联集的列表和这些接口对的状态，正常或旁路。
Fan Status	显示设备中风扇的列表和状态。

系统状态模式选项 （续）

选项	说明
Diagnostics	按从 Sourcefire 支持人员获取的特定键序列后可访问。 **警告！** 请**勿**在没有 Sourcefire 支持人员协助的情况下访问诊断菜单。在没有 Sourcefire 支持人员具体说明的情况下访问诊断菜单可能损坏您的系统。
LCD Brightness	可供您调整 LCD 显示屏的亮度。
LCD Contrast	可供您调整 LCD 显示屏的对比度。

要进入系统状态模式并查看受监视系统的信息，请执行以下操作：

1. 在空闲显示模式下，按任何多功能键进入主菜单。

   系统将显示主菜单：

   ```
   Network Config          →
   System Status        ↓ →
   ```

2. 按底行的向右箭头 (→) 键访问系统状态模式。

   LCD 面板将显示以下内容：

   ```
   Resources            ↓ →
   Link State           ↓ →
   ```

3. 按向下箭头 (↓) 键滚动浏览选项。在您要查看的状态旁边的那一行中按向右箭头键。

   根据所选选项， LCD 面板将显示第 104 页的系统状态模式选项表中列出的信息。要更改 LCD 面板的亮度和对比度，请参阅下一操作步骤。

要调整 LCD 面板的亮度和对比度，请执行以下操作：

1. 在系统状态模式下，按向下箭头 (↓) 键滚动浏览选项，直至 LCD 面板显示 LCD 亮度和 LCD 对比度选项：

   ```
   LCD Brightness       ↓ →
   LCD Contrast         ↓ →
   ```

2. 在您要调整的 LCD 显示屏特性 （亮度或对比度）旁边的那一行中按向右箭头键。

   LCD 面板将显示以下内容：

   ```
   Increase               →
   Decrease             ↓ →
   ```

3. 按向右箭头键以增大或减小您已选择的显示特性。

   当您按键时， LCD 显示屏将更改。

4. 按向下箭头以显示 Exit 选项：

```
Decrease          ↓ →
Exit                →
```

5. 在 Exit 行中按向右箭头键以保存设置并返回主菜单。

信息模式

LCD 面板的信息模式显示标识系统信息，例如，设备的机箱序列号、 IP 地址、型号以及软件和固件版本。您向 Sourcefire 支持人员求助时可能需要提供该信息。

下表介绍此模式下可用的信息。

信息模式选项

选项	说明
IP address	显示设备管理接口的 IP 地址。
Model	显示设备的型号。
Serial number	显示设备的机箱序列号。
Versions	显示设备的系统软件和固件版本。请使用多功能键滚动以下信息： • 产品版本 • NFE 版本 • 微引擎版本 • Flash 版本 • GerChr 版本

要进入信息模式并查看标识系统信息，请执行以下操作：

1. 在空闲显示模式下，按任何多功能键进入主菜单。

   系统将显示主菜单：

```
Network Config      →
System Status     ↓ →
```

2. 按向下箭头 (↓) 键滚动浏览模式，直至 LCD 面板显示信息模式：

```
System Status     ↓ →
Information       ↓ →
```

3. 按底行的向右箭头 (→) 键以访问信息模式。

4. 按向下箭头 (↓) 键滚动浏览选项。在您要查看的信息旁边的那一行中按向右箭头键。

   根据所选选项， LCD 面板将显示第 106 页的信息模式选项表中列出的信息。

错误警报模式

当发生错误或故障情况时，错误警报模式将中断空闲显示模式。在错误警报模式下， LCD 显示屏闪烁并显示下表中列出的一个或多个错误。

LCD 面板错误警报

错误	说明
硬件告警	有关硬件错误的警报
链路状态传播	显示成对接口的链路状态
旁路	显示在旁路模式中配置的内联集的状态
风扇状态	当风扇达到临界条件时发出警报

要查看多种错误警报，请执行以下操作：

▶ 使用多功能键滚动浏览错误警报列表：

有关详细信息，请参阅第 100 页的LCD 面板多功能键表。

要退出错误警报模式，请执行以下操作：

▶ 按照 LCD 显示屏上的指示按相应的多功能键。

如果您在解决触发警报的错误前退出错误警报模式，LCD 面板将返回错误警报模式。

第 6 章
硬件规格

Sourcefire 3D 系统可在各种设备上提供，以满足公司的需求。有关在机架中安装设备的详细信息，请参阅第 108 页的机架和机柜安装选项。

以下各节介绍每种设备的硬件规格：

- 第 108 页的Sourcefire 防御中心
- 第 126 页的Sourcefire 7000 系列设备
- 第 151 页的Sourcefire 8000 系列设备

机架和机柜安装选项

可以将 Sourcefire 设备安装在机架和服务器机柜中。设备附带机架安装套件（3D7010、 3D7020 和 3D7030 除外）。有关在机架中安装设备的详细信息，请参阅随机架安装套件提供的说明。

3D7010、 3D7020 和 3D7030 需要单独提供的托架和机架安装套件。您可以单独购买其他设备的机架和机柜安装套件。

Sourcefire 防御中心

有关防御中心的详细信息，请参阅以下各节：

- 第 109 页的Sourcefire DC750
- 第 115 页的Sourcefire DC1500
- 第 120 页的Sourcefire DC3500

Sourcefire DC750

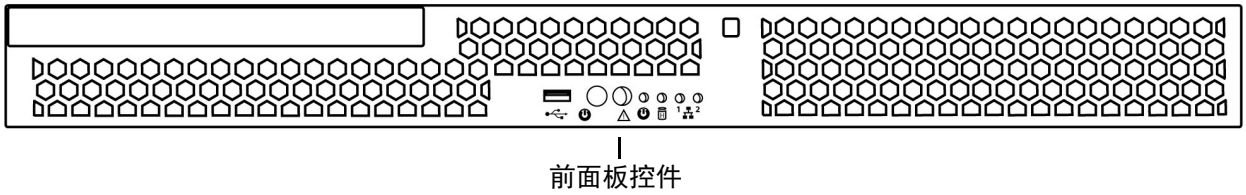
DC750 是在两个不同机箱 （第 1 版和第 2 版）上提供的 1U 设备。两种设备的规格不同，但功能相同。有关设备的详细信息，请参阅以下各节：

- 第 109 页的DC750 机箱前视图
- 第 112 页的DC750 机箱后视图
- 第 113 页的DC750 物理和环境参数

DC750 机箱前视图

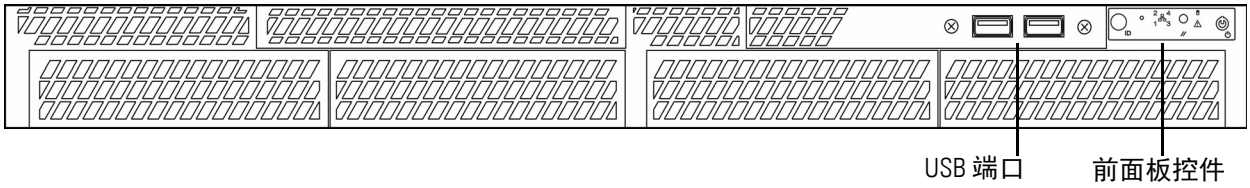
DC750 （第 1 版）机箱前面包含前面板控件。

DC750 （第 1 版）



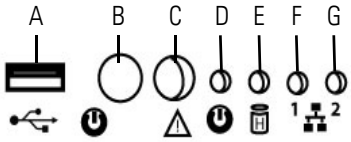
DC750 （第 2 版）机箱前面包含前面板控件。

DC750 （第 2 版）



下图显示 DC750 （第 1 版）的前面板控件和 LED。

DC750 （第 1 版）

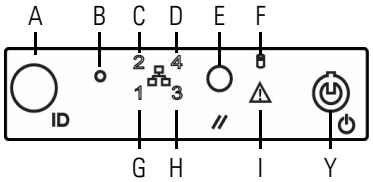


前面板组件 （第 1 版）

A	USB 端口	E	固定硬盘驱动器状态 LED
B	电源按钮	F	NIC 1 活动状态 LED
C	系统状态 LED	G	NIC 2 活动状态 LED
D	电源 LED		

下图显示 DC750 （第 2 版）的前面板控件和 LED。硬盘驱动器和系统状态图标、NIC （1、 2、 3 和 4）活动状态编号和电源按钮也是 LED。

DC750 （第 2 版）



前面板组件 （第 2 版）

A	带 ID LED 的 ID 按钮	F	硬盘驱动器状态 LED
B	不可屏蔽的中断按钮	G	NIC 1 活动状态 LED
C	NIC 2 活动状态 LED	H	NIC 3 活动状态 LED
D	NIC 4 活动状态 LED	I	系统状态 LED
E	复位按钮	Y	带电源 LED 的电源按钮

机箱前面板配有可以查看的五个显示系统运行状态的 LED。 DC750 前面板 LED表介绍前面板上的 LED。

DC750 前面板 LED

LED	说明
系统状态	指示系统状态： • 绿灯亮指示系统正常运行。 • 绿灯闪烁指示系统在某种降级状况下运行。 仅 DC750 （第 1 版）： • 琥珀色灯亮指示系统处于严重的或不可恢复的状况。 • 琥珀色灯闪烁指示系统处于不严重的状况。 **重要！** 琥珀色状态指示灯优先于绿色状态指示灯。当琥珀色指示灯亮起或闪烁时，绿灯熄灭。 有关详细信息，请参阅第 111 页的 DC750 系统状态表。

DC750 前面板 LED （续）

LED	说明
电源	指示系统是处于通电还是休眠状态： • 绿灯亮指示系统正常运行。 • 灯不亮表示系统关闭。 • 绿灯闪烁指示系统处于休眠状态。 休眠指示由芯片集在待机时维护。如果系统未通过 BIOS 断电，系统加电时将恢复断电时的状态，直到 BIOS 将其清除。如果系统未正常断电，可能出现电源指示灯闪烁，同时系统状态指示灯熄灭，原因在于故障或配置更改阻止 BIOS 运行。
硬盘驱动器活动	指示硬盘驱动器活动： • 绿灯闪烁指示固定硬盘驱动器处于活动状态。 • 灯不亮指示没有驱动器活动，或者系统已关闭电源或正在休眠。 仅 DC750 （第 1 版）：琥珀色指示灯亮指示一个固定硬盘驱动器故障。 驱动器活动由板载硬盘控制器确定。服务器板还提供一个插针，供插件控制器访问此指示灯。
NIC 活动	指示系统与网络之间的活动。 • 绿灯闪烁指示有活动。 • 灯不亮表示没有活动。

DC750 系统状态表介绍系统状态 LED 可能点亮的情况。

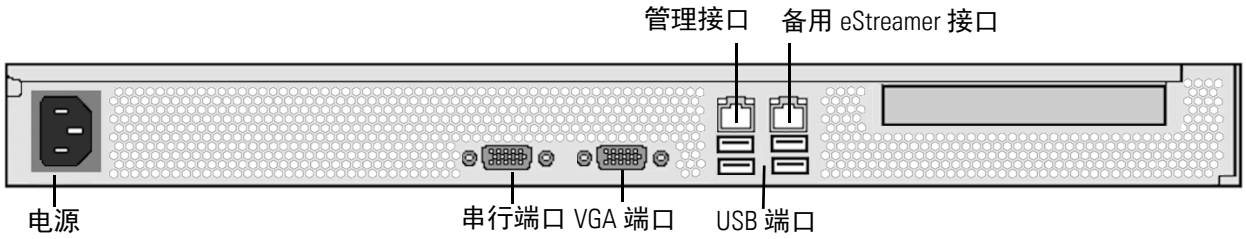
DC750 系统状态

情况	说明
严重	与以下事件关联的任何严重或不可恢复的阈值超出： • 温度、电压或风扇严重阈值超出 • 电源子系统故障 • 由于未正确安装处理器或处理器不兼容导致系统无法启动 • 严重事件记录错误，包括系统内存不可校正的 ECC 错误和严重 / 不可校正的总线错误，例如 PCI SERR 和 PERR
不严重	不严重情况是与以下事件关联的阈值超出： • 温度、电压或风扇非严重阈值超出 • 机箱入侵 • 通过系统 BIOS 设置故障指示命令； BIOS 可以使用命令来指示其他非严重的状态，例如，系统内存或 CPU 配置更改
降级	与以下事件相关的一种降级情况： • 一个或多个处理器由故障弹性启动 (FRB) 或 BIOS 禁用 • BIOS 已禁用或映射掉一些系统内存

DC750 机箱后视图

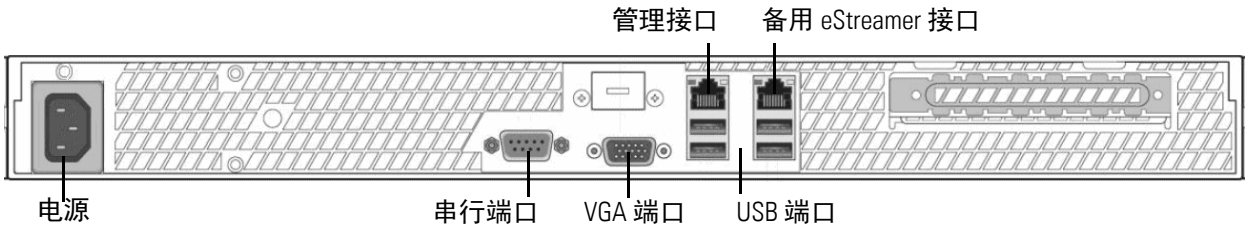
机箱背面包含 DC750 （第 1 版）的电源和连接端口。

DC750 （第 1 版）



机箱背面包含 DC750 （第 2 版）的电源和连接端口。

DC750 （第 2 版）



DC750 系统组件：后视图表介绍显示在设备背面的功能。

DC750 系统组件：后视图

功能	说明
电源	通过交流电源为防御中心供电
串行端口、 VGA 端口 USB 端口	允许您将显示器、键盘和鼠标连接到设备
10/100/1000 Mbps 以太网管理接口	提供带外管理网络连接。管理接口**仅**用于维护和配置用途，并非意在传输业务流量。
备用 eStreamer 接口：	为 eStreamer 客户端提供备用接口

10/100/1000 Mbps 管理接口位于设备的背面。DC750 管理接口 LED表介绍与管理接口相关的 LED。

DC750 管理接口 LED

LED	说明
左侧 （链路）	指示链路是否可用： • 如果指示灯亮，表示链路可用。 • 灯不亮表示没有链路。
右侧 （活动）	指示端口上的活动： • 指示灯闪烁指示活动。 • 灯不亮表示没有链路。

DC750 物理和环境参数

DC750 （第 1 版）物理和环境参数表介绍设备的物理属性和环境参数。

DC750 （第 1 版）物理和环境参数

参数	说明
外形	1U
尺寸 （深 x 宽 x 高）	20.0 英寸 x 16.93 英寸 x 1.67 英寸 （50.8 厘米 x 43.0 厘米 x 4.24 厘米）
最大重量	33 磅 （15 千克）
电源	120 VAC 的 350 W 电源 110 V、 50/60 Hz 时电流最大值为 9.5 A 220 V、 50/60 Hz 时电流最大值为 4.75 A
工作温度	50°F 到 95°F （10°C 到 35°C），最大温度变化率不超过每小时 18°F (10°C)
非工作温度	-40°F 到 +158°F （-40°C 到 +70°C）
非工作湿度	90%，非冷凝 - 温度为 95°F (35°C) 时
噪声	在典型办公室环境温度下处于空闲状态时 <7.0 dBA （机架安装）
工作冲击	2G 半正弦波冲击无错误 （持续 11 毫秒）
包装冲击	从 24 英寸 （60 厘米）处自由下落，尽管可能存在表面损坏，但仍可运行；机箱重量 40 到 80 磅 （18 到 36 千克）

DC750 （第 1 版）物理和环境参数 （续）

参数	说明
静电释放	+/- 12 kV （空气放电）和 8 K （接触放电）
空气流动	正面到背面
系统冷却需求	1660 BTU/ 小时

DC750 （第 2 版）物理和环境参数表介绍设备的物理属性和环境参数。

DC750 （第 2 版）物理和环境参数

参数	DC750 （第 2 版）
外形	1U
尺寸 （深 x 宽 x 高）	21.8 英寸 x 17.25 英寸 x 1.67 英寸 （55.37 厘米 x 43.82 厘米 x 4.24 厘米）
最大重量	33 磅 （15 千克）
电源	120 VAC 的 250 W 电源 110 V、 50/60 Hz 时电流最大值为 6.0 A 220 V、 50/60 Hz 时电流最大值为 3.0 A
工作温度	50°F 到 95°F （10°C 到 35°C），最大温度变化率不超过每小时 18°F (10°C)
非工作温度	-40°F 到 +158°F （-40°C 到 +70°C）
非工作湿度	90%，非冷凝 - 温度为 95°F (35°C) 时
噪声	在典型办公室环境温度下处于空闲状态时为 7.0 dBA (23 +/- 2°C, 73 +/- 4°F
工作冲击	2G 半正弦波冲击无错误 （持续 11 毫秒）
包装冲击	从 24 英寸 （60 厘米）处自由下落，尽管可能存在表面损坏，但仍可运行；机箱重量 40 到 80 磅 （18 到 36 千克）
静电释放	+/- 12 kV （空气放电）和 8 K （接触放电）
空气流动	正面到背面
系统冷却需求	1660 BTU/ 小时

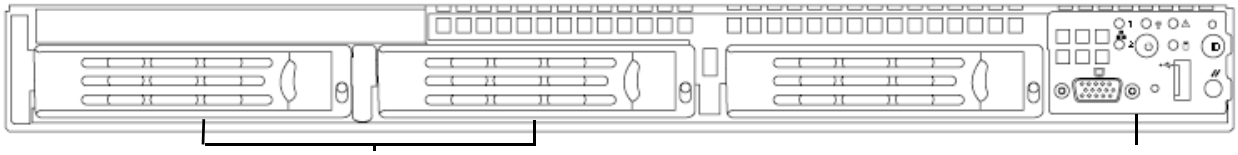
Sourcefire DC1500

DC1500 为 1U 设备。有关设备的详细信息，请参阅以下各节：

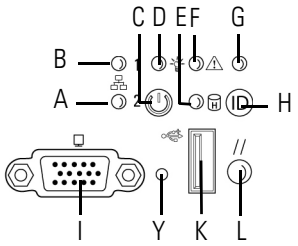
- 第 115 页的DC1500 机箱前视图
- 第 117 页的DC1500 机箱后视图
- 第 119 页的DC1500 物理和环境参数

DC1500 机箱前视图

机箱前面包含硬盘驱动器和前面板控件。



下图显示前面板控件和 LED。



前面板组件

A	NIC 2 活动 LED	G	ID LED
B	NIC 1 活动 LED	H	ID 按钮
C	电源按钮	I	视频连接器 （不可用）
D	电源 / 休眠 LED	Y	不可屏蔽的中断按钮
E	固定硬盘驱动器状态	K	USB 2.0 连接器
F	系统状态 LED	L	复位按钮

机箱的前面板配有可以查看的六个 LED，在有无前面板的情况下都会显示系统的运行状态。 DC1500 前面板 LED表介绍前面板上的 LED。

DC1500 前面板 LED

LED	说明
NIC 1 活动 NIC 2 活动	指示系统与网络之间的活动。 • 绿灯闪烁指示活动。 • 灯不亮表示没有活动。
电源 / 休眠	指示系统是处于通电还是休眠状态： • 绿灯亮指示系统正常运行。 • 绿灯闪烁指示系统处于休眠状态。 • 灯不亮表示系统未通电。 休眠指示由芯片集在待机时维护。如果系统未通过 BIOS 断电，系统加电时将恢复断电时的状态，直到 BIOS 将其清除。如果系统未正常断电，可能出现电源指示灯闪烁，同时系统状态指示灯熄灭，原因在于故障或配置更改阻止 BIOS 运行。
硬盘驱动器活动	指示硬盘驱动器活动： • 绿灯闪烁指示固定硬盘驱动器处于活动状态。 • 琥珀色指示灯亮指示固定硬盘驱动器故障。 • 灯不亮指示没有驱动器活动，或者系统已关闭电源或正在休眠。 驱动器活动由板载硬盘控制器确定。服务器板还提供一个插针，供插件控制器访问此指示灯。
系统状态	指示系统状态： • 绿灯亮指示系统正常运行。 • 绿灯闪烁指示系统在某种降级状况下运行。 • 琥珀色灯亮指示系统处于严重的或不可恢复的状况。 • 琥珀色灯闪烁指示系统处于不严重的状况。 • 灯不亮指示开机自检测试 (POST) 进行中或系统已停止。 **重要！** 琥珀色状态指示灯优先于绿色状态指示灯。当琥珀色指示灯亮起或闪烁时，绿灯熄灭。 有关详细信息，请参阅第 111 页的 DC750 系统状态表。
系统 ID	帮助识别安装在有其他类似系统的高密度机架中的系统 • 蓝色指示灯指示按下了 ID 按钮，并且设备背面的蓝灯亮。 • 灯不亮指示未按下 ID 按钮。

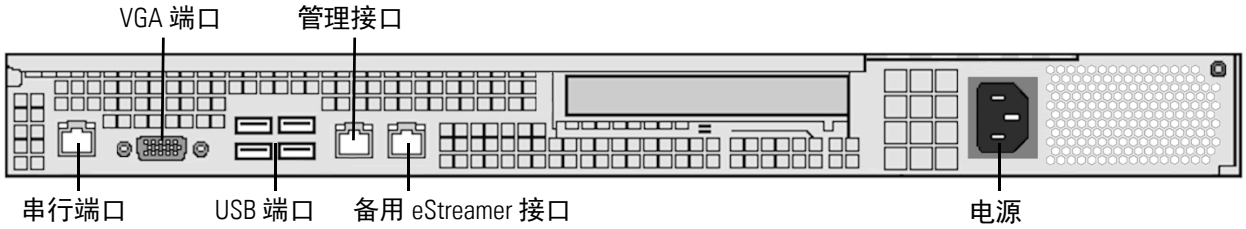
DC1500 系统状态表介绍系统状态 LED 可能点亮的情况。

DC1500 系统状态

情况	说明
严重	与以下事件关联的任何严重或不可恢复的阈值超出： • 温度、电压或风扇严重阈值超出 • 电源子系统故障 • 由于未正确安装处理器或处理器不兼容导致系统无法启动 • 严重事件记录错误，包括系统内存不可校正的 ECC 错误和严重 / 不可校正的总线错误，例如 PCI SERR 和 PERR
不严重	不严重情况是与以下事件关联的阈值超出： • 温度、电压或风扇非严重阈值超出 • 机箱入侵 • 通过系统 BIOS 设置故障指示命令； BIOS 可以使用命令来指示其他非严重的状态，例如，系统内存或 CPU 配置更改
降级	与以下事件相关的一种降级情况： • 一个或多个处理器由故障弹性启动 (FRB) 或 BIOS 禁用 • BIOS 已禁用或映射掉一些系统内存

DC1500 机箱后视图

机箱后部包含连接端口和电源。



DC1500 系统组件：后视图表介绍显示在设备背面的功能。

DC1500 系统组件：后视图

功能	说明
电源	通过交流电源为防御中心供电。
VGA 端口 USB 端口	允许您将显示器、键盘和鼠标连接到防御中心。
10/100/1000 Mbps 以太网管理接口	提供带外管理网络连接。管理接口**仅**用于维护和配置用途，并非意在传输业务流量。
备用 eStreamer 接口：	为 eStreamer 客户端提供备用接口
RJ45 串行端口	允许您建立工作站到设备的直接连接 （使用 RJ45 到 DB-9 适配器），以直接访问设备上的所有管理服务。 RJ45 串行端口**仅**用于维护和配置用途，并非意在传输业务流量。请参阅第 119 页的 DC1500 串行端口引脚分配表。 **重要！** 您不能同时使用前面板和后面板的串行端口。

10/100/1000 Mbps 管理接口位于设备的背面。 DC1500 管理接口 LED表介绍与管理接口相关的 LED。

DC1500 管理接口 LED

LED	说明
左侧 （链路）	指示链路是否可用： • 如果指示灯亮，表示链路可用。 • 灯不亮表示没有链路。
右侧 （活动）	指示端口上的活动： • 指示灯闪烁指示活动。 • 灯不亮表示没有活动。

DC1500 串行端口引脚分配表介绍 DB-9 连接器上提供的信号。

DC1500 串行端口引脚分配

引脚	信号	说明
1	DCD	载波检测
2	RD	接收的数据
3	TD	发送的数据
4	DTR	数据终端就绪
5	GND	接地
6	DSR	数据设置完成
7	RTS	请求发送
8	CTS	清除发送
9	RI	振铃指示器

DC1500 物理和环境参数

DC1500 物理和环境参数表介绍设备的物理属性和环境参数。

DC1500 物理和环境参数

参数	说明
外形	1U
尺寸 （深 x 宽 x 高）	27.2 英寸 x 16.93 英寸 x 1.7 英寸 （69.1 厘米 x 43.0 厘米 x 4.3 厘米）
最大重量	34 磅 （15.4 千克）
电源	120 VAC 的 600 W 电源 110 V、 50/60 Hz 时电流最大值为 9.5 A 220 V、 50/60 Hz 时电流最大值为 4.75 A
工作温度	50°F 至 95°F （10°C 至 35°C）
非工作温度	-40°F 到 +158°F （-40°C 到 +70°C）

DC1500 物理和环境参数 （续）

参数	说明
非工作湿度	90%，非冷凝 - 温度为 82.4°F (28°C) 时
噪声	在典型办公室环境温度下处于空闲状态时 <7.0 dBA （机架安装）
工作冲击	2G 半正弦波冲击无错误 （持续 11 毫秒）
包装冲击	从 24 英寸 （60 厘米）处自由下落，尽管可能存在表面损坏，但仍可运行；机箱重量 40 到 80 磅 （18 到 36 千克）
静电释放	+/- 15 kV （I/O 端口 +/-8 KV）根据英特尔环境测试规格
空气流动	正面到背面
系统冷却需求	2550 BTU/ 小时

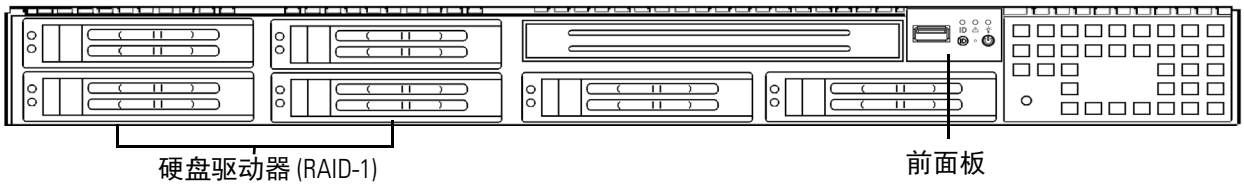
Sourcefire DC3500

DC3500 为 1U 设备。有关设备的详细信息，请参阅以下各节：

- 第 120 页的DC3500 机箱前视图
- 第 122 页的DC3500 机箱后视图
- 第 125 页的DC3500 物理和环境参数

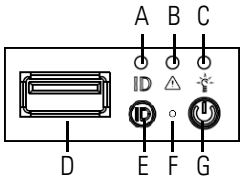
DC3500 机箱前视图

机箱前面包含硬盘驱动器和前面板。



设备前面包含前面板上的控件和 LED 显示屏。

下图显示前面板控件和 LED。



前面板组件

A	ID LED	E	ID 按钮
B	系统状态 LED	F	复位按钮
C	电源 LED	G	电源按钮
D	USB 端口		

机箱的前面板配有三个显示系统运行状态的 LED。 DC3500 前面板 LED表介绍前面板上的 LED。

DC3500 前面板 LED

LED	说明
电源	指示系统是否已通电： • 绿灯指示系统已通电。 • 灯不亮表示系统未通电。
系统状态	指示系统状态： • 绿灯亮指示系统正常运行。 • 绿灯闪烁指示系统在某种降级状况下运行。 • 琥珀色灯闪烁指示系统处于不严重的状况。 • 琥珀色灯亮指示系统处于严重的或不可恢复的状况。 • 灯不亮指示系统正在启动或关闭。 **重要！** 琥珀色状态指示灯优先于绿色状态指示灯。当琥珀色指示灯亮起或闪烁时，绿灯熄灭。 有关详细信息，请参阅第 122 页的 DC3500 系统状态表。
硬盘驱动器活动	指示硬盘驱动器状态： • 绿灯闪烁指示固定硬盘驱动器处于活动状态。 • 琥珀色指示灯亮指示固定硬盘驱动器故障。 • 灯不亮指示没有驱动器活动，或者系统已关闭电源。
NIC 活动	指示是否有任何网络活动。 • 绿灯亮指示有网络活动。 • 灯不亮表示没有网络活动。
系统 ID	帮助识别安装在有其他类似系统的高密度机架中的系统 • 蓝色指示灯指示按下了 ID 按钮，并且设备背面的蓝灯亮。 • 灯不亮指示未按下 ID 按钮。

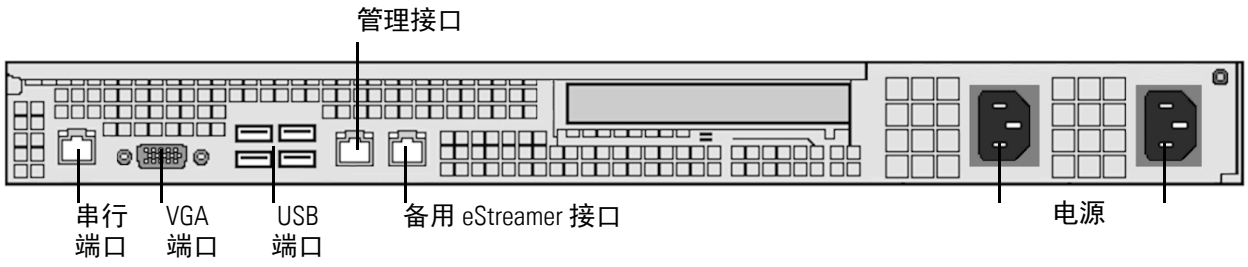
DC3500 系统状态表介绍系统状态 LED 可能点亮的情况。

DC3500 系统状态

情况	说明
严重	与以下事件关联的任何严重或不可恢复的阈值超出： • 温度、电压或风扇严重阈值超出 • 电源子系统故障 • 由于未正确安装处理器或处理器不兼容导致系统无法启动 • 严重事件记录错误，包括系统内存不可校正的 ECC 错误和严重 / 不可校正的总线错误，例如 PCI SERR 和 PERR
不严重	不严重情况是与以下事件关联的阈值超出： • 温度、电压或风扇非严重阈值超出 • 机箱入侵 • 通过系统 BIOS 设置故障指示命令； BIOS 可以使用命令来指示其他非严重的状态，例如，系统内存或 CPU 配置更改
降级	与以下事件相关的一种降级情况： • 一个或多个处理器由故障弹性启动 (FRB) 或 BIOS 禁用 • BIOS 禁用或映射掉某些系统内存 • 其中一个电源被拔下或无法使用 **提示！** 如果发现降级情况指示，请先检查您的电源连接。关闭设备电源，断开两条电源线，重新连接电源线，然后重新启动设备。 **警告！** 要安全关闭电源，请使用 《*Sourcefire 3D 系统用户指南*》 “ 管理设备 ” 章节中的操作步骤，或从防御中心外壳运行 `shutdown -h now` 命令。

DC3500 机箱后视图

机箱背部包含连接端口和电源。



DC3500 系统组件：后视图表介绍显示在设备背面的功能。

DC3500 系统组件：后视图

功能	说明
PS/2 鼠标连接器 PS/2 键盘连接器 VGA 端口 USB 端口	允许您将显示器、键盘和鼠标连接到设备，作为使用 RJ45 串行端口的备选方案，以建立工作站到设备的直接连接。您还必须通过 USB 端口使用设备随附的闪存盘将设备恢复到其原始出厂状态。
RJ45 串行端口	允许您建立工作站到设备的直接连接 （使用 RJ45 到 DB-9 适配器），以直接访问设备上的所有管理服务。 RJ45 串行端口**仅**用于维护和配置用途，并非意在传输业务流量。请参阅第 124 页的 DC3500 串行端口引脚分配表。 **重要！** 您不能同时使用前面板和后面板的串行端口。
10/100/1000 Mbps 以太网管理接口	提供带外管理网络连接。管理接口**仅**用于维护和配置用途，并非意在传输业务流量。
备用 eStreamer 接口：	为 eStreamer 客户端提供备用接口
冗余电源	通过交流电源为设备供电

10/100/1000 Mbps 管理接口位于设备的背面。 DC3500 管理接口 LED表介绍与管理接口相关的 LED。

DC3500 管理接口 LED

LED	说明
左侧 （活动）	指示端口上的活动： • 指示灯闪烁指示活动。 • 灯不亮表示没有活动。
右侧 （链路）	指示链路是否可用： • 指示灯亮指示链路可用。 • 灯不亮表示没有链路。

电源模块位于设备的背面。 DC3500 电源 LED表介绍与双电源相关的 LED。

DC3500 电源 LED

LED	说明
熄灭	没有接通电源。
琥珀色	未向此模块供电。 或 电源严重事件，例如，模块故障、保险丝熔断或风扇故障；电源关闭。
琥珀色闪烁	电源警告事件，例如，高温或风扇速度较慢；电源继续运行。
绿色闪烁	存在交流输入；有待机电压，电源已关闭。
绿色	电源已接通且打开。

DC3500 串行端口引脚分配表介绍 DB-9 连接器上提供的信号。

DC3500 串行端口引脚分配

引脚	信号	说明
1	DCD	载波检测
2	RD	接收的数据
3	TD	发送的数据
4	DTR	数据终端就绪
5	GND	接地
6	DSR	数据设置完成
7	RTS	请求发送
8	CTS	清除发送
9	RI	振铃指示器

DC3500 内部 USB 连接器引脚布局表介绍 USB 连接器上提供的信号。

DC3500 内部 USB 连接器引脚布局

引脚	信号名称	说明
1	USB2_VBUS4	USB 电源 （端口 4）
2	USB2_VBUS5	USB 电源 （端口 5）
3	USB_ICH_P4N_CONN	USB 端口 4 负信号
4	USB_ICH_P5N_CONN	USB 端口 5 负信号
5	USB_ICH_P4P_CONN	USB 端口 4 正信号
6	USB_ICH_P5P_CONN	USB 端口 5 正信号
7	接地	
8	接地	
9	密钥	没有引脚
10	TP_ISB_ICH_NC	测试点

DC3500 物理和环境参数

DC3500 物理和环境参数表介绍设备的物理属性和环境参数。

DC3500 物理和环境参数

参数	说明
外形	1U
尺寸 （深 x 宽 x 高）	26.2 英寸 x 16.93 英寸 x 1.7 英寸 （66.5 厘米 x 43.0 厘米 x 4.3 厘米）
重量	38 磅 （17.2 千克）
电源	120 VAC 的双 650 W 冗余电源 110 V、 50/60 Hz 时电流最大值为 8.5 A 220 V、 50/60 Hz 时电流最大值为 4.2 A
工作温度	50°F 至 95°F （10°C 至 35°C）

DC3500 物理和环境参数 （续）

参数	说明
非工作温度	-40°F 至 158°F （-40°C 至 70°C）
工作湿度	5% 至 85%
非工作湿度	90%，非冷凝 - 温度为 95°F (35°C) 时
噪声	在典型办公室环境温度下处于空闲状态时 <7.0 BA （机架安装）
工作冲击	2G 半正弦波冲击无错误 （持续 11 毫秒）
包装冲击	从 24 英寸 （60 厘米）处自由下落，尽管可能存在表面损坏，但仍可运行；机箱重量 40 到 80 磅 （18 到 36 千克）。
静电释放	+/- 15 kV （I/O 端口 +/-8 KV）根据英特尔环境测试规格
空气流动	正面到背面
系统冷却需求	2550 BTU/ 小时
RoHS	符合 RoHS 指令 2002/95/EC

Sourcefire 7000 系列设备

所有 7000 系列设备在设备正面都有一个可以查看的 LCD 面板，如果启用，您还可以配置设备。

有关设备的详细信息，请参阅以下各节：

- 第 126 页的Sourcefire 3D7010、 3D7020 和 3D7030
- 第 133 页的Sourcefire 3D7110 和 3D7120
- 第 141 页的Sourcefire 3D7115、 3D7125 和 AMP7150

Sourcefire 3D7010、 3D7020 和 3D7030

3D7010、 3D7020 和 3D7030 设备，也称为 70xx 系列，是 1U 设备，宽度为半个机架托架宽，带有八个铜缆接口，每个接口都具有可配置旁路功能。请参阅第 205 页的Sourcefire 3 系列信息以了解 70xx 系列设备的安全注意事项。

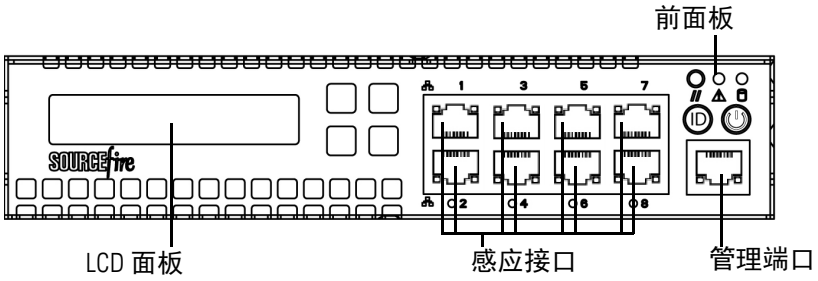
有关详细信息，请参阅以下各节：

- 第 127 页的70xx 系列前视图
- 第 131 页的70xx 系列后视图
- 第 132 页的70xx 系列物理和环境参数

70xx 系列前视图

机箱前面包含 LCD 面板、感应接口、前面板和管理端口。

70xx 系列 （机箱：CHRY-1U-AC）前视图



70xx 系列系统组件：前视图表介绍设备前面的功能。

70xx 系列系统组件：前视图

功能	说明
LCD 面板	在多种模式下运行，可以配置设备、显示错误消息和查看系统状态。有关详细信息，请参阅第 98 页的使用 3 系列设备上的 LCD 面板。
感应接口	包含连接到网络的感应接口。有关详细信息，请参阅第 129 页的感应接口。
10/100/1000 Mbps 以太网管理接口	提供带外管理网络连接。管理接口**仅**用于维护和配置用途，并非意在传输业务流量。
前面板	配有显示系统运行状态的 LED 以及各种控件 （如电源按钮）。有关详细信息，请参阅第 134 页的 3D7110 和 3D7120 前面板组件。

70xx 系列前面板

前面板组件

A	复位按钮	D	系统 ID 按钮
B	系统状态 LED	E	电源按钮和 LED
C	硬盘驱动器活动 LED		

机箱的前面板配有显示系统运行状态的 LED。 70xx 系列前面板 LED表介绍前面板上的 LED。

70xx 系列前面板 LED

LED	说明
复位按钮	使您可以重新启动设备，而无需将其与电源断开连接。
系统状态	指示系统状态： • 绿灯指示系统已启动且正常运行，或已断电并连接到交流电源。 • 琥珀色灯指示系统故障。 有关详细信息，请参阅第 129 页的 70xx 系列系统状态表。
硬盘驱动器活动	指示硬盘驱动器状态： • 绿灯闪烁指示固定硬盘驱动器处于活动状态。 • 如果指示灯熄灭，表示无驱动器活动或系统已关闭电源。
系统 ID	在按下时 ID 按钮显示蓝色灯光，并且设备背面的蓝灯亮。
电源按钮和 LED	指示设备是否已通电： • 绿灯指示设备已通电且系统已打开。 • 灯不亮表示系统关闭或未通电。

70xx 系列系统状态表介绍系统状态 LED 可能点亮的情况。

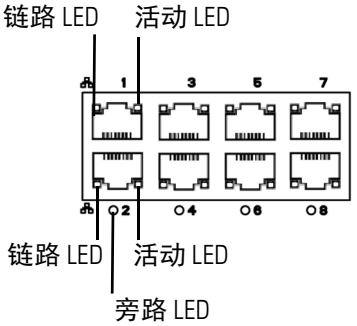
70xx 系列系统状态

情况	说明
严重	与以下事件关联的任何严重或不可恢复的阈值超出： • 温度、电压或风扇严重阈值超出 • 电源子系统故障 • 由于未正确安装处理器或处理器不兼容导致系统无法启动 • 严重事件记录错误，包括系统内存不可校正的 ECC 错误和严重 / 不可校正的总线错误，例如 PCI SERR 和 PERR
不严重	不严重情况是与以下事件关联的阈值超出： • 温度、电压或风扇非严重阈值超出 • 通过系统 BIOS 设置故障指示命令； BIOS 可以使用命令来指示其他非严重的状态，例如，系统内存或 CPU 配置更改
降级	与以下事件相关的一种降级情况： • 一个或多个处理器由故障弹性启动 (FRB) 或 BIOS 禁用 • BIOS 禁用或映射掉某些系统内存 • 其中一个电源被拔下或无法使用

感应接口

70xx 系列设备带有八个铜缆接口，每个接口都具有可配置旁路功能。

八端口 1000BASE-T 铜缆接口



请通过70xx 系列铜缆链路/活动 LED表了解铜缆接口上的活动和链路 LED。

70xx 系列铜缆链路 / 活动 LED

状态	说明
两个 LED 均熄灭	接口没有链路。
链路指示灯显示琥珀色	接口上的流量速度是 10 Mb 或 100 Mb。
链路指示灯显示绿色	接口上的流量速度是 1 Gb。
绿色活动指示灯闪烁	接口有链路且正在传输流量。

请通过 70xx 系列铜缆旁路 LED表了解铜缆接口上的旁路 LED。

70xx 系列铜缆旁路 LED

状态	说明
熄灭	接口对不处于旁路模式或未通电。
稳定绿色	接口对已准备好进入旁路模式。
稳定琥珀色	接口对已置为旁路模式且不检查流量。
琥珀色闪烁	接口对处于旁路模式；即无法打开。

10/100/1000 Mbps 管理接口位于设备的前面。70xx 系列管理接口 LED表介绍与管理接口相关的 LED。

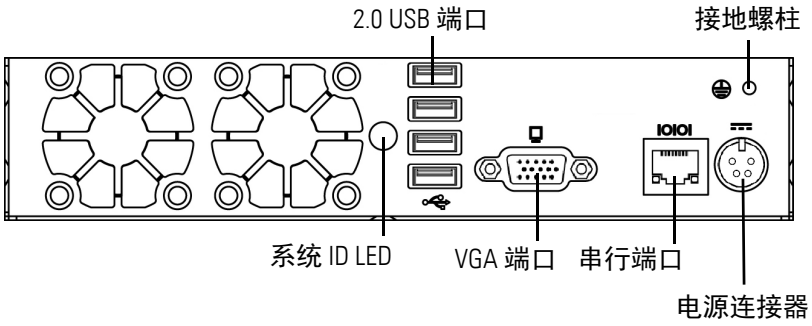
70xx 系列管理接口 LED

LED	说明
左侧 （链路）	指示链路是否可用。如果指示灯亮，表示链路可用。如果指示灯熄灭，表示没有链路。
右侧 （活动）	指示端口上的活动。如果指示灯闪烁，指示有活动。如果指示灯熄灭，表示没有活动。

70xx 系列后视图

机箱背面包含系统 ID LED、连接端口、接地螺柱和电源连接器。

70xx 系列 （机箱：CHRY-1U-AC）后视图



70xx 系列系统组件：后视图表介绍显示在设备背面的功能。

70xx 系列系统组件：后视图

功能	说明
系统 ID LED	帮助识别安装在有其他类似系统的高密度机架中的系统。蓝色 LED 指示已按下 ID 按钮。
2.0 USB 端口 VGA 端口 串行端口	允许您将显示器、键盘和鼠标连接到设备，作为使用 RJ45 串行端口的备选方案，以建立工作站到设备直接连接。
接地螺柱	允许您将设备连接到公共连接网。有关详细信息，请参阅第 213 页的设备 Sourcefire 电源要求。
12V 电源连接器	通过交流电源为设备提供电源连接。

70xx 系列物理和环境参数

70xx 系列物理和环境参数表介绍设备的物理属性和环境参数。

70xx 系列物理和环境参数

参数	说明
外形	1U，半机架宽度
尺寸 （深 x 宽 x 高）	单个机箱：12.49 英寸 x 7.89 英寸 x 1.66 英寸 （31.74 厘米 x 20.04 厘米 x 4.21 厘米） 2 机箱托架：25.05 英寸 x 17.24 英寸 x 1.73 英寸 （63.62 厘米 x 43.8 厘米 x 4.44 厘米）
安装后的最大机箱重量	机箱：7 磅。（3.17 千克） 托架中的单个机箱和电源：17.7 磅 （8.03 千克） 单个托架中的双机箱和电源：24.7 磅 （11.2 千克）
铜缆 1000BASE-T	成对配置中的千兆铜缆以太网可旁路接口 电缆和距离：Cat5E （50 米距离）
电源	200 W 交流电源 电压：100 VAC 至 240 VAC 额定 （最大：90 VAC 至 264 VAC） 电流：在整个范围内最大为 2A 频率范围：50/60 Hz 额定 （最大：47 Hz 至 63 Hz）
工作温度	0°C 至 40°C （32°F 至 104°F）
非工作温度	-20°C 至 70°C （-29°F 至 158°F）
工作湿度	5% 至 95%，无冷凝 不建议在这些限制范围之外运行，并且也不对这种运行提供保证。
非工作湿度	0% 至 95%，非冷凝 在低于 95% 非冷凝相对湿度的条件下存储设备。将设备置于低于最大工作湿度的环境中至少 48 小时，然后再投入使用。
海拔	0 英尺 （海平面）至 5905 英尺 （0 至 1800 米）
冷却要求	682 BTU/ 小时 您必须提供足够的冷却以使设备运行在其需要的工作温度范围内。不这么做可能导致设备出现故障或损坏。

70xx 系列物理和环境参数 （续）

参数	说明
噪声	53 dBA （空闲时）。 62 dBA （处理器满负载运行时）。
工作冲击	5G 半正弦波冲击无错误 （持续 11 毫秒）
空气流动	每分钟 20 立方英尺 （0.57 立方米） 气流从设备前面进入并从背面排出，不从侧面通过。

Sourcefire 3D7110 和 3D7120

作为 71xx 系列一部分的 3D7110 和 3D7120 设备是 1U 设备，带有八个铜缆或八个光纤接口，每个接口都具有可配置的旁路功能。请参阅第 205 页的Sourcefire 3 系列信息以了解 71xx 系列设备的安全注意事项。

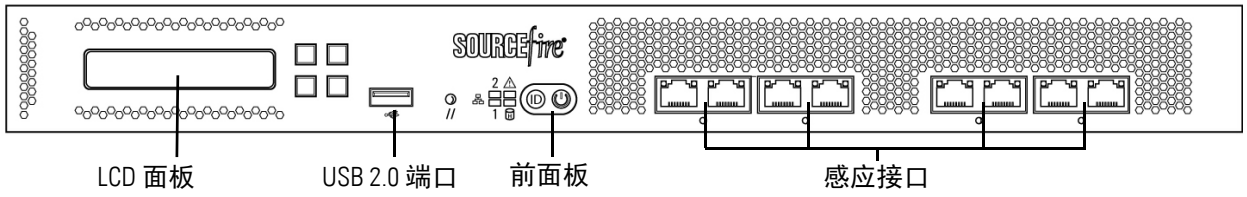
有关详细信息，请参阅以下各节：

- 第 133 页的3D7110 和 3D7120 机箱前视图
- 第 138 页的3D7110 和 3D7120 机箱后视图
- 第 140 页的3D7110 和 3D7120 物理和环境参数

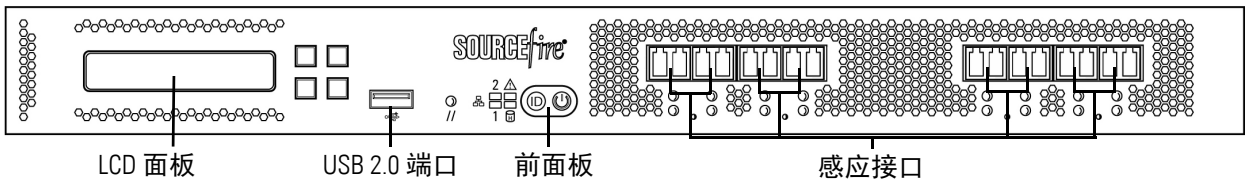
3D7110 和 3D7120 机箱前视图

机箱前面包含 LCD 面板、 USB 端口、前面板和铜缆或光纤感应接口。

提供铜缆接口的 3D7110 和 3D7120 （机箱：GERY-1U-8-C-AC）



提供光纤接口的 3D7110 和 3D7120 （机箱：GERY-1U-8-FM-AC）

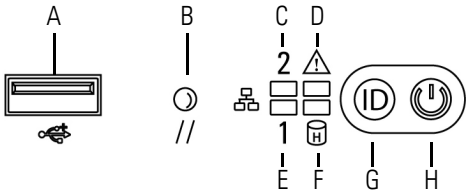


3D7110 和 3D7120 系统组件：前视图表介绍设备前面的功能。

3D7110 和 3D7120 系统组件：前视图

功能	说明
LCD 面板	在多种模式下运行，可以配置设备、显示错误消息和查看系统状态。有关详细信息，请参阅第 98 页的使用 3 系列设备上的 LCD 面板。
前面板 USB 2.0 端口	允许您将键盘连接到设备上。
前面板	配有显示系统运行状态的 LED 以及各种控件 （如电源按钮）。有关详细信息，请参阅第 134 页的 3D7110 和 3D7120 前面板。
感应接口	包含连接到网络的感应接口。有关详细信息，请参阅第 136 页的 3D7110 和 3D7120 感应接口。

3D7110 和 3D7120 前面板



3D7110 和 3D7120 前面板组件

A	USB 2.0 连接器	E	NIC 1 活动 LED
B	复位按钮	F	硬盘驱动器活动 LED
C	NIC 2 活动 LED	G	ID 按钮
D	系统状态 LED	H	电源按钮和 LED

机箱的前面板配有显示系统运行状态的 LED。 8000 系列前面板组件表介绍前面板上的 LED。

3D7110 和 3D7120 前面板 LED

LED	说明
NIC 活动 （1 和 2）	指示是否有任何网络活动。 • 绿灯亮指示有网络活动。 • 灯不亮表示没有网络活动。
系统状态	指示系统状态： • 灯不亮指示系统正常运行或已关闭电源。 • 红灯指示系统错误。 有关详细信息，请参阅第 136 页的 3D7110 和 3D7120 系统状态。
复位按钮	使您可以重新启动设备，而无需将其与电源断开连接。
硬盘驱动器活动	指示硬盘驱动器状态： • 绿灯闪烁指示固定硬盘驱动器处于活动状态。 • 琥珀色指示灯亮指示固定硬盘驱动器故障。 • 如果指示灯熄灭，表示无驱动器活动或系统已关闭电源。
系统 ID	帮助识别安装在有其他类似系统的高密度机架中的系统 • 蓝色指示灯指示按下了 ID 按钮，并且设备背面的蓝灯亮。 • 灯不亮指示未按下 ID 按钮。
电源按钮和 LED	指示设备是否已通电： • 绿灯指示设备已通电且系统已打开。 • 绿灯闪烁表示设备已通电且已关闭。 • 如果指示灯熄灭，表示系统未通电。

下表介绍系统状态 LED 可能点亮的情况。

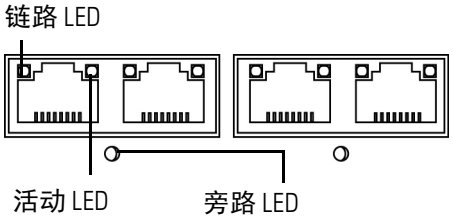
3D7110 和 3D7120 系统状态

情况	说明
严重	与以下事件关联的任何严重或不可恢复的阈值超出： • 温度、电压或风扇严重阈值超出 • 电源子系统故障 • 由于未正确安装处理器或处理器不兼容导致系统无法启动 • 严重事件记录错误，包括系统内存不可校正的 ECC 错误和严重 / 不可校正的总线错误，例如 PCI SERR 和 PERR
不严重	不严重情况是与以下事件关联的阈值超出： • 温度、电压或风扇非严重阈值超出 • 机箱入侵 • 通过系统 BIOS 设置故障指示命令； BIOS 可以使用命令来指示其他非严重的状态，例如，系统内存或 CPU 配置更改
降级	与以下事件相关的任何降级情况： • 一个或多个处理器由故障弹性启动 (FRB) 或 BIOS 禁用 • BIOS 禁用或映射掉某些系统内存 • 其中一个电源被拔下或无法使用 **提示！** 如果发现降级情况指示，请先检查您的电源连接。关闭设备电源，断开两条电源线，重新连接电源线，然后重新启动设备。 **警告！** 要安全关闭电源，请使用《*Sourcefire 3D 系统用户指南*》“管理设备”章节中的操作步骤，或从 CLI 运行 `system shutdown` 命令。

3D7110 和 3D7120 感应接口

3D7110 和 3D7120 设备带有八个铜缆端口接口或八个光纤端口接口，每个接口都具有可配置旁路功能。

八端口 1000BASE-T 铜缆接口



请通过下表了解铜缆接口上的活动和链路 LED。

3D7110 和 3D7120 铜缆链路 / 活动 LED

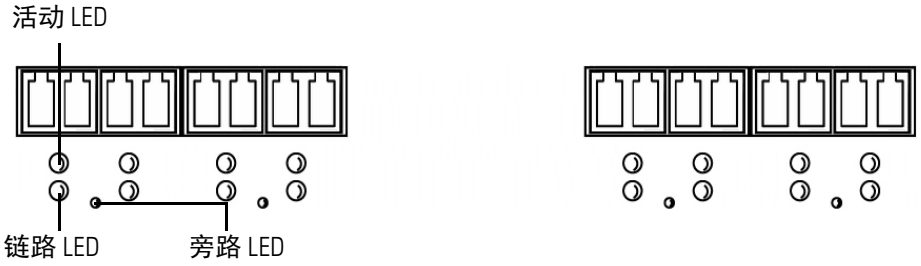
状态	说明
两个 LED 均熄灭	接口没有链路。
链路指示灯显示琥珀色	接口上的流量速度是 10 Mb 或 100 Mb。
链路指示灯显示绿色	接口上的流量速度是 1 Gb。
绿色活动指示灯闪烁	接口有链路且正在传输流量。

请通过下表了解铜缆接口的旁路 LED。

3D7110 和 3D7120 铜缆旁路 LED

状态	说明
熄灭	接口对不处于旁路模式或未通电。
稳定绿色	接口对已准备好进入旁路模式。
稳定琥珀色	接口对已置为旁路模式且不检查流量。
琥珀色闪烁	接口对处于旁路模式；即无法打开。

八端口 1000BASE-SX 光纤可配置旁路接口



请通过下表了解光纤接口上的链路和活动 LED。

3D7110 和 3D7120 光纤链路 / 活动 LED

状态	说明
顶部 （活动）	对于内联接口：当接口有活动时，指示灯亮。如果指示灯不亮，表示没有活动。 对于被动接口：指示灯无功能。
底部 （链路）	对于内联或被动接口：当接口有链路时，指示灯亮。如果指示灯不亮，表示没有链路。

请通过下表了解光纤接口上的活动和链路 LED。

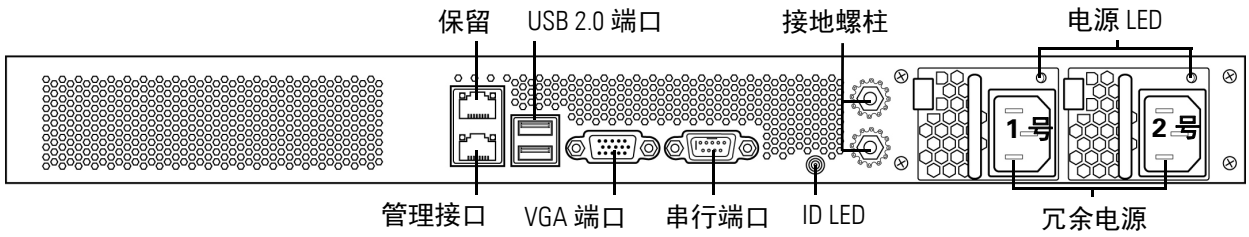
3D7110 和 3D7120 光纤旁路 LED

状态	说明
熄灭	接口对不处于旁路模式或未通电。
稳定绿色	接口对已准备好进入旁路模式。
稳定琥珀色	接口对已置为旁路模式且不检查流量。
琥珀色闪烁	接口对处于旁路模式；即无法打开。

3D7110 和 3D7120 机箱后视图

机箱背面包含管理端口、连接端口、接地螺柱和电源。

3D7110 和 3D7120 （机箱：GERY-1U-8-C-AC 或 GERY-1U-8-FM-AC）后视图



下表介绍显示在设备背面的功能。

3D7110 和 3D7120 系统组件：后视图

功能	说明
VGA 端口 USB 端口	允许您将显示器、键盘和鼠标连接到设备，以建立工作站到设备的直接连接。
10/100/1000 Mbps 以太网管理接口	提供带外管理网络连接。管理接口**仅**用于维护和配置用途，并非意在传输业务流量。
系统 ID LED	帮助识别安装在有其他类似系统的高密度机架中的系统。蓝灯指示已按下 ID 按钮。
接地螺柱	允许您将设备连接到公共连接网。有关详细信息，请参阅第 213 页的设备 Sourcefire 电源要求。
冗余电源	通过交流电源为设备供电。请查看机箱背面， 1 号电源位于左侧， 2 号电源位于右侧。
电源 LED	指示电源的状态。请参阅第 140 页的 3D7110 和 3D7120 电源 LED。

10/100/1000 Mbps 管理接口位于设备的背面。下表介绍与管理接口相关的 LED。

3D7110 和 3D7120 管理接口 LED

LED	说明
左侧 （活动）	指示端口上的活动： • 指示灯闪烁指示活动。 • 灯不亮表示没有活动。
右侧 （链路）	指示链路是否可用： • 指示灯亮指示链路可用。 • 灯不亮表示没有链路。

电源模块位于设备的背面。下表介绍与电源相关的 LED。

3D7110 和 3D7120 电源 LED

LED	说明
熄灭	未插入电源线。
红色	未向此模块供电。 或 电源严重事件，例如，模块故障、保险丝熔断或风扇故障；电源关闭。
红色闪烁	电源警告事件，例如，高温或风扇速度较慢；电源继续运行。
绿色闪烁	存在交流输入；有待机电压，电源已关闭。
绿色	电源已接通且打开。

3D7110 和 3D7120 物理和环境参数

下表介绍设备的物理属性和环境参数。

3D7110 和 3D7120 物理和环境参数

参数	说明
外形	1U
尺寸 （深 x 宽 x 高）	21.6 英寸 x 19.0 英寸 x 1.73 英寸 （54.9 厘米 x 48.3 厘米 x 4.4 厘米）
安装后的最大重量	27.5 磅 （12.5 千克）
铜缆 1000BASE-T	成对配置中的千兆铜缆以太网可旁路接口 电缆和距离：Cat5E （50 米距离）
光纤 1000BASE-SX	有 LC 连接器的光纤可旁路接口 线缆和距离：SX 是多模光纤 （850 纳米），距离为 550 米 （标准）
电源	450 W 双冗余 (1+1) 交流电源 电压：100 VAC 至 240 VAC 额定 （最大：85 VAC 至 264 VAC） 电流：90 VAC 到 132 VAC 的最大值为 3 A （每个电源） 187 VAC 到 264 VAC 的最大值为 1.5 A （每个电源） 频率范围：47 Hz 至 63 Hz
工作温度	5°C 至 40°C （41°F 至 104°F）

3D7110 和 3D7120 物理和环境参数 （续）

参数	说明
非工作温度	-20°C 至 70°C （-29°F 至 158°F）
工作湿度	5% 至 85%，非冷凝
非工作湿度	5% 至 90%，非冷凝，在温度从 25°C 到 35°C （77°F 到 95°F）时的最大湿球温度为 28°C (82°F) 在低于 95% 非冷凝相对湿度的条件下存储设备。将设备置于低于最大工作湿度的环境中至少 48 小时，然后再投入使用。
海拔	0 英尺 （海平面）至 5905 英尺 （1800 米）
冷却要求	900 BTU/ 小时 您必须提供足够的冷却以使设备运行在其需要的工作温度范围内。不这么做可能导致设备出现故障或损坏。
噪声	64 dBA （处理器满负载运行，风扇正常运行时） 符合 GR-63-CORE 4.6 噪声标准
工作冲击	符合 Bellecore GR-63-CORE 标准
空气流动	每分钟 140 立方英尺 （3.9 立方米） 气流从设备前面进入并从背面排出，不从侧面通过。

Sourcefire 3D7115、 3D7125 和 AMP7150

作为 71xx 系列一部分的 3D7115、3D7125 和 AMP7150 设备带有四个具有可配置旁路功能的铜缆端口接口和八个不具有旁路功能的小型封装热插拔 (SFP) 端口。为确保兼容性，请仅使用 Sourcefire SFP 收发器。请参阅第 205 页的Sourcefire 3 系列信息以了解 71xx 系列设备的安全注意事项。

重要！ Sourcefire AMP7150 有许多外形尺寸与 3D7115 和 3D7125 相同，但已被优化为可以利用 Sourcefire 基于网络的高级恶意软件防护 (AMP) 功能。

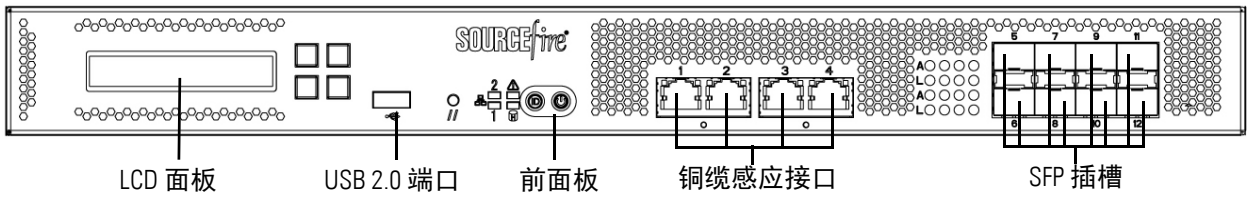
有关详细信息，请参阅以下各节：

- 第 142 页的3D7115、 3D7125 和 AMP7150 机箱前视图
- 第 147 页的3D7115、 3D7125 和 AMP7150 机箱后视图
- 第 149 页的3D7115、 3D7125 和 AMP7150 物理和环境参数

3D7115、 3D7125 和 AMP7150 机箱前视图

机箱前面包含 LCD 面板、 USB 端口、前面板、铜缆感应接口和 SFP 端口。

3D7115、 3D7125 和 AMP7150 （机箱：GERY-1U-8-4C8S-AC）前视图

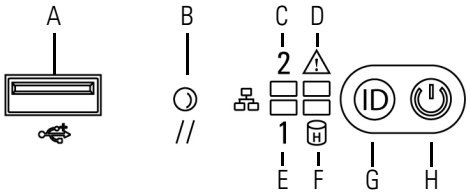


下表介绍设备前面的功能。

3D7115、 3D7125 和 AMP7150 系统组件：前视图

功能	说明
LCD 面板	在多种模式下运行，可以配置设备、显示错误消息和查看系统状态。有关详细信息，请参阅第 98 页的使用 3 系列设备上的 LCD 面板。
前面板 USB 2.0 端口	允许您将键盘连接到设备上。
前面板	配有显示系统运行状态的 LED 以及各种控件 （如电源按钮）。有关详细信息，请参阅第 142 页的 3D7115、3D7125 和 AMP7150 前面板。
感应接口	包含连接到网络的感应接口。有关详细信息，请参阅第 144 页的 3D7115、 3D7125 和 AMP7150 感应接口。

3D7115、 3D7125 和 AMP7150 前面板



3D7115、 3D7125 和 AMP7150 前面板组件

A	USB 2.0 连接器	E	NIC 1 活动 LED
B	复位按钮	F	硬盘驱动器活动 LED
C	NIC 2 活动 LED	G	ID 按钮
D	系统状态 LED	H	电源按钮和 LED

机箱的前面板配有显示系统运行状态的 LED。下表介绍前面板上的 LED。

3D7115、 3D7125 和 AMP7150 前面板组件 LED

LED	说明
NIC 活动 （1 和 2）	指示是否有任何网络活动。 • 绿灯亮指示有网络活动。 • 灯不亮表示没有网络活动。
系统状态	指示系统状态： • 灯不亮指示系统正常运行或已关闭电源。 • 红灯指示系统错误。 有关详细信息，请参阅第 144 页的 3D7115、 3D7125 和 AMP7150 系统状态。
复位按钮	使您可以重新启动设备，而无需将其与电源断开连接。
硬盘驱动器活动	指示硬盘驱动器状态： • 绿灯闪烁指示固定硬盘驱动器处于活动状态。 • 琥珀色指示灯亮指示固定硬盘驱动器故障。 • 如果指示灯熄灭，表示无驱动器活动或系统已关闭电源。
系统 ID	帮助识别安装在有其他类似系统的高密度机架中的系统 • 蓝色指示灯指示按下了 ID 按钮，并且设备背面的蓝灯亮。 • 灯不亮指示未按下 ID 按钮。
电源按钮和 LED	指示设备是否已通电： • 绿灯指示设备已通电且系统已打开。 • 绿灯闪烁表示设备已通电且已关闭。 • 灯不亮表示系统未通电。

下表介绍系统状态 LED 可能点亮的情况。

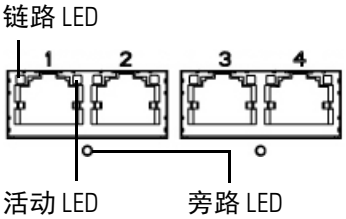
3D7115、 3D7125 和 AMP7150 系统状态

情况	说明
严重	与以下事件关联的任何严重或不可恢复的阈值超出： • 温度、电压或风扇严重阈值超出 • 电源子系统故障 • 由于未正确安装处理器或处理器不兼容导致系统无法启动 • 严重事件记录错误，包括系统内存不可校正的 ECC 错误和严重 / 不可校正的总线错误，例如 PCI SERR 和 PERR
不严重	不严重情况是与以下事件关联的阈值超出： • 温度、电压或风扇非严重阈值超出 • 机箱入侵 • 通过系统 BIOS 设置故障指示命令； BIOS 可以使用命令来指示其他非严重的状态，例如，系统内存或 CPU 配置更改
降级	与以下事件相关的任何降级情况： • 一个或多个处理器由故障弹性启动 (FRB) 或 BIOS 禁用 • BIOS 禁用或映射掉某些系统内存 • 其中一个电源被拔下或无法使用 **提示！** 如果发现降级情况指示，请先检查您的电源连接。关闭设备电源，断开两条电源线，重新连接电源线，然后重新启动设备。 **警告！** 要安全关闭电源，请使用《*Sourcefire 3D 系统用户指南*》“管理设备”章节中的操作步骤，或从 CLI 运行 `system shutdown` 命令。

3D7115、 3D7125 和 AMP7150 感应接口

3D7115、3D7125 和 AMP7150 设备带有四个具有可配置旁路功能的铜缆端口接口和八个不具有旁路功能的小型封装热插拔 (SFP) 端口。

四个 1000BASE-T 铜缆接口



请通过下表了解铜缆接口上的链路和活动 LED。

3D7115、 3D7125 和 AMP7150 铜缆链路 / 活动 LED

状态	说明
两个 LED 均熄灭	接口没有链路。
链路指示灯显示琥珀色	接口上的流量速度是 10 Mb 或 100 Mb。
链路指示灯显示绿色	接口上的流量速度是 1 Gb。
绿色活动指示灯闪烁	接口有链路且正在传输流量。

请通过下表了解铜缆接口的旁路 LED。

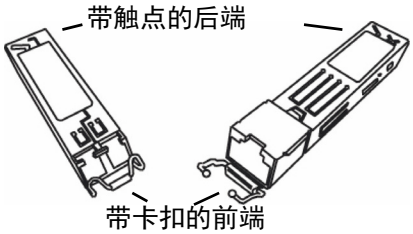
3D7115、 3D7125 和 AMP7150 铜缆旁路 LED

状态	说明
熄灭	接口对不处于旁路模式或未通电。
稳定绿色	接口对已准备好进入旁路模式。
稳定琥珀色	接口对已置为旁路模式且不检查流量。
琥珀色闪烁	接口对处于旁路模式；即无法打开。

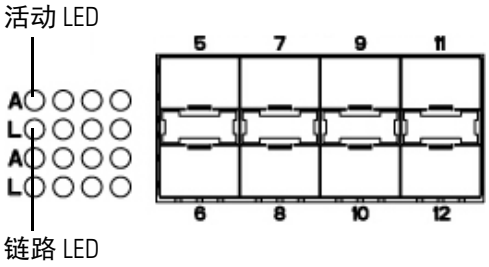
SFP 接口

您可以安装至多八个热插拔 Sourcefire SFP 收发器，收发器可以是 1G 铜缆收发器、 1G 短距离光纤收发器或 1G 长距离光纤收发器。 SFP 收发器没有旁路功能，不应用于入侵防御部署中。有关详细信息，请参阅第 231 页的在 3D7115、3D7125 和 AMP7150 设备中使用 SFP 收发器。

样本 SFP 收发器



样本光纤　　样本铜缆



请通过下表了解光纤 LED。

3D7115、 3D7125 和 AMP7150 SFP 插槽活动 / 链路 LED

状态	说明
顶部 （活动）	对于内联接口：当接口有活动时，指示灯亮。如果指示灯不亮，表示没有活动。 对于被动接口：指示灯无功能。
底部 （链路）	对于内联或被动接口：当接口有链路时，指示灯亮。如果指示灯不亮，表示没有链路。

请通过下表了解 SFP 光收发器的规格。

3D7115、 3D7125 和 AMP7150 SFP 光学参数

参数	1000BASE-SX	1000BASE-LX
光纤连接器	LC 双工	LC 双工
比特率	1000 Mbps	1000 Mbps
波特率 / 编码 / 容限	1250 Mbps/ 8b/10b 编码	1250 Mbps/ 8b/10b 编码
光纤接口	多模	仅单模

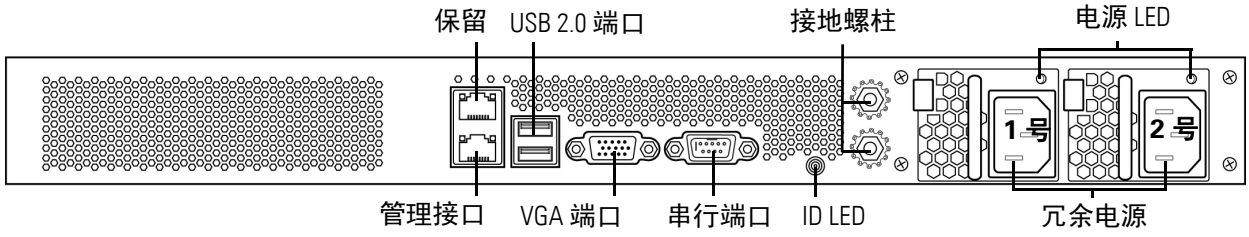
3D7115、 3D7125 和 AMP7150 SFP 光学参数 （续）

参数	1000BASE-SX	1000BASE-LX
操作距离	对于 62.5 微米 /125 微米光纤，距离为 200 米（656 英尺） 对于 50 微米 /125 微米光纤，距离为 500 米（1640 英尺）	对于 9 微米 /125 微米光纤，距离为 10 千米（6.2 英里）
发射器波长	770 - 860 纳米（典型值：850 纳米）	1270 - 1355 纳米（典型值：1310 纳米）
最大平均发射功率	0 dBm	-3 dBm
最小平均发射功率	-9.5 dBm	-11.5 dBm
接收器最大平均功率	0 dBm	-3 dBm
接收器灵敏度	-17 dBm	-19 dBm

3D7115、 3D7125 和 AMP7150 机箱后视图

机箱背面包含管理接口、连接端口、接地螺柱和电源。

3D7115、 3D7125 和 AMP7150 （机箱：GERY-1U-8-4C8S-AC）后视图



下表介绍显示在设备背面的功能。

3D7115、 3D7125 和 AMP7150 系统组件：后视图

功能	说明
VGA 端口 USB 端口	允许您将显示器、键盘和鼠标连接到设备，以建立工作站到设备的直接连接。
10/100/1000 Mbps 以太网管理接口	提供带外管理网络连接。管理接口**仅**用于维护和配置用途，并非意在传输业务流量。
系统 ID LED	帮助识别安装在有其他类似系统的高密度机架中的系统。蓝灯指示已按下 ID 按钮。
接地螺柱	允许您将设备连接到公共连接网。有关详细信息，请参阅第 213 页的设备 Sourcefire 电源要求。
冗余电源	通过交流电源为设备供电。请查看机箱背面， 1 号电源位于左侧， 2 号电源位于右侧。
电源 LED	指示电源的状态。请参阅第 149 页的 3D7115、 3D7125 和 AMP7150 电源 LED。

10/100/1000 Mbps 管理接口位于设备的背面。下表介绍与管理接口相关的 LED。

3D7115、 3D7125 和 AMP7150 管理接口 LED

LED	说明
左侧 （活动）	指示端口上的活动： • 指示灯闪烁指示活动。 • 灯不亮表示没有活动。
右侧 （链路）	指示链路是否可用： • 指示灯亮指示链路可用。 • 灯不亮表示没有链路。

电源模块位于设备的背面。下表介绍与电源相关的 LED。

3D7115、 3D7125 和 AMP7150 电源 LED

LED	说明
熄灭	未插入电源线。
红色	未向此模块供电。 或 电源严重事件，例如，模块故障、保险丝熔断或风扇故障；电源关闭。
红色闪烁	电源警告事件，例如，高温或风扇速度较慢；电源继续运行。
绿色闪烁	存在交流输入；有待机电压，电源已关闭。
绿色	电源已接通且打开。

3D7115、 3D7125 和 AMP7150 物理和环境参数

下表介绍设备的物理属性和环境参数。

3D7115、 3D7125 和 AMP7150 物理和环境参数

参数	说明
外形	1U
尺寸 （深 x 宽 x 高）	21.6 英寸 x 19.0 英寸 x 1.73 英寸 （54.9 厘米 x 48.3 厘米 x 4.4 厘米）
安装后的最大重量	29.0 磅 （13.2 千克）
铜缆 1000BASE-T	成对配置中的千兆铜缆以太网可旁路接口 电缆和距离：Cat5E （50 米距离）
铜缆 1000BASE-T SFP	成对配置中的千兆铜缆以太网非可旁路接口 电缆和距离：Cat5E （50 米距离）
光纤 1000BASE-SX SFP	有 LC 连接器的光纤非可旁路接口 线缆和距离：SX 是多模光纤 （850 纳米），距离为 550 米 （标准） 对于 62.5 微米 /125 微米光纤，距离为 200 米 （656 英尺） 对于 50 微米 /125 微米光纤，距离为 500 米 （1640 英尺）

3D7115、 3D7125 和 AMP7150 物理和环境参数 （续）

参数	说明
光纤 1000BASE-LX SFP	有 LC 连接器的光纤非可旁路接口 线缆和距离：LX 是单模光纤 （1310 纳米）：对于 9 微米 /125 微米光纤（标准），距离为 10 千米
电源	450 W 双冗余 (1+1) 交流电源 电压：100 VAC 至 240 VAC 额定 （最大：85 VAC 至 264 VAC） 电流：90 VAC 到 132 VAC 的最大值为 3 A （每个电源） 187 VAC 到 264 VAC 的最大值为 1.5 A （每个电源） 频率范围：47 Hz 至 63 Hz
工作温度	5°C 至 40°C （41°F 至 104°F）
非工作温度	-20°C 至 70°C （-29°F 至 158°F）
工作湿度	5% 至 85%，非冷凝
非工作湿度	5% 至 90%，非冷凝，在温度从 25°C 到 35°C （77°F 到 95°F）时的最大湿球温度为 28°C (82°F) 在低于 95% 非冷凝相对湿度的条件下存储设备。将设备置于低于最大工作湿度的环境中至少 48 小时，然后再投入使用。
海拔	0 英尺 （海平面）至 5905 英尺 （1800 米）
冷却要求	900 BTU/ 小时 您必须提供足够的冷却以使设备运行在其需要的工作温度范围内。不这么做可能导致设备出现故障或损坏。
噪声	64 dBA （处理器满负载运行，风扇正常运行时） 符合 GR-63-CORE 4.6 噪声标准
工作冲击	符合 Bellecore GR-63-CORE 标准
空气流动	每分钟 140 立方英尺 （3.9 立方米） 气流从设备前面进入并从背面排出，不从侧面通过。

Sourcefire 8000 系列设备

8000 系列设备使用包含铜缆或光纤感应接口的网络模块 (NetMod)。设备可以完全组装好再装运，或者您也可以安装模块。在安装 Sourcefire 3D 系统前组装设备。请参阅随模块提供的组装说明。

有些 8000 系列设备可以堆栈，以提高系统性能。对于每个堆栈套件，使用堆栈模块替换网络模块，并使用 8000 系列堆栈线缆将设备连接到一起。有关详细信息，请参阅第 66 页的使用堆栈配置中的设备。

以下各种机箱上都配备 8000 系列设备：

- 3D8120、 3D8130、 3D8140 和 AMP8150 （也称为 81xx 系列）是 1U 机箱，至多可以包含三个模块。仅对 3D8140 而言，您可以添加一个堆栈套件，以获得总计 2U 的配置。

  重要！ Sourcefire AMP8150 有许多外形尺寸与 3D8130 相同，但已被优化为可以利用 Sourcefire 基于网络的高级恶意软件防护 (AMP) 功能。

- 作为 82xx 系列一部分的 3D8250 是 2U 机箱，至多可以包含七个模块。您至多可以添加三个堆栈套件，以获得总计 8U 的配置。
- 作为 82xx 系列一部分的 3D8260 是有两个 2U 机箱的 4U 配置。主机箱包含一个堆栈模块和至多六个感应模块。辅助机箱包含一个堆栈模块。您至多可以添加两个堆栈套件，以获得总计 8U 的配置。
- 作为 82xx 系列一部分的 3D8270 是有三个 2U 机箱的 6U 配置。主机箱包含两个堆栈模块和至多五个感应模块。辅助机箱包含一个堆栈模块。您可以添加一个堆栈套件，以获得总计 8U 的配置。
- 作为 82xx 系列一部分的 3D8290 是有四个 2U 机箱的 8U 配置。主机箱包含三个堆栈模块和至多四个感应模块。辅助机箱包含一个堆栈模块。此型号配置已满，不接受堆栈套件。
- 作为 83xx 系列一部分的 3D8350 是 2U 机箱，至多可以包含七个模块。您至多可以添加三个堆栈套件，以获得总计 8U 的配置。
- 作为 83xx 系列一部分的 3D8360 是有两个 2U 机箱的 4U 配置。主机箱包含一个堆栈模块和至多六个感应模块。辅助机箱包含一个堆栈模块。您至多可以添加两个堆栈套件，以获得总计 8U 的配置。
- 作为 83xx 系列一部分的 3D8370 是有三个 2U 机箱的 6U 配置。主机箱包含两个堆栈模块和至多五个感应模块。辅助机箱包含一个堆栈模块。您可以添加一个堆栈套件，以获得总计 8U 的配置。
- 作为 83xx 系列一部分的 3D8390 是有四个 2U 机箱的 8U 配置。主机箱包含三个堆栈模块和至多四个感应模块。辅助机箱包含一个堆栈模块。此型号配置已满，不接受堆栈套件。

有关详细信息，请参阅以下各节：

8000 系列机箱前视图

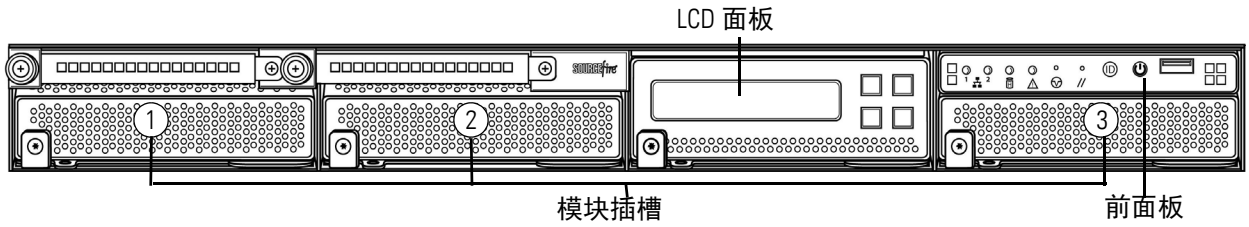
8000 系列机箱可以属于 81xx 系列、 82xx 系列或 83xx 系列。

有关 81xx 系列、82xx 系列和 83xx 系列设备的安全注意事项，请参阅第 205 页的 Sourcefire 3 系列信息。

81xx 系列机箱前视图

机箱的前视图包含 LCD 面板、前面板和三个模块插槽。

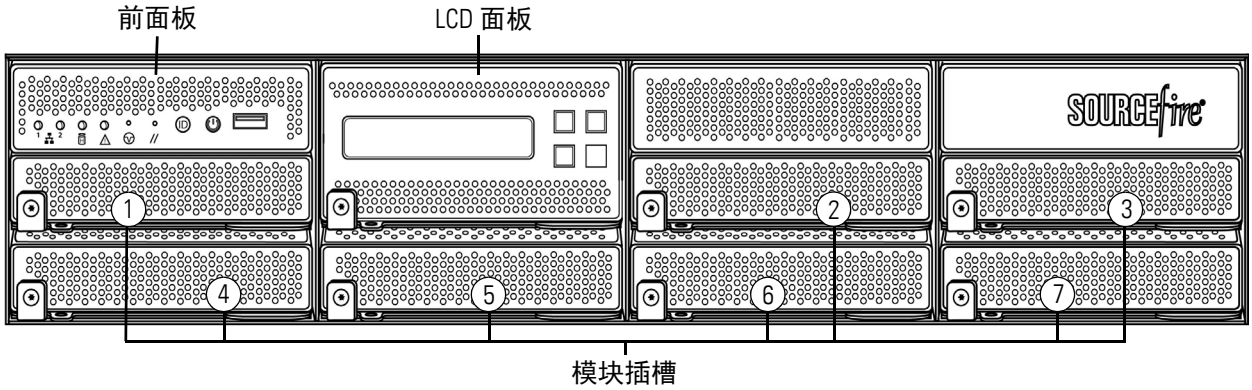
81xx 系列 （机箱：CHAS-1U-AC/DC）前视图



82xx 系列和 83xx 系列机箱前视图

机箱的前视图包含 LCD 面板、前面板与七个模块插槽。

82xx 系列 （机箱：CHAS-2U-AC/DC）和 83xx 系列 (PG35-2U-AC/DC) 前视图



8000 系列系统组件：前视图表介绍设备前面的功能。

8000 系列系统组件：前视图

功能	说明
模块插槽	包含模块。有关可用模块的详细信息，请参阅第 163 页的 8000 系列模块。
LCD 面板	在多种模式下运行，可以配置设备、显示错误消息和查看系统状态。有关详细信息，请参阅第 98 页的使用 3 系列设备上的 LCD 面板。
前面板控件	配有显示系统运行状态的 LED 以及各种控件 （如电源按钮）。有关详细信息，请参阅第 153 页的 82xx 系列和 83xx 系列前面板。
前面板 USB 端口	USB 2.0 端口用于将键盘连接到设备上。

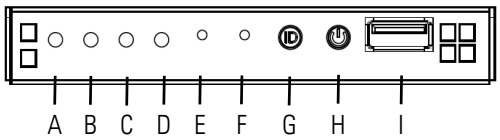
有关详细信息，请参阅以下各节：

- 第 153 页的8000 系列前面板
- 第 155 页的8000 系列机箱后视图

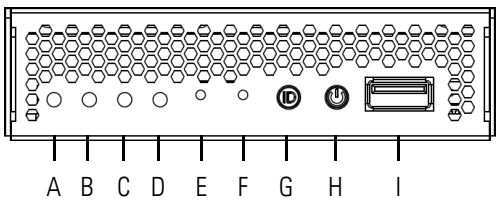
8000 系列前面板

81xx 系列、 82xx 系列和 83xx 系列的前面板包含相同的组件。

81xx 系列前面板



82xx 系列和 83xx 系列前面板



8000 系列前面板组件

A	NIC 活动 LED	F	复位按钮
B	保留	G	ID 按钮
C	硬盘驱动器活动 LED	H	电源按钮和 LED
D	系统状态 LED	I	USB 2.0 连接器
E	不可屏蔽的中断按钮		

机箱的前面板配有显示系统运行状态的 LED。8000 系列前面板 LED表介绍前面板上的 LED。

8000 系列前面板 LED

LED	说明
NIC 活动	指示是否有任何网络活动。 • 绿灯亮指示有网络活动。 • 如果指示灯熄灭，表示没有网络活动。
硬盘驱动器活动	指示硬盘驱动器状态： • 绿灯闪烁指示固定硬盘驱动器处于活动状态。 • 琥珀色灯亮指示固定硬盘驱动器故障。 • 如果指示灯熄灭，表示无驱动器活动或系统已关闭电源。
系统状态	指示系统状态： • 绿灯亮指示系统正常运行。 • 绿灯闪烁指示系统在某种降级状况下运行。 • 琥珀色灯闪烁指示系统处于不严重的状况。 • 琥珀色灯亮指示系统处于严重的或不可恢复的状况，或者系统正在启动。 • 如果指示灯熄灭，表示系统正在启动或关闭。 **重要！**琥珀色状态指示灯优先于绿色状态指示灯。当琥珀色指示灯亮起或闪烁时，绿灯熄灭。 有关详细信息，请参阅第 155 页的 8000 系列系统状态表。
系统 ID	帮助识别安装在有其他类似系统的高密度机架中的系统 • 蓝色指示灯指示按下了 ID 按钮，并且设备背面的蓝灯亮。 • 灯不亮指示未按下 ID 按钮。
电源按钮和 LED	指示系统是否已通电： • 绿灯亮指示系统已通电。 • 如果指示灯熄灭，表示系统未通电。

8000 系列系统状态表介绍系统状态 LED 可能点亮的情况。

8000 系列系统状态

情况	说明
严重	与以下事件关联的任何严重或不可恢复的阈值超出： • 温度、电压或风扇严重阈值超出 • 电源子系统故障 • 由于未正确安装处理器或处理器不兼容导致系统无法启动 • 严重事件记录错误，包括系统内存不可校正的 ECC 错误和严重 / 不可校正的总线错误，例如 PCI SERR 和 PERR
不严重	不严重情况是与以下事件关联的阈值超出： • 温度、电压或风扇非严重阈值超出 • 机箱入侵 • 通过系统 BIOS 设置故障指示命令； BIOS 可以使用命令来指示其他非严重的状态，例如，系统内存或 CPU 配置更改
降级	与以下事件相关的一种降级情况： • 一个或多个处理器由故障弹性启动 (FRB) 或 BIOS 禁用 • BIOS 禁用或映射掉某些系统内存 • 其中一个电源被拔下或无法使用 **提示！** 如果发现降级情况指示，请先检查您的电源连接。关闭设备电源，断开两条电源线，重新连接电源线，然后重新启动设备。 **警告！** 要安全关闭电源，请使用《*Sourcefire 3D 系统用户指南*》“管理设备”章节中的操作步骤，或从 CLI 运行 `system shutdown` 命令。

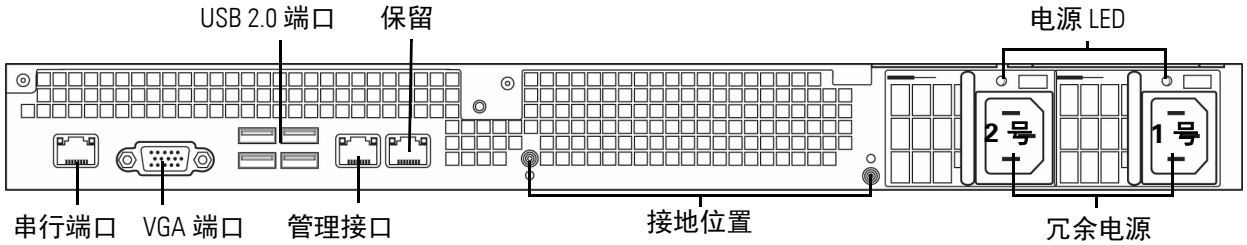
8000 系列机箱后视图

8000 系列机箱可能属于 81xx 系列、 82xx 系列或 83xx 系列。

81xx 系列机箱后视图

机箱后视图包含连接端口、管理接口和电源。

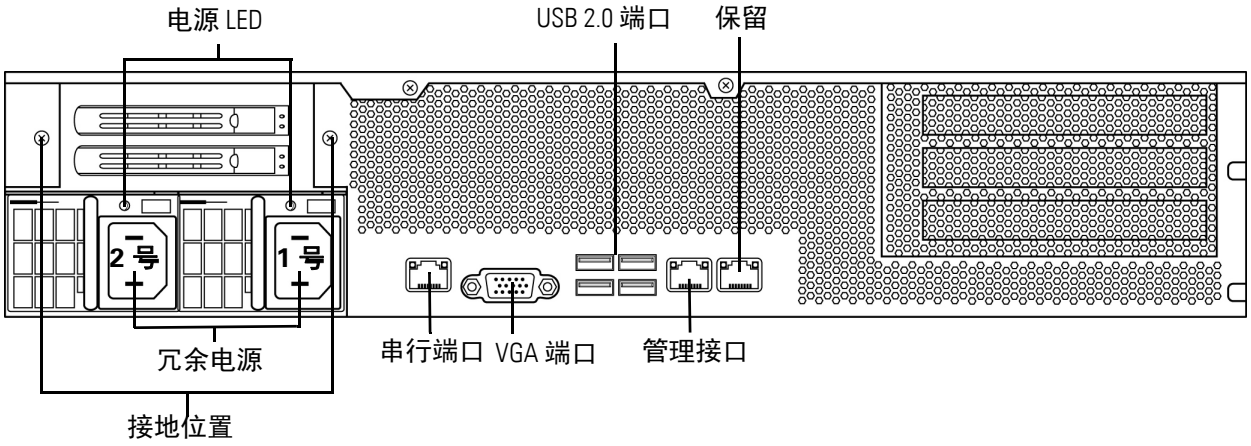
81xx 系列 （机箱：CHAS-1U-AC/DC）后视图



82xx 系列机箱后视图

机箱后视图包含电源、连接端口和管理接口。

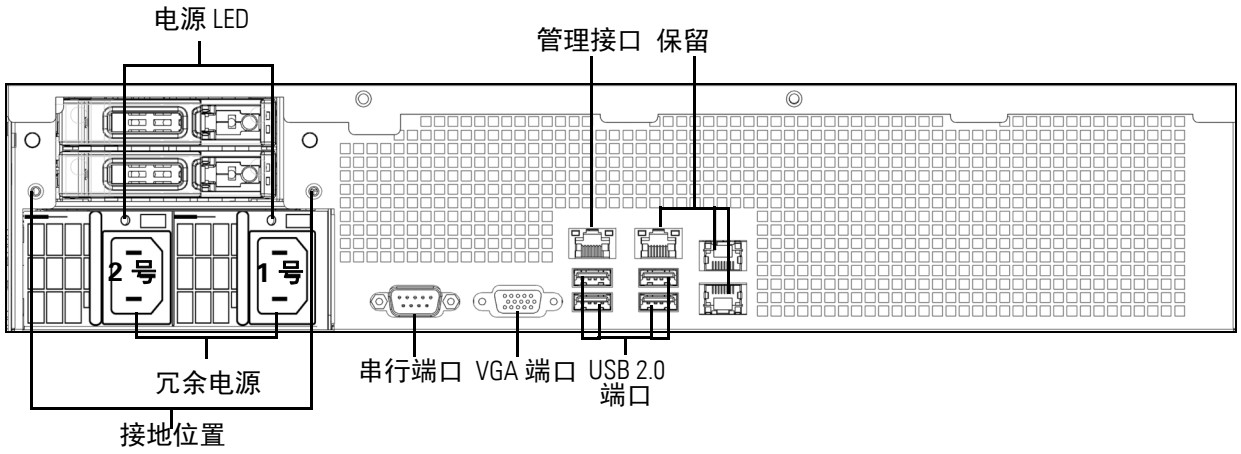
82xx 系列 （机箱：CHAS-2U-AC/DC）后视图



83xx 系列机箱后视图

机箱后视图包含电源、连接端口和管理接口。

83xx 系列 （机箱：PG35-2U-AC/DC）后视图



8000 系列系统组件：后视图表介绍显示在设备背面的功能。

8000 系列系统组件：后视图

功能	说明
VGA 端口 USB 2.0 端口	允许您将显示器、键盘和鼠标连接到设备，作为使用串行端口的备选方案，以建立工作站到设备的直接连接。
RJ45 串行端口（81xx 系列和 82xx 系列）	允许您建立工作站到设备的直接连接 （使用 RJ45 到 DB-9 适配器），以直接访问设备上的所有管理服务。RJ45 串行端口**仅**用于维护和配置用途，并非意在传输业务流量。请参阅第 158 页的 8000 系列 RJ45 到 DB-9 适配器引脚布局表。
RS232 串行端口（83xx 系列）	允许您建立工作站到设备的直接连接，以直接访问设备上的所有管理服务。 RJ232 串行端口**仅**用于维护和配置用途，并非意在传输业务流量。
10/100/1000 Mbps 以太网管理接口	提供带外管理网络连接。管理接口**仅**用于维护和配置用途，并非意在传输业务流量。
冗余电源	通过交流电源为设备供电。请查看机箱背面， 1 号电源位于右侧， 2 号电源位于左侧。
接地位置	允许您将设备连接到公共连接网。有关详细信息，请参阅第 213 页的设备 Sourcefire 电源要求。

10/100/1000 Mbps 管理接口位于设备的背面。 8000 系列管理接口 LED表介绍与管理接口相关的 LED。

8000 系列管理接口 LED

LED	说明
左侧 （活动）	指示端口上的活动： • 指示灯闪烁指示活动。 • 灯不亮表示没有活动。
右侧 （链路）	指示链路是否可用： • 指示灯亮指示链路可用。 • 灯不亮表示没有链路。

电源模块位于设备的背面。 8000 系列电源 LED表介绍与管理接口相关的 LED。

8000 系列电源 LED

LED	说明
熄灭	没有接通电源。
琥珀色	未向此模块供电。 或 电源严重事件，例如，模块故障、保险丝熔断或风扇故障；电源关闭。
琥珀色闪烁	电源警告事件，例如，高温或风扇速度较慢；电源继续运行。
绿色闪烁	存在交流输入；有待机电压，电源已关闭。
绿色	电源已接通且打开。

8000 系列 RJ45 到 DB-9 适配器引脚布局表列出典型 DB-9 串行连接器上的信号和设备的 RJ45 串行连接器上相应的引脚。您可以使用此表构建串行连接的适配器。

8000 系列 RJ45 到 DB-9 适配器引脚布局

DB-9 引脚	信号	说明	RJ45 引脚
1	DCD/DSR	数据载波检测 / 数据设置完成	7
2	RD	接收数据	6
3	TD	传输数据	3
4	DTR	数据终端就绪	2
5	GND	接地	4 和 5
6		无连接	
7	RTS	请求发送	1
8	CTS	清除发送	8
9		无连接	

8000 系列物理和环境参数

下表介绍 81xx 系列设备的物理属性和环境参数。

81xx 系列物理和环境参数

参数	说明
外形	1U
尺寸 （深 x 宽 x 高）	28.7 英寸 x 17.2 英寸 x 1.73 英寸 （72.8 厘米 x 43.3 厘米 x 4.4 厘米）
安装后的 最大重量	43.5 磅 （19.8 千克）
铜缆 1000BASE-T 可配置旁路网络模块	成对配置的四端口千兆铜缆以太网可配置旁路接口 电缆和距离：Cat5E （50 米距离）
光纤 10GBASE 可配置旁路 MMSR 或 SMLR 网络模块	带 LC 连接器的双端口光纤可配置旁路接口 线缆和距离： LR 是单模光纤，距离为 5000 米 （可用） SR 是多模光纤 （850 纳米），距离为 550 米 （标准）
光纤 1000BASE-SX 可配置旁路网络模块	带 LC 连接器的四端口光纤可配置旁路接口 1000BASE-SX 线缆和距离：SX 是多模光纤 （850 纳米），距离为 550 米 （标准）
铜缆 1000BASE-T 非旁路网络模块	成对配置的四端口千兆铜缆以太网非旁路接口 电缆和距离：Cat5E （50 米距离）
光纤 10GBASE 非旁路 MMSR 或 SMLR 网络模块	带 LC 连接器的四端口光纤非旁路接口 线缆和距离： LR 是单模光纤，距离为 5000 米 （可用） SR 是多模光纤 （850 纳米），距离为 550 米 （标准）
光纤 1000BASE-SX 非旁路网络模块	带 LC 连接器的四端口光纤非旁路接口 1000BASE-SX 线缆和距离：SX 是多模光纤 （850 纳米），距离为 550 米 （标准）
电源	设计为用于交流电或直流电的双 650 W 冗余电源。 交流电压：100 VAC 至 240 VAC 额定 （最大：85 VAC 至 264 VAC） 交流电流：在整个范围内最大为 5.2 A （每个电源） 187 VAC 到 264 VAC 的最大值为 2.6 A （每个电源） 交流频率范围：47 Hz 至 63 Hz 直流电压：-48 VDC 额定 （参考 RTN） 最大 -40 VDC 至 -72 VDC 直流电流：最大值 11 A （每个电源）
工作温度	10°C 到 35°C （50°F 到 95°F）

81xx 系列物理和环境参数 （续）

参数	说明
非工作温度	-20°C 至 70°C （-29°F 至 158°F）
工作湿度	5% 至 85%，非冷凝
非工作湿度	5% 至 90%，非冷凝，温度在 25°C 到 35°C （77°F 到 95°F）范围内的最大湿球温度为 28°C
海拔	0 英尺 （海平面）至 6000 英尺 （0 至 1800 米）
冷却要求	1725 BTU/ 小时 您必须提供足够的冷却以使设备运行在其需要的工作温度范围内。不这么做可能导致设备出现故障或损坏。
噪声	最大正常运行噪音是 87.6 dB LWAd （高温） 典型的正常运行噪音是 80 dB LWAd。
工作冲击	2G 半正弦波冲击无错误 （持续 11 毫秒）
空气流动	每分钟 160 平方英尺 （4.5 立方米） 即使环境温度在工作温度范围内，限制空气流动 （例如，阻塞前面或后面，或者将设备放置到没有足够空隙的机柜中）也可能会导致设备过热。 气流从设备前面进入并从背面排出。正面和背面的最小推荐空隙是 7.9 英寸 （20 厘米）。仅当您可确保在设备前面提供低温空气时，才可使用此最小值。

下表介绍 82xx 系列和 83xx 系列设备的物理属性和环境参数。

82xx 系列和 83xx 系列物理和环境参数

参数	说明
外形	2U
尺寸 （深 x 宽 x 高）	29.0 英寸 x 17.2 英寸 x 3.48 英寸 （73.5 厘米 x 43.3 厘米 x 88.2 厘米）
安装后的最大重量：	82xx 系列： 58 磅 （25.3 千克）
	83xx 系列： 67 磅 （30.5 千克）
铜缆 1000BASE-T 可配置旁路网络模块	成对配置的四端口千兆铜缆以太网可配置旁路接口 电缆和距离：Cat5E （50 米距离）

82xx 系列和 83xx 系列物理和环境参数 （续）

参数	说明
光纤 10GBASE MMSR 或 SMLR 可配置旁路网络模块	带 LC 连接器的双端口光纤可配置旁路接口 线缆和距离： LR 是单模光纤，距离为 5000 米 （可用） SR 是多模光纤 （850 纳米），距离为 550 米 （标准）
光纤 1000BASE-SX 可配置旁路网络模块	带 LC 连接器的四端口光纤可配置旁路接口 1000BASE-SX 线缆和距离：SX 是多模光纤 （850 纳米），距离为 550 米 （标准）
光纤 40GBASE-SR4 可配置旁路网络模块	带 OTP/MTP 连接器的双端口光纤可配置旁路接口 线缆和距离： OM3：使用 850 纳米多模光纤时距离为 100 米 OM4：使用 850 纳米多模光纤时距离为 150 米
铜缆 1000BASE-T 非旁路网络模块	成对配置的四端口千兆铜缆以太网非旁路接口 电缆和距离：Cat5E （50 米距离）
光纤 10GBASE 非旁路 MMSR 或 SMLR 网络模块	带 LC 连接器的四端口光纤非旁路接口 线缆和距离： LR 是单模光纤，距离为 5000 米 （可用） SR 是多模光纤 （850 纳米），距离为 550 米 （标准）
光纤 1000BASE-SX 非旁路网络模块	带 LC 连接器的四端口光纤非旁路接口 1000BASE-SX 线缆和距离： SX 是多模光纤 （850 纳米），距离为 550 米 （标准）

82xx 系列和 83xx 系列物理和环境参数 （续）

参数	说明	
电源	82xx 系列：	设计为用于交流电或直流电的双 750 W 冗余电源。 交流电压：100 VAC 至 240 VAC 额定 （最大：85 VAC 至 264 VAC） 交流电流：在整个范围内最大为 8 A （每个电源） 187 VAC 到 264 VAC 的最大值为 4 A （每个电源） 交流频率范围：47 Hz 至 63 Hz 直流电压：-48 VDC 额定 （参考 RTN） 最大 -40 VDC 至 -72 VDC 直流电流：最大值 18 A （每个电源）
	83xx 系列：	设计为用于交流电或直流电的双 1100 W 冗余电源。 交流电压：100 VAC 至 240 VAC 额定 （最大：85 VAC 至 264 VAC） 交流电流：在整个范围内最大为 11 A （每个电源） 187 VAC 到 264 VAC 的最大值为 5.5 A （每个电源） 交流频率范围：47 Hz 至 63 Hz 直流电压：-48 VDC 额定 （参考 RTN） 最大 -40 VDC 至 -72 VDC 直流电流：最大值 25 A （每个电源）
工作温度	10°C 到 35°C （50°F 到 95°F）	
非工作温度	-20°C 至 70°C （-29°F 至 158°F）	
工作湿度	5% 至 85%，非冷凝	
非工作湿度	5% 至 90%，非冷凝，温度在 25°C 到 35°C （77°F 到 95°F）范围内的最大湿球温度为 28°C	
海拔	0 英尺 （海平面）至 6000 英尺 （0 至 1800 米）	
冷却要求	最高 2900 BTU/ 小时 您必须提供足够的冷却以使设备运行在其需要的工作温度范围内。不这么做可能导致设备出现故障或损坏。	

82xx 系列和 83xx 系列物理和环境参数 （续）

参数	说明
噪声	最大正常运行噪音是 81.6 dB LWAd （高温） 典型的正常运行噪音是 81.4 dB LWAd
工作冲击	2G 半正弦波冲击无错误 （持续 11 毫秒）
空气流动	从前到后，每分钟 210 立方英尺 （6 立方米） 即使环境温度在工作温度范围内，限制空气流动 （例如，阻塞前面或后面，或者将设备放置到没有足够空隙的机柜中）也可能会导致设备过热。 气流从设备前面进入并从背面排出。正面和背面的最小推荐空隙是 7.9 英寸 （20 厘米）。仅当您可确保在设备前面提供低温空气时，才可使用此最小值。

8000 系列模块

8000 系列设备的感应接口可以配有铜缆或光纤接口。

警告！ 模块**不可**热插拔。有关详细信息，请参阅第 234 页的插入或拆除 8000 系列模块。

以下模块包含可配置旁路感应接口：

- 四端口 1000BASE-T 铜缆接口 （支持可配置旁路功能）。请参阅第 164 页的四端口 1000BASE-T 铜缆可配置旁路网络模块。
- 四端口 1000BASE-SX 光纤接口 （支持可配置旁路功能）。有关详细信息，请参阅第 165 页的四端口 1000BASE-SX 光纤可配置旁路网络模块。
- 双端口 10GBASE （MMSR 或 SMLR）光纤接口 （支持可配置旁路功能）。有关详细信息，请参阅第 167 页的双端口 10GBASE （MMSR 或 SMLR）光纤可配置旁路网络模块。
- 具有可配置旁路功能的双端口 40GBASE-SR4 光纤接口 （仅适用于 2U 设备）。有关详细信息，请参阅第 169 页的双端口 40GBASE-SR4 光纤可配置旁路网络模块。

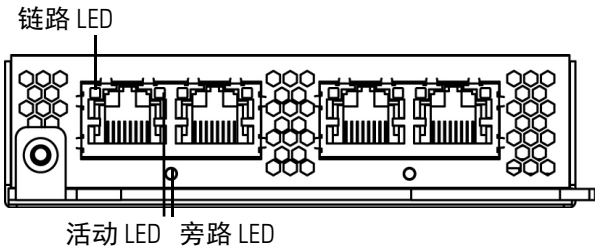
以下模块包含非旁路感应接口：

- 四端口 1000BASE-T 铜缆接口 （不支持旁路功能）。有关详细信息，请参阅第 171 页的四端口 1000BASE-T 铜缆非旁路网络模块。
- 四端口 1000BASE-SX 光纤接口 （不支持旁路功能）。有关详细信息，请参阅第 172 页的四端口 1000BASE-SX 光纤非旁路网络模块。
- 四端口 10GBASE （MMSR 或 SMLR）光纤接口 （不支持旁路功能）。有关详细信息，请参阅第 173 页的四端口 10GBASE （MMSR 或 SMLR）光纤非旁路网络模块。

此外，您还可以使用堆栈模块连接两个 3D8140、至多四个 3D8250，或者至多四个 3D8350 设备，以整合它们的处理能力和提高吞吐量。有关详细信息，请参阅第 175 页的堆栈模块。

四端口 1000BASE-T 铜缆可配置旁路网络模块

四端口 1000BASE-T 铜缆可配置旁路网络模块包含四个铜缆端口以及链路、活动和旁路 LED。



请通过铜缆链路/活动 LED 表了解铜缆接口上的活动和链路 LED。

铜缆链路 / 活动 LED

状态	说明
两个 LED 均熄灭	接口没有链路且不处于旁路模式。
链路指示灯显示琥珀色	接口上的流量速度是 10 Mb 或 100 Mb。
链路指示灯显示绿色	接口上的流量速度是 1 Gb。
绿色活动指示灯闪烁	接口有链路且正在传输流量。

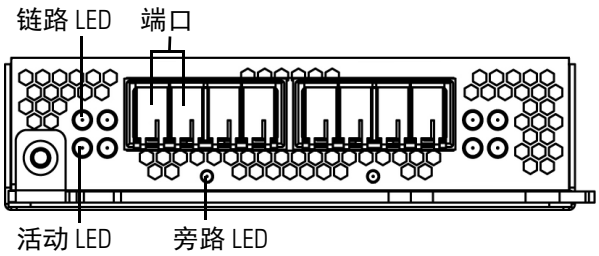
请通过铜缆旁路 LED表了解铜缆接口的旁路 LED。

铜缆旁路 LED

状态	说明
熄灭	接口没有链路且不处于旁路模式。
稳定绿色	接口有链路且正在传输流量。
稳定琥珀色	接口被故意关闭。
琥珀色闪烁	接口处于旁路模式；即无法打开。

四端口 1000BASE-SX 光纤可配置旁路网络模块

四端口 1000BASE-SX 光纤可配置旁路网络模块包含四个光纤端口以及链路、活动和旁路 LED。



请通过光纤链路/活动 LED 表了解光纤接口的链路和活动 LED。

光纤链路 / 活动 LED

状态	说明
顶部	对于内联或被动接口： • 指示灯闪烁指示接口有活动。 • 灯不亮表示没有活动。
底部	对于内联接口： • 指示灯亮指示接口有活动。 • 灯不亮表示没有活动。 对于被动接口：指示灯始终点亮。

请通过光纤旁路 LED表了解光纤接口的旁路 LED。

光纤旁路 LED

状态	说明
熄灭	接口没有链路且不处于旁路模式。
稳定绿色	接口有链路且正在传输流量。
稳定琥珀色	接口被故意关闭。
琥珀色闪烁	接口处于旁路模式；即无法打开。

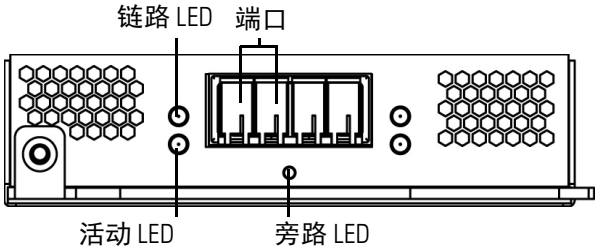
请通过1000BASE-SX 网络模块光学参数表了解光纤接口的光学规格。

1000BASE-SX 网络模块光学参数

参数	1000BASE-SX
光纤连接器	LC 双工
比特率	1000 Mbps
波特率 / 编码 / 容限	1250 Mbps/8b/10b 编码
光纤接口	多模
操作距离	对于 62.5 微米 /125 微米光纤，距离为 200 米 （656 英尺） 对于 50 微米 /125 微米光纤，距离为 500 米 （1640 英尺）
发射器波长	770-860 纳米 （典型值：850 纳米）
最大平均发射功率	0 dBm
最小平均发射功率	-9.5 dBm
接收器最大平均功率	0 dBm
接收器灵敏度	-17 dBm

双端口 10GBASE （MMSR 或 SMLR）光纤可配置旁路网络模块

双端口 10GBASE （MMSR 或 SMLR）光纤可配置旁路网络模块包含两个光纤端口以及链路、活动和旁路 LED。



请通过光纤链路/活动 LED 表了解光纤接口的链路和活动 LED。

光纤链路 / 活动 LED

状态	说明
顶部	对于内联或被动接口： • 指示灯闪烁指示接口有活动。 • 灯不亮表示没有活动。
底部	对于内联接口： • 指示灯亮指示接口有活动。 • 灯不亮表示没有活动。 对于被动接口：指示灯始终点亮。

请通过光纤旁路 LED 表了解光纤接口上的旁路 LED。

光纤旁路 LED

状态	说明
熄灭	接口没有链路且不处于旁路模式。
稳定绿色	接口有链路且正在传输流量。
稳定琥珀色	接口被故意关闭。
琥珀色闪烁	接口处于旁路模式；即无法打开。

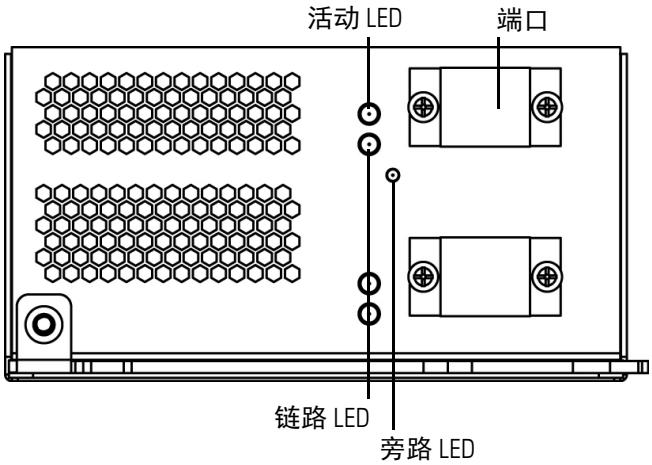
请通过 10GBASE MMSR 和 SMLR 网络模块光学参数表了解光纤接口的光学参数。

10GBASE MMSR 和 SMLR 网络模块光学参数

参数	10GBASE MMSR	10GBASE SMLR
光纤连接器	LC 双工	LC 双工
比特率	10.000 Gbps	10.000 Gbps
波特率 / 编码 / 容限	10.3125 Gbps/ 64/66b 编码 / +/- 100 ppm	10.3125 Gbps/ 64/166b 编码 / +/- 100 ppm
光纤接口	多模	仅单模
操作距离	840 - 860 纳米 （典型值：850 纳米） 对于 62.5 微米 /125 微米光纤，距离为 26 米 （85 英尺）至 33 米 （108 英尺）（模态分别为 BW 160 至 200） 对于 50 微米 /125 微米光纤，距离为 66 米 （216 英尺）至 82 米 （269 英尺）（模态分别为 BW 400 至 500） 对于更高质量的 (OM3) 光纤，距离可达到 300 米（980 英尺）。 最短距离 （全部）： 2 米 （6 英尺）	1270 - 1355 纳米 （典型值：1310 纳米） 对于 9 微米 /125 微米光纤，距离为 2 米到 10 千米 （6 英尺到 6.2 英里）
发射器波长	840 - 860 纳米 （典型值：850 纳米）	1270 - 1355 纳米 （典型值：1310 纳米）
最大平均发射功率	-1 dBm	-0.5 dBm
最小平均发射功率	-7.3 dBm	-8.2 dBm
接收器最大平均功率	-1 dBm	-0.5 dBm
接收器灵敏度	-9.9 dBm	-14.4 dBm

双端口 40GBASE-SR4 光纤可配置旁路网络模块

双端口 40GBASE-SR4 光纤可配置旁路网络模块包含两个光纤端口以及链路、活动和旁路 LED。



您仅可在 3D8270、3D8290、3D8360、3D8370 和 3D8390 中使用 40G 网络模块；或者在具有 40G 功能的 3D8250、3D8260 和 3D8350 中使用该网络模块。如果您尝试在不支持 40G 的设备上创建 40G 接口，在其管理防御中心网络界面上的 40G 接口屏幕将显示红色。支持 40G 的 3D8250 在 LCD 面板上显示“3D 8250-40G”，支持 40G 的 3D8350 在 LCD 面板上显示“3D 8350-40G”。有关位置信息，请参阅第 61 页的8000 系列模块。

请通过光纤链路/活动 LED 表了解光纤接口的链路和活动 LED。

光纤链路 / 活动 LED

状态	说明
顶部 （活动）	当接口有活动时，指示灯闪烁。如果指示灯不亮，表示没有活动。
底部 （链路）	当接口有链路时，指示灯亮。如果指示灯不亮，表示没有链路。

请通过光纤旁路 LED 表了解光纤接口的旁路 LED。

光纤旁路 LED

状态	说明
熄灭	接口对没有链路、不处于旁路模式或未通电。
稳定绿色	接口对有链路且正在传输流量。
稳定琥珀色	接口被故意关闭。
琥珀色闪烁	接口处于旁路模式；即无法打开。

请通过40GBASE-SR4 网络模块光学参数表了解光纤接口的光学参数。

40GBASE-SR4 网络模块光学参数

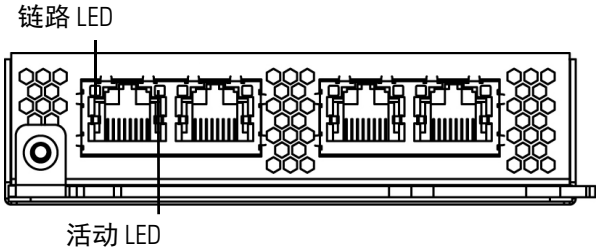
参数	40GBASE-SR4
光纤连接器	OTP/MTP 单行十二个光纤位。仅使用了外部八个光纤。
比特率	40.000 Gbps
波特率 / 编码 / 容限	10.3125 Gbps/ 64/66b 编码 /+/- 100 ppm
光纤接口	多模
操作距离	对于 50 微米 /125 微米光纤 (OM3)，距离为 100 米 （320 英尺） 最小距离：0.5 米 （2 英尺） 40G 光纤数据流量通过使用 MPO 连接器的八条光纤线缆传输。
发射器波长	840-860 纳米 （典型值：850 纳米）
最大平均发射功率	2.4 dBm
最小平均发射功率	-7.8 dBm

40GBASE-SR4 网络模块光学参数 （续）

参数	40GBASE-SR4
接收器最大平均功率	2.4 dBm
接收器灵敏度	-9.5 dBm

四端口 1000BASE-T 铜缆非旁路网络模块

四端口 1000BASE-T 铜缆非旁路网络模块包含四个铜缆端口以及链路和活动 LED。



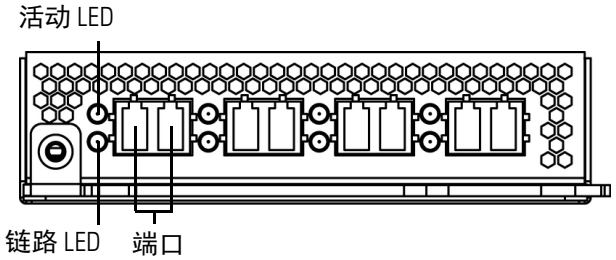
请通过非旁路铜缆链路/活动 LED 表了解铜缆 LED。

非旁路铜缆链路 / 活动 LED

状态	说明
两个 LED 均熄灭	接口没有链路。
链路指示灯显示琥珀色	接口上的流量速度是 10 Mb 或 100 Mb。
链路指示灯显示绿色	接口上的流量速度是 1 Gb。
绿色活动指示灯闪烁	接口有链路且正在传输流量。

四端口 1000BASE-SX 光纤非旁路网络模块

四端口 1000BASE-SX 光纤非旁路网络模块包含四个光纤端口以及链路和活动 LED。



请通过非旁路光纤链路/活动 LED 表了解光纤接口上的链路和活动 LED。

非旁路光纤链路 / 活动 LED

状态	说明
顶部 （活动）	对于内联或被动接口：当接口有活动时，指示灯闪烁。如果指示灯不亮，表示没有活动。
底部 （链路）	对于内联接口：当接口有链路时，指示灯亮。如果指示灯不亮，表示没有链路。 对于被动接口：指示灯始终亮起。

请通过 1000BASE-SX 网络模块光学参数表了解光纤接口的光学参数。

1000BASE-SX 网络模块光学参数

参数	1000BASE-SX
光纤连接器	LC 双工
比特率	1000 Mbps
波特率 / 编码 / 容限	1250 Mbps/8b/10b 编码
光纤接口	多模
操作距离	对于 62.5 微米 /125 微米光纤，距离为 200 米 （656 英尺） 对于 50 微米 /125 微米光纤，距离为 500 米 （1640 英尺）

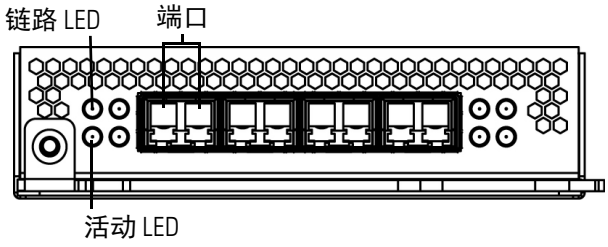
1000BASE-SX 网络模块光学参数 （续）

参数	1000BASE-SX
发射器波长	770-860 纳米 （典型值：850 纳米）
最大平均发射功率	0 dBm
最小平均发射功率	-9.5 dBm
接收器最大平均功率	0 dBm
接收器灵敏度	-17 dBm

四端口 10GBASE （MMSR 或 SMLR）光纤非旁路网络模块

四端口 10GBASE （MMSR 或 SMLR）光纤非旁路网络模块包含四个光纤端口以及链路和活动 LED。

警告！ 四端口 10GBASE 非旁路网络模块包含不可移除的 SFP。尝试移除 SFP 可能损坏该模块。



请通过光纤链路/活动 LED 表了解光纤接口的活动和链路 LED。

光纤链路 / 活动 LED

状态	说明
顶部	对于内联或被动接口：当接口有活动时，指示灯闪烁。如果指示灯不亮，表示没有活动。
底部	对于内联接口：当接口有链路时，指示灯亮。如果指示灯不亮，表示没有链路。 对于被动接口：指示灯始终亮起。

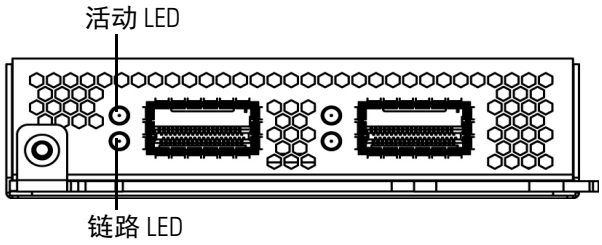
请通过 10GBASE MMSR 和 SMLR 网络模块光学参数表了解光纤接口的光学参数。

10GBASE MMSR 和 SMLR 网络模块光学参数

参数	10GBASE MMSR	10GBASE SMLR
光纤连接器	LC 双工	LC 双工
比特率	10.000 Gbps	10.000 Gbps
波特率 / 编码 / 容限	10.3125 Gbps/ 64/66b 编码 / +/- 100 ppm	10.3125 Gbps/ 64/66b 编码 / +/- 100 ppm
光纤接口	多模	仅单模
操作距离	840 - 860 纳米 （典型值：850 纳米） 对于 62.5 微米 /125 微米光纤，距离为 26 米（85 英尺）至 33 米 （108 英尺）（模态分别为 BW 160 至 200） 对于 50 微米 /125 微米光纤，距离为 66 米（216 英尺）至 82 米 （269 英尺）（模态分别为 BW 400 至 500） 对于更高质量的 (OM3) 光纤，距离可达到 300 米 （980 英尺）。 最短距离 （全部）： 2 米 （6 英尺）	1270 - 1355 纳米 （典型值：1310 纳米） 2 米到 10 千米 （6 英尺到 6.2 英里） 对于 9 微米 /125 微米光纤
发射器波长	840 - 860 纳米 （典型值：850 纳米）	1270 - 1355 纳米 （典型值：1310 纳米）
最大平均发射功率	-1 dBm	-0.5 dBm
最小平均发射功率	-7.3 dBm	-8.2 dBm
接收器最大平均功率	-1 dBm	-0.5 dBm
接收器灵敏度	-9.9 dBm	-14.4 dBm

堆栈模块

堆栈模块包含用于 8000 系列堆栈线缆的两个连接端口，以及活动和链路 LED。



请通过堆栈 LED表了解堆栈 LED。请注意， 3D8140、 3D8250 和 3D8350 提供堆栈模块，并且这些模块包括在 3D8260/3D8270/3D8290 和 3D8360/3D8370/3D8390 中。

堆栈 LED

状态	说明
顶部	指示接口上的活动： • 指示灯闪烁指示接口上有活动。 • 灯不亮表示没有活动。
底部	指示接口是否有链路： • 指示灯亮指示接口有链路。 • 灯不亮表示没有链路。

第 7 章

将 SOURCEFIRE 设备恢复至出厂默认设置

Sourcefire 在其支持站点上提供的 ISO 映像用于将防御中心和受管设备恢复或重新映像为其原始出厂设置。

有关详细信息，请参阅以下各节：

准备工作

开始将设备恢复至出厂默认设置之前，应熟悉系统在恢复过程中的预期行为。

配置和事件备份指南

开始恢复过程之前， Sourcefire 建议删除或移动驻留在设备上的任何备份文件，然后将当前事件和配置数据备份至外部位置。

将设备恢复至出厂默认设置将会使设备丢失几乎**所有**的配置和事件数据。虽然恢复实用程序可保留设备的许可证、网络、控制台和无人值守管理 (LOM) 设置，但在恢复过程完成之后，必须执行所有其他设置任务。

恢复过程中的流量

为避免网络上的流量中断， Sourcefire 建议在维护时段或中断对部署影响最小的时间恢复设备。

恢复以内联方式部署的受管设备会将该设备重置为非旁路 （发生故障时关闭）配置，从而中断网络上的流量。流量将被拦截，直至您在设备上配置支持旁路的内联集。

有关编辑设备配置以配置旁路的详细信息，请参阅*Sourcefire 3D 系统用户指南*中的“管理设备”章节。

了解恢复过程

Sourcefire *设备*为流量感知受管*设备*或管理*防御中心*：每种设备类型有若干*型号*；这些型号进一步分为多个*产品系列*。有关详细信息，请参阅第 11 页的了解设备系列、型号和功能。

恢复设备时要执行的具体步骤取决于设备的型号及您能否实际访问设备，但大体过程是相同的。

重要！ 应当仅在维护时段内重新映像设备。重新映像会将处于旁路模式的设备重置为非旁路配置并中断网络上的流量，直至您重新配置旁路模式。有关详细信息，请参阅第 177 页的恢复过程中的流量。

要恢复 Sourcefire 设备，请执行以下操作：

访问：管理员

1. 确定要恢复的设备 （装置或防御中心）的型号。
2. 从支持站点获取正确的恢复 ISO 映像。
3. 将映像复制至适当的存储介质。

4. 连接至设备。
5. 重新启动设备并调用恢复实用程序。
6. 安装 ISO 映像。

为方便起见，恢复过程中可以在大部分设备上安装系统软件和入侵规则更新。

下表概述了如何恢复不同型号的 Sourcefire 设备。

各类设备型号支持的恢复方法

型号	恢复方法	需要实际访问？	在恢复期间更新？
DC1000 DC3000	使用 Sourcefire 提供的预装有 ISO 映像的 CD-ROM 或创建您自己的 CD。	是，要加载 CD	否
DC500 所有 2 系列设备（除 3D9900）	从 Sourcefire 提供的外部 USB 驱动器启动，使用交互式菜单下载 ISO 映像并将其安装在设备上。	是，要插入 USB 驱动器	是
3D9900 3 系列设备	从设备的内部闪存驱动器启动，使用交互式菜单下载 ISO 映像并将其安装在设备上。	否；远程 KVM 切换器（所有）或 LOM（3 系列）可供您执行远程恢复	是

请注意，**不能**使用设备的网络接口恢复设备。要恢复设备，必须使用以下方式之一连接至该设备：

键盘和显示器/KVM

可将 USB 键盘和 VGA 显示器连接至任何 Sourcefire 设备，这对于连接至 KVM （键盘、视频和鼠标）切换器的机架式安装设备非常有用。如有可远程访问的 KVM，则无需实际访问就可恢复 3 系列设备和 3D9900。

串行连接/笔记本电脑

可使用串行电缆将计算机连接至除 3D2100/2500/3500/4500 设备外的任何 Sourcefire 设备。要与设备交互，请使用终端仿真软件 （例如，HyperTerminal 或 Xmodem）。此软件的设置为 9600 波特、 8 个数据位、无奇偶校验、 1 个停止位和无流量控制。

使用局域网串行连接执行无人值守管理

LOM 功能可供您使用局域网串行 (SOL) 连接在 3 系列设备上执行一组有限的操作。如需将支持 LOM 功能的设备恢复至出厂默认值，但无法实际访问该设备，则可使用 LOM 执行恢复过程。使用 LOM 连接至设备后，就像使用物理串行连接一样向恢复实用程序发出命令。有关详细信息，请参阅第 194 页的设置无人值守管理。

获取恢复 ISO 和更新文件

Sourcefire 提供的 ISO 映像用于将设备恢复至其原始出厂设置。在恢复设备前，请从 Sourcefire 支持站点获取正确的 ISO 映像。

应用于恢复设备的 ISO 映像取决于 Sourcefire 何时引入对该设备型号的支持。ISO 映像通常与系统软件的主要版本 （例如， 5.2 或 5.3）相关联，除非为适应新设备型号发布了次要版本的 ISO 映像。为避免安装系统的不兼容版本，Sourcefire 建议始终使用可用于设备的最新 ISO 映像。

大多数 Sourcefire 设备使用外部 USB 或内部闪存驱动器启动设备，以便您运行恢复实用程序。但是， DC1000 和 DC3000 防御中心需要恢复 ISO CD。如果您有 DC1000 或 DC3000，当您购买设备时， Sourcefire 通过 CD-ROM 向您提供 ISO 映像。如果要将设备恢复至其他版本，可下载相应的 ISO 映像并新建恢复 ISO （非数据） CD，然后可使用其恢复设备。

Sourcefire 还建议始终运行设备支持的系统软件的最新版本。将设备恢复至受支持的最新主要版本之后，应更新其系统软件、入侵规则和漏洞数据库 (VDB)。有关详细信息，请参阅要应用的更新的版本说明，以及 《*Sourcefire 3D 系统用户指南*》中的“更新系统软件”章节。

为方便起见，恢复过程中可以在大部分设备上安装系统软件和入侵规则更新。例如，可将设备恢复至 5.3 版本，并在该恢复过程中将设备更新至 5.3.0.1 版本。请记住，只有防御中心需要规则更新。

请注意，由于您使用 CD 恢复 DC1000 和 DC3000 防御中心，因此，您无法在恢复过程中在这些设备上安装更新。相反，请稍后再更新设备。

要获得恢复 ISO 和其他更新文件，请执行以下操作：

访问：任意

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，然后点击您想安装的系统软件的主版本。

   例如，要下载 V5.3 或 V5.3.1 ISO 映像，可点击 **Downloads > 3D System > 5.3**。
3. 找到要下载的映像 （ISO 映像）。

   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，可点击 **5.3.1 Images** 查看 Sourcefire 3D 系统 V5.3.1 的映像和版本说明。
4. 点击要下载的 ISO 映像。

   文件将开始下载。

5. 或者，下载系统软件和入侵规则更新：
   - 系统软件更新与 ISO 映像在支持站点的同一页面上。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，可点击 **5.3.1** 查看 Sourcefire 3D 系统 V5.3.1 的更新和版本说明。
   - 要下载规则更新，请选择 **Downloads > Rules & VDB > Rules**。最新规则更新位于页面顶部。

   请记住，如在恢复 DC1000 或 DC3000，则在恢复过程完成之后必须安装更新。
6. 准备如何恢复设备？
   - 对于大多数设备 （那些使用 USB 或内部闪存驱动器恢复的设备），请将文件复制至设备在其管理网络上可访问的 HTTP (Web) 服务器、 FTP 服务器或支持 SCP 的主机。
   - 对于 DC1000 和 DC3000，请使用 ISO 映像创建恢复 CD。

警告！ 请**勿**通过邮件传输 ISO 或更新文件；文件可能会损坏。此外，请**勿**更改文件的名称；恢复实用程序要求它们具有与在支持站点上相同的名称。

开始恢复过程

支持的设备：任意
支持的防御中心：除 DC1000 和 DC3000 外的所有型号

对于除 DC1000 和 DC3000 防御中心外的所有设备，请通过从外部 USB 或内部闪存驱动器启动设备开始恢复过程，具体取决于设备型号；请参阅第 178 页的各类设备型号支持的恢复方法表。

确保具有相应级别的设备访问权限、已建立到设备的连接，并获得正确的 ISO 映像之后，请使用以下操作步骤中的一个恢复设备：

- 第 181 页的使用 KVM 或物理串行启动恢复实用程序说明如何对不支持 LOM 的设备或无法使用 LOM 的设备开始恢复过程。可使用此方法恢复除 DC1000 或 DC3000 防御中心外的所有型号。
- 第 182 页的使用无人值守管理启动恢复实用程序说明如何使用 LOM 通过 SOL 连接开始 3 系列设备的恢复过程。
- 第 192 页的使用 CD 恢复 DC1000 或 DC3000说明如何使用 CD 恢复 DC1000 或 DC3000 防御中心。

警告！ 本章中的操作步骤说明如何在不关闭设备电源的情况下恢复设备。但是，如果由于任何原因需要关闭电源，请按照《*Sourcefire 3D 系统用户指南*》中“管理设备”章节中的操作步骤、从 3 系列设备上 CLI 中运行 `system shutdown` 命令，或从设备的外壳 （有时称为专家模式）中运行 `shutdown -h now` 命令。

使用 KVM 或物理串行启动恢复实用程序

支持的设备：任意
支持的防御中心：除 DC1000 和 DC3000 外的所有型号

对于除 DC1000 和 DC3000 防御中心外的所有设备， Sourcefire 均通过外部 USB 或内部闪存驱动器提供恢复实用程序，具体取决于设备型号；请参阅第 178 页的各类设备型号支持的恢复方法表。

提示！如需将 3 系列设备恢复至出厂默认值，但无法实际访问该设备，则可使用 LOM 执行恢复过程。请参阅第 182 页的使用无人值守管理启动恢复实用程序。

要启动恢复实用程序，请执行以下操作：

访问：管理员

1. 如果使用 USB 驱动器恢复 DC500 或除 3D9900 外的任何 2 系列设备，请将 USB 驱动器插入设备上的可用 USB 端口。

   否则，跳至下一步。

2. 以具有管理员权限的帐户身份使用键盘/显示器或串行连接登录设备。密码与设备网络界面的密码相同。

   系统将显示设备提示符。

3. 重新启动设备：
   - 在防御中心或 2 系列受管设备上，键入 `sudo su -`，然后再次键入您的密码。在 root 提示符位置，键入 `reboot` 以重新启动设备。
   - 在 3 系列受管设备上，键入 `system reboot`。

   设备重新启动。在 DC500 防御中心 或 3D500/1000/2000 设备上，出现 Sourcefire 启动屏幕。

4. 监视重新启动状态：
   - 在 DC500 防御中心或 3D500/1000/2000 设备上，在出现启动屏幕时缓慢地重复按 Ctrl + U 键。
   - 对于使用键盘和显示器连接的所有其他设备，系统将显示红色 LILO 启动菜单。快速按其中一个箭头键，防止设备启动当前安装的系统版本。
   - 对于使用串行连接的所有其他设备，看到 BIOS 启动选项时，缓慢地重复按 Tab 键 （防止设备启动当前安装的系统版本）。系统将显示 LILO 启动提示符：

     ```
     LILO 22.8 boot:
     3D-5.3 System_Restore
     ```

5. 指明您要恢复系统：
   - 在 DC500 防御中心 或 3D500/1000/2000 设备上，按 Enter 键。
   - 对于使用键盘和显示器连接的所有其他设备，请使用箭头键选择 `System_Restore`，然后按 Enter 键。
   - 对于使用串行连接的所有其他设备，在提示符处键入 `System_Restore`，然后按 Enter键。

   boot 提示符会在以下选项显示之后显示：

   ```
   0. Load with standard console
   1. Load with serial console
   ```

6. 为恢复实用程序的交互式菜单选择显示模式：
   - 对于键盘和显示器连接，键入 0，然后按 Enter 键。
   - 对于串行连接，键入 1，然后按 Enter 键。

   如未选择显示模式，恢复实用程序在 10 秒之后将默认选择标准控制台。

   除非这是您首次将设备恢复至此主要版本，否则，该实用程序将自动加载您上一次使用的恢复配置。要继续，请确认一系列页面上的设置。

   系统显示恢复实用程序版权声明。

7. 按 Enter 键确认版权声明，然后继续执行第 183 页的使用交互式菜单恢复设备。

使用无人值守管理启动恢复实用程序

支持的设备：3 系列
支持的防御中心：3 系列

如需将 3 系列设备恢复至出厂默认值，但无法实际访问该设备，则可使用 LOM 执行恢复过程。

重要！必须首先启用 LOM 功能，然后才能使用 LOM 恢复设备，请参阅第 194 页的设置无人值守管理。

要使用无人值守管理启动恢复实用程序，请执行以下操作：

访问：管理员

1. 在计算机的命令提示符处，输入 IPMI 命令启动 SOL 会话并显示设备提示：
   - 对于 IPMItool，键入：
     `ipmitool -I lanplus -H` *`IP_address`* `-U` *`username`* `sol activate`
   - 对于 ipmiutil，键入：
     `ipmiutil sol -a -V4 -J3 -N` *`IP_address`* `-U` *`username`* `-P` *password*

   其中 *`Ip_address`* 是设备管理接口的 IP 地址， *`username`* 是授权 LOM 帐户的用户名， *`password`* 是该帐户的密码。请注意， IPMItool 在您发出 `sol activate` 命令后会提示您输入密码。

2. 重新启动设备：
   - 对于防御中心，键入 `sudo su -`，然后再次键入您的密码。在 root 提示符位置，键入 `reboot` 以重新启动设备。
   - 对于 3 系列设备，键入 `system reboot`。

   设备重新启动。
3. 监视重新启动状态。看到 BIOS 启动选项时，缓慢地反复按 Tab 键 （防止设备启动当前安装的系统版本），直至显示 LILO 启动提示符：

   ```
   LILO 22.8 boot:
   3D-5.3 System_Restore
   ```
4. 在 boot 提示符处，键入 `System_Restore` 启动恢复实用程序。

   boot 提示符会在以下选项显示之后显示：

   ```
   0. Load with standard console
   1. Load with serial console
   ```
5. 键入 1，然后按 Enter 键通过设备的串行连接加载交互式恢复菜单。

   重要！ 如未选择显示模式，恢复实用程序在 10 秒之后将默认选择标准控制台。

   除非这是您首次将设备恢复至此主要版本，否则，该实用程序将自动加载您上一次使用的恢复配置。要继续，请确认一系列页面上的设置。

   系统显示恢复实用程序版权声明。
6. 按 Enter 键确认版权声明，然后继续执行第 183 页的使用交互式菜单恢复设备。

使用交互式菜单恢复设备

支持的设备：任意
支持的防御中心：除 DC1000/3000 外的所有型号

大多数 Sourcefire 设备的恢复实用程序均使用交互式菜单引导您完成恢复过程。

提示！ 如在使用 CD 恢复 DC1000 或 DC3000，请跳至第 192 页的使用 CD 恢复 DC1000 或 DC3000。

重要！ 应当仅在维护时段内重新映像设备。重新映像会将处于旁路模式的设备重置为非旁路配置并中断网络上的流量，直至您重新配置旁路模式。有关详细信息，请参阅第 177 页的恢复过程中的流量。

菜单显示下表中列出的选项。

恢复菜单选项

选项	说明	有关详细信息，请参阅 ...
1 IP Configuration	指定有关要恢复的设备上管理接口的网络信息，以便设备可与您存储 ISO 和任何更新文件的服务器进行通信。	第 185 页的识别设备的管理接口
2 Choose the transport protocol	指定将用于恢复设备的 ISO 映像的位置，以及设备下载文件所需的任何凭据。	第 186 页的指定 ISO 映像位置和传输方法
3 Select Patches/Rule Updates	指定设备恢复至 ISO 映像中的基础版本后要应用的系统软件和入侵规则更新。	第 187 页的在恢复期间更新系统软件和入侵规则
4 Download and Mount ISO	下载相应的 ISO 映像以及任何系统软件或入侵规则更新。加载 ISO 映像。	第 188 页的下载 ISO 和更新文件并加载映像
5 Run the Install	调用恢复过程。	第 188 页的调用恢复过程
6 Save Configuration 7 Load Configuration	保存任何恢复配置集供以后使用或加载已保存的恢复配置集。	第 191 页的保存和加载恢复配置
8 Wipe Contents of Disk	安全地擦除硬盘驱动器，确保其内容不再可访问。	第 193 页的擦除硬盘驱动器的内容

使用箭头键在菜单中导航。要选择菜单选项，请使用向上和向下箭头。使用向右和向左箭头键在页面底部的 **OK** 和 **Cancel** 按钮之间切换。

菜单中显示两种不同类型的选项：

- 要选择带编号的选项，首先使用向上和向下箭头键使正确的选项突出显示，然后在页面底部的 **OK** 按钮突出显示时，按 Enter 键。
- 要选择多项选择 （单选按钮）的选项，首先使用向上和向下箭头键使正确的选项突出显示，然后按空格键使该选项标有 x。要接受您的选择，在 **OK** 按钮突出显示时，按 Enter 键。

在大多数情况下，按顺序完成菜单选项 **1**、 **2**、 **4** 和 **5**。或者，添加菜单选项 **3**，在恢复过程中安装系统软件和入侵规则更新。

如在将设备恢复至与设备当前安装的版本不同的一个主要版本，需要执行一个分两轮的恢复过程。第一轮更新操作系统，第二轮安装系统软件的最新版本。

如果这是您的第二轮运行，或者，如果恢复实用程序自动加载了要使用的恢复配置，则可从菜单选项 **4** 开始：第 188 页的下载 ISO 和更新文件并加载映像。但是，Sourcefire 建议先仔细检查恢复配置中的设置，然后再继续。

提示！ 要使用以前保存的配置，从菜单选项 **6** 开始：第 191 页的保存和加载恢复配置。在加载配置后，请跳至菜单选项 **4**：第 188 页的下载 ISO 和更新文件并加载映像。

要使用交互式菜单恢复设备，请执行以下步骤：

1. **1 IP Configuration** — 请参阅第 185 页的识别设备的管理接口。
2. **2 Choose the transport protocol** — 请参阅第 186 页的指定 ISO 映像位置和传输方法。
3. **3 Select Patches/Rule Updates** （可选） —第 187 页的在恢复期间更新系统软件和入侵规则。
4. **4 Download and Mount ISO** — 请参阅第 188 页的下载 ISO 和更新文件并加载映像。
5. **5 Run the Install** — 请参阅第 188 页的调用恢复过程。

识别设备的管理接口

支持的设备：任意
支持的防御中心：除 DC1000/3000 外的所有型号

运行恢复实用程序的第一步是识别要恢复的设备的管理接口，以便设备可与从其复制 ISO 和任何更新文件的服务器进行通信。如在使用 LOM，请记住设备的管理 IP 地址**不是** LOM IP 地址。

要识别设备的管理接口，请执行以下操作：

访问：管理员

1. 从主菜单中，选择 **1 IP Configuration**。

   系统将显示 Pick Device 页面。

2. 选择设备的管理接口 （通常为 **eth0**）。

   系统将显示 IP Configuration 页面。

3. 选择用于管理网络的协议：**IPv4** 或 **IPv6**。

   系统将显示用于为管理接口分配 IP 地址的选项。

4. 选择一种为管理接口分配 IP 地址 的方法：**Static** 或 **DHCP**：
   - 如果选择 **Static**，一系列页面会提示您手动输入管理接口的 IP 地址、网络掩码或前缀长度和默认网关。
   - 如果选择 **DHCP**，设备自动检测管理接口的 IP 地址、网络掩码或前缀长度和默认网关，然后显示 IP 地址。
5. 在显示提示时，请确认您的设置。

   如果系统提示，请确认分配给设备的管理接口的 IP 地址。系统将再次显示主菜单。
6. 继续进行下一小节指定 ISO 映像位置和传输方法。

指定 ISO 映像位置和传输方法

支持的设备：任意
支持的防御中心：除 DC1000/3000 外的所有型号

在配置恢复过程将用于下载其所需文件的管理 IP 地址后，必须识别将用于恢复设备的 ISO 映像。这是从支持站点 （请参阅第 179 页的获取恢复 ISO 和更新文件）下载并存储在网络服务器、 FTP 服务器或支持 SCP 的主机上的 ISO 映像。

交互式菜单提示您输入任何必需信息以完成下载，如下表所列。

下载恢复文件所需的信息

要使用 ...	您必须提供 ...
HTTP	• 网络服务器的 IP 地址 • ISO 映像目录的完整路径 （例如， `/downloads/ISOs/`）
FTP	• FTP 服务器的 IP 地址 • ISO 映像目录的相对路径，相对于您要使用其凭证的用户的主目录（例如， `mydownloads/ISOs/`） • FTP 服务器的授权用户名和密码
SCP	• SCP 服务器的 IP 地址 • SCP 服务器的授权用户名 • ISO 映像目录的完整路径 • 您以前输入的用户名的密码 请注意，在输入密码之前，设备可能会要求您将 SCP 服务器添加至其受信任主机列表。您必须接受才能继续。

请注意，恢复实用程序将在 ISO 映像目录中查找更新文件。

要指定恢复文件的位置和传输方法，请执行以下操作：

访问：管理员

1. 从主菜单中，选择 **2 Choose the transport protocol**。
2. 在显示的页面上，选择 **HTTP**、 **FTP** 或 **SCP**。
3. 使用恢复实用程序显示的一系列页面为您选择的协议提供必需用信息，如第 186 页的下载恢复文件所需的信息表中所述。

   如果您的信息正确，则设备连接至服务器并在您指定的位置显示 Sourcefire ISO 映像列表。
4. 选择要使用的 ISO 映像。
5. 在显示提示时，请确认您的设置。

   系统将再次显示主菜单。
6. 是否要在恢复过程中安装系统软件或入侵规则更新？
   - 如果是，继续下一小节在恢复期间更新系统软件和入侵规则。
   - 如果否，请继续执行第 188 页的下载 ISO 和更新文件并加载映像。请注意，在恢复过程完成之后，可使用系统的网络界面手动安装更新。

在恢复期间更新系统软件和入侵规则

支持的设备：任意
支持的防御中心：除 DC1000/3000 外的所有型号

或者，在设备已恢复至 ISO 映像中基础版本后，可使用恢复实用程序更新系统软件和入侵规则。请注意，仅防御中心需要规则更新。

恢复实用程序只能使用一个系统软件更新以及一个规则更新。然而，系统更新将向后累积至上一个主要版本；规则更新也将累积。 Sourcefire 建议获取可用于您设备的最新可用更新；请参阅第 179 页的获取恢复 ISO 和更新文件。

如果选择在恢复过程中不更新设备，则可稍后使用系统的网络界面进行更新。有关详细信息，请参阅要安装的更新的版本说明，以及 《*Sourcefire 3D 系统用户指南*》中的“更新系统软件”章节。

要在恢复过程中安装更新，请执行以下操作：

访问：管理员

1. 从主菜单中，选择 **3 Select Patches/Rule Updates**。

   恢复实用程序使用您在上一操作步骤中指定的协议和位置 （请参阅第 186 页的指定 ISO 映像位置和传输方法）来检索并显示该位置的任何系统软件更新文件的列表。如在使用 SCP，请在系统提示时输入密码以显示更新文件列表。

2. 选择要使用的系统软件更新 （如有）。

   您并非必须选择更新；按 Enter 键，即可不选择更新并继续。如果相应位置无系统软件更新，系统会提示您按 Enter 键以继续。

   恢复实用程序检索并显示规则更新文件的列表。如在使用 SCP，请在系统提示时输入密码以显示列表。

3. 选择要使用的规则更新 （如有）。

   您并非必须选择更新；按 Enter 键，即可不选择更新并继续。如果相应位置无规则更新，系统会提示您按 Enter 键以继续。

   系统将保存您的选择，并且再次显示主菜单。

4. 继续进行下一小节下载 ISO 和更新文件并加载映像。

下载 ISO 和更新文件并加载映像

支持的设备：任意
支持的防御中心：除 DC1000 和 DC3000 外的所有型号

调用恢复过程之前的最后一步是下载必需的文件和加载 ISO 映像。

提示！ 开始此步骤之前，您可能想要保存恢复配置以供将来使用。有关详细信息，请参阅第 191 页的保存和加载恢复配置。

要下载并加载 ISO 映像，请执行以下操作：

访问：管理员

1. 从主菜单中，选择 **4 Download and Mount ISO**。
2. 在系统提示时，请确认您的选择。如在从 SCP 服务器下载，请在系统提示时输入密码。

   系统将下载并加载相应的文件。系统将再次显示主菜单。

3. 继续进行下一小节调用恢复过程。

调用恢复过程

支持的设备：任意
支持的防御中心：除 DC1000 和 DC3000 外的所有型号

在下载并加载 ISO 映像后，即可调用恢复过程。如在将设备恢复至与设备当前安装的版本不同的一个主要版本，需要执行一个分两轮的恢复过程。第一轮更新操作系统，第二轮安装系统软件的最新版本。

两轮中的第一轮 （仅更改主要版本）

在将设备恢复至另一主要版本时，恢复实用程序运行的第一轮更新设备的操作系统，并在必要时更新恢复实用程序本身。

重要！ 如在将设备恢复至同一主要版本，或者，如果这是您的第二轮运行，请跳至下一操作步骤：第 190 页的第二轮或仅有的一轮。

要执行两轮恢复过程的第一轮，请执行以下操作：

访问：管理员

1. 从主菜单中，选择 **5 Run the Install**。
2. 当系统提示时 （两次），请确认您要重新启动设备。

   重要！ 对于使用外部 USB 驱动器恢复的设备，如果该驱动器的恢复实用程序与系统的另一版本相关联，则只有更新该驱动器上的实用程序才能继续。在系统提示时，键入 `yes` 更新实用程序 （并删除任何保存的恢复配置）。然后，确认要从已更新的驱动器重新启动。如不更新 USB 驱动器，设备重新启动。无法使用该驱动器恢复设备。

3. 监视重新启动并再次调用恢复过程：
   - 对于键盘和显示器连接，系统将显示红色 LILO 启动菜单。快速按其中一个箭头键，防止设备启动当前安装的系统版本。
   - 对于串行或 SOL/LOM 连接，当您看到 BIOS 启动选项时，缓慢地重复按 Tab 键，直至显示 LILO 启动提示符：

     ```
     LILO 22.8 boot:
     3D-5.3 System_Restore
     ```

4. 指明您要恢复系统：
   - 对于键盘和显示器连接，请使用箭头键选择 `System_Restore`，然后按 Enter 键。
   - 对于串行或 SOL/LOM 连接，请在提示符处键入 `System_Restore` 并按 Enter 键。

   在任一种情况下，在选择以下选项后，均将显示 `boot` 提示符：

   ```
   0. Load with standard console
   1. Load with serial console
   ```

5. 为恢复实用程序的交互式菜单选择显示模式：
   - 对于键盘和显示器连接，键入 0，然后按 Enter 键。
   - 对于串行或 SOL/LOM 连接，键入 1，然后按 Enter 键。

   如未选择显示模式，恢复实用程序在 10 秒之后将默认选择标准控制台。

   除非这是您首次将设备恢复至此主要版本，否则，该实用程序将自动加载您上一次使用的恢复配置。要继续，请确认一系列页面上的设置。

   系统显示恢复实用程序版权声明。
6. 按 Enter 键确认版权声明，然后开始过程的第二轮，从第 183 页的使用交互式菜单恢复设备开始。

第二轮或仅有的一轮

遵循以下操作步骤执行第二轮或仅有的一轮完成恢复过程。

要执行第二轮或仅有的一轮完成恢复过程，请执行以下操作：

访问：管理员

1. 从主菜单中，选择 **5 Run the Install**。
2. 确认要恢复设备并继续下一步。
3. 选择是否想要删除设备的许可证和网络设置。删除这些设置也将重置显示（控制台）设置和 LOM （对于 3 系列设备）。

   在大多数情况下，您不想删除这些设置，因为它们可缩短初始设置过程。在恢复和后续的初始设置后，更改设置通常比现在重置所花的时间要短。有关详细信息，请参阅第 193 页的后续步骤。
4. 如在使用 USB 驱动器恢复设备，当恢复实用程序提示您键入要恢复设备的最终确认时，请移除该驱动器。
5. 键入要恢复设备的最终确认。

   恢复过程的最后阶段开始。在完成时，如果系统提示，确认您要重新启动设备。

警告！ 确保为完成恢复过程完成预留充足的时间。在带有内部闪存驱动器的设备上，该实用程序首先更新闪存驱动器，然后将其用于执行其他恢复任务。如果您在闪存更新期间退出 （例如，通过按 Ctrl+C），则可能导致不可恢复的错误。如果您认为恢复所花的时间过长或在恢复过程中遇到任何其他问题，请**不要**退出，而应联系支持部门。

重要！ 重新映像会将处于旁路模式的设备重置为非旁路配置并中断网络上的流量，直至您重新配置旁路模式。有关详细信息，请参阅第 177 页的恢复过程中的流量。

6. 继续执行第 193 页的后续步骤。

保存和加载恢复配置

支持的设备：任意
支持的防御中心：除 DC1000 和 DC3000 外的所有型号

对于大多数设备，均可使用恢复实用程序保存恢复配置以供需要再次恢复设备时使用。虽然恢复实用程序将自动保存最后使用的配置，但仍可保存多种配置，包括：

- 有关设备上管理接口的网络信息；请参阅第 185 页的识别设备的管理接口
- 恢复 ISO 映像的位置，以及传输协议和设备下载文件时所需的任何凭据；请参阅第 186 页的指定 ISO 映像位置和传输方法
- 在设备恢复至 ISO 映像中基础版本后要应用的系统软件和入侵规则更新 （如有）；请参阅第 187 页的在恢复期间更新系统软件和入侵规则

未保存 SCP 密码。如果配置指定实用程序必须使用 SCP 将 ISO 和其他文件传输至设备，则必须重新对服务器进行身份验证以完成恢复过程。

保存恢复配置的最佳时间是：在提供以上列出的信息之后，但在下载并加载 ISO 映像之前。请注意，如果更新恢复 USB 驱动器以与系统的另一个主要版本兼容，则任何已保存恢复配置均将丢失。

要保存恢复配置，请执行以下操作：

访问：管理员

1. 从恢复实用程序的主菜单中，选择 **6 Save Configuration**。

   实用程序将显示您在保存的配置中的设置。
2. 当系统提示时，请确认您要保存配置。
3. 当系统提示时，请输入配置的名称。

   系统将保存您的配置，并再次显示主菜单。
4. 如要使用您刚保存的配置恢复设备，请继续执行第 188 页的下载 ISO 和更新文件并加载映像。

要加载已保存的恢复配置，请执行以下操作：

访问：管理员

1. 从主菜单中，选择 **7 Load Configuration**。

   实用程序将显示已保存恢复配置列表。第一个选项 **default_config** 是您上次用于恢复设备的配置。其他选项是您已保存的恢复配置。
2. 选择要使用的配置。

   实用程序将显示您正在加载的配置中的设置。
3. 系统提示时，请确认您要加载配置。

   系统将加载配置。如果系统提示，请确认分配给设备的管理接口的 IP 地址。系统将再次显示主菜单。
4. 要使用刚刚加载的配置还原设备，请继续执行第 188 页的下载 ISO 和更新文件并加载映像。

使用 CD 恢复 DC1000 或 DC3000

支持的设备：无
支持的防御中心：DC1000 和 DC3000

对于具有 CD-ROM 驱动器的 DC1000 和 DC3000 防御中心， Sourcefire 在您购买设备时提供恢复 CD。如果想要将设备恢复至另一个版本，可下载相应的 ISO 映像并新建恢复 ISO （非数据） CD，然后可使用其恢复系统；请参阅第 179 页的获取恢复 ISO 和更新文件。

请注意，由于您正在使用 CD 恢复这些防御中心，您无法在恢复过程中在这些设备上安装更新。相反，请稍后再更新设备。

要使用 CD 恢复 DC1000 或 DC3000，请执行以下操作：

访问：管理员

1. 将恢复 CD 插入防御中心的 CD 托盘。

   如果设备已关闭，请为设备接通电源以打开托盘。

2. 借助于键盘/显示器或串行连接，使用具有管理员权限的帐户登录防御中心。密码与防御中心的网络界面的密码相同。

   系统将显示防御中心的提示符。

3. 在提示符位置，访问 root 权限：键入 `sudo su -`，按 Enter 键，然后提供密码。

4. 在 `root` 提示符位置，键入 `reboot` 重新启动防御中心。

   防御中心 从 CD 启动。此操作可能需要几分钟。

5. 当系统提示时，请确认您要恢复防御中心。

6. 选择是否想要删除设备的许可证和网络设置。删除这些设置将重置显示 （控制台）设置。

   在大多数情况下，您不想删除这些设置，因为它们可缩短初始设置过程。在恢复和后续的初始设置后，更改设置通常比现在重置所花的时间要短。有关详细信息，请参阅第 193 页的后续步骤。

7. 键入要恢复设备的最终确认。

   恢复过程开始并在屏幕上显示其进度。

警告！ 确保为完成恢复过程完成预留充足的时间。在极少数情况下，如果您退出 （例如，通过按 Ctrl+C 或关闭设备电源），可能导致不可恢复的错误。如果您认为恢复所花的时间过长或在恢复过程中遇到任何其他问题，请**不要**退出，而应联系支持部门。

8. 系统提示时，按 Enter 键继续。

   防御中心弹出 CD。取出 CD 并关闭托架。

9. 当系统再次提示时，按 Enter 键确认恢复完成并且您要重新启动设备。

   设备重新启动。

10. 继续执行后续步骤。

后续步骤

将设备恢复至出厂默认设置将导致丢失设备上的几乎**所有**配置和事件数据，包括以内联方式部署的设备的旁路配置。有关详细信息，请参阅第 177 页的恢复过程中的流量。

在恢复设备后，必须完成初始设置过程：

- 如未删除设备的许可证和网络设置，可使用管理网络上的计算机直接浏览至设备的网络界面以执行设置。有关详细信息，请参阅第 84 页的初始设置页面：设备和第 89 页的初始设置页面：防御中心。
- 如已删除许可证和网络设置，则必须像对新设备一样配置该设备，首先将其配置为在管理网络上进行通信。请参阅下一章：第 77 页的设置Sourcefire 3D 系统设备。

请注意，删除许可证和网络设置也将重置显示 （控制台）设置和 LOM 设置 （对于 3 系列设备）。在完成初始设置过程后：

- 如要使用串行或 SOL/LOM 连接访问设备的控制台，则应重定向控制台输出；请参阅第 74 页的重定向控制台输出。
- 如要使用 LOM，则必须重新启用该功能并至少启用一个 LOM 用户；请参阅第 195 页的启用 LOM 和 LOM 用户。

擦除硬盘驱动器的内容

支持的设备：任意
支持的防御中心：除 DC1000 和 DC3000 外的所有型号

可安全地擦除大多数 Sourcefire 设备上的硬盘驱动器，以确保其内容不再可访问。例如，如果需要退回包含敏感数据的有缺陷设备，可使用此功能覆盖数据。

此磁盘擦除模式符合下列美国军用标准：

标准

DoD 擦除序列符合 DoD 5220.22-M 程序，该程序用于擦除可移动和不可移动硬盘，要求使用一个字符、其补码和随机字符覆盖所有可寻址地址，然后进行验证。请参阅 DoD 文档了解其他限制。

警告！擦除硬盘驱动器将导致丢失设备上的**所有**数据，从而使设备无法运行。

要擦除硬盘驱动器，请执行以下操作：

访问：管理员

1. 按照以下其中一个小节中的说明显示恢复实用程序的交互式菜单，具体取决于您如何访问设备：
   - 第 181 页的使用 KVM 或物理串行启动恢复实用程序
   - 第 182 页的使用无人值守管理启动恢复实用程序

   请注意， DC1000 和 DC3000 不支持此功能。
2. 从主菜单中，选择 **8 Wipe Contents of Disk**。
3. 当系统提示时，请确认您要擦除硬盘驱动器。

   系统将擦除硬盘驱动器。擦除过程可能需要几个小时才能完成；驱动器越大，需要的时间越长。

设置无人值守管理

支持的设备：3 系列
支持的防御中心：3 系列

如需将 3 系列设备恢复至出厂默认值，但无法实际访问该设备，则可使用无人值守 (LOM) 执行恢复过程。**不能**使用 LOM 还原 2 系列设备。仅 3 系列设备支持 LOM。

LOM 功能可供您使用局域网串行 (SOL) 连接 在 3 系列防御中心或受管设备上执行一组有限的操作。借助于 LOM，可使用带外管理连接上的命令行界面执行诸如查看机箱序列号或监控运行状况 （如风扇速度和温度）之类的任务。

LOM 命令语法取决于您在使用的实用程序，但 LOM 命令通常包含下表列出的元素。

LOM 命令语法

IPMITOOL (LINUX/MAC)	IPMIUTIL (WINDOWS)	说明
`ipmitool`	`ipmiutil`	调用 IPMI 实用程序。
不适用	`-V4`	仅适用于 ipmiutil，为 LOM 会话启用管理员权限。
`-I lanplus`	`-J3`	为 LOM 会话启用加密。
`-H` *`IP_address`*	`-N` *`IP_address`*	指定设备上管理接口的 IP 地址。
`-U` *`username`*	`-U` *`username`*	指定授权 LOM 帐户的用户名。

LOM 命令语法 （续）

IPMItool (Linux/Mac)	IPMIutil (Windows)	说明
n/a (prompted on login)	-P *password*	仅适用于 ipmiutil，指定授权 LOM 帐户的密码。
command	*command*	要向设备发出的命令。请注意，您发出命令的时机取决于实用程序： • 对于 IPMItool，最后键入命令。 • 对于 ipmiutil，首先键入命令。

因此，对于 IPMItool：

```
ipmitool -I lanplus -H IP_address -U username command
```

或者，对于 ipmiutil：

```
ipmiutil command -V4 -J3 -N IP_address -U username -P
password
```

有关 Sourcefire 3D 系统支持的 LOM 命令的完整列表，请参阅《*Sourcefire 3D 系统用户指南*》中的“配置设备设置”章节。

重要！必须首先在连接至设备管理接口的任何第三方交换设备上禁用生成树协议 (STP)，然后才能使用 SOL 连接至 7000 系列设备。

必须首先同时为将执行恢复操作的设备和用户启用 LOM，才能使用 LOM 恢复设备。然后，使用第三方智能平台管理接口 (IPMI) 实用程序访问设备。还必须确保将设备的控制台输出重定向至串行端口。

有关详细信息，请参阅以下各节：

- 第 195 页的启用 LOM 和 LOM 用户
- 第 197 页的安装 IPMI 实用程序
- 第 74 页的重定向控制台输出

启用 LOM 和 LOM 用户

支持的设备：3 系列
支持的防御中心：3 系列

必须首先启用并配置 LOM 功能，然后才能使用 LOM 恢复设备。也必须向将使用 LOM 功能的用户明确授予对此功能的权限。

使用每台设备的本地网络界面逐一为每台设备配置 LOM 和 LOM 用户。也就是说，不能使用防御中心配置受管设备上的 LOM。类似地，因为独立于每台设备管理用户，在防御中心上启用或创建支持 LOM 功能的用户不将该功能转移给受管设备的用户。

LOM 用户还受到以下限制：

- 必须向该用户分配管理员角色。
- 用户名最多可包含 16 个字母数字字符。不支持对 LOM 用户使用连字符和更长的用户名。
- 密码最多可包含 20 个字母数字字符。不支持对 LOM 用户使用更长的密码。用户的 LOM 密码与其系统密码相同。
- 3 系列防御中心和 8000 系列设备最多可以有 13 个 LOM 用户。7000 系列设备最多可以有 8 个 LOM 用户。

提示！ 有关以下任务的详细说明，请参阅 《*Sourcefire 3D 系统用户指南*》中的“配置设备设置”章节。

要启用 LOM，请执行以下操作：

访问：管理员

1. 选择 **System > Local > Configuration**，然后点击 **Console Configuration**。
2. 下一步取决于设备型号：
   - 要在防御中心和 8000 系列设备上启用 LOM，请使用 **Physical Serial Port** 启用远程访问，然后才能指定 LOM IP 地址、网络掩码和默认网关 （或使用 DHCP 自动分配这些值）。
   - 在 7000 系列设备上，选择 **Lights Out Management** 配置 LOM 设置。7000 系列设备不支持同时进行 LOM 和物理串行访问。

重要！ LOM IP 地址必须不同于设备的管理接口 IP 地址。

要为 Sourcefire 3D 系统用户启用 LOM 功能，请执行以下操作：

访问：管理员

1. 选择 **System > Local > User Management**，然后编辑现有用户以添加 LOM 权限，或创建将用于通过 LOM 访问设备的新用户。
2. 在 User Configuration 页面上，如果尚未启用 **Administrator** 角色，请启用该角色。
3. 启用 **Allow Lights-Out Management Access** 复选框并保存更改。

安装 IPMI 实用程序

可使用计算机上的第三方 IPMI 实用程序创建到设备的 SOL 连接。

如果计算机运行 Linux 或 Mac OS，请使用 IPMItool。虽然 IPMItool 是许多 Linux 版本的标准配置，但在 Mac 上必须安装 IPMItool。首先，请确认您的 MAC 安装了 Apple 的 xCode 开发工具包。此外，请确保已安装命令行开发的可选组件 （较新版本中的“UNIX Development”和“System Tools”或较早版本中的“Command Line Support”）。最后，请安装 MacPorts 和 IPMItool。有关详细信息，请使用您常用的搜索引擎进行搜索或查看以下网址：

https://developer.apple.com/technologies/tools/

http://www.macports.org/

对于 Windows 环境，请使用 ipmiutil （必须自己编译该程序）。如果您无法访问编译器，则可使用 ipmiutil 自身来编译。有关详细信息，请使用您常用的搜索引擎进行搜索或查看此网址：

http://ipmiutil.sourceforge.net/

第 8 章
安全和认证信息

Sourcefire 设备在多个硬件平台上提供。一般安全准则适用于所有设备。在与每种设备相对应的小节中描述了每种设备的监管信息。请在安装设备前阅读以下各节，并在使用设备时遵守所有准则。

Sourcefire 强烈建议您遵循行业一般安全和电磁辐射准则。以下各小节包含更多信息：

一般安全准则

请遵循这些规则以确保一般安全：

1. 在维护期间及之后，保持设备所在区域的清洁。
2. 始终保持机箱区域无灰尘。
3. 当提起任何重物时：
   - 提起机箱可能需要两个人。
   - 确保您已站稳，脚下不会打滑。
   - 在您的双脚之间均等地分配物品的重量。

- 缓慢提拉。在尝试提起机箱时，请勿突然移动或扭转身体。
- 通过站立或使用腿部肌肉力量提起机箱；此动作会减轻背部的压力。请勿尝试提起超过 16 千克 （35 磅）的重物或您认为对您而言过重的物品。

4. 不要执行将导致危险或使设备不安全的任何操作。
5. 启动计算机之前，请确保其他服务代表和客户的人员不在危险位置。
6. 维修机器时，请将取下的盖板和其他部件放在安全位置，远离所有人员。
7. 将您的工具箱放到远离走动区域的地方，以防止其他人被其绊倒。
8. 请勿穿着任何可能被机器活动部件挂到的宽松服装。确保您的袖子已束紧或卷到手肘以上。如果您的头发较长，请扎紧头发。
9. 将领带或围巾末端插入衣服内部或使用不导电夹子固定 （距离末端约 8 厘米（3 英寸））。
10. 设备在连接到交流电源插座后必须适当接地。
11. 请勿佩戴首饰、项链、金属框眼镜或服装上的金属纽扣。

警告！请记住：金属物体是良好电导体。

12. 为避免触电，请勿在没有正确指导的情况下打开或移除机箱盖或金属部件。
13. 执行以下任务时务必戴上护目镜：锤打、钻孔、焊接、剪切电线，加装弹簧、使用溶剂或在任何其他可能伤害眼睛的环境中工作时。
14. 必须在机箱各节保留足够空隙，保持冷却空气进气口和排气口，以及方便接近网络接口模块 （不小于 2 英寸）。
15. 在使用设备前，拆除所有出厂包装。
16. 请勿覆盖或堵塞通风口，或者围住设备。

安全警告声明

在安装本产品之前，请阅读本小节中的安全信息。

声明 1

危险！电线、电话线和通信电缆中的电流可能造成危险。

要避免电击危险：

- 在雷暴天气中，请不要连接或断开任何电缆也不要执行此产品的安装、维护或重新配置。
- 将所有电源线连接至正确接线和接地的电源插座。
- 将要连接至此产品的任何设备连接至正确接线的电源插座。

- 如果可能，请仅使用一只手连接或断开信号电缆。
- 当发现火、水导致损坏或者结构损伤迹象时，不要启动任何设备。
- 在打开设备盖板前，请断开连接的电源线、电信系统、网络和调制解调器，除非安装和配置程序中另有说明。
- 当安装、移动或打开本产品或所连接设备的护盖时，请按照下表中所述连接和断开电缆。

要连接：

1. 关闭所有设备。
2. 将所有电缆连接至设备。
3. 将信号电缆连接至连接器。
4. 将电源线插入插座。
5. 开启设备。

要断开连接：

1. 关闭所有设备。
2. 从插座中拔出电源线。
3. 从连接器中拔出信号电缆。
4. 从设备上移除所有电缆。

声明 2

注意！ 在更换锂电池时，请仅使用制造商推荐的同等类型电池。如果您的系统具有包含锂电池的模块，只能使用同一制造商生产的同一种模块类型替换它。电池含锂，如果不当使用、处理或处置可能发生爆炸。

请勿：

- 投入或浸没在水中。
- 加热至超过 100° C (212° F)。
- 维修或拆卸。

根据当地法令或法规要求处理电池。

声明 3

注意！ 安装激光产品 （例如， CD-ROM、 DVD 驱动器、光纤设备或发射器）时，请注意以下事项：

- 请勿取下盖板。取下激光产品的盖板可能导致受到危险的激光辐射。设备内部没有可维修部件。
- 使用除此处指定外的其他控制步骤、调整步骤或执行步骤可能导致危险的辐射暴露。

危险！ 一些激光产品包含嵌入式 3A 类或 3B 类激光二极管。请注意以下提示。打开时有激光辐射。请勿直视射束，请勿直接通过光学仪器查看，并避免直接面对射束。

声明 4

注意！ 抬举设备时，请使用安全做法。

声明 5

注意！ 设备上的电源控制按钮以及电源上的电源开关不会切断提供给设备的电流。设备可能有多条电源线。要将设备彻底断电，请确保所有电源线都已与电源断开连接。

声明 6

注意！ 请勿取下电源或任何部件上粘贴有以下标签的盖板。

粘贴有此标签的所有组件内有危险电压、电流和能量水平。这些组件内部没有可维修部件。如果您怀疑这些部件之一有问题，请与维修技术人员联系。

声明 7

注意！ 以下标签指示附近有热表面。

声明 8

危险！ 在某些情况下,过载支路可能引起火灾和电击危险。为了避免这些危险，请确保系统电气要求不超过支路保护要求。

声明 9

注意！ 可能存在危险电压、电流和能量水平。只有合格的维修技术人员才有权卸下贴有以下标签的盖板。

声明 10

注意！ 请确保机架得到适当固定以避免在扩展服务器设备时翻倒。

声明 11

注意！ 某些附件或选件板输出超过 2 类或有限电源限制，必须使用符合国家电气规范的合适互连电缆来安装。

声明 12

注意！ 以下标签指明附近有活动部件。

警告！ 处理此产品的线缆或随此产品销售的相关附件的线缆时，您将接触到铅，此化学元素在加利福尼亚州已知会导致癌症和先天缺陷或其他生殖机能损害。接触后应洗手。

声明 13

警告！ 以下标签指明此产品包括危险活动部件。请远离正在转动的风扇叶片。

监管信息

在与每种设备相对应的小节中描述了每种设备的监管信息：

- 第 202 页的Sourcefire防御中心 750、 1500 和 3500 信息
- 第 204 页的Sourcefire 3D500 信息
- 第 205 页的Sourcefire 3 系列信息

Sourcefire防御中心 750、 1500 和 3500 信息

本产品符合以下安全标准和认证：

安全标准

以下信息适用于 DC750、 DC1500 和 DC3500：

- UL60950 - CSA 60950 （美国/加拿大）
- EN60950 （欧洲）
- IEC60950 （国际）
- CB 证书和报告， IEC60950 （包括所有国家/地区差异的报告）
- GS 许可证 （德国）

- GOST R 50377-92 - 许可证 （俄罗斯）
- 白俄罗斯许可证 （白俄罗斯）
- 乌克兰许可证 （乌克兰）
- CE - 低电压指令 73/23/EEE （欧洲）
- IRAM 认证 （阿根廷）
- GB4943 - CNCA 认证 （中国）
- FCC （A 类验证） - 辐射放射性和传导放射性 （美国）
- CISPR 22 - 放射性 （国际）
- EN55022 - 放射性 （欧洲）
- EN55024 - 抗扰性 （欧洲）
- EN61000-3-2 - 谐波电流 （欧洲）
- EN61000-3-3 - 电压闪烁 （欧洲）
- CE - EMC 指令 89/336/EEC （欧洲）
- VCCI 放射性 （日本）
- AS/NZS 3548 放射性 （澳大利亚/新西兰）
- BSMI CNS13438 放射性 （中国台湾）
- GOST R 29216-91 放射性 （俄罗斯）
- GOST R 50628-95 放射性 （俄罗斯）
- 白俄罗斯许可证 （白俄罗斯）
- 乌克兰许可证 （乌克兰）
- RRL MIC 公告编号 1997-41 (EMC) & 1997-42 (EMI) （韩国）
- GB 9254 - CNCA 认证 （中国）
- GB 17625 - （谐波电流） CNCA 认证 （中国）

认证/注册/声明

以下信息适用于 DC750/1500/3500：

- UL 认证 （美国/加拿大）
- CE 符合性声明 （CENELEC 欧洲）
- FCC/ICES-003 A 类证明 （美国/加拿大）
- VCCI 认证 （日本）
- C-Tick 符合性声明
- MED 符合性声明 （新西兰）
- BSMI 认证 （中国台湾）

- GOST R 认证/许可证 （俄罗斯）
- 白俄罗斯认证/许可证 （白俄罗斯）
- RRL 认证 （韩国）
- IRAM 认证 （阿根廷）
- CNCA 认证 （中国）
- 生态声明 （国际）

Sourcefire 3D500 信息

此设备符合以下电磁兼容性 (EMC) 法规：

美国联邦通信委员会 (FCC) 声明

注意：根据 FCC 规则的第 15 部分，经测试证明该设备符合对 A 类数字装置的限制。

这些限制旨在用于提供合理保护，使设备在商业环境下运行时免于有害干扰。该设备产生、使用且可能辐射射频能量；如未按照说明手册予以安装和使用，则会对无线电通信造成有害干扰。如在住宅区运行该设备，则有可能造成有害干扰，在这种情况下，用户必须自付费用纠正此类干扰。

必须使用正确屏蔽且接地的电缆和连接器以满足 FCC 排放限制。 Sourcefire 不对任何因使用其他非推荐电缆和连接器或对设备的未经授权的更改或修改导致的任何无线电或电视干扰负责。未经授权改装此设备，可能会撤销用户操作此设备的授权。

此设备符合 FCC 规则第 15 部分的规定。操作满足以下两个条件：

- 该设备不会造成有害干扰。
- 该设备必须接受任何收到的干扰，包括可能会造成不需要操作的干扰。

加拿大工业部 A 类辐射合规性声明

该 A 类数字设备符合加拿大 ICES-003 标准。

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

澳大利亚和新西兰 A 类声明

注意：本产品是 A 类产品。在生活环境中，此产品可能会造成无线电干扰，用户可能需要采取适当措施。

英国电信安全要求

致客户的通告：此设备已在批准文号 NS/G/1234/J/100003 下获得批准，可在英国用于间接连接到公共电信系统。

欧盟 EMC 指令符合性声明

此产品符合欧洲理事会指令 EMC 2004/108/EC 的保护要求。

此产品已经过测试证实符合 A 类信息技术设备的限制 （根据 CISPR 22/欧洲标准 EN 55022）。 A 类设备的限制源自为商业和工业环境提供对许可通信设备造成干扰的合理保护。

注意：本产品是 A 类产品。在生活环境中，此产品可能会造成无线电干扰，用户可能需要采取适当措施。

Sourcefire 3 系列信息

以下小节按系列、子系列和机箱硬件代码列出了 3 系列设备。机箱代码显示在机箱外部的监管标签上，该代码是硬件认证和安全的正式参考代码。

3 系列设备子系列

系列	子系列	设备
7000 系列	70xx 系列	3D7010 3D7020 3D7030
7000 系列	71xx 系列	3D7110 3D7115 3D7120 3D7125 AMP7150
8000 系列	81xx 系列	3D8120 3D8130 3D8140 AMP8150

3 系列设备子系列

系列	子系列	设备
8000 系列	82xx 系列	3D8250 3D8260 3D8270 3D8290
8000 系列	83xx 系列	3D8350 3D8360 3D8370 3D8390

以下安全和监管信息适用于 7000 系列和 8000 系列设备：

- 第 206 页的安全和合规性
- 第 208 页的机箱和网络模块名称
- 第 211 页的安全通告

安全和合规性

以下各节介绍 3 系列设备的安全和合规性

70xx 系列设备

以下信息适用于所有 70xx 系列设备：

排放：

- FCC 47 CFR，第 15 部分， A 类数字设备
- EN 55022:2010， A 类
- EN 55024:2010
- EN61000-3-2:2006
- EN61000-3-3:2008
- BSMI CNS 13438

安全：

- IEC 60950-1
- UL/CSA 60950-1：2011 年第 2 版
- EN 60950-1: 2006/A11:2009
- EC 委员会指令 2001/95/EC
- BSMI CNS 14336-1
- UL CB 方案
- 这些 Sourcefire 设备也符合：
- 指令 2011/65/EU，有害物质限制 (RoHS)
- 指令 1907/2006EC，化学品的注册、评估、授权和限制 (REACH)

71xx 系列和 8000 系列设备安全和合规性

此 71xx 系列和 8000 系列设备符合下列安全标准：

71xx 系列和 8000 系列安全和合规性

监管	说明
IEC 60950-1	信息技术设备安全
UL/CSA 60950-1：2007 年第 2 版	信息技术设备安全
EN 60950-1: 2006/A11:2009	信息技术设备安全
AS/NZS 60950-1: 2001	信息技术设备安全
AS/NZS CISPR22:2022	信息技术设备 - 无线电干扰特性
FCC 47 CFR，第 15 部分， A 类数字设备	射频设备 - 子部分 B - 无意辐射体
ICES-003 Issue 4 - Feb 2004， A 类	导致干扰装置标准 - 数字设备
EN 55022:2006， A 类	信息技术设备 - 无线电干扰特性
EN 55024:1998 + A1:2001 + A2:2003	信息技术设备 - 抗扰特性

71xx 系列和 8000 系列安全和合规性 （续）

监管	说明
CISPR 22:2005 + A1:2005+A2:2006，A 类	信息技术设备 - 无线电干扰特性
CISPR 24:1997	信息技术设备 - 抗扰特性
EN61000-3-2:2006	电线谐波电流
EN61000-3-3:2008	闪烁和电压波动
ANSI C63.4	低压电气和电子设备的无线电噪声排放
EC 委员会指令 2001/95/EC	安全性
EC 委员会指令 2006/95/EC	LVD
EC 委员会指令 2004/108/EC	电磁兼容性

机箱和网络模块名称

以下各节列出了在韩国销售的设备的 7000 系列和 8000 系列设备机箱、硬件机箱代码和韩国 KC 认证注册号：

7000 系列机箱名称

7000 系列机箱型号 - 全球和韩国名称表列出了在全球和韩国销售的 7000 系列型号的机箱名称。

7000 系列机箱型号 - 全球和韩国名称

3D 设备型号	硬件机箱代码	韩国 KC 认证注册号
3D7010、 3D7020 和 3D7030	CHRY-1U-AC	KCC-REM-SFi-CHRY1UAC
3D7110 和 3D7120	GERY-1U-8-C-AC	KCC-REM-SFi-GERY1U8CAC

7000 系列机箱型号 - 全球和韩国名称 （续）

3D 设备型号	硬件机箱代码	韩国 KC 认证注册号
3D7110 和 3D7120	GERY-1U-8-FM-AC	KCC-REM-SFi-GERY1U8FMAC
3D7115、 3D7125 和 AMP7150	GERY-1U-4C8S-AC	KCC-REM-SFi-GERY1U4C8SAC

8000 系列机箱名称

8000 系列机箱型号 - 全球名称表列出了在全球销售的 3 系列型号的机箱名称。

8000 系列机箱型号 - 全球名称

3D 设备型号	硬件机箱代码
3D8120、 3D8130、 3D8140 和 AMP8150（交流电源）	CHAS-1U-AC
3D8120、 3D8130、 3D8140 和 AMP8150（直流电源）	CHAS-1U-DC
3D8120、 3D8130、 3D8140 和 AMP8150（交流或直流电源）	CHAS-1U-AC/DC
3D8250、 3D8260、 3D8270 和 3D8290（交流电源）	CHAS-2U-AC
3D8250、 3D8260、 3D8270 和 3D8290（直流电源）	CHAS-2U-DC
3D8250、 3D8260、 3D8270 和 3D8290（交流或直流电源）	CHAS-2U-AC/DC
3D8350、 3D8360、 3D8370 和 3D8390（交流或直流电源）	PG35-2U-AC/DC

8000 系列机箱型号 - 韩国名称表列出了在韩国销售的 3 系列型号的机箱名称。请注意，每个列示的空置 （空位）插槽可能被替换为网络模块。

8000 系列机箱型号 - 韩国名称

3D 设备型号	硬件机箱代码	韩国 KC 认证注册号	网络模块配置
3D8120、 3D8130、 3D8140 和 AMP8150 （交流电源）	CHAS-1U-AC-0003	KCC-REM-SFi-CHAS1UAC0003	插槽 1：NM-C4-0 （或空置） 插槽 2：NM-C4-0 （或空置） 插槽 3：NM-FX4-0 （或空置）
3D8120、 3D8130、 3D8140 和 AMP8150 （直流电源）	CHAS-1U-DC-0003	KCC-REM-SFi-CHAS1UDC0003	插槽 1：NM-C4-0 （或空置） 插槽 2：NM-C4-0 （或空置） 插槽 3：NM-FX4-0 （或空置）
3D8120、 3D8130、 3D8140 和 AMP8150 （交流电源）	CHAS-1U-AC-0004	KCC-REM-SFi-CHAS1UAC0004	插槽 1：SF-3D-CLST-MOD-0 （或空置） 插槽 2：NM-*R2-0 （或空置） [1] 插槽 3：NM-*R2-0 （或空置） [1]
3D8120、 3D8130、 3D8140 和 AMP8150 （直流电源）	CHAS-1U-DC-0004	KCC-REM-SFi-CHAS1UDC0004	插槽 1：SF-3D-CLST-MOD-0 （或空置） 插槽 2：NM-*R2-0 （或空置） [1] 插槽 3：NM-*R2-0 （或空置） [1]
3D8250、 3D8260、 3D8270 和 3D8290 （交流电源）	CHAS-2U-AC-0005	KCC-REM-SFi-CHAS2UAC0005	插槽 1：SF-3D-CLST-MOD-0 （或空置） 插槽 2：NM-*R2-0 （或空置） [1] 插槽 3：NM-C4-0 （或空置） 插槽 4：NM-FX4-0 （或空置） 插槽 5：NM-FX4-0 （或空置） 插槽 6：NM-*R2-0 （或空置） [1] 插槽 7：NM-C4-0 （或空置）
3D8250、 3D8260、 3D8270 和 3D8290 （直流电源）	CHAS-2U-DC-0005	KCC-REM-SFi-CHAS2UDC0005	插槽 1：SF-3D-CLST-MOD-0 （或空置） 插槽 2：NM-*R2-0 （或空置） [1] 插槽 3：NM-C4-0 （或空置） 插槽 4：NM-FX4-0 （或空置） 插槽 5：NM-FX4-0 （或空置） 插槽 6：NM-*R2-0 （或空置） [1] 插槽 7：NM-C4-0 （或空置）

[1] 此网络模块可能是 NM-SR2-0 或 NM-LR2-0。

韩国网络模块名称

8000 系列韩国网络模块名称表列出了与在韩国销售的 3 系列型号对应的网络模块名称。

8000 系列韩国网络模块名称

网络模块型号	韩国 KC 认证注册号
SF-3D-CLST-MOD-0	KCC-REM-SFi-SF3DCLSTMOD0
NM-C4-0	KCC-REM-SFi-NMC40
NM-FX4-0	KCC-REM-SFi-NMFX40
NM-SR2-0	KCC-REM-SFi-NMSR20
NM-LR2-0	KCC-REM-SFi-NMLR20

安全通告

以下各节列出了适用于韩国、日本和中国台湾的安全通告：

适用于韩国的安全通告

需要指明 Sourcefire 设备为 A 类设备的声明。

이 기기는 업무용(A급) 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다.

适用于日本的安全通告

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI-A

适用于中国台湾的安全通告

警告使用者：
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

废弃电气电子设备指令 (WEEE)

Sourcefire 符合废弃电气电子设备指令 (WEEE)，指令编号 2002/96/EC （由 2003/108/EC 修订）。希望处置 Sourcefire 产品的欧盟客户可将其送至 Sourcefire 进行适当处置。

有关更多信息，请联系：

Sourcefire欧洲、中东和非洲 (EMEA)
C/O Seko Benelux BV - Operations
Valkweg 1
1118 EC Schiphol
The Netherlands

电话：+31-(0)20-8201 193
传真：+31-(0)20-6583 359

附录 A
设备SOURCEFIRE电源要求

以下小节介绍 Sourcefire 3D 系统设备的电源要求和相关信息：

警告和注意事项

本文档包含警告和注意事项。警告与安全相关。如不遵循警告可能导致受伤或设备损坏。注意事项是确保设备正常运行所要遵循的要求。如不遵循注意事项可能导致运行故障。

接口连接

警告！ 设备或组件的室内端口仅适用于连接室内或裸露的接线或电缆。设备或组件的室内端口**不得**与连接设备外部 (OSP) 或其接线的接口进行金属连接。这些接口旨在仅用作室内接口 （2 类或 4 类端口，如 GR-1089-CORE，第 4 版中所述）并要求与裸露的 OSP 电缆隔离。加装主保护器并不足以保护将这些接口直接连接至 OSP 接线。

静电控制

注意！ 在拆开设备包装、安装或移动设备之前，必须确保执行静电放电控制程序，例如，使用接地腕带和 ESD 工作台。过多的静电放电可能会损坏设备或导致意外操作。

70xx 系列设备

3D7010、 3D7020 和 3D7030 (CHRY-1U-AC) 适合由有资质人员在符合国家电气规范的网络通信场所和地点进行安装。请注意，此设备只能使用交流电源。

Sourcefire 建议保留包装材料，以备需要退货时使用。

有关详细信息，请参阅以下各节：

- 请参阅第 214 页的安装，了解有关电路安装、电压、电流、频率范围和电源线的信息。
- 请参阅第 215 页的接地要求，了解有关连接位置、推荐端子和地线的要求。

安装

Sourcefire 3D 系统设备的安装必须符合 NFPA 70 第 250 条、国家电气规范 (NEC) 手册和地方电力法规的要求。

设备使用单一电源。必须在将要安装 Sourcefire 3D 系统的网络设备输入端安装外部浪涌保护装置。

电路额定负载必须为设备满额功率。

电压

电源在 100VAC - 240VAC 额定电压 （90VAC - 264VAC 最大电压）下工作。使用此范围之外的电压可能会损坏设备。

电流

在整个电压范围内的标称额定电流最大为 2A。必须使用适当的电线和断路器以降低发生火灾的可能性。

频率范围

交流电源的频率范围为 47 Hz - 63 Hz。此范围之外的频率可能导致设备无法运行或无法正常运行。

电源线

电源上的电源连接使用 IEC C14 连接器并接受 IEC C13 连接器。必须使用 UL 认证电源线。最小线规是 16 AWG。随设备提供的是 16 AWG UL 认证电源线 （配有 NEMA 515P 插头）。要获得其他电源线，请与工厂联系。

重要！ 请**勿**划伤电源线。

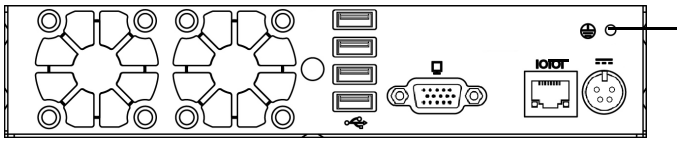
接地要求

设备必须接地至公共接地网。

连接位置：

机箱背面提供接地连接位置。提供一个 M4 螺柱。提供一个用于连接环形端子的外部齿形锁紧垫片。每个螺柱旁边均标有标准接地符号。

下图显示机箱上的连接位置。



推荐的端子

必须使用 UL 认证端子进行接地。可使用带有一个开孔 （适用于 #6 (M3.5) 螺柱）的环形端子。对于 16 AWG 电线，建议使用 AMP/Tyco 36151。这是 UL 认证带孔（适用于 #6 螺柱）的环形端子。

地线要求

地线规格必须确保在发生单路故障时足以承载电路的电流。地线规格应等于用于保护电路的断路器的电流。请参阅第 214 页的电流。

导线裸露部分，在拧接之前，必须覆有抗氧剂。仅可将铜线用于接地。

71xx 系列设备

此小节介绍以下 Sourcefire 设备的电源要求：

- 3D7110 和 3D7120 (GERY-1U-8-AC)
- 3D7115 和 3D7125 (GERY-1U-4C8S-AC)

这些 Sourcefire 设备适合由合格人员在符合国家电气规范的网络电信设施和地点进行安装。请注意，此设备只能使用交流电源。

Sourcefire 建议保留包装材料，以备需要退货时使用。

有关详细信息，请参阅以下各节：

- 请参阅第 216 页的安装，了解有关电路安装、电压、电流、频率范围和电源线的信息。
- 请参阅第 217 页的接地要求，了解有关连接位置、推荐端子和地线的要求。

安装

Sourcefire 3D 系统的安装必须符合 NFPA 70 第 250 条、国家电气规范 (NEC) 手册和地方电力法规的要求。

需要独立电路以创建冗余电源。使用不间断电源或电池备份电源防止由于输入线路故障导致的电源状态问题或断电。

为每个电源运行整个设备提供足够的功率。每个电源的电压和电流额定值标示在设备上的铭牌上。

在将要安装Sourcefire 3D 系统的网络设备输入端安装外部浪涌保护装置。

独立电路安装

如果使用独立电路，每个电路额定值必须等于设备的全额定值。此配置为电路故障和电源故障做好准备。

示例：每个电源均连接至另一个 220V 电路。每个电路均必须能够提供 5A 电流，如铭牌上所标示。

同一电路安装

如果同一电路用于为两个电源供电，则一个电源的额定功率适用于整个配电箱。此配置仅防止出现电源故障。

示例：两个电源均连接至同一 220V 电路。此电路的最大电流是 5A，如铭牌上所标示。

电压

电源在以下电压下工作：100VAC - 240VAC 额定电压 （85VAC - 264VAC 最大电压）。使用此范围之外的电压可能会损坏设备。

电流

每个电源的标称额定电流是：在整个电压范围内每条供电线路最大电流为 10A，在 187VAC - 264VAC 电压下每条供电线路最大电流为 5A。必须使用适当的电线和断路器以降低发生火灾的可能性。

频率范围

交流电源的频率范围为 47 Hz - 63 Hz。此范围之外的频率可能导致设备无法运行或无法正常运行。

电源线

电源上的电源连接是 IEC C14 连接器并接受 IEC C13 连接器。必须使用 UL 认证电源线。最小线规是 16 AWG。随设备提供的是 16 AWG UL 认证电源线 （配有 NEMA 5 15P 插头）。要获得其他电源线，请与工厂联系。

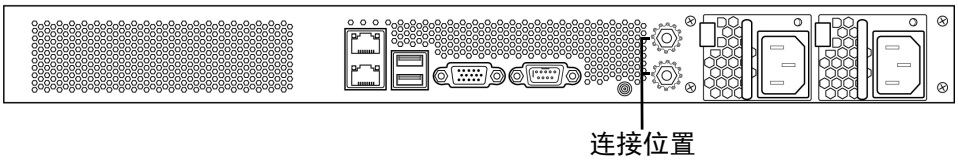
接地要求

Sourcefire 3D 系统必须接地到公共接地网。

连接位置

机箱背面提供接地连接位置。提供 M4 螺柱。提供用于连接环形端子的外部齿形锁紧垫片。每个螺柱旁边均标有标准接地符号。

下图显示机箱上的连接位置。



推荐的端子

必须使用 UL 认证端子进行接地连接。可使用带有一个开孔 （适用于 4 毫米或 #8 螺柱）的环形端子。对于 10 - 12 AWG 电线，建议使用 Tyco 34853。这是 UL 认证带孔 （适用于 #8 螺柱）环形端子。

地线要求

地线规格必须确保在发生单路故障时足以承载电路的电流。地线规格应等于用于保护电路的断路器的电流。请参阅第 217 页的电流。

导线裸露部分，在拧接之前，必须覆有抗氧剂。仅可将铜线用于接地。

81xx 系列设备

此小节涉及以下设备：

- 3D8120、 3D8130 和 3D8140 （CHAS-1U-AC、 CHAS-1U-DC 或 CHAS-1U-AC/DC）

这些 Sourcefire 设备适合由合格人员在符合国家电气规范的网络电信设施和地点进行安装。

Sourcefire 建议保留包装材料，以备需要退货时使用。

有关详细信息，请参阅以下各节：

- 请参阅第 218 页的交流电安装，了解有关电路安装、电压、电流、频率范围和电源线的信息。
- 请参阅第 219 页的直流安装，以了解有关电路安装、电压、电流、接地基准、端子、断路器要求和最低电线规格的信息。
- 请参阅第 221 页的接地要求，以了解有关连接位置、推荐端子、地线要求和直流电源的信息。

交流电安装

Sourcefire 3D 系统的安装必须符合 NFPA 70 第 250 条、国家电气规范 (NEC) 手册和地方电力法规的要求。

警告！ 请**勿**将直流供电线路连接至交流电源。

需要独立电路以创建冗余电源。使用不间断电源或电池备份电源防止由于输入线路故障导致的电源状态问题或断电。

为每个电源运行整个设备提供足够的功率。每个电源的电压和电流额定值标示在设备上的铭牌上。

在将要安装Sourcefire 3D 系统的网络设备输入端安装外部浪涌保护装置。

独立电路安装

如果使用独立电路，每个电路额定值必须等于设备的全额定值。此配置为电路故障和电源故障做好准备。

示例：每个电源均连接至另一个 220V 电路。每个电路均必须能够提供 5A 电流，如铭牌上所标示。

同一电路安装

如果同一电路用于为两个电源供电，则一个电源的额定功率适用于整个配电箱。此配置仅防止出现电源故障。

示例：两个电源均连接至同一 220V 电路。此电路的最大电流是 5A，如铭牌上所标示。

交流电压

电源在以下电压下工作：100VAC - 240VAC 额定电压 （85VAC - 264VAC 最大电压）。使用此范围之外的电压可能会损坏设备。

交流电流

每个电源的标称额定电流是：在整个电压范围内每条供电线路最大电流为 5.2A，在 187VAC - 264VAC 电压下每条供电线路最大电流为 2.6A。必须使用适当的电线和断路器以降低发生火灾的可能性。

频率范围

交流电源的频率范围为 47 Hz - 63 Hz。此范围之外的频率可能导致设备无法运行或无法正常运行。

电源线

电源上的电源连接是 IEC C14 连接器并接受 IEC C13 连接器。必须使用 UL 认证电源线。最小线规是 16 AWG。随设备提供的是 16 AWG UL 认证电源线 （配有 NEMA 5 15P 插头）。要获得其他电源线，请与工厂联系。

直流安装

需要独立电路以创建冗余电源。使用不间断电源或电池备份电源防止由于输入线路故障导致的电源状态问题或断电。

警告！请**勿**将交流供电线路连接至直流电源。

为每个电源运行整个设备提供足够的功率。每个电源的电压和电流额定值标示在设备上的铭牌上。

在将要安装Sourcefire 3D 系统的网络设备输入端安装外部浪涌保护装置。

独立电路安装

如果使用独立电路，每个电路额定值必须等于设备的全额定值。此配置为电路故障和电源故障做好准备。

示例：每个电源均连接至另一个 -48VDC 电路。每个电路均必须能够提供 20A 电流，如铭牌上所标示。

同一电路安装

如果同一电路用于为两个电源供电，则一个电源的额定功率适用于整个配电箱。此配置仅防止出现电源故障。

示例：两个电源均连接至同一 –48VDC 电路。此电路的最大电流是 20A，如铭牌上所标示。

警告！使用此优化方式要求电源线满足每个电源的全部额定功率要求。

直流电压

电源在以下电压下工作：

- -48VDC 额定 （参考 RTN）。
- -40VDC 至 -72VDC 最大

使用此范围之外的电压可能会损坏设备。

直流电流

每个电源的最大电流为 11A。

接地基准

直流电源与接地基准完全绝缘。

推荐的端子

将供电线路通过螺丝端子连接至直流电源。端子必须为 UL 认证端子。端子必须具有支持 M4 或 #8 螺丝的开孔。端子的最大宽度为 8.1 毫米 （0.320 英寸）。适用于 10 - 12 号电线的代表性扁形端子是 Tyco 325197。

断路器要求

必须提供足以承受额定电压下的额定电流的断路器。断路器必须满足以下要求：

- UL 认证
- CSA 认证 （推荐）
- VDE 认证 （推荐）

- 支持最大负载 (20A)
- 支持安装电压 （-40V 至 -72VDC，根据电源要求）
- 额定用于直流电

推荐断路器：Airpax IELK1-1-72-20.0-01-V。使用的端子选件取决于安装。此断路器为单极 20A 断路器，额定直流电压为 80V。它经过认证，具有*较长延迟*。有关此断路器的信息可在 http://www.airpax.net/site/utilities/eliterature/pdfs/ial.pdf 找到。

最低电线规格要求

每个线槽有三根电线 （一个电路）的供电线路可以使用 12 AWG 电线。每个线槽有多个电路的供电线路必须使用 10 AWG 电线。请注意，冗余电源的两个单独供电线路是两个电路，必须使用 10 AWG 电线。

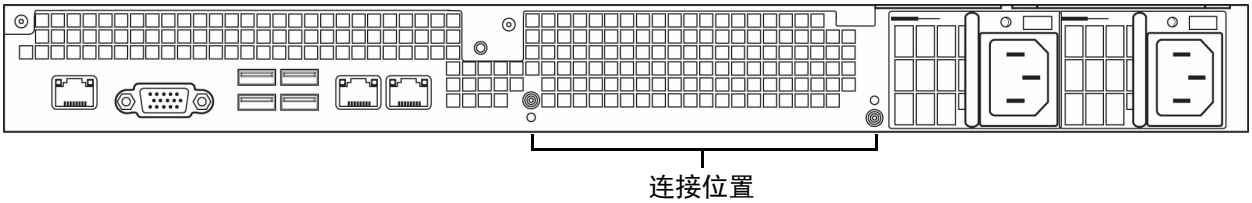
接地要求

Sourcefire 3D 系统必须接地到公共接地网。

连接位置

机箱背面提供接地连接位置。提供 M4 螺柱。提供用于连接环形端子的外部齿形锁紧垫片。每个螺柱旁边均标有标准接地符号。

下图指明 1U 机箱上的连接位置。



推荐的端子

必须使用 UL 认证端子进行接地连接。可使用带有一个开孔 （适用于 4 毫米或 #8 螺柱）的环形端子。对于 10 - 12 AWG 电线，建议使用 Tyco 34853。这是 UL 认证带孔 （适用于 #8 螺柱）环形端子。

地线要求

地线规格必须确保在发生单路故障时足以承载电路的电流。地线规格应等于用于保护电路的断路器的电流。有关交流电路，请参阅第 219 页的交流电流。有关直流电流，请参阅第 220 页的直流电流。

导线裸露部分，在拧接之前，必须覆有抗氧剂。仅可将铜线用于接地。

直流电源

直流电源在每个电源上都有额外的接地连接。这样，就可将热插拔电源连接至供电线路，使其返回并接地，以便安全插入。必须连接此接地接线片。

它是带有外部齿形锁紧垫片的 M4 螺丝。

地线规格应匹配电路的断路器。

82xx 系列设备

此小节涉及以下设备：

- 3D8250、3D8260、3D8270 和 3D8290 （CHAS-2U-AC、 CHAS-2U-DC 或 CHAS-2U-AC/DC）

这些 Sourcefire 设备适合由合格人员在符合国家电气规范的网络电信设施和地点进行安装。

Sourcefire 建议保留包装材料，以备需要退货时使用。

有关详细信息，请参阅以下各节：

- 请参阅第 222 页的交流电安装，了解有关电路安装、电压、电流、频率范围和电源线的信息。
- 请参阅第 223 页的直流安装，以了解有关电路安装、电压、电流、接地基准、端子、断路器要求和最低电线规格的信息。
- 请参阅第 225 页的接地要求，以了解有关连接位置、推荐端子、地线要求和直流电源的信息。

交流电安装

Sourcefire 3D 系统的安装必须符合 NFPA 70 第 250 条、国家电气规范 (NEC) 手册和地方电力法规的要求。

警告！ 请**勿**将直流供电线路连接至交流电源。

需要独立电路以创建冗余电源。使用不间断电源或电池备份电源防止由于输入线路故障导致的电源状态问题或断电。

为每个电源运行整个设备提供足够的功率。每个电源的电压和电流额定值标示在设备上的铭牌上。

在将要安装Sourcefire 3D 系统的网络设备输入端安装外部浪涌保护装置。

独立电路安装

如果使用独立电路，每个电路额定值必须等于设备的全额定值。此配置为电路故障和电源故障做好准备。

示例：每个电源均连接至另一个 220V 电路。每个电路均必须能够提供 5A 电流，如铭牌上所标示。

同一电路安装

如果同一电路用于为两个电源供电，则一个电源的额定功率适用于整个配电箱。此配置仅防止出现电源故障。

示例：两个电源均连接至同一 220V 电路。此电路的最大电流是 5A，如铭牌上所标示。

交流电压

电源在以下电压下工作：100VAC - 240VAC 额定电压 （85VAC - 264VAC 最大电压）。使用此范围之外的电压可能会损坏设备。

交流电流

每个电源的标称额定电流是：在整个电压范围内每条供电线路最大电流为 8A，在 187VAC - 264VAC 电压下每条供电线路最大电流为 4A。必须使用适当的电线和断路器以降低发生火灾的可能性。

频率范围

交流电源的频率范围为 47 Hz - 63 Hz。此范围之外的频率可能导致设备无法运行或无法正常运行。

电源线

电源上的电源连接是 IEC C14 连接器并接受 IEC C13 连接器。必须使用 UL 认证电源线。最小线规是 16 AWG。随设备提供的是 16 AWG UL 认证电源线 （配有 NEMA 5 15P 插头）。要获得其他电源线，请与工厂联系。

直流安装

需要独立电路以创建冗余电源。使用不间断电源或电池备份电源防止由于输入线路故障导致的电源状态问题或断电。

警告！请**勿**将交流供电线路连接至直流电源。

为每个电源运行整个设备提供足够的功率。每个电源的电压和电流额定值标示在设备上的铭牌上。

在将要安装Sourcefire 3D 系统的网络设备输入端安装外部浪涌保护装置。

独立电路安装

如果使用独立电路，每个电路额定值必须等于设备的全额定值。此配置为电路故障和电源故障做好准备。

示例：每个电源均连接至另一个 -48VDC 电路。每个电路均必须能够提供 20A 电流，如铭牌上所标示。

同一电路安装

如果同一电路用于为两个电源供电，则一个电源的额定功率适用于整个配电箱。此配置仅防止出现电源故障。

示例：两个电源均连接至同一 –48VDC 电路。此电路的最大电流是 20A，如铭牌上所标示。

警告！使用此优化方式要求电源线满足每个电源的全部额定功率要求。

直流电压

电源在以下电压下工作：

- -48VDC 额定 （参考 RTN）。
- -40VDC 至 -72VDC 最大

使用此范围之外的电压可能会损坏设备。

直流电流

每个电源的最大电流为 18A。

接地基准

直流电源与接地基准完全绝缘。

推荐的端子

将供电线路通过螺丝端子连接至直流电源。端子必须为 UL 认证端子。端子必须具有支持 M4 或 #8 螺丝的开孔。端子的最大宽度为 8.1 毫米 （0.320 英寸）。适用于 10 - 12 号电线的代表性扁形端子是 Tyco 325197。

断路器要求

必须提供足以承受额定电压下的额定电流的断路器。断路器必须满足以下要求：

- UL 认证
- CSA 认证 （推荐）
- VDE 认证 （推荐）
- 支持最大负载 (20A)
- 支持安装电压 （-40V 至 -72VDC，根据电源要求）
- 额定用于直流电

推荐断路器：Airpax IELK1-1-72-20.0-01-V。使用的端子选件取决于安装。此断路器为单极 20A 断路器，额定直流电压为 80V。它经过认证，具有*较长延迟*。有关此断路器的信息可在 http://www.airpax.net/site/utilities/eliterature/pdfs/ial.pdf 找到。

最低电线规格要求

每个线槽有三根电线 （一个电路）的供电线路可以使用 12 AWG 电线。每个线槽有多个电路的供电线路必须使用 10 AWG 电线。请注意，冗余电源的两个单独供电线路是两个电路，必须使用 10 AWG 电线。

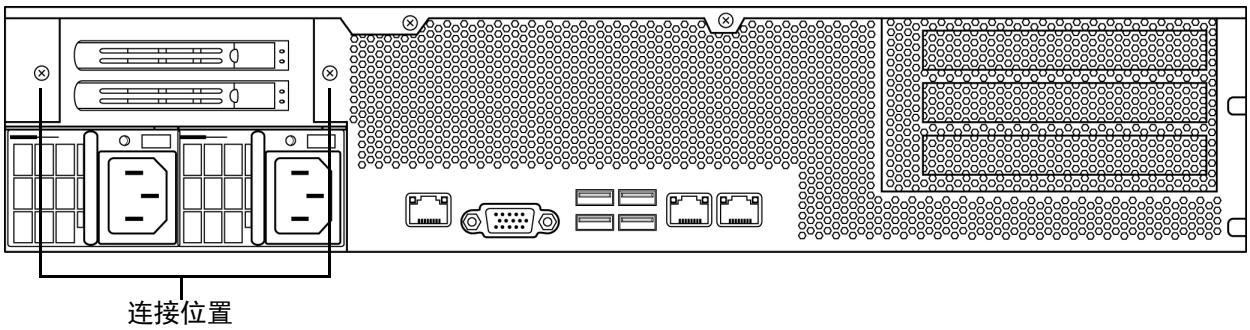
接地要求

Sourcefire 3D 系统必须接地到公共接地网。

连接位置

机箱背面提供接地连接位置。提供 M4 螺柱。提供用于连接环形端子的外部齿形锁紧垫片。每个螺柱旁边均标有标准接地符号。

下图指明 2U 机箱上的连接位置。



推荐的端子

必须使用 UL 认证端子进行接地连接。可使用带有一个开孔 （适用于 4 毫米或 #8 螺柱）的环形端子。对于 10 - 12 AWG 电线，建议使用 Tyco 34853。这是 UL 认证带孔 （适用于 #8 螺柱）环形端子。

地线要求

地线规格必须确保在发生单路故障时足以承载电路的电流。地线规格应等于用于保护电路的断路器的电流。有关交流电路，请参阅第 219 页的交流电流。有关直流电流，请参阅第 220 页的直流电流。

导线裸露部分，在拧接之前，必须覆有抗氧剂。仅可将铜线用于接地。

直流电源

直流电源在每个电源上都有额外的接地连接。这样，就可将热插拔电源连接至供电线路，使其返回并接地，以便安全插入。必须连接此接地接线片。

它是带有外部齿形锁紧垫片的 M4 螺丝。

地线规格应匹配电路的断路器。

83xx 系列设备

此小节涉及以下设备：

- 3D8350/8360/8370/8390 (PG35-2U-AC/DC)

这些 Sourcefire 设备适合由合格人员在符合国家电气规范的网络电信设施和地点进行安装。

Sourcefire 建议保留包装材料，以备需要退货时使用。

有关详细信息，请参阅以下各节：

- 请参阅第 227 页的交流电安装，了解有关电路安装、电压、电流、频率范围和电源线的信息。
- 请参阅第 228 页的直流安装，以了解有关电路安装、电压、电流、接地基准、端子、断路器要求和最低电线规格的信息。
- 请参阅第 229 页的接地要求，以了解有关连接位置、推荐端子、地线要求和直流电源的信息。

交流电安装

Sourcefire 3D 系统的安装必须符合 NFPA 70 第 250 条、国家电气规范 (NEC) 手册和地方电力法规的要求。

警告！请**勿**将直流供电线路连接至交流电源。

需要独立电路以创建冗余电源。使用不间断电源或电池备份电源防止由于输入线路故障导致的电源状态问题或断电。

为每个电源运行整个设备提供足够的功率。每个电源的电压和电流额定值标示在设备上的铭牌上。

在将要安装Sourcefire 3D 系统的网络设备输入端安装外部浪涌保护装置。

独立电路安装

如果使用独立电路，每个电路额定值必须等于设备的全额定值。此配置为电路故障和电源故障做好准备。

示例：每个电源均连接至另一个 220V 电路。每个电路必须能够提供 10A 电流，如铭牌上所标示。

同一电路安装

如果同一电路用于为两个电源供电，则一个电源的额定功率适用于整个配电箱。此配置仅防止出现电源故障。

示例：两个电源均连接至同一 220V 电路。此电路的最大电流是 10A，如铭牌上所标示。

交流电压

电源在以下电压下工作：100VAC - 240VAC 额定电压 （85VAC - 264VAC 最大电压）。使用此范围之外的电压可能会损坏设备。

交流电流

每个电源的标称额定电流是：在整个电压范围内每条供电线路最大电流为 11A，在 187VAC - 264VAC 电压下每条供电线路最大电流为 5.5A。必须使用适当的电线和断路器以降低发生火灾的可能性。

频率范围

交流电源的频率范围为 47 Hz - 63 Hz。此范围之外的频率可能导致设备无法运行或无法正常运行。

电源线

电源上的电源连接是 IEC C14 连接器并接受 IEC C13 连接器。必须使用 UL 认证电源线。最小线规是 16 AWG。随设备提供的是 16 AWG UL 认证电源线 （配有 NEMA 5 15P 插头）。要获得其他电源线，请与工厂联系。

直流安装

需要独立电路以创建冗余电源。使用不间断电源或电池备份电源防止由于输入线路故障导致的电源状态问题或断电。

警告！ 请**勿**将交流供电线路连接至直流电源。

为每个电源运行整个设备提供足够的功率。每个电源的电压和电流额定值标示在设备上的铭牌上。

在将要安装Sourcefire 3D 系统的网络设备输入端安装外部浪涌保护装置。

独立电路安装

如果使用独立电路，每个电路额定值必须等于设备的全额定值。此配置为电路故障和电源故障做好准备。

示例：每个电源均连接至另一个 -48VDC 电路。每个电路必须能够提供 25A 电流，如铭牌上所标示。

同一电路安装

如果同一电路用于为两个电源供电，则一个电源的额定功率适用于整个配电箱。此配置仅防止出现电源故障。

示例：两个电源均连接至同一 –48VDC 电路。此电路的最大电流是 25A，如铭牌上所标示。

警告！ 使用此优化方式要求电源线满足每个电源的全部额定功率要求。

直流电压

电源在以下电压下工作：

- -48VDC 额定 （参考 RTN）。
- -40VDC 至 -72VDC 最大

使用此范围之外的电压可能会损坏设备。

直流电流

每个供电线路的最大电流为 25A。

接地基准

直流电源与接地基准完全绝缘。

推荐的端子

将供电线路通过螺丝端子连接至直流电源。端子必须为 UL 认证端子。端子必须具有支持 M4 或 #8 螺丝的开孔。端子的最大宽度为 8.1 毫米 （0.320 英寸）。适用于 10 - 12 号电线的代表性扁形端子是 Tyco 325197。

断路器要求

必须提供足以承受额定电压下的额定电流的断路器。断路器必须满足以下要求：

- UL 认证
- CSA 认证 （推荐）
- VDE 认证 （推荐）
- 支持最大负载 (20A)
- 支持安装电压 （-40V 至 -72VDC，根据电源要求）
- 额定用于直流电

推荐断路器：Airpax IELK1-1-72-20.0-01-V。使用的端子选件取决于安装。此断路器为单极 20A 断路器，额定直流电压为 80V。它经过认证，具有*较长延迟*。有关此断路器的信息可在 http://www.airpax.net/site/utilities/eliterature/pdfs/ial.pdf 找到。

最低电线规格要求

每个线槽有三根电线 （一个电路）的供电线路可以使用 12 AWG 电线。每个线槽有多个电路的供电线路必须使用 10 AWG 电线。请注意，冗余电源的两个单独供电线路是两个电路，必须使用 10 AWG 电线。

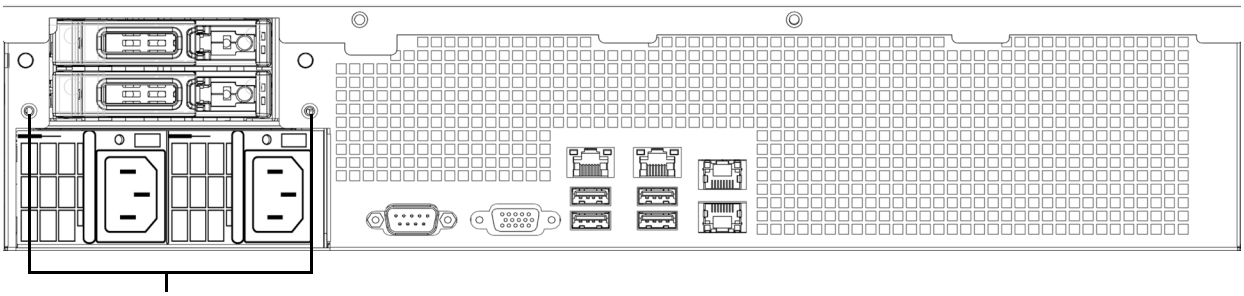
接地要求

Sourcefire 3D 系统必须接地到公共接地网。

连接位置

机箱背面提供接地连接位置。提供 M4 螺柱。提供用于连接环形端子的外部齿形锁紧垫片。每个螺柱旁边均标有标准接地符号。

下图指明 83xx 系列 2U 机箱上的连接位置。



推荐的端子

必须使用 UL 认证端子进行接地连接。可使用带有一个开孔 （适用于 4 毫米或 #8 螺柱）的环形端子。对于 10 - 12 AWG 电线，建议使用 Tyco 34853。这是 UL 认证带孔 （适用于 #8 螺柱）环形端子。

地线要求

地线规格必须确保在发生单路故障时足以承载电路的电流。地线规格应等于用于保护电路的断路器的电流。有关交流电路，请参阅第 227 页的交流电流。有关直流电流，请参阅第 229 页的直流电流。

导线裸露部分，在拧接之前，必须覆有抗氧剂。仅可将铜线用于接地。

直流电源

直流电源在每个电源上都有额外的接地连接。这样，就可将热插拔电源连接至供电线路，使其返回并接地，以便安全插入。必须连接此接地接线片。

它是带有外部齿形锁紧垫片的 M4 螺丝。

地线规格应匹配电路的断路器。

附录 B

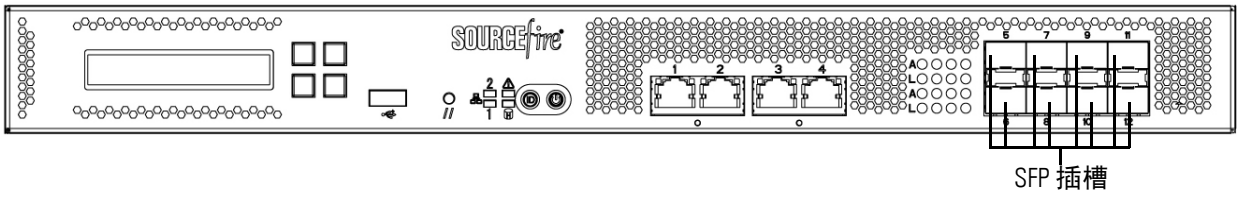
在 3D7115、 3D7125 和 AMP7150 设备中使用 SFP 收发器

以下各节提供有关在 3D7115、 3D7125 和 AMP7150 中使用小型可插拔 (SFP) 插槽和收发器的详细信息：

3D7115、 3D7125 和 AMP7150 SFP 插槽及收发器

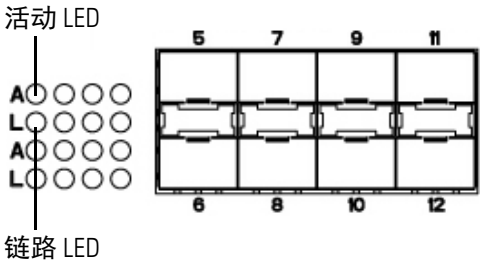
3D7115、3D7125 和 AMP7150 包含八个小型可插拔 (SFP) 插槽，并且可安装八个 SFP 收发器。

3D7115、 3D7125 和 AMP7150 前视图



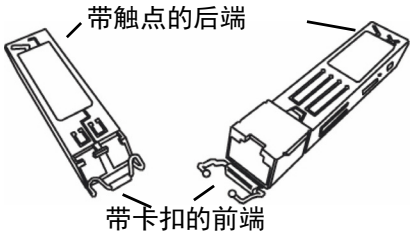
3D7115、 3D7125 和 AMP7150 SFP 插槽

八个 SFP 插槽按垂直方向顺序编号为从 5 到 12，并且采用中心对齐配置 （上面一行开口朝上，下面一行开口朝下）。



位于插槽左侧的 LED 显示有关每个接口的活动和链路信息。有关详细信息，请参阅第 146 页的3D7115、 3D7125 和 AMP7150 SFP 插槽活动/链路 LED。

样本 SFP 收发器



示例光纤　　示例铜缆

3D7115、 3D7125 和 AMP7150 可支持最多八个 SFP 收发器 （以下三种规格的任意组合）：

- SFP-C-1：铜缆收发器
- SFP-F-1-SR：短距离光纤收发器
- SFP-F-1-LR：长距离光纤收发器

请仅在 3D7115、3D7125 和 AMP7150 中使用 Sourcefire SFP 收发器 非 Sourcefire SFP 收发器会阻塞插槽，并可能导致收发器和 （或）机箱的永久性损害。

在设备保持正常运行时，可插拔收发器。请刷新防御中心上的用户界面查看配置更改。

SFP 收发器没有旁路功能。请将这些收发器用于被动部署或内联部署，您希望这些部署中的设备当设备故障或断电 （例如，虚拟交换机、虚拟路由器和某些访问控制策略）时停止传输所有流量。

对于被动部署，您可以在最多八个插槽中使用收发器的任意组合监控最多八个网段。对于内联式部署，您可以在垂直分布的连续插槽 （5 和 6、 7 和 8、 9 和 10、 11 和 12）中使用收发器的任意组合 （铜缆、光纤或混合）监控最多四个网段。

使用防御中心管理您的设备以配置收发器上的端口。

插入 SFP 收发器

在插入收发器时，请使用适当的静电释放 (ESD) 步骤。应避免接触后端的触点并防止触点和端口沾上灰尘。

警告！ 请不要强力将 SFP 收发器插入插槽，因为这会阻塞插槽，并可能导致收发器和 （或）机箱的永久性损害。

要插入 SFP 收发器，请执行以下操作：

1. 注意不要碰到后端的触点，使用您的手指抓住卡扣的两侧并将收发器后端滑入机箱插槽。请注意，上面一行的插槽开口朝上，下面一行的插槽开口朝下。
2. 轻轻地将卡扣向收发器推，合上卡扣并咬合锁定机制，将收发器固定到位。
3. 请按照第 52 页的安装 Sourcefire 3D 系统设备中的步骤配置收发器上的端口。

   请注意，如果您将收发器插入到当前正在工作中的设备，必须刷新防御中心用户界面查看更改。

移除 SFP 收发器

在移除收发器时，请使用适当的静电释放 (ESD) 步骤。应避免接触后端的触点并防止触点和端口沾上灰尘。

要移除 SFP 收发器，请执行以下操作：

1. 从要从设备移除的收发器断开所有电缆。
2. 使用您的手指轻轻将收发器的卡扣从机箱向外拉，以释放连接机制。

   对于上面一行的收发器，请向下拉。对于下面一行的收发器，请向上提。
3. 使用您的手指抓住卡扣两侧并使用卡扣作为手柄轻轻地将收发器拔出机箱，注意不要碰到收发器后端的触点。

附录 C
插入或拆除 8000 系列模块

8000 系列设备在部署中实现了模块化灵活性。按照此小节中的步骤：

- 将新模块插入设备
- 拆除或更换设备上的预安装模块

以下各小节介绍如何插入，拆除或更换 8000 系列模块：

8000 系列设备上的模块插槽

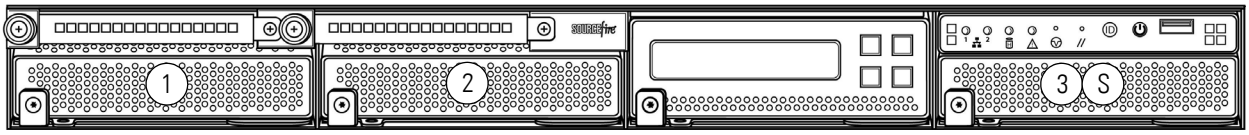
8000 系列设备可使用以下插槽中的模块：

将模块插入设备后，请参阅以下各节了解有关使用模块的详细信息：

- 有关配置感知接口的信息，请参阅第 56 页的识别感应接口。
- 有关使用堆栈模块的信息，请参阅第 66 页的使用堆栈配置中的设备。

81xx 系列

81xx 系列设备可使用以下插槽中的模块：



插槽 1-3：网络模块
插槽 S：堆栈模块

堆栈配置考虑因素

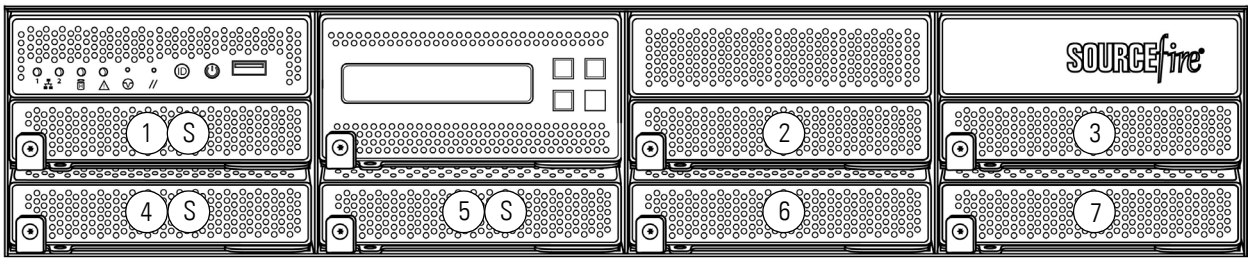
按以下说明为堆栈设备配置模块：

- 仅在主设备上安装网络模块。
- 将一个堆栈模块安装到主设备上，将另一个堆栈模块安装到辅助设备上。

82xx 系列和 83xx 系列

82xx 系列和 83xx 系列设备可在以下插槽中使用模块：

82xx 系列和 83xx 系列主设备



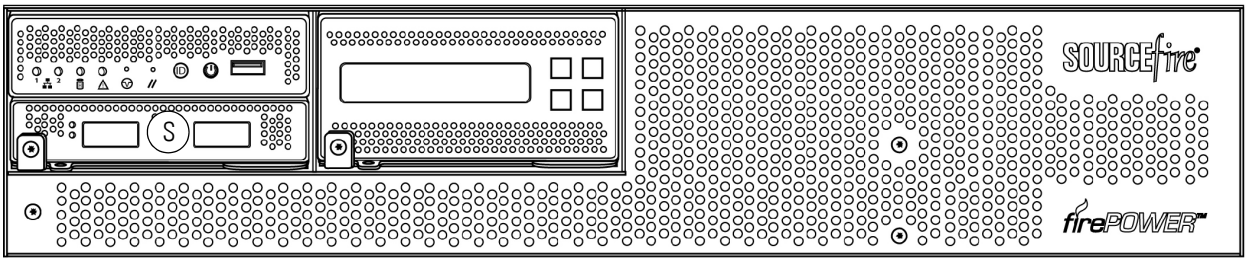
插槽 1-7：网络模块
插槽 S：堆栈模块

堆栈配置考虑因素

按以下说明为堆栈设备配置模块：

- 仅在主设备上安装网络模块。
- 将一个堆栈模块安装到每个堆栈辅助设备的主设备上，再将一个堆栈模块安装到一个辅助设备上。

82xx 系列和 83xx 系列辅助设备



插槽 S：堆栈模块

附件

模块组装套件包括 T8 梅花头螺丝刀和以下一个或多个模块：

- 四端口 1000BASE-T 铜可配置旁路网络模块。有关详细信息，请参阅第 164 页的四端口 1000BASE-T 铜缆可配置旁路网络模块。
- 四端口 1000BASE-SX 光纤可配置旁路网络模块。有关详细信息，请参阅第 165 页的四端口 1000BASE-SX 光纤可配置旁路网络模块。
- 双端口 10GBASE （MMSR 或 SMLR）光纤可配置旁路网络模块。有关详细信息，请参阅第 167 页的双端口 10GBASE （MMSR 或 SMLR）光纤可配置旁路网络模块。
- 双端口 40GBASE-SR4 光纤可配置旁路网络模块。有关详细信息，请参阅第 169 页的双端口 40GBASE-SR4 光纤可配置旁路网络模块。

重要！ 此双插槽网络模块仅在 40G 容量 3D8250 或 3D8350 上使用。如需升级设备，请参阅 《*Sourcefire8000 系列设备 40G 容量升级指南*》。

- 四端口 1000BASE-T 铜缆非旁路网络模块。有关详细信息，请参阅第 171 页的四端口 1000BASE-T 铜缆非旁路网络模块。
- 四端口 1000BASE-SX 光纤非旁路网络模块。四端口 1000BASE-SX 光纤非旁路网络模块。有关详细信息，请参阅第 172 页的四端口 1000BASE-SX 光纤非旁路网络模块。
- 四端口 10GBASE （MMSR 或 SMLR）光纤非旁路网络模块。有关详细信息，请参阅第 173 页的四端口 10GBASE （MMSR 或 SMLR）光纤非旁路网络模块。

警告！ 四端口 10GBASE 光纤非旁路网络模块包含固定小型可插拔 (SFP) 收发器。尝试卸下 SFP 可能损坏模块。

- 堆栈模块。有关详细信息，请参阅第 175 页的堆栈模块。

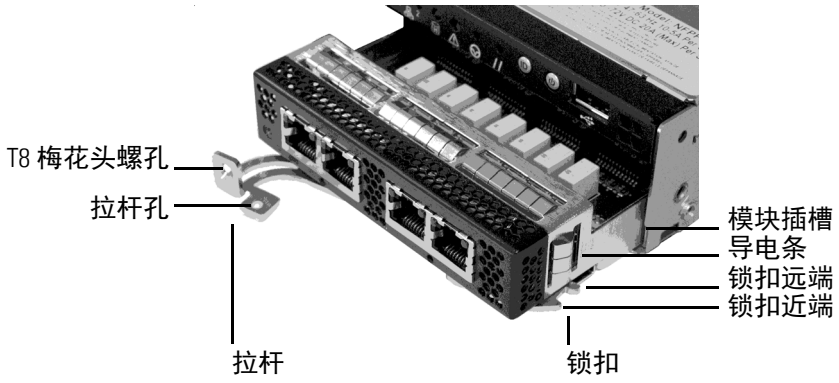
如在设备上不兼容的插槽中安装了网络模块，或网络模块与系统不兼容，则当您尝试配置网络模块时，管理防御中心上网络界面会显示错误或警告消息。请与 Sourcefire 支持人员联系请求协助。

重要！ 更换网络模块可能会改变完整配置的韩国认证 （KCC 标志）设备的配置。有关详细信息，请参阅设备的原始配置文档和第 208 页的机箱和网络模块名称。

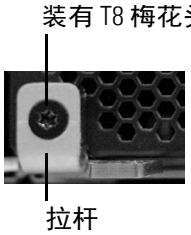
识别模块部件

所有模块均包含相同的部件，无论模块的感知接口、速度或大小如何。

示例模块或插槽盖 （打开）



示例模块拉杆 （合上，孔内已安装螺钉）



准备工作

遵循以下准则，准备插入或卸下模块：

- 识别所有设备和模块部件。
- 识别要安装网络模块的插槽。

提示！ 可将网络模块插入到任何可用的兼容插槽。

- 识别适合堆栈模块的插槽。请参阅第 66 页的使用堆栈配置中的设备和以下列表：
  - 3D8140：插槽 3
  - 3D8250、 3D8260、 3D8350 和 3D8360 主插槽：插槽 5
  - 3D8270 和 3D8370 主插槽：插槽 5 和 1
  - 3D8290 和 3D8390 主插槽：插槽 5、 1 和 4
  - 3D82xx 和 3D83xx 辅助插槽：插槽 S
- 确认导电条已放置到位。
- 从设备中拔出所有电源线。

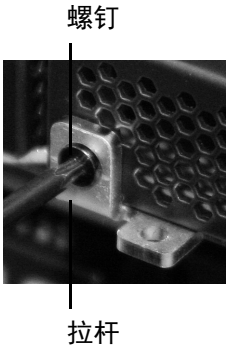
警告！ 不能热插拔模块。必须关闭电源并从设备拔出**两**条电源线，然后再插入或卸下模块。

卸下模块或插槽盖

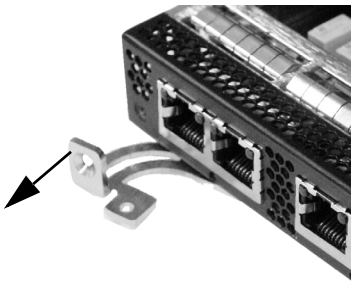
处理模块时，使用适当静电放电 (ESD) 方法 （例如，佩戴腕带和使用 ESD 工作台）。将未使用的模块存储在防静电袋或防静电盒中，以防止损坏。

要卸下模块或插槽盖：

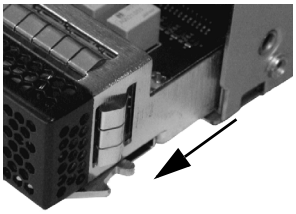
1. 使用随附的螺丝刀，从模块拉杆上卸下并保留 T8 梅花头螺钉。



2. 将拉杆拉离模块以释放锁扣。



3. 将模块滑出插槽。

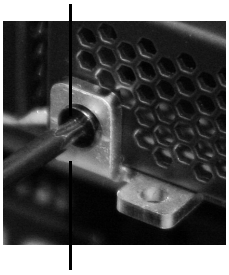


插入模块或插槽盖

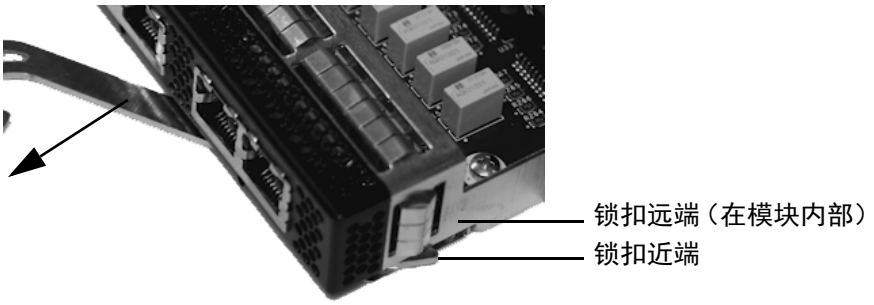
卸下现有模块或插槽盖以准备新模块的插槽。有关详细信息，请参阅第 238 页的卸下模块或插槽盖。

要插入模块或插槽盖：

1. 使用随附的螺丝刀，从模块拉杆上卸下并保留 T8 梅花头螺钉。

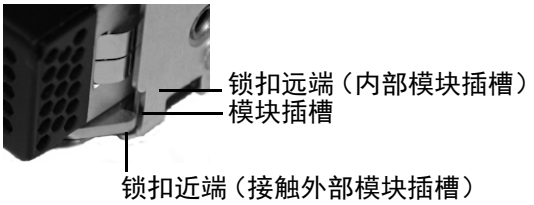


2. 将拉杆拉离模块以打开锁扣。锁扣的近端可见。锁扣的远端在模块内部。

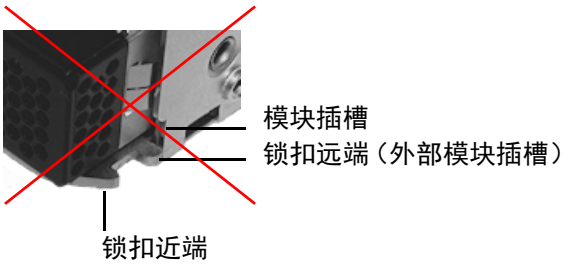


3. 将模块插入插槽，直至锁扣的远端在插槽内，锁扣的近端触及模块插槽的外侧。

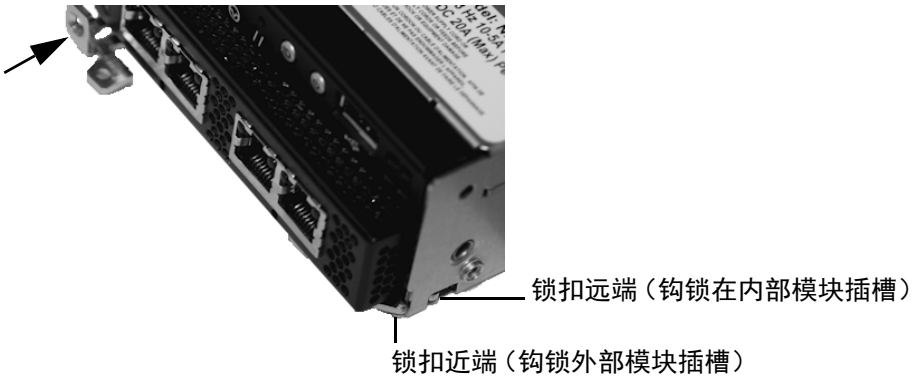
正确的模块对齐



不正确的模块对齐

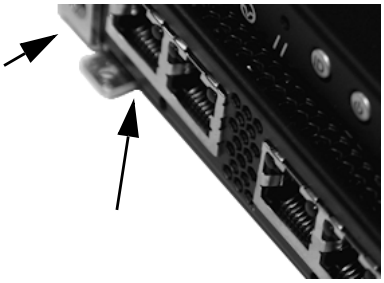


4. 将拉杆推向模块，以便锁扣锁紧并将模块推入插槽。

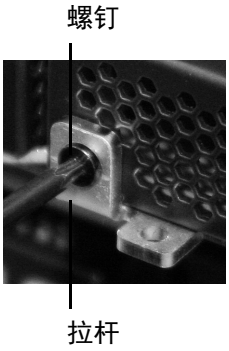


警告！请**不要**用力过大。如果锁扣未锁紧，请卸下并重新对齐模块，然后重试。

5. 用力按压螺孔，使拉杆完全紧贴模块以固定锁扣。
   拉杆完全紧贴模块，并且模块与机箱齐平。



6. 将预留的 T8 梅花头螺钉插入拉杆并拧紧。



附录 D
预配置 SOURCEFIRE 设备

可在*试运行*位置 （预配置或准备多台设备的一个中心位置）预配置要在*目标*位置（除试运行位置外的任何位置）部署的设备 （防御中心或设备）。

要预配置设备并将其部署至目标位置，请执行以下步骤：

- 在试运行位置将系统安装在设备上
- 或者，向防御中心注册设备
- 或者，将所有更新从管理防御中心推送至设备
- 或者，从防御中心取消注册设备
- 关闭设备并将其装运到目标位置
- 在目标位置部署设备

有关详细信息，请参阅以下各节：

- 第 243 页的准备工作
- 第 244 页的安装系统
- 第 244 页的注册设备
- 第 245 页的准备装运设备
- 第 247 页的设备预配置故障排除

提示！ 在重新包装设备时，请保留所有包装材料并包括所有参考资料和电源线。

准备工作

在预配置设备之前，收集网络设置、许可证和其他相关信息以备在试运行位置和目标位置使用。

提示！ 在试运行位置和目标位置创建电子表格管理此信息可能会非常有用。

在初始设置期间，使用足够信息配置设备以将设备连接到网络并安装系统。或者，可将设备连接到防御中心以将所有更新从防御中心推送至设备。还可启用其他初始设置不需要但对预配置可能有用的功能。有关详细信息，请参阅以下各节：

- 第 243 页的必需的预配置信息
- 第 243 页的可选预配置信息
- 第 244 页的预配置时间管理

必需的预配置信息

预配置设备至少需要以下信息：

- 新密码 （初始设置要求更改密码）
- 设备的主机名
- 设备的域名
- 设备的 IP 管理地址
- 设备在目标位置的网络掩码
- 设备在目标位置的默认网关
- 试运行位置或目标位置 （如果可访问）的 DNS 服务器的 IP 地址
- 试运行位置或目标位置 （如果可访问）的 NTP 服务器的 IP 地址
- 目标位置的检测模式

可选预配置信息

可更改某些默认配置，例如：

- 允许访问 LCD 面板以配置设备 （仅 3 系列受管设备）
- 设置时区 （如果选择为设置设置时间）
- 为自动备份设置远程存储位置
- 设置 3 系列设备上的无人值守管理 (LOM) IP 地址，以在设备上启用 LOM

如果要将设备注册至防御中心，则需要以下信息：

- 受管设备的名称或 IP 地址
- 管理主机 （防御中心）的名称
- 注册密钥 （个人创建的唯一字母数字密码，最大长度 37 个字符）

预配置时间管理

请记住以下注意事项：

- Sourcefire 建议与物理 NTP 服务器同步时间。请勿使受管设备与虚拟防御中心同步。虚拟设备上的性能优化可能影响实时时钟。
- 如果试运行位置的网络可访问目标位置的 DNS 和 NTP 服务器，请使用目标位置的 DNS 和 NTP 服务器的 IP 地址。否则，请使用试运行位置的信息，并在目标位置重置。
- 如将设备上的时间设置为手动 （而不是使用 NTP），请使用目标部署的时区。请参阅第 87 页的时间设置。

安装系统

使用第 52 页的安装 Sourcefire 3D 系统设备和第 77 页的设置Sourcefire 3D 系统设备中描述的安装操作步骤。在预配置系统时，请记住以下要点：

- 在 3 系列设备上，如果允许使用 LCD 面板访问设备的网络设置，则会引入通过物理方式访问设备进行未经授权的更改的安全风险。请参阅第 86 页的3 系列设备 LCD 面板配置。
- 使用目标部署中防御中心的主机名和 IP 地址预注册设备。请记住注册密钥以便将来完成注册。请参阅第 86 页的远程管理。
- 如果更改默认检测模式，请务必通知目标部署的适当人员。从检测模式以不同方式配置各接口可能导致系统不正确地分配接口。请参阅第 87 页的检测模式。
- 如果需要为设备配置网络地址转换 (NAT)，在使用设备上 （仅限于 3 系列设备）上的 CLI 或其管理防御中心上的网络界面注册设备时，请提供设备的 NAT ID。请参阅第 83 页的使用 CLI 将 3 系列设备注册至防御中心和《*Sourcefire 3D 系统用户指南*》中的“在 NAT 环境中工作”。
- 在初始设置期间添加许可证。如果此时未添加许可证，您在初始设置期间注册的所有设备将作为未授权设备添加到防御中心； 在初始设置过程结束后，您必须逐个为它们添加许可证。请参阅第 93 页的许可设置。

注册设备

如果防御中心运行的软件版本大于或等于设备上运行的软件版本，可以向防御中心注册设备以向受管设备推送策略和更新。

重要！ 如果将防御中心及其受管设备部署在不同的位置，则必须先从防御中心删除该设备，然后再关闭该设备。请参阅第 245 页的从防御中心删除设备。

要将设备注册至防御中心，请执行以下操作：

1. 在设备上，使用在目标部署中防御中心的主机名或 IP 地址配置远程管理。请记住注册密钥以便将来完成注册。请参阅第 86 页的远程管理。

   重要！ 您必须首先在设备上配置远程管理，然后才能向防御中心注册设备。

2. 在防御中心上，使用远程管理配置中的注册信息注册设备。请参阅第 95 页的设备注册。

准备装运设备

要准备装运设备，必须安全关闭设备电源并重新包装设备：

- 如果防御中心和受管设备将不用于目标位置的同一配置，则必须从防御中心删除设备，然后关闭设备电源并重新包装设备。请参阅第 245 页的从防御中心删除设备。
- 要安全关闭设备，请参阅第 246 页的关闭设备电源。
- 要确保设备已安全做好装运准备，请参阅第 246 页的装运注意事项。

从防御中心删除设备

除非在同一目标位置部署防御中心及其受管设备，否则，必须从防御中心删除设备。当向目标位置的不同防御中心注册设备时，这可防止设备查找原始防御中心的 UUID。

要从防御中心删除设备，请执行以下操作：

1. 在防御中心上，选择 **Devices > Device Management**。

   系统将显示 Device Management 页面。

2. 点击要删除的设备旁边的删除图标 ( )。

   出现提示时，请确认要删除设备。设备与防御中心之间的通信断开，并且设备从 Device Management 页面被删除。如果设备有一个系统策略使其通过 NTP 从防御中心接收时间，则设备将恢复为本地时间管理。

从防御中心删除设备后，确认设备未由防御中心远程管理。

要确认设备不受防御中心管理，请执行以下操作：

▶ 在受管设备上，可使用网络界面或 CLI：

- 在受管设备的网络界面上，转到 **System > Local > Registration > Remote Management** 并确认 Remote Management 屏幕上的 Host 列表为空。
- 在受管设备上的 CLI 上，运行命令 `show manager` 并确认未显示任何主机。

删除许可证防御中心

如果由于任何原因需要删除许可证，请执行以下操作步骤。请记住，因为 Sourcefire 根据每个防御中心的唯一许可证密钥生成许可证，所以，您无法从一个防御中心删除许可证，然后在不同防御中心上重复使用该许可证。有关详细信息，请参阅《*Sourcefire 3D 系统用户指南*》中的“为 Sourcefire 3D 系统获得许可证”。

要删除许可证，请执行以下操作：

1. 选择 **Systems > Licenses**。

   系统将显示 License 页面。

2. 点击要删除的设备旁边的删除图标 ( )。

   删除许可证将从使用该许可证的所有设备移除已许可的功能。例如，如果您的 Protection 许可证有效，并且已对 100 台受管设备启用，删除该许可证会从所有 100 台设备上移除保护功能。

3. 确认要删除许可证。

   许可证删除成功。

关闭设备电源

遵循以下操作步骤在断开电源之前安全关闭设备电源。

要关闭设备电源，请执行以下操作：

▶ 在防御中心上，在命令行中输入以下命令：

```
sudo shutdown -h now
```

防御中心安全关闭。

▶ 在设备上，在命令行中输入以下命令：

```
system shutdown
```

设备安全关闭。

装运注意事项

要准备将设备装运至目标位置，必须安全关闭设备电源并重新包装设备。请记住以下注意事项：

- 使用原始包装重新包装设备。
- 将所有参考资料和电源线随设备一起包装。
- 保护网络模块和 SFP，防止因不当操作或过大压力而导致的损坏。
- 向目标位置提供所有设置和配置信息，包括新密码和检测模式。

设备预配置故障排除

如果已为目标部署正确预配置设置，则无需进一步配置，即可安装和部署设备。

如果无法登录设备，则预配置可能有错误。请尝试以下故障排除操作步骤：

- 确认所有电源线和通信线缆正确连接至设备。
- 确认您有设备的当前密码。在试运行位置进行的初始设置将提示您更改密码。请在试运行位置提供的配置信息中查找新密码。
- 确认网络设置正确。请参阅第 84 页的初始设置页面：设备和第 89 页的初始设置页面：防御中心：
- 确认正确的通信端口正在正常运行。请参阅防火墙文档，了解有关管理防火墙端口的信息。请参阅第 24 页的打开通信端口要求，了解需要打开的端口。
- 如在部署中使用网络地址转换 (NAT) 设备，请确认已正确配置该 NAT。请参阅 《*Sourcefire 3D 系统用户指南*》中的“在 NAT 环境中工作”。

如果问题依然存在，请与 IT 部门联系。

术语表

2 系列	Sourcefire 设备型号的第二个系列。由于资源、架构和许可的限制， 2 系列设备支持有限的 Sourcefire 3D 系统功能集。 2 系列设备包括 3D500、 3D1000、3D2000、3D2100、3D2500、3D3500、3D4500、3D6500 和 3D9900。2 系列防御中心包括 DC500、 DC 1000 和DC 3000。
3 系列	Sourcefire设备型号的第三个系列。3 系列设备包括 7000 系列和 8000 系列设备，以及 DC750、 DC1500 和 DC3500 防御中心。
7000 系列	一组 3 系列 Sourcefire 受管设备。该系列设备包括 70xx 系列（3D7010、3D7020 和 3D7030 型号）以及 71xx 系列 （3D7110、 3D7115、 3D7120、 3D7125 和 AMP7150 型号）。
8000 系列	一组 3 系列 Sourcefire 受管设备。该系列设备包括 81xx 系列 （3D8120、3D8130、3D8140 和 AMP8150 型号）、82xx 系列（3D8250、3D8260、3D8270 和 3D8290 型号）以及 83xx 系列 （3D8350、 3D8360、 3D8370 和 3D8390 型号）。 8000 系列设备的功能通常比 7000 系列设备的功能更强大。
CLI	请参阅命令行界面。

术语表

Context Explorer	一个页面，使用入侵、连接、文件、地理定位、恶意软件和发现策略显示受监控网络的详细交互式图形化信息。各个不同部分以生动的曲线图、条形图、饼图和环形图展示信息，并配有详细列表。可轻松创建和应用自定义过滤器以优化您的分析，且可更详细地检查数据部分，只需点击图形区域或将鼠标指针悬停在图形区域上方。与高度可自定义、已划区且实时更新的控制面板相比， Context Explorer 手动更新，旨在为其数据提供更广泛的上下文，拥有专为活跃用户探索设计的单一且一致的布局。
eStreamer	Sourcefire 3D 系统的一个组件，可供您将事件数据从防御中心或受管设备流式传输至外部客户端应用。
FireAMP	Sourcefire 的企业级基于终端的高级恶意软件分析和防护解决方案，它能够发现、了解和阻止恶意软件爆发、持久威胁和针对性攻击。如果贵组织有 FireAMP订用，个别用户在终端 （计算机、移动设备）上安装轻量级 FireAMP 连接器，则该连接器将与 Sourcefire 云通信。这样，您就可快速识别和隔离恶意软件，以及在恶意软件爆发时识别出爆发事件、跟踪其轨迹、了解其影响和了解如何成功恢复。还可使用 FireAMP 门户网站创建自定义防护、阻止执行某些应用以及创建自定义白名单。与基于网络的高级恶意软件防护比较。
FireAMP 连接器	一种轻量级代理，在基于订用的 FireAMP 部署中，用户可以在终端 （例如，计算机和移动设备）上安装此连接器。连接器与 Sourcefire 云通信，交换信息以便您在整个贵组织中快速识别和隔离恶意软件。
FireAMP订用	一种单独购买的订用，允许贵组织使用 FireAMP 作为高级恶意软件防护 (AMP) 解决方案。与恶意软件许可证比较，可在受管设备上启用此解决方案以执行基于网络的 AMP。
FireAMP门户网站	网站 http://amp.sourcefire.com/，在该网站上可配置贵组织的基于订用的 FireAMP 部署。
FireSIGHT 许可证	防御中心上的默认许可证，可供您执行主机、应用和用户发现。 FireSIGHT 许可证还确定可使用防御中心及其受管设备监控多少个主机和用户，以及可在访问控制规则中用于执行用户控制的访问受控用户的数量。
GeoDB	请参阅地理定位数据库。
LDAP 身份验证	一种外部身份验证形式，通过将用户凭证与 LDAP 目录服务器上存储的轻量级目录访问协议 (LDAP) 目录比较来验证该用户凭证。
NAT	网络地址转换，一项在专用网络上的多个主机之间共享单个互联网连接时最常使用的功能。借助于发现，系统可将网络设备识别为逻辑接口。此外，在 Sourcefire 3D 系统的第 3 层部署中，可通过 NAT 策略配置与 NAT 的路由。
NAT 策略	使用 NAT 规则执行与 NAT 的路由的策略。

RADIUS 身份验证	远程身份验证拨入用户服务，该服务用于对用户访问网络资源进行身份验证、授权和追责。可创建外部身份验证对象以允许 Sourcefire 3D 系统用户通过 RADIUS 服务器进行身份验证。
SFP 模块	插入71xx 系列设备上的网络模块中的小型可插拔收发器。 SFP 模块上的感知接口不支持可配置旁路。
Sourcefire VRT	Sourcefire 的漏洞研究团队。
Sourcefire 情报源	由 Sourcefire VRT 确定的信誉不佳的定期更新的 IP 地址列表集合。源中的每个列表均表示特定类别：开放中继、已知攻击者和假冒 IP 地址 (bogon) 等。在访问控制策略中，您使用安全情报将任何或所有类别列入黑名单。由于情报源将定期更新，使用它可确保系统使用最新信息过滤网络流量。
Sourcefire 云	有时也被称为*云服务*，一个 Sourcefire 托管的外部服务器，防御中心可从其获得最新相关信息，包括恶意软件、安全情报和 URL 过滤数据。另请参阅恶意软件云查找。
URL 过滤	一项功能，可供您编写访问控制规则，这些规则根据受监控主机请求的 URL，同时结合与这些 URL 关联的 URL 类别和 URL 信誉信息 （由防御中心从 Sourcefire 云获得）确定流量是否可以穿越网络。可实现对网络流量的更细化的自定义控制，只需指定允许通过或阻止的单一 URL 或 URL 组。
URL 过滤许可证	可供您根据 URL 类别和 URL 信誉信息执行 URL 过滤的许可证。 URL 过滤许可证可能会过期。
URL 类别	URL 的一般分类，例如，恶意软件或社交网络。
UTC 时间	协调世界时。也称为格林尼治标准时间 (GMT)，UTC 是世界各地通用的标准时间。Sourcefire 3D 系统使用 UTC，然而可使用时区功能设置本地时间。
VDB	请参阅漏洞数据库。
VLAN	虚拟局域网。 VLAN 不是通过地理位置而是通过某些其他标准 （例如，按部门或主要用途）来映射主机。受监控主机的主机配置文件显示与该主机关联的任何 VLAN 信息。VLAN 信息也包括在入侵事件中，作为触发事件的数据包中最内部的 VLAN 标记。您可以按 VLAN 过滤入侵策略，还可以按 VLAN 确定合规性白名单的目标。在第 2 层和第 3 层部署中，您可以配置受管设备上的虚拟交换机和虚拟路由器以妥善处理标有 VLAN 的流量。
VPN	一项功能，可供您构建 Sourcefire受管设备上的虚拟路由器之间或从受管设备到远程设备或其他第三方 VPN 终端的安全 VPN 隧道。
VPN 许可证	一种许可证，可供您构建 Sourcefire受管设备上的虚拟路由器之间或从受管设备到远程设备或其他第三方 VPN 终端的安全 VPN 隧道。

术语表

VRT	请参阅Sourcefire VRT。
安全策略	组织的网络保护准则。例如，您的安全策略可能禁止使用无线接入点。安全策略还包括可接受的使用策略 (AUP)，该策略针对员工如何使用其组织的系统提供了相关准则。
安全策略违例	网络中的安全漏洞、攻击、漏洞攻击或其他滥用。
安全情报	一种可供您根据源或目标 IP 地址按访问控制策略指定可穿越网络的流量的功能。如果要在访问控制规则对流量进行分析之前将其加入黑名单 （拒绝发往和来自特定 IP 地址的流量），此功能尤其有用。或者，您可以使用监控设置执行安全情报过滤，这不仅使系统分析应该已列入黑名单的连接，同时将匹配项记入黑名单。
安全情报列表	您手动上传至防御中心作为安全情报对象的 IP 地址的简单静态集合。使用列表扩充和优化安全情报源以及全局黑名单和全局白名单。
安全情报源	一种安全情报对象类型，系统按您配置的间隔定期下载的 IP 地址的动态集合。由于源会定期更新，借助于它们，可确保系统通过安全情报功能使用最新信息过滤网络流量。另请参阅Sourcefire 情报源。
安全区域	由一个或多个内联、被动、交换或路由接口组成的一组接口，可用于在各种策略和配置中管理和分类流量。单个区域中的接口可以跨多个设备；还可在单个设备上配置多个安全区域。必须将配置的每个接口分配至安全区域，然后它才能处理流量，并且每个接口只能属于一个安全区域。
保护许可证	3 系列和虚拟设备的许可证可供您执行入侵检测和防御、文件控制和安全情报过滤。在无许可证的情况下， 2 系列设备自动具有除安全情报外的保护功能。
被动检测	对受管设备以被动方式收集的流量进行分析的发现策略的集合。与活动检测比较。
被动接口	配置的用于分析被动部署中的流量的感知接口。
表视图	一种显示事件信息的工作流程页面类型，每一列对应于数据库表中的一个字段。执行事件分析时，在转至表视图之前，您可使用向下钻取页面限制要调查的事件，表视图仅显示有关您感兴趣的事件的详细信息。表视图通常是系统提供的工作流程中的倒数第二个页面。
补救措施	缓解系统上潜在攻击的操作。可配置补救措施，并在关联策略内将其与关联规则和合规性白名单相关联，这样，当它们触发时，防御中心就会启动补救措施。这不仅将在您无法立即解决网络攻击问题时自动缓解攻击，还能确保系统符合贵组织的安全策略。防御中心配有预定义的补救措施模块，您也可以使用灵活的 API 创建自定义补救措施。
策略	一种设置应用机制，最常应用于设备。请参阅访问控制策略、关联策略、文件策略、健康策略、入侵策略、网络发现策略和系统策略。

术语表

层	入侵策略中的一整套入侵规则、预处理程序规则和高级设置配置。可将自定义用户层添加至策略中的一个或多个内置层。入侵策略中较高层的设置将覆盖较低层的设置。
导入	可用于将各种配置从设备传输到设备的一种方法。可导入之前从另一台同类型设备导出的配置。
地理定位	一种功能，该功能提供可路由 IP 地址 （在受监控网络上的流量中检测）的地理来源数据。可查看存储在地理定位数据库中的地理定位信息，也可以查看连接事件、入侵事件、文件事件和恶意软件事件事件以及主机配置文件中的地理定位信息。
地理定位数据库	也称为 GeoDB，一个包含与可路由 IP 地址关联的已知地理定位数据的定期更新的数据库。
堆栈	两台到四台共享检测资源的已连接设备。
堆栈	一项功能，可供您通过在堆栈配置中连接两到四台物理设备增加在网段上检测的流量。建立堆栈配置时，您将每个堆栈设备的资源合并至单个共享配置。
恶意软件防护	请参阅高级恶意软件防护。
恶意软件检测	Sourcefire 的基于网络的高级恶意软件防护 (AMP) 解决方案的一个组件。在访问控制整体配置中，应用于受管设备的文件策略会检查网络流量。作为检查网络流量的整体配置的一部分应用于受管的文件策略。然后，防御中心对特定的检测到的文件类型执行恶意软件云查找并生成事件，提醒您文件的恶意软件性质。随后 AMP 恶意软件阻止将起作用并阻止该文件或允许其上传或下载。将此功能与 FireAMP 订用 （FireAMP 的需要 Sourcefire 的基于终端的 AMP 工具）比较。
恶意软件事件	由 Sourcefire 的其中一个高级恶意软件防护解决方案生成的事件。当 Sourcefire 云返回在网络流量中检测到的文件的恶意软件性质时生成基于网络的恶意软件事件。与基于终端的恶意软件事件对照 （当部署的 FireAMP 连接器检测到威胁、会生成恶意软件事件），后者能阻止恶意软件执行，或隔离或无法隔离恶意软件。
恶意软件许可证	可供您在网络流量中执行高级恶意软件防护 (AMP) 的许可证。借助于文件策略，您可配置系统，使其对由受管设备检测到的特定文件类型执行恶意软件云查找。与 FireAMP订用比较。
恶意软件云查找	一种特殊流程，防御中心据此与 Sourcefire 云以根据文件的 SHA-256 哈希值确定网络流量中检测到的文件的恶意软件性质.
恶意软件阻止	Sourcefire 的基于网络的高级恶意软件防护 (AMP) 解决方案的一个组件。在恶意软件检测确定检测文件的性质为恶意软件后，您可以阻止该文件或允许其上传或下载。将此功能与 FireAMP订用 （FireAMP 的需要 Sourcefire 的基于终端的 AMP 工具）比较。

术语表

发现	Sourcefire 3D 系统的一个组件，该组件使用受管设备监控网络并提供完整的连续性网络视图。网络发现确定网络上主机 （包括网络设备和移动设备）的数量和类型，以及有关这些主机上的操作系统、活跃应用和开放端口的信息。还可将 Sourcefire 受管设备配置为监控网络上的用户活动，这使您能够识别策略违反、攻击或网络漏洞的来源。
发现策略	请参阅网络发现策略。
防御中心	一个中心管理点，可供您管理设备并自动整合和关联它们生成的事件。
访问控制	Sourcefire 3D 系统的一项功能，您可利用此项功能指定、检查和记录可穿越网络的流量。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功能，并确定可使用发现功能检查的流量。
访问控制策略	您应用于受管设备以对这些设备监控的网络流量执行访问控制的策略。访问控制策略可包括多个访问控制规则；它还指定默认操作，此操作确定如何处理和记录不符合任何这些规则之条件的流量。访问控制策略还可指定 HTTP 响应页面、安全情报以及其他高级设置。
访问控制规则	一组 Sourcefire 3D 系统用于检查受监控网络流量并让您能够实现精细访问控制的条件。填充访问控制策略的访问控制规则，可执行简单的 IP 地址匹配，也可表示涉及不同用户、应用、端口和 URL 的复杂连接的特性。访问控制规则操作确定系统如何处理符合规则条件的流量。其他规则设置确定如何 （和是否）记录连接，以及入侵策略或文件策略是否检查匹配的流量。
访问列表	在系统策略中配置的 IP 地址列表，代表可访问设备的主机。默认情况下，任何人均可使用端口 443 (HTTPS) 访问设备的网络界面，还可使用端口 22 (SSH) 访问命令行。也可使用端口 161 添加 SNMP 访问。
非旁路模式	内联集的一个特性，在该内联集中的感知接口因任何原因发生故障时，阻止流量。
分路模式	3D9900 和 3 系列设备上提供的一个高级内联集选项，可对每个数据包的副本进行分析，网络流量无需通过设备，因此不会受到干扰。由于您处理的是数据包的副本而不是数据包，因此设备无法影响数据包流，即使您将访问控制和入侵策略配置为丢弃、修改或阻止流量。
服务器	安装在主机上的服务器应用 （与客户端应用比较），通过应用协议流量识别。
感知接口	设备上用于监控网段的网络接口。与管理界面比较。
高级恶意软件防护	缩写形式为 AMP，表示 Sourcefire 3D 系统的基于网络的恶意软件检测和恶意软件云查找功能。将此功能与 FireAMP订用 （FireAMP 的需要 Sourcefire 的基于终端的 AMP 工具）比较。
高级设置	配置时需要特定专业知识的预处理程序或其他入侵策略功能。高级设置通常不需要或仅需很少的修改，且并非每个部署通用。

术语表

高可用性	一项功能，可供您配置冗余物理防御中心来管理一组设备设备。事件数据将从受管设备流式传输至两个防御中心，并且大多数配置元素在两个防御中心上同时维护。如果主防御中心发生故障，则可使用辅助防御中心监控网络，不会发生中断。与集群相比，高可用性可供您指定冗余设备。
告警	表明系统已生成特定事件的通知。可基于以下对象发出告警：入侵事件 （包括其影响标志）、发现事件、恶意软件事件、关联策略违反，运行状态变化和特定访问控制规则记录的连接。在大多数情况下，可以通过邮件、系统日志或 SNMP 陷阱发出告警。
构件	请参阅控制面板构件。
关联	一种可用于构建实时响应网络威胁的关联策略的功能。关联的补救措施组件提供灵活的 API，可供您创建和上传自己的自定义补救措施模块以应对策略违规
管理界面	用于管理 Sourcefire 3D 系统 设备的网络界面。在大多数部署中，管理接口连接至内部受保护的网络。与感知接口比较。
规则	通常用于策略中的一种结构，它提供检查网络流量时所依据的条件。
规则操作	确定系统如何处理符合规则条件的网络流量的设置。请参阅访问控制规则和文件规则操作。
规则更新	按需入侵规则更新，包含新的和更新的标准文本规则、共享对象规则和预处理程序规则。规则更新还可以删除规则、修改默认入侵策略设置以及添加或删除系统变量和规则类别。
规则状态	在入侵策略中入侵规则为启用 （设置为 Generate Events 或 Drop and Generate Events）还是禁用 （设置为 Disable）。如果启用规则，则将它用于评估网络流量；如果禁用规则，则不会使用该规则。
混合接口	受管设备上的逻辑接口，可供系统桥接虚拟路由器与虚拟交换机之间的流量。
集群	可供您在两个对等 3 系列设备或堆栈之间实现网络功能和配置数据冗余的功能。集群为策略应用、系统更新和注册提供了单个逻辑系统。与高可用性对照，后者其可供您配置冗余防御中心。
监控	在访问控制策略中使用的一种方法，它记录匹配安全情报黑名单或访问控制规则的流量，但允许系统继续评估流量，而不是立即允许或阻止该流量。
健康策略	检查部署中设备的运行状况时使用的条件。健康策略使用运行状况模块来指示 Sourcefire 3D 系统硬件和软件是否正常工作。可使用默认健康策略或创建自己的健康策略。
交换机	充当多端口网桥的网络设备。系统使用网络发现将交换机标识为网桥。此外，还可将受管设备配置为虚拟交换机，执行两个或更多网络之间的数据包交换。

术语表

交换接口	您要用于在第 2 层部署中交换流量的接口。可设置用于处理未标记 VLAN 流量的物理交换接口，和用于处理具有指定 VLAN 标记的流量的逻辑交换接口。
解码器	入侵检测和防御的一个组件，将嗅探过的数据包转换为预处理程序能够理解的某种格式。
可配置旁路	内联集的一项特征，可供您配置旁路模式。
客户端	也称为客户端应用，运行在一个主机上并依赖另一个主机 （一个服务器）以执行某些操作的应用。例如，邮件客户端可供您收发邮件。当系统检测到主机上的用户正在使用特定客户端访问另一个主机时，系统会在主机配置文件和网络映射中报告该信息，包括该客户端的名称和版本 （如可用）。
客户端应用	请参阅客户端。
控制面板	一个显示页面，提供当前系统状态的概览视图，包括关于系统收集和生成的事件的数据。为了扩充随系统提供的控制面板，可创建多个自定义控制面板，并选择控制面板构件来填充这些控制面板。与 Context Explorer 对照，后者可提供大量有关受监控网络的外观和运行状况的简洁且色彩丰富的视图。
控制面板构件	一种小型独立的控制面板组件，可提供有关 Sourcefire 3D 系统某个方面的洞察。
控制许可证	可供您实施应用和访问控制规则的许可证，只需将用户和用户控制条件添加至应用控制。它也可供您配置受管设备以执行交换和路由 （包括 DHCP 中继和 NAT），以及集群受管设备。
快速路径规则	您在设备的硬件层面配置的一种规则，该规则使用有限的一组条件，允许不需要分析的流量绕过处理。
连接	两个主机之间的受监控会话。可记录访问控制策略中的受管设备检测到的连接；可配置网络发现策略中记录的网络模块连接。 号或监控风扇速度和温度等运行状况。
链路状态传播	适合旁路模式下内联集的一个选项，它在内联集的其中一个接口发生故障时自动关闭接口对中的备用接口。当故障接口恢复时，备用接口也将自动恢复。换句话说，如果配对接口的链路状态发生变化，另一个接口的链路状态也会自动变化以与其匹配。
列表	请参阅安全情报列表。
漏洞	主机易遭受的特定危害的描述。防御中心在每个主机的主机配置文件中提供了有关该主机易受攻击的漏洞的信息。此外，还可使用漏洞网络映射获取针对系统在整个受监控网络上检测到的漏洞的总体视图。如果您认定一台或多台主机不再易于遭受特定危害，则可停用特定漏洞或将其标记为无效。

漏洞数据库	也称为 VDB，主机可能易受攻击的已知漏洞的数据库。系统将在每台主机上检测到的操作系统、应用协议和客户端与 VDB 关联，以帮助您确定特定主机是否会增加网络受危害的风险。 VDB 更新可包含新的和更新的漏洞，以及新的和更新的应用检测器。
路由接口	第 3 层部署中对流量进行路由的接口。您可设置用于处理未标记 VLAN 流量的物理路由接口，和用于处理具有指定 VLAN 标记的流量的逻辑路由接口。也可将静态地址解析协议 (ARP) 条目添加至路由接口。
路由器	位于网关上的一台网络设备，负责在网络之间转发数据包。系统可以使用网络发现标识路由器。此外，还可将受管设备配置为对两个或更多接口之间的流量进行路由的虚拟路由器。
逻辑接口	一种虚拟子接口，定义用于在具有特定 VLAN 标记的流量通过物理接口时，对这类流量进行处理。
命令行界面	3 系列和虚拟设备上受限的基于文本的界面。 CLI 用户可运行的命令取决于分配给用户的访问级别。
默认操作	作为访问控制策略的一部分，确定如何处理不符合策略中任何规则条件的流量。当您应用不包含任何访问控制规则或安全情报设置的访问控制策略时，默认策略操作确定如何处理网络上不使用快速路径的流量。可将默认操作设置为阻止或信任流量而不进行进一步检查，或者使用网络发现策略或入侵策略对其进行检查。
内联部署	一种 Sourcefire 3D 系统部署，在此类部署中受管设备在网络上处于内联模式。在此配置中，设备可使用交换、路由、访问控制和入侵检测和防御影响网络流量。
内联集	一个或多个内联接口对。
内联接口	配置为处理内联部署中的流量的感知接口。必须将内联接口成对添加至内联集。
旁路模式	内联集的一种特性，当该内联集中的感知接口由于任何原因发生故障时，允许流量继续通过。
区域	请参阅安全区域。
任务队列	设备需要执行的作业队列。当您应用一个策略、安装软件更新和执行其他长期作业时，作业将排队并在 Task Status 页面上报告其状态。 Task Status 页面提供详细的作业列表并每隔十秒刷新它们的状态。
入侵	在您的网络中出现的安全违反、攻击或漏洞攻击。

术语表

入侵策略	可将其配置为检查网络流量中的入侵和安全策略违规的各种组件。这些组件包括的入侵规则检查协议报头值、负载内容和某些数据包大小特性；入侵规则中的常用变量；FireSIGHT 建议的规则配置；诸如预处理程序和其他检测和性能功能等高级设置；以及可供您为关联的预处理程序选项生成事件的预处理程序规则。当网络流量符合访问控制规则中的条件时，可使用入侵策略检查流量；还可将入侵策略与默认操作关联。
入侵规则	一组关键字和参数，应用至受监控网络流量后可识别潜在的入侵、安全策略违规和安全漏洞。系统将数据包与规则条件相比较。如果数据包数据匹配条件，规则触发并生成入侵事件。入侵规则包括丢弃规则和通过规则。
入侵检测和防御	监控网络流量中的安全策略违规和 （在内联部署中）阻止或修改恶意流量的能力。在 Sourcefire 3D 系统中，当您将入侵策略与访问控制规则或默认操作相关联时，即可执行入侵检测和防御。
入侵事件	记录入侵策略违规的事件。入侵事件数据包括漏洞攻击的日期、时间和类型，以及有关攻击及其目标的其他情景信息。
上下文菜单	一种在网络界面的许多页面上提供的弹出菜单，可用作访问 Sourcefire 3D 系统中其他功能的快捷方式。该菜单的内容取决于多种因素，包括正在查看的页面，正在调查的特定数据和您的用户角色。上下文菜单选项包括入侵规则、事件和主机信息的链接；各种入侵规则设置， Context Explorer 快速链接；按主机的 IP 地址将其加入安全情报全局黑名单或全局白名单的选项；以及按文件的 SHA-256 哈希值将其添加至全局白名单的选项。
设备	防御中心或受管设备。设备可以是物理或虚拟设备。
设备	有多种吞吐量选择且具有容错能力的专用设备。可使用它们被动监控流量以构建网络资产、应用流量和用户活动的综合映射，执行入侵检测和防御，执行访问控制以及配置交换和路由，具体取决于您在设备上启用的已许可功能。您必须使用防御中心来管理设备。
设备堆栈	请参阅堆栈。
设备集群	请参阅集群。
事件	有关出现的特定状况的详细信息的集合，可使用工作流程在事件查看器中查看事件。事件可以表示网络上的攻击、检测到的网络资产的变化以及对贵组织的安全和网络使用策略的违反等。系统还生成包含以下信息的事件：有关设备的不断变化的运行状态、对网络界面的使用情况、规则更新和启动的补救措施的信息。最后，系统还将某些其他信息呈现为事件，即使这些“事件”不代表特定状况。例如，可使用事件查看器查看有关所检测到的主机、应用及其漏洞的详细信息。
事件查看器	系统的一个组件，可供您查看并操作事件。事件查看器使用工作流程先呈现一个宽泛的事件视图，随后呈现一个仅包含您感兴趣的事件的更精细化事件视图。可通过向下钻取工作流程或使用搜索来限制事件视图中的事件。

术语表

事件流化器	请参阅eStreamer。
受保护的网络	贵组织的内部网络，使用诸如防火墙之类的设备防御其他网络用户的攻击。随 Sourcefire 3D 系统提供的许多入侵规则使用变量定义受保护网络和未受保护的（或外部）网络。
受管设备	请参阅设备。
数据库访问	一种功能，允许第三方客户端对防御中心数据库进行只读访问。
调度的任务	可调度运行一次或按一定间隔重复运行的管理任务。
透明内联模式	一个高级内联集选项，可使设备充当“网络嵌入式配置 (bump in the wire)”并转发检测到的所有网络流量，不论其来源和目标如何。
网络发现	请参阅发现。
网络发现策略	指定系统针对特定网段收集的发现策略种类 （包括主机、用户和应用数据）的策略，包括支持网络模块的设备所监控的网络。网络发现策略还可管理导入解析首选项和活动检测源优先级。
网络模块	您在受管设备的机箱中安装的一个模块，该模块包含该设备的感知接口。
网络设备	在 Sourcefire 3D 系统中，被识别为网桥、路由器、 NAT 设备或逻辑接口的主机。
网络文件轨迹	主机在整个网络中传输文件的轨迹的直观再现。对于有关联 SHA-256 哈希值的任何文件，轨迹图显示已传输该文件的所有主机的 IP 地址、检测文件的时间、文件的恶意软件性质、关联的文件事件和恶意软件事件等。
网络应用	一种应用类型，代表 HTTP 流量的内容或请求的 URL。
网络映射	网络的详细再现。通过网络映射，可查看有关网络上运行的主机、移动设备和网络设备的网络拓扑，以及关联的主机属性、应用协议和漏洞。
文件策略	系统用于执行文件控制和高级恶意软件防护的策略。文化策略由文件规则填充，由访问控制策略中的访问控制规则调用。
文件轨迹	请参阅网络文件轨迹。
文件控制	访问控制的一项功能，可供您指定和记录可穿越网络的文件类型。
文件类型	文件格式的特定类型，例如， PDF、 EXE 或 MP3。
无人值守管理 (LOM)	一项 3 系列功能，可供您使用带外局域网串行 (SOL) 管理连接远程监控或管理设备，而无需登录该设备的网络界面。您可执行有限的任务，例如，查看机箱序列
物理接口	代表网络模块上的物理端口的接口。

术语表

系统策略	对于部署中的多个设备可能类似的设置，例如，邮件中继主机首选项和时间同步设置。使用防御中心将系统策略应用至其自身及其受管设备。
信誉 （IP 地址）	请参阅安全情报。
虚拟防御中心	您可在处于虚拟托管环境中的自己的设备上部署的防御中心。
虚拟交换机	处理网络上的入站和出站流量的一组交换接口。在第 2 层部署中，可将受管设备上的虚拟交换机配置为充当独立广播域，将网络划分为多个逻辑网段。虚拟交换机使用来自主机的媒体访问和控制 (MAC) 地址确定接收数据包的目标。
虚拟路由器	对第 3 层流量进行路由的一组路由接口。在第 3 层部署中，可将虚拟路由器配置为根据目标 IP 地址做出数据包转发决策，并据此对数据包进行路由。您可定义静态路由、配置路由信息协议 (RIP) 和开放最短路径优先 (OSPF) 动态路由协议，还可实施网络地址转换 (NAT)。
虚拟设备	您可以在处于虚拟托管环境中的自己的设备上部署的受管设备。您不能将虚拟设备配置为虚拟交换机或虚拟路由器。
移动设备	在 Sourcefire 3D 系统中，由发现功能识别为移动手持设备 （例如，移动电话或平板电脑）的主机。系统通常可检测移动设备是否已越狱。
应用	您执行的使策略或对策略的更改生效的操作。可将大多数策略从防御中心应用于其受管设备；但是，可激活和停用关联策略，因为它们不涉及对受管设备配置做出的更改。
应用	一种检测到的、可针对其编写访问控制规则的网络资产、通信方法或 HTTP 内容。系统检测三种类型的应用：应用协议、客户端应用和网络应用。
应用控制	访问控制的一项功能，可供您指定哪些应用流量可穿越网络。
应用协议	一种应用类型，表示在服务器与主机上的客户端应用通信期间检测到的应用协议流量；例如， SSH 或 HTTP。
用户	受管设备或用户代理已检测到其网络活动的用户。
用户代理	您在服务器上安装的代理，用于在用户登录网络或因任何其他原因对 Active Directory 凭证进行身份验证时对其进行监控。仅当用户代理报告受控访问用户的用户活动时，该活动才用于访问控制。
用户感知	一项功能，可供贵组织将威胁、终端和网络情报与用户身份信息相关联，且可供您执行用户控制。
用户活动	当系统检测到用户登录 （或者，包括某些失败的登录尝试）或从防御中心数据库添加或删除用户记录时生成的事件。

用户角色	授予 Sourcefire 3D 系统用户的访问权限级别。例如，您可以向事件分析师、管理 Sourcefire 3D 系统的管理员和使用第三方工具访问防御中心数据库的用户授予不同的网络界面访问权限。还可创建具有特殊访问权限的自定义角色。
用户控制	访问控制的一项功能，可供您指定和记录能够进入、退出网络或在不离开网络的情况下穿越网络的用户关联流量。
预处理程序	一项对入侵策略检查的流量标准化的功能，一项通过识别不适当的报头选项、分片重组 IP 数据报、提供 TCP 状态检查和数据流重组以及验证校验和来帮助识别网络层和传输层协议异常的功能。预处理程序还可将特定类型的数据包转换为系统能够分析的格式；这些预处理程序称为数据标准化预处理程序或应用层协议预处理程序。标准化应用层协议编码可使系统对以不同方式编码的数据包有效应用相同的内容相关入侵规则并获得有意义的结果。每当数据包触发您配置的预处理程序选项时，预处理程序就会生成预处理程序规则。
预处理程序规则	与预处理程序或端口扫描流量检测器相关联的入侵规则。如果您想要预处理程序规则生成事件，必须首先启用该规则。预处理程序规则具有预处理程序特定 GID（生成器 ID）。
源	请参阅安全情报源。
运行状况监控	一项功能，该功能持续监控部署中设备的性能。运行状况监控使用已应用健康策略中的运行状况模块测试设备。
运行状况模块	一项针对部署中的特定性能方面 （例如，设备的 CPU 使用率或可用磁盘空间）的测试。在健康策略中启用的运行状况模块在其监控的性能方面达到某一水平时生成运行状况事件。
终端	作为贵组织的高级恶意软件防护策略的一部分，您的用户安装 FireAMP 连接器所在的计算机或移动设备。
主机	连接到网络并具有唯一 IP 地址的一台设备。对于 Sourcefire 3D 系统，主机是未归类为移动设备、网桥、路由器、 NAT 设备或逻辑接口的任何已识别主机。
主机输入	一项功能，可供您使用脚本或命令行文件从第三方源导入数据，以扩充网络映射中的信息。网络界面还提供一些主机输入功能；您可修改操作系统或应用协议身份、使漏洞生效或失效以及从网络映射删除各个项目，包括客户端和服务器端口。
自定义用户角色	具有特殊访问权限的用户角色。自定义用户角色可能拥有任何一组基于菜单和系统的权限，且可能为完全原始的角色，或基于预定义用户角色。