FireSIGHT 系统安装指南

5.3.1 版本
2014 年 7 月 17 日

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

目 录

FireSIGHT 系统简介

思科 FireSIGHT® 系统兼具行业领先的网络入侵防御系统安全性和基于检测到的应用、用户和 URL 控制网络访问的能力。FireSIGHT 系统设备也可以用于交换式、路由式或混合式（交换路由式）的环境中，执行网络地址转换 (NAT) 以及在 FirePOWER 受管设备的虚拟路由器之间建立安全的虚拟专用网络 (VPN) 隧道。

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

被动部署中的设备可以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，且这些接口上所接收的任何流量都不会被重新传输。

内联部署中的虚拟设备能够让网络免受可能影响网络上的主机的可用性、完整性和保密性的攻击。内联接口无条件地接收所有流量，除非部署中的某些配置明确丢弃这些流量，否则这些接口上接收的流量都会被重新传输。可将内联设备部署为一个简单的入侵防御系统，也可以使用其他方法配置内联设备，以执行访问控制和管理网络流量。

本安装指南提供了有关部署、安装和设置 FireSIGHT 系统设备的信息 （设备和防御中心）。也提供了 FireSIGHT 系统设备的硬件规格、安全和监管信息。

提示 您可以将虚拟防御中心和设备进行托管，它们可以管理物理设备，或者由物理设备来进行管理。但是，虚拟设备不支持系统的基于硬件的任何功能：冗余、交换、路由等等。有关详细信息，请参阅 《*FireSIGHT 系统虚拟安装指南*》。

接下来的主题将介绍 FireSIGHT 系统并描述其主要组件：

FireSIGHT 系统设备

FireSIGHT 系统 *设备*可以是流量感应受管 *设备*，也可以是管理型*防御中心*：

物理设备是指拥有多种吞吐量和多项功能的容错专用网络设备。防御中心可用作这些设备的集中管理点，自动汇聚并关联这些设备生成的事件。每种物理设备类型都有多种*型号*；这些型号可进一步划分为多个*产品系列*。 FireSIGHT 系统的许多功能都取决于设备。

防御中心

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

防御中心的主要功能包括：

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

对于许多物理防御中心而言，高可用性 （冗余）功能有助于确保运行的连续性。

受管设备

部署在公司各网段上的设备可以监控流量，以便进行分析。被动部署的设备可帮助您深入了解您的网络流量。如果是内联部署， FirePOWER 设备可按不同条件影响流量。根据不同的型号和许可证，设备可：

- 收集有关公司主机、操作系统、应用、用户、文件、网络和漏洞的详细信息
- 根据各种基于网络的标准以及其他标准（包括应用、用户、 URL、 IP 地址信誉和入侵或恶意软件检查结果）来阻止或允许网络流量
- 具有交换、路由、DHCP、NAT 和 VPN 功能以及可配置的旁路接口、快速路径规则和严格的 TCP 实施
- 拥有可帮助您确保运营连续性的群集 （冗余）功能，以及可整合多台个设备的资源的堆叠功能

您**必须**使用防御中心对 FirePOWER 设备进行管理。

设备类型

FireSIGHT 系统可在思科专门设计的容错性*物理*网络设备上运行。每个防御中心和受管设备都有多种*型号*；这些型号进一步划分为多个*产品系列*。

受管的物理设备具有各种不同的吞吐量和功能。物理防御中心还有各种设备管理、事件存储以及主机和用户监控功能。

您还可以部署以下基于软件的设备：

- 64 位*虚拟*防御中心和*虚拟*受管设备可使用 VMware vSphere Hypervisor 或 vCloud Director 环境部署为 ESXi 主机。
- Blue Coat X 系列平台上也可以部署 X 系列专用 Sourcefire 软件；用作受管设备。

任何类型的防御中心 （物理或虚拟）可以管理任何类型的设备：物理、虚拟的具备 FirePOWER 服务的思科 ASA 防火墙以及 X 系列专用 Sourcefire 软件。但是，请注意，FireSIGHT 系统的许多功能取决于设备。

有关 FireSIGHT 系统设备的详细信息，包括所支持的功能，请参阅：

- 2 系列设备，第 1-3 页
- 3 系列设备，第 1-3 页
- 虚拟设备，第 1-3 页
- X 系列专用 Sourcefire 软件，第 1-4 页

2 系列设备

2 系列是传统物理设备的第二个系列。由于资源和架构的限制，2 系列设备支持有限的 FireSIGHT 系统功能集。

虽然思科不再提供新的 2 系列设备，但是，您可以将运行早期系统版本的 2 系列防御中心更新或重新映像到 5.3.1 版本。2 系列设备无法更新或重新映像到 5.3.1 版本。但是，5.3.1 版本的防御中心可管理 5.2 或 5.3 版本的设备。请注意，重新映像会导致设备上几乎**所有的**配置和事件数据丢失。有关详细信息，请参阅还原 FireSIGHT 系统设备为出厂默认设置，第 7-1 页。

提示 可将特定配置和事件数据从 4.10.3 版本部署迁移到 5.2 版本部署，然后更新至 5.3.1 版本。有关详细信息，请参阅适用于 5.2 版本的 《*思科 FireSIGHT 系统迁移指南*》。

2 系列可自动将大部分功能与保护许可证关联：入侵检测与防御、文件控制以及基本访问控制。但是， 2 系列设备无法执行安全情报过滤、高级访问控制或高级恶意软件防护。也可以在 2 系列设备上启用其他许可的功能。除支持快速路径规则、堆叠和侧录模式的 3D9900 外， 2 系列设备不支持任何与 3 系列设备关联并基于硬件的功能：交换、路由、NAT 等等。

如果正在运行 5.3.1 版本， DC1000 和 DC3000 2 系列防御中心支持 FireSIGHT 系统的所有功能；DC500 更多功能受限。

3 系列设备

3 系列是 FirePOWER 物理设备的第三个系列。所有 7000 系列和 8000 系列设备均为 3 系列设备。8000 系列设备功能更强大，并支持不受 7000 系列设备支持的部分功能。

注意事项 您无法将 3 系列设备更新或重新映像到 5.3.1 版本，但 5.3.1 版本的防御中心可管理 5.2 或 5.3 版本的虚拟设备。

虚拟设备

64 位虚拟防御中心和受管设备可使用 VMware vSphere Hypervisor 或 vCloud Director 环境部署为 ESXi 主机。

无论已安装和应用何种许可证，虚拟设备均不支持系统的任何基于硬件的功能：冗余、资源共享、交换和路由等等。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《*FireSIGHT 系统虚拟安装指南*》。

注意事项 您无法将虚拟设备更新或重新映射到 5.3.1 版本，但 5.3.1 版本的防御中心可以管理 5.2 或 5.3 版本的虚拟设备。

X 系列专用 Sourcefire 软件

您可以在 Blue Coat X 系列平台上安装 X 系列专用 Sourcefire 软件。此设备基于软件，功能类似于一台虚拟的受管设备。无论已安装和应用何种许可证， X 系列专用 Sourcefire 软件均不支持以下所有功能：

- X 系列专用 Sourcefire 软件不支持系统的基于硬件的功能：集群、堆叠、交换、路由、VPN、NAT 等等。
- 使用 X 系列专用 Sourcefire 软件，您无法基于网络流量的来源或目标所在的国家/地区或大洲，对网络流量进行过滤 （基于地理位置的访问控制）。
- 您无法使用防御中心的网络界面配置 X 系列专用 Sourcefire 软件的接口。
- 您无法使用防御中心关闭、重新启动或管理 X 系列专用 Sourcefire 软件的进程。
- 您无法使用防御中心来创建 X 系列专用 Sourcefire 软件的备份，也无法还原其备份。
- 您无法将运行状况或系统策略应用至 X 系列专用 Sourcefire 软件。其中包括管理时间设置。

X 系列专用 Sourcefire 软件没有网络界面。但是，它拥有 X 系列平台独有的命令行界面 (CLI)。此 CLI 可用于安装系统并执行平台特定的其他管理任务，如：

- 创建虚拟设备处理器 (VAP) 组，这使得您可以利用 X 系列平台的负载均衡和冗余性功能的优势 （与思科的物理设备集群相当）
- 配置被动和内联感应接口，包括配置接口的最大传输单位 (MTU)
- 管理进程
- 管理时间设置，包括 NTP 设置

注意事项 您无法将 X 系列设备更新或重新映射到 5.3.1 版本，但 5.3.1 版本的防御中心可以管理 5.2 或 5.3 版本的设备。

具备 FirePOWER 服务的思科 ASA 防火墙

可通过防御中心管理具备 FirePOWER 服务的思科 ASA 防火墙 (ASA FirePOWER) 设备。在此部署中， ASA 设备提供最重要的系统策略，并将流量传送至 FireSIGHT 系统，以进行访问控制、入侵检测与防御、发现以及高级恶意软件防护。请参阅 5.3.1 版本 FireSIGHT 系统设备表，查看受支持的 ASA 型号的列表。

无论已安装和应用何种许可证，ASA FirePOWER 设备无法通过 FireSIGHT 系统支持以下任何功能：

- ASA FirePOWER 设备不支持 FireSIGHT 系统的基于硬件的功能：集群、堆叠、交换、路由、VPN、NAT 等等。然而， ASA 平台的确会提供这些功能，您可以使用 ASA CLI 和 ASDM 来对其进行配置。有关详细信息，请参阅 ASA 文档。
- 您无法使用防御中心的网络界面配置 ASA FirePOWER 的接口。
- 您无法使用防御中心关闭、重启或管理 ASA FirePOWER 的进程。
- 您无法使用防御中心来创建 ASA FirePOWER 设备的备份，也无法还原其备份。
- 您无法使用 VLAN 标记条件编写访问控制规则来匹配流量。

ASA FirePOWER 设备没有 FireSIGHT 网络界面。但是，它拥有 ASA 平台特有的软件和命令行界面 (CLI)。您可以使用这些 ASA 特有的工具来安装系统和执行平台特有的其他管理任务。有关详细信息，请参阅 ASA FirePOWER 模块文档。

ASA FirePOWER 模块还包括用于 FirePOWER 设备的 CLI。您可以使用 CLI 来查看、配置 FireSIGHT 系统，以及对其进行故障排除。有关详细信息，请参阅 《*FireSIGHT 系统用户指南*》。

随 5.3.1 版本一起交付的设备

下表列出了思科随 FireSIGHT 系统 5.3.1 版本一同交付的设备。

注意事项 您可以将 2 系列、3 系列和运行早期系统版本的虚拟防御中心更新或重新映像到 5.3.1 版本。您不能将 2 系列、3 系列、虚拟或 X 系列设备更新或重新映射至 5.3.1版本，但是，5.3.1 版本的防御中心可以管理 5.2 或 5.3 版本的这些设备。

表 1-1 5.3.1 版本 FireSIGHT 系统设备

型号/系列：	系列	形态	类型
70xx 子系列： • 3D7010/3D7020/3D7030	3 系列 （7000 系列）	硬件	设备
71xx 子系列： • 3D7110/3D7120 • 3D7115/3D7125 • AMP7150	3 系列 （7000 系列）	硬件	设备
81xx 子系列： • 3D8120/3D8130/3D8140 • AMP8150	3 系列 （8000 系列）	硬件	设备
82 xx 子系列： • 3D8250 • 3D8260/3D8270/3D8290	3 系列 （8000 系列）	硬件	设备
83 xx 子系列： • 3D8350 • 3D8360/3D8370/3D8390	3 系列 （8000 系列）	硬件	设备
64 位虚拟设备	不适用	软件	设备
X 系列专用 Sourcefire 软件	不适用	软件	设备
ASA FirePOWER： • ASA5585-X-SSP-10、ASA5585-X-SSP-20、ASA5585-X-SSP-40、ASA5585-X-SSP-60	不适用	硬件	设备
ASA FirePOWER： • ASA5512-X、 ASA5515-X、ASA5525-X、 ASA5545-X、ASA5555-X	不适用	软件	设备

表 1-1 5.3.1 版本 FireSIGHT 系统设备 （续）

型号/系列：	系列	形态	类型
3 系列防御中心： • DC750/DC1500/DC3500	3 系列	硬件	防御中心
64 位虚拟防御中心	不适用	软件	防御中心

虽然思科不再提供新的 2 系列设备，但是，您可以将运行早期系统版本的 2 系列防御中心更新或重新映像到 5.3.1 版本。您不能将 2 系列设备更新或重新映射到 5.3.1 版本，但是 5.3.1 版本的防御中心可以管理 5.3 版本的设备。请注意，重新映像会导致设备上几乎**所有**配置和事件数据丢失。有关详细信息，请参阅还原 FireSIGHT 系统设备为出厂默认设置，第 7-1 页。

提示 可将特定配置和事件数据从 4.10.3 版本部署迁移到 5.2 版本部署，然后更新至 5.3.1 版本。有关详细信息，请参阅适用于 5.2 版本的 《*FireSIGHT 系统迁移指南*》。

不同防御中心型号支持的功能

运行 5.3.1 版本时，所有防御中心的功能相似，仅有少数功能受型号限制。下表列出了系统的主要功能以及支持这些功能的防御中心 （假设正在管理支持这些功能的设备并已安装和应用正确的许可证）。

除表中列出的功能外，防御中心型号在可管理的设备数量、可存储的事件数量以及可监控的主机和用户数量方面存在差异。有关详细信息，请参阅 《*FireSIGHT 系统用户指南*》。

另外，请记住，虽然您可以使用运行 5.3.1 版本系统的任何型号的防御中心来管理 5.3 或 5.3.1 版本的任意设备，但许多系统功能会受到设备型号的限制。例如，已经有 3 系列防御中心但没有部署 3 系列设备的话，您依然无法实施 VPN。有关详细信息，请参阅不同受管设备型号所支持的功能，第 1-7 页。

表 1-2 不同防御中心型号所支持的功能

功能	2 系列防御中心	3 系列防御中心	虚拟防御中心
收集受管设备所报告的发现数据 （主机、应用和用户）并为贵公司建立一个网络映射	支持	支持	支持
查看网络流量的地理定位数据	DC1000、 DC3000	支持	支持
管理入侵检测和防御 (IPS) 部署	支持	支持	支持
管理执行安全情报过滤的设备	DC1000、 DC3000	支持	支持
管理执行简单的基于网络控制的设备，包括基于地理定位的过滤	支持	支持	支持
管理执行应用控制的设备	支持	支持	支持
管理执行用户控制的设备	DC1000、 DC3000	支持	支持
管理通过文字 URL 过滤网络流量的设备	支持	支持	支持
管理按类别和信誉执行 URL 过滤的设备	DC1000、 DC3000	支持	支持
管理按文件类型执行简单文件控制的设备	支持	支持	支持
管理执行基于网络的高级恶意软件防护 (AMP) 的设备	DC1000、 DC3000	支持	支持

表 1-2 不同防御中心型号所支持的功能 （续）

功能	2 系列防御中心	3 系列防御中心	虚拟防御中心
从 FireAMP 部署接收基于终端的恶意软件 (FireAMP) 事件	支持	支持	支持
管理基于设备及硬件的功能： • 快速路径规则 • 严格的 TCP 执行 • 可配置的旁路接口 • 侧录模式 • 交换和路由 • NAT 策略 • VPN	支持	支持	支持
管理基于设备的冗余和资源共享： • 设备堆叠 • 设备集群 • X 系列专用 Sourcefire 软件 VAP 组 • 集群堆叠	支持	支持	支持
构建高可用性	DC1000、 DC3000	DC1500、DC3500	不支持
安装恶意软件存储包	DC1000、 DC3000	支持	不支持
连接到 eStreamer、主机输入或数据库客户端	支持	支持	支持

不同受管设备型号所支持的功能

设备是指那些能够处理网络流量的设备；因此， FireSIGHT 系统的许多功能取决于受管设备的型号。

下表列出了系统的主要功能以及支持这些功能的设备 （假设您已通过管理防御中心安装和应用正确的许可证）。

请记住，虽然您可以使用运行 5.3.1 版本系统的任何型号的防御中心来管理 5.3 或 5.3.1 版本的任意设备，但一些系功能会受到防御中心型号的限制。例如， 2 系列 DC500 不可用于管理执行安全情报过滤的设备，即使这些设备支持该功能。有关详细信息，请参阅不同防御中心型号支持的功能，第 1-6 页。

表 1-3 不同受管设备型号所支持的功能

功能	2 系列设备	3 系列设备	ASA FirePOWER	虚拟设备	X 系列
网络发现：主机、应用和用户	支持	支持	支持	支持	支持
入侵检测和防御 (IPS)	支持	支持	支持	支持	支持
安全情报过滤	不支持	支持	支持	支持	支持
访问控制：基础网络控制	支持	支持	支持	支持	支持
访问控制：基于地理定位的过滤	不支持	支持	支持	支持	不支持
访问控制：应用控制	不支持	支持	支持	支持	支持

表 1-3 不同受管设备型号所支持的功能 （续）

功能	2 系列设备	3 系列设备	ASA FirePOWER	虚拟设备	X 系列
访问控制：用户控制	不支持	支持	支持	支持	支持
访问控制：文字 URL	不支持	支持	支持	支持	支持
访问控制：按类别和信誉进行 URL 过滤	不支持	支持	支持	支持	支持
文件控制：按文件类型	支持	支持	支持	支持	支持
基于网络的高级恶意软件防护 (AMP)	不支持	支持	支持	支持	支持
自动应用旁路	支持	支持	不支持	支持	不支持
快速路径规则	3D9900	8000 系列	不支持	不支持	不支持
严格的 TCP 执行	不支持	支持	不支持	不支持	不支持
可配置的旁路接口	支持	硬件受限制的除外	不支持	不支持	不支持
侧录模式	3D9900	支持	不支持	不支持	不支持
交换和路由	不支持	支持	不支持	不支持	不支持
NAT 策略	不支持	支持	不支持	不支持	不支持
VPN	不支持	支持	不支持	不支持	不支持
设备堆叠	3D9900	3D8140 82 xx 子系列 83 xx 子系列	不支持	不支持	不支持
设备集群	不支持	支持	不支持	不支持	不支持
集群堆叠	不支持	3D8140 82 xx 子系列 83 xx 子系列	不支持	不支持	不支持
恶意软件存储包	不支持	支持	不支持	不支持	不支持
受限的命令行界面 (CLI)	不支持	支持	支持	支持	不支持
外部身份验证	支持	支持	不支持	不支持	不支持
连接到 eStreamer 客户端	支持	支持	支持	不支持	不支持

3 系列设备机箱名称

以下章节列出了 7000 系列和 8000 系列设备及其各自的机箱硬件代码。机箱代码显示在机箱外部的管制标签上，是硬件认证和安全的正式参考代码。

7000 系列机箱名称

下表列出了全球范围内提供的 7000 系列型号的机箱名称。

表 1-4 7000 系列机箱型号

3D 设备型号	硬件机箱代码
3D7010、 3D7020、 3D7030	CHRY-1U-AC
3D7110、 3D7120 （铜）	GERY-1U-8-C-AC

表 1-4 7000 系列机箱型号 （续）

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

8000 系列机箱名称

下表列出了全球范围内提供的 3 系列型号的机箱名称。

表 1-5 8000 系列机箱型号

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

FireSIGHT 系统组件

接下来的章节介绍用于保障公司安全的部分 FireSIGHT 系统关键功能、可接受的使用策略和流量管理战略。

提示 FireSIGHT 系统的许多功能取决于设备型号、许可证和用户角色。 FireSIGHT 系统文档会在需要的地方概述每个功能和任务的要求。

冗余和资源共享

FireSIGHT 系统的冗余和资源共享功能使得您可以确保运营的连续性，以及整合多台物理设备的处理资源：

- 防御中心的高可用性功能允许指定冗余的 DC1000、DC1500、DC3000 或 DC3500 防御中心以管理设备。
- 设备堆叠功能允许通过以堆叠配置连接两到四台物理设备，来增加某个网段中所检查的流量数量。
- 设备集群功能允许在两个或更多的 3 系列设备或堆叠之间创建网络功能和配置数据的冗余。

网络流量管理

FireSIGHT 系统的网络流量管理功能使得 3 系列设备成为公司网络基础设施的一部分。您可以：

- 配置第 2 层部署，实现两个或更多个网段之间的分组交换

- 配置第 3 层部署，为两个或更多个接口之间的流量提供路由
- 进行网络地址转换 (NAT)
- 从受管设备上的虚拟路由器到远程设备或其他第三方 VPN 终端，建立安全的 VPN 隧道

FireSIGHT

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

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

访问控制

访问控制是一项基于策略的功能，可指定、检查和记录流经网络的流量。作为访问控制的一部分，在对流量进行更深层次的分析之前，可使用安全情报功能将特定 IP 地址列入黑名单，拒绝发往和来自该地址的流量。

进行安全情报过滤后，可以定义目标设备处理哪些流量以及如何处理流量，从简单的 IP 地址匹配，到涉及不同用户、应用、端口和 URL 的复杂场景。可以信任、监控或阻止流量，或进行进一步分析，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

入侵检测和防御是一项基于策略的功能。该功能被集成至访问控制功能，可用于监控网络流量以检测安全违规以及在内联部署中阻止或修改恶意流量。入侵策略包含各种组件，包括：

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

文件跟踪、控制和基于网络的高级恶意软件防护 (AMP)

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

文件控制是一项基于策略的功能。该功能被集成至访问控制，允许受管设备检测并阻止用户上传（发送）或下载 （接收）超出特定应用协议范围的特定类型文件。

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

无论是否存储已检测到的文件，您都可以使用此文件的 SHA-256 哈希值，将文件提交至思科云，进行简单的已知文件性质查找。还可以提交文件用于*动态*分析，产生威胁得分。您可以利用此情景信息配置系统，以阻止或允许特定的文件。

FireAMP 是思科制定的企业级高级恶意软件分析和防护解决方案，可发现、了解和阻止高级恶意软件爆发、高级持续性威胁和针对性攻击。如果贵公司已订用 FireAMP，个人用户可在其计算机和移动设备 （也称为终端）上安装 FireAMP 连接器。这些轻型代理与思科云通信，该云进而与防御中心通信。

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

网络文件轨迹功能可以用来跟踪一个文件在网络中的传输路径。系统使用 SHA-256 哈希值跟踪文件。每个文件都有一个关联的轨迹图，其中包含随时间推移文件传输的视觉展示和其他文件补充信息。

应用编程接口

您可以使用应用编程接口 (API) 以不同的方式与系统交互。

- 通过 Event Streamer (eStreamer)，您可以将多种事件数据从 FireSIGHT 系统设备以流的形式发送至定制开发的客户端应用。
- 借助数据库访问功能，您可以通过支持 JDBC SSL 连接的第三方客户端，查询防御中心中的多个数据库表。
- 借助主机输入功能，您可以使用脚本或命令行文件从第三方源导入数据，从而添加信息至网络映射。
- 补救措施是防御中心在网络上的某些条件得到符合时自动启动的程序。该功能不仅可以在您无法立即解决攻击的时候自动缓解攻击，还可以确保系统符合贵公司的安全策略。

许可 FireSIGHT 系统

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

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

防御中心在购买时已包含一个 FireSIGHT 许可证。执行主机、应用和用户发现时均需该许可证。防御中心上的 FireSIGHT 许可证同时决定了使用防御中心及其受管设备时可以监控的主机和用户数量，以及进行用户控制的用户数量。 FireSIGHT 主机和用户许可证限制仅适用于特定型号，如下表所列。

表 1-6　　不同防御中心型号的 FireSIGHT 限制

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

如果防御中心以前运行的是 4.10.x 版本，那么您可以使用旧版 RNA 主机和 RUA 的用户许可证，而非 FireSIGHT 许可证。有关详细信息，请参阅使用旧版的 RNA 主机和 RUA 用户许可证，第 1-13 页。

其他特定于型号的许可证允许您的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进行入侵检测与防御、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，以及创建设备和堆叠集群。使用控制许可证需要有保护许可证。

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，哪些流量可以遍历您的网络。使用 URL 过滤许许可证需要保护许可证。

恶意软件

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

VPN

VPN 许可证允许您在思科受管设备的虚拟路由器之间，或从受管设备到远程设备或其他第三方 VPN 终端之间，构建安全的 VPN 隧道。使用 VPN 许可证需要保护和控制许可证。

由于架构和资源的限制，并非所有许可证都可应用于所有受管设备。一般而言，您无法许可设备不支持的功能；请参阅不同受管设备型号所支持的功能，第 1-7 页。

下表汇总了可以添加至防御中心并应用于每个设备型号的许可证。防御中心行 （适用于 FireSIGHT 之外的许可证）表示防御中心是否可使用这些许可证管理设备。例如，您可以通过 2 系列 DC1000 使用 3 系列创建一个 VPN 部署，但是，无论其管理何种设备，您无法用 DC500 执行基于类别和信誉的 URL 过滤。请注意，不适用表示与受管设备无关并基于防御中心的许可证。

表 1-7 不同型号所支持的许可证

型号	FireSIGHT	保护	控制	URL 过滤	恶意软件	VPN
2 系列设备： • 3D500/1000/2000 • 3D2100/2500/ 3500/4500 • 3D6500 • 3D9900	不适用	自动，无安全情报	不支持	不支持	不支持	不支持
3 系列设备： • 7000 系列 • 8000 系列	不适用	支持	支持	支持	支持	支持
虚拟设备	不适用	支持	支持，但不支持硬件功能	支持	支持	不支持
具备 FirePOWER 服务的思科 ASA 防火墙	不适用	支持	支持，但不支持硬件功能	支持	支持	不支持
X 系列专用 Sourcefire 软件	不适用	支持	支持，但不支持硬件功能	支持	支持	不支持

表 1-7 不同型号所支持的许可证 （续）

型号	FireSIGHT	保护	控制	URL 过滤	恶意软件	VPN
DC500 2 系列防御中心	支持	支持，但无安全情报	支持，但无用户控制	不支持	不支持	支持
DC1000/3000 2 系列防御中心	支持	支持	支持	支持	支持	支持
DC750/1500/3500 3 系列防御中心	支持	支持	支持	支持	支持	支持
虚拟防御中心	支持	支持	支持	支持	支持	支持

除本表中的信息外，请注意

- 2 系列设备自动拥有除安全情报过滤以外的保护功能。
- 虽然可以在虚拟设备上启用控制许可证，但虚拟设备不支持该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 带保护和控制许可证，可用来管理设备，但无法执行安全情报过滤或用户控制。

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

使用旧版的 RNA 主机和 RUA 用户许可证

在 FireSIGHT 系统的 4.10.x 版本中，RNA 主机 和 RUA 用户功能许可证分别决定了对受监控的主机和用户的限制。如果防御中心以前运行的是 4.10.x 版本，您可以使用旧版主机和用户许可证代替 FireSIGHT 许可证。

使用旧版许可证的 5.3.1 版本的防御中心将 RNA 主机限制用作 FireSIGHT 主机限制，并将 RUA 用户限制用作 FireSIGHT 用户限制和访问受控用户限制。FireSIGHT Host License Limit 运行状况模块会提供适当的许可限制警报。

请注意， RNA 主机和 RUA 用户限制是累积的。即可以将每种类型的多个许可证添加至防御中心，以监控许可证允许的主机或用户总数。

如果稍后添加一个 FireSIGHT 许可证，防御中心会采用更高的数量限制。例如， DC1500 的 FireSIGHT 许可证支持最多 50,000 个主机和用户。如果 4.10.x 版本 DC1500 的 RNA 主机限制大于 50,000，在运行 5.3.1 版本的同一防御中心上使用该旧版主机许可证，可获得更高的数量限制。为方便使用，网络界面仅显示代表更高数量限制的许可证。

注 由于 FireSIGHT 许可证限制与防御中心的硬件功能相匹配，如果使用旧版许可证，思科**不**推荐超过这些数量限制。有关指导信息，请联系技术支持部门。

由于不存在 4.10.x 版本到 5.3.1 版本的更新路径，因此，您必须使用 ISO 映像来“还原”防御中心。请注意，重新映像会导致设备上几乎**所有**的配置和事件数据丢失。重新映像后，该数据**无法**导入至设备。有关详细信息，请参阅还原 FireSIGHT 系统设备为出厂默认设置，第 7-1 页。

注 只能在维护窗口中重新映像设备。在重新映像后及重新配置旁路模式前，内联部署中的设备会被重置为非旁路配置，而且网络中的流量会被中断。有关详细信息，请参阅还原流程中的流量，第 7-2 页。

在恢复过程中，系统会提示删除许可和网络设置。尽管能在意外删除后重新添加设置，但也请保留这些设置。请注意，5.3.1 版本防御中心无法管理 4.10.x 版本设备。但是，可将支持的 4.10.x 版本设备还原并更新到最新版本。有关详细信息，请参阅还原 FireSIGHT 系统设备为出厂默认设置，第 7-1 页。

安全性、互联网接入和通信端口

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

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

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

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

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

有关详细信息，请参阅：

- 互联网访问要求，第 1-14 页
- 通信端口要求，第 1-15 页

互联网访问要求

FireSIGHT 系统配置为可通过默认打开的端口 443/tcp (HTTPS) 和端口 80/tcp (HTTP) 直接连接到互联网；请参阅通信端口要求，第 1-15 页。请注意，大多数 FireSIGHT 系统设备支持代理服务器；请参阅 《*FireSIGHT 系统用户指南*》中的“配置网络设置”章节。

为了确保业务的连续性，高可用性对中的两个防御中心都必须接入互联网。对于特定功能，主防御中心连接互联网，然后在同步过程中与辅助设备共享信息。因此，如果主设备故障，应按照《*FireSIGHT 系统用户指南*》中的“管理设备”章节所述将辅助设备升级为主设备。

下表描述了 FireSIGHT 系统特定功能的互联网接入需求。

表 1-8 FireSIGHT 系统功能的互联网接入需求

功能	需要互联网接入，以便.....	设备	高可用性考虑事项
动态分析：查询	查询综合安全情报云，了解以前提交以供动态分析的文件的威胁得分。	防御中心	配对的防御中心会独自查询云，以了解威胁得分。
动态分析：提交	提交文件至综合安全情报云以供动态分析。	受管设备	不适用
FireAMP 集成	接收来自综合安全情报云云的基于端点的 (FireAMP) 恶意软件事件。	防御中心	云连接没有同步。在两个防御中心上进行配置。

表 1-8 FireSIGHT 系统功能的互联网接入需求 （续）

功能	需要互联网接入，以便.....	设备	高可用性考虑事项
入侵规则、 VDB 和 GeoDB 更新	直接下载或安排下载入侵规则、 GeoDB 或 VDB 更新至设备。	防御中心	入侵规则、 GeoDB 和 VDB 更新同步。
基于网络的 AMP	执行恶意软件云查找。	防御中心	成对的防御中心独立执行云查找。
RSS 源控制面板构件	从外部来源，包括思科，下载 RSS 源数据。	任何设备，虚拟设备、X 系列和 ASA FirePOWER 除外	源数据不同步。
安全情报过滤	从外部来源下载安全情报源数据，包括 FireSIGHT 系统情报源。	防御中心	主防御中心下载源数据并与辅助设备共享此数据。在主设备故障的情况下，可将辅助设备升级为主设备。
系统软件更新	直接下载或安排下载系统更新至设备。	任何设备，虚拟设备、X 系列和 ASA FirePOWER 除外	系统更新不同步。
URL 过滤	下载基于云的 URL 类别和信誉数据进行访问控制，并执行未分类的 URL 查找。	防御中心	主防御中心下载 URL 过滤数据并与辅助设备共享此数据。在主设备故障的情况下，可将辅助设备升级为主设备。
whois	请求外部主机的 whois 信息。	任何设备，虚拟设备、X 系列和 ASA FirePOWER 除外	请求域名项信息的设备必须接入互联网。

通信端口要求

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

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

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

注意事项 在了解此操作对部署的影响之前，**请勿**关闭已打开的端口。

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

请注意，系统允许您更改某些通信端口：

- 在配置系统与身份验证服务器之间的连接时，您可以指定用于 LDAP 和 RADIUS 身份验证的自定义端口；请参阅 《*FireSIGHT 系统用户指南*》。
- 您可以更改管理端口 (8305/tcp)；请参阅*FireSIGHT 系统用户指南*。但是，思科**强烈**建议您保留默认设置。如果要更改管理端口，您必须更改部署中需要相互通信的所有设备的管理端口。

- 您可以通过端口 32137/tcp 将已升级的防御中心与综合安全情报云云进行通信。但是，思科建议切换到端口 443。该端口为 5.3.1 版本及更高版本全新安装的默认端口。有关详细信息，请参阅 《*FireSIGHT 系统用户指南*》。

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

表 1-9 FireSIGHT 系统功能和操作的默认通信端口

端口	说明	方向	在.....上打开	以.....
22/TCP	SSH/SSL	双向	任意	允许到设备的安全远程连接。
25/TCP	SMTP	出站	任意	从设备发送邮件通知和警报。
53/TCP	DNS	出站	任意	使用 DNS。
67/UDP 68/UDP	DHCP	出站	任何设备，X 系列 除外	使用 DHCP。 **注** 默认情况下，这些端口为**关闭状态**。
80/TCP	HTTP	出站	任何设备，虚拟设备、X 系列和 ASA FirePOWER 除外	允许 RSS 源控制面板构件连接到一个远程网络服务器。
		双向	防御中心	通过 HTTP 更新自定义和第三方安全情报源。 下载 URL 类别和信誉数据（还需要端口 443）。
161/UDP	SNMP	双向	任何设备，虚拟设备、X 系列和 ASA FirePOWER 除外	允许通过 SNMP 轮询访问设备的 MIB。
162/UDP	SNMP	出站	任意	发送 SNMP 警报至远程陷阱服务器。
389/TCP 636/TCP	LDAP	出站	任何设备，虚拟设备和 X 系列除外	与 LDAP 服务器通信以进行外部身份验证。
389/TCP 636/TCP	LDAP	出站	防御中心	获取检测到的 LDAP 用户元数据。
443/TCP	HTTPS	入站	任何设备，虚拟设备、X 系列和 ASA FirePOWER 除外	访问设备的网络界面。
443/TCP	HTTPS AMQP cloud comms.	双向	防御中心	获取： • 软件、入侵规则、 VDB 和 GeoDB 更新 • URL 类别和信誉数据（还需要端口 80）。 • 思科情报源和其他安全的安全情报源 • 基于终端的 (FireAMP) 恶意软件事件 • 网络流量中检测到的文件的恶意软件性质 • 已提交文件的动态分析信息
			2 系列和 3 系列设备	使用设备的本地网络界面下载软件更新。
			3 系列、虚拟设备、X 系列和 ASA FirePOWER	提交文件到思科云进行动态分析。
514/UDP	系统日志	出站	任意	向远程系统日志服务器发送警报。

表 1-9 FireSIGHT 系统功能和操作的默认通信端口 （续）

端口	说明	方向	在.....上打开	以.....
623/UDP	SOL/LOM	双向	3 系列	允许使用局域网承载串行 （SOL）连接执行无人值守管理。
1500/TCP 2000/TCP	数据库访问	入站	防御中心	允许第三方客户端对数据库进行只读访问。
1812/UDP 1813/UDP	RADIUS	双向	任何设备，虚拟设备、X 系列和 ASA FirePOWER 除外	与 RADIUS 服务器通信以进行外部身份验证和记帐。
3306/TCP	用户代理	入站	防御中心	与用户代理通信。
8302/TCP	eStreamer	双向	任何设备，虚拟设备和 X 系列除外	与 eStreamer 客户端通信。
8305/TCP	设备通信。	双向	任意	在同一部署中的设备之间安全地进行通信。
8307/TCP	主机输入客户端	双向	防御中心	与主机输入客户端通信。
32137/TCP	cloud comms.	双向	防御中心	允许升级的防御中心与思科云进行通信。

预配置设备

可以预配置在中心位置的多台设备和防御中心，以便在其他站点进行部署。关于预配置设备的考虑事项，请参阅预配置 FireSIGHT 系统设备，第 E-1 页。

了解部署

您可以部署 FireSIGHT 系统满足各个独特网络架构的需求。防御中心为 FireSIGHT 系统提供了一个集中管理控制台和数据库资源库。设备安装在网段上，收集流量连接以供分析。

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经过网络的流量，收集关于流经网络的流量性质的数据。可以通过内联部署中的设备监控网络是否存在影响网络上主机的可用性或机密性的攻击。设备可以部署于内联、交换、路由或混合 （第 2 层/第 3 层）环境中。

注 有关 ASA FirePOWER 设备部署方案的详细信息，请参阅 ASA 文档。

要进一步了解部署选项，请参阅以下各节，获取详细信息：

- 了解部署选项，第 2-1 页介绍设计部署时需要考虑的一些因素。
- 了解接口，第 2-2 页说明不同接口之间的差别及其在部署中的作用。
- 将设备与网络连接，第 2-5 页介绍如何在部署中使用集线器、 SPAN 和网络分路器。
- 部署选项，第 2-7 页描述基本部署并确定其内部的主要功能位置。
- 使用访问控制进行部署，第 2-12 页说明内联部署中使用访问控制的优势。
- 使用多端口受管设备，第 2-16 页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。
- 复杂的网络部署，第 2-18 页介绍高级部署方案，例如使用 VPN 或有多个入口点。

有关部署的详细信息，请参阅 《*最佳实践指南*》，可向思科销售部门索取。

了解部署选项

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

- 是否使用被动或内联接口部署受管设备？设备是否支持混合接口，即有些是被动接口，而其余是内联接口？有关详细信息，请参阅了解接口，第 2-2 页。
- 将要通过何种方式将受管设备与网络连接？集线器？网络分路器？交换机上的生成端口？虚拟交换机？有关详细信息，请参阅将设备与网络连接，第 2-5 页。
- 是想检测网络中的每个攻击，还是只想了解渗透防火墙的攻击？网络上是否存在特定资产，例如财务、会计核算或个人记录、生产代码或需要特殊安全策略保护的其他敏感、受保护的信息？有关详细信息，请参阅部署选项，第 2-7 页。

- 是否将使用受管设备上的多个端口重组网络分路器的独立连接或捕获和评估不同网络的流量？是否想要使用多个端口执行虚拟路由器或虚拟交换机的功能？有关详细信息，请参阅使用多端口受管设备，第 2-16 页。
- 是否为远程员工提供 VPN 或调制解调器访问？是否拥有也需要入侵防御部署的远程办公室？是否雇用合同工或其他临时员工？是否限制他们只能访问特定网段？是否将网络与客户、供应商或业务合作伙伴等其他组织的网络集成？有关详细信息，请参阅复杂的网络部署，第 2-18 页。

了解接口

以下各节将介绍不同接口对 FireSIGHT 系统功能有何影响。除了被动和内联接口外，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：

被动接口

许可证：任意

支持的设备：任意

您可以配置被动部署，使用交换机 SPAN、虚拟交换机或镜像端口监控整个网络的流量，从交换机的其他端口复制流量。可以通过被动接口检测网络中的流量，而无需进入网络流量中。当配置在被动部署中时，系统无法执行流量阻止或流量整形等操作。被动接口无条件地接收所有流量并且不会重新传输所接收的流量。

受管设备上的一个或多个物理接口可以配置成被动接口。有关详细信息，请参阅将设备与网络连接，第 2-5 页。有关在被动模式下配置 ASA FirePOWER 设备的详细信息，请参阅 ASA 文档。

内联接口

许可证：任意

支持的设备：任意

可以将两个端口结合到一起，在网段上进行内联部署透明配置。内联接口允许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所有流量，明确放弃的流量除外。

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。必须为内联集分配一对内连接口，它们才能在内联部署中处理流量。

注 如果将接口配置为内联接口，其网络模块上的相邻端口也自动变成内联接口来完成配对。

可配置旁路内联集可让您选择在硬件出现故障完全无法运行 （例如设备断电）的情况下如何处理流量。在某个网段，您可能确定连接性非常重；而在其他网段流量检测又非常重要，不允许不执行检测。使用可配置旁路内联集，可以通过以下方式之一来管理网络流量：

- *旁路*：将一个接口对配置为旁路模式，如果设备出现故障，则允许所有流量通过。流量绕过设备和设备执行的任何检查或其他处理。旁路允许整个网段的流量都不接受检查，但是可确保网络连接的畅通。
- *非旁路*：将一个接口对配置为非旁路模式，如果设备出现故障，则停止所有流量。到达故障设备的流量不会进入设备。非旁路模式不允许流量在未经检测的情况下通过网络，但是如果设备出现故障，网段将失去连接。在网络安全性比流量流失更加重要的部署情况下使用非旁路接口。

将内联集配置为旁路模式，确保如果设备出现故障，流量将继续传输。将内联集配置为非旁路模式，如果设备出现故障，将停止流量传输。请注意，重新映像会将旁路模式下的设备重置为非旁路配置并中断网络流量，直至重新配置了旁路模式。有关详细信息，请参阅还原流程中的流量，第 7-2 页。

所有设备均包含可配置旁路接口。 8000 系列设备还包含带有不能用于旁路配置的接口的网络模块。有关网络模块的详细信息，请参阅8000 系列模块，第 6-42 页。

高级选项依设备而定，可能包括 TAP 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详细信息，请参阅 《*FireSIGHT 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，请参阅将设备与网络连接，第 2-5 页。

无法使用 FireSIGHT 系统在 ASA FirePOWER 设备上配置旁路接口。有关在内联模式下配置 ASA FirePOWER 设备的详细信息，请参阅 ASA 文档。

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。也可以在受管设备上配置虚拟交换机作为独立的广播域，将网络划分为多个逻辑分段。虚拟交换机根据来自主机的媒体访问控制 (MAC) 地址来确定向哪里发送数据包。

交换接口具有物理或逻辑配置：

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

虚拟交换机可以作为独立的广播域，将网络划分为多个逻辑分段。虚拟交换机根据来自主机的媒体访问控制 (MAC) 地址来确定向哪里发送数据包。配置虚拟交换机时，交换机首先通过交换机上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和每个端口连接的网络上。

可以将设备配置为虚拟交换机并使用其余接口连接想要监控的网段。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 《*FireSIGHT 系统用户指南*》中“设置虚拟机”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，使其路由两个或多个接口之间的流量。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来路由流量。

可以配置路由接口，用于网关虚拟专用网络 （网关 VPN）或网络地址转换 (NAT)。有关详细信息，请参阅部署网关 VPN，第 2-11 页和使用基于策略的 NAT 进行部署，第 2-11 页。

还可以配置系统，通过根据目标地址做出数据包转发决策路由数据包。配置为路由接口的接口接收和转发第 3 层流量。路由器根据转发条件从传出接口获取目标位置，并且访问控制规则指定要应用的安全策略。

路由接口具有物理或逻辑配置：

- *物理路由接口*是已配置路由的物理接口。物理路由接口用于处理未标记的 VLAN 流量。
- *逻辑交换接口*是物理接口和 VLAN 标记之间的关联。逻辑接口用于处理带指定 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想要监控的网段。您还可以启用严格 TCP 强制，最大程度地确保 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 《*FireSIGHT 系统用户指南*》中“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，允许 FireSIGHT 系统桥接虚拟路由器和虚拟交换机之间的流量。如果在虚拟交换机的接口上收到的 IP 流量的目标地址为关联混合逻辑接口的 MAC 地址，系统将其视为第 3 层流量处理并根据目标 IP 地址路由或响应此流量。如果系统接收任何其他流量，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，首先要配置虚拟交换机和虚拟路由器，然后将虚拟交换机和虚拟路由器添加到混合接口上。未与虚拟交换机和虚拟路由器关联的混合接口无法用于路由，而且不会生成或响应流量。

可以利用网络地址转换 (NAT) 配置混合接口，在网络之间传输流量。有关详细信息，请参阅使用基于策略的 NAT 进行部署，第 2-11 页。

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 《*FireSIGHT 系统用户指南*》中“设置混合接口”的说明进行操作。

将设备与网络连接

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

使用集线器

以太网集线器是确保受管设备可以监视网段上所有流量的最简单方法。大多数的此类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。将接口集与集线器连接，监控网段上所有传入和传出的流量。由于可能存在数据包冲突，使用集线器无法保证检测引擎能监视更高流量网络上的所有数据包。对于低流量的简单网络，这不可能有问题。在高流量网络中，进行不同的选择可以实现更好的结果。请注意，如果集线器出现故障或断电，网络连接就会断开。在简单网络中，网络可能会断开。

某些设备虽然作为集线器销售，但实际上作用和交换机一样，并且不向各端口广播每个数据包。如果将受管设备与集线器连接，但无法监视所有流量，则可能需要购买一个不同的集线器或使用带 SPAN 端口的交换机。

使用 SPAN 端口

许多网络交换机包括能镜像一个或多个端口流量的 SPAN 端口。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。如果网络上已经配置包含此功能的交换机，只需在受管设备成本之外再多花一点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 端口可以处理 200 Mbps，并且三个镜像端口分别都可以处理 100 Mbps 的流量，则 SPAN 端口可能被过度订用并丢弃数据包，降低受管设备的效果。

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单个网段，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。受管设备提供多端口选项，可重新整合会话的双方，从而使解码器、预处理器和检测引擎可以评估整个流量。

铜接口上的内联部署布线

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，没有什么特殊布线问题。但是，如果用铜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) 支持一种叫做自动媒体相关接口交叉 (Auto-MDI-X) 的功能，该功能允许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。下表列出了各种设备以及它们是通过直通连接还是交叉连接执行旁路功能。

表 2-1　　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。在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到两个终端。

图 2-1　　直通旁路连接布线

对于使用交叉连接旁路的受管设备，请像在未部署设备的情况下一样正常连接设备。此链路应该在移除设备电源的情况下工作。大多数情况下应使用两根直通电缆将设备连接到两个终端。

图 2-2　　交叉旁路连接布线

下表列出了硬件旁路配置中哪些情况下应该使用交叉或直通电缆。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 （电缆和设备）数量应该为奇数，旁路才能正常工作。

表 2-2　　硬件旁路的有效配置

终端 1	电缆	受管设备	电缆	终端 2
MDIX	直通	直通	直通	MDI
MDI	交叉	直通	直通	MDI
MDI	直通	直通	交叉	MDI

表 2-2 硬件旁路的有效配置 （续）

终端 1	电缆	受管设备	电缆	终端 2
MDI	直通	直通	直通	MDIX
MDIX	直通	交叉	直通	MDIX
MDI	直通	交叉	直通	MDI
MDI	交叉	交叉	交叉	MDI
MDIX	交叉	交叉	直通	MDI

请注意，每个网络环境都可能是独一无二的，其终端都具有不同的 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，但是设备必须关机。确保两个终端之间可以通信。如果它们无法通信，则其中一根电缆类型不正确。将其中一根换成直通电缆或交叉电缆 （而且只能换一根）。

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，应重复此流程，确保在新设备断电的情况下两个终端可以通信，以防原装设备和更换设备具有不同的旁路特性。

只有在允许网络接口自动协商的情况下， Auto-MDI-X 设置才能正确运行。如果网络环境要求关闭 Network Interfaces 页面上的 Auto Negotiate 选项，则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 《*FireSIGHT 系统用户指南*》中“配置内联接口”。

特殊情况

连接8000 系列设备

向防御中心注册 8000 系列受管设备时，必须在连接的两端使用自动协商或将两端设置为相同的静态速度，确保稳定的网络链路。 8000 系列受管设备不支持半双工网络链路；也不支持连接的对端之间存在速度或双工配置上的差异。

更改远程控制台

在 70xx 子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从无人值守管理改为物理串行端口时，需要重新启动设备两次，查看预期的 LILO 启动提示符。

部署选项

将受管设备部署在网段上时，可以使用入侵检测系统监控流量或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：

- 使用虚拟交换机进行部署，第 2-8 页
- 使用虚拟路由器进行部署，第 2-9 页
- 使用混合接口进行部署，第 2-10 页
- 部署网关 VPN，第 2-11 页

- 使用基于策略的 NAT 进行部署，第 2-11 页
- 使用访问控制进行部署，第 2-12 页

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 强制和在域级丢弃网桥协议数据单元 (BPDU)。有关交换接口的详细信息，请参阅交换接口，第 2-3 页。

虚拟交换机必须包含两个或多个交换接口，用以处理流量。对于每个虚拟交换机，系统交换机仅为配置为交换接口的端口集交换流量。例如，如果配置带有四个交换接口的虚拟交换机，系统通过其中一个端口接收流量时，只将这些数据包广播至交换机的其余三个端口。

要配置允许流量通信的虚拟交换机，您可以在物理端口配置两个或多个交换接口，添加并配置虚拟交换机，然后将虚拟交换机分配给交换接口。系统会放弃在外部物理接口上接收的没有交换接口等待接收的任何流量。如果系统收到没有 VLAN 标记的数据包并且该端口未配置物理交换接口，系统将放弃该数据包。如果系统收到带有 VLAN 标记的数据包，并且未配置逻辑交换接口，系统也会放弃数据包。

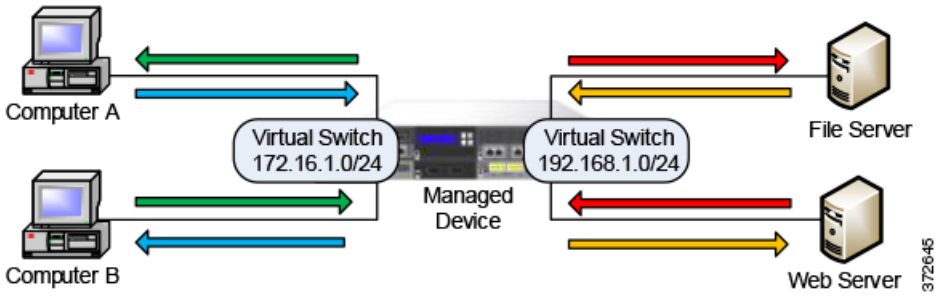
必要时可以在物理端口上定义更多逻辑交换接口，但是，必须将一个逻辑交换接口分配给虚拟交换机，用于处理流量。

虚拟交换机具有可扩展性优势。使用物理交换机时，会受到交换机上可用端口数量的限制。用虚拟交换机代替物理交换机，就只受带宽和想要实现的部署的复杂程度限制。

请在要使用第 2 层交换机的场景下使用虚拟交换机，例如要确保工作站连接和网络分段的情况下。第 2 层交换机在员工大部分时间都位于地网段的情况下特别有效。大型部署（例如，包含广播流量、 Voice-over-IP 或多个网络的部署）可以在部署的小型网段使用虚拟交换机。

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。

图 2-3　　受管设备上的虚拟交换机



在本示例中，该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 （用红线和橙色线表示）。但是，由于计算机和服务器不在同一虚拟交换机上，流量无法在计算机和网络或文件服务器之间传输。

有关配置交换接口和虚拟交换机的详细信息，请参阅 《*FireSIGHT 系统用户指南*》中“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*，路由两个或多个网络之间的流量，或将专用网络连接到公用网络 （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 强制。有关路由接口的详细信息，请参阅路由接口，第 2-4 页。必须使用带网关 VPN 的虚拟路由器。有关详细信息，请参阅部署网关 VPN，第 2-11 页。

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。必须为虚拟路由器分配逻辑路由接口，用以路由流量。

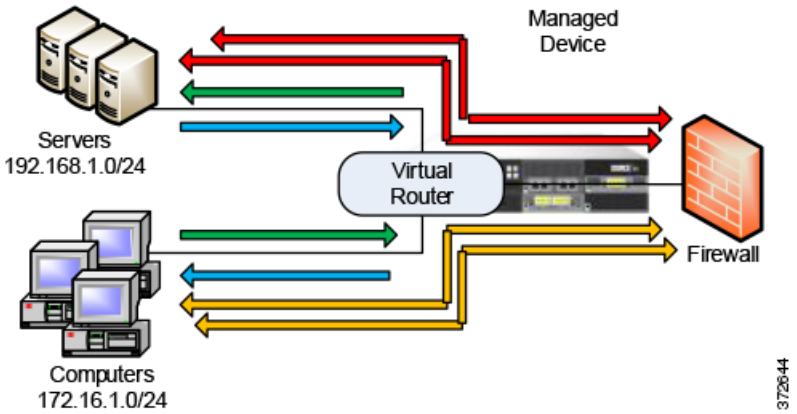
要配置虚拟路由器，您可以使用物理或逻辑配置设置路由接口。可以配置处理不带标记的 VLAN 流量的物理路由接口。还可以创建处理带指定 VLAN 标记的流量的逻辑路由接口。系统会丢弃在外部物理接口上接收的没有路由接口等待接收的任何流量。如果系统收到没有 VLAN 标记的数据包并且该端口未配置物理路由接口，系统将丢弃该数据包。如果系统收到带有 VLAN 标记的数据包，并且未配置逻辑路由接口，系统也会丢弃数据包。

虚拟路由器具有可扩展性优势。物理路由器限制可以连接的网络数量时，可在同一受管设备上配置多个虚拟路由器。将多个路由器配置在同一设备上可降低部署的物理复杂性，实现从同一设备监控和管理多个路由器。

在想要使用第 3 层物理路由器的情况下使用虚拟路由器在部署中的多个网络之间转发流量或将专用网络连接至公用网络。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，可以使用一台设备将多个网络互相连接起来，并连接至互联网。

图 2-4　　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，在网络 172.16.1.0/20 上的计算机和网络 192.168.1.0/24 上的服务器之间实现流量传输 （用蓝线和绿线表示）。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 （用红线和橙色线表示）。

有关详细信息，请参阅 《*FireSIGHT 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

可在受管设备上创建*混合接口*，使用虚拟交换机和虚拟路由器在第 2 层和第 3 层网络之间路由流量。这样就提供了一个接口，既可以路由交换机上的本地流量，又可以路由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。请参阅使用基于策略的 NAT 进行部署，第 2-11 页。

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。普通部署包括配置为虚拟交换机在本地网络上传输流量的两个交换接口和路由流向专用或公用网络的流量的虚拟路由器。

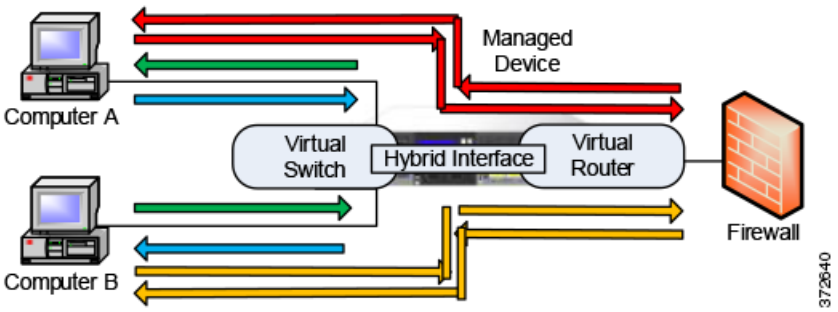
要创建混合接口，首先要配置虚拟交换机和虚拟路由器，然后将虚拟交换机和虚拟路由器添加到混合接口上。未与虚拟交换机和虚拟路由器关联的混合接口无法用于路由，而且不会生成或响应流量。

混合接口具有尺寸紧凑及可扩展性优势。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。在空间和资源有限的小分段部署中，这种部署方式是理想之选。

部署混合接口时，可以允许流量从本地网络传递到外部网络或互联网等公用网络，同时解决虚拟交换机和虚拟路由器的单独安全性顾虑。

图 2-5　　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 （用蓝线和绿线表示）。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递至防火墙 （用红线和橙色线表示）。

有关详细信息，请参阅 《*FireSIGHT 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，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它们之间的通信。

使用 Internet 协议安全 (IPSec) 协议集，配置 FireSIGHT 系统，在从思科受管设备的虚拟路由器到远程设备或其他第三方 VPN 终端之间建立 VPN 安全隧道。建立 VPN 连接后，本地网关后面的主机可以通过 VPN 安全隧道连接到远程网关后面的主机。VPN 终端利用 Internet 密钥交换 (IKE) V1 或 V2 协议相互验证，为此隧道创建安全关联。系统在 IPSec 验证报头 (AH) 模式或 IPSec 封装安全负载 (ESP) 模式下运行。 AH 和 ESP 都提供验证，而且 ESP 还提供加密。

网关 VPN 可以用于点对点、星型或网状部署：

- 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启用 VPN 的受管设备。

  远程主机使用公用网络连接网络中的主机时，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，集线器节点是一台启用 VPN 的受管设备，位于总部。叶节点位于分支机构并发起大部分流量。

  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和分支机构，为所有员工提供对组织网络的受控访问。

- 网状部署通过 VPN 隧道将所有终端连接在一起。这种部署方式可提供冗余，在某个终端出现故障时，其他终端仍然能够相互通信。

  使用网状部署连接一组分散的分支机构，确保即使一个或多个 VPN 隧道出现故障，流量仍然可以传输。此配置中部署的启用 VPN 的受管设备的数量决定了冗余级别。

有关网关 VPN 配置和部署的详细信息，请参阅 《*FireSIGHT 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：全部， ASA FirePOWER 除外

可以使用*基于策略的网络地址转换* (NAT) 定义指定想要如何执行 NAT 的策略。策略可以针对单个接口、一个或多个设备或整个网络。

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，直到应用第一条匹配规则。

基于策略的 NAT 通常用于以下部署：

- 隐藏专用网络地址。

  从专用网络访问公用网络时， NAT 将专用网络地址转换为公用网络地址。具体专用网络地址对公用网络是隐藏的。

- 允许访问专用网络服务。

  公用网络访问专用网络时， NAT 将公用地址转换为专用网络地址。公用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。

当专用网络上的服务器访问与其连接的专用网络上的服务器时， NAT 转换两个专用网络之间的专用地址，确保专用地址中没有重复而且流量可以在它们之间传输。

使用基于策略的 NAT 免除了对额外硬件的需求并且将入侵检测或防御系统和 NAT 的配置整合到了一个统一的用户界面中。有关详细信息，请参阅《*FireSIGHT 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、检查和记录可以进入、退出网络或在网络内传输的流量。下一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《*FireSIGHT 系统用户指南*》。

访问控制策略决定了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提供更细化的控制。

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，无需进一步检查
- 允许所有流量进入网络，并且仅仅使用网络发现策略检查流量
- 允许所有流量进入网络，并且通过入侵和网络发现策略检查流量

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 地址指定可以按照访问控制策略流经网络的流量。此功能可以创建关于不允许的 IP 地址的黑名单，系统会阻止并且不检查这些地址的流量。

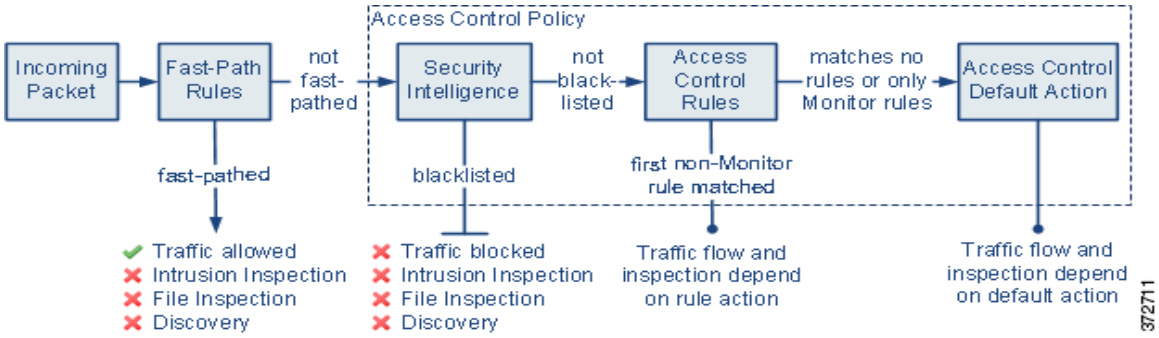
此部署示例说明了常见的网段。在这些位置中的每一处部署受管设备具有不同的作用。以下各节将提供典型的位置建议：

- 在防火墙内部，第 2-13 页说明访问控制如何对通过防火墙的流量发挥作用。
- 在 DMZ 上，第 2-13 页说明 DMZ 中的访问控制如何保护面向外部的服务器。
- 在内部网络上，第 2-14 页说明访问控制如何保护内部网络免受蓄意或意外攻击。
- 在核心网络上，第 2-14 页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。
- 在远程或移动网络上，第 2-15 页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、移动访问和远程网络。

下图说明了通过 FireSIGHT 系统的流量，并提供了一些关于对该流量执行的检测类型的详细信息。请注意，系统不检查通过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，但是系统不会对受信任或受阻止的流量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，流量通过快速路径传输。如果没有匹配项，基于安全情报的过滤功能将确定是否将此数据包列入黑名单。否则，将应用所有访问控制规则。如果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，它允许持续评估流量。）每个访问控制策略的默认操作管理未通过快速路径传输或未列入黑名单的流量，或与非监控规则匹配的流量。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提供更细化的控制。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）。

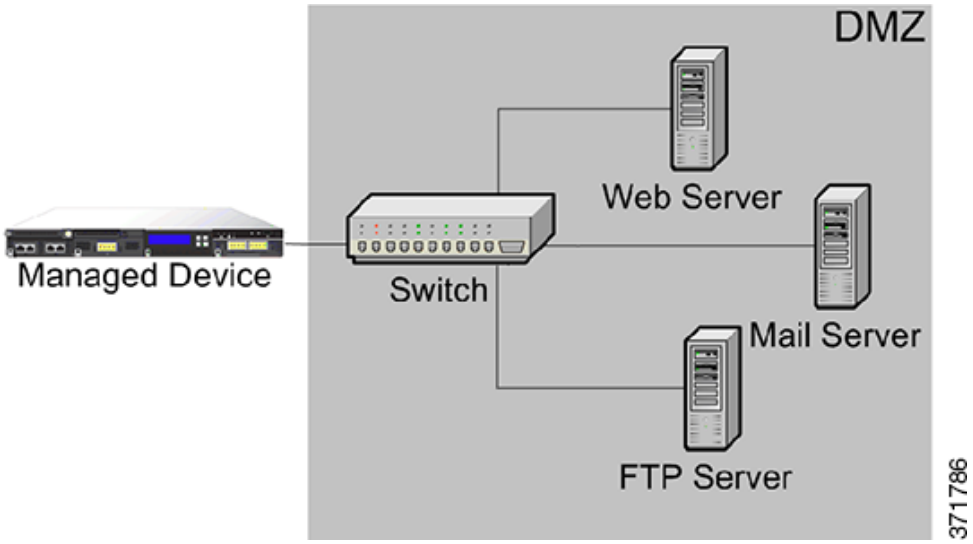
在 DMZ 上

DMZ 包含面向外部的服务器 （例如网络、 FTP、 DNS 和邮件），并可为内部网络上的用户提供邮件转发和网络代理等服务。

DMZ 中存储的内容是静态的，变更的计划和执行都会有明确的沟通和事先通知。本网段上的攻击通常是入站攻击，并且会立即变得透明，因为在 DMZ 中服务器上只允许执行事先计划好的变更。此网段的有效控制访问策略能够严密控制对服务的访问，并搜索是否存在任何新的网络事件。

DMZ 中的服务器可以包含 DMZ 能够通过网络查询的数据库。像 DMZ 一样，不应出现意外的变更，但是，数据库内容比网站或其他 DMZ 服务更加敏感，需要更好的保护。强大的入侵策略加上 DMZ 访问控制策略是一种行之有效的方法。

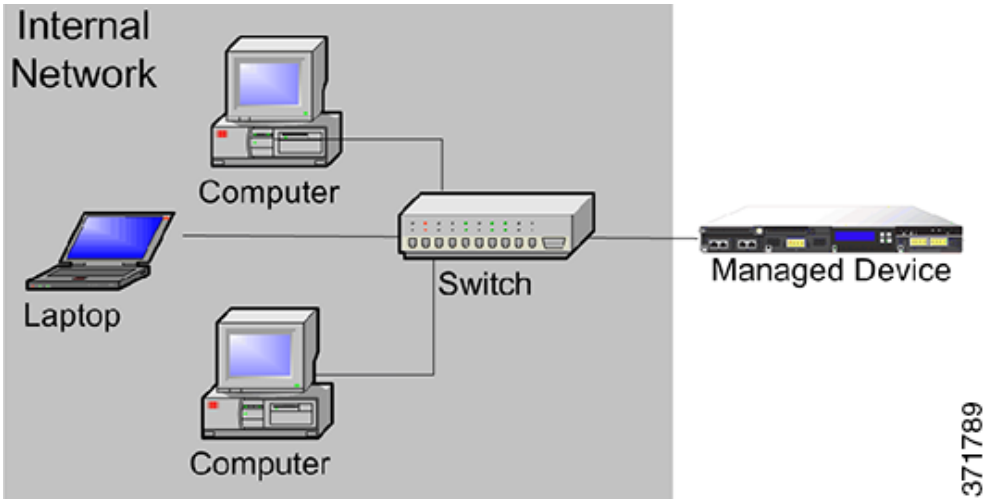
此网段上部署的受管设备可以检测来自 DMZ 中受威胁的服务器的针对互联网的攻击。使用网络发现监控网络流量有助于监控这些受威胁的服务器是否出现了可能表示 DMZ 中服务器受到了攻击的变化 （例如，突然出现意外的服务）。



在内部网络上

恶意攻击可能来自内部网络中的计算机。这种攻击可能是故意行为（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受到感染，在连接到内部网络后传播了病毒）。内部网络的风险也可能是出站风险（例如，计算机向外部可疑 IP 地址发送信息）。

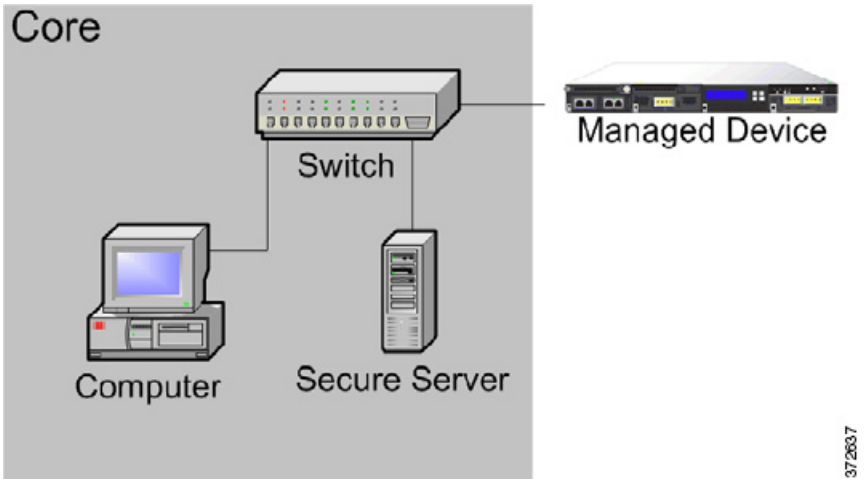
除了出站流量外，此动态网络要求对所有内部流量执行严格的访问控制策略。增加访问控制规则，严格控制用户和应用之间的流量。



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资产。虽然核心资产因企业性质而异，典型的核心资产包括财务与管理中心或知识产权资源库。如果核心资产的安全遭受侵犯，企业可能会毁灭。

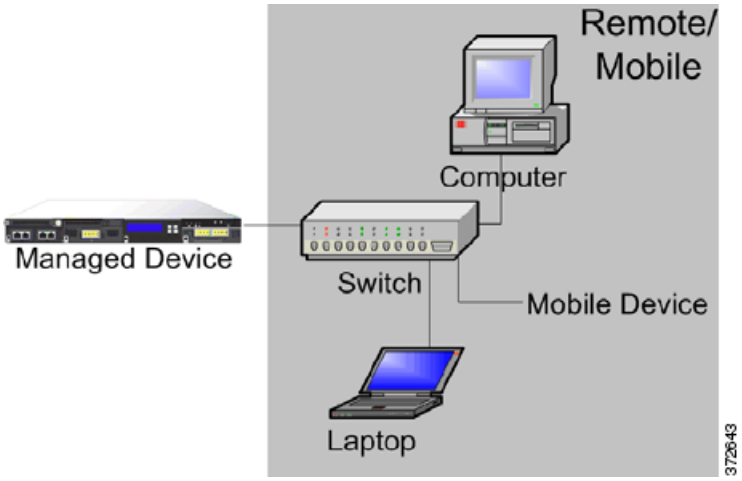
虽然此网段必须随时可用，以保证企业正常运行，但是必须进行严格的限制和控制。访问控制应确保远程网络或移动设备等存在最高风险的网段无法访问这些资产。此网段必须使用最严格的控制，对用户和应用访问执行严格的规则。



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。移动设备和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）变得越来越普遍。

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源的流量。策略通过严格限制用户、网络和应用访问核心资源的方式来降低风险。



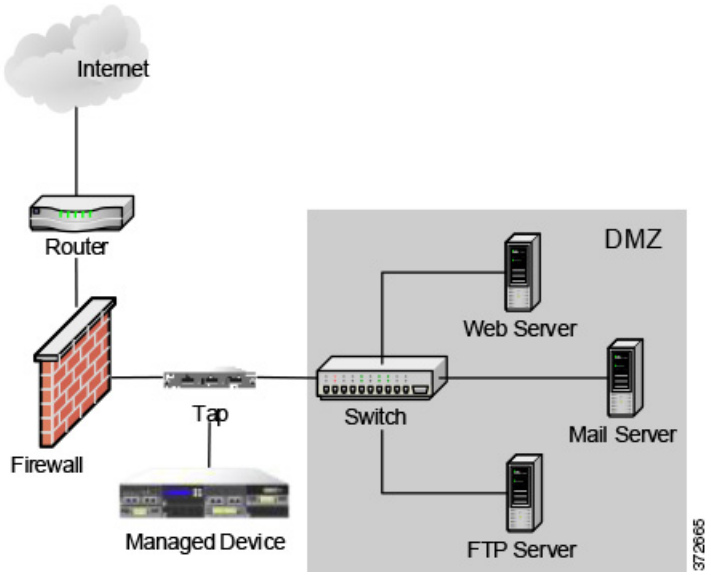
使用多端口受管设备

受管设备在其网络模块上提供多个检测端口。可以在受管设备上使用多端口执行以下操作：

- 重组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

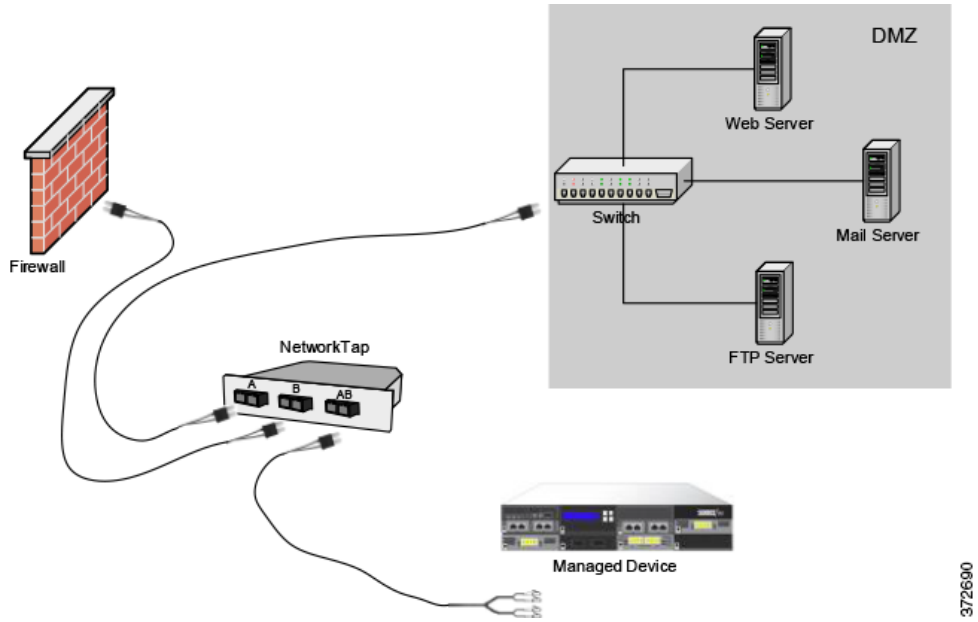
注　虽然每个端口能够接收设备额定的完整吞吐量，但是，如果受管设备的总流量超过额定带宽，一定会出现丢包现象。

在带网络分路器的受管设备上部署多端口的流程非常简单。下图显示了一个在大流量网段中安装的网络分路器。

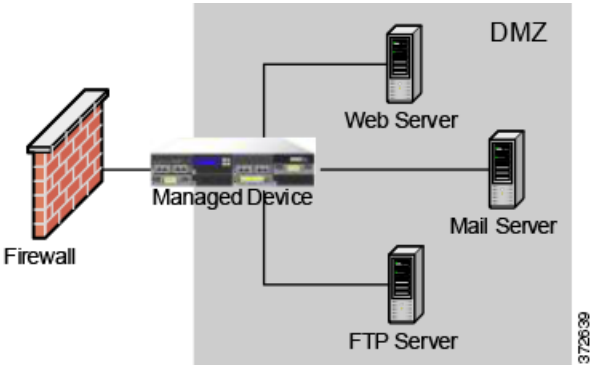


在此场景中，分路器通过单独的端口传输传入和传出的流量。在受管设备上将多端口接口适配器卡连接至分路器时，受管设备就能将流量整合到一个统一的数据流中，从而可以对其进行分析。

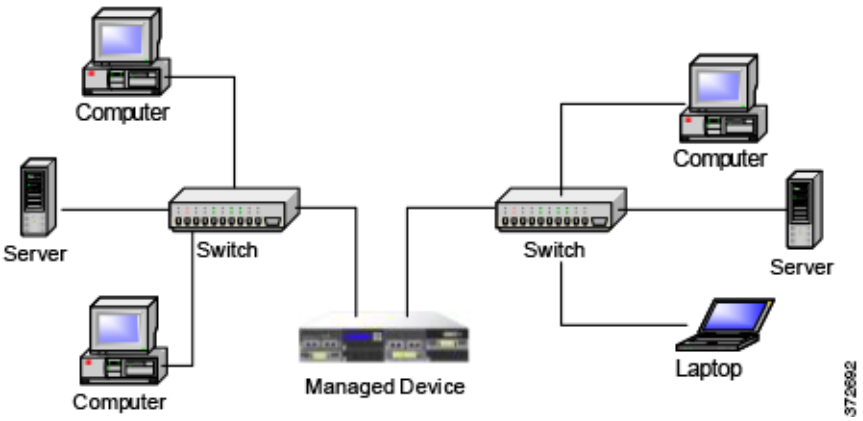
请注意，对于千兆光纤分路器，如下图所示，受管设备上的端口都被分路器的连接器占用。



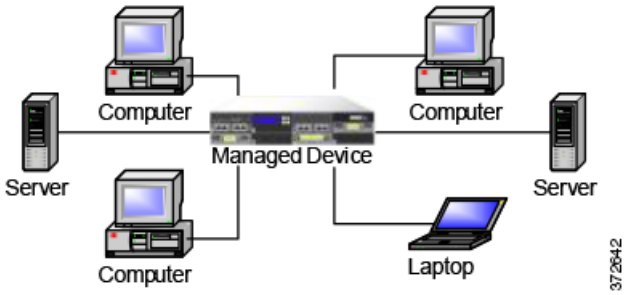
可以使用虚拟交换机替换部署中的分路器和交换机。请注意，如果使用虚拟交换机替换分路器，就会失去分路器数据包传输保障。



还可以创建接口，捕获来自单独网络的数据。下图显示了一台单独的设备，该设备带一个双端口适配器和两个接口，其中两个接口与两个网络连接。



除了使用一个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替换部署中的两个交换机。



复杂的网络部署

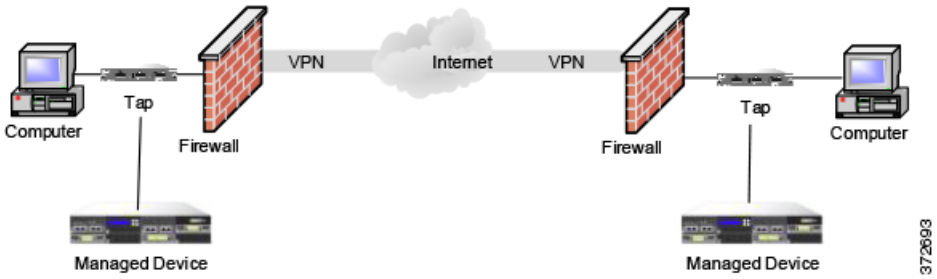
企业网络可能需要远程访问，例如使用 VPN 或有业务合作伙伴或银行连接等多个入口点。以下各节将介绍这些部署涉及的一些问题：

- 与 VPN 集成，第 2-18 页
- 检测其他入口点上的入侵，第 2-19 页
- 在多站点环境中进行部署，第 2-20 页
- 在复杂的网络中集成受管设备，第 2-22 页

与 VPN 集成

虚拟专用网络或 VPN 使用 IP 隧道技术为互联网上的远程用户提供本地网络安全性。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，从而使数据包可以通过公用网络采用与其他数据包大致一样的方式进行传输。数据包到达目标网络时，负载被解密，数据包被发送到正确的主机。

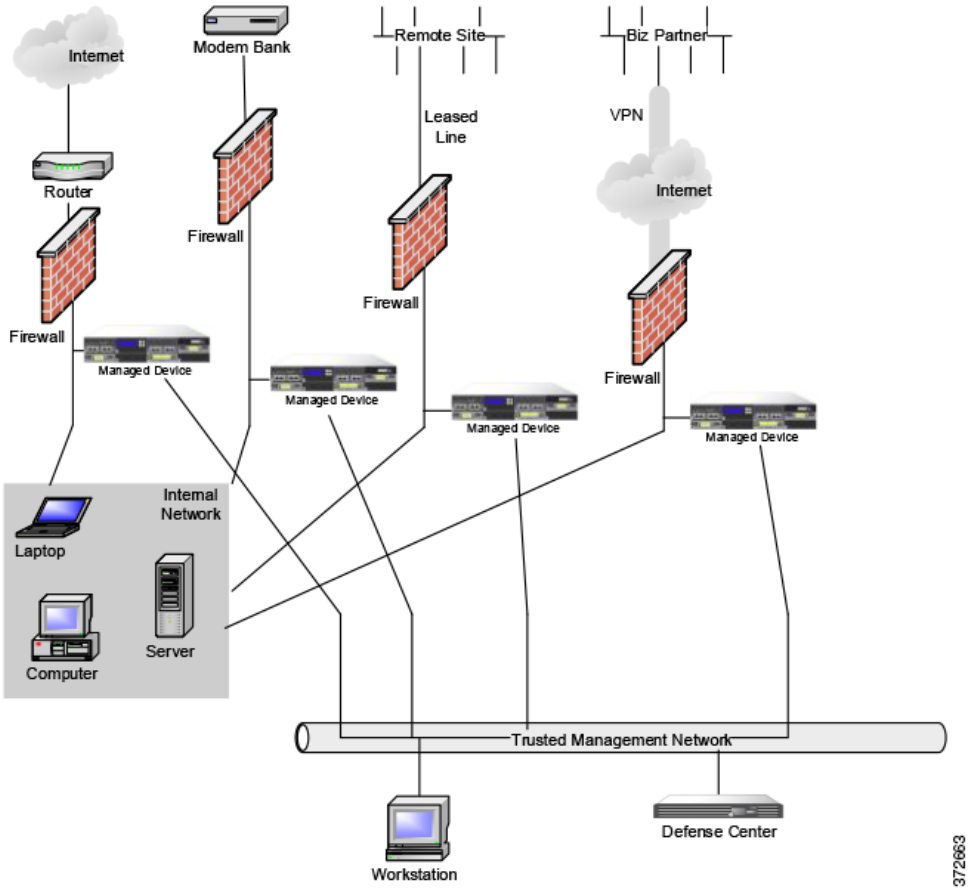
由于网络设备无法分析 VPN 数据包的加密负载，在 VPN 连接的端接终端之外配置受管设备能确保可以访问所有数据包信息。下图说明了如何在 VPN 环境中部署受管设备。



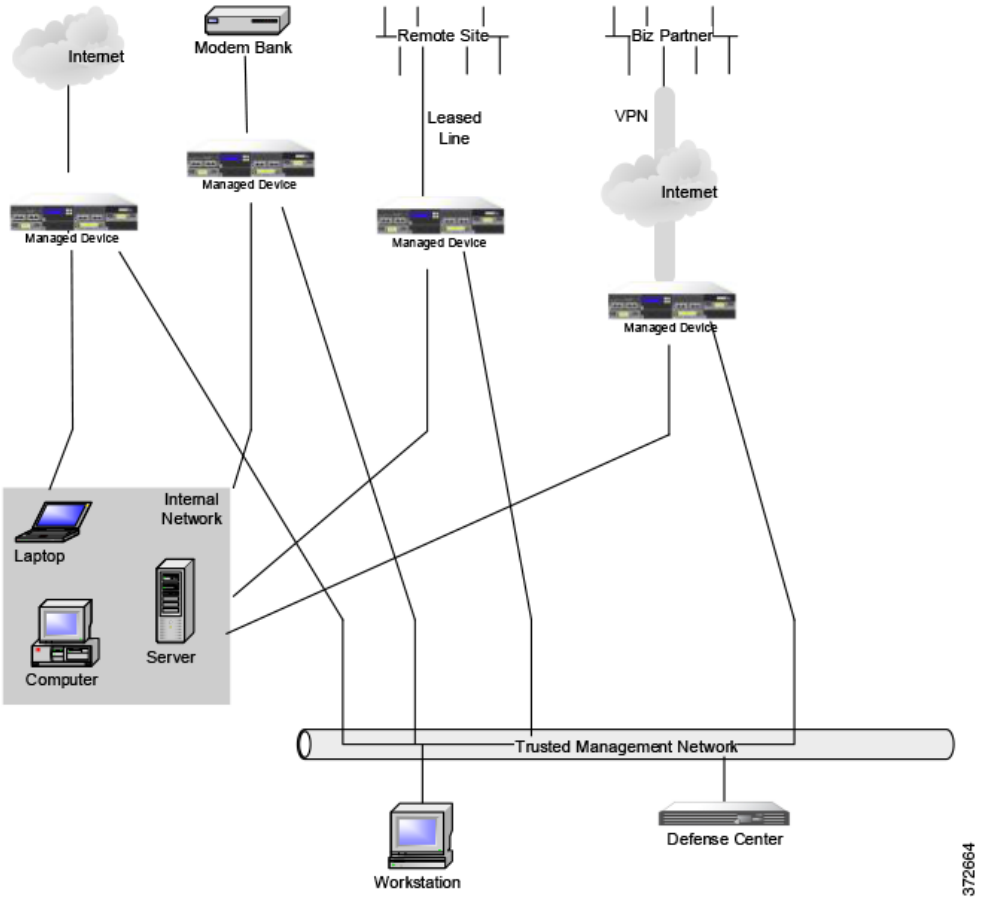
可用受管设备替换 VPN 连接任一端的分路器。请注意，如果使用虚拟交换机替换分路器，就会失去分路器数据包传输保障。

检测其他入口点上的入侵

许多网络包括不止一个接入点。有些企业不是使用一个边界路由器与互联网连接，而是使用互联网、调制解调器组与连接业务合作伙伴网络的直接链路的组合。一般来说，应在防火墙附近和对于企业数据完整性与机密性很重要的网段部署受管设备（在防火墙内部或在防火墙外部或在内外部都部署）。下图显示了如何在具有多个入口点的复杂网络上的关键位置安装受管设备。

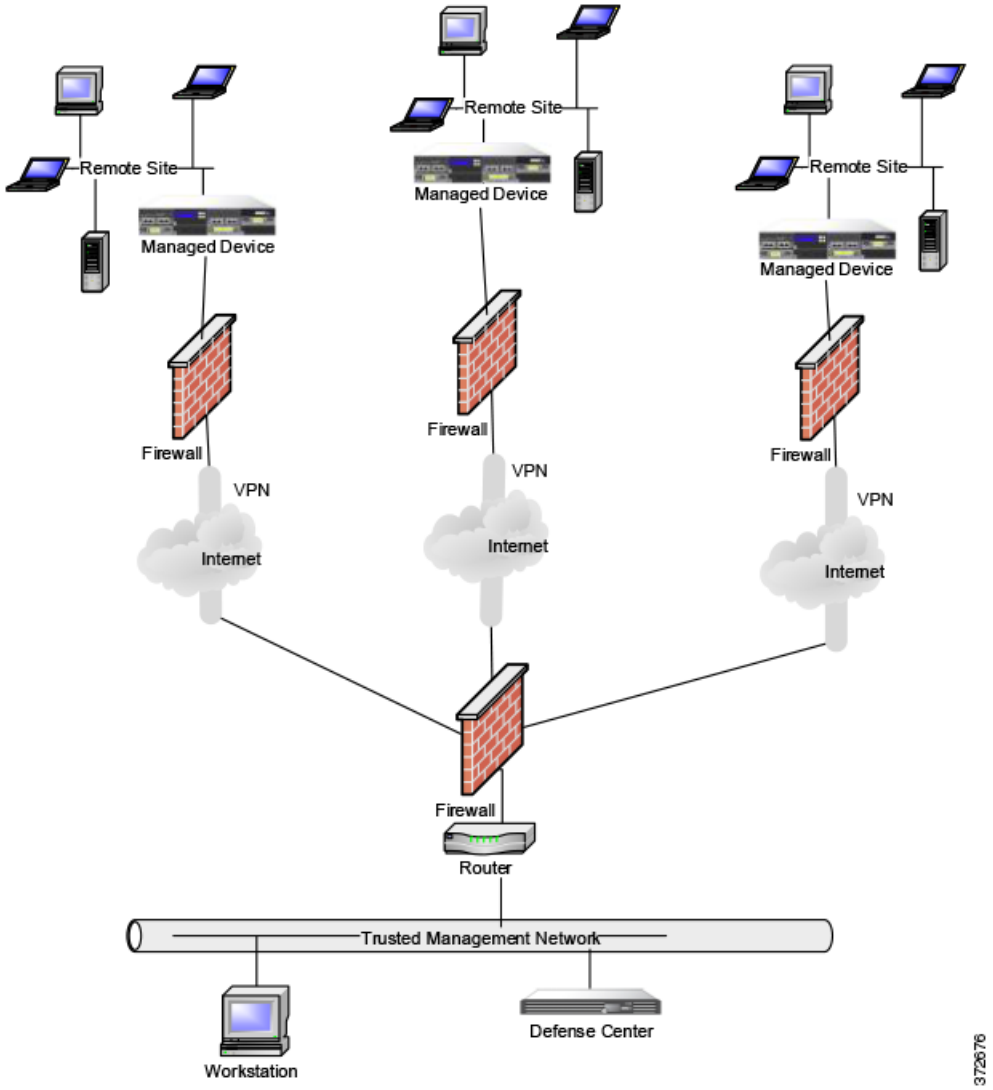


可以用网段上部署的受管设备替换防火墙和路由器。

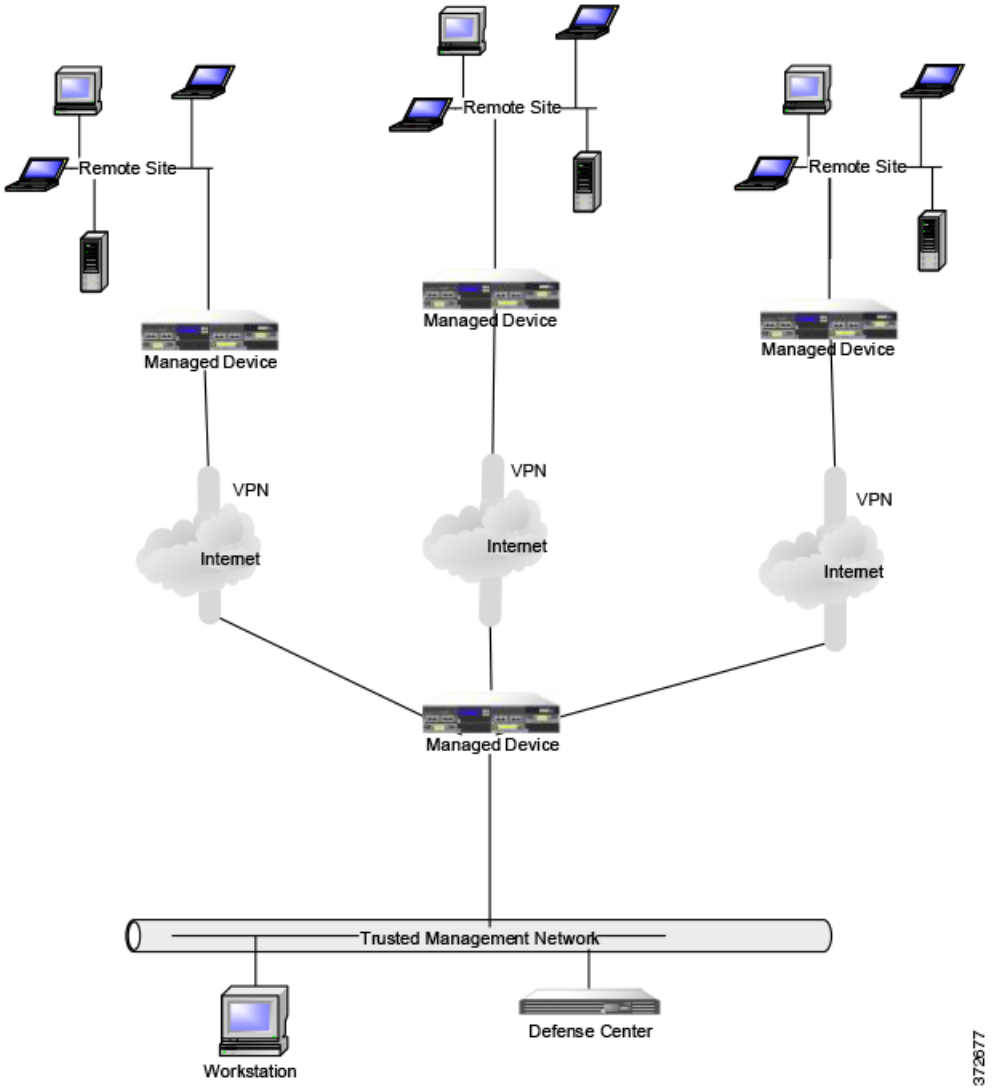


在多站点环境中进行部署

许多组织想要扩展入侵检测，使之覆盖地理位置分散的整个企业，然后从一个统一位置分析所有数据。 FireSIGHT 系统提供防御中心，汇聚和关联来自在整个组织中的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，如下图所示，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。



可以用每个网段上部署的受管设备替换防火墙和路由器。



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。此节描述在存在代理服务器、NAT 设备和 VPN 的环境中部署时与网络发现和漏洞分析相关的一些问题，此外还将提供关于使用 FireSIGHT 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) 设备或软件可在整个防火墙中使用，有效地隐藏防火墙后面的内部主机 IP 地址。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，思科建议将受管设备配置在受代理或 NAT 设备保护的网段内，从而确保主机能被正确检测。

与负载平衡方法集成

在有些网络环境中，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，系统检测操作系统的变更，无法提供高置信度的静态操作系统标识。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变更事件或以较低的置信度显示静态操作系统标识。

其他检测注意事项

如果正在识别的主机 TCP/IP 堆栈已经更改，系统可能无法正确识别此主机操作系统。在某些情况下，这样做是为了提高性能。例如，鼓励运行 Internet 信息服务 (IIS) 网络服务器的 Windows 主机的管理员增大 TCP 窗口，允许接收更大的数据量，从而提高性能。在其他情况下，可通过 TCP/IP 堆栈更改模糊真正的操作系统，阻止准确识别和避免有针对性的攻击。这么做旨在解决这样一种可能的情况，即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，然后利用针对该操作系统的漏洞进行有针对性的攻击。

安装 FireSIGHT 系统设备

FireSIGHT 系统设备可作为更大型 FireSIGHT 系统部署的一部分轻松安装在网络上。可将设备安装在网段上以检查流量，并根据应用的入侵策略生成入侵事件。这些数据将被传输到防御中心，后者负责管理一个或多个设备以关联整个部署中的数据，以及协调和应对您遇到的安全威胁。

您可以在一个位置预配置多个设备，以便用于不同的部署位置。有关预配置的指导，请参阅预配置 FireSIGHT 系统设备，第 E-1 页。

注 有关安装 ASA FirePOWER 设备的信息，请参阅 ASA 文档。

有关安装 FireSIGHT 系统设备的详细信息，请参阅以下各节：

附件

以下列表列出了随 FireSIGHT 系统设备一起提供的组件。打开系统及相关配件的包装后，请对照以下清单检查包装内容是否完整：

- 一台 FireSIGHT 系统设备
- 电源线 （配有冗余电源的设备随附两根电源线）
- 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
- 一个机架安装套件（单独提供适用于 3D7010、3D7020 和 3D7030 的必要托架和机架安装套件）

安全注意事项

在安装设备之前，思科建议您注意以下事项：

- 将 FireSIGHT 系统设备放在安全位置内的带锁的机架中，以防未经授权的访问。
- 只有经过培训的合格人员才可以安装、更换、管理或维修 FireSIGHT 系统设备。
- 务必将管理接口连接到未经授权不可访问的安全的内部管理网络。
- 确定可以访问设备的特定工作站 IP 地址。仅允许使用设备系统策略中的访问列表的特定主机访问设备。有关详细信息，请参阅 《*FireSIGHT 系统用户指南*》。

识别管理接口

可使用管理接口将部署中的每个设备连接到网络。这样使防御中心可以与其托管的设备进行通信并管理这些设备。

FireSIGHT 系统设备可安装在不同的硬件平台上交付。在安装过程中，请确保参阅适用于您设备的正确图示：

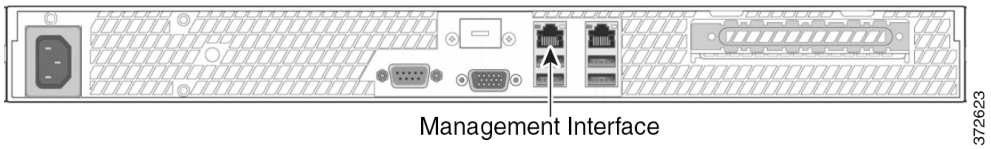
- FireSIGHT 防御中心 750，第 3-2 页
- FireSIGHT 防御中心 1500，第 3-2 页
- FireSIGHT 防御中心 3500，第 3-3 页
- FireSIGHT 7000 系列，第 3-3 页
- FireSIGHT 8000 系列，第 3-3 页

FireSIGHT 防御中心 750

DC750 可作为 1U 设备提供。

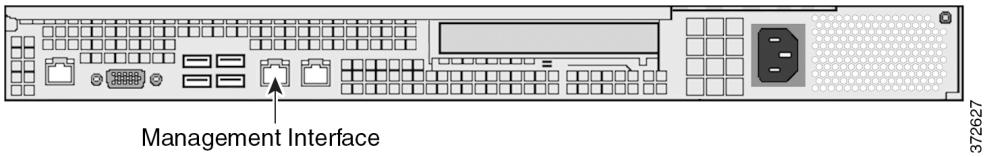
以下机箱背面图示出了 DC750 的管理接口的位置。

图 3-1 DC750



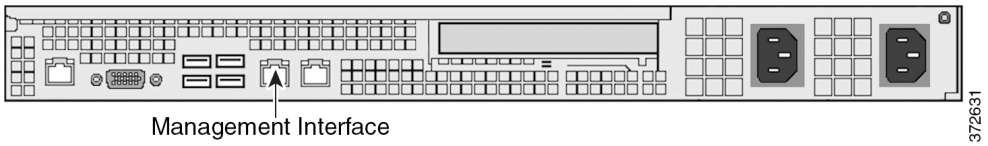
FireSIGHT 防御中心 1500

DC1500 可作为 1U 设备提供。以下机箱背面图示出了管理接口的位置。



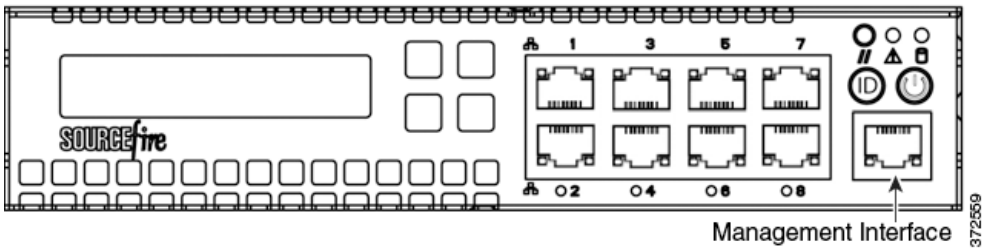
FireSIGHT 防御中心 3500

DC3500 可作为 1U 设备提供。以下机箱背面图示出了管理接口的位置。

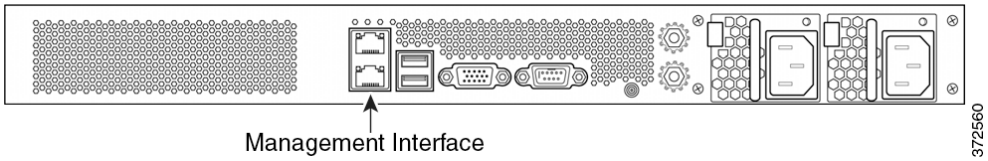


FireSIGHT 7000 系列

3D7010、3D7020 和 3D7030 是宽度为机箱托架宽度一半的 1U 设备。以下机箱正面图示出了管理接口。

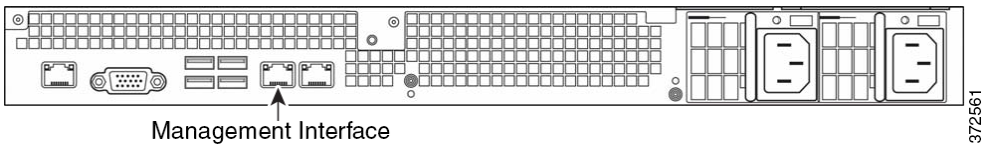


3D7110/7120、 3D7115/7125 和 AMP7150 可作为 1U 设备提供。以下机箱背面图示出了管理接口的位置。

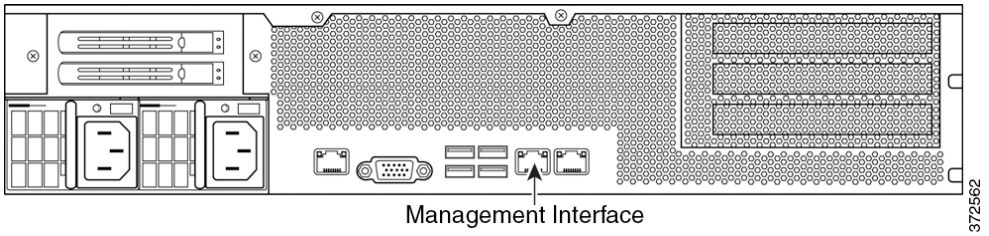


FireSIGHT 8000 系列

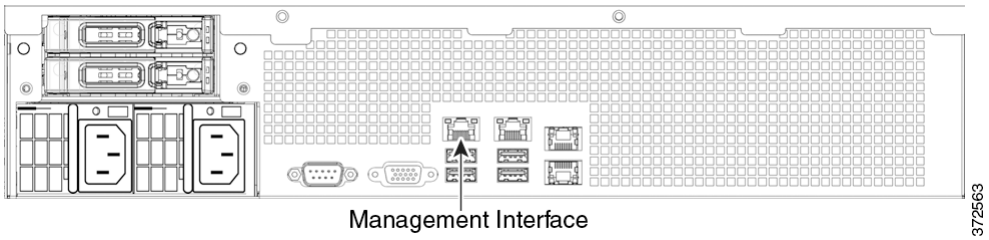
3D8120、3D8130、3D8140 和 AMP8150 可作为 1U 设备提供。以下机箱背面图示出了管理接口的位置。



3D8250 可作为 2U 设备提供。3D8260、3D8270 和 3D8290 可作为带有一个、两个或三个辅助 2U 设备的 2U 设备提供。以下机箱背面图示出了每个 2U 设备的管理接口的位置。



3D8350 可作为 2U 设备提供。3D8360、3D8370 和 3D8390 可作为带有一个、两个或三个辅助 2U 设备的 2U 设备提供。以下机箱背面图示出了每个 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到网段。每个设备可监控的网段数量取决于设备的感应接口数量以及您想要在网段上使用的连接类型 （被动、内联、路由或交换）。

以下部分介绍每个受管设备的感应接口：

- 要确定 7000 系列的感应接口的位置，请参阅 FirePOWER 7000 系列，第 3-4 页。
- 要确定 8000 系列的模块插槽的位置，请参阅 FirePOWER 8000 系列，第 3-7 页。
- 要确定 8000 系列网络模块的感应接口的位置，请参阅 8000 系列模块，第 3-9 页。

有关连接类型的信息，请参阅了解接口，第 2-2 页。

FirePOWER 7000 系列

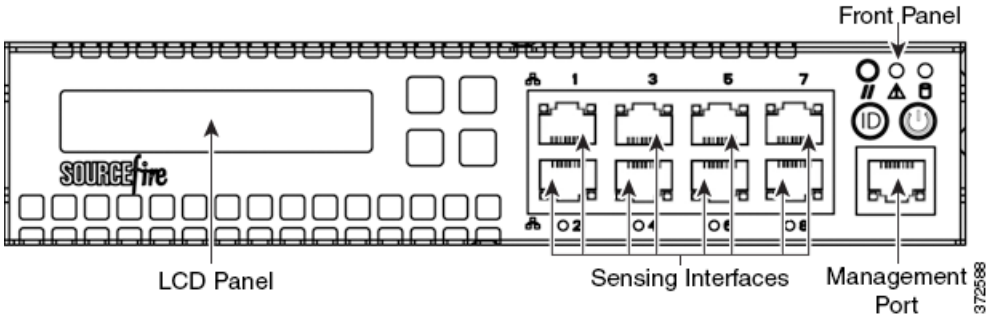
7000 系列可提供以下配置：

- 1U 设备，宽度为机架宽度一半，带八个铜接口，每个接口都支持可配置旁路功能。
- 1U 设备，带八个铜接口或八个光纤接口，每个接口都支持可配置旁路功能。
- 1U 设备，带四个支持可配置旁路功能的铜接口和八个不支持旁路功能的小型封装热插拔 (SFP) 端口。

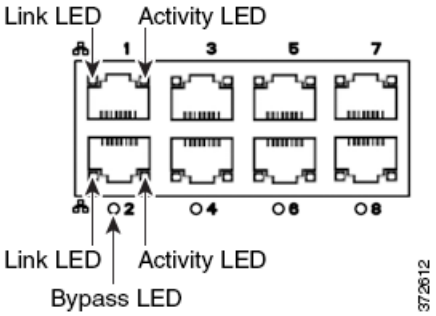
3D7010、 3D7020 和 3D7030

3D7010、 3D7020 和 3D7030 带有八个铜端口感应接口，每个接口都支持可配置旁路功能。以下机箱正面图示出了这些感应接口的位置。

图 3-2 支持可配置旁路功能的八端口 1000BASE-T 铜接口



使用这些接口最多可以对八个独立网段进行被动监控。您还可以内联方式使用成对接口或者在旁路模式下对成对接口进行内联，这样最多可在四个网络上将设备部署为入侵防御系统。



如果您想利用设备的自动旁路功能，必须将两个接口 （接口 1 和 2、接口 3 和 4、接口 5 和 6 或者接口 7 和 8）纵向连接到网段。有了自动旁路功能，即使在设备出现故障或断电的情况下也可以进行流量传输。用电缆连接接口后，您应该使用网络界面将一对接口配置为内联集并对其启用旁路模式。

3D7110 和 3D7120

3D7110 和 3D7120 带有八个铜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。以下机箱正面图示出了这些感应接口的位置。

图 3-3 3D7110 和 3D7120 的铜接口

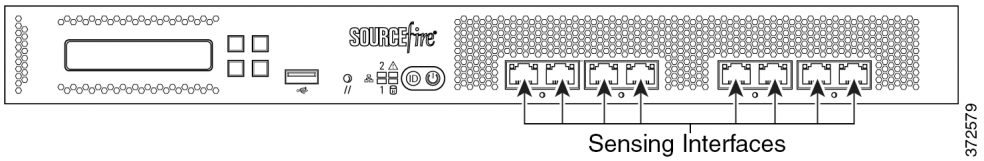
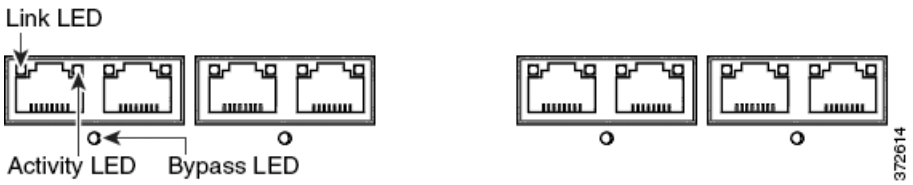


图 3-4 八端口 1000BASE-T 铜接口



使用这些接口最多可以对八个独立网段进行被动监控。您还可以内联方式使用成对接口或者在旁路模式下对成对接口进行内联，这样最多可在四个网络上将设备部署为入侵防御系统。

如果您想利用设备的自动旁路功能，必须将左侧或右侧的两个接口连接到网段。有了自动旁路功能，即使在设备出现故障或断电的情况下也可以进行流量传输。用电缆连接接口后，您应该使用网络界面将一对接口配置为内联集并对其启用旁路模式。

图 3-5 3D7110 和 3D7120 的光纤接口

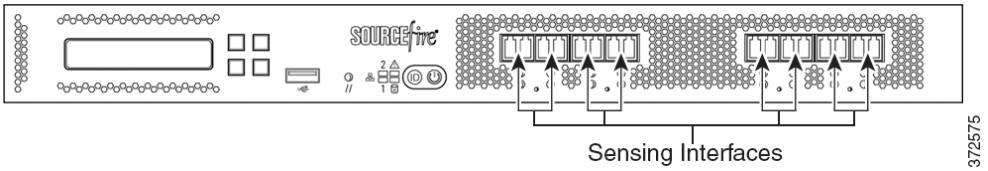


图 3-6 支持可配置旁路功能的八端口 1000BASE-SX 光纤接口

支持可配置旁路功能的八端口 1000BASE-SX 光纤配置使用 LC 型 （本地连接器）光纤收发器。

使用这些接口最多可以对八个独立网段进行被动监控。您还可以内联方式使用成对接口或者在旁路模式下对成对接口进行内联，这样最多可在四个网络上将设备部署为入侵防御系统。

提示 为了获得最佳性能，请按照连续顺序使用接口组。如果您跳过任何接口，可能会导致性能下降。

如果您想利用设备的自动旁路功能，必须将左侧或右侧的两个接口连接到网段。有了自动旁路功能，即使在设备出现故障或断电的情况下也可以进行流量传输。用电缆连接接口后，您应该使用网络界面将一对接口配置为内联集并对其启用旁路模式。

3D7115、 3D7125 和 AMP7150

3D7115、3D7125 和 AMP7150 设备带有四个支持可配置旁路功能的铜端口接口和八个不支持旁路功能的小型封装热插拔 (SFP) 端口。以下机箱正面图示出了这些感应接口的位置。

图 3-7 3D7115 和 3D7125 的铜接口和 SFP 接口

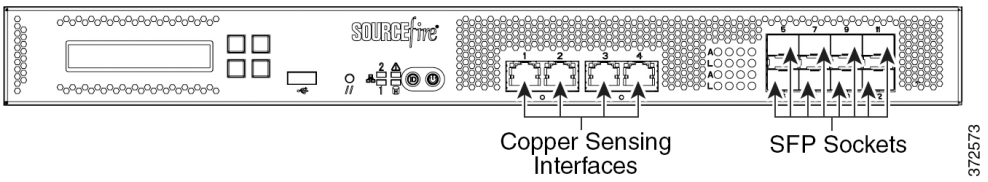
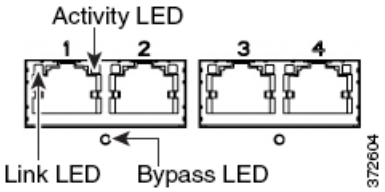


图 3-8 四个 1000BASE-T 铜接口



使用这些铜接口最多可以对四个独立网段进行被动监控。您还可以内联方式使用成对接口或者在旁路模式下对成对接口进行内联，这样最多可在两个网络上将设备部署为入侵防御系统。

如果您想利用设备的自动旁路功能，必须将左侧或右侧的两个接口连接到网段。有了自动旁路功能，即使在设备出现故障或断电的情况下也可以进行流量传输。用电缆连接接口后，您应该使用网络界面将一对接口配置为内联集并对其启用旁路模式。

SFP 接口

将思科 SFP 收发器安装到 SFP 插槽时，您最多可以对八个独立网段进行被动监控。您还可以内联方式使用成对接口或者使用非旁路模式，这样最多可在四个网络上将设备部署为入侵检测系统。

思科 SFP 收发器可以是 1G 铜缆收发器、 1G 短距离光纤收发器或 1G 长距离收发器，均可热插拔。您可以在采用被动或内联配置的设备中结合使用任何铜缆收发器或光纤收发器。请注意，SFP 收发器没有旁路功能，不应用于入侵防御部署中。为确保兼容性，请务必使用思科提供的 SFP 收发器。有关详细信息，请参阅在 3D71x5 和 AMP7150 设备中使用 SFP 收发器，第 B-1 页。

图 3-9 SFP 收发器示例

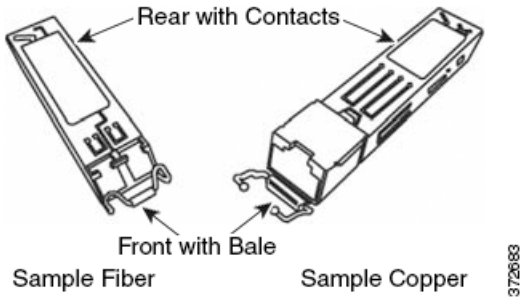
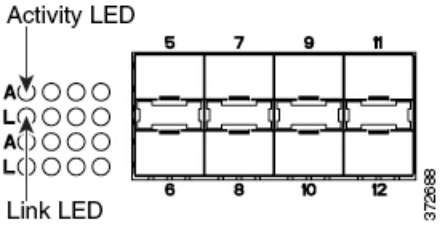


图 3-10 SFP 插槽



FirePOWER 8000 系列

8000 系列可作为带有 10G 网络交换机的 1U 设备提供，也可作为带有 10G 或 40G 网络交换机的 2U 设备提供。此设备可以完全组装的形式购买，或者，您可以自行安装带有感应接口的网络模块。

注 如果您将某网络模块安装在设备上与之不兼容的插槽中 （例如，将 40G 网络模块安装在 3D8250 或 3D8350 的插槽 1 和插槽 4 中），或者有网络模块与您的系统不兼容，那么，当您尝试配置不兼容的网络模块时，管理防御中心的网络界面中将会出现错误消息或警告消息。如需帮助，请联系支持部门。

以下模块包含可配置旁路感应接口：

- 四端口 1000BASE-T 铜接口，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
- 一个双端口 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 2U 设备）

以下模块包含非旁路感应接口：

- 四端口 1000BASE-T 铜接口，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，堆叠模块将两个或更多配置相同的设备的资源结合起来。堆叠模块在 3D8140、3D8250 和 3D8350 上是可选的；3D8260、3D8270 和 3D8290 以及 3D8360、3D8370 和 3D8390 堆叠配置带有堆叠模块。

注意事项 这些模块**不**可热插拔。有关详细信息，请参阅插入和拆卸 8000 系列模块，第 C-1 页。

以下机箱正面图示出了包含感应接口的模块插槽的位置。

图 3-11 81xx 子系列机箱正面图

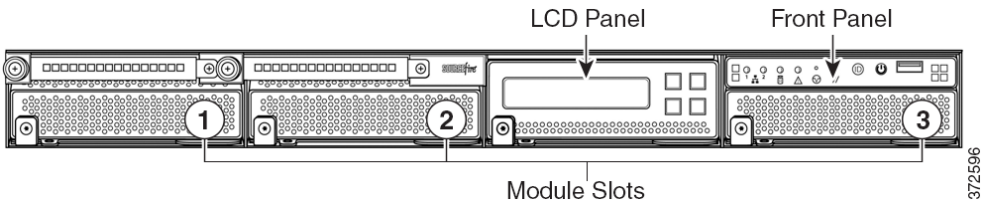
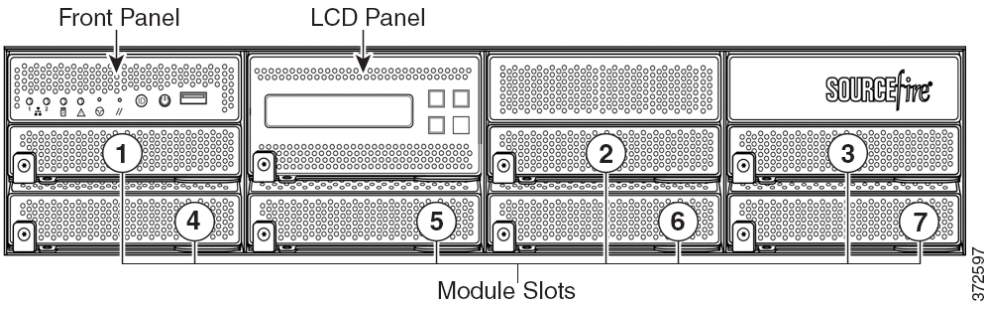


图 3-12 82xx 子系列和83xx 子系列机箱正面图



8000 系列模块

8000 系列可配备以下支持可配置旁路功能的模块：

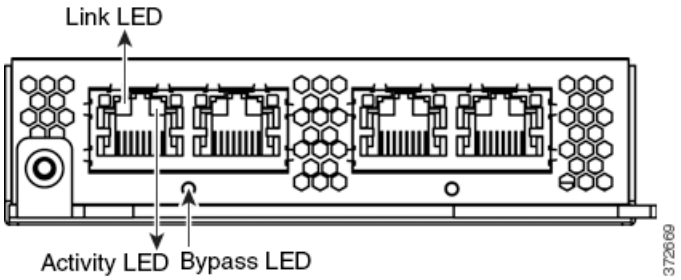
- 四端口 1000BASE-T 铜接口，支持可配置旁路功能。有关详细信息，请参阅图 3-13 四端口 1000BASE-T 铜可配置旁路网络模块，第 3-9 页。
- 四端口 1000BASE-SX 光纤接口，支持可配置旁路功能。有关详细信息，请参阅图 3-14 四端口 1000BASE-SX 光纤可配置旁路网络模块，第 3-9 页。
- 双端口 10GBASE（MMSR 或 SMLR）光纤接口，支持可配置旁路功能。有关详细信息，请参阅图 3-15 双端口 10GBASE （MMSR 或 SMLR）光纤接口，支持可配置旁路功能，第 3-10 页。
- 双端口 40GBASE-SR4 光纤接口，支持可配置旁路功能。有关详细信息，请参阅图 3-16 双端口 40GBASE-SR4 光纤可配置旁路网络模块，第 3-10 页。

8000 系列可配备以下不支持可配置旁路功能的模块：

- 四端口 1000BASE-T 铜接口，不支持旁路功能。有关详细信息，请参阅图 3-18 四端口 1000BASE-T 铜可配置旁路网络模块，第 3-11 页。
- 四端口 1000BASE-SX 光纤接口，不支持旁路功能。有关详细信息，请参阅图 3-19 四端口 1000BASE-SX 光纤非旁路网络模块，第 3-11 页。
- 四端口 10GBASE （MMSR 或 SMLR）光纤接口，不支持旁路功能。有关详细信息，请参阅图 3-20 四端口 10GBASE （MMSR 或 SMLR）光纤非旁路网络模块，第 3-12 页。

堆叠模块在 3D8140、 3D8250 和 3D8350 上是可选的；3D8260、 3D8270 和 3D8290 以及 3D8360、 3D8370 和 3D8390 堆叠配置带有堆叠模块。有关详细信息，请参阅 8000 系列堆叠模块，第 3-12 页。

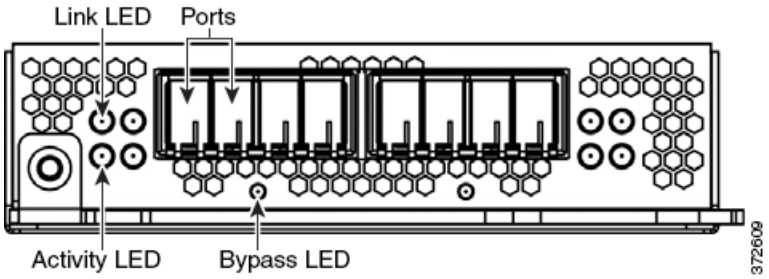
图 3-13 四端口 1000BASE-T 铜可配置旁路网络模块



使用这些接口最多可以对四个独立网段进行被动监控。您还可以内联方式使用成对接口或者在旁路模式下对成对接口进行内联，这样最多可在两个网络上将设备部署为入侵防御系统。

如果您想利用设备的自动旁路功能，必须将左侧或右侧的两个接口连接到网段。这样，即使在设备出现故障或断电的情况下也可以进行流量传输。您还必须使用网络界面将一对接口配置为内联集并对其启用旁路模式。

图 3-14 四端口 1000BASE-SX 光纤可配置旁路网络模块



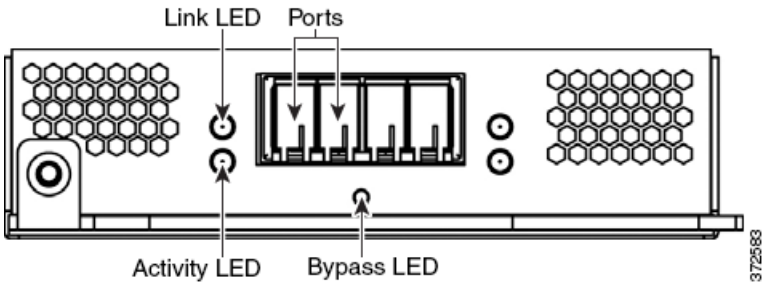
具有可配置旁路功能的四端口 1000BASE-SX 光纤配置使用 LC 型 （本地连接器）光纤收发器。

使用此配置最多可以对四个独立网段进行被动监控。您还可以内联方式使用成对接口或者在旁路模式下对成对接口进行内联，这样最多可在两个独立网络上将受管设备部署为入侵防御系统。

提示 为了获得最佳性能，请按照连续顺序使用接口组。如果您跳过任何接口，可能会导致性能下降。

如果您想利用设备的自动旁路功能，必须将左侧或右侧的两个接口连接到网段。这样，即使在设备出现故障或断电的情况下也可以进行流量传输。您还必须使用网络界面将一对接口配置为内联集并对其启用旁路模式。

图 3-15 双端口 10GBASE （MMSR 或 SMLR）光纤接口，支持可配置旁路功能



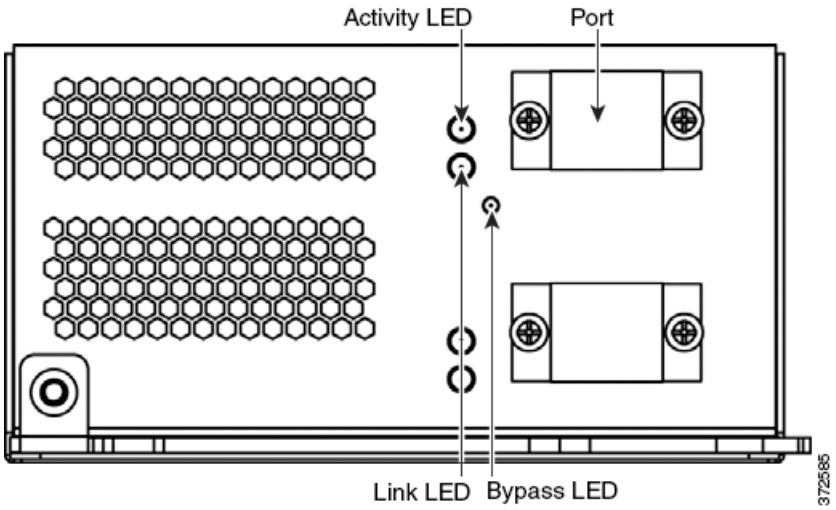
支持可配置旁路功能的双端口 10GBASE 光纤配置使用 LC 型 （本地连接器）光纤收发器。请注意，这些接口可以是 MMSR 或 SMLR 接口。

使用此配置最多可以对两个独立网段进行被动监控。您还可以内联方式使用成对接口或者在旁路模式下对成对接口进行内联，这样可在一个网络上将受管设备部署为入侵防御系统。

提示 为了获得最佳性能，请按照连续顺序使用接口组。如果您跳过任何接口，可能会导致性能下降。

如果您想利用设备的自动旁路功能，必须将两个接口连接到网段。这样，即使在设备出现故障或断电的情况下也可以进行流量传输。您还必须使用网络界面将一对接口配置为内联集并对其启用旁路模式。

图 3-16 双端口 40GBASE-SR4 光纤可配置旁路网络模块



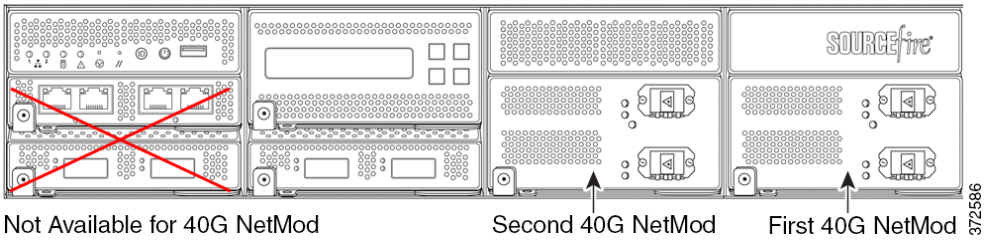
支持可配置旁路功能的双端口 40GBASE-SR4 光纤配置使用 MPO （多光纤推式）连接器光纤收发器。

40G 网络模块仅适用于 3D8270、 3D8290、 3D8360、 3D8370 和 3D8390 或者具有 40G 功能的 3D8250、 3D8260 和 3D8350。如果您尝试在不具有 40G 功能的设备上创建 40G 接口，管理防御中心的网络界面上的 40G 接口屏幕将会呈红色显示。支持 40G 功能的 3D8250 在 LCD 面板上显示“3D8250-40G”，支持 40G 功能的 3D8350 显示在 LCD 面板上显示“3D 8350-40G”。

使用此配置最多可以对两个独立网段进行被动监控。您还可以内联方式使用成对接口或者在旁路模式下对成对接口进行内联，这样最多可在一个网络上将设备部署为入侵防御系统。

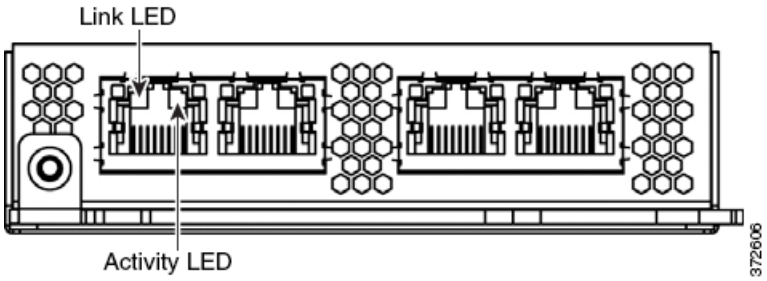
您最多可以使用两个 40G 网络模块。在插槽 3 和插槽 7 中安装第一个 40G 网络模块，在插槽 2 和插槽 6 中安装第二个 40G 网络模块。不能在插槽 1 和插槽 4 中使用 40G 网络模块。

图 3-17 40G 网络模块的放置



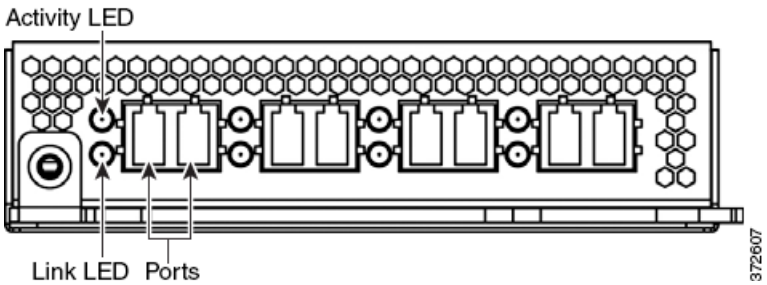
如果您想利用设备的自动旁路功能，必须使用网络界面将一对接口配置为内联集并对其启用旁路模式。

图 3-18 四端口 1000BASE-T 铜可配置旁路网络模块



使用这些接口最多可以对四个独立网段进行被动监控。您还可以在最多两个网段上使用具有内联配置的成对接口。

图 3-19 四端口 1000BASE-SX 光纤非旁路网络模块

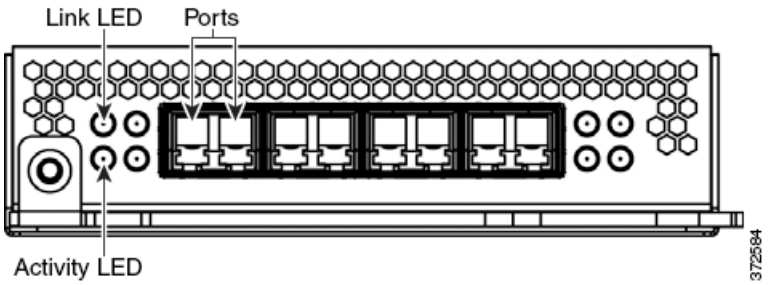


四端口 1000BASE-SX 光纤非旁路配置使用 LC 型 （本地连接器）光纤收发器。

使用这些接口最多可以对四个独立网段进行被动监控。您还可以在最多两个网段上使用具有内联配置的成对接口。

提示 为了获得最佳性能，请按照连续顺序使用接口组。如果您跳过任何接口，可能会导致性能下降。

图 3-20 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有 MMSR 或 SMLR 接口的 LC 型（本地连接器）光纤收发器。

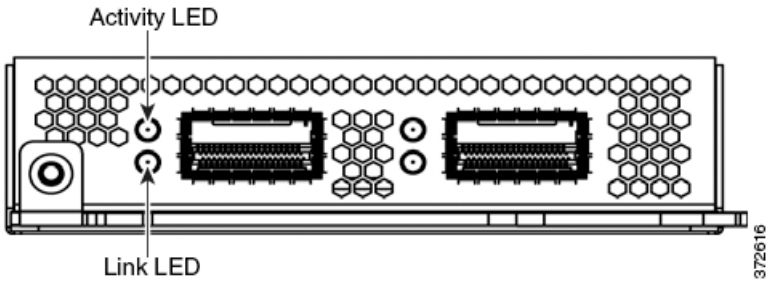
注意事项 四端口 10G BASE 非旁路网络模块包含不可拆卸的小型封装热插拔 (SFP) 收发器。尝试拆卸 SFP 可能会损坏模块。

使用这些接口最多可以对四个独立网段进行被动监控。您还可以在最多两个网段上使用具有内联配置的成对接口。

提示 为了获得最佳性能，请按照连续顺序使用接口组。如果您跳过任何接口，可能会导致性能下降。

8000 系列堆叠模块

堆叠模块将两个或更多配置相同的设备的资源结合起来。堆叠模块在 3D8140、 3D8250 和 3D8350 上是可选的；3D8260、 3D8270 和 3D8290 以及 3D8360、 3D8370 和 3D8390 堆叠配置带有堆叠模块。



堆叠模块使您可以将两个设备的资源结合起来，将其中一个设备用作主设备，另一个设备用作辅助设备。只有主设备带有感应接口。以下设备可以使用堆叠模块：

- 3D8140、 3D8250 和 3D8350 可选配堆叠模块。
- 3D8260 和 3D8360 在主设备中和辅助设备中各提供一个堆叠模块。
- 3D8270 和 3D8370 在主设备中提供两个堆叠模块，在两个辅助设备中各提供一个堆叠模块。
- 3D8290 和 3D8390 在主设备中提供三个堆叠模块，在三个辅助设备中各提供一个堆叠模块。

有关使用堆叠设备的详细信息，请参阅在堆叠配置中使用设备。

在堆叠配置中使用设备

通过将配置相同的设备的资源整合到堆叠配置中，可以增加在网段上检查的流量。一台设备被指定为主设备并连接到各网段。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。防御中心可以创建、编辑和管理堆叠配置。

主设备包含感应接口以及为连接到主设备的每个辅助设备提供的一组堆叠接口。您可以将主设备的感应接口连接到您想要监控的网段，方法与使用非堆叠设备时一样。主设备上的堆叠接口通过堆叠电缆连接到辅助设备上的堆叠接口。每台辅助设备均通过堆叠接口直接连接到主设备。不会使用辅助设备包含的感应接口。

您可以按照以下配置进行设备堆叠：

- 两个 3D8140
- 最多四个 3D8250
- 一个 3D8260 （一个具有 10G 能力的主设备和一个辅助设备）
- 一个 3D8270 （一个具有 40G 能力的主设备和两个辅助设备）
- 一个 3D8290 （一个具有 40G 能力的主设备和三个辅助设备）
- 最多四个 3D8350
- 一个 3D8360 （一个具有 40G 能力的主设备和一个辅助设备）
- 一个 3D8370 （一个具有 40G 能力的主设备和两个辅助设备）
- 一个 3D8390 （一个具有 40G 能力的主设备和三个辅助设备）

对于 3D8260、 3D8270、 3D8360 和 3D8370，您在堆叠配置中最多总共可堆叠四个额外设备。

一个设备被指定为主设备，并在防御中心的网络界面上显示为具有主角色。堆叠配置中的所有其他设备均为辅助设备，并在网络界面上显示为具有辅助角色。除了查看堆叠设备的信息，您都可以将组合资源作为单个实体使用。

将主设备连接到您想要分析的各个网段，就像连接单个 3D8140、 3D8250 或 3D8350 一样。如堆叠接线图所示，将辅助设备连接到主设备。

设备与网段以及设备与设备之间建立物理连接后，使用防御中心建立并管理堆叠。

以下部分提供有关如何连接和管理堆叠设备的详细信息：

- 连接 3D8140，第 3-13 页
- 连接 82xx 子系列和 83xx 子系列，第 3-14 页
- 使用 8000 系列堆叠电缆，第 3-16 页
- 管理堆叠设备，第 3-17 页

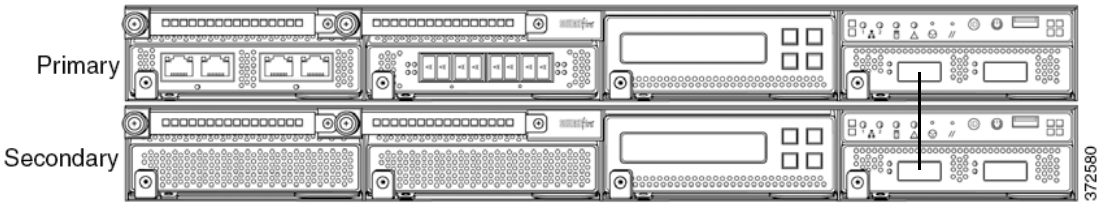
连接 3D8140

在堆叠配置中可以连接两个 3D8140。必须使用一根 8000 系列堆叠电缆在主设备和辅助设备之间建立物理连接。有关使用堆叠电缆的详细信息，请参阅使用 8000 系列堆叠电缆，第 3-16 页。

将设备安装在机架中，以方便您在堆叠模块之间连接电缆。可以将辅助设备安装在主设备的上方或下方。

将主设备连接到您想要分析的各个网段，就像连接单个 3D8140 一样。将辅助设备直接连接到主设备。

在下图中，辅助设备安装在主设备下方。



要连接 3D8140 辅助设备，请执行以下操作：

步骤 1 用一根 8000 系列堆叠电缆将主设备的左侧堆叠接口连接到辅助设备的左侧堆叠接口，然后使用管理这些设备的防御中心在系统中建立堆叠设备关系。请注意，右侧堆叠接口未连接。请参阅管理堆叠设备，第 3-17 页。

连接 82xx 子系列和 83xx 子系列

您可以连接以下任何配置：

- 最多四个 3D8250 或四个 3D8350
- 一个 3D8260 （一个具有 10G 能力的主设备和一个辅助设备）
- 一个 3D8360 （一个具有 40G 能力的主设备和一个辅助设备）
- 一个 3D8270 或 3D8370 （一个具有 40G 能力的主设备和两个辅助设备）
- 一个 3D8290 或 3D8390 （一个具有 40G 能力的主设备和三个辅助设备）

对于 3D8260、 3D8270、 3D8360 和 3D8370，您在堆叠配置中最多总共可堆叠四个额外设备。

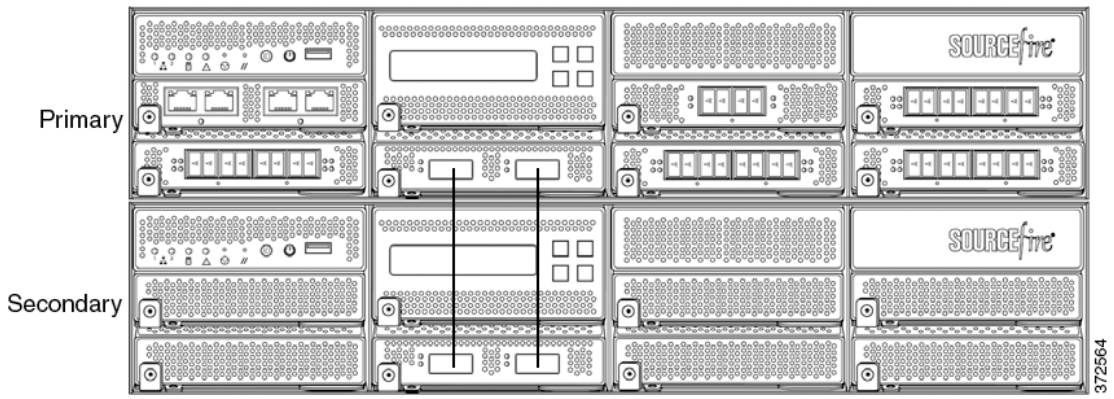
每个辅助设备与主设备之间的连接必须使用两根 8000 系列堆叠电缆。有关使用堆叠电缆的详细信息，请参阅使用 8000 系列堆叠电缆，第 3-16 页。

将设备安装在机架中，以方便您在堆叠模块之间连接电缆。可以将辅助设备安装在主设备的上方或下方。

将主设备连接到您想要分析的各个网段，就像连接单个 3D8250 或 3D8350 一样。将每个辅助设备直接连接到主设备，直至达到配置中所需的辅助设备数量。

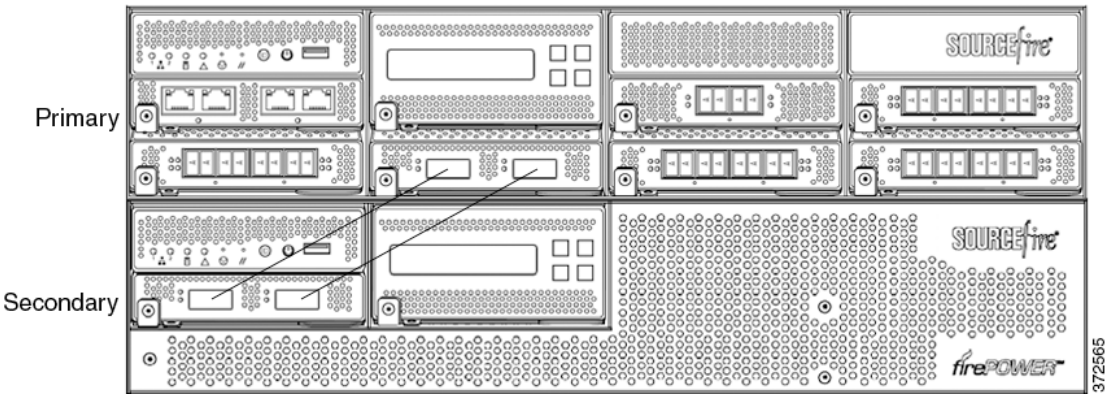
3D8250 或 3D8350 主设备和一个辅助设备

以下图例显示了 3D8250 或 3D8350 主设备和一个辅助设备。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。



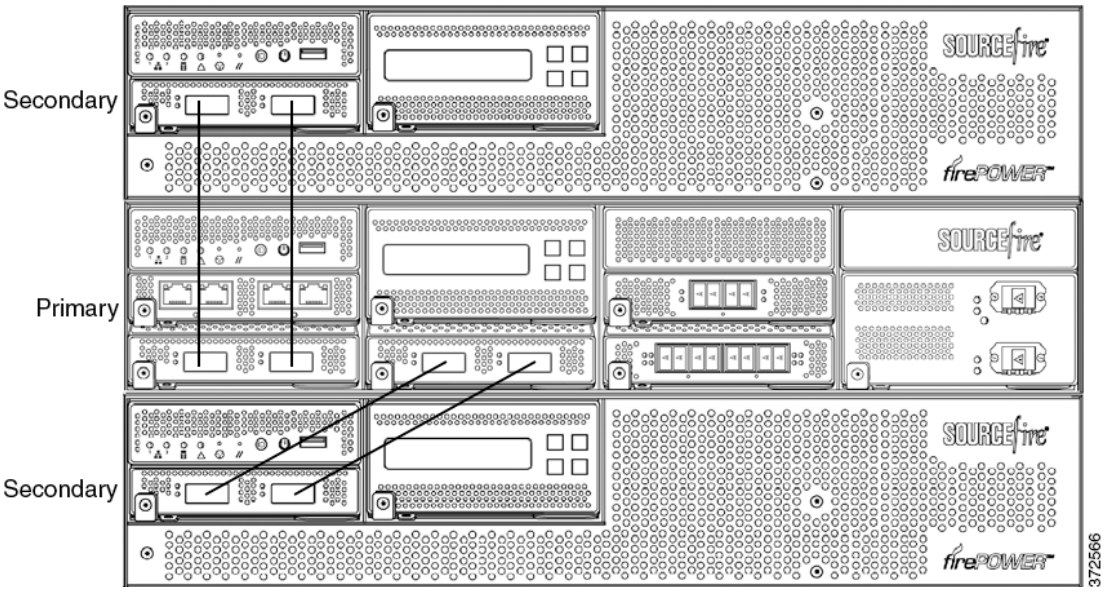
3D8260 或 3D8360 主设备和一个辅助设备

以下图例显示了 3D8260 或 3D8360 配置。3D8260 包括具有 10G 能力的 3D8250 主设备和一个专用辅助设备。 3D8360 包括具有 40G 能力的 3D8350 主设备和一个专用辅助设备。对于每个配置（3D8260 或 3D8360），辅助设备均安装在主设备下方。



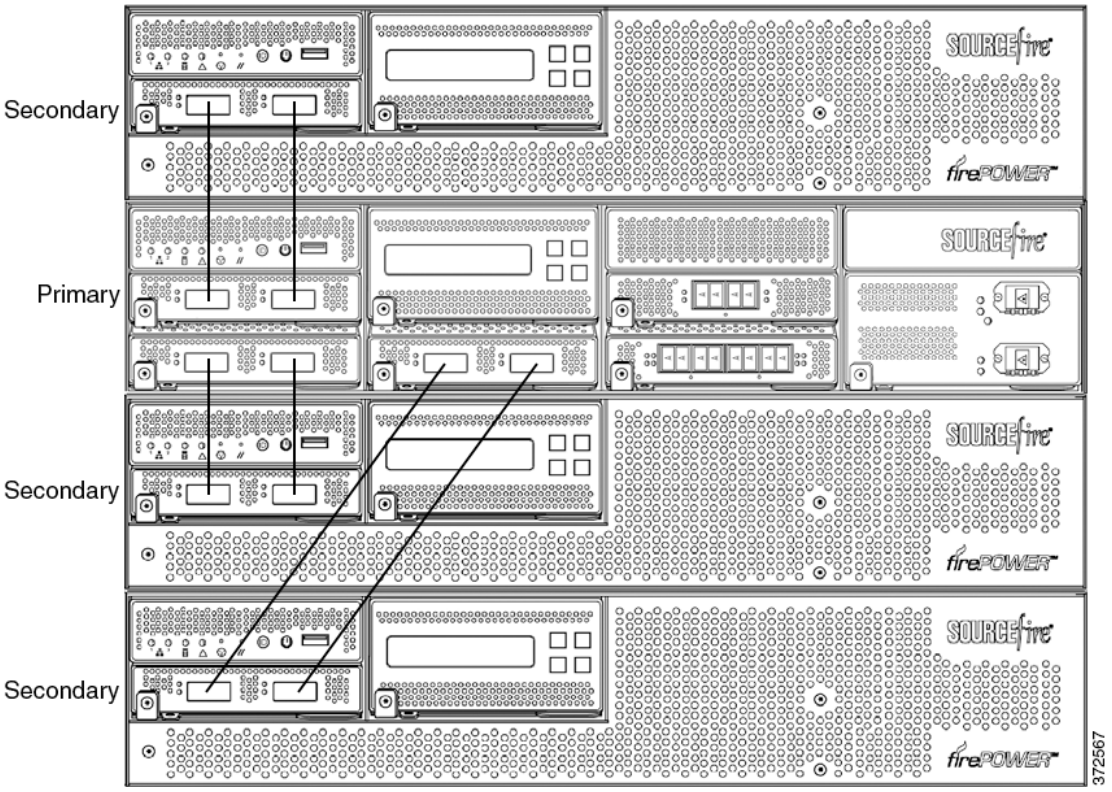
3D8270 或 3D8370 主设备 (40G) 和两个辅助设备

以下图例显示了 3D8270 或 3D8370 配置。3D8270 包括具有 40G 能力的 3D8250 主设备和两个专用辅助设备。 3D8370 包括具有 40G 能力的 3D8350 主设备和两个专用辅助设备。对于每个配置（3D8270 或 3D8370），一个辅助设备安装在主设备上方，另一个辅助设备安装在主设备下方。



3D8290 或 3D8390 主设备 (40G) 和三个辅助设备

以下图例显示了 3D8290 或 3D8390 配置。3D8290 包括具有 40G 能力的 3D8250 主设备和三个专用辅助设备。 3D8370 包括具有 40G 能力的 3D8350 主设备和两个专用辅助设备。对于每个配置（3D8290 或 3D8390），一个辅助设备安装在主设备上方，两个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：

步骤 1 用一根 8000 系列堆叠电缆将主设备的堆叠模块左侧接口连接到辅助设备的堆叠模块左侧接口。

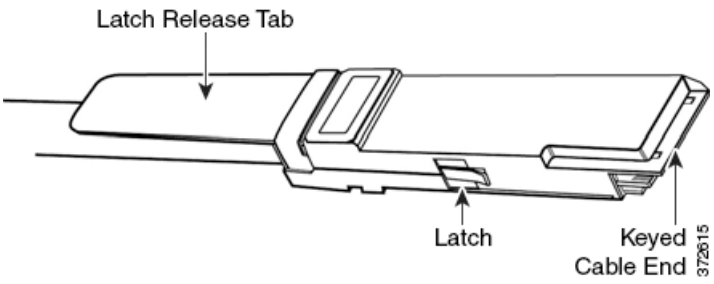
步骤 2 用另一根 8000 系列堆叠电缆将主设备的堆叠模块右侧接口连接到辅助设备的堆叠模块右侧接口。

步骤 3 对您想要连接的每个辅助设备重复步骤 1 和步骤 2。

步骤 4 使用管理这些设备的防御中心建立堆叠设备关系并管理其联合资源。请参阅管理堆叠设备，第 3-17 页。

使用 8000 系列堆叠电缆

8000 系列堆叠电缆有相同的锁定端，每个锁定端都带有闩锁 （用于将电缆固定在设备中）和解锁片。



对于每个配置，根据需要使用 8000 系列堆叠电缆在主设备和每个辅助设备之间建立物理连接：

- 对于 3D8250、 3D8260、 3D8270 和 3D8290，每个连接需要两根电缆
- 对于 3D8350、 3D8360、 3D8370 和 3D8390，每个连接需要两根电缆
- 3D8140 需要一根电缆

插入或拔出堆叠电缆时不需要关闭设备。

注意事项 连接设备时，请务必使用思科 8000 系列堆叠电缆。使用不受支持的电缆可能会导致无法预料的错误。

在设备之间建立物理连接后，使用防御中心管理堆叠设备。

要插入 8000 系列堆叠电缆，请执行以下操作：

步骤 1 要插入电缆，拿住电缆末端同时使解锁片正面朝上，将锁定端插入堆叠模块上的端口中，直至听到闩锁卡入到位。

要拔出 8000 系列堆叠电缆，请执行以下操作：

步骤 1 要拔出电缆，拉动解锁片以松开闩锁，然后拔出电缆末端。

管理堆叠设备

防御中心在设备之间建立堆叠关系，控制主设备的接口组，并管理堆叠配置中的组合资源。您不能在堆叠设备的本地网络界面上管理接口组。

堆叠关系建立后，每个设备都会使用单个共享的检测配置独立检查流量。如果主设备出现故障，将会根据主设备的配置来处理流量 （也就是说，就像堆叠关系不存在一样）。如果辅助设备出现故障，主设备会继续检测流量，生成警报，并将流量发送到流量中断的故障辅助设备上。

有关建立和管理堆叠设备的信息，请参阅 《*FireSIGHT 系统用户指南*》中的“管理堆叠设备”章节。

在机架中安装设备

FireSIGHT 系统可在不同的硬件平台上提供。所有 FireSIGHT 系统设备都可以安装在机架中 （对于 3D7010、3D7020 和 3D7030 ，需要购买 1U 安装套件）。安装设备时，您还必须确保您可以访问设备的控制台。要访问控制台以进行初始设置，请通过以下任意一种方式连接到 FireSIGHT 系统设备：

键盘和显示器/KVM

可以将 USB 键盘和 VGA 显示器连接到任何 FireSIGHT 系统设备；此方法对于连接到键盘、显示器和鼠标 (KVM) 切换器的机架式设备很有用。

注意事项 进行初始设置时，**切勿**使用带有 USB 大容量存储的 KVM 控制台来访问设备，因为设备可能会尝试将大容量存储设备用作启动设备。

与管理接口建立以太网连接

按照以下网络设置配置一台不连接到互联网的本地计算机：

- IP 地址：192.168.45.2
- 网络掩码：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的网络接口连接到设备的管理接口。要与设备交互，请使用 HyperTerminal 或 Xmodem 等终端仿真软件。终端仿真软件应具有如下设置：

- 9600 波特率
- 8 个数据位
- 无奇偶校验
- 1 个停止位
- 无流量控制。

请注意，物理 FireSIGHT 系统设备上的管理接口预配置为使用默认 IPv4 地址。但是，您可以在设置过程中将管理接口重新配置为使用 IPv6 地址。

完成初始设置后，您还可以通过以下方式访问控制台：

串行连接/笔记本电脑

可以使用物理串行端口将计算机连接到除 3D2100/2500/3500/4500 设备外的任何 FireSIGHT 系统设备。您可以随时连接适当的串行反转线 （又称为零调制解调器电缆或思科控制台电缆），然后配置远程管理控制台以将默认 VGA 输出重定向到串行端口。要与设备进行交互，请使用终端仿真软件 （如上所述）。

串行端口可能带有 RJ-45 接口或 DB-9 接口，具体取决于设备。请参阅下表，了解各个设备适用的连接器。

表 3-1 按型号列出的串行连接器

设备	连接器
3D500/1000/2000	DB-9 （凹式）
3D6500	RJ-45
3 系列防御中心	RJ-45
3D70xx 子系列	RJ-45
3D71xx 子系列	DB-9 （凹式）
3D8000 系列	RJ-45
3D9900	RJ-45

将适当的反转线连接到设备后，如重定向控制台输出，第 3-19 页中所述重定向控制台输出。要确定每个设备的串行端口的位置，请使用硬件规格，第 6-1 页中的图。

使用局域网承载串行进行无人值守管理

LOM 功能使您可以借助 SOL 连接在3 系列 设备上执行一组有限操作。如果您需要将具有 LOM 功能的设备恢复为出厂默认设置，但您没有对该设备的物理访问权限，则可以使用 LOM 执行恢复过程。使用 LOM 连接到设备后，您就可以像使用物理串行连接时一样向恢复实用程序发出命令。有关详细信息，请参阅设置无人值守管理，第 7-16 页。

要使用 LOM 将设备恢复为出厂设置，请**勿**删除网络设置。删除网络设置将会使 LOM 连接断开。有关详细信息，请参阅还原 FireSIGHT 系统设备为出厂默认设置，第 7-1 页。

要安装设备，请执行以下操作：

步骤 1 使用安装套件及随附的说明将设备安装到机架中。

步骤 2 使用键盘和显示器或以太网连接连接到设备。

步骤 3 如果是使用键盘和显示器来设置设备，请立即使用以太网电缆将管理接口连接到受保护的网段。

如果您打算通过将计算机直接连接到设备的物理管理接口来执行初始设置过程，应在完成设置时将管理接口连接到受保护的网络。

步骤 4 对于受管设备，使用适用于接口的电缆将感应接口连接到您想要分析的网段：

- 铜缆感应接口：如果您的设备包含铜缆感应接口，请务必使用适当的电缆将这些接口连接到网络；请参阅铜接口上的内联部署布线，第 2-6 页。
- 光纤适配器卡：对于带有光纤适配器卡的设备，将可选多模光纤电缆上的 LC 连接器以任何顺序连接到适配器上的两个端口。将 SC 插头连接到要分析的网段。
- 光纤分路器：如果要部署的设备带有可选的光纤分路器，请将可选多模光纤电缆上的 SC 插头连接到分路器上的“分析器”端口。将分路器连接到要分析的网段。
- 铜缆分路器：如果要部署的设备带有可选的铜缆分路器，请将分路器左侧的端口 A 和端口 B 连接到要分析的网段。将分路器右侧的端口 A 和端口 B （“分析器”端口）连接到适配器卡上的两个铜缆端口。

有关受管设备部署方案的详细信息，请参阅了解部署，第 2-1 页。

请注意，如果要部署的设备带有旁路接口，那么，即使设备出现故障，您仍可以利用设备的功能来保持网络连接。有关安装和延迟测试的信息，请参阅测试内联旁路接口的安装，第 3-20 页。

步骤 5 将电源线连接到设备并接通电源。

如果设备带有冗余电源，可以将电源线连接到主电源和冗余电源，再分别给它们接通电源。

步骤 6 打开设备。

如果您是通过直接以太网连接来设置设备，请确保本地计算机的网络接口以及设备的管理接口的链路 LED 都亮起。如果这两个 LED 不亮，请尝试使用交叉电缆。有关详细信息，请参阅铜接口上的内联部署布线，第 2-6 页。

步骤 7 继续下一章，安装 FireSIGHT 系统设备，第 3-1 页。

重定向控制台输出

默认情况下，FireSIGHT 系统设备会将初始化状态（即 *init*）消息定向到 VGA 端口。如果您将设备恢复为出厂默认设置并删除其许可证和网络设置，恢复实用程序也会将控制台输出重置到 VGA 端口。如果您要使用物理串行端口或 SOL 来访问控制台，思科建议您在完成初始设置后将控制台输出重定向到串行端口。

要使用外壳重定向控制台输出，可以从设备的外壳运行脚本。下表列出了您应使用的控制台设置，具体取决于您打算通过何种方式访问设备。

表 3-2 控制台重定向选项

选项	设置
VGA （默认值）	`tty0`
物理串行	`ttyS0`
通过 SOL 实现的 LOM	`ttyS0`

请注意，所有 3 系列设备都支持 LOM，但 7000 系列设备不同时支持 LOM 和物理串行接入。但是，无论您要使用哪种方式，控制台设置都是相同的。

要使用外壳重定向控制台输出，请执行以下操作：

访问：管理员

步骤 1 使用具有管理员权限的帐户通过键盘/显示器或串行连接登录到设备的外壳。密码与设备的网络界面的密码相同。

请注意，在 3 系列或虚拟受管设备上，必须键入 `expert` 以显示外壳提示符。

系统将显示设备提示。

步骤 2 在提示符后输入以下内容，能够以 root 用户身份设置控制台输出：

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

其中，*`console_value`* 是代表着您打算用于访问设备的方式的设置，如第 3-20 页上的表 3-2 中所述。

步骤 3 要使更改生效，请输入 `sudo reboot` 以重新启动设备。

设备重新启动。

测试内联旁路接口的安装

带有旁路接口的受管设备在设备断电或无法工作的情况下也能够保持网络连接。必须正确安装这些设备，以及量化这些设备的安装造成的任何延迟。

注 交换机的生成树发现协议可能会导致 30 秒的流量延迟。思科建议您在以下过程中禁用生成树。

以下过程 （仅适用于铜接口）介绍如何测试内联旁路接口的安装和 ping 延迟。您需要连接到网络以执行 ping 测试，以及连接到受管设备控制台。

要测试具有内联旁路接口的设备的安装情况，请执行以下操作：

访问：管理员

步骤 1 确保已针对内联旁路模式配置了设备的接口组类型。

有关为内联旁路模式配置接口组的说明，请参阅 《*FireSIGHT 系统用户指南*》中的“配置内联集”。

步骤 2 将交换机的所有接口、防火墙和设备感应接口设置为自动协商。

注 在设备上使用自动 MDIX 时，思科设备需要自动协商功能。

步骤 3 关闭设备并断开所有网络电缆。

重新连接设备并确保网络连接正确。查阅布线说明，以了解如何用交叉电缆或直通电缆将设备连接到交换机和防火墙；请参阅铜接口上的内联部署布线，第 2-6 页。

步骤 4 关闭设备后，确保可以通过设备实现防火墙与交换机之间的 ping 连接。

如果 ping 失败，请检查网络连接是否正确。

步骤 5 请连续执行 ping 操作，直至完成步骤 10。

步骤 6 重新启动设备。

步骤 7 使用具有管理员权限的帐户通过键盘/显示器或串行连接登录到设备。密码与设备的网络界面的密码相同。

系统将显示设备提示。

步骤 8 输入 `system shutdown` 以关闭设备。

也可以使用设备的网络界面来关闭设备；请参阅 《*FireSIGHT 系统用户指南*》的“管理设备”章节。大多数设备关闭时都会发出可听到的咔嗒声。这表示中继正在切换以及设备正在进入硬件旁路。

步骤 9 等待 30 秒。

确保 ping 流量已恢复。

步骤 10 重新启动设备，确保继续有 ping 流量通过。

步骤 11 对于支持侧录模式的设备，您可以在以下情况下测试并记录 ping 延迟结果：

- 设备已关闭
- 设备已启动，应用了没有规则的策略，内联入侵策略保护模式
- 设备已启动，应用了没有规则的策略，内联入侵策略保护侧录模式
- 设备已启动，应用了带有经过调整的规则的策略，内联入侵策略保护模式

确保延迟时间对于您的安装来说是可接受的。有关解决过度延迟问题的信息，请参阅《*FireSIGHT 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”章节。

设置 FireSIGHT 系统设备

部署并安装设备后，您必须完成设置流程，以使新设备能够在受信任的管理网络上进行通信。还必须更改管理员密码并接受最终用户许可协议 (EULA)。

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

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

注 有关设置 ASA FirePOWER 设备的详细信息，请参阅 ASA 文档。

有关初始设置流程每个步骤的详细信息，请参阅以下各节：

- 了解设置流程，第 4-2 页对设置流程进行了概述，该流程主要取决于设备的型号以及您是否可以对设备进行物理访问。

注 如果您尚不熟悉设置流程，思科**强烈**建议您先阅读本章节。

- 使用脚本配置网络设置，第 4-4 页说明了如何使用脚本来指定网络设置，以使新设备能够在您的管理网络上进行通信。您当前通过键盘和显示器访问的所有防御中心都需要执行该步骤。
- 使用 CLI 在 3 系列设备上进行初始设置，第 4-5 页说明了如何使用交互命令行界面 (CLI) 在3 系列 设备上执行设置流程。
- 初始设置页面：设备，第 4-7 页说明了如何使用各种设备的网络界面来完成其初始设置。
- 初始设置页面：防御中心，第 4-10 页说明了如何使用防御中心的网络界面来完成其初始设置。
- 后续步骤，第 4-14 页包含了设置 FireSIGHT 系统部署时可能执行的设置后任务的相关指南。

注意事项 本章的这些步骤说明了如何在不停止设备的情况下对设备进行设置。但是，如果需要停止设备，请使用《*FireSIGHT 系统用户指南*》中“管理设备”章节中的操作步骤、3 系列设备上 CLI 中的 `system shutdown` 命令或设备外壳中的 `shutdown -h now` 命令 （有时称为专家模式）。

了解设置流程

按本指南前些章所述部署并安装新的 FireSIGHT 系统设备之后，必须完成设置流程。开始设置之前，请确保符合以下条件。

设备型号

您必须知道设置的是什么设备。 FireSIGHT 系统*设备*可以是一台流量感应受管*设备*，也可以是一台管理*防御中心*：每种设备类型都有多个*型号*；这些型号又进一步划分为多个*产品*和*系列*。有关详细信息，请参阅 FireSIGHT 系统设备，第 1-1 页。

接入

要设置新设备，必须通过键盘和显示器/KVM （键盘、视频和鼠标）或通过直接以太网连接访问设备的管理接口。初始设置完成后，可配置串行存取的设备。有关详细信息，请参阅在机架中安装设备，第 3-17 页。

注 请**勿**使用带 USB 大容量存储的 KVM 控制台访问待初始设置的设备，因为该设备可能会尝试将大容量存储设备用作启动设备。

信息

已获得设备管理网络上通信所需的信息 （最低要求）：IPv4 或 IPv6 管理 IP 地址、网络掩码或前缀长度和默认网关。

如果知道设备如何部署，您可以利用设置流程执行多个初始管理级别的任务，包括注册和许可。

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

完成设置后，可使用防御中心的网络界面来执行部署相关的管理和分析任务。受管物理设备的网络界面受限，只能用于执行基本的管理任务。有关详细信息，请参阅后续步骤，第 4-14 页。

关于如何设置每类设备的详细信息，请参阅：

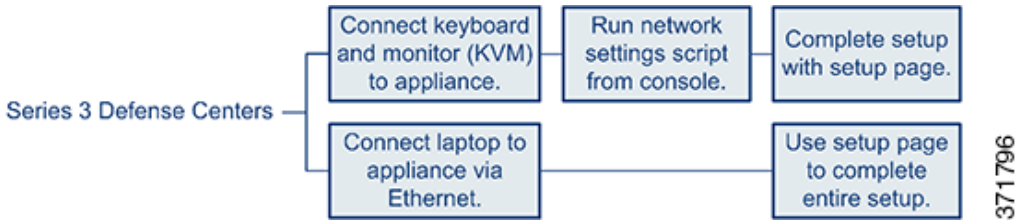
- 设置 3 系列防御中心，第 4-3 页
- 设置 3 系列设备，第 4-3 页

提示 如果在设置设备前已恢复出厂默认设置 （请参阅还原 FireSIGHT 系统设备为出厂默认设置，第 7-1 页），且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，然后执行设置。跳转至初始设置页面：设备，第 4-7 页或初始设置页面：防御中心，第 4-10 页。

设置 3 系列防御中心

支持的防御中心：3 系列

下图展示了设置 3 系列防御中心时可做的选择：



要设置，3 系列防御中心，请执行以下操作：

访问：管理员

步骤 1 如果使用键盘和显示器访问设备，可运行一个有助于配置设置的脚本，使设备能够在管理网络上通信；请参阅使用脚本配置网络设置，第 4-4 页。

如果您正在设置一个已重新映像的设备，并已在恢复过程中保存了网络设置，或者，如果通过直接以太网连接访问设备，可跳至下一步。

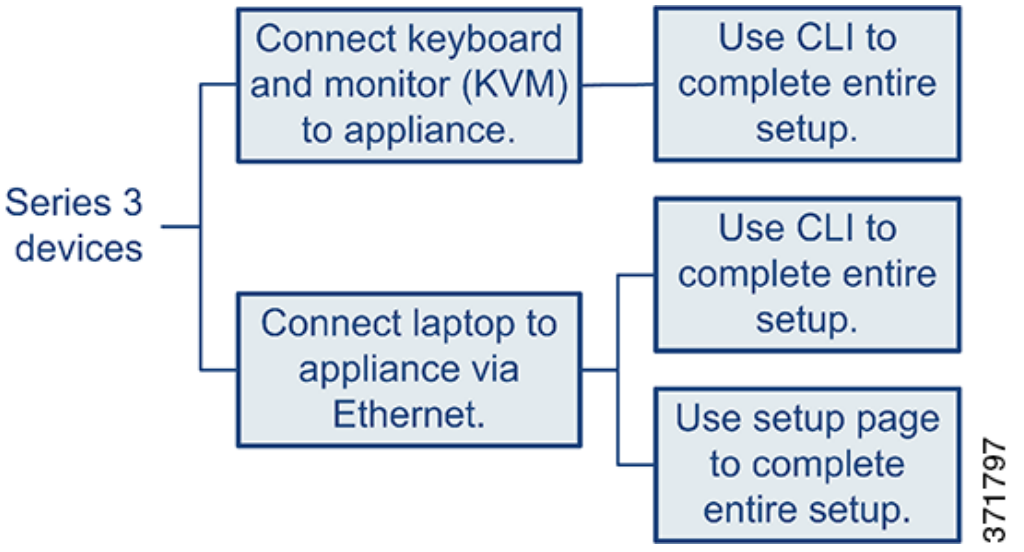
步骤 2 从管理网络上的计算机浏览至设备的网络界面，以完成设置流程：

- 要使用受管设备的网络界面完成其设置，请参阅初始设置页面：设备，第 4-7 页。
- 要使用防御中心的网络界面完成其设置，请参阅初始设置页面：防御中心，第 4-10 页。

设置 3 系列设备

支持的设备：3 系列

下图展示了在设置 3 系列设备时可做的选择：



对 3 系列设备的访问方式决定了如何对其进行设置。您有以下选择：

- 无论如何连接至设备，都可以使用 CLI 进行设置；请参阅使用 CLI 在 3 系列设备上进行初始设置，第 4-5 页。
- 如果通过直接以太网连接访问设备，可以从本地计算机浏览至设备的网络界面；请参阅初始设置页面：设备，第 4-7 页

如果您正在设置一个已重新映像的设备，并已在恢复过程中保存了网络设置，可通过 SSH 或无人值守管理 (LOM) 连接来访问 CLI。也可从管理网络上的计算机浏览至设备的网络界面。

使用脚本配置网络设置

支持的设备：2 系列

安装新的防御中心或 2 系列 设备后，或在重新映像中删除网络设置后，您必须配置设备，使设备能在管理网络上进行通信。通过在控制台运行脚本完成该步骤。

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

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

请注意，脚本将提示设置信息，这些信息与设备的设置页面提示的信息大致相同。有关详细信息，请参阅网络设置，第 4-8 页 （设备）和网络设置，第 4-11 页 （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

步骤 1 在控制台上登录设备。使用 `admin` 作为用户名，**思科**作为密码。

请注意，在 3 系列或虚拟受管设备上，必须键入 `expert` 以显示外壳提示符。

步骤 2 在管理员提示符下，运行以下脚本：

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

步骤 3 遵循脚本的提示。

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

- 输入 IPv4 地址，包括网络掩码，采用点分十进制格式。例如，可以指定 255.255.0.0 作为网络掩码。
- 以冒号隔开的十六进制格式输入 IPv6 地址。对于 IPv6 前缀，请指定位数；例如，前缀长度为 112。

步骤 4 确认设置正确。

如果输入的设置错误，您可以根据提示键入 `n`，然后按 Enter 键。然后，输入正确的信息。设置被执行后，控制台将显示消息。

步骤 5 从设备注销。

步骤 6 按照设备选择下一步：

- 要使用受管设备的网络界面完成其设置，请继续执行初始设置页面：设备，第 4-7 页。
- 要使用网络界面完成防御中心设置，请继续执行初始设置页面：防御中心，第 4-10 页。

使用 CLI 在 3 系列设备上进行初始设置

支持的设备：3 系列

或者，可以使用 CLI 而非设备的网络界面来配置 3 系列设备。首次使用 CLI 登录新配置的设备时，您必须阅读并接受 EULA。然后，按照设置提示更改管理员密码，配置设备的网络设置和检测模式。最后，将设备注册至管理此设备的防御中心。

设置提示符后，选项在圆括号中列出，如 `(y/n)`。默认值会列在方括号内，例如 `[y]`。按 Enter 键确认选择。

请注意， CLI 将提示设置信息，这些信息与设备的设置页面提示的信息大致相同。有关这些选项的详细信息，请参阅初始设置页面：设备，第 4-7 页。

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

步骤 1 登录设备。使用 `admin` 作为用户名，**思科**作为密码。

- 如果 3 系列设备连接到显示器和键盘，则从控制台登录设备。
- 如果已通过以太网线将计算机连接至 3 系列设备的管理接口，SSH 连接至接口的默认 IPv4 地址：192.168.45.45。

  设备立即提示您阅读 EULA。

步骤 2 阅读并接受 EULA。

步骤 3 更改管理员帐户的密码。该帐户拥有管理员权限，您无法将其删除。

管理员用户可利用该密码登录设备的网络界面及其 CLI；管理员用户有权访问配置 CLI。若更改了某设备网络界面的用户密码，相应 CLI 的密码也会相应更改，反之亦然。

思科建议使用安全性高的密码，至少含 8 个大小写混合的字母数字字符，其中至少有 1 位数字字符。避免使用词典中的单词。有关详细信息，请参阅更改密码，第 4-8 页。

步骤 4 配置设备的网络设置。

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

- 输入 IPv4 地址，包括网络掩码，采用点分十进制格式。例如，可以指定 255.255.0.0 作为网络掩码。
- 以冒号隔开的十六进制格式输入 IPv6 地址。对于 IPv6 前缀，请指定位数；例如，前缀长度为 112。

有关详细信息，请参阅网络设置，第 4-8 页。设置被执行后，控制台将显示消息。

步骤 5 选择是否允许通过 LCD 面板更改设备的网络设置。

注意事项 启用该选项会引起安全风险。您只需物理访问，无需身份验证，就可以使用 LCD 面板配置网络设置。有关详细信息，请参阅使用 3 系列设备上的 LCD 面板，第 5-1 页。

步骤 6 根据设备的部署方式指定检测模式。

有关详细信息，请参阅检测模式，第 4-9 页。设置被执行后，控制台将显示消息。完成后，设备将提醒您将该设备注册至防御中心，并显示 CLI 提示。

步骤 7 要使用 CLI 将设备注册至管理设备的防御中心，请继续下一节，使用 CLI 将 3 系列设备注册至防御中心。

您必须通过防御中心管理设备。如果您目前未注册设备，必须稍后登录，在注册后，才可将其添加至防御中心。

步骤 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

如果已使用 CLI 配置了 3 系列设备，思科建议在设置脚本结束时使用 CLI 将设备注册至防御中心。因为在初始设置过程中已登录设备的 CLI，所以在此过程中向防御中心注册设备最容易。

要注册设备，请使用 `configure manager add` 命令。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，最长达 37 个字符，并且不同于许可证密钥。

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

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

但是，如果设备和防御中心由一台 NAT 设备分隔，请与注册密钥一起输入一个唯一的 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：配置 CLI

步骤 1 以 Configuration CLI 访问级别的用户身份登录设备：

- 如果您正在从控制台执行初始设置，说明您已经以管理员用户身份登录，该身份拥有所需的访问级别。
- 否则，请通过 SSH 访问设备的管理 IP 地址或主机名。

步骤 2 在提示符中，使用 `configure manager add` 命令将设备注册至防御中心，命令的语法如下：

```
configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE} reg_key
[nat_id]
```

其中：

- `{hostname|IPv4_address| IPv6_address|DONTRESOLVE}` 指定防御中心的完全限定主机名或 IP 地址。如果防御中心不可直接寻址，则使用 `DONTRESOLVE`。
- *reg_key* 是一个唯一的字母数字注册密钥，最长达 37 个字符，您在将备注册至防御中心时需要此密钥。
- *nat_id* 是在防御中心与设备之间的注册过程中使用的可选的字母数字字符串。如果主机名设置为 `DONTRESOLVE`，则此项为必填项。

步骤 3 从设备注销。

此时，设备已准备好被添加至防御中心。

初始设置页面：设备

适用于所有受管设备（除使用 CLI 配置的 3 系列设备之外；请参阅使用 CLI 在 3 系列设备上进行初始设置，第 4-5 页），您必须通过登录设备的网络界面并在设置页面指定初始配置选项，来完成设置流程。

必须更改管理员密码，指定网络设置 （若尚无指定），并接受 EULA。您还可以将设备预注册至防御中心并指定一个检测模式；检测模式和在注册期间选择的其他选项决定了系统创建的默认接口、内联集、区域以及系统初始应用于受管设备的策略。

要使用物理受管设备的网络界面在其上完成初始设置，请执行以下操作：

访问：管理员

步骤 1 将您的浏览器转向 `https:// mgmt_ip/`，其中， *mgmt_ip* 是设备管理接口的 IP 地址。

- 对于通过以太网线连接至计算机的设备，请将该计算机的浏览器转向默认管理接口的 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至设备管理接口的 IP 地址。

系统将显示登录页面。

步骤 2 使用 `admin` 作为用户名、 `Sourcefire` 作为密码登录。

系统将显示设置页面。有关完成设置的详细信息，请参阅以下各节：

- 更改密码，第 4-8 页
- 网络设置，第 4-8 页
- 3 系列设备 LCD 面板配置，第 4-8 页
- 远程管理，第 4-8 页
- 时间设置，第 4-8 页
- 检测模式，第 4-9 页
- 自动备份，第 4-10 页
- 最终用户许可协议，第 4-10 页

步骤 3 完成设置后，点击 **Apply**。

设备已按您的选择配置好了。在系统显示中间页面后，您已经以管理员用户 （具有管理员角色）身份登录网络界面。

步骤 4 从设备注销。

设备已准备好被添加至防御中心。

注 如果已使用以太网线直接连接至设备，请断开计算机并将设备的管理接口连接至管理网络。如果需要随时访问设备的网络界面，您可以将管理网络上的计算机的浏览器转向设置过程中配置的 IP 地址或主机名。

更改密码

您必须更改管理员帐户的密码。该帐户拥有管理员权限，您无法将其删除。

管理员用户可利用该密码登录设备的网络界面及其 CLI；管理员用户有权访问配置 CLI。若更改了某设备网络界面的用户密码，相应 CLI 的密码也会相应更改，反之亦然。

思科建议使用包含至少 8 个大小写混合的字母数字字符和至少一个数字字符的强密码。避免使用词典中的单词。

网络设置

可通过网络设置，允许设备在管理网络上进行通信。如果已配置设备的网络设置，此页面中的本章节可预填充。

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

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

还可以指定多达三个 DNS 服务器，以及设备主机名和域。

3 系列设备 LCD 面板配置

支持的设备：3 系列

如果要配置 3 系列设备，请选择是否允许使用 LCD 面板更改设备的网络设置。

注意事项 启用该选项会引起安全风险。您只需物理访问，无需身份验证，就可以使用 LCD 面板配置网络设置。有关详细信息，请参阅使用 3 系列设备上的 LCD 面板，第 5-1 页。

远程管理

您必须通过防御中心管理思科设备。此流程包含两个步骤。首先配置设备的远程管理，然后添加设备至防御中心。为了方便操作，您可以通过设置页面将设备预注册至管理此设备的防御中心。

使 **Register This Device Now** 复选框保持启用状态，然后将管理防御中心的 IP 地址或完全限定域名指定为**管理主机**。此外，键入字母数字格式的**注册密钥**，稍后将设备注册至防御中心时需要此密钥。请注意，这是一个指定的简单密钥，最长达 37 个字符，并且不同于许可证密钥

注 如果设备和防御中心由一台网络地址转换 (NAT) 设备隔开，则将设备注册延迟至完成初始设置后。有关详细信息，请参阅 《*FireSIGHT 系统用户指南*》中的“管理设备”章节。

时间设置

您可以手动或通过 NTP 服务器 （包括防御中心）的网络时间协议 (NTP) 设置设备的时间。思科建议您使用防御中心作为其受管设备的 NTP 服务器。

您还可以为管理员帐户指定本地网络界面上使用的时区。点击当前时区，然后通过弹出窗口进行更改。

检测模式

您为设备选择的检测模式决定了系统对设备接口的初始配置方式，及这些接口是否属于内联集或安全区。

设置之后则不可更改检测模式；检测模式仅为一个在设置期间选择的选项，用于帮助系统定制设备的初始配置。一般来说，您应该根据设备的部署方式来选择检测模式：

被动

如果设备以被动方式被部署为一个入侵检测系统 (IDS)，则选择该模式。在被动部署中，您可以进行文件和恶意软件检测、安全情报监控，以及网络发现。

内联

如果设备以内联方式被部署为一个入侵防御系统，则选择该模式。入侵防御系统通常不允许*打开*，并且会*允许*不匹配的流量。

在内联部署中，您可以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。

虽然可以为所有设备选择内联模式，但请记住，使用以下接口的内联集不支持旁路功能：

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

注 重新映像会将内联部署中的设备重置为非旁路配置；这将中断网络上的流量，直到您重新配置了旁路模式。有关详细信息，请参阅还原流程中的流量，第 7-2 页。

访问控制

如果设备以内联方式部署为访问控制部署的一部分，即如果想要执行应用、用户和 URL 控制，则选择该模式。配置为执行访问控制的设备通常会不允许*关闭*，并且会*阻止*不匹配的流量。规则明确指定了可以通过的流量。

如果您希望利用设备特定的基于硬件的功能，包括 （依型号而定）：集群、严格的 TCP 执行、快速路径规则、交换、路由、 DHCP、 NAT 和 VPN，则应该选择该模式。

在访问控制部署中，您也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

如果设备被动方式部署为仅用于执行主机、应用和用户发现，则选择该模式。

下表列出了系统根据所选择的检测模式创建的接口、内联集和区域。

表 4-1 基于检测模式的初始配置

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

表 4-1 基于检测模式的初始配置 （续）

检测模式	安全区域	内联集	接口
访问控制	无	无	无
网络发现	被动	无	分配至被动区域的第一对接口

请注意，安全区域为防御中心级别的配置，系统在您将设备注册至防御中心后才会创建安全区域。注册完成后，如果防御中心上已存在相应的区域 （内部、外部或被动），则注册流程将所列的接口添加至现有区域。如果区域不存在，系统会创建并添加接口。有关接口、内联集和安全区域的详细信息，请参阅 《*FireSIGHT 系统用户指南*》。

自动备份

该设备提供一个数据存档机制，以便在发生故障时恢复配置和事件数据。在初始设置过程中，您可以选择 **Enable Automatic Backups**。

启用该设置后，将创建一项定期任务，即对设备上的配置创建周备份。

最终用户许可协议

请仔细阅读 EULA，如果您同意遵守本协议条款，请选择复选框。确保提供的所有信息都正确无误后，请点击 **Apply**。设备已根据您的选择配置好并准备被添加至其管理防御中心。

初始设置页面：防御中心

对于所有的防御中心，您必须通过登录防御中心的网络界面并在设置页面指定初始配置选项来完成设置流程。您必须更改管理员密码，指定网络设置 （若尚未指定），并且接受 EULA。

在设置流程中，您可以注册并许可设备。注册设备之前，您必须在设备上完成设置流程，并将防御中心添加为远程管理器，否则，注册将失败。

有关详细信息，请参阅不同受管设备型号所支持的功能，第 1-7 页和许可 FireSIGHT 系统，第 1-11 页。

要使用网络界面在防御中心上完成初始设置，请执行以下操作：

访问：管理员

步骤 1 将您的浏览器转向 `https://` *`mgmt_ip/`*，其中 *`mgmt_ip`* 是防御中心管理接口的 IP 地址：

- 对于通过以太网线连接至计算机的防御中心，将该计算机的浏览器转向默认管理接口的 IPv4 地址：`https://192.168.45.45/`。
- 对于已配置网络设置的防御中心，使用管理网络上的计算机浏览至防御中心的管理接口 IP 地址。

系统将显示登录页面。

步骤 2 使用 `admin` 作为用户名、`Sourcefire` 作为密码登录。

系统将显示设置页面。有关完成设置的详细信息，请参阅以下各节：

- 更改密码，第 4-11 页
- 网络设置，第 4-11 页
- 时间设置，第 4-12 页

- 重复规则更新导入，第 4-12 页
- 重复地理位置更新，第 4-12 页
- 自动备份，第 4-12 页
- 许可证设置，第 4-12 页
- 设备注册，第 4-13 页
- 最终用户许可协议，第 4-14 页

步骤 3 完成设置后，点击 **Apply**。

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

注 如果使用以太网线直接连接至设备，可断开计算机并将防御中心的管理接口连接至管理网络。使用管理网络上计算机的浏览器，访问位于刚刚配置的 IP 地址或主机名的防御中心，并完成本指南中的剩余步骤。

步骤 4 使用 Task Status 页面 (**System > Monitoring > Task Status**) 验证初始设置是否成功。

此页面每隔 10 秒自动更新一次。在页面为初始设备注册和策略应用任务列出 **Completed** 状态前，请保持监控此页面。如果在安装过程中配置了入侵规则或地理位置更新，您还可以监控这些任务。

现在，该防御中心可以使用了。有关配置部署的详细信息，请参阅 《*FireSIGHT 系统用户指南*》。

步骤 5 继续后续步骤，第 4-14 页中的内容。

更改密码

您必须更改管理员帐户的密码。该帐户拥有管理员权限，您无法将其删除。

思科建议使用包含至少 8 个大小写混合的字母数字字符和至少一个数字字符的强密码。避免使用词典中的单词。

网络设置

防御中心的网络设置允许该设备在管理网络上通信。如果已配置网络设置，此页面中的本章节可预填充。

FireSIGHT 系统提供 IPv4 和 IPv6 管理环境的双堆栈实施。您必须指定管理网络协议（**IPv4**、**IPv6** 或**两者**）。根据您的选择，设置页面将显示多种字段，在这些字段中必须设置 IPv4 或 IPv6 管理 IP 地址、网络掩码或前缀长度和默认网关：

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

还可以指定多达三个 DNS 服务器，以及设备主机名和域。

时间设置

您可以手动或通过 NTP 服务器的网络时间协议 (NTP) 设置防御中心的时间。

您还可以为管理员帐户指定本地网络界面上使用的时区。点击当前时区，然后通过弹出窗口进行更改。

重复规则更新导入

许可证：保护

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

如果您计划在部署中执行入侵检测和防御，思科建议您选择 **Enable Recurring Rule Update Imports**。

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

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

重复地理位置更新

支持的防御中心：除 DC500 外的所有型号

可以使用大多数防御中心查看与系统所生成事件相关的路由 IP 地址的地理信息，以及监控控制面板和 Context Explorer 中的地理位置统计数据。

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

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

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

自动备份

防御中心提供一个数据存档机制，以便在发生故障的情况下恢复配置。在初始设置过程中，您可以选择 **Enable Automatic Backups**。

启用该设置后，系统将创建一项定期任务，即对防御中心上的配置创建周备份。

许可证设置

您可以许可各种功能，为贵公司创建最佳的 FireSIGHT 系统部署。要求防御中心上有 FireSIGHT 的许可证，以执行主机、应用和用户发现。其他型号特定的许可证允许受管设备设备执行各种功能。由于架构和资源的限制，并非所有的许可证都以被应用至所有的受管设备；请参阅不同受管设备型号所支持的功能，第 1-7 页和许可 FireSIGHT 系统，第 1-11 页。

思科建议使用初始设置页面来添加公司购买的许可证。如果现在不添加许可证，您在初始设置过程中注册的所有设备将被作为未许可设备添加至防御中心；在初始设置流程结束后，您必须逐个许可每台设备。请注意，如果您正设置一个被重新映像的设备，并已将许可证设置在恢复过程中保存下来，本章节可预填充。

如果尚未获得许可证，请点击链接导航至 `https://keyserver.sourcefire.com/` 并遵循屏幕上的说明。您需要许可证秘钥 （在初始设置页面上列出）以及以前通过邮件发送给与支持合同相关的联系人的激活秘钥。

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

设备注册

防御中心可以管理所有物理或虚拟设备，目前的支持系统为 FireSIGHT 系统。

注 在将设备注册至防御中心之前，您必须在设备上配置远程管理。

您可以在初始设置过程中将大多数预注册的设备 （请参阅远程管理，第 4-8 页）添加至防御中心。但是，如果设备和防御中心由一台 NAT 设备隔开，您必须在设置过程完成后进行添加。

注册设备时，如果想在注册后将访问控制策略自动应用于设备，可使 **Apply Default Access Control Policies** 复选框保持启用状态。请注意，您无法选择防御中心对每台设备应用哪项策略，只能选择是否应用这些策略。应用于每台设备的策略取决于在配置设备时选择的检测模式 （请参阅检测模式，第 4-9 页），如下表所示。

表 4-2 按检测模式所应用的默认访问控制策略

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

此情况除外，即您以前使用防御中心管理设备并且已更改设备的初始界面配置。在这种情况下，此新防御中心页面应用的策略取决于已更改 （当前）的设备配置。如果有已配置的接口，防御中心会应用默认的入侵防御策略。否则，防御中心应用默认的访问控制策略。

要添加设备，请键入在注册设备时指定的 **Hostname** 或 **IP Address**，以及 **Registration Key**。请记住，这是一个指定的简单密钥，最长达 37 个字符，并且不同于许可证密钥。

然后，使用复选框将已许可功能添加至该设备。您只能选择已添加至防御中心的许可证；请参阅许可证设置，第 4-12 页。

由于架构和资源的限制，并非所有许可证都可应用于所有受管设备。然而，设置页面**不会**阻止您在受管设备上启用不支持的许可证，或者启用没有相应型号特定许可证的功能。这是因为防御中心稍后才能确定设备型号。系统无法启用无效的许可证，而且尝试启用无效的许可证不会减少可用许可证的数量。

有关许可的详细信息，包括可以使用哪种防御中心将每个许可证应用至每个设备型号，请参阅不同防御中心型号支持的功能，第 1-6 页和许可 FireSIGHT 系统，第 1-11 页。

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

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

最终用户许可协议

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

防御中心已根据您的选择配置。在系统显示中间页面后，您已经以管理员用户 （具有管理员角色）身份登录网络界面。继续初始设置页面：防御中心，第 4-10 页中的第 3 步，完成防御中心的初始设置。

后续步骤

完成虚拟设备的初始设置过程并验证设置成功后，思科建议您完成管理任务，以更轻松地管理部署。此外，还应该完成在初始设置过程中跳过的所有任务，例如设备注册和许可。有关以下各节描述的任何任务的详细信息，以及有关如何开始配置部署的详细信息，请参阅 《*FireSIGHT 系统用户指南*》。

提示 如果要使用串行或 LOM/SOL 来连接访问设备的控制台，应重新定向控制台输出；请参阅测试内联旁路接口的安装，第 3-20 页。如果要特别使用 LOM，您必须启用该功能及至少一个 LOM 用户；请参阅启用 LOM 和 LOM 用户，第 7-17 页。

单个用户帐户

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

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

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

运行状况和系统策略

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

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

软件和数据库更新

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

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

使用 3 系列设备上的 LCD 面板

3 系列设备允许使用设备正面的 LCD 面板代替系统的网络界面来查看设备信息或配置特定设置。

LCD 面板有一个显示屏和四个多功能键，在多种运行模式下会根据设备的状态显示不同的信息并且允许进行不同的配置。

有关详细信息，请参阅以下各节：

- 了解 LCD 面板组件，第 5-1 页说明如何识别 LCD 面板的组件和显示面板上的主菜单。
- 使用 LCD 多功能键，第 5-2 页说明如何使用 LCD 面板上的多功能键。
- 空闲显示模式，第 5-3 页描述设备空闲时， LCD 面板如何显示各种系统信息。
- 网络配置模式，第 5-4 页说明如何使用 LCD 面板配置设备的管理接口的网络配置：IPv4 或 IPv6 地址、子网掩码或前缀和默认网关。

注意事项 允许使用 LCD 面板进行配置可能带来安全风险。使用 LCD 面板，只需物理访问，而无需身份验证，即可进行配置。

- 系统状态模式，第 5-6 页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，以及如何更改 LCD 面板亮度和对比度。
- 信息模式，第 5-7 页说明如何查看系统标识信息，例如设备的机箱序列号、 IP 地址、型号以及软件和固件版本。
- 错误警报模式，第 5-8 页描述 LCD 面板如何进行错误或故障状态通信；例如旁路、风扇状态或硬件警报。

注 必须启动设备，才能使用 LCD 面板。有关如何安全启动或关闭设备的信息，请参阅《*FireSIGHT 系统用户指南*》中的“管理设备”章节。

了解 LCD 面板组件

3 系列设备正面的 LCD 面板具有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。映射用符号指示可以使用相应的多功能键执行的操作。
- 多功能键可用于查看系统信息并完成基本配置任务，这些都根据 LCD 面板的模式而异。有关详细信息，请参阅使用 LCD 多功能键，第 5-2 页。

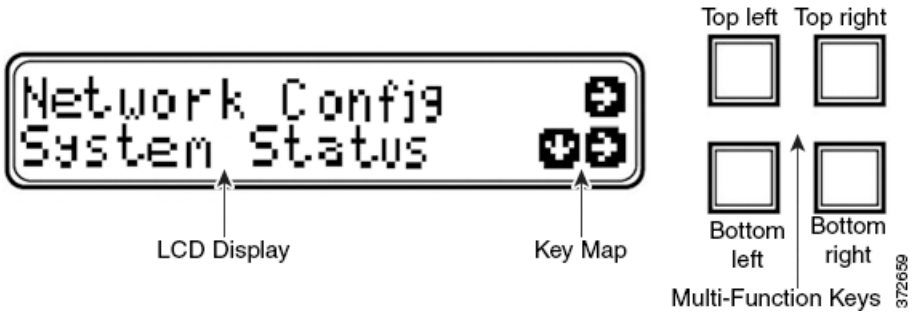
下图显示了面板的默认空闲显示模式，此模式不包含键映射。

图 5-1 LCD 面板空闲显示模式

在空闲显示模式下，面板交替显示 CPU 利用率和空闲可用内存以及机箱序列号。按任意键即可中断空闲显示模式并进入可以访问网络配置、系统状态和信息模式的 LCD 面板主菜单。

下图显示了该主菜单，其中包含与四个多功能键 （左上角、右上角、左下角或右下角）对应的键映射。

图 5-2 LCD 面板主菜单



要访问主菜单，请执行以下操作：

步骤 1 在空闲显示模式，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，请参阅网络配置模式，第 5-4 页。
- 要查看受监控的系统的信息或调整 LCD 面板亮度和对比度，请参阅系统状态模式，第 5-6 页。
- 要查看系统标识信息，请参阅信息模式，第 5-7 页。

注 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

四个多功能键允许导航 3 系列设备的 LCD 面板上的菜单和选项。显示屏上显示键映射时，可以使用多功能键。映射上符号的位置对应相应的功能和执行此功能所用的键的位置。如果没有显示符号，相应键就没有功能。

提示 符号的功能因 LCD 面板模式而异，因此键映射也相应地变化。如果没有获得期望的结果，请检查 LCD 面板的模式。

下表说明了多功能键的功能。

表 5-1 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。
↓	向下箭头	向下滚动当前菜单选项。
←	向左箭头	执行以下一种操作： • 不执行任何操作，只显示 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： • 进入该行显示的菜单选项。 • 将光标向右侧移动。 • 滚动浏览后续文本。
X	取消	取消操作。
+	加	将选择的数字增大一个单位。
-	减	将选择的数字减小一个单位。
✓	复选标记	接受操作。

空闲显示模式

LCD 在非活动状态 （未按任何多功能键）持续 60 秒钟后并且没有检测到任何错误的情况下进入空闲显示模式。如果系统检测到错误，面板进入错误警报模式模式 （请参阅错误警报模式，第 5-8 页），直到错误得以解决。编辑网络配置或运行诊断时，空闲显示模式也被禁用。

在空闲显示模式下，面板交替 （以五秒作为间隔）显示 CPU 利用率和空闲可用内存以及机箱序列号。

每个显示示例可能如下所示：

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

或：

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

在空闲显示模式下，按任意多功能键进入主菜单；请参阅了解 LCD 面板组件，第 5-1 页。

注 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

FireSIGHT 系统提供 IPv4 和 IPv6 管理环境的双堆栈实施。在网络配置模式下，可以使用 LCD 面板配置 3 系列设备的管理接口的网络设置：IP 地址、子网掩码或前缀和默认网关。

默认情况下，禁用使用 LCD 面板更改网络配置的功能。可在初始设置过程或使用设备的网络界面启用此功能。有关详细信息，请参阅允许使用 LCD 面板进行网络配置，第 5-5 页。

注意事项 启用此选项可能会产生安全风险。您只需物理访问，无需身份验证，就可以使用 LCD 面板配置网络设置。

要使用网络配置模式配置网络设置，请执行以下操作：

步骤 1 在空闲显示模式下，按任意多功能键进入主菜单。

系统将显示主菜单：

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

步骤 2 按顶行的向右箭头 (à) 键，访问网络配置模式。

LCD 面板显示以下信息：

```
IPv4                 ↓ →
IPv6                   →
```

步骤 3 按向右箭头键选择想要配置的 IP 地址：

- 对于 IPv4， LCD 面板会显示以下信息：

```
IPv4 set to DHCP.    ←

Enable Manual?       →
```

- 对于 IPv6， LCD 面板会显示如下信息：

```
IPv6 Disabled.       ←

Enable Manual?       →
```

步骤 4 按向右箭头键，手动配置网络：

- 对于 IPv4， LCD 面板显示 IPv4 地址。例如：

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

- 对于 IPv6， LCD 面板显示 IPv6 地址。例如：

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

面板上的第一行显示您是在编辑 IPv4 还是 IPv6 地址。第二行显示正在编辑的 IP 地址。光标位于第一个数字下面，代表正在编辑的数字。两个符号对应每行右侧的多功能键。

请注意，IPv6 地址不完全适配此显示屏。编辑各个数字并将光标向右移动时， IPv6 地址向右侧滚动。

步骤 5 编辑光标下划线所在的数字，如有必要，可以移到 IP 地址中的下一个数字：

- 要编辑此数字，请按顶行的减号 (-) 或 (+) 键，将数字加一或减一。
- 要移到 IP 地址的下一个数字，请按末行的向右箭头键将光标移动到右侧下一个数字。

光标位于第一个数字上时， LCD 面板在 IP 地址末尾显示取消和向右箭头符号。光标位于其他数字上时， LCD 面板显示左右箭头符号。

步骤 6 编辑完 IPv4 或 IPv6 地址时，再次按向右箭头键显示复选标记 (✓) 键接受更改。

按向右箭头键之前，显示屏上的功能符号看起来如下所示：

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

按向右箭头键之后，显示屏上的功能符号看起来如下所示：

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

步骤 7 按复选标记键接受对 IP 地址的更改。

对于 IPv4， LCD 面板显示以下信息：

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

对于 IPv6， LCD 面板显示以下信息：

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

步骤 8 按照和编辑 IP 地址相同的方式编辑子网掩码或前缀，然后按复选标记键接受更改。

LCD 面板显示以下信息：

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

步骤 9 按照和编辑 IP 地址相同的方式编辑默认网关，然后按复选标记键接受更改。

LCD 面板显示以下信息：

```
Save?                ✓
                     X
```

步骤 10 按复选标记键保存更改。

允许使用 LCD 面板进行网络配置

由于会产生安全风险，默认情况下禁用使用 LCD 面板更改网络配置的功能。可以在初始设置过程中（请参阅设置 3 系列设备，第 4-3 页）或按照以下程序中的描述使用设备的网络界面启用此功能。

要允许使用设备的 LCD 面板进行网络配置，请执行以下操作：

访问：管理员

步骤 1 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。

步骤 2 选择 **System > Local > Configuration**。

系统将显示信息页面。

步骤 3 点击 **Network**。

系统将显示 Network Settings 页面。

步骤 4 在 **LCD Panel** 下面，选择 **Allow reconfiguration of network configuration** 复选框。系统显示安全警告时，请确认想要启用此选项。

提示 有关此页面其他选项的信息，请参阅 《*FireSIGHT 系统用户指南*》。

步骤 5 点击 **Save**。

网络设置更改成功。

系统状态模式

LCD 面板的 System Status 模式显示受监控的系统的信息，例如链路状态传播、旁路状态和系统资源。也可以在 System Status 模式下更改 LCD 面板的亮度和对比度。

下表介绍了此模式下可以提供的信息和选项。

表 5-2 系统状态模式选项

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

Link State	显示正在使用的任何内联集的列表，以及该集合的链路状态。第一行标识内联集，第二行显示其状态 （正常或触发）。例如：
	`eth2-eth3:`
	`normal`

Fail Open	显示当前使用的旁路内联集的列表以及那些配对的状态：要么正常，要么处于旁路模式。
Fan Status	显示设备中风扇的列表和状态。
Diagnostics	可以按照支持部门提供的具体按键顺序访问此选项。 ⚠ **注意事项** 没有支持部门的指导，请**勿**访问 Diagnostics 菜单。在没有获得支持部门具体指导的情况下擅自访问 Diagnostics 菜单可能会损坏系统。
LCD Brightness	允许调整 LCD 显示屏的亮度。
LCD Contrast	允许调整 LCD 显示屏的对比度。

要进入 System Status 模式和查看受监控的系统信息，请执行以下操作：

步骤 1 在空闲显示模式下，按任意多功能键进入主菜单。

系统将显示主菜单：

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

步骤 2 按末行的向右箭头 (→) 键，访问 System Status 模式。

LCD 面板显示以下信息：

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

步骤 3 按向下箭头 (â) 键，滚动浏览选项。在想要查看的状态旁边的行中按向右箭头键。

根据所选的选项，LCD 面板显示第 5-6 页上的表 5-2 中列出的信息。要更改 LCD 面板亮度或对比度，请参阅下一步骤。

要调整 LCD 面板亮度或对比度，请执行以下操作：

步骤 1 在 System Status 模式下，按向下箭头 (â) 键滚动浏览选项，直到 LCD 面板显示 LCD Brightness 和 LCD Contrast 选项：

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

步骤 2 在想要调整的 LCD 显示屏特性 （亮度或对比度）旁边的行中按向右箭头键。

LCD 面板显示以下信息：

```
Increase              →
Decrease           ↓  →
```

步骤 3 按向右箭头键以增大或减小所选择的显示屏特性。

按这些键的时候 LCD 显示屏相应地变化。

步骤 4 按向下箭头显示 Exit 选项。

```
Decrease           ↓  →
Exit                  →
```

步骤 5 在 Exit 行中按向右箭头键，保存设置并返回主菜单。

信息模式

LCD 面板的信息模式显示系统标识信息，例如设备的机箱序列号、IP 地址、型号和软件与固件版本。如果您致电支持部门获取帮助，他们可能会要求提供这些信息。

下表介绍了此模式下可以提供的信息。

表 5-3 信息模式选项

选项	说明
IP address	显示设备的管理接口的 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。使用多功能键滚动浏览以下信息： • 产品版本 • NFE 版本 • Micro Engine 版本 • Flash 版本 • GerChr 版本

要进入信息模式并查看系统标识信息，请执行以下操作：

步骤 1 在空闲显示模式下，按任意多功能键进入主菜单。

系统将显示主菜单：

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

步骤 2 按向下箭头 (â) 键滚动浏览各个模式，直到 LCD 面板显示信息模式：

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

步骤 3 按末行的向右箭头 (→) 键，访问信息模式。

步骤 4 按向下箭头 (â) 键，滚动浏览选项。在想要查看的信息旁边的行中按向右箭头键。

根据所选的选项， LCD 面板显示第 5-7 页上的表 5-3 中列出的信息。

错误警报模式

出现硬件错误或故障状态时，错误警报模式会打断空闲显示模式。在空闲显示模式下，LCD 显示屏闪烁并显示下表中列出的一个或多个错误。

表 5-4 LCD 面板错误警报

错误	说明
Hardware alarm	出现硬件警告时发出此警报
Link state propagation	显示配对接口的链路状态
Bypass	显示在旁路模式下配置的内联集的状态
Fan status	风扇出现严重情况时发出此警报

出现硬件错误警报时， LCD 显示主要硬件警报菜单，如下所示：

```
HARDWARE ERROR!      →
Exit                 →
```

可以使用多功能键滚动浏览错误警报列表或退出错误警报模式模式。请注意，LCD 显示屏将继续闪烁并显示警报消息，直到所有错误情况都已解决。

LCD 面板总是首先显示平台守护程序错误消息，然后显示其他硬件错误消息的列表。下表提供了关于 3 系列设备错误消息的基本信息，其中 *x* 表示生成警报的 NFE 加速卡 （0 或 1）。

表 5-5 硬件警报错误消息

错误消息	监控的状况	说明
NFE_platformd*x*	平台守护程序	平台守护程序发生故障时发出此警报。
NFE_temp*X*	温度状态	加速卡的温度超出可接受的限制时发出此警报。 • WARNING：高于 80°C/176°F （7000 系列）或 97°C/206°F （8000 系列）。 • CRITICAL：高于 90°C/194°F （7000 系列）或 102°C/215°F （8000 系列）。
HeartBeat*X*	心跳	系统无法检测心跳时发出此警报。
frag*x*	nfe_ipfragd （主机分片）守护程序	当 ipfragd 守护程序出现故障时发出此警报。
rules*X*	Rulesd （主机规则）守护程序	当 Rulesd 守护程序出现故障时发出此警报。
TCAM*X*	TCAM 守护程序	当 TCAM 守护程序出现故障时发出此警报。
NFEMessD*X*	消息守护程序	当消息守护程序出现故障时发出此警报。
NFEHardware	硬件状态	当一个或多个加速卡不通信时发出此警报。
NFEcount	受检测的卡	当设备上检测到的加速卡的数量与平台的预期加速卡数量不一致时发出此警报。
仅限于 7000 系列：GerChr_comm 仅限于 7000 系列：NMSB_comm	通信	媒体组件不存在或不通信时发出此警报。

表 5-5 硬件警报错误消息 （续）

错误消息	监控的状况	说明
仅限于 7000 系列： gerd 仅限于 8000 系列： scmd	scmd 守护程序状态	当 scmd 守护程序出现故障时发出此警报。
仅限于 7000 系列： gpsl 仅限于 8000 系列： psls	psls 守护程序状态	当 psls 守护程序出现故障时发出此警报。
仅限于 7000 系列： gftw 仅限于 8000 系列： ftwo	ftwo 守护程序状态	当 ftwo 守护程序出现故障时发出此警报。
NFE_port18 NFE_port19 NFE_port20 NFE_port21	内部链路状态	当网络模块交换机和加速卡之间的链路发生故障时发出此警报： • 7000 系列 所有系列：仅限于 NFE_port18 • 8000 系列 81xx 子系列：仅限于 NFE_port18 和 NFE_port19 82xx 子系列和 83xx 子系列：NFE_port18、 NFE_port19、 NFE_port20 和 NFE_port21

使用以下程序在 LCD 显示屏上查看硬件警报错误消息。

要查看硬件警报错误警告，请执行以下操作：

步骤 1 在错误警报模式模式下，在 HARDWARE ERROR!行，按向右箭头 (→) 键查看触发错误警报模式模式的硬件错误。

LCD 面板从 NFE platform 守护程序故障开始列出错误警报消息，然后列出错误消息列表。

```
NFEplatformdX
NFEtempX                ↓
```

其中 *X* 表示生成警报的加速卡 （0 或 1）。

步骤 2 在错误消息行，按向下箭头 (â) 键查看其他错误。如果没有其他错误，系统将显示 Exit 行。

```
Exit                    →
```

步骤 3 按向右箭头 (→) 键退出错误警报模式模式。

如果在解决触发警报的错误之前退出错误警报模式模式，LCD 面板将返回错误警报模式模式。如需帮助，请联系支持部门。

硬件规格

FireSIGHT 系统随各种设备一起提供以满足组织的需求。有关在机架中安装设备的信息，请参阅机架和机柜安装选项，第 6-1 页。

注 有关 ASA FirePOWER 设备硬件规格的信息，请参阅ASA 文档。

以下节中将说明每个设备的硬件规格。

机架和机柜安装选项

可以将 FireSIGHT 系统设备安装在机架和服务器机柜中。除了 3D7010、 3D7020 和 3D7030，设备随附机架安装套件。有关在机架中安装设备的信息，请参阅机架安装套件随附的说明。

3D7010、 3D7020 和 3D7030 需要托架和机架安装套件 （可单独出售）。可以为其他设备单独购买机架和机柜安装套件。

防御中心

有关防御中心的详细信息，请参阅以下节：

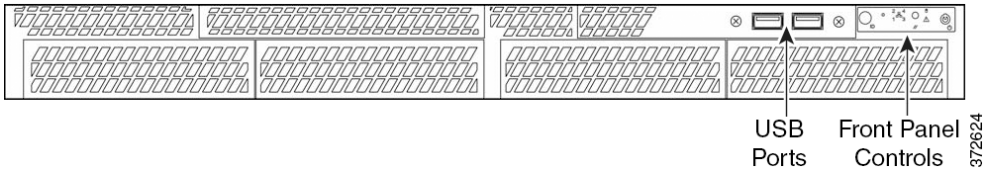
DC750

DC750 是 1U 设备。有关此设备的详细信息，请参阅以下节：

DC750 机箱前视图

DC750 机箱前面包含前面板控件。

图 6-1 DC750



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

图 6-2 DC750

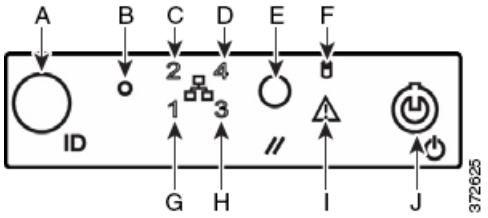


表 6-1 前面板组件

A	带有 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	J	带电源 LED 的电源按钮

机箱的前面板包括五个 LED，可以查看这些 LED 来显示系统的运行状态。下表介绍了前面板上的 LED。

表 6-2 DC750 前面板 LED

LED	说明
系统状态	指示系统状态： • 绿色指示灯表示系统在正常运行。 • 闪烁的绿色指示灯表示系统正在降级状态下运行。 有关详细信息，请参阅第 6-3 页上的表 6-3。

表 6-2 DC750 前面板 LED （续）

LED	说明
电源	指示系统是否有电或处于休眠状态： • 绿色指示灯表示系统在正常运行。 • 指示灯不亮表示系统已关闭。 • 闪烁的绿色指示灯表示系统处于休眠状态。 待机状态下由芯片组保持休眠指示。如果系统在不通过 BIOS 的情况下关机，系统开机时将存储关机时的实际状态，直至 BIOS 将其清除。如果由于阻止 BIOS 运行的故障或配置更改导致系统非正常关机，电源指示灯将闪烁，同时系统状态指示灯将关闭。
硬盘驱动器活动	指示硬盘驱动器活动： • 闪烁的绿色指示灯表示固定磁盘驱动器处于活动状态。 • 指示灯不亮表示无驱动器活动，或者系统已关机或处于休眠状态。 驱动器活动依据机载硬盘控制器确定。服务器主板也提供访问加载控制器此指示灯的标头。
NIC 活动	指示系统和网络之间的活动。 • 闪烁的绿色指示灯表示有活动。 • 指示灯不亮表示没有活动。

下表介绍了系统状态 LED 可能亮起的状况。

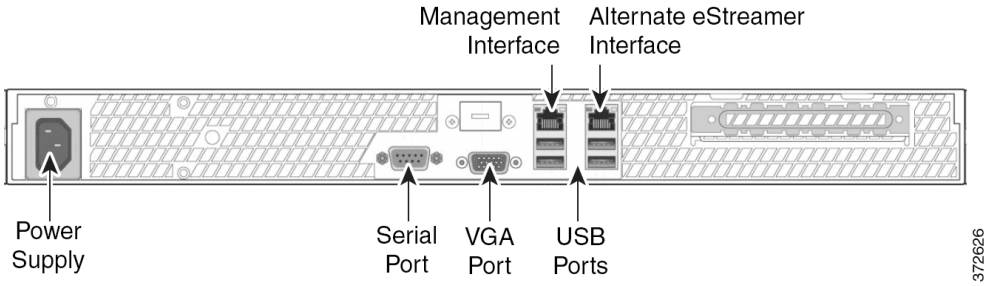
表 6-3 DC750 系统状态

状况	说明
严重	由于以下事件导致的任何严重或不可恢复的超出阈值状况： • 超出温度、电压或风扇重要阈值 • 电源子系统故障 • 由于处理器安装不正确或处理器不兼容系统无法启动 • 重要事件记录错误，包括系统内存无法纠正的 ECC 错误和毁灭性/无法纠正的总线错误，例如 PCI SERR 和 PERR
不严重	不严重的状况指由于以下事件导致的超出阈值的状况： • 超出温度、电压或风扇的非重要阈值 • 机箱入侵 • 来自 BIOS 的 Set Fault Indication 命令；BIOS 可能将此命令用于指示系统内存或 CPU 配置更改等其他非重要状态
降级	降级状况与以下事件相关： • 故障恢复开机 (FRB) 或 BIOS 禁用了一个或多个处理器 • BIOS 已禁用或映射部分系统内存

DC750 机箱后视图

机箱后部包含 DC750 的电源和连接端口。

图 6-3 DC750



下表介绍了设备后面的功能。

表 6-4 DC750 系统组件：后视图

功能	说明
电源	通过交流电源向防御中心供电
串行端口、 VGA 端口 USB 端口	可用于将显示器、键盘和鼠标连接到设备上
10/100/1000 Mbps 以太网管理接口	用于带外管理网络连接。管理接口**仅限**用于维护和配置用途，不可用于传输业务流量。
备用 eStreamer 接口	为 eStreamer 客户端提供备用接口

10/100/1000 Mbps 管理接口位于设备后面。下表介绍了与管理接口相关的 LED。

表 6-5 DC750 管理接口 LED

LED	说明
左侧 （链路）	指示链路是否启用： • 如果指示灯亮起，则链路已启用。 • 指示灯不亮表示没有链路。
右侧 （活动）	指示端口上的活动： • 指示灯闪烁表示有活动。 • 指示灯不亮表示没有链路。

DC750 物理和环境参数

下表介绍了设备的物理属性和环境参数。

表 6-6 DC750 物理和环境参数

参数	DC750
外形	1U
尺寸 （长 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 在 110 V、 50/60 Hz 下，最大 6.0 A 在 220 V、 50/60 Hz 下，最大 3.0 A
工作温度	50°F 至 95°F （10°C 至 35°C），每小时最大变化率不超过 18°F (10°C)
非工作温度	-40°F 至 +158°F （-40°C 至 +70°C）
非工作湿度	90%，在 95°F (35°C) 下无冷凝
噪声	在典型的办公室环境温度 (23+/-2°C, 73+/-4°F) 下为 7.0 调整分贝
工作冲击	在 2G 半正弦波冲击下无错误 （持续 11 毫秒 ）
包装冲击	从 24 英寸 （60 厘米）处自由下落之后仍可运行，但是可能出现表面损坏；机箱重量为 40 至 80 磅。（18 至 36 千克）
ESD	空气放电， 12 kV；接触放电， 8 K
气流	从正面到背面
系统冷却需求	1660 BTU/小时

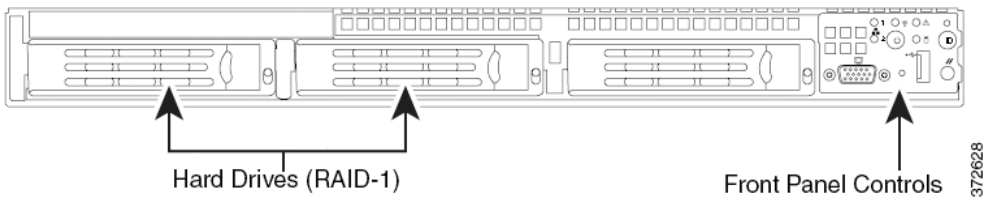
DC1500

DC1500 是 1U 设备。有关此设备的详细信息，请参阅以下节：

- DC1500 机箱前视图，第 6-5 页
- DC1500 机箱后视图，第 6-8 页
- DC1500 物理和环境参数，第 6-9 页

DC1500 机箱前视图

机箱前面包含硬盘驱动器和前面板控件。



下图显示了前面板控件和 LED。

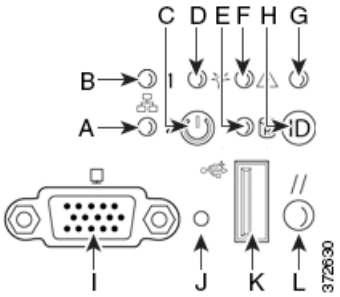


表 6-7 前面板组件

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	J	不可屏蔽的中断按钮
E	固定磁盘驱动器状态	K	USB 2.0 连接器
F	系统状态 LED	L	复位按钮

机箱的前面板包括六个 LED，可以在使用或不使用前挡板的情况下查看这些 LED，显示系统的运行状态。下表介绍了前面板上的 LED。

表 6-8 DC1500 前面板 LED

LED	说明
NIC 1 活动 NIC 2 活动	指示系统和网络之间的活动。 • 闪烁的绿色指示灯指示有活动。 • 指示灯不亮指示没有活动。
电源/休眠	指示系统是否有电或处于休眠状态： • 绿色指示灯表示系统在正常运行。 • 闪烁的绿色指示灯表示系统处于休眠状态。 • 指示灯不亮表示系统未通电。 待机状态下由芯片组保持休眠指示。如果系统在不通过 BIOS 的情况下关机，系统开机时将存储关机时的实际状态，直至 BIOS 将其清除。如果由于阻止 BIOS 运行的故障或配置更改导致系统非正常关机，电源指示灯将闪烁，同时系统状态指示灯将关闭。
硬盘驱动器活动	指示硬盘驱动器活动： • 闪烁的绿色指示灯表示固定磁盘驱动器处于活动状态。 • 黄色指示灯指示存在固定磁盘驱动器故障。 • 指示灯不亮表示无驱动器活动，或者系统已关机或处于休眠状态。 驱动器活动依据机载硬盘控制器确定。服务器主板也提供访问加载控制器此指示灯的标头。

表 6-8 DC1500 前面板 LED （续）

LED	说明
系统状态	指示系统状态： • 绿色指示灯表示系统在正常运行。 • 闪烁的绿色指示灯表示系统正在降级状态下运行。 • 黄色指示灯指示系统处于重要或不可恢复的状况下。 • 闪烁的黄色指示灯指示系统处于非重要状况下。 • 指示灯不亮表示正在进行开机自检 (POST) 或系统已停机。 **注** 黄色状态指示灯优先于绿色状态指示灯。当黄色指示灯亮起或闪烁时绿色指示灯关闭。 有关详细信息，请参阅第 6-3 页上的表 6-3。
系统 ID	帮助在带有其他类似系统的高密度机架中识别系统： • 蓝色指示灯指示已按 ID 按钮，并且设备背面的蓝色指示灯亮起。 • 指示灯不亮表示未按 ID 按钮。

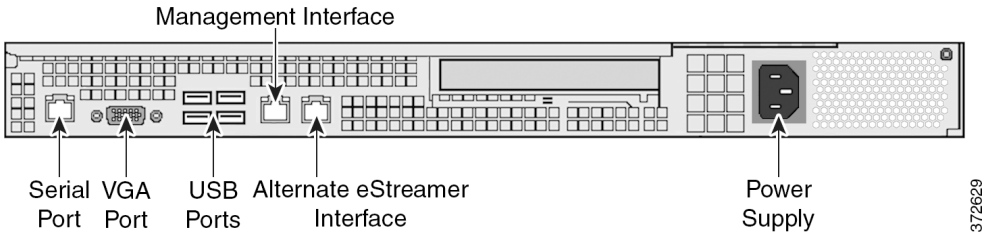
下表介绍了系统状态 LED 可能亮起的状况。

表 6-9 DC1500 系统状态

状况	说明
严重	由于以下事件导致的任何严重或不可恢复的超出阈值状况： • 超出温度、电压或风扇重要阈值 • 电源子系统故障 • 由于处理器安装不正确或处理器不兼容系统无法启动 • 重要事件记录错误，包括系统内存无法纠正的 ECC 错误和毁灭性/无法纠正的总线错误，例如 PCI SERR 和 PERR
不严重	不严重的状况指由于以下事件导致的超出阈值的状况： • 超出温度、电压或风扇的非重要阈值 • 机箱入侵 • 来自 BIOS 的 Set Fault Indication 命令；BIOS 可能将此命令用于指示系统内存或 CPU 配置更改等其他非重要状态
降级	降级状况与以下事件相关： • 故障恢复开机 (FRB) 或 BIOS 禁用了一个或多个处理器 • BIOS 已禁用或映射部分系统内存

DC1500 机箱后视图

机箱后部包含连接端口和电源。



下表介绍了设备后面的功能。

表 6-10 DC1500 系统组件：后视图

功能	说明
电源	通过交流电源向防御中心供电。
VGA 端口 USB 端口	可用于将显示器、键盘和鼠标连接到防御中心上。
10/100/1000 Mbps 以太网管理接口	用于带外管理网络连接。管理接口**仅限**用于维护和配置用途，不可用于传输业务流量。
备用 eStreamer 接口	为 eStreamer 客户端提供备用接口
RJ45 串行端口	可用于建立直接访问设备上所有管理设备的工作站-设备直接连接（使用 RJ45 转 DB-9 适配器）。 RJ45 串行端口**仅限**用于维护和配置用途，不可用于传输业务流量。 **注** 不能同时使用前后面板串行端口。

10/100/1000 Mbps 管理接口位于设备后面。下表介绍了与管理接口相关的 LED。

表 6-11 DC1500 管理接口 LED

LED	说明
左侧 （链路）	指示链路是否启用： • 如果指示灯亮起，则链路已启用。 • 指示灯不亮表示没有链路。
右侧 （活动）	指示端口上的活动： • 指示灯闪烁表示有活动。 • 指示灯不亮表示没有活动。

DC1500 物理和环境参数

下表介绍了设备的物理属性和环境参数。

表 6-12 DC1500 物理和环境参数

参数	说明
外形	1U
尺寸 （长 x 宽 x 高）	27.2 英寸 x 16.93 英寸 x 1.7 英寸 (69.1 x 43.0 x 4.3 cm)
最大重量	34 磅 （15.4 千克）
电源	120 VAC 的 600 W 电源 在 110 V、 50/60 Hz 下，最大 9.5 A 在 220 V、 50/60 Hz 下，最大 4.75 A
工作温度	50°F 至 95°F （10°C 至 35°C）
非工作温度	-40°F 至 +158°F （-40°C 至 +70°C）
非工作湿度	90%，在 82.4°F (28°C) 下无冷凝
噪声	在典型办公室环境温度下在空闲状态时小于 7.0 调整分贝 （机架安装）
工作冲击	在 2G 半正弦波冲击下无错误 （持续 11 毫秒 ）
包装冲击	从 24 英寸 （60 厘米）处自由下落之后仍可运行，但是可能出现表面损坏；机箱重量为 40 至 80 磅。（18 至 36 千克）
ESD	按照 Intel 环境测试规范为 +/-15 kV （I/O 端口 +/-8 kV）
气流	从正面到背面
系统冷却需求	2550 BTU/小时

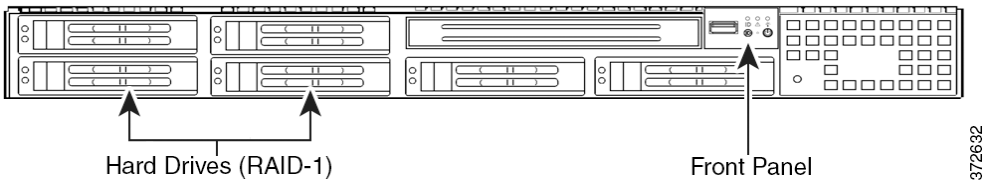
DC3500

DC3500 是 1U 设备。有关此设备的详细信息，请参阅以下节：

- DC3500 机箱前视图，第 6-9 页
- DC3500 机箱后视图，第 6-12 页
- DC3500 物理和环境参数，第 6-13 页

DC3500 机箱前视图

机箱前面包含硬盘驱动器和前面板。



设备正面包括控件和前面板 LED 显示屏。

下图显示了前面板控件和 LED。

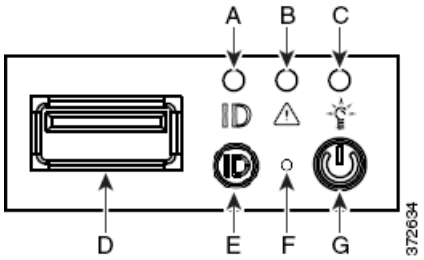


表 6-13 前面板组件

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		

机箱的前面板包括三个 LED，显示系统的运行状态。下表介绍了前面板上的 LED。

表 6-14 DC3500 前面板 LED

LED	说明
电源	指示系统是否有电： • 绿色指示灯指示系统有电。 • 指示灯不亮表示系统未通电。
系统状态	指示系统状态： • 绿色指示灯表示系统在正常运行。 • 闪烁的绿色指示灯表示系统正在降级状态下运行。 • 闪烁的黄色指示灯指示系统处于非重要状况下。 • 黄色指示灯指示系统处于重要或不可恢复的状况下。 • 指示灯不亮表示系统正在启动或已关闭。 **注** 黄色状态指示灯优先于绿色状态指示灯。当黄色指示灯亮起或闪烁时绿色指示灯关闭。 有关详细信息，请参阅第 6-11 页上的表 6-15。
硬盘驱动器活动	指示硬盘驱动器状态： • 闪烁的绿色指示灯表示固定磁盘驱动器处于活动状态。 • 黄色指示灯指示存在固定磁盘驱动器故障。 • 指示灯不亮表示无驱动器活动，或者系统已关机。

表 6-14 DC3500 前面板 LED （续）

LED	说明
NIC 活动	指示是否有任何网络活动： • 闪烁的绿色指示灯指示有网络活动。 • 指示灯不亮表示没有网络活动。
系统 ID	帮助在带有其他类似系统的高密度机架中识别系统： • 蓝色指示灯指示已按 ID 按钮，并且设备背面的蓝色指示灯亮起。 • 指示灯不亮表示未按 ID 按钮。

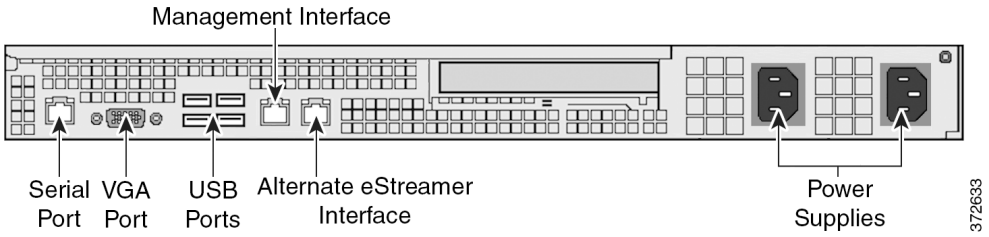
下表介绍了系统状态 LED 可能亮起的状况。

表 6-15 DC3500 系统状态

状况	说明
严重	由于以下事件导致的任何严重或不可恢复的超出阈值状况： • 超出温度、电压或风扇重要阈值 • 电源子系统故障 • 由于处理器安装不正确或处理器不兼容系统无法启动 • 重要事件记录错误，包括系统内存无法纠正的 ECC 错误和毁灭性/无法纠正的总线错误，例如 PCI SERR 和 PERR
不严重	不严重的状况指由于以下事件导致的超出阈值的状况： • 超出温度、电压或风扇的非重要阈值 • 机箱入侵 • 来自 BIOS 的 Set Fault Indication 命令；BIOS 可能将此命令用于指示系统内存或 CPU 配置更改等其他非重要状态
降级	降级状况与以下事件相关： • 故障恢复开机 (FRB) 或 BIOS 禁用了一个或多个处理器 • BIOS 禁用或映射某些系统内存 • 某个电源被拔下或不起作用 **提示** 如果发现降级状况指示，请先检查电源连接。关闭设备，断开两根电源线，重新连接电源线使其重新复位，然后重新启动设备。 ⚠ **注意事项** 要安全关机，请使用*FireSIGHT 系统用户指南*中“管理设备”章节中的操作步骤或防御中心的外壳的 `shutdown -h now` 命令。

DC3500 机箱后视图

机箱后部包含连接端口和电源。



下表介绍了设备后面的功能。

表 6-16 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	可用于将显示器、键盘和鼠标连接到设备上，以代替使用 RJ45 串行端口，建立直接的工作站-设备连接。还必须使用 USB 端口利用设备随附的闪盘将设备还原到其原始出厂状态。
RJ45 串行端口	可用于建立直接访问设备上所有管理设备的工作站-设备直接连接（使用 RJ45 转 DB-9 适配器）。 RJ45 串行端口**仅限**用于维护和配置用途，不可用于传输业务流量。 **注** 不能同时使用前后面板串行端口。
10/100/1000 Mbps 以太网管理接口	用于带外管理网络连接。管理接口**仅限**用于维护和配置用途，不可用于传输业务流量。
备用 eStreamer 接口	为 eStreamer 客户端提供备用接口
冗余电源	通过交流电源向设备供电

10/100/1000 Mbps 管理接口位于设备后面。下表介绍了与管理接口相关的 LED。

表 6-17 DC3500 管理接口 LED

LED	说明
左侧 （活动）	指示端口上的活动： • 指示灯闪烁表示有活动。 • 指示灯不亮表示没有活动。
右侧 （链路）	指示链路是否启用： • 指示灯亮起指示链路已启用。 • 指示灯不亮表示没有链路。

电源模块位于设备的后面。下表介绍了与双电源关联的 LED。

表 6-18 DC3500 电源 LED

LED	说明
关闭	没有接通电源。
黄色	未给此模块提供电源。 或 出现模块故障、保险丝熔断或风扇故障等严重的电源事件；电源关闭。
闪烁黄色	出现高温或风扇转速缓慢等电源警告事件；电源继续运行。
闪烁绿色	有交流电源输入；有待机电压，电源被关闭。
绿色	电源已插入而且正常运行。

DC3500 物理和环境参数

下表介绍了设备的物理属性和环境参数。

表 6-19 DC3500 物理和环境参数

参数	说明
外形	1U
尺寸 （长 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 VDC 的双 650 W 冗余电源 在 110 V、 50/60 Hz 下，最大 8.5 A 在 220 V、 50/60 Hz 下，最大 4.2 A
工作温度	50°F 至 95°F （10°C 至 35°C）
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%，在 95°F (35°C) 下无冷凝
噪声	在典型办公室环境温度下在空闲状态时小于 7.0 分贝 （机架安装）
工作冲击	在 2G 半正弦波冲击下无错误 （持续 11 毫秒 ）
包装冲击	从 24 英寸 （60 厘米）自由下落之后仍可运行，但是可能出现表面损坏；机箱重量为 40 至 80 磅 （18 至 36 千克）。
ESD	按照 Intel 环境测试规范为 +/-15 KV （I/O 端口 +/-8 KV）
气流	从正面到背面
系统冷却需求	2550 BTU/小时
RoHS	符合 RoHS 指令 2002/95/EC

7000 系列设备

所有 7000 系列设备都在设备的正面配有 LCD 面板，可以查看此面板，并且如果启用了配置功能，还可以配置设备。

有关设备的详细信息，请参阅以下各节：

- 3D7010、 3D7020 和 3D7030，第 6-14 页
- 3D7110 和 3D7120，第 6-18 页
- 3D7115、 3D7125 和 AMP7150，第 6-25 页

3D7010、 3D7020 和 3D7030

3D7010、 3D7020 和 3D7030 设备，也称为 70xx 子系列，是 1U 设备，宽度为机架托盘的一半并且随附八个铜接口，每个都支持可配置的旁路功能。有关 70xx 子系列设备的安全注意事项，请参阅 《*FirePOWER 与 FireSIGHT 设备监管合规性和安全性信息*》文档。

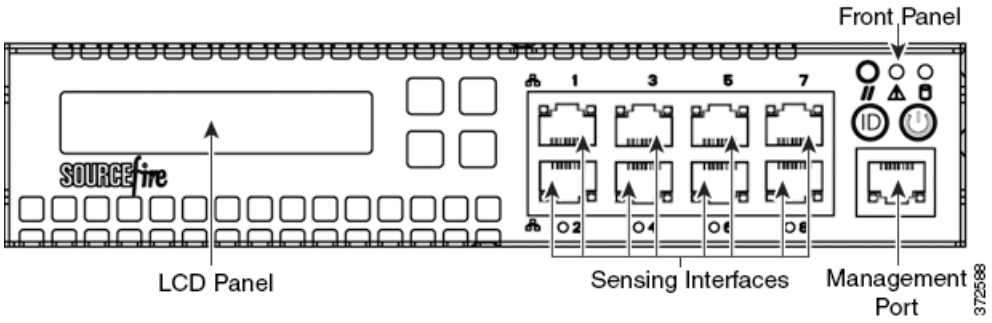
有关详细信息，请参阅以下各节：

- 70xx 子系列前视图，第 6-14 页
- 70xx 子系列后视图，第 6-17 页
- 70xx 子系列物理和环境参数，第 6-18 页

70xx 子系列前视图

机箱前面包含 LCD 面板、感应接口、前面板和管理接口。

图 6-4　　70xx 子系列（机箱：CHRY-1U-AC）前视图



下表介绍了设备前面的功能。

表 6-20　　70xx 子系列系统组件：前视图

功能	说明
LCD 面板	可以在多种模式下运行，用于配置设备、显示错误消息和查看系统状态。有关详细信息，请参阅使用 3 系列设备上的 LCD 面板，第 5-1 页。
感应接口	包含连接到网络的感应接口。有关信息，请参阅感应接口，第 6-16 页。
10/100/1000 Mbps 以太网管理接口	用于带外管理网络连接。管理接口**仅限**用于维护和配置用途，不可用于传输业务流量。

表 6-20 70xx 子系列系统组件：前视图 （续）

功能	说明
前面板	包括显示系统的运行状态的 LED，以及电源按钮等各种控件。有关详细信息，请参阅表 6-30 3D7110 和 3D7120 前面板组件，第 6-19 页。

图 6-5 70xx 子系列前面板

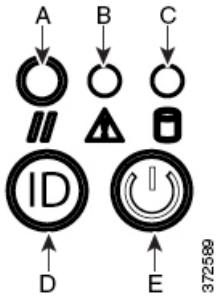


表 6-21 前面板组件

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		

机箱的前面板包括显示系统的运行状态的 LED。下表介绍了前面板上的 LED。

表 6-22 70xx 子系列前面板 LED

LED	说明
复位按钮	可用于重新启动设备，而无需断开其电源。
系统状态	指示系统状态： • 绿色指示灯指示系统已通电而且正常运行或已断电并连接到交流电源上。 • 黄色指示灯指示存在系统故障。 有关详细信息，请参阅第 6-16 页上的表 6-23。
硬盘驱动器活动	指示硬盘驱动器状态： • 闪烁的绿色指示灯表示固定磁盘驱动器处于活动状态。 • 如果指示灯关闭，则无驱动器活动或系统已关闭。
系统 ID	按 ID 按钮时，它显示蓝色指示灯，在机箱的后部可以看见蓝色指示灯。
电源按钮和 LED	指示设备是否有电： • 绿色指示灯指示设备已通电，而且系统打开。 • 指示灯不亮表示系统已关闭或未通电。

下表介绍了系统状态 LED 可能亮起的状态。

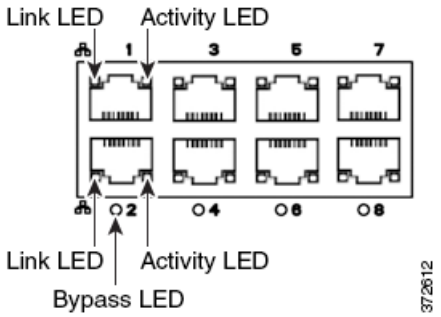
表 6-23 70xx 子系列系统状态

状况	说明
严重	由于以下事件导致的任何严重或不可恢复的超出阈值状况： • 超出温度、电压或风扇重要阈值 • 电源子系统故障 • 由于处理器安装不正确或处理器不兼容系统无法启动 • 重要事件记录错误，包括系统内存无法纠正的 ECC 错误和毁灭性/无法纠正的总线错误，例如 PCI SERR 和 PERR
不严重	不严重的状况指由于以下事件导致的超出阈值的状况： • 超出温度、电压或风扇的非重要阈值 • 来自 BIOS 的 Set Fault Indication 命令；BIOS 可能将此命令用于指示系统内存或 CPU 配置更改等其他非重要状态
降级	降级状况与以下事件相关： • 故障恢复开机 (FRB) 或 BIOS 禁用了一个或多个处理器 • BIOS 禁用或映射某些系统内存 • 某个电源被拔下或不起作用

感应接口

70xx 子系列设备随附八个铜接口，每个接口都支持可配置的旁路功能。

图 6-6 八端口 1000BASE-T 铜接口



使用下表了解铜接口上的活动和链路 LED。

表 6-24 70xx 子系列铜链路/活动 LED

状态	说明
两个 LED 都关闭	接口没有链路。
黄色链路	接口上流量的速度是 10 Mb 或 100 Mb。
绿色链路	接口上流量的速度是 1 Gb。
活动闪烁绿色指示灯	接口有链路而且正在传递流量。

使用下表了解铜接口上的旁路 LED。

表 6-25 70xx 子系列铜旁路 LED

状态	说明
关闭	接口对不在旁路模式下或没有电源。
稳定绿色	接口已经准备就绪进入旁路模式。
稳定黄色	接口对已进入旁路模式并且不检查流量。
闪烁黄色	接口对处于旁路模式下；即已在出故障时自动打开。

10/100/1000 管理接口位于设备前面。下表介绍了与管理接口相关的 LED。

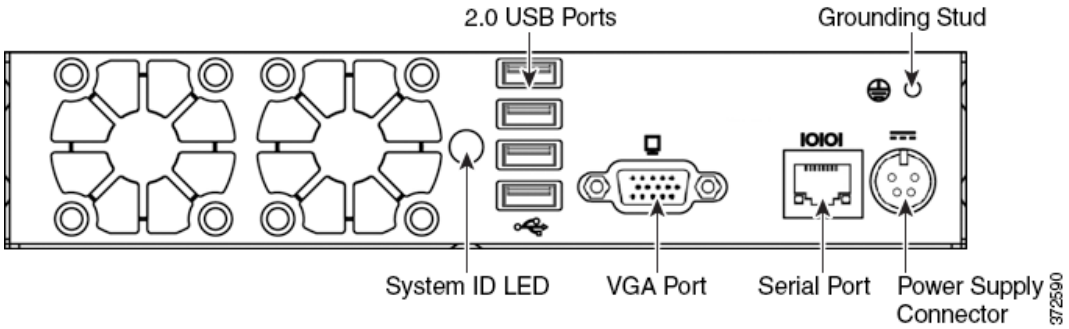
表 6-26 70xx 子系列管理接口 LED

LED	说明
左侧 （链路）	指示链路是否启用。如果指示灯亮起，则链路已启用。如果指示灯不良，则没有链路。
右侧 （活动）	指示端口上的活动。如果指示灯闪烁，则有活动。如果指示灯不亮，则没有活动。

70xx 子系列后视图

机箱后部包含系统 ID LED、连接端口，接地螺柱和电源连接器。

图 6-7 70xx 子系列 （机箱：CHRY-1U-AC）后视图



下表介绍了设备后面的功能。

表 6-27 70xx 子系列系统组件：后视图

功能	说明
系统 ID LED	帮助在带有其他类似系统的高密度机架中识别系统。蓝色 LED 指示已按 ID 按钮。
2.0 USB 端口 VGA 端口 串行端口	可用于将显示器、键盘和鼠标连接到设备上，以代替使用 RJ45 串行端口，建立直接的工作站-设备连接。
接地螺柱	可用于将设备连接到公共连接网络。有关详细信息，请参阅 FirePOWER 设备电源要求，第 A-1 页。
12 伏电源连接器	通过交流电源为设备提供电源连接。

70xx 子系列物理和环境参数

下表介绍了设备的物理属性和环境参数。

表 6-28 70xx 子系列物理和环境参数

参数	说明
外形	1U，半机架的宽度
尺寸 （长 x 宽 x 高）	单机箱：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） 双机箱托架：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）
机箱最大装机重量	机箱：7 磅 （3.17 千克） 单机箱和电源托架：17.7 磅 （8.03 千克） 双机箱和电源的单个托架：24.7 磅 （11.2 千克）
铜 1000BASE-T	成对配置的千兆铜以太网旁路接口 电缆和距离：Cat5E 类别， 50 米距离
电源	200 瓦交流电源 电压：100 VAC 至 240 VAC 标称电压 （最大 90 VAC 至 264 VAC） 电流：整个范围内最高 2A 频率范围：50/60 Hz 标称频率 （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 超出这些限制的操作无法保障，建议不要超出限制。
非工作湿度	0% 至 95%，无冷凝 将装置存储在相对湿度为 95% 的无冷凝条件下。请将装置置于低于最高工作湿度的环境下至少 48 小时，使之适应环境，然后再将装置投入使用。
海拔	0 英尺 （海平面）至 5905 英尺 （0 至 1800 米）
冷却要求	682 BTU/小时 必须提供足够的冷却，使设备维持在其要求的工作温度范围内。否则，可能导致设备故障或损坏。
噪声	空闲时为 53 调整分贝 处理器满载时为 62 调整分贝。
工作冲击	在 5G 半正弦波冲击下无错误 （持续 11 毫秒 ）
气流	20 立方英尺 （0.57 立方米）每分钟 通过设备的气流从前面进入并从后面退出，没有单侧通风。

3D7110 和 3D7120

3D7110 和 3D7120 设备属于 71xx 子系列，是 1U 设备，随附八个铜接口或八个光纤接口，每个接口都支持可配置的旁路功能。有关 71xx 子系列设备的安全注意事项，请参阅 《*FirePOWER 与 FireSIGHT 设备监管合规性和安全性信息*》文档。

有关详细信息，请参阅以下各节：

- 3D7110 和 3D7120 机箱前视图，第 6-19 页
- 3D7110 和 3D7120 机箱后视图，第 6-23 页
- 3D7110 和 3D7120 物理和环境参数，第 6-24 页

3D7110 和 3D7120 机箱前视图

机箱前面包含 LCD面板、 USB 端口、前面板以及铜或光纤感应接口。

图 6-8 带铜接口的 3D7110 和 3D7120 （机箱：GERY-1U-8-C-AC）

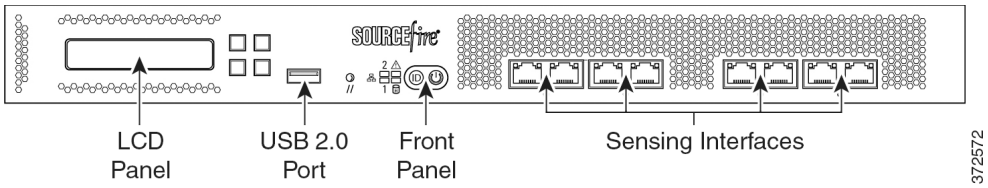
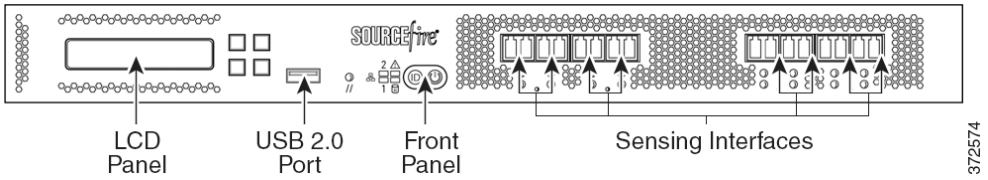


图 6-9 带光纤接口的 3D7110 和 3D7120 （机箱：GERY-1U-8-FM-AC）



下表介绍了设备前面的功能。

表 6-29 3D7110 和 3D7120 系统组件：前视图

功能	说明
LCD 面板	可以在多种模式下运行，用于配置设备、显示错误消息和查看系统状态。有关详细信息，请参阅使用 3 系列设备上的 LCD 面板，第 5-1 页。
前面板 USB 2.0 端口	可用于将键盘连接到设备。
前面板	包括显示系统的运行状态的 LED，以及电源按钮等各种控件。有关详细信息，请参阅图 6-10 3D7110 和 3D7120 前面板，第 6-19 页。
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 3D7110 和 3D7120 感应接口，第 6-21 页。

图 6-10 3D7110 和 3D7120 前面板

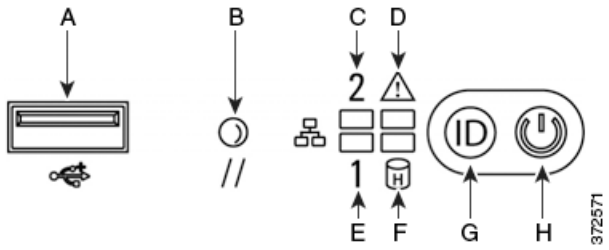


表 6-30 3D7110 和 3D7120 前面板组件

A	USB 2.0 连接器	E	NIC1 活动 LED
B	复位按钮	F	硬盘驱动器活动 LED
C	NIC2 活动 LED	G	ID 按钮
D	系统状态 LED	H	电源按钮和 LED

机箱的前面板包括显示系统的运行状态的 LED。下表介绍了前面板上的 LED。

表 6-31 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： • 闪烁的绿色指示灯指示有网络活动。 • 指示灯不亮表示没有网络活动。
系统状态	指示系统状态： • 指示灯不亮表示系统正常运行或已关机。 • 红色指示灯表示存在系统错误。 有关详细信息，请参阅表 6-32 3D7110 和 3D7120 系统状态，第 6-20 页。
复位按钮	可用于重新启动设备，而无需断开其电源。
硬盘驱动器活动	指示硬盘驱动器状态： • 闪烁的绿色指示灯表示固定磁盘驱动器处于活动状态。 • 黄色指示灯指示存在固定磁盘驱动器故障。 • 如果指示灯关闭，则无驱动器活动或系统已关闭。
系统 ID	帮助在带有其他类似系统的高密度机架中识别系统： • 蓝色指示灯指示已按 ID 按钮，并且设备背面的蓝色指示灯亮起。 • 指示灯不亮表示未按 ID 按钮。
电源按钮和 LED	指示设备是否有电： • 绿色指示灯指示设备已通电，而且系统打开。 • 闪烁的绿色指示灯表示设备有电且已经关机。 • 如果指示灯不亮，则系统未通电。

下表介绍了系统状态 LED 可能亮起的状态。

表 6-32 3D7110 和 3D7120 系统状态

状况	说明
严重	由于以下事件导致的任何严重或不可恢复的超出阈值状况： • 超出温度、电压或风扇重要阈值 • 电源子系统故障 • 由于处理器安装不正确或处理器不兼容系统无法启动 • 重要事件记录错误，包括系统内存无法纠正的 ECC 错误和毁灭性/无法纠正的总线错误，例如 PCI SERR 和 PERR

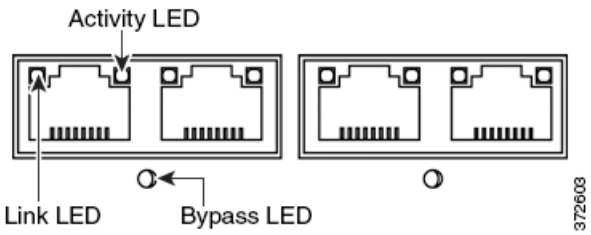
表 6-32 3D7110 和 3D7120 系统状态 （续）

状况	说明
不严重	不严重的状况指由于以下事件导致的超出阈值的状况： • 超出温度、电压或风扇的非重要阈值 • 机箱入侵 • 来自 BIOS 的 Set Fault Indication 命令；BIOS 可能将此命令用于指示系统内存或 CPU 配置更改等其他非重要状态
降级	降级状态与以下事件相关： • 故障恢复开机 (FRB) 或 BIOS 禁用了一个或多个处理器 • BIOS 禁用或映射某些系统内存 • 某个电源被拔下或不起作用 **提示** 如果发现降级状况指示，请先检查电源连接。关闭设备，断开两根电源线，重新连接电源线，重新安装它们，然后重新启动设备。 ⚠ **注意事项** 要安全关机，请使用《*FireSIGHT 系统用户指南*》中 “ 管理设备 ” 章节中的操作步骤或 CLI 的 `system shutdown` 命令。

3D7110 和 3D7120 感应接口

3D7110 和 3D7120 设备随附八端口铜接口或八端口光纤接口，每个都支持可配置的旁路功能。

图 6-11 八端口 1000BASE-T 铜接口



使用下表了解铜接口上的活动和链路 LED。

表 6-33 3D7110 和 3D7120 铜链路/活动 LED

状态	说明
两个 LED 都关闭	接口没有链路。
黄色链路	接口上流量的速度是 10 Mb 或 100 Mb。
绿色链路	接口上流量的速度是 1 Gb。
活动闪烁绿色指示灯	接口有链路而且正在传递流量。

使用下表了解铜接口上的旁路 LED。

表 6-34 3D7110 和 3D7120 铜旁路 LED

状态	说明
关闭	接口对不在旁路模式下或没有电源。
稳定绿色	接口已经准备就绪进入旁路模式。
稳定黄色	接口对已进入旁路模式并且不检查流量。
闪烁黄色	接口对处于旁路模式下；即已在出故障时自动打开。

图 6-12 八端口 1000BASE-SX 光纤可配置旁路接口

使用下表了解光纤接口上的链路和活动 LED。

表 6-35 3D7110 和 3D7120 光纤链路/活动 LED

状态	说明
顶部 （活动）	对于内联接口：接口有活动时，指示灯亮起。如果不亮，则没有活动。 对于被动接口：指示灯无法运行。
底部 （链路）	对于内联或被动接口：接口有链路时，指示灯亮起。如果不亮，则没有链路。

使用下表了解光纤接口上的活动和链路 LED。

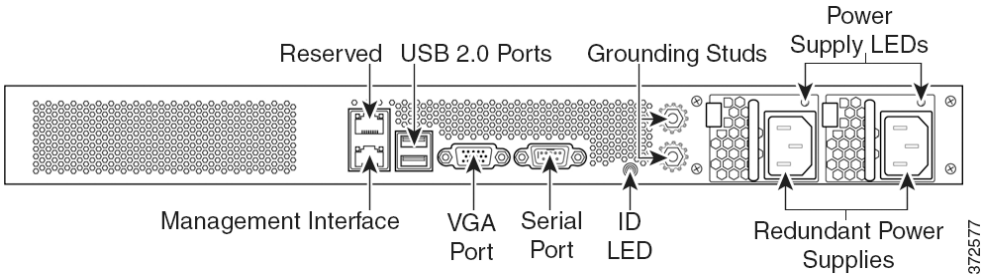
表 6-36 3D7110 和 3D7120 光纤旁路 LED

状态	说明
关闭	接口对不在旁路模式下或没有电源。
稳定绿色	接口已经准备就绪进入旁路模式。
稳定黄色	接口对已进入旁路模式并且不检查流量。
闪烁黄色	接口对处于旁路模式下；即已在出故障时自动打开。

3D7110 和 3D7120 机箱后视图

机箱后部包含管理接口、连接端口、接地螺柱和电源。

图 6-13 3D7110 和 3D7120 （机箱：GERY-1U-8-C-AC 或 GERY-1U-8-FM-AC）后视图



下表介绍了设备后面的功能。

表 6-37 3D7110 和 3D7120 系统组件：后视图

功能	说明
VGA 端口 USB 端口	可用于将显示器、键盘和鼠标连接到设备上，建立直接的工作站-设备连接。
10/100/1000 Mbps 以太网管理接口	用于带外管理网络连接。管理接口**仅限**用于维护和配置用途，不可用于传输业务流量。
系统 ID LED	帮助在带有其他类似系统的高密度机架中识别系统。蓝色指示灯指示已按 ID 按钮。
接地螺柱	可用于将设备连接到公共连接网络。有关详细信息，请参阅 FirePOWER 设备电源要求，第 A-1 页。
冗余电源	通过交流电源向设备供电。查看机箱后面， 1 号电源在左侧， 2 号电源在右侧。
电源 LED	表示电源的状态。请参阅表 6-39 3D7110 和 3D7120 电源 LED，第 6-24 页。

10/100/1000 管理接口位于设备后面。下表介绍了与管理接口相关的 LED。

表 6-38 3D7110 和 3D7120 管理接口 LED

LED	说明
左侧 （活动）	指示端口上的活动： • 指示灯闪烁表示有活动。 • 指示灯不亮表示没有活动。
右侧 （链路）	指示链路是否启用： • 指示灯亮起指示链路已启用。 • 指示灯不亮表示没有链路。

电源模块位于设备的后面。下表介绍了与电源关联的 LED。

表 6-39 3D7110 和 3D7120 电源 LED

LED	说明
关闭	没有插入电源线。
红色	未给此模块提供电源。 或 出现模块故障、保险丝熔断或风扇故障等严重的电源事件；电源关闭。
红色闪烁	出现高温或风扇转速缓慢等电源警告事件；电源继续运行。
闪烁绿色	有交流电源输入；有待机电压，电源被关闭。
绿色	电源已插入而且正常运行。

3D7110 和 3D7120 物理和环境参数

下表介绍了设备的物理属性和环境参数。

表 6-40 3D7110 和 3D7120 物理和环境参数

参数	说明
外形	1U
尺寸 （长 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）
最大 装机重量	27.5 磅 （12.5 千克）
铜 1000BASE-T	成对配置的千兆铜以太网旁路接口 电缆和距离：Cat5E 类别， 50 米距离
光纤 1000BASE-SX	有 LC 连接器的光纤旁路接口 电缆和距离：550 米 （标准）时， SX 是多模光纤 （850 纳米）
电源	450 W 双冗余 (1+1) 交流电源 电压：100 VAC 至 240 VAC 标称值 （最高 85 VAC 至 264 VAC） 电流：对于 90 VAC 至 132 VAC，每个电源最高电流 3 A 对于 187 VAC 至 264 VAC，每个电源最高电流 1.5 A 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%，无冷凝
非工作湿度	5% 至 90%，在 25°C 至 35°C （77°F 至 95°F）的温度下，最大湿球温度为 28°C （82°F）。 将装置存储在相对湿度为 95% 的无冷凝条件下。请将装置放置在低于最高工作湿度的条件下至少 48 小时，使之适应环境，然后再将装置投入使用。
海拔	0 英尺 （海平面）至 5905 英尺 （1800 米）
冷却要求	900 BTU/小时 必须提供足够的冷却，使设备维持在其要求的工作温度范围内。否则，可能导致设备故障或损坏。

表 6-40 3D7110 和 3D7120 物理和环境参数 （续）

参数	说明
噪声	处理器满载，风扇正常运行时为 64 调整分贝 符合 GR-63-CORE 4.6 噪声标准
工作冲击	符合 Bellecore GR-63-CORE 标准
气流	140 立方英尺 （3.9 立方米）每分钟 通过设备的气流从前面进入并从后面退出，没有单侧通风。

3D7115、 3D7125 和 AMP7150

3D7115、 3D7125 和 AMP7150 设备属于 71xx 子系列，随附具有可配置旁路功能的四端口铜接口和八个无旁路功能的可热插拔小型可插拔 (SFP) 端口。为确保兼容性，只能使用思科 SFP 收发器。有关71xx 子系列设备的安全注意事项，请参阅 《*FirePOWER 与 FireSIGHT 设备监管合规性和安全性信息*》文档。

注 FirePOWER AMP7150 具有和 3D7115 与 3D7125 相同的外形规格，但是进行了优化，以便利用 FireSIGHT 系统基于网络的高级恶意软件防护 (AMP) 功能。

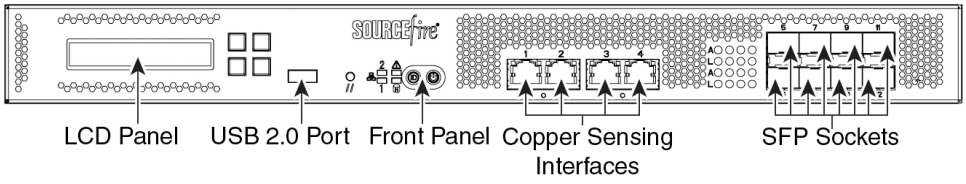
有关详细信息，请参阅以下各节：

- 3D7115、 3D7125 和 AMP7150 机箱前视图，第 6-25 页
- 3D7115、 3D7125 和 AMP7150 机箱后视图，第 6-30 页
- 3D7115、 3D7125 和 AMP7150 物理和环境参数，第 6-31 页

3D7115、 3D7125 和 AMP7150 机箱前视图

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

图 6-14 3D7115、 3D7125 和 AMP7150 （机箱：GERY-1U-8-4C8S-AC）前视图



下表介绍了设备前面的功能。

表 6-41 3D7115、 3D7125 和 AMP7150 系统组件：前视图

功能	说明
LCD 面板	可以在多种模式下运行，用于配置设备、显示错误消息和查看系统状态。有关详细信息，请参阅使用 3 系列设备上的 LCD 面板，第 5-1 页。
前面板 USB 2.0 端口	可用于将键盘连接到设备。

表 6-41 3D7115、 3D7125 和 AMP7150 系统组件：前视图 （续）

功能	说明
前面板	包括显示系统的运行状态的 LED，以及电源按钮等各种控件。有关详细信息，请参阅图 6-15 3D7115、3D7125 和 AMP7150 前面板，第 6-26 页。
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 3D7115、 3D7125 和 AMP7150 感应接口，第 6-28 页。

图 6-15 3D7115、 3D7125 和 AMP7150 前面板

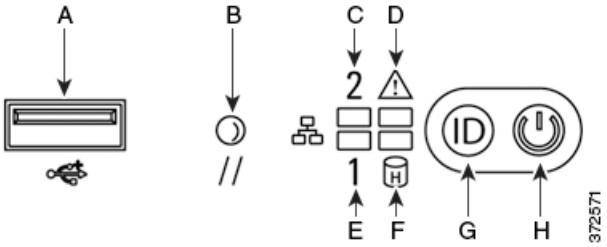


表 6-42 3D7115、 3D7125 和 AMP7150 前面板组件

A	USB 2.0 连接器	E	NIC1 活动 LED
B	复位按钮	F	硬盘驱动器活动 LED
C	NIC2 活动 LED	G	ID 按钮
D	系统状态 LED	H	电源按钮和 LED

机箱的前面板包括显示系统的运行状态的 LED。下表介绍了前面板上的 LED。

表 6-43 3D7115、 3D7125 和 AMP7150 前面板 LED

LED	说明
NIC 活动 （1 和 2）	指示是否有任何网络活动： • 闪烁的绿色指示灯表示有网络活动。 • 指示灯不亮表示没有网络活动。
系统状态	指示系统状态： • 指示灯不亮表示系统正常运行或已关机。 • 红色指示灯表示存在系统错误。 有关详细信息，请参阅表 6-44 3D7115、 3D7125 和 AMP7150 系统状态，第 6-27 页。
复位按钮	可用于重新启动设备，而无需断开其电源。
硬盘驱动器活动	指示硬盘驱动器状态： • 闪烁的绿色指示灯表示固定磁盘驱动器处于活动状态。 • 黄色指示灯表示存在固定磁盘驱动器故障。 • 如果指示灯关闭，则无驱动器活动或系统已关闭。

表 6-43 3D7115、3D7125 和 AMP7150 前面板 LED （续）

LED	说明
系统 ID	帮助在带有其他类似系统的高密度机架中识别系统： • 蓝色指示灯表示已按 ID 按钮，并且设备背面的蓝色指示灯亮起。 • 指示灯不亮表示未按 ID 按钮。
电源按钮和 LED	指示设备是否有电： • 绿色指示灯指示设备已通电，而且系统打开。 • 闪烁的绿色指示灯表示设备有电且已经关机。 • 指示灯不亮表示系统未通电。

下表介绍了系统状态 LED 可能亮起的状态。

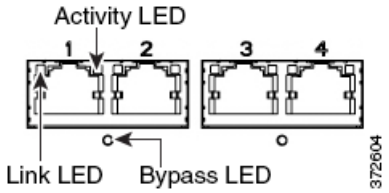
表 6-44 3D7115、3D7125 和 AMP7150 系统状态

状况	说明
严重	由于以下事件导致的任何严重或不可恢复的超出阈值状况： • 超出温度、电压或风扇重要阈值 • 电源子系统故障 • 由于处理器安装不正确或处理器不兼容系统无法启动 • 重要事件记录错误，包括系统内存无法纠正的 ECC 错误和毁灭性/无法纠正的总线错误，例如 PCI SERR 和 PERR
不严重	不严重的状况指由于以下事件导致的超出阈值的状况： • 超出温度、电压或风扇的非重要阈值 • 机箱入侵 • 来自 BIOS 的 Set Fault Indication 命令；BIOS 可能将此命令用于指示系统内存或 CPU 配置更改等其他非重要状态
降级	降级状态与以下事件相关： • 故障恢复开机 (FRB) 或 BIOS 禁用了一个或多个处理器 • BIOS 禁用或映射某些系统内存 • 某个电源被拔下或不起作用 **提示** 如果发现降级状况指示，请先检查电源连接。关闭设备，断开两根电源线，重新连接电源线，重新安装它们，然后重新启动设备。 ⚠ **注意事项** 要安全关机，请使用 《*FireSIGHT 系统用户指南*》中 “ 管理设备 ” 章节中的操作步骤或 CLI 的 `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。

图 6-16 四个 1000BASE-T 铜接口



使用下表了解铜接口上的链路和活动 LED。

表 6-45 3D7115、 3D7125 和 AMP7150 铜链路/活动 LED

状态	说明
两个 LED 都关闭	接口没有链路。
黄色链路	接口上流量的速度是 10 Mb 或 100 Mb。
绿色链路	接口上流量的速度是 1 Gb。
活动闪烁绿色指示灯	接口有链路而且正在传输流量。

使用下表了解铜接口上的旁路 LED。

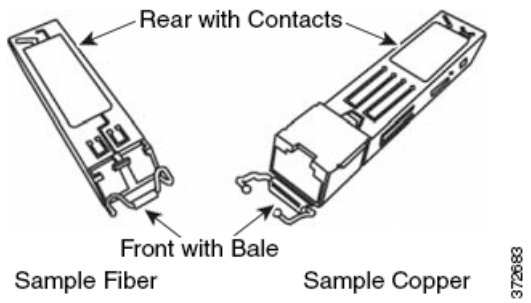
表 6-46 3D7115、 3D7125 和 AMP7150 铜旁路 LED

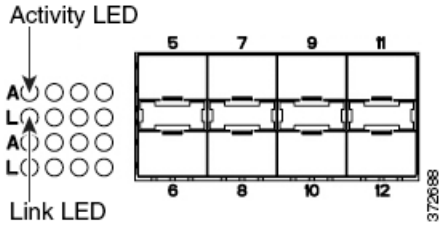
状态	说明
关闭	接口对不在旁路模式下或没有电源。
稳定绿色	接口已经准备就绪进入旁路模式。
稳定黄色	接口对已进入旁路模式并且不检查流量。
闪烁黄色	接口对处于旁路模式下；即已在出故障时自动打开。

SFP 接口

最多可以安装八个热插拔思科 SFP 收发器，提供 1G 铜、 1G 短距离光纤或 1G 远距离光纤规格。SFP 收发器没有旁路功能，不能用于入侵防御部署中。有关详细信息，请参阅在 3D71x5 和 AMP7150 设备中使用 SFP 收发器，第 B-1 页。

图 6-17 SFP 收发器示例





使用下表了解光纤 LED。

表 6-47　　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：接口有活动时，指示灯亮起。如果不亮，则没有活动。 对于被动接口：指示灯无法运行。
底部 （链路）	对于内联或被动接口：接口有链路时，指示灯亮起。如果不亮，则没有链路。

使用下表了解 SFP 光纤收发器的规格。

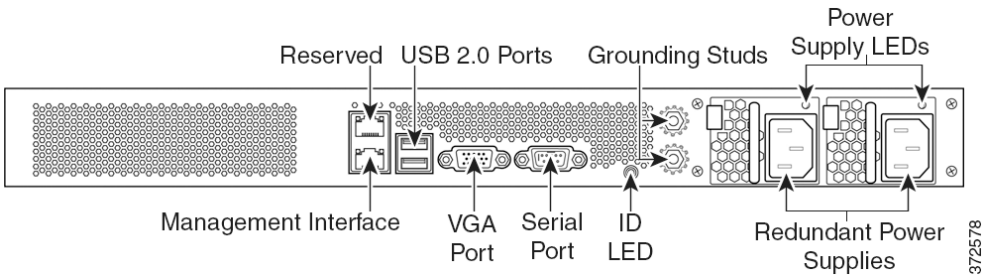
表 6-48　　3D7115、3D7125 和 AMP7150 SFP 光纤参数

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
运行距离	200 米 （656 英尺）， 62.5 微米/125 微米光纤 500 米 （1640 英尺）， 50 微米/125 微米光纤	10 公里 （6.2 英里）， 9 微米/125 微米光纤
发射器波长	770-860 纳米 （850 纳米典型值）	1270-1355 纳米 （1310 纳米典型值）
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
接收器的最大平均功率	0 dBm	-3 dBm
接收器灵敏度	-17 dBm	-19 dBm

3D7115、 3D7125 和 AMP7150 机箱后视图

机箱后部包含管理接口、连接端口、接地螺柱和电源。

图 6-18 3D7115、 3D7125 和 AMP7150 （机箱：GERY-1U-8-4C8S-AC）后视图



下表介绍了设备后面的功能。

表 6-49 3D7115、 3D7125 和 AMP7150 系统组件：后视图

功能	说明
VGA 端口 USB 端口	可用于将显示器、键盘和鼠标连接到设备上，建立直接的工作站-设备连接。
10/100/1000 Mbps 以太网管理接口	用于带外管理网络连接。管理接口**仅限**用于维护和配置用途，不可用于传输业务流量。
系统 ID LED	帮助在带有其他类似系统的高密度机架中识别系统。蓝色指示灯指示已按 ID 按钮。
接地螺柱	可用于将设备连接到公共连接网络。有关详细信息，请参阅 FirePOWER 设备电源要求，第 A-1 页。
冗余电源	通过交流电源向设备供电。查看机箱后面， 1 号电源在左侧， 2 号电源在右侧。
电源 LED	表示电源的状态。请参阅表 6-51 3D7115、3D7125 和 AMP7150 电源 LED，第 6-31 页。

10/100/1000 管理接口位于设备后面。下表介绍了与管理接口相关的 LED。

表 6-50 3D7115、 3D7125 和 AMP7150 管理接口 LED

LED	说明
左侧 （活动）	指示端口上的活动： • 指示灯闪烁表示有活动。 • 指示灯不亮表示没有活动。
右侧 （链路）	指示链路是否启用： • 指示灯亮起表示链路已启用。 • 指示灯不亮表示没有链路。

电源模块位于设备的后面。下表介绍了与电源关联的 LED。

表 6-51 3D7115、 3D7125 和 AMP7150 电源 LED

LED	说明
关闭	没有插入电源线。
红色	未给此模块提供电源。 或 出现模块故障、保险丝熔断或风扇故障等严重的电源事件；电源关闭。
闪烁红色	出现高温或风扇转速缓慢等电源警告事件；电源继续运行。
闪烁绿色	有交流电源输入；有待机电压，电源被关闭。
绿色	电源已插入而且正常运行。

3D7115、 3D7125 和 AMP7150 物理和环境参数

下表介绍了设备的物理属性和环境参数。

表 6-52 3D7115、 3D7125 和 AMP7150 物理和环境参数

参数	说明
外形	1U
尺寸 （长 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）
最大 装机重量	29.0 磅 （13.2 千克）
铜 1000BASE-T	成对配置的千兆铜以太网旁路接口 电缆和距离：Cat5E 类别， 50 米距离
铜 1000BASE-T SFP	成对配置的千兆铜以太网非旁路接口 电缆和距离：Cat5E 类别， 50 米距离
光纤 1000BASE-SX SFP	有 LC 连接器的光纤非旁路接口 电缆和距离：550 米 （标准）时， SX 是多模光纤 （850 纳米） 200 米 （656 英尺）， 62.5 微米/125 微米光纤 500 米 （1640 英尺）， 50 微米/125 微米光纤
光纤 1000BASE-LX SFP	有 LC 连接器的光纤非旁路接口 电缆和距离：LX 是单模光纤 （1310 纳米）， 10 千米 9 微米/125 微米光纤 （标准）
电源	450 W 双冗余 (1+1) 交流电源 电压：100 VAC 至 240 VAC 标称值 （最高 85 VAC 至 264 VAC） 电流：对于 90 VAC 至 132 VAC，每个电源最高电流 3 A 对于 187 VAC 至 264 VAC，每个电源最高电流 1.5 A 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%，无冷凝

表 6-52 3D7115、3D7125 和 AMP7150 物理和环境参数 （续）

参数	说明
非工作湿度	5% 至 90%，在 25°C 至 35°C （77°F 至 95°F）的温度下，最大湿球温度为 28°C （82°F）。 将装置存储在相对湿度为 95% 的无冷凝条件下。请将装置置于低于最高工作湿度的条件下至少 48 小时，使之适应环境，然后再将装置投入使用。
海拔	0 英尺 （海平面）至 5905 英尺 （1800 米）
冷却要求	900 BTU/小时 必须提供足够的冷却，使设备维持在其要求的工作温度范围内。否则，可能导致设备故障或损坏。
噪声	处理器满载，风扇正常运行时为 64 调整分贝 符合 GR-63-CORE 4.6 噪声标准
工作冲击	符合 Bellecore GR-63-CORE 标准
气流	140 立方英尺 （3.9 立方米）每分钟 通过设备的气流从前面进入并从后面排出，没有单侧通风。

8000 系列设备

8000 系列设备使用包含铜或光纤感应接口的网络模块 (NetMod)。设备可能在发货时已完全装配好，也可能要自行安装模块。请先组装设备，再安装 FireSIGHT 系统。请参阅模块随附的组装说明。

有些 8000 系列设备可以堆叠以提高系统的性能。对于每个堆叠的套件，用堆叠模块替换网络模块并使用 8000 系列堆叠电缆连接设备。有关详细信息，请参阅在堆叠配置中使用设备，第 3-13 页。

8000 系列设备可提供多种机箱：

- 3D8120、3D8130、3D8140 和 AMP8150，又叫做 81xx 子系列，是 1U 机箱，最多可以包含三个模块。仅限 3D8140，可以添加总计 2U 配置的堆叠套件。

  注 FirePOWER AMP8150 具有和 3D8130 相同的外形规格，但是进行了优化，以便利用 FireSIGHT 系统基于网络的高级恶意软件防护 (AMP) 功能。

- 3D8250 属于 82xx 子系列，是 2U 机箱，最多可以包含七个模块。总计 8U 的配置最多可以添加三个堆叠式套件。
- 3D8260 属于 82xx 子系列，是 4U 配置，带两个 2U 机箱。主要机箱包含一个堆叠模块和最多六个检测模块。辅助机箱包含一个堆叠模块。总计 8U 的配置最多可以添加两个堆叠式套件。
- 3D8270 属于 82xx 子系列，是 6U 配置，带三个 2U 机箱。主要机箱包含两个堆叠模块和最多五个检测模块。每个辅助机箱包含一个堆叠模块。总计 8U 的配置可以添加一个堆叠套件。
- 3D8290 属于 82xx 子系列，是 8U 配置，带四个 2U 机箱。主要机箱包含三个堆叠模块和最多四个检测模块。每个辅助机箱包含一个堆叠模块。此模式未完全配置并且不接受堆叠套件。
- 3D8350 属于 83xx 子系列，是 2U 机箱，最多可以包含七个模块。总计 8U 的配置最多可以添加三个堆叠式套件。
- 3D8360 属于 83xx 子系列，是 4U 配置，带两个 2U 机箱。主要机箱包含一个堆叠模块和最多六个检测模块。辅助机箱包含一个堆叠模块。总计 8U 的配置最多可以添加两个堆叠式套件。

- 3D8370 属于 83xx 子系列，是 6U 配置，带三个 2U 机箱。主要机箱包含两个堆叠模块和最多五个检测模块。每个辅助机箱包含一个堆叠模块。总计 8U 的配置可以添加一个堆叠套件。
- 3D8390 属于 83xx 子系列，是 8U 配置，带四个 2U 机箱。主要机箱包含三个堆叠模块和最多四个检测模块。每个辅助机箱包含一个堆叠模块。此模式未完全配置并且不接受堆叠套件。

有关详细信息，请参阅以下各节：

- 8000 系列机箱前视图，第 6-33 页
- 8000 系列机箱后视图，第 6-36 页
- 8000 系列物理和环境参数，第 6-38 页
- 8000 系列模块，第 6-42 页

8000 系列机箱前视图

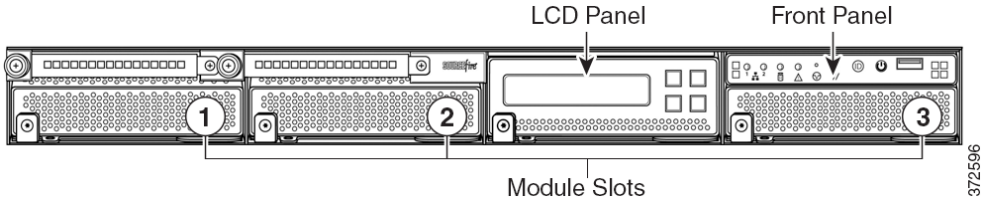
8000 系列机箱可以放在 81xx 子系列、 82xx 子系列或者 83xx 子系列中。

有关 81xx 子系列、 82xx 子系列和 83xx 子系列设备的安全注意事项，请参阅 《*FirePOWER 与 FireSIGHT 设备监管合规性和安全性信息*》文档。

81xx 子系列机箱前视图

机箱的前视图包含 LCD 面板、前面板和三个模块插槽。

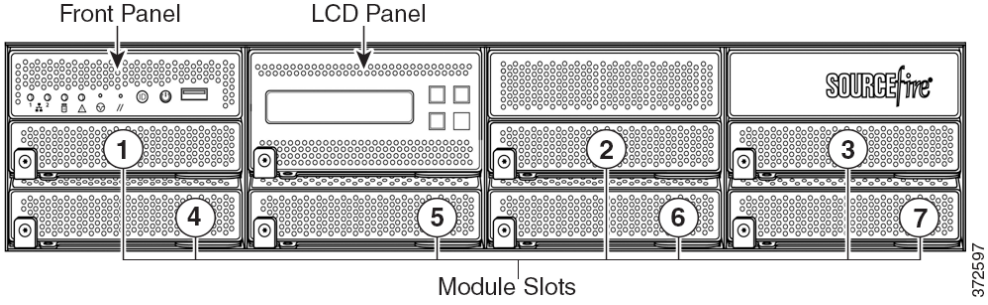
图 6-19　　81xx 子系列（机箱：CHAS-1U-AC/DC）前视图



82xx 子系列和 83xx 子系列机箱前视图

机箱的前视图包含 LCD 面板、前面板和七个模块插槽。

图 6-20　　82xx 子系列（机箱：CHAS-2U-AC/DC）和 83xx 子系列 (PG35-2U-AC/DC) 前视图



下表介绍了设备前面的功能。

表 6-53 8000 系列系统组件：前视图

功能	说明
模块插槽	包含模块。有关可用模块的信息，请参阅 8000 系列模块，第 6-42 页。
LCD 面板	可以在多种模式下运行，用于配置设备、显示错误消息和查看系统状态。有关详细信息，请参阅使用 3 系列设备上的 LCD 面板，第 5-1 页。
前面板控件	包括显示系统的运行状态的 LED，以及电源按钮等各种控件。有关详细信息，请参阅图 6-22 82xx 子系列和 83xx 子系列前面板，第 6-34 页。
前面板 USB 端口	USB 2.0 端口可用于将键盘连接到设备上。

有关详细信息，请参阅以下各节：

- 8000 系列前面板，第 6-34 页
- 8000 系列机箱后视图，第 6-36 页

8000 系列前面板

81xx 子系列、 82xx 子系列和 83xx 子系列的前面板包含相同的组件。

图 6-21 81xx 子系列前面板

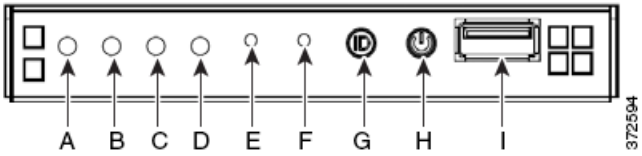


图 6-22 82xx 子系列和 83xx 子系列前面板

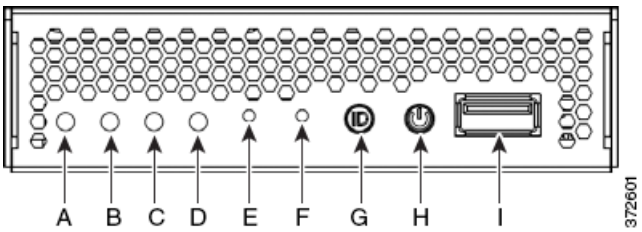


表 6-54 8000 系列前面板组件

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		

机箱的前面板包括显示系统的运行状态的 LED。下表介绍了前面板上的 LED

表 6-55 8000 系列前面板 LED

LED	说明
NIC 活动	指示是否有任何网络活动： • 绿色表示有网络活动。 • 如果指示灯不亮，则表示没有网络活动。
硬盘驱动器活动	指示硬盘驱动器状态： • 闪烁的绿色指示灯表示固定磁盘驱动器处于活动状态。 • 黄色表示存在固定磁盘驱动器故障。 • 如果指示灯关闭，则无驱动器活动或系统已关闭。
系统状态	指示系统状态： • 绿色表示系统正常运行。 • 闪烁绿色表示系统处于降级运行状态。 • 闪烁黄色表示系统处于非重要状态。 • 黄色表示系统处于重要或不可恢复的状态，或者系统正在启动。 • 如果指示灯不亮，则系统正在启动或已经关闭。 **注** 黄色状态指示灯优先于绿色状态指示灯。当黄色指示灯亮起或闪烁时绿色指示灯关闭。 有关详细信息，请参阅第 6-35 页上的表 6-56。
系统 ID	帮助在带有其他类似系统的高密度机架中识别系统： • 蓝色指示灯表示已按 ID 按钮，并且设备背面的蓝色指示灯亮起。 • 指示灯不亮表示未按 ID 按钮。
电源按钮和 LED	指示系统是否有电： • 绿色表明系统有电。 • 如果指示灯不亮，则系统未通电。

下表介绍了系统状态 LED 可能亮起的状态。

表 6-56 8000 系列系统状态

状况	说明
严重	由于以下事件导致的任何严重或不可恢复的超出阈值状况： • 超出温度、电压或风扇重要阈值 • 电源子系统故障 • 由于处理器安装不正确或处理器不兼容系统无法启动 • 重要事件记录错误，包括系统内存无法纠正的 ECC 错误和毁灭性/无法纠正的总线错误，例如 PCI SERR 和 PERR

表 6-56 8000 系列系统状态 （续）

状况	说明
不严重	不严重的状况指由于以下事件导致的超出阈值的状况： • 超出温度、电压或风扇的非重要阈值 • 机箱入侵 • 来自 BIOS 的 Set Fault Indication 命令；BIOS 可能将此命令用于指示系统内存或 CPU 配置更改等其他非重要状态
降级	降级状况与以下事件相关： • 故障恢复开机 (FRB) 或 BIOS 禁用了一个或多个处理器 • BIOS 禁用或映射某些系统内存 • 某个电源被拔下或不起作用 **提示** 如果发现降级状况指示，请先检查电源连接。关闭设备，断开两根电源线，重新连接电源线，重新安装它们，然后重新启动设备。 ⚠ **注意事项** 要安全关机，请使用 《*FireSIGHT 系统用户指南*》中 “ 管理设备 ” 章节中的操作步骤或 CLI 的 `system shutdown` 命令。

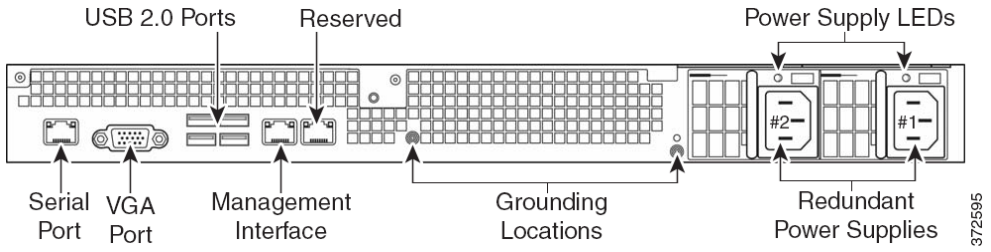
8000 系列机箱后视图

8000 系列机箱可以放在 81xx 子系列、 82xx 子系列或者 83xx 子系列。

81xx 子系列机箱后视图

机箱后视图包含连接端口、管理接口和电源。

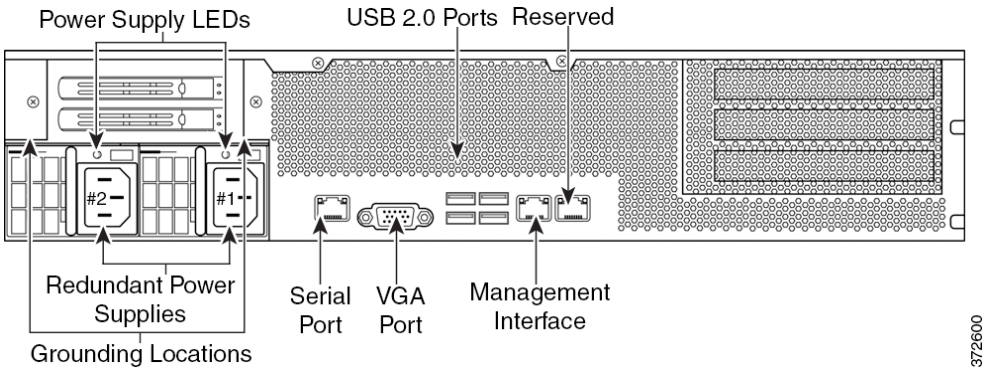
图 6-23 81xx 子系列 （机箱：CHAS-1U-AC/DC）后视图



82xx 子系列机箱后视图

机箱后视图包含电源、连接端口和管理接口。

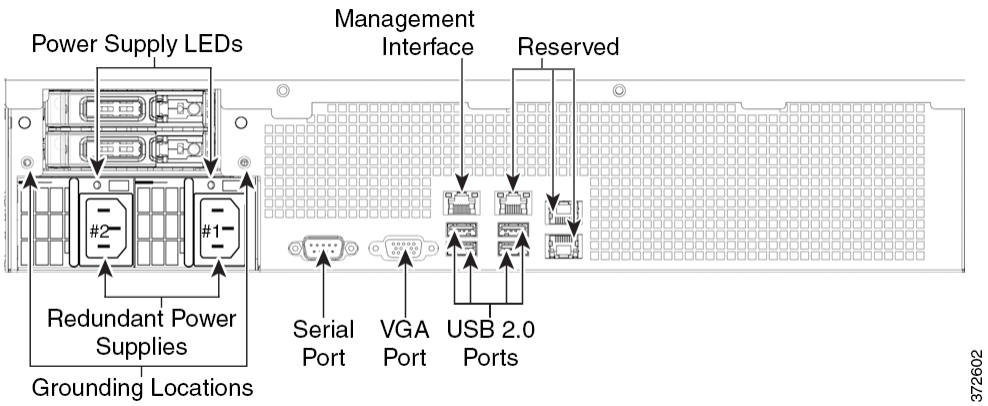
图 6-24 82xx 子系列（机箱：CHAS-2U-AC/DC）后视图



83xx 子系列机箱后视图

机箱后视图包含电源、连接端口和管理接口。

图 6-25 83xx 子系列（机箱：PG35-2U-AC/DC）后视图



下表介绍了设备后面的功能。

表 6-57 8000 系列系统组件：后视图

功能	说明
VGA 端口 USB 2.0 端口	可用于将显示器、键盘和鼠标连接到设备上，以代替使用串行端口，建立直接的工作站-设备连接。
RJ45 串行端口 (81xx 子系列和 82xx 子系列)	可用于建立直接访问设备上所有管理设备的工作站-设备直接连接（使用 RJ45 转 DB-9 适配器）。 RJ45 串行端口**仅限**用于维护和配置用途，不可用于传输业务流量。
RS232 串行端口 （83xx 子系列）	可用于建立直接的工作站-设备连接，用以直接访问设备上的所有管理服务。 RJ232 串行端口**仅限**用于维护和配置用途，不可用于传输业务流量。
10/100/1000 Mbps 以太网管理接口	用于带外管理网络连接。管理接口**仅限**用于维护和配置用途，不可用于传输业务流量。

表 6-57 8000 系列系统组件：后视图 （续）

功能	说明
冗余电源	通过交流电源向设备供电。查看机箱后面， 1 号电源在右侧， 2 号电源在左侧。
接地位置	可用于将设备连接到公共连接网络。有关详细信息，请参阅 FirePOWER 设备电源要求，第 A-1 页。

10/100/1000 管理接口位于设备后面。下表介绍了与管理接口相关的 LED。

表 6-58 8000 系列管理接口 LED

LED	说明
左侧 （活动）	指示端口上的活动： • 指示灯闪烁表示有活动。 • 指示灯不亮表示没有活动。
右侧 （链路）	指示链路是否启用： • 指示灯亮起表示链路已启用。 • 指示灯不亮表示没有链路。

电源模块位于设备的后面。下表介绍了与管理接口相关的 LED。

表 6-59 8000 系列电源 LED

LED	说明
关闭	没有接通电源。
黄色	未给此模块提供电源。 或 出现模块故障、保险丝熔断或风扇故障等严重的电源事件；电源关闭。
闪烁黄色	出现高温或风扇转速缓慢等电源警告事件；电源继续运行。
闪烁绿色	有交流电源输入；有待机电压，电源被关闭。
绿色	电源已插入而且正常运行。

8000 系列物理和环境参数

下表介绍了 81xx 子系列设备的物理属性和环境参数。

表 6-60 81xx 子系列物理和环境参数

参数	说明
外形	1U
尺寸 （长 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）

表 6-60 81xx 子系列物理和环境参数 （续）

参数	说明
最大 装机重量	43.5 磅 （19.8 千克）
铜 1000BASE-T 可配置旁路网络模块	成对配置的四端口千兆铜以太网可配置旁路接口 电缆和距离：Cat5E 类别， 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 电缆和距离： LR 是单模，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 电缆和距离：550 米 （标准）时， SX 是多模光纤 （850 纳米）
铜 1000BASE-T 非旁路网络模块	成对配置的四端口千兆铜以太网非旁路接口 电缆和距离：Cat5E 类别， 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 电缆和距离： LR 是单模，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 电缆和距离：550 米 （标准）时， SX 是多模光纤 （850 纳米）
电源	用于交流电或直流电的 650 瓦双冗余电源。 交流电压：100 VAC 至 240 VAC 标称值 （最高 85 VAC 至 264 VAC） 交流电流：整个范围内，每个电源最高电流 5.2 A 对于 187 VAC 至 264 VAC，每个电源最高电流 2.6 A 交流电频率范围：47 Hz 至 63 Hz 直流电压：-48 VDC 标称值，以 RTN 为参考 最高 -40 VDC 至 -72 VDC 直流电 直流电流：最高每个电源 11 A
工作温度	10°C 至 35°C （50°F 至 95°F）
非工作温度	-20°C 至 70°C （-29°F 至 158°F）
工作湿度	5% 至 85%，无冷凝
非工作湿度	5% 至 90%，在 25°C 至 35°C （77°F 至 95°F）的温度下，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 必须提供足够的冷却，使设备维持在其要求的工作温度范围内。否则，可能导致设备故障或损坏。
噪声	最大正常运行噪声是 87.6 分贝声功率标示值 （高温） 典型的正常运行噪声是 80 分贝声功率标示值。
工作冲击	在 2G 半正弦波冲击下无错误 （持续 11 毫秒 ）

表 6-60 81xx 子系列物理和环境参数 （续）

参数	说明
气流	160 立方英尺 （4.5 立方米）每分钟 诸如堵塞装置前部或后部，或将其封装在机柜中而不提供充分的空隙等限制气流的情况会导致装置过热，即使环境温度在工作温度范围内也会如此。 通过设备的气流从前面进入并从后面排出。正面和背面的最小建议空隙为 7.9 英寸 （20 厘米）。只有在可以确保在设备前面提供低温气流的情况下，方可采用此最小值。

下表介绍了 82xx 子系列和 83xx 子系列设备的物理属性和环境参数。

表 6-61 82xx 子系列和 83xx 子系列物理和环境参数

参数	说明	
外形	2U	
尺寸 （长 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）	
最大装机重量	82xx 子系列：	58 磅 （25.3 千克）
	83xx 子系列：	67 磅 （30.5 千克）
铜 1000BASE-T 可配置旁路网络模块	成对配置的四端口千兆铜以太网可配置旁路接口 电缆和距离：Cat5E 类别， 50 米距离	
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 电缆和距离： LR 是单模，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 电缆和距离：550 米 （标准）时， SX 是多模光纤 （850 纳米）	
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 电缆和距离： OM3：在 850 纳米多模下为 100 米 OM4：在 850 纳米多模下为 150 米	
铜 1000BASE-T 非旁路网络模块	成对配置的四端口千兆铜以太网非旁路接口 电缆和距离：Cat5E 类别， 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 电缆和距离： LR 是单模，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 电缆和距离： SX 是多模光纤 （850 纳米），距离为 550 米 （标准）	

表 6-61 82xx 子系列和 83xx 子系列物理和环境参数 （续）

参数	说明	
电源	82xx 子系列：	用于交流电或直流电的 750 W 双冗余电源。 交流电压：100 VAC 至 240 VAC 标称值 （最高 85 VAC 至 264 VAC） 交流电流：整个范围内，每个电源最高电流 8 A 对于 187 VAC 至 264 VAC，每个电源最高电流 4 A 交流电频率范围：47 Hz 至 63 Hz 直流电压：-48 VAC 标称值，以 RTN 为参考 最高 -40 VAC 至 -72 VAC 直流电流：最高每个电源 18 A
	83xx 子系列：	用于交流电或直流电的 1000 W 双冗余电源。 交流电压：100 VAC 至 240 VAC 标称值 （最高 85 VAC 至 264 VAC） 交流电流：整个范围内，每个电源最高电流 11 A 对于 187 VAC 至 264 VAC，每个电源最高电流 5.5 A 交流电频率范围：47 Hz 至 63 Hz 直流电压：-48 VDC，以 RTN 为参考 最高 -40 VDC 至 -72 VDC 直流电流：最高每个电源 25 A
工作温度	82xx 子系列：10°C 至 35°C （50°F 至 95°F）	
	83xx 子系列：	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%，无冷凝	
非工作湿度	5% 至 90%，在 25°C 至 35°C （77°F 至 95°F）的温度下，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 必须提供足够的冷却，使设备维持在其要求的工作温度范围内。否则，可能导致设备故障或损坏。	
噪声	最大正常运行噪声是 81.6 分贝声功率标示值 （高温） 典型的正常运行噪声是 81.4 分贝声功率标示值。	
工作冲击	在 2G 半正弦波冲击下无错误 （持续 11 毫秒 ）	
气流	自前而后， 210 立方英尺 （6 立方米）每分钟 诸如堵塞装置前部或后部，或将其封装在机柜中而不提供充分的空隙等限制气流的情况会导致装置过热，即使环境温度在工作温度范围内也会如此。 通过设备的气流从前面进入并从后面排出。建议正面和背面的最小空隙为 7.9 英寸 （20 厘米）。只有在可以确保在设备前面提供低温气流的情况下，方可采用此最小值。	

8000 系列模块

8000 系列的感应接口可以提供铜或光纤接口。

注意事项 这些模块**不可**热插拔。有关详细信息，请参阅插入和拆卸 8000 系列模块，第 C-1 页。

以下模块包含可配置旁路感应接口：

- 四端口 1000BASE-T 铜接口，带可配置旁路功能。请参阅四端口 1000BASE-T 铜可配置旁路网络模块，第 6-42 页。
- 四端口 1000BASE-SX 光纤接口，带可配置旁路功能。有关详细信息，请参阅四端口 1000BASE-SX 光纤可配置旁路网络模块，第 6-43 页。
- 一个双端口 10GBASE （MMSR 或 SMLR）光纤接口，带可配置旁路功能。有关详细信息，请参阅双端口 10GBASE （MMSR 或 SMLR）光纤可配置旁路网络模块，第 6-44 页。
- 一个双端口 40GBASE-SR4 光纤接口，带可配置旁路功能 （仅限 2U 设备）。有关详细信息，请参阅双端口 40GBASE-SR4 光纤可配置旁路网络模块，第 6-46 页。

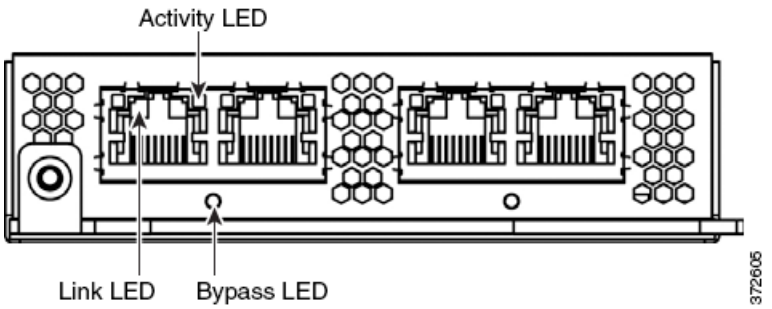
以下模块包含非旁路感应接口：

- 四端口 1000BASE-T 铜接口，无旁路功能。有关详细信息，请参阅四端口 1000BASE-T 铜可配置旁路网络模块，第 6-47 页。
- 不具有旁路功能的四端口 1000BASE-SX 光纤接口。有关详细信息，请参阅四端口 1000BASE-SX 光纤可配置旁路网络模块，第 6-48 页。
- 四端口 10GBASE （MMSR 或 SMLR）光纤接口，无旁路功能。有关详细信息，请参阅四端口 10GBASE （MMSR 或 SMLR）光纤非旁路网络模块，第 6-49 页。

此外，还可以使用堆叠模块连接两个 3D8140、最多四个 3D8250 或最多四个 3D8350 设备，组合其处理能力和提高吞吐量。有关详细信息，请参阅堆叠模块，第 6-50 页。

四端口 1000BASE-T 铜可配置旁路网络模块

四端口 1000BASE-T 铜可配置旁路网络模块包含铜端口和链路、活动与旁路 LED。



使用下表了解铜接口上的链路和活动 LED。

表 6-62 铜链路/活动 LED

状态	说明
两个 LED 都关闭	接口没有链路并且不在旁路模式下。
黄色链路	接口上流量的速度是 10 Mb 或 100 Mb。

表 6-62 铜链路/活动 LED （续）

状态	说明
绿色链路	接口上流量的速度是 1 Gb。
活动闪烁绿色指示灯	接口有链路而且正在传输流量。

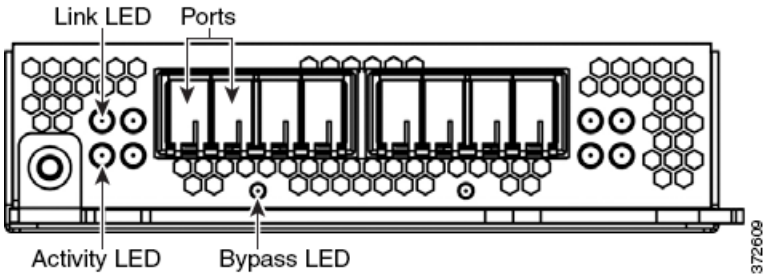
使用下表了解铜接口上的旁路 LED。

表 6-63 铜旁路 LED

状态	说明
关闭	接口没有链路并且不在旁路模式下。
稳定绿色	接口有链路而且正在传输流量。
稳定黄色	接口已被故意关闭。
闪烁黄色	接口处于旁路模式下；即已在出故障时自动打开。

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和链路、活动与旁路 LED。



使用下表了解光纤接口上的链路和活动 LED。

表 6-64 光纤链路/活动 LED

状态	说明
顶部	对于内联或被动接口： • 指示灯闪烁表示接口有活动。 • 指示灯不亮表示没有活动。
底部	对于内联接口： • 指示灯亮起表示接口有活动。 • 指示灯不亮表示没有活动。 对于被动接口：指示灯始终亮着。

使用下表了解光纤接口上的旁路 LED。

表 6-65 光纤旁路 LED

状态	说明
关闭	接口没有链路并且不在旁路模式下。
稳定绿色	接口有链路而且正在传输流量。
稳定黄色	接口已被故意关闭。
闪烁黄色	接口处于旁路模式下；即已在出故障时自动打开。

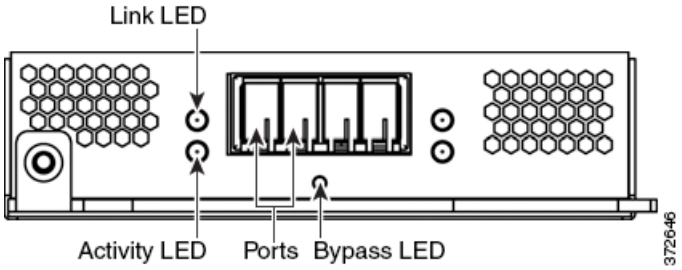
使用下表了解光纤接口的光纤维规格。

表 6-66 1000BASE-SX 网络模块光纤参数

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
运行距离	200 米 （656 英尺）， 62.5 微米/125 微米光纤 500 米 （1640 英尺）， 50 微米/125 微米光纤
发射器波长	770 - 860 纳米 （850 纳米典型值）
最大平均发射功率	0 dBm
最小平均发射功率	-9.5 dBm
接收器的最大平均功率	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

双端口和 10GBASE （MMSR 或 SMLR）光纤可配置旁路网络模块包含两个光纤端口和链路、活动与旁路 LED。



使用下表了解光纤接口上的链路和活动 LED。

表 6-67 光纤链路/活动 LED

状态	说明
顶部	对于内联或被动接口： • 指示灯闪烁表示接口有活动。 • 指示灯不亮表示没有活动。
底部	对于内联接口： • 指示灯亮起表示接口有活动。 • 指示灯不亮表示没有活动。 对于被动接口：指示灯始终亮着。

使用下表了解光纤接口上的旁路 LED。

表 6-68 光纤旁路 LED

状态	说明
关闭	接口没有链路并且不在旁路模式下。
稳定绿色	接口有链路而且正在传输流量。
稳定黄色	接口已被故意关闭。
闪烁黄色	接口处于旁路模式下；即已在出故障时自动打开。

使用下表了解光纤接口的光纤参数。

表 6-69 10GBASE MMSR 和 SMLR 网络模块光纤参数

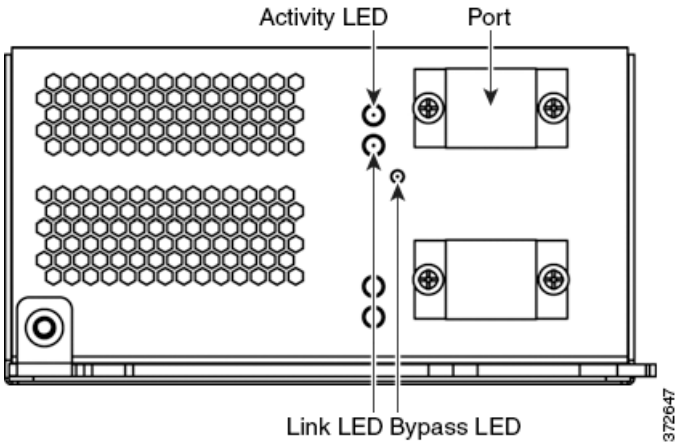
参数	10GBASE MMSR	10GBASE SMLR
光纤连接器	LC 双工：	LC 双工：
比特率	10.000 Gbps	10.000 Gbps
波特率/ 编码/ 容限	10.3125 Gbps/ 64/66b 编码/ +/-100 ppm	10.3125 Gbps/ 64/166b 编码/ +/-100 ppm
光纤接口：	多模	仅单模
工作距离	840 - 860 纳米 （850 纳米典型值） 26 米 （85 英尺）至 33 米 （108 英尺）， 62.5 微米/125 微米光纤 （模态带宽分别为 160 至 200） 66 米 （216 英尺）至 82 米 （269 英尺）， 50 微米/125 微米光纤 （模态带宽分别为 400 至 500） 高质量 (OM3) 光纤可提供 300 米（980 英尺）以内工作距离。 最短距离 （全部）：2 米 （6 英尺）	1270 - 1355 纳米 （1310 纳米典型值） 2 米至 10 千米（6 英尺至 6.2 英里），9 微米/125 微米光纤

表 6-69 10GBASE MMSR 和 SMLR 网络模块光纤参数 （续）

参数	10GBASE MMSR	10GBASE SMLR
发射器波长	840 - 860 纳米 （850 纳米典型值）	1270 - 1355 纳米 （1310 纳米典型值）
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
接收器的最大平均功率	-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和链路、活动与旁路 LED。



在 3D8270、3D8290、3D8360、3D8370 和 3D8390 中；或在支持 40G 功能的 3D8250、3D8260 和 3D8350 中，只能使用 40G 网络模块。如果您尝试在不具有 40G 功能的设备上创建 40G 接口，管理防御中心的网络界面上的 40G 接口屏幕将会呈红色显示。支持 40G 功能的 3D8250 在 LCD 面板上显示“3D 8250-40G”，支持 40G 功能的 3D8350 显示在 LCD 面板上显示“3D 8350-40G”。有关位置信息，请参阅 8000 系列模块，第 3-9 页。

使用下表了解光纤接口上的链路和活动 LED。

表 6-70 光纤链路/活动 LED

状态	说明
顶部 （活动）	接口有活动时，指示灯闪烁。如果不亮，则没有活动。
底部 （链路）	接口有链路时，指示灯亮起。如果不亮，则没有链路。

使用下表了解光纤接口的旁路 LED。

表 6-71 光纤旁路 LED

状态	说明
关闭	接口对没有链路并且不在旁路模式下或没有电源。
稳定绿色	接口对有链路而且正在传输流量。

表 6-71 光纤旁路 LED （续）

状态	说明
稳定黄色	接口已被故意关闭。
闪烁黄色	接口处于旁路模式下；即已在出故障时自动打开。

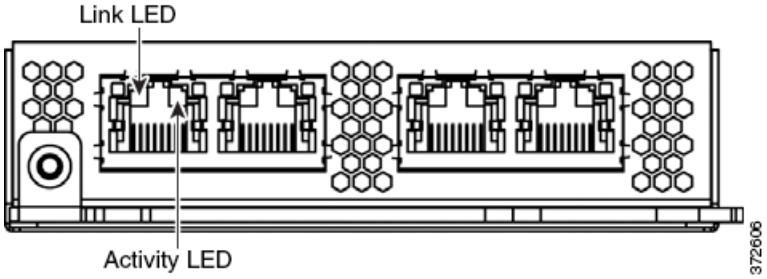
使用下表了解光纤接口的光纤参数。

表 6-72 40GBASE-SR4 网络模块光纤参数

参数	40GBASE-SR4
光纤连接器	OTP/MTP 单行十二个光纤位置 仅使用外部八个光纤
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
运行距离	100 米 （320 英尺）， 50 微米/125 微米光纤 (OM3) 最小距离：0.5 米 （2 英尺） 通过 MPO 连接器用八个光纤电缆传输 40 G 光学信号。
发射器波长	840-860 纳米 （850 纳米典型值）
最大平均发射功率	2.4 dBm
最小平均发射功率	-7.8 dBm
接收器的最大平均功率	2.4 dBm
接收器灵敏度	-9.5 dBm

四端口 1000BASE-T 铜可配置旁路网络模块

四端口 1000BASE-T 铜非旁路网络模块包含四个铜端口以及链路与活动 LED。



使用下表了解铜 LED。

表 6-73 非旁路铜链路/活动 LED

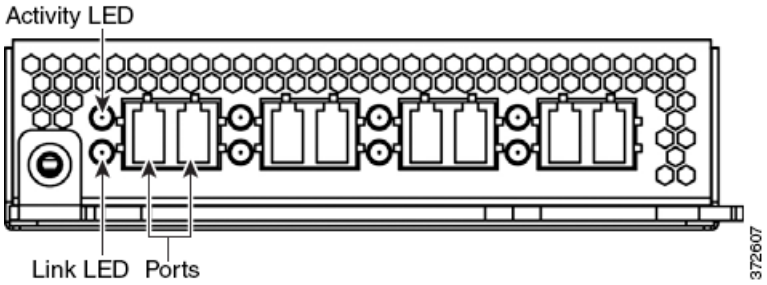
状态	说明
两个 LED 都关闭	接口没有链路。
黄色链路	接口上流量的速度是 10 Mb 或 100 Mb。

表 6-73 非旁路铜链路/活动 LED （续）

状态	说明
绿色链路	接口上流量的速度是 1 Gb。
活动闪烁绿色指示灯	接口有链路而且正在传输流量。

四端口 1000BASE-SX 光纤可配置旁路网络模块

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与活动 LED。



使用下表了解光纤接口上的链路和活动 LED。

表 6-74 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：接口有活动时，指示灯闪烁。如果不亮，则没有活动。
底部 （链接）	对于内联接口：接口有链路时，指示灯亮起。如果不亮，则没有链路。 对于被动接口：指示灯始终亮着。

使用下表了解光纤接口的光纤参数。

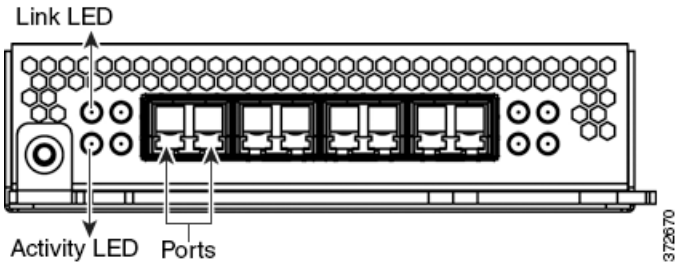
表 6-75 1000BASE-SX 网络模块光纤参数

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
运行距离	200 米 （656 英尺）， 62.5 微米/125 微米光纤 500 米 （1640 英尺）， 50 微米/125 微米光纤
发射器波长	770 - 860 纳米 （850 纳米典型值）
最大平均发射功率	0 dBm
最小平均发射功率	-9.5 dBm
接收器的最大平均功率	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与活动 LED。

注意事项 四端口 10GBASE 非旁路网络模块包含不可移动的 SFP。尝试移除 SFP 会损坏模块。



使用下表了解光纤接口上的链路和活动 LED。

表 6-76 光纤链路/活动 LED

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

使用下表了解光纤接口的光纤参数。

表 6-77 10GBASE MMSR 和 SMLR 网络模块光纤参数

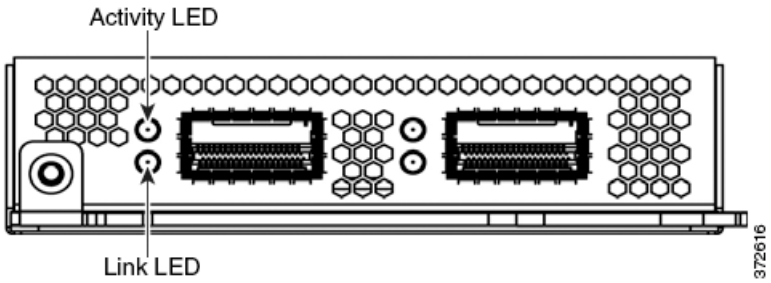
参数	10GBASE MMSR	10GBASE SMLR
光纤连接器	LC 双工：	LC 双工：
比特率	10.000 Gbps	10.000 Gbps
波特率/ 编码/ 容限	10.3125 Gbps/ 64/66b 编码/ +/-100 ppm	10.3125 Gbps/ 64/66b 编码/ +/-100 ppm
光纤接口：	多模	仅单模
工作距离	840 - 860 纳米 （850 纳米典型值） 26 米 （85 英尺）至 33 米 （108 英尺）， 62.5 微米/125 微米光纤 （模态带宽分别为 160 至 200） 66 米 （216 英尺）至 82 米 （269 英尺）， 50 微米/125 微米光纤 （模态带宽分别为 400 至 500） 高质量 (OM3) 光纤可提供 300 米 （980 英尺）以内工作距离。 最短距离 （全部）：2 米 （6 英尺）	1270 - 1355 纳米 （1310 纳米典型值） 2 米至 10 千米 （6 英尺至 6.2 英里）对于 9 微米/125 微米光纤
发射器波长	840 - 860 纳米 （850 纳米典型值）	1270 - 1355 纳米（1310 纳米典型值）
最大平均发射功率	-1 dBm	-0.5 dBm

表 6-77 10GBASE MMSR 和 SMLR 网络模块光纤参数 （续）

参数	10GBASE MMSR	10GBASE SMLR
最小平均发射功率	-7.3 dBm	-8.2 dBm
接收器的最大平均功率	-1 dBm	-0.5 dBm
接收器灵敏度	-9.9 dBm	-14.4 dBm

堆叠模块

堆叠模块包含两个适用于 8000 系列堆叠电缆的连接端口以及活动和链路 LED。



使用下表了解堆叠 LED。请注意，堆叠模块可用于 3D8140、 3D8250 和 3D8350 并且随附于 3D8260/3D8270/3D8290 和 3D8360/3D8370/3D8390 中。

表 6-78 堆叠 LED

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

还原 FireSIGHT 系统设备为出厂默认设置

思科在其支持站点提供 ISO 映像，用以将防御中心和受管设备还原或重新映像为其原始出厂设置。

注 有关还原或重新映像 ASA FirePOWER 设备的详细信息，请参阅 ASA 文档。

有关详细信息，请参阅以下各节：

准备工作

开始将设备还原为出厂默认设置前，应该熟悉系统在还原流程中的预期行为。

配置和事件备份指南

开始还原流程之前，思科建议删除或移动设备上的所有备份文件，然后将当前事件和配置数据备份到外部位置。

将设备还原为出厂默认设置会导致丢失设备上几乎**全部**配置和事件数据。虽然还原实用程序可以保留设备的许可证、网络、控制台和无人值守管理 (LOM) 设置，但是还原流程完成之后必须执行其他所有设置任务。

还原流程中的流量

为了避免网络出现流量中断，思科建议在维护时段或者流量中断时，这些对部署的影响最小时还原设备。

还原内联部署的受管设备会将设备重置为非旁路 （出故障时自动关闭）配置，导致网络流量中断。流量将被拦截，直到在设备上配置启用了旁路的内联集为止。

有关编辑设备配置从而配置旁路的详细信息，请参阅 *FireSIGHT 系统用户指南*的“管理设备”一章。

了解还原流程

FireSIGHT 系统 *设备*可以是一台流量感应受管 *设备*，也可以是一台管理*防御中心*：每个设备类型都有多种*型号*；这些型号又进一步划分分多个*产品*和*系列*。有关详细信息，请参阅 FireSIGHT 系统设备，第 1-1 页。

还原设备的准确步骤取决于设备的型号以及您是否对设备具备物理访问权限，但是总体过程都是一样的。

注 只能在维护窗口中重新映像设备。重新映像会将旁路模式下的设备重置为非旁路配置并中断网络流量，直至重新配置了旁路模式。有关详细信息，请参阅还原流程中的流量，第 7-2 页。

要还原 FireSIGHT 系统设备，请执行以下操作：

访问：管理员

步骤 1 确定要还原的设备 （设备或防御中心）的型号。

步骤 2 从支持站点获取正确的还原 ISO 映像。

步骤 3 将映像复制到适当的存储介质中。

步骤 4 连接设备。

步骤 5 重新启动设备并调用还原实用程序。

步骤 6 安装 ISO 映像。

为了方便起见，可以在还原流程中在大多数设备上安装系统软件和入侵规则更新。

下表总结了如何还原不同型号的 FireSIGHT 系统设备。

表 7-1 设备型号支持的还原方法

型号	还原方法	是否需要物理访问？	是否在还原流程中更新？
DC1000 DC3000	使用思科提供的预装了 ISO 映像的 CD-ROM 或创建自己的 CD。	是，加载 CD	否
DC500 所有 2 系列 设备（3D9900 除外）	从思科提供的外部 USB 驱动器启动，然后使用交互式菜单下载 ISO 映像并将其安装在设备上。	是，插入 USB 驱动器	是

表 7-1 设备型号支持的还原方法 （续）

型号	还原方法	是否需要物理访问？	是否在还原流程中更新？
3D9900 3 系列设备	从设备的内部闪存驱动器启动，然后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 交换机（所有）或 LOM （3 系列）用于远程还原	是

请注意，**无法**使用设备网络界面还原设备。要还原设备，必须按照以下任意一种方式连接设备：

键盘和显示器/KVM

可以将 USB 键盘和 VGA 显示器连接至任何 FireSIGHT 系统设备，这对于连接 KVM（键盘、视频和鼠标）交换机的机架安装式设备来说很有用。如果拥有可远程访问的 KVM，无需物理访问即可还原 3 系列设备和 3D9900。

串行连接/笔记本电脑

可以使用反转线串行电缆 （也称为 NULL 调制解调器电缆或思科控制台电缆）将计算机连接到除 3D2100/2500/3500/4500 之外的任何 FireSIGHT 系统设备。请参阅设备的硬件规格，找到串行端口。要与设备交互，请使用 HyperTerminal 或 Xmodem 等终端仿真软件。有关详细信息，包括按照设备分类的串行端口连接器表，请参阅串行连接/笔记本电脑，第 3-18 页。

使用 Serial over LAN 进行无人值守管理

可以通过 Serial over LAN (SOL) 连接使用无人值守管理 (LOM) 在 3 系列设备上执行一系列有限的操作。如果您需要将具有 LOM 功能的设备恢复为出厂默认设置，但您没有对该设备的物理访问权限，则可以使用 LOM 执行恢复过程。使用 LOM 连接到设备后，您就可以像使用物理串行连接时一样向恢复实用程序发出命令。有关详细信息，请参阅设置无人值守管理，第 7-16 页。

获取还原 ISO 和更新文件

思科提供 ISO 映像，用于还原设备原始出厂设置。在还原设备前，从支持站点获取正确 ISO 映像。

还原设备应该使用的 ISO 映像取决于思科为该设备型号推出支持的时间。除非 ISO 映像已发布了满足新设备型号的次要版本，否则 ISO 映像通常与系统软件的主要版本关联 （例如：5.2 或 5.3）。为避免安装不兼容版本的系统，思科建议始终为设备使用最新的 ISO 映像。

大多数设备使用外部 USB 或内部闪存驱动器启动设备，确保可以运行还原实用程序。但是，DC1000 和 DC3000 防御中心要求使用还原 ISO CD。如果有 DC1000 或 DC3000，购买设备时，思科会以 CD-ROM 的形式提供 ISO 映像。如果要将设备还原成另一版本，可以下载相应的 ISO 映像并创建新的还原 ISO （而非数据） CD，然后可以将其用于还原设备。

思科还建议始终运行设备所支持的最新版本的系统软件。将设备还原到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)。有关更多信息，请参阅要应用的更新的版本说明以及 《*FireSIGHT 系统用户指南*》中的“更新系统软件”一章。

为了方便起见，可以在还原流程中在大多数设备上安装系统软件和入侵规则更新。例如，可以将设备还原到 5.3 版本，在该流程中，还可以将设备更新到 5.3.0.1 版本。切记只有防御中心要求规则更新。

请注意，由于使用 CD 还原 DC1000 和 DC3000 防御中心，无法在还原流程中在这些设备上安装更新。应该在之后更新设备。

要获取还原 ISO 和其他更新文件，请执行以下操作：

访问：任意

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

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

例如，要下载 5.3 版本或 5.3.1 版本 ISO 映像，可以点击 **Downloads > 3D System > 5.3**。

步骤 3 查找要下载的映像 （ISO 映像）。

可以在页面左侧点击其中一个链接查看页面的相应部分。例如，可以点击 **5.3.1 Images**，查看 FireSIGHT 系统 5.3.1 版本的映像和版本说明。

步骤 4 点击要下载的 ISO 映像。

文件开始下载。

步骤 5 也可以下载系统软件和入侵规则更新：

- 系统软件更新位于和 ISO 映像相同的支持站点页面。可以在页面左侧点击其中一个链接查看页面的相应部分。例如，可以点击 **5.3.1**，查看 FireSIGHT 系统 5.3.1 版本的更新和版本说明。
- 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：如果还原 DC1000 或 DC3000，还原流程完成之后必须安装更新。

步骤 6 如何还原设备？

- 对于大多数设备，即利用 USB 或内部闪存驱动器还原的设备，请将文件复制到设备在其管理网络上可以访问的 HTTP （网络）服务器、 FTP 服务器或支持 SCP 的主机上。
- 对于 DC1000 和 DC3000，请使用 ISO 映像创建还原 CD。

注意事项 请**勿**通过邮件传输 ISO 或更新文件，否则可能损坏文件。此外，请**勿**更改文件的名称，因为还原实用程序要求文件名称与支持站点上的名称一样。

开始还原流程

支持的设备：任意

支持的防御中心：除 DC1000、 DC3000 外的所有型号

对于除 DC1000 和 DC3000 防御中心之外的所有设备，请从外部 USB 或内部闪存驱动器启动设备开始还原流程，具体取决于设备型号；请参阅第 7-2 页上的表 7-1。

确保具有适当级别的访问权限和设备连接以及正确的 ISO 映像之后，使用以下程序之一还原设备：

- 使用 KVM 或物理串行端口启动还原实用程序，第 7-5 页说明了如何开始不支持 LOM 的设备（即不具备 LOM 访问权限的设备）的设备还原流程。可以使用此方法还原除 DC1000 或 DC3000 防御中心外的所有型号。
- 使用无人值守管理启动还原实用程序，第 7-6 页说明了如何使用 LOM 通过 SOL 连接开始 3 系列设备的还原流程。
- 使用 CD 还原 DC1000 或 DC3000，第 7-15 页说明了如何使用 CD 还原 DC1000 或 DC3000 防御中心。

注意事项 本章中的步骤说明了如何在不关闭设备的情况下还原设备。但是，如果由于任何原因需要关机，请使用 《*FireSIGHT 系统用户指南*》“管理设备”一章中的步骤、 3 系列设备上 CLI 的 `system shutdown` 命令或设备外壳的 `shutdown -h now` 命令 （有时又称为专家模式）。

使用 KVM 或物理串行端口启动还原实用程序

支持的设备：任意

支持的防御中心：除 DC1000、 DC3000 外的所有型号

对于除 DC1000 和 DC3000 防御中心之外的所有设备，思科通过外部 USB 或内部闪存驱动器提供还原实用程序，具体取决于设备型号；请参阅第 7-2 页上的表 7-1。

注 因为设备可能尝试将大容量存储设备用作启动设备，因此请**勿**使用带 USB 大容量存储设备的 KVM 控制台访问设备以了解初始设置。

如果需要将 3 系列设备恢复出厂默认设置并且没有对设备的物理访问，可以使用 LOM 执行还原流程。请参阅使用无人值守管理启动还原实用程序，第 7-6 页。

要启动还原实用程序，请执行以下操作：

访问：管理员

步骤 1 如果使用 USB 驱动器还原 DC500 或除 3D9900 之外的任何 2 系列设备，请将 USB 驱动器插入设备上可用的 USB 端口中。

否则，跳到下一步。

步骤 2 请使用具有管理员权限的帐户，利用键盘/显示器或串行连接登录设备。密码与设备的网络界面的密码相同。

系统将显示设备提示。

步骤 3 重新启动设备：

- 在防御中心或 2 系列受管设备上，键入 `sudo reboot`。
- 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，系统显示启动屏幕。

步骤 4 监视重新启动状态：

- 如果系统执行数据库检查，则会发现以下消息：`The system is not operational yet.Checking and repairing database are in progress.This may take a long time to finish.`
- 在 DC500 防御中心或 3D500/1000/2000 设备上，出现启动屏幕时请缓慢地重复按 Ctrl + U。
- 对于使用键盘和显示器连接的所有其他设备，系统显示红色 LILO 启动菜单。快速按下其中一个箭头键，防止设备启动当前安装版本的系统。
- 对于使用串行连接的所有其他设备，看到 BIOS 启动选项时，请缓慢地重复按 Tab （防止设备启动当前安装版本的系统）。系统将显示 LILO 启动提示符：

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

步骤 5 指示想要还原系统：

- 在 DC500 防御中心或 3D500/1000/2000 设备上，请按 Enter。
- 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` 并按 Enter。
- 对于使用串行连接的所有其他设备，请在提示符下键入 `System_Restore` 并按 Enter。

完成以下选择之后系统将显示 `boot` 提示符：

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

步骤 6 为还原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，请键入 `0` 并按 Enter。
- 对于串行连接，请键入 `1` 并按 Enter。

如未选择显示模式， 30 秒之后还原实用程序默认选择标准控制台。

除非是首次将设备还原成此主要版本，否则此实用程序会自动加载上一次所使用的还原配置。要继续，请确认一系列页面上的设置。

系统将显示还原实用程序版权声明。

步骤 7 按 Enter 确认版权声明并继续执行使用交互式菜单还原设备，第 7-7 页。

使用无人值守管理启动还原实用程序

支持的设备：3 系列

支持的防御中心：3 系列

如果需要将 3 系列设备恢复出厂默认设置并且没有对设备的物理访问，可以使用 LOM 执行还原流程。请注意，如果要使用 LOM 配置初始设置，在初始设置期间**必须**保留网络设置。

注 使用 LOM 还原设备之前，必须启用此功能；请参阅设置无人值守管理，第 7-16 页。

要使用无人值守管理启动还原实用程序，请执行以下操作：

访问：管理员

步骤 1 在计算机显示命令提示符时，输入 IPMI 命令，启动 SOL 会话：

- 对于 IPMItool，请键入：

  ```
  sudo ipmitool -I lanplus -H IP_address -U username sol activate
  ```

- 对于 ipmiutil，请键入：

  ```
  sudo ipmiutil sol -a -V4 -J3 -N IP_address -U username -P password
  ```

其中 *`Ip_address`* 代表设备上管理接口的 IP 地址， *`username`* 代表授权 LOM 帐户的用户名，并且 *`password`* 代表该帐户的密码。请注意，发出 `sol activate` 命令后， IPMItool 会提示键入密码。

如果使用的是 3 系列虚拟受管设备，请键入 `expert` 显示外壳提示符。

步骤 2 以根用户的身份重新启动设备：

- 对于防御中心，请键入 `sudo reboot`。
- 对于 3 系列设备，请键入 `system reboot`。

设备重新启动。

步骤 3 监视重新启动状态。

如果系统执行数据库检查，则会显示以下消息：`The system is not operational yet.Checking and repairing database are in progress.This may take a long time to finish.`

看到 BIOS 启动选项时，请缓慢地重复按 Tab （防止设备启动当前安装版本的系统），直到系统将显示 LILO 启动提示符：

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

步骤 4 系统将显示 `boot` 提示符时，请键入 `System_Restore` 启动还原实用程序。

完成以下选择之后系统将显示 `boot` 提示符：

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

步骤 5 请键入 `1` 并按 Enter，通过设备的串行连接加载交互式还原菜单。

注 如未选择显示模式， 10 秒之后还原实用程序默认选择标准控制台。

除非是首次将设备还原成此主要版本，否则此实用程序会自动加载上一次所使用的还原配置。要继续，请确认一系列页面上的设置。

系统将显示还原实用程序版权声明。

步骤 6 按 Enter 确认版权声明并继续执行使用交互式菜单还原设备，第 7-7 页。

使用交互式菜单还原设备

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 FireSIGHT 系统设备的还原实用程序都使用交互式菜单来指导还原。

提示 如果用 CD 还原 DC1000 或 DC3000，请跳转到使用 CD 还原 DC1000 或 DC3000，第 7-15 页。

注 只能在维护窗口中重新映像设备。重新映像会将旁路模式下的设备重置为非旁路配置并中断网络流量，直至重新配置了旁路模式。有关详细信息，请参阅还原流程中的流量，第 7-2 页。

菜单显示下表中列出的选项。

表 7-2 还原菜单选项

选项	说明	有关详细信息，请参阅…
1 IP Configuration	指定有关在要还原的设备上管理接口的网络信息，从而使设备可以与存放 ISO 和任何更新文件的服务器通信。	识别设备的管理接口，第 7-9 页
2 Choose the transport protocol	指定用于还原设备的 ISO 映像的位置，以及设备下载此文件所需的任何凭据。	指定 ISO 映像位置和传输方法，第 7-9 页

表 7-2 还原菜单选项 （续）

选项	说明	有关详细信息，请参阅...
3 Select Patches/Rule Updates	指定设备还原到 ISO 映像中的基本版后要应用的系统软件和入侵规则更新。	在还原流程中更新系统软件和入侵规则，第 7-11 页
4 Download and Mount ISO	下载相应的 ISO 映像和任何系统软件或入侵规则更新。安装 ISO 映像。	下载 ISO 和更新文件并安装映像，第 7-11 页
5 Run the Install	调用还原流程。	调用还原流程，第 7-12 页
6 Save Configuration 7 Load Configuration	保存任何还原配置集合供以后使用或加载已保存的配置集合。	保存和加载还原配置，第 7-14 页
8 Wipe Contents of Disk	安全地清理硬盘驱动器，确保无法访问其内容。	清理硬盘驱动器，第 D-1 页

使用箭头键导航菜单。要选择菜单选项，请使用上下箭头。使用左右箭头键切换位于页面底部的 **OK** 和 **Cancel** 按钮。

菜单可以显示两种不同类型的选项：

- 要选择带编号的选项，请首先使用上下箭头突出显示正确的选项，然后在页面底部 **OK** 按钮突出显示时按 Enter。
- 要选择多项选择 （单选按钮）选项，请首先使用上下键突出显示正确的选项，然后按空格键用 x 标记该选项。要接受选择，在 **OK** 按钮突出显示时，请按 Enter。

大多数情况下，请依次完成菜单选项 **1**、**2**、**4** 和 **5**。也可以增加选项 **3**，在还原流程中安装系统软件和入侵规则更新。

如果将设备还原为与设备当前安装的版本不同的一个主要版本，则需要执行双步还原流程。第一步是更新操作系统，第二步是安装新版本的系统软件。

如果这是第二步，或还原实用程序自动加载了要使用的还原配置，则可以从菜单选项 **4**：下载 ISO 和更新文件并安装映像，第 7-11 页开始。但是，思科建议仔细检查还原配置中的设置，再继续操作。

提示 要使用以前保存的配置，则从菜单选项 **6**：保存和加载还原配置，第 7-14 页开始。加载配置后，请跳转至菜单选项 **4**：下载 ISO 和更新文件并安装映像，第 7-11 页。

要使用交互式菜单还原设备，请使用以下步骤：

步骤 1 **1 IP Configuration** — 请参阅识别设备的管理接口，第 7-9 页。

步骤 2 **2 Choose the transport protocol** — 请参阅指定 ISO 映像位置和传输方法，第 7-9 页。

步骤 3 **3 Select Patches/Rule Updates** （可选） — 请参阅在还原流程中更新系统软件和入侵规则，第 7-11 页。

步骤 4 **4 Download and Mount ISO** — 请参阅下载 ISO 和更新文件并安装映像，第 7-11 页。

步骤 5 **5 Run the Install** — 请参阅调用还原流程，第 7-12 页。

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

运行还原实用程序的第一步是识别您要还原的设备的管理接口，使设备可以与复制 ISO 和任何更新文件位置的服务器通信。如果使用 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

步骤 1 请从主菜单中选择 **1 IP Configuration**。

系统将显示 Pick Device 页面。

步骤 2 选择设备的管理接口 （通常是 **eth0**）。

系统将显示 IP Configuration 页面。

步骤 3 选择管理网络使用的协议：**IPv4** 或 **IPv6**。

系统将显示向管理接口分配 IP 地址的选项。

步骤 4 选择向管理接口分配 IP 地址的方法：**Static** 或 **DHCP**：

- 如果选择 **Static**，系统将显示一系列页面，提示手动输入 IP 地址、网络掩码或前缀长度以及管理接口的默认网关。
- 如果选择 **DHCP**，设备自动检测 IP 地址、网络掩码或前缀长度和管理接口的默认网关，然后显示 IP 地址。

步骤 5 系统提示时，请确认设置。

如果系统提示，请确认分配给设备管理接口的 IP 地址。系统再次显示主菜单。

步骤 6 继续执行下一节：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

配置还原流程用于下载其所需要的文件的管理 IP 地址后，必须指定使用哪个 ISO 映像来还原设备。这就是从支持站点 （请参阅获取还原 ISO 和更新文件，第 7-3 页）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。

交互式菜单提示输入完成下载所需的任何信息，如下表所示。

表 7-3 下载还原文件所需的信息

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 • 相对于要使用其凭据的用户的主目录，提供 ISO 映像目录路径 （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 • 之前输入的用户名的密码 请注意，输入密码之前，设备可能会要求将 SCP 服务器添加到其受信任主机的列表中。必须接受此要求，才能继续。

请注意，还原实用程序还会在 ISO 映像目录中查找更新文件。

要指定还原文件的位置和传输方法，请执行以下操作：

访问：管理员

步骤 1 在主菜单中，选择 **2 Choose the transport protocol**。

步骤 2 在系统显示的页面上，选择 **HTTP**、 **FTP** 或 **SCP**。

步骤 3 使用还原实用程序显示的一系列页面为选择的协议提供必要信息，详见第 7-10 页上的表 7-3。

如果信息正确，设备将连接服务器并在指定的位置显示思科 ISO 映像的列表。

步骤 4 选择要使用的 ISO 映像。

步骤 5 系统提示时，请确认设置。

系统再次显示主菜单。

步骤 6 是否要在还原流程中安装系统软件或入侵规则更新？

- 如果是，继续执行下一节：在还原流程中更新系统软件和入侵规则。
- 如果否，继续执行下载 ISO 和更新文件并安装映像，第 7-11 页。请注意，可以在还原流程完成之后使用系统的网络界面手动安装更新。

在还原流程中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

也可以使用还原实用程序在设备还原之后将系统软件和入侵规则还原为 ISO 映像中的基本版本。注意只有防御中心要求规则更新。

还原实用程序只能使用一个系统软件更新以及一个规则更新。但是，系统更新将从上一个主要版本开始累计；规则更新也是累计的。思科建议获取适用于设备的最新更新；请参阅获取还原 ISO 和更新文件，第 7-3 页。

如果选择不在还原流程中更新设备，可于以后使用系统的网络界面更新。有关详细信息，请参阅要安装的更新的版本说明以及《*FireSIGHT 系统用户指南*》中的“更新系统软件”一章。

要作为还原流程的一部分安装更新，请执行以下操作：

访问：管理员

步骤 1 请从主菜单中选择 **3 Select Patches/Rule Updates**。

还原实用程序使用上一步中指定的协议和位置（请参阅指定 ISO 映像位置和传输方法，第 7-9 页）检索和显示该位置任何系统软件更新文件的列表。如果使用 SCP，请在系统提示时输入密码，显示更新文件的列表。

步骤 2 选择要使用的系统软件更新（如有）。

并非必须选择更新；也可以在不选择更新的情况下按 Enter 继续操作。如果相应位置没有系统软件更新，系统会提示按 Enter 继续操作。

还原实用程序检索并显示规则更新文件的列表。如果使用 SCP，请在系统提示时输入密码，显示列表。

步骤 3 选择要使用的规则更新（如有）。

并非必须选择更新；也可以在不选择更新的情况下按 Enter 继续操作。如果相应位置没有规则更新，系统会提示按 Enter 继续操作。

选择保存成功，系统再次显示主菜单。

步骤 4 继续执行下一节：下载 ISO 和更新文件并安装映像。

下载 ISO 和更新文件并安装映像

支持的设备：任意

支持的防御中心：除 DC1000、 DC3000 外的所有型号

最后下载必要的文件并安装 ISO 映像，再调用还原流程。

提示 开始此流程之前，可能要保存还原配置以供以后使用。有关详细信息，请参阅保存和加载还原配置，第 7-14 页。

要下载和安装 ISO 映像，请执行以下操作：

访问：管理员

步骤 1 在主菜单中，选择 **4 Download and Mount ISO**。

步骤 2 系统提示时，请确认选择。如果从 SCP 服务器下载，请在系统提示时输入密码。

相应的文件将会下载并安装。系统再次显示主菜单。

步骤 3 继续执行下一节：调用还原流程。

调用还原流程

支持的设备：任意

支持的防御中心：除 DC1000、 DC3000 外的所有型号

下载并安装 ISO 映像后，即可调用还原流程。如果将设备还原为与设备当前安装的版本不同的一个主要版本，则需要执行双步还原流程。第一步是更新操作系统，第二步是安装新版本的系统软件。

双步流程的第一步 （仅更改主要版本）

将设备还原为另一个主要版本时，还原实用程序第一步将更新设备的操作系统，并且在必要时还原实用程序本身。

注 如果将设备还原为同一个主要版本，或者这是该流程的第二步，请跳至下一程序：双步或单步，第 7-13 页。

要执行双步还原流程的第一步，请执行以下操作：

访问：管理员

步骤 1 在主菜单中，选择 **5 Run the Install**。

步骤 2 系统提示 （两次）时，请确认要重新启动设备。

注 对于使用外部 USB 驱动器还原的设备，如果驱动器有与系统的不同版本关联的还原实用程序，必须在驱动器上更新此实用程序才能继续操作。系统提示时，请键入 `yes`，更新实用程序 （并删除任何保存的还原配置）。然后，请确认要从更新驱动器重新启动。如果不更新 USB 驱动器，设备重新启动。无法使用此驱动器还原设备。

步骤 3 监视重新启动并重新调用还原流程：

- 如果系统执行数据库检查，则会发现以下消息：`The system is not operational yet.Checking and repairing database are in progress.This may take a long time to finish.`
- 对于键盘和显示器连接，系统将显示红色 LILO 启动菜单。快速按下其中一个箭头键，防止设备启动当前安装版本的系统。
- 对于串行或 SOL/LOM 连接，当您看到 BIOS 启动选项时，请缓慢地重复按 Tab 键，直到系统显示 LILO 启动提示符为止：

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

步骤 4 指示想要还原系统：

- 对于键盘和显示器连接，请使用箭头键选择 `System_Restore` 并按 Enter。
- 对于串行或 SOL/LOM 连接，请在系统提示时键入 `System_Restore` 并按 Enter。

无论如何，完成下列选择之后系统都会显示 `boot` 提示符：

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

步骤 5 为还原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，请键入 `0` 并按 Enter。
- 对于串行或 SOL/LOM 连接，请键入 `1` 并按 Enter。

如未选择显示模式， 10 秒之后还原实用程序默认选择标准控制台。

除非是首次将设备还原成此主要版本，否则此实用程序会自动加载上一次所使用的还原配置。要继续，请确认一系列页面上的设置。

系统将显示还原实用程序版权声明。

步骤 6 按 Enter 确认版权声明，然后开始此流程的第二步，首先使用交互式菜单还原设备，第 7-7 页。

双步或单步

使用以下程序，执行还原流程的第二步或唯一一步。

要执行还原流程的第二步或唯一一步，请执行以下操作：

访问：管理员

步骤 1 在主菜单中，选择 **5 Run the Install**。

步骤 2 确认想要还原设备并继续下一步骤。

步骤 3 选择是否想要删除设备的许可证和网络设置。对于 3 系列设备、 LOM，删除这些设置还会重置显示器 （控制台）设置。

在大多数情况下，无需删除这些设置，因为这样可以缩短初始设置流程。在还原和随后的初始设置之后更改设置通常比在此时重置耗时更短。有关详细信息，请参阅后续步骤，第 7-16 页。

注意事项 如果使用 LOM 连接还原设备，请**勿**删除网络设置。重新启动设备后，无法通过 LOM 重新连接。

步骤 4 如果使用 USB 驱动器还原设备，则当还原实用程序提示您键入对是否想要还原设备的最终确认时，请移除此驱动器。

步骤 5 键入对想要还原设备的最终确认。

随即开始还原流程的最后阶段。完成此阶段后，如果系统提示，请确认是否要重新启动设备。

注意事项 确保有充足的时间完成还原流程。在带有内部闪存驱动器的设备上，实用程序首先更新闪存驱动器，然后将其用于执行其他还原任务。如果在闪存更新期间退出 （例如按 Ctrl+C 退出），可能导致不可恢复的错误。如果认为还原时间过长或在此流程中遇到任何其他问题，请**勿**退出。请联系支持部门。

注 重新映像会将旁路模式下的设备重置为非旁路配置并中断网络流量，直至重新配置了旁路模式。有关详细信息，请参阅还原流程中的流量，第 7-2 页。

步骤 6 继续后续步骤，第 7-16 页中的内容。

保存和加载还原配置

支持的设备：任意

支持的防御中心：除 DC1000、 DC3000 外的所有型号

对于大多数设备，如果需要再次还原设备，可以使用还原实用程序保存要用的还原配置。虽然还原实用程序会自动保存上一次使用的配置，但是您也可以保存多种配置，包括：

- 有关设备上的管理接口的网络信息；请参阅识别设备的管理接口，第 7-9 页
- 还原 ISO 映像的位置，以及传输协议和设备下载文件需要的任何凭据；请参阅指定 ISO 映像位置和传输方法，第 7-9 页
- 设备还原为 ISO 映像中的基本版本之后想要应用的系统软件和入侵规则更新 （如有）；请参阅在还原流程中更新系统软件和入侵规则，第 7-11 页

SCP 密码不保存。如果配置指定实用程序必须使用 SCP 向设备传输 ISO 和其他文件，必须重新验证服务器才能完成还原流程。

保存还原复配置的最佳时间是在提供上述信息之后，下载并安装 ISO 映像之前。请注意，如果更新还原 USB 驱动器，使之与系统的不同主要版本兼容，所有已保存的还原配置都将丢失。

要保存还原配置，请执行以下操作：

访问：管理员

步骤 1 请从还原实用程序主菜单中选择 **6 Save Configuration**。

实用程序显示所保存的配置中的设置。

步骤 2 系统提示时，请确认要保存配置。

步骤 3 系统提示时，请为配置输入一个名称。

系统将会保存配置，并再次显示主菜单。

步骤 4 如果要使用刚刚保存的配置来还原设备，继续执行下载 ISO 和更新文件并安装映像，第 7-11 页。

要加载已保存的还原配置，请执行以下操作：

访问：管理员

步骤 1 请从主菜单中选择 **7 Load Configuration**。

实用程序将显示已保存的还原配置的列表。第一个选项， **default_config**，是最后一次用于还原设备的配置。其他选项是已保存的还原配置。

步骤 2 选择要使用的配置。

实用程序显示正在加载的配置中的设置。

步骤 3 系统提示时，请确认要加载此配置。

配置加载成功。如果系统提示，请确认分配给设备管理接口的 IP 地址。系统再次显示主菜单。

步骤 4 要使用刚刚加载的配置还原设备，请继续执行下载 ISO 和更新文件并安装映像，第 7-11 页。

使用 CD 还原 DC1000 或 DC3000

支持的设备：无

支持的防御中心：DC1000、 DC3000

DC1000 和 DC3000 防御中心都有 CD-ROM 驱动器，购买设备时思科会提供一份还原 CD。如果要将设备还原成另一版本，可以下载相应的 ISO 映像并创建新 ISO （而非数据）还原 CD，然后可以将其用于还原系统；请参阅获取还原 ISO 和更新文件，第 7-3 页。

请注意，由于是使用 CD 还原这些防御中心，无法在此还原流程中在这些设备上安装更新。应该在之后更新设备。

要使用 CD 还原 DC1000 或 DC3000，请执行以下操作：

访问：管理员

步骤 1 将还原 CD 放在防御中心的 CD 托盘中。

如果设备已关闭，请接通设备电源以打开托盘。

步骤 2 请使用具有管理员权限的帐户，利用键盘/显示器或串行连接登录防御中心。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。

步骤 3 系统提示时，请键入 `sudo reboot`，以根用户的身份重新启动防御中心。

防御中心从 CD 启动。此操作会花费几分钟的时间。

步骤 4 系统提示时，请确认要还原防御中心。

步骤 5 选择是否想要删除设备的许可证和网络设置。删除这些设置还会重置显示器 （控制台）设置。

在大多数情况下，无需删除这些设置，因为这样可以缩短初始设置流程。在还原和随后的初始设置之后更改设置通常比在此时重置耗时更短。有关详细信息，请参阅后续步骤，第 7-16 页。

步骤 6 键入对想要还原设备的最终确认。

还原流程开始并在屏幕上显示其进度。

注意事项 确保有充足的时间完成还原流程。极少数情况下，如果退出 （例如通过按 Ctrl+C 或关闭设备电源退出），可能导致不可恢复的错误。如果认为还原时间过长或在此流程中遇到任何其他问题，请**勿**退出。请联系支持部门。

步骤 7 出现提示时，按 Enter 继续。

防御中心弹出 CD。取出 CD，关闭托盘。

步骤 8 系统再次提示时，按 Enter 确认已完成还原并且确认要重新启动设备。

设备重新启动。

步骤 9 继续后续步骤中的内容。

后续步骤

将设备还原为出厂默认设置会导致丢失设备上的几乎**全部**配置和事件数据，包括内联部署设备的旁路配置。有关详细信息，请参阅还原流程中的流量，第 7-2 页。

还原设备后，必须完成初始设置流程：

- 如未删除设备的许可证和网络设置，可以使用管理网络上的计算机直接浏览至设备的网络界面，执行此设置。有关详细信息，请参阅初始设置页面：设备，第 4-7 页和 初始设置页面：防御中心，第 4-10 页。
- 如果删除了许可证和网络设置，必须像对待新设备一样配置设备，首先配置设备使之通过管理网络通信。请参阅设置 FireSIGHT 系统设备，第 4-1 页。

请注意，删除许可证和网络设置还会重置显示器 （控制台）设置，对于 3 系列设备，还会重置 LOM 设置。完成初始设置流程后：

- 如果想要使用串行或 SOL/LOM 连接访问设备的控制台，应重定向控制台输出；请参阅测试内联旁路接口的安装，第 3-20 页。
- 如果想要使用 LOM，必须重新启用此功能并且启用至少一个 LOM 用户；请参阅启用 LOM 和 LOM 用户，第 7-17 页。

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

如果需要将 3 系列设备还原出厂默认设置并且没有对设备的物理访问，可以使用无人值守管理 (LOM) 来执行还原流程。**无法**使用 LOM 还原 2 系列 设备。只有 3 系列设备支持 LOM。

通过 LOM 功能可以使用 Serial over LAN (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。利用 LOM，可以在带外管理连接上使用命令行界面执行诸如查看机箱序列号或监控风扇速度和温度等状况的任务。

LOM 命令语法取决于所使用的实用程序，但是， LOM 命令通常包含下表列出的元素。

表 7-4 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`	启用 LOM 会话加密。
`-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。
不适用 （在登录时提示）	-P *password*	仅适用于 ipmiutil，指定授权 LOM 帐户的密码。
command	*command*	想要发送至设备的命令。注意发出命令的地点取决于实用程序： • 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
```

另外，对于 ipmiutil：

```
ipmiutil command -V4 -J3 -N IP_address -U username -P password
```

注意在 70xx 子系列设备上 `chassis power off` 和 `chassis power cycle` 命令无效。有关 FireSIGHT 系统支持的 LOM 命令的完整列表，请参阅 《*FireSIGHT 系统用户指南*》中“配置设备设置”一章。

注 必须禁用与设备管理接口连接的所有第三方交换设备上的生成树协议 (STP)，才能使用 SOL 连接 7000 系列设备。

使用 LOM 还原设备之前，必须为设备和执行还原的用户启用 LOM。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到串行端口。

有关详细信息，请参阅以下各节：

- 启用 LOM 和 LOM 用户，第 7-17 页
- 安装 IPMI 实用程序，第 7-18 页

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

使用 LOM 还原设备之前，必须启用和配置此功能。还必须向使用此功能的用户明确授予 LOM 权限。

使用每个设备的本地网络界面，可以基于设备配置 LOM 和 LOM 用户。换句话说，无法用防御中心在受管设备上配置 LOM。同样，因为对于每个设备用户都是独立管理的，在防御中心上启用或创建启用 LOM 的用户不会将此功能传递至受管设备上的用户。

LOM 用户还有如下限制：

- 必须向用户指定管理员角色。
- 用户名称可以有最多 16 个字母数字字符。 LOM 用户名不支持短划线和更长的用户名。
- 密码可以有最多 20 个字母数字字符。LOM 用户不支持更长的密码。用户的 LOM 密码与该用户的系统密码相同。
- 3 系列防御中心和 8000 系列设备可以有最多 13 个 LOM 用户。7000 系列设备可以有最多八个 LOM 用户。

提示 有关以下任务的详细说明，请参阅 《*FireSIGHT 系统用户指南*》中“配置设备设置”一章。

要启用 LOM，请执行以下操作：

访问：管理员

步骤 1 选择 **System > Local > Configuration**，然后点击 **Console Configuration**。

步骤 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，必须使用**物理串行端口**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 （也可以使用 DHCP 来自动给这些值赋值）。

- 在 7000 系列设备上，选择 **Lights Out Management**，配置 LOM 设置。7000 系列设备不同时支持 LOM 和物理串行访问。

注 LOM IP 地址必须与设备的管理接口 IP 地址不同。

要为 FireSIGHT 系统用户启用 LOM 功能，请执行以下操作：

访问：管理员

步骤 1 选择 **System > Local > User Management**，然后编辑现有用户来添加 LOM 权限，或创建要用于对设备的 LOM 访问的新用户。

步骤 2 在 User Configuration 页面，启用 **Administrator** 角色 （如尚未启用）。

步骤 3 启用 **Allow Lights-Out Management Access** 复选框并保存更改。

安装 IPMI 实用程序

在计算机上使用第三方 IPMI 实用程序创建与设备的 SOL 连接。

如果计算机运行的是 Linux 或 Mac OS，请使用 IPMItool。虽然 IPMItool 对于许多 Linux 版本是标准配置，但是在 Mac 上必须安装 IPMItool。首先，请确认 MAC 安装了 Apple 的 xCode 开发者工具包。此外，请确保安装了命令行开发的可选组件 （较高版本中的“UNIX Development”和“System Tools”或较低版本中的“Command Line Support”）。最后，请安装 MacPorts 和 IPMItool。有关详细信息，请使用首选搜索引擎搜索或浏览下列网站：

```
https://developer.apple.com/technologies/tools/
http://www.macports.org/
```

对于 Windows 环境，请使用 ipmiutil，这需要自己编译。如果无法访问编译器，可以使用 ipmiutil 自身来编译。有关详细信息，请使用首选搜索引擎搜索或浏览以下网站：

```
http://ipmiutil.sourceforge.net/
```

FirePOWER 设备电源要求

以下章节介绍 FirePOWER 设备电源要求和相关信息

注 有关 ASA FirePOWER 设备电源要求的信息，请参阅 ASA 文档。

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。如果不遵守警告可能导致人身伤害或设备损坏。注意事项是正常运行所需满足的要求。如果不遵守注意事项可能导致不当操作。

注意事项 设备或部件的建筑内端口仅适用于连接至建筑内或明线连接。**禁止**使用金属线将设备或部件的建筑内端口连接到布线或连接到厂外 (OSP) 连接的接口。这些接口仅能用作建筑内接口（类型 2 或类型 4 端口在 GR-1089-CORE 第 4 版中有描述）并要求与 OSP 明线隔离。即使添加了主保护器，也不足以为使用金属将这些接口线连接到 OSP 布线提供充足保护。

静电控制

注意事项 在开箱、安装或移动设备之前，必须执行静电放电控制程序，如使用接地静电手环和一个 ESD 工作台。过度的静电放电可能会损坏设备或引发意外操作。

70xx 子系列设备

本章节介绍下列思科设备的电源要求：

- 3D7010、 3D7020 和 3D7030 (CHRY-1U-AC)

这些思科设备适合由合格人员安装在符合国家电气规范的网络电信设施和位置中。请注意，每台设备仅可作为一台交流电设备。

思科建议您保留包装材料，以防需要退换货时使用。

有关详细信息，请参阅以下各节：

- 请参阅安装，第 A-2 页，以了解关于电路安装、电压、电流、频率范围和电源线的详细信息。
- 请参阅接地要求，第 A-3 页，以了解对连接位置、推荐端子及地线的要求。

安装

FireSIGHT 系统设备安装必须遵循美国国家电气规范 (NEC) 手册 NFPA 70 第 250 款以及当地电气规范的要求。

设备使用单一的供电电源。必须在待安装 FireSIGHT 系统的网络设备输入端安装一个外部浪涌保护装置。

电路的额定值必须满足设备的最大额定值范围。

电压

电源标称工作范围为 100 VAC 到 240 VAC （最大范围是 90 VAC 到 264 VAC）。电压超过此范围可能导致设备损坏。

电流

标记的额定电流在整个运行条件范围内，最大为 2 A。必须使用合适的电线和断路器减少火灾风险。

频率范围

交流电电源的频率范围为 47 Hz - 63 Hz。频率超过此范围可能导致设备停止运行或非正常运行。

电源线

电源采用 IEC C14 连接器，也可使用 IEC C13 连接器。必须使用 UL 认证的电源线。最小线规是 16 AWG。设备提供的电缆是 16 AWG， UL 认证的电缆带 NEMA 515P 插头。如需其他电源线，请与工厂联系。

注 请勿切割带电的电线。

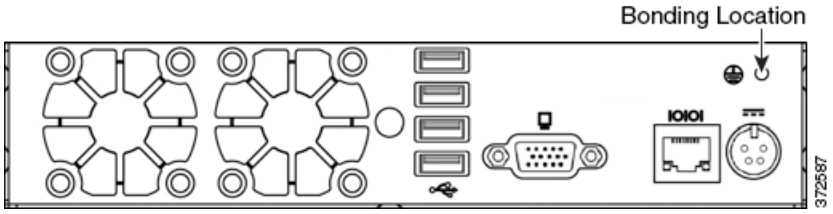
接地要求

设备必须与公共连接网连接实现接地。

连接位置

在机箱后面有一个接地连接位置。随附有 M4 螺栓。随附有齿轮向外的锁紧垫圈，以将其固定到环状端子。每个螺栓都有一个标准的接地符号。

下图显示机箱上的连接位置。



推荐端子

必须使用 UL 认证的端子进行接地连接。可以使用一个环状端子，该端子带有一个适合 #6 (M3.5) 螺栓的穿通孔。对于 16 AWG 电线，建议使用 AMP/Tyco 36151 规格的端子。这种 UL 认证的环状端子带有一个适合 #6 螺栓的穿通孔。

地线要求

地线必须大小合适，以便出现单次故障时可以有效地处理电路的电流。地线的大小应与保护电路的断路器电流一致。请参阅电流，第 A-2 页。

在压接连接之前，必须为裸导线涂一层抗氧剂。只有铜缆可用于接地。

71xx 子系列设备

本章节介绍下列思科设备的电源要求：

- 3D7110 和 3D7120 (GERY-1U-8-AC)
- 3D7115 和 3D7125 (GERY-1U-4C8S-AC)

这些思科设备适合由合格人员安装在符合国家电气规范的网络电信设施和位置中。请注意，每台设备仅可作为一台交流电设备。

思科建议您保留包装材料，以防需要退换货时使用。

有关详细信息，请参阅以下各节：

- 请参阅安装，第 A-4 页，以了解关于电路安装、电压、电流、频率范围和电源线的详细信息。
- 请参阅接地要求，第 A-5 页，以了解对连接位置、推荐端子及地线的要求。

安装

FireSIGHT 系统安装必须遵循美国国家电气规范 (NEC) 手册 NFPA 70 第 250 款以及当地电气规范的要求。

需将不同电路分开，以创建冗余的电源。使用不间断电源或电池备用电源，防止由于输入线电源故障造成的电源状态问题或电源损失。

向每条电源提供充足的电力，为整个设备运行提供支持。每条供电线的电压和电流额定值都列在设备的标签上。

必须在待安装 FireSIGHT 系统的网络设备输入端安装一个外部浪涌保护装置。

不同电路分开安装

如果使用了不同的电路，每条电路的额定值必须满足设备的最大额定值范围。此配置可在电路故障和电源故障时提供保护。

示例：每条供电线都另附一条 220 V 电路。每条电路必须能够提供 5 A 电流，如标签上的说明。

相同电路安装

如果使用同一条电路向两条供电线供电，则其中一条供电线的额定功率适用于整个箱体。此配置只在电源故障时提供保护。

示例：两条供电线连接到同一条 220 V 电路。此电路的最大牵引电流是 5 A，如标签上的说明。

电压

电源在以下电压范围中可正常工作：100 VAC 到 240 VAC 标称值 （极限范围是 85 VAC 到 264 VAC）。电压超过此范围可能导致设备损坏。

电流

每条供电线标记的额定电流：在整个运行条件范围内，最大为 10 A；从 187 VAC 到 264 VAC，在整个运行条件范围内，最大为 5 A。必须使用合适的电线和断路器减少火灾风险。

频率范围

交流电电源的频率范围为 47 Hz - 63 Hz。频率超过此范围可能导致设备停止运行或非正常运行。

电源线

供电线的电源连接采用 IEC C14 连接器，也可使用 IEC C13 连接器。必须使用 UL 认证的电源线。最小线规是 16 AWG。设备随附的电线是 16 AWG， UL 认证电线及 NEMA 515P 插座。如需其他电源线，请与工厂联系。

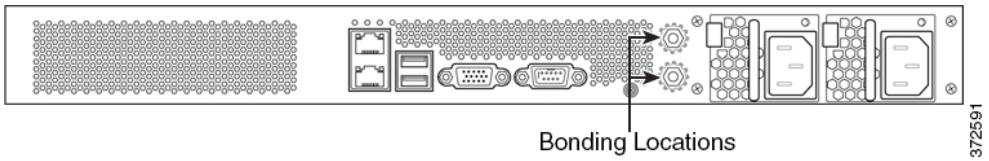
接地要求

FireSIGHT 系统必须与公共连接网连接实现接地。

连接位置

在机箱后面有多个接地连接位置。随附 M4 螺栓。随附有齿轮向外的锁紧垫圈，以将其固定到环状端子。每个螺栓都有一个标准的接地符号。

下图显示机箱上的连接位置。



推荐端子

必须使用 UL 认证的端子进行接地连接。可以使用环状端子，该端子带有一个适合 4 毫米或 #8 螺栓的穿通孔。对于 10 - 12 AWG 电线，建议使用 Tyco 34853。这种 UL 认证的环状端子带有一个适合 #8 螺栓的穿通孔。

地线要求

地线必须大小合适，以便出现单次故障时可以有效地处理电路的电流。地线的大小应与保护电路的断路器电流一致。请参阅电流，第 A-4 页。

在压接连接之前，必须为裸导线涂一层抗氧剂。只有铜缆可用于接地。

81xx 子系列设备

本章节介绍下列思科设备的电源要求：

- 3D8120、 3D8130 和 3D8140 （CHAS-1U-AC、 CHAS-1U-DC 或 CHAS-1U-AC/DC）

这些思科设备适合由合格人员安装在符合国家电气规范的网络电信设施和位置中。

思科建议您保留包装材料，以防需要退换货时使用。

有关详细信息，请参阅以下各节：

- 请参阅交流安装，第 A-6 页，以了解关于电路安装、电压、电流、频率范围和电源线的详细信息。
- 请参阅直流安装，第 A-7 页，以了解关于电路安装、电压、电流、地线基准、端子、断路器要求和最小电线尺寸的详细信息。
- 请参阅接地要求，第 A-8 页，以了解关于连接位置、推荐端子、地线要求和直流电供电线的详细信息。

交流安装

FireSIGHT 系统安装必须遵循美国国家电气规范 (NEC) 手册 NFPA 70 第 250 款以及当地电气规范的要求。

注意事项 请勿将直流电源与交流电供电线进行连接。

需将不同电路分开，以创建冗余的电源。使用不间断电源或电池备用电源，防止由于输入线电源故障造成的电源状态问题或电源损失。

向每条电源提供充足的电力，为整个设备运行提供支持。每条供电线的电压和电流额定值都列在设备的标签上。

必须在待安装 FireSIGHT 系统的网络设备输入端安装一个外部浪涌保护装置。

不同电路分开安装

如果使用了不同的电路，每条电路的额定值必须满足设备的最大额定值范围。此配置可在电路故障和电源故障时提供保护。

示例：每条供电线都另附一条 220 V 电路。每条电路必须能够提供 5 A 电流，如标签上的说明。

相同电路安装

如果使用同一条电路向两条供电线供电，则其中一条供电线的额定功率适用于整个箱体。此配置只在电源故障时提供保护。

示例：两条供电线连接到同一条 220 V 电路。此电路的最大牵引电流是 5 A，如标签上的说明。

交流电压

电源在以下电压范围中可正常工作：100 VAC 到 240 VAC 标称值 （极限范围是 85 VAC 到 264 VAC）。电压超过此范围可能导致设备损坏。

交流电流

每条供电线标记的额定电流：在整个运行条件范围内，最大为 5.2 A；从 187 VAC 到 264 VAC，在整个运行条件范围内，最大为 2.6 A。必须使用合适的电线和断路器减少火灾风险。

频率范围

交流电电源的频率范围为 47 Hz - 63 Hz。频率超过此范围可能导致设备停止运行或非正常运行。

电源线

供电线的电源连接采用 IEC C14 连接器，也可使用 IEC C13 连接器。必须使用 UL 认证的电源线。最小线规是 16 AWG。设备随附的电线是 16 AWG， UL 认证电线及 NEMA 515P 插座。如需其他电源线，请与工厂联系。

直流安装

需将不同电路分开，以创建冗余的电源。使用不间断电源或电池备用电源，防止由于输入线电源故障造成的电源状态问题或电源损失。

注意事项 请**勿**将交流电源与直流电供电线进行连接。

向每条电源提供充足的电力，为整个设备运行提供支持。每条供电线的电压和电流额定值都列在设备的标签上。

必须在待安装 FireSIGHT 系统的网络设备输入端安装一个外部浪涌保护装置。

不同电路分开安装

如果使用了不同的电路，每条电路的额定值必须满足设备的最大额定值范围。此配置可在电路故障和电源故障时提供保护。

示例：每条供电线都另附一条 -48 VDC 电路。每条电路必须能够提供 20 A 电流，如标签上的说明。

相同电路安装

如果使用同一条电路向两条供电线供电，则其中一条供电线的额定功率适用于整个箱体。此配置只在电源故障时提供保护。

示例：两条供电线连接到同一条 –48 VDC 电路。此电路的最大牵引电流是 20 A，如标签上的说明。

注意事项 使用这个优化功能需要将供电线的额定值设定为每条电源的最高额定值。

直流电压

电源在下列电压下可以正常工作：

- -48 VDC 标称值基准到 RTN。
- 极限范围为 -40 VDC 到 -72 VDC

电压超过此范围可能导致设备损坏。

直流电流

每条供电线最高 11 A。

接地基准

直流电源与接地基准完全隔离。

推荐端子

将电源通过螺栓型端子连接到直流电源。端子必须获得 UL 认证。端子必须带有一个适合 M4 或 #8 螺钉的孔。端子的最大宽度为 8.1 毫米（0.32 英寸）。10 - 12 号标准线的典型扁形接头是 Tyco 325197。

断路器要求

必须配备一个断路器，此断路器在额定电压下可以有效传送额定电流。断路器必须满足以下要求：

- 通过 UL 认证
- 通过 CSA 认证 （推荐）
- 通过 VDE 认证 （推荐）
- 支持最大负载 (20 A)
- 支持安装电压 （电源要求范围是 -40 V 到 -72 VDC）
- 直流电使用额定电流

推荐断路器：Airpax IELK1-1-72-20.0-01-V 使用的端子选项取决于安装类型。此断路器是一个单极的 20 A 断路器，带有 80 V 的额定直流电。它有一个*长时延迟*。有关此断路器的详细信息，可访问 http://www.airpax.net/site/utilities/eliterature/pdfs/ial.pdf。

最低线号要求

有三条电线 （一条电路）的电源供电每个线槽可以使用 12 AWG 电线。有一条以上电路的电源供电每个线槽可以使用 10 AWG 电线。请注意，冗余供电线的两条单独供电需要两条电路，必须使用 10 AWG 电线。

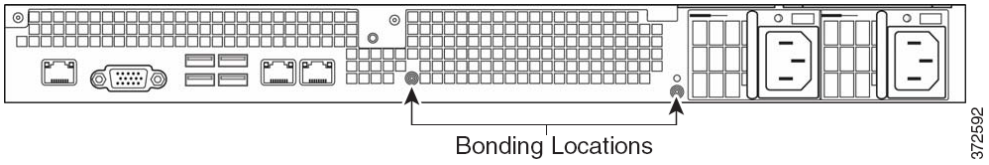
接地要求

FireSIGHT 系统必须与公共连接网连接实现接地。

连接位置

在机箱后面有多个接地连接位置。随附 M4 螺栓。随附有齿轮向外的锁紧垫圈，以将其固定到环状端子。每个螺栓都有一个标准的接地符号。

下图显示 1U 机箱上的连接位置。



推荐端子

必须使用 UL 认证的端子进行接地连接。可以使用环状端子，该端子带有一个适合 4 毫米或 #8 螺栓的穿通孔。对于 10 - 12 AWG 电线，建议使用Tyco 34853。这种 UL 认证的环状端子带有一个适合 #8 螺栓的穿通孔。

地线要求

地线必须大小合适，以便出现单次故障时可以有效地处理电路的电流。地线的大小应与保护电路的断路器电流一致。有关交流电电路的详细信息，请参阅交流电流，第 A-6 页。有关直流电电路的详细信息，请参阅直流电流，第 A-7 页。

在压接连接之前，必须为裸导线涂一层抗氧剂。只有铜缆可用于接地。

直流电供电线

直流电供电线的每条供电线上都有附加的接地连接。这可以使连接的热插拔供电线连接电源、回路和接地，以便安全插入。必须附上此接地片。

它是一个带齿轮向外锁紧垫圈螺丝的 M4 螺丝。

接地线尺寸应与电路的断路器相匹配。

82xx 子系列设备

本章节介绍下列思科设备的电源要求：

- 3D8250、 3D8260、 3D8270 和 3D8290 （CHAS-2U-AC、 CHAS-2U-DC 或 CHAS-2U-AC/DC）

这些思科设备适合由合格人员安装在符合国家电气规范的网络电信设施和位置中。

思科建议您保留包装材料，以防需要退换货时使用。

有关详细信息，请参阅以下各节：

- 请参阅交流安装，第 A-9 页，以了解关于电路安装、电压、电流、频率范围和电源线的详细信息。
- 请参阅直流安装，第 A-10 页，以了解关于电路安装、电压、电流、地线基准、端子、断路器要求和最小电线尺寸的详细信息。
- 请参阅接地要求，第 A-12 页，以了解关于连接位置、推荐端子、地线要求和直流电供电线的详细信息。

交流安装

FireSIGHT 系统安装必须遵循美国国家电气规范 (NEC) 手册 NFPA 70 第 250 款以及当地电气规范的要求。

注意事项 请勿将直流电源与交流电供电线进行连接。

需将不同电路分开，以创建冗余的电源。使用不间断电源或电池备用电源，防止由于输入线电源故障造成的电源状态问题或电源损失。

向每条电源提供充足的电力，为整个设备运行提供支持。每条供电线的电压和电流额定值都列在设备的标签上。

必须在待安装 FireSIGHT 系统的网络设备输入端安装一个外部浪涌保护装置。

不同电路分开安装

如果使用了不同的电路，每条电路的额定值必须满足设备的最大额定值范围。此配置可在电路故障和电源故障时提供保护。

示例：每条供电线都另附一条 220 V 电路。每条电路必须能够提供 5 A 电流，如标签上的说明。

相同电路安装

如果使用同一条电路向两条供电线供电，则其中一条供电线的额定功率适用于整个箱体。此配置只在电源故障时提供保护。

示例：两条供电线连接到同一条 220 V 电路。此电路的最大牵引电流是 5 A，如标签上的说明。

交流电压

电源在以下电压范围中可正常工作：100 VAC 到 240 VAC 标称值 （极限范围是 85 VAC 到 264 VAC）。电压超过此范围可能导致设备损坏。

交流电流

每条供电线标记的额定电流：在整个运行条件范围内，最大为 8 A；从 187 VAC 到 264 VAC，在整个运行条件范围内，最大为 4 A。必须使用合适的电线和断路器减少火灾风险。

频率范围

交流电电源的频率范围为 47 Hz - 63 Hz。频率超过此范围可能导致设备停止运行或非正常运行。

电源线

供电线的电源连接采用 IEC C14 连接器，也可使用 IEC C13 连接器。必须使用 UL 认证的电源线。最小线规是 16 AWG。设备随附的电线是 16 AWG， UL 认证电线及 NEMA 515P 插座。如需其他电源线，请与工厂联系。

直流安装

需将不同电路分开，以创建冗余的电源。使用不间断电源或电池备用电源，防止由于输入线电源故障造成的电源状态问题或电源损失。

⚠

注意事项 请**勿**将交流电源与直流电供电线进行连接。

向每条电源提供充足的电力，为整个设备运行提供支持。每条供电线的电压和电流额定值都列在设备的标签上。

必须在待安装 FireSIGHT 系统的网络设备输入端安装一个外部浪涌保护装置。

不同电路分开安装

如果使用了不同的电路，每条电路的额定值必须满足设备的最大额定值范围。此配置可在电路故障和电源故障时提供保护。

示例：每条供电线都另附一条 -48 VDC 电路。每条电路必须能够提供 20 A 电流，如标签上的说明。

相同电路安装

如果使用同一条电路向两条供电线供电，则其中一条供电线的额定功率适用于整个箱体。此配置只在电源故障时提供保护。

示例：两条供电线连接到同一条 -48 VDC 电路。此电路的最大牵引电流是 20 A，如标签上的说明。

注意事项 使用这个优化功能需要将供电线的额定值设定为每条电源的最高额定值。

直流电压

电源在下列电压下可以正常工作：

- -48 VDC 标称值基准到 RTN。
- 极限范围为 -40 VDC 到 -72 VDC

电压超过此范围可能导致设备损坏。

直流电流

每条供电线最高 18 A。

接地基准

直流电源与接地基准完全隔离。

推荐端子

将电源通过螺栓型端子连接到直流电源。端子必须获得 UL 认证。端子必须带有一个适合 M4 或 #8 螺钉的孔。端子的最大宽度为 8.1 毫米 （0.32 英寸）。 10 - 12 号标准线的典型扁形接头是 Tyco 325197。

断路器要求

必须配备一个断路器，此断路器在额定电压下可以有效传送额定电流。断路器必须满足以下要求：

- 通过 UL 认证
- 通过 CSA 认证 （推荐）
- 通过 VDE 认证 （推荐）
- 支持最大负载 (20 A)
- 支持安装电压 （电源要求范围是 -40 V 到 -72 VDC）
- 直流电使用额定电流

推荐断路器：Airpax IELK1-1-72-20.0-01-V 使用的端子选项取决于安装类型。此断路器是一个单极的 20 A 断路器，带有 80 V 的额定直流电。它有一个*长时延迟*。有关此断路器的详细信息，可访问 http://www.airpax.net/site/utilities/eliterature/pdfs/ial.pdf。

最低线号要求

有三条电线（一条电路）的电源供电每个线槽可以使用 12 AWG 电线。有一条以上电路的电源供电每个线槽可以使用 10 AWG 电线。请注意，冗余供电线的两条单独供电需要两条电路，必须使用 10 AWG 电线。

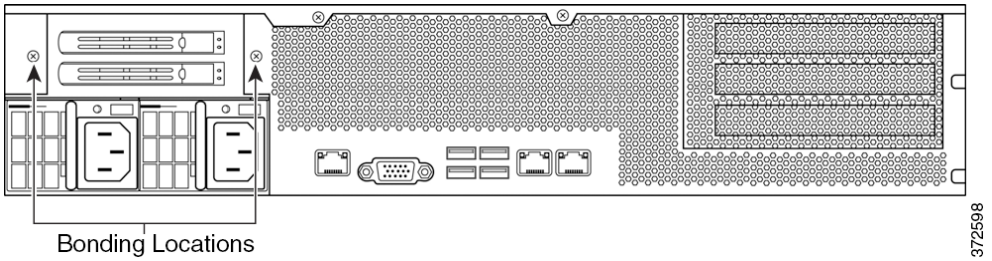
接地要求

FireSIGHT 系统必须与公共连接网连接实现接地。

连接位置

在机箱后面有多个接地连接位置。随附 M4 螺栓。随附有齿轮向外的锁紧垫圈，以将其固定到环状端子。每个螺栓都有一个标准的接地符号。

下图显示 2U 机箱上的连接位置。



推荐端子

必须使用 UL 认证的端子进行接地连接。可以使用环状端子，该端子带有一个适合 4 毫米或 #8 螺栓的穿通孔。对于 10 - 12 AWG 电线，建议使用 Tyco 34853。这种 UL 认证的环状端子带有一个适合 #8 螺栓的穿通孔。

地线要求

地线必须大小合适，以便出现单次故障时可以有效地处理电路的电流。地线的大小应与保护电路的断路器电流一致。有关交流电电路的详细信息，请参阅交流电流，第 A-6 页。有关直流电电路的详细信息，请参阅直流电流，第 A-7 页。

在压接连接之前，必须为裸导线涂一层抗氧剂。只有铜缆可用于接地。

直流电供电线

直流电供电线的每条供电线上都有附加的接地连接。这可以使连接的热插拔供电线连接电源、回路和接地，以便安全插入。必须附上此接地片。

它是一个带齿轮向外锁紧垫圈螺丝的 M4 螺丝。

接地线尺寸应与电路的断路器相匹配。

83xx 子系列设备

本章节介绍下列思科设备的电源要求：

- 3D8350、 3D8360、 3D8370 和 3D8390 (PG35-2U-AC/DC)

这些思科设备适合由合格人员安装在符合国家电气规范的网络电信设施和位置中。

思科建议您保留包装材料，以防需要退换货时使用。

有关详细信息，请参阅以下各节：

- 请参阅交流安装，第 A-13 页，以了解关于电路安装、电压、电流、频率范围和电源线的详细信息。
- 请参阅直流安装，第 A-14 页，以了解关于电路安装、电压、电流、地线基准、端子、断路器要求和最小电线尺寸的详细信息。
- 请参阅接地要求，第 A-15 页，以了解关于连接位置、推荐端子、地线要求和直流电供电线的详细信息。

交流安装

FireSIGHT 系统安装必须遵循美国国家电气规范 (NEC) 手册 NFPA 70 第 250 款以及当地电气规范的要求。

注意事项 请**勿**将直流电源与交流电供电线进行连接。

需将不同电路分开，以创建冗余的电源。使用不间断电源或电池备用电源，防止由于输入线电源故障造成的电源状态问题或电源损失。

向每条电源提供充足的电力，为整个设备运行提供支持。每条供电线的电压和电流额定值都列在设备的标签上。

必须在待安装 FireSIGHT 系统的网络设备输入端安装一个外部浪涌保护装置。

不同电路分开安装

如果使用了不同的电路，每条电路的额定值必须满足设备的最大额定值范围。此配置可在电路故障和电源故障时提供保护。

示例：每条供电线都另附一条 220 V 电路。每条电路必须能够提供 10 A 电流，如标签上的说明。

相同电路安装

如果使用同一条电路向两条供电线供电，则其中一条供电线的额定功率适用于整个箱体。此配置只在电源故障时提供保护。

示例：两条供电线连接到同一条 220 V 电路。此电路的最大牵引电流是 10 A，如标签上的说明。

交流电压

电源在以下电压范围中可正常工作：100 VAC 到 240 VAC 标称值 （极限范围是 85 VAC 到 264 VAC）。电压超过此范围可能导致设备损坏。

交流电流

每条供电线标记的额定电流：在整个运行条件范围内，最大为 11 A；从 187 VAC 到 264 VAC，在整个运行条件范围内，最大为 5.5 A。必须使用合适的电线和断路器减少火灾风险。

频率范围

交流电电源的频率范围为 47 Hz - 63 Hz。频率超过此范围可能导致设备停止运行或非正常运行。

电源线

供电线的电源连接采用 IEC C14 连接器，也可使用 IEC C13 连接器。必须使用 UL 认证的电源线。最小线规是 16 AWG。设备随附的电线是 16 AWG， UL 认证电线及 NEMA 515P 插座。如需其他电源线，请与工厂联系。

直流安装

需将不同电路分开，以创建冗余的电源。使用不间断电源或电池备用电源，防止由于输入线电源故障造成的电源状态问题或电源损失。

注意事项 请**勿**将交流电源与直流电供电线进行连接。

向每条电源提供充足的电力，为整个设备运行提供支持。每条供电线的电压和电流额定值都列在设备的标签上。

必须在待安装 FireSIGHT 系统的网络设备输入端安装一个外部浪涌保护装置。

不同电路分开安装

如果使用了不同的电路，每条电路的额定值必须满足设备的最大额定值范围。此配置可在电路故障和电源故障时提供保护。

示例：每条供电线都另附一条 -48 VDC 电路。每条电路必须能够提供 25 A 电流，如标签上的说明。

相同电路安装

如果使用同一条电路向两条供电线供电，则其中一条供电线的额定功率适用于整个箱体。此配置只在电源故障时提供保护。

示例：两条供电线连接到同一条 –48 VDC 电路。此电路的最大牵引电流是 25 A，如标签上的说明。

注意事项 使用这个优化功能需要将供电线的额定值设定为每条电源的最高额定值。

直流电压

电源在下列电压下可以正常工作：

- -48 VDC 标称值基准到 RTN。
- 极限范围为 -40 VDC 到 -72 VDC

电压超过此范围可能导致设备损坏。

直流电流

每条供电线最高 25 A。

接地基准

直流电源与接地基准完全隔离。

推荐端子

将电源通过螺栓型端子连接到直流电源。端子必须获得 UL 认证。端子必须带有一个适合 M4 或 #8 螺钉的孔。端子的最大宽度为 8.1 毫米（0.32 英寸）。10 - 12 号标准线的典型扁形接头是 Tyco 325197。

断路器要求

必须配备一个断路器，此断路器在额定电压下可以有效传送额定电流。断路器必须满足以下要求：

- 通过 UL 认证
- 通过 CSA 认证 （推荐）
- 通过 VDE 认证 （推荐）
- 支持最大负载 (20 A)
- 支持安装电压 （电源要求范围是 -40 V 到 -72 VDC）
- 直流电使用额定电流

推荐断路器：Airpax IELK1-1-72-20.0-01-V 使用的端子选项取决于安装类型。此断路器是一个单极的 20 A 断路器，带有 80 V 的额定直流电。它有一个 *长时延迟*。有关此断路器的详细信息，可访问 http://www.airpax.net/site/utilities/eliterature/pdfs/ial.pdf。

最低线号要求

有三条电线 （一条电路）的电源供电每个线槽可以使用 12 AWG 电线。有一条以上电路的电源供电每个线槽可以使用 10 AWG 电线。请注意，冗余供电线的两条单独供电需要两条电路，必须使用 10 AWG 电线。

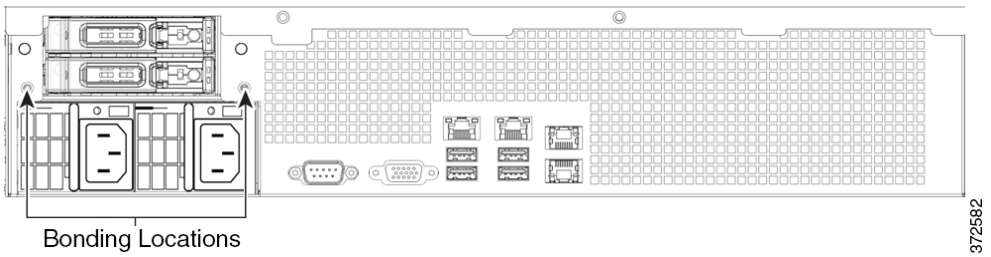
接地要求

FireSIGHT 系统必须与公共连接网连接实现接地。

连接位置

在机箱后面有多个接地连接位置。随附 M4 螺栓。随附有齿轮向外的锁紧垫圈，以将其固定到环状端子。每个螺栓都有一个标准的接地符号。

下图显示 83xx 子系列 2U 机箱上的连接位置。



推荐端子

必须使用 UL 认证的端子进行接地连接。可以使用环状端子，该端子带有一个适合 4 毫米或 #8 螺栓的穿通孔。对于 10 - 12 AWG 电线，建议使用 Tyco 34853。这种 UL 认证的环状端子带有一个适合 #8 螺栓的穿通孔。

地线要求

地线必须大小合适，以便出现单次故障时可以有效地处理电路的电流。地线的大小应与保护电路的断路器电流一致。有关交流电电路的详细信息，请参阅交流电流，第 A-14 页。有关直流电电路的详细信息，请参阅直流电流，第 A-15 页。

在压接连接之前，必须为裸导线涂一层抗氧剂。只有铜缆可用于接地。

直流电供电线

直流电供电线的每条供电线上都有附加的接地连接。这可以使连接的热插拔供电线连接电源、回路和接地，以便安全插入。必须附上此接地片。

它是一个带齿轮向外锁紧垫圈螺丝的 M4 螺丝。

接地线尺寸应与电路的断路器相匹配。

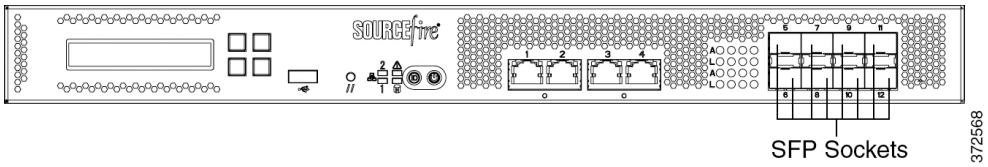
在 3D71x5 和 AMP7150 设备中使用 SFP 收发器

以下节介绍关于在 3D7115 和 3D7125（统称 3D71x5）和 AMP7150 中使用小型可插拔 (SFP) 插槽和收发器的详细信息。

3D71x5 和 AMP7150 SFP 插槽和收发器

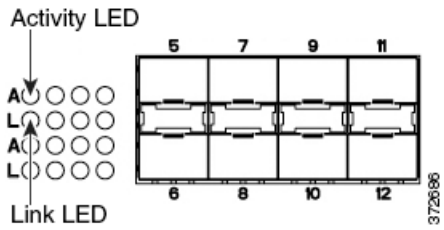
3D71x5 和 AMP7150 设备包含八个小型可插拔 (SFP) 插槽，最多可以容纳八个 SFP 收发器。

图 B-1　　3D71x5 和 AMP7150 前视图



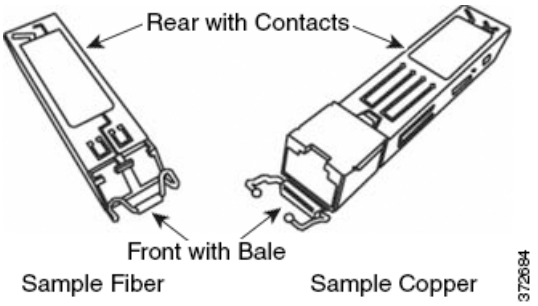
3D71x5 和 AMP7150 SFP 插槽

八个 SFP 插槽垂直从上往下依次编号为 5 至 12，采用中心分流式方向配置 （即上排朝上，下排朝下）。



插槽左侧随附的 LED 显示每个接口的活动和链路信息。有关详细信息，请参阅表 6-473D7115、3D7125 和 AMP7150 SFP 插槽活动/链路 LED，第 6-29 页。

SFP 收发器示例



3D71x5 和 AMP7150 最多可支持按照任意以下三种形式组合的八个 SFP 收发器：

- SFP-C-1：铜收发器
- SFP-F-1-SR：短距离光纤收发器
- SFP-F-1-LR：远距离光纤收发器

在 3D71x5 和 AMP7150 中只能使用思科 SFP 收发器。非思科 SFP 收发器可能会卡在插槽中，可能对收发器、机箱或两者造成永久性损坏。

可以在设备正常运行时插入或移除收发器。在防御中心上刷新用户界面来查看配置中的更改。

SFP 收发器没有旁路功能。在被动部署或内联部署中，如果想要在设备出现故障或丧失电源时让设备断开所有流量（例如虚拟交换机、虚拟路由器和某些访问控制策略），可以使用这些收发器。

对于被动部署，可以在八个插槽中使用任意组合的收发器监控最多八个网段。对于内联部署，可以在从上往下垂直排序的插槽（5 和 6、7 和 8、9 和 10 或 11 和 12）中使用任意组合形式（铜、光纤或混合形式）的收发器监控四个网段。

使用管理设备的防御中心在收发器上配置端口。

插入 SFP 收发器

插入收发器时，请采取适当的静电释放 (ESD) 措施。避免接触后面的触点，并且避免触点和端口沾染灰尘和污垢。

注意事项 不要强制将 SFP 收发器插入插槽中，否则可能会堵塞收发器，并且可能对收发器、机箱或两者造成永久性损坏。

要插入 SFP 收发器，请执行以下操作：

步骤 1 注意不要接触后面的触点，用手指抓住手柄两侧，然后将收发器后端滑入机箱上的插槽中。请注意，上排的插槽朝上，下排的插槽朝下。

步骤 2 轻轻地向收发器方向推动手柄，使手柄闭合，然后接合锁定机构，将收发器固定到位。

步骤 3 按照安装 FireSIGHT 系统设备，第 3-1 页中的程序在收发器上配置端口。

请注意，如果向运行中的设备插入收发器，必须在防御中心上刷新用户界面来查看更改。

移除 SFP 收发器

移除收发器时，请采取适当的静电释放 (ESD) 措施。避免接触后面的触点，并且避免触点和端口沾染灰尘和污垢。

要移除 SFP 收发器，请执行以下操作：

步骤 1 从收发器上断开想要从设备上移除的所有电缆。

步骤 2 用手指轻轻地从收发器中拉出手柄，断开连接机构。

对于上排的收发器，请向下拉。对于下排的收发器，请向上提。

步骤 3 用手指抓住手柄侧面，轻轻地从机箱中将收发器拉出来，注意不要接触收发器后面的触点。

插入和拆卸 8000 系列模块

8000 系列设备允许在部署中实现模块化灵活性。使用本节中的步骤：

- 在设备中插入新的模块
- 拆卸或更换设备上预安装的模块

以下节将介绍如何插入、拆卸或更换 8000 系列模块：

8000 系列设备上的模块插槽

8000 系列设备可在以下插槽中使用这些模块：

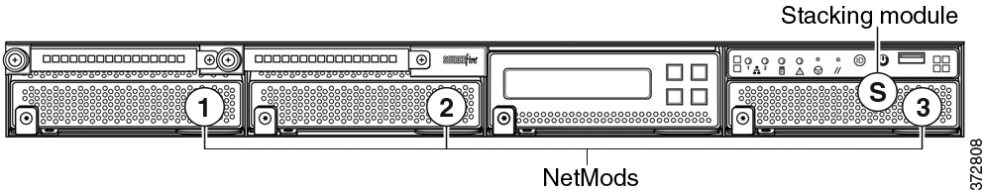
将模块插入设备后，有关使用模块的详细信息，请参阅以下节：

- 有关配置感应接口的信息，请参阅识别感应接口，第 3-4 页。
- 有关使用堆叠模块的信息，请参阅在堆叠配置中使用设备，第 3-13 页。

81xx 子系列

81xx 子系列设备可在以下插槽中使用这些模块：

图 C-1 81xx 系列主要设备



堆叠配置注意事项

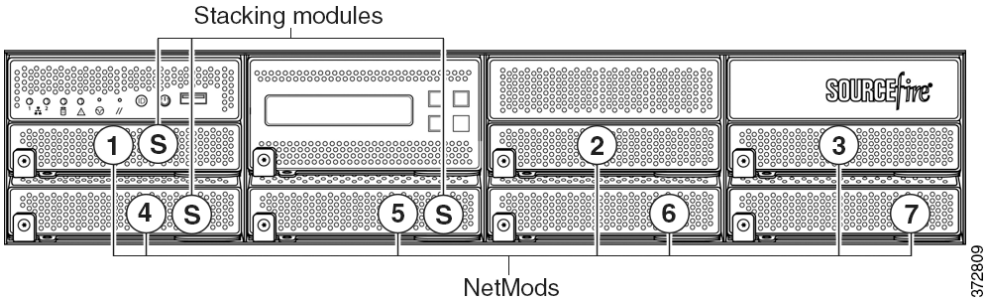
按照如下说明为堆叠设备配置模块：

- 仅在主要设备上安装 NetMod。
- 在主要设备上安装一个堆叠模块并在辅助设备上安装一个堆叠模块。

82xx 子系列和 83xx 子系列

82xx 子系列和 83xx 子系列设备可在以下插槽中使用这些模块：

图 C-2 82xx 子系列和 83xx 子系列主要设备

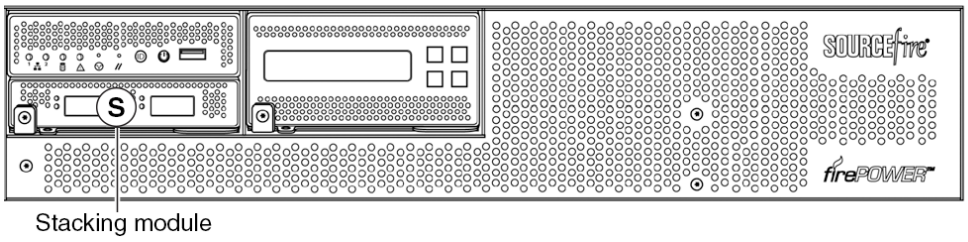


堆叠配置注意事项

按照如下说明为堆叠设备配置模块：

- 仅在主要设备上安装 NetMod。
- 在主要设备上为每个堆叠辅助设备安装一个堆叠模块，并在每个辅助设备上安装一个堆叠模块。

图 C-3 82xx 子系列和 83xx 子系列辅助设备



随附项目

模块组合套件包括一把 T8 花形螺丝起子和以下一个或多个模块：

- 四端口 1000BASE-T 铜可配置旁路 NetMod。有关详细信息，请参阅四端口 1000BASE-T 铜可配置旁路网络模块，第 6-42 页。
- 四端口千兆位光纤可配置旁路 NetMod。有关详细信息，请参阅四端口 1000BASE-SX 光纤可配置旁路网络模块，第 6-43 页。
- 双端口 10GBASE（MMSR 或 SMLR）光纤可配置旁路 NetMod。有关详细信息，请参阅双端口 10GBASE（MMSR 或 SMLR）光纤可配置旁路网络模块，第 6-44 页。
- 双端口 40GBASE-SR4 光纤可配置旁路 NetMod。有关详细信息，请参阅双端口 40GBASE-SR4 光纤可配置旁路网络模块，第 6-46 页。

注 仅可在 40G 容量的 3D8250 或 3D8350 上使用此双插槽 NetMod。如果需要升级设备，请参阅《*思科 8000 系列 40G 容量设备升级指南*》。

- 四端口 1000BASE-T 铜可配置旁路 NetMod。有关详细信息，请参阅四端口 1000BASE-T 铜可配置旁路网络模块，第 6-47 页。
- 四端口 1000BASE-SX 光纤非旁路 NetMod。四端口 1000BASE-SX 光纤非旁路 NetMod。有关详细信息，请参阅四端口 1000BASE-SX 光纤可配置旁路网络模块，第 6-48 页。
- 四端口 10GBASE（MMSR 或 SMLR）光纤非旁路 NetMod。有关详细信息，请参阅四端口 10GBASE（MMSR 或 SMLR）光纤非旁路网络模块，第 6-49 页。

注意事项 四端口 10GBASE 光纤非旁路 NetMod 包含不可移动的小型可插拔 (SFP) 收发器。尝试拆卸 SFP 可能会损坏模块。

- 堆叠模块。有关详细信息，请参阅堆叠模块，第 6-50 页。

尝试配置 NetMod 时，如果在设备的不兼容插槽安装 NetMod 或 NetMod 与系统不兼容，管理防御中心的网络界面将显示错误或警告消息。如需帮助，请联系支持部门。

注 更换 NetMod 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，请参阅该设备的原始配置文档以及 *“FirePOWER 和 FireSIGHT 设备的监管合规和安全信息 (Regulatory Compliance and Safety Information for FirePOWER and FireSIGHT Appliances)”* 文件。

识别模块零件

无论模块的检测接口、速度或大小如何，所有模块都包含相同的零件。

图 C-4 示例模块或插槽盖 （打开状态）

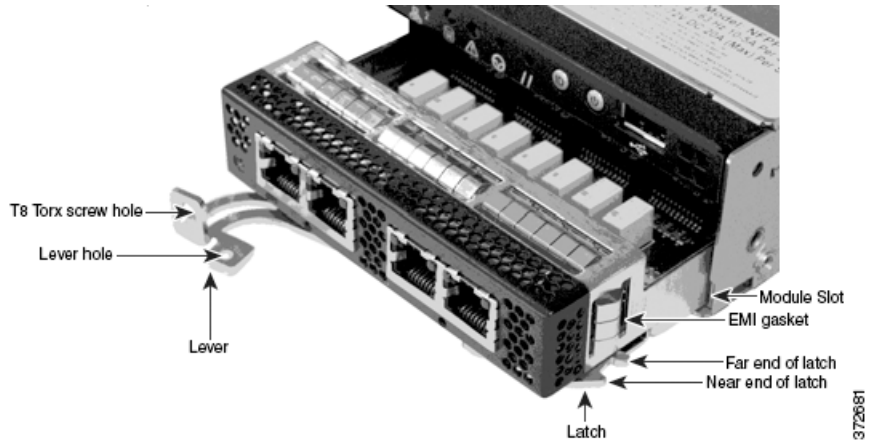
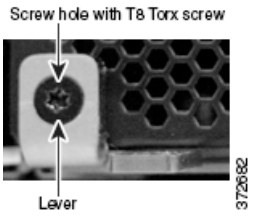


图 C-5 示例模块操纵杆 （闭合状态，孔内安装了螺丝）



准备工作

根据以下说明，准备插入或拆卸模块：

- 标识所有设备和模块零件。
- 标识要安装 NetMod 的插槽。

提示 可以将 NetMod 插入任何可用的兼容插槽。

- 确定堆叠模块正确的插槽。请参阅在堆叠配置中使用设备，第 3-13 页。
- 3D8140：插槽 3
- 3D8250、 3D8260 和 3D8350、 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 次插槽：插槽 S
- 确认 EMI 垫圈安装到位。
- 拔出设备的所有电源线。

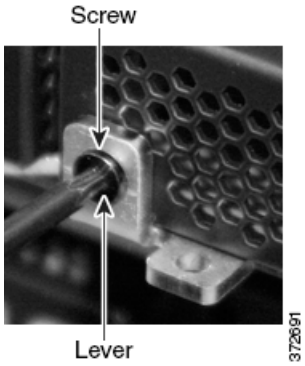
注意事项 这些模块**不可**热插拔。插入或拆卸模块之前，必须断开电源并从设备拔出**两根**电源线。

拆卸模块或插槽盖

处理模块时，适当进行静电释放 (ESD)，比如佩戴腕带和使用 ESD 工作台。将未使用的模块存储在静电屏蔽袋或防静电箱中，防止损坏。

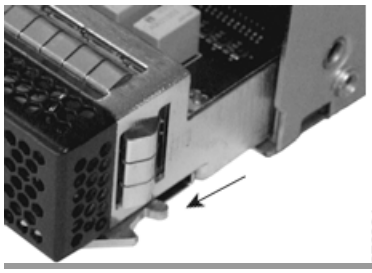
要拆卸模块或插槽盖，请执行以下操作：

步骤 1 使用随附的螺丝刀从模块操纵杆拆卸 T8 梅花头螺钉并保留备用。



步骤 2 从模块上抽出操纵杆，松开闩锁。

步骤 3 从插槽中滑出模块。

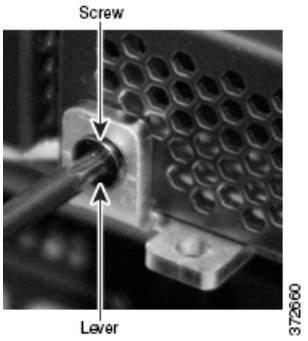


插入模块或插槽盖

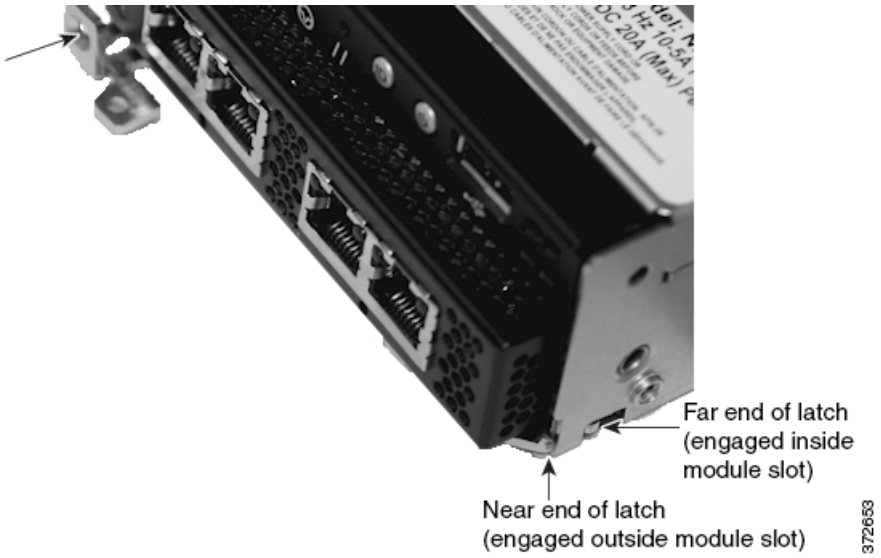
拆卸现有模块或插槽盖，准备插入新模块。有关详细信息，请参阅拆卸模块或插槽盖，第 C-5 页。

要插入模块或插槽盖：

步骤 1 使用随附的螺丝刀从模块操纵杆拆卸 T8 梅花头螺钉并保留备用。

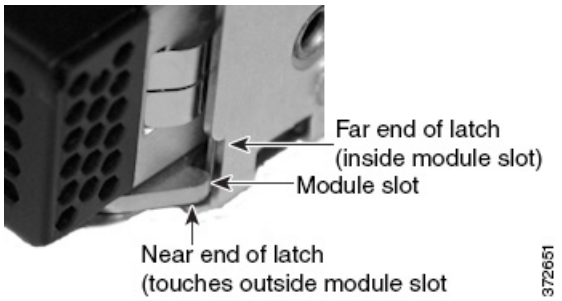


步骤 2 从模块上抽出操纵杆，打开闩锁。露出闩锁的近端。闩锁的远端留在模块。

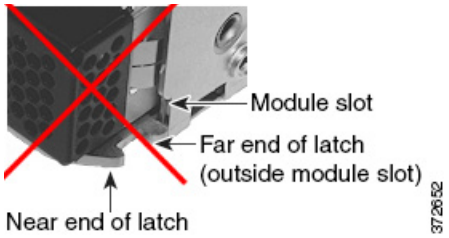


步骤 3 将模块插入插槽，直至闩锁的远端进入插槽内，并且闩锁的近端能碰到模块插槽的外部。

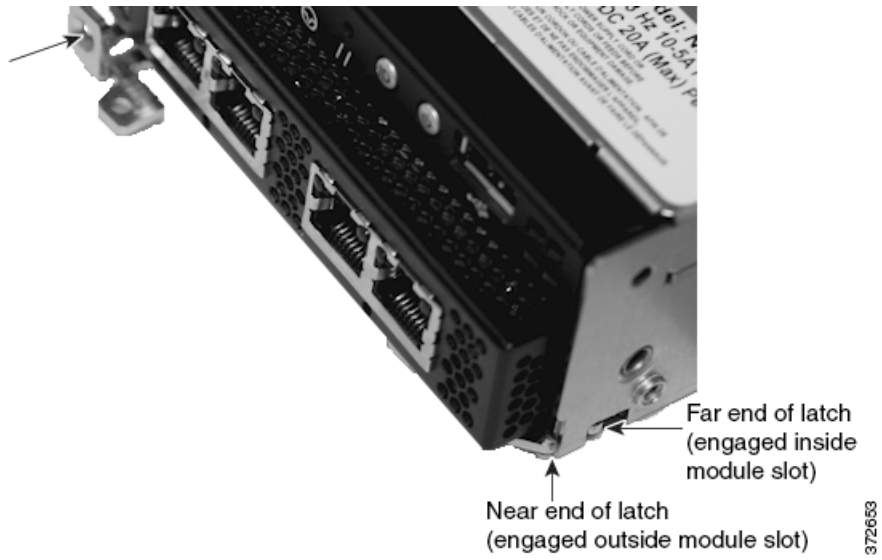
正确的模块安装



不正确的模块安装



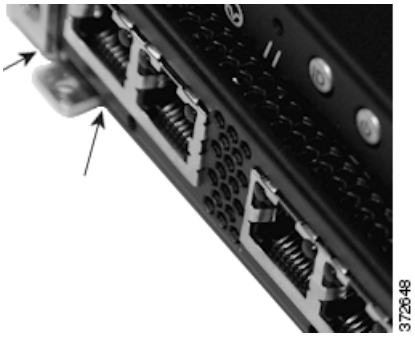
步骤 4 朝模块方向推送模块操纵杆，使闩锁啮合并将模块拉入插槽。



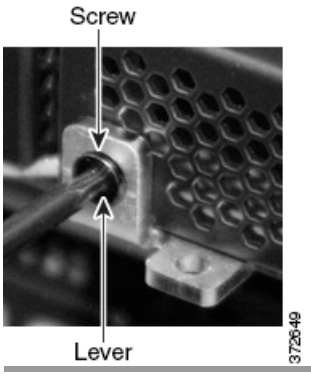
注意事项 请勿用力过猛。如果闩锁不能啮合，请拆卸并重新调整模块，然后重试。

步骤 5 用力按压螺丝孔，使操纵杆完全紧靠模块以固定闩锁。

操纵杆完全紧靠模块，并且模块与机箱齐平。



步骤 6 将保留的 T8 梅花头螺钉插入操纵杆并拧紧。



清理硬盘驱动器

可以安全地清理大多数防御中心上的硬盘驱动器，确保无法再访问其内容。如果需要返回包含敏感数据的缺陷设备，可以使用此功能覆盖数据。

清理硬盘驱动器的内容

支持的设备：任意

支持的防御中心：除 DC1000、 DC3000 外的所有型号

这种清理磁盘的模式符合以下军事标准：

标准

DoD 清理程序符合整理移动式和非移动式刚性磁盘的 DoD 5220.22-M 规程，其要求用其一个字符、字符补码然后是一个任意字符覆盖所有可寻址位置，并进行验证。有关其他限制，请参阅 DoD 文档。

注意事项 清理硬盘驱动器会导致丢失设备上的**所有**数据，使设备无法运行。

使用使用交互式菜单还原设备，第 7-7 页中描述的交互式菜单选项清理硬盘驱动器。

要清理硬盘驱动器，请执行以下操作：

访问：管理员

步骤 1 执行以下小节之一的说明显示还原实用程序的交互式菜单，具体取决于访问设备的方式：

- 使用 KVM 或物理串行端口启动还原实用程序，第 7-5 页
- 使用无人值守管理启动还原实用程序，第 7-6 页

注意 DC1000 和 DC3000 不支持此功能。

步骤 2 在主菜单上选择 **8 Wipe Contents of Disk**。

步骤 3 系统提示时，请确认想要清理硬盘驱动器。

硬盘驱动器清理成功。清理流程可能需要数小时才能完成；驱动器越大，需要的时间越长。

预配置 FireSIGHT 系统设备

可在*暂存*位置 （一个用来预配置或暂存多个设备的中心位置）预配置设备 （防御中心或设备），以便在*目标*位置 （暂存位置外的任何位置）进行部署。

要预配置并部署设备至目标位置，请执行以下步骤：

- 在暂存位置的设备上安装系统
- 或者，将设备注册至防御中心
- 或者，将所有更新从管理的防御中心推送至设备
- 或者，从防御中心注销设备
- 关闭设备并装运至目标位置
- 在目标位置部署设备

有关详细信息，请参阅以下各节：

- 准备工作，第 E-1 页
- 安装系统，第 E-3 页
- 注册设备，第 E-3 页
- 准备装运设备，第 E-3 页
- 设备预配置故障排除，第 E-5 页

提示 保存所有包装材料，并在重新包装设备时将所有参考材料和电源线一起包装。

准备工作

在预配置设备之前，收集暂存位置和目标位置的网络设置、许可证和其他相关信息。

提示 创建一个电子数据表，以便在暂存位置和目标位置管理这些信息。

在初始设置过程中，利用所需信息配置设备，以连接设备和网络并安装系统。或者，将设备连接至防御中心，以将所有更新从防御中心推送至设备。还可以启用其他功能，初始设置虽然不需要这些功能，但可以用于预配置。有关详细信息，请参阅以下各节：

- 预配置所需信息，第 E-2 页
- 预配置可选信息，第 E-2 页
- 预配置时间管理，第 E-2 页

预配置所需信息

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
- DNS 服务器在暂存位置或目标位置 （如可访问）的 IP 地址
- NTP 服务器在暂存位置或目标位置 （如可访问）的 IP 地址
- 目标位置的检测模式

预配置可选信息

可更改某些默认配置，如：

- 允许通过 LCD 面板配置设备 （仅限 3 系列受管设备）
- 设置时区 （如果选择手动设置设备的时间）
- 设置自动备份的远程存储位置
- 设置 3 系列设备上的无人值守管理 (LOM) IP 地址，以启用设备上的 LOM

如果要将设备注册至防御中心，需要以下信息：

- 受管设备的名称或 IP 地址
- 管理主机的名称 （防御中心）
- 注册密钥 （个人创建的具有唯一性的字母数字密钥，最长 37 个字符）

预配置时间管理

请注意以下事项：

- 思科建议将时间与物理 NTP 服务器同步。请勿将受管设备与虚拟防御中心同步。在虚拟设备上进行性能优化会影响实时时钟。
- 如果暂存位置的网络可访问目标位置的 DNS 和 NTP 服务器，则使用目标位置 DNS 和 NTP 服务器的 IP 地址。否则，使用暂存位置信息并在目标位置重置。
- 如果不是利用 NTP，而是手动在设备上设置时间，则使用目标部署的时区。请参阅时间设置，第 4-8 页。

安装系统

采用安装 FireSIGHT 系统设备，第 3-1 页和设置 FireSIGHT 系统设备，第 4-1 页所述的安装步骤。预配置系统时，请记住以下事项：

- 在 3 系列设备上，如果允许通过 LCD 面板访问设备的网络设置，则物理访问设备后可进行未授权的更改，这样会带来安全风险。请参阅 3 系列设备 LCD 面板配置，第 4-8 页。
- 利用防御中心的主机名或 IP 地址在目标部署中预注册设备。请注意稍后完成注册所需的注册密钥。请参阅远程管理，第 4-8 页。
- 如果已更改默认的检测模式，务必将其通知给目标部署处的相关人员。若接口配置方式与检测模式不一致，系统就不能正确地分配接口。请参阅检测模式，第 4-9 页。
- 如果需要配置设备的网络地址转换 (NAT)，则在利用设备的 CLI （仅限 3 系列设备）或管理其的防御中心的网络界面来注册设备时，提供设备的 NAT ID。请参阅使用 CLI 将 3 系列设备注册至防御中心，第 4-6 页和 《*FireSIGHT 系统用户指南*》中的“在 NAT 环境运行”。
- 在初始设置过种中添加许可证。如果在此过程中未添加许可证，初始设置过程中注册的设备就会作为无许可证设备添加至防御中心；初始设置流程结束后，必须逐个许可每个设备。请参阅许可证设置，第 4-12 页。

注册设备

可将设备注册至防御中心，如果防御中心上运行的软件版本等于或高于设备上的软件版本，可将策略和更新推送至受管设备。

注 如果将防御中心及其受管设备部署在不同的目标位置，则必须在关闭设备前从防御中心删除受管设备。请参阅从防御中心删除设备，第 E-4 页。

要将设备注册至防御中心，请执行以下操作：

步骤 1 在设备上，利用目标部署中防御中心的主机名或 IP 地址配置远程管理。请注意稍后完成注册所需的注册密钥 请参阅远程管理，第 4-8 页。

注 在将设备注册至防御中心之前，您必须在设备上配置远程管理。

步骤 2 在防御中心上，利用远程管理配置中的注册信息来注册设备。请参阅设备注册，第 4-13 页。

准备装运设备

装运设备前，必须安全关闭并重新包装设备：

- 如果在目标位置的不同配置中使用防御中心和受管设备不在目标位置的同一配置中使用，必须从防御中心中删除受管设备，然后关闭并重新包装设备。请参阅从防御中心删除设备，第 E-4 页。
- 要安全关闭设备，请参阅关闭设备，第 E-5 页。
- 为确保安全地准备装运设备，请参阅关于装运的注意事项，第 E-5 页。

从防御中心删除设备

除非将防御中心及其受管设备部署在相同的目标位置，否则须从防御中心删除受管设备。这样可在将设备注册至目标位置一个不同的防御中心时，防止设备寻找原始防御中心的 UUID。

要从防御中心删除设备，请执行以下操作：

步骤 1 在防御中心中，选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2 在要删除的设备旁，点击删除图标 ( )。

收到提示后，确认要删除该设备。设备和防御中心之间的通信断开，已从 Device Management 页面删除设备。如果设备的系统策略使其通过 NTP 从防御中心接收时间，设备恢复至本地时间管理。

从防御中心删除设备后，验证设备不再受到防御中心的远程管理。

要验证设备不受防御中心管理，请执行以下操作：

步骤 1 在受管设备上，使用网络界面或 CLI：

- 在受管设备的网络界面，选择 **System > Local > Registration > Remote Management** 并确认 Remote Management 屏幕的 Host 列表为空。
- 在受管设备的 CLI 上，运行命令 `show manager` 并确认无主机显示。

从防御中心删除许可证

如果由于任何原因需要删除许可证，可执行以下步骤。请记住，由于思科根据每个防御中心具有唯一性的许可密钥生成许可证，因此，在从一个防御中心删除一个许可证后，不可以在另一个防御中心上再使用该许可证。有关详细信息，请参阅 《*FireSIGHT 系统用户指南*》中的“见许可 FireSIGHT 系统”部分。

要删除许可证，请执行以下操作：

步骤 1 选择 **Systems > Licenses**。

系统将显示 License 页面。

步骤 2 在要删除的许可证旁，点击删除图标 ( )。

删除一个许可证后，将从所有在使用此许可证的设备上删除相关的许可功能。例如，如果保护许可证有效且对已 100 台受管设备启用，删除该许可证后，会删除所有这 100 台设备的保护功能。

步骤 3 确认要删除许可证。

许可证删除成功。

关闭设备

断开电源前采用以下步骤安全地关闭设备。

要关闭防御中心，请执行以下操作：

步骤 1 在防御中心上，将以下命令输入命令行：

```
sudo shutdown -h now
```

防御中心已安全关闭。

要关闭受管设备，请执行以下操作：

步骤 1 在设备上，将以下命令输入命令行：

```
system shutdown
```

设备已安全关闭。

关于装运的注意事项

要准备将设备运往目标位置，必须安全地关闭并重新包装设备。请注意以下事项：

- 用原装包装重新包装设备。
- 将参考材料和电源线与设备一起包装。
- 避免操作不当或压力过度，不然网络模块和 SFP 会遭到损坏。
- 为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

如果已针对目标部署正确地预配置了设备，则无需进一步配置就可安装并部署设备。

如果不能正常登录设备，则预配置可能出现错误。尝试操作以下步骤以排除故障：

- 确认所有电源线和通信线已正确地连接到设备。
- 确认拥有设备的当前密码。暂存位置的初始设置提示更改密码。有关新密码，请参阅暂存位置提供的配置信息。
- 确认网络设置是正确的。请参阅初始设置页面：设备，第 4-7 页和初始设置页面：防御中心，第 4-10 页。
- 确认通信端口正确并正常运行。有关如何管理防火墙端口的详细信息，请参阅防火墙有关文档。有关所需的开放端口，请参阅通信端口要求，第 1-15 页。
- 如果在部署中使用了一台网络地址转换 (NAT) 设备，则确认 NAT 已配置正确。请参阅《FireSIGHT *系统用户指南*》中的“在 NAT 环境运行”。

如果仍有问题，可与 IT 部门联系。

词 汇 表

2 系列

思科设备型号的第二个系列。由于资源、架构和许可的限制， 2 系列设备只支持有限的 FireSIGHT 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、 DC1000 和 DC3000。

3 系列

思科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 FirePOWER 受管设备。该系列的设备包括 70xx 子系列（3D7010、3D7020、3D7030 型号）和 71xx 子系列 （3D7110、 3D7115、 3D7120、 3D7125、 AMP7150 型号）。

8000 系列

一组3 系列 FirePOWER 受管设备。该系列的设备包括 81xx 子系列 （3D8120、 3D8130、 3D8140、AMP8150 型号）、82xx 子系列（3D8250、3D8260、3D8270、3D8290 型号）和 83xx 子系列（3D8350、3D8360、3D8370、3D8390 型号）。8000 系列设备通常比 7000 系列设备功能更强大。

CLI

请参阅命令行界面。

Context Explorer

采用入侵、连接、文件、地理定位、恶意软件和发现策略，显示关于受监控网络的详细、交互式图形信息的页面。不同的部分以生动的线条、柱状图、饼状图和环岛状图的形式展示信息，同时提供详细的列表。可以轻松创建和应用自定义过滤器来调整分析，并且可以通过点击或将光标悬停在图形区域检查数据部分。控制面板高度可自定义，可以划分成独立的各个部分而且可以实时更新；与之相比，Context Explorer 是手动更新的，旨在为其数据提供更广泛的上下文，而且具有适用于活跃的用户浏览操作的统一、一致的布局。

eStreamer

FireSIGHT 系统的一种组件，用于将事件数据从防御中心或外部设备流式传输至客户端应用。

Fast-Path 规则

在设备的硬件级别使用一系列有限的条件配置的规则，从而允许流量不需要分析，绕过处理。

FireAMP 订用

使组织可以将 FireAMP 用作高级恶意软件防护 (AMP) 解决方案的、单独购买的订用。请与恶意软件许可证进行比较，后者是在设备上启用的，从而执行基于网络的 AMP。

FireAMP 连接器

基于订用的 FireAMP 部署中的用户在电脑和移动设备等终端上安装的轻型代理。连接器与思科云通信，交换用于快速识别和隔离整个组织中的恶意软件的信息。

FireAMP 门户

网站 http://amp.sourcefire.com/，可以在此网站配置组织的基于订用的 FireAMP 部署。

FireAMP

思科的企业级、基于终端的高级恶意软件分析和防护解决方案，可以发现、识别和阻止恶意软件入侵、持续性威胁和有针对性的攻击。如果组织有FireAMP 订用，各个用户可以在终端 （电脑、移动设备）上安装轻型 FireAMP 连接器，然后其将与思科云通信。这样就可以快速识别和隔离恶意软件，以及在其入侵时识别入侵、跟踪其轨迹、理解其影响并了解如何成功恢复。可以使用 FireAMP 门户创建自定义防护，阻止执行特定应用以及创建自定义白名单。请与基于网络的高级恶意软件防护进行比较。

FireSIGHT 许可证

防御中心上的默认许可证，允许执行主机、应用和用户发现。 FireSIGHT 许可证还决定着可以使用防御中心及其受管设备监控多少个独立主机和用户以及可以在访问控制规则中用于执行用户控制的受访问控制的用户的数量。

GeoDB

请参阅地理定位数据库。

LDAP 身份验证

将用户凭据与轻量级目录访问协议 (LDAP) 目录服务器中存储的 LDAP 目录进行比较，的一种外部身份验证形式。

link state propagation

旁路模式下内联集的一个选项，在内联集中当一对接口中有一个被关闭时，自动关闭第二个接口。当被关闭的接口恢复运行时，第二个接口也自动恢复运行。换句话说，如果一个已配对的接口的链路状态改变，另一个接口的链路状态会自动变为与之一致的状态。

NAT 策略

使用 NAT 规则执行包含 NAT 的路由的一个策略。

NAT

网络地址转换，在多个主机之间共享一个 Internet 连接的最常用功能。使用发现，系统可将网络设备识别为逻辑接口。此外，在 FireSIGHT 系统的第 3 层部署中，您可以通过 NAT 策略用 NAT 配置路由。

NetMod

在受管设备的机箱中安装的一个模块，其包含适用于该设备的检测接口。

RADIUS 身份验证

远程身份验证拨入用户服务，用于验证/授权和说明用户对网络资源的访问的一种服务。可以创建外部身份验证对象，允许 FireSIGHT 系统用户通过 RADIUS 服务器进行身份验证。

SFP 模块

插入到 71xx 子系列设备上的网络模块中的小型可插拔收发器。SFP 模块上的感应接口不允许使用可配置的旁路。

URL 过滤许可证

允许根据 URL 类别和 URL 信誉信息执行 URL 过滤的许可证。 URL 过滤许可证会过期。

URL 过滤

一种功能，允许写入根据受监控主机请求的 URL 决定可以访问网络的流量的访问控制规则，与 URL 类别以及这些 URL 的 URL 信誉信息相关，防御中心可从思科云获取这些信息。还可以通过指定要允许或阻止的单个的 URL 或成组的 URL 对网络流量实现更细化的自定义控制。

URL 类别

URL 的通用分类，例如恶意软件或社交网络。

UTC 时间

协调世界时。又叫做格林尼治标准时间 (GMT)， UTC 是全球各地共同使用的标准时间。虽然 FireSIGHT 系统使用 UTC，但是可以使用 Time Zone 功能设置本地时间。

VDB

请参阅漏洞数据库。

VLAN

虚拟局域网。 VLAN 不是按照地理位置，而是按照部门或主要用途等一些其他标准映射主机。受监控主机的主机配置文件会显示与该主机关联的任何 VLAN 信息。入侵事件中也包含 VLAN 信息，作为触发事件的数据包中最内部的 VLAN 标记。可以按照 VLAN 过滤入侵策略并且按照 VLAN 指定合规白名单目标。在第 2 层和第 3 层部署中，可以在受管设备上配置虚拟交换机和虚拟路由器，相应地处理带 VLAN 标记的流量。

VPN 许可证

允许在思科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 终端之间创建安全的 VPN 隧道的一种许可证。

VPN

允许在思科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 终端之间创建安全的 VPN 隧道的一种功能。

VRT

请参阅思科 VRT。

安全策略

保护组织网络的组织准则。例如，安全策略可能禁止使用无线接入点。安全策略还可能包括可接受的使用策略 (AUP)，其为员工提供关于如何利用其组织的系统的指导。

安全情报

按照访问控制策略，根据源或目标 IP 地址，指定可以穿越网络的流量的一种功能。如果在流量接受访问控制规则分析之前，要将特定 IP 地址列入黑名单或阻止它们之间的流量，这个功能就特别有用。或者，可以为安全情报过滤使用监控设置，让系统可以分析本应该已经列入黑名单的连接，而且可以记录符合黑名单的匹配项。

安全情报列表

手动上载到防御中心作为安全情报对象的 IP 地址的纯静态集合。使用列表增加和调整安全情报源以及全局黑名单和全局白名单。

安全情报源

一类安全情报对象，系统按照配置的时间间隔定期下载的一个 IP 地址动态集合。由于安全情报源会定期更新，使用它们可以确保系统使用最新信息来利用安全情报功能过滤网络流量。另请参阅思科情报源。

安全区域

可以用于管理和分类各种策略与配置中流量的一个或多个内联、被动、交换或路由接口。单个区域的接口可以跨多个设备；还可以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给安全区域，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

允许执行入侵检测和防御、文件控制和安全情报过滤的、适用于 3 系列和虚拟设备的许可证。没有许可证， 2 系列设备自动具备保护功能，但是安全情报除外。

被动检测

通过分析受管设备被动收集的流量执行的一系列发现策略。请与主动检测进行比较。

被动接口

被配置用于分析被动部署中的流量的检测接口。

表视图

显示事件信息的一种工作流程页面，其中数据库表中的每一个字段都分别占用一列。执行事件分析时，可以使用向下钻取页面限制进入向您显示有关您所感兴趣事件的详细信息的表视图之前想要调查的事件。表视图通常是系统提供的工作流程的倒数第二页。

侧录模式

3D9900 和 3 系列设备上可用的一种高级内联集选项，其中要分析每个数据包的一个副本并且网络流量不受干扰，无需通过设备。由于处理的是数据包的副本而不是数据包本身，因此即使将访问控制和入侵策略配置为放弃、修改或阻止流量，设备都不会影响数据包数据流。

策略

应用设置，通常是向设备应用设置，的一种机制。请参阅、访问控制策略、关联策略、文件策略、运行状况策略、入侵策略、网络发现策略和系统策略。

层

入侵策略内一套完整的入侵规则、预处理器规则和高级设置配置。可以在内建层或策略中的层添加自定义用户层。入侵策略高层的设置会覆盖低层的设置。

导入

可以用于将各种配置从一个设备传输至另一个设备的一种方法。可以导入之前从相同类型的另一设备中导出的配置。

地理定位

对在受监控网络上的流量中检测到的可路由 IP 地址提供关于其地域来源的数据的一种功能，包括提供连接类型、 Internet 服务提供商等数据。可以查看地理定位数据库、连接事件、入侵事件、文件事件和恶意事件以及主机配置文件中存储的地理定位信息。

地理定位数据库

又叫做 GeoDB，包含与可路由 IP 地址关联的已知地理定位数据的一种定期更新的数据库。

堆叠

共享检测资源的二至四个相互连接的设备。

堆栈

允许通过在一个堆栈配置中连接二至四个物理设备，从而增加网段上检查的流量的一种功能。建立堆栈配置时，要将每个堆叠设备的资源集成到单个统一的共享配置中。

恶意软件防护

请参阅高级恶意软件防护。

恶意软件检测

思科基于网络的高级恶意软件防护 (AMP) 解决方案的一个组成部分。作为全局访问控制配置组成部分向受管设备应用的文件策略检查网络流量。防御中心然后针对受检测的特定文件类型执行恶意软件云查找，并生成警告文件的恶意软件性质的事件。随后执行 AMP 恶意软件阻止，其将阻止文件或允许其上载或下载。将此功能与 FireAMP 比较，后者是思科基于终端的 AMP 工具，要求采用 FireAMP 订用。

恶意软件许可证

允许在网络流量中执行高级恶意软件防护 (AMP) 的许可证。使用文件策略，可以配置系统，对受管设备检测的特定文件类型执行恶意软件云查找。请与 FireAMP 订用比较。

恶意软件云查找

防御中心与思科云通信，从而根据在网络流量中检测到的文件的 SHA-256 哈希值，确定对该文件的恶意软件性质的一种流程。

恶意软件阻止

思科基于网络的高级恶意软件防护 (AMP) 解决方案的一个组成部分。在恶意软件检测为检测到的文件生成恶意软件性质后，可以阻止该文件或允许其上载或下载。将此功能与 FireAMP 比较，后者是思科基于终端的 AMP 工具，要求采用 FireAMP 订用。

恶意事件

思科的高级恶意软件防护解决方案之一生成的事件。当思科云返回对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；当该性质变化时，生成追溯性恶意软件事件。请与基于终端的恶意事件比较，后者是在部署的 FireAMP 连接器检测到威胁、阻止恶意软件执行或隔离或无法隔离恶意软件时生成的。

发现

FireSIGHT 系统的一种组件，使用受管设备监控网络并提供网络的完整统一视图。网络发现可以确定网络上的主机（包括网络设备和移动设备）的数量和类型以及关于操作系统、活跃应用和这些主机上的开放端口的信息。还可以配置思科受管设备来监控网络上的用户活动，从而识别违反策略的原因、攻击或网络漏洞。

发现策略

请参阅网络发现策略。

防御中心

用于管理设备和自动聚合与关联其所生成的事件的集中管理点。

访问控制

FireSIGHT 系统的一种功能，用于指定、检查和记录可以流经网络的流量。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，而且还决定着使用发现功能可以检查的流量。

访问控制策略

应用于管理设备从而在这些设备监控的网络流量执行访问控制的策略。访问控制策略可能包括多个访问控制规则；它还指定决定着如何处理和记录不符合任何这些规则条件的流量的默认操作。访问控制策略还可以指定 HTTP 响应页面、安全情报以及其他高级设置。

访问控制规则

FireSIGHT 系统用于检查所监控网络流量以及实现细化访问控制一组条件。构成访问控制策略的访问控制规则可以执行简单的 IP 地址匹配，或定义涉及不同用户、应用、端口和 URL 的复杂连接。访问控制规则操作决定着系统如何处理符合规则条件的流量。其他规则设置决定着如何（以及是否）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

IP 地址列表，在系统策略中配置，描述可以访问设备的主机。默认情况下，任何人都可以使用端口 443（HTTPS）访问设备的网络界面，也可以使用端口 22 (SSH) 访问命令行。还可以使用端口 161 增加 SNMP 访问。

非旁路模式

内联集的一种特性，如果集合内的检测接口由于任何原因出现故障，它会阻止流量。

服务器

主机上安装的、按照应用协议流量进行识别的服务器应用（请与客户端应用相比较）。

高级恶意软件防护

简称 AMP， FireSIGHT 系统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 比较，后者是思科基于终端的 AMP 工具，要求采用 FireAMP 订用。

高级设置

需要具备特定专业知识才能配置的预处理器或其他入侵策略功能。高级设置通常很少需要修改或根本就不需要修改，而且对于每个部署都不是通用的。

高可用性

允许配置冗余物理防御中心来管理成群设备的一种功能。从受管设备流式传输至两种防御中心的事件数据流和大多数配置元素在两种防御中心上都会保存。如果主要防御中心出现故障，可以使用辅助防御中心监控网络，而不会中断监控。请与集群比较，后者允许指定冗余设备。

构件

请参阅控制面板构件。

管理接口

用于管理 FireSIGHT 系统设备的网络接口。在大多数部署中，管理接口连接到内部受保护的网络。请与检测接口比较。

规则操作

确定系统如何处理符合规则条件的网络流量的一种设置。请参阅访问控制和文件规则操作。

规则更新

包含新的和更新的标准文本规则、共享对象规则以及预处理器规则的按需入侵规则更新。规则更新也可能删除规则，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

提供用作检查网络流量的标准的一种结构，通常是在策略内。

规则状态

入侵策略内入侵规则是被启用 （设置为 Generate Events 或 Drop and Generate Events），还是被禁用 （设置为 Disable）。如果启用规则，它将用于评估网络流量；如果禁用规则，则不使用此规则。

混合接口

受管设备上的一种逻辑接口，使系统可以桥接虚拟路由器和虚拟交换机之间的流量。

集群

用于在两个对等3 系列设备或堆栈之间实现网络功能和配置数据冗余的一种功能。集群为策略应用、系统更新和注册提供了一个统一的逻辑系统。请与高可用性比较，后者允许配置冗余的防御中心。

计划任务

安排运行一次或按照一定间隔重复运行的管理任务。

监控

在访问控制策略中是指记录与安全情报黑名单或访问控制规则匹配的流量，但是允许系统继续评估流量而不是立即允许或阻止流量的一种方式。

检测接口

在设备上用于监控网段的网络接口。请与管理接口比较。

运行状况策略

检查部署中的设备的运行状况时使用的标准。运行状况策略使用运行状况模块来指示 FireSIGHT 系统硬件和软件是否在正常运行。可以使用默认的运行状况策略，也可以自己创建。

交换机

用作多端口网桥的网络设备。利用网络发现，系统将交换机识别为网桥。此外，还可以将受管设备配置为虚拟交换机，在两个或多个网络之间执行数据包交换。

交换接口

想要用于交换第 2 层部署中流量的接口。可以设置处理不带标记的 VLAN 流量的物理交换接口和处理带指定 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，将抓取的数据包处理成预处理器可以理解的格式。

警报

告知系统已经生成特定事件的通知。可以基于入侵事件 （包括其影响标记）、发现事件恶意事件、关联策略违反情况、运行状况变化以及具体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 陷阱发出警报。

具备 FirePOWER 服务的思科 ASA 防火墙

一组思科自适应安全设备 (ASA) 受管设备。此系列中的设备包括 ASA5512-X、 ASA5515-X、ASA5525-X、 ASA5545-X、 ASA5555-X、 ASA5585-X-SSP-10、 ASA5585-X-SSP-20、ASA5585-X-SSP-40 和 ASA5585-X-SSP-60 型号。

可配置的旁路

内联集的一种特性，允许配置旁路模式。

客户端应用

请参阅客户端。

客户端

又叫做客户端应用，指在一个主机上运行并且依靠另一个主机 （服务器）来执行某些操作的应用。例如，邮件客户端允许发送和接收邮件。系统检测到主机上的用户正在使用特定客户端访问另一主机时，将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 （如可获知）。

控制面板构件

控制面板自带的一种小组件，用于深入了解 FireSIGHT 系统的某个方面。

控制面板

提供当前系统状态快速浏览视图的一种显示，包括显示关于系统收集和生成的事件的数据。要增加系统提供的控制面板，可以创建多个自定义控制面板，并用选择的控制面板构件填充。请与 Context Explorer 比较，后者提供关于受监控网络外观和操作的宽泛、简略和彩色的视图。

控制许可证

允许通过将用户和应用条件加入访问控制规则中实施用户控制和应用控制的一种许可证。它还允许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。

连接

两个主机之间受监控的会话。可以记录访问控制策略中受管设备检测到的连接；请在网络发现策略中配置 NetMod 连接日志记录。

列表

请参阅安全情报列表。

漏洞

关于主机容易感染的特定威胁的一种描述。防御中心在主机的主机配置文件中提供关于每个主机容易感染的漏洞的信息。此外，可以使用漏洞网络映射获取系统在整个受监控网络上检测到的漏洞的整体描述。如果认为主机不再容易感染特定威胁，可以撤销特定漏洞或将其标记为无效漏洞。

漏洞数据库

又叫做 VDB，指关于主机可能感染的已知漏洞的数据库。系统将操作系统、应用协议和在每台主机上检测的客户端与 VDB 关联，从而帮助确定特定主机是否增加了遭受网络威胁的风险。 VDB 更新可能包含新的和更新的漏洞以及新的和更新的应用探测器。

路由接口

路由第 3 层部署中的流量的接口。可以设置处理不带标记的 VLAN 流量的物理路由接口和处理带指定 VLAN 标记的流量的逻辑路由接口。还可以将静态地址解析协议 (ARP) 添加到路由接口中。

路由器

位于网关上，在网络之间转发数据包的一种网络设备。使用网络发现，系统可识别路由器。此外，还可以将受管设备配置为路由两个或多个接口之间的流量的虚拟路由器。

逻辑接口

定义使用特定 VLAN 标记在标记的流量通过物理接口时处理流量的虚拟子接口。

命令行界面

3 系列和虚拟设备上一种受限制的、基于文本的界面。命令行界面 (CLI) 用户可以根据用户分配到的访问级别运行系统。

默认操作

作为访问控制策略的组成部分，决定着如何处理不符合策略中任何规则的流量。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，默认策略操作决定着如何处理网络上不执行 Fast Path 操作的流量。可以将默认操作设置成阻止流量或信任流量而不执行进一步检查，或者利用网络发现策略或入侵策略检查流量。

内联部署

FireSIGHT 系统的一种部署，其中受管设备以内联方式部署在网络上。在此配置中，设备可以使用交换、路由、访问控制、和入侵检测和防御影响网络流量。

内联集

一对或多对内联接口。

内联接口

为了处理内联部署中的流量而配置的一种检测接口。必须向内联集成对添加内联接口。

旁路模式

内联集的一种特性，如果组内的检测接口由于任何原因出现故障，它会让流量可以继续流动。

区域

请参阅安全区域。

任务队列

设备需要执行的工作的队列。当应用策略、安装软件更新以及执行其他长期的工作时，这些工作将加入队列中并且在 Task Status 页面显示它们的状态。 Task Status 页面提供工作的详细列表并且每隔十秒钟刷新一次来更新它们的状态。

入侵策略

可以配置用来检查网络流量的入侵和违反安全策略的情况的各种组件。这些组件包括检查协议报头值、负载内容和某些数据包大小特性的入侵规则；入侵规则中常用的变量；FireSIGHT 建议的规则配置；高级设置，例如预处理器及其他检测和性能功能；以及允许为关联预处理器选项生成事件的预处理器规则。网络流量符合访问控制规则中的条件时，可以使用入侵策略检查流量；还可以将入侵策略与默认操作关联。

入侵规则

一组关键字和参数，将其应用于受监控网络流量时，其将识别潜在的入侵、违反安全策略的情况以及安全漏洞。系统将数据包与规则条件比较。如果数据包符合条件，规则触发并生成入侵事件。入侵规则包括放弃规则和通过规则。

入侵检测和防御

对网络流量监控违反安全策略的情况，以及在内联部署中阻止或修改恶意流量的功能。在 FireSIGHT 系统中，将入侵策略与访问控制规则或默认操作关联时执行入侵检测和防御。

入侵事件

记录违反入侵策略的情况的事件。入侵事件数据包括攻击出现的日期、时间和类型，以及有关攻击与其目标的其他背景信息。

入侵

在网络中出现的安全破坏、攻击或漏洞。

上下文菜单

一种弹出菜单，网络界面的很多页面都提供此菜单，可以用作访问 FireSIGHT 系统中其他功能的快捷方式。此菜单的上下文取决于多个因素，包括当时查看的页面、当时调查的具体数据以及用户角色。上下文菜单选项包括指向入侵规则、事件、和主机信息的链接；各种入侵规则设置、指向 Context Explorer 的快速链接；按照主机 IP 地址将主机加入安全情报全局黑名单或全局白名单的选项；以及按照文件的 SHA-256 哈希值将文件加入全局白名单的选项。

设备堆叠

请参阅堆栈。

设备

防御中心或受管设备。设备可以是物理或虚拟设备。

设备集群

请参阅集群。

设备

适用于各种吞吐量的容错、专用设备。根据设备的许可功能，可以将其用于被动监控流量，创建关于网络资产、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。您必须通过防御中心管理设备。

事件查看器

用于查看和操作事件的系统组件。事件查看器使用工作流程显示宽泛的事件视图，然后重点显示只包含您感兴趣的事件的详细事件视图。可以通过向下钻取整个工作流程或使用搜索功能，限制事件视图中的事件。

事件

关于特定活动的一系列详细信息，可以通过工作流程在事件查看器中查看。事件可能表示网络上的攻击、受检测网络资产中的变更、违反组织安全和网络使用策略的情况等等。系统还会生成关于设备不断变化的运行状态、网络界面的使用、规则更新以及已启动的修复的信息的活动。最后，系统还会将其他信息显示为事件，即使这些“事件”不代表特定活动。例如，可以使用事件查看器查看关于受检测的主机、应用及其漏洞的详细信息。

事件流处理器

请参阅eStreamer。

受保护的网络

通过防火墙等设备保护不受用户或其他网络侵扰的组织内部网络。 FireSIGHT 系统提供的很多入侵规则都使用变量来定义受保护的网络和不受保护的 （或外部）网络。

受管设备

请参阅设备。

数据库访问

允许第三方客户端以只读形式访问防御中心的一种功能。

思科 VRT

思科的漏洞研究组。

思科情报源

被思科 VRT 判定信誉不良的 IP 地址的一系列列表，这些列表定期更新。情报源中的每个列表分别代表一个特定的类别：开放式中继站、已知攻击者、假的 IP 地址 (bogon) 等等。在访问控制策略中，可以使用安全情报将任何或所有类别列入黑名单。由于情报源定期更新，所以使用它可以确保系统使用最新的信息来过滤网络流量。

思科云

有时候又称为*云服务*，指思科承载的外部服务器，其中防御中心可以获取最新的相关信息，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。

透明内联模式

允许设备用作“线缆焊块”并转发其所检测到的所有网络流量（不管其来源和目标）的一种高级内联集选项。

网络发现策略

指定针对特定网段，包括由支持 NetMod 的设备监控的网络，系统收集的发现策略种类的策略（包括主机、用户和应用数据）。网络发现策略还可管理导入分辨率首选项和活动检测源优先级。

网络发现

请参阅发现。

网络设备

在 FireSIGHT 系统中指被识别为网桥、路由器、 NAT 设备或逻辑接口的主机。

网络文件轨迹

对主机在整个网络传输文件时的文件路径的直观表示。对于带有关联 SHA-256 哈希值的任何文件，轨迹映射显示传输了该文件的所有主机 IP 地址、文件检测的时间、文件的恶意软件性质、关联的文件事件和恶意事件等等。

网络应用

展示 HTTP 流量的内容或为其请求获取的 URL 的一种应用。

网络映射

对网络的详细展现。您可以通过网络映射查看网络拓扑，包括网络上运行的主机、移动设备、和网络设备及其关联主机属性、应用协议和漏洞等方面。

违反安全策略的情况

安全破坏、攻击、漏洞，或者其他不当的网络使用方式。

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。用文件规则填充文件策略，由访问控制策略内的访问控制规则调用文件策略。

文件轨迹

请参阅网络文件轨迹。

文件控制

作为访问控制组成部分的一种功能，允许指定和记录可以流经网络的文件的类型。

文件类型

具体的文件格式类型，例如 PDF、 EXE 或 MP3。

无人值守管理 (LOM)

允许使用带外 Serial over LAN (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的一种 3 系列功能。可以执行有限的任务，例如查看机箱序列号或监控风扇转速和温度等情况。

物理接口

代表 NetMod 上物理端口的接口。

系统策略

对于部署中的多个设备来说类似的设置，例如邮件中继主机首选项和时间同步设置等。使用防御中心将系统策略应用到自身及其受管设备上。

相关性

一种功能，可以用于创建实时响应网络威胁的关联策略。有相关性的修复组件提供灵活的 API，可以使用此 API 创建和上载自定义补救模块以回应违反策略的情况。

信誉 （IP 地址）

请参阅安全情报。

修复

降低系统的潜在攻击的操作。可以配置修复，并且在关联策略内还可以将其与规则和合规性白名单关联，这样，当它们触发时，防御中心会启动修复。这不仅可以在您没有时间处理攻击的时候减轻攻击，而且可以确保系统保持符合组织的安全策略。防御中心带有预定义的修复模块，也可以使用一个灵活的 API 创建自定义修复。

虚拟防御中心

可以在虚拟宿主环境中在设备上部署的防御中心。

虚拟交换机

处理通过网络的出站和入站流量的一组交换接口。在第 2 层部署中，可以在受管设备上配置虚拟交换机，用作独立广播域，将网络分为不同逻辑分段。虚拟交换机使用来自主机的媒体访问和控制 (MAC) 地址确定向哪里发送数据包。

虚拟路由器

路由第 3 层流量的一组路由接口。在第 3 层部署中，可以通过依据目标 IP 地址制定数据包转发决策将虚拟路由器配置为路由数据包。可以定义静态路由，配置路由信息协议 (RIP) 和开放最短路径优先 (OSPF) 动态路由协议以及实施网络地址转换 (NAT)。

虚拟设备

可以在虚拟宿主环境中在设备上部署的受管设备。无法将虚拟设备配置为虚拟交换机或虚拟路由器。

移动设备

在 FireSIGHT 系统中是指被发现功能识别为移动、手持设备的主机 （例如手机或平板电脑）。系统通常可以检测移动设备是否被越狱。

应用控制

一种功能，是访问控制的组成部分，允许指定哪些应用流量可以流经网络。

应用

使策略或对该策略的更改生效所采取的操作。可以将防御中心的大多数策略应用到其受管设备上；但是，可以激活和停用相关性策略，因为它们不涉及对受管设备的配置的更改。

ASA FirePOWER

具备 FirePOWER 服务的思科 ASA 防火墙的简称。

应用

受检测的网络资产、通信方式或 HTTP 内容，可以针对它写入访问控制规则。系统可检测三种类型的应用：应用协议、客户端应用和网络应用。

应用协议

一种应用，描述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。

用户代理

在服务器上安装的代理，用于在用户登录网络或出于任何其他原因按照 Active Directory 凭据进行身份验证时监控用户。对于受访问控制的用户，用户活动仅在被用户代理报告时用于访问控制。

用户感知

允许组织将威胁、终端和网络智能与用户身份信息关联并且允许执行用户控制的一种功能。

用户活动

系统检测到用户登录 （或者包括一些失败的登录尝试）或向防御中心数据库添加或从中删除用户记录时，会生成事件。

用户角色

对 FireSIGHT 系统的用户授予的访问级别。例如，对于事件分析师、管理 FireSIGHT 系统的管理员、使用第三方工具访问防御中心数据库的用户等等，可以授予不同的网络界面访问权限。还可以创建具备特殊访问权限的自定义用户角色。

用户控制

属于访问控制组成部分的一种功能，其允许指定和记录可以进入网络、退出网络或从内部跨越网络而不离开网络的用户相关流量。

用户

网络活动已被受管设备或用户代理检测到的用户。

预处理器规则

与预处理器或端口扫描流量探测器关联的入侵规则。如果想要预处理器规则生成事件，必须启用预处理器规则。预处理器规则有预处理器特定的 GID （生成器 ID）。

预处理器

通过识别不合适的报头选项、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，规范化入侵策略检查的流量并帮助识别网络层和传输层协议异常的一种功能。预处理器可以用系统可以分析的格式直接显示特定类型的数据包数据；这些预处理器叫做数据规范化预处理器或应用层协议预处理器。系统可通过规范化应用层协议编码有效地将相同的与内容相关的入侵规则应用于采用不同数据表示形式的数据包并获取有意义的结果。每当数据包触发配置的预处理器选项时，预处理器都会生成预处理器规则。

源

请参阅安全情报源。

运行状况监控

持续监控部署中的设备性能的一种功能。运行状况监控功能在应用的运行状况策略内使用运行状况模块来测试设备。

运行状况模块

对部署中的设备的 CPU 使用情况或可用磁盘空间等特定性能进行的一种测试。在运行状况策略中启用的运行状况模块在其监控的性能达到特定水平时生成运行状况事件。

终端

计算机或移动设备，其中用户在上面安装了 FireAMP 连接器，作为组织高级恶意软件防护战略的一部分。

主机输入

允许使用脚本或命令行文件从第三方资源导入数据，从而增加网络映射中的信息的一种功能。网络界面也提供一些主机输入功能；可以修改操作系统或应用协议标识、验证或阻止漏洞以及从网络映射删除各种项目，包括客户端和服务器端口。

主机

与网络连接并且具有独一无二 IP 地址的一种设备。对于 FireSIGHT 系统，主机是指未被分类为移动设备、网桥、路由器、 NAT 设备或逻辑接口的任何已识别的主机。

自定义用户角色

具有专用访问权限的用户角色。自定义用户角色可以具有任何基于菜单的权限和系统权限，并且可以是完全原创的或基于预定义的用户角色。