思科 Firepower 管理中心安装指南

版本 6.0
2015 年 11 月 5 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

Firepower 系统简介

思科 Firepower 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。Firepower 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。

思科 Firepower 管理中心为 Firepower 系统提供了一个集中管理控制台和数据库资源库。网段上安装的受管设备将监控要分析的流量。

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

可以通过内联部署中的设备保护网络免受可能影响网络上主机可用性、完整性或机密性的攻击。内联接口无条件地接收所有流量，除非部署中的某些配置明确放弃这些流量，否则这些接口上接收的流量都会被重新传输。内联设备可以部署为简单的入侵防御系统。也可以使用其他方法配置内联设备，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 Firepower 系统设备的信息（设备和管理中心）。也提供了 Firepower 系统设备的硬件规格、安全和监管信息。

提示 您可以将虚拟 Firepower 管理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*《适用于 VMware 的 Firepower NGIPSv 快速入门指南》*。

接下来的主题将介绍 Firepower 系统并描述其主要组件：

- Firepower 系统设备，第 1-1 页
- Firepower 系统组件，第 1-8 页
- 许可 Firepower 系统，第 1-10 页
- 安全、互联网接入和通信端口，第 1-11 页
- 预配置设备，第 1-14 页

Firepower 系统设备

Firepower 系统*设备*可以是流量感应受管*设备*，也可以是管理型 *Firepower 管理中心*：

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。Firepower 管理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*。Firepower 系统的许多功能都取决于设备。

Firepower 管理中心

Firepower 管理中心为 Firepower 系统部署提供集中管理点和事件数据库。Firepower 管理中心汇聚和关联入侵、文件、恶意软件、发现、连接和性能数据，从而评估事件对特定主机的影响并用危害表现来标记主机。借助此功能，可以监控设备相互报告的信息，并评估和控制网络中发生的总体活动。

Firepower 管理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
- 关联、危害表现以及实时威胁响应的补救功能
- 自定义和基于模板的报告

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。被动部署的设备有助于深入了解网络流量。采用内联部署时，可以基于多个条件使用 Firepower 设备影响通信流量。根据型号和许可证，设备具有以下特性和功能：

- 收集有关贵公司的主机、操作系统、应用、用户、文件、网络和漏洞的详细信息
- 根据各种基于网络的标准以及其他标准（包括应用、用户、URL、IP 地址信誉和入侵或恶意软件检查结果）来阻止或允许网络流量
- 具有交换、路由、DHCP、NAT 和 VPN 功能以及可配置的旁路接口、快速路径规则和严格的 TCP 实施
- 具有高可用性（冗余），有助于确保运行连续性和堆栈，整合多种设备的资源

必须用 Firepower 管理中心管理 Firepower 设备。

设备类型

Firepower 系统可以在容错设备上运行，这是思科提供的专用*物理*网络设备。每个Firepower 管理中心和受管设备都有多种*型号*；这些型号进一步分为*系列*和*子系列*。

物理受管设备具有很多种吞吐量和大量功能。物理 Firepower 管理中心还有各种设备管理、事件存储和主机与用户监控功能。

可以将 64 位*虚拟* Firepower 管理中心和*虚拟* Firepower 受管设备部署为使用 VMware vSphere 虚拟机监控程序或 vCloud Director 环境的 ESXi 主机。

任何类型（物理或虚拟）的管理中心都可以管理任何类型的设备：物理、虚拟和提供 FirePOWER 服务的思科 ASA。但是，请注意，许多 Firepower 系统功能都取决于设备。

有关 Firepower 系统设备的详细信息，包括设备支持的功能，请参阅：

- 7000 和 8000 系列设备，第 1-3 页
- 虚拟设备，第 1-3 页
- 提供 FirePOWER 服务的思科 ASA，第 1-3 页
- 版本 6.0 随附设备，第 1-4 页
- Firepower 管理中心型号支持的功能，第 1-5 页
- 按照受管设备型号划分的受支持功能，第 1-6 页

7000 和 8000 系列设备

7000 和 8000 系列是 Firepower 物理设备。Firepower 8000 系列设备更强大并且支持 Firepower 7000 系列设备不支持的一些功能。有关 7000 和 8000 系列设备的详细信息，请参阅《*Firepower 7000 和 8000 系列安装指南*》。

虚拟设备

可以将 64 位虚拟 Firepower 管理中心和受管设备部署为使用 VMware vSphere 虚拟机监控程序或 vCloud Director 环境的 ESXi 主机。

无论安装和应用了何种许可证，虚拟设备都不支持任何基于硬件的系统功能：冗余和资源共享、交换、路由等等。此外，虚拟设备没有网络界面。有关虚拟设备的详细信息，请参阅《*适用于 VMware 的 Firepower NGIPSv 快速入门指南*》。

提供 FirePOWER 服务的思科 ASA

提供 FirePOWER 服务的思科 ASA（ASA FirePOWER 设备）的功能类似于受管设备。在此部署中，ASA 设备提供最重要的系统策略，并将流量传递至 Firepower 系统进行访问控制、入侵检测和防御、发现以及高级恶意软件防护。请参阅版本 6.0 Firepower 系统设备表，查看受支持的 ASA 型号的列表。

无论安装和应用何种许可证，ASA FirePOWER 设备都不支持以下任何 Firepower 系统功能：

- ASA FirePOWER 设备不支持 Firepower 系统的基于硬件的功能：高可用性、堆叠、交换，路由、VPN、NAT 等等。但是，ASA 平台确实提供这些功能，可以使用 ASA CLI 和 ASDM 配置这些功能。有关详细信息，请参阅 ASA 文档。
- 无法使用 Firepower 管理中心 Web 界面配置 ASA FirePOWER 接口。在 SPAN 端口模式中部署 ASA FirePOWER 时，Firepower 管理中心不显示 ASA 接口。
- 无法使用 Firepower 管理中心关闭、重新启动或以其他方式管理 ASA FirePOWER 进程。

ASA FirePOWER 设备拥有 ASA 平台特有的软件和命令行界面 (CLI)。使用这些特定于 ASA 的工具可安装系统以及执行其他特定于平台的管理任务，例如：

注　如果编辑 ASA FirePOWER 设备并从多情景模式切换至单情景模式（或反之），设备会重命名其所有接口。您必须重新配置所有 Firepower 系统安全区域、关联规则以及相关的配置，才能使用更新的 ASA FirePOWER 接口名称。

版本 6.0 随附设备

下表列出了思科随版本 6.0 的 Firepower 系统提供的设备。

表 1-1　　版本 6.0 Firepower 系统设备

型号/系列	Firepower 系列	形式	类型
70xx 子系列： • 7010、7020、7030、7050	7000 系列	硬件	设备
71xx 子系列： • 7110、7120 • 7115、7125 • AMP7150	7000 系列	硬件	设备
80xx 系列： • AMP8050	8000 系列	硬件	设备
81xx 子系列： • 8120、8130、8140 • AMP8150	8000 系列	硬件	设备
82xx 子系列： • 8250 • 8260、8270、8290	8000 系列	硬件	设备
83xx 子系列： • 8350 • 8360、8370、8390 • AMP8350 • AMP8360、AMP8370、AMP8390	8000 系列	硬件	设备
64 位虚拟 NGIPSv	n/a	服务	设备
ASA FirePOWER： • ASA5585-X-SSP-10、ASA5585-X-SSP-20、ASA5585-X-SSP-40、ASA5585-X-SSP-60	n/a	硬件	设备
ASA FirePOWER： • ASA5506-X ASA5506H-X、5506W-X、5508-X、ASA5512-X、ASA5515-X、ASA5518-X、ASA5525-X、ASA5545-X、ASA5555-X	n/a	服务	设备
Firepower 管理中心： • MC750、MC1500、MC2000、MC3500、MC2000、MC4000	n/a	硬件	管理中心
64 位虚拟 Firepower 管理中心	n/a	服务	管理中心

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，请参阅将 Firepower 管理中心还原为出厂默认设置，第 6-1 页。

提示　您可以将特定配置和事件数据从版本 4.10.3 部署迁移到版本 5.2 部署。然后，可以通过一系列过程更新到版本 6.0。有关详细信息，请参阅版本 5.2 的《*Firepower 系统迁移指南*》。

Firepower 管理中心型号支持的功能

运行版本 6.0 时，所有 Firepower 管理中心都具有类似的功能，但是存在一些基于型号的限制。下表列出了系统的主要功能以及支持这些功能的 Firepower 管理中心（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，Firepower 管理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《*Firepower 管理中心配置指南*》。

另外，请记住：虽然可以使用运行版本 6.0 系统的任何型号的 Firepower 管理中心来管理任何版本 6.0 设备，但是很多系统功能都受到设备型号的限制。有关详细信息，请参阅按照受管设备型号划分的受支持功能，第 1-6 页。

表 1-2　　Firepower 管理中心型号支持的功能

特性或功能	管理中心	虚拟管理中心
收集受管设备报告的发现数据（主机、应用和用户）并为公司创建网络映射	是	是
查看网络流量的地理定位数据	是	是
管理入侵检测和防御 (IPS) 部署	是	是
管理执行安全情报过滤的设备	是	是
管理执行基于网络的控制的设备，包括基于地理位置的过滤	是	是
管理执行应用控制的设备	是	是
管理执行用户控制的设备	是	是
管理按照文字 URL 过滤网络通信的设备	是	是
管理按类别和信誉执行 URL 筛选的设备	是	是
管理按照文件类型执行简单文件控制的设备	是	是
管理执行基于网络的高级恶意软件防护 (AMP) 的设备	是	是
接受来自 FireAMP 部署的基于终端的恶意软件 (FireAMP) 活动	是	是
管理基于设备和硬件的功能： • 快速路径规则 • 严格 TCP 实施 • 可配置旁路接口 • 分路模式 • 交换和路由 • NAT 策略 • VPN	是	是

表 1-2　Firepower 管理中心型号支持的功能（续）

特性或功能	管理中心	虚拟管理中心
管理基于设备的冗余和资源共享： • 设备堆栈 • 设备高可用性 • 高可用性对中的堆栈	是	是
使用流量信道分隔并管理内部和外部流量	是	是
使用多个管理接口隔离并管理不同网络上的流量	是	是
安装恶意软件存储包	是	否
连接 eStreamer、主机输入或数据库客户端	是	是

按照受管设备型号划分的受支持功能

设备是处理网络流量的设备；因此，许多 Firepower 系统功能都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 Firepower 管理中心安装和应用了正确的许可证）。

请记住：虽然可以使用运行版本 6.0 系统的任何型号的 Firepower 管理中心来管理任何版本 6.0 设备，有些系统功能要受 Firepower 管理中心型号的限制。有关详细信息，请参阅 Firepower 管理中心型号支持的功能，第 1-5 页。

表 1-3　按照受管设备型号划分的受支持功能

特性或功能	7000 和 8000 系列设备	ASA FirePOWER	虚拟设备
网络发现：主机、应用和用户	是	是	是
入侵检测和防御 (IPS)	是	是	是
安全情报过滤	是	是	是
访问控制：基本网络控制	是	是	是
访问控制：基于地理定位的过滤	是	是	是
访问控制：应用控制	是	是	是
访问控制：用户控制	是	是	是
访问控制：文字 URL	是	是	是
访问控制：按类别和信誉进行 URL 筛选	是	是	是
文件控制：按文件类型	是	是	是
基于网络的高级恶意软件防护 (AMP)	是	是	是
自动应用旁路	是	否	是
快速路径规则	8000 系列	否	否
严格 TCP 实施	是	否	否
可配置旁路接口	受硬件限制的情况除外	否	否
分路模式	是	否	否
交换和路由	是	否	否

表 1-3　按照受管设备型号划分的受支持功能（续）

特性或功能	7000 和 8000 系列设备	ASA FirePOWER	虚拟设备
NAT 策略	是	否	否
VPN	是	否	否
设备堆叠	8140 82xx 子系列 83xx 子系列	否	否
设备高可用性	是	否	否
高可用性对中的堆栈	8140 82xx 子系列 83xx 子系列	否	否
流量信道	是	否	否
多个管理接口	是	否	否
恶意软件存储包	是	否	否
受限制的命令行界面 (CLI)	是	是	是
外部身份验证	是	否	否
连接到 eStreamer 客户端	是	是	否

7000 和 8000 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

Firepower 和 AMP 设备型号	硬件机箱代码
7010、7020、7030	CHRY-1U-AC
7050	NEME-1U-AC
7110、7120（铜缆）	GERY-1U-8-C-AC
7110、7120（光纤）	GERY-1U-8-FM-AC
7115、7125、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 7000 和 8000 系列型号的机箱名称。

表 1-5　　8000 系列机箱型号

Firepower 和 AMP 设备型号	硬件机箱代码
AMP8050（交流或直流电源）	CHAS-1U-AC/DC
8120、8130、8140、AMP8150（交流或直流电源）	CHAS-1U-AC/DC
8250、8260、8270、8290（交流或直流电源）	CHAS-2U-AC/DC
8350、8360、8370、8390（交流或直流电源）	PG35-2U-AC/DC
AMP830、AMP8360、AMP8370、AMP8390（交流或直流电源）	PG35-2U-AC/DC

Firepower 系统组件

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

提示 Firepower 系统的许多功能取决于设备型号、许可证和用户角色。Firepower 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

Firepower 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：

- 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。
- 设备高可用性允许在两个或更多个 7000 和 8000 系列设备或堆叠之间建立网络功能和配置数据的冗余。

多个管理接口

您可以使用 Firepower 管理中心、设备，或两者上的*多个管理接口*，将流量分离到两个流量信道中，以提高性能：*管理流量信道*承载设备间的通信，而*事件流量信道*承载高容量事件流量，如入侵事件。这两个流量信道可承载于同一管理接口或在两个管理接口之间分开，每个接口承载一个流量信道。

此外，您可以从 Firepower 管理中心上的一个特定管理接口，创建一条到另一个不同网络的路由，以便 Firepower 管理中心隔离和分开管理不同网络的设备流量。

其他管理接口的许多功能与默认管理接口相同，但以下情况除外：

- 只能在默认 (`eth0`) 管理接口上配置 DHCP。其他（`eth1` 等）接口需要唯一的静态 IP 地址和主机名。

- 如果 Firepower 管理中心和受管设备被一台 NAT 设备隔开，您必须配置两个流量信道以使用同一个非默认管理接口。
- 只能在默认管理接口上使用无人值守管理。
- 在 70xx 子系列上，您可以将流量分至两个信道并对信道进行配置，以将流量发送至 Firepower 管理中心上的一个或多个管理接口。但是，由于 70xx 子系列只带一个管理接口，该设备仅通过一个管理接口接收从 Firepower 管理中心发送来的流量。

在安装设备之后，请使用 Web 浏览器配置多个管理接口。有关详细信息，请参阅*《Firepower 管理中心配置指南》*中的“多个管理接口”。

网络流量管理

Firepower 系统的网络流量管理功能使得 7000 和 8000 系列设备成为公司网络基础设施的一部分。您可以执行以下操作：

- 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

发现和身份

思科的发现和感知技术能够收集主机、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。

可以使用 Firepower 管理中心的 Web 界面来查看和分析系统收集的数据。还可以使用发现和感知技术帮助您执行访问控制并修改入侵规则状态。

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：

- 检查协议报头值、负载内容和某些数据包大小特性的规则
- 基于 FireSIGHT 建议的规则状态配置
- 高级设置，例如预处理器和其他检测与性能功能
- 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，Firepower 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。这些轻量级代理与思科云通信，后者又与 Firepower 管理中心通信。

配置 Firepower 管理中心连接云之后，可以使用 Firepower 管理中心 Web 界面查看由于贵公司终端上的扫描、检测和隔离而生成的基于终端的恶意软件事件。Firepower 管理中心还使用 FireAMP 数据生成和跟踪主机上的危害表现以及显示网络文件轨迹。

网络文件轨迹功能可以跟踪网络中的文件传输路径。系统使用 SHA-256 哈希值跟踪文件。每个文件都具有相关的轨迹图，其中包含文件在一段时间内的传输轨迹视觉展示和与文件相关的其他信息。

可为网络服务、协调和服务管理功能体现出网络价值的

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 Firepower 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 Firepower 管理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。
- 补救措施是当满足网络上的某些条件时，Firepower 管理中心可以自动启动的程序。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 Firepower 系统

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

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

默认情况下，Firepower 管理中心可执行域控制、主机、应用和用户发现，以及解密和检查 SSL 和 TLS 加密的流量。

特定于功能的经典许可证允许受管设备执行各种功能，包括：

- 入侵检测和防御
- 安全情报过滤
- 文件控制和 Fireower 的 AMP

- 应用、用户和 URL 控制
- 交换和路由
- 设备高可用性
- 网络地址转换 (NAT)
- 虚拟专用网 (VPN) 部署

有多种方式可能让您失去对 Firepower 系统中许可功能的访问权。可从 Firepower 管理中心移除许可证，这将影响其所有受管设备。也可在特定受管设备上禁用已许可的功能。最后，某些许可证可能过期。虽然有一些例外情况，但不能使用与已到期或删除的许可证关联的功能。

以下内容总结了 Firepower 系统经典许可证：

保护

保护许可证允许受管设备进行入侵检测和防御、文件控制以及安全情报过滤。

可控性

控制许可证允许受管设备执行用户和应用控制、交换和路由（包括 DHCP 中继）和 NAT。它还允许将设备和堆栈配置到高可用性对。使用可控性许可证需要保护许可证。

URL 筛选

URL 筛选许可证允许受管设备基于受监控主机请求的 URL，使用定期更新的基于云的类别和信誉数据确定哪些流量可以流经网络。使用 URL 筛选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 许可证需要保护和可控性许可证。

有关经典许可证类型和限制的完整信息，请参阅*《Firepower 管理中心配置指南》*。

安全、互联网接入和通信端口

为了保护 Firepower 管理中心的安全，应将其安装在受保护的内部网络中。虽然 Firepower 管理中心已配置为仅拥有必需的服务和可用端口，但必须确保无法从防火墙外部攻击它（或任何受管设备）。

如果 Firepower 管理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 Firepower 管理中心相同的受保护内部网络。这样，就可以安全地从 Firepower 管理中心控制设备。您还可以配置多个管理接口，使 Firepower 管理中心能够管理和隔离来自其他网络上设备的流量。

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

另请注意，Firepower 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，系统还要求某些端口对基本内部设备通信保持开放以实现安全的设备访问，以便特定系统功能访问其正常运行所需的本地或互联网资源。

提示 除提供 FirePOWER 服务的思科 ASA 之外，Firepower 系统设备支持使用代理服务器。有关详细信息，请参阅《*Firepower 管理中心配置指南*》。

有关详情，请参阅：

- 互联网访问要求，第 1-12 页
- 通信端口要求，第 1-13 页

互联网访问要求

Firepower 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 1-13 页。请注意，大多数 Firepower 系统设备支持代理服务器；请参阅《*Firepower 管理中心配置指南*》中的“配置网络设置”一章。还请注意，代理服务器不能用于 whois 访问。

下表介绍了 Firepower 系统特定功能的互联网接入要求。

表 1-6　　Firepower 系统功能互联网接入要求

特性	需要互联网接入以便...	设备
动态分析：查询	查询综合安全情报云，了解以前提交进行动态分析的文件的威胁得分。	管理中心
动态分析：提交	提交文件至综合安全情报云进行动态分析。	受管设备
FireAMP 集成	接收来自 FireAMP 云的基于终端的 (综合安全情报云) 恶意软件事件。	管理中心
入侵规则、VDB 和 GeoDB 更新	直接下载或安排下载入侵规则、GeoDB 或 VDB 更新至设备。	管理中心
基于网络的 AMP	执行恶意软件云查找。	管理中心
RSS 源控制面板构件	从外部源下载 RSS 源数据，包括思科。	任何设备，除了虚拟设备和 ASA FirePOWER
安全情报过滤	从外部来源下载安全情报源数据，包括 Firepower 系统情报源。	管理中心
系统软件更新	将系统更新下载至设备或安排该等下载。	任何设备，除了虚拟设备和 ASA FirePOWER
URL 筛选	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。	管理中心
whois	请求外部主机的 whois 信息。	任何设备，除了虚拟设备和 ASA FirePOWER

通信端口要求

Firepower 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。其他开放端口允许：

- 访问设备的网络界面。
- 与设备的安全远程连接
- 系统的某些功能访问其正常运行所需的本地或互联网资源

一般来说，功能相关端口会保持关闭，直至启用或配置关联的功能。例如，在将 Firepower 管理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，7000 和 8000 系列设备上的 623/udp 端口会一直保持关闭，直至启用 LOM。

注意　在了解此操作对部署的影响之前，请**勿**关闭打开的端口。

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 *《Firepower 管理中心配置指南》*）。又例如，可通过关闭端口 443/tcp (HTTPS) 禁用对物理受管设备网络接口的接入，但是，这也可能阻止设备将可疑恶意软件文件提交给云端供动态分析。

请注意，系统允许更改其某些通信端口：

- 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 *《Firepower 管理中心配置指南》*。
- 您可以更改管理端口 (8305/tcp)；请参阅 *《Firepower 管理中心配置指南》*。但是，思科**强烈**建议保留默认设置。如果更改管理端口，则必须在部署中需要相互通信的所有设备上做出该更改。
- 可使用 32137/tcp 端口，以使升级的 Firepower 管理中心与综合安全情报云进行通信。但是，思科建议切换到端口 443。该端口为版本 6.0 及更高版本全新安装的默认端口。有关详细信息，请参阅 *《Firepower 管理中心配置指南》*。

下表列出了各种设备类型所要的开放端口，以便利用 Firepower 系统功能。

表 1-7　用于 Firepower 系统功能和操作的默认通 信端口

端口	说明	方向	开放对象...	目的
22/tcp	SSH/SSL	双向	任意	允计与设备进行安全远程连接。
25/tcp	SMTP	发送	任意	从设备发送邮件通知和警报。
53/tcp	DNS	发送	任意	使用 DNS。
67/udp 68/udp	DHCP	发送	任意	使用 DHCP。 **注意**　默认情况下，这些端口已**关闭**。
80/tcp	HTTP	发送	任何设备，除了虚拟设备和 ASA FirePOWER	允许 RSS 源控制面板构件连接至远程网络服务器。
		双向	管理中心	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 443 端口）。
161/udp	SNMP	双向	任何设备，除了虚拟设备和 ASA FirePOWER	允许通过 SNMP 轮询接入设备的 MIB。
162/udp	SNMP	发送	任意	发送 SNMP 警报至远程陷阱服务器。

表 1-7　用于 Firepower 系统功能和操作的默认通（续）信端口

端口	说明	方向	开放对象...	目的
389/tcp 636/tcp	LDAP	发送	任何设备，虚拟设备除外	与一个 LDAP 服务器通信，以进行外部身份验证。
389/tcp 636/tcp	LDAP	发送	管理中心	获取检测到的 LDAP 用户元数据。
443/tcp	HTTPS	接收	任何设备，除了虚拟设备和 ASA FirePOWER	接入设备的网络接口
443/tcp	HTTPS AMQP 云通信	双向	管理中心	获取： • 软件、入侵规则、VDB 和 GeoDB 更新 • URL 类别和信誉数据（还需要 80 端口） • 思科智能源和其他安全的安全情报源 • 基于端点的 (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
			7000 和 8000 系列设备	使用设备的本地网络界面下载软件更新。
			7000 和 8000 系列、虚拟设备、和 ASA FirePOWER	提交文件到思科云进行动态分析。
514/UDP	系统日志	发送	任意	发送警报至远程系统日志服务器。
623/udp	SOL/LOM	双向	7000 和 8000 系列	允许使用 LAN 上串行 (SOL) 连接执行无人值守管理。
1500/TCP 2000/TCP	数据库访问	接收	管理中心	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，除了虚拟设备和 ASA FirePOWER	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	接收	管理中心	与用户代理通信。
8302/tcp	eStreamer	双向	任何设备，虚拟设备除外	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。**需要。**
8307/tcp	主机输入客户端	双向	管理中心	与主机输入客户端通信。
32137/tcp	云通信	双向	管理中心	允许升级的管理中心与思科云进行通信。

预配置设备

您可以在一个中心位置预配置多台设备和 Firepower 管理中心，以便稍后用于其他站点的部署。关于预配置设备的考虑事项，请参阅预配置 Firepower 管理中心，第 D-1 页。

在管理网络上部署

您可以部署 Firepower 系统满足各个独特网络架构的需求。管理中心为 Firepower 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。

管理中心使用管理接口连接到*可信管理网络*（即未向外部公开流量的安全内部网络）。设备使用管理接口连接到管理中心。

然后设备使用感应接口连接到外部网络，以监控流量。有关如何在您的部署中使用感应接口的信息，请参阅*《Firepower 7000 和 8000 系列安装指南》*中的“部署 Firepower 受管设备”。

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

管理部署注意事项

管理部署决策依赖于各种因素。回答以下问题可以帮助您了解部署选项，从而配置最高效经济的系统：

- 您是否会使用默认的单一管理接口将您的设备连接到管理中心？您是否会启用额外的管理接口来提高性能，或者隔离管理中心上从不同网络接收的流量？有关详细信息，请参阅了解管理接口，第 2-1 页。
- 您是否想要启用流量信道来在管理中心和受管设备之间创建两个连接以提高性能？您是否想要使用多个管理接口来进一步提升管理中心和受管设备之间的吞吐能力？有关详细信息，请参阅使用流量信道进行部署，第 2-3 页。
- 您是否希望使用一个管理中心来管理和隔离来自不同网络上的设备的流量？有关详细信息，请参阅使用网络路由进行部署，第 2-4 页。
- 您是否是在受保护的环境中部署管理接口？设备访问权限是否限于特定的工作站 IP 地址？安全注意事项，第 2-4 页介绍安全部署管理接口方面的注意事项。
- 您是否正在部署 8000 系列设备？有关详细信息，请参阅特例：连接 8000 系列设备，第 2-4 页。

了解管理接口

管理接口提供管理中心与其管理的设备之间的通信方式。在设备之间维持良好的流量控制是部署成功的关键。

在管理中心和 Firepower 设备上，您可以启用管理中心、设备或这两者上的管理接口，从而将设备之间的流量归入两个独立的流量信道。*管理流量信道*传送所有内部流量（即特定于设备和系统管理的设备内部流量），*事件流量信道*传送所有事件流量（即大容量事件流量，例如入侵和恶意

软件事件）。将流量拆分到两个信道会在设备之间创建两个连接点，这会提高吞吐量，从而提高性能。您还可以启用*多个管理接口*，以在设备间提供更大的吞吐量，或管理和隔离来自不同网络上的设备的流量。

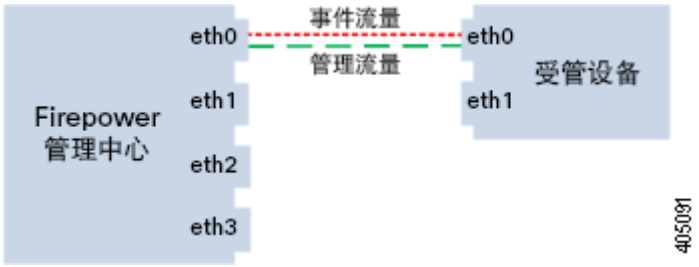
向管理中心注册设备后，可以更改默认配置，使用每个设备上的 Web 界面启用流量信道和多个管理接口。有关配置信息，请参阅《*Firepower 管理中心配置指南*》中的“配置设备设置”。

管理接口通常位于设备背面。有关详细信息，请参阅识别管理接口，第 3-2 页。

单一管理接口

当您向管理中心注册您的设备时，会建立一个传送管理中心上的管理接口和设备上的管理接口之间所有流量的通信信道。

下图显示默认的单一通信信道。一个接口传送包含管理和事件流量的通信信道。



多个管理接口

您可以启用并配置多个管理接口，每个接口使用指定的 IPv4 或 IPv6 地址和（可选的）主机名，通过将每个流量信道发送至不同的管理接口提高流量吞吐量。配置较小的接口传送较少的管理流量负载，配置较大的接口传送较大的事件流量负载。您可以注册设备以分离管理接口，并为同一接口配置两个通信信道，或者使用一个专用管理接口传送由管理中心管理的所有设备的事件流量信道。

此外，您可以从管理中心上的一个特定管理接口，创建一条到另一个不同网络的路由，以便管理中心隔离和分开管理不同网络的设备流量。

其他管理接口的许多功能与默认管理接口相同，但以下功能除外：

- 只能在默认 (`eth0`) 管理接口上配置 DHCP。其他（`eth1` 等）接口需要唯一的静态 IP 地址和主机名。思科建议您不设置其他管理接口的 DNS 条目，而是仅按 IP 地址为这些接口注册管理中心和设备。
- 当您使用一个非默认的管理接口来连接管理中心和受管设备，且这些设备被一台 NAT 设备隔开时，您必须配置两条流量信道使用同一个管理接口。
- 只能在默认管理接口上使用无人值守管理。
- 在 70xx 子系列上，您可以将流量分至两个信道并对信道进行配置，以将流量发送至管理中心上的一个或多个管理接口。但是，由于 70xx 子系列只带一个管理接口，该设备仅通过一个管理接口接收从管理中心发送来的流量。

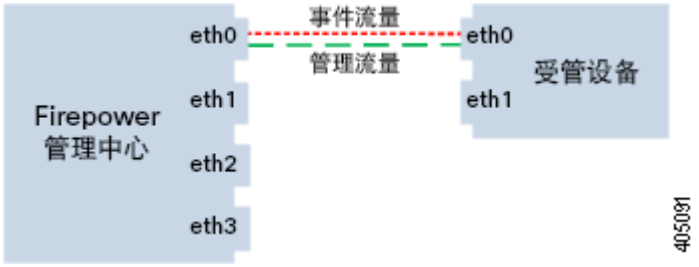
部署选项

可以使用流量信道管理流量，从而使用一个或多个管理接口改善系统性能。此外，可以使用管理中心及其受管设备上的特定管理接口创建到不同网络的路由，从而隔离不同网络上的设备之间的流量。有关详细信息，请参阅以下各节：

使用流量信道进行部署

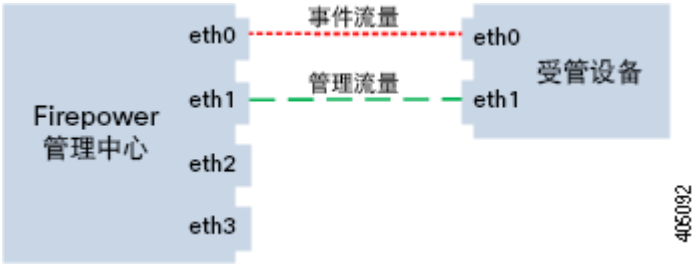
在一个管理接口上使用两个流量信道时，会在管理中心和受管设备之间创建两个连接。一个信道传送管理流量，一个信道传送事件流量，这两种流量在同一接口上单独进行传送。

以下示例显示同一接口上有两个独立流量信道的通信信道。



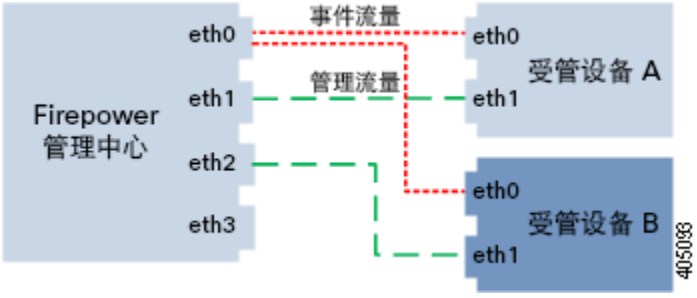
使用多个管理接口时，可以在两个管理接口上划分流量信道，进而可以通过添加两个接口的容量来增加流量，从而进一步提高性能。一个接口传送管理流量信道，另一个接口传送事件流量信道。如果任一接口发生故障，则所有流量重新路由到活动接口，并且连接得以维持。

下图显示了两个管理接口上的管理流量信道和事件流量信道。



可以使用专用管理接口仅传送来自多台设备的事件流量。在此配置中，每台设备分别注册到不同管理接口上以传送管理流量信道，并且管理中心上的一个管理接口传送来自所有设备的所有事件流量信道。如果任一接口发生故障，流量重新路由到活动接口，并且连接得以维持。请注意，由于所有设备的事件流量都在同一接口上传送，因此未在网络之间隔离流量。

下图显示了使用不同管理通道流量接口的两台设备共用相同的事件流量信道专用接口。



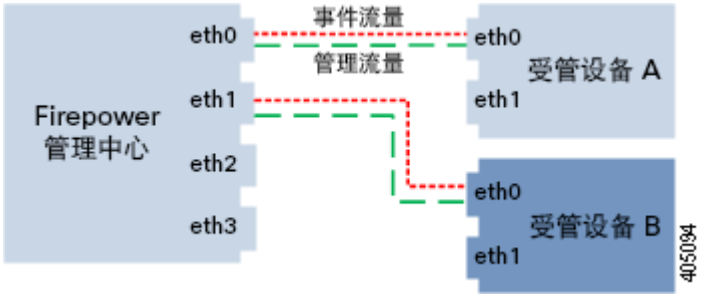
使用网络路由进行部署

您可以从管理中心上的特定管理接口创建通向不同网络的路由。当您从该网络向管理中心上指定的管理接口注册设备时，您将在管理中心和其他网络上的设备之间提供一个隔离连接。将两个流量信道配置为使用相同的管理接口，以确保来自该设备的流量与其他网络上的设备流量保持隔离。由于路由接口与管理中心上的所有其他接口隔离，因此，如果路由管理接口发生故障，连接会丢失。

提示　必须向除默认 (eth0) 管理接口外的任何管理接口静态 IP 地址注册设备。只有默认的管理接口上才支持 DHCP。

安装管理中心后，使用网络界面配置多个管理接口。有关详细信息，请参阅*《Firepower 管理中心配置指南》*中的“配置设备设置”。

下图显示通过为所有流量使用独立管理接口隔离网络流量的两台设备。您可以添加更多管理接口，为每台设备配置独立的管理和事件流量信道接口。



安全注意事项

要在安全环境中部署管理接口，思科建议您考虑以下事项：

- 务必将管理接口连接到未经授权不可访问的可信内部管理网络。
- 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*《Firepower 管理中心配置指南》*。

特例：连接 8000 系列设备

支持的设备：8000 系列

在向管理中心注册 8000 系列设备时，必须在连接两端自动协商或在两端设置相同的静态速度，以确保稳定的网络链路。8000 系列设备不支持半双工网络链路，也不支持两端的速度或双工配置存在差异的连接。

安装 Firepower 管理中心

Firepower 管理中心和 Firepower 受管设备可作为更大型 Firepower 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 Firepower 管理中心，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。

提示 您可以使用多个管理接口来提高性能，或者隔离和管理来自两个不同网络的流量。应在初始安装时配置默认管理接口 (`eth0`)。您可以在安装后通过用户界面配置其他管理接口。有关详细信息，请参阅 *《Firepower 管理中心配置指南》*。

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 Firepower 管理中心，第 D-1 页。

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

随附项目

以下列表列出了随管理中心一起提供的组件。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
- 单机架安装套件

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 *《Firepower 管理中心配置指南》*。

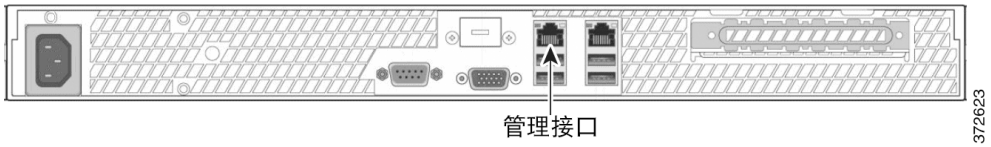
识别管理接口

可使用管理接口将部署中的每个设备连接到网络。这样，Firepower 管理中心可以与其托管的设备进行通信并管理这些设备。在执行安装操作步骤时，请务必参考正确的设备示意图：

Firepower 管理中心 750

MC750 可作为 1U 设备提供。以下机箱背面图示标出了 MC750 的默认管理接口的位置。

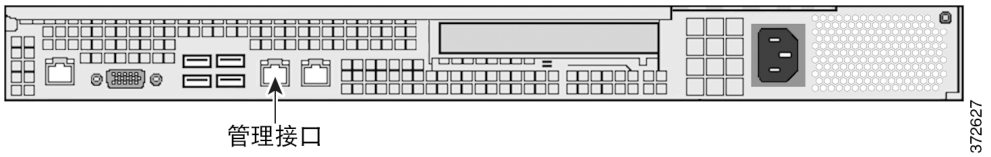
图 3-1　　MC750



Firepower 管理中心 1500

MC1500 可作为 1U 设备提供。以下机箱背面图示标出了默认管理接口的位置。

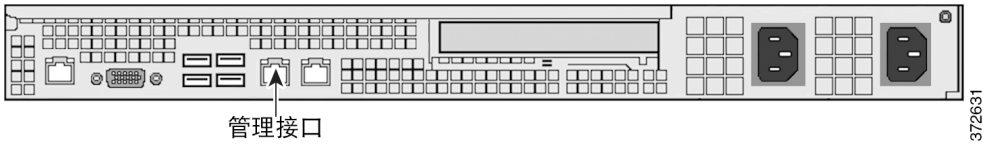
图 3-2　　MC1500



Firepower 管理中心 3500

MC3500 可作为 1U 设备提供。以下机箱背面图示标出了默认管理接口的位置。

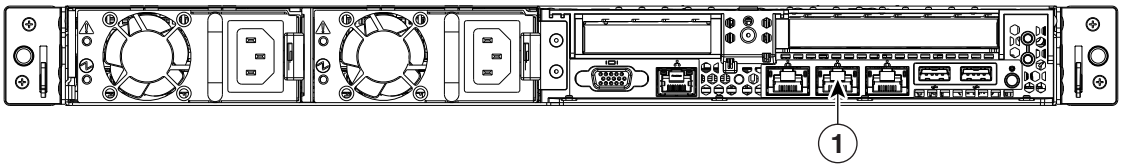
图 3-3　　MC3500



Firepower 管理中心 2000 和 4000

MC2000 和 MC4000 均为 1U 设备。以下机箱背面图示标出了 MC2000 和 MC4000 的默认管理接口 (1) 的位置。

图 3-4　　MC2000 和 MC4000



机架安装管理中心

您可以使用机架安装所有管理中心。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设备：

键盘和显示器/KVM

可以将 USB 键盘和 VGA 显示器连接到管理中心设备，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　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。

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，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。

在初始设置后，可通过以下其他方式访问控制台：

串行连接/笔记本电脑

可以使用设备的串行端口，将计算机连接到管理中心。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）。

Firepower 管理中心上的串行端口使用 RJ-45 连接。

将适当的反转线连接到设备后，如重定向控制台输出，第 3-4 页中所述重定向控制台输出。要确定每个设备型号的串行端口的位置，请使用硬件规格，第 5-1 页中的图。

使用 LAN 上串行进行无人值守管理

LOM 功能使您可以借助 SOL 连接在管理中心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 6-13 页。

注　无人值守管理仅适用于默认 (eth0) 管理接口。

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，请参阅将 Firepower 管理中心还原为出厂默认设置，第 6-1 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　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 5　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。

后续操作

- 继续下一章，设置 Firepower 管理中心，第 4-1 页。

重定向控制台输出

默认情况下，管理中心会将初始化状态（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。

使用外壳

您可以使用外壳重定向控制台输出。

要使用外壳重定向控制台输出，请执行以下操作：

访问权限：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。

系统将显示设备提示符。

步骤 2　在提示符后输入以下命令之一，能够设置控制台输出：

- 要使用 VGA 端口访问设备：

  ```
  sudo /usr/local/sf/bin/configure_console.sh vga
  ```

- 要使用物理串行端口访问设备：

  ```
  sudo /usr/local/sf/bin/configure_console.sh serial
  ```

- 要通过 SOL 使用 LOM 访问设备：

  ```
  sudo /usr/local/sf/bin/configure_console.sh sol
  ```

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。

使用网络界面

您还可以通过网络界面重定向控制台输出。

要使用 Web 界面重定向控制台输出，请执行以下操作：

访问权限：管理员

步骤 1　选择**系统 (System) > 许可证 (Licenses)**。

步骤 2　选择**控制台配置 (Console Configuration)**。

步骤 3　选择远程控制台访问选项：

- 选择 **VGA** 将会使用设备的 VGA 端口。这是默认选项。
- 选择**物理串行端口 (Physical Serial Port)** 将会使用设备的串行端口或使用管理中心上的 LOM/SOL。

  如果选择**物理串行端口 (Physical Serial Port)**，将显示 LOM 设置。

步骤 4　要通过 SOL 配置 LOM，请输入适当的设置：

- 设备的 **DHCP 配置 (DHCP Configuration)**（**DHCP** 或**静态 [Static]**）。
- 将要用于 LOM 的 **IP 地址 (IP Address)**。LOM IP 地址必须与设备的管理接口 IP 地址不同。
- 设备的**网络掩码 (Netmask)**
- 设备的**默认网关 (Default Gateway)**。

步骤 5　点击**保存 (Save)**。

将会保存设备的远程控制台配置。如果配置了无人值守管理，则必须至少为一个用户启用此功能；请参阅启用 LOM 和 LOM 用户，第 6-13 页。

设置 Firepower 管理中心

部署并安装 Firepower 管理中心后，必须完成设置过程，以便新设备能够在可信管理网络上通信。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，您可以执行多种初始管理级别的任务，例如设置时间、注册和许可设备及安排更新。设置和注册过程中所选择的选项决定系统将要创建并应用到受管设备的默认接口、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 Firepower 管理中心，都可以随时使用管理中心更改其配置。

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 4-1 页介绍了设置过程。

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。

- 配置管理中心网络设置，第 4-3 页说明了如何使用脚本来指定网络设置，以使新的 Firepower 管理中心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管理中心都需要执行该步骤。
- 初始设置页面：管理中心，第 4-4 页说明了如何使用管理中心的网络界面来完成其初始设置。
- 后续步骤，第 4-8 页包含了设置 Firepower 系统部署时可能执行的设置后任务的相关指南。

注意 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，如果由于任何原因需要关机，请使用 *《Firepower 管理中心配置指南》* 中的“系统配置”一章中的程序，或从设备的外壳运行 `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 Firepower 管理中心之后，必须完成设置流程。开始设置之前，请确保符合以下条件。

型号

您必须知道设置的是什么设备。有关详细信息，请参阅 Firepower 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，请参阅机架安装管理中心，第 3-3 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 Firepower 管理中心。在设备初始设置流程中，您可以将设备预注册到管理中心；在管理中心的设置过程中，可添加并许可已预注册的受管设备。

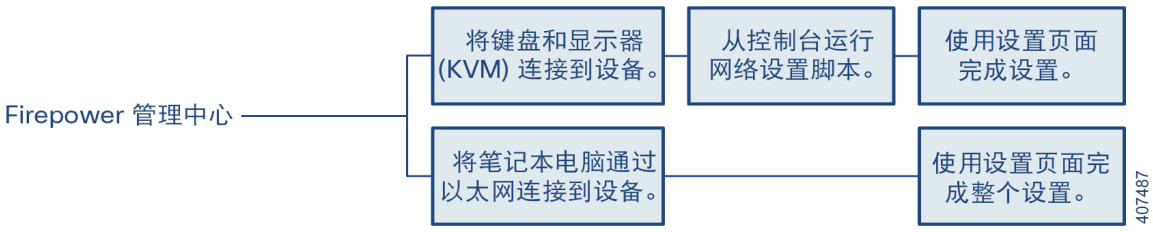
完成设置后，可使用 Firepower 管理中心的 Web 界面来执行部署相关的大部分管理和分析任务。请注意 Firepower 设备的 Web 界面受限，只能用于执行基本的管理任务。有关详细信息，请参阅后续步骤，第 4-8 页。

提示 如果在设置设备前已恢复出厂默认设置（请参阅将 Firepower 管理中心还原为出厂默认设置，第 6-1 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：管理中心，第 4-4 页。

开始设置

访问权限：管理员

下图展示了设置管理中心时可做的选择：



要设置管理中心，请执行以下操作：

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；请参阅配置管理中心网络设置，第 4-3 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。

后续操作

- 从管理网络上的计算机浏览至设备的 Web 界面，以完成设置流程；参阅初始设置页面：管理中心，第 4-4 页。

配置管理中心网络设置

访问权限：管理员

安装新的管理中心或在重新映像期间删除其网络设置后，您必须配置设备以使其能够在管理网络上通信。通过在控制台运行脚本完成该步骤。

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

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

请注意，脚本将提示设置信息，这些信息与管理中心的设置网页提示的信息大致相同；参阅网络设置，第 4-5 页。

要使用脚本配置网络设置，请执行以下操作：

步骤 1　在控制台上登录管理中心。使用 `admin` 作为用户名，`Admin123` 作为密码。

步骤 2　在管理员提示符下，运行以下脚本：

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

步骤 3　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　注销管理中心。

后续操作

- 要使用管理中心的 Web 界面完成其设置，请参阅初始设置页面：管理中心，第 4-4 页。

初始设置页面：管理中心

访问权限：管理员

对于所有的管理中心，您必须通过登录管理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，必须在设备上完成设置流程，并将管理中心添加为远程管理器，否则，注册将失败。

有关详细信息，请参阅按照受管设备型号划分的受支持功能，第 1-6 页和许可 Firepower 系统，第 1-10 页。

要使用网络界面在管理中心上完成初始设置，请执行以下操作：

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

- 对于通过以太网线连接至计算机的管理中心，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管理中心，使用管理网络上的计算机浏览至管理中心的管理接口 IP 地址。

步骤 2　使用 `admin` 作为用户名，`Admin123` 作为密码登录。

有关完成设置的详细信息，请参阅以下各节：

- 更改密码，第 4-5 页
- 网络设置，第 4-5 页
- 时间设置，第 4-5 页
- 重复规则更新导入，第 4-5 页
- 重复地理位置更新，第 4-6 页
- 自动备份，第 4-6 页
- 许可证设置，第 4-6 页
- 设备注册，第 4-6 页
- 最终用户许可协议，第 4-7 页

步骤 3　完成设置后，点击**应用 (Apply)**。

管理中心会根据您的选择进行配置。您已经以管理员用户（具有管理员角色）身份登录 Web 界面。

注　如果使用以太网线直接连接至设备，可断开计算机并将管理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 地址或主机名的管理中心，并完成本指南中的剩余步骤。

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

此页面每隔 10 秒自动更新一次。在页面为初始设备注册和策略应用任务列出**已完成 (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，该管理中心可以使用了。有关配置部署的详细信息，请参阅《*Firepower 管理中心配置指南*》。

后续操作

- 继续执行后续步骤，第 4-8 页。

更改密码

您必须更改管理员帐户的密码。该帐户拥有管理员权限，您无法将其删除。

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

网络设置

管理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。

Firepower 系统为 IPv4 和 IPv6 管理环境提供了双堆栈实施。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**使用路由器自动配置分配 IPv6 地址 (Assign the IPv6 address using router autoconfiguration)** 复选框，自动分配 IPv6 网络设置。否则，必须以冒号隔开的十六进制格式设置地址和前缀的位数（例如：前缀长度为 112）。

还可以指定最多三个 DNS 服务器以及设备的主机名和域。

时间设置

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

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

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**启用重复规则更新导入 (Enable Recurring Rule Update Imports)**。

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

注　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

Firepower 管理中心可显示与系统生成的事件相关的路由 IP 地址的地理信息，并监控控制面板和 Context Explorer 中的地理位置统计信息。

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

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

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

自动备份

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

启用该设置后，将创建一项定期任务，即对管理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 Firepower 系统部署。您可使用 Firepower 管理中心为其本身及其管理的设备管理许可证。Firepower 系统提供的许可证类型取决于您要管理的设备类型：

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

默认情况下，Firepower 管理中心可执行域控制、主机、应用和用户发现，以及解密和检查 SSL 和 TLS 加密的流量。特定于功能的经典许可证允许受管设备执行各种功能；参阅按照受管设备型号划分的受支持功能，第 1-6 页和许可 Firepower 系统，第 1-10 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管理中心；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。

有关许可的完整信息，请参阅*《Firepower 管理中心配置指南》*。

设备注册

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

注　在将设备注册至管理中心之前，您**必须**在设备上配置远程管理。

在初始设置过程中，可以将大多预注册设备添加到管理中心。但是，如果设备和管理中心由一台 NAT 设备隔开，您必须在设置过程完成后进行添加；请参阅*《Firepower 7000 和 8000 系列安装指南》*。

注　当您使用一个非默认的管理接口来连接管理中心和受管设备，且这些设备被一台 NAT 设备隔开时，您必须配置两条流量信道使用同一个管理接口。有关详细信息，请参阅在管理网络上部署，第 2-1 页。

在管理中心注册受管设备时，如果希望注册后将访问控制策略自动应用于设备，请启用**应用默认访问控制策略 (Apply Default Access Control Policies)** 复选框。请注意，您无法选择管理中心对每台设备应用哪项策略，只能选择是否应用这些策略。应用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*《Firepower 7000 和 8000 系列安装指南》*中的“设置 Firepower 受管设备”），如下表所示。

表 4-1　　按检测模式所应用的默认访问控制策略

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

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

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

要添加设备，请键入在设备注册时指定的**主机名 (Hostname)** 或 **IP 地址 (IP Address)**，以及**注册密钥 (Registration Key)**。请记住，这是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管理中心的许可证；请参阅许可证设置，第 4-6 页。

并非所有受管设备均支持所有许可证。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。这是因为管理中心稍后才能确定设备型号。系统无法启用无效的许可证，而且尝试启用无效的许可证不会减少可用许可证的数量。

有关许可的详细信息，包括可以使用哪些管理中心向每种设备型号应用每个许可证，请参阅Firepower 管理中心型号支持的功能，第 1-5 页、按照受管设备型号划分的受支持功能，第 1-6 页和许可 Firepower 系统，第 1-10 页。

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

最终用户许可协议

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

管理中心会根据您的选择进行配置。您已经以管理员用户（具有管理员角色）身份登录 Web 界面。继续初始设置页面：管理中心，第 4-4 页中的第 3 步，完成管理中心的初始设置。

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*《Firepower 管理中心配置指南》*。

单个用户帐户

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

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

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

运行状况和系统策略

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

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

软件和数据库更新

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

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

硬件规格

管理中心在各种平台上提供，以满足组织的需求。

机架和机柜安装选项

可以将管理中心安装在机架和服务器机柜中。该设备附带机架安装套件。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。

可以为其他设备单独购买机架和机柜安装套件。

管理中心

有关管理中心的详细信息，请参阅以下各节：

- MC750，第 5-1 页
- MC1500，第 5-5 页
- MC3500，第 5-9 页
- MC2000 和 MC4000，第 5-14 页

MC750

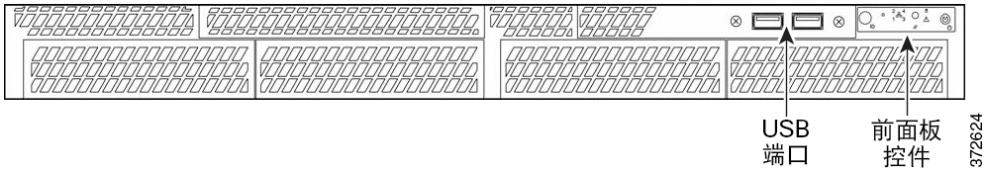
MC750 是 1U 设备。有关详细信息，请参阅以下各节：

- MC750 机箱前视图，第 5-2 页
- MC750 机箱后视图，第 5-3 页
- MC750 物理和环境参数，第 5-4 页

MC750 机箱前视图

MC750 机箱前面包含前面板控件。

图 5-1　　MC750



下图显示了 MC750 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 5-2　　MC750

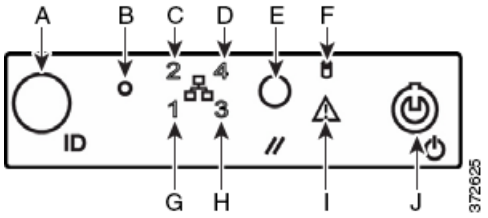


表 5-1　　前面板组件

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	Y	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 5-2　　MC750 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，请参阅表 5-3，第 5-3 页。
功率	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。

表 5-2　　MC750 前面板 LED（续）

LED	说明
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。服务器主板还提供一个插针，供插件控制器访问此指示灯。
NIC 活动	指示系统和网络之间的活动。 • 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。

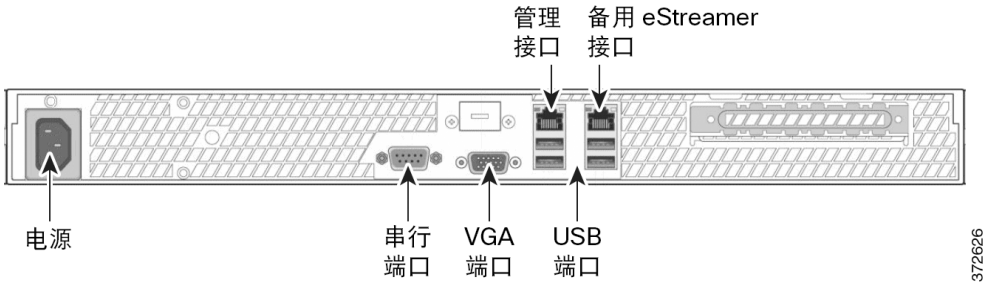
表 5-3　　MC750 系统状态

情况	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 • 通过系统 BIOS 设置故障指示命令；BIOS 可以使用命令来指示其他非严重的状态，例如，系统内存或 CPU 配置更改
降级	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

MC750 机箱后视图

机箱后部包含 MC750 的电源和连接端口。

图 5-3　　MC750



下表介绍显示在设备背面的功能。

表 5-4　　MC750 系统组件：后视图

特性	说明
电源	通过交流电源向管理中心供电。
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 管理接口位于设备背面。下表介绍了与管理接口相关的 LED。

表 5-5　　MC750 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。

MC750 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 5-6　　MC750 物理和环境参数

参数	MC750
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	在 95°F (35°C) 下为 90%，无冷凝
噪声	在典型办公室环境温度下处于空闲状态时为 7 BA (73°F +/- 4°F，23°C +/- 2°C)
工作冲击	在 2G 半正弦波冲击下无错误（11 毫秒持续时间）
包装冲击	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）

表 5-6　　MC750 物理和环境参数（续）

参数	MC750
ESD	空气放电，+/- 12 kV；接触放电，8 K
气流	正面到背面
系统冷却需求	1660 BTU/小时

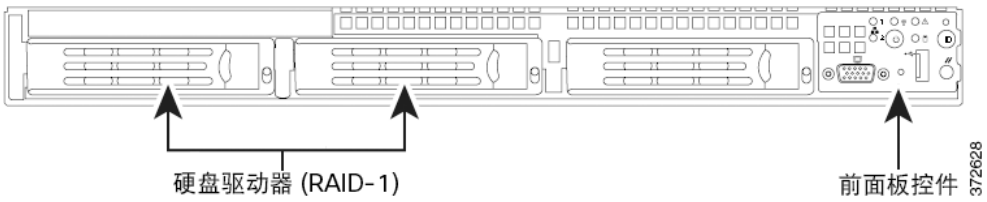
MC1500

MC1500 是 1U 设备。有关详细信息，请参阅以下各节：

- MC1500 机箱前视图，第 5-5 页
- MC1500 机箱后视图，第 5-7 页
- MC1500 物理和环境参数，第 5-8 页

MC1500 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。

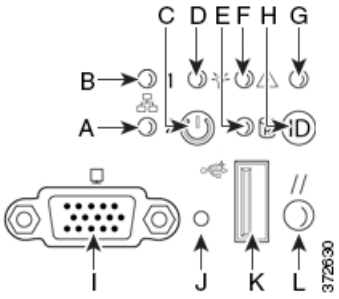


表 5-7　　前面板组件

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	Y	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 5-8　　MC1500 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。服务器主板还提供一个插针，供插件控制器访问此指示灯。
系统状态	指示系统状态： • 绿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。 • 琥珀色指示灯表示系统处于严重的或不可恢复的状况。 • 闪烁的琥珀色指示灯表示系统处于不严重的状况。 • 指示灯不亮表示正在进行开机自检 (POST) 或系统已停机。 **注意**　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，请参阅表 5-3，第 5-3 页。
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。

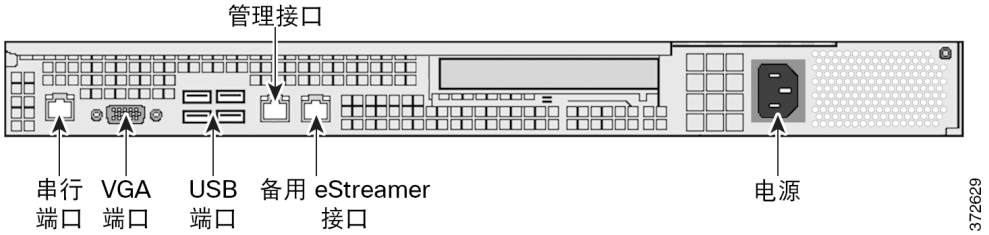
下表介绍了系统状态 LED 可能亮起的状况。

表 5-9　　MC1500 系统状态

情况	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 • 通过系统 BIOS 设置故障指示命令；BIOS 可以使用命令来指示其他非严重的状态，例如，系统内存或 CPU 配置更改
降级	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

MC1500 机箱后视图

机箱背面包含连接端口和电源。



下表介绍显示在设备背面的功能。

表 5-10　　MC1500 系统组件：后视图

特性	说明
电源	通过交流电源向管理中心供电。
VGA 端口 USB 端口	可用于将显示器、键盘和鼠标连接到管理中心上。
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**用于维护和配置用途，并非意在传输业务流量。 **注意**　不能同时使用前后面板串行端口。

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

表 5-11　　MC1500 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。

串行端口位于设备的背面。下表描述了 DB-9 连接器上的信号。

表 5-12　　MC1500 串行端口引脚分配

引脚	信号	说明
1	DCD	载波检测
2	RD	接收数据
3	TD	传输数据
4	DTR	数据终端就绪
5	接地线	接地
6	DSR	数据设置就绪
7	RTS	请求发送
8	CTS	允许发送
9	RI	振铃指示器

MC1500 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 5-13　　MC1500 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 厘米 x 43.0 厘米 x 4.3 厘米）
最大重量	34 磅（15.4 千克）
电源	120 VAC 的 600 W 电源 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	在 82.4°F (28°C) 下为 90%，无冷凝

表 5-13　MC1500 物理和环境参数（续）

参数	说明
噪声	在典型办公室环境温度下处于空闲状态时为 7 BA（机架安装） (73°F +/- 4°F，23°C +/- 2°C)
工作冲击	在 2G 半正弦波冲击下无错误（11 毫秒持续时间）
包装冲击	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	正面到背面
系统冷却需求	2550 BTU/小时

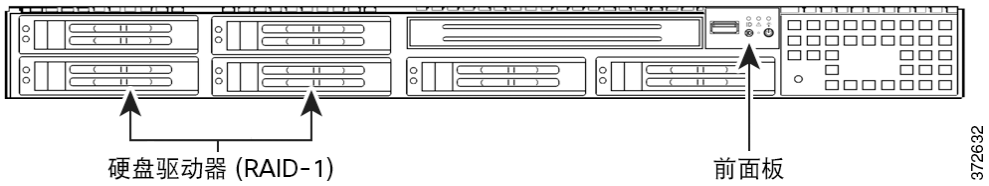
MC3500

MC3500 是 1U 设备。有关详细信息，请参阅以下各节：

- MC3500 机箱前视图，第 5-9 页
- MC3500 机箱后视图，第 5-11 页
- MC3500 物理和环境参数，第 5-13 页

MC3500 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。

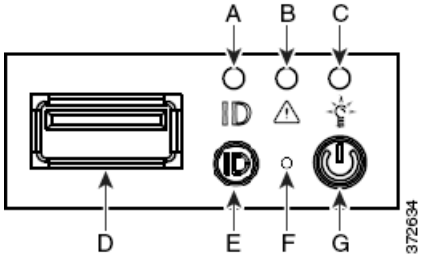


表 5-14　前面板组件

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 5-15　MC3500 前面板 LED

LED	说明
功率	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。 • 闪烁的琥珀色指示灯表示系统处于不严重的状况。 • 琥珀色指示灯表示系统处于严重的或不可恢复的状况。 • 指示灯不亮表示系统正在启动或已关闭。 **注意**　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，请参阅表 5-16，第 5-10 页。
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。
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 5-16　MC3500 系统状态

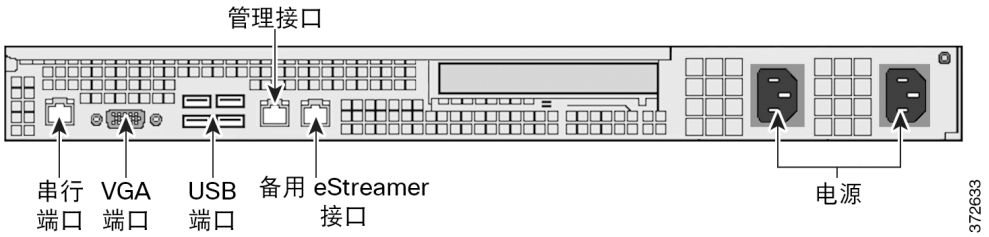
情况	说明
严重	由于以下事件导致的任何严重或不可恢复的超出阈值状况： • 超出温度、电压或风扇重要阈值 • 电源子系统故障 • 由于处理器安装不正确或处理器不兼容系统无法启动 • 重要事件记录错误，包括系统内存无法纠正的 ECC 错误和毁灭性/无法纠正的总线错误，例如 PCI SERR 和 PERR

表 5-16　　MC3500 系统状态（续）

情况	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 • 通过系统 BIOS 设置故障指示命令；BIOS 可以使用命令来指示其他非严重的状态，例如，系统内存或 CPU 配置更改
降级	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。关闭设备电源，断开两条电源线，重新连接电源线，然后重新启动设备。 ⚠ **注意**　要安全关闭电源，请使用《*Firepower 管理中心配置指南*》中的“管理设备”一章中的操作步骤，或从管理中心外壳运行 `shutdown -h now` 命令。

MC3500 机箱后视图

机箱背面包含连接端口和电源。



下表介绍显示在设备背面的功能。

表 5-17　　MC3500 系统组件：后视图

特性	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拇指驱动器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**用于维护和配置用途，并非意在传输业务流量。 **注意**　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 管理接口位于设备背面。下表介绍了与管理接口相关的 LED。

表 5-18　MC3500 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背面。下表介绍了与双电源关联的 LED。

表 5-19　MC3500 电源 LED

LED	说明
关闭	没有接通电源。
琥珀色	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。
琥珀色闪烁	出现高温或风扇转速缓慢等电源警告事件；电源继续运行。
绿色闪烁	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。

串行端口位于设备的背面。下表描述了 DB-9 连接器上的信号。

表 5-20　MC3500 串行端口引脚分配

引脚	信号	说明
1	DCD	载波检测
2	RD	接收数据
3	TD	传输数据
4	DTR	数据终端就绪
5	接地线	接地
6	DSR	数据设置就绪
7	RTS	请求发送
8	CTS	允许发送
9	RI	振铃指示器

USB 端口位于设备的背面。下表描述了 USB 连接器上的信号。

表 5-21　　MC3500 内部 USB 连接器引脚布局

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

MC3500 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 5-22　　MC3500 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 VAC 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	在 95°F (35°C) 下为 90%，无冷凝
噪声	在典型办公室环境温度下处于空闲状态时为 7 BA（机架安装） (73°F +/- 4°F，23°C +/- 2°C)
工作冲击	在 2G 半正弦波冲击下无错误（11 毫秒持续时间）
包装冲击	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 +/- 8KV）
气流	正面到背面
系统冷却需求	2550 BTU/小时
RoHS	符合 RoHS 指令 2002/95/EC

MC2000 和 MC4000

MC2000 和 MC4000 是 1U 设备。有关此设备的详细信息，请参阅以下各节：

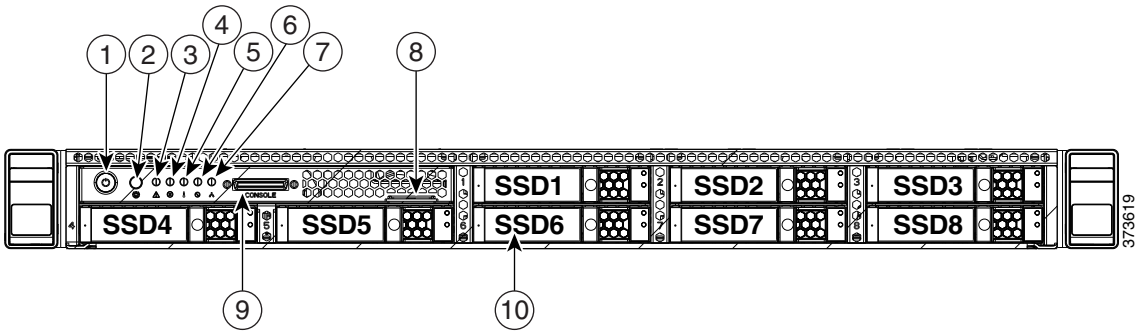
- MC2000 和 MC4000 机箱前视图，第 5-14 页
- MC2000 和 MC4000 机箱后视图，第 5-16 页
- MC2000 和 MC4000 物理和环境参数，第 5-17 页

MC2000 和 MC4000 机箱前视图

机箱前面包含存储驱动器、前面板和 KVM 连接器。机箱最多容纳八个小型封装 (SFF) 2.5 英寸存储驱动器。

- MC2000 机箱配有四个串行连接 SCSI (SAS) 驱动器。
- MC4000 机箱配有六个固态驱动器 (SSD)。

下图显示设备的前面板功能，包括前面板控件、LED 和存储驱动器布局。对于 MC2000 和 MC4000，存储驱动器槽位从左到右编号，从顶行开始，然后在底行继续从左到右编号。



1	电源按钮/电源状态 LED	6	电源状态 LED
2	标识按钮/LED	7	网络链路活动 LED
3	系统状态 LED	8	拉出式资产标签
4	风扇状态 LED	9	KVM 连接器（与 KVM 电缆一起使用，提供两个 USB，一个 VGA 和一个串行连接器）
5	温度状态 LED	10	驱动器，支持热插拔（最多 8 个 2.5 英寸驱动器）

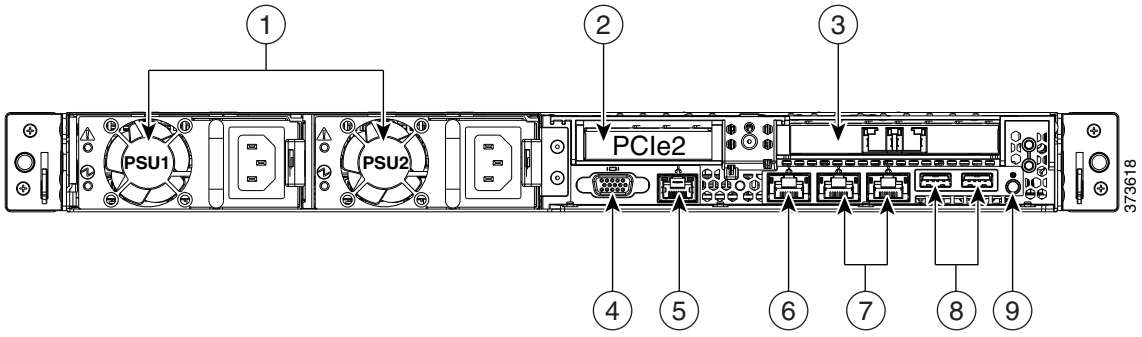
机箱的前面板包括七个 LED，显示系统的运行状态。MC2000 和 MC4000 前面板 LED，状态定义表介绍前面板上的 LED。

表 5-23　　MC2000 和 MC4000 前面板 LED，状态定义

LED 名称	状态
电源按钮/电源状态 LED	• 熄灭 - 服务器没有交流电源。 • 琥珀色 - 服务器处于备用电源模式。仅向 CIMC 和一些主板功能供电。 • 绿色 - 服务器处于主电源模式。向所有服务器组件供电。
标识	• 熄灭 - 未使用标识 LED。 • 蓝色 - 已激活标识 LED。
系统状态	• 绿色 - 服务器在正常工作条件下运行。 • 绿色（闪烁）- 服务器正在执行系统初始化和内存检查。 • 琥珀色（稳定）- 服务器处于降级运行状态。例如： – 失去电源冗余。 – CPU 不匹配。 – 至少一个 CPU 出现故障。 – 至少一个 DIMM 出现故障。 – RAID 配置中至少一个驱动器出现故障。 • 琥珀色（闪烁）- 服务器处于致命故障状态。例如： – 启动失败。 – 检测到严重的 CPU 和/或总线错误。 – 服务器处于过热状态。
风扇状态	• 绿色 - 所有风扇模块均正常运行。 • 琥珀色（恒亮） - 一个风扇模块出现故障。 • 琥珀色（闪烁） - 关键故障，两个或多个风扇模块出现故障。
温度状态	• 绿色 - 服务器在正常温度下运行。 • 琥珀色（恒亮） - 一个或多个温度传感器超出警告阈值。 • 琥珀色（闪烁） - 一个或多个温度传感器超出关键阈值。
电源状态	• 绿色 - 所有电源均正常供电。 • 琥珀色（恒亮） - 一个或多个电源处于降级运行状态。 • 琥珀色（闪烁） - 一个或多个电源处于关键故障状态。
网络链接活动	• 熄灭 - 以太网链路闲置。 • 绿色 - 一个或多个以太网 LOM 端口处于链路激活状态，但是没有活动。 • 绿色（闪烁） - 一个或多个以太网 LOM 端口处于链路激活状态，并且有活动。
硬盘驱动器故障	• 熄灭 - 硬盘驱动器正常运行。 • 琥珀色 - 硬盘驱动器出现故障。 • 琥珀色（闪烁）- 设备正在重建。
硬盘驱动器活动	• 熄灭 - 硬盘驱动器滑板中没有硬盘驱动器（无访问、无故障）。 • 绿色 - 硬盘驱动器准备就绪。 • 绿色（闪烁） - 硬盘驱动器正在读取或写入数据。

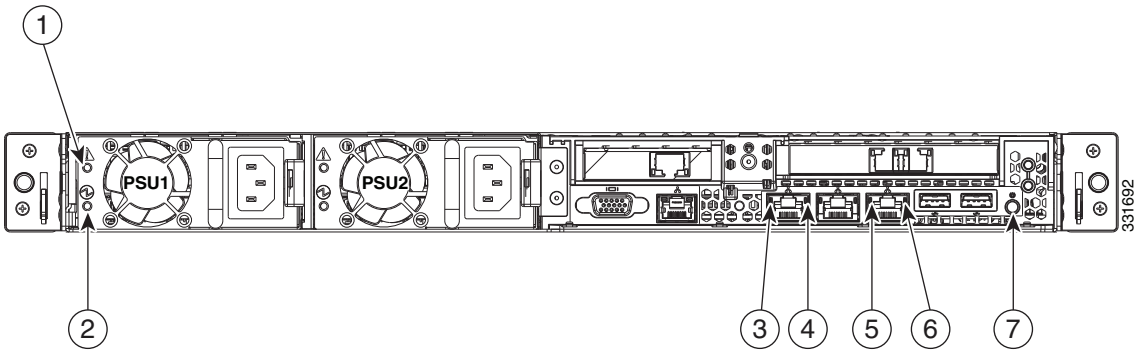
MC2000 和 MC4000 机箱后视图

机箱背面包含连接端口和电源。设备提供一个 1Gb 以太网默认管理接口，两个 1Gb Base-T 以太网端口，一个 RS-232 串行端口（RJ-45 连接器），一个 15 引脚 VGA 连接器和两个 USB 2.0 连接器。下图显示了设备的背面。



1	电源（两个）	6	1Gb 以太网默认管理接口
2	提升板上的薄型 PCIe 插槽 2 （半高，半长，x8 通道）	7	两个 1 Gb 以太网端口 (LAN1 和 LAN2)
3	两个 10 Gb 以太网端口	8	USB 端口
4	VGA 视频连接器	9	背部识别按钮/LED
5	串行端口（RJ-45 连接器）		–

下图标出了设备背面与连接端口和电源相关的 LED 及系统识别按钮。



1	电源故障 LED	5	1 Gb 以太网链路速度 LED
2	电源状态 LED	6	1 Gb 以太网链路状态 LED
3	1Gb 以太网默认管理接口链路状态 LED	7	背部识别按钮/LED
4	1Gb 以太网默认管理接口链路速度 LED		–

MC2000 和 MC4000 后面板 LED，状态定义表介绍了机箱背面与默认管理接口相关以及位于设备背面的其他连接端口、电源和系统识别按钮相关的 LED。

表 5-24　　MC2000 和 MC4000 后面板 LED，状态定义

LED 名称	状态
电源故障	• 熄灭 - 电源正常供电。 • 琥珀色（闪烁）- 已达到某个事件警告阈值，但是电源仍在继续工作。 • 琥珀色（恒亮）- 已达到某个致命故障阈值，导致电源停止供电（例如，风扇故障或过热条件）。
电源状态	交流电源： • 熄灭 - 没有连接到电源的交流电源。 • 绿色（闪烁）- 交流电源状态良好，未启用直流输出。 • 绿色（恒亮）- 交流电源状态良好，直流输出状态良好。 直流电源： • 熄灭 - 没有连接到电源的直流电源。 • 绿色（闪烁）- 直流电源状态良好，未启用直流输出。 • 绿色（恒亮）- 直流电源状态良好，直流输出状态良好。
1Gb 以太网默认管理接口链路速度	• 熄灭 - 链路速度为 10Mbps。 • 琥珀色 - 链路速度为 100Mbps。 • 绿色 - 链路速度为 1Gbps。
1Gb 以太网默认管理接口链路状态	• 熄灭 - 无链路存在。 • 绿色 - 链路处于激活状态。 • 绿色（闪烁）- 激活链路中存在流量。
1GB 以太网链路速度	• 熄灭 - 链路速度为 10Mbps。 • 琥珀色 - 链路速度为 100Mbps。 • 绿色 - 链路速度为 1Gbps。
1GB 以太网链路状态	• 熄灭 - 无链路存在。 • 绿色 - 链路处于激活状态。 • 绿色（闪烁）- 激活链路中存在流量。
标识	• 熄灭 - 未使用标识 LED。 • 蓝色 - 已激活标识 LED。

MC2000 和 MC4000 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 5-25　　MC2000 和 MC4000 物理和环境参数

参数	说明
外形	1U
尺寸（长 x 宽 x 高）	28.5 英寸 x 16.9 英寸 x 1.7 英寸（72.4 厘米 x 42.9 厘米 x 4.3 厘米）
重量	35.6 磅（16.1 千克）最多（8 个 SSD、2 个 CPU、16 个 DIMM、2 个电源） 22 磅（10 千克）裸机（0 个 SSD、0 个 CPU、0 个 DIMM、1 个电源）

表 5-25　　MC2000 和 MC4000 物理和环境参数（续）

参数	说明
电源	双 650 W 冗余电源 交流输入电压： 90 至 264 VAC 自适应范围 100 至 120 VAC 额定范围 200 至 240 VAC 额定范围 交流输入频率： 47 至 63Hz（单相，50 至 60 Hz 额定值） 最大交流输入电流： 在 100 V 下，最大 7.6 A 在 208 V 下，最大 3.65 A 最大交流突入电流： 11A 最大输出功率： 650 W 电源输出电压： 主电源：12VDC 备用电源：12VDC
工作温度	41°F 至 104°F（5°C 至 40°C） 海拔高速每上升 305 米，最高温度下降 33.8° F (1°C)。
非工作温度	-40°F 至 149°F（-40°C 至 65°C）
非工作湿度（相对），无冷凝	10% 至 90%
工作海拔高度	0 至 10000 英尺（0 至 3000 米）
非工作海拔高度	0 至 40000 英尺（0 至 12192 米）
声功率级 依据 ISO7779 标准测量 A 计权声功率级（贝尔） 工作温度 73°F (23°C)	5.4
声压级 依据 ISO7779 标准测量 A 计权声压级 (dBA) 工作温度 73°F (23°C)	37
气流	从前到后

将 Firepower 管理中心还原为出厂默认设置

思科在其支持站点提供 ISO 映像，用以将管理中心还原或重新映像为其原始出厂设置。

有关详细信息，请参阅以下各节：

准备工作

开始将设备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。

了解还原流程

访问权限：管理员

要还原管理中心，首先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。为方便起见，可以在还原流程中安装系统软件和入侵规则更新。

只能在维护窗口中重新映像设备。

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。如有可远程访问的 KVM，无需物理访问即可还原设备。

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。

使用 LAN 上串行进行无人值守管理

可以通过 LAN 上串行 (SOL) 连接使用无人值守管理 (LOM) 在管理中心上执行一系列有限的操作。如果您没有对设备的物理访问权限，可以使用 LOM 执行还原流程。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。请注意，只能在默认 (`eth0`) 管理接口使用无人值守管理。有关详细信息，请参阅设置无人值守管理，第 6-13 页。

准备工作

- 从支持站点获取设备的还原 ISO 映像。请参阅要获取还原 ISO 和其他更新文件，请执行以下操作：第 6-3 页

要还原管理中心，请执行以下操作：

步骤 1　将映像复制到适当的存储介质中。

步骤 2　连接设备。

步骤 3　重新启动设备并调用还原实用程序。

后续操作

- 使用要还原管理中心，请执行以下操作：第 6-2 页中的程序安装 ISO 映像。

获取还原 ISO 和更新文件

访问权限：任意

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：5.3 或 5.4）。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。

管理中心使用内部闪存驱动器启动设备，确保可以运行还原实用程序。

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*《Firepower 管理中心配置指南》*。

为方便起见，可以在还原流程中安装系统软件和入侵规则更新。例如，可以将设备还原到 6.0 版本，在该流程中，还可以将设备更新到 6.0.0.1 版本。切记只有管理中心要求规则更新。

要获取还原 ISO 和其他更新文件，请执行以下操作：

步骤 1　使用支持帐户的用户名和密码登录支持站点 (https://sso.cisco.com/autho/forms/CDClogin.html)。

步骤 2　浏览到软件下载部分 (https://software.cisco.com/download/navigator.html)。

步骤 3　在您想要下载和安装的系统软件显示的页面上，在**查找 (Find)** 区域中输入搜索字符串。

例如，要查找管理中心的软件下载，您可以输入 **Management Center**。

步骤 4　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**规则更新 (Rules Updates)** 查看入侵规则和漏洞数据库 (VDB) 更新，然后浏览 Firepower 管理中心软件的正确版本的版本号。

步骤 5　点击要下载的 ISO 映像或添加到购物车中。

文件开始下载。

步骤 6　将文件复制到设备在其管理网络上可以访问的 HTTP (Web) 服务器、FTP 服务器或支持 SCP 的主机上。

注意　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

通过从内部闪存驱动器启动设备，开始还原流程。

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 6-4 页说明如何对不具备 LOM 访问权限的设备开始还原流程。
- 使用无人值守管理启动还原实用程序，第 6-5 页说明如何使用 LOM 通过 SOL 连接开始还原流程。

注意　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，请使用设备的 Web 界面或从设备的外壳运行 `shutdown -h now` 命令（有时称为专家模式）。

使用 KVM 或物理串行端口启动还原实用程序

访问权限：管理员

对于管理中心，思科在内部闪存驱动器上提供还原实用程序。

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。

如果需要将设备还原为出厂默认设置但没有对设备的物理访问权限，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 6-5 页。

要启动还原实用程序，请执行以下操作：

步骤 1　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。

步骤 2　重新启动设备：

- 在管理中心上，键入 `sudo 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.`
- 对于键盘和显示器连接，快速按下任何一个箭头键，防止设备启动当前安装的系统版本。
- 对于串行连接，看到 BIOS 启动选项时，请缓慢地重复按 Tab 键（防止设备启动当前安装的系统版本）。系统将显示 LILO 启动提示符。例如：

```
LILO 22.8 boot:

System-5.4 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。
- 对于串行连接，在系统提示时键入 `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 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。

步骤 6　按 Enter 确认版权声明。

后续操作

- 继续执行使用交互式菜单还原设备，第 6-6 页。

使用无人值守管理启动还原实用程序

访问权限：管理员

如果需要将设备还原为出厂默认设置，但您没有对设备的物理访问权限，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。另请注意，只能在默认 (eth0) 管理接口使用无人值守管理。

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 6-13 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：

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。

步骤 2　以根用户的身份重新启动设备：

- 对于管理中心，请键入 `sudo 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，缓慢地重复按 Tab 键（防止设备启动当前安装的系统版本），直到系统显示 LILO 启动提示符。例如：

```
LILO 22.8 boot:
System-5.4 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，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。

步骤 6　按 Enter 确认版权声明。

后续操作

- 继续执行使用交互式菜单还原设备，第 6-6 页。

使用交互式菜单还原设备

管理中心的还原实用程序使用交互式菜单来指导还原。

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 6-1 页。

菜单显示下表中列出的选项。

表 6-1　还原菜单选项

选项	说明	有关详细信息，请参阅 ...
1 IP 配置 (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 6-7 页
2 选择传输协议 (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 6-8 页
3 选择补丁 / 规则更新 (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 6-9 页
4 下载和安装 ISO (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 6-9 页
5 运行安装 (5 Run the Install)	调用还原流程。	调用还原流程，第 6-10 页
6 保存配置 (6 Save Configuration) 7 加载配置 (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 6-11 页
8 擦除磁盘内容 (8 Wipe Contents of Disk)	安全地清理硬盘驱动器，确保无法再访问其内容。	清理硬盘驱动器，第 A-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**确定 (OK)** 和**取消 (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**确定 (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**确定 (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 6-9 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 6-11 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 6-9 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 配置 (1 IP Configuration)** - 请参阅识别设备的管理接口，第 6-7 页。

步骤 2　**2 选择传输协议 (2 Choose the transport protocol)** - 请参阅指定 ISO 映像位置和传输方法，第 6-8 页。

步骤 3　**3 选择补丁/规则更新 (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 6-9 页。

步骤 4　**4 下载和安装 ISO (4 Download and Mount ISO)** - 请参阅下载 ISO 和更新文件并安装映像，第 6-9 页。

步骤 5　**5 运行安装 (5 Run the Install)** - 请参阅调用还原流程，第 6-10 页。

识别设备的管理接口

访问权限：管理员

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：

步骤 1　请从主菜单中选择 **1 IP 配置 (1 IP Configuration)**。

步骤 2　选择设备的管理接口（通常是 **eth0**）。

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：**静态 (Static)** 或 **DHCP**：

- 如果选择**静态 (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。

后续操作

- 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

访问权限：管理员

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 6-2 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 6-2　　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 • ISO 映像目录的路径，相对于您要使用其凭证的用户的主目录 （例如 `mydownloads/ISOs/`） • FTP 服务器的授权用户名和密码
SCP	• SCP 服务器的 IP 地址 • SCP 服务器的授权用户名 • ISO 映像目录的完整路径 • 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。您必须接受才能继续。

请注意，恢复实用程序将在 ISO 映像目录中查找更新文件。

要指定恢复文件的位置和传输方法，请执行以下操作：

步骤 1　在主菜单中，选择 **2 选择传输协议 (2 Choose the transport protocol) - 请参阅**。

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，详见表 6-2，第 6-8 页。

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。

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 6-9 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

访问权限：管理员

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。注意只有管理中心要求规则更新。

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 6-2 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《*Firepower 管理中心配置指南*》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：

步骤 1　请从主菜单中选择 **3 选择补丁/规则更新 (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 6-8 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。

后续操作

- 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

访问权限：管理员

最后下载必要的文件并安装 ISO 映像，再调用还原流程。

准备工作

- 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 6-11 页。

要下载和安装 ISO 映像，请执行以下操作：

步骤 1　在主菜单中，选择 **4 下载和安装 ISO (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。

后续操作

- 继续执行下一节：调用还原流程。

调用还原流程

访问权限：管理员

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 6-11 页。

要执行双步还原流程的第一步，请执行以下操作：

步骤 1　在主菜单中，选择 **5 运行安装 (5 Run the Install)**。

步骤 2　系统提示（两次）时，请确认要重新启动设备。

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.`
- 对于键盘和显示器连接，快速按下任何一个箭头键，防止设备启动当前安装的系统版本。
- 对于串行或 SOL/LOM 连接，当您看到 BIOS 启动选项时，缓慢地重复按 Tab 键，直到系统显示 LILO 启动提示符为止，例如：

```
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，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。

步骤 6　按 Enter 确认版权声明。

后续操作

- 开始此流程的第二步，首先使用交互式菜单还原设备，第 6-6 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：

步骤 1　在主菜单中，选择 **5 运行安装 (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。删除这些设置还会重置显示器（控制台）和 LOM 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 6-12 页。

注意　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　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　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 6-1 页。

后续操作

- 继续执行后续步骤，第 6-12 页。

保存和加载还原配置

访问权限：管理员

如果需要再次还原管理中心和 Firepower 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 6-7 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 6-8 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 6-9 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。

要保存还原配置，请执行以下操作：

步骤 1　请从还原实用程序主菜单中选择 **6 保存配置 (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。

后续操作

- 要使用刚刚保存的配置还原设备，请继续执行下载 ISO 和更新文件并安装映像，第 6-9 页。

要加载已保存的还原配置，请执行以下操作：

步骤 1　请从主菜单中选择 **7 加载配置 (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。

后续操作

- 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 6-9 页。

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 6-1 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：管理中心，第 4-4 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 Firepower 管理中心，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）和 LOM 设置。完成初始设置流程后：

- 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 6-13 页。

设置无人值守管理

如果需要将管理中心还原为出厂默认设置，但您没有对设备的物理访问权限，可以使用无人值守管理 (LOM) 来执行还原流程。请注意，只能在默认 (eth0) 管理接口使用无人值守管理。

LOM 功能可供您使用局域网串行 (SOL) 连接在管理中心上执行一组有限的操作。借助于 LOM，可使用带外管理连接上的命令行界面执行诸如查看机箱序列号或监控运行状况（如风扇速度和温度）之类的任务。

LOM 命令语法取决于所使用的实用程序，但是，LOM 命令通常包含下表列出的元素。

表 6-3　　LOM 命令语法

IPMItool (Linux/Mac)	ipmiutil (Windows)	说明
`ipmitool`	`ipmiutil`	调用 IPMI 实用程序。
n/a	`-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
```

有关 Firepower 系统支持的 LOM 命令的完整列表，请参阅《*Firepower 管理中心配置指南*》中“配置设备设置”一章。

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 6-13 页
- 安装 IPMI 实用程序，第 6-14 页

启用 LOM 和 LOM 用户

访问权限：管理员

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。也就是说，不能使用管理中心配置 Firepower 设备的 LOM。同样，因为每个设备的用户都是独立管理的，因此，在管理中心上启用或创建 LOM 用户不会将此功能转移到 Firepower 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 密码不得与该用户的系统密码相同。
- 管理中心最多可以有 13 个 LOM 用户。

提示 有关以下任务的详细说明，请参阅 *《Firepower 管理中心配置指南》* 中“配置设备设置”一章。

要启用 LOM，请执行以下操作：

步骤 1 依次选择**系统 (System) > 本地 (Local) > 配置 (Configuration)**，然后点击**控制台配置 (Console Configuration)**。

步骤 2 使用**物理串行端口 (Physical Serial Port)** 启用远程访问。

步骤 3 指定 LOM IP 地址、子网掩码和默认网关（或使用 DHCP 自动分配这些值）。

注 LOM IP 地址必须与设备的管理接口 IP 地址不同。

要为 Firepower 系统用户启用 LOM 功能，请执行以下操作：

步骤 1 依次选择**系统 (System) > 用户管理 (User Management)**，然后编辑现有用户来添加 LOM 权限，或创建要用于设备的 LOM 访问的新用户。

步骤 2 在“用户配置”(User Configuration) 页面，启用**管理员 (Administrator)** 角色（如尚未启用）。

步骤 3 启用**允许无人值守管理访问 (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，请确保已安装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/
```

清理硬盘驱动器

可以安全地清理管理中心和 Firepower 设备上的硬盘驱动器，确保其内容无法再访问。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

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、字符补码然后加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 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 6-6 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：

访问权限：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 6-4 页
- 使用无人值守管理启动还原实用程序，第 6-5 页

步骤 2 在主菜单上选择 **8 擦除磁盘内容 (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。

Firepower 管理中心的内存升级说明

本节介绍如何更换位于思科 Firepower 管理中心内部的内存模块。您需要卸下设备顶盖，才能更换这些组件。本文档具体包含以下部分：

内存升级概述

对于某些管理中心型号（之前称为 FireSIGHT 管理中心或防御中心），Firepower 的版本 6.0 比之前的版本需要更多的内存。具体来说，MC750 需要两个 4GB 双重内嵌式内存模块 (DIMM)。同样，6GB 的 MC1500 也需要额外内存。

由于内存增加是由思科产品要求所致，因而思科为使用这些型号的客户提供内存升级套件。对于有权利在合格的 MC750 或 MC1500 管理中心型号上运行版本 6.0 的客户，可免费订购这些套件。

有关订购内存套件的详细信息，请参阅 http://www.cisco.com/c/en/us/support/docs/field-notices/640/fn64077.html。

在 ESD 环境中工作

静电放电 (ESD) 可损坏设备和电路。电子组件处理不当可能发生 ESD 损害，并可能导致全面或间歇性故障。卸下和更换组件时，务必遵循 ESD 预防程序。确保机箱电气接地。佩戴防静电腕带，确保腕带与皮肤良好接触。将接地夹连接到机箱架未上漆的表面，以使不需要的 ESD 电压安全接地。为防范 ESD 损害和电击，腕带和电源线必须保持正常工作。如果没有腕带，请通过触摸机箱的金属部分使自己接地。

注意 为设备安全起见，请定期检查防静电腕带的电阻值。测量值应介于 1 至 10 兆欧 (Mohm) 之间。

安全警告

本节包含有关设备安装和使用的重要安全警告。

警告　**在操作具有“打开/关闭”开关的系统前，关闭电源并拔下电源线。声明 1**

警告　**仅允许经过培训的合格人员安装、更换或维修本设备。声明 1030**

警告　**本设备必须接地。切勿使接地导体失效，或者在没有正确安装接地导体的情况下操作该设备。如果您不能确定是否已正确接地，请联系合适的电路检测方面的权威人士或电工。声明 1024**

警告　**请勿在发生雷电天气期间使用系统或者连接或断开电缆。声明 1001**

警告　**连接系统到电源之前请阅读安装说明。声明 1004**

警告　**本产品的最终处理应根据所有国家法律法规进行。声明 1040**

拆卸机箱盖

Firepower 管理中心具有可从机箱后侧滑出的顶盖。以下部分所述的机箱型号之间略有差异。

- 从 Firepower 管理中心 750 拆下顶盖，第 B-2 页
- 从 Firepower 管理中心1500 和 3500 拆下顶盖，第 B-4 页

从 Firepower 管理中心 750 拆下顶盖

从 Firepower 管理中心 750 拆下顶盖的过程根据设备的版本（版本 1 或版本 2）而有所不同。有关 MC750 版本 1 机箱的图示，请参见图 B-1。有关 MC750 版本 2 机箱的图示，请参见图 B-2。

要拆下 Firepower MC 750 的顶盖：

注　可能需要将 MC750（版本 1 或版本 2）置于防滑表面或在其后面放置一个阻挡物，以防止设备在您的工作表面滑动。

步骤 1　遵守在 ESD 环境中工作，第 B-1 页中介绍的 ESD 预防措施和安全警告，第 B-2 页中介绍的安全措施。

步骤 2　从机箱的正面拆下安全螺钉：

- 版本 1 有两 (2) 个螺钉（见图 B-1 中的“1”）。
- 版本 2 有三 (3) 个螺钉（见图 B-2 中的“1”）。

步骤 3　从机箱后部拆下安全螺钉。见图 B-1 和图 B-2 中的“2”。

步骤 4　按住机箱盖上的蓝色抓握点，向机箱后部滑动盖子：

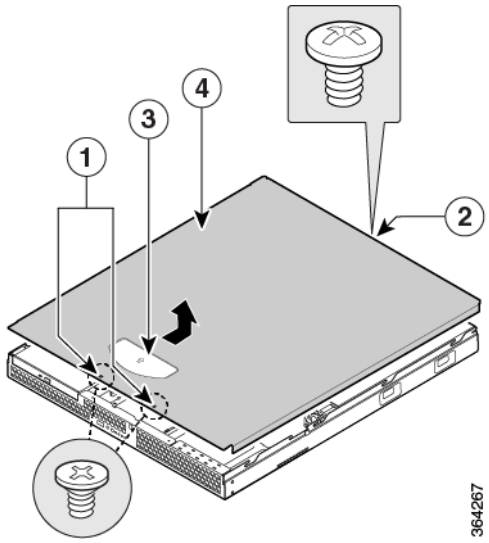
- 版本 1 有一 (1) 个抓握点（见图 B-1 中的“3”）。
- 版本 2 有两 (2) 个抓握点（见图 B-2 中的“3”）。

步骤 5　将盖子抬起并放在一边。

后续操作：

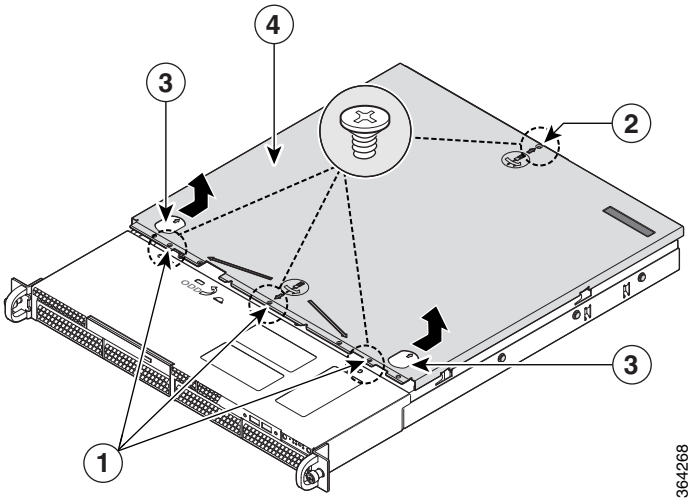
- 按“从 Firepower 管理中心 750 拆除处理器导风管”一节，第 B-5 页中的说明，拆除处理器导风管。

图 B-1　　从 MC750 版本 1 拆下顶盖



1	前安全螺钉	**3**	橡胶抓握点
2	后安全螺钉	**4**	顶盖

图 B-2　　从 MC750 版本 2 拆下顶盖



1	前安全螺钉	3	橡胶抓握点
2	后安全螺钉	4	顶盖

从 Firepower 管理中心1500 和 3500 拆下顶盖

MC1500 和 MC3500 管理中心在外形方面有一些相同之处。以下过程对这两款设备都适用。

要从 Firepower MC1500 或 MC3500 拆下顶盖：

注　可能需要将 MC1500 或 MC3500 置于防滑表面或在其后面放置一个阻挡物，以防止设备在您的工作表面滑动。

步骤 1　遵守在 ESD 环境中工作，第 B-1 页中介绍的 ESD 预防措施和<Blue>安全警告（第 2 页）中介绍的安全措施。

步骤 2　若安装有安全螺钉，请拆下（见图 B-3 中的“1”）。

步骤 3　如果设备上的保修标签是完整的，将其割开。

步骤 4　按住机箱顶部的蓝色按钮（见图 B-3 中的“3”），同时将顶盖滑回，直到滑不动时停下（见图 B-3 中的“4”）。

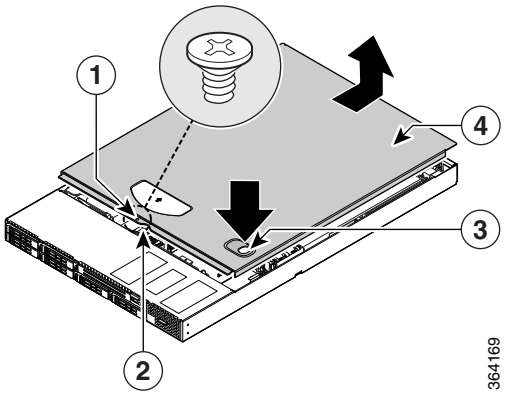
- 在 MC1500 上，此按钮位于左侧。
- 在 MC3500 上，此按钮位于右侧，如图 B-3 所示。

步骤 5　将手指插入槽口中（见图 B-3 中的“2”），将顶盖向上提起以拆下来。

后续操作：

- 按“从 Firepower 管理中心 1500 和 3500 拆除处理器导风管”一节，第 B-6 页中的说明，拆除处理器导风管。

图 B-3　　从 MC1500 或 MC3500 上拆下顶盖



1	安全螺钉	3	顶盖
2	按钮	4	槽口

拆除处理器导风管

需要保证处理器导风管安装到位，Firepower 管理中心才能正常运行。导风管是保证机箱内适当空气流动的必须组件。需要拆除导风管，才能完全接触机箱上的 DIMM 插槽。以下部分所述的机箱型号之间存在一些差异：

- 从 Firepower 管理中心 750 拆除处理器导风管，第 B-5 页
- 从 Firepower 管理中心 1500 和 3500 拆除处理器导风管，第 B-6 页

从 Firepower 管理中心 750 拆除处理器导风管

设备版本不同（版本 1 或版本 2），从 Firepower MC750 拆除处理器导风管的程序也不同。有关 MC750 版本 1 机箱的图示，请参见图 B-4。有关 MC750 版本 2 机箱的图示，请参见图 B-5。

从 Firepower MC750 拆除处理器导风管：

步骤 1　遵守在 ESD 环境中工作，第 B-1 页中介绍的 ESD 预防措施和安全警告，第 B-2 页中介绍的安全措施。

步骤 2　从系统冷却风扇后部提起处理器导风管：

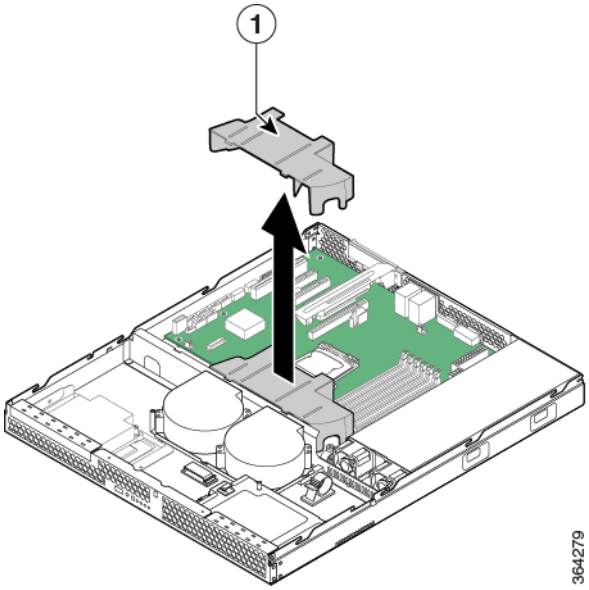
- 版本 1 机箱见图 B-4 中的“1”。
- 版本 2 机箱见图 B-5 中的“1”。

步骤 3　将导风管放在一旁。

后续操作：

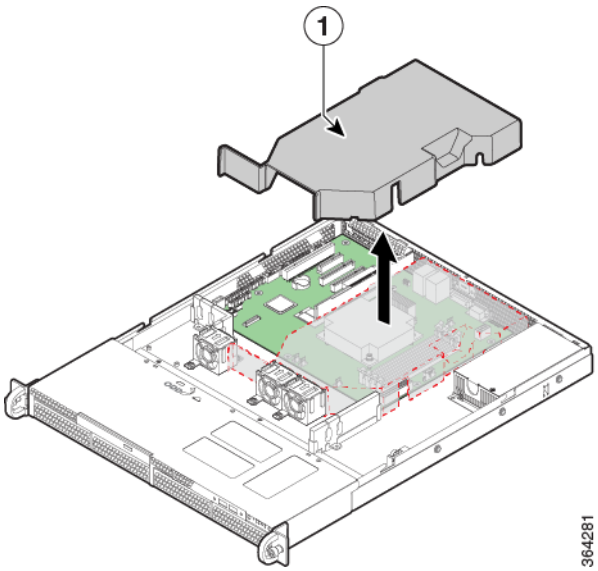
- 按“更换 DIMM”一节，第 B-8 页中所述，拆除 Firepower MC750 DIMM。

图 B-4 从 MC750 版本 1 拆除处理器导风管



1	处理器导风管	-	-

图 B-5 从 MC750 版本 2 拆除处理器导风管



1	处理器导风管	-	-

从 Firepower 管理中心 1500 和 3500 拆除处理器导风管

Firepower MC1500 和 MC3500 在外形方面有一些相同之处。以下过程对这两款设备都适用。

注 从 MC1500 和 MC3500 拆除处理器导风管之前，必须先拆下相邻的 PCI 提升板组件。

要从 Firepower MC1500 或 MC3500 拆除处理器导风管：

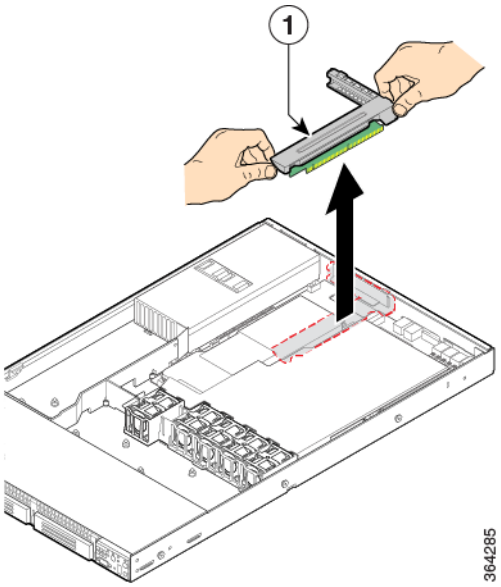
步骤 1 遵守在 ESD 环境中工作，第 B-1 页中介绍的 ESD 预防措施和安全警告，第 B-2 页中介绍的安全措施。

步骤 2 断开任何附加卡上所带的任何电缆。

步骤 3 用拇指和食指抓住两个提升板的扣夹，拉起以释放提升板组件。

步骤 4 直接将提升板组件抬起（见图 B-6 中的“1”）。

图 B-6 从 MC1500 或 MC3500 拆除 PCI 提升板组件

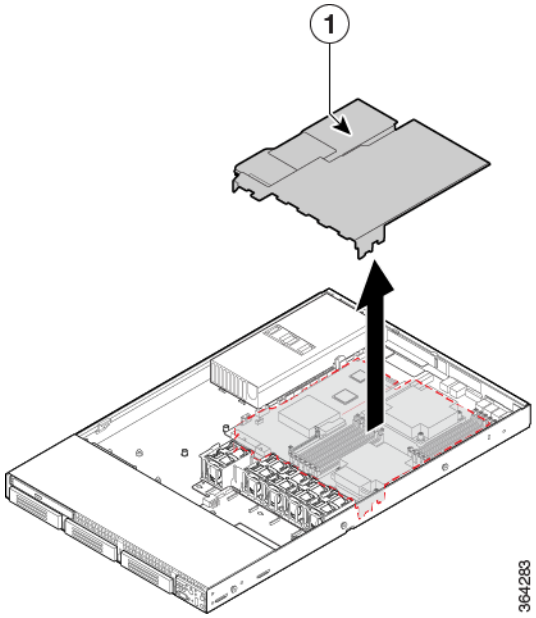


1	PCI 提升板组件	-	-

步骤 5 将提升板组件倒置，以避免对提升板卡连接器造成损坏。

步骤 6 将处理器导风管从两个处理器插座（见图 B-7 中的“1”）上方位置提起。

图 B-7　　从 MC1500 或 MC3500 拆除处理器导风管



1	处理器导风管	-	-

后续操作：

- 按“更换 DIMM”一节，第 B-8 页中的描述，拆除 MC1500 或 MC3500 DIMM。

更换 DIMM

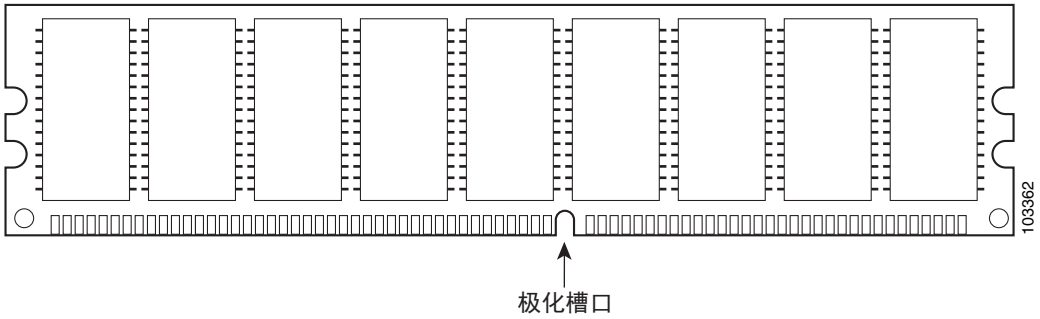
DIMM 位置和方向

在 Firepower MC750（版本 1 或版本 2）、MC1500 和 MC3500 上，DIMM 连接器位于系统主板上并带有丝网印刷标签标识。您还可以借助机箱顶盖内部的“快速参考标签”寻找组件的位置。

提示　请注意，仅蓝色 DIMM 连接器填充了模块。

DIMM 在联合边缘有一个极化槽口，用于防止不正确插入。图 B-8 显示了 DIMM 上的极化槽口。

图 B-8 DIMM 的极化槽口展示



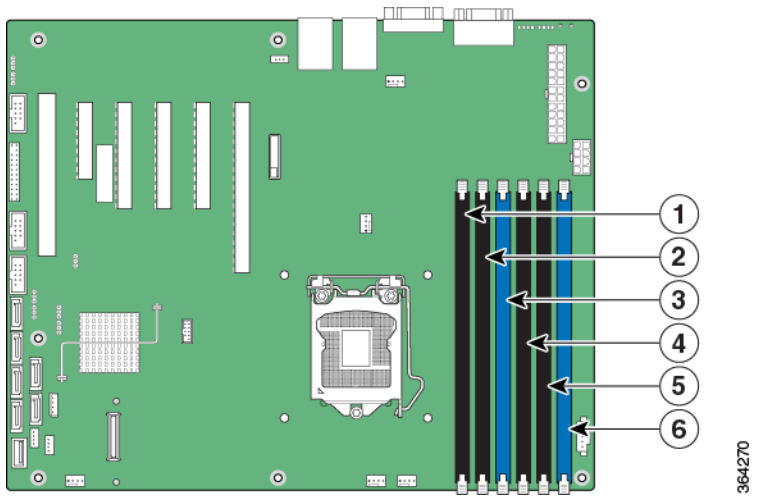
1	极化槽口	-	-

在 Firepower 管理中心中找到 DIMM 的位置

使用下面的图找出满足表 B-1 中确定的内存升级要求的正确 DIMM 连接器。系统主板上的丝网印刷也显示了 DIMM 标签（从主板的中间开始）。

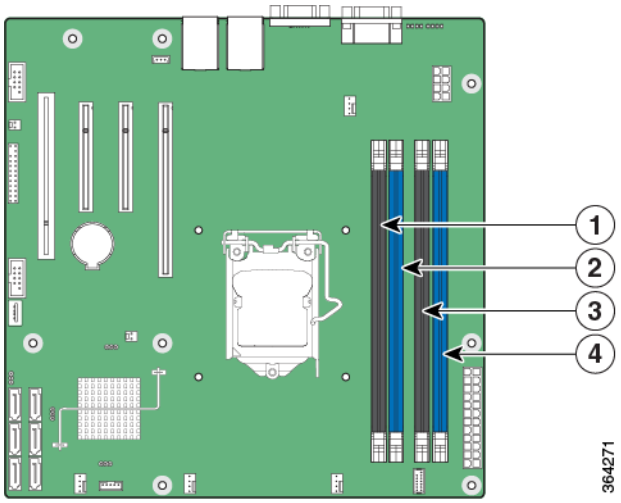
- 参考图 B-9 寻找 MC750（版本 1）上 DIMM 连接器的位置。
- 参考图 B-10 寻找 MC750（版本 2）上 DIMM 连接器的位置。
- 参考图 B-11 寻找 MC1500 和 MC3500 上 DIMM 连接器的位置。

图 B-9 MC750 版本 1 的内存配置和填充顺序



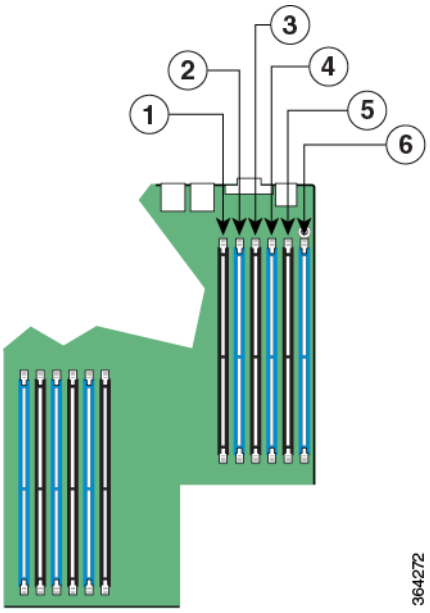
1	DIMM A3	4	DIMM B3
2	DIMM A2	5	DIMM B2
3	DIMM A1	6	DIMM B1

图 B-10 MC750 版本 2 的内存配置和填充顺序



1	DIMM A2	**3**	DIMM B2
2	DIMM A1	**4**	DIMM B1

图 B-11 MC1500 和 MC3500 的内存配置和填充顺序



1	DIMM A2	**4**	DIMM B1
2	DIMM A1	**5**	DIMM C2
3	DIMM B2	**6**	DIMM C1

从 Firepower 管理中心拆除 DIMM

Firepower MC750（版本 1 和版本 2）管理中心的系统主板上安装了 4GB 的系统内存。您必须拆除安装的所有 DIMM，更换为升级套件中的模块，以完成 8GB RAM 的系统升级。

Firepower MC1500 和 MC3500 管理中心的系统主板上安装了 12GB 的系统内存。您必须拆除安装的所有 DIMM，更换为升级套件中的模块，以完成 48GB RAM 的系统升级。

注意　当您拆除或安装 DIMM 时，请始终佩戴防静电腕带，并确保它与您的皮肤良好接触。将腕带的设备末端连接到机箱的金属部件。

注意　仅从边缘部分处理 DIMM。DIMM 是静电敏感组件，处理不当会导致损坏。

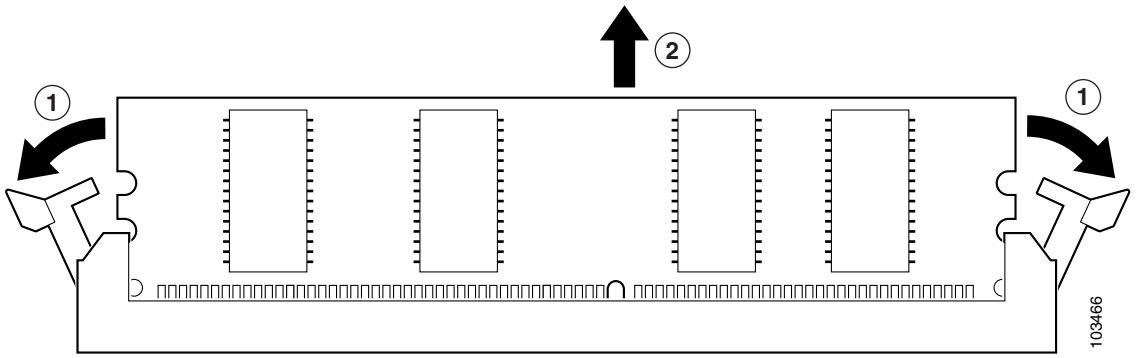
从系统主板上拆除 DIMM：

步骤 1　遵守在 ESD 环境中工作，第 B-1 页中介绍的 ESD 预防措施和安全警告，第 B-2 页中介绍的安全措施。

步骤 2　找到系统主板上的 DIMM。根据您的 FireSIGHT 管理中心型号，参考图 B-9、图 B-10 或图 B-11找到 DIMM 连接器的位置。

步骤 3　拉下 DIMM 两端的扣夹；这会将 DIMM 稍稍抬起。然后将 DIMM 从连接器中提出。请参阅图 B-12。

图 B-12　　拆除 DIMM



1	打开扣夹	2	将 DIMM 提出

后续操作：

- 将拆除的 DIMM 放在抗静电袋中，以防范 ESD 损害。遵守关于处理这些组件的适用联邦、州和地方法规。
- 将您的内存升级套件中的新 DIMM 安装在 FireSIGHT 管理中心中，如“将 DIMM 安装在 Firepower 管理中心中”一节，第 B-12 页中所描述。

将 DIMM 安装在 Firepower 管理中心中

要将 DIMM 安装在 Firepower MC750（版本 1 和 2）、MC1500 和 MC3500 中：

步骤 1　在系统主板中找到 DIMM 的位置：

- 参考图 B-9 寻找 MC750（版本 1）上 DIMM 连接器的位置。
- 参考图 B-10 寻找 MC750（版本 2）上 DIMM 连接器的位置。
- 参考图 B-11 寻找 MC1500 和 MC3500 上 DIMM 连接器的位置。
- 请参阅表 B-1，了解每个管理中心型号的内存升级配置。

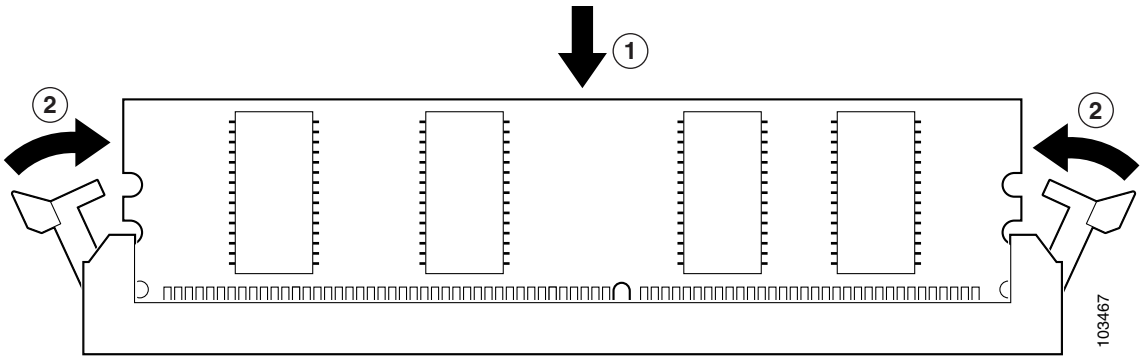
步骤 2　确保 DIMM 连接器上的两个扣夹都处于打开状态。

步骤 3　调整 DIMM 的方向，使极化槽口与连接器的极化键对齐。请参阅图 B-8。

步骤 4　小心地将 DIMM 对齐插入连接器。

步骤 5　小心地用力地将 DIMM 按入连接器，直到扣夹扣在 DIMM 上。确保旋转 DIMM 上的两个扣夹，使它们处于关闭状态。请参阅图 B-13。

图 B-13　　安装 DIMM



1	插入 DIMM	2	关闭扣夹

后续操作：

- 按“安装处理器导风管”一节，第 B-12 页中的说明，更换 Firepower 管理中心中的处理器导风管。

安装处理器导风管

必须保证处理器导风管安装到位，Firepower 管理中心才能正常运行。导风管是保证机箱内适当空气流动的必须组件。执行任何维护程序之后，都有必要重新安装导风管。以下部分所述的机箱型号之间存在一些差异：

- 在 Firepower 管理中心 750 上安装处理器导风管，第 B-13 页
- 在 Firepower 管理中心 1500 和 3500 上安装处理器导风管，第 B-14 页

在 Firepower 管理中心 750 上安装处理器导风管

设备版本不同（版本 1 或版本 2），在 Firepower MC750 上安装处理器导风管的程序也不同。有关 Firepower MC750 版本 1 机箱的图示，请参见图 B-14。有关 Firepower MC750 版本 2 机箱的图示，请参见图 B-15。

要在 Firepower MC750 上安装导风管：

步骤 1 遵守在 ESD 环境中工作，第 B-1 页中介绍的 ESD 预防措施和安全警告，第 B-2 页中介绍的安全措施。

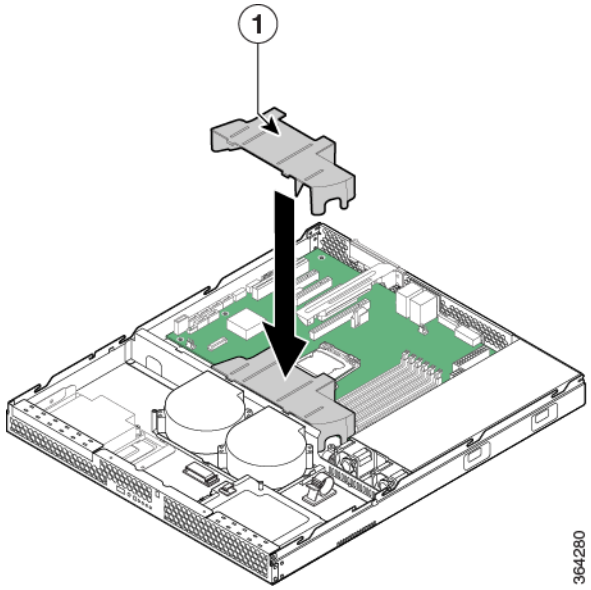
步骤 2 将处理器导风管放低入位。

- 对于版本 1 机箱，将处理器导风管前的两个挂钩插入两个系统冷却风扇后面支架上的相应插槽中（见图 B-14 中的“1”）。
- 对于版本 2 机箱，将处理器导风管前的两个挂钩插入两个系统冷却风扇后面支架上的相应插槽中。注意不要挤压或解开靠近或位于导风管下方的电缆（见图 B-15 中的“1”）。

后续操作：

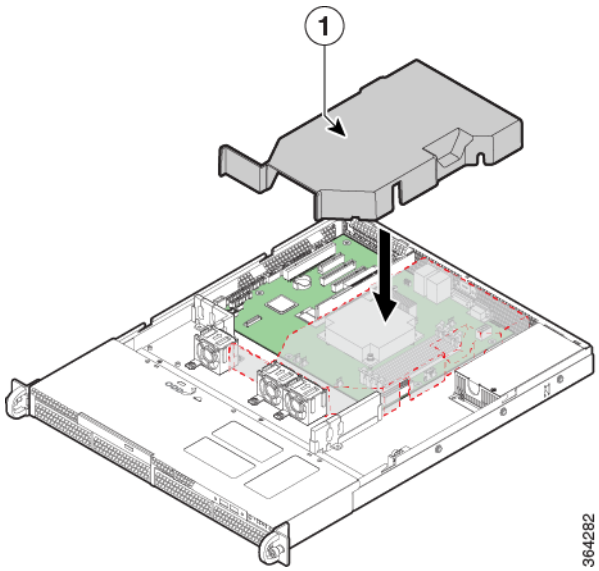
- 按照“在 Firepower 管理中心 750 上安装顶盖”一节，第 B-16 页中所述安装机箱顶盖。

图 B-14 在 MC750 版本 1 上安装处理器导风管



1	处理器导风管	-	-

图 B-15 在 MC750 版本 2 上安装处理器导风管



1	处理器导风管	-	-

在 Firepower 管理中心 1500 和 3500 上安装处理器导风管

Firepower MC1500 和 MC3500 管理中心在外形方面有一些相同之处。以下过程对这两款设备都适用。

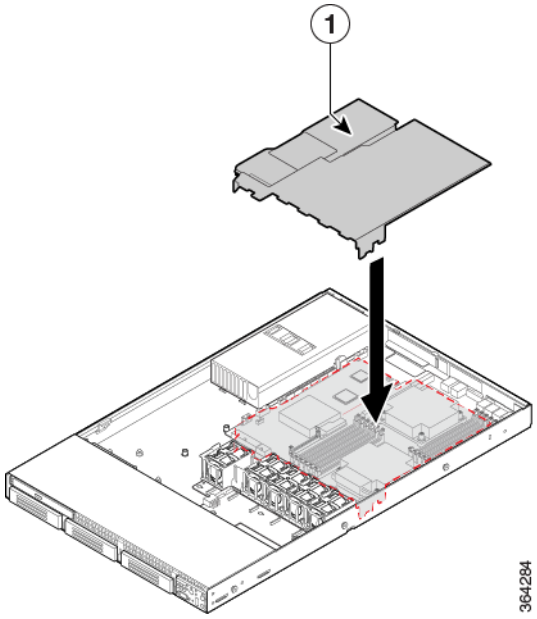
注 在 Firepower MC1500 和 MC3500 上安装处理器导风管之后，必须安装相邻的 PCI 提升板组件。

要在 Firepower MC1500 或 MC3500 上安装处理器导风管：

步骤 1 遵守在 ESD 环境中工作，第 B-1 页中介绍的 ESD 预防措施和安全警告，第 B-2 页中介绍的安全措施。

步骤 2 将处理器导风管放置在处理器插槽上方。导风管的前边缘应与风扇模块的槽口对齐。注意不要挤压或解开靠近或位于导风管下方的电缆。见图 B-16 中的“1”。

图 B-16 在 MC1500 或 MC3500 上安装处理器导风管

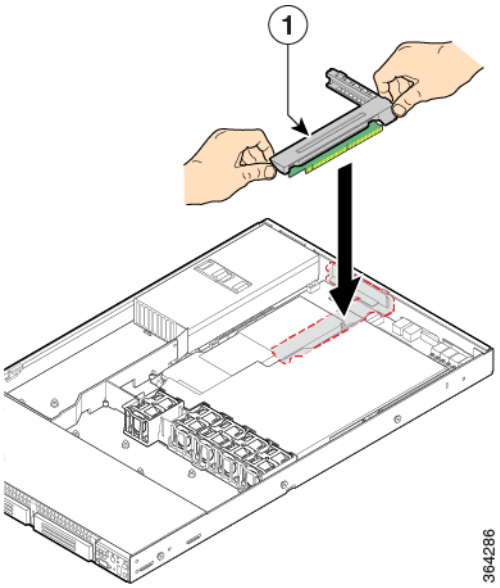


1	处理器导风管	-	-

步骤 3 将 PCI 提升板组件放低入位。将提升板组件中的两个挂钩与机箱背面的匹配插槽对齐（见图 B-17 中的“1”）。

步骤 4 一直按下，直到 PCI 提升板组件后部的两个挂钩挂入机箱的后面板插槽。提升板卡将插入系统主板上的匹配插槽。

图 B-17 在 MC1500 或 MC3500 上安装 PCI 提升板组件



1	PCI 提升板组件	-	-

后续操作：

- 重新连接任何附加卡上所带的任何电缆。
- 按照“在 Firepower 管理中心 1500 和 3500 上安装顶盖”一节，第 B-18 页中所述安装机箱顶盖。

安装机箱盖

FireSIGHT 管理中心具有可向机箱后侧滑动的顶盖。以下部分所述的机箱型号之间略有差异。

- 在 Firepower 管理中心 750 上安装顶盖，第 B-16 页
- 在 Firepower 管理中心 1500 和 3500 上安装顶盖，第 B-18 页

在 Firepower 管理中心 750 上安装顶盖

要在 Firepower MC750 上安装顶盖：

注 可能需要将 MC750 置于防滑表面或在其后面放置一个阻挡物，以防止设备在您的工作表面滑动。

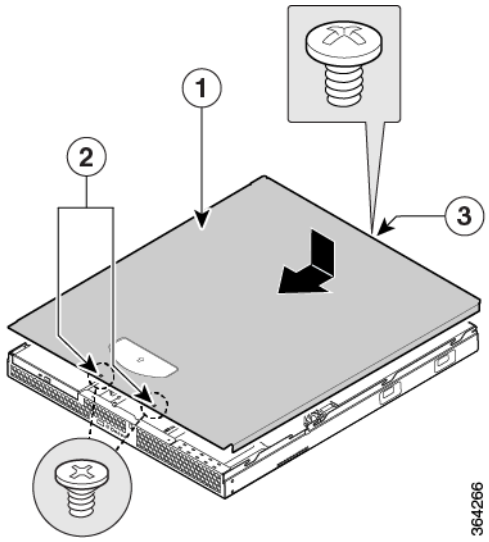
步骤 1 将顶盖放置在机箱上并向前滑动（见图 B-18 和图 B-19 中的“1”）。

步骤 2 在机箱正面安装安全螺钉：

- 版本 1 有两 (2) 个螺钉（见图 B-18 中的“1”）。
- 版本 2 有三 (3) 个螺钉（见图 B-19 中的“1”）。

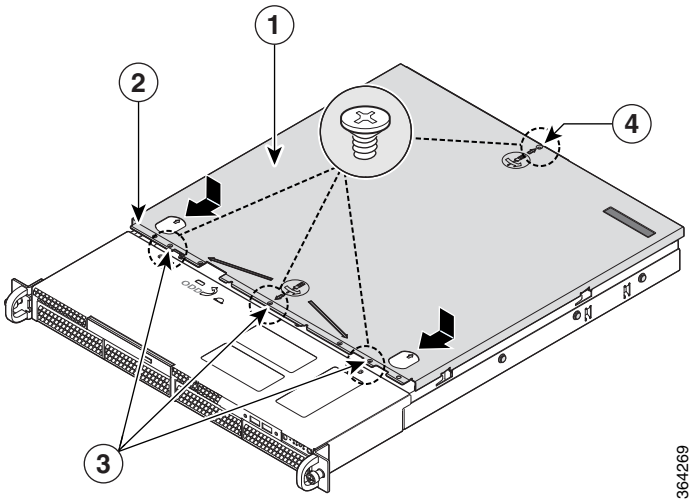
步骤 3 在机箱后部安装安全螺钉。见图 B-18 中的“3”和图 B-19 中的“4”。

图 B-18 在 MC750 版本 1 上安装顶盖



1	顶盖	3	后安全螺钉
2	前安全螺钉	-	-

图 B-19 在 MC750 版本 2 上安装顶盖



1	顶盖	3	前安全螺钉
2	凹形边缘	4	后安全螺钉

在 Firepower 管理中心 1500 和 3500 上安装顶盖

要在 Firepower MC1500 或 MC3500 上安装顶盖：

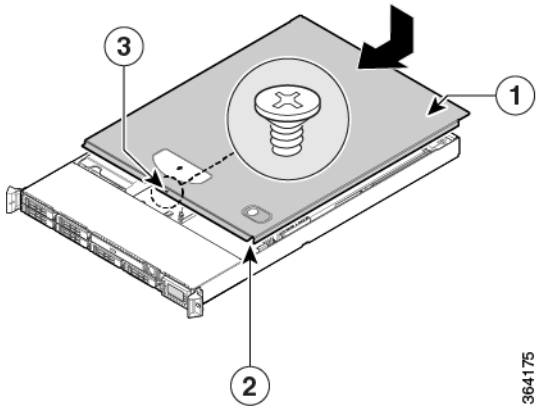
注 可能需要将 MC1500 或 MC3500 置于防滑表面或在其后面放置一个阻挡物，以防止设备在您的工作表面滑动。

步骤 1 如图 B-20 所示将顶盖放置在设备上，使顶盖的侧边缘正好位于机箱侧壁内。

步骤 2 向前滑动顶盖，让顶盖的凹形边缘与机箱正面吻合（见图 B-20 中的“2”）。确定顶盖扣夹扣到位。

步骤 3 将安全螺钉插入顶盖的中心位置（见图 B-20 中的“3”）。

图 B-20 在 MC1500 和 MC3500 上安装顶盖



1	顶盖	**3**	安全螺钉
2	凹形边缘	**-**	-

更换 Firepower 管理中心 3500 上的 RAID 电池备份单元组合

使用以下说明更换 Firepower 管理中心 3500 上的 RAID 电池备份单元 (BBU) 组合。在维护窗口打开期间，您应先关闭设备，再更换 BBU 组合。有关详细信息，请参阅以下各节：

BBU 概述

Firepower 管理中心 3500 包含一个电池备份单元 (BBU)，可在交流电源完全丧失或短暂的电力中断时通过提供备份电源，保护 RAID 控制器上所缓存数据的完整性。思科建议您每年更换一次此 BBU。

思科提供新的 BBU 更换组合。该组合包括具有五年使用寿命的新 BBU 型号 (BBU8)，及新的塑料电池托架。BBU 使用此塑料电池托架固定（参见图 C-1），此托架可安全地锁定在 Firepower MC3500 机箱的底座上。请拆下已安装的 BBU 和托架，更换为新的 BBU 组合。

在 ESD 环境中工作

静电放电 (ESD) 可损坏设备和电路。电子组件处理不当可能发生 ESD 损害，并可能导致全面或间歇性故障。卸下和更换组件时，务必遵循 ESD 预防程序。确保机箱电气接地。佩戴防静电腕带，确保腕带与皮肤良好接触。将接地夹连接到机箱架未上漆的表面，以使不需要的 ESD 电压安全接地。为防范 ESD 损害和电击，腕带和电源线必须保持正常工作。如果没有腕带，请通过触摸机箱的金属部分使自己接地。

注意 为设备安全起见，请定期检查防静电腕带的电阻值。测量值应介于 1 至 10 兆欧 (Mohm) 之间。

安全警告

本节包含有关设备安装和使用的重要安全警告。

警告　**在操作具有“打开/关闭”开关的系统前，关闭电源并拔下电源线。声明 1**

警告　**仅允许经过培训的合格人员安装、更换或维修本设备。声明 1030**

警告　**本设备必须接地。切勿使接地导体失效，或者在没有正确安装接地导体的情况下操作该设备。如果您不能确定是否已正确接地，请联系合适的电路检测方面的权威人士或电工。声明 1024**

警告　**请勿在发生雷电天气期间使用系统或者连接或断开电缆。声明 1001**

警告　**连接系统到电源之前请阅读安装说明。声明 1004**

警告　**本产品的最终处理应根据所有国家法律法规进行。声明 1040**

为更换 BBU 做准备

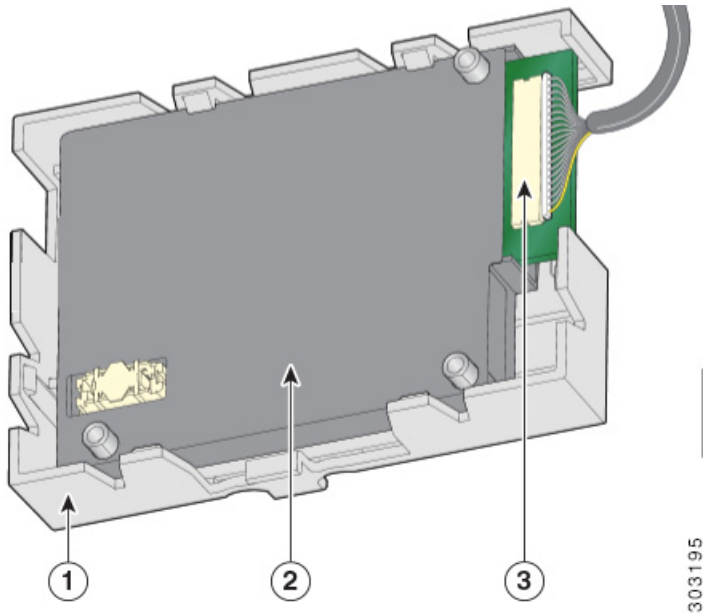
您需提供的工具

您必须准备 2 号十字螺丝刀和剃刀用来更换 BBU。

BBU 组件

下图显示了您在更换 BBU 时需熟悉的 BBU 组合组件。

图 C-1　　BBU 组合组件

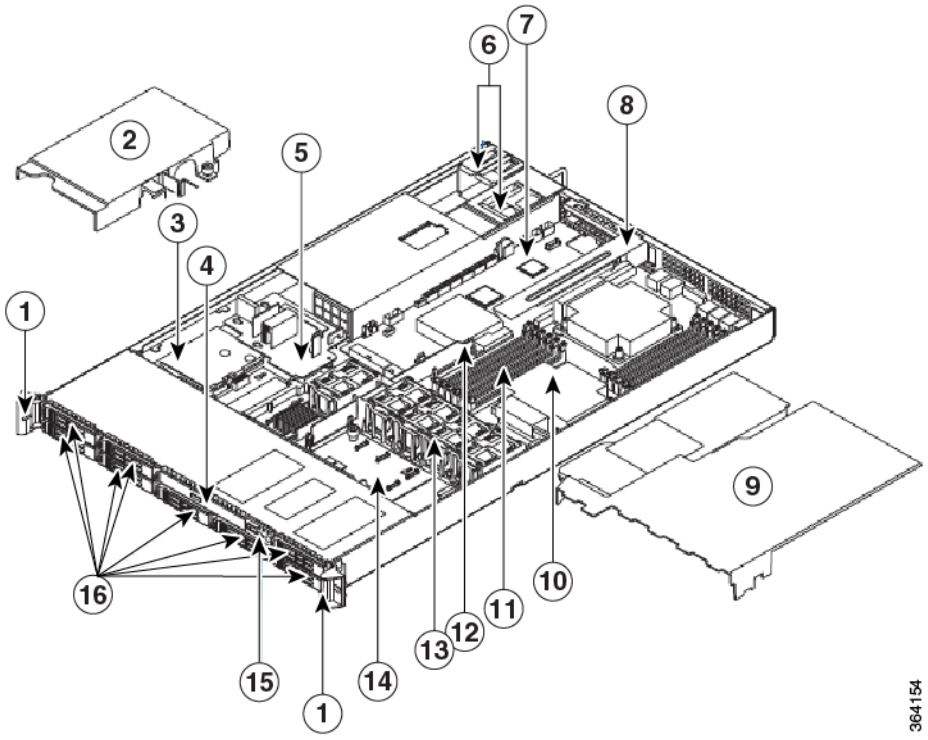


1	BBU 托架	**2**	BBU
3	BBU 接线器和电缆	**-**	-

Firepower 管理中心 3500 组件

本部分将帮助您识别 Firepower MC3500 系统的组件。如果您在靠近系统的位置，也可以使用机箱盖内侧提供的“快速参考标签”来识别组件。

图 C-2　　MC3500 机箱组件



1	机架把手	**9**	处理器导风管
2	电源导风管	**10**	处理器和散热器
3	电池备份单元 (BBU) 组合	**11**	系统内存
4	驱动器槽位	**12**	网桥板
5	配电板	**13**	风扇组件
6	电源模块	**14**	中板
7	服务器主板	**15**	迷你控制面板
8	PCI 提升板组件	**16**	磁盘驱动器槽位

BBU 更换说明

以下部分说明了如何更换 Firepower MC3500 中的 RAID BBU。请按以下顺序的说明操作：

- 拆卸顶盖（第 C-5 页）
- 拆卸电源导风管（第 C-5 页）
- 拆卸旧的 BBU 组合（第 C-6 页）
- 安装新的 BBU 组合（第 C-7 页）
- 更换电源导风管（第 C-8 页）
- 更换顶盖（第 C-9 页）
- 处理旧 BBU（第 C-10 页）

拆卸顶盖

必须保证机箱盖安装到位，才能确保 Firepower MC3500 适当冷却。您需要拆下顶盖，才能在设备内增加或更换组件。

注　可能需要将 MC3500 置于防滑表面或在其后面放置一个阻挡物，以防止设备在您的工作表面滑动。

要拆下 Firepower MC3500 顶盖：

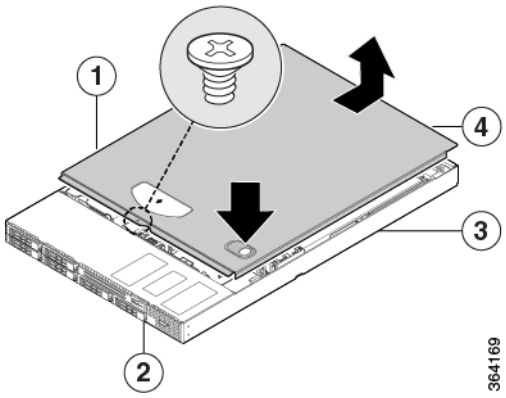
步骤 1　若安装有安全螺钉，请拆下（见图 C-3 中的“1”）。

步骤 2　如果设备上的保修标签是完整的，将其割开。

步骤 3　按住 FireSIGHT 3500 顶部的蓝色按钮（见图 C-3 中的“3”），同时将顶盖滑回，直到滑不动时停下（见图 C-3 中的“4”）。

步骤 4　将手指插入槽口中（见图 C-3 中的“2”），将顶盖向上提起以拆下来。

图 C-3　　拆下 MC3500 顶盖



1	安全螺钉	3	顶盖
2	按钮	4	槽口

拆卸电源导风管

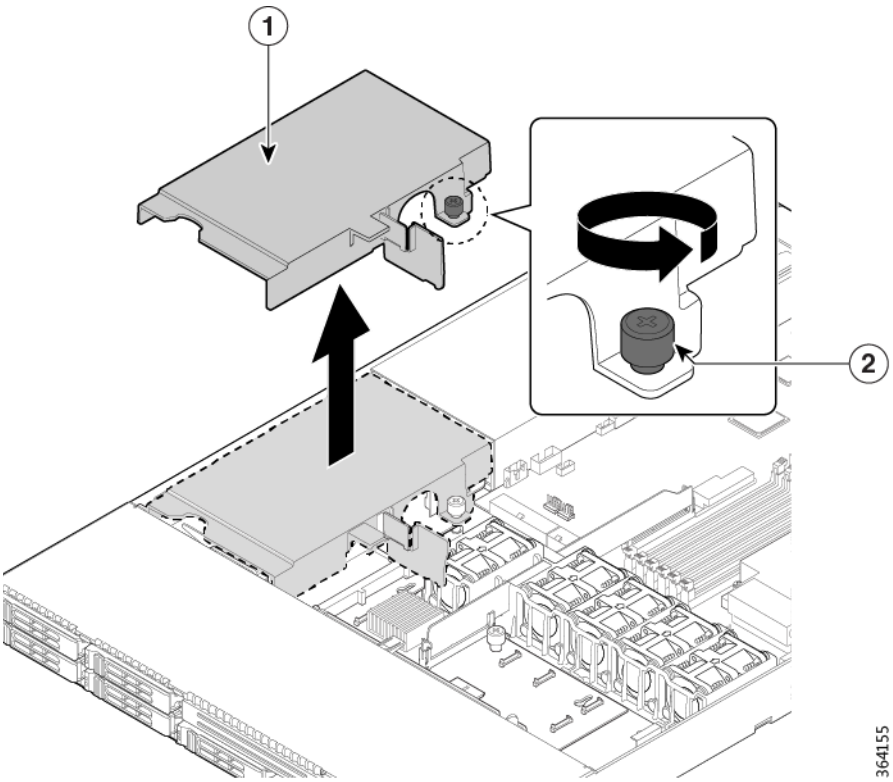
RAID BBU 位于电源导风管下（见图 C-2）。要拆卸导风管，请按以下步骤操作：

步骤 1　找到电源导风管的位置（见图 C-4 中的“1”）。

步骤 2　使用手指或十字螺丝刀旋出指旋螺钉（见图 C-4 中的“2”）。注意保留指旋螺钉。

步骤 3　小心地向上提起导风管并放在一边。

图 C-4　　拆卸电源导风管



1	电源导风管	2	指旋螺钉

拆卸旧的 BBU 组合

RAID BBU 使用塑料电池托架固定（见图 C-1），而托架通过电池座下面的两个卡扣牢固地锁定到机箱的底座。卡扣安全地滑入位于机箱底部的两个槽口。思科建议您按如下所述步骤拆除 BBU 组合。

注　替换 BBU 组合所包含的塑料托架与当前已安装的不同。在安装了替换 BBU 组合后，可以丢弃旧的塑料托架。

要拆卸 BBU：

步骤 1　从 BBU 连接器中均匀用力拉出连接器（而非电缆），然后从 BBU 单元的后部小心地拆卸电缆。在拆卸连接器时请注意电缆的极性。这对于重新连接电缆非常重要。

步骤 2　找到 BBU 组合托架的侧卡扣（见图 C-5 中的“2”）。此卡扣可以将电池托架锁定到位，从而固定 BBU 组合。

步骤 3　将侧卡扣朝着电池方向向内推，在 BBU 组合上向下施力，并将组合朝机箱正面方向（电源反方向）滑动。

步骤 4　从机箱中拆下 BBU 组合。

安装新的 BBU 组合

从机箱上拆下旧的 BBU 组合后，您可以轻松安装已预先组装的替换 BBU 组合。思科建议您按如下所述步骤安装替换 BBU 组合。

要安装替换 BBU 组合：

步骤 1　找到将 BBU 组合固定到机箱的卡扣。它们位于机箱内部底板的左侧，靠近机箱正面，在电源旁（见图 C-6）。

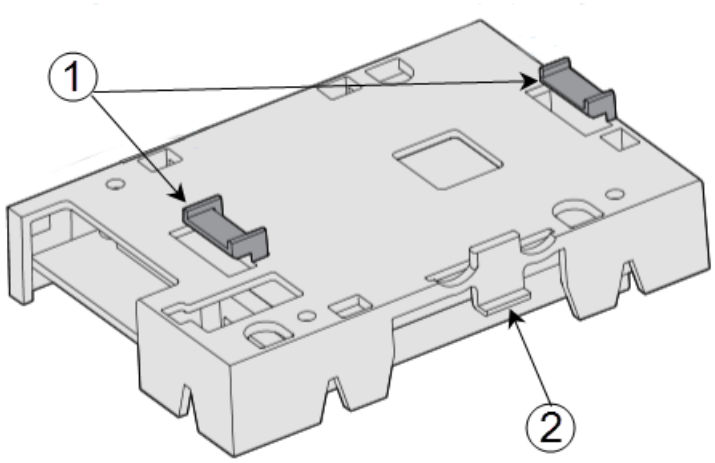
步骤 2　将塑料电池托架（见图 C-5 中的“1”）底部的固定夹与机箱上的卡扣对齐。

步骤 3　将 BBU 组合单元朝电源方向滑动，直到卡扣卡入机箱槽口。

注意　确定滑动固定夹（见图 C-5 中的“2”）完全与机箱吻合，使托架锁定到位。如果未能妥当固定电池托架，BBU 组合可能会在机箱内自由移动。这可能导致故障，例如 BBU 电缆松动，这将影响电池的保护。

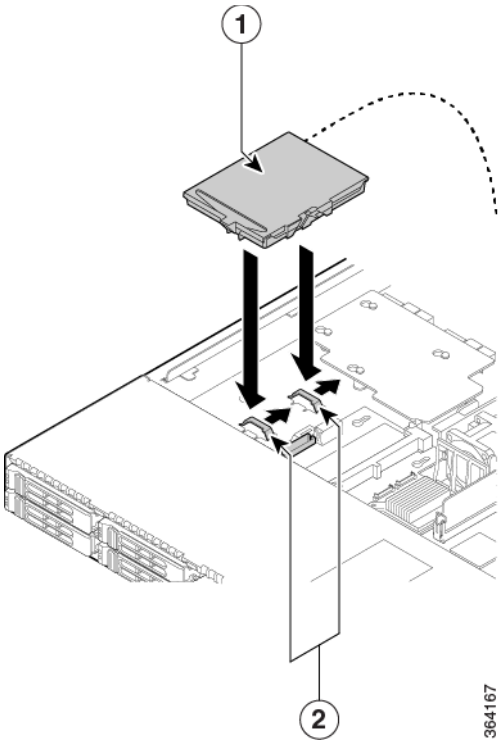
步骤 4　小心地将电缆连接到新的 BBU。确保观察电缆极性，然后将连接器一致插入 BBU 连接器中。

图 C-5　　BBU 电池托架底部



1	托架固定夹	2	侧固定夹

图 C-6　　安装替换 BBU 组合



1	BBU 和托盘组合	2	机箱卡扣

更换电源导风管

在替换 BBU 组合固定到位并连接后，更换电源导风管（见图 C-7）。

要更换导风管：

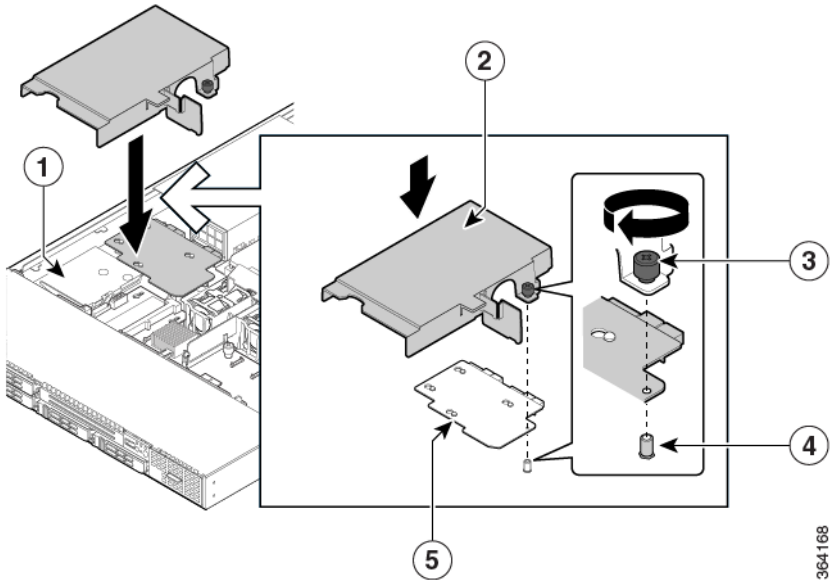
步骤 1　找到电源导风管和您之前拆下的指旋螺钉。

步骤 2　将电源导风管置于上方，与 BBU 组合、配电板和匹配的指旋螺钉孔对齐。请注意指旋螺钉附于配电板下的机箱螺柱上（见图 C-7 中的“4”）。

在固定导风管前，确保电源导风管的任何部分不会挤压电缆。

步骤 3　使用手指或十字螺丝刀拧紧指旋螺钉。

图 C-7　　更换电源导风管



1	已安装的 BBU 组合	4	机箱螺柱
2	电源导风管	5	配电装置
3	指旋螺钉	-	-

更换顶盖

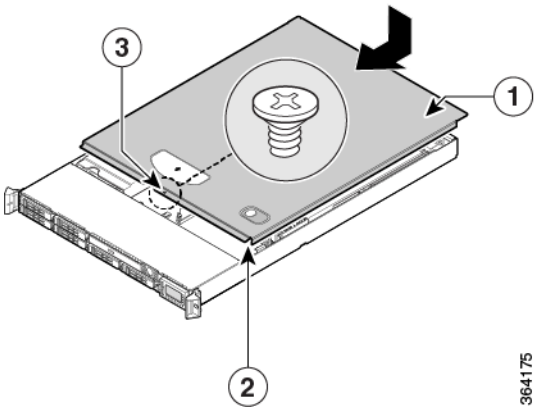
要更换 Firepower MC3500 顶盖：

步骤 1　如图 C-8 所示将顶盖放置在设备上，使顶盖的侧边缘正好位于机箱侧壁内。

步骤 2　向前滑动顶盖，让顶盖的凹形边缘与机箱正面吻合（见图 C-8 中的“2”）。确定顶盖扣夹扣到位。

步骤 3　将安全螺钉插入顶盖的中心位置（见图 C-8 中的“3”）。

图 C-8　　更换 MC3500 顶盖



1	顶盖	**3**	安全螺钉
2	凹形边缘	**-**	-

处理旧 BBU

警告　**不要以任何方式破坏电池组。破坏电池组可能会使有毒化学物质释放出来。**

电池组的材料包含会污染环境的重金属。联邦、州和地方法规禁止在公共垃圾填埋场处理可充电电池。请务必妥当回收旧电池组。思科提醒您必须遵守使用 BBU 时所在的国家/地区或其他司法管辖区的所有适用的电池处理和危险材料处理法律和法规。

监控 BBU

在安装新的 BBU 后，请使用 Intel® RAID BIOS 控制台电池模块配置实用程序，将电池的充电循环计数器重置为零。该实用程序独立于操作系统，可在设备启动时按 **<Ctrl><G>** 访问。

要查看 BBU 信息：

步骤 1　启动设备后，在系统提示时按 **<Ctrl><G>**。

步骤 2　在 Intel® RAID BIOS 控制台的主菜单中，选择**适配器属性 (Adapter Properties)**。

步骤 3　点击**下一步 (Next)** 查看第二个**适配器属性 (Adapter Properties)** 屏幕。

步骤 4　在“适配器属性”(Adapter Properties) 屏幕左上角的“电池备用”(Battery Backup) 字段中，点击**当前 (Present)**。

步骤 5　出现“电池模块”(Battery Module) 屏幕， 所示。 该屏幕包含以下信息：

— 电池信息

— 设计信息

— 容量信息

— 属性和设置

步骤 6　在**电池类型 (Battery Type)** 字段中验证 BBU8 是否已安装。

步骤 7　将**Bbu 模式 (Bbu Mode)** 选项设置为 **1**。

这会将 BBU 充电模式设置为断电情况下提供 12 个小时的数据保留及 5 年的 BBU 使用寿命，前提是假设 BBU 的使用温度保持在 45 摄氏度以下。

步骤 8　点击**继续 (Go)** 保存设置。

步骤 9　点击**主页 (Home)** 返回到主 RAID BIOS 屏幕，然后退出。

预配置 Firepower 管理中心

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）预配置管理中心，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
- 关闭设备并装运至目标位置
- 在目标位置部署设备

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。

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

预配置可选信息

可更改某些默认配置，如：

- 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
- 设置无人值守管理 (LOM) IP 地址，以启用 LOM

注 在某些重新启动场景，通过管理接口连接到网络的 3D7050 的基板管理控制器 (BMC) 会丢失 DHCP 服务器分配给它的 IP 地址。因此，思科建议您使用静态 IP 地址配置 3D7050 的 BMC。或者，您可以断开网线然后重新连接，或断开再恢复设备电源，以强制进行重新连接。

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。
- 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。
- 如将设备上的时间设置为手动（而不是使用 NTP），请使用目标部署的时区；请参阅时间设置，第 4-5 页。

安装系统

采用安装 Firepower 管理中心，第 3-1 页和设置 Firepower 管理中心，第 4-1 页所述的安装步骤。预配置系统时，请记住以下事项：

- 在初始设置期间，为受管设备添加许可证。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管理中心；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 4-6 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：

- 要安全关闭设备，请参阅关闭设备，第 D-3 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 D-3 页。

从管理中心删除许可证

访问权限：管理员

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，由于思科根据每个管理中心具有唯一性的许可密钥生成许可证，因此，在从一个管理中心删除一个许可证后，不可在另一个管理中心上再使用该许可证。有关详细信息，请参阅*《Firepower 管理中心配置指南》*中的“参见为 Firepower 系统获得许可证”。

要删除许可证，请执行以下操作：

步骤 1 依次选择**系统 (Systems) > 许可证 (Licenses)**。

步骤 2 在要删除的许可证旁边，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

访问权限：管理员

断开电源前采用以下步骤安全地关闭设备。

要关闭管理中心，请执行以下操作：

步骤 1 在管理中心上，将以下命令输入命令行：

```
sudo shutdown -h now
```

管理中心已安全关闭。

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。
- 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：管理中心，第 4-4 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 1-13 页。

如果仍有问题，可与 IT 部门联系。