思科 Firepower 发行说明，版本 6.4.0.1、 6.4.0.2、6.4.0.3、 6.4.0.4、6.4.0.5 和 6.4.0.6

首次发布日期: 2019 年 5 月 15 日

上次修改日期: 2019 年 10 月 16 日

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

目录

第 1 章 欢迎使用版本 6.4.0.x 1

关于发行说明 1

发布日期 1

第 2 章 兼容性 3

Firepower 管理中心s 3

Firepower 设备 4

管理器-设备的兼容性 6

网络浏览器兼容性 7

屏幕分辨率要求 8

第 3 章 特性和功能 11

Firepower 中的新功能 版本 6.4.0.x 11

弃用的功能 12

FMC 操作方法演练 12

第 4 章 升级到版本 6.4.0.x 15

指引和警告： 版本 6.4.0.x 15

升级失败：容器实例上的磁盘空间不足 16

Firepower 1010 设备上的 Etherchannel 可以将出口流量引入黑洞 16

Firepower 1000 系列不支持版本 6.4.0.1 和 6.4.0.2 16

一般指引和警告 16

要升级的最低版本 18

时间测试和磁盘空间要求 18

关于时间测试 19
关于磁盘空间要求 19
版本 6.4.0.6 的时间和磁盘空间 20
版本 6.4.0.5 的时间和磁盘空间 20
版本 6.4.0.4 的时间和磁盘空间 21
版本 6.4.0.3 的时间和磁盘空间 22
版本 6.4.0.2 的时间和磁盘空间 22
版本 6.4.0.1 的时间和磁盘空间 23
流量、检查和设备行为 23
FTD升级行为： Firepower 4100/9300 机箱 24
FTD升级行为：其他设备 27
Firepower 7000/8000 系列升级行为 28
ASA FirePOWER升级行为 30
NGIPSv升级行为 30
升级说明 31
升级程序包 31

第 5 章 卸载版本 6.4.0.x 修补程序 33
卸载的指引和限制 33
高可用性/可扩展性部署的卸载顺序 35
卸载说明 37
从独立的 FMC 卸载 37
从高可用性 FMC 卸载 38
从任意设备卸载（FMC 管理） 39
从 ASA FirePOWER 卸载（ASDM 管理） 41
卸载软件包 42

第 6 章 全新安装 版本 6.4.0 45
决定全新安装 45
全新安装的指引和限制 46
取消注册智能许可证 48

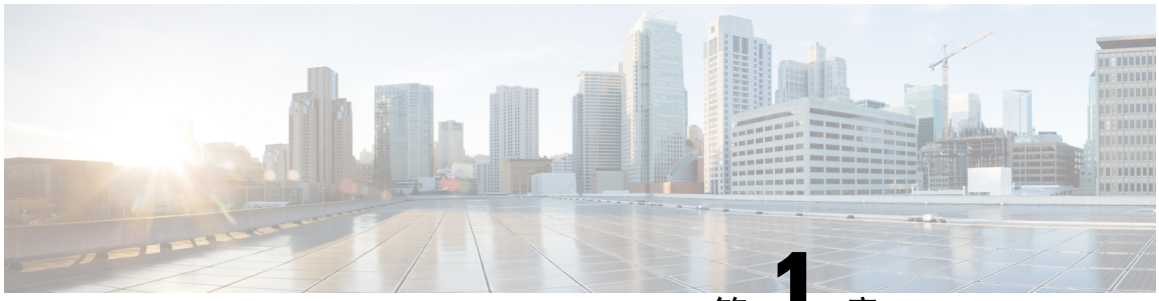
注销 Firepower 管理中心 49
注销 FTD 设备，使用 FDM 49
安装说明 50

第 7 章 文档 53
更新的文档 版本 6.4.0.x 53
新增和更新的文档 53
文档目录 55

第 8 章 已解决的问题 57
搜索已解决的问题 57
新内部版本中已解决的问题 58
版本 6.4.0.6 已解决的问题 58
版本 6.4.0.5 已解决的问题 60
版本 6.4.0.4 已解决的问题 61
版本 6.4.0.3 已解决的问题 65
版本 6.4.0.2 已解决的问题 66
版本 6.4.0.1 已解决的问题 69

第 9 章 已知问题 71
搜索已知问题 71

第 10 章 获取帮助 73
网上资源 73
联系思科 73



第 1 章

欢迎使用版本 6.4.0.x

感谢选择 Firepower。

- 关于发行说明，第 1 页
- 发布日期，第 1 页

关于发行说明

发行说明提供了关于版本 6.4.0.x的关键和版本特定信息，包括升级警告和行为更改。即使您熟悉 Firepower 版本并且具有 Firepower 部署升级经验，也请阅读此文档。

升级或全新安装（重新映像）Firepower 部署可能是一个复杂的过程。在这里，发行说明并未提供具体的说明，而是提供了指向对应资源的链接。有关升级和安装说明的链接，请参阅：

- 升级说明，第 31 页
- 安装说明，第 50 页

发布日期

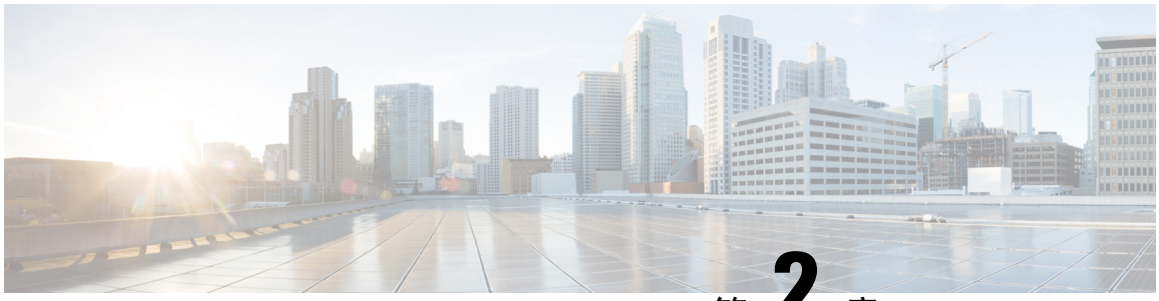
有关随版本 6.4.0.x提供的所有平台的列表，请参阅兼容性，第 3 页。

有时，思科会发布更新的内部版本。在大多数情况下，上只能找到每个平台最新的内部版本。 思科支持和下载站点我们 强烈建议您使用最新版本。如果您下载的是较旧的版本，请不要使用。有关详细信息，请参阅新内部版本中已解决的问题，第 58 页。

表 *1:* 版本 *6.4.0.x* 发行日期

版本	内部版本号	日期	平台
6.4.0.6	28	2019-10-16	全部
6.4.0.5	23	2019-09-18	全部
6.4.0.4	34	2019-08-21	全部

版本	内部版本号	日期	平台
6.4.0.3	29	2019-07-17	全部
6.4.0.2	35	2019-07-03	FMC/FMCv FTD/FTDv，除了 Firepower 1000 系列
	34	2019-06-27	-
		2019-06-26	Firepower 7000/8000 系列 ASA FirePOWER NGIPSv
6.4.0.1	17	2019-06-27	FMC 1600、2600、4600
		2019-06-20	Firepower 4115、4125、4145 具有 SM-40、SM-48 和 SM-56 模块的 Firepower 9300
		2019-05-15	FMC 750、1000、1500、2000、2500、3500、4000、4500 FMCv Firepower 2110、2120、2130、2140 Firepower 4110、4120、4140、4150 具有 SM-24、SM-36 和 SM-44 模块的 Firepower 9300 ASA 5508-X、5515-X、5516-X、5525-X、5545-X、5555-X ASA 5585-X-SSP-10、-20、-40、-60 ISA 3000 FTDv Firepower 7000/8000 系列 NGIPSv



第 2 章

兼容性

本章提供 Firepower 版本 6.4.0.x修补程序的兼容性信息。

有关所有受支持 Firepower 版本的详细兼容性信息，包括捆绑组件和集成产品，请参阅思科 Firepower 兼容性指南。

- Firepower 管理中心s， 第 3 页
- Firepower 设备， 第 4 页
- 管理器-设备的兼容性， 第 6 页
- 网络浏览器兼容性， 第 7 页
- 屏幕分辨率要求， 第 8 页

Firepower 管理中心s

物理和虚拟平台都支持 版本 6.4.0.xFirepower 管理中心 软件；有关支持的 FMCv 实例，请参阅《思科虚拟 Firepower 管理中心入门指南》。FMC 可以管理任何 Firepower 设备。

Firepower 管理中心物理平台：

- FMC 1600、2600、4600
- FMC 1000、2500、4500
- FMC 2000、4000
- FMC 750、1500、3500

Firepower 管理中心虚拟：

- VMware vSphere/VMware ESXi 6.0 或 6.5 上的 FMCv
- 基于内核的虚拟机 (KVM) 上的 FMCv
- Amazon Web 服务 (AWS) 上的 FMCv
- Microsoft Azure 上的 FMCv

Firepower 设备

版本 6.4.0.x众多物理和虚拟平台都支持 Firepower 设备软件。

- **软件:** 有些 Firepower 设备运行 Firepower 威胁防御 (FTD) 软件；有些运行 NGIPS/ASA FirePOWER 软件。有些两种都能运行 - 但不能同时运行两者。
- **远程管理:** 所有 Firepower 设备均支持使用 Firepower 管理中心进行远程管理，该中心可管理多个设备。
- **本地管理：** 一些Firepower 设备支持本地、单设备管理。您可以使用Firepower 设备管理器 (FDM) 或 ASA FirePOWER 与 ASDM 来管理 FTD。一次只能使用一种管理方法来管理设备。
- **操作系统/管理程序:** 有些 Firepower 实施方案将操作系统与软件捆绑在一起。有些则要求您自行升级操作系统。适用于捆绑操作系统的版本和内部版本，请参阅思科 Firepower 兼容性指南中的捆绑组件信息。

下表提供了运行版本 6.4.0.x的 Firepower 设备的兼容性信息。再次提醒，请记住，所有设备都支持远程 FMC 管理。

表 *2:* 版本 *6.4.0.x* 的 *Firepower* 设备

设备平台	软件	本地管理	操作系统/管理程序
Firepower 1010、1120 和 1140 Firepower 2110、2120、2130、2140	FTD	FDM	-
Firepower 4110、4120、4140、4150 Firepower 4115、4125、4145 Firepower 9300具有 SM-24、SM-36、SM-44 模块 Firepower 9300具有 SM-40、SM-48、SM-56 模块	FTD	-	FXOS 2.6.1.157 或更高的内部版本。 单独升级。先升级 FXOS。 要解决问题，您可能需要将FXOS升级到最新的内部版本。请参阅《思科 Firepower 4100/9300 FXOS 发行说明 [2.6(1)]》以帮助您做决定。

设备平台	软件	本地管理	操作系统/管理程序
ISA 3000	FTD	FDM	-
ASA 5508-X、5516-X ASA 5515-X、5525-X、5545-X、5555-X	ASA FirePOWER (NGIPS)	ASDM	以下项中的任一个： • ASA 9.5(2)、9.5(3) • ASA 9.6(x) 至 9.13 （x） 例外： • 运行 ASA 9.13（X）+ 的 ASA 5515-X 设备不支持。 ASA FirePOWER。 单独升级。请参阅《思科 ASA 升级指南》以了解操作顺序。 ASA 与 ASA FirePOWER 版本之间有广泛的兼容性。但是，即使并非严格要求进行 ASA 升级，但是解决问题可能需要升级到支持的最新版本。 我们建议您将 ASA 5508-X和 5516-X 升级到最新的 ROMMON 映像;请参阅 思科 ASA 和 Firepower 威胁防御重新映像指南中的说明。
ASA 5585-X-SSP-10、-20、-40、-60	ASA FirePOWER (NGIPS)	ASDM	以下项中的任一个： • ASA 9.5(2)、9.5(3) • ASA 9.6(x) 至 9.12(x) 单独升级。请参阅《思科 ASA 升级指南》以了解操作顺序。 ASA 与 ASA FirePOWER 版本之间有广泛的兼容性。但是，即使并非严格要求进行 ASA 升级，但是解决问题可能需要升级到支持的最新版本。

设备平台	软件	本地管理	操作系统/管理程序
FTDv	FTD	FDM（仅 VMware 和 KVM）	以下项中的任一个： • VMware vSphere/VMware ESXi 6.0 或 6.5 • KVM • AWS • Microsoft Azure 有关受支持的实例，请参阅对应的 FTDv 快速入门/入门指南。
NGIPSv	NGIPS	-	VMware vSphere/VMware ESXi 6.0 或 6.5 有关受支持的实例，请参阅适用于 VMware 的思科 Firepower NGIPSv 快速入门指南。
Firepower 7010、7020、7030、7050 Firepower 7110、7115、7120、7125 Firepower 8120、8130、8140 Firepower 8250、8260、8270、8290 Firepower 8350、8360、8370、8390 AMP 7150、8050、8150 AMP 8350、8360、8370、8390	NGIPS	用于选择管理功能的有限本地 GUI。	-

管理器-设备的兼容性

FMC 运行的主版本必须至少与其管理的设备相同。 尽管您可以使用没有修补程序的 FMC 管理安装了修补程序的设备，新功能和解决的问题通常需要 FMC 及其管理的设备上都有最新的修补程序。强烈建议您对整个部署安装修补程序。

表 *3:* 版本 *6.4.0.x* 管理器-设备的兼容性

Firepower 管理中心		
版本 6.4.0.x FMC	可以管理	版本 6.1 至 6.4.0.x 的设备

版本 6.4.0.x 的设备	要求	6.4.0 版 FMC
Firepower 设备管理器		
版本 6.4.0.x FDM	可以管理	一个 FTD 设备
ASDM		
版本 7.12.1 ASDM	可以管理	6.4.0.x 及更低版本的 ASA FirePOWER 模块
版本 6.4.0.x ASA FirePOWER 模块	要求	版本 7.12.1 ASDM

网络浏览器兼容性

从 Firepower 监控的网络浏览 Web

许多浏览器默认使用传输层安全 (TLS) v1.3。如果您使用 SSL 策略来处理加密流量，并且受监控网络中的人员使用启用了 TLS v1.3 的浏览器，则系统可能无法加载支持 TLS v1.3 的网站。

有关更多信息，请参阅标题为使用启用了 *SSL* 检查的 *TLS 1.3* 加载网站时出现故障的软件公告。

与 FMC 进行安全通信

SSL 证书使得 FMC（和 7000/8000 系列设备）能够在设备和浏览器之间建立起加密通道。

默认情况下，系统附带自签 HTTPS 服务器证书。我们建议您将其替换为由全球知名或内部受信任的证书颁发机构 (CA) 签名的证书。您可以在 HTTPS Certificates 页面上生成自定义服务器证书请求并导入自定义服务器证书；选择 **System** > **Configuration**，然后单击 **HTTPS Certificates**。

有关详细信息，请参阅联机帮助或Firepower 管理中心配置指南。

使用 Firepower Web 界面对浏览器进行了测试

Firepower Web 界面使用最新版本的热门浏览器进行测试： Google Chrome、Mozilla Firefox 和 Microsoft Internet Explorer。如果您遇到任何其他浏览器的问题，我们会要求您切换。如果问题持续存在，请联系思科 TAC。

注释 虽然我们不使用 Apple Safari 或 Microsoft 边缘执行广泛的测试， 思科 TAC还欢迎您对您在最新版本的浏览器中遇到的问题提供反馈。

表 *4:* 使用 ***Firepower Web*** 界面对浏览器进行了测试

浏览器	必要设置和其他警告
Google Chrome	JavaScript、Cookie Chrome 不会使用系统提供的自签证书缓存静态内容，例如图像、CSS 或 JavaScript。特别是在低带宽环境中，这会使得页面加载时间延长。如果您不想替换自签证书，可以将其添加到浏览器/操作系统的信任库中。
Mozilla Firefox	JavaScript、cookie、TLS v1.2 当其更新时，Firefox 有时会停止信任系统提供的自签名证书。如果不想替换证书，并且登录页面未加载，请刷新 Firefox。在 Firefox 搜索栏中键入 **`about:support`**，然后单击 **Refresh Firefox**。您会丢失一些设置；请参阅刷新 Firefox 支持页面。
Microsoft Internet Explorer 11 (Windows)	JavaScript、cookie、TLS v1.2、128 位加密 此外，您还必须： • 对于 **Check for newer versions of stored pages** 浏览历史选项，选择 **Automatically**。 • 禁用**当将文件上载到服务器时包括本地目录路径**自定义安全设置。 • 为 Firepower Web 界面 IP 地址/URL 启用兼容性视图。 未使用 FMC 演练进行测试。

浏览器扩展兼容性

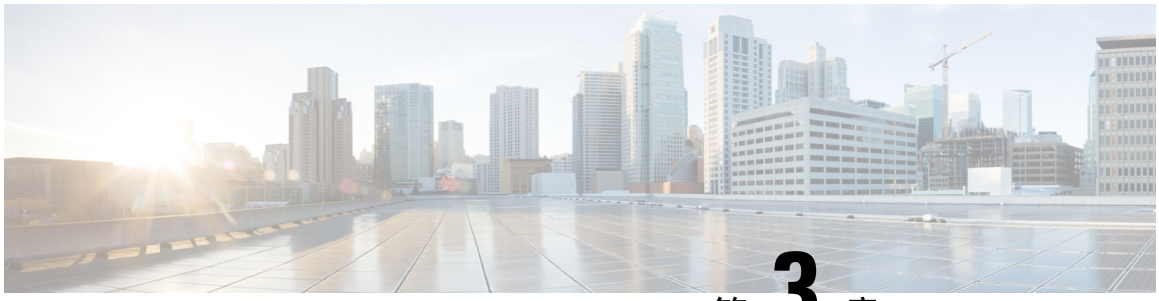
某些浏览器扩展（例如，Grammarly 和 Whatfix 编辑器）可以防止您在 PKI 对象中的证书和密钥等字段中保存值。这些扩展名在字段中插入字符（例如HTML），这会导致FMC将其视为无效。我们建议您在使用 FMC 时禁用这些扩展。

屏幕分辨率要求

表 *5: Firepower* 用户界面的屏幕分辨率要求

接口	分辨率
Firepower 管理中心	1280 x 720
7000/8000 系列设备（有限的本地接口）	1280 x 720
Firepower 设备管理器	1024 x 768
ASDM 管理着 ASA FirePOWER 模块	1024 x 768

接口	分辨率
Firepower 机箱管理器for Firepower 4100/9300 机箱	1024 x 768



第 3 章

特性和功能

Firepower 版本 6.4.0.x包括：

- Firepower 中的新功能 版本 6.4.0.x，第 11 页
- 弃用的功能，第 12 页
- FMC 操作方法演练，第 12 页

Firepower 中的新功能 版本 6.4.0.x

此表概述了 Firepower 版本 6.4.0.x 修补程序中的新增功能。

表 *6:* 版本 *6.4.0.x* 新增的功能

特性	版本	说明
检测 FTD NAT 策略中的规则冲突	6.4.0.2	升级到版本 6.4.0.2 之后，您无法再创建具有冲突规则的 FTD NAT 策略（通常称为重复或重叠的规则）。这解决了无序应用冲突的 NAT 规则的问题。 如果您当前具有冲突的 NAT 规则，可以部署升级后的版本。但是，您的 NAT 规则将继续无序应用。 因此，我们建议您在升级后通过编辑（无需更改）并重新保存，检查 FTD NAT 策略。如果有规则冲突，系统会阻止您保存。更正问题、保存，然后部署。 支持的平台：使用 FMC 的 FTD
ISE 连接状态监控运行状况模块	6.4.0.2	新的运行状况模块（*ISE* 连接状态监控器）监控思科身份服务引擎 (ISE) 与 FMC 之间的服务器连接状态。 新增/经修改的屏幕： **系统 > 运行状况 > 策略 >** 创建或编辑策略 **> ISE 连接状态监控器** 支持的平台：FMC

特性	版本	说明
新的系统日志字段	6.4.0.4	这些新的系统日志字段共同标识一个唯一的连接事件： • 传感器 UUID • 第一个数据包时间 • 连接实例 ID (Connection Instance ID) • 连接计数器 (Connection Counter) 这些字段也会显示在系统日志中，用于入侵、文件和恶意软件事件，允许连接事件与这些事件相关联。 支持的平台：任意

弃用的功能

本主题列示了 Firepower 版本 6.4.0.x修补程序弃用的功能和平台。

有关所有受支持的Firepower版本的详细兼容性信息，包括弃用平台的销售终止和生命周期终止公告的链接，请参阅思科 Firepower 兼容性指南。

FMC 操作方法演练

版本 6.3.0 引入 FMC 上的演练（也称为使用方法），该演练将指导您完成各种基本任务，例如设备设置和策略配置。仅需单击浏览器窗口底部的**使用方法**，选择某一演练，然后按照分步说明进行操作。

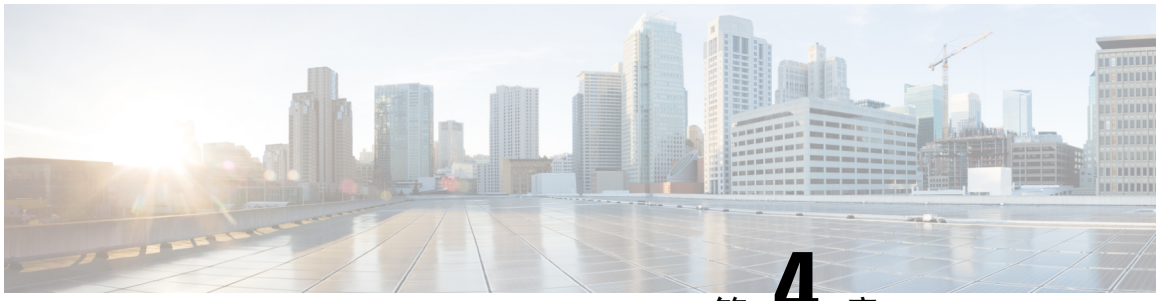
注释 演练已在 Firefox 和 Chrome 浏览器上进行了测试。如果您在使用其他浏览器时遇到问题，我们会要求您切换到 Firefox 或 Chrome。如果问题持续存在，请联系 Cisco TAC。

下表列出了一些常见的问题和解决方案。要在任何时候结束演练，请点击右上角的 **x** 。

表 *7:* 故障排除演练

问题	解决方案
找不到**使用方法**链接来启动演练。	请确保演练已启用。在用户名下面的下拉列表中，选择**用户首选项**，然后单击**方法设置**。
当您不期望时，系统会显示演练。	如果在您不期望的情况下出现本演练， 会结束本演练。

问题	解决方案
演练会突然消失或退出。	如果演练消失，请执行以下操作： • 移动指针。 有时，FMC 会停止显示正在进行的演练。例如，指向不同的顶级菜单可以实现这种情况。 • 导航到其他页面，然后重试。 如果移动指针不起作用，则本演练可能会退出。
演练与 FMC 不同步： • 从错误的步骤开始。 • 过早进行。 • 不会进行。	如果演练不同步，您可以执行以下操作： • 尝试继续。 例如，如果在字段中输入的值无效，并且 FMC 显示错误，则演练可能会提前进行。您可能需要返回并解决该错误以完成任务。 • 结束本演练，导航至其他页面，然后重试。 有时，您无法继续。例如，如果在完成某一步后未点击**下一步**，则可能需要结束本演练。



第 4 章

升级到版本 6.4.0.x

本章提供版本 6.4.0.x的关键和版本特定信息。

您还应该参阅特性和功能， 第 11 页，了解有关任何新的、更改的或弃用的特性和功能。

- 指引和警告： 版本 6.4.0.x， 第 15 页
- 一般指引和警告， 第 16 页
- 要升级的最低版本， 第 18 页
- 时间测试和磁盘空间要求， 第 18 页
- 流量、检查和设备行为， 第 23 页
- 升级说明， 第 31 页
- 升级程序包， 第 31 页

指引和警告： 版本 6.4.0.x

此核对表中包含适用于版本 6.4.0.x修补程序的重要升级指南和警告。此外，确保查看一般指引和警告， 第 16 页。

表 *8:* 版本 *6.4.0.x* 指引

	指南	平台	升级自	直接至
	升级失败：容器实例上的磁盘空间不足， 第 16 页	Firepower 4100/9300	6.4.0.x	更高版本的修补程序 6.5.0
	Firepower 1010 设备上的 Etherchannel 可以将出口流量引入黑洞， 第 16 页	Firepower 1010	仅 6.4.0	6.4.0.3 至 6.4.0.5
	Firepower 1000 系列不支持版本 6.4.0.1 和 6.4.0.2， 第 16 页	Firepower 1000 系列	仅 6.4.0	6.4.0.1 或 6.4.0.2

升级失败：容器实例上的磁盘空间不足

部署：使用 FTD 的 Firepower 4100/9300

升级自：版本 6.3.0 至 6.4.0.x

直接到：版本 6.3.0.1 到版本 6.5.0

最常见的情况是在主要升级期间，但在修补过程中，配置了容器实例的FTD 设备可能会在预检查阶段失败，并出现错误磁盘空间不足的警告。

如果发生这种情况，您可以尝试释放更多的磁盘空间。如果不起作用，请联系思科 TAC。

Firepower 1010 设备上的 Etherchannel 可以将出口流量引入黑洞

部署：使用 FTD 的 Firepower 1010

受影响的版本：版本 6.4.0 至 6.4.0.5

相关漏洞： CSCvq81354

我们强烈建议您不要在运行 FTD 版本 6.4.0 到版本 6.4.0.5 的 Firepower 1010 设备上配置 etherchannel。（请注意，此型号不支持版本 6.4.0.1 和 6.4.0.2。）

由于内部流量散列问题，Firepower 1010 设备上的某些 Etherchannel 可能会将某些出口流量引入黑洞。散列计算基于源/目标 IP 地址，因此对于给定的源/目标 IP 而言，行为将一致。也就是说，某些流量会正常工作，有些流量会失败。

我们将在即将推出的 6.4.0 补丁中修复此问题。它也已在版本 6.5.0 中修复。

Firepower 1000 系列不支持版本 6.4.0.1 和 6.4.0.2

部署：Firepower 1000 系列

升级自：版本 6.4.0

直接至：版本 6.4.0.1 或 6.4.0.2

不能将 Firepower 1000 系列设备升级至版本 6.4.0.1 或 6.4.0.2。

一般指引和警告

这些重要的指引和警告适用于所有升级。但这份清单并不全面。如需与升级过程相关的其他重要信息的链接，包括规划升级路径、操作系统升级、准备情况检查、备份、维护窗口等，请参阅升级说明，第 31 页。

备份事件和配置数据

我们强烈建议备份到外部位置并验证传输是否成功。在升级设备时，它会清除本地存储的备份。在 FMC 部署中，我们还建议您在升级部署后备份 FMC。这是因为您有一个新的 FMC 备份文件，它 "知道" 其设备已升级。

作为任何备份的第一步，请注意补丁级别和VDB版本。这一点很重要，因为如果您需要将备份恢复到新的或重新映像设备，则必须首先将该新设备更新为完全这些版本。您只能从相同型号和Firepower版本、具有相同 VDB 的设备还原备份。

设备访问

Firepower 设备可以在升级期间或在升级失败时停止传输流量（具体取决于接口配置）。在升级Firepower设备之前，请确保来自您所在位置的流量不必遍历设备本身即可访问设备的管理界面。在Firepower 管理中心部署中，您还必须能够访问 FMC 管理界面而不遍历设备。

签名的升级软件包

因此，Firepower可以证实您使用的是正确的文件，来自版本 6.2.1+ 的升级包（以及到版本 6.2.1+ 的热补丁）是签名的 tar 档案 (.tar)。早期版本的升级继续使用未签名的包。

当您手动从思科支持和下载站点下载升级包时 - 例如用于重要升级或物理隔离部署 - 确保下载正确的包。 不要解压签名的 (.tar) 包。

注释 上传签名的升级包后，GUI 可能需要几分钟才能加载，因为系统需要对包进行验证。要加快显示速度，可删除不再需要的签名的包。

在 ASA FirePOWER 设备上禁用 ASA REST API

在升级 ASA FirePOWER 模块之前，确保禁用 ASA REST API。否则，升级可能会失败。从 ASA CLI：`no rest api agent`。可以在卸载后重新启用：`rest-api agent`。

与思科共享数据

一些功能包括与思科共享数据。

在 6.2.3+ 中，思科成功网络会将使用情况信息和统计信息发送到思科，这些信息对于为您提供技术支持至关重要。升级期间，系统可能会要求您接受或拒绝参与。您还可以随时选择加入或退出。

在 6.2.3+ 中，*Web* 分析跟踪会将非个人可识别使用情况数据发送到思科，包括但不限于页面交互情况、浏览器版本、产品版本、用户位置以及您的 FMC 的管理 IP 地址或主机名。如果要从版本 6.1 升级到 6.2.2.x，升级将启用 Web 分析跟踪。如果您不希望思科收集这些数据，可以在升级后选择退出。（如果是从版本 6.2.3.x或版本 6.3.0.x 升级，升级过程会考虑您当前的设置。）

在 6.5.0+ 中，思科支持诊断 （有时称为思科主动支持）将配置和运行状况数据发送到思科，并通过我们的自动化问题检测系统处理该数据，使我们能够主动通知您的问题。在TAC情况下，此功能还允许思科TAC从您的设备收集基本信息。升级期间，系统可能会要求您接受或拒绝参与。您还可以随时选择加入或退出。

升级可以导入和自动启用入侵规则

如果新的入侵规则使用您的不受当前Firepower版本支持的关键字，则在更新入侵规则数据库 (SRU) 时不会导入该规则。

升级 Firepower 软件并支持这些关键字后，系统将导入新的入侵规则，并且根据 IPS 配置，可以自动启用，从而开始生成事件并影响流量。

受支持的关键字取决于 Firepower 软件随附的 Snort 版本：

- FMC：依次选择**帮助 > 关于**。
- 使用 FDM 的 FTD：使用**show summary** CLI 命令。
- 使用 ASDM 的 ASA FirePOWER：选择**ASA FirePOWER 配置 > 系统信息**。

您还可以在《Cisco Firepower 兼容性指南》的捆绑组件部分找到您的 Snort 版本。

Snort 版本说明包含有关新关键字的详细信息。您可以阅读 Snort 下载页面上的版本说明：https://www.snort.org/downloads。

无响应的升级

请勿将更改部署到正在升级的设备或从其部署更改，手动重启正在升级的设备，或者关闭正在升级的设备。请勿重启正在进行的升级。升级过程在预检查期间可能会显示为非活动；这是预期行为。如果您遇到升级问题，包括升级失败或设备无响应，请联系思科 TAC。

要升级的最低版本

只能在当前主版本序列中修补 Firepower 软件。修补程序是累积的，因此始终可以直接跳到最新的修补程序。

表 *9:* 将 *Firepower* 软件升级到 *6.4.0.x* 的最低版本

平台	最低版本
Firepower 管理中心 FMC 部署中的所有受管设备）。	6.4.0
使用 FDM 的 Firepower 威胁防御（所有平台）	6.4.0
使用 ASDM 的 ASA FirePOWER	6.4.0

时间测试和磁盘空间要求

要升级 Firepower 设备，必须具有足够的可用磁盘空间，否则升级会失败。使用 Firepower 管理中心升级受管设备时，FMC 的 /Volume 分区必须具备额外的磁盘空间来存放设备升级包。此外，您还必须具有足够的时间来执行升级。

我们提供内部时间和磁盘空间测试报告以供参考。

关于时间测试

此处给出的时间值基于内部测试。虽然我们报告的是针对特定平台/系列测试的所有升级的最慢时间，但由于多种原因（见下文），您的升级所需的时间可能比提供的时间长。

基本测试条件

- 部署：值来自于Firepower管理中心部署中的测试。这是因为在类似条件下，远程和本地管理设备的原始升级时间相似。
- 版本：对于主版本升级，我们测试所有先前符合条件的主版本的升级。对于修补程序，我们测试基础版本和前一个修补程序的升级。
- 型号：大多数情况下，我们测试每个系列中的最低端型号，有时会对系列中的多个型号进行测试。
- 虚拟设置：我们使用内存和资源的默认设置进行测试。

不包括推送和重新启动

值仅表示 Firepower 升级脚本本身以运行所花费的时间。值不包括将升级包上传到本地受管设备或 FMC 所需的时间，也不包括将升级包从 FMC 复制（推送）到受管设备所需的时间。

在 FMC部署中，如果 FMC与受管设备之间的带宽不足，可能会延长升级时间甚至导致升级超时。请确保您的带宽足以将大量数据从 FMC传输到其设备。有关详细信息，请参阅将数据从 Firepower 管理中心下载到受管设备的准则（故障排除技术说明）。

值也不包括重新启动、准备情况检查、操作系统升级或配置部署。

时间适用于单个设备

值是按设备提供的。在高可用性或群集配置中，设备一次升级一个可保持操作的连续性，每个设备在升级时以维护模式运行。因此，升级一对设备或整个群集所需的时间比升级独立设备所需的时间长。

请注意，堆叠的8000系列设备会同时升级，堆栈在有限的混合版本状态下运行，直到所有设备完成升级。这样做所需的时间应该不会比升级独立设备花费的时间长。

受影响的配置和数据

我们对具有最小配置和流量负载的设备进行了测试。升级时间会随着配置的复杂性、事件数据库的大小以及这些事物是否/如何受到升级的影响而增加。例如，如果您使用大量访问控制规则并且升级需要对这些规则的存储方式进行后端更改，则升级可能需要更长时间。

关于磁盘空间要求

空间估计值在为所有升级报告的值中最大，为：

- 没有四舍五入（小于 1 MB）。

- 四舍五入到下一个 1 MB (1 MB - 100 MB)。
- 四舍五入到下一个 10 MB (100 MB - 1GB)。
- 四舍五入到下一个 100 MB（大于 1 GB）。

版本 6.4.0.6 的时间和磁盘空间

表 *10:* 版本 *6.4.0.6* 的时间和磁盘空间

平台	/Volume 上的空间	/ 上的空间	FMC 上的空间	来自 6.4.0 的时间
FMC	5.5 GB	170 MB	-	38 分钟
FMCv：VMware 6.0	3.4 GB	36 MB	-	33 分钟
Firepower 1000 系列	2.4 GB	2.4 GB	530 MB	25 分钟
Firepower 2100 系列	2.4 GB	2.4 GB	500 MB	16 分钟
Firepower 4100 系列	1.8 GB	1.8 GB	310 MB	12 分钟
Firepower 9300	1.8 GB	1.8 GB	310 MB	15 分钟
具有 ASA 5500-X 系列的 FTD	1.8 GB	110 MB	290 MB	23 分钟
FTDv：VMware 6.0	1.8 GB	110 MB	290 MB	10 分钟
Firepower 7000/8000 系列	3.6 GB	170 MB	650 MB	25 分钟
ASA FirePOWER	4.1 GB	36 MB	590 MB	45 分钟
NGIPSv：VMware 6.0	2.1 GB	150 MB	450 MB	10 分钟

版本 6.4.0.5 的时间和磁盘空间

表 *11:* 版本 *6.4.0.5* 的时间和磁盘空间

平台	/Volume 上的空间	/ 上的空间	FMC 上的空间	来自 6.4.0 的时间
FMC	5 GB	170 MB	-	39 分钟
FMCv：VMware 6.0	3.7 GB	170 MB	-	27 分钟
Firepower 1000 系列	2.9 GB	2.9 GB	530 MB	26 分钟
Firepower 2100 系列	2.5 GB	2.5 GB	500 MB	16 分钟

平台	/Volume 上的空间	/ 上的空间	FMC 上的空间	来自 6.4.0 的时间
Firepower 4100 系列	1.8 GB	1.8 GB	310 MB	12 分钟
Firepower 9300	1.8 GB	1.8 GB	310 MB	11 分钟
具有 ASA 5500-X 系列的 FTD	1.8 GB	110 MB	290 MB	20 分钟
FTDv：VMware 6.0	1.8 GB	110 MB	290 MB	10 分钟
Firepower 7000/8000 系列	3.6 GB	170 MB	650 MB	26 分钟
ASA FirePOWER	4.1 GB	36 MB	590 MB	45 分钟
NGIPSv：VMware 6.0	2.1 GB	150 MB	450 MB	10 分钟

版本 6.4.0.4 的时间和磁盘空间

表 *12:* 版本 *6.4.0.4* 的时间和磁盘空间

平台	/Volume 上的空间	/ 上的空间	FMC 上的空间	来自 6.4.0 的时间
FMC	4.4 GB	170 MB	-	35 分钟
FMCv：VMware 6.0	4.8 GB	170 MB	-	31 分钟
Firepower 1000 系列	2.9 GB	2.9 GB	520 MB	28 分钟
Firepower 2100 系列	2.4 GB	2.4 GB	500 MB	10 分钟
Firepower 4100 系列	2 GB	2 GB	310 MB	12 分钟
Firepower 9300	1.7 GB	1.7 GB	310 MB	10 分钟
具有 ASA 5500-X 系列的 FTD	1.8 GB	110 MB	290 MB	29 分钟
FTDv：VMware 6.0	1.8 GB	110 MB	290 MB	8 分钟
Firepower 7000/8000 系列	3.6 GB	170 MB	650 MB	24 分钟
ASA FirePOWER	4.2 GB	36 MB	600 MB	55 分钟
NGIPSv：VMware 6.0	2.1 GB	150 MB	550 MB	10 分钟

版本 6.4.0.3 的时间和磁盘空间

表 *13:* 版本 *6.4.0.3* 的时间和磁盘空间

平台	/Volume 上的空间	/ 上的空间	FMC 上的空间	来自 6.4.0 的时间
FMC	3.2 GB	24 MB	-	34 分钟
FMCv：VMware 6.0	2.5 GB	23 MB	-	25 分钟
Firepower 1000 系列	2.9 GB	2.9 GB	520 MB	22 分钟
Firepower 2100 系列	2.4 GB	2.4 GB	500 MB	19 分钟
Firepower 4100 系列	1.7 GB	1.7 GB	310 MB	12 分钟
Firepower 9300	1.7 GB	1.7 GB	310 MB	14 分钟
具有 ASA 5500-X 系列的 FTD	1.8 GB	110 MB	290 MB	18 分钟
FTDv：VMware 6.0	1.8 GB	110 MB	290 MB	12 分钟
Firepower 7000/8000 系列	1.9 GB	21 MB	370 MB	20 分钟
ASA FirePOWER	2.5 GB	2.5 GB	320 MB	28 分钟
NGIPSv：VMware 6.0	690 MB	21 MB	210 MB	8 分钟

版本 6.4.0.2 的时间和磁盘空间

表 *14:* 版本 *6.4.0.2* 的时间和磁盘空间

平台	/Volume 上的空间	/ 上的空间	FMC 上的空间	来自 6.4.0 的时间
FMC	3.1 GB	24 MB	-	39 分钟
FMCv：VMware 6.0	2.5 GB	23 MB	-	24 分钟
Firepower 2100 系列	1.9 GB	1.9 GB	480 MB	19 分钟
Firepower 4100 系列	2.3 GB	2.3 GB	290 MB	11 分钟
Firepower 9300	1.7 GB	1.7 GB	290 MB	11 分钟
具有 ASA 5500-X 系列的 FTD	1.8 GB	110 MB	270 MB	21 分钟
FTDv：VMware 6.0	1.2 GB	110 MB	270 MB	10 分钟

平台	/Volume 上的空间	/ 上的空间	FMC 上的空间	来自 6.4.0 的时间
Firepower 7000/8000 系列	1.9 GB	36 MB	350 MB	20 分钟
ASA FirePOWER	2 GB	21 MB	300 MB	34 分钟
NGIPSv：VMware 6.0	630 MB	21 MB	190 MB	10 分钟

版本 6.4.0.1 的时间和磁盘空间

表 *15:* 版本 *6.4.0.1* 的时间和磁盘空间

平台	/Volume 上的空间	/ 上的空间	FMC 上的空间	来自 6.4.0 的时间
FMC	1.8 GB	24 MB	-	50 分钟
FMCv：VMware 6.0	1.8 GB	23 MB	-	20 分钟
Firepower 2100 系列	1.4 GB	1.4 GB	300 MB	17 分钟
Firepower 4100 系列	1.1 GB	1.1 GB	95 MB	9 分钟
Firepower 9300	1.1 GB	1.1 GB	95 MB	10 分钟
具有 ASA 5500-X 系列的 FTD	550 MB	110 MB	76 MB	16 分钟
FTDv：VMware 6.0	550 MB	110 MB	76 MB	15 分钟
Firepower 7000/8000 系列	59 MB	21 MB	2 MB	14 分钟
ASA FirePOWER	85 MB	20 MB	2 MB	30 分钟
NGIPSv：VMware 6.0	45 MB	21 MB	2 MB	10 分钟

流量、检查和设备行为

升级期间必须确定流量和检测中的潜在中断。以下情况下可能出现这种问题：

- 设备重新启动时。
- 在设备上升级操作系统或虚拟主机环境时。
- 在设备上升级 Firepower 软件或卸载修补程序时。
- 在升级或卸载过程中部署配置更改时（Snort 进程重新启动）。

设备类型、部署类型（独立、高可用性、群集）和接口配置（被动、IPS、防火墙等）决定了中断的性质。我们强烈建议在维护窗口或者中断对部署的影响最小时执行升级或卸载。

FTD升级行为： Firepower 4100/9300 机箱

本部分介绍在升级含 FTD的 Firepower 4100/9300 机箱时的设备和流量行为。

Firepower 4100/9300 机箱：FXOS 升级

在每个机箱上独立升级 FXOS，即使配置了机箱间群集或高可用性对也是如此。您执行升级的方式会确定设备在 FXOS 升级期间处理流量的方式。

表 *16: FXOS* 升级期间的流量行为

部署	方法	流量行为
独立式	-	被丢弃
高可用性	**最佳实践**：在备用设备上更新FXOS，切换主用对等设备，升级新的备用设备。	不受影响
	在备用设备完成升级之前，在主用对等设备上升级 FXOS。	被丢弃，直到一个对等设备处于在线状态
机箱间群集（6.2及更高版本）	**最佳实践**：一次升级一个机箱，以便至少有一个模块始终处于在线状态。	不受影响
	同时升级机箱，因此在某个时间所有模块都处于关闭状态。	被丢弃，直到至少一个模块处于在线状态
机箱内群集（仅限Firepower 9300）	已启用故障时自动绕过：**Bypass: Standby** 或 **Bypass-Force**。（6.1 及更高版本）	不检查直接通过
	已禁用故障时自动绕过：**Bypass: Disabled**。（6.1 及更高版本）	被丢弃，直到至少一个模块处于在线状态
	没有故障时自动旁路模块。	被丢弃，直到至少一个模块处于在线状态

独立式 FTD 设备：Firepower 软件升级

接口配置会确定在升级期间独立设备如何处理流量。

表 *17: Firepower* 软件升级期间的流量行为：独立式 *FTD* 设备

接口配置		流量行为
防火墙接口	路由或交换，包括 EtherChannel、冗余、子接口 切换接口也称为桥接组或透明接口。	被丢弃
仅限 IPS 接口	内联集，故障时自动旁路启用：**Bypass: Standby** 或 **Bypass-Force** (6.1+)	可以为以下任意一项： • 被丢弃（6.1 至 6.2.2.x） • 不检查直接通过（6.2.3 及更高版本）
	内联集，已禁用故障时自动旁路：**Bypass: Disabled** (6.1+)	被丢弃
	内联集，没有故障时自动旁路模块	被丢弃
	内联集，分流模式	立即传出数据包，不检查副本
	被动，ERSPAN 被动	不中断，不检查

高可用性对：Firepower 软件升级

在高可用性对中的设备上升级 Firepower 软件时，流量或检查中不应出现中断。为确保操作的连续性，它们一次升级一个。升级时，设备会在维护模式下运行。

首先升级备用设备。设备会交换角色，然后新的备用设备进行升级。升级完成后，设备的角色保持交换后的状态。如果您想要保留主用/备用角色，请先手动交换角色，然后再进行升级。这样，升级流程会将它们交换回来。

群集：Firepower 软件升级

在 Firepower 威胁防御群集中的设备上升级 Firepower 软件时，流量或检查中不应出现中断。为确保操作的连续性，它们一次升级一个。升级时，设备会在维护模式下运行。

首先升级一个或多个从属安全模块，然后升级主模块。升级时，安全模块在维护模式下运行。

在主安全模块升级期间，尽管流量检查和处理通常会继续，但系统会停止记录事件。升级完成后，在日志记录关闭期间处理的流量事件显示有不同步的时间戳。但是，如果日志记录关闭较长时间，则系统可能会删除最早事件，然后再记录事件。

注释 从版本 6.2.0、6.2.0.1 或 6.2.0.2 升级机箱间群集会导致从群集中删除每个模块时，流量检查中出现 2-3 秒的流量中断。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于设备处理流量的方式。

高可用性和集群无中断升级要求

执行无中断升级具有以下其他要求。

流负载分流：由于在流负载分流功能中修复了漏洞，因此 FXOS 和 FTD 的一些组合不支持流负载分流；请参阅思科 Firepower 兼容性指南。要在高可用性或集群部署中执行无中断升级，必须确保始终运行兼容的组合。

如果您的升级路径包括将 FXOS 升级到 2.2.2.91、2.3.1.130 或更高版本（包括 FXOS 2.4.1. x、2.6.1. x 等），请使用此路径：

1. 将 FTD 升级到 6.2.2.2 或更高版本。
2. 将 FXOS 升级到 2.2.2.91、2.3.1.130 或更高版本。
3. 将 FTD 升级到您的最终版本。

例如，如果您运行的是 FXOS 2.2.2.17/FTD 6.2.2.0，并且要升级到 FXOS 2.6.1/FTD 6.4.0，则可以执行以下操作：

1. 将 FTD 升级到 6.2.2.5。
2. 将 FXOS 升级到 2.6.1。
3. 将 FTD 升级到 6.4.0。

版本 6.1.0 升级：将 FTD 高可用性对无故障升级到版本 6.1.0 需要一个预安装包。有关详细信息，请参阅Firepower 系统发行说明 6.1.0 版预安装包。

部署过程中的流量行为

升级过程中，您需要多次部署配置。如果在升级后立即进行首次部署，Snort 通常会重启。该进程在其他部署期间不重启，除非您在部署之前修改特定策略或设备配置。有关详细信息，请参阅Firepower 管理中心配置指南中的在部署或激活时重启 *Snort* 进程的配置。

在部署时，资源需求可能会导致少量数据包未经检测而被丢弃。此外，重启 Snort 进程会中断所有 Firepower 设备上的流量检查，包括为 HA/可伸缩性配置的检查。在中断期间，接口配置会确定是丢弃流量还是在不检查的情况下允许流量通过。

表 *18: FTD* 部署过程中的流量行为

接口配置		流量行为
防火墙接口	路由或交换，包括 EtherChannel、冗余、子接口 切换接口也称为桥接组或透明接口。	被丢弃

接口配置		流量行为
仅限 IPS 接口	内联集，已启用或禁用 **Failsafe** (6.0.1-6.1.0.x)	不检查直接通过 如果已禁用 **Failsafe**，并且 Snort 处于繁忙而非关闭状态，则系统可能会丢弃一些数据包。
	内联集，**Snort Fail Open: Down**：已禁用（6.2 及更高版本）	被丢弃
	内联集，**Snort Fail Open: Down**：启用 (6.2+)	不检查直接通过
	内联集，分流模式	立即传出数据包，不检查副本
	被动，ERSPAN 被动	不中断，不检查

FTD升级行为：其他设备

本部分介绍在 Firepower 1000/2100 系列、ASA 5500-X 系列、 ISA 3000、和 FTDv上升级 Firepower 威胁防御时的设备和流量行为。

独立式 FTD 设备：Firepower 软件升级

接口配置会确定在升级期间独立设备如何处理流量。

表 *19: Firepower* 软件升级期间的流量行为：独立式 *FTD* 设备

接口配置		流量行为
防火墙接口	路由或交换，包括 EtherChannel、冗余、子接口 切换接口也称为桥接组或透明接口。	被丢弃
仅限 IPS 接口	内联集，故障时自动旁路启用：**Bypass: Standby** 或 **Bypass-Force** (6.1+)	可以为以下任意一项： • 被丢弃（6.1 至 6.2.2.x） • 不检查直接通过（6.2.3 及更高版本）
	内联集，已禁用故障时自动旁路：**Bypass: Disabled** (6.1+)	被丢弃
	内联集，没有故障时自动旁路模块	被丢弃
	内联集，分流模式	立即传出数据包，不检查副本
	被动，ERSPAN 被动	不中断，不检查

高可用性对：Firepower 软件升级

在高可用性对中的设备上升级 Firepower 软件时，流量或检查中不应出现中断。为确保操作的连续性，它们一次升级一个。升级时，设备会在维护模式下运行。

首先升级备用设备。设备会交换角色，然后新的备用设备进行升级。升级完成后，设备的角色保持交换后的状态。如果您想要保留主用/备用角色，请先手动交换角色，然后再进行升级。这样，升级流程会将它们交换回来。

部署过程中的流量行为

升级过程中，您需要多次部署配置。如果在升级后立即进行首次部署，Snort 通常会重启。该进程在其他部署期间不重启，除非您在部署之前修改特定策略或设备配置。有关详细信息，请参阅 Firepower 管理中心配置指南中的在部署或激活时重启 *Snort* 进程的配置。

在部署时，资源需求可能会导致少量数据包未经检测而被丢弃。此外，重启 Snort 进程会中断所有 Firepower 设备上的流量检查，包括为 HA/可伸缩性配置的检查。在中断期间，接口配置会确定是丢弃流量还是在不检查的情况下允许流量通过。

表 *20: FTD* 部署过程中的流量行为

接口配置		流量行为
防火墙接口	路由或交换，包括 EtherChannel、冗余、子接口 切换接口也称为桥接组或透明接口。	被丢弃
仅限 IPS 接口	内联集，已启用或禁用 **Failsafe** (6.0.1-6.1.0.x)	不检查直接通过 如果已禁用 **Failsafe**，并且 Snort 处于繁忙而非关闭状态，则系统可能会丢弃一些数据包。
	内联集，**Snort Fail Open: Down**：已禁用（6.2 及更高版本）	被丢弃
	内联集，**Snort Fail Open: Down**：启用 (6.2+)	不检查直接通过
	内联集，分流模式	立即传出数据包，不检查副本
	被动，ERSPAN 被动	不中断，不检查

Firepower 7000/8000 系列升级行为

以下部分介绍升级 Firepower 7000/8000 系列设备时的设备和流量行为。

独立式 7000/8000 系列：Firepower 软件升级

接口配置会确定在升级期间独立设备如何处理流量。

表 *21:* 升级时的流量行为：独立式 *7000/8000* 系列

接口配置	流量行为
内联，已启用硬件绕过 (**Bypass Mode: Bypass**)	不检查直接通过，但是流量会在以下两个时间点短暂中断： • 升级过程开始时，链路关闭并重新开启（振荡），网卡切换到硬件绕过模式。 • 升级完成后，链路再次出现振荡，网卡退出硬件绕过模式。终端重新连接并与设备接口重新建立链路后，检查会恢复。
内联，没有硬件绕过模块，或已禁用硬件绕过模式 (**Bypass Mode: Non-Bypass**)	被丢弃
内联，分流模式	立即传出数据包，不检查副本
被动	不中断，不检查
路由式、交换式	被丢弃

7000/8000 系列高可用性对：Firepower 软件升级

在高可用性对中升级设备（或设备堆叠）时，流量流或检查不应出现中断。为确保操作的连续性，它们一次升级一个。升级时，设备会在维护模式下运行。

首先升级哪一个对等设备取决于您的部署：

- 路由式或交换式：优先升级备用设备。设备会交换角色，然后新的备用设备进行升级。升级完成后，设备的角色保持交换后的状态。如果您想要保留主用/备用角色，请先手动交换角色，然后再进行升级。这样，升级流程会将它们交换回来。
- 纯访问控制：优先升级主用设备。升级完成后，主用设备和备用设备保持其原有角色。

8000 系列堆栈：Firepower 软件升级

在8000系列堆栈中，设备同时进行升级。在主设备完成其升级并且堆栈恢复操作之前，流量都会受到影响，就像堆栈是一个独立设备一样。在所有设备完成升级之前，堆栈会在一个受限的混合版本状态下运行。

部署过程中的流量行为

升级过程中，您需要多次部署配置。如果在升级后立即进行首次部署，Snort通常会重启。该进程在其他部署期间不重启，除非您在部署之前修改特定策略或设备配置。有关详细信息，请参阅Firepower管理中心配置指南中的在部署或激活时重启 *Snort* 进程的配置。

在部署时，资源需求可能会导致少量数据包未经检测而被丢弃。此外，重启 Snort 进程会中断所有 Firepower 设备上的流量检查，包括为 HA/可伸缩性配置的检查。在中断期间，接口配置会确定是丢弃流量还是在不检查的情况下允许流量通过。

表 *22:* 部署期间的流量行为： *7000/8000* 系列

接口配置	流量行为
内联，**Failsafe** 已启用或已禁用	不检查直接通过 如果已禁用 **Failsafe**，并且 Snort 处于繁忙而非关闭状态，则系统可能会丢弃一些数据包。
内联，分流模式	立即传出数据包，副本绕过 Snort
被动	不中断，不检查
路由式、交换式	被丢弃

ASA FirePOWER升级行为

在 Firepower 软件升级期间（包括在您部署会导致 Snort 进程重启的某些配置时），模块处理流量的方式由用于将流量重定向到 ASA FirePOWER 模块的 ASA 服务策略决定。

表 *23: ASA FirePOWER* 升级期间的流量行为

流量重定向策略	流量行为
故障时打开 (**sfr fail-open**)	不检查直接通过
故障时关闭 (**sfr fail-close**)	被丢弃
仅监控 (**sfr {fail-close}|{fail-open} monitor-only**)	立即传出数据包，不检查副本

ASA FirePOWER部署过程中的流量行为

Snort 进程重启时的流量行为与升级 ASA FirePOWER 模块时相同。

升级过程中，您需要多次部署配置。如果在升级后立即进行首次部署，Snort通常会重启。该进程在其他部署期间不重启，除非您在部署之前修改特定策略或设备配置。有关详细信息，请参阅Firepower管理中心配置指南中的在部署或激活时重启 *Snort* 进程的配置。

在部署时，资源需求可能会导致少量数据包未经检测而被丢弃。此外，重启 Snort 进程会中断流量检查。在中断期间，您的服务策略会确定是丢弃流量还是在不检查的情况下允许流量通过。

NGIPSv升级行为

本部分介绍在升级 NGIPSv时的设备和流量行为。

Firepower 软件升级

接口配置决定了NGIPSv在升级期间如何处理流量。

表 *24: NGIPSv*升级期间的流量行为

接口配置	流量行为
内联	被丢弃
内联，分流模式	立即传出数据包，不检查副本
被动	不中断，不检查

部署过程中的流量行为

升级过程中，您需要多次部署配置。如果在升级后立即进行首次部署，Snort通常会重启。该进程在其他部署期间不重启，除非您在部署之前修改特定策略或设备配置。有关详细信息，请参阅Firepower管理中心配置指南中的在部署或激活时重启 *Snort* 进程的配置。

在部署时，资源需求可能会导致少量数据包未经检测而被丢弃。此外，重启Snort进程会中断流量检查。在中断期间，接口配置会确定是丢弃流量还是在不检查的情况下允许流量通过。

表 *25: NGIPSv*部署过程中的流量行为

接口配置	流量行为
内联，**Failsafe** 已启用或已禁用	不检查直接通过 如果已禁用 **Failsafe**，并且 Snort 处于繁忙而非关闭状态，则系统可能会丢弃一些数据包。
内联，分流模式	立即传出数据包，副本绕过 Snort
被动	不中断，不检查

升级说明

发行说明中不含升级说明。读完这些发行说明中的指引和警告后，参阅以下任一资料：

- 《思科 Firepower 管理中心升级指南》：升级 FMC 部署，包括受管设备和配套的操作系统。
- 思科 ASA 升级指南：使用 ASDM 升级 ASA FirePOWER 模块
- 适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南：使用 FDM 升级 FTD。

升级程序包

思科支持和下载站点上提供了升级包。

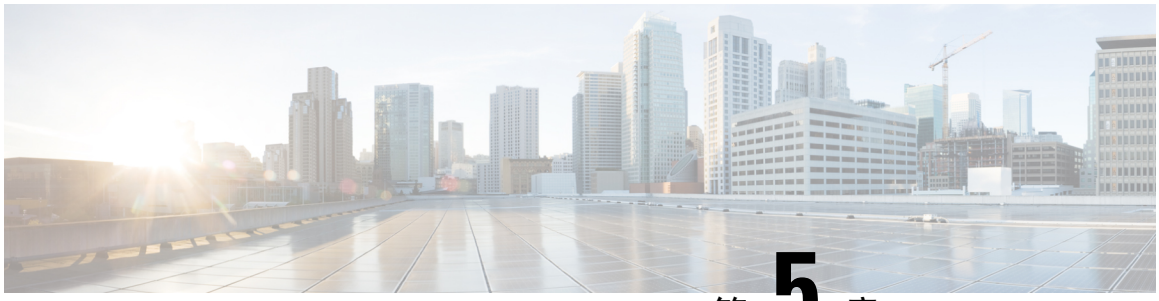
- Firepower 管理中心，包括FMCv：https://www.cisco.com/go/firepower-software
- Firepower 威胁防御 (ISA 3000)： https://www.cisco.com/go/isa3000-software

- Firepower 威胁防御（所有其他型号，包括 FTDv）：https://www.cisco.com/go/ftd-software
- Firepower 7000 系列： https://www.cisco.com/go/7000series-software
- Firepower 8000 系列： https://www.cisco.com/go/8000series-software
- 具备 FirePOWER 服务的 ASA（ASA 5500-X 系列）： https://www.cisco.com/go/asa-firepower-sw
- 具备 FirePOWER 服务的 ASA (ISA 3000)： https://www.cisco.com/go/isa3000-software
- NGIPSv： https://www.cisco.com/go/ngipsv-software

不要解压签名的 (.tar) 包。

表 *26:* 升级包 版本 *6.4.0.x*

平台	数据包
FMC/FMCv	Cisco_Firepower_Mgmt_Center_Patch-版本-内部版本.sh.REL.tar
Firepower 1000 系列	Cisco_FTD_SSP_FP1K_Patch-版本-内部版本.sh.REL.tar
Firepower 2100 系列	Cisco_FTD_SSP_FP2K_Patch-版本-内部版本.sh.REL.tar
Firepower 4100/9300 机箱	Cisco_FTD_SSP_Patch-版本-内部版本.sh.REL.tar
ASA 5500-X 系列，含 FTD ISA 3000，含 FTD Firepower 威胁防御虚拟	Cisco_FTD_Patch-版本-内部版本.sh.REL.tar
Firepower 7000/8000 系列	Cisco_Firepower_NGIPS_Appliance_Patch-版本-内部版本.sh.REL.tar
ASA FirePOWER	Cisco_Network_Sensor_Patch-版本-内部版本.sh.REL.tar
NGIPSv	Cisco_Firepower_NGIPS_Virtual_Patch-版本-内部版本.sh.REL.tar



第 5 章

卸载版本 6.4.0.x 修补程序

您可以从以下位置卸载 Firepower 修补程序：

- FMC 及其受管设备
- 通过 ASDM 管理的 ASA FirePOWER 模块

卸载修补程序会导致设备运行您升级之前的版本。

注释 不能从 FDM 管理的 FTD 设备卸载修补程序。也不能从任何设备卸载主版本的 Firepower 软件。在这些情况下，您必须重新安装。

有关详情，请参阅：

- 卸载的指引和限制，第 33 页
- 高可用性/可扩展性部署的卸载顺序，第 35 页
- 卸载说明，第 37 页
- 卸载软件包，第 42 页

卸载的指引和限制

这些重要的准则和限制适用于卸载。

验证您的补丁是否支持卸载

卸载特定的修补程序可能会在 Firepower 设备上造成问题，包括：

- 操作系统与 Firepower 软件之间的不兼容性。
- 如果您在启用安全认证合规性的情况下安装修补程序（CC/UCAPL 模式），则设备重新启动时 FSIC（文件系统完整性检查）失败。

⚠

注意 如果启用了安全认证合规性并且 FSIC 失败，则 Firepower 软件无法启动，远程 SSH 访问会被禁用，并且您只能通过本地控制台访问该设备。如果出现此情况，请联系思科 TAC。

在这些情况下，如果您需要恢复到较早的补丁，我们建议您重新映像，然后再进行升级。

下表列出了不应卸载的情况。

表 *27:* 版本 *6.4.0.x* 的修补程序，在卸载时会出现后续问题

平台	卸载起始版本	升级起始版本
FMC/FMCv Firepower 7000/8000 系列 ASA FirePOWER NGIPSv	6.4.0.2+	6.4.0 至 6.4.0.1
FMC/FMCv Firepower 7000/8000 系列 ASA FirePOWER NGIPSv	6.4.0.3+	6.4.0 至 6.4.0.2
任意	6.4.0.4 +	6.4.0. 至 6.4.0.3

使用外壳程序先从设备卸载

在 FMC 部署中，先从受管设备卸载修补程序。我们建议 FMC 运行比其受管设备更高的版本。

要卸载设备修补程序，必须使用 Linux 外壳程序，也称为“专家模式”。这意味着您可以单独在本地从设备卸载。换句话说：

- 不能从群集、堆叠或高可用性 (HA) Firepower 设备批量卸载修补程序，也不能通过 FirePOWER 服务设备将其从群集或故障转移ASA批量卸载。要规划最大限度减少中断的卸载顺序，请参阅高可用性/可扩展性部署的卸载顺序，第 35 页。
- 您不能使用 FMC、ASDM 或 FDM 从设备卸载修补程序，也不能在 7000/8000 系列设备上使用本地 Web 界面。
- 您不能使用 FMC 用户帐户登录并从其受管设备之一卸载修补程序。Firepower 设备会维护自己的用户帐户。
- 您必须能够以设备的管理员用户或者具有CLI配置访问权限的其他本地用户身份访问设备外壳程序。如果禁用了外壳程序访问，则无法卸载设备修补程序。联系思科 TAC以撤销设备锁定。

从设备卸载后再从 FMC 卸载

从受管设备卸载后，再从 FMC 卸载修补程序。与升级一样，必须从高可用性 FMC 一次卸载一个；请参阅高可用性/可扩展性部署的卸载顺序，第 35 页。

我们建议您使用 FMC web 界面卸载 FMC 修补程序。您必须有管理员访问权限。如果无法使用 Web 界面，可以作为外壳的管理员用户或者具有外壳访问权限的外部用户使用 Linux 外壳程序。如果禁用了外壳程序访问，请联系思科 TAC以撤销FMC锁定。

设备访问

Firepower 设备可以在卸载期间或在卸载失败时停止传输流量（具体取决于接口配置）。从 Firepower 设备卸载修补程序之前，请确保来自您所在位置的流量不必遍历设备本身即可访问设备的管理界面。在 Firepower 管理中心部署中，您还必须能够访问 FMC 管理界面而不遍历设备。

在 ASA FirePOWER 设备上禁用 ASA REST API

在卸载 ASA FirePOWER 修补程序之前，请确保禁用 ASA REST API。否则，卸载可能会失败。从 ASA CLI：`no rest api agent`。可以在卸载后重新启用：`rest-api agent`。

卸载无响应

请勿将更改部署到正在卸载的设备或从其部署更改，手动重启正在卸载的设备，或者关闭正在卸载的设备。请勿重启正在进行的卸载。卸载过程有时可能会显示为非活动状态；这是预期行为。如果您遇到卸载问题，包括卸载失败或设备无响应，请联系思科 TAC。

失败的卸载可能需要重新映像，从而让大多数设置恢复为出厂默认设置。因此，在重新映像之前，我们强烈建议您将事件和配置数据备份到外部位置。

流量、检查和设备行为

卸载期间的流量和检查中断与升级期间发生的中断相同。我们强烈建议在维护窗口或者中断对部署的影响最小时执行卸载。有关详细信息，请参阅流量、检查和设备行为，第 23 页。

高可用性/可扩展性部署的卸载顺序

您可以单独从 Firepower 设备卸载修补程序，甚至是作为一个单元升级的修补程序。特别是在高可用性 (HA) 和可扩展性部署中，您应该规划好卸载顺序，以最大限度地减少中断。与升级不同，系统不会为您执行此操作。下表列出了适用于高可用性/可扩展性部署的卸载顺序。

请注意，在大多数情况下，您将：

- 先从辅助/备用/从设备卸载，然后是主要/主用/主设备。
- 一次卸载一个。等到修补程序从一个设备完全卸载后，再转到下一个设备。

表 *28: HA* 中 *FMC* 的卸载顺序

FMC 部署	卸载顺序
FMC 高可用性	同步暂停后（即一种称为裂脑的状态），每次从FMC对等设备卸载一个。请勿在对处于群集脑裂的情况下执行或部署配置更改。 **1.** 暂停同步（进入裂脑）。 **2.** 从备用设备卸载。 **3.** 从主用设备卸载。 **4.** 重启同步（退出裂脑）。

表 *29: HA* 或群集中 *FTD* 设备的卸载顺序

FTD 部署	卸载顺序
FTD 高可用性	不能从配置为高可用性的FTD设备卸载修补程序。必须先中断高可用性。 **1.** 中断高可用性。 **2.** 从先前的备用设备卸载。 **3.** 从先前的主用设备卸载。 **4.** 重新建立高可用性。
FTD 群集	一次从一个单元卸载，将主单元留到最后。卸载修补程序时，群集单元在维护模式下运行。 **1.** 从从模块逐一卸载。 **2.** 让其中一个从模块成为新的主模块。 **3.** 从先前的主模块卸载。

表 *30: HA* 或堆栈中 *7000/8000* 系列设备的卸载顺序

7000/8000 系列部署	卸载顺序
7000/8000 系列高可用性	始终从备用设备卸载。卸载修补程序时，HA 对中的 7000/8000 系列设备在维护模式下运行。 **1.** 从备用设备卸载。 **2.** 切换角色。 **3.** 从新的备用设备卸载。
8000 系列堆栈	同时从堆栈中的所有设备卸载。在从堆栈中的所有设备卸载修补程序之前，堆栈以有限的混合版本状态运行。

表 *31: ASA* 故障转移对/群集中带 *FirePOWER* 服务设备的 *ASA* 的卸载顺序

ASA 部署	卸载顺序
ASA 主用/备用故障转移对，带 ASA FirePOWER	始终从备用设备卸载。 **1.** 从备用 ASA 设备上的 ASA FirePOWER 模块卸载。 **2.** 故障转移。 **3.** 从新备用 ASA 设备上的 ASA FirePOWER 模块卸载。
ASA 主用/主用故障转移对，带 ASA FirePOWER	在您未卸载的设备上使两个故障转移组均处于主用状态。 **1.** 使两个故障转移组在主要 ASA 设备上均处于主用状态。 **2.** 从辅助 ASA 设备上的 ASA FirePOWER 模块卸载。 **3.** 使两个故障转移组在辅助 ASA 设备上均处于主用状态。 **4.** 从主要 ASA 设备上的 ASA FirePOWER 模块卸载。
ASA 群集，带 ASA FirePOWER	卸载前，在每个单元上禁用群集。一次从一个单元卸载，将主单元留到最后。 **1.** 在从单元上禁用群集。 **2.** 从该单元上的 ASA FirePOWER 模块卸载。 **3.** 重新启用群集。等待单元重新加入群集。 **4.** 对每个从属设备重复上述操作。 **5.** 在主单元上禁用群集。等待新的主设备接管。 **6.** 从先前主设备上的 ASA FirePOWER 模块卸载。 **7.** 重新启用群集。

卸载说明

以下各节说明如何从符合条件的设备卸载 Firepower 修补程序。

从独立的 FMC 卸载

遵照此程序从独立的 Firepower 管理中心（包括 Firepower 管理中心虚拟）卸载修补程序。

开始之前

从受管设备卸载修补程序。我们建议 FMC 运行比其受管设备更高的版本。

步骤 1 部署到其配置已过期的受管设备。

在卸载之前进行部署可减少失败的可能性。

步骤 2 执行预先检查。

- 检查运行状况：使用 FMC 上的消息中心（单击菜单栏上的“系统状态”图标）。确保部署中的设备能够成功通信，并且运行状况监控器未报告任何问题。
- 正在运行的任务：此项也位于消息中心中，用于确保完成重要任务。在卸载开始时运行的任务已停止，成为失败的任务，且不能恢复。您可以稍后手动删除具有失败状态的消息。

步骤 3 依次选择**系统 (System)** > **更新 (Updates)**。

步骤 4 单击 FMC 卸载软件包旁边的安装图标，然后选择 FMC。

如果没有正确的卸载软件包，请联系思科 TAC。

步骤 5 单击**安装**以开始卸载。

确认要卸载并重新启动 FMC。

步骤 6 在消息中心中监控进度，直到注销。

在卸载修补程序期间，不进行配置更改或部署到任何设备。即使消息中心在数分钟内不显示进度，或指示卸载失败，请勿重新开始卸载或重启 FMC。相反，请联系思科 TAC。

步骤 7 在修补程序卸载完成且 FMC 重新启动后，重新登录 FMC。

步骤 8 验证是否成功。

选择**帮助** > **关于**以显示当前的软件版本信息。

步骤 9 使用消息中心重新检查部署运行状况。

步骤 10 重新部署配置。

从高可用性 FMC 卸载

遵照此程序从高可用性对中的 Firepower 管理中心卸载修补程序。

每次从对等设备卸载一个。在暂停同步的情况下，首先从备用设备卸载，然后是主用设备。当备用 FMC 开始卸载时，其状态从备用切换到主用，以便两个对等设备都处于主用状态。此临时状态称为裂脑，仅在升级和卸载期间受支持。请勿在对处于群集脑裂的情况下执行或部署配置更改。重启同步后，您所做的更改将丢失。

开始之前

从受管设备卸载修补程序。我们建议 FMC 运行比其受管设备更高的版本。

步骤 1 在主用 FMC上，部署到其配置已过期的受管设备。

在卸载之前进行部署可减少失败的可能性。

步骤 2 在暂停同步之前，使用消息中心检查部署运行状况。

单击 FMC菜单上的“系统状态”图标以显示消息中心。确保部署中的设备能够成功通信，并且运行状况监控器未报告任何问题。

步骤 3 暂停同步。

a) 选择**系统** > **集成**。
b) 在**高可用性**选项卡，单击**暂停同步**。

步骤 4 每次从 FMC 卸载一个修补程序 - 先是备用设备，再是主用设备。

请按照从独立的 FMC 卸载，第 37 页中的说明进行操作，但省略初始部署，并在验证每个 FMC 上的更新均成功后停止。总而言之，对于每个 FMC：

a) 执行预先检查（运行状况、正在运行的任务）。
b) 在**系统** > **更新**页面上，卸载修补程序。
c) 监控进度，直到您注销，然后在可以时重新登录。
d) 验证卸载是否成功。

请勿在对处于群集脑裂的情况下执行或部署配置更改。

步骤 5 在您想要设为主用对等设备的 FMC上，重新开始同步。

a) 选择**系统** > **集成**。
b) 在**高可用性**选项卡，单击**设为主用**。
c) 等待直至同步重新开始，并且其他 FMC 切换到备用模式。

步骤 6 使用消息中心重新检查部署运行状况。

步骤 7 重新部署配置。

从任意设备卸载（FMC 管理）

遵照此程序从Firepower管理中心部署中的单个受管设备卸载修补程序。这包括物理和虚拟设备、安全模块以及 ASA FirePOWER 模块。

开始之前

- 确保您从正确的设备卸载，尤其是在高可用性/可扩展性部署中。请参阅高可用性/可扩展性部署的卸载顺序，第 35 页。
- 对于 ASA FirePOWER 模块，确保禁用 ASA REST API。从 ASA CLI：`no rest api agent`。可以在卸载后重新启用：`rest-api agent`。

步骤 1 如果设备的配置过期，请立即从 FMC 部署。

在卸载之前进行部署可减少失败的可能性。

例外：不要部署到混合版本的堆栈、群集或 HA 对。在高可用性/可扩展性部署中，先部署，然后从第一个设备卸载，但在您从所有成员卸载修补程序之前，不要再继续。

步骤 2 执行预先检查。

- 检查运行状况：使用 FMC 上的消息中心（单击菜单栏上的“系统状态”图标）。确保部署中的设备能够成功通信，并且运行状况监控器未报告任何问题。
- 正在运行的任务：此项也位于消息中心中，用于确保完成重要任务。在卸载开始时运行的任务已停止，成为失败的任务，且不能恢复。您可以稍后手动删除具有失败状态的消息。

步骤 3 在设备上访问 Firepower CLI。使用配置访问权限作为管理员或其他 Firepower CLI 用户登录。

您可以通过 SSH 登录到设备的管理界面（主机名或 IP 地址），也可以使用控制台。 请注意，ASA 5585-X 系列设备有专用的 ASA FirePOWER 控制台端口。

如果使用控制台，有些设备默认使用操作系统 CLI，并且需要完成额外的步骤才能访问 Firepower CLI。

Firepower 1000/2100 系列	`connect ftd`
Firepower 4100/9300 机箱	连接模块 *`slot_number`* 控制台，然后连接 `ftd`（仅限首次登录）
ASA FirePOWER，ASA 5585-X 系列除外	`session sfr`

步骤 4 Firepower CLI 提示时，使用 `expert` 命令访问 Linux 外壳程序。

步骤 5 运行卸载命令，在系统提示时输入密码。

```
sudo install_update.pl --detach /var/sf/updates/uninstall_package_name
```

软件包名称因平台而异；请参阅卸载软件包，第 42 页。 不要解压签名的 (.tar) 包。

除非您从控制台运行卸载，否则使用 `--detach` 选项确保在用户会话超时的情况下卸载不会停止。否则，卸载将作为用户外壳程序的子进程运行。如果终止连接，此进程也会中止，检查将中断，而且设备可能处于不稳定状态。

注意 系统不会要求您确认是否要卸载。输入此命令将启动卸载，其中包括设备重新启动。卸载期间的流量和检查中断与升级期间发生的中断相同。确保您已准备就绪。

步骤 6 监控卸载。

如果未分离卸载，进度会显示在控制台或终端上。如果已经分离，则可以使用 `tail` 或 `tailf` 来显示日志：

- FTD 设备：`tail /ngfw/var/log/sf/update.status`
- 所有其他设备：`tail /var/log/sf/update.status`

步骤 7 验证是否成功。

在修补程序卸载完成并且设备重新启动后，确认设备的软件版本正确。在 FMC 上，选择**设备** > **设备管理**。

步骤 8 使用消息中心重新检查部署运行状况。

步骤 9 重新部署配置。

例外：在高可用性/可扩展性部署中，不要部署到混合版本的堆栈、群集或 HA 对。仅在对所有成员重复此程序后才部署。

下一步做什么

- 对于高可用性/可扩展性部署，对计划序列中的每个设备重复此程序。然后，进行最终调整。例如，在 FTD HA 部署中，从两个对等设备卸载后重新建立 HA。
- 对于 ASA FirePOWER 模块，重新启用 ASA REST API（如果其之前被禁用）。从 ASA CLI：`rest-api agent`.

从 ASA FirePOWER 卸载（ASDM 管理）

遵照此程序从本地管理的 ASA FirePOWER 模块卸载修补程序。如果使用 FMC 管理 ASA FirePOWER，请参阅从任意设备卸载（FMC 管理），第 39 页。

开始之前

- 确保您从正确的设备卸载，尤其是 ASA 故障转移/群集部署。请参阅高可用性/可扩展性部署的卸载顺序，第 35 页。
- 确保禁用 ASA REST API。从 ASA CLI：`no rest api agent`。可以在卸载后重新启用：`rest-api agent`。

步骤 1 如果设备的配置过期，请立即从 ASDM 部署。

在卸载之前进行部署可减少失败的可能性。

步骤 2 执行预先检查。

- 系统状态：选择**监控** > **ASA FirePOWER 监控** > **统计信息**并确保一切都跟预期一样。
- 正在运行的任务：选择**监控** > **ASA FirePOWER 监控** > **任务**并确保完成必要任务。在卸载开始时运行的任务已停止，成为失败的任务，且不能恢复。您可以稍后手动删除具有失败状态的消息。

步骤 3 访问 ASA FirePOWER 模块上的 Firepower CLI。使用配置访问权限作为管理员或其他 Firepower CLI 用户登录。

您可以通过 SSH 登录到模块的管理界面（主机名或 IP 地址），也可以使用控制台。如果使用控制台，请注意，ASA 5585-X 系列设备有专用的 ASA FirePOWER 控制台端口。在其他 ASA 模型上，控制台端口默认为 ASA CLI，您必须使用 `session sfr` 命令访问 Firepower CLI。

步骤 4 Firepower CLI 提示时，使用 `expert` 命令访问 Linux 外壳程序。

步骤 5 运行卸载命令，在系统提示时输入密码。

```
sudo install_update.pl --detach /var/sf/updates/Cisco_Network_Sensor_Patch_Uninstaller-版本-内部版本.sh.REL.tar
```

不要解压签名的 (.tar) 包。

除非您从控制台运行卸载，否则使用 `--detach` 选项确保在用户会话超时的情况下卸载不会停止。否则，卸载将作为用户外壳程序的子进程运行。如果终止连接，此进程也会中止，检查将中断，而且设备可能处于不稳定状态。

注意 系统不会要求您确认是否要卸载。输入此命令将启动卸载，其中包括设备重新启动。卸载期间的流量和检查中断与升级期间发生的中断相同。确保您已准备就绪。

步骤 6 监控卸载。

如果未分离卸载，进度会显示在控制台或终端上。如果已经分离，则可以使用 `tail` 或 `tailf` 来显示日志：

```
tail /var/log/sf/update.status
```

在修补程序卸载过程中，不要将配置部署到设备。即使日志在数分钟内不显示进度，或指示升级失败，请勿重新开始卸载或重启设备。相反，请联系思科 TAC。

步骤 7 验证是否成功。

在修补程序卸载完成并且模块重新启动后，确认模块的软件版本正确。选择**配置** > **ASA FirePOWER 配置** > **设备管理** > **设备**。

步骤 8 重新部署配置。

下一步做什么

- 对于 ASA 故障转移/群集部署，对计划序列中的每个设备重复此程序。
- 对于 ASA FirePOWER 模块，重新启用 ASA REST API（如果其之前被禁用）。从 ASA CLI：`rest-api agent`.

卸载软件包

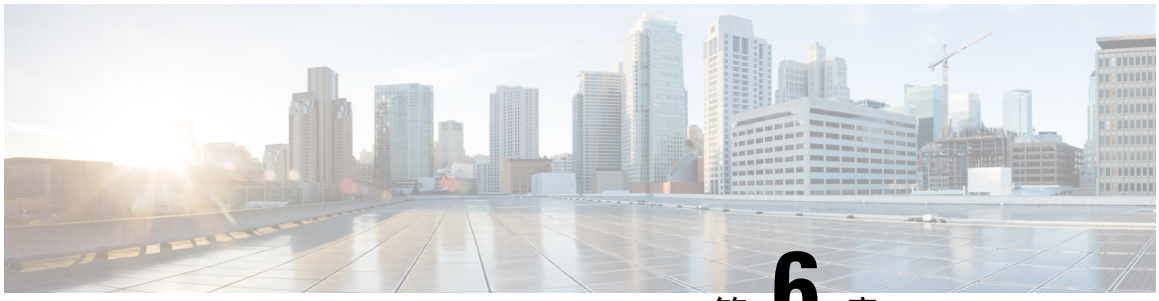
在 Firepower 设备上安装修补程序时，升级目录中会自动创建该修补程序的卸载程序：

- FTD上的 `/ngfw/var/sf/updates`
- FMC 和所有其他设备（7000/8000 系列、ASA FirePOWER、NGIPSv）上的 `/var/sf/updates`

如果程序包不在升级目录中（例如，您手动将其删除了），请联系思科 TAC。不要解压签名的 (.tar) 包。

平台	数据包
FMC/FMCv	Cisco_Firepower_Mgmt_Center_Patch_Uninstaller-版本-内部版本.sh.REL.tar
Firepower 1000 系列	Cisco_FTD_SSP_FP1K_Patch_Uninstaller-版本-内部版本.sh.REL.tar
Firepower 2100 系列	Cisco_FTD_SSP_FP2K_Patch_Uninstaller-版本-内部版本.sh.REL.tar

平台	数据包
Firepower 4100/9300 机箱	Cisco_FTD_SSP_Patch_Uninstaller-版本-内部版本.sh.REL.tar
ASA 5500-X 系列，含 FTD ISA 3000，含 FTD FTDv	Cisco_FTD_Patch_Uninstaller-版本-内部版本.sh.REL.tar
Firepower 7000/8000 系列	Cisco_Firepower_NGIPS_Appliance_Patch_Uninstaller-版本-内部版本.sh.REL.tar
NGIPSv	Cisco_Firepower_NGIPS_Virtual_Patch_Uninstaller-版本-内部版本.sh.REL.tar
ASA FirePOWER	Cisco_Network_Sensor_Patch_Uninstaller-版本-内部版本.sh.REL.tar



第 6 章

全新安装 版本 6.4.0

如果您无法升级 Firepower 设备，或者不愿意遵循要求的升级路径，可以新安装主要的 Firepower 版本。要运行特定的修补程序，先安装 版本 6.4.0，然后升级。

- 决定全新安装， 第 45 页
- 全新安装的指引和限制， 第 46 页
- 取消注册智能许可证， 第 48 页
- 安装说明， 第 50 页

决定全新安装

利用此表来识别您需要新安装的情况（亦称为重新映像）。所有情况下 - 包括在本地和远程之间切换设备管理 - 您将丢失设备配置。

注释 在重新映像或切换管理之前，始终要解决好许可问题。如果使用的是思科智能许可，则必须从思科智能软件管理器 (CSSM) 取消注册，以避免产生孤立的权利。这些可以阻止您重新注册。

表 *32:* 场景：需要全新安装吗？

场景	解决方案	许可
从较旧的 Firepower 版本升级 FMC管理的设备。	较旧版本的升级路径可以包含中间版本。特别是在必须替换 FMC 和设备升级的大型部署中，这个多步骤过程可能非常耗时。 为节省时间，您可以重新映像旧设备而不是升级： **1.** 从 FMC删除设备。 **2.** 仅将 FMC升级至其目标版本。 **3.** 重新映像设备。 如果需要重新映像运行版本 5.x 的 7000/8000 系列设备，请参阅全新安装的指引和限制，第 46 页。 **4.** 将设备重新添加到FMC。	从FMC删除设备会取消它们的注册。重新添加设备后重新分配许可证。
将 FTD 管理从 FDM 更改为 FMC（从本地到远程）。	使用 **configure manager** CLI 命令；请参阅《Firepower 威胁防御的命令参考》。	在切换管理之前取消设备的注册。将其添加到 FMC 后重新分配许可证。
将 FTD 管理从 FMC 更改为 FDM（从远程到本地）。	使用 **configure manager** CLI 命令；请参阅《Firepower 威胁防御的命令参考》。 **例外：**设备正在运行或者是从版本 6.0.1 升级。这种情况下，请重新映像。	从 FMC 中删除设备以取消注册。使用 FDM 重新注册。
在 ASDM 和 FMC 之间更改ASA FirePOWER管理。	开始使用其他管理方法。	联系销售人员以获取新的传统许可证。ASA FirePOWER 许可证与特定的管理器相关联。
在同一物理设备上将 ASA FirePOWER 替换为 FTD。	重新映像。	将传统许可证转换为智能许可证；请参阅Firepower 管理中心配置指南。
将 NGIPSv替换为 FTDv。	重新映像。	联系销售人员以获取新的智能许可证。
卸载含 FDM 的 FTD 修补程序。	重新映像。 不能在 FDM 部署中卸载修补程序。	在重新映像之前取消设备的注册。之后重新注册。

全新安装的指引和限制

认真规划和准备可以帮助您避免失误。即使您熟悉 Firepower 版本并且具有重新映像 Firepower 设备的经验，也请务必阅读这些指引和限制以及安装说明，第 50 页中链接的说明。

备份事件和配置数据

我们强烈建议备份到外部位置并验证传输是否成功。重新映像会将大多数设置恢复为出厂默认设置，包括系统密码 (Admin123)。

但请注意，如果要重新映像以便不必升级，则无法使用备份导入旧配置。您只能从相同型号和 Firepower 版本、具有相同 VDB 的设备还原备份。

作为任何备份的第一步，请注意补丁级别和 VDB 版本。在恢复备份之前，必须将重新映像设备更新为与这些版本完全相同的设备。

从以下位置删除设备 Firepower 管理中心

在重新映像之前，始终从远程管理中删除设备。如果您：

- 重新映像 FMC，从管理中删除其所有设备。
- 重新映像单个设备或从远程管理切换到本地管理，则删除该设备。

解决许可问题

在重新映像任何 Firepower 设备之前，解决许可问题。您可能需要从思科智能软件管理器取消注册，或者需要联系销售人员以取得新的许可证。请参阅决定全新安装以确定您需要执行的操作，具体取决于您所处的状况。

有关许可的详细信息，请参阅：

- 思科 Firepower 系统功能许可证指南
- Firepower 许可相关常见问题解答 (FAQ)
- 配置指南中的许可章节。

设备访问

重新映像会将大多数设置恢复为出厂默认设置。

如果您没有对设备的物理访问权限，则重新映像过程可让您保留管理网络设置。这样，您就可以在重新映像后连接到设备以执行初始配置。如果您删除网络设置，必须拥有对设备的物理访问权限。您不能使用无人值守管理 (LOM)。

注释 重新映像为较早的主要版本会自动删除网络设置。在这种极少数情况下，您必须具有物理访问权限。

对于设备，请确保来自您所在位置的流量不必遍历设备本身即可访问设备的管理界面。在FMC部署中，您还必须能够访问 FMC 管理界面而不遍历设备。

与思科共享数据

一些功能包括与思科共享数据。

在 6.2.3+ 中，思科成功网络会将使用情况信息和统计信息发送到思科，这些信息对于为您提供技术支持至关重要。初始设置期间，系统可能会要求您接受或拒绝参与。您还可以随时选择加入或退出。

在 6.2.3+ 中，*Web* 分析跟踪会将非个人可识别使用情况数据发送到思科，包括但不限于页面交互情况、浏览器版本、产品版本、用户位置以及您的 FMC 的管理 IP 地址或主机名。 Web 分析跟踪默认启用，但您可以在完成初始设置后随时退出。

在 6.5.0+ 中，思科支持诊断 （有时称为思科主动支持）将配置和运行状况数据发送到思科，并通过我们的自动化问题检测系统处理该数据，使我们能够主动通知您的问题。在 TAC 情况下，此功能还允许思科 TAC 从您的设备收集基本信息。初始设置期间，系统可能会要求您接受或拒绝参与。您还可以随时选择加入或退出。

将 Firepower 1000/2100 系列设备重新映像到较早的主版本

如果需要将 Firepower1000/2100 系列设备复原到较早的主版本，我们建议您执行完整的重新映像。如果您使用的是擦除配置方法，FXOS 可能无法与 Firepower 威胁防御软件一起使用。这可能会导致故障，尤其是在高可用性部署中。

有关更多信息，请参阅《适用于运行 Firepower 威胁防御的 Firepower 1000/2100 系列的思科 FXOS 故障排除指南》中的重新映像程序。

将版本 5.x 硬件重新映像到版本 6.3.0+

版本 6.3+ 中经重命名的安装包会导致重新映像较旧的物理设备时出现问题：DC750、1500、2000、3500 和 4000，以及 7000/8000 系列设备和 AMP 型号。如果您当前在运行版本 5.x 并需要全新安装版本 6.4.0，请下载后将安装包重命名为“旧”名称；请参阅思科 Firepower 发行说明，版本 6.3.0 中的重命名的升级和安装包信息。

当您将 FMC（防御中心）从版本 5.x 重新映像到更新的版本之后，其将无法管理较旧的设备。您还应该重新映像这些设备，并将它们重新添加至 FMC。请注意，系列 2 设备是 EOL，不能运行超过版本 5.4.0.x 的 Firepower 软件。必须换掉它们。

取消注册智能许可证

无论是本地（Firepower 设备管理器）还是远程 (Firepower 管理中心) 管理的 Firepower 威胁防御设备，都使用思科智能许可。要使用许可的功能，必须注册 Cisco Smart Software Manager (CSSM)。如果您以后决定重新映像或切换管理，必须取消注册以免产生孤立权利。这些可以阻止您重新注册。

取消注册操作会将设备从您服务取消注册，然后释放关联的许可证，以便可以重新分配。取消注册设备后，它将进入“强制”模式。其当前配置和策略将继续按原样运行，但您无法进行或部署任何更改。

在执行以下操作之前，先从 CSSM 手动取消注册：

- 重新映像管理 FTD 设备的 Firepower 管理中心。
- 重新映像 FDM 本地管理的 Firepower 威胁防御设备。
- 将 Firepower 威胁防御设备从 FDM 管理切换到 FMC 管理。

从 FMC 中删除设备时自动取消 CSSM 注册，以便可以：

- 重新映像 FMC 管理的 Firepower 威胁防御设备。
- 将 Firepower 威胁防御设备从 FMC 管理切换到 FDM 管理。

请注意，在这两种情况下，从 FMC中删除设备都会自动取消设备注册。只要您从 FMC删除设备，就无须手动取消注册。

提示 NGIPS 设备的经典许可证与特定管理器 (ASDM/FMC) 关联，并且不使用 CSSM 进行控制。如果要切换经典设备的管理，或者要从 NGIPS 部署迁移到 FTD 部署，请联系销售部门。

注销 Firepower 管理中心

在重新映像 FMC 之前，请从思科智能软件管理器注销 Firepower 管理中心。此操作还会注销任何受管的 Firepower 威胁防御设备。

如果 FMC配置为高可用性，许可更改将自动同步。您无须注销其他 FMC。

步骤 1 登录至Firepower 管理中心。

步骤 2 选择**系统** > **许可证** > **智能许可证**。

步骤 3 单击智能许可证状态旁边的停止标志 ( )。

步骤 4 请阅读警告并确认希望注销。

注销 FTD 设备，使用 FDM

在重新映像或切换为远程 (FMC) 管理之前，请从思科智能软件管理器注销本地受管的 Firepower 威胁防御设备。

如果该设备已配置高可用性，那么您必须登录到高可用性对的另一台设备才能注销该设备。

步骤 1 登录至Firepower 设备管理器。

步骤 2 单击 **设备**，然后单击 Smart License 摘要中的 **View Configuration**。

步骤 3 从齿轮下拉列表中选择 **Unregister Device**。

步骤 4 请阅读警告并确认希望注销。

安装说明

发行说明和升级指南中都不包含安装说明。相反，请参阅以下文档之一。思科支持和下载站点 上提供了安装包。

表 *33: Firepower* 管理中心安装说明

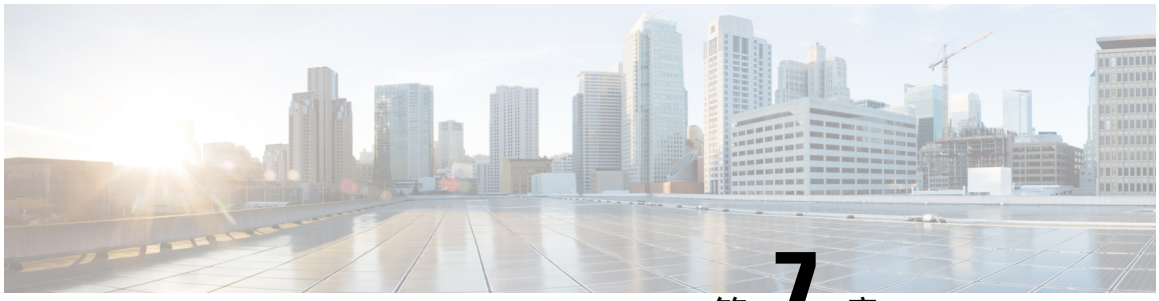
FMC 平台	指南
FMC1600、2600、4600	思科 Firepower 管理中心 1600、2600 和 4600 硬件安装指南：将 Firepower 管理中心恢复为出厂默认设置
FMC1000、2500、4500	1000、2500 和 4500 型号思科 Firepower 管理中心入门指南：将 *Firepower* 管理中心恢复为出厂默认设置
FMC750、1500、2000、3500、4000	750、1500、2000、3500 和 4000 型号思科 Firepower 管理中心入门指南：将 *Firepower* 管理中心恢复为出厂默认设置
FMCv	《思科虚拟 Firepower 管理中心入门指南》

表 *34: Firepower* 威胁防御安装说明

FTD 平台	指南
Firepower 1000/2100 系列	思科 ASA 和 Firepower 威胁防御重新映像指南 《适用于运行 Firepower 威胁防御的 Firepower 1000/2100 系列的思科 FXOS 故障排除指南》
Firepower 4100/9300 机箱	思科 Firepower 4100/9300 FXOS 配置指南：映像管理章节 《思科 Firepower 4100 入门指南》 《思科 Firepower 9300 入门指南》
ASA 5500-X 系列	思科 ASA 和 Firepower 威胁防御重新映像指南
ISA 3000	思科 ASA 和 Firepower 威胁防御重新映像指南
FTDv：VMware	《适用于 VMware 的思科虚拟 Firepower 威胁防御入门指南》
FTDv：KVM	《适用于 KVM 部署的思科虚拟 Firepower 威胁防御入门指南》
FTDv：AWS	适用于 AWS 云的思科 Firepower 威胁防御虚拟快速入门指南
FTDv：Azure	适用于 Microsoft Azure 云的思科 Firepower 威胁防御虚拟快速入门指南

表 *35: Firepower 7000/8000* 系列、*NGIPSv*、*ASA FirePOWER* 安装说明

NGIPS 平台	指南
Firepower 7000 系列	思科 Firepower 7000 系列入门指南：将设备恢复为出厂默认设置
Firepower 8000 系列	思科 Firepower 8000 系列入门指南：将设备恢复为出厂默认设置
NGIPSv	适用于 VMware 的思科 Firepower NGIPSv 快速入门指南
ASA FirePOWER	思科 ASA 和 Firepower 威胁防御重新映像指南 ASDM 手册 2：思科 ASA 系列防火墙 ASDM 配置指南：管理 *ASA FirePOWER* 模块



第 7 章

文档

以下主题提供 Firepower 文档：

- 更新的文档 版本 6.4.0.x，第 53 页
- 新增和更新的文档，第 53 页
- 文档目录，第 55 页

更新的文档 版本 6.4.0.x

针对至少一个版本 6.4.0.x修补程序更新了以下 Firepower 文档：

- 思科 Firepower 兼容性指南
- Firepower 管理中心配置指南（版本 6.4）和联机帮助

有关此版本未更新或新增可用文档的链接，请参阅文档目录，第 55 页。

新增和更新的文档

以下 Firepower 文档已更新或新增可用于版本 6.4.0.x。 有关此版本未更新或新增可用文档的链接，请参阅文档目录，第 55 页。

Firepower 配置指南和联机帮助

- Firepower 管理中心配置指南（版本 6.4）和联机帮助
- 适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南（版本 6.4.0）和联机帮助
- 具备 FirePOWER 服务的思科 ASA 本地管理配置指南（版本 6.4）和联机帮助
- 思科 Firepower 威胁防御命令参考

FXOS 配置指南和发行说明

- 思科 Firepower 4100/9300 FXOS Firepower 机箱管理器配置指南，2.6(1)

- 思科 Firepower 4100/9300 FXOS CLI 配置指南，2.6(1)
- 思科 Firepower 4100/9300 FXOS 命令参考
- 思科 Firepower 4100/9300 FXOS 发行说明，2.6(1)

强化指南

- 思科 Firepower 管理中心强化指南，版本 6.4 全新
- 思科 Firepower 威胁防御强化指南，版本 6.4 全新
- 《思科 Firepower 4100/9300 强化指南》全新

升级指南

- 《思科 Firepower 管理中心升级指南》
- 《思科 Firepower 4100/9300 升级指南》
- 思科 ASA 升级指南

硬件安装指南

- 思科 Firepower 管理中心 1600、2600 和 4600 硬件安装指南全新
- 《思科 Firepower 1010 硬件安装指南》全新
- 《思科 Firepower 1100 系列硬件安装指南》全新
- 《思科 Firepower 4115、4125 和 4145 硬件安装指南》全新
- 思科 Firepower 9300 硬件安装指南

入门指南

- 《适用于型号 1600、2600 和 4600 的思科 Firepower 管理中心入门指南》全新
- 《思科虚拟 Firepower 管理中心入门指南》
- 《适用于 VMware 的思科虚拟 Firepower 威胁防御入门指南》
- 《适用于 KVM 部署的思科虚拟 Firepower 威胁防御入门指南》
- 《思科 Firepower 1010 入门指南》全新
- 《思科 Firepower 1100 系列入门指南》全新
- 《思科 Firepower 4100 入门指南》全新
- 《思科 Firepower 9300 入门指南》全新

API 和集成指南

- Firepower 管理中心 REST API 快速入门指南，版本 6.4.0
- 思科 Firepower 威胁防御 REST API 指南
- Cisco Firepower App for Splunk 用户手册 全新
- 《Firepower 和思科威胁响应集成指南》全新

《兼容性指南》

- 思科 Firepower 兼容性指南
- 思科 ASA 兼容性
- 思科 Firepower 4100/9300 FXOS 兼容性

许可

- 思科 Firepower 系统功能许可证
- Firepower 许可相关常见问题解答 (FAQ)

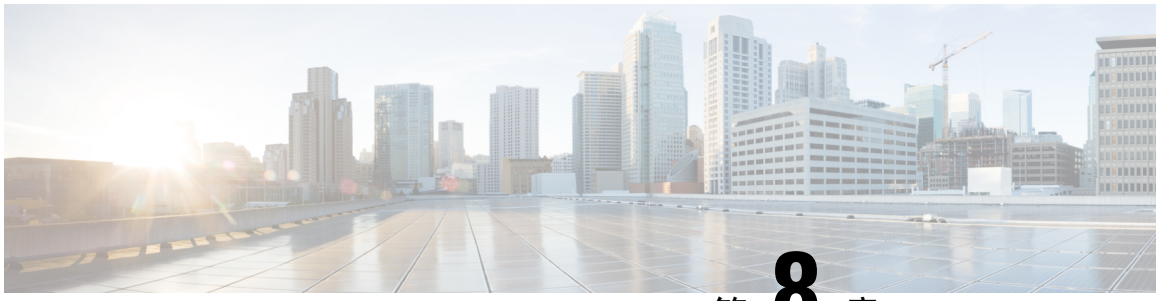
故障排除和配置示例

- 思科 Firepower 威胁防御系统日志消息
- 为 Firepower 威胁防御部署可扩展性和高可用性群集
- 《适用于运行 Firepower 威胁防御的 Firepower 1000/2100 系列的思科 FXOS 故障排除指南》

文档目录

文档路线图提供指向当前可用和旧版文档的链接：

- 导航思科 Firepower 文档
- Cisco ASA 系列文档一览
- 浏览思科 FXOS 文档



第 8 章

已解决的问题

当该修补程序最初发布时，所列的修补程序错误被证实已解决。

注释 为方便起见，本文档提供了每个补丁的已解决漏洞列表。这些列表会自动生成一次，并且随后不会进行更新。根据系统中特定解决问题的分类或更新方式（和时间），该问题可能不会显示在版本说明中。这并不意味着问题未得到解决。您应将思科缺陷搜索工具视为“真实的来源”。

- 搜索已解决的问题， 第 57 页
- 新内部版本中已解决的问题， 第 58 页
- 版本 6.4.0.6 已解决的问题， 第 58 页
- 版本 6.4.0.5 已解决的问题， 第 60 页
- 版本 6.4.0.4 已解决的问题， 第 61 页
- 版本 6.4.0.3 已解决的问题， 第 65 页
- 版本 6.4.0.2 已解决的问题， 第 66 页
- 版本 6.4.0.1 已解决的问题， 第 69 页

搜索已解决的问题

如果您有支持合同，可以通过思科漏洞搜索工具获取 Firepower 产品最新的已解决错误列表。这些常规查询显示已解决的、与运行 版本 6.4.0.x 修补程序的 Firepower 产品相关的问题：

- Firepower 管理中心
- Firepower 管理中心虚拟
- 具备 FirePOWER 服务的 ASA
- NGIPSv

可以将搜索范围限制为影响特定 Firepower 平台和版本的错误。还可以按错误 ID 搜索或者搜索特定关键字。

新内部版本中已解决的问题

有时，思科会发布更新的内部版本。在大多数情况下，上只能找到每个平台最新的内部版本。 思科支持和下载站点我们 强烈建议您使用最新版本。如果您下载的是较旧的版本，请不要使用。

对于相同的Firepower版本，您无法从一个内部版本升级到另一个内部版本。如果新内部版本可以解决您的问题，请确定是否可以使用升级或热补丁。如果不可以，您必须卸载并重新安装。有时，您可能需要。

使用此表确定新版本 6.4.0.x版本是否适用于您的平台。

表 *36:* 带有新版本的 *6.4.0.x* 版本修补程序

版本	新内部版本	已发布	平台	解决
6.4.0.2	35	2019-07-03	FMC/FMCv FTD/FTDv，除了 Firepower 1000 系列	CSCvq34224： Firepower 主要检测引擎进程在管理器升级后终止 如果您已升级到版本 6.4.0.2-34 并将 FTD 设备配置为高可用性，请应用修补程序F。在FMC部署中，将修补程序应用于FMC。在FDM部署中，将修补程序应用于两台设备。 此热补丁可从思科支持和下载站点获取，与版本 6.4.0.2 升级包位于同一位置。

版本 6.4.0.6 已解决的问题

表 *37:* 版本 *6.4.0.6* 已解决的问题

漏洞 ID	标题
CSCvm48451	入侵事件性能图形在 4100 和 9300 上加载空白
CSCvn77388	使用良好的服务器完成身份验证后，SDI 挂起的服务器会导致 15sec 延迟
CSCvo11280	ASA 增强功能：在 SDI 集群的成员更改状态后生成系统日志消息
CSCvo28118	当成员尝试加入集群时，VPN 集群 HA 计时器线程中的生成回溯
CSCvo43795	即使清除 OSPF 进程，OSPF 进程 ID 也不会更改
CSCvo73250	ENH：警告“找到重复元素”的 ACE 详细信息
CSCvo74397	ENH：将进程信息添加到 "命令已忽略，正在进行配置 ..."
CSCvo88762	FTD 内联/透明通过入口接口向后发送数据包

漏洞 ID	标题
CSCvp04186	cts 导入-pac tftp：语法不起作用
CSCvp12582	用于在 ASA 上显示访问列表上的端口号而不是众所周知的端口名称的选项
CSCvp23109	ASA HA IKEv2 通用 RA-AnyConnect 高级版备用中的所有使用不正确
CSCvp33341	Cisco ASA 和 Firepower 威胁防御软件 WebVPN 跨站脚本漏洞
CSCvp55901	ASA 上的 LINA 生成回溯重复高可用性主用设备
CSCvp55941	文件恢复块是随机引发的，导致 SMB 共享上的文件发生访问问题。
CSCvp56805	“写入期间数据过多”消息充斥通信通道
CSCvp76944	思科 ASA 和 FTD 软件 WebVPN CPU 拒绝服务漏洞
CSCvp85736	集群主设备重新加载导致管理虚拟 IP 的 ping 故障
CSCvp87623	使用 CAC （HTTPS 客户端证书）时，上传更新会使 "更新请求实体太大" 错误。
CSCvq05113	ASA 故障切换 LANTEST 消息在配置中的前 10 个接口上发送。
CSCvq09093	每台设备的 VPN 预部署验证大约需要 20 秒
CSCvq17263	FTD LINA 在 DATAPATH-8-15821 生成回溯
CSCvq24494	FP2100 流超订用环/CPU 核心，导致 FP2100 平台上的工作流中断
CSCvq28250	ENH：用于 syn cookie 问题的 ASA 集群调试
CSCvq36042	丢失的心跳导致重新加载
CSCvq39317	ASA 无法验证文件完整性
CSCvq40943	FTD 4150 VPN s2s 部署故障，6K 轮辐
CSCvq44665	FTD/ASA：在禁用 assert snp_tcp_intercept_assert_ 的数据路径中回溯
CSCvq45000	配置 NAT 后，对 FP 8000 传感器的策略部署失败
CSCvq54667	由于 SSL 协商问题，SSL VPN 可能无法建立
CSCvq57591	当只有 IP 通信在故障切换链路上中断时，LANTEST 消息不会在数据接口上发送
CSCvq59702	在丢失握手消息后，连接事件停止来自设备
CSCvq60131	将 EZVPN spoke 移动到设备时，发现出现 ASA 回溯。
CSCvq63024	双堆叠 ASAv 手动故障切换问题

漏洞 ID	标题
CSCvq64742	线程名称 ssh 中出现 ASA5515-K9 备用回溯
CSCvq65241	线程名称 IPv6 ID 中的 Saleen 上出现 ASA 回溯
CSCvq65542	在修复所有漏洞之前，从 fp2100 禁用 asp 负载均衡功能
CSCvq69111	回溯：线程名称“群集控制器”中出现群集单元 lina 断言
CSCvq70468	ASA 集群不刷新 OSPF 路由
CSCvq70485	慢速 "securityzones" REST API
CSCvq70775	FPR2100 FTD 备用设备泄漏 9K 块
CSCvq71217	由于 mysql-server 而导致的磁盘使用率高，在 CSCvn30118 后未能旋转
CSCvq75743	ASA：对目标 3 跳离开的 BGP 递归路由查找失败。
CSCvq76533	MC4000 的 F_RNA_EVENT_LIMIT 应为 20,000,000
CSCvq77547	由于端口通道上的故障切换描述符不匹配，连接无法在故障切换中复制
CSCvq80318	在枚举 Internal-Internal-data0/1 时，ASA 会生成有关 PCI cfg 空间的错误消息
CSCvq81516	FMC 上不显示 12和 1 PM UTC 之间的 VPN 事件
CSCvq83168	无法使用管理 VRF 进行 DNS 查找，因为 FMC 不允许在服务器地址后使用接口
CSCvq87703	主用设备未报告正确的对等体状态。
CSCvq91645	流分流散列行为更改
CSCvq92126	线程 IPsec 消息处理程序中生成 ASA 回溯
CSCvq94729	当在增量 cli 的仅 LINA 部分出错时，部署回滚会导致暂时丢弃流量
CSCvr00892	Where 子句不能用于外部数据库访问
CSCvr07421	由于 deployDB 的构成错误，策略部署在安全 zone 中的 400 + 接口失败

版本 6.4.0.5 已解决的问题

表 *38:* 版本 *6.4.0.5* 已解决的问题

漏洞 ID	标题
CSCvh73096	在 ISE 可用时，从 ISE 读取 sAMAccountUserName

漏洞 ID	标题
CSCvp95663	IPS 事件缺少元数据的 InlineResult“将被阻止”
CSCvp97061	URL 过滤将所有 URL 显示为“未分类”
CSCvq32678	升级异常导致策略部署失败：映射文件中缺少 NGFW_UPGRADE
CSCvq32681	在 FTD 升级期间，为多个接口对内联集禁用了线路配置失败
CSCvq39083	启用 SSL 策略后，安全情报不会丢弃列入黑名单的 URL 的 HTTPS 连接
CSCvq41936	添加新用户后，必须在 FMC UI 中禁用并重新启用 SNMP
CSCvq44594	使用消息 "未知 HPQ 规则密钥" 来淹没日志
CSCvq46804	无法使用包含大小写 RADIUS 的 AD 用户名登录
CSCvq46918	升级后删除的 SNMPv3 用户
CSCvq54242	SSL 策略中的 "源网络中存在空组" （Warrning）
CSCvq56138	如果密码中包含空格，则用户登录会失败到 LDAP 用户的 FMC GUI 中
CSCvq56462	文件策略未检查某些恶意软件文档（.doc）和 Adobe flash （swf）文件。
CSCvq65092	与设备相关的 REST API 调用缓慢
CSCvq66217	FMT |MTU 值不在允许的范围内
CSCvr23858	由于 domain_snapshot_timeout （20m），从 FMC 到 FTD 的策略部署失败

版本 6.4.0.4 已解决的问题

表 *39:* 版本 *6.4.0.4* 已解决的问题

漏洞 ID	标题
CSCvf83160	线程名称的回溯：DATAPATH-2-1785
CSCvg29468	对于一般微引擎故障，为误报
CSCvh13869	ASA IKEv2 无法打开 aaa 会话：已达到会话限制 [2048]
CSCvj61580	ASA 线程回溯：DATAPATH-8-2035
CSCvk22322	从主用设备（inc cachefs_umount）同步配置时，ASA 生成回溯（监视程序超时）
CSCvk26612	"默认密钥环的证书无效，原因：已过期" 运行状况警报

漏洞 ID	标题
CSCvk29685	ASA 上的 DATAPATH 的回溯
CSCvm36362	路由跟踪失败
CSCvm39901	ENH： ASA - 在多模式下支持 4 台以上服务器。
CSCvm40288	高可用性链路上的端口通道问题
CSCvm64400	IKEv2: IKEv2-PROTO-2：未能从平台分配 PSH
CSCvm68648	在 Firepower 软件上查看 CVE-2016-8858 （OpenSSH）
CSCvn76875	正常重启 BGP 不会间歇性工作
CSCvn78593	控制平面 ACL 在 FTD 上无法正常工作
CSCvn78870	ASA 多情景生成回溯，由于分配接口超出范围命令而重新加载
CSCvn99658	FXOS lacp 相关的日志 pktmgr.out 和 lacp.out 变得过大
CSCvo03700	当在从属设备上启用集群时，ASA 可能会在线程记录器中生成回溯
CSCvo14961	ASA 在等待 "dns_cache_timer" 进程完成时可能会生成回溯和重新加载。
CSCvo29989	Cisco FirePower 威胁防御信息泄露漏洞
CSCvo31695	释放内存块时，在线程名称 DATAPATH-0-1668 中回溯
CSCvo45755	ASA SCP 转移到 box 延迟中间传输
CSCvo47390	线程 SSH 中的 ASA 回溯
CSCvo48838	Lina 未正确报告过长的配置行错误
CSCvo51265	SCP 大文件传输到盒子中会导致生成回溯
CSCvo55809	ASA 应用在少量映像上停滞安装状态
CSCvo65741	ASA：发生故障切换后，在路由表上清除 BGP 路由，并且更改了 bgp 路由
CSCvo66534	引用数据路径作为受影响的线程时回溯和重新加载
CSCvo68184	仅辅助 FTD 上的诊断 I/F 管理消失
CSCvo74350	ASA 可能生成回溯并重新加载。可能与 WebVPN 流量相关
CSCvo74625	6.4.0 - 当管理网关配置为数据接口时，IPv6 路由不适用于 WM 和 KP
CSCvo78789	思科自适应安全设备智能隧道漏洞
CSCvo80501	执行手动故障切换时，备用防火墙使用生成回溯重新加载

漏洞 ID	标题
CSCvo87930	使用 w3m 的 ipv6 的 HTTP 失败
CSCvo87985	ASA 以纯文本形式发送 "copy" 命令的密码
CSCvo90153	ASA 无法通过 https 对具有特殊字符的用户进行身份验证
CSCvo90998	不应将 LACPDUs 发送到内联集接口的 snort
CSCvo97979	重启后，接口配置中的 delay 命令会被修改
CSCvp12052	ASA 可能生成回溯并重新加载。怀疑 webvpn 相关
CSCvp14674	ASAv Azure：当 ASAv 故障切换时，路由表 BGP 传播设置重置
CSCvp19910	无法处理报头 TEID：0 的 gtpv1 标识请求消息
CSCvp19998	ASA 丢弃 GTPV1 SGSN Context 请求消息，标题为 TEID：0
CSCvp23137	ASA/FTD 会为缺失 SSD 2 生成系统日志：/dev/sdb 存在。状态：不可操作。
CSCvp30447	在入侵策略上禁用全局规则阈值时，系统日志警报不会发送到服务器
CSCvp32617	升级到 9.6.2 之后，“已建立的 tcp”无法运行
CSCvp35141	ASA 为 POST 请求发送无效的重定向响应
CSCvp35384	IKEv2 RA 通用客户端-阻塞的外发 asp 表条目-使用过时 SPI 加密的流量
CSCvp38530	无法配置超过 100 aaa-已达到服务器组限制
CSCvp42275	适用于 WR8 的 CCM 基础设施更新
CSCvp43066	如果配置为 DHCP 中继，则由 ASA 从 DHCP 服务器发送的 DHCP NACK 静默丢弃
CSCvp46341	故障时（FTW）端口无法在 2100 Firepower 平台上恢复。
CSCvp49576	FTD 集群生成回溯在其他设备离开集群时遇到
CSCvp54261	SFR 模块/7000/8000 设备的审核系统日志使用 TCP 而非 UDP 进行系统日志通信
CSCvp55880	故障关闭 FTD 通过 Snort 进程传递数据包
CSCvp59864	IP 地址滞留在本地池中，并显示为 "正在使用"，即使 AnyConnect 客户端断开连接
CSCvp63068	线程名称： CP DP SFR 事件处理生成回溯
CSCvp65134	ASA 不响应 BVI 接口上的 DHCP 请求数据包

漏洞 ID	标题
CSCvp70020	重新启动后，"ssh 版本 1 2" 已添加到运行配置
CSCvp70699	在重新启动 Firepower 机箱后，ASA 故障切换分裂大脑（两台设备处于活动状态）
CSCvp71180	使用 RADIUS 的 MCA + AAA + OTP 无法在质询中发送 aggauth 句柄
CSCvp72412	系统日志消息中的时间 zone
CSCvp73555	网络发现部署后，rna_networks 为空。
CSCvp79157	在运行多个设备的同时部署时，FTD/Firepower 策略部署会失败。
CSCvp80775	客户端 WebVPN 重写程序中不支持的运行时 JavaScript 异常处理
CSCvp83687	Firepower：网络文件轨迹图未加载
CSCvp84546	ASA 9.9.2 无客户端 WebVPN-HTML 实体在处理 HTML 时被错误地解码
CSCvq00005	LINA 线程上的 FTD 生成回溯和重新加载
CSCvq06790	Snort 在系列 3 设备上处理转储核心，内存损坏
CSCvq08684	由于特殊字符 & 编码，策略部署失败
CSCvq08767	Snort 验证中的部署失败-SMTP：无法分配 SMTP mime cisco-enhanced-mempool-mib
CSCvq11513	回溯： "saml identity-provider" 命令导致多个上下文 ASA 崩溃
CSCvq12411	尽管已修复 CSCvj98964，ASA 仍有可能因 SCTP 流量而回溯
CSCvq13442	删除情景时，ssh 密钥交换将全局变为默认值！
CSCvq21607	在通过 CLI 恢复备份时，将删除 "ssl 信任点" 命令
CSCvq24134	ASA IKEv2-ASA 在启动第 2 阶段密钥更新后发送额外的删除消息
CSCvq25626	当日志记录到缓冲区时，ASAv 上的监视器
CSCvq25912	关联规则警报在 6.4.0 中不起作用
CSCvq26794	不明原因的 GTP 响应消息将被丢弃，错误消息 TID 为 0
CSCvq27010	当 ASA-SFR 数据平面通信摆动时观察到内存泄漏
CSCvq37902	TID 无法将源添加为 URL 平面文件
CSCvq39828	升级到 6.4.0 之后，packet_log 表中插入 SFDC 崩溃
CSCvq50314	未通过系统日志导出失败的 SSH 登录尝试

漏洞 ID	标题
CSCvq57710	Firepower 主检测引擎进程可能在管理器升级后终止
CSCvq61651	FMC 上的 URL DB 下载失败警报;新 URL 数据库更新在 FMC/FDM 上不会生效
CSCvq86553	更新到 6.4.0 后，流量未匹配预期的 ACP 规则
CSCvq87068	删除的 URL 对象不会从 ngfw.rules 中删除。
CSCvq97301	从 6.4.0-102 > 6.4.0.4-31 升级 5525 时，FMC GUI 中出现致命错误消息，但升级完成

版本 6.4.0.3 已解决的问题

表 *40:* 版本 *6.4.0.3* 已解决的问题

漏洞 ID	标题
CSCve24102	GUI 应允许每个 DHCP 池最多 256 个地址
CSCvp10132	由于超出 TCP 连接限制错误，AnyConnect 连接失败
CSCvp66559	由于解析大 xml 响应时出现异常，在 FTD HA 上部署失败
CSCvp25570	如果在同一向导流中编辑了策略组属性和 FQDN，则无法创建 RAVPN Conn-Profile
CSCvp32659	FDM-HA 构造在升级到 6.3.0.3-69 后失败
CSCvp56910	帮助页面始终以英文显示
CSCvo68448	在 5585 平台上重新加载 ASA 模块后，ASA 报告 SFR 模块为“无响应”
CSCvp01542	FMC 6.3 多租户/域 LDAPS 用户/组下载失败，因为证书位置
CSCvp23579	每次加载“网络文件轨迹”页面大约需要 90 秒
CSCvp33052	由于未处理的资源暂时不可用，Firepower 8000 接口可能已摆动
CSCvp37779	FTD show tech from 故障排除文件不完整
CSCvp46173	子域中的接口组或接口 zone 中的更改覆盖全局域。
CSCvp58028	nfm_exceptiond 的 natd 线程大约占用 90% 至 100% 的 CPU 时间
CSCvp72601	FMC UI： VPN 中心和辐射型拓扑加载缓慢
CSCvp72770	从 FMC 到 vFTD 的 BCDB 文件副本被截断，vFTD 在 Azure 平台上运行。

漏洞 ID	标题
CSCvp75594	在运行 FTD 的 ASA5500-X 中升级到 6.4 之后部署失败
CSCvp94588	HTTP 黑名单 - 黑名单规则在未分配和从 FMC 中部署时，不会从传感器中删除
CSCvp97799	6.5.0-1148 在 SSL 极化导出期间使用 CC 模式和 openSSL 调用升级之后策略部署失败
CSCvp98066	在重置 CD 上，未清除其标志 [parseFailoverReqIssued] 以防止进一步的节点加入尝试
CSCvq07914	FMC 6.4.0 - 策略部署失败，domains.conf 中存在重复的域条目
CSCvq14586	如果数据库更新失败，600_schema/100_update_database. sh 应返回错误。

版本 6.4.0.2 已解决的问题

表 *41:* 版本 *6.4.0.2* 已解决的问题

漏洞 ID	漏洞 ID
CSCvi63474	升级到 6.2.2 后，无法通过 ASDM 编辑 SFR 模块的系统策略
CSCvk06386	尽管存在文件策略判定，系统仍允许 FTD 文件通过多个预先存在的连接
CSCvk14242	FTD 中的 sfstunnel 进程正在保存已删除的大型云数据库文件
CSCvm70274	tcp 代理：DATAPATH 上的 ASA 回溯
CSCvn07452	将内联集从分流切换到内联时，712x 设备变得不稳定
CSCvn12381	4140 多实例未正确实现负载均衡（含 4 个实例）
CSCvn34246	加载 AC 策略编辑器需要太长时间，需要加载指示器
CSCvn45750	在部署到 3D 设备 -GUI/SYSLOG 时，FMC 审计日志仅将管理员和系统显示为所有者
CSCvn57284	FTD 上的 EC 曲线 x25519 不受支持
CSCvn74112	FTDv 没有关于 vmxnet3 和 ixgbevf 混合接口初始启动的配置
CSCvn75368	FPR 平台 IPsec VPN 断断续续
CSCvn86777	在具有低内存的 FTD 上部署将导致接口名称被删除
CSCvo02097	将 ASA 群集升级到 9.10.1.7 会导致回溯
CSCvo17775	添加新子接口并启用“mac-address auto”时，EIGRP 中断

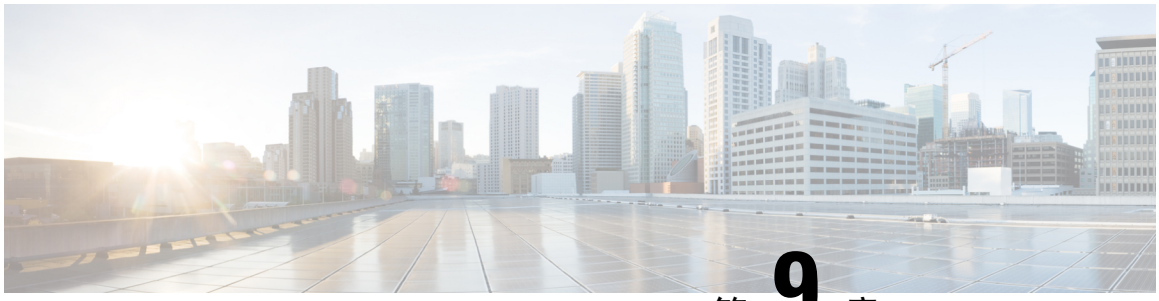
漏洞 ID	漏洞 ID
CSCvo23366	自适应剖析配置文件损坏导致部署失败
CSCvo24145	firewall_rule_cache 表过大导致 ids_event_alerter 内存使用率高
CSCvo33348	非标准端口上的 Mysql 流量未正确分类
CSCvo33851	如果 ngfw.properties 为空，ngfwManager 不正确启动
CSCvo41572	FMC 显示数据包计数为 0 的连接事件
CSCvo45209	FTD-CLUSTER：在群集中添加新单元可能导致流量下降
CSCvo47562	由于在重新生成密钥期间未释放 PKI 句柄，VPN 会话失败
CSCvo50168	审核日志设置失败导致无法编辑系统设置
CSCvo56836	可扩展性：UMS 具有 500 多个设备，导致 UI 挂起，尤其是在部署期间
CSCvo58847	增强功能以解决由于隧道替换方案而导致的 IKE CPU 使用率高的问题
CSCvo60580	发出 "show inventory" 命令时 ASA 追溯并重新加载
CSCvo60862	编辑访问控制策略时出现内部错误
CSCvo62031	运行 IKE 调试时 ASA 回溯并重新加载
CSCvo62060	当 FMC 管理大量设备时，不发送遥测
CSCvo66920	增强功能：为重复远程代理添加计数器
CSCvo72179	对于 SMB，远程存储配置应允许使用点 (.) 配置版本字符串
CSCvo72462	不解密规则会导致流量中断。
CSCvo74745	生成大量连续 URL 查找 (>30M) 后的云代理核心
CSCvo88188	具有 App-ID 条件的 SSL 规则可能会限制解密功能
CSCvo88306	当您有重复的规则时，NAT 规则可能会以错误的顺序应用
CSCvo89224	FMC 在获取用于部署的设备列表 10 分钟后超时
CSCvo90550	Firepower 建议不启用是 GID 3 的 IPS 规则
CSCvo90805	Cisco Firepower 管理中心 RSS 跨站脚本漏洞
CSCvp03498	FMC 上用户身份功能的运行状况监控选项。
CSCvp07143	DTLS 1.2 和 AnyConnect oMTU
CSCvp14576	ENH - 在 FTD 上配置端口块分配的选项

漏洞 ID	漏洞 ID
CSCvp18878	ASA：在 Datapath 中回溯看门狗信息
CSCvp19549	FTD lina 核心采用进程名称：cli_xml_server
CSCvp21837	允许 FTD 直接执行 URL 查找，而无需通过 FMC
CSCvp24728	FTD 添加的随机 SGT 标签
CSCvp24787	(snort) 通过 HTTPS 时未检测到文件（SSL 重新签名）
CSCvp25583	当我们通过 FMC GUI 将 OSPF 重新分配到 BGP 时，FTD 会自动设置公制 0。
CSCvp27263	适用于 6.5.0 之前的思科 Firepower 管理中心的多个 ClamAV 漏洞
CSCvp29692	从失败的策略部署回滚后，FIPS 模式被禁用
CSCvp35359	如果显式 UPN 与隐式 UPN 不匹配，则 FMC-ISE 集成不起作用
CSCvp36425	线程名称 octnic_hm_thread 中 ASA 5506/5508/5516 回溯
CSCvp43474	REST API 查询 /api/fmc_config/v1/domain/UUID/devices/devicerecords 失败
CSCvp43536	在升级的 FMC 设备上，即使部署成功，FXOS 设备也显示为脏污。
CSCvp54634	使用模糊的 DND 时，匹配的是错误的规则
CSCvp58310	集成 pxgrid 功能，连接挂起，curl 挂起问题
CSCvp75098	部署 Flex Config 策略时出现误导性部署警告消息
CSCvp78197	策略部署删除并加回 ospf 邻居
CSCvp81967	当有超过 500 个受管设备时，在 FMC 上加载设备管理页面的速度很慢
CSCvp82945	NAT 策略应用失败，错误重复
CSCvp96934	确保具有重复 NAT 的错误消息被清除且可操作
CSCvq07573	升级到 6.4 之后，FMC 全局预部署阶段需要更长时间
CSCvq09209	策略部署失败，错误 snort 验证失败（为 memcap 指定了错误的值）
CSCvq34224	Firepower 主检测引擎进程在管理器升级后终止

版本 6.4.0.1 已解决的问题

表 *42:* 版本 *6.4.0.1* 已解决的问题

漏洞 ID	标题
CSCvh51853	会话预处理器丢弃随机数据包
CSCvp59960	网络发现不适用于包含文字的网络组 - 用户或思科创建。



第 9 章

已知问题

对于已知的问题，请参阅：

- 搜索已知问题 ， 第 71 页

搜索已知问题

如果您有支持合同，可以通过思科漏洞搜索工具获取 Firepower 产品最新的未解决错误列表。这些常规查询显示尚未解决的、与运行 版本 6.4.0.x 修补程序的 Firepower 产品相关的问题：

- Firepower 管理中心
- Firepower 管理中心虚拟
- 具备 FirePOWER 服务的 ASA
- NGIPSv

可以将搜索范围限制为影响特定 Firepower 平台和版本的错误。还可以按错误 ID 搜索或者搜索特定关键字。

第 10 章

获取帮助

感谢选择 Firepower。

- 网上资源，第 73 页
- 联系思科，第 73 页

网上资源

思科提供在线资源来下载文档/软件/工具、查询错误以及创建服务请求。这些资源可用于安装和配置 Firepower 软件以及解决和消除技术问题。

- 思科支持和下载站点：https://www.cisco.com/c/en/us/support/index.html
- 思科漏洞搜索工具：https://tools.cisco.com/bugsearch/
- 思科通知服务：https://www.cisco.com/cisco/support/notifications.html

使用思科支持和下载站点上的大多数工具时，需要 Cisco.com 用户 ID 和密码。

联系思科

如果使用上面列出的在线资源无法解决问题，请联系思科 TAC：

- 邮箱思科 TAC：tac@cisco.com
- 致电思科 TAC（北美）：1.408.526.7209 或 1.800.553.2447
- 致电思科 TAC（全球）：思科全球支持联系人