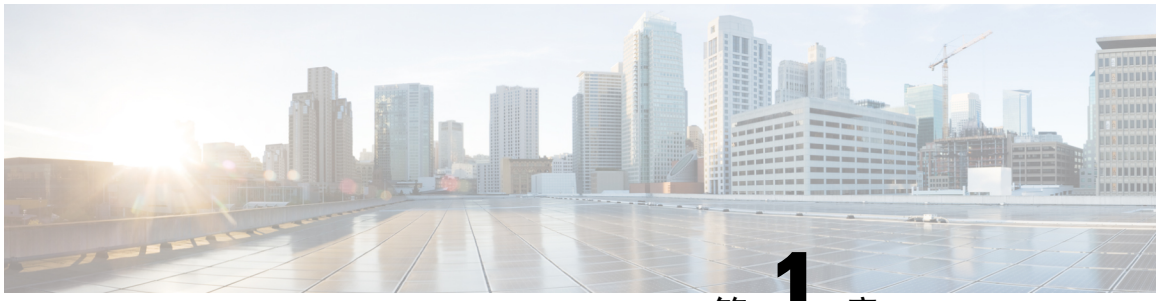
思科 Firepower 发行说明，版本 6.5.0

首次发布日期: 2019 年 9 月 26 日

上次修改日期: 2019 年 10 月 11 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 6.5.0

感谢选择 Firepower。

关于发行说明

发行说明提供了关于版本 6.5.0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：

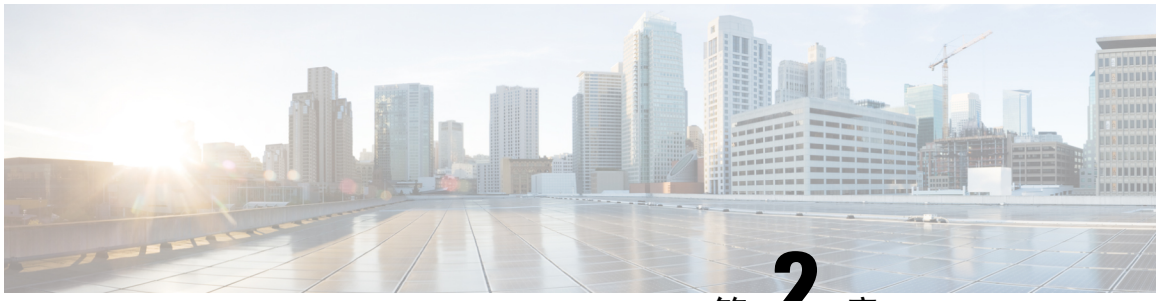
发布日期

有关随版本 6.5.0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 77 页。

表 *1:* 版本 *6.5.0* 发行日期

内部版本号	日期	平台：升级	平台：重新映像
120	2019-10-08	FMC/FMCv	-
115	2019-09-26	所有设备	全部



第 2 章

兼容性

本章提供 Firepower 版本 6.5.0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

物理和虚拟平台都支持 版本 6.5.0Firepower 管理中心 软件；有关支持的 FMCv 实例，请参阅《思科 Firepower Management Center Virtual 快速入门指南》。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

Firepower Management Center Virtual：

- VMware vSphere/VMware ESXi 6.0、6.5 或 6.7 上的 FMCv 和 FMCv 300
- 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 6.5.0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 6.5.0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 *6.5.0* 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、1140、1150 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	FDM	FXOS 2.7.1.92 + 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 FXOS 发行说明 [2.7(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 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） 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。
FTDv	FTD	FDM（AWS 除外）	以下项中的任一个： • VMware vSphere/VMware ESXi 6.0、6.5 或 6.7 • 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、6.5 或 6.7 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。

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 *6.5.0* 管理器-设备的兼容性

Firepower 管理中心		
版本 6.5.0 FMC	可以管理	版本 6.2.3 至 6.5.0.x 的设备
版本 6.5.0 的设备	要求	版本 6.5.0 FMC
Firepower 设备管理器		
版本 6.5.0 FDM	可以管理	一个 FTD 设备
ASDM		
版本 7.13.1 ASDM	可以管理	6.5.0.x 及更低版本的 ASA FirePOWER 模块
版本 6.5.0 ASA FirePOWER 模块	要求	版本 7.13.1 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。

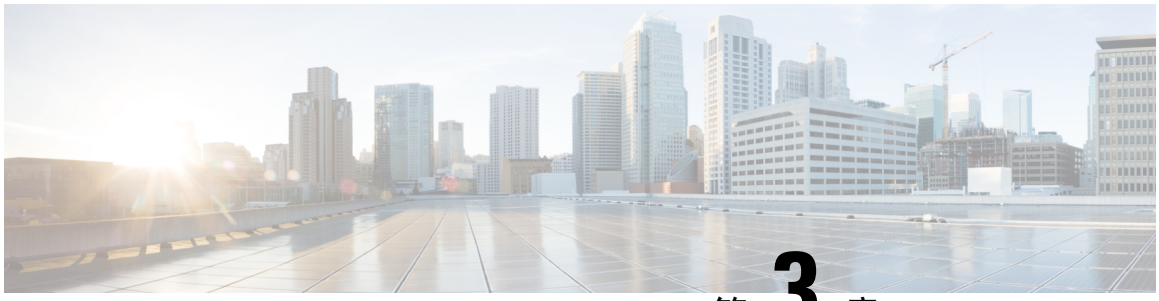
浏览器扩展兼容性

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
Firepower 设备管理器	1024 x 768
ASDM 管理着 ASA FirePOWER 模块	1024 x 768
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 6.5.0包括：

新功能

以下主题列示了 Firepower 版本 6.5.0中可用的新功能。如果您的升级路径跳过了一个或多个主版本，请参阅思科 Firepower 发行说明查看过去的新功能列表。

Firepower 管理中心/版本 6.5.0 中的新增功能

下表列出了在使用 Firepower 管理中心进行配置时 Firepower 版本 6.5.0 中可用的新功能：

表 *6:* 版本 *6.5.0* 新增功能： *FMC* 部署

特性	说明
硬件和虚拟硬件	
Firepower 1150 上的 FTD	我们推出了 Firepower 1150。
Azure 上的更大 FTDv 实例	Microsoft Azure 上的 Firepower 威胁防御虚拟现在支持更大的实例： D4_v2 和 D5_v2。
VMware 上的 FMCv 300	我们推出了 FMCv 300，一个更大的 适用于 VMware 的 Firepower Management Center Virtual。与其他 FMCv 实例的 25 台设备相比，它最多可以管理 300 台设备。 您可以使用 FMC 模型迁移功能从功能较低的平台切换到 FMCv 300。

特性	说明
VMware vSphere/VMware ESXi 6.7 支持	现在，您可以在 VMware vSphere/VMware ESXi 6.7 上部署 FMCv、FTDv 和 NGIPSv 虚拟设备。
Firepower 威胁防御	
Firepower 1010 硬件交换机支持	现在，Firepower 1010 支持将各以太网接口设置为交换机端口或防火墙接口。 新增/修改的屏幕： • **设备 > 设备管理 > 接口** • **设备 > 设备管理 > 接口 > 编辑物理接口** • **设备 > 设备管理 > 接口 > 添加 VLAN 接口** 支持的平台：Firepower 1010
Firepower 1010 PoE + 支持以太网 1/7 和以太网 1/8	现在，Firepower 1010 支持以太网接口 1/7 和 1/8 上的增强型以太网供电+ (PoE+)。 新增/修改的屏幕：**设备 > 设备管理 > 接口 > 编辑物理接口 > PoE** 支持的平台：Firepower 1010
对运营商级 NAT 的改进。	对于运营商级或大规模 PAT，您可以为每台主机分配端口块，而无需通过 NAT 一次分配一个端口转换（请参阅 RFC 6888）。 新增/修改的屏幕： **设备** > **NAT** >添加/编辑 FTD NAT 策略>添加/编辑 NAT 规则> **PAT 池**选项卡> **块分配**选项 支持的平台：任何FTD设备

特性	说明
Firepower 4100/9300 上的多个容器实例的 TLS 加密加速	现在，在 Firepower 4100/9300 机箱上的多个容器实例（最多16个）上支持 TLS 加密加速。以前，每个模块/安全引擎只能为一个容器实例启用 TLS 加密加速。 新实例默认启用此功能。但是，升级不会在现有实例上启用加速。相反，使用 **create hw-crypto**和 **scope hw-crypto** CLI 命令。有关详细信息，请参阅思科 Firepower 4100/9300 FXOS 命令参考。 新的 FXOS CLI 命令： • **create hw-crypto** • **delete hw-crypto** • **scope hw-crypto** • **show hw-crypto** 删除的 FXOS CLI 命令： • **show hwCrypto**（已替换为 **show hw-crypto**） • **config hwCrypto** 删除的 FTD CLI 命令： • **show crypto accelerator status** 支持的平台：Firepower 4100/9300
访问控制和事件分析	
访问控制规则筛选	现在，您可以根据搜索条件过滤访问控制规则。 新增/修改的屏幕：**策略 > 访问控制 > 访问控制** >添加/编辑策略> 过滤器按钮（' 仅显示符合过滤器条件的规则 '） 支持的平台： FMC
争议 URL 类别或信誉	您现在可以对 URL 的类别或信誉进行争议。 新增/修改的屏幕： • **分析 > 连接事件** >右键点击类别或信誉> **争议**。 • **分析 > 高级 > URL** > 搜索 URL > **争议**按钮 • **系统 > 集成 > 云服务 > 争议**链接 支持的平台： FMC

特性	说明
使用基于目标的安全组标记（SGT）进行用户控制	现在，您可以在访问控制规则中将 ISE SGT 标记用于源匹配条件和目标匹配条件。SGT 标记是 ISE 获取的标签到主机/网络映射。 新建连接事件字段： • 目标 SGT（系统日志：DestinationSecurityGroupTag）：用于连接响应方的 SGT 属性。 重命名连接事件字段： • 目标 SGT（系统日志：SourceSecurityGroupTag）：用于连接发起方的 SGT 属性。替换安全组标记（系统日志：SecurityGroup）。 新增/修改的屏幕：**系统 > 集成 > 身份源 > 身份服务引擎 >**订阅**会话目录主题**和**SXP 主题**选项 支持的平台：任意
Cisco Firepower 用户代理版本 2.5 的集成	我们已发布 Cisco Firepower 用户代理版本 2.5，您可以将其与 Firepower 版本 6.4.0 和 6.5.0 集成。 **注释** 尽管版本 6.5.0 支持它，但我们计划使用思科 Firepower 用户代理软件和身份源结束对用户控制的支持。强烈建议您立即切换到思科身份服务引擎/被动身份连接器 (ISE/ISE-PIC)。这同时使得您可以利用用户代理不可用的功能。有关详细信息，请参阅思科 Firepower 管理中心配置指南页面对应于您的版本的《思科 *Firepower* 用户代理配置指南》。 新增/修改的 FMC CLI 命令： **configure user-agent** 支持的平台： FMC
“数据包配置文件”CLI 命令	现在，您可以使用 FTD CLI 获取有关设备如何处理网络流量的统计信息。也就是说，预过滤器策略快速路径的数据包数量、作为大型流进行了卸载、完全通过访问控制（Snort）进行评估等。 新增的 FTD CLI 命令： • **asp packet-profile** • **no asp packet-profile** • **show asp packet-profile** • **clear asp packet-profile** 支持的平台： FTD

特性	说明
思科威胁响应的其他事件类型 (CTR)	Firepower 现在可以将文件和恶意软件事件以及高优先级连接事件（即：与入侵、文件、恶意软件和安全情报事件相关的事件）发送到 CTR。 **注释** 对这些事件类型的支持在云中尚不可用，但很快就会出现。 新增/经修改的屏幕：**系统 > 集成 > 云服务**。 支持的平台：FTD（通过系统日志或直接集成）和经典（通过系统日志）设备
管理	
适用于 ISA 3000 设备的精确时间协议 (PTP) 配置。	可以使用 FlexConfig 在 ISA 3000 设备上配置精确时间协议 (PTP)。PTP 是一种时间同步协议，用于在基于数据包的网络中同步各种设备的时钟。该协议专为工业、网络测量和控制系统而设计。 现在，我们允许在 FlexConfig 对象中包含 **ptp**（接口模式）命令和全局命令 **ptp mode e2etransparent** 和 **ptp domain** 新增/经修改的命令： **show ptp** 支持的平台：ISA 3000 和 FTD
配置更多域（多租户）	在实施多租户（对托管设备、配置和事件进行分段用户访问权限）时，最多可以在一个顶级全局域下以两个或三个级别创建 100 个子域。以前的最大值为 50 个域。 支持的平台： FMC
ISE 连接状态监视器增强功能	ISE 连接状态监控运行状况模块现在会提醒您 TrustSec SXP（SGT 交换协议）订用状态的问题。 支持的平台： FMC
区域云	如果您使用 Cisco 威胁响应集成、Cisco 支持诊断或 Cisco 成功网络功能，您现在可以选择区域云。默认情况下，升级会将您分配给美国（北美）区域。 新增/经修改的屏幕：**系统 > 集成 > 云服务**。 支持的平台：FMC、FTD

特性	说明
思科支持诊断结果	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。 在升级和重映像期间，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。 目前，Cisco 支持诊断支持仅限于选择平台。 新增/修改的屏幕： • **系统 > 智能许可证** • **系统 > 智能许可证 > 注册** 支持的平台：FMC 和托管的 Firepower 4100/9300
FMC 模型迁移	现在，您可以使用“备份和恢复”功能在 FMC 之间（即使是不同的型号）迁移配置和事件。这使得更换FMC（由于不断增长的组织、从物理实施迁移到虚拟实施、硬件更新等技术或业务等方面的原因）变得更容易。 一般情况下，可以从低端迁移到更高端的FMC，但不能反向。不支持从 KVM 和 Microsoft Azure 迁移。您还必须在 Cisco Smart Software Manager (CSSM) 中取消注册并重新注册。 有关详细信息（包括支持的目标和目标型号），请参阅《Firepower 管理中心型号迁移指南》。 支持的平台： FMC
增强安全性	
在基于 FXOS 的 FTD 设备上安全清除设备组件	现在，您可以使用 FXOS CLI 安全地擦除指定的设备组件。 新的 FXOS CLI 命令： **erase secure** 支持的平台：Firepower 1000/2000 和 Firepower 4100/9300 FTD 系列
在初始设置期间FMC，管理员帐户的密码要求更严格	FMC初始设置现在要求您为管理员帐户选择 "强" 密码。设置过程会将此强密码应用于 FMC Web 界面和 CLI 管理员帐户。 **注释** 升级到版本6.5.0+不会强制您将弱密码更改为强密码。除了在物理FMC上使用LOM用户（这确实包括管理员用户），您不会被禁止选择新的弱密码。但是，我们建议所有 Firepower 用户帐户（尤其是具有管理员访问权限的用户帐户）具有强密码。 支持的平台： FMC

特性	说明
并发用户会话限制	现在，您可以将可以登录的用户数量限制FMC在同一时间。您可以为具有只读角色、读/写角色或两者的用户限制并发会话。请注意，CLI 用户受读/写设置的限制。 新增/修改的屏幕：**系统 > 配置 > 用户配置 > 最大并发会话数允许**的选项 支持的平台： FMC
已通过身份验证的 NTP 服务器	现在，您可以使用 SHA1 或 MD5 对称密钥身份验证配置 FMC 与 NTP 服务器之间的安全通信。对于系统安全，我们建议使用此功能。 新增/经修改的屏幕：**系统 > 配置 > 时间同步** 支持的平台： FMC
可用性	
改进了初始配置体验	在新的和FMC重新映像上，向导会替换之前的初始设置过程。如果使用 GUI 向导，则在初始设置完成时，FMC 将显示 "设备管理" 页面，以便您可以立即开始许可 并设置部署。 设置过程还会自动安排以下各项： • 软件下载。系统会创建每周计划任务，以下载（但不安装）软件补丁和适用于您的部署的公开可用的修复程序。 • FMC 仅配置备份。系统会创建每周计划的任务，以备份 FMC 配置并将其存储在本地。 • GeoDB 更新系统启用每周地理位置数据库更新。 这些任务计划为 UTC，这意味着在本地发生时，取决于日期和您的特定位置。此外，由于任务是以 UTC 为单位进行计划的，因此它们不会针对夏令时、夏令时或您在地点可能观察到的任何季节性调整进行调整。如果受影响，则根据当地时间，计划任务会在夏天比冬季中的一个小时开始。 **注释** 我们强烈建议您查看自动计划的任务/GeoDB 更新，并根据需要进行调整。 升级FMC的不受影响。有关初始配置向导的详细信息，请参阅 FMC 型号的《入门指南》；有关计划任务的详细信息，请参阅《Firepower 管理中心配置指南》。 支持的平台： FMC

特性	说明
FMC Web 界面 Light 主题（体验）	系统默认为经典主题，但您也可以选择实验性的 "浅色" 主题。 **注释** 由于光主题是实验性的，因此您可能会看到未对齐的文本或其他 UI 元素。在某些情况下，您可能还会遇到比平时慢的响应时间。如果遇到阻止您使用页面或功能的问题，请切换回经典主题。虽然我们无法对每个人作出响应，但我们也欢迎您提供反馈，请使用 "用户首选项" 页面上的反馈链接，或联系我们的 fmc-light-theme-feedback@cisco.com。 新增/修改的屏幕：**用户首选项**, 从您用户名下的下拉列表中 支持的平台： FMC
查看对象的可用性增强	我们已增强了网络、端口、VLAN 和 URL 对象的 "查看对象" 功能，如下所示： • 在访问控制策略中，在配置FTD路由时，您可以右键点击对象，然后选择 "**查看对象**" 以显示有关该对象的详细信息。 • 查看有关对象的详细信息时，或者当您在对象管理器中浏览对象时，点击**查找使用情况**（）现在允许您深入了解对象组和嵌套对象。 新增/修改的屏幕： • **对象 > 对象管理**>选择支持的对象类型>**查找使用情况**（） • **策略 > 访问控制 > 访问控制** >创建或编辑策略>创建或编辑规则>选择支持的条件类型>右键点击对象> **查看对象** • **设备 > 设备管理** > 编辑 FTD 设备 > **路由器** > 右键点击受支持的对象 > **查看对象** 支持的平台： FMC
部署配置更改的可用性增强功能	我们简化了与部署配置更改相关的错误和警告的显示。现在，您可以**点击查看所有详细**信息，而不是立即详细视图，查看有关特定错误或警告的详细信息。 新增/修改的屏幕： **"请求的部署的错误和警告"** 对话框 支持的平台： FMC

特性	说明
FTD NAT 策略管理的可用性增强功能	在配置 FTD NAT 时，您现在可以执行以下操作： • 按设备查看NAT策略中的警告和错误。警告和错误标记出会对流量产生不利影响或阻碍策略部署的配置。 • 每页显示最多 1000 个 NAT 规则。默认值为 100。 新增/修改的屏幕：**设备 > NAT >**创建或编辑 FTD NAT 策略**> 显示每个页面**的警告和规则选项 支持的平台： FTD
FMC REST API	
新的 REST API 功能	添加了以下 REST API 对象以支持版本 6.5.0 的功能： • cloudregions：区域云 添加了以下 REST API 对象以支持较旧的功能： • 类别：访问控制规则的类别 • 域、inheritancesettings：域和策略继承 • prefilterpolicies，prefilterrules，tunneltags：预过滤器策略 • Vlan界面： VLAN 接口 支持的平台： FMC

Firepower 设备管理器/FTD6.5.0 版本中的新增功能

发布日期：2019 年 9 月 26 日

下表列出了在使用 Firepower 设备管理器进行配置时 FTD 6.5.0 中可用的新功能：

特性	说明
Firepower 4100/9300 的 FDM 支持。	现在，您可以使用 FDM 在 Firepower 4100/9300 上配置 Firepower 威胁防御。仅支持本地实例；不支持容器实例。
适用于 Microsoft Azure 云的 Firepower Threat Defense Virtual FDM 支持。	可以使用 Firepower 设备管理器在适用于 Microsoft Azure 云的 Firepower Threat Defense Virtual 上配置 Firepower 威胁防御。
支持 Firepower 1150。	我们推出了用于 Firepower 1150 的 FTD。

特性	说明
Firepower 1010 硬件交换机支持，PoE+ 支持。	Firepower 1010 支持将各以太网接口设置为交换机端口或常规防火墙接口。将各交换机端口分配给 VLAN 接口。Firepower 1010 还支持以太网接口 1/7 和 1/8 上的增强型以太网供电+ (PoE+)。 现在，默认配置将 Ethernet1/1 设置为外部，将 Ethernet1/2 到 1/8 设置为内部 VLAN1 接口上的交换机端口。升级至版本 6.5 将保留现有的接口配置。
接口扫描和替换。	接口扫描会检测机箱上的任何已添加、已删除或已恢复接口。还可以将旧接口替换为配置中的新接口，使接口无缝更改。
系统将显示经过改进的界面。	**设备** > **接口**页面已重新组织。物理接口、桥接组、EtherChannel 和 VLAN 现有单独的选项卡。对于任何给定的设备型号，仅显示与该型号相关的那些选项卡。例如，VLAN 选项卡仅适用于 Firepower 1010 型号。此外，列表提供有关各接口配置和使用的更多详细信息。
ISA 3000 新的默认配置。	ISA 3000 默认配置已更改如下： • 所有接口均是 BVI1 中的桥接组成员，未命名，因此不参与路由 • GigabitEthernet1/1 和 1/3 是外部接口，GigabitEthernet1/2 和 1/4 是内部接口 • 如果可用，则启用各内部/外部对的硬件旁路 • 允许从内部到外部以及从外部到内部的的所有流量 升级至版本 6.5 将保留现有的接口配置。
对 ASA 5515-X 的支持终止。最新支持版本为 FTD 6.4。	无法在 ASA 5515-X 上安装 FTD 6.5。ASA 5515-X 的最新支持版本为 FTD 6.4。
支持思科 ISA 3000 设备上访问控制规则中的通用工业协议 (CIP) 和 Modbus 应用过滤。	可以在思科 ISA 3000 设备上启用通用工业协议 (CIP) 和 Modbus 预处理器，并在访问控制规则中过滤 CIP 和 Modbus 应用。所有 CIP 应用名称均以“CIP”开头，例如 CIP Write。仅有一个应用适用于 Modbus。 要启用预处理器，必须在 CLI 会话（SSH 或控制台）进入专家模式，然后发出 **sudo /usr/local/sf/bin/enable_scada.sh {cip | modbus | both}** 命令。必须在每次部署后发出此命令，因为部署会关闭预处理器。

特性	说明
适用于 ISA 3000 设备的精确时间协议 (PTP) 配置。	可以使用 FlexConfig 在 ISA 3000 设备上配置精确时间协议 (PTP)。PTP 是一种时间同步协议，用于在基于数据包的网络中同步各种设备的时钟。该协议专为工业、网络测量和控制系统而设计。 现在，我们允许在 FlexConfig 对象中包含 **ptp** 和 **igmp**（接口模式）命令和全局命令 **ptp mode e2etransparent** 与 **ptp domain**。我们还向 FTD CLI 添加了 **show ptp** 命令。
EtherChannel（端口通道）接口。	可以配置 EtherChannel 接口，也称为端口通道。 **注释** 仅可将 FDM 中的 EtherChannel 添加至 Firepower 1000 和 2100 系列。Firepower 4100/9300 支持 EtherChannel，但必须在机箱上的 FXOS 中执行 EtherChannel 的所有硬件配置。Firepower 4100/9300 EtherChannel 显示在单个物理接口旁的 FDM **接口**页面中。 我们已更新**设备** > **接口**页面以允许创建 EtherChannel。
能够从 FDM 重新启动和关闭系统。	现在，可以从新的**重新启动/关闭**系统设置页面中重新启动或关闭系统。以前，需要通过 CLI 控制台在 FDM 中或从 SSH 或控制台会话发出 **reboot** 和 **shutdown** 命令。要使用这些命令，必须具有管理员权限。
在 FDM CLI 控制台中支持 **failover** 命令。	现在，可以通过 FDM CLI 控制台发出 **failover** 命令。
用于静态路由的服务级别协议 (SLA) 监控器。	配置服务级别协议 (SLA) 监控对象，以与静态路由配合使用。通过使用 SLA 监控，您可以跟踪静态路由的运行状况，并自动使用新路由替换故障路由。我们已将**SLA 监控器**添加至**对象**页面，并更新静态路由，以便您可以选择 SLA 监控器对象。

特性	说明
智能 CLI 和 FTD API 中的路由更改。	此版本包括对智能 CLI 和 FTD API 中的路由配置进行的一些更改。在先前版本中，存在用于 BGP 的单个智能 CLI 模板。现在，BGP（路由进程配置）和 BGP 常规设置（全局设置）有单独的模板。 在 FTD API 中，所有方法的路径均已更改，在路径中插入了“/virtualrouters”，但新的 BGP 常规设置方法除外。 • 静态路由方法路径为 /devices/default/routing/{parentId}/staticrouteentries，现在为 devices/default/routing/virtualrouters/default/staticrouteentries。 • BGP 方法分为两个新路径：/devices/default/routing/bgpgeneralsettings 和 /devices/default/routing/virtualrouters/default/bgp。 • OSPF 路径现在为 /devices/default/routing/virtualrouters/default/ospf and /devices/default/routing/virtualrouters/default/ospfinterfacesettings。 如果正在使用 FTD API 配置任何路由进程，请检查调用并在需要时更正。
新的 URL 类别和信誉数据库。	系统使用思科 Talos 团队提供的不同的 URL 数据库。新数据库的 URL 类别较老数据库有所不同。升级后，如有任何访问控制或 SSL 解密规则使用的类别不再存在，系统将使用相应的新类别作为替代。要使更改生效，请在升级后部署配置。待处理更改对话框将显示有关类别更改的详细信息。您可能想要检查URL过滤策略，以确认它们可继续提供所需的结果。 此外，在访问控制和 SSL 解密策略中以及**设备** > **系统设置** > **URL 过滤首选项**页面上的 URL 选项卡中添加了 URL 查找功能。此功能可用于检查分配给特定 URL 的类别。如果您对此类别持有异议，还可通过一个链接提交类别争议。使用这两项功能时您会转到一个外部网站，其中提供了有关此 URL 的详细信息。
安全情报对使用 IP 地址而不是主机名的 URL 请求使用 IP 地址信誉。	如果 HTTP/HTTPS 请求针对使用 IP 地址而不是主机名的 URL，则系统会在网络地址列表中查找IP地址信誉。无需在网络和URL列表中复制IP地址。这使得最终用户难以使用代理来避免安全情报信誉阻止。

特性	说明
支持向思科云发送连接和高优先级入侵、文件和恶意软件事件。	可以将事件发送至思科云服务器。各种思科云服务均可从这里访问事件。然后，可以使用这些云应用（例如思科威胁响应）来分析事件并评估设备可能遇到的威胁。启用该服务后，设备将向思科云发送连接和高优先级入侵、文件和恶意软件事件。 我们已将**设备** > **系统设置** > **云服务**上的思科威胁响应项目重命名为“将事件发送至思科云”。
思科云服务区域支持。	系统现在要求在注册智能许可时选择思科云区域。此区域用于思科防御协调器、思科威胁响应、思科成功网络和任何通过思科云的云功能。如果从先前的版本升级已注册设备，则会自动分配至US区域；如果需要更改区域，则必须注销智能许可，然后重新注册并选择新区域。 我们已在“智能许可证”页面和“初始设备设置向导”中的许可证注册流程中添加一步。您还可以在**设备** > **系统设置** > **云服务**页面上查看该区域。
FTD REST API 版本 4 (v4)。	适用于软件版本 6.5 的 FTD REST API 已升级到第 4 版。必须将 API URL 中的第 1 版/第 2 版/第 3 版替换为第 4 版。第 4 版 API 包括许多涵盖软件版本 6.5 中添加的所有功能的新资源。请重新评估所有现有的调用，因为正在使用的资源型号可能已发生更改。要打开 API Explorer，以便在其中查看这些资源，请登录 FDM，然后点击更多选项按钮 (⋮) 并选择 **API Explorer**。

特性	说明
FTD API 支持 TrustSec 安全组作为访问控制规则中的源和目的地匹配条件。	可以使用 FTD API 配置访问控制策略规则，将 TrustSec 安全组用于源或目的地流量匹配条件。系统从 ISE 下载安全组标记 (Sgt) 的列表。可以将系统配置为侦听 SXP 更新，以获取静态 SGT 到 IP 地址映射。 可以使用 GET/object/securitygrouptag 方法查看已下载标记列表，并使用 SGTDynamicObject 资源为一个或多个标记创建动态对象。这是动态对象，可在访问控制规则中用于定义基于源或目的安全组的流量匹配条件。 请注意，如果在 FDM 中编辑这些对象，则会保留对 ISE 对象或与安全组相关的访问控制规则所做的任何更改。但是，如果在 FDM 中编辑规则，则无法在该访问规则中看到安全组条件。如果使用 API 配置基于安全组的访问规则，随后使用 FDM 编辑访问控制策略中的规则时，请小心。 我们添加或修改了以下 FTD API 资源：AccessRule（SourceDynamicObjects 和 destinationDynamicObjects 属性）、IdentityServicesEngine（SubscribeToSessionDirectoryTopic 和 subscribeToSxpTopic 属性）、SecurityGroupTag 和 SGTDynamicObject。 我们在事件查看器中添加源和目的安全组标记，并将其命名为列。
使用 FTD API 导入/导出配置。	可以使用 FTD API 导出设备配置和导入配置文件。可以编辑配置文件以更改值，例如分配给接口的 IP 地址。因此，可以使用导入/导出创建用于新设备的模板，以便快速应用基线配置并更快地在线获取新设备。还可以使用导入/导出在重新映像设备后恢复配置。或者，还可以用它将一组网络对象或其他项目分发至一组设备。 我们添加了 ConfigurationImportExport 资源和方法（/action/configexport、/jobs/configexportstatus、/action/downloadconfigfile、/action/uploadconfigfile、/action/configfiles、/action/configimport 和 /jobs/configimportstatus）。
创建和选择自定义文件策略。	可以使用 FTD API 创建自定义文件策略，然后使用 FDM 选择访问控制规则的这些策略。 我们添加了以下 FTD API FileAndMalwarePolicies 资源：filepolicies、filetypes、filetypecategories、ampcloudconfig、ampservers 和 ampcloudconnections。 还删除了两个预定义策略，“阻止 Office 文档和 PDF 上传，阻止其他恶意软件”和“阻止 Office 文档上传，阻止其他恶意软件”。如果使用这些策略，则会在升级期间转换为用户定义策略，以便可以对其进行编辑。

特性	说明
采用 FTD API 的安全情报 DNS 策略配置。	可以使用 FTD API 配置安全情报 DNS 策略。此策略不会显示在 FDM 中。 我们添加了以下 SecurityIntelligence 资源：domainnamefeeds、domainnamegroups、domainnamefeedcategories 和 securityintelligencednspolicies。
使用 Duo LDAP 进行远程接入 VPN 双因素身份验证。	可以将 Duo LDAP 配置为远程接入 VPN 连接配置文件的第二个身份验证源，以使用 Duo 密码、推送通知或电话呼叫提供双因素身份验证。虽然必须使用 FTD API 创建 Duo LDAP 身份源对象，但可以使用 FDM 选择该对象作为 RA VPN 连接配置文件的身份验证源。 我们向 FTD API 添加了 duoldapidentitysources 资源和方法。
FTD API 支持用于授权远程接入 VPN 连接的 LDAP 属性映射。	可以使用自定义 LDAP 属性映射增加远程接入 VPN 的 LDAP 授权。LDAP 属性映射会将客户特定的 LDAP 属性名称和值等同于思科属性名称和值。可以使用这些映射根据 LDAP 属性值将组策略分配给用户。仅可使用 FTD API 配置这些映射；无法使用 FDM 对其进行配置。但是，如果使用 API 设置这些选项，则随后可在 FDM 中编辑 Active Directory 身份源，并保留您的设置。 我们添加或修改了以下 FTD API 对象模型：LdapAttributeMap、LdapAttributeMapping、LdapAttributeToGroupPolicyMapping、LDAPRealm、LdapToCiscoValueMapping、LdapToGroupPolicyValueMapping 和 RadiusIdentitySource。
FTD API 支持站点间 VPN 连接反向路由注入和安全关联 (SA) 生存期。	可以使用 FTD API 启用站点间 VPN 连接反向路由注入。通过反向路由注入 (RRI)，静态路由能够自动插入到受远程隧道终端保护的网络和主机的路由进程中。默认情况下，启用配置连接时添加路由的静态 RRI。动态 RRI（仅在建立安全关联 [SA] 时才会插入路由，且在 SA 断开时予以删除）会被禁用。请注意，动态 RRI 仅支持 IKEv2 连接。 还可以设置连接的安全关联 (SA) 生存期（传输的秒数或千字节数）。还可以设置无限生存期。默认生命周期是 28800 秒（八小时）和 4608000 千字节（传输一小时，每秒钟 10 兆字节）。达到生存期后，终端会协商新的安全关联和密钥。 无法使用 FDM 配置这些功能。但是，如果使用 API 设置这些选项，则随后可在 FDM 中编辑连接配置文件，并保留您的设置。 我们已将以下属性添加至 SToSConnectionProfile 资源：dynamicRRIEnabled、ipsecLifetimeInSeconds、ipsecLifetimeInKiloBytes、ipsecLifetimeUnlimited 和 rriEnabled。

特性	说明
在 IKE 策略中支持 Diffie-hellman 组 14、15 和 16。	现在，可以将 IKEv1 策略配置为使用 DH 组 14，将 IKEv2 策略配置为使用 DH 组 14、15 和 16。如果使用 IKEv1，请将所有策略升级到 DH 组 14，因为未来版本中将删除组 2 和组 5。此外，应该避免在 IKEv2 策略中使用 DH 组 24，避免在任何 IKE 版本中使用 MD5，因为未来版本中也会删除这些组。
部署更改时的性能改进。	如果添加、编辑或删除访问控制规则，则系统已得到增强，部署更改的速度比先前版本更快。 对于在用于故障切换的高可用性组中配置的系统，将已部署更改同步至备用设备的过程已得到改进，从而加快同步速度。
改进了系统控制面板上 CPU 和内存使用情况的计算方法。	计算 CPU 和内存使用情况的方法已得到改进，使得系统控制面板上显示的信息能够更准确地反映设备的实际状态。
升级至 FTD 6.5 后，系统不再提供历史报告数据。	将现有系统升级至 FTD 6.5 时，由于数据库架构发生变化，历史报告数据将不可用。因此，升级前，在控制面板中将不会看到使用情况数据。

已弃用的功能

本主题按 Firepower 版本列示了弃用的功能和平台。如果您的升级路径跳过了一个或多个主版本，必须查看中间版本的信息。

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。

版本 6.5.0 弃用的功能

这些功能在版本 6.5.0 中被弃用。

注释 尽管版本 6.5.0 支持它，但我们计划使用思科 Firepower 用户代理软件和身份源结束对用户控制的支持。强烈建议您立即切换到思科身份服务引擎/被动身份连接器 (ISE/ISE-PIC)。这同时使得您可以利用用户代理不可用的功能。有关详细信息，请参阅思科 Firepower 管理中心配置指南页面对应于您的版本的《思科 *Firepower* 用户代理配置指南》。

表 *7:* 版本 *6.5.0* 弃用的功能

特性	说明
禁用 FMC CLI 的能力	版本 6.3.0 中引入了 FMC CLI，您必须明确启用它。版本 6.5.0 会为新部署和升级的部署自动启用 FMC CLI。如果要访问 Linux 外壳程序（亦称为专家模式），必须登录到 CLI，然后使用 **expert** 命令。 注意　我们强烈建议您不要使用外壳程序访问 Firepower 设备，除非思科 TAC 让您这样做。 弃用的选项：**System > Configuration > Console Configuration > Enable CLI access** 复选框
TLS 1.0 & 1.1	要增强安全性，请执行以下操作： • 强制网络门户（主动身份验证）已删除对 TLS 1.0 的支持。 • 主机输入已删除对 TLS 1.0 和 TLS 1.1 的支持。 如果您的客户端无法与 Firepower 设备连接，我们建议您升级客户端以支持 TLS 1.2。
适用于 Firepower 4100/9300 的 TLS 加密加速 FXOS CLI 命令	作为允许在 Firepower 4100/9300 上为多个容器实例执行 TLS 加密加速的一部分，我们删除了以下 FXOS CLI 命令： • **show hwCrypto** • **config hwCrypto** 并添加了以下 FTD CLI 命令： • **show crypto accelerator status** 有关替换的详细信息，请参阅新功能文档。
思科安全数据包分析器集成	版本 6.5.0 不再支持 FMC 与思科安全数据包分析器集成。 弃用的屏幕/选项： • **System > Integration > Packet Analyzer** • **Analysis > Advanced > Packet Analyzer Queries** • 右键单击仪表板或事件查看器中的事件时 **Query Packet Analyzer**
Firepower 管理中心型号 MC750、1500 和 3500	不能在型号 MC750、MC1500 和 MC3500 上升级到或全新安装版本 6.5.0+ 的 Firepower 管理中心软件。不能利用这些 FMC 管理版本 6.5.0+ 的设备。

特性	说明
安装了 Firepower 软件的 ASA 5515-X 和 ASA 5585-X 系列设备	不能在这些型号上升级或全新安装版本 6.5.0+ 的 Firepower 软件（包括 FTD 和 ASA FirePOWER）： • ASA 5515-X • ASA 5585-X-SSP-10、-20、-40、-60 但是，您可以通过版本 6.5.0 的 FMC 管理较旧的设备（版本 6.2.3 至 6.4.x）。
Firepower 7000/8000 系列设备	不能在 Firepower 7000/8000 系列设备（包括 AMP 型号）上升级或全新安装版本 6.5.0+ 的 Firepower 软件：但是，您可以通过版本 6.5.0 的 FMC 管理较旧的设备（版本 6.2.3 至 6.4.x）。

版本 6.4.0 弃用的功能

这些功能在版本 6.4.0 中被弃用。

表 *8:* 版本 *6.4.0* 弃用的功能

特性	说明
SSL 硬件加速 FTD CLI 命令	作为 TLS 加密加速功能的一部分，我们删除了以下 FTD CLI 命令： • **system support ssl-hw-accel enable** • **system support ssl-hw-accel disable** • **system support ssl-hw-status** 有关替换的详细信息，请参阅新功能文档。

版本 6.3.0 弃用的功能

这些功能在版本 6.3.0 中被弃用。

表 *9:* 版本 *6.3.0* 弃用的功能

特性	说明
EMS 对于解密的扩展支持（仅 6.3.0）	版本 6.3.0 不再提供 EMS 扩展支持，版本 6.2.3.8/6.2.3.9 中引入了此支持。这意味着**解密 - 重新签名**及**解密 - 已知密钥** SSL 策略操作在 ClientHello 协商期间不再支持有助实现更安全通信的 EMS 扩展。EMS 扩展由 RFC 7627 定义。 在FMC部署中，此功能取决于设备版本。只要设备运行支持的版本，将 FMC 升级到版本 6.3.0 就不会造成支持中断。但是，将设备升级到版本 6.3.0 会导致支持中断。 版本 6.3.0.1 中重新提供支持。
无源和内联分流接口的解密	版本6.3.0不再支持在无源或内联分流模式下解密接口上的流量，即使 GUI 允许您这样配置也不例外。对加密流量的任何检查都必须受到限制。
VMware 5.5 托管	尚未在 VMware vSphere/VMware ESXi 5.5 上测试版本 6.3.0+ 的虚拟部署。我们建议您在升级 Firepower 软件之前升级托管环境。
安装了 Firepower 软件的 ASA 5506-X 系列和 ASA 5512-X 设备	不能在这些型号上升级或全新安装版本 6.3.0+ 的 Firepower 软件（包括 FTD和 ASA FirePOWER）： • ASA 5506-X、5506H-X、5506W-X • ASA 5512-X 但是，您可以通过版本 6.3.0 的 FMC 管理较旧的设备（版本 6.1.0 至 6.2.3.x）。

弃用的 FlexConfig 命令

某些 Firepower 威胁防御功能需使用 ASA 配置命令进行配置。从版本 6.2（FMC 部署）或版本 6.2.3（FDM 部署）开始，您可以使用 Smart CLI 或 FlexConfig 手动配置 Web 界面中不支持的各种 ASA 功能。

FTD升级可以为先前使用 FlexConfig 配置的功能添加 GUI 或 Smart CLI 支持。这可以弃用您当前使用的 FlexConfig 命令。虽然现有配置仍然有效，且仍然可以部署，但无法使用新近弃用的命令分配或创建 FlexConfig 对象。

升级后，检查 FlexConfig 策略和对象。如果有任何对象包含已被弃用的命令，则消息会指出问题所在。我们建议您重新进行配置。对新配置感到满意后，可以删除有问题的 FlexConfig 对象或命令。

使用 Firepower 管理中心的 FTD

此表列示了已弃用的 FlexConfig 对象及其关联的文本对象。有关预定义对象的完整列表，请参阅《Firepower 管理中心配置指南》。

表 *10*: 使用 *FMC* 的 *FTD*：弃用的 *FlexConfig* 对象

弃用	对象	详细信息	新建地点
6.3.0+	FlexConfig 对象： • Default_DNS_Configure 关联的文本对象： • defaultDNSNameServerList • defaultDNSParameters	配置默认 DNS 组，该组定义在数据接口上解析完全限定域名时可以使用的 DNS 服务器。这使您可以使用 CLI 中的命令（如 **ping**），并且使用主机名而不是 IP 地址。	在 FTD平台设置策略中为数据接口配置 DNS。
6.3.0+	FlexConfig 对象： • TCP_Embryonic_Conn_Limit • TCP_Embryonic_Conn_Timeout 关联的文本对象： • tcp_conn_misc • tcp_conn_limit • tcp_conn_timeout	配置初始连接限制和超时以防止 SYN 洪流拒绝服务 (DoS) 攻击。	在 FTD服务策略中配置这些功能，您可以在分配给设备的访问控制策略的 Advanced 选项卡上找到该策略。

此表列示了版本 6.2.3+ 中为使用 FDM 的 FTD 新近弃用的 CLI 命令。有关弃用命令的完整列表，包括在版本 6.2.0 中引入功能时弃用的命令，请参阅《Firepower 管理中心配置指南》。

表 *11*: 使用 *FMC* 的 *FTD*：弃用的 *CLI* 命令

弃用	命令	详细信息
6.2.3+	**pager**	阻止配置。

使用 Firepower 设备管理器的 FTD

此表列示了版本 6.3.0+ 中为使用 FDM 的 FTD 新近弃用的 CLI 命令。有关弃用命令的完整列表，包括在版本 6.2.3 中引入功能时弃用的命令，请参阅《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》。

表 *12*: 使用 *FDM* 的 *FTD*：弃用的 *CLI* 命令

弃用	命令	详细信息
6.3.0+	**access-list**	不能再创建 **extended** 和 **standard** 访问列表。使用智能 CLI 扩展访问列表或标准访问列表对象创建这些 ACL。然后，可以在按对象名称引用 ACL 且支持 FlexConfig 的命令中使用，例如带扩展 ACL 的 **match access-list** 用于服务策略流量类别。

弃用	命令	详细信息
6.3.0+	**as-path**	创建智能 CLI AS 路径对象，并将其用于智能 CLI BGP 对象，以配置自治系统路径过滤器。
6.3.0+	**community-list**	创建智能 CLI 扩展社区列表或标准社区列表对象，并将其用于智能 CLI BGP 对象，以配置社区列表过滤器。
6.3.0+	**dns-group**	使用 **Objects** > **DNS Groups** 配置 DNS 组，并使用 **Device** > **System Settings** > **DNS Server** 分配这些组。
6.3.0+	**policy-list**	创建智能 CLI 策略列表对象，并将其用于智能 CLI BGP 对象，以配置策略列表。
6.3.0+	**prefix-list**	创建智能 CLI IPv4 前缀列表对象，并将其用于智能 CLI OSPF 或 BGP 对象，以配置 IPv4 前缀列表过滤。
6.3.0+	**route-map**	创建智能 CLI 路由映射对象，并将其用于智能 CLI OSPF 或 BGP 对象，以配置路由映射。
6.3.0+	**router bgp**	使用适用于 BGP 的 Smart CLI 模板。

FMC 菜单更改

此表列示了更改后的Firepower管理中心菜单（页面更改）。有关新增和删除的菜单选项，请参阅新功能和弃用功能文档。

表 *13: Firepower* 管理中心菜单更改

版本	新菜单路径	旧菜单路径
6.4.0	**System** > **Integration** > **Cloud Services**	**System** > **Integration** > **Cisco CSI**
6.3.0	**Analysis > Lookup > Whois**	**Analysis > Advanced > Whois**
6.3.0	**Analysis > Lookup > Geolocation**	**Analysis > Advanced > Geolocation**
6.3.0	**Analysis > Lookup > URL**	**Analysis > Advanced > URL**
6.3.0	**Analysis > Custom > Custom Workflows**	**Analysis > Advanced > Custom Workflows**
6.3.0	**Analysis > Custom > Custom Tables**	**Analysis > Advanced > Custom Tables**
6.3.0	**Analysis > Vulnerabilities > Vulnerabilities**	**Analysis > Hosts > Vulnerabilities**
6.3.0	**Analysis > Vulnerabilities > Third-Party Vulnerabilities**	**Analysis > Hosts > Third-Party Vulnerabilities**

FMC 操作方法演练

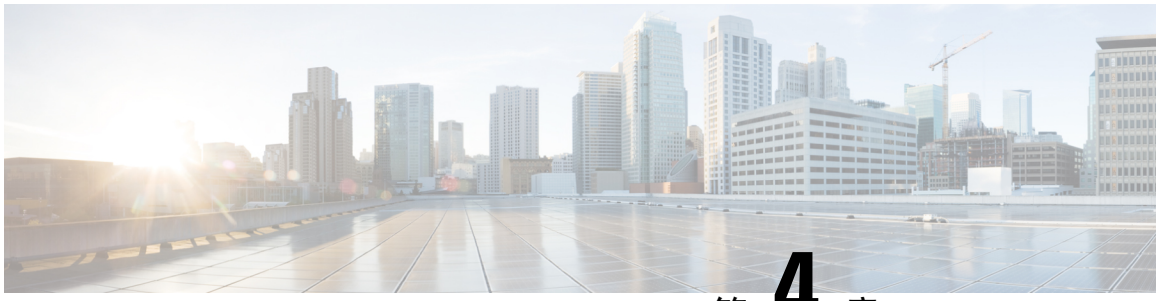
版本 6.3.0 引入 FMC 上的演练（也称为使用方法），该演练将指导您完成各种基本任务，例如设备设置和策略配置。仅需单击浏览器窗口底部的**使用方法**，选择某一演练，然后按照分步说明进行操作。

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，请单击右上角的 **x** 。

表 *14:* 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。
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单击**下一步**，则可能需要结束本演练。



第 4 章

升级到版本 6.5.0

本章提供版本 6.5.0的关键和版本特定信息。

您还应该参阅特性和功能， 第 9 页，了解有关任何新特性和功能、弃用的功能和平台、菜单和术语更改、列入黑名单的 FlexConfig 命令等的信息。

指引和警告： 版本 6.5.0

此核对表中包含为版本 6.5.0新增的重要升级指引和警告。您还应查看以前发布的指引和警告， 第 48 页和一般指引和警告， 第 54 页。

表 *15:* 版本 *6.5.0* 新指引

	指南	平台	升级自	直接至
	Firepower 1000 系列设备需要升级后的电源周期， 第 32 页	Firepower 1000 系列	6.4.0.x	6.5.0+
	使用版本 6.5.0-120 升级多域 FMC，第 32 页	FMC	6.2.3 至 6.4.0. x	仅限 6.5.0
	升级失败：具有不同步 NTP 的设备， 第 33 页	任意	6.2.3 至 6.4.0. x	仅限 6.5.0
	升级会将部署分配给北美洲思科云，第 33 页	任意	6.2.3 至 6.4.0. x	6.5.0+

	指南	平台	升级自	直接至
	思科 Threat Intelligence Director (TID) 行为更改，第 33 页	FMC	6.2.3 至 6.4.0. x	6.5.0+
	FTD/FDM 升级期间删除历史数据，第 34 页	使用 FDM 的 FTD	6.2.3 至 6.4.0. x	6.5.0+
	新 URL 类别和信誉，第 34 页	任意	6.2.3 至 6.4.0. x	6.5.0+

Firepower 1000 系列设备需要升级后的电源周期

部署：Firepower 1000 系列

升级自：版本 6.4.0.x

直接至：版本 6.5.0+

版本 6.5.0 引入了适用于 Firepower 1000/2100 和 Firepower 4100/9300 系列设备的 FXOS CLI‘安全擦除’功能。

对于 Firepower 1000 系列设备，您必须在升级到版本 6.5.0+ 后重新启动设备，此功能才能正常工作。自动重启不足。其他支持的设备不需要重启电源。

使用版本 6.5.0-120 升级多域 FMC

部署：FMC

升级自：版本 6.2.3 至 6.4.x

直接至：仅版本 6.5.0

相关漏洞： CSCvr47499

如果您的部署使用域(多租户)，则 FMC 升级到版本 6.5.0-**115**（发布于 2019 年 9 月 26 日）将失败，如果在子域中，访问控制策略使用也在子域中创建的自定义网络分析策略作为默认 NAP。

如果出现以下情况，升级不会失败：

- 在子域中，访问控制策略使用在全局域中创建的自定义网络分析策略作为默认 NAP。
- 在子域中，访问控制策略在 NAP 规则中使用自定义 NAP。

在多域部署中，请使用版本 6.5.0-**120**（发布于 2019 年 10 月 8 日）升级软件包。

注释 如果您错误地使用了版本 6.5.0-115，并且升级失败，请联系思科 TAC以了解解决问题的步骤并恢复升级。

升级失败：具有不同步 NTP 的设备

部署：任意

升级自：版本 6.2.3 至 6.4.x

直接至：仅版本 6.5.0

在升级到版本 6.5.0 之前，必须确保 Firepower 设备与您用于提供时间的任何 NTP 服务器同步。不同步可能会导致升级失败。

在 FMC 部署中，如果时钟不同步超过 10 秒，时间同步状态运行状况模块会发出警报，但您仍应手动进行检查。

要检查时间，请执行以下操作：

- FMC：选择**系统 > 配置 > 时间**。
- 设备：使用**show time** CLI 命令。

升级会将部署分配给北美洲思科云

部署：任意

升级自：版本 6.2.3 至 6.4.x

直接至：版本 6.5.0+

我们现在推出了思科云服务区域。您的部署的区域云用于以下功能：思科防御协调器、思科威胁响应、思科成功网络网络和思科支持诊断功能。

对于 FMC 部署，默认情况下，升级会将您分配给美国（北美）区域。您可以在**系统 > 集成 > 云服务**页面上更改您的区域。

对于带 FDM 的 FTD，您可以在使用智能许可注册时选择您所在的区域。如果升级已注册的设备，升级会将您分配给美国（北美）区域。要更改区域，必须取消注册并向 思科智能软件管理器(CSSM) 注册。

思科 Threat Intelligence Director (TID) 行为更改

部署：FMC

升级自：版本 6.2.3 至 6.4.0.x

直接至：版本 6.5.0+

在版本 6.5.0+ 中，TID 阻止/监控可观察对象操作的优先级现在高于使用安全情报黑名单的阻止/监控。

如果配置了**阻止**TID 可观察对象操作，即使流量也与设置为**阻止**的安全情报黑名单匹配：

- 连接事件中的安全情报类别是 `TID 阻止`的变体。
- 系统会生成一个 TID 事件，其中包含被阻止的操作。

如果您配置**监控**TID 可观察对象操作，即使流量与设置为**监控**的安全情报黑名单匹配也是如此：

- 连接事件中的安全情报类别是`TID 监控器`的一种变体
- 系统会生成一个 TID 事件，其中包含被监控的操作。

以前，在上述每种情况下，系统通过分析报告类别，但未生成 TID 事件。

注释 系统仍会像以前一样有效地处理流量。之前被阻止的流量仍被阻止，并且受监控的流量仍受到监控。这只会更改哪个组件获得‘积分’。您可能还会看到生成了更多 TID 事件。

有关同时启用安全情报和 TID 时系统行为的完整信息，请参阅《Firepower 管理中心配置指南》中的 *TID-Firepower* 管理中心操作优先级信息。

FTD/FDM 升级期间删除历史数据

部署：Firepower 设备管理器

升级自：版本 6.2.3 至 6.4.x

直接至：6.5.0+

由于数据库架构更改，升级期间将删除所有历史报告数据。升级后，无法查询历史数据，也无法在仪表板中查看历史数据。

新 URL 类别和信誉

部署：任意

升级自：版本 6.2.3 至 6.4.0.x

直接至：版本 6.5.0+

思科 Talos 情报小组 (Talos) 引入了新的类别，并对信誉进行了重命名，以对 URL 进行分类和过滤。有关新 URL 类别的说明，请参阅 Talos 情报类别站点。

此外，新增的是未分类和无信誉 URL 的概念，但规则配置选项保持不变：

- 未分类的 *URL* 可能具有可疑的、中立的、有利的或可信的信誉。

  您可以过滤**未分类**的URL，但不能通过信誉进一步限制。这些规则将匹配所有未分类的URL，而不考虑信誉。

  请注意，没有任何类别的不受信任规则。否则，系统会将具有不可信信誉的未分类URL 自动分配给新的恶意站点威胁类别。

- 无信誉 *URL* 可以属于任何类别。

  不能过滤无信誉 URL。规则编辑器中没有“无信誉”选项。但是，您可以使用**任何**信誉过滤URL，包括无信誉URL。这些URL 也必须按类别进行约束。没有实用程序遵循任意/任意规则。

下表总结了升级的变化。尽管它们是为最小影响而设计的，但不会阻止对大多数客户进行升级后部署，但我们强烈建议您查看这些版本说明和当前的URL过滤配置。仔细的规划和准备可以帮助您避免失误，并减少升级后的故障排除时间。

表 *16:* 升级时的部署更改

变化	详细信息
修改 URL 规则类别。	升级会修改 URL 规则以使用新类别集中最接近的等效项，位于以下策略中： • 访问控制 • SSL • QoS （仅限 FMC） • 关联（仅限 FMC） 这些更改可能会创建冗余或抢占规则，这会降低性能。如果您的配置包括合并的类别，则您可能会遇到允许或阻止的 URL 有细微更改的情况。 有关类别更改的详细列表，请参阅URL 类别更改，第 39 页。
重命名URL规则信誉。	升级会修改 URL 规则以使用新的信誉名称： 1. 不受信（为高风险） 2. 有问题（为可疑站点） 3. 中立（为具有安全风险的良性站点） 4. 良好（为良性站点） 5. 受信（为众所周知）
清除 URL 缓存。	升级会清除 URL 缓存，其中包含系统先前在云中查找的结果。对于不在本地数据集中的 URL，您的用户可能会暂时遇到访问时间稍长的问题。
标示“遗留”事件。	对于已经记录的事件，升级会将任何关联的 URL 类别和信誉信息标示为遗留。随着时间的推移，这些遗留传统事件将逐渐退出数据库。

用于 URL 类别和信誉的升级前操作

在升级之前，请执行以下操作。

表 *17:* 升级前操作

操作	详细信息
请确保您的设备可以访问 Talos 资源。	升级后，系统必须能够与以下 Cisco 资源进行通信： • https://regsvc.sco.cisco.com/-注册 • https://est.sco.cisco.com/-获取安全通信的证书 • https://updates-talos.sco.cisco.com/-获取客户端/服务器清单 • http://updates.ironport.com/ — 下载数据库（注意：使用端口 80） • https://v3.sds.cisco.com/-云查询 云查询服务还使用以下 IP 地址块： • IPv4 云查询： • 146.112.62.0/24 • 146.112.63.0/24 • 146.112.255.0/24 • 146.112.59.0/24 • IPv6 云查询： • 2a04:e4c7:ffff::/48 • 2a04:e4c7:fffe::/48
确定潜在的规则问题。	了解即将进行的更改。检查您当前的 URL 过滤配置，并确定您需要执行的升级后操作（请参阅下一部分）。 **注释** 您可能希望立即修改使用已否决类别的 URL 规则。否则，使用这些规则的规则将在升级后阻止部署。 在 FMC 部署中，我们建议您生成一份访问控制策略报告。它会详述策略当前保存的配置，包括访问控制规则以及从属策略（例如 SSL）中的规则。对于每个URL规则，您可以查看当前类别、信誉和关联的规则操作。在 FMC 上，选择 **策略** > **访问控制** ，然后单击相应策略旁边的报告图标 ()。

URL 类别和声誉的升级后操作

升级后，您应重新检查URL过滤配置，并尽快采取以下操作。根据部署类型和升级所做的更改，某些（但不是全部）问题可能会在 GUI 中进行标记。例如，在 FMC/FDM 上的访问控制策略中，您可以点击**显示警告**（FMC）或**显示问题规则**（FDM）。

表 *18:* 升级后操作

操作	详细信息
从规则中删除**弃用类别**。Required. 列表: 弃用的类别，第 43 页。	升级不会修改使用弃用类别的URL规则。使用它们的规则将阻止部署。 在 FMC 上，这些规则会被标记。
创建或修改规则以包含**新类别**。 列表：新范畴，第 42 页。	大多数新类别可识别威胁。强烈建议您使用它们。 在 FMC 上，此升级后不会标记这些新类别，但 Talos 可能会在将来添加其他类别。发生这种情况时，会对新类别进行标记。
评估由于**合并类别**而更改的规则。 列表：合并的类别，第 43 页。	包含任何受影响类别的每个规则现在都包含所有受影响的类别。如果原始类别与不同的信誉相关联，则新规则与更广泛、更具包容性的信誉相关联。要像以前一样过滤 URL，可能需要修改或删除某些配置；请参阅含合并 URL 类别的规则的指南，第 37 页。 根据您的平台处理规则警告的变化和方式，可能会对更改进行标记。例如，FMC会标记完全冗余和完全抢占的规则，但不会标记具有部分重叠的规则。
评估由于**划分类别**而更改的规则。 列表：拆分类别，第 44 页。	升级会将URL规则中的每个旧类别替换为映射到旧类别的所有新类别。这不会更改过滤URL的方式，但可以修改受影响的规则以利用新粒度。 这些更改不会被标记。
了解哪些类别经**重命名**，哪些**无更改**。 列表： 重命名的类别，第 46 页和未更改的类别，第 47 页。	虽然不需要采取任何措施，但您应该了解这些更改。 这些更改不会被标记。
评估如何处理**未分类**和**无信誉**的URL。	尽管现在可能会存在未分类的和无信誉的 URL，但仍无法按信誉过滤未分类的 URL，也无法过滤无信誉的 URL。 请确保按**未分类**的类别或**任何**信誉过滤的规则按预期运行。

含合并 URL 类别的规则的指南

在升级之前检查URL过滤配置时，请确定以下哪些情景和指南适用于您。这将确保您的升级后配置符合预期，并且您可以快速采取行动来解决任何问题。

表 *19:* 含合并 *URL* 类别的规则的指南

指南	详细信息
规则顺序决定与流量匹配的规则	在考虑包含相同类别的规则时，请记住流量与列表中包含条件的第一条规则匹配。

指南	详细信息
同一规则中的类别与不同规则中的类别	如果是合并一个规则中的类别，结果将合并到规则的单个类别中。例如，如果类别 A 和类别 B 合并为类别 AB，并且您有一个同时具有类别 A 和类别 B 的规则，则合并后该规则只有一个类别，即类别 AB。 合并不同规则中的类别将导致合并后每个规则中具有相同类别的单独规则。例如，如果类别 A 和类别 B 合并为类别 AB，并且您有包含类别 A 的规则 1 和包含类别 B 的规则 2，则合并后规则 1 和规则 2 将各自包含类别 AB。您选择如何解决此问题取决于规则顺序、与规则关联的操作和信誉级别、规则中包含的其他 URL 类别，以及规则中包含的非 URL 条件。
关联操作	如果不同规则中合并的类别与不同操作相关联，那么在合并之后，您可能有两个或更多规则对同一类别具有不同的操作。
关联的信誉级别	如果合并之前，单个规则包含与不同信誉级别关联的类别，则合并的类别将与更具包容性的信誉级别关联。例如，如果类别 A 在特定规则中与**任何信誉**关联，类别 B 在该规则中与信誉级别 **3（具有安全风险的良性站点）关联**，则合并后，该规则中的类别 AB 将与**任何信誉**关联。
重复及冗余的类别和规则	合并后，不同的规则可能具有与不同操作和信誉级别关联的相同类别。 冗余规则可能不是完全重复的，但如果规则序列中有另一个更早的规则与之匹配，则它们可能不再匹配流量。例如，如果您将规则 1 与适用于任何信誉的类别 A 预先合并，将规则 2 与仅适用于信誉 1-3 的类别 B 预先合并，则合并后，规则 1 和规则 2 都将为类别 AB，但如果规则 1 在规则序列中处于靠前的位置，规则 2 永远不会匹配。 在 FMC 上，具有相同类别和信誉的规则将显示警告。但是，这些警告不会指示包含相同类别但信誉不同的规则。 警告：在确定如何解决重复或冗余类别时，考虑规则中的所有条件。
规则中的其他 URL 类别	含合并 URL 的规则还可能包含其他 URL 类别。因此，如果在合并后特定类别重复，可能需要修改而不是删除这些规则。
规则中的非 URL 条件	具有合并 URL 类别的规则还可以包括其他规则条件，例如应用条件。因此，如果在合并后特定类别重复，可能需要修改而不是删除这些规则。

下表中的示例使用类别 A 和类别 B，现在合并到类别 AB 中。在两个规则示例中，规则 1 位于规则 2 之前。

表 *20:* 含合并 *URL* 类别的规则的示例

场景	升级前	升级后
同一规则中的合并类别	规则 1 有类别 A 和类别 B。	规则 1 有类别 AB。

场景	升级前	升级后
不同规则中的合并类别	规则 1 有类别 A。 规则 2 有类别 B。	规则 1 有类别 AB。 规则 2 有类别 AB。 具体结果因列表中规则的序列、信誉级别和关联操作而异。在确定如何解决任何冗余时，还应考虑规则中的所有其他条件。
不同规则中的合并类别具有不同的操作 （信誉相同）	规则 1 将类别 A 设置为允许。 规则 2 将类别 B 设置为阻止。 （信誉相同）	规则 1 将类别 AB 设置为允许。 规则 2 将类别 AB 设置为阻止。 规则 1 将匹配此类别的所有流量。 规则2将永远不会匹配流量；如果您在合并后显示警告，其会显示警告指示符，因为类别和信誉都相同。
同一规则中的合并类别具有不同的信誉级别	规则 1 包括： 含任何信誉的类别 A 含信誉 1-3 的类别 B	规则 1 包括含任何信誉的类别 AB。
不同规则中的合并类别具有不同的信誉级别	规则 1 包括含任何信誉的类别 A。 规则 2 包括含信誉 1-3 的类别 B。	规则 1 包括含任何信誉的类别 AB。 规则 2 包括含信誉 1-3 的类别 AB。 规则 1 将匹配此类别的所有流量。 规则2永远不会匹配流量，但由于信誉不同，您不会看到警告指示符。

URL 类别更改

使用此表确定 URL 类别的更改方式。

表 *21:* 旧 *URL* 类别的索引

旧类别	变化		旧类别	变化
堕胎	合并的类别，第 43 页		军事	未更改的类别，第 47 页
滥用药物	合并的类别，第 43 页		机动车	重命名的类别，第 46 页
成人和色情	拆分类别，第 44 页		音乐	重命名的类别，第 46 页

旧类别	变化		旧类别	变化
酒精和烟草	拆分类别，第 44 页		新闻与媒体	重命名的类别，第 46 页
僵尸网络	重命名的类别，第 46 页		裸体	重命名的类别，第 46 页
商业与经济	拆分类别，第 44 页		在线贺卡	重命名的类别，第 46 页
作弊程序	重命名的类别，第 46 页		打开 HTTP 代理	重命名的类别，第 46 页
计算机和互联网信息	拆分类别，第 44 页		寄放域	未更改的类别，第 47 页
计算机和互联网安全	拆分类别，第 44 页		付费冲浪	合并的类别，第 43 页
已确认的垃圾邮件源	合并的类别，第 43 页		点对点	重命名的类别，第 46 页
内容交付网络	合并的类别，第 43 页		个人网站和博客	拆分类别，第 44 页
小众和神秘	拆分类别，第 44 页		个人存储	拆分类别，第 44 页
约会	未更改的类别，第 47 页		哲学和政治宣传	重命名的类别，第 46 页
死网站	重命名的类别，第 46 页		网络钓鱼和其他欺诈	重命名的类别，第 46 页
动态生成的内容	合并的类别，第 43 页		专用 IP 地址	弃用的类别，第 43 页
教育机构	合并的类别，第 43 页		代理规避和匿名程序	重命名的类别，第 46 页
娱乐和艺术	拆分类别，第 44 页		可疑	重命名的类别，第 46 页
时尚和美容	重命名的类别，第 46 页		房地产	未更改的类别，第 47 页
金融服务业	重命名的类别，第 46 页		娱乐和爱好	合并的类别，第 43 页

旧类别	变化		旧类别	变化
食品餐饮	重命名的类别，第 46 页		参考和研究	拆分类别，第 44 页
赌博	拆分类别，第 44 页		宗教	未更改的类别，第 47 页
游戏	未更改的类别，第 47 页		搜索引擎	合并的类别，第 43 页
政府	合并的类别，第 43 页		性教育	合并的类别，第 43 页
毛额	合并的类别，第 43 页		共享软件和免费软件	重命名的类别，第 46 页
黑客攻击	合并的类别，第 43 页		购物	未更改的类别，第 47 页
仇恨和种族主义	重命名的类别，第 46 页		社交网络	拆分类别，第 44 页
健康和医疗	重命名的类别，第 46 页		社会	拆分类别，第 44 页
家居和园艺	拆分类别，第 44 页		垃圾邮件 URL	合并的类别，第 43 页
狩猎和钓鱼	重命名的类别，第 46 页		体育	合并的类别，第 43 页
违法	拆分类别，第 44 页		间谍软件和广告软件	未更改的类别，第 47 页
图片和视频搜索	重命名的类别，第 46 页		流媒体	重命名的类别，第 46 页
个人炒股建议和工具	重命名的类别，第 46 页		泳衣和内衣	重命名的类别，第 46 页
互联网通信	拆分类别，第 44 页		培训和工具	合并的类别，第 43 页
互联网门户	合并的类别，第 43 页		差旅费	未更改的类别，第 47 页
求职	未更改的类别，第 47 页		未分类	弃用的类别，第 43 页

旧类别	变化		旧类别	变化
按键记录器和监控	合并的类别，第 43 页		未确认的垃圾邮件源	合并的类别，第 43 页
童鞋	重命名的类别，第 46 页		暴力类	合并的类别，第 43 页
法务	合并的类别，第 43 页		武器	未更改的类别，第 47 页
本地信息	重命名的类别，第 46 页		网络广告	合并的类别，第 43 页
恶意软件网站	未更改的类别，第 47 页		基于 Web 的邮件	拆分类别，第 44 页
大麻	合并的类别，第 43 页		Web 托管站点	重命名的类别，第 46 页

新范畴

这些表列出了全新的 URL 类别，其中大多数都标识了威胁。我们强烈建议您创建或修改 URL 规则以包含新的威胁类别。请注意，某些现有的URL类别确实可识别威胁；我们建议您也包括这些。有关这些类别的列表，请参阅 Talos 情报类别站点。

表 *22*: 新范畴

新类别
动态和住宅

表 *23*: 新威胁类别

新威胁类别
Bogon
加密劫持
DNS 隧道
域生成算法
动态 DNS
电子银行欺诈
攻击
高风险站点和位置

新威胁类别
感染指标 (IOC)
主页广告
恶意站点
移动威胁
新发现的域
开放邮件中继
P2P 恶意软件节点
潜在的 DNS 重新绑定
TOR 出口节点

弃用的类别

升级不会修改使用弃用类别的 URL 规则。这些规则将阻止部署；您应删除或修改它们。

表 *24:* 弃用的类别

弃用的类别
未分类
专用 IP 地址

合并的类别

包含任何受影响类别的每个规则现在都包含所有受影响的类别。如果原始类别与不同的信誉相关联，则新规则与更广泛、更具包容性的信誉相关联。要像以前一样过滤 URL，可能需要修改或删除某些配置；请参阅含合并 URL 类别的规则的指南， 第 37 页。

我们还强烈建议您创建或修改 URL 规则以包含新指定的威胁类别（垃圾邮件）。

表 *25:* 合并的类别

旧类别	合并后的新类别
网络广告	广告
付费冲浪	
教育机构	教育
培训和工具	

旧类别	合并后的新类别
暴力类	极高
毛额	
政府	政府和法律
法务	
滥用药物	违禁药物
大麻	
动态生成的内容	基础设施
内容交付网络	
黑客攻击	黑客攻击
按键记录器和监控	
搜索引擎	搜索引擎和门户
互联网门户	
性教育	性教育
堕胎	
已确认的垃圾邮件源	垃圾邮件（威胁类别）
垃圾邮件 URL	
未确认的垃圾邮件源	
娱乐和爱好	体育和娱乐网站
体育	

拆分类别

升级会将URL规则中的每个旧类别替换为映射到旧类别的所有新类别。升级后，您可以修改受影响的规则以利用新粒度。

表 *26:* 拆分类别

旧的单一类别	新的拆分类别
成人和色情	色情
	成人

旧的单一类别	新的拆分类别
酒精和烟草	酒类
	烟草
商业与经济	商业和工业
	手机
计算机和互联网信息	软件更新
	计算机和互联网
	SaaS 和 B2B
	在线会议
计算机和互联网安全	计算机安全
	个人 VPN
小众和神秘	超过正常范围
	占星
娱乐和艺术	艺术
	娱乐
赌博	赌博
	彩票
家居和园艺	自然
	DIY 项目
违法	非法活动
	虐童内容
	非法下载
互联网通信	互联网电话服务
	聊天和即时消息
个人网站和博客	个人网站
	在线社区

旧的单一类别	新的拆分类别
个人存储	在线存储和备份
	文件传输服务
参考和研究	科技
	社会科学
社交网络	社交网络
	职业社交网络
社会	社会文化
	非政府组织
基于 Web 的邮件	基于 Web 的电子邮件
	组织电子邮件

重命名的类别

虽然不需要采取任何措施，但您应该了解这些更改。我们强烈建议您创建或修改URL规则，以包括新指定的威胁类别（僵尸网络、开放 HTTP 代理、网络钓鱼）。

表 *27*: 重命名的类别

旧类别名称	新类别名称
僵尸网络	僵尸网络（威胁类别）
作弊程序	欺诈和剽窃
死网站	不可操作
时尚和美容	时尚
金融服务业	财经
食品餐饮	餐饮
仇恨和种族主义	仇恨言论
健康和医疗	健康和营养
狩猎和钓鱼	正在查找
图片和视频搜索	照片搜索和图片
个人炒股建议和工具	在线交易

旧类别名称	新类别名称
童鞋	儿童安全
本地信息	参考
机动车	交通运输业
音乐	流式音频
新闻与媒体	新闻
裸体	非色情裸体
在线贺卡	数字明信片
打开 HTTP 代理	开放式 HTTP 代理（威胁类别）
点对点	对等文件传输
哲学和政治宣传	政治
网络钓鱼和其他欺诈	网络钓鱼 （威胁类别）
代理规避和匿名程序	规避过滤网站
可疑	幽默
共享软件和免费软件	免费软件和共享软件
流媒体	流视频
泳衣和内衣	女用内衣和泳装
Web 托管站点	Web 托管

未更改的类别

虽然不需要采取任何措施，但您应该了解这些更改。我们强烈建议您创建或修改URL规则以包含新指定的威胁类别（恶意软件站点、间谍软件和广告软件）。

表 *28:* 未更改的类别

未更改的类别
约会
游戏
求职
军事

未更改的类别
寄放域
房地产
宗教
购物
差旅费
武器

表 *29:* 未更改的威胁类别

未更改威胁类别
恶意软件站点（威胁类别）
间谍软件和广告软件（威胁类别）

以前发布的指引和警告

如果升级路径跳过主版本，请查看此核对表。您可以从多个之前的主版本升级到版本 6.5.0；请参阅要升级的最低版本，第 56 页。

表 *30:* 版本 *6.5.0* 以前发布的指南

	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 49 页	Firepower 4100/9300	6.3.0 至 6.4.0.x	6.3.0.1 至 6.5.0
	TLS 加密加速已启用/不能禁用，第 49 页	Firepower 2100 系列 Firepower 4100/9300	6.2.3 至 6.3.0. x	6.4.0+
	URL 过滤缓存的超时可能会更改，第 50 页	任意	6.2.3.x	6.3.0+

	指南	平台	升级自	直接至
	对 FMC、NGIPSv 的准备情况检查可能失败，第 50 页	FMC Firepower 7000/8000 系列 NGIPSv	6.1.0 至 6.1.0.6 6.2.0 至 6.2.0.6 6.2.1 6.2.2 至 6.2.2.4 6.2.3 至 6.2.3.4	6.3.0+
	RA VPN 默认设置更改可以封锁 VPN 流量，第 51 页	使用 FMC 的 FTD	6.2.0 至 6.2.3.x	6.3.0+
	FMC 1000/2500/4500 可能需要预升级修复程序，第 51 页	MC1000、2500 和 4500	6.2.0 至 6.2.3.7	6.3.0+
	更新了设备访问的安全性，第 52 页	任意	6.1.0 至 6.2.3.x	6.3.0+
	安全情报启用应用程序识别，第 52 页	FMC 部署	6.1.0 至 6.2.3.x	6.3.0+
	升级后更新 VDB 以启用 CIP 检测，第 53 页	任意	6.1.0 至 6.2.3.x	6.3.0+
	无效的入侵变量集可能导致部署失败，第 53 页	任意	6.1.0 至 6.2.3.x	6.3.0+
	连接和入侵事件的系统日志行为更改，第 54 页	FMC	6.1.0 至 6.2.3.x	6.3.0+

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。

TLS 加密加速已启用/不能禁用

部署：Firepower 2100 系列、Firepower 4100/9300 机箱

升级自：版本 6.1.0 至 6.3.x

直接至：版本 6.4.0+

SSL 硬件加速已重命名为 *TLS* 加密加速。

根据设备的不同，TLS 加密加速可以在软件或硬件中执行。升级会自动在所有符合条件的设备上启用加速，即使先前已手动禁用该功能也不例外。在大多数情况下，您无法配置此功能；它会自动启用，您无法禁用它。

升级到版本 *6.4.0*： 如果您使用的是 Firepower 4100/9300 机箱的多实例功能，则可以使用 FXOS CLI 为每个模块/安全引擎的一个容器实例启用 TLS 加密加速。加速对其他容器实例禁用，但对本地实例启用。

升级到版本 *6.5.0*+： 如果您使用的是 Firepower 4100/9300 机箱的多实例功能，可以使用 FXOS CLI 为 Firepower 4100/9300 机箱上的多个容器实例（最多16个）启用 TLS 加密加速。新实例默认启用此功能。但是，升级不会在现有实例上启用加速。相反，使用 **config hwCrypto enable** CLI 命令。

URL 过滤缓存的超时可能会更改

部署：任意

升级自：版本 6.2.3.x

直接至：版本 6.3.0+

版本 6.3.0 新功能 - 您可以通过 GUI 为 URL 过滤缓存配置超时值。要尽量减少与过时数据匹配的 URL 实例，可以将缓存中的 URL 设置为过期。如果您与思科 TAC 合作为 URL 过滤缓存指定超时值，则升级可能会更改该值。

升级完成后：

- FMC：选择 **System** > **Integration**，单击 Cisco CSI 选项卡，评估 **Cached URLs Expire** 设置。
- FDM：选择 **System Settings** > **Traffic Settings** > **URL Filtering Preferences**，评估 **URL Time to Live** 设置。

对 FMC、NGIPSv 的准备情况检查可能失败

部署：FMC、NGIPSv

升级自：版本 6.1.0 至 6.1.0.6、版本 6.2.0 至 6.2.0.6、版本 6.2.1、版本 6.2.2 至 6.2.2.4，以及版本 6.2.3 至 6.2.3.4

直接至：版本 6.3.0+

如果是从上方列出的任一Firepower版本升级，无法对列出的型号运行准备情况检查。发生这种情况的原因是，准备情况检查过程与较新的升级包不兼容。

表 *31:* 适用于版本 *6.3.0+* 的含准备情况检查的修补程序

不支持准备情况检查	含补丁的第一个修补程序
6.1.0 至 6.1.0.6	6.1.0.7
6.2.0 至 6.2.0.6	6.2.0.7

不支持准备情况检查	含补丁的第一个修补程序
6.2.1	无。升级至版本 6.2.3.5+。
6.2.2 至 6.2.2.4	6.2.2.5
6.2.3 至 6.2.3.4	6.2.3.5

RA VPN 默认设置更改可以封锁 VPN 流量

部署： Firepower 威胁防御为远程访问 VPN 配置

升级自：版本 6.2.x

直接至：版本 6.3+

版本 6.3 更改了隐藏选项的默认设置，**sysopt connection permit-vpn**。升级可能导致远程访问 VPN 停止传送流量。如果发生这种情况，请采用以下任一方法：

- 创建配置 **sysopt connection permit-vpn** 命令的 FlexConfig 对象。此命令的新默认值是 **no sysopt connection permit-vpn**。

  外部用户无法在远程接入 VPN 地址池中伪造 IP 地址，因此这种允许 VPN 流量的方法较为安全。但它的缺点是，VPN流量得不到检测，也就是说不会对流量应用入侵和文件保护、URL过滤或其他高级功能。

- 创建访问控制规则以允许来自远程接入 VPN 地址池的连接。

  此方法可确保对VPN流量进行检测，并将高级服务应用于连接。但它的缺点是，有可能造成外部用户伪造 IP 地址，进而获得访问　内部网络的权限。

FMC 1000/2500/4500 可能需要预升级修复程序

部署： Firepower 管理中心型号 FMC 1000、2500 和 4500

升级自：版本 6.2.0 至 6.2.3.7

直接至：版本 6.3.0+

在将 FMC1000、MC2500 或 MC4500 从版本 6.2.0 到 6.2.3.7 升级到版本 6.3.0+ 之前，必须应用预安装修复程序。或者，您也可以升级到版本 6.2.3.8 +。请勿将此修复程序应用于其他 FMC 型号或版本。

此修复程序（或补丁）将 RAID 控制器的固件更新为 24.12.1-0411 版本。如果没有更新固件，则运行版本 6.3.0+ 的受影响的升级版 FMC 可能会遇到性能问题。

注释 在某些情况下，即使您运行的是受影响的版本，您的固件也可能已是最新的。在这种情况下，修复程序失败，显示错误：映像文件的版本比控制器上的版本低。控制器未刷新。如果您看到此消息，则无需此修复程序即可安全地进行升级。

要在应用修复程序之前仔细检查固件版本，请访问 FMC 上的 Linux shell（也称为专家模式）并运行以下命令：**`sudo storcli/c0 show | Grep "FW version"`**。

此修复程序可从思科支持和下载站点获取，与您主要版本的升级和安装包在同一位置。通过常规升级页面（**系统** > **更新**）应用热补丁。

表 *32*: 预安装热补丁包

当前版本	修复程序	数据包
6.3.0+	—	如果您在没有安装修复程序或补丁的情况下升级到 6.3.0+，请联系思科 TAC。
6.2.3.8 或更高版本补丁	—	正常升级。无需任何修复程序。
6.2.3 至 6.2.3.7	热补丁 AJ	Sourcefire_3D_Defense_Center_S3_Hotfix_AJ-6.2.3.999-5.sh.REL.tar
6.2.2.x	热补丁 BY	Sourcefire_3D_Defense_Center_S3_Hotfix_BY-6.2.2.999-1.sh.REL.tar
6.2.1	-	升级到版本 6.2.3 并对 6.2.3.8+ 应用修复程序 AJ 或补丁。
6.2.0.x	—	升级到版本 6.2.3 并对 6.2.3.8+ 应用修复程序 AJ 或补丁。

更新了设备访问的安全性

部署：任意

升级自：版本 6.1 至 6.2.3.x

直接至：版本 6.3+

为提高安全性，在版本 6.3 中，我们更新了支持的密码和加密算法列表，以实现安全的 SSH 访问。如果由于密码错误导致 SSH 客户端无法与 Firepower 设备连接，请将客户端更新到最新版本。

安全情报启用应用程序识别

部署：Firepower 管理中心

升级自：版本 6.1 至 6.2.3.x

直接至：版本 6.3+

在版本 6.3 中，安全情报配置支持应用程序检测和识别。如果在当前部署中禁用了发现，升级进程可能会再次启用它。在不需要的情况下禁用发现（例如，在仅限 IPS 的部署中）可以提高性能。

要禁用发现，您必须：

- 从网络发现策略中删除所有规则。
- 仅使用简单的、基于网络的条件执行访问控制：区域、IP 地址、VLAN 标记和端口。不要执行任何类型的应用程序、用户、URL 或地理位置控制。
- （**全新**）通过从访问控制策略的安全情报配置中删除所有白名单和黑名单（包括默认全局名单）来禁用基于网络和 URL 的安全情报。
- （**全新**）通过删除或禁用关联的 DNS 策略中的所有规则（包括 DNS 的默认全局白名单和 DNS 规则的全局黑名单）来禁用基于 DNS 的安全情报。

升级后更新 VDB 以启用 CIP 检测

部署：任意

升级自：版本 6.1.0 至 6.2.3.x，使用 VDB 299+

直接至：版本 6.3.0+

如果在使用漏洞数据库 (VDB) 299 或更高版本时升级，则升级过程会出现问题，使得您在升级后无法使用 CIP 检测。这包括从 2018 年 6 月到现在发布的每个 VDB，甚至是最新的 VDB。

尽管我们一直建议您在升级后将漏洞数据库 (VDB) 更新到最新版本，但这一做法在这种情况下尤为重要。

要检查您是否受到此问题的影响，请尝试使用基于 CIP 的应用程序条件配置访问控制规则。如果在规则编辑器中找不到任何 CIP 应用程序，请手动更新 VDB。

无效的入侵变量集可能导致部署失败

部署：任意

升级自：版本 6.1 至 6.2.3.x

直接至：版本 6.3.0+

对于入侵变量集中的网络变量，排除的任何 IP 地址必须为包含的 IP 地址的子集。此表显示了有效和无效配置的示例。

生效	无效
包含：10.0.0.0/8 排除：10.1.0.0/16	包含：10.1.0.0/16 排除：172.16.0.0/12 排除：10.0.0.0/8

在版本6.3.0之前，您可以使用此类无效配置成功保存网络变量。现在，这些配置会阻止部署并显示错误：变量集有无效的排除值。

如果发生这种情况，识别并编辑错误配置的变量集，然后重新部署。请注意，您可能必须编辑变量集引用的网络对象和组。

连接和入侵事件的系统日志行为更改

部署：Firepower 管理中心

升级自：版本 6.1.0 至 6.2.3.x

直接至：版本 6.3.0+

版本6.3.0更改并集中了系统通过系统日志记录连接和入侵事件的方式。您可以在访问控制策略中的新 Logging 选项卡上访问这些设置。

升级不会更改连接事件日志记录的现有设置。但是，您可能会突然开始通过系统日志收到预期外的入侵事件。这是因为在升级到版本 6.3.0+ 之后，入侵策略会将系统日志事件发送到新 Logging 选项卡上的目标。（在版本6.3.0之前，您可以在入侵策略中配置系统日志警报，以将事件发送到受管设备本身 [而非外部主机] 的系统日志。）

此外，NGIPS 设备（ASA FirePOWER、NGIPSv）发送的消息现在使用 RFC 5425 中指定的 ISO 8601 时间戳格式。

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 65 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与这些版本完全相同的设备完全相同的设备。您只能从运行相同 Firepower 版本且具有相同 VDB 的设备还原备份。在大多数情况下，只能还原到同一模型；请参阅《Firepower 管理中心型号迁移指南》了解例外情况。

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

为了让 Firepower 可以证实您使用的是正确的文件，升级包和热补丁包是签名的档案。 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。您可以随时选择加入或退出。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

您可以从多个之前的主版本序列直接升级到版本6.5.0。不需要运行任何先前版本的最新修补程序即可升级。

表 *33*: 将 *Firepower* 软件升级到 *6.5.0* 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（Firepower 4100/9300 系列除外）。	6.2.3
使用 FMC 的 Firepower 4100/9300 上的 Firepower 威胁防御	使用 FXOS 2.7.1.92+ 的 6.2.3（先升级 FXOS）
使用 FDM 的 Firepower 威胁防御（所有平台）	6.2.3
使用 ASDM 的 ASA FirePOWER	6.2.3

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 6.5.0 的时间和磁盘空间

表 *34:* 版本 *6.5.0* 的时间和磁盘空间

平台	/Volume 上的空间	/ 上的空间	FMC 上的空间	时间
FMC	18.6 GB	24 MB	-	47 分钟
FMCv：VMware 6.0	18.7 GB	30 MB	-	35 分钟
Firepower 1000 系列	1 GB	11.3 GB	1.1 GB	10 分钟
Firepower 2100 series	1.1 GB	12.3 GB	1 GB	12 分钟
Firepower 4100 系列	20 MB	10.8 GB	990 MB	8 分钟
Firepower 9300	23 MB	10.9 GB	990 MB	8 分钟
具有 ASA 5500-X 系列的 FTD	10.4 GB	120 KB	1.1 GB	17 分钟
FTDv：VMware 6.0	10 GB	120 KB	1.1 GB	10 分钟
ASA FirePOWER	12.2 GB	26 MB	1.3 GB	81 分钟
NGIPSv：VMware 6.0	6.6 GB	22 MB	870 MB	9 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 *35: 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 *36: 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

接口配置		流量行为
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额外要求。

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 *37: 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 *38: 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 *39: 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

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 *40: 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 *41: 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 *42: 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。

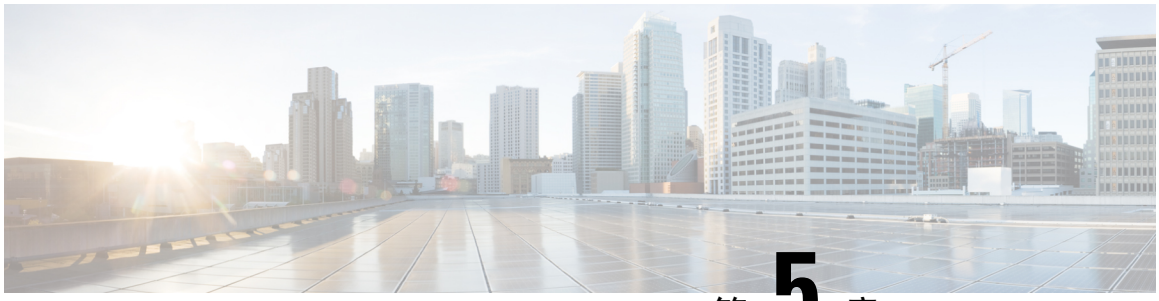
- Firepower 管理中心，包括FMCv：https://www.cisco.com/go/firepower-software
- Firepower 威胁防御 (ISA 3000)： https://www.cisco.com/go/isa3000-software
- Firepower 威胁防御（所有其他型号，包括 FTDv）：https://www.cisco.com/go/ftd-software
- 具备 FirePOWER 服务的 ASA（ASA 5500-X 系列）： https://www.cisco.com/go/asa-firepower-sw
- 具备 FirePOWER 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 *43:* 升级包 版本 *6.5.0*

平台	数据包
FMC/FMCv	Cisco_Firepower_Mgmt_Center_Upgrade-版本-内部版本.sh.REL.tar
Firepower 1000 系列	Cisco_FTD_SSP_FP1K_Upgrade-版本-内部版本.sh.REL.tar

平台	数据包
Firepower 2100 系列	Cisco_FTD_SSP_FP2K_Upgrade-版本-内部版本.sh.REL.tar
Firepower 4100/9300 机箱	Cisco_FTD_SSP_Upgrade-版本-内部版本.sh.REL.tar
ASA 5500-X 系列，含 FTD ISA 3000，含 FTD Firepower Threat Defense Virtual	Cisco_FTD_Upgrade-版本-内部版本.sh.REL.tar
ASA FirePOWER	Cisco_Network_Sensor_Upgrade-版本-内部版本.sh.REL.tar
NGIPSv	Cisco_Firepower_NGIPS_Virtual_Upgrade-版本-内部版本.sh.REL.tar



第 5 章

全新安装 版本 6.5.0

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。

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 *44:* 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。 **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。

场景	解决方案	许可
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。

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 71 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。您只能从运行相同 *Firepower* 版本且具有相同 VDB 的设备还原备份。在大多数情况下，只能还原到同一模型；请参阅《Firepower 管理中心型号迁移指南》了解例外情况。

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（接受 EULA 即表示您同意 Web 分析跟踪），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：DC2000 和 4000。如果您当前在运行版本 5.x 并需要全新安装版本 6.5.0，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的虚拟帐户中删除，从云和云服务取消注册，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。
- 型号迁移期间关闭源 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 点击**设备**，然后点击“智能许可证”摘要中的**查看配置**。

步骤 3 从齿轮下拉列表中选择**注销设备**。

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 *45: 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

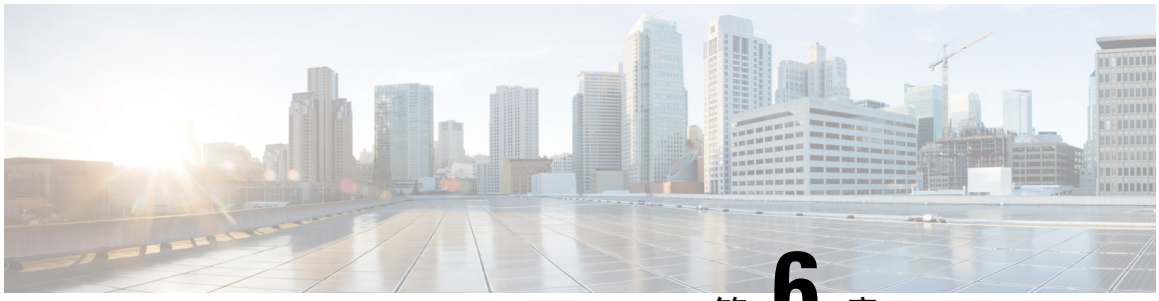
FMC 平台	指南
FMCv及 FMCv 300	《思科 Firepower Management Center Virtual 快速入门指南》

表 *46: 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 Firepower Threat Defense Virtual 入门指南》
FTDv：KVM	《适用于 KVM 部署的思科 Firepower Threat Defense Virtual 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 *47: NGIPSvASA FirePOWER* 安装说明

NGIPS 平台	指南
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 6 章

文档

以下主题提供 Firepower 文档：

更新的文档 版本 6.5.0

针对至少一个版本 6.5.0修补程序更新了以下 Firepower 文档：

- 思科 Firepower 兼容性指南

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 75 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 6.5.0。 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 75 页。

Firepower 配置指南和联机帮助

- Firepower 管理中心配置指南（版本 6.5）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 6.5.0）和联机帮助
- 具备 FirePOWER 服务的思科 ASA 本地管理配置指南（版本 6.5）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，2.7(1)
- 思科 Firepower 4100/9300 FXOS CLI 配置指南，2.7(1)

- 思科 Firepower 4100/9300 FXOS 命令参考
- 思科 Firepower 4100/9300 FXOS 发行说明，2.7(1)

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》

迁移指南

- 《Firepower 管理中心型号迁移指南》全新

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》
- 《1000、2500 和 4500 型思科 Firepower 管理中心入门指南》
- 《750、1500、2000、3500 和 4000 型思科 Firepower 管理中心入门指南》
- 《思科 Firepower Management Center Virtual 快速入门指南》
- 《适用于 VMware 的思科 Firepower Threat Defense Virtual 入门指南》
- 适用于 Microsoft Azure 云的思科 Firepower 威胁防御虚拟快速入门指南
- 《思科 ISA 3000 入门指南》全新
- 《思科 Firepower 1010 入门指南》
- 《思科 Firepower 1100 系列入门指南》
- 《思科 Firepower 2100 系列入门指南》 最新
- 《思科 Firepower 4100 入门指南》
- 《思科 Firepower 9300 入门指南》

API 和集成指南

- Firepower 管理中心 REST API 快速入门指南，版本 6.5.0
- 思科 Firepower 威胁防御 REST API 指南
- Firepower 系统事件流转换器集成指南，版本 6.5.0
- 《Firepower 系统主机输入 API 指南 v6.5》
- 《思科 Firepower 用户代理配置指南，版本 2.5》

- 《Firepower 和思科威胁响应集成指南》

《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

许可和开放源代码

- 思科 Firepower 系统功能许可证
- Firepower 许可相关常见问题解答 (FAQ)
- Firepower 版本 6.5.0 中使用的开源

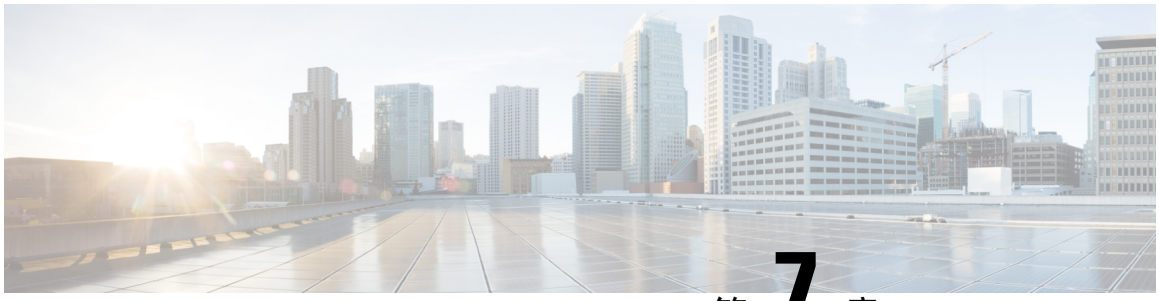
故障排除和配置示例

- 思科 Firepower 威胁防御系统日志消息
- 在 Firepower 4100/9300 上使用多实例功能全新
- 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 7 章

已解决的问题

当此 Firepower 版本最初发布时，此处所列的错误被证实已解决。

注释 为方便起见，本文档提供此版本的已解决漏洞列表。此列表自动生成一次，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

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 6.5.0：

- 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，您必须重新映像。

使用此表确定新版本 6.5.0版本是否适用于您的平台。

表 *48:* 版本 *6.5.0* 新版本

新内部版本	已发布	软件包	平台	解决
120	2019-10-08	升级	FMC	CSCvr47499：Firepower FMC 升级故障在 800_post/1028_latency_settings_upgrade. pl 中 在多域部署中，使用版本 6.5.0-120 升级软件包。有关详细信息，请参阅使用版本 6.5.0-120 升级多域 FMC，第 32 页。

版本 6.5.0 已解决的问题

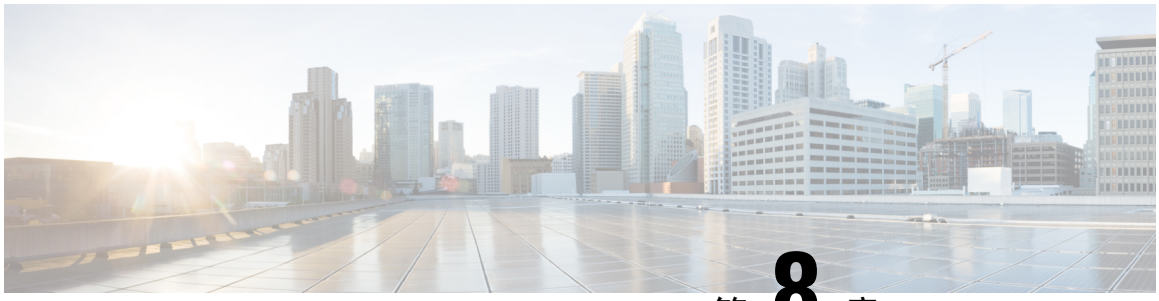
表 *49:* 版本 *6.5.0* 已解决的问题

漏洞 ID	标题
CSCvc88690	5.4.x AC 管理员和根规则组仍是 6.x 用户角色，并且具有完全权限
CSCvd80045	从“运行状况策略”页面切换域时出错
CSCvd87211	尝试删除配置的捕获时发生 ASA 回溯
CSCvh16358	无法在 CLI 上取消命令
CSCvh65500	FTP 主动模式下的 Firepower 2100 客户端无法与服务器建立控制通道
CSCvh78264	即使 FMC 已配置显式 HTTP 代理，Clamupdates 也需要运行 DNS
CSCvi01404	ssl 检查策略可能导致使用 ECDSA 签名证书的站点失败
CSCvi23774	Firepower 建议更新不考虑已转移至无效状态的第三方漏洞
CSCvi47847	未通过 Firepower 检测到外壳应用程序
CSCvi73452	byte_math 从 byte_extract 提取到空值会导致拒绝服务
CSCvi93955	未检测到安全信头 - CWE-693：保护机制故障
CSCvi95403	缺少第 5 级通知字符串。
CSCvj27949	FMC 在夏季没有使用正确的时区校正。
CSCvj53804	由于 icmp 事件域 ID 损坏，软件升级到 6.2.3 失败

漏洞 ID	标题
CSCvj70886	API-Explorer 必须支持 4096 位证书
CSCvj73432	NTP 将 Eth0 IP 地址从 Eth1 接口发送出去
CSCvj74441	在 ASDM 上通过 CLI 安装 SRU 时不会更新 /etc/sf/sru_versions 中的版本详细信息。
CSCvj91418	Cisco FTD 软件 SMB 协议预处理器检测引擎低系统内存 DoS 漏洞
CSCvk16568	如果检测到应用程序 ID，则 AppID 停止处理流量
CSCvk21405	外壳应用程序不从服务器对新配置进行 pin holing 处理
CSCvk56513	当通过代理传递流量时，Tor 未被阻止。
CSCvk58188	因 max_sessions 的指定值超出界限而导致 Snort 配置验证失败
CSCvk63804	在按计划处理更新建议的规则时，启用敏感数据检测
CSCvk66669	FPR2100：配置 ssl 协议不会更改 FDM GUI 证书的配置
CSCvm31905	OpenSSH Bailout 延迟用户枚举漏洞
CSCvm80434	在具有大量用户时，FMC GUI 发生性能降级
CSCvm84357	活动传输模式的文件事件源和目标不正确
CSCvm89006	FTD：FTD converged_cli 中配置命令“配置用户添加”的系统日志
CSCvn12373	FMC HA 的 rna_attribute dup 键上的策略部署失败
CSCvn31390	计算处理器 PortSmash 侧通道信息披露漏洞
CSCvn31886	使用 TLS 1.3 进行 SSL 检查会导致不解密流量以执行会话未缓存的操作
CSCvn38101	这样针对 nat 与备用地址重叠情况的 ui 检查
CSCvn57267	安全情报包含重复对象
CSCvn73998	包含等号的 OSPFv2 md5 密码在第二次部署期间被删除。
CSCvn75713	FMC 上的 CVE Nmap 版本
CSCvn75722	FMC 上的 CVE Nmap 版本
CSCvn75729	FMC 上的 CVE Nmap 版本
CSCvn78076	Firepower：关于系统 -> 监控 -> 统计信息下显示的“内存使用率”，存在误导性统计信息
CSCvn80464	警报配置不正确跟踪使用中的策略

漏洞 ID	标题
CSCvo11077	当我们建立和终止新的 IKEv1 隧道时，在 IPsec 中发现内存泄漏。
CSCvo30347	UI 错误 - 扩展访问列表对象拖放不起作用
CSCvo37273	在 FMC UI 中添加验证检查，以验证在静态路由中配置的对象网络
CSCvo39231	由于 CSM 侧的过时条目，部署策略选项卡未能从 FMC 填充设备列表
CSCvo39356	线程名称 IP Address Assign 出现回溯
CSCvo40478	因为 FMC 最新的产品更新，FMC 控制板显示的值不正确
CSCvo43260	强制部署应仅加载当前设备，而不是检查所有已注册设备
CSCvo43311	无法保存 VPN 站点到站点策略，出现错误“拓扑中存在未知终端”
CSCvo48400	FTD 升级称已成功，但并非如此。
CSCvo49295	RabbitMQ 经常无法启动，出现错误“case_clause,undefined”
CSCvo57287	FMC：无法使用 apiuser 凭证登录 RESTAPI UI
CSCvo59424	FMC UI 不允许为 FTD 集群的诊断接口分配 IP 地址
CSCvo59683	大量过时的 IPList 对象导致高 CPU 使用率
CSCvo61418	当事件表的大小和数量很大时，FMC 事件恢复会失败。
CSCvo65521	由于 TID 目录不正确，还原备份失败
CSCvo66575	pxGrid 与 ISE 2.6 以及 ISE 2.4p6 和 2.3p6 的连接断开
CSCvo66732	修补程序更新期间的自动 SRU 下载可能会导致更新失败
CSCvo70169	[FMC 6.3] 显示规则冲突，它不起作用
CSCvo72659	对现有关联规则所做的编辑不生效。
CSCvo74786	进程管理器在非正常退出时不跟踪 Mojo 进程
CSCvo74802	进程管理器不按预期处理非托管进程
CSCvo74833	由于未跟踪的文件，Firepower 设备上的非托管磁盘空间很大
CSCvo77024	由于 https://nvd.nist.gov/vuln/detail/CVE-2015-9251，需要升级 FMC Jquery
CSCvo92100	FMC 在平台设置下允许 SNMP 的社区字符串存在空格
CSCvo92913	Cisco Firepower 管理中心 RSS 跨站脚本漏洞
CSCvp26173	FMC：为主机输入客户端 TCP 8307 端口 永久禁用 TLS 1.0

漏洞 ID	标题
CSCvp26548	由于对象验证失败，FDM 升级失败
CSCvp31204	snmp 社区字符串不接受特殊字符
CSCvp39970	/var/opt/CSCOpx/MDC/tomcat/log/stdout.logs 编写过多日志消息，可能会填满磁盘
CSCvp43987	运行状况策略运行时间隔应小于运行状况监控器进程警报阈值
CSCvp50929	备份恢复后，FMC 显示错误的许可证密钥
CSCvp58287	连接事件的“交换工作流程”中存在 FMC GUI 错误
CSCvp66802	升级 6.4.0.1-14 时，QP-HA 失败
CSCvp66941	如果用户具有现有会话，并且密码中包含空格，则 FMC 登录会失败
CSCvp81615	删除域时，会删除路由配置。
CSCvp82265	在形成 FMC HA 后记录的错误 uuidprefix 导致编辑对象时出错
CSCvp90060	在最新的 Firepower SRU 更新 (24.05.2019) 后，RDP 连接失败
CSCvp99930	在主设备主用状态下，部署失败且发生 sftunnel 异常。
CSCvq05335	由于 NFS 远程存储未响应，FMC 在启动过程中停滞
CSCvq07624	在 rest API 中配置的 s2s vpn 具有非匹配 ID
CSCvq12173	配置有回应应答 ICMP(1):0 参数的规则未触发
CSCvq18237	文档错误 - FMC HA 配置指南 - 软件要求不正确
CSCvq21935	运行 6.3.0.3 的 FTD 在 DATAPATH 上发生回溯
CSCvq25791	未正确描述在文件高级设置上启用干净列表的策略。
CSCvq27739	如果 SSH 服务器配置为保存覆盖文件的副本，则备份到远程 SSH 存储失败
CSCvq30298	部署统计文件不会轮换，这可能导致其变得非常大
CSCvq36042	丢失的心跳导致重新加载
CSCvq76785	当身份验证中存在未处理的错误时，用户名和密码将打印到日志中
CSCvq79042	由于来自服务器的 DNS 响应较大且被截断，导致 FQDN ACL 条目不完整
CSCvq87585	在重复 50000 次运行 ping 后，Clish 将不响应且 CPU 核心使用率高
CSCvr35956	组合 ServerKeyExchange 和 ClientKeyExchange 失败时阻止双重释放 --> lina 崩溃



第 8 章

已知问题

当此 Firepower 版本最初发布时，此处所列的错误即已知存在。

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 6.5.0：

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

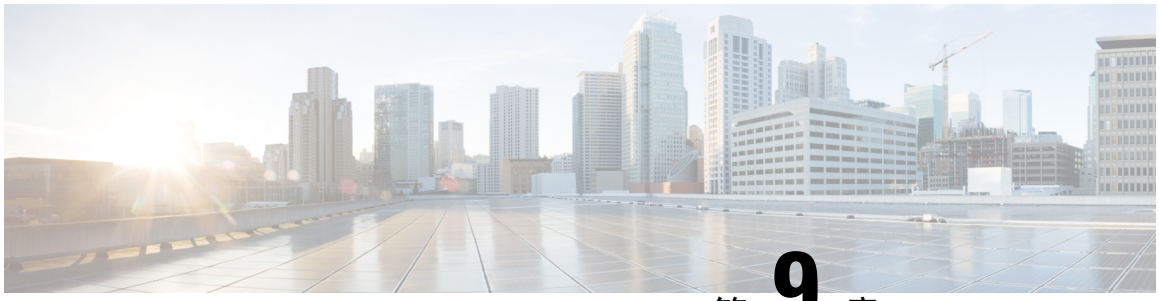
可以将搜索范围限制为影响特定 Firepower 平台和版本的错误。还可以按错误 ID 搜索或者搜索特定关键字。

版本 6.5.0已知问题

表 *50:* 版本 *6.5.0* 已知问题

漏洞 ID	标题
CSCvq03466	ISA 3000 FTD 部署失败，硬件旁路已激活
CSCvq11310	FTD 性能已丢弃大约 5% 的 6.5 SRTS 运行
CSCvq30293	FTD 版本降级后，引导程序配置未更新
CSCvq47804	从 FDM 关闭后，FXOS 安全模块不会启动。

漏洞 ID	标题
CSCvq70849	在高可用性对中部署时，从 6.4 升级到 6.5 FDM 失败
CSCvq91091	在 1024B 和 MaxCPS 测试中，ASA 55xx-x 系列在 6.5 上执行的速度比预期要慢
CSCvr09194	FXOS 升级后已找到 core. run_hm. pl
CSCvr17786	API GET 使用 HitCount "true" 和过滤器 "fetchZeroHitCount" 调用访问策略时返回所有规则
CSCvr21119	在 FP1000 设备上发出 SSD 安全擦除 cmd 时，添加电源周期消息
CSCvr22260	常规压力下 IkeAddFailEntry 中的 line 在 ike_mib.c:578 中重新加载
CSCvr23986	在 mh_magic_verify 中以及在负载下的 SrDoMgmt 中触发的断言
CSCvr24059	源 SGT 关联不适用于 FMC 和 FTD 6.5
CSCvr28977	FTD：即使在 API 中关闭 API，也会下载 API 自动恶意软件更新
CSCvr34163	当 FTD 处于路由或透明模式时，不应在入侵事件下看到 VLAN ID
CSCvr35470	FMCv-6.5.0 上的 CloudAgent 核心
CSCvr37728	在一个角落中重新连接到 ISE 后，ADI 进程可能会崩溃和核心
CSCvr39516	modexp-octeon 中 malloc 故障导致 lina 分段故障/重新加载
CSCvr39818	FTD：将接口 IP 从静态交换到 DHCP 会导致 FTD 使用不同的 DHCP 客户端 ID
CSCvr46892	在模式之间切换后，接口保持关闭状态
CSCvr47499	800_post/1028_latency_settings_upgrade. pl 中出现 Firepower FMC 升级故障



第 9 章

获取帮助

感谢选择 Firepower。

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