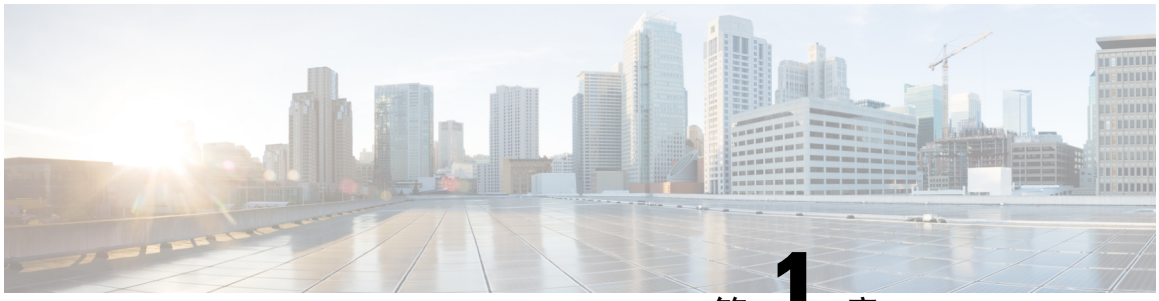
思科 Firepower 发行说明，版本 6.4.0

首次发布日期: 2019 年 4 月 24 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 6.4.0

感谢选择 Firepower。

关于发行说明

发行说明提供了关于版本 6.4.0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。

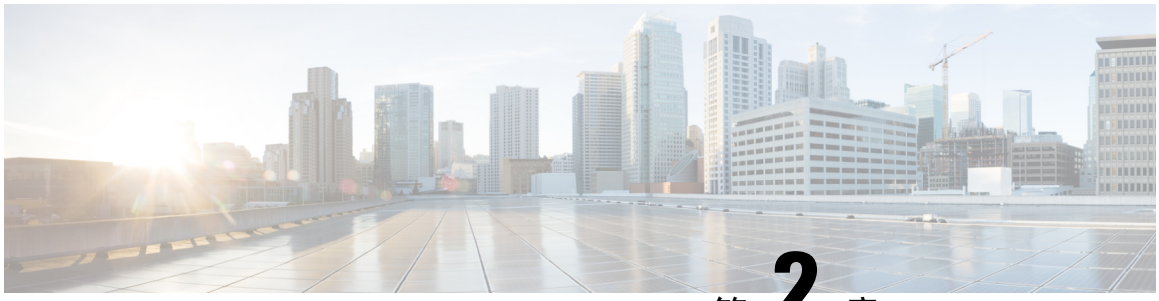
升级或全新安装（重新映像）Firepower 部署可能是一个复杂的过程。在这里，发行说明并未提供具体的说明，而是提供了指向对应资源的链接。有关升级和安装说明的链接，请参阅：

发布日期

有关随版本 6.4.0提供的所有平台的列表，请参阅兼容性，第 3 页。

表 *1:* 版本 *6.4.0* 发行日期

内部版本号	日期	平台
102	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
	2019-06-13	Firepower 1010、1120 和 1140
	2019-04-24	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 6.4.0Firepower 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* 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* 管理器-设备的兼容性

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

版本 6.4.0 的设备	要求	6.4.0 版 FMC
Firepower 设备管理器		
版本 6.4.0 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 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 **Include local directory path when uploading files to server** 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

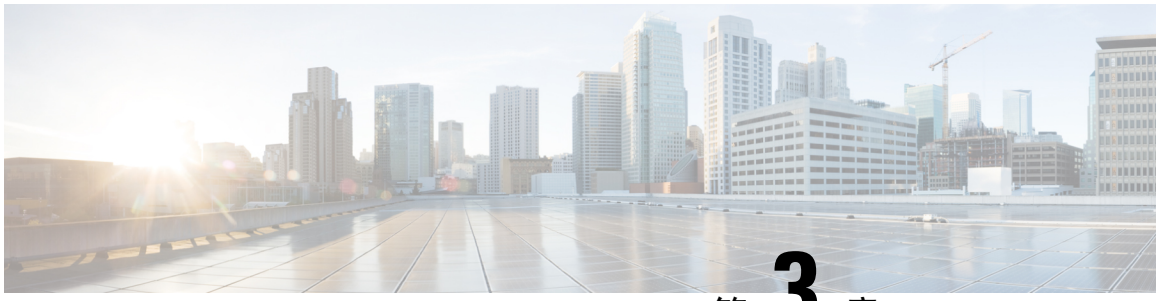
某些浏览器扩展（例如，Grammarly 和 Whatfix 编辑器）可以防止您在 PKI 对象中的证书和密钥等字段中保存值。这些扩展名在字段中插入字符（例如 HTML），这会导致 FMC 将其视为无效。我们建议您在使用 FMC 时禁用这些扩展。

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

接口	分辨率
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 6.4.0包括：

新功能

以下主题列示了 Firepower 版本 6.4.0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 版本说明查看过去的新功能列表。

Firepower 管理中心/Firepower 版本 6.4.0 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 6.4.0 中可用的新功能：

表 *6:* 版本 *6.4.0* 新增功能：*FMC* 部署

功能	说明
硬件和虚拟硬件	
FMC型号 MC1600、2600 和 4600	我们推出了 Firepower 管理中心型号 MC1600、2600 和 4600。请注意，这些型号也支持 6.3.x。
FMCv（位于 Azure 上）	我们将 Firepower 管理中心虚拟引入到 Microsoft Azure 上。
FTD（位于 Firepower 1010、1120 和 1140 上）	我们推出了 Firepower 1010、1120 和 1140。
FTD（位于 Firepower 4115、4125 和 4145 上）	我们推出了 Firepower 4115、4125 和 4145。

功能	说明
Firepower 9300 SM-40、SM-48 和 SM-56 支持	我们推出了三个安全模块：SM-40、SM-48 和 SM-56。
ASA 和 FTD（位于同一 Firepower 9300 上）	您现在可以在同一个 Firepower 9300 上同时部署 ASA 和 FTD逻辑设备。需要 FXOS 2.6.1。
许可	
新许可功能，适用于 ISA 3000	对于 ASA FirePOWER 和 FTD部署，ISA 3000 现支持 URL 过滤和恶意软件许可证及其相关功能。 仅对于 FTD，ISA 3000 现在还支持为经过核准的客户预留特定许可证。 支持的平台： ISA 3000
Firepower 威胁防御 路由	
OSPFv2 路由的轮换式（密钥链）身份验证	现在，您可以在配置 OSPFv2 路由时使用轮换式（密钥链）身份验证。 新增/修改的屏幕： • **Objects** > **Object Management** > **Key Chain** 对象 • **Devices** > **Device Management** > edit device **> Routing** 选项卡 **> OSPF** settings **> Interface** 选项卡 > add/edit interface > **Authentication** 选项 • **Devices** > **Device Management >** edit device **> Routing** 选项卡 **> OSPF** settings **> Area** 选项卡 **>** add/edit area **> Virtual Link** 子选项卡 **>** add/edit virtual link **> Authentication** 选项 支持的平台： FTD
Firepower 威胁防御 加密和 VPN	
RA VPN：辅助身份验证	辅助身份验证（也称为双重身份验证）通过使用两个不同的身份验证服务器，为 RA VPN 连接额外添加了一层安全性。启用辅助身份验证后，AnyConnect VPN 用户必须提供两组凭证才能登录 VPN 网关。 RA VPN 支持仅 AAA 和客户端证书以及 AAA 身份验证方法的辅助身份验证。 新增/经修改的屏幕：**Devices** > **VPN** > **Remote Access >** add/edit configuration **> Connection Profile > AAA** 区域 支持的平台： FTD

功能	说明
站点到站点VPN：外联网终端的动态 IP 地址	您现在可以配置站点到站点 VPN 以使用外联网终端的动态 IP 地址。在中心辐射型部署中，可以将集线器用作外联网终端。 新增/经修改的屏幕：**Devices** > **VPN** > **Site To Site >** add/edit FTD VPN topology **> Endpoints** 选项卡 **>** add endpoint **> IP Address** 选项 支持的平台： FTD
站点到站点VPN：用于点对点拓扑的动态加密映射	您现在可以在点对点以及中心辐射型VPN拓扑中使用动态加密映射。全网状拓扑仍不支持动态加密映射。 配置拓扑时需指定加密映射类型。确保同时为拓扑中的对等设备之一指定动态 IP 地址。 新增/经修改的屏幕：**Devices** > **VPN** > **Site To Site >** add/edit FTD VPN topology **> IPsec** 选项卡 **> Crypto Map Type** 选项 支持的平台： FTD
TLS 加密加速	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。版本 6.4 升级进程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。但是，如果您使用的是 Firepower 4100/9300 机箱的多实例功能，则可以为每个模块/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。 Firepower 4100/9300 机箱的新 FXOS CLI 命令： • **show hwCrypto** • **config hwCrypto** 新增的 FTD CLI 命令： • **show crypto accelerator status**（取代 **system support ssl-hw-status**） 删除的 FTD CLI 命令： • **system support ssl-hw-accel** • **system support ssl-hw-status** 支持的平台：Firepower 2100 系列、Firepower 4100/9300 机箱
事件、日志记录和分析	

功能	说明
针对文件和恶意软件事件系统日志消息的改进	现在可以通过系统日志从受管设备发送完全限定的文件和恶意软件事件数据。 新增/经修改的屏幕：**Policies** > **Access Control** > **Access Control** > add/edit policy > **Logging** 选项卡 > **File and Malware Settings** 区域 支持的平台：任意
按 CVE ID 搜索入侵事件	现在可以搜索由于特定 CVE 漏洞而引起的入侵事件。 新增/经修改的屏幕：**Analysis** > **Search** 支持的平台： FMC
系统日志中现包括 IntrusionPolicy 字段	入侵事件系统日志消息现在指定触发事件的入侵策略。 支持的平台：任意
思科威胁响应 (CTR) 集成	思科 Threat Response是一款全新的思科云产品，可帮助您快速检测、调查和响应威胁。通过 CTR，您可以联合来自多个产品（包括 Firepower 威胁防御）的数据来分析事件。有关详细信息，请参阅《Firepower 和思科威胁响应集成指南》。 新增/经修改的屏幕：**System** > **Integration** > **Cloud Services** 支持的平台： FTD
Splunk 集成	Splunk 用户可以使用新的独立 Splunk 应用程序 Cisco Firepower App for Splunk分析事件。可用功能受 Firepower 版本的影响。 支持的平台： FMC
管理	
VMware 上的 FTDv 默认为 vmxnet3 接口	创建虚拟设备时，VMware 上的 FTDv 现在默认为 vmxnet3 接口。先前，默认值为 e1000。vmxnet3 设备驱动器和网络处理与 ESXi 虚拟机监控程序集成，因此其使用更少的资源并提供更好的网络性能。 **注释** 如果您使用的是 e1000 接口，我们强烈建议您切换。如需详细信息，请参阅《适用于 VMware 的思科虚拟 Firepower 威胁防御入门指南》中有关添加和配置 VMware 接口的说明。 支持的平台：VMware 上的 FTDv

功能	说明
能够在管理接口上禁用重复地址检测 (DAD)	启用 IPv6 后，可以禁用 DAD。您可能希望禁用 DAD，因为使用 DAD 可能会导致拒绝服务攻击。如果禁用此设置，则需要手动检查此接口是否未使用已分配的地址。 新增/经修改的屏幕：**System** > **Configuration** > **Management Interfaces** > **Interfaces** 区域 **>** edit interface **> IPv6 DAD** 复选框 支持的平台：FMC、7000 和 8000 系列
能够在管理接口上禁用 ICMPv6 回应应答和目的地不可达消息	启用 IPv6 后，此时您可以禁用 ICMPv6 回应应答和目的地不可达消息。您可能希望禁用这些数据包以防止潜在的拒绝服务攻击。禁用回应应答数据包意味着无法使用 IPv6 ping 到设备管理接口，以进行测试。 新增/修改的屏幕： **System** > **Configuration** > **Management Interfaces** > **ICMPv6** 新增/经修改的命令： • **configure network ipv6 destination-unreachable** • **configure network ipv6 echo-reply** 支持的平台：FMC（仅限 Web 界面）、受管设备（仅限 CLI）
对 RADIUS 服务器上定义的 FTD 用户的 Service-Type 属性的支持	对于 FTDCLI 用户的 RADIUS 身份验证，以往，您须预定义 RADIUS 外部身份验证对象中的用户名，且须手动确保该列表匹配 RADIUS 服务器上定义的用户名。现在，您可以使用 Service-Type 属性在 RADIUS 服务器上定义 CLI 用户，亦可同时定义“基本”和“配置”用户角色。要使用此方法，请务必将外部身份验证对象中的外壳访问过滤器留空。 新增/经修改的屏幕：**System** > **Users** > **External Authentication** 选项卡 **>** add/edit external authentication object **> Shell Access Filter** 支持的平台： FTD
查看对象使用情况	现在，您可以通过对象管理器查看使用网络、端口、VLAN 或 URL 对象的策略、设置和其他对象。 新增/经修改的屏幕：**Objects > Object Management >** choose object type **>** Find Usage（双筒望远镜）图标 支持的平台： FMC

功能	说明
签名的 SRU、VDB 和 GeoDB 更新（增强的安全性）	因此，Firepower 可以验证您使用的是正确的更新文件，版本 6.4+ 使用签名的入侵规则 (SRU)、漏洞数据库 (VDB) 和地理位置数据库 (GeoDB) 更新。早期版本继续使用未签名的更新。除非您从思科支持和下载站点手动下载更新 - 例如，在物理隔离部署中 - 否则您应该不会察觉到功能上的任何差异。 但是，如果您手动下载并安装 SRU、VDB 和 GeoDB 更新，请确保为当前版本下载正确的软件包。版本 6.4+ 的签名更新文件以“Cisco”（而不是“Sourcefire”）开头，以 .sh.REL.tar（而不是 .sh）结尾： • SRU：Cisco_Firepower_SRU-日期-内部版本-vrt.sh.REL.tar • VDB：Cisco_VDB_Fingerprint_Database-4.5.0-版本.sh.REL.tar • GeoDB：Cisco_GEODB_Update-日期-内部版本.sh.REL.tar 版本 5.x 至 6.3 的更新文件仍然使用旧的命名方案： • SRU：Sourcefire_Rule_Update-日期-内部版本-vrt.sh • VDB：Sourcefire_VDB_Fingerprint_Database-4.5.0-版本.sh • GeoDB：Sourcefire_Geodb_Update-日期-内部版本.sh 我们将同时提供签名和未签名的更新，直到对需要未签名更新的版本的支持结束为止。 不要解压签名的 (.tar) 包。 **注释** 如果您意外将已签名的更新上传到较早的 FMC 或 ASA FirePOWER 设备，则必须手动将其删除。离开软件包会占用磁盘空间，并且还可能导致未来升级出现问题。 支持的平台：任意
受管设备的预定远程备份	您现在可以使用 FMC 来预定某些受管设备的远程备份。以前，只有 Firepower 7000/8000 系列设备支持预定备份，且必须使用设备的本地 GUI。 新增/经修改的屏幕：**System** > **Tools** > **Scheduling** > add/edit task > 选择 **Job Type: Backup** > 选择 **Backup Type** 支持的平台：FTD物理平台、适用于 VMware 的 FTDv、Firepower 7000/8000 系列 例外：不支持 FTD群集设备或容器实例
监控和故障排除	

功能	说明
URL 过滤监控器改进	您可以配置 URL 过滤监控器警报的时间阈值。 新增/经修改的屏幕：**System** > **Health** > **Policy >** add/edit policy > **URL Filtering Monitor** 支持的平台：任意
访问控制和预过滤规则的命中计数	您现在可以访问您的 FTD 设备上的访问控制和预过滤规则命中计数。 新增/修改的屏幕： • **Policies** > **Access Control** > **Access Control >** add/edit policy > **Analyze Hit Counts** • **Policies** > **Access Control** > **Prefilter >** add/edit policy > **Analyze Hit Counts** 新增的命令： • **show rule hits** • **clear rule hits** • **cluster exec show rule hits** • **cluster exec clear rule hits** • **show cluster rule hits** 经修改的命令： • **show failover** 现在包含与高可用性对等设备之间的同步命中计数相关的对象静态计数 支持的平台： FTD
基于连接的故障排除	基于连接的故障排除或调试可跨模块提供统一调试，以收集特定连接的相应日志。它还支持最多 7 级的基于级别的调试，并为 lina 和 Snort 日志启用统一的日志收集机制。 新增/经修改的命令： • **clear packet debugs** • **debug packet start** • **debug packet stop** • **show packet debugs** 支持的平台： FTD

功能	说明
新的思科成功网络监控功能	新增了以下思科成功网络监控功能： • CSPA（思科安全数据包分析器）查询信息 • FMC 上启用了上下文交叉启动实例 • TLS/SSL 检查事件 • Snort 重新启动 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。您可以随时选择加入或退出。 支持的平台： FMC
Firepower 管理中心 REST API	
新的 REST API 功能	添加了 REST API 对象以支持版本 6.4 的功能： • cloudeventsconfigs：管理思科威胁响应集成。 • ftddevicecluster：管理机箱群集。 • hitcounts：管理访问控制和预过滤规则的命中计数统计信息。 • keychain：管理配置 OSPFv2 路由时，用于轮换式身份验证的密钥链对象。 • loggingsettings：管理访问控制策略的日志记录设置 支持的平台： FMC
基于 OAS 的 API Explorer	版本 6.4 使用基于 OpenAPI 规范 (OAS) 的 API Explorer。作为 OAS 的一部分，您现在可以使用 CodeGen 生成示例代码。如果愿意，您仍然可以访问旧版 API Explorer。 支持的平台： FMC
性能	
Snort 重新启动改进	在版本 6.4 之前，Snort 重新启动期间，系统会丢弃与“不解密”SSL 规则或默认策略操作匹配的加密连接。现在，只要您没有禁用大流量负载分流或 Snort 保留连接，已路由/透明流量不经检查即会通过而不会被丢弃。 支持的平台：Firepower 4100/9300

功能	说明
选定 IPS 流量的性能改进	出口优化是针对所选IPS流量的性能特征。此功能默认在所有FTD平台上启用。 版本 6.4 升级进程可在符合条件的设备上启用出口优化。有关详细信息，请参阅《思科Firepower威胁防御命令参考》。要排查与出口优化相关的问题，请联系思科 TAC。 支持的平台： FTD 新增/经修改的命令： • **asp inspect-dp egress optimization** • **show asp inspect-dp egress optimization** • **clear asp inspect-dp egress optimization** • **show conn state egress_optimization**
更快的 SNMP 事件记录	将入侵和连接事件发送到外部 SNMP 陷阱服务器时的性能改进。 支持的平台：任意
更快的部署	设备通信和部署框架的改进。 支持的平台： FTD
更快的升级	事件数据库改进。 支持的平台：任意

Firepower 设备管理器/FTD6.4.0 版本中的新增功能

发布日期：2019 年 4 月 24 日

下表列出了在使用 Firepower 设备管理器进行配置时 FTD6.4.0 中可用的新功能：

表 *7:*

功能	说明
Firepower 1000 系列设备配置。	您可以在 Firepower 1000 系列设备上使用 Firepower 设备管理器配置 Firepower 威胁防御。 请注意，您可以将以太网供电 (PoE) 端口当做常规以太网端口来进行配置和使用，但您不能启用或配置任何 PoE 相关的属性。

功能	说明
适用于 ISA 3000 的硬件旁路。	现在，您可以在 **Device** > **Interfaces** 页面上配置适用于 ISA 3000 的硬件旁路。在版本 6.3 中，您需要使用 FlexConfig 配置硬件旁路。如果您正在使用 FlexConfig，请在 Interfaces 页面上重新配置并从 FlexConfig 中删除硬件旁路命令。但是，我们仍建议保留 FlexConfig 中用于禁用 TCP 序列号随机化的部分。
能够从 FDM CLI 控制台重新启动和关闭系统。	现在，可以通过 FDM 中的 CLI 控制台发出 **reboot** 和 **shutdown** 命令。先前，需要打开与设备的单独 SSH 会话，以重新启动或关闭系统。要使用这些命令，必须具有管理员权限。
使用 RADIUS 对 FTDCLI 用户进行外部身份验证和授权	您可以使用外部 RADIUS 服务器对登录到 FTD CLI 的用户进行身份验证和授权。您可以为外部用户提供配置（管理员）或基本（只读）权限。 在 **Device** > **System Settings** > **Management Access** 页面上的 **AAA Configuration** 选项卡中增加了 SSH 配置。
对网络范围对象和嵌套网络组对象的支持。	您现在可以创建指定一系列 IPv4 或 IPv6 地址的网络对象和包括其他网络组（即，嵌套组）的网络组对象。 修改了网络对象和网络组对象 Add/Edit 对话框以增加这些功能，并且修改了安全策略以允许使用这些对象，具体取决于相应类型的地址规范是否适用于策略情景。
对象和规则的全文本搜索选项。	您可以在对象和规则中执行全文本搜索。通过搜索包含大量条目的策略或对象列表，您可以找到规则或对象中包含搜索字符串的所有条目。 在具备规则的所有策略中以及 **Objects** 列表中的所有页面上都添加了一个搜索对话框。此外，您还可以使用 API 内受支持对象 GET 调用中的**filter=fts~**搜索字符串选项来根据全文本搜索检索条目。
获取 FDM 管理 FTD 设备支持的 API 版本列表。	您可以使用 GET/api/版本 (ApiVersions) 方法获取设备支持的 API 版本列表。您可以在 API 客户端上使用任何受支持版本支持的命令和语法来与设备通信和配置设备。
FTDREST API 版本 3 (v3)。	软件版本 6.4 的 FTDREST API 已升级到第 3 版。必须将 API URL 中的第 1 版/第 2 版替换为第 3 版。第 3 版 API 包括涵盖软件版本 6.4 中所有新增功能的许多新资源。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（您可以在其中查看资源），登录后请将 Firepower 设备管理器 URL 的末尾改为 **/#/api-explorer**。

功能	说明
访问控制规则的命中计数。	您现在可以查看访问控制规则的命中计数。命中计数表示连接与规则匹配的频率。 更新了访问控制策略，在其中加入了命中计数信息。在 FTD API 中的 GET Access Policy Rules 资源中添加了 HitCounts 资源以及 **includeHitCounts** 和 **filter=fetchZeroHitCounts** 选项。
适用于动态编址和证书身份验证的站点间 VPN 增强功能。	您现在可以配置站点间VPN连接，从而使用证书而非预共享密钥来进行对等体身份验证。您还可以配置其远程对等体包含未知（动态）IP 地址的连接。在站点间 VPN 向导和 IKEv1 策略对象中新增了一些选项。
支持RADIUS服务器和远程接入 VPN 中的授权更改。	您现在可以使用 RADIUS 服务器对远程接入 VPN (RA VPN) 用户进行身份验证、授权和记帐操作 。您还可以配置身份验证更改 (CoA)（也称为动态授权），以便在使用思科ISE RADIUS服务器时，可以在身份验证之后更改用户的授权。 在 RADIUS 服务器和服务器组对象中添加一些属性，并使用户能够选择 RA VPN 连接配置文件中的 RADIUS 服务器组。
适用于远程接入 VPN 的多个连接配置文件和组策略。	您可以配置多个连接配置文件，并创建与这些配置文件一起使用的组策略。 调整了 **Device** > **Remote Access VPN** 页面，现在连接配置文件和组策略分别位于单独的页面上，此外还更新了RA VPN连接向导，以便允许用户选择组策略。此前需在向导中配置的一些项目现在可以在组策略中进行配置。
远程接入 VPN 支持基于证书的辅助身份验证源和双因素身份验证。	您可以使用证书进行用户身份验证，并配置辅助身份验证源，以便用户在建立连接之前必须进行两次身份验证。您还可以配置双因素身份验证，使用 RSA 令牌或 Duo 密码作为第二个因素。 更新了 RA VPN 连接向导，以支持配置这些新增选项。
远程接入 VPN 支持带多个地址范围的 IP 地址池和 DHCP 地址池。	您现在可以选择多个网络对象来指定子网，从而配置拥有多个地址范围的地址池。此外，您还可以在DHCP服务器中配置地址池，并使用此服务器为RA VPN客户端提供地址。如果您使用RADIUS进行授权，您也可以在 RADIUS 服务器中配置地址池。 更新了 RA VPN 连接向导，以支持配置这些新增选项。您可以选择在组策略中而非连接配置文件中配置地址池。

功能	说明
Active Directory 领域的增强功能。	您现在可以在单个领域中添加多达 10 个冗余 Active Directory (AD) 服务器。您还可以创建多个领域，并删除不再需要的领域。此外，单个领域中下载用户的数量限制已从此前版本的 2,000 增加到 50,000。 更新了 **Objects** > **Identity Sources** 页面，以支持多个领域和服务器。您可以在访问控制用户标准和 SSL 解密规则中选择领域，从而对此领域中的所有用户应用此规则。您还可以在身份规则和RA VPN 连接配置文件中选择领域。
ISE 服务器的冗余支持。	在将思科身份服务引擎 (ISE) 配置为被动身份验证的身份源时，如果具有 ISE 高可用性设置，现在可以配置辅助 ISE 服务器。 在 ISE 身份对象中添加了辅助服务器的属性。
发送到外部系统日志服务器的文件/恶意软件事件。	您可以配置要接收文件/恶意软件事件的外部系统日志服务器，这些事件是由访问控制规则配置的文件策略生成的。文件事件使用的消息 ID 为 430004，恶意软件事件则为 430005。 在 **Device** > **System Settings** > **Logging Settings** 页面中添加了文件/恶意软件系统日志服务器选项。
记录到内部缓冲区并支持自定义事件日志过滤器。	您可以将内部缓冲区配置为系统日志记录的目的地。此外，您可以创建事件日志过滤器，来自定义需要分别为系统日志服务器和内部缓冲区日志记录目的地生成的消息。 在 **Objects** 页面中添加了 Event Log Filter 对象，并在 **Device** > **System Settings** > **Logging Settings** 页面添加了使用此对象的功能。**Logging Settings** 页面也添加了内部缓冲区选项。
Firepower 设备管理器 Web 服务器证书。	您现在可以配置用于 HTTPS 连接到 Firepower 设备管理器配置接口的证书。通过上传 Web 浏览器已经信任的证书，可避免使用默认内部证书时获得的“不受信任的颁发机构”的消息。添加了 **Device** > **System Settings** > **Management Access** > **Management Web Server** 页面。
思科威胁响应支持。	您可以配置系统将入侵事件发送到思科威胁响应基于云的应用。您可以使用思科威胁响应分析入侵事件。 在 **Device** > **System Settings** > **Cloud Services** 页面添加了思科威胁响应。

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 6.4.0 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

功能	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

功能	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。

功能	说明
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）。

版本 6.2.0 弃用的功能

这些功能在版本 6.2.0 中被弃用。

表 *10:* 版本 *6.2.0* 弃用的功能

功能	说明
嵌套的关联规则	版本 6.2.0 不再支持嵌套的关联规则。如果关联规则用作另一个关联规则的触发器，则关联规则即为嵌套。例如，如果您创建规则 A 和规则 B，这两个规则都会触发入侵事件，则可以使用条件“规则 A 为真”作为规则 B 的限制。在此配置中，规则 A 被视为嵌套在规则 B 内。 **自动配置更改** 升级过程通过将被嵌套关联规则（规则 A）中的设置复制到嵌套关联规则（规则 B）并删除被嵌套规则，将某些被嵌套关联规则“展平”。升级过程还会将被嵌套规则中的主机配置文件/用户限定条件和暂停/非活动时段复制到嵌套规则。 对于除非活动时段外的所有这些设置，仅当嵌套规则中缺少相应设置时，系统才可将被嵌套规则中的设置复制到嵌套规则。系统将被嵌套规则中的非活动时段复制到嵌套规则时，它将保留嵌套规则中的非活动时段，以便生成的规则使用最初参与嵌套配置的两个规则中的设置。 **避免升级失败** 在升级之前，确保嵌套关联规则可以“展平”。否则，升级将失败。请注意，如果被嵌套规则和嵌套规则具有特定类型的冲突，则升级无法展平被嵌套规则。为避免升级失败，请在升级之前修改关联规则： • 删除被嵌套规则或嵌套规则中的主机配置文件限定条件、用户限定条件和暂停时段设置，以便被嵌套配置中只有一个规则指定这些设置。 • 删除任何被嵌套规则中的连接跟踪器。 • 从不必为真的被嵌套规则中的主机配置文件限定文件、用户限定文件、暂停时段和非活动时段；也就是说，从被嵌套规则中删除使用 OR 运算符链接到嵌套规则中的其他规则条件的元素。

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 *11:* 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 *12:* 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 *13:* 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。
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 *14: 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**

版本	新菜单路径	旧菜单路径
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。

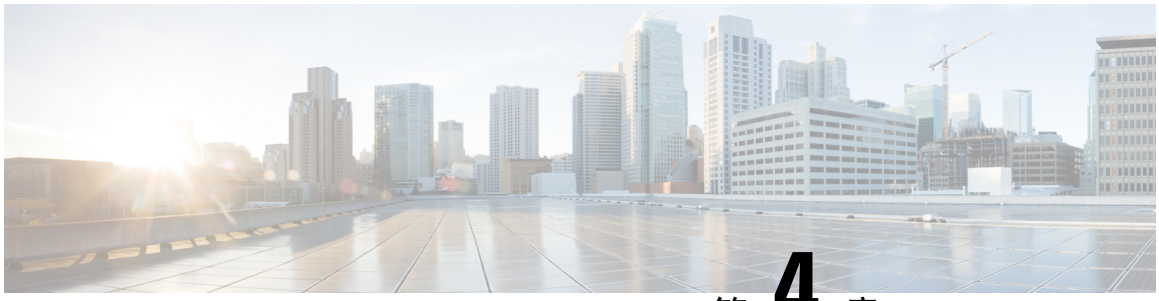
注释 演练已在 Firefox 和 Chrome 浏览器上进行了测试。如果您在使用其他浏览器时遇到问题，我们会要求您切换到 Firefox 或 Chrome。如果问题持续存在，请联系 Cisco TAC。

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 *15:* 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。

问题	解决方案
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 6.4.0

本章提供版本 6.4.0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 6.4.0

此核对表中包含为版本 6.4.0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 33 页和一般指引和警告， 第 41 页。

表 *16:* 版本 *6.4.0* 新指引

	指南	平台	升级自	直接至
	Firepower 1010 设备上的 Etherchannel 可以将出口流量引入黑洞， 第 32 页	Firepower 1010	6.4.0	6.4.0.3 至 6.4.0.5
	升级失败：容器实例上的磁盘空间不足， 第 32 页	Firepower 4100/9300	6.3.0 至 6.4.0.x	6.3.0.1 至6.5。0
	升级失败：版本 6.2.3.12 之前的 NGIPS 设备， 第 32 页	Firepower 7000/8000 系列 ASA FirePOWER NGIPSv	6.2.3 至 6.3.0.x	仅 6.4.0

	指南	平台	升级自	直接至
	TLS 加密加速已启用/不能禁用，第 33 页	Firepower 2100 系列 Firepower 4100/9300	6.1.0 至 6.3.0.x	6.4.0+
	Firepower 4100/9300 需要版本 6.2.0 以进行升级，第 33 页	Firepower 4100/9300	6.1.0.x	仅 6.4.0

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 version 6.4.0 to version 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，有些流量会一直失败。

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

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。

升级失败：版本 6.2.3.12 之前的 NGIPS 设备

部署：7000/8000 系列、ASA FirePOWER 和 NGIPSv

相关漏洞：CSCvp42398

升级自：版本 6.2.3 至 6.3.0.x

直接至：仅版本 6.4.0

以下情况不能将 NGIPS 设备升级到版本 6.4.0：

- 设备之前运行版本 6.2.3.12，然后
- 您卸载了版本 6.2.3.12 的修补程序，或者已升级到版本 6.3.0.x。

  这也包括您卸载版本 6.2.3.12 的修补程序并升级到版本 6.3.0.x 的情况。

如果这是您目前的情况，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。

Firepower 4100/9300 需要版本 6.2.0 以进行升级

部署：使用 FTD 的 Firepower 4100/9300

升级自：版本 6.1.x

直接至：仅版本 6.4.0

与其他 FMC 管理的设备不同，您无法在 Firepower 4100/9300 系列设备上直接将 Firepower 威胁防御软件从版本 6.1 升级到 6.4。这是因为 FXOS 2.6.1 与 FTD 版本 6.1 不兼容，但对版本 6.4 而言必要。

我们建议将 FXOS 2.3.1 上的版本 6.2.3 作为中间版本，并记住先升级 FXOS。不要将版本 6.3 用作中间版本；请参阅 Firepower 发行说明（版本 6.3.0）中的指导原则和警告。

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 6.4.0；请参阅要升级的最低版本，第 43 页。

表 *17:* 版本 *6.4.0* 以前发布的指引

	指南	平台	升级自	直接至
	URL 过滤缓存的超时可能会更改，第 35 页	任意	6.2.3.x	6.3.0+
	对 FMC、7000/8000 系列、NGIPSv 的准备情况检查可能失败，第 35 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 36 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 36 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 37 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 37 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 38 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 38 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 38 页	FMC	6.1.0 至 6.2.3.x	6.3.0+
	升级可以从 CSSM 取消 FTD/FDM 的注册，第 39 页	使用 FDM 的 FTD	6.2.0 至 6.2.2.x	6.2.3 至 6.4.0
	报告中对结果限制的更改，第 39 页	FMC	6.1.0 至 6.2.2.x	6.2.3 至 6.4.0
	升级前从版本 6.1.x FTD群集删除站点 ID，第 40 页	FTD 群集	6.1.0.x	6.2.3 至 6.4.0
	升级失败：6.2.0 版本 ASA 5500-X 系列上的 FDM，第 40 页	使用 FDM 的 FTD	仅 6.2.0	6.2.2 至 6.4.0
	访问控制可以从 SRU 获取基于延迟的性能设置，第 40 页	FMC	6.1.0.x	6.2.0 至 6.4.0

	指南	平台	升级自	直接至
	FTD 上“Snort 故障时自动打开”取代了“故障保护” ，第 41 页	使用 FMC 的 FTD	6.1.0.x	6.2.0 至 6.4.0

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、7000/8000 系列、NGIPSv 的准备情况检查可能失败

部署：FMC、7000/8000 系列设备、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 *18:* 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
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 (**System** > **Updates**) 应用热补丁。

表 *19:* 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（7000/8000 系列、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。

升级可以从 CSSM 取消 FTD/FDM 的注册

部署：使用 FDM 的 FTD

升级自：版本 6.2 至 6.2.2.x

直接至：版本 6.2.3 至 6.4.0

升级 Firepower 设备管理器管理的 Firepower 威胁防御设备可能会从思科智能软件管理器取消设备的注册。升级完成后，请检查您的许可证状态。

步骤 1 单击 **设备**，然后单击 Smart License 摘要中的 **View Configuration**。

步骤 2 如果设备没有注册，单击 **Register Device**。

报告中对结果限制的更改

部署： Firepower 管理中心

升级自：版本 6.1.0 至 6.2.2.x

直接至：版本 6.2.3 至 6.4.0

版本 6.2.3 限制您可以在报告部分中使用或包括的结果数，如下所示。对于表格和详细信息视图，您可以在 PDF 报告中包括比 HTML/CSV 报告少的记录。

表 *20:* 报告中对结果的新限制

报告部分类型	最大记录数：HTML/CSV 报告部分	最大记录数：PDF 报告部分
条形图 饼图	100（顶部或底部）	100（顶部或底部）
表格视图	400,000	100,000
详细信息视图	1,000	500

如果在升级 Firepower 管理中心之前，报告模板中的某个部分指定的结果数大于 HTML/CSV 最大值，则升级进程会将该设置降至新的最大值。

对于生成PDF报告的报告模板，如果在任何模板部分中超过PDF限制，升级过程会将输出格式更改为HTML。要继续生成PDF，请将结果限制降低到PDF最大值。如果您在升级后执行此操作，则将输出格式设置回PDF。

升级前从版本 6.1.x FTD群集删除站点 ID

部署： Firepower 威胁防御群集

升级自：版本 6.1.x

直接至：版本 6.2.3 至 6.4.0

Firepower 威胁防御版本 6.1.x 群集不支持站点间群集（您可以从版本 6.2.0 开始使用 FlexConfig 配置站点间功能）。

如果在 FXOS 2.1.1 中部署或重新部署了版本 6.1.x 群集，并且输入了（不受支持的）站点 ID 值，请在升级之前删除 FXOS 中每个设备上的站点 ID（设置为 **0**）。否则，升级后设备将无法重新加入群集。

如果已经升级，请从每个设备中删除站点 ID，然后重新建立群集。要查看或更改站点 ID，请参阅《思科 FXOS CLI 配置指南》。

升级失败：6.2.0 版本 ASA 5500-X 系列上的 FDM

部署：使用 FDM 的 FTD，在内存较小的 ASA 5500-X 系列设备上运行

升级自：版本 6.2.0

直接至：版本 6.2.2 至 6.4.0

如果从版本6.2.0升级，升级可能会失败并显示一则错误消息：`Uploaded file is not a valid system upgrade file`。即使您使用的是正确的文件，也可能出现这种情况。

如果发生这种情况，您可以尝试以下解决办法：

- 请重试。
- 使用 CLI 进行升级。
- 先升级至 6.2.0.1。

访问控制可以从 SRU 获取基于延迟的性能设置

部署：FMC

升级自：6.1.x

直接至： 6.2.0+

版本 6.2.0+ 中的新访问控制策略默认从最新的入侵规则更新 (SRU) 获取其基于延迟的性能设置。此行为受 **Apply Settings From** 选项控制。要配置此选项，请编辑或创建访问控制策略，单击 **Advanced**，然后编辑基于延迟的性能设置。

升级到版本 6.2.0+ 后，系统将根据当前（版本 6.1.x）配置设置新选项。如果您的当前设置是：

- 默认：新选项设置为 **Installed Rule Update**。在升级后部署时，系统将使用最新 SRU 中基于延迟的性能设置。流量处理可能会发生变化，具体取决于最新 SRU 指定的内容。
- 自定义：新选项设置为 **Custom**。系统保留其当前的性能设置。由于此选项，行为应该不会有任何更改。

我们建议您在升级之前查看配置。在版本 6.1.x FMC Web 界面中，如前所述查看策略的基于延迟的性能设置，并查看 **Revert to Defaults** 按钮是否变暗。如果按钮变暗，表示您使用的是默认设置。如果其处于活动状态，则表示您已配置自定义设置。

FTD 上“Snort 故障时自动打开”取代了“故障保护”

部署：使用 FMC 的 FTD

升级自：版本 6.1.x

直接至：版本 6.2+

在 6.2 版本中，Snort 故障时自动打开的配置将取代 FMC 管理的 Firepower 威胁防御设备上的故障保护选项。虽然故障保护允许您在 Snort 忙碌时丢弃流量，但当 Snort 关闭时，流量会自动通过而不会接受检查。借助 Snort 故障时自动打开功能，您可以丢弃此流量。

升级 FTD 设备时，其新的 Snort 故障时自动打开设置取决于旧的故障保护设置，如下所示。虽然新配置不应更改流量处理，我们仍建议您在升级之前考虑是启用还是禁用故障保护。

表 *21:* 将故障保护迁移至 *Snort* 故障时自动打开

版本 6.1 故障保护	版本 6.2 Snort 故障时自动打开	行为
已禁用（默认行为）	**忙碌**：禁用 **关闭**：启用	新的和现有的连接在 Snort 进程繁忙时丢弃，在 Snort 进程关闭时不检查直接通过。
已启用	**忙碌**：启用 **关闭**：启用	新的和现有的连接在 Snort 进程繁忙或关闭时不检查直接通过。

请注意，Snort 故障时自动打开需要在设备上安装版本 6.2。如果您管理的是版本 6.1.x 的设备，FMC Web 界面会显示故障保护选项。

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 54 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

您可以从多个之前的主版本序列直接升级到版本 6.4.0。不需要运行任何先前版本的最新修补程序即可升级。

表 *22:* 将 *Firepower* 软件升级到 *6.4.0* 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）。	6.1.0

平台	最低版本
使用 FMC 的 Firepower 4100/9300 上的 Firepower 威胁防御	使用 FXOS 2.6.1.157+ 的 6.2.0（先升级 FXOS） 在 FMC 管理的 Firepower 4100/9300 系列设备上，无法将 FTD 直接从版本 6.1 升级到 6.4。我们建议将 FXOS 2.3.1 上的版本 6.2.3 作为中间版本。请参阅 Firepower 4100/9300 需要版本 6.2.0 以进行升级，第 33 页。 如果要从版本 6.2.0.x、6.2.2.0 或 6.2.2.1 升级高可用性或集群部署，并且需要无故障升级，请参阅 FTD 升级行为：Firepower 4100/9300 机箱，第 46 页。
使用 FDM 的 Firepower 威胁防御（所有平台）	6.2.0
使用 ASDM 的 ASA FirePOWER	6.2.0

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 的时间和磁盘空间

表 *23:* 版本 *6.4.0* 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	13.3 GB	26 MB	-	41 分钟
FMCv：VMware 6.0	13.6 GB	29 MB	-	30 分钟
Firepower 2100 系列	12 MB	8.9 GB	950 MB	20 分钟

平台	/Volume 上的空间	/ 上的空间	FMC 上的空间	时间
Firepower 4100 系列	10 MB	7.5 GB	920 MB	6 分钟
Firepower 9300	10 MB	7.7 GB	920 MB	7 分钟
具有 ASA 5500-X 系列的 FTD	9 GB	110 KB	1.1 GB	24 分钟
FTDv：VMware 6.0	7.5 GB	100 KB	1.1 GB	12 分钟
Firepower 7000/8000 系列	7.7 GB	19 MB	980 MB	34 分钟
ASA FirePOWER	11.5 GB	22 MB	1.3 GB	66 分钟
NGIPSv：VMware 6.0	6.5 GB	19 MB	840 MB	16 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 *24: FXOS* 升级期间的流量行为

部署	方法	流量行为
独立式	-	被丢弃

部署	方法	流量行为
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 *25: 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：对 FTD 高可用性对执行到版本 6.1.0 升级的无中断升级需要预安装软件包。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 *26: 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 *27: 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 *28: 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 *29:* 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 *30:* 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 *31: 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 *32: 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 *33: 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

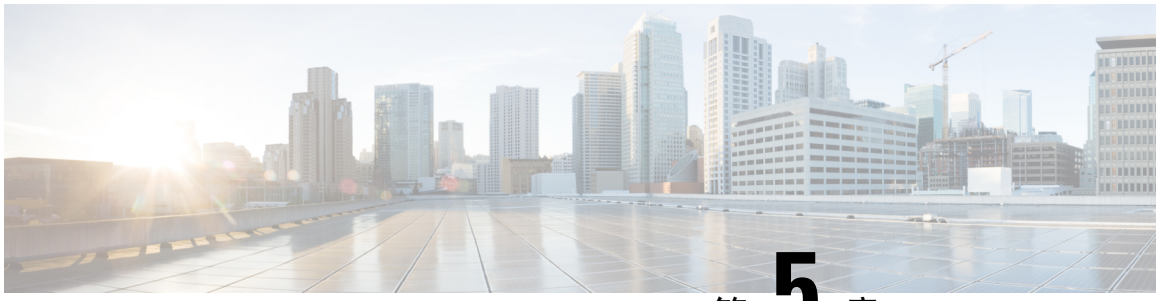
版本 6.2.1+ 中的升级包是签名的 tar 存档 (.tar)。不要解压。

表 *34:* 从版本 *6.2.1+* 升级的升级包

平台	数据包
FMC/FMCv	Cisco_Firepower_Mgmt_Center_Upgrade-版本-内部版本.sh.REL.tar
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 威胁防御虚拟	Cisco_FTD_Upgrade-版本-内部版本.sh.REL.tar
Firepower 7000/8000 系列	Cisco_Firepower_NGIPS_Appliance_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

表 *35:* 从版本 *6.1.x* 或 *6.2.0.x* 升级的升级包

平台	数据包
FMC/FMCv	Cisco_Firepower_Mgmt_Center_Upgrade-版本-内部版本.sh
Firepower 4100/9300 机箱	Cisco_FTD_SSP_Upgrade-版本-内部版本.sh
ASA 5500-X 系列，含 FTD Firepower 威胁防御虚拟	Cisco_FTD_Upgrade-版本-内部版本.sh
Firepower 7000/8000 系列	Cisco_Firepower_NGIPS_Appliance_Upgrade-版本-内部版本.sh
ASA FirePOWER	Cisco_Network_Sensor_Upgrade-版本-内部版本.sh
NGIPSv	Cisco_Firepower_NGIPS_Virtual_Upgrade-版本-内部版本.sh



第 5 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。

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 *36:* 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 58 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。

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 61 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 重新映像到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 *37: 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》

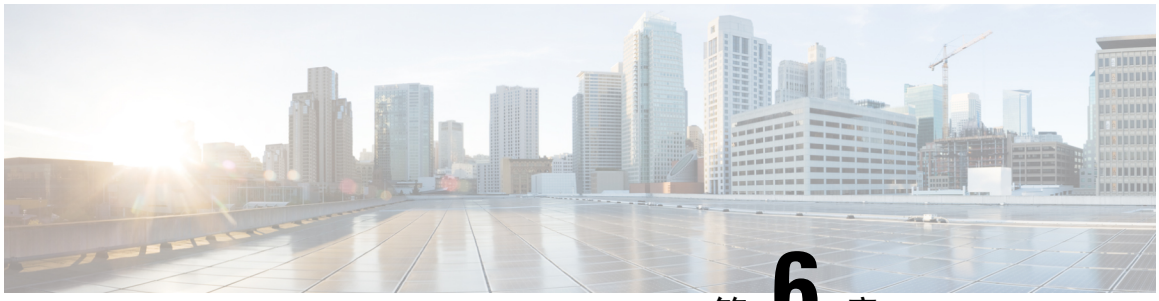
表 *38: Firepower* 威胁防御安装说明

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 *39: 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

NGIPS 平台	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 6.4.0

针对至少一个版本 6.4.0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 67 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。 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 67 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)

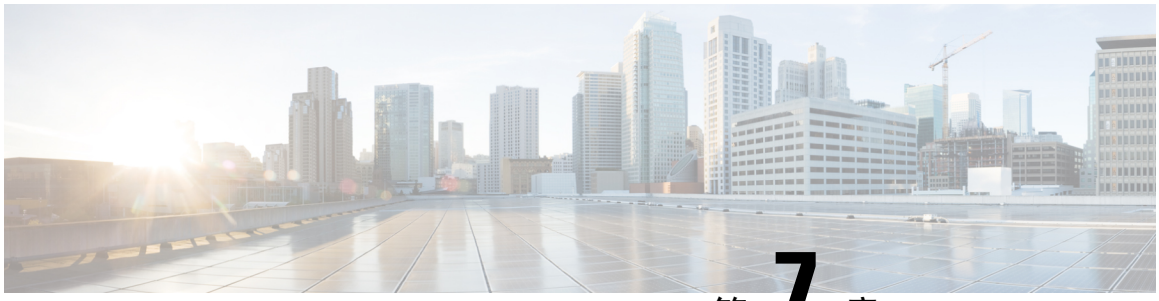
故障排除和配置示例

- 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 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 6.4.0：

- 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 6.4.0 已解决的问题

表 *40:* 版本 *6.4.0* 已解决的问题

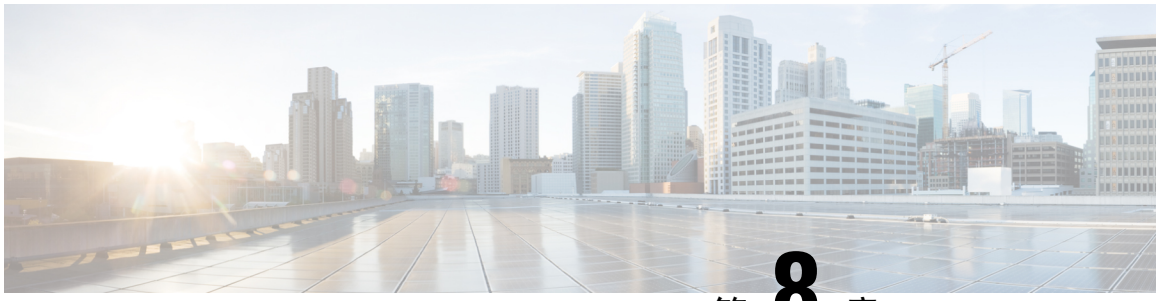
漏洞 ID	标题
CSCvc56570	策略部署失败会导致瞬间流量下降和已建立的连接失败

漏洞 ID	标题
CSCvf83504	SYS_FW_INTERFACE_NAME_LIST and SYS_FW_NON_INLINE_INTERFACE_NAME_LIST 无法识别子接口
CSCvg11366	确保在调用 MOJO, Syncd.pl 等使用的 File::Temp 之后进行清理
CSCvh93045	如果具有不同 ip 的相同设备（SN 相同）尝试注册，FMC 应该清理数据库本身
CSCvi01404	ssl 检查策略可能导致使用 ECDSA 签名证书的站点失败
CSCvi16039	Firepower 管理中心不接受 SNMPv3 密码中的各种字符
CSCvi16074	Firepower 管理中心在输入 SNMPv3 密码时会产生误导性错误
CSCvi25965	Sybase 升级：SRU 安装后，僵尸解散过程导致策略部署失败
CSCvi49522	具有应用程序标记、搜索或类别过滤器的 POST 或 PUT 规则 -> 无法访问 ACP 规则 GUI
CSCvi71622	备用 FTD 上 DATAPATH 中的回溯
CSCvi81022	思科 Firepower 威胁防御 SSL/TLS 策略绕过漏洞
CSCvi89202	恢复升级时磁盘空间检查被省略
CSCvi93680	应该警示用户首次启动失败
CSCvj08826	FMC：ibdata1 文件变大（从 300Gb 增大到 2.4TB+）
CSCvj13960	启用 SNMP 时看到 CPU 使用率高
CSCvj27949	FMC 在夏季没有使用正确的时区校正。
CSCvj50451	无法在 FMC 上添加网络对象 0.0.0.0/32
CSCvj57511	ASDM：提交更改后，层策略的已禁用规则状态恢复为继承
CSCvj70886	API-Explorer 必须支持 4096 位证书
CSCvk20209	FMC 的外部身份验证不通过 ISE 为 RADIUS 对象工作。
CSCvk20381	在新的 ASAv Azure、KVM 和 VMWare 部署中看到回溯循环
CSCvk23653	在从组策略中取消引用 ip 池之前，其被否定
CSCvk29558	FTD VPN：禁用 S2S 选项“证书 OU 字段以确定隧道”不会生效
CSCvk33503	未解析 Flexconfig ethertype 命令，导致部署失败
CSCvk34648	重新生成数据密钥时，Firepower 2100 隧道摆动并生成高吞吐量的 Lan 对 Lan VPN 流量

漏洞 ID	标题
CSCvk43854	思科 Firepower 威胁防御检测引擎策略绕过漏洞
CSCvk45941	需要更好地记录部署失败 - VPN 策略中存在错误的字符
CSCvm04150	首次启动脚本运行两次后，所有运行状况模块都在运行状况模块表中标记为已删除
CSCvm05768	https 服务器证书中的必填字段
CSCvm41983	Policy Deployment 页面最终单击 'deploy' 即返回 'Deploy' 窗口。
CSCvm50153	FMC - 使用手动输入的 ip 范围的 VPN 拆分隧道扩展 ACL 导致部署失败
CSCvm54029	6.4.0 - ADI 处理了无效的 IPV6 RA_VPN 会话并将其置于 user_ip_map 文件中
CSCvm54062	文件从主用设备复制到备用设备后，操作队列任务卡住了。
CSCvm60056	下载自定义 DNS 安全情报源后，webGUI 时间戳不更新
CSCvm70274	tcp 代理：DATAPATH 上的 ASA 回溯
CSCvm72980	FDM：- FTD 在 SSL 握手中不发送完整的链
CSCvm75251	在 KP FTD 平台上，出现 "error-code": "backend-connect-error" 时，未发生 restapi post 登录
CSCvm78028	无法在 RIP 配置中添加 2 个具有相同“流量方向”和“路由类型过滤器”的过滤器
CSCvm84459	bad call_home_ca 文件阻止智能许可注册
CSCvm85453	FMC HA：故障转移后，不会从新的主用 FMC 发送 SNMP 陷阱
CSCvm90290	Firepower 软件中的 ImageMagick 包可能已过时
CSCvm92210	如果包含用户定义的端口号，则无法在 FTD 中部署 anyconnect Group-Url
CSCvm96642	目前，主动身份验证不支持 DSA 证书。
CSCvn00312	尝试显示错误和警告时部署卡住
CSCvn12373	FMC HA 的 rna_attribute dup 键上的策略部署失败
CSCvn13880	启用多播路由时，计时器事件导致线程 PIM IPv4 或 IGMP IPv4 上的单元回溯
CSCvn14276	FlexConfig 不支持 'arp permit-nonconnected'
CSCvn14511	FMC 在 SNMP 用户身份验证配置中不接受大括号（例如 "{"）
CSCvn19609	Flex 对象编辑器可能会引入意外的换行符，导致策略部署失败

漏洞 ID	标题
CSCvn23926	OSPFv3 接口认证 SPI 必须对设备的每个接口唯一
CSCvn31882	如果部署模式设置为 "Everytime"，Flex 配置语句会重复
CSCvn36022	FMC 对象管理提供使用给定对象的每个 ACP/设备的相关信息
CSCvn38101	这样针对 nat 与备用地址重叠情况的 ui 检查
CSCvn39960	在 FMC 中为中心和分支 VPN 配置受保护的网络不会影响 lina CLI。
CSCvn46358	由于发送 VPN 状态消息而导致 lina msglyr infra 过载
CSCvn47504	应该为 6.x 禁用 VMware 气球驱动程序
CSCvn58125	在仪表板上进行空白过滤时生成报告
CSCvn75713	FMC 上的 CVE Nmap 版本
CSCvn75722	FMC 上的 CVE Nmap 版本
CSCvn75729	FMC 上的 CVE Nmap 版本
CSCvn82823	当接口名称区分大小写时，FTD HA 接口监控更改不生效
CSCvn82891	httpd 中存在多个漏洞
CSCvn85761	FMC 不允许使用对象名称中的特殊字符创建密钥
CSCvn91775	FMC GUI 不允许在“对象”>VPN>“证书映射”中创建具有数字名称的证书映射
CSCvo04444	Ikev2 隧道创建失败
CSCvo06383	由于数据库关闭，FMC 从版本 6.0.1 升级到 6.1.0 失败
CSCvo19433	Flexconfig 文档应指定不正确配置的效果范围
CSCvo19666	28 核心实例的性能比预期低 20%
CSCvo20847	由于同步时 xlate 分配损坏，活动 FTP 因群集而失败
CSCvo30697	在多个平台上应用 LINA 捕获时吞吐量下降
CSCvo31831	删除基本策略不会删除子策略的 EO
CSCvo35129	需要在 epol_wait 事件处理中进行更正
CSCvo38051	ctm_ipsec_pfkey_parse_msg at ctm_ipsec_pfkey.c:602 中出现分段错误
CSCvo40478	因为 FMC 最新产品更新，6.4 FMC 仪表板显示的值不正确

漏洞 ID	标题
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
CSCvo74765	由于 Lina 响应在 10000 毫秒后超时，导致 FDM 策略部署失败
CSCvo80725	由于“错误：ip_multicast_ctl 无法获取通道”，vFTD 6.4 无法建立 OSPF 邻接
CSCvp59960	网络发现不适用于包含文字的网络组 - 用户或思科创建。
CSCvp67392	由于反向路径检查，ASA/FTD HA 数据接口心跳丢失



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 6.4.0：

- 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。

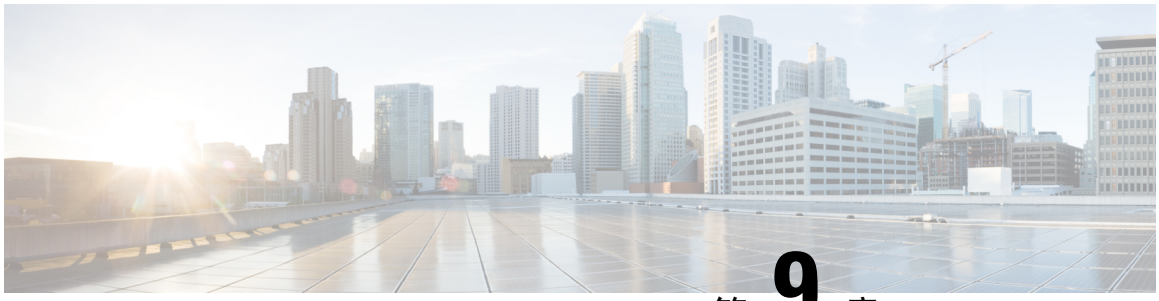
版本 6.4.0已知问题

表 *41:* 版本 *6.4.0* 的已知问题

漏洞 ID	标题
CSCvo00852	对于 FTDv ESXi 12 核心和 FTDv KVM 12 核心平台，Lina CPU 低且流量丢失
CSCvo03589	在 MI 情境下，应用程序代理心跳可能丢失
CSCvo40478	因为 FMC 最新产品更新，6.4 FMC 仪表板显示的值不正确
CSCvo80725	由于“错误：ip_multicast_ctl 无法获取通道”，vFTD 6.4 无法建立 OSPF 邻接

漏洞 ID	标题
CSCvp06568	在 6.4 FMC 管理的 6.3 FTD 上，系统日志中的 NAP 策略/SSL 策略名称未知
CSCvp14864	当端口 4 上的 poe 与端口 3 一起启用时，3504 wlc 变得无法访问
CSCvp19669	用户未在 FDM 事件中正确显示
CSCvp21403	验证：数据平面 - 管理访问不处理 RA-VPN 端口冲突
CSCvp23703	第一个启动脚本 S97compress-client-resources 在 FTD 中悄然失败。
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
CSCvp27818	更改日期的日期命令在 SM-48 上显示错误
CSCvp29817	将 TempID 转换为 RealID 时无法更新登录历史记录。每个 ID 1 个日志，历史记录丢失
CSCvp30194	ASA SFR：尝试使用 IPS 导入 ACP 时看到“导入 SFO 时出错：无法加载容器”
CSCvp33797	从 AD 下载用户信息后，在 FMC 上有会话的用户未正确更新
CSCvp34148	内存泄漏导致 WLC 重启
CSCvp37229	如果从“策略层”的“我的更改”层启用，则少数预处理器不会启用
CSCvp45752	如果在子域中添加了自定义应用程序，则 snort 不会在旧版本的已注册设备上重新启动
CSCvp47260	生成故障排除文件时以日文显示停止
CSCvp47535	新添加的应用程序协议无法在主机下查看
CSCvp48523	访问策略未正确反映经修改的用户
CSCvp48525	无法在任务详细信息上编辑计划的任务
CSCvp48534	无法在入侵规则中添加类别
CSCvp48545	无法创建使用日文名称的警报
CSCvp48565	VPN 故障排除日志设置需要的时间异常长
CSCvp48583	IPv6 DAD 复选框默认启用
CSCvp53608	WLC 对某些主机的 HTTP/HTTPS/SSH 没有响应
CSCvp56916	S2S VPN 向导显示没有可用的预配置证书
CSCvp56951	FDM/FTDvirtual 无法支持/部署 "ignore-ipsec-keyusage" flexconfig 对象

漏洞 ID	标题
CSCvp57096	到 6.4.0 的升级可能会失败，因为 ids_event_msg_map 表的 msg 字段中有 NULL 条目
CSCvp59960	网络发现不适用于包含文字的网络组 - 用户或思科创建。
CSCvp67132	emWeb 上的 WLC 崩溃



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