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，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 18 页和一般指引和警告， 第 24 页。

表 *1:* 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 2 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 2 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 3 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 3 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 3 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 4 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 4 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 *2:* 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 9 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 *3:* 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 *4:* 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 13 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 12 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 13 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 7 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 14 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 16 页和未更改的类别，第 17 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 *5:* 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 *6:* 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 7: 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 13 页		军事	未更改的类别，第 17 页
滥用药物	合并的类别，第 13 页		机动车	重命名的类别，第 16 页
成人和色情	拆分类别，第 14 页		音乐	重命名的类别，第 16 页

旧类别	变化		旧类别	变化
酒精和烟草	拆分类别，第 14 页		新闻与媒体	重命名的类别，第 16 页
僵尸网络	重命名的类别，第 16 页		裸体	重命名的类别，第 16 页
商业与经济	拆分类别，第 14 页		在线贺卡	重命名的类别，第 16 页
作弊程序	重命名的类别，第 16 页		打开 HTTP 代理	重命名的类别，第 16 页
计算机和互联网信息	拆分类别，第 14 页		寄放域	未更改的类别，第 17 页
计算机和互联网安全	拆分类别，第 14 页		付费冲浪	合并的类别，第 13 页
已确认的垃圾邮件源	合并的类别，第 13 页		点对点	重命名的类别，第 16 页
内容交付网络	合并的类别，第 13 页		个人网站和博客	拆分类别，第 14 页
小众和神秘	拆分类别，第 14 页		个人存储	拆分类别，第 14 页
约会	未更改的类别，第 17 页		哲学和政治宣传	重命名的类别，第 16 页
死网站	重命名的类别，第 16 页		网络钓鱼和其他欺诈	重命名的类别，第 16 页
动态生成的内容	合并的类别，第 13 页		专用 IP 地址	弃用的类别，第 13 页
教育机构	合并的类别，第 13 页		代理规避和匿名程序	重命名的类别，第 16 页
娱乐和艺术	拆分类别，第 14 页		可疑	重命名的类别，第 16 页
时尚和美容	重命名的类别，第 16 页		房地产	未更改的类别，第 17 页
金融服务业	重命名的类别，第 16 页		娱乐和爱好	合并的类别，第 13 页

旧类别	变化		旧类别	变化
食品餐饮	重命名的类别，第 16 页		参考和研究	拆分类别，第 14 页
赌博	拆分类别，第 14 页		宗教	未更改的类别，第 17 页
游戏	未更改的类别，第 17 页		搜索引擎	合并的类别，第 13 页
政府	合并的类别，第 13 页		性教育	合并的类别，第 13 页
毛额	合并的类别，第 13 页		共享软件和免费软件	重命名的类别，第 16 页
黑客攻击	合并的类别，第 13 页		购物	未更改的类别，第 17 页
仇恨和种族主义	重命名的类别，第 16 页		社交网络	拆分类别，第 14 页
健康和医疗	重命名的类别，第 16 页		社会	拆分类别，第 14 页
家居和园艺	拆分类别，第 14 页		垃圾邮件 URL	合并的类别，第 13 页
狩猎和钓鱼	重命名的类别，第 16 页		体育	合并的类别，第 13 页
违法	拆分类别，第 14 页		间谍软件和广告软件	未更改的类别，第 17 页
图片和视频搜索	重命名的类别，第 16 页		流媒体	重命名的类别，第 16 页
个人炒股建议和工具	重命名的类别，第 16 页		泳衣和内衣	重命名的类别，第 16 页
互联网通信	拆分类别，第 14 页		培训和工具	合并的类别，第 13 页
互联网门户	合并的类别，第 13 页		差旅费	未更改的类别，第 17 页
求职	未更改的类别，第 17 页		未分类	弃用的类别，第 13 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 13 页		未确认的垃圾邮件源	合并的类别，第 13 页
童鞋	重命名的类别，第 16 页		暴力类	合并的类别，第 13 页
法务	合并的类别，第 13 页		武器	未更改的类别，第 17 页
本地信息	重命名的类别，第 16 页		网络广告	合并的类别，第 13 页
恶意软件网站	未更改的类别，第 17 页		基于 Web 的邮件	拆分类别，第 14 页
大麻	合并的类别，第 13 页		Web 托管站点	重命名的类别，第 16 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 *8:* 新范畴

新类别
动态和住宅

表 *9:* 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 *10:* 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 7 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 *11:* 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 *12*: 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 *13*: 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 *14:* 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 *15:* 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 26 页。

表 *16:* 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 19 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 19 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 20 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 20 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 21 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 21 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 22 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 22 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 23 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 23 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 24 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 *17:* 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 *18:* 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 35 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 *19*: 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 *20:* 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 *21: 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 *22: 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 *23: 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 *24: 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 *25: 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 *26: 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 *27: 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 *28: 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 *29:* 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