更新

产品升级

本指南不包含有关如何升级系统软件或防火墙机箱的信息。请改为参阅随附的升级指南：https://cisco.com/go/ftd-fmc-upgrade-100。

内容更新

系统可以从互联网获取内容更新。我们建议您尽可能安排或启用自动内容更新。某些更新在初始设置过程中或在您启用相关功能时自动启用。完成初始设置后，我们建议您查看所有自动更新，并在必要时进行调整。

表 *1:* 内容更新

组件	说明	详细信息
漏洞数据库 (VDB)	思科漏洞数据库 (VDB) 包含主机可能易受感染的已知漏洞，以及操作系统、客户端和应用指纹。系统借助 VDB 来确定某个特定主机是否会增加遭受危害的风险。	**计划：**作为计划任务。 **卸载：**从 VDB 357 开始，您可以安装任何可追溯到 防火墙管理中心 的基准 VDB 的 VDB。 **请参阅：** 更新漏洞数据库 (VDB)， 第 3 页

组件	说明	详细信息
地理位置数据库 (GeoDB)	思科地理位置数据库 (GeoDB) 将 IP 地址映射到国家/地区/大洲。	**计划：**从其自己的更新页面。 **卸载：** 否。 **请参阅：** 更新地理位置数据库 (GeoDB)，第 5 页
入侵规则 (SRU/LSP)	入侵规则更新提供全新和更新的入侵规则及预处理器规则、现有规则的修改状态和修改的默认入侵策略设置。 另外，规则更新还可能删除规则，提供新规则类别和默认变量，并修改默认变量值。	**计划：**从其自己的更新页面。 **卸载：** 否。 **请参阅：** 更新入侵规则，第 6 页
安全情报源	安全情报源是 IP 地址、域名和 URL 的集合，可用于快速过滤与条目匹配的流量。	**计划：**从对象管理器。 **卸载：** 否。 **请参阅：** *Cisco Secure Firewall Management Center* 设备配置指南
新 URL 类别和信誉	URL 过滤可以根据 URL 的一般分类（类别）和风险级别（信誉）控制对网站的访问。	**计划：**配置集成/云服务时，或作为计划任务。 **卸载：** 否。 **请参阅：** *Cisco Secure Firewall Management Center* 设备配置指南

内容更新的要求和前提条件

型号支持

任意

Cisco Secure Firewall 220 使用更小的漏洞数据库 VDB Lite，以提高处理效率。

支持的域

全局 除非另有说明。

用户角色

管理员

内容更新的准则和限制

发行说明

我们建议您阅读内容更新随附的任何发行说明或公告文本。这些内容提供版本特定的关键信息，包括兼容性、前提条件、新功能、行为更改和警告。

计划的更新

查看计划的更新，确保它们按预期进行。系统以UTC时间安排任务（包括更新）。这意味着它们在本地发生的时间取决于日期和您的特定位置。此外，由于更新是以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，计划的更新会在夏天比冬季中的一个小时开始。

更新漏洞数据库 (VDB)

思科漏洞数据库 (VDB) 包含主机可能易受感染的已知漏洞，以及操作系统、客户端和应用指纹。系统借助 VDB 来确定某个特定主机是否会增加遭受危害的风险。

思科定期发布 VDB 更新。在 防火墙管理中心上更新 VDB 及其关联映射所需的时间取决于网络映射中的主机数量。一般说来，将主机数除以 1000，即可估算出执行更新所需的大致时间（分钟）。

防火墙管理中心 上的初始设置会自动下载并安装思科提供的最新VDB，作为一次性操作。它还会安排每周任务，以下载最新可用软件更新，其中包括最新VDB。我们建议您查看此每周任务，并在必要时进行调整。或者，安排新的周期性任务，以便实际更新 VDB 和/或软件并部署配置。有关详细信息，请参阅漏洞数据库更新自动化。

对于 Cisco Secure Firewall 220，系统安装较小的 VDB（也称为 *VDB lite*）。这个较小的 VDB 包含相同的应用，但检测模式更少。与使用完整 VDB 的 设备相比，使用较小 VDB 的设备可能会错过某些应用标识。

对于 VDB 343+，所有应用检测器信息均可通过 Cisco Secure Firewall 应用检测器来获取。该站点包含一个可搜索的应用检测器数据库。版本说明提供了有关特定 VDB 版本的变更信息。

安排 VDB 更新

如果 防火墙管理中心可以访问互联网，我们建议您安排定期更新 GeoDB。请参阅漏洞数据库更新自动化。

手动更新 VDB

使用此程序手动更新 VDB。从 VDB 357 开始，您可以安装任何 VDB，直至 防火墙管理中心的基准 VDB。

⚠

注意 请勿执行与映射的漏洞相关的任务，直至更新完成。即使消息中心在几分钟内不显示进度或指示更新失败，也不要重启更新。相反，请联系思科 TAC。

在大多数情况下，VDB 更新后的第一次部署会重新启动 Snort 进程，从而中断流量检查。系统会在发生这种情况时向您发出警告 （更新的应用检测器和操作系统指纹需要重新启动；漏洞信息不需要）。在此中断期间，流量是被丢弃还是不经进一步检查直接通过，将取决于目标设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为。

开始之前

如果 防火墙管理中心 无法访问互联网 ，或者您安装的是较旧的 VDB，请自行获取更新：https://www.cisco.com/go/firepower-software。选择或搜索您的型号（或选择任何型号 - 对所有 防火墙管理中心型号使用相同的 VDB），然后浏览至 覆盖和内容更新 页面。

过程

步骤 1 选择**管理** > **升级和更新** > **内容更新** > **VDB 更新** 。

步骤 2 选择您希望以什么方式将 VDB 上传到 防火墙管理中心。

- 直接下载：点击 **下载更新** 按钮。
- 手动上传：点击 **上传更新**，然后点击 **选择文件** 然后浏览至 VDB。选择文件后，点击 **上传**。

步骤 3 安装 VDB。

a) 在要安装的 VDB 更新旁边，点击**安装**图标（适用于较新的 VDB）或**回滚**图标（适用于较旧的 VDB）。
b) 选择 防火墙管理中心。
c) 点击**安装 (Install)**。

在消息中心监控更新进度。在更新完成后，系统将使用新的漏洞信息。但您必须先进行部署，已更新的应用检测器和操作系统指纹才会生效。

步骤 4 验证更新是否成功。

当前版本显示在 VDB 更新页面和 **帮助** （ ） > **关于** 上。

下一步做什么

- 部署配置更改；请参阅 *Cisco Secure Firewall Management Center* 设备配置指南。
- 如果您基于漏洞、应用检测器或不再可用的指纹进行配置，请检查这些配置以确保按预期处理流量。另请记住，更新 VDB 的计划任务可以撤消回滚。要避免这种情况，请更改计划任务或删除任何较新的 VDB 软件包。

更新地理位置数据库 (GeoDB)

地理位置数据库 (GeoDB) 是可用于根据地理位置查看和过滤流量的数据库。我们会定期更新 GeoDB，您必须定期更新 GeoDB 才能获得准确的地理位置信息。作为初始配置的一部分，系统会安排每周更新 GeoDB。我们建议您查看此任务，并在必要时进行更改，如 安排 GeoDB 更新，第 5 页。

GeoDB 更新会覆盖之前的任何版本。防火墙管理中心会自动更新其托管设备，除非更新添加新的国家（很少见），否则您不需重新部署。您可以在 GeoDB 更新页面和 **帮助** （ ） > **关于** 查看您的当前版本。

安排 GeoDB 更新

作为初始配置的一部分，系统会安排每周更新 GeoDB。我们建议您查看此任务，并在必要时进行更改，如此程序。

请注意，系统不会在 GeoDB 更新后自动部署，因为在大多数情况下没有必要。但是，在计划的 GeoDB 更新添加新的国家/地区后（这种情况很少见），请尽快部署。这将允许新国家/地区将计为其所属大洲的一部分。例如，如果更新将国家/地区添加到大洲，则在您部署之前，基于“大洲”过滤的规则不匹配通过国家/地区的流量。

开始之前

确保 防火墙管理中心可以访问互联网。

过程

步骤 1 选择**管理** > **升级和更新** > **内容更新** > **地理位置更新** 。

步骤 2 在 **周期性地理位置更新**下，选择 **启用周期性每周更新...** 。

步骤 3 指定**更新开始时间**。

步骤 4 点击**保存**。

手动更新 GeoDB

使用此程序执行按需 GeoDB 更新。

开始之前

如果 防火墙管理中心 无法访问互联网，请自行获取更新：https://www.cisco.com/go/firepower-software。选择或搜索您的型号（或选择任何型号 - 对所有 防火墙管理中心型号使用相同的 GeoDB），然后浏览至 覆盖和内容更新 页面。

过程

步骤 1 选择**管理** > **升级和更新** > **内容更新** > **地理位置更新** 。

步骤 2 在 **一次性地理位置更新**下，选择要如何更新 GeoDB。

- 直接下载：选择 **下载并安装...** 。
- 手动上传：选择**上传和安装... (Upload and install...)**， 然后点击**选择文件 (Choose File)** 并浏览到您之前下载的包。

步骤 3 点击**导入 (Import)**。

在消息中心监控更新进度。

步骤 4 验证更新是否成功。

当前版本显示在 GeoDB 更新页面和 **帮助** （ ） > **关于** 上。

下一步做什么

如果更新添加了新国家/地区（这种情况很少见），请立即部署。在部署之前，新国家/地区不会算作其所在大陆的一部分。例如，如果更新将国家/地区添加到大洲，则在您部署之前，基于“大洲”过滤的规则不匹配通过国家/地区的流量。

更新入侵规则

随着新的漏洞被发现， Talos 智能小组 会发布入侵规则更新。这些更新会影响入侵规则、预处理器规则和使用这些规则的策略。入侵规则更新是累积性的，我们建议您随时更新系统。不能导入与当前安装的规则的版本匹配或早于该版本的入侵规则更新。

入侵规则更新可能提供：

- **新的和修改的规则和规则状态** - 规则更新提供新的和更新的入侵和预处理器规则。对于新的规则，每个系统提供的入侵规则中的规则状态可能不同。例如，一个新规则在 Security over Connectivity 入侵策略中可能是启用状态，在 Connectivity over Security 入侵策略中则可能是禁用状态。规则更新也可以更改现有规则的默认状态，或者完全删除现有规则。
- **新规则类别** - 规则更新可能包括始终添加的新规则类别。
- **修改的预处理器和高级设置** - 规则更新可能更改系统提供的入侵策略中的高级设置，以及系统提供的网络分析策略中的预处理器设置。它们也可以更新访问控制策略中的高级预处理和性能选项的默认值。
- **新的和修改的变量** - 规则更新可能修改现有默认变量的默认值，但不会覆盖您的更改。始终会添加新变量。

在多域部署中，可以在任何域中导入本地入侵规则，但是，只能在全局域中从 Talos 导入入侵规则更新。

了解入侵规则更新何时修改策略

入侵规则更新可以影响系统提供的和自定义网络分析策略，以及所有访问控制策略：

- **系统提供** - 对系统提供的网络分析和入侵策略的更改以及对高级访问控制设置的任何更改将在您更新后重新部署策略时自动生效。
- **自定义** - 因为每个自定义网络分析和入侵策略都使用系统提供的策略作为其基础，或作为策略链中的事件基础，所以规则更新可以影响自定义网络分析和入侵策略。但是，您可以阻止规则更新自动执行这些更改。这使您能够在独立于规则更新导入的计划中手动更新系统提供的基本策略。无论您的选择（在每个自定义策略基础上实施）如何，更新系统提供的策略都不会覆盖您定制的任何设置。

请注意，导入规则更新会丢弃对网络分析和入侵策略所做的所有已缓存更改。为了方便起见，Rule Updates 页面列出了包含已缓存更改的策略以及做出这些更改的用户。

部署入侵规则更新

为使入侵规则更新所做的更改生效，必须重新部署配置。在导入规则更新时，可以将系统配置为自动重新部署到受影响设备。如果允许入侵规则更新修改系统提供的基本入侵策略，则此方法尤其有用。

注意 虽然在部署时规则更新本身不会重新启动 Snort 进程，但您所做的其他更改可能会重新启动。重启 Snort 会短暂中断所有设备上的流量和检查，包括为高可用性/可扩展性配置的检查。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。在不重启 Snort 进行部署时，资源需求可能会导致少量数据包未经检测而被丢弃。

定期入侵规则更新

作为初始配置的一部分，系统会安排每日入侵规则更新。我们建议您查看此任务，并在必要时进行更改，如 安排入侵规则更新，第 8 页。您可能需要更改频率，或在规则导入后启用自动部署。 对于 防火墙管理中心的高可用性，您只需在主用设备上导入更新。

导入本地入侵规则

本地入侵规则是从本地计算机以采用 ASCII 或 UTF-8 编码的纯文本文件形式导入的自定义标准文本规则。可以使用 Snort 用户手册（可在 http://www.snort.org 上获取）中的说明创建本地规则。

在多域部署中，可以在任何域中导入本地入侵规则。可以查看在当前域和祖先域中导入的本地入侵规则。

安排入侵规则更新

作为初始配置的一部分，系统会安排每日入侵规则更新。我们建议您查看此任务，并在必要时进行更改，如此程序。

开始之前

- 确保更新入侵规则的流程符合您的安全策略。
- 请考虑更新因带宽约束和Snort重启而带给流量和检测的影响。我们建议在维护窗口执行更新。
- 确保 防火墙管理中心可以访问互联网。

过程

步骤 1 选择**管理** > **升级和更新** > **内容更新** > **规则更新** 。

步骤 2 在**重复规则更新导入 (Recurring Rule Update Imports)** 下，选中**启用重复规则更新导入 (Enable Recurring Rule Update Imports)**。

步骤 3 指定**导入频率 (Import Frequency)** 和开始时间。

步骤 4 （可选）选中 **Deploy all policies to Targeted devices after rule update completes** 以在每次更新后部署。

步骤 5 点击**保存**。

手动更新入侵规则

使用此程序执行按需入侵规则更新。

开始之前

- 确保更新入侵规则的流程符合您的安全策略。
- 请考虑更新因带宽约束和Snort重启而带给流量和检测的影响。我们建议在维护窗口执行更新。
- 如果 防火墙管理中心 无法访问互联网，请自行获取更新：https://www.cisco.com/go/firepower-software。选择或搜索您的型号（或选择任何型号 - 对所有 防火墙管理中心型号使用相同的更新），然后浏览至覆盖和内容更新 *(Coverage and Content Updates)* 页面。

过程

步骤 1 选择**管理** > **升级和更新** > **内容更新** > **规则更新** 。

步骤 2 在 **一次性规则更新/规则导入**下，选择要如何更新入侵规则。

- 直接下载：选择 **下载新规则更新...** 。
- 手动上传：选择 **规则更新或文本规则文件...**，然后点击 **选择文件** 并浏览到入侵规则更新。

步骤 3 （可选）选中 **重新应用所有策略...** 以在更新后部署。

步骤 4 点击**导入 (Import)**。

在消息中心监控更新进度。即使消息中心在几分钟内不显示进度或指示更新失败，也不要重启更新。相反，请联系思科 TAC。

步骤 5 验证更新是否成功。

当前版本显示在规则更新页面和 **帮助** （ ） > **关于** 上。

下一步做什么

如果您未在更新过程中部署，请立即部署。

导入本地入侵规则

使用以下程序导入本地入侵规则。导入的入侵规则以被禁用的状态显示在本地规则类别中。您可以在任何域中执行此任务。

开始之前

- 请确保您的本地规则文件遵循导入本地入侵规则最佳实践，第 10 页中所述的准则，
- 并确保导入本地入侵规则的过程符合您的安全策略。
- 请考虑导入因带宽约束和 Snort 重启而带给流量和检测的影响。我们建议将规则更新安排在维护窗口执行。

过程

步骤 1 选择**管理** > **升级和更新** > **内容更新** > **规则更新** 。

也可以点击入侵规则编辑器页面（**策略** > **+ 显示更多** > **安全策略** > **入侵规则**）上的**导入规则**。

步骤 2 （可选）删除现有的本地规则。

点击**删除所有本地规则**，然后确认是否想要将创建和导入的所有入侵规则移至删除的文件夹。

步骤 3 在 **一次性规则更新/规则导入**下，选择 **规则更新或文本规则文件以上传和安装**，然后点击 **选择文件** 并浏览到您的本地规则文件。

步骤 4 点击 **导入**。

您可以在消息中心监控导入进度。即使消息中心在几分钟内不显示进度或指示更新失败，也不要重启导入。相反，请联系思科 TAC。

下一步做什么

- 编辑入侵策略，并启用已导入的规则。
- 部署配置更改；请参阅 *Cisco Secure Firewall Management Center* 设备配置指南。

导入本地入侵规则最佳实践

导入本地规则文件时，请遵循以下准则：

- 规则导入程序要求以 ASCII 或 UTF-8 编码的纯文本文件导入所有自定义规则。
- 文本文件名称可包含字母数字字符和空格，不可包含除下划线 (_)、句号 (.) 和破折号 (-) 以外的其他特殊字符。
- 系统会导入以一个井号 (#) 开头的本地规则，但它们被标记为已删除。
- 系统会导入以一个井号 (#) 开头的本地规则，但不会导入以两个井号 (##) 开头的本地规则。
- 规则不能包含任何转义字符。
- 在多域部署中，系统将为导入到“全局”域或在该域中创建的规则分配一个为 1 的 GID，并为所有其他域分配一个特定于域的 GID，数值介于 1000 与 2000 之间。
- 导入本地规则时，不必指定生成器 ID (GID)。如果指定了生成器 ID，则请仅为标准文本规则指定 GID 1。
- 首次导入规则时，请勿指定 Snort ID (SID) 或修订版本号。这可避免与其他规则的 SID 发生冲突，包括已删除的规则。系统会自动为规则分配下一个可用的自定义规则 SID（1000000 或更高） 以及版本号 1。

  如果必须导入带有 SID 的规则，则 SID 可以是 1,000,000 或以上的任何唯一数字。

  在多域部署中，如果多个管理员同时导入本地规则，则单个域中的 SID 可能不连续，因为系统已将该序列的中间编号分配给其他域。
- 导入之前已导入的本地规则的更新版本时，或者重新安装已删除的本地规则时，必须包含由系统分配的 SID 以及高于当前编号的修订版本号。您可以通过编辑规则确定当前或已删除规则的修订版本号。

注释 删除本地规则时，系统会自动增加修订版本号；这样方便恢复本地规则。所有已删除的本地规则从会从本地规则类别转移到已删除规则类别。

- 请在高可用性对中的主 防火墙管理中心 上导入本地规则，以避免 SID 编号问题。
- 如果规则包含以下任意一项，则导入失败：

- 大于 2147483647 的 SID。
- 长度超过 64 个字符的源或目的端口列表。
- 在多域部署中，在导入到“全局”域时，GID:SID 组合使用 GID 1 和一个已存在于其他域中的 SID；这表示该组合在版本 6.2.1 之前就已存在。可以使用 GID 1 和一个唯一的 SID 重新导入规则。

- 如果启用某个导入的本地规则，而该规则将弃用的 `threshold` 关键字与某个入侵策略中的入侵事件阈值功能结合起来使用，策略验证将会失败。
- 所有导入的本地规则都会自动保存在本地规则类别中。
- 系统始终将导入的本地规则设置为禁用状态。必须手动设置本地规则的状态后，才能将其用于入侵策略中。

查看入侵规则更新日志

系统会生成规则更新/导入日志，按时间戳、用户以及每次更新是成功还是失败列出。这些日志包含有关所有更新的规则和组件的详细导入信息；请参阅 入侵规则更新日志详情，第 11 页。使用此程序可查看规则导入日志。请注意，删除导入日志不会删除导入的对象。 在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

步骤 1 选择**管理** > **升级和更新** > **内容更新** > **规则更新** 。

步骤 2 点击 **Rule Update Log**。

步骤 3 （可选）点击日志文件旁边的 **视图** ( )，查看任何规则更新的详细信息。

入侵规则更新日志详情

注释 即使是通过在仅显示单个导入文件记录的“规则更新导入日志”(Rule Update Import Log) 详细视图中的工具栏上点击**搜索 (Search)** 发起搜索，也可以搜索整个规则更新导入日志数据库。确保将时间限制条件设置为包含所有搜索中要包含的对象。

表 *2:* 入侵规则更新日志详情

字段	说明
操作	指明对对象类型执行了以下其中一项操作： • `新`（对于规则而言，是指第一次存储此规则） • `changed`（对于规则更新组成部分或规则而言，规则更新组成部分已被修改，或者规则的版本号更高且 GID 和 SID 相同） • `collision`（对于规则更新组成部分或规则而言，由于其版本与现有组成部分或规则相冲突，因此跳过导入） • `deleted`（对于规则而言，已从规则更新删除规则） • `enabled`（对于规则更新编辑而言，已在系统提供的默认策略中启用了预处理器、规则或其他功能） • `disabled`（对于规则而言，已在系统提供的默认策略中禁用规则） • `drop`（对于规则而言，已在系统提供的默认策略中将规则设置为“丢弃并生成事件”[Drop and Generate Events]） • `error`（对于规则更新或本地规则文件而言，导入失败） • `apply`（为导入启用了**在规则更新导入完成后重新应用所有策略 [Reapply all policies after the rule update import completes]** 选项）
默认操作	规则更新定义的默认操作。当导入对象类型是 `rule` 时，默认操作是 `Pass`、`Alert` 或 `Drop`。对于所有其他导入对象类型，没有默认操作。
详细信息	组成部分或规则独有的字符串。对于规则、GID、SID 以及已更改规则的上一个版本号，此字段显示为 `previously (GID:SID:Rev)`。对于未更改的规则，此字段为空白。
域	其入侵策略可使用更新规则的域。后代域中的入侵策略也可以使用该规则。此字段只存在于多域部署中。
GID	规则的生成器 ID。例如，`1`（标准文本规则、全局域或旧 GID）或 `3`（共享对象规则）。
名称	导入对象的名称全部（对于规则，对应的是规则“消息”[Message] 字段；对于规则更新，对应的是组成部分名称）。
策略	对于导入的规则，将显示此字段。这表示规则导入成功，并可在所有相应的默认入侵策略中启用。对于其他导入对象类型，此字段为空白。
版本	规则的版本号。
规则更新	规则更新文件名。
SID	规则的 SID。

字段	说明
时间	导入开始的时间和日期。
类型	导入对象的类型，可以是以下类型之一： • `rule update component`（已导入的组成部分，例如规则包或策略包） • `rule`（对于规则，是指新的或更新的规则） • `policy apply`（为导入启用了**在规则更新导入完成后重新应用所有策略**选项）
计数	每条记录的计数 (`1`)。当表受限时，“计数”(Count) 字段显示在表视图中，而且在默认情况下，“规则更新日志”(Rule Update Log) 详细视图受限于规则更新记录。此字段不可搜索。

维护 air gap 部署

如果防火墙管理中心未连接到互联网，则将不会自动进行必要更新。您必须手动获取并安装这些更新。

有关详细信息，请参阅：

- 手动更新 VDB，第 3 页
- 手动更新入侵规则，第 8 页
- 手动更新 GeoDB，第 5 页

内容更新的历史记录

表 *3:* 内容更新的历史记录

功能	最低管理中心版本	最低威胁防御版本	详细信息
自动 VDB 下载。	7.3.0	任意	防火墙管理中心的初始设置安排了每周下载最新可用软件更新的任务，其中现在包括最新的漏洞数据库 (VDB)。我们建议您查看此每周任务，并在必要时进行调整。或者，安排新的周期性任务，以便实际更新 VDB 和/或软件并部署配置。 新增/修改的屏幕：默认情况下，系统创建的 **每周软件下载** 计划任务中的 **漏洞数据库** 复选框现在处于启用状态。

功能	最低管理中心版本	最低威胁防御版本	详细信息
安装任何 VDB。	7.3.0	任意	从 VDB 357 开始，您可以安装任何 VDB，直至防火墙管理中心的基准 VDB。 更新 VDB 后，部署配置更改。如果您基于漏洞、应用检测器或不再可用的指纹进行配置，请检查这些配置以确保按预期处理流量。另请记住，更新 VDB 的计划任务可以撤消回滚。要避免这种情况，请更改计划任务或删除任何较新的 VDB 软件包。 新增/修改的屏幕：在**系统**（⚙）> **更新 (Updates)** > **产品更新 (Product Updates)** > **可用更新 (Available Updates)**，如果上传较旧的 VDB，系统将显示新的**回滚**图标，而不是**安装**图标。
内容更新和产品升级不再共用一个页面。	7.2.6 7.4.1	任意	内容更新和产品升级不再共用一个页面。 • **系统**（⚙）> **内容更新**可以更新入侵规则、VDB 和 GeoDB。 • **系统**（⚙）> **产品升级**可以升级防火墙管理中心和所有托管设备，以及管理升级包。 • **系统**（⚙）> **更新 (Updates)**已弃用。所有Firewall Threat Defense升级使用向导。
已弃用：维护版本的计划下载。	7.2.6 7.4.1	任意	**升级影响。计划的下载任务停止检索维护版本。** **下载最新更新**计划任务不再下载维护版本；现在，它仅下载最新的适用补丁和 VDB 更新。要将维护（和主要）版本直接下载到防火墙管理中心，请使用**系统**（⚙）> **产品升级**。
规则冲突时，自定义入侵规则导入会发出警告。	6.7.0	任意	现在，当您导入自定义（本地）入侵规则时，系统会警告您发生规则冲突。以前，系统会以静默方式跳过导致冲突的规则 - 版本 6.6.0.1 除外，其中包含冲突的规则导入将完全失败。 在“规则更新”页面上，如果规则导入发生冲突，则“状态”列中会显示警告图标。有关详细信息，请将鼠标指针悬停在警告图标上，然后阅读工具提示。 请注意，当您尝试导入与现有规则具有相同SID/修订号的入侵规则时，会发生冲突。您应始终确保自定义规则的更新版本具有新的修订版本号。 新增/修改的屏幕：我们在**系统**（⚙）> **更新 (Updates)** > **规则更新 (Rule Updates)** 中添加了一个警告图标。
在初始设置期间自动更新 VDB。	6.6.0	任意	设置新的或重新映像的 防火墙管理中心时，系统会尝试更新漏洞数据库 (VDB)。 这是一次性操作。如果 防火墙管理中心 已接入互联网，我们建议您安排自动定期下载和安装 VDB 更新的任务。

功能	最低管理中心版本	最低威胁防御版本	详细信息
自动软件下载和GeoDB更新。	6.5.0	任意	当您设置新的或重新镜像的防火墙管理中心时，系统会安排每周补丁下载和 GeoDB 更新。
签名的 SRU、VDB 和 GeoDB 更新。	6.4.0	任意	因此，系统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。 除非您手动下载更新（例如，在物理隔离部署中），否则您应该不会注意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。 签名更新文件以“Cisco”（而不是“Sourcefire”）开头，以 .sh.REL.tar（而不是 .sh）结尾，如下所示： • 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 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。如果您意外将已签名的更新上传到较早的 防火墙管理中心 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。
VDB 更新前的 Snort 重启警告。	6.2.3	任意	系统现在会警告您漏洞数据库 (VDB) 更新会重启 Snort 进程。这会中断流量检查，并且可能会中断流量，具体取决于托管设备处理流量的方式。您可以取消安装，直到更方便的时间，例如在维护窗口期间。 可能会出现以下警告： • 下载并手动安装 VDB 后。 • 当您创建计划任务来安装 VDB 时。 • VDB在后台安装，例如，在之前安排的任务期间，或作为软件升级的一部分。
已弃用：地理位置详细信息	6.2.3	任意	我们不再提供 地理位置 IP 包，其中包含与可路由 IP 地址关联的情景数据。这样可以节省磁盘空间，而且不会以任何方式影响地理位置规则或流量处理。任何上下文数据现在都是过时的，升级到大多数后续版本都会删除 IP 包。用于下载 IP 软件包或查看情景数据的选项不起作用，并在更高版本中被删除。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。