更新

以下主题介绍如何更新 Firepower 部署：

关于系统更新

您可以使用管理中心为自身及其管理的设备升级系统软件。您还可以更新提供高级服务的各种数据库和源。

对于可以访问互联网的 管理中心，系统通常可以直接从思科获取更新。我们建议您尽可能安排或启用自动更新。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 。您必须自行安排其他更新。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:* 升级和更新

组件	说明	详细信息
系统软件	主要 软件版本包含新功能、新功能和增强功能。它们可能包括基础设施或架构更改。 维护 版本包含常规漏洞和安全相关修复。行为更改很少见，并且与这些修复相关。 补丁 是按需更新，仅限于具有紧急性的关键修复程序。 热补丁 可以解决特定的客户问题。	**直接下载：** 仅选择版本，通常在版本可用于手动下载后的一段时间。延迟的长度取决于版本类型、版本采用情况和其他因素。 **计划：** 仅安装补丁，在 **系统**（⚙）> **工具** > **计划**。 **卸载：** 仅修补程序。 **恢复/重新映像：** 仅限主版本和维护版本。 **请参阅：** 升级系统软件，第 4 页
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。	**直接下载：** 确认。 **计划：** 确认，在 **系统**（⚙）> **工具** > **计划**。 **卸载：** 否。 **请参阅：** 更新漏洞数据库 (VDB)，第 4 页
地理位置数据库 (GeoDB)	思科地理位置数据库 (GeoDB) 是一个与可路由的 IP 地址关联的地理数据数据库。	**直接下载：** 确认。 **计划：** 确认，在 **系统**（⚙）> **更新**。 **卸载：** 否。 **请参阅：** 更新地理定位数据库，第 6 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。	**直接下载：** 确认。 **计划：** 确认，在 **系统**（⚙）> **更新**。 **卸载：** 否。 **请参阅：** 更新入侵规则，第 7 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。	**直接下载：** 确认。 **计划：** 确认，在 **对象** > **对象管理**。 **卸载：** 否。 **请参阅：** 《Cisco Secure Firewall Management Center 设备配置指南》

组件	说明	详细信息
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。	**直接下载：** 确认。 **计划：** 是，在 **集成** > **其他集成** > **云服务** 或 **系统**（⚙）> **工具** > **计划**上，具体取决于您的要求。 **卸载：** 否。 **请参阅：** 《Cisco Secure Firewall Management Center 设备配置指南》

系统更新的要求和必备条件

型号支持

任意

支持的域

全局 除非另有说明。

用户角色

管理员

系统更新的准则和限制

在更新之前

在更新 Firepower 部署的任何组件（包括入侵规则、VDB 或 GeoDB）之前，请阅读更新随附的版本说明或建议性文本。这些内容提供版本特定的关键信息，包括兼容性、必备条件、新功能、行为更改和警告。

计划的更新

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。

重要事项 我们 强烈 建议您查看计划任务，确保计划的更新在您预期的时间执行。

带宽准则

要升级 Firepower 设备（或执行就绪性检查），升级包必须位于设备上。Firepower 升级程序包大小不同。请确保您的带宽足以将大量数据传输到您管理的设备。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）。

升级系统软件

本指南不包含系统软件或配套操作系统的详细升级说明。请参阅适用于您的版本的《适用于管理中心的 Cisco 安全防火墙威胁防御升级指南》 。

有关安排系统软件补丁下载和安装的信息，请参阅 软件更新自动化。请注意，初始设置过程会自动安排每周下载一次补丁。设置后，您应查看自动安排的配置，并在必要时对其进行调整。

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 Cisco Secure Firewall Management Center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）。

设置新的或重新映像时 管理中心，系统会自动尝试更新漏洞数据库 (VDB)。这是一次性操作。如果管理中心 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。

注意 在大多数情况下，更新 VDB 后的第一次部署会重新启动受管设备上的 Snort 进程。系统会警告您可能会发生这种情况 - 警告可能会在手动 VDB 更新后、安排 VDB 更新时、在后台 VDB 更新期间以及在部署时出现。Snort 重启会导致流量检查中断，并且可能会中断流量，具体取决于受管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。

手动更新 VDB

要更新 VDB，VDB 更新包必须位于 管理中心上。

如果 管理中心 无法访问互联网，或者希望将 VDB 更新手动上传到 管理中心，则请使用此程序。要自动执行 VDB 更新，请使用任务计划（**系统**（⚙）> **工具** > **计划**）。有关详细信息，请参阅漏洞数据库更新自动化。

开始之前

- 从 https://www.cisco.com/go/firepower-software 下载更新。

注释 从 VDB 版本 343 开始，所有应用检测器信息均可通过思科安全防火墙应用检测器来获取。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。

- 请考虑更新因 Snort 重启而对流量和检测的影响。我们建议在维护窗口执行更新。

过程

步骤 1 选择 **系统**（⚙）> **更新**，然后点击**产品更新 (Product Updates)**。

步骤 2 选择您希望以什么方式将 VDB 更新上传到 管理中心。

- 直接从 Cisco.com 下载：点击**下载更新 (Download Updates)**。如果可以访问思科支持和下载站点，则管理中心会下载最新的VDB。请注意，管理中心还会下载与设备当前运行版本关联的各个补丁和修补程序（而非主要版本）的数据包。
- 手动上传：点击**上传更新 (Upload Update)**，然后点击**选择文件 (Choose File)**。浏览到之前下载的更新，然后点击**上传**。

VDB 更新与 Firepower 软件升级和卸载程序软件包在同一页面上显示。

步骤 3 安装更新。

a) 点击漏洞和指纹数据库更新旁的“安装”(Install)。
b) 选择 管理中心。
c) 点击**安装**。

步骤 4 （可选）在消息中心监控更新进度。

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。而是联系思科 TAC。

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 5 验证更新是否成功。

选择**帮助** > **关于**查看当前的 VDB 版本。

下一步做什么

部署配置更改；请参阅 《Cisco Secure Firewall Management Center 管理指南》 。

安排 VDB 更新

如果 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。

更新地理定位数据库

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。

系统随附一个将 IP 地址映射到国家/地区/大洲的初始 GeoDB 国家/地区代码包，因此信息应始终可用。如果您更新 GeoDB，系统还会下载 包含 情景数据的 IP 数据包。此情景数据包括其他位置详细信息，以及连接信息，例如 ISP、连接类型、代理类型、域名等。我们还会定期更新 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， 系统配置每周的自动 GeoDB 更新。如果配置更新失败且 管理中心 可以访问互联网，我们建议您配置常规 GeoDB 更新，如 安排 GeoDB 更新，第 6 页。

更新 GeoDB 所需的时间取决于您的设备，但最多可能需要 45 分钟，具体取决于更新的大小（例如，如果这是您第一次下载完整的 GeoDB）。虽然 GeoDB 更新不会中断任何其他系统功能（包括正在进行的地理位置信息收集），但更新执行时的确会占用系统资源。制定更新计划时需要考虑这一点。

GeoDB 更新将会覆盖之前的所有 GeoDB 版本并立即生效。更新 GeoDB 时，管理中心会自动更新其受管设备上的相关数据。GeoDB 更新可能需要几分钟时间才能在整个部署中生效。更新后，无需重新部署。

系统（⚙） > **更新** > **地理位置更新** 页面和 **帮助** （?） > **关于** 页面均列出了当前版本。

安排 GeoDB 更新

作为初始配置的一部分， 系统配置每周的自动 GeoDB 更新。如果配置更新失败且 管理中心 可以访问互联网，我们建议您配置常规 GeoDB 更新，如 此程序。

开始之前

确保 管理中心可以访问互联网。

过程

步骤 1 选择**系统**（⚙） > **更新** > **地理位置更新**。

步骤 2 在周期性地理位置更新下，选择 **从支持站点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（互联网连接）

如果 管理中心 可以访问互联网，请使用此程序对 GeoDB 执行按需更新。

过程

步骤 1 选择**系统**（⚙）> **更新** > **地理位置更新**。

步骤 2 在一次性地理位置更新下，选择 **从支持站点下载并安装地理位置更新**。

步骤 3 点击**导入**。

您可以在消息中心监控更新的进度。

步骤 4 验证更新是否成功。

“地理位置更新”页面和 **帮助** （?）> **关于** 页面均列出当前版本。

手动更新 GeoDB（无互联网连接）

如果 管理中心 无法访问互联网，请使用此程序执行 GeoDB 的按需更新。

过程

步骤 1 从 思科支持和下载站点下载 GeoDB： 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 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。

确保下载国家/地区代码和 IP 软件包。

步骤 2 选择**系统**（⚙）> **更新** > **地理位置更新**。

步骤 3 在一次性地理位置更新下，选择 **上传并安装地理位置更新**。

步骤 4 点击 **选择文件**，然后浏览到您之前下载的 国家/地区代码 包。

步骤 5 点击**导入**。

您可以在消息中心监控更新的进度。

步骤 6 对 IP 包重复步骤 4 和 5。

步骤 7 验证更新是否成功。

“地理位置更新”页面和 **帮助** （?）> **关于** 页面均列出当前版本。

更新入侵规则

随着新漏洞的暴露，Talos 情报小组 会发布可导入到 Cisco Secure Firewall Management Center上的入侵规则更新，然后通过将已更改的配置部署到受管设备进行实施。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。

入侵规则更新是累加性的，并且思科建议始终导入最新的更新。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以下内容：

- **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。

周期性入侵规则更新

可以在 Rule Updates 页面上设置为按日、周或月导入规则更新。

如果部署包括Cisco Secure Firewall Management Center的高可用性对，则仅在主防御中心上导入更新。辅助Cisco Secure Firewall Management Center会在常规同步过程中接收规则更新。

入侵规则更新导入中的适用子任务按以下顺序出现：下载、安装、基本策略更新和策略部署。完成一个子任务后，才会开始下一个子任务。

在计划的时间，系统按照在先前步骤中所指定，安装规则更新并部署已更改的配置。在导入之前或导入过程中，可注销或使用 Web 界面执行其他任务。在导入过程中访问时，“规则更新日志”显示**红色状态**（  ），此外，您还可以在“规则更新日志”详细视图中查看消息。根据规则更新大小和内容，可能几分钟之后才会显示状态消息。

作为初始配置的一部分，系统配置每日从 思科支持和下载站点自动更新入侵规则。（系统在下次部署受影响的策略时向受影响的受管设备部署自动化入侵规则更新。）如果配置更新失败且 管理中心可以访问互联网，我们建议您配置定期入侵规则更新，如 计划入侵规则更新，第 10 页.

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。

一次性手动更新入侵规则

如果 Cisco Secure Firewall Management Center无法访问互联网，则请手动导入新的入侵规则更新。

过程

步骤 1 从思科支持站点 (http://www.cisco.com/cisco/web/support/index.html) 手动下载更新。

步骤 2 选择 **系统**（  ）> **更新**，然后点击 **规则更新**。

步骤 3 如果要将已创建或导入的所有用户定义的规则都移至已删除的文件夹，则必须点击工具栏中的**删除所有本地规则 (Delete All Local Rules)**，然后点击**确定 (OK)**。

步骤 4 选择**要上传并安装的规则更新或文本规则文件 (Rule Update or text rule file to upload and install)**，然后点击**浏览 (Browse)** 以浏览并选择规则更新文件。

步骤 5 如果要在更新完成后自动将策略重新部署到受管设备，请选择**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)**。

步骤 6 点击 **Import**。系统将安装规则更新并显示“规则更新日志”(Rule Update Log) 详细视图。

注释 如果在安装规则更新时出现错误消息，请联系支持部门。

一次性自动更新入侵规则

注释 此部分适用于 Snort 2。

要自动导入新的入侵规则更新，设备必须具有互联网访问权限以连接到支持站点。

开始之前

- 确保 管理中心能够访问互联网；请参阅安全、互联网接入和通信端口。

过程

步骤 1 选择**系统**（⚙）> **更新**。

注释 也可以点击入侵规则编辑器页面（**对象** > **入侵规则**）上的**导入规则**。

步骤 2 点击 **规则更新**。

步骤 3 如果要将已创建或导入的所有用户定义的规则都移至已删除的文件夹，请点击工具栏中的**删除所有本地规则 (Delete All Local Rules)**，然后点击**确定 (OK)**。

步骤 4 选择**从支持站点下载新规则更新 (Download new Rule Update from the Support Site)**。

步骤 5 如果要在更新完成后自动将已更改的配置部署到受管设备，请选中**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)** 复选框。

步骤 6 点击 **Import**。
系统将安装规则更新并显示“规则更新日志”(Rule Update Log) 详细视图。

注意 如果在安装规则更新时出现错误消息，请联系支持部门。

计划入侵规则更新

注释 此部分适用于 Snort 2。

作为初始配置的一部分，系统配置每日从 思科支持和下载站点自动更新入侵规则。（系统在下次部署受影响的策略时向受影响的受管设备部署自动化入侵规则更新。）如果配置更新失败且 管理中心可以访问互联网，我们建议您配置定期入侵规则更新，如 此部分。

过程

步骤 1 选择**系统**（⚙）> **更新**。

注释　也可以点击入侵规则编辑器页面（**对象** > **入侵规则**）上的**导入规则**。

步骤 2 点击 **规则更新**。

步骤 3 如果要将已创建或导入的所有用户定义的规则都移至已删除的文件夹，请点击工具栏中的**删除所有本地规则 (Delete All Local Rules)**，然后点击**确定 (OK)**。

步骤 4 选中 **启用从支持网站重复规则更新导入** 复选框。

导入状态消息显示在 **Recurring Rule Update Imports** 部分下方。

步骤 5 在**导入频率 (Import Frequency)** 字段中，指定：

- 更新频率（**每天 [Daily]**、**每周 [Weekly]** 或**每月 [Monthly]**）
- 要发生更新的周日期或月日期
- 要开始更新的时间

步骤 6 如果要在更新完成后自动将已更改的配置重新部署到受管设备，请选中**在规则更新完成后将已部署的策略部署到目标设备 (Deploy updated policies to targeted devices after rule update completes)** 复选框。

步骤 7 点击**保存 (Save)**。

注意　如果在安装入侵规则更新时收到错误消息，请联系支持部门。

Recurring Rule Update Imports 部分下方的状态信息会发生变化，以指明尚未运行规则更新。

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 Firepower 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。

导入本地入侵规则

- 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 11 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。
- 您可以在任何域中执行此任务。

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。

过程

步骤 1 选择 **系统**（⚙）> **更新**，然后点击 **规则更新**。

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 **Import**。

步骤 5 可以在消息中心监控导入进度。

要显示消息中心，请点击菜单栏上的“系统状态”。即使在消息中心有几分钟时间不显示，或指示导入失败，也不要重启导入，而是联系思科 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》中的 部署配置更改

规则更新日志

Cisco Secure Firewall Management Center会为导入的规则更新和本地规则文件生成记录。

每个记录都包含时间戳、导入文件的用户名称以及指明导入成功或失败的状态图标。可保留导入的所有规则更新和本地规则文件的列表，删除列表中的任何记录，以及访问有关所有导入的规则和规则更新组成部分的详细记录。

“规则更新导入日志”详细视图列出导入到规则更新或本地规则文件中的每个对象的详细记录。此外，还可以根据列出的记录创建仅包含符合特定需求的信息的自定义工作流程或报告。

入侵规则更新日志表

表 *2:* 入侵规则更新日志字段

字段	说明
摘要	导入文件的名称。如果导入失败，文件名称下方会显示有关导入失败原因的简要说明。
时间	导入开始的时间和日期。
用户 ID	触发导入的用户的用户名。

字段	说明
状态	导入有以下状态： • **成功图标**（） • 失败或进行中 **红色状态**（） 导入过程中，Rule Update Log 页面上会显示红色状态图标，表示导入失败或未完成；成功完成导入后，该红色状态图标会变为绿色状态图标。

提示 可以在入侵规则更新导入正在进行中时查看显示的导入详细信息。

查看入侵规则更新日志

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**系统**（）> **更新**。

提示 也可以点击入侵规则编辑器页面（**对象** > **入侵规则**）上的**导入规则**。

步骤 2 点击 **规则更新**。

步骤 3 点击 **Rule Update Log**。

步骤 4 此时您有两种选择：

- 查看 - 要查看规则更新或本地规则文件中导入的每个对象的详细信息，请点击要查看的文件旁边的 **视图**（）；请参阅 查看入侵规则更新导入日志的详细信息，第 16 页。
- 删除 - 要删除导入日志中的导入文件记录（包括文件中包含的所有对象的详细记录），请点击导入文件名旁边的 **删除**（）。

  注释 删除日志中的文件并不会删除导入到导入文件中的任何对象，而只是删除导入日志记录。

入侵规则更新日志中的字段

提示 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 *3:* 规则更新导入日志详细视图字段

字段	说明
操作	指明对对象类型执行了以下其中一项操作： • `new`（对于规则而言，是指第一次把规则存储在此设备上） • `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，由于版本与设备上的现有组成部分或规则冲突，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（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，此字段显示`所有`。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。
时间	导入开始的时间和日期。

字段	说明
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`（对于规则而言，是指新的或更新后的规则；请注意，在版本 5.0.1 中，此值替换为 `update` 值，后者已被弃用） • `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。

查看入侵规则更新导入日志的详细信息

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**系统**（⚙）> **更新**。

提示 也可以点击入侵规则编辑器页面（**对象** > **入侵规则**）上的**导入规则**。

步骤 2 点击 **规则更新**。

步骤 3 点击 **Rule Update Log**。

步骤 4 点击要查看的详细记录的文件的旁边的 **视图**（👁）。

步骤 5 可以采取以下任何操作：

- 书签 - 要将当前页面加入书签，请点击 **将此页面加入书签**。
- 编辑搜索 - 要打开使用当前单一限制预填充的搜索页面，请选择“搜索限制”旁边的 **编辑搜索** 或 **保存搜索** 。
- 管理书签 - 要导航至书签管理页面，请点击 **报告设计器**。
- 报告 - 要根据当前视图中的数据生成报告，请点击 **报告设计器**。
- 搜索 - 要搜索整个规则更新导入日志数据库以查找规则更新导入记录，请点击 **搜索**。
- 排序 - 要对当前工作流程页面上的记录进行排序和限制，请参阅 使用向下钻取页面 以了解详细信息。
- 切换工作流程 - 要暂时使用其他工作流程，请点击 （**切换工作流程**）。

维护气隙部署

如果 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。请参阅以下信息：

- 手动更新 VDB， 第 4 页
- 一次性手动更新入侵规则， 第 9 页
- 手动更新 GeoDB（无互联网连接）， 第 7 页
- 升级指南位于 https://www.cisco.com/c/en/us/td/docs/security/firepower/upgrade/fpmc-upgrade-guide.html

系统更新的历史记录

功能	版本	详细信息
在设备之间复制升级包（“点对点同步”）。	7.2	您可以使用 威胁防御 CLI 在设备之间复制升级包，而不是从 管理中心 或内部 Web 服务器将升级包复制到每台设备（“点对点同步”）。这种安全可靠的资源共享通过管理网络进行，但不依赖于 管理中心。每个设备可容纳 5 个数据包并发传输。 由同一独立设备管理的 7.2 及更高版本的独立设备支持此功能 管理中心 。不支持： • 容器实例。 • 设备高可用性对和集群。 请注意，版本 7.1+ 的组成员可以在正常同步过程中相互获取软件包。将升级包复制到一个组成员会自动将其同步到所有组成员。 • 由高可用性 管理中心管理的设备。 • 由云提供的管理中心管理，但在分析模式下添加到客户部署的 管理中心 。 • 不同域中的设备或由 NAT 网关分隔的设备。 • 从版本 7.1 或更早版本升级的设备，无论 管理中心 版本如何。 新增/修改的CLI 命令： **configure p2psync enable**、 **configure p2psync disable**、 **show peers**、 **show peer details**、 **sync-from-peer**、 **show p2p-sync-status**

功能	版本	详细信息
成功升级威胁防御后自动升级到 Snort 3。	7.2	当您使用版本 7.2+ 管理中心升级威胁防御时，您现在可以选择是否 **将 Snort 2 升级到 Snort 3**。 在软件升级后，当您部署配置时，符合条件的设备将从 Snort 2 升级到 Snort 3。对于因使用自定义入侵或网络分析策略而不符合条件的设备，我们强烈建议您手动升级到 Snort 3 以提高检测和性能。有关迁移方面的帮助，请参阅适用于您的版本的 《Cisco Secure Firewall Management Center Snort 3 配置指南》 。 此选项支持主要和维护威胁防御升级到版本 7.2+。威胁防御升级到版本 7.0 或 7.1 或任何版本的补丁均不支持此功能。
升级单节点集群。	7.2	现在，您可以使用设备升级页面（**设备** > **设备升级**）升级只有一个主用节点的集群。任何已停用的节点也会升级。以前，此类升级会失败。系统更新页面不支持此功能（**系统** > **更新**）。 在这种情况下，也不支持无中断升级。流量和检测的中断取决于单独的主用设备的接口配置，就像使用独立设备一样。 支持的平台：Firepower 4100/9300、安全防火墙 3100
从 CLI 恢复威胁防御升级。	7.2	如果管理中心和设备之间的通信中断，您现在可以从设备 CLI 恢复威胁防御升级。请注意，在高可用性/可扩展性部署中，当所有设备同时恢复时，恢复更成功。使用 CLI 恢复时，打开所有设备的会话，验证每个设备是否可以恢复，然后同时启动进程。 **注意** 从 CLI 恢复可能会导致设备和管理中心之间的配置不同步，具体取决于您在升级后所做的更改。这可能会导致进一步的通信和部署问题。 新增/修改的CLI 命令： **upgrade revert**、 **show upgrade revert-info**。 有关详细信息，请参阅管理中心升级指南中的 恢复升级 。
GeoDB 分为两个软件包。	7.2	在 2022 年 5 月，版本 7.2 发布前不久，我们将 GeoDB 拆分为两个包：一个将 IP 地址映射到国家/地区/大洲的国家/地区代码包，以及一个包含与可路由 IP 地址相关的上下文数据的 IP 包。此 IP 包中的情景数据可包括其他位置详细信息，以及连接信息，例如 ISP、连接类型、代理类型、域名等。 如果您的版本 7.2+ 管理中心可以访问互联网，并且您启用定期更新或从 思科支持和下载站点手动启动一次性更新，则系统会自动获取并导入这两个软件包。但是，如果您手动下载更新（例如，在气隙式部署中），请确保获取并导入两个 GeoDB 软件包： • 国家代码包： Cisco_GEODB_Update-*date-build*.sh.REL.tar • IP 软件包： Cisco_IP_GEODB_Update-*date-build*.sh.REL.tar 地理位置更新（**系统**（⚙） > **更新** > **地理位置更新**）页面和关于页面（**帮助** > **关于**）列出系统当前使用的软件包的版本。

功能	版本	详细信息
升级不会自动生成故障排除文件。	7.2	为了节省时间和磁盘空间，管理中心升级过程在升级开始前不再自动生成故障排除文件。请注意，设备升级 不受影响 ，并会继续生成故障排除文件。 要为管理中心手动生成故障排除文件，请选择 **系统**（⚙）> **运行状况** > **监控**，点击左侧面板中的 **防火墙管理中心** ，然后 **查看系统和故障排除详细信息**，然后 **生成故障排除文件**。
恢复成功的设备升级。	7.1	现在，您可以从 管理中心 Web 接口将主要升级和维护升级恢复为 威胁防御 。恢复可将软件恢复到上次升级前的状态，也称为 快照。修补后恢复必然也会删除修补程序。 如果您认为可能需要恢复，则必须使用 **系统** > **升级** 页面进行升级 威胁防御。“系统更新”页面是唯一可以启用 **成功升级后启用恢复** 选项的位置，该选项会将系统配置为在启动升级时保存恢复快照。这与我们通常建议使用 **设备** > **设备升级** 页面上的向导形成鲜明对比。 Firepower 4100/9300 上的容器实例不支持此功能。
改进了集群和高可用性设备的升级工作流程。	7.1	威胁防御 升级向导现在可以正确地将集群和高可用性设备显示为组，而不是单个设备。系统可以识别、报告和预先要求修复您可能遇到的组相关问题。例如，如果在 机箱管理器上进行了未同步的更改，则无法升级 Firepower 4100/9300 上的集群。 您还可以指定集群中数据设备的升级顺序。
改进了 威胁防御 升级性能和状态报告。	7.0	升级 威胁防御 现在更容易、更快速、更可靠，并且占用的磁盘空间更少。消息中心的新 **升级** 选项卡进一步增强了升级状态和错误报告功能。

功能	版本	详细信息
易于遵循 威胁防御 升级工作流程。	7.0	新的设备升级页面（**设备** > **设备升级**）为升级版本 6.4+ 威胁防御提供了易于遵循的工作流程。 系统将引导您完成重要的预升级阶段，包括： • 选择要升级的设备。 • 将升级包复制到设备。 • 兼容性和就绪性检查。 首先，请使用“设备管理”页面上的新 **升级 Firepower 软件** 操作（**设备** > **设备管理** > **选择操作**）。 **注释** 您仍必须使用“系统更新”页面 **(系统** > **更新)** 页面上传或指定 威胁防御 升级包的位置。您还必须使用“系统更新”页面升级 管理中心 本身以及所有非-威胁防御 受管设备。 继续升级工作流程操作时，系统会显示有关所选设备的基本信息以及当前的升级相关状态。这包括无法升级的任何原因。如果设备未在工作流程中“通过”某个阶段，则该阶段不会显示在下一阶段。 如果您离开工作流程，系统会保留您的进度，但具有管理员访问权限的其他用户可以重置、修改或继续工作流程。 **注释** 在版本 7.0，设备升级页面无法正确显示集群或高可用性对中的设备。即使必须将这些设备作为一个单元进行选择和升级，工作流程也会将其显示为独立设备。设备状态和升级就绪性会逐个评估和报告。这意味着一台设备可能会“传递”到下一阶段，而另一台设备则不会。但是，这些设备仍然分组。因此，在一台设备上运行就绪性检查，所有设备上都会运行。在一台设备上启动升级，在所有设备上都会启动升级。 为避免可能的耗时升级失败，请 手动 确保所有组成员都已准备好继续执行工作流程的下一步，然后再点击 **下一步**。

功能	版本	详细信息
立即升级更多威胁防御设备。	7.0	威胁防御 升级工作流程解除了以下限制： • 同步设备升级。 一次可以升级的设备数量现在受管理网络带宽的限制，而不是系统管理同步升级的能力。以前，我们建议不要一次升级超过五台设备。 **重要事项** 只有升级到版本 6.7+ 才能看到此改进。威胁防御如果您要将设备升级到较旧的 威胁防御 版本（即使您使用的是新的升级工作流程），我们仍建议您一次限制为五台设备。 • 按设备型号分组升级。 现在，只要系统有权访问相应的升级包，您就可以同时对所有 威胁防御 型号进行排队和调用。 以前，您需要选择一个升级包，然后使用该包选择要升级的设备。这意味着 只有 共享升级包时，您才能同时升级多台设备。例如，您可以同时升级两台 Firepower 2100 系列设备，但不能同时升级 Firepower 2100 系列和 Firepower 1000 系列。

功能	版本	详细信息
改进了 威胁防御 升级状态报告和取消/重试选项。	6.7	您现在可以在“设备管理”页面上查看 威胁防御 设备升级和就绪性检查的状态，以及升级成功/失败的 7 天历史记录。消息中心还提供增强的状态和错误消息。 在“设备管理”和“消息中心”中点击一下即可访问新的“升级状态”弹出窗口，其中显示详细的升级信息，包括剩余百分比/时间、特定升级阶段、成功/失败数据、升级日志等。 此外，在此弹出窗口中，您可以手动取消失败或正在进行的升级（**取消升级**），或重试失败的升级（**重试升级**）。取消升级会将设备恢复到升级前的状态。 **注释** 要能够手动取消或重试失败的升级，必须禁用使用 管理中心 升级 威胁防御 设备时出现的新自动取消选项：**升级失败时自动取消并回滚到以前的版本**。启用选项后，设备会在升级失败时自动恢复到升级前的状态。 补丁不支持自动取消。在高可用性或集群部署中，自动取消会单独应用于每个设备。也就是说，如果一台设备上的升级失败，则仅恢复该设备。 新增/修改的屏幕： • **系统** > **更新** > **产品更新** > **可用更新**威胁防御 **升级包的 安装** 图标 • **设备** > **设备管理** > **升级** • **消息中心** > **任务** 新增/修改的CLI 命令： **show upgrade status detail**，**show upgrade status continuous**，**show upgrade status**，**upgrade cancel**，**upgrade retry**
升级会删除 PCAP 文件以节省磁盘空间。	6.7	升级现在会删除本地存储的 PCAP 文件。必须拥有足够的可用磁盘空间，否则升级会失败。
规则冲突时，自定义入侵规则导入会发出警告。	6.7	现在，当您导入自定义（本地）入侵规则时， 管理中心 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。应始终确保自定义规则的更新版本具有新的修订版本号；有关更多最佳实践，请参阅 导入本地入侵规则最佳实践 ，第 11 页。 新增/修改的屏幕：我们在 **系统** > **更新** > **规则**更新中添加了一个警告图标。

功能	版本	详细信息
从内部 Web 服务器获取威胁防御 升级包。	6.6	威胁防御 设备现在可以从您自己的内部 Web 服务器而不是从 管理中心获取升级包。这在 管理中心 及其设备之间的带宽有限时尤其有用。它还可以节省 管理中心 上的空间。 **注释** 此功能仅支持运行版本 6.6+ 的 威胁防御 设备。它不支持升级 到 版本 6.6，也不支持 管理中心 或经典设备。 新增/修改的屏幕：我们在上传升级包的页面中添加了 **指定软件更新源** 选项。
管理中心 会在初始设置期间下载并安装最新的 VDB。	6.6	设置新的或重新映像的 管理中心时，系统会自动尝试更新漏洞数据库 (VDB)。 这是一次性操作。如果 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。
管理中心 在初始设置期间安排软件下载和 GeoDB 更新。	6.5	当您设置新的或重新映像的 管理中心时，系统会自动安排： • 为 管理中心 及其托管设备下载软件更新的每周任务。 • GeoDB 的每周更新。 任务是在 UTC 中安排的，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，由于任务是以 UTC 为单位进行计划的，因此它们不会针对夏令时、夏令时或您在地点可能观察到的任何季节性调整进行调整。如果您受到影响，则根据当地时间，安排的任务在夏季要比冬季“晚”一个小时。我们建议您查看自动安排的配置，并在必要时对其进行调整。
管理中心 升级期间推迟的计划任务。	6.7 6.6.3 6.4.0.10	现在，计划任务会在 管理中心 升级期间推迟。任何计划在升级期间开始的任务都将在升级后重新启动后五分钟开始。 **注释** 在开始任何升级之前，您仍必须确保运行任务已完成。在升级开始时运行的任务会停止，成为失败的任务，且不能恢复。 请注意，从受支持的版本进行的所有升级均支持此功能。这包括 6.4.0.10 及更高版本补丁、版本 6.6.3 及更高维护版本以及版本 6.7.0+。从不支持的版本升级到支持的版本时，不支持此功能。

功能	版本	详细信息
签名的 SRU、VDB 和 GeoDB 更新。	6.4	因此，系统可以验证您使用的是正确的更新文件，系统现在使用 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。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 不要解压签名的 (.tar) 包。
更快的升级。	6.4	事件数据库改进允许更快的升级。
升级前，将升级包复制到托管设备。	6.2.3	现在，您可以在运行实际升级之前，将升级软件包从 管理中心 复制（或推送）到受管设备。这是非常有用的，因为您可以在“升级维护”窗口之外的低带宽使用时间内推送。 当您推送到高可用性、群集或可堆叠设备时，系统首先将升级软件包发送到活动/主要/首要设备，然后再发送到备用/数据/辅助设备。 新增/修改的屏幕： **系统** > **更新**
在 VDB 更新之前， 管理中心 会重新启动警告。	6.2.3	现在 管理中心 会警告您漏洞数据库 (VDB) 更新会重新启动 Snort 进程。这会中断流量检查，并且可能会中断流量，具体取决于受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。

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。