

从 Snort 2 迁移到 Snort 3

从版本 7.0 开始，Snort 3 是具有 防火墙管理中心 的新 防火墙威胁防御 部署的默认检测引擎。如果您仍在使用 Snort 2 检测引擎，请立即切换到 Snort 3 以提高检测和性能。

将 防火墙威胁防御 升级到版本 7.2 至 7.6 也会将符合条件的 Snort 2 设备升级到 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，可在此处手动升级到 Snort 3 以提高检测和性能。

虽然您可以切换回单个设备，但不应这样做。Snort 2 将在未来版本中弃用，最终将阻止 防火墙威胁防御 升级。

- Snort 3 检测引擎，第 1 页
- 网络分析和入侵策略的必备条件，第 2 页
- 如何从 Snort 2 迁移到 Snort 3，第 2 页
- 查看 Snort 2 和 Snort 3 基本策略映射，第 6 页
- 将 Snort 2 规则与 Snort 3 同步 ，第 6 页
- 部署配置更改，第 7 页

Snort 3 检测引擎

Snort 3 是版本 7.0 及更高版本的新注册 防火墙威胁防御 设备的默认检测引擎。但是，对于较低版本的 防火墙威胁防御 设备，Snort 2 是默认检测引擎。将受管 防火墙威胁防御 设备升级到版本 7.0 或更高版本时，检测引擎仍保留在 Snort 2 上。要在 7.0 及更高版本的升级后 防火墙威胁防御的使用 Snort 3，必须明确启用它。当启用 Snort 3 作为设备的检测引擎时，在设备上应用（通过访问控制策略）的入侵策略的 Snort 3 版本将被激活并应用于通过该设备的所有流量。

您可以根据需要切换 Snort 版本。映射 Snort 2 和 Snort 3 入侵规则，映射由系统提供。但是，您可能无法在 Snort 2 和 Snort 3 中找到所有入侵规则的一对一映射。如果更改 Snort 2 中的一条规则的规则操作，则在切换到 Snort 3 的情况下，不会保留 Snort 2 与 Snort 3 的同步。有关同步的详细信息，请参阅 将 Snort 2 规则与 Snort 3 同步 ，第 6 页。

网络分析和入侵策略的必备条件

要允许 Snort 检测引擎处理流量以进行入侵和恶意软件分析，必须为 防火墙威胁防御 设备启用 IPS 许可证。

您必须是管理员用户，才能管理网络分析、入侵策略和执行迁移任务。

如何从 Snort 2 迁移到 Snort 3

从 Snort 2 迁移到 Snort 3 需要将 防火墙威胁防御 设备的检测引擎从 Snort 2 切换到 Snort 3。

根据您的要求，下表列出了完成设备从 Snort 2 迁移到 Snort 3 的任务：

步骤	任务	程序链接
1	启用 Snort 3	• 在单个设备上启用 Snort 3，第 3 页 • 在多台设备上启用 Snort 3，第 3 页
2	将 Snort 2 自定义规则转换为 Snort 3	• 将所有入侵策略中的所有 Snort 2 自定义规则转换为 Snort 3，第 4 页 • 将单个入侵策略的 Snort 2 自定义规则转换为 Snort 3，第 5 页
3	将 Snort 2 规则与 Snort 3 同步	将 Snort 2 规则与 Snort 3 同步 ，第 6 页

从 Snort 2 迁移到 Snort 3 的必备条件

以下是在将设备从 Snort 2 迁移到 Snort 3 之前必须考虑的建议前提条件。

- 具备 Snort 的应用知识。要了解有关 Snort 3 架构的信息，请参阅 Snort 3 采用。
- 备份您的管理中心。请参阅 备份管理中心。
- 备份您的入侵策略。请参阅 导出配置。
- 克隆入侵策略。为此，您可以使用现有策略作为基本策略来创建入侵策略的副本。在**入侵策略**页面中，点击**创建策略**，然后从**基本策略**下拉列表中选择现有入侵策略。

在单个设备上启用 Snort 3

重要事项 在部署过程中，由于需要关闭当前检测引擎，因此会出现短暂的流量丢失。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 点击设备以转到设备主页。

注释
设备被标记为 Snort 2 或 Snort 3，显示设备上的当前版本。

步骤 3 点击**设备 (Device)** 选项卡。

步骤 4 在“检测引擎”(Inspection Engine) 部分中，点击**升级 (Upgrade)**。

注释
如果要禁用 Snort 3，请点击“检测引擎”部分中的 **恢复为 Snort 2** 。

步骤 5 点击**是**。

下一步做什么

在设备上部署更改。请参阅部署配置更改，第 7 页。

系统会在部署过程中转换您的策略配置，使其与所选的 Snort 版本兼容。

在多台设备上启用 Snort 3

要在多台设备上启用 Snort 3，请确保所有所需 防火墙威胁防御 设备的版本均为 7.0 或更高版本。

重要事项 在部署过程中，由于需要关闭当前检测引擎，因此会出现短暂的流量丢失。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 选择要启用或禁用 Snort 3 的所有设备。

注释

设备被标记为 Snort 2 或 Snort 3，显示设备上的当前版本。

步骤 3 点击**选择批量操作**下拉列表，然后选择**升级到 Snort 3**。

步骤 4 点击**是**。

下一步做什么

在设备上部署更改。请参阅部署配置更改，第 7 页。

系统会在部署过程中转换您的策略配置，使其与所选的 Snort 版本兼容。

将 Snort 2 自定义规则转换为 Snort 3

如果您使用的是来自第三方供应商的规则集，请联系该供应商以确认其规则将成功转换为 Snort 3 或获取为 Snort 3 编写的本地规则集。如果您有自己编写的自定义规则，请在转换之前熟悉如何编写 Snort 3 规则，以便在转换后更新规则以优化 Snort 3 检测。请参阅下面的链接，了解有关在 Snort 3 中编写规则的更多信息。

- https://blog.snort.org/2020/08/how-rules-are-improving-in-snort-3.html
- https://blog.snort.org/2020/10/talos-transition-to-snort-3.html

您可以参阅 https://blog.snort.org/ 上的其他博客，了解有关 Snort 3 规则的更多信息。

要使用系统提供的工具将 Snort 2 规则转换为 Snort 3 规则，请参阅以下程序。

- 将所有入侵策略中的所有 Snort 2 自定义规则转换为 Snort 3，第 4 页
- 将单个入侵策略的 Snort 2 自定义规则转换为 Snort 3，第 5 页

重要事项 Snort 2 网络分析策略 (NAP) 设置 无法 自动复制到 Snort3。必须在 Snort 3 中手动复制 NAP 设置。

将所有入侵策略中的所有 Snort 2 自定义规则转换为 Snort 3

过程

步骤 1 选择**对象** > **入侵规则**。

步骤 2 点击 **Snort 3 所有规则** 选项卡。

步骤 3 确保在左侧窗格中选择 **更新** 。

步骤 4 点击 **任务** 下拉列表，然后选择：

- **转换 Snort 2 规则和导入** - 将所有入侵策略中的所有 Snort 2 自定义规则自动转换为 Snort 3，并将其作为 Snort 3 自定义规则导入 防火墙管理中心 。

- **转换 Snort 2 规则并夏泽** - 将所有入侵策略中的所有 Snort 2 自定义规则自动转换为 Snort 3，并将其下载到本地系统。

步骤 5 点击**确定**。

注释

- 如果在上一步中选择了 **转换并导入**，则所有转换后的规则都将保存在 **本地规则**下新创建的规则组 **所有 Snort 2 转换后的全局** 下。
- 如果在上一步中选择了 **转换并下载**，则在本地保存规则文件。您可以在下载的文件中查看转换后的规则，然后按照 将自定义规则添加到规则组中的步骤进行上传。

有关其他支持和信息，请参阅视频 将 Snort 2 规则转换为 Snort 3 。

下一步做什么

部署配置更改；请参阅部署配置更改，第 7 页。

将单个入侵策略的 Snort 2 自定义规则转换为 Snort 3

过程

步骤 1 选择**策略** > **访问控制标题** > **入侵**。

步骤 2 在 **入侵策略** 选项卡中，点击 **显示 Snort 3 同步状态**。

步骤 3 点击入侵策略的**同步**图标 **Snort 不同步**（ ）。

注释

如果入侵策略的 Snort 2 和 Snort 3 版本已同步，则**同步**图标为绿色**Snort 同步**（）。它表示没有要转换的自定义规则。

步骤 4 仔细阅读摘要，然后点击 **自定义规则** 选项卡。

步骤 5 选择:

- **将转换后的规则导入到此策略**-将入侵策略中的 Snort 2 自定义规则转换为 Snort 3，并将其作为 Snort 3 自定义规则导入 防火墙管理中心 。
- **下载转换后的规则**-将入侵策略中的 Snort 2 自定义规则转换为 Snort 3，并将其下载到本地系统中。您可以在下载的文件中查看转换后的规则，然后通过点击上传图标上传文件。

步骤 6 点击 **重新同步**。

下一步做什么

部署配置更改；请参阅部署配置更改，第 7 页。

查看 Snort 2 和 Snort 3 基本策略映射

过程

步骤 1 选择**策略** > **访问控制标题** > **入侵**。

步骤 2 确保选择**入侵策略**选项卡。

步骤 3 点击 **IPS 映射**。

步骤 4 在 **IPS 策略映射** 对话框中，点击 **查看映射** 以查看 Snort 3 到 Snort 2 的入侵策略映射。

步骤 5 点击**确定 (OK)**。

将 Snort 2 规则与 Snort 3 同步

为确保 Snort 2 版本设置和自定义规则保留并转移到 Snort 3， 防火墙管理中心 提供了同步功能。同步可帮助 Snort 2 规则覆盖设置和自定义规则，这些设置和自定义规则可能是您在过去几个月或几年内更改和添加的，以便在 Snort 3 版本上进行复制。此实用程序帮助将 Snort 2 版本策略配置与 Snort 3 版本同步，以便从相似的覆盖范围开始。

如果 防火墙管理中心 从 6.0 之前的版本升级到 7.0 或更高版本，系统会同步配置。如果 防火墙管理中心 是新的 7.0 版本或更高版本，您可以升级到更高版本，并且系统在升级过程中不会同步任何内容。

在将设备升级到 Snort 3 之前，如果在 Snort 2 版本中进行了更改，可以使用此实用程序将最新 Snort 2 版本同步到 Snort 3 版本，以便从相似的覆盖范围开始。

注释 迁移到 Snort 3 后，建议单独管理 Snort 3 版本的策略，且不要将此实用程序用作常规操作。

重要事项

- 只有 Snort 2 规则覆盖和自定义规则会复制到 Snort 3，而不会反过来。您可能无法在 Snort 2 和 Snort 3 中找到所有入侵规则的一对一映射。当您执行以下程序时，您对两个版本中存在的规则的规则操作更改会同步。
- 同步 不会 将任何自定义或系统提供的规则的阈值和抑制设置从 Snort 2 迁移到 Snort 3。

过程

步骤 1 选择**策略** > **访问控制标题** > **入侵**。

步骤 2 确保选择**入侵策略**选项卡。

步骤 3 点击 **显示 Snort 3 同步状态**。

步骤 4 确定不同步的入侵策略。

步骤 5 点击 “**同步**” **(Sync)** 图标 **Snort 不同步**（ ）。

注释
如果入侵策略的 Snort 2 和 Snort 3 版本已同步，则**同步**图标为绿色**Snort 同步**（ ）。

步骤 6 仔细阅读摘要，并根据需要下载摘要副本。

步骤 7 点击 **重新同步**。

注释
- 仅当在设备上应用并成功部署后，同步设置才适用于 Snort 3 入侵引擎。
- 可以使用系统提供的工具将 Snort 2 自定义规则转换为 Snort 3。如果您有任何 Snort 2 自定义规则，请点击自定义规则选项卡，然后按照屏幕上的说明转换规则。有关详细信息，请参阅将单个入侵策略的 Snort 2 自定义规则转换为 Snort 3，第 5 页。

下一步做什么

部署配置更改；请参阅部署配置更改，第 7 页。

部署配置更改

更改配置后，将其部署到受影响的设备。

注释 本主题介绍部署配置更改的基本步骤。我们强烈建议您在继续执行这些步骤之前，参考最新版本的 *Cisco Secure Firewall Management Center* 指南 中的 部署配置更改 主题，了解部署更改的前提条件和影响。

注意 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，部署某些配置会重新启动 Snort 进程，这会中断流量检测。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。

过程

步骤 1 在 Cisco Secure Firewall Management Center 菜单栏中，点击 **部署** ，然后选择 **部署**。

GUI 页面列出了具有 **待处理** 状态的过期配置的设备。

- **修改者**列列出了修改策略或对象的用户。展开设备列表以参照每个策略列表查看修改了策略的用户。

  注释
  没有为已删除的策略和对象提供用户名。

- **检查中断** 列指示在部署过程中是否可能导致设备中的流量检查中断。

  如果设备的此为空白，则表明在部署过程中该设备上不会出现流量检查中断。

- **上次修改时间** 列指定上次更改配置的时间。
- **预览**列允许您预览下一次要部署的更改。
- **状态**列提供每个部署的状态。

步骤 2 识别并选择要部署配置更改的设备。

- 搜索 - 在搜索框中搜索设备名称、类型、域、组或状态。
- 展开 - 点击 **展开箭头**（ ） 以查看要部署的设备特定的配置更改。

  选中设备旁边的复选框时，系统会推送对设备进行的所有更改并在设备下列出这些更改以进行部署。但是，您可以使用 **策略选择**（ ） 选择部署个别或指定策略或配置，而保留其余的更改不予部署。

  注释
  - 当 **检查中断** 列中的状态指示（**是**）部署会中断 防火墙威胁防御 设备上的检查并可能中断流量时，展开的列表将用 **检查中断**（ ）指示导致中断的特定配置。
  - 当接口组、安全区或对象发生更改时，受影响的设备在 防火墙管理中心中显示为过期。为确保这些更改生效，包含这些接口组、安全区或对象的策略也需要随这些更改一起部署。受影响的策略在 防火墙管理中心的 **预览**页上显示为过期。

步骤 3 点击**部署 (Deploy)**。

步骤 4 如果系统在要部署的更改中发现错误或警告，则会在**验证消息**窗口中显示它们。要查看完整详细信息，请点击警告或错误前的箭头图标。

有以下选项可供选择：

- 部署 - 继续部署而无需解决警告情况。如果系统识别错误，则无法继续。

- 关闭 - 退出而不部署。解决错误和警告情况，并尝试重新部署该配置。

下一步做什么

在部署过程中，如果有部署失败，则可能会影响流量。不过，这取决于某些条件。如果部署中存在特定的配置更改，则部署失败可能导致流量中断。有关部署过程的详细信息，请参阅 *Cisco Secure Firewall Management Center* 配置指南中的部署配置更改主题。

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。