从 Snort 2 迁移到 Snort 3

从 Snort 2 迁移到 Snort 3 一章涵盖了从 Snort 2 迁移到 Snort 3 的各个方面。它还提供有关启用和禁用 Snort 3 以及将 Snort 2 规则与 Snort 3 同步的信息。

Snort 2 与 Snort 3

与 Snort 2 相比，Snort 3 在架构上进行了重新设计，以使用相同的资源检查更多流量。Snort 3 提供简化且灵活的流量解析器插入。Snort 3 还提供了新的规则语法，使规则编写更加容易，并且共享对象规则等效项可见。

下表列出了 Snort 2 和 Snort 3 版本在检测引擎功能方面的差异。

特性	Snort 2	Snort 3
数据包线程	每个进程一个	每个进程的任意数量
配置内存分配	进程数 * *x* GB	*x* GB 总计；更多内存可用于数据包
配置重新加载	较慢	更快；一个线程可以固定到单独的核心
规则语法	不一致，需要换行	具有任意空格的统一系统
规则注释	仅注释	#、#begin 和 #end 标记； C 语言风格

其他参考： Firepower 中 Snort 2 和 Snort 3 之间的差异。

管理中心管理的 威胁防御 的 Snort 3 的功能限制

下表列出了 管理中心管理的 威胁防御 设备的 Snort 2 支持但 Snort 3 不支持的功能。

表 *1: Snort 3* 的功能限制

策略/区域	不支持的功能
访问控制策略	以下应用设置： • 安全搜索 • YouTube EDU

威胁情报检测器	当 IPv4 或 IPv6 流量为：
	• 已阻止：
	  • 无 TID 事件
	  • 无 SI 事件
	• 受监控：
	  • 无 ITD 事件

入侵策略	• 策略层 • 全局规则阈值 • 日志记录配置： • SNMP • SRU 规则更新，因为 Snort 3 仅支持 LSP 规则更新
应用检测	在 Snort 3 中，默认情况下为所有网络启用应用检测。与 Snort 2 不同的是，您无法使用网络发现策略的网络过滤器控制仅对特定网络启用或禁用应用检测。有关详细信息，请参阅最新版本的 *Firepower* 管理中心配置指南中的 *Snort 2* 和 *Snort 3* 中的应用检测 主题。
网络发现/RNA	• 主机端口/服务标识（如网络映射所示） • 操作系统指纹（您无法根据网络映射调整入侵策略）

从 Snort 2 迁移到 Snort 3

策略/区域	不支持的功能
其他功能	使用 FQDN 名称进行事件日志记录

从 Snort 2 迁移到 Snort 3

从 Snort 2 迁移到 Snort 3 需要将 威胁防御 设备的检测引擎从 Snort 2 切换到 Snort 3。请注意，只有 7.0 及更高版本的设备支持 Snort 3。

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。要在受支持的设备上启用 Snort 3，请参阅启用和禁用 Snort 3 ， 第 3 页。

Snort 2 自定义规则的转换工具

如果您使用的是自定义规则，请确保在从 Snort 2 转换为 Snort 3 之前准备好管理 Snort 3 的规则集。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，请参阅将 Snort 2 自定义规则转换为 Snort 3。

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。

启用和禁用 Snort 3

Snort 3 是版本 7.0 及更高版本的新注册 威胁防御 设备的默认检测引擎。但是，对于较低版本的 威胁防御 设备，Snort 2 是默认检测引擎。将受管 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 威胁防御的使用 Snort 3，必须明确启用它。请注意，您可以随时从 Snort 3 切换回 Snort 2。

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 5 页。

在单个设备上启用和禁用 Snort 3

开始之前

可以执行这些步骤的受支持用户角色包括：

- 管理
- 入侵管理员

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 单击**设备 (Device)** 选项卡。

步骤 4 在检测引擎部分，点击 **升级**。

注释 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 **Yes**。

下一步做什么

在设备上部署更改。请参阅部署配置更改。

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。

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。

在多台设备上启用和禁用 Snort 3

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

开始之前

可以执行这些步骤的受支持用户角色包括：

- 管理
- 入侵管理员

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 **选择操作** 下拉列表。

步骤 4 点击 **升级到 Snort 3**。

注释 要禁用 Snort 3，请点击 **降级到 Snort 2**。

步骤 5 点击 **Yes**。

下一步做什么

在设备上部署更改。请参阅部署配置更改。

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。

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。

查看 Snort 2 和 Snort 3 基本策略映射

步骤 1 依次选择**策略** > **入侵**。

步骤 2 确保选择 **入侵策略** 选项卡。

步骤 3 点击 **IPS 映射**。

将 Snort 2 规则与 Snort 3 同步

此实用程序用于将 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 管理中心 从 7.0 之前的版本升级到 7.0 或更高版本，系统会同步配置。如果 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。

为确保 Snort 2 版本设置和自定义规则保留并转移到 Snort 3， 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。

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。

步骤 1 依次选择**策略** > **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** 图标（）。

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 ()。

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。

下一步做什么

部署配置更改；请参阅部署配置更改。