

使用规则调整入侵策略

本章提供有关Snort 3中的自定义规则、入侵规则操作、入侵策略中的入侵事件通知过滤器、将Snort 2自定义规则转换为Snort 3以及将具有自定义规则的规则组添加到入侵策略的信息。

- 调整入侵规则概述， 第 1 页
- 入侵规则类型， 第 2 页
- 网络分析和入侵策略的必备条件， 第 3 页
- Snort 3 中的自定义规则， 第 3 页
- 查看入侵策略中的 Snort 3 入侵规则， 第 6 页
- 入侵规则操作， 第 7 页
- 入侵策略中的入侵事件通知过滤器， 第 8 页
- 添加入侵规则注释， 第 13 页
- 将 Snort 2 自定义规则转换为 Snort 3， 第 13 页
- 将自定义规则添加到规则组， 第 15 页
- 将具有自定义规则的规则组添加到入侵策略， 第 16 页
- 管理 Snort 3 中的自定义规则， 第 17 页
- 删除自定义规则， 第 18 页
- 删除规则组， 第 18 页

调整入侵规则概述

您可以为共享对象规则、标准文本规则和检查器规则配置规则状态和其他设置。

通过将规则状态设置为“警报”或“阻止”来启用规则。启用规则后，系统将对与该规则匹配的流量生成事件。禁用规则将停止该规则的处理。您还可以设置入侵策略，以便在内联部署中设置为阻止的规则在匹配流量时生成事件并丢弃该匹配流量。

您可以对规则进行过滤来显示规则的一个子集，这样就能选择要更改其规则状态或规则设置的确切规则集。

当入侵规则或规则参数要求禁用的检查器时，系统会自动使用其当前设置，即使其在网络分析策略网络界面中保持禁用状态。

注释 建议您不要修改共享对象规则，而建议仅为威胁防御设备启用或禁用这些规则。要创建自定义 Snort 规则，请联系思科支持部门。

入侵规则类型

入侵规则是系统用于检测利用网络漏洞企图的一组指定关键字和参数。当系统分析网络流量时，它将数据包与每个规则中指定的条件相比较，并在数据包满足规则中指定的所有条件的情况下触发规则。

入侵策略包含：

- 入侵规则，可细分为共享对象规则和标准文本规则
- 检查器规则，与数据包解码器的检测选项或与系统随附的检查器相关联

下表总结了这些规则类型的属性：

表 *1:* 入侵规则类型

类型	生成器 ID (GID)	Snort ID (SID)	来源	可以复制？	可以编辑？
共享对象规则	3	低于 1000000	思科 Talos 智能小组 (Talos)	是	有限
标准文本规则	1（全局域或旧式 GID）	低于 1000000	Talos 协作	是	有限
	1000 - 2000（后代域）	1000000 或更高	由用户创建或导入	是	是
预处理器规则	特定于解码器或预处理器	低于 1000000	Talos 协作	否	否
		1000000 或更高	由系统在选项配置期间生成	否	否

无法保存对 Talos 创建的任何规则所做的更改，但是可以将已修改的规则的副本另存为自定义规则。可以修改在规则或规则报头信息中使用的变量（例如源和目标端口及 IP 地址）。在多域部署中，Talos 所创建的规则属于全局域。后代域中的管理员可以保存随后可编辑的规则的本地副本。

对于所创建的规则，Talos 在每个默认入侵策略中分配默认规则状态。大多数预处理器规则在默认情况下已禁用，如果希望系统为预处理器规则生成事件并在内联部署中丢弃违规的数据包，则必须启用这些规则。

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。

Snort 3 中的自定义规则

您可以通过以下方式创建自定义入侵规则。规则文件可以具有 `.txt` 或 `.rules` 扩展名。无论您使用哪种创建方法，系统都会将自定义规则保存在本地规则类别中。自定义规则必须属于规则组。但是，自定义规则也可以是两个或多个组的一部分。

当您创建自定义入侵规则时，系统会为它分配唯一的规则编号（其格式为 `GID:SID:Rev`）。此编号的元素如下：

- **GID**—生成器 ID。对于自定义规则，无需指定 GID。上传规则时，系统会根据您是在全局域还是子域中自动生成 GID。对于所有标准文本规则，此值为 2000。
- **SID**—Snort ID。指示规则是否为系统规则的本地规则。创建新规则时，请为该规则分配唯一的 SID。

  本地规则的 Snort ID 号从 1000000 开始，且每个本地新规则的 SID 号以 1 递增。
- **Rev**—修订号。对于新规则，修订号为 1。每修改一次自定义规则，修订号就增加一。

在自定义标准文本规则中，可以设置规则报头设置、规则关键字和规则参数。您可以通过规则报头设置将规则设置为仅匹配使用特定协议以及发往或来自特定 IP 地址或端口的流量。

要检查 SID 是已启用还是已禁用，请验证 snort.lua 文件中的条目，该文件位于 `./file-contents/ngfw/var/sf/detection_engines/<id>/ips/<id>` 目录。

- 如果 SID 默认为禁用，则 文件中将不会有任何条目。
- 如果手动启用 SID，您将看到包含 **enable:yes** 的条目。
- 如果 SID 在手动启用后被禁用，该条目将保留在文件中，并将显示 **enable:no**。

注释

- 无法编辑 Snort 3 自定义规则。确保自定义规则在规则文本中具有 `classtype` 的有效分类消息。如果导入没有分类或错误分类的规则，请删除并重新创建该规则。
- 您可以使用 Snort 3 来创建自定义入侵规则。但是，目前不支持对这些规则进行调整和故障排除。
- Snort 规则中的 *classtype* 为规则分配分类，指示与事件关联的攻击类型。每个 *classtype* 还关联了一个 1-4 优先级。但是，威胁防御设备上某些类 类型 的优先级与 Snort 文档 中提到的开源 Snort 类类型优先级不匹配。例如， *tcp-connection* 在开源 Snort 中的优先级为 4，而在威胁防御设备上为其分配的优先级为 3。

Snort 3 中的敏感数据检测

社会保险号、信用卡号、电子邮件等敏感数据可能会被有意或无意地在互联网上泄露。敏感数据检测用于检测可能的敏感数据泄漏并生成事件。仅当传输大量个人身份信息 (PII) 数据时，才会生成事件。敏感数据检测可以屏蔽事件输出中的 PII。

sd_pattern 选项

使用 `sd_pattern` IPS 选项检测和过滤 PII。这些信息包括信用卡号、美国社会保险号、电话号码和电子邮件地址。正则表达式 (regex) 语法可用于定义您自己的 PII。

sd_pattern 选项具有以下设置：

- 模式 - 指定要在 PDU 中查找的正则表达式的隐式必需设置。正则表达式必须使用 PCRE 语法编写。
- 阈值 - 明确的可选设置，指定生成事件所需的 PDU 中的匹配数。

`sd_pattern` as IPS 规则选项在 Snort 中可用，对其他检查器没有要求。规则选项的语法为：

```
sd_pattern: "<pattern> "[, threshold<count> ];
```

例如：

```
sd_pattern:"credit_card", threshold 2;
```

内置模式

敏感数据有五种内置模式。要在"模式"设置中使用内置模式，必须指定需要匹配的 PII 类型的名称，并将其替换为必要的正则表达式。PII 名称和正则表达式映射或模式如下所述：

- credit_card—

```
\d{4}\D?\d{4}\D?\d{2}\D?\d{2}\D?\d{3,4}
```

- us_social—

```
[0-8]\d{2}-\d{2}-\d{4}
```

- us_social_nodashes—

```
[0-8]\d{8}
```

- Email—

```
[a-zA-Z0-9!#$%&'*+\/=?^_`{|}~-]+(?:\.[a-zA-Z0-9!#$%&'*+\/=?^_`{|}~-]+)*@(?:[a-zA-Z0-9]
(?:[a-zA-Z0-9-]*[a-zA-Z0-9])?\.)+[a-zA-Z0-9](?:[a-zA-Z0-9-]*[a-zA-Z0-9])?
```

- us_phone—

```
(?:\+?1[-\.\s]?)?\(?([2-9][0-8]\d)\)?[-\.\s]([2-9]\d{2})[-\.\s](\d{4})
```

PII Name	模式
credit_card	`\d{4}\D?\d{4}\D?\d{2}\D?\d{2}\D?\d{3,4}`
us_social	`[0-8]\d{2}-\d{2}-\d{4}`
us_social_nodashes	`[0-8]\d{8}`
邮件	`[a-zA-Z0-9!#$%&'*+\/=?^_`{\|}~-]+(?:\.[a-zA-Z0-9!#$%&'*+\/=?^_`{|}~-]+)*@(?:[a-zA-Z0-9](?:[a-zA-Z0-9-]*[a-zA-Z0-9])?\.)+[a-zA-Z0-9](?:[a-zA-Z0-9-]*[a-zA-Z0-9])?`
us_phone	`(?:\+?1[-\.\s]?)?\(?([2-9][0-8]\d)\)?[-\.\s]([2-9]\d{2})[-\.\s](\d{4})`

与这些模式匹配的数据的掩码仅适用于信用卡、美国社会保险号、邮箱和美国电话号码的系统提供的规则或内置模式。屏蔽不适用于自定义规则或用户定义的PII模式。敏感数据的轻量级安全包(LSP)中提供了规则，gid:13。默认情况下，它们在任何系统提供的策略中均未启用。

LSP 中的敏感数据规则涵盖所有内置模式，并具有以下阈值：

- credit_card: 2
- us_social: 2
- us_social_nodashes: 20
- email: 20
- us_phone: 20

您可以使用 sd_pattern 选项创建自定义规则并修改现有规则。要执行此操作，请使用 Snort 3 入侵策略接口。

具有自定义模式和阈值的 sd_pattern 规则示例：

*alert tcp (sid: 1000000001; sd_pattern:"[\w-\.]+@([\w-]+\.)+[\w-]{2,4}",threshold 4; msg: "email,*阈值 *4")*

示例

使用敏感数据检测的自定义规则示例：

具有内置模式的规则：

```
alert tcp (
        msg:"SENSITIVE-DATA Email";
        flow:only_stream;
        pkt_data;
        sd_pattern:"email", threshold 5;
```

```
        service:http, smtp, ftp-data, imap, pop3;
        gid:2000;
        sid:1000001;
)
```

具有自定义模式的规则

```
alert tcp (
        msg:"SENSITIVE-DATA US phone numbers";
        flow:only_stream;
        file_data;
        sd_pattern:"+?3?8?(0[\s\.-]\d{2}[\s\.-]\d{3}[\s\.-]\d{2}[\s\.-]\d{2})", threshold
2;
        service:http, smtp, ftp-data, imap, pop3;
        gid:2000;
        sid:1000002;
)
```

以下是具有内置敏感数据模式的完整 Snort IPS 规则的更多示例：

- alert tcp (sid:1; msg:"Credit Card"; sd_pattern:"credit_card", threshold 2;)
- alert tcp (sid:2; msg:"US Social Number"; sd_pattern:"us_social", threshold 2;)
- alert tcp (sid:3; msg:"US Social Number No Dashes"; sd_pattern:"us_social_nodashes", threshold 2;)
- alert tcp (sid:4; msg:"US Phone Number"; sd_pattern:"us_phone", threshold 2;)
- alert tcp (sid:5; msg:"Email"; sd_pattern:"email", threshold 2;)

Cisco Secure Firewall Management Center 和安全防火墙设备管理器不支持禁用数据屏蔽。

有关如何向规则组添加自定义规则的信息，请参阅将自定义规则添加到规则组 ， 第 15 页。

查看入侵策略中的 Snort 3 入侵规则

您可以调整规则在入侵策略中的显示方式。也可以显示特定规则的详细信息，以便查看规则设置、规则文档和其他规则详细信息。

过程

步骤 1 选择**策略** > **访问控制标题** > **入侵**。

步骤 2 点击策略旁边的 **Snort 3 版本**。

步骤 3 查看规则时，您可以执行以下操作：

- 过滤器规则。
- 选择规则组以查看与该组相关的规则。
- 查看入侵规则的详细信息。
- 查看规则备注。
- 查看规则文档。

有关执行这些任务的详细信息，请参阅 编辑 Snort 3 入侵策略 。

入侵规则操作

通过入侵规则操作，您可在个别入侵策略中启用或禁用规则，以及指定受监控条件触发该规则时系统采取的操作。

Cisco Talos 智能组 (Talos) 设置每个默认策略中每个入侵和检查器规则的默认操作。例如，一条规则可能会在 Security over Connectivity 默认策略中启用而在 Connectivity over Security 默认策略中禁用。Talos 有时会使用规则更新来更改默认策略中一条或多条规则的默认策略。如果允许规则更新对基本策略进行更新，则意味着当用于创建策略的默认策略中的默认操作发生更改时，也允许规则更新更改策略中的规则默认操作。但请注意，如果您已经更改了规则操作，规则更新不会覆盖您的更改。

创建入侵规则时，它会继承用于创建策略的默认策略中相应规则的默认操作。

入侵规则操作选项

在入侵策略中，可以将规则的状态设置为以下值：

警报

您希望系统检测特定入侵企图，并在其发现匹配流量时生成入侵事件。当恶意数据包通过网络并触发该规则时，数据包被发送到其目标，系统生成入侵事件。该恶意数据包到达其目标，但是您通过事件日志记录收到通知。

阻止

您希望系统检测特定入侵企图，丢弃包含攻击的数据包，并在其发现匹配流量时生成入侵事件。该恶意数据包永远不会到达其目标，并且您通过事件日志记录收到通知。

禁用

您不希望系统评估匹配流量。



注释 选择 **警报** 或 **阻止** 选项可启用规则。选择**禁用 (Disable)** 会禁用规则。

我们 **强烈** 建议您 **不要** 启用入侵策略中的所有入侵规则。如果启用所有规则，则您的托管设备的性能可能会下降。相反，应调整规则集，使之与网络环境尽可能匹配。

设置入侵规则操作

入侵规则操作为策略特定的。

过程

步骤 1 选择**策略** > **访问控制标题** > **入侵**。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

提示
此页面显示以下总数：

- 已禁用的规则
- 已启用的规则设置为警报
- 已启用的规则设置为阻止
- 已覆盖的规则

步骤 3 选择要在其中设置规则操作的一条或多条规则。

步骤 4 从 **规则操作** 下拉框中选择规则操作之一：有关不同规则操作的详细信息，请参阅 编辑 Snort 3 入侵策略 。

步骤 5 点击**保存 (Save)**。

下一步做什么

部署配置更改；请参阅部署配置更改。

入侵策略中的入侵事件通知过滤器

入侵事件的重要性可根据发生频率或者源或目标 IP 地址而定。在某些情况下，直至事件发生一定次数后您可能才会在意。例如，如果有人企图登录服务器，在其失败达到一定次数之前，您可能不会担心。但在其他情况下，也许只需要发生几次，就能让您知道存在普遍性问题。例如，如果有人对网络服务器发动 DoS 攻击，可能只需要发生区区数次入侵事件，您就会明白需要解决这种情况。发生数百次相同事件只会让系统不堪重负。

入侵事件阈值

您可以为各条规则设置阈值，根据事件在指定时间段内生成的次数来限制系统记录和显示入侵事件的次数。这可以防止因相同事件数量过多而使系统不堪重负。您可以根据共享对象规则、标准文本规则或检查器规则设置阈值。

设置入侵事件阈值

要设置阈值，请先指定阈值类型。

表 *2:* 阈值选项

选项	说明
限制	为指定时间段内触发规则的指定数量的数据包（由“计数”[Count] 参数指定）记录并显示事件。例如，如果将类型设置为**限制 (Limit)**，将**计数 (Count)** 设置为 `10`，并将**秒数 (Seconds)** 设置为 `60`，而同一分钟内有 14 个数据包触发规则，则系统在显示发生的前 10 个违反该规则的事件后将停止记录违反该规则的事件。
阈值	在指定时间段内，当指定数量的数据包（由“计数”[Count] 参数指定）触发规则时，记录并显示一个事件。请注意，达到事件阈值计数且系统记录该事件之后，时间计数器将重新开始计数。例如，将类型设置为**阈值 (Threshold)**，将**计数 (Count)** 设置为 `10`，并将**秒数 (Seconds)** 设置为 `60` 时，如果到 33 秒时规则触发 10 次，系统将生成一个事件，然后将“秒数”(Seconds) 和“计数”(Count) 计数器重置为 0。其后，该规则在接下来 25 秒内又触发 10 次。由于计数器在第 33 秒时已重置为 0，因此，系统此时会记录另一个事件。
双向	每个指定时间段在指定数量（计数）的数据包触发规则后记录并显示一次事件。例如，如果将类型设置为**两者 (Both)**，将**计数 (Count)** 设置为 2，并将**秒数 (Seconds)** 设置为 `10`，则事件计数结果如下： • 如果 10 秒内触发规则一次，系统不会生成任何事件（未达到阈值） • 如果 10 秒内触发规则两次，系统将生成一个事件（第二次触发规则时达到阈值） • 如果 10 秒内触发规则四次，系统将生成一个事件（第二次触发规则时达到阈值，忽略其后的事件）

其次，指定跟踪，从而确定事件阈值是按源 IP 地址计算还是按目标 IP 地址计算。

表 *3:* 阈值 *IP* 选项

选项	说明
来源	按源 IP 地址计算事件实例计数。
目标	按目标 IP 地址计算事件实例计数。

最后，指定用于定义阈值的实例数和时间段。

表 *4:* 阈值实例/时间选项

选项	说明
计数	每个跟踪 IP 地址在每个指定时间段内达到阈值所需的事件实例数量。

选项	说明
秒	计数重置之前经过的秒数。如果将阈值类型设置为**限制 (limit)**，将跟踪设置为**源 IP (Source IP)**，将**计数 (count)** 设置为 `10`，并将**秒数 (seconds)** 设置为 `10`，则系统将记录并显示 10 秒钟内发生的来自指定源端口的前 10 个事件。如果前 10 秒内只发生了 7 个事件，系统将记录并显示这些事件，而如果前 10 秒内发生了 40 个事件，系统将记录并显示 10 个事件，然后在为期 10 秒的时间段过后重新开始计数。

请注意，入侵事件阈值可单独使用，也可与基于速率的攻击防御、`detection_filter` 关键字和入侵事件抑制的任意组合配合使用。

提示 也可以在入侵事件的数据包视图中添加阈值。

在 Snort 3 中为入侵规则设置阈值

您可以在“规则详细信息”(Rule Detail) 页面中为规则设置一个阈值。添加阈值将覆盖该规则的任何现有阈值。您为入侵规则设置的阈值将应用于每个数据包线程。但是，该配置仅在唯一流的上下文中完全应用。不同的网络流上可能有更多警报，但警报数不会少于配置的数量。

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 从入侵规则的警报配置列中，点击 **无** 链接。

步骤 4 请点击 **编辑** (✎)。

步骤 5 在警报配置窗口中，点击 **阈值** 选项卡。

步骤 6 从**类型 (Type)** 下拉列表中，选择要设置的阈值的类型：

- 选择**限制 (Limit)** 以将通知限于每个时间段的指定数量的事件实例。
- 选择**阈值 (Threshold)** 以在每个时间段内每次事件实例数达到指定数量时提供通知
- 选择**两者 (Both)** 以在每个时间段内事件实例数达到指定数量后提供一次通知。

步骤 7 从 **跟踪方式** 下拉列表中，选择 **源**或 **目标** 以指示希望按源 IP 地址还是目标 IP 地址跟踪事件实例。

步骤 8 在 **计数** 字段中，输入要用作阈值的事件实例数。

步骤 9 在 **秒** 字段中，输入用于指定跟踪事件实例的时间段的数字（以秒为单位）。

步骤 10 点击**保存**。

有关其他支持和信息，请参阅视频 Snort 3 抑制和阈值 。

下一步做什么

部署配置更改；请参阅部署配置更改。

查看和删除入侵事件阈值

要查看或删除存在的规则的阈值设置，使用“规则详细信息”视图显示为阈值配置的设置，看其是否适合系统。如果不适合，可以添加新的阈值来覆盖现有值。

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 选择具有已配置阈值的规则，如 **警报配置** 列中所示（ **警报配置** 列将 **阈值** 显示为该规则的链接）。

步骤 4 要删除规则的阈值，请点击 **警报配置** 列中的 **阈值** 链接。

步骤 5 请点击 **编辑** ()。

步骤 6 点击 **阈值** 选项卡。

步骤 7 点击**重置**。

步骤 8 点击**保存 (Save)**。

下一步做什么

部署配置更改；请参阅部署配置更改。

入侵策略抑制配置

您可以在特定 IP 地址或 IP 地址范围触发特定规则或检查器时抑制入侵事件通知。这对杜绝误报十分有用。例如，如果邮件服务器传输的数据包看起来像某种特定的漏洞，则可能会在邮件服务器触发该事件时抑制对其发出的事件通知。所有数据包都会触发该规则，但您只会看到真正的攻击事件。

入侵策略抑制类型

请注意，入侵事件抑制可单独使用，也可与基于速率的攻击防御、`detection_filter` 关键字和入侵事件阈值的任意组合配合使用。

提示 可以在入侵事件的数据包视图中添加抑制。您还可以使用入侵规则编辑器页面上的 **警报配置** 列（ **对象** > **入侵规则**，点击**对象** 入侵规则Snort 3 所有规则）访问抑制设置。

在 Snort 3 中为入侵规则设置抑制

可以为入侵策略中的规则设置一个或多个抑制。

开始之前

确保创建要添加用于源或目标抑制的所需网络对象。

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 点击入侵规则的警报配置列中的 **无** 链接。

步骤 4 请点击 **编辑** (✎)。

步骤 5 在**抑制 (Suppressions)** 选项卡中，点击以下任何选项旁边的添加图标 **添加** (+)：

- 选择 **源** 将抑制由指定源 IP 地址发出的数据包生成的事件。
- 选择 **目标网络** 将抑制由发往指定目标 IP 地址的数据包生成的事件。

步骤 6 在 **网络** 下拉列表中选择任何预设网络。

步骤 7 点击**保存**。

步骤 8 （可选）如果需要，请重复最后三个步骤。

步骤 9 点击警报配置窗口中的 **保存** 。

下一步做什么

部署配置更改；请参阅部署配置更改。

查看和删除抑制条件

您可能需要查看或删除现有抑制条件。例如，由于某个邮件服务器通常会传输看起来像漏洞的数据包，因此可以抑制由该邮件服务器 IP 地址发出的数据包的事件通知。如果以后停用该邮件服务器并将此 IP 地址重新分配给其他主机，应删除对该源 IP 地址的抑制条件。

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 选择要查看或删除其抑制的规则。

步骤 4 点击 **警报配置** 列中的 **抑制** 。

步骤 5 请点击 **编辑** (✎)。

步骤 6 点击 **抑制** 选项卡。

步骤 7 点击抑制旁边的 **清除** (✕) 以删除抑制。

步骤 8 点击**保存 (Save)**。

下一步做什么

部署配置更改；请参阅部署配置更改。

添加入侵规则注释

可以向入侵策略中的规则添加注释。按这种方式添加的注释是策略特定的；即添加到一个入侵策略的规则中的注释在其他入侵策略中不可见。

过程

步骤 1 选择**策略** > **访问控制标题** > **入侵**。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

步骤 3 在列出所有规则的页面右侧，选择要添加注释的规则。

步骤 4 点击 **注释** 列下方的 **注释**（）。

步骤 5 在 **注释** 字段中，输入规则注释。

步骤 6 点击**添加注释 (Add Comment)**。

步骤 7 点击**保存**。

提示

系统将并在“注释”(Comments) 列中的规则旁显示 **注释**（）。

下一步做什么

部署配置更改；请参阅部署配置更改。

将 Snort 2 自定义规则转换为 Snort 3

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。

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 ， 第 15 页中的步骤进行上传。

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。

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。

将自定义规则添加到规则组

在 防火墙管理中心 中上传自定义规则会将您在本地创建的自定义规则添加到所有 Snort 3 规则的列表中。

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 点击 **任务** 下拉列表。

步骤 4 点击 **上传 Snort 3 规则**。

步骤 5 拖放包含已创建的 Snort 3 自定义规则的 `.txt` 或 `.rules` 文件。

步骤 6 点击**确定 (OK)**。

注释
如果所选文件中有任何错误，则无法继续。修复错误后，您可以下载错误文件和**替换文件**链接，以上传文件的第 2 版。

步骤 7 将规则关联到规则组以将新规则添加到该组。

您还可以创建新的自定义规则组（通过点击 **创建新的自定义规则组** 链接），然后将规则添加到新组。

注释
如果没有现有的本地规则组，请点击 **创建新的自定义规则组以继续**。为该搜索输入一个 **名称**，然后点击 **保存**。

步骤 8 选择以下其中一个选项：

- **合并规则** 以合并您要添加的新规则与规则组中的现有规则。
- **将组中的所有规则替换为文件内容** 以将所有现有规则替换为您添加的新规则。

注释
如果在上一步中选择了多个规则组，则只有 **合并规则** 选项可用。

步骤 9 点击**下一步 (Next)**。

查看摘要以了解正在添加的新规则 ID，并可选择下载。

步骤 10 点击**完成 (Finish)**。

重要事项 所有已上传规则的规则操作均处于禁用状态。您必须将其更改为所需的状态，以确保规则处于活动状态。

下一步做什么

- 在 防火墙管理中心 中上传自定义规则会将您创建的自定义规则添加到所有 Snort 3 规则的列表中。要对流量实施这些自定义规则，请在所需的入侵策略中添加并启用这些规则。有关将具有自定义规则的规则组添加到入侵策略的信息，请参阅 将具有自定义规则的规则组添加到入侵策略，第 16 页。有关启用自定义规则的详细信息，请参阅 管理 Snort 3 中的自定义规则，第 17 页。
- 部署配置更改；请参阅部署配置更改。

将具有自定义规则的规则组添加到入侵策略

必须在入侵策略中启用系统中上传的自定义规则，才能对流量实施这些规则。在 防火墙管理中心上传自定义规则后，在入侵策略中添加具有新自定义规则的规则组。

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，点击入侵策略的 **Snort 3 版本** 。

步骤 3 点击规则组搜索栏旁边的 **添加** (+)。

步骤 4 在**添加规则组**窗口中，点击规则组旁边的 **展开箭头**（ › ） 图标以展开本地规则组。

步骤 5 选中已上传的自定义规则组旁边的复选框。

步骤 6 点击**保存 (Save)**。

下一步做什么

部署配置更改；请参阅部署配置更改。

管理 Snort 3 中的自定义规则

系统中上传的自定义规则必须添加到入侵策略并启用，以启用对流量实施这些规则。您可以跨所有策略或选择性地对单个策略启用已上传的自定义规则。

按照以下步骤在一个或多个入侵策略中启用自定义规则：

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 展开 **本地规则**。

步骤 4 选择所需的规则组。

步骤 5 通过选中规则旁边的复选框来选择规则。

步骤 6 从 **规则操作** 下拉框中，选择 **按照入侵策略** 。

步骤 7 选择:

- **所有策略**-对要添加的所有规则具有相同的规则操作。
- **按入侵策略**-为每个入侵策略设置不同的规则操作。

步骤 8 设置规则操作：

- 如果在上一步中选择了所有策略，请从 **选择覆盖状态** 下拉列表中选择所需的规则操作。
- 如果在上一步中选择了按入侵策略，则根据策略名称选择 **规则操作**。要添加更多策略，请点击 **添加其他**。

步骤 9 或者，在 **注释** 文本框中添加注释。

步骤 10 点击**保存**。

下一步做什么

在设备上部署更改。请参阅部署配置更改。

删除自定义规则

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 展开左侧窗格中的 **本地规则** 。

步骤 4 选中要删除的策略的复选框。

步骤 5 确保所选的所有规则的规则操作均为 **禁用**。

如果需要，请按照以下步骤为多个选定规则禁用规则操作：

a) 从 **规则操作** 下拉框中，选择按 **入侵策略**。
b) 选择 **所有策略** 单选按钮。
c) 从 **选择覆盖状态** 下拉列表中选择 **禁用** 。
d) 点击**保存**。
e) 选中要删除的策略的复选框。

步骤 6 从 **规则操作** 下拉框中，选择 **删除**。

步骤 7 在删除规则弹出窗口中点击 **删除** 。

下一步做什么

部署配置更改；请参阅部署配置更改。

删除规则组

开始之前

从包含该规则组的所有入侵策略中排除要删除的规则组。有关从入侵策略中排除规则组的步骤，请参阅 编辑 Snort 3 入侵策略。

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 展开左侧窗格中的 **本地规则** 。

步骤 4 选择要删除的规则组。

步骤 5 在继续之前，请确保将组中所有规则的规则操作设置为 **禁用** 。

如果任何规则的规则操作不是 **禁用**，则无法删除规则组。如果需要，请按照以下步骤禁用所有规则的规则操作：

a) 选中 **规则操作** 下拉列表下方的复选框，以选择组中的所有规则。
b) 从 **规则操作** 下拉框中，选择按 **入侵策略**。
c) 选择 **所有策略** 单选按钮。
d) 从 **选择覆盖状态** 下拉列表中选择 **禁用** 。
e) 点击**保存**。

步骤 6 点击规则组旁边的 **删除** ( ) 。

步骤 7 在 Delete Rule Group 弹出窗口中点击 **OK** 。

下一步做什么

部署配置更改；请参阅部署配置更改。

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。