使用规则调整入侵策略

以下主题介绍如何使用规则调整入侵策略：

- 入侵规则调整基础知识， 第 1 页
- 入侵规则类型， 第 2 页
- 入侵规则的许可证要求， 第 2 页
- 入侵规则的要求和必备条件， 第 3 页
- 查看入侵策略中的入侵规则， 第 3 页
- 入侵策略中的入侵规则过滤器， 第 9 页
- 入侵规则状态， 第 15 页
- 入侵策略中的入侵事件通知过滤器， 第 17 页
- 动态入侵规则状态， 第 22 页
- 添加入侵规则注释， 第 25 页

入侵规则调整基础知识

您可以 使用入侵策略中的规则页面 为共享对象规则、标准文本规则和 预处理器 规则配置规则状态和其他设置。

将规则的状态设置为 生成事件或丢弃并生成事件即可启用该规则。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，以便规则设置为 在内联部署中丢弃并生成事件 规则在匹配流量时生成事件并丢弃该匹配流量。在被动部署中，设置为 Drop and Generate Events 的规则仅对匹配的流量生成事件。

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 预处理器时，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。

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
- 预处理器规则，与数据包解码器的检测选项或与系统随附的预处理器相关联

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	Talos 情报小组	是	有限
标准文本规则	1（全局域或旧式 GID）	低于 1000000	Talos	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	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。

入侵规则的许可证要求

威胁防御 许可证

IPS

经典许可证

保护

入侵规则的要求和必备条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员
- 入侵管理员 (Intrusion Admin)

查看入侵策略中的入侵规则

您可以调整规则在入侵策略中的显示方式，并且可按多个条件将规则排序。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情。

过程

步骤 1 选择**策略** > **访问控制** > **入侵**。

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

如果显示**视图**（  ），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中**策略信息 (Policy Information)** 下的**规则 (Rules)**。

步骤 4 查看规则时，您可以执行以下操作：

- 过滤规则，如在入侵策略中设置规则过滤器，第 14 页中所述。
- 通过点击要按其排序的列顶部的标题对规则进行排序。
- 查看入侵规则的详细信息，如查看入侵规则详细信息，第 5 页中所述。
- 通过从**策略 (Policy)** 下拉列表中选择一个层来查看不同策略层中的规则。

“入侵规则”页面列

“入侵规则”(Intrusion Rules) 页面在其菜单栏和列标题中使用相同的图标。例如，“规则状态”(Rule State) 菜单使用与“规则状态”(Rule State) 列相同的**生成事件 (Generate Events)** 来列出规则。

表 2:“规则”(Rules) 页面列

标题	说明
GID	该整数表示规则的生成器 ID (GID)。
SID	该整数表示充当规则唯一标识符的 Snort ID (SID)。 对于自定义规则， SID 为 1000000 或更大值。
消息	此规则生成的事件中包含的消息，亦作为该规则的名称。
Generate Events	规则的规则状态： • **Drop and Generate Events** • **Generate Events** • **已禁用** 请注意，与为生成事件而不丢弃流量设置的规则的图标相比，已禁用规则的图标只是暗一些而已。此外，您还可以通过点击规则的规则状态图标来更改规则状态。
思科建议的规则状态	思科 为规则建议的规则状态。
事件过滤	事件过滤器，包括应用于该规则的事件阈值和事件抑制。
动态状态	该规则的动态规则状态，如果发生指定的速率异常则会生效。
错误（  ）	为规则配置的警报（当前仅限 SNMP 警报）。
注释（  ）	向规则添加的注释。

也可以使用层下拉列表切换到策略中其他层的“规则”(Rules) 页面。请注意，除非向策略中添加层，否则下拉列表中列出的唯一可编辑视图是策略的 Rules 页面和最初命名为 `My Changes` 的策略层的 Rules 页面；另请注意，在这些视图其中之一进行更改与在其他视图中进行更改相同。该下拉列表中还会列出只读基本策略的 Rules 页面。

入侵规则详细信息

您可以从“规则详细信息”视图查看规则文档、 Cisco 建议和规则开销。还可以查看和添加特定于规则的功能。

表 3: 规则详细信息

项目	说明
摘要	规则摘要。对基于规则的事件，此行将在规则文档包含摘要信息时显示。
规则状态 (Rule State)	规则的当前规则状态。也表示已设置规则状态的层。
思科 建议	如果已生成Cisco建议，则图标表示建议的规则状态；请参阅“入侵规则”页面列，第 4 页。如果建议是启用规则，系统还会指出触发该建议的网络资产或配置。
规则开销	规则对系统性能的潜在影响以及规则产生误报的可能性。本地规则没有分配的开销，除非被映射到漏洞。
阈值	当前为此规则设置的阈值，以及用于为该规则添加阈值的工具。
抑制 (Suppressions)	当前为此规则设置的抑制设置，以及用于为该规则添加抑制的工具。
动态状态 (Dynamic State)	当前为此规则设置的基于速率的规则状态，以及用于为该规则添加动态规则状态的工具。
风险通告	为此规则设置的 SNMP 警报，以及用于为此规则添加警报的工具。
备注	向此规则添加的注释，以及用于为该规则添加注释的工具。
文档	当前规则的规则文档，由Talos 情报小组 提供。或者，点击**规则文档**来查看更具体的规则详细信息。

查看入侵规则详细信息

过程

步骤 1 选择**策略** > **访问控制** > **入侵**。

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

如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 在导航窗格中，点击**规则 (Rules)**。

步骤 4 点击要查看其规则详细信息的规则，然后点击页面底部的**显示详细信息 (Show details)**。
屏幕上将显示规则详细信息，如入侵规则详细信息，第 4 页中所述。

步骤 5 从规则详细信息中，您可以配置：

- 警报 - 请参阅为入侵规则设置 SNMP 警报，第 8 页。
- 注释 - 请参阅将注释添加到入侵规则，第 8 页。
- 动态规则状态 - 请参阅从规则详细信息页面设置动态规则状态，第 7 页。
- 阈值 - 请参阅为入侵规则设置阈值，第 6 页。

- 抑制 - 请参阅为入侵规则设置抑制，第 6 页。

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。

请注意，当输入无效值时，在字段中会显示**恢复**；点击该图标可恢复为该字段的上一个有效值，如果没有先前值，则会清除该字段。

过程

步骤 1 从入侵规则的详细信息中，点击**阈值 (Thresholds)** 旁边的**添加 (Add)**。

步骤 2 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 3 从**跟踪方式 (Track By)** 下拉列表中，选择**源 (Source)** 或**目标 (Destination)** 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 4 在**计数 (Count)** 字段中，输入要用作阈值的事件实例数。

步骤 5 在**秒 (Seconds)** 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 6 点击 **OK**。

提示 系统在“事件过滤”列中的规则旁边显示**事件过滤器**。如果向规则中添加多个事件过滤器，系统将注明事件过滤器的数量。

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。

请注意，当键入的值无效时，字段中会显示**恢复 (Revert)**；点击该图标可恢复为该字段的上一个有效值，如果没有上一个值，则会清除该字段。

过程

步骤 1 从入侵规则的详细信息中，点击**抑制 (Suppressions)** 旁边的**添加 (Add)**。

步骤 2 从**抑制类型 (Suppression Type)** 下拉列表中，选择下列选项之一：

- 选择**规则 (Rule)** 将完全抑制所选规则的事件。
- 选择**源 (Source)** 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 (Destination)** 将抑制由发往指定目标 IP 地址的数据包生成的事件。

步骤 3 如果为抑制类型选择**源 (Source)** 或**目标 (Destination)**，则在**网络 (Network)** 字段中输入 IP 地址、地址块或由这些值的任意组合组成并以逗号分隔的列表。

如果入侵策略与某个访问控制策略的默认操作相关联，则还可以在默认操作变量集中指定或列出网络变量。

系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。

步骤 4 点击 **OK**。

提示 系统将在被抑制规则旁边的“事件过滤”(Event Filtering) 列中的规则旁边显示**事件过滤器 (Event Filter)**。如果向规则中添加多个事件过滤器，过滤器上的数字表示过滤器的数量。

从规则详细信息页面设置动态规则状态

您可以为规则设置一个或多个动态规则状态。列出的第一个动态规则状态具有最高优先级。当两个动态规则状态相冲突时，将执行第一个状态的操作。

动态规则状态为策略特定的。

请注意，当输入无效值时，在字段中会显示**恢复**；点击该图标可恢复为该字段的上一个有效值，如果没有先前值，则会清除该字段。

过程

步骤 1 从入侵规则的详细信息中，点击**动态状态 (Dynamic State)** 旁边的**添加 (Add)**。

步骤 2 从**跟踪方式 (Track By)** 下拉列表中，选择用于指示要如何跟踪规则匹配项的选项：

- 选择**源 (Source)** 将跟踪由特定的一个或一组源地址发出的该规则匹配项的数量。
- 选择**目标 (Destination)** 将跟踪发往特定的一个或一组目标地址的该规则匹配项的数量。
- 选择**规则 (Rule)** 将跟踪该规则的所有匹配项。

步骤 3 如果将**跟踪方式 (Track By)** 设置为**源 (Source)** 或**目标 (Destination)**，请在**网络 (Network)** 字段中输入要跟踪的每台主机的 IP 地址。

系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。

步骤 4 在**速率 (Rate)** 旁边，指定每个时间段的规则匹配项数，以设置攻击速率：

- 在**计数 (Count)** 字段中，指定要用作阈值的规则匹配数。
- 在**秒数 (Seconds)** 字段中，指定跟踪攻击的时间段的秒数。

步骤 5 从**新状态 (New State)** 状态下拉列表中，选择满足条件时要采取的新操作。

步骤 6 在**超时 (Timeout)** 字段中输入值。

在超时后，规则将恢复到其原始状态。输入 0 可防止新操作超时。

步骤 7 点击 **OK**。

提示 系统将在“动态状态”()列中的规则旁边显示动态状态。如果向规则中添加多个动态规则状态过滤器，过滤器上的数字表示过滤器的数量。

为入侵规则设置 SNMP 警报

您可以从 Rule Detail 页面为规则设置 SNMP 警报。

过程

从入侵规则的详细信息中，点击**警报 (Alerts)** 旁边的**添加 SNMP 警报 (Add SNMP Alert)**。

提示 系统将在“警报”列中的规则旁边显示警报**错误**（  ）。如果向规则中添加多个警报，则系统将指示警报的数量。

将注释添加到入侵规则

过程

步骤 1 从入侵规则的详细信息中，点击**注释 (Comments)** 旁边的**添加 (Add)**。

步骤 2 在**注释 (Comment)** 字段中，输入规则注释。

步骤 3 点击 **OK**。

提示 系统将并在“注释”(Comments) 列中的规则旁显示**注释**（  ）。如果向规则中添加多个注释，注释上的数字表示注释的数量。

步骤 4 要删除规则注释，请点击规则注释部分的**删除 (Delete)**。仅当缓存的注释具有未提交的入侵策略更改时，才能删除该注释。

下一步做什么

- 部署配置更改；请参阅部署配置更改。

入侵策略中的入侵规则过滤器

可以按单一条件或按一个或多个条件的组合来过滤 Rules 页面中显示的规则。

规则过滤器关键字可帮助您找到要对其应用规则状态或事件过滤器等规则设置的规则。您可以按关键字进行过滤，同时从“规则”(Rules) 页面的过滤器面板选择所需参数作为关键字的参数。

入侵规则过滤器说明

您所构造的过滤器显示于“过滤器”(Filter) 文本框中。点击过滤器面板中的关键字和关键字参数可以构造过滤器。当选择多个关键字时，系统会使用 AND 逻辑将其组合以创建复合搜索过滤器。例如，如果选择**类别 (Category)** 下的**预处理器 (preprocessor)**，然后选择**规则内容 (Rule Content)** > **GID** 并输入 `116`，则会获得过滤器 `Category: “preprocessor” GID:”116”`，用于检索属于预处理器规则**并且** GID 为 116 的所有规则。

通过 Category、Microsoft Vulnerabilities、Microsoft Worms、Platform Specific、Preprocessor 和 Priority 过滤器组，可以为一个关键字提交多个参数（以逗号分隔）。例如，可以从**类别 (Category)** 中选择 **os-linux** 和 **os-windows** 以生成过滤器 `Category:"os-windows,os-linux"`，用于检索 `os-linux` 类别或 `os-windows` 类别中的任意规则。

要显示过滤器面板，请点击**显示图标**。

要隐藏过滤器面板，请点击**隐藏图标**。

入侵策略规则过滤器构建准则

在大多数情况下，当构建过滤器时，可以使用入侵策略中“规则”(Rules) 页面左侧的过滤器面板选择要使用的关键字/参数。

规则过滤器在过滤器面板中分为不同的规则过滤器组。许多规则过滤器组包含子条件，因此可以更轻松地找到所需的特定规则。有些规则过滤器有多个级别，可展开以向下钻取到各个规则。

过滤器面板中的项有时表示过滤器类型组，有时表示关键字，还有时表示关键字的参数。请注意以下提示：

- 当选择不是关键字的过滤器类型组标题（“规则配置”[Rule Configuration]、“规则内容”[Rule Content]、“平台特定”[Platform Specific] 和“优先级”[Priority]）时，该标题会展开以列出可用关键字。

  通过点击条件列表中的节点来选择关键字时，将显示一个弹出窗口，其中提供要作为过滤条件的参数。

  如果过滤器中已在使用该关键字，则提供的参数将替换该关键字的现有参数。

  例如，如果点击过滤器面板中**规则配置 (Rule Configuration)** > **建议 (Recommendation)** 下的**丢弃并生成事件 (Drop and Generate Events)**，则会将 `Recommendation:"Drop and Generate Events"` 添加到过滤器文本框中。如果随后点击**规则配置** > **建议** 下的**生成事件**，则过滤器会更改为`建议: “生成事件”`。

- 当选择属于关键字的过滤器类型组标题（“类别”[Category]、“分类”[Classifications]、“Microsoft 漏洞”[Microsoft Vulnerabilities]、“Microsoft 蠕虫”[Microsoft Worms]、“优先级”[Priority] 和“规则更新”[Rule Update]）时，该标题会列出可用参数。

  从此类型的组中选择项目时，该参数及其应用到的关键字会立即添加到过滤器中。如果该关键字已经在过滤器中，它将替换与该组对应的关键字的现有参数。

  例如，如果点击过滤器面板中**类别**下的 **os-linux**，则会将 类别：“os-linux”添加到过滤器文本框中。如果随后点击 **Category** 下的 **os-windows**，过滤器将更改为 `Category:"os-windows"`。

- Rule Content 下的 Reference 是关键字，其下方列出的特定引用 ID 类型同样如此。选择任何引用关键字时，会显示一个弹出窗口，其中提供添加到现有过滤器的参数和关键字。如果过滤器中已在使用该关键字，则提供的新参数将替换现有参数。

  例如，如果依次点击过滤器面板中的**规则内容 (Rule Content)** > **引用 (Reference)** > **CVE ID**，系统将显示弹出窗口，提示您提供 CVE ID。如果输入 `2007`，则会将 `CVE:”2007”` 添加到过滤器文本框中。又例如，如果依次点击过滤器面板中的**规则内容 (Rule Content)** > **引用 (Reference)**，系统将显示弹出窗口，提示您提供该引用。如果输入 `2007`，则会将 `Reference:”2007”` 添加到过滤器文本框中。

- 从不同的组中选择规则过滤器关键字时，会将每个过滤器关键字都添加到过滤器中并保留所有现有关键字（除非被同一关键字的新值覆盖）。

  例如，如果点击过滤器面板中**类别**下的 **os-linux**，则会将 类别：“os-linux”添加到过滤器文本框中。如果随后点击 **Microsoft Vulnerabilities** 下的 **MS00-006**，过滤器将更改为 `Category:"os-linux" MicrosoftVulnerabilities:"MS00-006"`。

- 当选择多个关键字时，系统会使用 AND 逻辑将其组合以创建复合搜索过滤器。例如，如果选择**类别 (Category)** 下的**预处理器 (preprocessor)**，然后选择**规则内容 (Rule Content)** > **GID** 并输入 `116`，则会获得过滤器 `Category: “preprocessor” GID:”116”`，用于检索属于预处理器规则**并且** GID 为 116 的所有规则。

- Category、Microsoft Vulnerabilities、Microsoft Worms、Platform Specific 和 Priority 过滤器组可以为一个关键字提交多个参数（以逗号分隔）。例如，可以从**类别 (Category)** 中选择 **os-linux** 和 **os-windows** 以生成过滤器 `Category:"os-windows,app-detect"`，用于检索 `os-linux` 类别或 `os-windows` 类别中的任意规则。

同一规则可以按多个过滤器关键字/参数对进行检索。例如，如果按类别 **dos** 来过滤规则，系统将显示 DOS 思科尝试规则 (SID 1545)，按优先级 **High** 进行过滤亦如此。

注释 Talos 情报小组 可能会使用规则更新机制添加和删除规则过滤器。

请注意，“规则”页面上的规则可以是共享对象规则（生成器 ID 3）或标准文本规则（生成器 ID 1，全局域或旧式 GID；1000-2000，子代域）。下表介绍不同的规则过滤器。

表 *4:* 规则过滤器组

过滤器组	说明	是否支持多个参数？	标题为.....	列表中的项目为.....
规则配置 (Rule Configuration)	根据规则的配置查找规则。	否	一组	关键词
规则内容 (Rule Content)	根据规则的内容查找规则。	否	一组	关键词
类别 (Category)	根据规则编辑器使用的规则类别来查找规则。请注意，本地规则显示于本地子组中。	是	一个关键字	参数
分类 (Classifications)	根据规则生成的事件的数据包显示中所显示的攻击分类来查找规则。	否	一个关键字	参数
Microsoft 漏洞 (Microsoft Vulnerabilities)	根据 Microsoft 公告号查找规则。	是	一个关键字	参数
Microsoft 蠕虫 (Microsoft Worms)	根据影响 Microsoft Windows 主机的特定蠕虫查找规则。	是	一个关键字	参数
平台特定 (Platform Specific)	根据规则与特定操作系统版本的关联性来查找规则。 请注意，规则可能会影响多个操作系统或某个操作系统的多个版本。例如，启用 SID 2260 会影响多个版本的 Mac OS X、IBM AIX 以及其他操作系统。	是	一个关键字	参数 请注意，如果从子列表中选择其中一项，则会向参数添加修饰符。
预处理程序	查找各个预处理器的规则。 请注意，在启用预处理器时，必须启用与预处理器选项相关联的预处理器规则才能生成事件并在内联部署中丢弃攻击性数据包该选项的事件。	是	一组	子组
优先级	根据高、中和低优先级查找规则。 分配给规则的分类将确定该规则的优先级。这些组进一步分为不同的规则类别。请注意，本地规则（即您导入或创建的规则）不会显示在优先级组中。	是	一个关键字	参数 请注意，如果从子列表中选择其中一项，则会向参数添加修饰符。
规则更新 (Rule Update)	查找通过特定规则更新添加或修改的规则。对于每个规则更新，可以查看更新中的所有规则、仅查看更新中导入的新规则或仅查看更新所更改的现有规则。	否	一个关键字	参数

入侵规则配置过滤器

您可以按多个规则配置设置来过滤“规则”(Rules) 页面中列出的规则。例如，如果要查看规则状态与建议的规则状态不匹配的一组规则，可以选择**不匹配建议 (Does not match recommendation)** 来根据规则状态进行过滤。

通过点击条件列表中的节点来选择关键字时，可以提供要作为过滤条件的参数。如果过滤器中已在使用该关键字，则提供的参数将替换该关键字的现有参数。

例如，如果点击过滤器面板中**规则配置 (Rule Configuration)** > **建议 (Recommendation)** 下的**丢弃并生成事件 (Drop and Generate Events)**，则会将 `Recommendation:"Drop and Generate Events"` 添加到过滤器文本框中。如果随后点击**规则配置 (Rule Configuration)** > **建议 (Recommendation)** 下的**生成事件 (Generate Events)**，则过滤器会更改为 `Recommendation:"Generate Events"`。

入侵规则内容过滤器

您可以按多个规则内容项来过滤 Rules 页面中列出的规则。例如，通过搜索规则的 SID 可以快速检索该规则。也可以查找用于检测发往特定目标端口的流量的所有规则。

通过点击条件列表中的节点来选择关键字时，可以提供要作为过滤条件的参数。如果过滤器中已在使用该关键字，则提供的参数将替换该关键字的现有参数。

例如，如果点击过滤器面板中**规则内容**下的 **SID**，系统将显示弹出窗口，提示您提供 SID。如果键入 `1045`，则 `SID:”1045”` 会被添加到过滤器文本框中。如果随即再次点击 **SID** 并将 SID 过滤器更改为 `1044`，过滤器将更改为 `SID:”1044”`。

表 *5:* 规则内容过滤器

以下过滤器	查找符合以下条件的规则
消息	在消息字段中包含所提供的字符串。
SID	具有指定的 SID。
GID	具有指定的 GID。
参考	在引用字段中包含所提供的字符串。您也可以按特定类型的引用和所提供字符串进行过滤。
操作	首先执行 `alert` 或 `pass`。
协议	包含所选协议。
方向	基于规则是否包含指示的方向设置。
源 IP	使用指定的地址或变量作为规则中的源 IP 地址指定。可以按有效 IP 地址、CIDR 块/前缀长度或者使用 `$HOME_NET` 或 `$EXTERNAL_NET` 等变量进行过滤。
目标 IP	使用指定的地址或变量作为规则中的源 IP 地址指定。可以按有效 IP 地址、CIDR 块/前缀长度或者使用 `$HOME_NET` 或 `$EXTERNAL_NET` 等变量进行过滤。

以下过滤器	查找符合以下条件的规则
源端口	包括指定的源端口。端口值必须为 1 到 65535 之间的整数或端口变量。
目的端口	包括指定的目标端口。端口值必须为 1 到 65535 之间的整数或端口变量。
规则开销	具有所选规则开销。
元数据	具有包含匹配的键值对的元数据。例如，键入 `metadata:"service http"` 可查找元数据与 HTTP 应用协议相关的规则。

入侵规则类别

Firepower 系统根据规则检测的流量类型对规则分类。在 Rules 页面中，可以按规则类别过滤，从而可为某个类别中的所有规则设置规则属性。例如，如果网络中没有 Linux 主机，则可以按 **os-linux** 类别过滤，然后禁用表明将禁用整个 **os-linux** 类别的所有规则。

可以将鼠标指针悬停在类别名称上方来显示该类别中的规则数。

注释 Talos 情报小组 可能会使用规则更新机制来添加和删除规则类别。

入侵规则过滤器组件

通过编辑过滤器可以修改您在过滤器面板中点击过滤器时所提供的特定关键字及其参数。“规则”(Rules) 页面中的自定义过滤器的功能与规则编辑器中使用的过滤器类似，但除此之外，您还可以使用在“规则”(Rules) 页面过滤器中提供的任何关键字，使用在过滤器面板中选择过滤器时显示的语法。要确定供今后使用的关键字，请点击右侧过滤器面板中的相应参数。过滤器关键字和参数语法显示在过滤器文本框中。请记住，仅对“类别”和“优先级”过滤器类型支持关键字的多个以逗号分隔的参数。

您可以使用关键字和参数、字符串及带引号的原义字符串，以空格分隔多个过滤条件。过滤器不能包含正则表达式、通配符或任何特殊运算符，例如取反字符 (!)、大于号 (>) 和小于号 (<) 等。当键入的搜索条件没有关键字、关键字的首字母没有大写或者没有用引号将参数引起来时，该搜索将被视为字符串搜索，并搜索类别、消息和 SID 字段中有无指定条件。

除关键字 `gid` 和 `sid` 之外，所有参数和字符串都被视为部分字符串。`gid` 和 `sid` 的参数只会返回完全匹配项。

每个规则过滤器都可以包含一个或多个关键字，其格式如下：

`keyword``:"`*`argument`*`"`

其中，keyword 是入侵规则过滤器组中的关键字之一，argument 是要在与该关键字相关的一个或多个特定字段中搜索的字母数字字符串，用双引号引起来且不区分大小写。请注意，键入的关键字应该首字母大写。

除 gid 和 sid 之外，所有关键字的参数都会被视为部分字符串。例如，参数 123 将返回 "12345"、"41235"、"45123" 等。gid 和 sid 的参数只会返回完全匹配项；例如，sid:3080 只会返回结果 SID 3080。

每个规则过滤器还可以包含一个或多个字母数字字符串。字符串将搜索规则的“消息”字段、Snort ID (SID) 和生成器 ID (GID)。例如，字符串 123 会返回规则消息中的 "Lotus123"、"123mania" 等字符串，也会返回 SID 6123、SID 12375 等。使用一个或多个字符串来进行过滤可以搜索部分 SID。

所有字符串都不区分大小写并被视为部分字符串。例如，字符串 ADMIN、admin 或 Admin 中的任意一个都会返回 "admin"、"CFADMIN"、"Administrator" 等等。

用引号将字符串引起来可以返回完全匹配项。例如，用引号引起来的原义字符串 "overflow attempt" 只会返回完全匹配的该字符串，而由 overflow 和 attempt 这两个字符串组成的未加引号的过滤器则会返回 "overflow attempt"、"overflow multipacket attempt"、"overflow with evasion attempt" 等结果。

输入关键字、字符串或这二者的任意组合并以空格分隔可以缩小过滤结果的范围。结果包括符合所有过滤条件的任意规则。

可以按照任意顺序输入多个过滤条件。例如，以下每个过滤器返回的规则相同：

- url:at login attempt cve:200
- login attempt cve:200 url:at
- login cve:200 attempt url:at

入侵规则过滤器的使用

可以从入侵策略中“规则”(Rules) 页面左侧的过滤器面板中选择预定义的过滤器关键字。选择过滤器时，该页面会显示所有匹配的规则，或者指出没有匹配的规则。

您可以对过滤器添加关键字来进一步对其进行限制。输入的任何过滤器都会搜索整个规则数据库并返回所有匹配的规则。当您在页面仍显示上一过滤器的结果时输入过滤器，页面将清空，转而返回新过滤器的结果。

您也可以使用在选择过滤器时提供的相同关键字和参数语法来键入过滤器，或者在选择过滤器后修改其中的参数值。当键入的搜索条件没有关键字、关键字的首字母没有大写或者没有用引号将参数引起来时，该搜索将被视为字符串搜索，并搜索类别、消息和 SID 字段中有无指定条件。

在入侵策略中设置规则过滤器

您可以对 Rules 页面中的规则进行过滤来显示其中一组规则。然后，可以使用任何页面功能，包括选择情景菜单中可用的任何功能。例如，当您需要为某个特定类别中的所有规则设置阈值时，此功能会非常有用。您可以对已过滤或未过滤列表中的规则使用相同的功能。例如，您可以将新的规则状态应用到已过滤或未过滤列表中的规则。

所有过滤器关键字、关键字参数和字符串都不区分大小写。如果点击过滤器中已存在的关键字的参数，则该参数将替换现有的参数。

过程

步骤 1 选择**策略** > **访问控制** > **入侵**。

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

如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 使用以下任一方法单独或以组合形式构建过滤器：

- 在**过滤器 (Filter)** 文本框中输入值，然后按 Enter 键。
- 展开任何预定义的关键字。例如，点击**规则配置 (Rule Configuration)**。
- 点击一个关键字，并指定参数值（如果提示）。例如：
  - 在**规则配置 (Rule Configuration)** 下，可以点击**规则状态 (Rule State)**，从下拉列表中选择生成事件 (Generate Events)，然后点击**确定 (OK)**。
  - 在**规则配置 (Rule Configuration)** 下，可以点击**注释 (Comment)**，输入要筛选的注释文本字符串过滤，然后点击**确定 (OK)**。
  - 在**类别 (Category)** 下，可以点击**应用检测 (app-detect)**，系统将其用作参数值。
- 展开关键字，然后点击一个参数值。例如，展开**规则状态 (Rule State)**，然后点击**生成事件 (Generate Events)**。

入侵规则状态

通过入侵规则状态，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。

Talos 情报小组 为每个默认策略中的每条入侵规则和预处理器规则设置默认状态。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状态。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状态发生更改时，也允许规则更新更改策略中的规则默认状态。但请注意，如果您已经更改了规则状态，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状态。

入侵规则状态选项

在入侵策略中，可以将规则的状态设置为以下值：

生成事件

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。

丢弃并生成事件

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。

请注意，设置为此规则状态的规则在被动部署中生成事件但不丢弃数据包。为使系统丢弃数据包，还必须在入侵策略中启用**内联时丢弃 (Drop when Inline)** 并部署设备内联，并且您必须内联部署设备。

禁用

您不希望系统评估匹配流量。

注释 选择**生成事件 (Generate Events)** 或**丢弃并生成事件 (Drop and Generate Events)** 选项可启用规则。选择**禁用 (Disable)** 会禁用规则。

思科**强烈**建议**不要**启用入侵策略中的所有入侵规则。如果启用所有规则，则您的受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。

设置入侵规则状态

入侵规则状态为策略特定的。

过程

步骤 1 选择**策略** > **访问控制** > **入侵**。

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

如果显示**视图**（  ），则表明配置属于祖先域，或者您没有修改配置的权限。

提示 此页面指示已启用规则的总数、设置为“生成事件”的已启用规则的总数，以及设置为“丢弃并生成事件”的总数。另请注意，在被动部署中，设置为 Drop and Generate Events 的规则仅生成事件。

步骤 3 点击导航面板中**策略信息 (Policy Information)** 正下方的**规则 (Rules)**。

步骤 4 选择要在其中设置规则状态的一条或多条规则。

步骤 5 选择以下其中一个选项：

- **规则状态** > **生成事件**
- **规则状态** > **丢弃并生成事件**
- **规则状态** > **禁用**

步骤 6 要保存自上次策略提交以来在此策略中进行的更改，请点击导航面板中的**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

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

您可以逐个入侵策略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、标准文本规则或预处理器规则设置阈值。

入侵事件阈值配置

要设置阈值，请先指定阈值类型。

表 *6:* 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。

选项	说明
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）

接下来，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 *7:* 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 *8:* 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。
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。

相关主题

detection_filter 关键字

添加和修改入侵事件阈值

可以为入侵策略中的一条或多条特定规则设置阈值。也可以单独或同时修改现有阈值设置。可以为每条规则设置一个阈值。添加阈值将覆盖该规则的任何现有阈值。

还可以修改默认应用到与入侵策略关联的所有规则和预处理器生成的事件的全局阈值。

当输入无效值时，字段中会显示**恢复 (Revert)**；点击该图标可恢复为该字段的上一个有效值，如果没有上一个值，则会清除该字段。

提示 在有多个 CPU 的受管设备上，全局阈值或单独的阈值可能会导致事件数量高于预期。

过程

步骤 1 选择**策略** > **访问控制** > **入侵**。

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

如果显示**视图**（  ），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航窗格中**策略信息 (Policy Information)** 正下方的**规则 (Rules)**。

步骤 4 选择要在其中设置阈值的一条或多条规则。

步骤 5 选择**事件过滤 (Event Filtering)** > **阈值 (Threshold)**。

步骤 6 从**类型 (Type)** 下拉列表中选择阈值类型。

步骤 7 从**跟踪方式 (Track By)** 下拉列表中，选择要按**源 (Source)** 还是**目标 (Destination)** IP 地址跟踪事件实例。

步骤 8 在**计数 (Count)** 字段中输入值。

步骤 9 在**秒数 (Seconds)** 字段中输入值。

步骤 10 点击 **OK**。

提示 系统在“事件过滤”(Event Filtering) 列中的规则旁边显示**事件过滤器 (Event Filter)** 。如果向规则中添加多个事件过滤器，过滤器上的数字表示事件过滤器的数量。

步骤 11 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

下一步做什么

- 部署配置更改；请参阅部署配置更改。

相关主题

全局规则阈值基础知识

查看和删除入侵事件阈值

您可能需要查看或删除一个规则的现有阈值设置。可以使用“规则详细信息”(Rules Details) 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。

请注意，还可以修改全局阈值，它默认应用到入侵策略所记录的所有规则和预处理器生成的事件。

过程

步骤 1 选择**策略** > **访问控制** > **入侵**。

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

如果显示**视图**（  ），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航窗格中**策略信息 (Policy Information)** 正下方的**规则 (Rules)**。

步骤 4 选择配置了要查看或删除的阈值的一条或多条规则。

步骤 5 要删除每条所选规则的阈值，请依次选择 **事件过滤器** > **删除阀值**。

步骤 6 点击 **OK**。

步骤 7 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

下一步做什么

- 部署配置更改；请参阅部署配置更改。

相关主题

全局规则阈值基础知识

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预处理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。在入侵规则编辑器页面（**对象** > **入侵规则**）和任何入侵事件页面（如果该事件由入侵规则触发）上，也可以使用右键单击情景菜单访问抑制设置。

相关主题

detection_filter 关键字

抑制特定规则的入侵事件

您可以在入侵策略中抑制一个或多个规则的入侵事件通知。当某条规则的通知被抑制时，规则会触发，但不会生成事件。可以为一个规则设置一个或多个抑制。列出的第一个抑制的优先级最高。当两个抑制发生冲突时，将执行第一个抑制的操作。

请注意，当输入无效值时，在字段中会显示**恢复 (Revert)**；点击该图标可恢复为该字段的上一个有效值，如果没有先前值，则会清除该字段。

过程

步骤 1 选择**策略** > **访问控制** > **入侵**。

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

如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中**策略信息 (Policy Information)** 正下方的**规则 (Rules)**。

步骤 4 选择要为其配置抑制条件的一个或多个规则。

步骤 5 依次选择**事件过滤 (Event Filtering)** > **抑制 (Suppression)**。

步骤 6 选择**抑制类型 (Suppression Type)**。

步骤 7 如果为抑制类型选择了**源 (Source)** 或**目标 (Destination)**，请在**网络 (Network)** 字段中输入要指定为源或目标 IP 地址的 IP 地址、地址块或变量，或者输入由这些值的任意组合组成的逗号分隔列表。

系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。

步骤 8 点击 **OK**。

提示 系统将在被抑制规则旁边的“事件过滤”(Event Filtering) 列中的规则旁边显示**事件过滤器 (Event Filter)**。如果向规则中添加多个事件过滤器，过滤器上的数字表示事件过滤器的数量。

步骤 9 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

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**策略** > **访问控制** > **入侵**。

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

如果显示**视图**（  ），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中**策略信息 (Policy Information)** 正下方的**规则 (Rules)**。

步骤 4 选择要查看或删除其抑制的一个或多个规则。

步骤 5 有以下选项可供选择：

- 要删除规则的所有抑制，请依次选择 **事件过滤** > **删除抑制**。
- 要删除特定抑制设置，请点击规则，然后点击**显示详细信息 (Show details)**。展开抑制设置，然后点击要删除的抑制设置旁边的 **Delete**。

步骤 6 点击 **OK**。

步骤 7 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

下一步做什么

- 部署配置更改；请参阅部署配置更改。

动态入侵规则状态

基于速率的攻击通过向网络或主机发送过多的流量，企图让网络或主机不堪重负，导致其速度下降或拒绝合法请求。为了应对特定规则出现过多规则匹配项的情况，可以使用基于速率的防御来更改规则的操作。

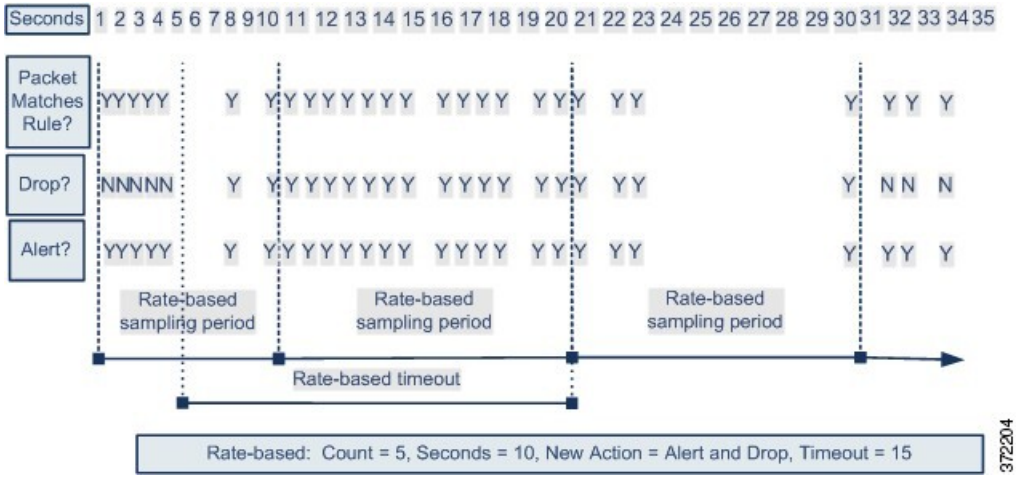
您可以配置入侵策略，使其包含基于速率的过滤器，从而检测指定时间段内出现某条规则匹配项过多的情况。此功能可以用于内联部署的受管设备上，先在指定时间内拦截基于速率的攻击，然后恢复为规则匹配项仅生成事件而不丢弃流量的规则状态。

基于速率的攻击防御可确定异常流量模式，并可将这些流量对合法请求的影响降至最低。您可以识别出发往一个或多个特定目标 IP 地址或者由一个或多个特定源 IP 地址发出的流量中存在的过多规则匹配项。也可以对检测的所有流量中符合特定规则的过多匹配项作出响应。

在某些情况下，您可能不希望将某规则设置为“丢弃并生成事件”(Drop and Generate Events) 状态，因为您不想丢弃与该规则匹配的每个数据包，但同时您又确实希望在指定事件内出现特定频率的匹配项时丢弃与该规则匹配的数据包。动态规则状态可用于配置应该触发规则操作更改的速率、达到该速率时应该改而执行的操作以及新操作应该持续的时间。

下图显示的例子中，攻击者正在尝试访问主机。反复尝试查找密码触发了配置有基于速率的攻击防御的规则。当在 10 秒的时间跨度内发生五次规则匹配之后，基于速率的设置会将规则属性更改为“丢弃并生成事件”(Drop and Generate Events)。新的规则属性在 15 秒之后超时。

请注意，到达超时时间后，在接下来的基于速率的采样周期内，系统仍然丢弃数据包。如果采样速率高于当前或前一个采样周期的阈值，新操作将继续。只有在采样周期完毕而采样速率低于阈值速率之后，新操作才会恢复为“生成事件”(Generate Events)。



动态入侵规则状态配置

在入侵策略中，可以为任何入侵规则或预处理器规则配置基于速率的过滤器。基于速率的过滤器包含三个组成部分：

- 规则的匹配速率，配置为特定秒数内的规则匹配项数量
- 超过速率时要执行的新操作，可用的操作有三项：“生成事件”(Generate Events)、“丢弃并生成事件”(Drop and Generate Events) 和“禁用”(Disable)。
- 操作的持续时间，配置为超时值

请注意，新操作自开始之后，在到达超时时间之前会一直执行，即使速率在这段时间内降到配置的速率以下亦不会停止。达到超时后，如果速率低于阈值，则规则的操作会恢复到为该规则最初配置的操作。

在内联部署中，可以配置基于速率的攻击防御来临时或永久拦截攻击。如果没有基于速率的配置，设置为“生成事件”(Generate Events) 的规则确实会生成事件，但系统不会丢弃这些规则的数据包。

但是，如果攻击流量所匹配的规则配置了基于速率的条件，则基于速率的操作可能会导致系统在该操作处于活动状态的时间内丢弃数据包，即便这些规则最初并未设置为“丢弃并生成事件”(Drop and Generate Events)。

注释 基于速率的操作无法启用禁用的规则，也无法丢弃与禁用的规则匹配的流量。

可以对同一规则定义多个基于速率的过滤器。入侵策略中列出的第一个过滤器优先级最高。请注意，当两个基于速率的过滤器的操作相冲突时，系统将执行第一个基于速率的过滤器的操作。

从规则页面设置动态规则状态

您可以为规则设置一个或多个动态规则状态。列出的第一个动态规则状态具有最高优先级。当两个动态规则状态相冲突时，将执行第一个状态的操作。

动态规则状态为策略特定的。

当输入无效值时，字段中会显示**恢复 (Revert)**；点击该图标可恢复为该字段的上一个有效值，如果没有上一个值，则会清除该字段。

注释 动态规则状态无法启用禁用的规则，也无法丢弃与禁用的规则匹配的流量。

过程

步骤 1 选择**策略** > **访问控制** > **入侵**。

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

如果显示**视图**（  ），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航窗格中**策略信息 (Policy Information)** 正下方的**规则 (Rules)**。

步骤 4 选择要在其中添加动态规则状态的一条或多条规则。

步骤 5 依次选择**动态状态 (Dynamic State)** > **添加基于速率的规则状态 (Add Rate-Based Rule State)**。

步骤 6 从**跟踪方式 (Track By)** 下拉列表中选择一个值。

步骤 7 如果将 **Track By** 设置为 **Source** 或 **Destination** 时，请在 **Network** 字段中输入要跟踪的每台主机的地址。可以指定单个 IP 地址、地址块、变量或由这些值的任意组合组成并以逗号分隔的列表。

系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。

步骤 8 在**速率 (Rate)** 旁边，指定每个时间段的规则匹配项数，以设置攻击速率：

- 在**计数 (Count)** 字段中输入值。
- 在**秒数 (Seconds)** 字段中输入值。

步骤 9 从**新状态 (New State)** 状态下拉列表中，指定满足条件时要采取的新操作。

步骤 10 在**超时 (Timeout)** 字段中输入值。

在超时后，规则将恢复到其原始状态。指定 0 或将**超时 (Timeout)** 字段留空可防止新操作超时。

步骤 11 点击 **OK**。

提示 系统将在“动态状态”(Dynamic State) 列中的规则旁边显示**动态状态** 。如果向规则中添加多个动态规则状态过滤器，过滤器上的数字表示过滤器的数量。

提示 要删除一组规则的所有动态规则设置，请在“规则”(Rules) 页面中选择这些规则，然后依次选择**动态状态 (Dynamic State)** > **删除基于速率的状态 (Remove Rate-Based States)**。也可以从规则的规则详细信息中删除个别基于速率的规则状态过滤器，方法是选择该规则后点击**显示详细信息 (Show details)**，然后点击要删除的基于速率的过滤器旁边的**删除 (Delete)**。

步骤 12 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

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。添加的任何注释都将显示在该入侵策略的“规则”(Rules) 页面的“规则详细信息”(Rule Details) 视图中。

提交包含注释的入侵策略更改后，点击该规则 Edit 页面中的 **Rule Comment** 也可查看该注释。

过程

步骤 1 选择**策略** > **访问控制** > **入侵**。

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

如果显示**视图**（  ），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中**策略信息 (Policy Information)** 正下方的**规则 (Rules)**。

步骤 4 选择要在其中添加注释的一条或多条规则。

步骤 5 依次选择 **注释** > **添加规则注释**。

步骤 6 在**注释 (Comment)** 字段中，输入规则注释。

步骤 7 点击 **OK**。

提示 系统将并在“注释”(Comments) 列中的规则旁显示 **注释**（  ）。如果向规则中添加多个注释，注释上的数字表示注释的数量。

步骤 8 或者，通过点击注释旁边的**删除 (Delete)** 以删除规则注释。

仅当缓存的注释具有未提交的入侵策略更改时，才能删除该注释。提交入侵策略更改之后，规则注释即是永久性的。

步骤 9 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

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。