入侵事件日志记录的全局限制

以下主题介绍如何全局限制入侵事件日志记录：

全局规则阈值基础知识

全局规则阈值为入侵策略记录的事件设置了限制。您可以跨所有流量设置全局规则阈值，用于限制策略在每个指定时间段记录和显示来自特定源地址或目标地址的事件的频率。您还可以根据策略中的共享对象规则、标准文本规则或预处理器规则设置阈值。设置全局阈值后，该阈值将应用于策略中没有特定阈值可覆盖该阈值的每条规则。阈值可以防止因事件数量过多而使系统不堪重负。

每个入侵策略包含一个默认应用于所有入侵规则和预处理器规则的默认全局规则阈值。此默认阈值将发往目标地址的流量的事件数限制为每 60 秒一个事件。

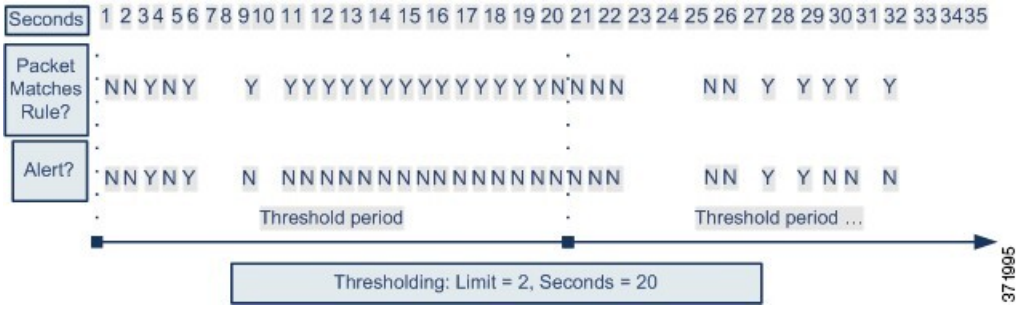
您可以执行以下操作：

- 更改全局阈值。
- 禁用全局阈值。
- 通过为特定规则设置单独的阈值来覆盖全局阈值。

  例如，可将全局限值阈值设置为每 60 秒生成五个事件，然后为 SID 1315 设置每 60 秒生成十个事件的特定阈值。所有其他规则每 60 秒生成的事件不超过五个，但是系统每 60 秒可为 SID 1315 生成多达十个事件。

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。

下图展示了全局规则阈值的工作方式。在此示例中，系统正受到违反特定规则的攻击。全局限值阈值设置为将每条规则的事件生成频率限制为每 20 秒生成两个事件。请注意，该时间段在 1 秒时开始，在21秒时结束。该时间段结束后，时间周期重新开始，接下来两次规则匹配生成了事件，随后系统在这一时间段内不再生成事件。



全局规则阈值选项

默认阈值将每条规则的事件生成频率限制为对发往同一个目标地址的流量每60秒生成一个事件。全局规则阈值选项的默认值如下：

- **类型 (Type)** -“限制”(Limit)
- **跟踪依据 (Track By)** -“目标”(Destination)
- **计数 (Count)** - 1
- **秒数 (Seconds)** - 60

您可以如下修改这些默认值：

表 *1:* 阈值类型

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 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 (Threshold)	在指定时间段内，当指定数量的数据包（由 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`，因此系统此时会再记录一个事件。

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，如将类型设置为**两者 (Both)**，将**计数 (Count)** 设置为 `2`，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）

跟踪依据 (Track By) 选项确定事件实例计数是按源 IP 地址计算还是按目标 IP 地址计算。

您还可以如下指定用于定义阈值的实例数和时间段：

表 *2:* 阈值实例/时间选项

选项	说明
计数	对于**限制 (Limit)** 阈值，是指每个跟踪 IP 地址或地址范围在每个指定时间段内达到阈值所需的事件实例数。 对于**阀值 (Threshold)** 阈值，是指要用作阈值的规则匹配项的数量。
秒	对于**限制 (Limit)** 阈值，是指组成跟踪攻击的时间段的秒数。 对于**阀值 (Threshold)** 阈值，是指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 (Source)**，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。

相关主题

配置全局阈值，第 4 页
入侵事件阈值

全局阈值的许可证要求

威胁防御 许可证

IPS

经典许可证

保护

全局阈值的要求和必备条件

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)

配置全局阈值

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

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 点击导航面板中的**高级设置 (Advanced Settings)**。

步骤 4 如果**入侵规则阈值 (Intrusion Rule Thresholds)** 下的**全局规则阈值** （**Global Rule Thresholding**） 已禁用，请点击**已启用 (Enabled)**。

步骤 5 点击**全局规则阈值 (Global Rule Thresholding)** 旁边的 **编辑**（  ）。

步骤 6 使用**类型 (Type)**，指定在**秒数 (Seconds)** 字段中指定的时间内将应用的阈值类型。

步骤 7 使用**跟踪方式 (Track By)**，请指定跟踪方式。

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 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。

相关主题

全局规则阈值选项，第 2 页
配置层中的入侵规则
冲突和更改：网络分析和入侵策略

禁用全局阈值

如果要为特定规则的事件设置阈值而不是将阈值默认应用于每条规则，则可以在最高策略层禁用全局阈值。

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

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 点击导航面板中的**高级设置 (Advanced Settings)**。

步骤 4 点击**入侵规则阈值 (Intrusion Rule Thresholds)** 下的**全局规则阈值 (Global Rule Thresholding)** 旁边的**已禁用 (Disabled)**。

步骤 5 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。

相关主题

冲突和更改：网络分析和入侵策略
配置层中的入侵规则

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。