具体威胁检测

以下主题介绍如何在网络分析策略中使用预处理器检测特定威胁：

特定威胁检测简介

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

您可以在网络分析策略中使用若干预处理器检测对受监控网络的具体威胁（例如，后洞攻击、若干端口扫描类型和尝试通过大量流量淹没网络的基于速率的攻击）。在启用特定于预处理器的 GID 签名时，Web 上的网络分析策略将显示为已禁用。但是，预处理器将使用可用的默认设置来开启设备。

您还可以使用在入侵规则中配置的敏感数据检测来检测以非安全方式传输的敏感数字数据。

特定威胁检测的许可证要求

威胁防御 许可证

IPS

经典许可证

保护

特定威胁检测的要求和必备条件

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)

Back Orifice 检测

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

Firepower 系统提供用于检测是否存在 Back Orifice 程序的预处理器。此程序可用于获取对 Windows 主机的管理员访问权限。

Back Orifice 检测预处理器

Back Orifice 预处理器为 Back Orifice 神奇 cookie "*!*QWTY?"（位于数据包的前八个字节且使用 XOR 加密）分析 UDP 流量。

Back Orifice 预处理器具有配置页面，但没有配置选项。如果启用此预处理器，则还必须为其启用预处理器规则，以生成事件并在内联部署中丢弃攻击性数据包。

表 1: Back Orifice GID:SID

预处理器规则 GID:SID	说明
105:1	检测到 Back Orifice 流量
105:2	检测到 Back Orifice 客户端流量
105:3	检测到 Back Orifice 服务器流量

预处理器规则 GID:SID	说明
105:4	检测到 Back Orifice Snort 缓冲区攻击

检测 Back Orifice

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)**，然后点击**网络分析策略 (Network Analysis Policy)** 或**策略** > **访问控制** > **入侵**，然后点击 **网络分析策略**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

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

步骤 3 点击您要编辑的策略旁边的**编辑**（）。

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 4 点击导航面板中的**设置 (Settings)**。

步骤 5 如果**特定威胁检测 (Specific Threat Detection)** 下的 **Back Orifice 检测 (Back Orifice Detection)** 已禁用，请点击**已启用 (Enabled)**。

注释 Back Orifice 无用户可配置选项。

步骤 6 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

- 如果要生成事件并在内联部署中丢弃攻击性数据包，请启用 Back Orifice 检测规则 105:1、105:2、105:3 或 105:4 有关详细信息，请参阅入侵规则状态和Back Orifice 检测预处理器，第 2 页。
- 部署配置更改；请参阅 部署配置更改。

端口扫描检测

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

端口扫描是一种通常被攻击者用作攻击前奏的网络侦察形式。在端口扫描中，攻击者将特制的数据包发送到目标主机。通过检查主机响应时所用的数据包，攻击者通常可以直接或通过推理确定主机上的哪些端口是开放的，以及哪种应用协议正在这些端口上运行。

端口扫描本身不算是攻击。事实上，攻击者使用的一些端口扫描技术也可能会被网络上的合法用户使用。思科的端口扫描检测器旨在通过检测活动模式来帮助确定哪些端口扫描可能是恶意的。

注意 设备将跨内部资源进行负载均衡检查。如果端口扫描检测未按预期工作，您可能需要将灵敏度级别配置为**高 (High)**。

我们强烈建议您升级到 Snort 3 并使用版本 7.2.0 中引入的端口扫描功能。有关更多详细信息，请参阅 《Cisco Secure Firewall Management Center Snort 3 配置指南》 和 Snort 3 检查器参考。

端口扫描类型、协议和过滤的灵敏度级别

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

攻击者可能会使用多种方法来探测网络。他们通常使用不同的协议从目标主机获取不同的响应，以期即使某一种协议被阻止，也可以使用另一种。

表 2: 协议类型

协议 (Protocol)	说明
TCP	检测 TCP 探针，例如 SYN 扫描、ACK 扫描、TCP connect() 扫描和带异常标志组合（如 Xmas tree、FIN 和 NULL）的扫描
UDP	检测 UDP 探针，如零字节 UDP 数据包
ICMP	检测 ICMP 回应请求 (ping)
IP	检测 IP 协议扫描。这些扫描与 TCP 和 UDP 扫描不同，因为攻击者不是查找开放端口，而是尝试去发现目标主机支持哪些 IP 协议。

根据目标主机的数量、扫描主机的数量和扫描的端口数量，端口扫描通常分为四种类型。

表 3: 端口扫描类型

类型	说明
端口扫描检测	一对一端口扫描，在这种扫描中，攻击者使用一个或几个主机扫描单个目标主机上的多个端口。 一对一端口扫描具有如下特征： • 扫描主机的数量少 • 扫描单个主机 • 扫描的端口数量多 此选项检测 TCP、UDP 和 IP 端口扫描。
端口扫描	一对多端口清扫，在这种扫描中，攻击者使用一个或几个主机扫描多个目标主机上的单个端口。 端口清扫具有如下特征： • 扫描主机的数量少 • 扫描的主机数量多 • 扫描的唯一端口数量少 此选项检测 TCP、UDP、ICMP 和 IP 端口清扫。
诱骗端口扫描	一对一端口扫描，在这种攻击中，攻击者将伪造的源 IP 地址与真实的扫描 IP 地址混合在一起。 诱骗端口扫描具有如下特征： • 扫描主机的数量多 • 一次扫描的端口数量少 • 扫描的主机为一个（或数量少） 诱骗端口扫描选项检测 TCP、UDP 和 IP 协议端口扫描。

类型	说明
分布式端口扫描	多对一端口扫描，在这种攻击中，多个主机查询单个主机是否有开放端口。 分布式端口扫描具有如下特征： • 扫描主机的数量多 • 一次扫描的端口数量多 • 扫描的主机为一个（或数量少） 分布式端口扫描选项检测 TCP、UDP 和 IP 协议端口扫描。

端口扫描检测器所了解的关于探针的信息主要是基于查看探测主机的否定响应。例如，当 Web 客户端尝试连接到 Web 服务器时，客户端会使用端口 80/tcp 且可以依靠服务器将该端口打开。但是，当攻击者探测服务器时，攻击者事先并不知道该服务器是否提供 Web 服务。当端口扫描检测器看到否定响应（即，ICMP 不可达或 TCP RST 数据包）时，它会将该响应记录为潜在的端口扫描。当目标主机位于设备（例如，过滤否定响应的防火墙或路由器）的另一端时，这个过程更难以执行。在这种情况下，端口扫描检测器可以根据选择的灵敏度级别生成已过滤端口扫描事件。

表 *4:* 灵敏度级别

级别	说明
低	只检测目标主机的否定响应。选择此级别的灵敏度可抑制误报，但请记住，这样可能会遗漏某些类型的端口扫描（慢速扫描、过滤扫描）。 此级别使用最短的时间窗口进行端口扫描检测。
中等	根据主机的连接数量检测端口扫描，这意味着，可以检测过滤的端口扫描。但是，非常活跃的主机（例如网络地址转换器和代理）可能会生成误报。 请注意，可以将这些活跃主机的 IP 地址添加到**忽略已扫描项 (Ignore Scanned)** 字段以减少此类误报。 此级别使用较长的时间窗口进行端口扫描检测。
高	根据时间窗口检测端口扫描，这意味着，可以检测基于时间的端口扫描。但是，如果使用此选项，应通过在 **Ignore Scanned** 和 **Ignore Scanner** 字段中指定 IP 地址，随时间小心地调整检测器。 此级别使用更长的时间周期进行端口扫描检测。

端口扫描事件生成

当启用端口扫描检测时，必须启用生成器 ID (GID) 为 122 且 Snort ID (SID) 为 1 至 27 的规则，以便检测各种端口扫描和端口清扫。

注释 对于端口扫描连接检测器生成的事件，协议号设置为 255。由于默认情况下端口扫描没有特定协议与之关联，因此，互联网编号分配机构 (IANA) 未将协议号分配给它。IANA 指定 255 作为保留号码，因此，该号码用于端口扫描事件中以指明事件没有关联的协议。

表 *5:* 端口扫描检测 ***SID (GID 122)***

端口扫描类型	协议	灵敏度级别	预处理器规则 **SID**
端口扫描检测	TCP UDP ICMP IP	低 中等或高 低 中等或高 低 中等或高 低 中等或高	1 5 17 21 不生成事件。 不生成事件。 9 13
端口扫描	TCP UDP ICMP IP	低 中等或高 低 中等或高 低 中等或高 低 中等或高	3, 27 7 19 23 25 26 11 15
诱骗端口扫描	TCP UDP ICMP IP	低 中等或高 低 中等或高 低 中等或高 低 中等或高	2 6 18 22 不生成事件。 不生成事件。 10 14

端口扫描类型	协议	灵敏度级别	预处理器规则 SID
分布式端口扫描	TCP UDP ICMP IP	低 中等或高 低 中等或高 低 中等或高 低 中等或高	4 8 20 24 不生成事件。 不生成事件。 12 16

端口扫描事件数据包视图

启用随附的预处理器规则后，端口扫描检测器会生成入侵事件，可以像任何其他事件一样进行查看。但是，数据包视图上显示的信息不同于其他类型的入侵事件。

首先使用入侵事件视图钻取到端口扫描事件的数据包视图。请注意，不能下载端口扫描数据包，因为单个端口扫描事件是基于多个数据包；但是，端口扫描数据包视图提供了所有可用的数据包信息。

对于所有 IP 地址，可点击地址查看上下文菜单并选择 **whois** 以在 IP 地址上执行查找，或者选择 **View Host Profile** 以查看该主机的主机配置文件。

表 *6:* 端口扫描数据包视图

信息	说明
设备	检测事件的设备。
时间	事件发生的时间。
消息	预处理器生成的事件消息。
源 IP	扫描主机的 IP 地址。
目标 IP	被扫描主机的 IP 地址。
优先级计数	被扫描主机发出的否定响应（例如，TCP RST 和 ICMP 无法访问）的数量。否定响应的数量越多，优先级计数就越高。
连接计数	主机上的活动连接数量。此值对于基于连接的扫描（例如 TCP 和 IP）而言更准确。

信息	说明
IP 计数 (IP Count)	与被扫描主机联系的IP地址变化的次数。例如，如果第一个IP地址是10.1.1.1，第二个 IP 是 10.1.1.2，第三 IP 是 10.1.1.1，那么 IP 计数为 3。 此数字对于活跃的主机（例如代理和 DNS 服务器）而言不太准确。
扫描工具/已扫描 IP 范围 (Scanner/Scanned IP Range)	被扫描主机或扫描主机的IP地址范围，具体取决于扫描类型。对于端口清扫，此字段显示被扫描主机的 IP 范围。对于端口扫描，此字段显示扫描主机的 IP 范围。
端口/协议计数 (Port/Proto Count)	对于 TCP 和 UDP 端口扫描，是指正被扫描的端口变化的次数。例如，如果扫描的第一个端口是 80，扫描的第二个端口是 8080，扫描的第三个端口又是 80，那么端口计数为 3。 对于 IP 协议端口扫描，是指正用于连接至被扫描主机的协议变化的次数。
端口/协议范围 (Port/Proto Range)	对于 TCP 和 UDP 端口扫描，是指被扫描端口的范围。 对于 IP 协议端口扫描，是指已用于尝试连接至扫描的主机的 IP 协议号的范围。
开放端口 (Open Ports)	在被扫描主机上打开的 TCP 端口。此字段仅在端口扫描检测到一个或多个开放端口时显示。

配置端口扫描检测

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

端口扫描检测配置选项可用于精细调整端口扫描检测器如何报告扫描活动。

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。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)**，然后点击**网络分析策略 (Network Analysis Policy)** 或**策略** > **访问控制** > **入侵**，然后点击 **网络分析策略**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

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

步骤 3 点击您要编辑的策略旁边的**编辑**（ ）。

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 4 点击**设置**。

步骤 5 如果**特定威胁检测 (Specific Threat Detection)** 下的**端口扫描检测 (Portscan Detection)** 已禁用，请点击**已启用 (Enabled)**。

步骤 6 点击**端口扫描检测 (Portscan Detection)** 旁边的 **编辑**（  ）。

步骤 7 在**协议 (Protocol)** 字段中，指定要启用的协议。

注释 必须确保已启用 TCP 数据流处理以在 TCP 上检测扫描，并且确保已启用 UDP 流处理以在 UDP 上检测扫描。

步骤 8 在**扫描类型 (Scan Type)** 字段中，指定要检测的的端口扫描类型。

步骤 9 从**灵敏度级别 (Sensitivity Level)** 列表中选择级别；请参阅端口扫描类型、协议和过滤的灵敏度级别，第 4 页。

步骤 10 如果要监控特定主机的端口扫描活动迹象，请在**监视 IP (Watch IP)** 字段中输入主机 IP 地址。

可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。将此字段留空则监视所有网络流量。

步骤 11 如果要忽略作为扫描工具的主机，请在**忽略扫描工具 (Ignore Scanners)** 字段中输入主机 IP 地址。

可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。

步骤 12 如果要忽略作为扫描对象的主机，请在**忽略已扫描项 (Ignore Scanned)** 字段中输入主机 IP 地址。

可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。

提示 可使用**忽略扫描工具 (Ignore Scanners)** 和**忽略已扫描项 (Ignore Scanned)** 字段指示在网络上特别活跃的主机。可能需要随时间修改此主机列表。

步骤 13 如果要对中途恢复的会话中断监控，请清除**检测 Ack 扫描 (Detect Ack Scans)** 复选框。

注释 检测中途会话有助于识别ACK扫描，但可能会导致错误事件，特别是在含大流量和丢弃数据包的网络中。

步骤 14 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

- 如果希望端口扫描检测不同的端口检测和端口端口清扫，则请启用规则 122:1 至 122:27。有关详细信息，请参阅入侵规则状态和端口扫描事件生成，第 6 页。
- 部署配置更改；请参阅 部署配置更改。

基于速率的攻击防御

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

基于速率的攻击是取决于连接频率或攻击实施重复次数的攻击。可以使用基于速率的检测标准检测发生的基于速率的攻击，采取应对措施，在攻击停止后返回到常规检测设置。

可以将网络分析策略配置为包括基于速率的过滤器，这种过滤器可检测针对网络中主机的过多活动。可以在内联模式下部署的受管设备上使用此功能，以在指定时间内阻止基于速率的攻击，然后恢复为仅生成事件而不丢弃流量。

SYN 攻击防御选项有助于保护网络主机免受 SYN 泛洪攻击。可以根据在一段时间内看到的数据包数量保护单个主机或整个网络。如果设备采用被动部署，可以生成事件。如果设备采用内联部署，还可以丢弃恶意数据包。超时周期结束后，如果速率条件已停止，将会停止事件生成和数据包丢弃。

例如，您可以配置设置来允许来自任一 IP 地址的最大 SYN 数据包数，并阻止来自该 IP 地址的更多连接达 60 秒。

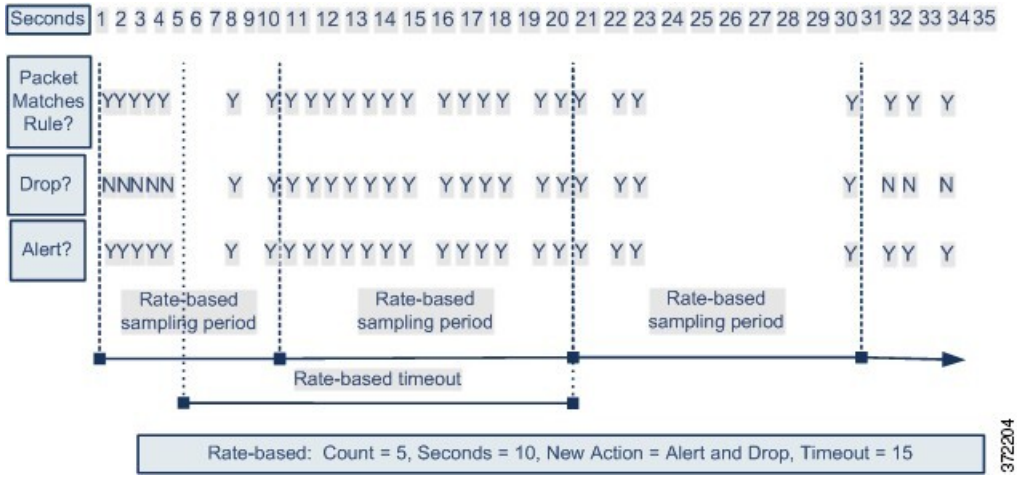
可以限制与网路上主机之间的 TCP/IP 连接，以防止拒绝服务 (DoS) 攻击或用户进行过多活动。当系统检测到与指定 IP 地址成功连接的配置数量或地址范围时，它会对额外连接生成事件。基于速率的事件生成继续进行，直到超时周期结束且未发生速率条件。在内联部署中，可以选择丢弃数据包，直到速率条件超时。

例如，您可以配置设置来允许来自任一 IP 地址的最多 10 个成功同时连接，并阻止来自该 IP 地址的更多连接达 60 秒。

注释 设备将跨内部资源进行负载均衡检查。在配置基于速率的攻击防御时，可以为每个源配置触发率，而不是每个设备。如果基于速率的攻击防御达不到预期，您可能需要降低触发率。如果用户在规定的时间间隔内发送过多的连接尝试，则会触发警报。因此，建议对规则进行速率限制。为了帮助确定正确的速率，请联系支持人员。

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。在采样速率地区阈值速率的情况下，新操作将恢复为仅在采样期完成后生成事件。



相关主题

动态入侵规则状态

基于速率的攻击防御示例

关键字 `detection_filter`、阈值和抑制功能提供了其他方式来过滤流量或系统生成的事件。可以单独使用基于速率的攻击防御，也可以将其与阈值、抑制功能或 `detection_filter` 关键字随意组合使用。

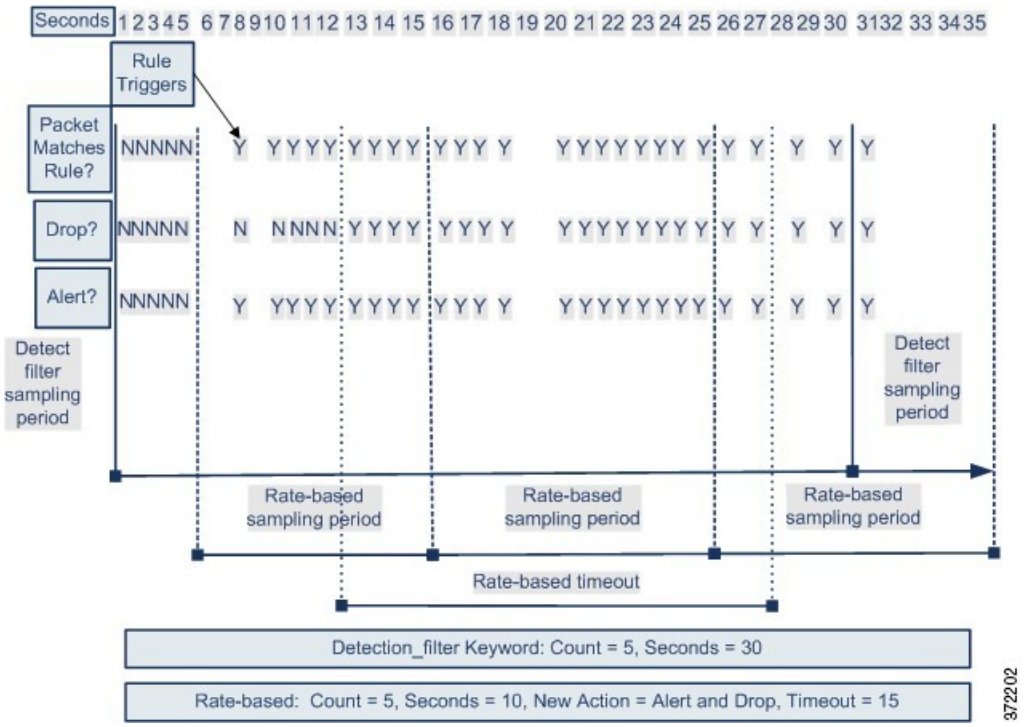
`detection_filter` 关键字、阈值或抑制以及基于速率的条件可能全都适用于同一流量。为规则启用抑制功能后，系统会为指定 IP 地址抑制事件，即使发生基于速率的变化。

detection_filter 关键字示例

下面的示例显示了一个攻击者尝试发动暴力登录攻击。重复尝试查找密码会触发还包含 `detection_filter` 关键字且计数设置为 5 的规则。此规则已配置基于速率的攻击防御。如果在 10 秒内出现五次规则匹配，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) 并保持 20 秒。

如图所示，与规则匹配的前五个数据包不会生成事件，因为在速率超过 `detection_filter` 关键字所指示的速率之前规则不会触发。规则触发后，事件通知开始，但基于速率的标准在再通过五个数据包之前不会触发新操作“丢弃并生成事件”(Drop and Generate Events)。

如果符合基于速率的标准，将会生成事件并会丢弃数据包，直到基于速率的超时周期结束且速率低于阈值。20 秒之后，基于速率的操作超时。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。由于采样的速率高于之前采样周期的阈值速率，因此发生超时时，基于速率的操作会继续。



请注意，虽然示例未进行描述，但可以将“丢弃并生成事件”(Drop and Generate Events) 规则状态与 `detection_filter` 关键字结合使用，以在规则的匹配速率达到指定速率时开始丢弃流量。确定是否为规则配置基于速率的设置时，请考虑将规则设置为“丢弃并生成事件”(Drop and Generate Events) 和包含 `detection_filter` 关键字是否会获得相同的结果，或者是否要在入侵策略中管理速率和超时设置。

相关主题

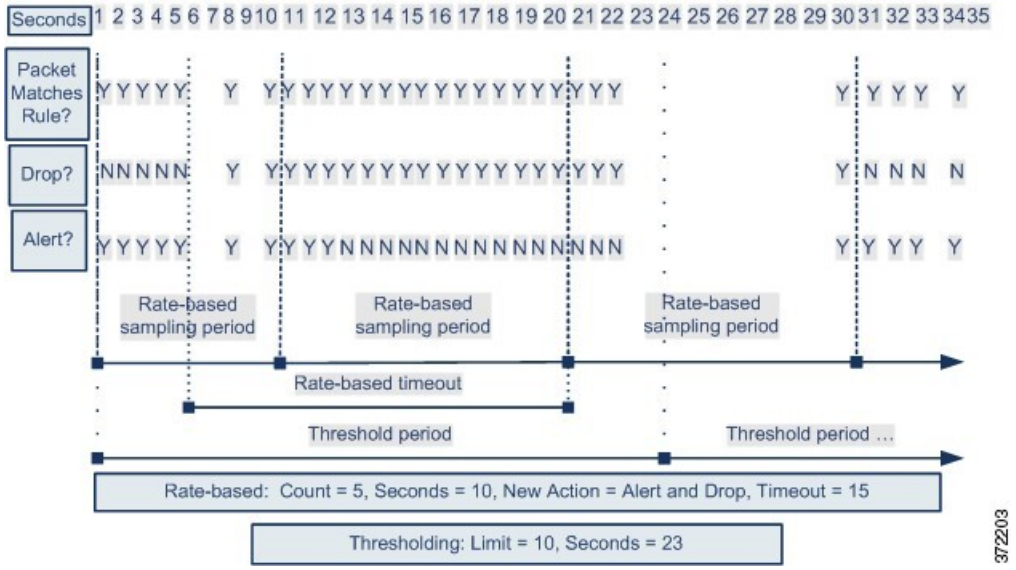
入侵规则状态

动态规则状态阈值或抑制示例

下面的示例显示了一个攻击者尝试发动暴力登录攻击。反复尝试查找密码将触发一条已经配置了基于速率的攻击预防的规则。如果在10秒内出现五次规则攻击，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) 并保持 15 秒。此外，一个限制阈值还会将该规则可生成的事件数限制为 23 秒内 10 个事件。

如图所示，该规则将为前五个匹配数据包生成事件。五个数据包之后，基于速率的标准会触发新操作“丢弃并生成事件”(Drop and Generate Events)，对于接下来的五个数据包，规则会生成事件且系统会丢弃数据包。第十个数据包之后，已达到极限阈值，因此，对于剩余的数据包，系统不会生成事件，但会丢弃数据包。

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采样期的阈值速率，则新操作将继续。在采样速率地区阈值速率的情况下，新操作将恢复为仅在采样期完成后生成事件。



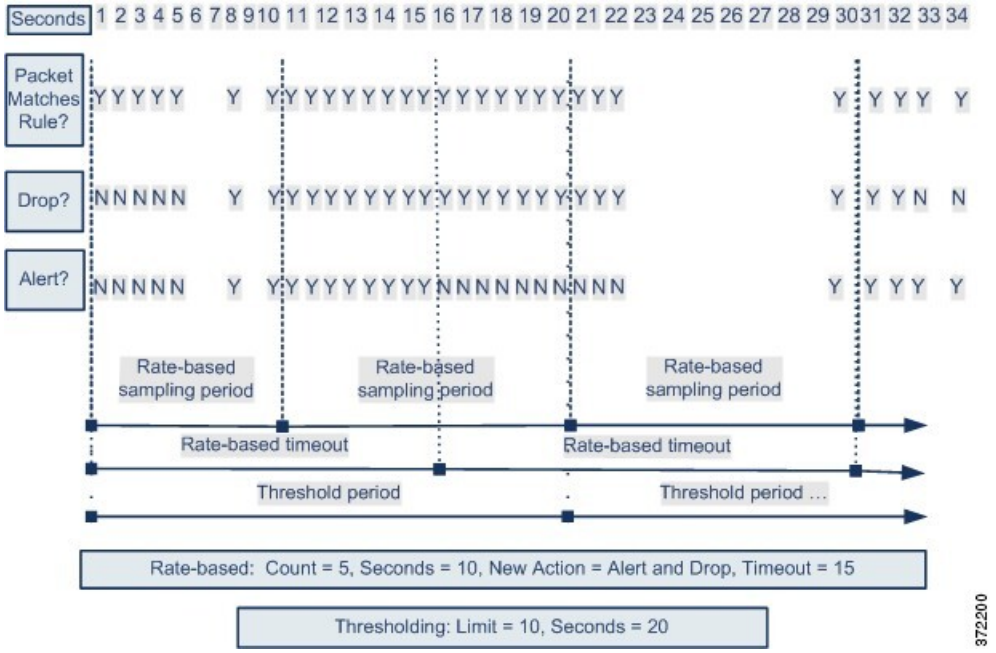
请注意，虽然本例中未显示，但如果在达到阈值后因基于速率的标准而触发新操作，系统会生成一个事件以指示操作变化。因此，例如，对于第 14 个数据包，如果达到极限阈值 10，系统停止生成事件且操作从从“生成事件”(Generate Events) 更改为“丢弃并生成事件”(Drop and Generate Events)，系统会生成第十一个事件以指示操作变化。

整个策略基于速率的检测和阈值或抑制示例

以下示例显示了尝试对网络中的主机进行拒绝服务 (DoS) 攻击的攻击者。许多来自相同源的同步主机连接会触发整个策略的“控制同步连接”设置。如果在10秒内一个源有五个连接，设置会生成事件并丢弃恶意流量。此外，全局极限阈值会在 20 秒内将所有规则或设置可生成的事件数量限制为 10。

如图所示，整个策略的设置会为前十个匹配数据包生成事件并丢弃流量。第十个数据包之后，已达到极限阈值，因此，对于剩余的数据包，不会生成事件，但会丢弃数据包。

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。如果采样的速率高于当前或之前采样周期的阈值速率，生成事件和丢弃流量这两种基于速率的操作将会继续。基于速率的操作只在采样周期结束后停止，在此情况下采样的速率低于阈值速率。



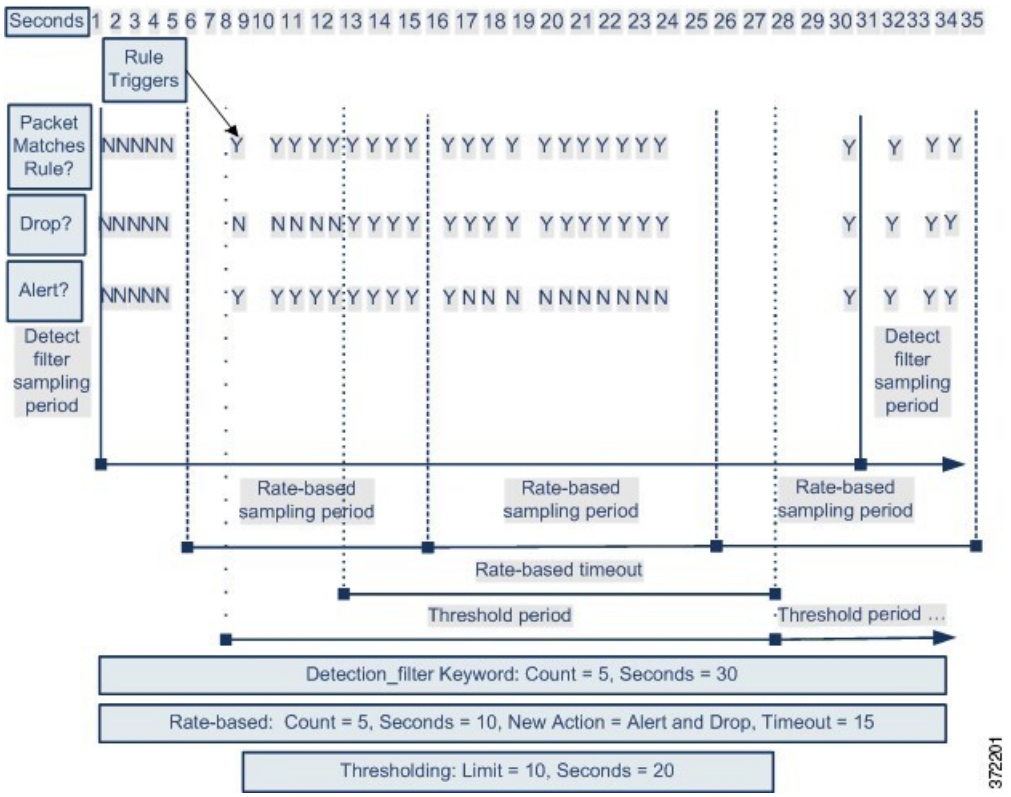
请注意，虽然本例中未显示，但如果在达到阈值后因基于速率的标准而触发新操作，系统会生成一个事件以指示操作变化。因此，例如，对于第 14 个数据包，如果达到极限阈值 10，系统停止生成事件且操作更改为 Drop and Generate Events，系统会生成第十一个事件以指示操作变化。

使用多种过滤方法进行基于速率的检测示例

以下示例显示了尝试强行登录的攻击者，并描述了 `detection_filter` 关键字、基于速率的过滤和阈值功能交互的情况。重复尝试查找密码会触发包括 `detection_filter` 关键字且计数设置为 5 的规则。此规则还具有基于速率的攻击防御设置，如果在 15 秒内出现五次规则匹配，该设置会将规则属性更改为“丢弃并生成事件”(Drop and Generate Events) 并保持 30 秒。此外，极限阈值会在 30 秒内将规则限为 10 个事件。

如图所示，与规则匹配的前五个数据包不会产生事件通知，因为在速率超过 `detection_filter` 关键字所指示的速率之前规则不会触发。规则触发后，事件通知开始，但基于速率的标准在再通过五个数据包之前不会触发新操作“丢弃并生成事件”(Drop and Generate Events)。如果符合基于速率的标准，系统会为数据包 11 至 15 生成事件并丢弃数据包。第十五个数据包之后，已达到极限阈值，因此，对于剩余的数据包，系统不会生成事件，但会丢弃数据包。

请注意，基于速率的超时后，数据包仍会在随后的基于速率的采样周期内丢弃。由于采样的速率高于之前采样周期的阈值速率，新操作将会继续。



基于速率的攻击防御选项和配置

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。基于速率的攻击通常具有以下其中一种特征：

- 任何包含与网络主机之间过多不完整连接的流量，表示 SYN 泛洪攻击
- 任何包含与网络主机之间过多完整连接的流量，表示 TCP/IP 连接泛洪攻击
- 在流向特定目标 IP 地址或来自一个或多个特定源 IP 地址的流量中规则匹配过多
- 所有流量中某个特定规则的匹配过多

在网络分析策略中，您可以为整个策略配置 SYN 泛洪或 TCP/IP 连接泛洪检测；在入侵策略中，您可以为单独的入侵或预处理器规则设置基于速率的过滤器。请注意，不能手动将基于速率的过滤器添加到 GID 135 规则或修改其规则状态。GID 为 135 的规则使用客户端作为源值，使用服务器作为目标值。

在启用 **SYN 攻击防御 (SYN Attack Prevention)** 后，如果超过定义的速率条件，则会触发规则 135:1。

在启用 **控制同时连接 (Control Simultaneous Connections)** 后，如果超过定义的速率条件，则触发规则 135:2，如果会话关闭或超时，则触发规则 135:3。

注释 设备将跨内部资源进行负载均衡检查。在配置基于速率的攻击防御时，可以为每个源配置触发率，而不是每个设备。如果基于速率的攻击防御达不到预期，您可能需要降低触发率。如果用户在规定的时间间隔内发送过多的连接尝试，则会触发警报。因此，建议对规则进行速率限制。为了帮助确定正确的速率，请联系支持人员。

每个基于速率的过滤器都包含下列几个组成部分：

- 网络地址名称（适用于整个策略或基于规则的源或目标设置）
- 规则的匹配速率，配置为特定秒数内的规则匹配项数量
- 超过该速率时要执行的新操作

  为整个策略设置基于速率的设置时，系统会在其检测到基于速率的攻击时生成事件，并且可以在内联部署中丢弃流量。为具体规则设置基于速率的操作时，有三个可用的操作：Generate Events、Drop and Generate Event 和 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。当超时时段结束后，如果速率低于阈值，则规则的操作会恢复到最初为该规则配置的操作。对于整个策略的设置，操作会恢复到流量匹配的每个规则的操作；如果不匹配任何规则，操作会停止。

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。在没有基于速率的配置的情况下，设置为“生成事件”(Generate Events) 的规则会创建事件，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。但是，如果在策略级别设置基于速率的过滤器，则可以在指定时段内生成事件或生成事件并丢弃包含过多SYN数据包或SYN/ACK 交互的流量。

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操作相冲突时，系统会实施第一个基于速率的过滤器的操作。同样，如果对整个策略设置的基于速率的过滤器与对具体规则设置的基于速率的过滤器相冲突，前者优先。

相关主题

从规则页面设置动态规则状态

基于速率的攻击防御、检测过滤和阈值或抑制

关键字 `detection_filter` 可防止触发规则，直至在指定时间内出现规则匹配项的阈值数量为止。当规则包括关键字 `detection_filter` 时，系统将跟踪每个超时期间传入的匹配规则中模式的数据包数

量。系统可统计来自特定源 IP 地址或特定目标 IP 地址的规则匹配项的数量。在速率超出规则中的速率后，系统将开始发送该规则的事件通知。

可以使用阈值和抑制来减少过多的事件，方法是限制规则、源或目标的事件通知数量或者抑制该规则的所有通知。您还可以配置适用于没有首要特定阈值的每个规则的全局规则阈值。

如果对规则应用抑制，则系统会为所有适用的 IP 地址抑制该规则的事件通知，即使由于策略范围或规则特定的基于速率的设置而发生基于速率的操作更改也如此。

相关主题

入侵事件阈值
入侵策略抑制配置
全局规则阈值基础知识

配置基于速率的攻击防御

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

可以在策略级别配置基于速率的攻击防御以阻止SYN泛洪攻击，也可以阻止来自特定源或到达特定目标的过多连接。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)**，然后点击**网络分析策略 (Network Analysis Policy)** 或**策略** > **访问控制** > **入侵**，然后点击 **网络分析策略**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

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

步骤 3 点击您要编辑的策略旁边的**编辑**（）。

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 4 点击**设置**。

步骤 5 如果**特定威胁检测 (Specific Threat Detection)** 下的**基于速率的攻击防御 (Rate-Based Attack Prevention)** 已禁用，请点击**已启用 (Enabled)**。

步骤 6 点击**基于速率的攻击防御 (Rate-Based Attack Prevention)** 旁边的 **编辑**（）。

步骤 7 您有两种选择：

- 要防止旨在对主机发起泛洪攻击的不完整连接，请点击 **SYN Attack Prevention** 下的 **Add**。
- 要防止过多连接，请点击 **Control Simultaneous Connections** 下的 **Add**。

步骤 8 指定要跟踪流量的方式：

- 要跟踪来自特定源或一系列源的所有流量，请从**跟踪方式(Track By)**下拉列表中选择**源 (Source)**，然后在**网络 (Network)** 字段中输入单个 IP 地址或地址块。
- 要跟踪到达特定目标或一系列目标的所有流量，请从**跟踪方式 (Track By)** 下拉列表中选择**目标 (Destination)**，然后在**网络 (Network)** 字段中输入单个 IP 地址或地址块。

注释
- 请勿在网络字段中输入 IP 地址 0.0.0.0/0 来监控所有子网或 IP。系统不支持使用此 IP 地址（通常用于识别所有子网或 IP）进行基于速率的攻击预防。
- 系统会单独跟踪**网络 (Network)** 字段中包含的每个 IP 地址的流量。来自超过所配置速率的 IP 地址的流量会带来仅为该 IP 地址生成的事件。例如，进行网络设置时，可将源 CIDR 块设置为 `10.1.0.0/16` 并将系统配置为在有十个同步连接打开时生成事件。如果 10.1.4.21 有八个连接打开，10.1.5.10 有六个连接打开，则系统不会生成事件，因为这两个源地址的打开连接均未达到触发数量。但是，如果 10.1.4.21 有十一个同步连接打开，系统只会为来自 10.1.4.21 的连接生成事件。

  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。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

步骤 9 指定速率跟踪设置的触发速率：

- 对于 SYN 攻击配置，在**速率 (Rate)** 字段中输入每个秒数的 SYN 数据包数量。
- 对于同步连接配置，在**计数 (Count)** 字段中输入连接数量。

设备将跨内部资源进行负载均衡检查。在配置基于速率的攻击防御时，可以为每个源配置触发率，而不是每个设备。如果基于速率的攻击防御达不到预期，您可能需要降低触发率。如果用户在规定的时间间隔内发送过多的连接尝试，则会触发警报。因此，建议对规则进行速率限制。为了帮助确定正确的速率，请联系支持人员。

步骤 10 要丢弃与基于速率的攻击防御设置匹配的数据包，请选中**丢弃 (Drop)** 复选框。

步骤 11 在**超时 (Timeout)** 字段中输入时间段，在该时间段结束后将会停止生成针对具有 SYN 的匹配模式或同步连接的流量的事件（如适用，丢弃）。

注意 设置较高的超时值可能会完全阻止连接到内联部署中的某个主机。

步骤 12 点击 **OK**。

步骤 13 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。