入侵事件的外部警报

以下主题介绍如何配置入侵事件的外部警报：

关于入侵规则的外部警报

外部入侵事件通知可帮助进行关键系统监控：

- SNMP - 按照入侵策略配置并从受管设备发送。您可以按照入侵规则启用 SNMP 警报。
- 系统日志 - 按照入侵策略配置并从受管设备发送。当您在入侵策略中启用系统日志警报时，可以为该策略中的每个规则将其打开。
- 邮件 - 跨所有入侵策略配置并从 Cisco Secure Firewall Management Center发送。您可以按照入侵规则启用邮件警报，并限制警报的长度和频率。

请记住，如果您配置了入侵事件抑制或阈值，系统可能不会每次在规则触发时都生成入侵事件（因此可能不会发送警报）。

在多域部署中，可以配置任何域中的外部警报。在祖先域中，系统会为后代域中的入侵事件生成通知。

注释 Cisco Secure Firewall Management Center还使用 SNMP、系统日志和邮件警报响应来发送不同类型的外部警报；请参阅Cisco Secure Firewall Management Center 警报响应。系统不使用警报响应来根据单个入侵事件发送警报。

相关主题

入侵策略中的入侵事件通知过滤器

入侵事件外部警报的许可证要求

威胁防御 许可证

IPS

经典许可证

保护

入侵事件外部警报的要求和前提条件

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)

配置入侵事件的 SNMP 警报

在入侵策略中启用外部 SNMP 警报后，可以配置各个规则以便在触发规则时发送 SNMP 警报。这些警报是从受管设备发送的。

过程

步骤 1 在入侵策略编辑器的导航窗格中，点击**高级设置**。

步骤 2 确保 **SNMP 警报**是**已启用**状态，然后点击**编辑**。
页面底部消息会识别包含配置的入侵策略层。

步骤 3 选择 **SNMP 版本**，然后按入侵 SNMP 警报选项，第 3 页中所述指定配置选项。

步骤 4 在导航窗格中，点击**规则**。

步骤 5 在规则窗格中，选择要设置 SNMP 警报的规则，然后选择**警报** > **添加 SNMP 警报**。

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，请选择**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 《Cisco Secure Firewall Management Center 设备配置指南》 。

入侵 SNMP 警报选项

如果网络管理系统要求使用管理信息库文件 (MIB)，您可以从Cisco Secure Firewall Management Center 中获取，具体位置为 `/etc/sf/DCEALERT.MIB`。

SNMP v2 选项

选项	说明
陷阱类型	警报中出现的 IP 地址所用到的陷阱类型。 如果网络管理系统正常显现 INET_IPV4 地址类型，则选择**二进制形式**选项。否则，应选择**字符串形式**。例如，HP Openview 需要选择**字符串形式**。
陷阱服务器 (Trap Server)	收到 SNMP 陷阱通知的服务器。 可指定单一 IP 地址或主机名。
社区字符串 (Community String)	群体名称。

SNMP v3 选项

受管设备使用引擎 ID 值对 SNMPv3 警报进行编码。要解码警报，您的 SNMP 服务器需要此值，即发送设备的管理接口 IP 地址的十六进制版本，并附加“01”。

例如，如果发送 SNMP 警报的设备的管理接口 IP 地址是 172.16.1.50，则引擎 ID 值为 0xAC10013201。

选项	说明
陷阱类型	警报中出现的 IP 地址所用到的陷阱类型。 如果网络管理系统正常显现 INET_IPV4 地址类型，则选择**二进制形式**选项。否则，应选择**字符串形式**。例如，HP Openview 需要选择**字符串形式**。

选项	说明
陷阱服务器 (Trap Server)	收到 SNMP 陷阱通知的服务器。 可指定单一 IP 地址或主机名。
身份验证密码 (Authentication Password)	身份验证所需的密码。SNMP v3 使用消息摘要 5 (MD5) 散列函数或安全散列算法 (SHA) 散列函数进行密码加密，具体取决于配置。 一旦指定身份验证密码，身份验证即可启用。
私有密码 (Private Password)	用于保护隐私的 SNMP 密钥。SNMP v3 采用数据加密标准 (DES) 分组密码对密码进行加密。输入 SNMP v3 密码后，初始配置期间的密码会以明文显示，但以加密格式保存。 如果指定私有密码，则隐私被启用，且还必须指定身份验证密码。
用户名	SNMP 用户名。

为入侵事件配置系统日志警报

在入侵策略中启用系统日志警报后，系统将在受管设备自身或者一台或多台外部主机上向系统日志发送所有入侵事件。如果指定了外部主机，系统将从受管设备发送系统日志警报。

过程

步骤 1 在入侵策略编辑器的导航窗格中，点击**高级设置 (Advanced Settings)**。

步骤 2 请确保**系统日志警报 (Syslog Alerting)** 为**已启用 (Enabled)**，然后点击**编辑 (Edit)**。
页面底部消息会识别包含配置的入侵策略层。**系统日志警报**页面添加在**高级设置**下。

步骤 3 输入您要发送系统日志警报的**日志记录主机**的 IP 地址。

如果您将**日志记录主机**字段留空，则系统将从关联访问控制策略中的“日志记录”获取日志记录主机详细信息。

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 4 选择**设施**和**严重性**级别，如入侵系统日志警报的设施和严重性，第 5 页中所述。

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，请选择**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 《Cisco Secure Firewall Management Center 设备配置指南》。

入侵系统日志警报的设施和严重性

受管设备可以使用特定的设施和**严重性**将入侵事件作为系统日志警报发送，以便日志主机可以对警报进行分类。设施指定生成警报的子系统。这些设施和**严重性**值不会出现在实际的系统日志消息中。

根据您的环境选择有意义的值。本地配置文件（如基于 UNIX 的日志记录主机上的 syslog.conf）可能指示将哪些设施保存到哪些日志文件中。

系统日志警报设施

设施	说明
AUTH	与安全和授权关联的消息。
AUTHPRIV	与安全和授权关联的访问受限的消息。在很多系统上，这些消息会转发至一个安全文件。
控制台	警报消息。
CRON	时钟守护程序生成的消息。
DAEMON	系统后台守护程序生成的消息。
FTP	FTP 后台守护程序生成的消息。
KERN	内核生成的消息。很多系统会在这些消息出现后将其传送至控制台打印。
LOCAL0-LOCAL7	内部进程生成的消息。
LPR	打印子系统生成的消息。
邮件	邮件系统生成的消息。
NEWS	网络新闻子系统生成的消息。
SYSLOG	系统日志后台守护程序生成的消息。
USER	用户级进程生成的消息。
UUCP	UUCP 子系统生成的消息。

系统日志警报严重性

级别	说明
EMERG	紧急状况，向所有用户广播
ALERT	需要立即更正的状况
CRIT	严重的状况

级别	说明
ERR	错误状况
WARNING	警告消息
通知	并未出现错误，但需引起注意的状况
INFO	参考性消息
DEBUG	包含调试信息的消息

配置入侵事件的邮件警报

如果启用了入侵邮件警报，无论哪个受管设备或入侵策略检测到入侵，系统都可以在生成入侵事件时发送邮件。这些警报从 Cisco Secure Firewall Management Center发送。

开始之前

- 配置邮件主机以接收邮件警报；请参阅配置邮件中继主机和通知地址。
- 确保 Cisco Secure Firewall Management Center可以反转解析自己的 IP 地址。

过程

步骤 1 选择**策略** > **操作** > **警报**。

步骤 2 点击 **入侵邮件**。

步骤 3 如入侵邮件警报选项，第 6 页中所述，选择警报选项，包括要警报的入侵规则或规则组。

步骤 4 点击**保存 (Save)**。

入侵邮件警报选项

On/Off

启用或禁用入侵邮件警报。

注释 启用它将为所有规则启用警报，除非选择单个规则。

发件人/收件人地址

邮件发件人和收件人。您可以指定一个以逗号分隔的收件人列表。

最大警报数和频率

Cisco Secure Firewall Management Center将按时间间隔发送（**频率**）的邮件警报最大数（**最大警报数**）。

Coalesce Alerts

通过将具有相同源 IP 和规则 ID 的警报分组来减少发送的警报数。

Summary Output

启用简要警报，适用于文本受限的设备。简要警报包含以下内容：

- 时间戳
- 协议
- 源和目标 IP 和端口
- 消息
- 同一个源 IP 生成的入侵事件数量

例如：`2011-05-18 10:35:10 10.1.1.100 icmp 10.10.10.1:8 -> 10.2.1.3:0 snort_decoder: Unknown Datagram decoding problem! (116:108)`

如果启用**摘要输出**，还应考虑启用**组合警报**。您可能还希望降低**最大警报数**，以避免超过文本消息限制。

时区

警报时间戳的时区。

Email Alerting on Specific Rules Configuration

允许您选择要在其中设置邮件警报的规则。

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。