使用事件操作过滤器，调整错误肯定预防的IPS

目录

简介

使用IPS设备管理器(IDM)或IPS管理器Express (IME)，本文提供要求的步骤为了调整错误肯定预防的入侵防御系统(IPS)。调整在IPS的错误肯定由呼叫事件操作过滤器的功能达到(EAF)。

开始使用前

要求

本文读者应该有思科IPS的知识。

使用的组件

本文档中的信息没有根据特定的硬件和软件版本。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

了解EAFs

EAFs主要为错误肯定调整配置。EAF提供能力安排一个特定的签名不采取流量的一子集的所需的动作。

EAFs是有用的在要求满足多个条件的情况，例如：

- 签名x不采取流量一希望的子网的行动y。
- 签名x采取其他流量的行动y。

EAFs是有用的与良性触发签名打交道。

配置

示例：错误肯定事件：来自和到已知可信的主机的流量的签名1300触发。

注意： 这是示例只用于示范目的。如果是不确定的是否一个特定的事件由于签名触发良性，请与进一步分析的思科技术支持联系。

注意： 关于IPS签名的更多信息参考的思科入侵防御系统签名。

完成这些步骤：

1. 检查默认操作签名(1300，在本例中) EAF需要配置。默认操作签名1300包括**导致警报**并且**拒绝连接线型**。
2. 识别此签名不应该射击的主机。例如，您不希望签名为来自一委托子网的流量射击，例如10.1.1.1-10.1.1.254。
3. 创建在步骤2:描述的标准的EAF从IDM/IME，请去**Configuration>策略> IPS策略**。点击**事件操作过滤器**选项卡。在此选项卡下，请单击**添加**。此窗口显示：配置多种字段例如**名称**，**签名ID**、**攻击者IP**等等。在**操作减去**字段右边单击图标为了打开编辑操作对话框。在此窗口，您能指定您不希望IPS执行的签名操作。**注意：** 为了正确地选择您要减去的签名操作，您请需要了解默认签名操作正如Step1所描述。在本例中，我们选择**导致警报**并且**拒绝连接线型**。IPS不会采取这些行动，如果来自10.1.1.1-10.1.1.254的流量的1300签名触发。对于其他流量，**Produce警报的**默认签名操作和**拒绝线型连接**将应用。在您选择后请导致警报并且丢弃数据包线型，您将看到这些操作在底部的EAF屏幕填充：点击OK键，然后**应用**为了保存更改。

对于事件操作过滤器的配置使用CLI，参考在配置指南页的IPS命令行界面部分。从相应的配置指南，请单击**配置事件操作规则**，并且“配置的事件操作搜索过滤”。

相关信息

- 技术支持和文档 - Cisco Systems