Cisco Secure IPS -除了假善意告警

Contents

Introduction

本文描述假善意告警排除Cisco Secure入侵防御系统(IPS)的。

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

本文的信息根据Cisco Secure入侵防御系统(IPS)版本7.0和Cisco IPS管理器Express 7.0。

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

错误肯定和错误否定告警

当信息包一个特定信息包或顺序匹配已知攻击配置文件的特性在Cisco Secure IPS签名时，定义的Cisco Secure IPS触发警报。重要IPS签名设计准则是使错误肯定和错误否定告警减到最小出现时间

。

假善意告警(良性触发器)发生，当IPS报告某一良性活动如有恶意。这要求人为干预诊断事件。很大数量的假善意告警能极大排泄资源，并且要求的专门化的技能分析他们是昂贵和难查找。

当IPS不发现并且报告实际恶意活动，假攻击发生。此的后果可以是灾难的，并且必须不断地更新签名，当发现新的检测安全漏洞代码和删改技术。使假攻击减到最小牺牲假善意告警更高的出现时间产生一非常高优先权，有时。

由于IPS使用发现恶意活动签名的本质，完全地排除假善意告警和负的是几乎不可能的，无需严重降低IPS的效果或严重打乱组织的计算基础设施(例如主机和网络)。定制的调整，当IPS配置时使假善意告警减到最小。需要定期重新调节，当计算环境更改时(例如，当新的系统和应用程序被实施)时。Cisco Secure IPS提供在稳定操作期间，能使假善意告警减到最小的一个灵活的调整的功能。

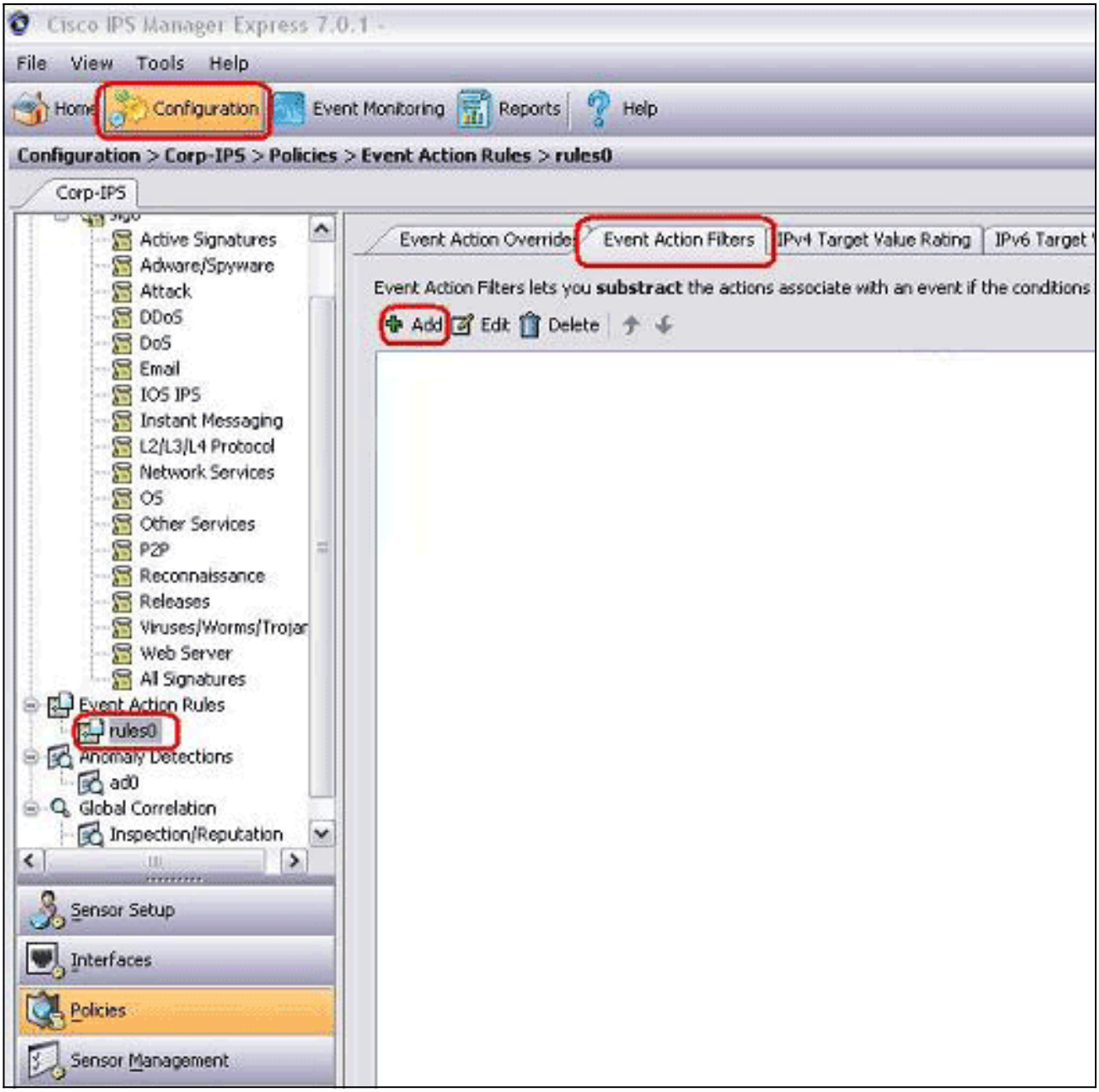
Cisco Secure IPS排除机制

Cisco Secure IPS提供功能排除一个特定签名从或到一台特定主机或网络地址。被排除的签名不生成告警图标或日志记录，当他们从通过此机制特别地被屏蔽的主机或网络时被触发。例如，网络管理位置也许通过运行查验清扫进行网络发现，触发与响应签名(签名ID 2100)的ICMP网络清除。如果排除签名，您不必须分析警报和删除它，在网络发现过程运行时候。

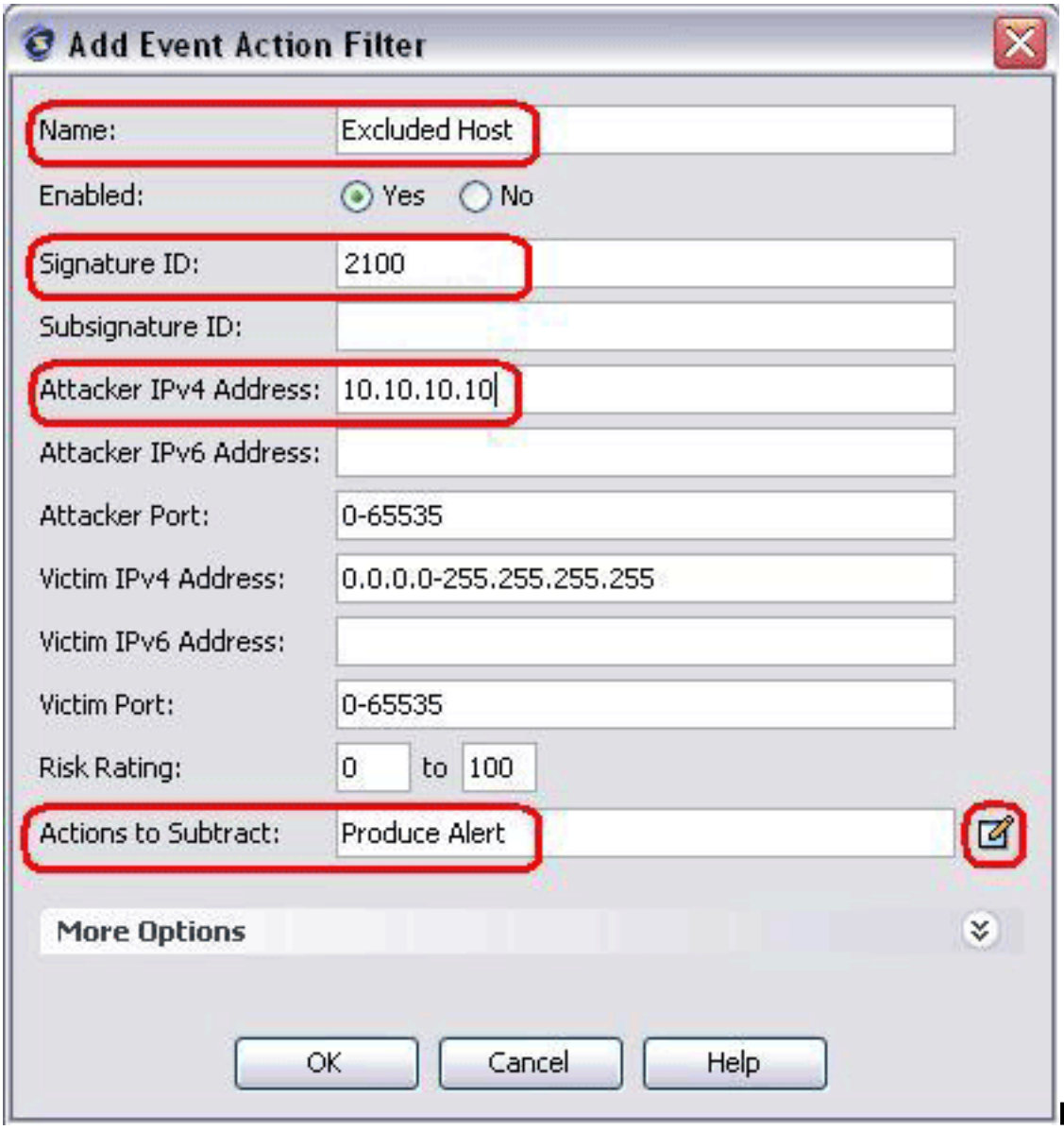
屏蔽主机

完成这些步骤为了从生成一个特定签名告警屏蔽一台特定主机(IP原地址)：

1. 选择**Configuration> Corp IPS >策略>事件操作规定> rules0**，并且点击**事件操作过滤器**选项。



2. 单击 **Add**。
3. 键入过滤器名称、签名ID、攻击者的IPv4地址和动作减去在适当的域，然后点击OK键。



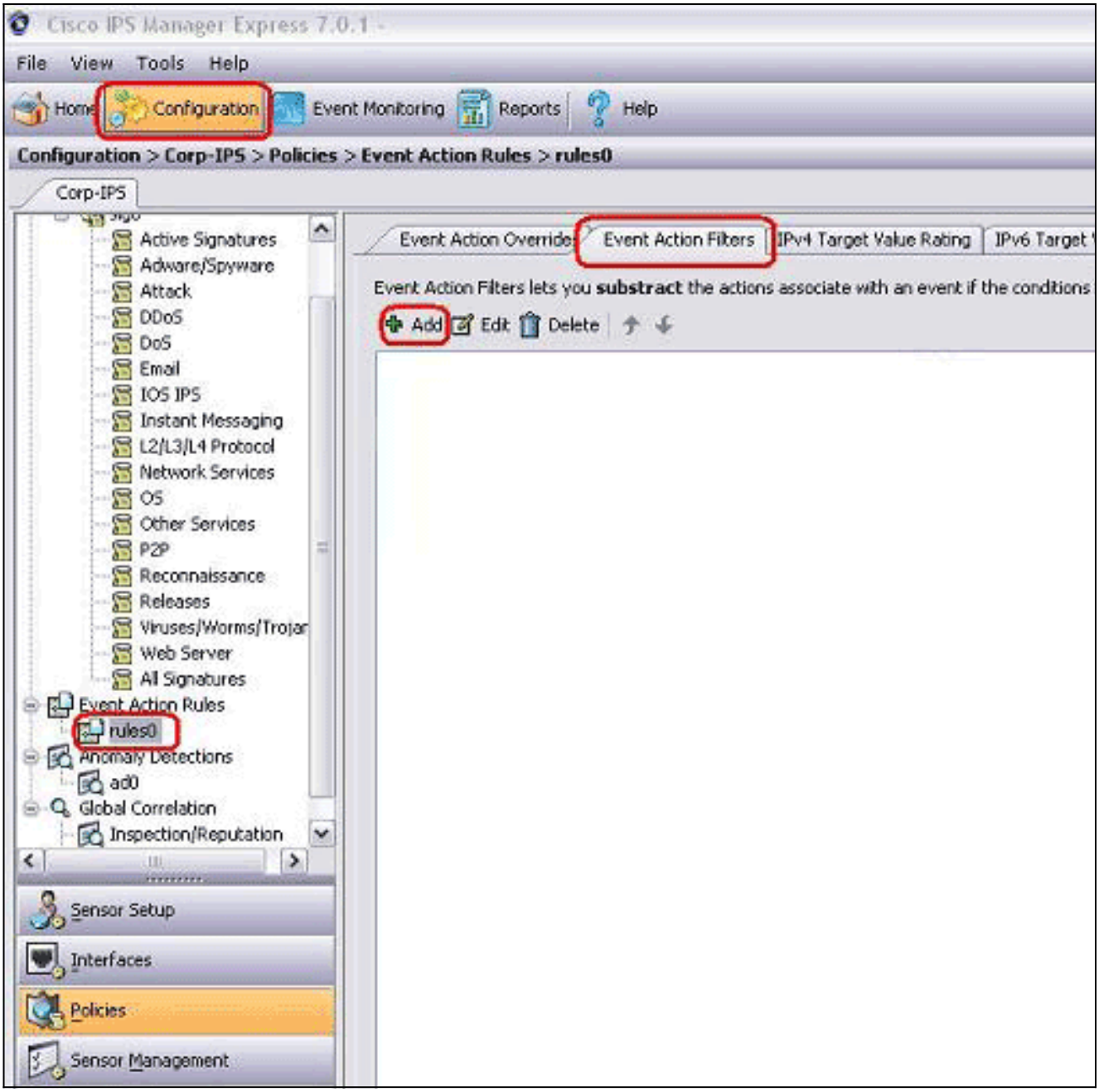
Note: 如果需要从不同的网络屏蔽多个IP地址，您能使用逗号作为分隔符。然而，如果使用一个逗号，请在逗号以后避免句尾空格;否则，您也许收到错误。**Note:** 另外，您在事件变量选项能使用被定义的变量。当在多台事件操作过滤器时，必须重复同一值这些变量是有用的。您必须使用美元的符号($)作为前缀到变量。变量可以是这些格式之一：充分的IP地址;例如， 10.77.23.23。IP地址的范围;例如， 10.9.2.10-10.9.2.155。套IP地址的范围;例如， 172.16.33.15-172.16.33.100,192.168.100.1-192.168.100.11。

屏蔽网络

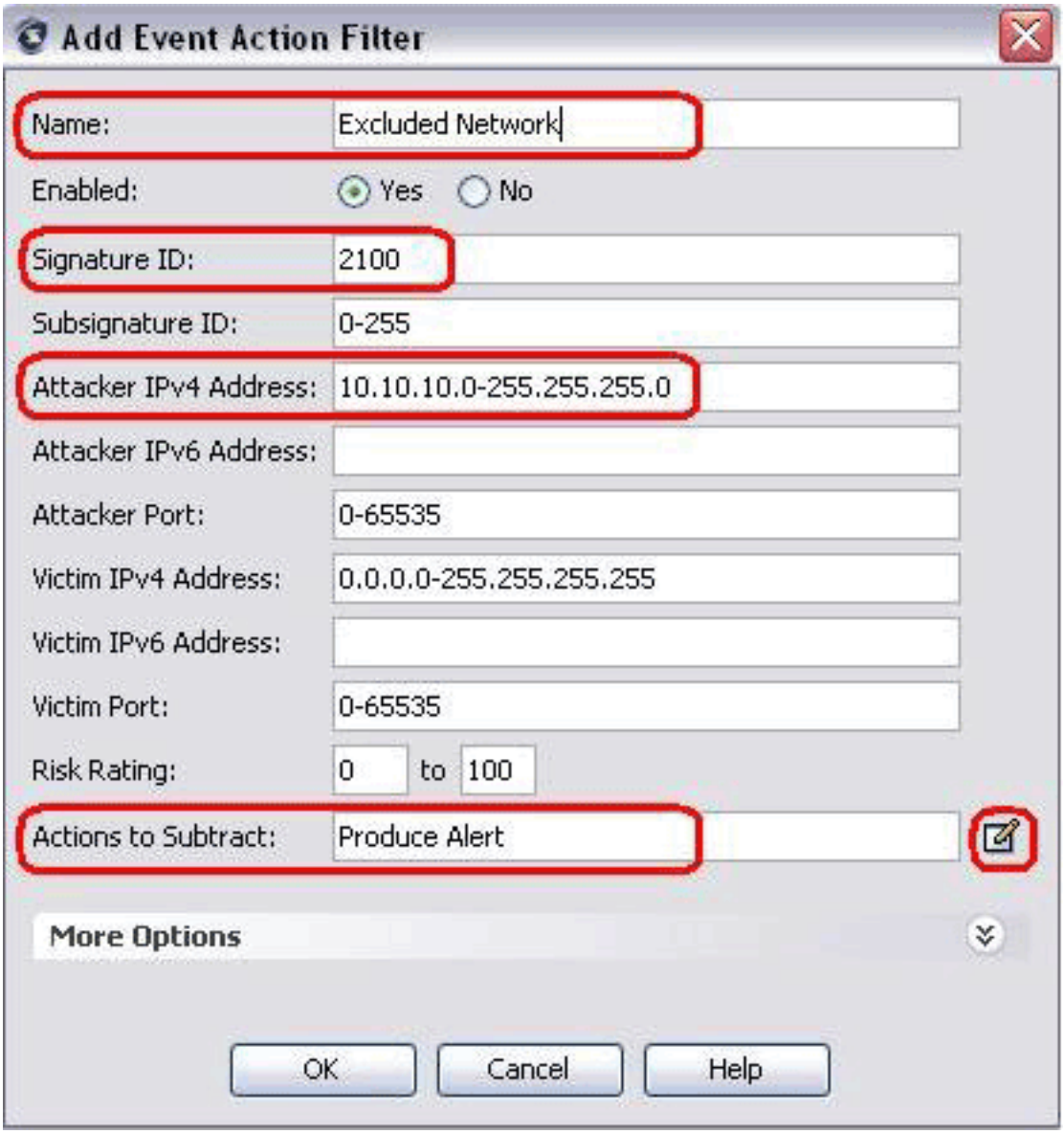
事件操作过滤器也排除特定签名射击根据源或目的地网络地址的警报。

完成这些步骤为了从生成一个特定签名告警屏蔽网络：

1. 点击**事件操作过滤器**选项。



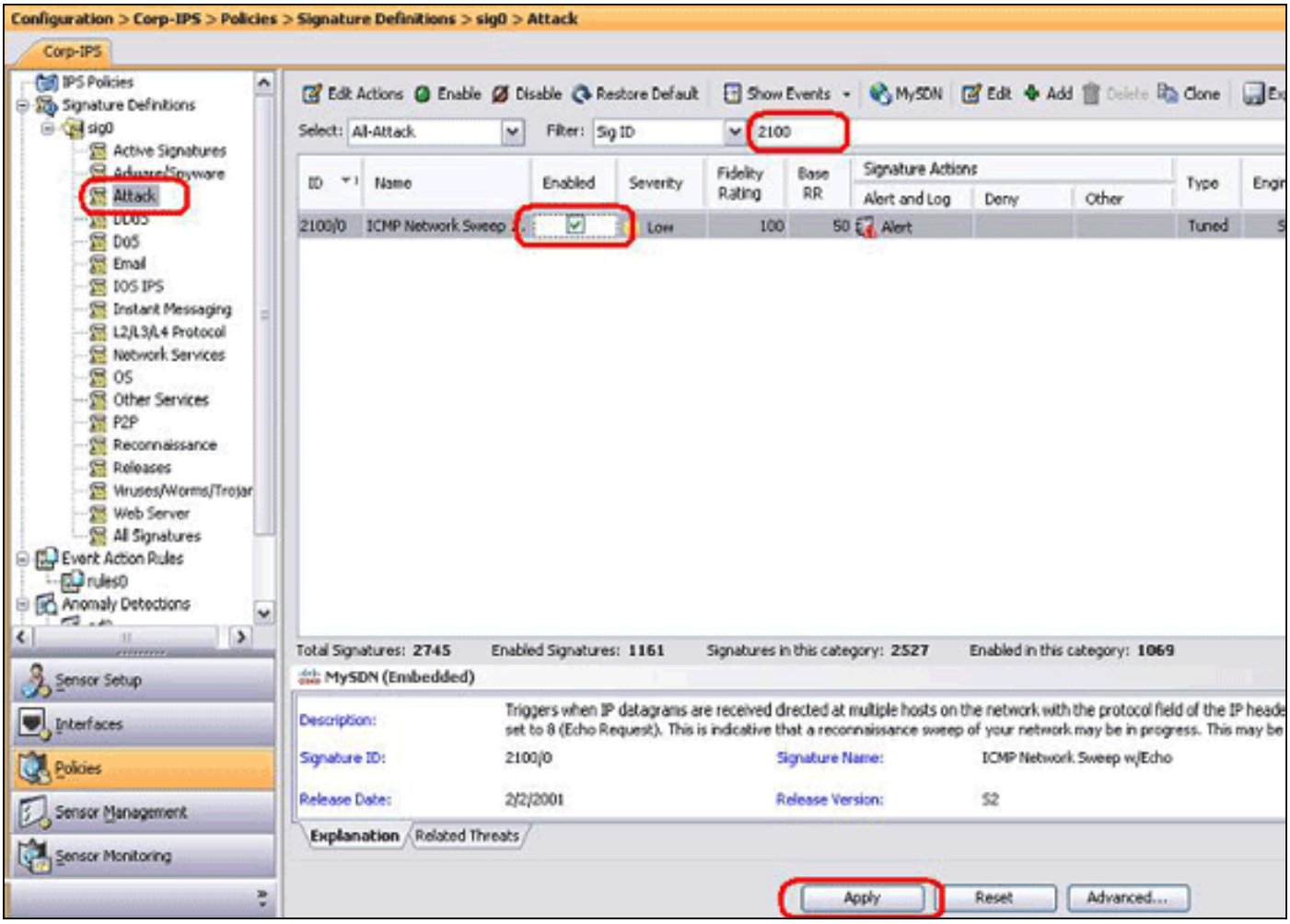
2. 单击 **Add**。
3. 键入过滤器名称、签名ID、网络地址与子网掩码和动作减去在适当的域，然后点击OK键。



全局请禁用签名

您也许要禁用从在任何时间警报的一个签名。为了enable (event)，功能失效，和退休签名，完成这些步骤：

1. 使用一个帐户有管理员或运算符权限，登陆对IME。
2. 选择**Configuration> sensor_name >策略>签名定义> sig0 >所有签名**。
3. 为了找出签名，从过滤器下拉列表请选择一个排序的选项。例如，如果搜索ICMP网络清除签名，请选择**所有签名**在sig0下，然后由签名ID搜索或命名。sig0面刷新并且显示匹配您排序的标准仅的那些签名。
4. 为了enable (event)或禁用一个现有的签名，选择签名，并且完成这些步骤：查看Enabled列确定签名的状态。是启用的签名有被检查的复选框。为了enable (event)是失效的签名，检查**Enabled复选框**。为了禁用是启用的签名，请不选定**Enabled复选框**。为了退休一个或更多签名，请选择签名，用鼠标右键单击和然后点击**更改状态对>退休**。
5. 点击**适用**为了应用您的更改和保存修改过的配置。



Related Information

- 销售结尾Cisco Secure IDS导向器的
- Cisco安全入侵检测支持页
- Technical Support & Documentation - Cisco Systems