

Cisco Secure IPS -除了假善意告警

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[错误肯定和错误否定警告](#)

[Cisco Secure IPS排除机制](#)

[屏蔽主机](#)

[屏蔽网络](#)

[全局请禁用签名](#)

[相关信息](#)

简介

本文描述假善意告警排除Cisco Secure入侵防御系统(IPS)的。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

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

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始(默认)配置。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息,请参阅 [Cisco 技术提示规则](#)。

错误肯定和错误否定警告

当数据包一个给的数据包或顺序匹配已知攻击配置文件特性在Cisco Secure IPS签名时,定义的Cisco Secure IPS触发报警。关键IPS签名设计准则是最小化错误肯定和错误否定警告出现。

错误肯定(良性触发)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。很大数量的错误肯定能极大排泄资源，并且要求的专门化技能分析他们是昂贵和难查找。

当IPS不检测并且报告实际恶意活动，假攻击发生。此的结果可以是灾难的，并且必须不断地更新签名如新建的检测安全漏洞代码和删改技术已发现。最小化假攻击牺牲错误肯定更高的出现给一非常高优先权，有时。

由于IPS使用检测恶意活动签名的本质，完全排除错误肯定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)。调整的Customized，当IPS部署时最小化错误肯定。定期重新调节要求，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，能最小化错误肯定的一个灵活调整的功能。

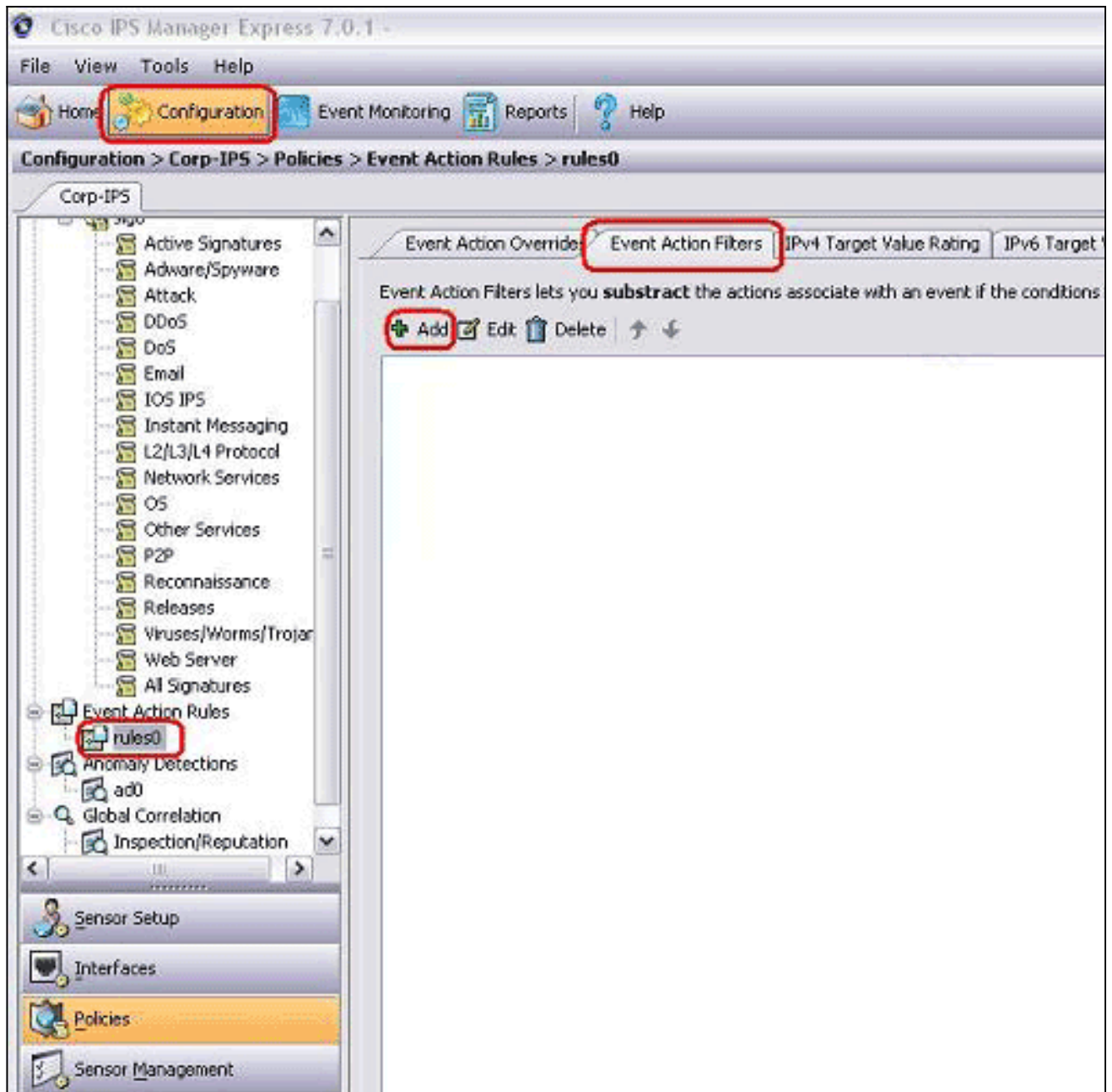
[Cisco Secure IPS排除机制](#)

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。不包括签名不生成告警图标也不记录记录，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，网络管理站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，您不必须分析报警和删除它，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(源IP地址)：

1. 选择Configuration>公司IPS >策略>事件操作规定> rules0，并且点击事件操作过滤器选项卡。



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

Add Event Action Filter

Name: Excluded Host

Enabled: Yes No

Signature ID: 2100

Subsignature ID:

Attacker IPv4 Address: 10.10.10.10

Attacker IPv6 Address:

Attacker Port: 0-65535

Victim IPv4 Address: 0.0.0.0-255.255.255.255

Victim IPv6 Address:

Victim Port: 0-65535

Risk Rating: 0 to 100

Actions to Subtract: Produce Alert

More Options

OK Cancel Help

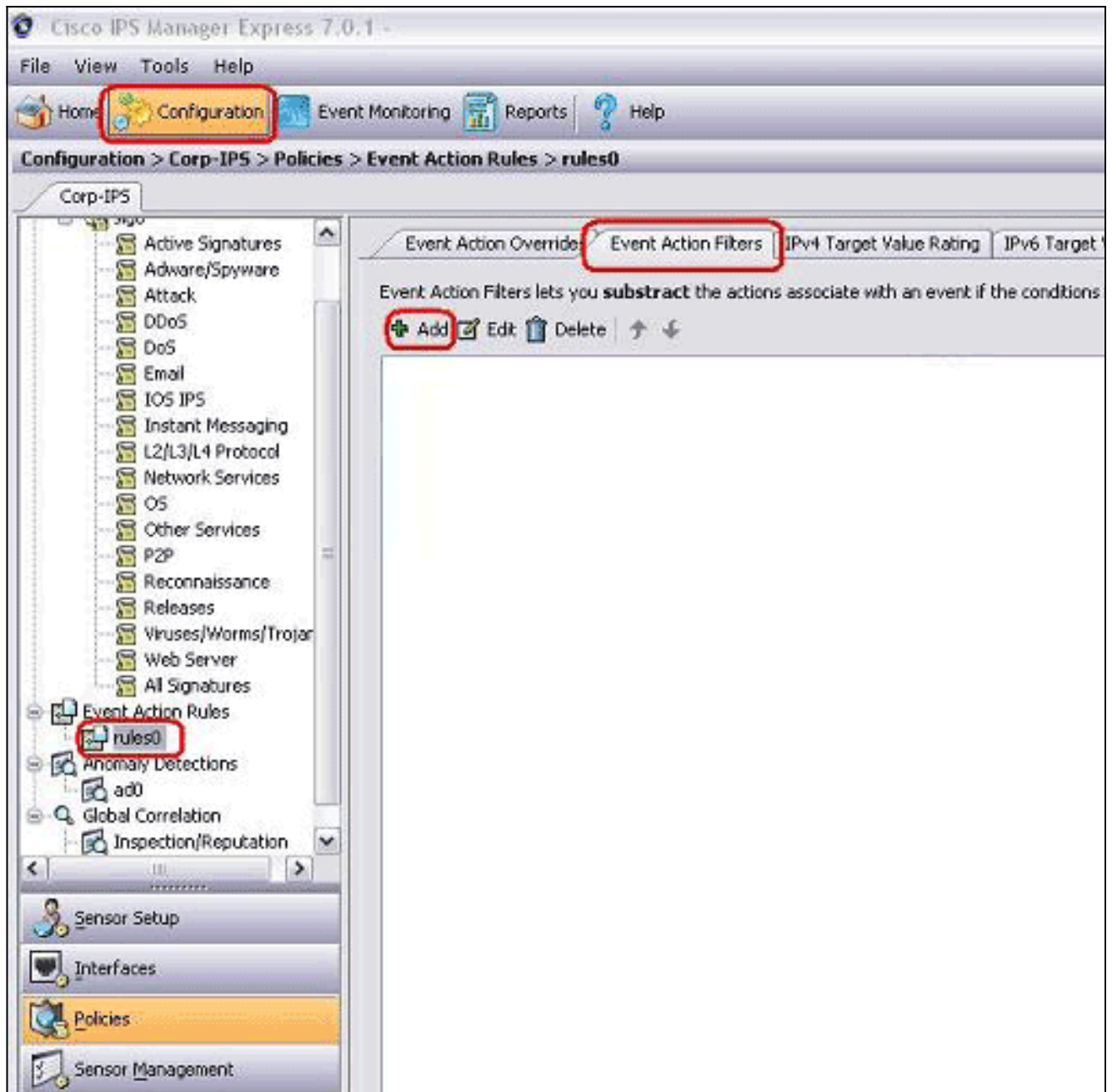
注意：如果需
要从不同的网络屏蔽多个IP地址，您能使用逗号作为分隔符。然而，如果使用一个逗号，请在
逗号以后避免句尾空格；否则，您也许收到错误。**注意：**另外，您在事件变量选项卡能使用定
义的变量。当在多个事件操作过滤器时，必须重复同一个值这些变量是有用的。您必须使用美
元的符号(\$)作为前缀到变量。变量可以是这些格式之一：全双工IP地址；例如，10.77.23.23。
IP地址范围；例如，10.9.2.10-10.9.2.155。套IP地址范围；例如，172.16.33.15-
172.16.33.100,192.168.100.1-192.168.100.11。

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报警。

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**选项卡。



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操作在适当的域减去，然后点击OK键。

Add Event Action Filter

Name: Excluded Network

Enabled: Yes No

Signature ID: 2100

Subsignature ID: 0-255

Attacker IPv4 Address: 10.10.10.0-255.255.255.0

Attacker IPv6 Address:

Attacker Port: 0-65535

Victim IPv4 Address: 0.0.0.0-255.255.255.255

Victim IPv6 Address:

Victim Port: 0-65535

Risk Rating: 0 to 100

Actions to Subtract: Produce Alert

More Options

OK Cancel Help

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。为了启用，禁用和退休签名，请完成这些步骤：

1. 使用一个帐户有管理员或操作员权限，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，请从过滤器下拉列表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或名称搜索。sig0窗格刷新并且显示匹配您排序的标准仅的那些签名。
4. 为了启用或禁用一个现有签名，请选择签名，并且完成这些步骤：查看Enabled列确定签名的状态。启用的签名有被检查的复选框。为了启用禁用的签名，请检查**Enabled复选框**。为了禁用启用的签名，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单击**崔凡吉莱状态对>退休了**。
5. 单击**应用**为了应用您的更改和保存已修订配置。

Configuration > Corp-IPS > Policies > Signature Definitions > sig0 > Attack

Corp-IPS

IPS Policies
Signature Definitions
sig0
Active Signatures
Adware/Spyware
Attack
DDOS
DoS
Email
IOS IPS
Instant Messaging
L2/L3/L4 Protocol
Network Services
OS
Other Services
P2P
Reconnaissance
Releases
Viruses/Worms/Trojan
Web Server
All Signatures

Event Action Rules
rules0
Anomaly Detections

Sensor Setup
Interfaces
Policies
Sensor Management
Sensor Monitoring

Edit Actions Enable Disable Restore Default Show Events MySDN Edit Add Delete Clone Ex

Select: All-Attack Filter: Sig ID 2100

ID	Name	Enabled	Severity	Fidelity Rating	Base RR	Signature Actions			Type	Engn
						Alert and Log	Deny	Other		
2100 0	ICMP Network Sweep	<input checked="" type="checkbox"/>	Low	100	50	Alert			Tuned	S

Total Signatures: 2745 Enabled Signatures: 1161 Signatures in this category: 2527 Enabled in this category: 1069

MySDN (Embedded)

Description: Triggers when IP datagrams are received directed at multiple hosts on the network with the protocol field of the IP header set to 8 (Echo Request). This is indicative that a reconnaissance sweep of your network may be in progress. This may be

Signature ID: 2100|0 Signature Name: ICMP Network Sweep w/Echo

Release Date: 2/2/2001 Release Version: S2

Explanation / Related Threats

Apply Reset Advanced...

相关信息

- [Cisco Secure IDS导向器的销售终止](#)
- [Cisco安全入侵检测支持页](#)
- [技术支持和文档 - Cisco Systems](#)