IPS 5.x和以后：使用CLI和IDM调整有事件操作过滤器的签名

目录

简介

本文描述如何调整与事件操作过滤器的签名在思科入侵防御系统(IPS)有命令行界面(CLI)和IDS服务管理器的(IDM)。

先决条件

要求

本文假设，思科IPS安装并且适当地运作。

使用的组件

本文档中的信息根据运行软件版本5.0及以上版本的Cisco 4200系列IDS/IPS设备。

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。

事件操作过滤器

了解事件操作过滤器

当排好序的列表和您能上上下下移动过滤器在列表，事件操作过滤器处理。

过滤器让传感器进行某些操作以回应事件，无需要求传感器进行所有操作或删除整个事件。过滤器工作在操作旁边删除从事件。从事件删除所有操作的过滤器其效果相当于消耗事件。

注意： 当您过滤清除签名时，思科建议您不过滤目的地址。如果有多个目的地地址，只有最后一个地址用于匹配过滤器。

您能配置事件操作过滤器从事件取消特定操作或丢弃一个整个事件和由传感器防止进一步处理。您能该使用事件操作的变量您定义对您的过滤器的组地址。关于关于怎样的步骤配置事件操作变量，请参阅添加，编辑和删除事件操作变量部分。

注意： 您必须加序言变量与美元的符号($)为了表明您使用一变量而不是字符串。否则，您收到Bad。

事件操作过滤器配置使用CLI

完成这些步骤为了配置事件操作过滤器：

1. 使用具有管理员权限的帐户登录 CLI。
2. 输入事件操作规则从属方式：
   ```
   sensor#configure terminal
   sensor(config)#service event-action-rules rules1
   sensor(config-eve)#
   ```
3. 创建过滤器名称：
   ```
   sensor(config-eve)#filters insert name1 begin
   ```

   请使用**name1，name2**，等等为了命名您的事件操作过滤器。请使用**开始|末端|非激活|以前|在**关键字为了指定后您要插入过滤器的地方。
4. 指定此过滤器的值：指定签名ID范围：
   ```
   sensor(config-eve-fil)#signature-id-range 1000-1005
   ```

   默认是900到65535。指定签名ID范围：
   ```
   sensor(config-eve-fil)#subsignature-id-range 1-5
   ```

   默认是0到255。指定攻击者地址范围：
   ```
   sensor(config-eve-fil)#attacker-address-range 10.89.10.10-10.89.10.23
   ```

   默认是0.0.0.0对255.255.255.255。指定受害者地址范围：
   ```
   sensor(config-eve-fil)#victim-address-range 192.56.10.1-192.56.10.255
   ```

   默认是0.0.0.0对255.255.255.255。指定受害者端口范围：
   ```
   sensor(config-eve-fil)#victim-port-range 0-434
   ```

   默认是0到65535。指定OS相关性：
   ```
   sensor(config-eve-fil)#os-relevance relevant
   ```

   默认是0到100。指定风险等级范围。
   ```
   sensor(config-eve-fil)#risk-rating-range 85-100
   ```

默认是0到100。指定操作删除：

```
sensor(config-eve-fil)#actions-to-remove reset-tcp-connection
```

如果过滤一拒绝操作，设置百分比拒绝您希望的操作：

```
sensor(config-eve-fil)#deny-attacker-percentage 90
```

默认是100。指明过滤器的状态对禁用或启用。

```
sensor(config-eve-fil)#filter-item-status {enabled | disabled}
```

默认启用。指定在匹配参数的终止。

```
sensor(config-eve-fil)#stop-on-match {true | false}
```

如果此项目配比，**真**告诉传感器停止处理过滤器。**错误**告诉传感器继续处理过滤器，即使此项目配比。添加您要使用为了解释此过滤器的任何意见：

```
sensor(config-eve-fil)#user-comment NEW FILTER
```

5. 验证过滤器的设置：

```
sensor(config-eve-fil)#show settings
 NAME: name1

   ----------------------------------------------

      signature-id-range: 1000-10005 default: 900-65535

      subsignature-id-range: 1-5 default: 0-255

      attacker-address-range: 10.89.10.10-10.89.10.23 default: 0.0.0.0-255.255.255.255

      victim-address-range: 192.56.10.1-192.56.10.255 default: 0.0.0.0-255.255.255.255

      attacker-port-range: 0-65535 <defaulted>

      victim-port-range: 1-343 default: 0-65535

      risk-rating-range: 85-100 default: 0-100

      actions-to-remove: reset-tcp-connection default:

      deny-attacker-percentage: 90 default: 100

      filter-item-status: Enabled default: Enabled

      stop-on-match: True default: False

      user-comment: NEW FILTER default:

      os-relevance: relevant default: relevant|not-relevant|unknown

   ----------------------------------------------

senor(config-eve-fil)#
```

6. 为了编辑一个现有过滤器：

```
sensor(config-eve)#filters edit name1
```

7. 欲知更多信息，编辑参数并且通过4l请参阅步骤4a。
8. 为了上上下下移动一个过滤器在过滤器列表：

```
sensor(config-eve-fil)#exit
sensor(config-eve)#filters move name5 before name1
```

9. 验证您移动过滤器：

```
sensor(config-eve-fil)#exit
sensor(config-eve)#show settings

 ----------------------------------------------

   filters (min: 0, max: 4096, current: 5 - 4 active, 1 inactive)

   ----------------------------------------------

   ACTIVE list-contents

   ----------------------------------------------

      NAME: name5

      ----------------------------------------------

         signature-id-range: 900-65535 <defaulted>

         subsignature-id-range: 0-255 <defaulted>

         attacker-address-range: 0.0.0.0-255.255.255.255 <defaulted>

         victim-address-range: 0.0.0.0-255.255.255.255 <defaulted>

         attacker-port-range: 0-65535 <defaulted>

         victim-port-range: 0-65535 <defaulted>

         risk-rating-range: 0-100 <defaulted>

         actions-to-remove: <defaulted>

         filter-item-status: Enabled <defaulted>

         stop-on-match: False <defaulted>

         user-comment: <defaulted>

      ----------------------------------------------

      ----------------------------------------------

      NAME: name1

      ----------------------------------------------

         signature-id-range: 900-65535 <defaulted>

         subsignature-id-range: 0-255 <defaulted>

         attacker-address-range: 0.0.0.0-255.255.255.255 <defaulted>

         victim-address-range: 0.0.0.0-255.255.255.255 <defaulted>

         attacker-port-range: 0-65535 <defaulted>

         victim-port-range: 0-65535 <defaulted>

         risk-rating-range: 0-100 <defaulted>
```

```
        actions-to-remove: <defaulted>
        filter-item-status: Enabled <defaulted>
        stop-on-match: False <defaulted>
        user-comment: <defaulted>
      ------------------------------------------------
      ------------------------------------------------
      NAME: name2
      ------------------------------------------------
        signature-id-range: 900-65535 <defaulted>
        subsignature-id-range: 0-255 <defaulted>
        attacker-address-range: 0.0.0.0-255.255.255.255 <defaulted>
        victim-address-range: 0.0.0.0-255.255.255.255 <defaulted>
        attacker-port-range: 0-65535 <defaulted>
        victim-port-range: 0-65535 <defaulted>
        risk-rating-range: 0-100 <defaulted>
        actions-to-remove: <defaulted>
        filter-item-status: Enabled <defaulted>
        stop-on-match: False <defaulted>
        user-comment: <defaulted>
      ------------------------------------------------
      ------------------------------------------------
    ------------------------------------------------
    INACTIVE list-contents
    ------------------------------------------------
  ------------------------------------------------
  sensor(config-eve)#
```

10. 为了移动过滤器向非激活列表：

```
sensor(config-eve)#filters move name1 inactive
```

11. 验证过滤器移动向非激活列表：

```
sensor(config-eve-fil)#exit
sensor(config-eve)#show settings
    ------------------------------------------------
    INACTIVE list-contents
    ------------------------------------------------
```

```
        ------------------------------------------------

        NAME: name1

        ------------------------------------------------

           signature-id-range: 900-65535 <defaulted>

           subsignature-id-range: 0-255 <defaulted>

           attacker-address-range: 0.0.0.0-255.255.255.255 <defaulted>

           victim-address-range: 0.0.0.0-255.255.255.255 <defaulted>

           attacker-port-range: 0-65535 <defaulted>

           victim-port-range: 0-65535 <defaulted>

           risk-rating-range: 0-100 <defaulted>

           actions-to-remove: <defaulted>

           filter-item-status: Enabled <defaulted>

           stop-on-match: False <defaulted>

           user-comment: <defaulted>

        ------------------------------------------------

        ------------------------------------------------

    sensor(config-eve)#
```

12. 退出事件操作规则从属方式：

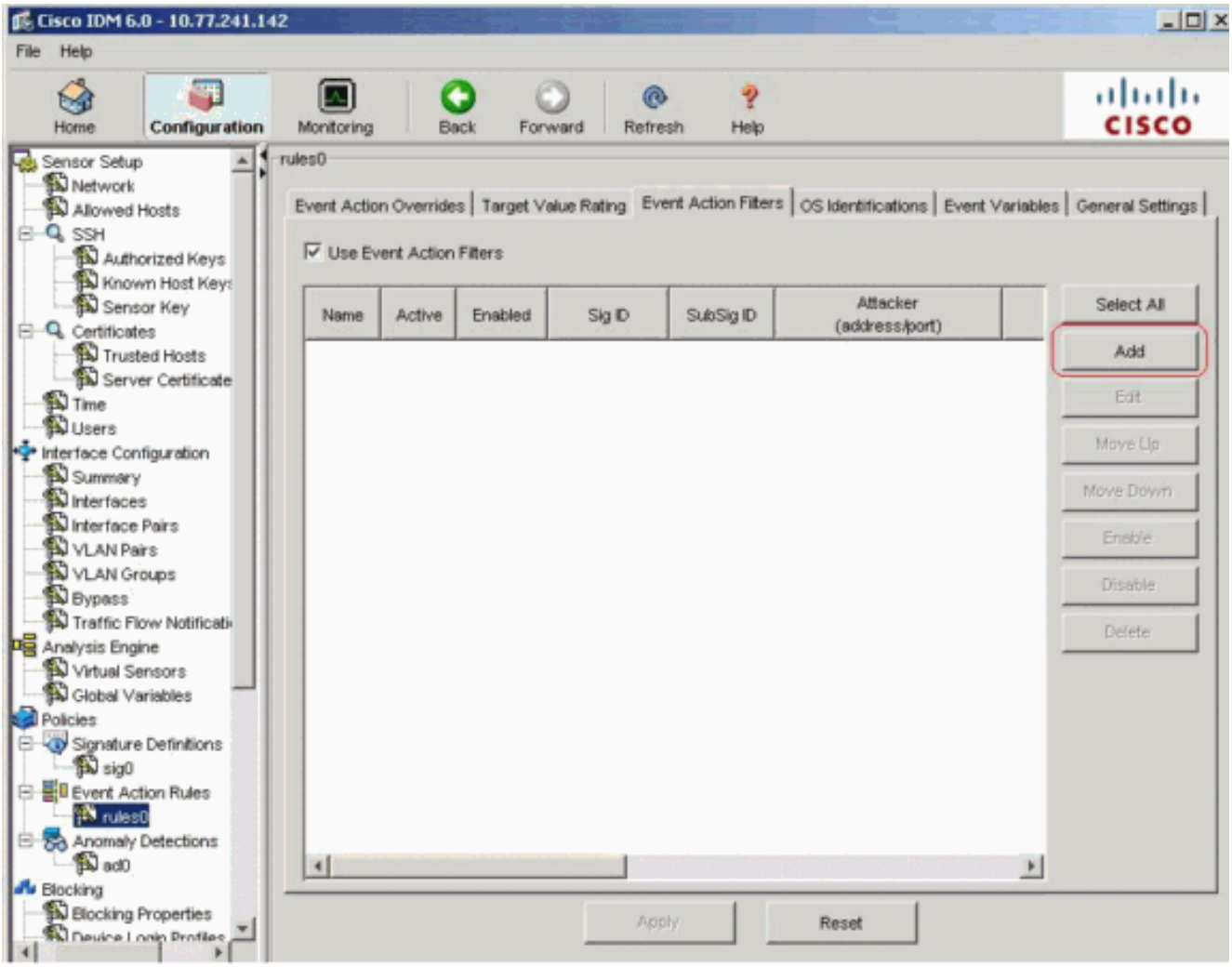
```
sensor(config-eve)#exit
Apply Changes:?[yes]:
```

13. 按回车为了应用您的更改或输入**没有**为了丢弃他们。

事件操作过滤器配置使用IDM

完成这些步骤为了添加，编辑，删除，启用，禁用和移动事件操作过滤器：

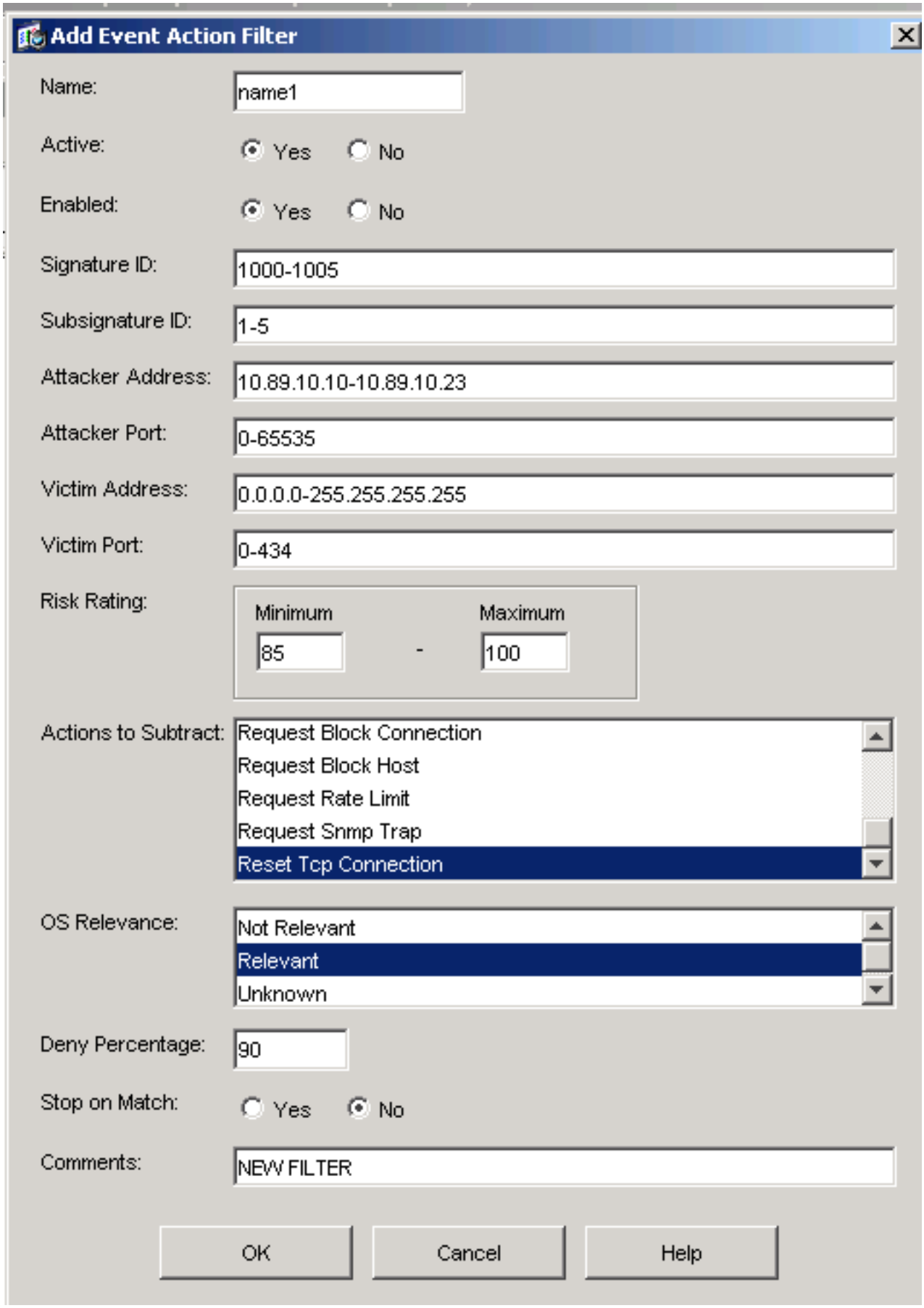
1. 登陆对与有管理员或操作员权限的帐户的IDM。
2. 如果软件版本是6.x，请选择**Configuration>策略>事件操作规定> rules0 >事件操作过滤器**。对于软件版本5.x，请选择**Configuration>事件操作规则>事件操作过滤器。**事件操作过滤器选项卡出现如显示。



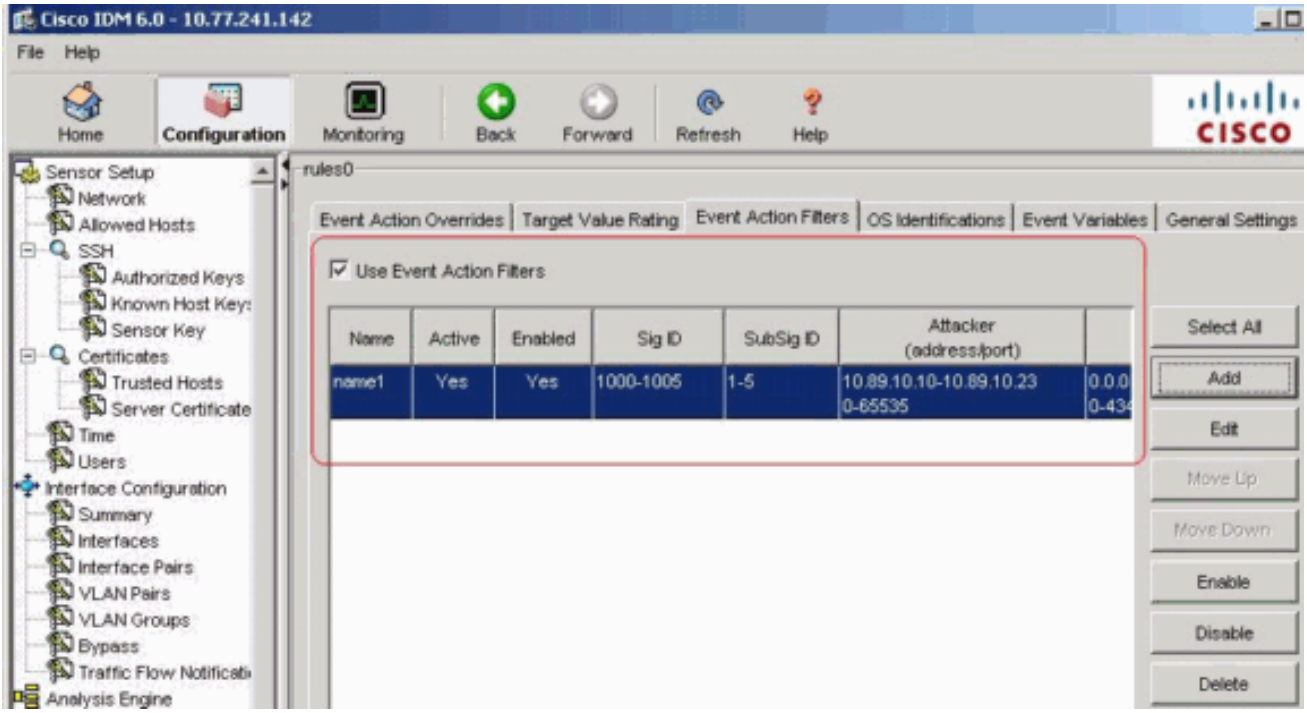
3. 单击**添加**为了添加事件操作过滤器。添加事件操作过滤器对话框出现。
4. 在Name字段，请输入名称作为事件操作过滤器的**name1**。供应默认名称，但是您能更改它到一更加有意义的名称。
5. 在有效域，请点击**Yes单选按钮**为了添加此过滤器到列表，以便生效对过滤事件的。
6. 在Enabled字段，请点击**Yes单选按钮**为了启用过滤器。**注意：** 您必须也检查在事件操作过滤器选项卡的**使用事件操作过滤器**复选框或事件操作都不过滤变得已启用不管您是否检查在添加事件操作过滤器对话框的**Yes复选框**。
7. 在签名ID字段，请进入此过滤器应该应用所有签名的签名ID。如果在事件变量选项卡，定义他们您能使用列表，例如， 1000， 1005或者范围，例如， **1000-1005**或其中一SIG变量。前言与$的变量。
8. 在签名ID字段，请进入此过滤器应该应用子签名的签名ID。例如， **1-5**。
9. 在攻击者地址字段，请输入源主机的IP地址。如果在事件变量选项卡，定义他们您能使用其中一变量。前言与$的变量。您能也输入地址范围，例如， **10.89.10.10-10.89.10.23**。默认是0.0.0.0-255.255.255.255。
10. 在攻击者端口字段，请输入攻击者用于的端口号为了发送已损坏的数据包。
11. 在受害者地址字段，请输入接收主机的IP地址。如果在事件变量选项卡，定义他们您能使用其中一变量。前言与$的变量。您能也输入地址范围，例如， **192.56.10.1-192.56.10.255**。默认是0.0.0.0-255.255.255.255。
12. 在受害者端口字段，请输入受害主机用于的端口号为了接收已损坏的数据包。例如， **0-434**。
13. 在风险等级字段，请输入此过滤器的一个RR范围。例如， **85-100**。如果事件的RR属于您指定的范围，事件处理此过滤器标准。
14. 从操作减去下拉列表，请选择您希望此过滤器从事件取消的操作。例如，请选择**重置TCP连**

接。提示： 持续Ctrl密钥为了选择超过在列表的一事件操作。

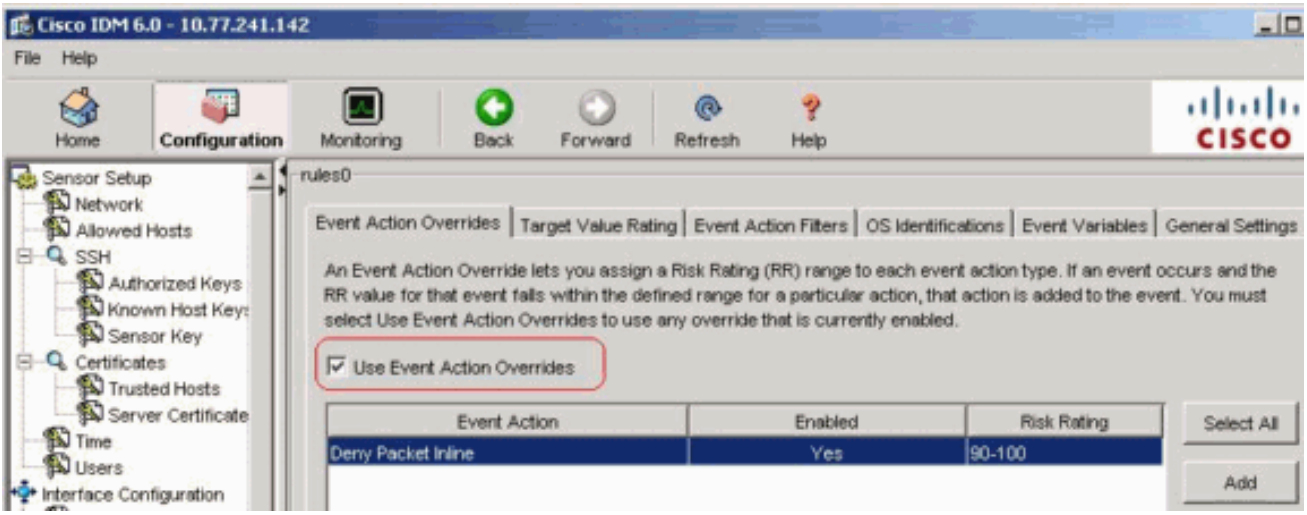
15. 在OS相关性下拉列表中，请选择您是否要知道为受害者识别的警报是否与OS是相关的。例如，请选择**相关**。
16. 在拒绝百分比字段，请输入数据包的百分比为了拒绝为拒绝攻击者功能。例如， **90**。默认是100百分比。
17. 在匹配字段的终止，请选择这些单选按钮之一：**是**—如果希望事件操作过滤组件停止处理，在此特定的过滤器的操作删除后保持的任何过滤器没有处理;因此，另外的操作不可以从事件删除。**NO-，**如果要继续处理另外的过滤器
18. 在注解栏，请输入您要用此过滤器存储，例如此过滤器目的任何意见或您为什么配置此过滤器用一个特定的方式。例如，**新建的过滤器。提示**： 点击**取消**为了取消您的更改和关闭添加事件操作过滤器对话框。



19. 单击 **Ok**。新的事件操作过滤器在事件操作过滤器选项卡的列表当前出现如显示。

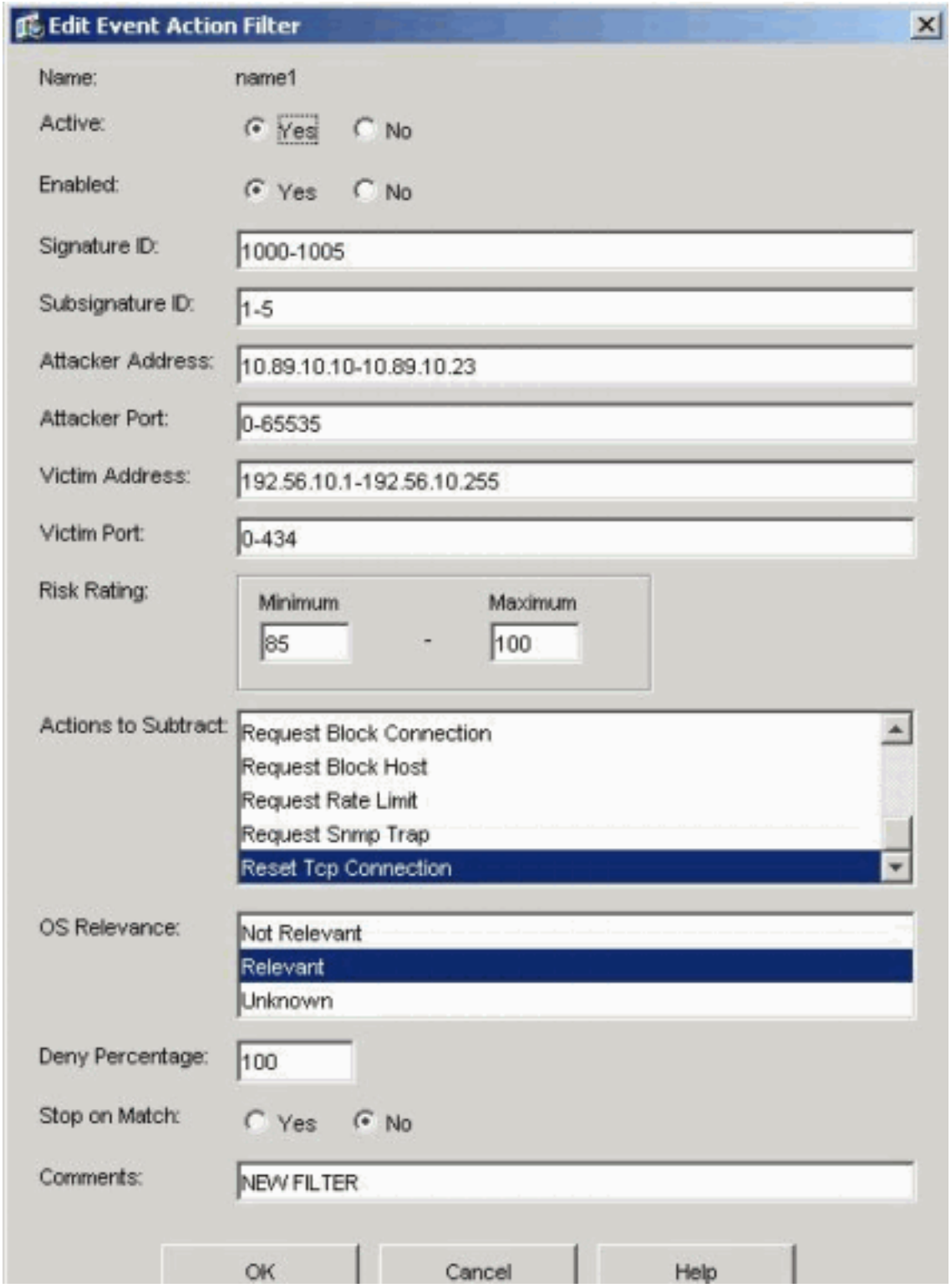


20. 检查**使用事件操作改写**复选框如显示。



注意： 您必须检查**使用事件操作改写**在事件操作的复选框改写选项卡或事件操作都不改写变为已启用不管值您在添加事件操作过滤器对话框的集。

21. 选择在列表的一现有事件操作过滤器为了编辑它，然后单击**编辑**。编辑事件操作过滤器对话



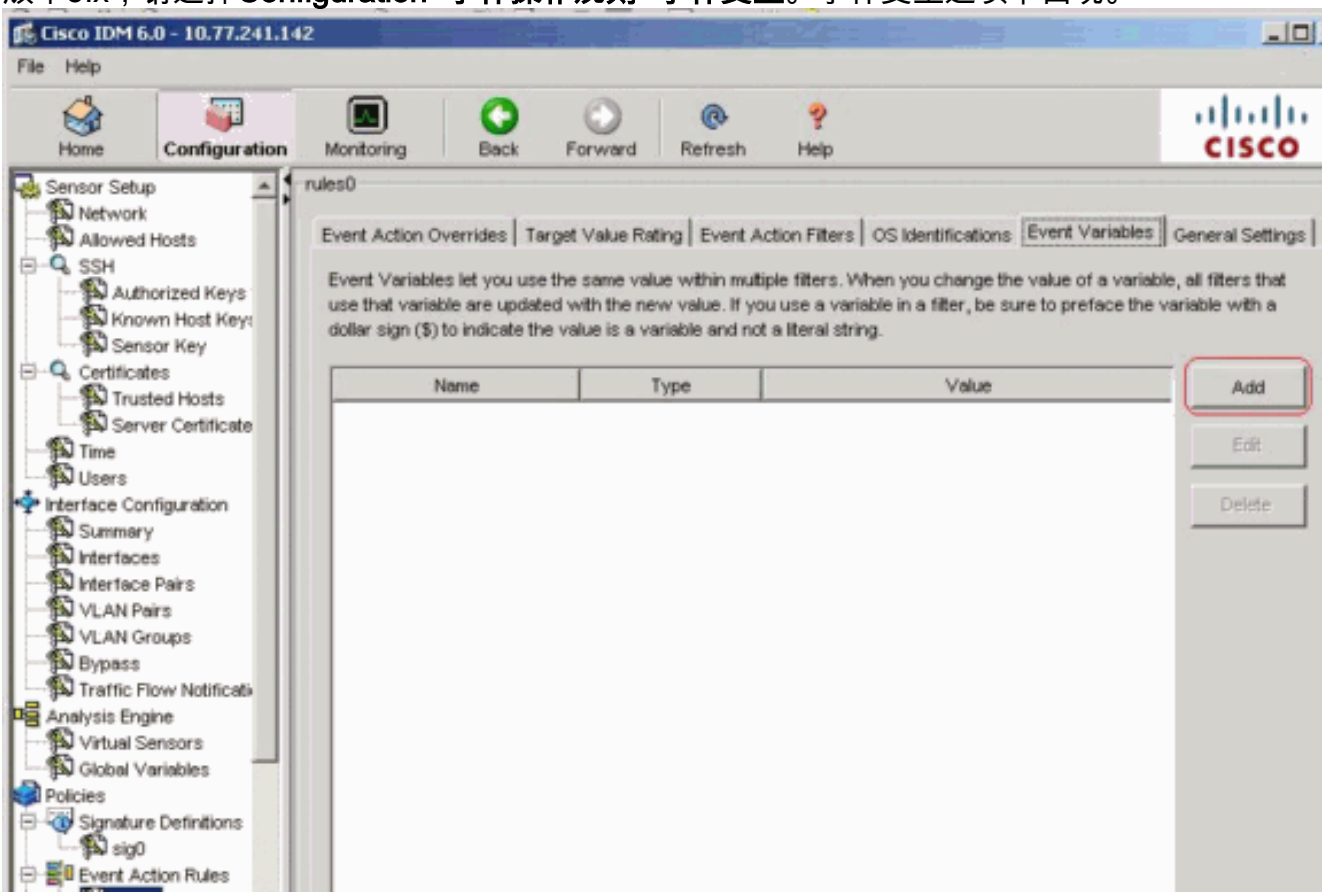
框出现。

22. 在您需要修改的字段更改所有值。请参阅关于如何的步骤4至18填入字段的信息。**提示**： 点击**取消**为了取消您的更改和关闭编辑事件操作过滤器对话框。
23. 单击 **Ok**。编辑的事件操作过滤器在事件操作过滤器选项卡的列表当前出现。
24. 检查**使用事件操作改写**复选框。**注意**： 您必须检查**使用事件操作改写**在事件操作的复选框改写选项卡或事件操作都不改写启用不管值您在编辑事件操作过滤器对话框的集。
25. 选择在列表的一事件操作过滤器为了删除它，然后单击**删除**。事件操作过滤器在事件操作过滤器选项卡的列表不再出现。
26. 上上下下过滤在列表为了移动事件操作，选择它和然后单击**提高**或**调低**。**提示**： 点击**"Reset"**为了取消您的更改。
27. 单击**应用**为了应用您的更改和保存已修订配置。

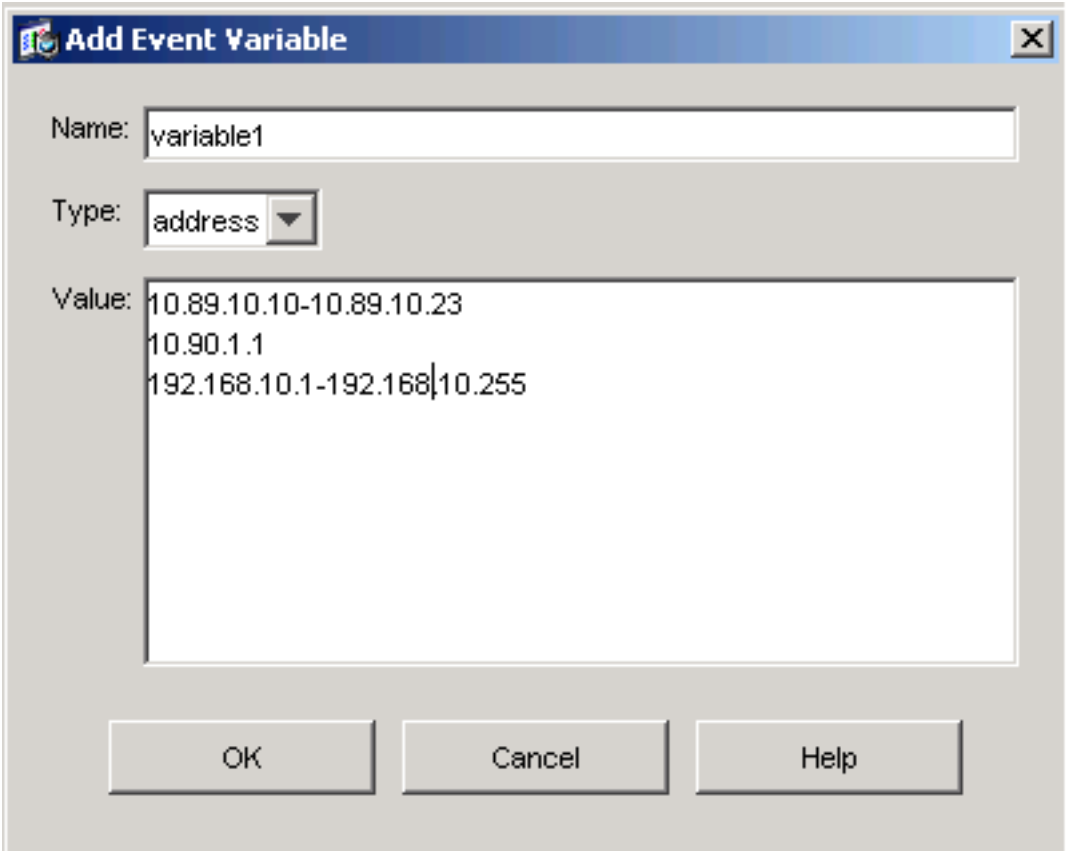
事件变量配置

完成这些步骤为了添加，编辑和删除事件变量：

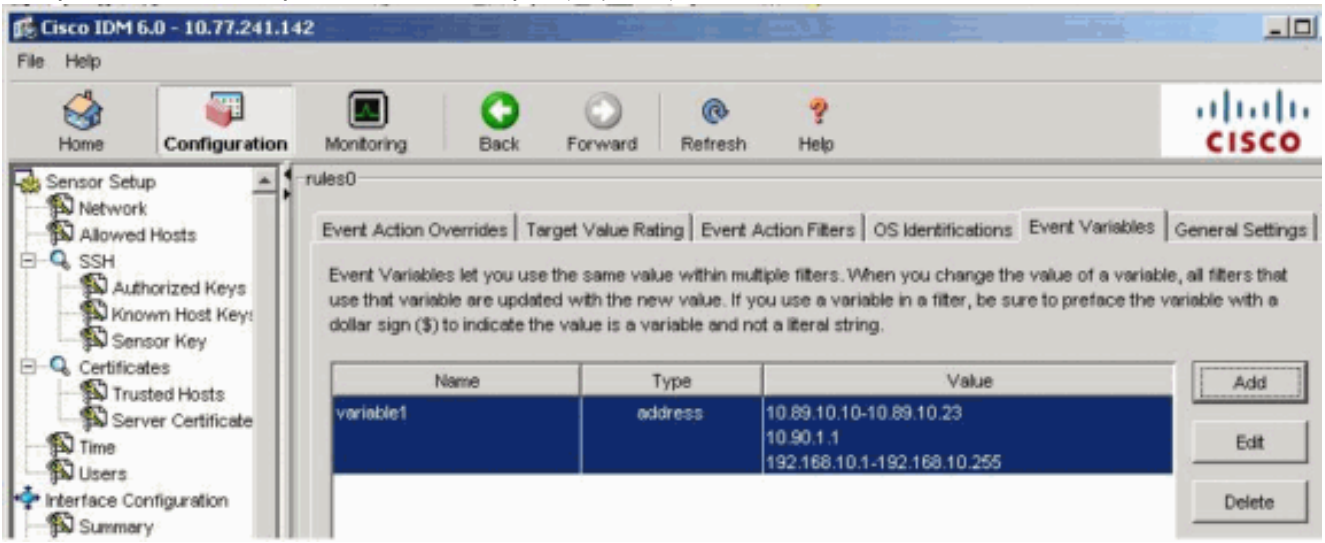
1. 登录。例如，请以管理员或操作员权限使用一个帐户。
2. 如果软件版本是6.x，请选择**Configuration>策略>事件操作规定> rules0 >事件变量**。对于软件版本5.x，请选择**Configuration>事件操作规则>事件变量**。事件变量选项卡出现。



3. 单击**添加**为了创建变量。添加可变对话框出现。
4. 在Name字段，请输入一名称对于此变量。**注意：** 有效名称能只包含编号或字母。您能也使用连字符(-)或下划线(_)。
5. 在Value字段，请输入此变量的值。指定全双工IP地址或范围或者套范围。例如：10.89.10.10-10.89.10.2310.90.1.1192.168.10.1-192.168.10.255**注意：** 您能使用逗号作为分隔符。确保那里是没有句尾空格在逗号以后。否则，您收到错误消息。**提示：** 点击**取消**为了取消您的更改和关闭添加事件变量对话框。



6. 单击 **Ok**。新的变量在事件变量选项卡的列表出现。



7. 选择在列表的现有变量为了编辑它，然后单击**编辑**。编辑事件变量对话框出现。
8. 在Value字段，请输入您的对值的更改。
9. 单击 **Ok**。编辑的事件变量在事件变量选项卡的列表当前出现。**提示**： 选择**重置**为了取消您的更改。
10. 单击**应用**为了应用您的更改和保存已修订配置。

相关信息

- Cisco 入侵防御系统支持页
- 技术支持和文档 - Cisco Systems