IPS 5.x及更高版本：使用CLI和IDM使用事件操作過濾器調整簽名

目錄

簡介

本文檔介紹如何通過命令列介面(CLI)和IDS裝置管理器(IDM)在Cisco Intrusion Prevention System(IPS)中使用事件操作過濾器來調整簽名。

必要條件

需求

本檔案假設Cisco IPS已安裝且工作正常。

採用元件

本檔案中的資訊是根據執行軟體版本5.0和更新版本的Cisco 4200系列IDS/IPS裝置。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

事件操作過濾器

瞭解事件操作過濾器

事件操作過濾器作為有序清單處理，您可以在清單中上下移動過濾器。

過濾器允許感測器響應事件執行某些操作，而不需要感測器執行所有操作或刪除整個事件。過濾器通過從事件中刪除操作來發揮作用。從事件中移除所有操作的過濾器會有效使用該事件。

注意：過濾掃描簽名時，思科建議您不要過濾目標地址。如果有多個目的地址，則僅使用最後一個地址來匹配過濾器。

可以配置事件操作過濾器來刪除事件中的特定操作，或丟棄整個事件並阻止感測器進一步處理。您可以使用已定義的事件操作變數對過濾器地址進行分組。有關如何配置事件操作變數的過程，請參閱新增、編輯和刪除事件操作變數部分。

注意：必須使用美元符號($)作為變數的字首，以指示使用變數而不是字串。否則，您將收到`Bad source and destination`錯誤。

事件操作過濾器使用CLI配置

完成以下步驟以配置事件操作過濾器：

1. 使用具有管理員許可權的帳戶登入到CLI。
2. 輸入事件操作規則子模式：
   ```
   sensor#configure terminal
   sensor(config)#service event-action-rules rules1
   sensor(config-eve)#
   ```
3. 建立篩選器名稱：
   ```
   sensor(config-eve)#filters insert name1 begin
   ```

   使用name1、name2等來命名事件操作過濾器。使用begin |結束 |非活動 |之前 | after keywords，指定要將過濾器插入的位置。
4. 指定此篩選器的值：指定簽名ID範圍：
   ```
   sensor(config-eve-fil)#signature-id-range 1000-1005
   ```

   預設值為900到65535。指定子簽名ID範圍：
   ```
   sensor(config-eve-fil)#subsignature-id-range 1-5
   ```

   預設值為0到255。指定攻擊者地址範圍：
   ```
   sensor(config-eve-fil)#attacker-address-range 10.89.10.10-10.89.10.23
   ```

   預設值為0.0.0.0到255.255.255.255。指定受害者地址範圍：
   ```
   sensor(config-eve-fil)#victim-address-range 192.56.10.1-192.56.10.255
   ```

   預設值為0.0.0.0到255.255.255.255。指定受害埠範圍：
   ```
   sensor(config-eve-fil)#victim-port-range 0-434
   ```

   預設值為0到65535。指定作業系統相關性：
   ```
   sensor(config-eve-fil)#os-relevance relevant
   ```

   預設值為0到100。指定風險評級範圍。
   ```
   sensor(config-eve-fil)#risk-rating-range 85-100
   ```

預設值為0到100。指定要刪除的操作：

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

如果過濾拒絕操作，請設定所需的拒絕操作百分比：

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

預設值為100。將篩選器的狀態指定為「已禁用」或「已啟用」。

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

預設為啟用。指定stop on match引數。

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

True指示感測器在此項匹配時停止處理過濾器。False指示感測器繼續處理過濾器，即使該專案匹配。新增要用於解釋此篩選器的任何註釋：

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

5. 驗證篩選器的設定：

```
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. 若要編輯現有篩選器：

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

7. 編輯引數並參閱步驟4a至4l以瞭解更多資訊。
8. 若要在篩選清單中上下移動篩選條件：

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

9. 驗證是否已移動篩選條件：

```
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. 要將過濾器移動到非活動清單，請執行以下操作：

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

11. 驗證過濾器是否已移至非活動清單：

```
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. 退出事件操作規則子模式：

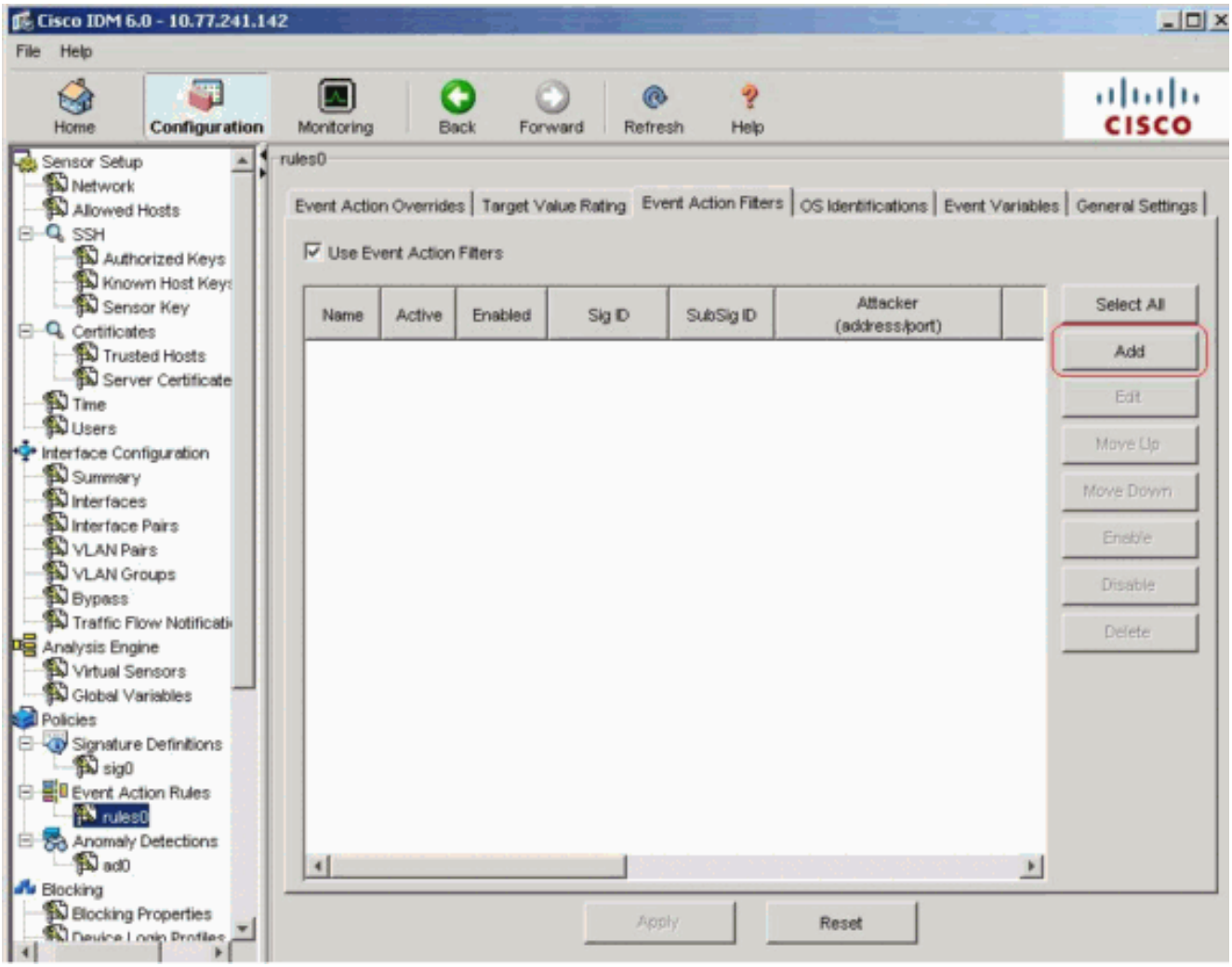
```
sensor(config-eve)#exit
Apply Changes:?[yes]:
```

13. 按Enter以應用更改，或輸入no以放棄更改。

事件操作過濾器使用IDM的配置

完成以下步驟，以便新增、編輯、刪除、啟用、禁用和移動事件操作過濾器：

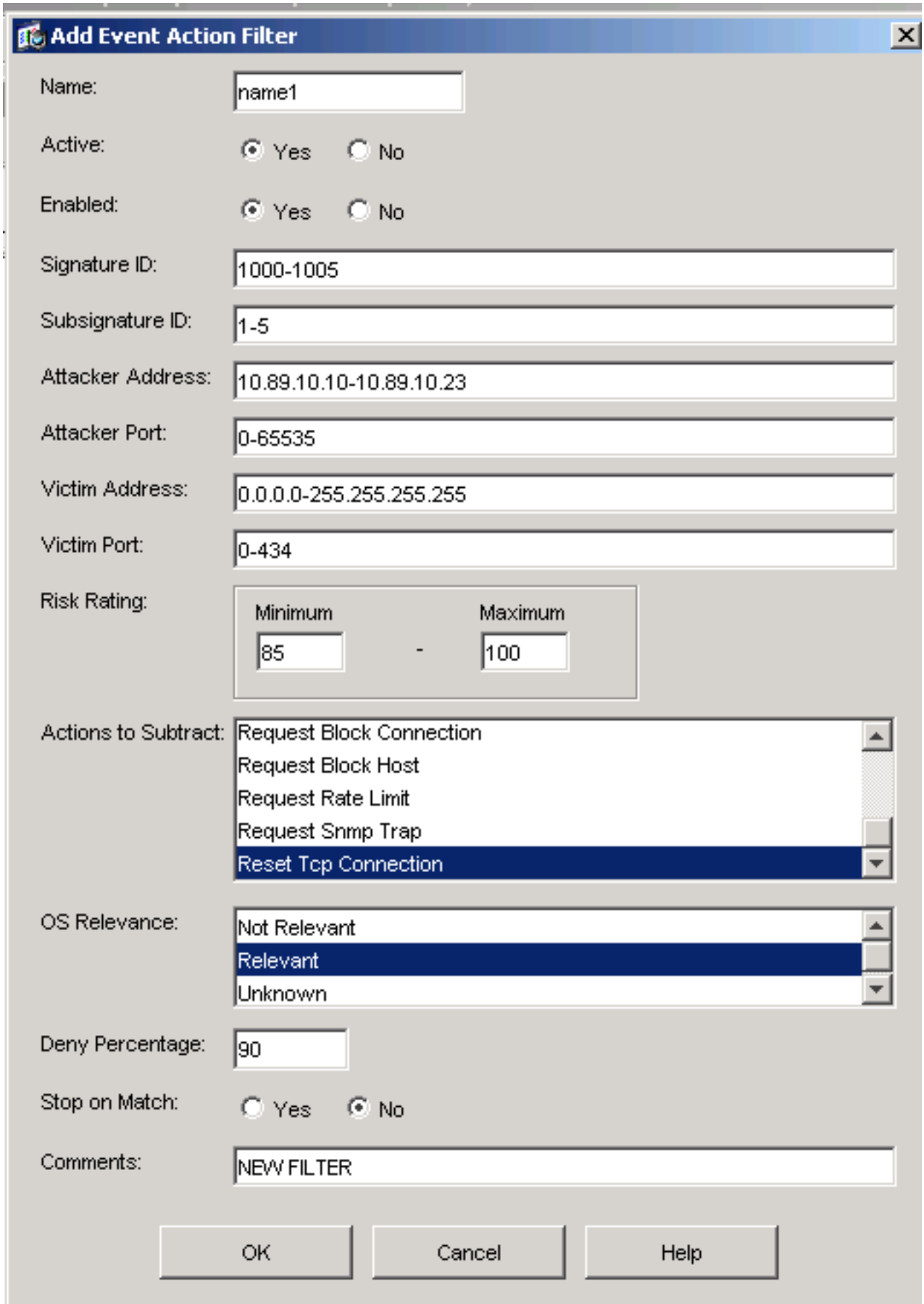
1. 使用具有管理員或操作員許可權的帳戶登入到IDM。
2. 如果軟體版本為6.x，請選擇Configuration > Policies > Event Action Rules > rules0 > Event Action Filters。對於軟體版本5.x，請選擇Configuration > Event Action Rules > Event Action Filters。此時將顯示「事件操作過濾器」頁籤，如下所示。



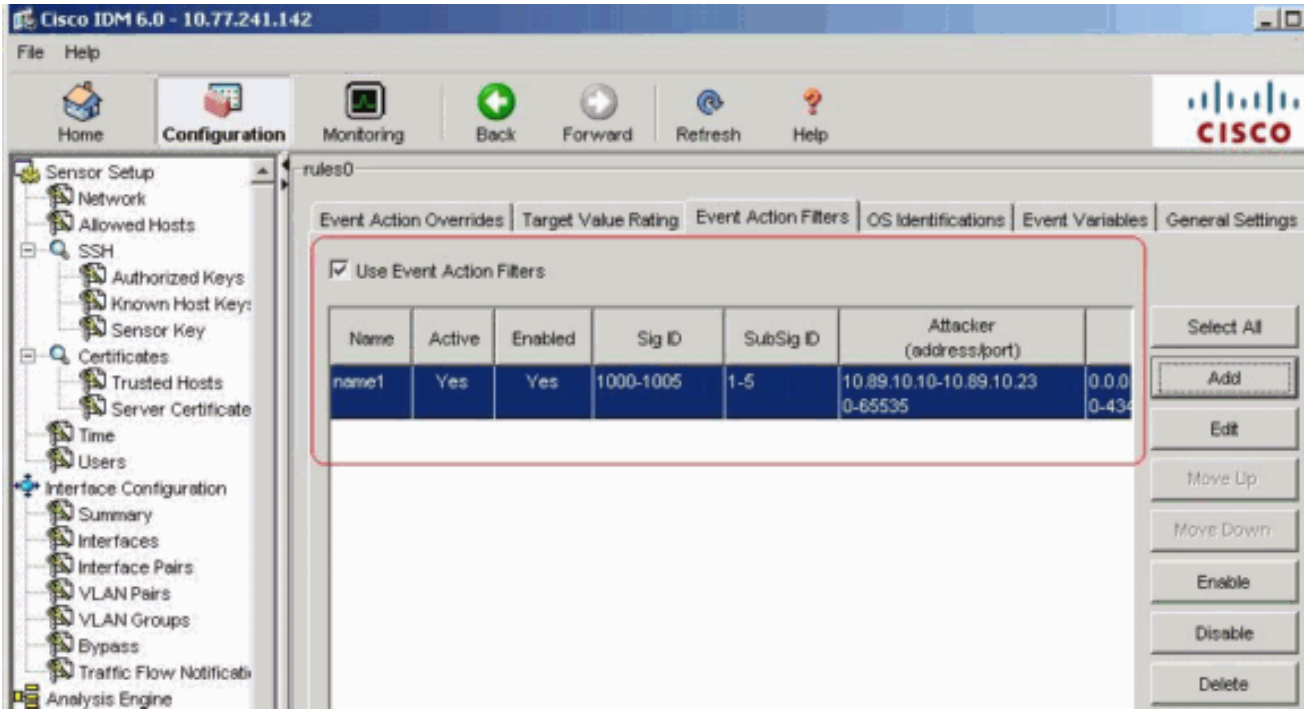
3. 按一下**Add**以新增事件操作過濾器。系統將顯示Add Event Action Filter對話方塊。
4. 在「名稱」欄位中，為事件操作過濾器輸入名為**name1**的名稱。提供了預設名稱，但您可以將其更改為更有意義的名稱。
5. 在Active欄位中，按一下**Yes**單選按鈕，以便將此過濾器新增到清單中，使其在過濾事件時生效。
6. 在「已啟用」欄位中，按一下**Yes**單選按鈕以啟用過濾器。**註：您還必須**在「事件操作過濾器」頁籤上選中**使用事件操作過濾器**覈取方塊，否則無論是否選中「新增事件操作過濾器」對話方塊中的**「是」覈取方塊，都不會啟用任何事件操作過濾器。**
7. 在簽名ID欄位中，輸入應應用此過濾器的所有簽名的簽名ID。可以使用清單（例如1000、1005）或範圍(例如**1000-1005)或其中一個SIG變數(如果您在「事件變數」(Event Variables)頁籤上定義了這些變數)。**在變數前面加上$。
8. 在SubSignature ID欄位中，輸入應應用此過濾器的子簽名的子簽名ID。例如，**1-5**。
9. 在Attacker Address欄位中，輸入源主機的IP地址。如果在「事件變數」(Event Variables)頁籤上定義了變數，則可以使用其中一個。在變數前面加上$。您還可以輸入地址範圍，例如**10.89.10.10-10.89.10.23**。預設值為0.0.0.0-255.255.255.255。
10. 在Attacker Port欄位中，輸入攻擊者用來傳送違規資料包的埠號。
11. 在「受害者地址」欄位中，輸入收件人主機的IP地址。如果在「事件變數」(Event Variables)頁籤上定義了變數，則可以使用其中一個。在變數前面加上$。您還可以輸入地址範圍，例如**192.56.10.1-192.56.10.255**。預設值為0.0.0.0-255.255.255.255。
12. 在「受害者埠」欄位中，輸入受害者主機用來接收違規資料包的埠號。例如**0-434**。
13. 在「風險等級」欄位中，輸入此篩選器的風險等級範圍。例如**85-100**。如果事件的RR在您指定的範圍內，則會根據此篩選器的條件處理事件。
14. 從「要減去的操作」下拉選單中，選擇希望此過濾器從事件中刪除的操作。例如，選擇**Reset**

TCP connection。**提示：**按住**Ctrl**鍵可在清單中選擇多個事件操作。

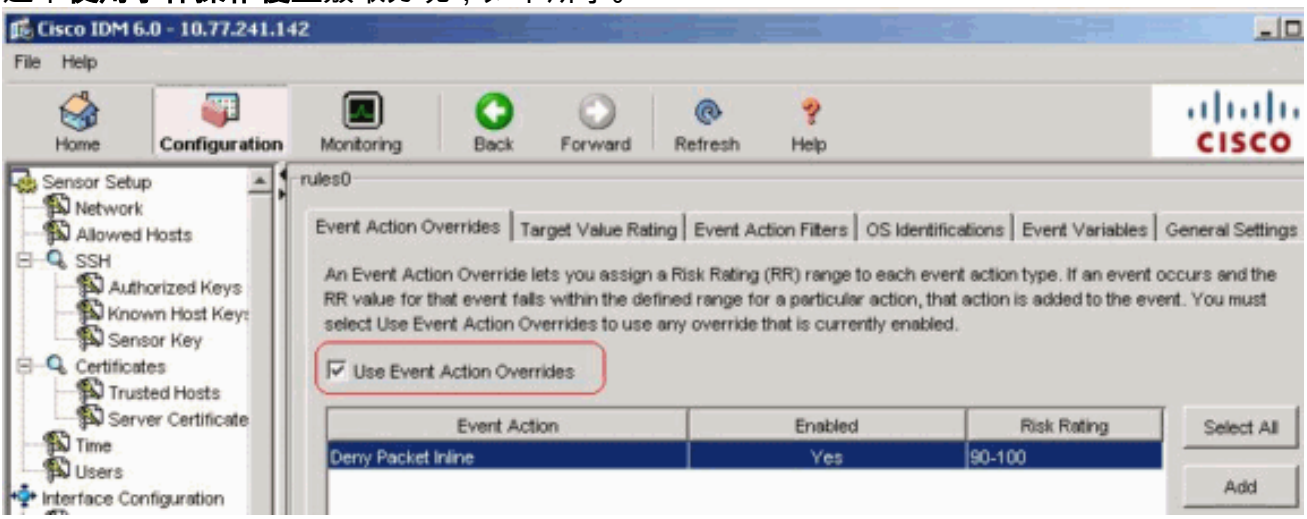
15. 在OS Relevance（作業系統相關性）下拉選單中，選擇您是否要知道警報是否與已為受害者標識的作業系統相關。例如，選擇**Relevant**。
16. 在Deny Percentage欄位中，輸入資料包的百分比，以拒絕拒絕攻擊者的功能。例如**90**。預設值為100%。
17. 在「匹配時停止」欄位中，選擇以下單選按鈕之一：**Yes** — 如果希望事件操作過濾器元件在刪除此特定過濾器的操作後停止處理不會處理剩餘的任何過濾器；因此，不能從事件中刪除其他操作。**No** — 如果要繼續處理其他過濾器
18. 在「註釋」欄位中，輸入要使用此篩選器儲存的任何註釋，例如此篩選器的用途或您以特定方式配置此篩選器的原因。例如**NEW FILTER**。**提示：**按一下**取消**可撤消更改並關閉「新增事件操作過濾器」對話方塊。



19. 按一下「**OK**」（確定）。新的事件操作過濾器現在顯示在「事件操作過濾器」(Event Action Filters)頁籤的清單中，如下所示。

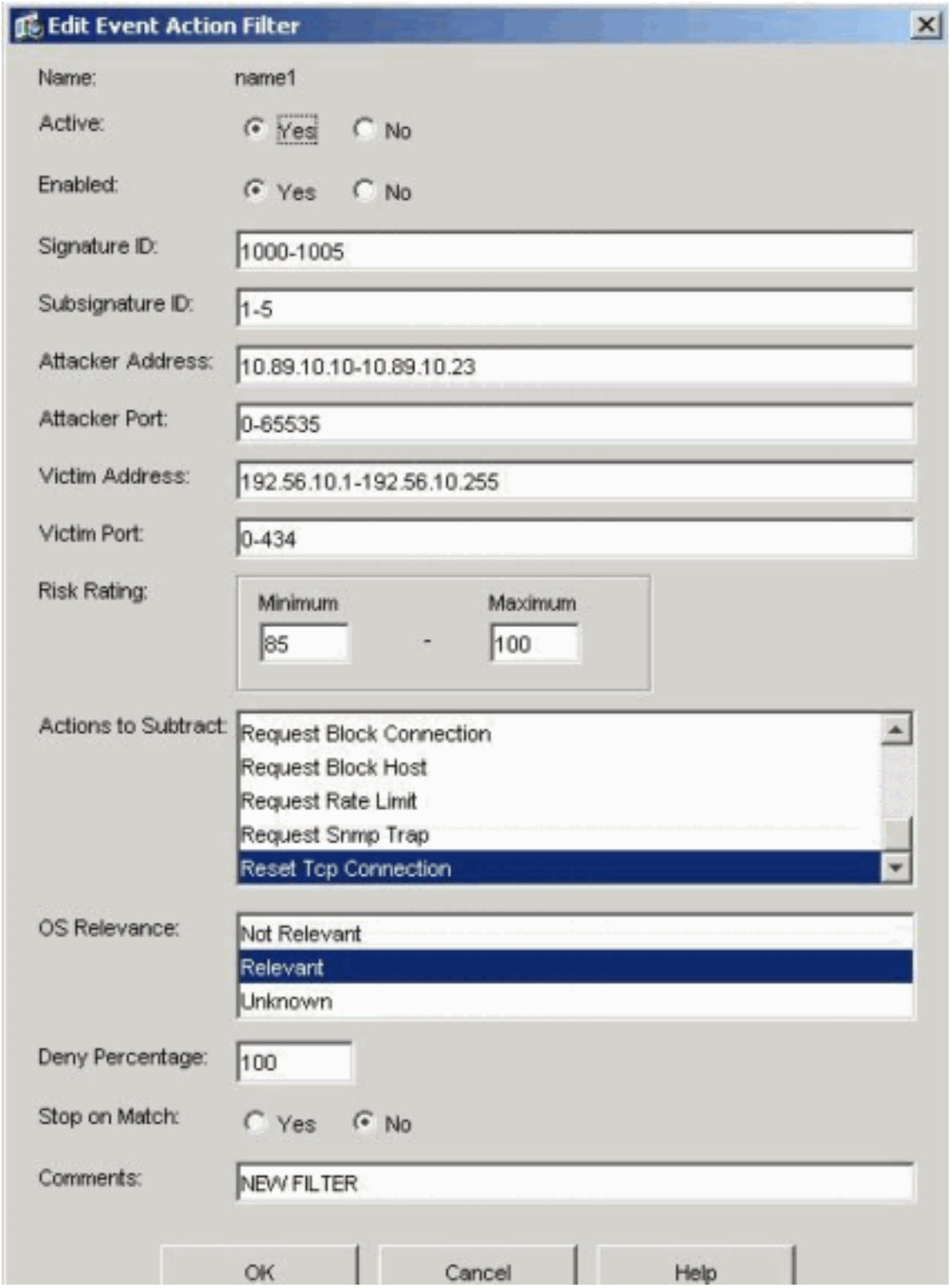


20. 選中**使用事件操作覆蓋**覈取方塊，如下所示。



註：您必須在「事件操作覆蓋」頁籤上選中「**使用事件操作覆蓋」複選**框，否則無論您在「新增事件操作過濾器」對話方塊中設定的值如何，都不會啟用任何事件操作覆蓋。

21. 選擇清單中的現有事件操作過濾器以進行編輯，然後按一下**編輯**。系統將顯示Edit Event Action Filter對話方塊。

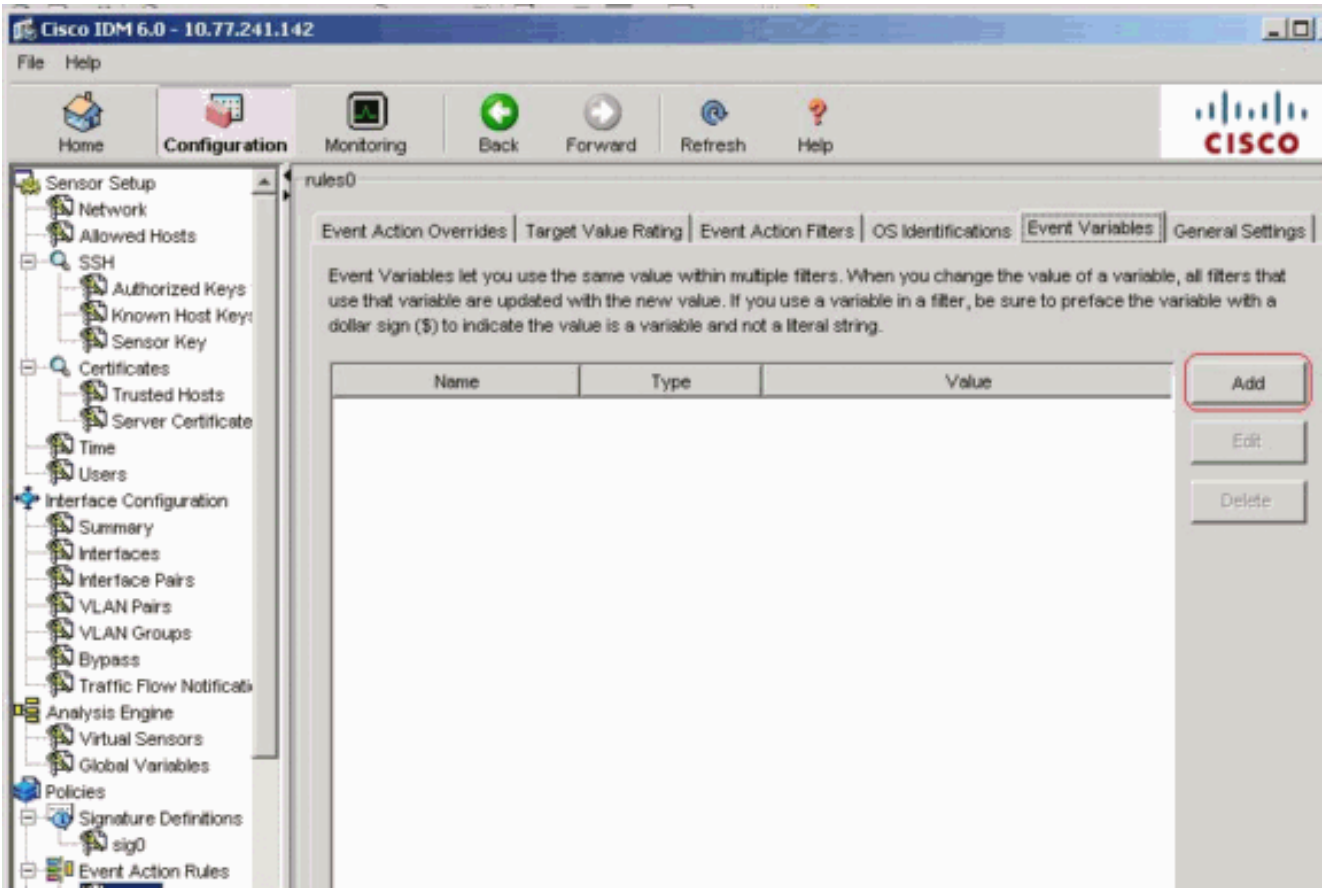


22. 更改需要更改的欄位中的任何值。有關如何填寫欄位的資訊，請參閱步驟4至18。**提示：**按一下**取消**可撤消更改並關閉「編輯事件操作過濾器」對話方塊。
23. 按一下「**OK**」（確定）。編輯的事件操作過濾器現在顯示在「事件操作過濾器」(Event Action Filters)頁籤的清單中。
24. 選中**使用事件操作覆蓋**覈取方塊。**註：您必須**在「事件操作覆蓋」頁籤上選中「**使用事件操作覆蓋」複選**框，否則無論您在「編輯事件操作過濾器」對話方塊中設定的值如何，都不會啟用任何事件操作覆蓋。
25. 選擇清單中的事件操作過濾器以將其刪除，然後按一下**Delete**。事件操作過濾器不再出現在事件操作過濾器頁籤的清單中。
26. 在清單中上下過濾以移動事件操作，請選擇該操作，然後按一下**上移**或**下移**。提示：按一下**Reset以移除變更。**
27. 按一下「**Apply**」以應用變更並儲存修訂的組態。

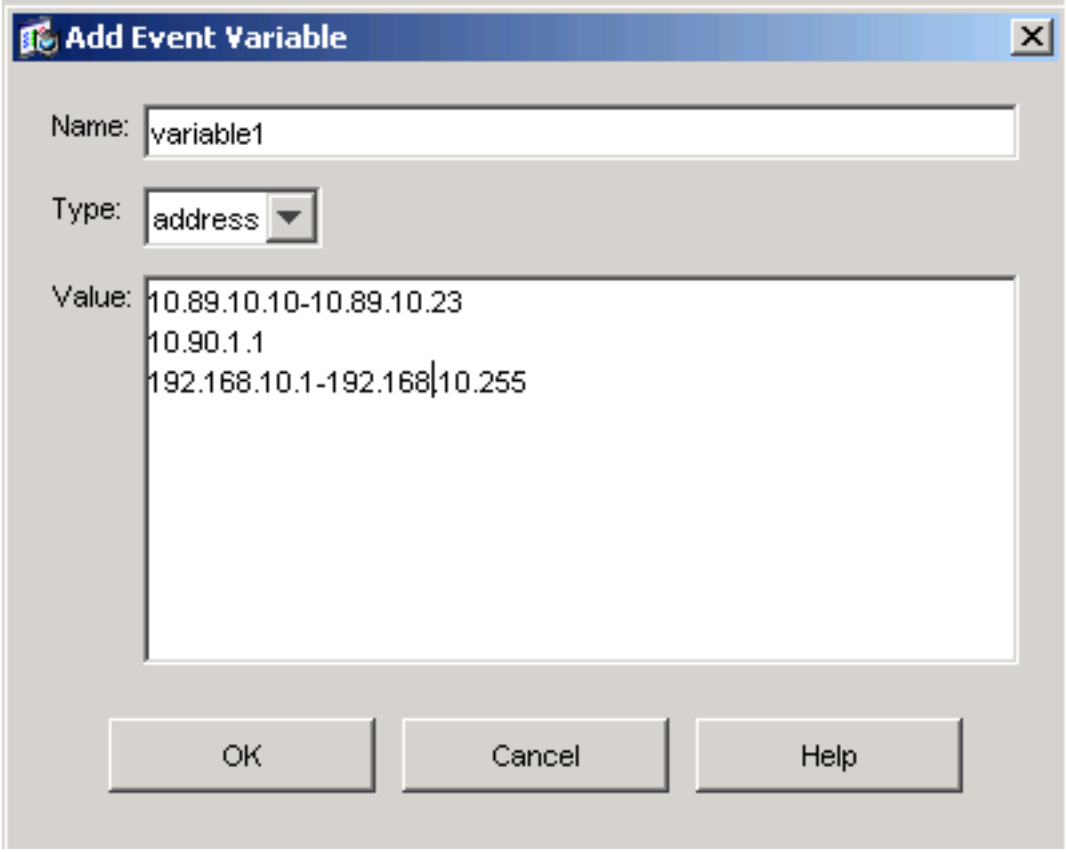
事件變數配置

完成以下步驟以新增、編輯和刪除事件變數：

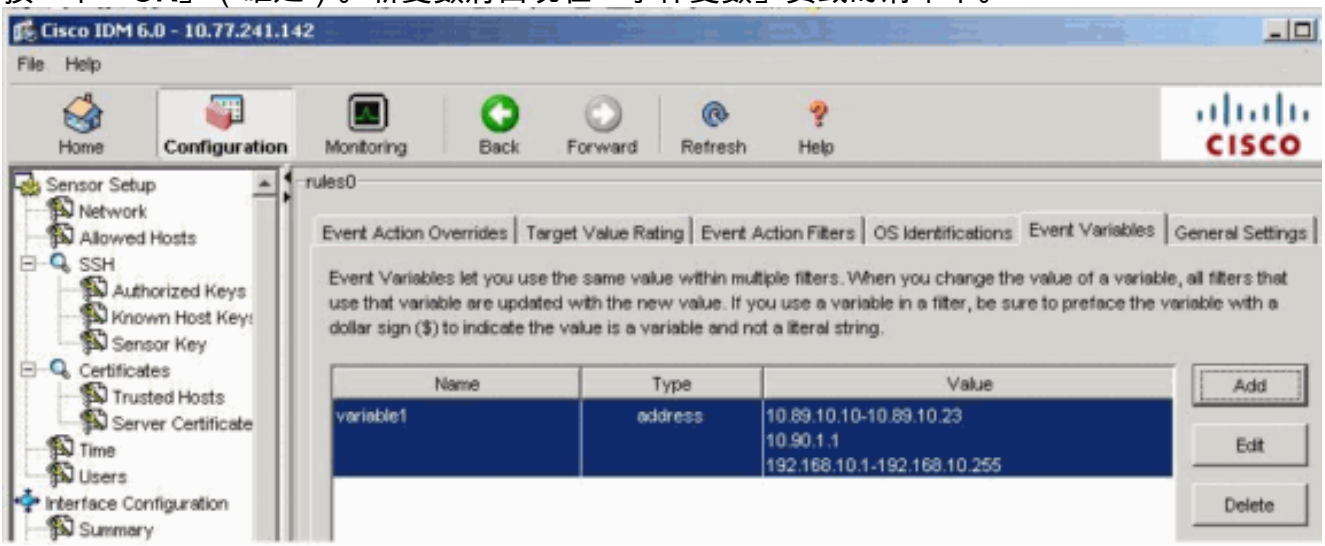
1. 登入。例如，使用具有管理員或操作員許可權的帳戶。
2. 如果軟體版本為6.x，請選擇**Configuration > Policies > Event Action Rules > rules0 > Event Variables**。對於軟體版本5.x，請選擇**Configuration > Event Action Rules > Event Variables**。系統將顯示Event Variables頁籤。



3. 按一下**Add**以建立一個變數。系統將顯示Add Variable對話方塊。
4. 在名稱欄位中，輸入此變數的名稱。**注意**：有效名稱只能包含數字或字母。還可以使用連字元(-)或下劃線(_)。
5. 在值欄位中，輸入此變數的值。指定完整的IP地址或範圍或範圍集。例如：10.89.10.10-10.89.10.2310.90.1.1192.168.10.1-192.168.10.255**注意**：您可以使用逗號作為分隔符。請確保逗號後沒有尾隨空格。否則，您將收到錯誤消息。**提示**：按一下**取消**可撤消更改並關閉「新增事件變數」對話方塊。



6. 按一下「**OK**」（確定）。新變數將出現在「事件變數」頁籤的清單中。



7. 選擇清單中的現有變數以進行編輯，然後按一下**編輯**。將出現「編輯事件變數」對話方塊。
8. 在「值」欄位中，輸入您對值的更改。
9. 按一下「**OK**」（確定）。編輯後的事件變數現在顯示在「事件變數」(Event Variables)頁籤的清單中。提示：選擇**Reset以刪除您的更改。**
10. 按一下「**Apply**」以應用變更並儲存修訂的組態。

相關資訊

- 思科入侵防禦系統支援頁面
- 技術支援與文件 - Cisco Systems