IPS 5.x والإصدارات الأحدث: ضبط التوقيع باستخدام عامل تصفية إجراء الحدث باستخدام CLI و IDM

المحتويات

المقدمة

يصف هذا المستند كيفية ضبط التوقيع باستخدام عامل تصفية إجراءات الحدث في نظام منع التسلل (IPS) من Cisco باستخدام واجهة سطر الأوامر (CLI) ومدير جهاز IDM (IDS).

المتطلبات الأساسية

المتطلبات

يفترض هذا المستند أن Cisco IPS مثبت ويعمل بشكل صحيح.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى جهاز Cisco 4200 Series IDS/IPS الذي يشغل الإصدار 5.0 من البرنامج والإصدارات الأحدث.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

عوامل تصفية إجراء الحدث

فهم عوامل تصفية إجراء الحدث

تتم معالجة عوامل تصفية إجراء الحدث كقائمة مرتبة ويمكنك نقل عوامل التصفية لأعلى أو لأسفل في القائمة.

تتيح عوامل التصفية للمستشعر تنفيذ إجراءات معينة إستجابة للحدث دون مطالبة المستشعر بتنفيذ جميع الإجراءات أو إزالة الحدث بالكامل. تعمل عوامل التصفية بإزالة الإجراءات من حدث ما. مرشح يزيل كل الإجراءات من حدث ما يستهلك الحدث بشكل فعال.

ملاحظة: عند تصفية توقيعات الكنس، توصي Cisco بعدم تصفية عناوين الوجهة. في حالة وجود عناوين وجهة متعددة، يتم إستخدام العنوان الأخير فقط لمطابقة عامل التصفية.

يمكنك تكوين عوامل تصفية إجراءات الحدث لإزالة إجراءات معينة من حدث ما أو لتجاهل حدث كامل ومنع معالجة إضافية بواسطة المستشعر. يمكنك إستخدام متغيرات إجراء الحدث التي قمت بتعريفها لتجميع عناوين عوامل التصفية الخاصة بك. للحصول على الإجراء الخاص بكيفية تكوين متغيرات إجراء الحدث، راجع قسم إضافة متغيرات إجراء الحدث وتحريرها وحذفها.

ملاحظة: يجب أن تستبق المتغير بعلامة دولار ($) للإشارة إلى أنك تستخدم متغير بدلا من سلسلة. وإلا، فإنك تتلقى .

تكوين عوامل تصفية إجراء الحدث باستخدام CLI (واجهة سطر الأوامر)

أكمل الخطوات التالية لتكوين عوامل تصفية إجراء الحدث:

1. قم بتسجيل الدخول إلى CLI باستخدام حساب له امتيازات المسؤول.
2. إدخال الوضع الفرعي لقواعد إجراء الحدث:
```
sensor#configure terminal
sensor(config)#service event-action-rules rules1
#(sensor(config-eve
```
3. إنشاء اسم عامل التصفية:
```
sensor(config-eve)#filters insert name1 begin
```

أستخدم name1، name2، وهكذا دواليك لتسمية عوامل تصفية إجراءات الحدث. إستخدام **البداية | نهاية | غير نشط | قبل | بعد** الكلمات الأساسية لتحديد المكان الذي تريد إدراج عامل التصفية فيه.

4. تحديد قيم عامل التصفية هذا:حدد نطاق معرف التوقيع:
```
sensor(config-eve-fil)#signature-id-range 1000-1005
```

الافتراضي هو 900 إلى 65535.حدد نطاق معرف التوقيع الفرعي:
```
sensor(config-eve-fil)#subsignature-id-range 1-5
```

الافتراضي هو 0 إلى 255.حدد نطاق عنوان المهاجم:
```
sensor(config-eve-fil)#attacker-address-range 10.89.10.10-10.89.10.23
```

الإعداد الافتراضي هو 0.0.0.0 إلى 255.255.255.255.حدد نطاق عنوان الضحية:
```
sensor(config-eve-fil)#victim-address-range 192.56.10.1-192.56.10.255
```

الإعداد الافتراضي هو 0.0.0.0 إلى 255.255.255.255.حدد نطاق منفذ الضحية:
```
sensor(config-eve-fil)#victim-port-range 0-434
```

الافتراضي هو 0 إلى 65535.تحديد الصلة بنظام التشغيل:

```
sensor(config-eve-fil)#os-relevance relevant
```

الافتراضي هو من 0 إلى 100.حدد نطاق تصنيف المخاطر.

```
sensor(config-eve-fil)#risk-rating-range 85-100
```

الافتراضي هو من 0 إلى 100.حدد الإجراءات المراد إزالتها:

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

إذا قمت بتصفية إجراء رفض، قم بتعيين نسبة إجراءات الرفض التي تريدها:

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

الافتراضي هو 100.حدد حالة عامل التصفية إلى "معطل" أو "ممكن".

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

التقصير مكنت.حدد نقطة التوقف عند المعلمة المطابقة.

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

يطلب **True** من المستشعر إيقاف معالجة عوامل التصفية في حالة تطابق هذا العنصر. **يعلم خطأ** المستشعر بالاستمرار في معالجة عوامل التصفية حتى في حالة تطابق هذا العنصر.قم بإضافة أي تعليقات تريد إستخدامها لشرح عامل التصفية هذا:

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

5. دققت العملية إعداد المرشح:

```
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. لتحرير عامل تصفية موجود:

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

7. قم بتحرير المعلمات وانظر الخطوات من 4a إلى 4l للحصول على مزيد من المعلومات.
8. لنقل عامل تصفية لأعلى أو لأسفل في قائمة عوامل التصفية:

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

9. تحقق من نقل عوامل التصفية:

```
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. لنقل مرشح إلى القائمة غير النشطة:

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

11. تحقق من نقل عامل التصفية إلى القائمة غير النشطة:

```
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. الوضع الفرعي لقواعد إجراء حدث الإنهاء:

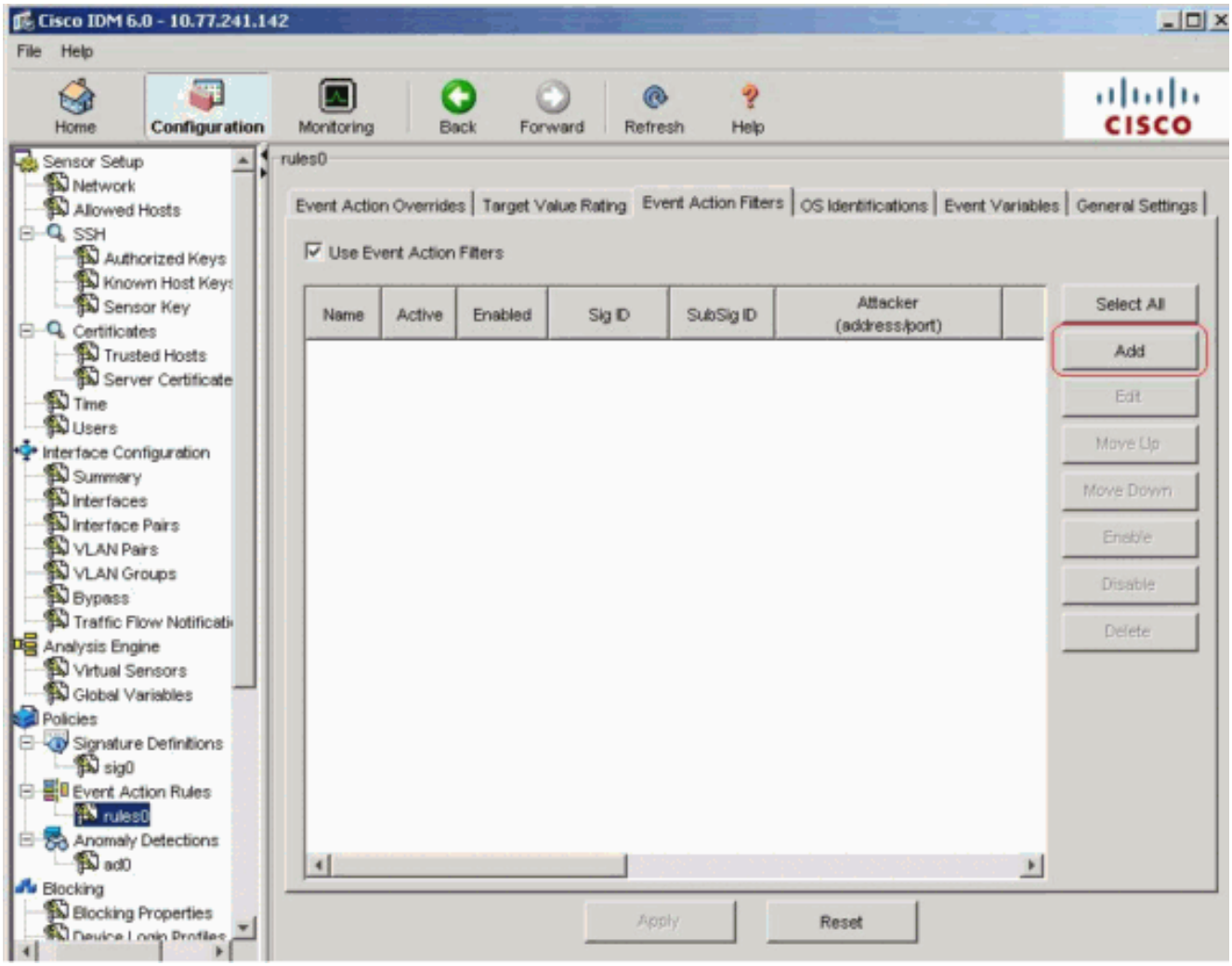
```
sensor(config-eve)#exit
:[Apply Changes:?[yes
```

13. اضغط على **Enter** لتطبيق التغييرات التي قمت بها أو أدخل **no** لتجاهلها.

تكوين عوامل تصفية إجراء الحدث باستخدام IDM

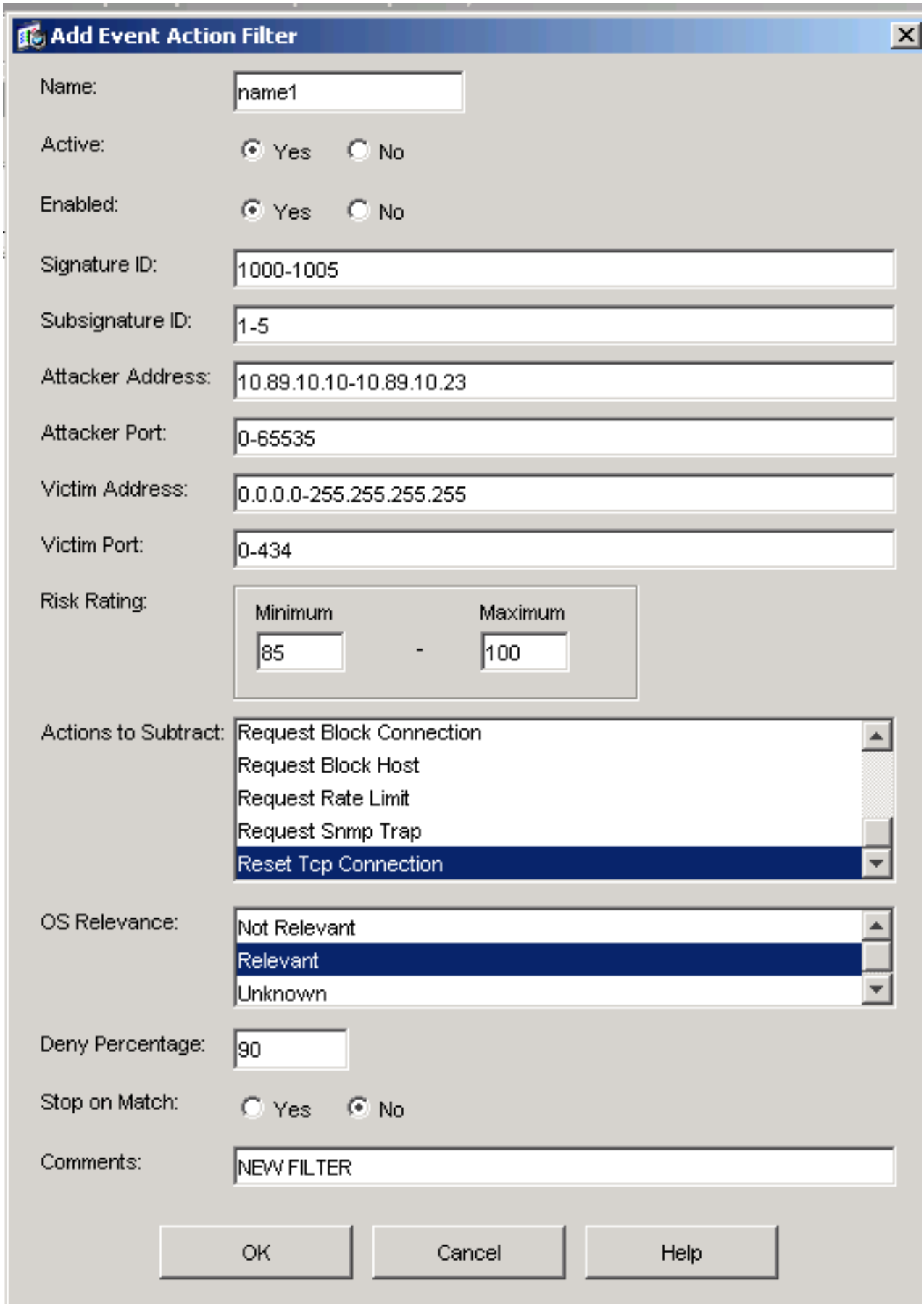
أكمل الخطوات التالية لإضافة عوامل تصفية إجراءات الحدث وتحريرها وحذفها وتمكينها وتعطيلها ونقلها:

1. قم بتسجيل الدخول إلى IDM باستخدام حساب له امتيازات المسؤول أو عامل التشغيل.
2. أختر **تشكيل > سياسات > قواعد إجراء الحدث > قواعد0 > مرشحات إجراء الحدث** إذا كان إصدار البرنامج x.6. بالنسبة للبرنامج الإصدار x.5، أختر **تكوين > قواعد إجراء الحدث > عوامل تصفية إجراء الحدث.**تظهر علامة التبويب عوامل تصفية إجراء الحدث كما هو موضح.

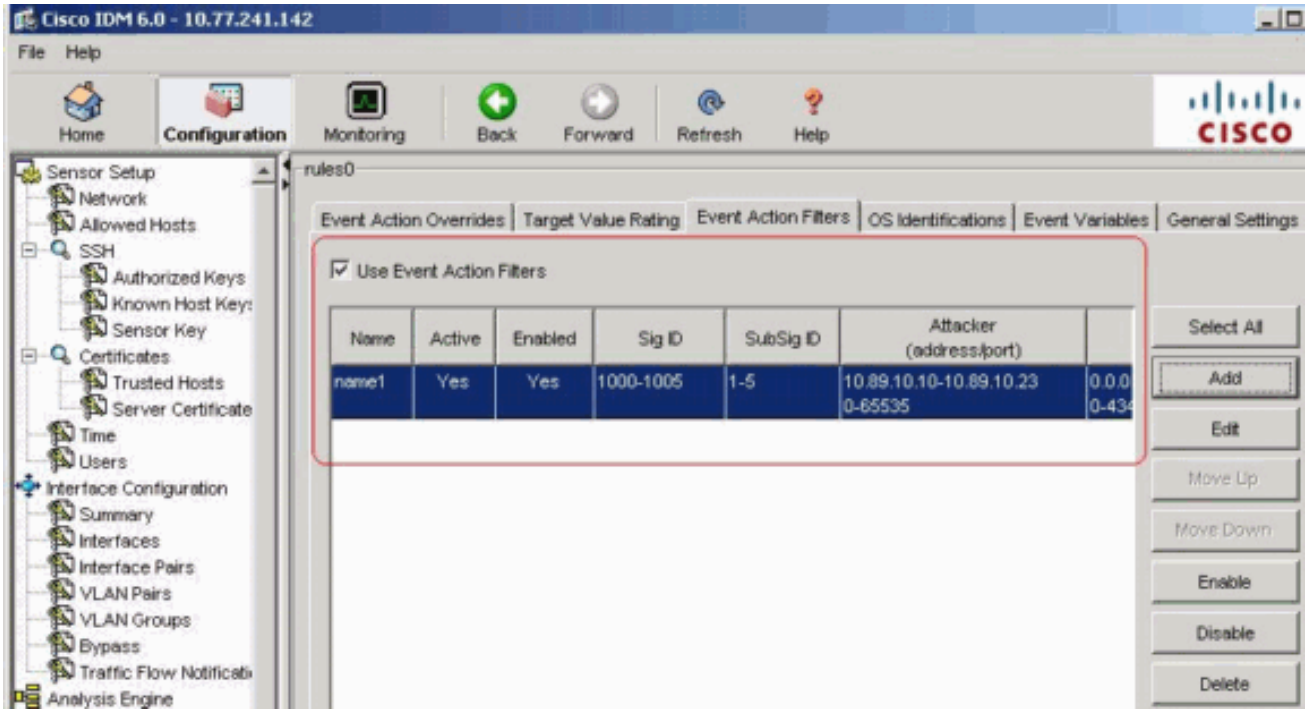


3. انقر فوق **إضافة** لإضافة عامل تصفية إجراء حدث.سوف يظهر مربع الحوار إضافة مرشح إجراء حدث.
4. في حقل "الاسم"، أدخل اسما **كاسم 1** لعامل تصفية إجراءات الحدث.يتم توفير اسم افتراضي، ولكن يمكنك تغييره إلى اسم أكثر معنى.
5. في الحقل النشط، انقر فوق زر **نعم** للإرسال لإضافة عامل التصفية هذا إلى القائمة بحيث يصبح نافذ المفعول على تصفية الأحداث.
6. في الحقل ممكن، انقر فوق زر **نعم** للإرسال لتمكين عامل التصفية.**ملاحظة:** يجب عليك أيضا تحديد خانة الاختيار **إستخدام عوامل تصفية إجراءات الحدث** في علامة التبويب "عوامل تصفية إجراءات الحدث" أو لا يتم تمكين أي من عوامل تصفية إجراءات الحدث بغض النظر عما إذا كنت قد حددت خانة الاختيار **نعم** في مربع الحوار "إضافة عامل تصفية إجراءات الحدث".
7. في حقل معرف التوقيع، قم بإدخال معرفات التوقيع لكل التوقيعات التي يجب تطبيق عامل التصفية هذا عليها.يمكنك إستخدام قائمة، على سبيل المثال، 1000، 1005، أو نطاق، على سبيل المثال، **1000-1005** أو أحد متغيرات SIG إذا قمت بتعريفهم في صفحة متغيرات الحدث. قم بتمهيد المتغير بالدولار.
8. في حقل معرف التوقيع الفرعي، أدخل معرفات التوقيع الفرعي للتواقيع الفرعية التي يجب تطبيق عامل التصفية هذا عليها. على سبيل المثال، **1-5**.
9. دخلت في المهاجم عنوان مجال، العنوان من المصدر مضيف.يمكنك إستخدام أحد المتغيرات إذا قمت بتعريفهم في صفحة متغيرات الحدث. قم بتمهيد المتغير بالدولار. يمكنك أيضا إدخال نطاق من العناوين، على سبيل المثال، **10.89.10.23-10.89.10.10**. الافتراضي هو 0.0.0.0-255.255.255.255.
10. دخلت في المهاجم ميناء مجال، الرقم أيسر يستعمل بالمهاجم in order to أرسلت الربط المخالف.
11. في حقل عنوان الضحية، أدخل عنوان IP الخاص بمضيف المستلم.يمكنك إستخدام أحد المتغيرات إذا قمت بتعريفهم في صفحة متغيرات الحدث. قم بتمهيد المتغير بالدولار. يمكنك أيضا إدخال نطاق من العناوين، على سبيل المثال، **192.56.10.255-192.56.10.1**. الافتراضي هو 0.0.0.0-255.255.255.255.
12. في حقل منفذ الضحية، أدخل رقم المنفذ الذي يستخدمه مضيف الضحية لتلقي الحزمة المخالفة. على سبيل المثال، **0-434**.

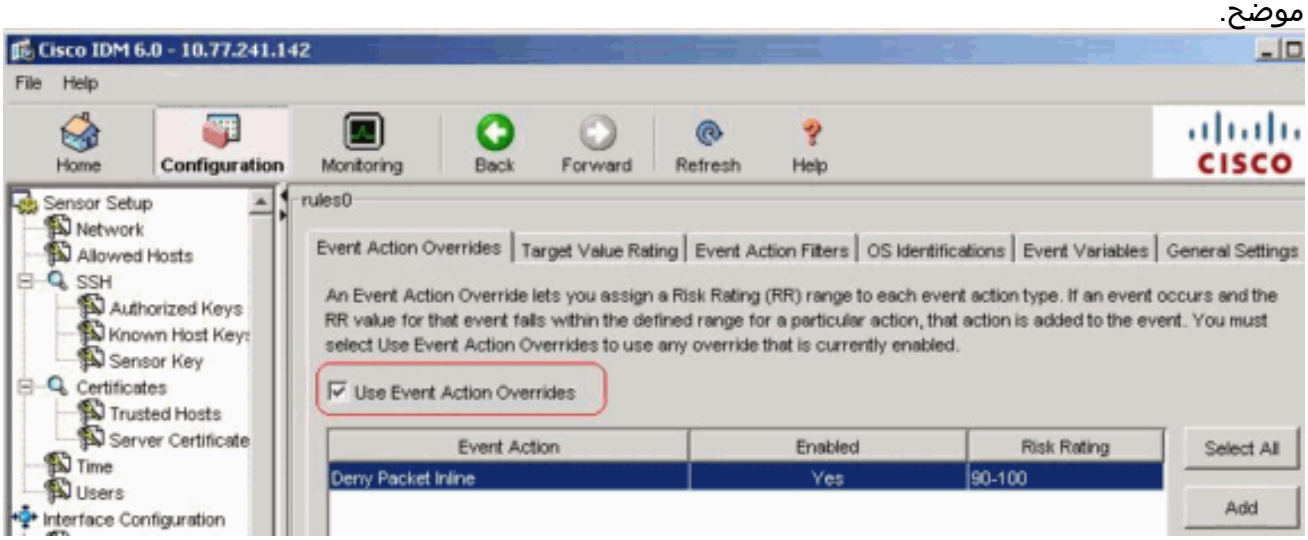
13. في حقل تصنيف المخاطر، أدخل نطاق RR لعامل التصفية هذا. على سبيل المثال، **85-100**.إذا كان RR لحدث ما يقع ضمن النطاق الذي تحدده، فسيتم معالجة الحدث وفقا لمعايير عامل التصفية هذا.
14. من القائمة المنسدلة إجراءات لاستقطاع، أختر الإجراءات التي تريد من عامل التصفية هذا إزالتها من الحدث. على سبيل المثال، أختر **إعادة ضبط اتصال TCP**.**تلميح:** ابق مفتاح **Ctrl مضغوطا** لاختيار أكثر من إجراء حدث واحد في القائمة.
15. في القائمة المنسدلة أهمية نظام التشغيل، أختر ما إذا كنت تريد معرفة ما إذا كان التنبيه ذا صلة بنظام التشغيل الذي تم تعريفه للضحية. على سبيل المثال، أختر **مناسب**.
16. في حقل رفض النسبة المئوية، أدخل النسبة المئوية للحزم لرفض ميزات المهاجم. على سبيل المثال، **90**.الافتراضي هو 100 بالمائة.
17. في حقل إيقاف التطابق، أختر أحد أزرار الانتقاء التالية:**نعم**—إذا كنت تريد أن يتوقف مكون عوامل تصفية إجراءات الحدث عن المعالجة بعد إزالة إجراءات عامل التصفية هذالم تتم معالجة أي عوامل تصفية متبقية، وبالتالي، لا يمكن إزالة أي إجراءات إضافية من الحدث.**لا** — إذا كنت تريد الاستمرار في معالجة عوامل التصفية الإضافية
18. في حقل التعليقات، قم بإدخال أي تعليقات تريد تخزينها مع عامل التصفية هذا، مثل الغرض من عامل التصفية هذا أو لماذا قمت بتكوين عامل التصفية هذا بطريقة معينة. على سبيل المثال، **عامل تصفية جديد**.**تلميح:** انقر فوق **إلغاء الأمر** للتراجع عن تغييراتك وإغلاق مربع الحوار إضافة مرشح إجراء حدث.



19. وانقر فوق **OK**.يظهر الآن عامل تصفية إجراء الحدث الجديد في القائمة الموجودة في علامة التبويب عوامل تصفية إجراء الحدث كما هو موضح.

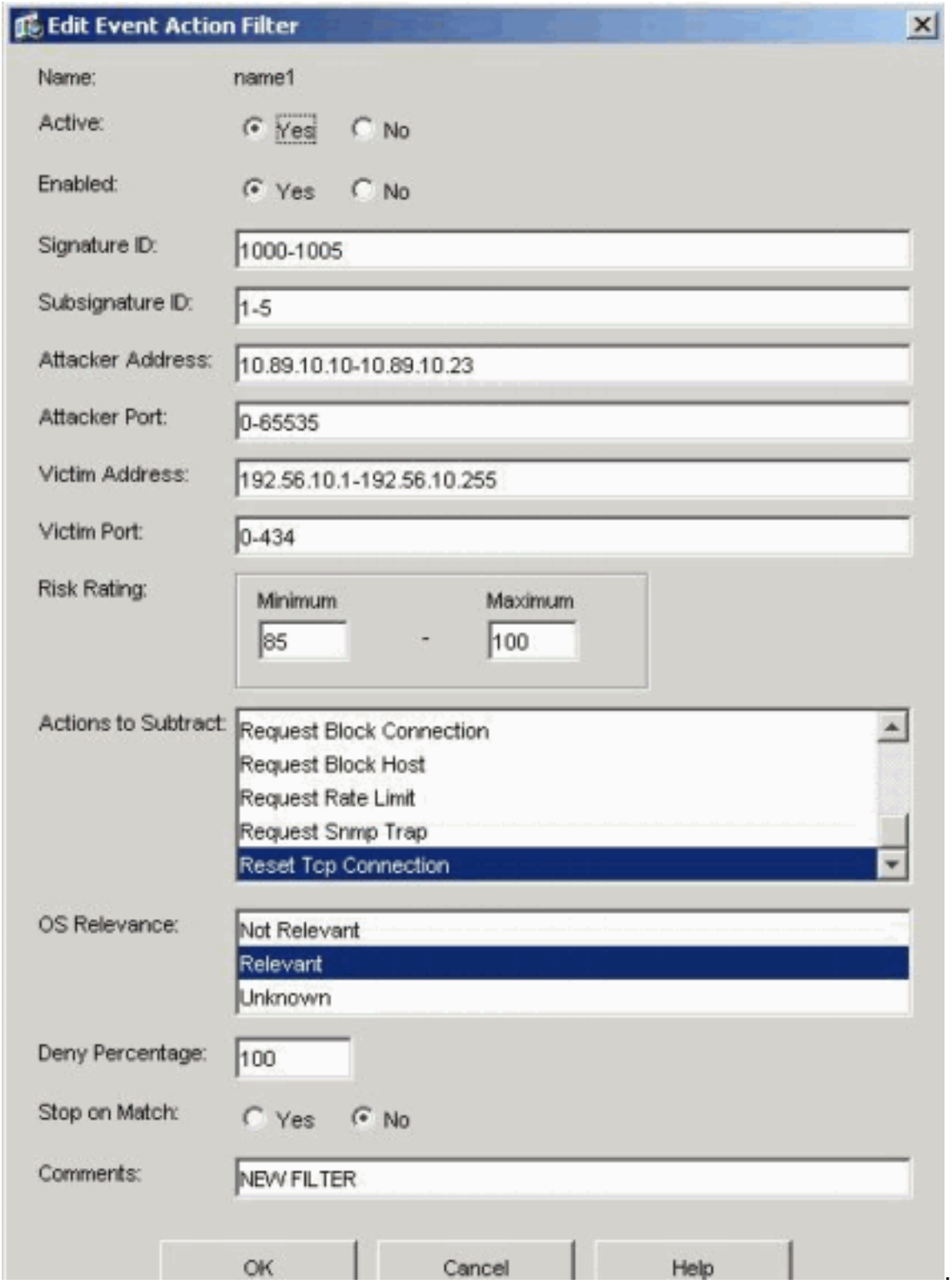


20. حدد خانة الاختيار **إستخدام تجاوزات إجراء الحدث** كما هو موضح.



ملاحظة: يجب عليك تحديد خانة الاختيار **إستخدام تخطيات إجراء الحدث** في علامة التبويب تخطيات إجراء الحدث أو لا يتم تمكين أي من تخطيات إجراء الحدث بغض النظر عن القيمة التي قمت بتعيينها في مربع الحوار إضافة مرشح إجراء الحدث.

21. أختر عامل تصفية إجراء حدث موجود في القائمة لتحريره، ثم انقر فوق **تحرير**.سوف يظهر مربع الحوار تحرير مرشح إجراء



الحدث.

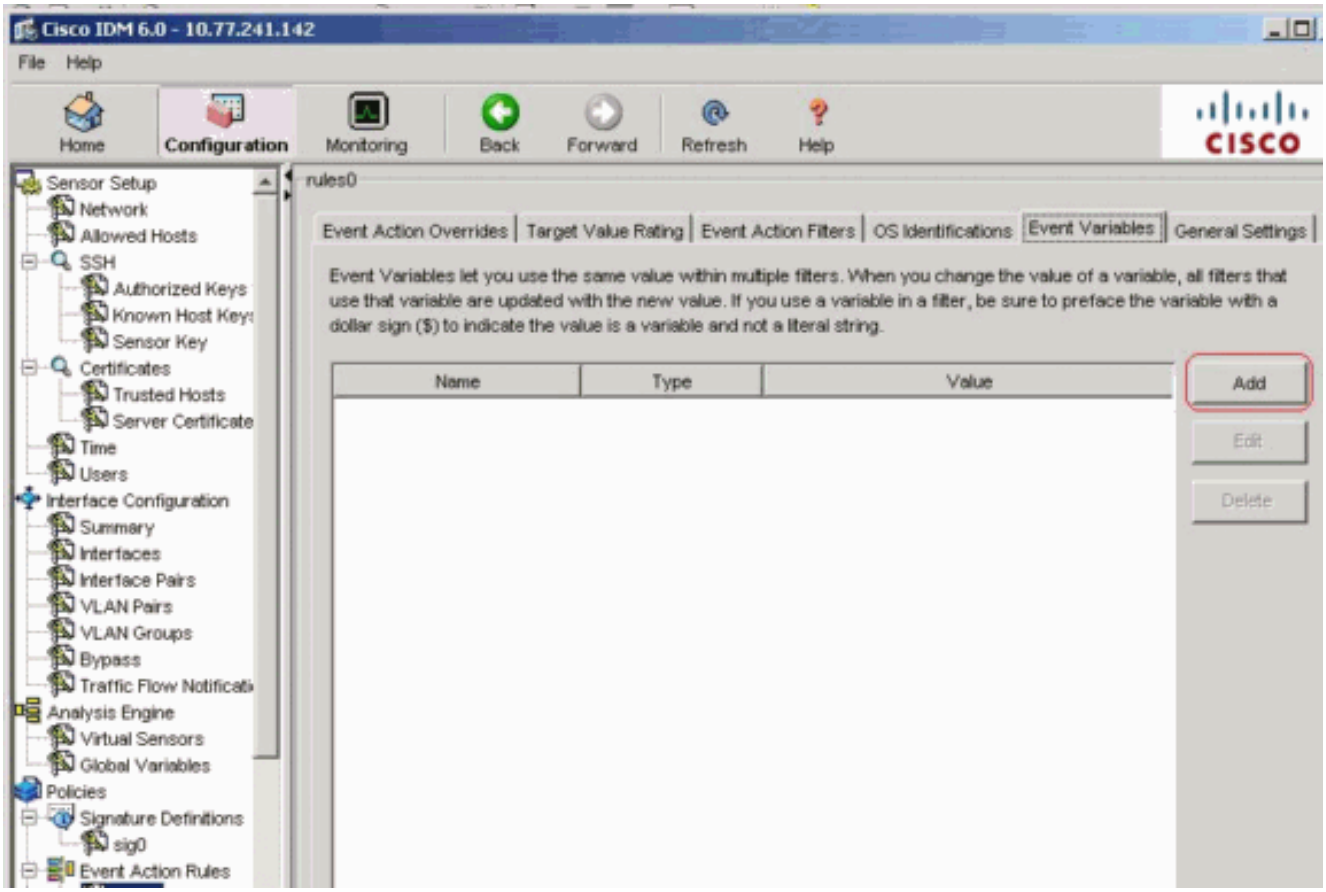
22. قم بتغيير أي قيم في الحقول التي تحتاج لتغييرها.راجع الخطوات من 4 إلى 18 للحصول على معلومات حول كيفية إكمال الحقول.**تلميح:** انقر فوق **إلغاء الأمر** للتراجع عن تغييراتك وإغلاق مربع الحوار تحرير مرشح إجراء الحدث.
23. وانقر فوق **OK**.يظهر الآن عامل تصفية إجراء الحدث الذي تم تحريره في القائمة في علامة التبويب عوامل تصفية إجراء الحدث.
24. حدد خانة الاختيار **إستخدام تجاوزات إجراء الحدث**.**ملاحظة:** يجب عليك تحديد خانة الاختيار **إستخدام تجاوزات إجراءات الحدث** في علامة التبويب تجاوزات إجراءات الحدث أو لا يتم تمكين أي من تخطيات إجراءات الحدث بغض النظر عن القيمة التي قمت بتعيينها في شاشة تحرير مرشح إجراء الحدث.
25. أختر عامل تصفية إجراء حدث في القائمة لحذفه، ثم انقر فوق **حذف**.لم يعد عامل تصفية إجراء الحدث يظهر في القائمة الموجودة في علامة التبويب عوامل تصفية إجراء الحدث.
26. قم بالتصفية لأعلى أو لأسفل في القائمة لنقل إجراء حدث، إختره، ثم انقر **تحريك لأعلى** أو **تحريك لأسفل**.**تلميح:** انقر فوق **إعادة ضبط** لإزالة التغييرات.

27. انقر فوق **تطبيق** لتطبيق التغييرات التي قمت بها وحفظ التكوين الذي تمت مراجعته.

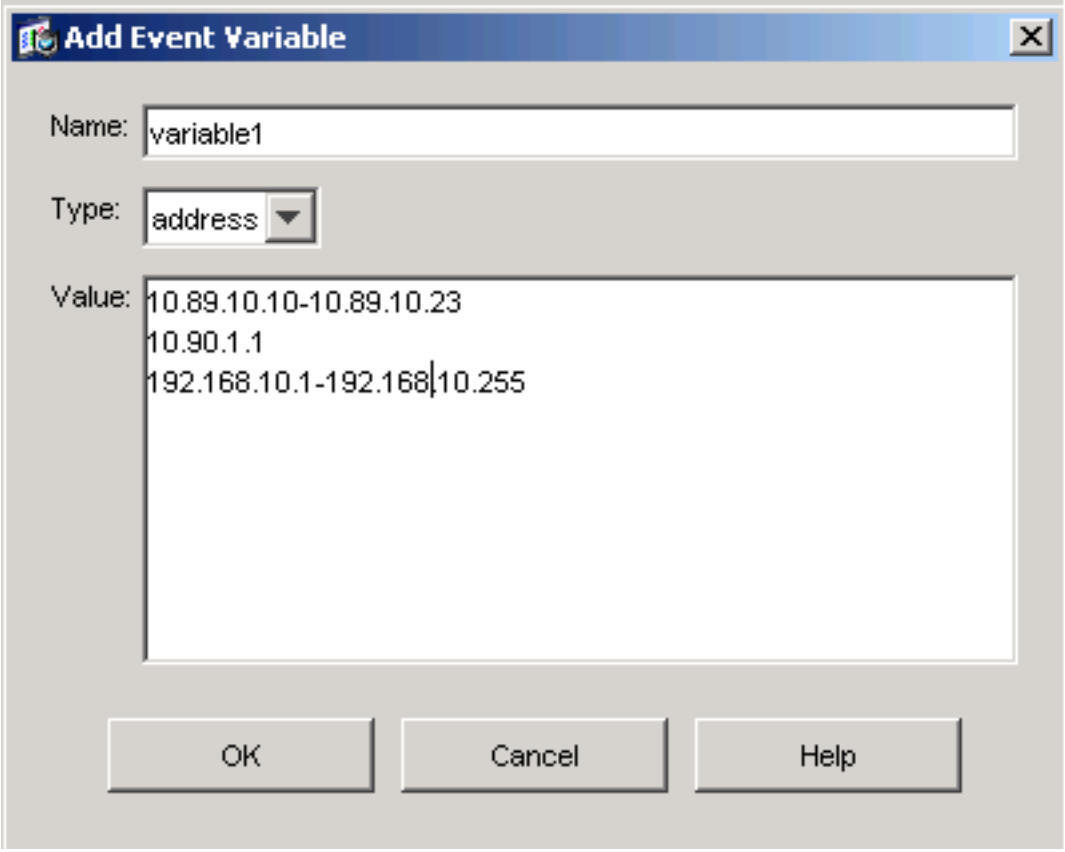
تكوين متغير الحدث

أتمت هذا steps in order to أضفت، حررت، وحذف متغيرات الحدث:

1. سجل الدخول. على سبيل المثال، أستخدم حسابا له امتيازات المسؤول أو عامل التشغيل.
2. أختر **تشكيل > سياسات > قواعد إجراء الحدث > قواعد0 > متغيرات الحدث** إذا كان إصدار البرنامج x.6. بالنسبة للبرنامج الإصدار x.5، أختر **تكوين > قواعد إجراء الحدث > متغيرات الحدث**.سوف تظهر علامة التبويب متغيرات الحدث.

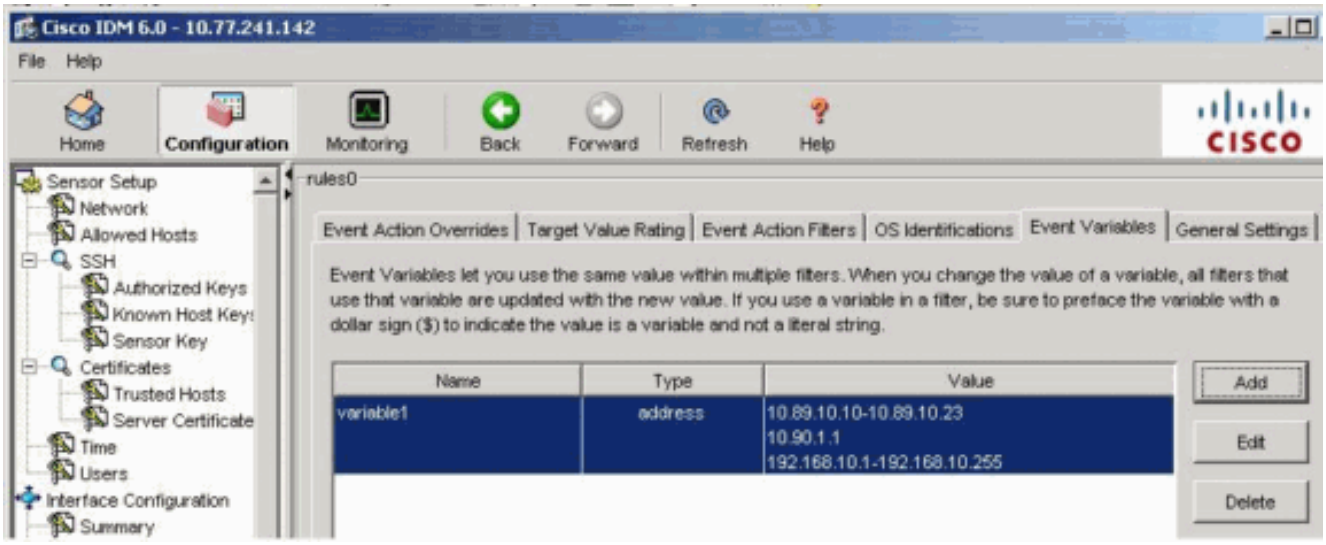


3. طقطقة **يضيف** in order to خلقت متغير.تظهر شاشة إضافة متغير.
4. في حقل "الاسم"، أدخل اسم لهذا المتغير.**ملاحظة:** يمكن أن يحتوي الاسم الصحيح على أرقام أو أحرف فقط. يمكنك أيضا إستخدام واصلة (-) أو شرطة سفلية (_).
5. في حقل القيمة، قم بإدخال القيم لهذا المتغير.حدد عنوان IP الكامل أو النطاقات أو مجموعة النطاقات. على سبيل المثال:10.89.10.10-10.89.10.2310.90.1.1192.168.10.1-192.168.10.255**ملاحظة:** يمكنك إستخدام الفواصل كمحددات. تأكد من عدم وجود مسافات زائدة بعد الفاصلة. وإلا، فستتلقى رسالة خطأ .**تلميح:** انقر فوق **إلغاء الأمر** للتراجع عن تغييراتك وإغلاق مربع الحوار إضافة متغير



الحدث.

6. وانقر فوق **OK**.يظهر المتغير الجديد في القائمة على علامة التبويب متغيرات الحدث.



7. أختر المتغير الموجود في القائمة لتحريره، ثم انقر فوق **تحرير**.سوف يظهر مربع الحوار تحرير متغير الحدث.
8. في حقل القيمة، أدخل التغييرات التي أجريتها على القيمة.
9. وانقر فوق **OK**.يظهر متغير الحدث الذي تم تحريره الآن في القائمة في علامة التبويب متغيرات الحدث.**تلميح:** أختر **إعادة ضبط** لإزالة التغييرات.
10. انقر فوق **تطبيق** لتطبيق التغييرات التي قمت بها وحفظ التكوين الذي تمت مراجعته.

معلومات ذات صلة

- صفحة دعم نظام منع الاقتحام من Cisco
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).