ةزهجأ نيوكت - ثدحألا تارادصإلاو IPS 6.x مادختساب ةيهاظرلا راعشتسالا IME

المحتويات

المقدمة

يشرح هذا المستند وظيفة Analysis Engine وكيفية إنشاء أجهزة الاستشعار الظاهرية على نظام منع التسلل الآمن (IPS) من Cisco وتحريرها وحذفها باستخدام IME) Cisco IPS Manager Express). كما يشرح كيفية تخصيص واجهات للمستشعر الظاهري.

ملاحظة: لا يدعم كل من AIM-IPS و NME-IPS المحاكاة الافتراضية.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات أساسية خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- جهاز Cisco 4200 Series IPS الذي يشغل الإصدار 6.0 من البرنامج والإصدارات الأحدث
- Cisco IPS Manager Express (IME)، الإصدار 6.1.1 والإصدارات الأحدث**ملاحظة:** بينما يمكن إستخدام IME لمراقبة أجهزة الاستشعار التي تعمل بنظام Cisco IPS 5.0 والإصدارات الأحدث، فإن بعض الميزات والوظائف الجديدة التي يتم توفيرها في IME مدعومة فقط على أجهزة الاستشعار التي تعمل بنظام Cisco IPS 6.1 أو إصدار أحدث.**ملاحظة:** يدعم نظام Cisco لمنع التسلل الآمن (IPS) 5.x المستشعر الافتراضي فقط مقابل0. يتم دعم أجهزة الاستشعار الظاهرية الأخرى غير الافتراضية vs0 في بروتوكول IPS 6.x والإصدارات الأحدث.

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

المنتجات ذات الصلة

يمكن إستخدام هذا التكوين أيضا مع أجهزة الاستشعار هذه:

- IPS-4240
- الطراز IPS-4255
- IPS-4260
- IPS-4270-20
- AIP-SSM

الاصطلاحات

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

معلومات أساسية

حول محرك التحليل

يقوم محرك التحليل بتحليل الحزمة واكتشاف التنبيه. إنه يراقب حركة مرور أن يتدفق عبر قارن محدد. يمكنك إنشاء أجهزة إستشعار افتراضية في Analysis Engine. يحتوي كل مستشعر ظاهري على اسم فريد مع قائمة من الواجهات وأزواج الواجهة المضمنة وأزواج شبكات VLAN المضمنة ومجموعات شبكات VLAN المقترنة به. لتجنب مشاكل ترتيب التعريف، لا يسمح بأي تعارضات أو تداخلات في التعيينات. أنت تعين قارن، قارن مضغوط، أزواج VLAN مضمنة، ومجموعات VLAN إلى مستشعر ظاهري خاص بحيث لا تتم معالجة أي حزمة بواسطة أكثر من مستشعر ظاهري واحد. كما يتم إقران كل مستشعر ظاهري بتعريف توقيع مسمى بشكل خاص وقواعد إجراء الحدث وتكوين اكتشاف الأخطاء. يتم التخلص من الحزم من الواجهات، وأزواج الواجهة المضمنة، وأزواج شبكات VLAN المضمنة، ومجموعات VLAN التي لا يتم تعيينها إلى أي مستشعر ظاهري استنادا إلى تكوين الالتفاف داخل السطر.

حول أجهزة الاستشعار الظاهرية

يمكن للمستشعر تلقي مدخلات البيانات من واحد أو أكثر من تدفقات البيانات المراقبة. هذا monitore معطيات تيار يستطيع إما كنت قارن طبيعي ميناء أو قارن ظاهري ميناء. على سبيل المثال، يمكن لمستشعر واحد مراقبة حركة مرور البيانات من أمام جدار الحماية، أو من خلف جدار الحماية، أو من أمام جدار الحماية ووراءه في نفس الوقت. ويمكن

لمستشعر واحد مراقبة تدفق بيانات أو أكثر. في هذه الحالة، يتم تطبيق سياسة مستشعر واحدة أو تكوين واحد على جميع تدفقات البيانات المراقبة. المستشعر الظاهري هو مجموعة بيانات معرفة بواسطة مجموعة من سياسات التكوين. يتم تطبيق المستشعر الظاهري على مجموعة من الحزم كما هو محدد بواسطة مكون الواجهة. يمكن للمستشعر الظاهري مراقبة مقاطع متعددة، كما يمكنك تطبيق سياسة أو تكوين مختلف لكل مستشعر افتراضي داخل مستشعر مادي واحد. يمكنك إعداد نهج مختلف لكل مقطع مراقب تحت التحليل. يمكنك أيضا تطبيق نفس مثيل النهج، على سبيل المثال، sig0 أو rules0 أو ad0، على أجهزة إستشعار ظاهرية مختلفة. يمكنك تخصيص الواجهات وأزواج الواجهة المضمنة وأزواج شبكات VLAN المضمنة ومجموعات VLAN للمستشعر الظاهري.

ملاحظة: لا يدعم نظام Cisco لمنع الاقتحام الآمن (IPS) أكثر من أربعة أجهزة إستشعار افتراضية. المستشعر الافتراضي هو vs0. لا يمكنك حذف المستشعر الظاهري الافتراضي. تعد قائمة الواجهة ووضع عملية اكتشاف الأخطاء ووضع تعقب جلسة عمل TCP المضمنة ووصف المستشعر الظاهري ميزات التكوين الوحيدة التي يمكنك تغييرها للمستشعر الظاهري الافتراضي. لا يمكنك تغيير تعريف التوقيع أو قواعد إجراء الحدث أو نهج الكشف عن الأخطاء.

مزايا وقيود المحاكاة الافتراضية

مزايا المحاكاة الافتراضية

تتمتع المحاكاة الافتراضية بهذه الميزات:

- يمكنك تطبيق تكوينات مختلفة على مجموعات مختلفة من حركة المرور.
- يمكنك مراقبة شبكتين بمسافات IP متداخلة باستخدام مستشعر واحد.
- أنت يستطيع راقبت على حد سواء داخل وخارج جدار حماية أو جهاز nat.

قيود المحاكاة الافتراضية

تفرض المحاكاة الافتراضية هذه القيود:

- يجب تعيين كلا جانبي حركة المرور غير المتماثلة إلى المستشعر الظاهري نفسه.
- لا يتوافق إستخدام التقاط VACL أو فسحة بين دعامتين (المراقبة المختلطة) مع إعتبار تمييز شبكة VLAN، والذي يسبب مشاكل مع مجموعات VLAN.عندما يستعمل أنت cisco ios برمجية، VACL التقاط ميناء أو فسحة بين دعامتين غاية لا يستلم دائما حددت ربط even if هو يكون شكلت ل trunking.عندما تستخدم MSFC، يؤدي التحويل السريع للمسار للمسارات المتعلمة إلى تغيير سلوك التقاط VACL وفسحة بين دعامتين.
- المخزن الدائم محدود.

متطلبات المحاكاة الافتراضية

تشتمل المحاكاة الافتراضية على متطلبات التقاط حركة مرور البيانات هذه:

- يجب أن يستلم المستشعر الظاهري حركة مرور أن يتلقى 802.1Q رؤوس، بخلاف حركة مرور البيانات على شبكة VLAN الأصلية من الالتقاط ميناء.
- يجب أن يرى المستشعر كلا الاتجاهين لحركة المرور في مجموعة VLAN نفسها في المستشعر الظاهري نفسه لأي مستشعر معين.

التكوين

في هذا القسم، تقدم لك معلومات لإضافة أجهزة الاستشعار الظاهرية وتحريرها وحذفها.

إضافة أجهزة إستشعار افتراضية

قم بإصدار الأمر virtual-sensor name في الوضع الفرعي لمحرك تحليل الخدمة من أجل إنشاء مستشعر ظاهري. تقوم بتعيين النهج (اكتشاف الأخطاء وقواعد إجراءات الحدث وتعريف التوقيع) للمستشعر الظاهري. ثم تقوم بتخصيص الواجهات (المختلطة، وأزواج الواجهة المضمنة، وأزواج شبكات VLAN المضمنة، ومجموعات VLAN) للمستشعر الظاهري. يجب تكوين أزواج الواجهة المضمنة وأزواج شبكات VLAN قبل أن تتمكن من تخصيصها لمستشعر ظاهري. يتم تطبيق هذه الخيارات:

- **اكتشاف** الأخطاء—معلمات اكتشاف الأخطاء.اسم **اكتشاف** الأخطاء **-** اسم نهج اكتشاف الأخطاء**وضع التشغيل**—وضع اكتشاف الأخطاء (**غير نشط، تعلم، كشف**)
- **الوصف** — وصف المستشعر الظاهري
- **الحدث - الإجراء - القواعد** - اسم سياسة قواعد إجراءات الحدث
- **inline-TCP-evasion-protection-mode**—يتيح لك إختيار أي نوع من الوضع القياسي تحتاج إلى فحص حركة مرور البيانات:**غير المتماثل**— يمكن أن ترى فقط إتجاه واحد لتدفق حركة المرور ثنائي الإتجاه. تعمل حماية الوضع غير المتماثل على إسترخاء حماية التهرب في طبقة TCP.**ملاحظة:** يتيح الوضع غير المتماثل قيام المستشعر بتزامن الحالة مع التدفق ويحافظ على فحص تلك المحركات التي لا تتطلب كلا الاتجاهين. يقلل الوضع غير المتماثل من الأمان لأن الحماية الكاملة تتطلب رؤية كلا جانبي حركة المرور.**صارم**— إذا تم فقد حزمة لأي سبب، فلن تتم معالجة جميع الحزم بعد الحزمة التي تم فقدها. توفر الحماية الصارمة للتهرب الإنفاذ الكامل لحالة TCP وتتبع التسلسل.**ملاحظة:** يمكن أن ينتج عن أي حزم غير مرتبة أو حزم فائتة توقيعات محركات التكييف 1300 أو 1330 تجريدات، والتي تحاول تصحيح الوضع، ولكن يمكن أن ينتج عنها إتصالات مرفوضة.
- **inline-TCP-session-tracking-mode**— أسلوب متقدم أن يسمح أنت أن يعين مضاعفة TCP جلسة في خط حركة مرور. الافتراضي هو المستشعر الافتراضي، والذي هو دائما تقريبا أفضل خيار.**Virtual-Sensor** —تنتمي جميع الحزم ذات مفتاح جلسة العمل نفسه (AaBb) داخل مستشعر ظاهري إلى نفس جلسة العمل.**interface-and-vlan**— تنتمي جميع الحزم ذات مفتاح الجلسة نفسه (ABb) في شبكة VLAN نفسها (أو زوج شبكة VLAN داخلي) وعلى الواجهة نفسها إلى الجلسة نفسها. يتم تعقب الحزم ذات المفتاح نفسه ولكن على شبكات VLAN أو الواجهات المختلفة بشكل مستقل.**vlan-only**— تنتمي جميع الحزم ذات مفتاح الجلسة نفسه (ABb) في شبكة VLAN نفسها (أو زوج شبكة VLAN داخلي) بغض النظر عن الواجهة إلى نفس الجلسة. يتم تعقب الحزم ذات المفتاح نفسه ولكن على شبكات VLAN المختلفة بشكل مستقل.
- **تعريف التوقيع**- اسم نهج تعريف التوقيع
- **الواجهات المنطقية** — اسم الواجهات المنطقية (أزواج الواجهة المضمنة)
- **الواجهات المادية** — اسم الواجهات المادية (المختلطة، أزواج VLAN المضمنة، ومجموعات VLAN)**subinterface-number**—رقم الواجهة الفرعية المادية. إذا كان نوع الواجهة الفرعية بلا، فإن قيمة 0 تشير إلى تعيين الواجهة بالكامل في الوضع المختلطة.**لا** — يزيل مدخل أو تحديد

لإضافة مستشعر ظاهري، أكمل الخطوات التالية:

1. قم بتسجيل الدخول إلى CLI باستخدام حساب له امتيازات المسؤول.
2. أدخل وضع تحليل الخدمة.
```
sensor# configure terminal

sensor(config)# service analysis-engine

#(sensor(config-ana
```
3. إضافة مستشعر ظاهري.
```
sensor(config-ana)# virtual-sensor vs2

#(sensor(config-ana-vir
```
4. أضف وصفا لهذا المستشعر الظاهري.
```
sensor(config-ana-vir)# description virtual sensor 2
```
5. قم بتعيين نهج كشف الأخطاء ووضع التشغيل لهذا المستشعر الظاهري.
```
sensor(config-ana-vir)# anomaly-detection

sensor(config-ana-vir-ano)# anomaly-detection-name ad1
```

```
sensor(config-ana-vir-ano)# operational-mode learn
```

6. قم بتعيين نهج قواعد إجراءات الحدث إلى هذا المستشعر الظاهري.
```
sensor(config-ana-vir-ano)# exit

sensor(config-ana-vir)# event-action-rules rules1
```

7. قم بتعيين نهج تعريف توقيع إلى هذا المستشعر الظاهري.
```
sensor(config-ana-vir)# signature-definition sig1
```

8. قم بتعيين وضع تعقب جلسة عمل TCP المضمنة.
```
sensor(config-ana-vir)# inline-TCP-session-tracking-mode virtual-sensor
```

الوضع الافتراضي هو وضع المستشعر الظاهري، وهو دائما تقريبا أفضل خيار للاختيار.

9. قم بتعيين وضع حماية التهرب من بروتوكول TCP المضمن.
```
sensor(config-ana-vir)# inline-TCP-evasion-protection-mode strict
```

الوضع الافتراضي هو الوضع المقيد، والذي غالبا ما يكون أفضل خيار للاختيار.

10. عرض قائمة الواجهات المتاحة.
```
? sensor(config-ana-vir)# physical-interface

.GigabitEthernet0/0     GigabitEthernet0/0 physical interface

.GigabitEthernet0/1     GigabitEthernet0/1 physical interface

.GigabitEthernet2/0     GigabitEthernet0/2 physical interface

.GigabitEthernet2/1     GigabitEthernet0/3 physical interface

sensor(config-ana-vir)# physical-interface

? sensor(config-ana-vir)# logical-interface

<none available>
```

11. قم بتعيين واجهات الوضع المختلطة التي تريد إضافتها إلى هذا المستشعر الظاهري.
```
sensor(config-ana-vir)# physical-interface GigabitEthernet0/2
```

كرر هذه الخطوة لجميع الواجهات المختلطة التي تريد تعيينها على هذا المستشعر الظاهري.

12. قم بتعيين أزواج الواجهة المضمنة التي تريد إضافتها إلى هذا المستشعر الظاهري.
```
sensor(config-ana-vir)# logical-interface inline_interface_pair_name
```

يجب أن تكون قد قمت بالفعل بإقران الواجهات.

13. قم بتخصيص الواجهات الفرعية لأزواج أو مجموعات VLAN المضمنة التي تريد إضافتها إلى هذا المستشعر الظاهري كما هو موضح أدناه:
```
sensor(config-ana-vir)# physical-interface GigabitEthernet2/0 subinterface-number
subinterface_number
```

أنت ينبغي يتلقى بالفعل قسمت أي قارن داخل أزواج أو مجموعات VLAN.

14. تحقق من إعدادات المستشعر الظاهري.
```
sensor(config-ana-vir)# show settings

name: vs2

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

:description: virtual sensor 1 default
```

```
                                    signature-definition: sig1 default: sig0

                                  event-action-rules: rules1 default: rules0

                                                        anomaly-detection

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

                                    anomaly-detection-name: ad1 default: ad0

                                     operational-mode: learn default: detect

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

                            (physical-interface (min: 0, max: 999999999, current: 2

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

                                                    name: GigabitEthernet0/2

                                          <subinterface-number: 0 <defaulted

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

        inline-TCP-session-tracking-mode: virtual-sensor default: virtual-sensor

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

                             (logical-interface (min: 0, max: 999999999, current: 0

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

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

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

                                                        #(sensor(config-ana-vir
```

15. خرجت تحليل محرك أسلوب.

```
sensor(config-ana-vir)# exit

sensor(config-ana)# exit

#(sensor(config

:[Apply Changes:?[yes
```

16. اضغط على **Enter** لتطبيق التغييرات أو أدخل **no** لتجاهلها.

يؤدي هذا إلى اكتمال العملية لإضافة مستشعر ظاهري إلى نظام منع التسلل الآمن (IPS) من Cisco. أكمل الإجراء نفسه لإضافة المزيد من أجهزة الاستشعار الظاهرية.

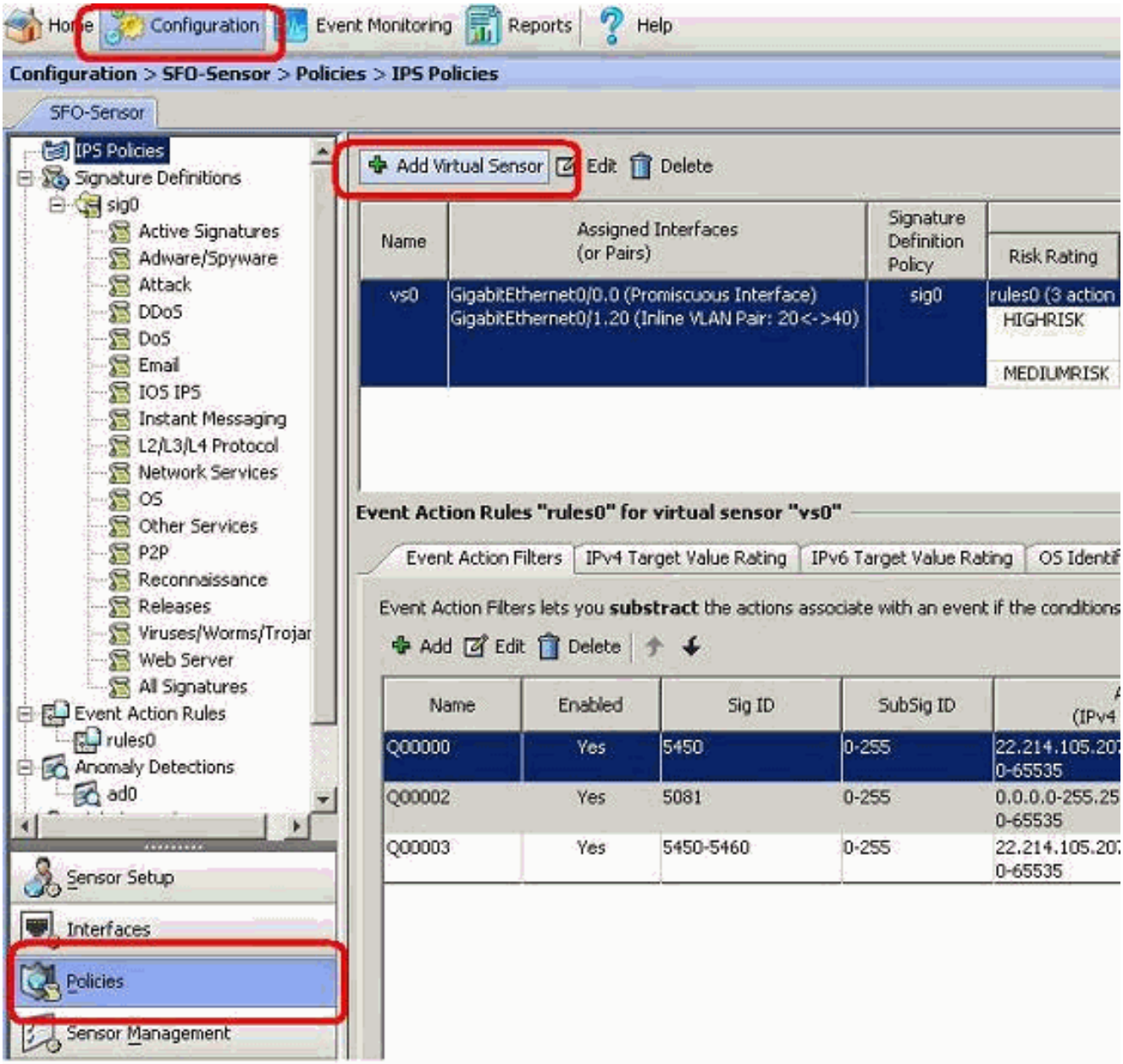
ملاحظة: لا يدعم نظام Cisco لمنع الاقتحام الآمن (IPS) أكثر من أربعة أجهزة إستشعار افتراضية. المستشعر الافتراضي هو vs0.

إضافة مستشعر ظاهري باستخدام IME

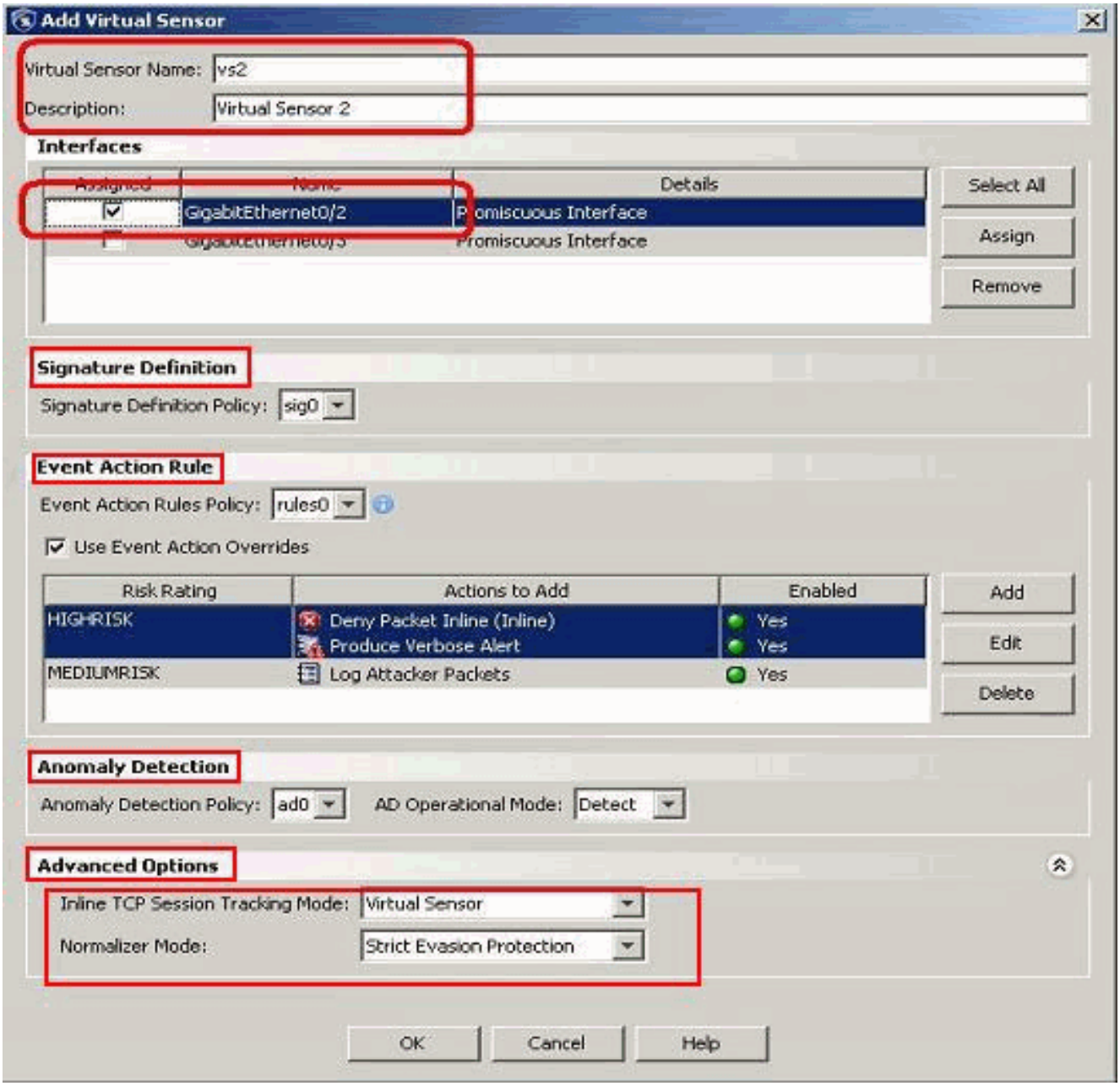
أكمل هذه الخطوات لتكوين مستشعر ظاهري على نظام منع التسلل الآمن (IPS) من Cisco باستخدام Cisco IPS Manager Express:

1. أخترت **تشكيل>SFO-Sensor> سياسة> IPS**. ثم انقر فوق **إضافة المستشعر الظاهري** كما هو موضح في

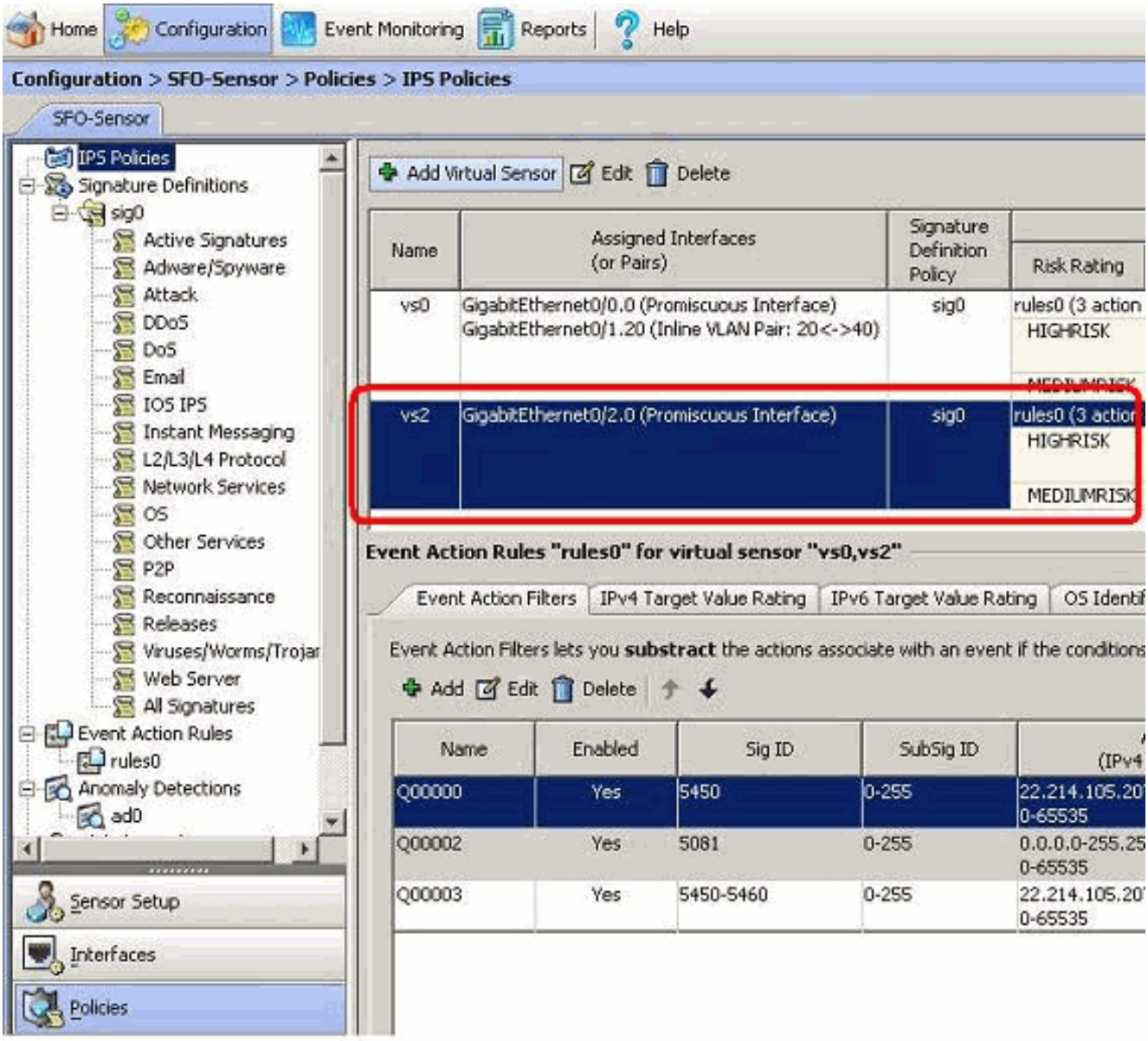
لقطة
الشاشة.



2. قم بتسمية المستشعر الظاهري (VS2 في هذا المثال) وإضافة وصف إلى المستشعر الظاهري في المساحة المتوفرة. قم أيضا بتعيين واجهات الوضع المختلطة التي تريد إضافتها إلى هذا المستشعر الظاهري. يتم إختيار إيثرنت جيجابت 2/0 هنا. قم الآن بتوفير التفاصيل في أقسام **تعريف التوقيع** و**قاعدة إجراء الحدث** و**اكتشاف الأخطاء** و**الخيارات المتقدمة** كما هو موضح في لقطة الشاشة.ضمن **الخيارات المتقدمة** توفر تفاصيل حول وضع تعقب جلسة عمل TCP ووضع التطبيع. هنا **ال TCP جلسة تعقب أسلوب مستشعر ظاهري** وال **NormalMode** هو **يقيد التهرب حماية** أسلوب.



3. وانقر فوق **OK**.
4. المستشعر الظاهري VS2 الذي تمت إضافته حديثا يظهر في قائمة أجهزة الاستشعار الظاهرية. انقر فوق **تطبيق** للحصول على تكوين المستشعر الظاهري الجديد الذي سيتم إرساله إلى نظام Cisco Secure Intrusion Prevention System (IPS).



يؤدي هذا إلى اكتمال التكوين لإضافة مستشعر ظاهري.

تحرير أجهزة الاستشعار الظاهرية

يمكن تحرير هذه المعلمات للمستشعر الظاهري:

- نهج تعريف التوقيع
- سياسة قواعد إجراءات الحدث
- نهج كشف الأخطاء
- وضع تشغيل اكتشاف الأخطاء
- وضع تعقب جلسة عمل TCP المضمنة
- الوصف
- الواجهات المعينة

لتحرير مستشعر ظاهري، أكمل الخطوات التالية:

1. قم بتسجيل الدخول إلى CLI باستخدام حساب له امتيازات المسؤول.
2. أدخل وضع تحليل الخدمة.

```
sensor# configure terminal

sensor(config)# service analysis-engine
```

```
#(sensor(config-ana
```

3. قم بتحرير المستشعر الظاهري، vs1.

```
sensor(config-ana)# virtual-sensor vs2

#(sensor(config-ana-vir
```

4. تحرير وصف هذا المستشعر الظاهري.

```
sensor(config-ana-vir)# description virtual sensor A
```

5. قم بتغيير نهج الكشف عن الأخطاء ووضع التشغيل المعين لهذا المستشعر الظاهري.

```
sensor(config-ana-vir)# anomaly-detection

sensor(config-ana-vir-ano)# anomaly-detection-name ad0

sensor(config-ana-vir-ano)# operational-mode learn
```

6. قم بتغيير نهج قواعد إجراءات الحدث المعينة إلى هذا المستشعر الظاهري.

```
sensor(config-ana-vir-ano)# exit

sensor(config-ana-vir)# event-action-rules rules0
```

7. تغيير نهج تعريف التوقيع المعين إلى هذا المستشعر الظاهري.

```
sensor(config-ana-vir)# signature-definition sig0
```

8. تغيير وضع تعقب جلسة عمل TCP المضمنة.

```
sensor(config-ana-vir)# inline-TCP-session-tracking-mode interface-and-vlan
```

الوضع الافتراضي هو وضع المستشعر الظاهري، وهو دائما تقريبا أفضل خيار للاختيار.

9. عرض قائمة الواجهات المتاحة.

```
? sensor(config-ana-vir)# physical-interface

.GigabitEthernet0/0     GigabitEthernet0/0 physical interface

.GigabitEthernet0/1     GigabitEthernet0/1 physical interface

.GigabitEthernet2/0     GigabitEthernet0/2 physical interface

.GigabitEthernet2/1     GigabitEthernet0/3 physical interface

sensor(config-ana-vir)# physical-interface

? sensor(config-ana-vir)# logical-interface

<none available>
```

10. قم بتغيير واجهات الوضع المختلطة المعينة إلى هذا المستشعر الظاهري.

```
sensor(config-ana-vir)# physical-interface GigabitEthernet0/2
```

11. قم بتغيير أزواج الواجهة المضمنة التي تم تعيينها إلى هذا المستشعر الظاهري.

```
sensor(config-ana-vir)# logical-interface inline_interface_pair_name
```

يجب أن تكون قد قمت بالفعل بإقران الواجهات.

12. قم بتغيير الواجهة الفرعية باستخدام أزواج أو مجموعات VLAN المضمنة التي تم تعيينها لهذا المستشعر الظاهري.

```
sensor(config-ana-vir)# physical-interface GigabitEthernet2/0 subinterface-number
subinterface_number
```

أنت ينبغي يتلقى بالفعل قسمت أي قارن داخل أزواج أو مجموعات VLAN.

13. تحقق من إعدادات المستشعر الظاهري المحررة.

```
sensor(config-ana-vir)# show settings
```

```
                                                    name: vs2
                                    ----------------------------------------------
                                         :description: virtual sensor 1 default
                                       signature-definition: sig1 default: sig0
                                      event-action-rules: rules1 default: rules0
                                                        anomaly-detection
                                    ----------------------------------------------
                                        anomaly-detection-name: ad1 default: ad0
                                         operational-mode: learn default: detect
                                    ----------------------------------------------
                                (physical-interface (min: 0, max: 999999999, current: 2
                                    ----------------------------------------------
                                                    name: GigabitEthernet0/2
                                          <subinterface-number: 0 <defaulted
                                    ----------------------------------------------
inline-TCP-session-tracking-mode: interface-and-vlan default: virtual-sensor
                                    ----------------------------------------------
                                 (logical-interface (min: 0, max: 999999999, current: 0
                                    ----------------------------------------------
                                    ----------------------------------------------
                                       ----------------------------------------------

                                                    #(sensor(config-ana-vir
```

14. خرجت تحليل محرك أسلوب.

```
sensor(config-ana)# exit

#(sensor(config

:[Apply Changes:?[yes
```

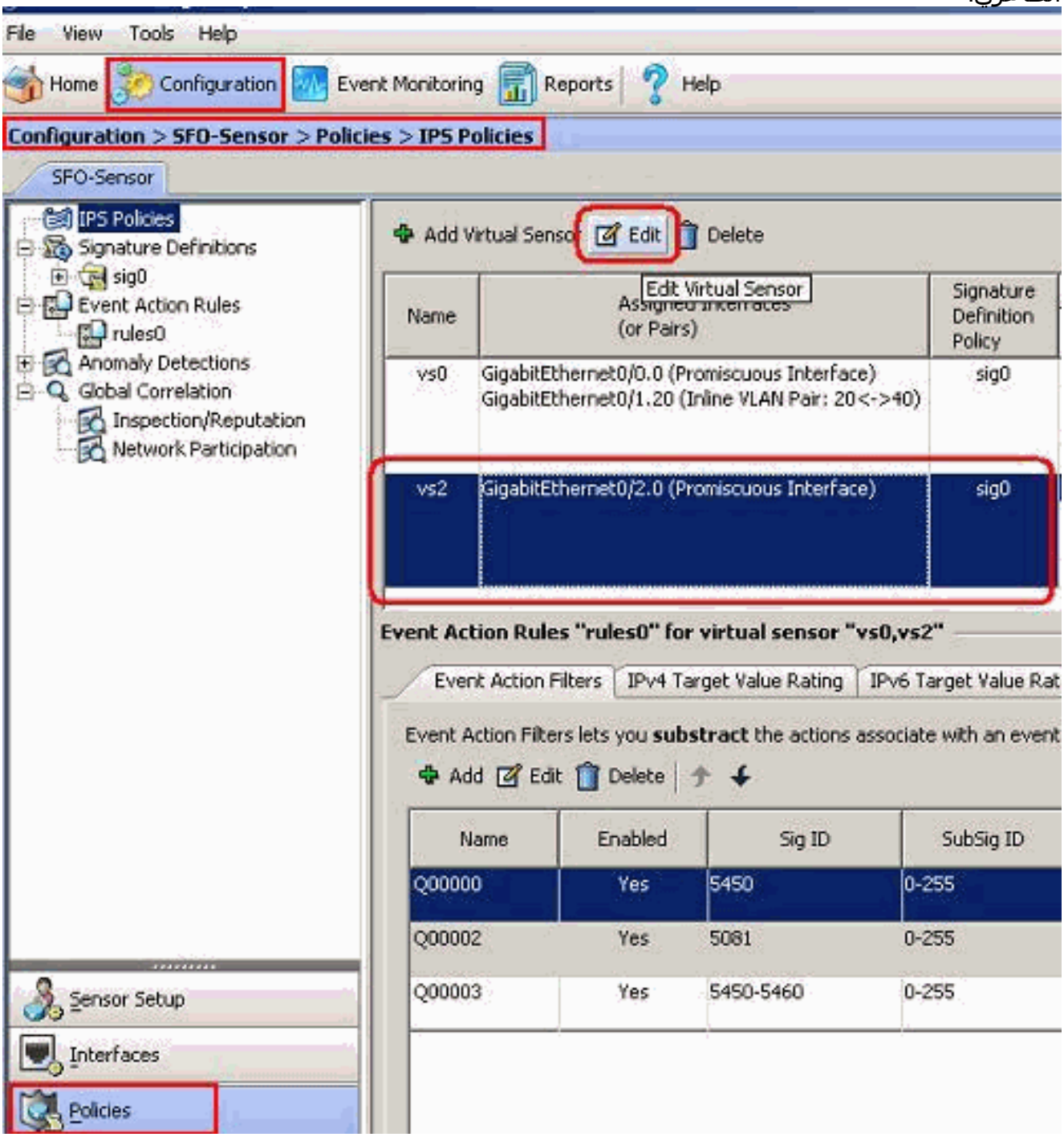
15. اضغط على **Enter** لتطبيق التغييرات أو أدخل **no** لتجاهلها.

تحرير المستشعر الظاهري باستخدام IME

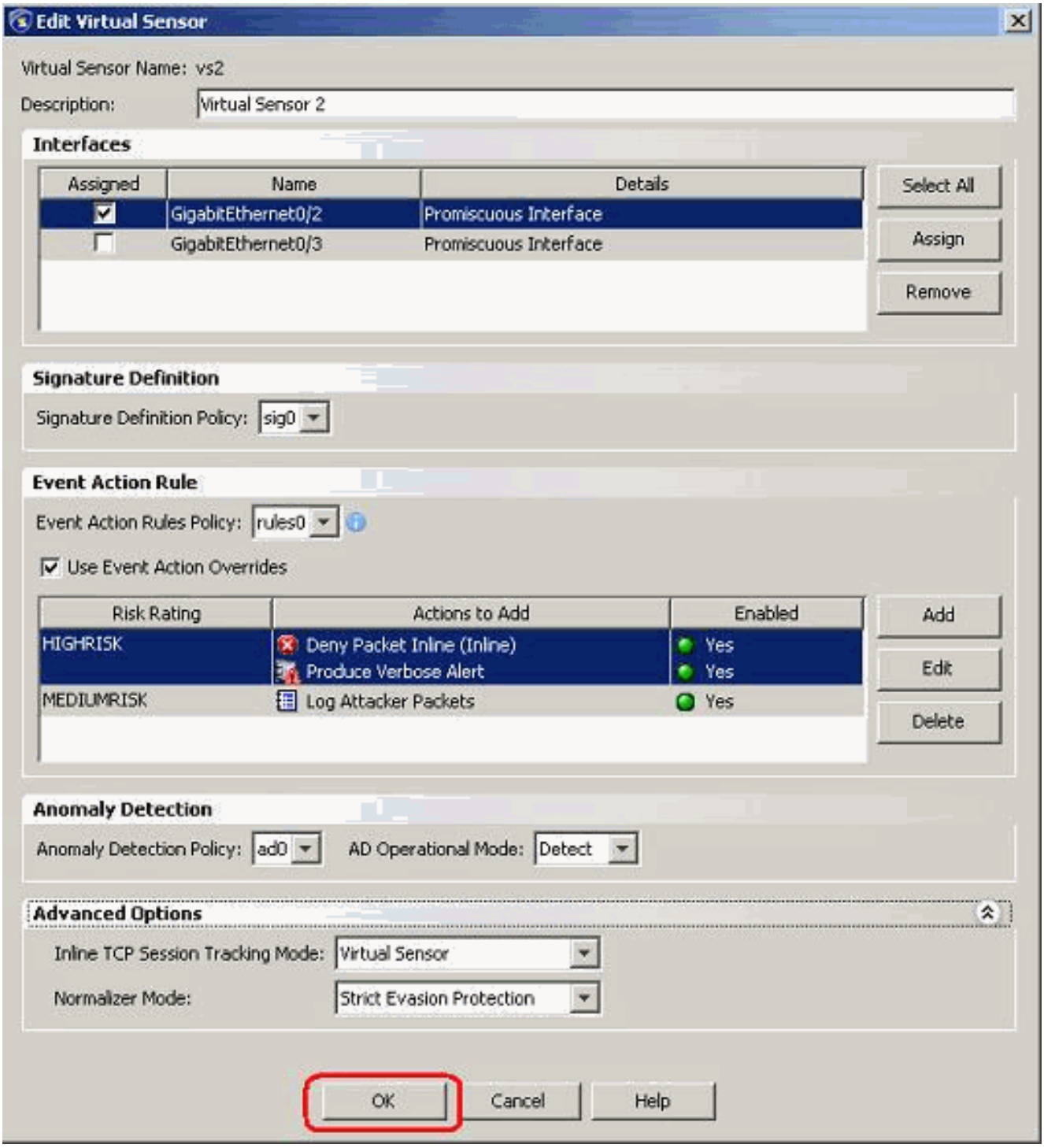
أكمل هذه الخطوات لتحرير مستشعر ظاهري على نظام منع التسلل الآمن (IPS) من Cisco باستخدام Cisco IPS Manager Express:

1. أخترت **تشكيل>SFO-Sensor> سياسة> IPS**.
2. أختر المستشعر الظاهري المراد تحريره، ثم انقر فوق **تحرير** كما هو موضح في لقطة الشاشة. في هذا المثال VS2، يتم تحرير المستشعر

الظاهري.



3. في نافذة Edit Virtual Sensor"، قم بإجراء تغييرات على معلمات المستشعر الظاهري الموجود ضمن **تعريف توقيع** الأقسام، و**قاعدة إجراء الحدث**، و**اكتشاف الأخطاء** و**الخيارات المتقدمة**. انقر فوق **موافق**، ثم انقر فوق **تطبيق**.



يؤدي هذا إلى اكتمال عملية تحرير مستشعر ظاهري.

حذف أجهزة الاستشعار الظاهرية

لحذف مستشعر ظاهري، أكمل الخطوات التالية:

1. لحذف مستشعر ظاهري، قم بإصدار الأمر **no virtual-sensor**.

```
sensor(config-ana)# virtual-sensor vs2

                #(sensor(config-ana-vir

sensor(config-ana-vir)# exit

sensor(config-ana)# no virtual-sensor vs2
```

2. تحقق من المستشعر الظاهري المحذوف.

```
sensor(config-ana)# show settings

                                global-parameters

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

                                    ip-logging

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

          <max-open-iplog-files: 20 <defaulted

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

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

     (virtual-sensor (min: 1, max: 255, current: 2

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

                                <protected entry>

                             <name: vs0 <defaulted

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

  <description: default virtual sensor <defaulted

           <signature-definition: sig0 <protected

           <event-action-rules: rules0 <protected

                             anomaly-detection

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

       <anomaly-detection-name: ad0 <protected

          <operational-mode: detect <defaulted

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

(physical-interface (min: 0, max: 999999999, current: 0

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

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

 (logical-interface (min: 0, max: 999999999, current: 0

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

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

                                #(sensor(config-ana
```

المستشعر الافتراضي فقط، **vs0**، موجود.

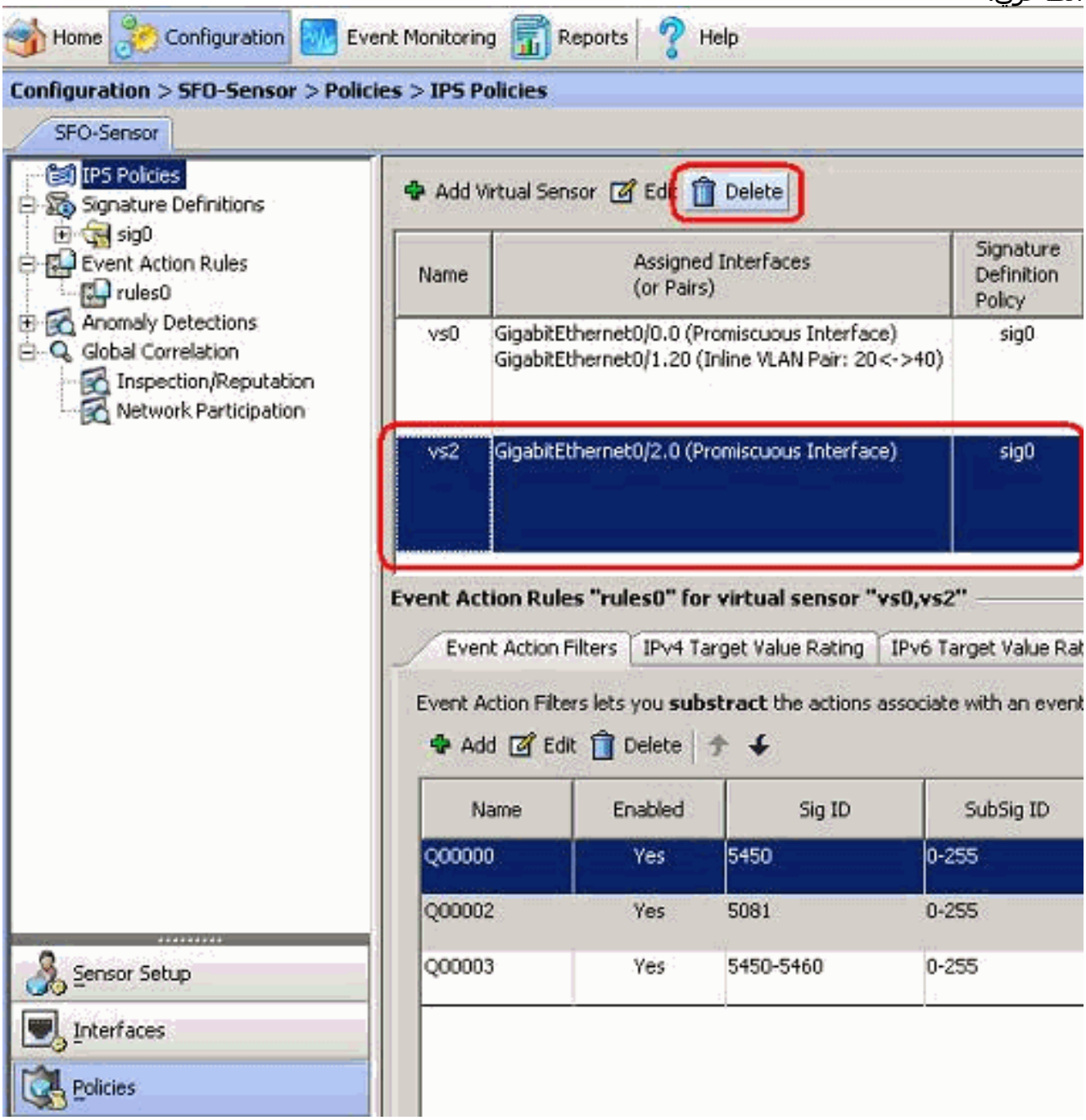
3. خرجت تحليل محرك أسلوب.

```
sensor(config-ana)# exit

                    #(sensor(config

:[Apply Changes:?[yes
```

حذف المستشعر الظاهري باستخدام IME

أكمل هذه الخطوات لحذف مستشعر ظاهري على نظام منع التسلل الآمن (IPS) من Cisco باستخدام Cisco IPS Manager Express:

1. أخترت **تشكيل>SFO-Sensor> سياسة> IPS**.
2. أختر المستشعر الظاهري المراد حذفه، ثم انقر فوق **حذف**، كما هو موضح في لقطة الشاشة. في هذا المثال VS2، يتم حذف المستشعر الظاهري.



يؤدي هذا إلى اكتمال عملية حذف مستشعر ظاهري. تم حذف المستشعر الظاهري مقابل 2.

استكشاف الأخطاء وإصلاحها

لا يتم تشغيل IPS Manager Express

المشكلة

عند إجراء محاولة للوصول إلى IPS من خلال IME، لا يتم بدء تشغيل IPS Manager Express ويتم تلقي رسالة الخطأ هذه:

```
.Cannot start IME client. Please check if it is already started"
"Exception: Address already in use: Cannot bind
```

الحل

لحل هذه المشكلة، قم بإعادة تحميل كمبيوتر محطة عمل IME.

معلومات ذات صلة

- صفحة دعم نظام منع الاقتحام من Cisco
- صفحة الدعم السريع ل Cisco IPS Manager
- بروتوكول وقت الشبكة (NTP)
- طلبات التعليقات (RFCs)
- 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).