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

المحتويات

<u>المقدمة</u> المتطلبات الأساسية المتطلبات المكونا<u>ت المستخدمة</u> المنتج<u>ات ذات الصلة</u> الاصطلاحات معلومات أساسية حول محرك التحليل <u>حول أجهزة الاستشعار الظاهرية</u> مزايا وقيود المحاكاة الافتراضية مزايا المحاكاة الافتراضية قبود المحاكاة الافتراضية متطلبات المحاكاة الافتراضية <u>التكوين</u> إضافة أجهزة إستشعار افتراضية إضافة مستشعر ظاهري باستخدام IME تحرير أجهزة الاستشعار الظاهرية <u>تحرير المستشعر الظاهري باستخدام IME</u> حذف أجهزة الاستشعار الظاهرية حذف المستشعر الظاهري باستخدام IME استكشاف الأخطاء واصلاحها لا يتم تشغيل IPS Manager Express معلومات ذات صلة

<u>المقدمة</u>

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

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

<u>المتطلبات الأساسية</u>

<u>المتطلبات</u>

لا توجد متطلبات أساسية خاصة لهذا المستند.

<u>المكونات المستخدمة</u>

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
- IME الأحدثم**لاحظة:** بينما يمكن إستخدام IME والإصدارات الأحدثم**لاحظة:** بينما يمكن إستخدام IME لمراقبة أجهزة الاستشعار التي تعمل بنظام Cisco IPS 5.0 والإصدارات الأحدث، فإن بعض الميزات والوظائف المراقبة 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 LPS لمنع التسلل الآمن (IPS (S.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.

<u>المنتجات ذات الصلة</u>

يمكن إستخدام هذا التكوين أيضا مع أجهزة الاستشعار هذه:

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

<u>الاصطلاحات</u>

راجع <u>اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.</u>

<u>معلومات أساسية</u>

<u>حول محرك التحليل</u>

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 VLAN المضمنة، ومجموعات VLAN التعريف الأخطاء الحد في العريف توقيع مسمى بشكل خاص وقواعد إجراء الحدث وتكوين اكتشاف

<u>حول أجهزة الاستشعار الظاهرية</u>

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 sig0 أو ado، على أجهزة إستشعار ظاهرية مختلفة. يمكنك أيضا تطبيق نفس مثيل النهج، 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

<u>مزايا المحاكاة الافتراضية</u>

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.

<u>التكوين</u>

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

إضافة أجهزة إستشعار افتراضية

قم بإصدار الأمر <u>virtual-sensor name</u> 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 الأخطاءوضع التشغيل—وضع اكتشاف الأخطاء (غير نشط، تعلم، كشف)
 - **الوصف** وصف المستشعر الظاهري
 - الحدث الإجراء القواعد اسم سياسة قواعد إجراءات الحدِث
- 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 قيام يغير 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 قيام يغير المتماثل من الأمان لأن الحماية التهرب وي 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 العبب، فلن تتم معالجة جميع الحزم بعد الحزمة التي تم فقدها. توفر الحماية الصارمة للتهرب الإنفاذ الكامل لحالة رسبب، فلن تتم معالجة جميع الحزم بعد الحزمة التي من فقدها. توفر الحماية الصارمة للتهرب الإنفاذ الكامل لحالة العب التهرب المائية أو مردة التهم معالجة جميع الحزم بعد الحزمة التي تم فقدها. توفر الحماية الصارمة للتهرب الإنفاذ الكامل لحالة رسبب، فلن تتم معالجة جميع الحزم بعد الحزمة التي مر مزمة أو حزم فائية توقيعات محركات التكييف الصارمة التسلسل. ملاحظة: يمكن أن ينتج عن أي حزم غير مرتبة أو حزم فائية توقيعات محركات التكييف التول التول القراد الحماية حمل مالي مال الخلي 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 race مرعة مرور. الافتراضي هو المستشعر الافتراضي، والذي هو دائما تقريبا أفضل خيار.virtual-Sensor تنتمي جميع الحزم ذات مفتاح جلسة العمل نفسه (ABB) داخل مستشعر ظاهري إلى نفس جلسة العمل.
 vLAN جميع الحزم ذات مفتاح جلسة العمل نفسه (ABb) داخل مستشعر ظاهري إلى نفس جلسة العمل.
 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 داخلي) وعلى الواجهة نفسها إلى الجلسة نفسها. يتم تعقب الحزم ذات المفتاح نفسه ولكن على شبكات VLAN أو الواجهات المختلفة بشكل مستقل.
 vLAN نفسها (أو زوج شبكة NLAN) في شبكة NLAN نفسها (أو زوج شبكة VLAN نفسها (أو زوج شبكة VLAN) داخلي) وعلى الواجهة نفسها إلى الجلسة نفسها. يتم تعقب الحزم ذات المفتاح نفسه ولكن على شبكات VLAN داخلي) وعلى الواجهة نفسها إلى الجلسة نفسها.
 vLAN نفسها (أو زوج شبكة NLAN) مستقل.
 vLAN نفسها (أو زوج شبكة VLAN) داخلي) بغض النظر عن الواجهة إلى نفس الجلسة. يتم تعقب الحزم ذات المفتاح نفسه ولكن على شبكات 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) أضف وصفا لهذا المستشعر الظاهري. sensor(config-ana-vir)# **description virtual sensor 2**

قم بتعيين نهج كشف الأخطاء ووضع التشغيل لهذا المستشعر الظاهري. sensor(config-ana-vir)# **anomaly-detection**

.4

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

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

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

8. قم بتعیین 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

.6

.7

```
signature-definition: sig1 default: sig0
                              event-action-rules: rules1 default: rules0
                                                anomaly-detection
                            _____
                             anomaly-detection-name: adl default: ad0
                             operational-mode: learn default: detect
                          _____
                    (physical-interface (min: 0, max: 999999999, current: 2
                          _____
                                         name: GigabitEthernet0/2
                                 <subinterface-number: 0 <defaulted</pre>
                           _____
       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.

<u>إضافة مستشعر ظاهري باستخدام IME</u>

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

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

لقطة الشاشة.

	cies > IPS P	olicies				
SFO-Sensor						
P (IPS Policies A Signature Definitions	🔹 Add V	/irtual Senso	Edit [Delete		
🖻 🤤 sig0 🎦 Active Signatures 🖀 Adware/Spyware	Name		Assigne (or Pairs	d Interfaces s)	Signature Definition Policy	Risk Rating
📓 Attack 📓 DDoS 📓 DoS	vs0	GigabitEthe GigabitEthe	rnet0/0.0 (P rnet0/1.20 (sig0	rules0 (3 action HIGHRISK	
Email						MEDIUMRISK
Reconnaissance	Eve	nt Action Filt	ers IPv4 T	arget Value Rating TPv6	Target Value R	ating OS Identif
Reconnaissance	Event #	nt Action Filt Action Filters Id (결) Edit	ers IPv4 To lets you sub Delete Enabled	arget Value Rating ∏Pv6 stract the actions associ	Target Value R ate with an ever SubSig ID	ating OS Identif
Reconnaissance	Event A Ac COULT	nt Action Filt Action Filters Id (2) Edit Jame	ers IPv4 To lets you sub I Delete Enabled Ves	arget Value Rating ∏IPv6 stract the actions associ Sig ID 5450	Target Value R ate with an even SubSig ID	ating OS Identif nt if the conditions (IPv4 22,214,105,20 0-65595
Reconnaissance	Event A P Ac Q0000 Q0000	nt Action Filters Id [2] Edit Iame 0	ers IPv4 To lets you sub Delete Enabled Ves Yes	arget Value Rating IPv6 stract the actions associ	Target Value R ate with an even SubSig ID)-255	ating OS Identif nt if the conditions (IPv4 22.214.105.20 0-65535 0.0.0.0-255.25 0-65535
Reconnaissance	Event # @ Ac 0 0 0 0 0 0 0 0 0 0 0 0 0	nt Action Filters Id (2) Edit Iame 0 2 3	ers IPv4 To lets you sub Delete Enabled Ves Yes Yes	arget Value Rating ☐ IPv6 stract the actions associ Sig ID 5450 5081 1 5450-5460	Target Value R ate with an even SubSig ID 0-255 0-255	ating OS Identif nt if the conditions (IPv4 22.214.105.20 0-65535 0.0.0.0-255.25 0-65535 22.214.105.20 0-65535

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 وقاعدة إجراء الحدث واكتشاف إيثرنت جيجابت 2/0 هنا. قم الآن بتوفير التفاصيل في أقسام تعريف التوقيع وقاعدة إجراء الحدث واكتشاف إيثرنت جيجابت 2/0 هنا. قم الآن بتوفير التفاصيل في أقسام تعريف التوقيع وقاعدة إجراء الحدث واكتشاف إيثرنت جيجابت 2/0 هنا. قم الآن بتوفير التفاصيل في أقسام تعريف التوقيع وقاعدة إجراء الحدث واكتشاف الأخطاء والخيارات 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 المات تعقب جلسة عمل NormalMode هو يقيد التوابية.

Juar Serisor Marrie.	vs2	1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1		
scription:	Virtual Sensor 2	- C		
nterfaces		Charge Protocol		
Andgreed	None		Details	Select All
	gabitEthernet0/2	Pomiscuous Interface		Assign
	publication in the cost of	Promiscous incorrect		
				Remove
Signature Definit	ion			
Signature Definition	Policy: sig0 👻			
	-			
Event Action Rule				
Event Action Rules	Policy: rules0 💌 🙂			
Use Event Actio	on Overrides			
-	a	Actions to Add	Enabled	Add
Risk Ratin	9	ACCIONS CO ACC		
HIGHRISK	g Deny Pa	scket Inline (Inline)	Yes	C de
RISK RATIN HIGHRISK MEDIUMRISK	B Deny Pa	acket Inline (Inline) Verbose Alert acker Packets	Yes Yes	Edit
Risk Ratin HIGHRISK MEDIUMRISK	9 Deny Pa M Produce E Log Atta	acket Inline (Inline) Verbose Alert acker Packets	Ves Yes Ves	Edit
RISK Ratin HIGHRISK MEDIUMRISK	9 R Deny Pa R Produce Dog Atta	acket Inline (Inline) Verbose Alert acker Packets	Yes Yes Yes	Edit Delete
RISK Ratin HIGHRISK MEDJUMRISK Anomaly Detecti	on	acket Inline (Inline) Verbose Alert acker Packets	Yes Yes Yes	Edit Delete
Anomaly Detection	ng Deny Pa Con Policy: ad0 - AD	ocket Inline (Inline) Verbose Alert acker Packets	Yes Yes @ Yes	Edit Delete
Anomaly Detection	on Policy: ad0 y AD	Operational Mode: Detect	Yes Yes	Edit Delete
Anomaly Detection	ng Peny Pa The Produce E Log Atta on Policy: ad0 Y AD	acket Inline (Inline) Verbose Alert acker Packets	Yes Yes	Edit Delete
Anomaly Detection Advanced Option	n Tracking Mode: Virtu	acket Inline (Inline) Verbose Alert acker Packets Operational Mode: Detect ual Sensor	Yes Yes	Edit Delete
RISK Ratin HIGHRISK MEDIUMRISK Anomaly Detection Anomaly Detection Advanced Option Inline TCP Session Normalizer Mode:	n Tracking Mode: Virtu	acket Inline (Inline) Verbose Alert acker Packets Operational Mode: Detect ual Sensor	Yes Yes	Edit Delete

- 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).

SFO-Sensor	ies > 125 Pol	cies						
IPS Poicies Signature Definitions Signature Definitions Active Signatures Adware/Spyware Attack DOS DoS Email IOS IPS Instant Messaging IST OF OS OS OS OS OS OS OS OS OS P2P Releases Viruses/Worms/Trojar Web Server	Add Virtual Sensor 🗹 Edit 📋 Delete							
	Name	Assigned Interfaces (or Pairs)			Signature Definition Policy	Risk Rating		
	vs0 G	igabitEthernet0/ igabitEthernet0/).0 (Promiscuous) 1.20 (Inline VLAN)	Interface) Pair: 20<->40)	sig0	rules0 (3 action HIGHRISK		
	vs2 (3	igabitEthernet0/	2.0 (Promiscuous)	Interface)	sig0	rules0 (3 action HIGHRISK MEDIUMRISK		
	Event Actio Event Event Act	n Rules "rules Action Filters [] Ion Filters lets yo [] Edit 🎁 Del	D" for virtual se V4 Target Value I u substract the ete 🛧 🗲	ensor "vs0,vs2 Rating IPv6 Ta actions associate	• arget Value Ra	ating OS Identi at if the condition		
	🗣 Add	2.40°						
Viruses/Worms/Trojar	Add Nan	ne Enab	led 5	ig ID	SubSig ID	(IPv4		
Viruses/Worms/Trojar Web Server All Signatures Event Action Rules Rules0 Anomaly Detections	Add Nan Q00000	ie Enab	led 5 s 5450	ig ID 0-2	SubSig ID SS	(IPv4 22.214.105.20 0.65535		
Viruses/Worms/Trojar Web Server All Signatures Event Action Rules Compared Provide Anomaly Detections	Add Nan Q00000 Q00002	ie Enab Ve Ve	led 5 s 5450 s 5081	ig ID 0-2 0-2	SubSig ID 55 55	(IPv4 22.214.105.20 0-65535 0.0.0.0-255.25 0-65535		

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. أدخل وضع تحليل الخدمة. sensor# **configure termina**1

	#(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
	<pre>sensor(config-ana-vir-ano)# anomaly-detection-name ad0</pre>
	<pre>sensor(config-ana-vir-ano)# operational-mode learn</pre>
.6	قم بتغيير نهج قواعد إجراءات الحدث المعينة إلى هذا المستشعر الظاهري. sensor(config-ana-vir-ano)# exit
	<pre>sensor(config-ana-vir)# event-action-rules rules0</pre>
.7	تغيير نهج تعريف التوقيع المعين إلى هذا المستشعر الظاهري. sensor(config-ana-vir)# signature-definition sig0
	8. تغییر وضع تعقب جلسة عمل TCP المضمنة. sensor(config-ana-vir)# inline-тср-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
	<pre>sensor(config-ana-vir)# physical-interface</pre>
	? sensor(config-ana-vir)# logical-interface
	<none available=""></none>
	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 بإقرانٍ الواجِهات.
	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. 12. تحقق بين اعدادات البيرية مسلطالها مسلمه مسلمة 12.
	sensor(config-ana-vir)# show settings

_____ :description: virtual sensor 1 default signature-definition: sig1 default: sig0 event-action-rules: rules1 default: rules0 anomaly-detection _____ anomaly-detection-name: adl default: ad0 operational-mode: learn default: detect _____ (physical-interface (min: 0, max: 999999999, current: 2 _____ name: GigabitEthernet0/2 <subinterface-number: 0 <defaulted</pre> _____ 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.

<u>تحرير المستشعر الظاهري باستخدام IME</u>

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

File View Tools Help						
🚮 Home ಶ Configuration 🌆 Ev	vent Monitoring 🚮	Reports 7	Help			
Configuration > SFO-Sensor > Poli	cies > IP5 Policies	de la companya de la comp				
SFO-Sensor						
E Signature Definitions	Add Virtual Senso Edit Delete					
Constant Sign Constan	Name	Assigned (or Pairs	Virtual Sensor or Internaces :)	Signature Definition Policy		
	vs0 Gigabit Gigabit	Ethernet0/0.0 (P Ethernet0/1.20 (romiscuous Interface Inline VLAN Pair: 20<) sig0 ->40)		
	vs2 Gigabit	Ethernet0/2.0 (P	romiscuous Interface) sig0		
	Event Action Ru	les "rules0" fo	r virtual sensor "v	s0,vs2"		
	Event Action	Filters IPv4 Ta	arget Value Rating 🏹	IPv6 Target Value Rat		
	Event Action Fi	ters lets you sub dit 📋 Delete	stract the actions a: テーチ	ssociate with an event		
	Name	Enabled	Sig ID	SubSig ID		
	Q00000	Yes	5450	0-255		
	Q00002	Yes	5081	0-255		
🚴 Sensor Setup	Q00003	Yes	5450-5460	0-255		
Interfaces						
Policies						

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 والخيارات المتقدمة**. انقر فوق **موافق**، ثم انقر فوق **تطبيق**.

Assigned	Name	1	Details	Select All
	GigabitEthernet0/2	Promiscuous Interface		
	GigabitEthernet0/3	Promiscuous Interface		Assign
				Remove
Signature De	finition			
Signature Defir	nition Policy: sig0 🔻			
Event Action	Rule			
Event Action R	ules Policy: rules0 💌 🜖			
🔽 Use Event	Action Overrides			
Risk F	Pating	Actions to Add	Enabled	T Add
HIGHRISK	🔯 Deny Pa	ocket Inline (Inline)	Yes	
	Produce	Verbose Alert	🗿 Yes	Edit
MEDIUMRISK	🗄 Log Atta	acker Packets	Yes	Delete
an bu da an ta ta ta ta	ection		-	
Anomaly Det	tion Policy: ad0 - AD	Operational Mode: Detect	<u> </u>	
Anomaly Det Anomaly Detec				*
Anomaly Det Anomaly Detec Advanced Op	tions			
Anomaly Det Anomaly Detec Advanced Op	tions	al Sensor		
Anomaly Det Anomaly Detec Advanced Op Inline TCP Se	tions ession Tracking Mode: Virtu	Jal Sensor		

يؤدي هذا إلى اكتمال عملية تحرير مستشعر ظاهري.

حذف أجهزة الاستشعار الظاهرية

لحذف مستشعر ظاهري، أكمل الخطوات التالية:

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

.1

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</pre>

<event-action-rules: rules0 <protected</pre>

anomaly-detection

<anomaly-detection-name: ad0 <protected</pre>

<operational-mode: detect <defaulted</pre>

(physical-interface (min: 0, max: 9999999999, 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

<u>حذف المستشعر الظاهري باستخدام IME</u>

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.

		· (III)	· •	and in		
SEO-Sepsor	cies > IPS P	olicies				
PS Policies	Add Virtual Sensor 🕜 Ed					
Gradient Street St	Name		Assigned Interfaces (or Pairs)			Signature Definition Policy
	vsD	vs0 GigabitEthernet0/0.0 (Promiscuous Interface) GigabitEthernet0/1.20 (Inline VLAN Pair: 20<->40)		ce))<->40)	sig0	
	VS2	GigabitEl	GigabitEthernet0/2.0 (Promiscuous Interface)			sig0
	Event Ac Even Event A	tion Rule nt Action F Action Filte	e s "rules0" fo Filters [] IPv4 Ta ers lets you sub t îî Delete	r virtual sensor " arget Value Rating stract the actions	'vs0,vs2 IPv6 Ta associate	rget Value Ra
	N	lame	Enabled	Sig ID		SubSig ID
	Q0000	0	Yes	5450	0-2	55
	Q0000	2	Yes	5081	0-2	55
Sensor Setup	Q0000	3	Yes	5450-5460	0-2	55
Interfaces						
Policies						

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

استكشاف الأخطاء وإصلاحها

لا يتم تشغيل IPS Manager Express

<u>المشكلة</u>

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.

<u>معلومات ذات صلة</u>

- <u>صفحة دعم نظام منع الاقتحام من Cisco</u>
- <u>صفحة الدعم السريع ل Cisco IPS Manager</u>
 - بروتوكول وقت الشبكة (NTP<u>)</u>
 - <u>طلبات التعليقات (RFCs)</u>
 - الدعم التقني والمستندات Cisco Systems

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما