IPS 6.x والإصدارات الأحدث/IDSM2: وضع تجاوز الواجهة المضمنة باستخدام مثال تكوين IDM

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
المنتجات ذات الصلة
الاصطلاحات
تكوين أزواج الواجهة المضمنة
تكوين واجهة سطر الأوامر (CLI)
تكوين IDM
شكلت المفتاح ل IDSM-2 في خط أسلوب
استكشاف الأخطاء وإصلاحها
المشكلة
الحل
معلومات ذات صلة

المقدمة

يضع التشغيل في وضع زوج الواجهة المضمنة نظام منع التسلل (IPS) مباشرة في تدفق حركة المرور ويؤثر على معدلات إعادة توجيه الحزم، مما يجعلها أبطأ عند إضافة زمن الوصول. وهذا يسمح للمستشعر بوقف الهجمات حتى يسقط حركة المرور الخبيثة قبل أن يصل إلى الهدف المقصود، وبالتالي يوفر خدمة الحماية. ليس فقط معالجة الجهاز في السطر معلومات على طبقة 3 و 4، ولكنه أيضا يحلل محتويات وحمولة الحزم من أجل هجمات مضمنة أكثر تعقيدا (طبقات 3 إلى 7). يتيح هذا التحليل الأعمق للنظام التعرف على الهجمات التي تمر عادة عبر جهاز جدار حماية تقليدي وإيقافها و/أو حظرها.

في وضع زوج الواجهة الداخلية، تأتي الحزمة من خلال الواجهة الأولى للزوج على المستشعر وخارج الواجهة الثانية للزوج. يتم إرسال الحزمة إلى الواجهة الثانية للزوج ما لم يتم رفض هذه الحزمة أو تعديلها بواسطة توقيع.

ملاحظة: يمكنك تكوين AIM-IPS و AIP-SSM للعمل داخل السطر على الرغم من أن هذه الوحدات تحتوي على واجهة إستشعار واحدة فقط.

ملاحظة: إذا كانت الواجهات المزدوجة متصلة بنفس المحول، فيجب عليك تكوينها على المحول كمنافذ وصول مع شبكات VLAN للوصول المختلفة للمنفذين. وإلا، فحركة المرور لا تتدفق من خلال الواجهة الداخلية.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى مستشعر Cisco IPS الذي يستخدم واجهة سطر الأوامر 6.0 ومدير الأجهزة (IDM) لنظام منع التسلل 6.0.

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.

المنتجات ذات الصلة

تنطبق المعلومات الواردة في هذا المستند أيضا على وحدة خدمات نظام اكتشاف الاقتحام (IDSM-2).

الاصطلاحات

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

تكوين أزواج الواجهة المضمنة

أستخدم الأمر name **inline-interfaces** في الوضع الفرعي لواجهة الخدمة لإنشاء أزواج الواجهة المضمنة.

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

ملاحظة: يتم تكوين AIP-SSM لوضع الواجهة المضمنة من Cisco ASA CLI وليس من Cisco IPS CLI.

يتم تطبيق هذه الخيارات:

- *اسم* ***الواجهات الداخلية*** — اسم زوج الواجهة المضمنة المنطقي**ملاحظة:** في جميع واجهات إستشعار اللوحة الخلفية في جميع الوحدات النمطية (IDSM-2 NM-CIDS، و AIP-SSM)، يتم تعيين **admin-state** على ممكن ومحمي (لا يمكنك تغيير الإعداد). ليس ل **admin-state** تأثير (ومحمي) على واجهة الأمر والتحكم. فهو يؤثر فقط على واجهات الاستشعار. لا يلزم تمكين واجهة الأمر والتحكم لأنه لا يمكن مراقبتها.
- **الافتراضي**—يعيد القيمة إلى الإعداد الافتراضي للنظام
- **الوصف**—الوصف الخاص بك لزوج الواجهة المضمنة
- **interface1** *interface_name* — أول واجهة في زوج الواجهة المضمنة
- **interface2** *interface_name* — الواجهة الثانية في زوج الواجهة المضمنة
- **لا**- يزيل إعداد إدخال أو تحديد
- **تم تمكين الحالة** {admin {enabled | disabled}— حالة الارتباط الإداري للواجهة، سواء كانت الواجهة ممكنة أو معطلة.

تكوين واجهة سطر الأوامر (CLI)

أتمت هذا steps in order to شكلت ال VLAN زوج عملية إعداد على المستشعر:

1. قم بتسجيل الدخول إلى CLI باستخدام حساب له امتيازات المسؤول.
2. دخلت القارن submode:

```
sensor#configure terminal
```

```
sensor(config)#service interface
#(sensor(config-int
```

3. تحقق من وجود أي واجهات داخل السطر. يجب أن يقرأ نوع الواجهة الفرعية none إذا لم يتم تكوين واجهات مضمنة:

```
sensor(config-int)#show settings
(physical-interfaces (min: 0, max: 999999999, current: 2
        -----------------------------------------------
                                    <protected entry>
                  <name: GigabitEthernet0/0 <defaulted
      -----------------------------------------------
                         <media-type: tx <protected
                           <description: <defaulted
                  <admin-state: disabled <protected
                           <duplex: auto <defaulted
                            <speed: auto <defaulted
                            alt-tcp-reset-interface
   -----------------------------------------------
                                          none
-----------------------------------------------
-----------------------------------------------
   -----------------------------------------------
                                subinterface-type
   -----------------------------------------------
                                          none
-----------------------------------------------
-----------------------------------------------
   -----------------------------------------------
      -----------------------------------------------
                                       <protected entry>
                  <name: GigabitEthernet0/1 <defaulted
      -----------------------------------------------
                         <media-type: tx <protected
                           <description: <defaulted
                  <admin-state: disabled <defaulted
                           <duplex: auto <defaulted
                            <speed: auto <defaulted
                            alt-tcp-reset-interface
   -----------------------------------------------
                                          none
-----------------------------------------------
-----------------------------------------------
   -----------------------------------------------
                                subinterface-type
   -----------------------------------------------
                                          none
-----------------------------------------------
-----------------------------------------------
   -----------------------------------------------
      -----------------------------------------------
                                    <protected entry>
                  <name: GigabitEthernet0/2 <defaulted
      -----------------------------------------------
                         <media-type: tx <protected
                           <description: <defaulted
                  <admin-state: disabled <defaulted
                           <duplex: auto <defaulted
                            <speed: auto <defaulted
                            alt-tcp-reset-interface
   -----------------------------------------------
                                          none
-----------------------------------------------
-----------------------------------------------
   -----------------------------------------------
```

```
                                    subinterface-type
   ---------------------------------------------
                                          none
-----------------------------------------------
-----------------------------------------------
   ---------------------------------------------
      -------------------------------------------------
                                  <protected entry>
                <name: GigabitEthernet0/3 <defaulted
      -------------------------------------------------
                       <media-type: tx <protected
                         <description: <defaulted
                <admin-state: disabled <defaulted
                         <duplex: auto <defaulted
                          <speed: auto <defaulted
                          alt-tcp-reset-interface
   ---------------------------------------------
                                          none
-----------------------------------------------
-----------------------------------------------
   ---------------------------------------------
                                subinterface-type
   ---------------------------------------------
                                          none
-----------------------------------------------
-----------------------------------------------
   ---------------------------------------------
      -------------------------------------------------
                                  <protected entry>
                    <name: Management0/0 <defaulted
      -------------------------------------------------
                       <media-type: tx <protected
                         <description: <defaulted
                <admin-state: disabled <protected
                         <duplex: auto <defaulted
                          <speed: auto <defaulted
                          alt-tcp-reset-interface
   ---------------------------------------------
                                          none
-----------------------------------------------
-----------------------------------------------
   ---------------------------------------------
                                subinterface-type
   ---------------------------------------------
                                          none
-----------------------------------------------
-----------------------------------------------
   ---------------------------------------------
      -------------------------------------------------
         -----------------------------------------------
              <command-control: Management0/0 <protected
  (inline-interfaces (min: 0, max: 999999999, current: 0
         -----------------------------------------------
         -----------------------------------------------
                          <bypass-mode: auto <defaulted
                                interface-notifications
         -----------------------------------------------
   <missed-percentage-threshold: 0 percent <defaulted
        <notification-interval: 30 seconds <defaulted
         <idle-interface-delay: 30 seconds <defaulted
         -----------------------------------------------
                                     #(sensor(config-int
```

4. قم بتسمية الزوج المضمن:

```
sensor(config-int)#inline-interfaces PAIR1
```

5. عرض قائمة الواجهات المتاحة:

```
sensor(config-int)#physical-interfaces ?
  GigabitEthernet0/0 physical interface     .GigabitEthernet0/0
  GigabitEthernet0/1 physical interface     .GigabitEthernet0/1
  GigabitEthernet0/2 physical interface     .GigabitEthernet0/2
  GigabitEthernet0/3 physical interface     .GigabitEthernet0/3
       Management0/0 physical interface          .Management0/0
sensor(config-int)#physical-interfaces
```

6. تكوين واجهتين في زوج:

```
sensor(config-int)#interface1 GigabitEthernet0/0
```

```
sensor(config-int-inl)#interface2 GigabitEthernet0/1
```

يجب تعيين الواجهة لمستشعر ظاهري وتمكينها قبل أن تتمكن من مراقبة حركة مرور البيانات. راجع الخطوة 10 للحصول على مزيد من المعلومات.

7. إضافة وصف لهذه الواجهة:

```
sensor(config-int-phy)#description PAIR1 Gig0/0 and Gig0/1
```

8. كرر الخطوات من 4 إلى 7 لأي واجهات أخرى تريد تكوينها على أزواج الواجهة المضمنة.
9. دققت العملية إعداد:

```
sensor(config-int-inl)#show settings
                                name: PAIR1
-----------------------------------------------
 :description: PAIR1 Gig0/0 & Gig0/1 default
              interface1: GigabitEthernet0/0
              interface2: GigabitEthernet0/1
-----------------------------------------------
```

10. تمكين الواجهات التي تم تعيينها لزوج الواجهة:

```
sensor(config-int)#exit
sensor(config-int)#physical-interfaces GigabitEthernet0/0
sensor(config-int-phy)#admin-state enabled
sensor(config-int-phy)#exit
sensor(config-int)#physical-interfaces GigabitEthernet0/1
sensor(config-int-phy)#admin-state enabled
sensor(config-int-phy)#exit
#(sensor(config-int
```

11. تحقق من تمكين الواجهات:

```
sensor(config-int)#show settings
(physical-interfaces (min: 0, max: 999999999, current: 5
        -----------------------------------------------
                                <protected entry>
                          name: GigabitEthernet0/0
     -------------------------------------------------
                     <media-type: tx <protected
                       <description: <defaulted
          admin-state: enabled default: disabled
                       <duplex: auto <defaulted
                        <speed: auto <defaulted
                    <default-vlan: 0 <defaulted
                        alt-tcp-reset-interface
   -----------------------------------------------
                                        none
-------------------------------------------------
-------------------------------------------------
   -----------------------------------------------
```

```
                                    subinterface-type
   ---------------------------------------------
                                        none
-----------------------------------------------
-----------------------------------------------
   ---------------------------------------------
      -------------------------------------------------
                                  <protected entry>
                              name: GigabitEthernet0/1
      -------------------------------------------------
                         <media-type: tx <protected
                           <description: <defaulted
                admin-state: enabled default: disabled
                           <duplex: auto <defaulted
                            <speed: auto <defaulted
                       <default-vlan: 0 <defaulted
                            alt-tcp-reset-interface
   ---------------------------------------------
                                        none
-----------------------------------------------
-----------------------------------------------
   ---------------------------------------------
                                    subinterface-type
   ---------------------------------------------
                                        none
-----------------------------------------------
-----------------------------------------------
   ---------------------------------------------
      -------------------------------------------------
                                  <protected entry>
                     <name: GigabitEthernet0/2 <defaulted
      -------------------------------------------------
                           <media-type: tx <protected
                             <description: <defaulted
                     <admin-state: disabled <defaulted
                           <duplex: auto <defaulted
                            <speed: auto <defaulted
                       <default-vlan: 0 <defaulted
                            alt-tcp-reset-interface
   ---------------------------------------------
                                        none
-----------------------------------------------
-----------------------------------------------
   ---------------------------------------------
                                    subinterface-type
   ---------------------------------------------
                                        none
-----------------------------------------------
-----------------------------------------------
   ---------------------------------------------
      -------------------------------------------------
                                  <protected entry>
                     <name: GigabitEthernet0/3 <defaulted
      -------------------------------------------------
                           <media-type: tx <protected
                                                --MORE--
```

12. قم بإصدار هذا الأمر لحذف زوج واجهة في السطر وإرجاع الواجهات إلى الوضع المختلطة:

```
sensor(config-int)#no inline-interfaces PAIR1
```

يجب أيضا حذف زوج الواجهة المضمنة من المستشعر الظاهري الذي يتم تعيينه إليه.

13. تحقق من حذف زوج الواجهة المضمنة:

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

```
-------------------------------------------
    <command-control: Management0/0 <protected
(inline-interfaces (min: 0, max: 999999999, current: 0
-------------------------------------------
-------------------------------------------
                <bypass-mode: auto <defaulted
                    interface-notifications
-------------------------------------------
```

14. خرجت قارن تشكيل أسلوب:

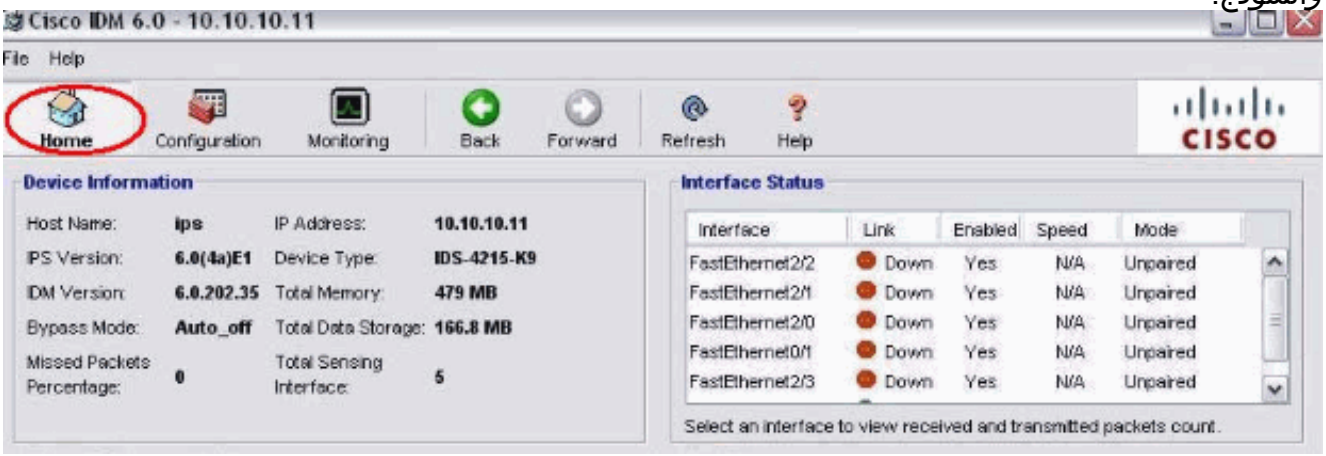
```
sensor(config-int)#exit
:[Apply Changes:?[yes
```

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

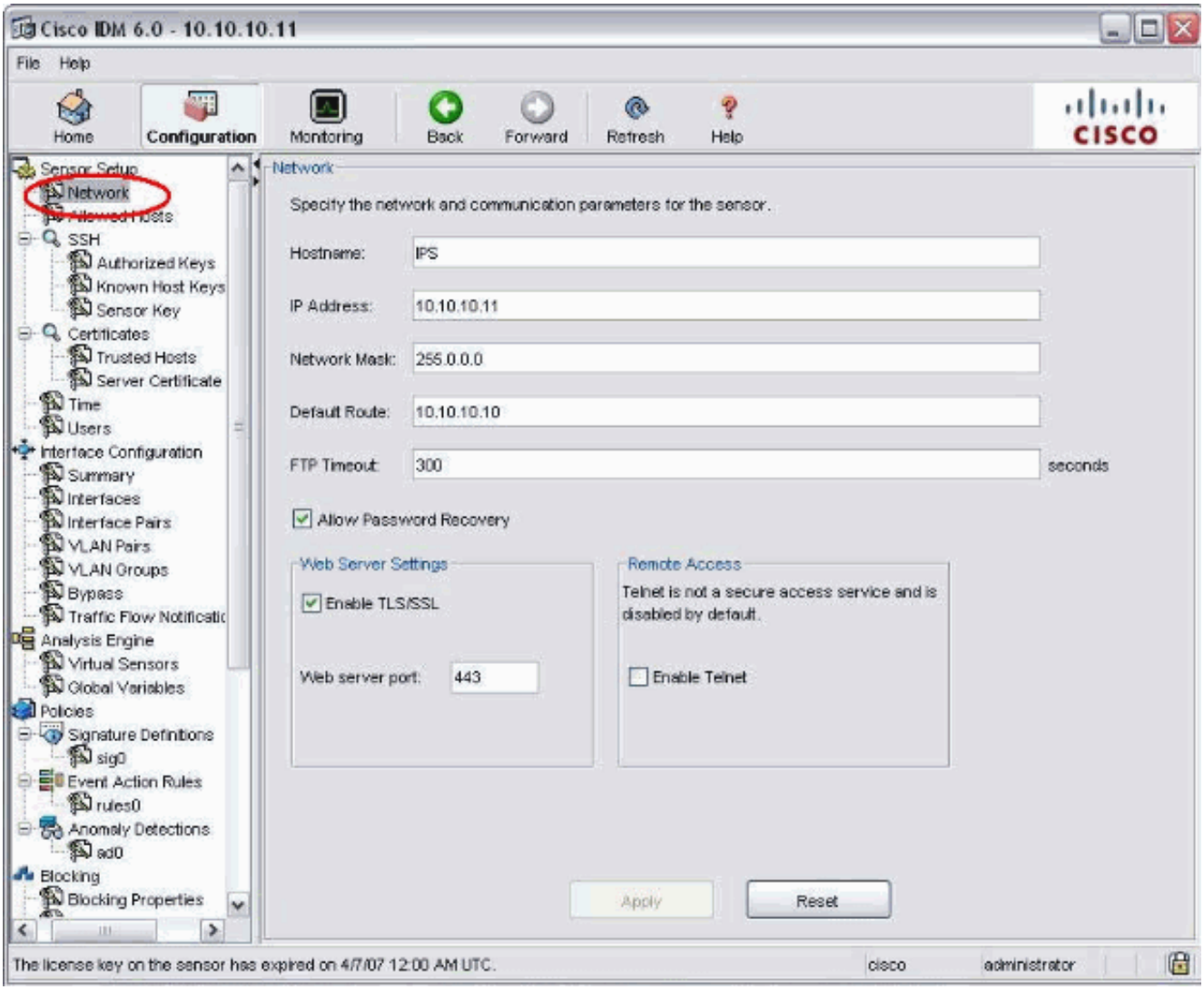
تكوين IDM

أتمت هذا steps in order to شكلت ال VLAN زوج عملية إعداد على المستشعر يستعمل ال IDM:

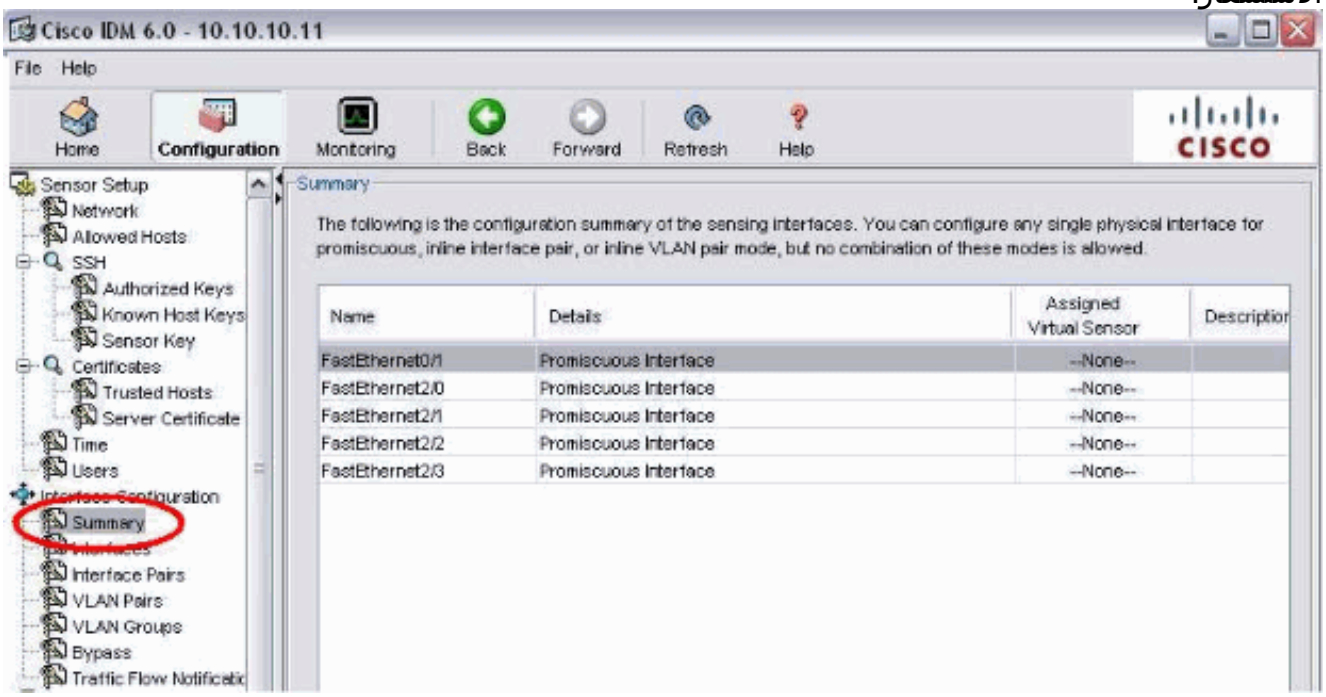
1. افتح المستعرض وأدخل **<https://<management_ip_address_of_ips** للوصول إلى IDM على IPS.
2. انقر فوق **تنزيل مشغل IDM وبدء IDM** لتنزيل المثبت للتطبيق.
3. انتقل إلى الصفحة الرئيسية لعرض معلومات الجهاز مثل اسم المضيف وعنوان IP والإصدار والنموذج.



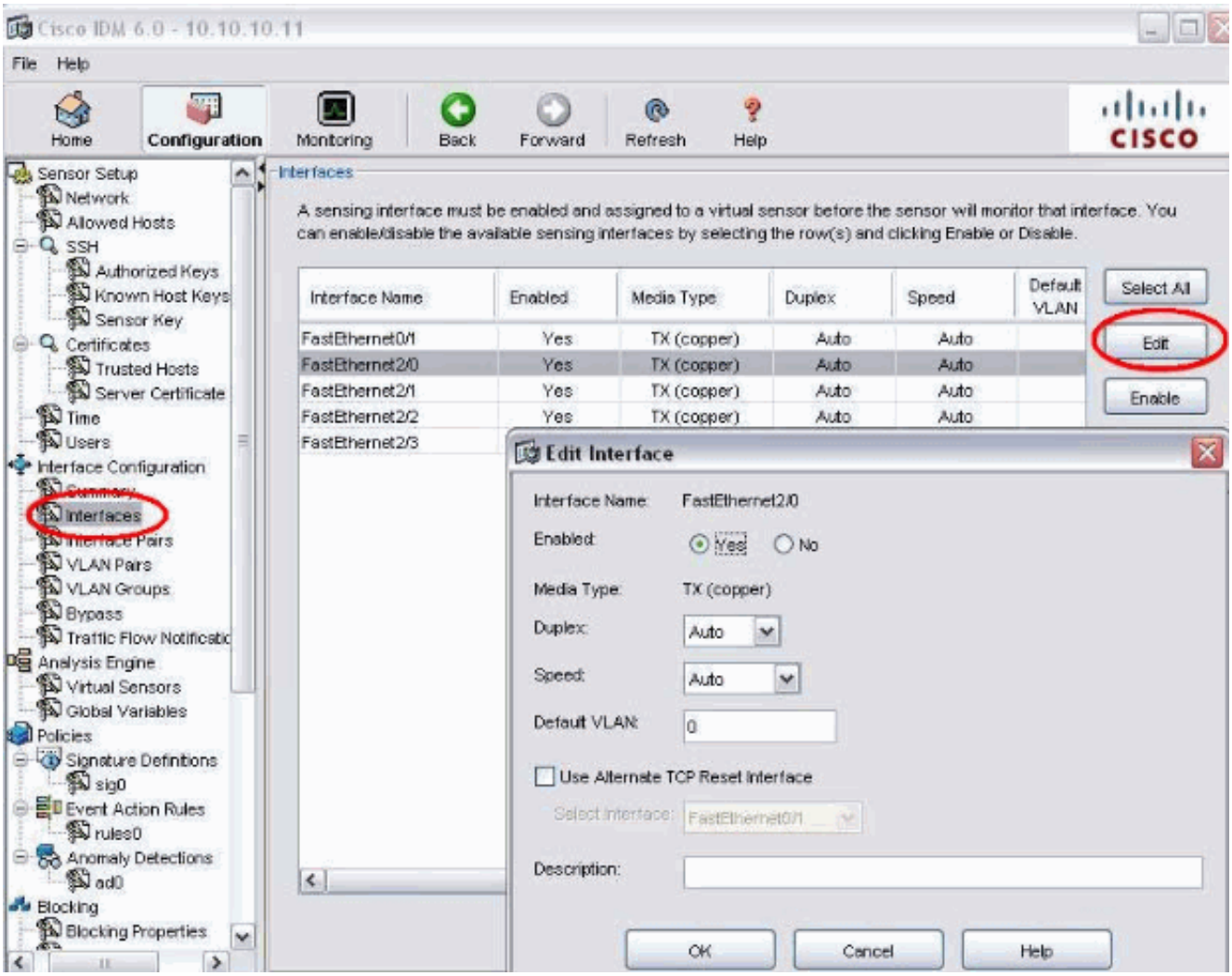
4. انتقل إلى **التكوين > إعداد المستشعر** وانقر فوق **الشبكة**. هنا أنت يستطيع عينت ال hostname، عنوان وقصير طريق.



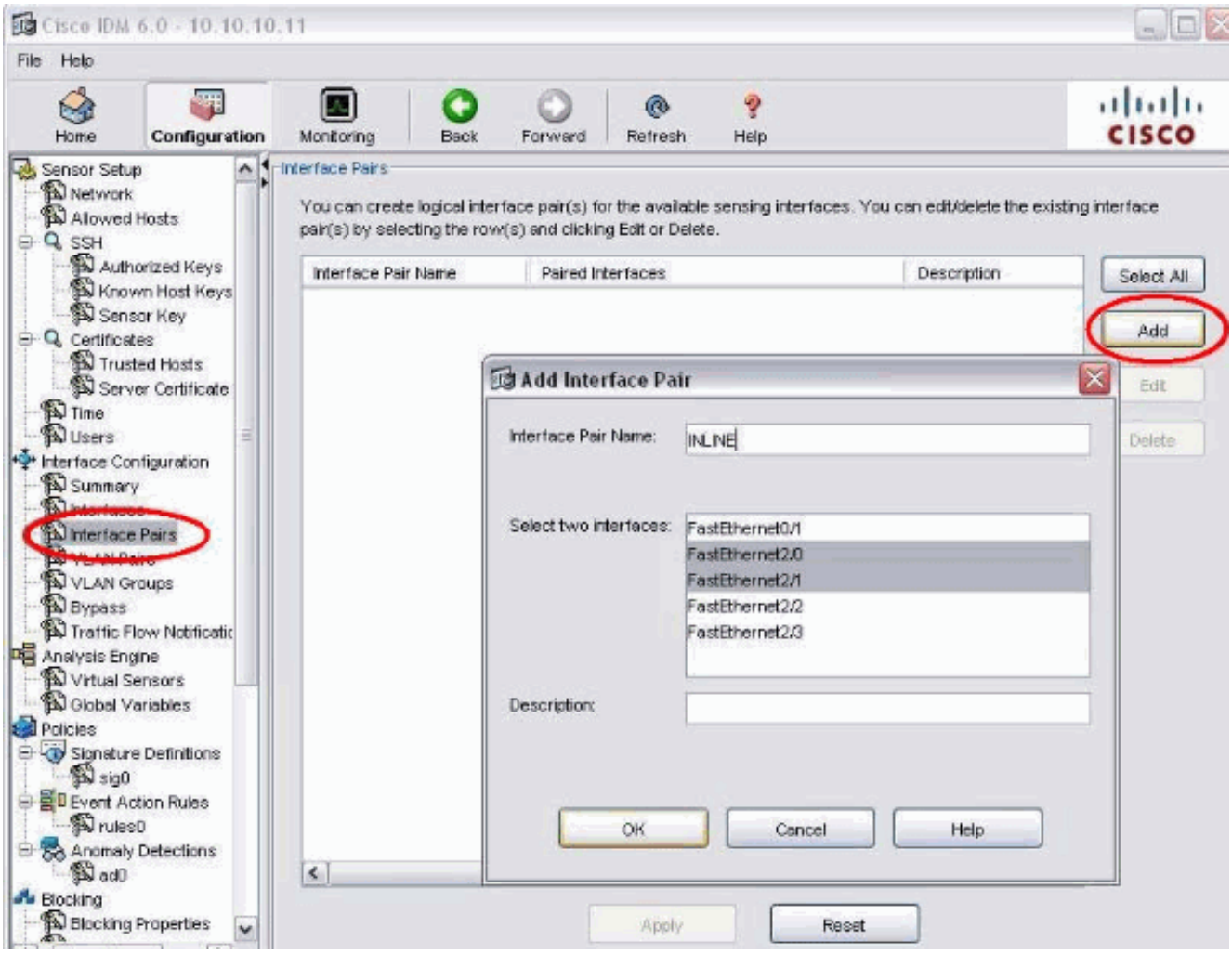
5. انتقل إلى **التكوين > تكوين الواجهة** وانقر فوق **ملخص**.تعرض هذه الصفحة ملخص تكوين واجهة الاستشعار:



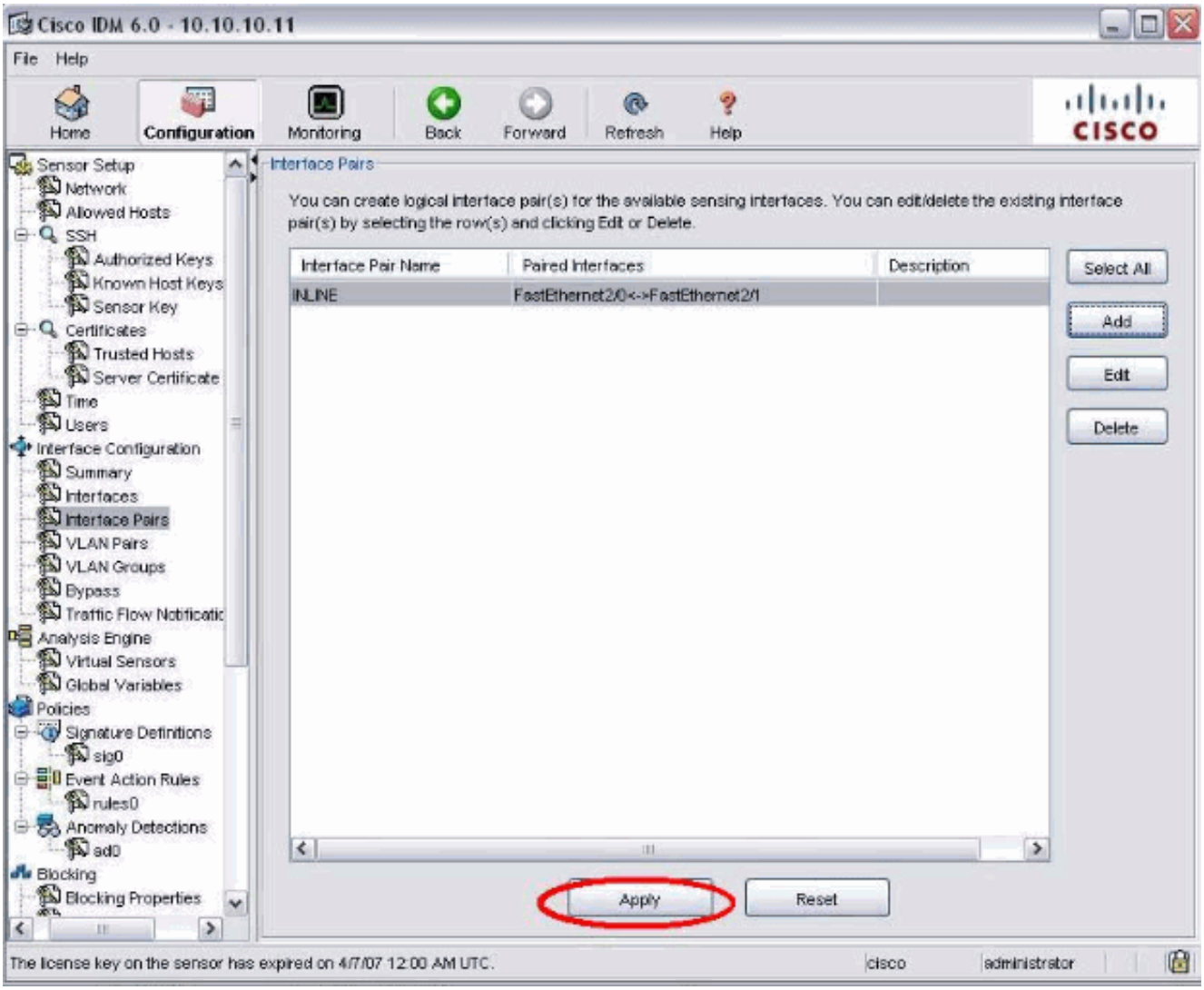
6. انتقل إلى **التكوين > تكوين الواجهة > الواجهات** وحدد اسم الواجهة. طقطقت بعد ذلك **يمكن** in order to مكنت الاستشعار قارن. قم أيضا بتكوين معلومات الإرسال ثنائي الإتجاه والسرعة وشبكة VLAN.



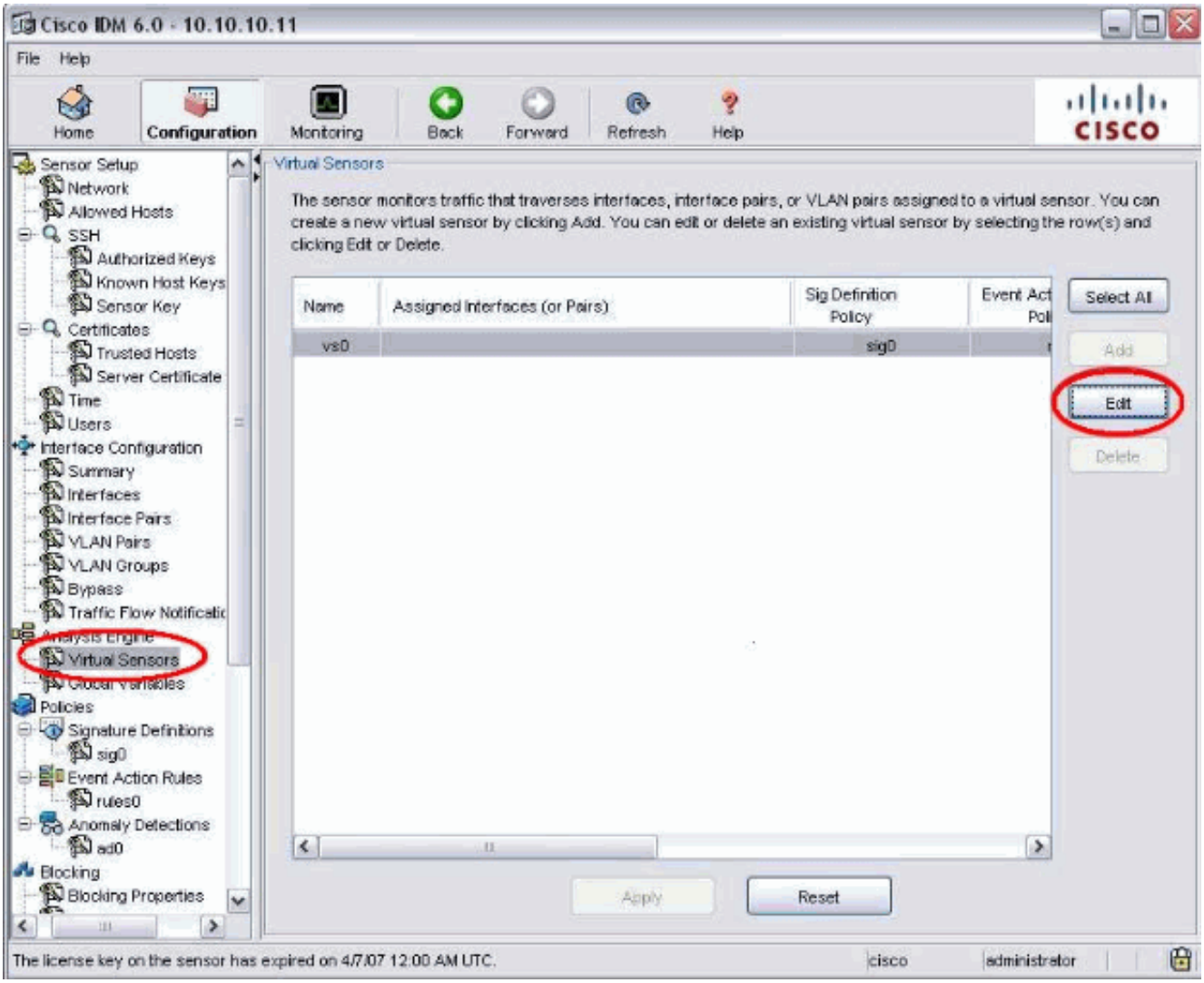
7. انتقل إلى **التكوين > تكوين الواجهة > أزواج الواجهة** وانقر فوق **إضافة** لإنشاء الزوج الداخلي.



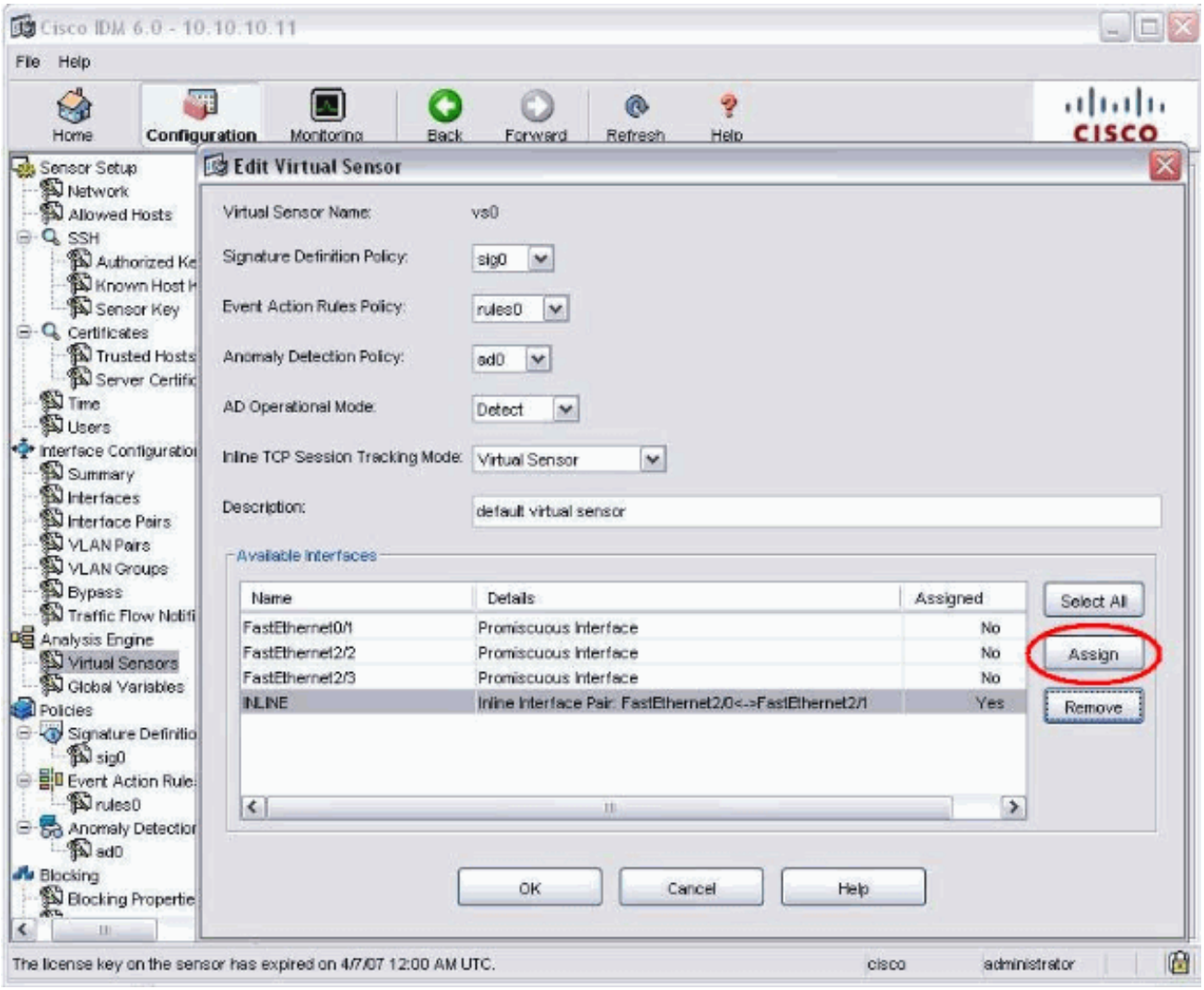
8. عرض ملخص تكوين الزوج المضمن وتطبيقه.



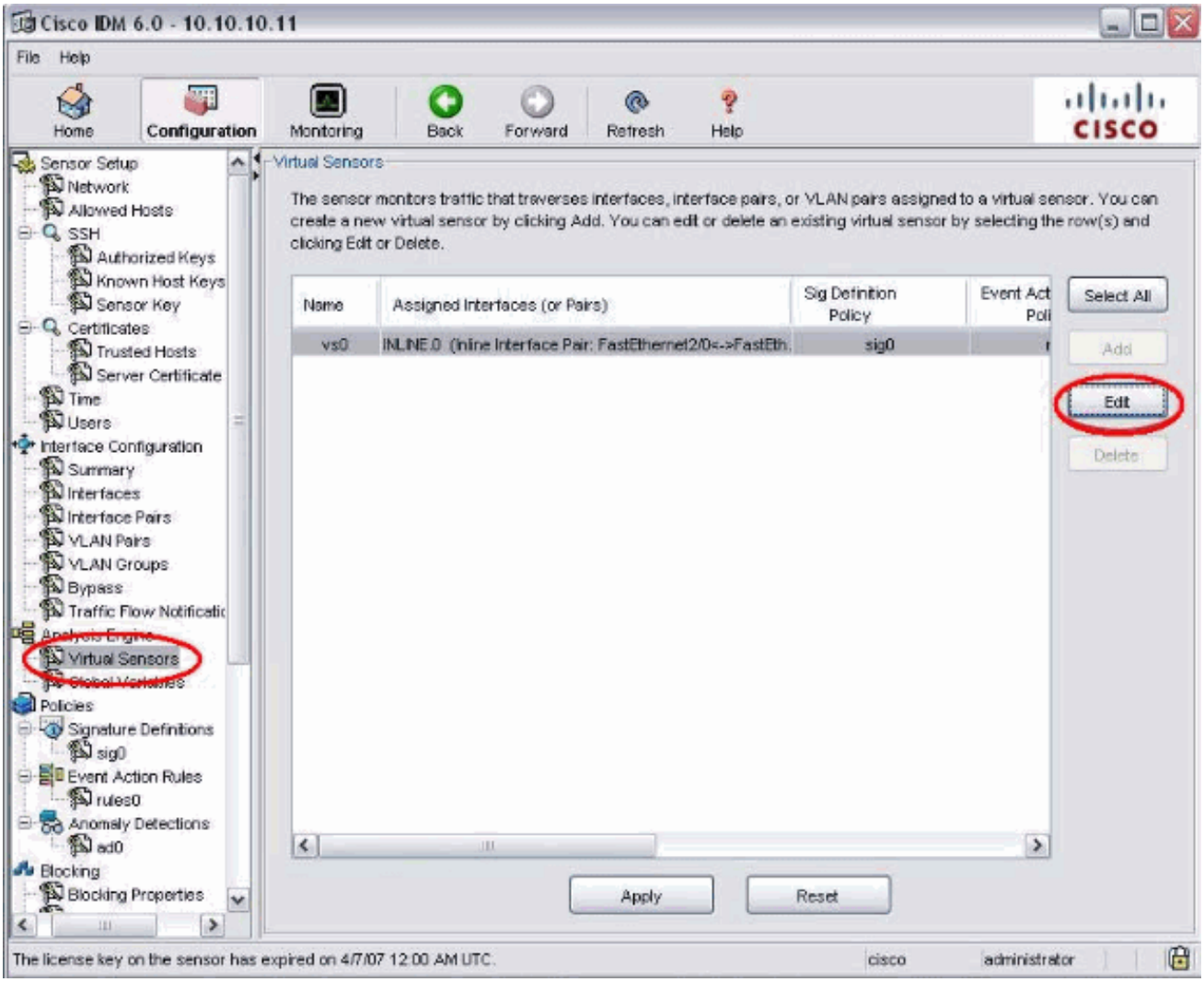
9. انتقل إلى **Configuration (التكوين) > Analysis Engine (محرك التحليل) > Virtual Sensor (المستشعر الظاهري)** وانقر فوق **Edit** (تحرير) لإنشاء المستشعر الظاهري الجديد.



10. قم بتعيين الزوج المضمن **في السطر** إلى المستشعر الظاهري مقابل0.



11. عرض ملخص معلومات المستشعر الظاهري المعينة.



شكلت المفتاح ل IDSM-2 في خط أسلوب

أحلت ال بشكل المادة حفازة sery 6500 مفتاح ل IDSM-2 في خط أسلوب قسم من بشكل IDSM-2 in order to شكلت المفتاح ل IDSM-2 داخل أسلوب.

استكشاف الأخطاء وإصلاحها

المشكلة

إذا فشل بروتوكول الإنترنت (IPS) وتم تكوينه في السطر، فهل فشلت الواجهات في الفتح (تستمر حركة المرور) أو أغلقت (يتم إسقاط حركة المرور).

الحل

يمكنك تكوين IPS في حالة فشل الفتح. وهكذا، إذا فشل نظام منع الاختراق (IPS) فسيواصل تمرير حركة المرور، ولكنه لن يراقب حركة المرور.

معلومات ذات صلة

- أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances

- نظام Cisco لمنع الاقتحام
- أجهزة إستشعار Cisco IPS 4200 Series
- 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).