

# جاوزاً عضو: IDSM2/ثدحأل ا تارادصلإ او IPS 6.x IDM نيوكت لاثم مادختساب ةنمضملا ةهجالا

## المحتويات

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

## المقدمة

يضع التشغيل في وضع زوج الواجهة المضمنة نظام منع التسلسل (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 استشعار واحدة فقط.

**ملاحظة:** إذا كانت الواجهات المزدوجة متصلة بنفس المحول، فيجب عليك تكوينها على المحول كمنافذ وصول مع شبكات VLAN للوصول المختلفة للمنفذين. والا، 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

تتطبق المعلومات الواردة في هذا المستند أيضا على وحدة خدمات نظام اكتشاف الاقحام (IDS-2).

## الاصطلاحات

راجع [اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.](#)

## تكوين أزواج الواجهة المضمنة

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

**ملاحظة:** أستخدم [أداة بحث الأوامر](#) (للعلماء [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 (IDS-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
```



```

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

```

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

.5

عرض قائمة الواجهات المتاحة:

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

The screenshot shows the Cisco IDM 6.0 web interface. The title bar reads "Cisco IDM 6.0 - 10.10.10.11". The navigation menu includes "Home" (circled in red), "Configuration", "Monitoring", "Back", "Forward", "Refresh", and "Help". The "Device Information" section displays the following details:

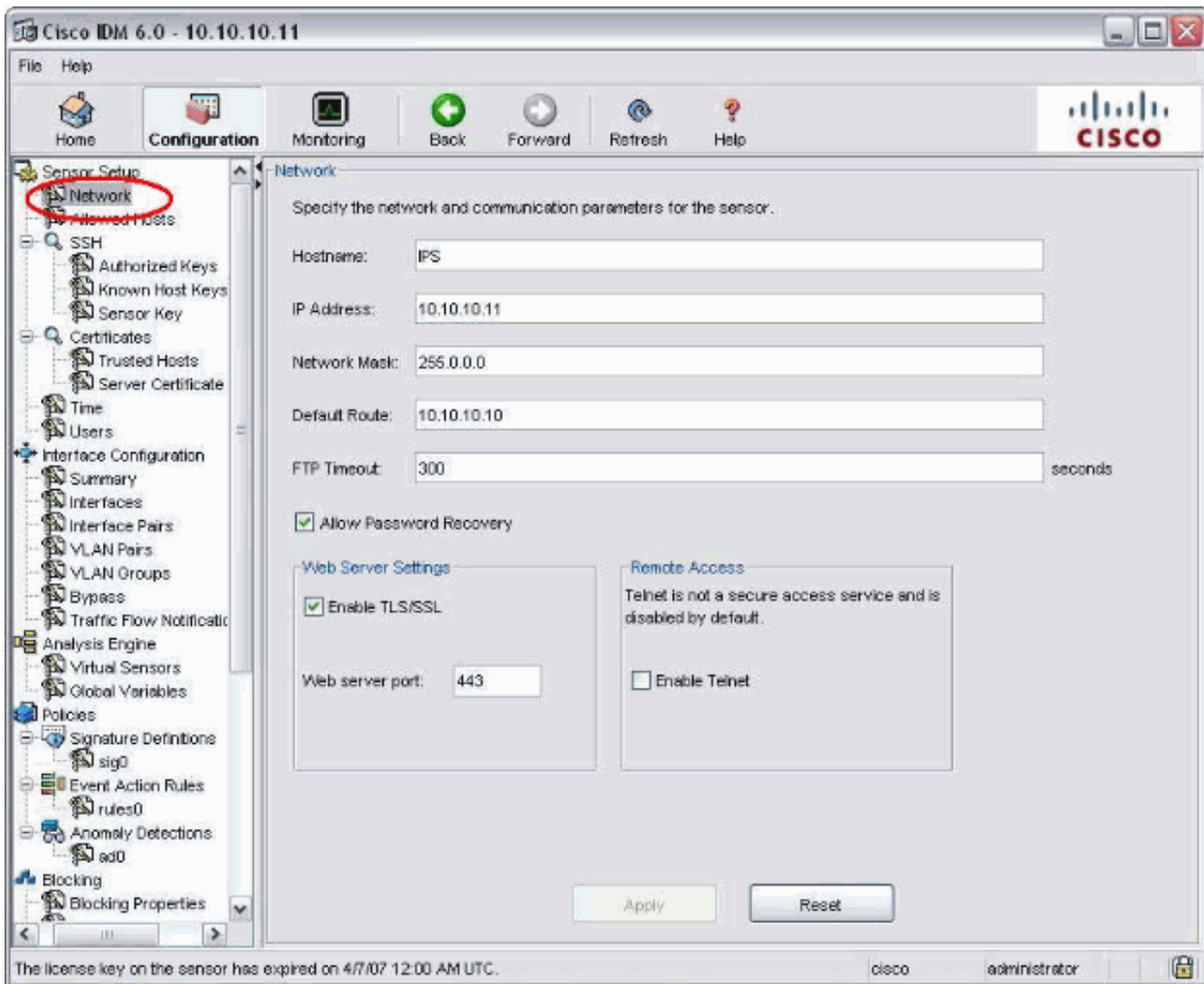
Host Name:	ips	IP Address:	10.10.10.11
IPS Version:	6.0(4a)E1	Device Type:	IDS-4215-K9
IDM Version:	6.0.202.35	Total Memory:	479 MB
Bypass Mode:	Auto_off	Total Data Storage:	166.8 MB
Missed Packets Percentage:	0	Total Sensing Interface:	5

The "Interface Status" section shows a table of interfaces:

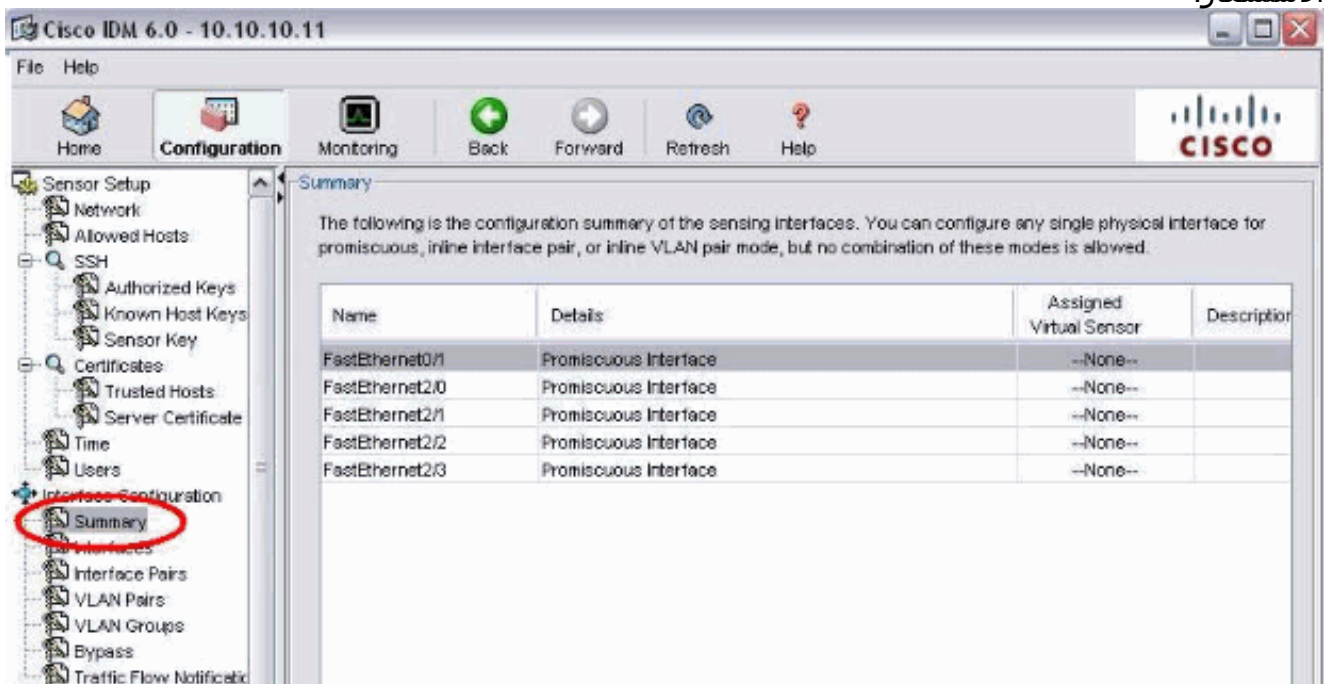
Interface	Link	Enabled	Speed	Mode
FastEthernet2/2	Down	Yes	N/A	Unpaired
FastEthernet2/1	Down	Yes	N/A	Unpaired
FastEthernet2/0	Down	Yes	N/A	Unpaired
FastEthernet0/1	Down	Yes	N/A	Unpaired
FastEthernet2/3	Down	Yes	N/A	Unpaired

Below the table, it says: "Select an interface to view received and transmitted packets count."

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 وحدد اسم الواجهة. طقطقت بعد ذلك يمكن in order to يمكنك الاستشعار قارن. قم أيضا بتكوين معلومات الإرسال ثنائي الإنجاه والسرعة وشبكة VLAN.



Cisco IDM 6.0 - 10.10.10.11

File Help

Home Configuration Monitoring Back Forward Refresh Help

Sensor Setup

- Network
- Allowed Hosts
- SSH
  - Authorized Keys
  - Known Host Keys
  - Sensor Key
- Certificates
- Trusted Hosts
- Server Certificate
- Time
- Users
- Interface Configuration
  - Summary
  - Interfaces**
  - Interface Pairs
  - VLAN Pairs
  - VLAN Groups
  - Bypass
  - Traffic Flow Notification
- Analysis Engine
  - Virtual Sensors
  - Global Variables
- Policies
  - Signature Definitions
    - sig0
  - Event Action Rules
    - rules0
  - Anomaly Detections
    - ad0
- Blocking
  - Blocking Properties

Interfaces

A sensing interface must be enabled and assigned to a virtual sensor before the sensor will monitor that interface. You can enable/disable the available sensing interfaces by selecting the row(s) and clicking Enable or Disable.

Interface Name	Enabled	Media Type	Duplex	Speed	Default VLAN
FastEthernet0/1	Yes	TX (copper)	Auto	Auto	
FastEthernet2/0	Yes	TX (copper)	Auto	Auto	
FastEthernet2/1	Yes	TX (copper)	Auto	Auto	
FastEthernet2/2	Yes	TX (copper)	Auto	Auto	
FastEthernet2/3					

Select All Edit Enable

**Edit Interface**

Interface Name: FastEthernet2/0

Enabled:  Yes  No

Media Type: TX (copper)

Duplex: Auto

Speed: Auto

Default VLAN: 0

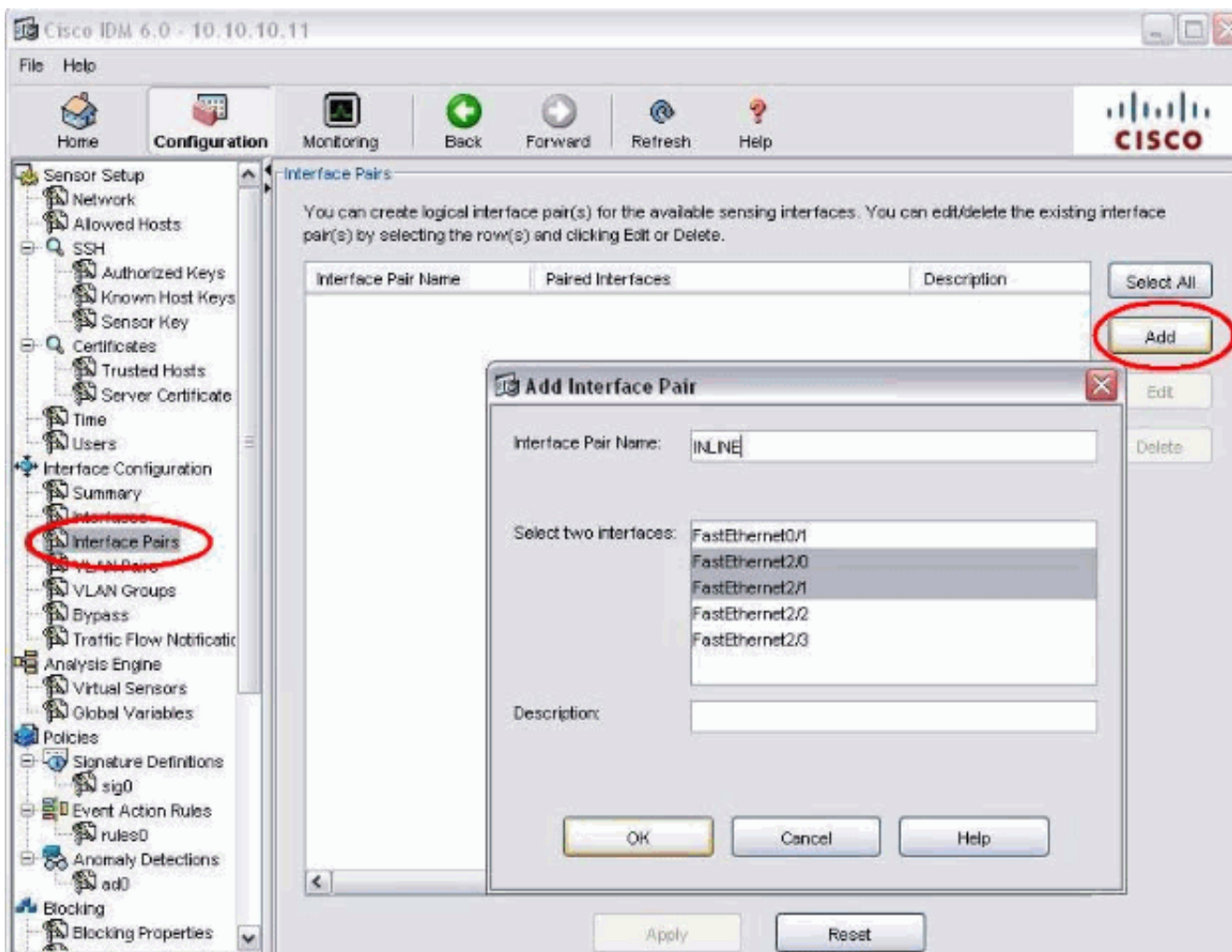
Use Alternate TCP Reset interface

Select interface: FastEthernet0/1

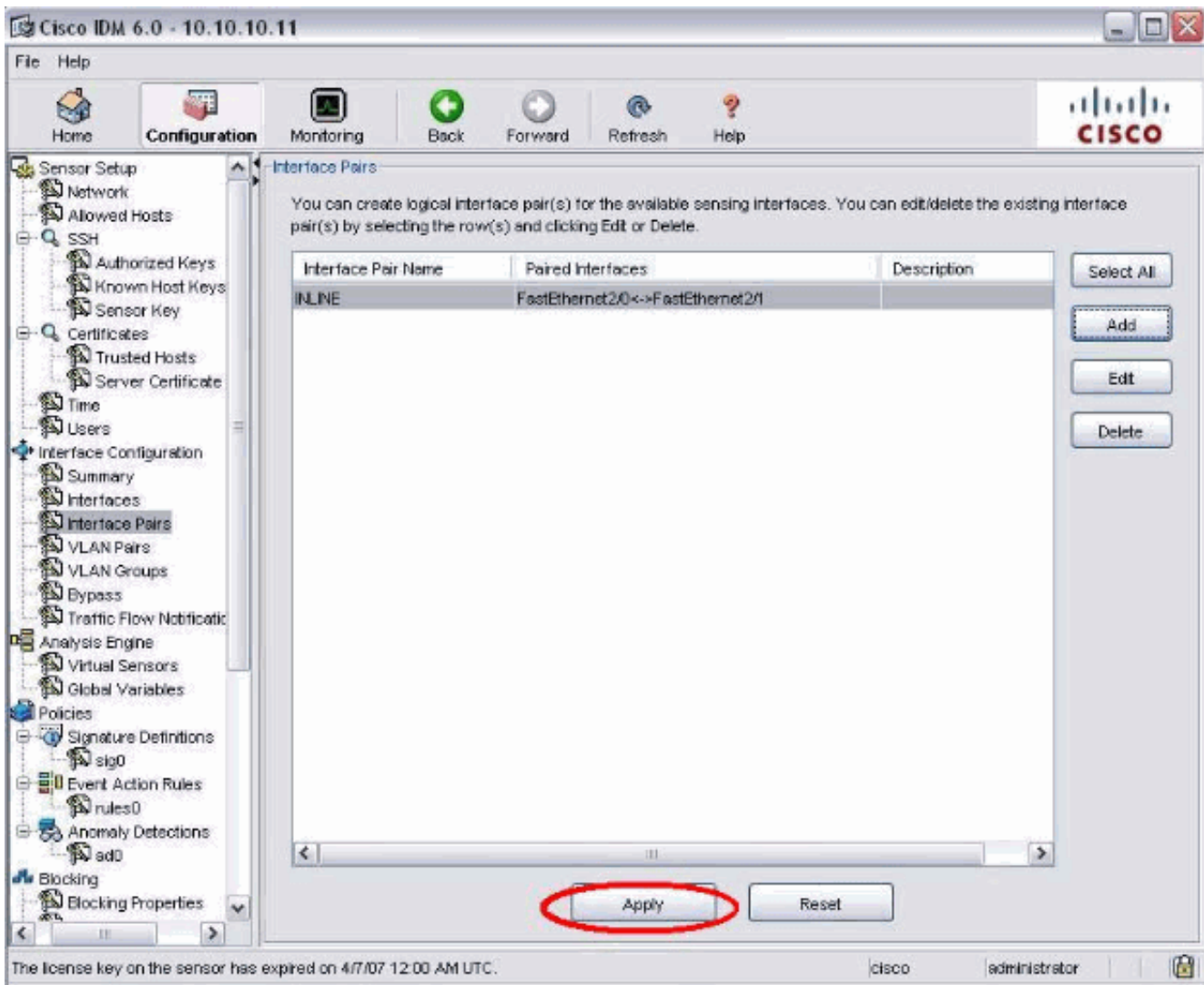
Description:

OK Cancel Help

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.

Cisco IDM 6.0 - 10.10.10.11

File Help

Home Configuration Monitoring Back Forward Refresh Help

Sensor Setup

- Network
  - Allowed Hosts
  - SSH
    - Authorized Keys
    - Known Host Keys
    - Sensor Key
  - Certificates
    - Trusted Hosts
    - Server Certificate
  - Time
  - Users
- Interface Configuration
  - Summary
  - Interfaces
  - Interface Pairs
  - VLAN Pairs
  - VLAN Groups
  - Bypass
  - Traffic Flow Notificatio
- Analysis Engine
  - Virtual Sensors
  - Global variables
- Policies
  - Signature Definitions
    - sig0
  - Event Action Rules
    - rules0
  - Anomaly Detections
    - ad0
- Blocking
  - Blocking Properties

Virtual Sensors

The sensor monitors traffic that traverses interfaces, interface pairs, or VLAN pairs assigned to a virtual sensor. You can create a new virtual sensor by clicking Add. You can edit or delete an existing virtual sensor by selecting the row(s) and clicking Edit or Delete.

Name	Assigned Interfaces (or Pairs)	Sig Definition Policy	Event Act Pol
vs0		sig0	

Select All

Add

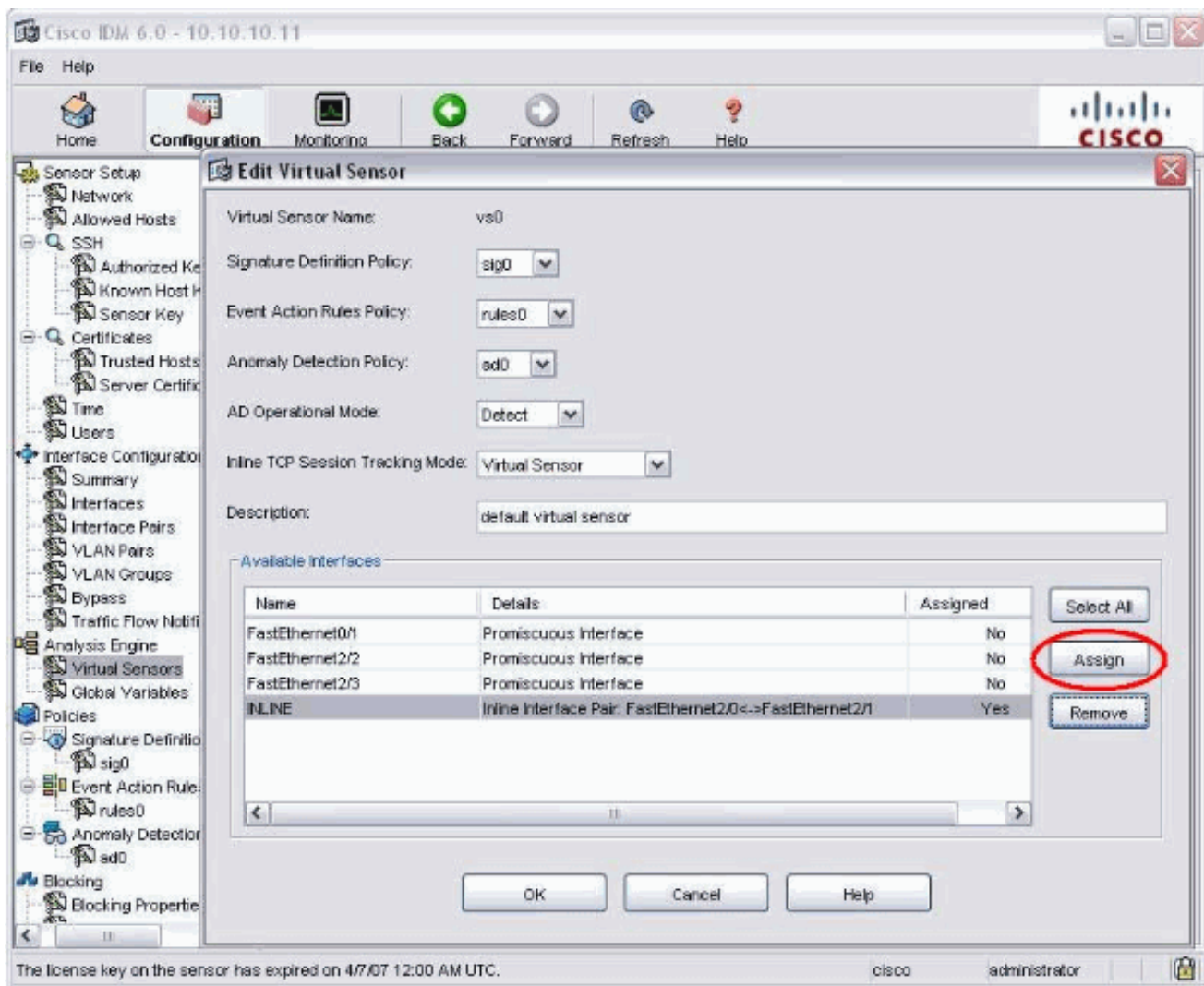
Edit

Delete

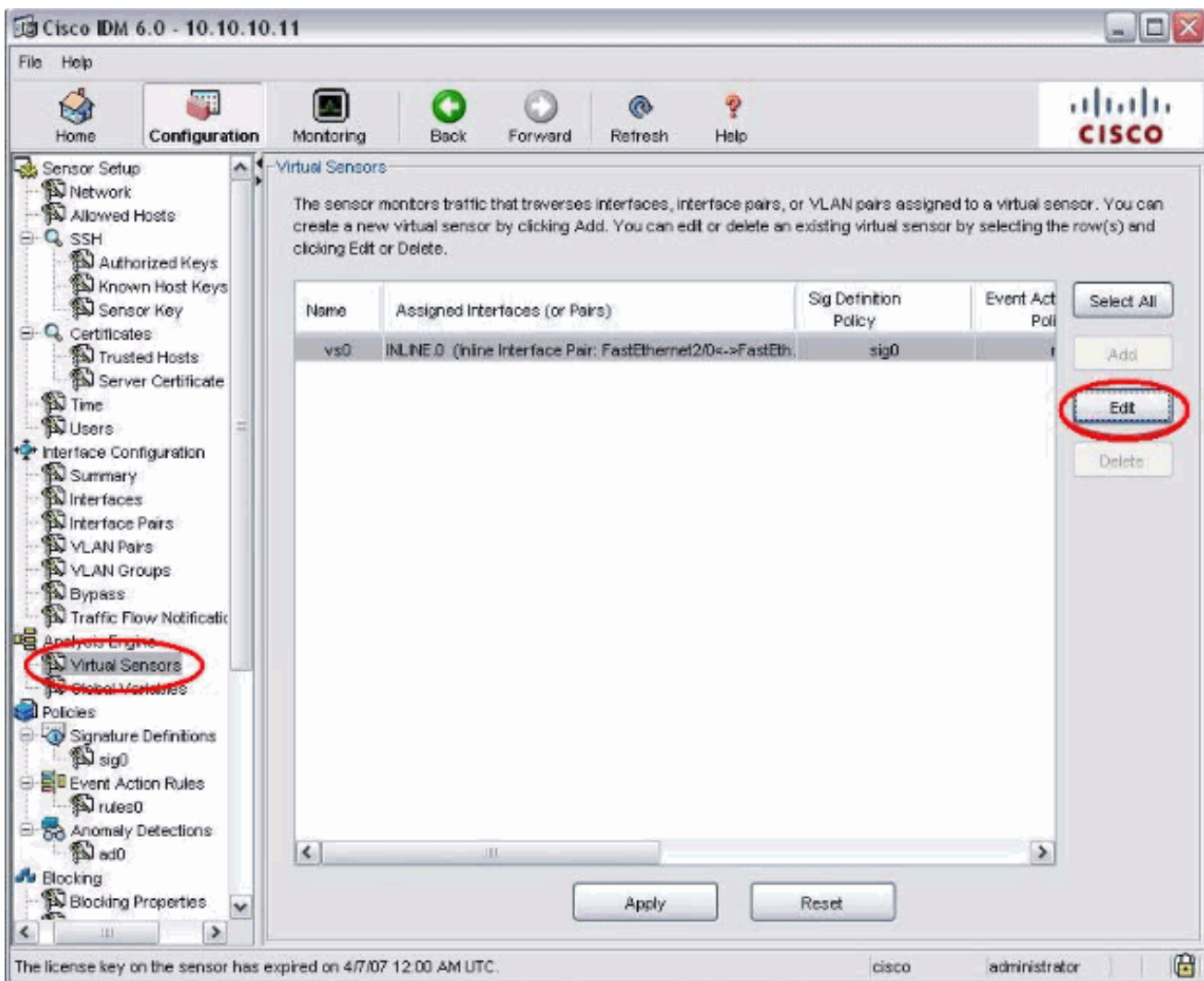
Apply Reset

The license key on the sensor has expired on 4/7/07 12:00 AM UTC. | cisco administrator

10. قم بتعيين الزوج المضمن في السطر إلى المستشعر الظاهري مقابل 0.



11. عرض ملخص معلومات المستشعر الظاهري المعينة.



## شكلت المفتاح ل IDSM-2 في خط أسلوب

أحلت ال بشكل المادة حفازة 6500 sery 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 لمنع الاقتحام Cisco](#)
- [أجهزة إستشعار Cisco IPS 4200 Series](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا ذه Cisco ت مچرت  
م ل ا ل اء ان ا ع مچ ي ف ن م دخت س م ل ل م عد و ت ح م م ي دقت ل ة ي ر ش ب ل و  
امك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ال م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب  
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ال ا ة مچرت ل ا ع م ل ا ح ل ا و ه  
ل ا ا م اء ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco  
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا