

# جوز عضو و: IDSM2/ثدحأل ا تارادصإل او IPS 5.x ل اثم مادختساب ةنمضمم ل ا VLAN تالكبش IDM و CLI نيوكت

## المحتويات

[المقدمة](#)

[المتطلبات الأساسية](#)

[المتطلبات](#)

[المكونات المستخدمة](#)

[المنتجات ذات الصلة](#)

[الاصطلاحات](#)

[تكوين التقاط VACL](#)

[تكوين وضع زوج شبكات VLAN المضمنة](#)

[تكوين واجهة سطر الأوامر \(CLI\)](#)

[تكوين IDM](#)

[استكشاف الأخطاء وإصلاحها](#)

[معلومات ذات صلة](#)

## المقدمة

يعرف اقتران شبكات VLAN في أزواج على واجهة مادية باسم وضع زوج شبكات VLAN المضمنة. يتم تحليل الحزم المستلمة على أحد شبكات VLAN المقترنة وإعادة توجيهها إلى شبكة VLAN الأخرى في الزوج. يتم دعم أزواج الشبكات المحلية الظاهرية (VLAN) المضمنة على جميع أجهزة الاستشعار المتوافقة مع نظام منع التسلسل (5.1 IPS)، باستثناء NM-CIDS و AIP-SSM-10 و AIP-SSM-20.

وضع زوج شبكة VLAN المضمنة هو وضع إستشعار نشط حيث تعمل واجهة الاستشعار كمنفذ خط اتصال 802.1Q، ويقوم المستشعر بتنفيذ ربط شبكة VLAN بين أزواج الشبكات المحلية الظاهرية (VLANs) على خط الاتصال. هذا يعني أن المفتاح يربط إلى الاستشعار قارن ينبغي كنت في شحنة أسلوب.

يقوم المستشعر بفحص حركة المرور التي تتلقاها على كل شبكة VLAN في كل زوج، ويمكن أن يقوم إما بإعادة توجيه الحزم على شبكة VLAN الأخرى في الزوج أو إسقاط الحزمة إذا تم اكتشاف محاولة إقحام. يمكنك تكوين مستشعر IPS لإنشاء جسر حتى 255 زوج من شبكات VLAN في نفس الوقت على كل واجهة إستشعار. يستبدل المستشعر ال VLAN id مجال في ال 802.1q رأس من كل ربط يستلم مع ال id من مخرج VLAN على أي المستشعر يرسل الربط. يقوم المستشعر بإسقاط جميع الحزم المستلمة على أي شبكات VLAN لا يتم تعيينها إلى أزواج VLAN المضمنة.

**ملاحظة:** بالنسبة ل IPS-4260، لا يتم دعم تجاوز الأجهزة التي تفتح الأعطال على أزواج VLAN المضمنة. راجع [تقيدات تكوين تجاوز الأجهزة](#) للحصول على مزيد من المعلومات.

## المتطلبات الأساسية

## المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

## المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى مستشعر نظام منع الاقتحام من Cisco الذي يستخدم الإصدار 5.1 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.

## المنتجات ذات الصلة

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

## الاصطلاحات

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

## تكوين التقاط VACL

أحلت ال [بشكل VACL التقاط](#) قسم من [بشكل](#) `IDS-2 in order to` أرسلت حركة مرور إلى ال `IDS-2` على المفتاح.

## تكوين وضع زوج شبكات VLAN المضمنة

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

**ملاحظة:** استخدم [أداة بحث الأوامر](#) (للعلماء [المسجلين](#) فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

أستخدم الأمر `physical-interfaces interface_name` في الوضع الفرعي لواجهة الخدمة لتكوين أزواج VLAN المضمنة باستخدام CLI (واجهة سطر الأوامر). اسم الواجهة هو `FastEthernet` أو `GigabitEthernet`.

يتم تطبيق هذه الخيارات:

- تم تمكين الحالة `{admin {enabled | disabled}}` — حالة الارتباط الإداري للواجهة، سواء كانت الواجهة ممكنة أو معطلة. **ملاحظة:** في جميع واجهات إستشعار اللوحة الخلفية في جميع الوحدات النمطية (IDS-2 NM-CIDS، و AIP-SSM)، يتم تعيين حالة المسؤول إلى تمكين وهي محمية (لا يمكنك تغيير الإعداد). لا يكون لـ `admin-state` أي 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.
- الإرسال ثنائي الإتجاه — إعداد الإرسال ثنائي الإتجاه للواجهة `auto`—يضبط الواجهة على التفاوض التلقائي على الإرسال ثنائي الإتجاه `full`—يضبط الواجهة إلى الإرسال ثنائي الإتجاه الكامل `half`—يضبط الواجهة إلى `half-duplex`. **ملاحظة:** خيار الإرسال ثنائي الإتجاه محمي على جميع الوحدات النمطية.
- لا — يزيل إعداد إدخال أو تحديد.

- **السرعة**—إعداد سرعة الواجهة. **تلقائي**—يضبط الواجهة إلى سرعة التفاوض التلقائي. 10—يضبط الواجهة إلى 10 ميغابايت (لواجهات TX فقط). 100—يضبط الواجهة إلى 100 ميغابايت (لواجهات TX فقط). 1000—يضبط الواجهة إلى 1 غيغابايت (لواجهات جيغابت) **ملاحظة**: خيار السرعة محمي على جميع الوحدات النمطية.
- **subinterface-type**— يحدد أن الواجهة هي واجهة فرعية وما هو نوع الواجهة الفرعية المحدد. **inline-vlan-pair**— يتيح لك تعريف الواجهة الفرعية كزوج شبكات VLAN داخلي. **none**— لم يتم تعريف واجهات فرعية.
- **الواجهة الفرعية**— يحدد الواجهة الفرعية كزوج شبكات VLAN داخلي. **VLAN1**— شبكة VLAN الأولى في زوج شبكات VLAN الداخلي. **VLAN2**— الشبكة المحلية الظاهرية (VLAN) الثانية في زوج شبكات VLAN الداخلي.

## تكوين واجهة سطر الأوامر (CLI)

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

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 يكون نوع الواجهة الفرعية "بلا" إذا لم يتم تكوين واجهات داخل السطر):

```
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
- -----  
-----  
-----
- 4** أزلت أي قارن داخل أن يستعمل هذا قارن طبيعي:
- ```
sensor(config-int)#no inline-interfaces interface_name
```
- 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** تحديد واجهة:
- ```
sensor(config-int)#physical-interfaces GigabitEthernet0/2
```
- 7** مكنت ال admin-دولة من القارن:
- ```
sensor(config-int-phy)#admin-state enabled
```
- 8** يجب تعيين الواجهة للمستشعر الظاهري وتمكينها لمراقبة حركة المرور.  
إضافة وصف لهذه الواجهة:
- ```
sensor(config-int-phy)#description INT1
```
- 9** تكوين إعدادات الإرسال ثنائي الإتجاه:
- ```
sensor(config-int-phy)#duplex full
```
- هذا الخيار غير متوفر على الوحدات النمطية.
- 10** قم بتكوين السرعة:
- ```
sensor(config-int-phy)#speed 1000
```
- 11** هذا الخيار غير متوفر على الوحدات النمطية.  
قم بإعداد زوج شبكات VLAN الداخلي:
- ```
sensor(config-int-phy)#subinterface-type inline-vlan-pair  
sensor(config-int-phy-inl)#subinterface 1  
sensor(config-int-phy-inl-sub)#vlan1 52  
sensor(config-int-phy-inl-sub)#vlan2 53
```
- 12** إضافة وصف لزوج شبكات VLAN الداخلي:
- ```
sensor(config-int-phy-inl-sub)#description pairs vlans 52 and 53
```

### 13. دقت ال VLAN زوج عملية إعداد:

```
sensor(config-int-phy-inl-sub)#show settings
subinterface-number: 1
```

```
-----
:description: VLANpair1 default
vlan1: 52
vlan2: 53
-----
```

```
##(sensor(config-int-phy-inl-sub
```

### 14. خرجت القارن `submode`:

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

### 15. اضغط على `Enter` لتطبيق التغييرات، أو أدخل `no` لتجاهلها.

.16

دخلت الفعلي مستشعر تشكيل أسلوب:

```
sensor(config)#service analysis-engine
sensor(config-ana)#virtual-sensor vs0
```

.17

إضافة الواجهة إلى المستشعر الظاهري:

```
sensor(config-ana-vir)#physical-interface GigabitEthernet0/2
subinterface-number 1
```

### 18. قم بالخروج من الوضع الفرعي للمستشعر الظاهري:

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

### 19. اضغط على `Enter` لتطبيق التغييرات، أو أدخل `no` لتجاهلها.

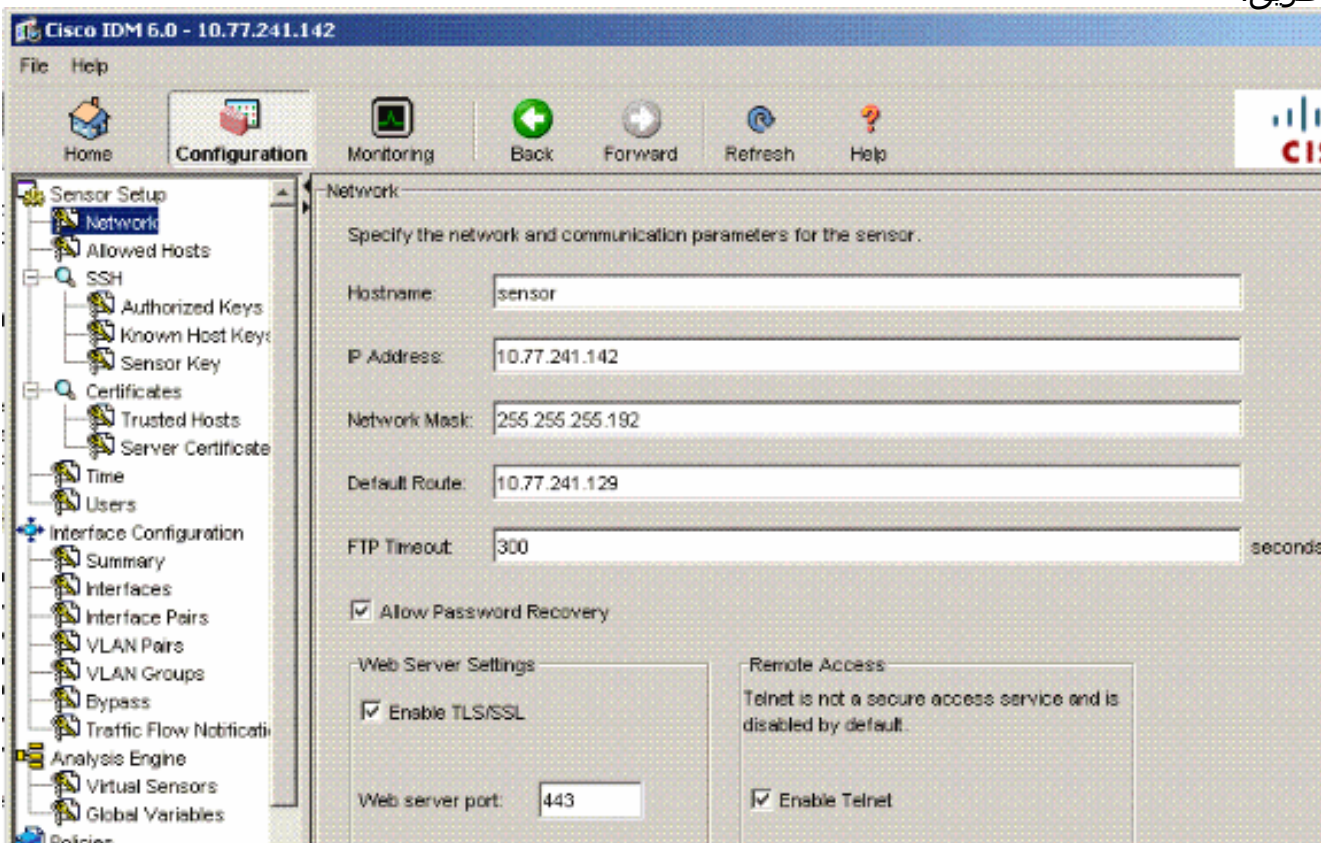
## تكوين IDM

أكمل الخطوات التالية لتكوين إعدادات زوج شبكات VLAN المضمنة على المستشعر باستخدام مدير أجهزة IDS ((IDM:

1. افتح المستعرض وأدخل `<https://<management_ip_address_of_ips` للوصول إلى IDM على IPS.
2. انقر فوق `تنزيل مشغل IDM` وابدأ IDM لتنزيل المثبت الخاص بالتطبيق.
3. انتقل إلى الصفحة الرئيسية لعرض معلومات الجهاز مثل اسم المضيف وعنوان IP والإصدار والنموذج، وما إلى ذلك.

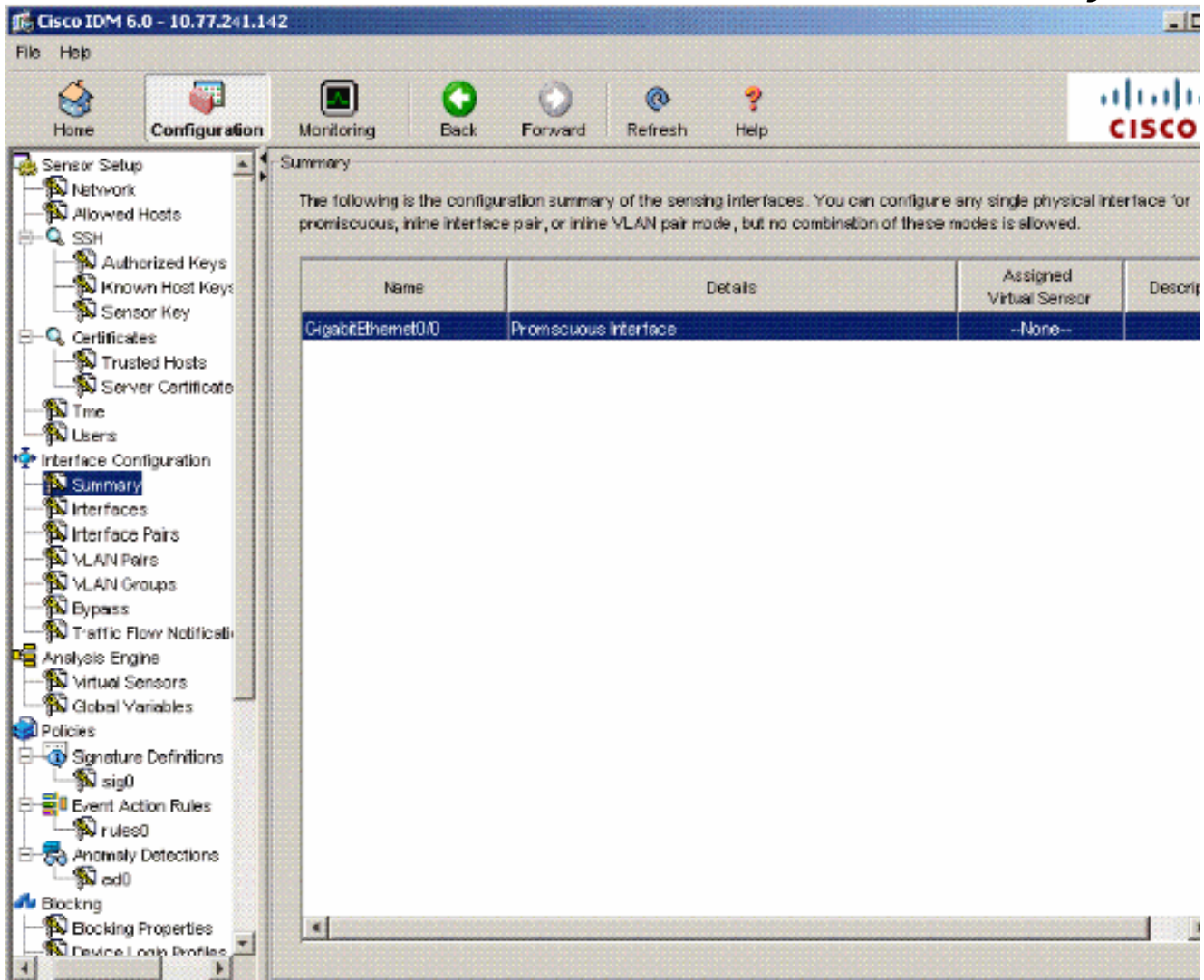


4. انتقل إلى التكوين < إعداد المستشعر وانقر فوق الشبكة. هنا أنت يستطيع عينت ال hostname، عنوان وقصير طريق.





5. انتقل إلى التكوين < تكوين الواجهة وانقر فوق ملخص. تعرض هذه الصفحة ملخص تكوين واجهة الاستشعار.



The screenshot shows the Cisco IDM 6.0 Configuration page. The left sidebar contains a tree view with categories like Sensor Setup, Network, Allowed Hosts, SSH, Authorized Keys, Known Host Keys, Sensor Key, Certificates, Trusted Hosts, Server Certificate, Time, Users, Interface Configuration, Analysis Engine, Policies, Signature Definitions, Event Action Rules, Anomaly Detections, and Blocking. The 'Interface Configuration' category is expanded, and the 'Summary' sub-item is selected. The main content area displays a table with the following data:

| Name               | Details               | Assigned Virtual Sensor | Description |
|--------------------|-----------------------|-------------------------|-------------|
| GigabitEthernet0/0 | Promiscuous Interface | --None--                |             |

6. انتقل إلى التكوين < تكوين الواجهة < الواجهات وحدد اسم الواجهة. ثم انقر فوق تمكين لتمكين واجهة الاستشعار. قم أيضا بتكوين معلومات الإرسال ثنائي الاتجاه والسرعة وشبكة VLAN.



Cisco IDM 6.0 - 10.77.241.142

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
    - ed0
- 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 |
|--------------------|---------|-------------|--------|-------|--------------|
| GigabitEthernet0/0 | Yes     | TX (copper) | Auto   | Auto  |              |

Select All Edit Enable Disable

**Edit Interface**

Interface Name: GigabitEthernet0/0

Enabled:  Yes  No

Media Type: TX (copper)

Duplex: Auto

Speed: Auto

Default VLAN: 0

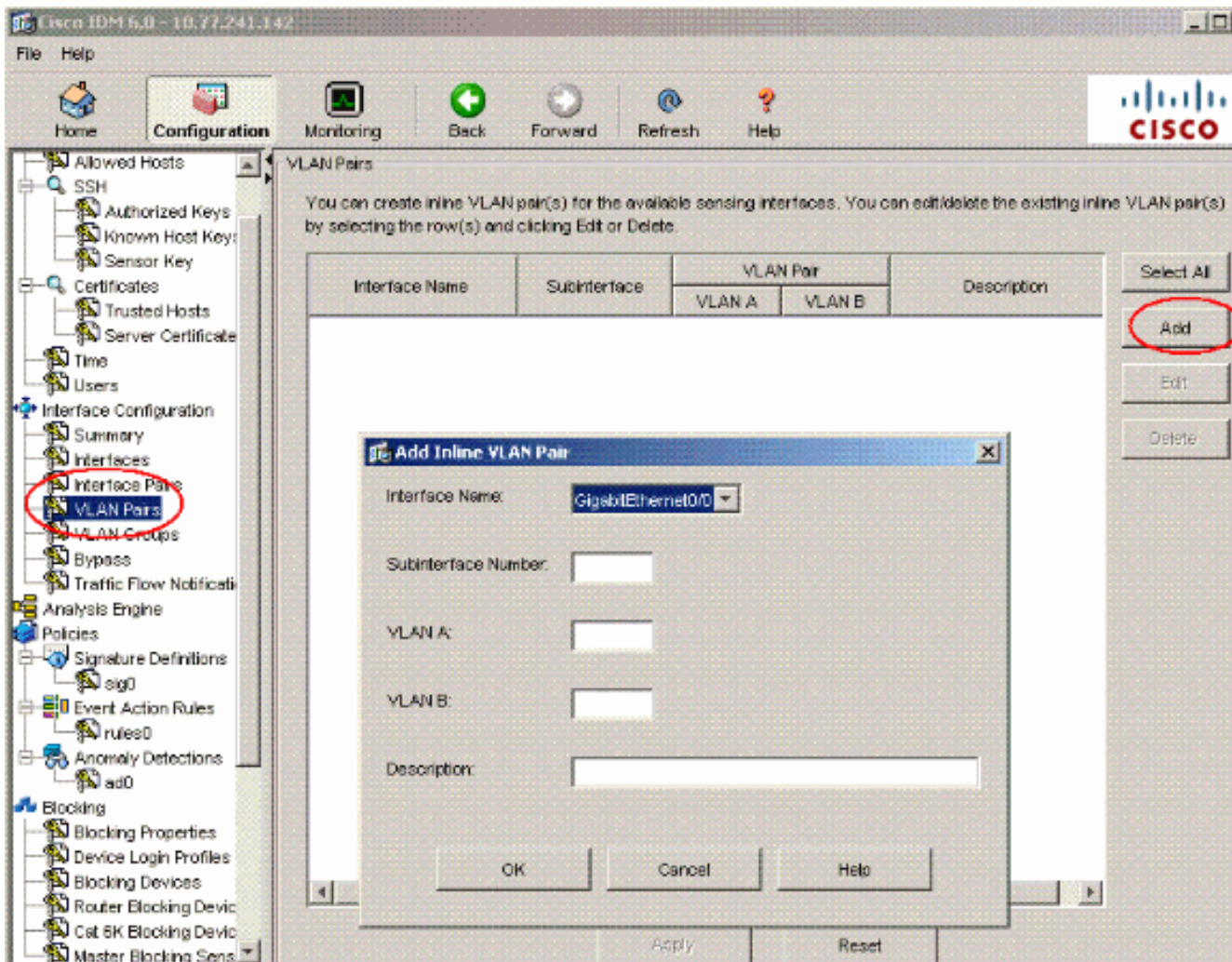
Use Alternate TCP Reset Interface

Select interface: [v]

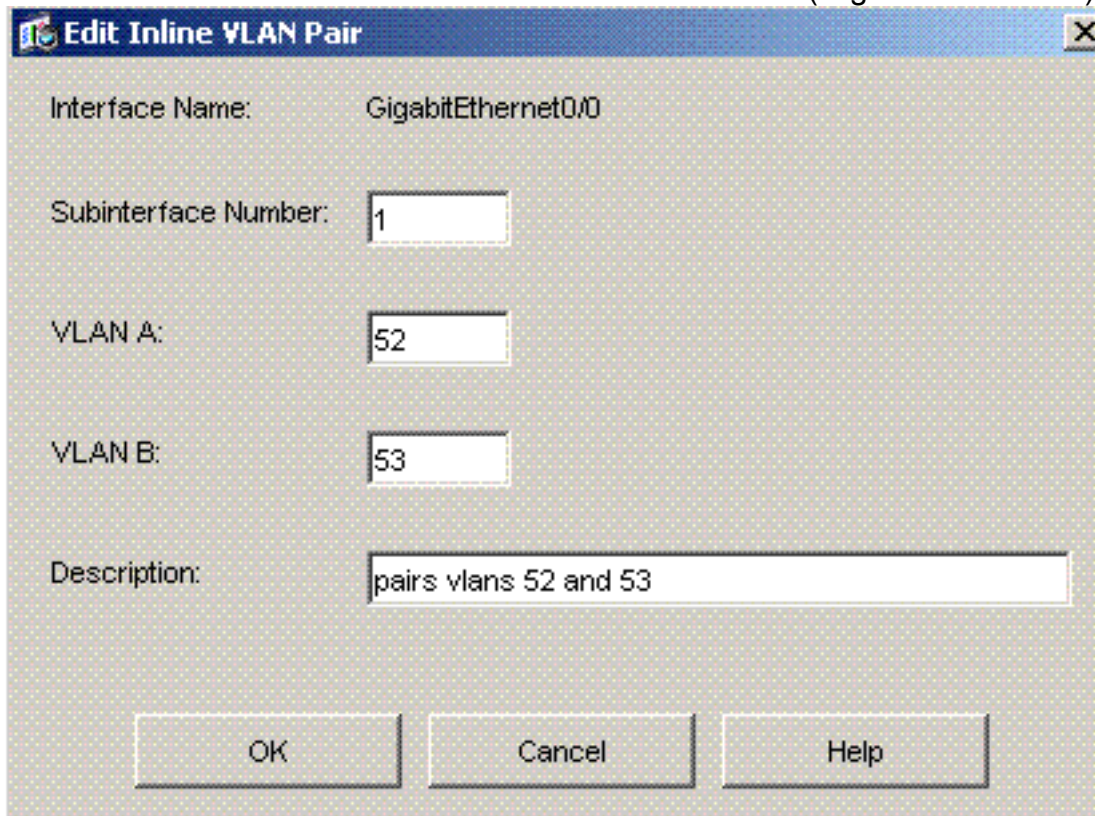
Description: [ ]

OK Cancel Help

7. انتقل إلى التكوين < واجهة التكوين > أزواج شبكات VLAN وانقر فوق إضافة لإنشاء أزواج شبكات VLAN المضمنة.



8. دخلت ال subinterface رقم، VLAN A و VLAN B ل الاستشعار قارن (GigabitEthernet0/0).



يمكنك عرض

ملخص تكوين زوج شبكات VLAN المضمنة.



Cisco IDM 6.0 - 10.77.241.142

File Help

Home Configuration Monitoring Back Forward Refresh Help

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  
Policies  
Signature Definitions  
sig0  
Event Action Rules  
rules0  
Anomaly Detections  
ad0  
Blocking  
Blocking Properties  
Device Login Profiles  
Blocking Devices  
Router Blocking Device  
Cat 6K Blocking Device  
Master Blocking Sens

VLAN Pairs

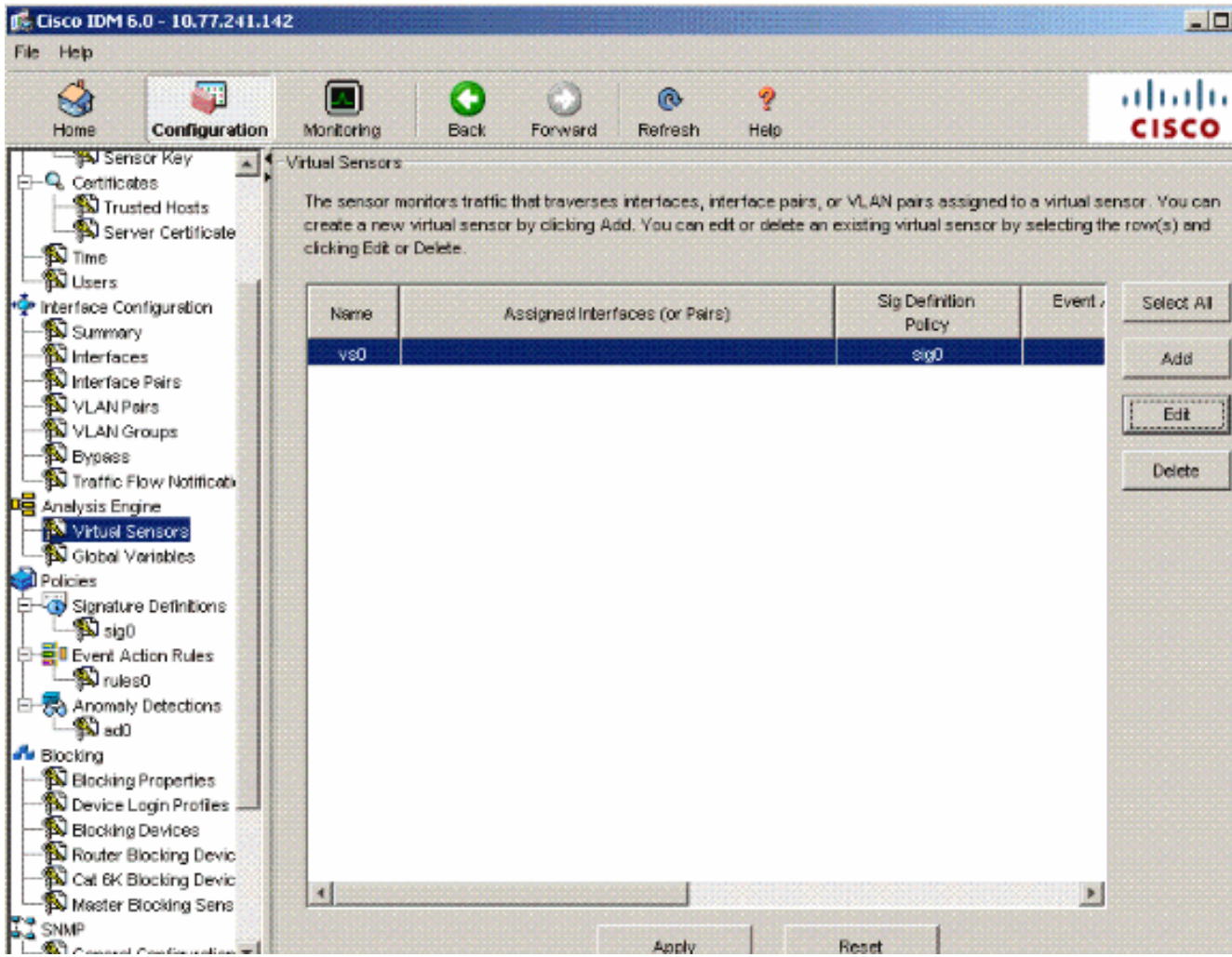
You can create inline VLAN pair(s) for the available sensing interfaces. You can edit/delete the existing inline VLAN pair(s) by selecting the row(s) and clicking Edit or Delete.

| Interface Name     | Subinterface | VLAN Pair |        | Description           |
|--------------------|--------------|-----------|--------|-----------------------|
|                    |              | VLAN A    | VLAN B |                       |
| GigabitEthernet0/0 | 1            | 52        | 53     | pairs vlans 52 and 53 |

Select All  
Add  
Edit  
Delete

Apply Reset

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



10. قم بتخصيص زوج شبكة VLAN المضمنة 52 و 53 للمستشعر الظاهري مقابل 0.

**Edit Virtual Sensor**

Virtual Sensor Name: vs0

Signature Definition Policy: sig0

Event Action Rules Policy: rules0

Anomaly Detection Policy: ad0

AD Operational Mode: Detect

Inline TCP Session Tracking Mode: Virtual Sensor

Description: default virtual sensor

Available Interfaces

| Name                 | Details                   | Assigned |
|----------------------|---------------------------|----------|
| GigabitEthernet0/0.1 | Inline VLAN Pair: 52<->53 | Yes      |

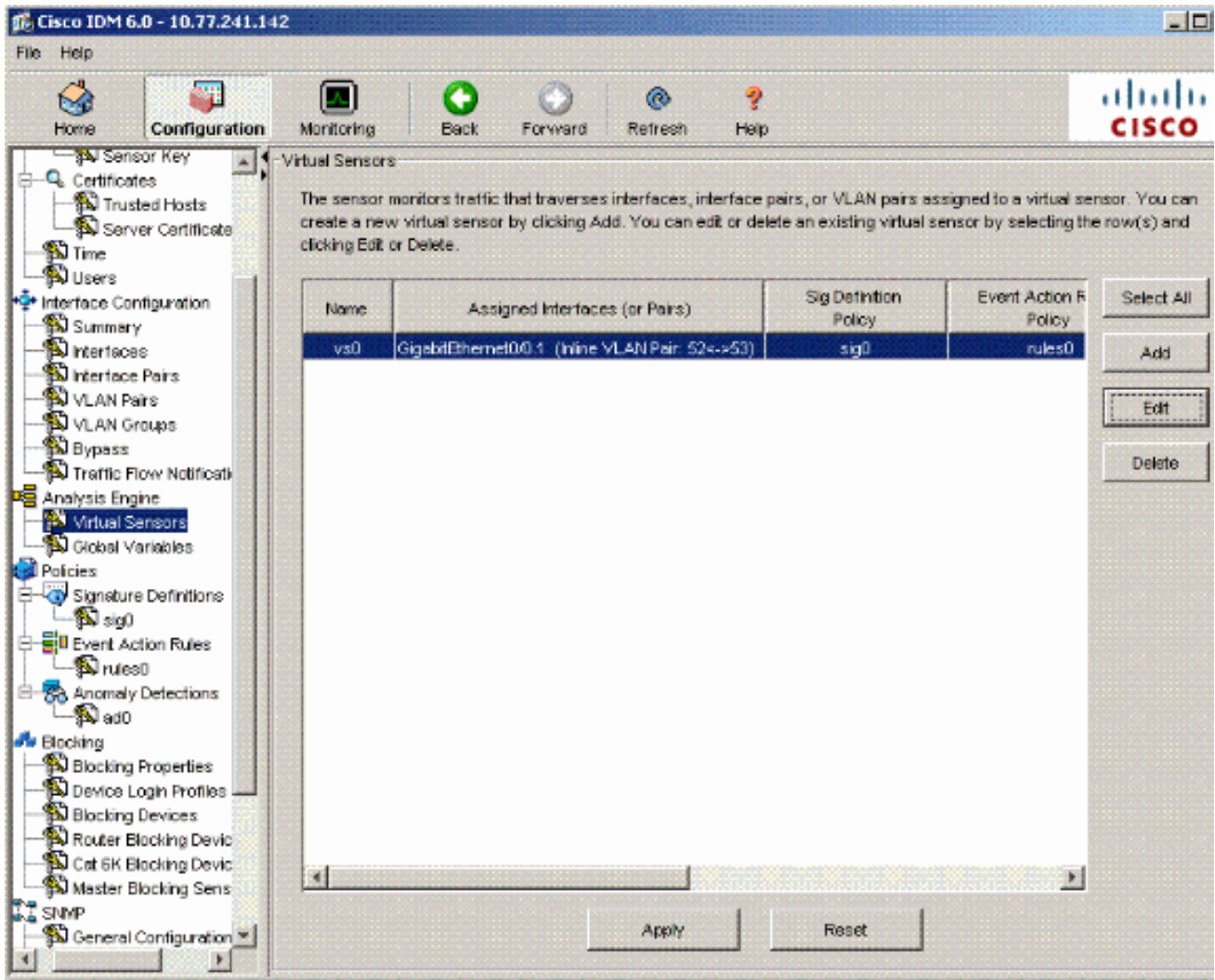
Select All

Assign

Remove

OK Cancel Help

عرض ملخص معلومات المستشعر الظاهري المعينة.



## استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

## معلومات ذات صلة

- [أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances](#)
- [نظام لمنع الاقتحام Cisco](#)
- [أجهزة استشعار 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 تسمل اذ ه Cisco ت مچرت  
ملاعلاء ان ا عي مچ ي ف ن ي م دخت سمل ل م عد ي و تح م مي دقت ل ة ي رش ب ل و  
امك ة ق ي قد ن و ك ت ن ل ة ي ل أ ة مچرت ل ض ف أ ن أ ة ظ حال م ي ج ر ي . ة ص ا خ ل 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 ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه  
ي ل ا م ئ ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه 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 أ ل ا ي ز ي ل ج ن ا ل ا دن تسمل ا