IPS 6.X及更高版本/IDSM2:使用IDM的內聯介面對模式配置示例

目錄

簡介

在內嵌介面配對模式下運作時，入侵防禦系統(IPS)會直接進入流量中，並影響封包轉送速率，這會在增加延遲時降低轉送速率。這使得感測器能夠停止攻擊，從而在其到達預定目標之前丟棄惡意通訊量，從而提供保護服務。內聯裝置不僅會處理第3層和第4層上的資訊，而且還會分析資料包的內容和負載，以便進行更複雜的嵌入式攻擊（第3層至第7層）。 這種更深入的分析讓系統能夠識別並阻止通常通過傳統防火牆裝置的攻擊。

在內嵌介面配對模式下，封包會透過感測器上配對的第一個介面進入，並流出配對的第二介面。資料包被傳送到該對的第二介面，除非該資料包被簽名拒絕或修改。

注意：您可以配置AIM-IPS和AIP-SSM以內聯方式運行，即使這些模組只有一個感應介面。

注意：**如**果成對介面連線到同一台交換機，您應該將交換機上的這些介面配置為具有兩個埠的不同接入VLAN的接入埠。否則，流量不會通過內嵌介面。

必要條件

需求

本文件沒有特定需求。

採用元件

本文檔中的資訊基於使用命令列介面6.0和入侵防禦系統裝置管理器(IDM)6.0的Cisco IPS感測器。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

相關產品

本文檔中的資訊也適用於入侵檢測系統(IDSM-2)服務模組。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

內嵌介面配對組態

在服務介面子模式下使用**inline-interfaces**name命令以建立內嵌介面對。

註：使用Command Lookup Tool(僅限註冊客戶)可獲取本節中使用的命令的詳細資訊。

注意：AIP-SSM是從Cisco ASA CLI而不是從Cisco IPS CLI配置為內聯介面模式。

這些選項適用：

- inline-interfaces *name* **— *邏輯內聯介面對的名稱*注意：在所有模組（IDSM-2 NM-CIDS和AIP-SSM）上的所有背板感應介面**上，**admin-state設定為enabled**且protected（您不能更改該設定）。 **admin-state**對命令和控制介面沒有影響（且受保護）。它只影響感應介面。不需要啟用命令和控制介面，因為無法對其進行監控。
- **default** — 將值設定回系統預設設定
- **description** — 內嵌介面配對的描述
- interface1 *interface_name* **— 內嵌介面配對中的第一個介面**
- interface2 *interface_name* **— 內嵌介面配對中的第二個介面**
- **no** — 移除條目或選取設定
- **admin-state {enabled | disabled}** — 介面的管理連結狀態，無論該介面是啟用還是禁用。

CLI組態

完成以下步驟，在感測器上設定內嵌VLAN對設定：

1. 使用具有管理員許可權的帳戶登入到CLI。
2. 進入介面子模式：
```
sensor#configure terminal
sensor(config)#service interface
sensor(config-int)#
```
3. 驗證是否存在任何內嵌介面。如果未配置任何內聯介面，則子介面型別應讀取為none:
```
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. 命名內嵌配對：

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

5. 顯示可用介面的清單：

```
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. 將兩個介面配置為一對：

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


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

您必須將介面分配給虛擬感測器並啟用它，然後虛擬感測器才能監控通訊量。如需詳細資訊，請參閱步驟10。

7. 新增此介面的說明：

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

8. 對要配置為內聯介面對的任何其他介面重複步驟4至7。
9. 驗證設定：

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

10. 啟用分配給介面對的介面：

```
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. 驗證介面是否已啟用：

```
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. 發出此命令，以刪除內嵌介面配對並將介面返回到混雜模式：

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

    您還必須將內聯介面對從分配給它的虛擬感測器中刪除。

13. 驗證內嵌介面配對是否已刪除：

```
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. 退出介面配置子模式：

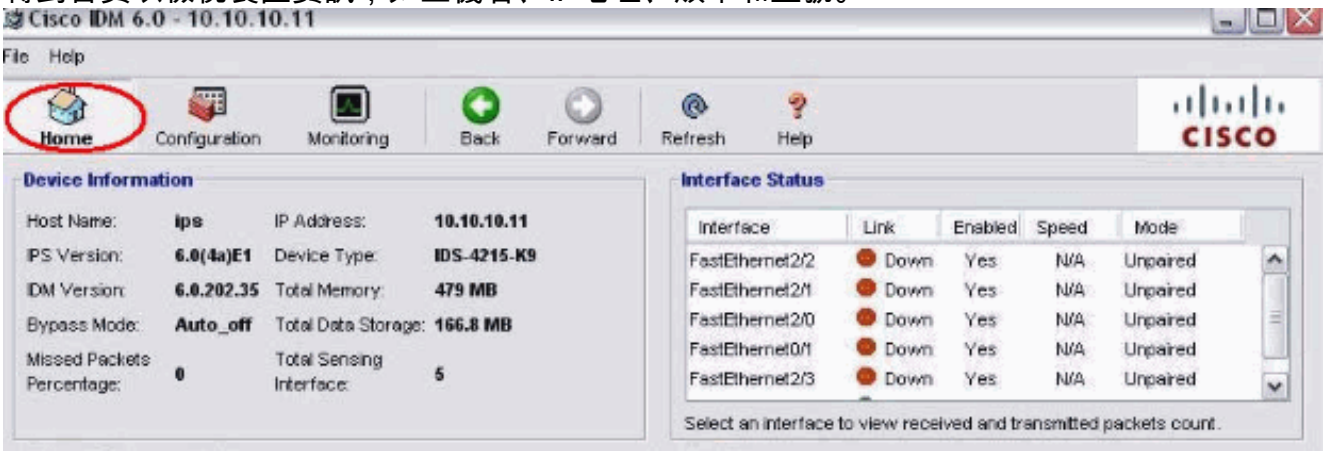
```
sensor(config-int)#exit
Apply Changes:?[yes]:
```

15. 按**Enter**以應用更改，或輸入**no**以放棄更改。

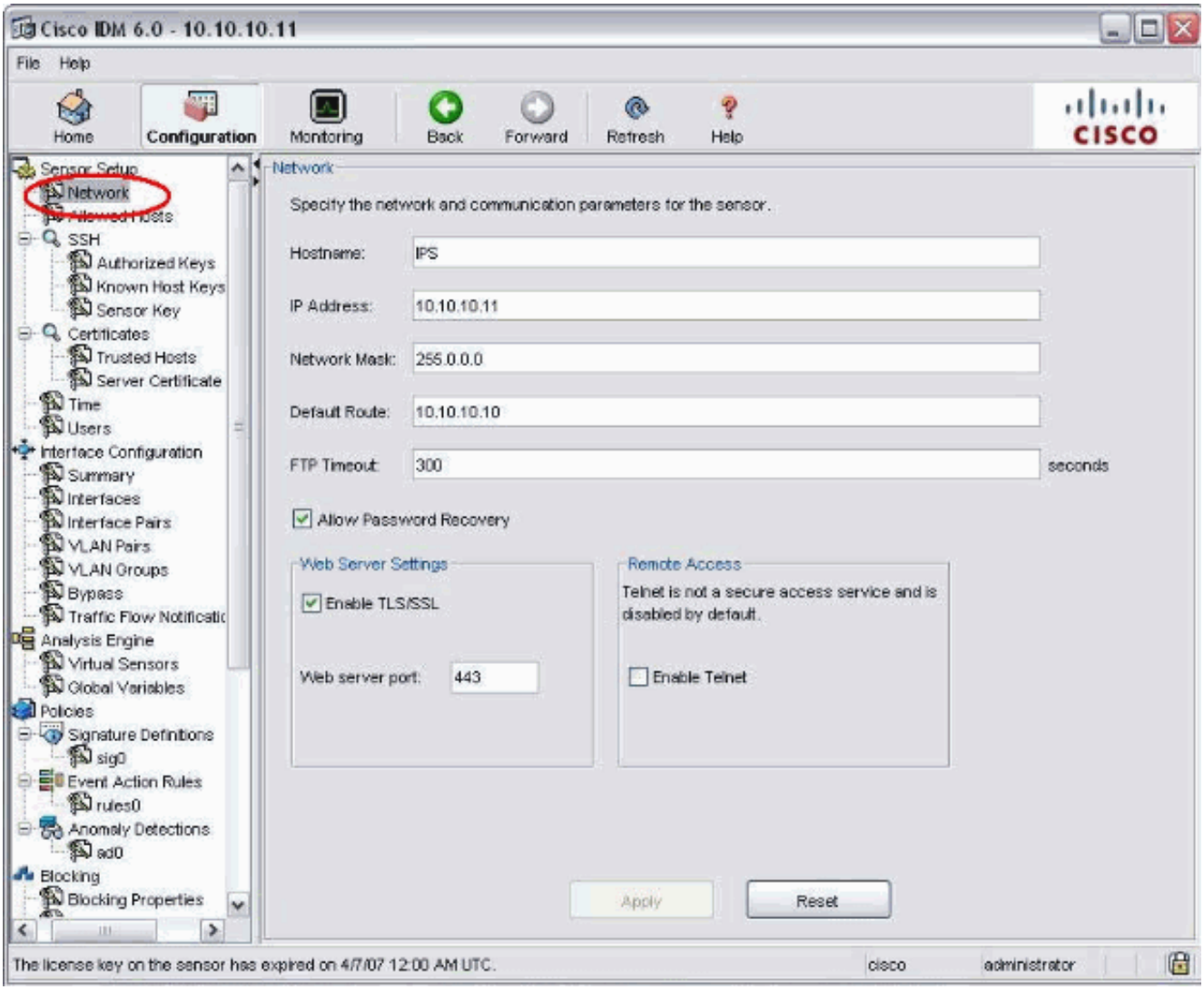
IDM配置

完成以下步驟，以便使用IDM在感測器上配置內聯VLAN對設定：

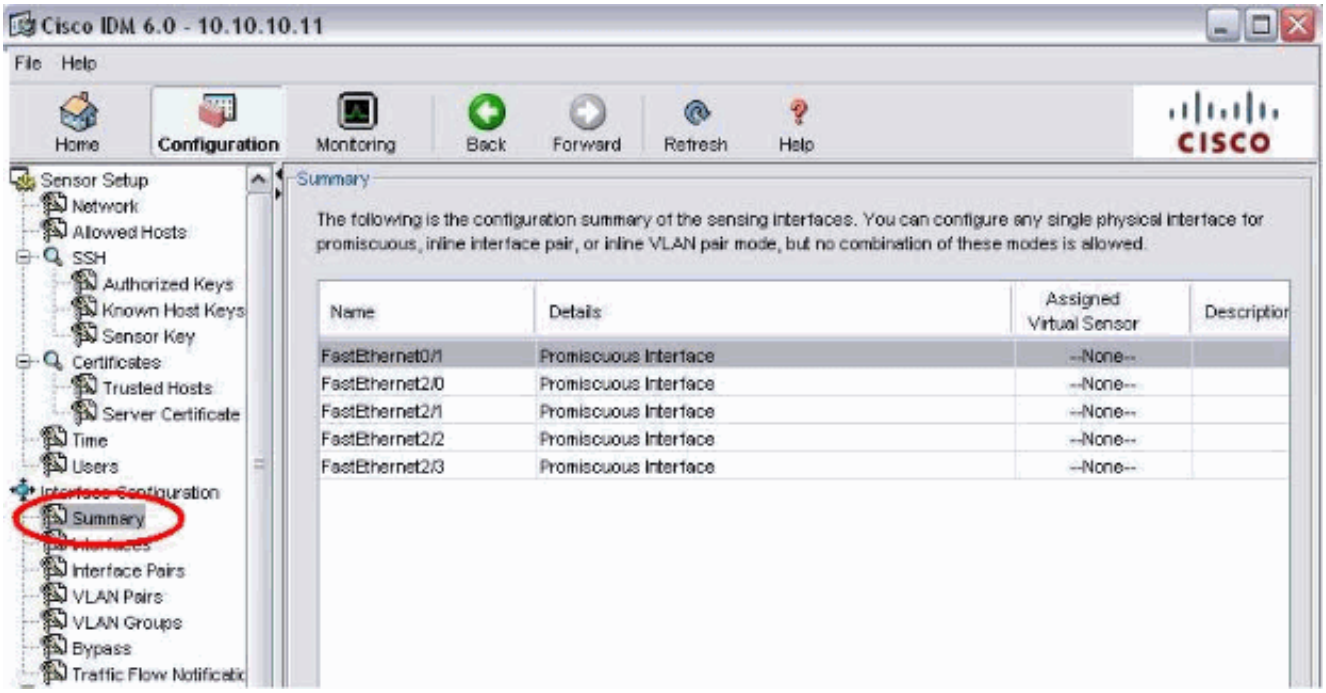
1. 開啟瀏覽器並輸入**https://<Management_IP_Address_of_IPS>**以訪問IPS上的IDM。
2. 按一下**Download IDM Launcher**和**Start IDM**，下載應用程式的安裝程式。
3. 轉到首頁以檢視裝置資訊，如主機名、IP地址、版本和型號。



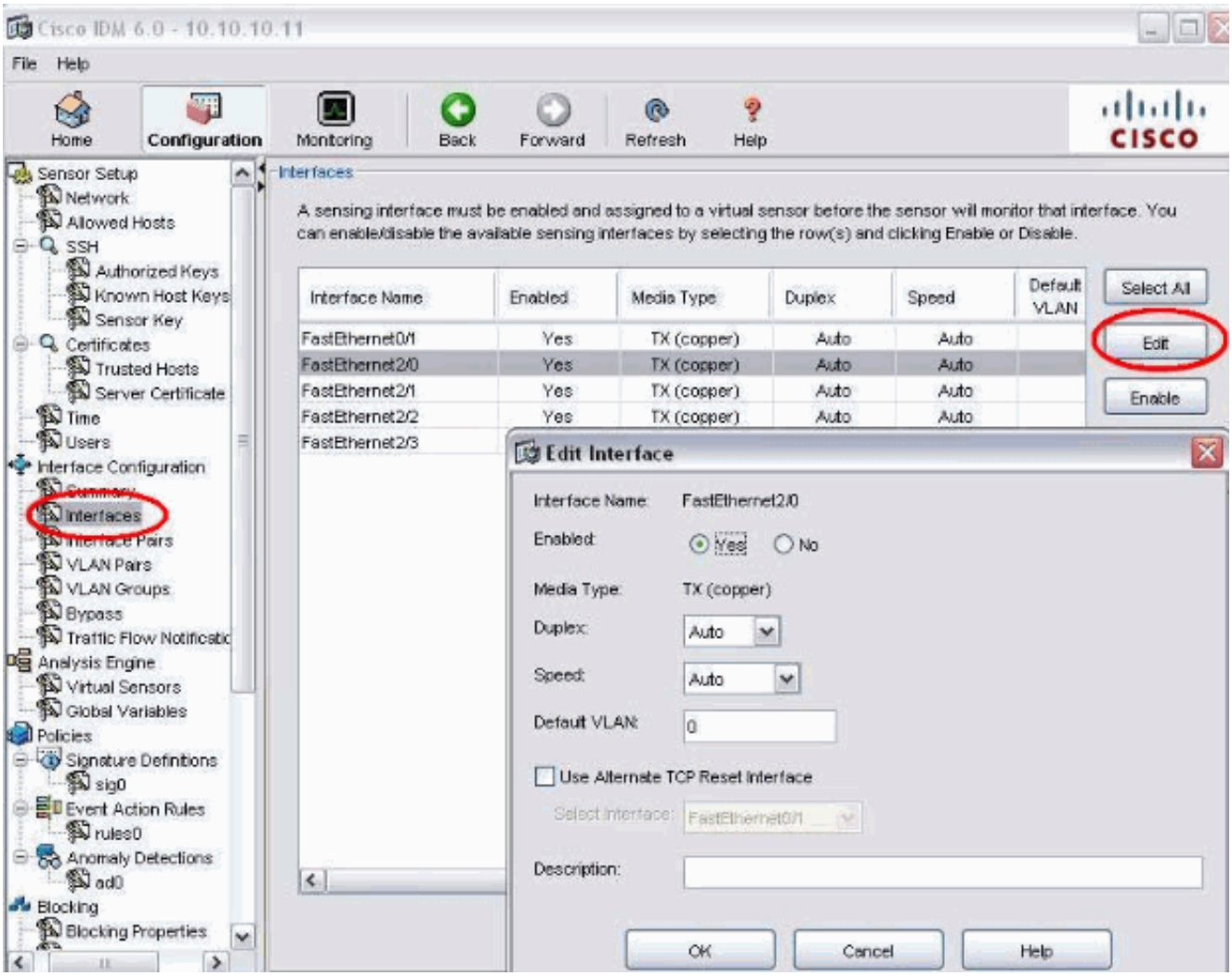
4. 轉到**Configuration > Sensor Setup**，然後按一下**Network**。您可以在此處指定主機名、IP地址和預設路由。



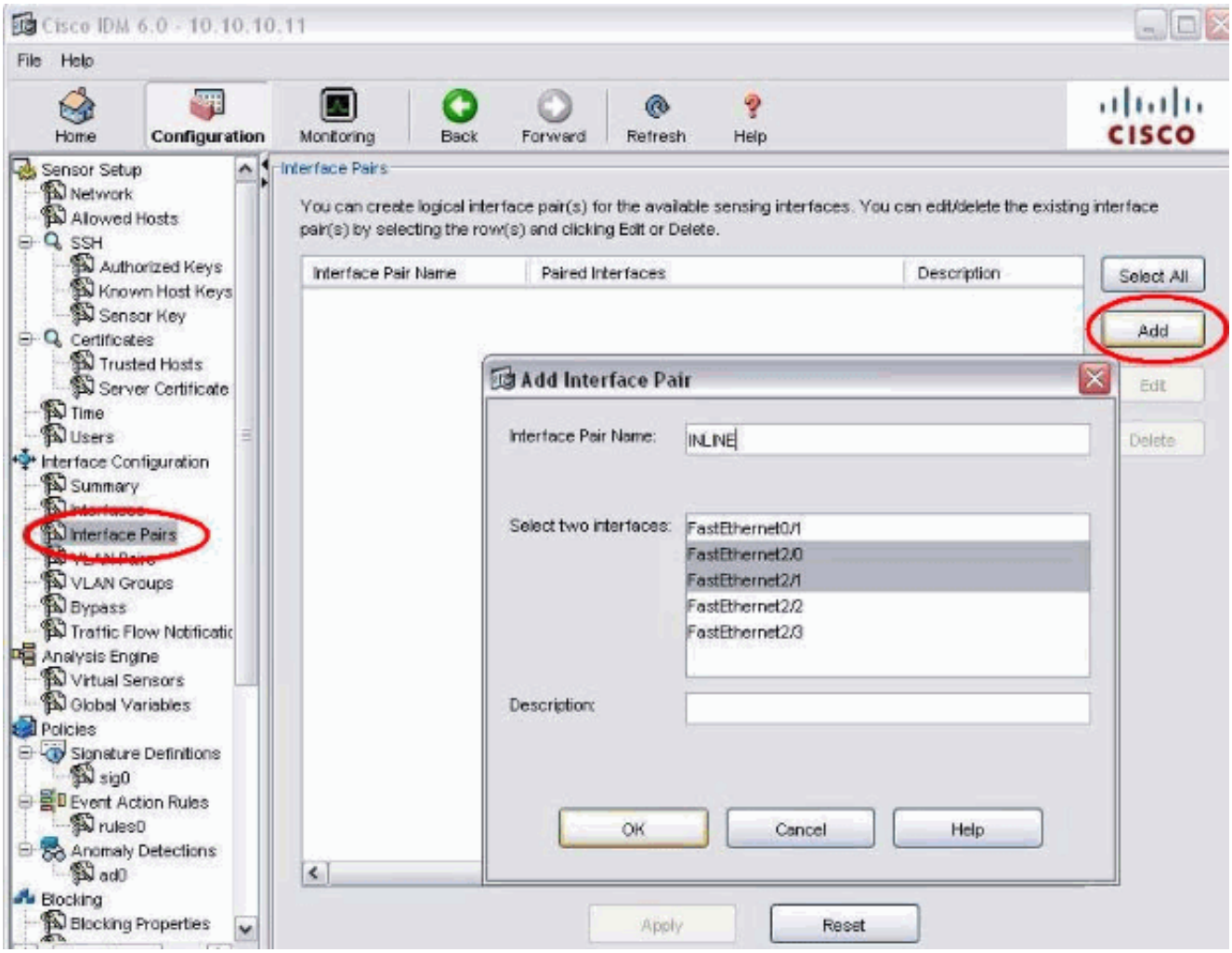
5. 前往**Configuration > Interface Configuration**，然後按一下**Summary**。此頁顯示感應介面的配置摘要
：



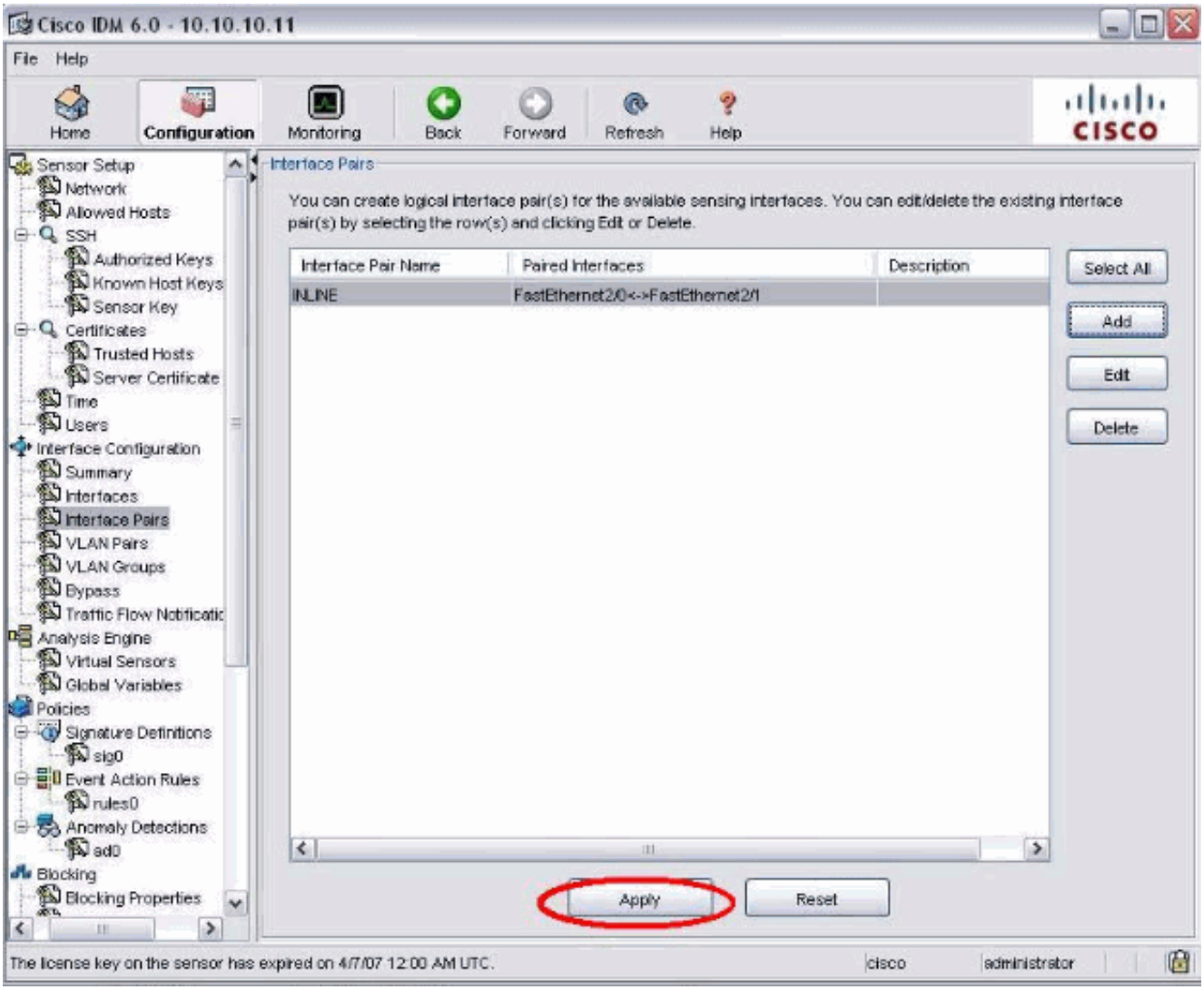
6. 轉至**Configuration > Interface Configuration > Interfaces**，然後選擇介面名稱。然後，按一下**Enable**以啟用感應介面。此外，配置雙工、速度和VLAN資訊。



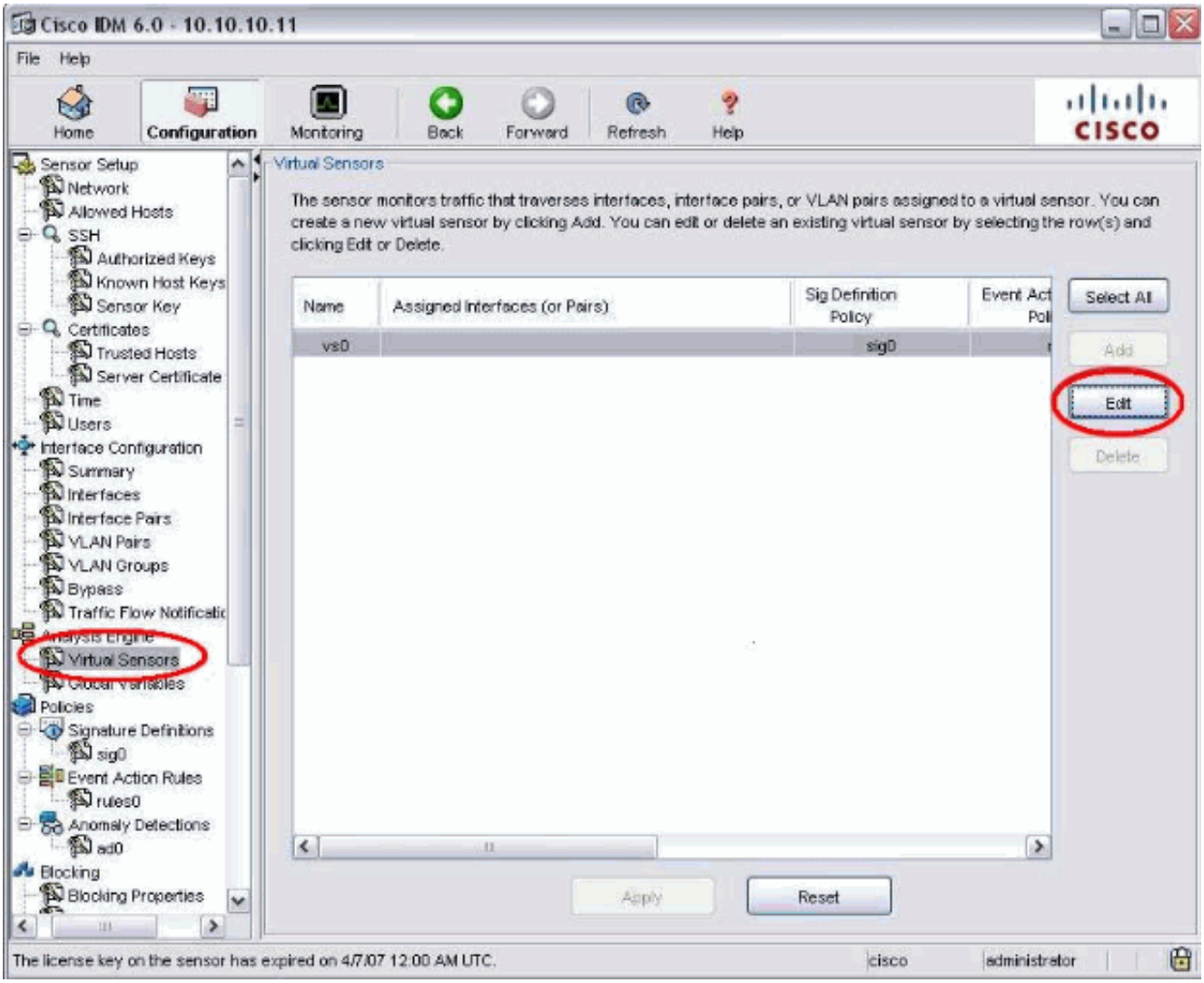
7. 前往**Configuration > Interface Configuration > Interface Pairs**，然後按一下**Add**以建立內嵌配對。



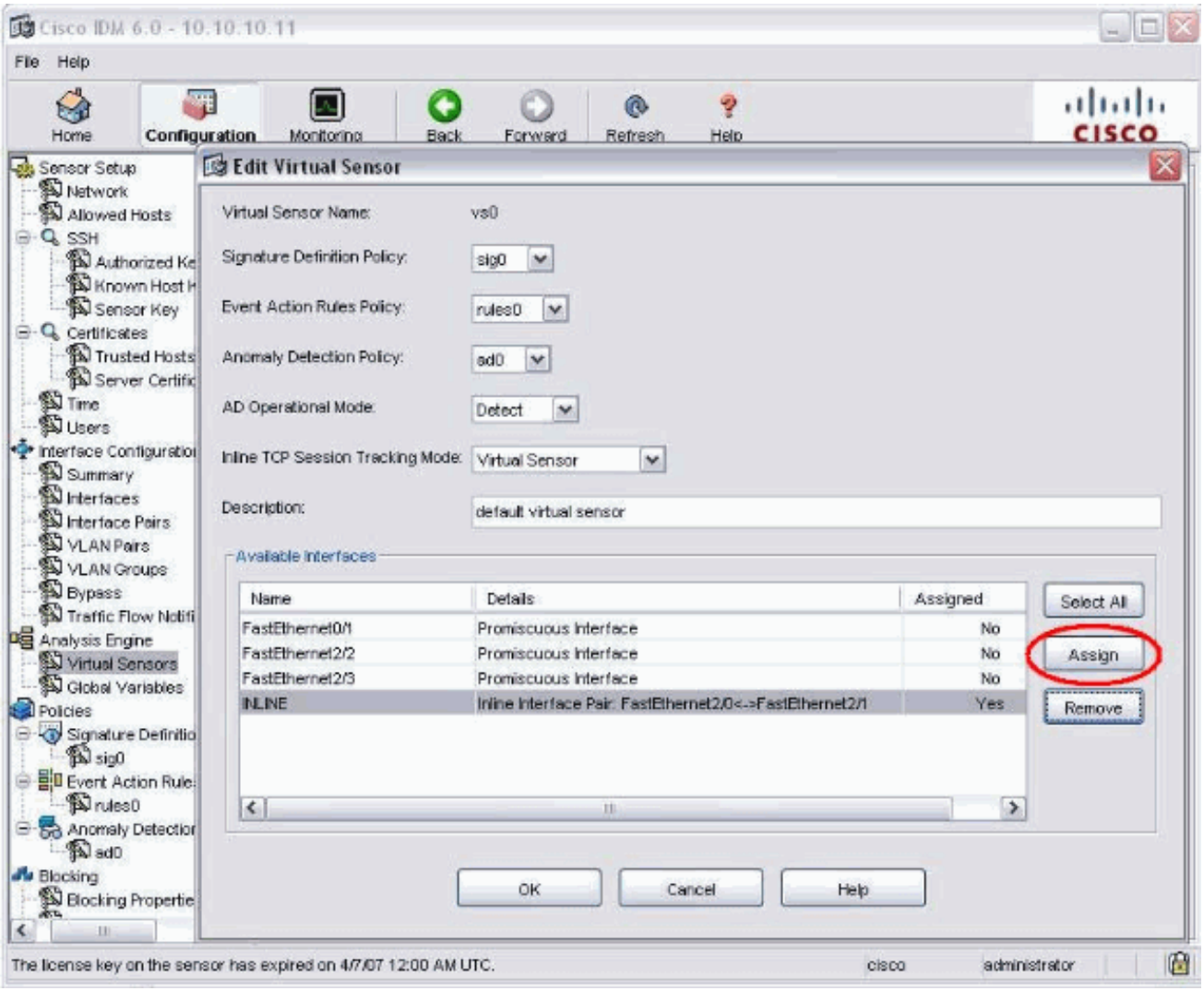
8. 檢視內嵌配對組態的摘要並加以套用。



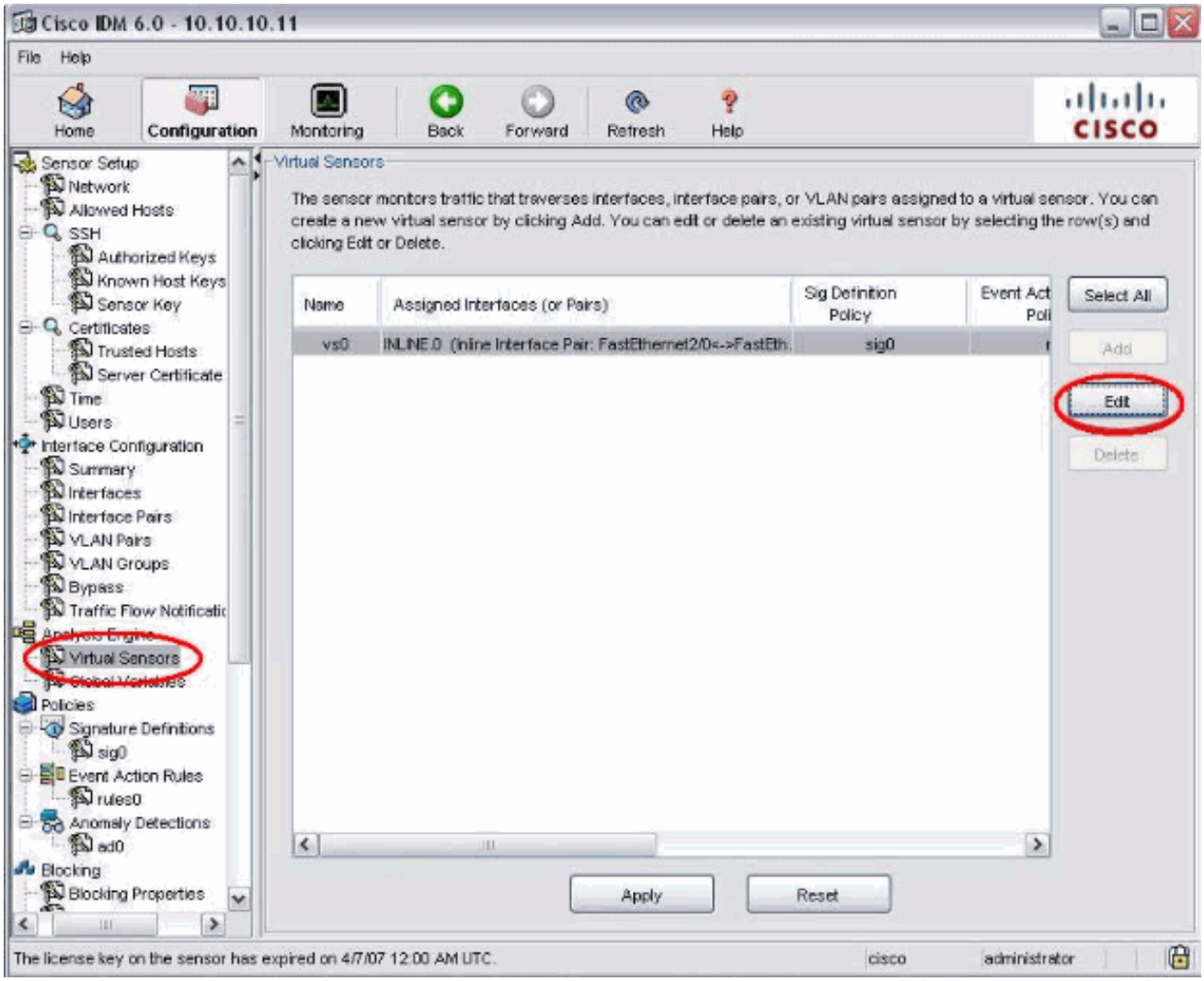
9. 轉至**Configuration > Analysis Engine > Virtual Sensor**，然後按一下**Edit**以建立新的虛擬感測器。



10. 將內嵌配對INLINE分配給虛擬感測器vs0。



11. 檢視分配的虛擬感測器資訊的摘要。



在內聯模式下為IDSM-2配置交換機

請參閱配置IDSM-2的在內嵌模式下設定Catalyst系列6500交換器以使用IDSM-2一節，將交換器設定為IDSM-2內嵌模式。

疑難排解

問題

如果IPS發生故障且已內聯配置，則介面是失效開放（流量繼續通過）還是關閉（流量被丟棄）。

解決方案

可以將IPS配置為失效開放狀態。因此，如果IPS失敗，它會繼續傳遞流量，但不會監控流量。

相關資訊

- Cisco ASA 5500系列調適型安全裝置
- 思科入侵防禦系統
- Cisco IPS 4200系列感應器

- 技術支援與文件 - Cisco Systems