IPS 5.X及更高版本/IDSM2:使用CLI和IDM的內聯VLAN對模式配置示例

目錄

簡介

在物理介面上成對關聯VLAN稱為內聯VLAN對模式。系統會分析其中一個成對VLAN上接收的封包，並將其轉送到該成對中的另一個VLAN。與Intrusion Prevention System(IPS)5.1相容的所有感測器均支援內聯VLAN對，但NM-CIDS、AIP-SSM-10和AIP-SSM-20除外。

內聯VLAN對模式是一種主動檢測模式，其中檢測介面用作802.1q中繼埠，並且感測器在中繼上的一對VLAN之間執行VLAN橋接。這表示連線到感應介面的交換機必須處於中繼模式。

感測器會檢查它在每個對中的每個VLAN上接收的流量，並可以在對中的其他VLAN上轉發資料包，或者在檢測到入侵嘗試時丟棄資料包。您可以配置IPS感測器，以同時橋接每個感應介面上的最多255個VLAN對。感測器將每個接收資料包的802.1q報頭中的VLAN ID欄位替換為感測器轉發資料包的輸出VLAN的ID。感測器會丟棄在未分配給內聯VLAN對的任何VLAN上收到的所有資料包。

注意：對於IPS-4260，內聯VLAN對不支援失效開放硬體旁路。如需詳細資訊，請參閱硬體略過組態限制。

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5.1及更高版本的思科入侵防禦系統感測器。

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。

VACL擷取組態

請參閱配置IDSM-2的配置VACL捕獲部分，將流量傳送到交換機上的IDSM。

內嵌VLAN配對模式組態

本節提供用於設定本文件中所述功能的資訊。

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

在服務介面子模式下使用**physical-interfaces interface_name**命令，以便使用CLI配置內聯VLAN對。介面名稱為FastEthernet或GigabitEthernet。

這些選項適用：

- **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。**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，管理狀態設定為已啟用且受到保護（您無法更改設定）。 admin-state對命令和控制介面沒有影響（且受到保護）。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** — 內嵌介面配對的說明。
- **duplex** — 介面的雙工設定。**auto** — 將介面設定為自動協商雙工。**full** — 將介面設定為全雙工。**half** — 將介面設定為半雙工。**註：**Duplex選項在所有模組上都受到保護。
- **no** — 移除條目或選取設定。
- **speed** — 介面的速度設定。**auto** — 將介面設定為自動協商速度。**10** — 將介面設定為10 MB（僅適用於TX介面）。**100** — 將介面設定為100 MB（僅適用於TX介面）。**1000** — 將介面設定為1 GB（用於Gigabit介面）**注意：**速度選項在所有模組上均受到保護。
- **subinterface-type** — 指定介面是子介面，並且定義了子介面的型別。**inline-vlan-pair** — 用於將子介面定義為內聯VLAN配對。**none** — 未定義子介面。
- **subinterface** — 將子介面定義為內聯VLAN對。**vlan1** — 內嵌VLAN對中的第一個VLAN。**vlan2** — 內嵌VLAN對中的第二個VLAN。

CLI組態

完成以下步驟，以便使用CLI在感測器上設定內嵌VLAN配對設定：

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聯介面（如果沒有配置任何內聯介面，則子介面型別應為「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. 移除任何使用此實體介面的內嵌介面：

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

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. 指定介面：

```
sensor(config-int)#physical-interfaces GigabitEthernet0/2
```

7. 啟用介面的管理狀態：

```
sensor(config-int-phy)#admin-state enabled
```

介面必須分配給虛擬感測器並啟用，才能監控通訊量。

8. 新增此介面的說明：

```
sensor(config-int-phy)#description INT1
```

9. 設定雙工設定：

```
sensor(config-int-phy)#duplex full
```

此選項在模組上不可用。

10. 配置速度：

```
sensor(config-int-phy)#speed 1000
```

此選項在模組上不可用。

11. 設定內嵌VLAN配對：

```
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. 新增內嵌VLAN對的說明：

```
sensor(config-int-phy-inl-sub)#description pairs vlans 52 and 53
```

13. 驗證內嵌VLAN配對設定：

```
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. 退出介面子模式：

```
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. 按**Enter**以應用更改，或輸入**no**以放棄更改。

16. 進入虛擬感測器配置模式：

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

17. 將介面新增到虛擬感測器：

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

18. 退出虛擬感測器子模式：

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

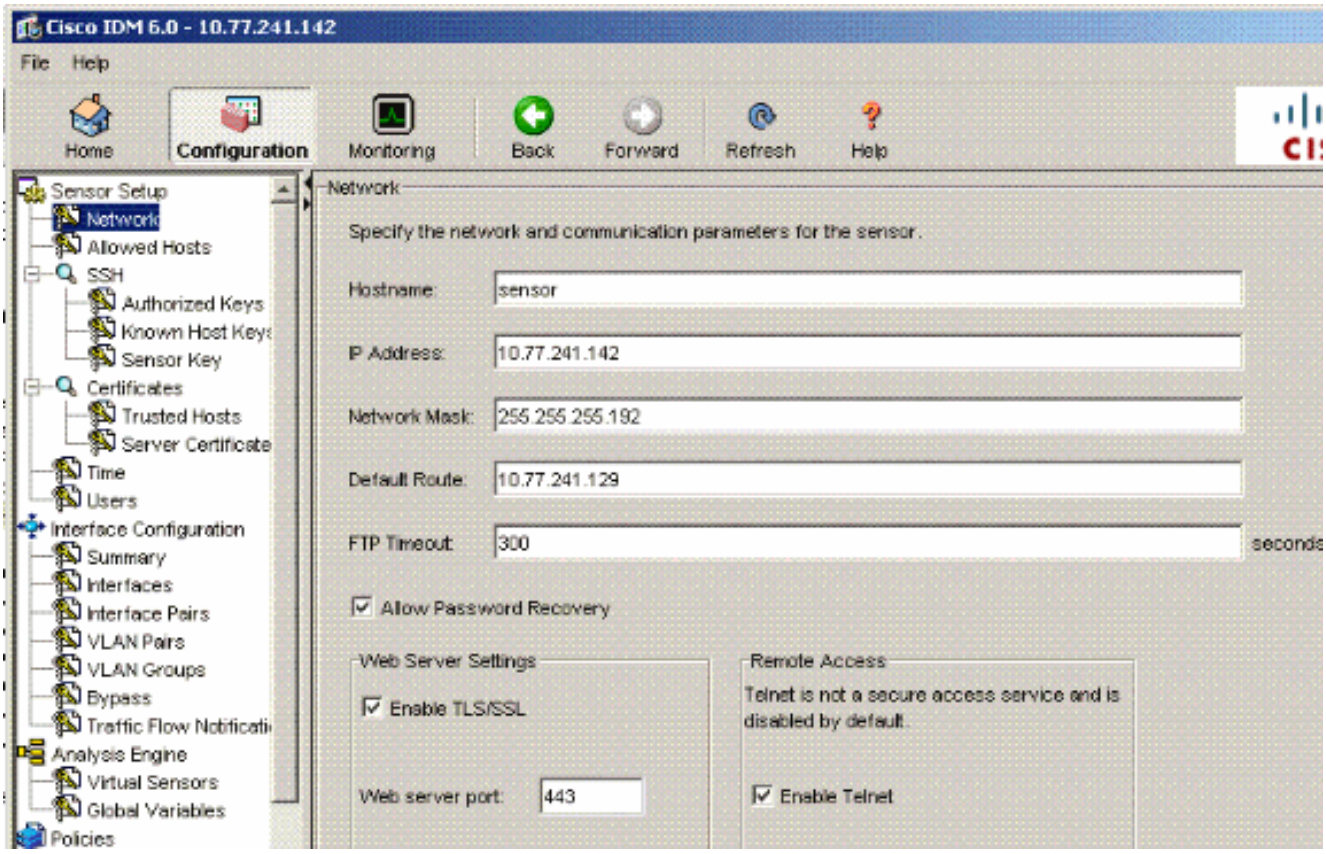
19. 按**Enter**以應用更改，或輸入**no**以放棄更改。

IDM配置

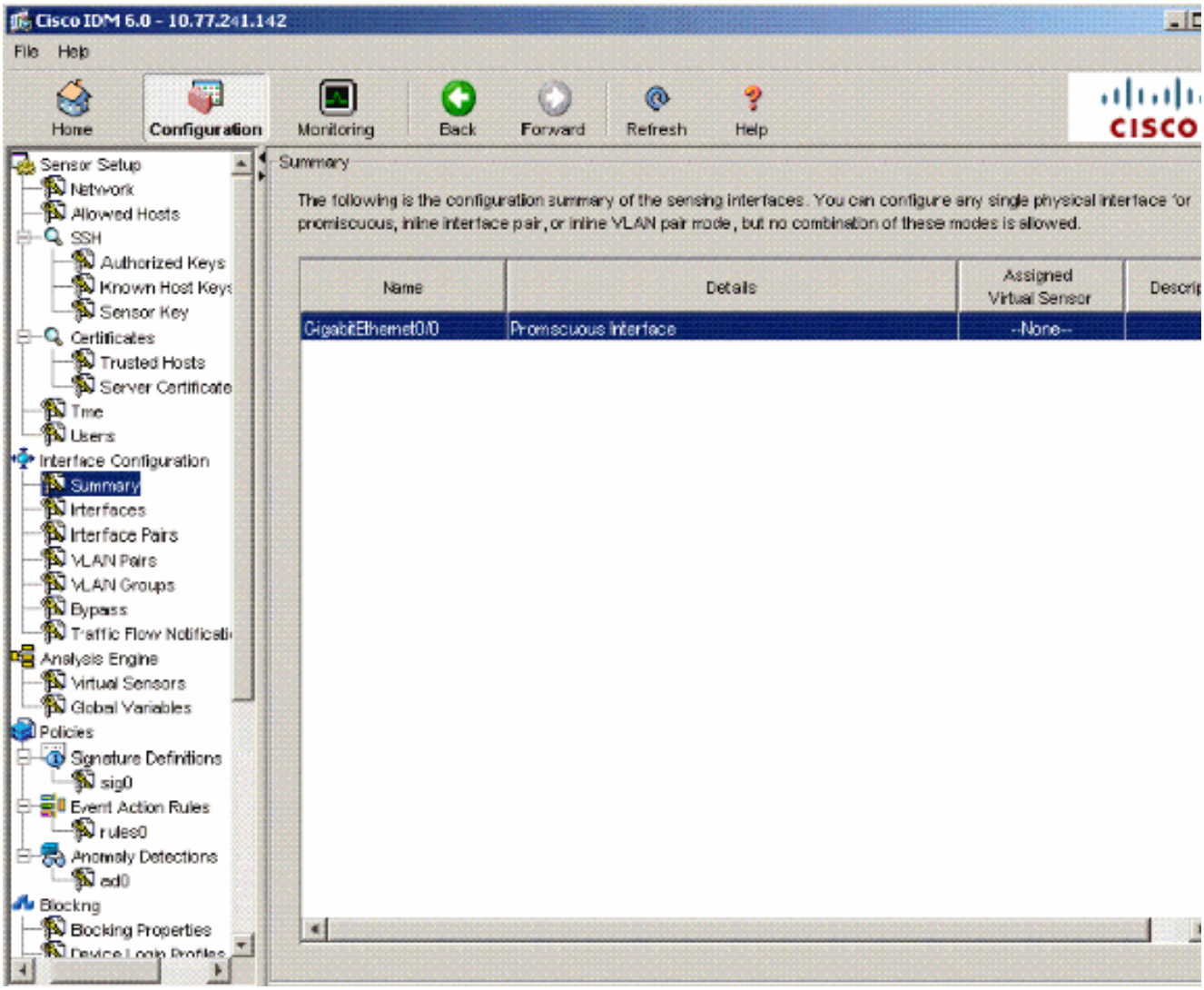
完成以下步驟，使用IDS裝置管理器(IDM)配置感測器上的內聯VLAN對設定：

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 and 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、版本和型號等。

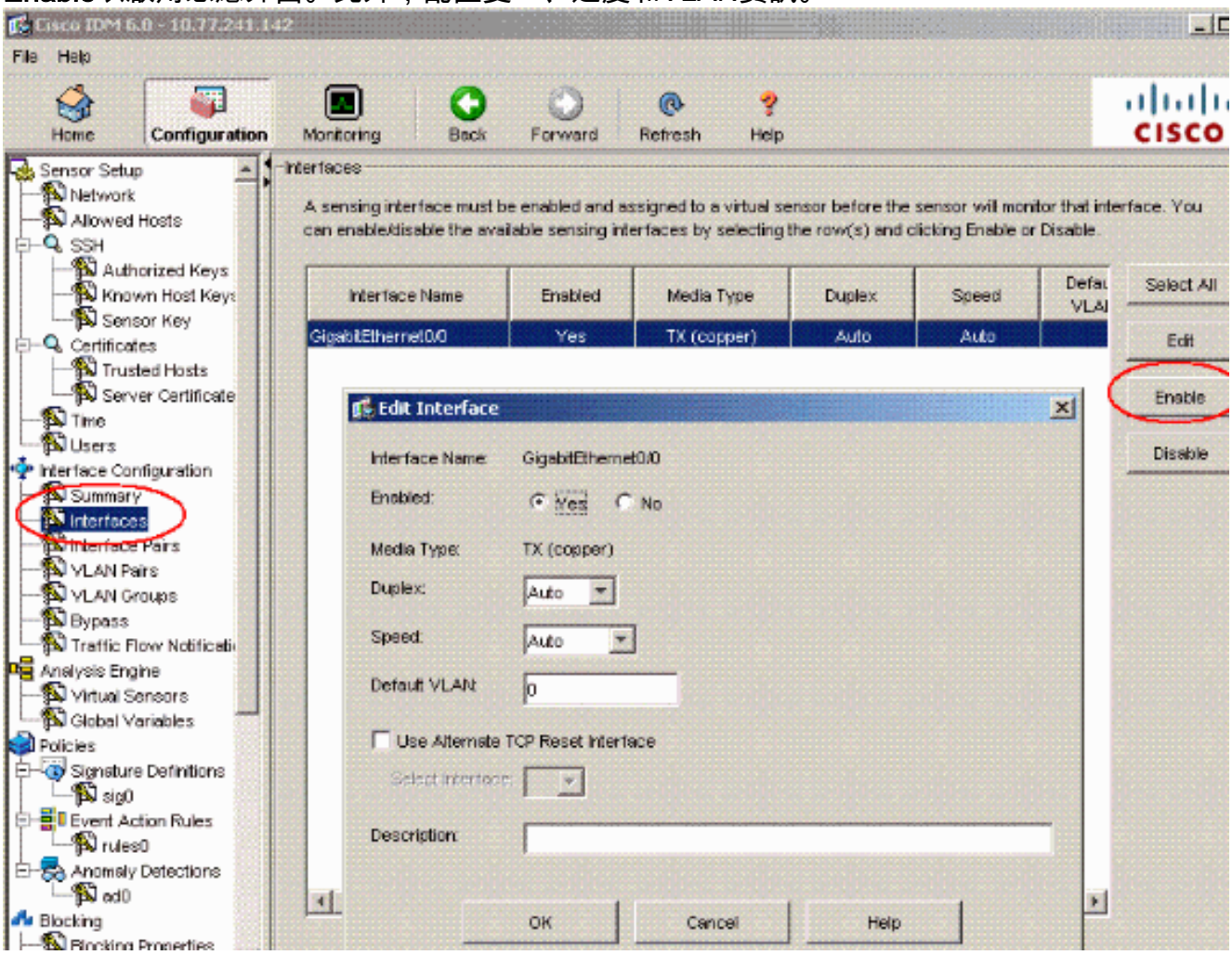
4. 轉到**Configuration > Sensor Setup**，然後按一下**Network**。您可以在此處指定主機名、IP地址和預設路由。



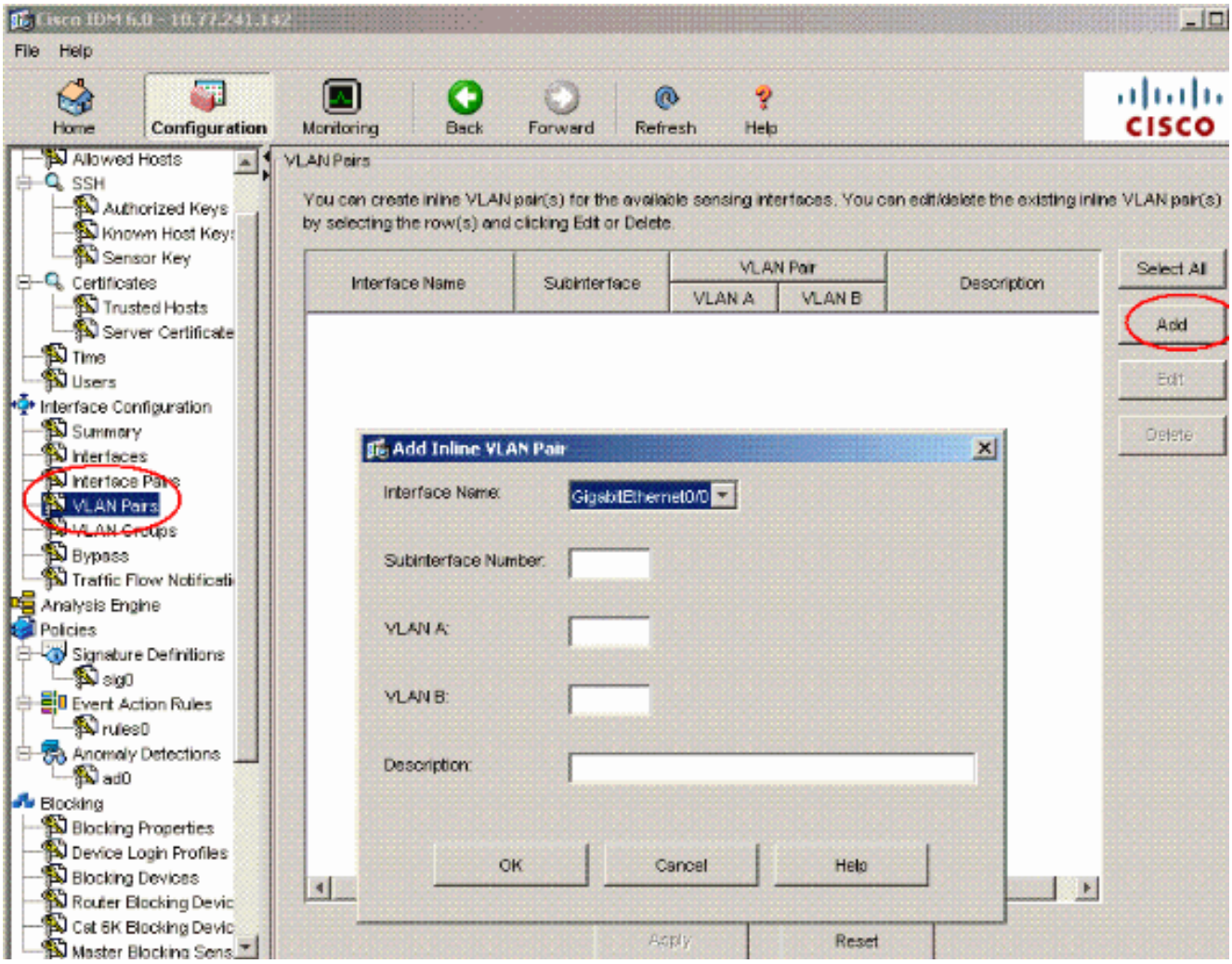
5. 前往**Configuration > Interface Configuration**，然後按一下**Summary**。此頁顯示感應介面的配置摘要。



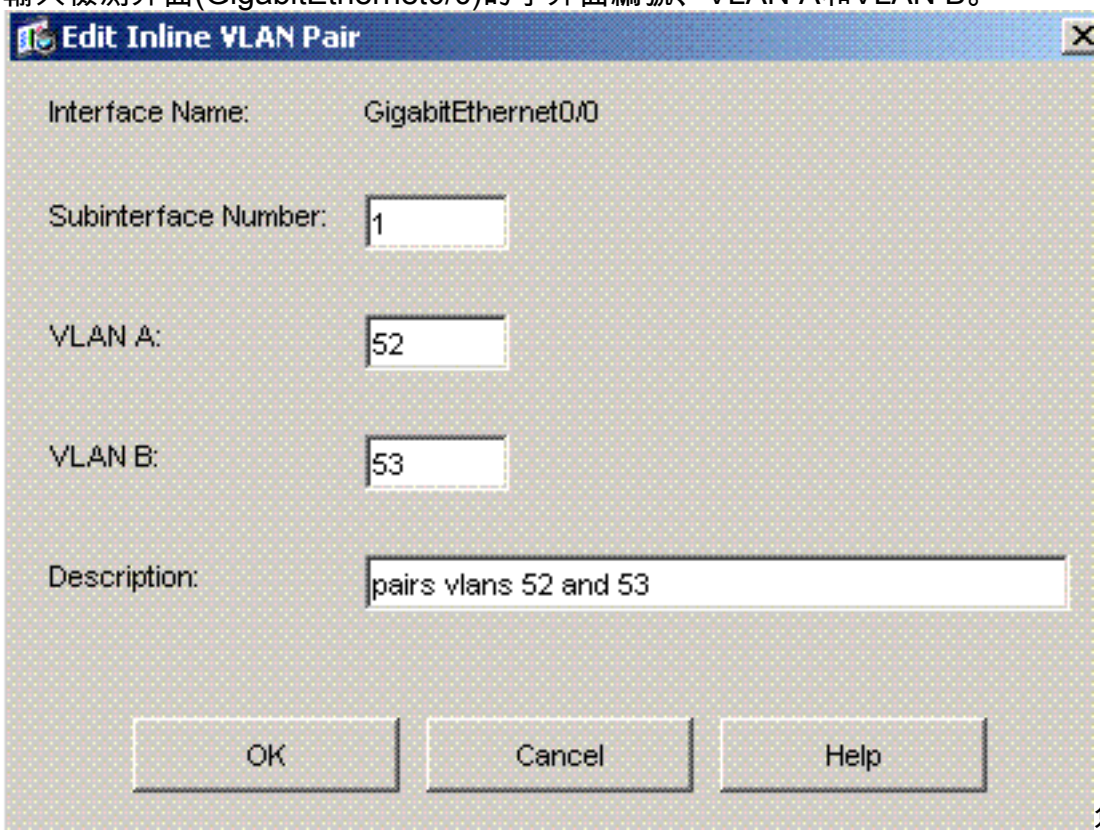
6. 轉至**Configuration > Interface Configuration > Interfaces**，然後選擇介面名稱。然後，按一下**Enable**以啟用感應介面。此外，配置雙工、速度和VLAN資訊。



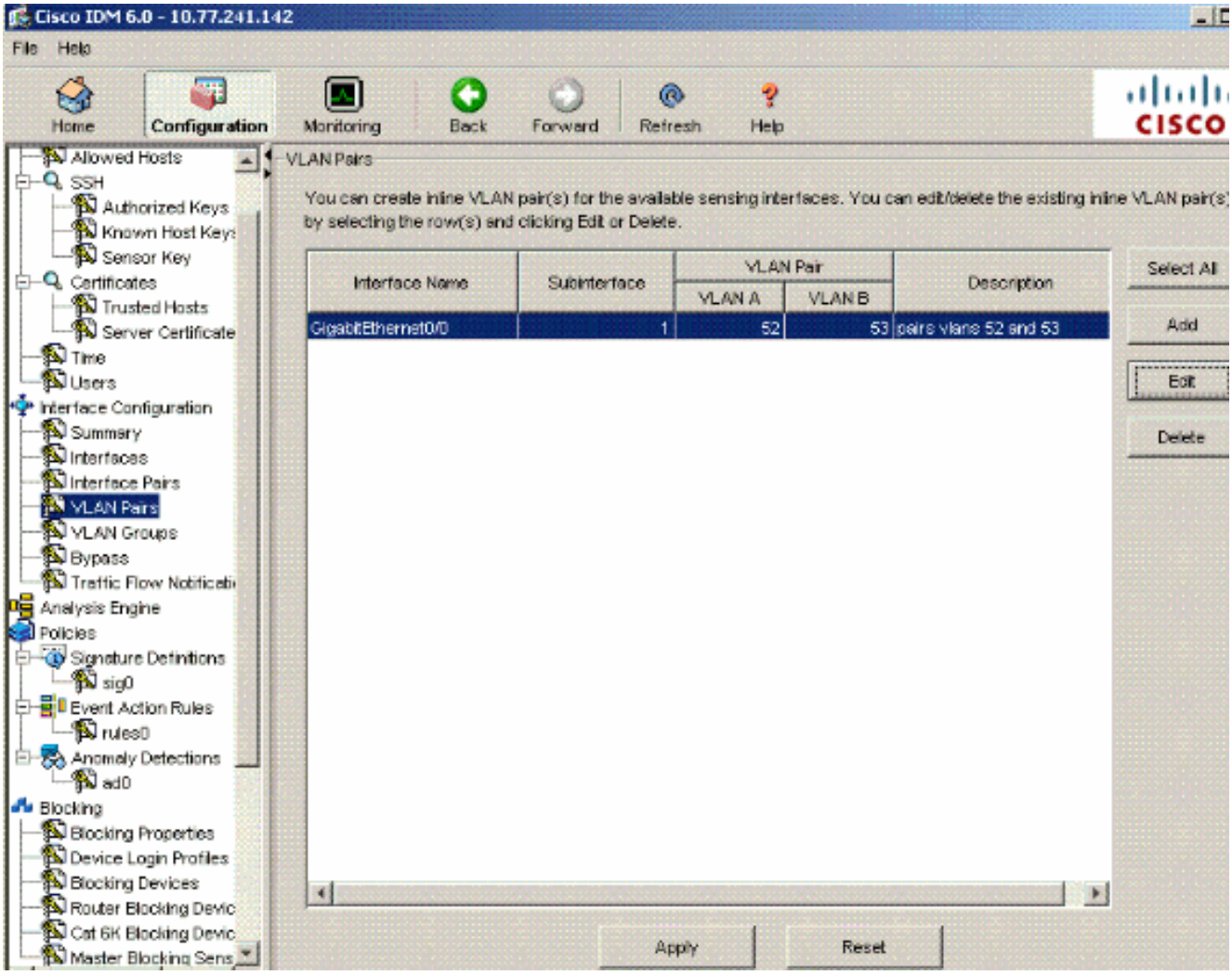
7. 前往**Configuration > Interface Configuration > VLAN Pairs**，然後按一下**Add**以建立內嵌VLAN對。



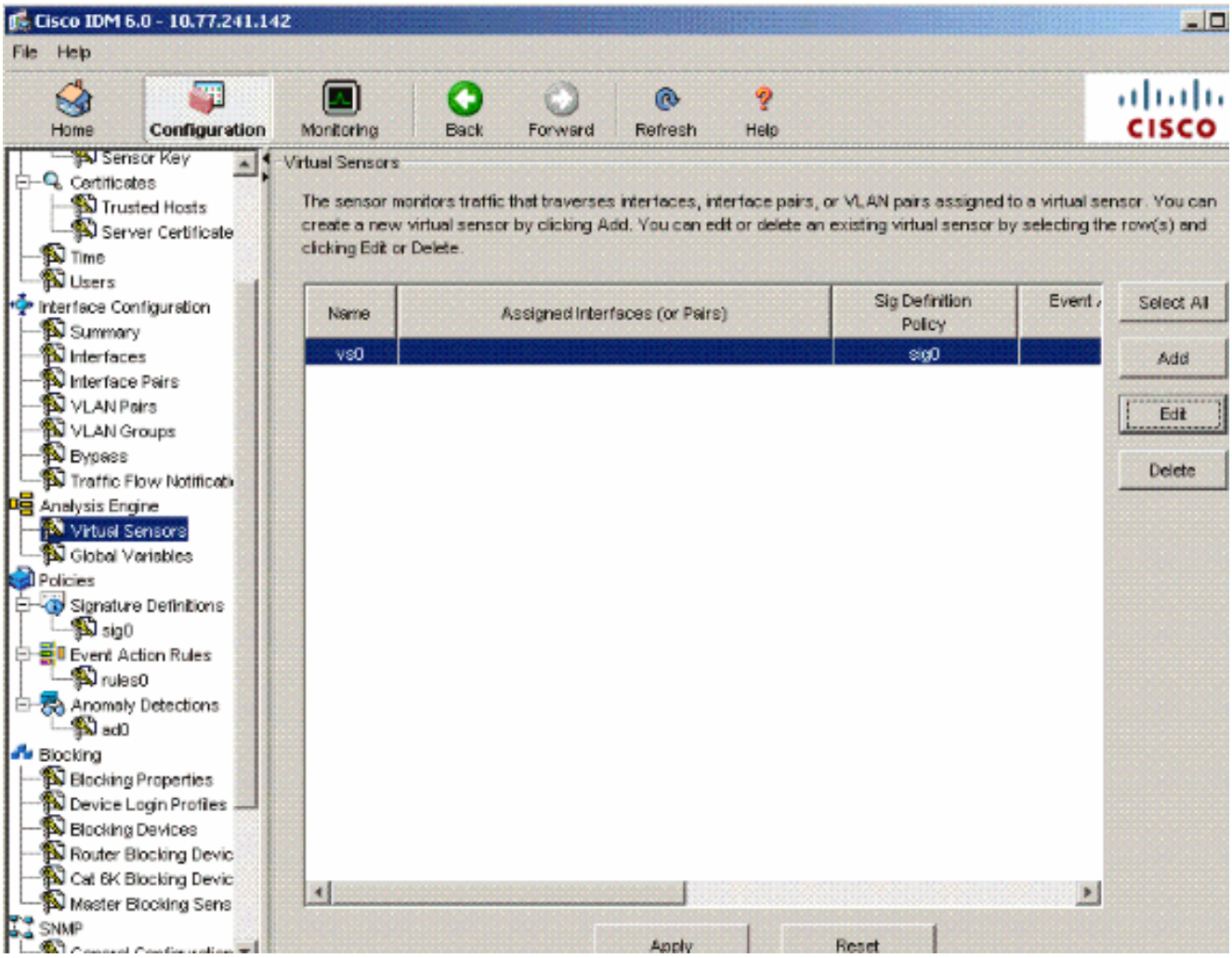
8. 輸入檢測介面(GigabitEthernet0/0)的子介面編號、VLAN A和VLAN B。



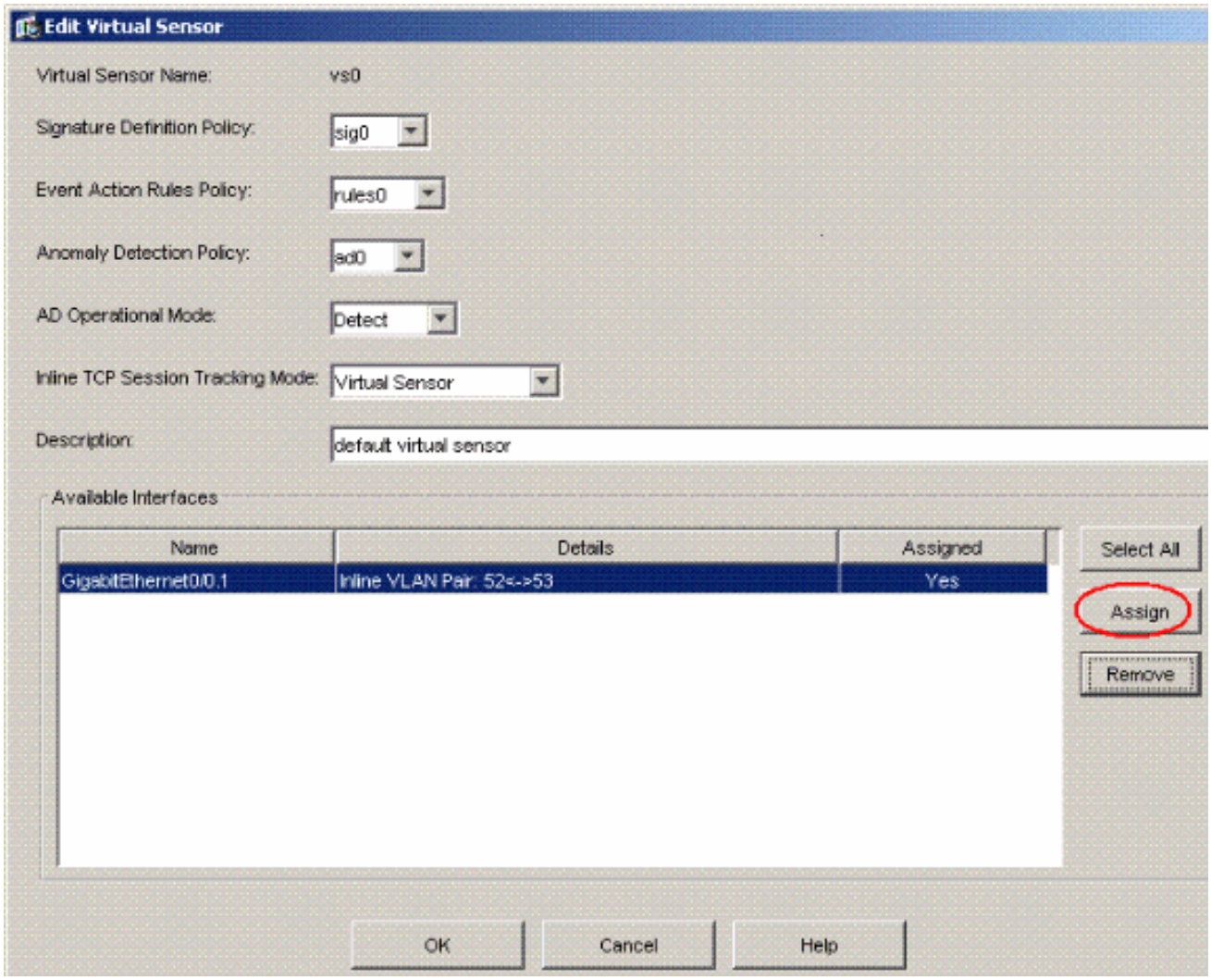
您可以檢視內嵌VLAN配對組態的摘要。



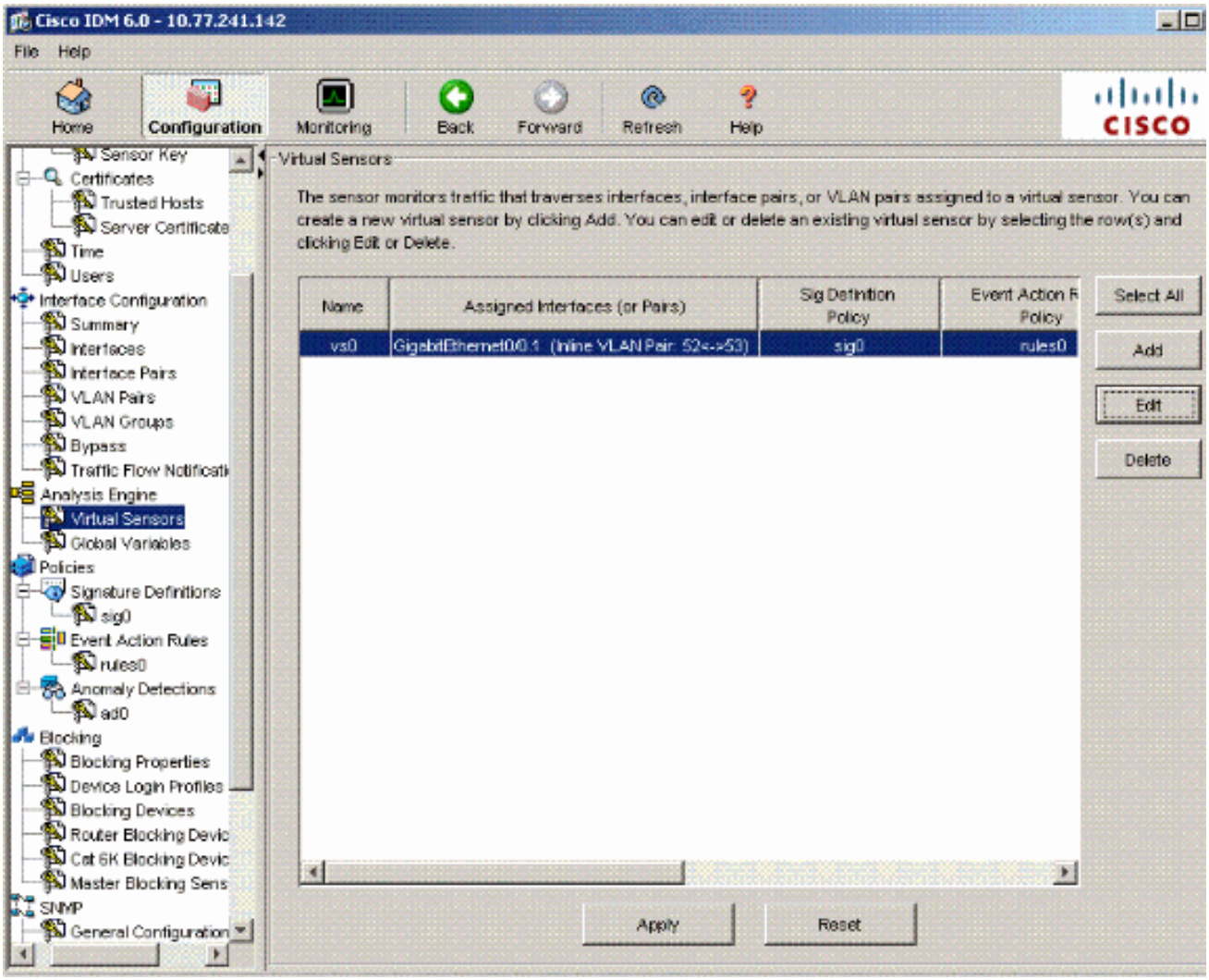
9. 轉至**Configuration > Analysis Engine > Virtual Sensor**，然後按一下**Edit**以建立新的虛擬感測器。



10. 將內聯VLAN對52和53分配給虛擬感測器vs0。



檢視分配的虛擬感測器資訊的摘要。



疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

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