IPS 5.X e versioni successive/IDSM2: Modalità inline per coppie VLAN con esempio di configurazione CLI e IDM

Sommario

Introduzione

L'associazione delle VLAN a coppie su un'interfaccia fisica è nota come modalità di coppia di VLAN in linea. I pacchetti ricevuti su una delle VLAN accoppiate vengono analizzati e inoltrati all'altra VLAN della coppia. Le coppie di VLAN in linea sono supportate su tutti i sensori compatibili con Intrusion Prevention System (IPS) 5.1, ad eccezione di NM-CIDS, AIP-SSM-10 e AIP-SSM-20.

La modalità inline di coppia di VLAN è una modalità di rilevamento attivo in cui un'interfaccia di rilevamento opera come porta trunk 802.1q e il sensore esegue il bridging VLAN tra coppie di VLAN sul trunk. Ciò significa che lo switch collegato all'interfaccia di rilevamento deve essere in modalità trunk.

Il sensore controlla il traffico che riceve su ciascuna VLAN in ciascuna coppia e può inoltrare i pacchetti sull'altra VLAN nella coppia o scartare il pacchetto se viene rilevato un tentativo di intrusione. È possibile configurare un sensore IPS in modo da collegare simultaneamente fino a 255 coppie di VLAN su ciascuna interfaccia di rilevamento. Il sensore sostituisce il campo VLAN ID nell'intestazione 802.1q di ciascun pacchetto ricevuto con l'ID della VLAN in uscita su cui il sensore inoltra il pacchetto. Il sensore scarta tutti i pacchetti ricevuti sulle VLAN che non sono assegnate a coppie di VLAN in linea.

Nota: per IPS-4260, il bypass hardware fail-open non è supportato sulle coppie di VLAN in linea. Per ulteriori informazioni, fare riferimento a Limitazioni della configurazione di bypass hardware.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sul sensore Cisco Intrusion Prevention System che usa la versione 5.1 e successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Prodotti correlati

Le informazioni discusse in questo documento si applicano anche al modulo Servizi del sistema di rilevamento delle intrusioni (IDSM-2).

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Configurazione acquisizione VACL

Per inviare il traffico a IDSM sullo switch, consultare la sezione Configurazione dell'acquisizione VACL in Configurazione di IDSM-2.

Configurazione in linea della modalità coppia VLAN

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Usare il comando **physical-interfaces interface_name** nella modalità secondaria dell'interfaccia del servizio per configurare le coppie di VLAN inline con la CLI. Il nome dell'interfaccia è FastEthernet o Gigabit Ethernet.

Si applicano le seguenti opzioni:

- **stato-amministratore {enabled | disabled}**: lo stato del collegamento amministrativo dell'interfaccia, sia essa abilitata o disabilitata.**Nota:** su tutte le interfacce di rilevamento backplane su tutti i moduli (IDSM-2 NM-CIDS e AIP-SSM), admin-state è impostato su

enabled ed è protetto (non è possibile modificare l'impostazione). Lo stato admin non ha alcun effetto (ed è protetto) sull'interfaccia di comando e controllo. Influisce solo sulle interfacce di rilevamento. Non è necessario abilitare l'interfaccia di comando e controllo perché non può essere monitorata.

- **default** - Ripristina l'impostazione di default del sistema.
- **description**: descrizione della coppia di interfacce inline.
- **duplex** - Impostazione del duplex dell'interfaccia.**auto**: imposta l'interfaccia per la negoziazione automatica del duplex.**full** - Imposta l'interfaccia su full duplex.**half** - Imposta l'interfaccia su half-duplex.**Nota:** l'opzione duplex è protetta su tutti i moduli.
- **no** - Rimuove una voce o un'impostazione di selezione.
- **speed** - Impostazione della velocità dell'interfaccia.**auto** - Imposta la velocità di negoziazione automatica per l'interfaccia.**10** - Imposta l'interfaccia su 10 MB (solo per interfacce TX).**100** - Imposta l'interfaccia su 100 MB (solo per interfacce TX).**1000** - Imposta l'interfaccia su 1 GB (per interfacce Gigabit)**Nota:** l'opzione speed è protetta su tutti i moduli.
- **tipo sottointerfaccia (subinterface-type**) - Specifica che l'interfaccia è una sottointerfaccia e il tipo di sottointerfaccia definito.**inline-vlan-pair**: consente di definire la sottointerfaccia come coppia di VLAN in linea.**none** - Nessuna sottointerfaccia definita.
- **subinterface** - Definisce la sottointerfaccia come coppia di VLAN in linea.**vlan1**: la prima VLAN nella coppia di VLAN in linea.**vlan2**: la seconda VLAN nella coppia di VLAN in linea.

Configurazione CLI

Completare questa procedura per configurare le impostazioni della coppia di VLAN in linea sul sensore con CLI:

1. Accedere alla CLI utilizzando un account con privilegi di amministratore.
2. Accedere alla modalità secondaria dell'interfaccia:
```
sensor#configure terminal
sensor(config)#service interface
sensor(config-int)#
```
3. Verificare se esistono interfacce inline (il tipo di sottointerfaccia deve essere "none" se non sono state configurate interfacce inline):
```
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. Rimuovere le interfacce inline che utilizzano questa interfaccia fisica:
   ```
   sensor(config-int)#no inline-interfaces interface_name
   ```

5. Visualizzare l'elenco delle interfacce disponibili:
   ```
   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. Specificare un'interfaccia:
   ```
   sensor(config-int)#physical-interfaces GigabitEthernet0/2
   ```

7. Abilitare lo stato admin-state dell'interfaccia:
   ```
   sensor(config-int-phy)#admin-state enabled
   ```

   Per monitorare il traffico, l'interfaccia deve essere assegnata al sensore virtuale e abilitata.

8. Aggiungere una descrizione dell'interfaccia:
   ```
   sensor(config-int-phy)#description INT1
   ```

9. Configurare le impostazioni duplex:
   ```
   sensor(config-int-phy)#duplex full
   ```

Questa opzione non è disponibile sui moduli.

10. Configurare la velocità:
```
sensor(config-int-phy)#speed 1000
```
Questa opzione non è disponibile sui moduli.

11. Configurare la coppia di VLAN in linea:
```
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. Aggiungere una descrizione per la coppia di VLAN inline:
```
sensor(config-int-phy-inl-sub)#description pairs vlans 52 and 53
```

13. Verificare le impostazioni della coppia di VLAN in linea:
```
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. Uscire dalla modalità secondaria dell'interfaccia:
```
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. Premere **Invio** per applicare le modifiche o immettere **no** per ignorarle.
16. Accedere alla modalità di configurazione del sensore virtuale:
```
sensor(config)#service analysis-engine
        sensor(config-ana)#virtual-sensor vs0
```

17. Aggiungere l'interfaccia al sensore virtuale:
```
sensor(config-ana-vir)#physical-interface GigabitEthernet0/2
subinterface-number 1
```

18. Uscire dalla modalità secondaria del sensore virtuale:
```
sensor(config-ana-vir)#exit
        sensor(config-ana)#exit
        Apply Changes:?[yes]:
```

19. Premere **Invio** per applicare le modifiche o immettere **no** per ignorarle.

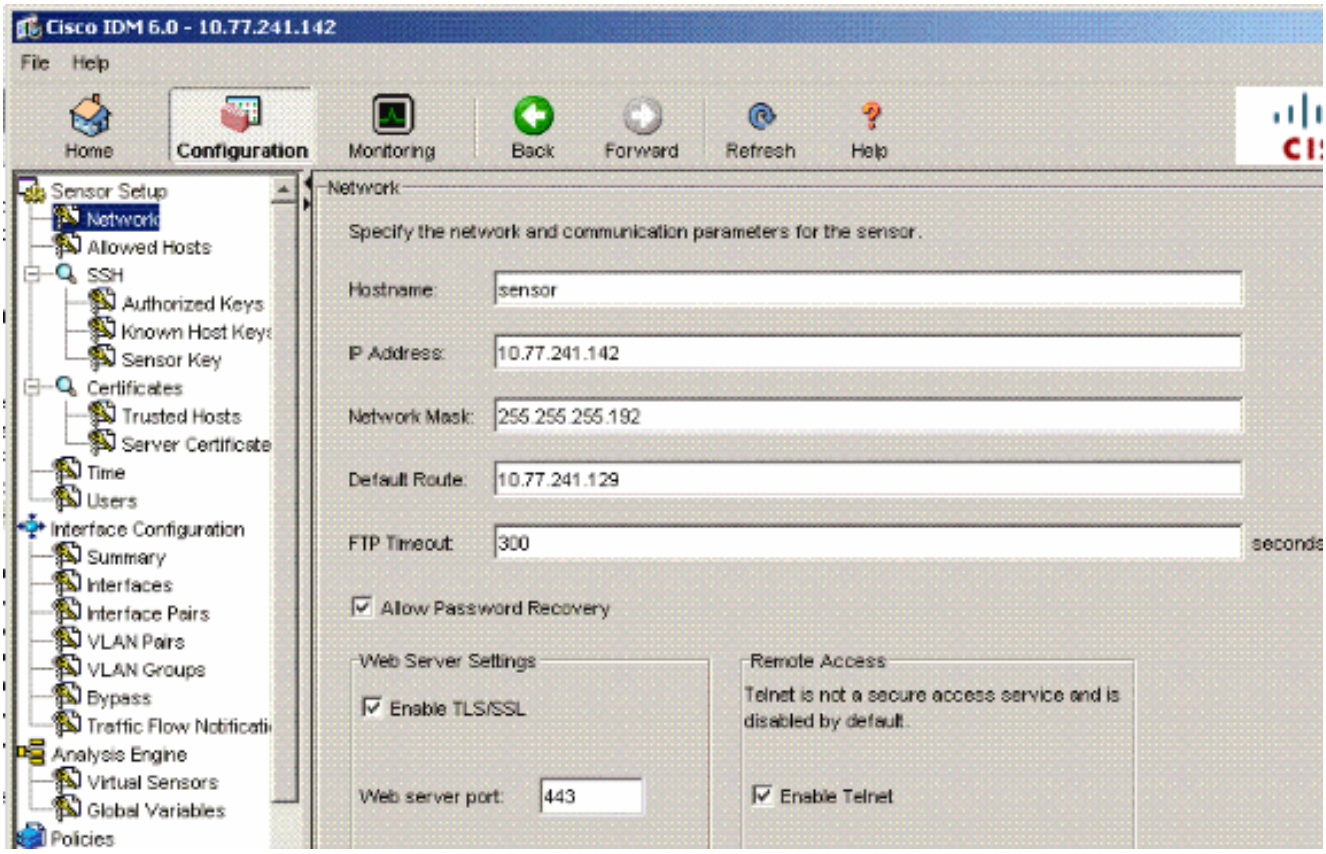
Configurazione IDM

Completare questa procedura per configurare le impostazioni della coppia di VLAN in linea sul sensore con IDS Device Manager (IDM):

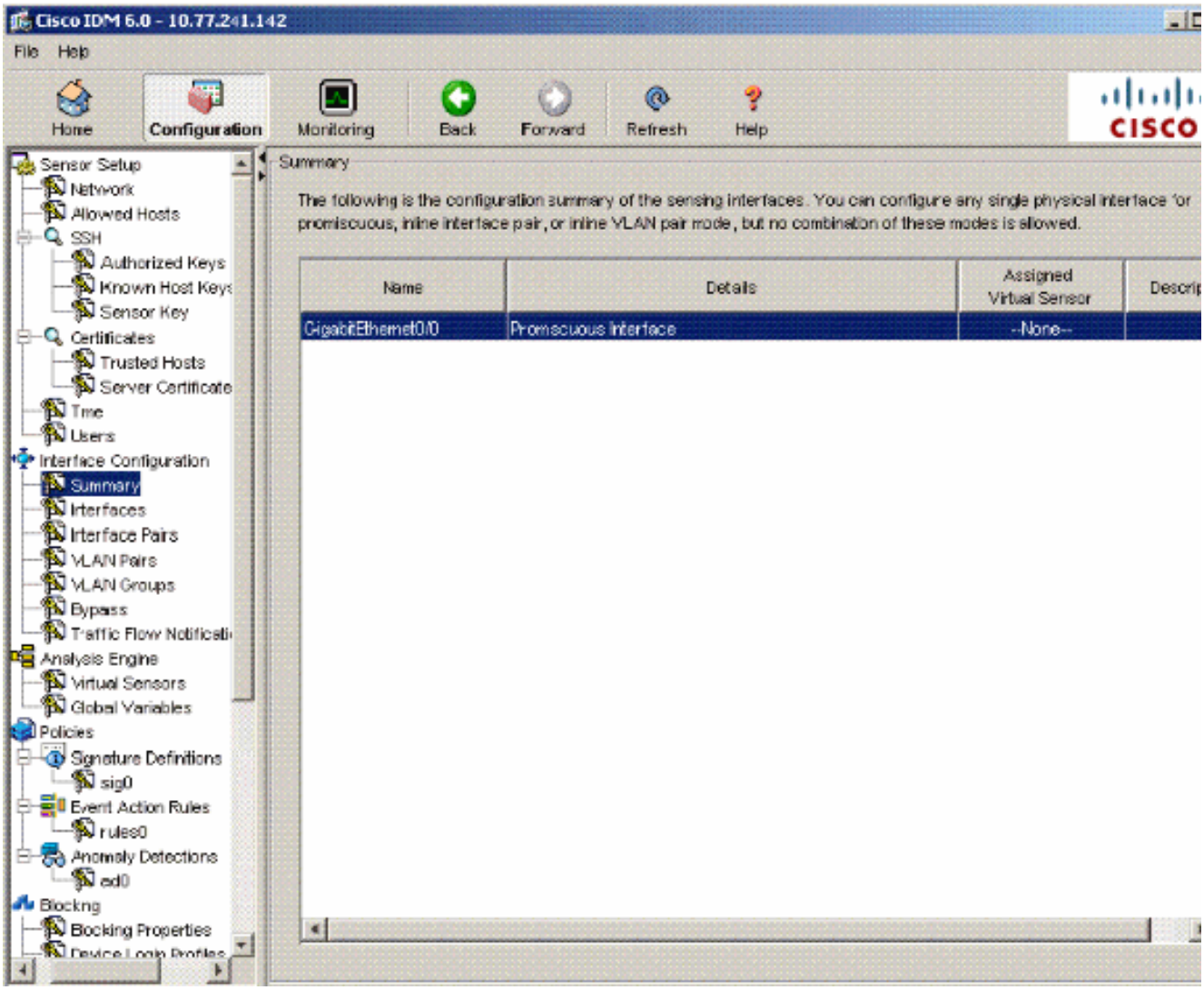
1. Aprire il browser e immettere **https://<Management_IP_Address_of_IPS>** per accedere a IDM su IPS.
2. Fate clic su **Download IDM Launcher e Avvia IDM** per scaricare il programma di installazione dell'applicazione.

3. Andare alla home page per visualizzare le informazioni sul dispositivo, quali il nome host, l'indirizzo IP, la versione e il modello,
ecc.

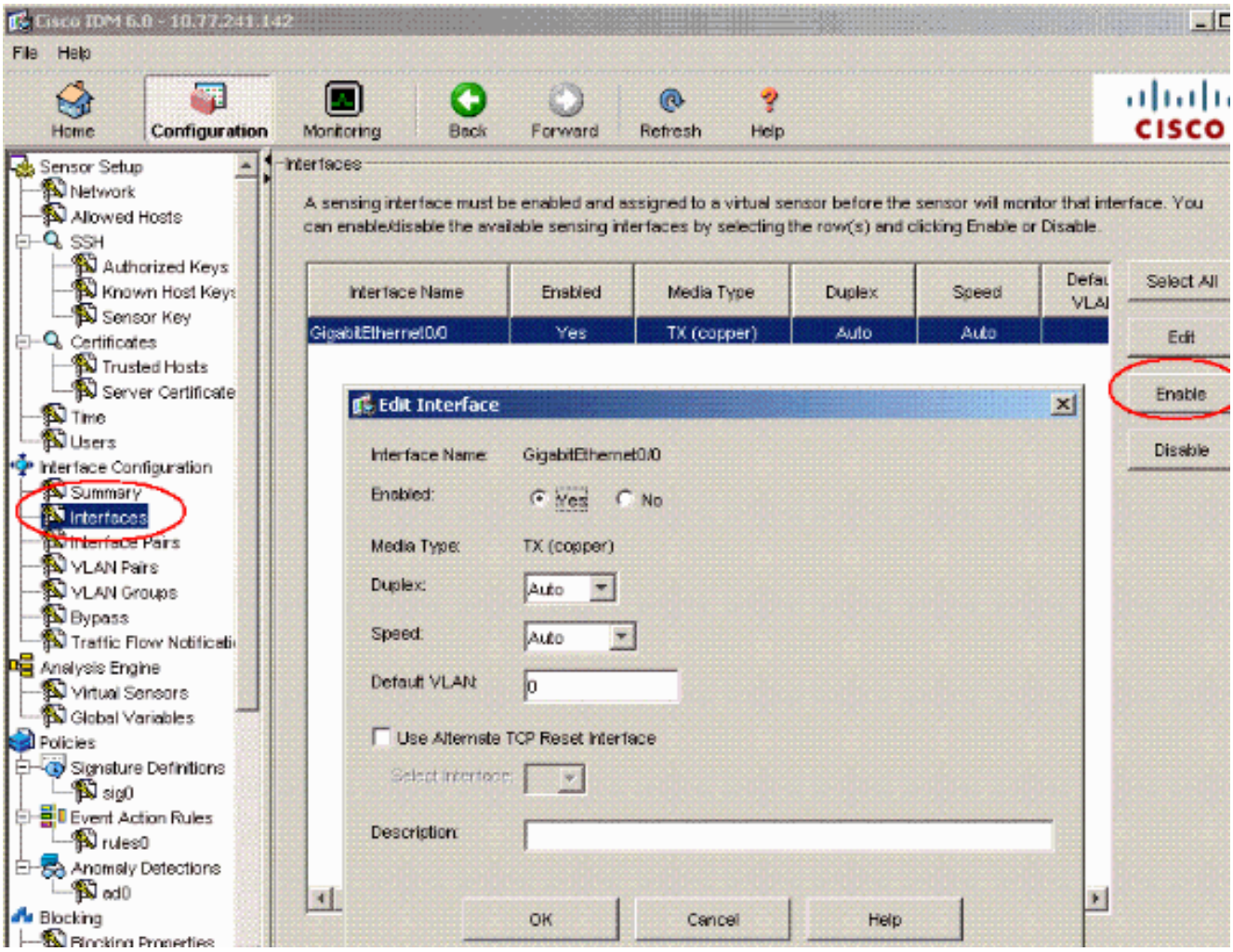
4. Selezionare **Configurazione > Impostazione sensore** e fare clic su **Rete**. Qui è possibile specificare il nome host, l'indirizzo IP e il percorso
predefinito.



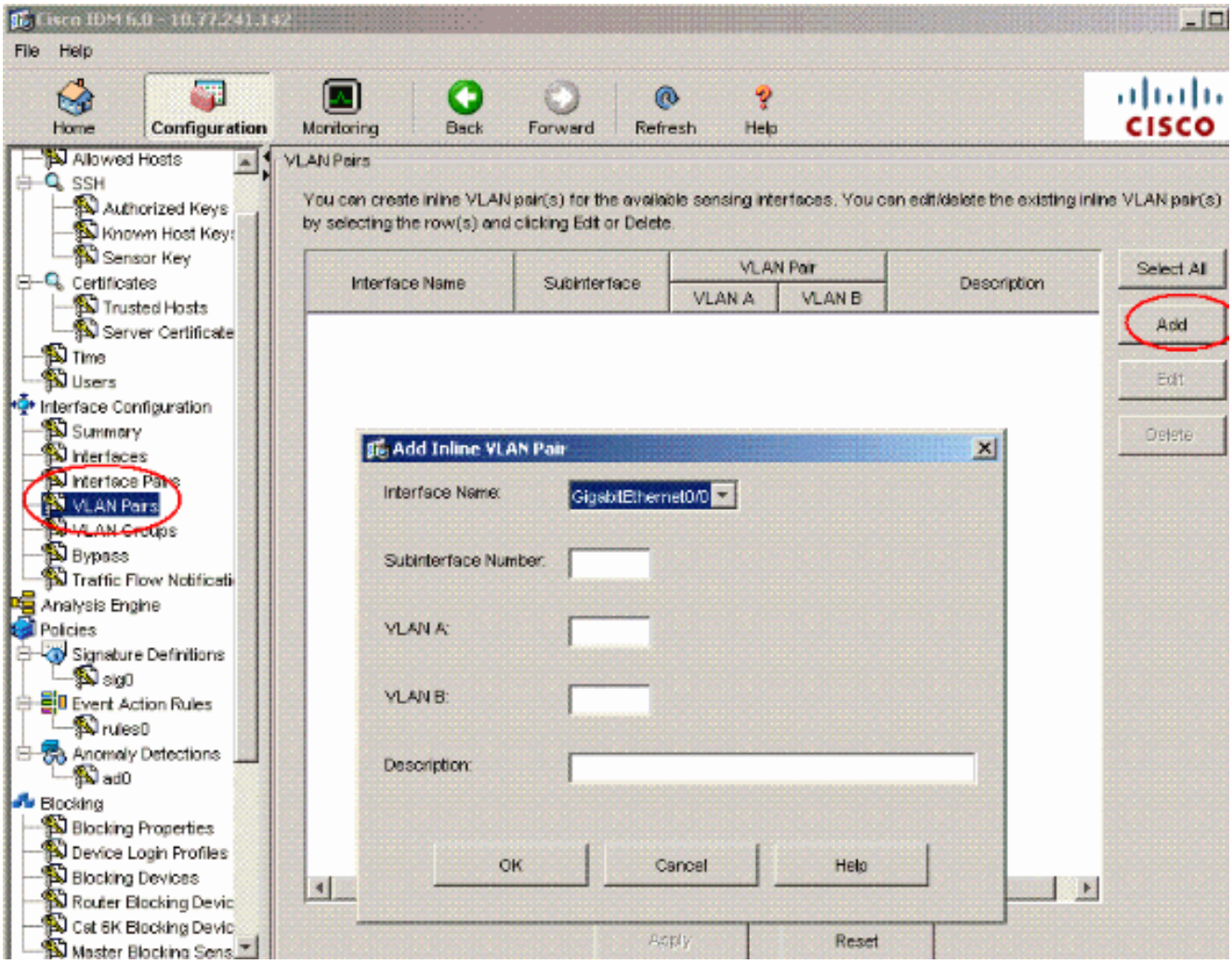
5. Selezionare **Configurazione > Configurazione interfaccia**, quindi fare clic su **Riepilogo**.Questa pagina mostra il riepilogo della configurazione dell'interfaccia di rilevamento.



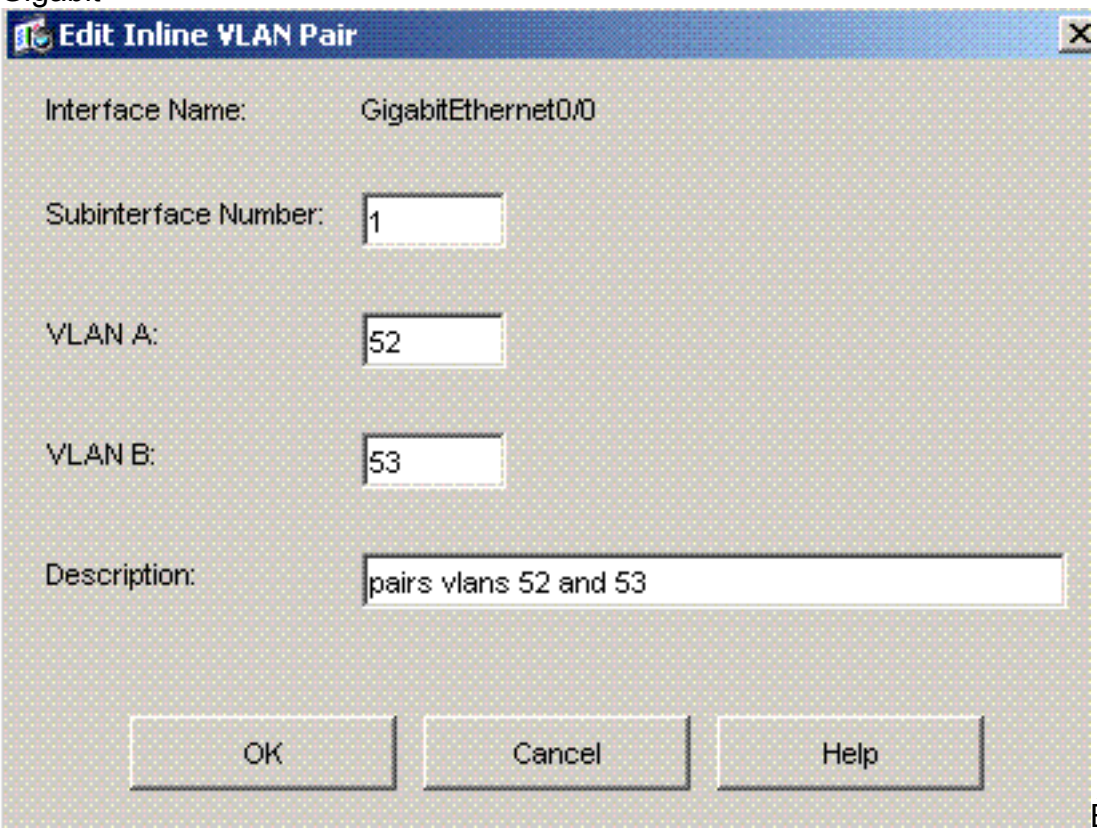
6. Selezionare **Configurazione > Configurazione interfaccia > Interfacce**, quindi selezionare il nome dell'interfaccia. Per abilitare l'interfaccia di rilevamento, fare clic su **Abilita**. Inoltre, configurare le informazioni duplex, velocità e
VLAN.



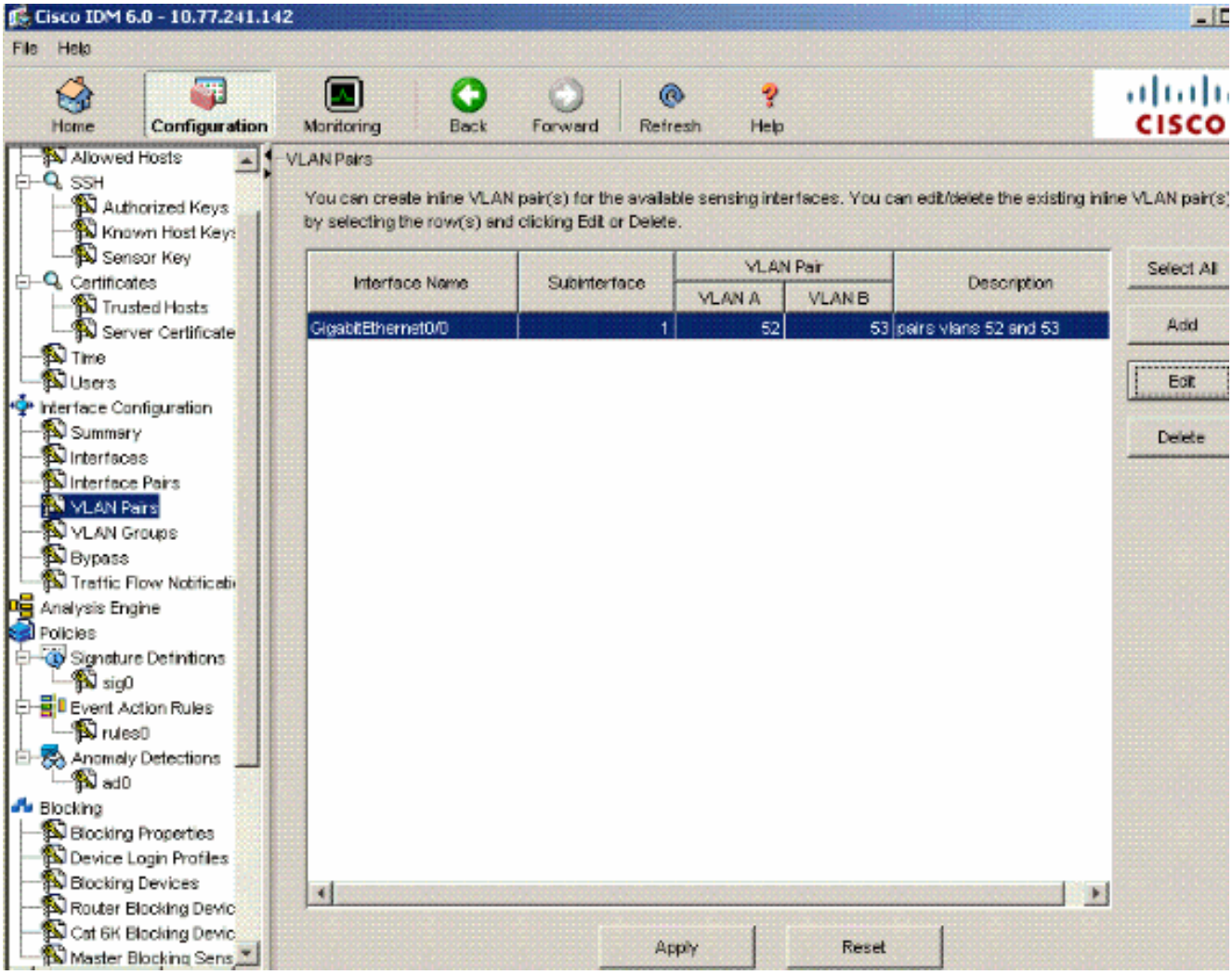
7. Per creare le coppie di VLAN in linea, selezionare **Configuration > Interface Configuration > VLAN Pairs** e fare clic su **Add**
(Aggiungi).



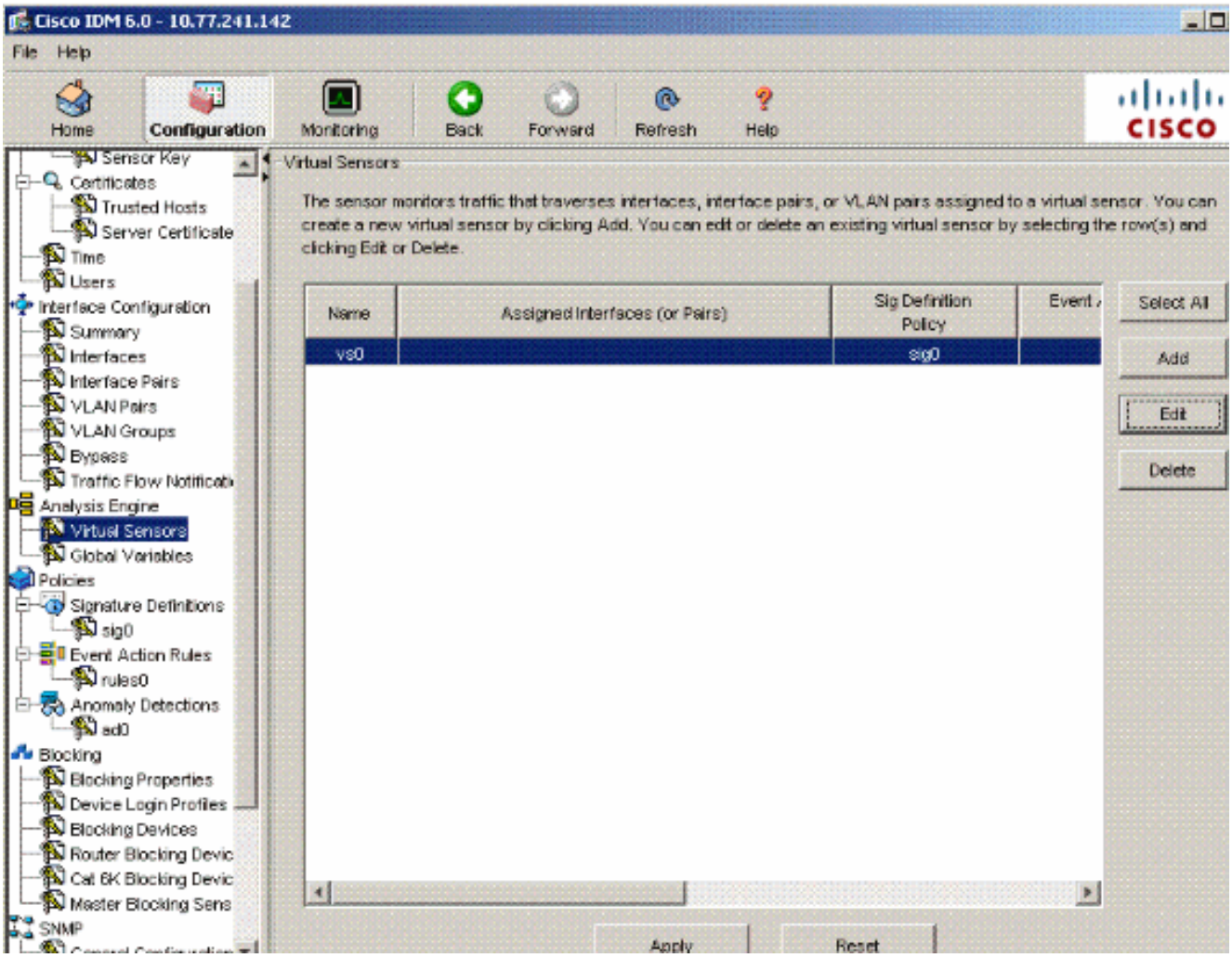
8. Immettere il numero della sottointerfaccia, la VLAN A e la VLAN B per l'interfaccia di rilevamento (Gigabit



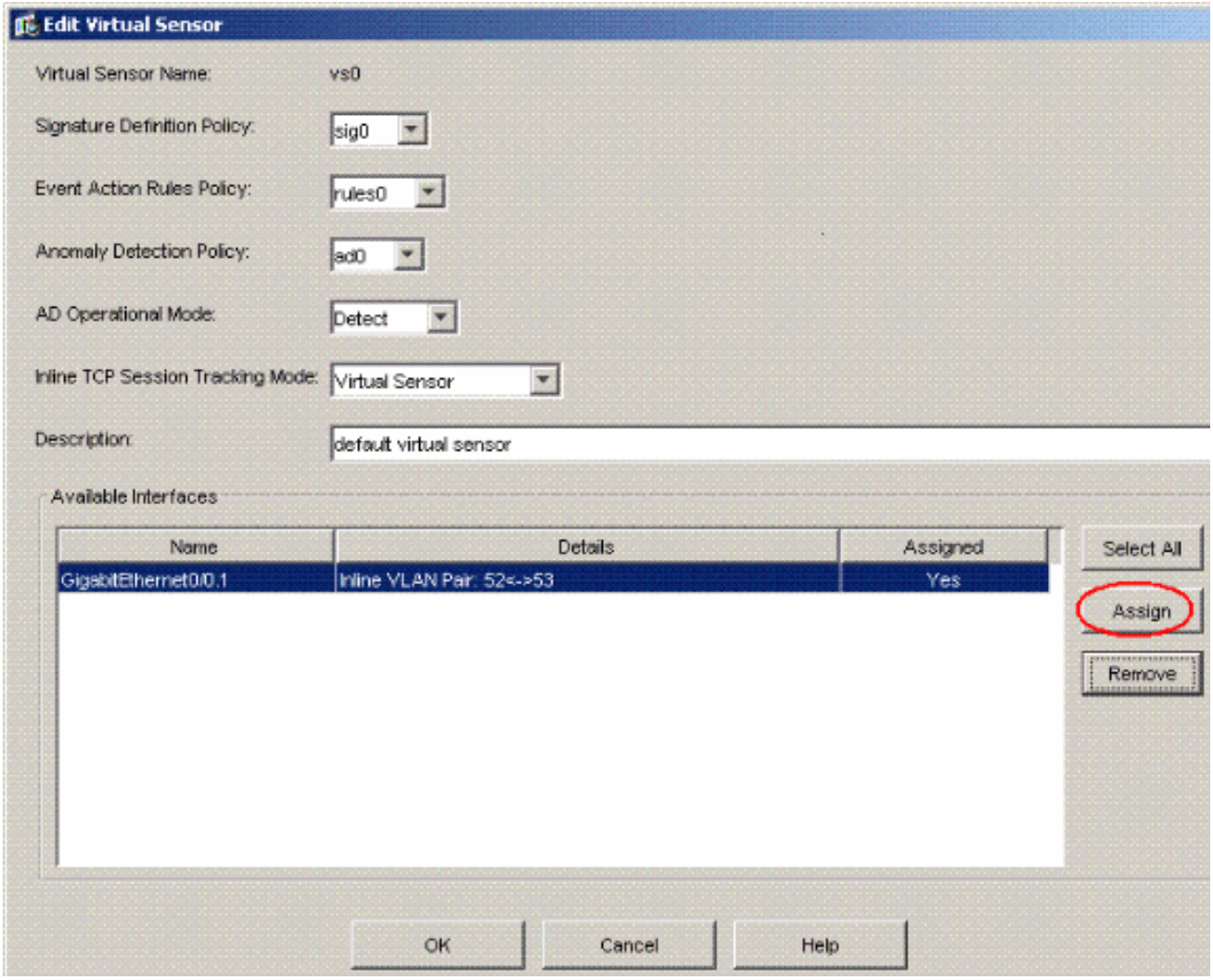
Ethernet0/0). È possibile visualizzare il riepilogo della configurazione della coppia di VLAN in linea.



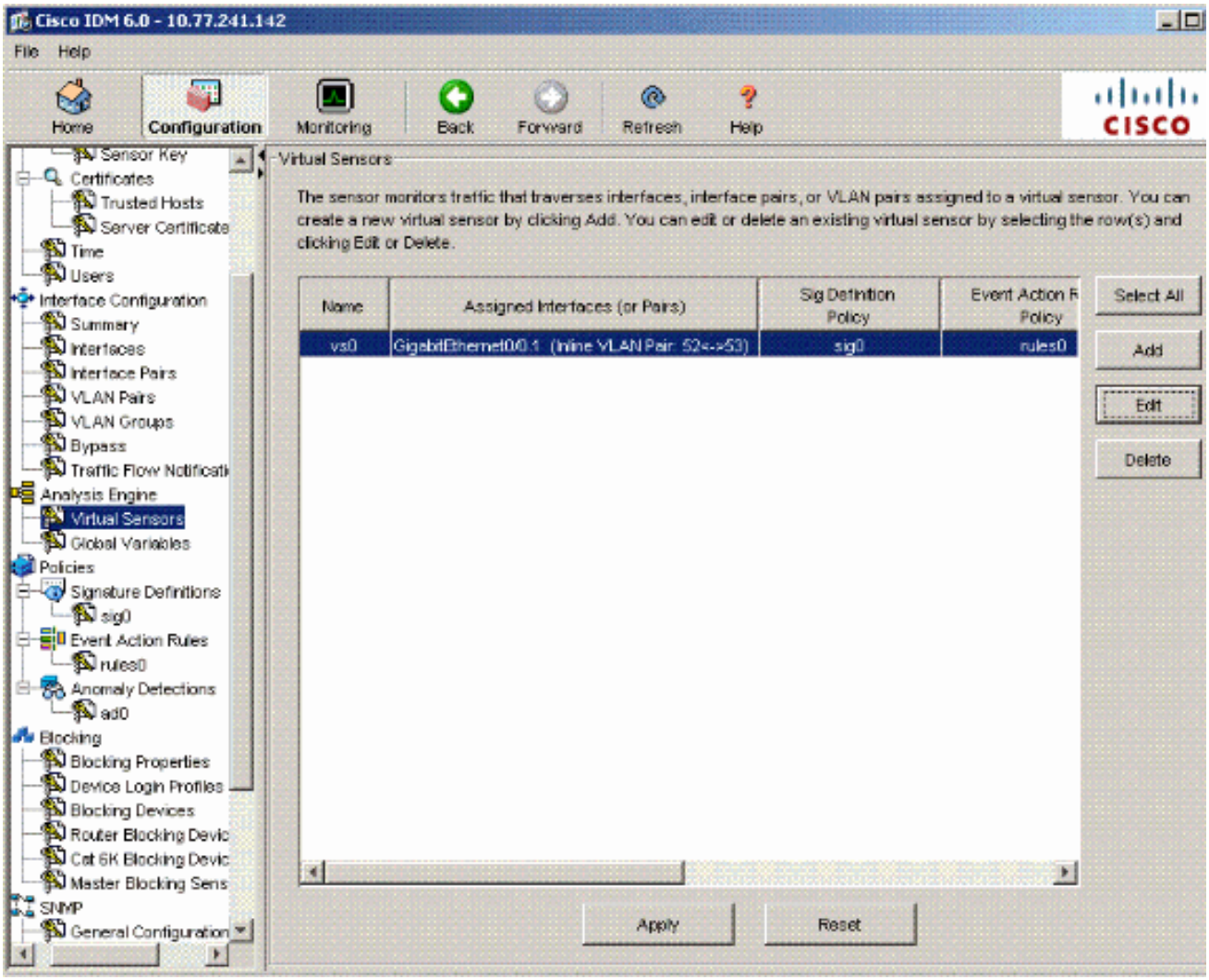
9. Per creare il nuovo sensore virtuale, selezionare **Configurazione > Analysis Engine > Virtual Sensor** e fare clic su **Modifica**.



10. Assegnare la coppia di VLAN inline 52 e 53 al sensore virtuale vs0.



Visualizza il riepilogo delle informazioni sul sensore virtuale assegnato.



Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Cisco ASA serie 5500 Adaptive Security Appliance
- Cisco Intrusion Prevention System
- Cisco IPS serie 4200 Sensori
- Documentazione e supporto tecnico – Cisco Systems