IPS 5.X en hoger/IDSM2: Inline VLAN-voorbeeldmodus met CLI- en IDM-configuratievoorbeeld

Inhoud

[Inleiding](#)
[Voorwaarden](#)
[Vereisten](#)
[Gebruikte componenten](#)
[Verwante producten](#)
[Conventies](#)
[Configuratie van VACL-opname](#)
[Configuratie van inline VLAN-paarmodus](#)
[CLI-configuratie](#)
[IDM-configuratie](#)
[Problemen oplossen](#)
[Gerelateerde informatie](#)

Inleiding

De associatie van VLANs in paren op een fysieke interface is gekend als inline VLAN paarmodus. Packets die op een van de gepaarde VLAN's worden ontvangen, worden geanalyseerd en naar het andere VLAN in het paar doorgestuurd. Inline VLAN-paren worden ondersteund op alle sensoren die compatibel zijn met Inbraakpreventiesysteem (IPS) 5.1, behalve NM-CIDS, AIP-SSM-10 en AIP-SSM-20.

De inline VLAN paarmodus is een actieve sensatiemodus waarin een sensatieinterface als een 802.1q kofferpoort werkt en de sensor VLAN-overbrugging tussen paren VLAN's op de romp uitvoert. Dit betekent dat de op de sensorinterface aangesloten schakelaar in de boomstand moet zijn.

De sensor inspecteert het verkeer dat het op elk VLAN in elk paar ontvangt en kan de pakketten op het andere VLAN in het paar doorsturen of het pakket laten vallen als een inbraakpoging wordt gedetecteerd. U kunt een IPS-sensor configureren om gelijktijdig een brug te slaan naar 255 VLAN-paren op elke sensatieinterface. De sensor vervangt het veld VLAN ID in de 802.1q-header van elk ontvangen pakket met de ID van het grotere VLAN waarop de sensor het pakket doorstuurt. De sensor laat alle pakketten vallen die op om het even welke VLAN worden ontvangen die niet aan inline VLAN paren worden toegewezen.

Opmerking: voor IPS-4260 wordt een indien-open hardwarebypass niet ondersteund op paren van inline VLAN. Raadpleeg de beperkingen van de hardwareconfiguratie voor meer informatie.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Inbraakpreventiesysteem Sensor die de 5.1 en hoger gebruikt.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Verwante producten

De informatie in dit document is ook van toepassing op de servicesmodule voor inbraakdetectiesysteem (IDSM-2).

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Configuratie van VACL-opname

Raadpleeg het gedeelte VACL-opname configureren van IDSM-2 configureren om verkeer naar IDSM op de switch te kunnen versturen.

Configuratie van inline VLAN-paarmodus

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik het Opname Gereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Gebruik de opdracht **Physical-interfaces interface_name** in de service interface submode om inline VLAN-paren te configureren met behulp van de CLI. De interfacenaam is FastEthernet of Gigabit Ethernet.

Deze opties zijn van toepassing:

- **beheerder {ingeschakeld |** —de administratieve verbindingsstaat van de interface, of de interface is ingeschakeld of uitgeschakeld.**Opmerking:** Op alle backplane sensorinterfaces op alle modules (IDSM-2 NM-CIDS en AIP-SSM) is de admin-status ingesteld op Aan-en wordt

beschermd (u kunt de instelling niet wijzigen). De admin-status heeft geen effect (en wordt beschermd) op de commando en controle interface. Het beïnvloedt alleen sensatieinterfaces. De opdracht en de bedieningsinterface hoeven niet te worden ingeschakeld omdat deze niet kan worden bewaakt.

- **standaard**: Hiermee stelt u de waarde weer in op de standaardinstelling van het systeem.
- **beschrijving** - Uw beschrijving van het online interfacepaar.
- **duplex** - de duplex instelling van de interface.**auto**-Stelt de interface in om te onderhandelen over duplex.Stelt de interface in op full duplex.**half**-stelt de interface in op half duplex.**Opmerking:** de duplexoptie is op alle modules beschermd.
- **Nee** - Verwijdert een ingang of selectie instelling.
- **snelheid**—de snelheidsinstelling van de interface.**auto**-stelt de interface in om snelheid te onderhandelen.**10**-Hiermee wordt de interface ingesteld op 10 MB (alleen voor TX-interfaces).**100**-Hiermee wordt de interface ingesteld op 100 MB (alleen voor TX-interfaces).**1000**—Hiermee wordt de interface ingesteld op 1 GB (voor Gigabit-interfaces)**Opmerking:** de snelheidsoptie wordt op alle modules beschermd.
- **subinterface-type** - Specificeert dat de interface een subinterface is en welk type subinterface wordt gedefinieerd.**inline-VLAN-**paar - Hiermee kunt u de subinterface definiëren als een inline VLAN-paar.**geen**-geen subinterfaces gedefinieerd.
- **subinterface**-definieert de subinterface als een inline VLAN-paar.**VLAN1**-het eerste VLAN in het inline VLAN-paar.**VLAN2**-het tweede VLAN in het inline VLAN paar.

CLI-configuratie

Voltooi deze stappen om de instellingen van het paar inline VLAN op de sensor te configureren met behulp van CLI:

1. Meld u aan bij de CLI met behulp van een account met Administrator-rechten.
2. Geef de submodus interface op:
```
sensor#configure terminal
sensor(config)#service interface
sensor(config-int)#
```
3. Controleer of er inline interfaces bestaan (het subinterfacetype zou "geen" moeten lezen als er geen inline interfaces zijn geconfigureerd):
```
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. Verwijder inline interfaces die deze fysieke interface gebruiken:

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

5. Toont de lijst met beschikbare interfaces:

```
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. Specificeer een interface:

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

7. Schakel de beheerstatus van de interface in:

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

   De interface moet aan de virtuele sensor worden toegewezen en ingeschakeld om het verkeer te bewaken.

8. Voeg een beschrijving van deze interface toe:

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

9. Configuratie van de duplexinstellingen:
```
sensor(config-int-phy)#duplex full
```

   Deze optie is niet beschikbaar voor modules.
10. Instellen van de snelheid:
```
sensor(config-int-phy)#speed 1000
```

    Deze optie is niet beschikbaar voor modules.
11. Stel het paar inline VLAN in:
```
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. Voeg een beschrijving toe voor het inline VLAN-paar:
```
sensor(config-int-phy-inl-sub)#description pairs vlans 52 and 53
```

13. Controleer de instellingen voor inline VLAN:
```
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. De interface-submodus verlaten:
```
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. Druk op **Voer** in om de wijzigingen toe te passen of voer **geen** om ze weg te gooien in.
16. Geef de configuratie van de virtuele sensor op:
```
sensor(config)#service analysis-engine
        sensor(config-ana)#virtual-sensor vs0
```

17. Voeg de interface toe aan de virtuele sensor:
```
sensor(config-ana-vir)#physical-interface GigabitEthernet0/2
subinterface-number 1
```

18. De virtuele-sensor-submodus verlaten:
```
sensor(config-ana-vir)#exit
        sensor(config-ana)#exit
        Apply Changes:?[yes]:
```
19. Druk op **Voer** in om de wijzigingen toe te passen of voer **geen** om ze weg te gooien in.

IDM-configuratie

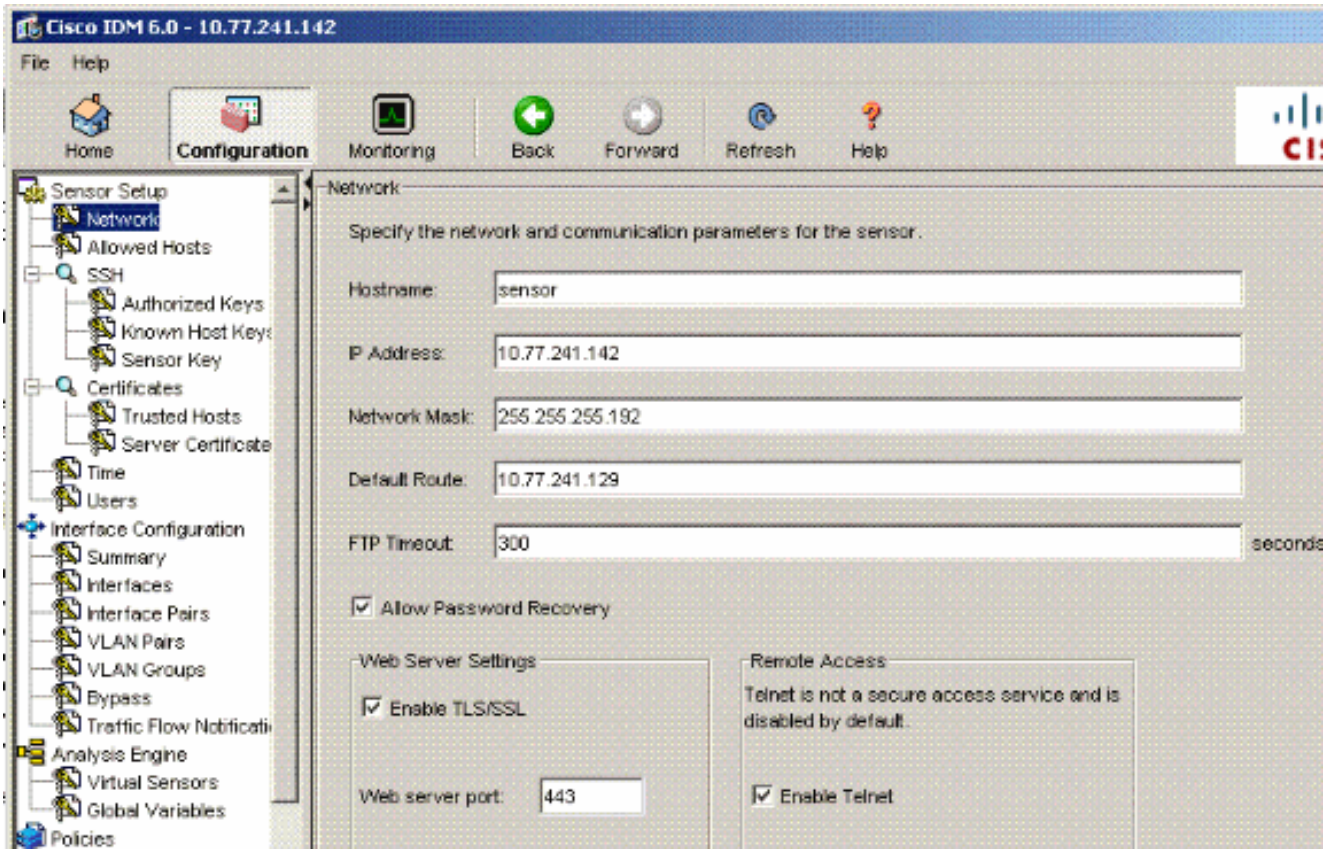
Voltooi deze stappen om de instellingen voor inline VLAN-paar op de sensor te configureren met behulp van IDS Apparaatbeheer (IDM):

1. Open uw browser en voer **https://<Management_IP_Address_of_IPS>**in om de IDM op de IPS te gebruiken.
2. Klik op **IDM Launcher downloaden en IDM starten** om het installatieprogramma voor de

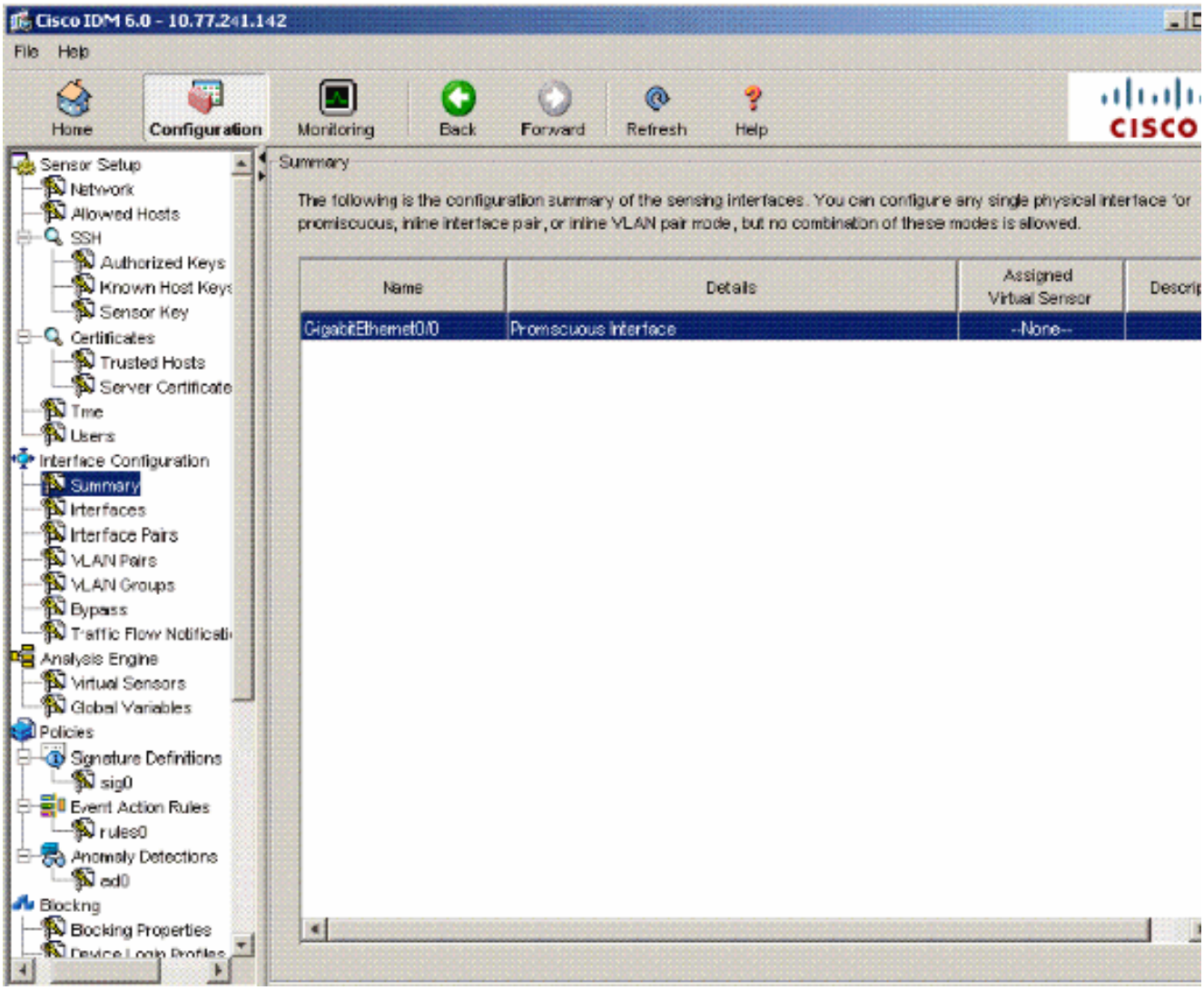
toepassing te downloaden.

3. Ga naar de startpagina om de apparaatinformatie te bekijken, zoals hostnaam, IP-adres, versie en het model.,
   enzovoort.

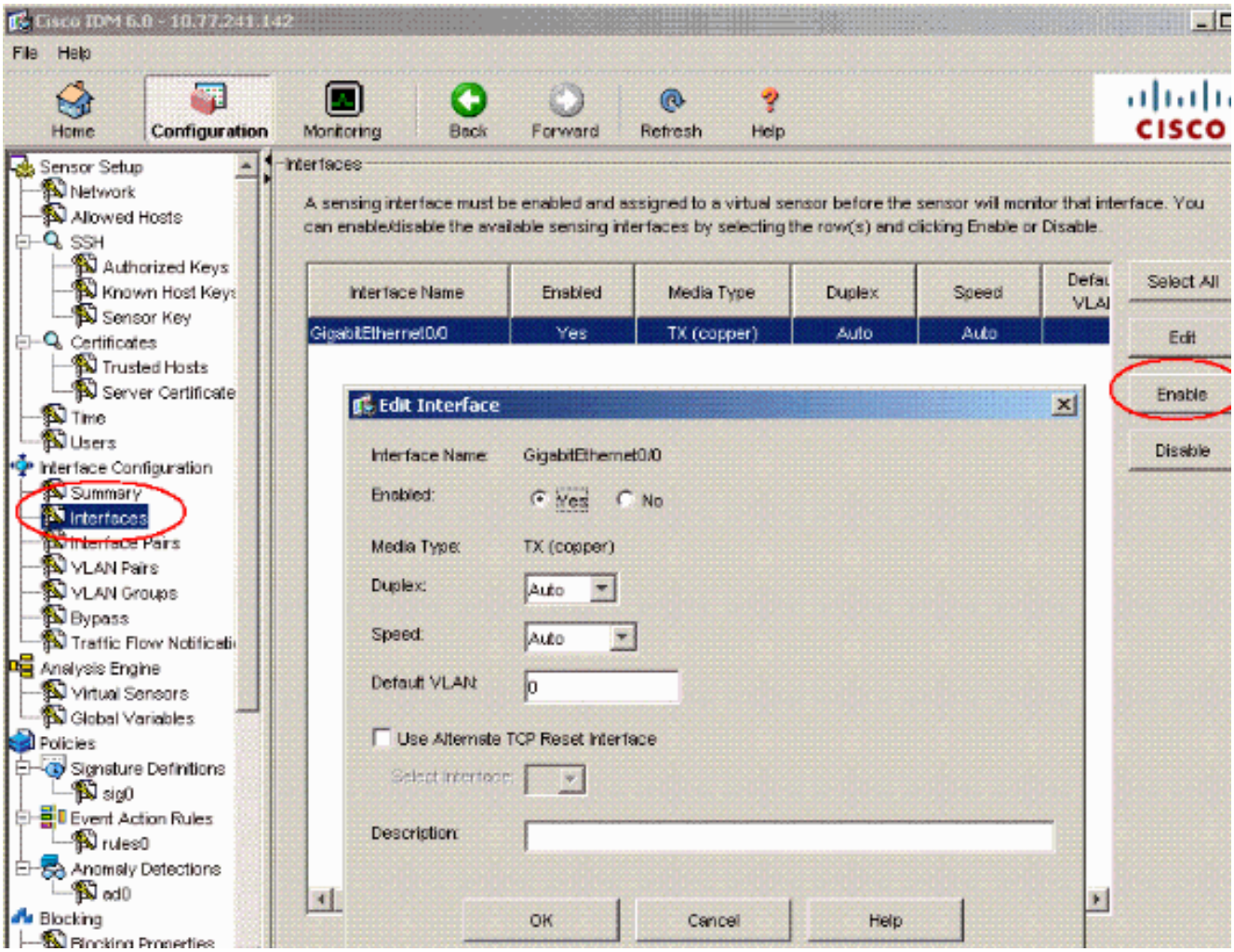
4. Ga naar **Configuration > Sensor Setup** en klik op **Network**. Hier kunt u de Hostnaam, IP-adres en standaardroute
   instellen.



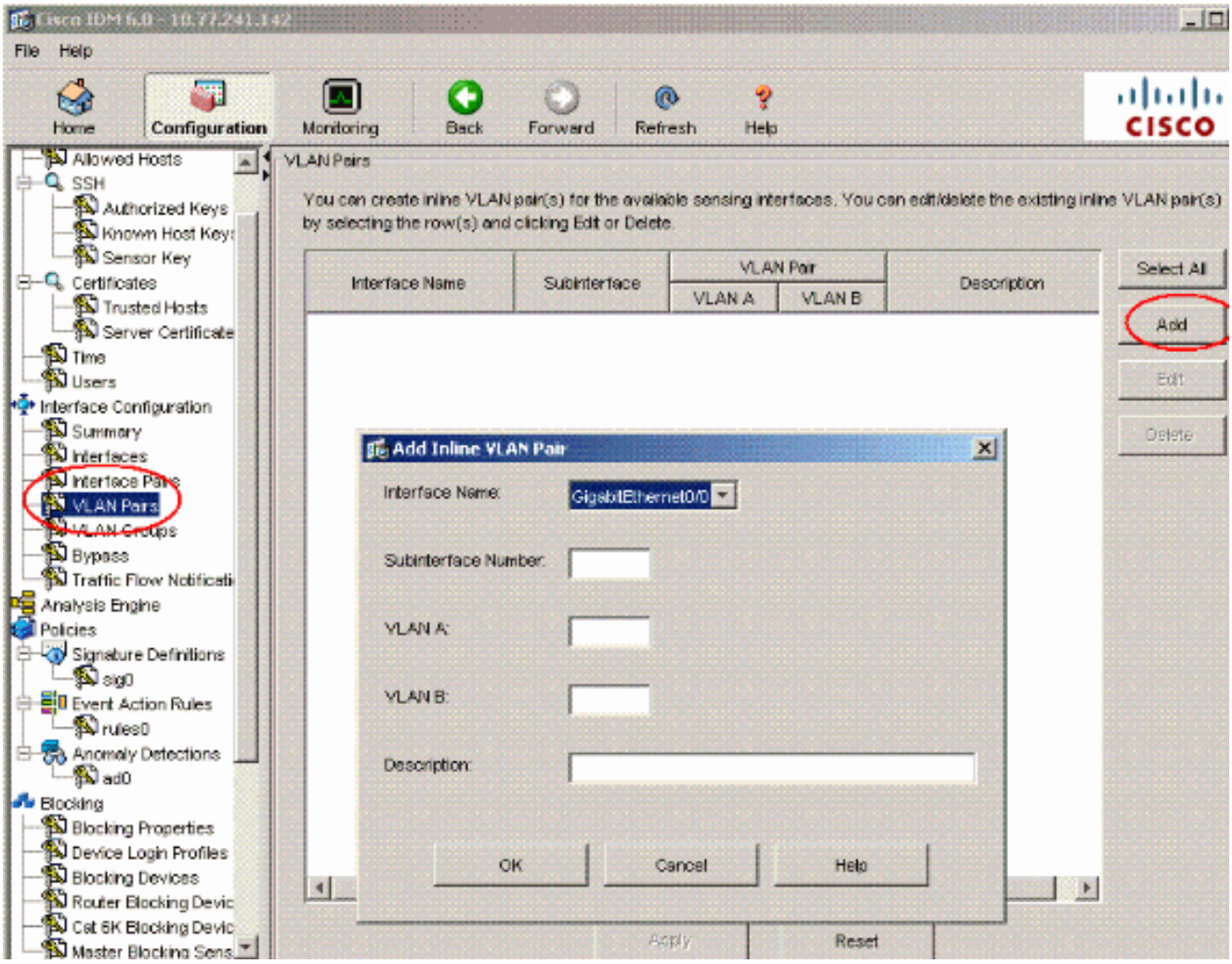
5. Ga naar **Configuration > Interface Configuration** en klik op **Summary**.Deze pagina toont de configuratiesamenvatting van de sensatieinterface.



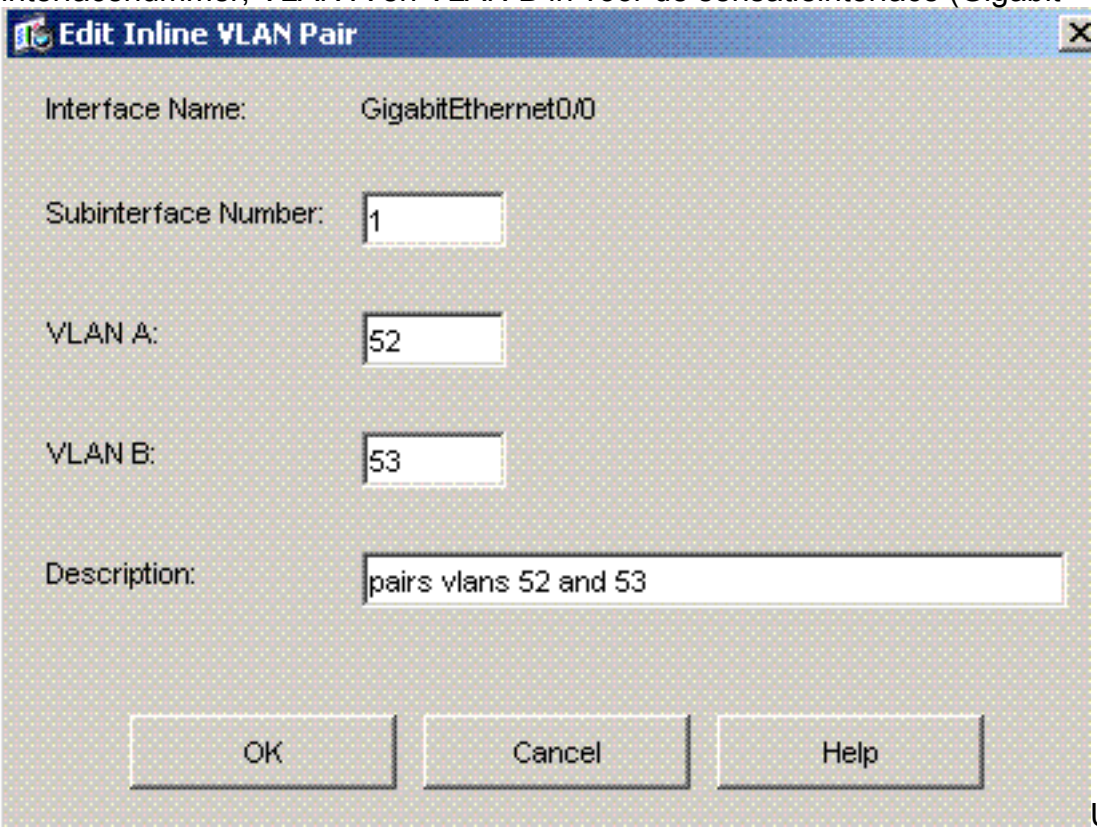
6. Ga naar **Configuration > Interface Configuration > Interfaces** en selecteer de interfacenaam.Klik vervolgens op **Enable** om de sensatieinterface in te schakelen. Configureer ook de informatie Duplex, Speed en VLAN.



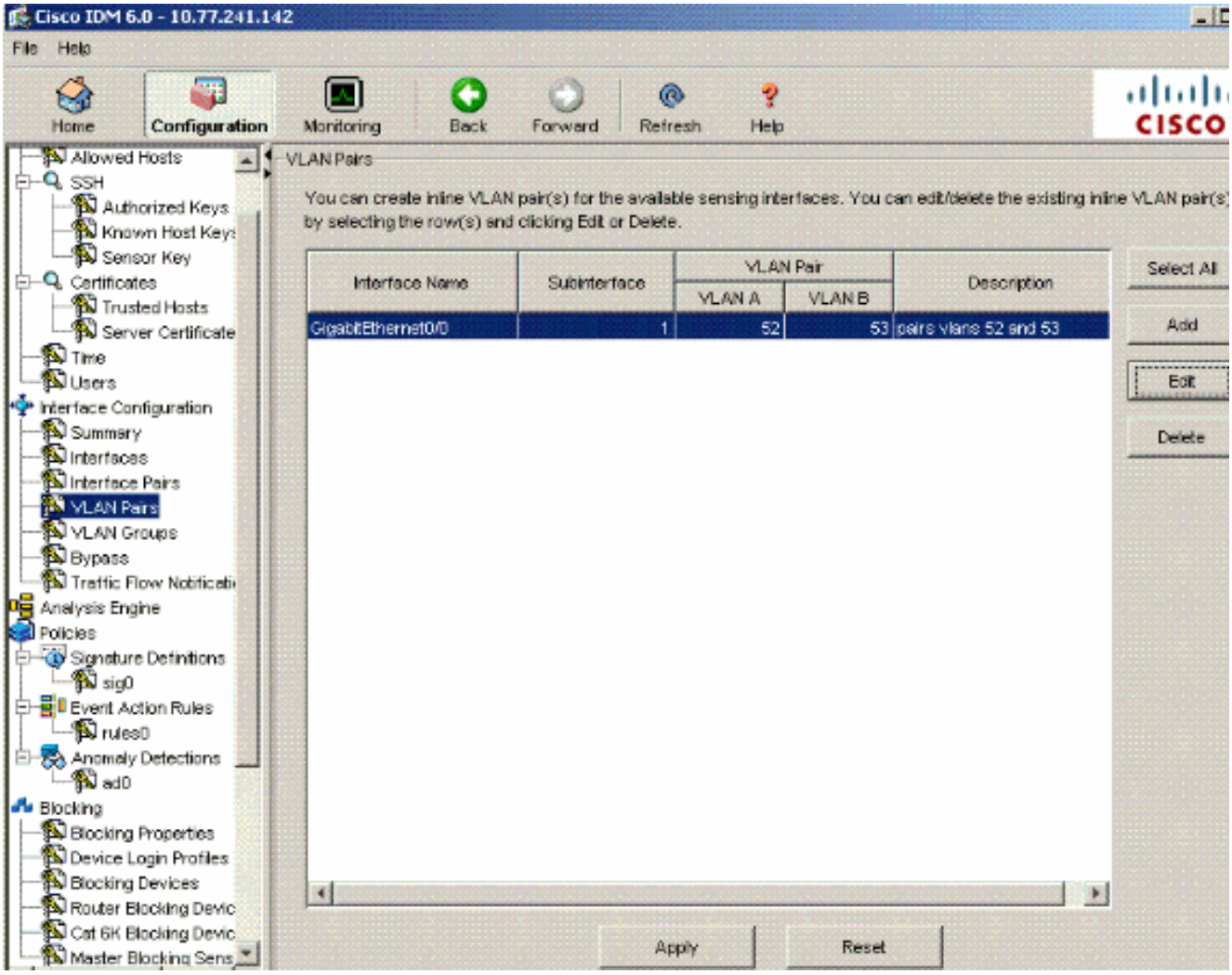
7. Ga naar **Configuration > Interface Configuration > VLAN-paren** en klik op **Add** om de inline VLAN-paren te
maken.



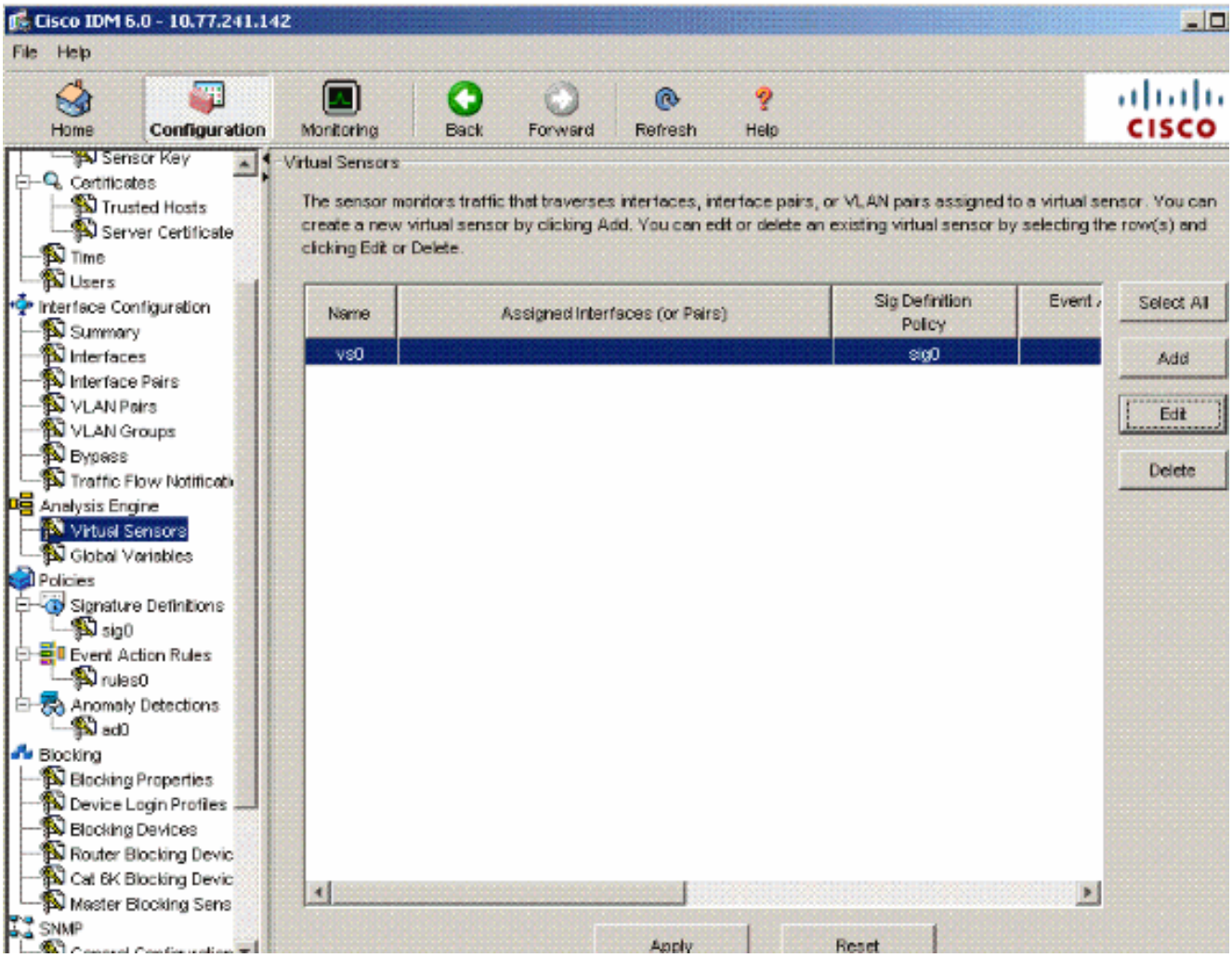
8. Voer het Subinterfacenummer, VLAN A en VLAN B in voor de sensatieinterface (Gigabit Ethernet0/0).



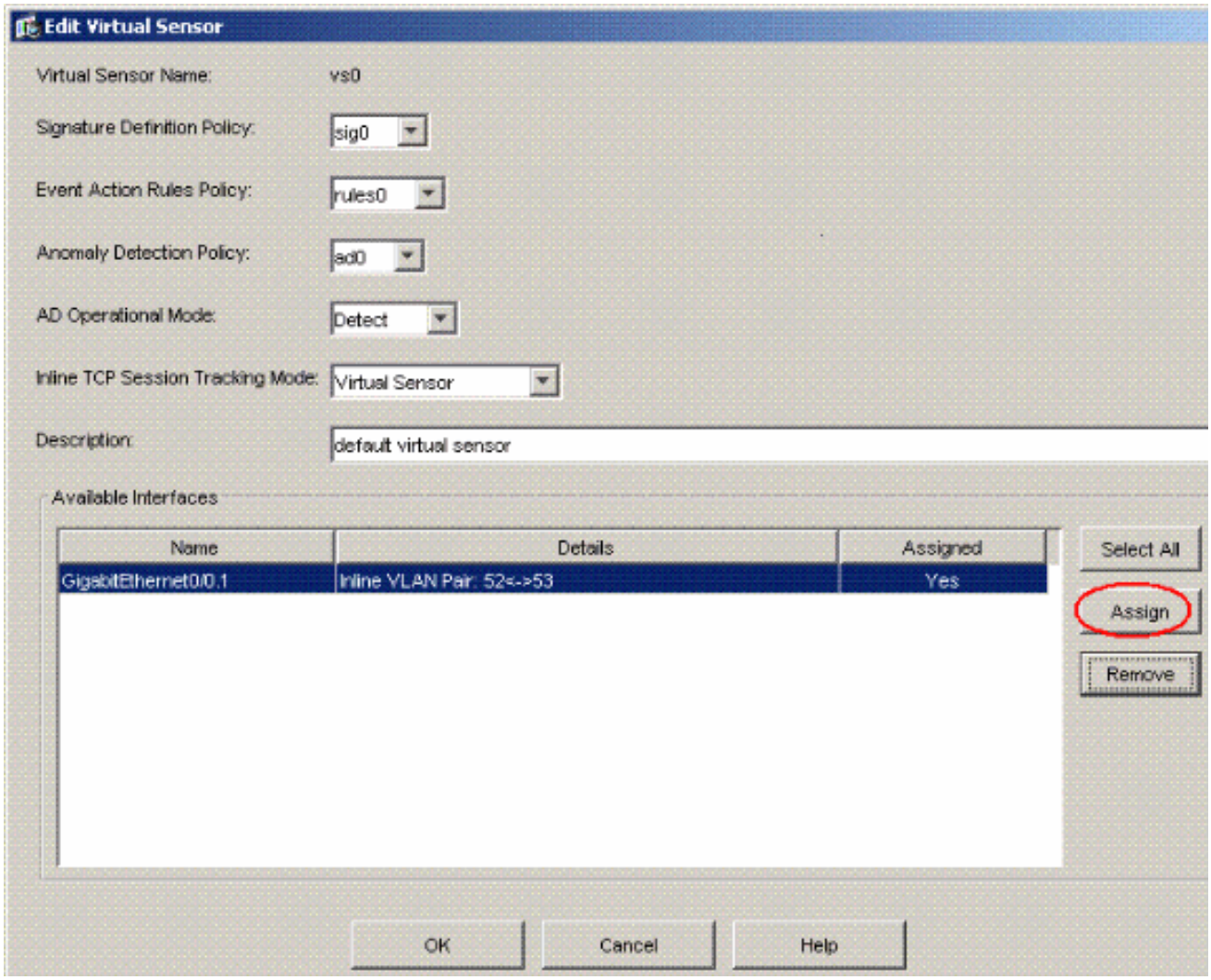
U kunt de samenvatting van de configuratie van het inline VLAN-paar bekijken.



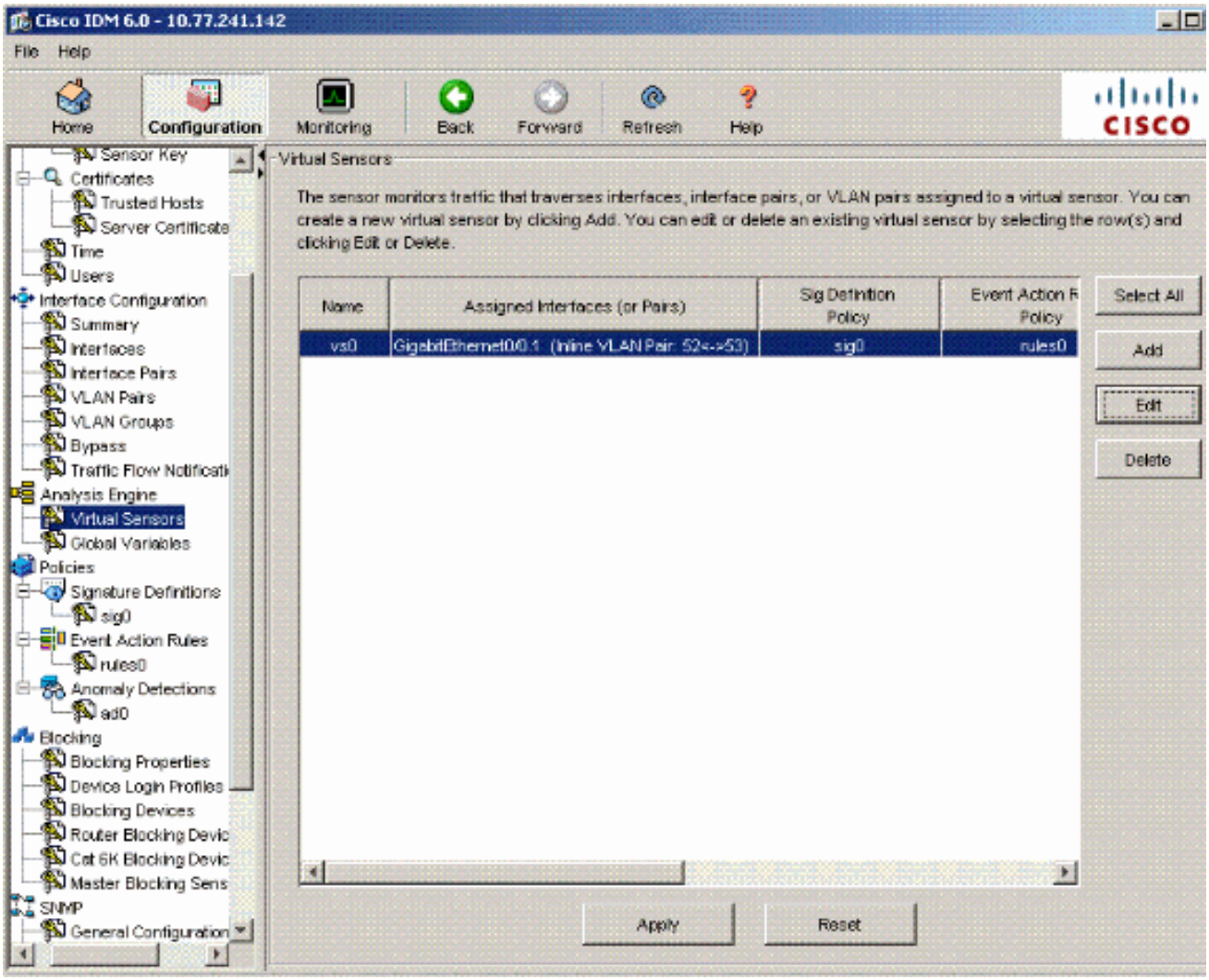
9. Ga naar **Configuration > Analysis Engine > Virtual Sensor** en klik op **Bewerken** om de nieuwe virtuele sensor te
maken.



10. Pas de inline VLAN-telefoon 52 en 53 aan de virtuele sensor vs0.



Bekijk de samenvatting van de toegewezen virtuele sensorinformatie.



Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- Cisco ASA 5500 Series adaptieve security applicaties
- Cisco-inbraakpreventiesysteem
- Cisco IPS 4200 Series sensoren
- Technische ondersteuning en documentatie – Cisco Systems