IPS 6.X en hoger/IDSM2: Inline interfacemodus met behulp van IDM-configuratievoorbeeld

Inhoud

Inleiding

Wanneer u in de modus Inline Interface air werkt, wordt het inbraakpreventiesysteem (IPS) rechtstreeks in de verkeersstroom gezet en heeft het effect op pakketsnelheden, waardoor deze trager worden wanneer er latentie wordt toegevoegd. Dit stelt de sensor in staat om aanvallen te stoppen zodat het kwaadaardig verkeer daalt voordat het doel bereikt, en het biedt dus bescherming. Niet alleen is de informatie over de verwerking van het inline apparaat op Lagen 3 en 4, maar het analyseert ook de inhoud en lading van de pakketten voor geavanceerdere ingebedde aanvallen (Lagen 3 tot 7). Deze diepere analyse laat het systeem aanvallen identificeren en stoppen en/of blokkeren die normaal door een traditioneel firewallapparaat lopen.

In de modus Inline-interface wordt een pakje ingevoerd in de eerste interface van het paar op de sensor en in de tweede interface van het paar. Het pakket wordt naar de tweede interface van het paar verzonden, tenzij het pakket wordt ontkend of gewijzigd door een handtekening.

Opmerking: U kunt AIM-IPS en AIP-SSM configureren om inline te werken, ook al hebben deze modules slechts één detecterende interface.

Opmerking: Als de gekoppelde interfaces op dezelfde schakelaar zijn aangesloten, dient u deze op de schakelaar te configureren als toegangspoorten met verschillende toegang VLAN's voor de twee poorten. Anders stroomt het verkeer niet door de inline interface.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco IPS Sensor die de Opdracht Line Interface 6.0 en Inbraakpreventiesysteem Manager (IDM) 6.0 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 inline-interfaceprocessors

Gebruik de opdracht *naam* ***van inline-interfaces in de submodus van de servicinterface om inline interfaceparen te maken.***

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

Opmerking: AIP-SSM is ingesteld voor inline interfacemodus vanuit Cisco ASA CLI en niet vanuit Cisco IPS CLI.

Deze opties zijn van toepassing:

- *Naam* ***van inline-interfaces*** - Naam van het logische inline interfacepaar**Opmerking:** Op alle backplane sensorinterfaces op alle modules (IDSM-2 NM-CIDS en AIP-SSM) is **de admin-status** ingeschakeld en 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
- **interface1** *interface_name* - De eerste interface in het inline interfacepaar
- **interface2** *interface_name*—De tweede interface in het inline interfacepaar
- **no**—Verwijdert een invoer of selectie-instelling
- **beheerder {ingeschakeld |** —de administratieve verbindingsstaat van de interface, of de

interface is ingeschakeld of uitgeschakeld.

CLI-configuratie

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

1. Meld u aan bij de CLI met een account met beheerrechten.
2. Geef de submodus interface op:
```
sensor#configure terminal
sensor(config)#service interface
sensor(config-int)#
```
3. Controleer of er 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. Geef het inline paar een naam:

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

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. Configuratie van twee interfaces in een paar:

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


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

   U moet de interface aan een virtuele sensor toewijzen en deze activeren voordat het verkeer kan bewaken. Zie stap 10 voor meer informatie.

7. Voeg een beschrijving van deze interface toe:

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

8. Herhaal stappen 4 door 7 voor andere interfaces die u wilt configureren tot inline interfaceparen.
9. Controleer de instellingen:

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

10. Schakel de interfaces in die aan het interfacepaar zijn toegewezen:

```
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. Controleer dat de interfaces zijn ingeschakeld:

```
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--
```

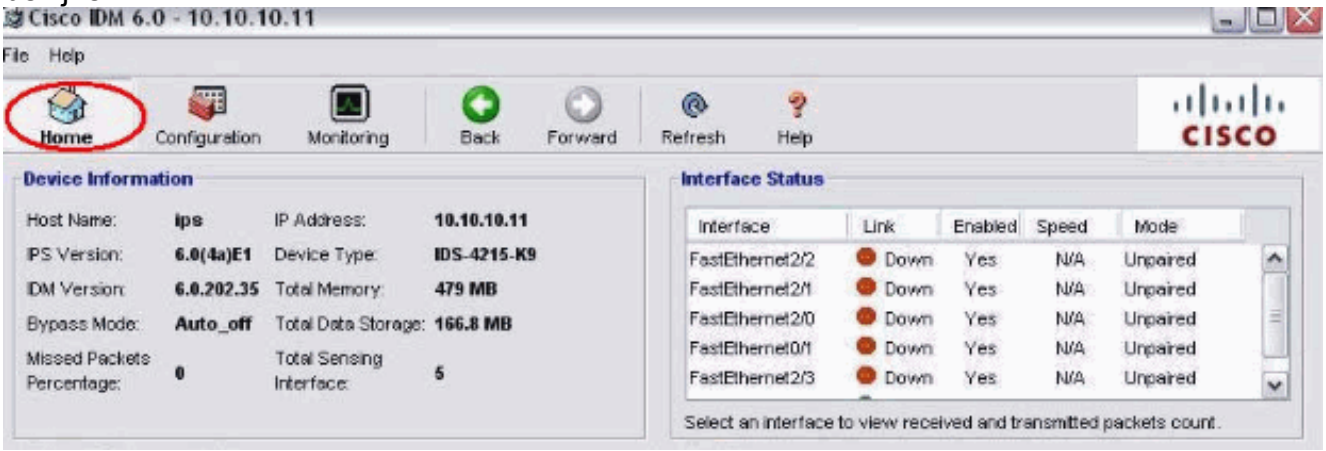
12. Geef deze opdracht uit om een inline interfacepaar te verwijderen en de interfaces terug te sturen naar de veelbelovende modus:
    ```
    sensor(config-int)#no inline-interfaces PAIR1
    ```

    U moet ook het inline-interfacepaar uit de virtuele sensor verwijderen waaraan het is toegewezen.
13. Controleer of het inline interfacepaar is verwijderd:
    ```
    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. Submodus interface-configuratie afsluiten:
    ```
    sensor(config-int)#exit
    Apply Changes:?[yes]:
    ```
15. Druk op **Voer** in om de wijzigingen toe te passen of **ga** het **niet** in om ze weg te gooien.

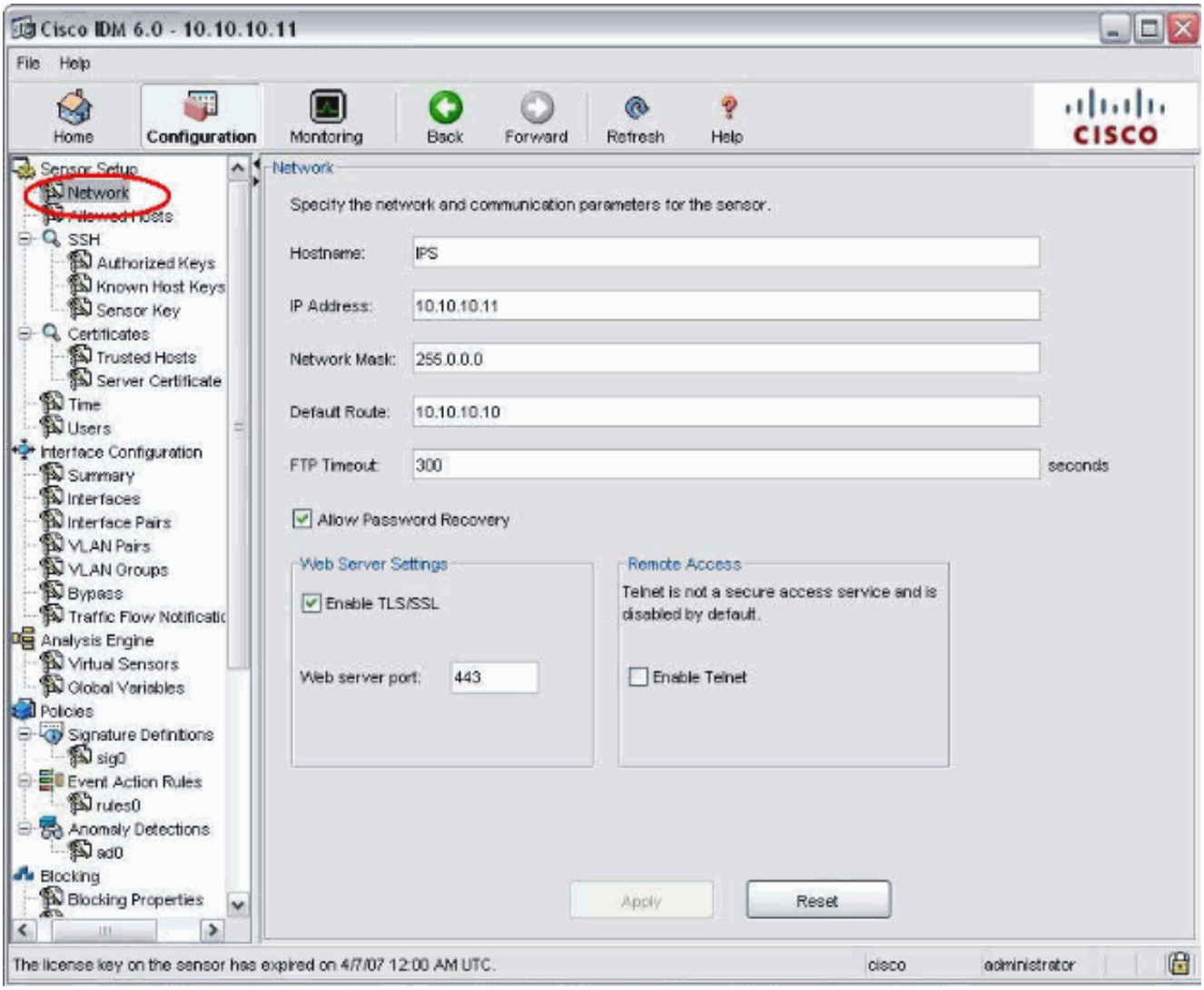
IDM-configuratie

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

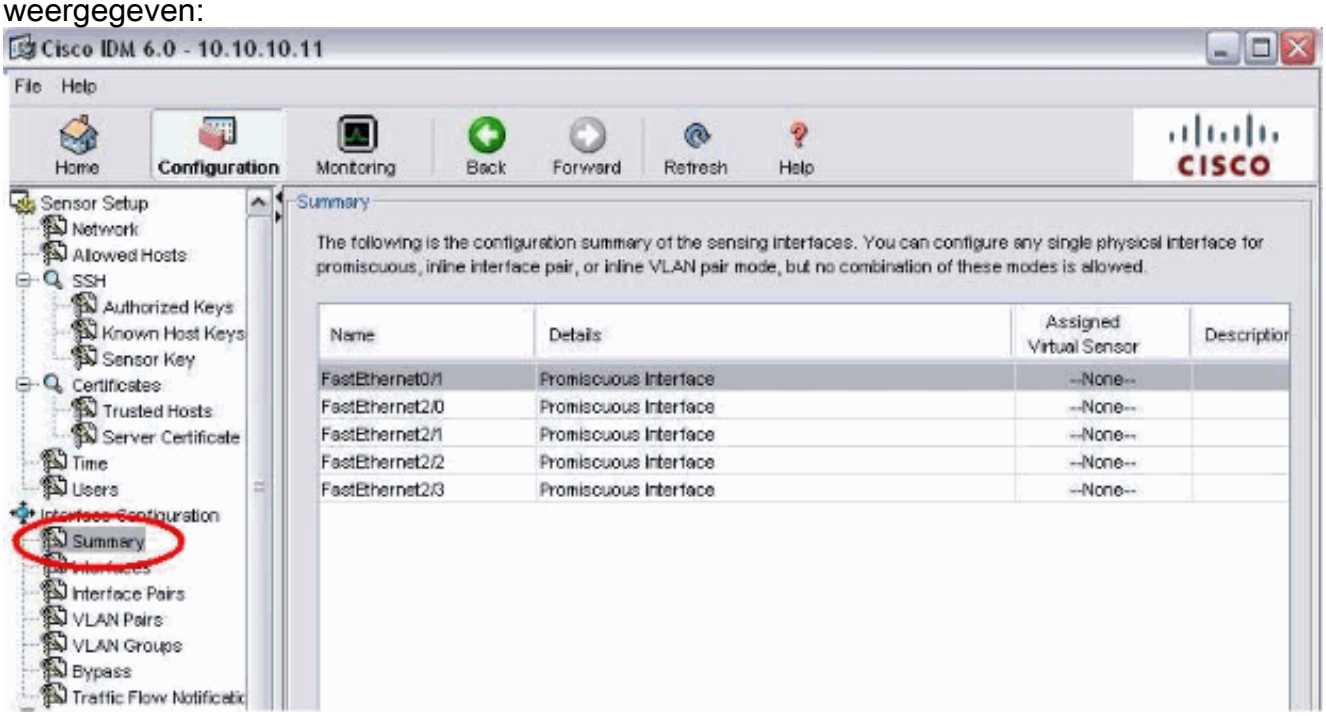
1. Open uw browser en voer **https://<Management_IP_Address_of_IPS>**in om de IDM op de IPS te gebruiken.
2. Klik op **Download IDM Launcher** en **Start IDM** om het installatieprogramma voor de toepassing te downloaden.
3. Ga naar de startpagina om de apparaatinformatie zoals Host Name, IP Address, versie en het model te
   bekijken.



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

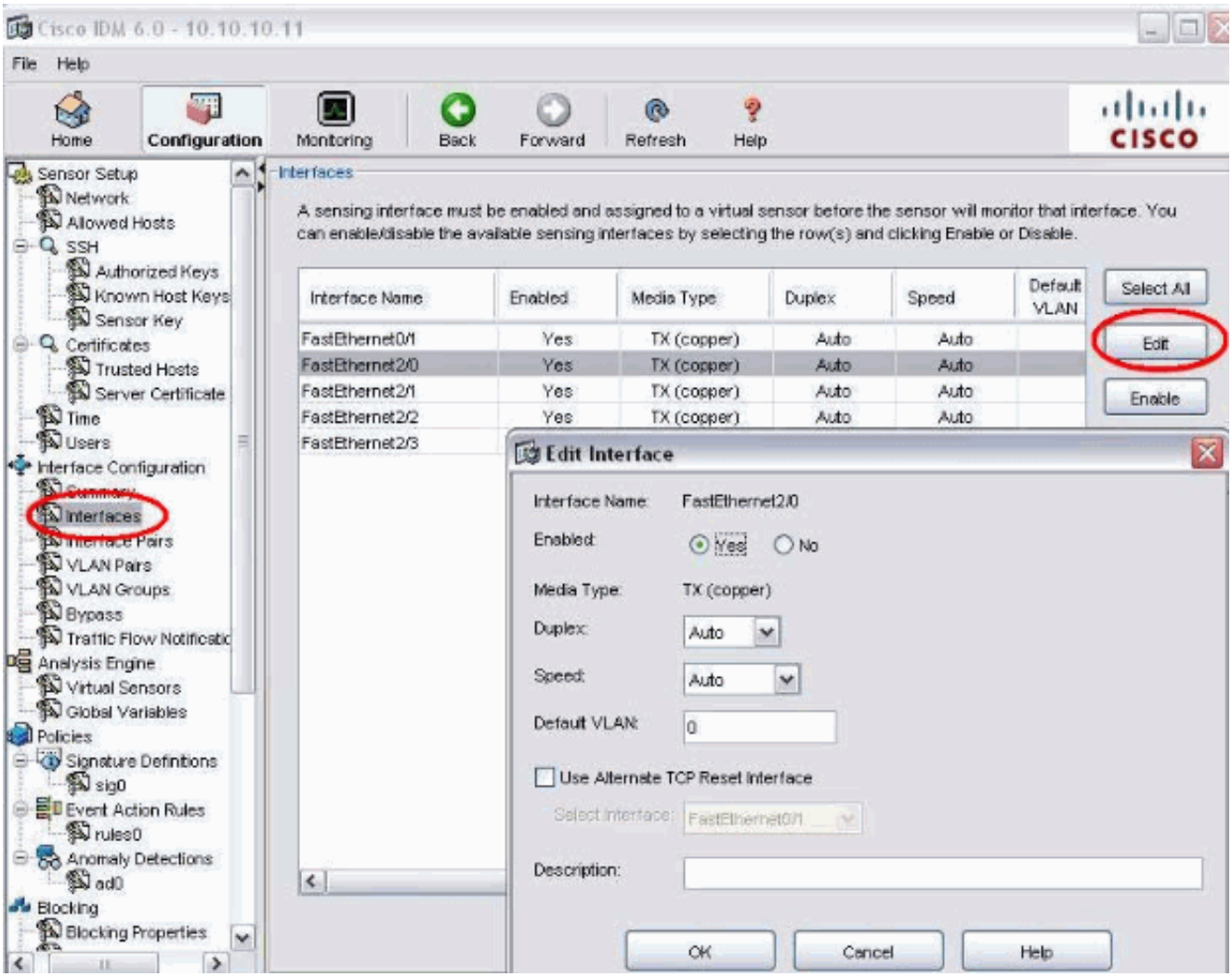


5. Ga naar **Configuration > Interface Configuration** en klik op **Summary**.Op deze pagina wordt de samenvatting van de configuratie van de sensorinterface weergegeven:

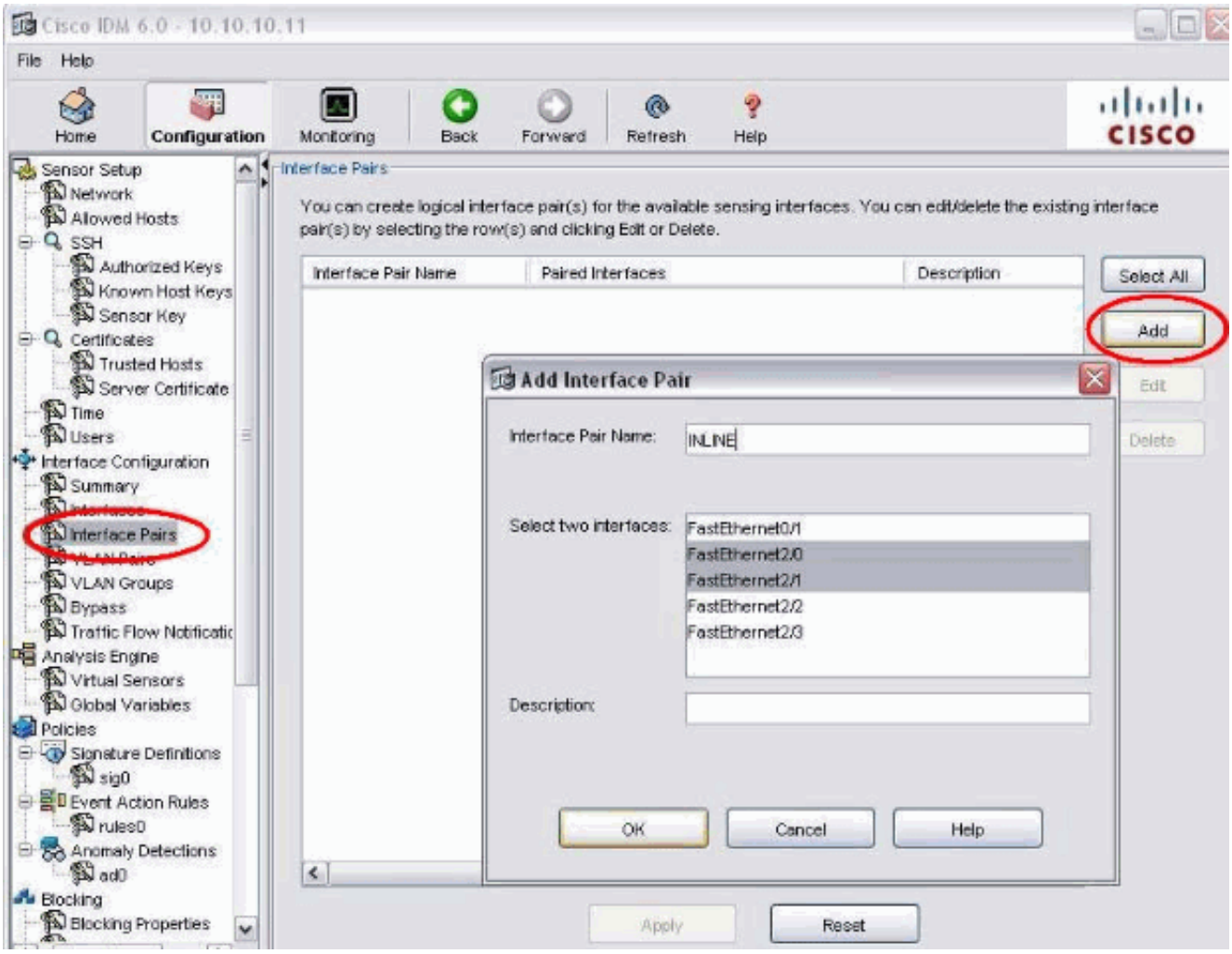


6. Ga naar **Configuration > Interface Configuration > Interfaces** en selecteer de interfacenaam. Klik vervolgens op **Inschakelen** om de detecterende interface in te schakelen. Configureer ook de informatie Duplex, Speed en

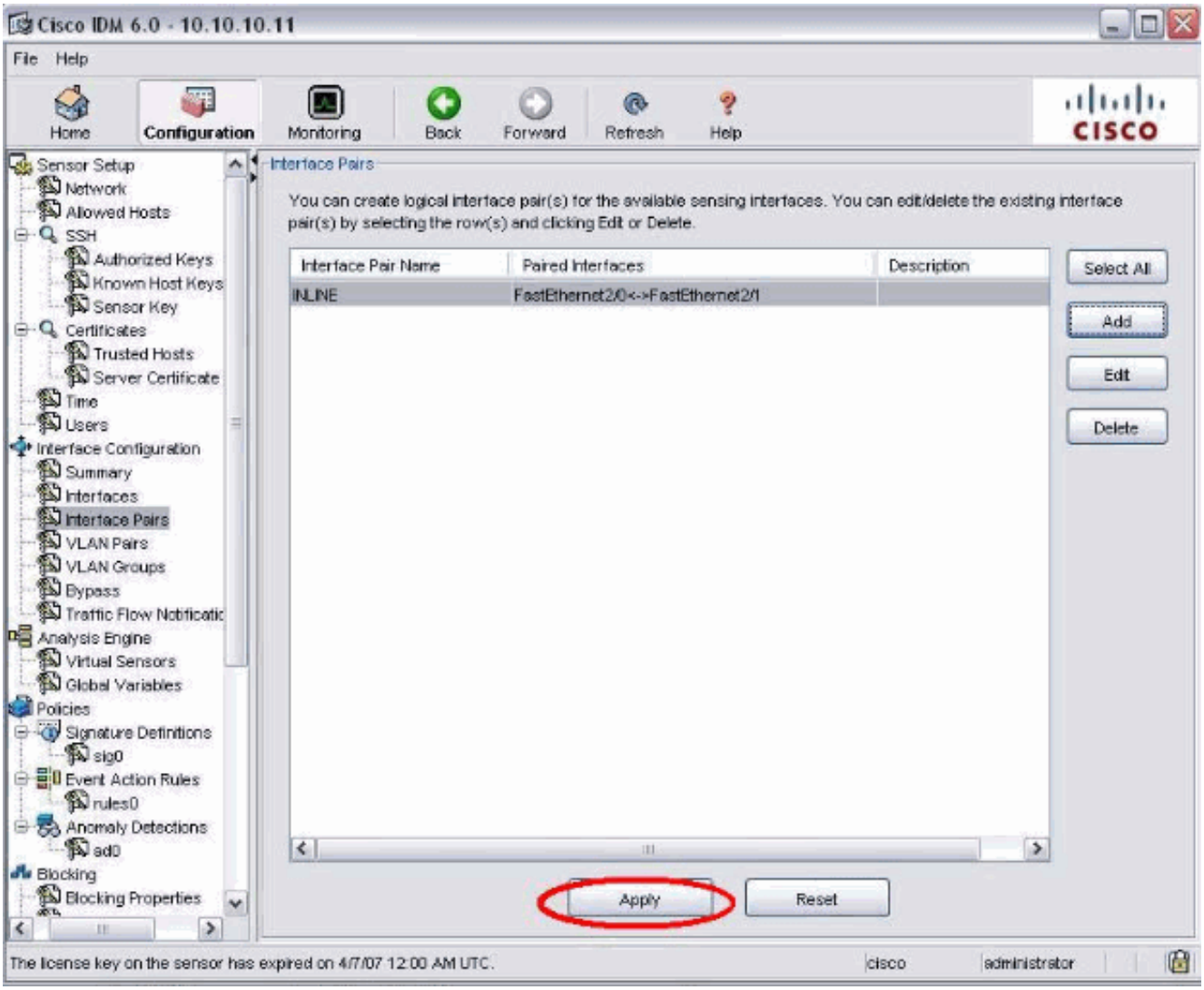
VLAN.



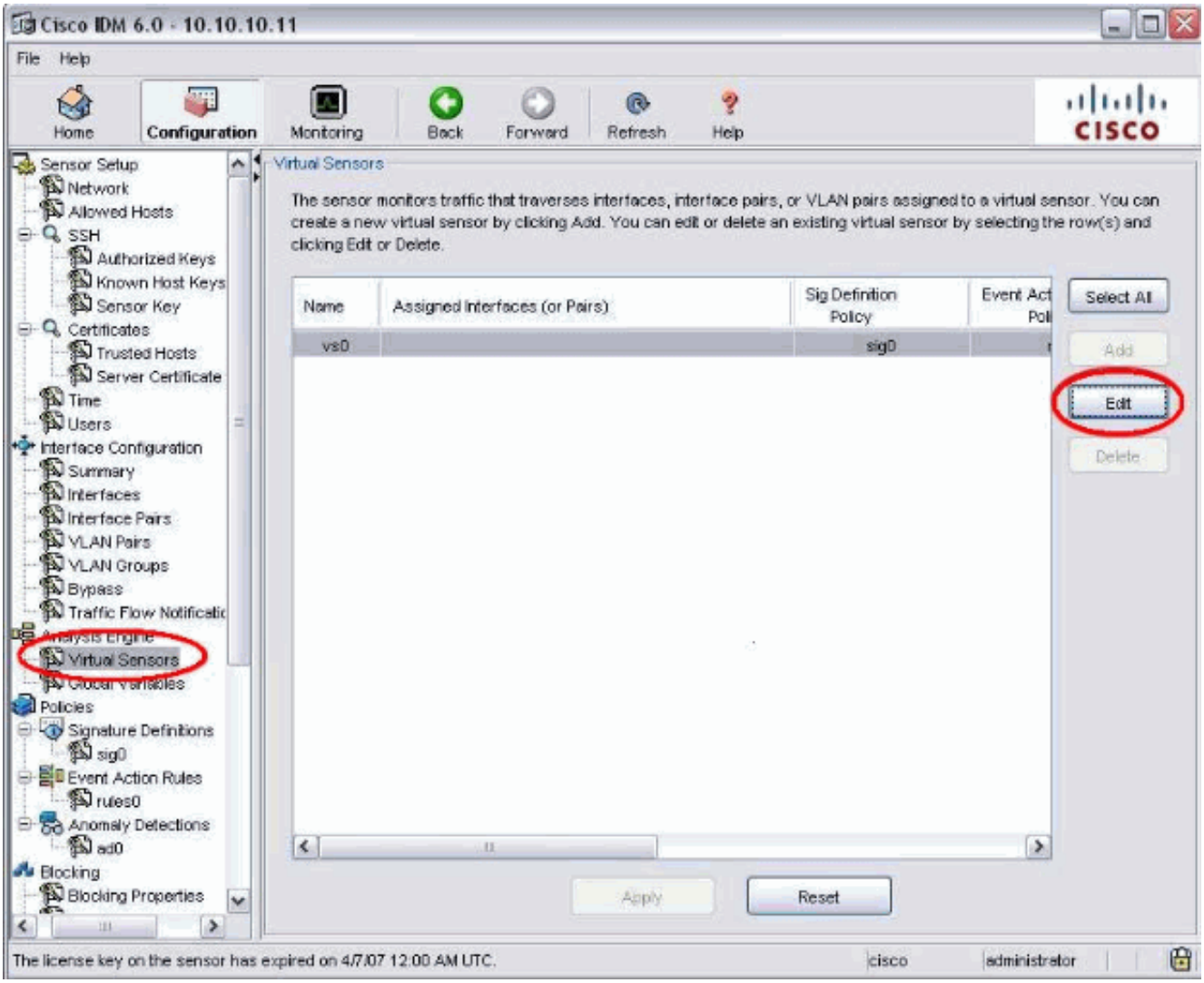
7. Ga naar **Configuration > Interface Configuration > Interface Parks** en klik op **Add** om het inline paar te
maken.



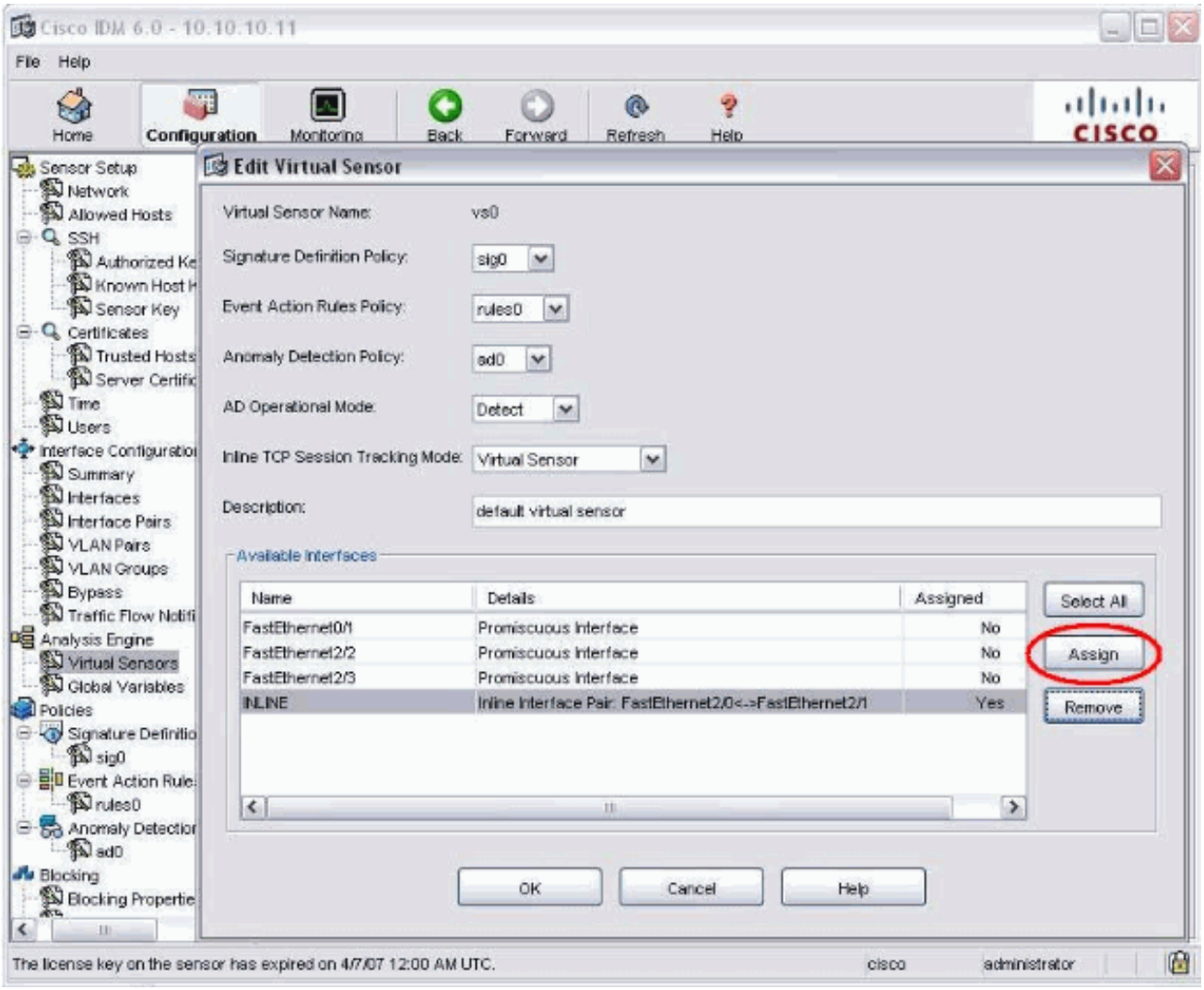
8. Bekijk de samenvatting van de configuratie van het inline paar en pas deze toe.



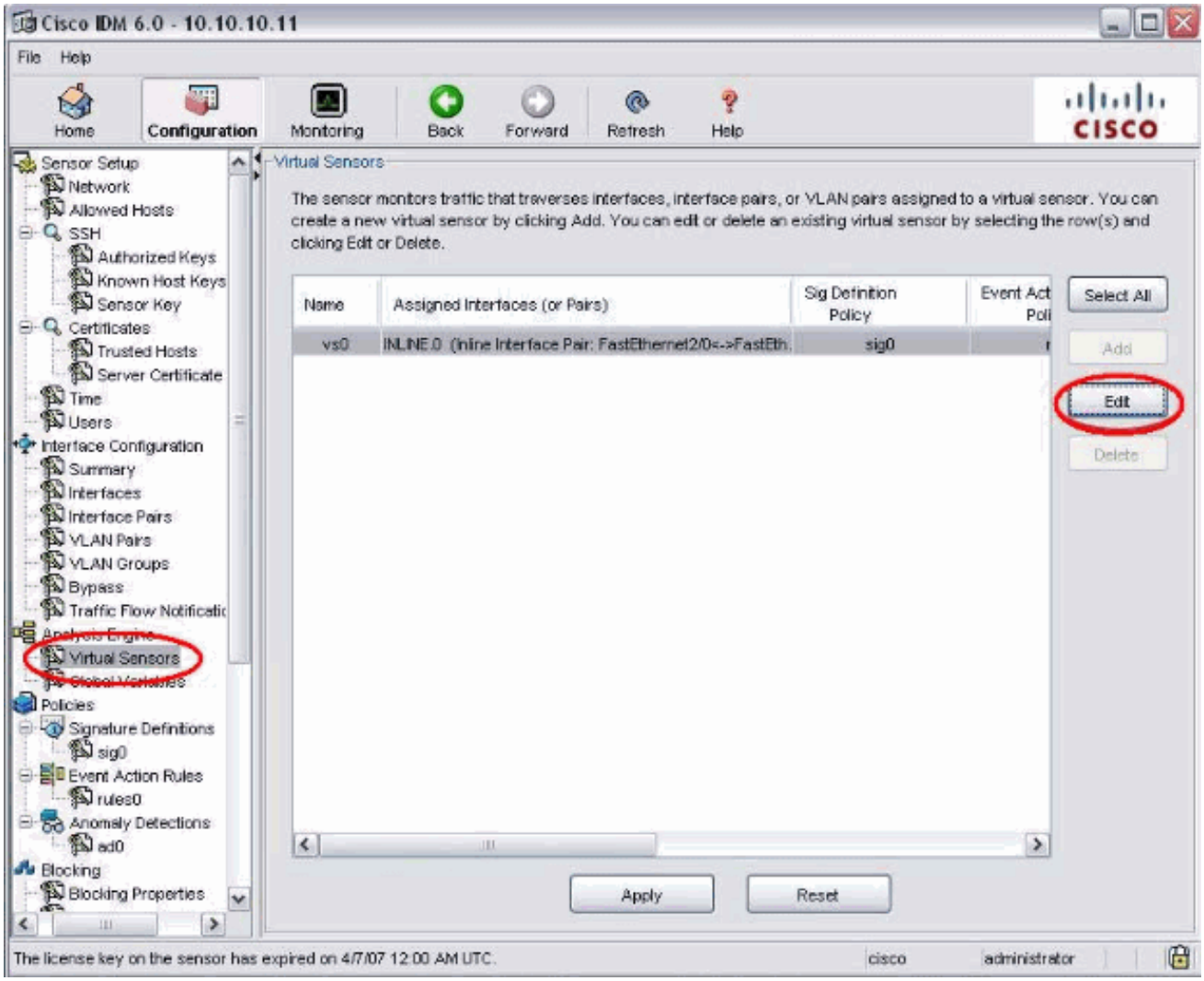
9. Ga naar **Configuration > Analysis Engine > Virtual Sensor** en klik op **Bewerken** om de nieuwe virtuele sensor te
maken.



10. Wijs de **INLINE-paar** toe aan de virtuele sensor vs0.



11. Bekijk de samenvatting van de toegewezen virtuele sensorinformatie.



Configureer de switch voor IDSM-2 in inline modus

Raadpleeg het gedeelte Catalyst Series 6500 switch voor IDSM-2 in het gedeelte Inline modus van IDSM-2 configureren om de schakelaar voor IDSM-2 inline modus te configureren.

Problemen oplossen

Probleem

Als IPS mislukt en inline wordt geconfigureerd falen de interfaces open (verkeer blijft doorlopen) of gesloten (verkeer wordt laten vallen).

Oplossing

U kunt IPS in een openstaande toestand configureren. Dus als IPS faalt zal het het verkeer blijven doorgeven maar het zal het verkeer niet controleren.

Gerelateerde informatie

- Cisco ASA 5500 Series adaptieve security applicaties

- Cisco-inbraakpreventiesysteem
- Cisco IPS 4200 Series sensoren
- Technische ondersteuning en documentatie – Cisco Systems