IPS 6.X und höher/IDSM2: Inline-Schnittstellenpaarmodus - IDM-Konfigurationsbeispiel

Inhalt

Einführung

Bei Betrieb im Inline-Schnittstellenpaarmodus wird das Intrusion Prevention System (IPS) direkt in den Datenverkehrsfluss integriert und beeinflusst die Paketweiterleitungsraten, was diese bei Hinzufügen von Latenz verlangsamt. So kann der Sensor Angriffe stoppen, sodass schädlicher Datenverkehr verworfen wird, bevor er das gewünschte Ziel erreicht, und so einen Schutzdienst bereitstellt. Die Informationen zur Inline-Geräteverarbeitung werden nicht nur auf Layer 3 und 4 analysiert, sondern auch Inhalt und Nutzlast der Pakete für komplexere, eingebettete Angriffe (Layer 3 bis 7). Diese tiefer gehende Analyse ermöglicht dem System, Angriffe zu identifizieren und zu stoppen bzw. zu blockieren, die normalerweise über ein herkömmliches Firewall-Gerät erfolgen.

Im Inline-Schnittstellenpaarmodus wird ein Paket über die erste Schnittstelle des Paars auf dem Sensor und über die zweite Schnittstelle des Paars empfangen. Das Paket wird an die zweite Schnittstelle des Paars gesendet, es sei denn, das Paket wird abgelehnt oder durch eine Signatur geändert.

Hinweis: Sie können AIM-IPS und AIP-SSM für den Betrieb inline konfigurieren, obwohl diese Module nur eine Sensorschnittstelle haben.

Hinweis: Wenn die gepaarten Schnittstellen mit demselben Switch verbunden sind, sollten Sie sie auf dem Switch als Access-Ports mit unterschiedlichen Zugriffs-VLANs für die beiden Ports

konfigurieren. Andernfalls fließt der Datenverkehr nicht über die Inline-Schnittstelle.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco IPS Sensor, der die Befehlszeilenschnittstelle 6.0 und den Intrusion Prevention System Device Manager (IDM) 6.0 verwendet.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Zugehörige Produkte

Die Informationen in diesem Dokument gelten auch für das Intrusion Detection System (IDSM-2) Services Module.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Konfiguration von Inline-Schnittstellenpaaren

Verwenden Sie den Befehl **inline-interface *name* im Dienstschnittstellenuntermodus, um Inline-Schnittstellenpaare zu erstellen.**

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Hinweis: AIP-SSM ist für den Inline-Schnittstellenmodus von der Cisco ASA-CLI und nicht von der Cisco IPS-CLI konfiguriert.

Diese Optionen gelten für:

- *Name der **Inline-Schnittstellen*** - Name des logischen Inline-Schnittstellenpaars**Hinweis:** An allen Backplane Sensing Interfaces auf allen Modulen (IDSM-2 NM-CIDS und AIP-SSM) ist **admin-state** aktiviert und geschützt (die Einstellung kann nicht geändert werden). Der **Admin-Status** hat keine Auswirkungen (und ist geschützt) auf die Command-and-Control-Schnittstelle. Es betrifft nur Sensorschnittstellen. Die Command-and-Control-Schnittstelle muss nicht aktiviert werden, da sie nicht überwacht werden kann.

- **default**: Setzt den Wert auf die Standardeinstellung des Systems zurück.
- **description** - Ihre Beschreibung des Inline-Schnittstellenpaars
- **interface1** *interface_name* - Die erste Schnittstelle im Inline-Schnittstellenpaar
- **interface2** *interface_name* - Die zweite Schnittstelle im Inline-Schnittstellenpaar
- **no** - Entfernt eine Eingabe- oder Auswahleinstellung
- **Admin-State {enabled, | disabled}** - Der Status der administrativen Verbindung der Schnittstelle, unabhängig davon, ob die Schnittstelle aktiviert oder deaktiviert ist.

CLI-Konfiguration

Gehen Sie wie folgt vor, um die Einstellungen für das Inline-VLAN-Paar auf dem Sensor zu konfigurieren:

1. Melden Sie sich bei der CLI mit einem Konto an, das über Administratorrechte verfügt.
2. Wechseln Sie in den Schnittstellenuntermodus:
```
sensor#configure terminal
sensor(config)#service interface
sensor(config-int)#
```
3. Überprüfen Sie, ob Inline-Schnittstellen vorhanden sind. Der Subschnittstellentyp sollte `none` lesen, wenn keine Inline-Schnittstellen konfiguriert wurden:
```
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. Nennen Sie das Inline-Paar:

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

5. Anzeigen der Liste der verfügbaren Schnittstellen:

```
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. Konfigurieren Sie zwei Schnittstellen in einem Paar:

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



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

Sie müssen die Schnittstelle einem virtuellen Sensor zuweisen und aktivieren, bevor sie den Datenverkehr überwachen kann. Weitere Informationen finden Sie in Schritt 10.

7. Fügen Sie eine Beschreibung dieser Schnittstelle hinzu:

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

8. Wiederholen Sie die Schritte 4 bis 7 für alle anderen Schnittstellen, die Sie für Inline-Schnittstellenpaare konfigurieren möchten.
9. Überprüfen Sie die Einstellungen:

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

10. Aktivieren Sie die Schnittstellen, die dem Schnittstellenpaar zugewiesen sind:

```
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. Überprüfen Sie, ob die Schnittstellen aktiviert sind:

```
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--
```

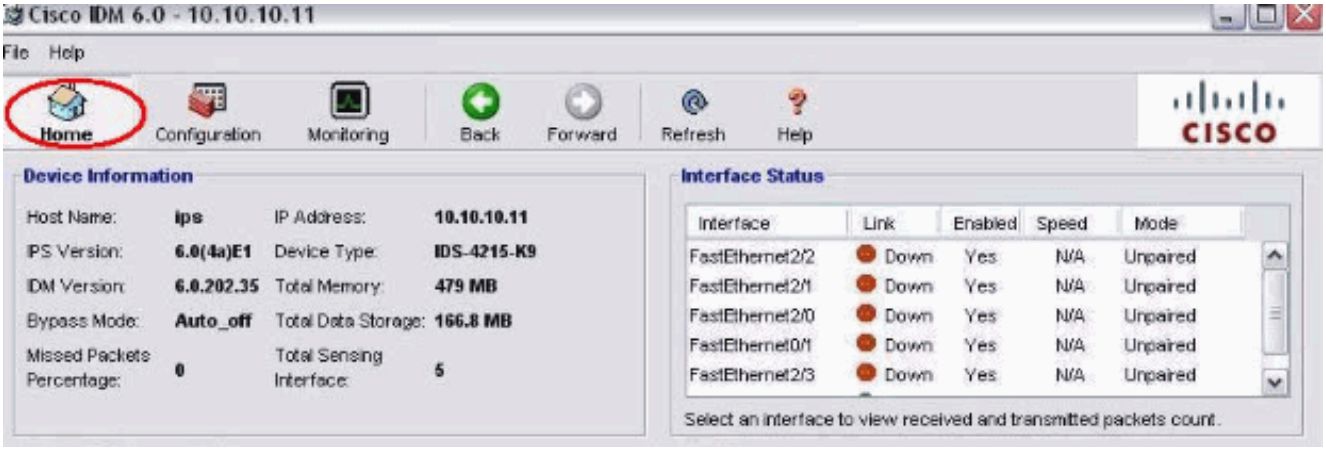
12. Geben Sie diesen Befehl ein, um ein Inline-Schnittstellenpaar zu löschen und die Schnittstellen in den Promiscuous-Modus zurückzugeben:
    ```
    sensor(config-int)#no inline-interfaces PAIR1
    ```

    Sie müssen auch das Inline-Schnittstellenpaar aus dem virtuellen Sensor löschen, dem es zugewiesen ist.
13. Überprüfen Sie, ob das Inline-Schnittstellenpaar gelöscht wurde:
    ```
    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. Exit Interface Configuration-Submodus:
    ```
    sensor(config-int)#exit
    Apply Changes:?[yes]:
    ```
15. Drücken Sie die **Eingabetaste**, um die Änderungen anzuwenden, oder geben Sie **no ein**, um sie zu verwerfen.

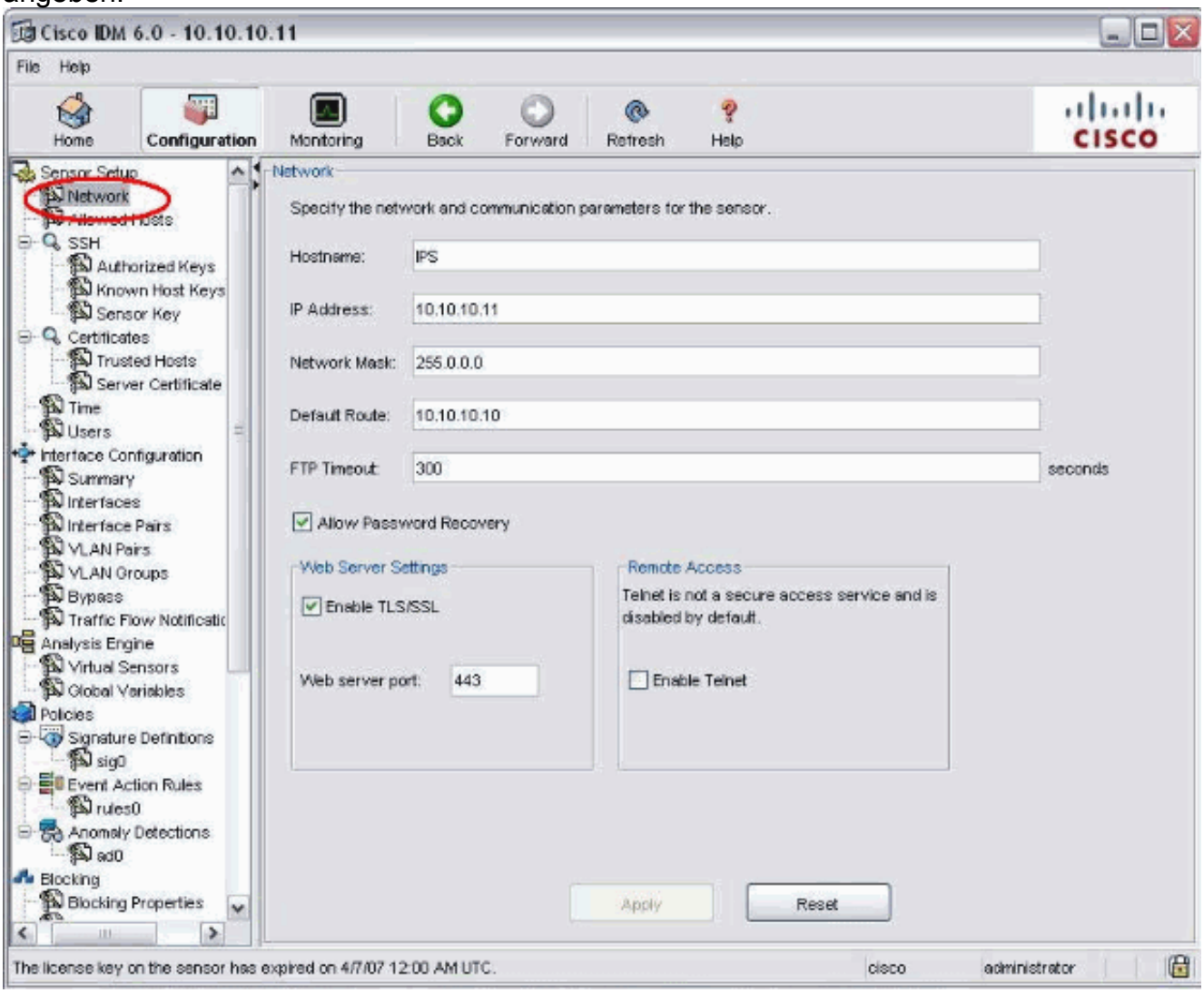
IDM-Konfiguration

Gehen Sie wie folgt vor, um die Inline-VLAN-Paareinstellungen auf dem Sensor mithilfe des IDM zu konfigurieren:

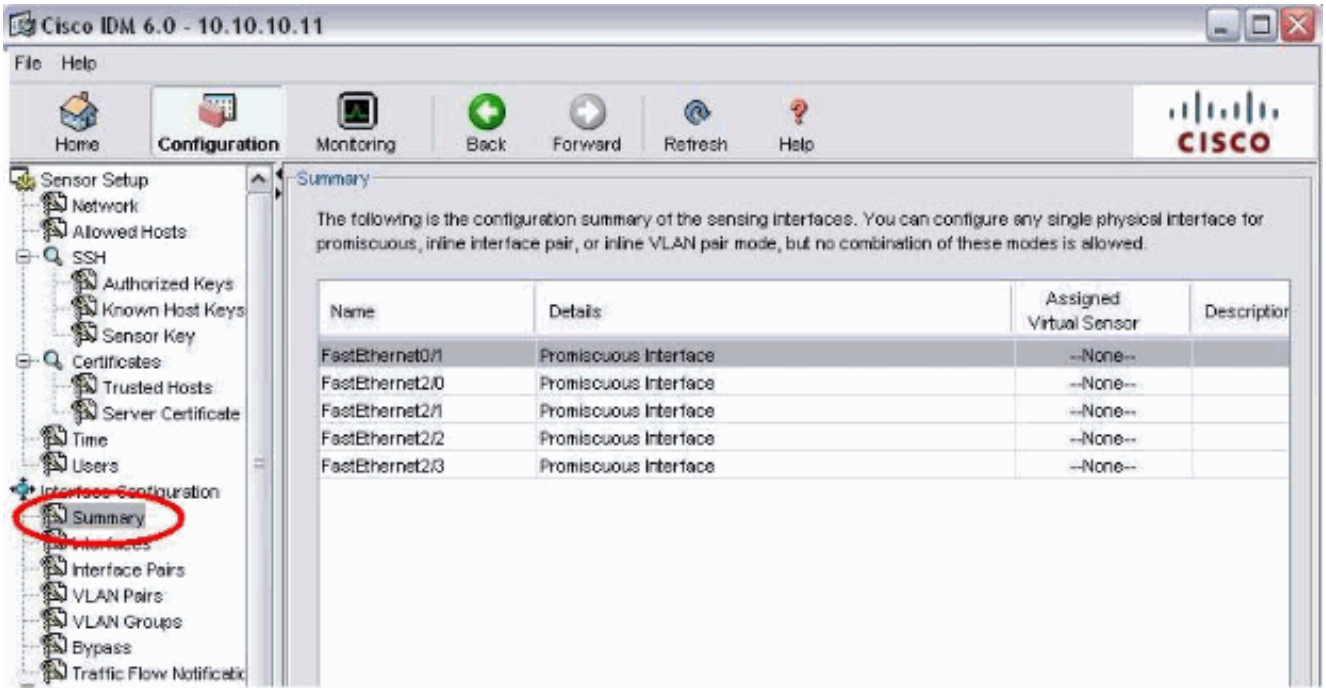
1. Öffnen Sie Ihren Browser, und geben Sie **https://<Management_IP_Address_of_IPS>** ein, um auf das IDM auf dem IPS zuzugreifen.
2. Klicken Sie auf **IDM-Launcher herunterladen** und **IDM starten**, um das Installationsprogramm für die Anwendung herunterzuladen.
3. Rufen Sie die Startseite auf, um Geräteinformationen wie Hostname, IP-Adresse, Version und Modell
   anzuzeigen.



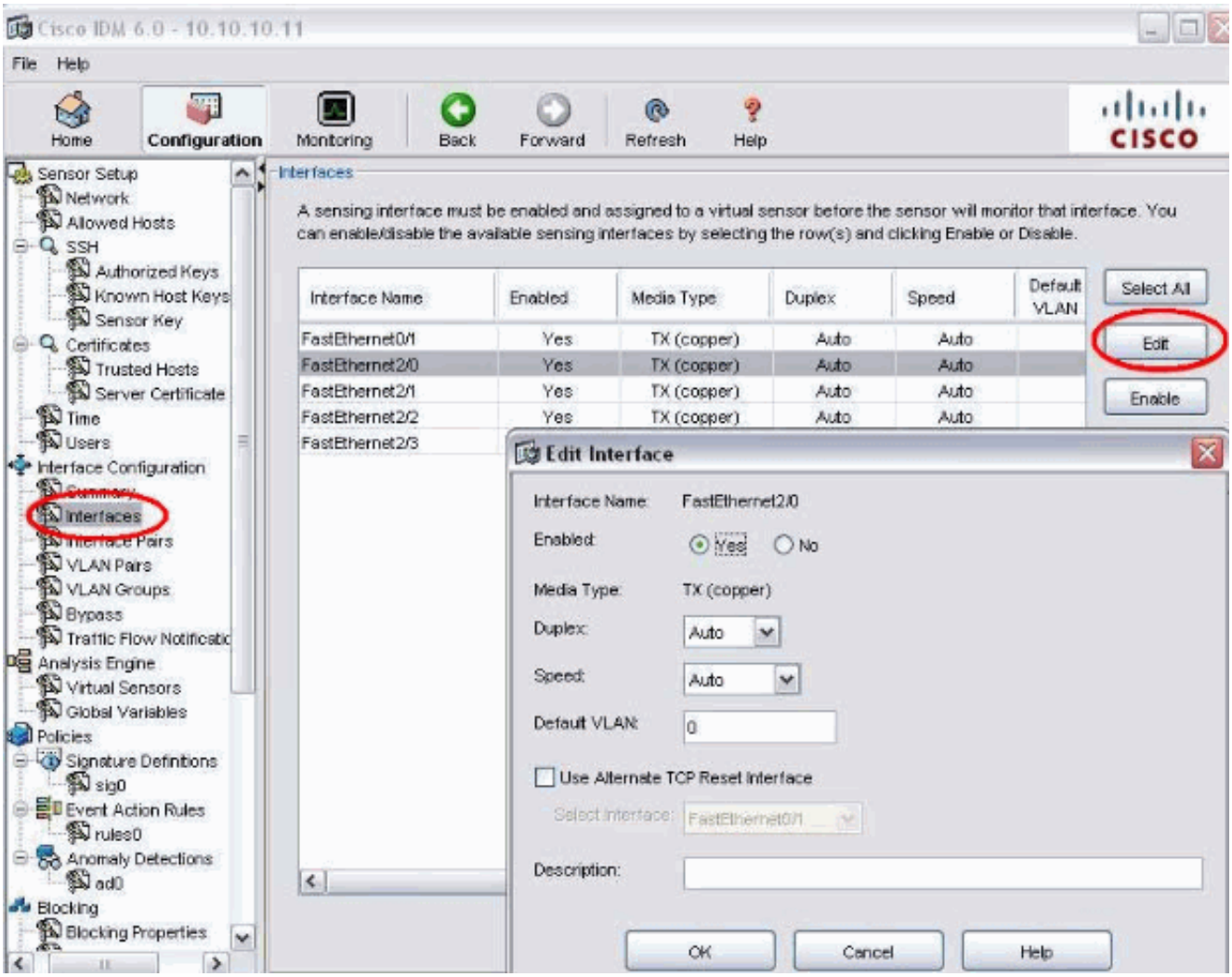
4. Gehen Sie zu **Konfiguration > Sensor Setup**, und klicken Sie auf **Netzwerk**. Hier können Sie den Hostnamen, die IP-Adresse und die Standardroute angeben.



5. Gehen Sie zu **Konfiguration > Schnittstellenkonfiguration**, und klicken Sie auf **Zusammenfassung**.Diese Seite zeigt die Konfigurationsübersicht der Sensorschnittstelle:

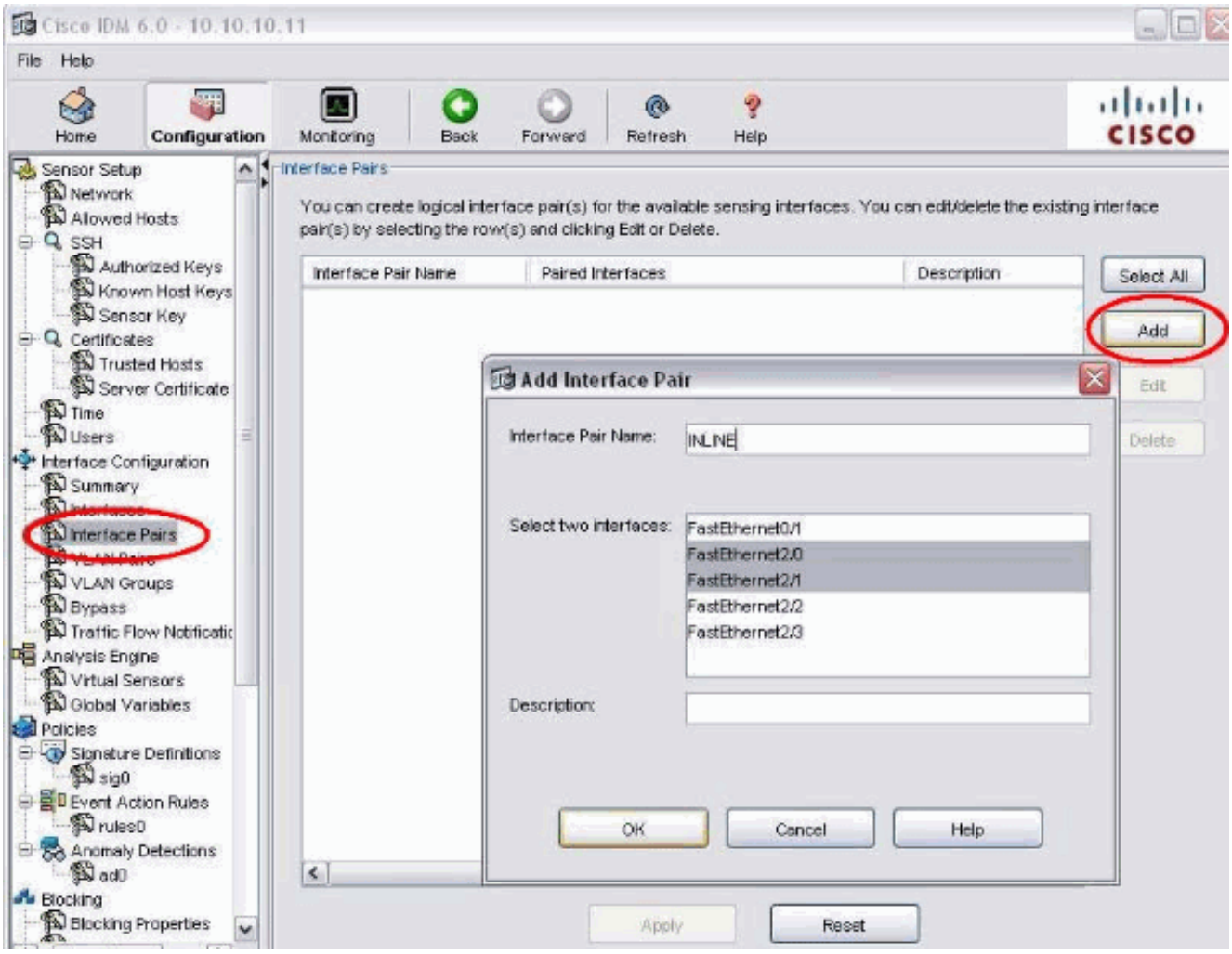


6. Gehen Sie zu **Konfiguration > Schnittstellenkonfiguration > Schnittstellen**, und wählen Sie den Schnittstellennamen aus. Klicken Sie anschließend auf **Aktivieren**, um die Sensorschnittstelle zu aktivieren. Konfigurieren Sie außerdem die Informationen zu Duplex, Geschwindigkeit und
VLAN.

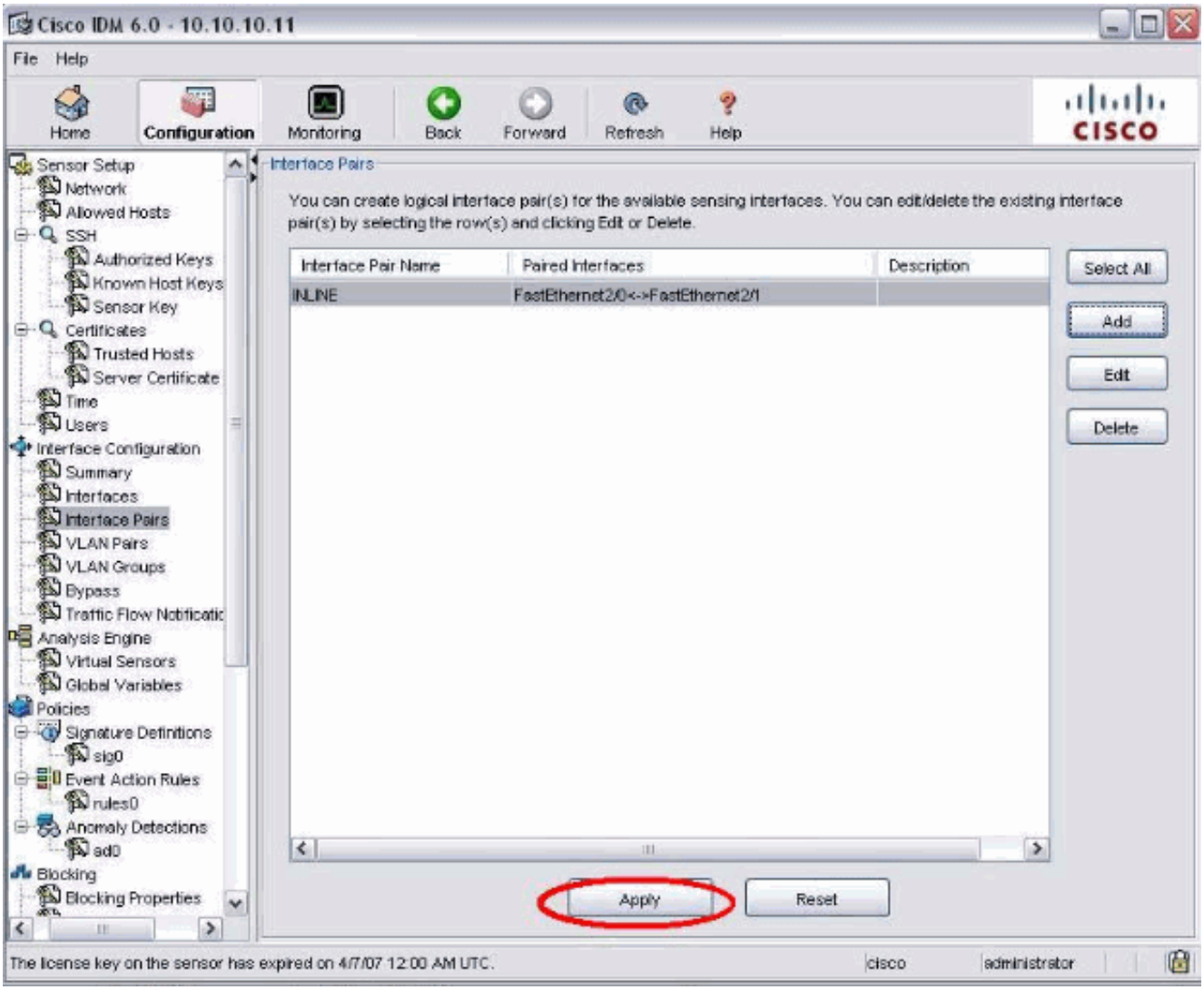


7. Gehen Sie zu **Konfiguration > Schnittstellenkonfiguration > Schnittstellenkombinationen,** und klicken Sie auf **Hinzufügen**, um das Inline-Paar zu

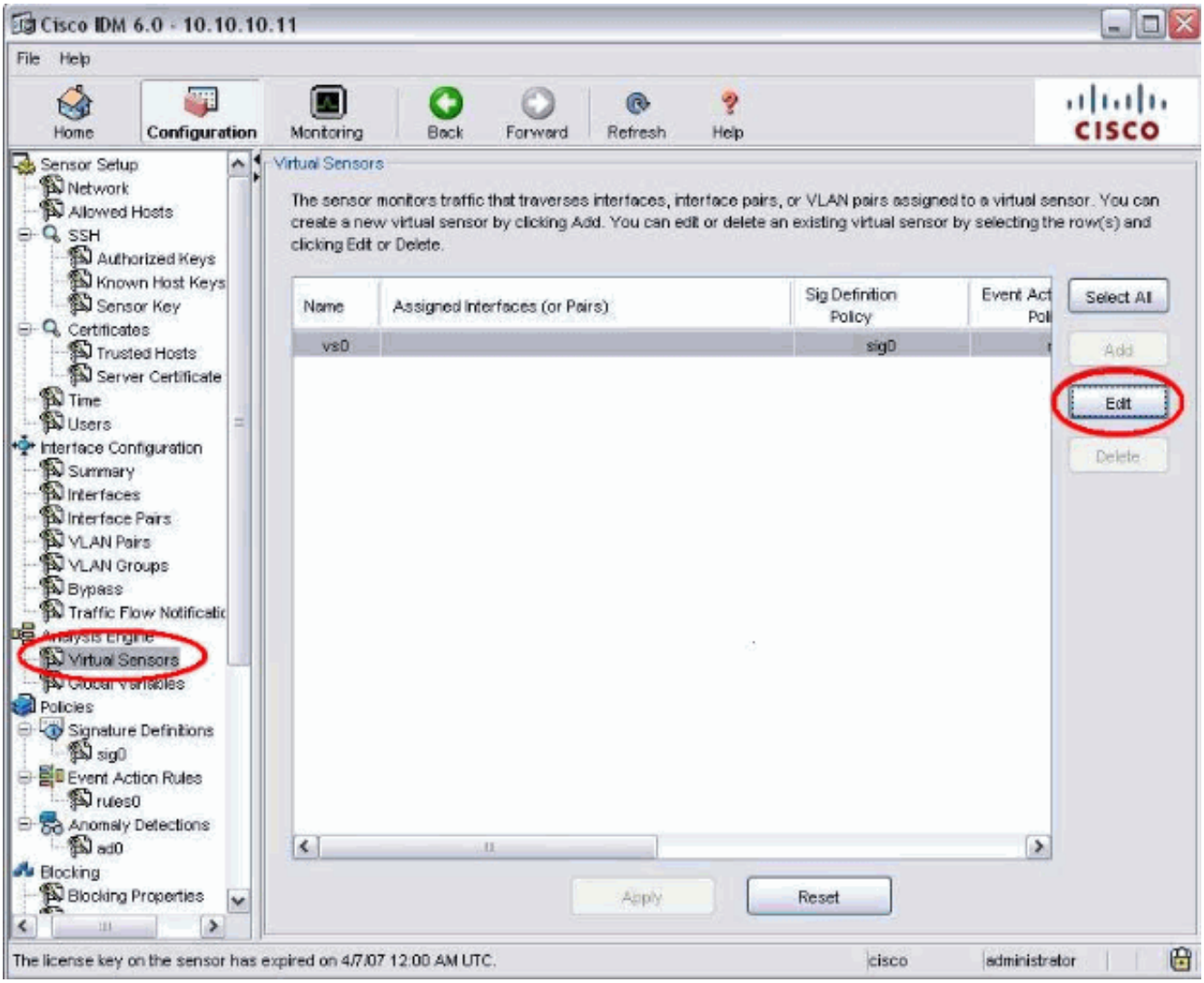
erstellen.



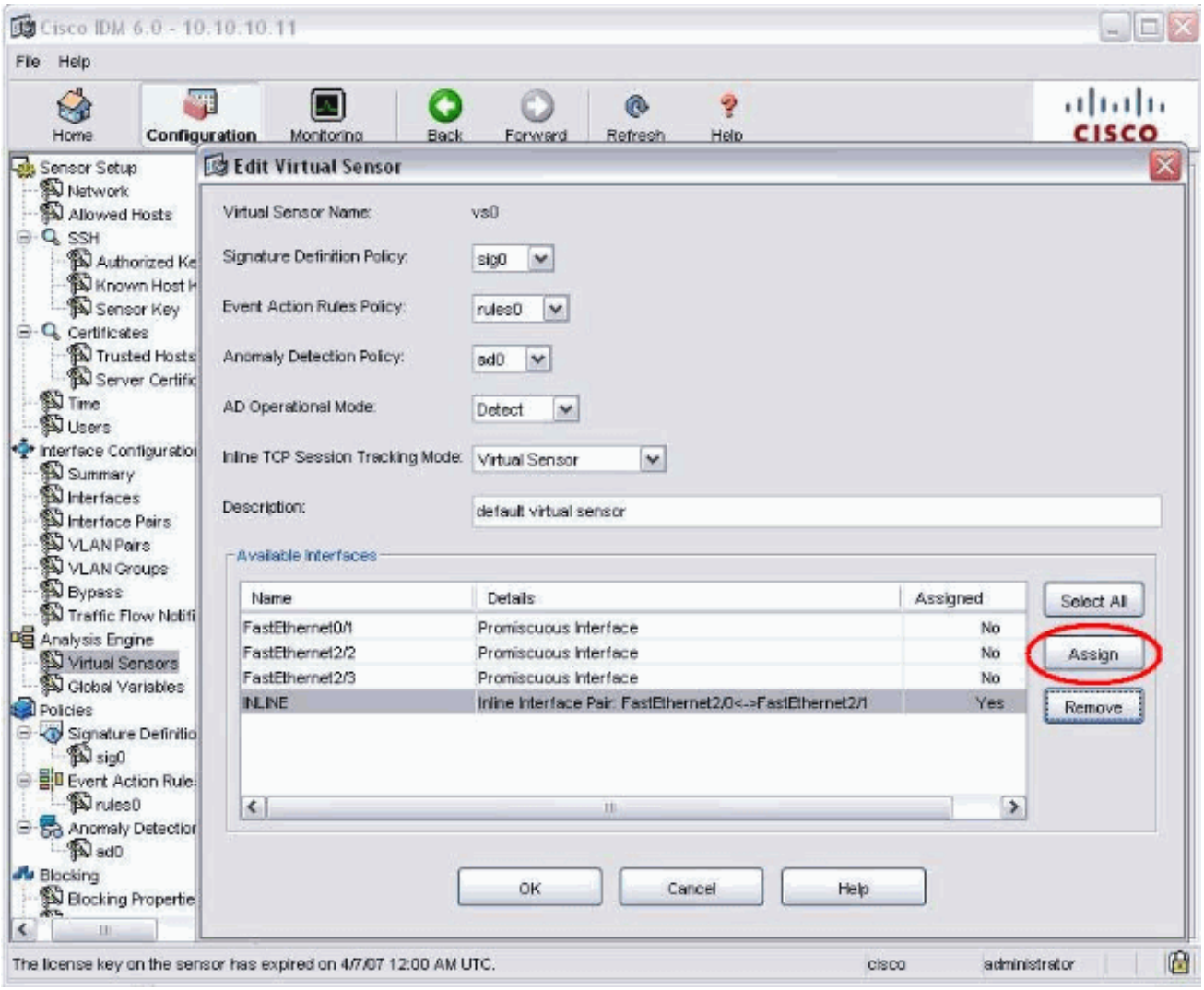
8. Zeigen Sie die Zusammenfassung der Inline-Paarkonfiguration an, und wenden Sie sie an.



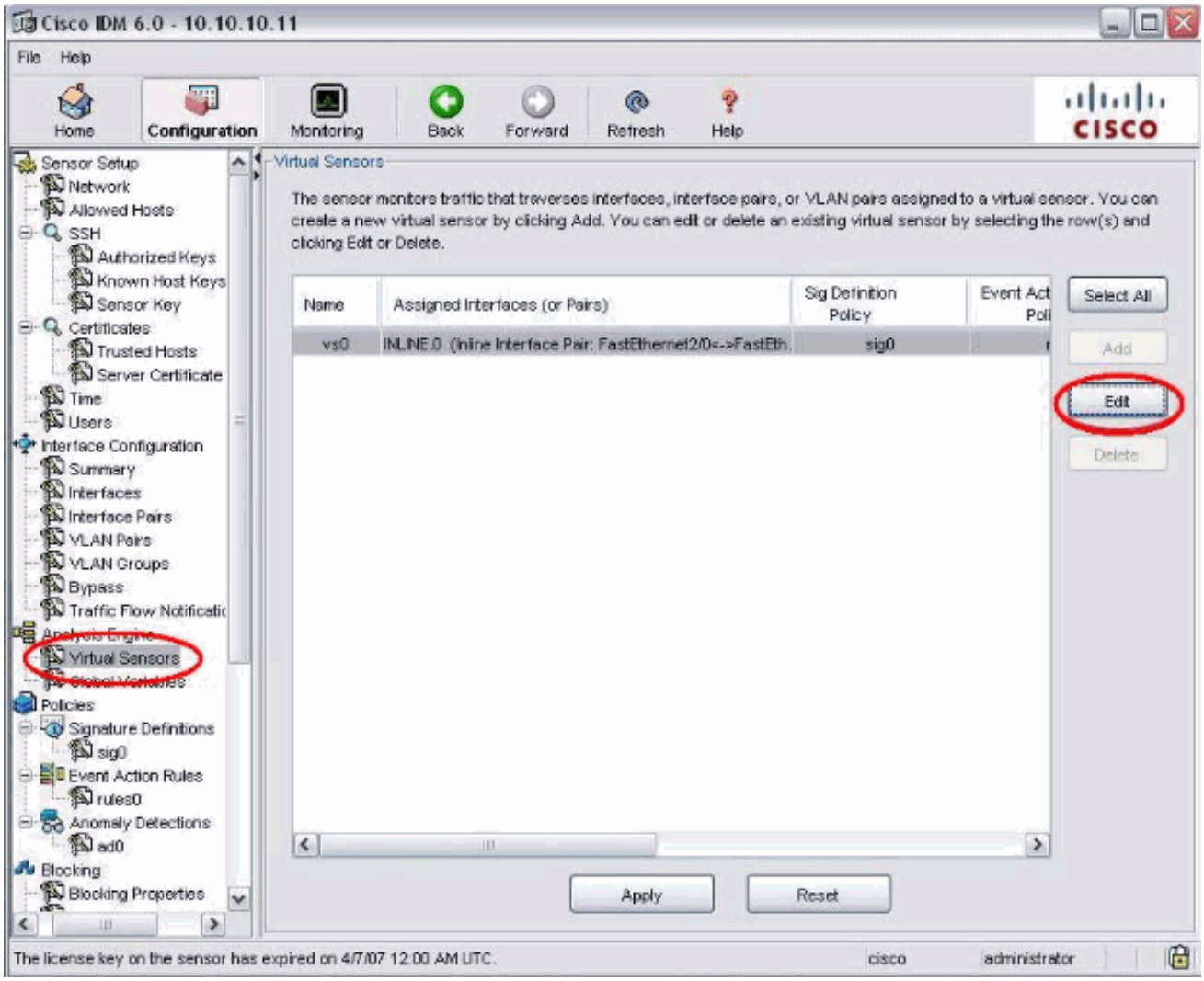
9. Gehen Sie zu **Configuration > Analysis Engine > Virtual Sensor**, und klicken Sie auf **Edit**, um den neuen virtuellen Sensor zu
erstellen.



10. Weisen Sie das Inline-Paar **INLINE** dem virtuellen Sensor vs0 zu.



11. Zeigen Sie die Zusammenfassung der zugewiesenen Informationen für virtuelle Sensoren an.



Konfigurieren des Switches für IDSM-2 im Inline-Modus

Im Abschnitt Konfiguration des Catalyst Switch der Serie 6500 für IDSM-2 im Inline-Modus unter Konfigurieren von IDSM-2 können Sie den Switch für den Inline-Modus IDSM-2 konfigurieren.

Fehlerbehebung

Problem

Wenn das IPS ausfällt und inline konfiguriert wird, können die Schnittstellen nicht geöffnet (Datenverkehr geht weiter über) oder geschlossen (Datenverkehr wird verworfen) werden.

Lösung

Sie können IPS im Fail-Open-Zustand konfigurieren. Wenn das IPS ausfällt, wird der Datenverkehr weiterhin weitergeleitet, der Datenverkehr wird jedoch nicht überwacht.

Zugehörige Informationen

- Cisco Adaptive Security Appliances der Serie ASA 5500

- Cisco Intrusion Prevention System
- Cisco Sensoren der Serie IPS 4200
- Technischer Support und Dokumentation - Cisco Systems