

IPS 5.X und höher/IDSM2: Inline-VLAN-Paarmodus mit CLI- und IDM-Konfigurationsbeispiel

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Zugehörige Produkte](#)

[Konventionen](#)

[Konfiguration der VACL-Erfassung](#)

[Konfiguration des Inline-VLAN-Paarmodus](#)

[CLI-Konfiguration](#)

[IDM-Konfiguration](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

[Einführung](#)

Die Zuordnung von VLANs in Paaren an einer physischen Schnittstelle wird als Inline-VLAN-Paarmodus bezeichnet. Pakete, die in einem der paarweise verbundenen VLANs empfangen werden, werden analysiert und an das andere VLAN im Paar weitergeleitet. Inline-VLAN-Paare werden auf allen Sensoren unterstützt, die mit Intrusion Prevention System (IPS) 5.1 kompatibel sind, mit Ausnahme von NM-CIDS, AIP-SSM-10 und AIP-SSM-20.

Der Inline-VLAN-Paarmodus ist ein aktiver Sensormodus, bei dem eine Sensorschnittstelle als 802.1q-Trunk-Port fungiert und der Sensor VLAN-Bridging zwischen VLAN-Paaren auf dem Trunk durchführt. Das bedeutet, dass sich der an die Sensorschnittstelle angeschlossene Switch im Trunk-Modus befinden muss.

Der Sensor prüft den Datenverkehr, den er in jedem VLAN in jedem Paar empfängt, und kann die Pakete entweder im anderen VLAN des Pairs weiterleiten oder das Paket verwerfen, wenn ein Eindringungsversuch erkannt wird. Sie können einen IPS-Sensor so konfigurieren, dass auf jeder Sensorschnittstelle gleichzeitig bis zu 255 VLAN-Paare überbrückt werden. Der Sensor ersetzt das VLAN-ID-Feld im 802.1q-Header jedes empfangenen Pakets durch die ID des Ausgangs-VLAN, auf dem der Sensor das Paket weiterleitet. Der Sensor verwirft alle Pakete, die auf VLANs empfangen werden, die nicht Inline-VLAN-Paaren zugewiesen sind.

Hinweis: Für IPS-4260 wird eine Fail-Open-Hardware-Umgehung nicht auf Inline-VLAN-Paaren unterstützt. Weitere Informationen finden Sie unter [Einschränkungen für die Hardware-Umgehung](#).

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf dem Cisco Intrusion Prevention System Sensor, der die Version 5.1 und höher 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 (IDS-2) Services Module.

Konventionen

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

Konfiguration der VACL-Erfassung

Informationen zum Senden von Datenverkehr an das IDS-2 auf dem Switch finden Sie im Abschnitt [Configuring VACL Capture \(VACL-Erfassung konfigurieren\) IDS-2](#).

Konfiguration des Inline-VLAN-Paarmodus

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

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

Verwenden Sie den Befehl `interface_name` für **physische Schnittstellen** im Dienstschnittstellenuntermodus, um Inline-VLAN-Paare mithilfe der CLI zu konfigurieren. Der Schnittstellename ist FastEthernet oder GigabitEthernet.

Diese Optionen gelten für:

- **Admin-State {enabled, | disabled}** - Der Status der administrativen Verbindung der Schnittstelle, unabhängig davon, ob die Schnittstelle aktiviert oder deaktiviert ist. **Hinweis:** An allen Backplane Sensing Interfaces auf allen Modulen (IDS-2 NM-CIDS und AIP-SSM) ist

der Admin-State aktiviert und geschützt (Sie können die Einstellung nicht ändern). Der Admin-Zustand 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.
- **duplex**: Die Duplexeinstellung der Schnittstelle.**auto** - Legt die Schnittstelle für die automatische Aushandlung von Duplex fest.**full** (Vollständig): Stellt die Schnittstelle auf Vollduplex ein.**half** (**halb**): Legt die Schnittstelle auf Halbduplex fest.**Hinweis**: Die Duplexoption ist auf allen Modulen geschützt.
- **no** - Entfernt eine Eingabe- oder Auswahleinstellung.
- **speed** (**Geschwindigkeit**): Die Geschwindigkeitseinstellung der Schnittstelle.**auto** (Automatisch): Stellt die Schnittstelle so ein, dass die Geschwindigkeit automatisch ausgehandelt wird.**10** - Legt die Schnittstelle auf 10 MB fest (nur für TX-Schnittstellen).**100** (**100**): Legt die Schnittstelle auf 100 MB fest (nur für TX-Schnittstellen).**1000** - Legt die Schnittstelle auf 1 GB fest (für Gigabit-Schnittstellen)**Hinweis**: Die Geschwindigkeitsoption ist auf allen Modulen geschützt.
- **subinterface-type**: Gibt an, dass es sich bei der Schnittstelle um eine Subschnittstelle handelt und welcher Subschnittstellentyp definiert ist.**inline-vlan-pair** - Ermöglicht es Ihnen, die Subschnittstelle als Inline-VLAN-Paar zu definieren.**none**: Keine Subschnittstellen definiert.
- **subinterface** - Definiert die Subschnittstelle als Inline-VLAN-Paar.**vlan1**: Das erste VLAN im Inline-VLAN-Paar.**vlan2**: Das zweite VLAN im Inline-VLAN-Paar.

CLI-Konfiguration

Gehen Sie wie folgt vor, um die Inline-VLAN-Paareinstellungen auf dem Sensor über die CLI zu konfigurieren:

1. Melden Sie sich mit einem Konto mit Administratorrechten bei der CLI an.
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" lauten, 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. Entfernen Sie alle Inline-Schnittstellen, die diese physische Schnittstelle verwenden:

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

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. Angeben einer Schnittstelle:

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

7. Aktivieren Sie den Admin-Status der Schnittstelle:

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

Die Schnittstelle muss dem virtuellen Sensor zugewiesen und aktiviert sein, um den Datenverkehr zu überwachen.

8. Fügen Sie eine Beschreibung dieser Schnittstelle hinzu:

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

9. Konfigurieren Sie die Duplexeinstellungen:

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

Diese Option ist für Module nicht verfügbar.

10. Konfigurieren Sie die Geschwindigkeit:

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

Diese Option ist für Module nicht verfügbar.

11. Einrichten des Inline-VLAN-Paars:

```
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. Fügen Sie eine Beschreibung für das Inline-VLAN-Paar hinzu:

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

13. Überprüfen Sie die Einstellungen für das Inline-VLAN-Paar:

```
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. Beenden Sie den Schnittstellenuntermodus:

```
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. Drücken Sie **die Eingabetaste**, um die Änderungen anzuwenden, oder geben Sie **no** ein, um sie zu verwerfen.

16. Wechseln Sie in den Konfigurationsmodus für virtuelle Sensoren:

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

17. Fügen Sie die Schnittstelle dem virtuellen Sensor hinzu:

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

18. Beenden Sie den Virtual-Sensor-Submodus:

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

19. Drücken Sie **die Eingabetaste**, um die Änderungen anzuwenden, oder geben Sie **no** ein, um sie zu verwerfen.

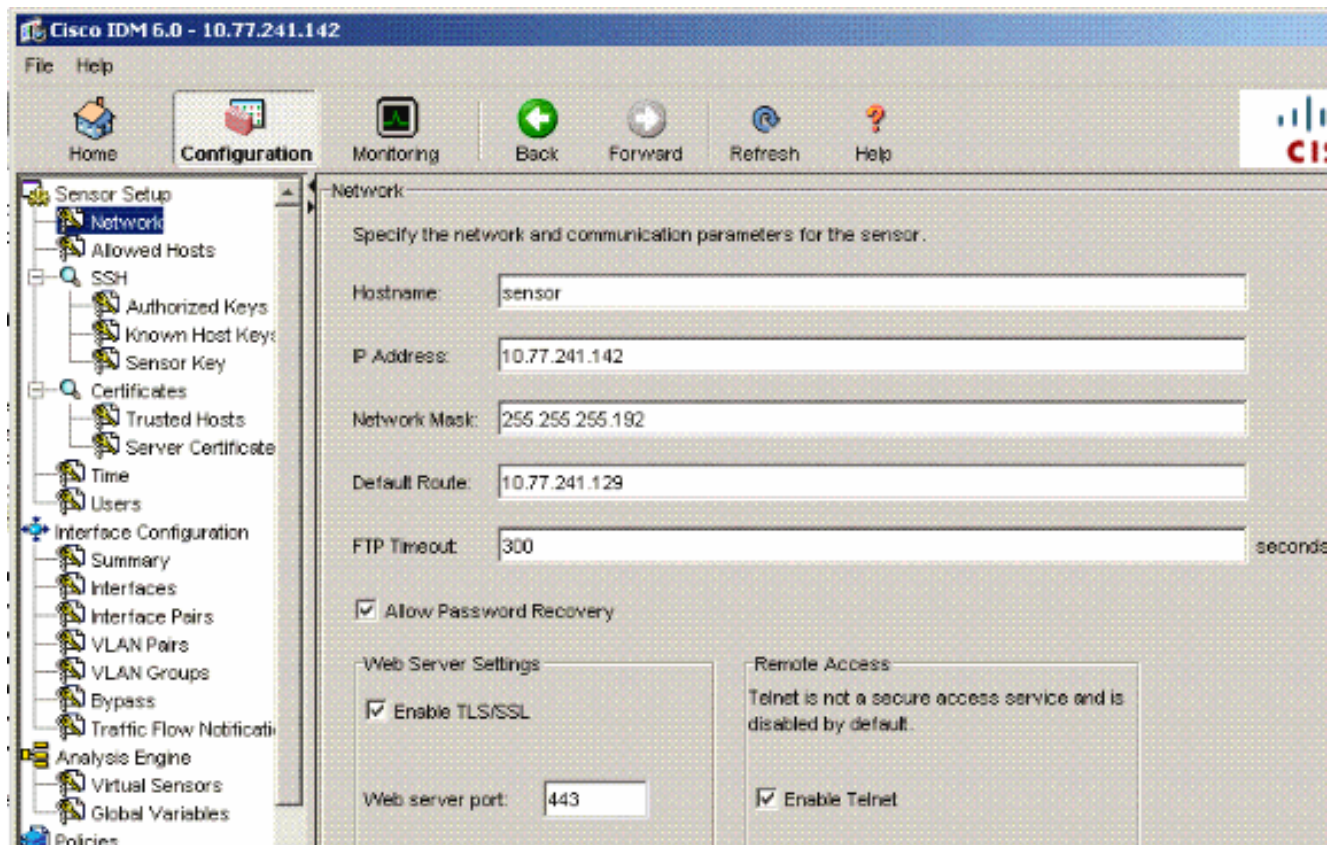
[IDM-Konfiguration](#)

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

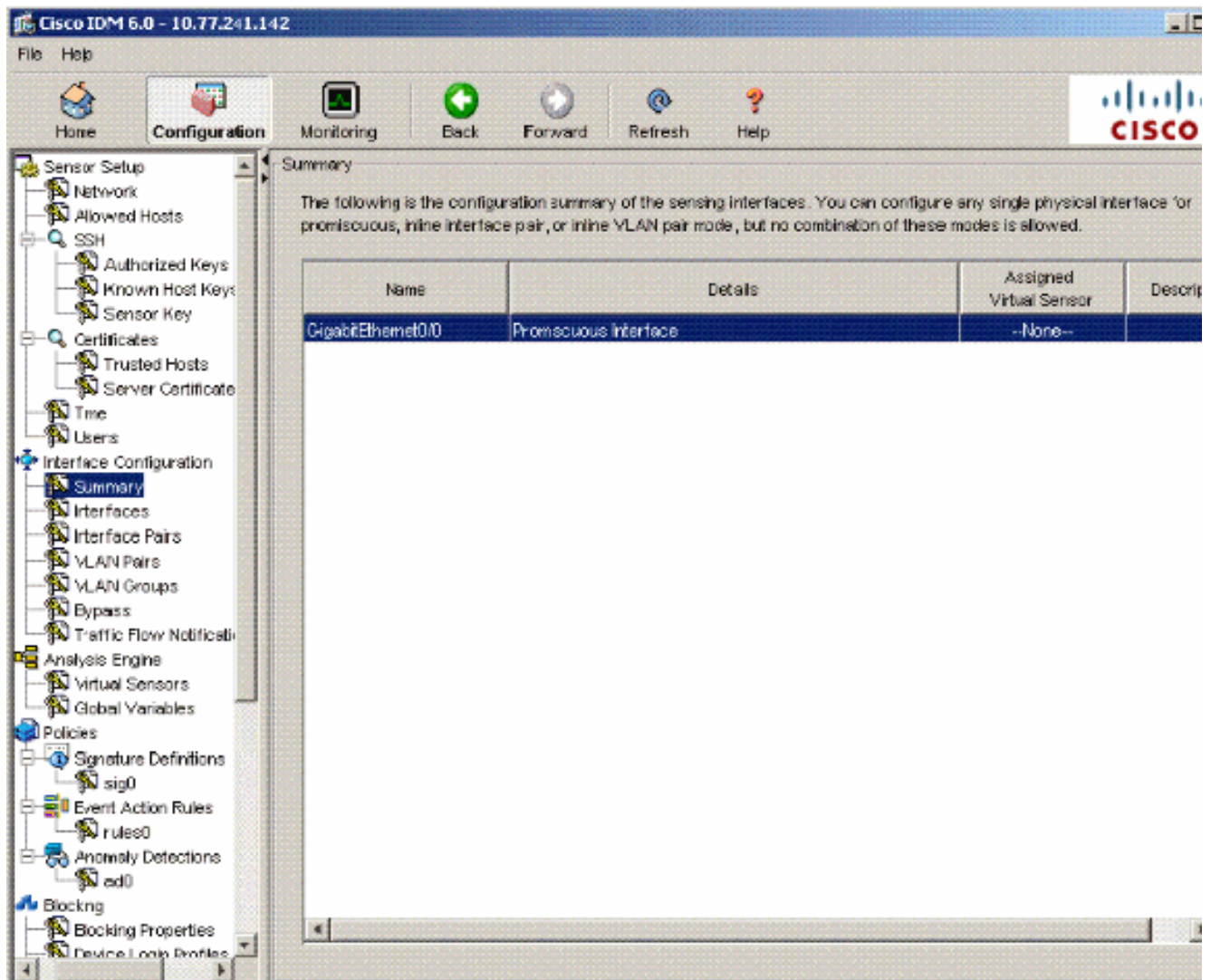
1. Öffnen Sie Ihren Browser, und geben Sie https://<Management_IP_Address_of_IPS> ein, um auf das IDM auf dem IPS zuzugreifen.
2. Klicken Sie auf **IDM Launcher herunterladen und IDM starten**, um das Installationsprogramm für die Anwendung herunterzuladen.
3. Rufen Sie die Startseite auf, um Geräteinformationen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



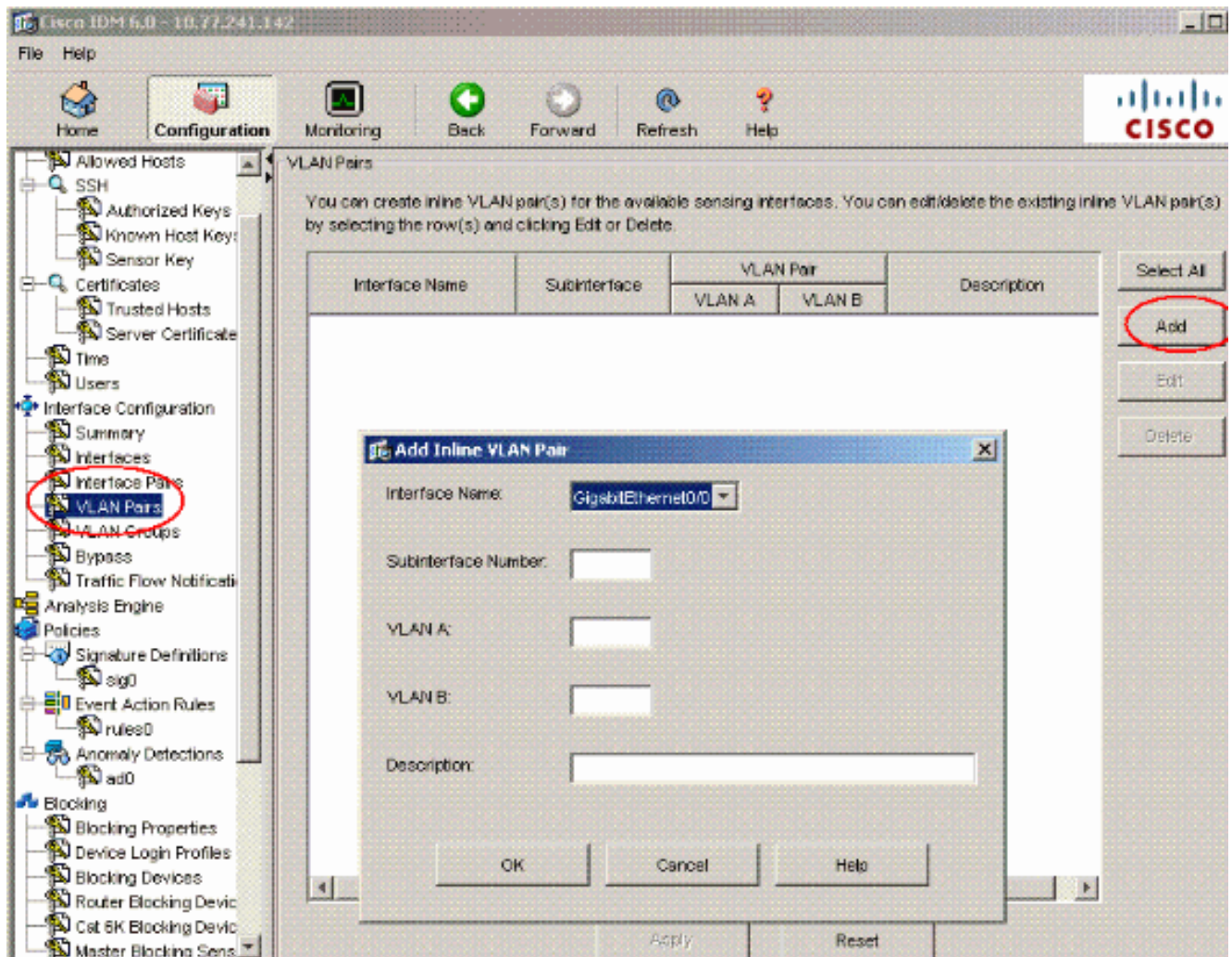
- Gehen Sie zu **Konfiguration > Schnittstellenkonfiguration > Schnittstellen**, und wählen Sie den Schnittstellennamen aus. Klicken Sie anschließend auf **Aktivieren**, um die Sensorschnittstelle zu aktivieren. Konfigurieren Sie außerdem die Informationen zu Duplex, Geschwindigkeit und VLAN.

The screenshot shows the Cisco IDM 6.0 configuration interface. The left sidebar contains a tree view with 'Interface Configuration' expanded, and 'Interfaces' selected. The main area displays a table of interfaces with the following data:

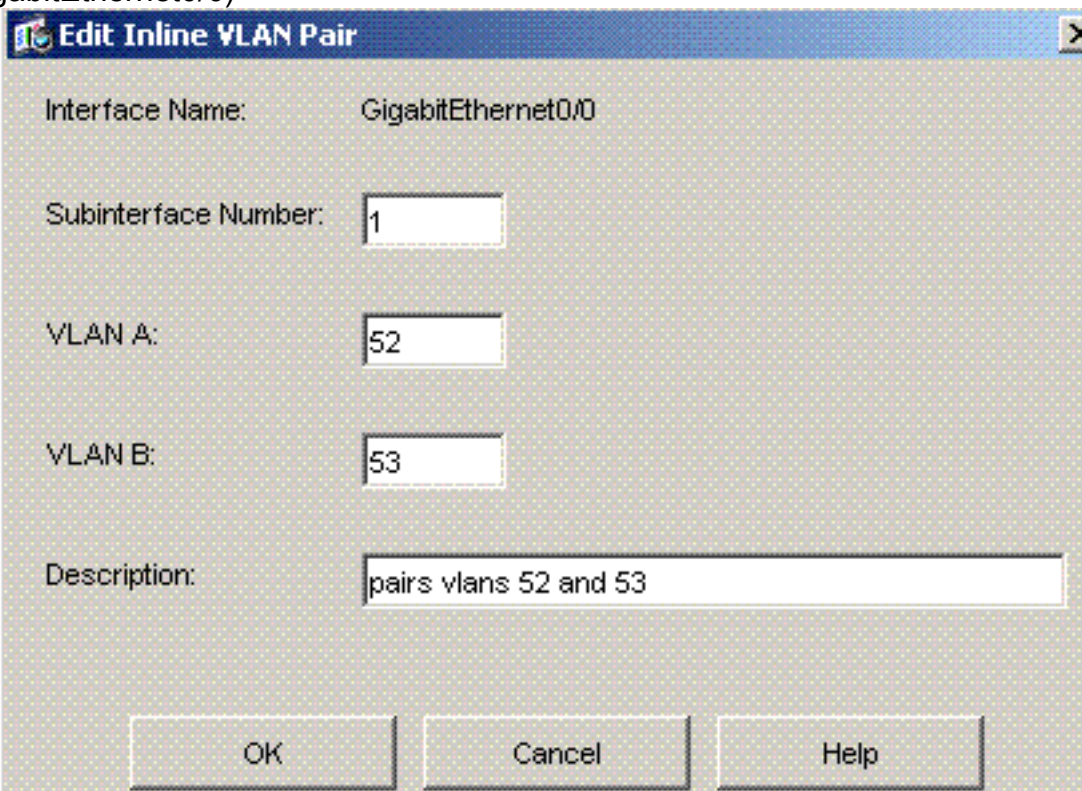
Interface Name	Enabled	Media Type	Duplex	Speed	Default VLAN
GigabitEthernet0/0	Yes	TX (copper)	Auto	Auto	

An 'Edit Interface' dialog box is open, showing the configuration for 'GigabitEthernet0/0'. The 'Enabled' field is set to 'Yes' (radio button selected). Other fields include 'Media Type: TX (copper)', 'Duplex: Auto', 'Speed: Auto', and 'Default VLAN: 0'. The 'Enable' button in the right sidebar is circled in red.

7. Gehen Sie zu **Konfiguration > Schnittstellenkonfiguration > VLAN-Paare**, und klicken Sie auf **Hinzufügen**, um Inline-VLAN-Paare zu erstellen.



8. Geben Sie die Subschnittstellennummer, VLAN A und VLAN B für die Sensorschnittstelle (GigabitEthernet0/0)



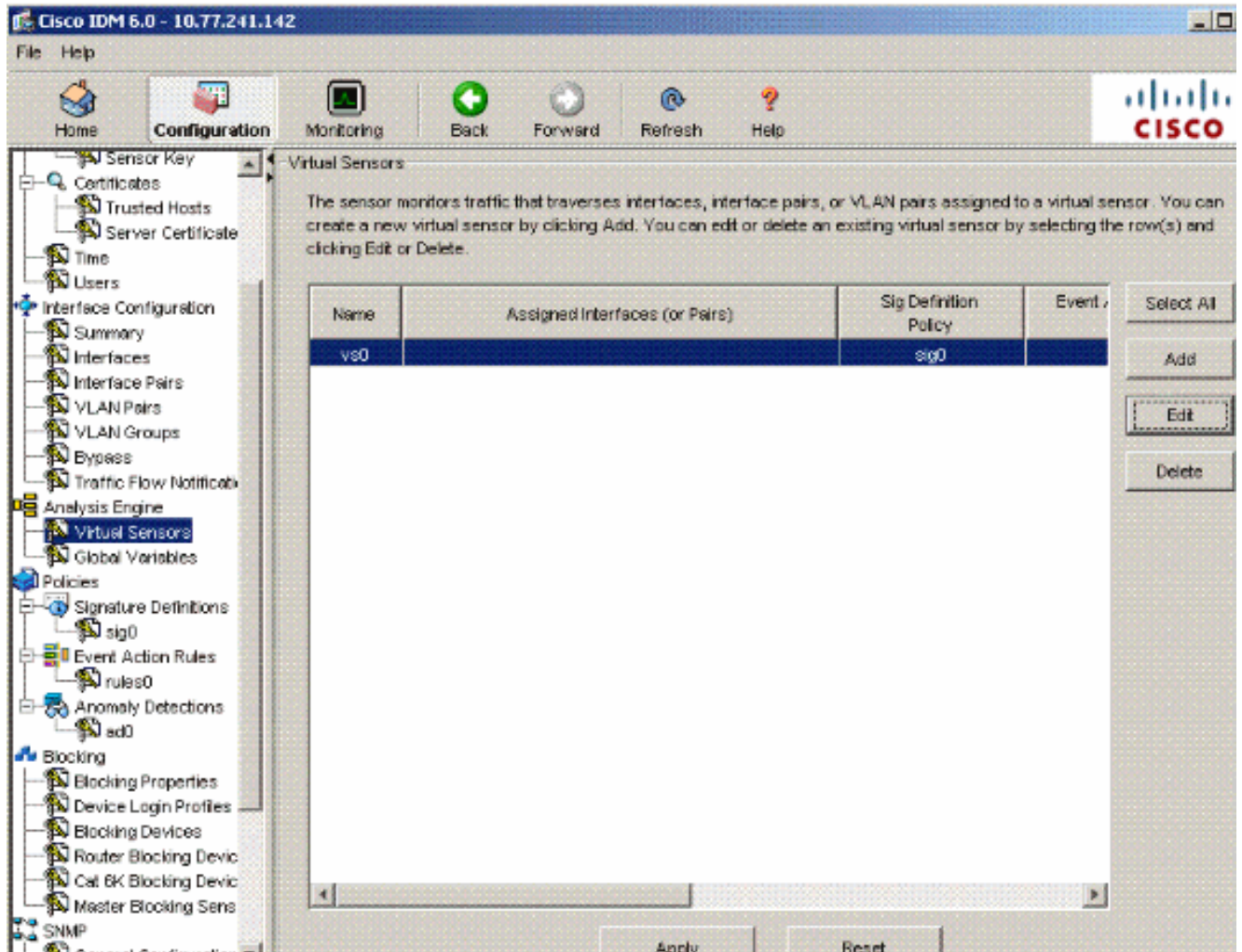
ein. Sie können die Zusammenfassung der Inline-VLAN-Parkonfiguration anzeigen.

The screenshot shows the Cisco IDM 6.0 web interface. The top navigation bar includes 'Home', 'Configuration', 'Monitoring', 'Back', 'Forward', 'Refresh', and 'Help'. The left sidebar contains a tree view with categories like 'Allowed Hosts', 'Certificates', 'Interface Configuration', 'Policies', and 'Blocking'. The 'VLAN Pairs' option is selected under 'Interface Configuration'. The main content area is titled 'VLAN Pairs' and contains a table with the following data:

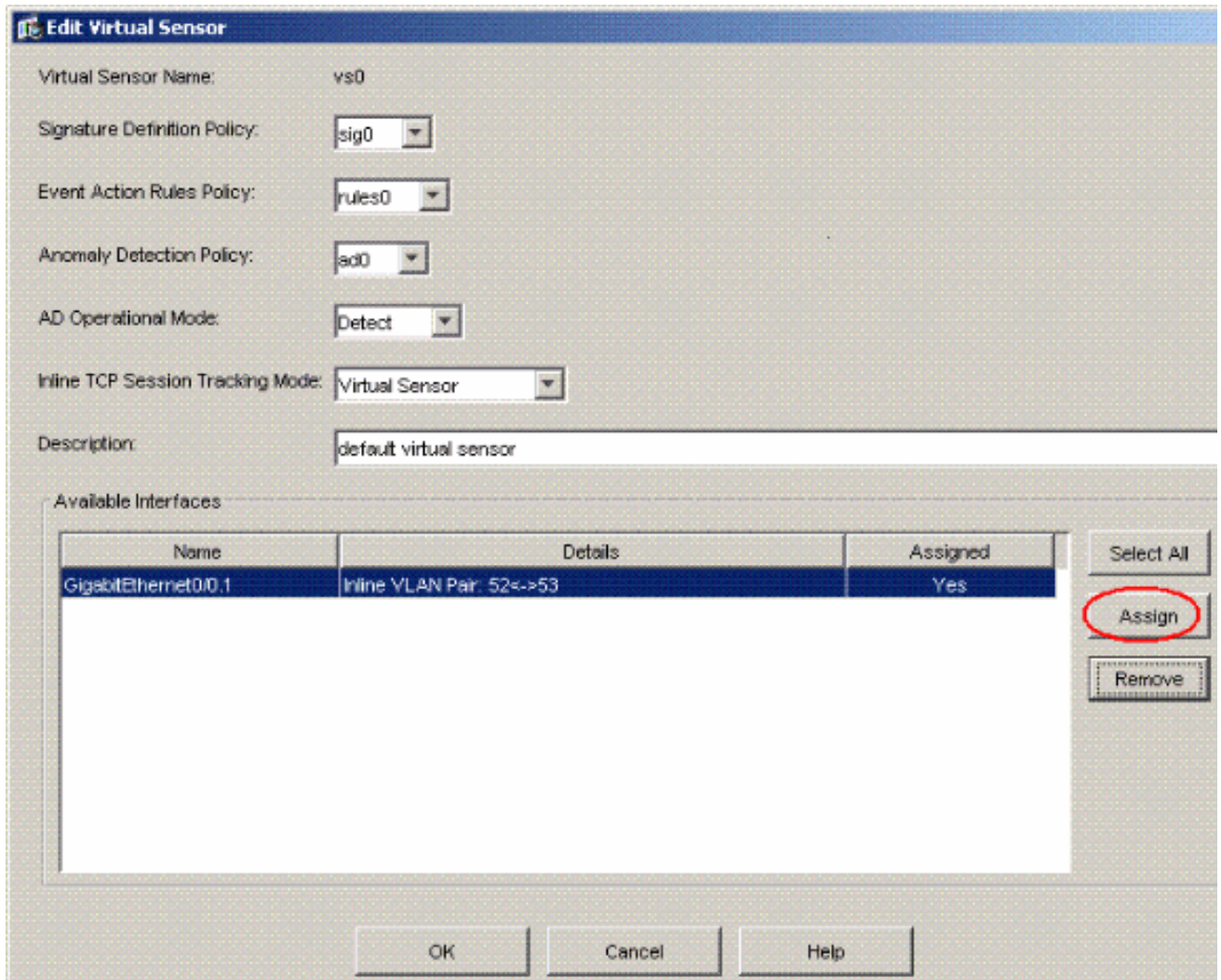
Interface Name	Subinterface	VLAN Pair		Description
		VLAN A	VLAN B	
GigabitEthernet0/0	1	52	53	pairs vlans 52 and 53

Below the table, there are 'Apply' and 'Reset' buttons. On the right side of the table, there are buttons for 'Select All', 'Add', 'Edit', and 'Delete'.

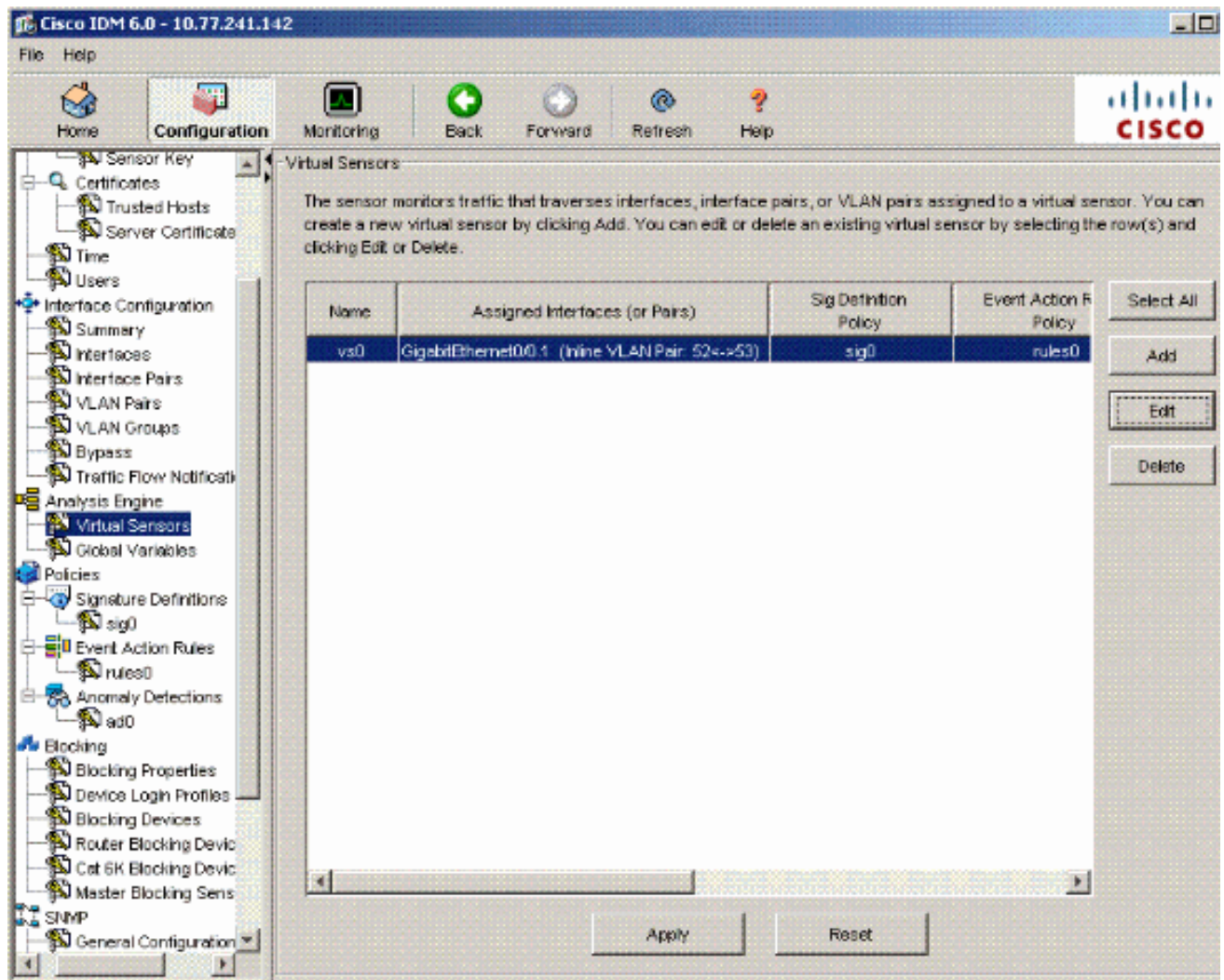
9. Gehen Sie zu **Configuration > Analysis Engine > Virtual Sensor**, und klicken Sie auf **Edit**, um den neuen virtuellen Sensor zu erstellen.



10. Weisen Sie dem virtuellen Sensor das Inline-VLAN-Paar 52 und 53 zu vs0.



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



Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

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](#)