IPS 5.X y later/IDSM2: Modo en línea de los pares del VLA N usando el ejemplo de configuración CLI y IDM

Contenido

Introducción

La asociación de VLAN por pares en una interfaz física se conoce como modo de pares VLAN en línea. Los paquetes recibidos en uno de los VLAN emparejados se analizan y se reenvían al otro VLAN en la pareja. Los pares en línea del VLA N se soportan en todos los sensores que sean compatibles con el Sistema de prevención de intrusiones (IPS) 5.1, excepto NM-CIDS, AIP-SSM-10, y AIP-SSM-20.

El modo en línea de los pares del VLA N es un modo de detección activo donde una interfaz de detección actúa como puerto de tronco 802.1q, y el sensor realiza el VLAN Bridging entre los pares de VLA N en el trunk. Esto significa que el Switch conectado con la interfaz de detección debe estar en el modo tronco.

El sensor examina el tráfico que recibe en cada VLA N en cada par, y puede adelante los paquetes en el otro VLA N en los pares o caer el paquete si se detecta una tentativa de la intrusión. Usted puede configurar un sensor IPS para interligar simultáneamente hasta 255 pares del VLA N en cada interfaz de detección. El sensor substituye el campo VLAN ID en la encabezado 802.1q de cada paquete recibido por el ID del VLA N de la salida en el cual el sensor adelante el paquete. El sensor cae todos los paquetes recibidos en cualquier VLA N que no se asigne a los pares en línea del VLA N.

Nota: Para el IPS-4260, puente fracaso-abierto del hardware no se soporta en los pares en línea del VLA N. Refiera a las restricciones de configuración de puente del hardware para más información.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en el sensor de Cisco Intrusion Prevention System que utiliza los 5.1 y posterior.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Productos Relacionados

La información en este documento es también aplicable al Módulo de servicios del sistema de la detección de intrusos (IDSM-2).

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

El VACL captura la configuración

Refiera a la sección de la captura VACL que configura de configurar el IDSM-2 para enviar el tráfico al IDSM en el Switch.

Configuración de modo en línea de los pares del VLA N

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

Utilice el comando del **interface_name de las interfaces físicas** en el submode de la interfaz del servicio para configurar los pares en línea del VLA N usando el CLI. El nombre de la interfaz es FastEthernet o gigabitethernet.

Estas opciones se aplican:

- **Estado del administrador {habilitado | discapacitado}** — el estado administrativo del link de la interfaz, si la interfaz está habilitada o inhabilitada.**Nota:** En todo el backplane que detecta las interfaces en todos los módulos (IDSM-2 NM-CIDS, y AIP-SSM), fijan a habilitado y se

protegen al Estado del administrador (usted no puede cambiar la configuración). El Estado del administrador no tiene ningún efecto (y se protege) sobre el comando y la interfaz de control. Afecta solamente a detectar las interfaces. El comando y la interfaz de control no necesita ser habilitado porque no puede ser monitoreada.

- **valor por defecto** — Fija el valor de nuevo a la configuración de valor predeterminado del sistema.
- **descripción** — Su descripción de los pares en línea de la interfaz.
- **duplex** — La configuración dúplex de la interfaz.**auto** — Fija la interfaz al auto negocian el duplex.**Conjuntos completos la** interfaz por completo - al duplex.**medio** — Fija la interfaz al half duplex.**Nota:** La opción dúplex se protege en todos los módulos.
- **no** — Quita una configuración de la entrada o de la selección.
- **velocidad** — La configuración de la velocidad de la interfaz.**auto** — Fija la interfaz al auto negocian la velocidad.**10** — Fija la interfaz al 10 MB (para las interfaces TX solamente).**100** — Fija la interfaz al 100 MB (para las interfaces TX solamente).**1000** — Fija la interfaz a 1 GB (para las interfaces Gigabit)**Nota:** La opción de la velocidad se protege en todos los módulos.
- **subinterfaz-tipo** — Especifica que la interfaz es una subinterfaz y definen a qué tipo de subinterfaz.**en línea-VLAN-pares** — Le deja definir la subinterfaz como par en línea del VLA N.**ningunos** — Ningunas subinterfaces definidas.
- **subinterfaz** — Define la subinterfaz como par en línea del VLA N.**vlan1** — El primer VLA N en los pares en línea del VLA N.**vlan2** — El segundo VLA N en los pares en línea del VLA N.

Configuración de CLI

Complete estos pasos para configurar las configuraciones en línea de los pares del VLA N en el sensor usando el CLI:

1. Inicie sesión al CLI usando una cuenta con los privilegios de administrador.
2. Ingrese el submode de la interfaz:
```
sensor#configure terminal
sensor(config)#service interface
sensor(config-int)#
```
3. Verifique si existen algunas interfaces en línea (el tipo de la subinterfaz no debe leer “ninguno” si no se ha configurado ningunas interfaces en línea):
```
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. Quite cualquier interfaz en línea que utilice esta interfaz física:
   `sensor(config-int)#` **`no inline-interfaces interface_name`**

5. Visualice la lista de interfaces disponibles:
   `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. Especifique una interfaz:
   `sensor(config-int)#` **`physical-interfaces GigabitEthernet0/2`**

7. Habilite al Estado del administrador de la interfaz:
   `sensor(config-int-phy)#` **`admin-state enabled`**

   La interfaz se debe asignar al sensor virtual y habilitar para monitorear el tráfico.

8. Agregue una descripción de esta interfaz:
   `sensor(config-int-phy)#` **`description INT1`**

9. Configure las configuraciones dúplex:
   `sensor(config-int-phy)#` **`duplex full`**

Esta opción no está disponible en los módulos.

10. Configure la velocidad:
```
sensor(config-int-phy)#speed 1000
```
Esta opción no está disponible en los módulos.

11. Configure los pares en línea del VLA N:
```
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. Agregue una descripción para los pares en línea del VLA N:
```
sensor(config-int-phy-inl-sub)#description pairs vlans 52 and 53
```

13. Verifique las configuraciones en línea de los pares del VLA N:
```
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. Salga el submode de la interfaz:
```
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. Presione ENTER para aplicar los cambios, o ingresar **no** para desecharlos.
16. Ingrese el modo virtual de la Configuración del sensor:
```
sensor(config)#service analysis-engine
        sensor(config-ana)#virtual-sensor vs0
```

17. Agregue la interfaz al virtual-sensor:
```
sensor(config-ana-vir)#physical-interface GigabitEthernet0/2
subinterface-number 1
```

18. Salga el submode del virtual-sensor:
```
sensor(config-ana-vir)#exit
        sensor(config-ana)#exit
        Apply Changes:?[yes]:
```
19. Presione ENTER para aplicar los cambios, o ingresar **no** para desecharlos.

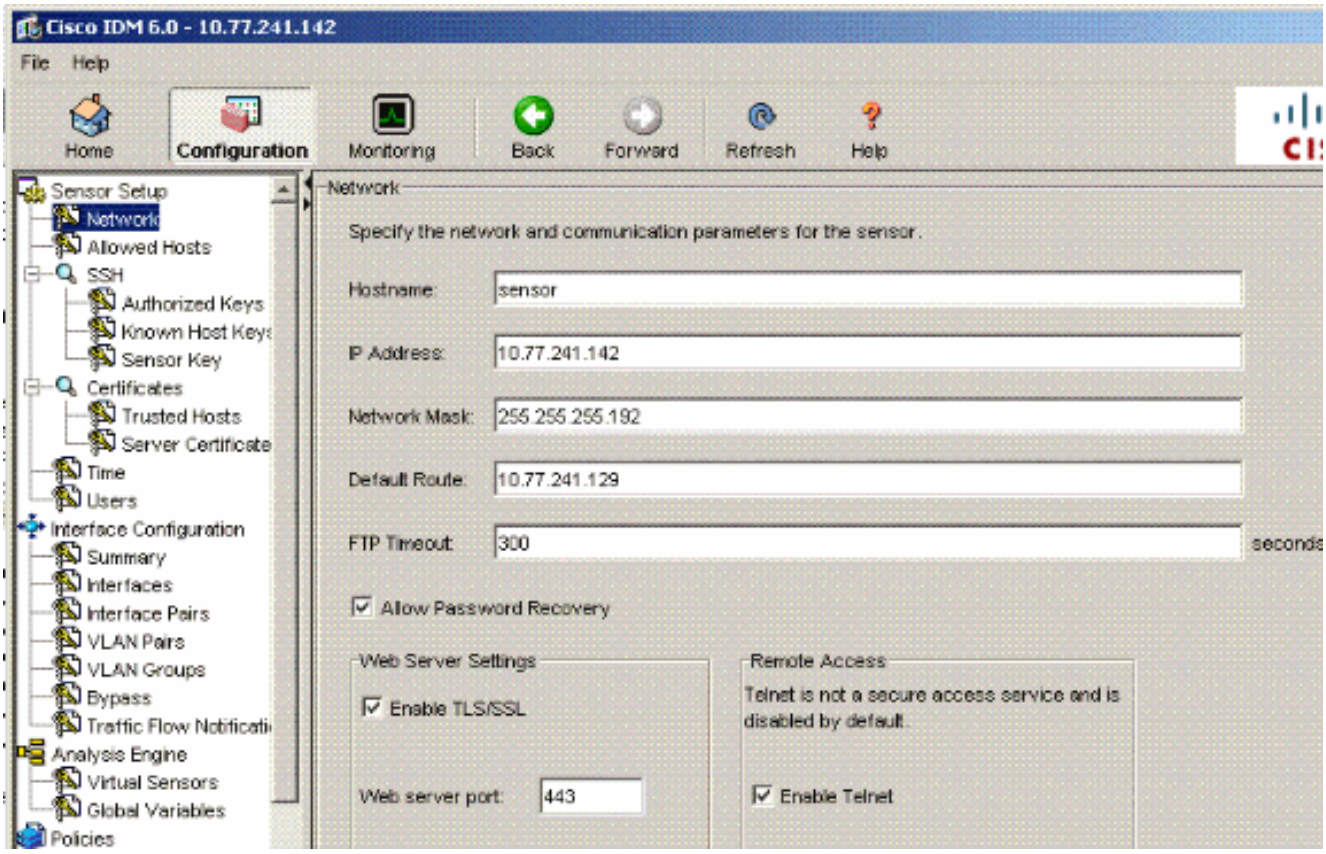
Configuración IDM

Complete estos pasos para configurar las configuraciones en línea de los pares del VLA N en el sensor usando el IDS Device Manager (IDM):

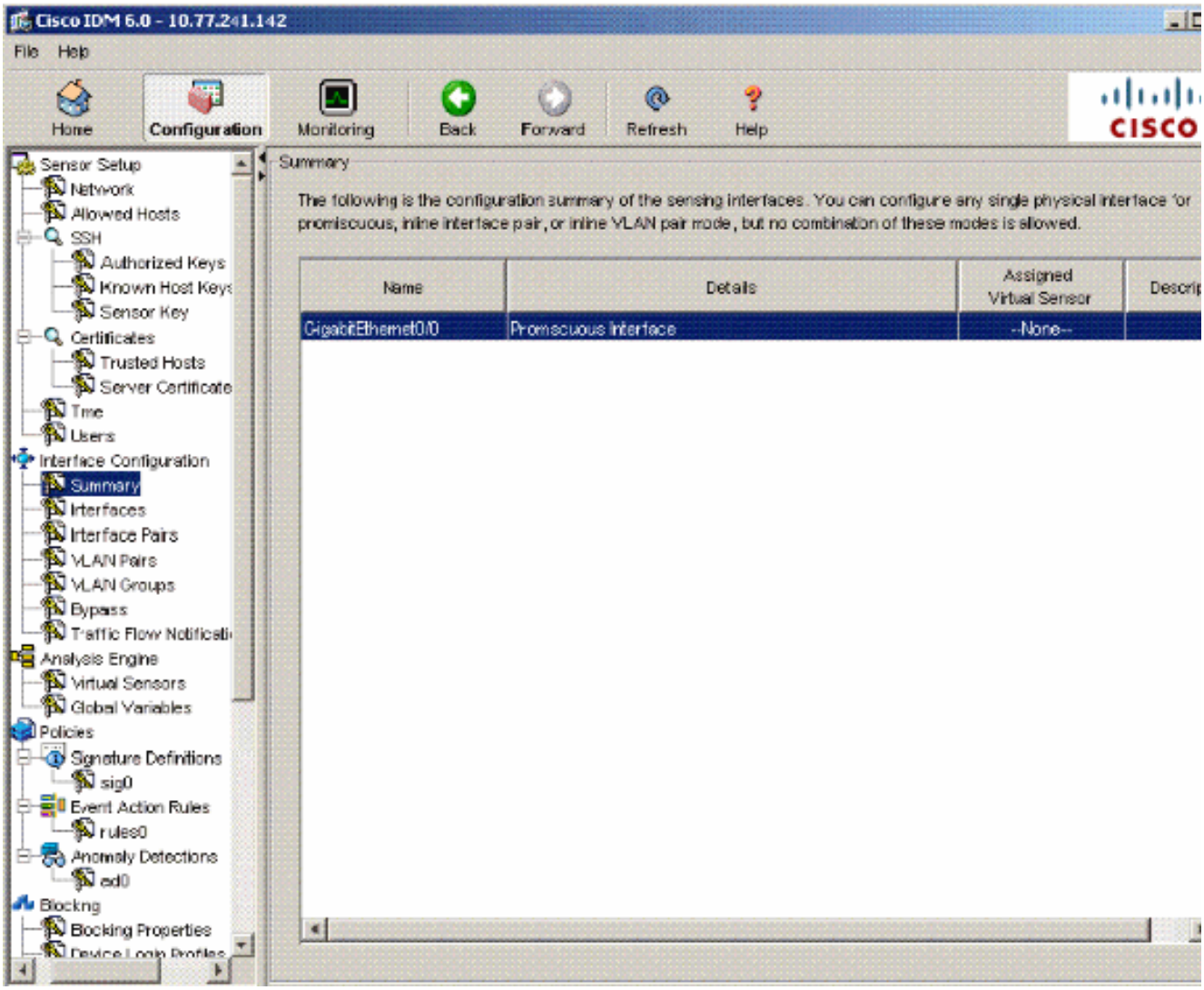
1. Abra su hojeador y ingrese el **<Management_IP_Address_of_IPS> de https://** para acceder el IDM en el IPS.
2. Haga clic el **lanzador de la descarga IDM y comience el IDM** para descargar el instalador para la aplicación.

3. Van al Home Page para ver la información del dispositivo tal como nombre del host, la dirección IP, la versión, y el modelo., los etc.

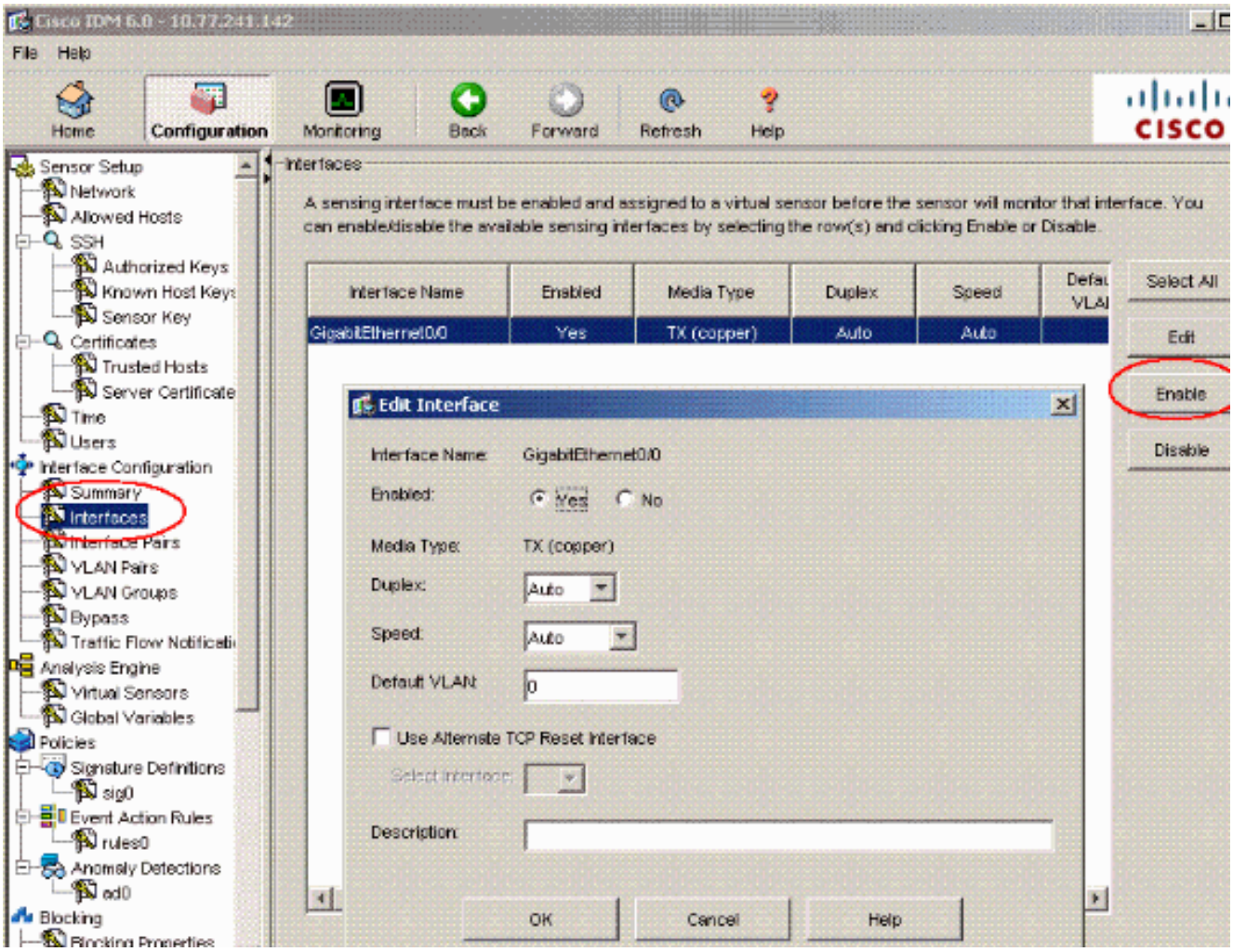
4. Vaya a la **configuración > a la configuración del sensor** y haga clic la **red**. Aquí usted puede especificar el nombre de host, la dirección IP y la ruta predeterminado.



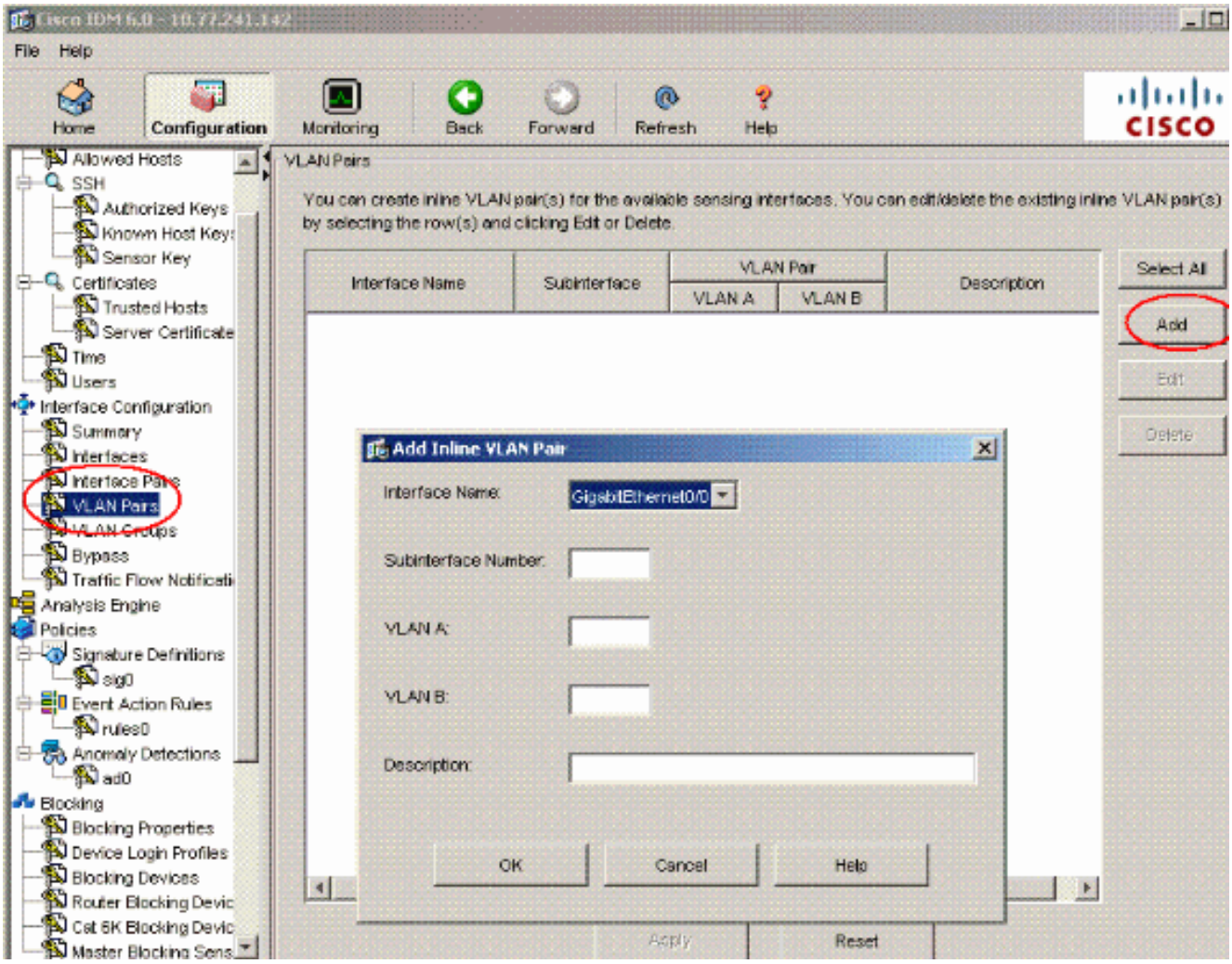
5. Vaya a la **configuración > a la configuración de la interfaz** y haga clic el **resumen**.Esta página muestra el resumen de la configuración de la interfaz de detección.



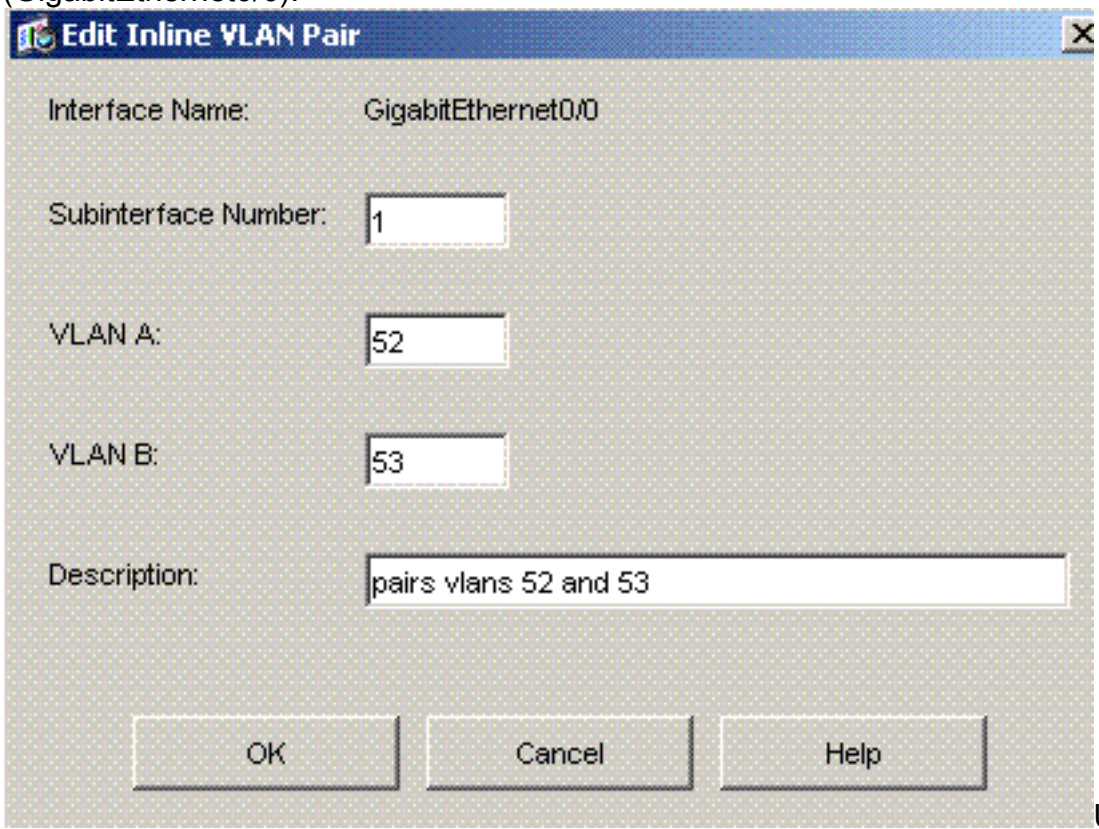
6. Vaya a la **configuración > a la configuración de la interfaz > a las interfaces** y seleccione el nombre de la interfaz. Entonces, **permiso del** tecleo para habilitar la interfaz de detección. También, configure el duplex, la velocidad y la información de VLAN.



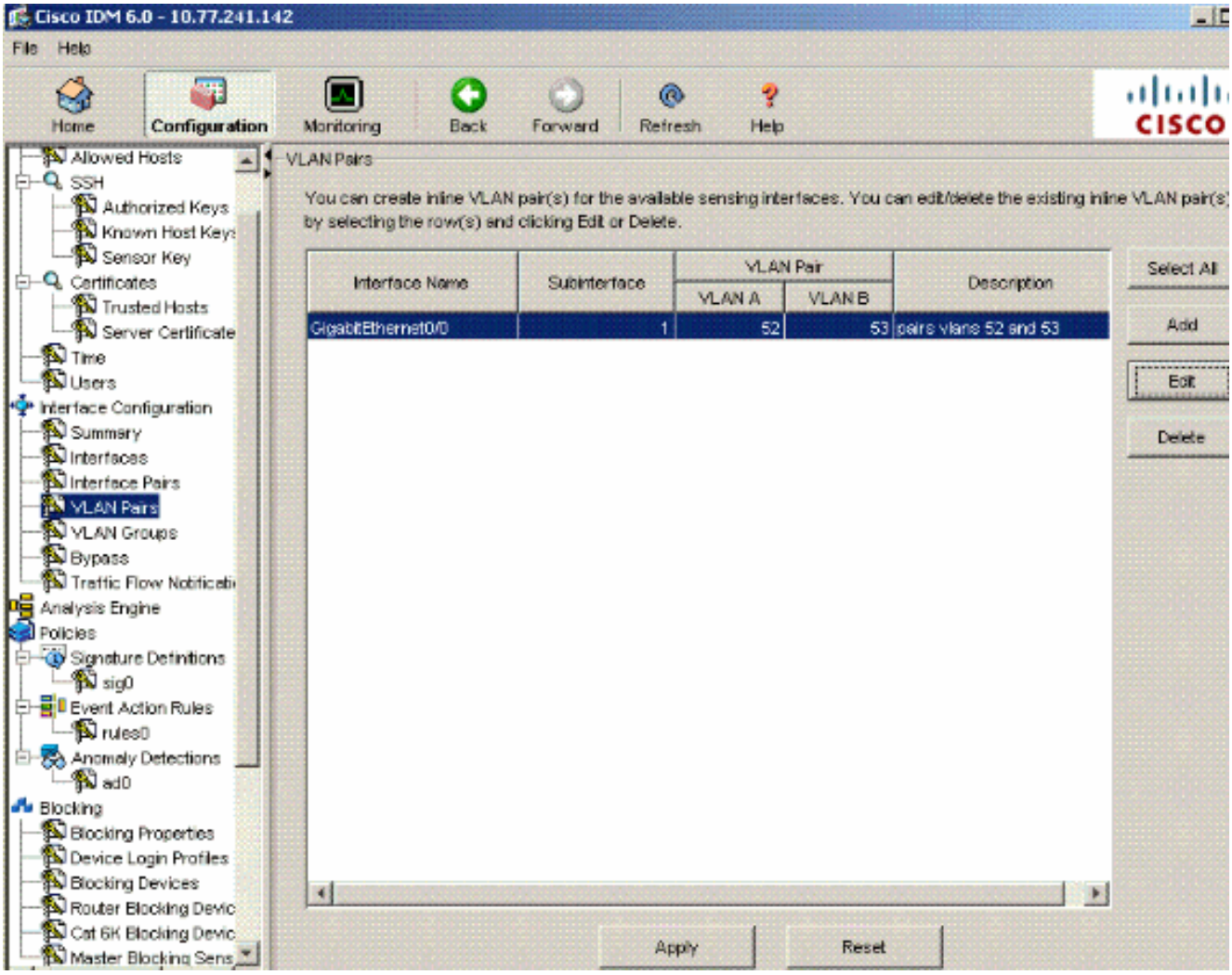
7. Vaya a la **configuración > a la configuración de la interfaz > a los pares del VLA N** y el tecleo **agrega** para crear los pares en línea del VLA
N.



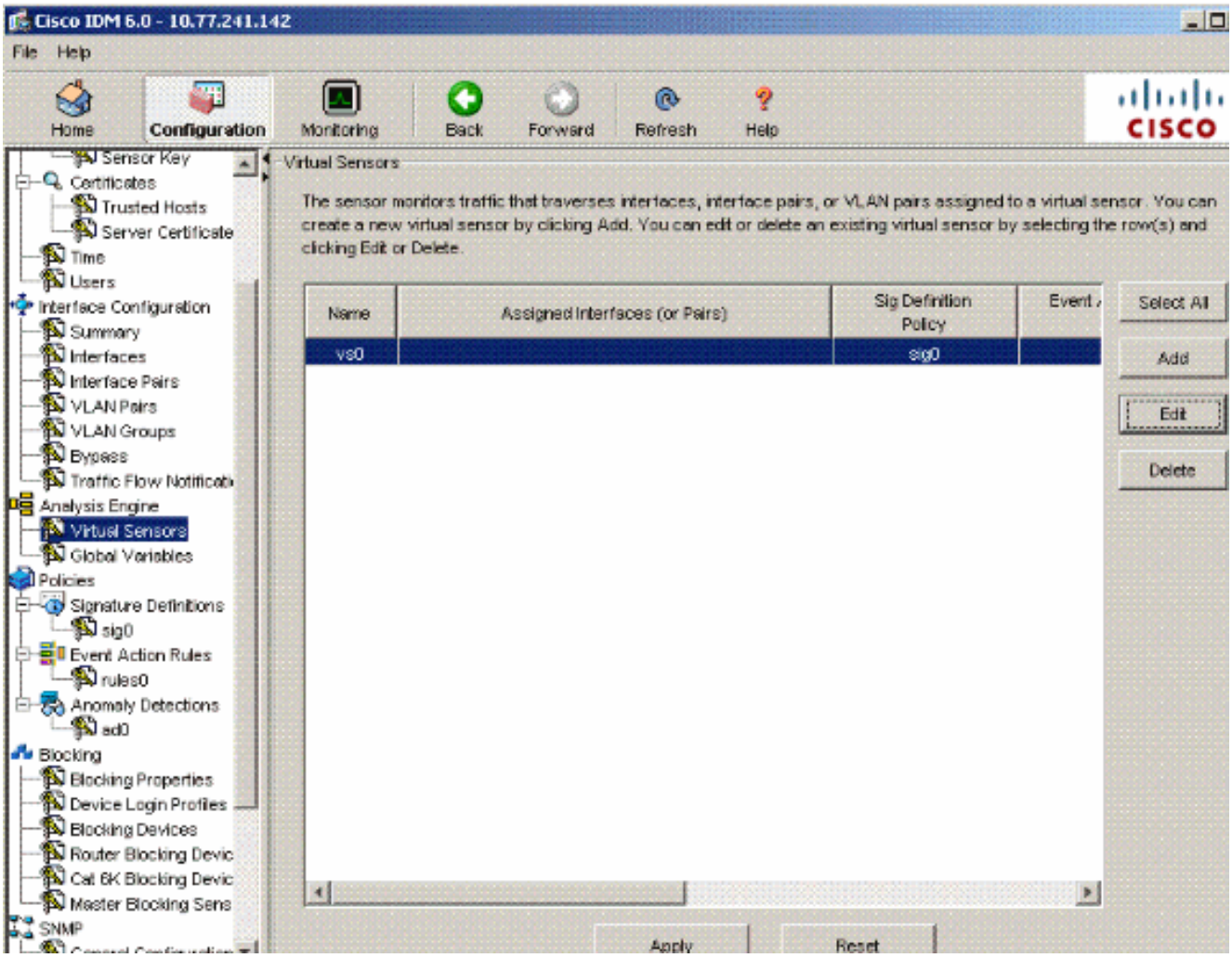
8. Ingrese el número de la subinterfaz, el VLA N A y el VLA N B para la interfaz de detección (GigabitEthernet0/0).



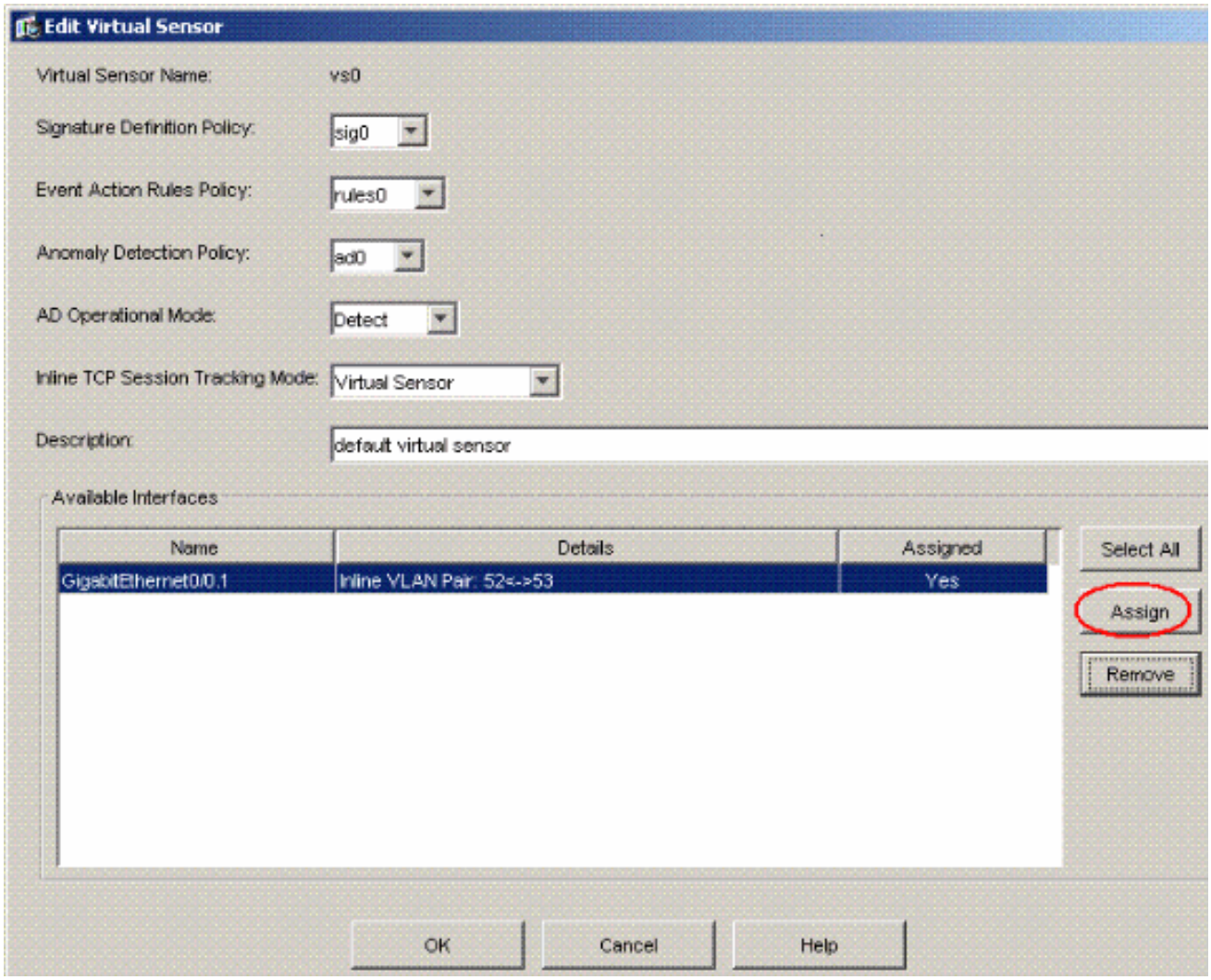
Usted puede ver el resumen de la configuración en línea de los pares del VLA N.



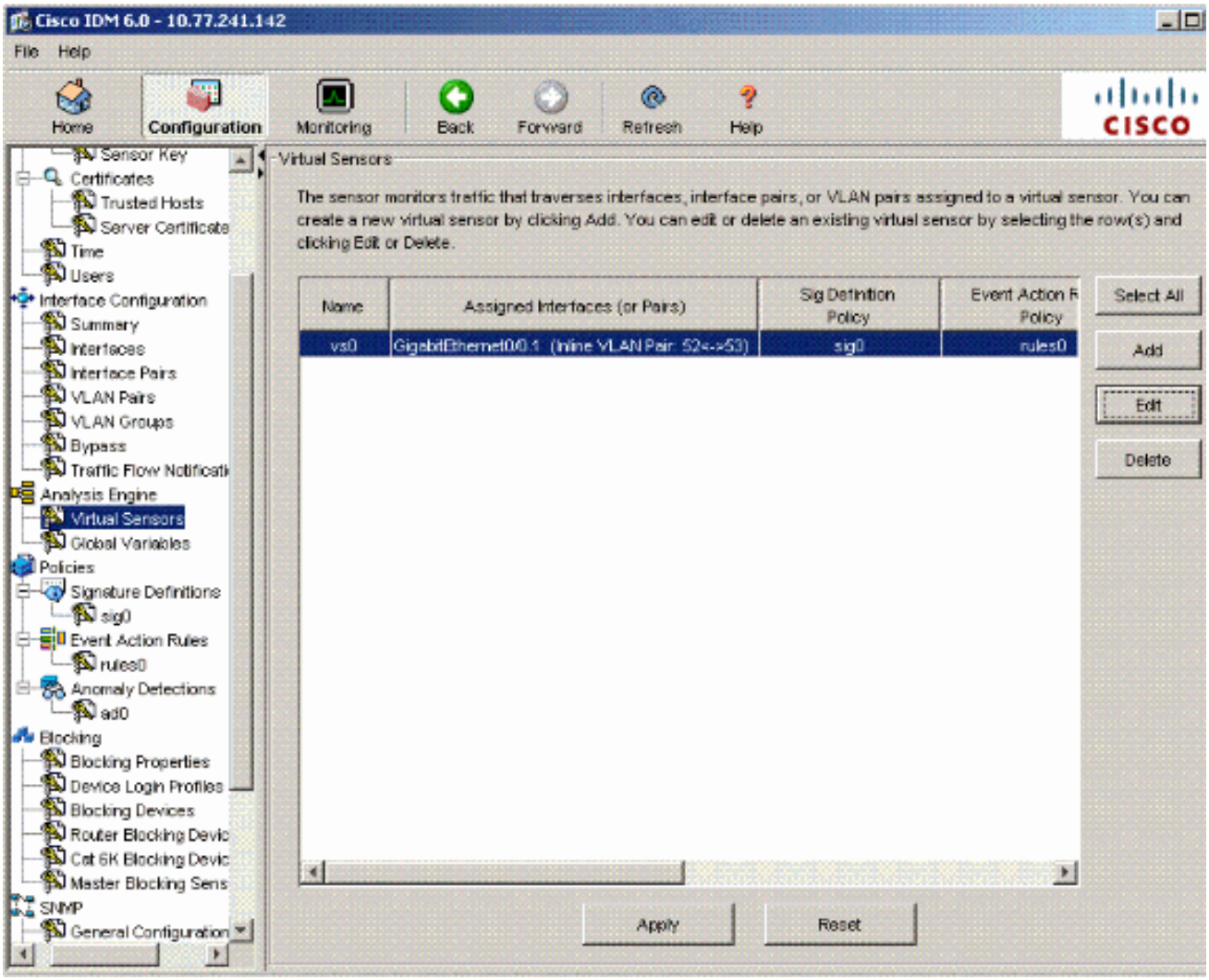
9. Va al **motor de la configuración > del análisis > el sensor virtual** y el tecleo **edita** para crear el nuevo sensor
virtual.



10. Asigne los pares en línea 52 y 53 del VLA N al sensor virtual vs0.



Vea el resumen de la información virtual asignada del sensor.



Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco Intrusion Prevention System
- Sensores Cisco IPS de la serie 4200
- Soporte Técnico y Documentación - Cisco Systems