IPS 6.X y later/IDSM2: La interfaz en línea empareja el modo usando el ejemplo de configuración IDM

Contenido

Introducción

El funcionamiento en el modo en línea de los pares de la interfaz pone el Sistema de prevención de intrusiones (IPS) directamente en el flujo de tráfico y afecta a las tarifas del reenvío de paquete, que las hace más lentas cuando se agrega el tiempo de espera. Esto permite que el sensor pare los ataques así que cae el tráfico malévolo antes de que alcance la blanco prevista, así proporciona un servicio protector. No sólo está la información de proceso en línea del dispositivo sobre las capas 3 y 4, pero también analiza el contenido y el payload de los paquetes para ataques integrados más sofisticados (capas 3 a 7). Este análisis más profundo deja el sistema identificar y parar y/o bloquear los ataques que pasan normalmente con un tradicional dispositivo de firewall.

En el modo en línea de los pares de la interfaz, un paquete viene adentro a través de la primera interfaz de los pares en el sensor y hacia fuera de la segunda interfaz de los pares. El paquete se envía a la segunda interfaz de los pares a menos que ese paquete esté siendo negado o modificado por una firma.

Nota: Usted puede configurar AIM-IPS y AIP-SSM para actuar en línea aunque estos módulos tienen solamente una interfaz de detección.

Nota: Si las interfaces emparejadas están conectadas con el mismo Switch, usted debe configurarlas en el Switch como puertos de acceso con diversos VLA N del acceso para los dos

puertos. Si no, el tráfico no atraviesa la interfaz en línea.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en el sensor del IPS de Cisco que utiliza la interfaz de línea de comando 6.0 y al administrador de dispositivo del sistema de prevención de intrusiones (IDM) 6.0.

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.

La interfaz en línea empareja la configuración

Utilice el *comando name de las en línea*-**interfaces** en el submode de la interfaz del servicio para crear los pares en línea de la interfaz.

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

Nota: AIP-SSM se configura para el modo en línea de la interfaz de Cisco ASA CLI y no del IPS de Cisco CLI.

Estas opciones se aplican:

- *nombre de las en línea*-**interfaces** — Nombre de los pares en línea lógicos de la interfaz**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
- *interface_name* **interface1** — La primera interfaz en los pares en línea de la interfaz
- *interface_name* **interface2** — La segunda interfaz en los pares en línea de la interfaz
- **no** — Quita una configuración de la entrada o de la selección
- **Estado del administrador {habilitado | discapacitado}** — el estado administrativo del link de la interfaz, si la interfaz está habilitada o inhabilitada.

Configuración de CLI

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

1. Inicie sesión al CLI con una cuenta que tenga 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. Nombre los pares en línea:`sensor(config-int)#` **`inline-interfaces PAIR1`**
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. Configure dos interfaces en un par:`sensor(config-int)#` **`interface1 GigabitEthernet0/0`**
   `sensor(config-int-inl)#` **`interface2 GigabitEthernet0/1`** Usted debe asignar la interfaz a un sensor virtual y habilitarla antes de que pueda monitorear el tráfico. Vea el paso 10 para más información.
7. Agregue una descripción de esta interfaz:`sensor(config-int-phy)#` **`description PAIR1 Gig0/0 and Gig0/1`**
8. Relance los pasos 4 a 7 para cualquier otra interfaz que usted quiera configurar a los pares en línea de la interfaz.
9. Verifique las configuraciones:`sensor(config-int-inl)#` **`show settings`** `name: PAIR1 ------------ ---------- description: PAIR1 Gig0/0 & Gig0/1 default: interface1: GigabitEthernet0/0 interface2: GigabitEthernet0/1 ---------- ------`
10. Habilite las interfaces asignadas a los pares de la interfaz:`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. Verifique que las interfaces estén habilitadas:`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 ----
---------- ----------
- ---------- ----------
```

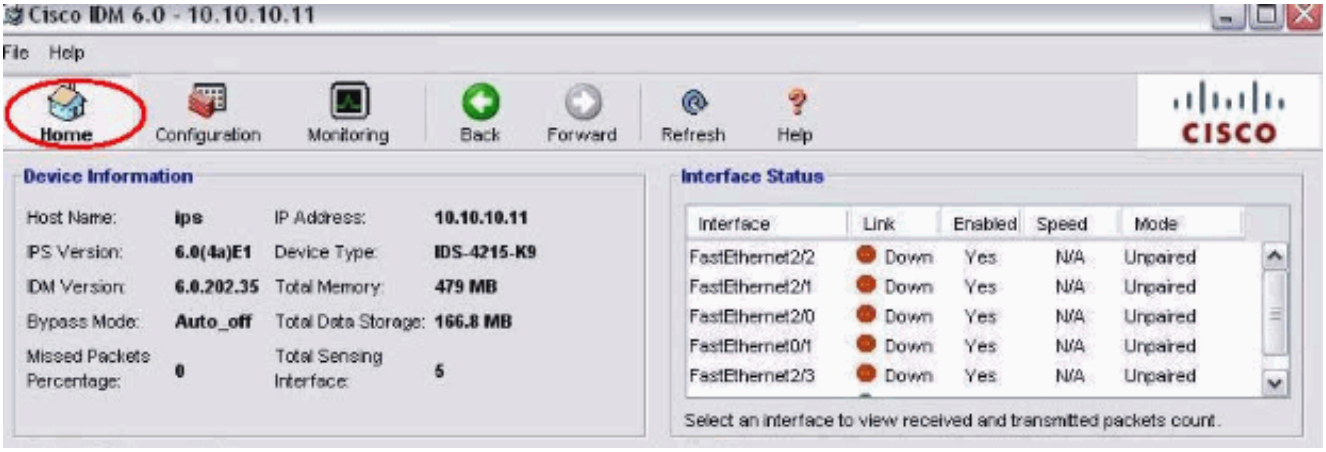
```
------- <protected entry> name: GigabitEthernet0/3 <defaulted> ----------------------------
------------------- media-type: tx <protected> --MORE--
```

12. Publique este comando para borrar un par en línea de la interfaz y volver las interfaces al modo promiscuo:`sensor(config-int)#` **`no inline-interfaces PAIR1`** Usted debe también borrar los pares en línea de la interfaz del sensor virtual al cual se asigna.
13. Verifique los pares en línea de la interfaz se ha borrado:`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. Salga el submode de la configuración de la interfaz:`sensor(config-int)#` **`exit`** `Apply Changes:?[yes]:`
15. Presione ENTER para aplicar los cambios o ingresar **ningún** para desecharlos.

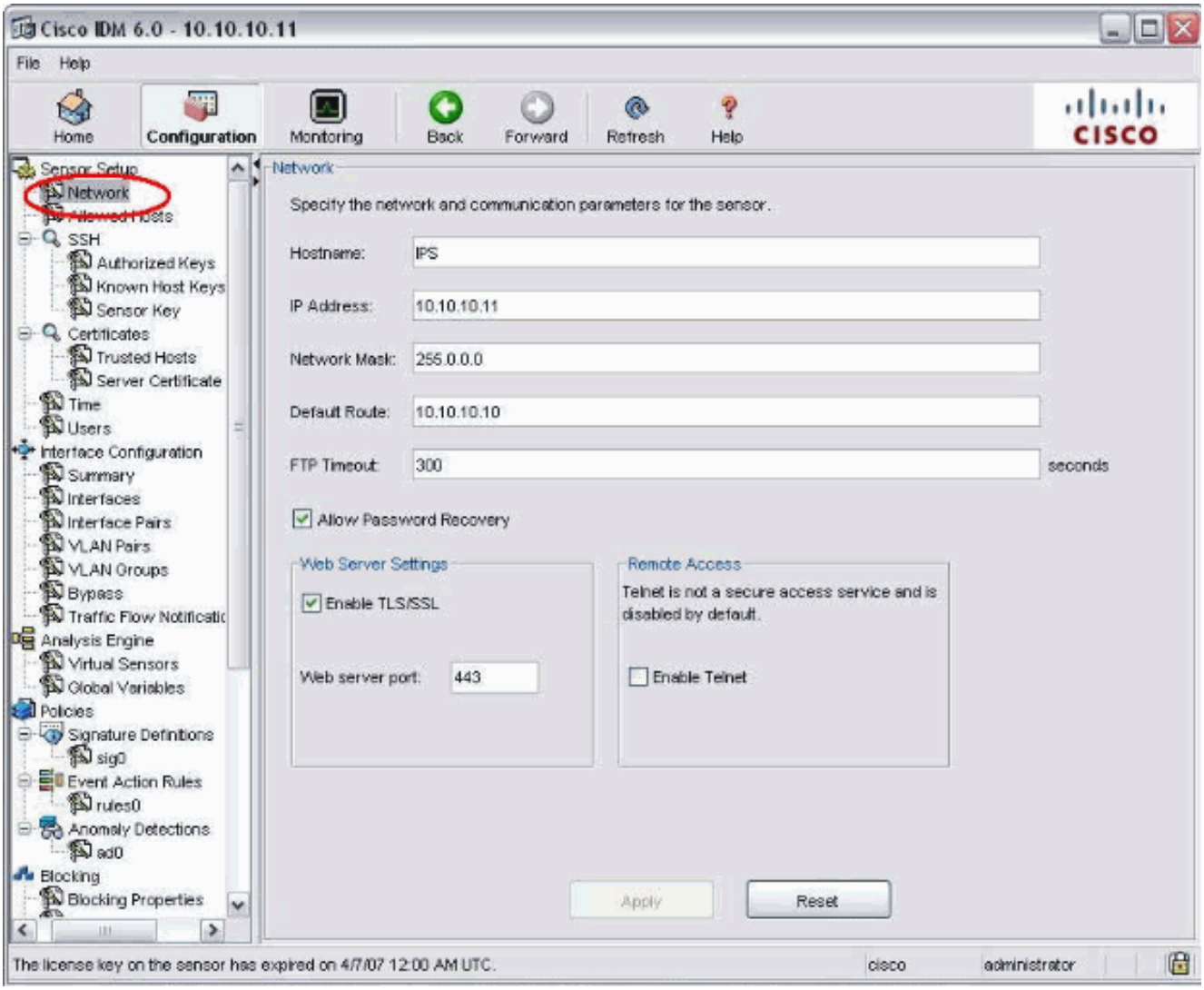
Configuración IDM

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

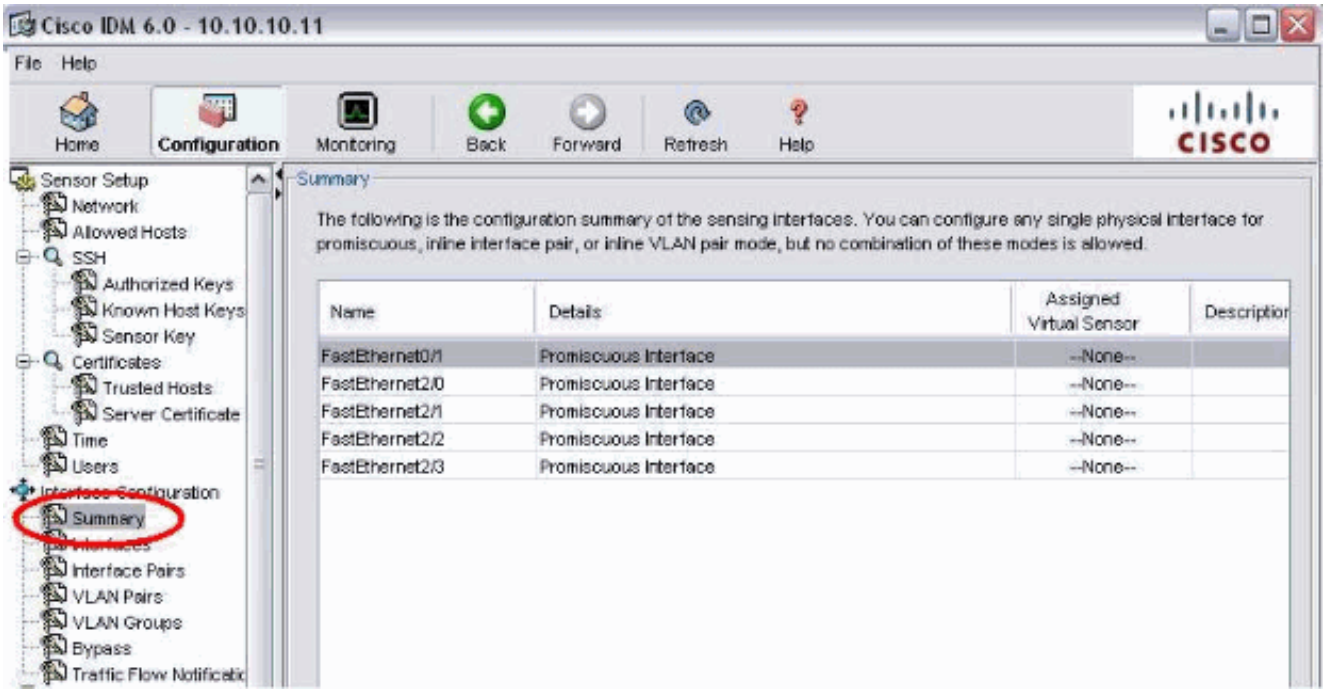
1. Abra su hojeador y ingrese el **<Management_IP_Address_of_IPS> de https://** para acceder el IDM en el IPS.
2. Haga clic el **lanzador de la descarga IDM** y **comience el IDM** para descargar el instalador para la aplicación.
3. Vaya al Home Page para ver la información del dispositivo tal como nombre del host, dirección IP, versión, y el modelo.



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.

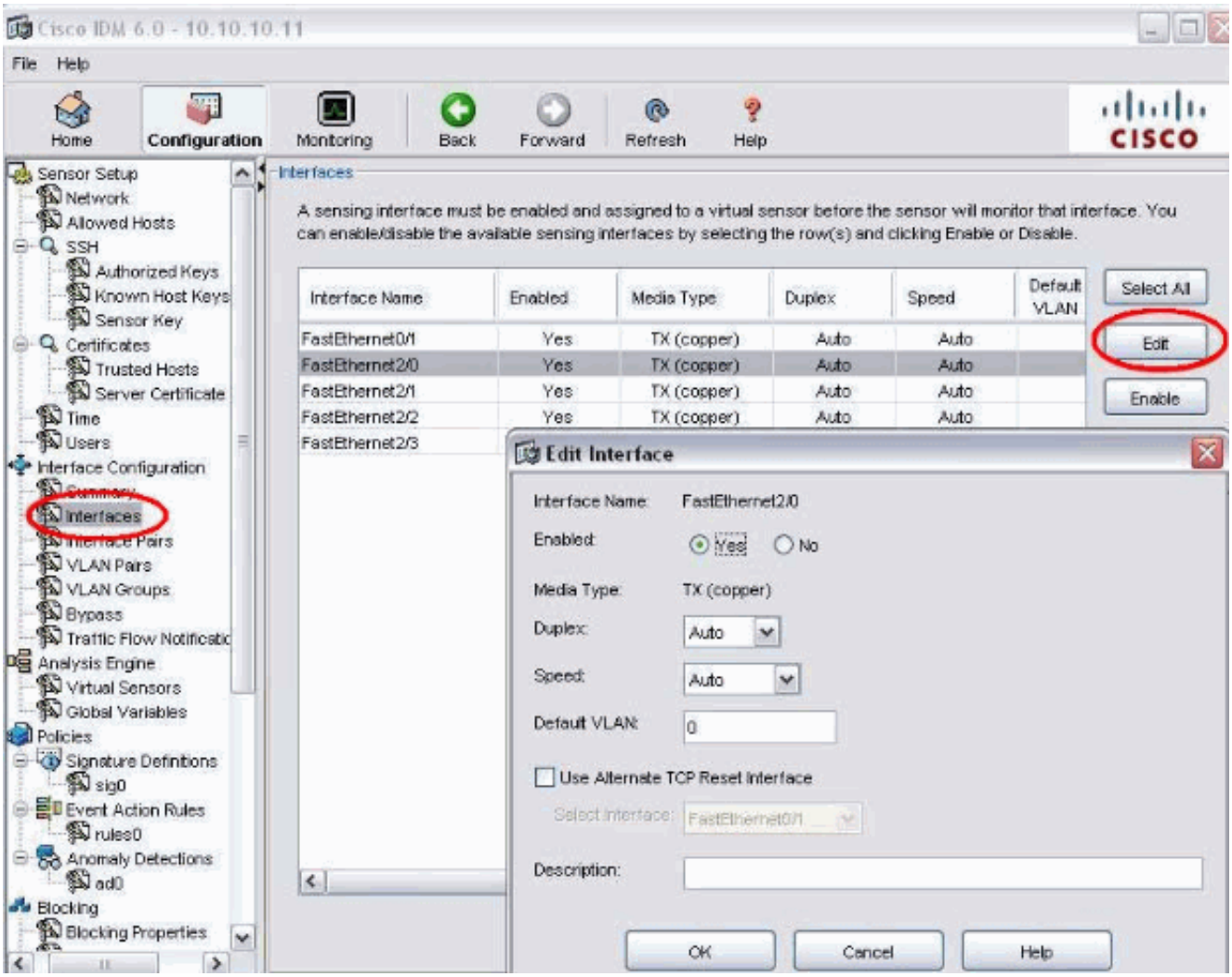


5. Vaya a la **configuración > a la configuración de la interfaz** y haga clic el **resumen**.Esta página muestra el resumen de la configuración de la interfaz de detección:

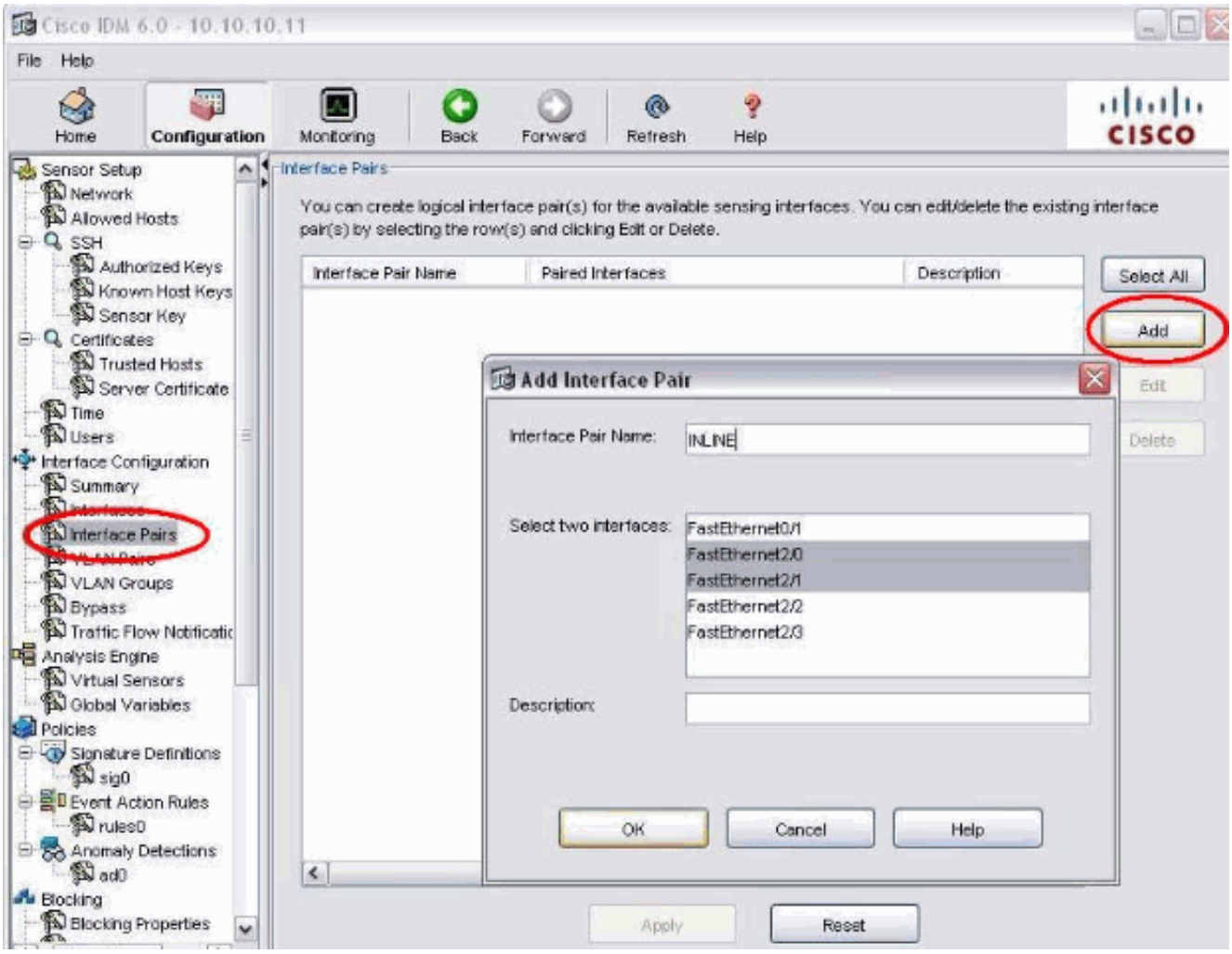


6. Vaya a la **configuración > a la configuración de la interfaz > a las interfaces** y seleccione el nombre de la interfaz. Entonces, **permiso del** tecleo para habilitar la interfaz de detección. También, configure el duplex, la velocidad y la información de

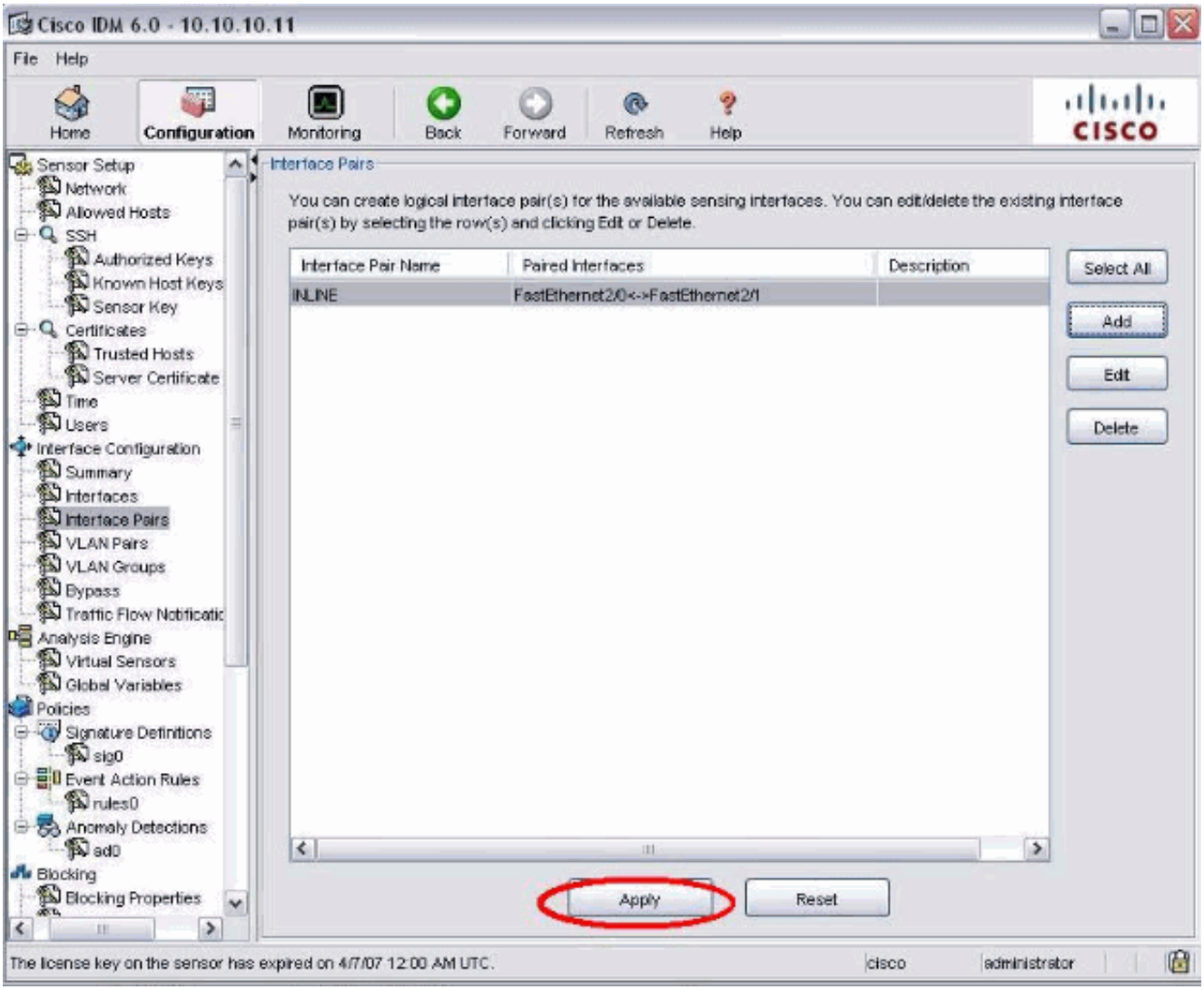
VLAN.



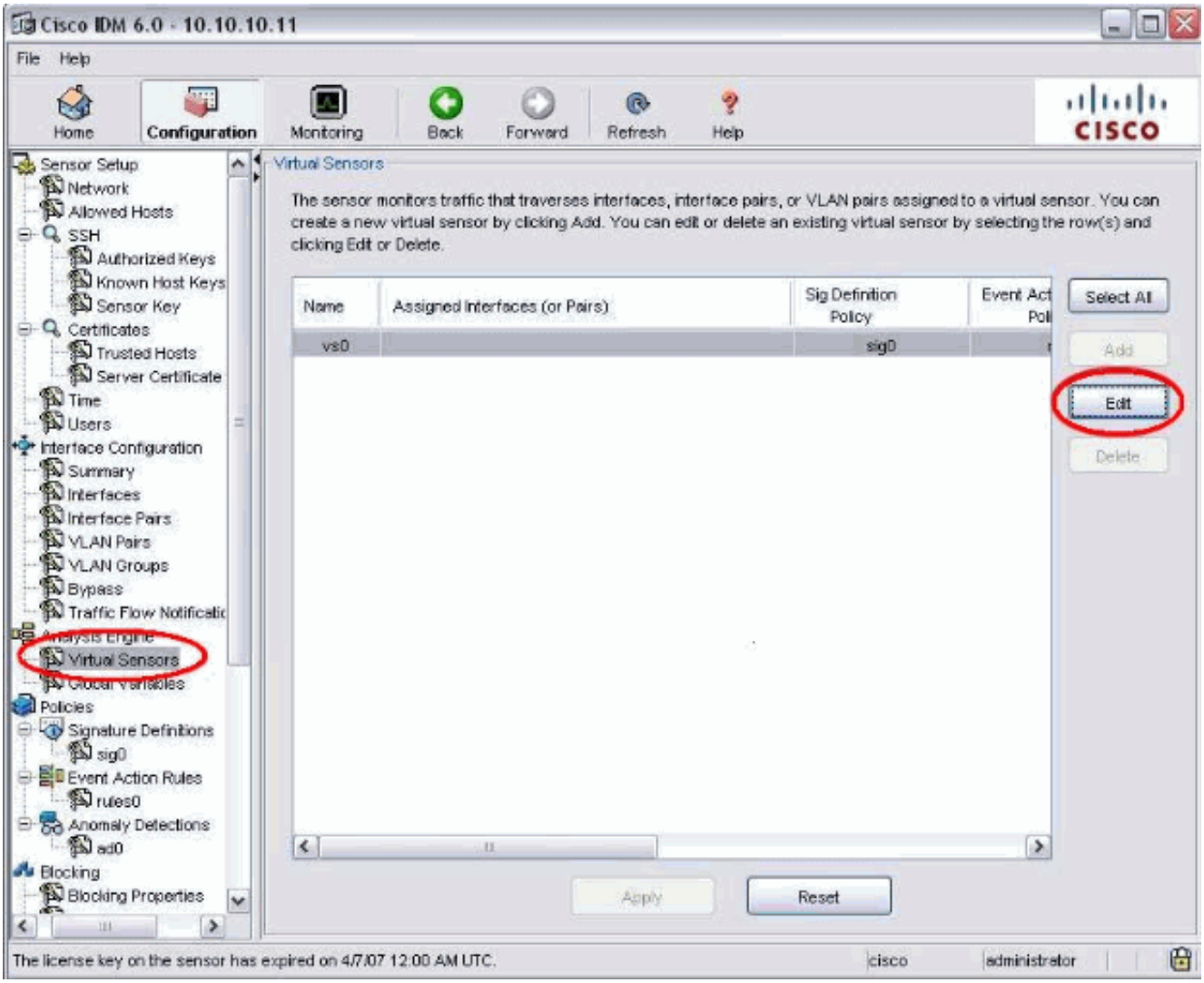
7. Vaya a los **pares de la configuración > de la configuración de la interfaz > de la interfaz** y el tecleo **agrega** para crear los pares en línea.



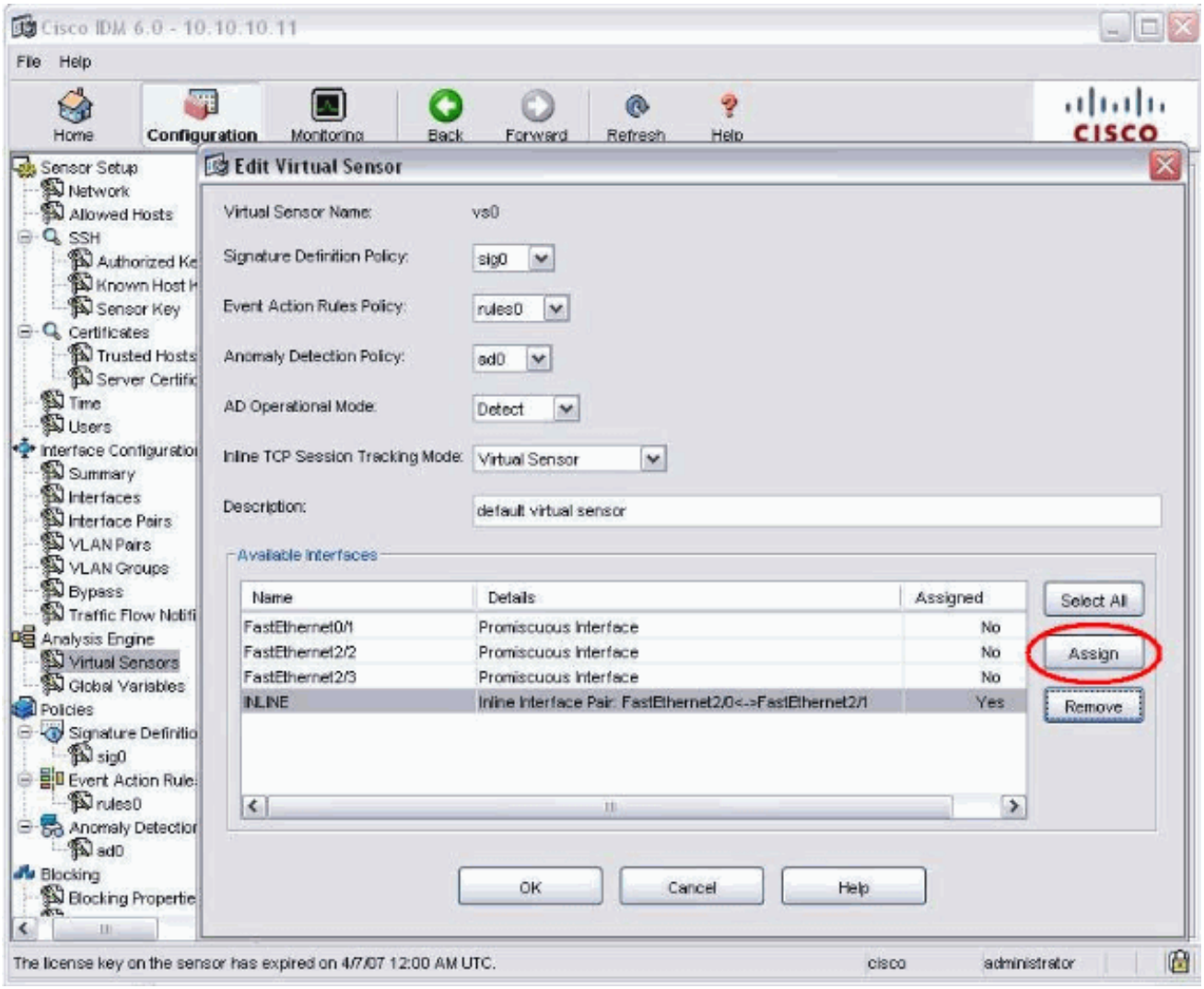
8. Vea el resumen de la configuración en línea de los pares y apliqúelo.



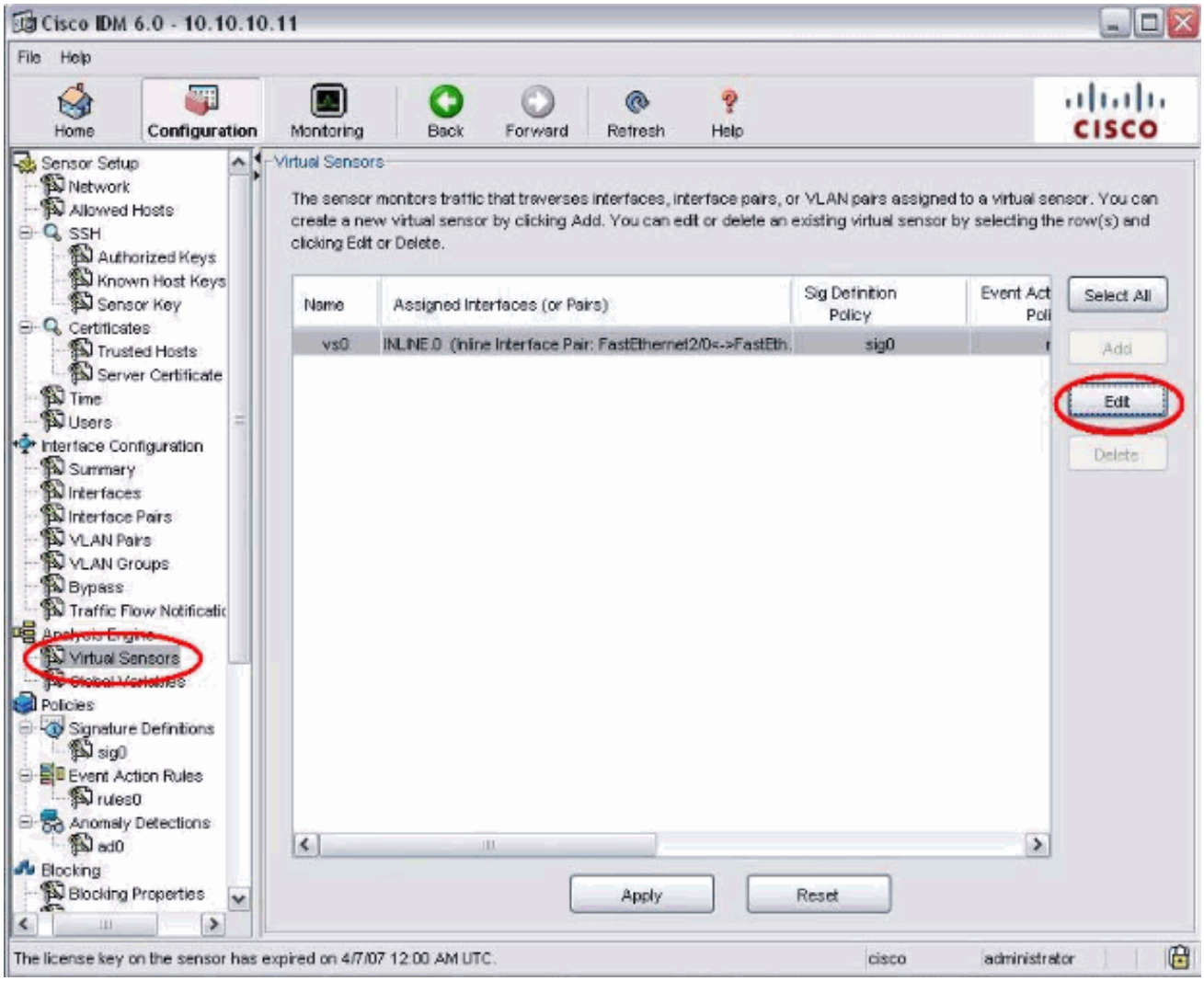
9. Va al **motor de la configuración > del análisis > el sensor virtual** y el tecleo **edita** para crear el nuevo sensor
virtual.



10. Asigne los pares en línea **EN LÍNEA al** sensor virtual vs0.



11. Vea el resumen de la información virtual asignada del sensor.



Configure el Switch para el IDSM-2 en el modo en línea

Refiera a configurar el 6500 Switch del Catalyst Series para el IDSM-2 en la sección de modo en línea de configurar el IDSM-2 para configurar el Switch para el modo en línea IDSM-2.

Troubleshooting

Problema

Si el IPS falla y se configura en línea, haga las interfaces fallan abierto (el tráfico continúa pasando) o cerrado (se cae el tráfico).

Solución

Usted puede configurar el IPS en el estado fracaso-abierto. Así, si el IPS falla continuará pasando el tráfico, pero no monitorea el tráfico.

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