Configuración de un Cisco Secure IDS Sensor en CSPM

Contenido

Introducción

Este documento explica el procedimiento usado para configurar un sensor del Cisco Secure Intrusion Detection System (IDS) en el Cisco Secure Policy Manager (CSPM). Este documento asume que instaló la versión 2.3.I de CSPM en el equipo. La versión "I" permite la administración de los dispositivos IDS (Sensores de aplicación, routers del IOS® de Cisco o de IDS Blades) en un switch Catalyst® 6000 de Cisco. Este documento también asume que los parámetros de la oficina de correo IDS están definidos correctamente. Éstos incluyen el HOSTID, el ORGID, el NOMBRE DE HOST, y el ORGNAME. Tenga en cuenta que para que el host CSPM se comunique con un Sensor, ORGID y ORGNAME deben coincidir con lo que está definido en el Sensor.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en CSPM 2.3.I 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.

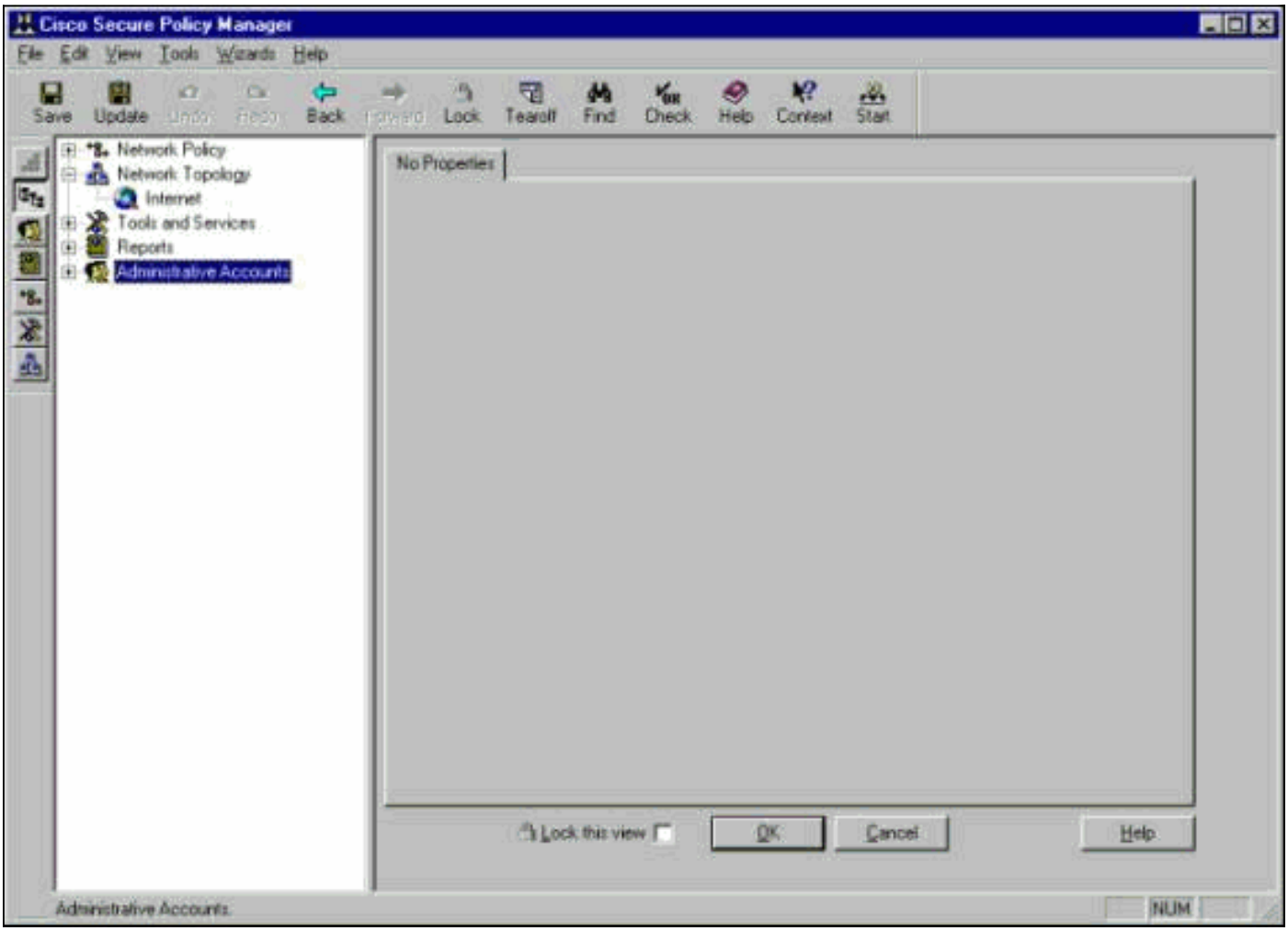
Convenciones

Para obtener más información sobre las convenciones del documento, consulte las Convenciones de Consejos Técnicos de Cisco.

Configuración

Estas secciones explican el proceso usado para configurar un sensor IDS en el CSPM.

Lanzamiento CSPM y login. Aparece un plantilla en blanco (primer inicio) que le permite definir la red.



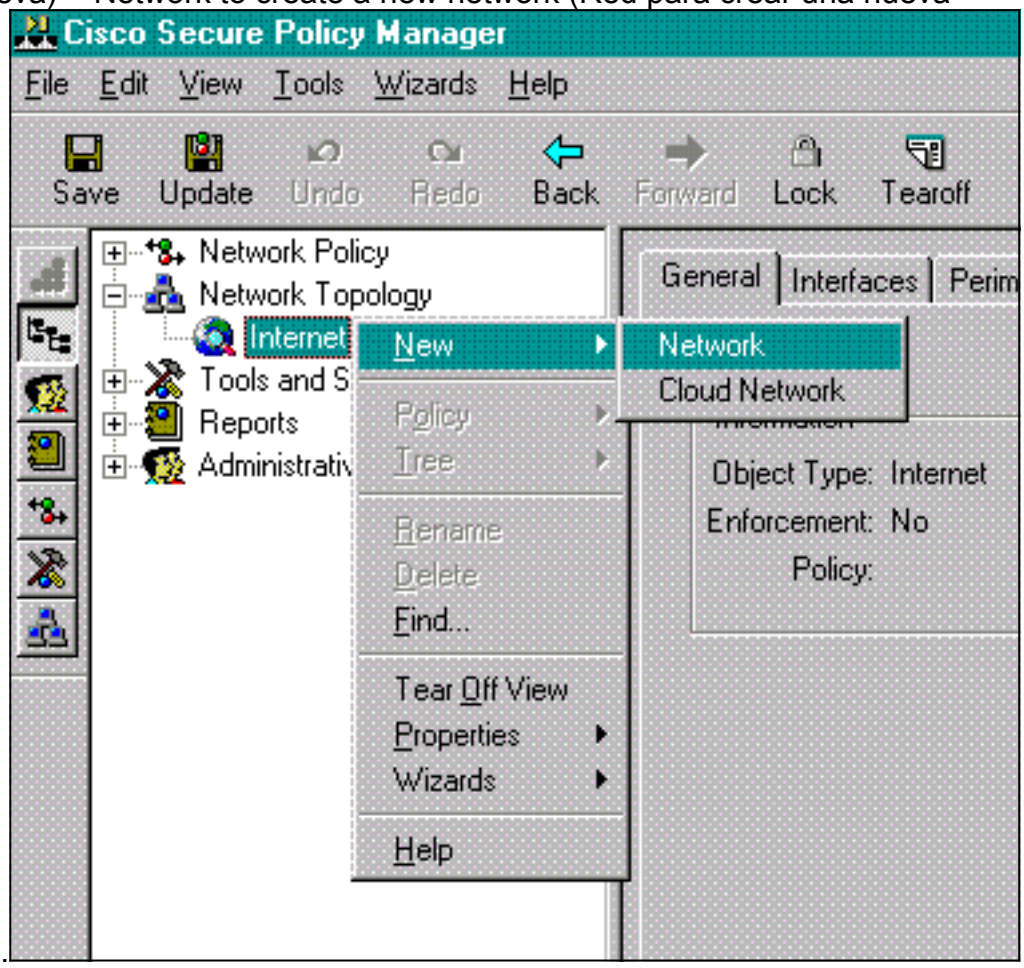
Estas tres definiciones se requieren en la topología CSPM para IDS.

1. Defina la red en la que se encuentra la interfaz de control del Sensor y la red en la que se encuentra el host CSPM. Si están en la misma subred, después solamente una red necesita ser definida. Primero defina la red.
2. Defina el host CSPM en su red. Sin la definición del host CSPM, no es posible administrar el Sensor.
3. Defina el sensor en su red.

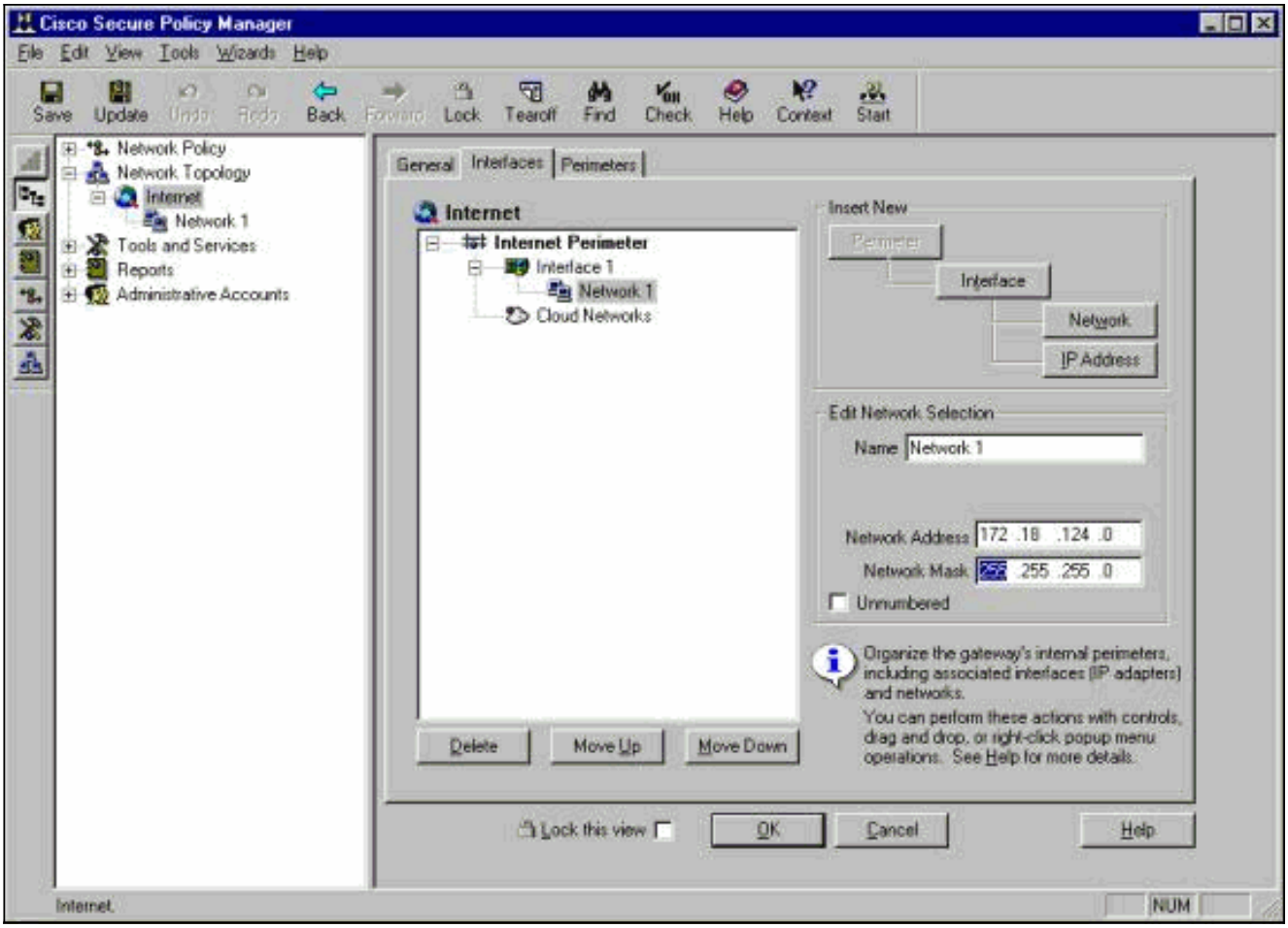
Definir la red en la que reside el host CSPM

Complete estos pasos:

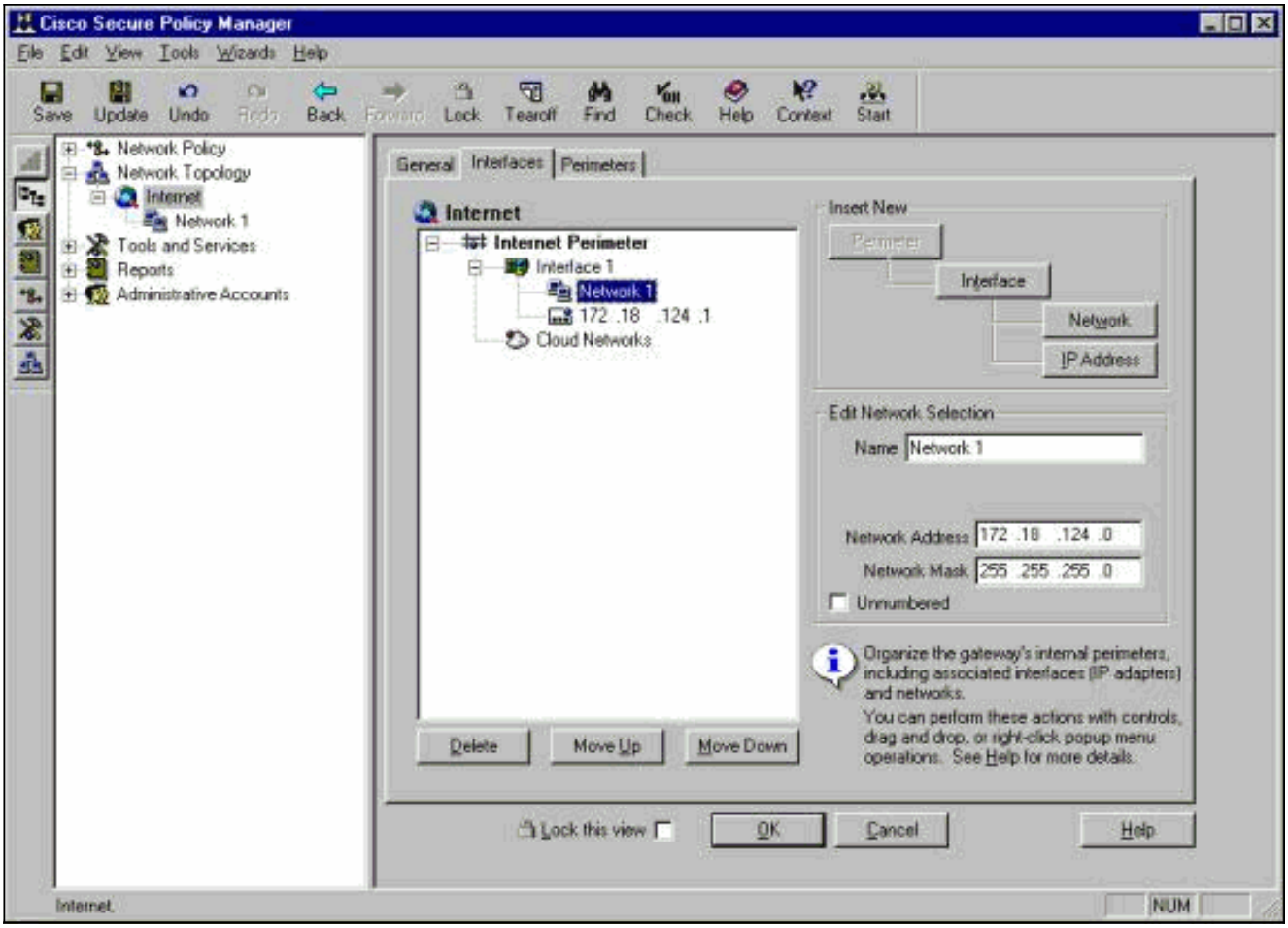
1. Haga clic con el botón derecho en el icono de Internet en la topología y seleccione New (Nueva) > Network to create a new network (Red para crear una nueva red).



2. En el lado derecho del panel de la red, agregue el nombre de la red nueva, la dirección de la red y la máscara que se utilizará.



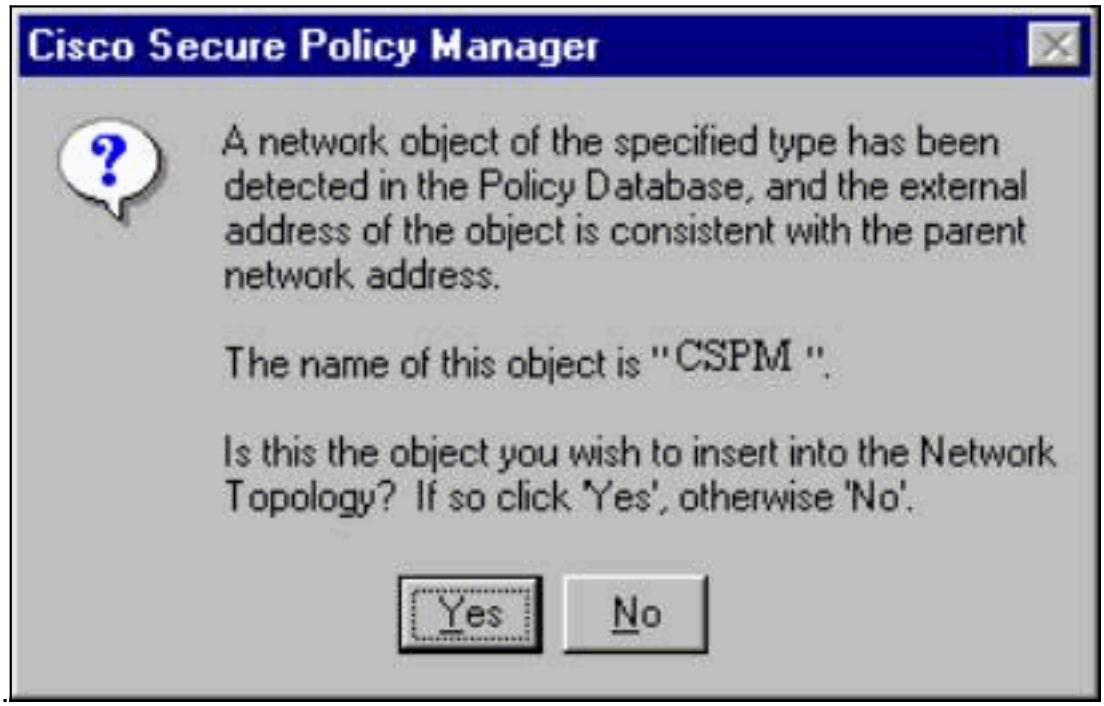
3. Haga clic en el botón IP Address (Dirección IP) e ingrese la dirección IP que su red utiliza para conectarse a Internet.Es normalmente el default gateway para la red.**Nota:** Cuando usted maneja los sensores, la dirección del gateway no tiene que necesariamente estar correcta puesto que el sensor no se envía esta información de gateway predeterminado. Debe ser definido ya en el sensor.
4. Haga clic en OK. La red se agrega a la correlación de topología sin ningunos errores.



Agregar el host CSPM

Utilice este procedimiento para agregar el host CSPM.

1. En la topología de red, haga clic con el botón derecho del ratón en la red que usted acaba de agregar y seleccione **New > Host**.El CSPM trae para arriba una pantalla similar a esto. De lo contrario, la red que acaba de definir no es la red en la que se ubica su host CSPM. Vuelva a verificar la dirección IP en su host de



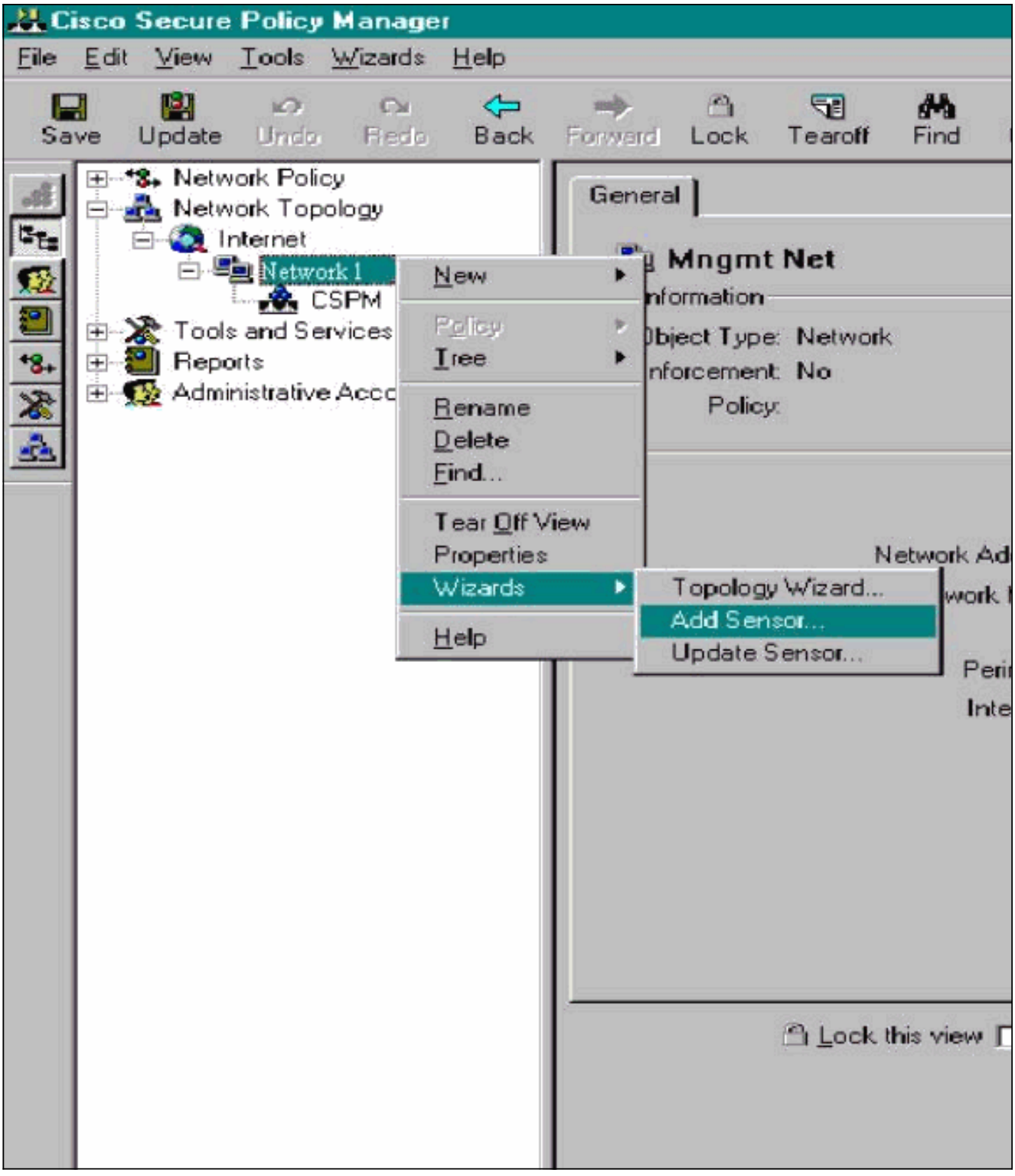
CSPM.

2. Haga clic en Yes (Sí) para instalar el host CSPM dentro de la topología.
3. Verifique que la información en la pantalla General para el host CSPM sea correcta.
4. Haga clic en OK (Aceptar) en la pantalla General del host CSPM.

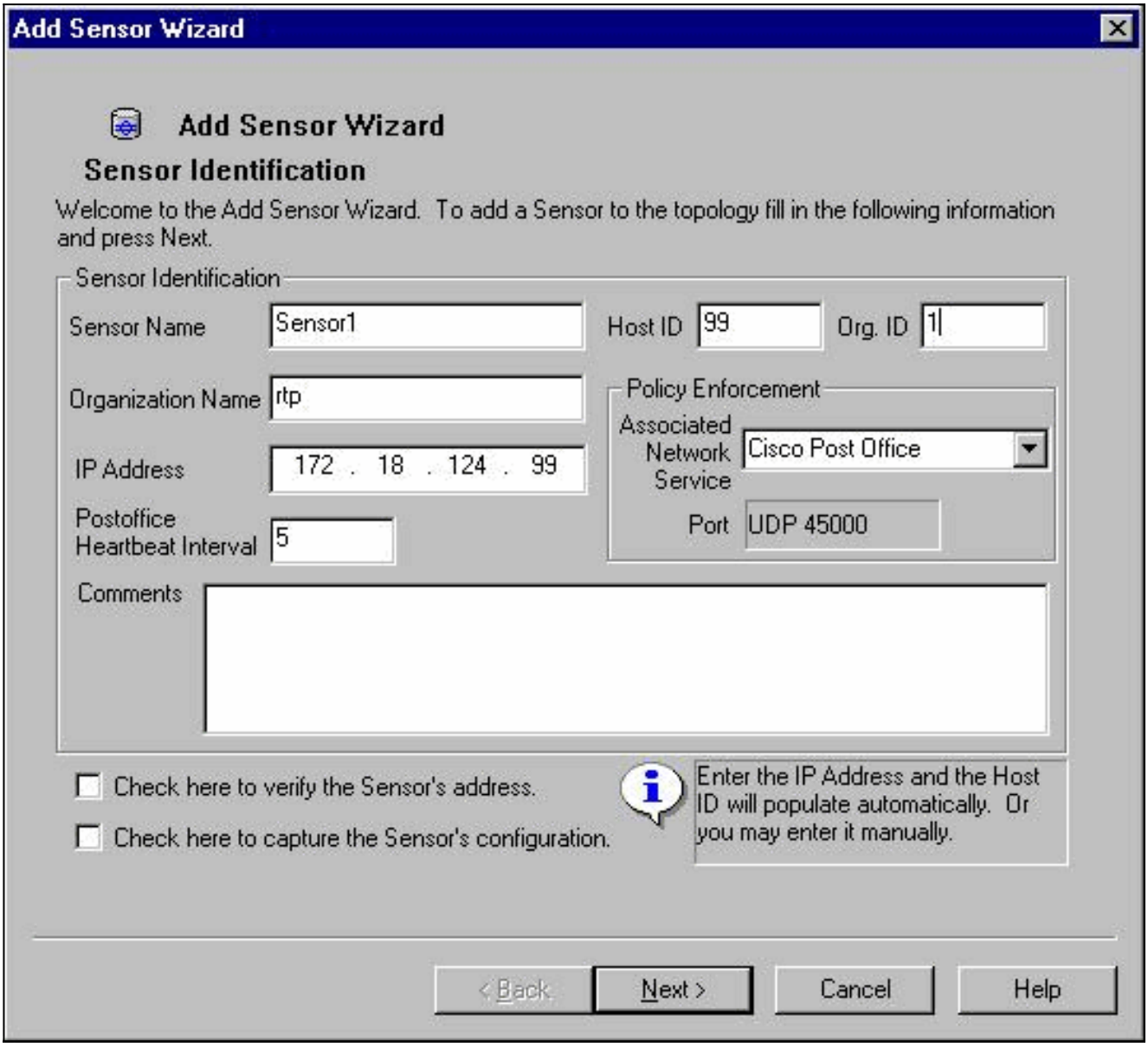
Agregar el dispositivo del sensor

Utilice este procedimiento para agregar el dispositivo sensor.

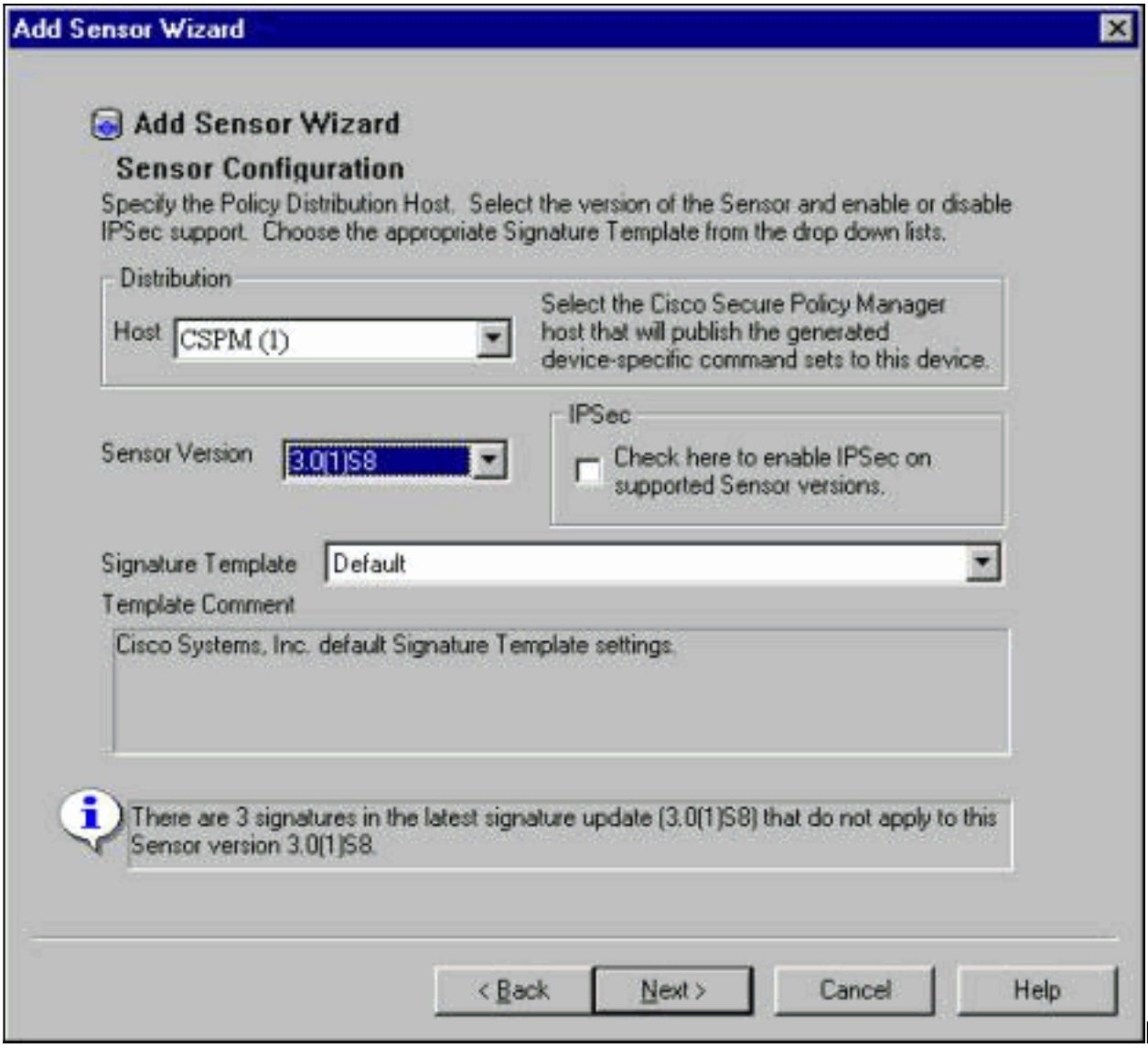
1. Haga clic con el botón derecho del ratón en la red en la cual su sensor reside y seleccione **Wizards > Add Sensor**.**Nota:** Si el host CSPM y la interfaz de control de su sensor no están en la misma red, defina la red en la cual su sensor reside.



2. Ingresar los parámetros correctos de oficina de correos para el sensor.



3. Haga clic en Check here (Verifique aquí) para verificar la casilla de dirección de Sensor.**Nota:** Si esto está la primera vez usted está configurando este sensor, usted no quiere capturar la configuración del sensor. Si usted ha configurado previamente este sensor a otra parte vía un UNIX Director u otro host CSPM y ha realizado los cambios de configuración a las firmas de sensores, después usted quiere capturar la configuración del sensor.
4. Haga clic en Next (Siguiente) para definir las versiones de firma de Sensor. Usted puede también publicar el **comando nrvers** de comprobar esto el sensor.



Nota: Si el CSPM no tiene la versión Sensor correcta que usted está funcionando con en su sensor, ponga al día las firmas en su host CSPM. [Consulte la descarga del software (sólo clientes registrados) para obtener actualizaciones.]

5. Haga clic el **botón Next Button** para continuar.
6. Clic en Finalizar para completar la instalación del sensor en la topología.
7. Del menú principal de CSPM, seleccione File (Archivo) > Save and Update (Guardar y actualizar) para recopilar la información ingresada en la topología en CSPM. Recuerde que este paso es necesario para iniciar el protocolo postoffice en el host CSPM.
8. Verifique que todo trabaje registrando en su sensor como el usuario del netrangr.
9. Ejecute el comando nrconns.`>nrconns Connection Status for gacy.rtp cspm.rtp Connection 1: 172.18.124.106 45000 1 [Established] sto:0004 with Version 1 netrangr@gacy:/usr/nr >`

   Nota: Si el sensor y el host CSPM no están comunicando, la salida similar a esto aparece en lugar de otro:`netrangr@gacy:/usr/nr`

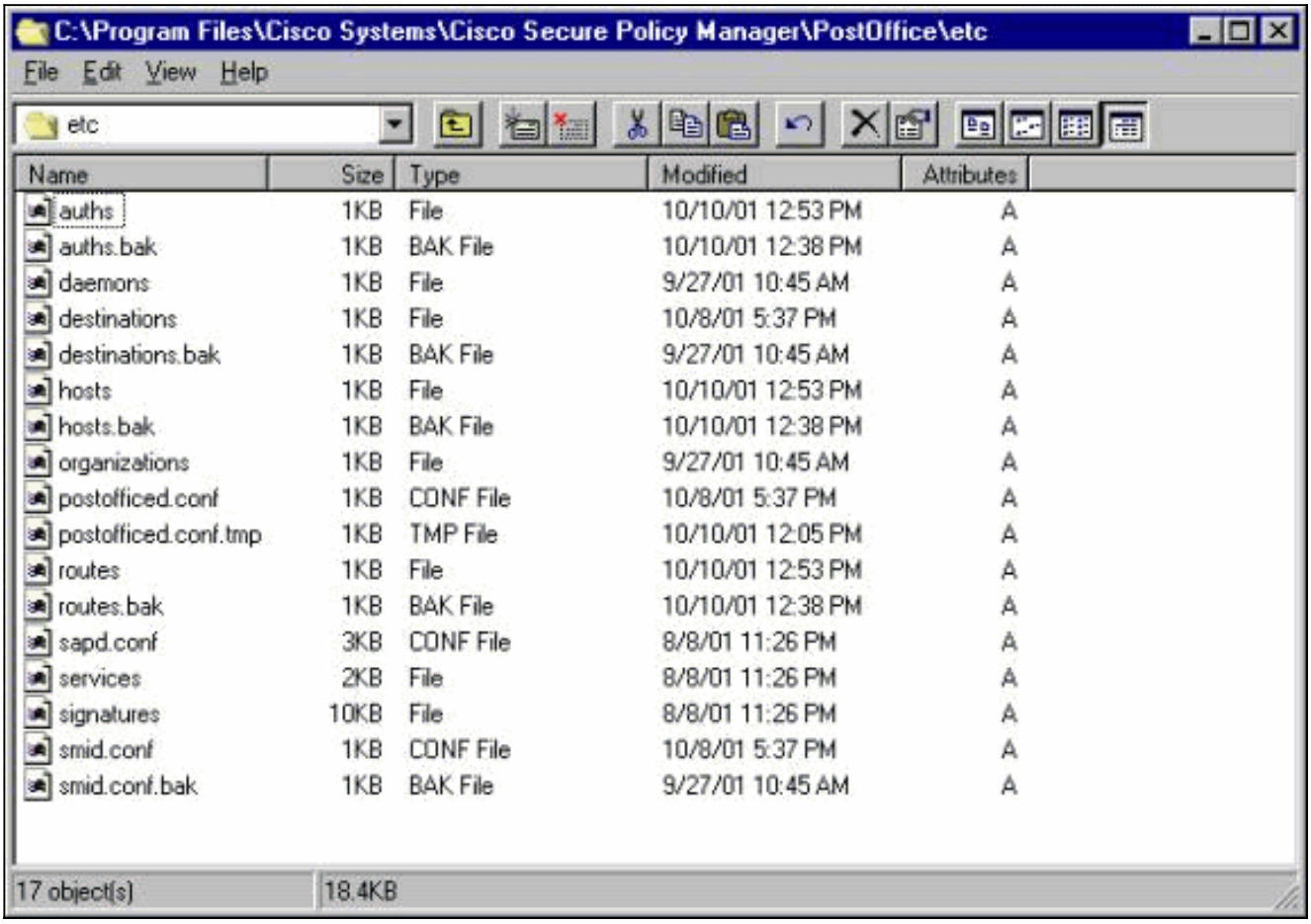
   `>nrconns Connection Status for gacy.rtp insane.rtp Connection 1: 172.18.124.194 45000 1 [SynSent] sto:5000 syn NOT rcvd! netrangr@gacy:/usr/nr` Si éste es el caso, consiga una traza de sniffer para ver si los ambos lados están enviando los paquetes UDP 45000. UDP 45000 el lo que usan los dispositivo IDS para comunicarse entre sí. Para probar esto en el sensor, su para arraigar y (dependiendo de qué sensor usted tiene) para ejecutar al **fisgón - puerto 45000 d iprb1** (para un sensor IDS 4210) y **fisgón - puerto 45000 del iprb0 d** (para cualquier otro modelo del sensor).Utilice el **<control-c>** para explotar de una sesión del fisgón.Esta salida aparece si no hay comunicaciones entre el sensor y el CSPM:`netrangr@gacy:/usr/nr`

```
>su - Password: Sun Microsystems Inc. SunOS 5.8 Generic February 2000 # snoop -d spwr0 port 45000 Using device /dev/spwr (promiscuous mode) 172.18.124.100 -> 172.18.124.106 UDP D=45000 S=45000 LEN=52 172.18.124.100 -> 172.18.124.106 UDP D=45000 S=45000 LEN=52 172.18.124.100 -> 172.18.124.106 UDP D=45000 S=45000 LEN=52 172.18.124.100 -> 172.18.124.106 UDP D=45000 S=45000 LEN=52 ^C#
```

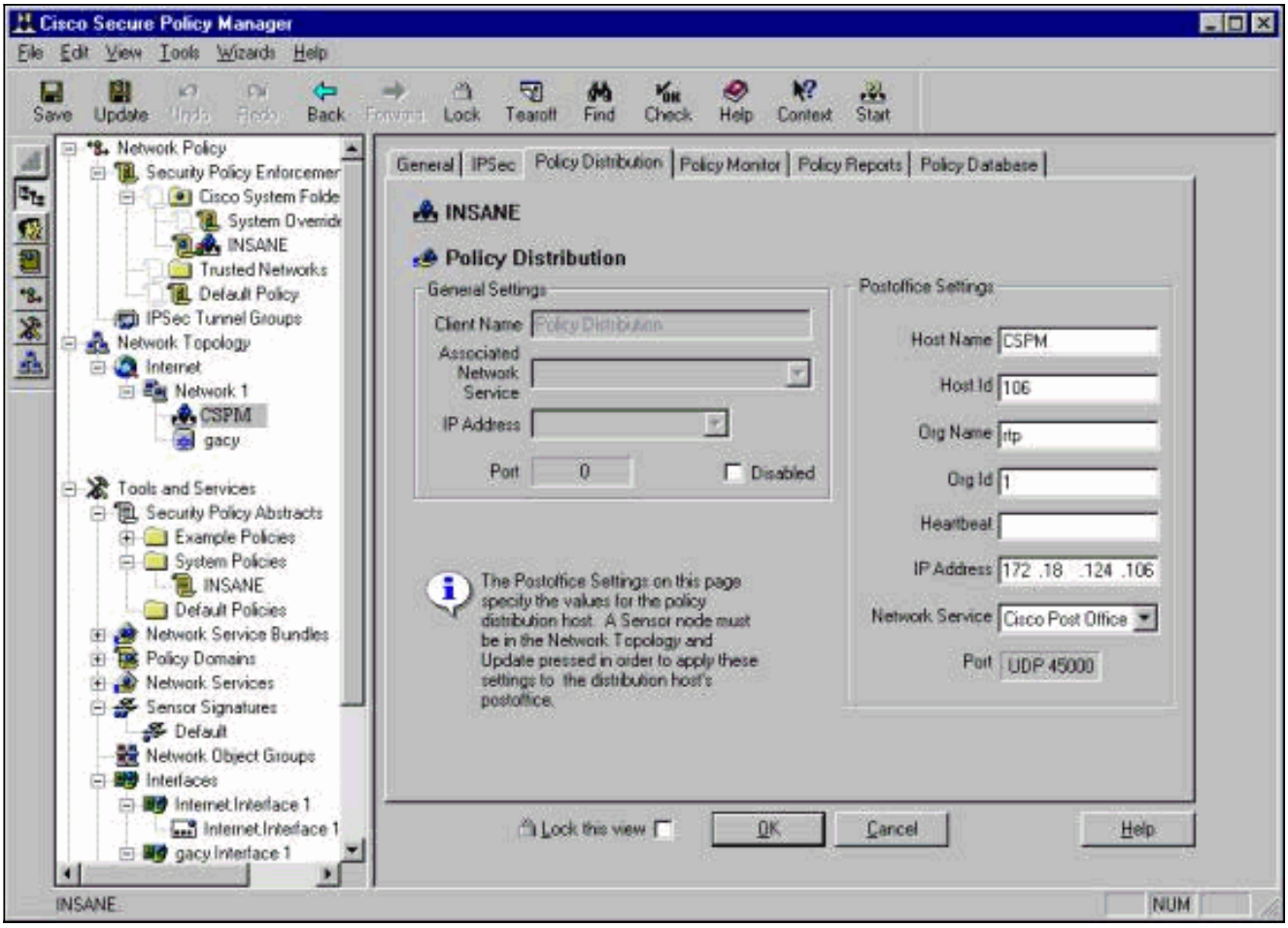
En la salida antedicha, el sensor envía los paquetes UDP 45000, pero no recibe ningunos. Una configuración correcta produce la salida similar a esto:

```
# snoop -d spwr0 port 45000 Using device /dev/iprb (promiscuous mode) 172.18.124.106 -> gacy UDP D=45000 S=45000 LEN=56 gacy -> 172.18.124.106 UDP D=45000 S=45000 LEN=56 172.18.124.142 -> gacy UDP D=45000 S=45000 LEN=56 gacy -> 172.18.124.194 UDP D=45000 S=45000 LEN=56
```

En la salida antedicha, el tráfico UDP 45000 entra en las ambas direcciones.Si los paquetes UDP 45000 fluyen en las ambas direcciones y la salida de los **nrconns** en el sensor todavía dice que no hay conexión establecida, los parámetros de postoffice (oficina de correo) en el sensor y el host CSPM no hacen juego.Para marcar los parámetros de postoffice (oficina de correo) en el CSPM reciba manualmente:Utilice al explorador Explorador de Windows para navegar a donde usted tiene CSPM instalado en la máquina
NT.



Edite el host, ruta, y los archivos de organización con escriben o Wordpad (no utilice la libreta porque el formato será corrompido).Asegúrese de que estos archivos tengan el aspecto adecuado para su instalación. Si los valores uces de los no están correctos, editelos y reinicie su ordenador de NT usando estos pasos:Haga clic en el **icono CSPM** en la topología de red.Haga clic en la lengueta de la distribución de la directiva para ingresar sus parámetros de postoffice (oficina de correo).Guarde y actualice los cambios.Reiniciar la computadora
NT.



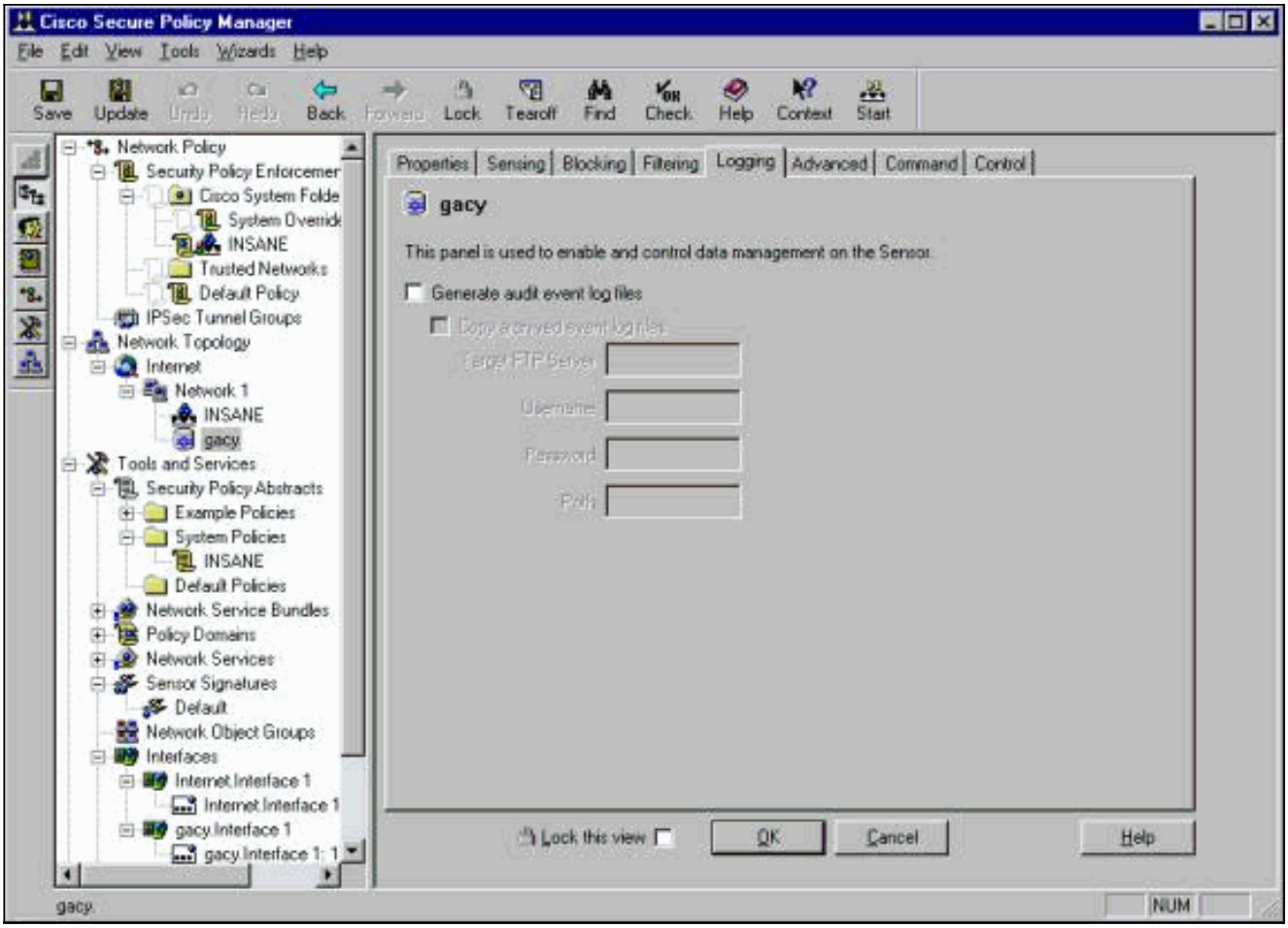
Configure el sensor

Después de que la configuración se guarde en el CSPM, configure el sensor. Para hacer esto, primero fije el sensor para escribir las alarmas que consideran a su propio registro. Entonces fije el sensor “para oler” en la interfaz correcta.

Escriba alarmas en el registro

Utilice este procedimiento para escribir las alarmas al registro.

1. Haga clic en el cuadro Generate audit event log files para indicarle al Sensor que envíe alertas a los registros locales.También envía las alarmas al cuadro CSPM por abandono después de que usted empuje una configuración hacia abajo a ella.

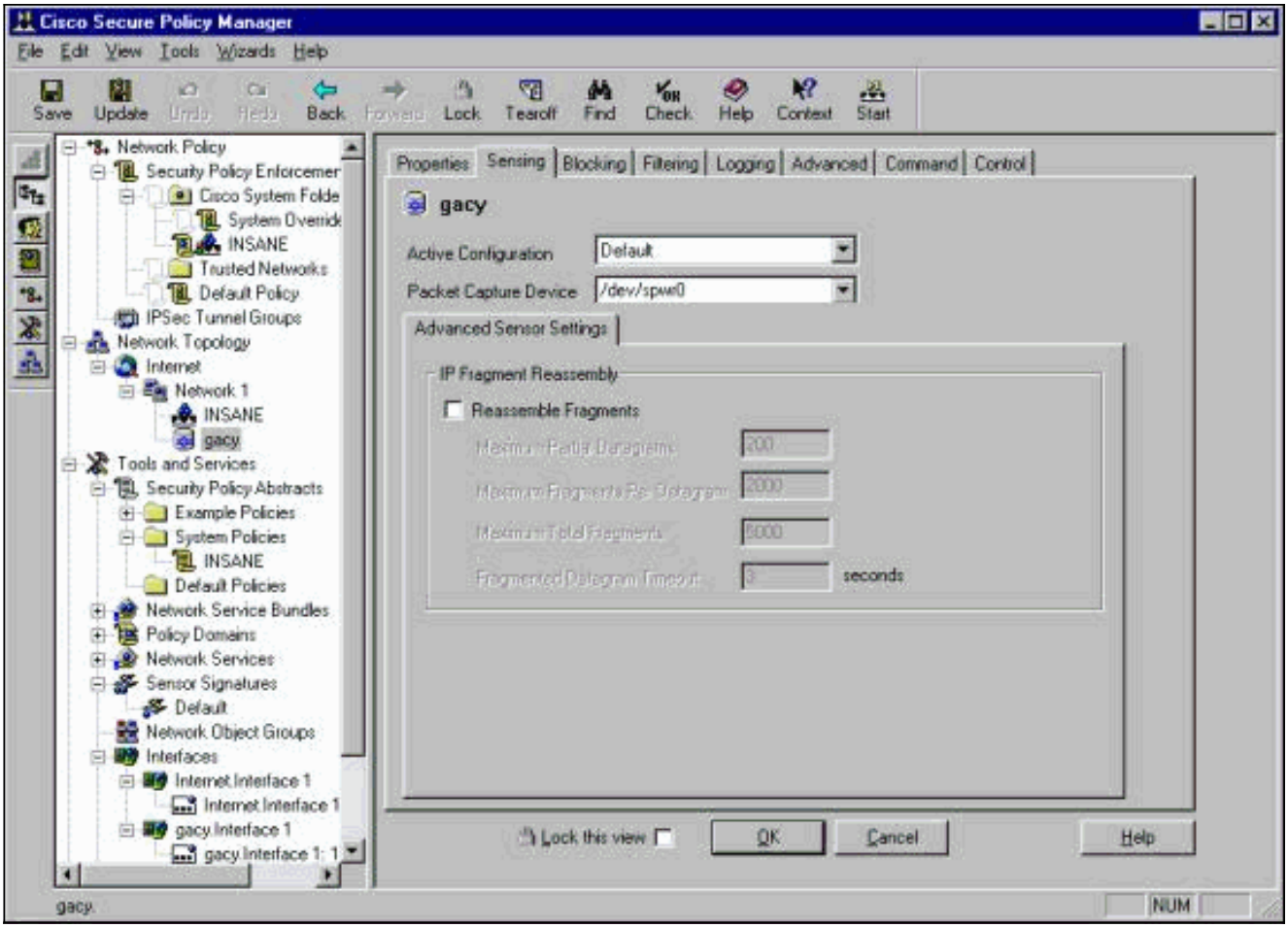


2. Para continuar, haga clic en OK (Aceptar).

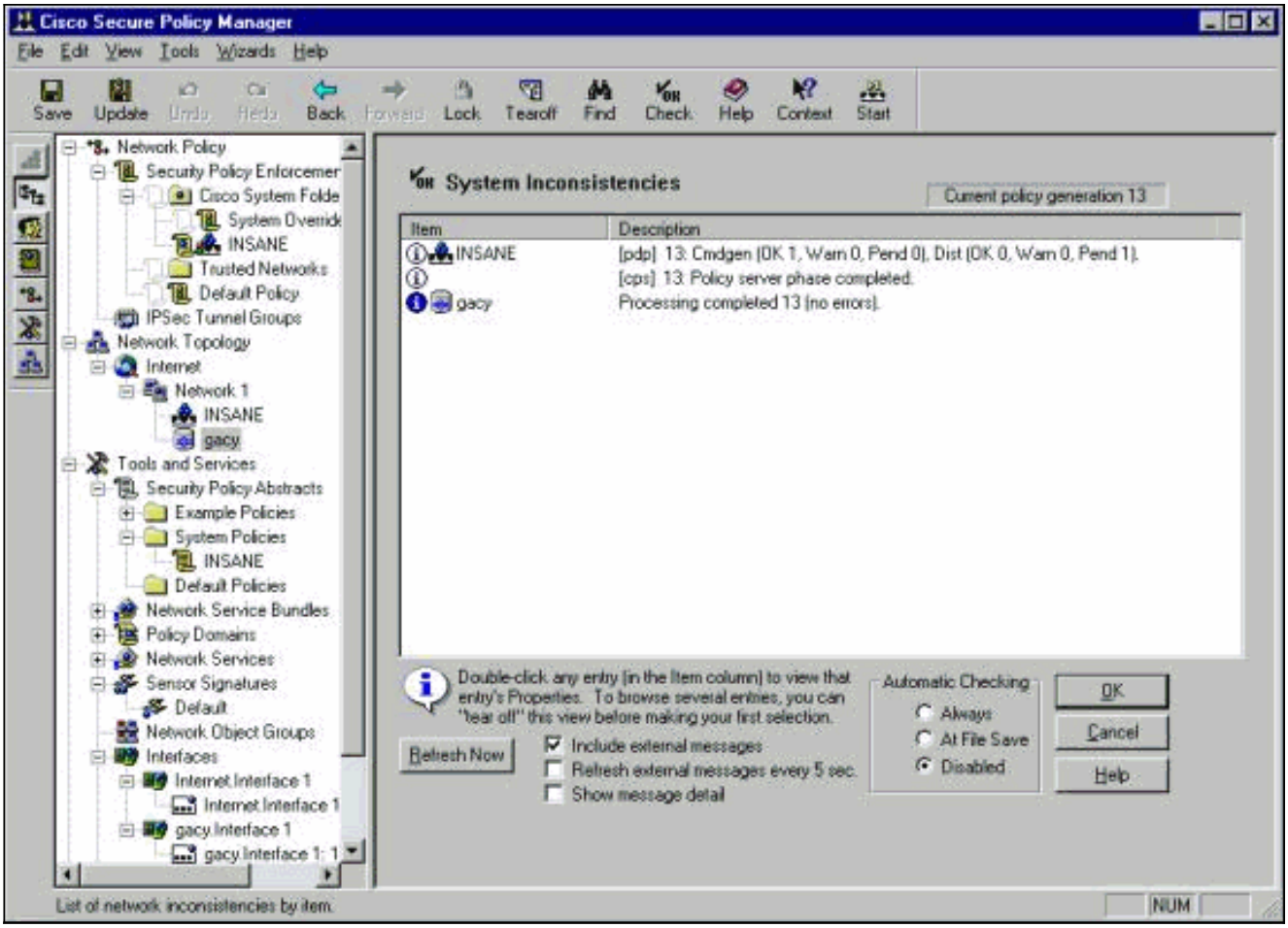
Fije el sensor “para oler”

Utilice este procedimiento para fijar el sensor “para oler”.

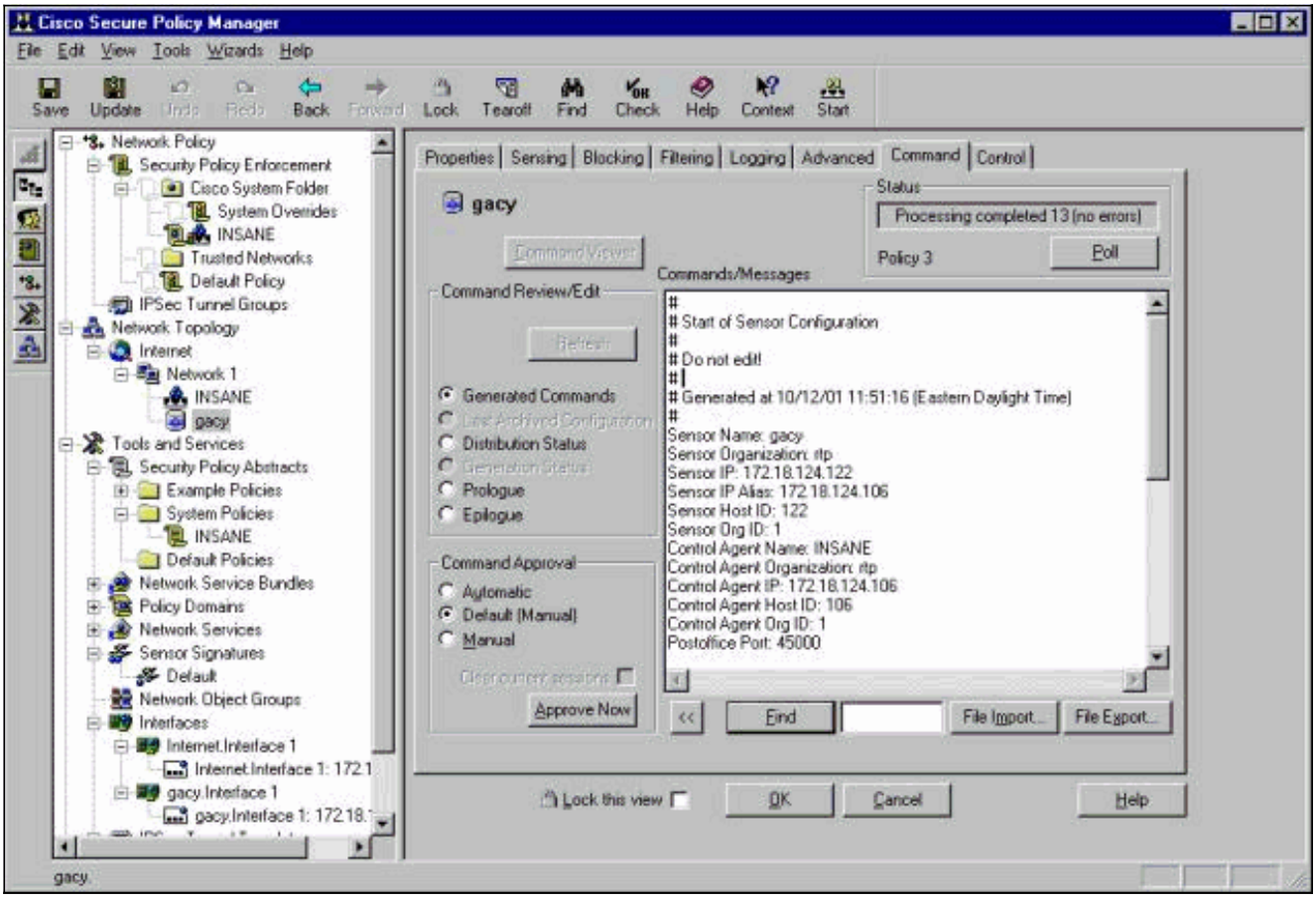
1. Seleccione el sensor en su topología de CSPM y haga clic en la ficha Sensing (Detección).
2. Defina el dispositivo de captura de paquetes:iprb0 - para un sensor IDS 4210spwr0 - para cualquier otro modelo del
   sensor



3. Para continuar, haga clic en OK (Aceptar).
4. Haga clic en el icono Update (actualizar) de la barra de menú CSPM para actualizar el CSPM con la información.**Nota:** Si va todo bien, una pantalla similar a esto aparece. Observe que no hay errores en rojo. Normalmente, las advertencias amarillas están bien.

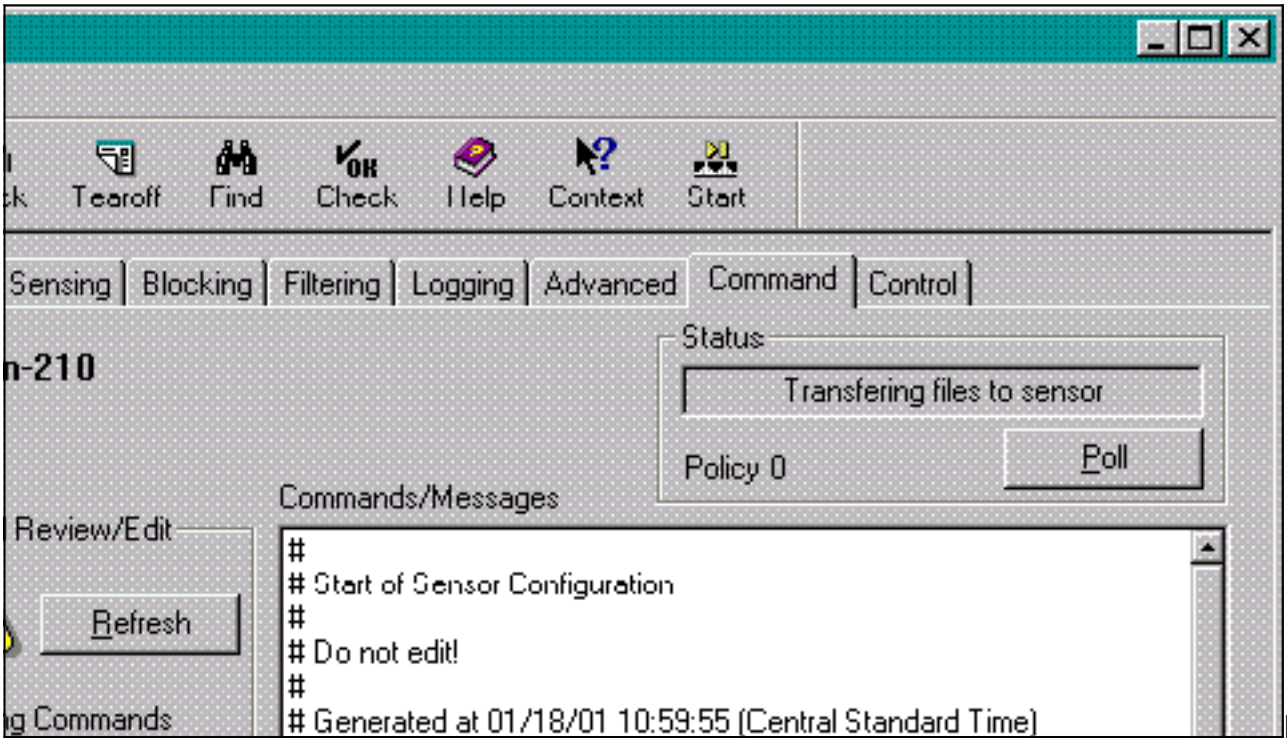


5. Seleccione el sensor en la topología de red y haga clic en la ficha Command (Comando) para enviarle la configuración actualizada al sensor.

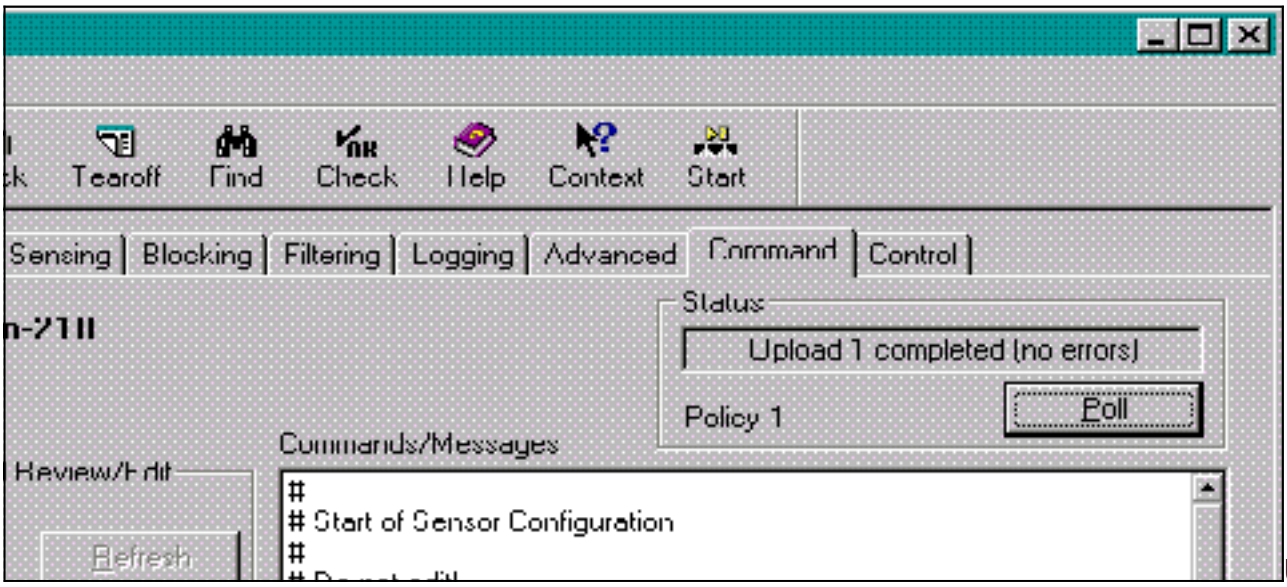


6. Haga clic el **botón Approve Now Button** para enviar la configuración al

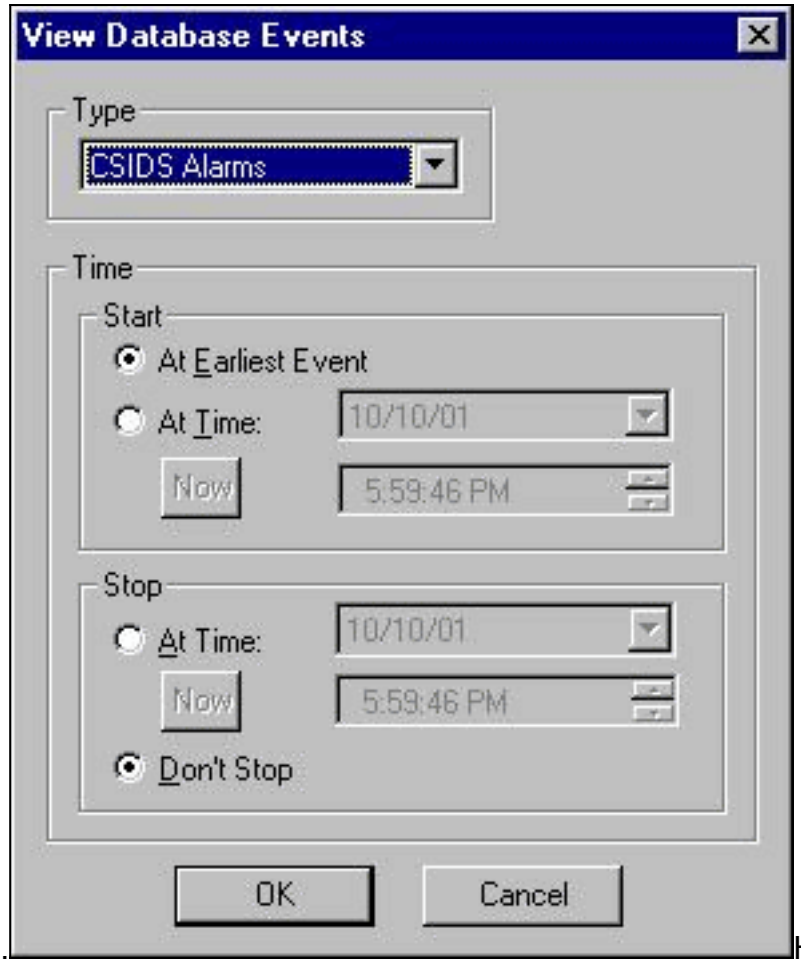
sensor.



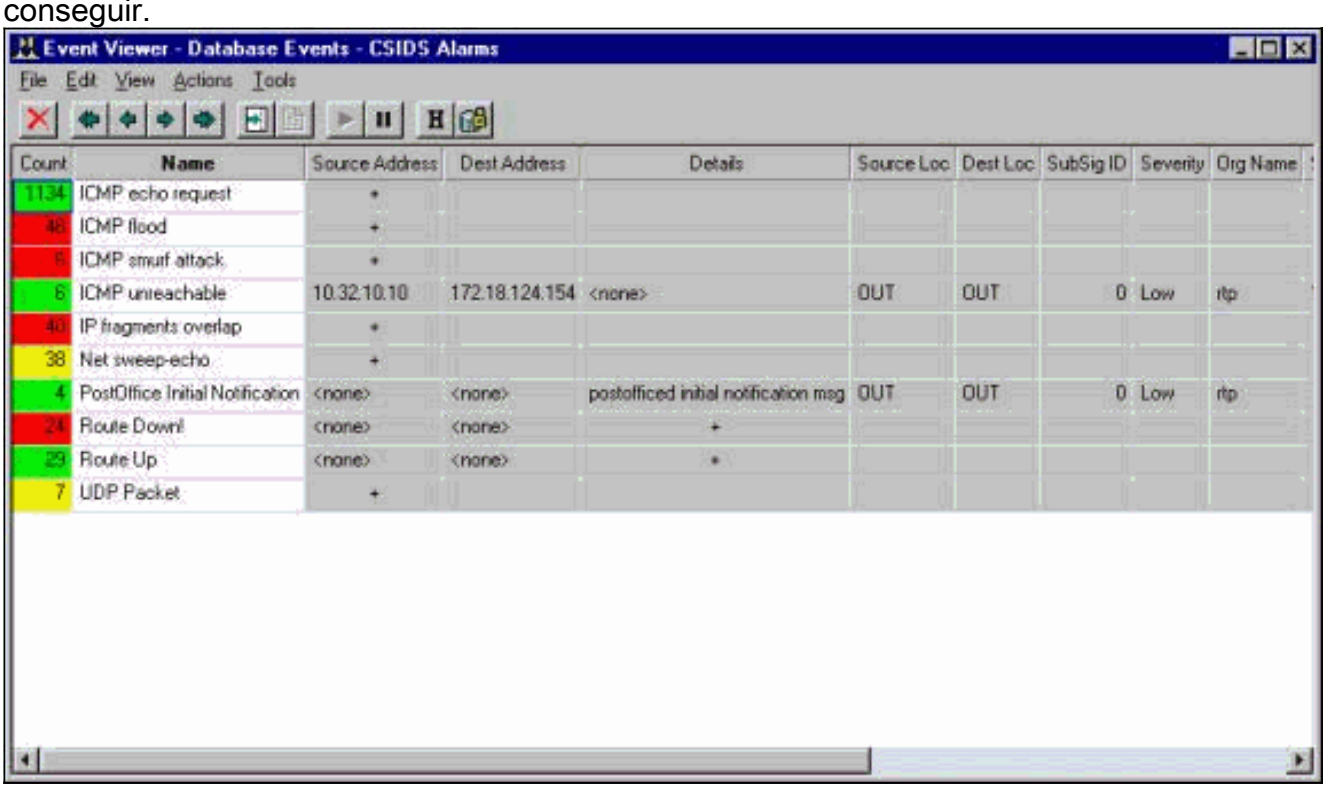
El cristal del estatus visualiza el mensaje completado **<#>** de la “carga”. Esto indica un proceso válido y completo de la transferencia. El sensor ahora se pone al día y debe ahora ejecutarse normalmente.Si el Sensor no funciona normalmente, vaya al Sensor y verifique la salida del comando nrconns para asegurarse de que la conexión entre el host CSPM y el Sensor esté
establecida.



Una vez realizado esto, puede buscar las alarmas que el sensor envía al host CSPM en el visor de eventos. Para ver el visor de eventos, de las **herramientas del** menú principal CSPM **>** de los **eventos >** de la **base de datos** selectos del **sensor de la**



visión. Haga clic en OK (Aceptar) para ver la ventana de base de datos de eventos. Su pantalla variará dependiendo de las alarmas que usted puede conseguir.



Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems