Configuración Reset TCP (reinicio TCP) mediante el director IDS

Contenido

Introducción

Este documento describe cómo configurar un director del sistema de la detección de intrusos (IDS, antes Netranger) y un sensor para enviar las restauraciones TCP en Telnet frustrado a un rango de direcciones que incluyen al router manejado si la cadena enviada es “testattack”.

prerrequisitos

Requisitos

Cuando en vista de esta configuración, recuerde por favor a:

- Instale el sensor y verifiquelo que trabaja correctamente antes de que usted realice esta configuración.
- Asegúrese de que los palmos de la interfaz de rastreo a la interfaz exterior del router manejado.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y

hardware.

- Cisco IDS Director 2.2.3
- Sensor 3.0.5 del Cisco IDS
- Software Release 12.2.6 corriente del router del ® del Cisco IOS

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.

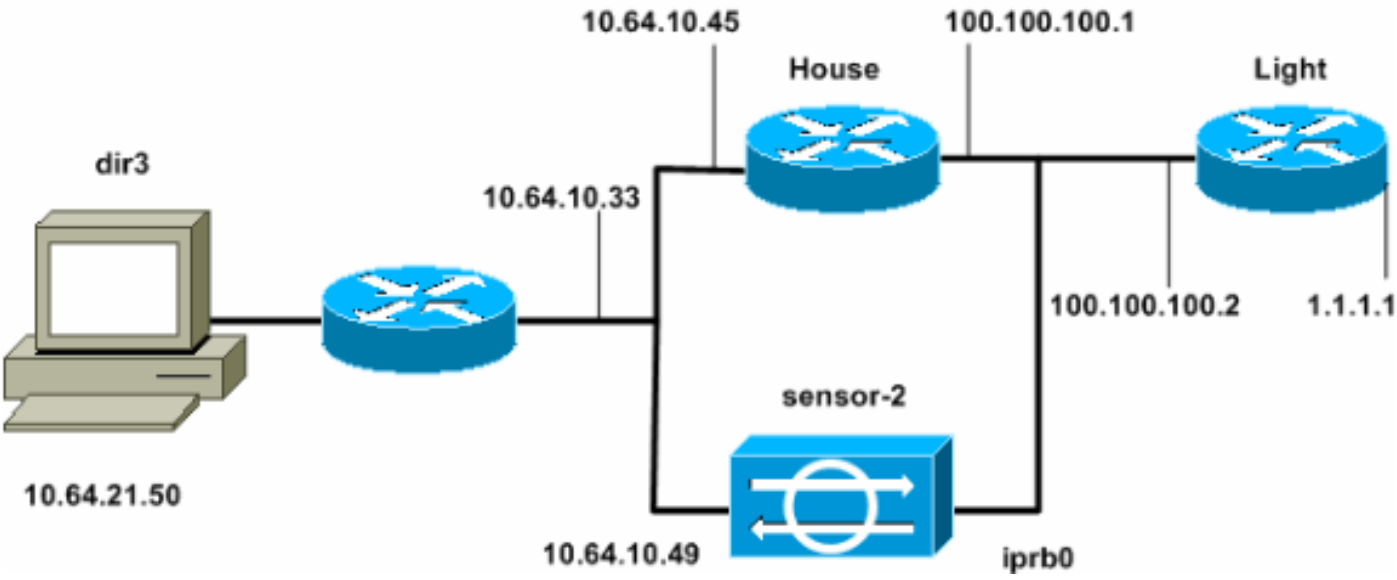
Configurar

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

Nota: Para obtener información adicional sobre los comandos que se utilizan en este documento, use la Command Lookup Tool (solo para clientes registrados).

Diagrama de la red

Este documento utiliza la configuración de red que se muestra en el siguiente diagrama.



Configuraciones

Este documento usa estas configuraciones.

- Luz del router
- Base del router

Luz del router

```
Current configuration : 906 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname light ! enable password cisco ! username cisco
password 0 cisco ip subnet-zero ! ! ! ip ssh time-out
120 ip ssh authentication-retries 3 ! call rsvp-sync ! !
! fax interface-type modem mta receive maximum-
recipients 0 ! controller E1 2/0 ! ! ! interface
FastEthernet0/0 ip address 100.100.100.2 255.255.255.0
duplex auto speed auto ! interface FastEthernet0/1 ip
address 1.1.1.1 255.255.255.0 duplex auto speed auto !
interface BRI4/0 no ip address shutdown ! interface
BRI4/1 no ip address shutdown ! interface BRI4/2 no ip
address shutdown ! interface BRI4/3 no ip address
shutdown ! ip classless ip route 0.0.0.0 0.0.0.0
100.100.100.1 ip http server ip pim bidir-enable ! !
dial-peer cor custom ! ! line con 0 line 97 108 line aux
0 line vty 0 4 login ! end
```

Base del router

```
Current configuration : 2187 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname house ! enable password cisco ! ! ! ip subnet-
zero ! ! fax interface-type modem mta receive maximum-
recipients 0 ! ! ! ! interface FastEthernet0/0 ip
address 100.100.100.1 255.255.255.0 duplex auto speed
auto ! interface FastEthernet0/1 ip address 10.64.10.45
255.255.255.224 duplex auto speed auto ! ! ! interface
FastEthernet4/0 no ip address shutdown duplex auto speed
auto ! ip classless ip route 0.0.0.0 0.0.0.0 10.64.10.33
ip route 1.1.1.0 255.255.255.0 100.100.100.2 ip http
server ip pim bidir-enable ! ! ! snmp-server manager !
call rsvp-sync ! ! mgcp profile default ! dial-peer cor
custom ! ! ! ! line con 0 line aux 0 line vty 0 4
password cisco login ! ! end house#
```

Configure el sensor

Complete estos pasos para configurar el sensor.

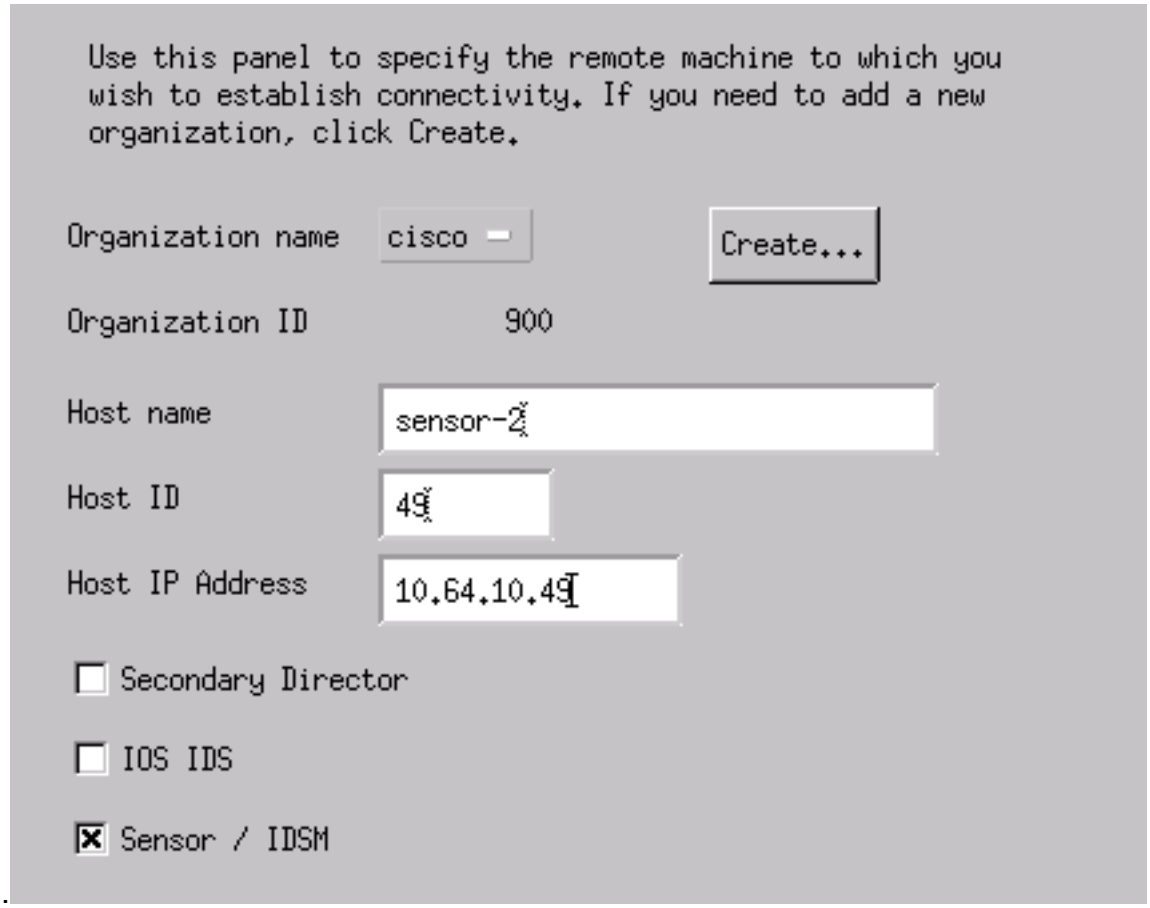
1. Telnet a 10.64.10.49 (el sensor IDS) con el nombre de usuario raíz y el ataque de contraseña.
2. **Sysconfig-sensor del** tipo.
3. Cuando se le pregunte, ingrese la información de la configuración, tal y como se muestra en de este ejemplo:`1 - IP Address: **10.64.10.49** 2 - IP Netmask: **255.255.255.224** 3 - IP Host Name: **sensor-2** 4 - Default Route: **10.64.10.33** 5 - Network Access Control **64. 10.** 6 - Communications Infrastructure Sensor Host ID: **49** Sensor Organization ID: **900** Sensor Host Name: **sensor-2** Sensor Organization Name: **cisco** Sensor IP Address: **10.64.10.49** IDS Manager Host ID: **50** IDS Manager Organization ID: **900** IDS Manager Host Name: **dir3** IDS Manager Organization Name: **cisco** IDS Manager IP Address: **10.64.21.50**`

4. Cuando se le pregunte, salve la configuración y permita que el sensor reinicie.

Agregue el sensor en el director

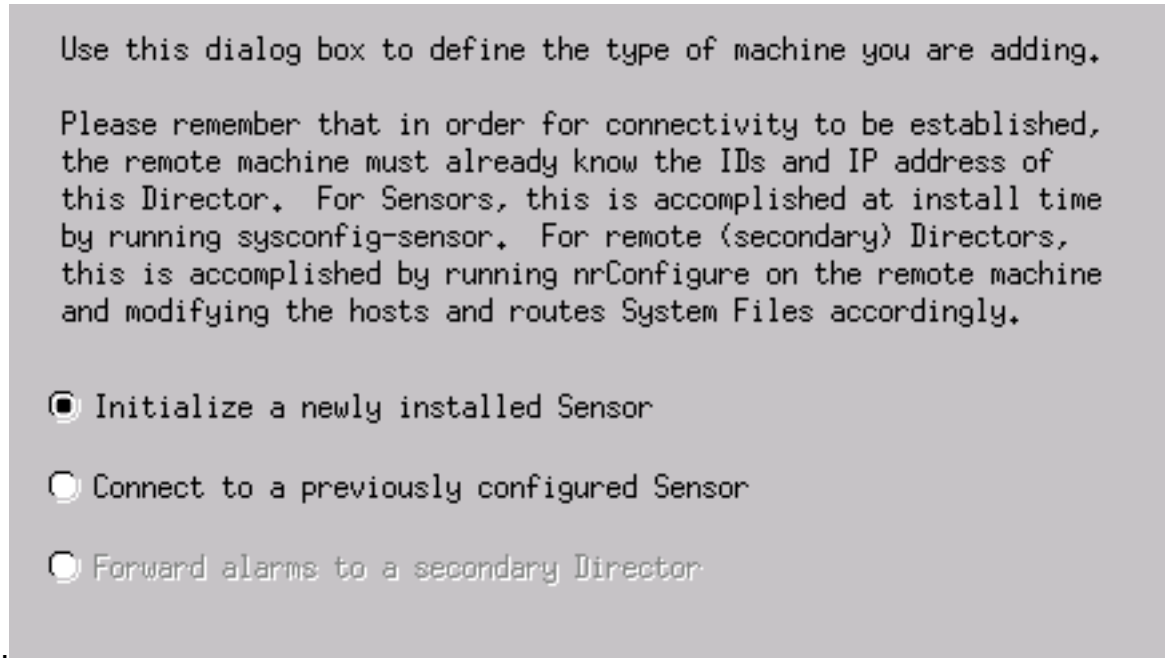
Complete estos pasos para agregar el sensor en el director.

1. Telnet a 10.64.21.50 (el director IDS) con el **netrangr del** nombre de usuario y el ataque de contraseña.
2. **Ovw& del** tipo para poner en marcha el HP OpenView.
3. Del menú principal, vaya al **Security (Seguridad) > Configure (Configurar)**.
4. En la utilidad de la administración de archivos de configuración, vaya a **file > add host** y haga clic **después**.
5. Complete la información del host del sensor, tal y como se muestra en de este ejemplo. Haga clic en Next



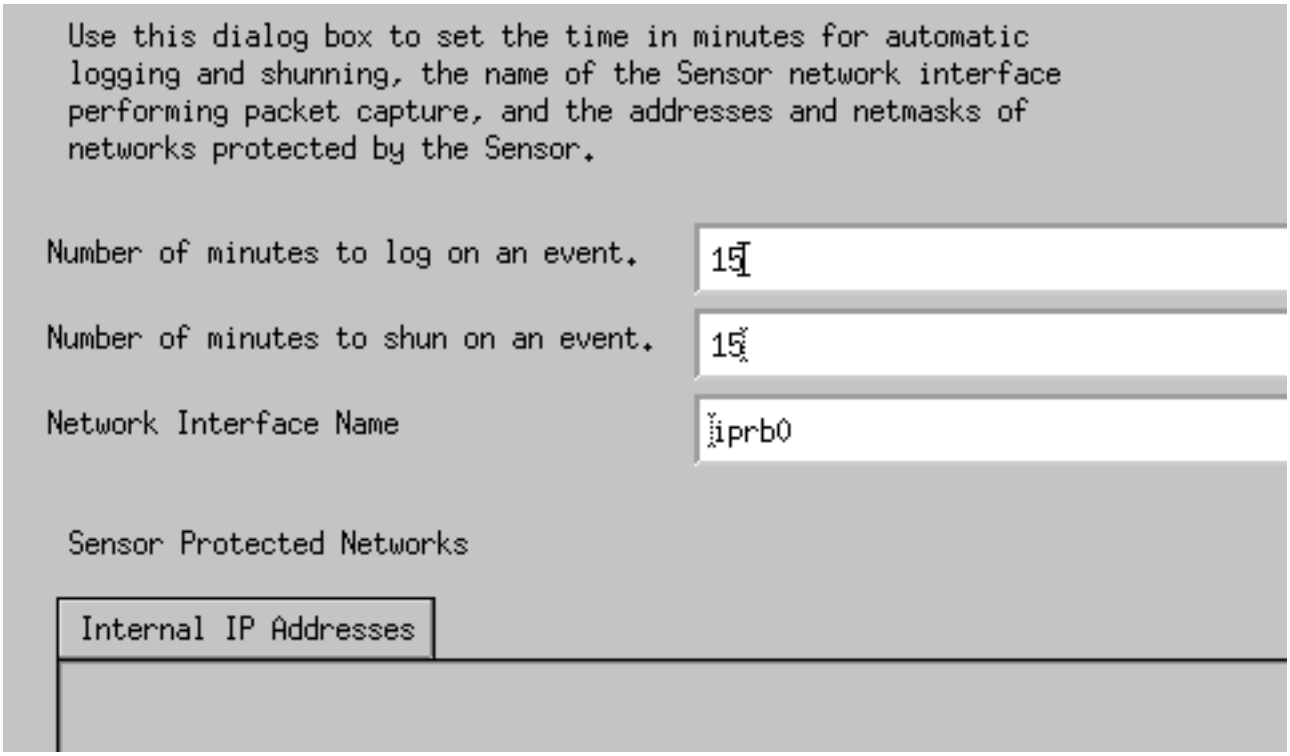
(Siguiente).

6. Valide las configuraciones predeterminadas para el tipo de máquina, y haga clic **después**, tal y como se muestra en de este

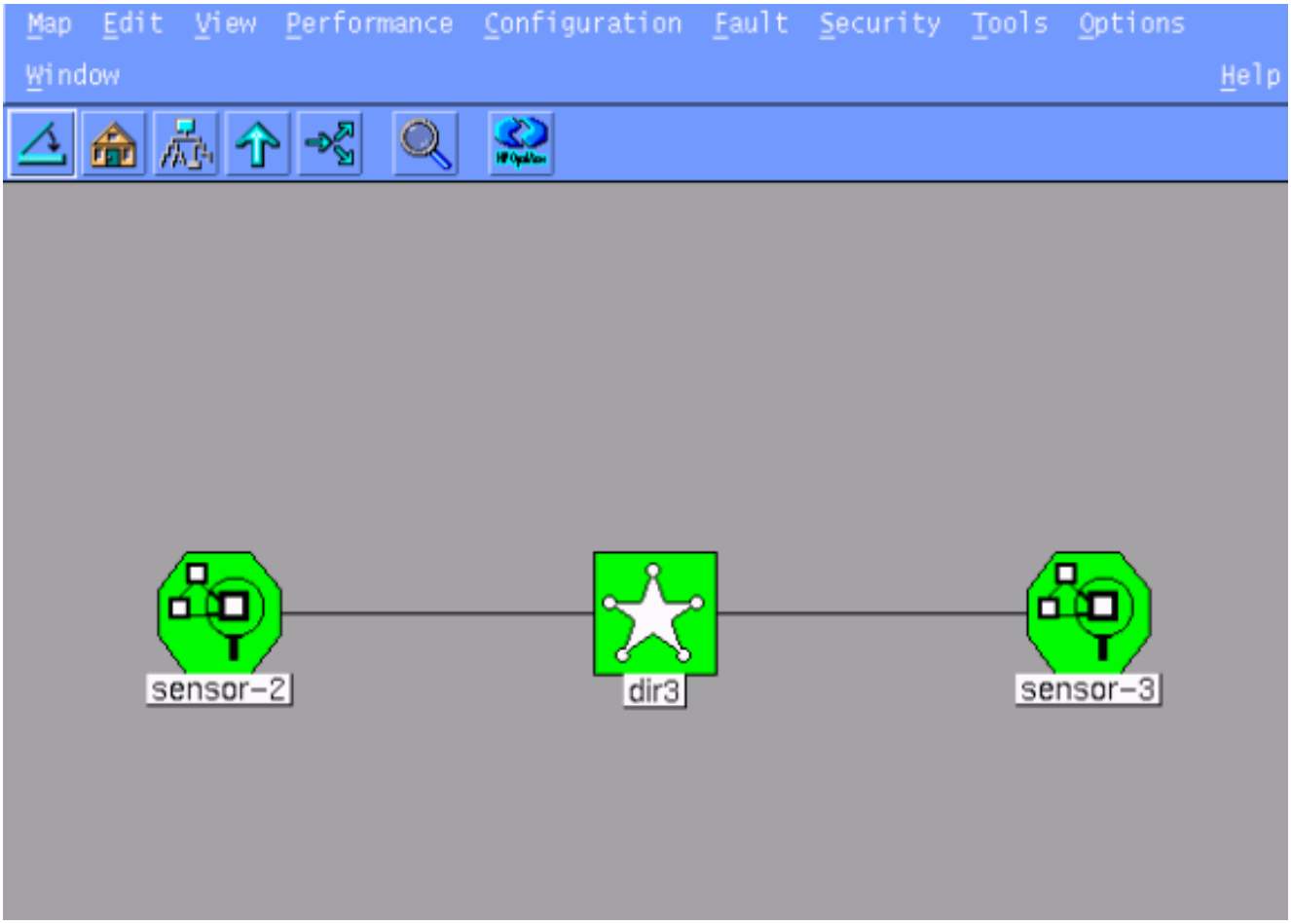


ejemplo.

7. Usted puede cambiar el registro y evitar los minutos o le puede validar los valores predeterminados. Sin embargo, usted debe cambiar el nombre de la interfaz de red al nombre de su interfaz de rastreo. En este ejemplo, es el "iprb0". Puede ser el "spwr0" o cualquier otra cosa dependiendo del tipo de sensor y cómo usted conecta su sensor.



8. Continúe **después** y después haciendo clic clic en Finalizar para agregar el sensor en el director. Del menú principal, usted debe ahora ver el sensor 2, como en este ejemplo.

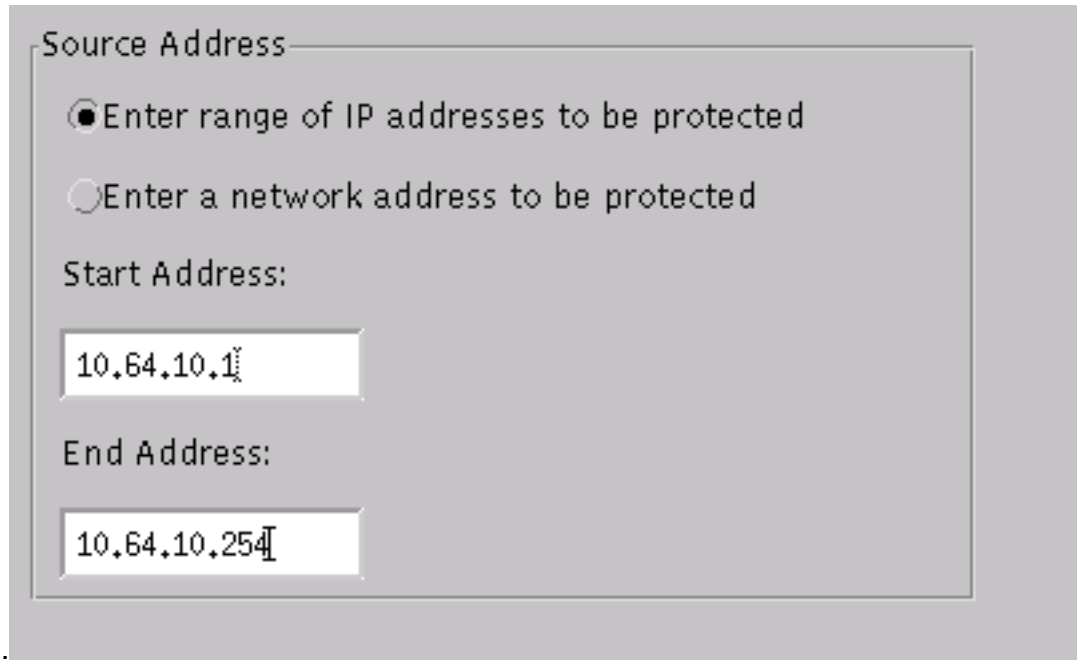


Restablecimiento TCP de la configuración para el router del Cisco IOS

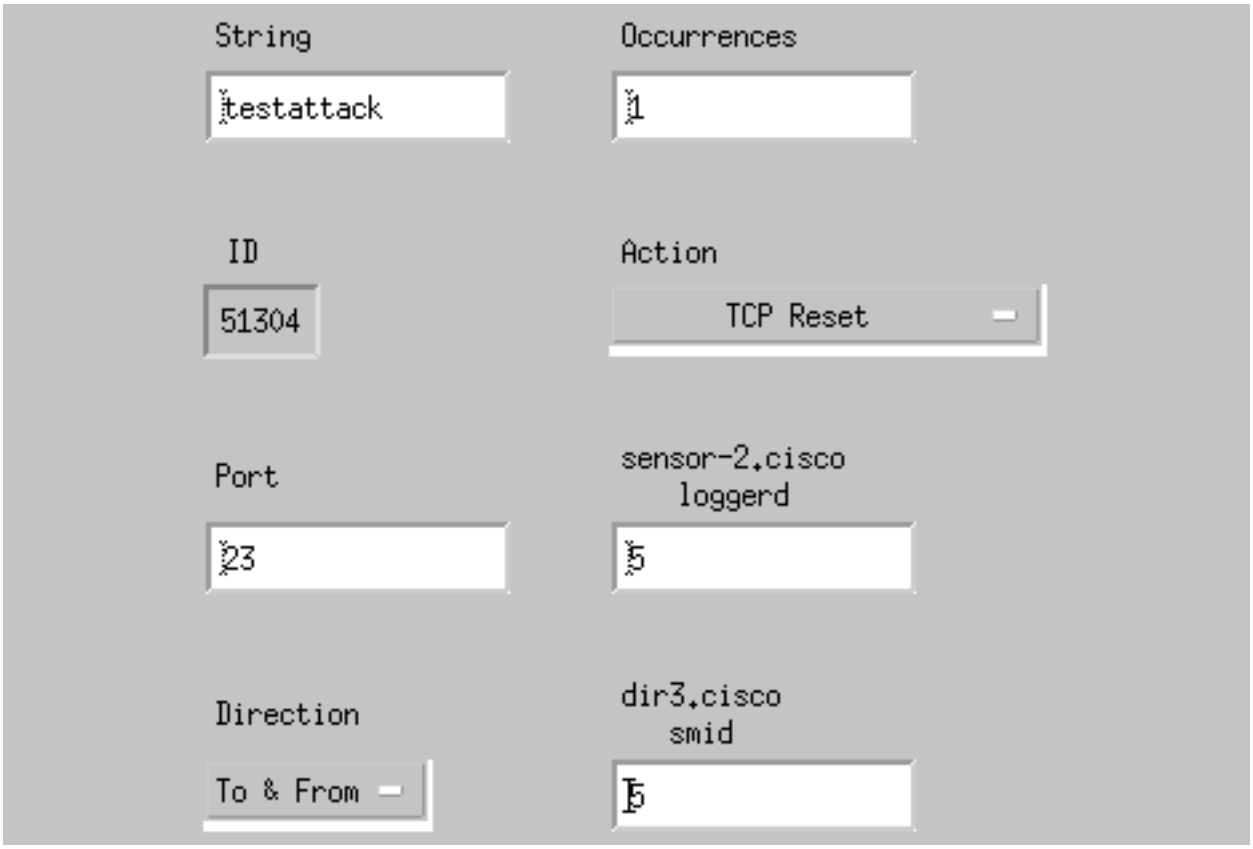
Complete estos pasos para configurar el Restablecimiento TCP para el router del Cisco IOS.

1. En el menú principal, vaya al **Security (Seguridad) > Configure (Configurar)**.
2. En la utilidad de la administración de archivos de configuración, resalte el **sensor 2** y hagalo doble clic.
3. Abra la Administración de dispositivos.
4. Haga clic el **Devices (Dispositivos) > Add (Agregar)**. Ingrese la información del dispositivo, tal y como se muestra en del siguiente ejemplo. Para continuar, haga clic en OK (Aceptar). Telnet y las contraseñas habilitadas son
   Cisco.

5. Abra la ventana de la detección de intrusos y haga clic las **redes protegidas**. Agregue el rango de direcciones de 10.64.10.1 a 10.64.10.254 en la red protegida.

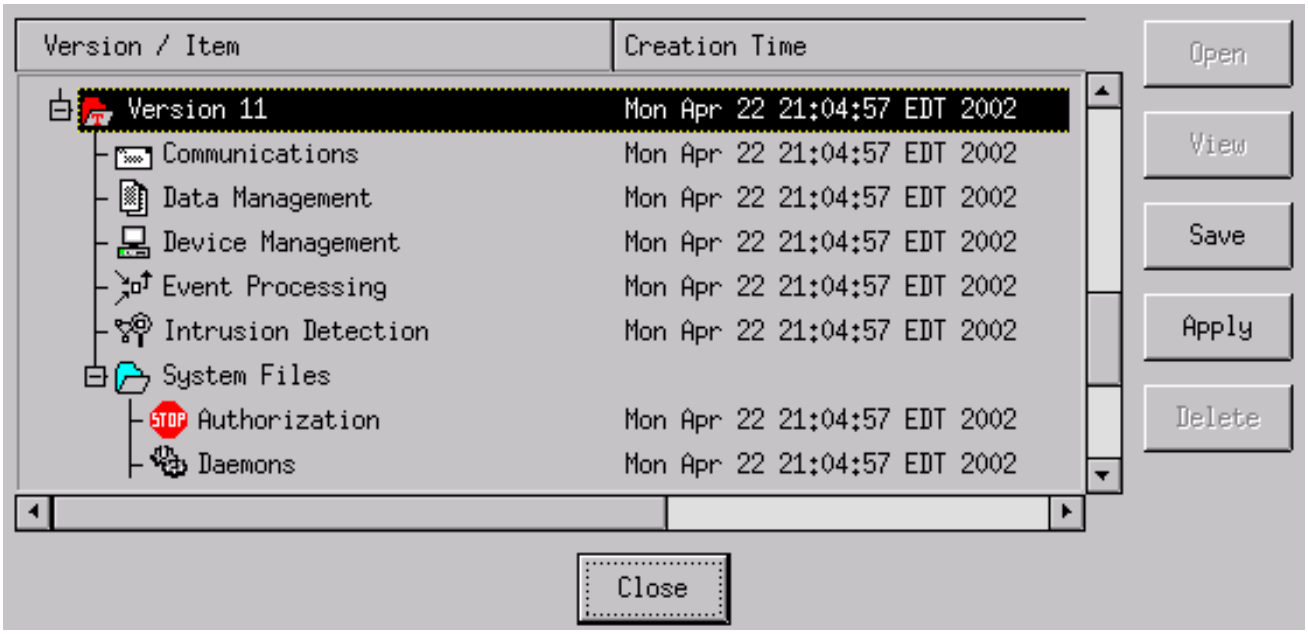


6. Haga clic el **perfil** y seleccione la **configuración manual**. Después, el tecleo **modifica las firmas**. Elija las **cadenas correspondidas con** con un ID de 8000. Haga clic **Expand > Add** para agregar una nueva cadena llamada **testattack**. Ingrese la información de la cadena, tal y como se muestra en de este ejemplo, y haga clic la **AUTORIZACIÓN** para continuar.



7. Usted ha acabado a esta parte de la configuración. Haga Click en OK para cerrar la ventana de la detección de intrusos.
8. Abra la carpeta de archivos del sistema, entonces la ventana de Daemons. Aseegurese le hacer estas daemones
   habilitar:

9. Para continuar, haga clic en OK (Aceptar).
10. Elija la versión que usted acaba de modificarse, haga clic la **salvaguardia** y después **apliqúese**. Espere el sistema para decirle que el sensor ha acabado de recomenzar los servicios, después cierran todas las ventanas para la configuración del director.



Inicie el ataque y reinicie TCP

Telnet del indicador luminoso del router al **testattack de la** Casa y del tipo del router. Tan pronto como usted golpeara el espacio o tecla Enter (Intro), sus restauraciones de la sesión telnet. Usted conectará con la Casa del router.

```
light#telnet 10.64.10.45 Trying 10.64.10.45 ... Open User Access Verification Password: house>en
Password: house#testattack [Connection to 10.64.10.45 closed by foreign host] !--- Telnet
session has been reset because the !--- signature testattack was triggered.
```

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Telnet a 10.64.10.49, el sensor, usando el nombre de usuario raíz y el ataque de contraseña. **Cd /usr/nr/etc del** tipo. **Gato packetd.conf del** tipo**. Si** usted fija correctamente el Restablecimiento TCP para el testattack, usted debe ver cuatro (4) en el campo de los códigos de acción. Esto indica el Restablecimiento TCP tal y como se muestra en de este ejemplo.

```
netrangr@sensor-2:/usr/nr/etc
>cat packetd.conf | grep "testattack" RecordOfStringName 51304 23 3 1 "testattack"
SigOfStringMatch 51304 4 5 5 # "testattack"
```

Si usted fija accidentalmente la acción a “ningunos” en la firma, usted verá un cero (0) en el campo de los códigos de acción. Esto no indica ninguna acción como se ve en este ejemplo.

```
netrangr@sensor-2:/usr/nr/etc
>cat packetd.conf | grep "testattack" RecordOfStringName 51304 23 3 1 "testattack"
SigOfStringMatch 51304 0 5 5 # "testattack"
```

Las restauraciones TCP se envían de la interfaz de rastreo del sensor. Si hay un Switch que conecta la interfaz del sensor con la interfaz exterior del router manejado, cuando usted configura usando el **comando set span** en el Switch, utilice este sintaxis:

```
set span <src_mod/src_port><dest_mod/dest_port> both inpkts enable banana (enable) set span 2/12
3/6 both inpkts enable Overwrote Port 3/6 to monitor transmit/receive traffic of Port 2/12
Incoming Packets enabled. Learning enabled. Multicast enabled. banana (enable) banana (enable)
banana (enable) show span Destination : Port 3/6 !--- Connect to sniffing interface of the
Sensor. Admin Source : Port 2/12 !--- Connect to FastEthernet0/0 of Router House. Oper Source :
Port 2/12 Direction : transmit/receive Incoming Packets: enabled Learning : enabled Multicast :
enabled
```

Información Relacionada

- Avisos de problemas
- Página de soporte segura de la prevención de intrusiones de Cisco
- Soporte Técnico y Documentación - Cisco Systems