Configurar evitar en un UNIX Director

Contenido

Introducción

El director y el sensor del Sistema de detección de intrusos de Cisco (IDS) pueden ser utilizados para manejar a un router Cisco para evitar. En este documento, un sensor (sensor 2) se configura para detectar los ataques en el router “Casa” y para comunicar esta información al director el "dir3." configurado una vez, un ataque se inicia (el ping de más en gran parte de 1024 bytes, que es la firma 2151, y de una inundación del [ICMP] del protocolo Protocolo de control de mensajes de Internet (ICMP), que es la firma 2152) del router la “luz.” El sensor detecta el ataque y comunica esto al director. Una lista de control de acceso (ACL) se descarga al router para evitar el tráfico del atacante. En el atacante `imposible acceder al host` se muestra, y en la víctima se muestra el ACL descargado.

prerrequisitos

Requisitos

Antes de utilizar esta configuración, asegúrese de que cumple con los siguientes requisitos:

- Instale el sensor y aseegurese lo trabaja correctamente.
- Asegúrese de que los palmos de la interfaz de rastreo a la interfaz exterior del router.

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
- Router del ® del Cisco IOS con 12.2.6

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

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

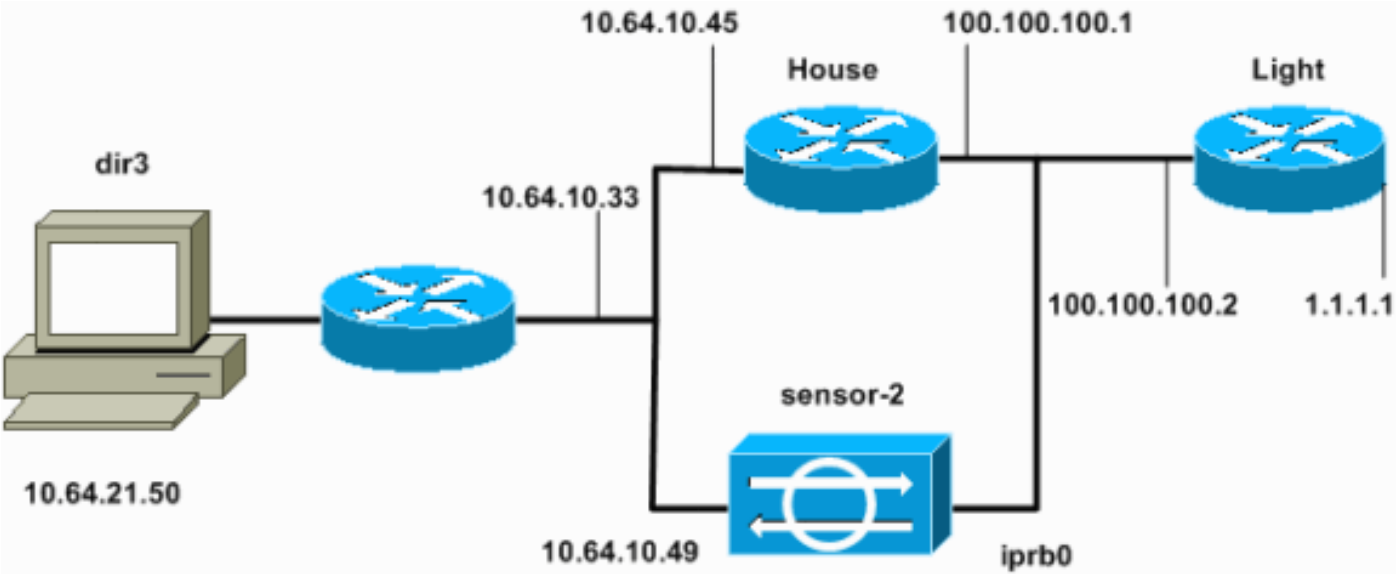
Configurar

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
!
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
!--- After you configure shunning, IDS Sensor puts this
line in. ip access-group IDS_FastEthernet0/0_in_1 in


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
!
!
!--- After you configure shunning, IDS Sensor puts these
lines in. ip access-list extended IDS_FastEthernet0/0_in
deny ip host 100.100.100.2 any
permit ip host 10.64.10.49 any
 permit ip any any

!
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** con el nombre de usuario raíz y el ataque de contraseña.
2. Ingrese el sysconfig-**sensor**.
3. Cuando se le pregunte, ingrese la información de la configuración, tal y como se muestra en de este ejemplo.

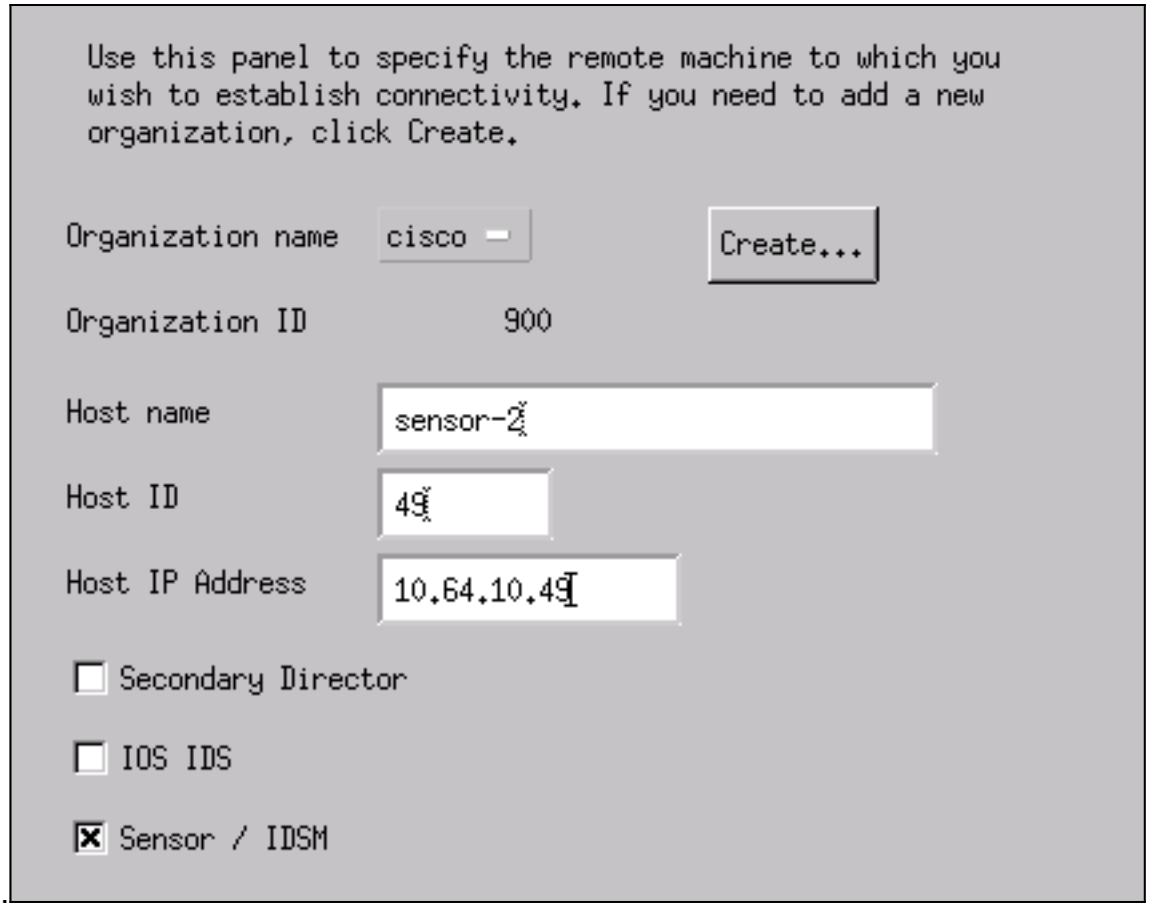
```
1 - IP Address: 10.64.10.49
2 - IP Netmask: 255.255.255.224
3 - IP Host Name:  sensor-2
4 - Default Route     10.64.10.33
5 - Network Access Control
         64.
         10.
6 - Communications Infrastructure
Sensor Host ID: 49
Sensor Organization ID:     900
Sensor Host Name: sensor-2
Sensor Organization 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

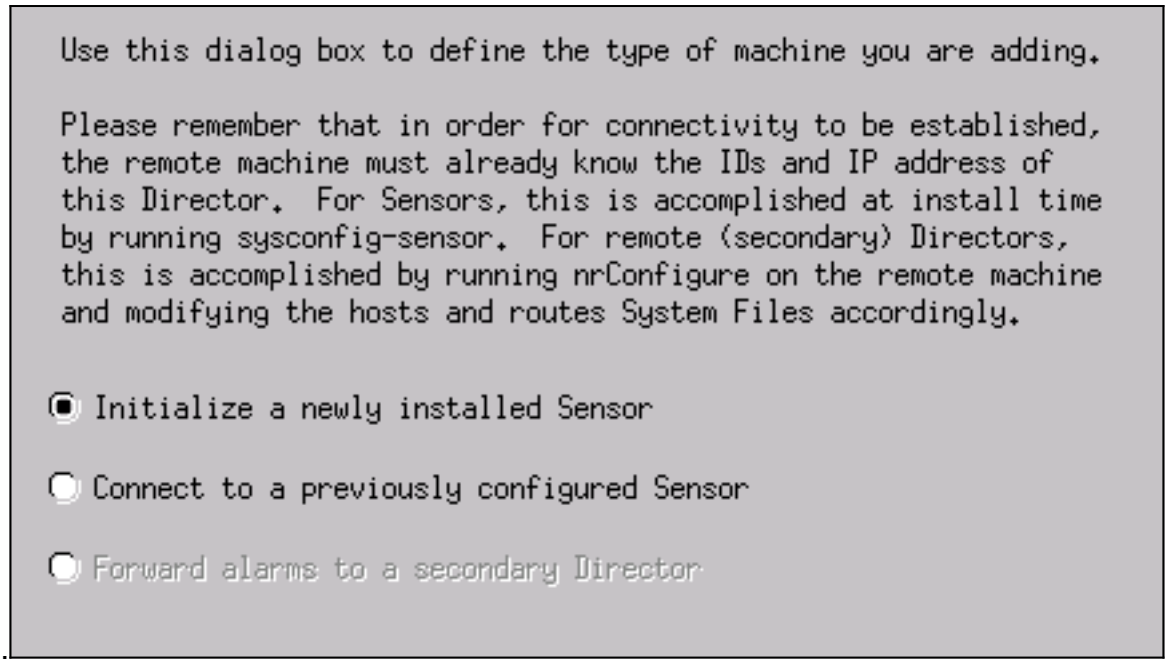
Complete estos pasos para agregar el sensor en el director.

1. Telnet a **10.64.21.50** con el **netrangr** y el ataque de contraseña del nombre de usuario.
2. Ingrese el **ovw&** para poner en marcha el HP OpenView.
3. En el menú principal, seleccione el **Security (Seguridad) > Configure (Configurar)**.
4. En la utilidad de la administración de archivos de configuración, seleccione **file > add host**, y haga clic **después**.
5. Éste es un ejemplo de cómo completar la información



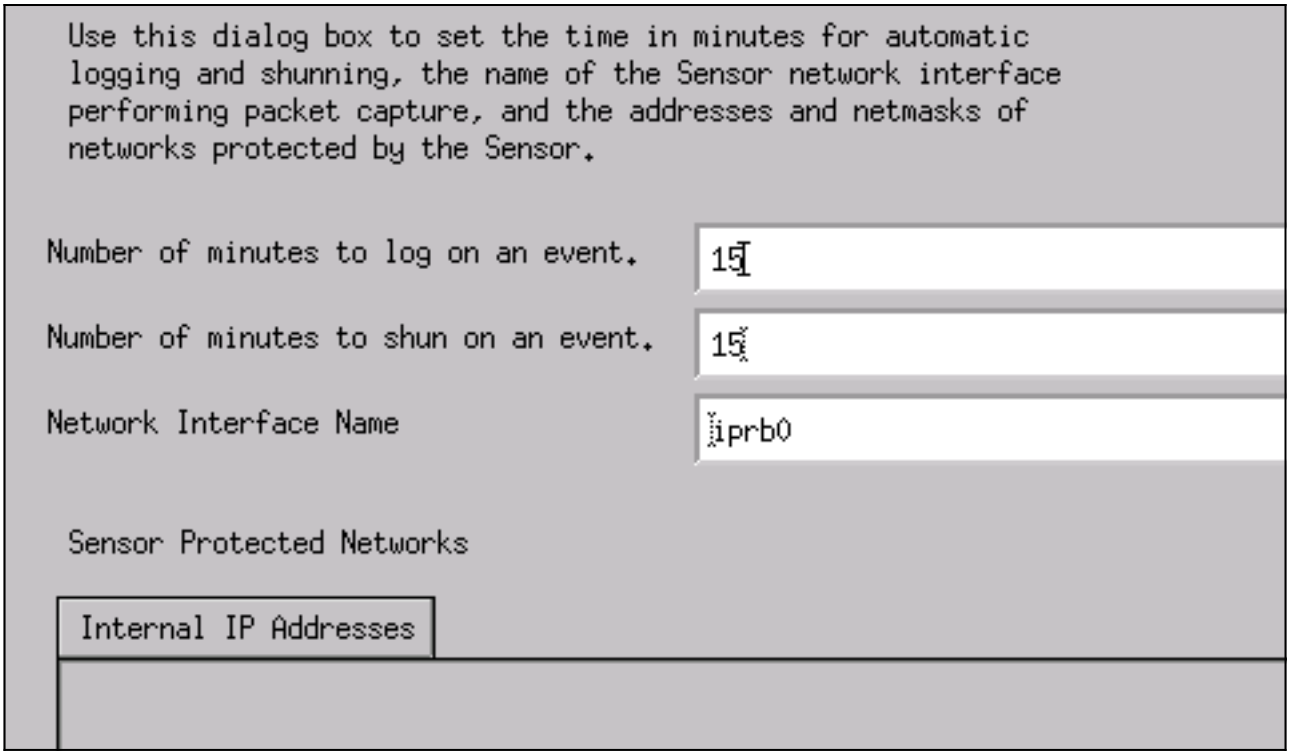
pedida.

6. Valide la configuración predeterminada para el tipo de máquina, y haga clic **después**, tal y como se muestra en de este

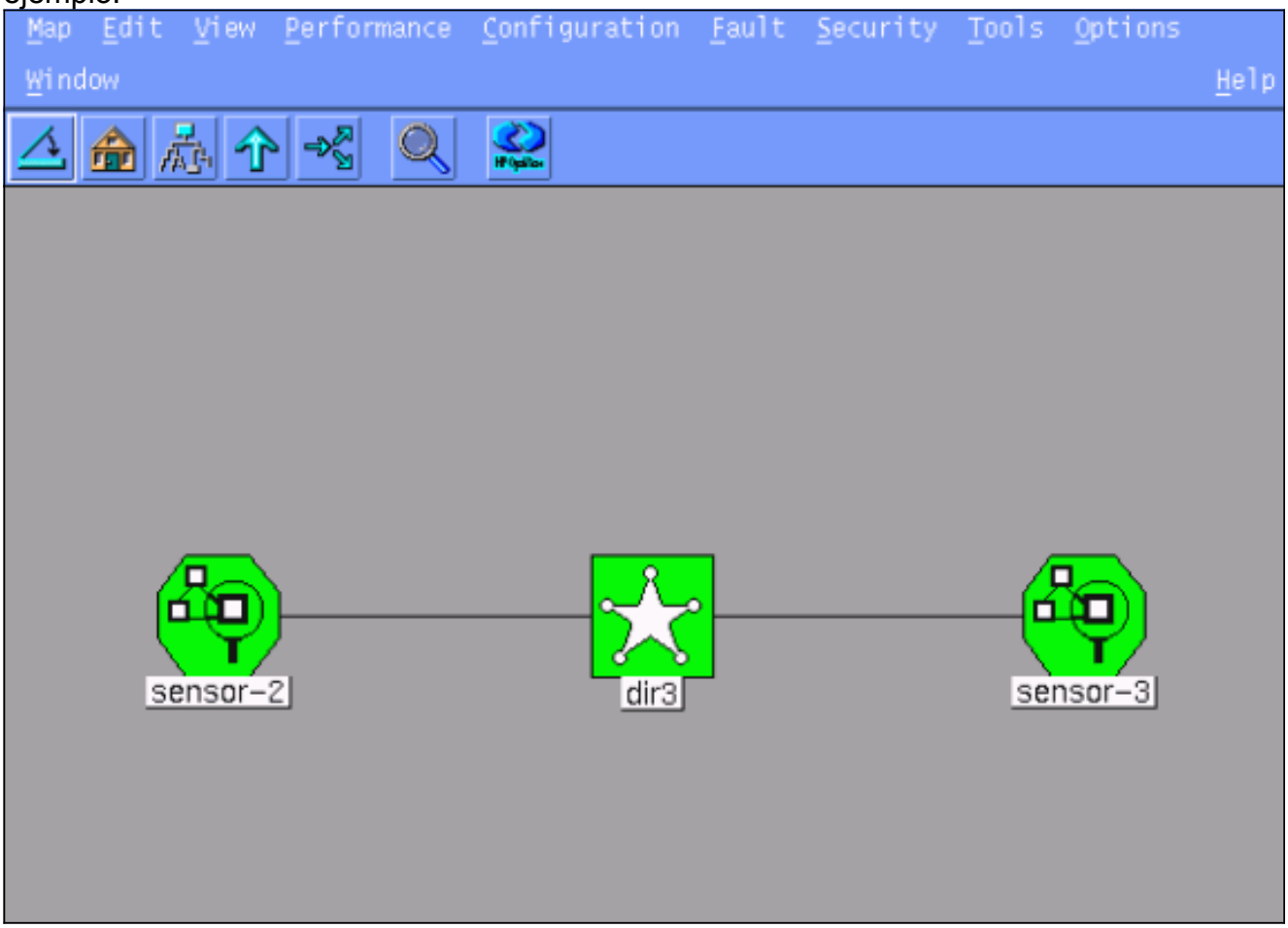


ejemplo.

7. Cambie el registro y evite los minutos, o déjelos como el valor por defecto si los valores son aceptables. Cambie el nombre de la interfaz de red al nombre de su interfaz de rastreo.En este ejemplo es el "iprb0." que puede ser el "spwr0" o cualquier otra cosa dependiendo del tipo de sensor y cómo usted conecta su
sensor.



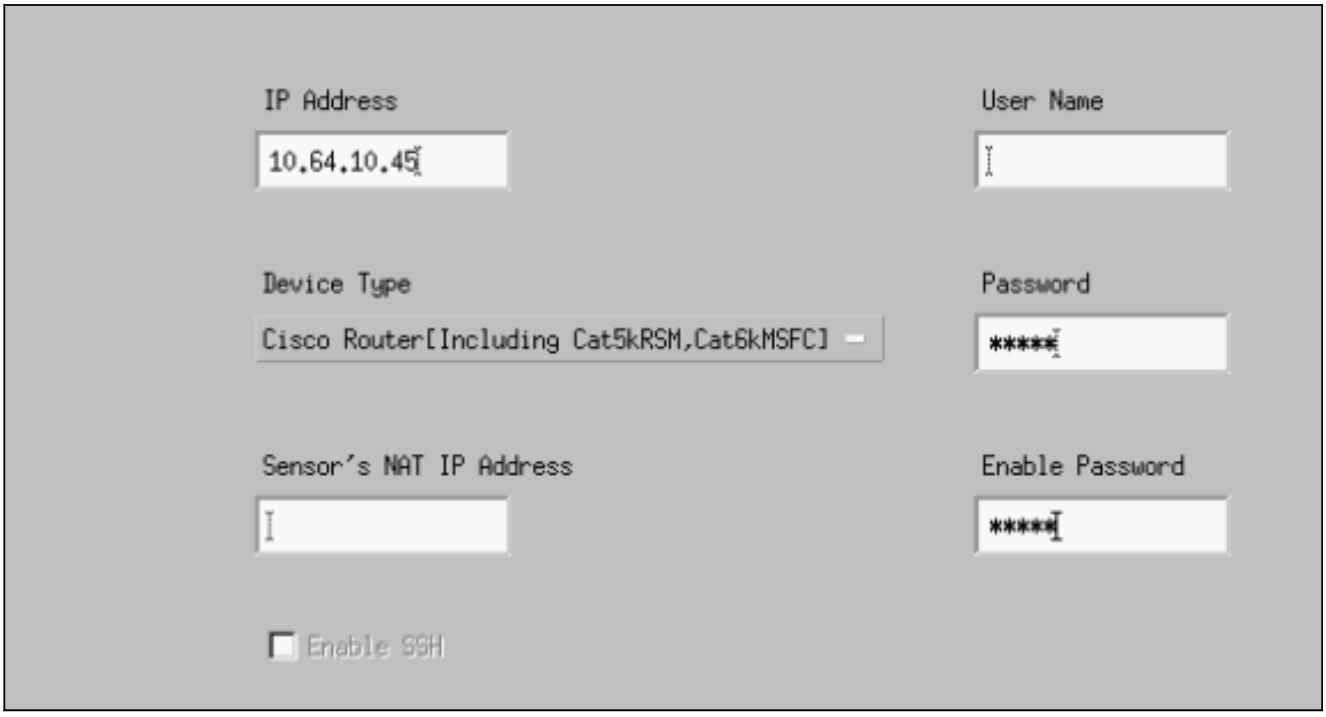
8. Haga clic **después** hasta que haya una opción al clic en Finalizar.Usted ha agregado con éxito el sensor en el director. Del menú principal, usted debe ver el `sensor 2`, como en este ejemplo.



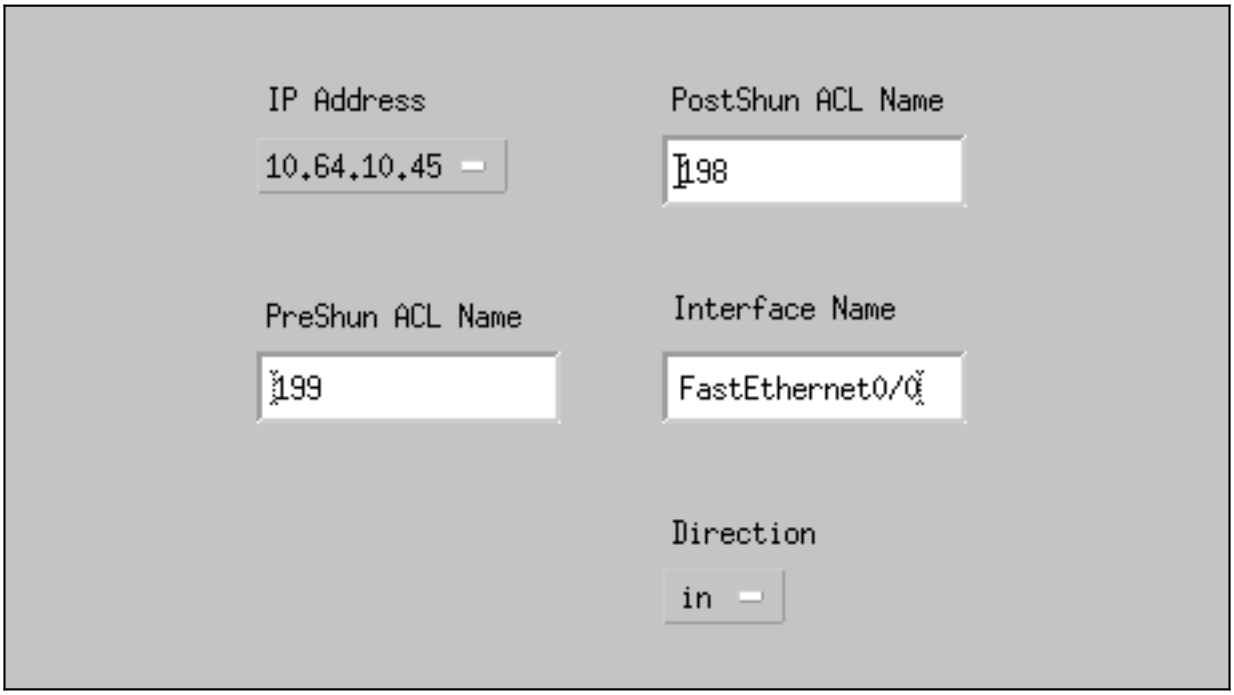
Configuración que evita para el router del Cisco IOS

Complete estos pasos para configurar evitar para el router del Cisco IOS.

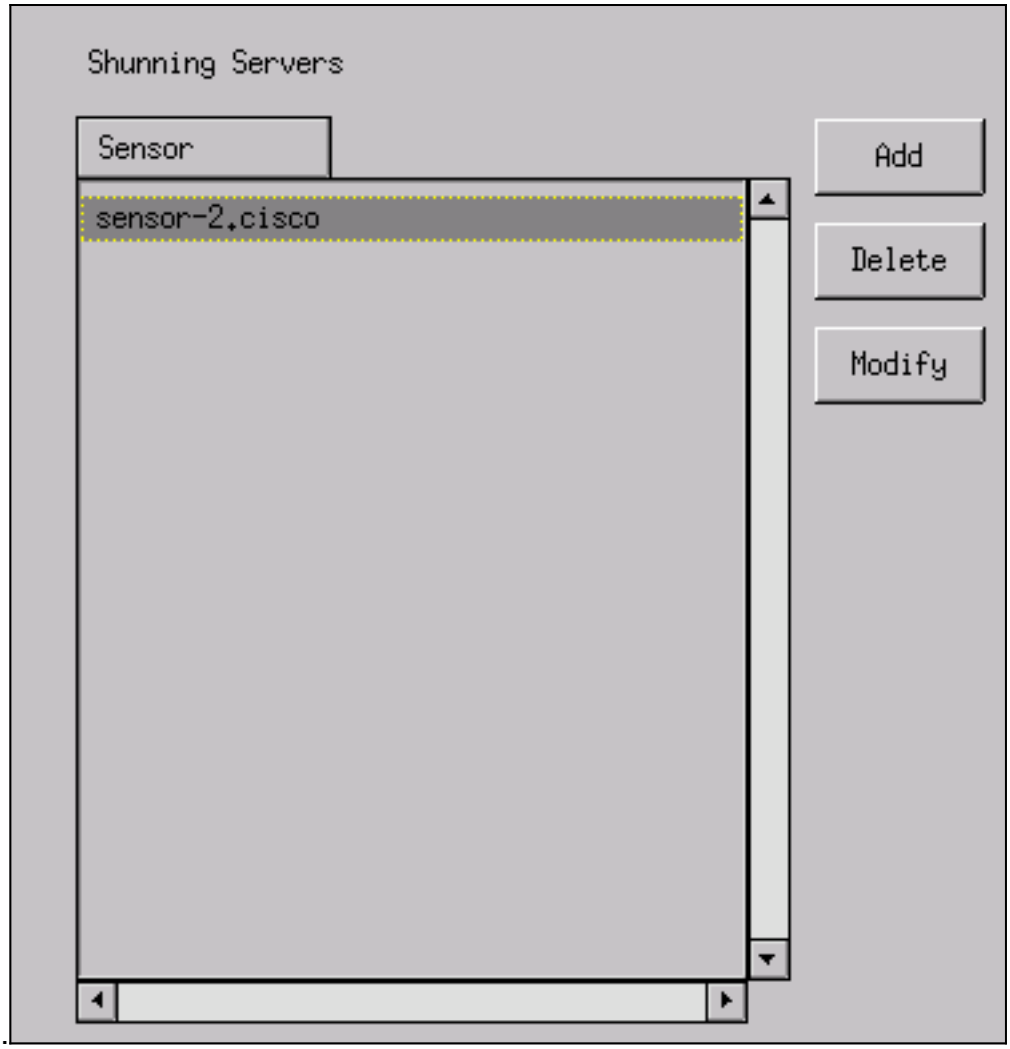
1. En el menú principal, seleccione el **Security (Seguridad) > Configure (Configurar)**.
2. En la utilidad de la administración de archivos de configuración, resalte el **sensor 2** y el tecleo doble él.
3. Abra la **Administración de dispositivos**.
4. Haga clic el **Devices (Dispositivos) > Add (Agregar)**, y ingrese la información tal y como se muestra en de este ejemplo. Para continuar, haga clic en OK (Aceptar).Telnet y la coincidencia de las contraseñas habilitadas cuál está en el router la "Casa."



5. **Las interfaces del** tecleo **> Add**, ingresan esta información, y hacen clic la **AUTORIZACIÓN** para
continuar.

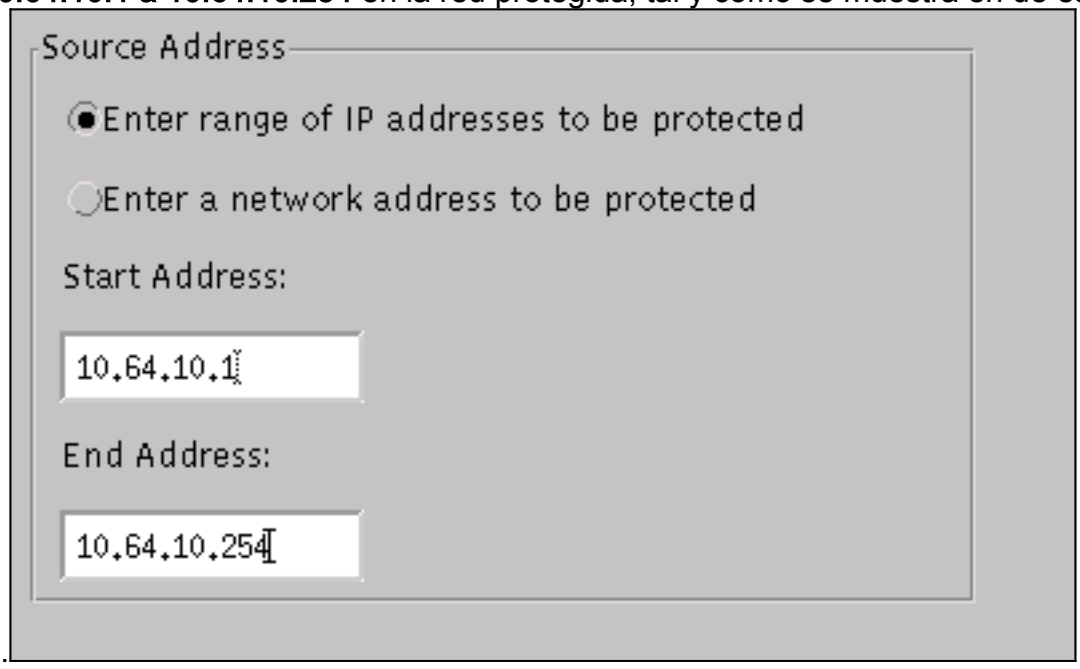


6. Haga clic **Shunning > Add** y seleccione **sensor-2.cisco** como el servidor que evita. Cierre la ventana de la Administración de dispositivos cuando le



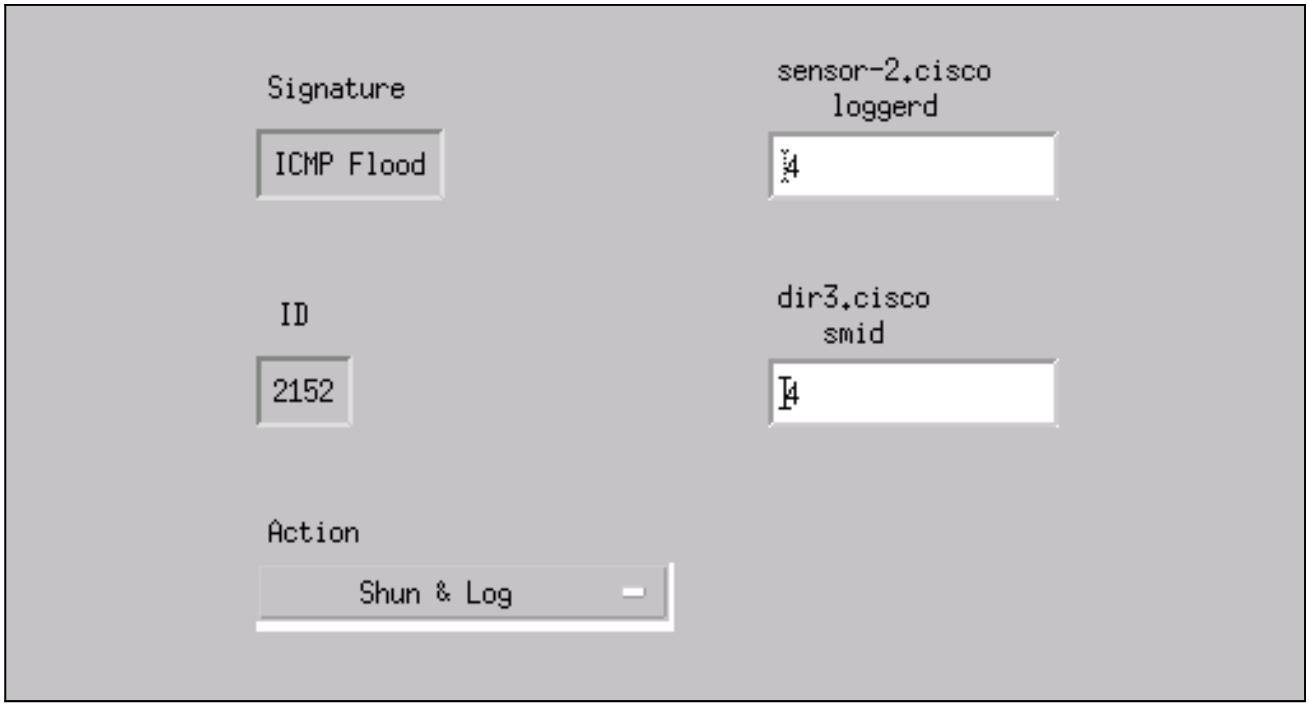
acaban.

7. Abra la ventana de la detección de intrusos, y haga clic las **redes protegidas**. Agregue el rango **10.64.10.1 a 10.64.10.254** en la red protegida, tal y como se muestra en de este

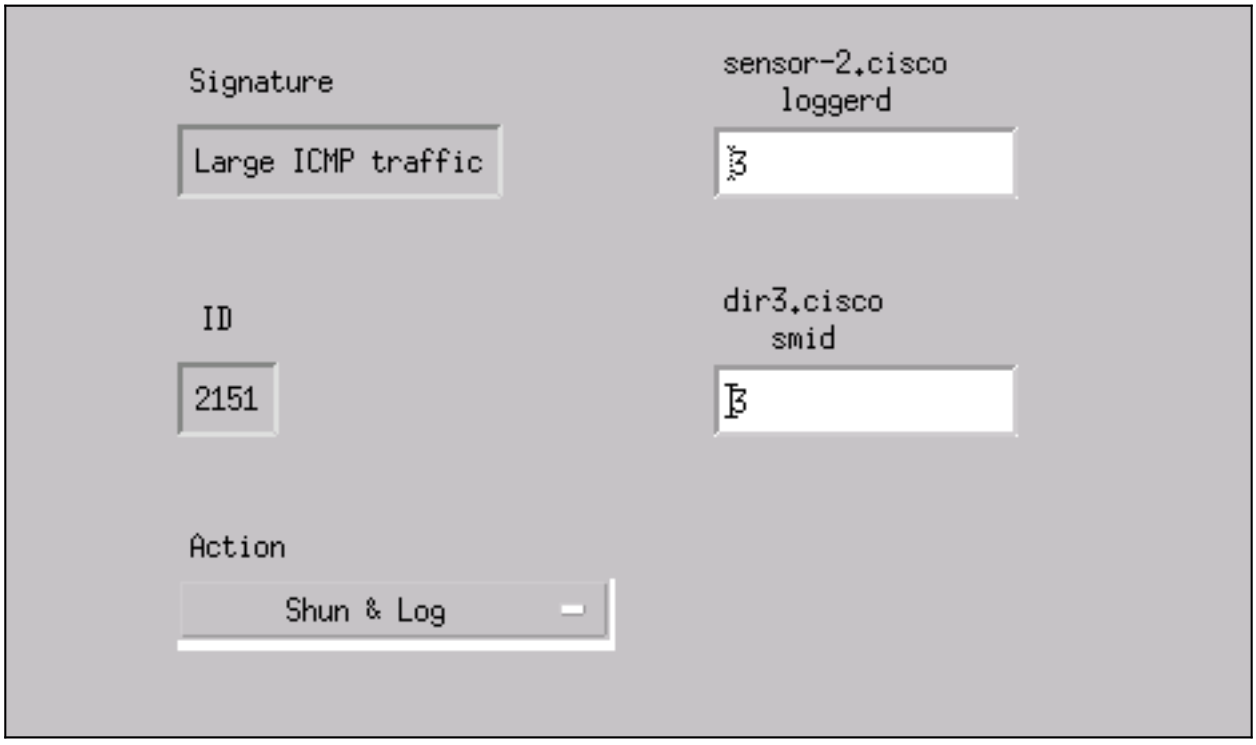


ejemplo.

8. Haga clic el **perfil > la configuración manual**.
9. Selecto **modifique las firmas > tráfico grande ICMP** con un ID de **2151**.
10. El tecleo **se modifica**, cambia la **acción de** ningunos **evitar y del registro**, y hace clic la **AUTORIZACIÓN** para continuar.

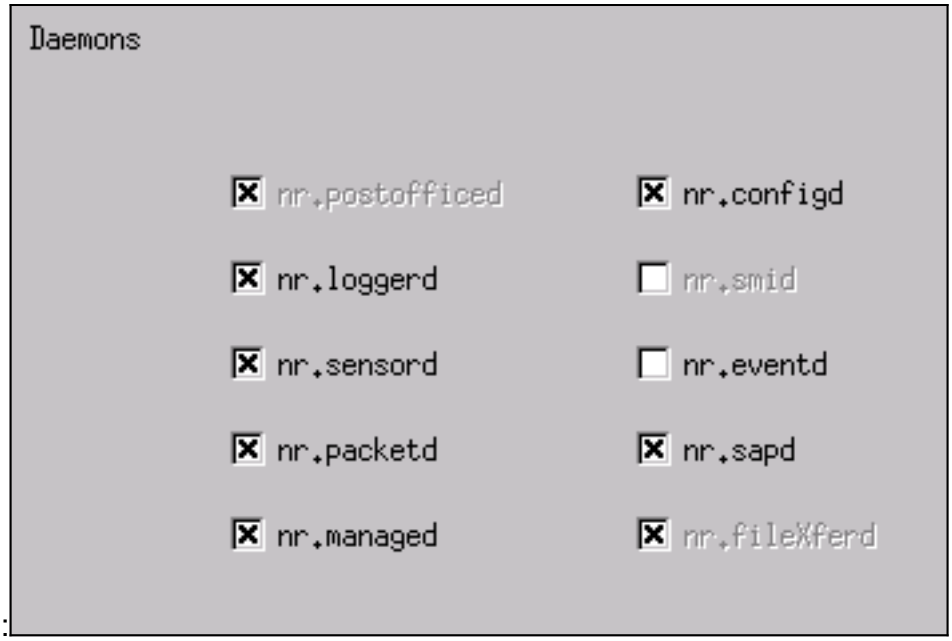


11. Elija la **inundación de ICMP** con un ID de **2152**, y el tecleo **se modifica**. Cambie la **acción de** ningunos **evitar y del registro**, y haga clic la **AUTORIZACIÓN** para continuar.

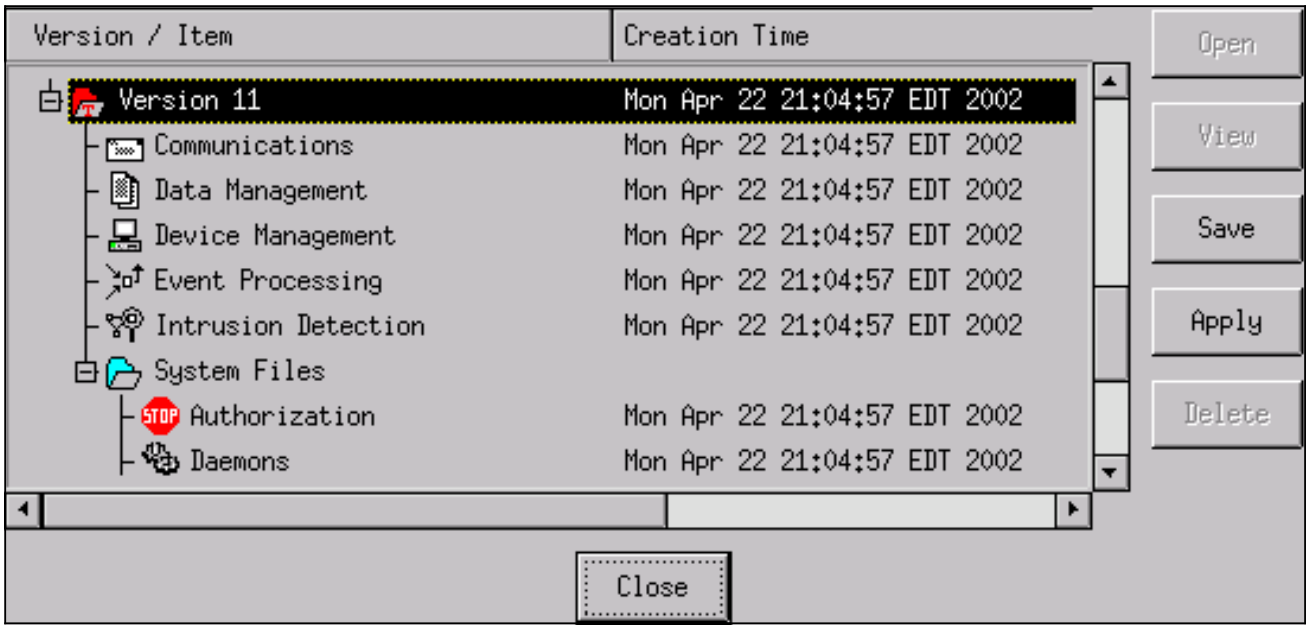


12. Haga Click en OK para cerrar la ventana de la detección de intrusos.
13. Abra la carpeta de archivos del sistema, y abra la ventana de Daemons.Aseegurese le haber habilitado estas

daemones:



14. Haga Click en OK a continuar, para elegir la versión apenas modificada, y para hacer clic la **salvaguardia** y después **a aplicarse**.La espera para que el sistema le diga el sensor acabado recomenzando los servicios, entonces cierra todas las ventanas para la configuración del
director.



Verificación

En esta sección encontrará información que puede utilizar para confirmar que su configuración esté funcionando correctamente.

La herramienta Output Interpreter (sólo para clientes registrados) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

- **lista de acceso de la demostración** - Enumera las declaraciones de **comando access-list** en la configuración del router. También enumera una cuenta del golpe que indique que la cantidad de veces un elemento se ha correspondido con durante una búsqueda del **comando access-list**.

- **ping** - Utilizado para diagnosticar la conectividad de red básica.

Antes de un ataque se inicia

Antes de que se inicie un ataque, publique estos comandos.

```
house#show access-list
Extended IP access list IDS_FastEthernet0/0_in_1
    permit ip host 10.64.10.49 any
    permit ip any any (12 matches)
house#

light#ping 10.64.10.45

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.64.10.45, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
light#
```

Ponga en marcha el Ataque y evasión

Ponga en marcha su ataque del router “luz” a la víctima “Casa.” Cuando el ACL toma la influencia, se ve el unreachables.

```
light#ping
Protocol [ip]:
Target IP address: 10.64.10.45
Repeat count [5]: 1000000
Datagram size [100]: 18000
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 1000000, 18000-byte ICMP Echos to 10.64.10.45, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!U.U.U.U.U.U.U.U.U.U.U.U.U.U.U.U.U.U.
```

Una vez que el sensor ha detectado el ataque, y se descarga el ACL, y esta salida se visualiza en la “Casa.”

```
house#show access-list
Extended IP access list IDS_FastEthernet0/0_in_0
  permit ip host 10.64.10.49 any
  deny ip host 100.100.100.2 any (459 matches)
  permit ip any any
```

El unreachables todavía se ve en la “luz,” tal y como se muestra en de este ejemplo.

```
Light#ping 10.64.10.45
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.64.10.45, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
```

Quince minutos más adelante, la “Casa” vuelve a normal, porque el evitar fue fijado a 15 minutos.

```
House#show access-list
Extended IP access list IDS_FastEthernet0/0_in_1
    permit ip host 10.64.10.49 any
    permit ip any any (12 matches)
house#
```

La “luz” puede hacer ping la “Casa.”

```
Light#ping 10.64.10.45

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.64.10.45, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

Troubleshooting

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

Información Relacionada

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