Rechazo de PIX IDS mediante Cisco IDS UNIX Director

Contenido

Introducción

Este documento describe cómo configurar evitar en un PIX con la ayuda del Cisco IDS Unix Director (conocido antes como Director Netranger) y del sensor. Este documento asume que el sensor y el director son operativos y la interfaz de rastreo del sensor está configurada para atravesar a la interfaz exterior PIX.

prerrequisitos

Requisitos

No hay requisitos previos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software y hardware.

- Cisco IDS Unix Director 2.2.3
- Sensor UNIX 3.0.5 del Cisco IDS

- Secure PIX de Cisco con 6.1.1**Nota:** Si usted utiliza la versión 6.2.x, usted puede utilizar la Administración del protocolo secure shell (SSH), pero no Telnet. Refiera al Id. de bug Cisco CSCdx55215 (clientes registrados solamente) para más información.

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, le presentan con la información usada para configurar las características descritas en este documento.

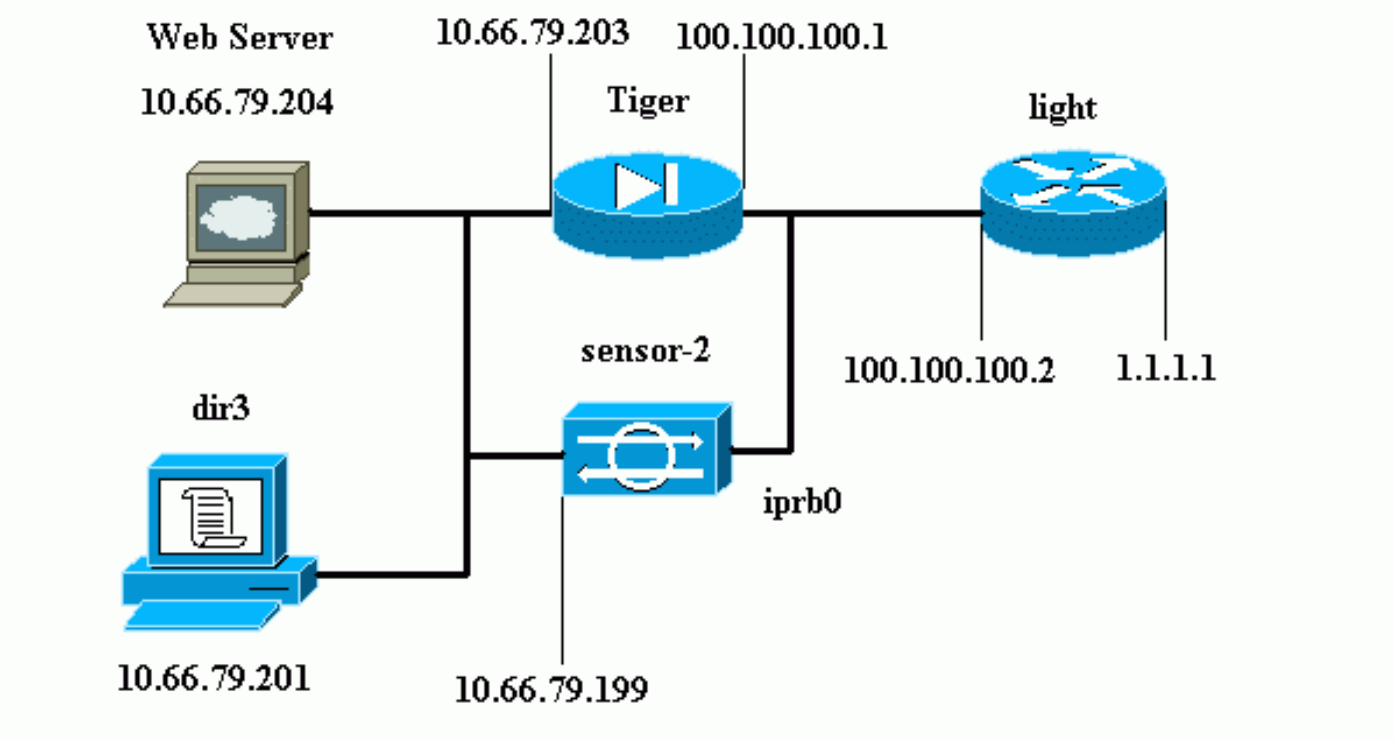
Utilizan al Cisco IDS Unix Director y el sensor para manejar un Secure PIX de Cisco para evitar. Cuando usted considera esta configuración, recuerde estos conceptos:

- Instale el sensor y aseegurese los trabajos del sensor correctamente.
- Asegúrese de que los palmos de la interfaz de rastreo a la interfaz exterior del PIX.

Nota: Para encontrar la información adicional en los comandos usados en este documento, refiera a la herramienta de búsqueda de comandos (clientes registrados solamente).

Diagrama de la red

Este documento utiliza esta configuración de red:



Configuraciones

Este documento usa estas configuraciones.

- Luz del router
- PIX Tiger

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
```

PIX Tiger

```
PIX Version 6.1(1)
nameif gb-ethernet0 intf2 security10
nameif gb-ethernet1 intf3 security15
nameif ethernet0 outside security0 nameif ethernet1
inside security100 enable password 2KFQnbNIdI.2KYOU
encrypted passwd 9jNfZuG3TC5tCVH0 encrypted hostname
Tiger fixup protocol ftp 21 fixup protocol http 80 fixup
protocol h323 1720 fixup protocol rsh 514 fixup protocol
rtsp 554 fixup protocol smtp 25 fixup protocol sqlnet
1521 fixup protocol sip 5060 fixup protocol skinny 2000
names !--- Allows ICMP traffic and HTTP to pass through
the PIX !--- to the Web Server. access-list 101 permit
icmp any host 100.100.100.100 access-list 101 permit tcp
any host 100.100.100.100 eq www pager lines 24 logging
on logging buffered debugging interface gb-ethernet0
1000auto shutdown interface gb-ethernet1 1000auto
shutdown interface ethernet0 auto interface ethernet1
auto mtu intf2 1500 mtu intf3 1500 mtu outside 1500 mtu
inside 1500 ip address intf2 127.0.0.1 255.255.255.255
ip address intf3 127.0.0.1 255.255.255.255 ip address
outside 100.100.100.1 255.255.255.0 ip address inside
10.66.79.203 255.255.255.224 ip audit info action alarm
ip audit attack action alarm no failover failover
timeout 0:00:00 failover poll 15 failover ip address
intf2 0.0.0.0 failover ip address intf3 0.0.0.0 failover
ip address outside 0.0.0.0 failover ip address inside
0.0.0.0 pdm history enable arp timeout 14400 global
(outside) 1 interface nat (inside) 1 0.0.0.0 0.0.0.0 0 0
!--- Static NAT for the Web Server. static
```

```
(inside,outside) 100.100.100.100 10.66.79.204 netmask
255.255.255.255 0 0 access-group 101 in interface
outside route outside 0.0.0.0 0.0.0.0 100.100.100.2 1
route inside 10.66.0.0 255.255.0.0 10.66.79.193 1
timeout xlate 3:00:00 timeout conn 1:00:00 half-closed
0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00 s0 timeout
uauth 0:05:00 absolute aaa-server TACACS+ protocol
tacacs+ aaa-server RADIUS protocol radius aaa-server
LOCAL protocol tacacs+ no snmp-server location no snmp-
server contact snmp-server community public no snmp-
server enable traps floodguard enable no sysopt route
dnat !--- Allows Sensor Telnet to the PIX from the
inside interface. telnet 10.66.79.199 255.255.255.255
inside telnet timeout 5 ssh timeout 5 terminal width 80
Cryptochecksum:b4c820ba31fbb3996ca8891503ebacbc : end
```

Configure el sensor

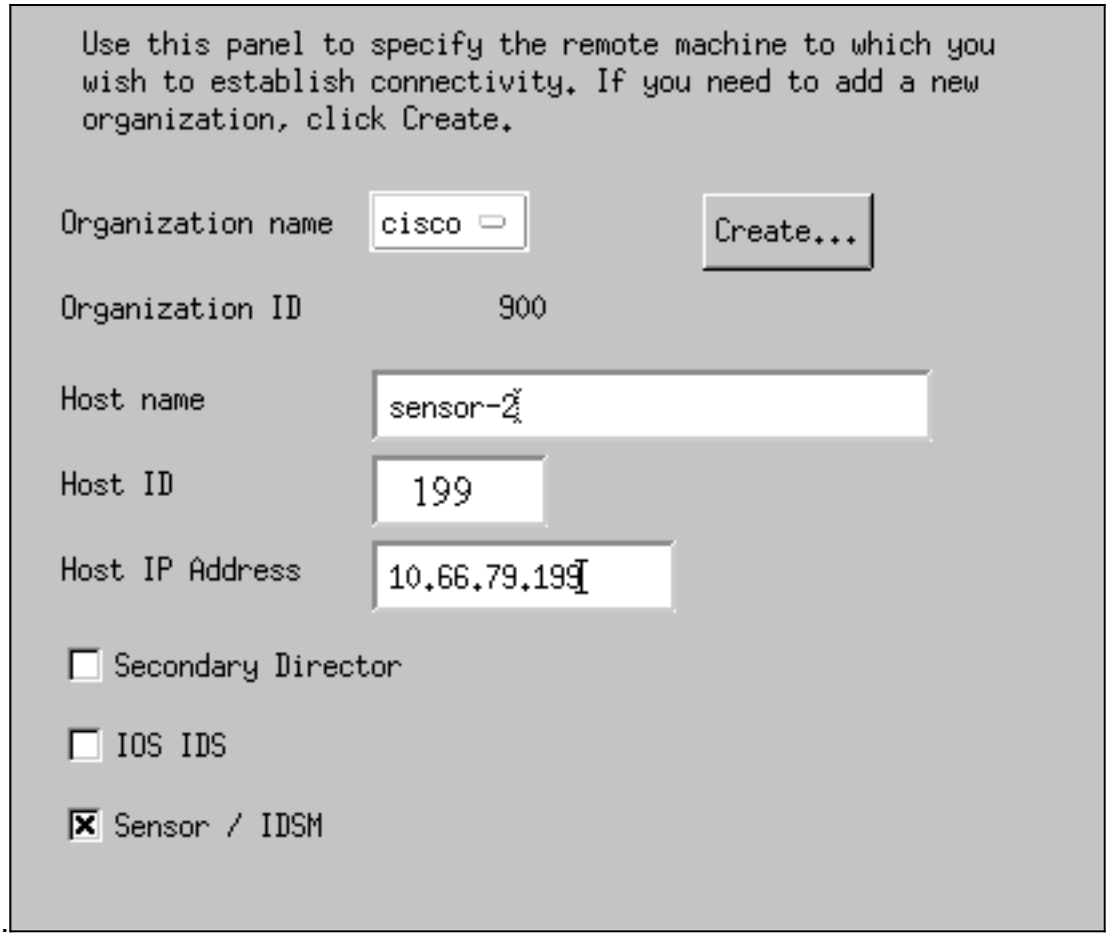
Estos pasos describen cómo configurar el sensor.

1. Telnet a **10.66.79.199** con el nombre de usuario raíz y el ataque de contraseña.
2. Ingrese el sysconfig-**sensor**.
3. Ingresar esta informaciónDirección IP: **10.66.79.199**Máscara de red IP: **255.255.255.224**Nombre de host IP: **sensor 2**Ruta predeterminado: **10.66.79.193**Control de acceso a la red**10.**Infraestructura de comunicacionesID del host del sensor: **49**ID de la organización del sensor: **900**Nombre del host del sensor: **sensor 2**Nombre de la organización del sensor: **Cisco**Dirección IP del sensor: **10.66.79.199**ID del host del Administrador IDS: **50**ID de la organización del Administrador IDS: **900**Nombre del host del Administrador IDS: **dir3**Nombre de la organización del Administrador IDS: **Cisco**Dirección IP del Administrador IDS: **10.66.79.201**
4. Guarde la configuración. Las reinicializaciones del sensor entonces.

Agregue el sensor en el director

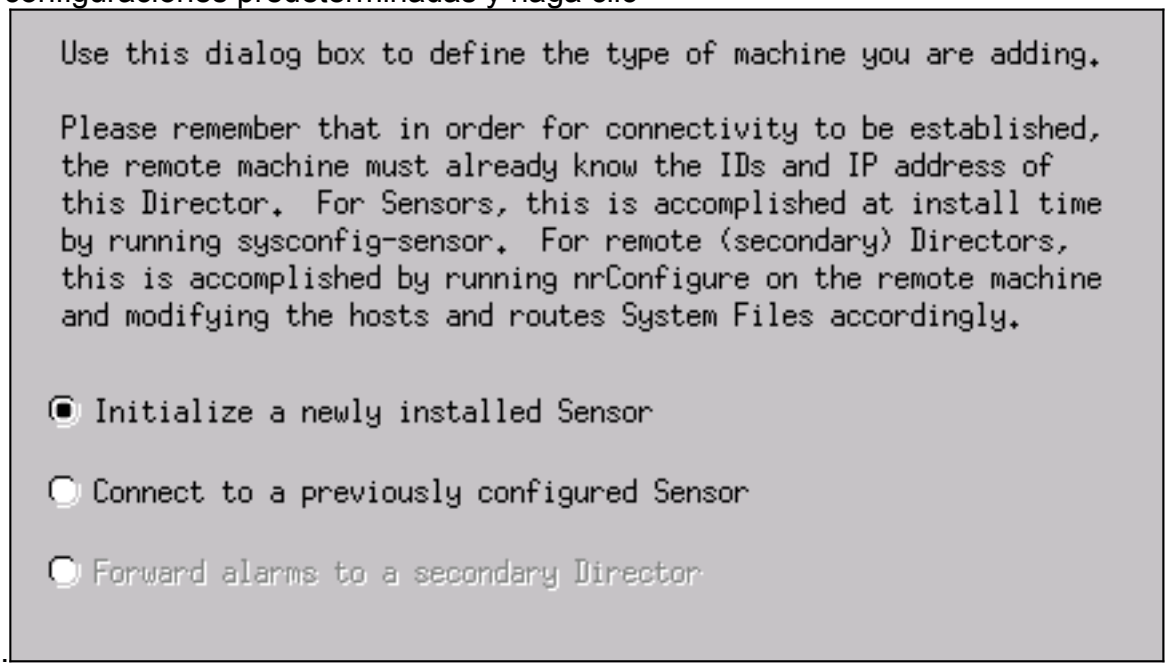
Complete estos pasos para agregar el sensor en el director.

1. Telnet a **10.66.79.201** 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 el menú de la configuración Netranger, seleccione **file > add host**, y haga clic **después**.
5. Ingrese esta información, y haga clic



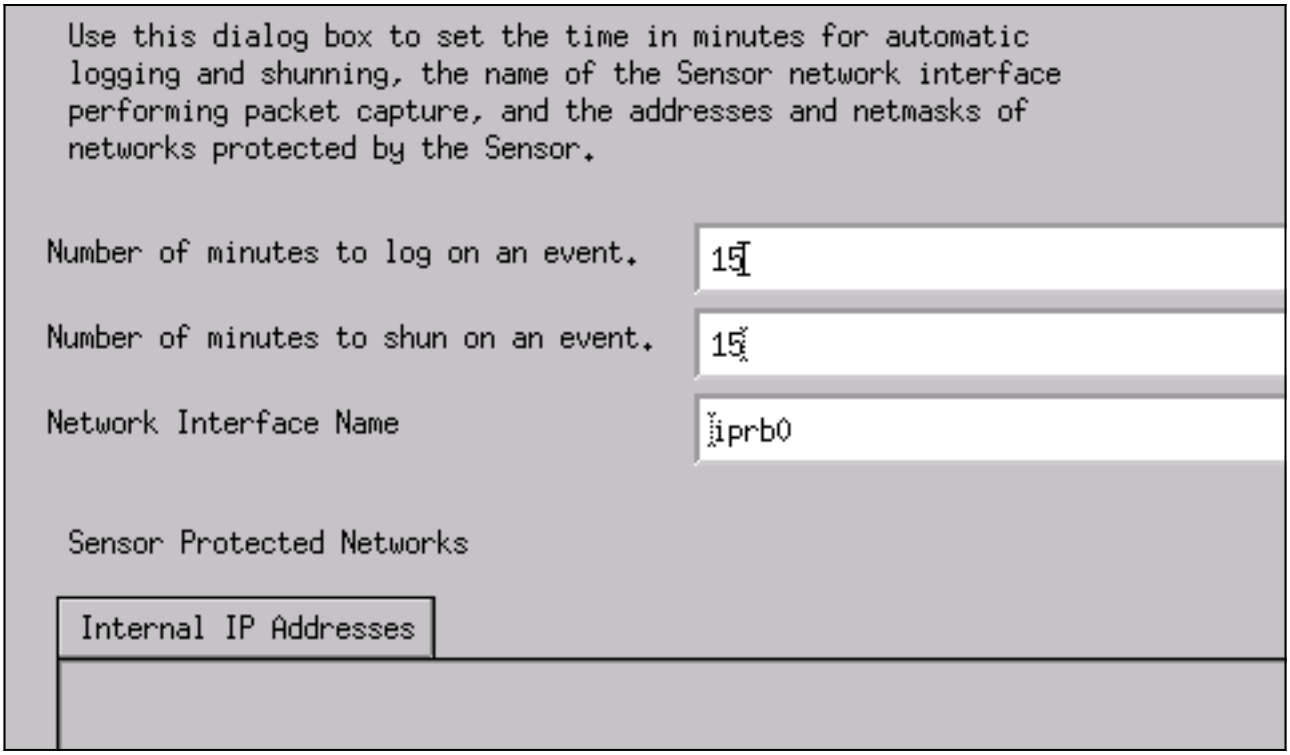
después.

6. Deje las configuraciones predeterminadas y haga clic

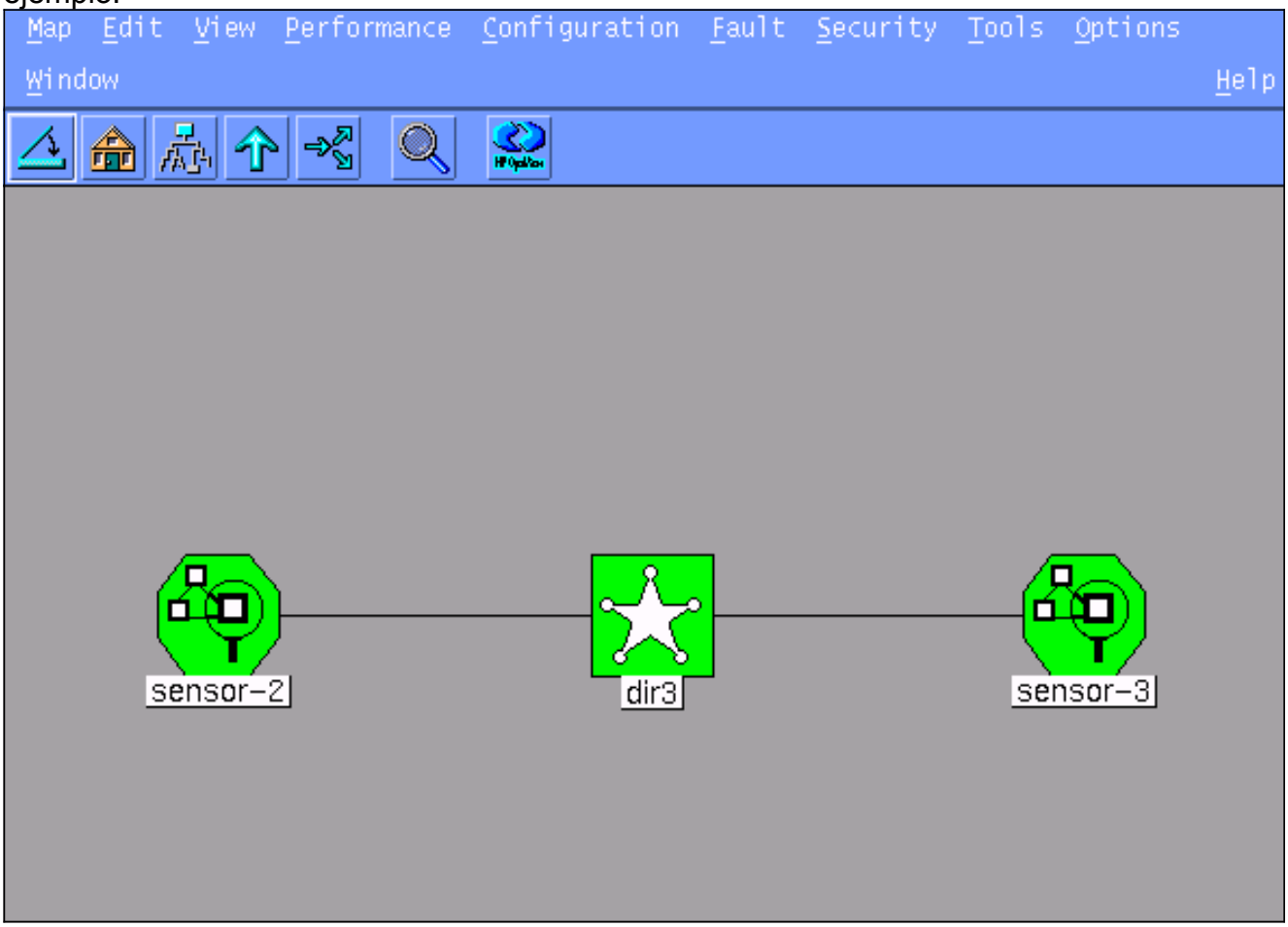


después.

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". Puede ser el "spwr0" o cualquier otra cosa basado en el tipo de sensor y cómo usted conecta el
sensor.



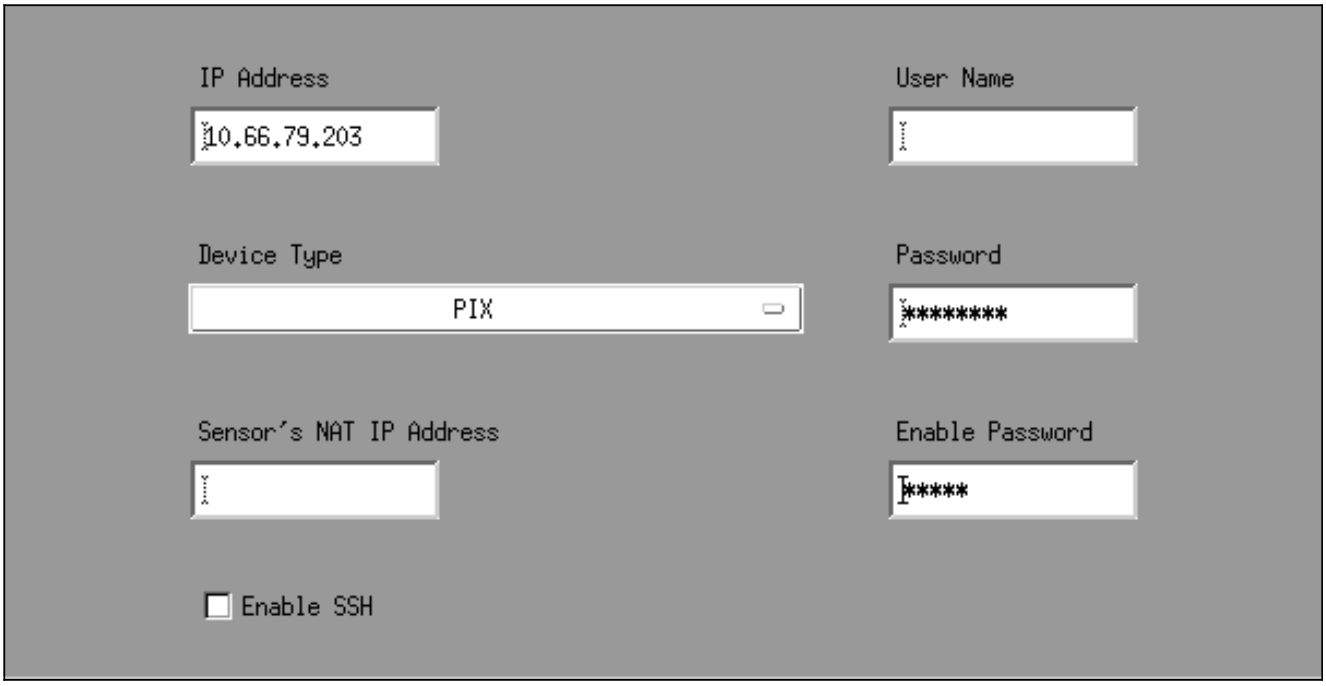
8. Haga clic **después** hasta que haya una opción al clic en Finalizar.El sensor ahora se agrega con éxito en el director. Del menú principal, el **sensor 2** se visualiza, tal y como se muestra en de este
ejemplo.



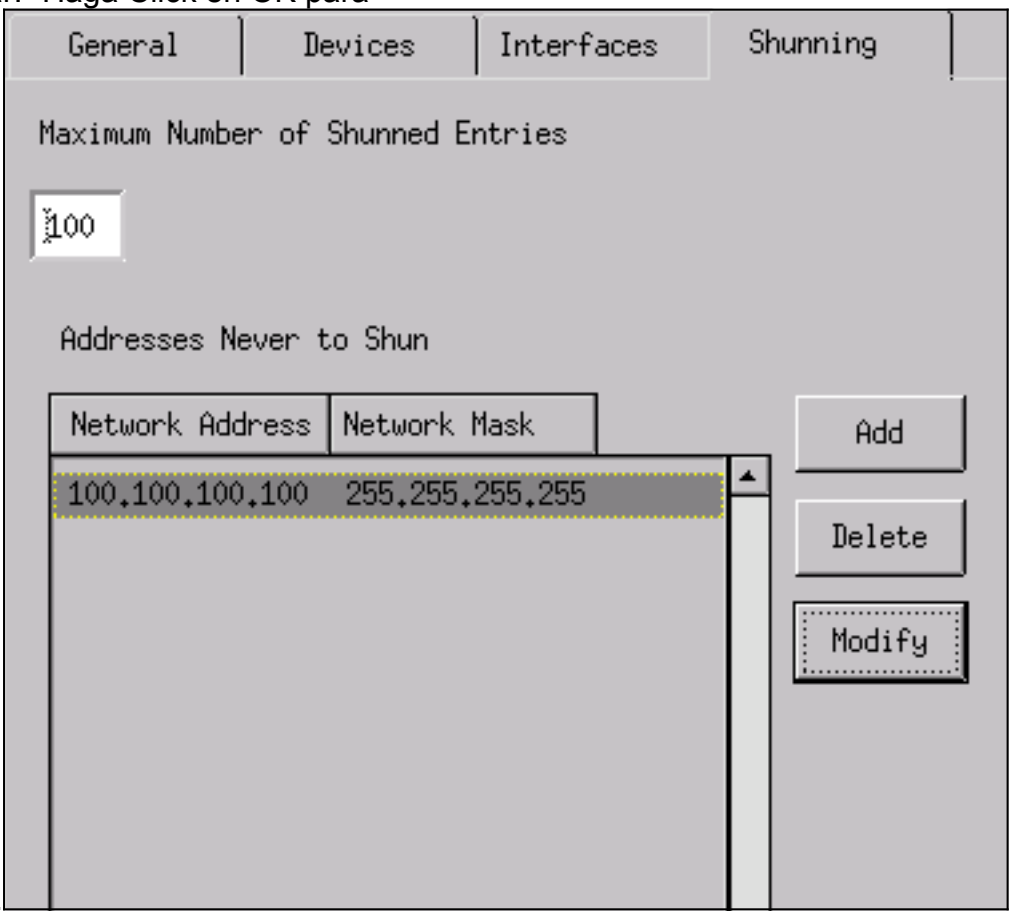
Configuración que evita para el PIX

Complete estos pasos para configurar evitar para el PIX.

1. En el menú principal, seleccione el **Security (Seguridad) > Configure (Configurar)**.
2. En el menú de la configuración Netranger, 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. Haga Click en OK para continuar. Telnet y la contraseña habilitada son ambo
   “Cisco”.

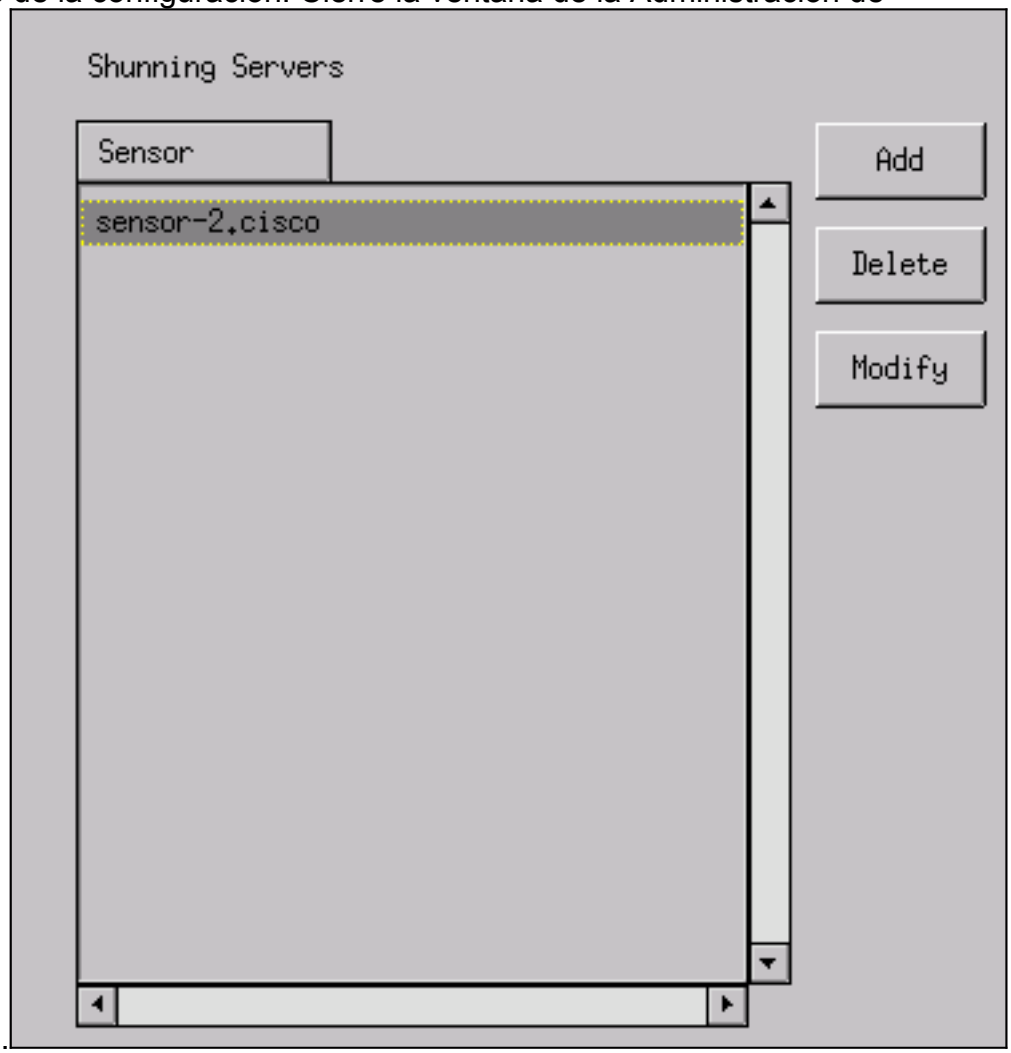


5. Tecleo **Shunning > Add**. Nunca agregue el host **100.100.100.100** bajo “direccionamientos para evitar.” Haga Click en OK para continuar.

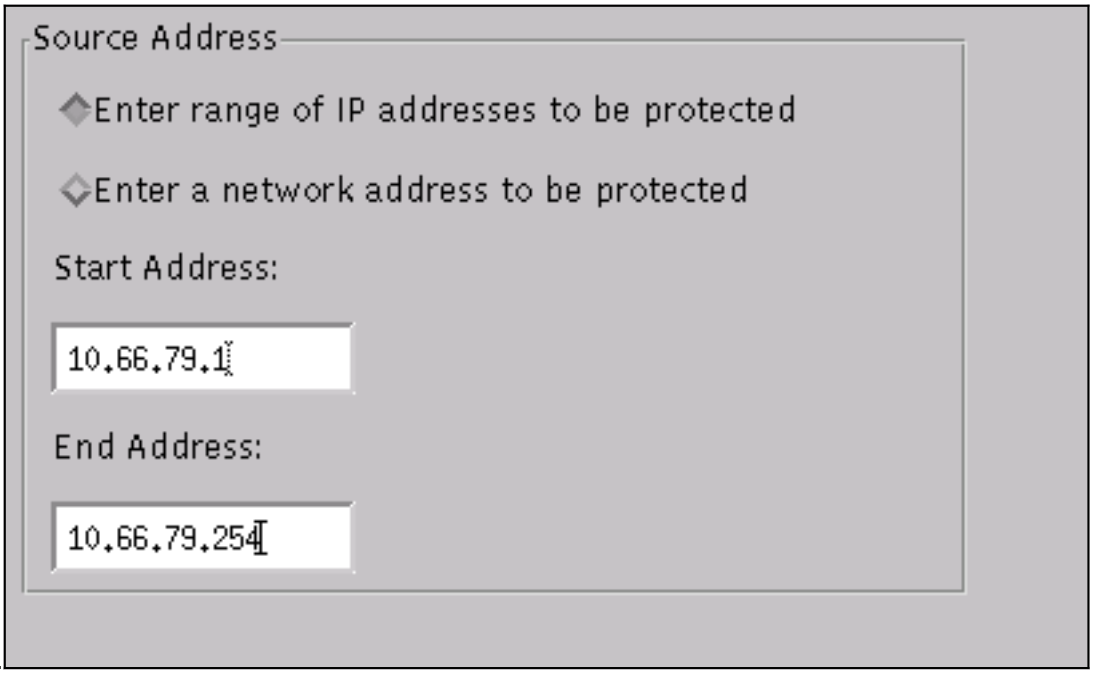


6. Tecleo **Shunning > Add** y **sensor-2.cisco** selecto como los servidores que evitan. Completan

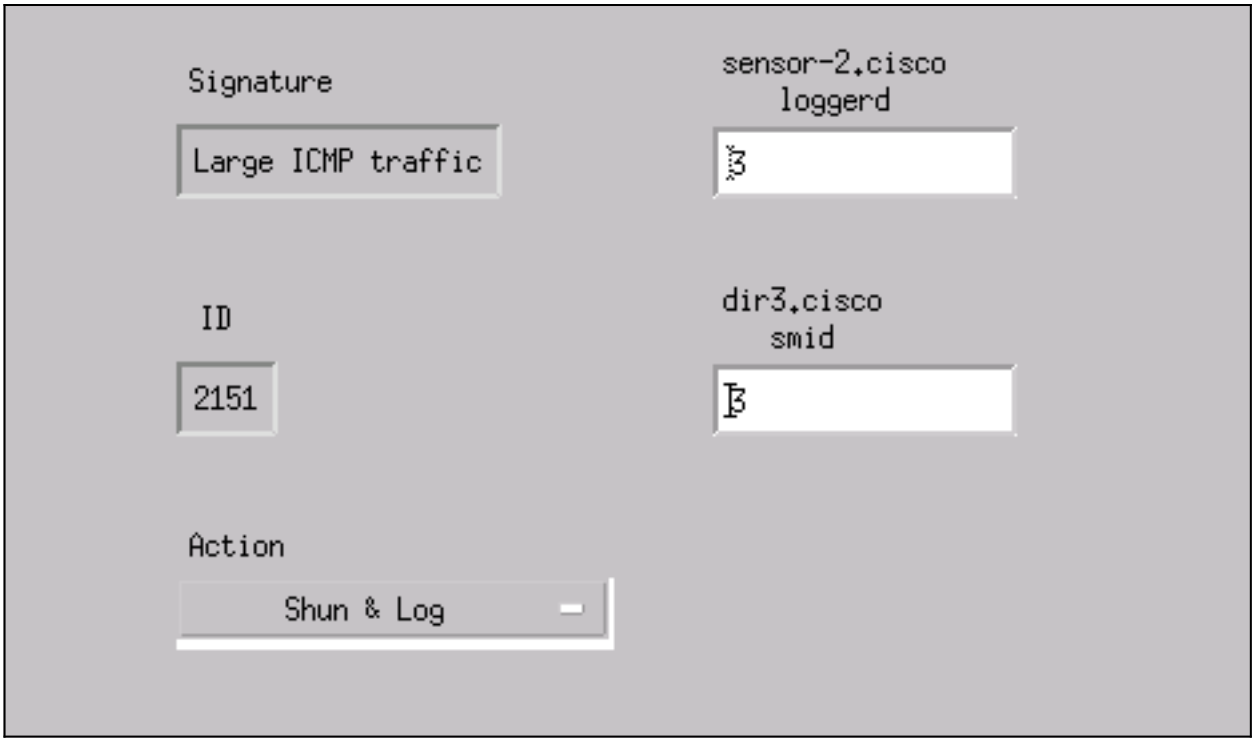
a esta parte de la configuración. Cierre la ventana de la Administración de dispositivos.



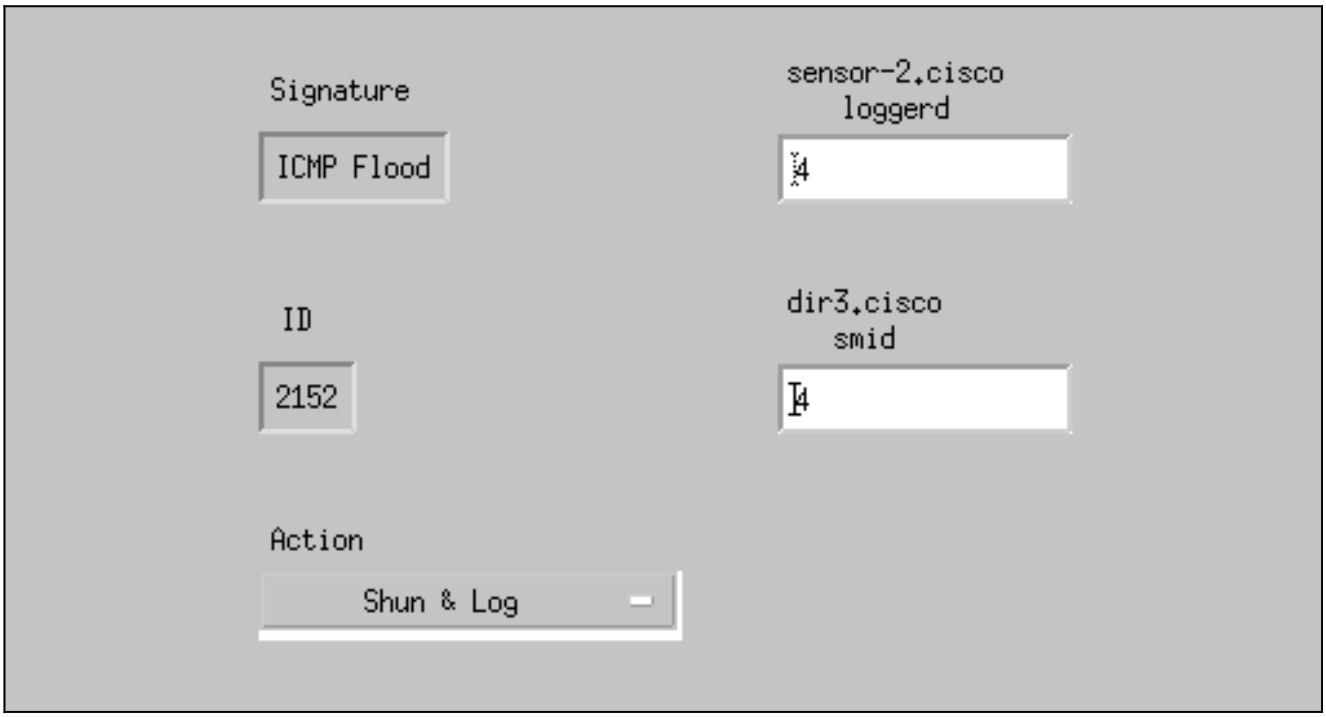
7. Abra la ventana de la detección de intrusos y haga clic las **redes protegidas**. Agregue **10.66.79.1 a 10.66.79.254** en la red protegida.



8. Haga clic el **perfil** y seleccione las **firmas de la configuración manual** > Modify. Seleccione el **tráfico grande ICMP** y el **ID: 2151**, tecleo **modifican**, y cambian la acción de ningunos **evitar y registrar**. Haga Click en OK para continuar.

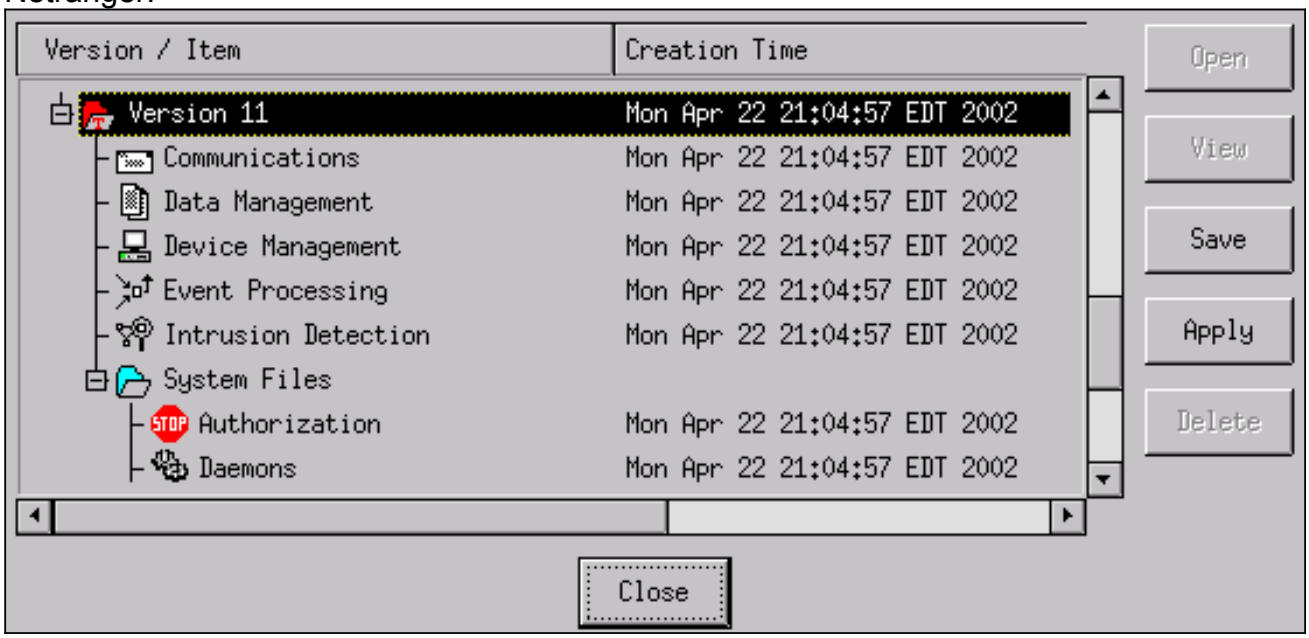


9. Seleccione la **inundación de ICMP** y el **ID: 2152**, tecleo **modifican**, y cambian la acción de **ningunos evitar y registrar**. Haga Click en OK para continuar.



10. Esta configuración de la parte de es completa. Haga Click en OK para cerrar la ventana de la detección de intrusos.
11. Abra la carpeta de **archivos del sistema** y abra la **ventana de Daemons**. Asegúrese que usted haya habilitado estas daemones:

12. Haga Click en OK para continuar, y seleccionar la versión que usted acaba de modificarse. **La salvaguardia del** tecleo **> se aplica**. Espere el sistema para decirle que el sensor está acabado, que recomienza los servicios, y que cierra todas las ventanas para la configuración
Netranger.



Verificación

Esta sección proporciona la información que le ayuda a confirmar sus trabajos de la configuración correctamente.

Antes de que usted ponga en marcha el ataque

```
Tiger(config)# show telnet 10.66.79.199 255.255.255.255 inside Tiger(config)# who 0:
10.66.79.199 Tiger(config)# show xlate 1 in use, 1 most used Global 100.100.100.100 Local
10.66.79.204 static Light#ping 100.100.100.100 Type escape sequence to abort. Sending 5, 100-
byte ICMP Echos to 100.100.100.100, timeout is 2 seconds: !!!!! Success rate is 100 percent
(5/5), round-trip min/avg/max = 112/195/217 ms Light#telnet 100.100.100.100 80 Trying
100.100.100.100, 80 ... Open
```

Ponga en marcha el Ataque y evasión

```
Light#ping Protocol [ip]: Target IP address: 100.100.100.100 Repeat count [5]: 100000 Datagram
size [100]: 18000 Timeout in seconds [2]: Extended commands [n]: Sweep range of sizes [n]: Type
escape sequence to abort. Sending 100000, 18000-byte ICMP Echos to 100.100.100.100, timeout is 2
seconds: !..................... Success rate is 4 percent (1/21), round-trip min/avg/max =
281/281/281 ms Light#telnet 100.100.100.100 80 Trying 100.100.100.100, 80 ... % Connection timed
out; remote host not responding Tiger(config)# show shun Shun 100.100.100.2 0.0.0 Tiger(config)#
show shun stat intf2=OFF, cnt=0 intf3=OFF, cnt=0 outside=ON, cnt=2604 inside=OFF, cnt=0
intf4=OFF, cnt=0 intf5=OFF, cnt=0 intf6=OFF, cnt=0 intf7=OFF, cnt=0 intf8=OFF, cnt=0 intf9=OFF,
cnt=0 Shun 100.100.100.2 cnt=403, time=(0:01:00).0 0 0
```

Quince minutos más adelante, vuelve a normal porque el evitar se fija a quince minutos.

```
Tiger(config)# show shun Tiger(config)# show shun stat intf2=OFF, cnt=0 intf3=OFF, cnt=0
outside=OFF, cnt=4437 inside=OFF, cnt=0 intf4=OFF, cnt=0 intf5=OFF, cnt=0 intf6=OFF, cnt=0
intf7=OFF, cnt=0 intf8=OFF, cnt=0 intf9=OFF, cnt=0 Light#ping 100.100.100.100 Type escape
sequence to abort. Sending 5, 100-byte ICMP Echos to 100.100.100.100, timeout is 2 seconds:
!!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms Light#telnet
100.100.100.100 80 Trying 100.100.100.100, 80 ... Open
```

Troubleshooting

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

Información Relacionada

- Fin de la Venta para el Cisco IDS Director
- Fin de vida para la versión 3.x del software de IDS Sensor de Cisco
- Soporte de productos del Cisco Intrusion Prevention System
- Soporte de productos del Software Cisco PIX Firewall
- Referencias de Comandos de Cisco Secure PIX Firewall
- Soporte Técnico y Documentación - Cisco Systems