Configurando a reinicialização de TCP usando o IDS Director

Índice

Introdução

Este documento descreve como configurar um diretor do sistema de detecção de intrusões (IDS, anteriormente Netranger) e um sensor para enviar as restaurações TCP em um telnet tentado a um intervalo de endereço que incluem o roteador controlado se a corda enviada é “ataque de teste”.

Pré-requisitos

Requisitos

Quando considerando esta configuração, recorde por favor a:

- Instale o sensor e verifique que trabalha corretamente antes que você execute esta configuração.
- Assegure-se de que os períodos do farejando interface à interface externa do roteador controlado.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco IDS Diretor 2.2.3
- Sensor 3.0.5 do Cisco IDS
- Software Release 12.2.6 running do roteador do ® do Cisco IOS

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

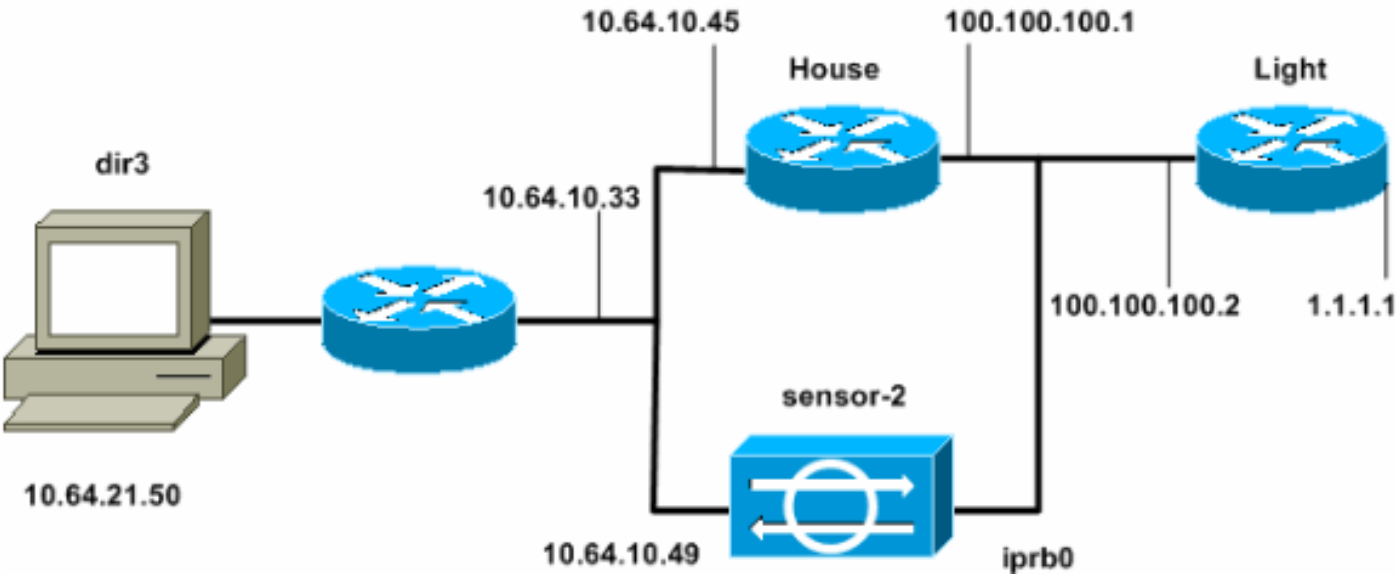
Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Para localizar informações adicionais sobre os comandos usados neste documento, utilize a Ferramenta Command Lookup (somente clientes registrados).

Diagrama de Rede

Este documento utiliza a configuração de rede mostrada neste diagrama.



Configurações

Este documento utiliza estas configurações.

- Luz do Roteador
- Companhia do Roteador

Luz do Roteador

```
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
```

Companhia do Roteador

```
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 o sensor

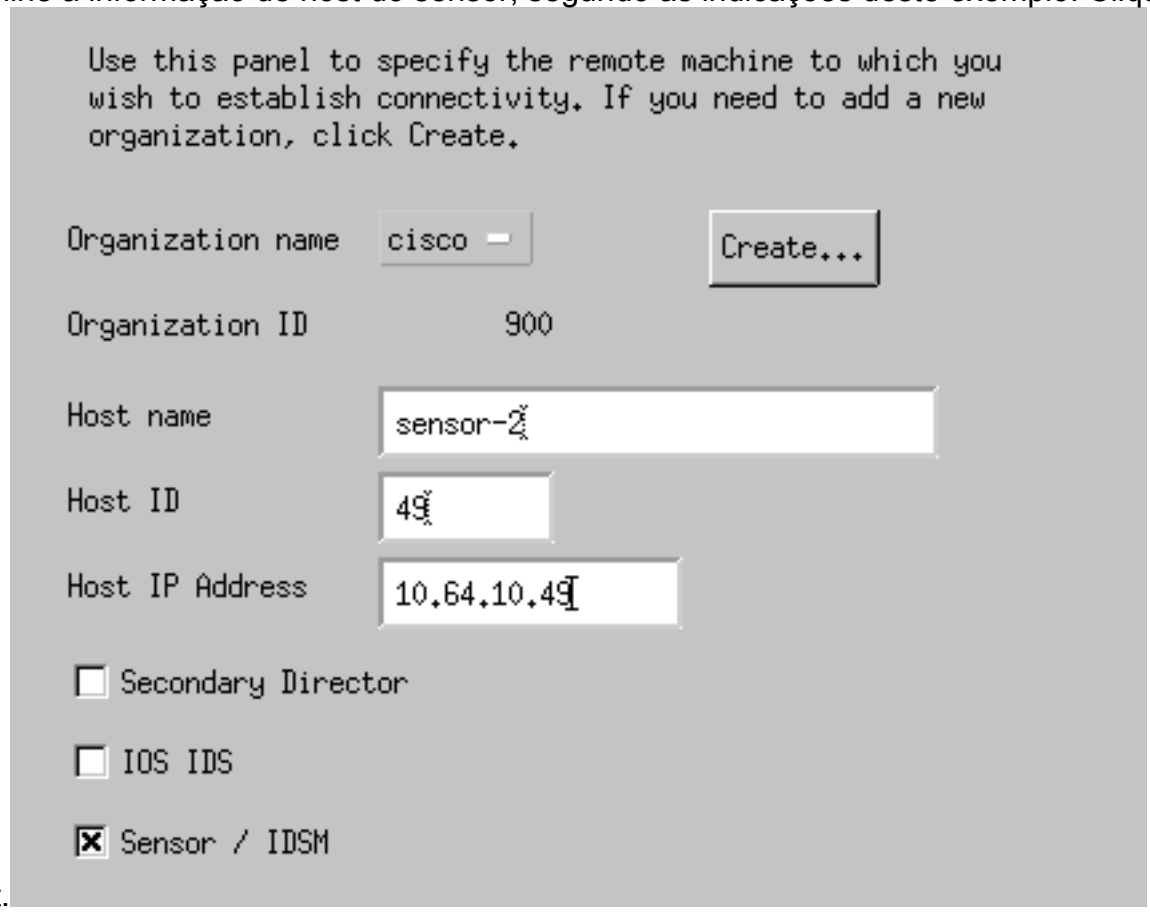
Termine estas etapas para configurar o sensor.

1. Telnet a 10.64.10.49 (o sensor de IDS) com a raiz do nome de usuário e o ataque de senha.
2. Datilografe o sysconfig-**sensor**.
3. Quando alertado, incorpore a informação de configuração, segundo as indicações deste exemplo:`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. Quando alertado, salvar a configuração e permita que o sensor recarregue.

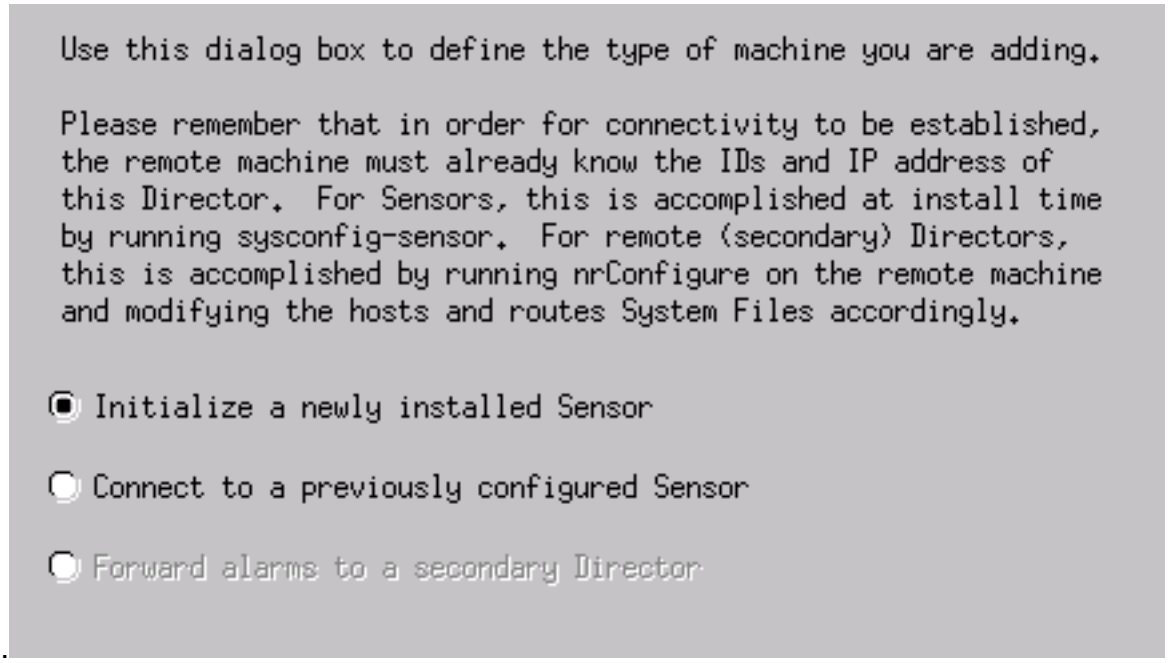
Adicionar o sensor no diretor

Termine estas etapas para adicionar o sensor no diretor.

1. Telnet a 10.64.21.50 (IDS diretor) com o **netrangr** username e o ataque de senha.
2. Datilografe o **ovw&** para lançar o HP OpenView.
3. Do menu principal, vá ao **Segurança > Configurar**.
4. Na utilidade do gerenciamento de arquivo de configuração, vá a **File > Add Host** e clique **em seguida**.
5. Termine a informação de host do sensor, segundo as indicações deste exemplo. Clique em Next.

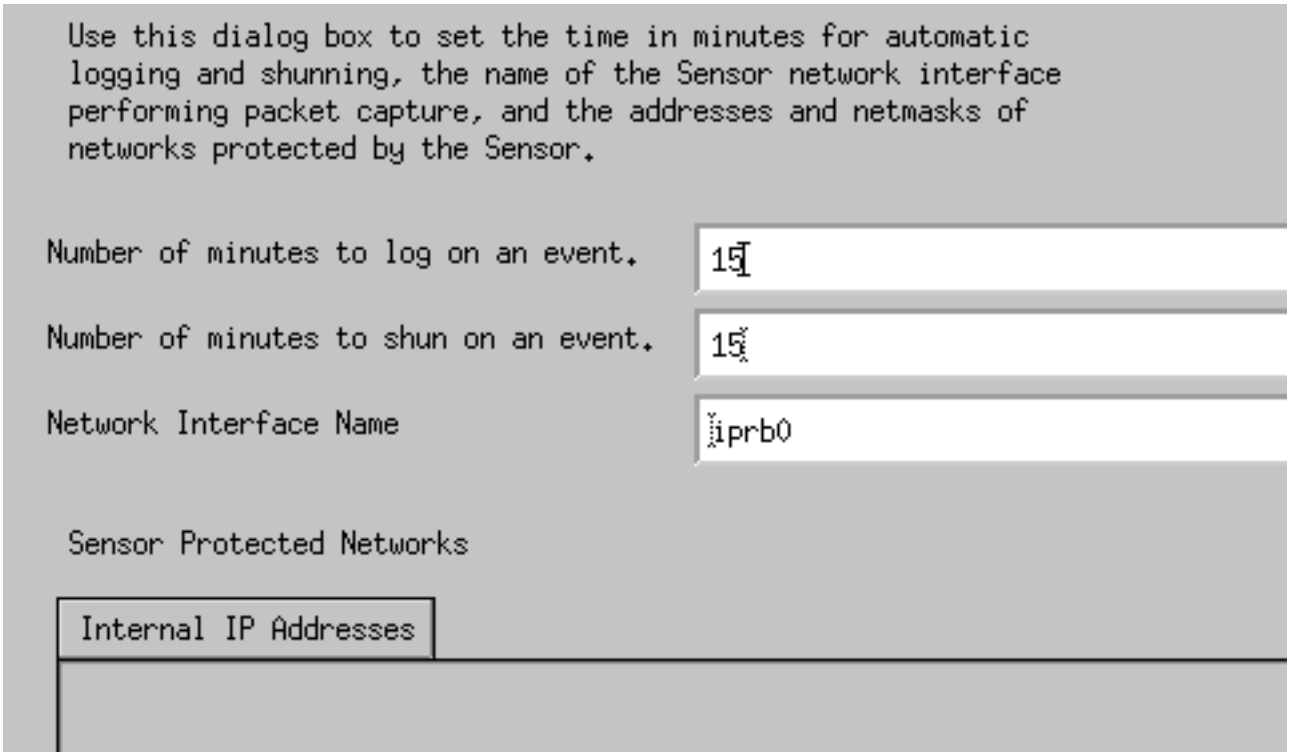


6. Aceite as configurações padrão para o tipo de máquina, e clique-as **em seguida**, segundo as indicações deste

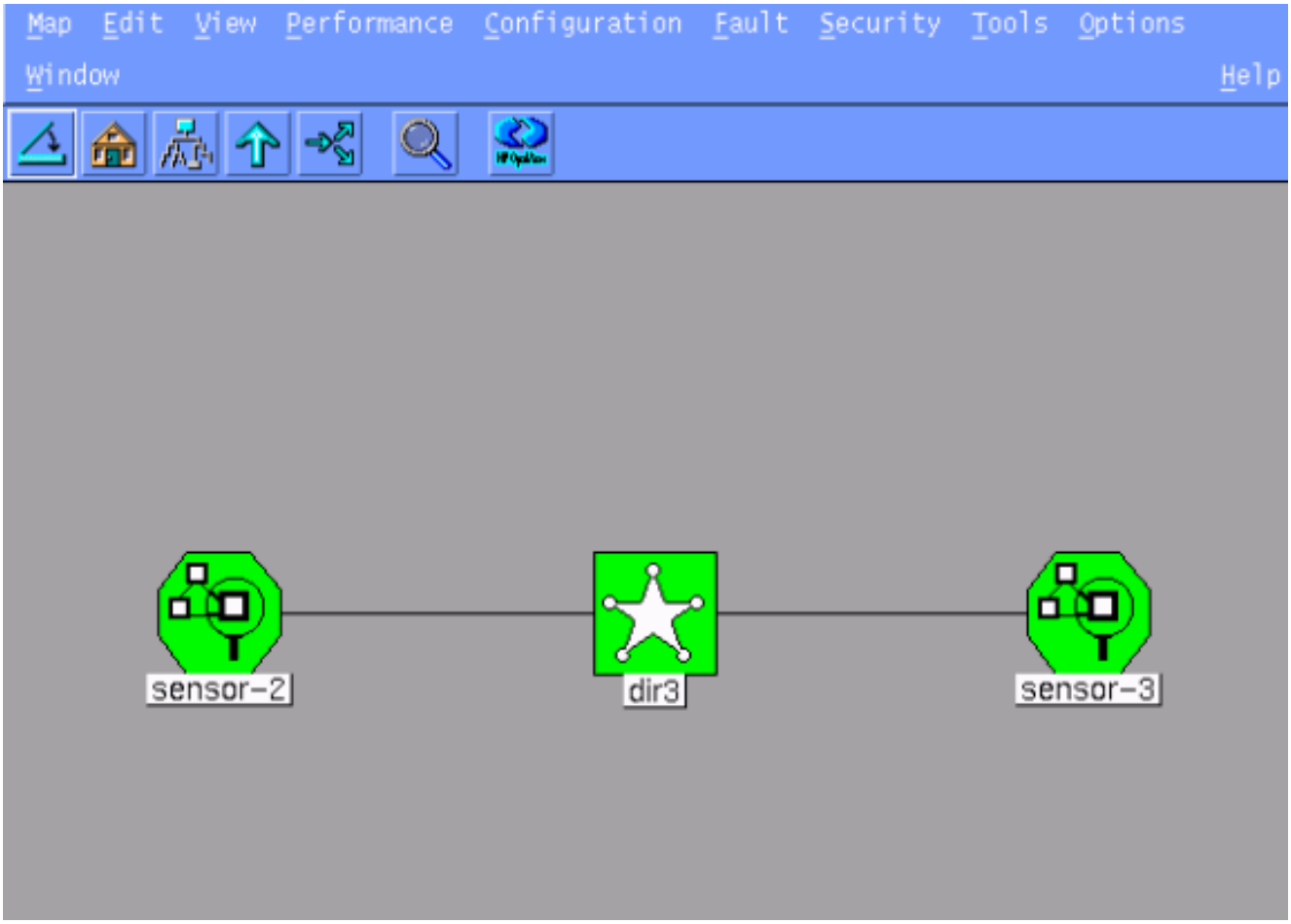


exemplo.

7. Você pode mudar o log e evitar-lo minutos ou pode aceitar os valores padrão. Contudo, você deve mudar o nome de interface de rede ao nome de seu farejando interface. Neste exemplo, é "iprb0". Pode ser "spwr0" ou qualquer outra coisa segundo o tipo de sensor e como você conecta seu
sensor.



8. Continue a clicar **em seguida** e a clicar então o **revestimento** para adicionar o sensor no diretor. Do menu principal, você deve agora ver o sensor 2, como neste
exemplo.

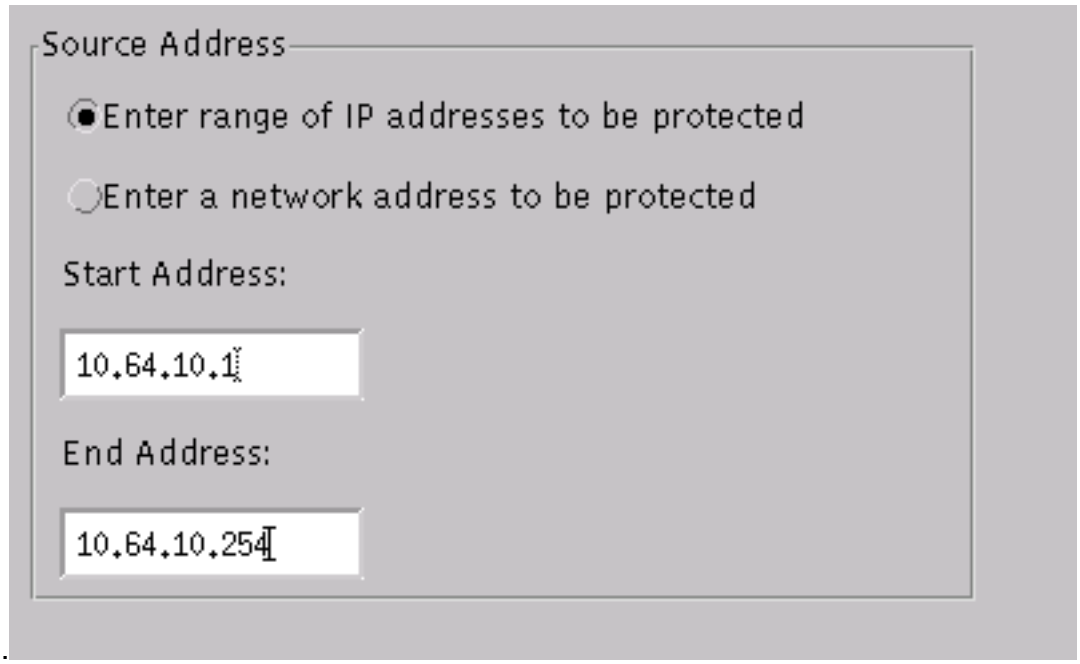


Configurar o TCP Reset para o roteador do Cisco IOS

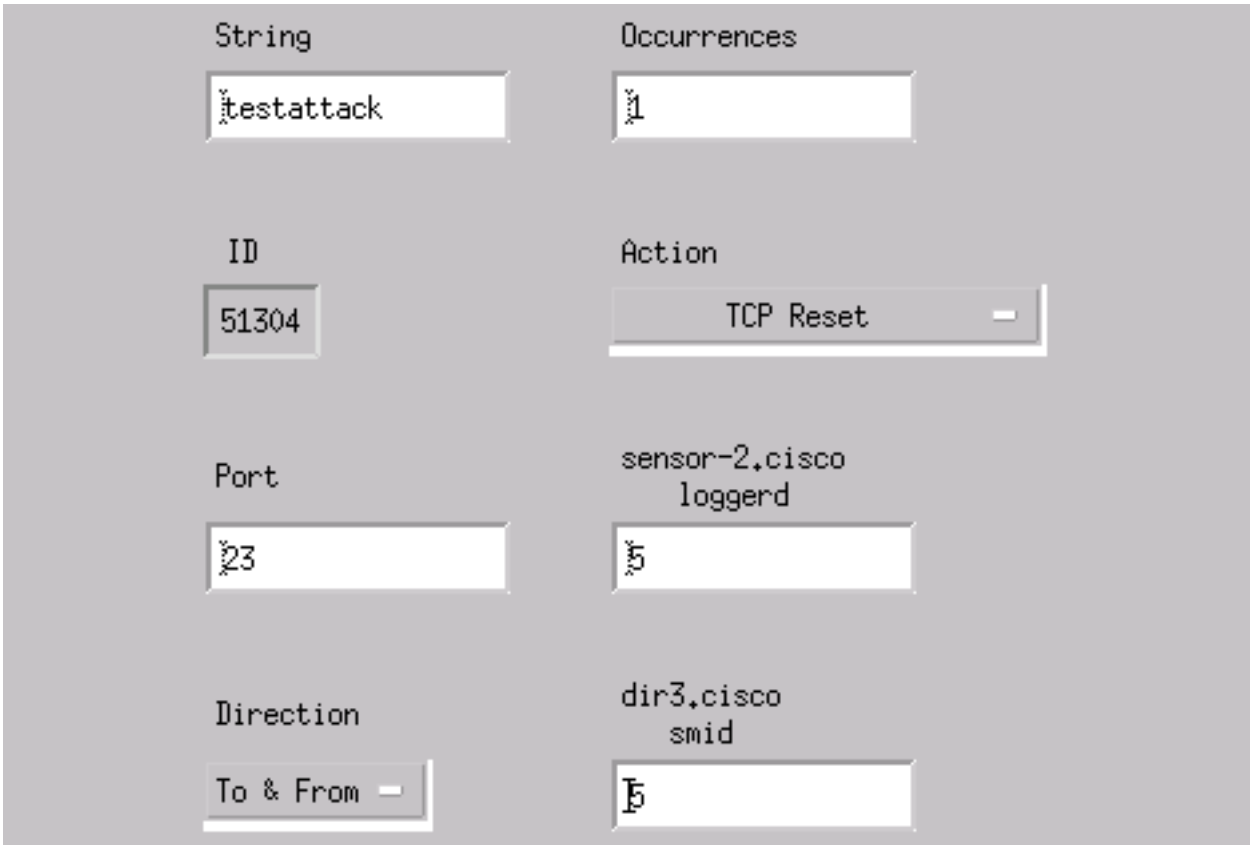
Termine estas etapas para configurar o TCP Reset para o roteador do Cisco IOS.

1. No menu principal, vá ao **Segurança > Configurar**.
2. Na utilidade do gerenciamento de arquivo de configuração, destaque o **sensor 2** e fazer-lo duplo clique.
3. Abra o Gerenciamento de dispositivos.
4. Clique o **Dispositivos > Adicionar**. Incorpore a informação do dispositivo, segundo as indicações do exemplo seguinte. Clique em OK para continuar. O telnet e permite senhas é Cisco.

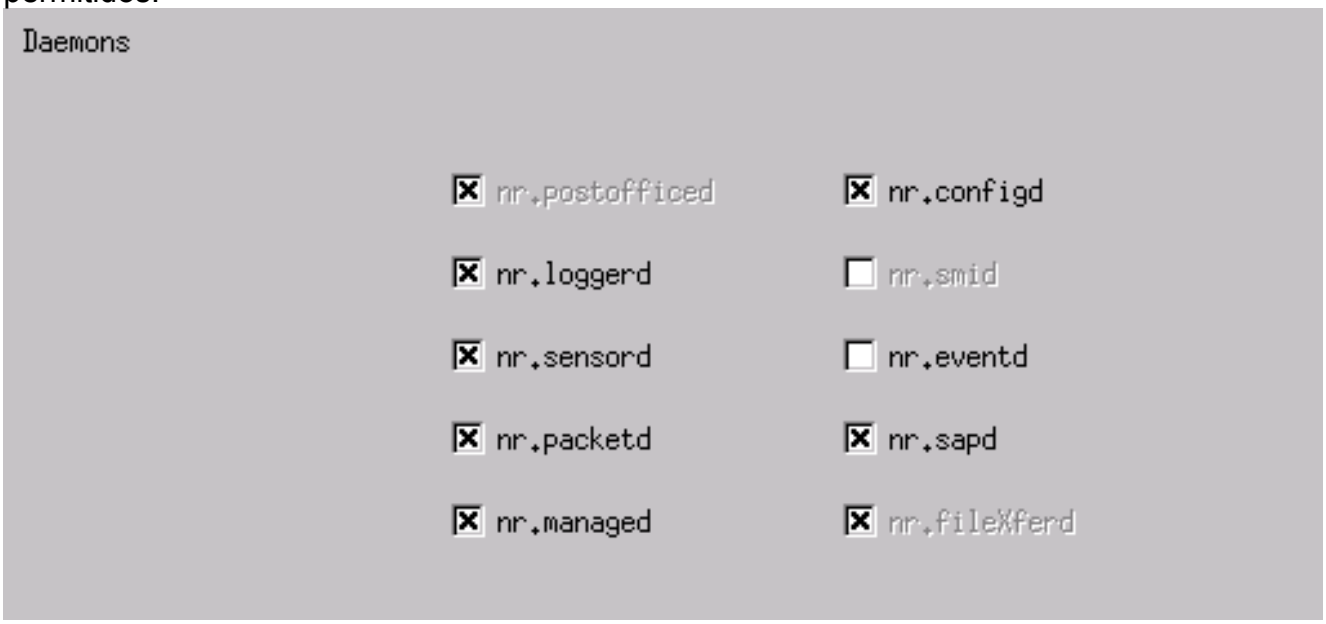
5. Abra o indicador da intrusion detection e clique **redes protegidas**. Adicionar o intervalo de endereço de 10.64.10.1 a 10.64.10.254 na rede protegida.



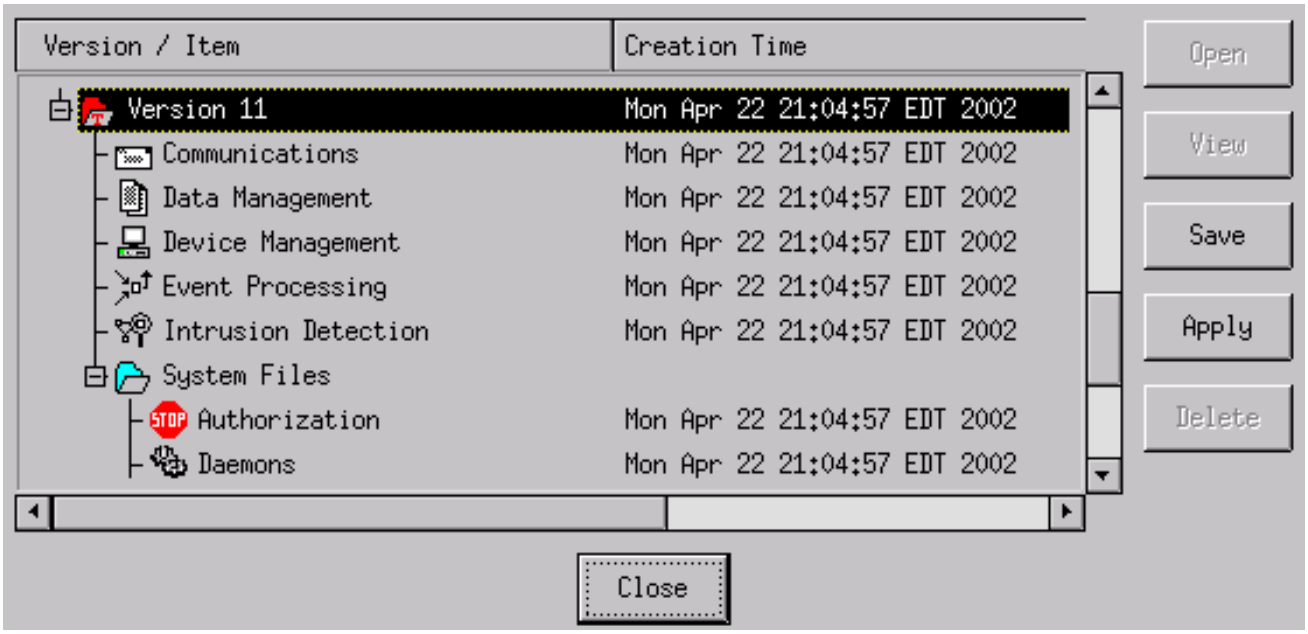
6. Clique o **perfil** e selecione a **configuração manual**. Em seguida, o clique **altera assinaturas**. Escolha **cordas combinadas** com um ID de 8000. Clique **Expand > Add** para adicionar uma corda nova chamada **ataque de teste**. Incorpore a informação da corda, segundo as indicações deste exemplo, e clique a **APROVAÇÃO** para continuar.



7. Você terminou este parte da configuração. **APROVAÇÃO do** clique para fechar o indicador da intrusion detection.
8. Abra o dobrador de arquivos de sistema, então a janela de Daemons. Certifique-se de você ter estes demônios
   permitidos:



9. Clique em OK para continuar.
10. Escolha a versão que você apenas alterou, clique a **salvaguarda** e **aplique-a** então. Espere o sistema para dizê-lo que o sensor terminou reiniciar serviços, a seguir fecham todos os indicadores para a configuração de
    diretor.



Inicie o ataque e a redefinição TCP

Telnet da luz de roteador à casa do roteador e ao tipo **ataque de teste**. Assim que você bater o espaço ou a tecla ENTER, suas restaurações da sessão de Telnet. Você conectará à casa do roteador.

```
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.
```

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Telnet a 10.64.10.49, o sensor, usando a raiz do nome de usuário e o ataque de senha. Datilografe o **CD /usr/nr/etc**. Datilografe o **gato packetd.conf. Se** você ajusta corretamente o TCP Reset para o ataque de teste, você deve ver uns quatro (4) no campo dos códigos de ação. Isto indica o TCP Reset segundo as indicações deste exemplo.

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

Se você ajusta acidentalmente a ação a “nenhuns” na assinatura, você verá um zero (0) no campo dos códigos de ação. Isto não indica nenhuma ação como visto neste exemplo.

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

As restaurações TCP são enviadas do farejando interface do sensor. Se há um interruptor que conecta a relação do sensor à interface externa do roteador controlado, quando você configura usando o **comando set span no** interruptor, use esta sintaxe:

```
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
```

Informações Relacionadas

- Notas de campo
- Página de suporte segura da prevenção de intrusão de Cisco
- Suporte Técnico e Documentação - Cisco Systems