

Estabelecendo evitar em um UNIX Diretor

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Verificar](#)

[Antes de um ataque é lançado](#)

[Lance o ataque e afastamento](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

[Introdução](#)

O diretor e o sensor do Sistema de Detecção de Intrusão da Cisco (IDS) podem ser usados para controlar um roteador Cisco para evitar. Neste documento, um sensor (sensor 2) é configurado a fim detectar ataques no roteador “casa” e a fim comunicar esta informação ao diretor “dir3.” configurado uma vez, um ataque é lançado (o sibilo de maior de 1024 bytes, que é a assinatura 2151, e de uma inundação do [ICMP] do protocolo Protocolo de control de mensajes de Internet (ICMP), que seja a assinatura 2152) do roteador a “luz.” O sensor detecta o ataque e comunica este ao diretor. Um Access Control List (ACL) é transferido ao roteador para evitar o tráfego do atacante. No host inalcançável do atacante é mostrado, e na vítima o ACL transferido é mostrado.

[Pré-requisitos](#)

[Requisitos](#)

Antes de você tentar esta configuração, verifique se estes requisitos são atendidos:

- Instale o sensor e certifique-se que trabalha corretamente.
- Assegure-se de que os períodos do farejando interface à interface externa do roteador.

[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
- Roteador do [®] do Cisco IOS com 12.2.6

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](#).

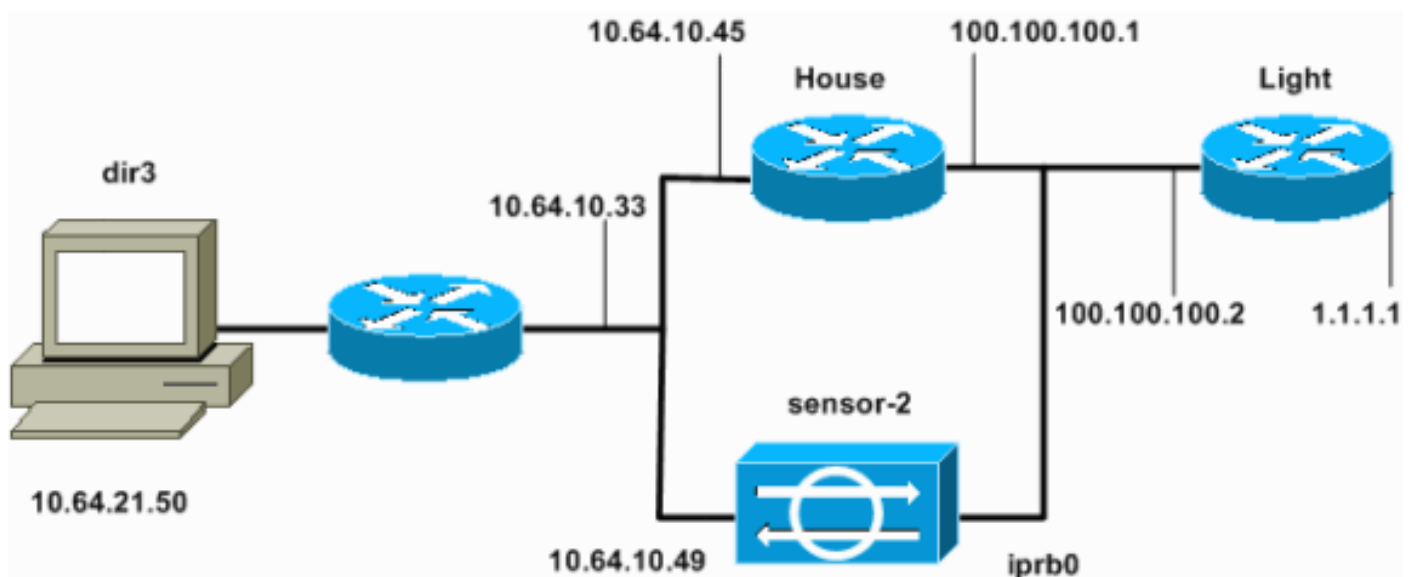
Configurar

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 !
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 !--- 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 o sensor](#)

Termine estas etapas para configurar o sensor.

1. Telnet a **10.64.10.49** com raiz do nome de usuário e ataque de senha.
2. Entre no **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.

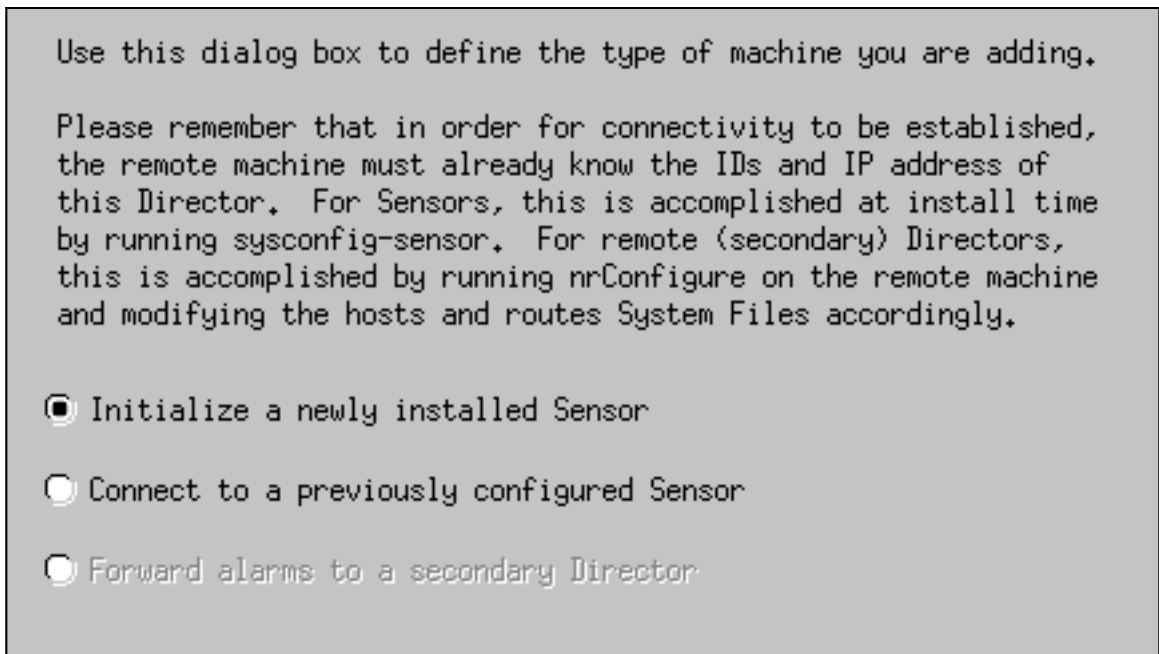
1. Telnet a **10.64.21.50** com **netrangr** e ataque de senha username.
2. Entre no **ovw&** para lançar o HP OpenView.
3. No menu principal, selecione o **Segurança > Configurar**.
4. Na utilidade do gerenciamento de arquivo de configuração, selecione **File > Add Host**, e clique **em seguida**.
5. Este é um exemplo de como completar a informação

Use this panel to specify the remote machine to which you wish to establish connectivity. If you need to add a new organization, click Create.

Organization name	cisco	Create...
Organization ID	900	
Host name	sensor-2	
Host ID	49	
Host IP Address	10.64.10.49	
<input type="checkbox"/>	Secondary Director	
<input type="checkbox"/>	IOS IDS	
<input checked="" type="checkbox"/>	Sensor / IDSM	

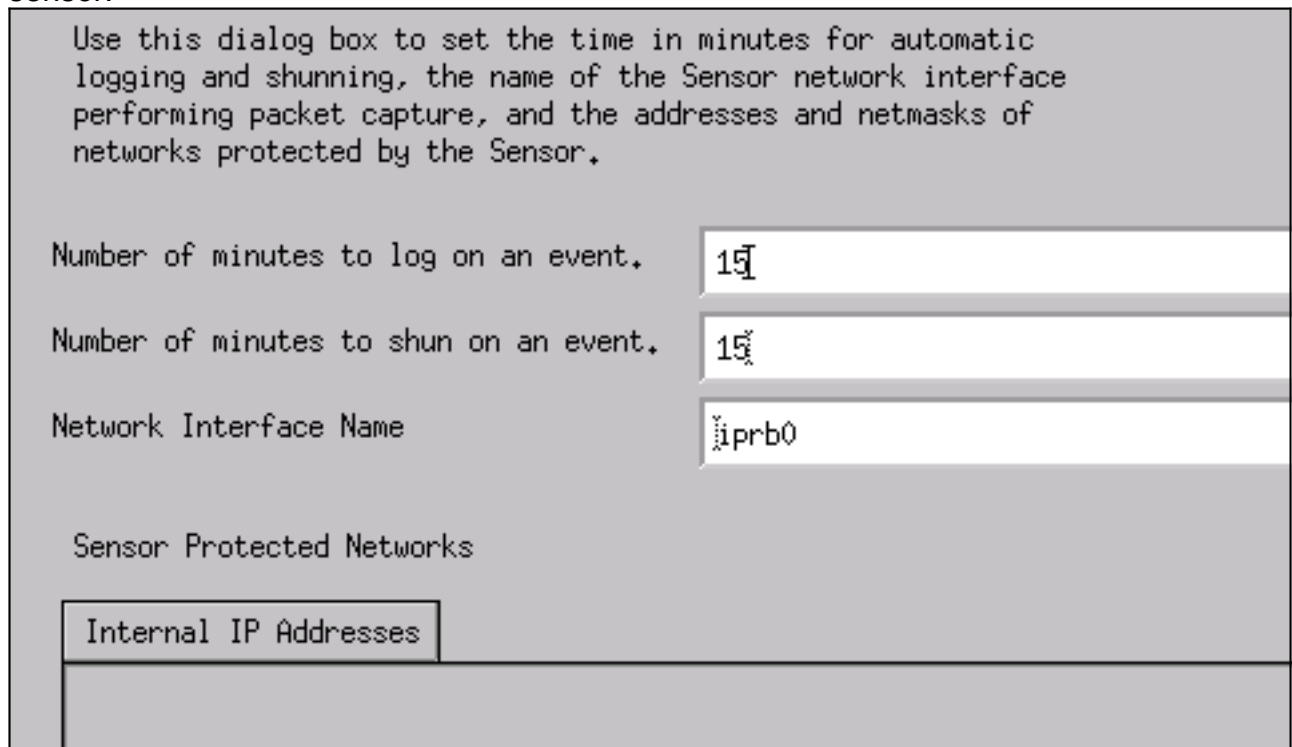
pedida.

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

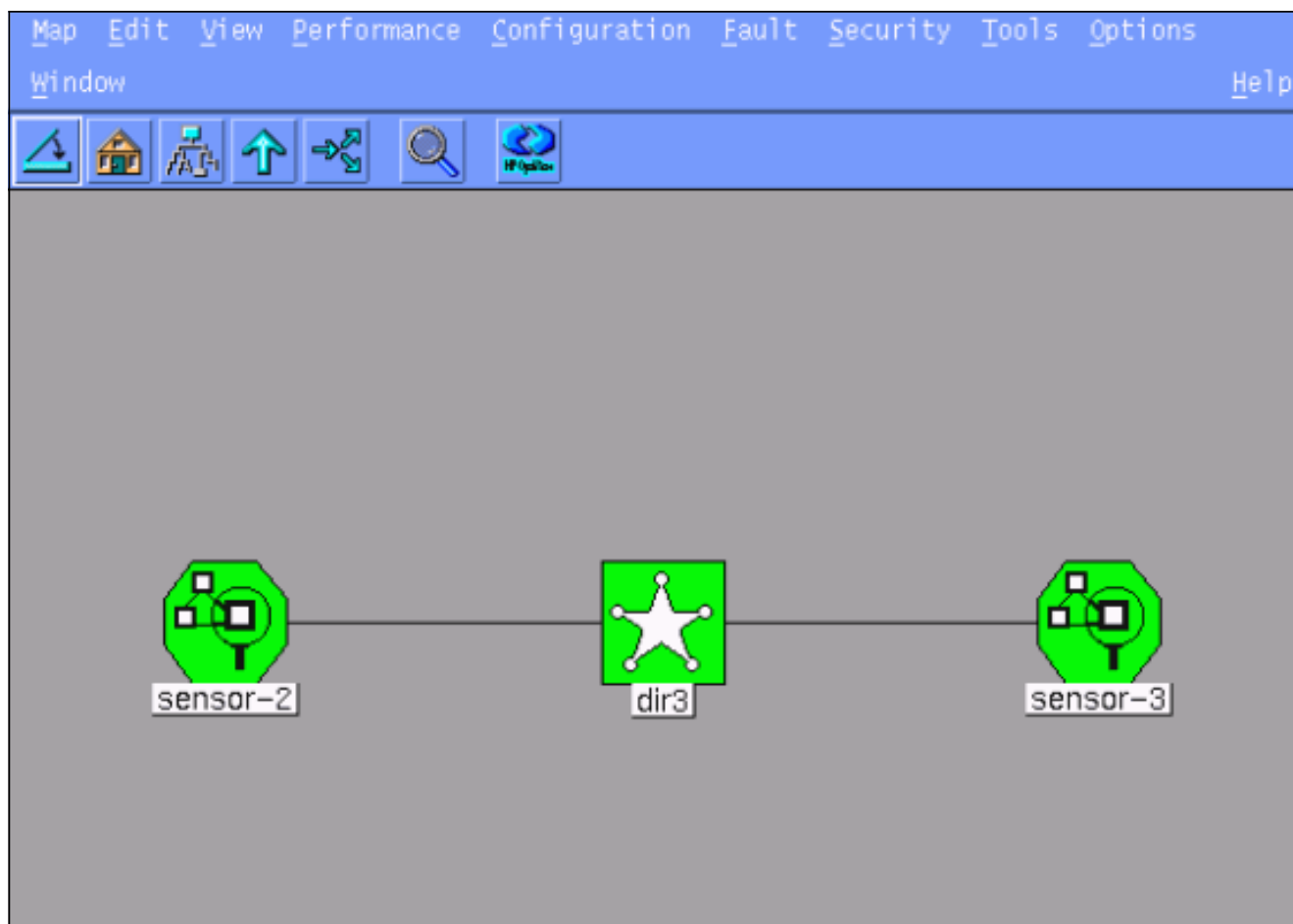


exemplo.

7. Mude o log e evitar minutos, ou deixe-os como o padrão se os valores são aceitáveis. Mude o nome de interface de rede ao nome de seu farejando interface. Neste exemplo é "iprb0." que pode ser "spwr0" ou qualquer outra coisa segundo o tipo de sensor e como você conecta seu sensor.



8. Clique **em seguida** até que haja uma opção para clicar o **revesti mento**. Você adicionou com sucesso o sensor no diretor. Do menu principal, você deve ver o `sensor 2`, como neste exemplo.



[Configurar evitar para o roteador do Cisco IOS](#)

Termine estas etapas para configurar evitar para o roteador do Cisco IOS.

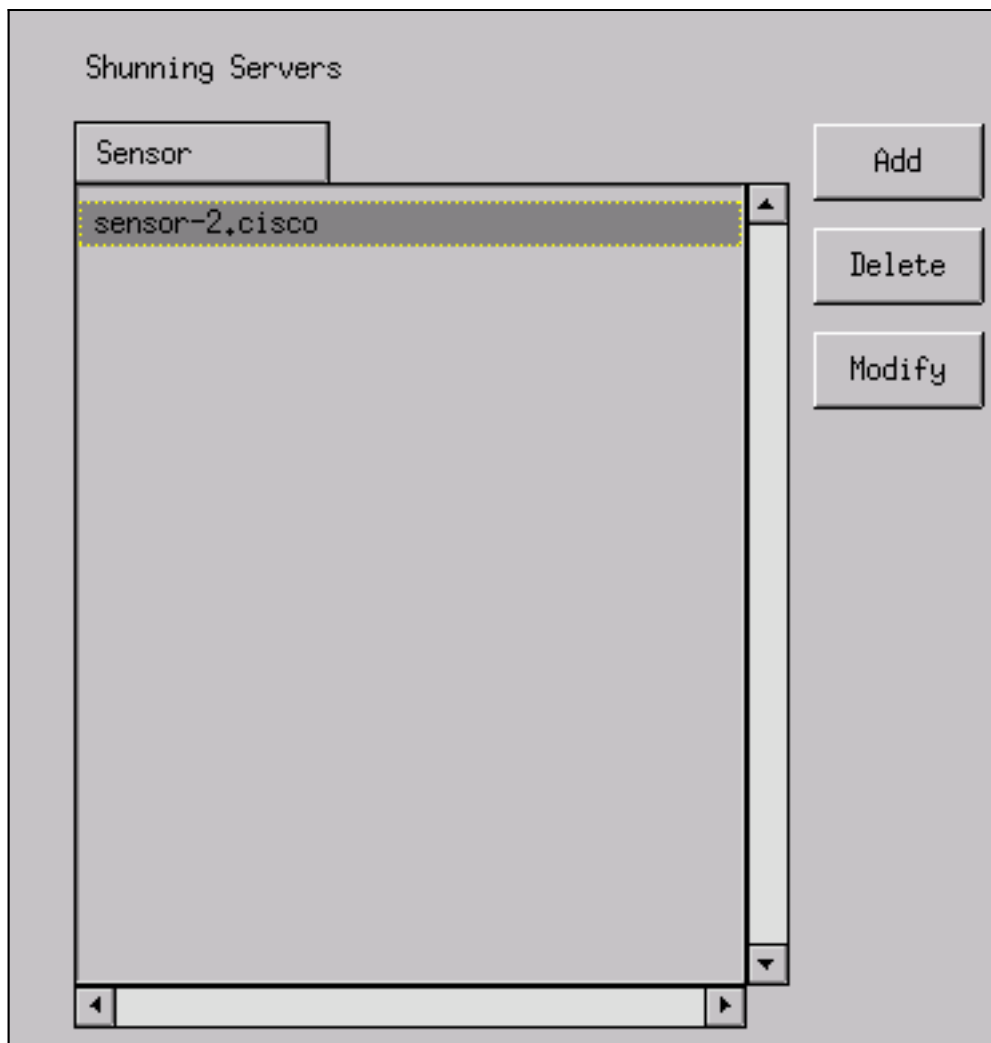
1. No menu principal, selecione o **Segurança > Configurar**.
2. Na utilidade do gerenciamento de arquivo de configuração, destaque o **sensor 2** e fazer-lo duplo clique.
3. Abra o **Gerenciamento de dispositivos**.
4. Clique o **Dispositivos > Adicionar**, e incorpore a informação segundo as indicações deste exemplo. Clique em OK para continuar. O telnet e permite o fósforo das senhas o que está no roteador
"casa."

IP Address	10.64.10.45	User Name	
Device Type	Cisco Router[Including Cat5kRSM,Cat6kMSFC] -	Password	****
Sensor's NAT IP Address		Enable Password	****
<input type="checkbox"/> Enable SSH			

5. Clicam o > **Add das relações**, incorporam esta informação, e clicam a **APROVAÇÃO** para continuar.

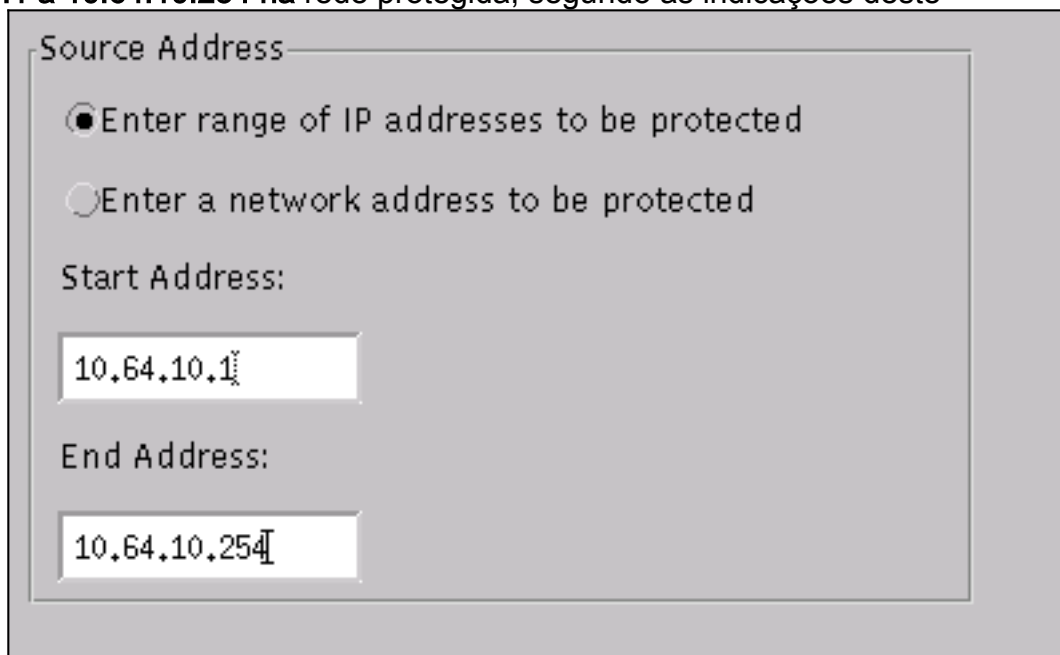
IP Address	10.64.10.45 -	PostShun ACL Name	198
PreShun ACL Name	199	Interface Name	FastEthernet0/0
Direction			
in -			

6. Clicam **Shunning** o > **Add** e seleccionam **sensor-2.cisco** como o server shunning. Feche o indicador do Gerenciamento de dispositivos quando você é



terminado.

7. Abra o indicador da intrusion detection, e clique **redes protegidas**. Adicionar a escala **10.64.10.1 a 10.64.10.254** na rede protegida, segundo as indicações deste



exemplo.

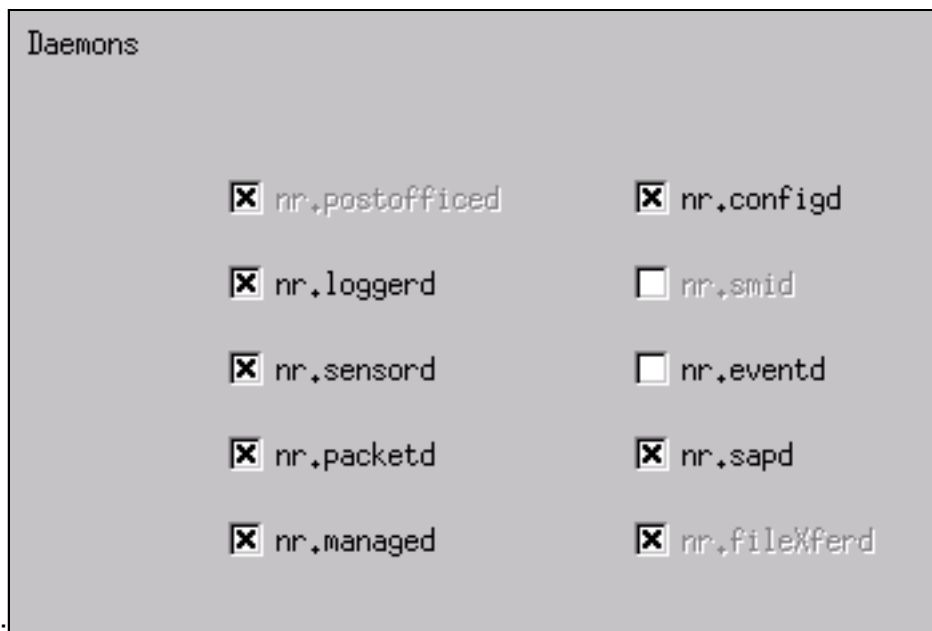
8. Clique o perfil > a configuração manual.
9. Seletor altere assinaturas > grande tráfego ICMP com um ID de 2151.
10. O clique altera, muda a ação de nenhuns evitar & registrar, e clica a APROVAÇÃO para continuar.

Signature	sensor-2,cisco loggerd
ICMP Flood	4
ID	dir3,cisco smid
2152	4
Action	
Shun & Log	

11. Escolha a **inundação ICMP** com um ID de **2152**, e o clique **altera**. Mude a **ação de nenhuns evitar & registrar**, e clique a **APROVAÇÃO** para continuar.

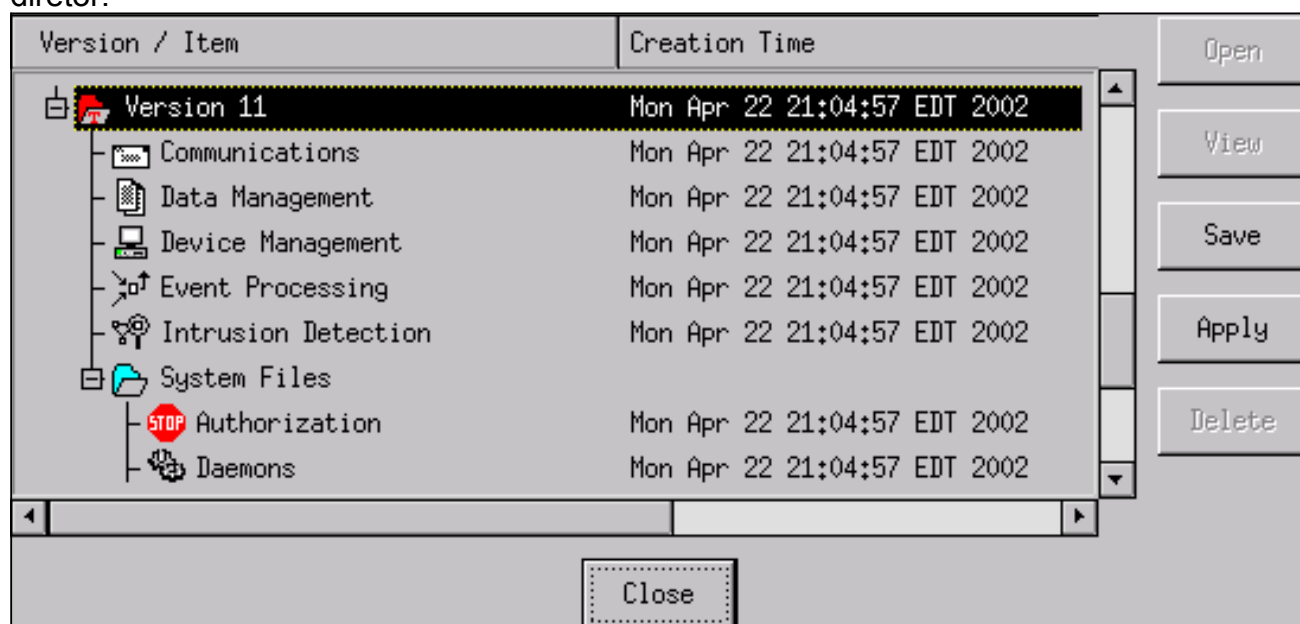
Signature	sensor-2,cisco loggerd
Large ICMP traffic	3
ID	dir3,cisco smid
2151	3
Action	
Shun & Log	

12. Clique a **APROVAÇÃO** para fechar o indicador da intrusion detection.
 13. Abra o dobrador de arquivos de sistema, e abra a janela de Daemons. Certifique-se de você ter permitido estes



demônios:

14. Clique a **APROVAÇÃO** para continuar, escolher a versão apenas alterada, e para clicar a **salv guarda** e **para aplicar-se** então. Espere o sistema para dizer-lhe o sensor terminado reiniciando serviços, a seguir feche todos os indicadores para a configuração de diretor.



Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração está funcionando adequadamente.

A [Output Interpreter Tool \(somente clientes registrados\)](#) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

- **lista de acesso da mostra** - Alista as indicações de **comando access-list** na configuração de roteador. Igualmente alista uma contagem da batida que indique que o número de vezes um elemento esteve combinado durante uma busca do **comando access-list**.
- **sibilo** - Usado para diagnosticar a conectividade de rede básica.

Antes de um ataque é lançado

Antes que um ataque esteja lançado, emita estes 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#
```

Lance o ataque e afastamento

Lance seu ataque do roteador “luz” à vítima “casa.” Quando o ACL toma a influência, os inalcançáveis estão vistos.

```
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.U.U.U.U.
```

Uma vez que o sensor detectou o ataque, e o ACL é transferido, e esta saída estão indicados na “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
```

Os inalcançáveis são vistos ainda na “luz,” segundo as indicações deste exemplo.

```
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)
```

Quinze minutos mais tarde, a “casa” vai para trás ao normal, porque evitar foi ajustado 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#
```

A “luz” pode sibilar a “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

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- [Página de suporte segura da prevenção de intrusão de Cisco](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)