

# Afastamento de IDS PIX usando o Cisco IDS UNIX Director

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Configure o sensor](#)

[Adicionar o sensor no diretor](#)

[Configurar evitar para o PIX](#)

[Verificar](#)

[Antes que você lançar o ataque](#)

[Lance o ataque e afastamento](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

## [Introdução](#)

Este documento descreve como configurar evitar em um PIX com a ajuda do Cisco IDS Unix Diretor (conhecido anteriormente como o Netranger Diretor) e do sensor. Este documento supõe que o sensor e o diretor são operacionais e o farejando interface do sensor se estabelece para medir à interface externa PIX.

## [Pré-requisitos](#)

### [Requisitos](#)

Não existem requisitos específicos para este documento.

### [Componentes Utilizados](#)

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

- Cisco IDS Unix Diretor 2.2.3
- UNIX Sensor 3.0.5 do Cisco IDS

- PIX seguro Cisco com 6.1.1 **Nota:** Se você usa a versão 6.2.x, você pode usar o Gerenciamento do protocolo secure shell (SSH), mas não o telnet. Refira a identificação de bug Cisco [CSCdx55215 \(clientes registrados somente\)](#) para mais informações.

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 é apresentado com a informação usada para configurar as características descritas neste documento.

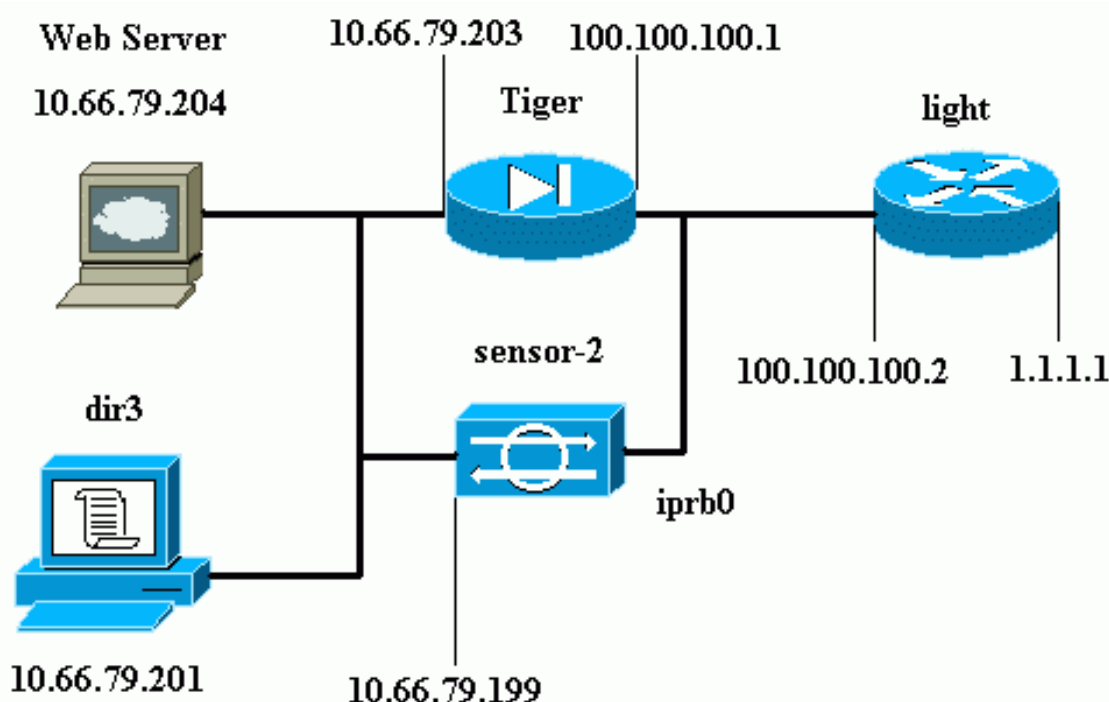
O Cisco IDS Unix Diretor e o sensor são usados a fim controlar um PIX seguro Cisco para evitar. Quando você considera esta configuração, recorde estes conceitos:

- Instale o sensor e certifique-se dos trabalhos do sensor corretamente.
- Assegure-se de que os períodos do farejando interface à interface externa do PIX.

**Nota:** A fim encontrar a informação adicional nos comandos usados neste documento, refira a [ferramenta de consulta de comandos \(clientes registrados somente\)](#).

## Diagrama de Rede

Este documento utiliza a seguinte configuração de rede.



## Configurações

Este documento utiliza estas configurações.

- [Luz do Roteador](#)
- [PIX Tiger](#)

### 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
```

### 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 o sensor

Estas etapas descrevem como configurar o sensor.

1. Telnet a **10.66.79.199** com raiz do nome de usuário e ataque de senha.
2. Entre no **sysconfig-sensor**.
3. Insira esta informação:Endereço IP: **10.66.79.199**IP netmask: **255.255.255.224**Nome de Host IP: **sensor 2**Rota padrão: **10.66.79.193**Controle de acesso de rede**10**.Infraestrutura de comunicaçõesID do host do sensor: **49**Identificação de organização do sensor: **900**Nome de host do sensor: **sensor 2**Nome de organização do sensor: **cisco**Endereço IP de Um ou Mais Servidores Cisco ICM NT do sensor: **10.66.79.199**ID do host do gerenciador de IDS: **50**Identificação de organização do gerenciador de IDS: **900**Nome de host do gerenciador de IDS: **dir3**Nome de organização do gerenciador de IDS: **cisco**Endereço IP de Um ou Mais Servidores Cisco ICM NT do gerenciador de IDS: **10.66.79.201**
4. Salve a configuração. As repartições do sensor então.

## Adicionar o sensor no diretor

Termine estas etapas a fim adicionar o sensor no diretor.

1. Telnet a **10.66.79.201** com **netrangr** e ataque de senha **username**.
2. Entre no **ovw&** a fim lançar o HP OpenView.
3. No menu principal, selecione o **Segurança > Configurar**.
4. No menu da configuração Netranger, selecione **File > Add Host**, e clique **em seguida**.
5. Incorpore esta informação, e clique-a **em**

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

Organization ID 900

Host name

Host ID

Host IP Address

Secondary Director

IOS IDS

Sensor / IDSM

seguida.

6. Deixe as configurações padrão e clique-as em

Use this dialog box to define the type of machine you are adding.

Please remember that in order for connectivity to be established, the remote machine must already know the IDs and IP address of this Director. For Sensors, this is accomplished at install time by running sysconfig-sensor. For remote (secondary) Directors, this is accomplished by running nrConfigure on the remote machine and modifying the hosts and routes System Files accordingly.

Initialize a newly installed Sensor

Connect to a previously configured Sensor

Forward alarms to a secondary Director

seguida.

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". Pode ser "spwr0" ou qualquer outra coisa baseado no tipo de sensor e como você conecta o sensor.

Use this dialog box to set the time in minutes for automatic logging and shunning, the name of the Sensor network interface performing packet capture, and the addresses and netmasks of networks protected by the Sensor.

Number of minutes to log on an event.

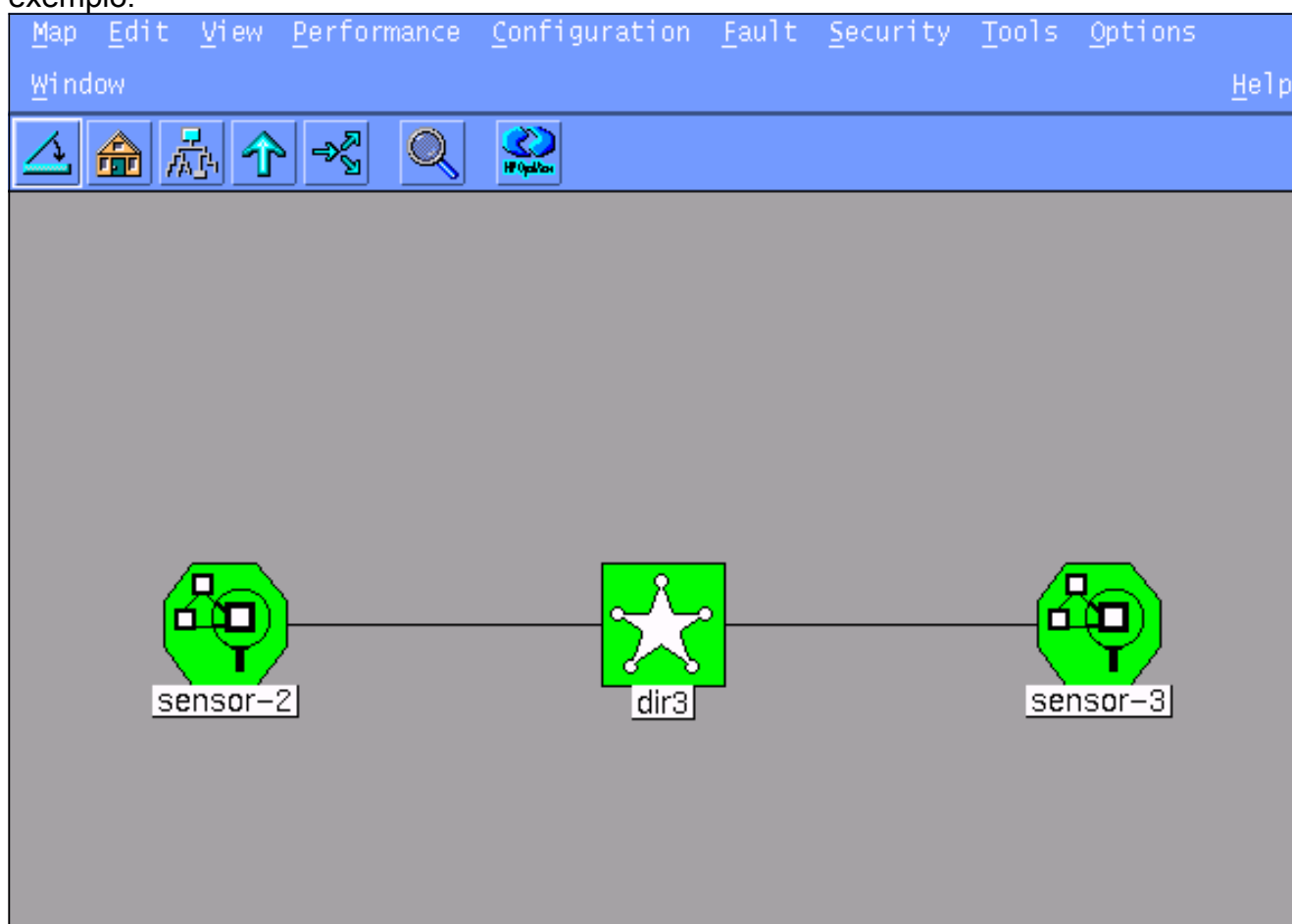
Number of minutes to shun on an event.

Network Interface Name

Sensor Protected Networks

Internal IP Addresses

8. Clique **em seguida** até que haja uma opção para clicar o **revestimento**. O sensor é adicionado agora com sucesso no diretor. Do menu principal, o **sensor 2** é indicado, segundo as indicações deste exemplo.



## [Configurar evitar para o PIX](#)

Termine estas etapas a fim configurar evitar para o PIX.

1. No menu principal, selecione o **Segurança > Configurar**.
2. No menu da configuração Netranger, 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 a **APROVAÇÃO** a fim continuar. O telnet e permite a senha é ambo o "Cisco".

IP Address: 10.66.79.203

User Name: [ ]

Device Type: PIX

Password: \*\*\*\*\*

Sensor's NAT IP Address: [ ]

Enable Password: \*\*\*\*\*

Enable SSH

5. >Add **Shunning** do clique. Adicionar o host 100.100.100.100 sob "endereços nunca para evitar." Clique a **APROVAÇÃO** a fim

General | Devices | Interfaces | **Shunning**

Maximum Number of Shunned Entries: 100

Addresses Never to Shun

Network Address	Network Mask
100.100.100.100	255.255.255.255

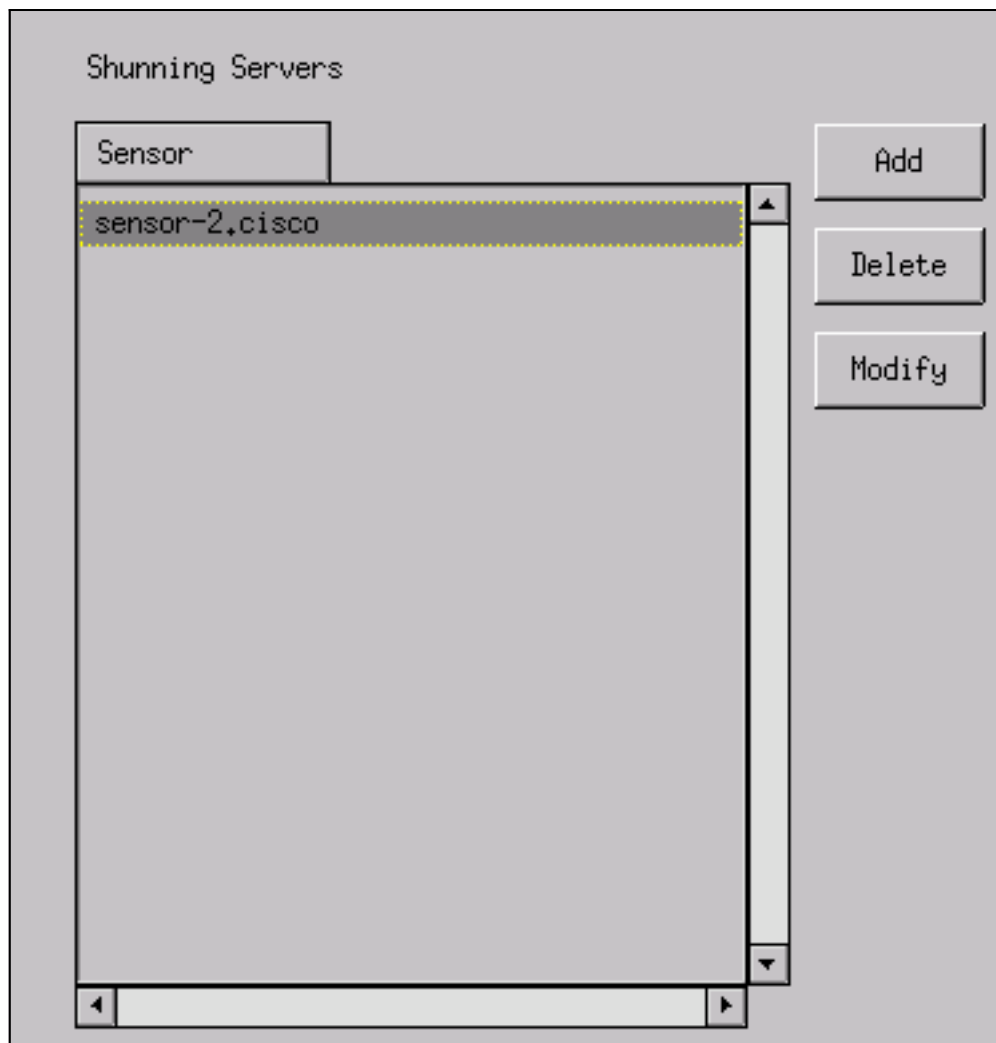
Add

Delete

Modify

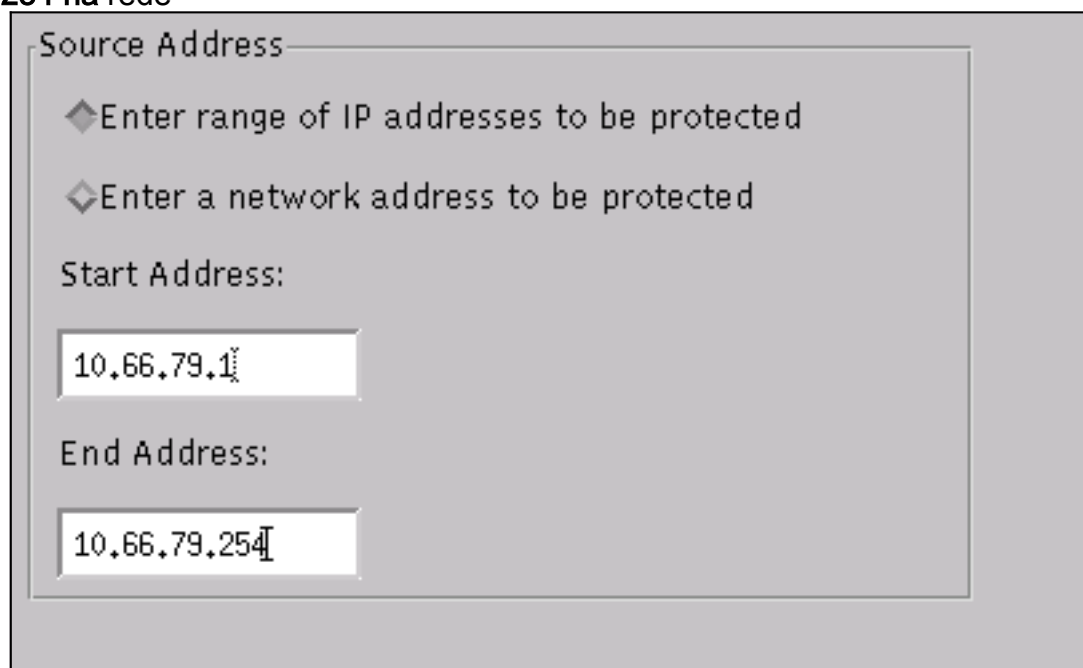
continuar.

6. Clique **Shunning** o > Add e selecione **sensor-2.cisco** como os server shunning. Isto a configuração é terminado parte de. Feche o indicador do Gerenciamento de



dispositivos.

7. Abra o indicador da intrusion detection e clique **redes protegidas**. Adicionar **10.66.79.1 a 10.66.79.254** na rede



protegida.

8. Clique o **perfil** e selecione **assinaturas da configuração manual** > **Modify**. Selecione o **grande tráfego ICMP** e o **ID: 2151**, clique **altera**, e muda a ação de nenhuns **evitar e registrar**. **APROVAÇÃO** do clique a fim continuar.



Signature	sensor-2,cisco loggerd
<input type="text" value="Large ICMP traffic"/>	<input type="text" value="3"/>
ID	dir3,cisco smid
<input type="text" value="2151"/>	<input type="text" value="3"/>
Action	
<input type="text" value="Shun &amp; Log -"/>	

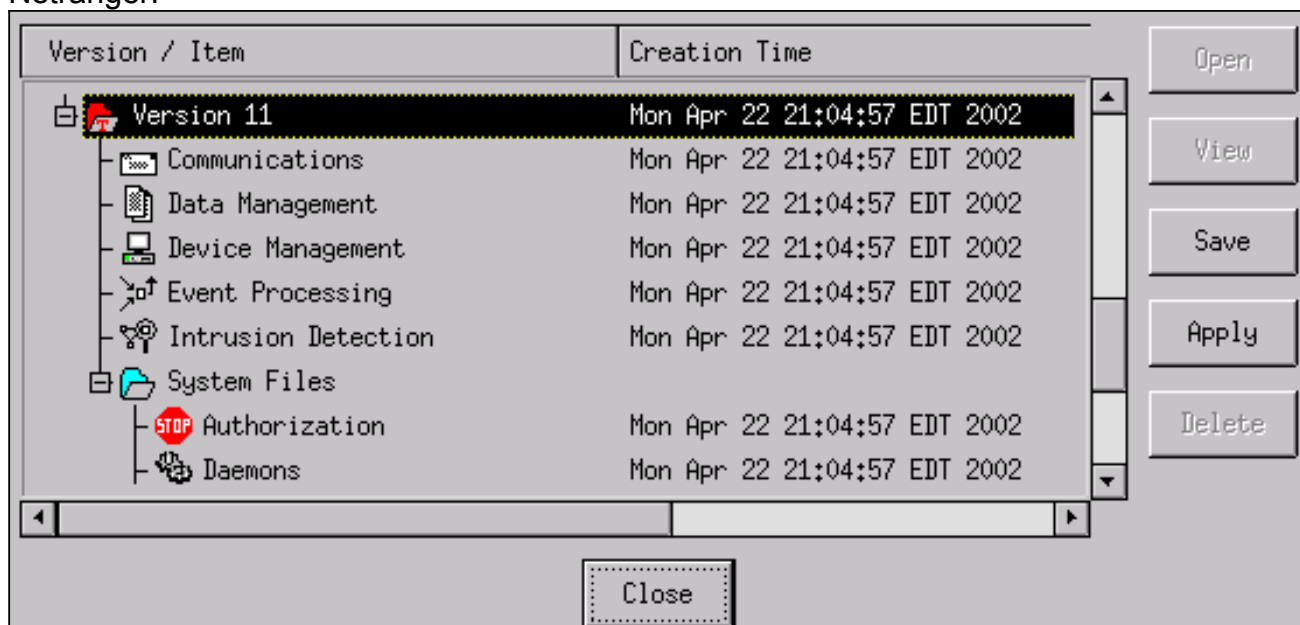
9. Selecione a **inundação ICMP** e o **ID: 2152**, clique **alterar**, e mudam a ação de **nenhuns evitar e registrar**. **APROVAÇÃO** do clique a fim continuar.

Signature	sensor-2,cisco loggerd
<input type="text" value="ICMP Flood"/>	<input type="text" value="4"/>
ID	dir3,cisco smid
<input type="text" value="2152"/>	<input type="text" value="4"/>
Action	
<input type="text" value="Shun &amp; Log -"/>	

10. Esta parte de configuração está completa. **APROVAÇÃO** do clique a fim fechar o indicador da intrusion detection.
11. Abra o dobrador de **arquivos de sistema** e abra a **janela de Daemons**. Assegure-se de que você permita estes demônios:



12. Clique a **APROVAÇÃO** a fim continuar, e selecionar a versão que você apenas alterou. A **salv guarda** do clique > **aplica-se**. Espere o sistema para dizê-lo que o sensor está terminado, reinicia serviços, e fecha todos os indicadores para a configuração Netranger.



## Verificar

Esta seção fornece a informação que o ajuda a confirmar corretamente seus trabalhos da configuração.

## Antes que você lançar o 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
```

## Lance o ataque e afastamento

```
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
```

Quinze minutos mais tarde, vai para trás ao normal porque evitar é ajustado a quinze 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

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

## Informações Relacionadas

- [Fim--venda para o Cisco IDS Diretor](#)
- [Fim da vida útil para a versão 3.x do Software do Cisco IDS Sensor](#)
- [Sustentação do produto do Sistema de prevenção de intrusões da Cisco](#)
- [Sustentação do produto do Software do firewall Cisco PIX](#)
- [Referências do comando Cisco Secure PIX Firewall](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)