Защита IDS PIX с использованием Cisco IDS UNIX Director

Содержание

Введение
Предварительные условия
Требования
Используемые компоненты
Условные обозначения
Настройка
Схема сети
Конфигурации
Настройка датчика
Добавьте датчик в управляющий узел
Настройте избегание для PIX
Проверка
Прежде чем вы пойдете в наступление
Запустите блокирование атак
Устранение неполадок
Дополнительные сведения

Введение

Этот документ описывает, как настроить избегание на PIX с помощью Cisco IDS Unix Director (раньше известный как Netranger Director) и Датчик. Этот документ предполагает, что Датчик и Управляющий узел в рабочем состоянии, и интерфейс анализатора Датчика установлен для охвата к внешнему интерфейсу PIX.

Предварительные условия

Требования

Для данного документа отсутствуют предварительные условия.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования.

- Cisco IDS Unix Director 2.2.3

- Датчик Unix Cisco IDS 3.0.5
- Cisco Secure PIX с 6.1.1**Примечание:** При использовании 6.2.x версия, можно использовать Протокол Secure Shell (SSH) управление, но не Telnet. См. идентификатор ошибки Cisco CSCdx55215 (только зарегистрированные клиенты) для получения дополнительной информации.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Настройка

В этом разделе приводятся сведения о настройке функций, описанных в данном документе.

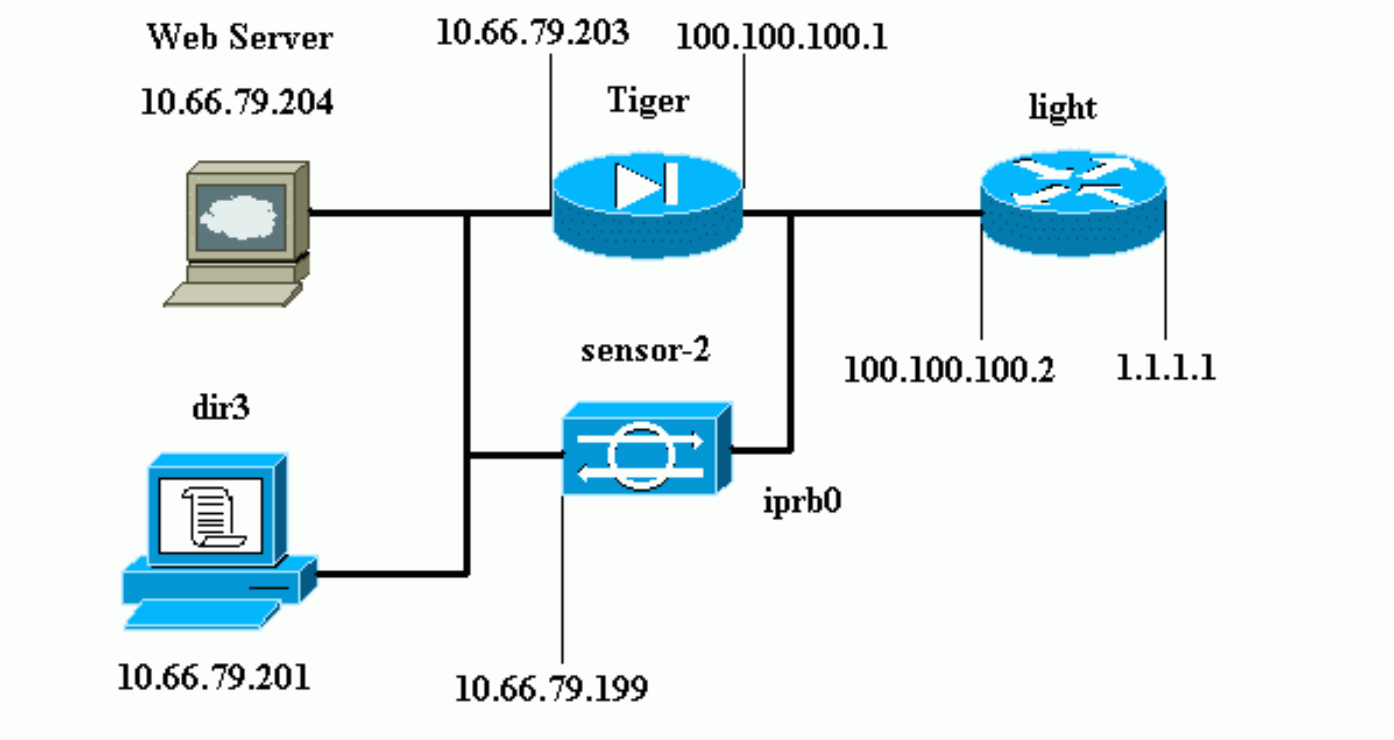
Cisco IDS Unix Director и Датчик используются для управления Cisco Secure PIX для того, чтобы избежать. Когда вы рассмотрите эту конфигурацию, помните эти понятия:

- Установите Датчик и удостоверьтесь, что Датчик работает должным образом.
- Гарантируйте, что интерфейс анализатора охватывает к внешнему интерфейсу PIX.

Примечание: Чтобы найти, что дополнительные сведения о командах, используемых в этом документе, обращаются к Средству поиска команд Command Lookup Tool (только зарегистрированные клиенты).

Схема сети

В настоящем документе используется следующая схема сети.



Конфигурации

Эти конфигурации используются в данном документе.

- Маршрутизатор light
- PIX Tiger

Маршрутизатор light

```
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
```

Настройка датчика

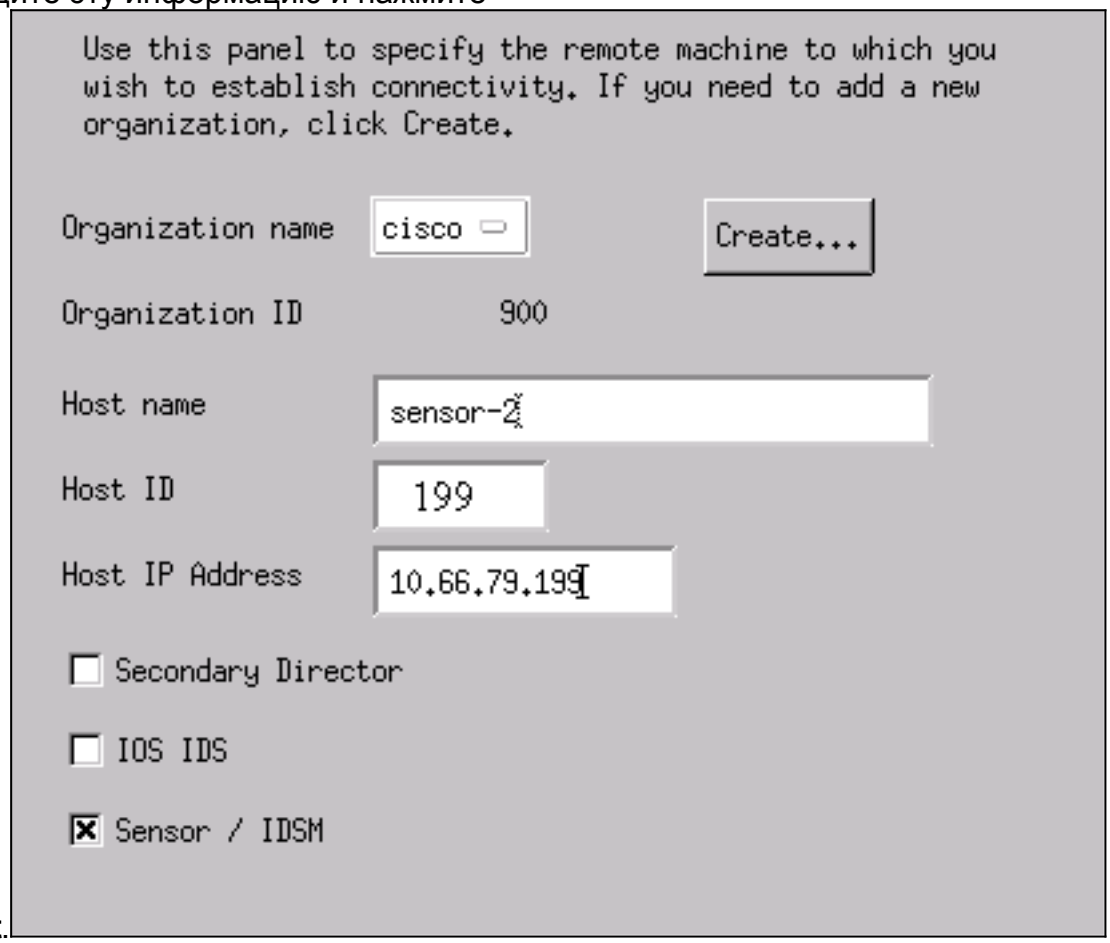
Эти шаги описывают, как настроить Датчик.

1. Telnet к **10.66.79.199** с **пользователем root** и **атакой пароля**.
2. Введите **sysconfig-sensor**.
3. Введите эти сведения:IP-адрес: **10.66.79.199**IP Netmask: **255.255.255.224**Название IP-узла: **sensor-2**Маршрут по умолчанию: **10.66.79.193**Управление доступом к сети**10.**Инфраструктура связиИдентификатор хоста датчика: **49**Идентификатор организации датчика: **900**Имя хоста датчика: **sensor-2**Название организации датчика: **cisco**IP-адрес датчика: **10.66.79.199**Идентификатор хоста диспетчера IDS: **50**Идентификатор организации диспетчера IDS: **900**Имя хоста Диспетчера IDS: **dir3**Название организации диспетчера IDS: **cisco**IP-адрес диспетчера IDS: **10.66.79.201**
4. Сохраните конфигурацию. Датчик тогда перезагрузки.

Добавьте датчик в управляющий узел

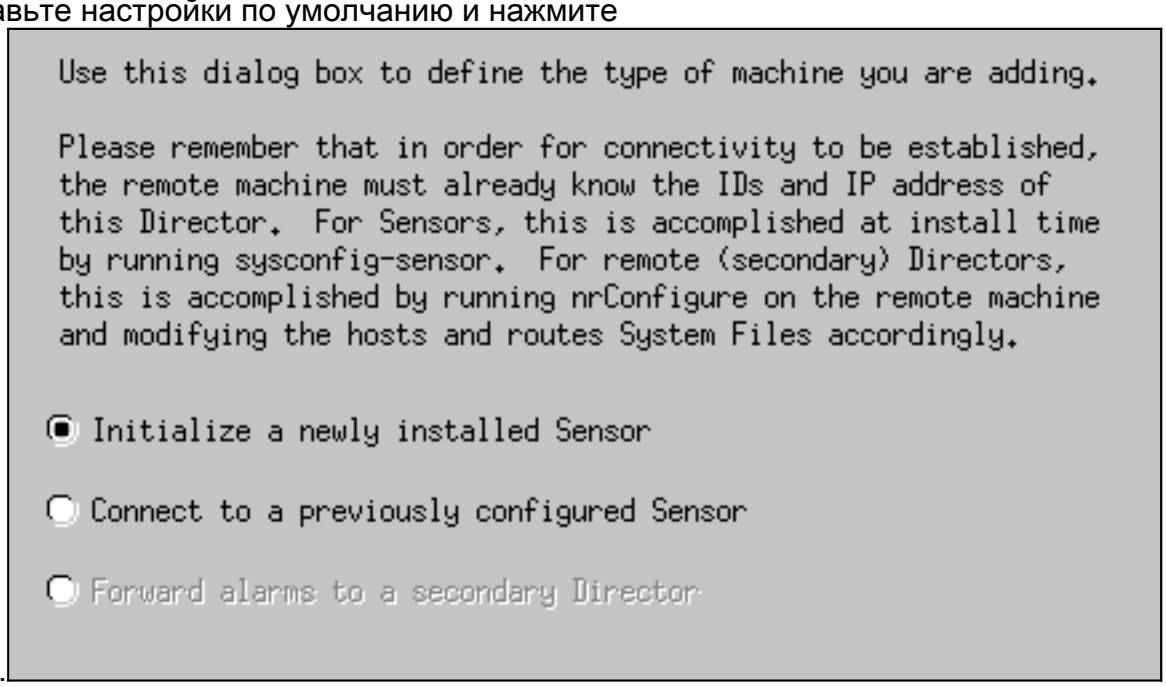
Выполните эти шаги для добавления Датчика в Управляющий узел.

1. Telnet к **10.66.79.201** с **netrangr** имени пользователя и **атакой пароля**.
2. Введите **ovw&** для запуска HP OpenView.
3. В Главном меню выберите **Security> Configure**.
4. В Меню конфигурации Netranger выберите **File> Add Host** и нажмите **Next**.
5. Введите эту информацию и нажмите



Next.

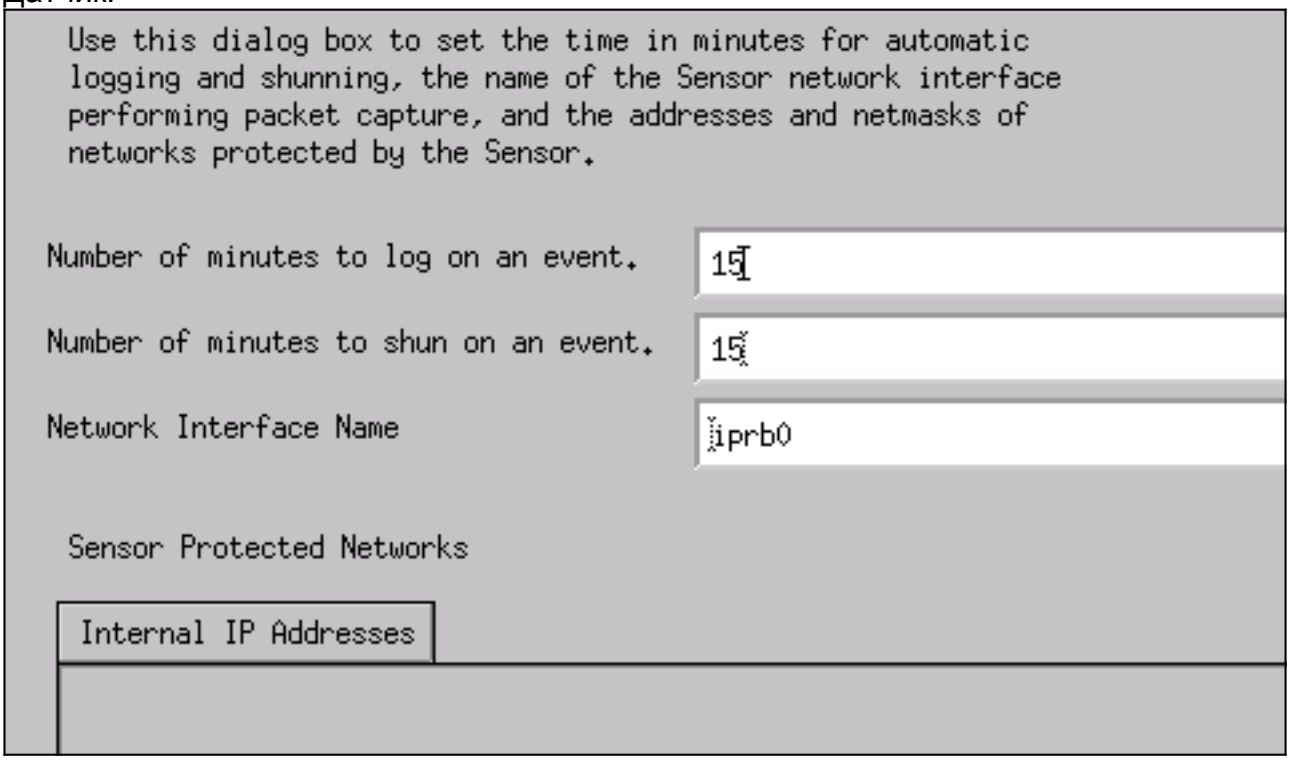
6. Оставьте настройки по умолчанию и нажмите



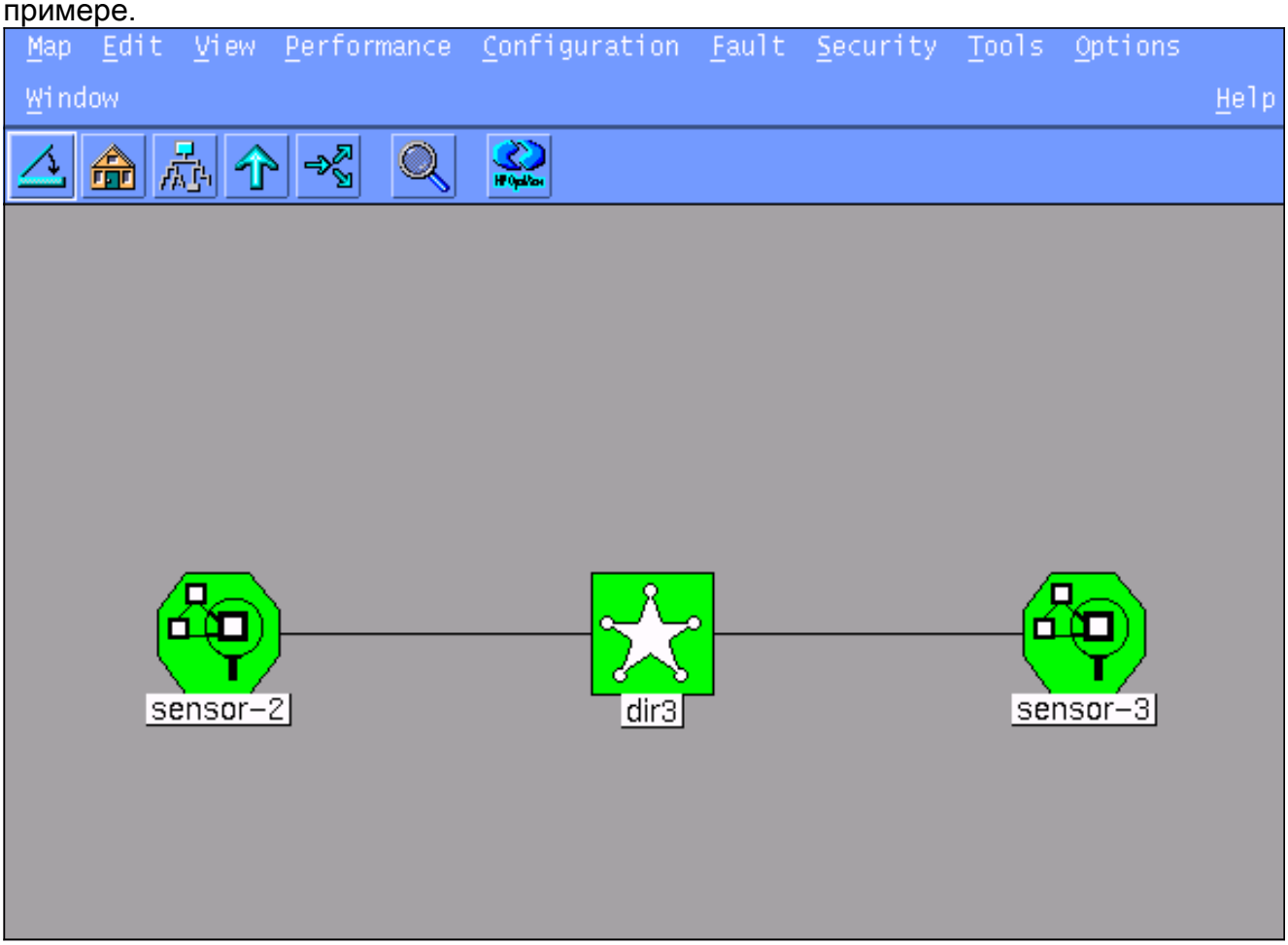
Next.

7. Измените журнал и избегите минут или оставьте их как по умолчанию, если значения приемлемы. Измените Имя сетевого интерфейса на название вашего интерфейса

анализатора. В данном примере это - "iprb0". Это может быть "spwr0" или что-либо еще на основе Типа датчика и как вы подключаете
Датчик.



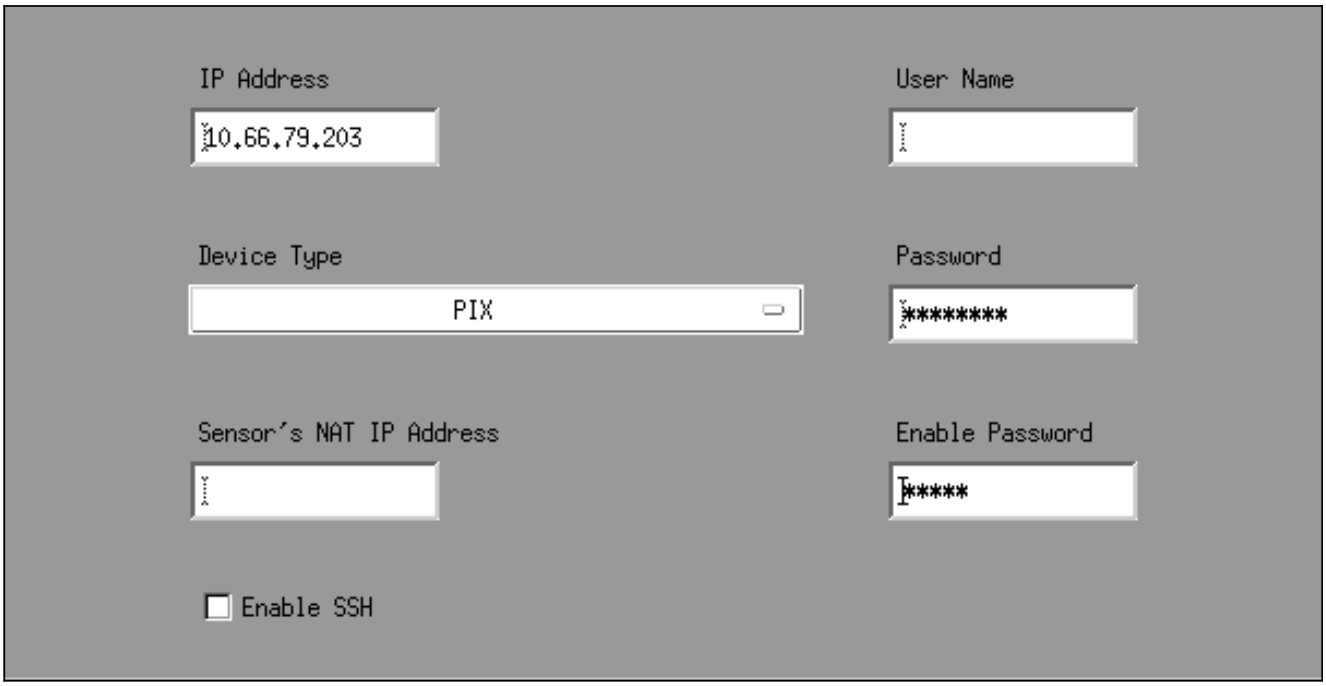
8. Нажмите **Next**, пока не будет опция для нажатия **Finish**.Датчик теперь успешно добавлен в Управляющий узел. Из главного меню **sensor-2** отображен, как показано в данном
примере.



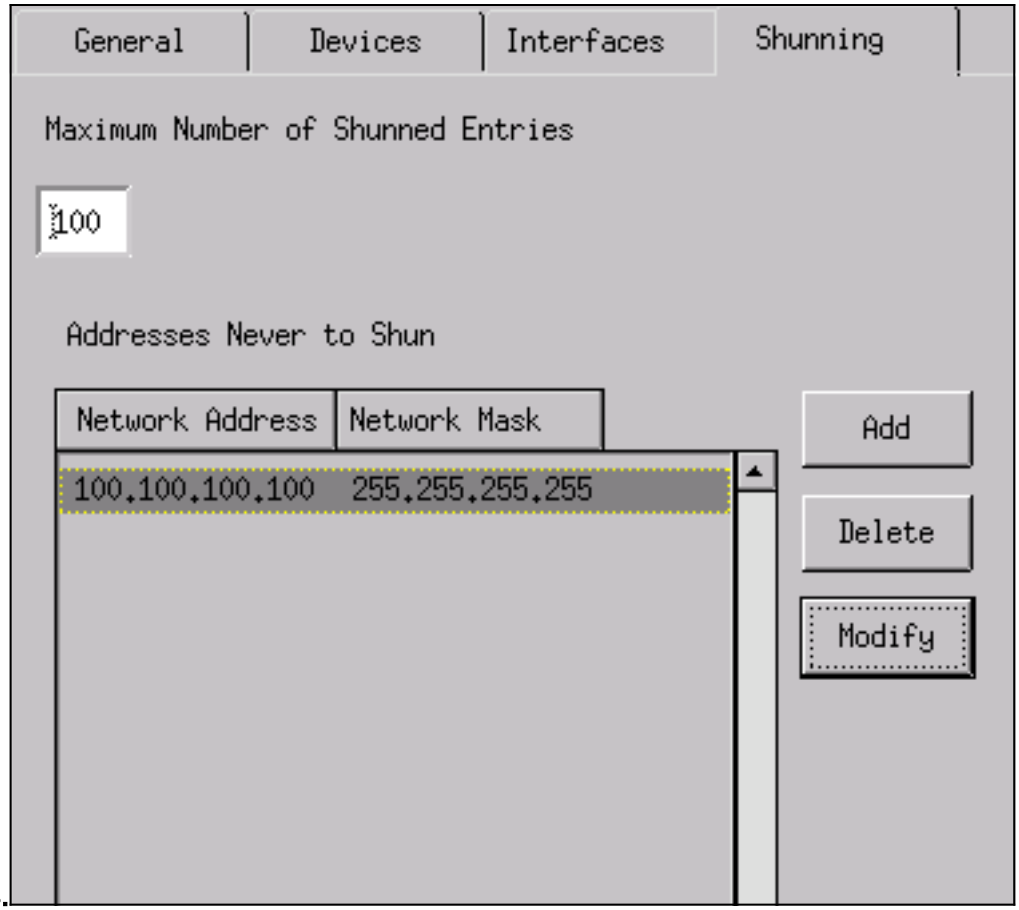
Настройте избегание для PIX

Выполните эти шаги для настройки избегания для PIX.

1. В Главном меню выберите **Security> Configure**.
2. В Меню конфигурации Netranger выделите **sensor-2** и двойной щелчок это.
3. Открытое **управление устройствами**.
4. Нажмите **Devices> Add** и введите информацию как показано в данный пример. **Нажмите OK, чтобы продолжить**. Telnet и enable password является оба "Cisco".

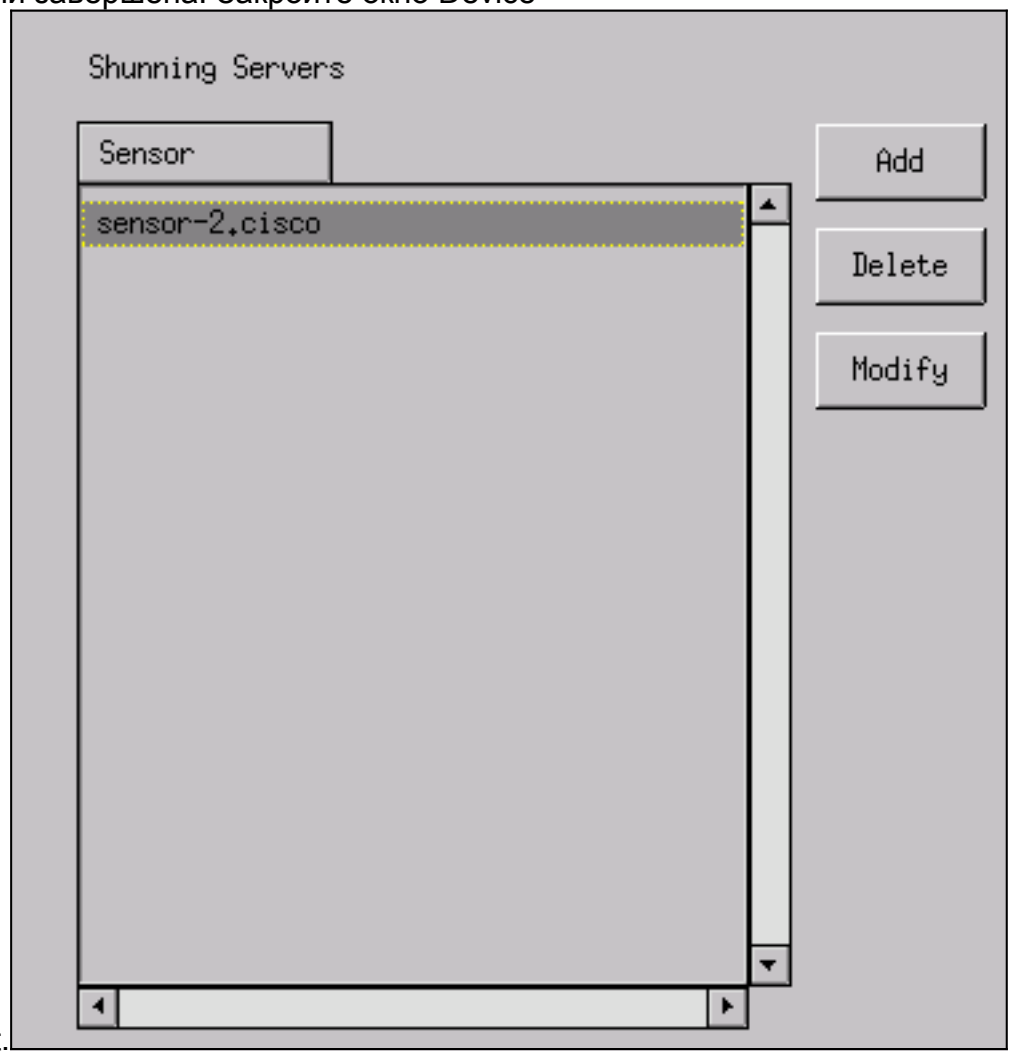


5. Нажмите **Shunning> Add**. Добавьте **хост 100.100.100.100** под "Адресами, чтобы никогда Избежать. **Нажмите OK, чтобы**



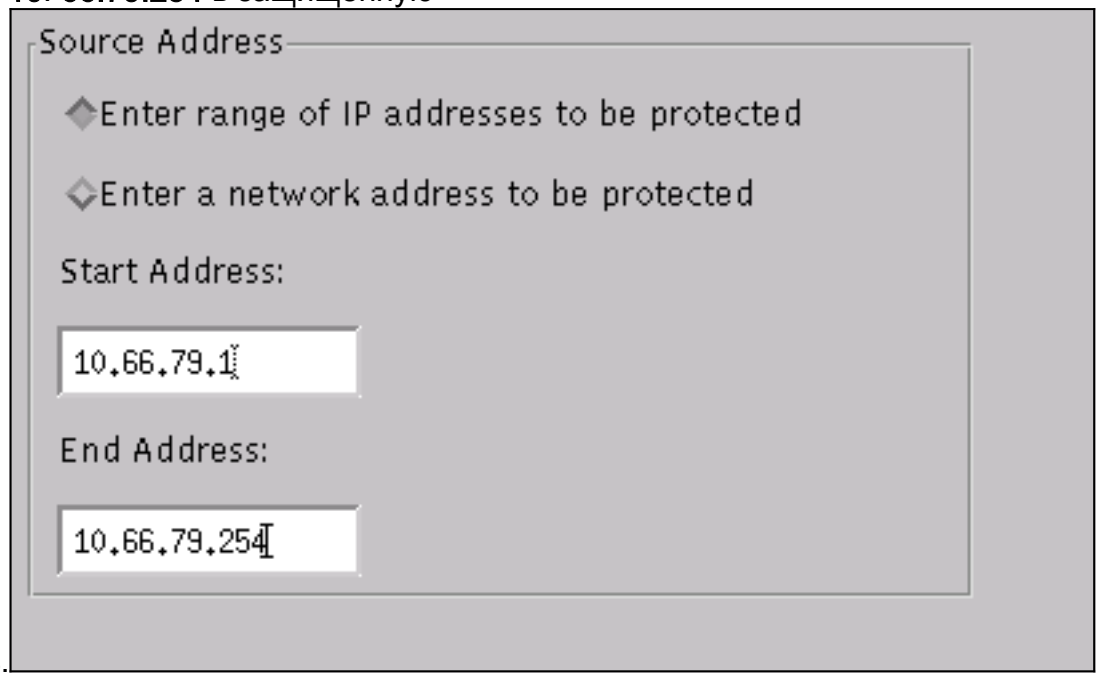
продолжить.

6. Нажмите **Shunning> Add** и выберите **датчик-2.cisco** как избегающие серверы. Эта часть конфигурации завершена. Закройте окно Device



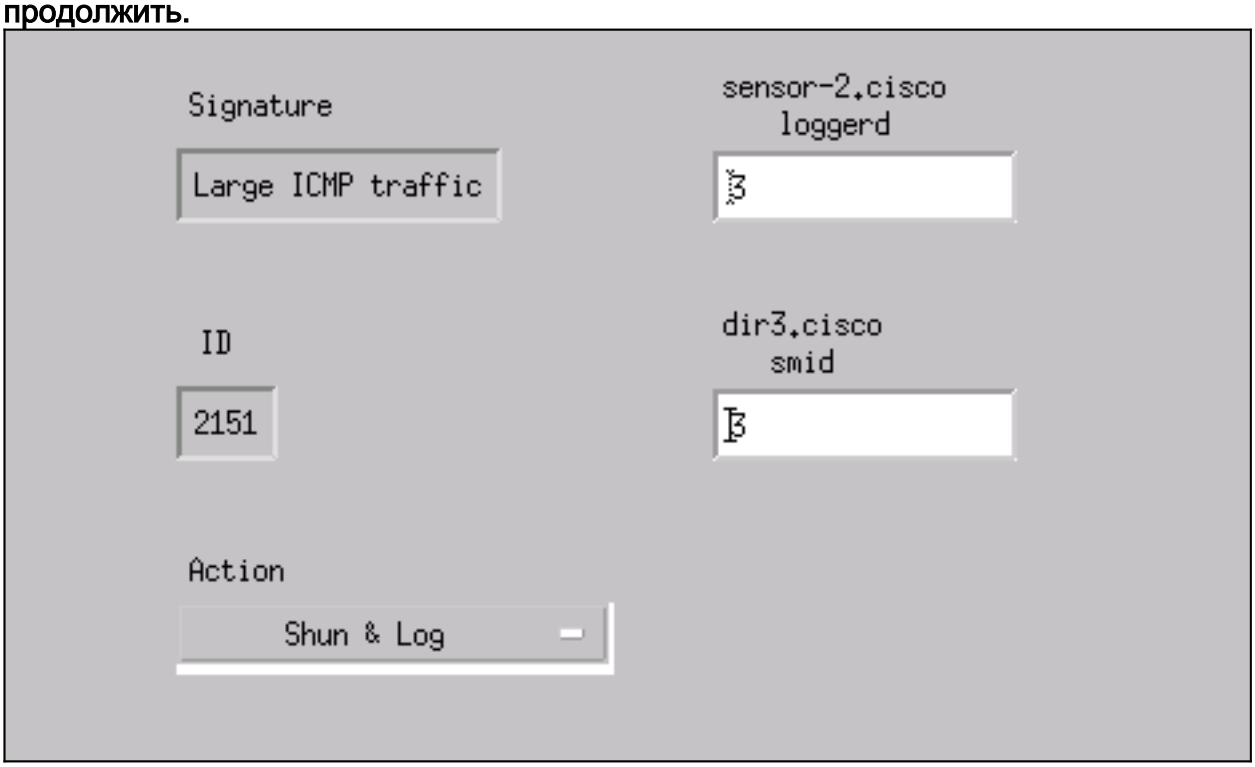
Management.

7. Откройте окно Intrusion Detection и нажмите **Protected Networks**. Добавьте **10.66.79. От 1 до 10**. **66.79.254** в защищенную

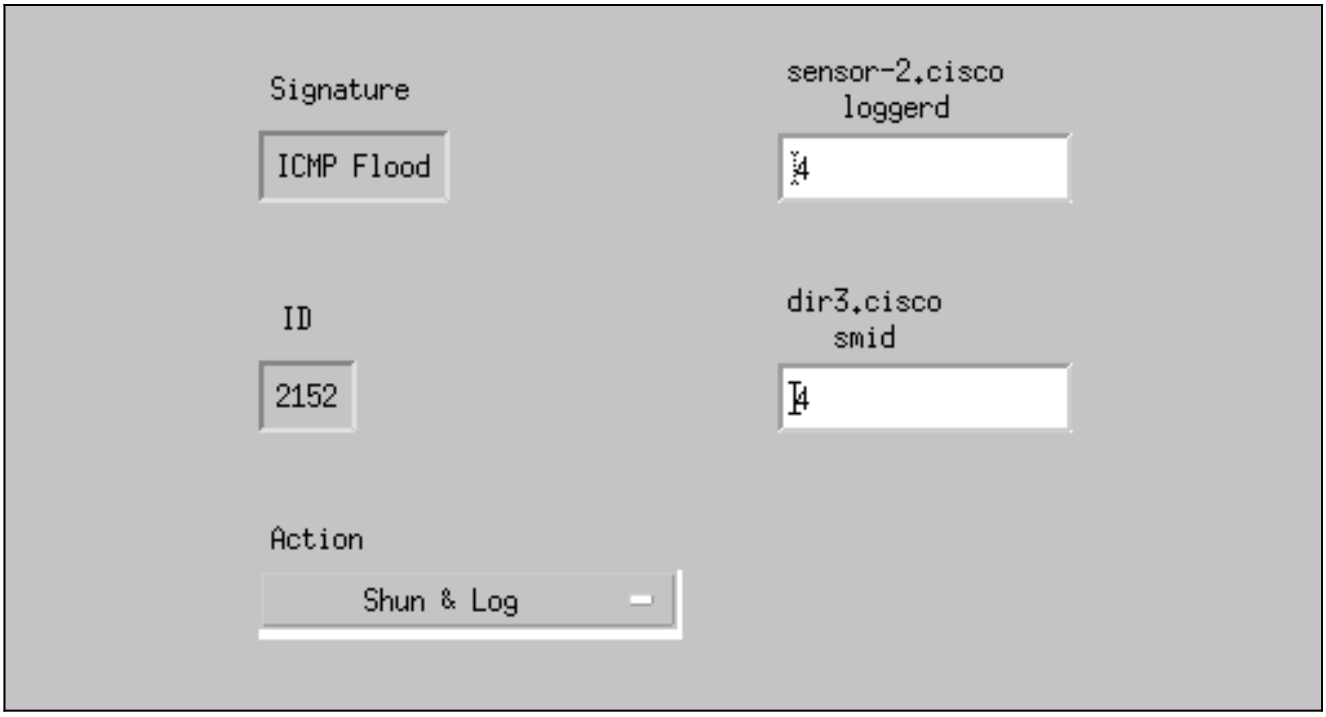


сеть.

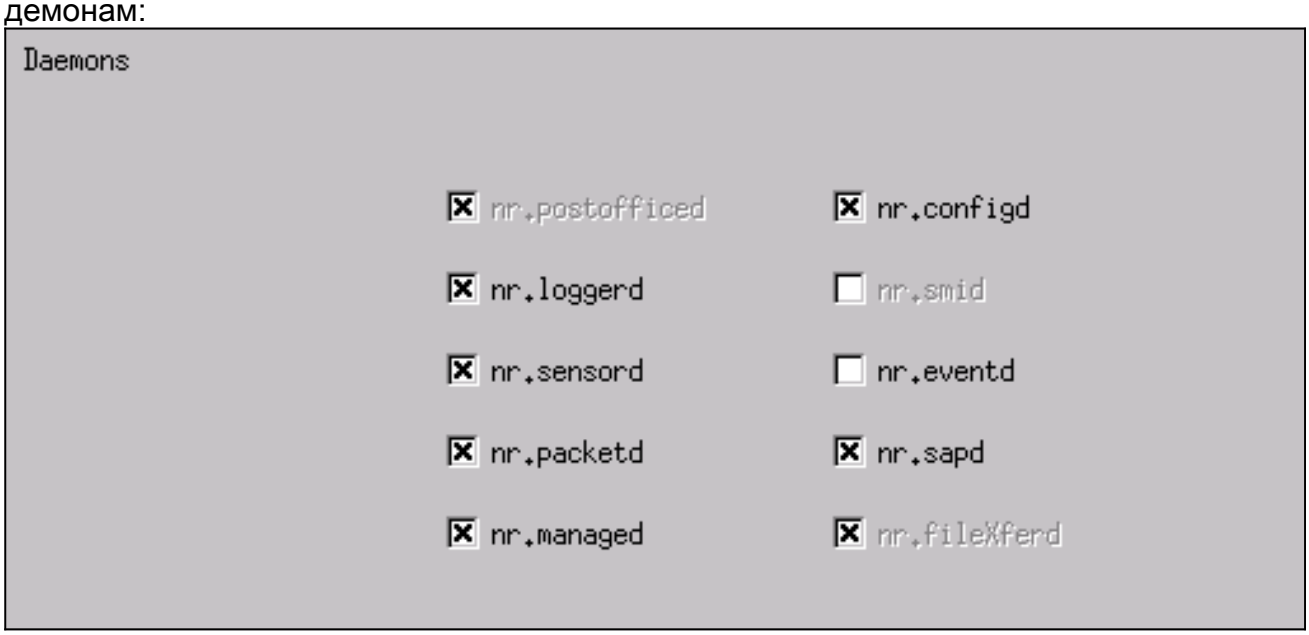
8. Нажмите **Profile** и выберите **Manual Configuration,> Modify Подписи**. Выберите **Large ICMP Traffic** и **ID: 2151**, нажмите **Modify** и измените Действие ни от Одного, чтобы **Избежать и Регистрировать**. **Нажмите OK, чтобы продолжить.**



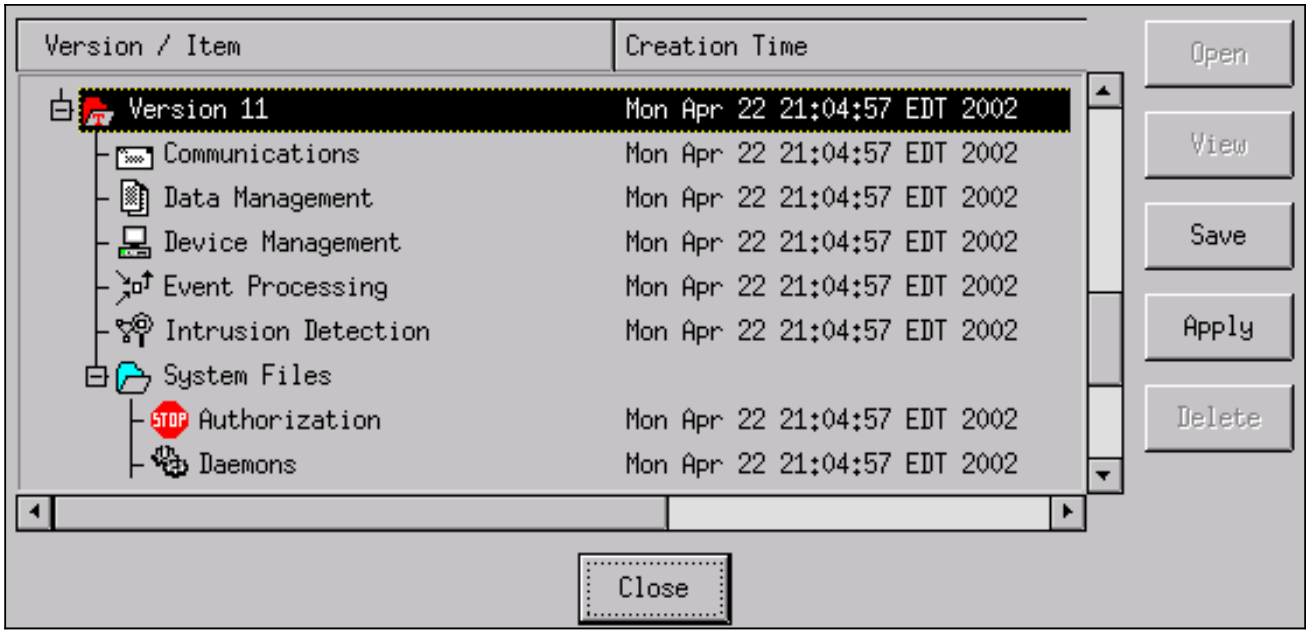
9. Выберите **ICMP Flood** и **ID: 2152**, нажмите **Modify** и измените Действие ни от **Одного**, чтобы **Избежать и Регистрировать**. **Нажмите OK, чтобы продолжить.**



10. Эта часть конфигурации завершена. Нажмите **OK** для закрытия окна Intrusion Detection.
11. Откройте папку **System Files** и откройте **окно Daemons**. Гарантируйте, что вы включили этим
демонам:



12. Нажмите **OK**, чтобы продолжить, и выбрать версию, которую вы просто модифицировали. Нажмите **Save> Apply**. Ждите системы, чтобы сказать вам, что Датчик закончен, Сервисы перезапуска, и закройте все окна для конфигурации Netranger.



Проверка

Этот раздел предоставляет сведения, который помогает вам подтверждать, что ваша конфигурация работает должным образом.

Прежде чем вы пойдете в наступление

```
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
```

Запустите блокирование атак

```
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
```

Пятнадцать минут спустя это возвращается к обычному, потому что избегание установлено в пятнадцать минут.

```
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
```

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- Окончание продаж для Cisco IDS Director
- Поддержка закончена для версии 3 Па для датчика Cisco IDS. x
- Поддержка продуктов системы предотвращения вторжений Cisco (IPS)
- Поддержка продуктов программного обеспечения Cisco PIX Firewall
- Справочники по командам для межсетевого экрана PIX Cisco Secure
- Cisco Systems – техническая поддержка и документация