Настройка TCP Reset при помощи IDS Director

Содержание

Введение

Этот документ описывает, как настроить Систему обнаружения проникновения (IDS, раньше NetRanger) Управляющий узел и Датчик для передачи сброса TCP на предпринятой Telnet к диапазону адресов, которые включают управляемый маршрутизатор, если передаваемая строка является "testattack".

Предварительные условия

Требования

При рассмотрении этой конфигурации не забудьте:

- Установите Датчик и проверьте, что он работает должным образом перед выполнением этой конфигурации.
- Гарантируйте, что интерфейс анализатора охватывает к внешнему интерфейсу управляемого маршрутизатора.

Используемые компоненты

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

- Cisco IDS Director 2.2.3
- Датчик Cisco IDS 3.0.5
- Выпуск ПО выполнения маршрутизатора Cisco IOS® 12.2.6

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.

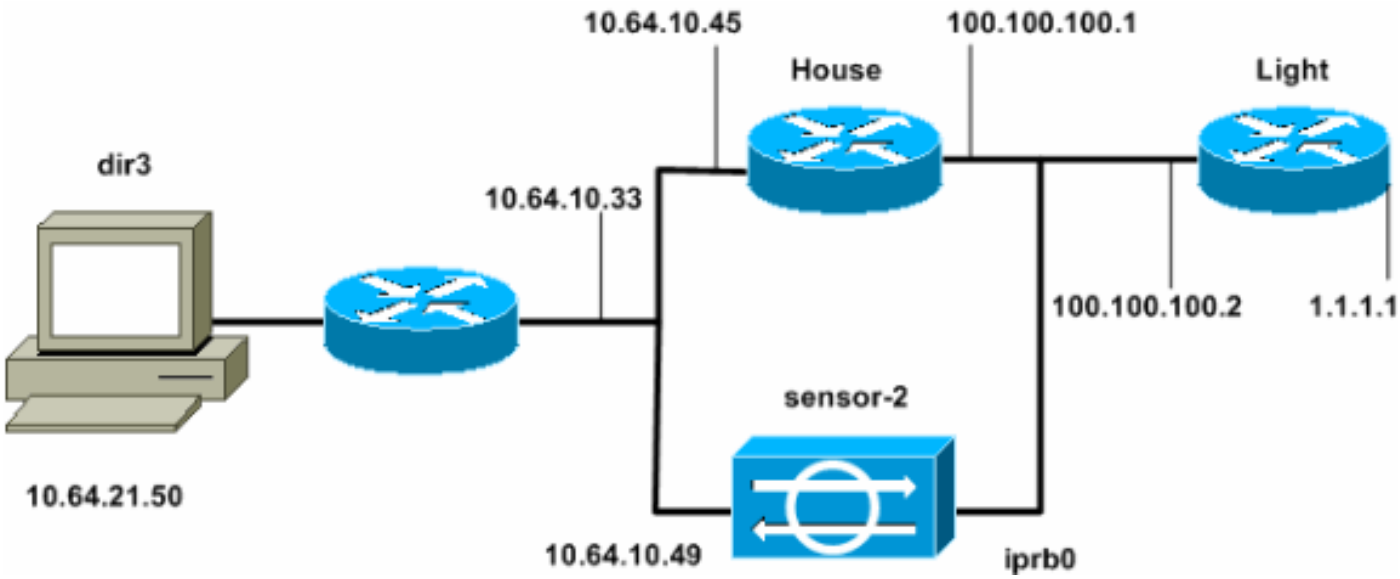
Настройка

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

Примечание: Поиск дополнительной информации о командах в данном документе можно выполнить с помощью средства "Command Lookup" (Поиск команд) (только для зарегистрированных клиентов).

Схема сети

В этом документе используются настройки сети, показанные на данной диаграмме.



Конфигурации

Эти конфигурации используются в данном документе.

- Маршрутизатор light
- Маршрутизатор house

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
```

Маршрутизатор house

```
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#
```

Настройка датчика

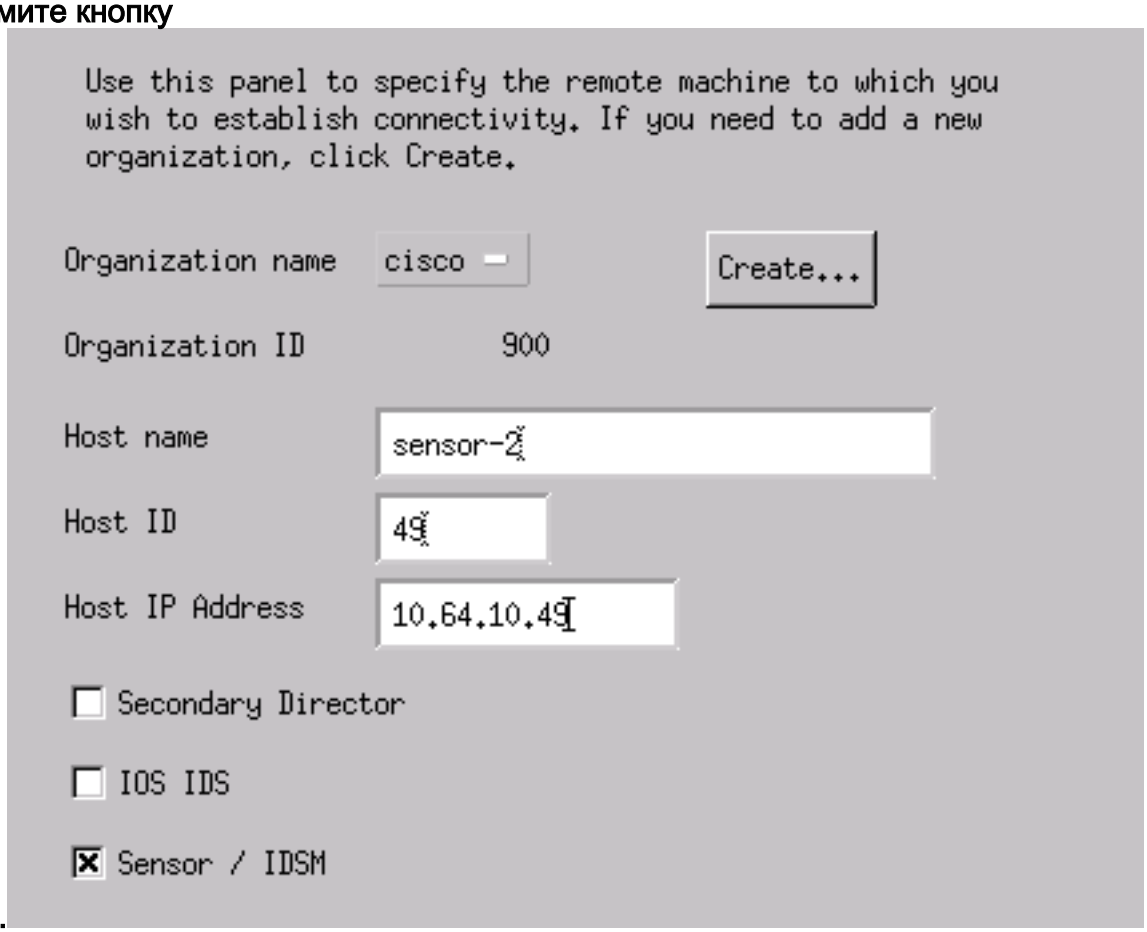
Выполните эти шаги для настройки Датчика.

1. Telnet к 10.64.10.49 (сенсор IDS) с **пользователем root** и **атакой пароля**.
2. Введите **sysconfig-sensor**.
3. Когда предложено, введите сведения о конфигурации, как показано в данном примере:`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. Когда предложено, сохраните конфигурацию и позвольте Датчик перезагрузке.

Добавьте датчик в управляющий узел

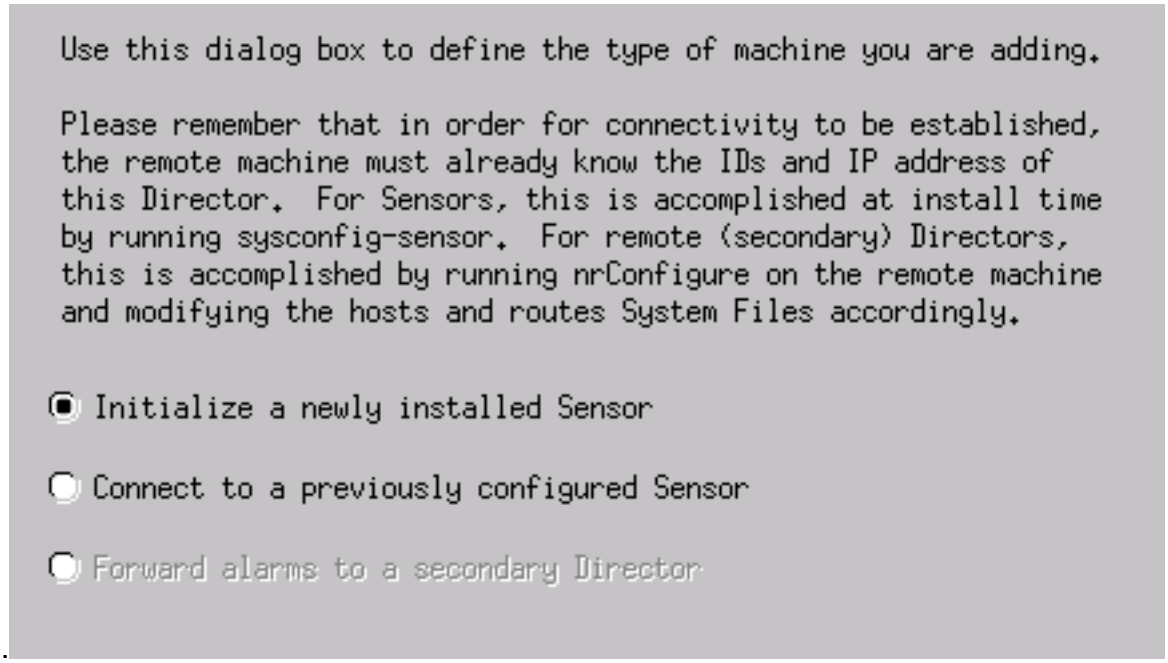
Выполните эти шаги для добавления Датчика в Управляющий узел.

1. Telnet к 10.64.21.50 (IDS Director) с **netrangr** имени пользователя и **атакой пароля**.
2. Введите **ovw&** для запуска HP OpenView.
3. Из Главного меню перейдите **к Security> Configure**.
4. В Утилите Управления файлами конфигурации перейдите **к File> Add Host** и нажмите **Next**.
5. Завершите сведения о главном хосте Датчика, как показано в данном примере. **Нажмите кнопку**



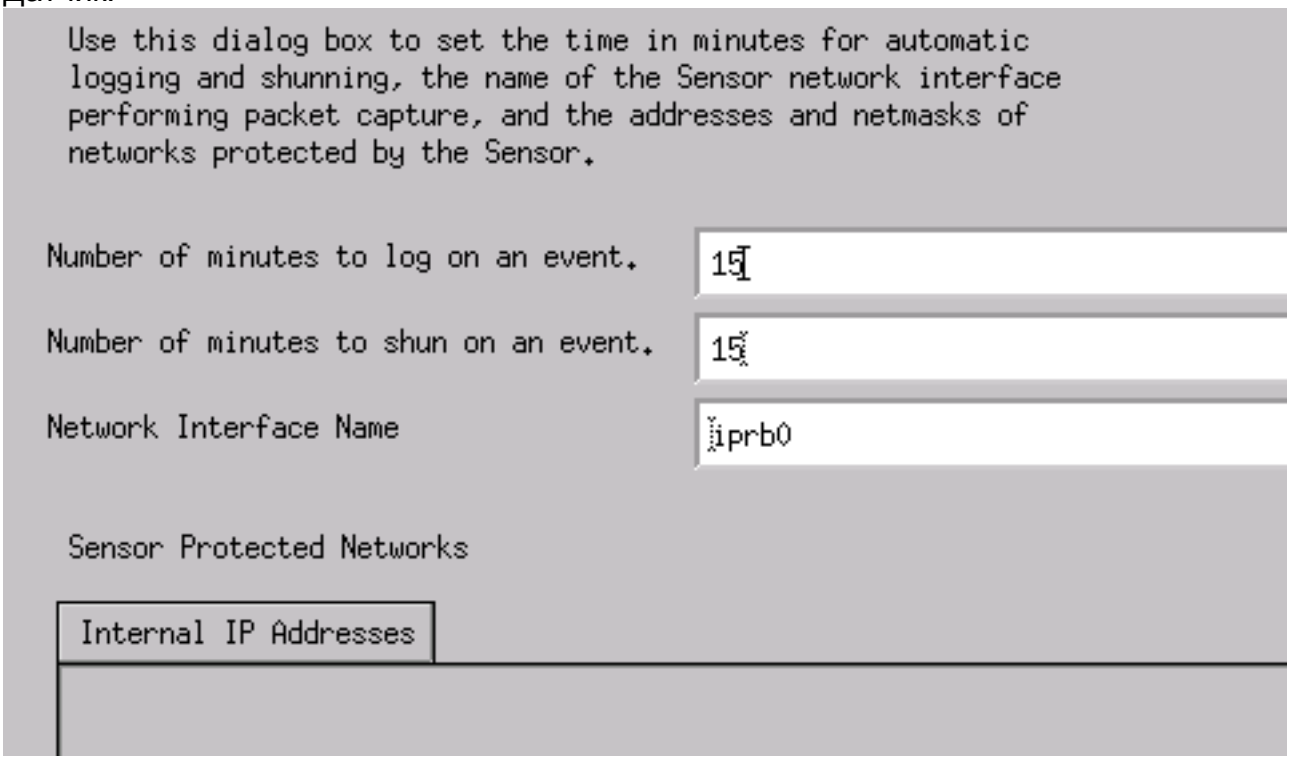
Next.

6. Примите настройки по умолчанию для типа машины и **нажмите Next**, как показано в данном

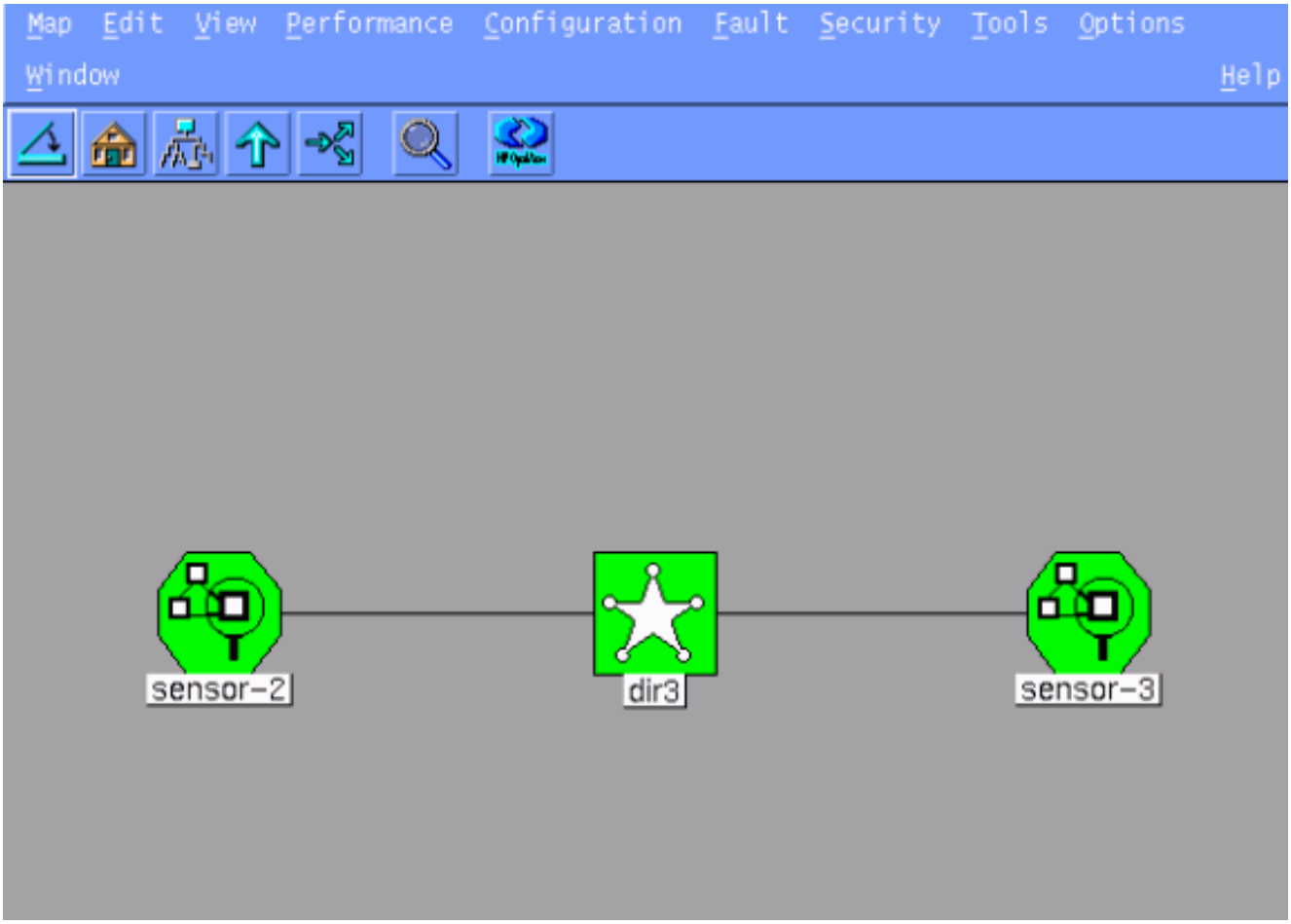


примере.

7. Можно или изменить журнал и избежать минут, или можно принять значения по умолчанию. Однако необходимо изменить Имя сетевого интерфейса на название интерфейса анализатора. В данном примере это - "iprb0". Это может быть "spwr0" или что-либо еще в зависимости от Типа датчика и как вы подключаете свой Датчик.



8. Продолжите нажимать **Next** и затем нажимать **Finish** для добавления Датчика в Управляющий узел. Из главного меню необходимо теперь видеть sensor-2, как в данном
примере.

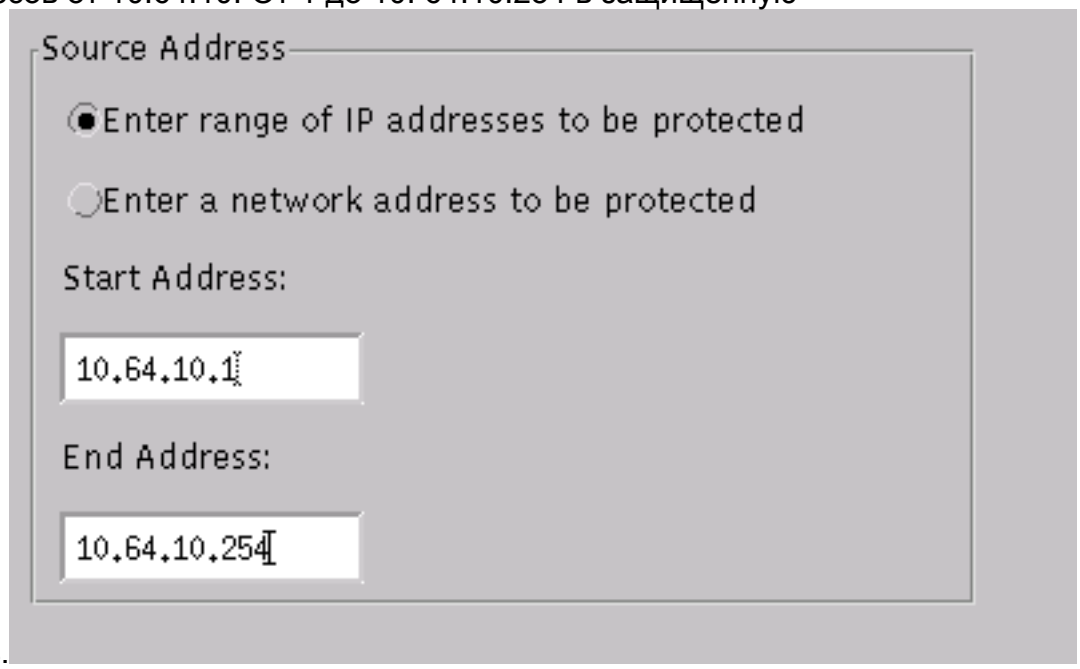


Настройте сброс TCP для маршрутизатора Cisco IOS

Выполните эти шаги для настройки сброса TCP для маршрутизатора Cisco IOS.

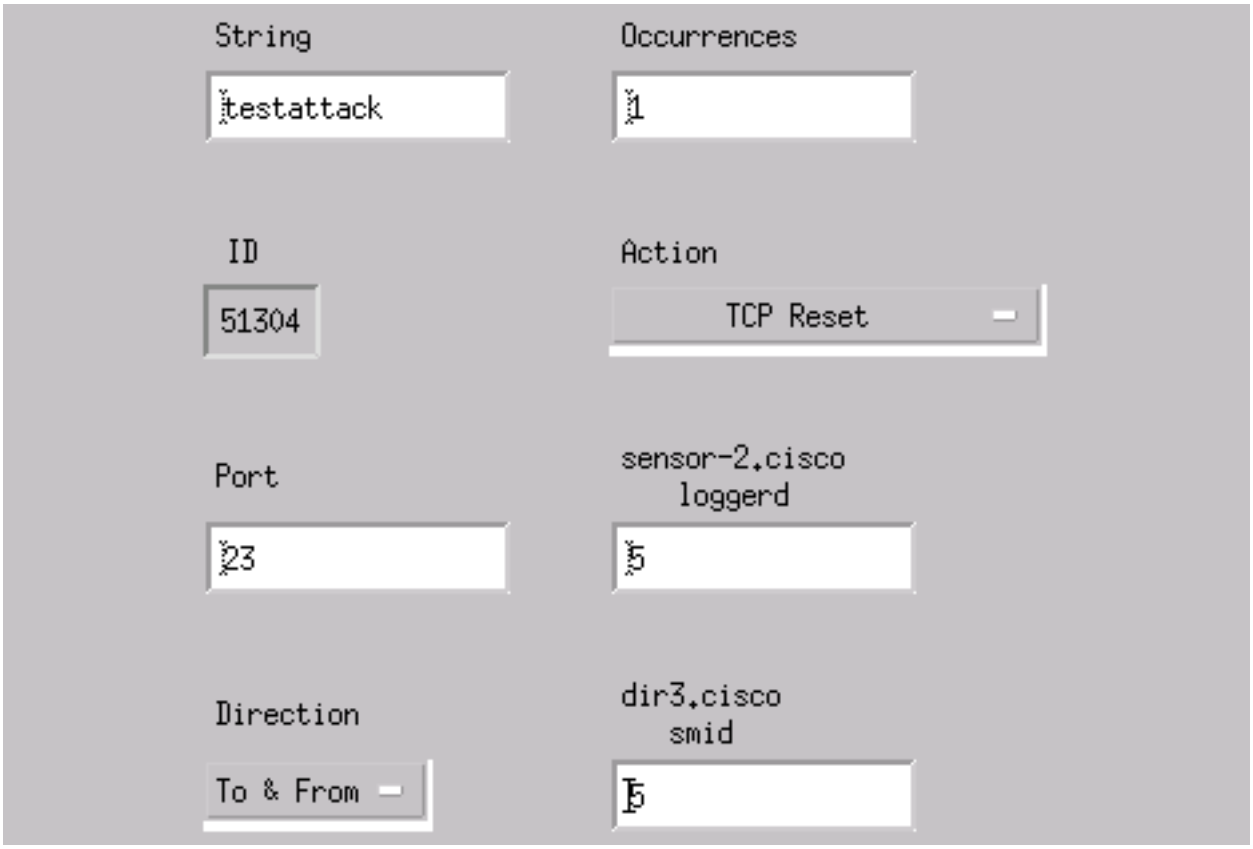
1. В Главном меню перейдите **к Security> Configure**.
2. В Утилите Управления файлами конфигурации выделите **sensor-2** и дважды нажмите его.
3. Открытое управление устройствами.
4. Нажмите **Devices> Add**. Введите сведения об устройстве, как показано в следующем примере. **Для продолжения нажмите кнопку OK**. И Telnet и enable password является Cisco.

5. Откройте окно Intrusion Detection и нажмите **Protected Networks**. Добавьте диапазон адресов от 10.64.10. От 1 до 10. 64.10.254 в защищенную

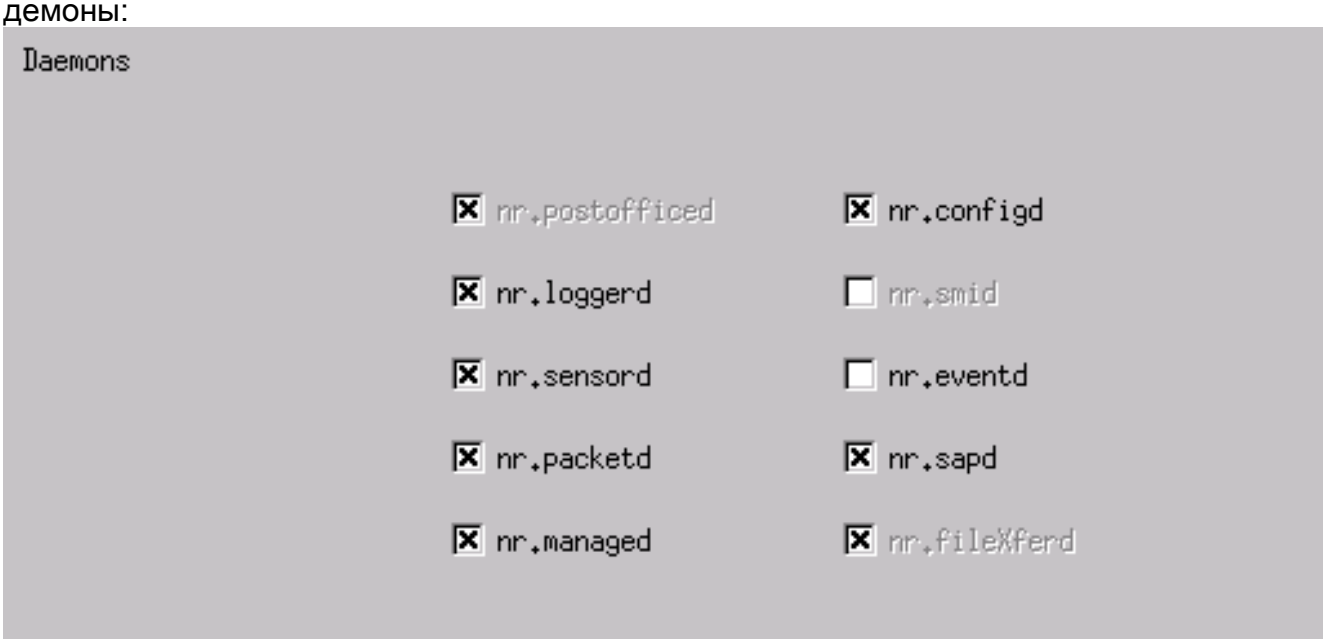


сеть.

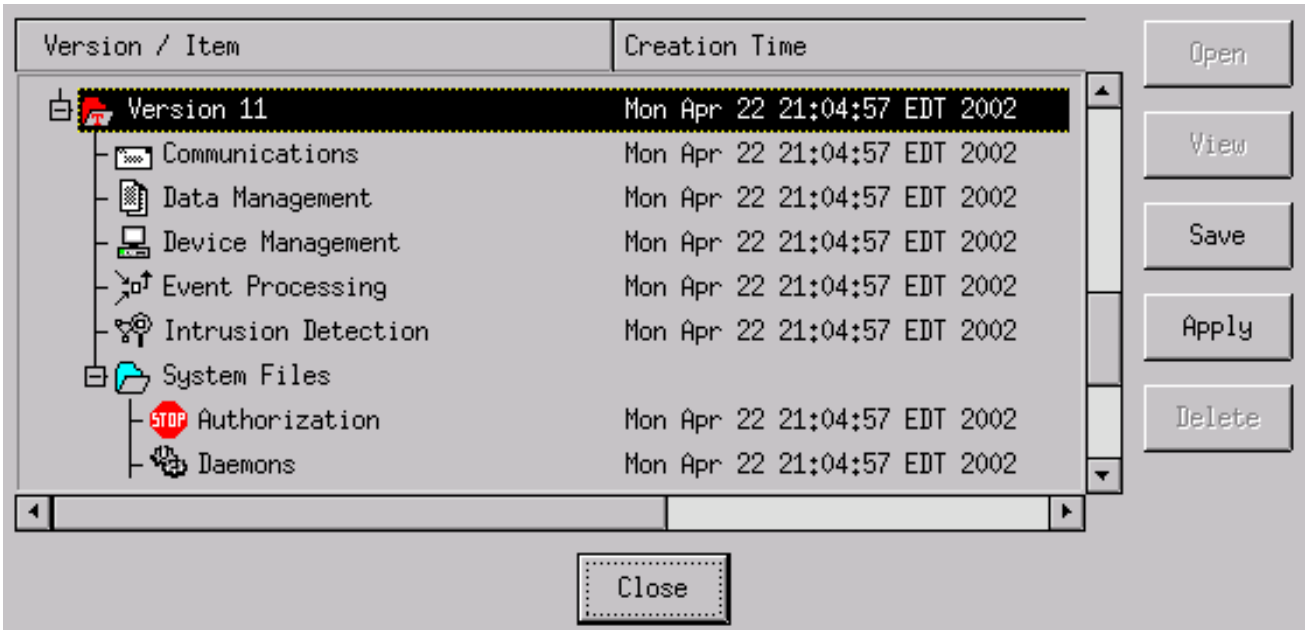
6. Нажмите **Profile** и выберите **Manual Configuration**. Затем, нажмите **Modify Signatures**. Выберите **Matched Strings** с ID 8000. Нажмите **Expand> Add** для добавления новой строки, названной **testattack**. Введите информацию о строке, как показано в данном примере, и нажмите **OK** для продолжения.



7. Вы закончили эту часть конфигурации. Нажмите **OK** для закрытия окна Intrusion Detection.
8. Откройте папку System Files, тогда окно Daemons. Удостоверьтесь, что вам включили эти
   демоны:



9. **Для продолжения нажмите кнопку OK.**
10. Выберите версию, которую вы просто модифицировали, нажмите **Save** и затем **Применитесь**. Ждите системы, чтобы сказать вам, что Датчик закончил перезапускать сервисы, затем закрывает все окна для Настройки устройства управления.



Выполните атаку и сброс TCP

Telnet от Маршрутизатора Light до House маршрутизатора и **testattack** типа. Как только вы поражаете Пространство или Клавишу Enter, ваш сброс сеанса Telnet. Вы соединитесь с House маршрутизатора.

```
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.
```

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Telnet к 10.64.10.49, Датчик, с помощью **пользователя root** и **атаки пароля**. Введите **CD/usr/nr/etc**. Введите **кошку packetd.conf**. При корректной установке сброса TCP для testattack необходимо видеть четыре (4) в поле Action Codes. Это указывает на сброс TCP как показано в данном примере.

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

При случайной установке действия ни в "один" в подписи вы будете видеть нуль (0) в поле Action Codes. Это не указывает ни на какое действие, как замечено в данном примере.

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

Сброс TCP передается от интерфейса анализатора Датчика. Если существует коммутатор, подключающий интерфейс Датчика с внешним интерфейсом управляемого маршрутизатора при настройке использования **команды set span** в коммутаторе используйте этот синтаксис:

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

Дополнительные сведения

- Сообщения о дефектах
- Страница технической поддержки предотвращения вторжений Cisco Secure
- Cisco Systems – техническая поддержка и документация