Настройка сбора IDS TCP с помощью VMS IDS MC

Содержание

Введение

Документ предоставляет пример конфигурации Cisco Intrusion Detection System (IDS) через VPN/Security Management Solution (VMS), Консоль управления IDS (MC IDS). В этом случае Сброс TCP от сенсора IDS до маршрутизатора Cisco настроен.

Предварительные условия

Требования

Убедитесь, что вы обеспечили выполнение следующих требований, прежде чем попробовать эту конфигурацию:

- Датчик установлен и настроен для считывания необходимого трафика.
- Интерфейс анализатора охвачен к внешнему интерфейсу маршрутизатора.

Используемые компоненты

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

- VMS 2.2 с MC IDS и монитором безопасности 1.2.3
- Датчик Cisco IDS 4.1.3S (63)
- Маршрутизатор Cisco, который выполняет Выпуск 12.3.5 программного обеспечения Cisco IOS

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 Условные обозначения технических терминов Cisco.

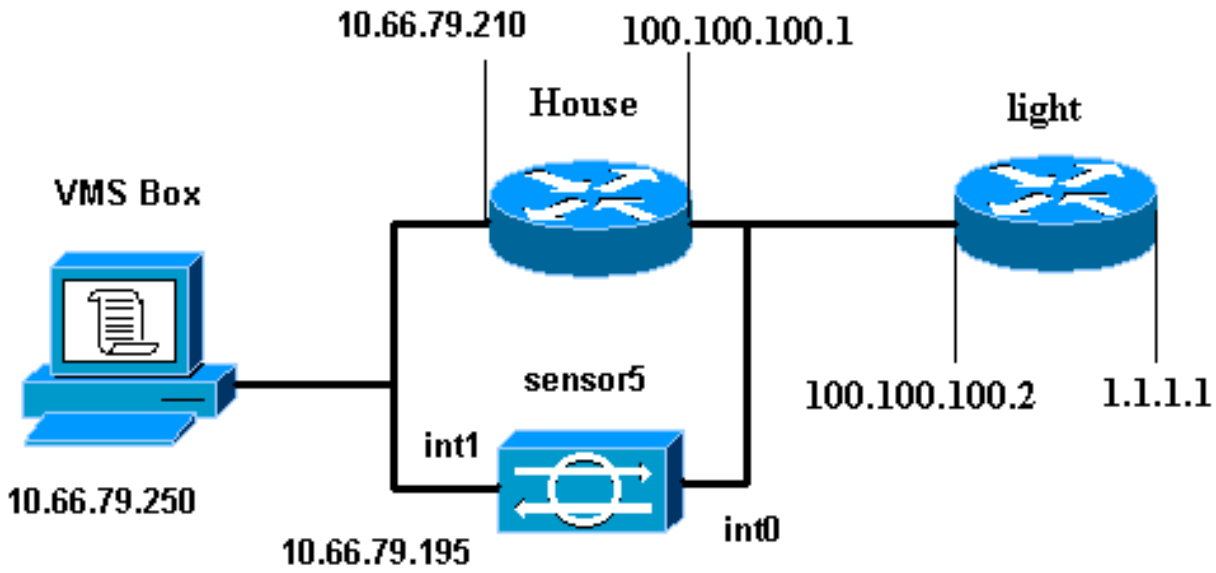
Настройка

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

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Схема сети

В настоящем документе используется следующая схема сети:



Конфигурации

Эти конфигурации используются в данном документе.

- Маршрутизатор light
- Маршрутизатор house

Маршрутизатор light

```
Current configuration : 906 bytes
!
version 12.3
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

```
Building configuration...

Current configuration : 797 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname House ! logging queue-limit 100 enable password
cisco ! ip subnet-zero no ip domain lookup ! ! interface
Ethernet0 ip address 10.66.79.210 255.255.255.224 hold-
queue 100 out ! interface Ethernet1 ip address
100.100.100.1 255.255.255.0 ip classless ip route
0.0.0.0 0.0.0.0 10.66.79.193 ip route 1.1.1.0
255.255.255.0 100.100.100.2 ip http server no ip http
secure-server ! ! ! line con 0 stopbits 1 line vty 0 4
password cisco login ! scheduler max-task-time 5000 end
```

Начальная конфигурация сенсора

Примечание: Если вы уже выполнили начальную настройку своего Датчика, продолжитесь к Импорту Датчик в раздел MC IDS.

1. Консоль в датчик.Будет предложено ввести имя пользователя и пароль. Если это первоначально, вы подключаетесь с консоли в Датчик, необходимо войти с **именем пользователя cisco** и **паролем cisco**.
2. Вам предлагают изменить пароль и перепечатать новый пароль для подтверждения.
3. Введите **настройку** и введите соответствующую информацию в каждое приглашение

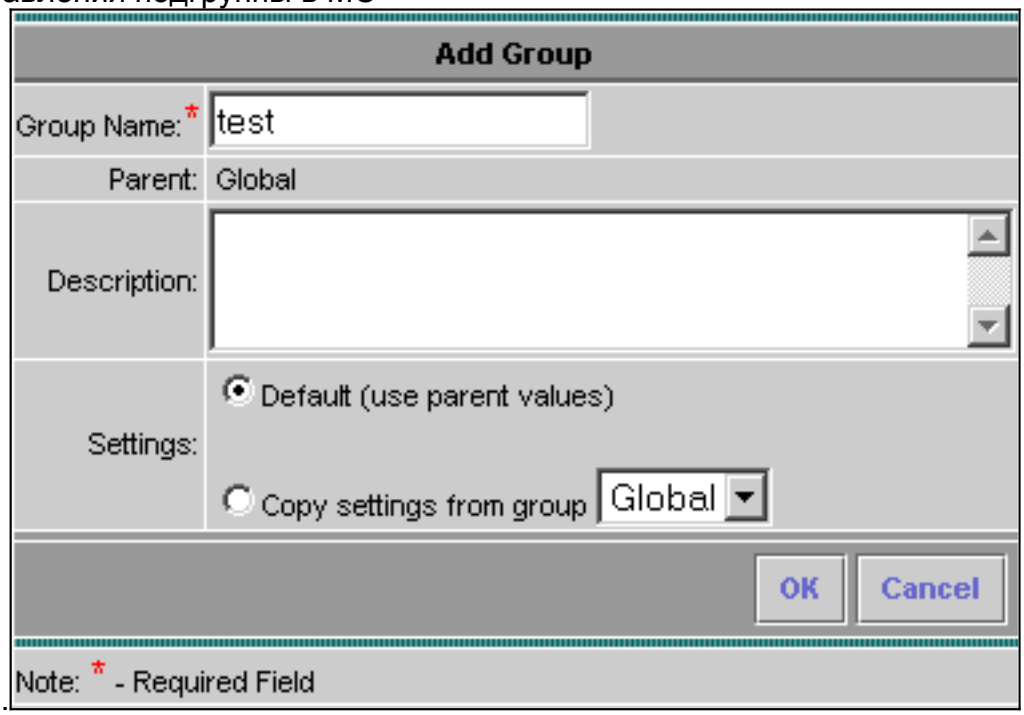
для устанавливания основных параметров для Датчика согласно данному примеру:

```
sensor5#setup --- System Configuration Dialog --- At any point you may enter a
question mark '?' for help. User ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'. Current Configuration: networkParams
ipAddress 10.66.79.195 netmask 255.255.255.224 defaultGateway 10.66.79.193 hostname sensor5
telnetOption enabled accessList ipAddress 10.66.79.0 netmask 255.255.255.0 exit timeParams
summerTimeParams active-selection none exit exit service webServer general ports 443 exit
exit 5 Save the config: (It might take a few minutes for the sensor saving the
configuration) [0] Go to the command prompt without saving this config. [1] Return back to
the setup without saving this config. [2] Save this configuration and exit setup. Enter
your selection[2]: 2
```

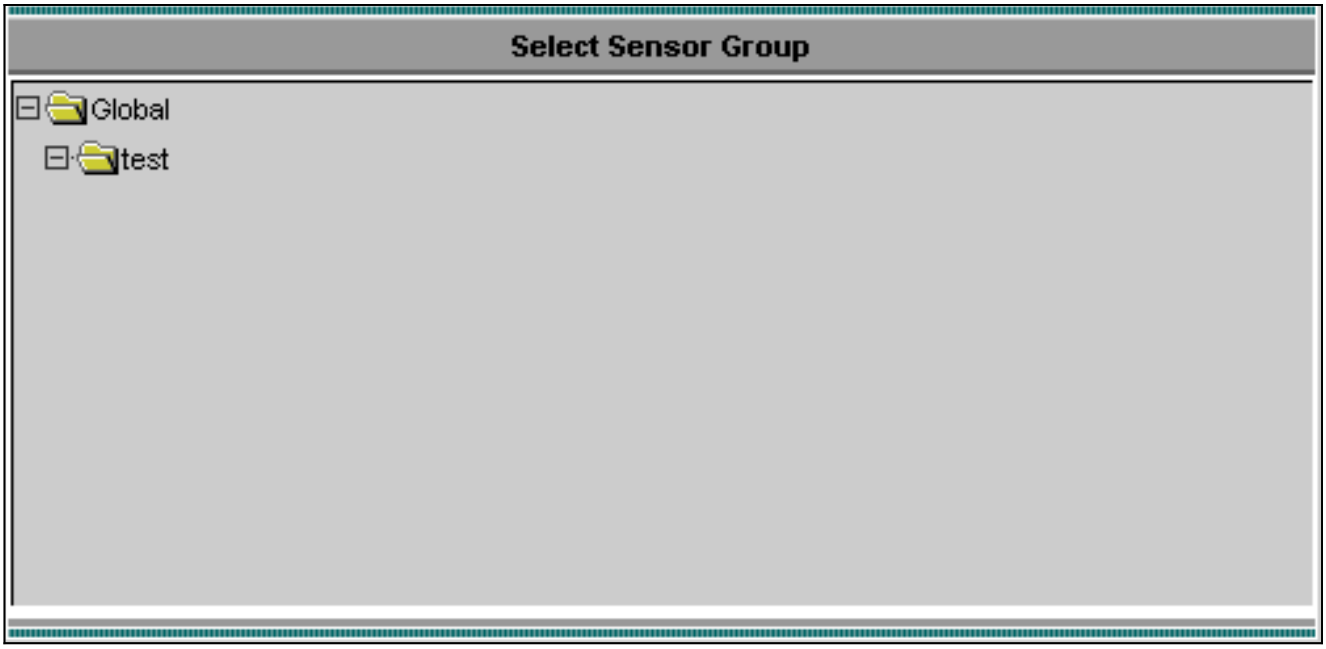
Импортируйте датчик в MC IDS

Выполните эти шаги для импорта Датчика в MC IDS.

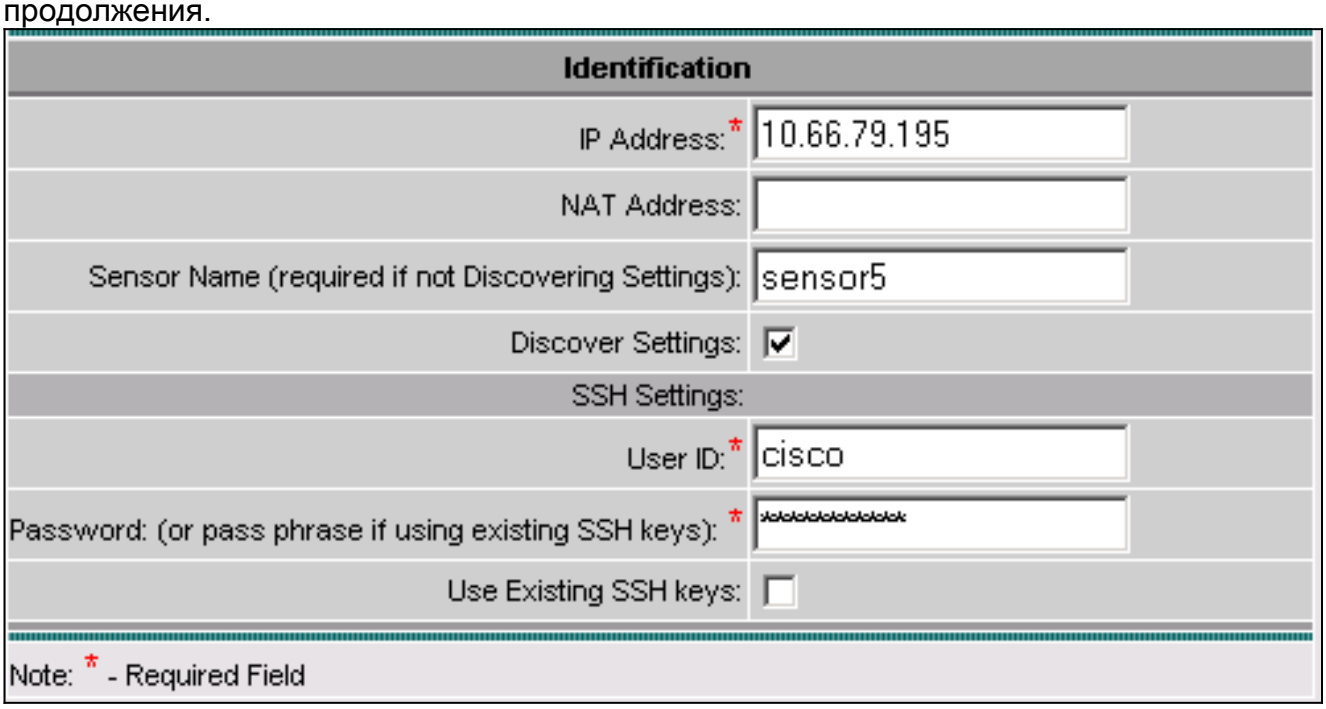
1. Перейдите к своему Датчику. В этом случае, или **http://10.66.79.250:1741** или **https://10.66.79.250:1742**.
2. Вход в систему с соответствующим именем пользователя и паролем.В данном примере имя пользователя является **admin**, и пароль является **Cisco**.
3. Выберите **VPN/Security Management Solution> Management Center** и нажмите **IDS Sensors**.
4. Нажмите вкладку Devices и выберите **Sensor Group**.
5. Выделите **Глобальный** и нажмите **Create Subgroup**.
6. Введите Имя группы и гарантируйте, что **По умолчанию** выбран, затем нажмите **OK** для добавления подгруппы в MC IDS.



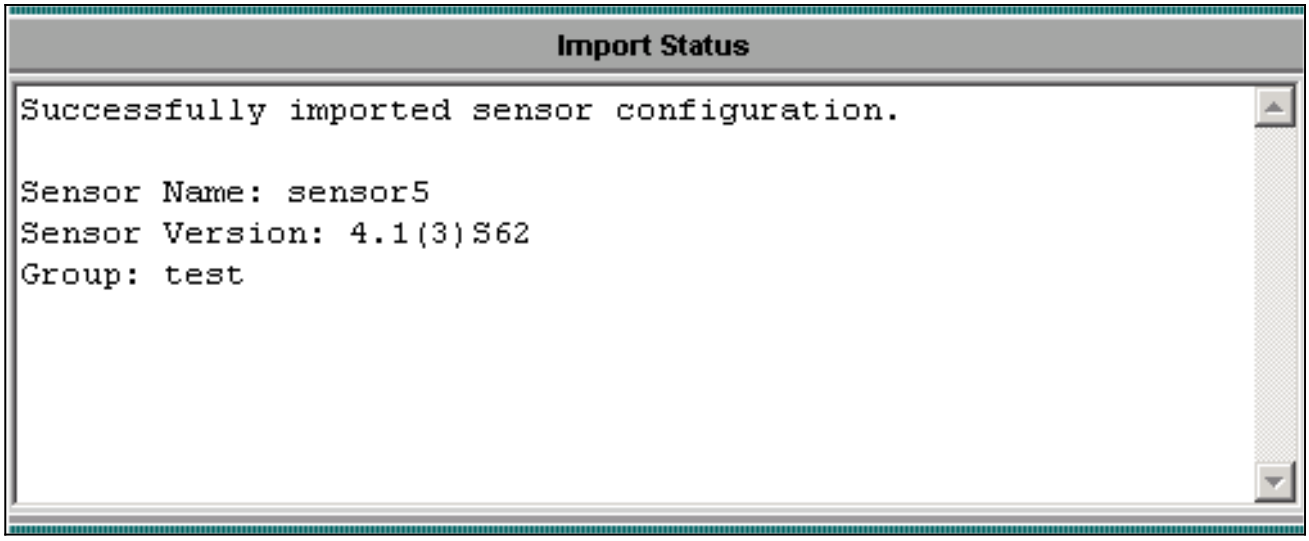
7. Выберите **Devices> Sensor**, выделите подгруппу, созданную в предыдущем шаге (в этом случае, **тест**), и **нажмите Add**.
8. Выделите подгруппу и нажмите **Next**.



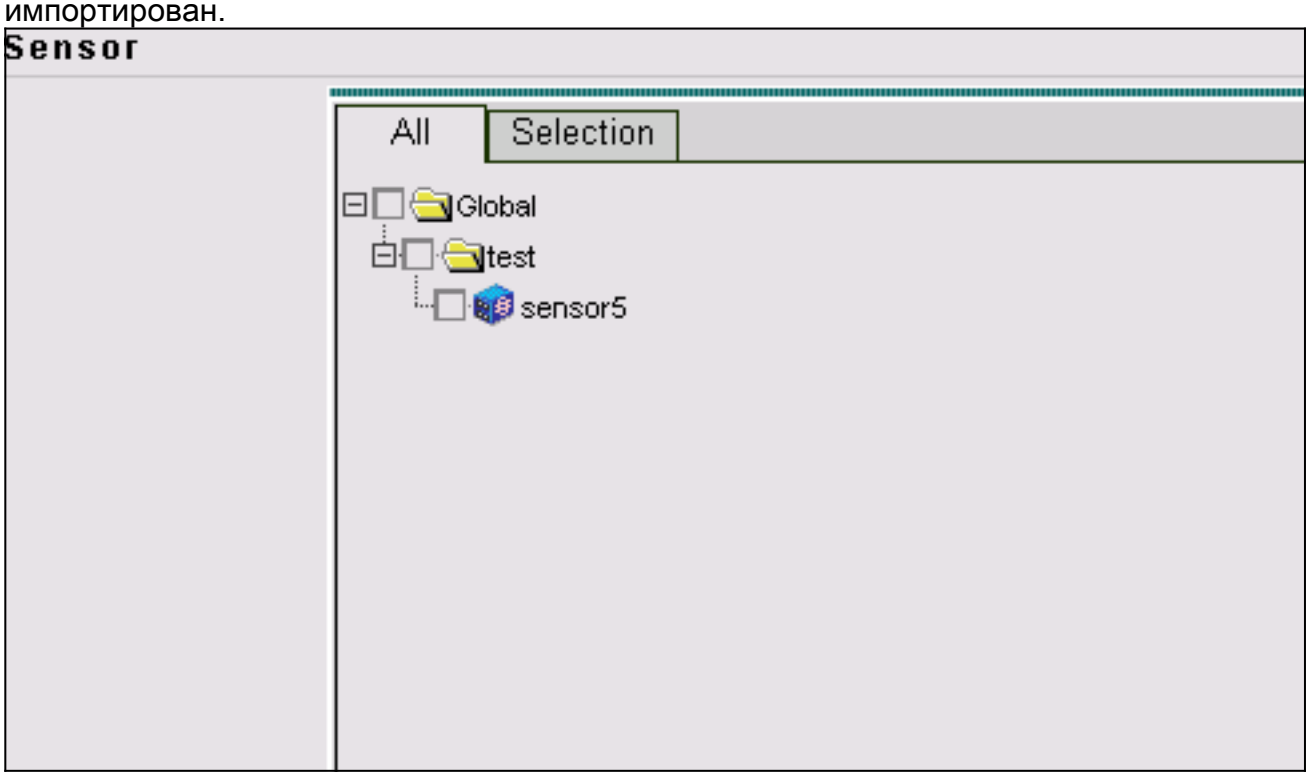
9. Введите подробные данные согласно данному примеру и нажмите **Next** для продолжения.



10. Когда вам предоставляют сообщение, которое сообщает `Successfully imported sensor configuration`, нажмите **Finish** для продолжения.



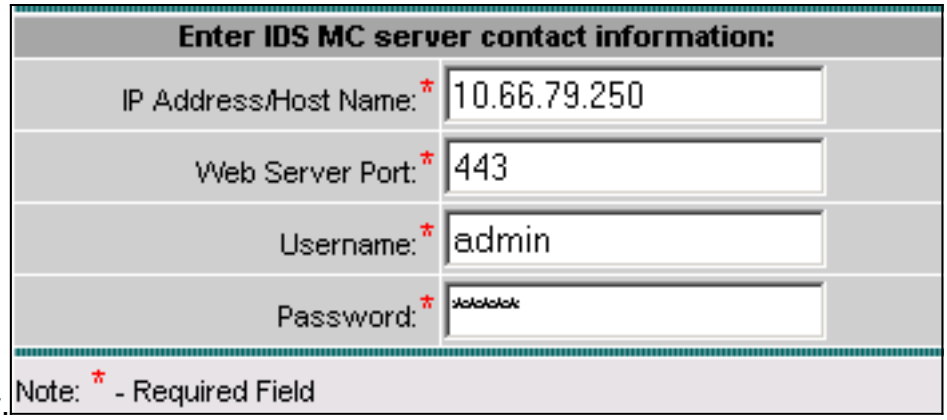
11. Ваш Датчик импортирован в MC IDS. В этом случае Sensor5 импортирован.



Импортируйте датчик в монитор безопасности

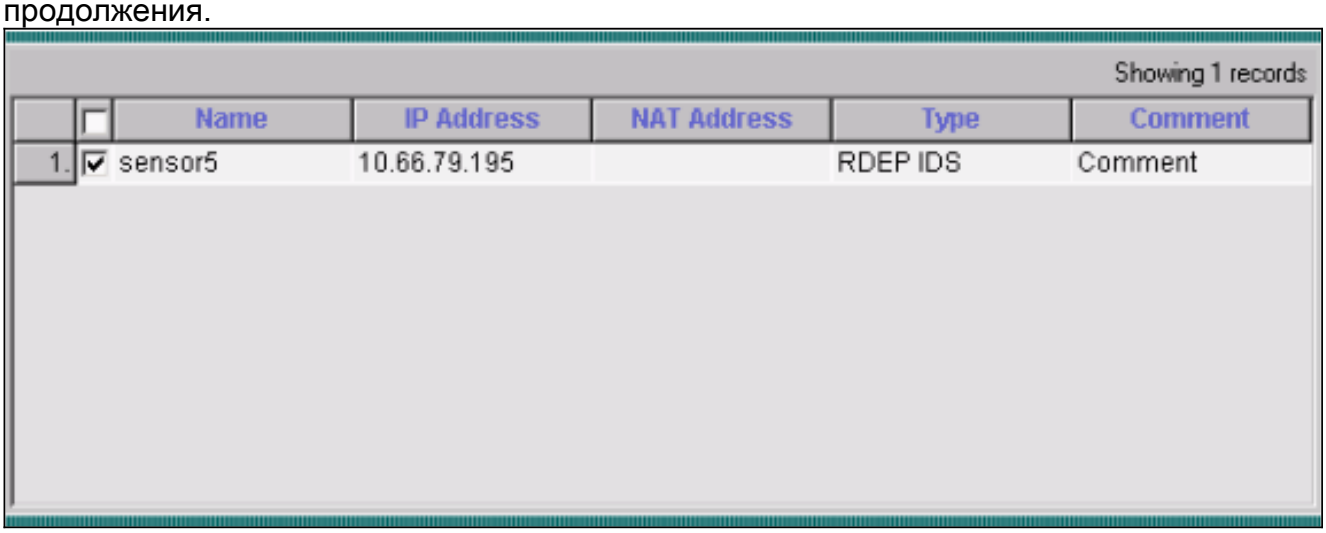
Выполните эти шаги для импорта Датчика в Монитор Безопасности.

1. В Меню сервера VMS выберите **VPN/Security Management Solution>> Security Monitoring Center Монитор**.
2. Выберите вкладку Devices, затем нажмите **Import** и введите Информацию сервера MC IDS согласно данному

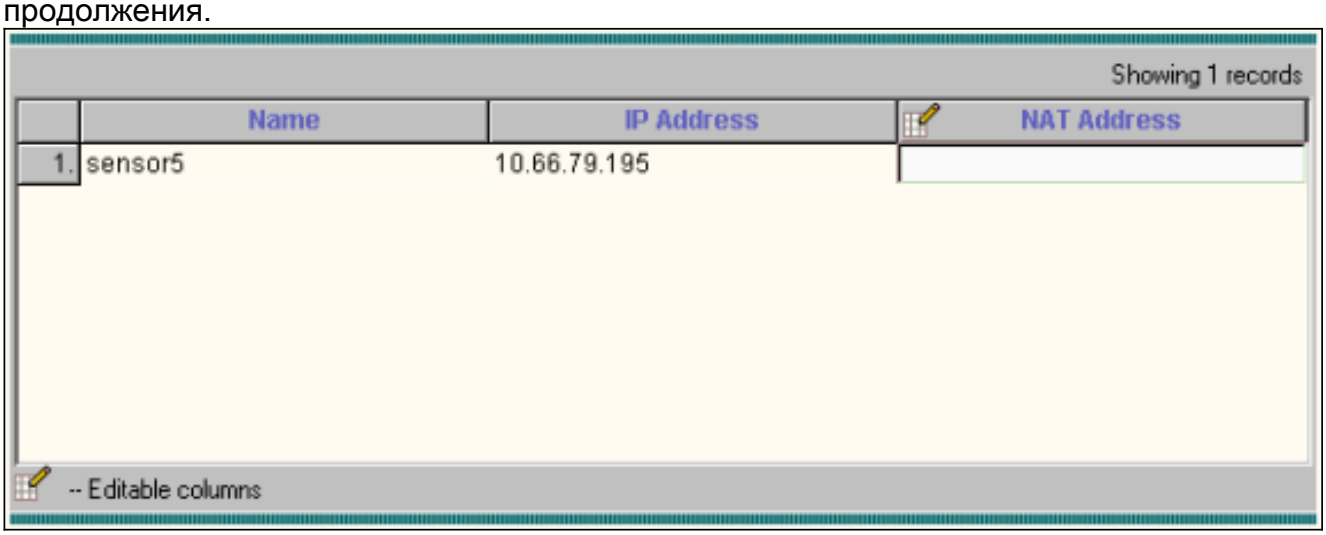


примеру.

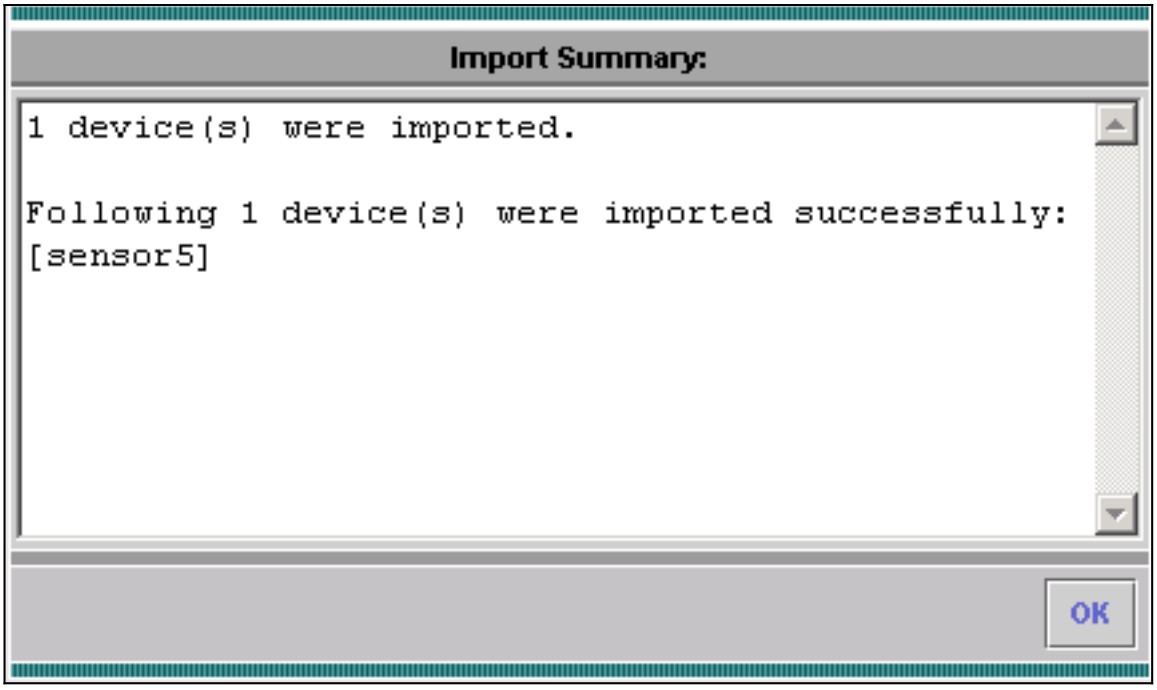
3. Выберите свой Датчик (в этом случае, **sensor5**) и нажмите **Next** для продолжения.



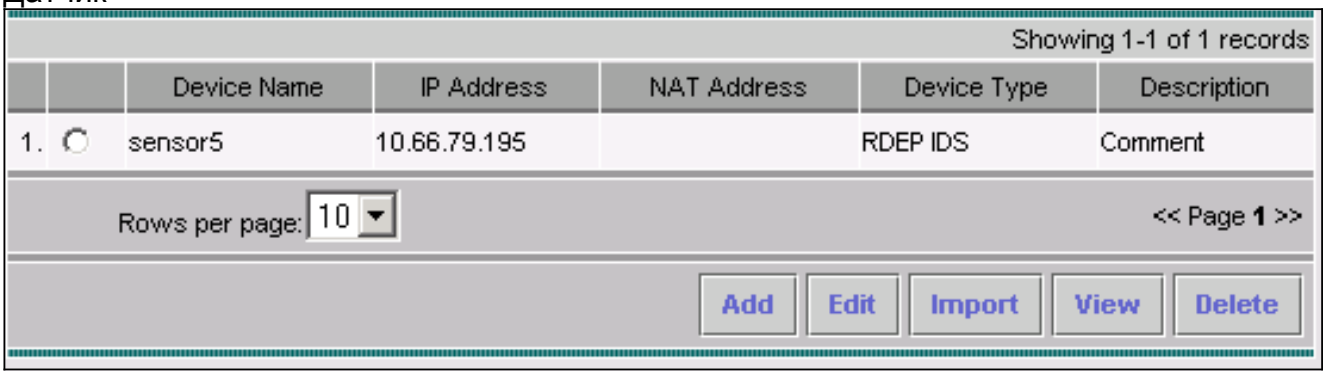
4. В случае необходимости обновите адрес NAT для своего Датчика, затем нажмите **Finish** для продолжения.



5. Нажмите **OK**, чтобы закончить импортировать Датчик из MC IDS в Монитор Безопасности.



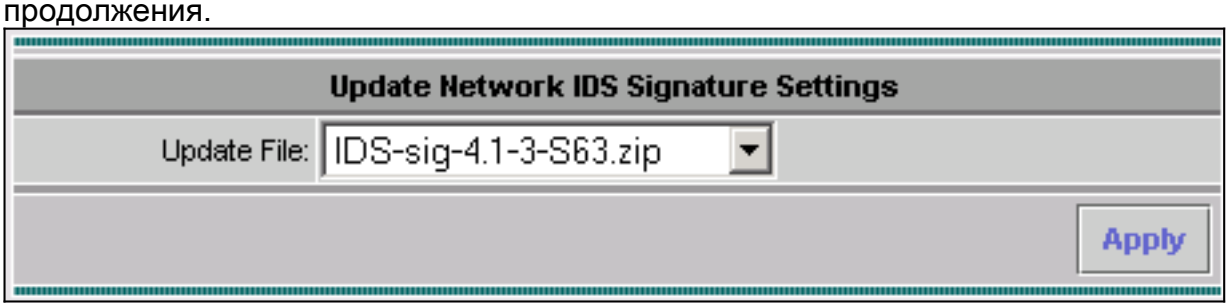
6. Можно теперь видеть, что успешно импортирован Датчик



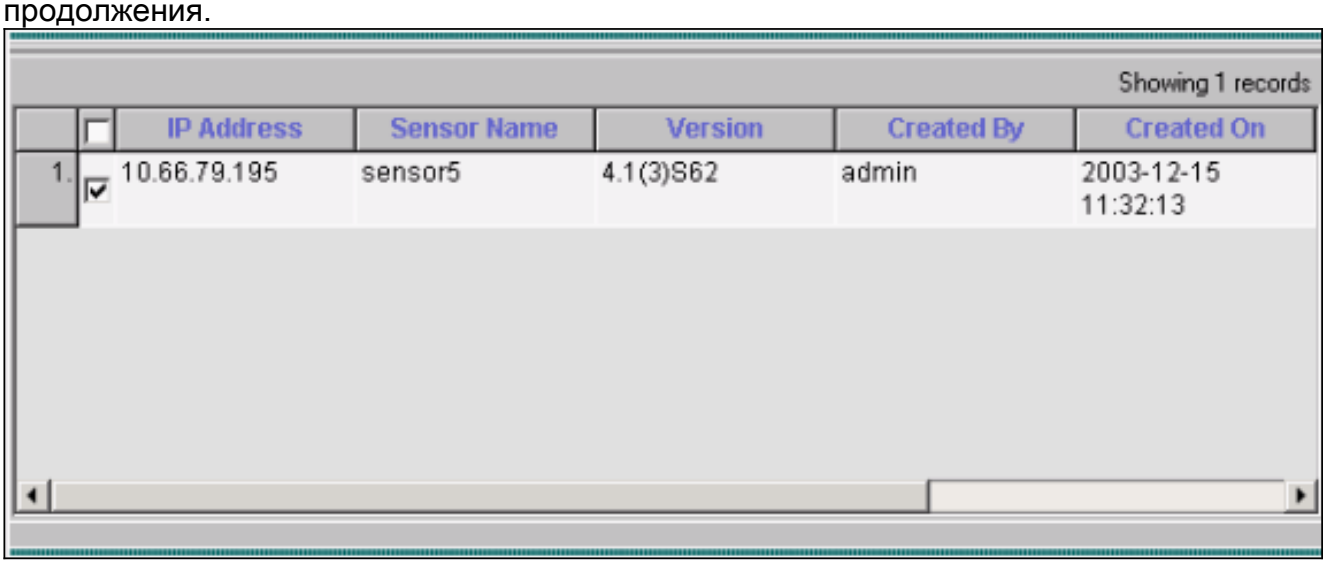
Используйте MC IDS для обновлений подписи

Эта процедура объясняет, как использовать MC IDS для обновлений подписи.

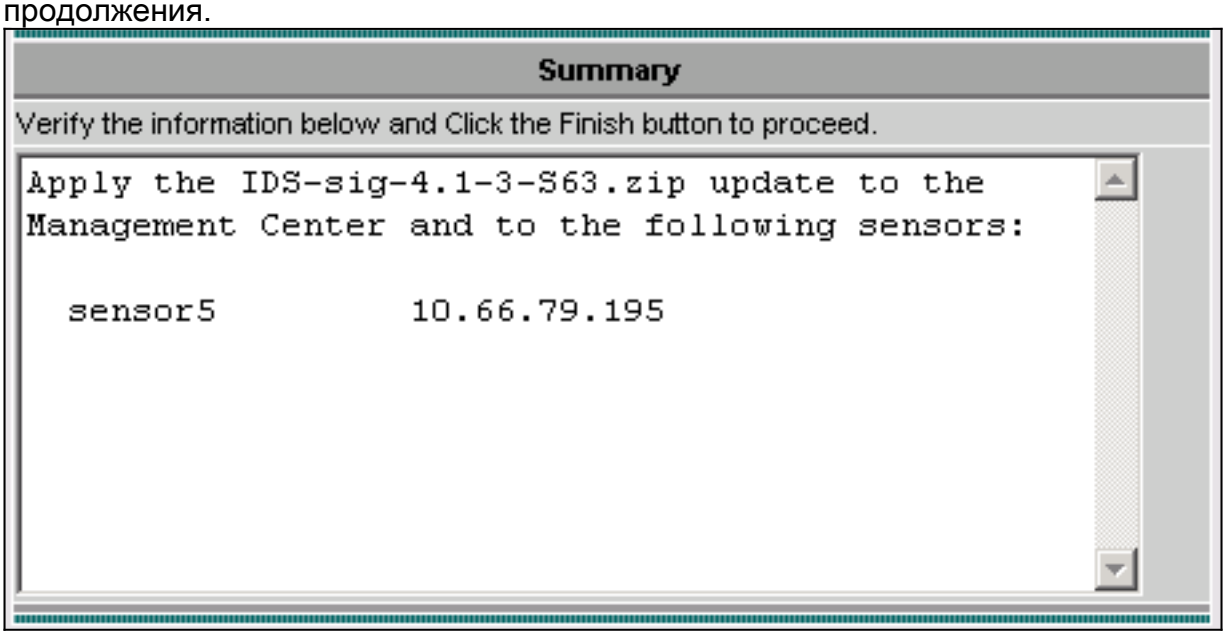
1. Загрузите Обновления подписи Обнаружения несанкционированного доступа к сети (только зарегистрированные клиенты) и сохраните их в каталоге **C:\PROGRA~1\CSCOpx\MDC\etc\ids\updates**на вашем Сервере VMS.
2. В консоли сервера VMS выберите **VPN/Security Management Solution> Management Center> IDS Sensors**.
3. Выберите Вкладку конфигурация и нажмите **Updates**.
4. Нажмите **Update Network IDS Signatures**.
5. Выберите подпись, которую вы хотите обновить от раскрывающегося меню и нажать **Apply** для продолжения.



6. Выберите Sensor, чтобы обновить и нажать **Next** для продолжения.



7. После того, как вам предлагают применить обновление Центра управления, а также Датчик, нажмите **Finish** для продолжения.



8. Telnet или консоль в интерфейс командной строки Датчика. Вы видите информацию, подобную этому:`sensor5#`
`Broadcast message from root (Mon Dec 15 11:42:05 2003):`
`Applying update` **`IDS-sig-4.1-3-S63. This may take several minutes.`** `Please do not reboot the sensor during this update. Broadcast message from root (Mon Dec 15 11:42:34 2003):` **`Update complete. sensorApp is restarting This may take several minutes.`**
9. Ждите в течение нескольких минут, чтобы позволить обновлению завершать, затем вводить **show version** для проверки.`sensor5#`**`show version`** `Application Partition:` **`Cisco Systems Intrusion Detection Sensor, Version 4.1(3)S63 Upgrade History: * IDS-sig-4.1-3-S62 07:03:04 UTC Thu Dec 04 2003 IDS-sig-4.1-3-S63.rpm.pkg 11:42:01 UTC Mon Dec 15 2003`**

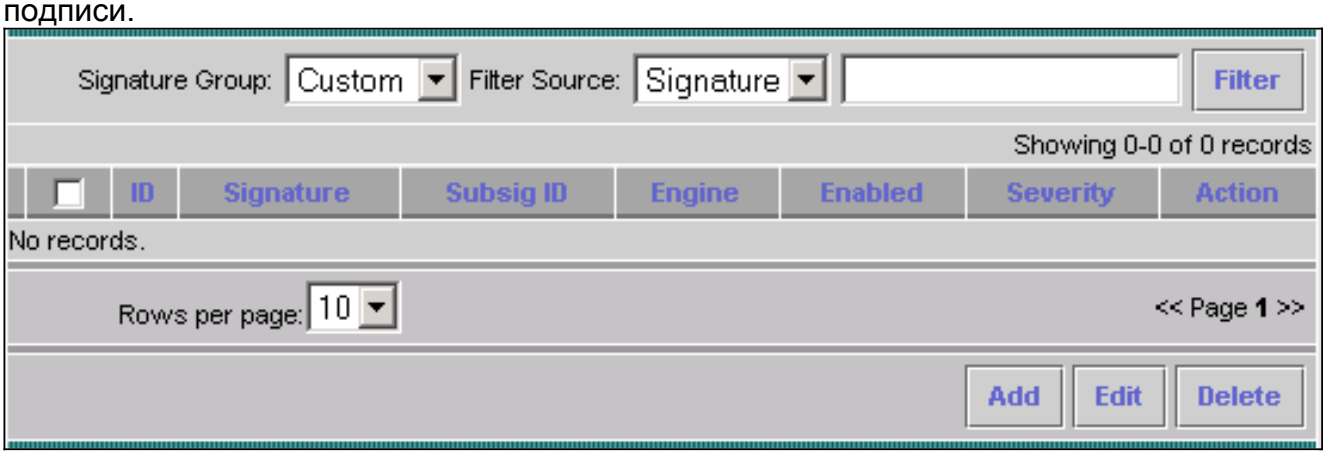
Настройте сброс TCP для маршрутизатора IOS

Выполните эти шаги для настройки сброса TCP для маршрутизатора IOS.

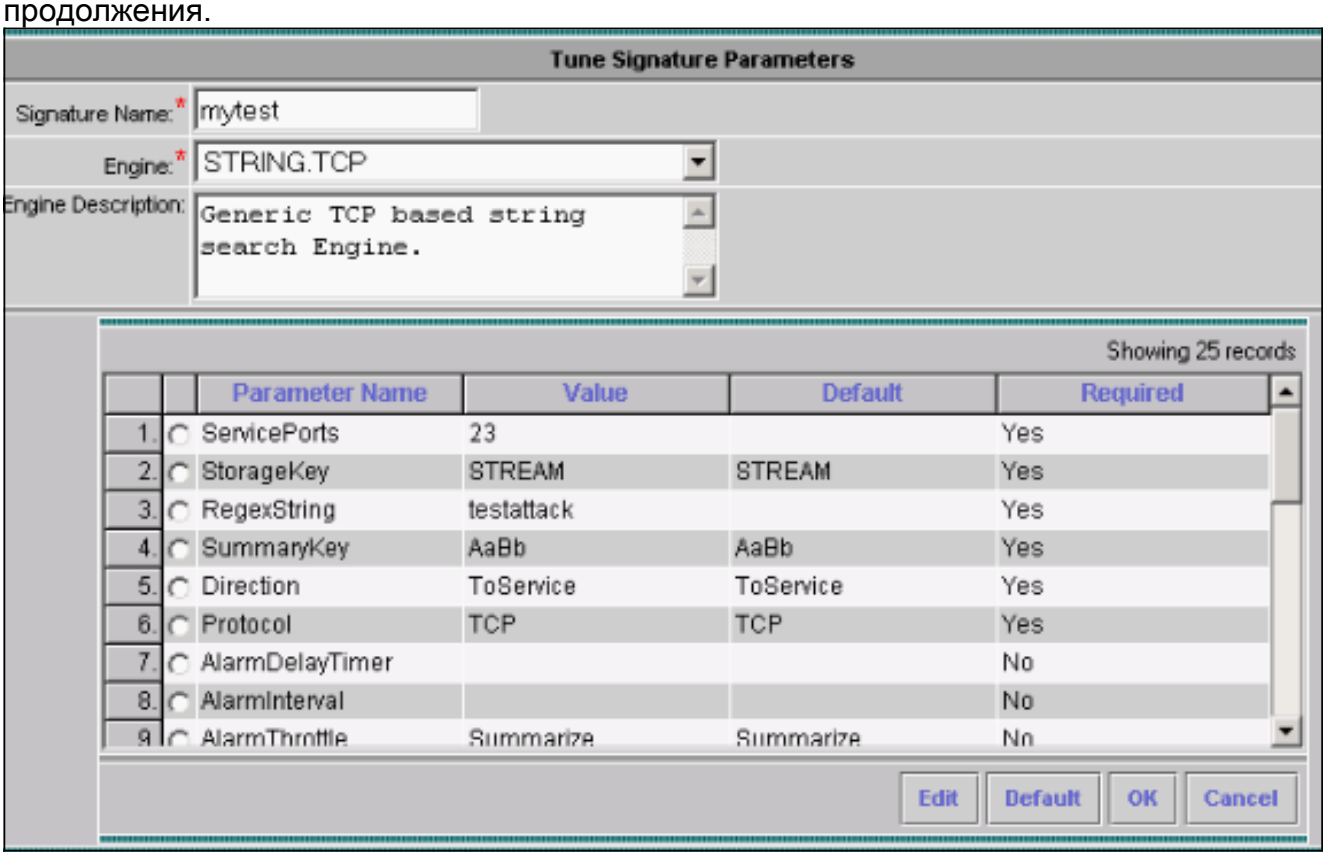
1. Выберите **VPN/Security Management Solution> Management Center> IDS Sensors**.
2. Выберите Вкладку конфигурация, выберите свой Датчик от Селектора объектов, затем

нажмите **Settings**.

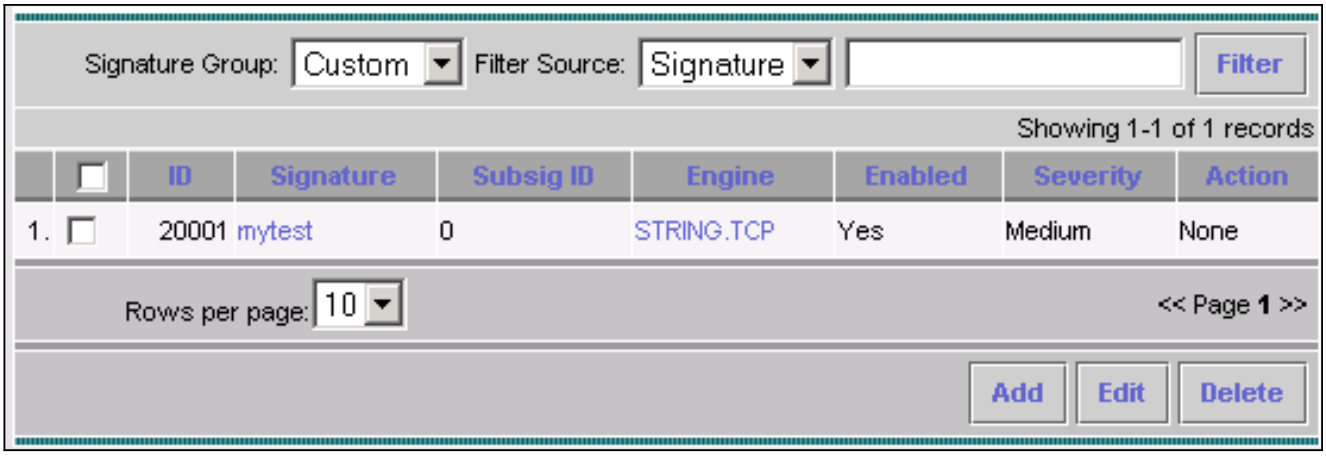
3. Выберите **Signatures**, нажмите **Custom** и **нажмите Add** для добавления новой подписи.



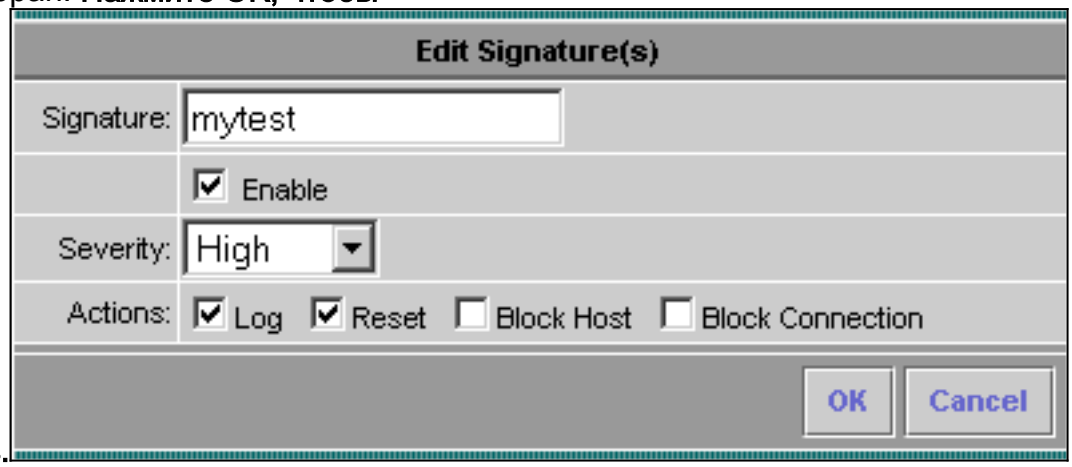
4. Введите новое Имя Подписи, затем выберите Engine (в этом случае, **Строка TCP).**
5. Проверьте соответствующую кнопку с зависимой фиксацией, чтобы настроить доступные параметры и затем нажать **Edit**.В данном примере параметр ServicePorts отредактирован для изменения его значения на **23** (для порта 23). Параметр RegexString также отредактирован для добавления **testattack** значения. Когда это будет завершено, нажмите **OK** для продолжения.



6. Нажмите название подписи для редактирования Строгости подписи и Действий или к Позволить/запретить подпись.

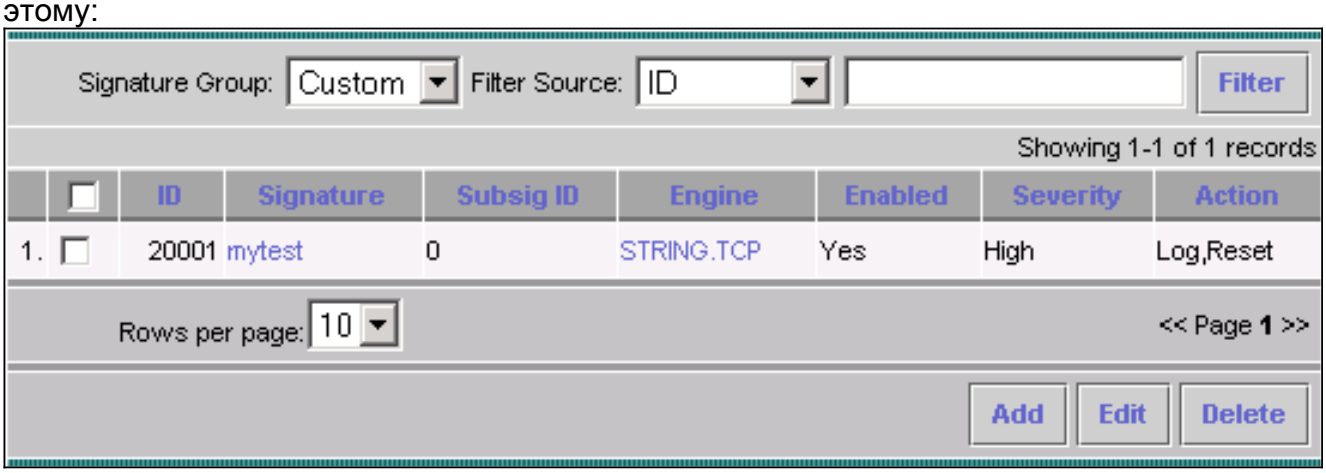


7. В этом случае степени серьезности ошибки изменены на **Высокий** и **Журнал** действия, **и Сброс** выбран. **Нажмите OK, чтобы**

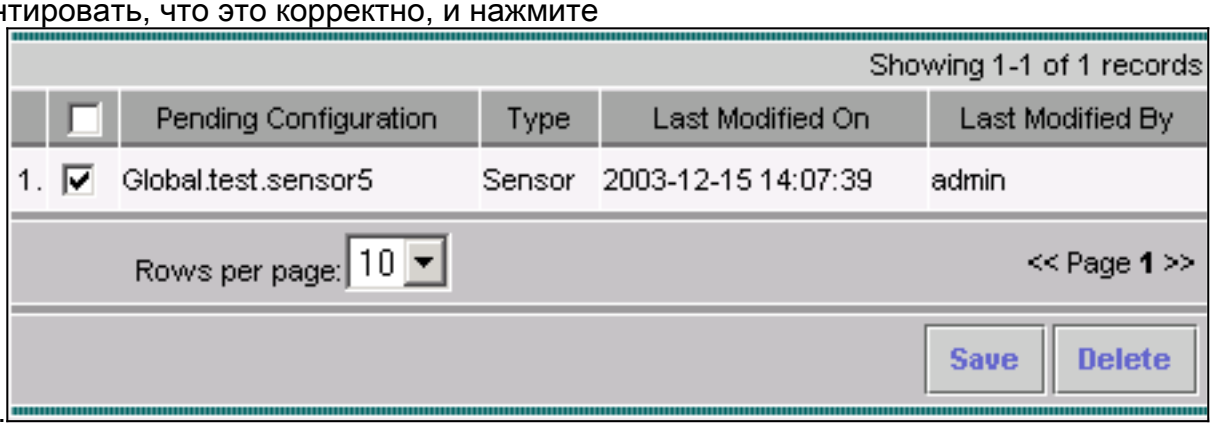


продолжить.

8. Завершенная подпись выглядит подобной этому:

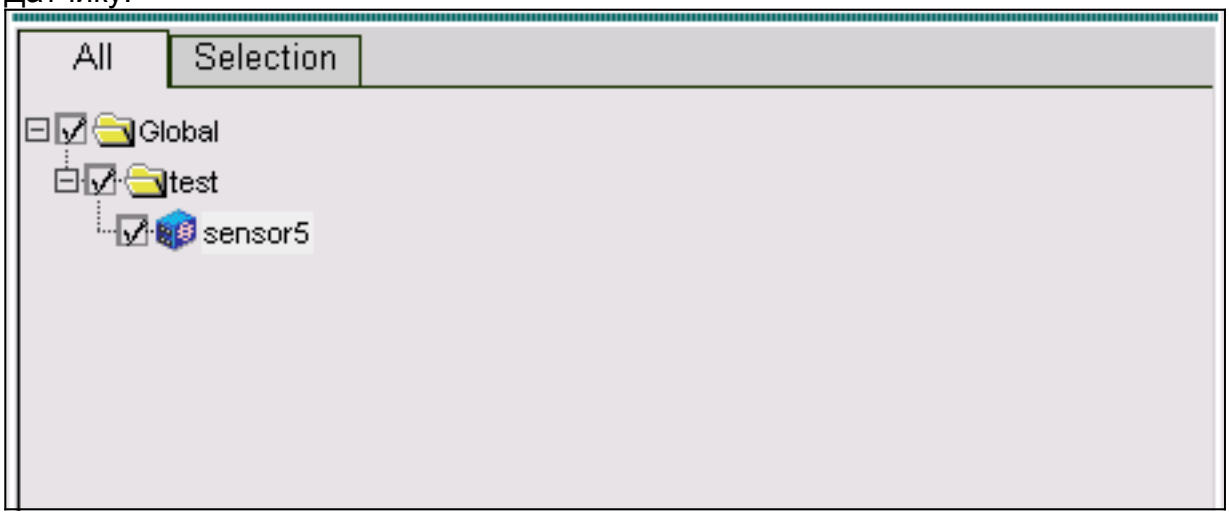


9. Выберите **Configuration> Pending**, проверьте конфигурацию ожидания, чтобы гарантировать, что это корректно, и нажмите

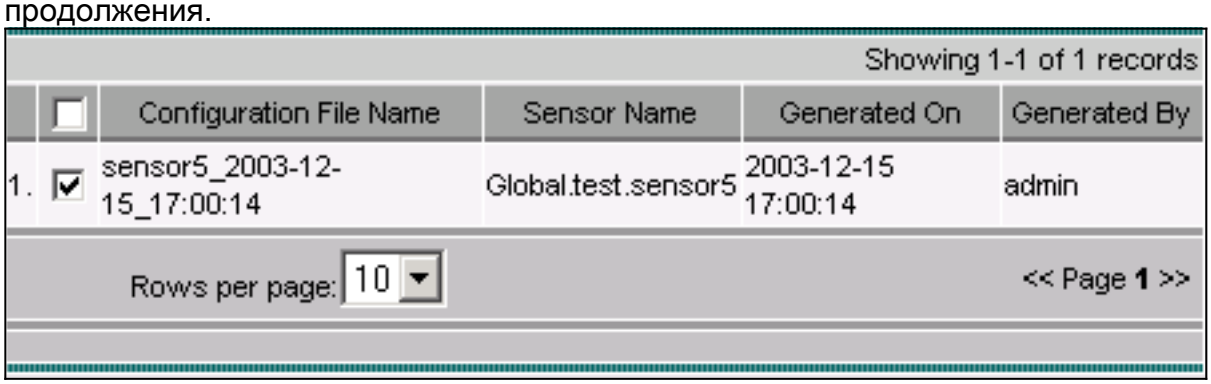


Save.

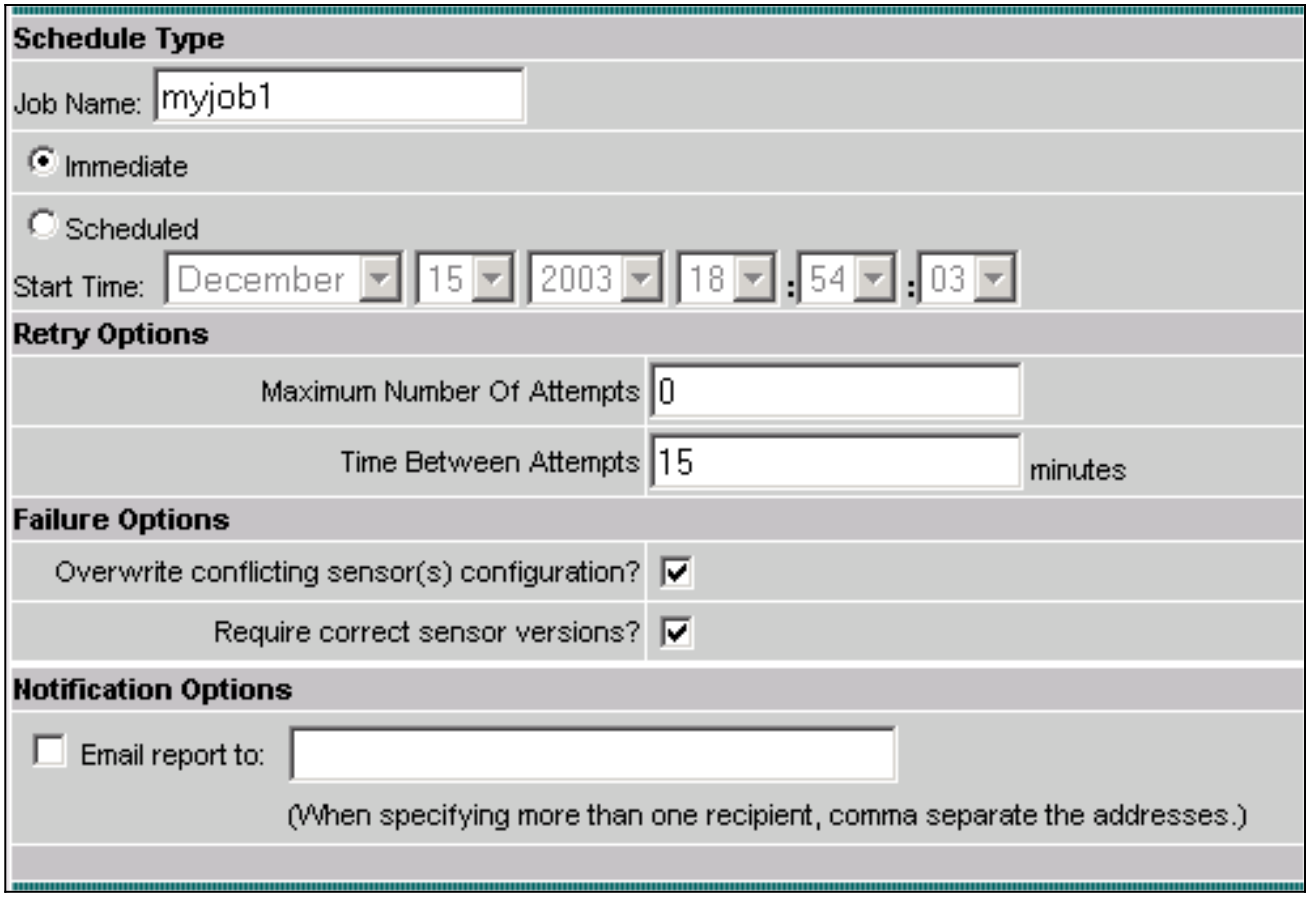
10. Выберите **Deployment> Generate**, и затем нажмите **Apply** для продвижения изменений конфигурации к
    Датчику.



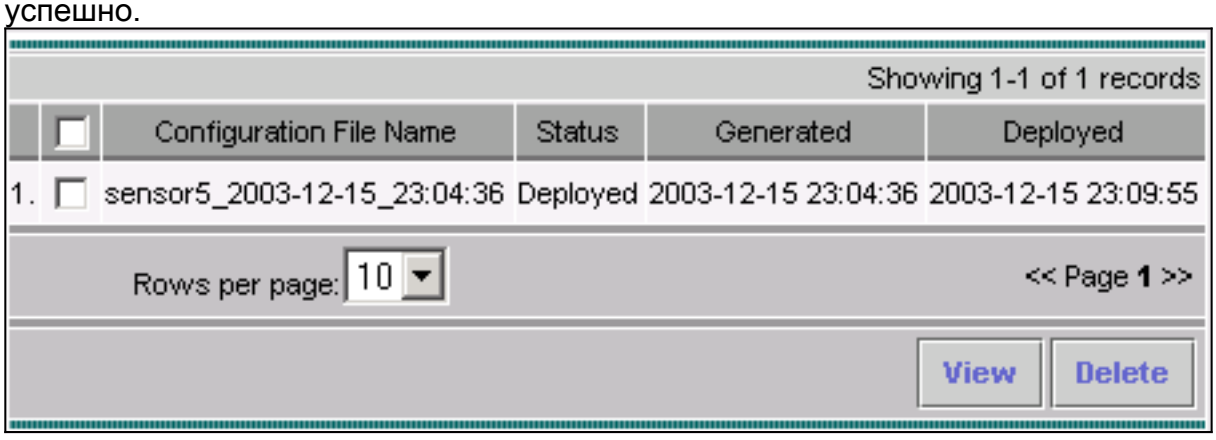
11. Выберите **Deployment> Deploy** и нажмите **Submit**.
12. Проверьте флажок рядом со своим Датчиком и нажмите **Deploy**.
13. Проверьте флажок для задания в очереди и нажмите **Next** для
    продолжения.



14. Введите Имя задания и планируйте задание как **Непосредственное**, затем нажмите **Finish**.



15. Выберите **Deployment> Deploy> Pending**.Ждите несколько минут, пока не были завершены все ожидающие задания. Очередь должна тогда быть пустой.
16. Выберите **Configuration> History** для подтверждения развертываний.Гарантируйте, что статус конфигурации отображен как **Развернутый**. Это означает, что Конфигурация сенсора обновлена
успешно.



Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

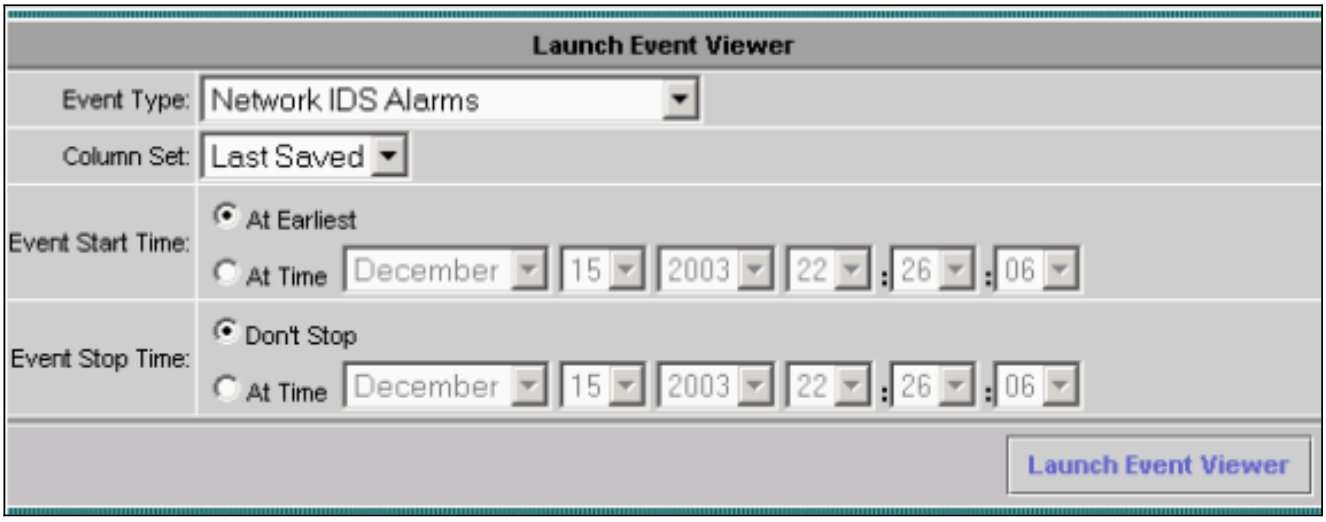
Выполните атаку и сброс TCP

Пойдите в тестовое наступление и проверьте результаты, чтобы проверить, что Блокирующий процесс работает правильно.

1. Прежде чем в наступление идут, выберите **VPN/Security Management Solution>>**

Security Monitoring Center Монитор.

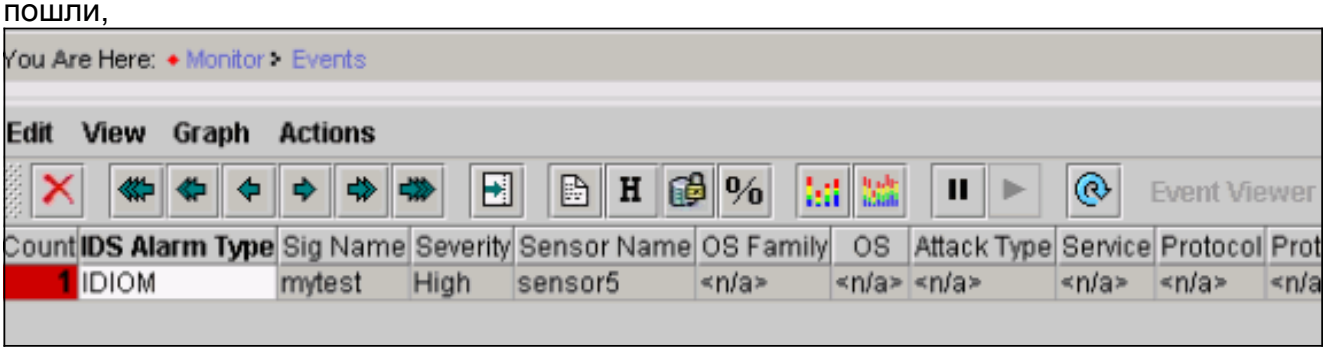
2. Выберите **Monitor** из главного меню и нажмите **Events**.
3. Нажмите **Launch Event Viewer**.



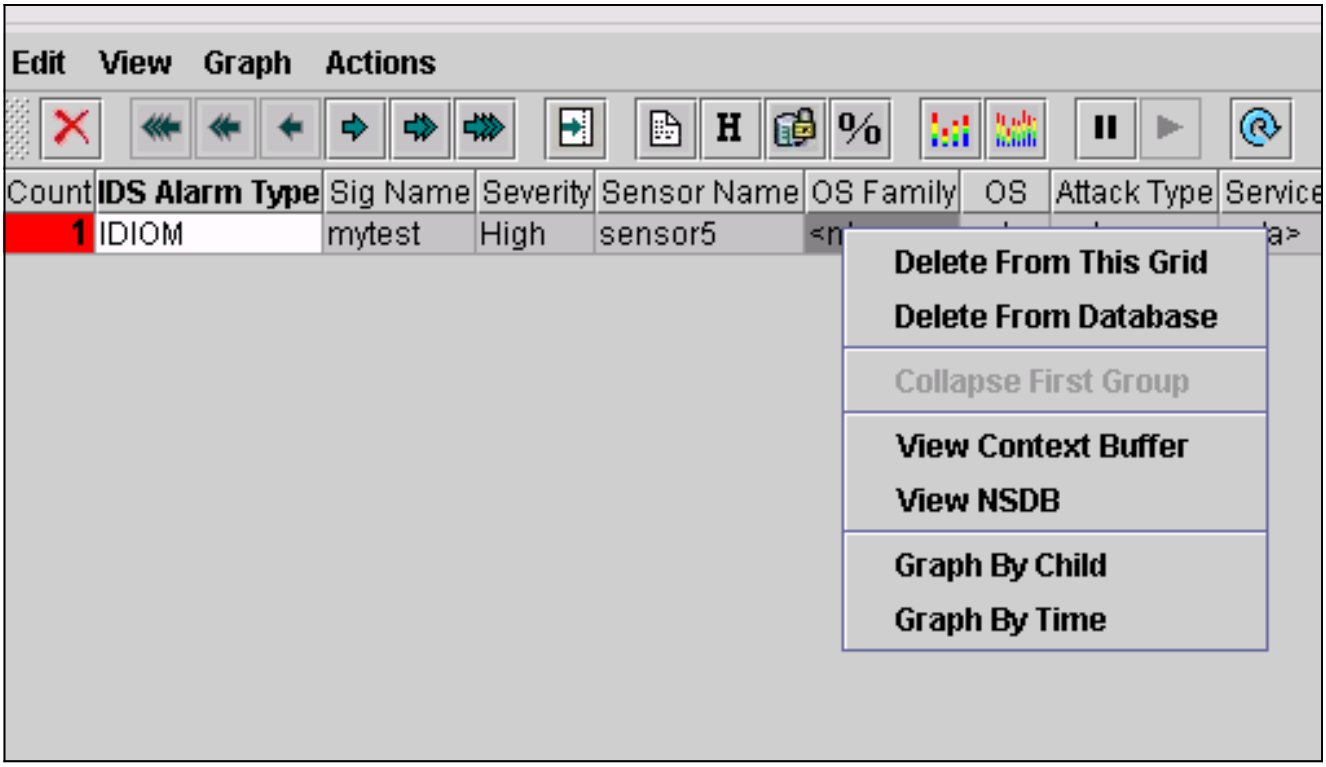
4. Telnet от одного маршрутизатора до другого и **testattack** типа, чтобы пойти в наступление.В этом случае, мы Telnetted от маршрутизатора Light до House маршрутизатора. Как только вы нажимаете **<располагают с интервалами>** или **<входят>** после ввода **testattack** сеанс Telnet должен быть перезагружен.

```
light#telnet 100.100.100.1 Trying 100.100.100.1 ... Open User Access Verification Password: house>en Password: house#testattack !--- The Telnet session is reset due to the !--- signature "testattack" being triggered. [Connection to 100.100.100.1 lost]
```

5. От Просмотра событий нажмите **Query Database** для новых событий теперь.Вы видите предупреждение для наступления, в которое ранее пошли,



6. В конечном счете Средство просмотра, выделите сигнал тревоги, щелкните правой кнопкой мыши его и выберите **View Context Buffer** или **View NSDB** для просмотра более подробной информации о сигнале тревоги.



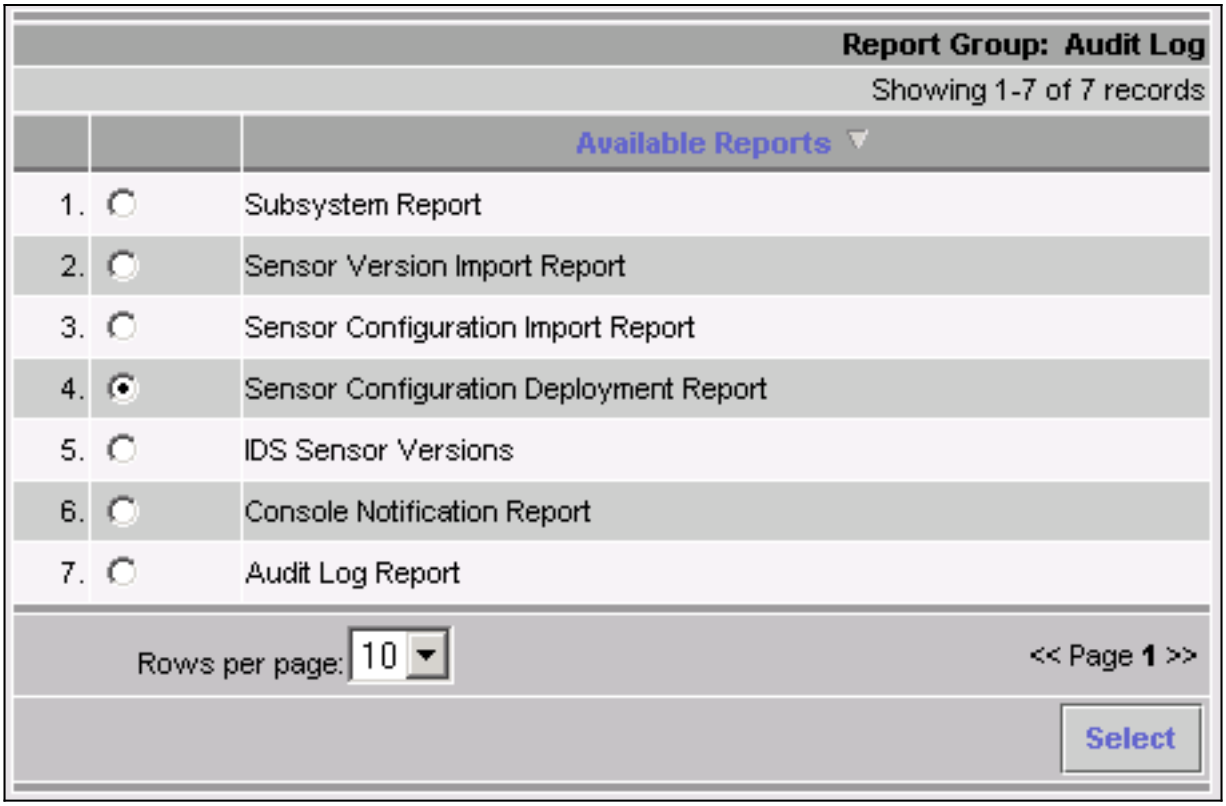
Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Процедура устранения неполадок

Выполните эти шаги, чтобы найти и устранить неисправность.

1. В MC IDS выберите **Reports> Generate**.В зависимости от типа проблемы более подробная информация должна быть найдена в одном из семи доступных отчётов.



2. В то время как Блокирование использует порт Командования и управления для настройки списков доступа к маршрутизатору, Сброс TCP передается от интерфейса анализатора Датчика. Гарантируйте охват правильного порта, с помощью **команды set span** на коммутаторе, подобном этому:
```
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 !--- In this case, connect to Ethernet1 of Router House. Oper Source : Port 2/12 Direction : transmit/receive Incoming Packets: enabled Learning : enabled Multicast : enabled
```
3. Если Сброс TCP не работает, вход в систему к Датчику, и введите **команду show event**.Пойдите в наступление и проверку, чтобы видеть, инициирован ли сигнал тревоги. Если сигнал тревоги инициирован, проверьте, чтобы гарантировать, что он установлен для **сброса TCP** типа действия.

Дополнительные сведения

- Страница поддержки системы обнаружения несанкционированного доступа Cisco
- Документация по системе обнаружения несанкционированного доступа Cisco
- Страница технической поддержки Решения CiscoWorks VPN/Security Management Solution
- Cisco Systems – техническая поддержка и документация