Настройка Cisco Secure IDS Sensor в CSPM

Содержание

Введение

Этот документ объясняет, что процедура использовала настраивать Cisco Secure Intrusion Detection System (IDS) Датчик на Cisco Secure Policy Manager (CSPM). Документ предполагает, что CSPM версии 2.3.I на компьютере уже установлена. Версия "I" разрешает управление устройствами IDS (сенсоры устройств, маршрутизаторы Cisco IOS® и выводы IDS) в коммутаторе Cisco Catalyst® 6000. Этот документ также предполагает, что правильно определены параметры почтовой станции IDS. Они включают HOSTID, ORGID, ИМЯ ХОСТА и ORGNAME. Обратите внимание, что для того, чтобы узел CSPM смог установить связь с Sensor, ORGID и ORGNAME должны соответствовать значениям, определенным на Sensor.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на CSPM 2.3. Я и позже.

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.

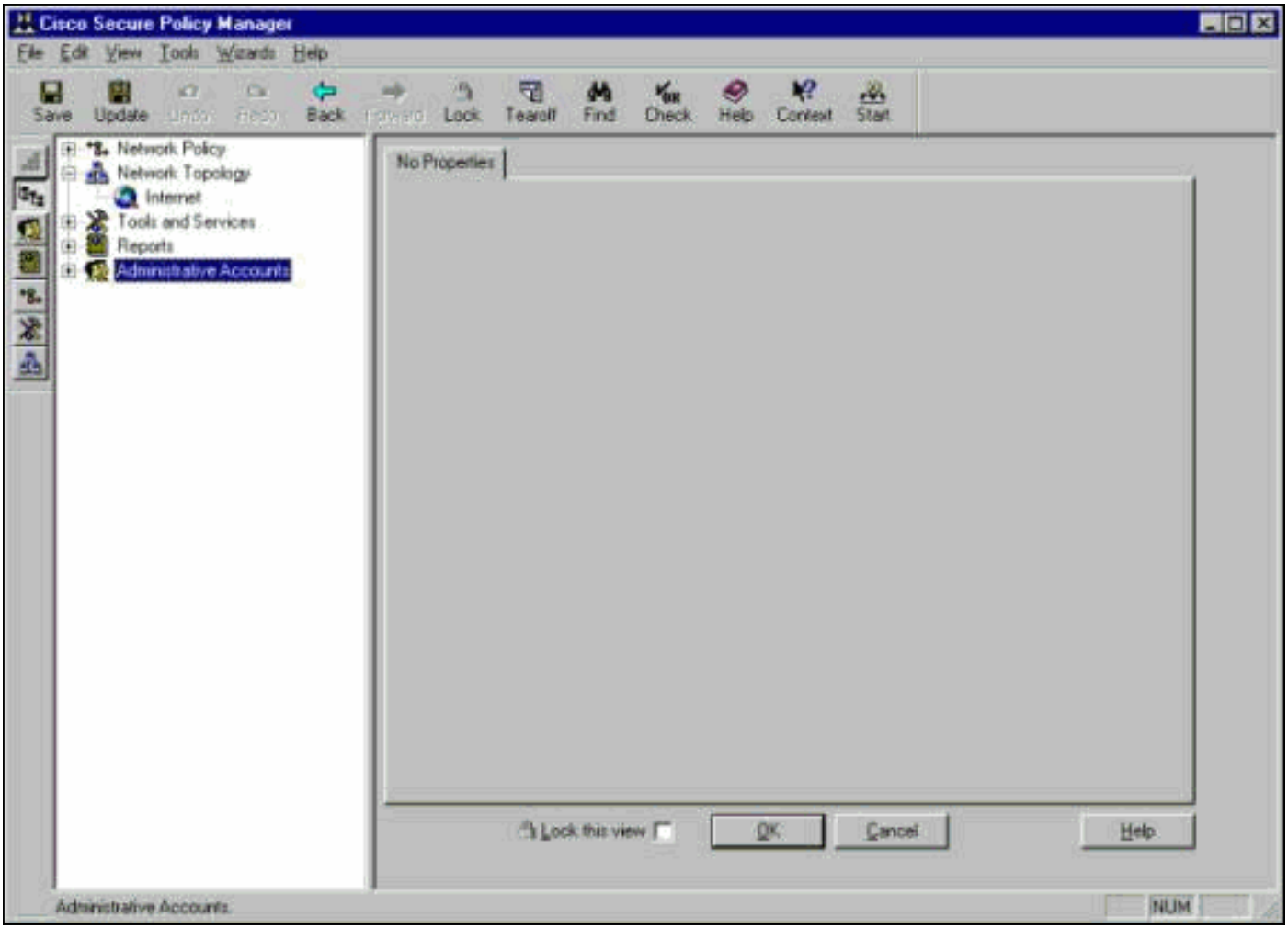
Условные обозначения

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

!--- конфигурацию

Эти разделы объясняют, что процесс использовал настраивать Детектор обнаружения несанкционированного доступа (IDS Sensor) в CSPM.

CSPM запуска и входит. Появляется чистый шаблон (первый запуск), который позволяет определить сеть.

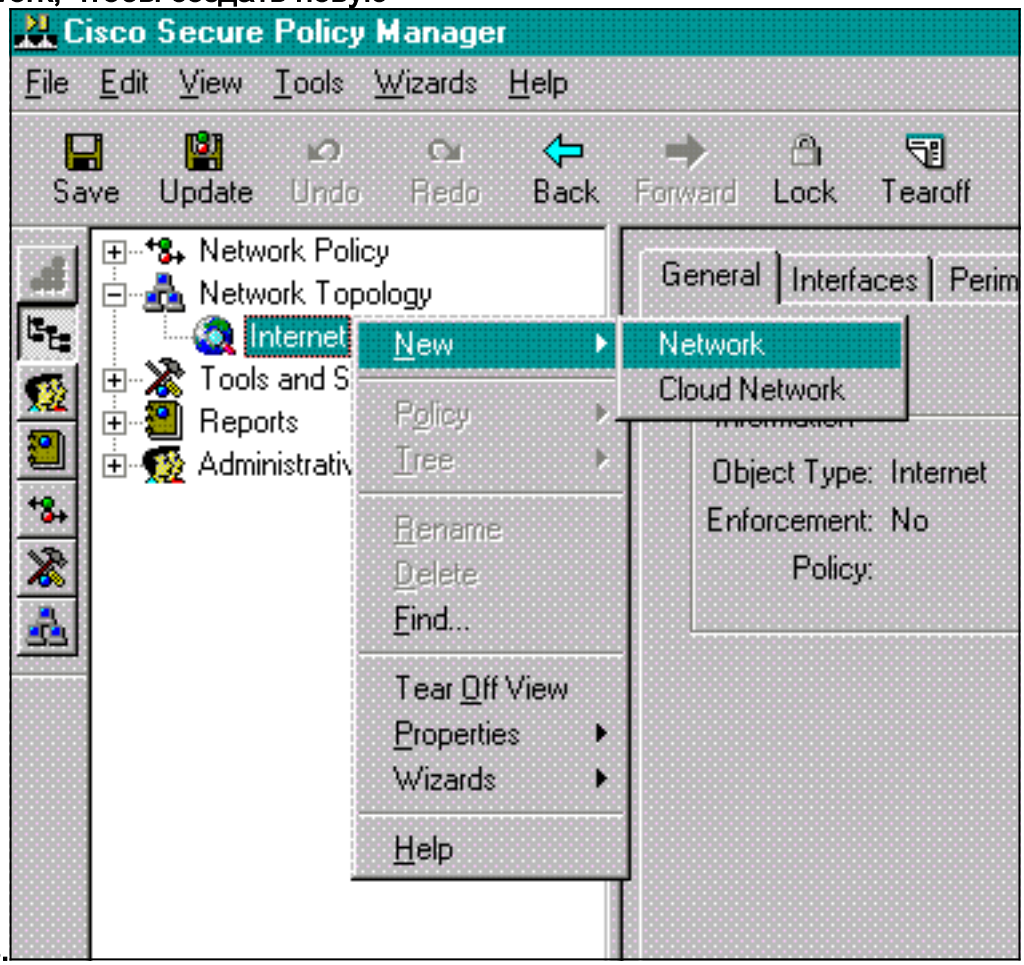


Эти три определения требуются в Топологии CSPM для IDS.

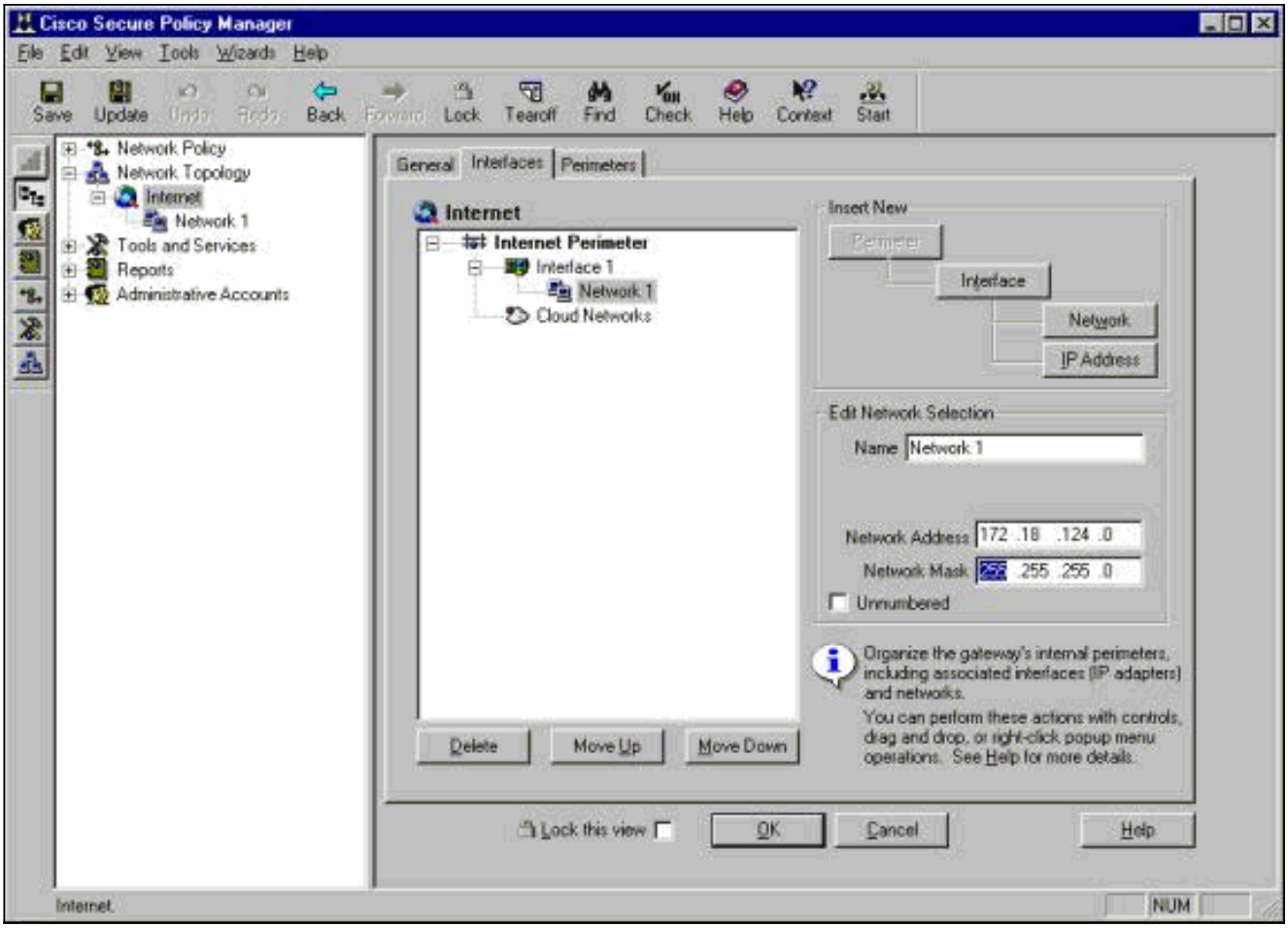
1. Определите сеть, в которой расположен интерфейс управления детектором, и сеть, в которой расположен хост CSPM. Если они находятся в той же подсети, то только одна сеть должна быть определена. Прежде всего, определить эту сеть.
2. Определите хост CSPM в его сети. Без определения хоста CSPM управление датчиком Sensor невозможно.
3. Определите датчик в его сети.

Определите сеть, на которой размещается хост CSPM

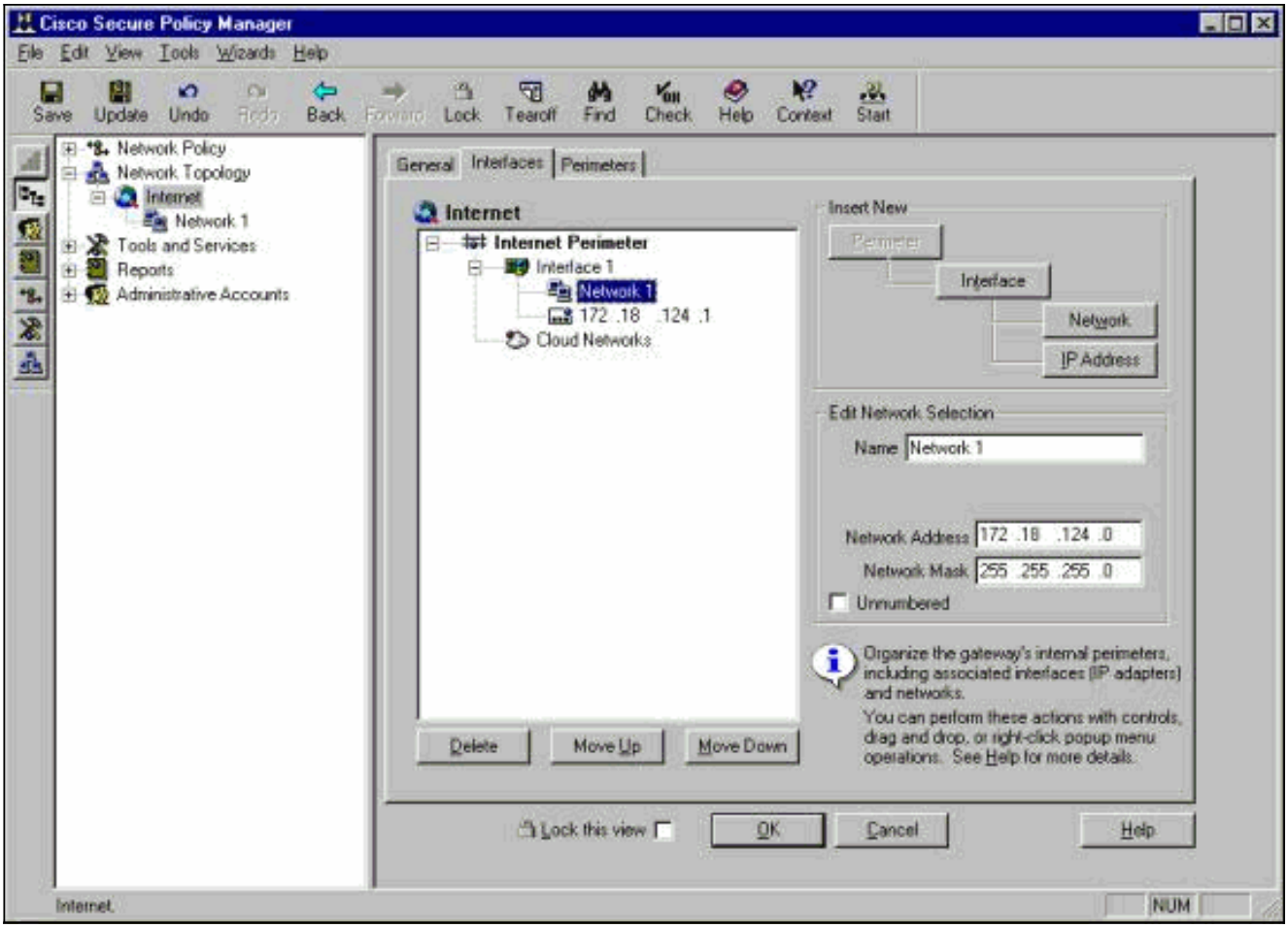
Выполните следующие действия:

1. **Щелкните значок Интернета в топологии правой кнопкой мыши и выберите New > Network, чтобы создать новую**


сеть.
2. В правой стороне сетевой панели укажите имя новой сети, адрес сети и используемую маску
подсети.



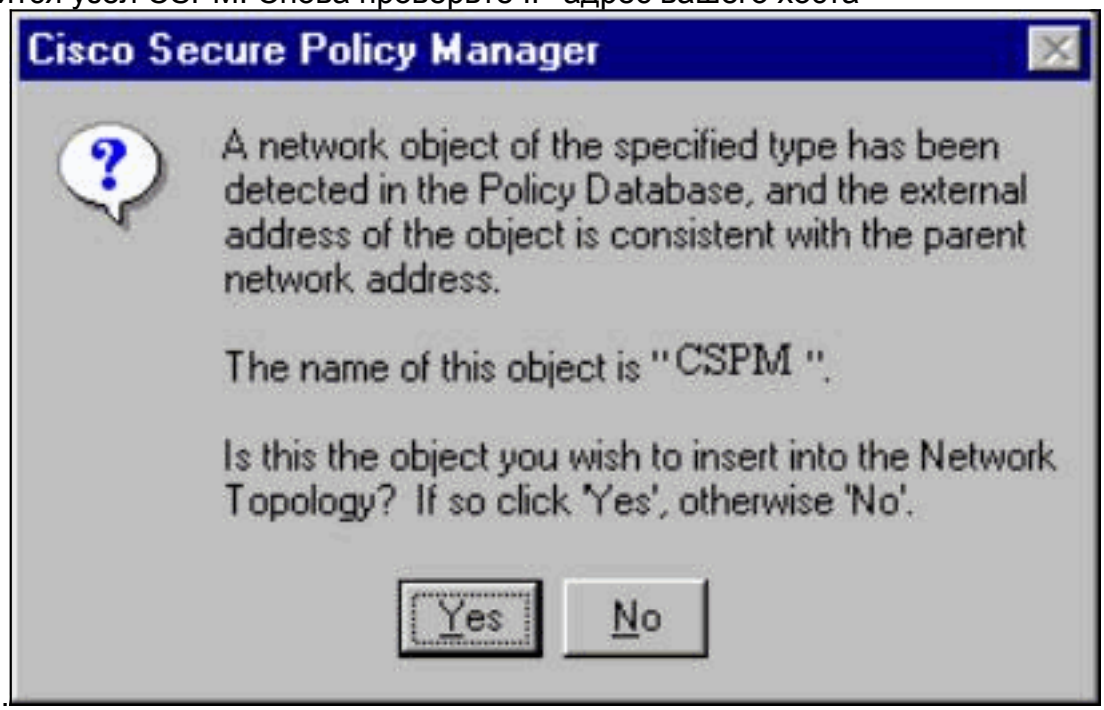
3. **Нажмите кнопку IP Address (IP-адрес) и введите IP-адрес для сети, используемый для выхода в интернет.**Обычно это - Шлюз по умолчанию для сети.**Примечание:** При управлении Датчиками адрес шлюза должен не обязательно быть корректным, так как Датчик не передается эти сведения о шлюзе по умолчанию. Это должно уже быть определено в Датчике.
4. **Нажмите кнопку OK.** Сеть добавлена к схеме топологии без любых ошибок.



Добавление узла CSPM

Используйте эту процедуру для добавления хоста CSPM.

1. В Топологии сети щелкните правой кнопкой мыши в сети, которую вы просто добавили, и выберите **New> Host**.CSPM переводит в рабочее состояние экран, подобный этому. Если этого не произойдет, значит, указанная вами сеть не является сетью, в которой находится узел CSPM. Снова проверьте IP-адрес вашего хоста



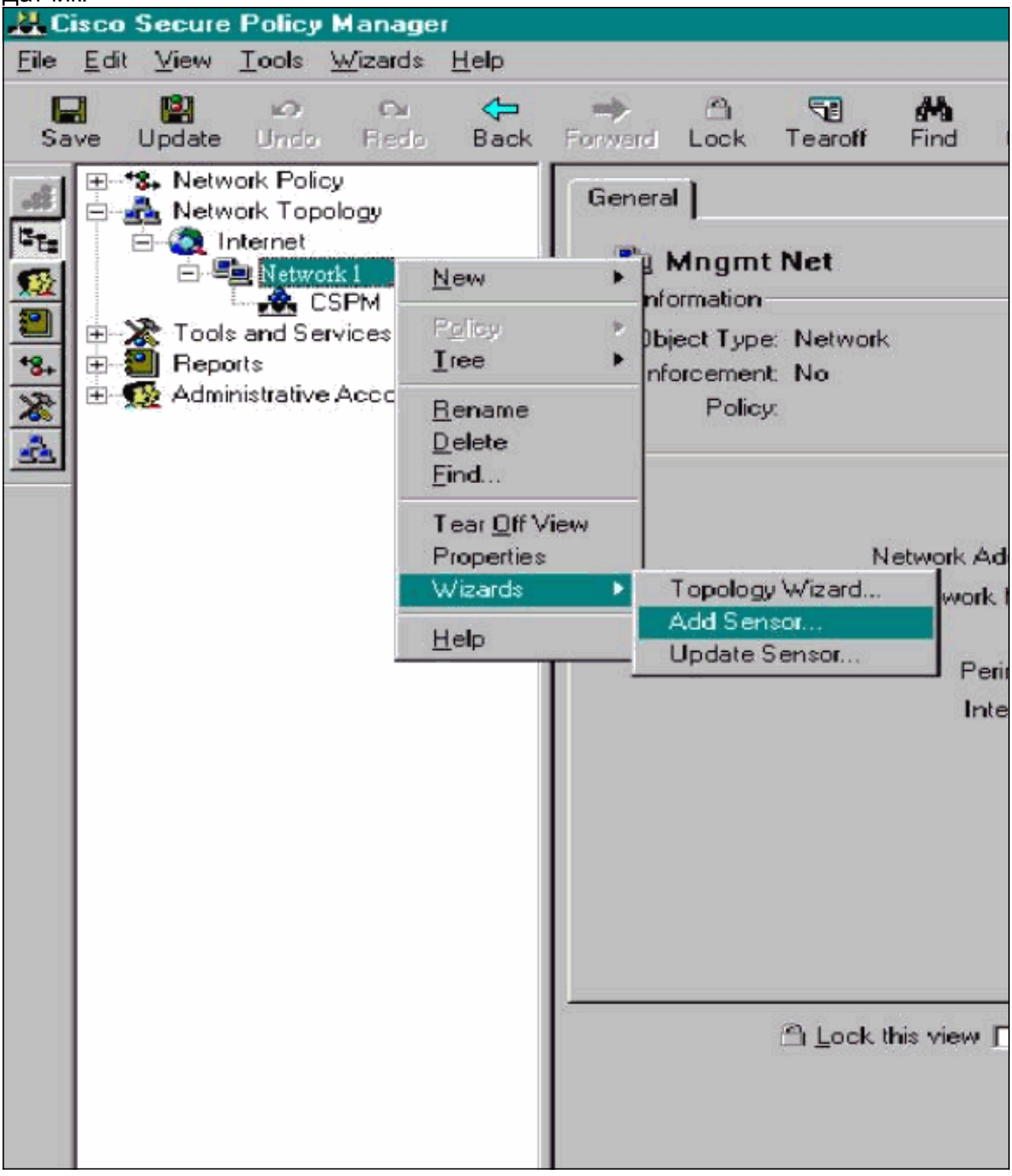
CSPM.

2. **Нажмите кнопку "Да", чтобы установить хост CSPM в топологию.**
3. Проверьте правильность данных, указанных на главном экране для хоста CSPM.
4. **Нажмите кнопку OK на главном экране хоста CSPM.**

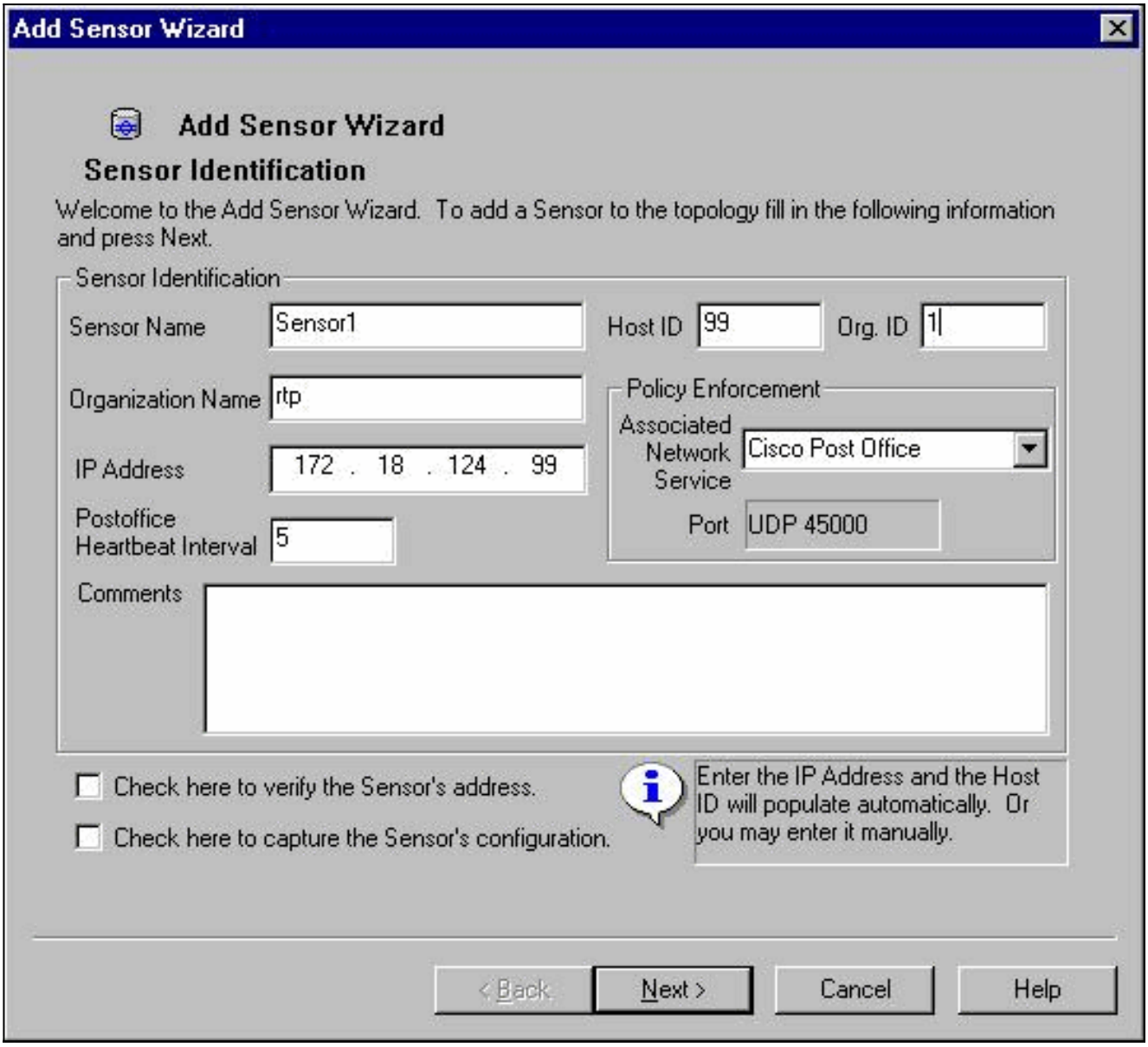
Добавление сенсорного устройства

Используйте эту процедуру для добавления Датчика.

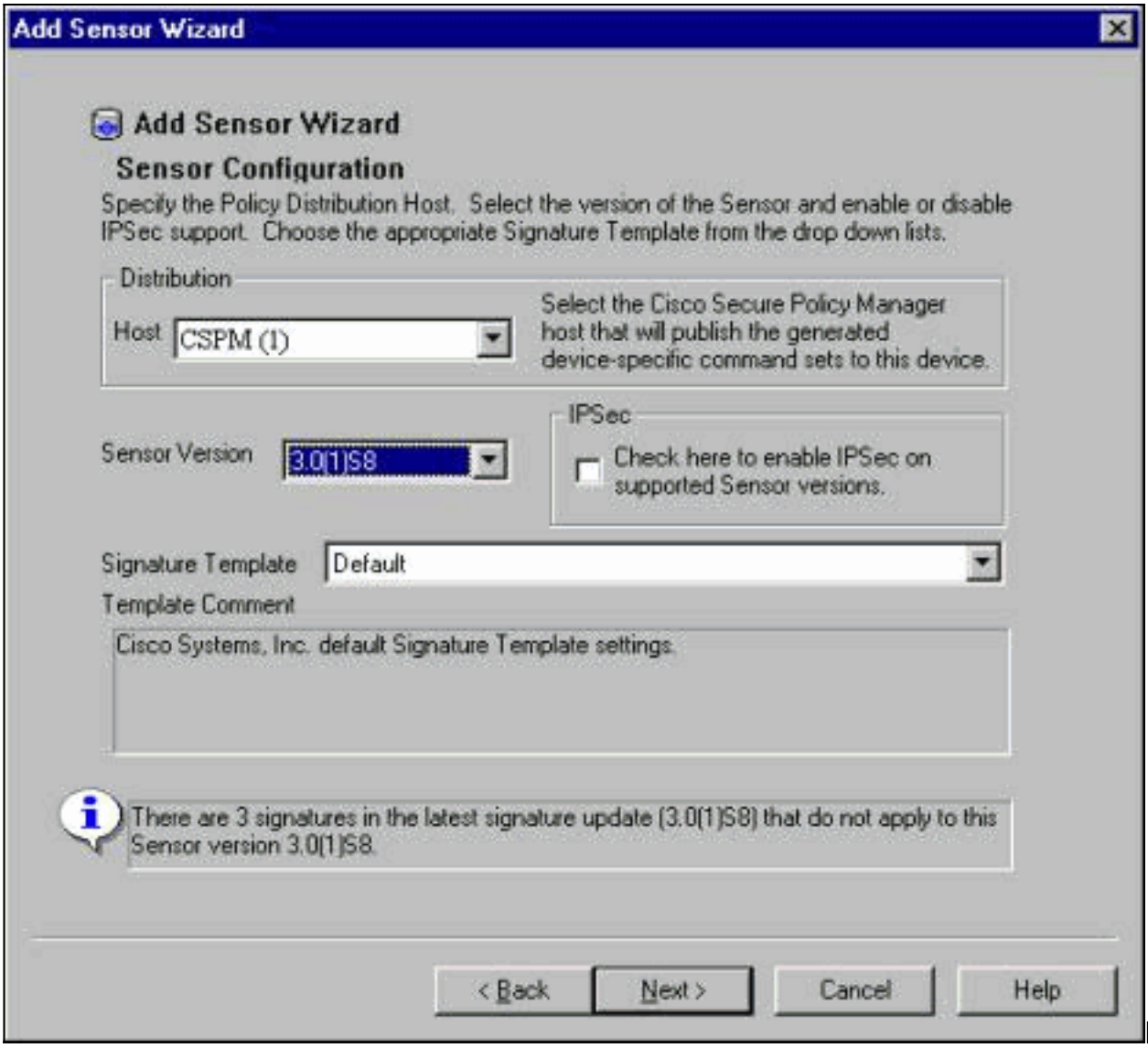
1. Щелкните правой кнопкой мыши в сети, в которой находится ваш Датчик, и выберите **Wizards> Add Sensor**.**Примечание:** Если хост CSPM и контрольный интерфейс вашего Датчика не находятся в той же сети, определяют сеть, в которой находится ваш Датчик.



2. Введите правильные параметры postoffice для Sensor.



3. **Щелкните поле Check here to verify the Sensor's address.Примечание:** Если это первоначально, вы устанавливаете этот Датчик, вы не хотите перехватывать конфигурацию Датчика. Если вы ранее настроили этот Датчик в другом месте или через UNIX Director или через другой хост CSPM и изменили конфигурацию Подписей датчиков, то вы хотите перехватить конфигурацию Датчика.
4. **Нажмите кнопку Next для определения версий подписи датчика.** Можно также выполнить **команду nrvers** для проверки этого на Датчике.



Примечание: Если CSPM не имеет корректной Версии датчика, что вы работаете на своем Датчике, обновляете подписи на вашем хосте CSPM. [Для обновления просмотрите Software Download (только для зарегистрированных пользователей).]

5. **Нажмите кнопку Next (Далее) для продолжения.**
6. Нажмите **Finish** для завершения установки Датчика в топологию.
7. **В главном меню CSPM выберите File > Save and Update, чтобы скомпилировать данные, введенные в топологии, в CSPM.** Учтите, что этот шаг необходим для запуска протокола PostOffice на хосте CSPM.
8. Проверьте, что все работает путем вхождения в Датчик как в пользователя netrangr.
9. **Выполните команду nrconns.**`>nrconns Connection Status for gacy.rtp cspm.rtp Connection 1: 172.18.124.106 45000 1 [Established] sto:0004 with Version 1 netrangr@gacy:/usr/nr >`

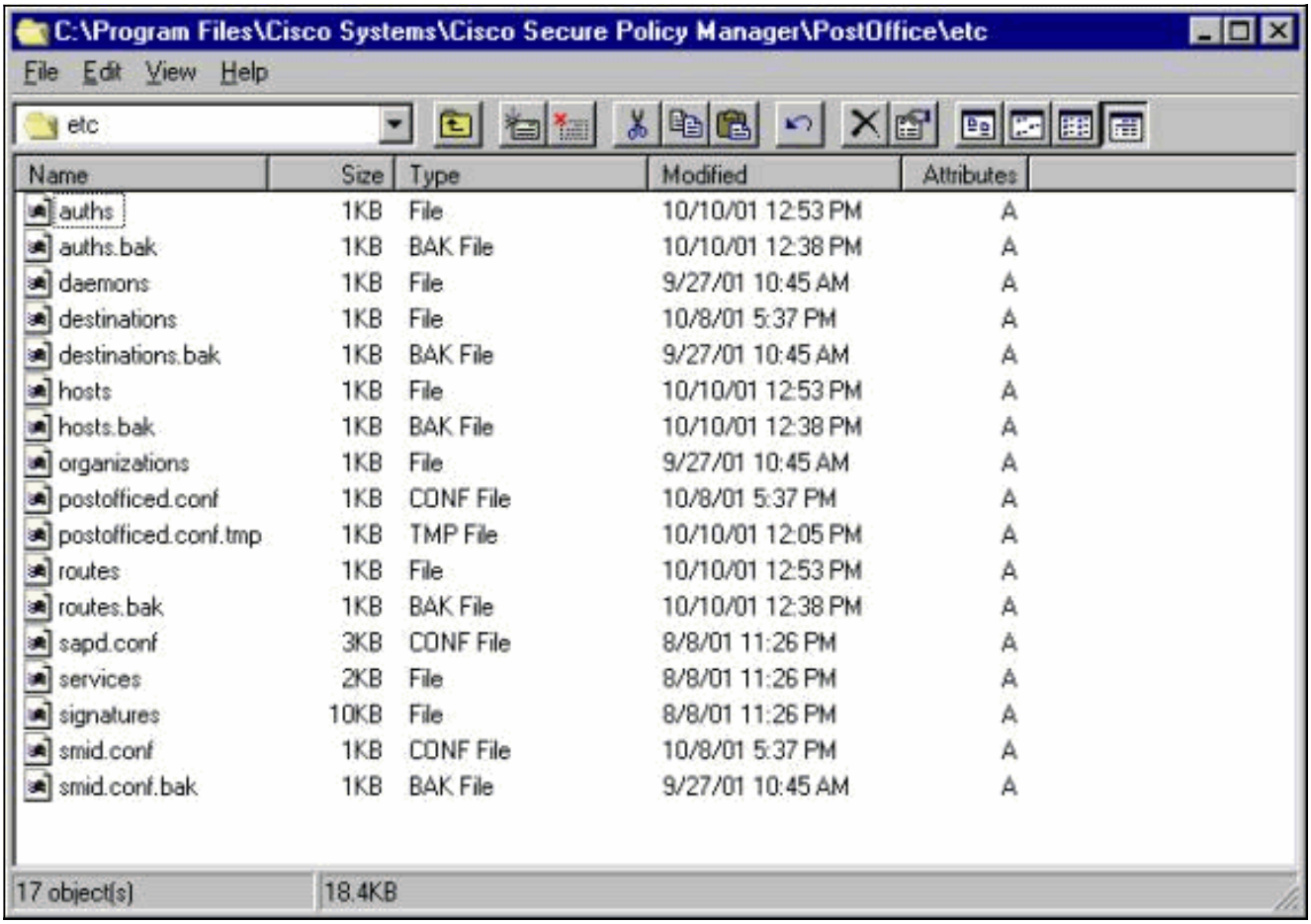
Примечание: Если Датчик и хост CSPM не связываются, выведите подобный этому, появляется вместо этого:`netrangr@gacy:/usr/nr`

`>nrconns Connection Status for gacy.rtp insane.rtp Connection 1: 172.18.124.194 45000 1 [SynSent] sto:5000 syn NOT rcvd! netrangr@gacy:/usr/nr` Если это верно, заставьте отслеживание средств прослушивания видеть, передают ли обе стороны UDP 45000 пакетов. UDP 45000 – это то, чем пользуются IDS-устройства для связи друг с другом. Для тестирования этого на Датчике, **su** для укоренения и (в зависимости от того, какой Датчик вы имеете) выполняют **порт 45000-d iprb1 ищейки** (для датчика IDS 4210) и **ищейка-d порт 45000 iprb0** (для любой другой модели Датчика).Используйте **<Control-c>** для убегания из сеанса ищейки.Если нет никакой связи между Датчиком и CSPM, эти

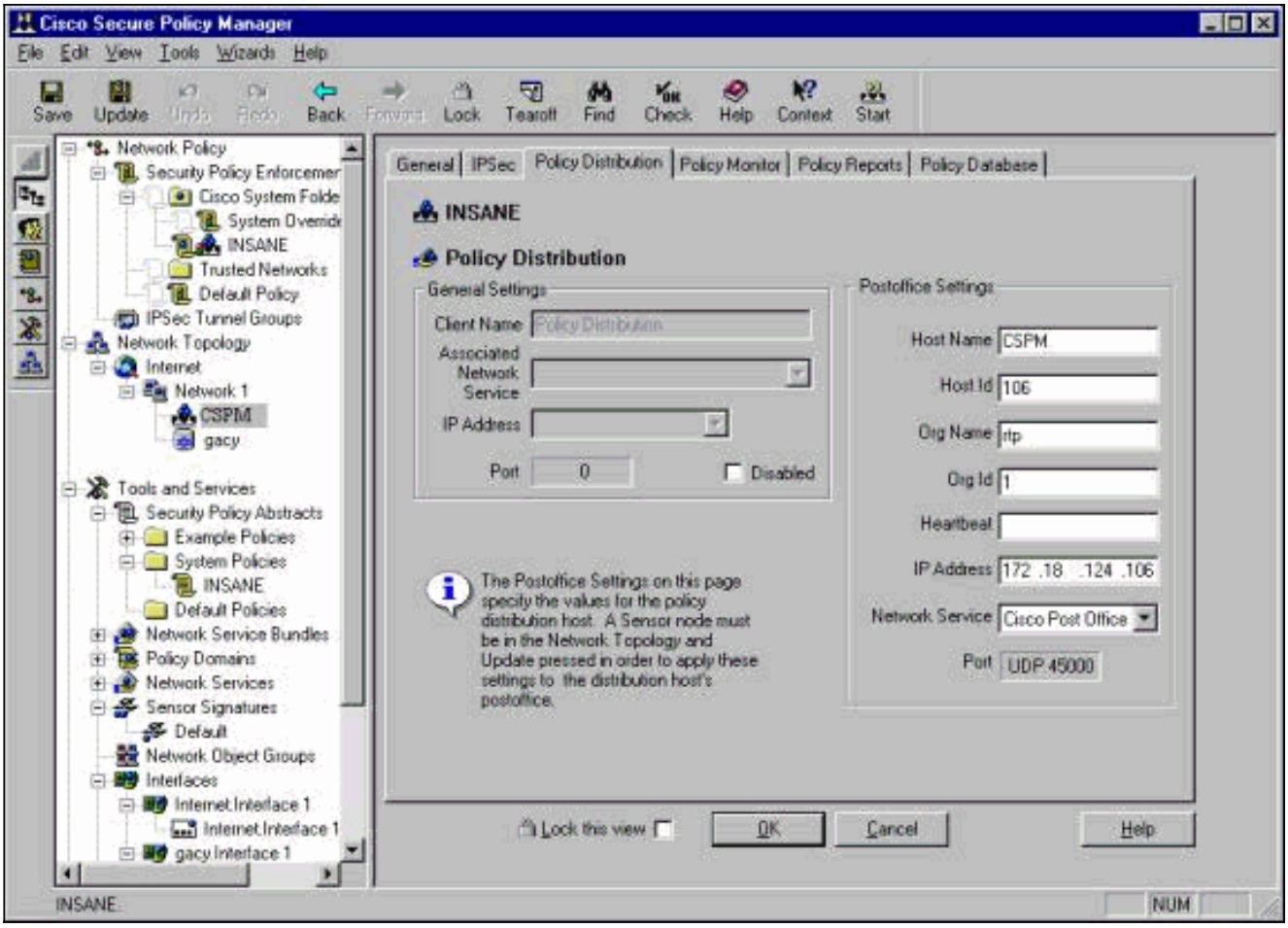
выходные данные появляются:`netrangr@gacy:/usr/nr`

```
>su - Password: Sun Microsystems Inc. SunOS 5.8 Generic February 2000 # snoop -d spwr0 port 45000 Using device /dev/spwr (promiscuous mode) 172.18.124.100 -> 172.18.124.106 UDP D=45000 S=45000 LEN=52 172.18.124.100 -> 172.18.124.106 UDP D=45000 S=45000 LEN=52 172.18.124.100 -> 172.18.124.106 UDP D=45000 S=45000 LEN=52 172.18.124.100 -> 172.18.124.106 UDP D=45000 S=45000 LEN=52 ^C#
```

В вышеупомянутых выходных данных Датчик передает UDP 45000 пакетов, но не получает никого. Корректная конфигурация производит выходные данные, подобные этому:`# snoop -d spwr0 port 45000 Using device /dev/iprb (promiscuous mode) 172.18.124.106 -> gacy UDP D=45000 S=45000 LEN=56 gacy -> 172.18.124.106 UDP D=45000 S=45000 LEN=56 172.18.124.142 -> gacy UDP D=45000 S=45000 LEN=56 gacy -> 172.18.124.194 UDP D=45000 S=45000 LEN=56` В вышеупомянутых выходных данных трафик UDP 45000 входит в оба направления.Если не совпадает UDP, 45000 пакетных потоков в обоих направлениях и выходных данных **nrconns** на Датчике все еще говорят, что нет никакого установленного соединения, параметры postoffice на Датчике и хосте CSPM.Для проверки параметров postoffice на CSPM размещают вручную:Используйте Проводник Windows для навигации туда, где вам установили CSPM на компьютере под управлением ОС
NT.



Отредактируйте хост, маршрут и файлы организации с Записью или Wordpad (не используйте Блокнот, потому что форматирование будет повреждено).Убедитесь, что данные файлы подходят для установки. Если какое-либо из значений не корректно, редактирует их и перезагружает ваш NT, использующий компьютеры эти шаги:Щелкните **по значку CSPM** в топологии сети.Щелкните по вкладке Policy Distribution для ввода параметров postoffice.**Сохраните и Обновите ваши изменения.**Перезагрузите NT-
компьютер.



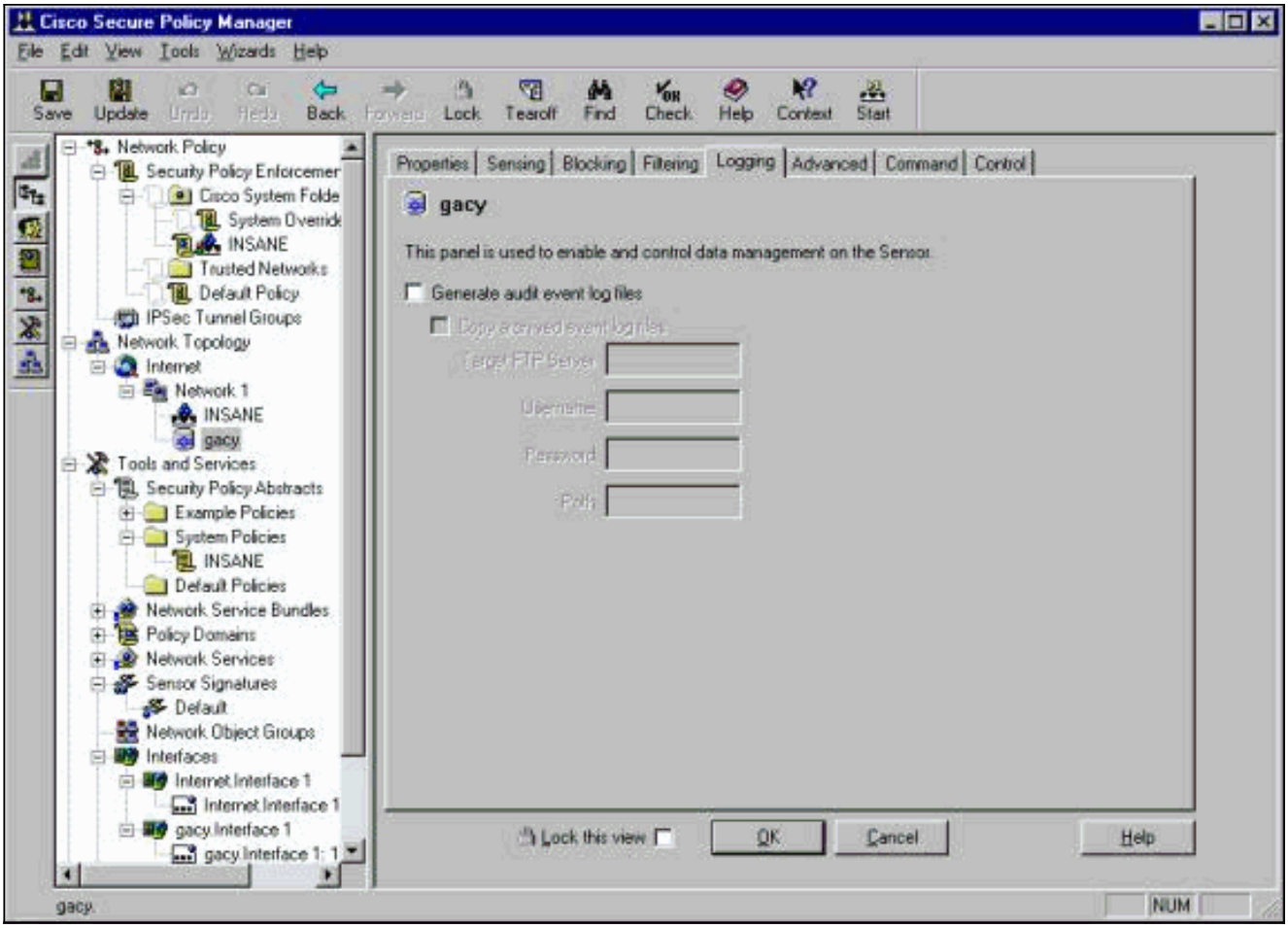
Настройка датчика

После того, как конфигурация сохранена в CSPM, настройте Датчик. Чтобы сделать это, сначала заставьте Датчик писать сигналы тревоги, которые он видит к его собственному журналу. Затем заставьте Датчик "осуществлять сниффинг" на корректном интерфейсе.

Запишите аварийные сигналы в журнал

Используйте эту процедуру для записи сигналов тревоги в журнал.

1. **Отметьте файлы журнала проведения проверки, чтобы датчик отослал аварийный сигнал локальным журналам.**Это также передает сигналы тревоги к коробке CSPM по умолчанию после того, как вы оттолкнете конфигурацию к
нему.

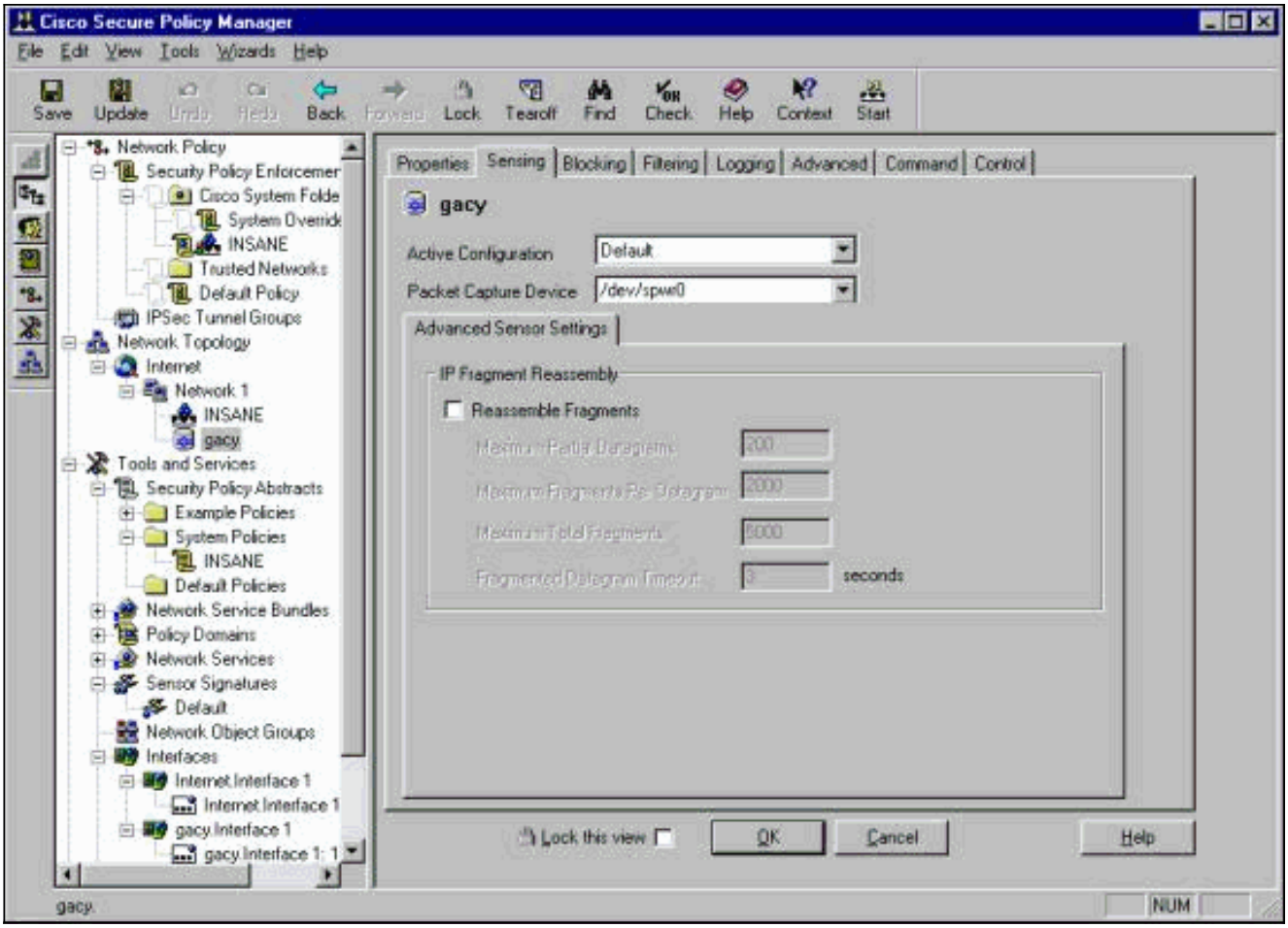


2. **Для продолжения нажмите кнопку OK.**

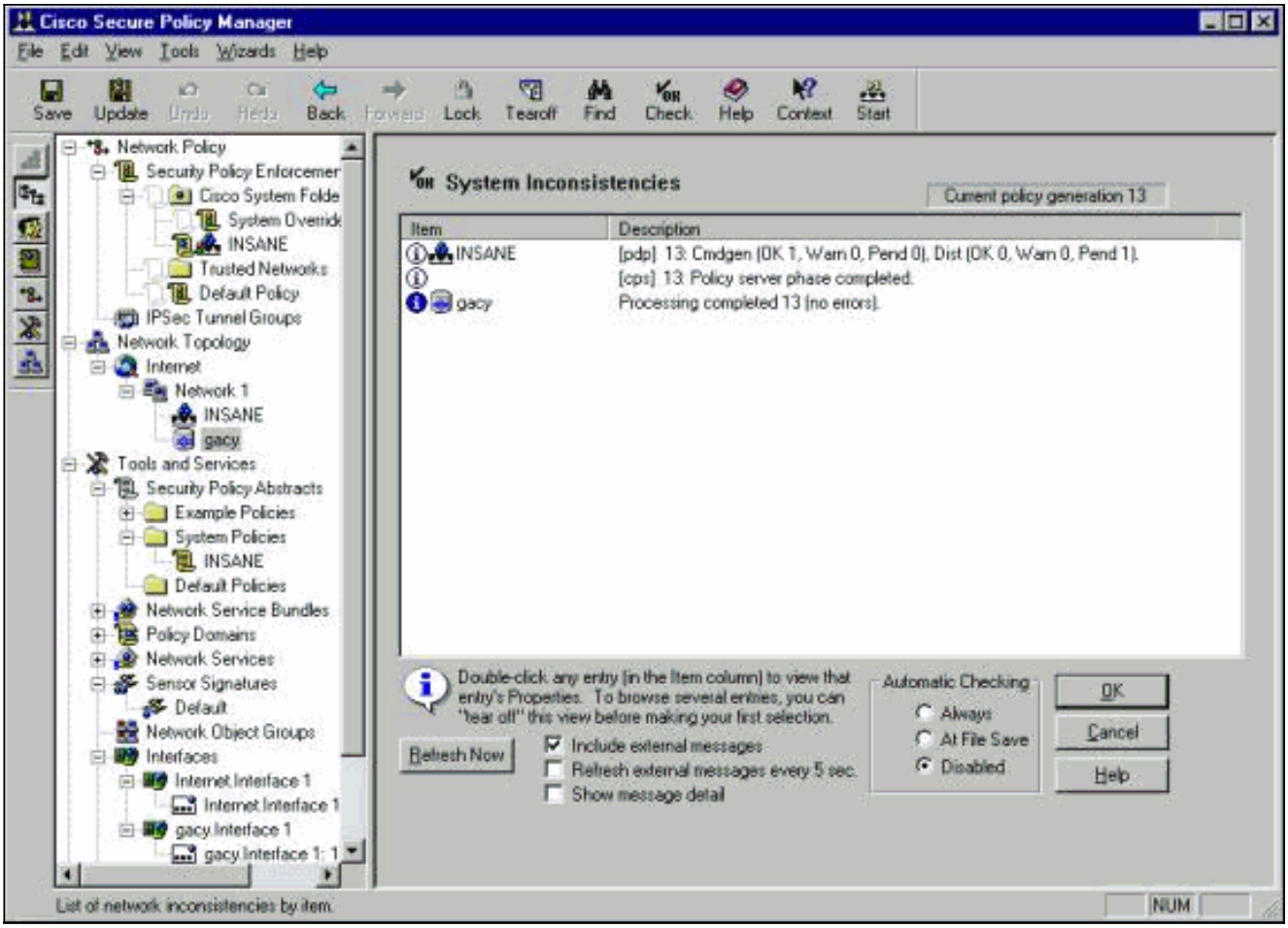
Заставьте датчик "осуществлять сниффинг"

Используйте эту процедуру, чтобы заставить Датчик "Осуществлять сниффинг".

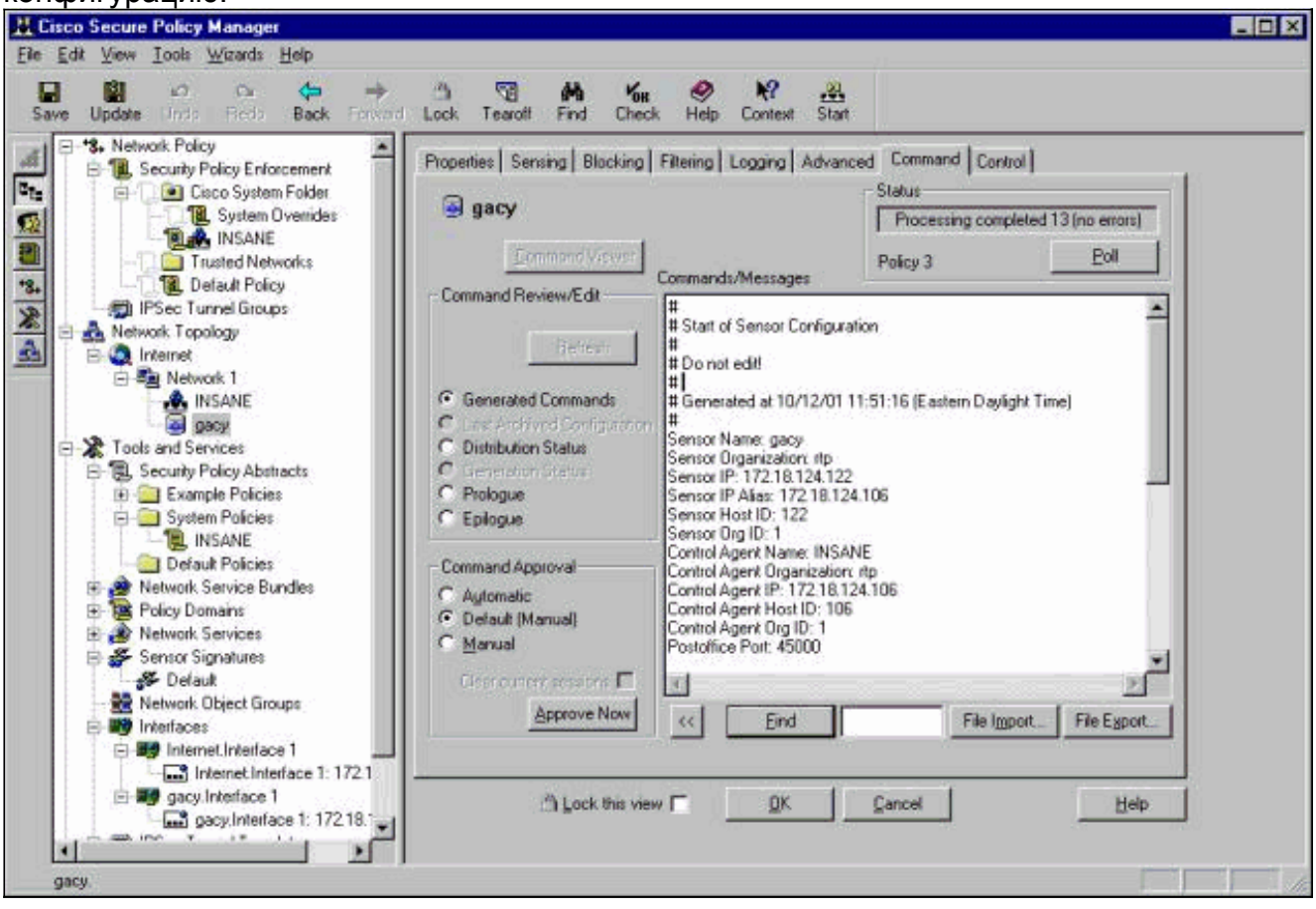
1. Выберите датчик в топологии CSPM и щелкните вкладке Sensing (Считывание).
2. Определите устройство захвата пакетов:iprb0 - для датчика IDS 4210spwr0 - для любой другой модели
   Датчика



3. **Для продолжения нажмите кнопку OK.**
4. **Щелкните значок обновления на панели меню CSPM, чтобы обновить сведения в CSPM.Примечание:** Если все подходит, экран, подобный этому, появляется. Обратите внимание на то, что красные ошибки отсутствуют. Желтые предупреждения обычно не страшны.

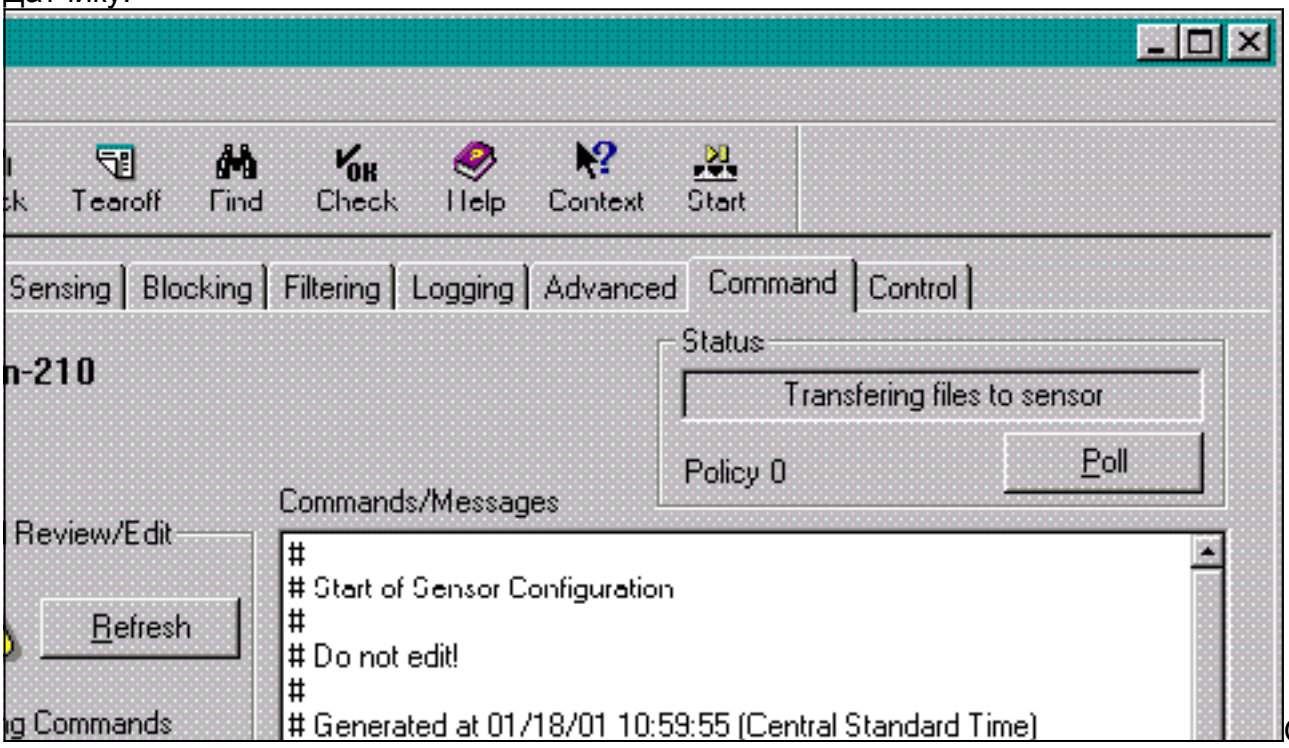


5. В сетевой топологии выберите сенсор и перейдите на вкладку Command, чтобы отправить на сенсор обновленную конфигурацию.



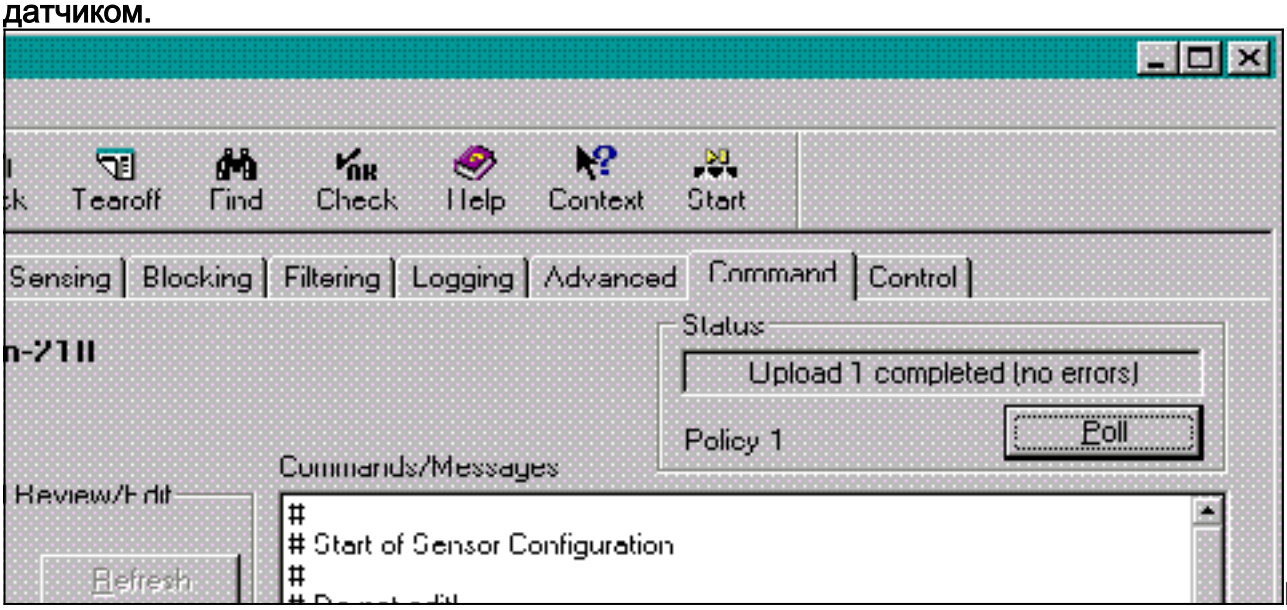
6. Нажмите кнопку **Approve Now** для передачи конфигурации к

Датчику.



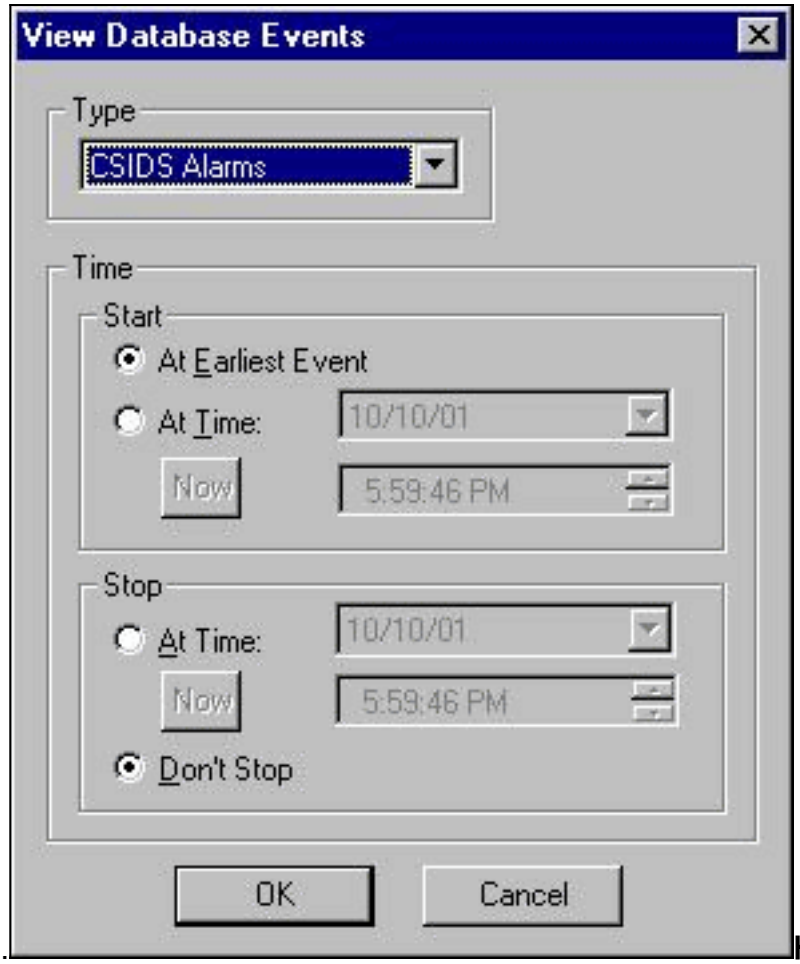
О

бласть Status отображает "Загрузку <#> завершенное" сообщение. Это указывает на допустимый и завершенный процесс передачи. Датчик теперь обновлен и должен теперь обычно работать.**Если датчик не выполняется должным образом, вернитесь к датчику и проверьте выходные данные команды nrconns, чтобы удостовериться в существовании соединения между хостом CSPM и датчиком.**

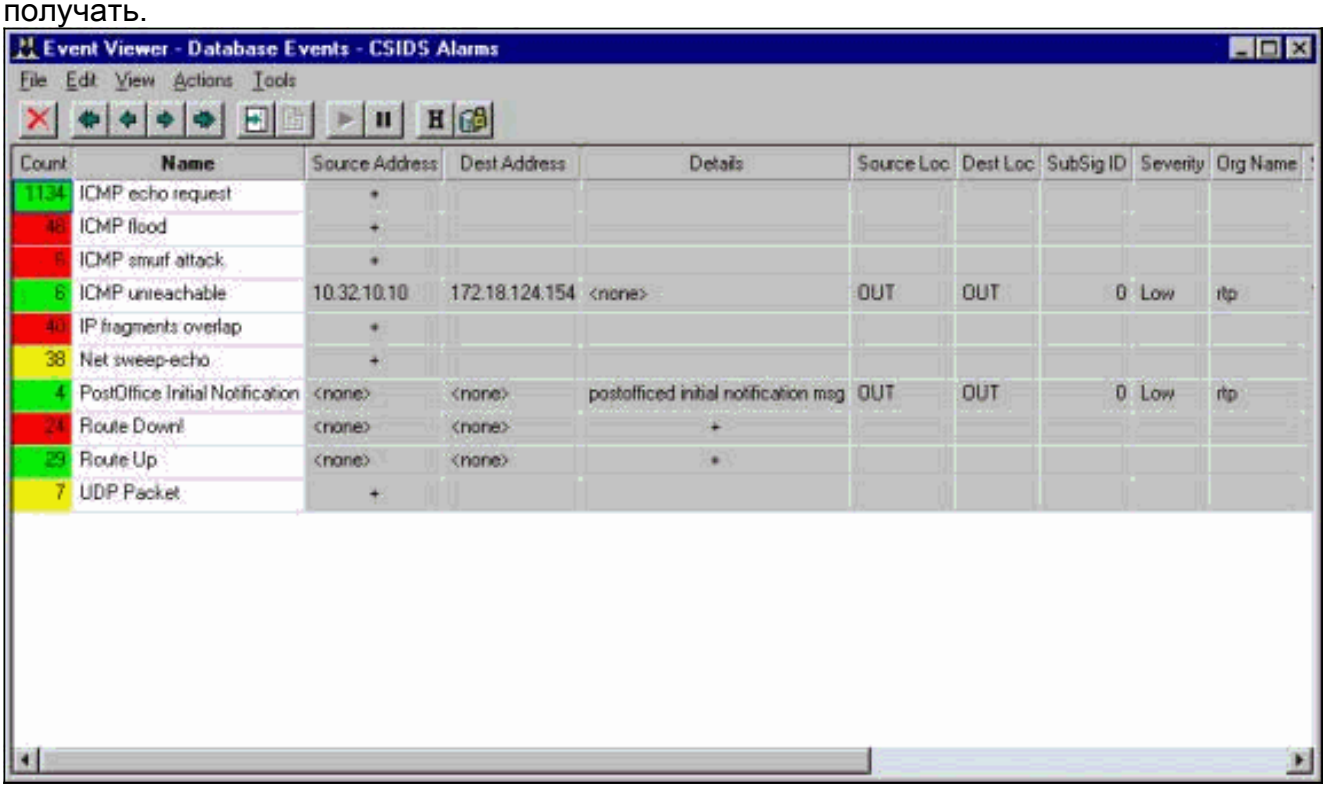


П

о завершении проверки проверьте наличие сигналов тревоги, передаваемых датчиком на хост CSPM с помощью программы просмотра событий. Для просмотра просмотра событий, из главного меню CSPM выбирают **Tools> View Sensor Events>**



Database. **Нажмите кнопку OK, чтобы отобразить окно событий базы данных.** Ваш экран будет варьироваться в зависимости от сигналов тревоги, которые можно получать.



Дополнительные сведения

- Cisco Systems – техническая поддержка и документация