Сброс TCP IPS Настройки Использование IME

Содержание

Введение

Этот документ обсуждает конфигурацию Сброса TCP Системы предотвращения вторжений (IPS) с помощью IPS Manager Express (IME). IME и Сенсоры IPS используются для управления маршрутизатором Cisco для Сброса TCP. При рассмотрении этой конфигурации помните эти элементы:

- Установите Датчик и удостоверьтесь, что Датчик работает должным образом.
- Интерфейс следует настроить так, чтобы анализ трафика применялся в маршрутизаторе за пределами интерфейса.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- Cisco IPS Manager Express 7.0
- Датчик Cisco IPS 7.0 (0.88) E3
- Маршрутизатор Cisco IOS® с Cisco IOS Software Release 12.4

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.

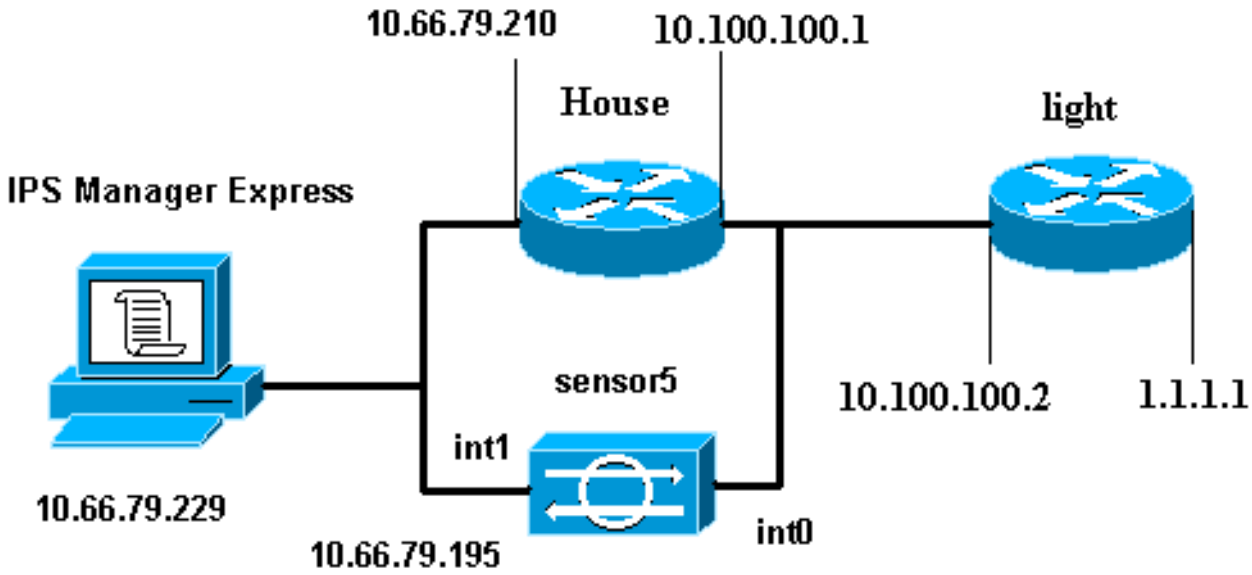
Условные обозначения

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

Настройка

Схема сети

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



Конфигурации

В данном документе используется следующая конфигурация.

- Маршрутизатор light
- Маршрутизатор house

Маршрутизатор light

```
Current configuration : 906 bytes
!
version 12.4
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 10.100.100.2 255.255.255.0
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
10.100.100.1 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 : 939 bytes
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname house ! logging queue-limit 100 enable password
cisco ! ip subnet-zero ! ! no ip cef no ip domain lookup
! ip audit notify log ip audit po max-events 100 ! ! no
voice hpi capture buffer no voice hpi capture
destination ! ! ! ! interface FastEthernet0/0 ip address
10.66.79.210 255.255.255.224 duplex auto speed auto !
interface FastEthernet0/1 ip address 10.100.100.1
255.255.255.0 duplex auto speed auto ! interface ATM1/0
no ip address shutdown no atm ilmi-keepalive ! 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 10.100.100.2 no ip http server no
ip http secure-server ! ! ! ! call rsvp-sync ! ! mgcp
profile default ! ! line con 0 exec-timeout 0 0 line aux
0 line vty 0 4 exec-timeout 0 0 password cisco login
line vty 5 15 login ! ! end
```

Запустите конфигурацию сенсора

Выполните эти шаги для начала конфигурации Датчика.

1. Если это - ваш первоначально для вхождения в Датчик, необходимо ввести **Cisco** как имя пользователя и **Cisco** как пароль.
2. По запросу системы измените свой пароль.**Примечание:** Cisco123 является словом словаря и не позволен в системе.
3. Введите **настройку** и завершите системное приглашение для устанавливания основных параметров для Датчиков.
4. Введите эти сведения:`sensor5#setup --- System Configuration Dialog --- !--- At any point you may enter a question mark '?' for help. !--- Use ctrl-c to abort the 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 Corp-IPS telnetOption enabled !--- Permit the IP address of workstation or network with IME 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
```

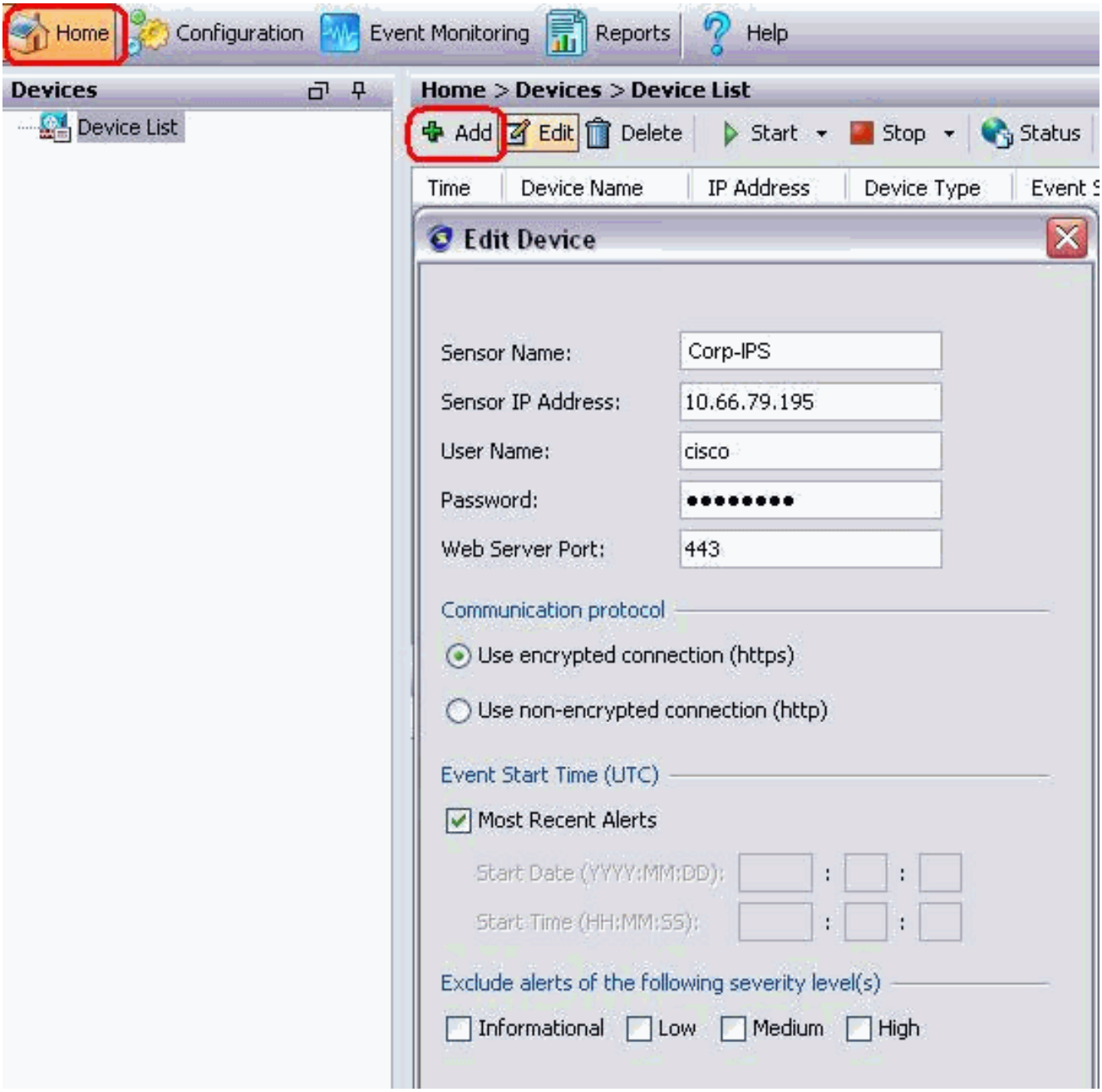
5. Сохраните конфигурацию.Может потребоваться несколько минут для Датчика для сохранения конфигурации.
```
[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.

Enter your selection[2]: 2
```

Добавьте датчик в IME

Выполните эти шаги для добавления Датчика в IME:

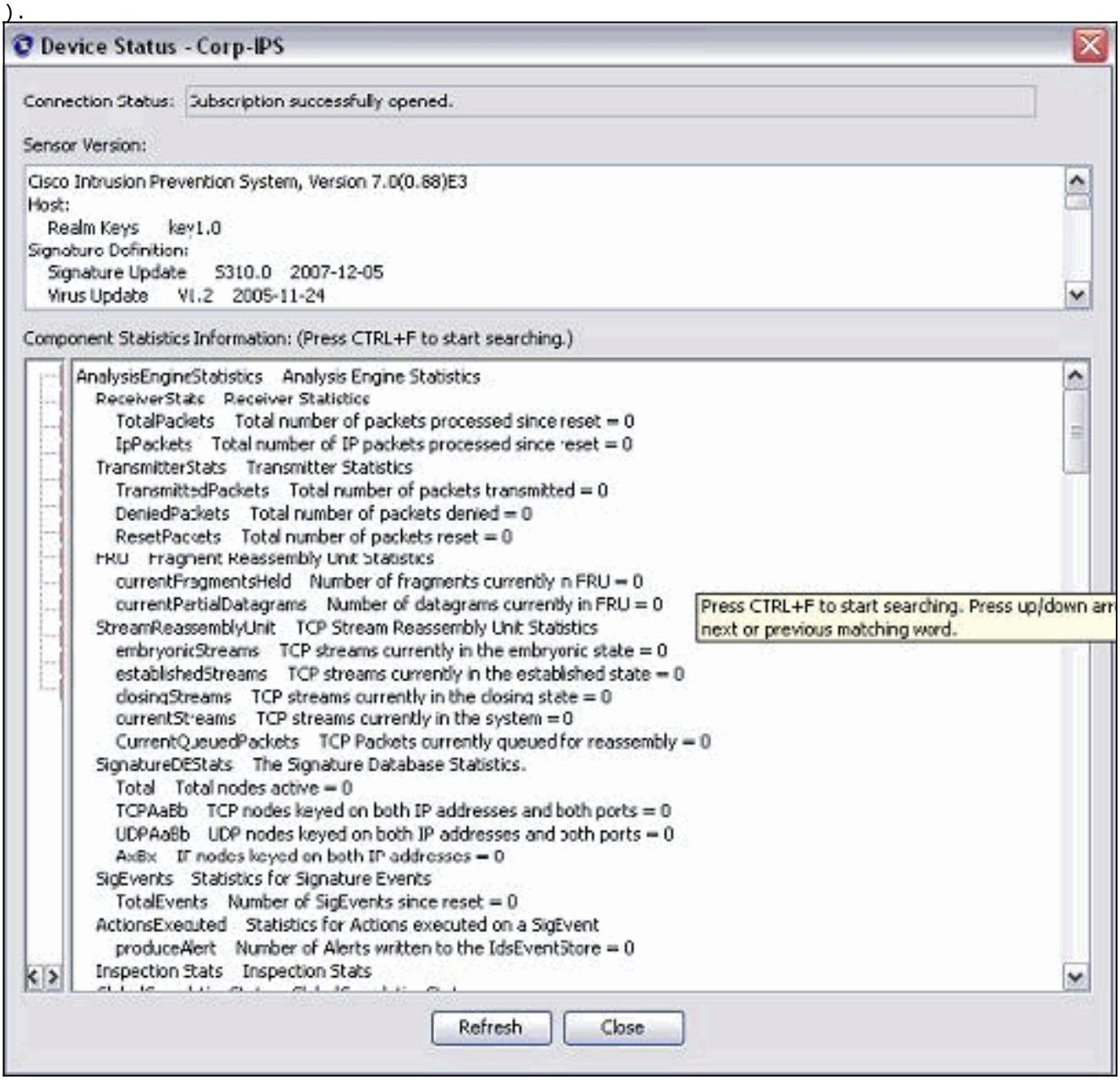
1. Перейдите к Компьютеру с операционной системой Windows, который установил IPS Manager Express, и откройте IPS Manager Express.
2. Выберите **Home>**
   Add.



3. Введите в этой информации и нажмите **OK** для завершения конфигурации.
4. Выберите **Devices> Corp-IPS**, чтобы проверить Статус сенсора и затем щелкнуть

правой кнопкой мыши для выбора **Device Status**., `"Subscription successfully opened" (`

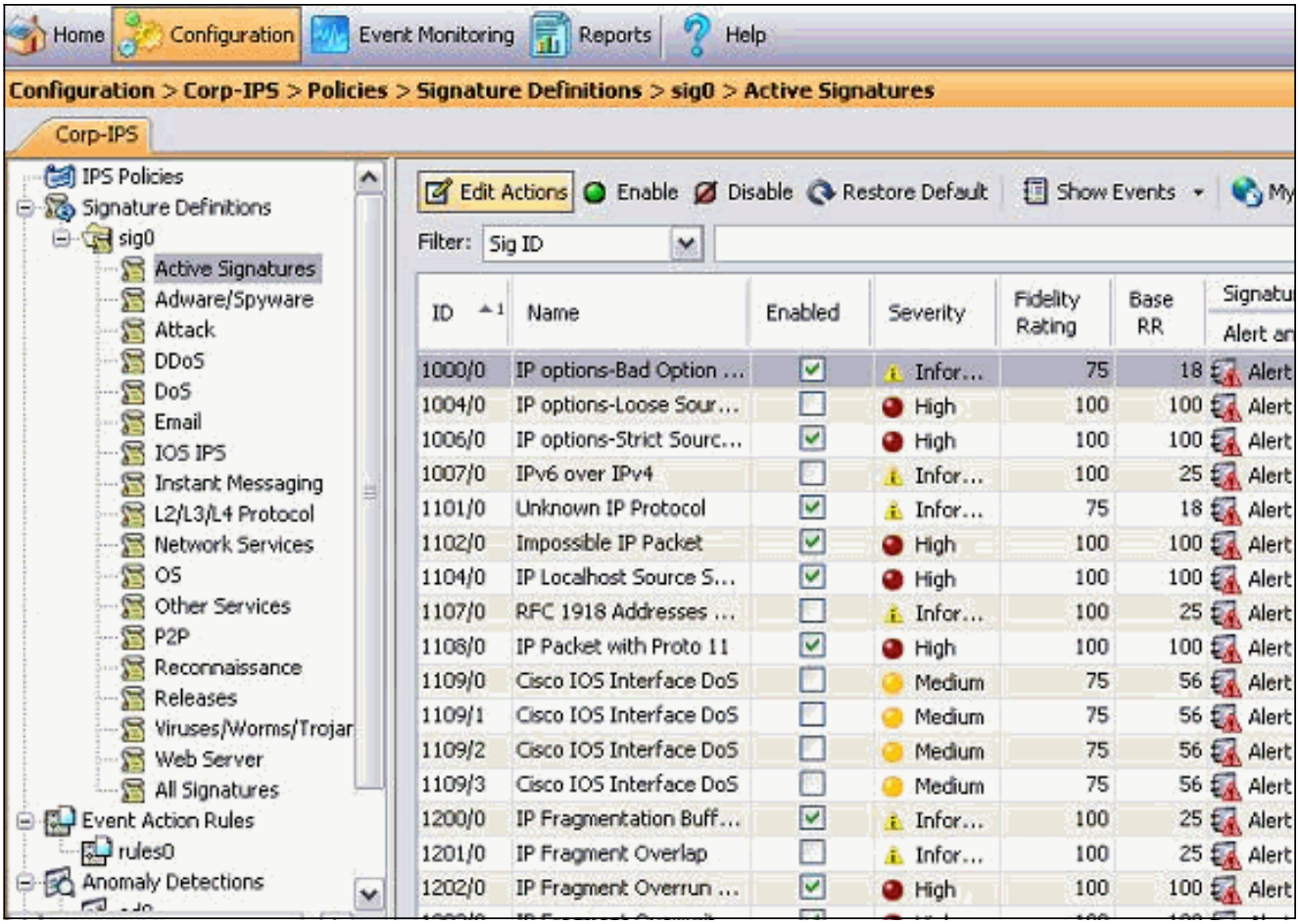
).



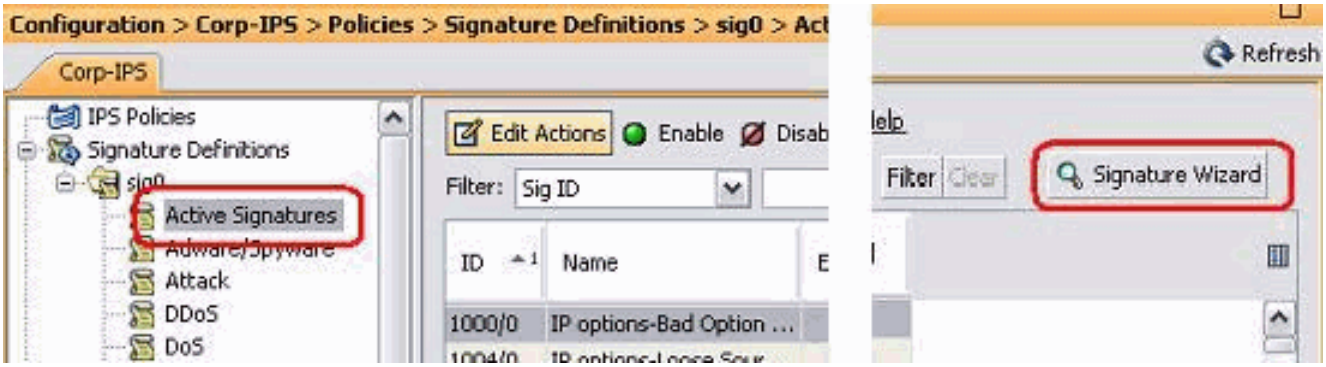
Настройте сброс TCP для маршрутизатора Cisco IOS

Выполните эти шаги для настройки Сброса TCP для маршрутизатора Cisco IOS:

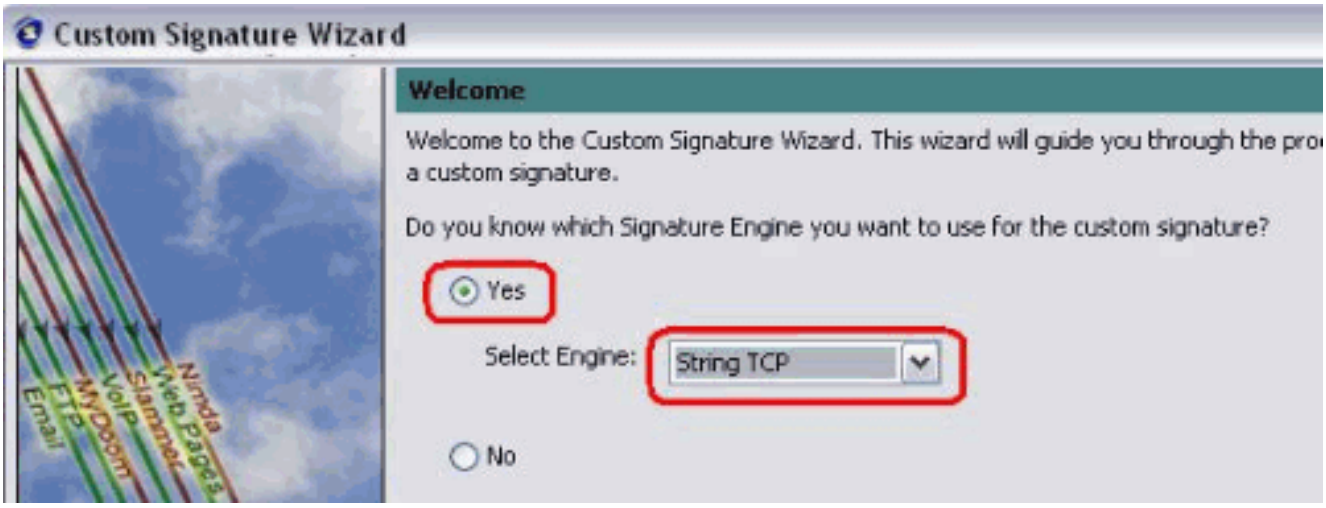
1. От ПК IME откройте свой web-браузер и перейдите **к https://10.66.79.195**.
2. Нажмите **OK** для принятия сертификата HTTPS, загруженного от Датчика.
3. **В окне Login введите cisco как имя пользователя и 123cisco123 в качестве пароля.**Этот интерфейс управления IME
появляется:



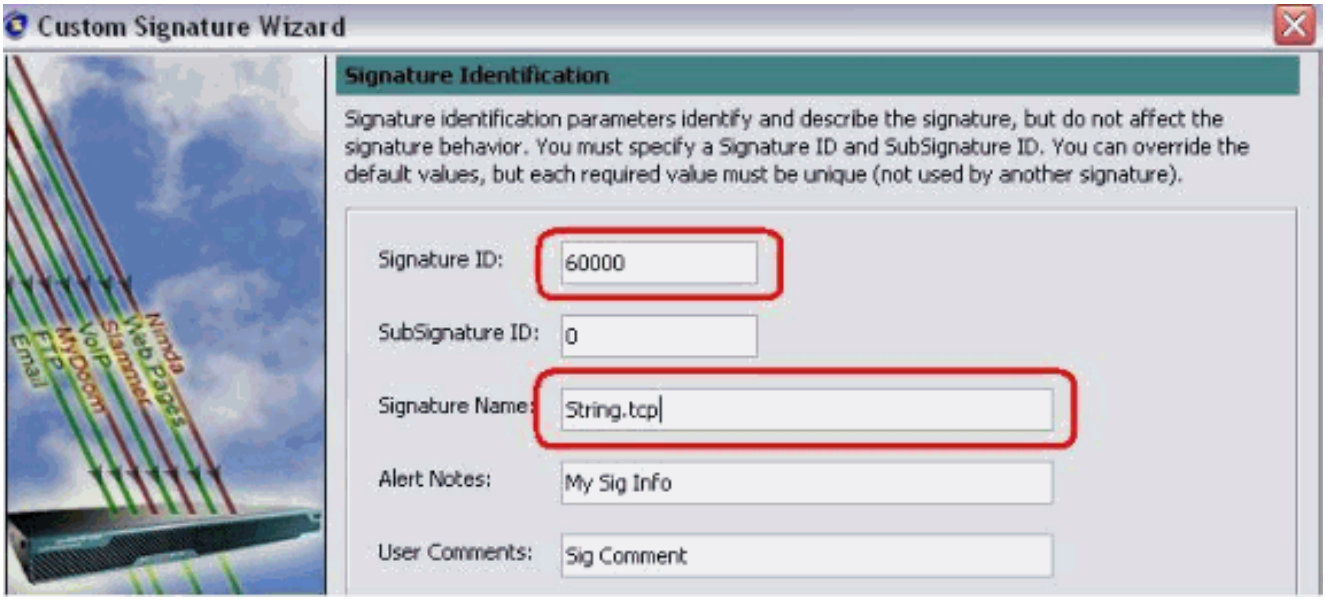
4. От Вкладки конфигурация нажмите **Active Signatures**.
5. Затем нажмите **Signature Wizard.**



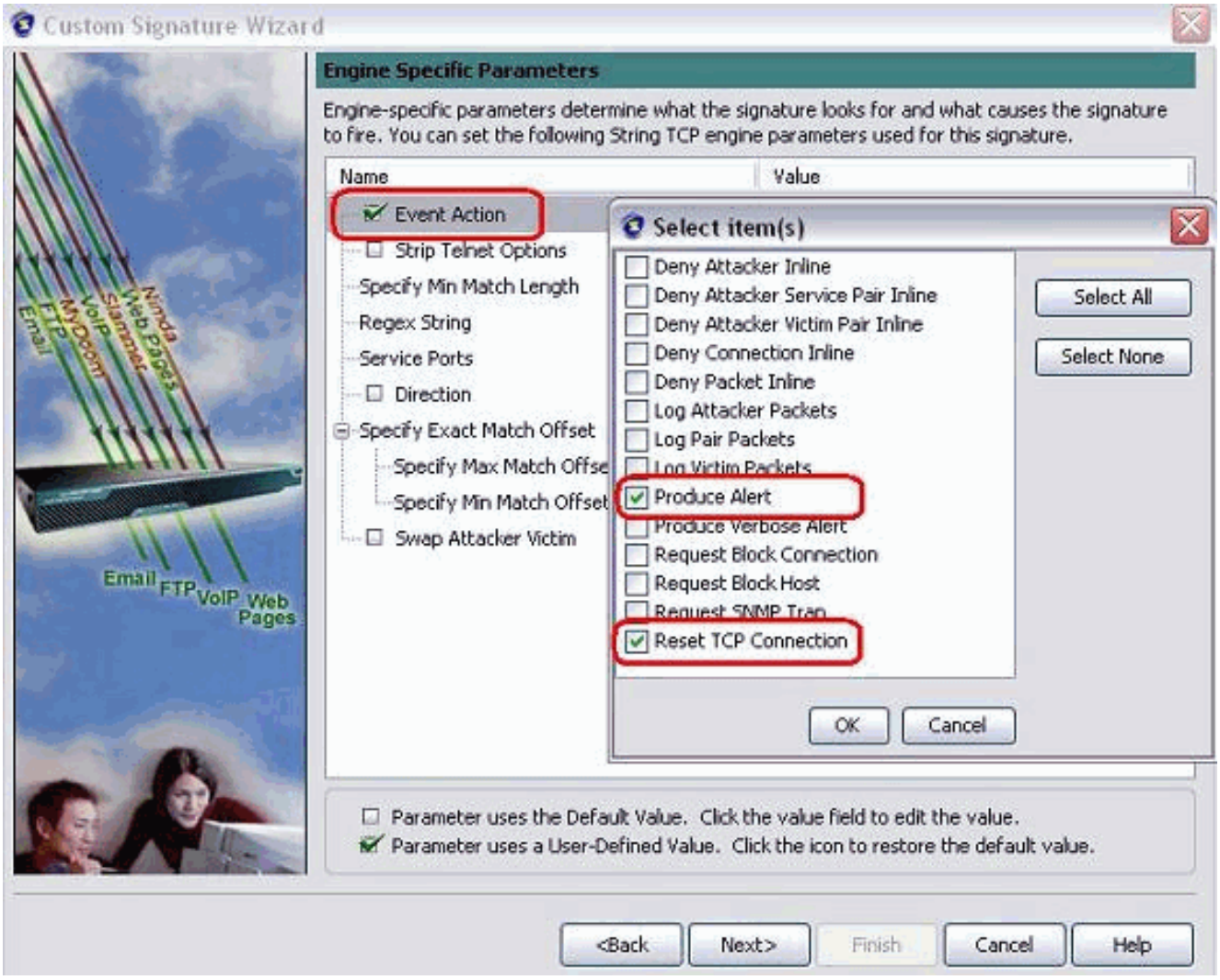
6. В мастере выберите **Yes** и выберите **String TCP** в качестве Устройства для подписи. **Нажмите кнопку Next.**



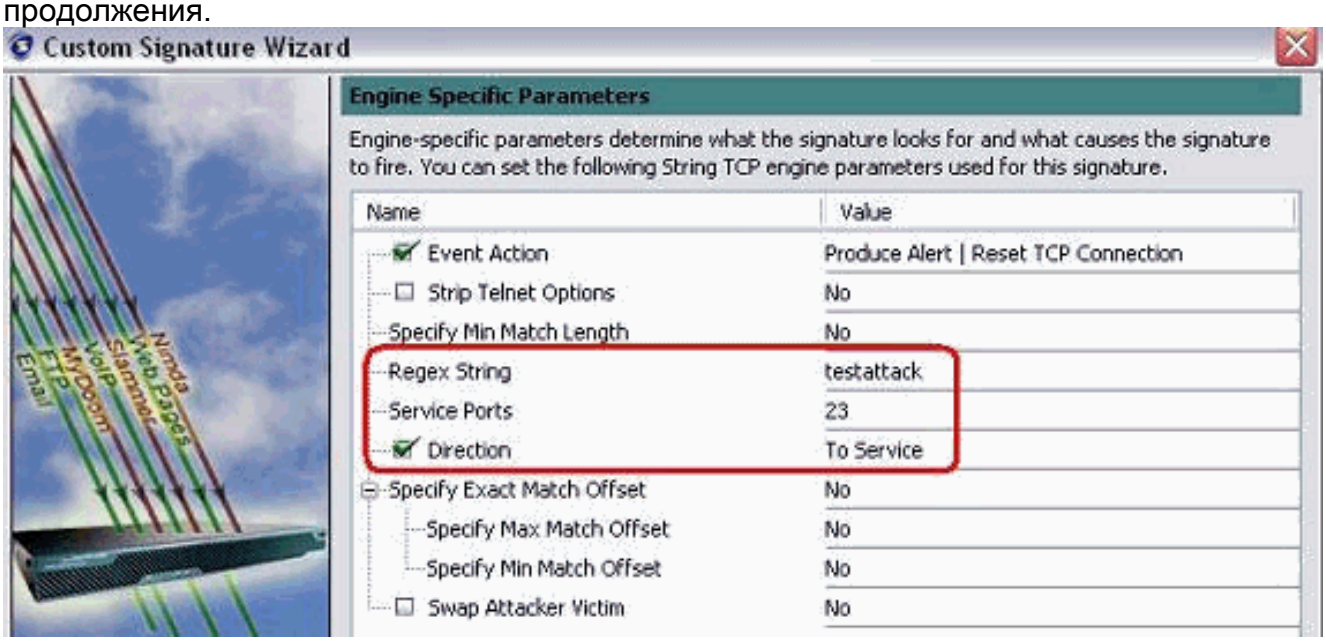
7. Можно оставить эту информацию как efdault или ввести собственный Идентификатор подписи, Название Подписи и Пользовательские Примечания. **Нажмите кнопку Next.**



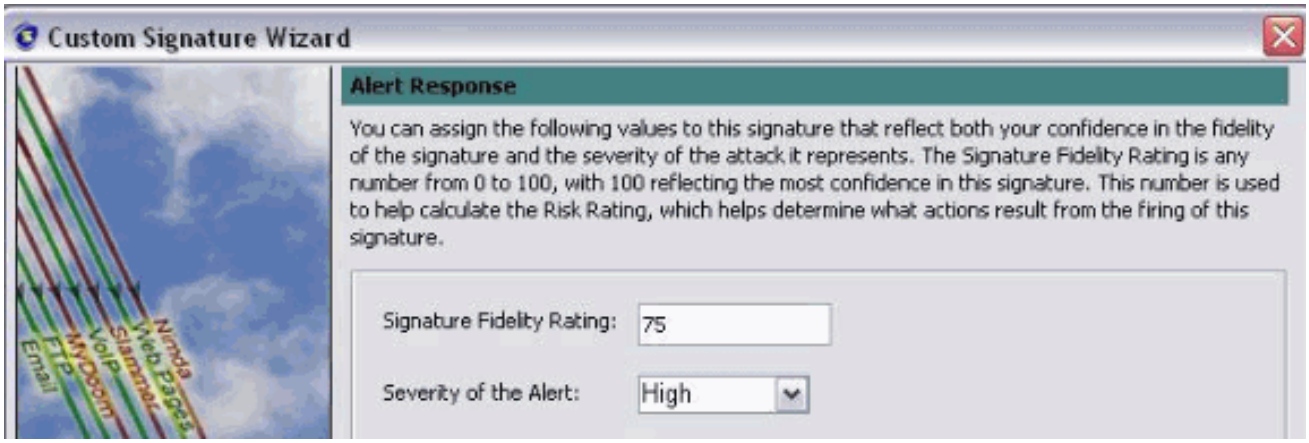
8. Выберите **Event Action** и выберите **Produce Alert** и **Reset TCP Connection**. Нажмите **OK** и затем **Затем** для продолжения.



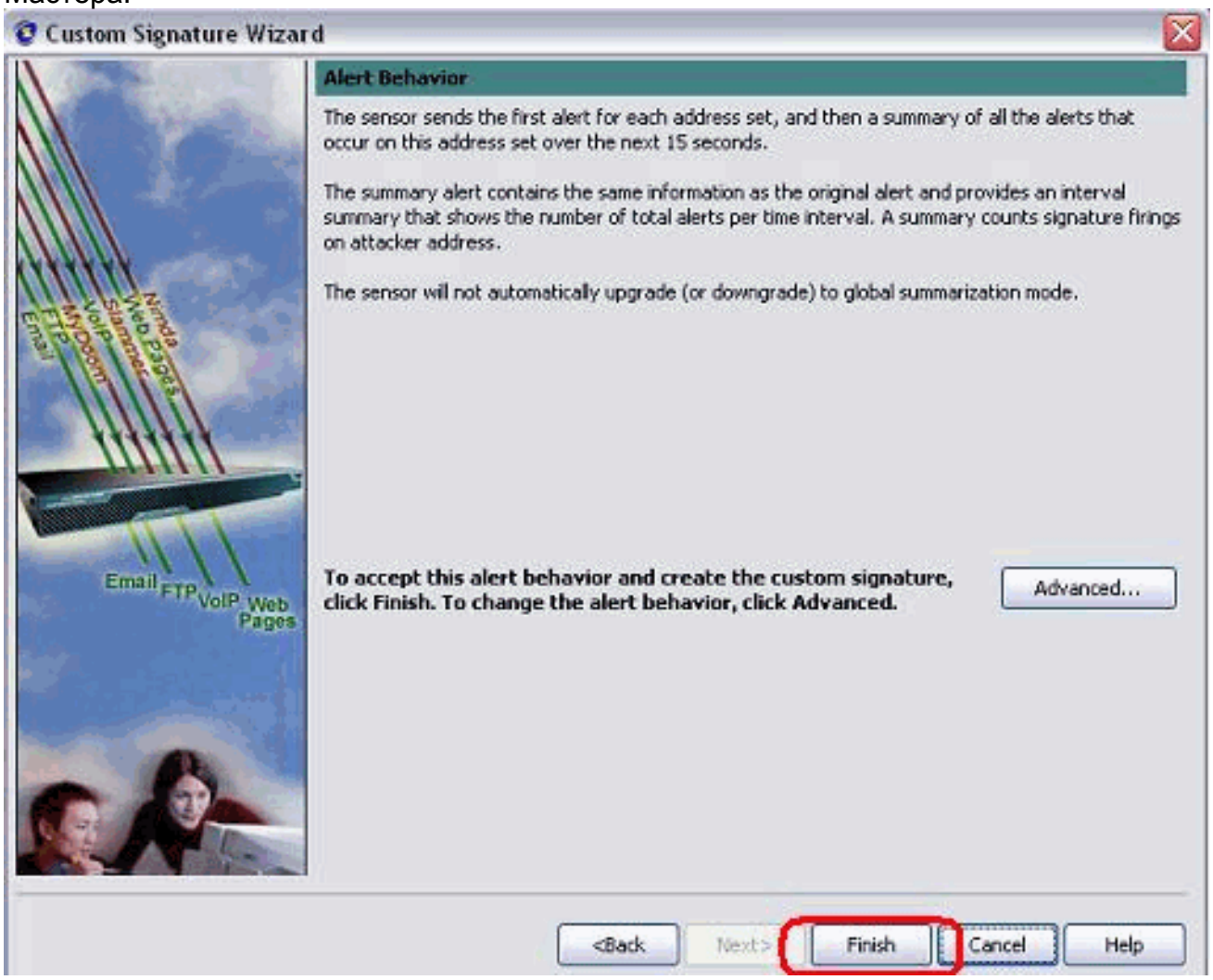
9. Введите Регулярное выражение, и `testattack` используется в данном примере. Войдите **23** для Сервисных портов, выберите **To Service** для Направления и нажмите **Next** для продолжения.



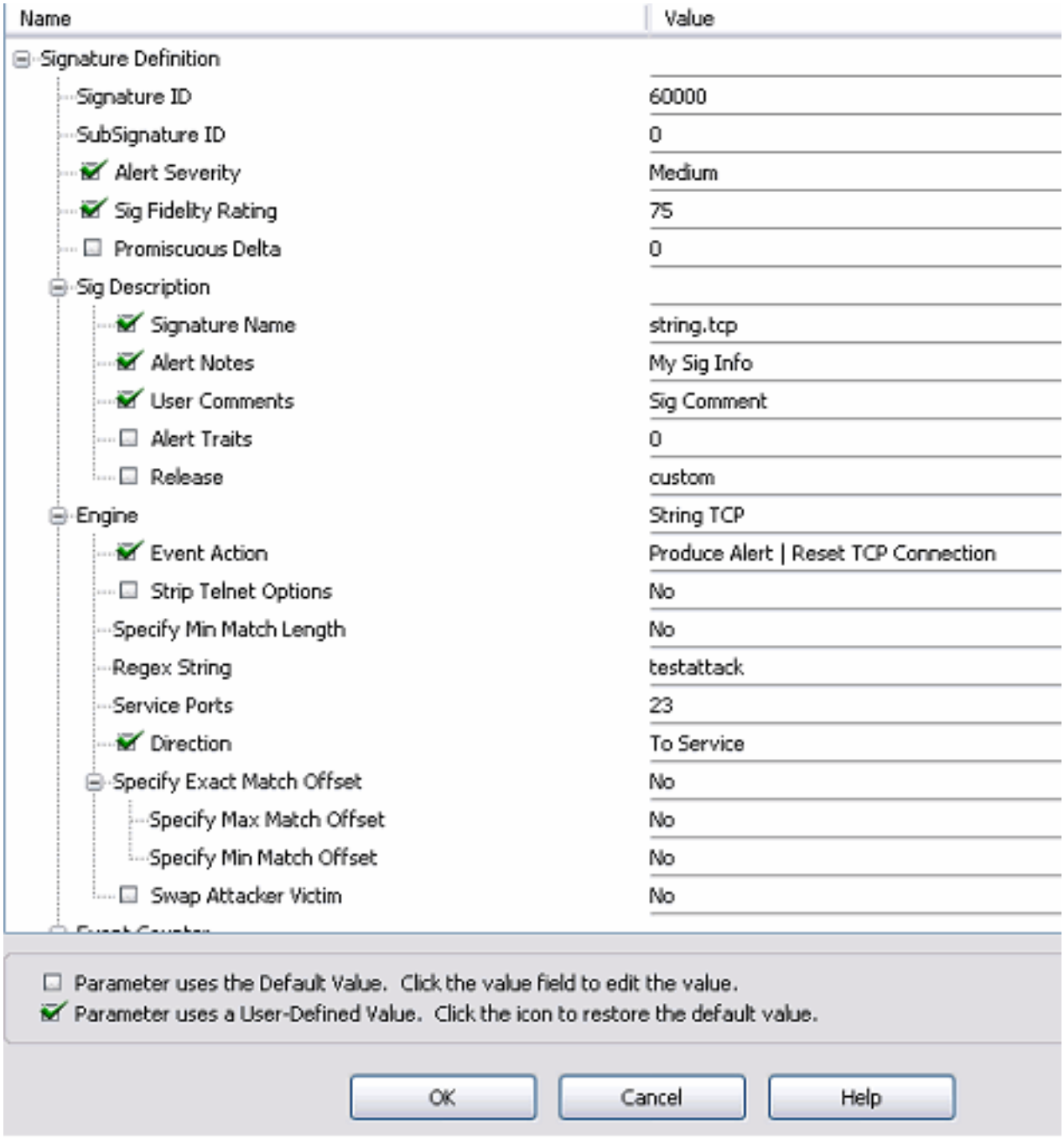
10. Можно оставить эту информацию как По умолчанию. **Нажмите кнопку Next.**



11. Нажмите **Finish** для завершения
Мастера.



12. Выберите **Configuration> sig0> Активные Подписи** для определения местоположения недавно созданной подписи **ID Сигнала** или **Названием Сигнала**. Нажмите **Edit** для просмотра
Подписи.



13. Нажмите **OK** после того, как вы подтверждаете и нажимаете кнопку **Apply** для применения подписи к Датчику.

Проверка

Пойдите в наступление и сброс TCP

Выполните эти шаги, чтобы пойти в наступление и Сброс TCP:

1. Прежде чем вы пойдете в наступление, перейдете **к IME**, выберете **Event Monitoring> Dropped Attacks View** и выберете датчик справа.
2. **C Router Light при помощи Telnet подключитесь к Router House, а потом введите testattack.**Соответствие или **<пространство>** или **<входит>** для сброса сеанса Telnet.`light#telnet 10.100.100.1 Trying 10.100.100.1 ... Open User Access Verification Password: house>en Password: house#testattack [Connection to 10.100.100.1 closed by foreign host] !--- Telnet session has been reset due to the !--- signature "String.tcp" triggered.`

3. От Информационной панели Просмотра событий IPS появляется Красный сигнал, как только идут в
наступление.

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Советы

Используйте эти советы по устранению проблем:

- Избегание работает из порта командования и управления для перепрограммирования списков контроля доступа маршрутизатора (ACL). Сброс TCP передается от **интерфейса анализатора** Датчика. Когда вы **set span** в коммутаторе, используйте **set span <src_mod/src_port>** команда **<dest_mod/dest_port>** с обоими входящими пакетами, включенными как показано здесь.`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`** `Multicast : enabled`
- Если Сброс TCP работает, проверьте, инициирован ли сигнал тревоги для Сброса TCP типа действия. Если сигнал тревоги появляется, проверьте, что тип подписи установлен в сброс TCP.Вход в систему с помощью учетной записи сервиса su, чтобы базироваться и выполнить эту команду. Эта команда предполагает, что интерфейс считывания установлен в eth0.`[root@sensor1 root]#`**`tcpdump -i eth0 -n`** **Примечание:** Сброс tcp сто передается жертве/цели тогда, сто передаются атакующему/клиенту.Пример выходных данных:

```
03:06:00.598777 64.104.209.205.1409 >
 10.66.79.38.telnet: R 107:107(0) ack 72 win 0
03:06:00.598794 64.104.209.205.1409 >
 10.66.79.38.telnet: R 108:108(0) ack 72 win 0

03:06:00.599360 10.66.79.38.telnet >
 64.104.209.205.1409: R 72:72(0) ack 46 win 0
03:06:00.599377 10.66.79.38.telnet >
 64.104.209.205.1409: R 73:73(0) ack 46 win 0
```

Дополнительные сведения

- Страница технической поддержки предотвращения вторжений Cisco Secure
- Документация для системы предотвращения вторжений Cisco Secure
- Cisco Systems – техническая поддержка и документация