Блокирование IPS Настройки Использование IME

Содержание

Введение

Этот документ обсуждает конфигурацию Системы предотвращения вторжений (IPS), блокирующейся с использованием IPS Manager Express (IME). IME и Сенсоры IPS используются для управления маршрутизатором Cisco для блокирования. Помните эти элементы, когда вы рассмотрите эту конфигурацию:

- 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.

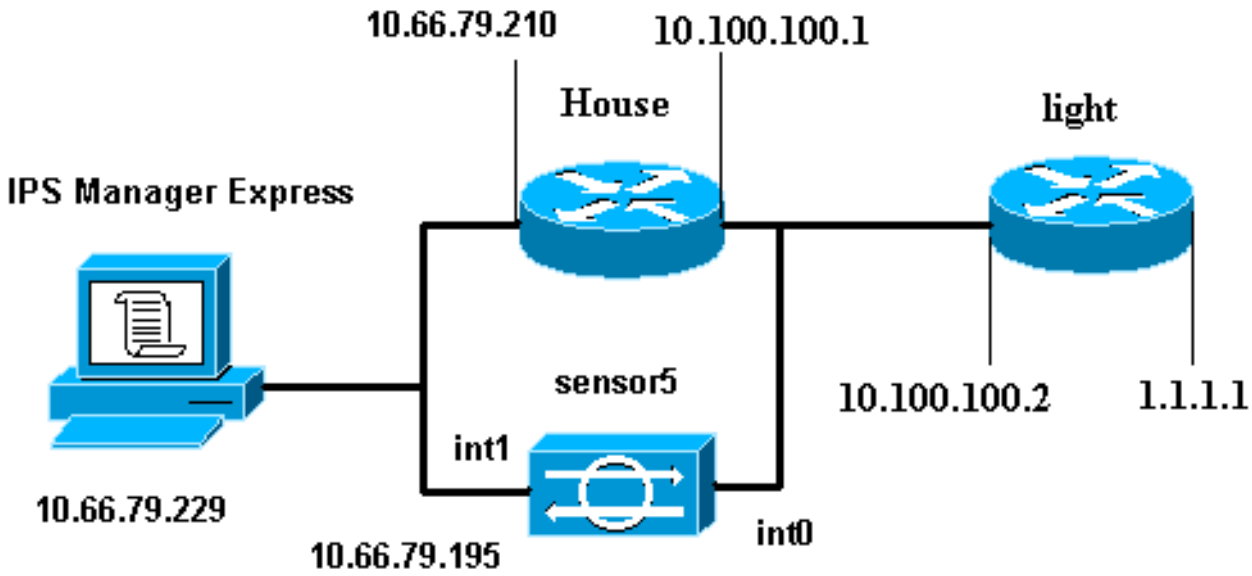
Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Настройка

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 12.4
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 ip access-group IDS_FastEthernet0/1_in_0
in !--- After you configure blocking, !--- IDS Sensor
inserts this line. 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 ! ! ip access-list extended
IDS_FastEthernet0/1_in_0 permit ip host 10.66.79.195 any
permit ip any any !--- After you configure blocking, !--
- IDS Sensor inserts this line. ! 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. **При первом входе в Sensor нужно ввести cisco в качестве имени пользователя и в качестве пароля.**
2. По запросу системы измените свой пароль.**Примечание:** Cisco123 является словом словаря и не позволен в системе.
3. **Введите "setup" и следуйте указаниям для настройки основных параметров сенсоров.**

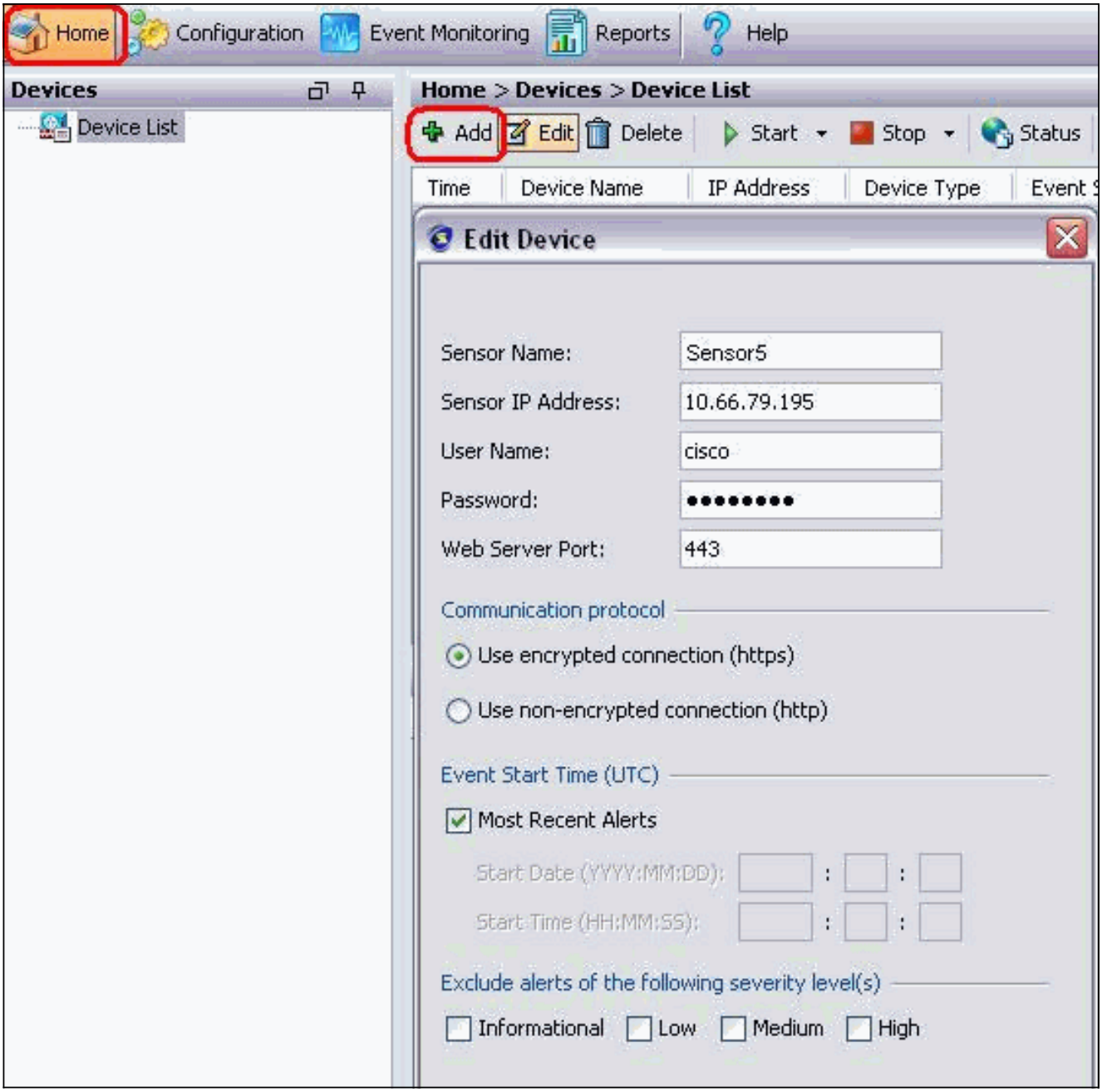
4. Введите эти сведения:`sensor5#`**`setup`** `--- System Configuration Dialog --- !--- At any point you may enter a question mark '`**`?`**`' for help. !--- Use `**`ctrl-c`**` to abort the configuration dialog at any prompt. !--- Default settings are in square brackets '[]'. Current time: Thu Oct 22 21:19:51 2009 Setup Configuration last modified: Enter host name[sensor]: Enter IP interface`**`[10.66.79.195/24,10.66.79.193]`**`: Modify current access list?[no]: Current access list entries: !--- permit the ip address of workstation or network with IME Permit:`**`10.66.79.0/24`** `Permit: Modify system clock settings?[no]: Modify summer time settings?[no]: Use USA SummerTime Defaults?[yes]: Recurring, Date or Disable?[Recurring]: Start Month[march]: Start Week[second]: Start Day[sunday]: Start Time[02:00:00]: End Month[november]: End Week[first]: End Day[sunday]: End Time[02:00:00]: DST Zone[]: Offset[60]: Modify system timezone?[no]: Timezone[UTC]: UTC Offset[0]: Use NTP?[no]: yes NTP Server IP Address[]: Use NTP Authentication?[no]: yes NTP Key ID[]: 1 NTP Key Value[]: 8675309`
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`**

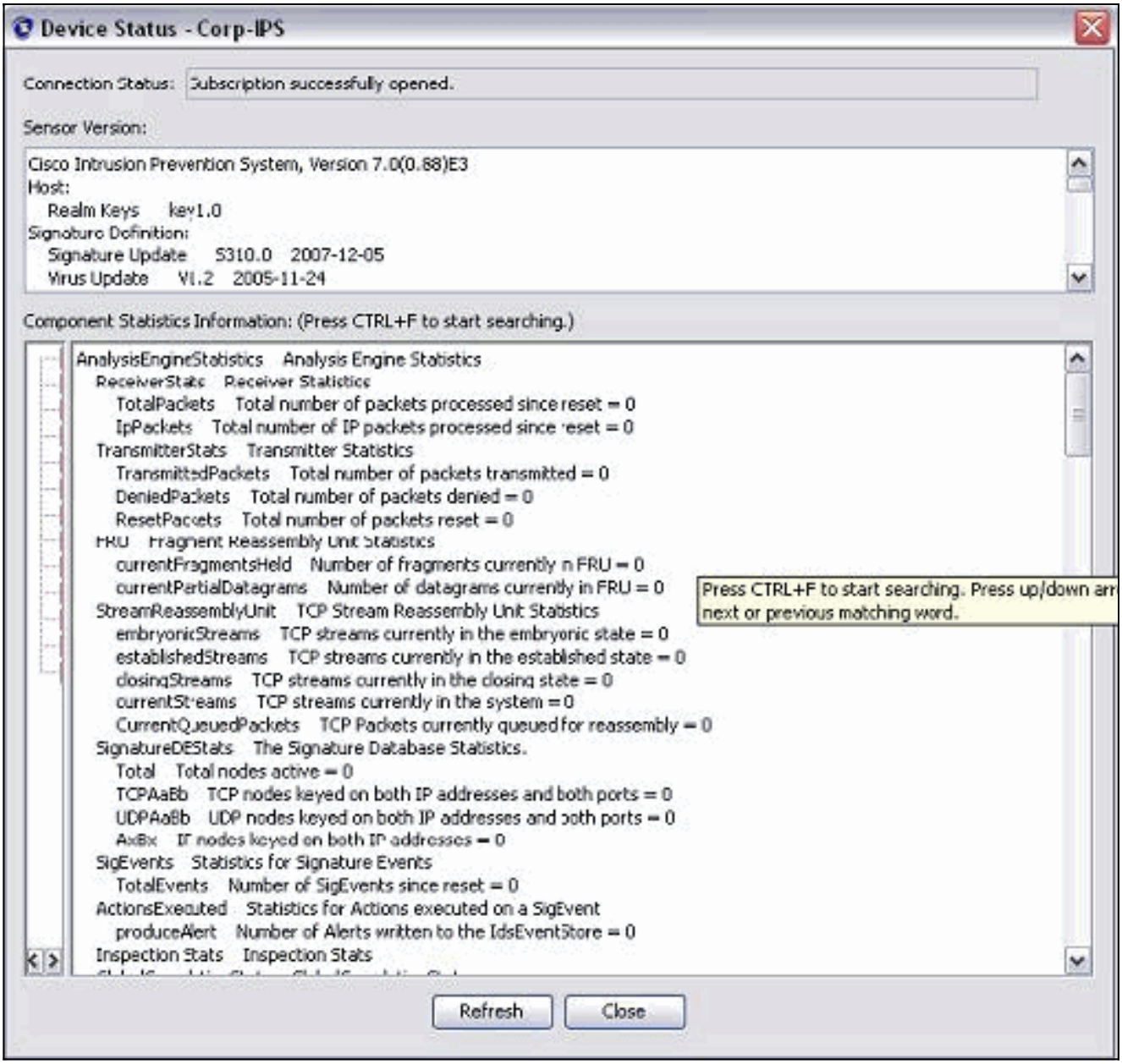
Добавьте датчик в IME

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.



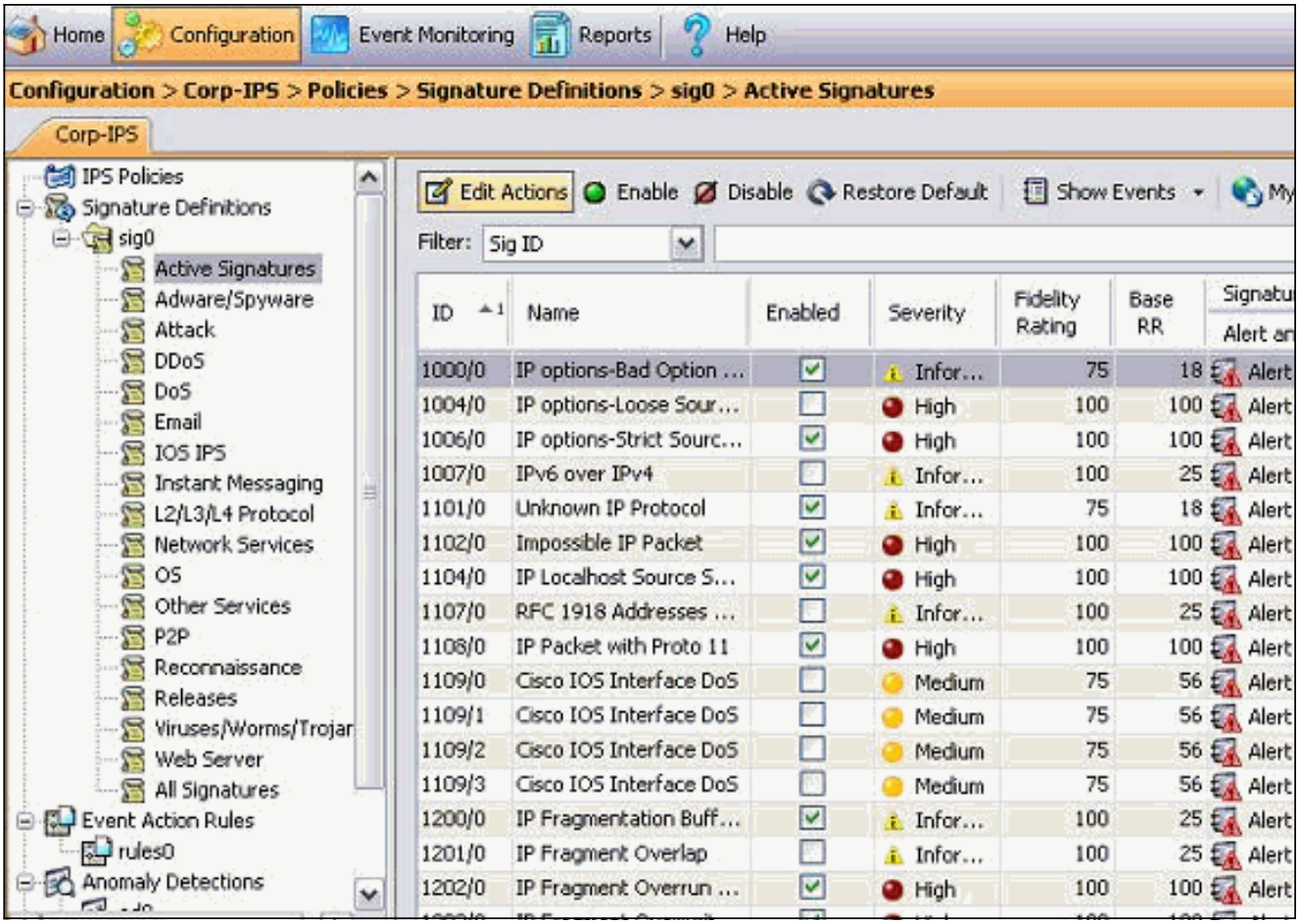
4. Выберите **Devices> sensor5**, чтобы проверить Статус сенсора и затем щелкнуть правой кнопкой мыши для выбора **Status**.Удостоверьтесь, что вы видите *Подписку, успешно открытую.*
сообщение.



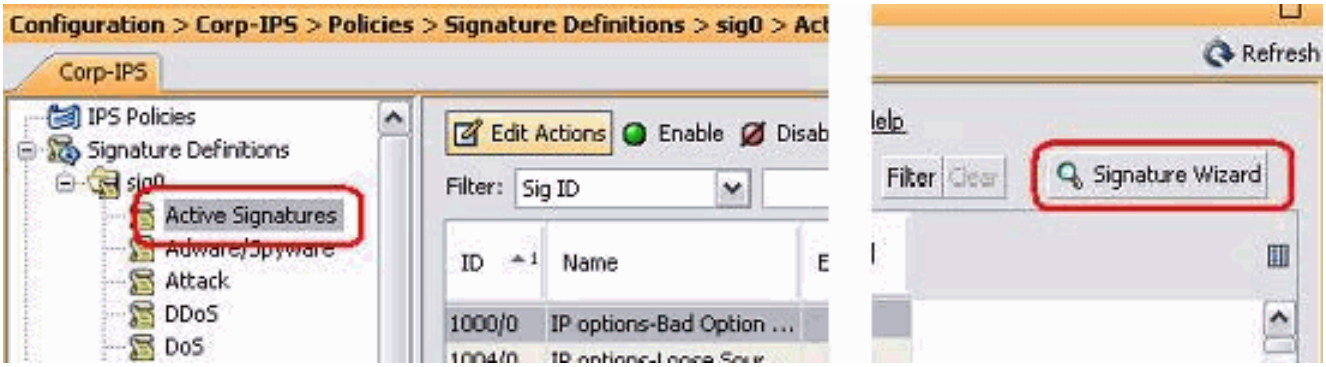
Настройте блокирование для маршрутизатора Cisco IOS

Выполните эти шаги для настройки блокирования для Cisco IOS route:.

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:

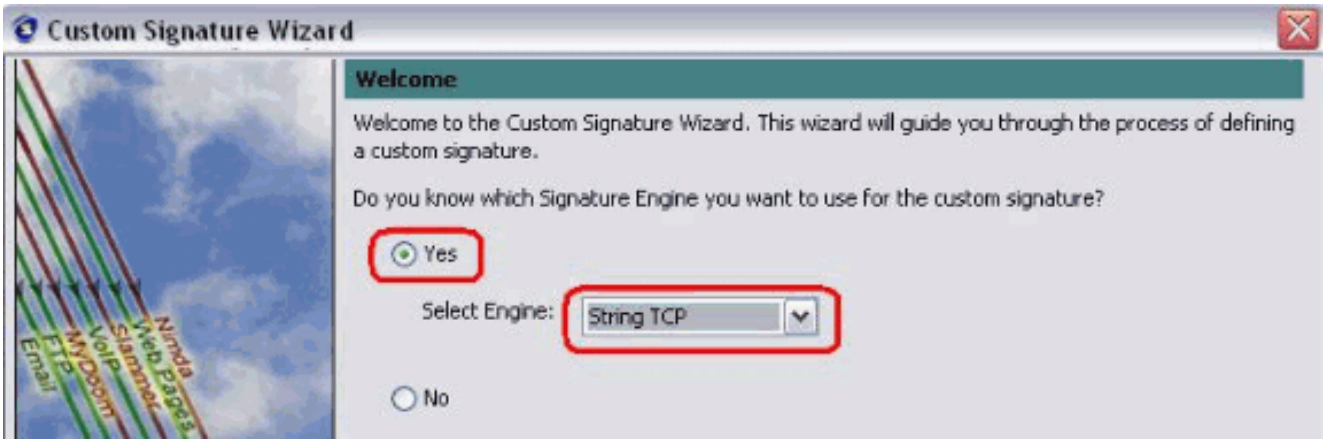


4. От Вкладки конфигурация нажмите **Active Signatures**.
5. Затем нажмите **Signature Wizard**.

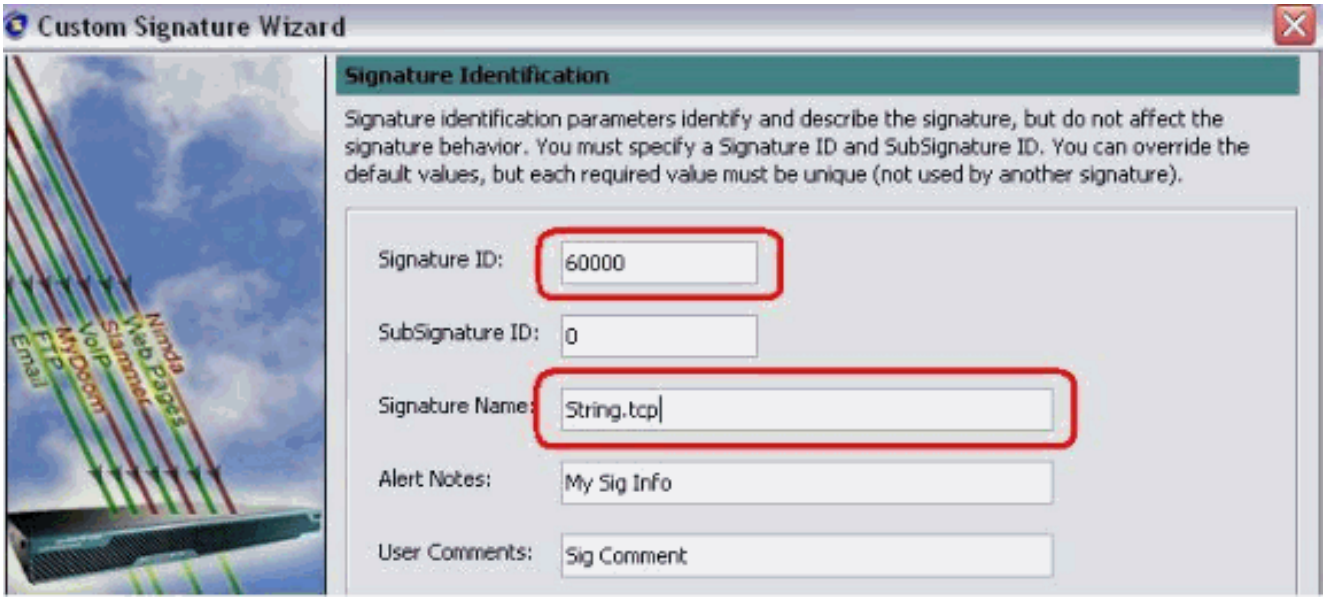


Примечание: Предыдущий снимок экрана был вырезан в две части из-за ограничения длины.

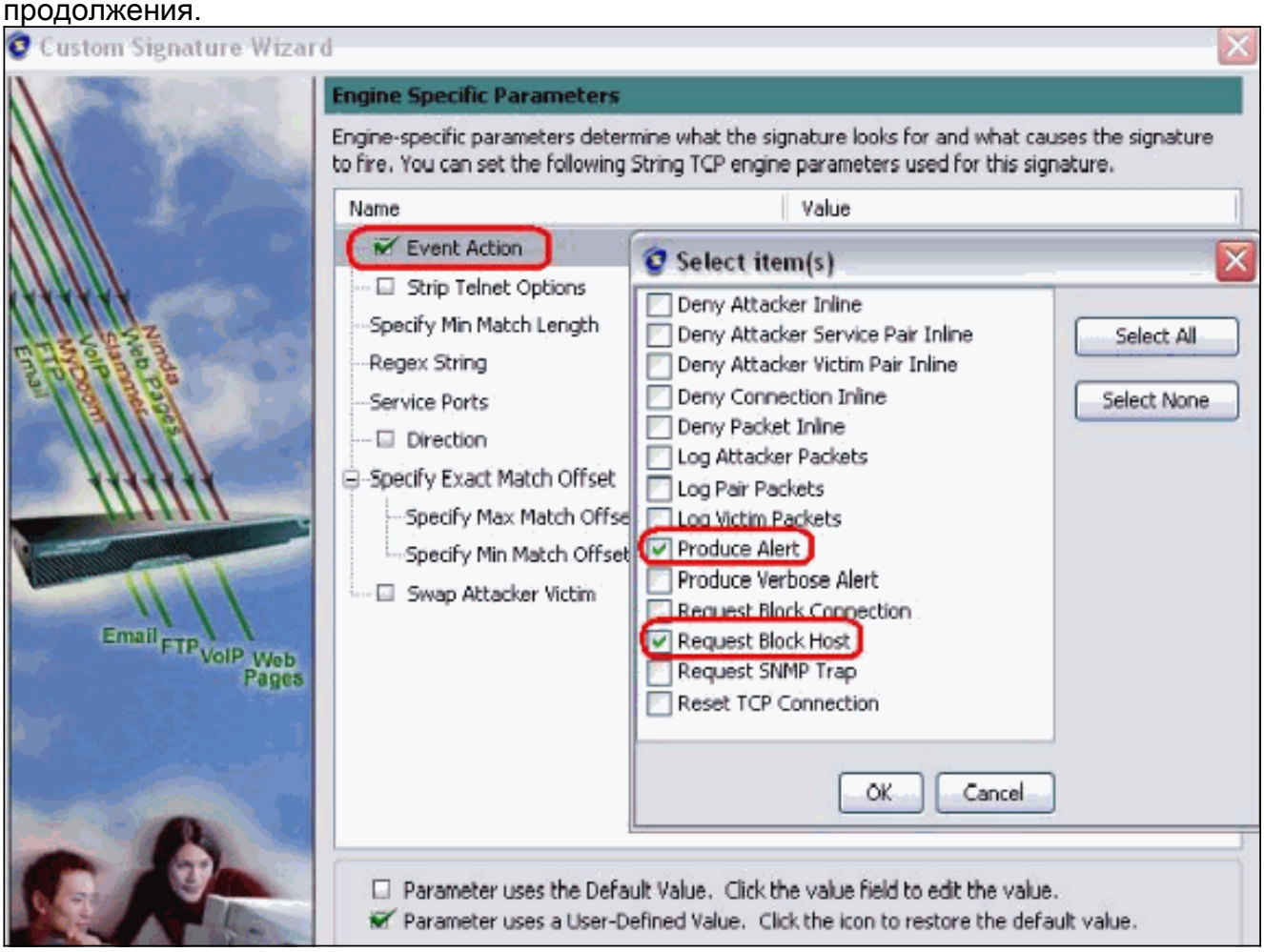
6. Выберите **Yes** и **String TCP** как Устройство для подписи. **Нажмите кнопку Next.**



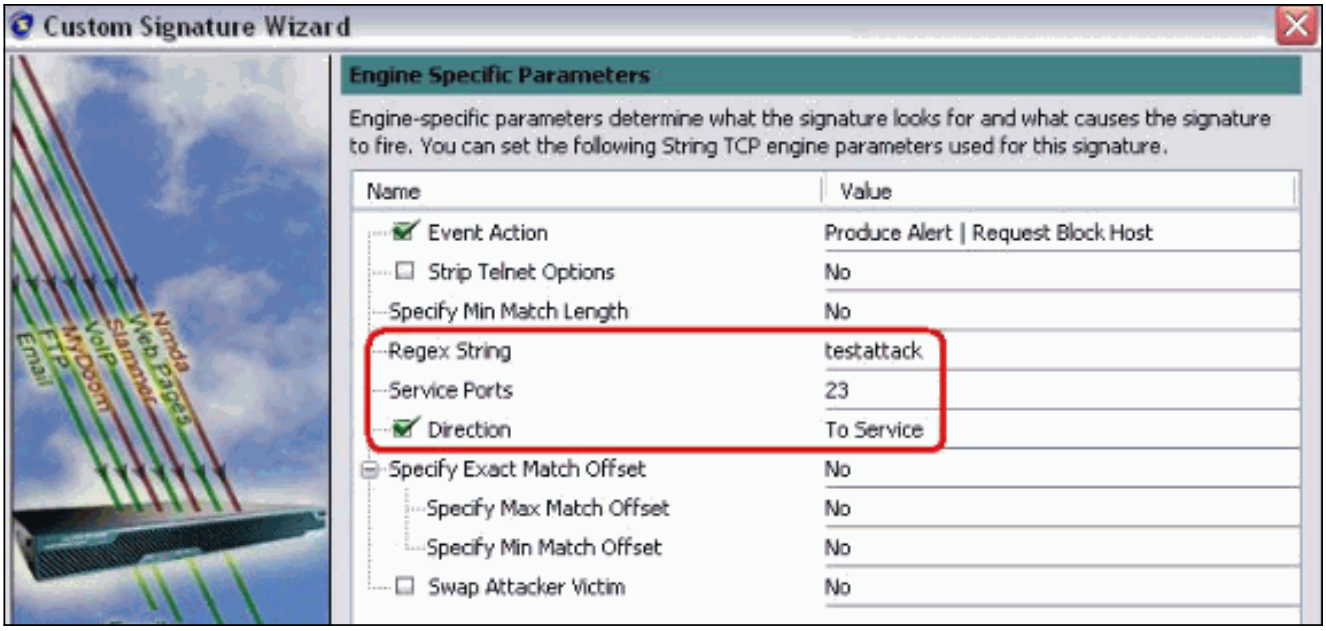
7. Можно оставить эту информацию как По умолчанию или ввести собственный Идентификатор подписи, Название Подписи и Пользовательские Примечания. **Нажмите кнопку Next.**



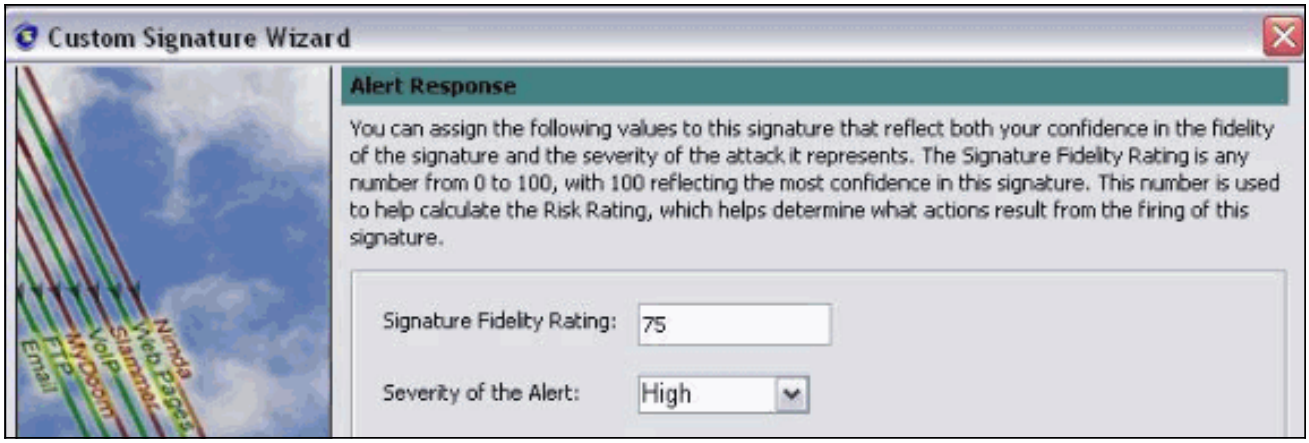
8. Выберите **Event Action** и выберите **Produce Alert** и **Request Block Host**. Нажмите **Next** для продолжения.



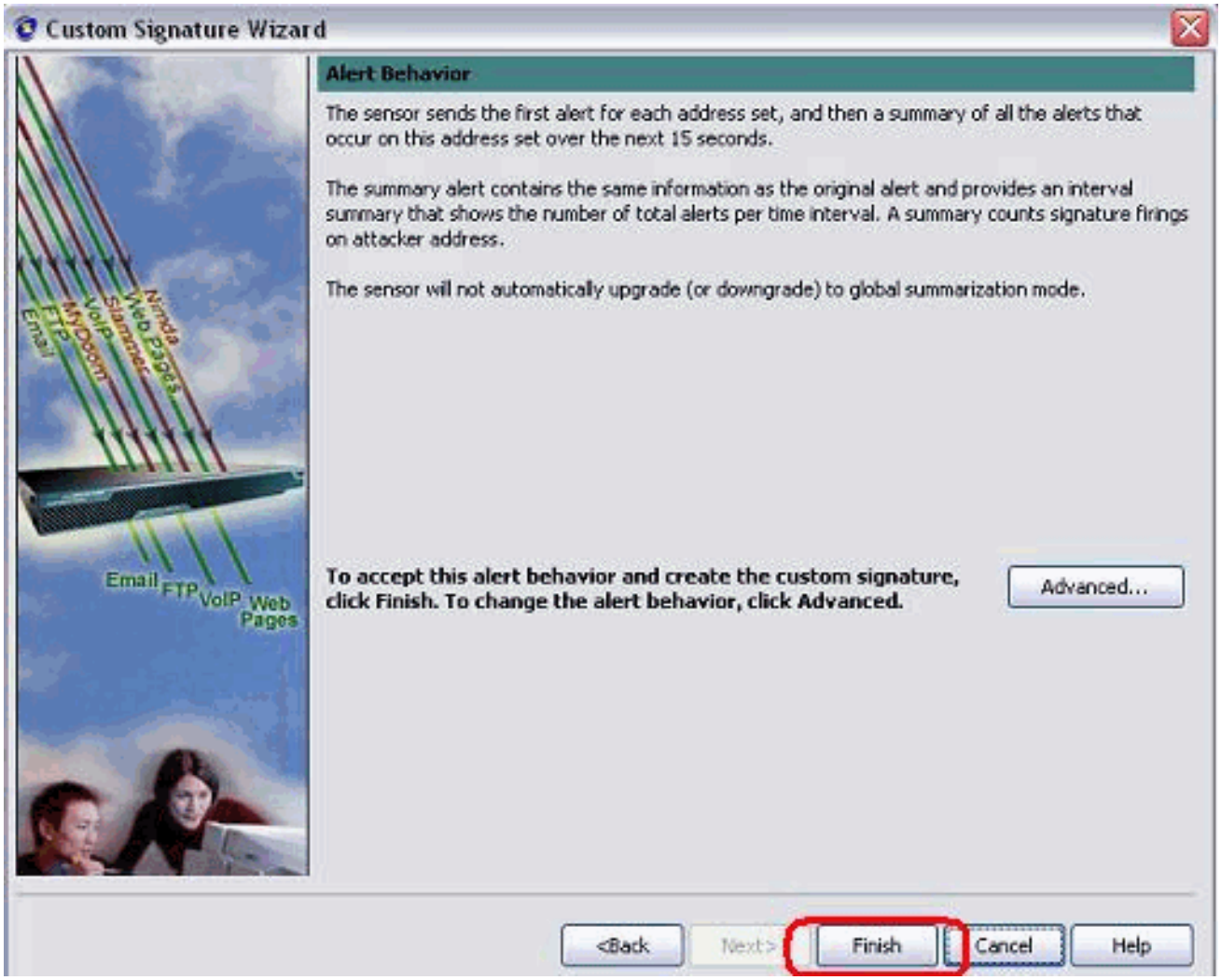
9. Введите Регулярное выражение, которое в данном примере является *testattack*, войдите **23** для Сервисных портов, выберите **To Service** для Направления и нажмите **Next** для продолжения.



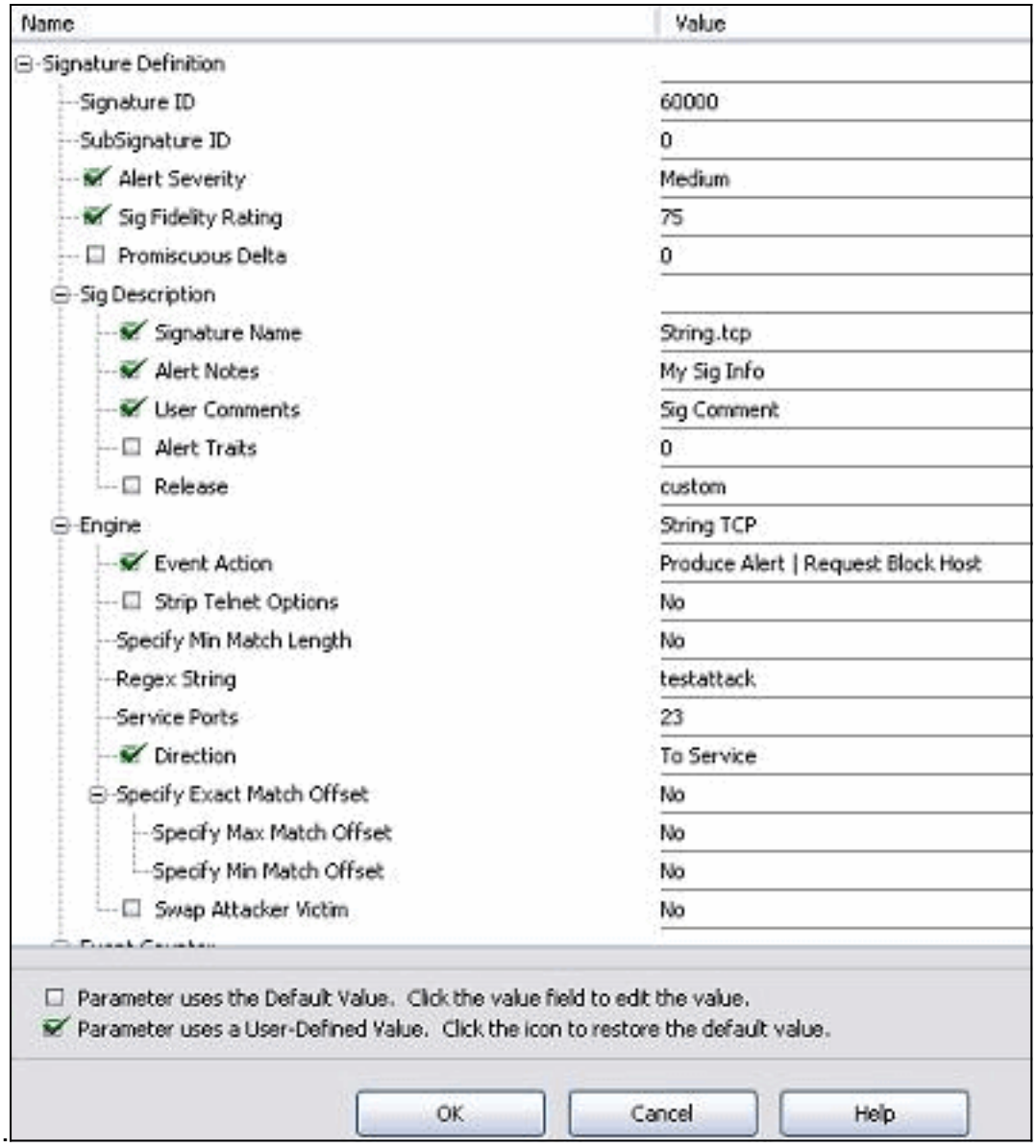
10. Можно оставить эту информацию как По умолчанию. **Нажмите кнопку Next.**



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

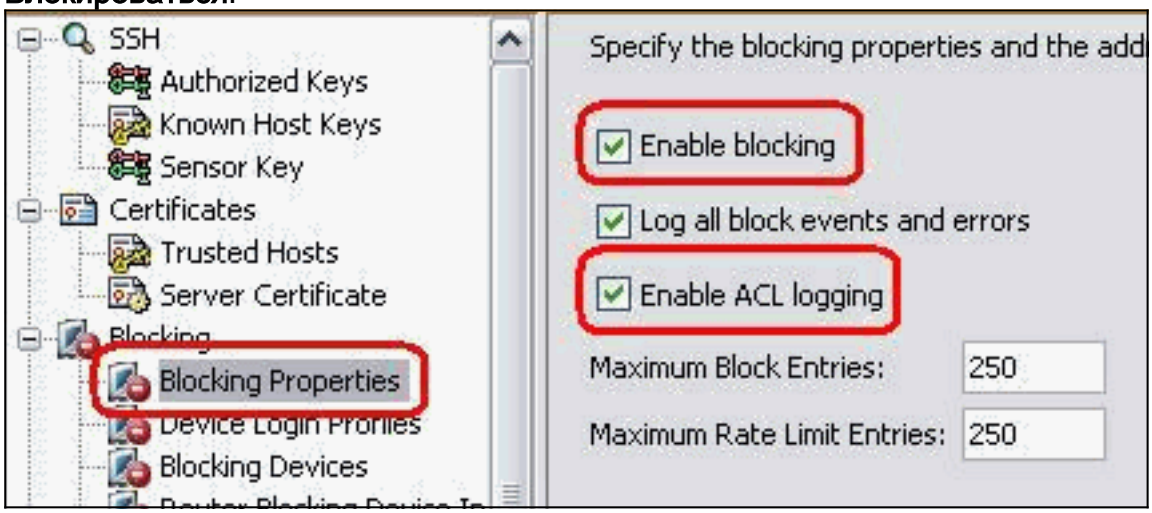


12. Выберите **Configuration> sig0>, Активные Подписи** в заказе определяют местоположение недавно созданной подписи **ID Сигнала** или **Названием Сигнала**. Нажмите **Edit** для просмотра



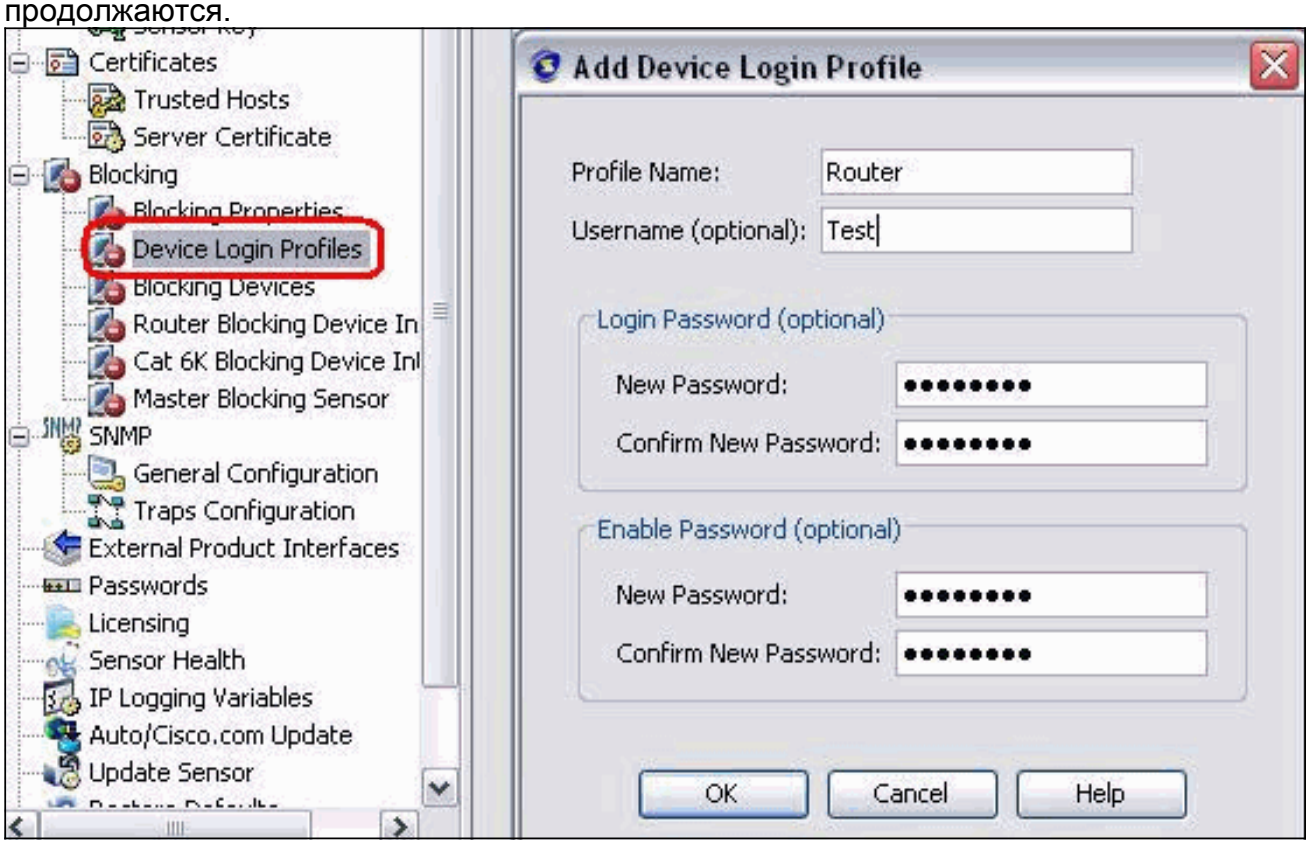
подписи.

13. Нажмите **OK** после того, как вы подтверждаете и нажимаете кнопку **Apply** для применения подписи к Датчику.
14. От Вкладки конфигурация, под менеджментом Датчика нажимают **Blocking**. От левой панели выберите **Blocking Properties**, и проверка **Позволяют Блокироваться**.

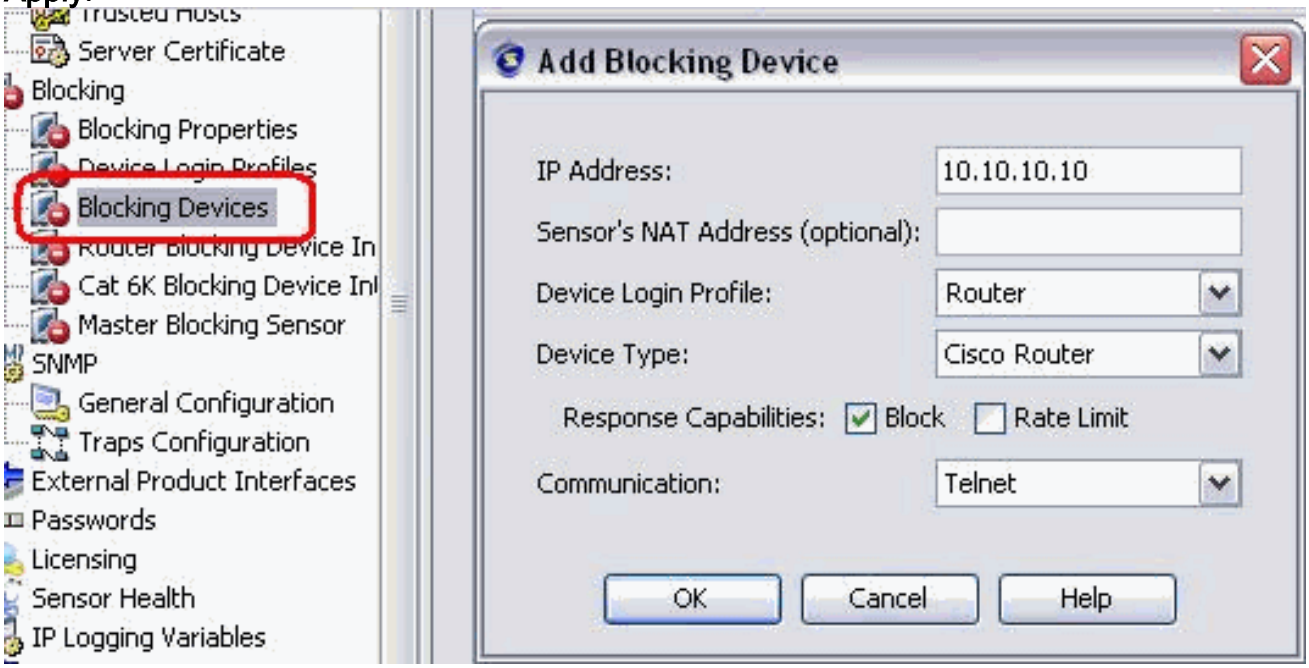


15. Теперь от левой панели, перейдите **к Профилю Входа в систему Устройства**. Для создания нового профиля **нажмите Add**. После того, как созданный нажимают **OK** и **Apply**, чтобы к датчику и

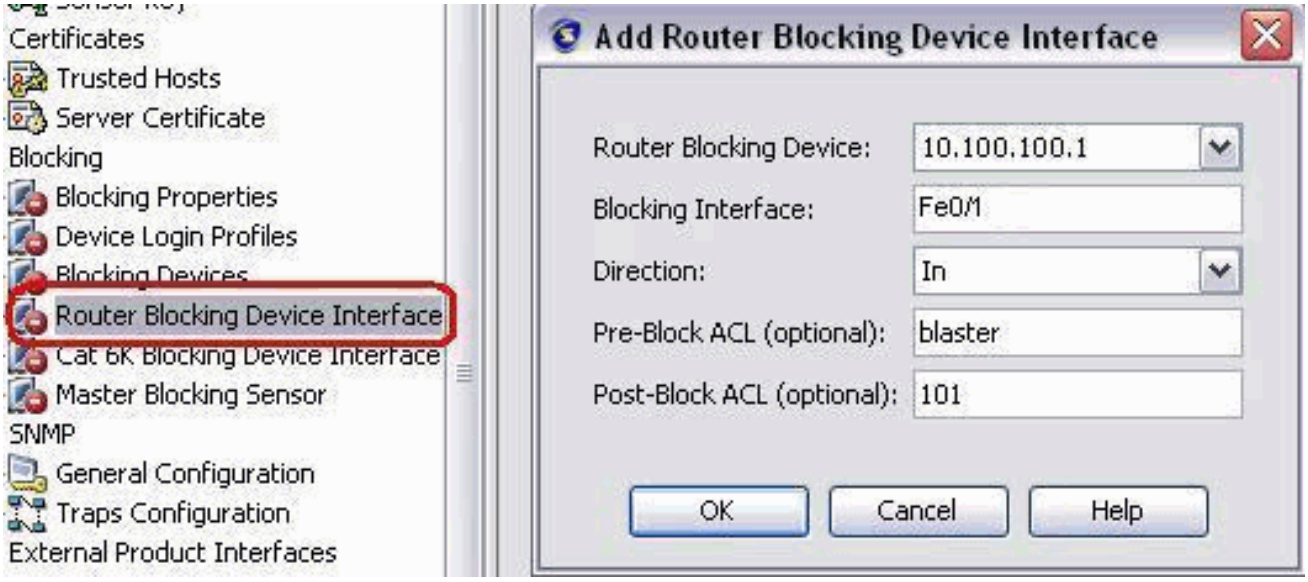
продолжаются.



16. Следующий шаг должен настроить маршрутизатор как Устройство блокировки. От левой панели выберите **Blocking Device**, **нажмите Add** для добавления этой информации. Затем нажмите **OK** и **Apply**.



17. Теперь от левой панели настраивают интерфейсы Устройства блокировки. Добавьте информацию, нажмите **OK** и **Apply**..

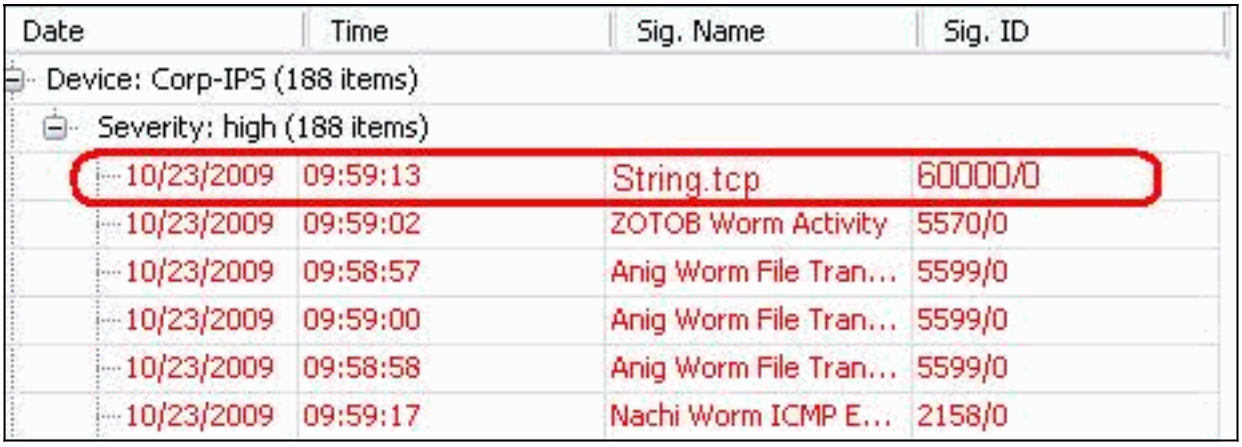


Проверка

Запустите Attack and Blocking

Выполните эти шаги, чтобы пойти в наступление и блокирование:

1. Прежде чем вы пойдете в наступление, перейдете к IME, выберете **Event Monitoring> Dropped Attacks View** и выберете датчик справа.
2. Telnet в House маршрутизатора и проверяет связь от сервера с этими командами.`house#`**`show user`** `Line User Host(s) Idle Location * 0 con 0 idle 00:00:00 226 vty 0 idle 00:00:17 10.66.79.195 house#`**`show access-list`** `Extended IP access list IDS_FastEthernet0/1_in_0 permit ip host 10.66.79.195 any permit ip any any (12 matches) house#`
3. **С индикатора маршрутизатора следует подключиться к центру маршрутизации по протоколу Telnet и ввести команду 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 lost]`** *`!--- Host 10.100.100.2 has been blocked due to the !--- signature "testattack" triggered.`*
4. Telnet в House маршрутизатора и использование команда **show access-list** как показано здесь.`house#`**`show access-list`** `Extended IP access list IDS_FastEthernet0/1_in_0 10 permit ip host 10.66.79.195 any` **`20 deny ip host 10.100.100.2 any (71 matches)`** `30 permit ip any any`
5. От Информационной панели IDS Event Viewer появляется Красный сигнал, как только идут в
наступление.



Date	Time	Sig. Name	Sig. ID
Device: Corp-IPS (188 items)			
Severity: high (188 items)			
10/23/2009	09:59:13	String.tcp	60000/0
10/23/2009	09:59:02	ZOTOB Worm Activity	5570/0
10/23/2009	09:58:57	Anig Worm File Tran...	5599/0
10/23/2009	09:59:00	Anig Worm File Tran...	5599/0
10/23/2009	09:58:58	Anig Worm File Tran...	5599/0
10/23/2009	09:59:17	Nachi Worm ICMP E...	2158/0

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Советы

Используйте эти советы по устранению проблем:

- От Датчика посмотрели на выходные данные **сетевого доступа статистики показа** и удостоверяются, что `state` "активен. От консоли или SSH к Датчику, просматривается эта информация:`sensor5#show statistics network-access Current Configuration AllowSensorShun = false ShunMaxEntries = 100 NetDevice Type = Cisco IP = 10.66.79.210 NATAddr = 0.0.0.0 Communications = telnet ShunInterface InterfaceName = FastEthernet0/1 InterfaceDirection = in State ShunEnable = true NetDevice IP = 10.66.79.210 AclSupport = uses Named ACLs State = Active ShunnedAddr Host IP = 10.100.100.2 ShunMinutes = 15 MinutesRemaining = 12 sensor5#`
- Удостоверьтесь, что коммуникационный параметр показывает, что соответствующий протокол используется, такие как Telnet или SSH с 3DES. Можно попробовать ручной SSH или Telnet от SSH/клиента Telnet на ПК, чтобы проверить, что учетные данные имени пользователя и пароля корректны. Затем попробуйте к Telnet или SSH от самого Датчика к маршрутизатору и посмотрите, можно ли войти успешно к маршрутизатору.

Дополнительные сведения

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