IPS 5.X и более поздние версии/IDSM2: Пример конфигурации встроенной пары VLAN, использующей CLI и IDM

Содержание

Введение

Ассоциация VLAN в парах на физическом интерфейсе известна как встроенный режим пары VLAN. Пакеты, полученные на одной из парных VLAN, проанализированы и переданы к другой VLAN в паре. Встроенные пары VLAN поддерживаются на всех датчиках, которые совместимы с Системой предотвращения вторжений (IPS) 5.1, кроме CID NM, AIP-SSM-10 и AIP-SSM-20.

Встроенный режим пары VLAN является активным режимом считывания, где интерфейс считывания действия как порт магистрали "802.1q" и датчик выполняет Маршрутизацию VLAN между парами VLAN на транке. Это означает, что коммутатор, связанный с интерфейсом считывания, должен быть в режиме магистрали.

Датчик осматривает трафик, который он получает на каждой VLAN в каждой паре, и может или передать пакеты на другой VLAN в паре или отбросить пакет, если обнаружена попытка проникновения. Можно настроить сенсор IPS для одновременного мостового соединения до 255 пар VLAN на каждом интерфейсе считывания. Датчик заменяет поле VLAN ID в 802.1q заголовок каждого полученного пакета с ID выходной VLAN, на которой датчик передает пакет. Датчик отбрасывает все пакеты, полученные на любых VLAN, которым не назначают встроить пар VLAN.

Примечание: Для IPS 4260 открытый для сбоя аппаратный обход не поддерживается на встроенных парах VLAN. См. Аппаратные Ограничения конфигурации Обхода для получения дополнительной информации.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на Датчике системы предотвращения вторжений Cisco (IPS), который использует 5.1 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.

Родственные продукты

Сведения в этом документе также применимы к Системе обнаружения проникновения (IDSM-2) Сервисный модуль.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Конфигурация VACL Capture

См. раздел VACL Capture Настройки IDSM-2 Настройки для передачи трафика к IDSM на коммутаторе.

Встроенная конфигурация режима пары VLAN

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.

Используйте **команду physical-interfaces interface_name** в сервисном интерфейсном подрежиме для настройки встроенных пар VLAN с помощью CLI. Именем интерфейса является FastEthernet или GigabitEthernet.

Эти опции применяются:

- **{enabled | disabled} административное состояние** — административное состояние канала интерфейса, включен ли интерфейс или отключен.**Примечание:** На всех интерфейсах считывания объединительной платы на всех модулях (CID NM IDSM-2 и

SSM AIP), административное состояние установлено во включенный и защищено (вы не можете изменить настройки). Административное состояние не имеет никакого эффекта (и защищен) на интерфейсе команд и управления. Это только влияет на интерфейсы считывания. Интерфейс команд и управления не должен быть включен, потому что он не может быть проверен.

- **default — возвращает значение по умолчанию.**
- **описание** описание встроенной интерфейсной пары.
- **duplex** — Настройка дуплекса интерфейса.**автоматический** — Устанавливает интерфейс в автоматический, выполняют согласование о дуплексе.**полный** — Устанавливает интерфейс в полный дуплекс.**половина** — Устанавливает интерфейс в полудуплекс.**Примечание:** Опция duplex защищена на всех модулях.
- **no — удаляет параметр записи или выбора.**
- **скорость** — параметр настройки скорости интерфейса.**автоматический** — Устанавливает интерфейс в автоматический, выполняют согласование о скорости.**10** — Устанавливает интерфейс в 10 МБ (только для интерфейсов TX).**100** — Устанавливает интерфейс в 100 МБ (только для интерфейсов TX).**1000** — Устанавливает интерфейс в 1 ГБ (для Гигабитных интерфейсов)**Примечание:** Опция скорости защищена на всех модулях.
- **тип подинтерфейса** — Указывает, что интерфейс является подинтерфейсом и какой подинтерфейс определен.**inline-vlan-pair** — Позволяет вам определить подинтерфейс как встроенную пару VLAN.**ни один** — Никакие подинтерфейсы не определен.
- **подинтерфейс** — Определяет подинтерфейс как встроенную пару VLAN.**vlan1** — первая VLAN во встроенной паре VLAN.**vlan2** — Вторая VLAN во встроенной паре VLAN.

Конфигурация интерфейса командой строки CLI

Выполните эти шаги для настройки встроенных параметров настройки пары VLAN на датчике с помощью CLI:

1. Войдите к CLI с помощью учетной записи с администраторскими привилегиями.
2. Введите интерфейсный подрежим:`sensor#configure terminal sensor(config)#service interface sensor(config-int)#`
3. Проверьте, существуют ли какие-либо встроенные интерфейсы (тип подинтерфейса не должен читать "ни один", если никакие встроенные интерфейсы не были настроены):`sensor(config-int)#show settings physical-interfaces (min: 0, max: 999999999, current: 2) ---------- <protected entry> name: GigabitEthernet0/0 <defaulted> ---------- media-type: tx <protected> description: <defaulted> admin-state: disabled <protected> duplex: auto <defaulted> speed: auto <defaulted> alt-tcp-reset-interface ---------- none ---------- ---------- subinterface-type ---------- none ---------- <protected entry> name: GigabitEthernet0/1 <defaulted> ---------- media-type: tx <protected> description: <defaulted> admin-state: disabled <defaulted> duplex: auto <defaulted> speed: auto <defaulted> alt-tcp-reset-interface ---------- none ---------- ---------- subinterface-type ---------- none ---------- <protected entry> name: GigabitEthernet0/2 <defaulted> ---------- media-type:`

```
tx <protected> description: <defaulted> admin-state: disabled <defaulted> duplex: auto
<defaulted> speed: auto <defaulted> alt-tcp-reset-interface ----------------------------
--------------- none ------------------------------------------------ --------------------
------------------------ ------------------------------------------------ subinterface-
type ------------------------------------------- none ---------------------------------
------------- ------------------------------------------------ -------------------------
----------------- ------------------------------------------------ <protected entry> name:
GigabitEthernet0/3 <defaulted> ------------------------------------------- media-type:
tx <protected> description: <defaulted> admin-state: disabled <defaulted> duplex: auto
<defaulted> speed: auto <defaulted> alt-tcp-reset-interface ----------------------------
--------------- none ------------------------------------------------ --------------------
------------------------ ------------------------------------------------ subinterface-
type ------------------------------------------- none ---------------------------------
------------- ------------------------------------------------ -------------------------
----------------- ------------------------------------------------ <protected entry> name:
Management0/0 <defaulted> ------------------------------------------- media-type: tx
<protected> description: <defaulted> admin-state: disabled <protected> duplex: auto
<defaulted> speed: auto <defaulted> alt-tcp-reset-interface ----------------------------
--------------- none ------------------------------------------------ --------------------
------------------------ ------------------------------------------------ subinterface-
type ------------------------------------------- none ---------------------------------
------------- ------------------------------------------------ -------------------------
----------------- ------------------------------------------------ ---------------------
---------------------- command-control: Management0/0 <protected> inline-interfaces (min:
0, max: 999999999, current: 0) ---------------------------------------------- ------------
---------------------------------- bypass-mode: auto <defaulted> interface-notifications -
--------------------------------------------- missed-percentage-threshold: 0 percent
<defaulted> notification-interval: 30 seconds <defaulted> idle-interface-delay: 30 seconds
<defaulted> ---------------------------------------------- sensor(config-int)#
```

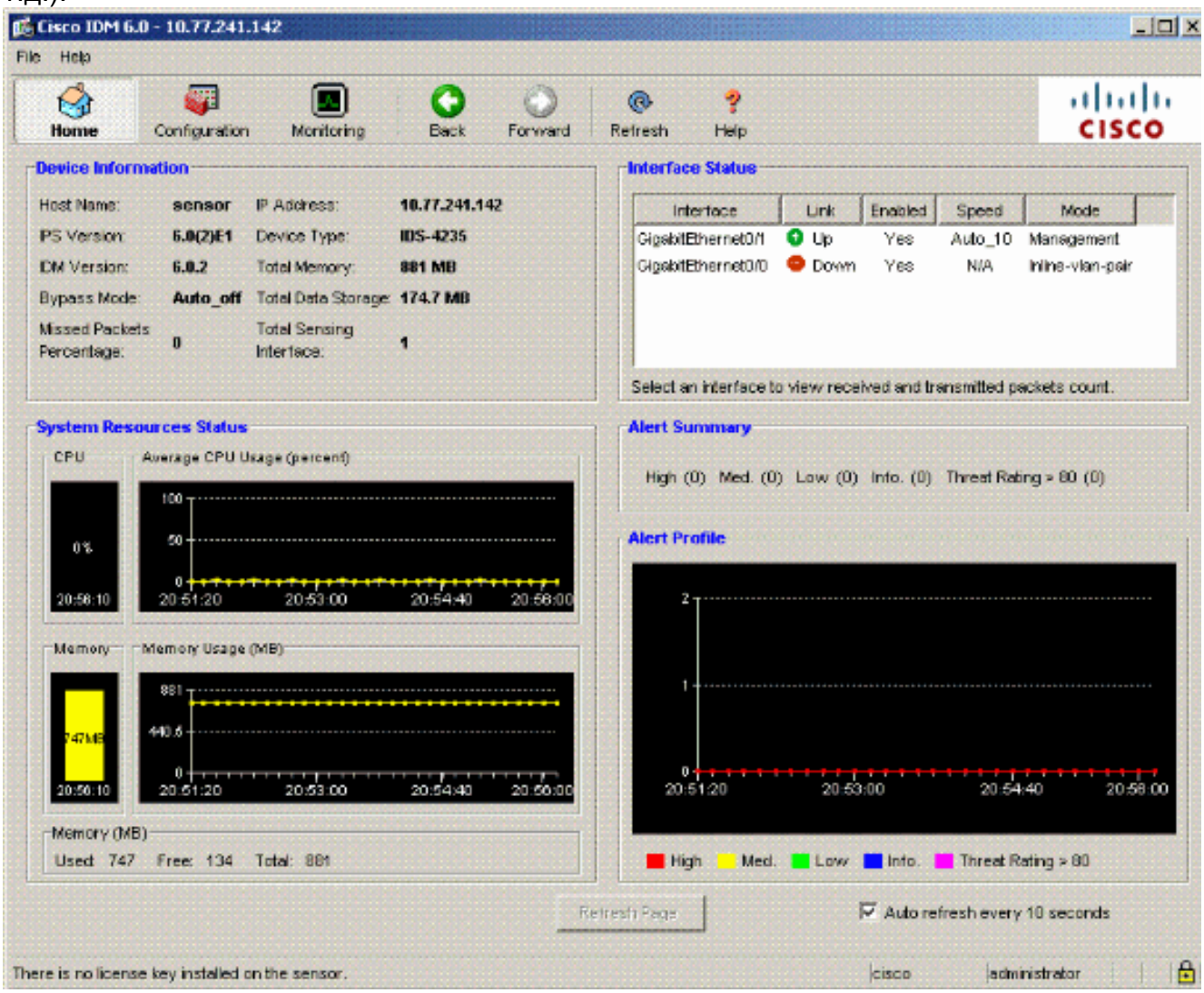
4. Демонтируйте любые встроенные интерфейсы, которые используют этот физический интерфейс:`sensor(config-int)#` **`no inline-interfaces interface_name`**
5. Отобразите список доступных интерфейсов:`sensor(config-int)#` **`physical-interfaces ?`**
   `GigabitEthernet0/0 GigabitEthernet0/0 physical interface. GigabitEthernet0/1 GigabitEthernet0/1 physical interface. GigabitEthernet0/2 GigabitEthernet0/2 physical interface. GigabitEthernet0/3 GigabitEthernet0/3 physical interface. Management0/0 Management0/0 physical interface. sensor(config-int)#` **`physical-interfaces`**
6. Задайте интерфейс:`sensor(config-int)#` **`physical-interfaces GigabitEthernet0/2`**
7. Включите административное состояние интерфейса:`sensor(config-int-phy)#` **`admin-state enabled`** Интерфейс должен быть назначен на действительный датчик и включен для мониторинга трафика.
8. Добавьте описание этого интерфейса:`sensor(config-int-phy)#` **`description INT1`**
9. Настройте настройки дуплекса:`sensor(config-int-phy)#` **`duplex full`** Эта опция не доступна на модулях.
10. Настройте скорость:`sensor(config-int-phy)#` **`speed 1000`** Эта опция не доступна на модулях.
11. Установите встроенную пару VLAN:`sensor(config-int-phy)#` **`subinterface-type inline-vlan-pair`** `sensor(config-int-phy-inl)#` **`subinterface 1`** `sensor(config-int-phy-inl-sub)#` **`vlan1 52`** `sensor(config-int-phy-inl-sub)#` **`vlan2 53`**
12. Добавьте описание для встроенной пары VLAN:`sensor(config-int-phy-inl-sub)#` **`description pairs vlans 52 and 53`**
13. Проверьте встроенные параметры настройки пары VLAN:`sensor(config-int-phy-inl-sub)#` **`show settings`** `subinterface-number: 1 ---------- description: VLANpair1 default: vlan1: 52 vlan2: 53 ---------- sensor(config-int-phy-inl-sub)#`
14. Выйдите из интерфейсного подрежима:`sensor(config-int-phy-inl-sub)#` **`exit`** `sensor(config-int-phy-inl)#` **`exit`** `sensor(config-int-phy)#` **`exit`** `sensor(config-int)#` **`exit`** `Apply Changes:?[yes]:`
15. Нажмите **Enter**, чтобы применить изменения или войти **не** для отмены от них.

16. Перейдите в действительный режим конфигурации сенсора:`sensor(config)#`**`service analysis-engine`** `sensor(config-ana)#`**`virtual-sensor vs0`**
17. Добавьте интерфейс к действительному датчику:`sensor(config-ana-vir)#`**`physical-interface GigabitEthernet0/2 subinterface-number 1`**
18. Выйдите из подрежима действительного датчика:`sensor(config-ana-vir)#`**`exit`**
`sensor(config-ana)#`**`exit`** `Apply Changes:?[yes]:`
19. Нажмите **Enter**, чтобы применить изменения или войти **не** для отмены от них.

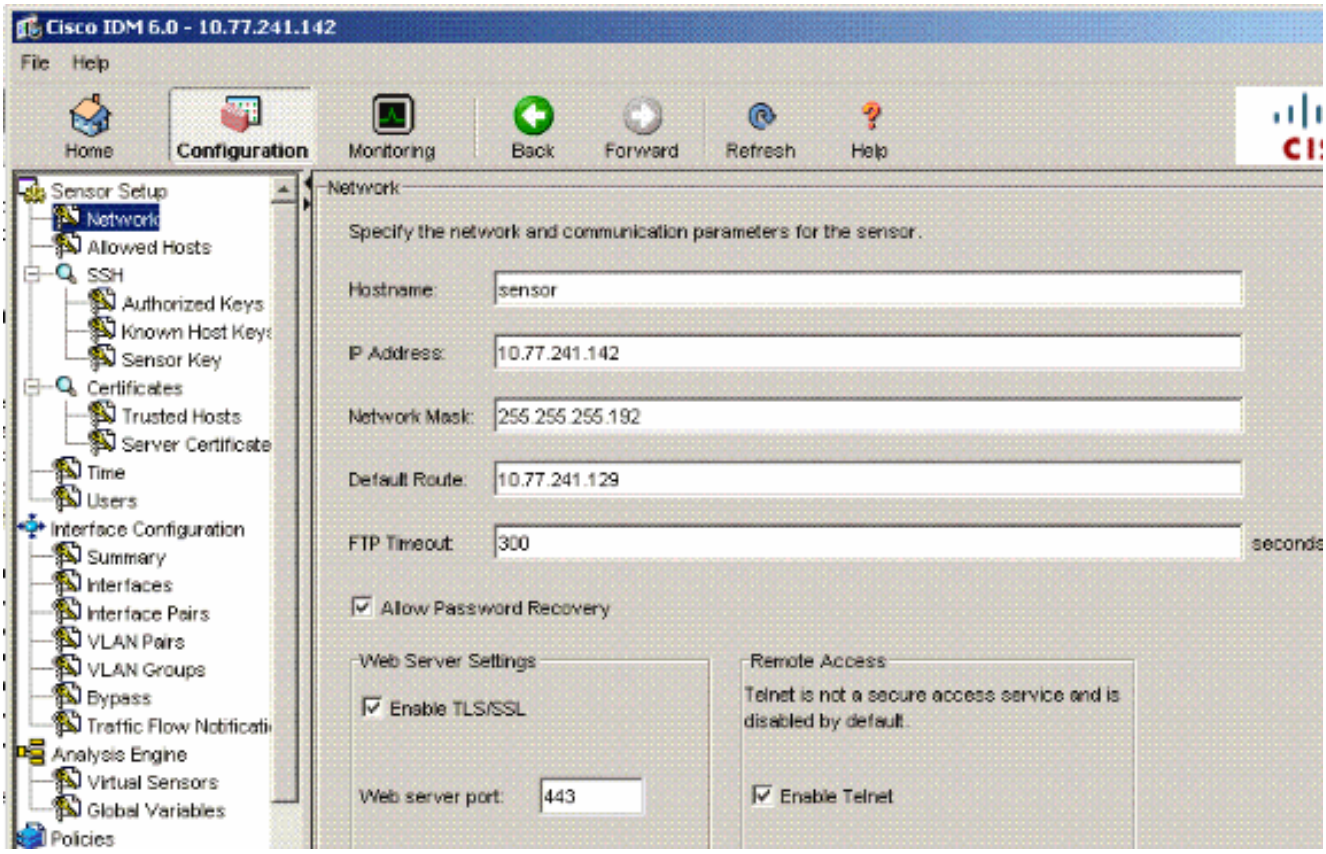
Конфигурация IDM

Выполните эти шаги для настройки встроенных параметров настройки пары VLAN на датчике с помощью IDS Device Manager (IDM):

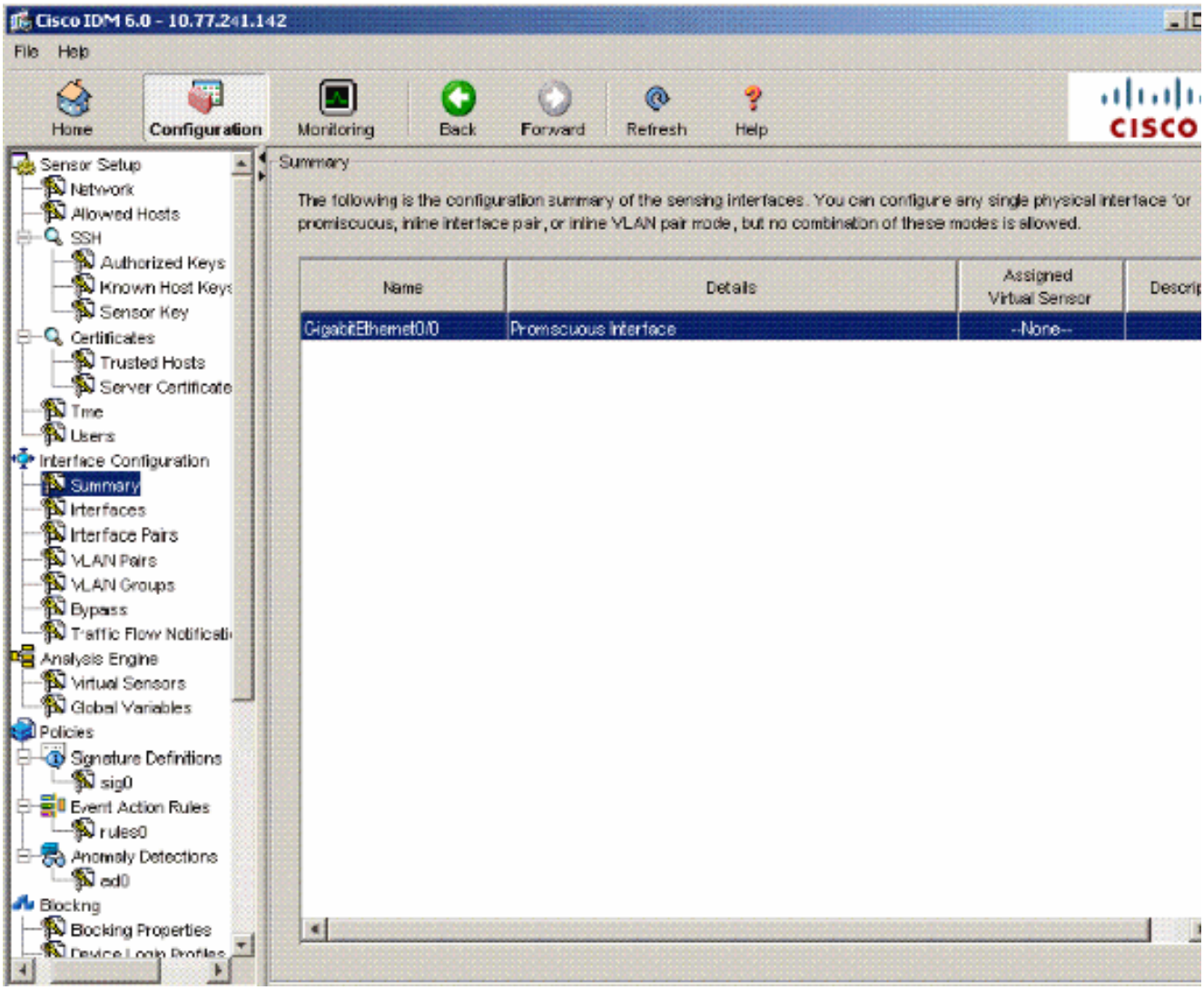
1. Откройте свой браузер и введите **https://<Management_IP_Address_of_IPS>** для доступа к IDM на IPS.
2. Нажмите **Download IDM Launcher и Start IDM** для загрузки установщика для приложения.
3. Перейдите к Домашней странице для просмотра сведений об устройстве, таких как Имя хоста, IP-адрес, версия и модель. и т.д.).



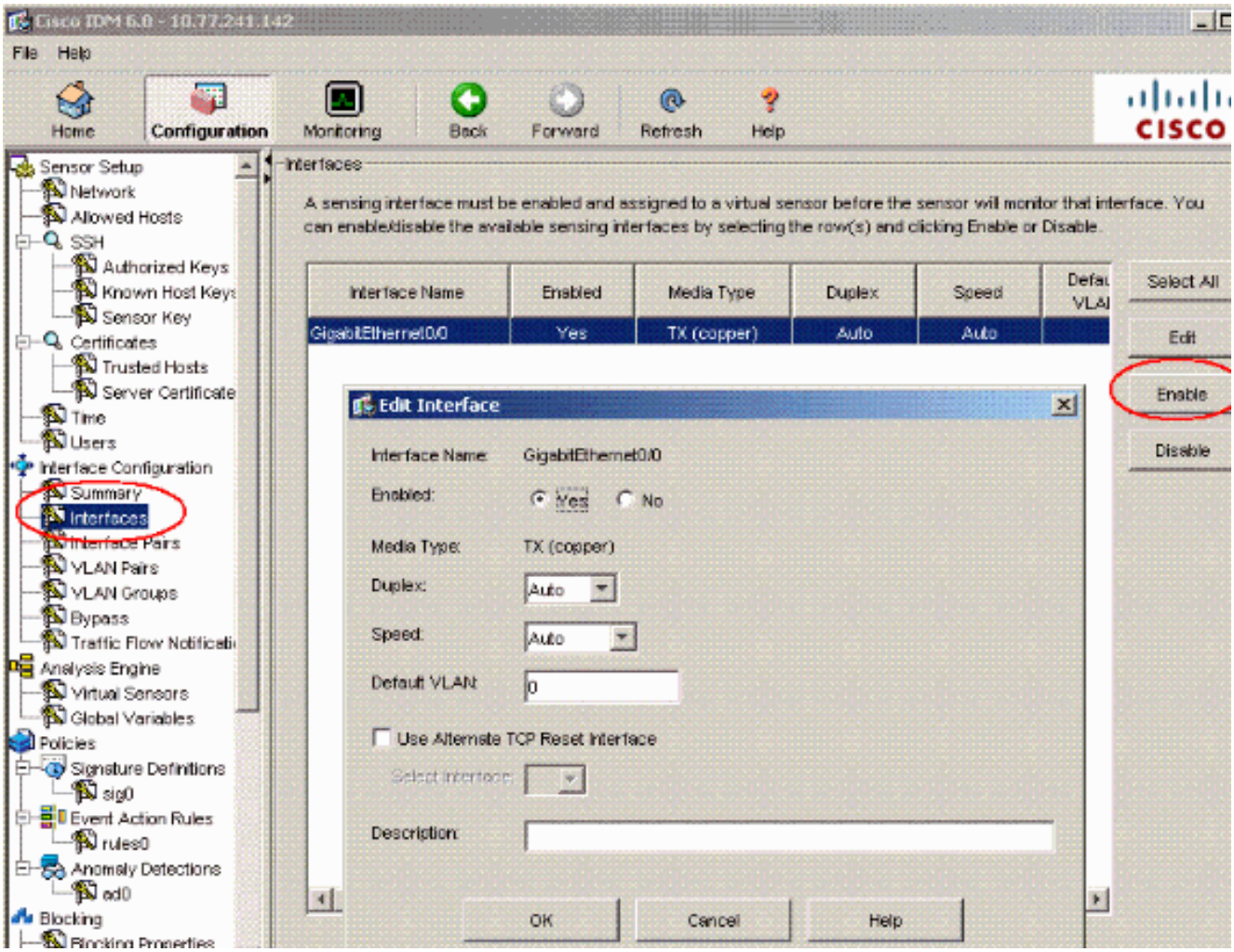
4. Перейдите **к Конфигурации> Настройка Датчика** и нажмите **Network**. Здесь можно задать Имя хоста, IP-адрес и Маршрут по умолчанию.



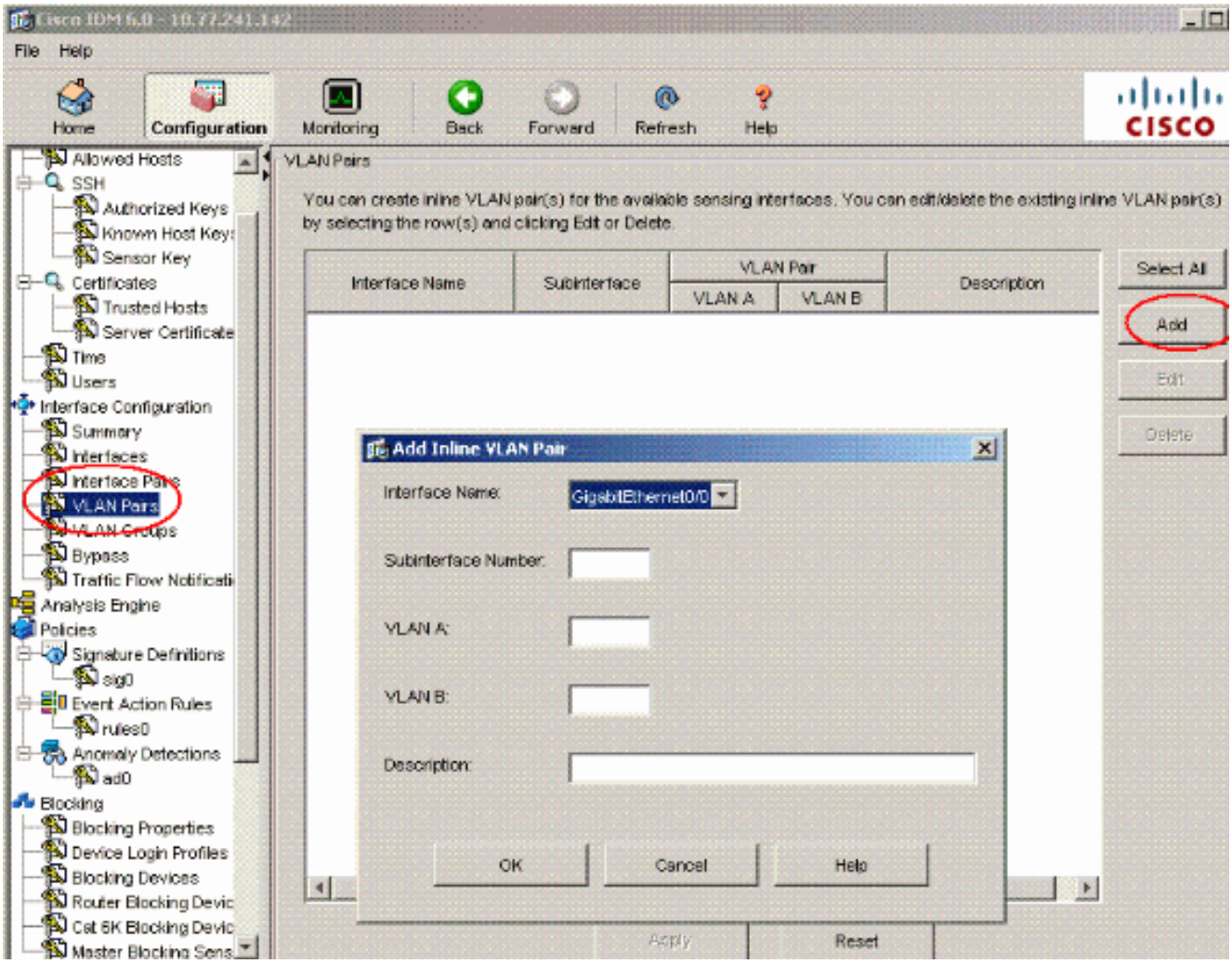
5. Перейдите **к Конфигурации> Конфигурация интерфейса** и нажмите **Summary**.Эта страница показывает сводку конфигурации интерфейса считывания.



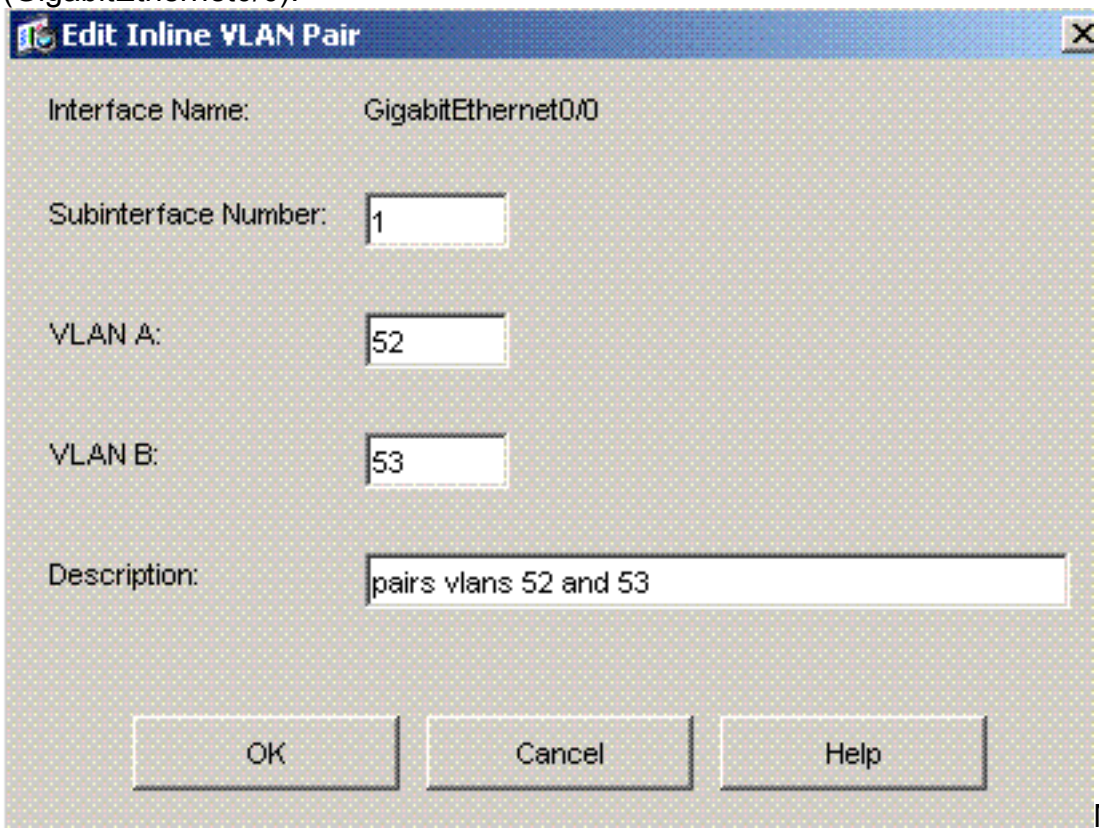
6. Перейдите **к Конфигурации> Конфигурация интерфейса> Интерфейсы** и выберите имя интерфейса. Затем нажмите **Enable** для включения интерфейса считывания. Кроме того, настройте дуплекс, Скорость и сведения о виртуальной локальной сети (VLAN).



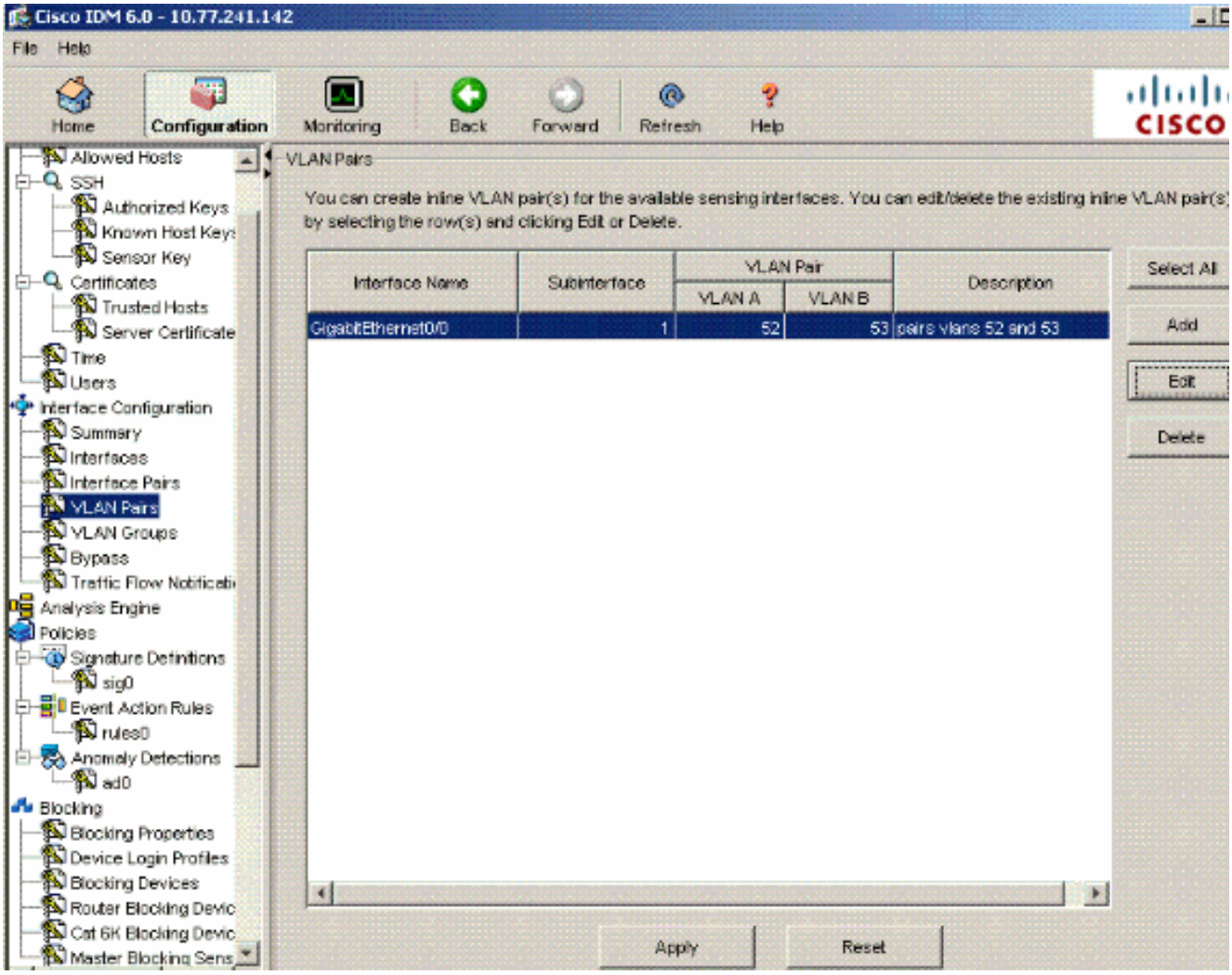
7. Перейдите к **Конфигурации> Конфигурация интерфейса> Пары VLAN** и **нажмите Add** для создания Встроенных Пар VLAN.



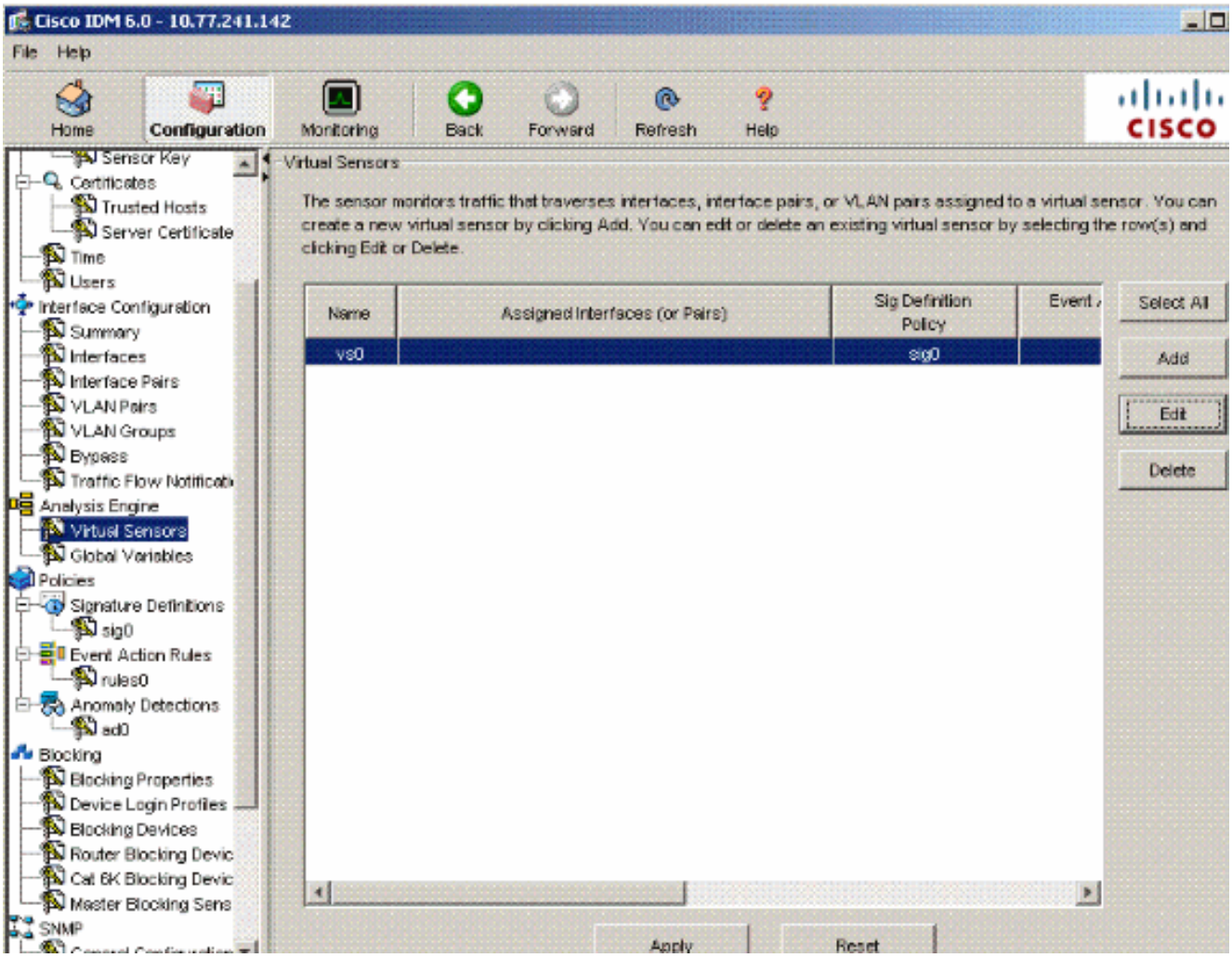
8. Введите Номер Подинтерфейса, VLAN A и VLAN B для интерфейса считывания (GigabitEthernet0/0).



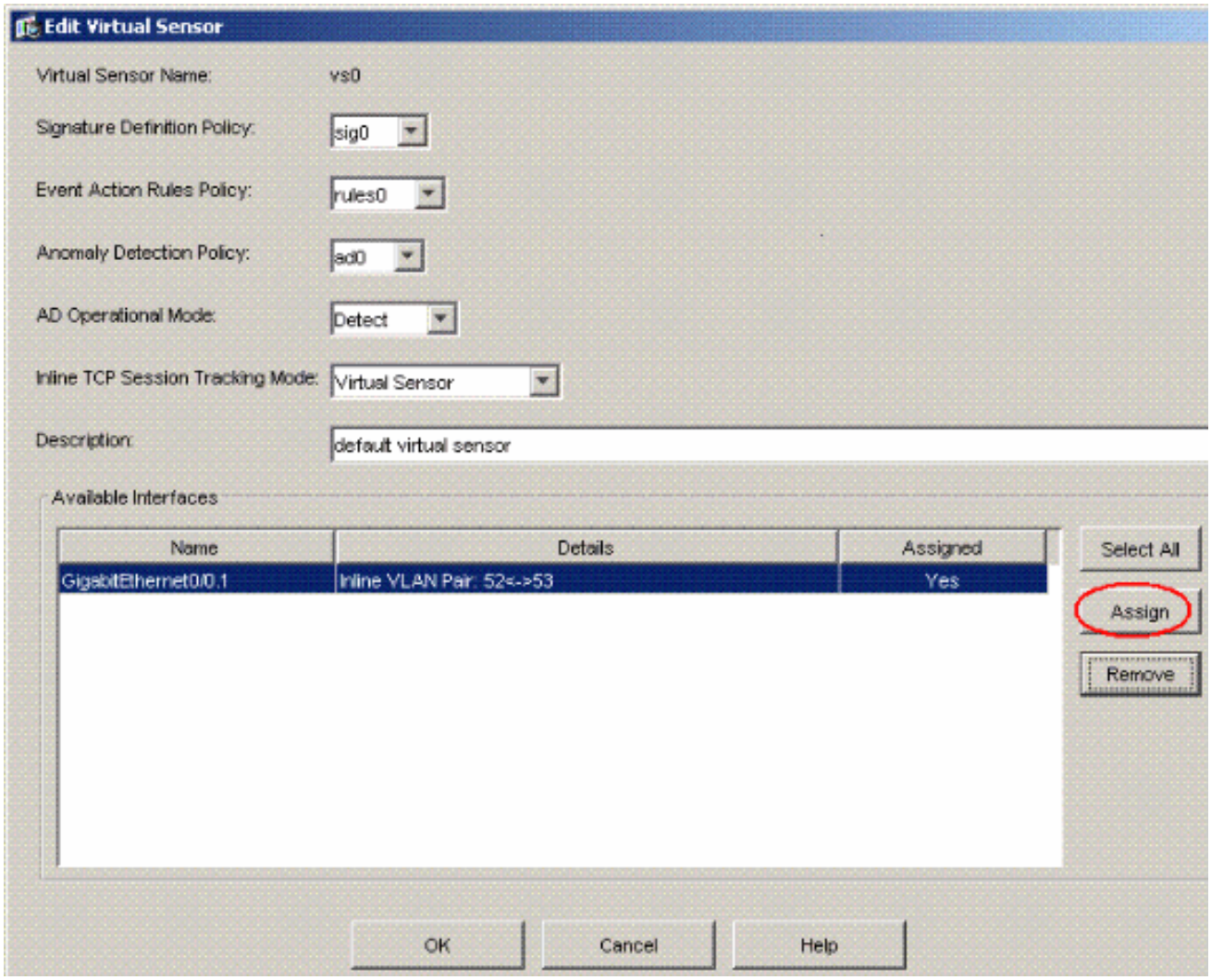
Можно просмотреть сводку Встроенной Конфигурации Пары VLAN.



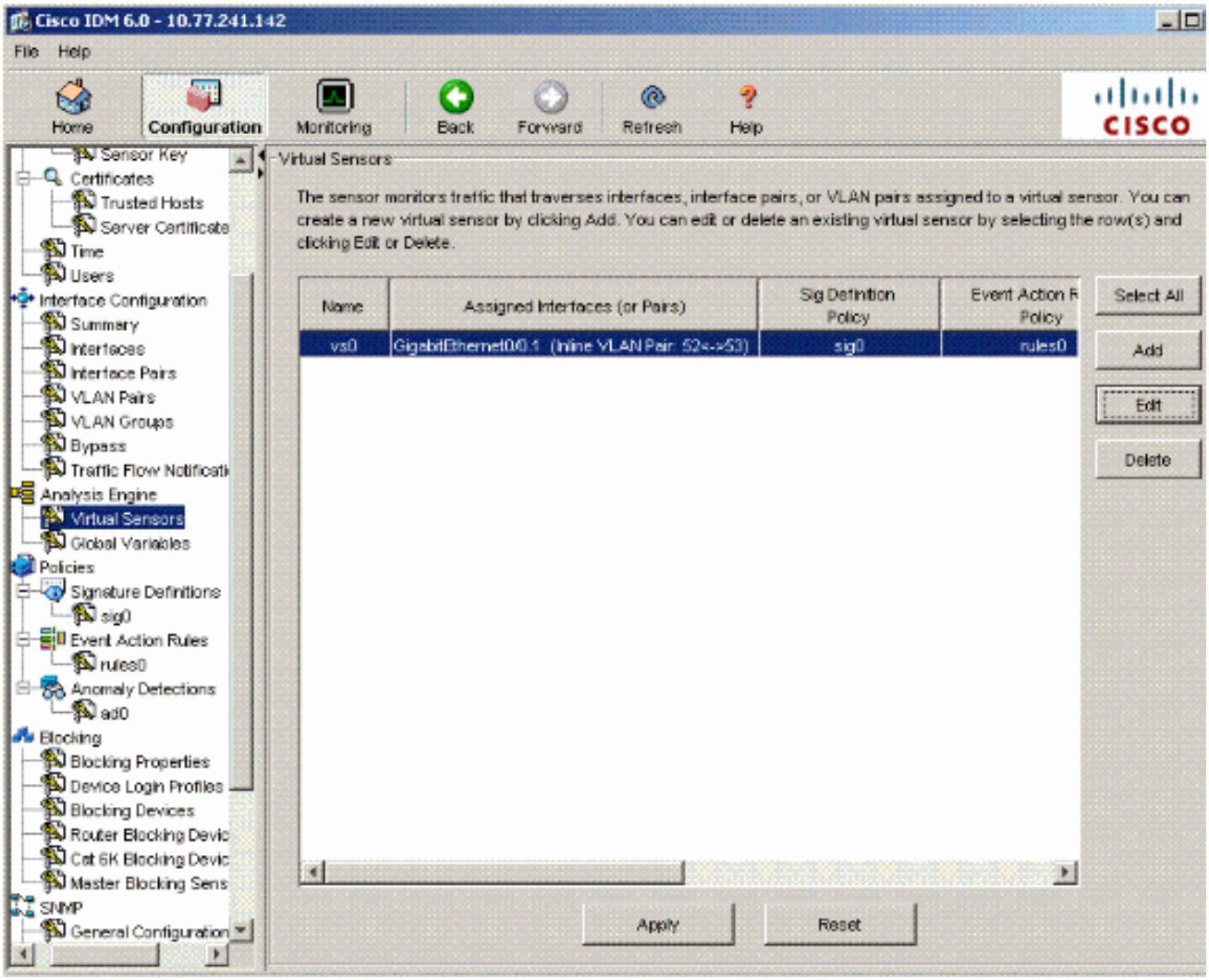
9. Перейдите к **Конфигурации> Аналитический Механизм> Действительный Датчик** и нажмите **Edit** для создания нового действительного датчика.



10. Назначьте Встроенную Пару VLAN 52 и 53 к Действительному Датчику vs0.



Просмотрите сводку назначенной действительной информации о датчике.



Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- CISCO ASA 5500 SERIES ADAPTIVE SECURITY APPLIANCES
- Cisco Intrusion Prevention System
- Cisco IPS 4200 Series Sensors
- Cisco Systems – техническая поддержка и документация