IPS 6. X и позже / IDSM2: Встроенный Интерфейсный Режим Пар с помощью Примера конфигурации IDM

Содержание

Введение

Работа во Встроенном Интерфейсном Парном режиме помещает Систему предотвращения вторжений (IPS) непосредственно в трафик и влияет на скорости передачи пакетов, который делает их медленнее, когда добавлена задержка. Это позволяет датчику останавливать атаки, таким образом, он отбрасывает вредоносный трафик, прежде чем он достигнет намеченной цели, таким образом он предоставляет защитный сервис. Мало того, что встроенное устройство обрабатывает информацию об Уровнях 3 и 4, но это также анализирует содержание и информационное наполнение пакетов для более сложных встроенных атак (Уровни 3 к 7). Этот более глубокий анализ позволяет системе определить и остановить и/или заблокировать атаки, которые обычно проходят через традиционное устройство с функциями межсетевого экрана.

Во Встроенном Интерфейсном Парном режиме пакет входит через первый интерфейс пары на датчике и второй интерфейс пары. Пакет передан к второму интерфейсу пары, пока тот пакет не запрещается или модифицируется подписью.

Примечание: Можно настроить IPS AIM и SSM AIP для работы встроенный даже при том, что эти модули имеют только один интерфейс считывания.

Примечание: Если парные интерфейсы связаны с тем же коммутатором, необходимо настроить их на коммутаторе как порты доступа с другими VLAN доступа для этих двух

портов. В противном случае трафик не течет через встроенный интерфейс.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на датчике Cisco IPS, который использует Интерфейс командной строки 6.0 и Менеджер устройств Системы предотвращения вторжений (IDM) 6.0.

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.

Встроенная интерфейсная конфигурация пар

Используйте команду *названия* **встроенных интерфейсов** в сервисном интерфейсном подрежиме для создания встроенных интерфейсных пар.

Примечание: Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Примечание: SSM AIP настроен для встроенного интерфейсного режима от CLI Cisco ASA а не от CLI Cisco IPS.

Эти опции применяются:

- *название* **встроенных интерфейсов** — Название логической встроенной интерфейсной пары**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
- **interface1 interface_name** — первый интерфейс во встроенной интерфейсной паре
- **interface2 interface_name** — второй интерфейс во встроенной интерфейсной паре
- **no — удаляет параметр записи или выбора**
- **{enabled | disabled} административное состояние** — административное состояние канала интерфейса, включен ли интерфейс или отключен.

Конфигурация интерфейса командой строки CLI

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

1. Войдите к CLI с учетной записью, которая имеет администраторские привилегии.
2. Введите интерфейсный подрежим:`sensor#**configure terminal** sensor(config)#**service interface** sensor(config-int)#`
3. Проверьте, существуют ли какие-либо встроенные интерфейсы. Если никакие встроенные интерфейсы не были настроены, тип подинтерфейса должен считать

```
none: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. Назовите встроенную пару:`sensor(config-int)#`**`inline-interfaces PAIR1`**
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. Настройте два интерфейса в пару:`sensor(config-int)#`**`interface1 GigabitEthernet0/0`**
   `sensor(config-int-inl)#`**`interface2 GigabitEthernet0/1`** Необходимо назначить интерфейс на действительный датчик и включить его, прежде чем он сможет контролировать трафик. Посмотрите шаг 10 для получения дополнительной информации.
7. Добавьте описание этого интерфейса:`sensor(config-int-phy)#`**`description PAIR1 Gig0/0 and Gig0/1`**
8. Повторите шаги 4 - 7 для любых других интерфейсов, которые вы хотите настроить для встраивания интерфейсных пар.
9. !--- Проверьте настройки:`sensor(config-int-inl)#`**`show settings`** `name: PAIR1 ----------
   ------------------------------ description: PAIR1 Gig0/0 & Gig0/1 default: interface1:
   GigabitEthernet0/0 interface2: GigabitEthernet0/1 ------------------------------------
   ------`
10. Включите интерфейсы, назначенные на интерфейсную пару:`sensor(config-int)#`**`exit`**
    `sensor(config-int)#`**`physical-interfaces GigabitEthernet0/0`** `sensor(config-int-phy)#`**`admin-state enabled`** `sensor(config-int-phy)#`**`exit`** `sensor(config-int)#`**`physical-interfaces GigabitEthernet0/1`** `sensor(config-int-phy)#`**`admin-state enabled`** `sensor(config-int-phy)#`**`exit`**
    `sensor(config-int)#`
11. Проверьте, что включены интерфейсы:`sensor(config-int)#`**`show settings`** `physical-interfaces (min: 0, max: 999999999, current: 5) --
    ----- <protected entry> name: GigabitEthernet0/0 --
    ------ media-type: tx <protected> description: <defaulted> admin-state: enabled default:
    disabled duplex: auto <defaulted> speed: auto <defaulted> default-vlan: 0 <defaulted> alt-
    tcp-reset-interface -- none ----------------
    ------------------------------ -- -----------
    ---------------------------------- subinterface-type ----------------------------------
    ------------ none -- ----------------------
    ---------------------- -- -----------------
    ------------------------------ <protected entry> name: GigabitEthernet0/1 -----------------
    ------------------------------ media-type: tx <protected> description: <defaulted> admin-
    state: enabled default: disabled duplex: auto <defaulted> speed: auto <defaulted> default-
    vlan: 0 <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> default-vlan: 0 <defaulted> alt-tcp-reset-interface --
    --- none ------------------------------------
    -------- -- ----------------------------
    -------------- subinterface-type -- none ----
    -- --
    - -- ----------------------------------
    ------- <protected entry> name: GigabitEthernet0/3 <defaulted> -------------------------`
```
```

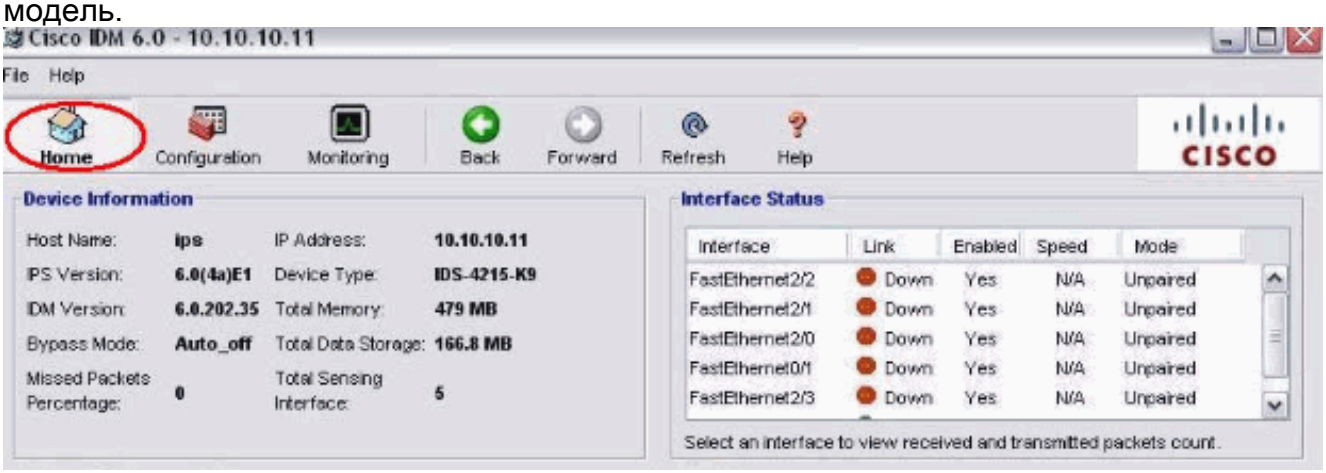
```
------------------- media-type: tx <protected> --MORE--
```

12. Выполните эту команду, чтобы удалить встроенную интерфейсную пару и возвратить интерфейсы к случайному режиму:`sensor(config-int)#` **`no inline-interfaces PAIR1`** Необходимо также удалить встроенную интерфейсную пару от действительного датчика, до которого она назначена.
13. Проверьте, что была удалена встроенная интерфейсная пара:`sensor(config-int)#` **`show settings`** `--- command-control: Management0/0 <protected> inline-interfaces (min: 0, max: 999999999, current: 0) ----------------------- ----------------------- -- bypass-mode: auto <defaulted> interface-notifications --`
14. Выходной подрежим конфигурации интерфейса:`sensor(config-int)#` **`exit`** `Apply Changes:?[yes]:`
15. Нажмите **Enter**, чтобы применить изменения или войти **не** для отмены от них.

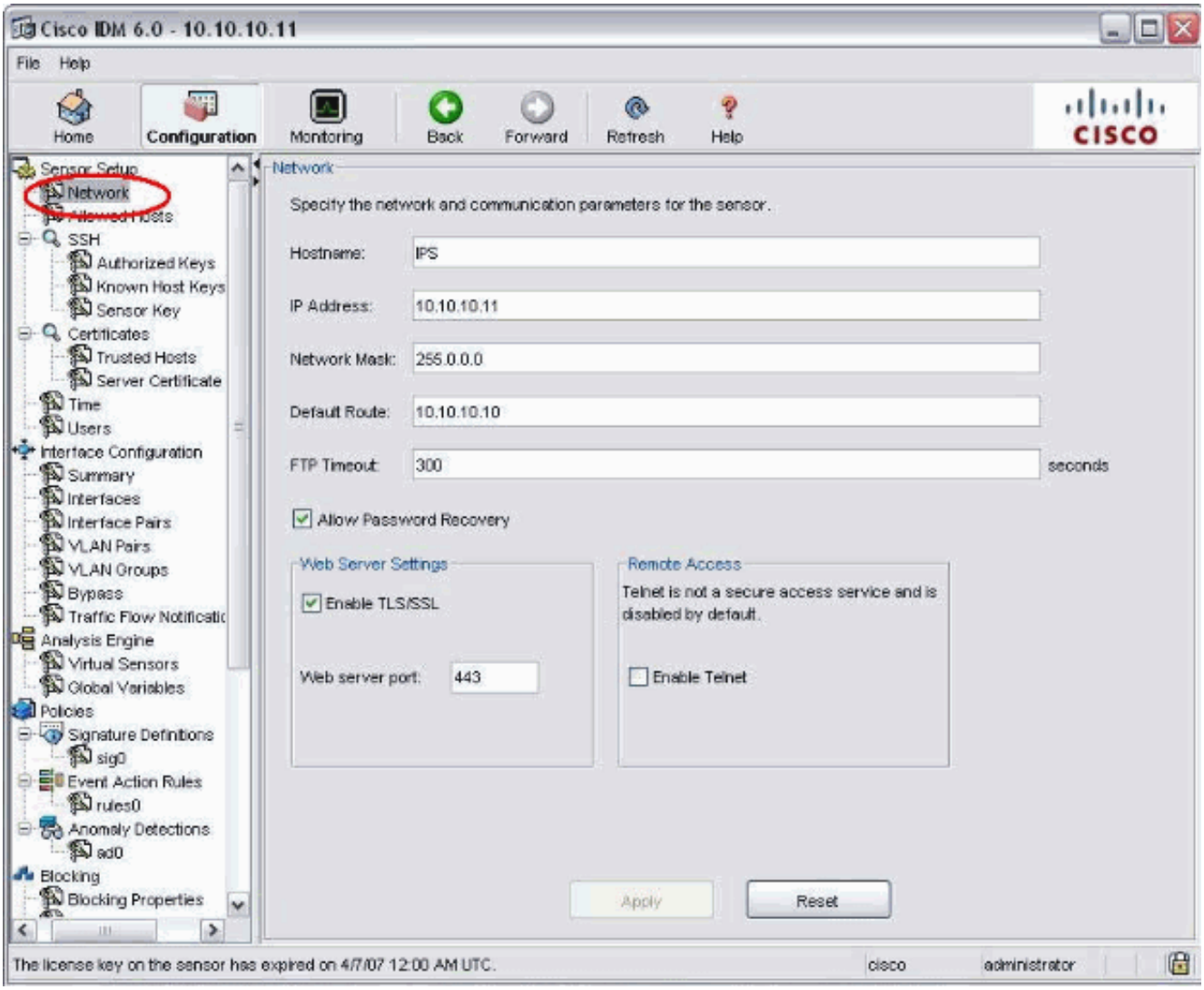
Конфигурация IDM

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

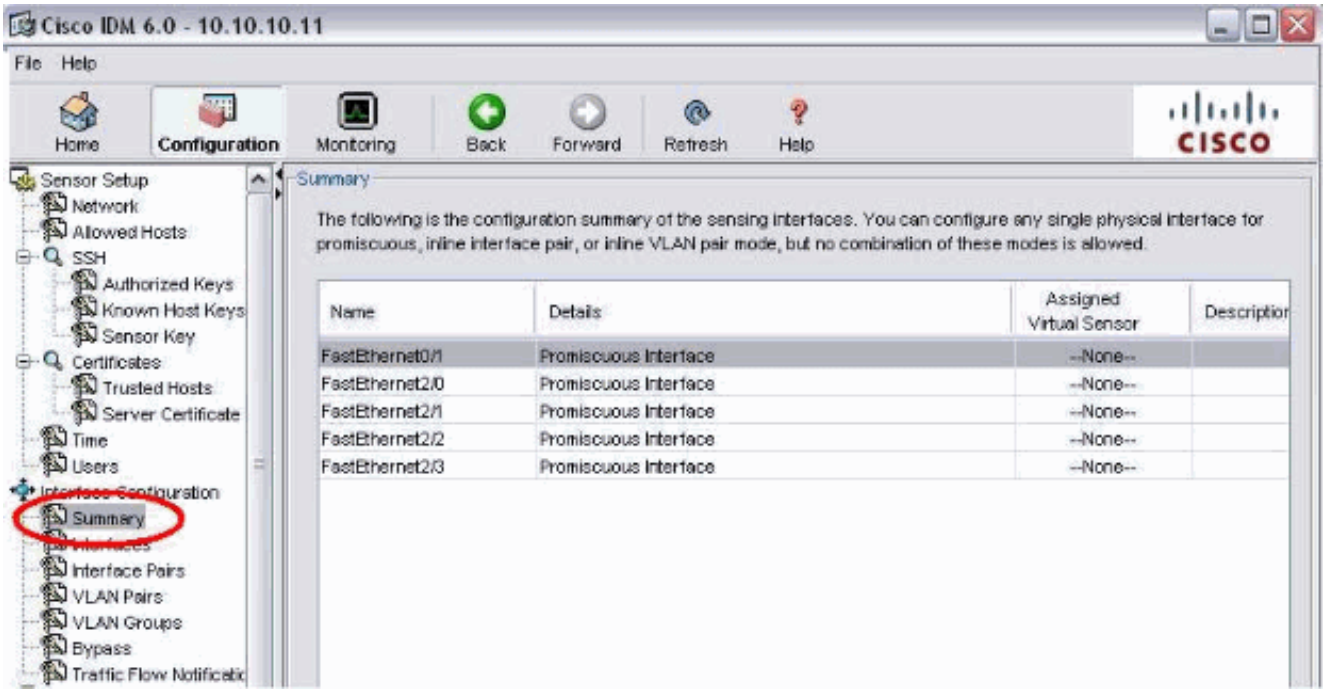
1. Откройте свой браузер и введите **https://<Management_IP_Address_of_IPS>** для доступа к IDM на IPS.
2. Нажмите **Download IDM Launcher** и **Start IDM** для загрузки установщика для приложения.
3. Перейдите к Домашней странице для просмотра сведений об устройстве, таких как Имя хоста, IP-адрес, версия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



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

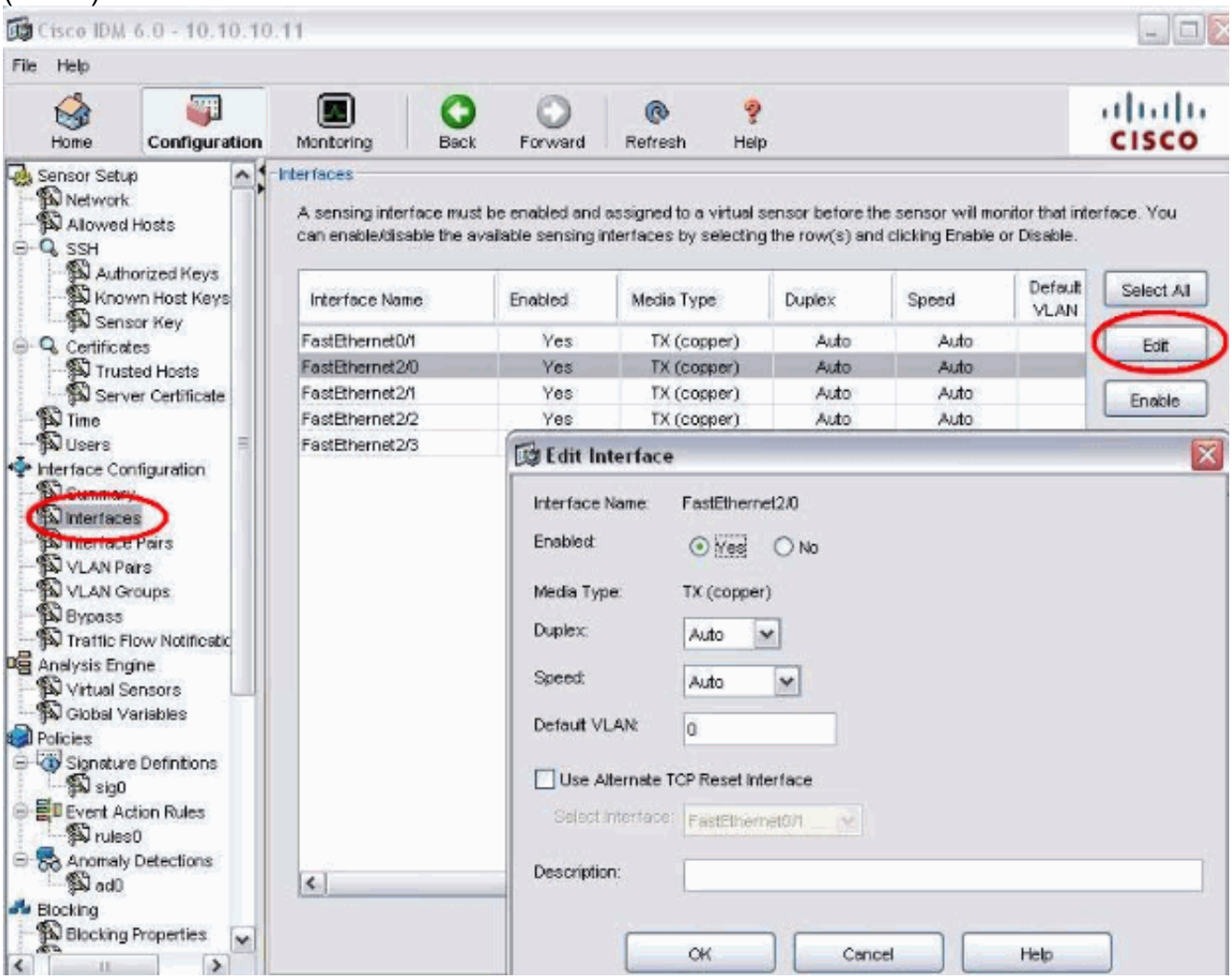


5. Перейдите **к Конфигурации> Конфигурация интерфейса** и нажмите **Summary**.Эта страница показывает сводку конфигурации интерфейса считывания:

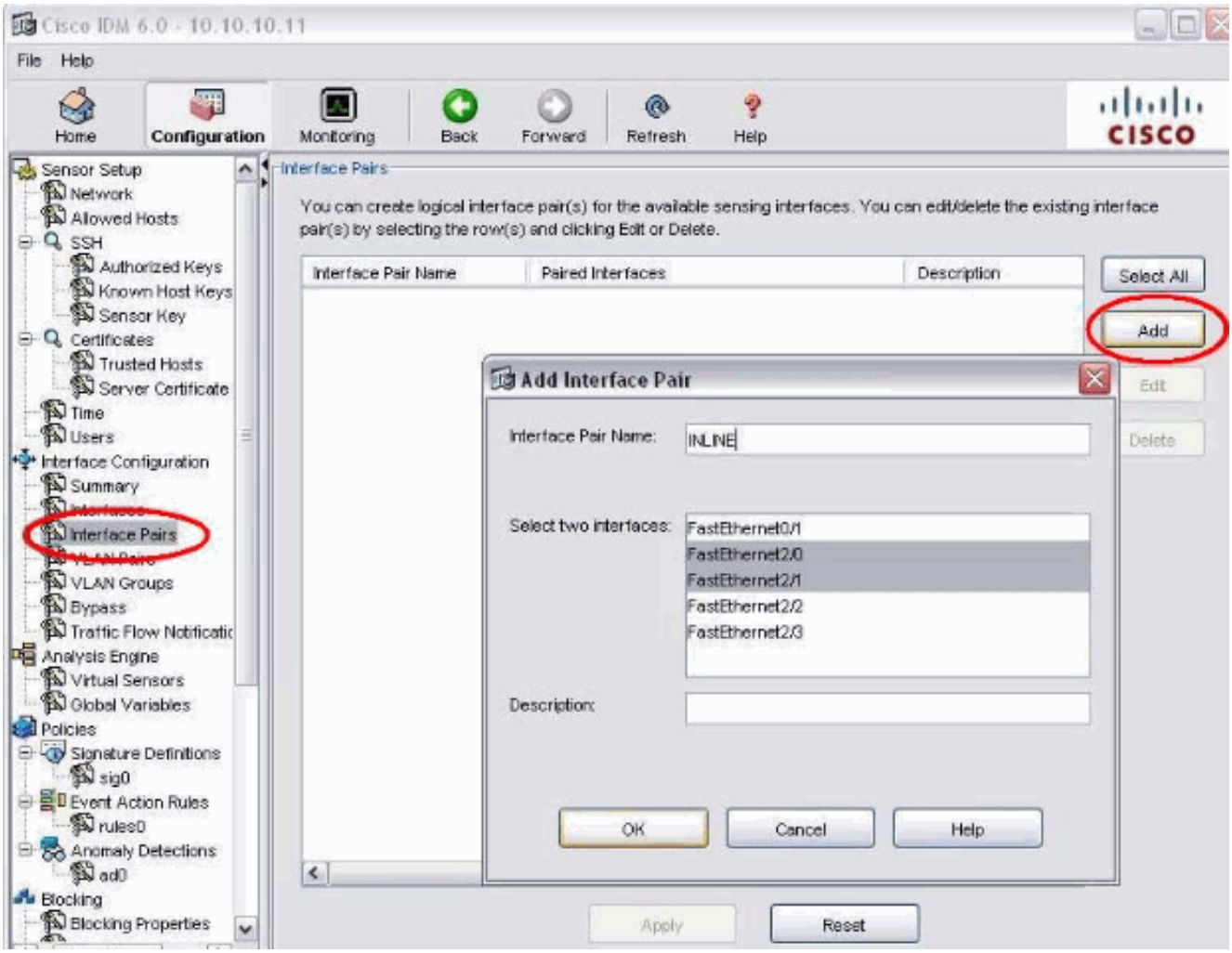


6. Перейдите **к Конфигурации> Конфигурация интерфейса> Интерфейсы** и выберите имя интерфейса. Затем нажмите **Enable** для включения интерфейса считывания. Кроме того, настройте дуплекс, Скорость и сведения о виртуальной локальной сети

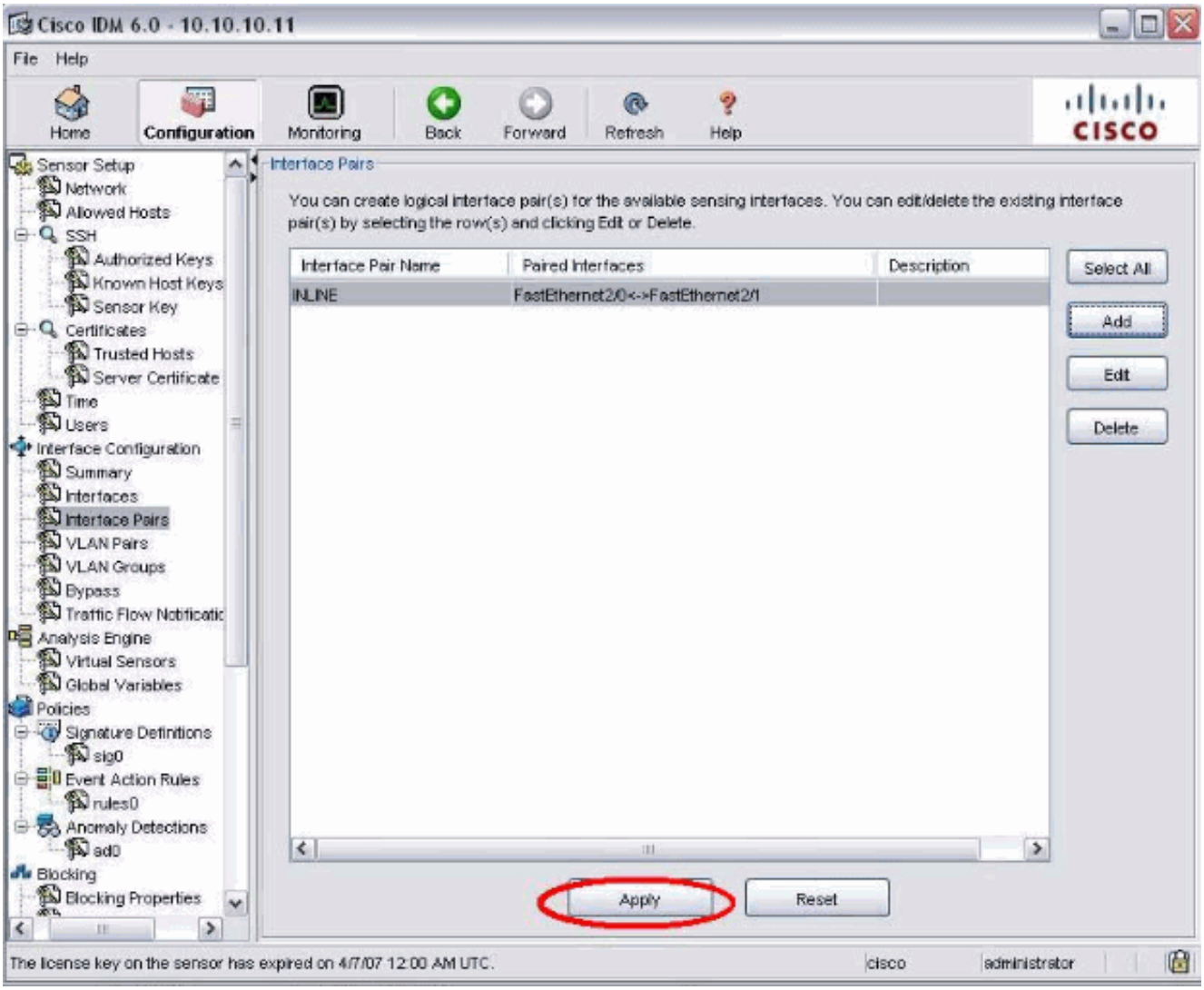
(VLAN).



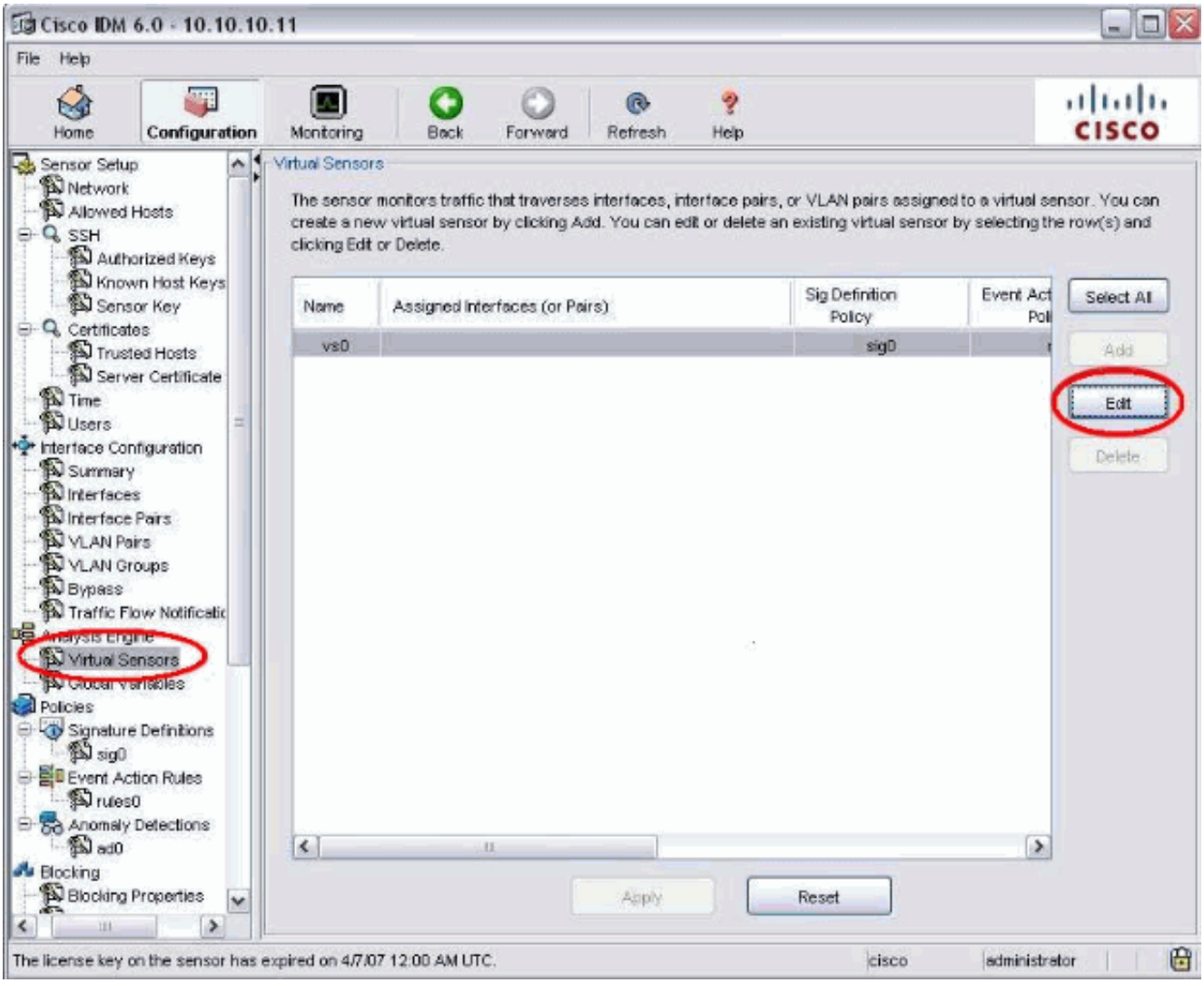
7. Перейдите **к Конфигурации> Конфигурация интерфейса> Интерфейсные Пары** и **нажмите Add** для создания Встроенной
Пары.



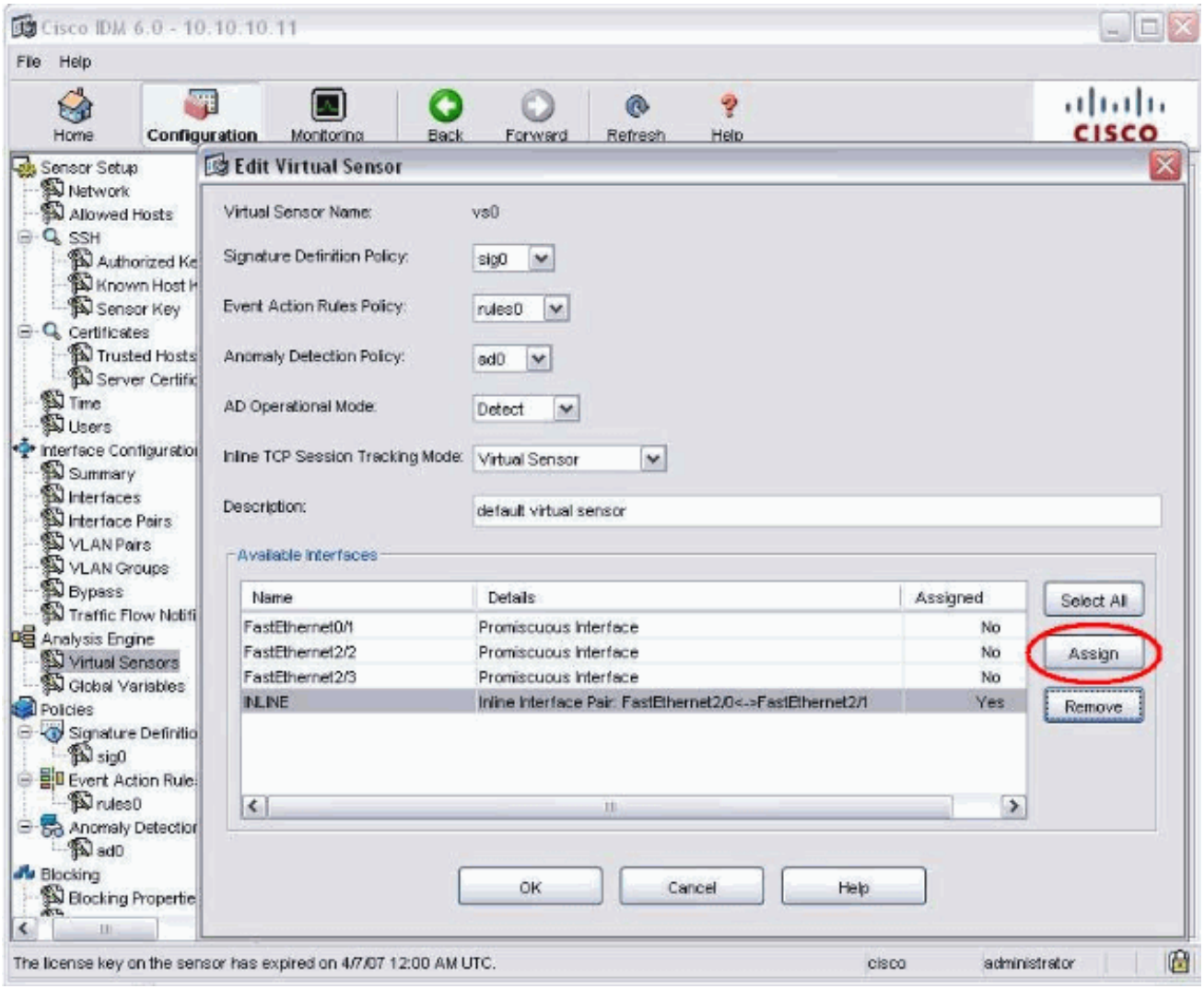
8. Просмотрите сводку Встроенной Парной Конфигурации и примените его.



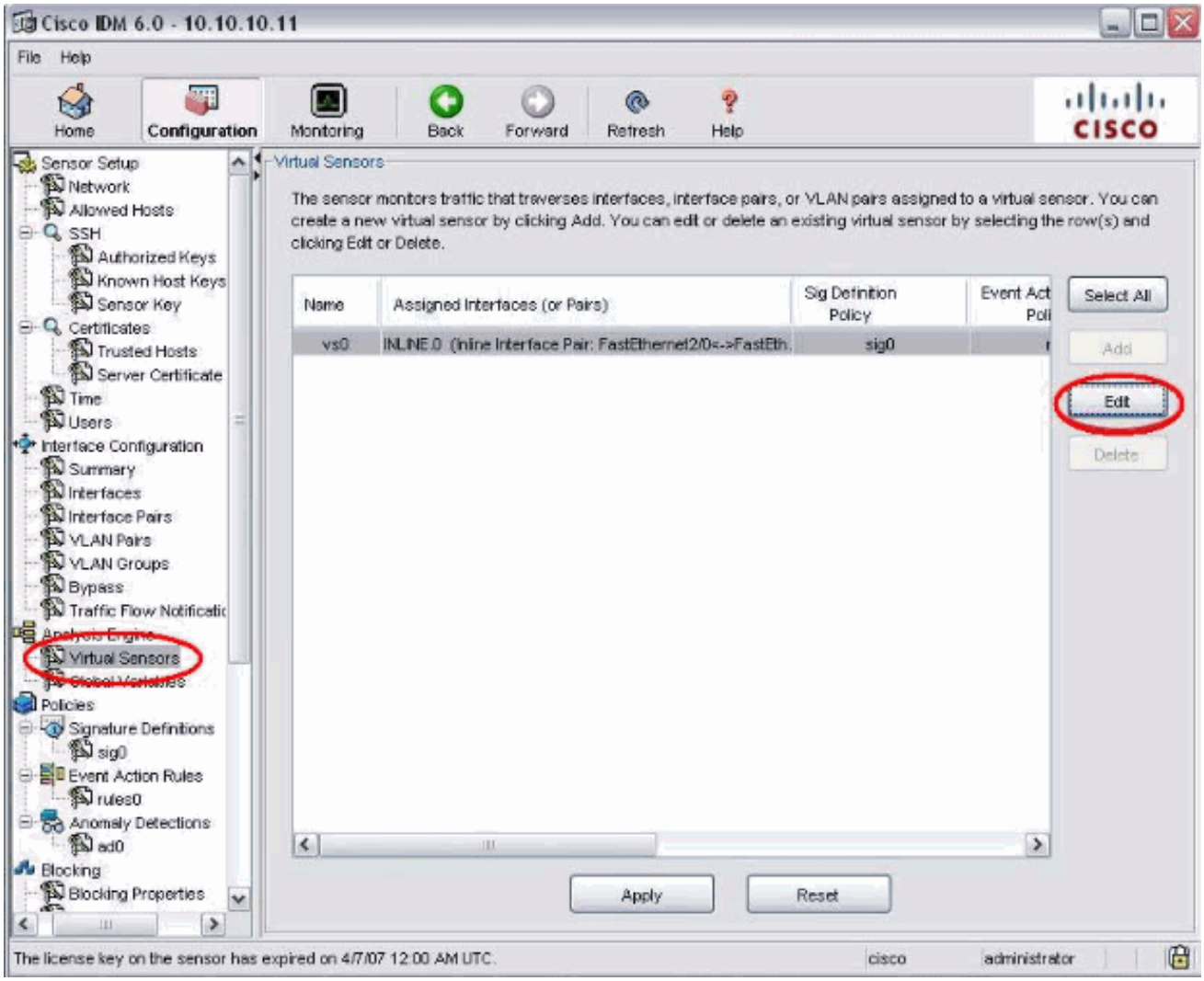
9. Перейдите **к Конфигурации> Аналитический Механизм> Действительный Датчик** и нажмите **Edit** для создания нового действительного датчика.



10. Назначьте Встроенную пару, **ВСТРОЕННУЮ** на Действительный Датчик vs0.



11. Просмотрите сводку назначенной действительной информации о датчике.



Настройте коммутатор для IDSM-2 во встроенном режиме

См. Настройку Серии Catalyst 6500 Коммутаторов для IDSM-2 во Встроенном Выборе режима IDSM-2 Настройки для настройки коммутатора для IDSM-2 встраивают режим.

Устранение неполадок

Проблема

Если IPS отказывает, и он настроен встроенный, сделайте открытый сбой интерфейсов (трафик продолжает проходить), или закрытый (трафик отброшен).

Решение

Можно настроить IPS в открытом состоянии сбоя. Таким образом, если сбои IPS, это продолжит передавать трафик, но это не будет контролировать трафик.

Дополнительные сведения

- CISCO ASA 5500 SERIES ADAPTIVE SECURITY APPLIANCES

- Cisco Intrusion Prevention System
- Cisco IPS 4200 Series Sensors
- Cisco Systems – техническая поддержка и документация