IPS 6.X 이상/IDSM2:IDM 컨피그레이션 예를 사용하는 인라인 인터페이스 쌍 모드

목차

소개

Inline Interface Pair 모드에서 작동하면 IPS(Intrusion Prevention System)가 트래픽 흐름에 직접 영향을 미치며 패킷 전달 속도에 영향을 미치므로 레이턴시가 추가될 때 속도가 느려집니다.이렇게 하면 센서가 공격을 중지하여 목적지 대상에 도달하기 전에 악성 트래픽을 삭제하여 보호 서비스를 제공합니다.레이어 3 및 4의 인라인 디바이스 처리 정보뿐만 아니라, 더 정교한 임베디드 공격을 위해 패킷의 내용과 페이로드도 분석합니다(레이어 3~7). 이 심층적인 분석을 통해 시스템은 일반적으로 기존 방화벽 디바이스를 통과하는 공격을 식별, 차단 및 차단할 수 있습니다.

Inline Interface Pair(인라인 인터페이스 쌍) 모드에서는 센서에서 쌍의 첫 번째 인터페이스를 통해 패킷이 들어오고 쌍의 두 번째 인터페이스를 나갑니다.패킷이 시그니처에 의해 거부되거나 수정되지 않는 한 패킷은 쌍의 두 번째 인터페이스로 전송됩니다.

참고: 이러한 모듈에는 하나의 센싱 인터페이스만 있는 경우에도 인라인으로 작동하도록 AIM-IPS 및 AIP-SSM을 구성할 수 있습니다.

참고: 페어링된 인터페이스가 동일한 스위치에 연결된 경우 두 포트에 대해 액세스 VLAN이 서로 다른 액세스 포트로 스위치에서 구성해야 합니다.그렇지 않으면 트래픽이 인라인 인터페이스를 통해 전달되지 않습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 명령줄 인터페이스 6.0 및 IDM(Intrusion Prevention System Device Manager) 6.0을 사용하는 Cisco IPS Sensor를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

관련 제품

이 문서의 정보는 IDSM-2(Intrusion Detection System) 서비스 모듈에도 적용됩니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

인라인 인터페이스 쌍 구성

인라인 인터페이스 **쌍을** 생성하려면 서비스 인터페이스 하위 모드에서 inline-interfaces name 명령을 사용합니다.

참고: 이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 명령 조회 도구(등록된 고객만 해당)를 사용하십시오.

참고: AIP-SSM은 Cisco IPS CLI가 아닌 Cisco ASA CLI에서 인라인 인터페이스 모드로 구성됩니다.

다음 옵션이 적용됩니다.

- **inline-interfaces** ***name*****—**논리적 인라인 인터페이스 쌍의 이름입니다.**참고:** 모든 모듈(IDSM-2 NM-CIDS 및 AIP-SSM)의 모든 백플레인 센싱 인터페이스에서 **admin-state**는 enabled로 설정되고 보호됩니다(설정을 변경할 수 없음). admin **상태**는 명령 및 제어 인터페이스에 영향을 미치지 않으며 보호됩니다.센싱 인터페이스에만 영향을 미칩니다.명령 및 제어 인터페이스는 모니터링할 수 없으므로 활성화할 필요가 없습니다.
- **default** - 값을 시스템 기본 설정으로 다시 설정합니다.
- **description** - 인라인 인터페이스 쌍에 대한 설명입니다.
- **interface1** *interface_name* - 인라인 인터페이스 쌍의 첫 번째 인터페이스입니다.
- **interface2** *interface_name* - 인라인 인터페이스 쌍의 두 번째 인터페이스입니다.
- **no** - 항목 또는 선택 설정을 제거합니다.
- **관리 상태 {활성화됨 | disabled}—**인터페이스의 관리 링크 상태(인터페이스가 활성화되었는지 비활성화되었는지 여부)입니다.

CLI 컨피그레이션

센서에서 인라인 VLAN 쌍 설정을 구성하려면 다음 단계를 완료합니다.

1. 관리자 권한이 있는 계정으로 CLI에 로그인합니다.
2. 인터페이스 하위 모드를 입력합니다.
```
sensor#configure terminal
sensor(config)#service interface
sensor(config-int)#
```
3. 인라인 인터페이스가 있는지 확인합니다.인라인 인터페이스가 구성되지 않은 경우 하위 인터페이스 유형 `none`을 읽어야 합니다.
```
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. 인라인 쌍의 이름을 지정합니다.

```
sensor(config-int)#inline-interfaces PAIR1
```

5. 사용 가능한 인터페이스 목록을 표시합니다.

```
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. 두 인터페이스를 한 쌍으로 구성합니다.

```
sensor(config-int)#interface1 GigabitEthernet0/0



sensor(config-int-inl)#interface2 GigabitEthernet0/1
```

가상 센서가 트래픽을 모니터링하려면 먼저 인터페이스를 가상 센서에 할당하고 활성화해야 합니다.자세한 내용은 10단계를 참조하십시오.

7. 이 인터페이스에 대한 설명을 추가합니다.

```
sensor(config-int-phy)#description PAIR1 Gig0/0 and Gig0/1
```

8. 인라인 인터페이스 쌍으로 구성할 다른 인터페이스에 대해 4~7단계를 반복합니다.
9. 설정을 확인합니다.

```
sensor(config-int-inl)#show settings
   name: PAIR1
   ------------------------------------------------
      description: PAIR1 Gig0/0 & Gig0/1 default:
      interface1: GigabitEthernet0/0
      interface2: GigabitEthernet0/1
   ------------------------------------------------
```

10. 인터페이스 쌍에 할당된 인터페이스를 활성화합니다.

```
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. 인터페이스가 활성화되었는지 확인합니다.

```
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. 인라인 인터페이스 쌍을 삭제하고 인터페이스를 프로미스큐어스 모드로 되돌리려면 다음 명

령을 실행합니다.

```
sensor(config-int)#no inline-interfaces PAIR1
```

또한 인라인 인터페이스 쌍을 할당된 가상 센서에서 삭제해야 합니다.

13. 인라인 인터페이스 쌍이 삭제되었는지 확인합니다.

```
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. 인터페이스 구성 하위 모드 종료:

```
sensor(config-int)#exit
Apply Changes:?[yes]:
```

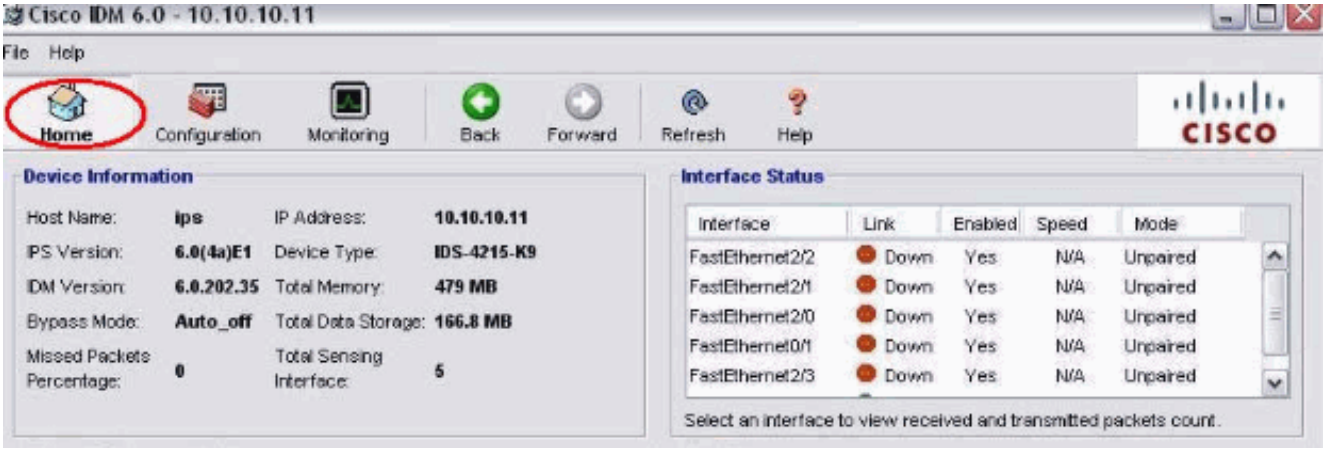
15. Enter를 눌러 변경 사항을 적용하거나 no를 입력하여 취소합니다.

IDM 구성

IDM을 사용하여 센서에서 인라인 VLAN 쌍 설정을 구성하려면 다음 단계를 완료합니다.

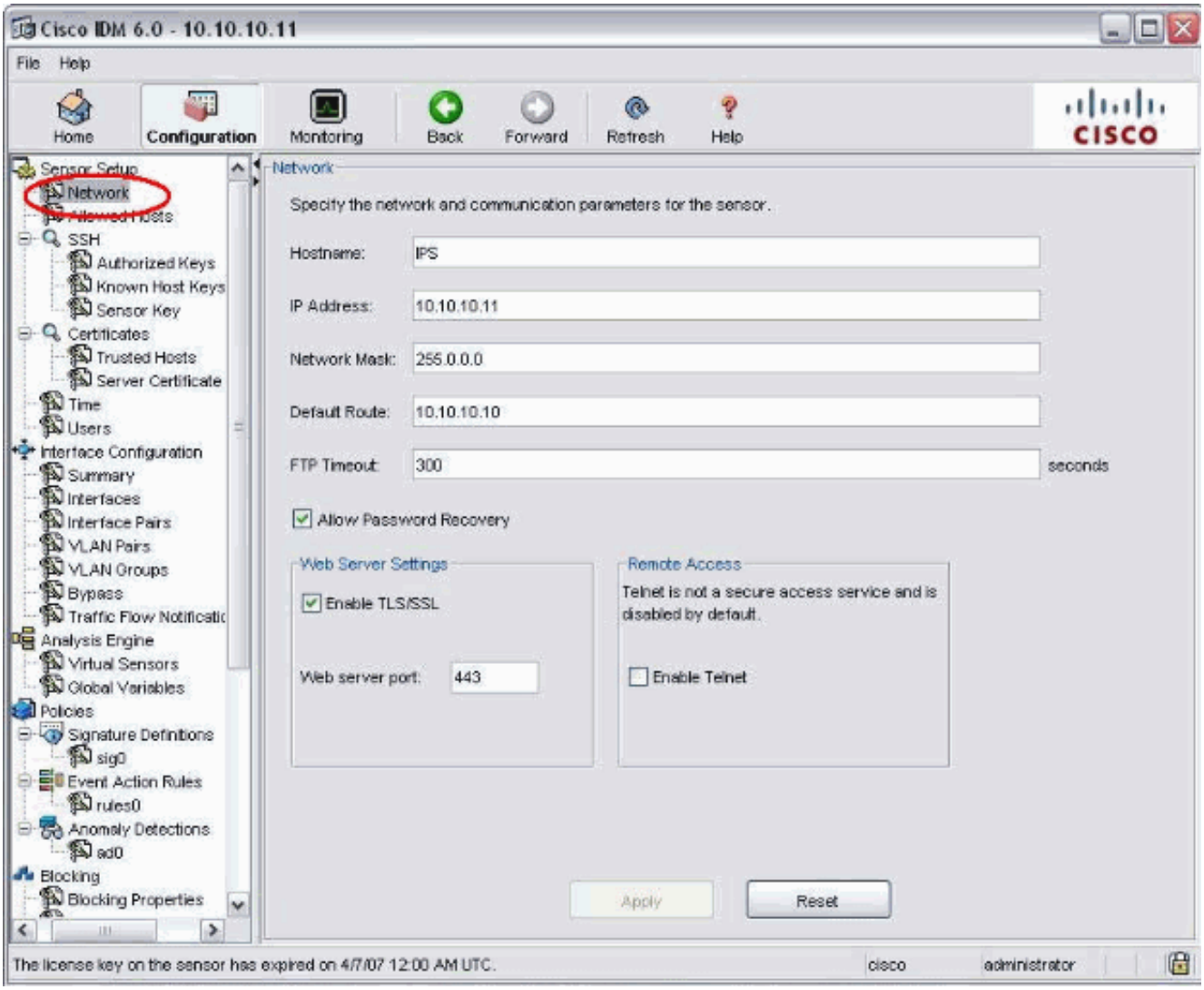
1. 브라우저를 열고 **https://<Management_IP_Address_of_IPS>를 입력하여** IPS에서 IDM에 액세스합니다.
2. IDM **Launcher 다운로드** 및 **IDM 시작**을 클릭하여 응용 프로그램의 설치 프로그램을 다운로드합니다.
3. 호스트 이름, IP 주소, 버전 및 모델과 같은 디바이스 정보를 보려면 홈 페이지로 이동합니다

.



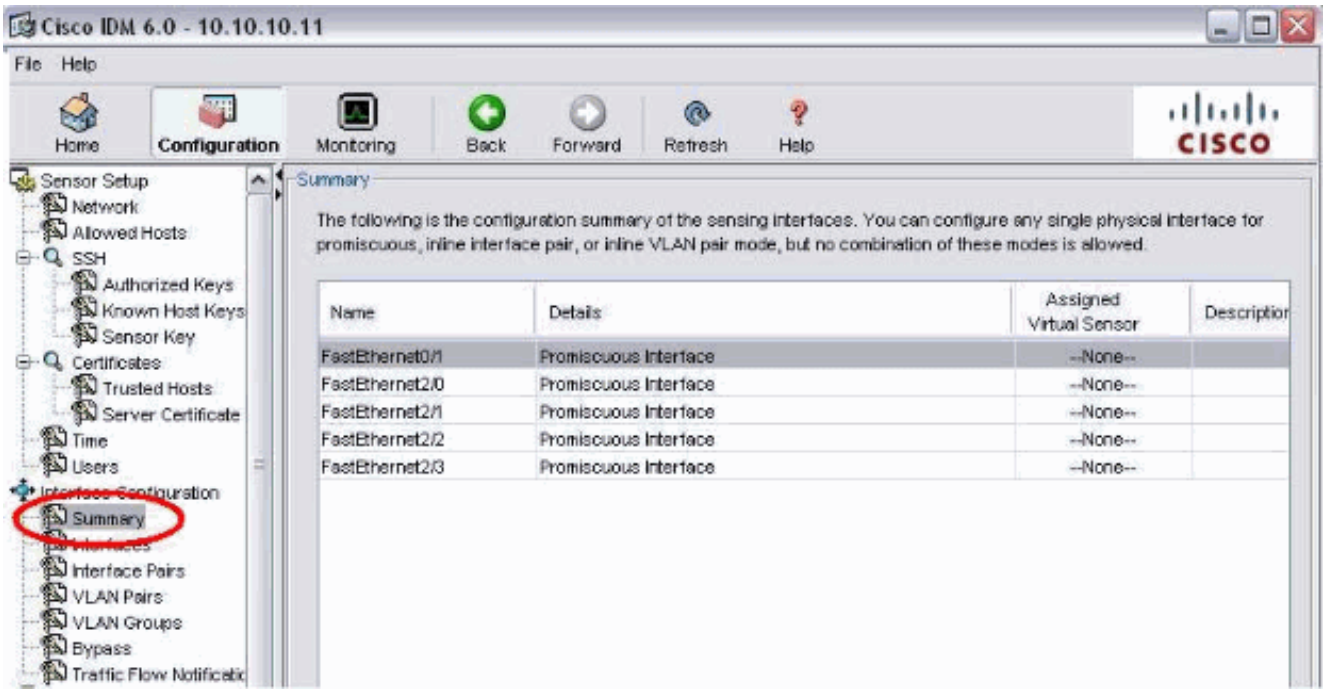
4. Configuration(컨피그레이션) > **Sensor Setup(센서 설정)**으로 이동하고 **Network(네트워크)**를 클릭합니다.여기서 호스트 이름, IP 주소 및 기본 경로를 지정할 수 있습니다

.



5. Configuration(컨피그레이션) > **Interface Configuration(인터페이스 컨피그레이션)**으로 이동하고 **Summary(요약)**를 클릭합니다.이 페이지에는 센싱 인터페이스의 컨피그레이션 요약이 표시됩니다

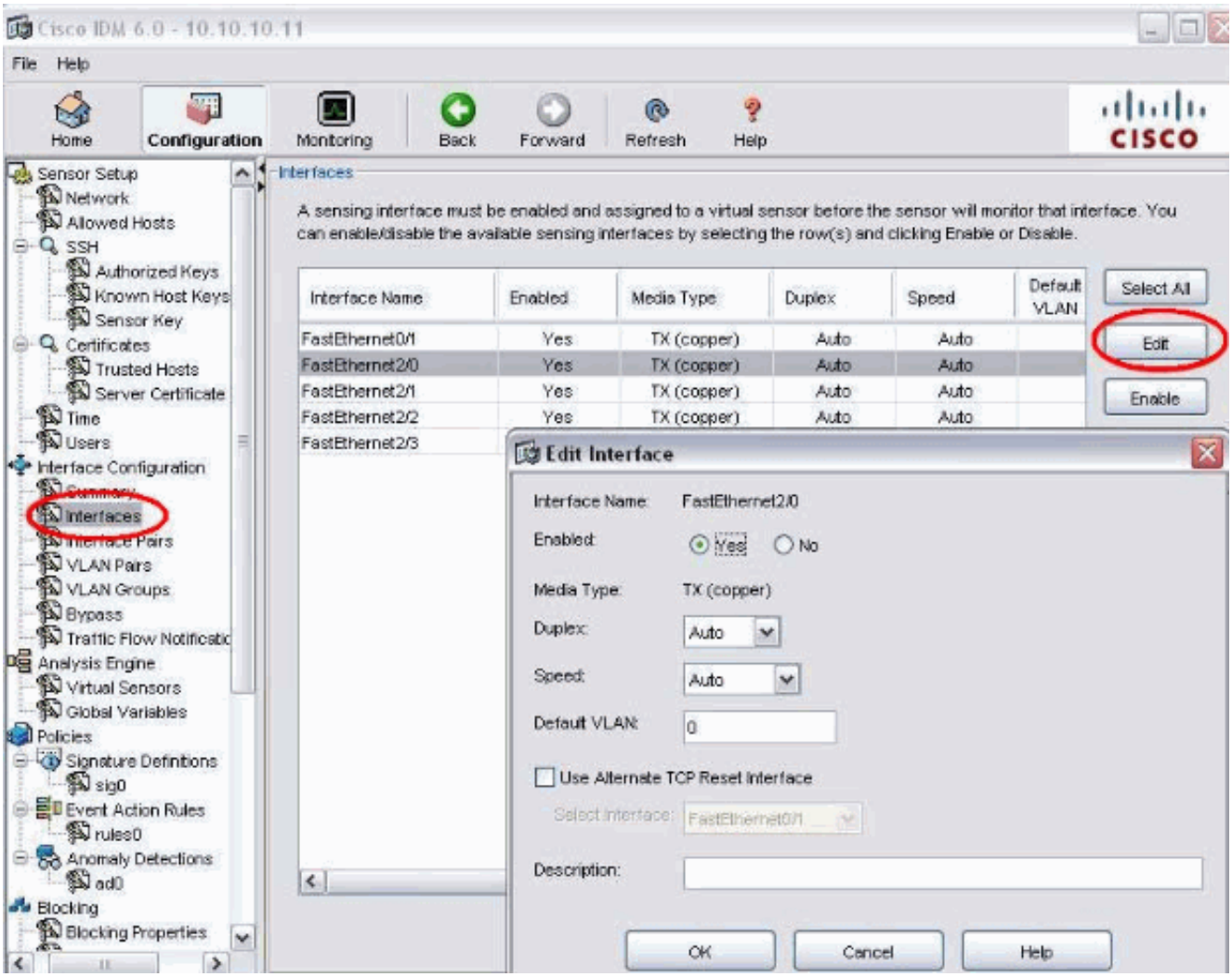
.



6. Configuration(컨피그레이션) > **Interface Configuration(인터페이스 컨피그레이션) > Interfaces(인터페이스)**로 이동하여 인터페이스 이름을 선택합니다.그런 다음 **Enable(활성화**

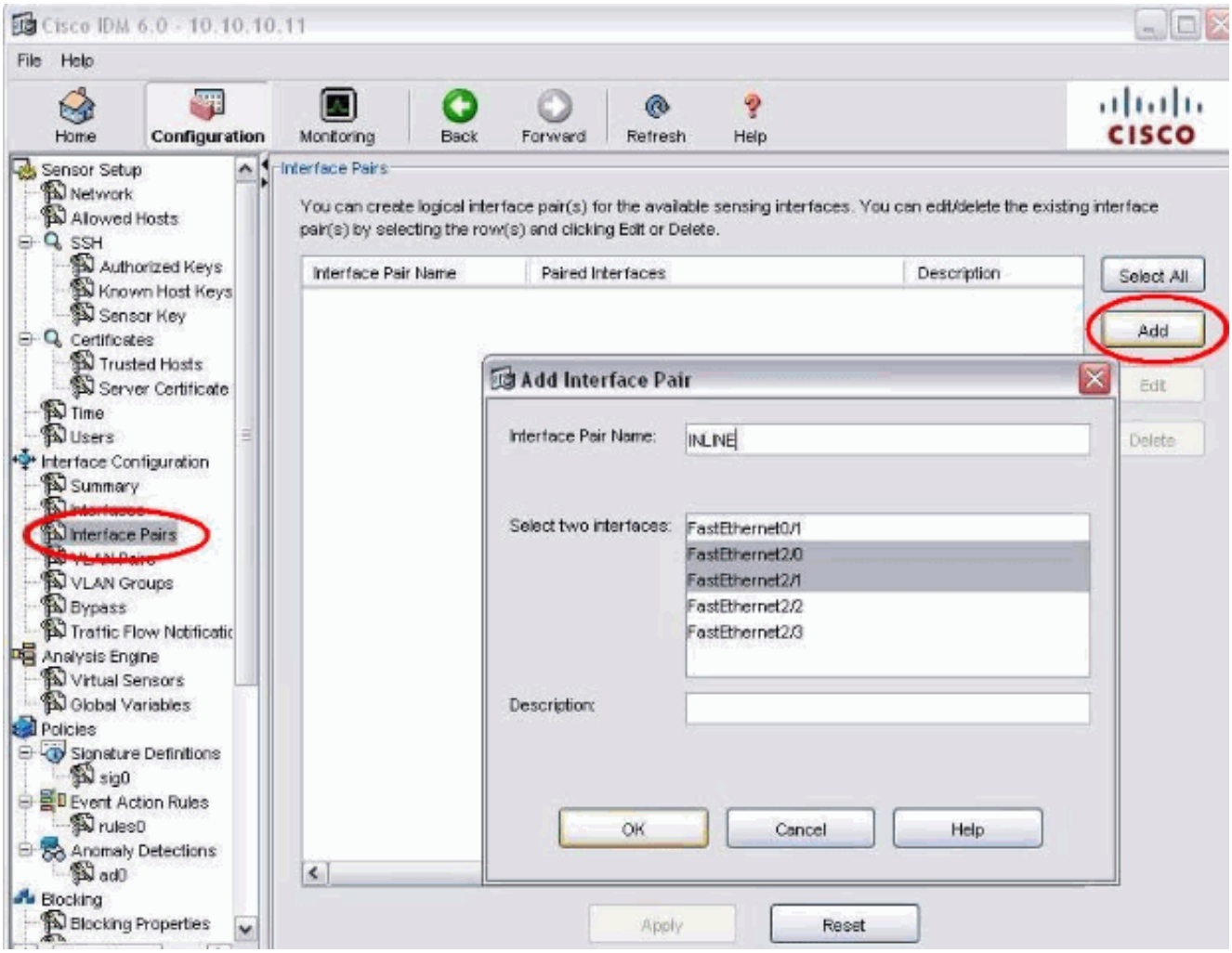
)을 클릭하여 센싱 인터페이스를 활성화합니다.또한 듀플렉스, 속도 및 VLAN 정보를 구성합니다

.



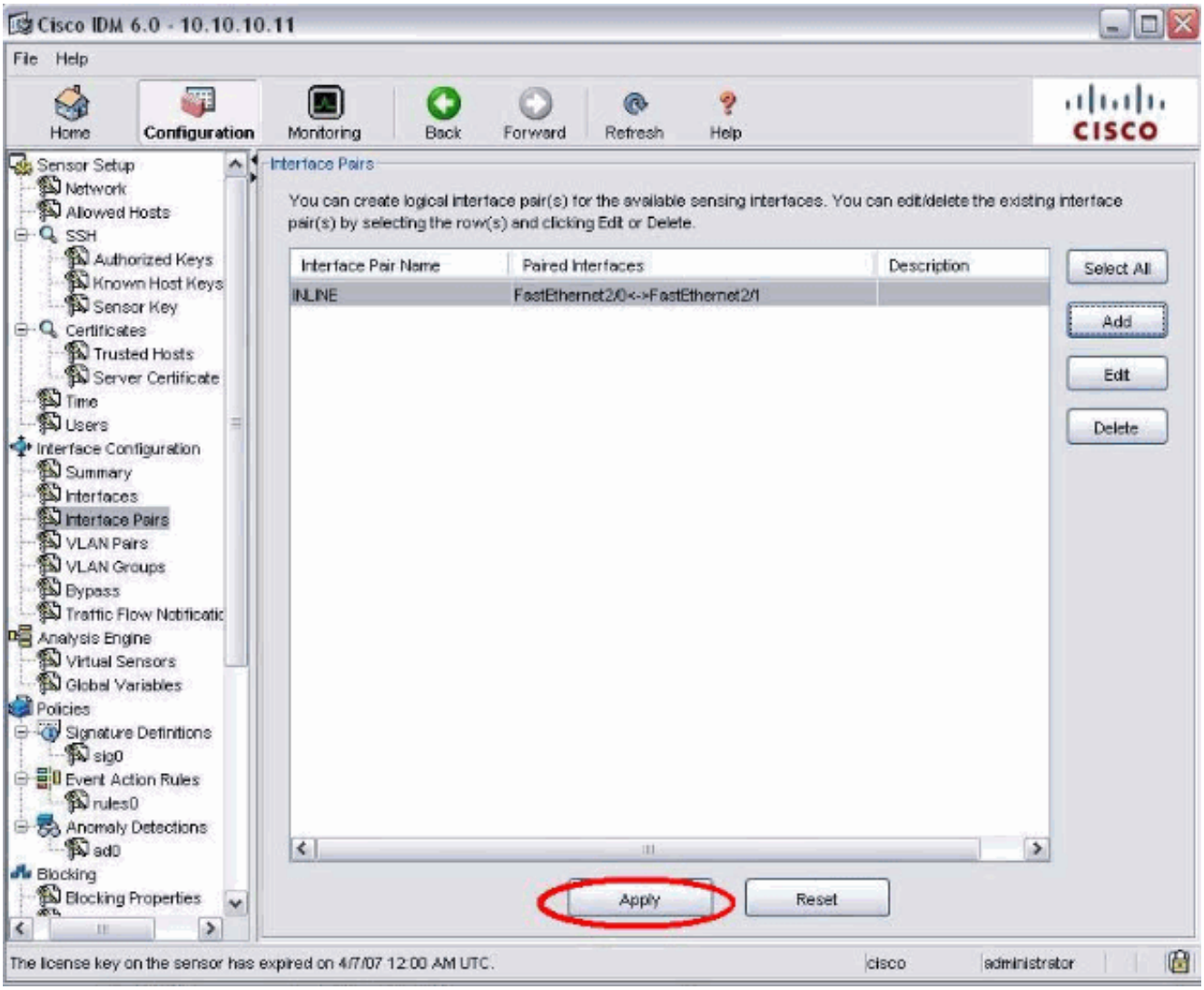
7. Configuration(컨피그레이션) > **Interface Configuration(인터페이스 컨피그레이션) > Interface Pairs(인터페이스 쌍)**로 이동하고 **Add(추가)**를 클릭하여 인라인 쌍을 생성합니다

.



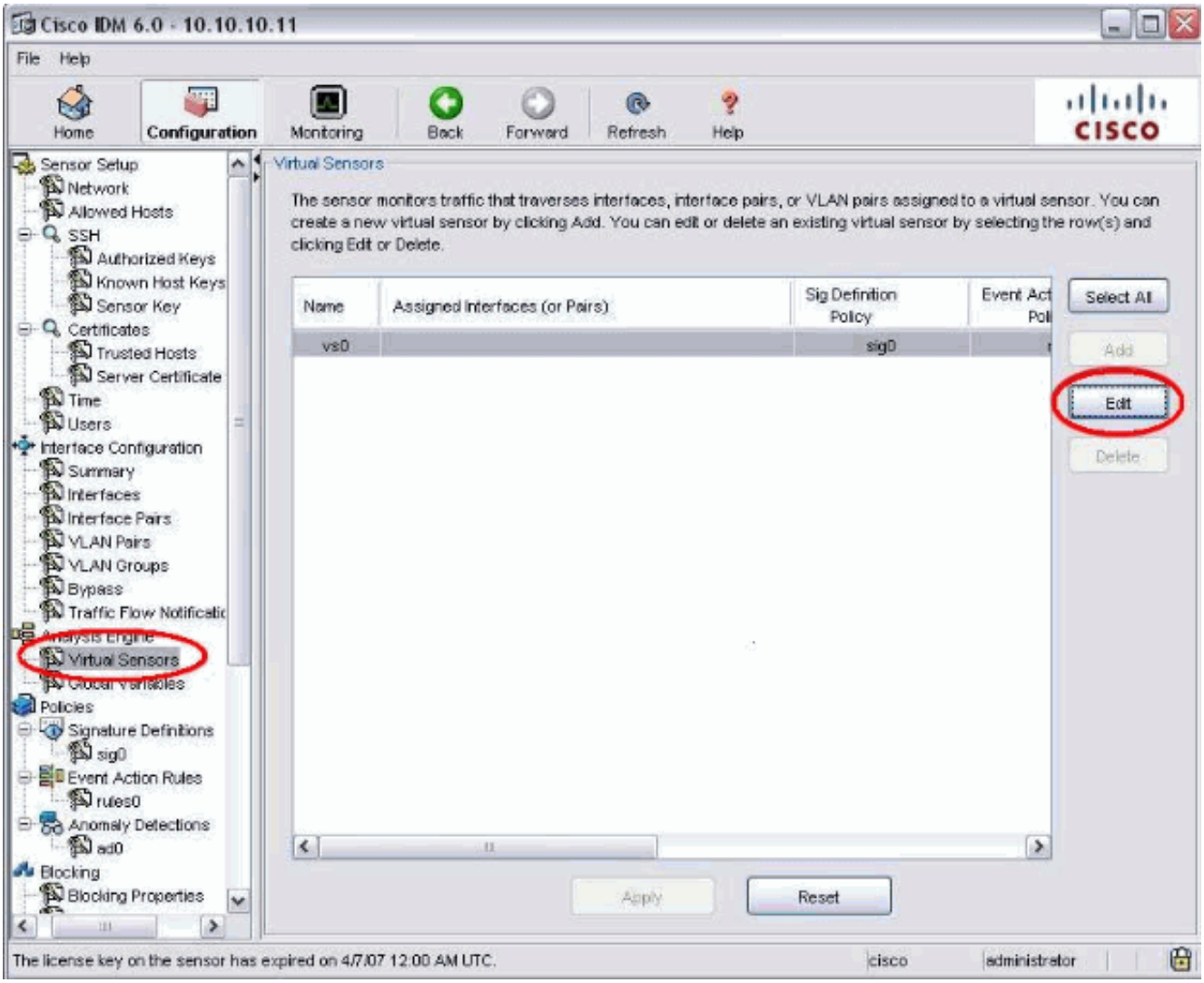
8. 인라인 쌍 구성의 요약을 보고 적용합니다

.



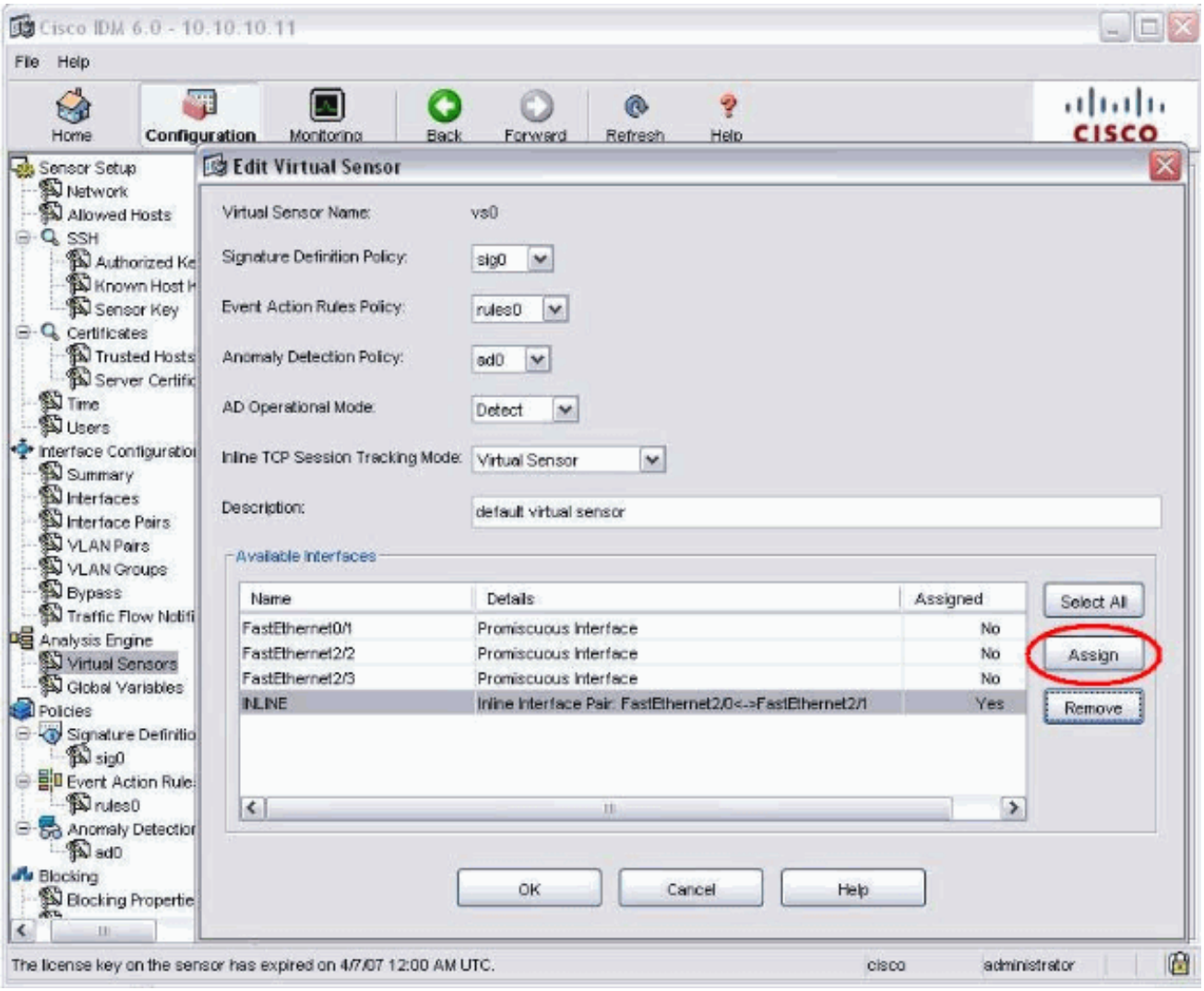
9. Configuration(컨피그레이션) > **Analysis Engine(분석 엔진) > Virtual Sensor(가상 센서)로** 이동하고 **Edit(편집)**를 클릭하여 새 가상 센서를 생성합니다

.



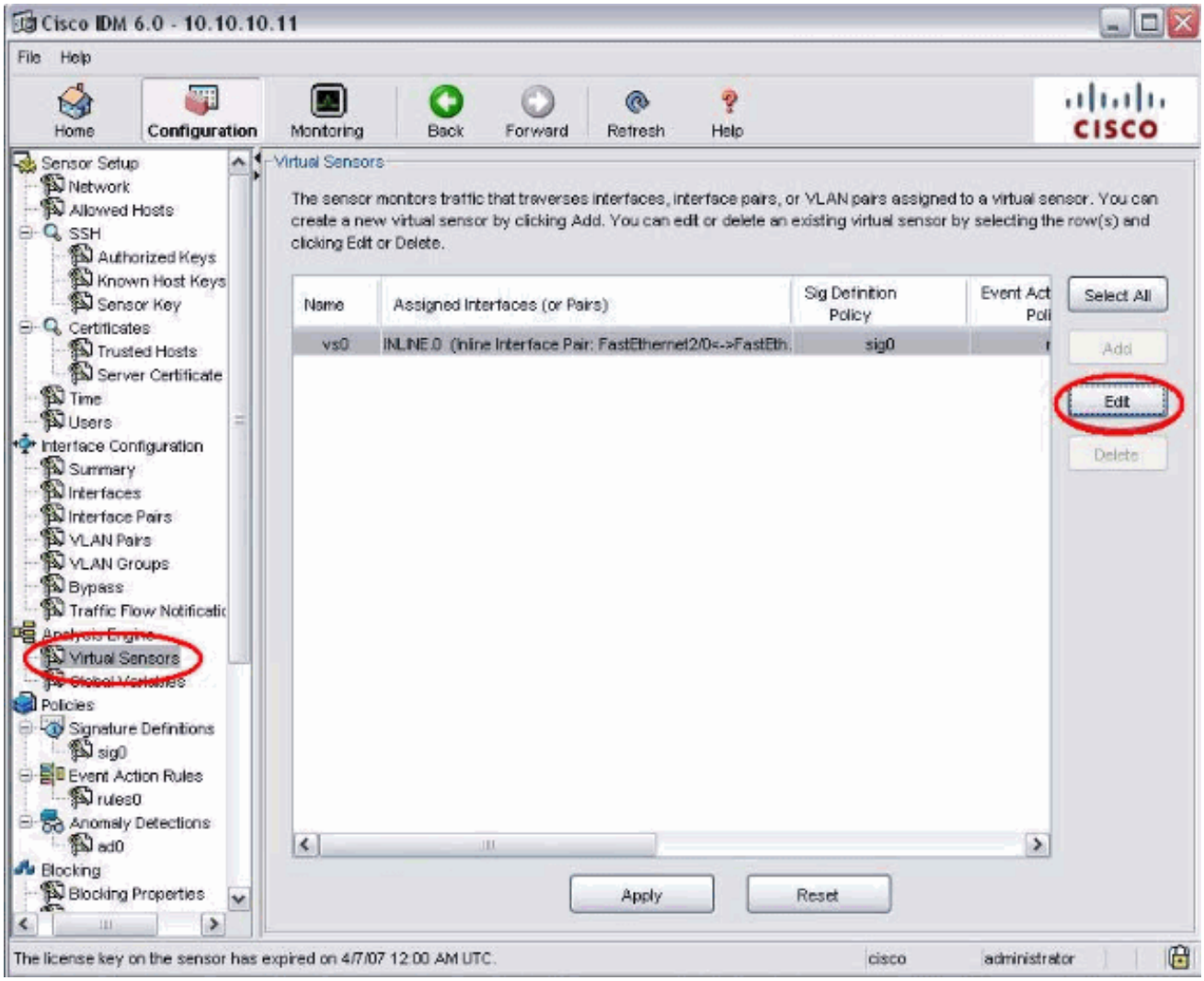
10. 인라인 쌍을 가상 센서 vs0에 할당합니다

.



11. 할당된 가상 센서 정보의 요약을 봅니다

.



인라인 모드에서 IDSM-2용 스위치 구성

IDSM-2 인라인 모드에 대한 스위치를 구성하려면 IDSM-2 구성의 인라인 모드에서 IDSM-2에 대한 Catalyst Series 6500 스위치 구성 섹션을 참조하십시오.

문제 해결

문제

IPS가 실패하고 인라인으로 구성된 경우 인터페이스가 fail open(트래픽이 계속 전달) 또는 닫힘(트래픽이 삭제됨)을 수행합니까?

솔루션

IPS를 fail-open 상태로 구성할 수 있습니다.따라서 IPS에 장애가 발생하면 트래픽은 계속 전달되지만 트래픽은 모니터링하지 않습니다.

관련 정보

- Cisco ASA 5500 Series Adaptive Security Appliance

- Cisco 침입 방지 시스템
- Cisco IPS 4200 Series 센서
- 기술 지원 및 문서 – Cisco Systems