무선 LAN 컨트롤러 및 IPS 통합 가이드

목차

소개

Cisco IDS(Unified Intrusion Detection System)/IPS(Intrusion Prevention System)는 Cisco Self-Defending Network의 일부이며 업계에서 최초로 통합된 유무선 보안 솔루션입니다.Cisco Unified IDS/IPS는 무선 에지, 유선 에지, WAN 에지 및 데이터 센터를 통해 포괄적인 보안 접근 방식을 사용합니다.연결된 클라이언트가 Cisco Unified Wireless Network를 통해 악성 트래픽을 전송하면, Cisco 유선 IDS 장치는 공격을 탐지하고 차단 요청을 Cisco WLC(Wireless LAN Controller)에 보낸 다음 클라이언트 장치의 연결을 해제합니다.

Cisco IPS는 비즈니스 연속성에 영향을 미치기 전에 버그, 스파이웨어/애드웨어, 네트워크 바이러스, 애플리케이션 오용 등 악성 트래픽을 정확하게 식별, 분류 및 중단하도록 설계된 네트워크 기반 인라인 솔루션입니다.

Cisco IPS 솔루션은 Cisco IPS Sensor 소프트웨어 버전 5의 활용과 함께 인라인 방지 서비스와 혁

신적인 기술을 결합하여 정확성을 높입니다.그 결과 합법적인 트래픽이 중단되는 것에 대한 두려움 없이 IPS 솔루션의 보호 기능을 완벽하게 보장할 수 있습니다.또한 Cisco IPS 솔루션은 다른 네트워크 보안 리소스와 협업할 수 있는 고유한 기능을 통해 네트워크를 포괄적으로 보호하고 네트워크 보호에 대한 사전 대응적 접근 방식을 제공합니다.

Cisco IPS 솔루션은 다음과 같은 기능을 사용하여 더 확실하게 위협을 차단할 수 있도록 지원합니다.

- **정확한 인라인 방지 기술**—합법적인 트래픽 삭제 위험 없이 더 광범위한 위협에 대한 예방 조치를 취할 수 있는 탁월한 자신감을 제공합니다.이러한 고유한 기술은 지능적이고 자동화된 상황 분석을 제공하여 침입 방지 솔루션을 최대한 활용할 수 있도록 지원합니다.
- **멀티 벡터 위협 식별** - 레이어 2~7에서 트래픽을 자세히 검사하여 정책 위반, 취약성 악용 및 비정상적인 활동으로부터 네트워크를 보호합니다.
- **고유한 네트워크 협업**—효율적인 트래픽 캡처 기술, 로드 밸런싱 기능, 암호화된 트래픽에 대한 가시성 등 네트워크 협업을 통해 확장성과 복원력을 향상시킵니다.
- **포괄적인 구축 솔루션**—SMB(중소기업) 및 지사에서 대기업 및 통신 사업자 설치에 이르는 모든 환경에 적합한 솔루션을 제공합니다.
- **강력한 관리, 이벤트 상관관계 및 지원 서비스**—구성, 관리, 데이터 상관관계, 고급 지원 서비스를 포함한 완벽한 솔루션을 구현합니다.특히 Cisco MARS(Security Monitoring, Analysis, and Response System)는 네트워크 전반의 침입 방지 솔루션을 위해 문제의 요소를 식별, 격리 및 제거할 것을 권장합니다.또한 Cisco Incident Control System은 네트워크를 신속하게 적응하고 분산형 대응을 제공함으로써 새로운 WORM 및 바이러스 침투를 방지합니다.

이러한 요소를 결합하면 포괄적인 인라인 방지 솔루션을 제공하며 비즈니스 연속성에 영향을 미치기 전에 가장 광범위한 악성 트래픽을 탐지하고 차단할 수 있는 확신을 제공합니다.Cisco Self-Defending Network 이니셔티브는 네트워크 솔루션을 위한 통합 및 내장 보안을 요구합니다.현재 LWAPP(Lightweight Access Point Protocol) 기반 WLAN 시스템은 기본적으로 레이어 2 시스템이며 제한된 라인 처리 능력을 갖추고 있기 때문에 기본 IDS 기능만 지원합니다.Cisco는 새로운 코드에 향상된 새로운 기능을 포함하기 위해 적시에 새로운 코드를 릴리스합니다.릴리스 4.0에는 LWAPP 기반 WLAN 시스템과 Cisco IDS/IPS 제품 라인의 통합이 포함된 최신 기능이 있습니다.이번 릴리스의 목표는 Cisco IDS/IPS 시스템이 특정 클라이언트가 무선 네트워크에 액세스하는 것을 차단하도록 WLC에 지시하는 것입니다. 이 때 클라이언트 관련 공격이 레이어 3에서 레이어 7까지 탐지될 경우 이를 차단합니다.

사전 요구 사항

요구 사항

다음과 같은 최소 요구 사항을 충족해야 합니다.

- WLC 펌웨어 버전 4.x 이상
- Cisco IPS 및 Cisco WLC를 구성하는 방법에 대한 지식이 필요합니다.

사용되는 구성 요소

Cisco WLC

이러한 컨트롤러는 IDS 수정을 위해 소프트웨어 릴리스 4.0에 포함되어 있습니다.

- Cisco 2000 Series WLC

- Cisco 2100 Series WLC
- Cisco 4400 Series WLC
- Cisco Wireless Services Module(WiSM)
- Cisco Catalyst 3750G Series Unified Access Switch
- Cisco WLCM(Wireless LAN Controller Module)

액세스 포인트

- Cisco Aironet 1100 AG Series Lightweight 액세스 포인트
- Cisco Aironet 1200 AG Series Lightweight 액세스 포인트
- Cisco Aironet 1300 Series Lightweight 액세스 포인트
- Cisco Aironet 1000 Series Lightweight 액세스 포인트

관리

- Cisco WCS(Wireless Control System)
- Cisco 4200 Series 센서
- Cisco IDS Management - Cisco IDS Device Manager(IDM)

Cisco Unified IDS/IPS 플랫폼

- Cisco IPS 4200 Series Sensor 및 Cisco IPS Sensor Software 5.x 이상
- Cisco ASA 5500 Series Adaptive Security Appliance용 SSM10 및 SSM20(Cisco IPS Sensor Software 5.x 포함)
- Cisco ASA 5500 Series Adaptive Security Appliances with Cisco IPS Sensor Software 5.x
- Cisco IPS Sensor Software 5.x가 포함된 Cisco IDS Network Module(NM-CIDS)
- Cisco Catalyst 6500 Series IDSM-2(Intrusion Detection System Module 2) with Cisco IPS Sensor Software 5.x

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.

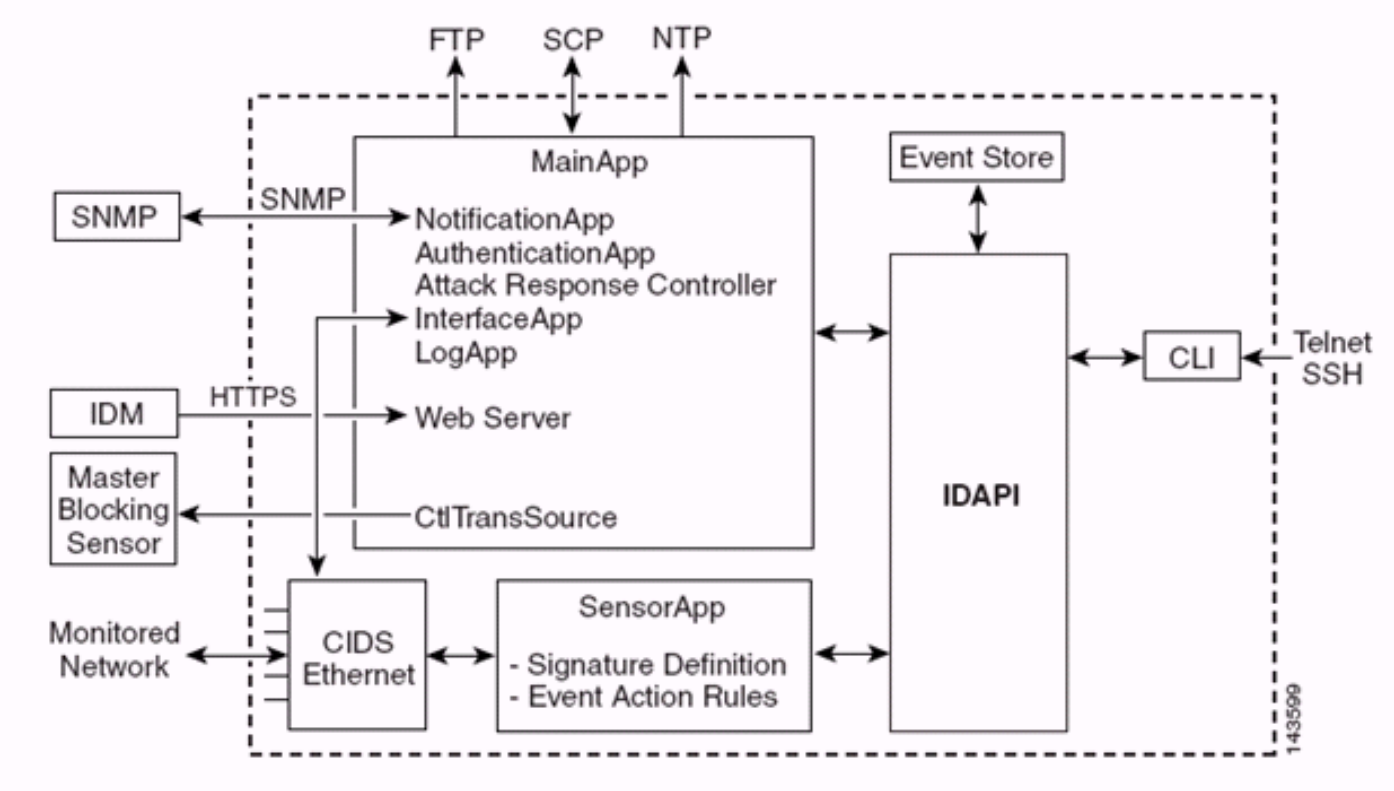
표기 규칙

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

Cisco IDS 개요

Cisco IDS(버전 5.0)의 주요 구성 요소는 다음과 같습니다.

- **Sensor App** - 패킷 캡처 및 분석을 수행합니다.
- **Event Storage Management and Actions Module(이벤트 스토리지 관리 및 작업 모듈)** - 정책 위반 저장을 제공합니다.
- **Imaging, Install and Startup Module(이미징, 설치 및 시작 모듈)** - 모든 시스템 소프트웨어를 로드, 초기화 및 시작합니다.
- **User Interfaces and UI Support Module(사용자 인터페이스 및 UI 지원 모듈)** - 내장된 CLI 및 IDM을 제공합니다.
- **센서 OS** - 호스트 운영 체제(Linux 기반).



센서 애플리케이션(IPS 소프트웨어)은 다음과 같이 구성됩니다.

- **Main App**(기본 앱) - 시스템을 초기화하고, 다른 애플리케이션을 시작 및 중지하고, OS를 구성하고, 업그레이드를 담당합니다.여기에는 다음 구성 요소가 포함됩니다.**Control Transaction Server(제어 트랜잭션 서버)** - 센서가 Attack Response Controller(이전의 Network Access Controller) Master Blocking Sensor 기능을 활성화하는 데 사용되는 제어 트랜잭션을 전송할 수 있습니다.**이벤트 저장소** - CLI, IDM, ASDM(Adaptive Security Device Manager) 또는 RDEP(Remote Data Exchange Protocol)를 통해 액세스할 수 있는 IPS 이벤트(오류, 상태 및 경고 시스템 메시지)를 저장하는 데 사용되는 인덱스 저장소입니다.
- **Interface App**(인터페이스 앱) - 바이패스 및 물리적 설정을 처리하고 페어링된 인터페이스를 정의합니다.물리적 설정은 속도, 이중 및 관리 상태로 구성됩니다.
- **Log App**(로그 앱) - 애플리케이션의 로그 메시지를 로그 파일에 기록하고 오류 메시지를 이벤트 저장소에 기록합니다.
- **ARC(Attack Response Controller)(이전 명칭: Network Access Controller)**—원격 네트워크 디바이스(방화벽, 라우터, 스위치)를 관리하여 경고 이벤트가 발생할 때 차단 기능을 제공합니다.ARC는 제어 네트워크 디바이스에 ACL(Access Control List)을 생성 및 적용하거나 shun 명령(방화벽)을 사용합니다.
- **Notification App**(알림 앱) - 알림, 상태 및 오류 이벤트에 의해 트리거될 때 SNMP 트랩을 전송합니다.알림 앱은 이를 위해 공용 도메인 SNMP 에이전트를 사용합니다.SNMP GET은 센서의 상태에 대한 정보를 제공합니다.**웹 서버(HTTP RDEP2 서버)** - 웹 사용자 인터페이스를 제공합니다.또한 IPS 서비스를 제공하기 위해 여러 서블릿을 사용하여 RDEP2를 통해 다른 IPS 디바이스와 통신할 수 있는 수단을 제공합니다.**Authentication App**(인증 앱) - 사용자가 CLI, IDM, ASDM 또는 RDEP 작업을 수행할 권한이 있는지 확인합니다.
- **Sensor App (Analysis Engine)** - 패킷 캡처 및 분석을 수행합니다.
- **CLI** - 사용자가 텔넷 또는 SSH를 통해 센서에 성공적으로 로그인할 때 실행되는 인터페이스입니다.CLI를 통해 생성된 모든 어카운트는 CLI를 셸로 사용합니다(서비스 어카운트 제외 - 서비스 어카운트는 하나만 허용됨). 허용되는 CLI 명령은 사용자의 권한에 따라 다릅니다.

모든 IPS 애플리케이션은 IDAPI라는 공통 API(Application Program Interface)를 통해 서로 통신합니다.원격 애플리케이션(기타 센서, 관리 애플리케이션 및 타사 소프트웨어)은 RDEP2 및

SDEE(Security Device Event Exchange) 프로토콜을 통해 센서와 통신합니다.

센서에 다음과 같은 디스크 파티션이 있습니다.

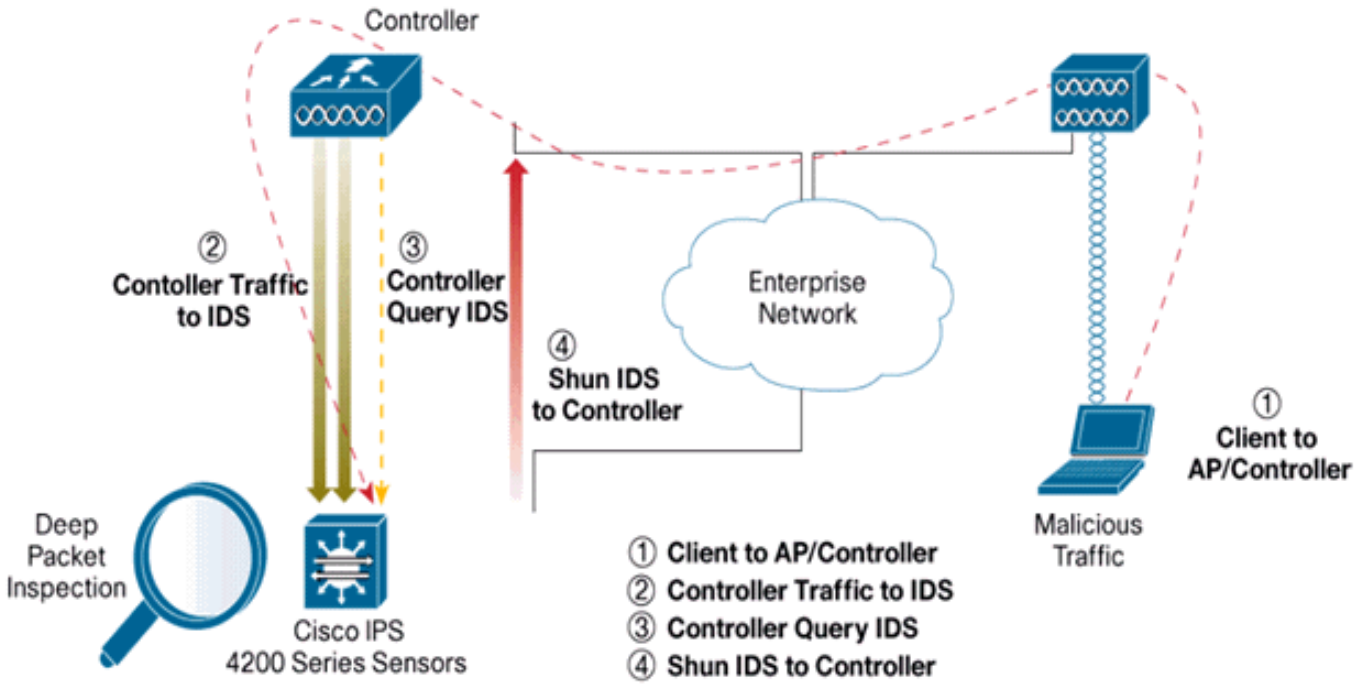
- **Application Partition(애플리케이션 파티션)** - 전체 IPS 시스템 이미지를 포함합니다.
- **유지 관리 파티션** - IDSM-2의 응용 프로그램 파티션을 다시 이미징하는 데 사용되는 특수 목적의 IPS 이미지입니다. 유지 관리 파티션의 이미지를 다시 적용하면 구성 설정이 손실됩니다.
- **복구 파티션** - 센서 복구에 사용되는 특수 용도 이미지입니다.복구 파티션으로 부팅하면 사용자가 애플리케이션 파티션을 완전히 다시 이미지화할 수 있습니다.네트워크 설정은 유지되지만 다른 모든 컨피그레이션은 손실됩니다.

Cisco IDS 및 WLC - 통합 개요

Cisco IDS 버전 5.0에는 정책 위반(서명)이 탐지될 때 거부 작업을 구성하는 기능이 도입되었습니다.IDS/IPS 시스템의 사용자 컨피그레이션에 따라 차단 요청을 방화벽, 라우터 또는 WLC로 전송하여 특정 IP 주소에서 오는 패킷을 차단할 수 있습니다.

Cisco Wireless Controller용 Cisco Unified Wireless Network Software Release 4.0을 사용하면 컨트롤러에서 사용 가능한 클라이언트 블랙리스트 또는 제외 동작을 트리거하려면 WLC에 차단 요청을 보내야 합니다.컨트롤러가 차단 요청을 받기 위해 사용하는 인터페이스는 Cisco IDS의 명령 및 제어 인터페이스입니다.

- 컨트롤러는 지정된 컨트롤러에 최대 5개의 IDS 센서를 구성할 수 있습니다.
- 구성된 각 IDS 센서는 IP 주소 또는 인증된 네트워크 이름 및 권한 부여 자격 증명으로 식별됩니다.
- 각 IDS 센서는 고유한 쿼리 속도로 컨트롤러에서 구성할 수 있습니다(초).



IDS 차단

컨트롤러가 구성된 쿼리 속도로 센서를 쿼리하여 모든 차단 이벤트를 검색합니다.지정된 차단 요청은 IDS 센서에서 요청을 검색하는 컨트롤러의 전체 모빌리티 그룹에 배포됩니다.클라이언트 IP 주

소에 대한 각 차단 요청은 지정된 시간 제한 초 값에 적용됩니다.시간 초과 값이 무한 시간을 나타내는 경우 IDS에서 차단 항목이 제거된 경우에만 차단 이벤트가 종료됩니다.차단된 클라이언트 상태는 컨트롤러 중 하나 또는 전체가 재설정되더라도 모빌리티 그룹의 각 컨트롤러에서 유지됩니다.

참고: 클라이언트 차단 결정은 항상 IDS 센서에서 수행합니다.컨트롤러가 레이어 3 공격을 탐지하지 않습니다.클라이언트가 레이어 3에서 악의적인 공격을 시작하는지 확인하는 것은 훨씬 더 복잡한 프로세스입니다. 클라이언트는 레이어 2에서 인증되며, 이는 컨트롤러가 레이어 2 액세스를 허용하기에 충분합니다.

참고: 예를 들어, 클라이언트가 이전 위반(회피) IP 주소를 할당받은 경우, 이 새 클라이언트에 대한 레이어 2 액세스 차단을 해제하기 위해 센서 시간 초과가 됩니다.컨트롤러가 레이어 2에 액세스를 제공하더라도 Sensor가 라우터에 차단 이벤트를 알리기 때문에 클라이언트 트래픽이 레이어 3의 라우터에서 차단될 수 있습니다.

클라이언트에 IP 주소 A가 있다고 가정합니다. 이제 컨트롤러가 차단 이벤트를 위해 IDS를 폴링하면 IDS는 IP 주소 A를 대상 IP 주소로 사용하여 컨트롤러에 차단 요청을 보냅니다.이제 컨트롤러 블랙은 이 클라이언트 A를 나열합니다. 컨트롤러에서 클라이언트는 MAC 주소를 기반으로 비활성화됩니다.

이제 클라이언트가 IP 주소를 A에서 B로 변경한다고 가정합니다. 다음 폴링 동안 컨트롤러는 IP 주소를 기반으로 차단된 클라이언트 목록을 가져옵니다.이번에는 IP 주소 A가 여전히 차단 목록에 있습니다.그러나 클라이언트가 IP 주소를 A에서 B로 변경했으므로(IP 주소 목록에 없는), 컨트롤러에서 블랙리스트 클라이언트의 시간 제한에 도달하면 새 IP 주소가 B인 이 클라이언트가 해제됩니다.이제 컨트롤러는 B의 새 IP 주소를 사용하여 이 클라이언트를 허용하기 시작합니다. 그러나 클라이언트 MAC 주소는 동일하게 유지됩니다.

따라서 클라이언트가 컨트롤러 제외 시간 동안 비활성화된 상태로 유지되며 이전 DHCP 주소를 다시 가져올 경우 다시 제외되지만, 차단된 클라이언트의 IP 주소가 변경되면 해당 클라이언트는 더 이상 비활성화되지 않습니다.예를 들어 클라이언트가 동일한 네트워크에 연결되고 DHCP 임대 시간 제한이 만료되지 않은 경우

컨트롤러는 컨트롤러에서 관리 포트를 사용하는 클라이언트 차단 요청에 대해서만 IDS 연결을 지원합니다.컨트롤러는 무선 클라이언트 트래픽을 전달하는 해당 VLAN 인터페이스를 통해 패킷 검사를 위해 IDS에 연결합니다.

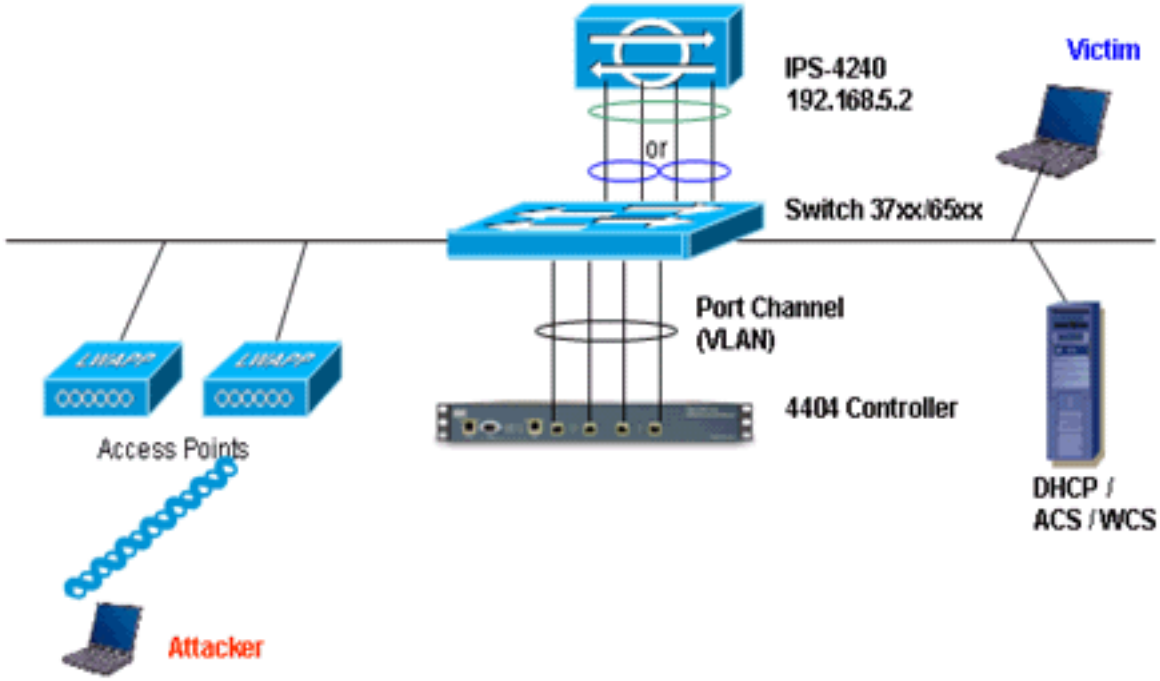
컨트롤러에서 Disable Clients(클라이언트 비활성화) 페이지에는 IDS 센서 요청을 통해 비활성화된 각 클라이언트가 표시됩니다.CLI **show** 명령은 블랙리스트 클라이언트 목록도 표시합니다.

WCS의 Security(보안) 하위 탭에 제외된 클라이언트가 표시됩니다.

다음은 Cisco IPS Sensor 및 Cisco WLC의 통합을 완료하기 위한 단계입니다.

1. 무선 컨트롤러가 있는 동일한 스위치에 IDS 어플라이언스를 설치하고 연결합니다.
2. IDS 어플라이언스로 무선 클라이언트 트래픽을 전달하는 WLC 포트를 SPAN(Mirror)합니다.
3. IDS 어플라이언스는 모든 패킷의 복사본을 수신하고 레이어 3~7에서 트래픽을 검사합니다.
4. IDS 어플라이언스는 다운로드 가능한 서명 파일을 제공하며, 사용자 정의할 수도 있습니다.
5. IDS 어플라이언스는 공격 시그니처가 탐지될 때 이벤트 동작 shun과 함께 경보를 생성합니다.
6. WLC는 경보에 대한 IDS를 폴링합니다.
7. WLC에 연결된 무선 클라이언트의 IP 주소가 있는 경보가 감지되면 클라이언트는 제외 목록에 추가됩니다.
8. WLC에서 트랩이 생성되고 WCS에 알림이 전송됩니다.
9. 사용자가 지정된 기간 후에 제외 목록에서 제거됩니다.

네트워크 아키텍처 설계



Cisco WLC는 Catalyst 6500의 기가비트 인터페이스에 연결됩니다.기가비트 인터페이스에 대한 포트 채널을 생성하고 WLC에서 LAG(Link Aggregation)를 활성화합니다.

```
(Cisco Controller) >show interface summary

Interface Name                   Port  Vlan Id   IP Address       Type     Ap Mgr
-------------------------------  ----  --------  ---------------  -------  ------
ap-manager                       LAG   untagged  10.10.99.3       Static   Yes
management                       LAG   untagged  10.10.99.2       Static   No
service-port                     N/A   N/A       192.168.1.1      Static   No
virtual                          N/A   N/A       1.1.1.1          Static   No
vlan101                          LAG   101       10.10.101.5      Dynamic  No
```

컨트롤러는 Catalyst 6500의 인터페이스 기가비트 5/1 및 기가비트 5/2에 연결됩니다.

```
cat6506#show run interface gigabit 5/1
Building configuration...

Current configuration : 183 bytes
!
interface GigabitEthernet5/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 99
 switchport mode trunk
 no ip address
 channel-group 99 mode on
end

cat6506#show run interface gigabit 5/2
Building configuration...

Current configuration : 183 bytes
```

```
!
interface GigabitEthernet5/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 99
 switchport mode trunk
 no ip address
 channel-group 99 mode on
end

cat6506#show run interface port-channel 99
Building configuration...

Current configuration : 153 bytes
!
interface Port-channel99
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 99
 switchport mode trunk
 no ip address
end
```

IPS 센서의 센싱 인터페이스는 프로미스큐어스 **모드**에서 개별적으로 작동할 수 있으며, 인라인 센싱 **모드**를 위한 인라인 인터페이스를 생성하기 위해 페어링할 수 있습니다.

프로미스큐어스 모드에서는 패킷이 센서를 통과하지 않습니다.센서는 실제 전달된 패킷이 아닌 모니터링되는 트래픽의 복사본을 분석합니다.프로미스큐어스(Promiscuous) 모드에서 작동의 장점은 센서가 전달된 트래픽의 패킷 흐름에 영향을 주지 않는다는 것입니다.

참고: 아키텍처 다이어그램은 WLC 및 IPS 통합 아키텍처 설정의 예일 뿐입니다.여기에 표시된 예제 컨피그레이션에서는 프로미스큐어스 모드에서 작동하는 IDS 센싱 인터페이스에 대해 설명합니다.아키텍처 다이어그램은 인라인 쌍 모드에서 작동하도록 함께 페어링되는 센싱 인터페이스를 보여줍니다.인라인 인터페이스 모드에 대한 자세한 내용은 인라인 모드를 참조하십시오.

이 컨피그레이션에서는 센싱 인터페이스가 프로미스큐어스 모드에서 작동하는 것으로 가정합니다.Cisco IDS Sensor의 모니터링 인터페이스는 Catalyst 6500의 기가비트 인터페이스 5/3에 연결됩니다.Catalyst 6500에서 모니터 세션을 생성합니다. 여기서 port-channel 인터페이스는 패킷의 소스이고 대상은 Cisco IPS 센서의 모니터링 인터페이스가 연결된 기가비트 인터페이스입니다.이렇게 하면 컨트롤러 유선 인터페이스에서 레이어 3에서 레이어 7 검사를 위한 IDS로 모든 인그레스 및 이그레스 트래픽이 복제됩니다.

```
cat6506#show run | inc monitor
monitor session 5 source interface Po99
monitor session 5 destination interface Gi5/3

cat6506#show monitor session 5
Session 5
---------
Type                   : Local Session
Source Ports           :
    Both               : Po99
Destination Ports      : Gi5/3
cat6506#
```

Cisco IDS 센서 구성

Cisco IDS 센서의 초기 컨피그레이션은 콘솔 포트에서 또는 모니터와 키보드를 센서에 연결하여 수

행됩니다.

1. 어플라이언스에 로그인합니다.센서에 콘솔 포트를 연결합니다.모니터와 키보드를 센서에 연결합니다.
2. 로그인 프롬프트에 사용자 이름과 비밀번호를 입력합니다.**참고:** 기본 사용자 이름과 비밀번호는 모두 cisco입니다.어플라이언스에 처음 로그인할 때 이를 변경하라는 메시지가 표시됩니다.먼저 cisco인 UNIX 비밀번호를 입력해야 합니다.그런 다음 새 비밀번호를 두 번 입력해야 합니다.

```
login: cisco
Password:
***NOTICE***
This product contains cryptographic features and is subject to
United States and local country laws governing import, export,
transfer and use. Delivery of Cisco cryptographic products does
not imply third-party authority to import, export, distribute or
use encryption. importers, exporters, distributors and users are
responsible for compliance with U.S. and local country laws.
By using this product you agree to comply with applicable laws
and regulations. If you are unable to comply with U.S. and local laws,
return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may
be found at:

http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending
email to export@cisco.com.
***LICENSE NOTICE***
There is no license key installed on the system.
Please go to https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet (registered
customers only) to obtain a new license or install a license.
```

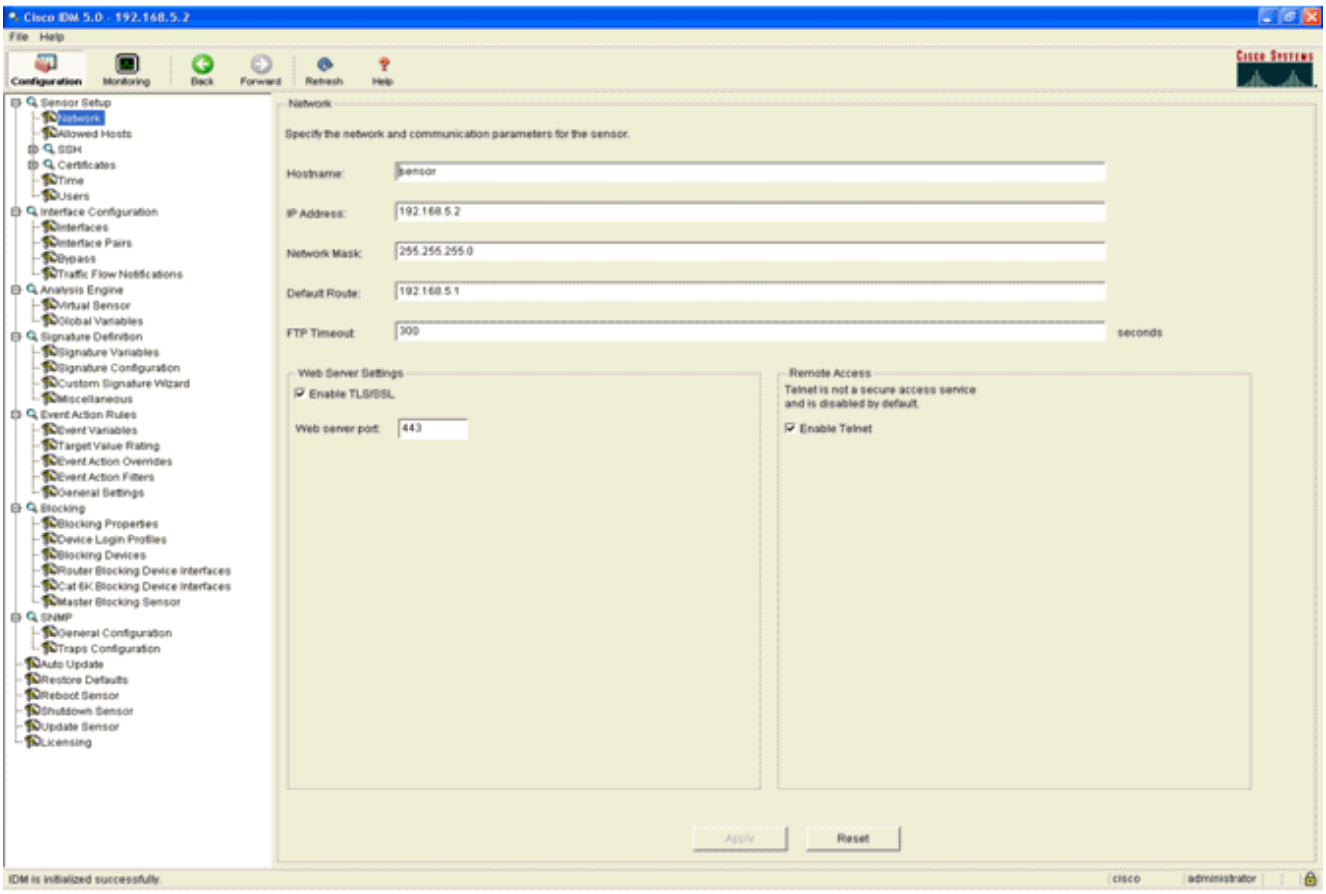
3. 센서에서 IP 주소, 서브넷 마스크 및 액세스 목록을 구성합니다.**참고:** 컨트롤러 통신에 사용되는 IDS의 명령 및 제어 인터페이스입니다.이 주소는 컨트롤러 관리 인터페이스에 라우팅할 수 있어야 합니다.센싱 인터페이스에는 주소 지정이 필요하지 않습니다.액세스 목록에는 컨트롤러 관리 인터페이스 주소와 IDS 관리를 위한 허용 가능한 주소가 포함되어야 합니다.

```
sensor#configure terminal
sensor(config)#service host
sensor(config-hos)#network-settings
sensor(config-hos-net)#host-ip 192.168.5.2/24,192.168.5.1
sensor(config-hos-net)#access-list 10.0.0.0/8
sensor(config-hos-net)#access-list 40.0.0.0/8
sensor(config-hos-net)#telnet-option enabled
sensor(config-hos-net)#exit
sensor(config-hos)#exit
Apply Changes:?[yes]: yes
sensor(config)#exit
sensor#
sensor#ping 192.168.5.1
PING 192.168.5.1 (192.168.5.1): 56 data bytes
64 bytes from 192.168.5.1: icmp_seq=0 ttl=255 time=0.3 ms
64 bytes from 192.168.5.1: icmp_seq=1 ttl=255 time=0.9 ms
64 bytes from 192.168.5.1: icmp_seq=2 ttl=255 time=0.3 ms
64 bytes from 192.168.5.1: icmp_seq=3 ttl=255 time=1.0 ms
--- 192.168.5.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.3/0.6/1.0 ms
sensor#
```

4. 이제 GUI에서 IPS 센서를 구성할 수 있습니다.브라우저를 센서의 관리 IP 주소로 이동합니다

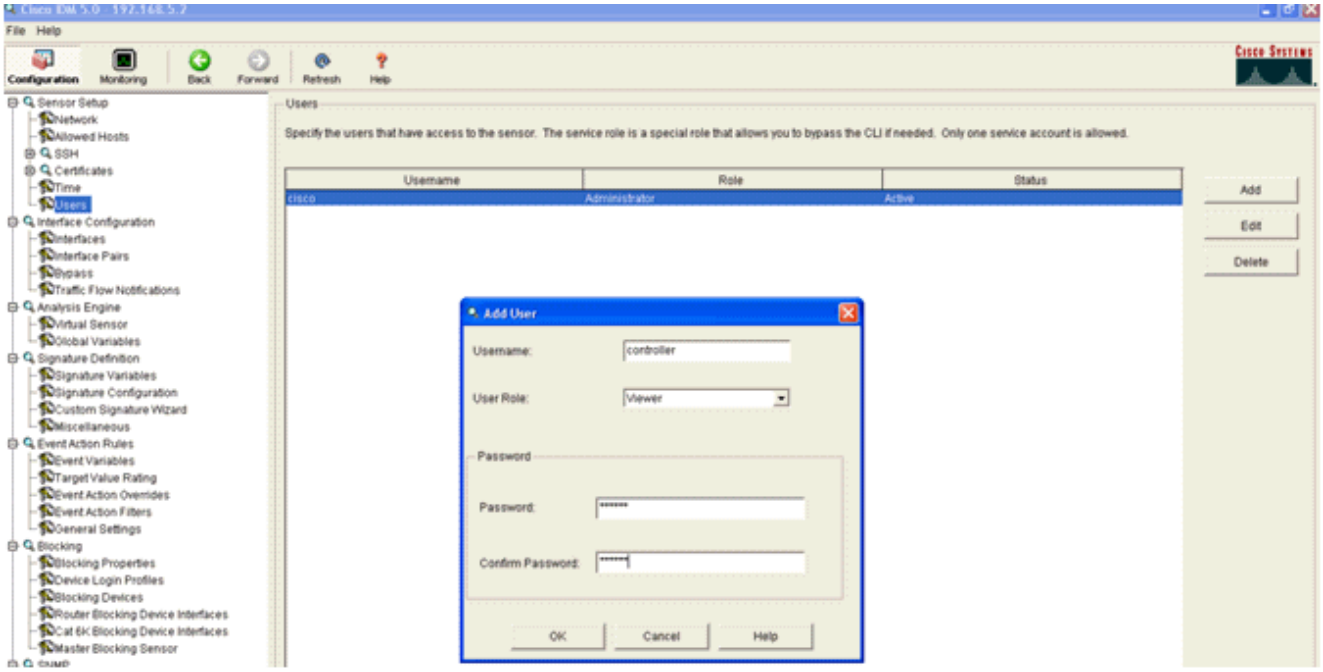
.이 이미지는 센서가 192.168.5.2으로 구성된 샘플입니다

.



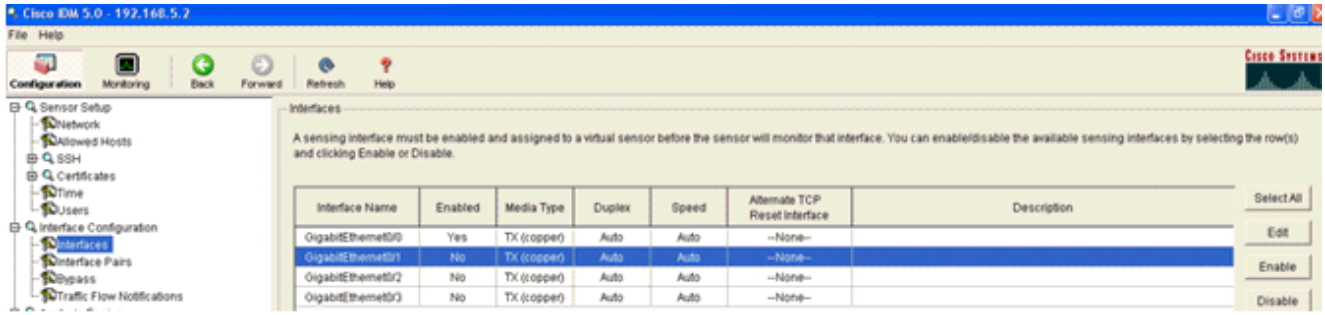
5. WLC에서 IPS 센서 이벤트에 액세스하는 데 사용하는 사용자를 추가합니다

.



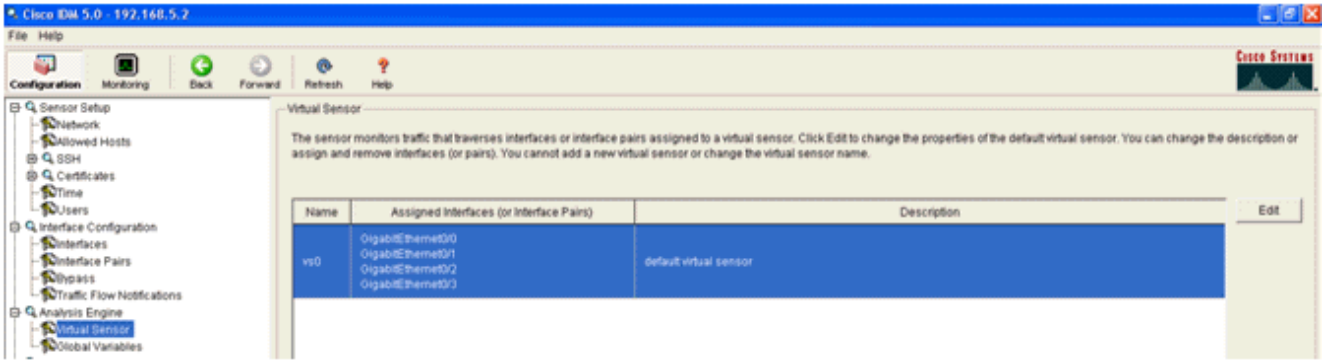
6. 모니터링 인터페이스를 활성화합니다

.



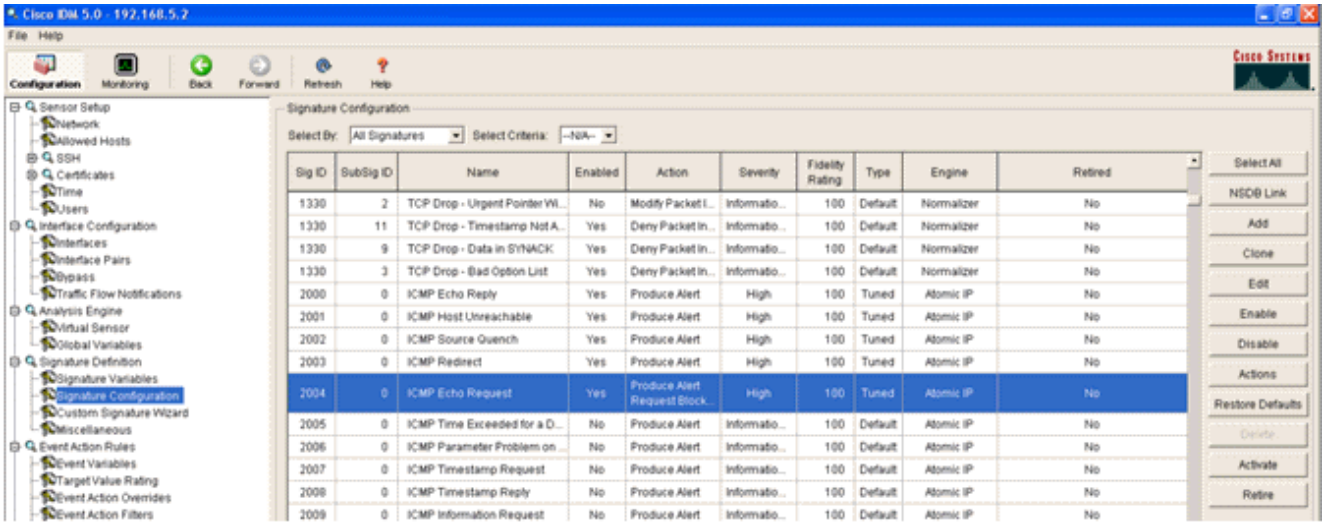
이 창에 다음과 같이 모니터링 인터페이스를 분석 엔진에 추가해야 합니다

.



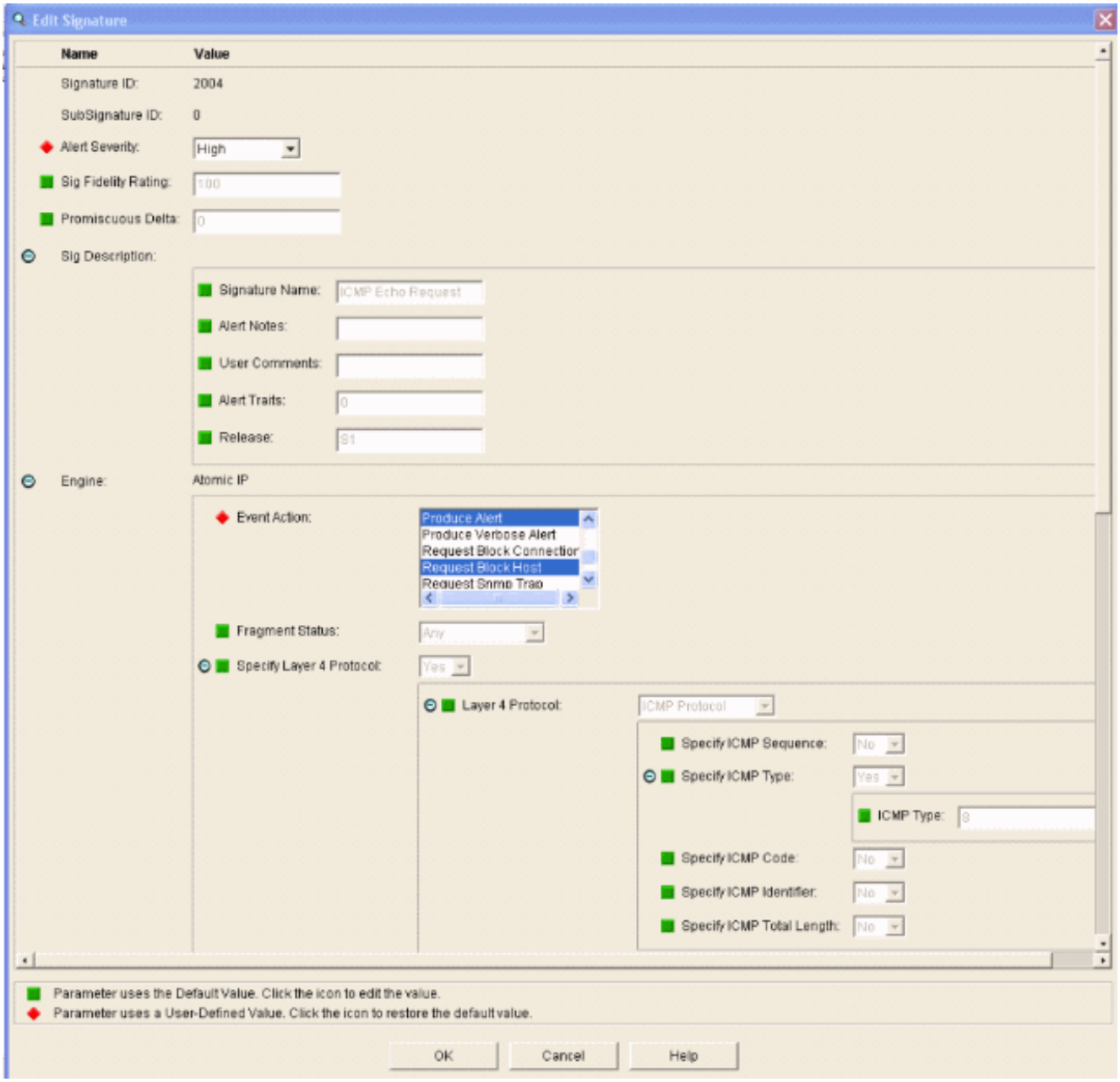
7. 빠른 설정 확인을 수행하려면 2004 서명(ICMP Echo Request)을 선택합니다

.



이 확인 단계를 완료하기 위해 시그니처를 활성화하고, Alert Severity(경고 심각도)를 **High(높음)**로 설정하고, Event Action(이벤트 작업)을 Produce Alert(**경고 생성)** 및 **Request Block Host(요청 블록 호스트)**로 설정해야 합니다

.

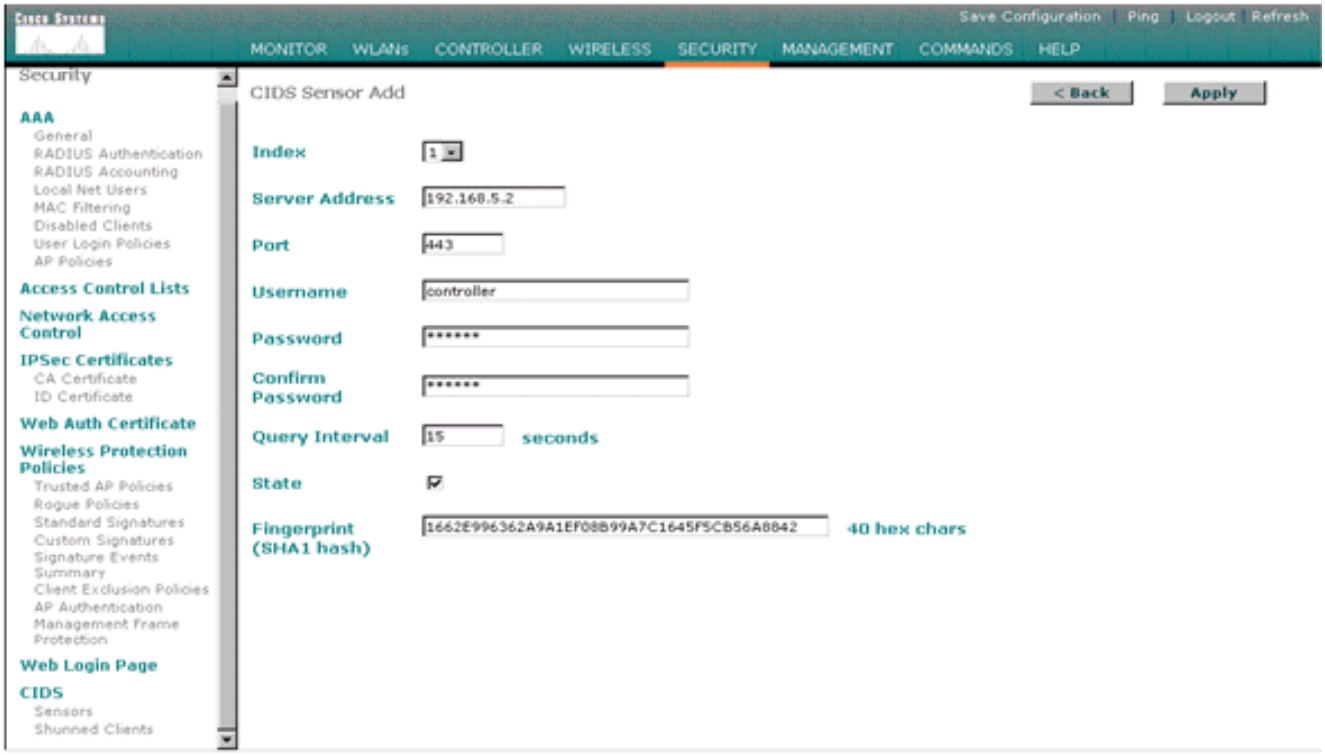


WLC 구성

WLC를 구성하려면 다음 단계를 완료합니다.

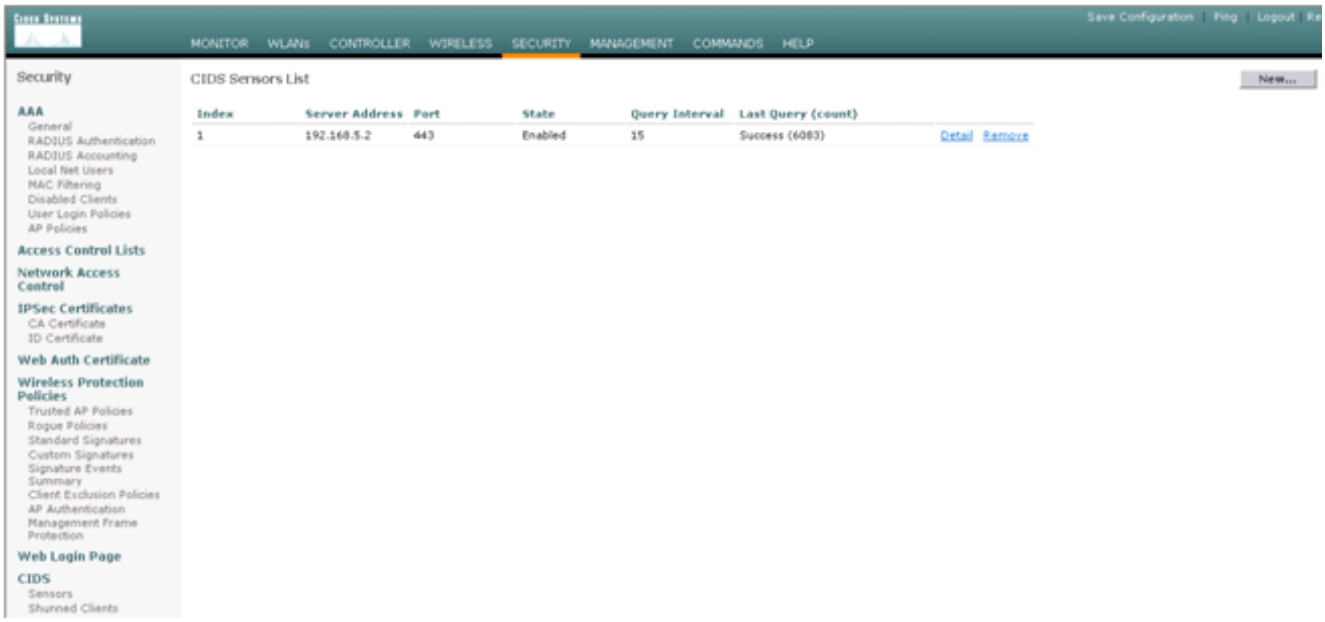
1. IPS 어플라이언스를 구성하고 컨트롤러에 추가할 준비가 되었으면 Security(**보안**) > CIDS > **Sensors(센서) > New(새로 만들기)를** 선택합니다.
2. 이전에 생성한 IP 주소, TCP 포트 번호, 사용자 이름 및 비밀번호를 추가합니다.IPS 센서에서 핑거프린트를 가져오려면 IPS 센서에서 이 명령을 실행하고 WLC에 SHA1 핑거프린트를 추가합니다(콜론 없음). 이는 컨트롤러-IDS 폴링 통신을 보호하는 데 사용됩니다.

```
sensor#show tls fingerprint
MD5: 1A:C4:FE:84:15:78:B7:17:48:74:97:EE:7E:E4:2F:19
SHA1: 16:62:E9:96:36:2A:9A:1E:F0:8B:99:A7:C1:64:5F:5C:B5:6A:88:42
```



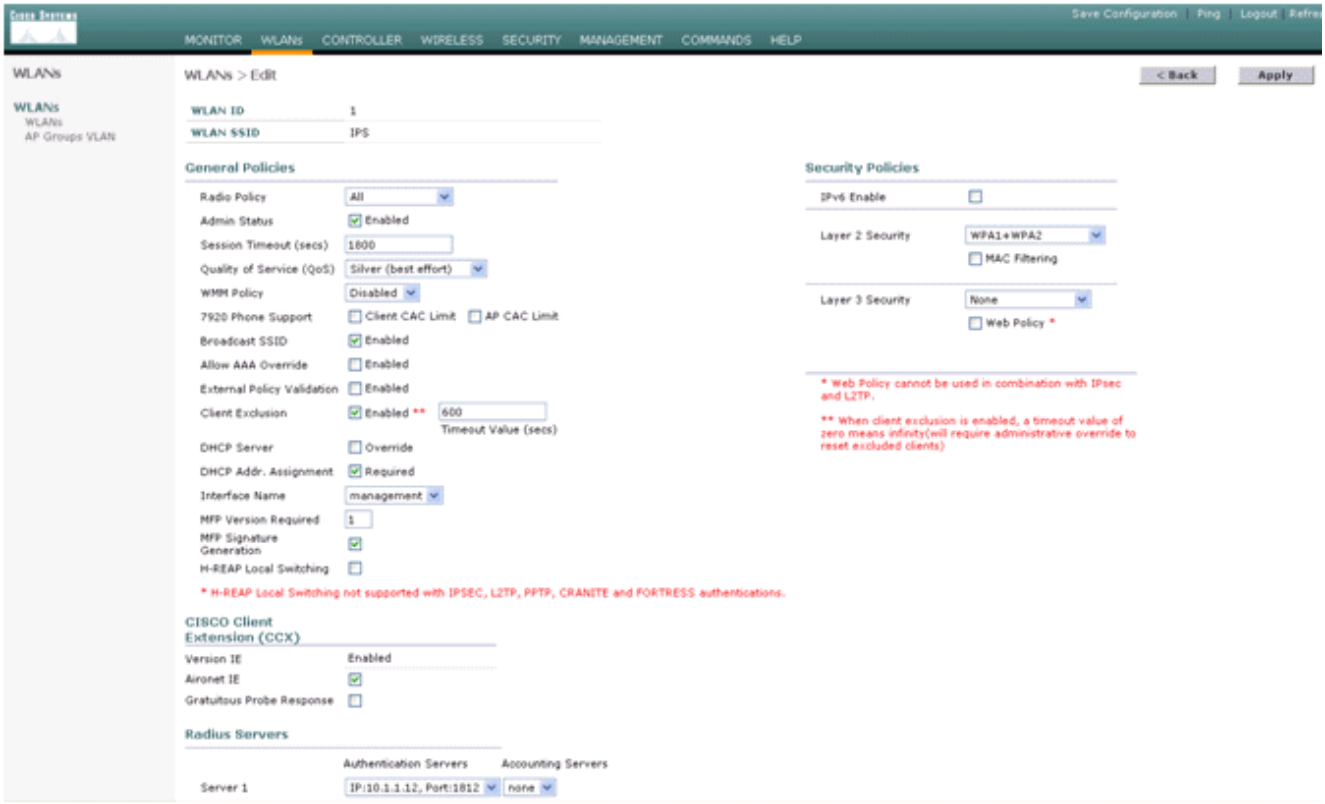
3. IPS 센서와 WLC 간의 연결 상태를 확인합니다

.



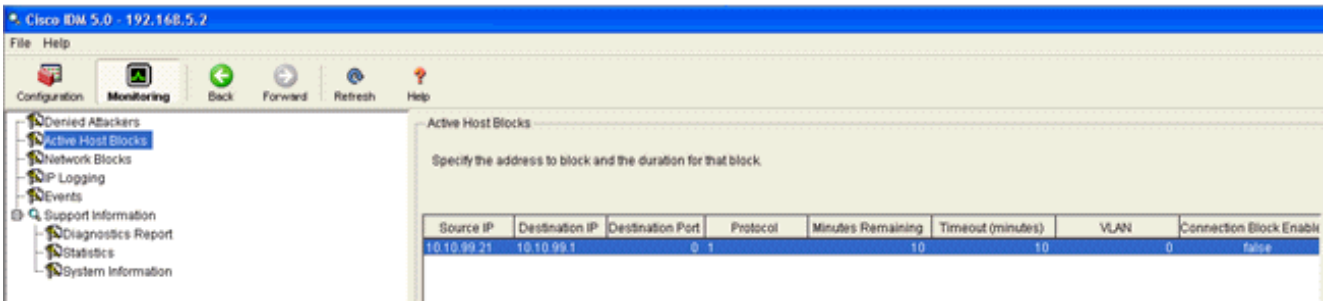
4. Cisco IPS Sensor와의 연결을 설정한 후에는 WLAN 컨피그레이션이 올바르며 **Client Exclusion**을 활성화했는지 **확인합니다**.기본 클라이언트 제외 시간 초과 값은 60초입니다.또한 클라이언트 제외 타이머와 상관없이 IDS에서 호출한 클라이언트 블록이 활성 상태로 유지되는 한 클라이언트 제외는 계속 유지됩니다.IDS의 기본 차단 시간은 30분입니다

.

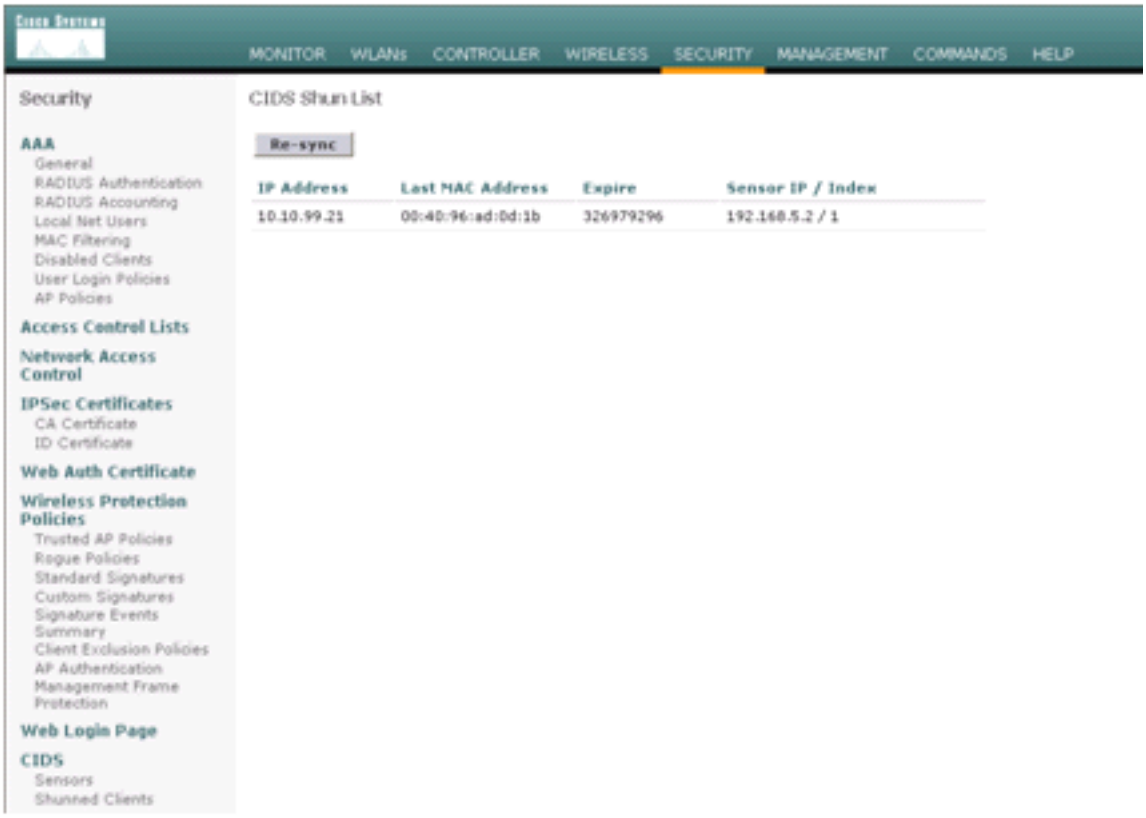


5. 네트워크의 특정 디바이스에 대한 NMAP 스캔을 수행하거나 Cisco IPS 센서에서 모니터링하는 일부 호스트에 대해 ping을 수행할 때 Cisco IPS 시스템에서 이벤트를 트리거할 수 있습니다.Cisco IPS에서 경보가 트리거되면 Monitoring and **Active Host Blocks(모니터링 및 활성 호스트 블록**)로 이동하여 호스트에 대한 세부 정보를 확인합니다

.

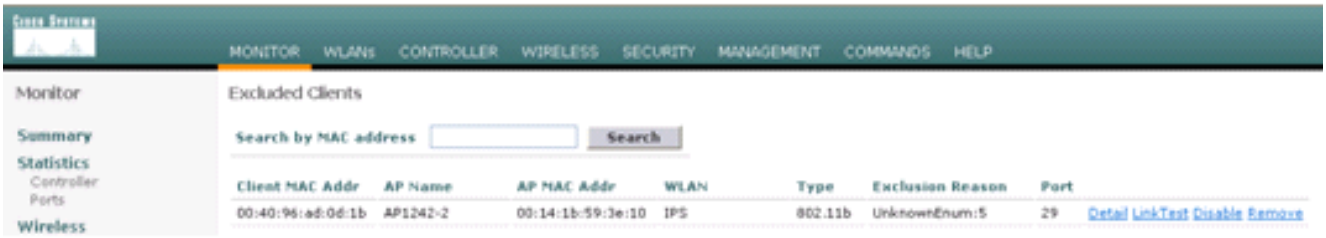


이제 컨트롤러의 회피 클라이언트 목록이 호스트의 IP 및 MAC 주소로 채워집니다



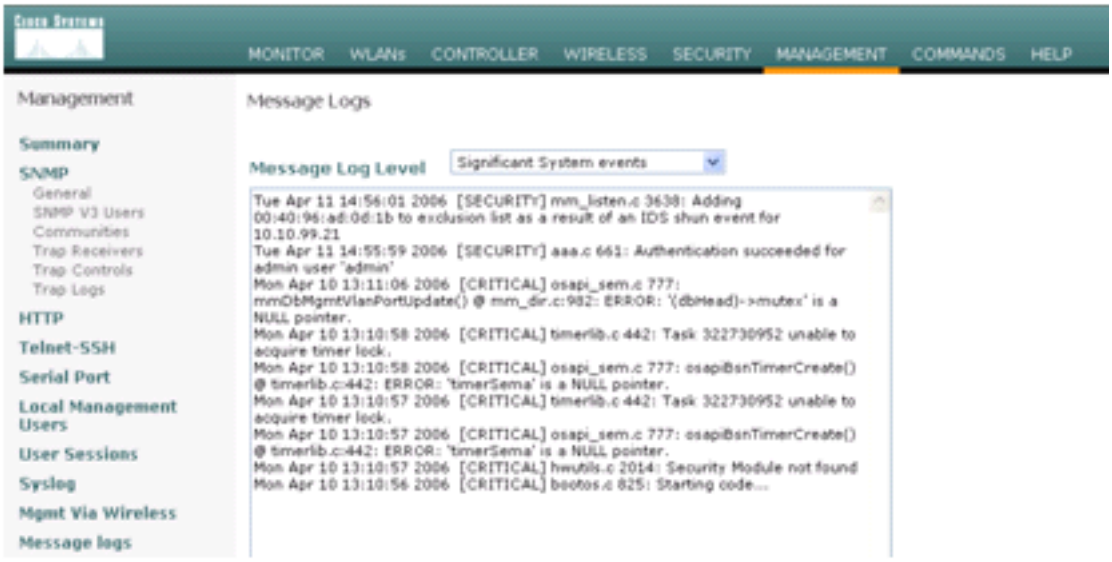
. 사용자가 클라이언트 제외 목록에 추가됩니다

.

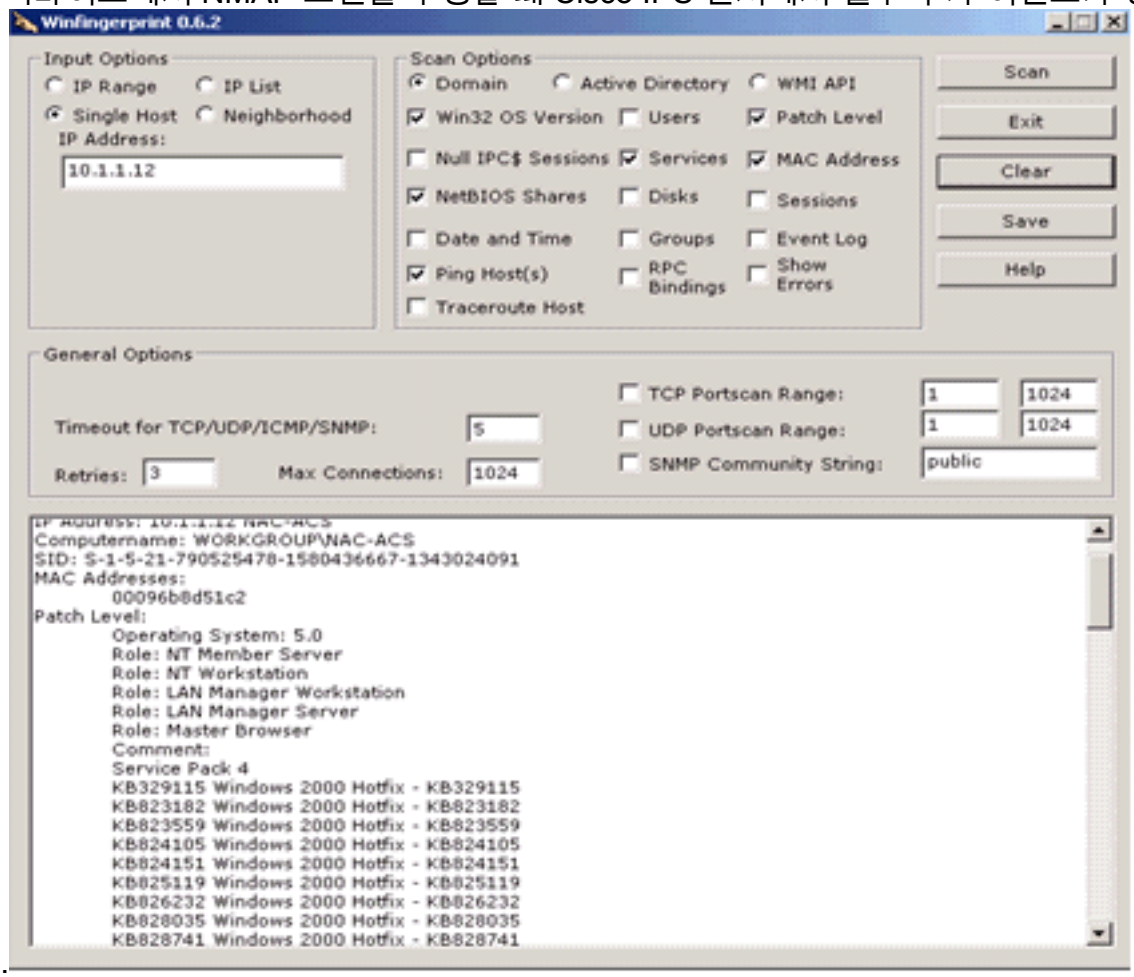


클라이언트가 차단 목록에 추가되면 트랩 로그가 생성됩니다

. 이벤트에 대한 메시지 로그도 생성됩니다

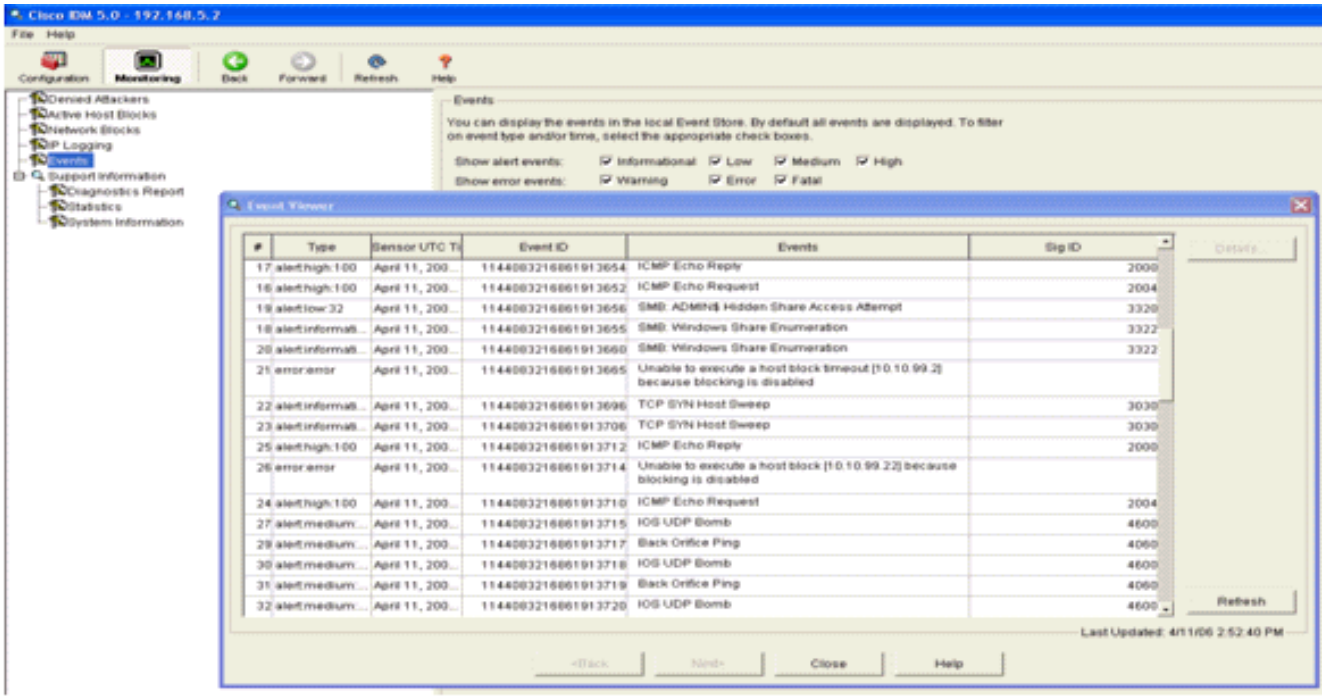


. 모니터링하는 디바이스에서 NMAP 스캔을 수행할 때 Cisco IPS 센서에서 일부 추가 이벤트가 생성됩니다



. 이 창에는 Cisco IPS 센서에서 생성된 이벤트가 표시됩니다

.



Cisco IDS 센서 샘플 컨피그레이션

다음은 설치 스크립트의 출력입니다.

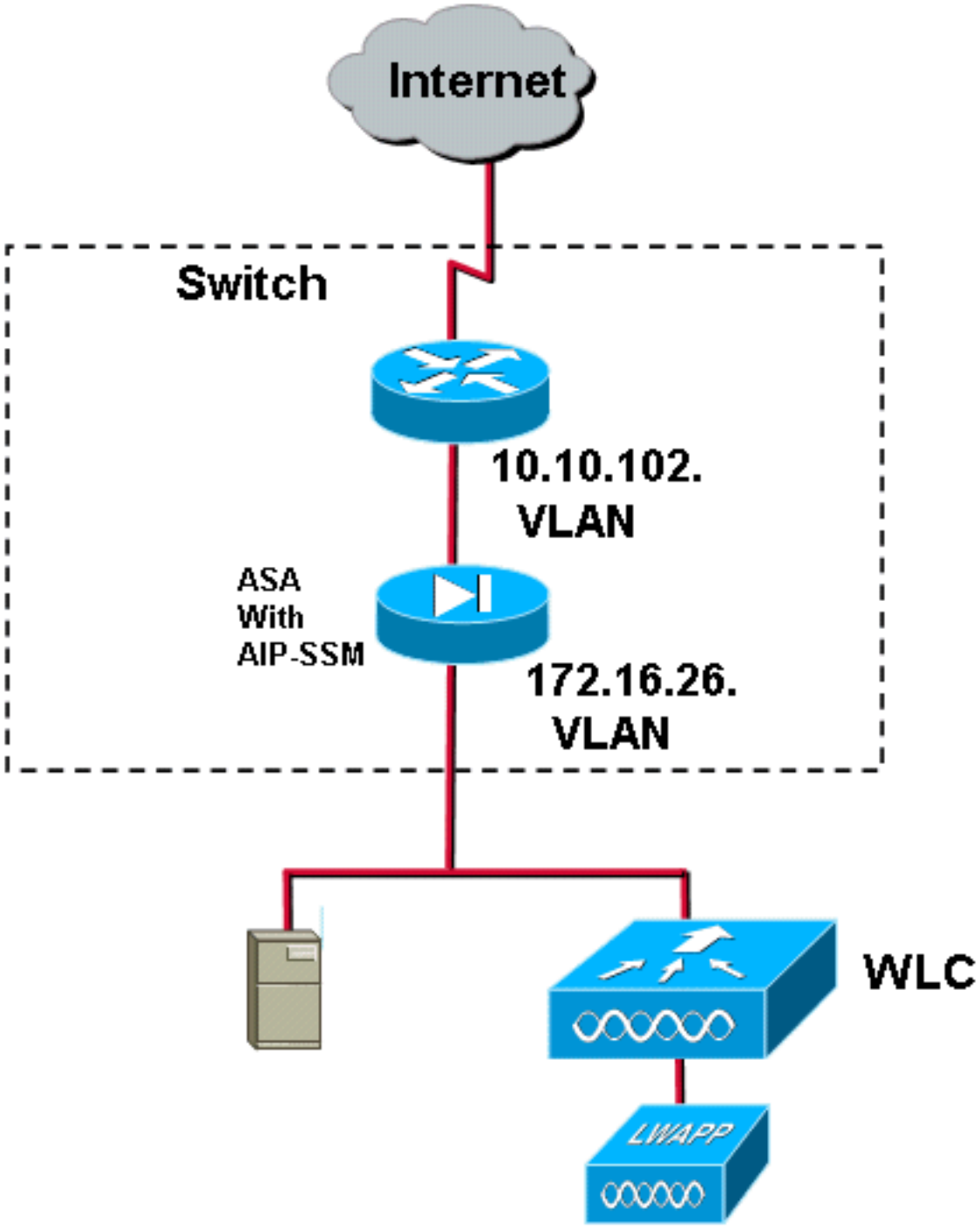
```
sensor#show config
! ------------------------------
! Version 5.0(2)
! Current configuration last modified Mon Apr 03 15:32:07 2006
! ------------------------------
service host
network-settings
host-ip 192.168.5.2/25,192.168.5.1
host-name sensor
telnet-option enabled
access-list 10.0.0.0/8
access-list 40.0.0.0/8
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
signatures 2000 0
alert-severity high
status
enabled true
exit
exit
signatures 2001 0
alert-severity high
status
enabled true
exit
```

```
exit
signatures 2002 0
alert-severity high
status
enabled true
exit
exit
signatures 2003 0
alert-severity high
status
enabled true
exit
exit
signatures 2004 0
alert-severity high
engine atomic-ip
event-action produce-alert|request-block-host
exit
status
enabled true
exit
exit
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service authentication
exit
! ------------------------------
service web-server
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service analysis-engine
virtual-sensor vs0
description default virtual sensor
physical-interface GigabitEthernet0/0
exit
exit
! ------------------------------
service interface
physical-interfaces GigabitEthernet0/0
admin-state enabled
exit
exit
! ------------------------------
service trusted-certificates
exit
sensor#
```

IDS용 ASA 구성

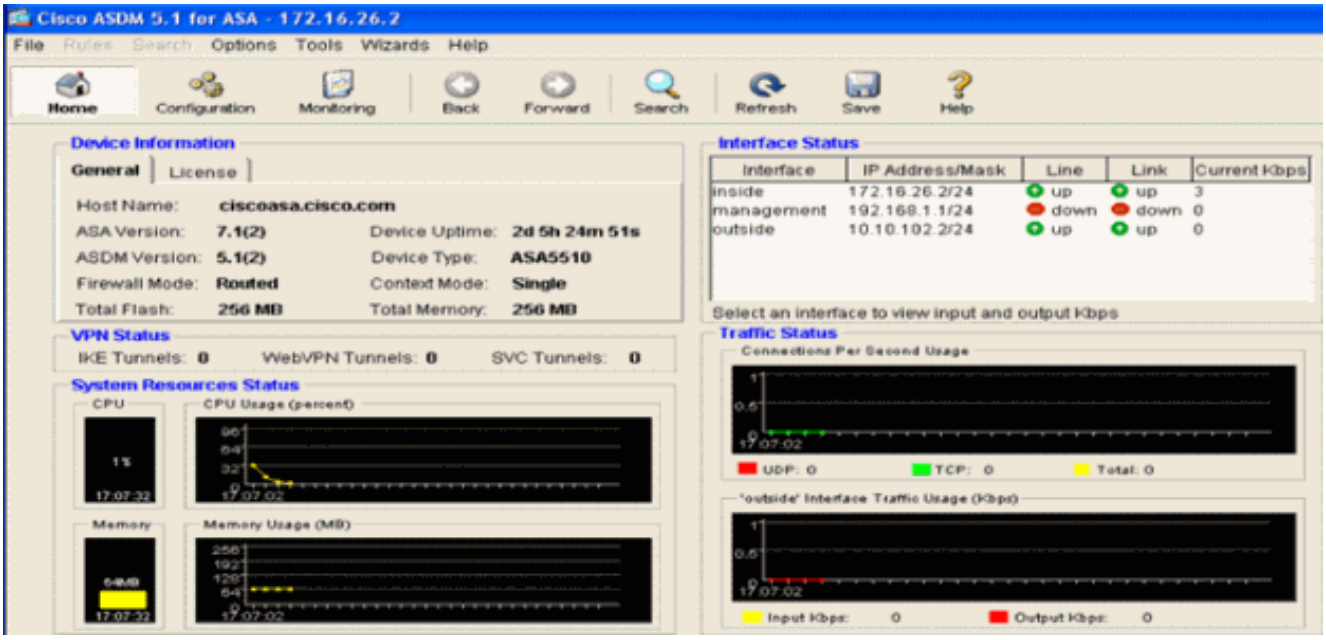
기존 침입 탐지 센서와 달리 ASA는 항상 데이터 경로에 있어야 합니다.즉, 스위치 포트에서 센서의 패시브 스니핑 포트로 트래픽을 스패닝하는 대신 ASA는 한 인터페이스에서 데이터를 수신하여 내

부적으로 처리한 다음 다른 포트로 전달해야 합니다.IDS의 경우, ASA에서 수신한 트래픽을 검사할 내부 AIP-SSM(Advanced Inspection and Prevention Security Services Module)에 복사하려면 MPF(Modular Policy Framework)를 사용합니다.



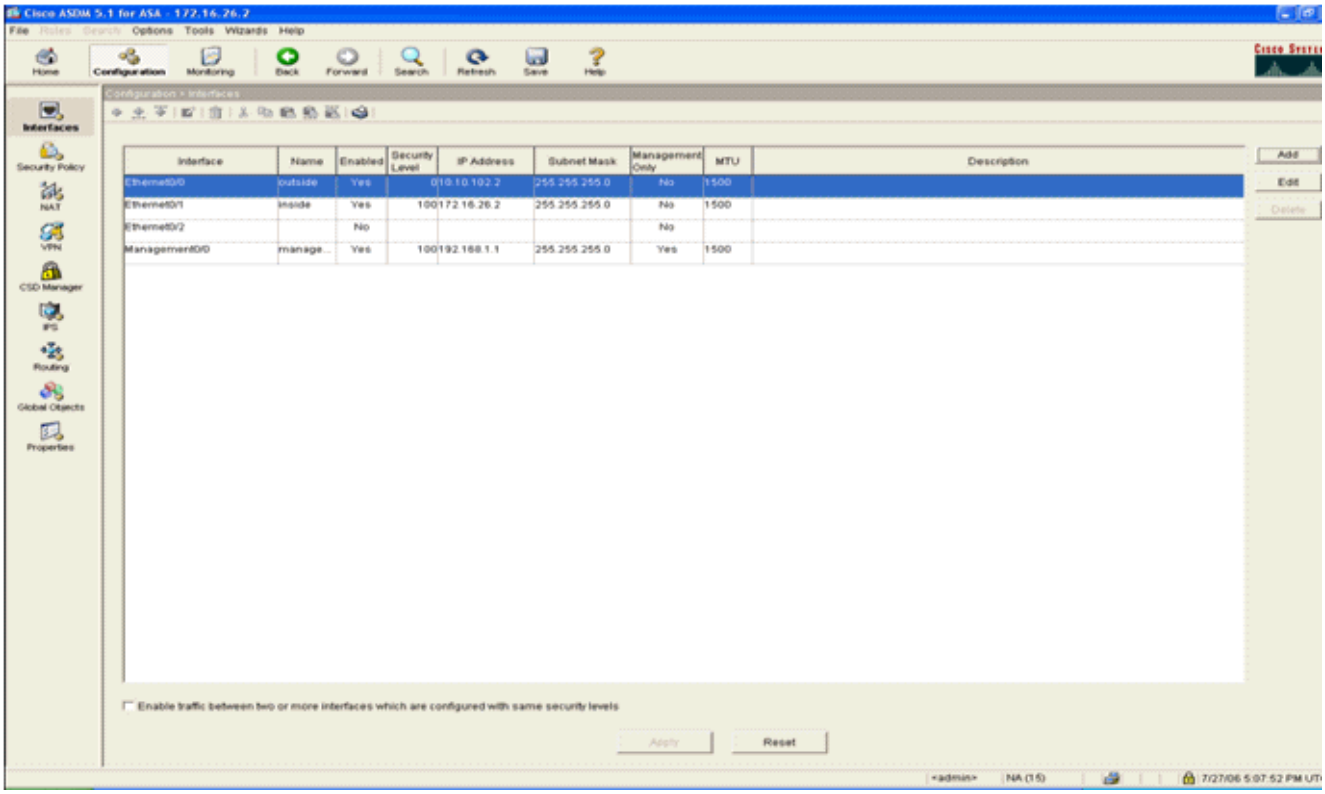
이 예에서 사용된 ASA는 이미 설정되어 트래픽을 전달합니다.이러한 단계는 AIP-SSM에 데이터를 전송하는 정책을 생성하는 방법을 보여줍니다.

1. ASDM을 사용하여 ASA에 로그인합니다.로그인에 성공하면 ASA Main System 창이 나타납니다
.



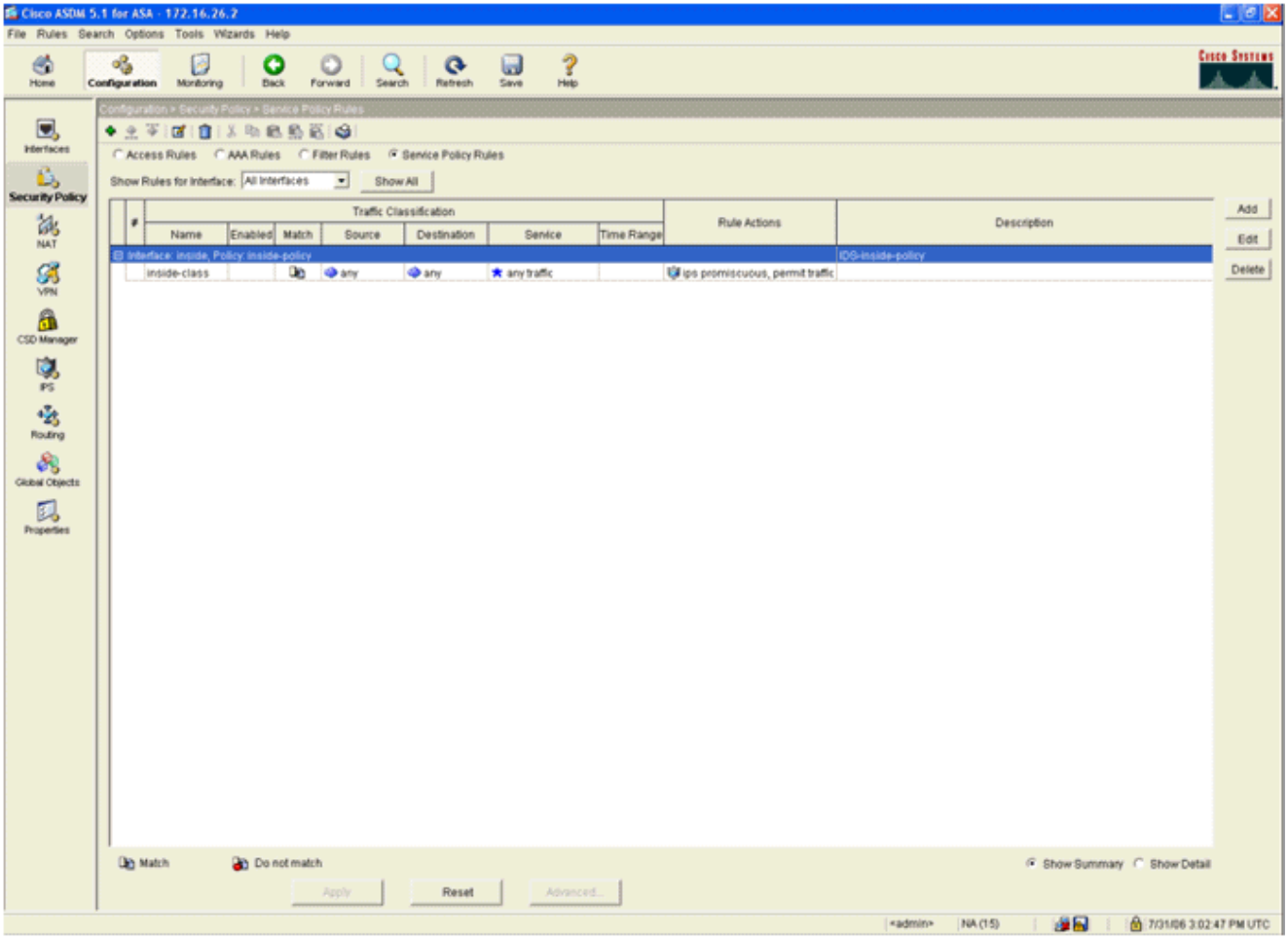
2. 페이지 상단에서 Configuration을 클릭합니다.창이 ASA 인터페이스의 보기로 전환됩니다

.



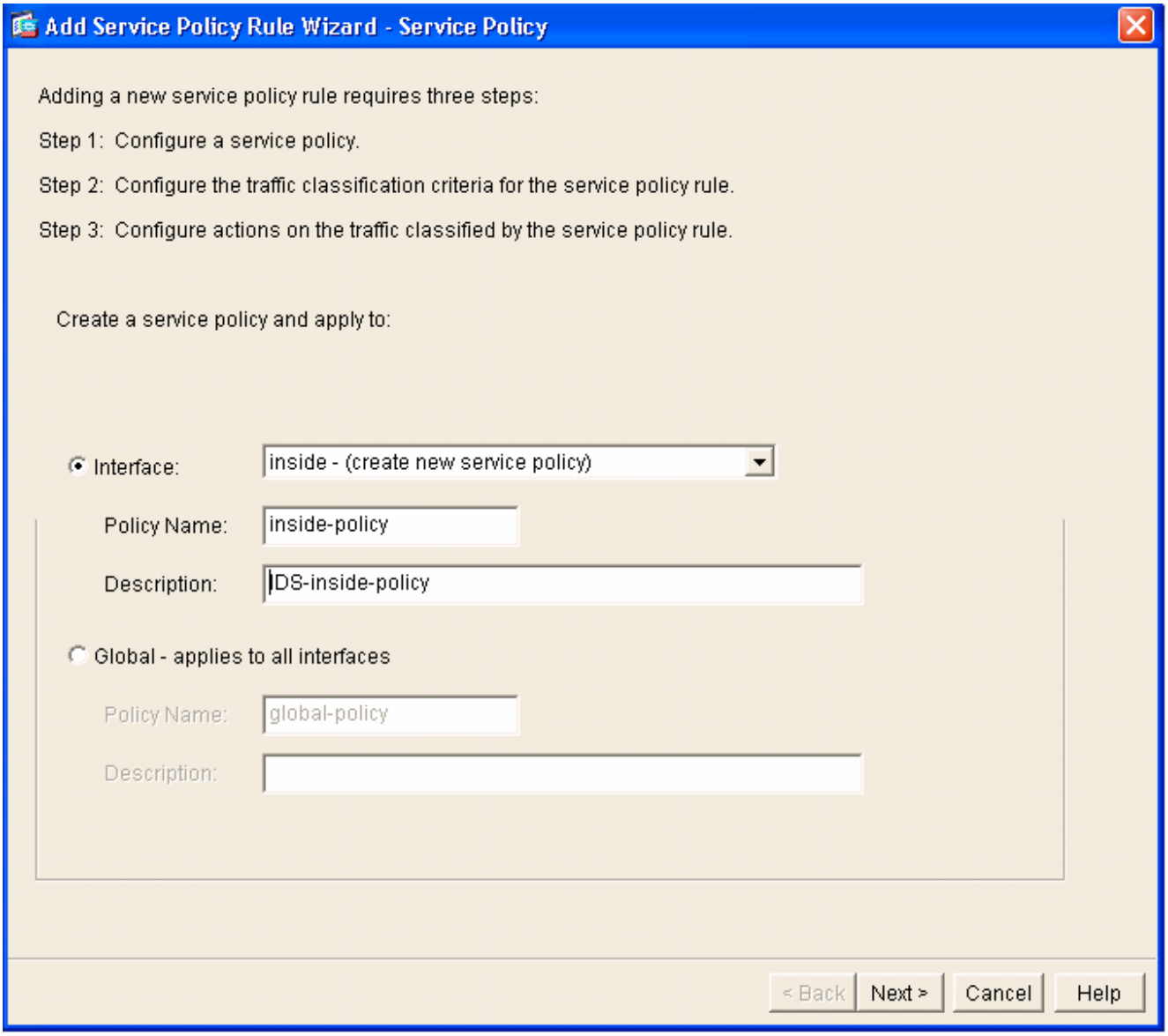
3. 창 왼쪽에서 Security Policy를 클릭합니다.결과 창에서 **서비스 정책 규칙** 탭을 선택합니다

.



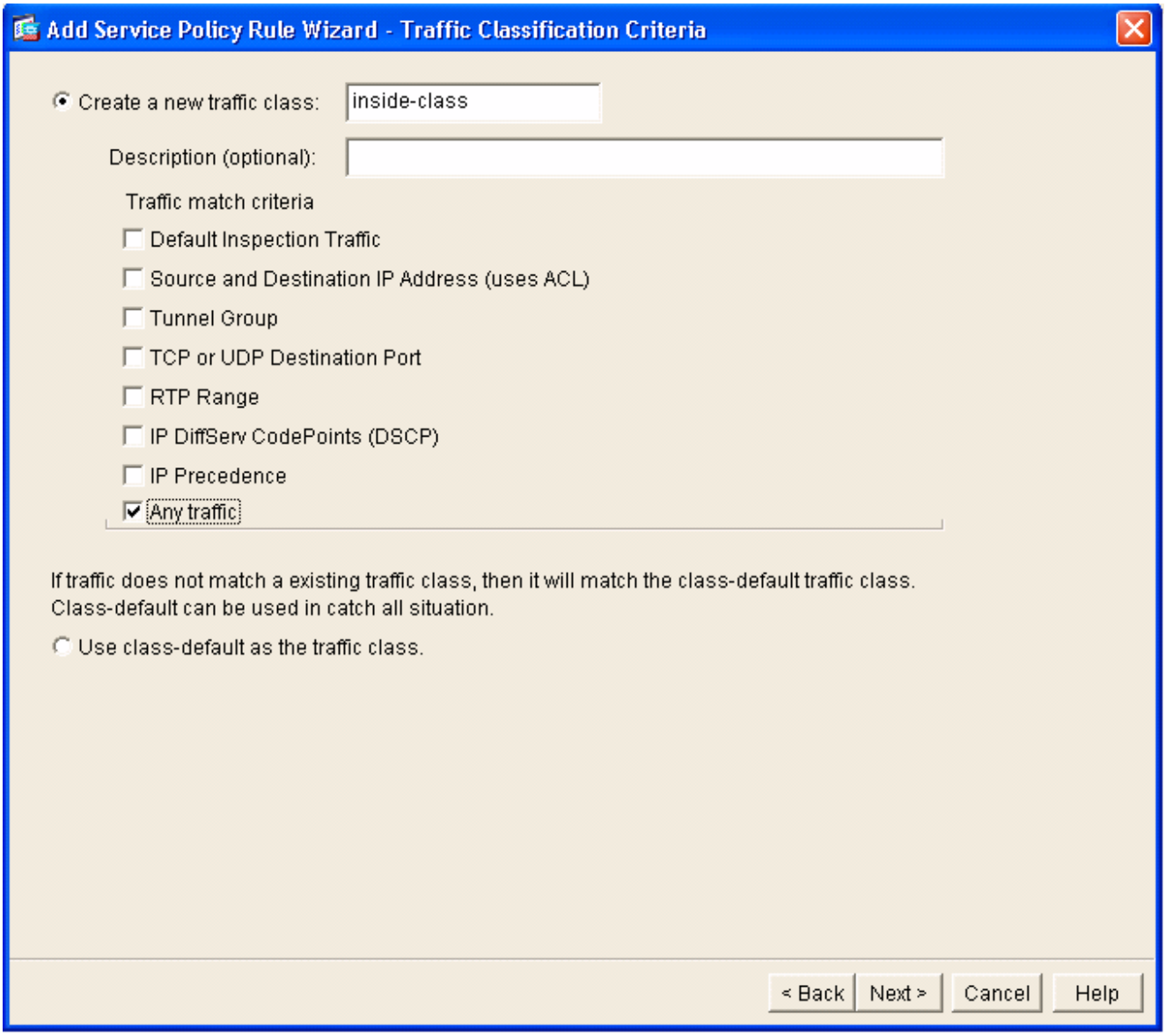
4. 새 정책을 생성하려면 Add(추가)를 클릭합니다.서비스 정책 규칙 추가 마법사가 새 창에서 실행됩니다.**Interface**를 클릭한 다음 드롭다운 목록에서 올바른 인터페이스를 선택하여 트래픽을 전달하는 인터페이스 중 하나에 바인딩된 새 정책을 생성합니다.정책에 두 텍스트 상자를 사용하여 정책이 수행하는 작업에 대한 이름과 설명을 지정합니다.다음 단계로 이동하려면 Next를 클릭합니다

.



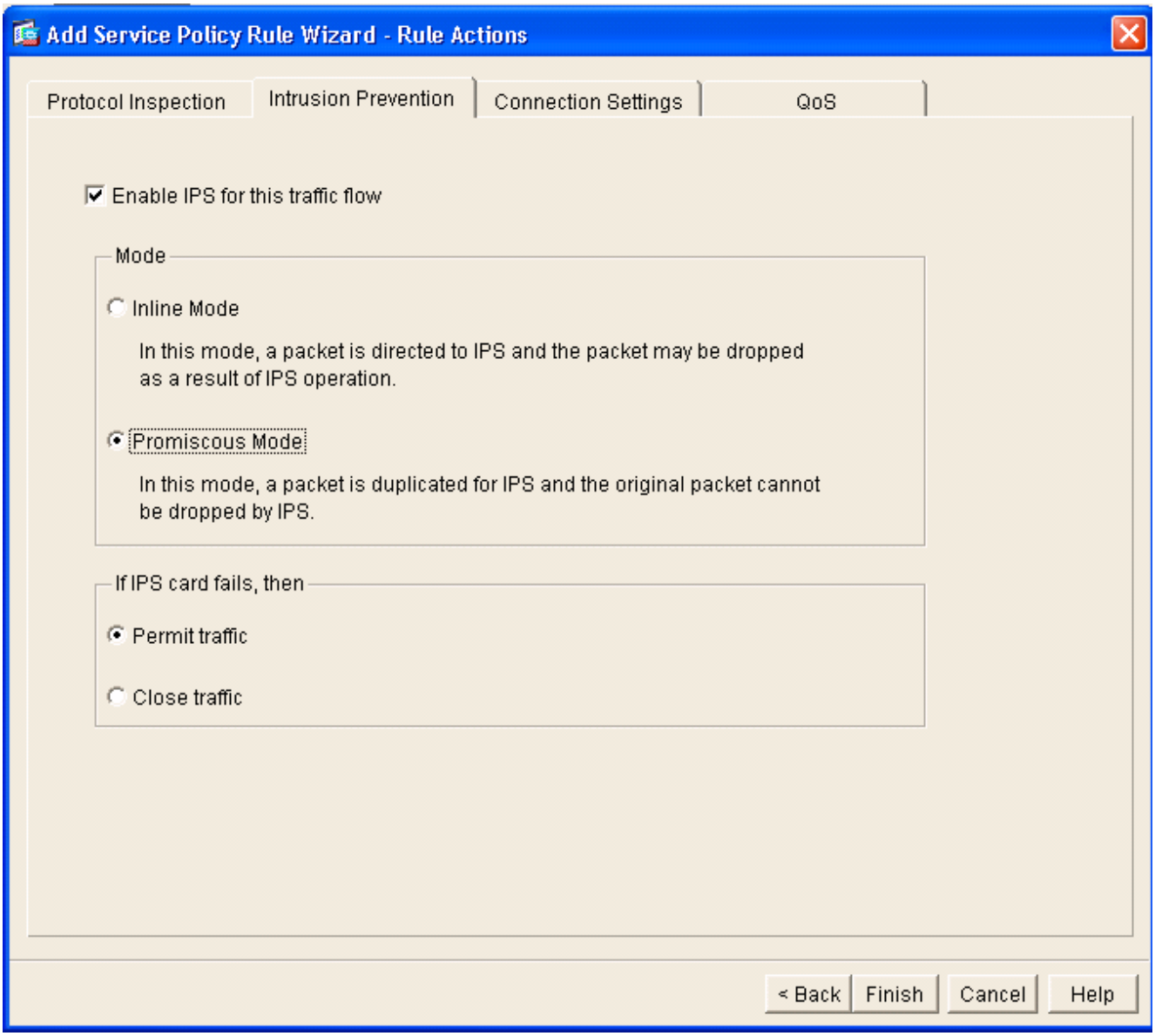
5. 정책에 적용할 새 트래픽 클래스를 구축합니다.특정 데이터 유형을 검사하기 위해 특정 클래스를 구축하는 것이 합리적이지만, 이 예에서는 단순성을 위해 Any Traffic이 선택됩니다.계속하려면 **다음**을 클릭합니다

.



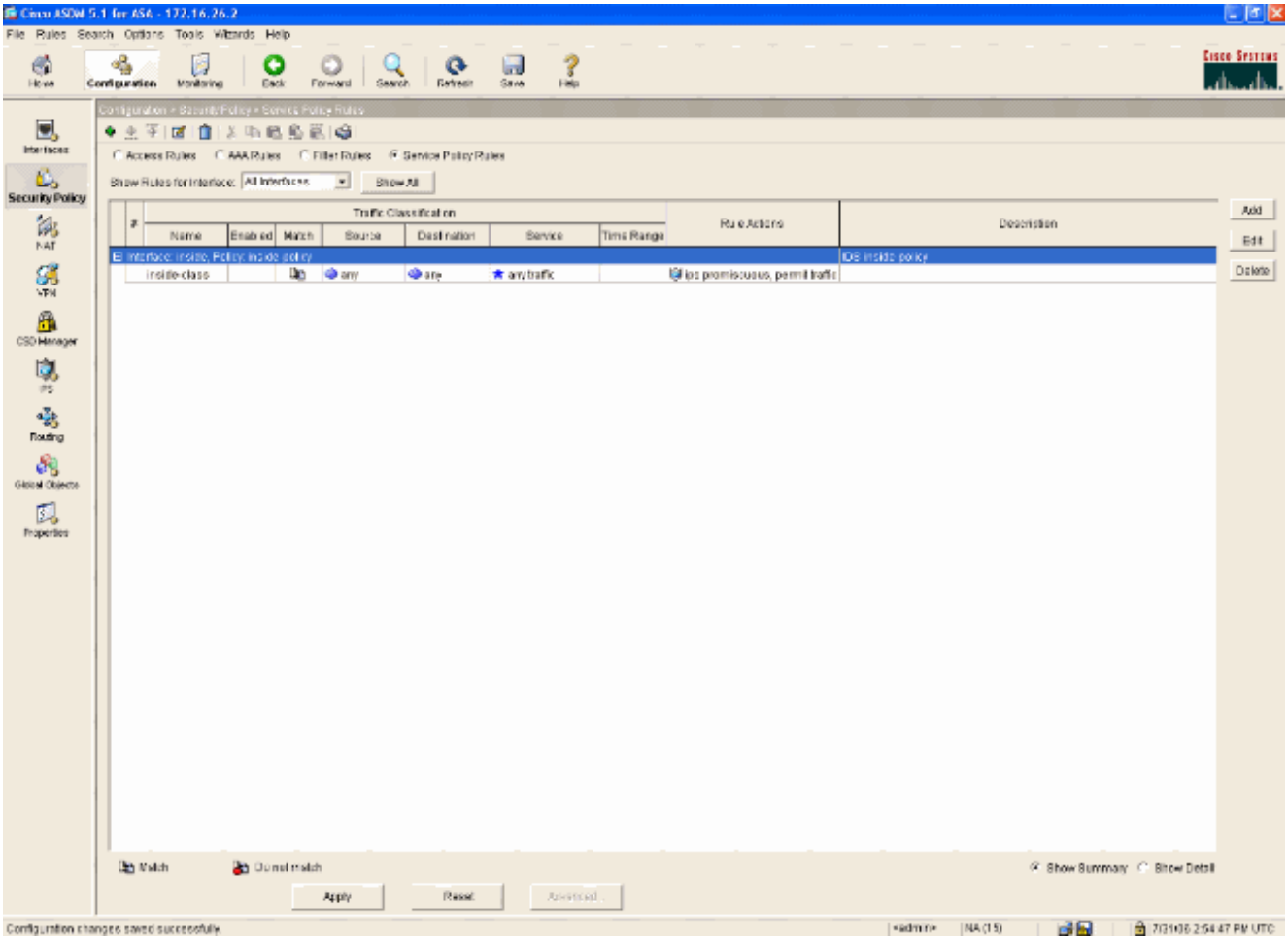
6. 다음 단계를 수행하여트래픽을 AIP-SSM으로 전달하도록 ASA에 지시합니다.침입 탐지**를 활성화하려면 Enable IPS for this traffic flow(이 트래픽 흐름**에 IPS 활성화)를 선택합니다.데이터 흐름을 사용하여 모듈을 인라인으로 배치하는 대신 트래픽의 복사본이 아웃오브밴드(out-of-band)로 모듈로 전송되도록 모드를 프로미스큐어스(Promiscuous)로 설정합니다.AIP-SSM이 실패하는 경우 ASA가 fail-open 상태로 전환되도록 하려면 Permit **traffic**을 클릭합니다.변경 사항을 커밋하려면 완료를 클릭합니다

.



7. 이제 ASA가 IPS 모듈로 트래픽을 전송하도록 구성되었습니다.ASA에 변경 사항을 기록하려면 맨 위 행에서 Save(저장)를 클릭합니다

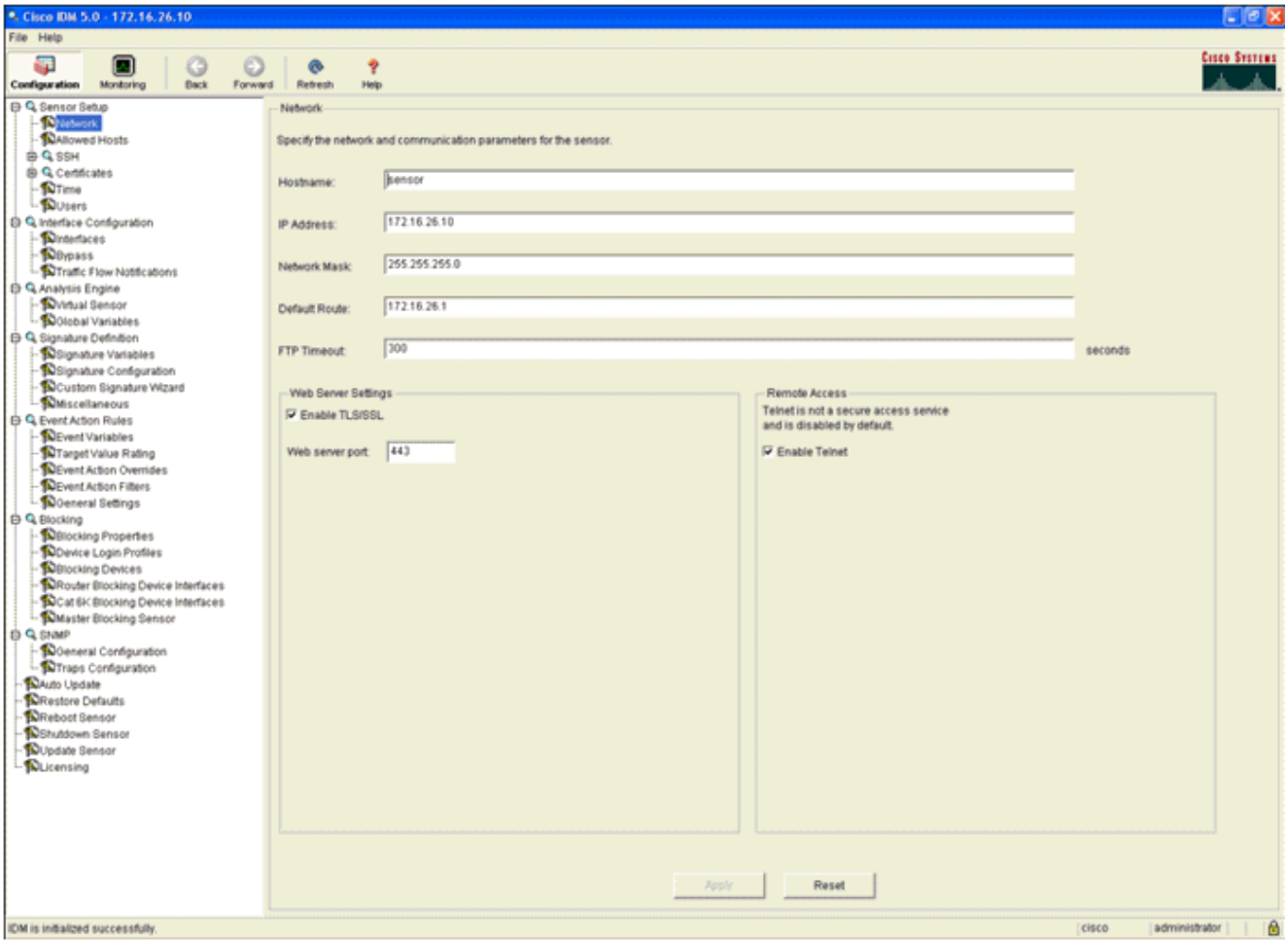
.



트래픽 검사를 위한 AIP-SSM 구성

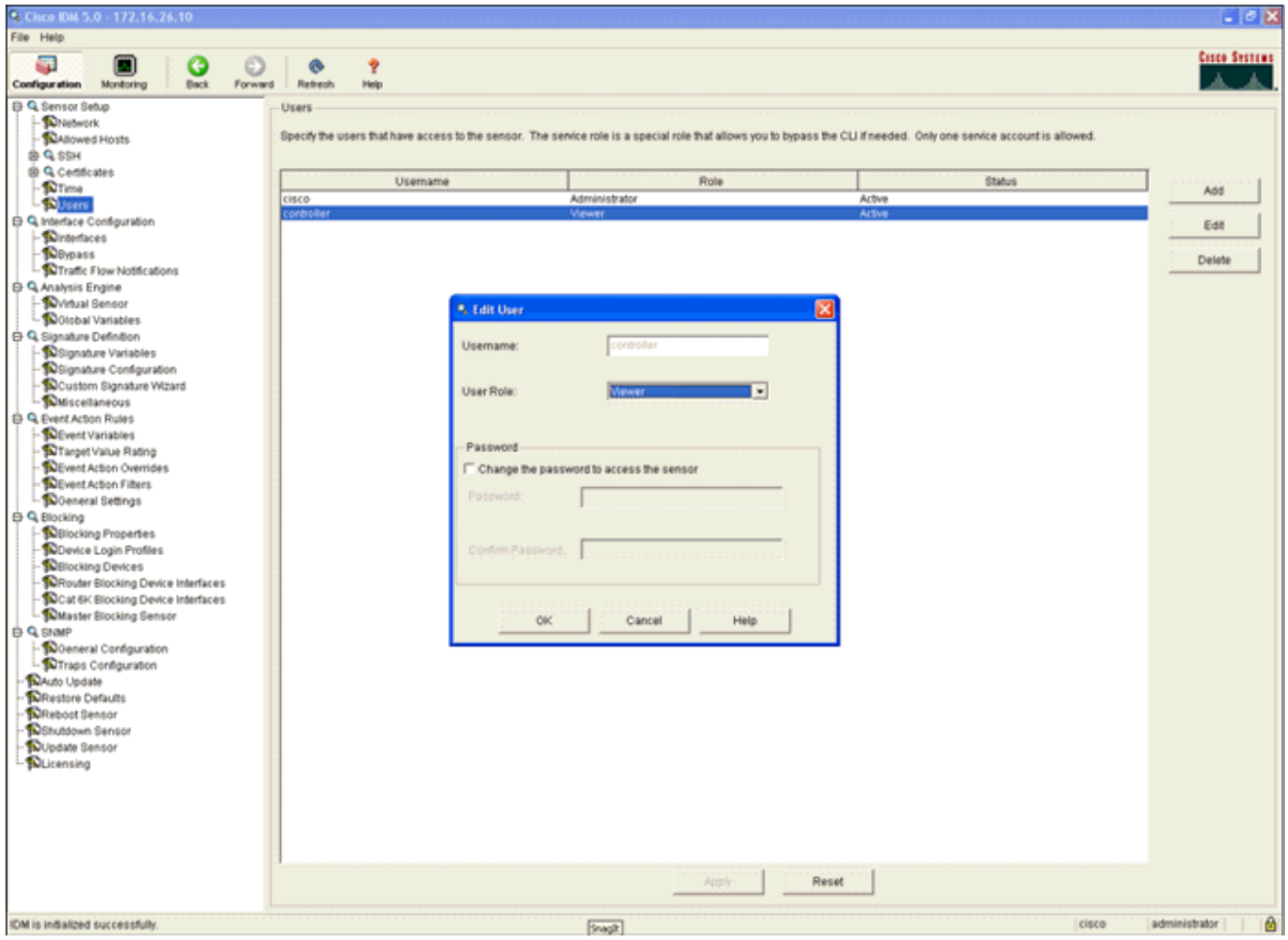
ASA가 IPS 모듈로 데이터를 전송하는 동안 AIP-SSM 인터페이스를 가상 센서 엔진에 연결합니다.

1. IDM을 사용하여 AIP-SSM에 로그인합니다
   .



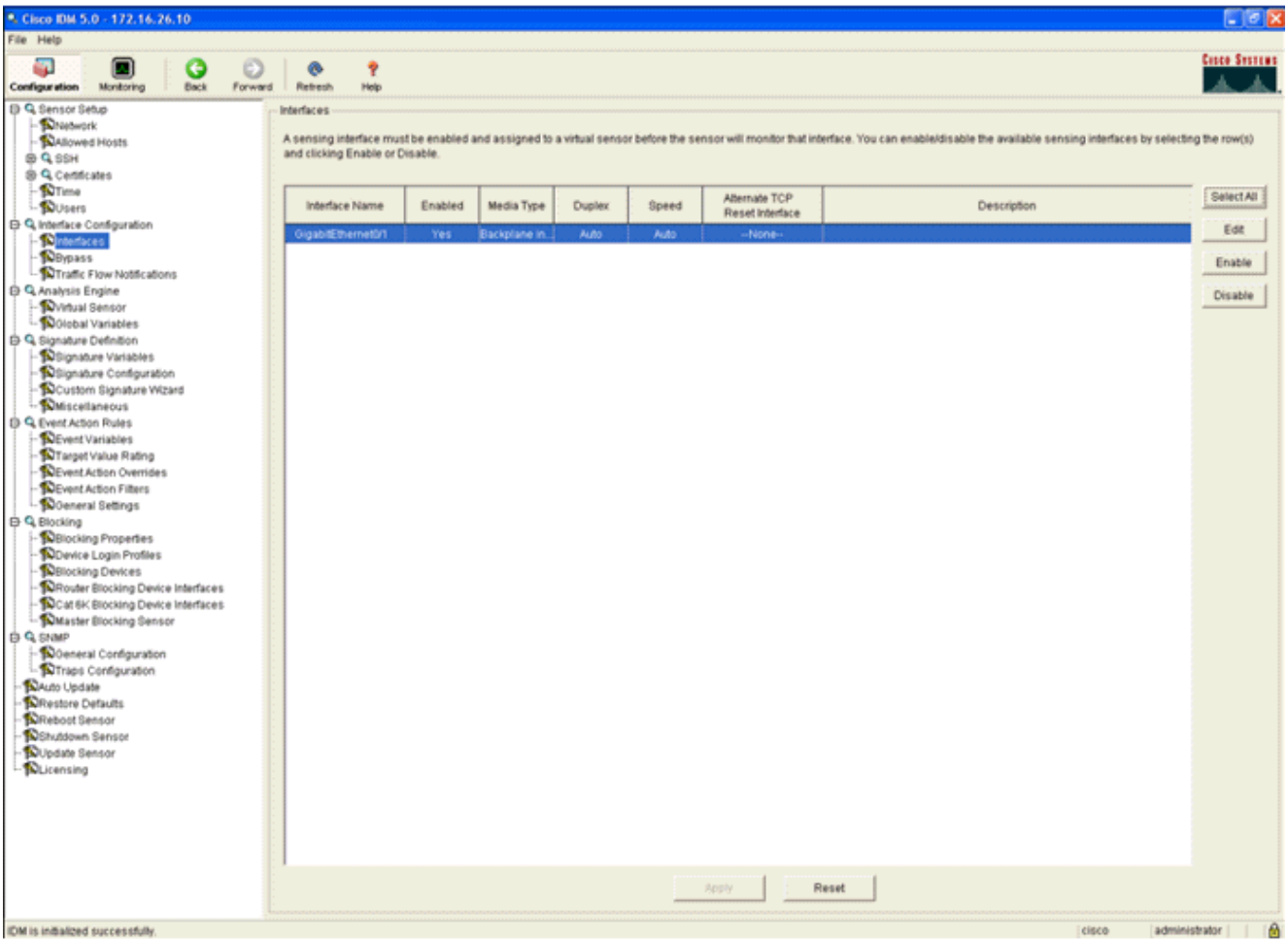
2. 최소한 뷰어 권한이 있는 사용자를 추가합니다

.



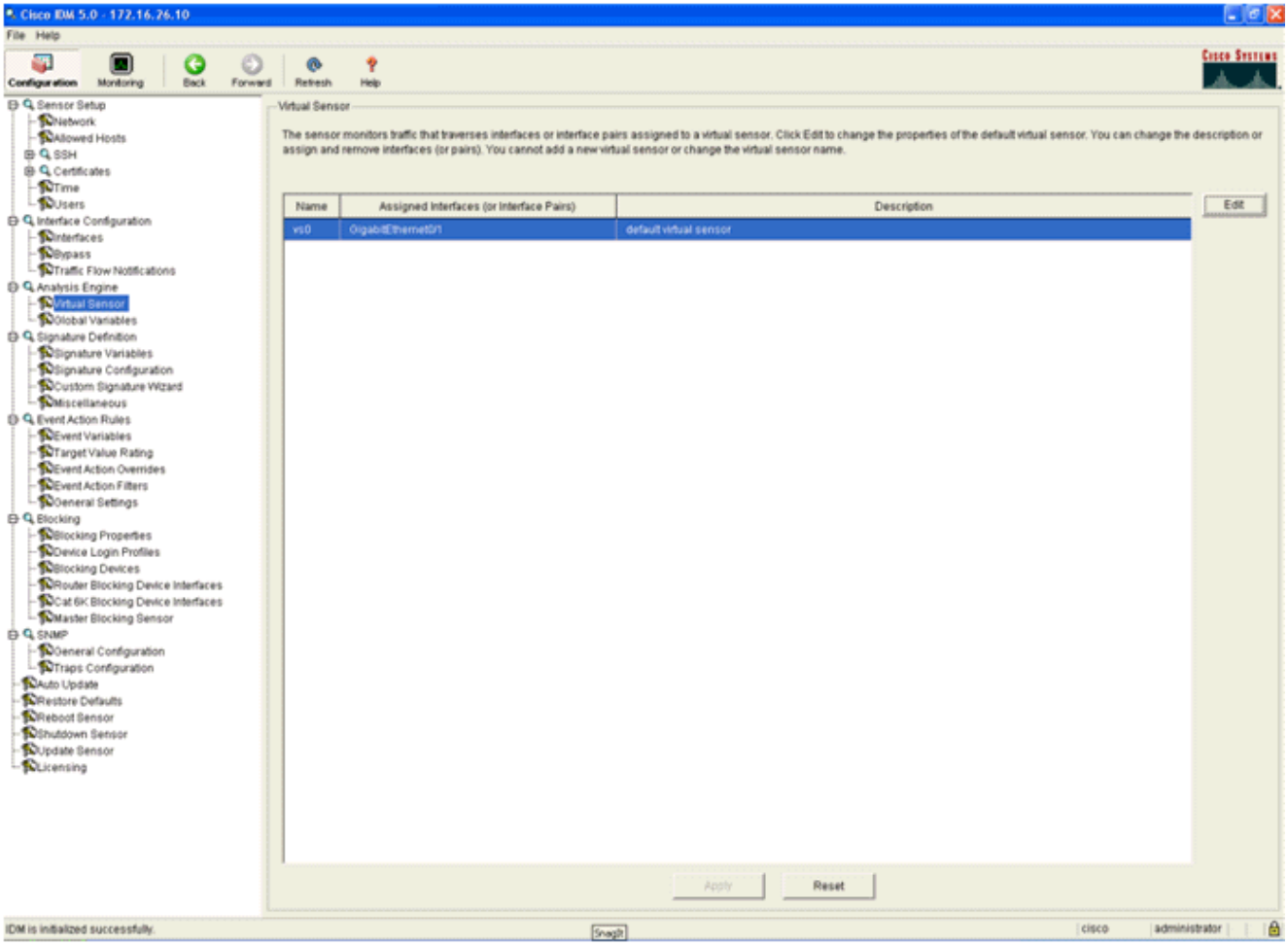
3. 인터페이스를 활성화합니다

.



4. Virtual Sensor 컨피그레이션을 확인합니다

.

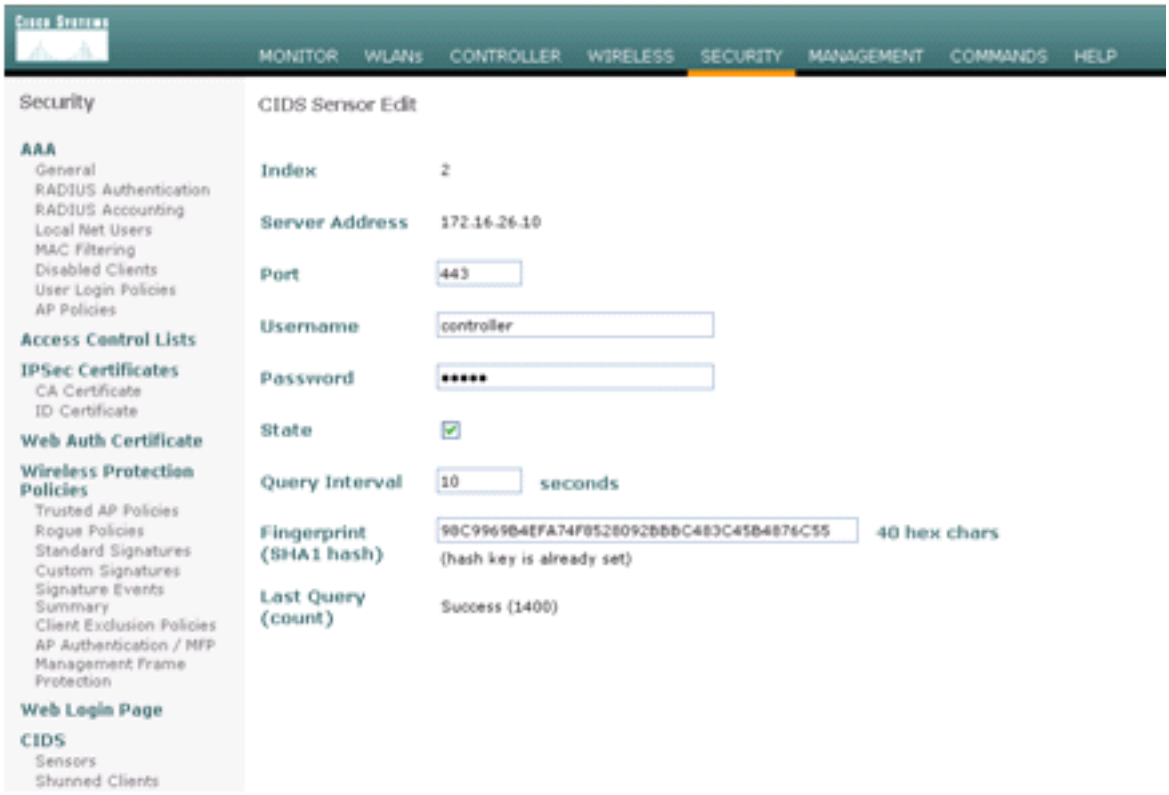


클라이언트 블록에 대해 AIP-SSM을 폴링하도록 WLC 구성

센서를 구성하고 컨트롤러에 추가할 준비가 되면 다음 단계를 완료합니다.

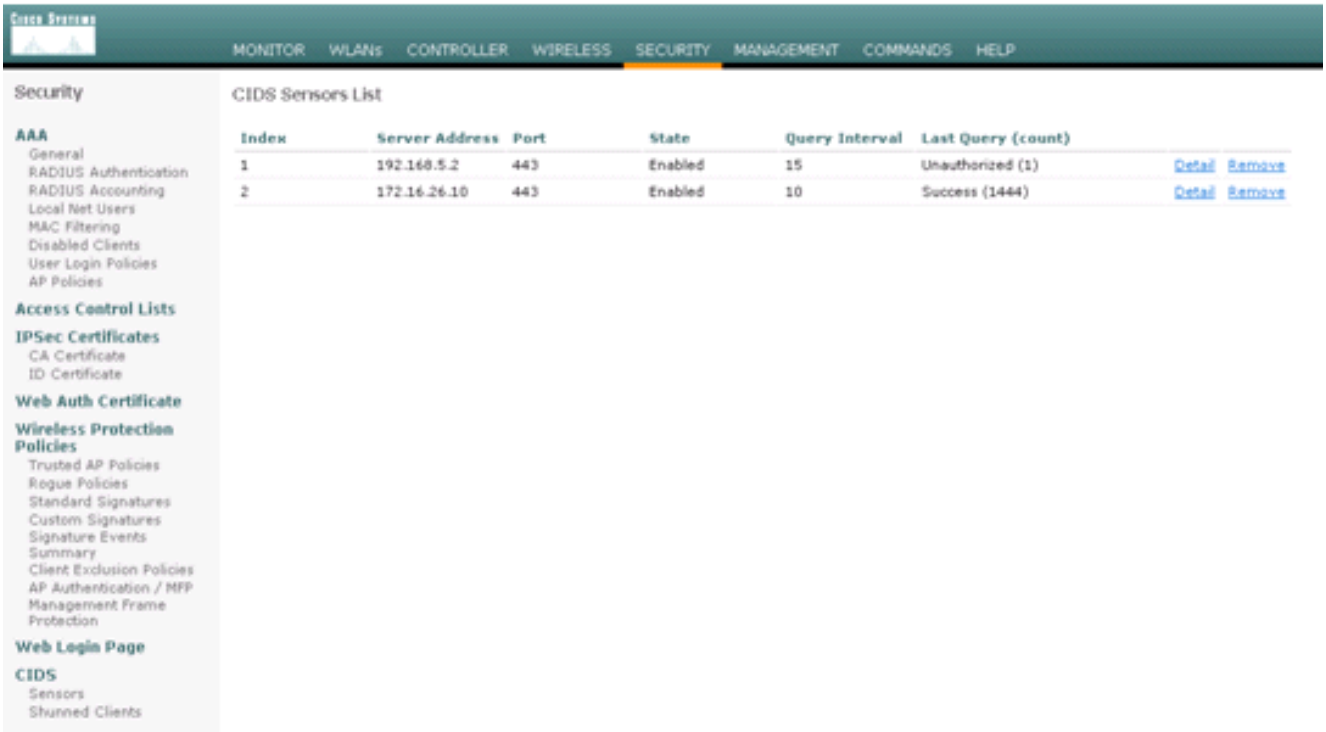
1. WLC에서 **Security > CIDS > Sensors > New**를 선택합니다.
2. 이전 섹션에서 생성한 IP 주소, TCP 포트 번호, 사용자 이름 및 비밀번호를 추가합니다.
3. 센서에서 핑거프린트를 가져오려면 센서에서 이 명령을 실행하고 WLC에 콜론 없이 SHA1 핑거프린트를 추가합니다. 이는 컨트롤러-IDS 폴링 통신을 보호하는 데 사용됩니다.

```
sensor#show tls fingerprint
MD5: 07:7F:E7:91:00:46:7F:BF:11:E2:63:68:E5:74:31:0E
SHA1: 98:C9:96:9B:4E:FA:74:F8:52:80:92:BB:BC:48:3C:45:B4:87:6C:55
```



4. AIP-SSM과 WLC 간의 연결 상태를 확인합니다

.

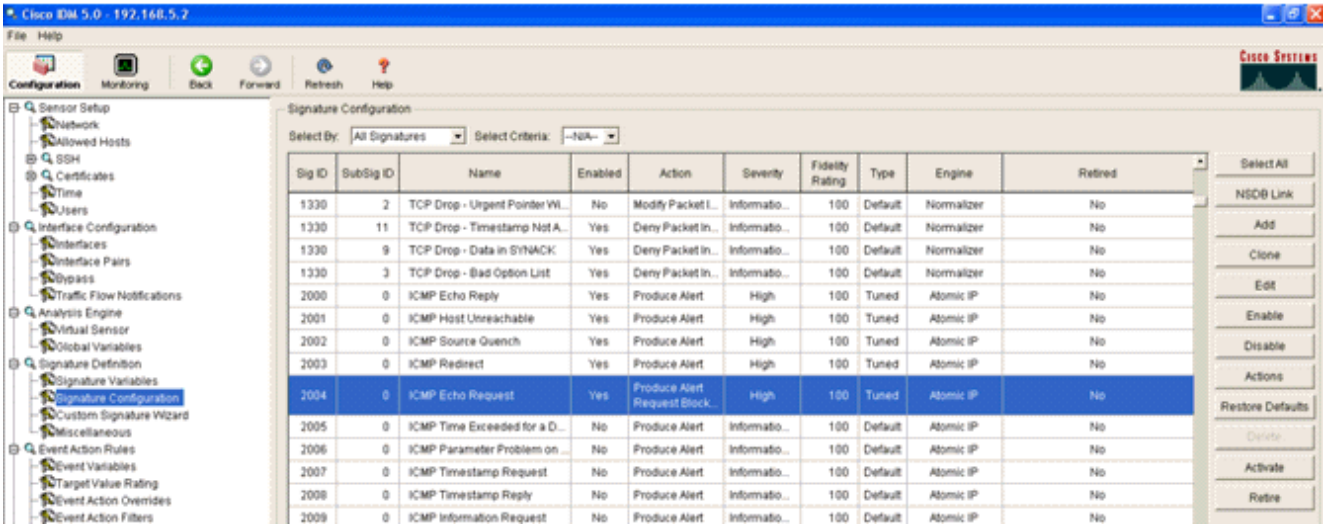


AIP-SSM에 차단 서명 추가

트래픽을 차단하려면 검사 서명을 추가합니다.사용 가능한 툴을 기반으로 작업을 수행할 수 있는 시그니처가 많이 있지만, 이 예에서는 ping 패킷을 차단하는 시그니처를 생성합니다.

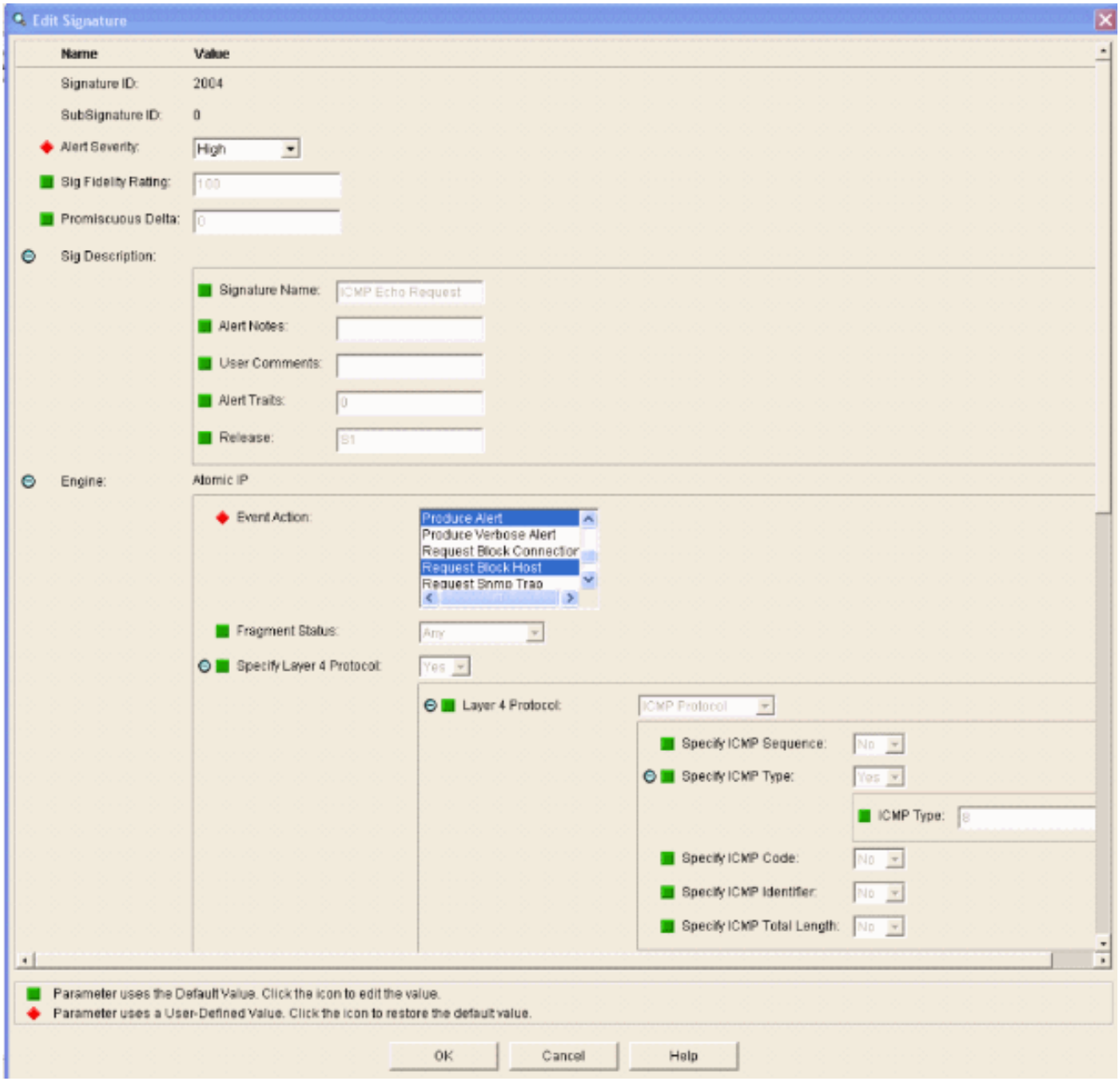
1. 빠른 설정 확인을 수행하려면 **2004 서명(ICMP Echo Request)**을 선택합니다

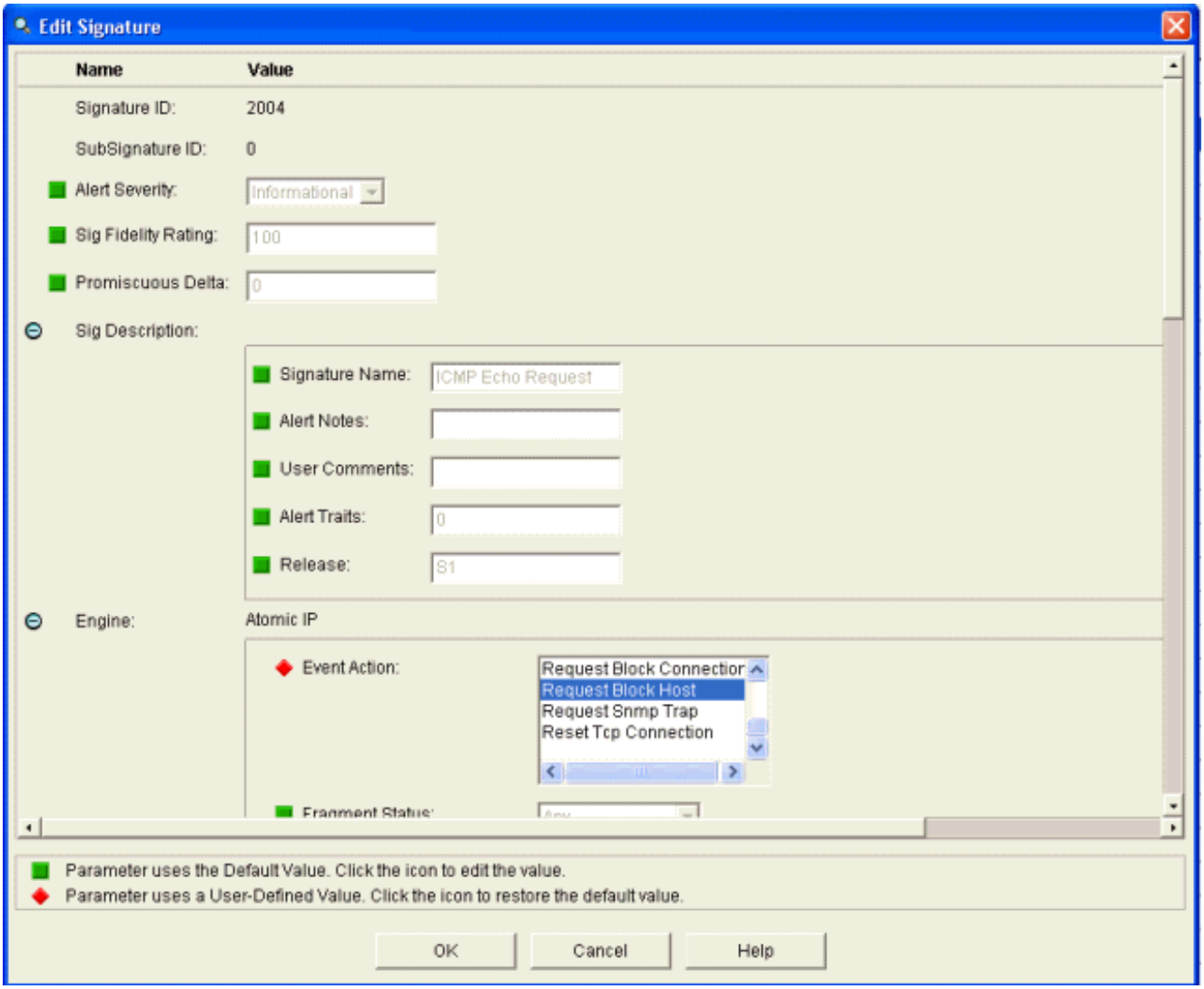
.



2. 서명을 활성화하고 Alert Severity(경고 심각도)를 **High(높음**)로 설정하고 Event Action(이벤트 작업)을 Produce Alert and **Request Block Host(경고 생성** 및 **요청 블록 호스트**)로 설정하여 이 확인 단계를 완료합니다.Request Block Host 작업은 클라이언트 예외를 생성하기 위해 WLC에 신호를 보내는 키입니다

.



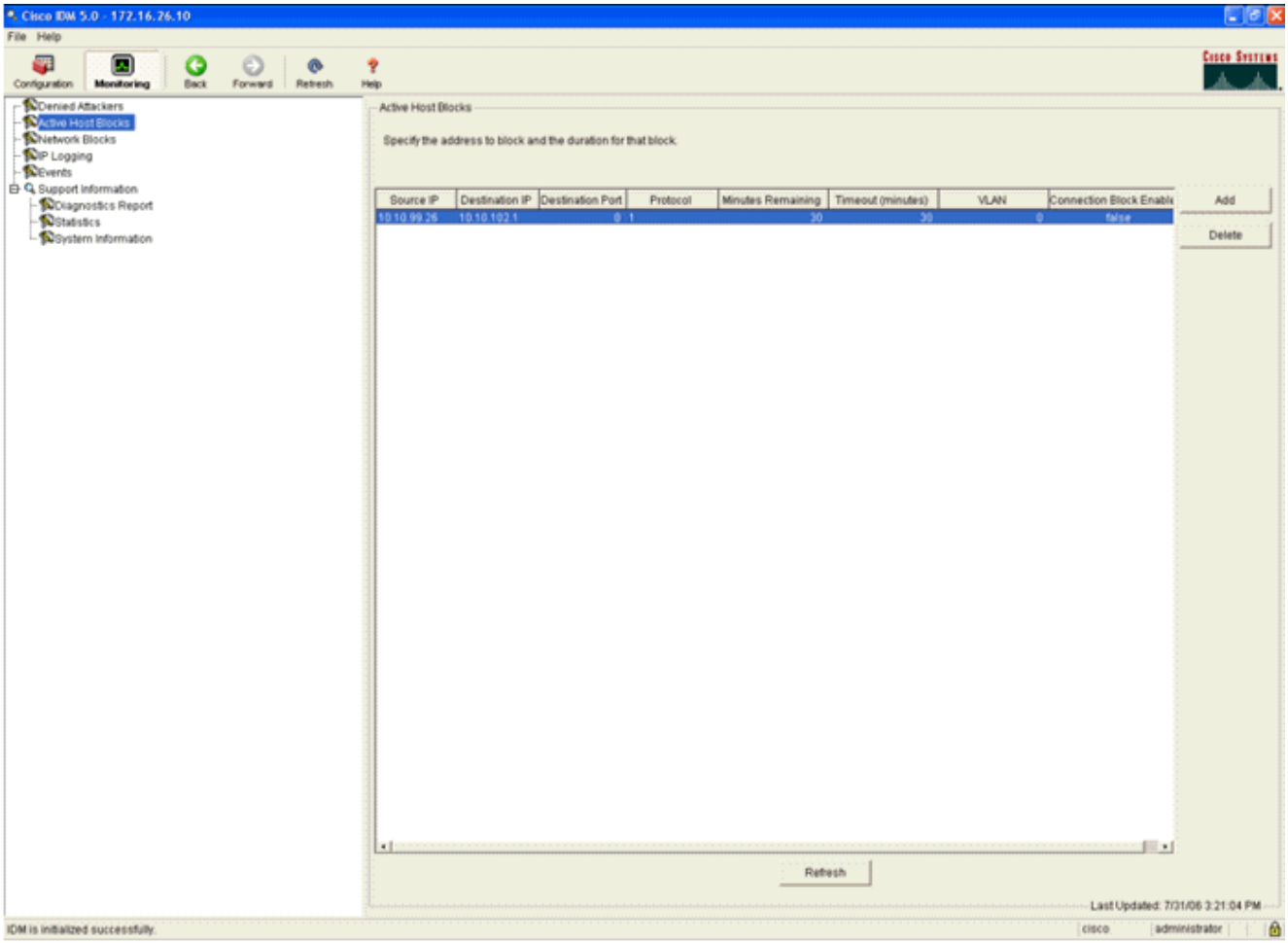


3. 서명을 저장하려면 확인을 클릭합니다.
4. 서명이 활성 상태이고 차단 작업을 수행하도록 설정되어 있는지 확인합니다.
5. 모듈에 서명을 커밋하려면 Apply를 클릭합니다.

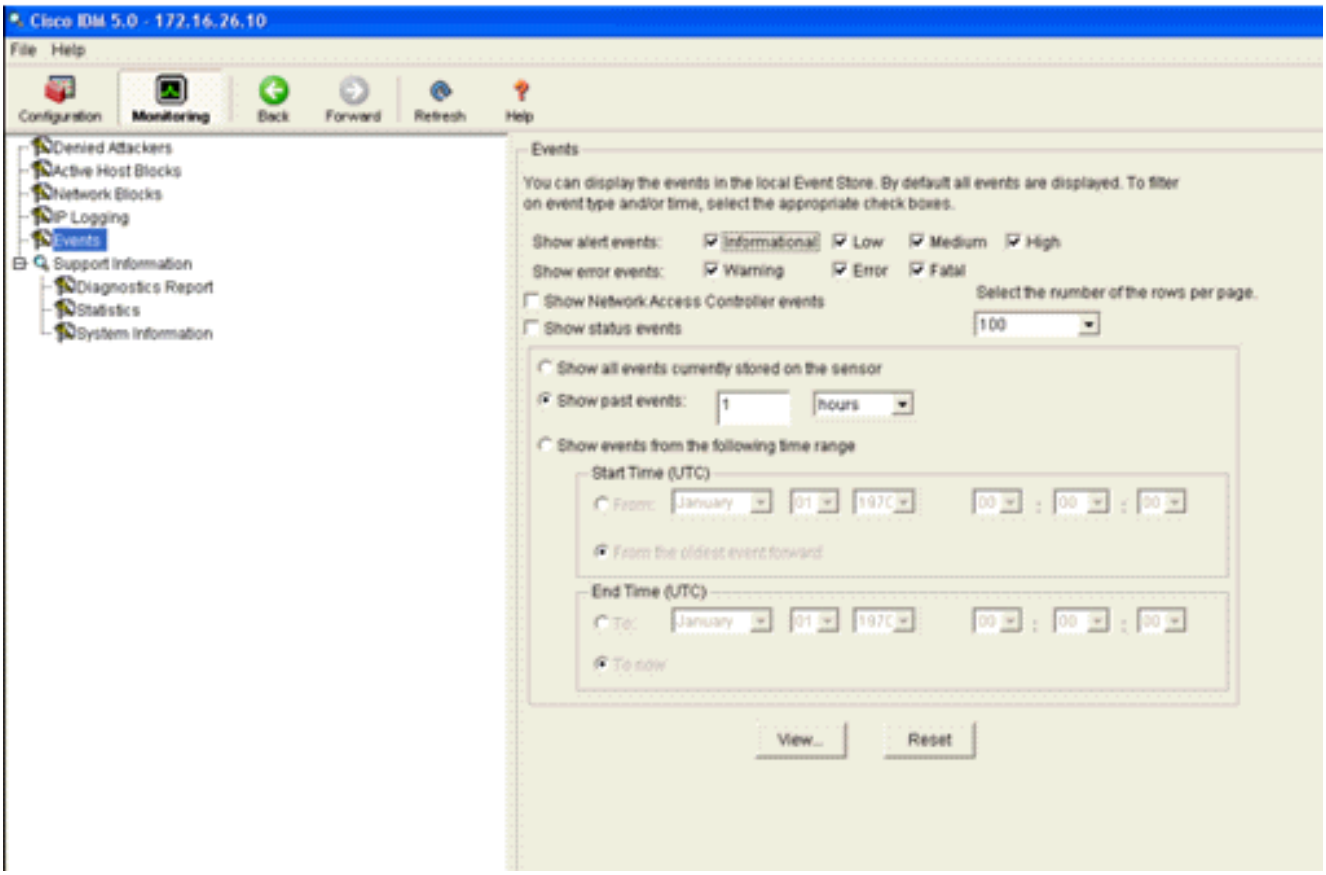
IDM으로 차단 및 이벤트 모니터링

다음 단계를 완료하십시오.

1. 서명이 성공적으로 실행되면 IDM에는 이 사항을 기록할 두 개의 위치가 있습니다.첫 번째 방법은 AIP-SSM이 설치한 활성 블록을 보여줍니다.맨 위 행의 Monitoring(모니터링)을 클릭합니다.왼쪽에 표시되는 항목 목록에서 **Active Host Blocks**를 선택합니다.Ping 서명이 트리거될 때마다 Active Host Blocks(활성 호스트 블록) 창에는 공격자의 IP 주소, 공격 중인 디바이스의 주소 및 차단이 적용되는 남은 시간이 표시됩니다.기본 차단 시간은 30분이며 조정 가능합니다.그러나 이 값의 변경은 이 문서에서 다루지 않습니다.이 매개 변수를 변경하는 방법에 대한 자세한 내용은 필요한 경우 ASA 구성 설명서를 참조하십시오.즉시 블록을 제거하고 목록에서 선택한 다음 **삭제**를 클릭합니다
.



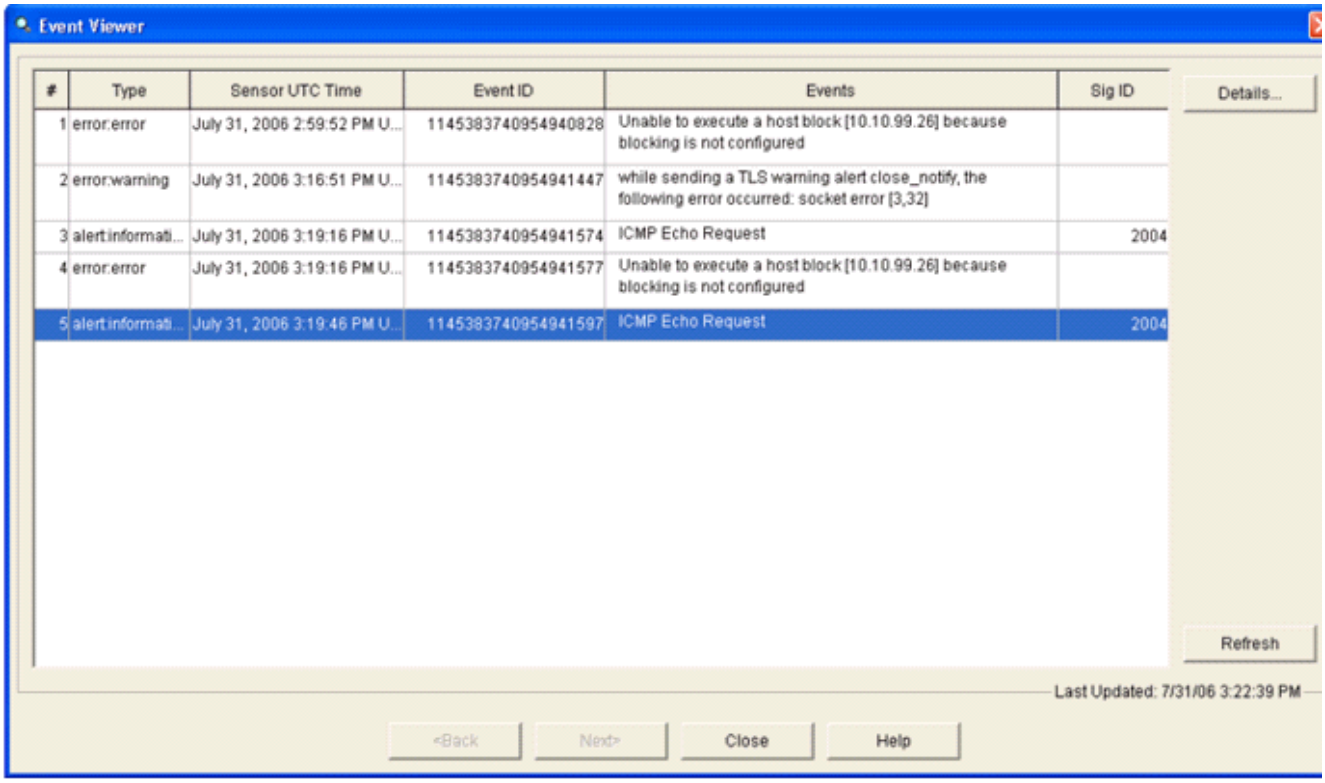
트리거된 시그니처를 보는 두 번째 방법은 AIP-SSM 이벤트 버퍼를 사용합니다.IDM Monitoring(IDM 모니터링) 페이지의 왼쪽에 있는 항목 목록에서 **Events(이벤트)**를 선택합니다.이벤트 검색 유틸리티가 나타납니다.적절한 검색 조건을 설정하고 보기...**를** 클릭합니다..



2. 그런 다음 지정된 기준과 일치하는 이벤트 목록과 함께 이벤트 뷰어가 나타납니다.목록을 스

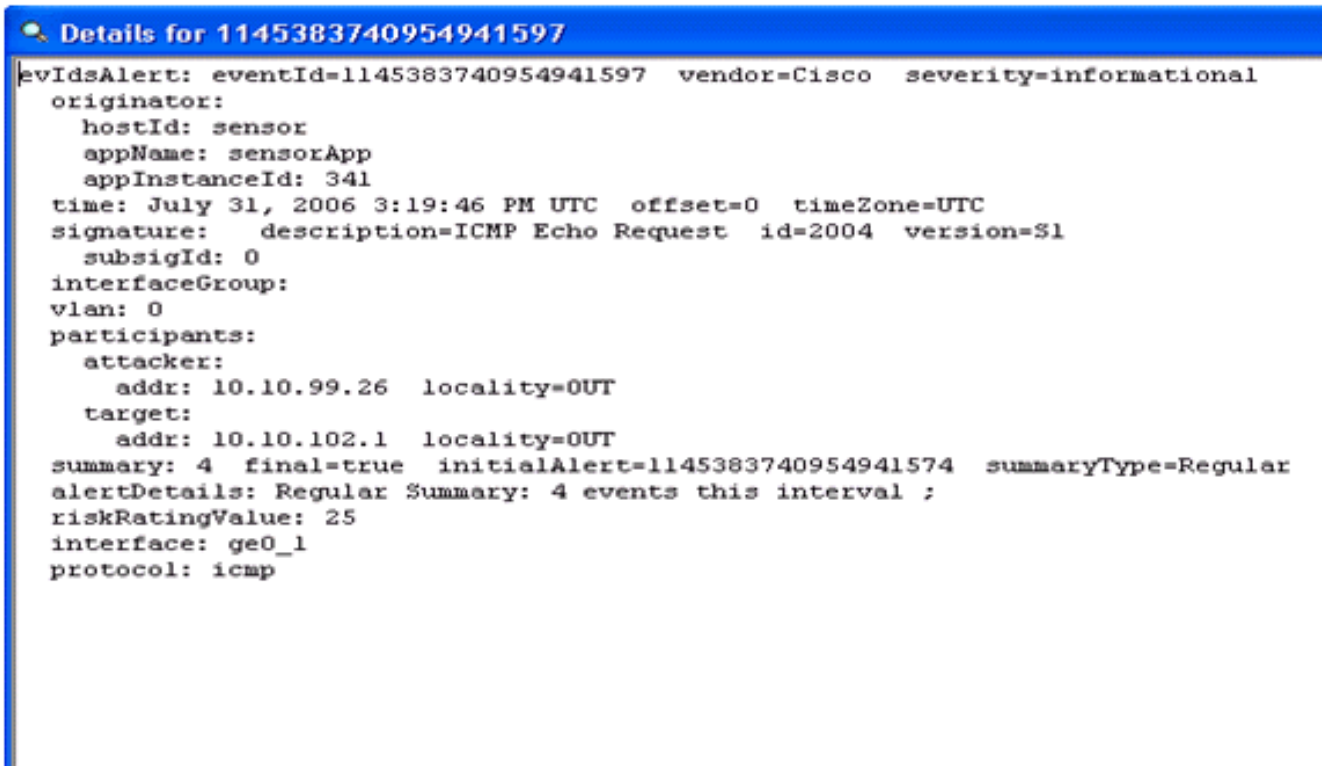
크롤하여 이전 컨피그레이션 단계에서 수정된 ICMP 에코 요청 서명을 찾습니다.Events 열에서 시그니처의 이름을 찾거나 Sig ID 열 아래에서 서명의 식별 번호를 검색합니다

.



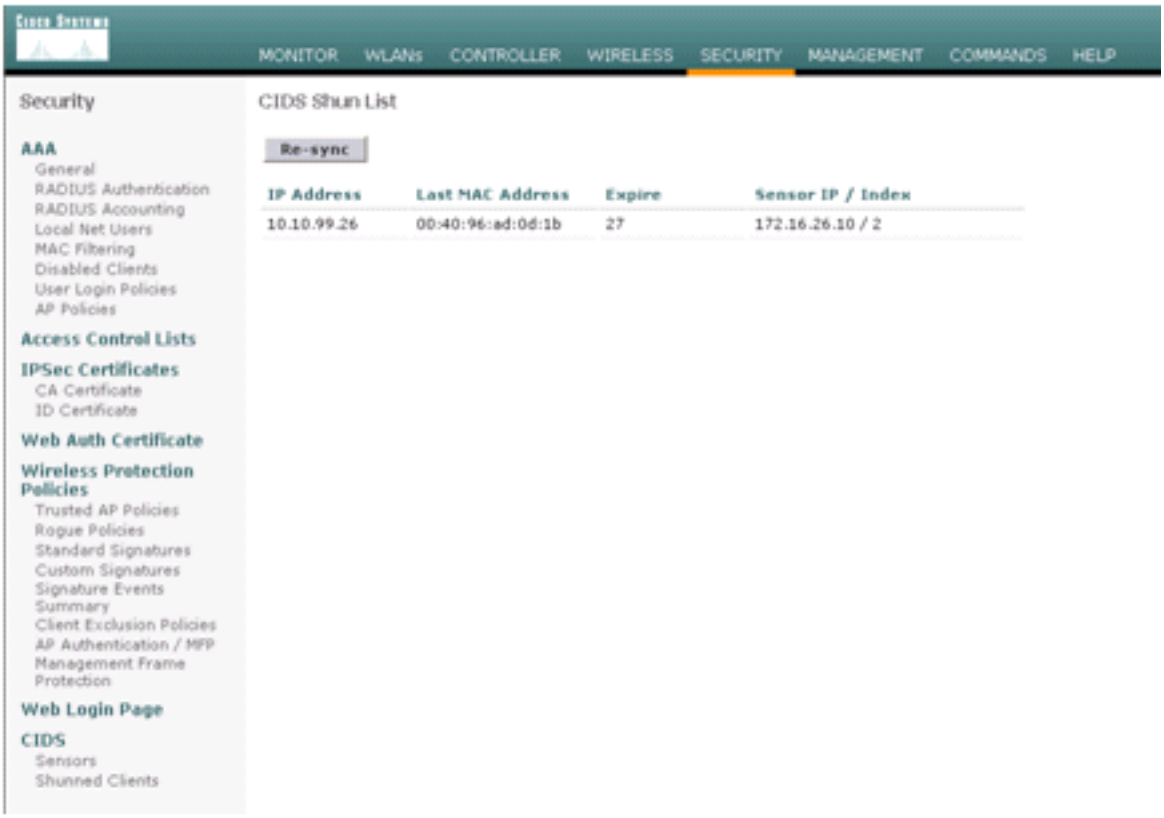
3. 서명을 찾은 후 새 창을 열려면 항목을 두 번 클릭합니다.새 창에는 서명을 트리거한 이벤트에 대한 자세한 정보가 포함되어 있습니다

.

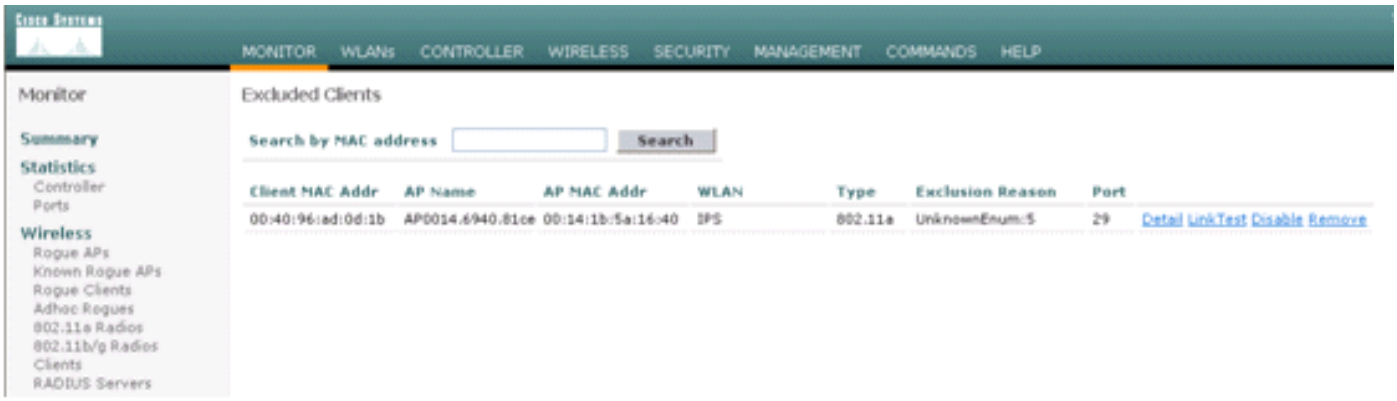


무선 컨트롤러에서 클라이언트 제외 모니터링

컨트롤러의 회피 클라이언트 목록은 이 시점에 호스트의 IP 및 MAC 주소로 채워집니다.



사용자가 클라이언트 제외 목록에 추가됩니다.

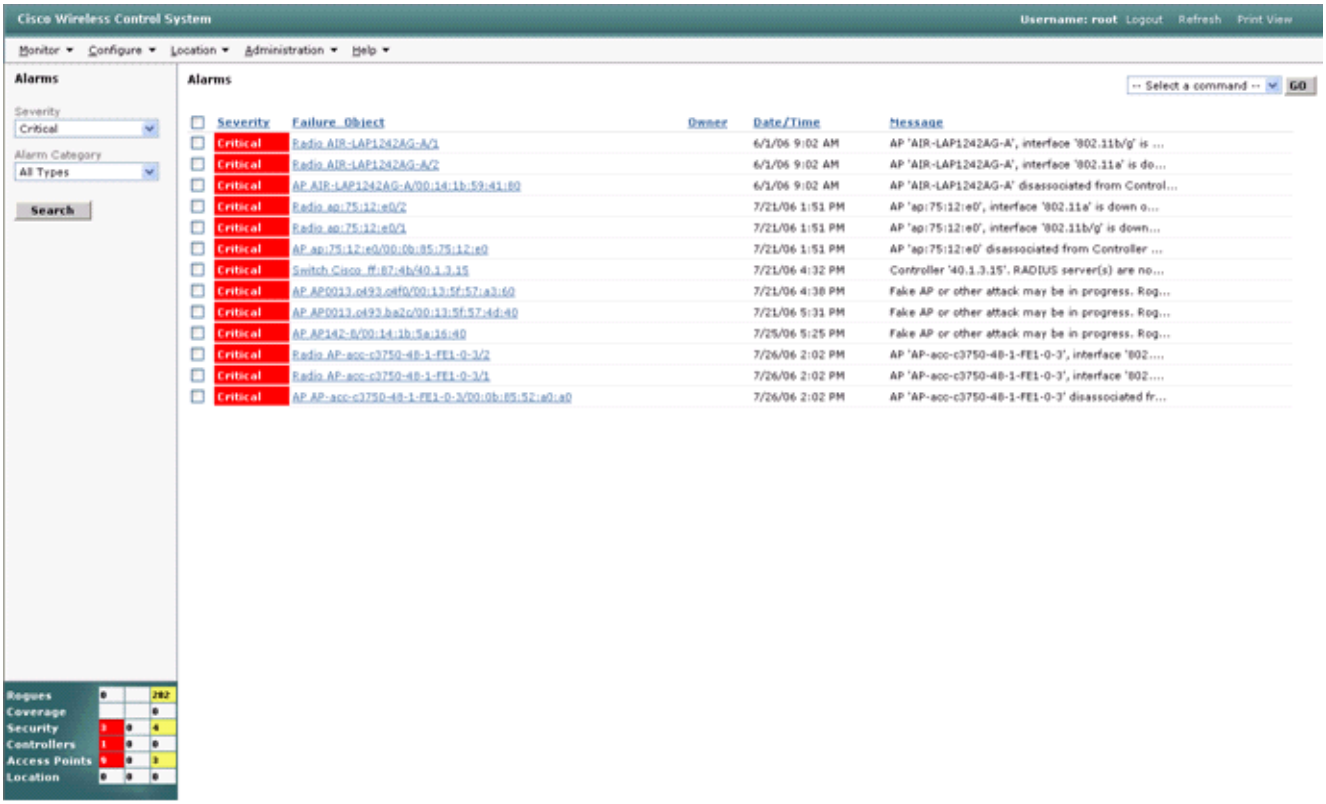


WCS에서 이벤트 모니터링

AIP-SSM 내에서 블록을 트리거하는 보안 이벤트로 인해 컨트롤러가 클라이언트 제외 목록에 위반자의 주소를 추가합니다.또한 WCS 내에서 이벤트가 생성됩니다.

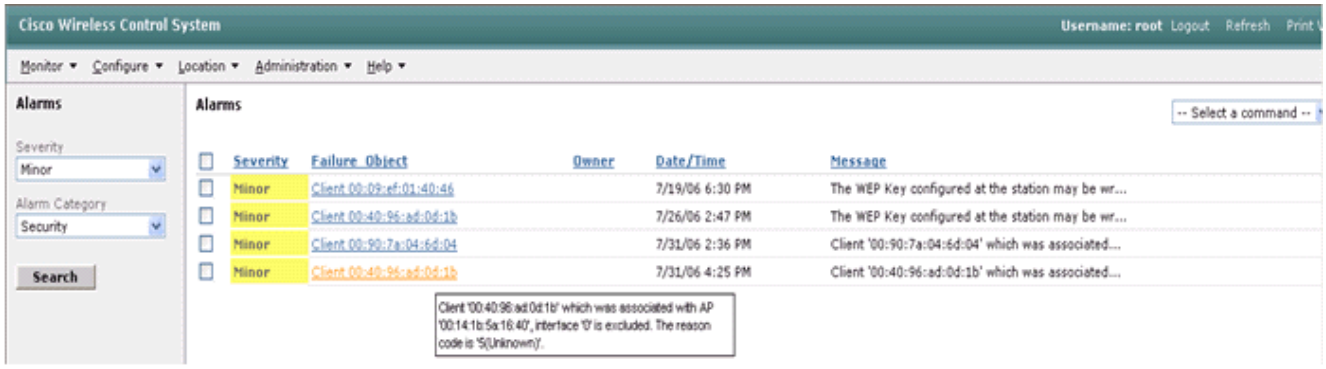
1. 제외 **이벤트를** 보려면 WCS 주 메뉴에서 Monitor(모니터링) > Alarms 유틸리티를 사용합니다.WCS는 처음에 모든 미연결 경보를 표시하고 창의 왼쪽에 검색 기능을 표시합니다.
2. 검색 조건을 수정하여 클라이언트 블록을 찾습니다.Severity(심각도)에서 **Minor(**마이너)를 선택하고 Alarm Category(경보 카테고리)를 Security(**보안**)로 **설정합니다**.
3. Search를 **클릭합니다**

.



4. 그런 다음 Alarm(경보) 창에 심각도가 낮은 보안 경보입니다.AIP-SSM 내에서 블록을 트리거한 이벤트를 마우스로 가리킵니다.특히 WCS는 경보를 발생시킨 클라이언트 스테이션의 MAC 주소를 표시합니다.적절한 주소를 가리키면 WCS는 이벤트 세부사항이 포함된 작은 창을 팝업합니다.다른 창에서 동일한 세부 정보를 보려면 링크를 클릭합니다

.



Cisco ASA 샘플 컨피그레이션

```
ciscoasa#show run
: Saved
:
ASA Version 7.1(2)
!
hostname ciscoasa
domain-name cisco.com
enable password 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 10.10.102.2 255.255.255.0
!
```

```
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 172.16.26.2 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 nameif management
 security-level 100
 ip address 192.168.1.1 255.255.255.0
 management-only
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name cisco.com
pager lines 24
logging asdm informational
mtu inside 1500
mtu management 1500
mtu outside 1500
asdm image disk0:/asdm512-k8.bin
no asdm history enable
arp timeout 14400
nat-control
global (outside) 102 interface
nat (inside) 102 172.16.26.0 255.255.255.0
nat (inside) 102 0.0.0.0 0.0.0.0
route inside 0.0.0.0 0.0.0.0 172.16.26.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
http server enable
http 10.1.1.12 255.255.255.255 inside
http 0.0.0.0 0.0.0.0 inside
http 192.168.1.0 255.255.255.0 management
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet 0.0.0.0 0.0.0.0 inside
telnet timeout 5
ssh timeout 5
console timeout 0
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 50
dhcpd enable management
!
class-map inside-class
 match any
!
!
policy-map inside-policy
 description IDS-inside-policy
 class inside-class
  ips promiscuous fail-open
!
```

```
service-policy inside-policy interface inside
Cryptochecksum:699d110f988e006f6c5c907473939b29
: end
ciscoasa#
```

Cisco Intrusion Prevention System Sensor 샘플 컨피그레이션

```
sensor#show config
! ------------------------------
! Version 5.0(2)
! Current configuration last modified Tue Jul 25 12:15:19 2006
! ------------------------------
service host
network-settings
host-ip 172.16.26.10/24,172.16.26.1
telnet-option enabled
access-list 10.0.0.0/8
access-list 40.0.0.0/8
exit
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
signatures 2004 0
engine atomic-ip
event-action produce-alert|request-block-host
exit
status
enabled true
exit
exit
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service authentication
exit
! ------------------------------
service web-server
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service analysis-engine
virtual-sensor vs0
description default virtual sensor
physical-interface GigabitEthernet0/1
exit
exit
! ------------------------------
service interface
exit
! ------------------------------
```

```
service trusted-certificates
exit
sensor#
```

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- Cisco Intrusion Prevention System Device Manager 5.1 설치 및 사용
- Cisco ASA 5500 Series Adaptive Security Appliances - 컨피그레이션 가이드
- Command Line Interface 5.0을 사용하여 Cisco Intrusion Prevention System Sensor 구성 - 인터페이스 구성
- WLC 컨피그레이션 가이드 4.0
- 무선 기술 지원
- WLC(Wireless LAN Controller) FAQ
- 무선 LAN 컨트롤러 및 경량 액세스 포인트 기본 구성 예
- 보안 솔루션 구성
- 기술 지원 및 문서 – Cisco Systems