Aironet AP의 ACL 필터 컨피그레이션 예

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[배경 정보](#)
[구성](#)
[ACL 생성 위치](#)
[MAC 주소 필터](#)
[IP 필터](#)
[이더 타입 필터](#)

소개

이 문서에서는 GUI를 사용하여 Cisco Aironet AP(Access Point)에서 ACL(Access Control List) 기반 필터를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대한 기본 지식을 갖춘 것을 권장합니다.

- Aironet AP 및 Aironet 802.11 a/b/g Client Adapter 사용을 통한 무선 연결 구성
- ACL

사용되는 구성 요소

이 문서에서는 Cisco IOS® 소프트웨어 릴리스 15.2(2)JB를 실행하는 Aironet 1040 Series AP를 사용합니다.

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.

배경 정보

AP에서 필터를 사용하여 다음 작업을 수행할 수 있습니다.

- 무선 LAN(WLAN) 네트워크에 대한 액세스 제한

- 추가 무선 보안 레이어 제공

다음과 같은 기준으로 트래픽을 필터링하려면 다양한 유형의 필터를 사용할 수 있습니다.

- 특정 프로토콜
- 클라이언트 장치의 MAC 주소
- 클라이언트 장치의 IP 주소

유선 LAN에서 사용자의 트래픽을 제한하기 위해 필터를 활성화할 수도 있습니다. IP 주소 및 MAC 주소 필터는 특정 IP 또는 MAC 주소로 또는 그로부터 전송되는 유니캐스트 및 멀티캐스트 패킷의 전달을 허용하거나 허용하지 않습니다.

프로토콜 기반 필터는 AP의 이더넷 및 무선 인터페이스를 통해 특정 프로토콜에 대한 액세스를 보다 세분화할 수 있는 방법을 제공합니다. 다음 방법 중 하나를 사용하여 AP에 필터를 구성할 수 있습니다.

- 웹 GUI
- CLI

이 문서에서는 GUI를 통해 필터를 구성하기 위해 ACL을 사용하는 방법에 대해 설명합니다.

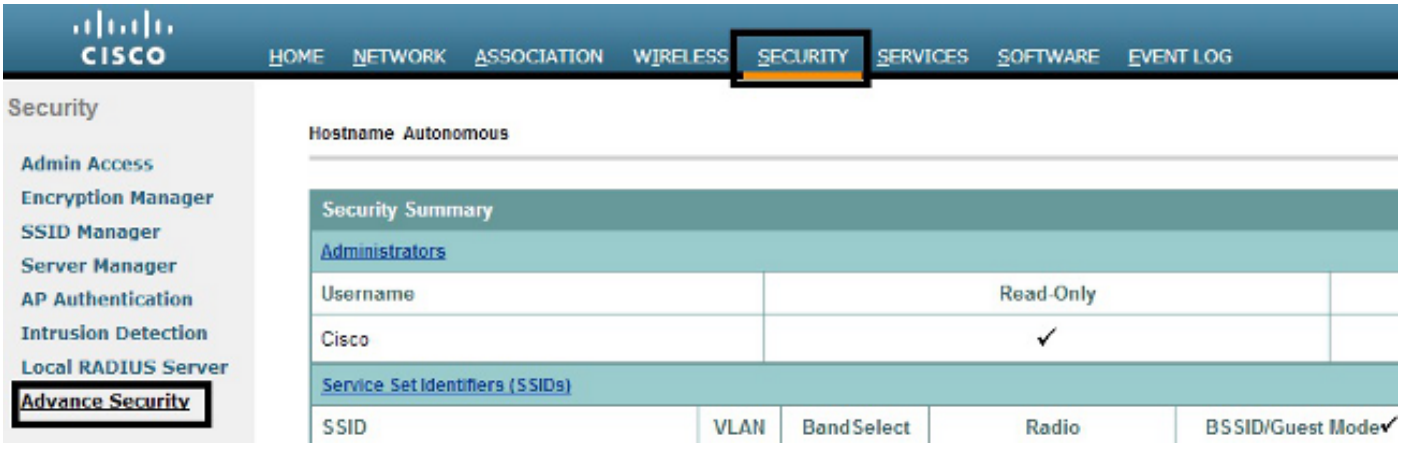
> 참고: CLI 사용을 통한 컨피그레이션에 대한 자세한 내용은 액세스 포인트 ACL 필터 컨피그레이션 예 Cisco 기사를 참조하십시오.

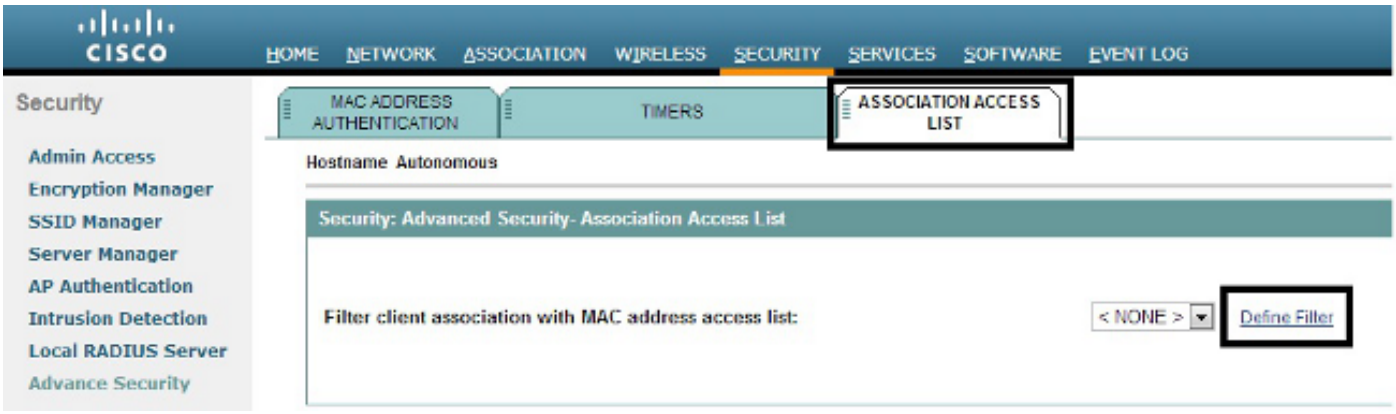
구성

이 섹션에서는 GUI를 사용하여 Cisco Aironet AP에서 ACL 기반 필터를 구성하는 방법에 대해 설명합니다.

ACL 생성 위치

Security(보안) > Advance Security(고급 보안)로 이동합니다. Association Access List(연결 액세스 목록) 탭을 선택하고 Define Filter(필터 정의)를 클릭합니다.



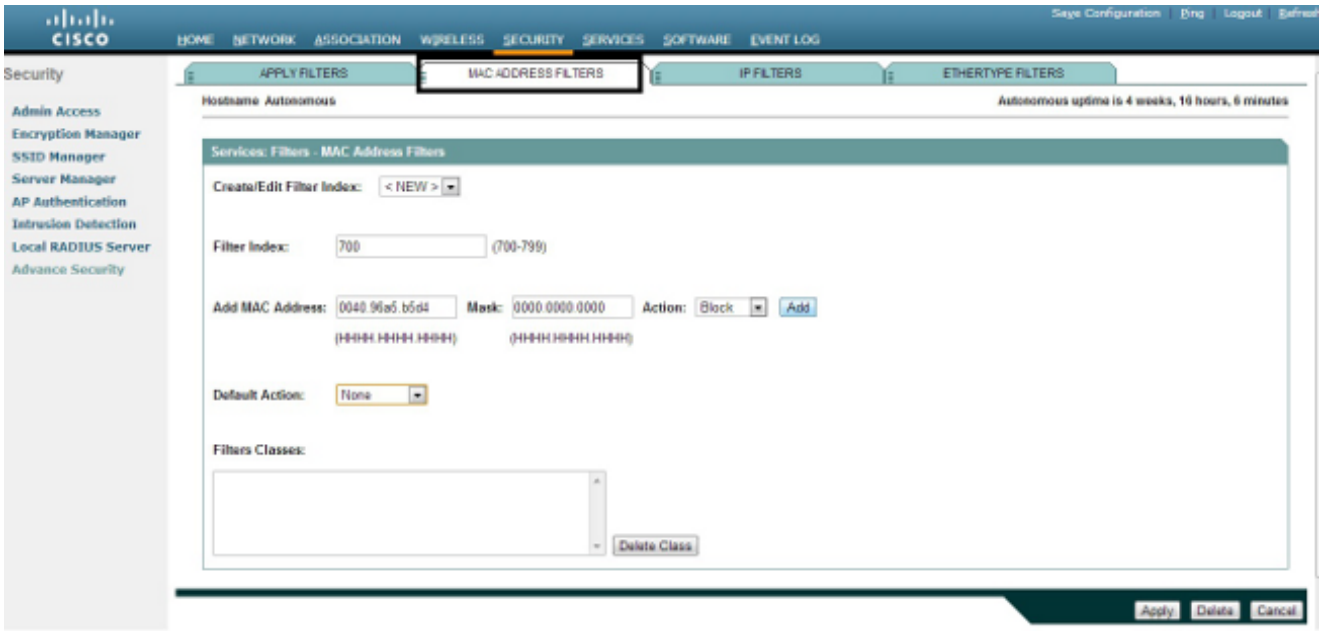


MAC 주소 필터

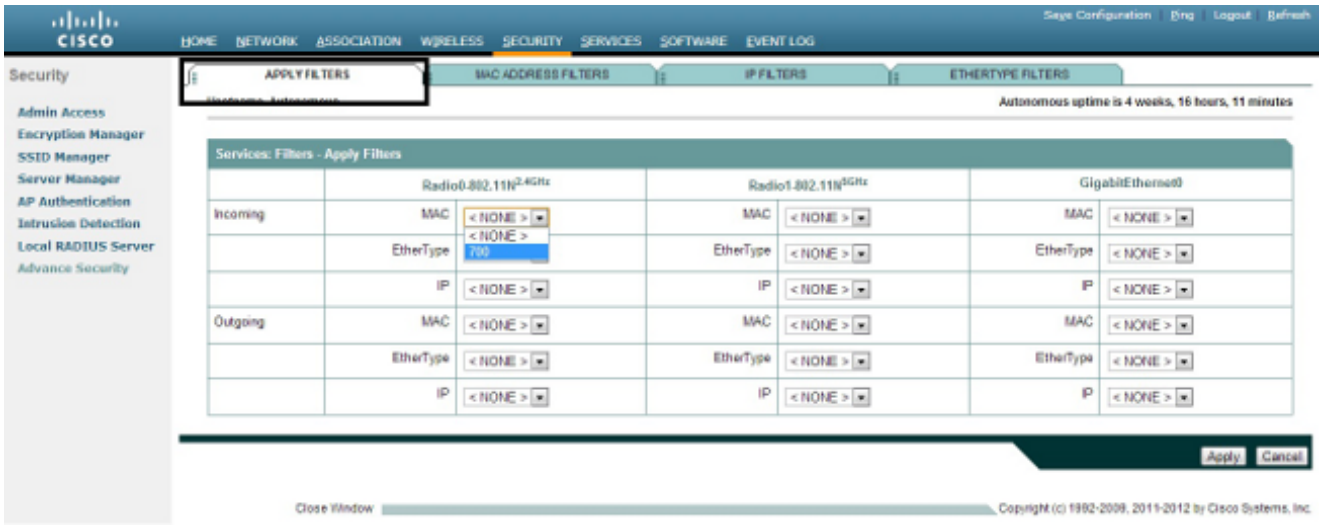
하드 코딩된 MAC 주소를 기반으로 클라이언트 디바이스를 필터링하려면 MAC 주소 기반 필터를 사용할 수 있습니다. MAC 기반 필터를 통해 클라이언트에 대한 액세스가 거부되면 클라이언트는 AP와 연결할 수 없습니다. MAC 주소 필터는 특정 MAC 주소에서 보내거나 주소로 보내는 유니캐스트 및 멀티캐스트 패킷의 전달을 허용하거나 허용하지 않습니다.

다음 예에서는 MAC 주소가 0040.96a5.b5d4인 클라이언트를 필터링하기 위해 GUI를 통해 MAC 기반 필터를 구성하는 방법을 보여 줍니다.

1. MAC 주소 ACL 700을 생성합니다. 이 ACL에서는 클라이언트 0040.96a5.b5d4를 AP와 연결할 수 없습니다.



2. 필터 클래스에 이 필터를 추가하려면 Add를 클릭합니다. 기본 작업을 모두 전달 또는 모두 거부로 정의할 수도 있습니다.
3. 적용을 클릭합니다. 이제 ACL 700이 생성됩니다.
4. 무선 인터페이스에 ACL 700을 적용하려면 Apply Filters(필터 적용) 섹션으로 이동합니다. 이제 이 ACL을 수신 또는 발신 라디오 또는 GigabitEthernet 인터페이스에 적용할 수 있습니다.



IP 필터

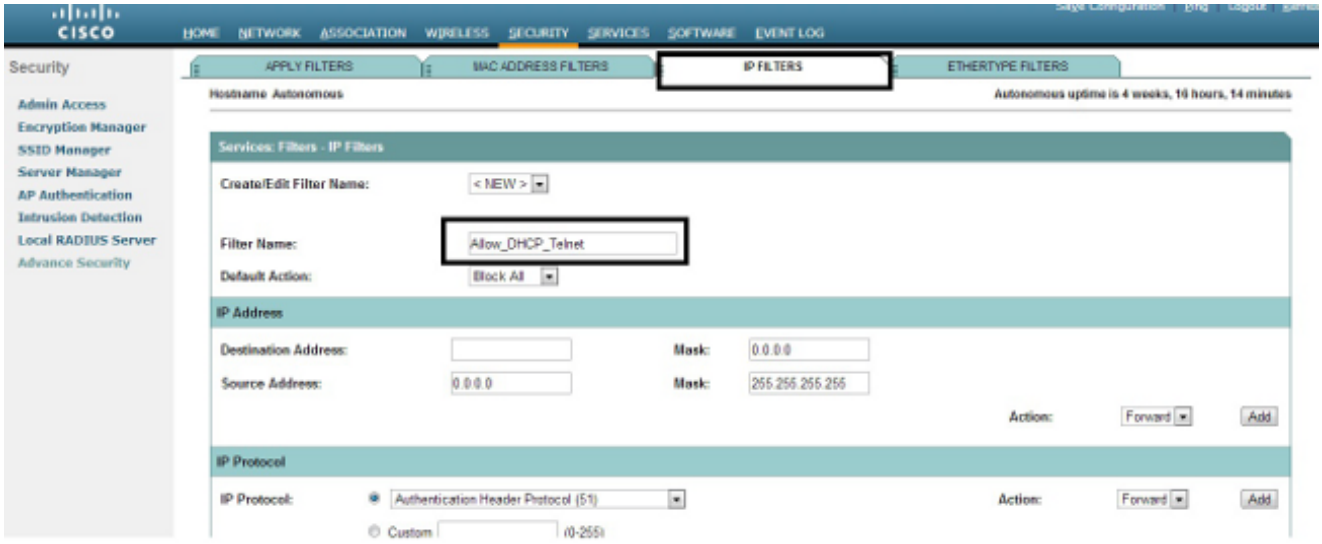
표준 또는 확장 ACL을 사용하여 클라이언트의 IP 주소를 기반으로 WLAN 네트워크에 클라이언트 디바이스를 입력하는 것을 허용하거나 허용하지 않을 수 있습니다.

이 컨피그레이션 예에서는 확장 ACL을 사용합니다. 확장 ACL은 클라이언트에 대한 텔넷 액세스를 허용해야 합니다. WLAN 네트워크의 다른 모든 프로토콜을 제한해야 합니다. 또한 클라이언트는 IP 주소를 얻기 위해 DHCP를 사용합니다. 다음과 같은 확장 ACL을 생성해야 합니다.

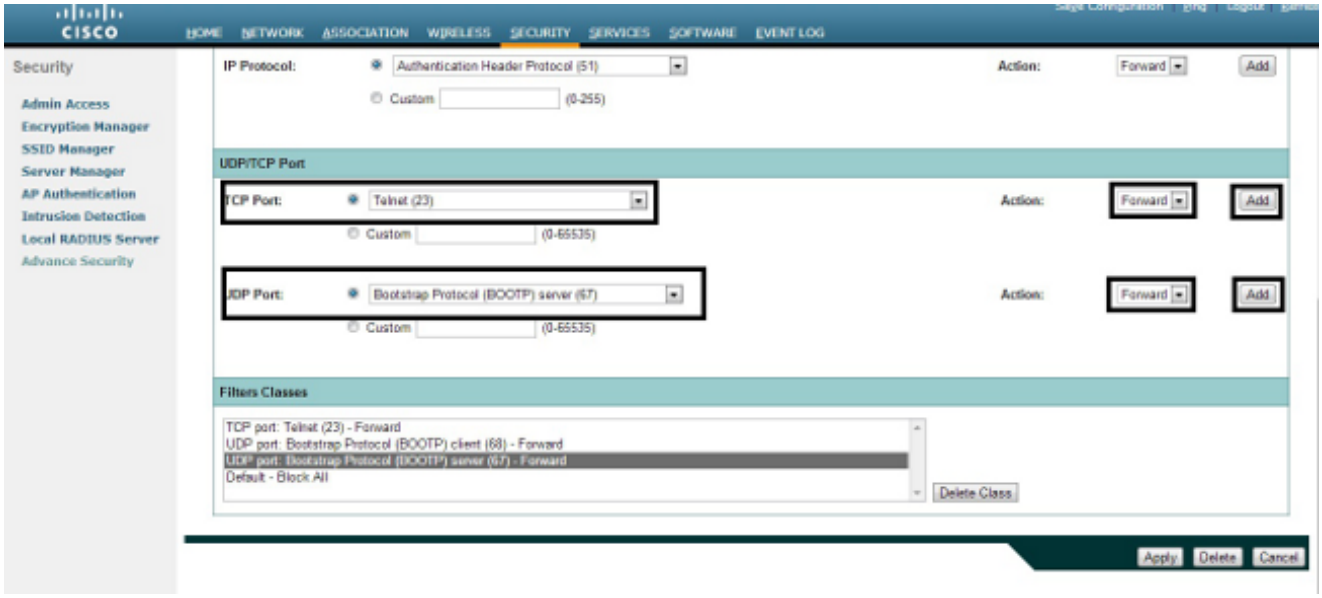
- DHCP 및 텔넷 트래픽 허용
- 다른 모든 트래픽 유형을 거부합니다

작성하려면 다음 단계를 완료하십시오.

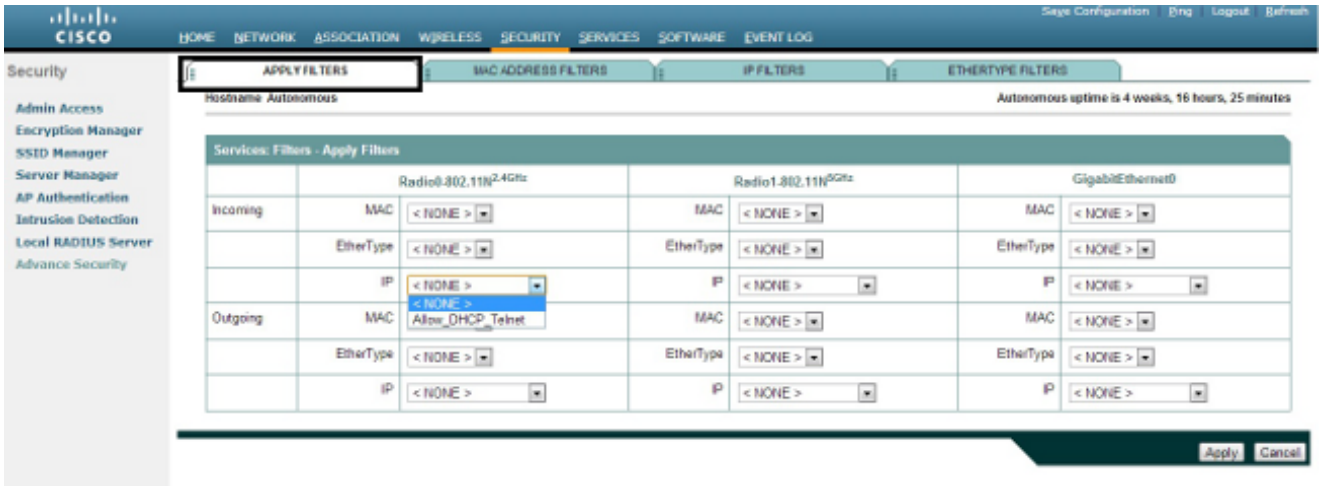
1. 나머지 트래픽은 차단해야 하므로 필터의 이름을 지정하고 Default Action 드롭다운 목록에서 Block All을 선택합니다.



2. TCP Port(TCP 포트) 드롭다운 목록에서 Telnet(텔넷)을 선택하고 UDP Port(UDP 포트) 드롭다운 목록에서 BOOTP 클라이언트 및 BOOTP 서버(BOOTP 서버)를 선택합니다.



3. 적용을 클릭합니다. 이제 IP 필터 Allow_DHCP?_Telnet이 생성되며 이 ACL을 수신 또는 발신 라디오 또는 GigabitEthernet 인터페이스에 적용할 수 있습니다.

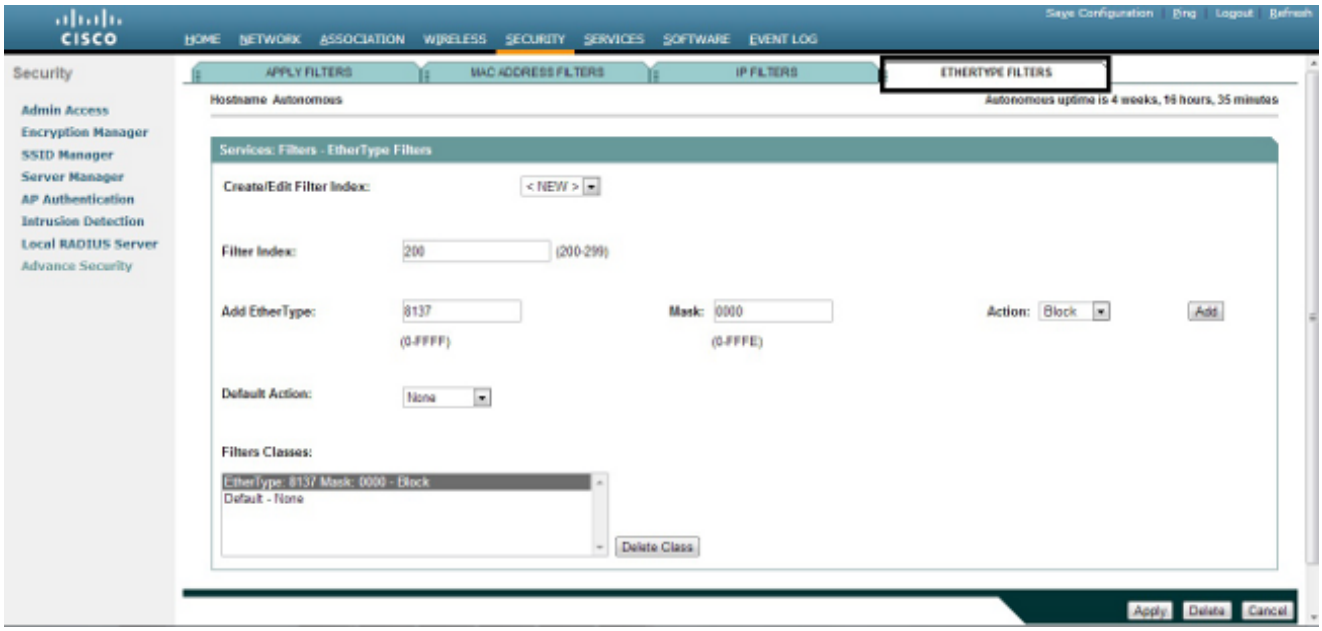


이더 타입 필터

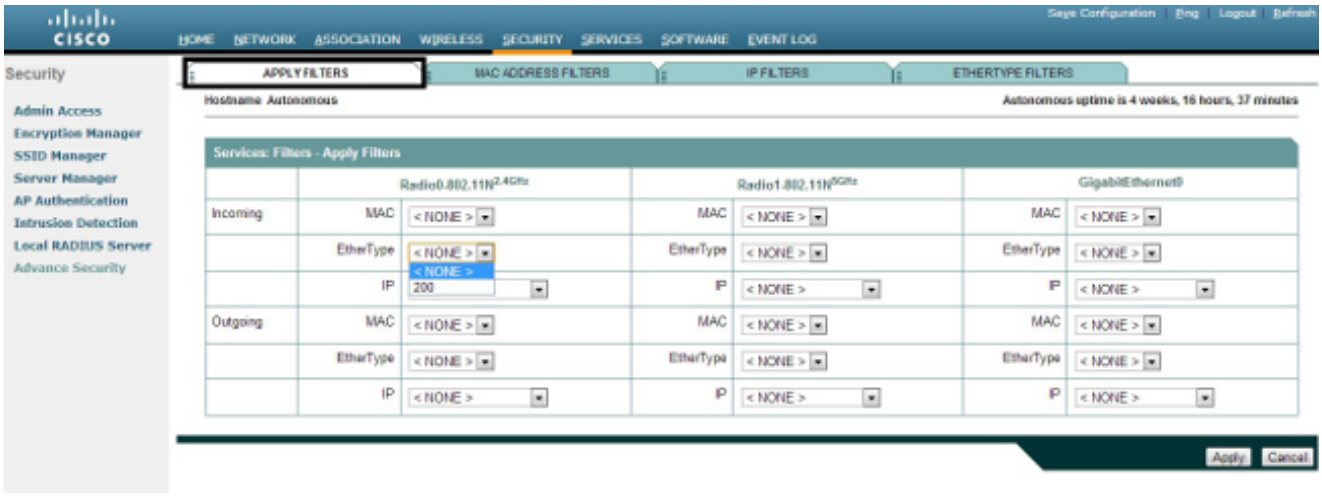
Cisco Aironet AP에서 IPX(Internetwork Packet Exchange) 트래픽을 차단하려면 이더 타입 필터를 사용할 수 있습니다. 이 방법이 유용한 일반적인 상황은 IPX 서버에서 브로드캐스트할 때 무선 링크가 혼잡해지는 경우입니다. 이는 대기업 네트워크에서 종종 발생합니다.

IPX 트래픽을 차단하는 필터를 구성하고 적용하려면 다음 단계를 완료하십시오.

1. Ethertype Filters(이더 타입 필터) 탭을 클릭합니다.
2. Filter Index 필드에서 필터의 이름을 200~299의 숫자로 지정합니다. 지정하는 번호로 필터에 대한 ACL이 생성됩니다.
3. Add Ethertype(이더 타입 추가) 필드에 8137을 입력합니다.
4. 이더 타입의 마스크는 Mask 필드에 기본값으로 둡니다.
5. 작업 메뉴에서 Block을 선택하고 Add를 클릭합니다.



6. Filters Classes 목록에서 이더 타입을 제거하려면 이더 타입을 선택하고 Delete Class를 클릭합니다. 이전 단계를 반복하고 유형 8138, 00ff 및 00e0을 필터에 추가합니다. 이제 이 ACL을 수신 또는 발신 라디오 또는 GigabitEthernet 인터페이스에 적용할 수 있습니다.



이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.