# Wireless LAN Controller에서 ACL 구성 예

## 목차



## 소개

이 문서에서는 WLAN(Wireless LAN Controller)에서 ACL(Access Control List)을 구성하여 WLAN을 통해 트래픽을 필터링하는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 기본 작동을 위해 WLC 및 LAP(Lightweight Access Point)를 구성하는 방법
- LWAPP(Lightweight Access Point Protocol) 및 무선 보안 방법에 대한 기본 지식

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 펌웨어 4.0을 실행하는 Cisco 2000 Series WLC
- Cisco 1000 Series LAP
- 펌웨어 2.6을 실행하는 Cisco 802.11a/b/g 무선 클라이언트 어댑터
- Cisco Aironet Desktop Utility(ADU) 버전 2.6

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

### 표기 규칙

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

# WLC의 ACL

WLC의 ACL은 무선 클라이언트가 WLAN의 서비스에 액세스하도록 제한하거나 허용하는 것입니다 .

WLC 펌웨어 버전 4.0 이전에는 ACL이 관리 인터페이스에서 우회되므로 WLC로 향하는 트래픽에 영향을 줄 수 없습니다. 무선 클라이언트를 통해 관리 옵션을 사용하여 컨트롤러를 관리하는 것만 방지할 수 있습니다. 따라서 ACL은 동적 인터페이스에만 적용할 수 있습니다. WLC 펌웨어 버전 4.0에는 관리 인터페이스로 향하는 트래픽을 필터링할 수 있는 CPU ACL이 있습니다. 자세한 내용은 CPU ACL 구성 섹션을 참조하십시오.

최대 64개의 ACL을 정의할 수 있으며, 각 ACL에는 최대 64개의 규칙(또는 필터)이 있습니다. 각 규칙에는 작업에 영향을 주는 매개변수가 있습니다. 패킷이 규칙에 대한 모든 매개변수와 일치하면 해당 규칙에 대한 작업 집합이 패킷에 적용됩니다. GUI 또는 CLI를 통해 ACL을 구성할 수 있습니다 .

다음은 WLC에서 ACL을 구성하기 전에 알아야 할 몇 가지 규칙입니다.

- sourceanddestination이 any**이면** 이 ACL이 적용되는 방향은 any가 될 수 **있습니다**.
- sourceordestination 중 하나가 **없으면 필터**의 방향을 지정하고 반대 방향의 역문을 만들어야 합니다.
- 인바운드와 아웃바운드의 WLC 개념은 직관적이지 않습니다. 이는 클라이언트의 관점이 아니라 무선 클라이언트를 향하는 WLC의 관점에서입니다. 따라서 인바운드 방향은 무선 클라이언트에서 WLC로 들어오는 패킷을 의미하고 아웃바운드 방향은 WLC에서 무선 클라이언트로 나가는 패킷을 의미합니다.
- ACL의 끝에 암시적 거부가 있습니다.

# WLC에서 ACL을 구성할 때 고려할 사항

WLC의 ALC는 라우터와 다르게 작동합니다. WLC에서 ACL을 구성할 때 기억해야 할 몇 가지 사항은 다음과 같습니다.

- 가장 일반적인 실수는 IP 패킷을 거부하거나 허용하려는 경우 IP를 선택하는 것입니다. IP 패킷 내의 내용을 선택하므로 IP-in-IP 패킷을 거부하거나 허용합니다.
- 컨트롤러 ACL은 WLC 가상 IP 주소를 차단할 수 없으므로 무선 클라이언트에 대한 DHCP 패킷을 차단합니다.
- 컨트롤러 ACL은 무선 클라이언트로 향하는 유선 네트워크에서 수신된 멀티캐스트 트래픽을 차단할 수 없습니다. 컨트롤러 ACL은 무선 클라이언트에서 시작하여 유선 네트워크 또는 동일한 컨트롤러의 다른 무선 클라이언트로 향하는 멀티캐스트 트래픽에 대해 처리됩니다.
- ACL은 라우터와 달리 인터페이스에 적용될 때 양방향으로 트래픽을 제어하지만 스테이트풀 방화벽을 수행하지 않습니다. 반환 트래픽을 위해 ACL에 구멍을 여는 것을 잊은 경우 문제가 발생합니다.
- 컨트롤러 ACL은 IP 패킷만 차단합니다. IP가 아닌 레이어 2 ACL 또는 레이어 3 패킷은 차단할 수 없습니다.
- 컨트롤러 ACL은 라우터처럼 역 마스크를 사용하지 않습니다. 여기서, 255는 IP 주소의 옥텟을 정확히 매칭함을 의미한다.

- 컨트롤러의 ACL은 소프트웨어에서 수행되며 포워딩 성능에 영향을 미칩니다.

  **참고**: ACL을 인터페이스 또는 WLAN에 적용하면 무선 처리량이 저하되고 패킷이 손실될 수 있습니다. 처리량을 개선하기 위해 인터페이스 또는 WLAN에서 ACL을 제거하고 ACL을 인접한 유선 디바이스로 이동합니다.

# WLC에 ACL 구성

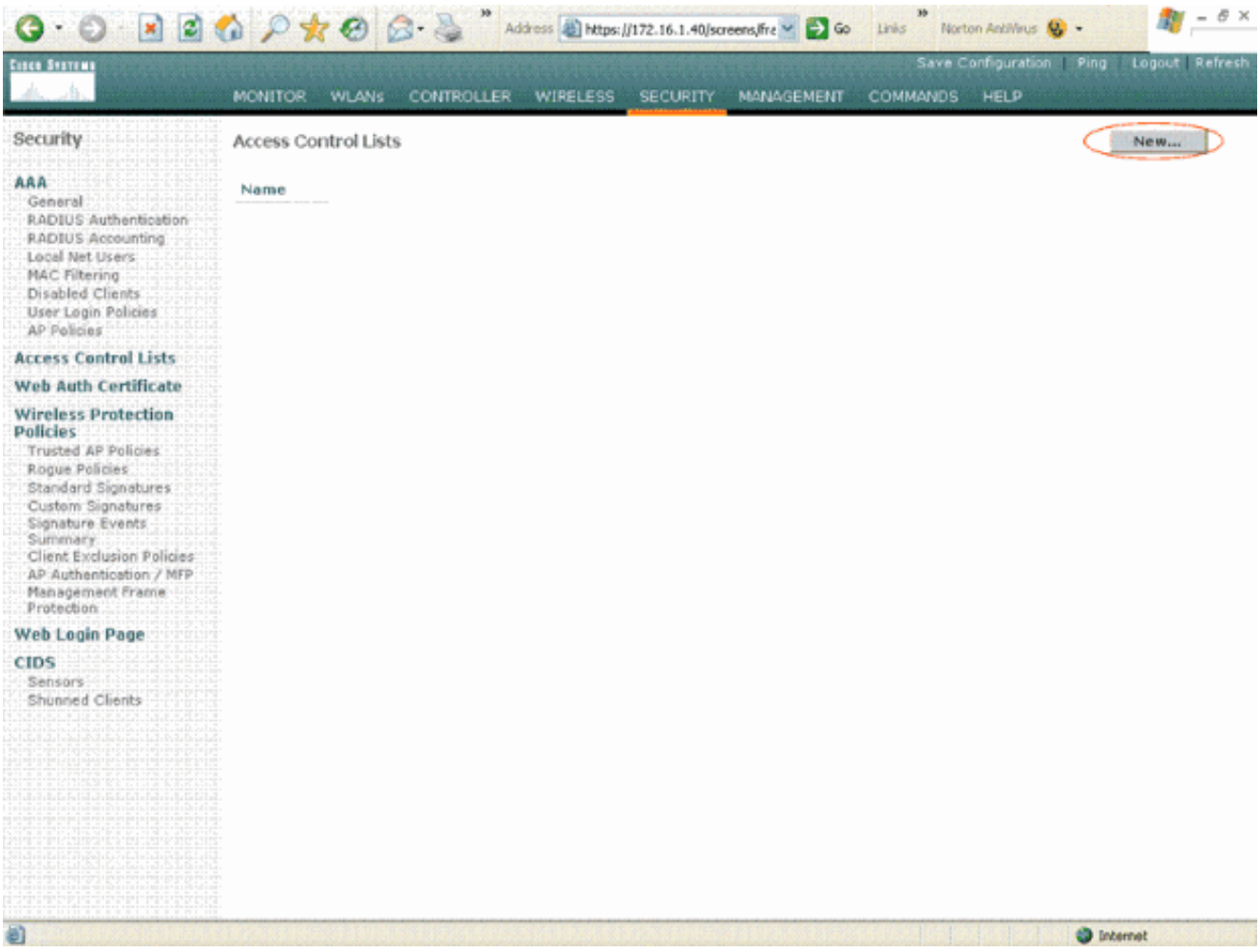
이 섹션에서는 WLC에서 ACL을 구성하는 방법에 대해 설명합니다. 게스트 클라이언트가 다음 서비스에 액세스할 수 있도록 ACL을 구성하는 것이 목적입니다.

- 무선 클라이언트와 DHCP 서버 간의 DHCP(Dynamic Host Configuration Protocol)
- 네트워크의 모든 디바이스 간 ICMP(Internet Control Message Protocol)
- 무선 클라이언트와 DNS 서버 간의 DNS(Domain Name System)
- 특정 서브넷에 대한 텔넷

다른 모든 서비스는 무선 클라이언트에 대해 차단되어야 합니다. WLC GUI를 사용하여 ACL을 생성하려면 다음 단계를 완료합니다.

1. WLC GUI로 이동하고 **Security(보안) > Access Control Lists(액세스 제어 목록)를** 선택합니다 .Access Control Lists 페이지가 나타납니다. 이 페이지에는 WLC에 구성된 ACL이 나열됩니다 . 또한 ACL을 수정하거나 제거할 수 있습니다. 새 ACL을 생성하려면 New(새로 만들기)를 **클릭합니다**

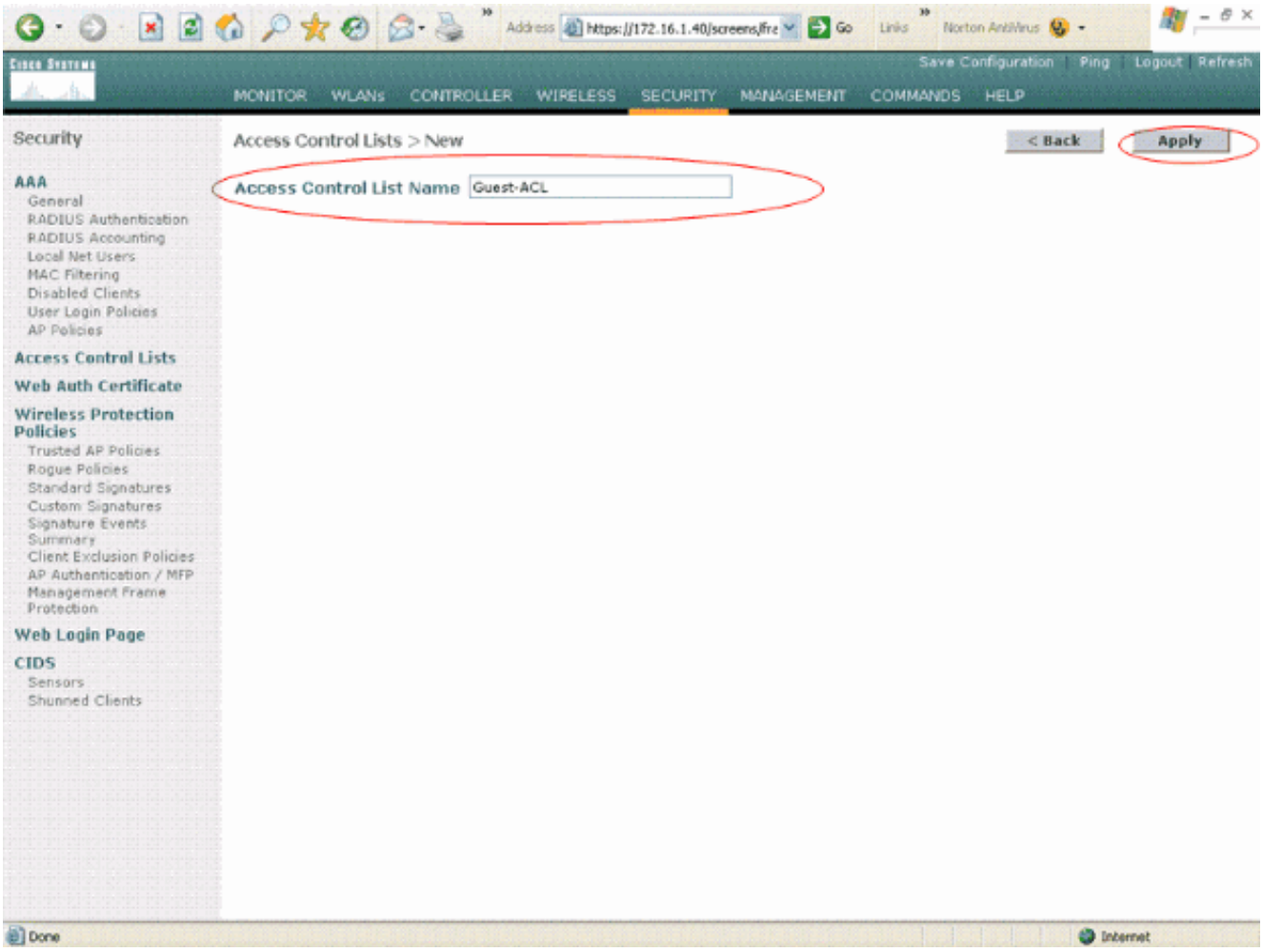
   .




*액세스 제어 목록*

2. ACL의 이름을 입력하고 Apply를 **클릭합니다**.최대 32자의 영숫자를 입력할 수 있습니다. 이 예에서 ACL의 이름은 **Guest-ACL입니다**. ACL이 생성되면 Edit를 클릭하여 **ACL**에 대한 규칙을 생성합니다

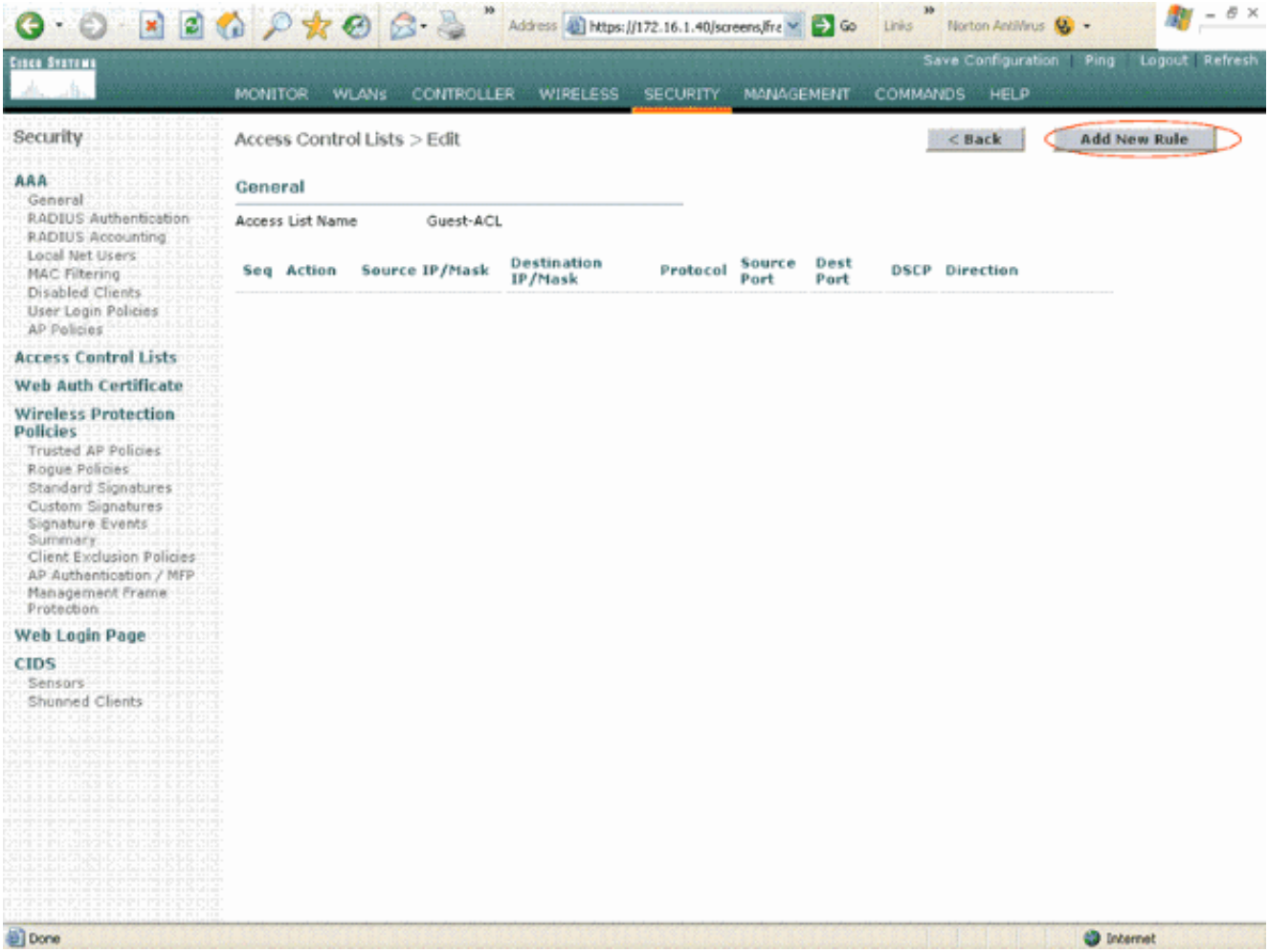
.




*ACL의 이름 입력*

3. Access Control Lists(액세스 제어 목록) > Edit(수정) 페이지가 나타나면 Add **New Rule(새 규칙 추가)을** 클릭합니다.Access Control Lists > Rules > New 페이지가 나타납니다

.




*새 ACL 규칙 추가*

4. 게스트 사용자에게 다음 서비스를 허용하는 규칙을 구성합니다.무선 클라이언트와 DHCP 서버 간의 DHCP네트워크의 모든 디바이스 간 ICMP무선 클라이언트와 DNS 서버 간의 DNS특정 서브넷에 대한 텔넷

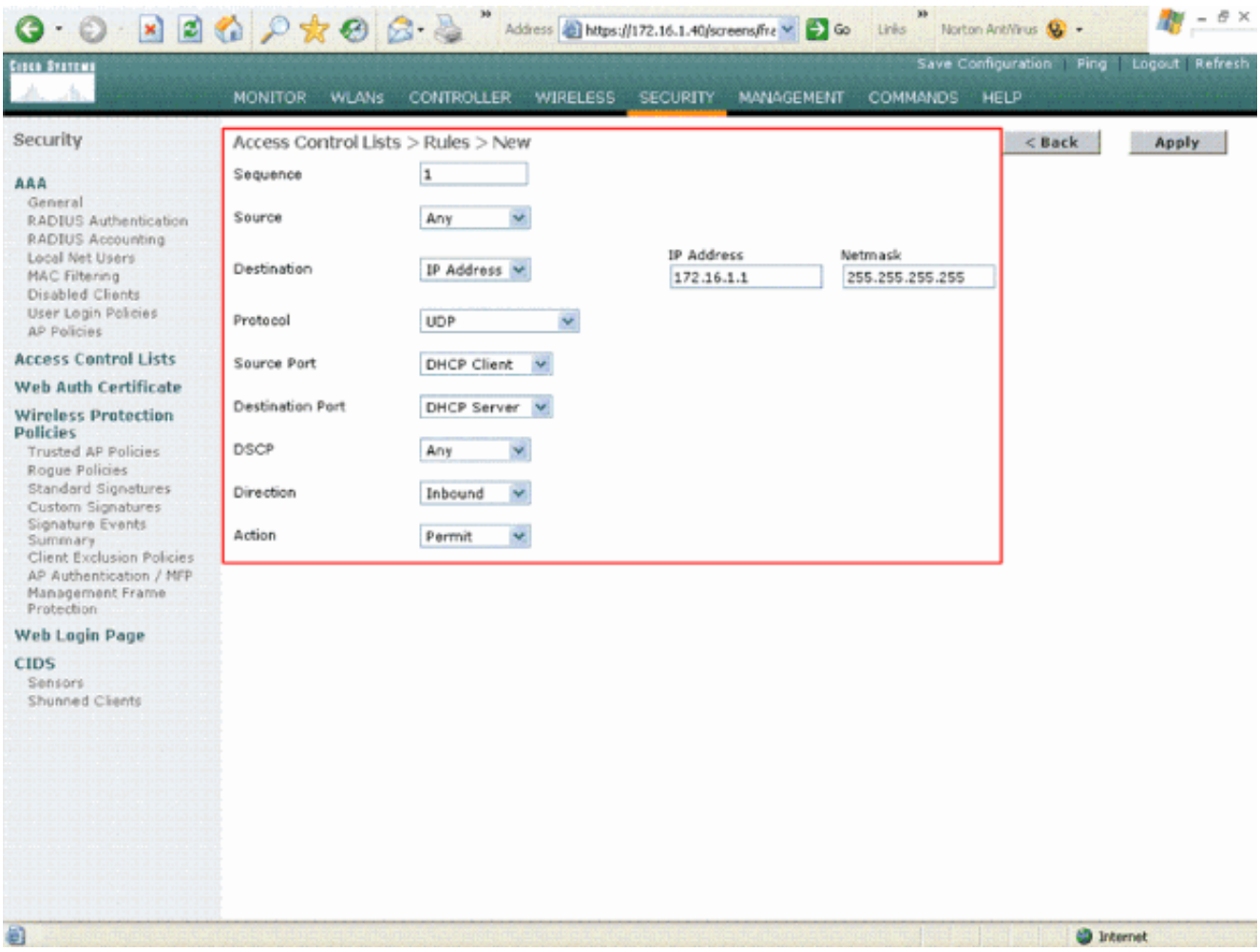
## 게스트 사용자 서비스를 허용하는 규칙 구성

이 섹션에서는 이러한 서비스에 대한 규칙을 구성하는 방법에 대한 예를 보여줍니다.

- 무선 클라이언트와 DHCP 서버 간의 DHCP
- 네트워크의 모든 디바이스 간 ICMP
- 무선 클라이언트와 DNS 서버 간의 DNS
- 특정 서브넷에 대한 텔넷

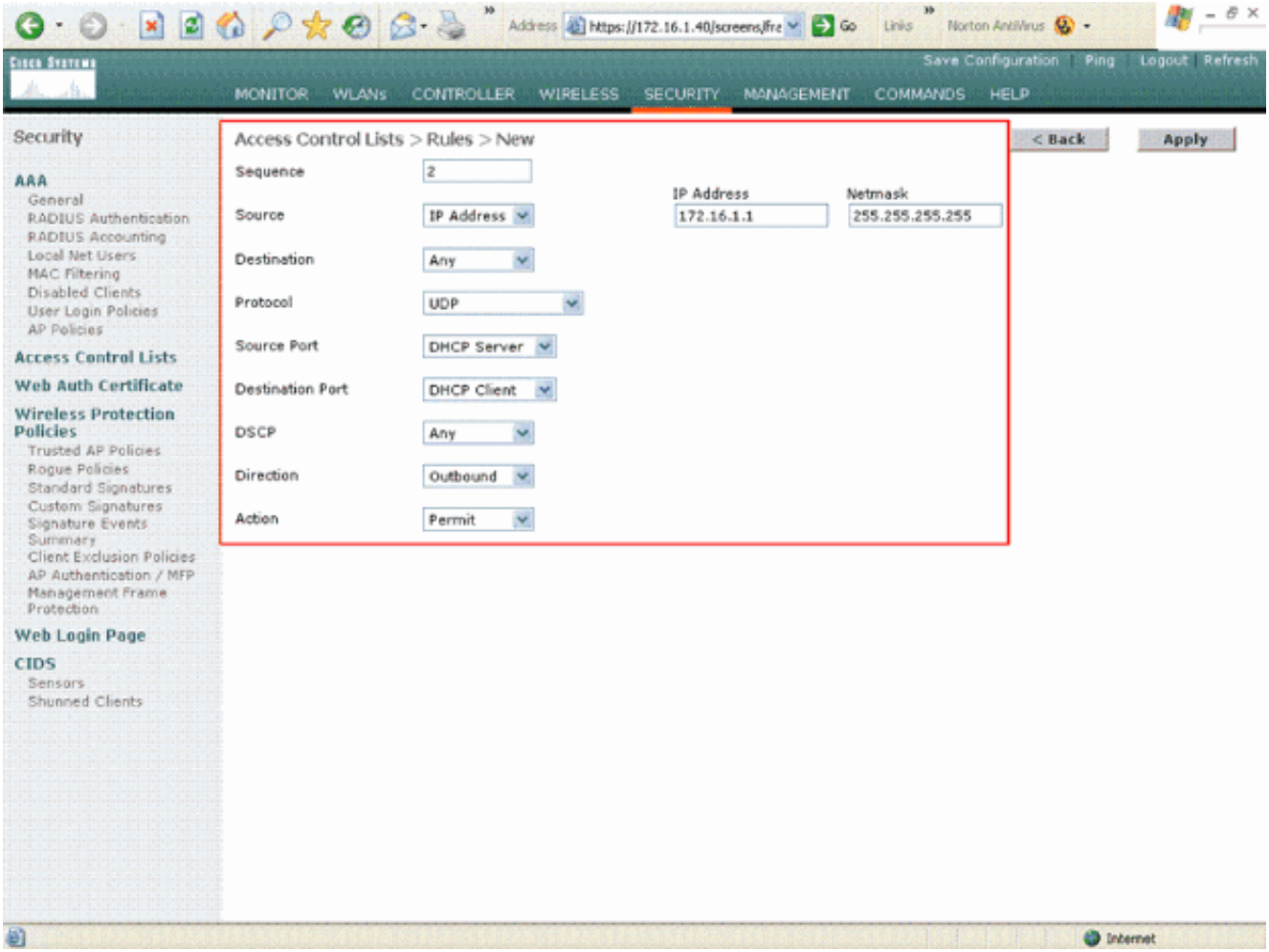
1. DHCP 서비스에 대한 규칙을 정의하려면 소스 및 대상 IP 범위를 선택합니다.이 예에서는 소스에 any를 사용하므로 모든 무선 클라이언트가 DHCP 서버에 액세스할 수 있습니다. 이 예에서 서버 172.16.1.1은 DHCP 및 DNS 서버 역할을 합니다. 따라서 대상 IP 주소는 172.16.1.1/255.255.255.255(호스트 마스크 사용)입니다.DHCP는 UDP 기반 프로토콜이므로 Protocol 드롭다운 **필드**에서 UDP를 선택합니다. 이전 단계에서 TCP 또는 UDP를 선택한 경우 Source Port(소스 포트)와 Destination Port(대상 포트)라는 두 가지 추가 매개변수가 표시됩니다. Source 및 Destination 포트 세부 정보를 지정합니다. 이 규칙의 소스 포트는 DHCP **클라이언트이고 대상** 포트는 DHCP **서버입니다**.ACL을 적용할 방향을 선택합니다. 이 규칙은 클라이언트에서 서버로 전송되므로 이 예에서는 Inbound를 **사용합니다**. Action(작업) 드롭다운 상자에서 Permit(허용)을 선택하여 이 ACL이 무선 클라이언트에서 DHCP 서버로의 DHCP 패킷을 허용하도록 합니다. 기본값은 Deny입니다. Apply를 **클릭합니다**

.




*ACL에서 DHCP 패킷을 허용하도록 허용을 선택합니다* 소스 또는 대상 중 하나가 **없으면** 반대 방향의 역문을 생성해야 합니다. 이제 DDoS 공격의 실제 사례를 살펴보겠습니다

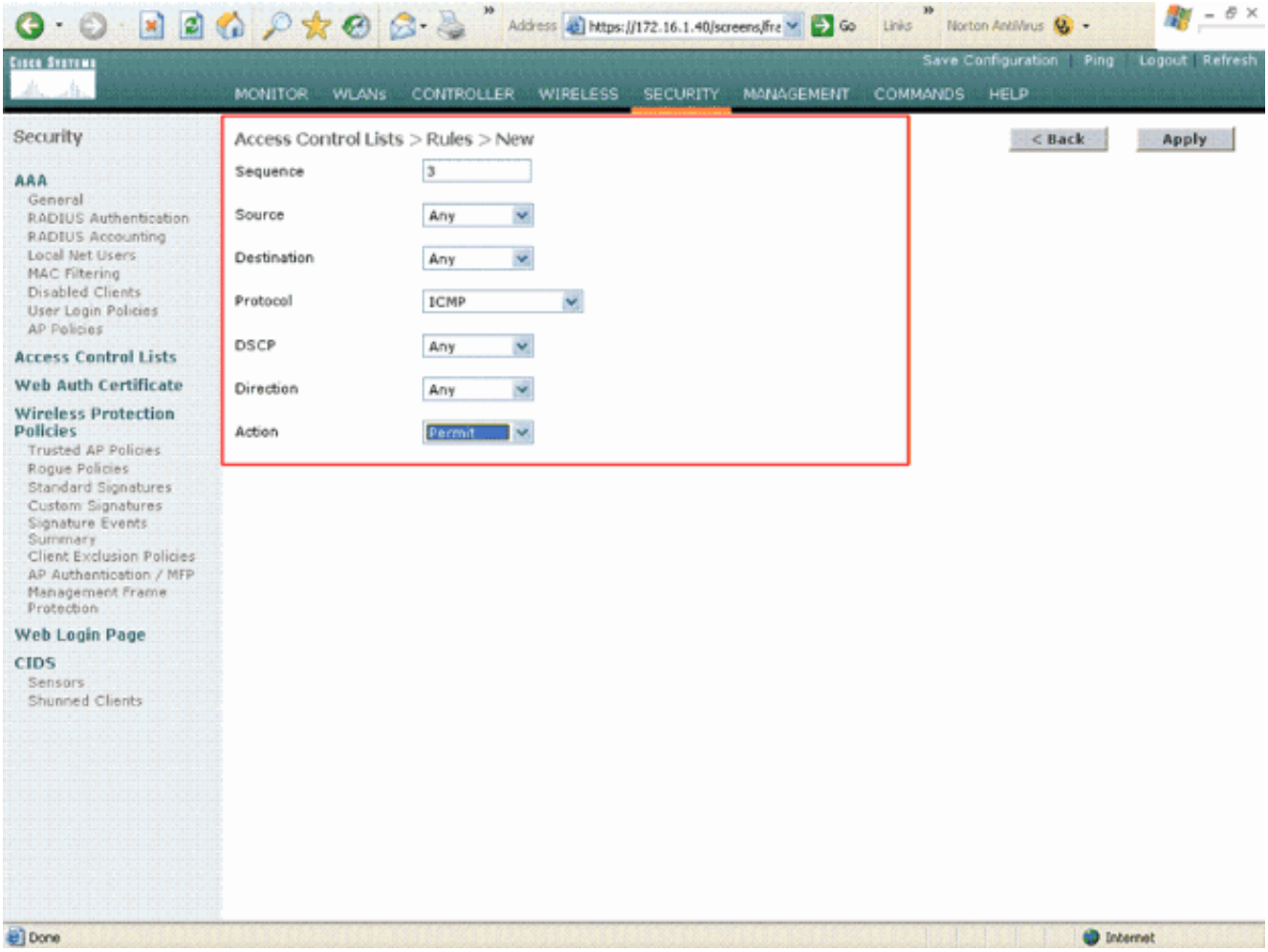
.




*Source 또는 Destination이 Any로 설정됨*

2. 모든 디바이스 간에 ICMP 패킷을 허용하는 규칙을 정의하려면 Source 및 Destination 필드에 대해 **any**를 선택합니다. 이것이 기본값입니다.Protocol 드롭다운 필드에서 **ICMP**를 선택합니다. 이 예에서는 Source 및 Destination 필드에 **any**를 사용하므로 방향을 지정할 필요가 없습니다. 기본값 any로 그대로 둘 수 **있습니다**. 또한 반대 방향의 역문이 필요하지 않다.이 ACL이 DHCP 서버에서 무선 **클라이언트**로 DHCP 패킷을 허용하도록 하려면 Action(작업) 드롭다운 메뉴에서 Permit(허용)을 선택합니다. Apply를 **클릭합니다**

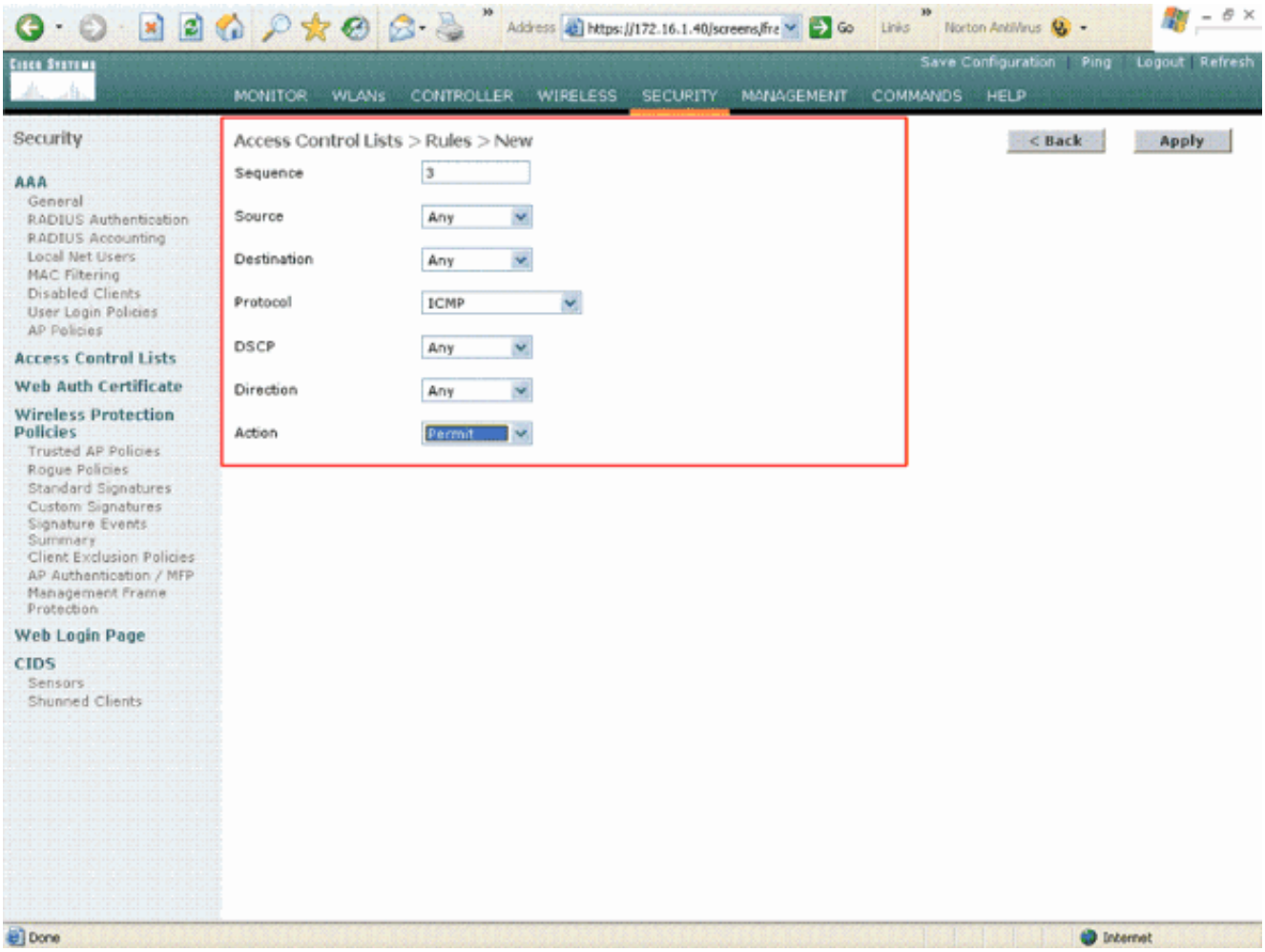
.



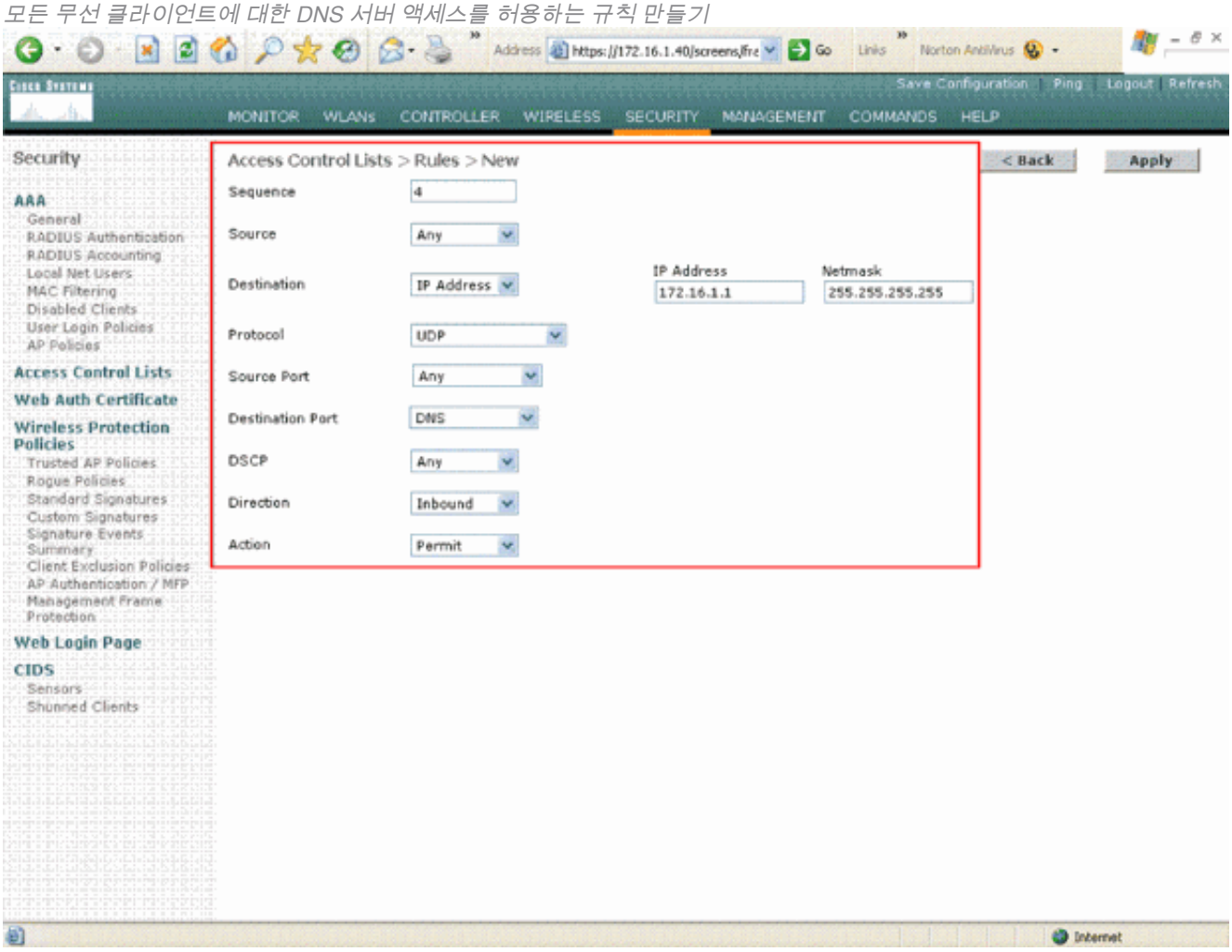

*ACL이 DHCP 서버에서 무선 클라이언트로의 DHCP 패킷을 허용하도록 허용*

3. 마찬가지로, 모든 무선 클라이언트에 대한 DNS 서버 액세스와 특정 서브넷에 대한 무선 클라이언트에 대한 텔넷 서버 액세스를 허용하는 규칙을 만듭니다. 다음은 그 예입니다

.

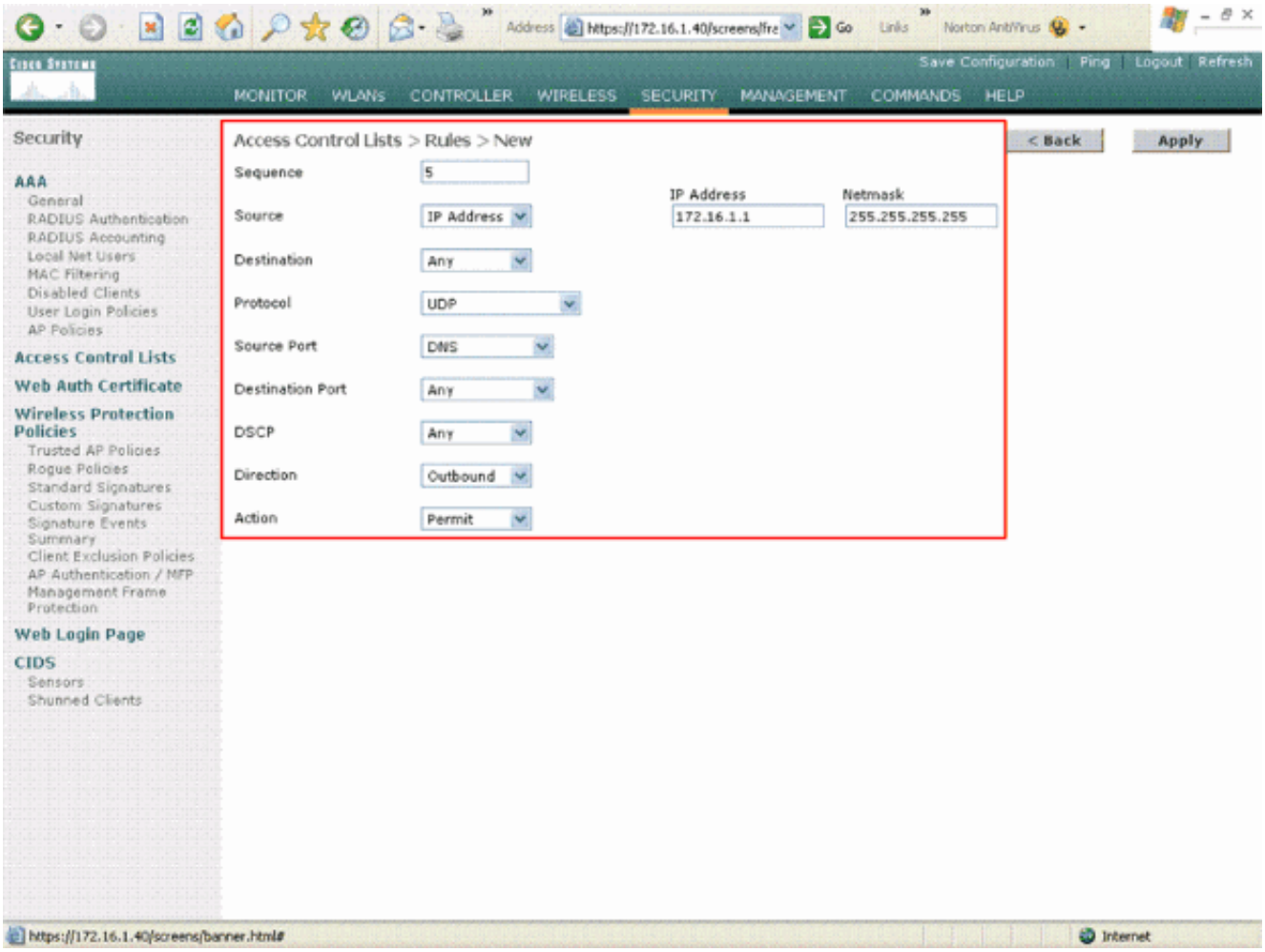



*모든 무선 클라이언트에 대한 DNS 서버 액세스를 허용하는 규칙 만들기*

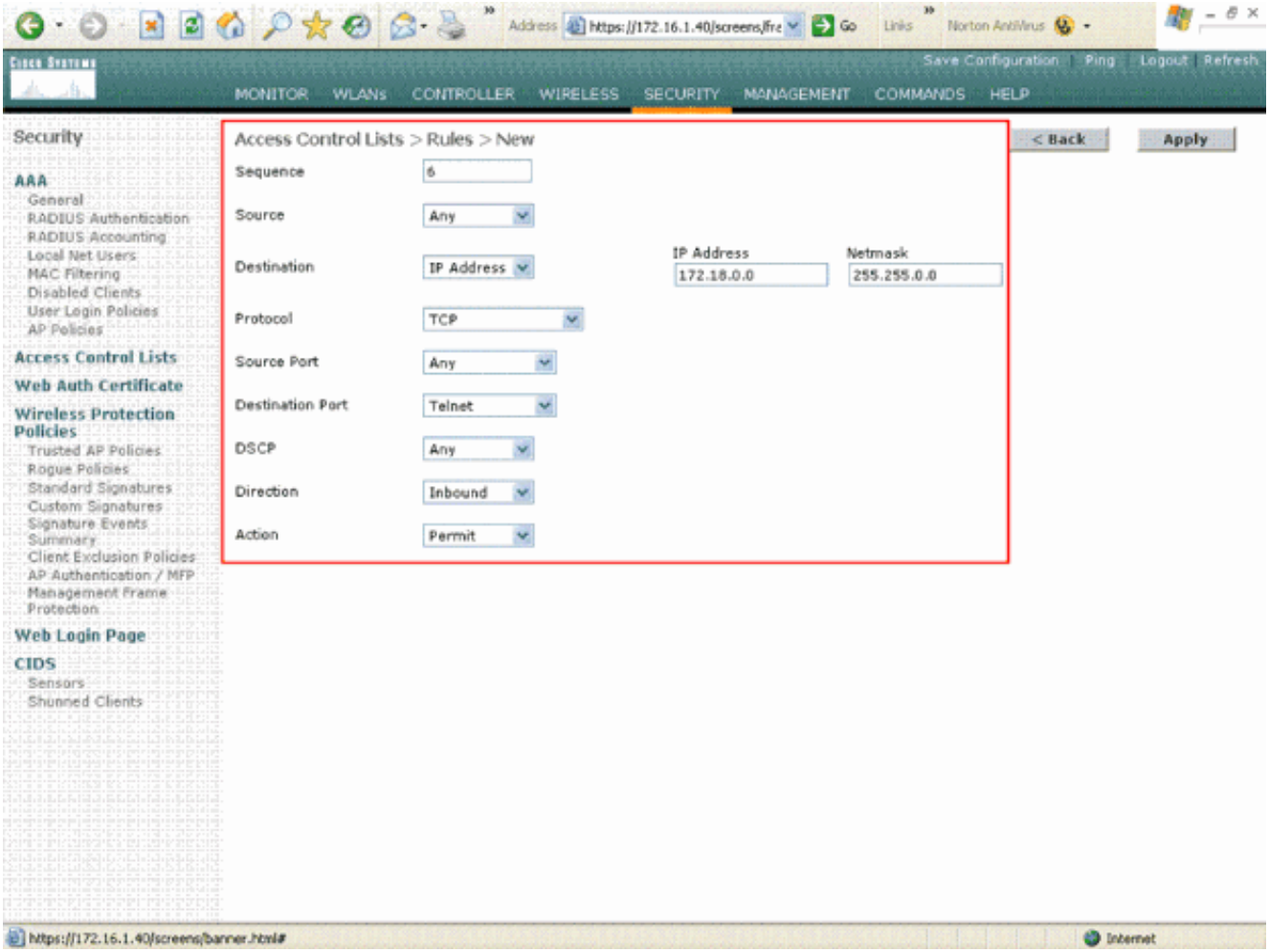


*서브넷에 대한 무선 클라이언트의 텔넷 서버 액세스를 허용하는 규칙 만들기* 무선 클라이언트가 텔넷 서비스에 액세스할 수 있도록 하려면 이 규칙을 정의합니다

.

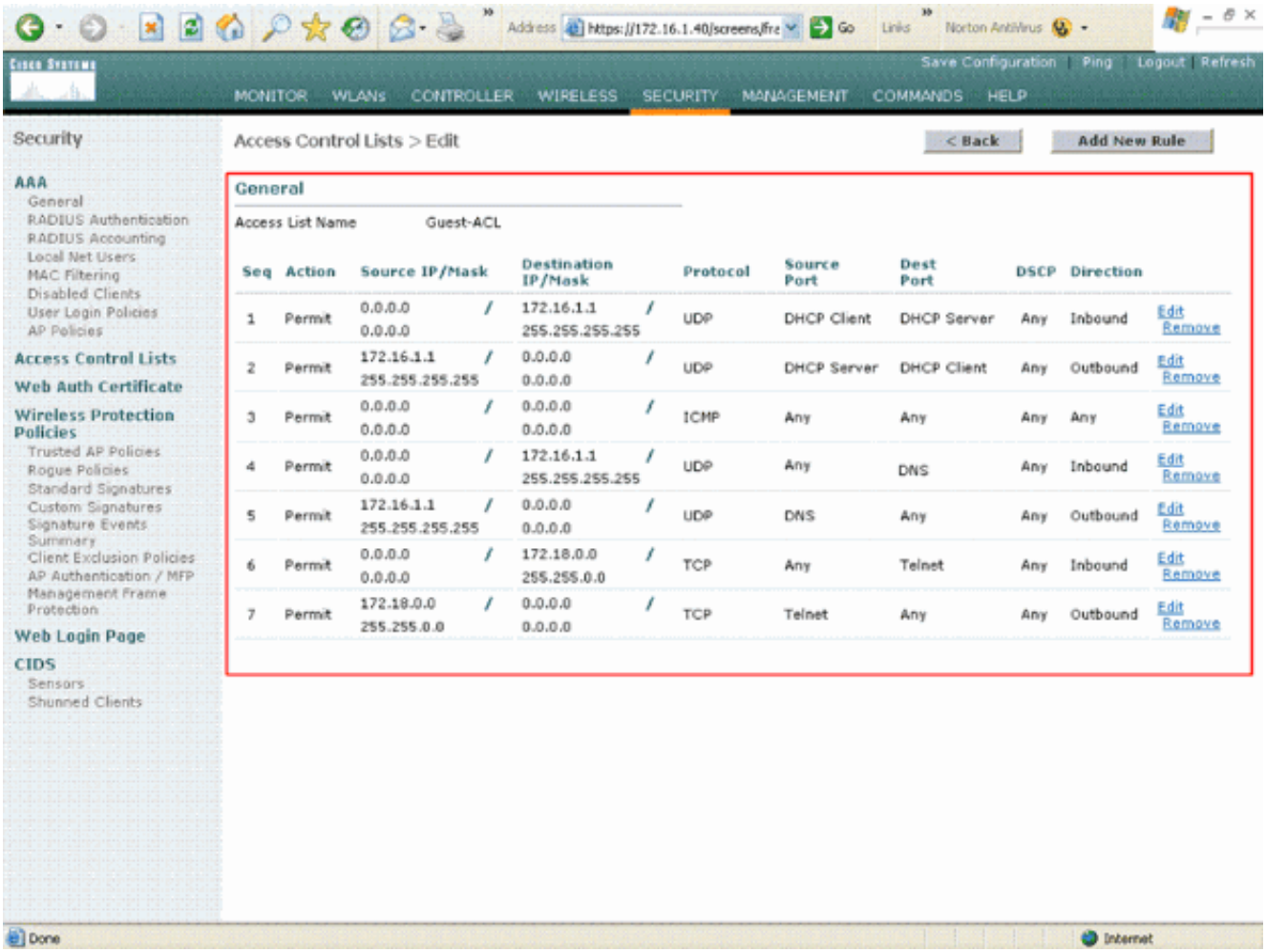



*텔넷 서비스에 대한 무선 클라이언트 액세스 허용*




*텔넷 서비스에 대한 무선 클라이언트 액세스의 또 다른 예* ACL **> Edit 페이지**는 ACL에 대해 정의된 모든 규칙을 나열합니다

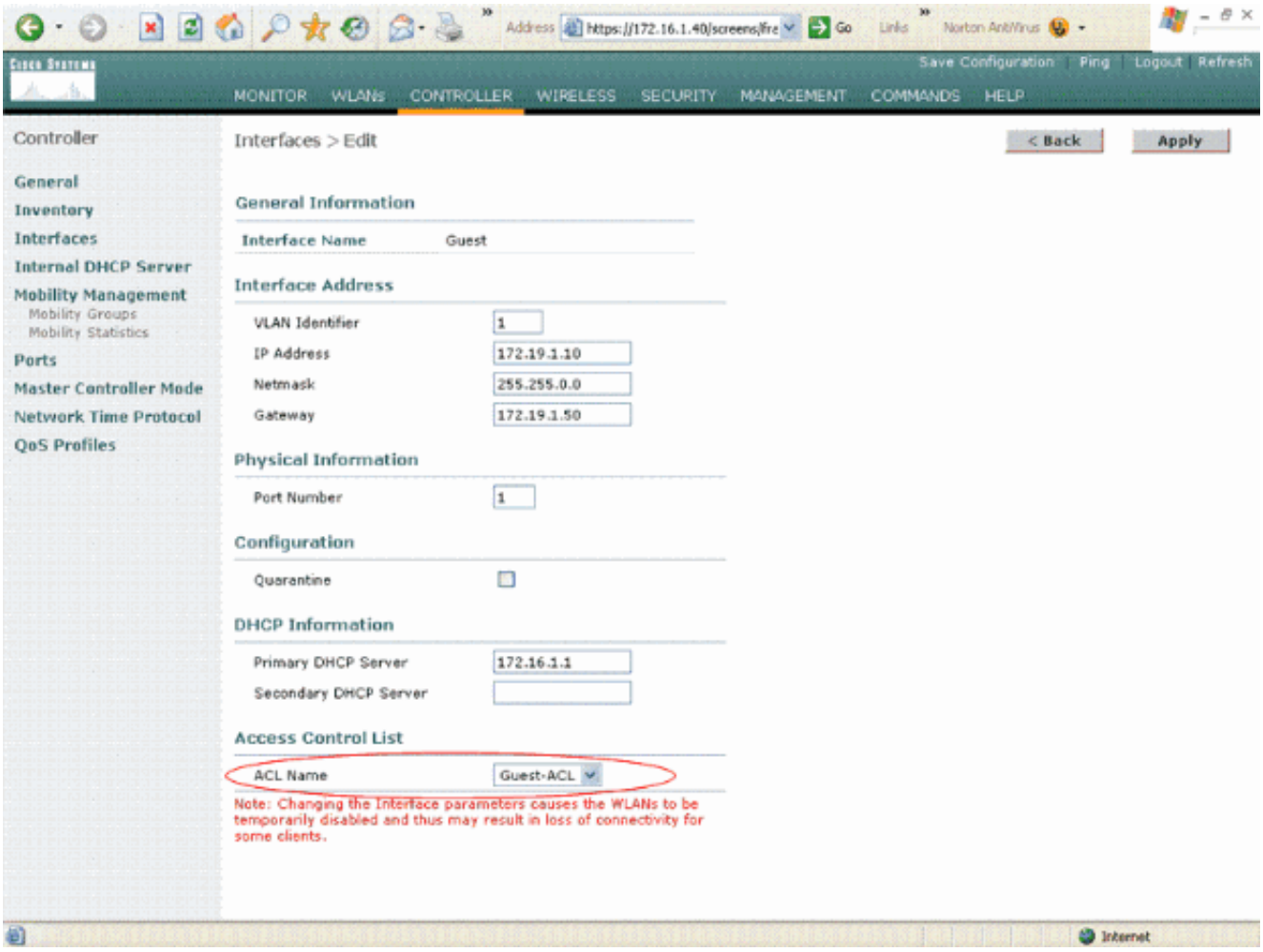
.




*Edit(수정) 페이지에는 ACL에 대해 정의된 모든 규칙이 나열됩니다.*

4. ACL이 생성되면 동적 인터페이스에 적용해야 합니다. ACL을 적용하려면 **Controller(컨트롤러) > Interfaces(인터페이스)**를 선택하고 ACL을 적용할 인터페이스를 수정합니다.
5. 동적 인터페이스에 대한 **Interfaces > Edit** 페이지의 Access Control Lists 드롭다운 메뉴에서 적절한 ACL을 선택합니다. 이제 DDoS 공격의 실제 사례를 살펴보겠습니다

.




*Access Control List 메뉴에서 적절한 ACL을 선택합니다*

이 작업이 완료되면 ACL은 이 동적 인터페이스를 사용하는 WLAN에서 (구성된 규칙에 따라) 트래픽을 허용하고 거부합니다. 인터페이스 ACL은 연결 모드의 H-Reap AP에만 적용할 수 있지만 독립형 모드에는 적용할 수 없습니다.

> **참고**: 이 문서에서는 WLAN 및 동적 인터페이스가 구성되었다고 가정합니다. 무선 LAN 컨트롤러에 VLAN 구성 또는 WLC에 동적 인터페이스를 생성하는 방법에 대한 정보를 참조하십시오.

## CPU ACL 구성

이전에는 WLC의 ACL에 LWAPP/CAPWAP 데이터 트래픽, LWAPP/CAPWAP 제어 트래픽, 관리 및 AP 관리자 인터페이스로 이동하는 모빌리티 트래픽을 필터링할 수 있는 옵션이 없었습니다. 이 문제를 해결하고 LWAPP 및 모빌리티 트래픽을 필터링하기 위해 WLC 펌웨어 릴리스 4.0에 CPU ACL을 도입했습니다.

CPU ACL의 컨피그레이션에는 두 단계가 포함됩니다.

1. CPU ACL에 대한 규칙을 구성합니다.
2. WLC에 CPU ACL을 적용합니다.

CPU ACL에 대한 규칙은 다른 ACL과 유사한 방식으로 구성해야 합니다.

# 다음을 확인합니다.

ACL 컨피그레이션을 올바르게 구성했는지 확인하기 위해 무선 클라이언트로 ACL 컨피그레이션을 테스트하는 것이 좋습니다. 올바르게 작동하지 않을 경우 ACL 웹 페이지에서 ACL을 확인하고 ACL 변경 사항이 컨트롤러 인터페이스에 적용되었는지 확인합니다.

또한 다음 show 명령을 사용하여 컨피그레이션을 확인할 수 있습니다.

- **show acl summary** - 컨트롤러에 구성된 ACL을 표시하려면 show acl summary **명령을** 사용합니다.예를 들면 다음과 같습니다.

```
(Cisco Controller) >show acl summary

ACL Name                         Applied
-------------------------------- -------
Guest-ACL                        Yes
```

- **show acl detailedACL_Name** - 구성된 ACL에 대한 자세한 정보를 표시합니다.예를 들면 다음과 같습니다.

```
(Cisco Controller) >show acl detailed Guest-ACL

                  Source                        Destination               Source Port
Dest Port
I  Dir       IP Address/Netmask             IP Address/Netmask        Prot    Range
Range    DSCP Action
-- --- ------------------------------ ------------------------------ ---- ----------- ----
------- ---- ------
 1  In         0.0.0.0/0.0.0.0             172.16.1.1/255.255.255.255   17    68-68
67-67     Any Permit
 2 Out      172.16.1.1/255.255.255.255         0.0.0.0/0.0.0.0           17    67-67
68-68     Any Permit
 3 Any         0.0.0.0/0.0.0.0                 0.0.0.0/0.0.0.0            1     0-65535
0-65535  Any Permit
 4  In         0.0.0.0/0.0.0.0             172.16.1.1/255.255.255.255   17     0-65535
53-53     Any Permit
 5 Out      172.16.1.1/255.255.255.255         0.0.0.0/0.0.0.0           17    53-53
0-65535  Any Permit
 6  In         0.0.0.0/0.0.0.0             172.18.0.0/255.255.0.0             60-65535
23-23     Any Permit
 7 Out      172.18.0.0/255.255.0.0             0.0.0.0/0.0.0.0            6    23-23
0-65535  Any Permit
```

- **show acl cpu** - CPU에 구성된 ACL을 표시하려면 show acl **cpu 명령을** 사용합니다.예를 들면 다음과 같습니다.

```
(Cisco Controller) >show acl cpu

CPU Acl Name.............................. CPU-ACL
Wireless Traffic.......................... Enabled
Wired Traffic............................. Enabled
```

# 문제 해결

컨트롤러 소프트웨어 릴리스 4.2.x 이상에서는 ACL 카운터를 구성할 수 있습니다. ACL 카운터는 컨트롤러를 통해 전송된 패킷에 어떤 ACL이 적용되었는지 확인하는 데 도움이 될 수 있습니다. 이 기능은 시스템 문제를 해결할 때 유용합니다.

ACL 카운터는 다음 컨트롤러에서 사용할 수 있습니다.

- 4400 시리즈
- Cisco WiSM

- Catalyst 3750G Integrated Wireless LAN Controller Switch

이 기능을 사용하려면 다음 단계를 완료하십시오.

1. Security(**보안) > Access Control Lists(액세스 제어 목록) > Access Control Lists(액세스 제어 목록)**를 선택하여 Access Control Lists(액세스 제어 목록) 페이지를 엽니다.이 페이지에는 이 컨트롤러에 대해 구성된 모든 ACL이 나열됩니다.
2. 패킷이 컨트롤러에 구성된 ACL에 도달했는지 확인하려면 Enable Counters(카운터 활성화) **확인란**을 선택하고 Apply(적용)를 **클릭합니다**. 그렇지 않으면 확인란을 선택하지 않은 상태로 둡니다. 이것이 기본값입니다.
3. ACL에 대한 카운터를 지우려면 해당 ACL에 대한 파란색 드롭다운 화살표 위로 커서를 이동하고 **Clear Counters(카운터 지우기)**를 선택합니다.

## 관련 정보

- Cisco Wireless LAN Controller 컨피그레이션 가이드, 릴리스 6.0
- 무선 LAN 컨트롤러에서 VLAN 구성
- WLC 연결에 실패한 경량 AP 문제 해결
- Cisco 기술 지원 및 다운로드

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.