WLC의 ACL - 규칙, 제한 및 예

목차

소개

이 문서에서는 WLC(무선 LAN 컨트롤러)의 ACL(액세스 제어 목록)에 대한 정보를 제공합니다. 이 문서에서는 현재의 제한 및 규칙에 대해 설명하고 관련 예를 제공합니다. 이 문서는 무선 LAN 컨트롤러 컨피그레이션 예의 ACL을 대체하는 것이 아니라 추가 정보를 제공하기 위한 것입니다.

참고: 레이어 2 ACL 또는 레이어 3 ACL 규칙의 추가적인 유연성을 위해 컨트롤러에 연결된 첫 번째 홉 라우터에 ACL을 구성하는 것이 좋습니다.

가장 일반적인 실수는 프로토콜 필드가 IP 패킷을 허용하거나 거부할 목적으로 ACL 라인에서 IP(protocol=4)로 설정된 경우 발생합니다. 이 필드는 TCP, UDP(User Datagram Protocol), ICMP(Internet Control Message Protocol) 등 IP 패킷 내부에서 캡슐화된 항목을 실제로 선택하므로 IP-in-IP 패킷을 차단하거나 허용하는 것으로 해석됩니다. 모바일 IP 패킷을 차단하려는 경우가 아니면 ACL 행에서 IP를 선택하지 않아야 합니다. Cisco 버그 ID CSCsh22975(등록된 고객만 해당)는 IP를 IP-in-IP로 변경합니다.

사전 요구 사항

요구 사항

이 컨피그레이션을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

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

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

표기 규칙

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

WLC의 ACL 이해

ACL은 하나 이상의 ACL 행으로 구성되며 그 뒤에 ACL의 끝에 암시적 "deny any any"가 옵니다. 각 라인에는 다음 필드가 있습니다.

- 시퀀스 번호
- 방향
- 소스 IP 주소 및 마스크
- 대상 IP 주소 및 마스크
- 프로토콜
- 소스 포트
- 대상 포트
- DSCP
- 작업

이 문서에서는 다음 각 필드에 대해 설명합니다.

- **Sequence Number**(시퀀스 번호) - 패킷에 대해 ACL 라인이 처리되는 순서를 나타냅니다. 패킷은 첫 번째 ACL 라인과 일치할 때까지 ACL에 대해 처리됩니다. 또한 ACL이 생성된 후에도 ACL의 아무 곳에나 ACL 행을 삽입할 수 있습니다. 예를 들어, 시퀀스 번호가 1인 ACL 라인이 있는 경우 새 ACL 라인에 시퀀스 번호 1을 입력하여 앞에 새 ACL 라인을 삽입할 수 있습니다. 이렇게 하면 ACL에서 현재 행이 자동으로 아래로 이동합니다.
- **Direction**(방향) - ACL 라인을 적용할 방향을 컨트롤러에 알립니다. Inbound(인바운드), Outbound(아웃바운드), Any(모두)의 3가지 방향이 있습니다. 이러한 방향은 무선 클라이언트가 아니라 WLC에 대한 위치에서 가져옵니다.Inbound(인바운드) - 무선 클라이언트에서 소싱된 IP 패킷이 ACL 라인과 일치하는지 검사합니다.Outbound(아웃바운드) - 무선 클라이언트로 향하는 IP 패킷이 ACL 라인과 일치하는지 검사합니다.Any(모두) - 무선 클라이언트에서 발생하며 무선 클라이언트로 전달되는 IP 패킷이 ACL 라인과 일치하는지 검사합니다. ACL 라인은 인바운드 및 아웃바운드 방향에 모두 적용됩니다.**참고:** 방향에 대해 Any를 선택할 때 사용해야 하는 주소와 마스크는 0.0.0.0/0.0.0.0(Any)뿐입니다. 반환 트래픽을 허용하기 위해 스왑된 주소 또는 서브넷과 함께 새 회선이 필요하므로 "Any" 방향으로 특정 호스트 또는 서브넷을 지정하면 안 됩니다.Any 방향은 무선 클라이언트(아웃바운드)로 이동하고 무선 클라이언트(인바운드)로부터 들어오는 특정 IP 프로토콜 또는 포트를 양방향으로 차단하거나 허용하려는 특정 상황에서만 사용해야 합니다.IP 주소 또는 서브넷을 지정할 때 방향을 Inbound(인바운드) 또는 Outbound(아웃바운드)로 지정하고 반대 방향의 반환 트래픽을 위해 두 번째 새 ACL 라인을 생성해야 합니다. ACL이 인터페이스에 적용되고 반환 트래픽이 다시 통과하도록 구체적으로 허용하지 않는 경우 반환 트래픽은 ACL 목록 끝에 있는 암시적 "deny any"(모두 거부)에 의해 거부됩니다.
- **Source IP Address and Mask**(소스 IP 주소 및 마스크) - 마스크에 따라 달라지는 단일 호스트에서 여러 서브넷으로의 소스 IP 주소를 정의합니다. 마스크는 IP 주소와 함께 사용되어 IP 주소

를 패킷의 IP 주소와 비교할 때 무시해야 하는 IP 주소의 비트를 결정합니다.**참고:** WLC ACL의 마스크는 Cisco IOS® ACL에 사용되는 와일드카드 또는 반전 마스크와 다릅니다. 컨트롤러 ACL에서 255는 IP 주소의 옥텟과 정확히 일치함을 의미하며 0은 와일드카드입니다. 주소와 마스크는 비트 단위로 결합됩니다.마스크 비트 1은 해당 비트 값을 확인하는 것을 의미한다. 마스크의 사양 255는 검사되는 패킷의 IP 주소의 옥텟이 ACL 주소의 해당 옥텟과 정확히 일치해야 함을 나타냅니다.마스크 비트 0은 해당 비트 값을 확인(무시)하지 않음을 의미한다. 마스크에서 0의 사양은 검사되는 패킷의 IP 주소의 옥텟이 무시됨을 나타냅니다.0.0.0.0/0.0.0.0은 "Any" IP 주소(주소로 0.0.0.0, 마스크로 0.0.0)에 해당합니다.

- **Destination IP Address and Mask(대상 IP** 주소 및 마스크) - 소스 IP 주소 및 마스크와 동일한 마스크 규칙을 따릅니다.
- **Protocol**(프로토콜) - IP 패킷 헤더의 프로토콜 필드를 지정합니다. 일부 프로토콜 번호는 고객의 편의를 위해 변환되며 풀다운 메뉴에서 정의됩니다. 다른 값은 다음과 같습니다.모두(모든 프로토콜 번호가 일치함)TCP(IP 프로토콜 6)UDP(IP 프로토콜 17)ICMP(IP 프로토콜 1)ESP(IP 프로토콜 50)AH(IP 프로토콜 51)GRE(IP 프로토콜 47)IP(IP 프로토콜 4 IP-in-IP [CSCsh22975])Eth Over IP(IP 프로토콜 97)OSPF(IP 프로토콜 89)기타(명시)Any 값은 패킷의 IP 헤더에 있는 모든 프로토콜과 일치합니다. 이는 특정 서브넷을 오가는 IP 패킷을 완전히 차단하거나 허용하는 데 사용됩니다. IP-in-IP 패킷과 일치시키려면 IP를 선택합니다. 일반적으로 특정 소스 및 목적지 포트를 설정하는 UDP 및 TCP를 선택합니다. Other(기타)를 선택하는 경우 IANA에서 정의한 IP 패킷 프로토콜 번호를 지정할 수 있습니다.
- **Src Port**(소스 포트) - TCP 및 UDP 프로토콜에 대해서만 지정할 수 있습니다. 0-65535은 Any 포트와 동일합니다.
- **Dest Port**(대상 포트) - TCP 및 UDP 프로토콜에 대해서만 지정할 수 있습니다. 0-65535은 Any 포트와 동일합니다.
- **Differentiated Services Code Point(DSCP)** - IP 패킷 헤더에서 매칭할 특정 DSCP 값을 지정할 수 있습니다. 풀다운 메뉴의 선택 항목은 특정 또는 Any입니다. 특정 항목을 구성하는 경우 DSCP 필드에 값을 지정합니다. 예를 들어 0~63의 값을 사용할 수 있습니다.
- **Action(작업)** - 두 가지 작업은 거부 또는 허용입니다. Deny는 지정된 패킷을 차단합니다. 허용 - 패킷을 전달합니다.

ACL 규칙 및 제한 사항

WLC 기반 ACL의 제한 사항

다음은 WLC 기반 ACL의 제한 사항입니다.

- 어떤 ACL 라인이 패킷과 일치하는지 확인할 수 없습니다(Cisco 버그 ID CSCse36574(등록된 고객만 해당) 참조).
- 특정 ACL 라인과 일치하는 패킷은 로깅할 수 없습니다(Cisco 버그 ID CSCse36574(등록된 고객만) 참조).
- IP 패킷(IP[0x0800]과 같은 이더넷 프로토콜 필드가 있는 모든 패킷)은 ACL에서 검사하는 유일한 패킷입니다. 다른 유형의 이더넷 패킷은 ACL로 차단할 수 없습니다. 예를 들어 ARP 패킷(이더넷 프로토콜 0x0806)은 ACL에서 차단하거나 허용할 수 없습니다.
- 컨트롤러는 최대 64개의 ACL을 구성할 수 있으며, 각 ACL은 최대 64개의 라인을 포함할 수 있습니다.
- ACL은 액세스 포인트(AP) 및 무선 클라이언트에서 전달되거나 해당 클라이언트로 전달되는 멀티캐스트 및 브로드캐스트 트래픽에 영향을 주지 않습니다(Cisco 버그 ID CSCse65613(등록된 고객만 해당) 참조).

- WLC 버전 4.0 이전에는 ACL이 관리 인터페이스에서 우회되므로 관리 인터페이스로 향하는 트래픽에 영향을 줄 수 없습니다. WLC 버전 4.0 후에는 CPU ACL을 생성할 수 있습니다. 이 유형의 ACL을 구성하는 방법에 대한 자세한 내용은 CPU ACL 구성을 참조하십시오.**참고:** 관리 및 AP-Manager 인터페이스에 적용되는 ACL은 무시됩니다. WLC의 ACL은 유선 네트워크와 WLC가 아닌 무선 및 유선 네트워크 간의 트래픽을 차단하도록 설계되었습니다. 따라서 특정 서브넷의 AP가 WLC와 완전히 통신하지 못하게 하려면 간헐적 스위치 또는 라우터에 액세스 목록을 적용해야 합니다. 이렇게 하면 해당 AP(VLAN)에서 WLC로의 LWAPP 트래픽이 차단됩니다.
- ACL은 프로세서에 따라 달라지며 과부하 상태에서 컨트롤러의 성능에 영향을 미칠 수 있습니다.
- ACL은 가상 IP 주소(1.1.1.1)에 대한 액세스를 차단할 수 없습니다. 따라서 무선 클라이언트의 경우 DHCP를 차단할 수 없습니다.
- ACL은 WLC의 서비스 포트에 영향을 주지 않습니다.

WLC 기반 ACL 규칙

다음은 WLC 기반 ACL에 대한 규칙입니다.

- ACL은 IP 패킷으로만 제한되므로 ACL 행에서 IP 헤더(UDP, TCP, ICMP 등)의 프로토콜 번호만 지정할 수 있습니다. IP를 선택하면 IP-in-IP 패킷을 허용하거나 거부함을 나타냅니다. Any(모두)를 선택하면 IP 프로토콜의 패킷을 허용하거나 거부함을 나타냅니다.
- 방향에 대해 Any를 선택하면 소스와 대상이 Any(0.0.0.0/0.0.0.0)여야 합니다.
- 소스 또는 목적지 IP 주소 중 하나가 Any가 아니면 필터의 방향을 지정해야 합니다. 또한 반환 트래픽에 대해 반대 방향의 역문(소스 IP 주소/포트 및 목적지 IP 주소/포트 스와핑됨)을 생성해야 합니다.
- ACL의 끝에 암시적 "deny any any"가 있습니다. 패킷이 ACL의 어떤 라인과도 일치하지 않으면 컨트롤러에 의해 삭제됩니다.

설정

DHCP, PING, HTTP 및 DNS를 사용하는 ACL 예

이 컨피그레이션 예에서는 클라이언트만 다음을 수행할 수 있습니다.

- DHCP 주소 수신(DHCP는 ACL에 의해 차단될 수 없음)
- Ping 및 ping됨(모든 ICMP 메시지 유형 - ping으로만 제한할 수 없음)
- HTTP 연결 만들기(아웃바운드)
- DNS(Domain Name System) 확인(아웃바운드)

이러한 보안 요구 사항을 구성하려면 ACL에 다음 항목을 허용할 행이 있어야 합니다.

- 어느 한 방향의 모든 ICMP 메시지(ping으로만 제한할 수 없음)
- DNS 인바운드에 대한 모든 UDP 포트
- 모든 UDP 포트 아웃바운드(반환 트래픽)에 대한 DNS
- HTTP 인바운드에 대한 모든 TCP 포트
- 임의의 TCP 포트 아웃바운드(반환 트래픽)에 대한 HTTP

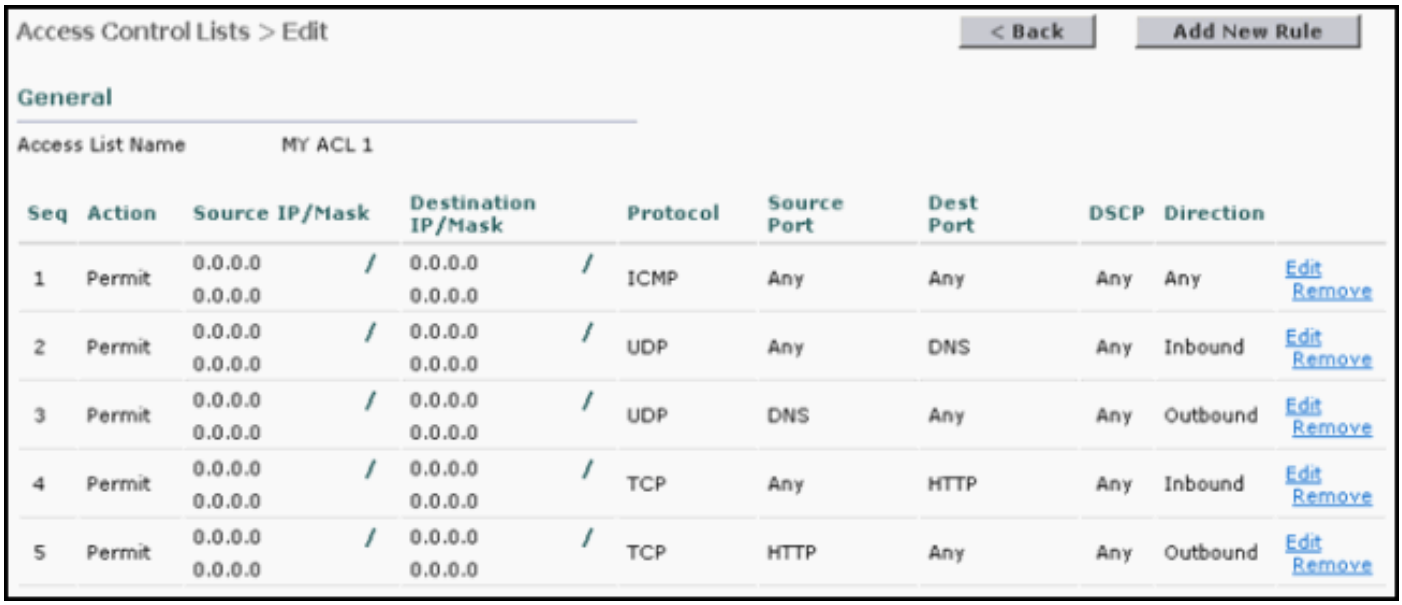
show acl detailed "MY ACL 1"(ACL 이름이 1단어 이상인 경우에만 따옴표가 필요함) 명령 출력에서 ACL이 다음과 같이 표시됩니다.

```
Seq  Direction  Source IP/Mask    Dest IP/Mask      Protocol  Src Port  Dest Port  DSCP  Action
---  ---------  ---------------   ---------------   --------  --------  ---------  ----  ------
1      Any      0.0.0.0/0.0.0.0   0.0.0.0/0.0.0.0       1     0-65535   0-65535     Any  Permit
2      In       0.0.0.0/0.0.0.0   0.0.0.0/0.0.0.0      17     0-65535   53-53       Any  Permit
3      Out      0.0.0.0/0.0.0.0   0.0.0.0/0.0.0.0      17     53-53     0-65535     Any  Permit
```

DNS 및 HTTP ACL 행의 Any IP 주소 대신 무선 클라이언트가 있는 서브넷을 지정하면 ACL이 더 제한될 수 있습니다.

참고: 클라이언트가 처음에 0.0.0.0을 사용하여 IP 주소를 수신한 다음 서브넷 주소를 통해 IP 주소를 갱신하므로 DHCP ACL 라인은 서브넷을 제한할 수 없습니다.

GUI에서 동일한 ACL은 다음과 같습니다.



DHCP, PING, HTTP 및 SCCP를 사용하는 ACL 예

이 컨피그레이션 예에서는 7920 IP Phone에서 다음 기능만 수행할 수 있습니다.

- DHCP 주소 수신(ACL로 차단할 수 없음)
- Ping 및 ping됨(모든 ICMP 메시지 유형 - ping으로만 제한할 수 없음)
- DNS 확인 허용(인바운드)
- CallManager에 대한 IP 전화 연결 또는 그 반대(모든 방향)
- TFTP 서버에 대한 IP 전화 연결(CallManager는 UDP 포트 69에 대한 초기 TFTP 연결 후 동적 포트를 사용함)(아웃바운드)
- 7920 IP Phone과 IP Phone 간 통신 허용(모든 방향)
- IP 전화 웹 또는 전화 디렉터리(아웃바운드)를 허용하지 않습니다. 이는 ACL의 끝에 있는 암시적 "deny any any" ACL 행을 통해 수행됩니다.이렇게 하면 IP Phone 간의 음성 통신은 물론 IP Phone과 CallManager 간의 정상적인 부팅 작업이 허용됩니다.

이러한 보안 요구 사항을 구성하려면 ACL에 다음 항목을 허용할 행이 있어야 합니다.

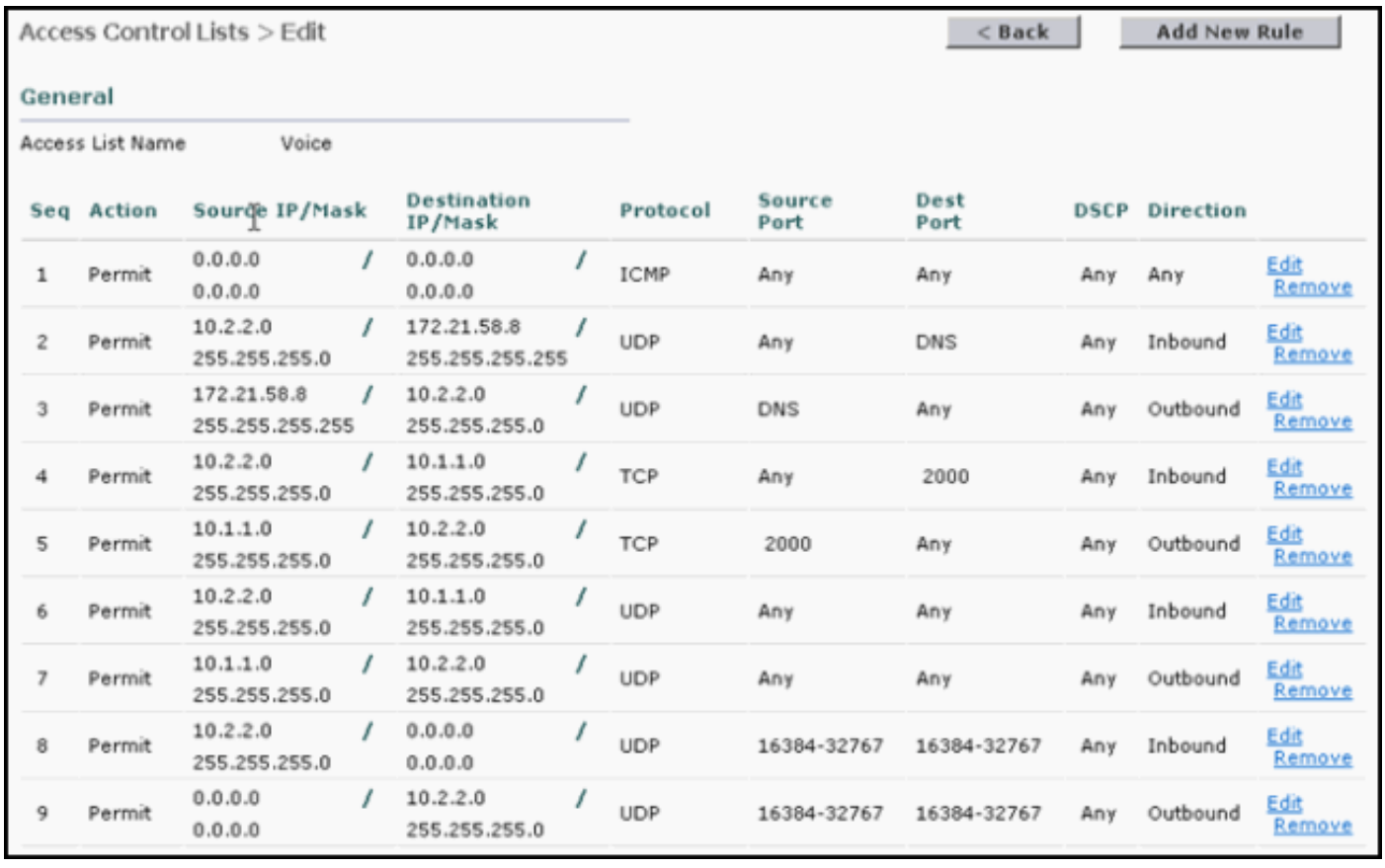
- 모든 ICMP 메시지(ping으로만 제한할 수 없음)(모든 방향)
- DNS 서버에 대한 IP 전화(UDP 포트 53)(인바운드)
- IP 전화에 대한 DNS 서버(UDP 포트 53)(아웃바운드)
- CallManager TCP 포트 2000(기본 포트)에 대한 IP Phone TCP 포트(인바운드)
- CallManager에서 IP Phone으로의 TCP 포트 2000(아웃바운드)

- IP 전화에서 TFTP 서버로의 UDP 포트. CallManager가 데이터 전송을 위한 초기 연결 요청 후 동적 포트를 사용하므로 이를 표준 TFTP 포트(69)로 제한할 수 없습니다.
- IP 전화 간 오디오 트래픽 RTP용 UDP 포트(UDP 포트16384-32767)(모든 방향)

이 예에서 7920 IP 전화 서브넷은 10.2.2.0/24이고 CallManager 서브넷은 10.1.1.0/24입니다. DNS 서버는 172.21.58.8입니다. 다음은 show acl **detail Voice 명령**의 출력입니다.

```
Seq Direction Source IP/Mask          Dest IP/Mask             Protocol Src Port  Dest Port  DSCP
Action
--- --------- ---------------         ---------------          -------- --------  ---------  ----
------
1     Any     0.0.0.0/0.0.0.0         0.0.0.0/0.0.0.0             1     0-65535   0-65535    Any
Permit
2     In      10.2.2.0/255.255.255.0 172.21.58.8/255.255.255.255 17    0-65535   53-53      Any
Permit
3     Out     172.21.58.8/255.255.255.255 10.2.2.0/255.255.255.0 17    53-53     0-65535    Any
Permit
4     In      10.2.2.0/255.255.255.0  10.1.1.0/255.255.255.0      6     0-65535   2000-2000  Any
Permit
5     Out     10.1.1.0/255.255.255.0  10.2.2.0/255.255.255.0      6     2000-2000 0-65535    Any
Permit
6     In      10.2.2.0/255.255.255.0  10.1.1.0/255.255.255.0      17    0-65535   0-65535    Any
Permit
7     Out     10.1.1.0/255.255.255.0  10.2.2.0/255.255.255.0      17    0-65535   0-65535    Any
Permit
8     In      10.2.2.0/255.255.255.0  0.0.0.0/0.0.0.0             17 16384-32767 16384-32767 Any
Permit
9     Out     0.0.0.0/0.0.0.0         10.2.2.0/255.255.255.0      17 16384-32767 16384-32767 Any
Permit
```

GUI에서는 다음과 같이 표시됩니다.



Access Control Lists > Edit

< Back | Add New Rule

General

Access List Name: Voice

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	ICMP	Any	Any	Any	Any	Edit Remove
2	Permit	10.2.2.0 / 255.255.255.0	172.21.58.8 / 255.255.255.255	UDP	Any	DNS	Any	Inbound	Edit Remove
3	Permit	172.21.58.8 / 255.255.255.255	10.2.2.0 / 255.255.255.0	UDP	DNS	Any	Any	Outbound	Edit Remove
4	Permit	10.2.2.0 / 255.255.255.0	10.1.1.0 / 255.255.255.0	TCP	Any	2000	Any	Inbound	Edit Remove
5	Permit	10.1.1.0 / 255.255.255.0	10.2.2.0 / 255.255.255.0	TCP	2000	Any	Any	Outbound	Edit Remove
6	Permit	10.2.2.0 / 255.255.255.0	10.1.1.0 / 255.255.255.0	UDP	Any	Any	Any	Inbound	Edit Remove
7	Permit	10.1.1.0 / 255.255.255.0	10.2.2.0 / 255.255.255.0	UDP	Any	Any	Any	Outbound	Edit Remove
8	Permit	10.2.2.0 / 255.255.255.0	0.0.0.0 / 0.0.0.0	UDP	16384-32767	16384-32767	Any	Inbound	Edit Remove
9	Permit	0.0.0.0 / 0.0.0.0	10.2.2.0 / 255.255.255.0	UDP	16384-32767	16384-32767	Any	Outbound	Edit Remove

부록: 7920 IP 전화 포트

다음은 7920 IP Phone에서 CCM(Cisco CallManager) 및 기타 IP Phone과 통신하는 데 사용하는 포트에 대한 요약 설명입니다.

- CCM[TFTP]에 전화(UDP 포트 69는 처음에 데이터 전송을 위해 동적 포트 [Ephemeral]로 변경) - 펌웨어 및 컨피그레이션 파일을 다운로드하는 데 사용되는 TFTP(Trivial File Transfer Protocol)입니다.
- Phone to CCM [Web Services, Directory](TCP 포트 80) - XML 애플리케이션, 인증, 디렉토리, 서비스 등에 대한 전화 URL입니다. 이러한 포트는 서비스 단위로 구성할 수 있습니다.
- Phone to CCM [Voice Signaling](TCP 포트 2000) - SCCP(Skinny Client Control Protocol). 이 포트는 구성 가능합니다.
- Phone to CCM [Secure Voice Signaling](TCP 포트 2443) - SCCPS(Secure Skinny Client Control Protocol)
- Phone to CAPF [Certificates] (TCP 포트 3804) - IP 전화에 LSC(Locally Significant Certificates)를 발급하기 위한 CAPF(Certificate Authority Proxy Function) 수신 포트입니다.
- Voice Bearer to/from Phone [Phone Calls](UDP 포트 16384 - 32768) - RTP(Real-Time Protocol), SRTP(Secure Real Time Protocol)**참고:** CCM은 UDP 포트 24576-32768만 사용하지만 다른 디바이스에서는 전체 범위를 사용할 수 있습니다.
- IP Phone to DNS Server [DNS] (UDP 포트 53)(IP Phone to DNS Server [DNS](UDP 포트 53)) - 시스템이 IP 주소 대신 이름을 사용하도록 구성된 경우 전화기에서 DNS를 사용하여 TFTP 서버, CallManager 및 웹 서버 호스트 이름을 확인합니다.
- IP Phone to DHCP server [DHCP] (UDP 포트 67 [client] & 68 [server]) - 정적으로 구성되지 않은 경우 DHCP를 사용하여 IP 주소를 검색합니다.

5.0 CallManager가 통신하는 데 사용하는 포트는 Cisco Unified CallManager 5.0 TCP 및 UDP Port Usage에서 확인할 수 있습니다. 또한 7920 IP 전화와 통신하는 데 사용하는 특정 포트도 있습니다.

4.1 CallManager가 통신에 사용하는 포트는 Cisco Unified CallManager 4.1 TCP 및 UDP Port Usage에서 확인할 수 있습니다. 또한 7920 IP 전화와 통신하는 데 사용하는 특정 포트도 있습니다.

관련 정보

- Wireless LAN Controller의 ACL 설정 예시
- Cisco Wireless LAN Controller 컨피그레이션 가이드, 릴리스 4.0
- 기술 지원 및 문서 – Cisco Systems

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.