WAP121 및 WAP321 액세스 포인트에서 IPv4 기반 ACL(Access Control List)에 대한 규칙 생성 및 구성

목표

ACL(Access Control List)은 보안을 개선하는 데 사용되는 네트워크 트래픽 필터 및 상호 관련된 작업의 목록입니다.ACL에는 네트워크 장치에 대한 액세스가 허용되거나 거부된 호스트가 포함되어 있습니다. QoS 기능에는 정의된 홉별 동작에 따라 트래픽을 스트림으로 분류하고 특정 QoS 처리를 허용하는 DiffServ(차별화된 서비스) 지원이 포함되어 있습니다.

이 문서에서는 WAP121 및 WAP321 WAP(Access Point)에서 IPv4 기반 ACL을 생성하고 구성하는 방법에 대해 설명합니다.

적용 가능한 디바이스

·WAP121
· WAP321

소프트웨어 버전

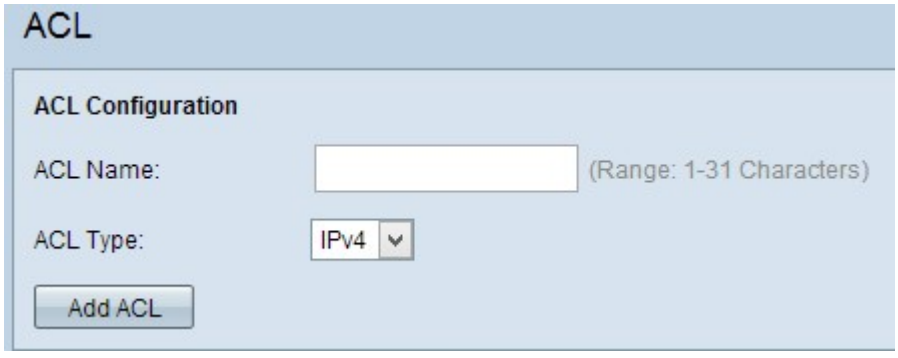
·v1.0.3.4

IPv4 기반 ACL 컨피그레이션

IP ACL은 IP 스택의 레이어 3에 대한 트래픽을 분류합니다.각 ACL은 무선 클라이언트에서 전송되거나 무선 클라이언트에서 수신되는 트래픽에 적용되는 최대 10개의 규칙 집합입니다.각 규칙은 지정된 필드의 내용을 사용하여 네트워크에 대한 액세스를 허용할지 또는 거부할지를 지정합니다.규칙은 다양한 기준을 기반으로 할 수 있으며, 소스 또는 목적지 IP 주소, 소스 또는 목적지 포트 또는 패킷에 포함된 프로토콜과 같은 패킷 내의 하나 이상의 필드에 적용할 수 있습니다.

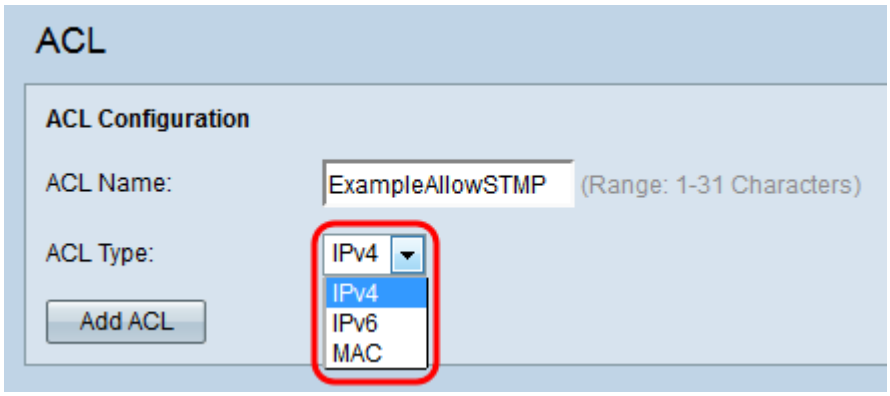
IPv4 ACL 생성

1단계. Access Point Configuration Utility에 로그인하고 Client QoS **> ACL을** 선택합니다.*ACL* 페이지가 열립니다.

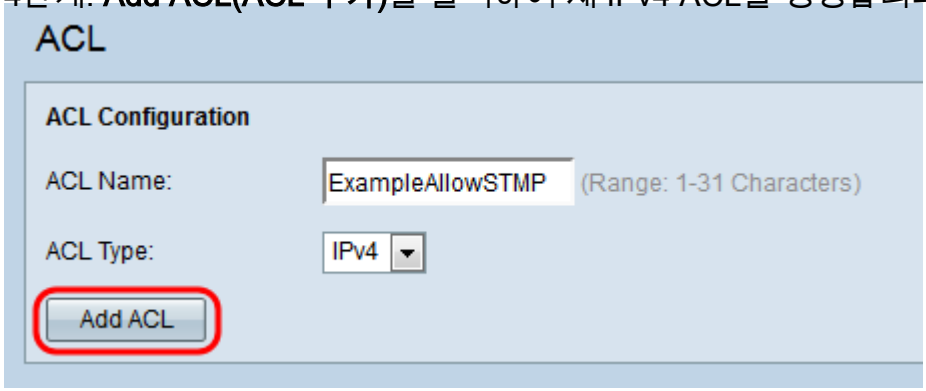


2단계. *ACL 이름* 필드에 ACL의 이름을 입력합니다.

3단계. *ACL Type* 드롭다운 목록에서 ACL의 IPv**4** 유형을 선택합니다.



4단계. **Add ACL(ACL 추가)**을 클릭하여 새 IPv4 ACL을 생성합니다.



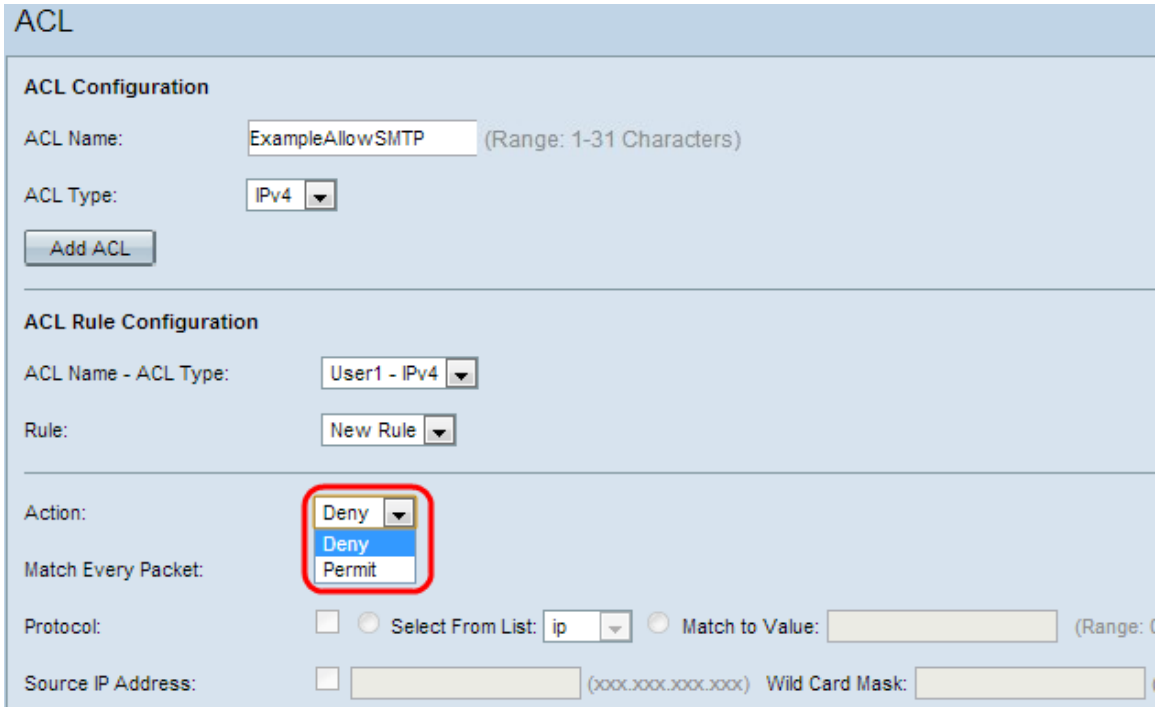
IPv4 ACL에 대한 규칙 구성

1단계. ACL *Name-ACL Type(ACL 이름-ACL 유형)* 드롭다운 목록에서 규칙을 구성해야 하는 ACL을 선택합니다.

2단계. 선택한 ACL에 대해 새 규칙을 구성해야 하는 경우 *Rule* 드롭다운 목록에서 **New Rule(새 규칙)**을 선택합니다.그렇지 않으면 Rule 드롭다운 목록에서 현재 규칙 중 하나*를* 선택합니다.

참고:단일 ACL에 대해 최대 10개의 규칙을 생성할 수 있습니다.

3단계. Action(작업) 드롭다운 목록에서 ACL 규칙에 대한 작업을 선택합니다.

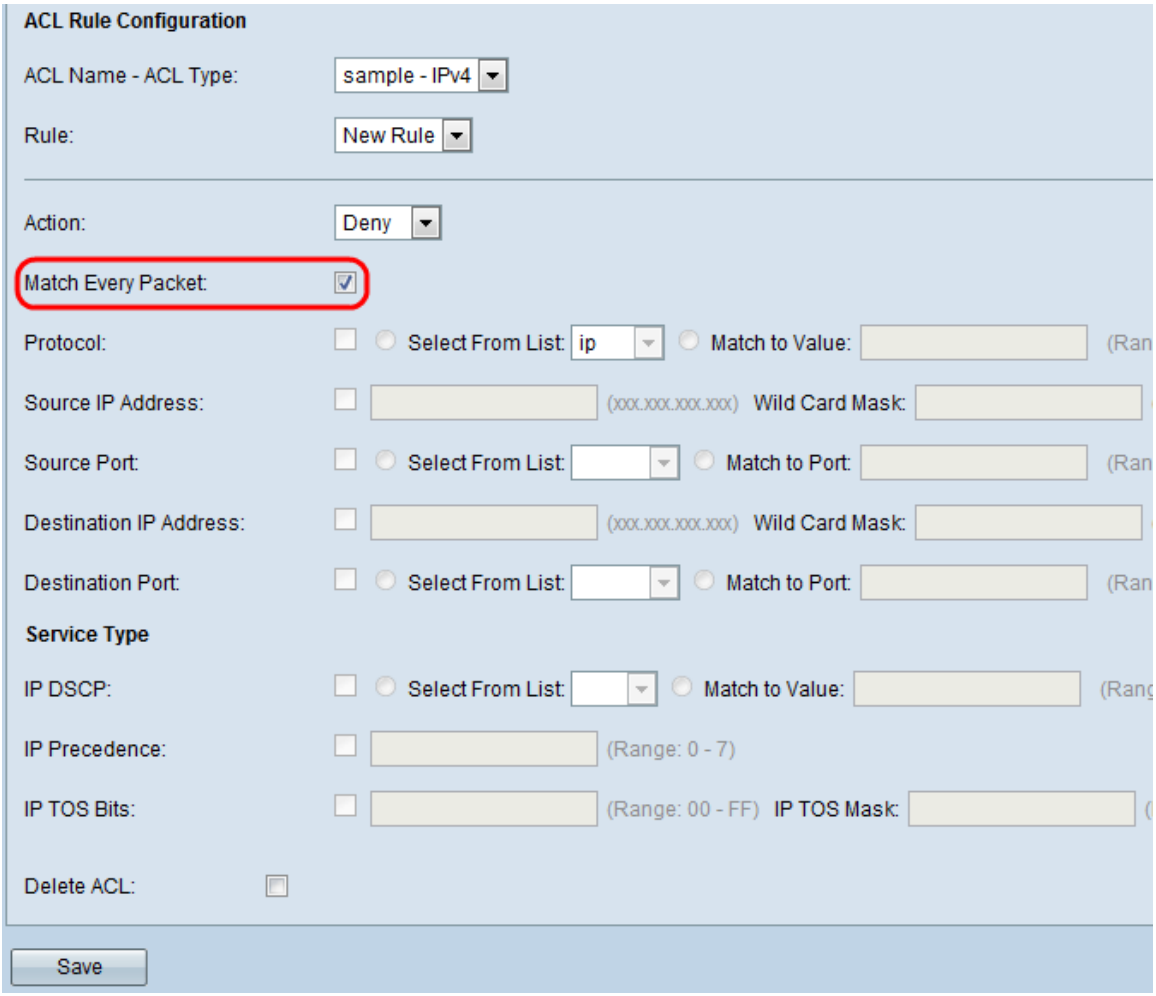


사용 가능한 옵션은 다음과 같이 설명합니다.

·거부 — 규칙 기준을 충족하는 모든 트래픽을 차단하여 WAP 디바이스를 입력하거나 종료합니다.

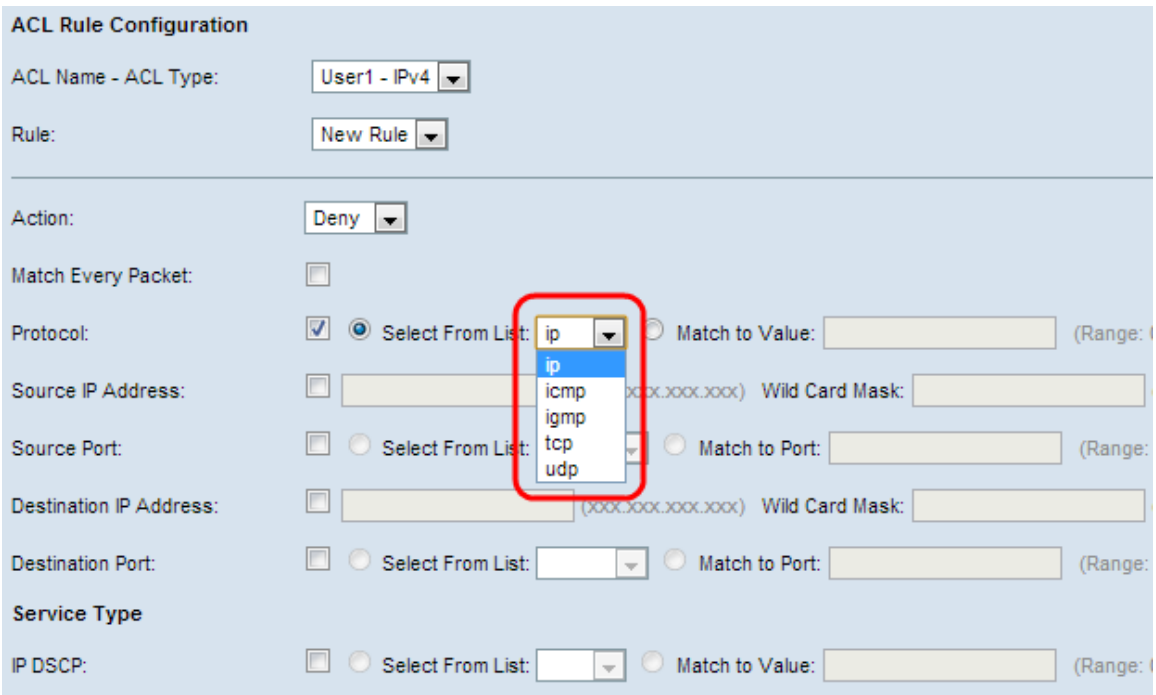
·허용 — 규칙 기준을 충족하는 모든 트래픽이 WAP 디바이스를 입력하거나 종료할 수 있습니다.

4단계. Match *Every Packet(모든 패킷* 일치) 확인란을 선택하여 해당 내용에 관계없이 모든 프레임 또는 패킷에 대해 규칙을 확인합니다.특정 일치 기준을 구성하려면 Match Every *Packet* 확인란을 선택 취소합니다.



시간 절약: Match Every Packet(*모든 패킷 일치*) 확인란을 선택한 경우 13단계로 건너뜁니다.

5단계. (선택 사항) IPv4 패킷의 IP Protocol 필드 값을 기반으로 L3 또는 L4 프로토콜 일치 조건의 Protocol 확인란을 선택합니다.Protocol(*프로토콜*) 확인란을 선택한 경우 다음 라디오 버튼 중 하나를 클릭합니다.

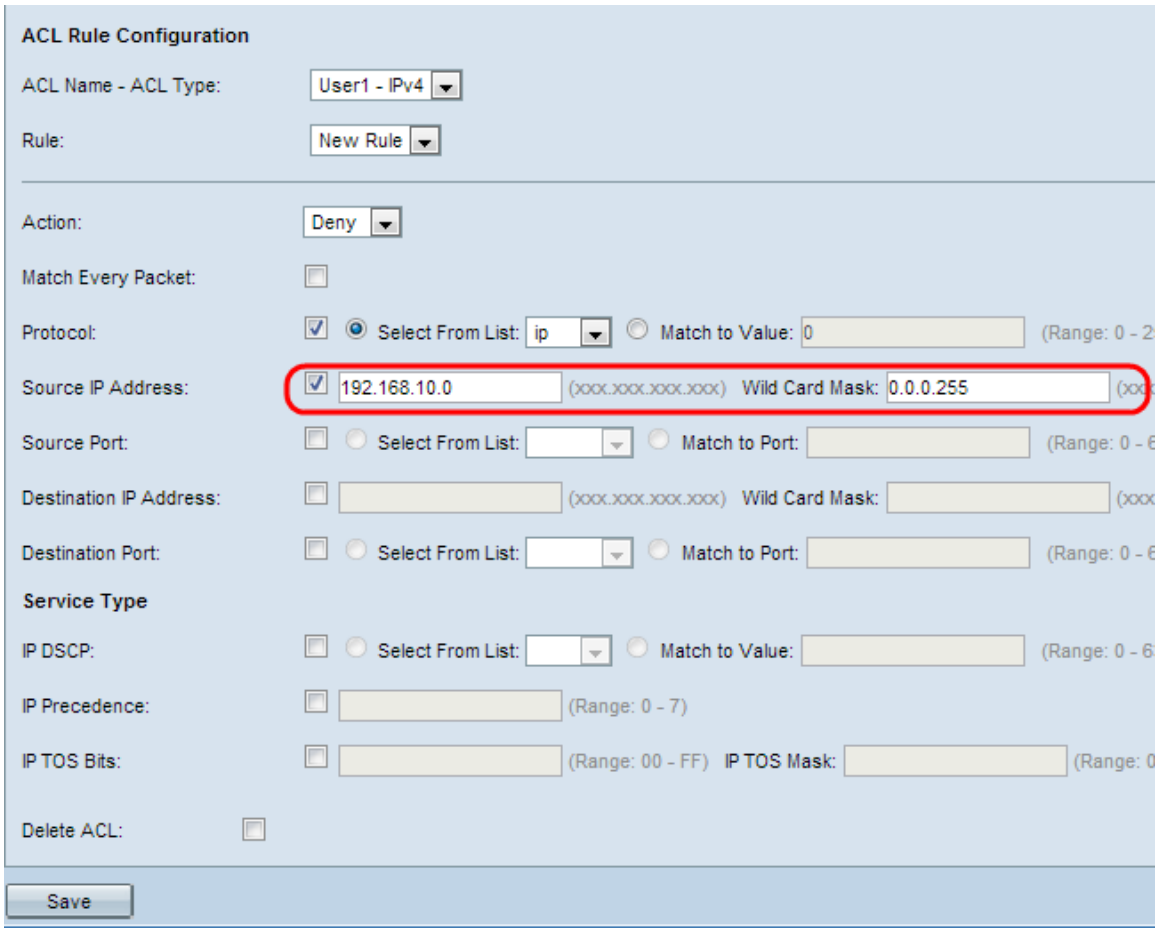


옵션은 다음과 같이 설명합니다.

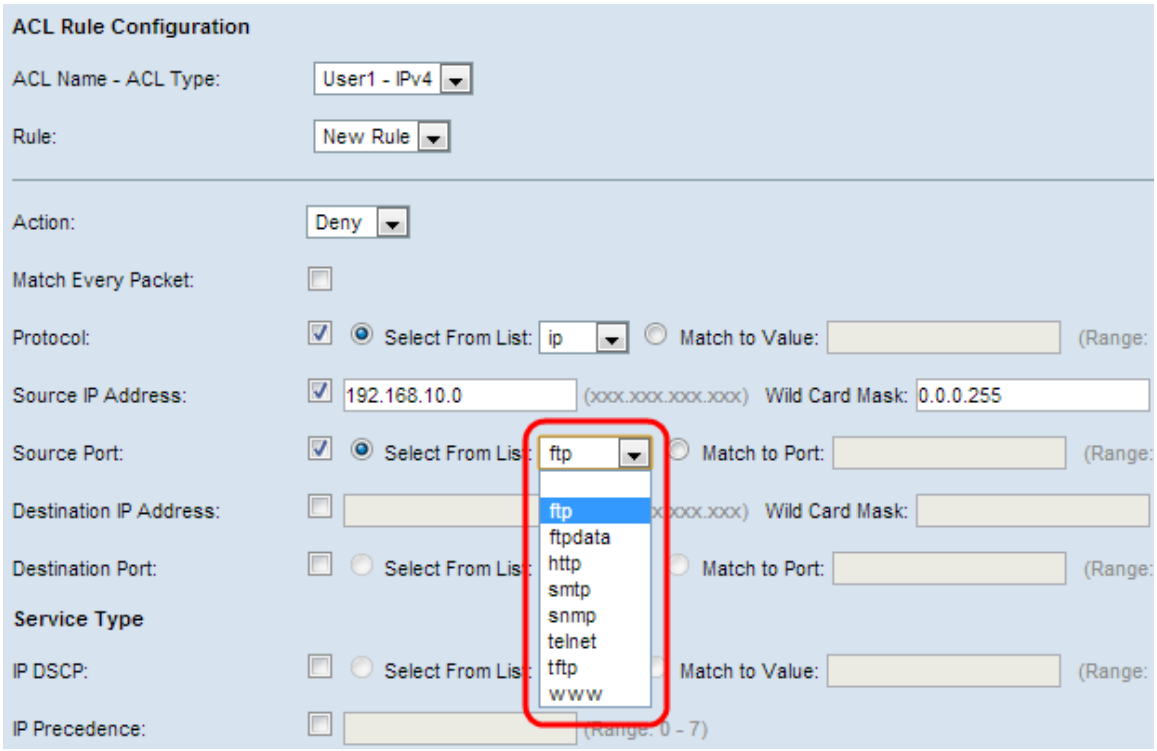
·목록에서 선택 — 목록에서 선택 드롭다운 목록에서 프로토콜을 선택합니다.드롭다운 목록에는 ip, icmp, igmp, tcp, udp 프로토콜이 있습니다.

·Match to Value — 목록에 없는 프로토콜의 경우0~255의 표준 IANA 할당 프로토콜 ID를 입력합니다.

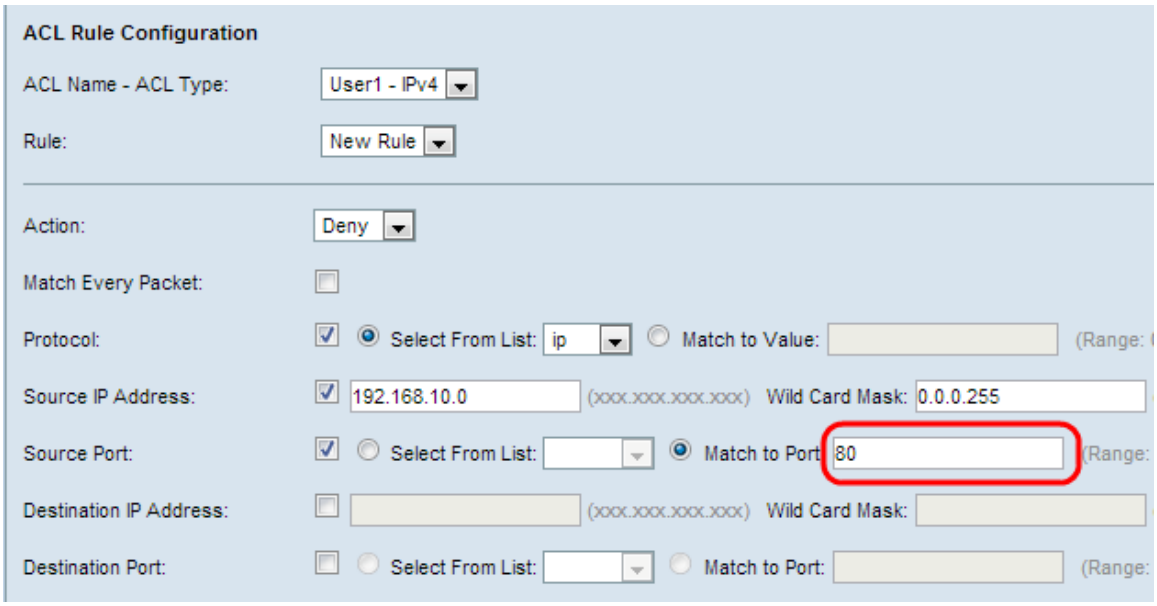
6단계. (선택 사항) 소스의 IP 주소를 일치 조건에 포함하려면 *Source IP Address* 확인란을 선택합니다.각 필드에 소스의 IP 주소 및 *와일드카드 마스크*를 입력합니다.와일드카드 마스크를 사용하면 이 액세스 목록이 적용되는 소스 IP 주소의 호스트를 지정할 수 있습니다.



7단계. (선택 사항) **Source Port** 확인란을 선택하여 일치 조건에 소스 포트를 포함합니다 .Source *Port(소스 포트)* 확인란을 선택한 경우 이러한 라디오 버튼 중 하나를 클릭합니다.

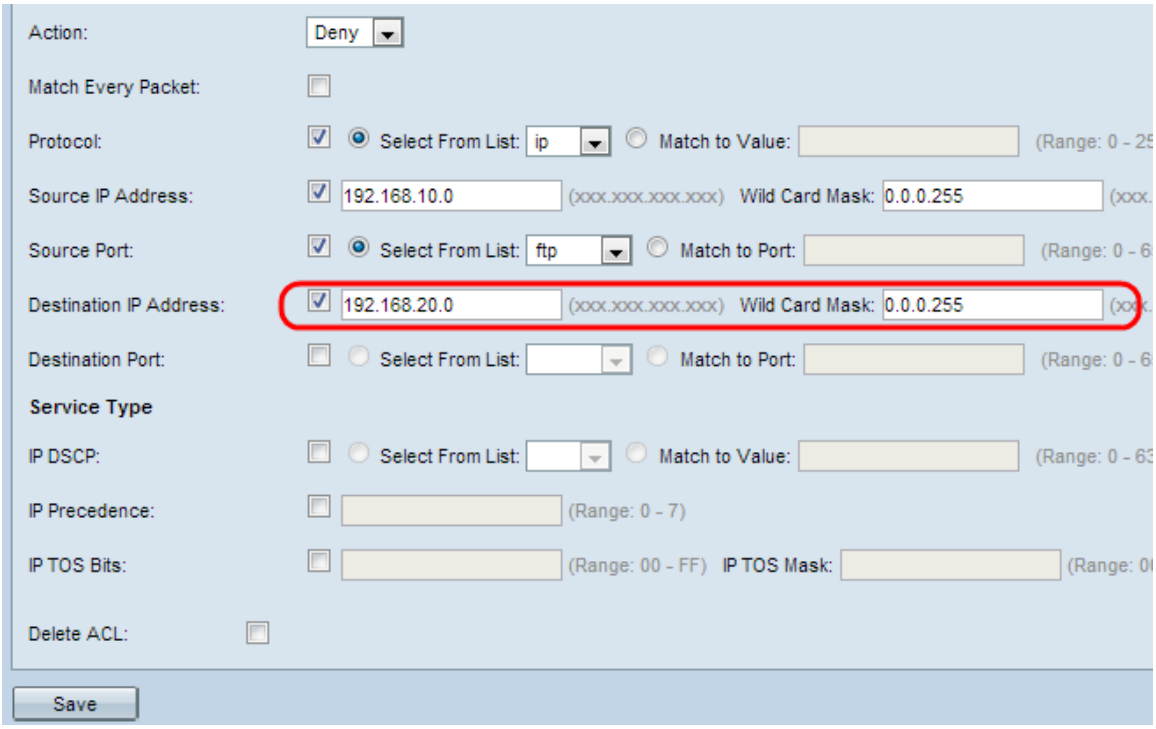


·목록에서 선택 — 목록에서 선택 드롭다운 목록에서 소스 포트를 선택합니다.드롭다운 목록에는 ftp, ftpdata, http, smtp, snmp, telnet, tftp, www 포트가 있습니다.

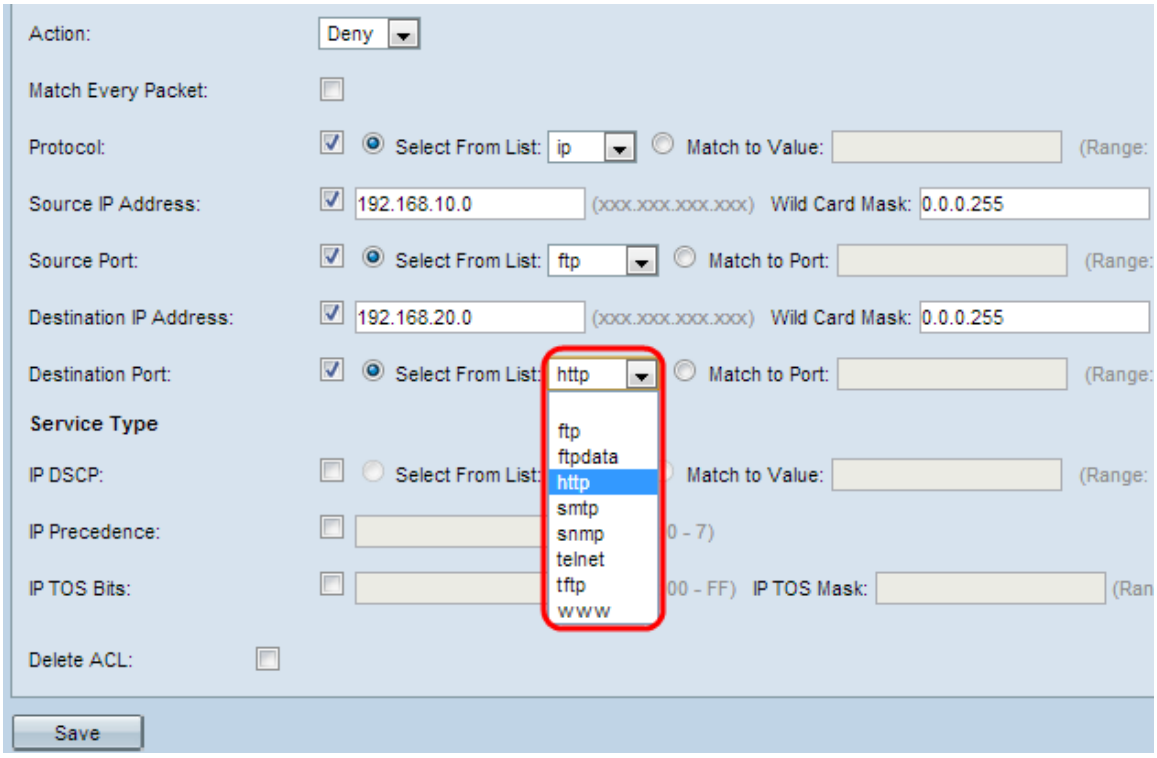


·Match to Port(포트에 일치) - 목록에 없는 소스 포트의 경우0~65535 범위의 포트 번호를 입력합니다.

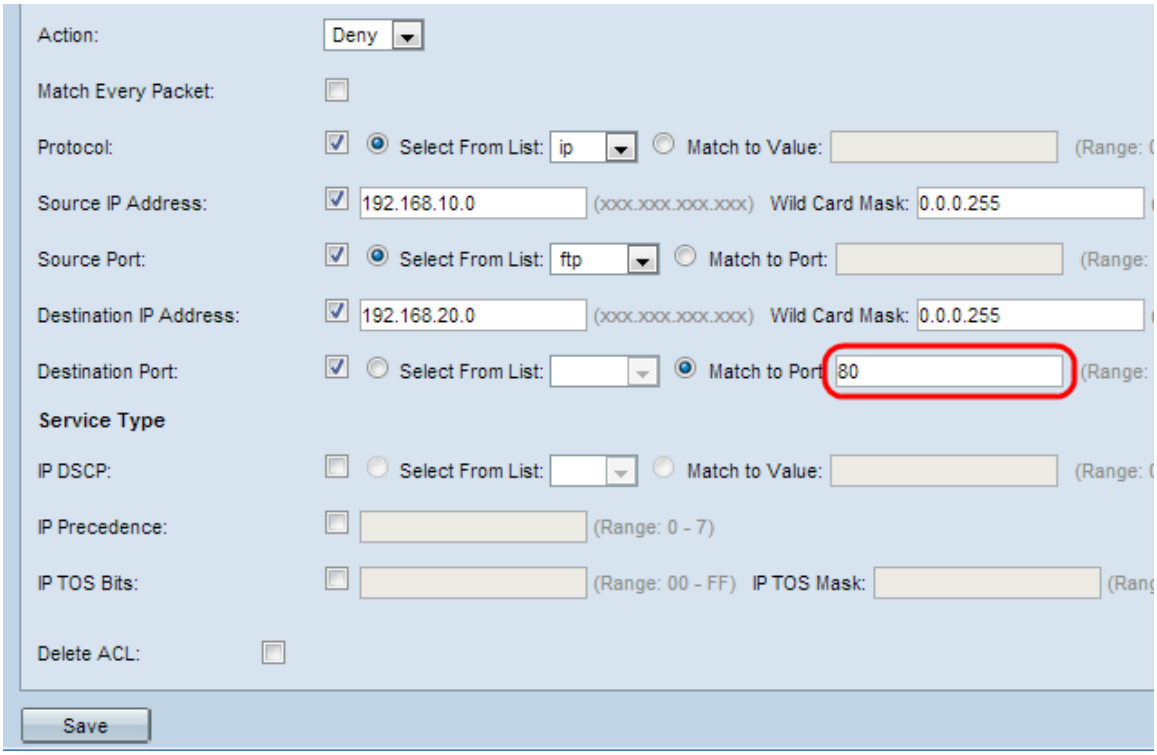
8단계. (선택 사항) 대상의 IP 주소를 일치 조건에 포함하려면 *Destination IP Address* 확인란을 선택합니다.각 필드에 대상의 IP 주소 및 *와일드카드 마스크*를 입력합니다.와일드카드 마스크를 사용하면 이 액세스 목록이 적용되는 대상 IP 주소의 호스트를 지정할 수 있습니다.



9단계. (선택 사항) **Destination Port** 확인란을 선택하여 일치 조건에 대상 포트를 포함합니다 .Destination *Port*(대상 포트) 확인란을 선택한 경우 다음 라디오 버튼 중 하나를 클릭합니다.



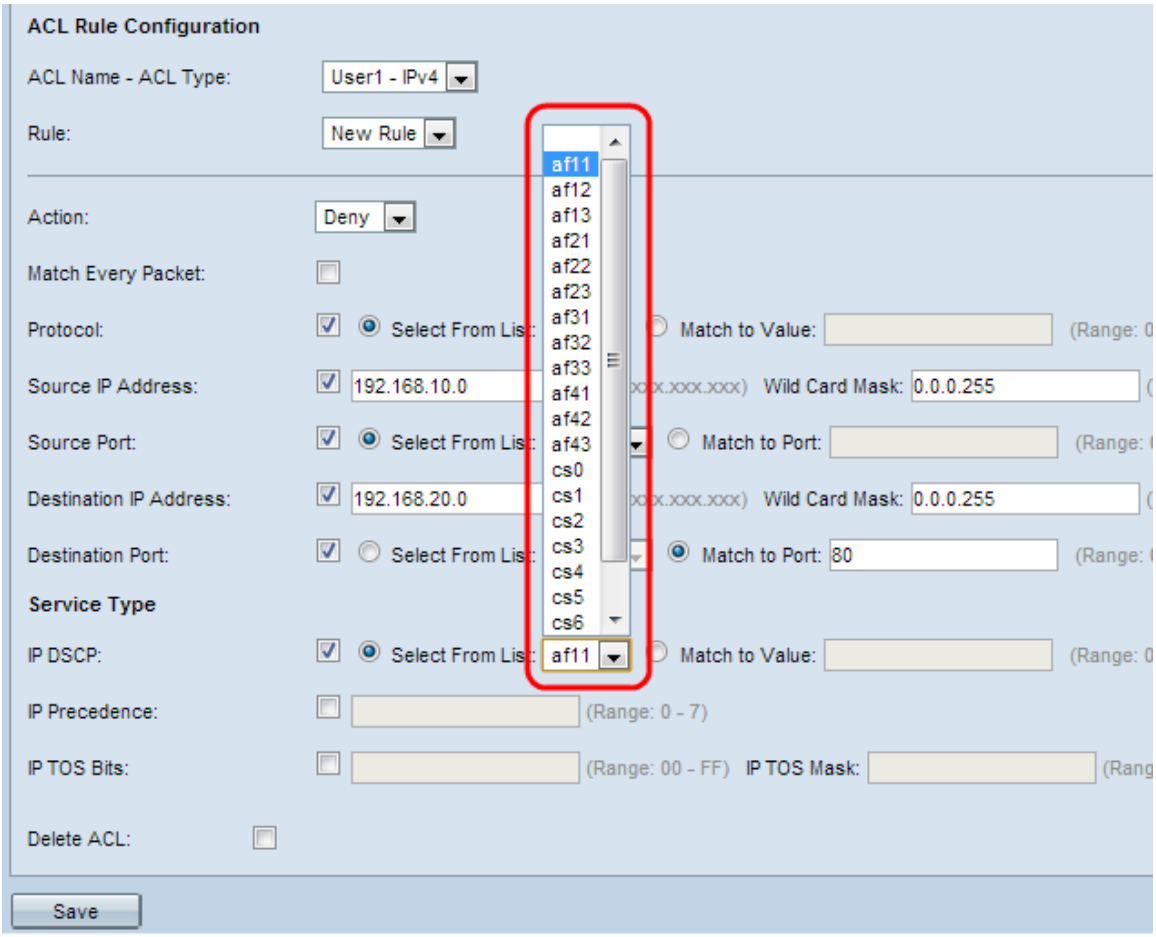
·목록에서 선택 — 목록에서 선택 드롭다운 목록에서 대상 포트를 선택합니다.드롭다운 목록에는 ftp, ftpdata, http, smtp, snmp, telnet, tftp, www 포트가 있습니다.



·Match to Port(포트에 일치) - 목록에 없는 대상 포트의 경우Match to Port 필드에 0~65535 범위의 포트 번호를 입력합니다.

참고:서비스 유형 영역에서 서비스 중 하나만 선택할 수 있으며 일치 조건에 대해 추가할 수 있습니다.

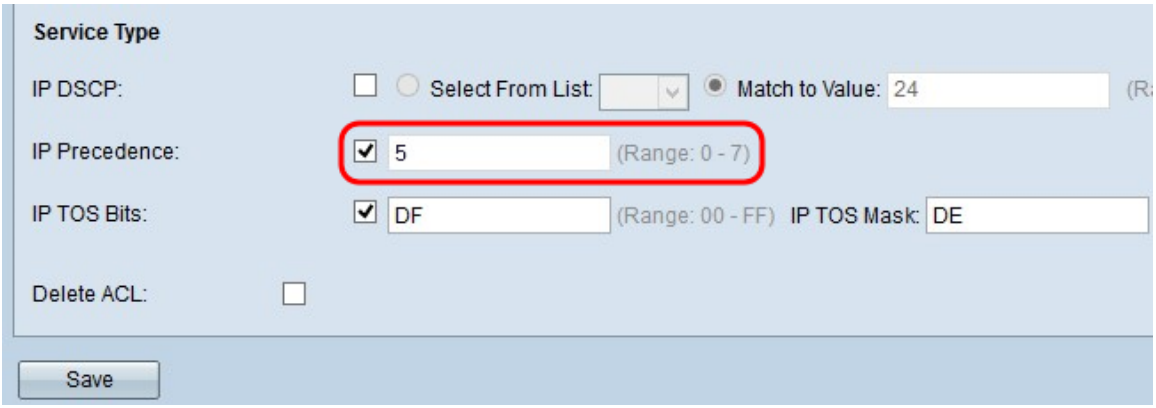
10단계. (선택 사항) *IP DSCP* 값을 기반으로 패킷을 매칭하려면 IP DSCP 확인란을 선택합니다.*IP DSCP* 확인란을 선택한 경우 이러한 라디오 버튼 중 하나를 클릭합니다.DSCP는 프레임의 IP 헤더에 대한 트래픽 우선순위를 지정하는 데 사용됩니다.그러면 연결된 트래픽 스트림에 대한 모든 패킷이 목록에서 선택한 IP DSCP 값으로 분류됩니다.DSCP에 대한 자세한 내용은 여기를 참조하십시오.



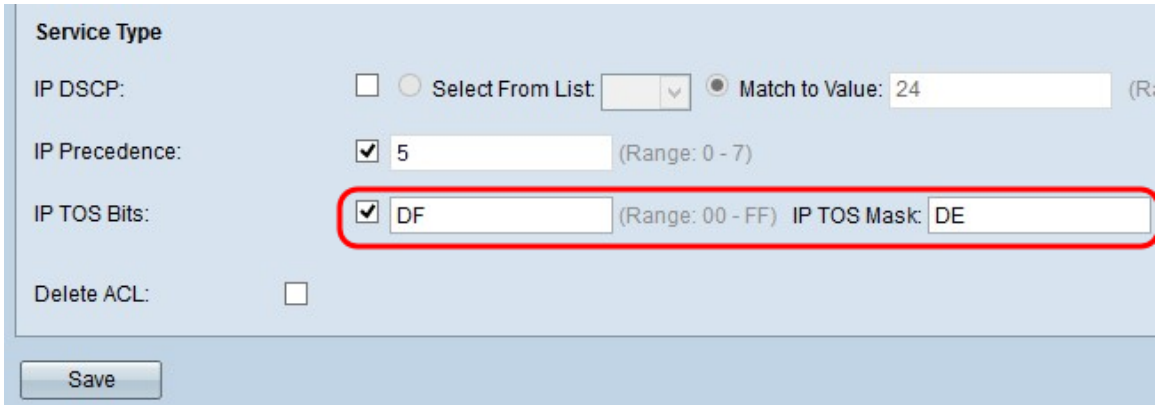
·목록에서 선택 — 목록에서 선택 드롭다운 목록에서 IP DSCP 값을 선택합니다.드롭다운 목록에는 DSCP AS(Assured Forwarding), CS(Class of Service) 또는 EF(Shipped Forwarding) 값이 있습니다.

·값에 일치 — DSCP 값을 사용자 정의합니다.Match to Value(값 일치) 필드에 0~63 범위의 DSCP 값을 입력합니다.

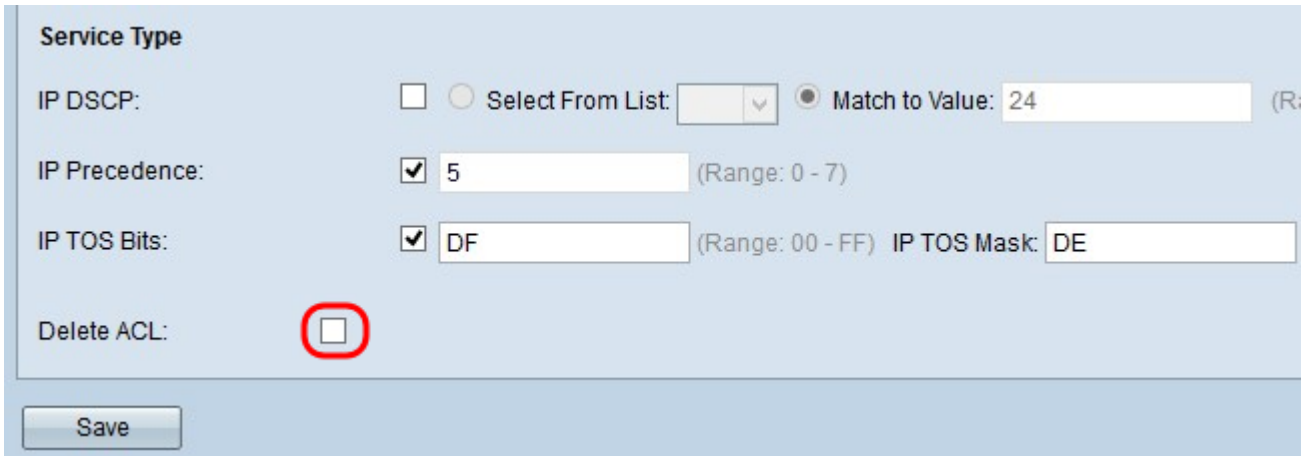
11단계. (선택 사항) *IP Precedence* 확인란을 선택하여 일치 조건에 IP Precedence 값을 포함합니다.IP Precedence(IP 우선 순위) 확인란을 선택한 경우 0~7 범위의 IP 우선 순위 값을 입력합니다. IP 우선 순위에 대한 자세한 내용은 여기를 참조하십시오.



12단계(선택 사항) IP 헤더에서 패킷의 서비스 유형 비트를 일치 기준으로 사용하려면 *IP TOS Bits* 확인란을 선택합니다.IP TOS Bits(IP TOS 비트) 확인란을 선택한 경우 각 필드에 00-FF 및 IP TOS 마스크의 범위가 00-FF인 IP TOS 비트를 입력합니다.



13단계. (선택 사항) 구성된 ACL을 삭제하려면 *Delete ACL* 확인란을 선택합니다.



14단계. **저장**을 클릭하여 설정을 저장합니다.