무선 액세스 포인트에서 MAC, IPv4 및 IPv6 액세스 제어 목록 구성

목표

ACL(Access Control List)은 보안을 개선하는 데 사용되는 네트워크 트래픽 필터 및 상호 관련된 작업의 목록입니다.권한이 없는 사용자를 차단하고 권한이 있는 사용자가 특정 리소스에 액세스할 수 있도록 합니다.ACL에는 네트워크 디바이스에 대한 액세스가 허용되거나 거부된 호스트가 포함됩니다.ACL은 다음 두 가지 방법 중 하나로 정의할 수 있습니다.IPv4 주소 또는 IPv6 주소별.

이 문서에서는 ACL을 성공적으로 생성하고 WAP(무선 액세스 포인트)에서 IPv4, IPv6 및 MAC(Media Access Control) 기반 ACL을 구성하여 네트워크 보안을 개선하는 방법에 대해 설명합니다.

적용 가능한 디바이스

- WAP100 시리즈
- WAP300 시리즈
- WAP500 시리즈

소프트웨어 버전

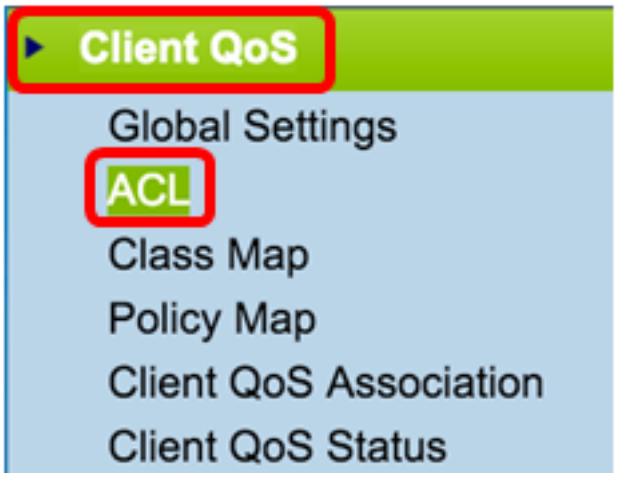
- 1.0.6.2 - WAP121, WAP321
- 1.2.0.2 - WAP371, WAP551, WAP561
- 1.0.1.4 - WAP131, WAP351
- 1.0.0.16 - WAP150, WAP361

ACL 생성

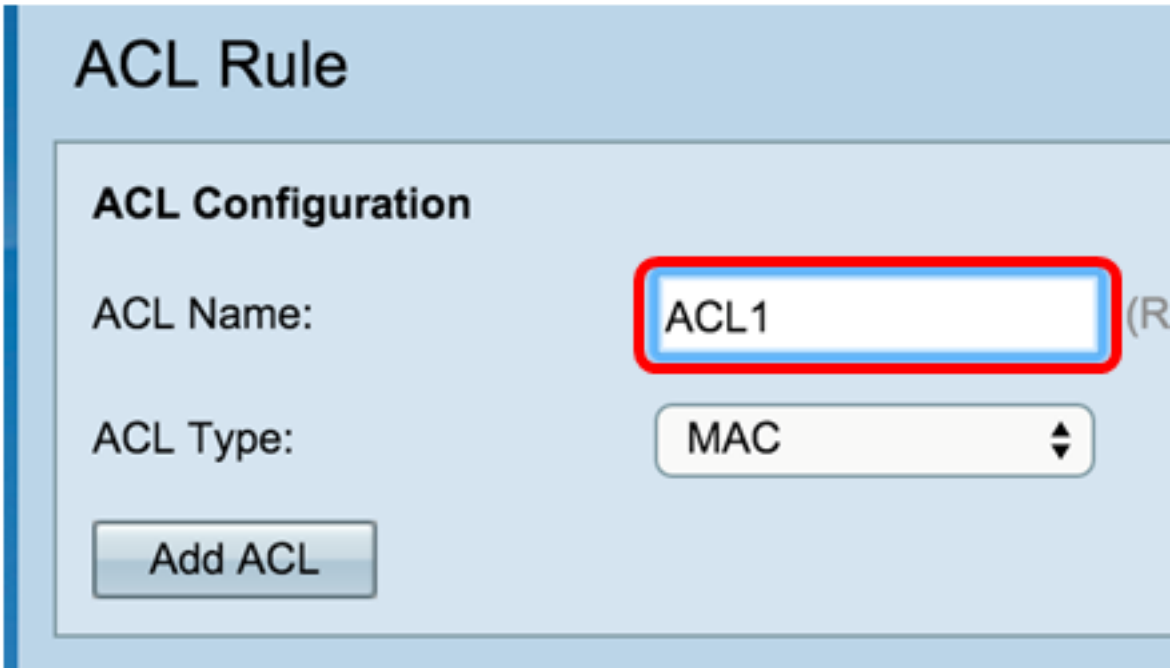
참고:이 구성에 사용된 이미지는 WAP150에서 가져온 것입니다.

1단계. 액세스 포인트 웹 기반 유틸리티에 로그인하고 **ACL > ACL Rule을** 선택합니다.

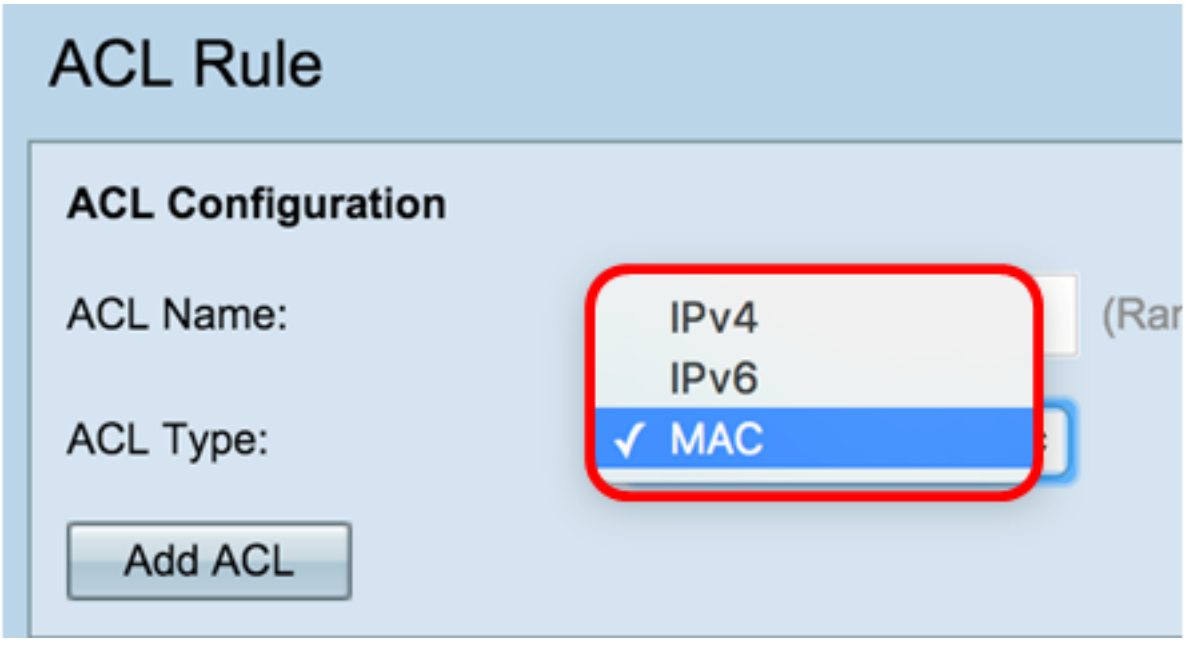
참고:WAP121, WAP321, WAP371, WAP551 및 WAP561의 경우:액세스 포인트 웹 기반 유틸리티에 로그인하고 Client QoS > ACL을 선택합니다.



2단계. ACL Configuration(ACL 컨피그레이션) 페이지가 열리면 *ACL Name(ACL 이름)* 필드에 ACL 이름을 입력합니다.



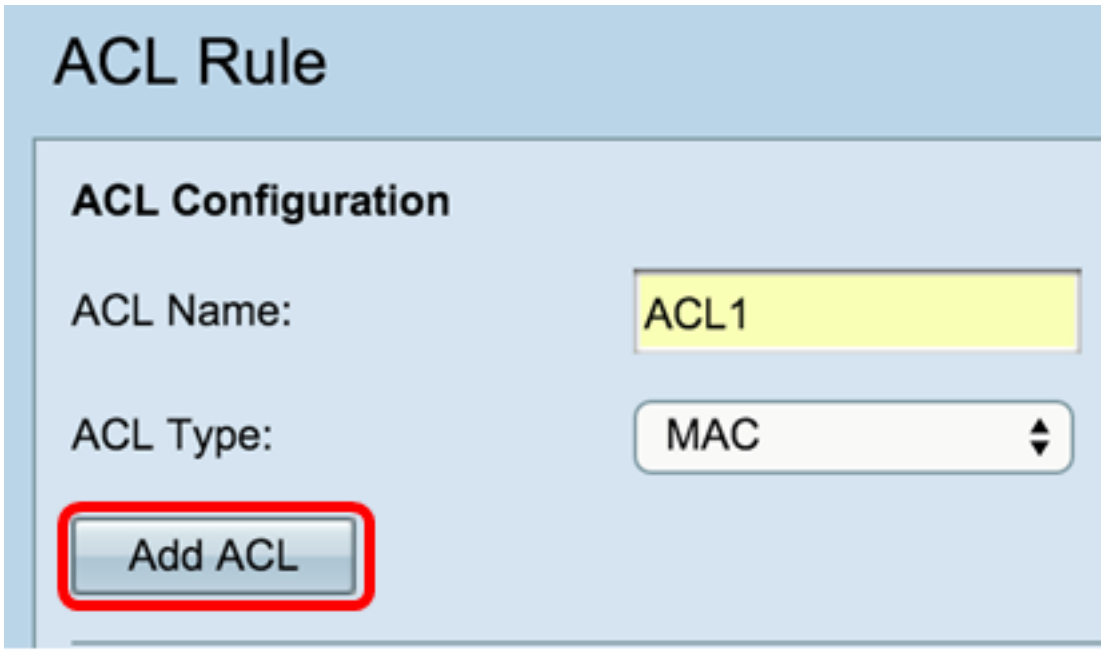
3단계. ACL 유형 드롭다운 목록에서 **ACL 유형**을 선택합니다.



- IPv4 — 32비트(4바이트) 주소입니다.

- IPv6 — IPv4의 후속 항목은 128비트(8바이트) 주소로 구성됩니다.
- MAC — MAC 주소는 네트워크 인터페이스에 할당된 고유 주소입니다.

4단계. Add **ACL(ACL 추가)** 버튼을 클릭합니다.



MAC을 선택한 경우 Configure MAC-based ACL로 건너뜁니다.

IPv4를 선택한 경우 Configure IPv4-based ACL로 건너뜁니다.

IPv6을 선택한 경우 Configure IPv6-based ACL로 건너뜁니다.

이제 성공적으로 ACL을 생성했어야 합니다.

MAC 기반 ACL 구성

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

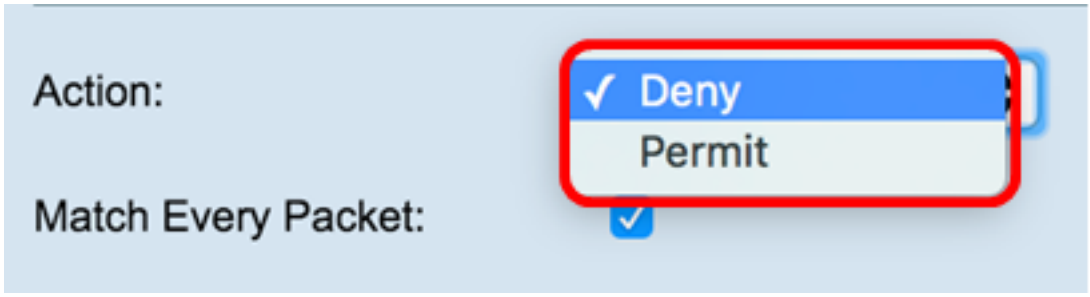
참고:아래 그림에서 예제로 ACL1 MAC을 선택했습니다.

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 하나를 선택합니다.

참고: 단일 ACL에 대해 최대 10개의 규칙을 생성할 수 있습니다.

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

참고: 이 예에서는 Deny 문이 생성됩니다.

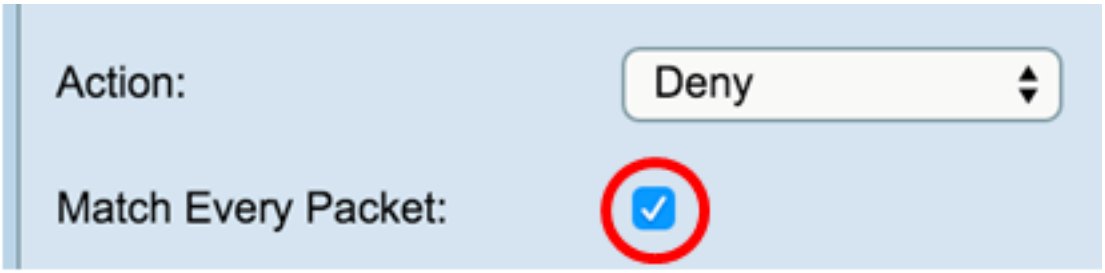


- 거부 — 규칙 기준을 충족하는 모든 트래픽을 차단하여 WAP를 입력하거나 종료합니다.모든 ACL의 끝에 암시적 deny-all 규칙이 있으므로 명시적으로 허용되지 않는 트래픽은 삭제됩니다.
- 허용 — 규칙 기준을 충족하는 모든 트래픽이 WAP에 들어오거나 나갈 수 있습니다.기준을 충족하지 않는 트래픽은 삭제됩니다.

참고:4~11단계는 선택 사항입니다.선택한 필터가 활성화됩니다.이 특정 규칙에 적용하지 않을 필터의 확인란을 선택 취소합니다.

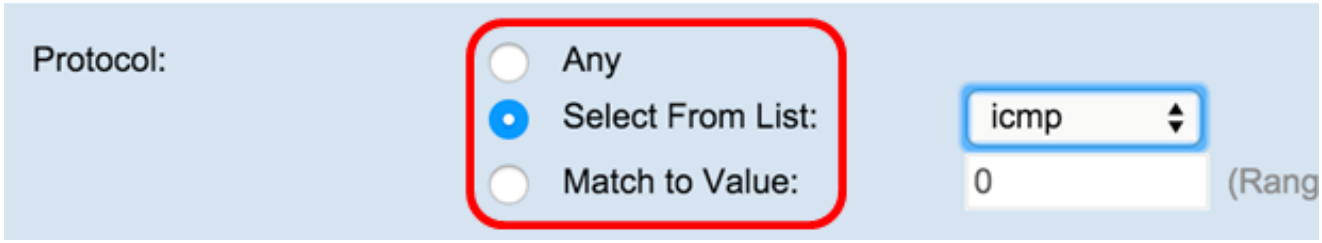
4단계. Match **Every Packet(모든 패킷** 일치) 확인란을 선택하여 해당 내용에 관계없이 모든 프레임 또는 패킷에 대해 규칙을 확인합니다.일치하는 추가 기준을 구성하려면 이 확인란을 선택 취소합니다.

팁: Match Every Packet(모든 패킷 일치)이 이미 선택된 경우 12단계로 건너뜁니다.



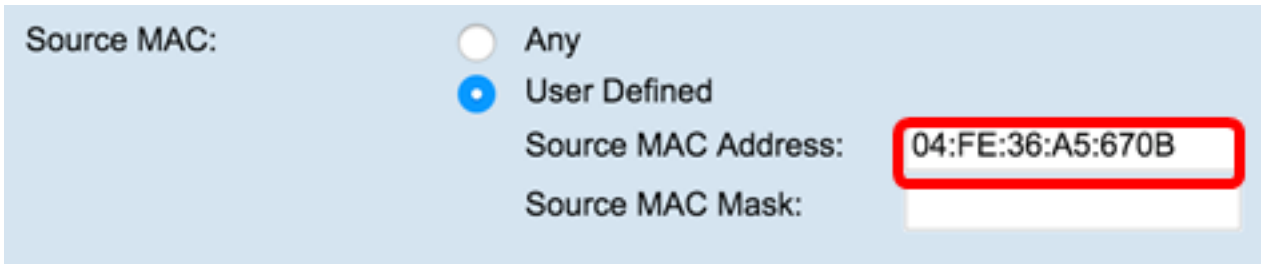
5단계. EtherType 영역에서 라디오 버튼을 선택하여 일치하는 기준을 이더넷 프레임 헤더의 값과 비교합니다.다음 옵션 중 하나를 선택하거나 Any(모두)를 선택할 수 있습니다.

- 목록에서 선택 — 드롭다운 목록에서 프로토콜을 선택합니다.목록에는 다음 옵션이 있습니다.appletalk, arp, IPv4, IPv6, ipx, netbios, pppoe
- 값에 일치 — 사용자 지정 프로토콜 식별자의 경우 0600에서 FFFF까지의 범위를 나타내는 식별자를 입력합니다.



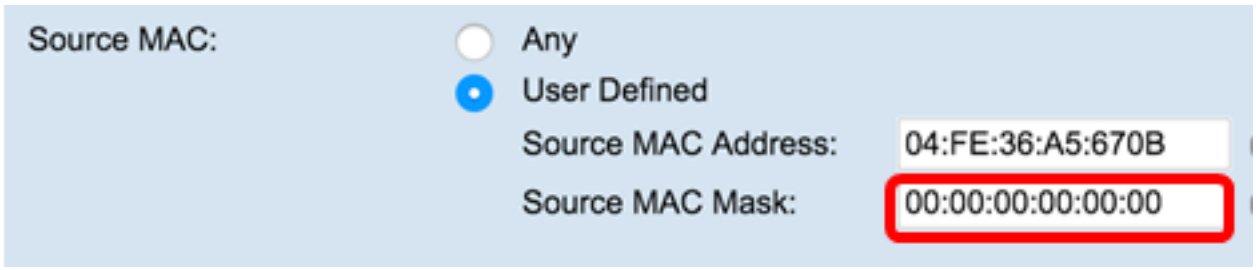
6단계. Class Of Service(서비스 클래스) 영역에서 라디오 버튼을 선택하여 이더넷 프레임과 비교할 802.1p 사용자 우선순위를 입력합니다.Any 또는 User Defined 우선순위를 선택할 수 있습니다.*User Defined* 필드에 0~7의 우선순위를 입력합니다.

7단계. Source MAC 영역에서 라디오 버튼을 선택하여 소스 MAC 주소를 이더넷 프레임과 비교합니다.**Any(모두)**를 선택하거나 **User Defined(사용자 정의)**를 선택하고 제공된 필드에 소스 MAC 주소를 입력할 수 있습니다.

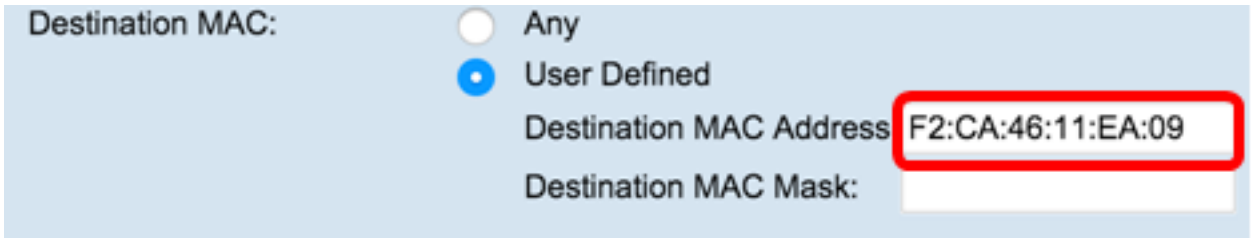


8단계. 소스 MAC의 비트를 이더넷 프레임과 비교할 소스 *MAC*의 비트를 지정하는 소스 MAC 주소 마스크를 Source MAC Mask 필드에 입력합니다.

참고:MAC 마스크가 0비트를 사용하는 경우 주소가 수락되고 1비트를 사용하는 경우 주소가 무시됩니다.

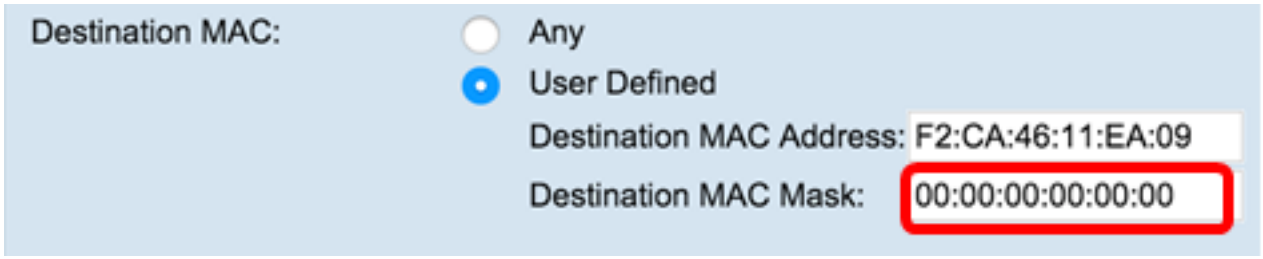


9단계. Destination MAC(대상 MAC) 영역에서 라디오 버튼을 선택하여 대상 MAC 주소를 이더넷 프레임과 비교합니다 .Any(모두)를 선택하거나 User Defined(사용자 정의)를 선택하고 제공된 필드에 대상 MAC 주소를 입력할 수 있습니다.

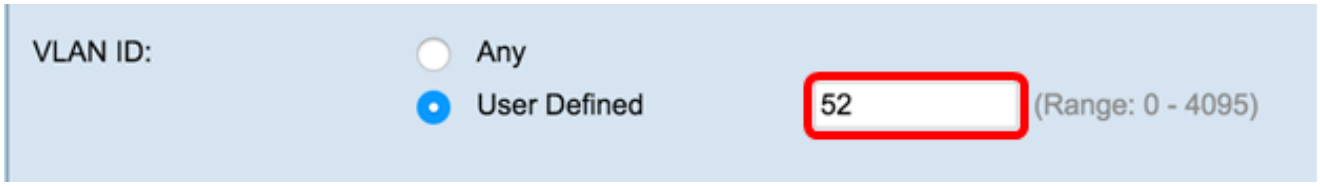


10단계. 대상 MAC의 비트를 이더넷 프레임과 비교할 대상 MAC의 비트를 지정하는 *Destination MAC Mask* 필드에 대상 MAC 주소 마스크를 입력합니다.

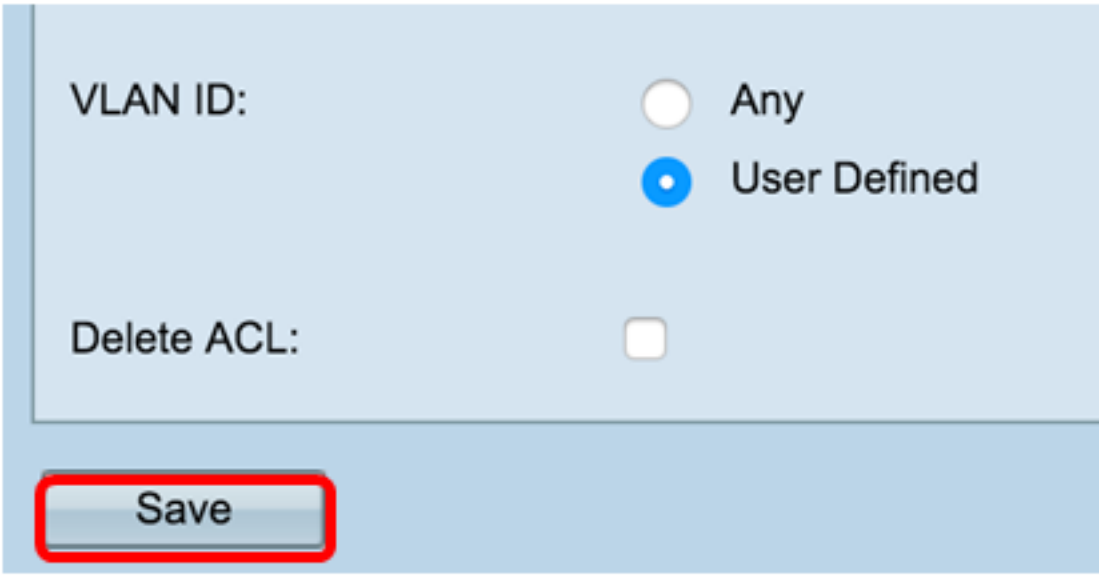
참고:MAC 마스크가 0비트를 사용하는 경우 주소가 수락되고 1비트를 사용하는 경우 주소가 무시됩니다.



11단계. **VLAN ID** 영역에서 라디오 버튼을 선택하여 VLAN ID를 이더넷 프레임과 비교합니다.제공된 필드에 0~4095 범위의 VLAN ID를 입력합니다.



12단계. 저장을 **클릭합니다**.



13단계. (선택 사항) 구성된 ACL을 삭제하려면 **Delete ACL(ACL 삭제)** 확인란을 선택한 다음 Save(저장)를 **클릭합니다**.

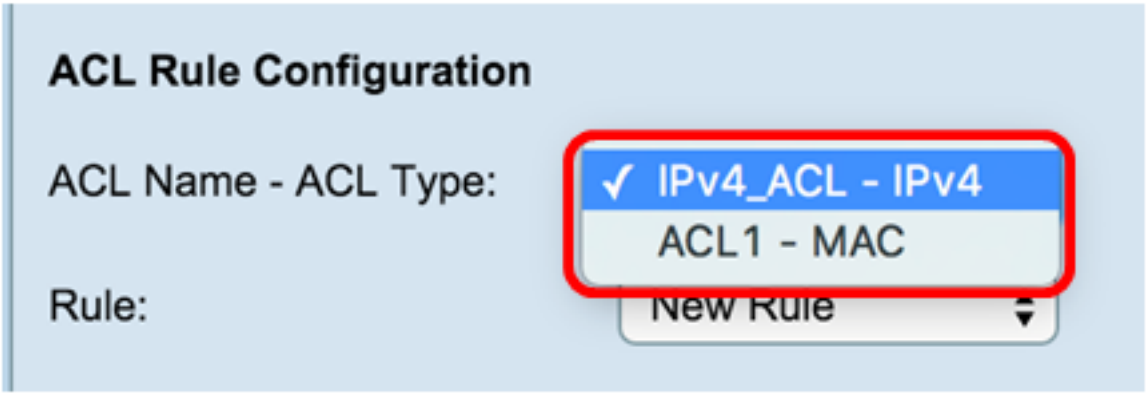
이제 WAP에서 MAC ACL을 성공적으로 구성했어야 합니다.

IPv4 기반 ACL 구성

1. ACL Rule Configuration .

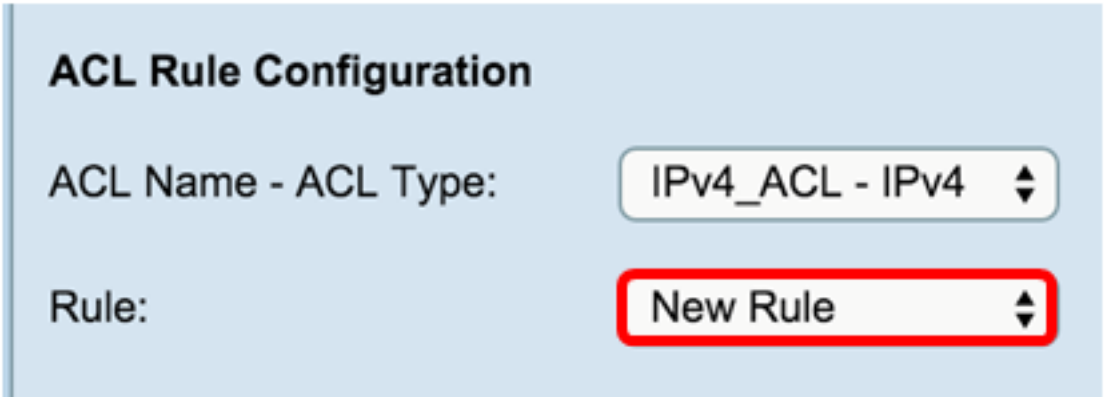
ACL - ACL ACL .

: IPv4_ACL-IPv4 .



2. ACL *Rule* **New Rule**( ) . Rule .

: ACL 10 .



3. Action() ACL .

: Permit .

- — WAP . ACL deny-all .
- — WAP . .

:4~9 . . .

4. Match **Every Packet(**) . .

: Match Every Packet . 11 .

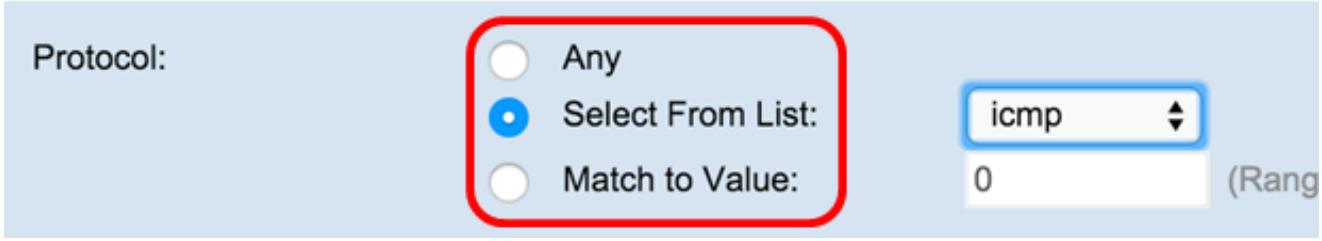
5. Protocol() .Any() .

- — .

— IP — Internet Protocol Suite .
— ICMP — Internet Protocol Suite .

— IGMP — IPv4 .
— TCP — .
— UDP — Internet Protocol Suite .

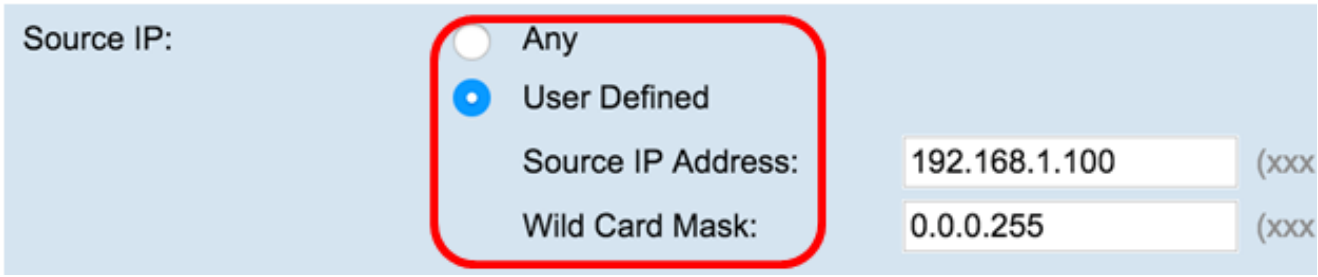
- — 0~255 IANA ID . .



6. Source IP(IP) IP .Any() User Defined( ) IP .

- IP — IP .
- Wild Card Mask( ) — IP . . 255.255.255.255 . 0.0.0.0. Source IP Address(IP) .

: . 0.0.0.0 . 24 (: 192.168.10.0/24) 0.0.0.255 .



7. Source Port( ) .Any .

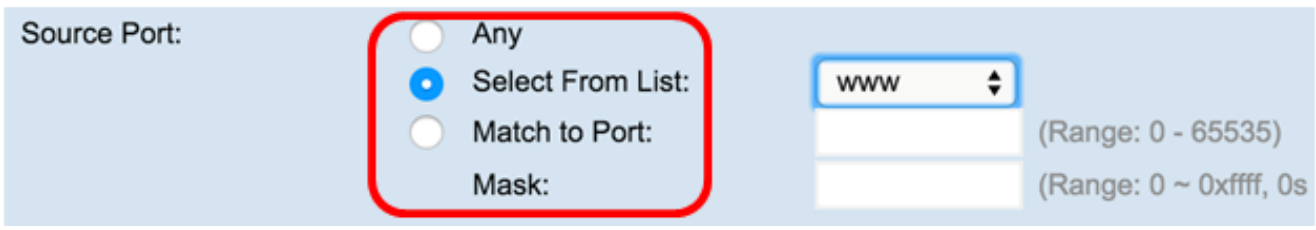
- — . .

— FTP(File Transfer Protocol) — FTP TCP(Transmission Control Protocol) .
— FTP — 20 .
— HTTP(Hypertext Transfer Protocol) — HTTP World Wide Web .
— SMTP(Simple Mail Transfer Protocol) — SMTP () .
— SNMP(Simple Network Management Protocol) — SNMP IP .
— — LAN .
— TFTP(Trivial File Transfer Protocol) — TFTP FTP .
— World Wide Web(WWW) — WWW HTTP .

- Match to Port( ) - . Match to *Port* 0~65535. 3 .

— 0~1023 —
— 1024~49151 —
— 49152~65535 — /

- — . .16(0 - 0xFFFF) .0 1 .

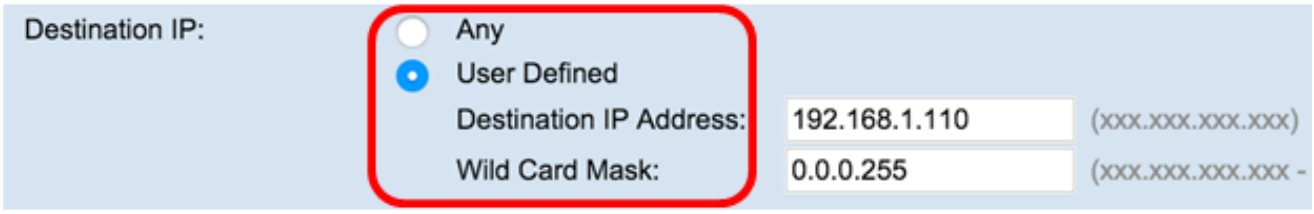


8. Destination IP(IP) IP .Any() User Defined( ) IP .

- IP — IP .

- Wild Card Mask( ) — IP . . 255.255.255.255 . 0.0.0.0. IP .

: . 0.0.0.0 . 24 (: 192.168.10.0/24) 0.0.0.255 .



9. Destination Port( ) .Any() .

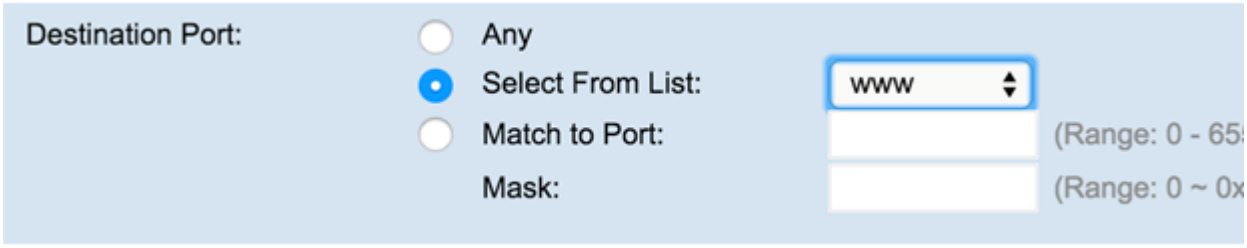
- — .

— FTP — TCP .
— FTP — 20 .
— HTTP — World Wide Web .
— SMTP — () .
— SNMP — IP .
— — LAN .
— TFTP — FTP .
— WWW — HTTP .

- Match to Port( ) - . Match to *Port* 0~65535. 3 . .

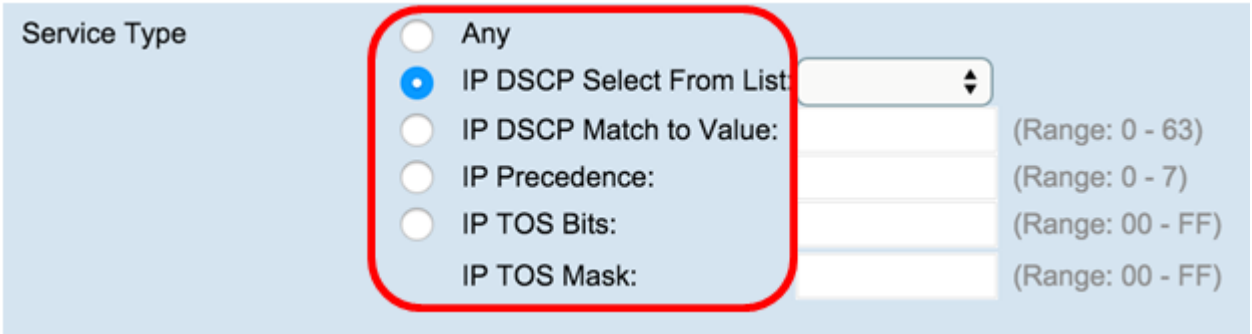
— 0~1023 —
— 1024~49151 —
— 49152~65535 — /

- — . .16(0-0xFFFF) .0 1 .

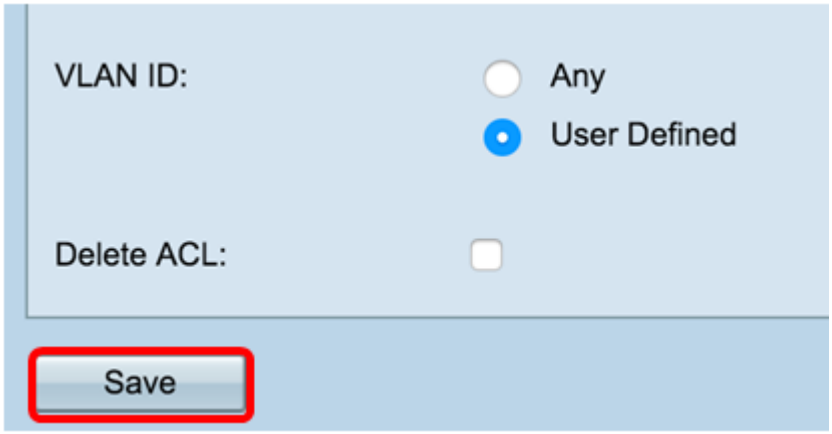


10. Service Type( ) .Any() .

- IP DSCP Select From List — DSCP(Differentiated Services Code Point) AS(Assured Forwarding), CS(Class of Service) EF(Raped Forwarding) .
- IP DSCP Match to Value — DSCP . 0~63 .
- IP Precedence — IP . 0~7 IP .
- IP TOS Bits — IP TOS .
- IP TOS IP 8 8 .IP TOS Bits 00 ff 2 16. 3 IP . 6 IP DSCP .
- IP TOS Mask — IP TOS Mask IP TOS IP TOS .
- IP TOS Mask 00 FF 16, (,) .IP TOS 0 IP TOS IP TOS . , 7 5 1 IP TOS 7 IP TOS 0 IP TOS 00 .



11. .



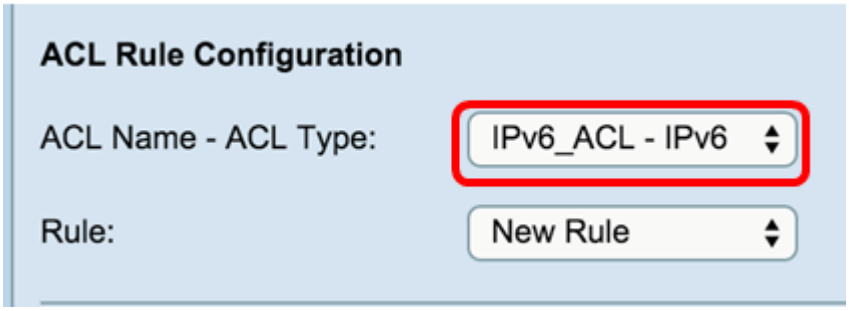
IPv4 ACL .

IPv6 기반 ACL 구성

1. ACL Rule Configuration .

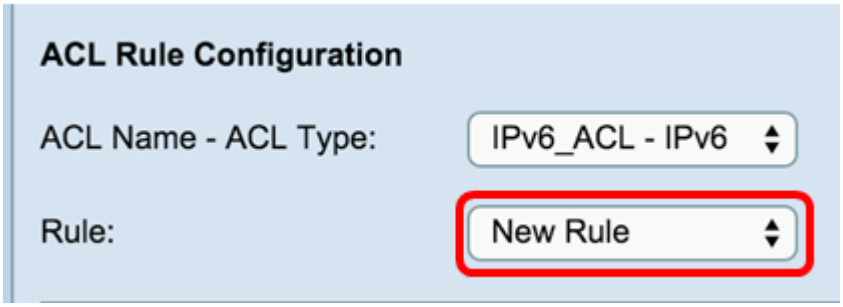
ACL - ACL — ACL .

: IPv6_ACL — Pv6 .



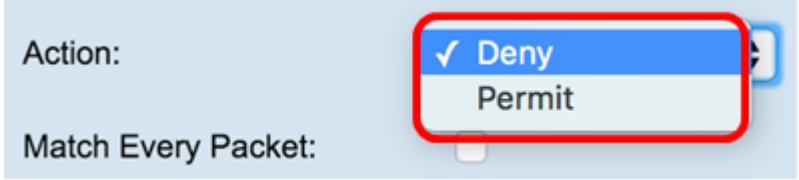
2. ACL Rule New Rule . Rule .

: ACL 10 .



3. Action() ACL .

- — WAP . ACL deny-all .
- — WAP . .



:4~11 . . .

4. Match *Every Packet(*) . .

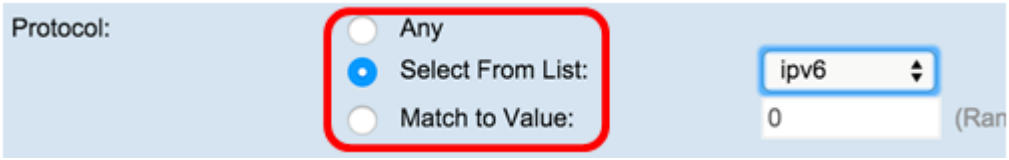
:Match Every Packet . 12 .

5. Protocol() . Any() .

- — .

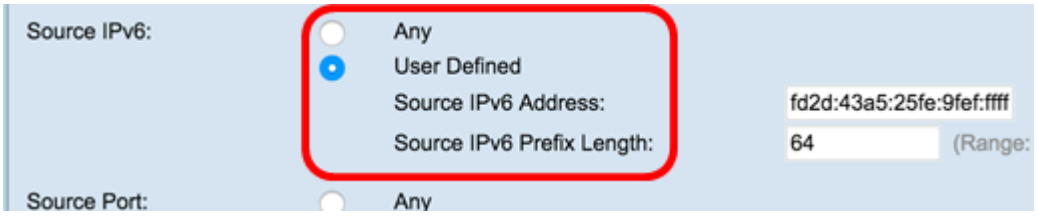
— IP — Internet Protocol Suite .
— ICMP — Internet Protocol Suite .
— IGMP — IPv4 .
— TCP — .
— UDP — Internet Protocol Suite .

- — 0~255 IANA ID . .



6. Source IPv6(IPv6) IP .Any() User Defined( ) IPv6 IPv6 Prefix Length(IPv6) .

- IPv6 — IPv6 .
- IPv6 — IPv6 .



7. Source *Port(*) .Any() .

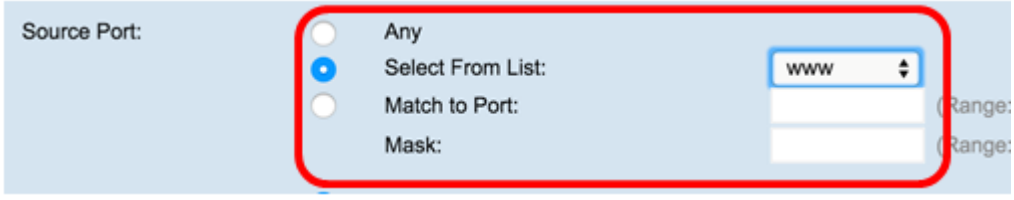
- — . .

— FTP — TCP .
— FTP — 20 .
— HTTP — World Wide Web .
— SMTP — () .
— SNMP — IP .
— — LAN .
— TFTP — FTP .
— WWW — HTTP .

- Match to Port( ) - . Match to *Port* 0~65535. 3 . .

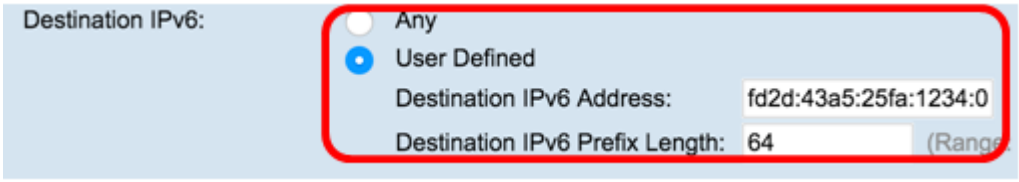
— 0~1023 —
— 1024~49151 —
— 49152~65535 — /

- — . .16(0 xFFFF) .0 1 .



8. Destination IPv6(IPv6) IP .Any() User Defined( ) IPv6 Destination IPv6 Prefix Length(IPv6) .

- IPv6 — IPv6 .
- IPv6 — IPv6 .

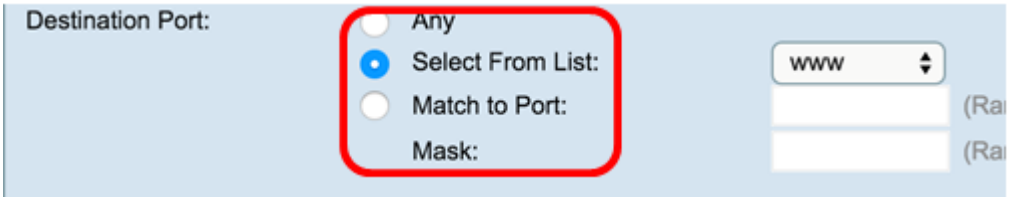


9. Destination Port( ) .Any() .

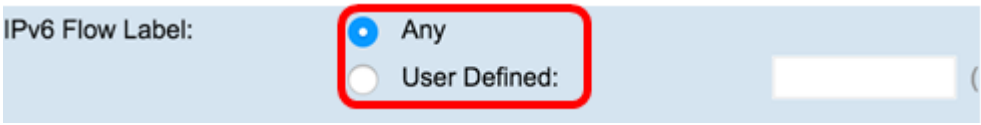
- — . FTP, FTP , HTTP, SNMP, SMTP, TFTP, , WWW.
- Match to Port( ) - . Match to *Port* 0~65535. 3 . .

— 0~1023 —
— 1024~49151 —
— 49152~65535 — /

- — . .16(0-0xFFFF) .0 1 .

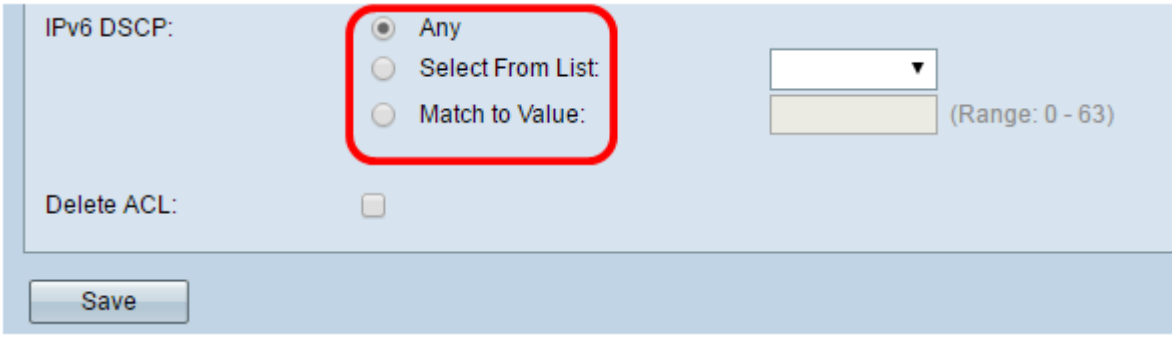


10. IPv6 Flow Label(IPv6) IPv6 .Any() User Defined( ) IPv6 20 . 0~0xffff.

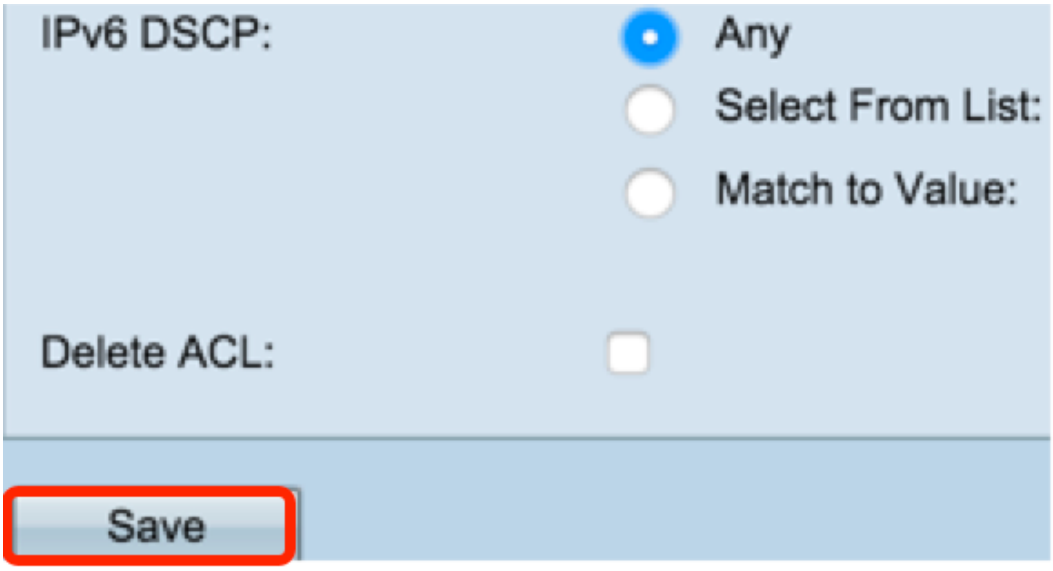


11. IPv6 DSCP IP DSCP .Any() .

- — .DSCP AF(Assured Forwarding), CS(Class of Service) EF(Raped Forwarding).
- Match to Value( ) - 0 63 DSCP .



12. Save() .



13. ( ) ACL ACL Name-ACL Type(ACL -ACL) ACL Delete ACL(ACL) .

IPv6 ACL .