WAP121 및 WAP321 액세스 포인트에서 IPv6 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.액세스 제어 목록에는 네트워크 디바이스에 대한 액세스가 허용되거나 거부된 호스트가 포함됩니다.QoS 기능에는 정의된 홉별 동작에 따라 트래픽을 스트림으로 분류하고 특정 QoS 처리를 허용하는 DiffServ(Differentiated Services) 지원이 포함되어 있습니다.

이 문서에서는 WAP121 및 WAP321 액세스 포인트에서 IPv6 ACL을 생성하고 구성하는 방법에 대해 설명합니다.

적용 가능한 디바이스

·WAP121
· WAP321

소프트웨어 버전

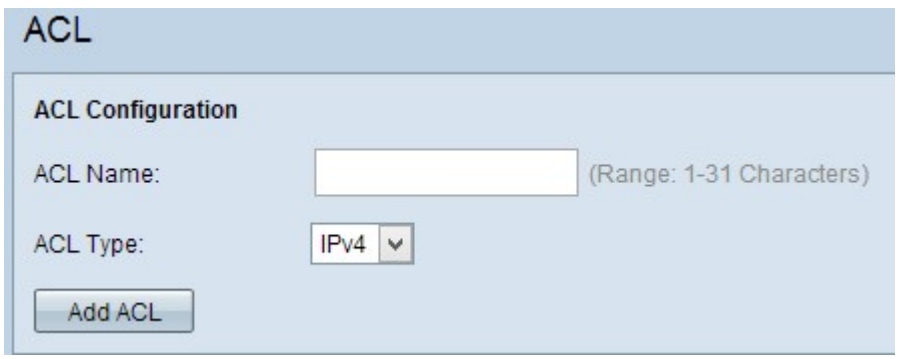
·v1.0.3.4

IPv6 기반 ACL 컨피그레이션

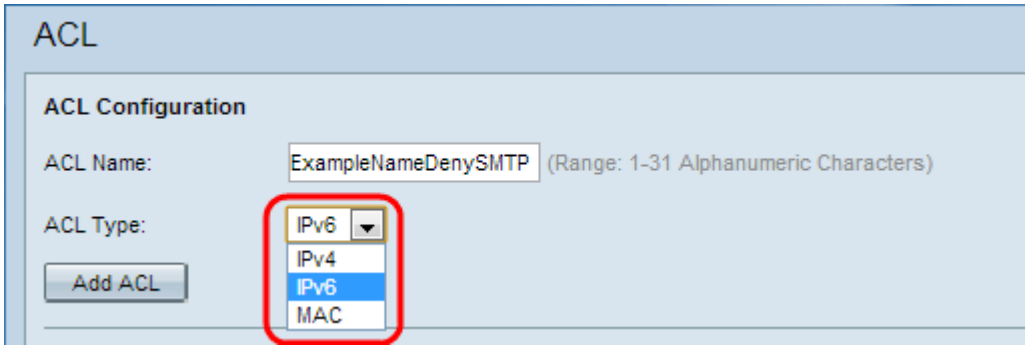
IP ACL은 IP 스택의 레이어 3에 대한 트래픽을 분류합니다.각 ACL은 무선 클라이언트에서 전송되거나 무선 클라이언트에서 수신되는 트래픽에 적용되는 최대 10개의 규칙 집합입니다.각 규칙은 지정된 필드의 내용을 사용하여 네트워크에 대한 액세스를 허용할지 또는 거부할지를 지정합니다.규칙은 다양한 기준을 기반으로 할 수 있으며, 소스 또는 목적지 IP 주소, 소스 또는 목적지 포트 또는 패킷에 포함된 프로토콜과 같은 패킷 내의 하나 이상의 필드에 적용할 수 있습니다.

IPv6 ACL 생성

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



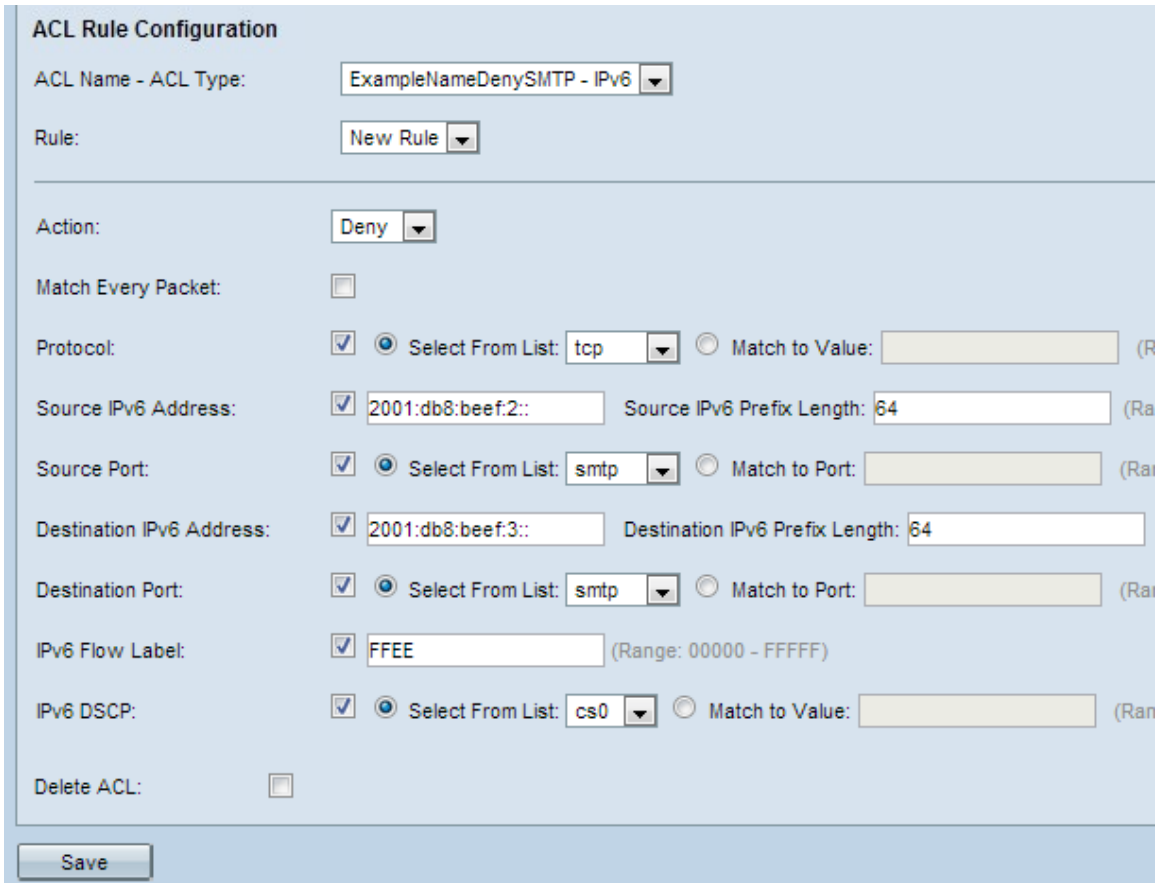
2단계. *ACL 이름* 필드에 ACL의 이름을 입력합니다.



3단계. *ACL Type* 드롭다운 목록에서 ACL의 IPv6 유형을 선택합니다.

4단계. **Add ACL(ACL 추가)**을 클릭하여 새 IPv6 ACL을 생성합니다.

IPv6 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 하나를 선택합니다.

참고:단일 ACL에 대해 최대 10개의 규칙을 생성할 수 있습니다.

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

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

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

주의:허용 또는 거부가 선택된 경우 항상 모든 규칙의 끝에 암시적 거부가 있기 때문에 허용 규칙을 추가해야 합니다.

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

시간 절약: Match *Every Packet(모든 패킷 일치)* 확인란을 선택한 경우 12단계로 건너뜁니다.

5단계. IPv6 패킷의 *IP Protocol* 필드 값을 기반으로 L3 또는 L4(IP 스택의 네트워크 및 전송 계층) 프로토콜 일치 조건을 활성화하려면 Protocol(*프로토콜*) 확인란을 선택합니다 .Protocol(프로토콜) 확인란을 선택한 경우 이러한 라디오 버튼 중 하나를 클릭합니다.

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

·Match to Value(값에 일치) - 목록에 없는 프로토콜의 경우표준 IANA 할당 프로토콜 ID 범위를 0~255까지 입력합니다.

6단계. 소스*의* IP 주소를 일치 조건에 포함하려면 소스 IPv*6* 주소 확인란을 선택합니다.상대 필드에 소스의 IPv6 주소 및 IPv6 접두사 길이를 입력합니다.

7단계. *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 입력하고 세 가지 유형의 포트를 포함합니다.

- 0~1023 — 잘 알려진 포트서버 프로세스에서 연결 포트로 사용하는 포트입니다.연결 포트는 잘 알려진 포트라고도 합니다.

- 1024~49151 — 등록된 포트.특정 프로토콜 또는 애플리케이션에 사용되는 네트워크 포트입니다.

- 49152~65535 — 동적 및/또는 전용 포트동적 포트는 IANA와 같은 관리 기관에서 관리하지 않으며 특별한 사용 제한이 없습니다.

8단계. 대상 *IPv6* 주소 확인란을 선택하여 일치 조건에 대상의 IP 주소를 포함합니다.상대 필드에 대상의 IPv6 주소 및 IPv6 접두사 길이를 입력합니다.

9단계. *Destination Port(대상 포트*) 확인란을 선택하여 일치 조건에 대상 포트를 포함합니다 .Destination Port(대상 포트) 확인란을 선택한 경우 이러한 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 경우0~65535 범위의 포트 번호를 입력하고 세 가지 유형의 포트를 포함합니다.

- 0~1023 — 잘 알려진 포트

- 1024~49151 — 등록된 포트.

- 49152~65535 — 동적 및/또는 전용 포트

10단계. IPv6 플로우 레이블 확인란을 선택하여 일치 조건에 IPv6 플로우 레이블을 포함합니다.IPv6 헤더의 20비트 플로우 레이블 필드는 소스에서 같은 흐름에 속하는 패킷 집합에 레이블을 지정하기 위해 사용할 수 있습니다.IPv6 Flow 레이블 필드에 0000~FFFFF의 범위를 입력합니다.

11단계. *IP DSCP* 확인란을 선택하여 일치 조건에 IP DSCP 값을 포함합니다.IP DSCP 확인란을 선택한 경우 이러한 라디오 버튼 중 하나를 클릭합니다.

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

·값에 일치 — 0~63 범위의 DSCP 값을 사용자 지정합니다.

12단계(선택 사항) 구성된 ACL을 삭제하려면 *Delete ACL(ACL 삭제)* 확인란**을** 선택합니다.

13단계. **저장**을 클릭하여 설정을 저장합니다.