대상 ACL 제한이 있는 RV34x 라우터의 VLAN 간 라우팅

목표

이 문서에서는 특정 트래픽을 제한하기 위해 RV34x Series 라우터에서 VLAN(Inter-Virtual Local Area Network) 라우팅을 대상 ACL(Access Control List)과 함께 구성하는 방법에 대해 설명합니다 .트래픽은 IP 주소, 주소 그룹 또는 프로토콜 유형별로 제한할 수 있습니다.

소개

VLAN은 훌륭하며 레이어 2 네트워크에서 브로드캐스트 도메인을 정의합니다.일반적으로 브로드캐스트 도메인은 라우터가 브로드캐스트 프레임을 전달하지 않으므로 라우터로 제한됩니다.레이어 2 스위치는 스위치의 컨피그레이션을 기반으로 브로드캐스트 도메인을 생성합니다.트래픽은 스위치 내의 다른 VLAN(브로드캐스트 도메인 간) 또는 두 스위치 간에 직접 전달될 수 없습니다 .VLAN을 사용하면 서로 다른 부서를 서로 독립적으로 유지할 수 있습니다.예를 들어, 영업 부서가 회계 부서와 어떠한 관여도 하지 않도록 할 수 있습니다.

독립성은 환상적입니다. 그러나 VLAN의 최종 사용자가 서로 라우팅할 수 있게 하려면 어떻게 해야 합니까?판매 부서는 레코드나 작업표를 회계 부서에 제출해야 할 수 있습니다.회계 부서는 급여나 세일즈 수치에 대한 알림을 세일즈 팀에 보낼 수 있습니다.즉, VLAN 간 라우팅으로 하루를 절약할 수 있습니다!

VLAN 간 통신에는 일반적으로 라우터인 OSI(Open Systems Interconnections) 레이어 3 디바이스가 필요합니다.이 레이어 3 디바이스는 각 VLAN 인터페이스에 IP(Internet Protocol) 주소가 있어야 하며 각 IP 서브넷에 연결된 경로가 있어야 합니다.그런 다음 각 IP 서브넷의 호스트는 각 VLAN 인터페이스 IP 주소를 기본 게이트웨이로 사용하도록 구성할 수 있습니다.구성된 후에는 최종 사용자가 다른 VLAN의 최종 사용자에게 메시지를 보낼 수 있습니다.완벽할 것 같지?

하지만 잠깐, 경리부의 서버는 어떤가요?해당 서버에 보호된 상태로 유지해야 하는 중요한 정보가 있습니다.두려워하지 말고, 그것에 대한 해결책도 있습니다!RV34x Series 라우터의 액세스 규칙 또는 정책을 사용하면 규칙을 구성하여 네트워크의 보안을 강화할 수 있습니다.ACL은 특정 사용자로부터 트래픽을 보내거나 받는 것을 차단하거나 허용하는 목록입니다.액세스 규칙은 항상 적용되도록 구성하거나 정의된 일정에 따라 구성할 수 있습니다.

이 문서에서는 두 번째 VLAN, VLAN 간 라우팅 및 ACL을 구성하는 단계를 안내합니다.

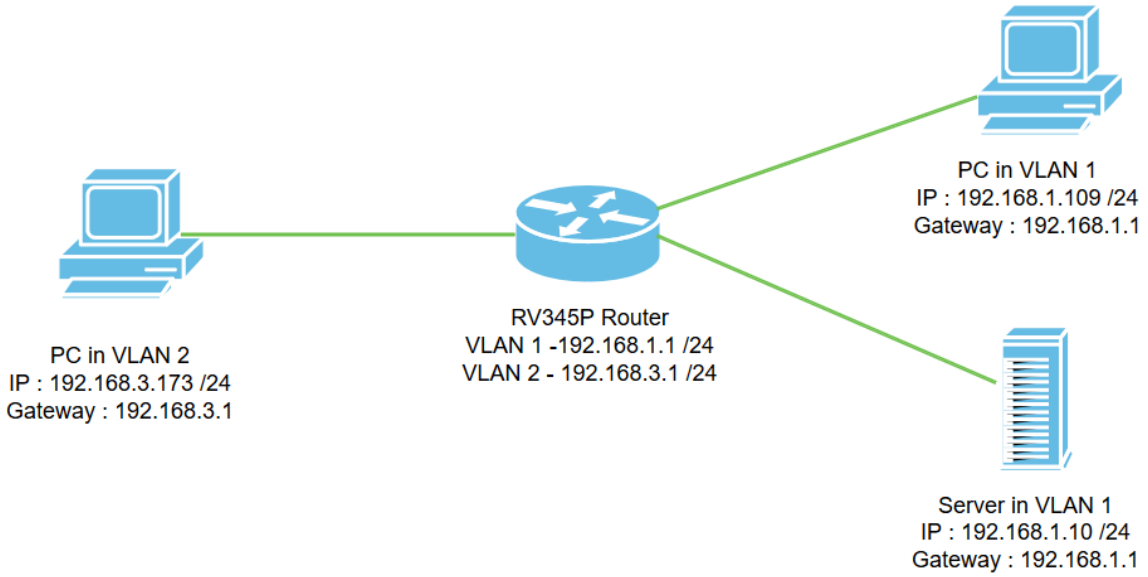
적용 가능한 디바이스

- RV340
- RV340W
- RV345
- RV345P

소프트웨어 버전

- 1.0.03.16

토폴로지



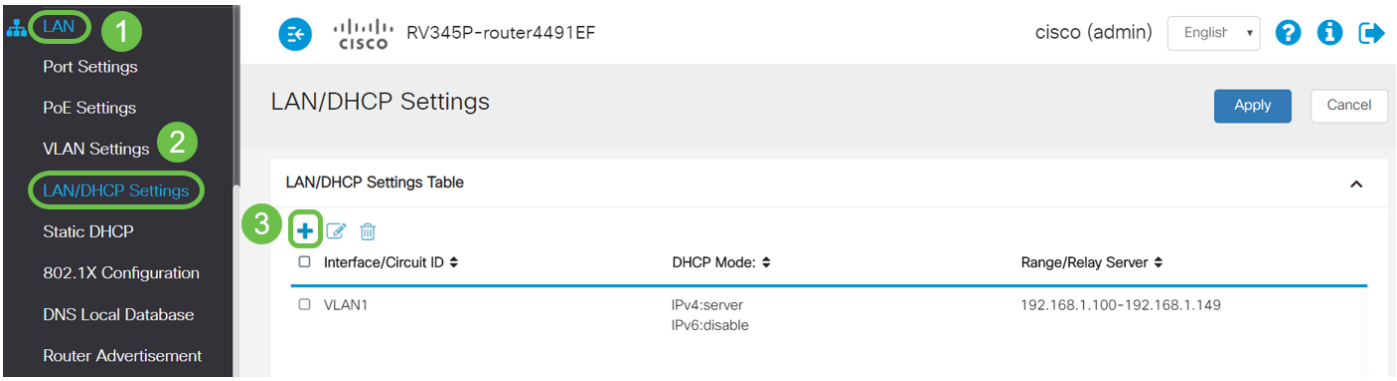
이 시나리오에서는 VLAN1과 VLAN2에 대해 VLAN 간 라우팅이 활성화되므로 이러한 VLAN의 사용자가 서로 통신할 수 있습니다.보안상의 측면으로 VLAN2 사용자가 VLAN1 서버[IPv4(Internet Protocol version 4))에 액세스하지 못하게 합니다.192.168.1.10 /24].

사용된 라우터 포트:

- VLAN1의 PC(Personal Computer)가 *LAN1* 포트에 연결됩니다.
- VLAN2의 PC(Personal Computer)가 *LAN2* 포트에 연결됩니다.
- VLAN1의 서버는 *LAN3* 포트에 연결됩니다.

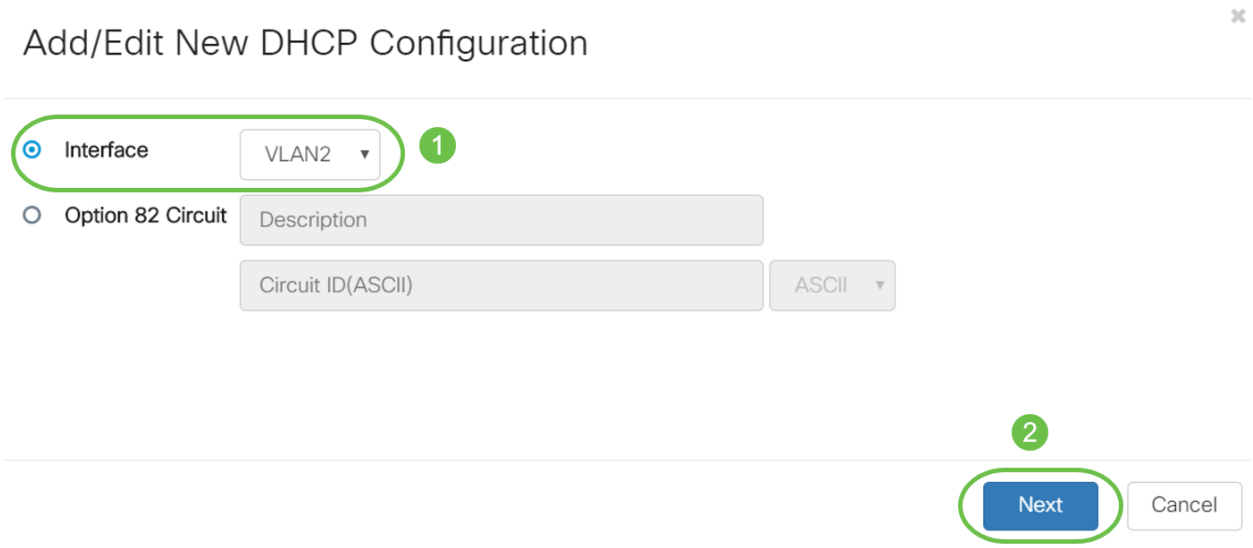
구성

1단계. 라우터의 웹 구성 유틸리티에 로그인합니다.라우터에 새 VLAN 인터페이스를 추가하려면 **LAN > LAN/DHCP Settings(LAN/DHCP 설정)**로 이동하고 *LAN/DHCP Settings(LAN/DHCP 설정) 테이블*에서 **더하기 아이콘**을 클릭합니다.

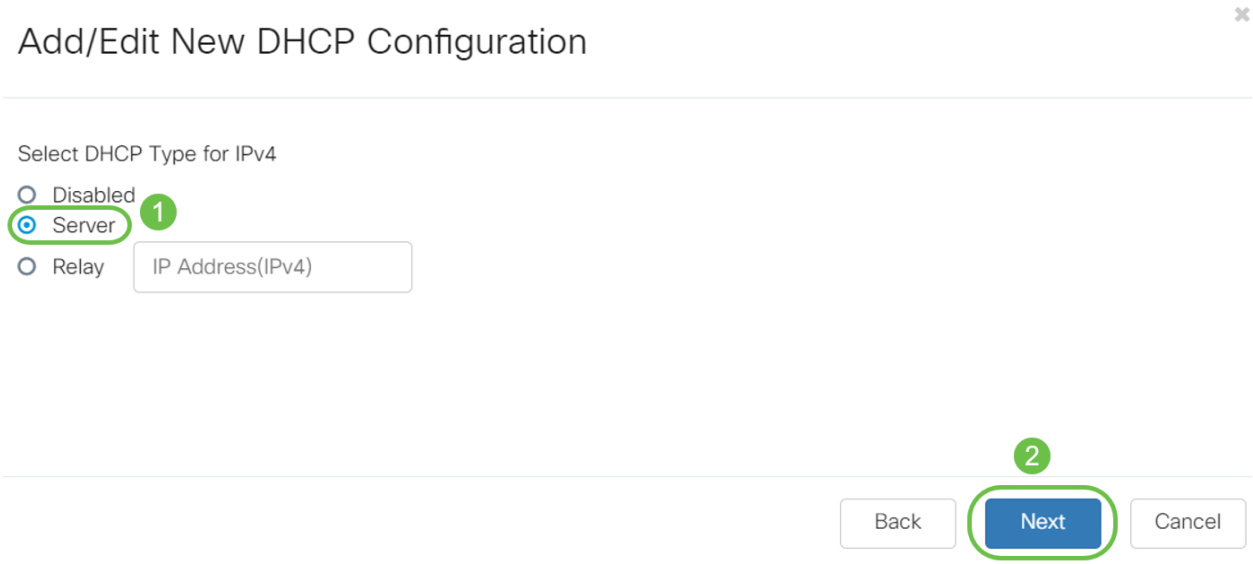


참고:VLAN1 인터페이스는 기본적으로 RV34x 라우터에서 생성되고 IPv4용 DHCP(Dynamic Host Configuration Protocol) 서버가 활성화됩니다.

2단계. 새 팝업 창이 열리고 *VLAN2* **인터페이스**가 선택되며 **Next**(다음)를 클릭합니다.



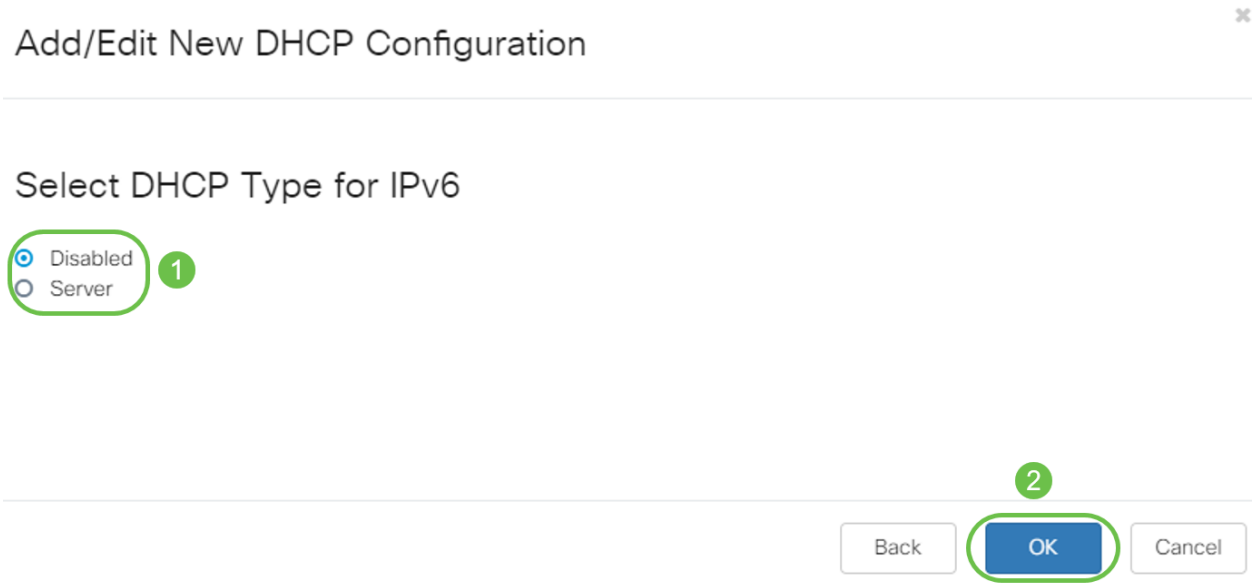
3단계. VLAN2 인터페이스에서 DHCP 서버를 활성화하려면 Select DHCP Type for IPv*4(IPv4의 DHCP 유형 선택)에서 Server(*서버)**를** 선택합니다.Next(**다음)를 클릭합니다**.



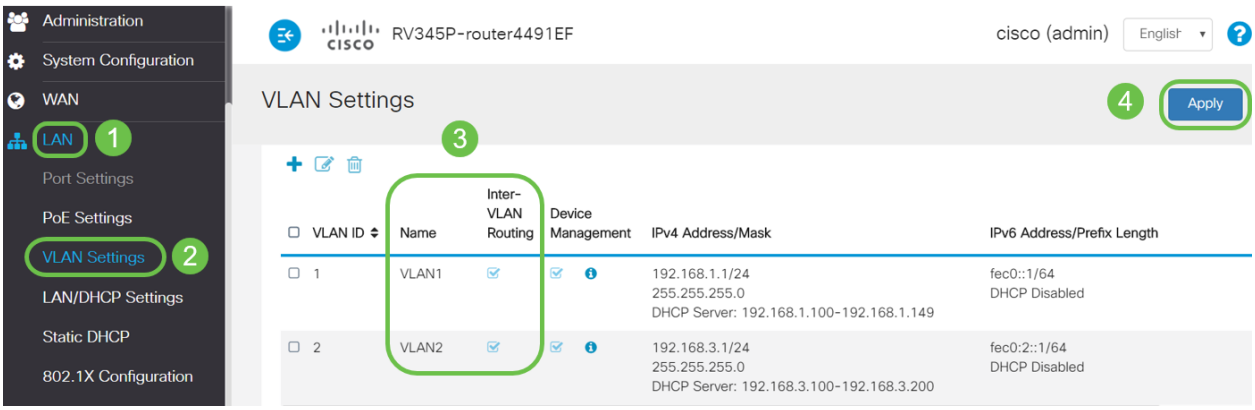
4단계. *클라이언트 리스 시간, 범위 시작, 범위 끝* 및 *DNS 서버*를 포함한 DHCP 서버 구성 매개 변수*를 입력합니다*.Next(**다음)를 클릭합니다**.

5단계. (선택 사항) IPv4를 기반으로 하므로 *Disabled* 확인란을 선택하여 IPv*6*에 *대한 DHCP 유형*을 비활성화할 수 있습니다. **OK**를 클릭합니다.DHCP 서버 구성이 완료되었습니다.

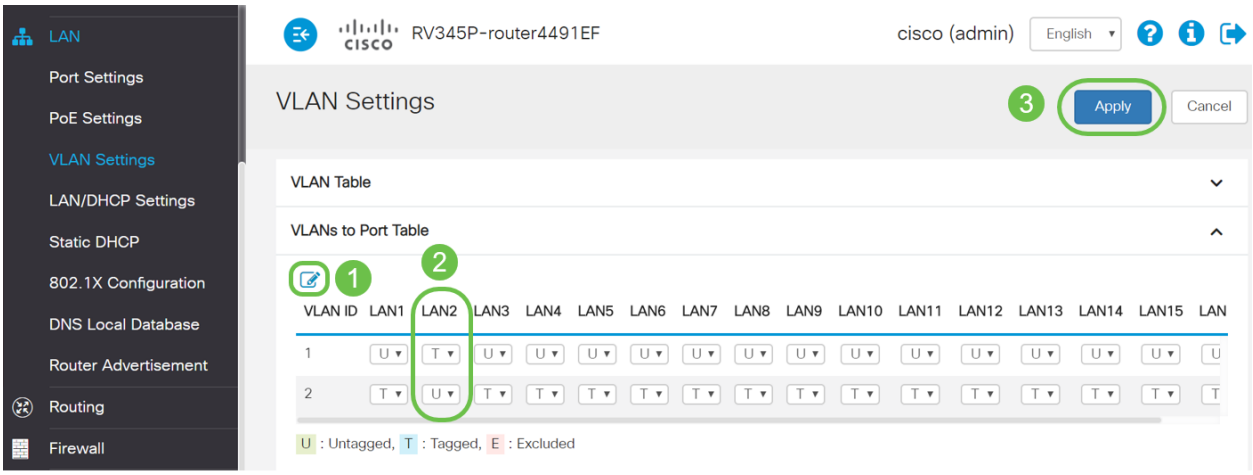
참고:IPv6를 사용할 수 있습니다.



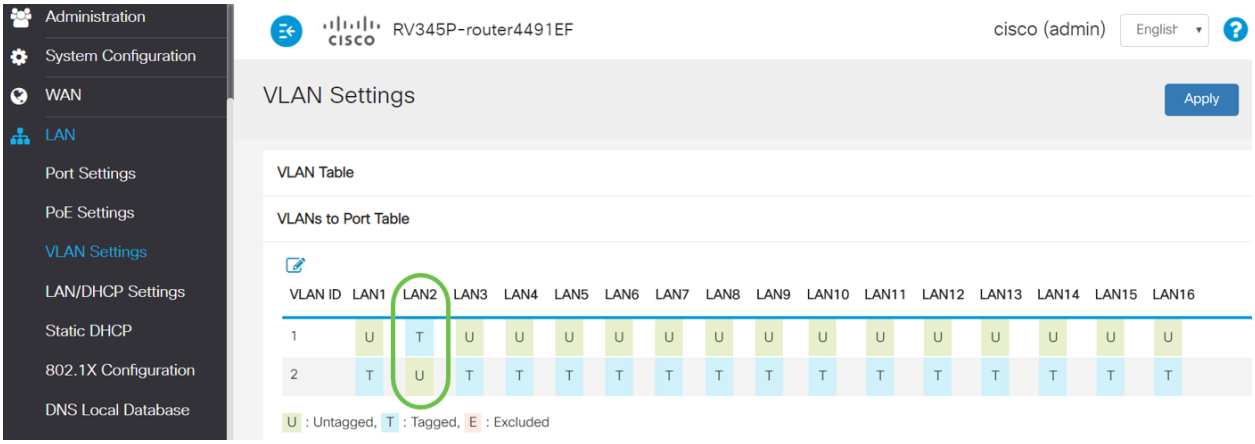
6단계. **LAN > VLAN 설정**으로 이동하고 VLAN, VLAN1 및 VLAN2 모두에 대해 VLAN *간 라우팅*이 활성화되었는지 확인합니다. 이 컨피그레이션을 통해 두 VLAN 간의 통신이 활성화됩니다.Apply를 **클릭합니다**.



7단계. *LAN2* 포트에서 VLAN2에 대해 태그 없는 트래픽을 할당하려면 *VLANs to Port Table* 옵션 아래*의* 수정 버튼을 클릭합니다.이제 *LAN2* 포트에서 *드롭다운 메뉴*에서 VLAN*2*에 대한 **T** (Tagged) 옵션과 VLAN1의 **U**(Untagged*) 옵션을 선택합니다*.Apply(**적용**)를 클릭하여 컨피그레이션을 저장합니다.이 컨피그레이션은 LAN2 포트의 VLAN2에 대한 태그 없는 트래픽을 전달하여 일반적으로 VLAN 태깅을 지원하지 않는 PC NIC(Network Interface Card)가 VLAN2에서 DHCP IP를 가져오고 VLAN2의 일부가 되도록 합니다.

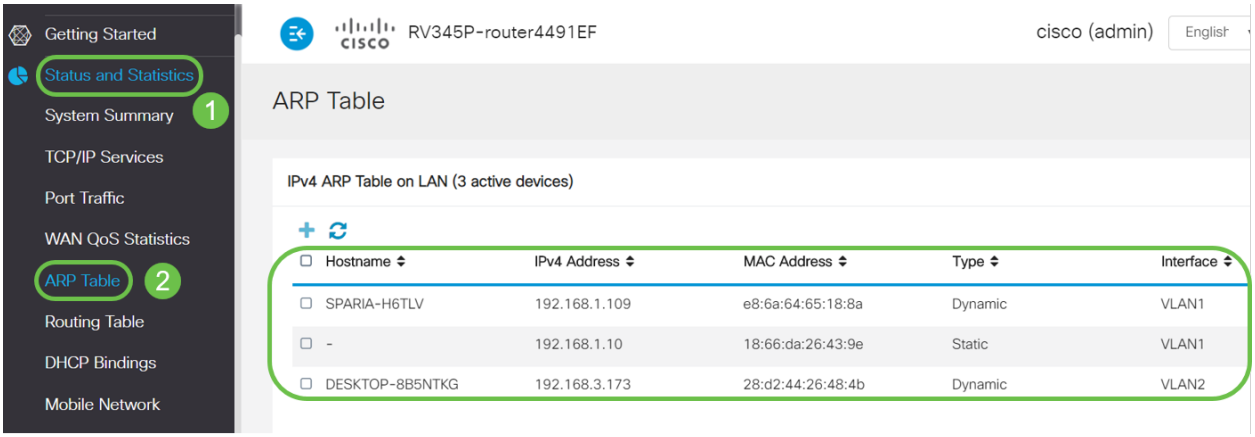


8단계. *LAN2* 포트에 대한 VLAN2 설정이 U*(태그 없음)로 표시되는지 확인합니다*. 나머지 LAN 포트의 VLAN2 설정은 *T(Tagged)* 및 VLAN1 트래픽은 *U(Untagged)가 됩니다*.

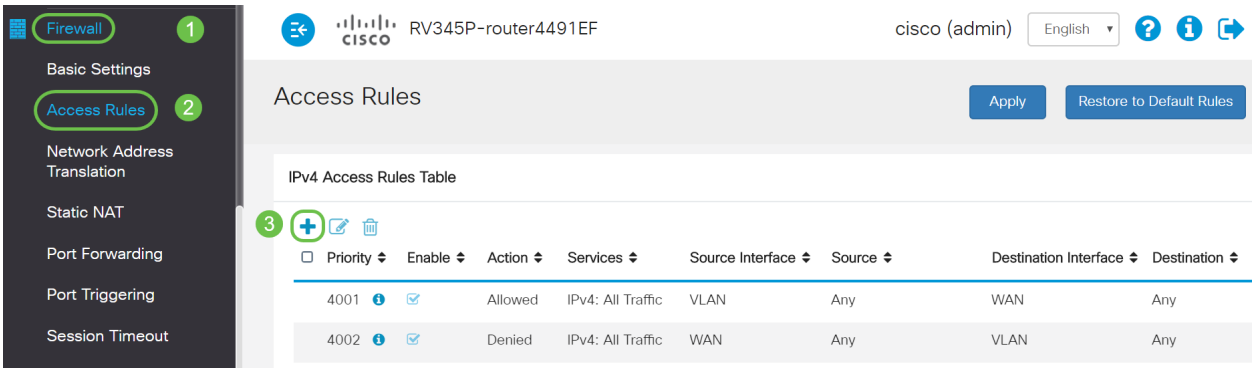


9단계. Status **and Statistics(상태 및 통계) > ARP Table(ARP 테이블**)으로 이동하고 PC에 대한 동적 *IPv4* 주소가 서로 다른 VLAN에 있는지 확인합니다.

참고:VLAN1의 서버 IP가 정적으로 할당되었습니다.



10단계. ACL을 적용하여 서버를 제한합니다(IPv4:192.168.1.10/24) VLAN2 사용자로부터의 액세스ACL을 구성하려면 **Firewall(방화벽) > Access Rules(액세스 규칙**)로 이동하고 **더하기 아이콘**을 클릭하여 새 규칙을 추가합니다.



11단계. *액세스 규칙* 매개변수를 구성합니다.이 시나리오의 매개변수는 다음과 같습니다.

규칙 상태:사용

작업:거부

서비스:모든 트래픽

로그:참

소스 인터페이스:VLAN2

소스 주소:모두

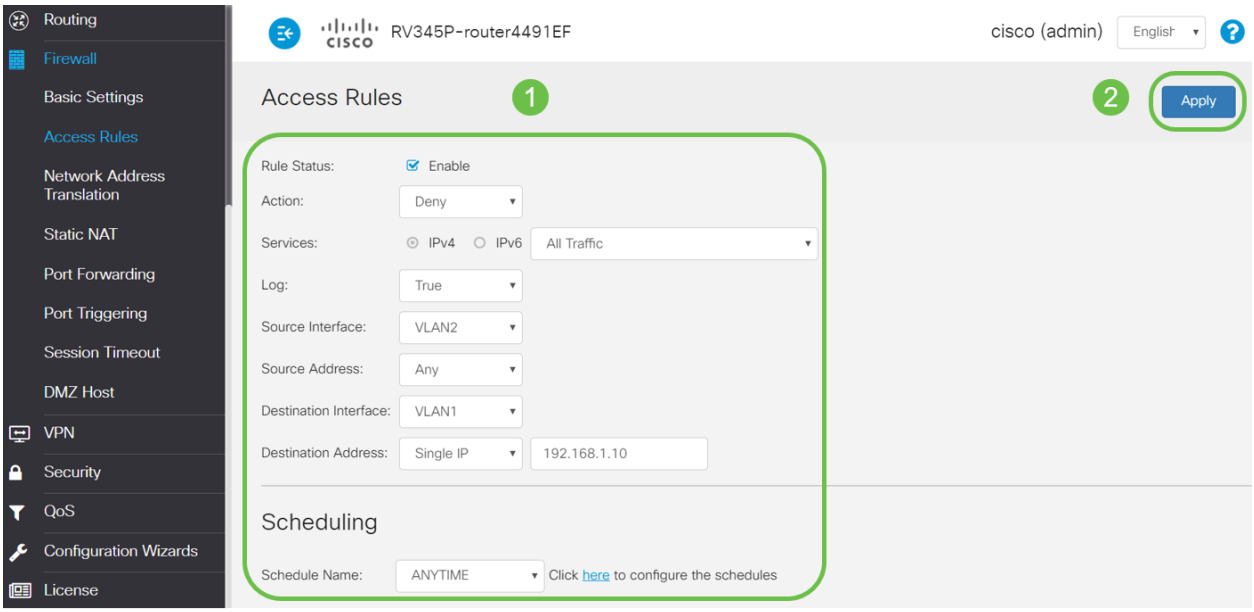
대상 인터페이스:VLAN1

대상 주소:단일 IP 192.168.1.10

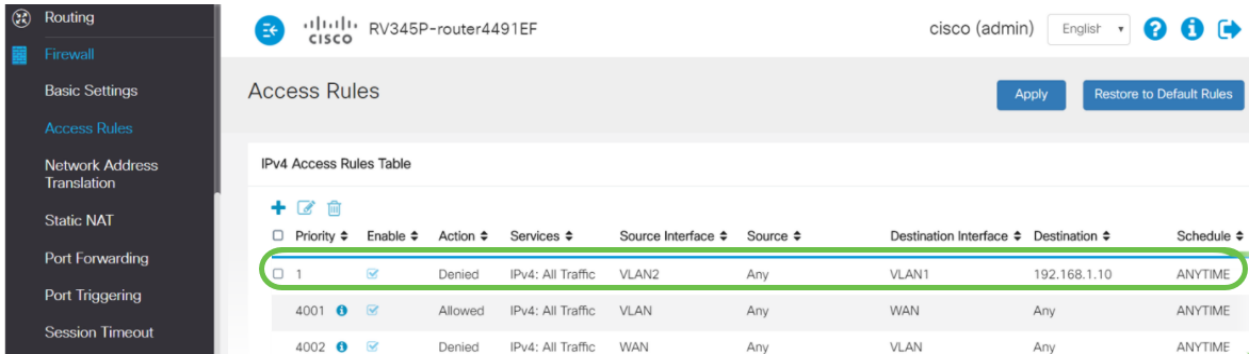
일정 이름:언제든지

Apply를 **클릭합니다**.

참고:이 예에서는 VLAN2에서 서버로의 모든 디바이스에 대한 액세스를 거부한 다음 VLAN1의 다른 디바이스에 대한 액세스를 허용합니다. 사용자의 요구 사항은 다를 수 있습니다.



12단계. *액세스 규칙* 목록은 다음과 같이 표시됩니다.



액세스 규칙은 VLAN2 사용자로부터의 서버 192.168.1.10 액세스를 제한하기 위해 명시적으로 정의됩니다.

확인

서비스를 확인하려면 명령 프롬프트를 엽니다.Windows 플랫폼에서는 Windows 단추를 클릭한 다음 컴퓨터의 왼쪽 아래 검색 상자에 **cmd**를 입력한 다음 메뉴에서 **명령 프롬프트**를 선택하여 이 작업을 수행할 수 있습니다.

다음 명령을 입력합니다.

- VLAN2의 PC(192.168.3.173)에서 서버(IP:192.168.1.10). 통신이 허용되지 *않는다는* 의미인 *요청 시간 초과* 알림을 받게 됩니다.
- VLAN2의 PC(192.168.3.173)에서 VLAN1의 다른 PC(192.168.1.109)을 ping합니다. 성공적으로 회신하게 됩니다.

```
C:\Users\Cisco>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Cisco>ping 192.168.1.109

Pinging 192.168.1.109 with 32 bytes of data:
Reply from 192.168.1.109: bytes=32 time=1ms TTL=127
Reply from 192.168.1.109: bytes=32 time<1ms TTL=127
Reply from 192.168.1.109: bytes=32 time=1ms TTL=127
Reply from 192.168.1.109: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.1.109:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Cisco>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::249b:cf42:b4fc:384f%20
   IPv4 Address. . . . . . . . . . . : 192.168.3.173
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.3.1
```

결론

RV34x 시리즈 라우터에서 VLAN 간 라우팅을 구성하는 데 필요한 단계와 대상 ACL 제한을 수행하는 방법을 확인했습니다.이제 이러한 모든 지식을 활용하여 네트워크에 필요한 VLAN을 생성할 수 있습니다!