RV160/RV260 라우터의 DMZ 옵션

목표

이 문서에서는 RV160X/RV260X Series 라우터에 DMZ 호스트 및 DMZ 서브넷을 설정하는 두 가지 옵션에 대해 설명합니다.

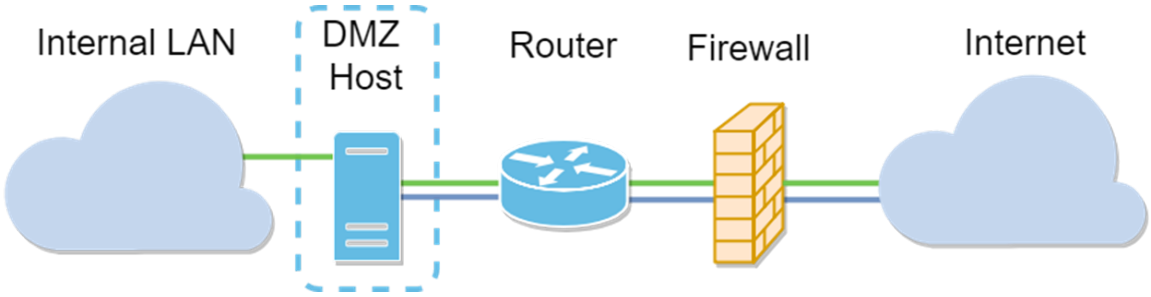
요구 사항

- RV160X
- RV260X

소개

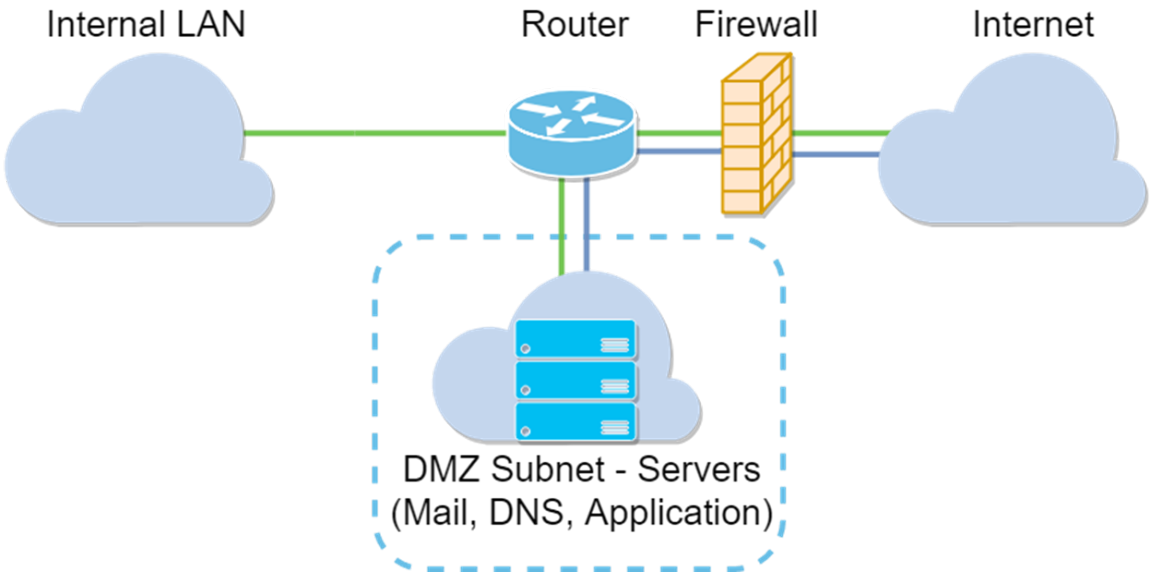
DMZ는 인터넷에 개방된 네트워크의 위치이며 방화벽 뒤에 있는 LAN(Local Area Network)을 보호합니다.기본 네트워크를 단일 호스트 또는 전체 하위 네트워크 또는 "서브넷"에서 분리하면 DMZ를 통해 웹 사이트 서버를 방문하는 사람들이 LAN에 액세스할 수 없게 됩니다.Cisco는 네트워크에서 DMZ를 사용하는 두 가지 방법을 제공합니다. 이 두 방법 모두 DMZ의 운영 방식에 있어 중요한 특징을 갖습니다.아래는 두 운영 모드 간의 차이점을 강조 표시하는 시각적 참조입니다.

호스트 DMZ 토폴로지



참고:호스트 DMZ를 사용할 때 호스트가 불량 행위자에 의해 감염되면 내부 LAN에 추가 보안 침해가 발생할 수 있습니다.

서브넷 DMZ 토폴로지



DMZ 유형	비교	대비
호스트	트래픽을 분리	인터넷에 완전히 개방되는 단일 호스트
서브넷/범위	트래픽을 분리	여러 장치 및 유형, 인터넷에 완전히 개방되어 있습니다.**RV260 하드웨어에서만 사용할 수 있습니다.**

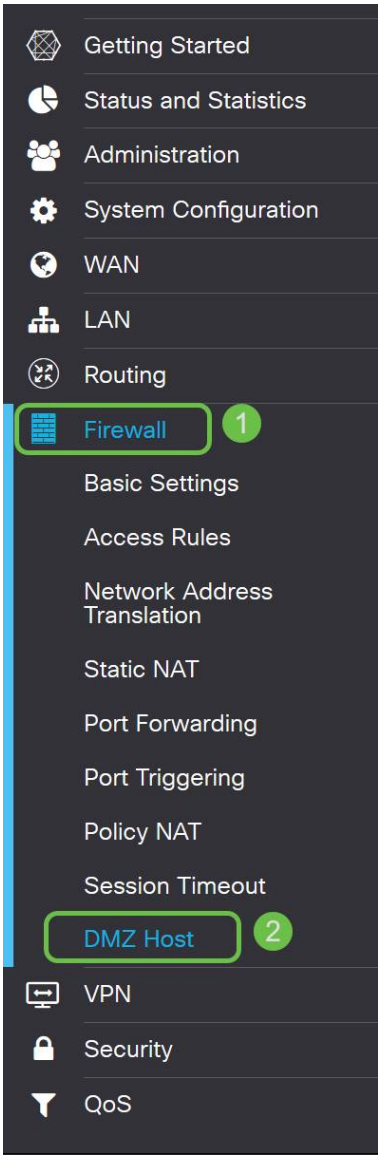
관련 IP 주소 지정

이 문서에서는 사용법에 약간의 차이가 있는 IP 주소 지정 체계를 사용합니다.DMZ를 계획할 때 사설 또는 공용 IP 주소를 사용하는 것을 고려할 수 있습니다.개인 IP 주소는 LAN에서만 고유합니다.공용 IP 주소는 조직 고유 하며 인터넷 서비스 공급자가 할당합니다.공용 IP 주소를 구매하려면 (ISP)에 문의해야 합니다.

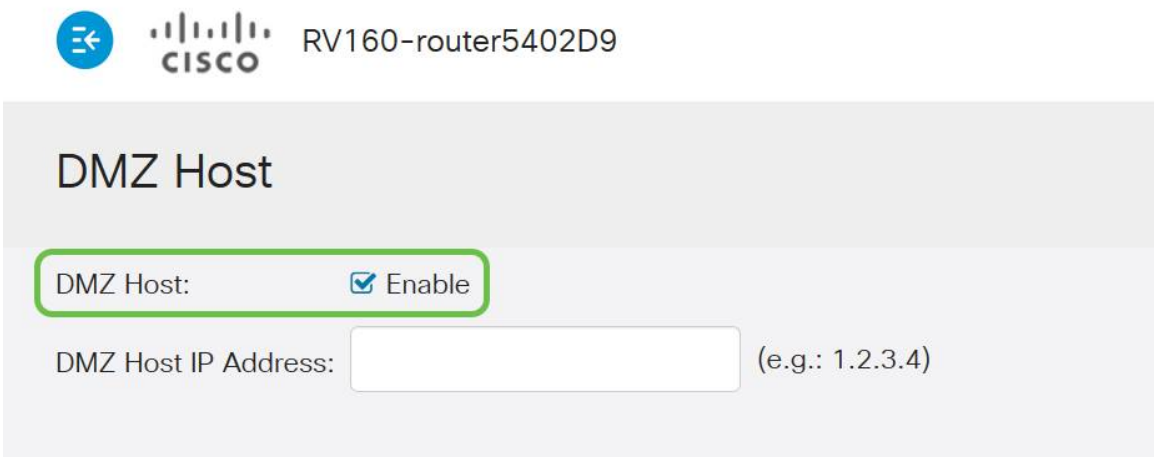
DMZ 호스트 구성

이 방법에 필요한 정보에는 의도된 호스트의 IP 주소가 포함됩니다.IP 주소는 public 또는 private일 수 있지만 공용 IP 주소는 WAN IP 주소와 다른 서브넷에 있어야 합니다.DMZ 호스트 옵션은 RV160X 및 RV260X에서 모두 사용할 수 있습니다.아래 단계에 따라 DMZ 호스트를 구성합니다.

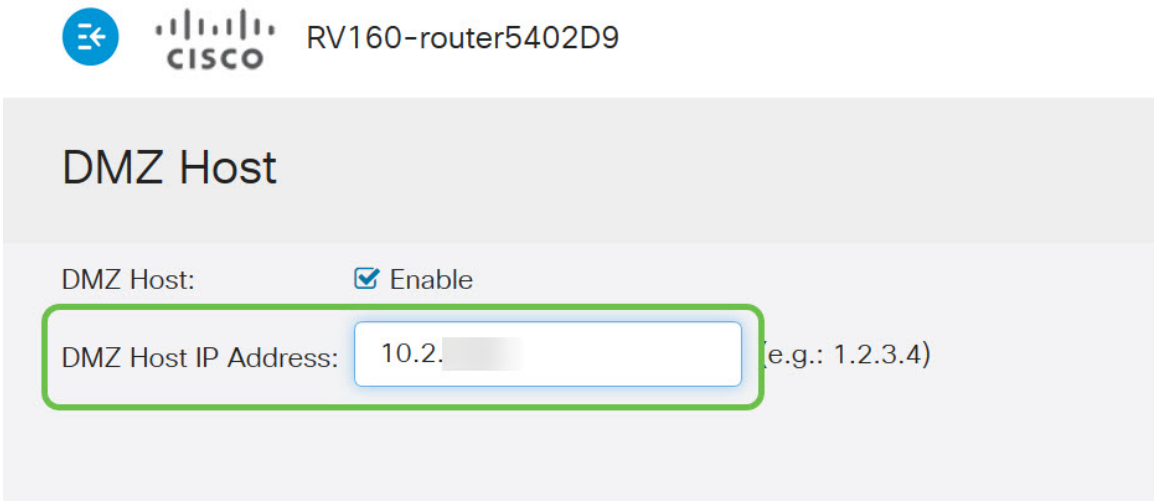
1단계. 라우팅 디바이스에 로그인한 후 왼쪽 메뉴 모음에서 **Firewall > DMZ Host를** 클릭합니다.



2단계. **사용** 확인란을 클릭합니다.



3단계. WAN 액세스를 열려는 호스트의 지정된 IP 주소를 입력합니다.



4단계. 주소 지정에 만족하면 적용 버튼을 클릭합니다.

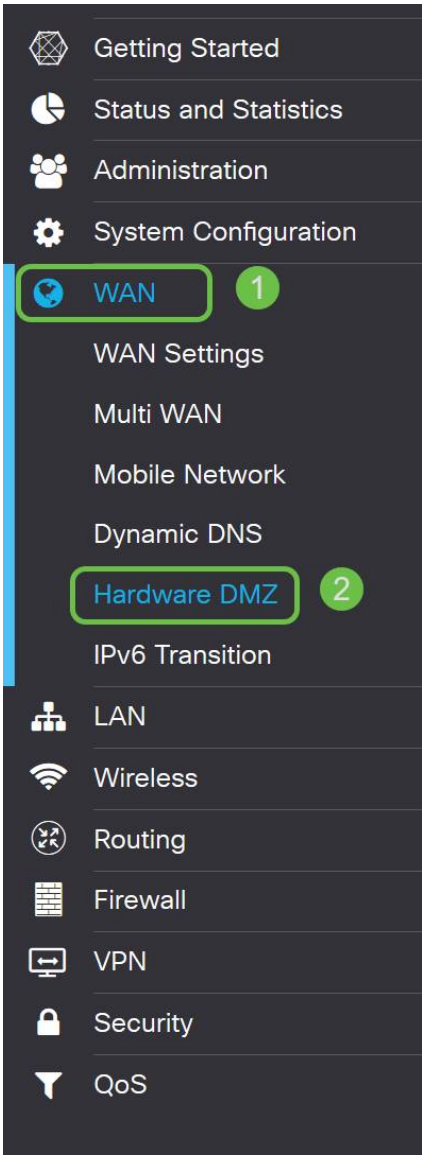
참고:RV160X 시리즈로만 작업하는 경우 확인 지침으로 건너뛰려면 여기를 클릭하여 이 문서의 해당 섹션으로 이동하십시오.

하드웨어 DMZ 구성

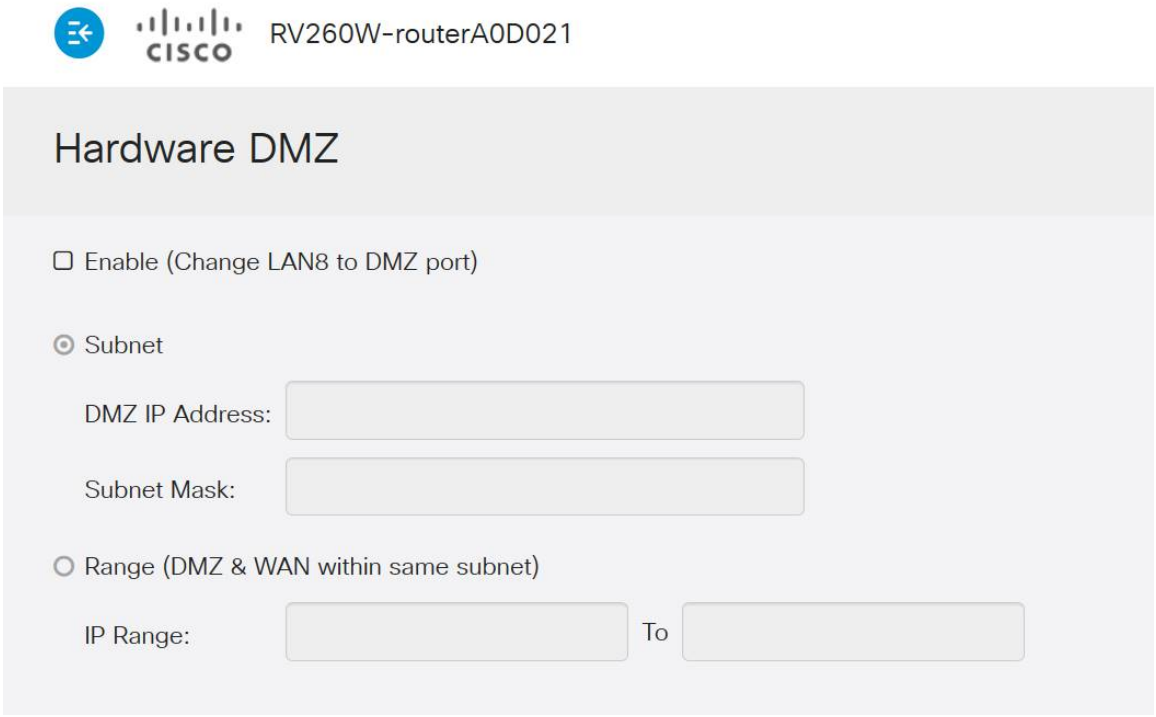
RV260X 시리즈에서만 사용할 수 있는 이 방법에는 선택한 방법에 따라 다른 IP 주소 지정 정보가 필요합니다.두 방법 모두 실제로 하위 네트워크를 사용하여 영역을 정의합니다. 이 차이점은 하위 네트워크의 양을 사용하여 비보호 영역을 생성하는 것과 같습니다.이 경우 옵션은 *모두* 또는 *일부* 입니다.Subnet(*all*) 방법에는 서브넷 마스크와 함께 DMZ 자체의 IP 주소가 필요합니다.이 방법은 해당 하위 네트워크에 속하는 모든 IP 주소를 차지합니다.Range(*일부*) 방법을 사용하면 DMZ 내에 배치할 연속 IP 주소 범위를 정의할 수 있습니다.

참고:어떤 경우든 ISP와 함께 하위 네트워크의 IP 주소 지정 체계를 정의해야 합니다.

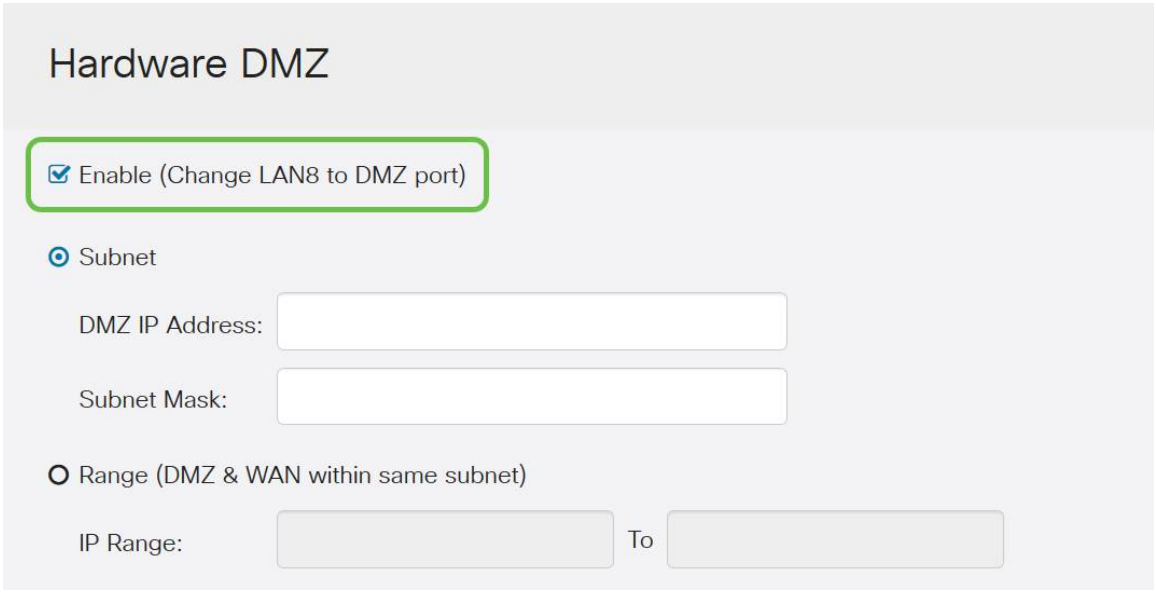
1단계. RV260X 디바이스에 로그인한 후 **WAN > Hardware DMZ**를 클릭합니다.



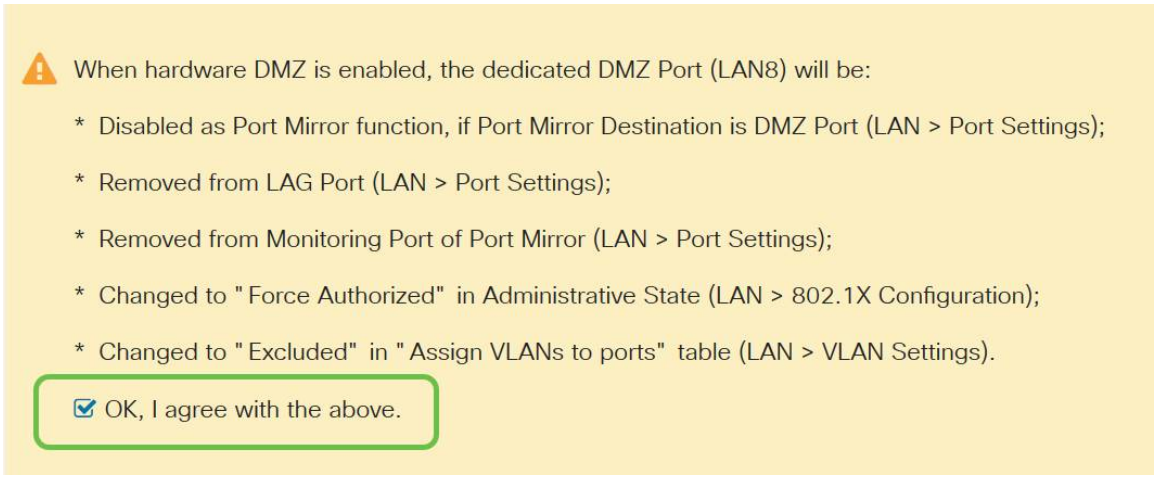
참고:스크린샷은 RV260X 사용자 인터페이스에서 가져옵니다.다음은 이 페이지에 표시될 하드웨어 DMZ 옵션의 스크린샷입니다.



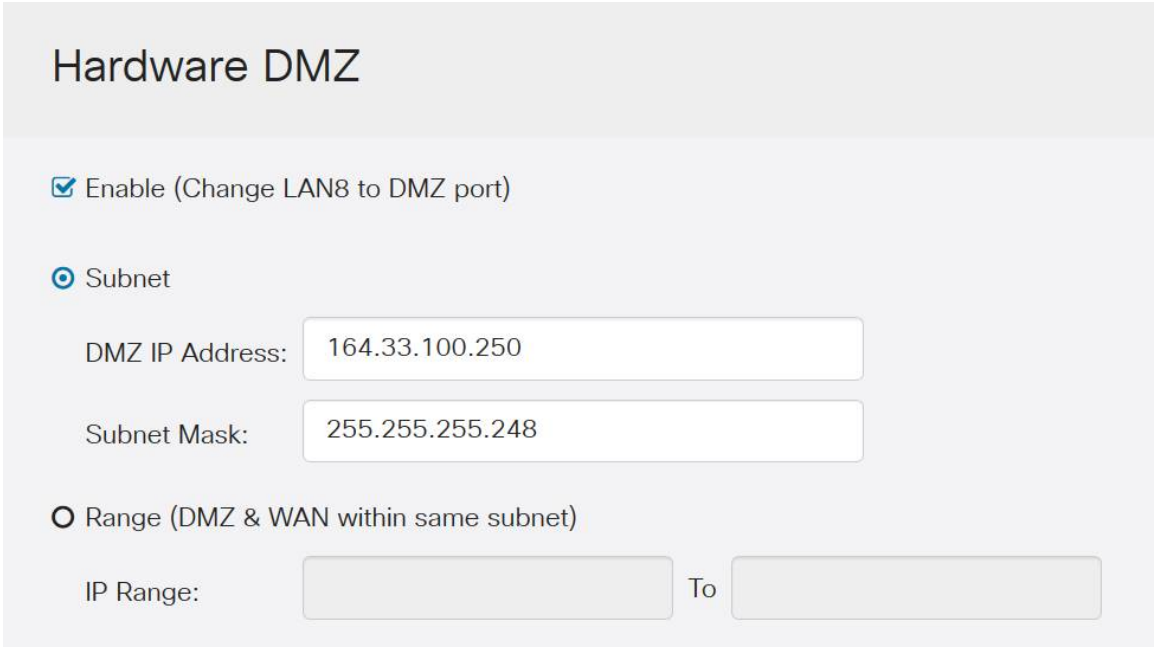
2단계. Enable(**LAN8을 DMZ 포트로 변경)** 확인란을 클릭합니다.이렇게 하면 라우터의 8번째 포트가 DMZ 전용 "창"으로 변환되어 보안이 강화된 서비스로 변환됩니다.



3단계. *사용*을 클릭하면 선택 가능한 옵션 아래에 정보 메시지가 표시됩니다.네트워크에 영향을 미칠 수 있는 점에 대한 세부 정보를 검토하고 **확인, 위** 확인란**에 동의합니다**.

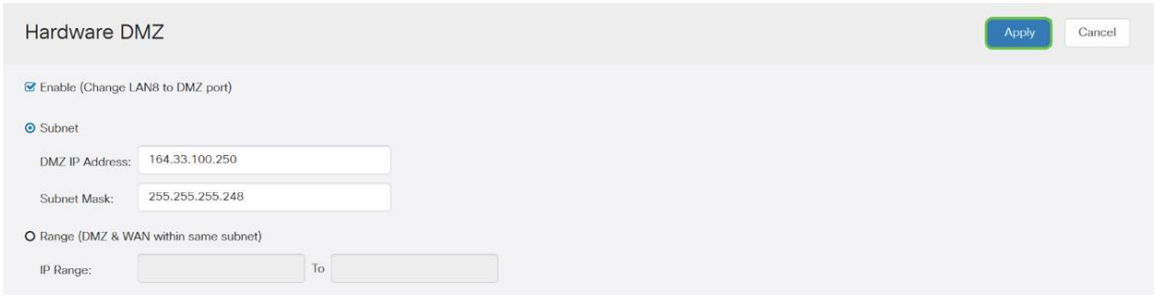


4단계. 다음 단계는 두 가지 잠재적 옵션인 서브넷 및 범위로 분할됩니다.아래 예에서는 서브넷 방법을 선택했습니다.



참고: Range(범위) 방법을 사용하려는 경우 **Range(범위)** 레이디얼 버튼을 클릭한 다음 ISP에서 할당한 IP 주소의 범위를 입력해야 합니다.

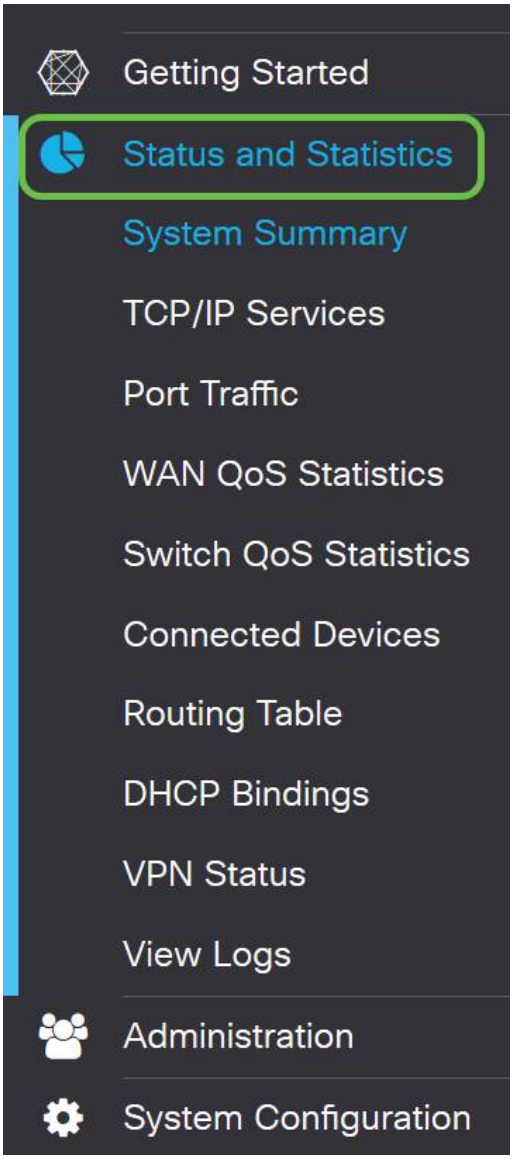
6단계. 오른쪽 상단 모서리에 있는 Apply(적용)를 클릭하여 DMZ 설정을 적용합니다.



DMZ가 올바르게 설정되었는지 확인

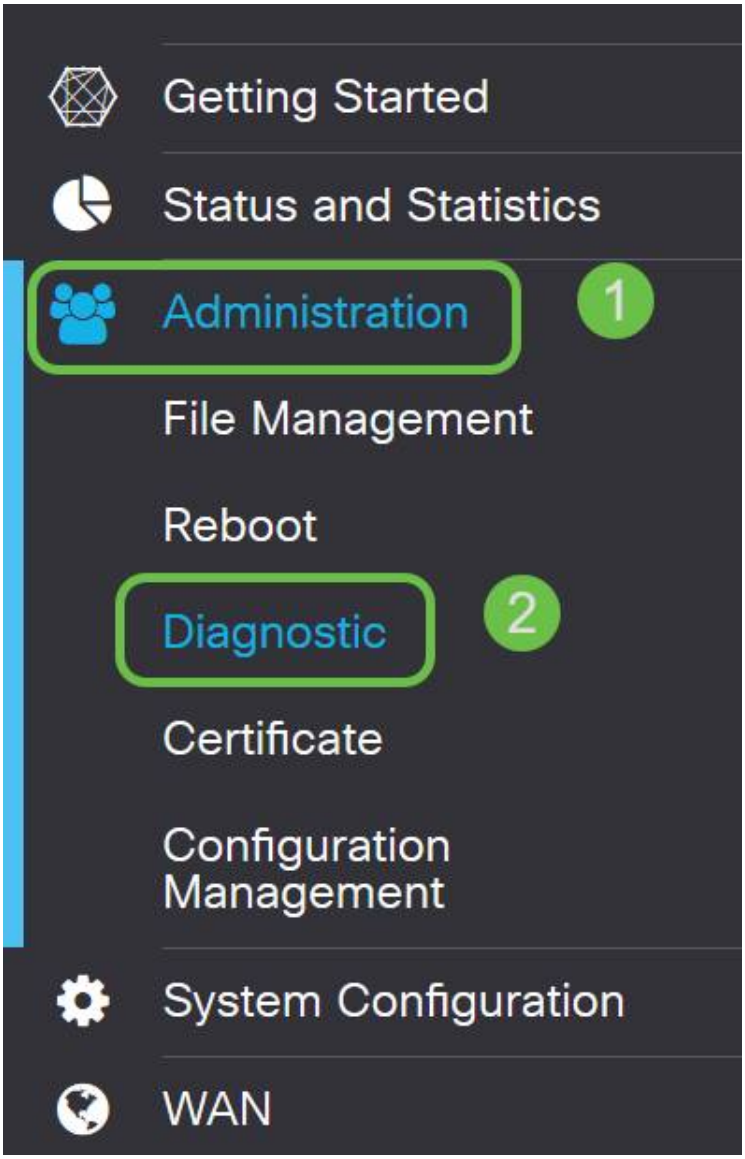
DMZ가 영역 외부 소스의 트래픽을 적절하게 수락하도록 구성되었는지 확인하면 ping 테스트로 충분합니다.먼저 관리 인터페이스에 들러 DMZ의 상태를 확인합니다.

1단계. DMZ가 구성되었는지 확인하려면 **Status & Statistics(상태 및 통계)**로 이동하여 System Summary(시스템 요약) 페이지가 자동으로 로드됩니다.포트 8 또는 "LAN 8"은 DMZ의 상태를 "*Connected*"로 나열합니다.



DMZ가 예상대로 작동하는지 테스트하려면 신뢰할 수 있는 ICMP ping 기능을 사용할 수 있습니다 .ICMP 메시지 또는 "ping"은 DMZ의 문을 노크하려고 시도합니다.DMZ가 "Hello"라고 응답하면 ping이 완료됩니다.

2단계. 브라우저를 ping 기능으로 이동하려면 Administration(관리) **> Diagnostic(진단)을** 클릭합니다.



3단계. **DMZ의 IP 주소**를 입력하고 **Ping** 버튼을 클릭합니다.

ping에 성공하면 위와 같은 메시지가 표시됩니다.ping에 실패하면 DMZ에 연결할 수 없음을 의미합니다.DMZ 설정이 적절하게 구성되었는지 확인합니다.

결론

이제 DMZ 설정을 완료했으므로 LAN 외부에서 서비스에 액세스할 수 있습니다.