RV160 및 RV260 Series 라우터에서 액세스 규칙 구성

목표

라우터는 외부 네트워크에서 데이터를 수신하며, 로컬 네트워크 보안과 관련하여 첫 번째 방어선입니다.라우터에서 액세스 규칙을 활성화하면 IP 주소 또는 포트 번호와 같은 특정 매개변수를 기준으로 패킷을 필터링할 수 있습니다.아래 단계에 따라 이 문서는 네트워크에 들어오는 패킷을 보다 효과적으로 제어하기 위해 액세스 규칙을 구성하는 방법을 안내하는 데 목적이 있습니다.또한 이 문서에서는 액세스 규칙을 사용하여 최상의 보안을 위한 잠재력을 최대한 활용할 수 있는 몇 가지 모범 사례를 중점적으로 살펴봅니다.

적용 가능한 디바이스

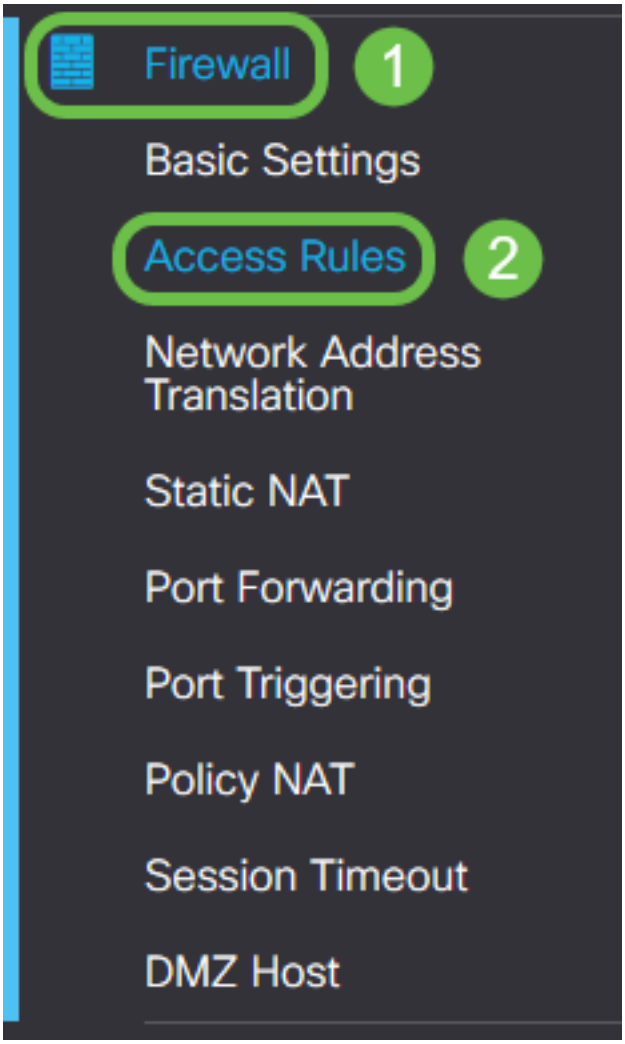
- RV160x
- RV260x

소프트웨어 버전

- 1.0.00.13

액세스 규칙 구성

1단계. 구성 유틸리티 왼쪽의 탐색 창에서 **Firewall > Access Rules**를 선택합니다.

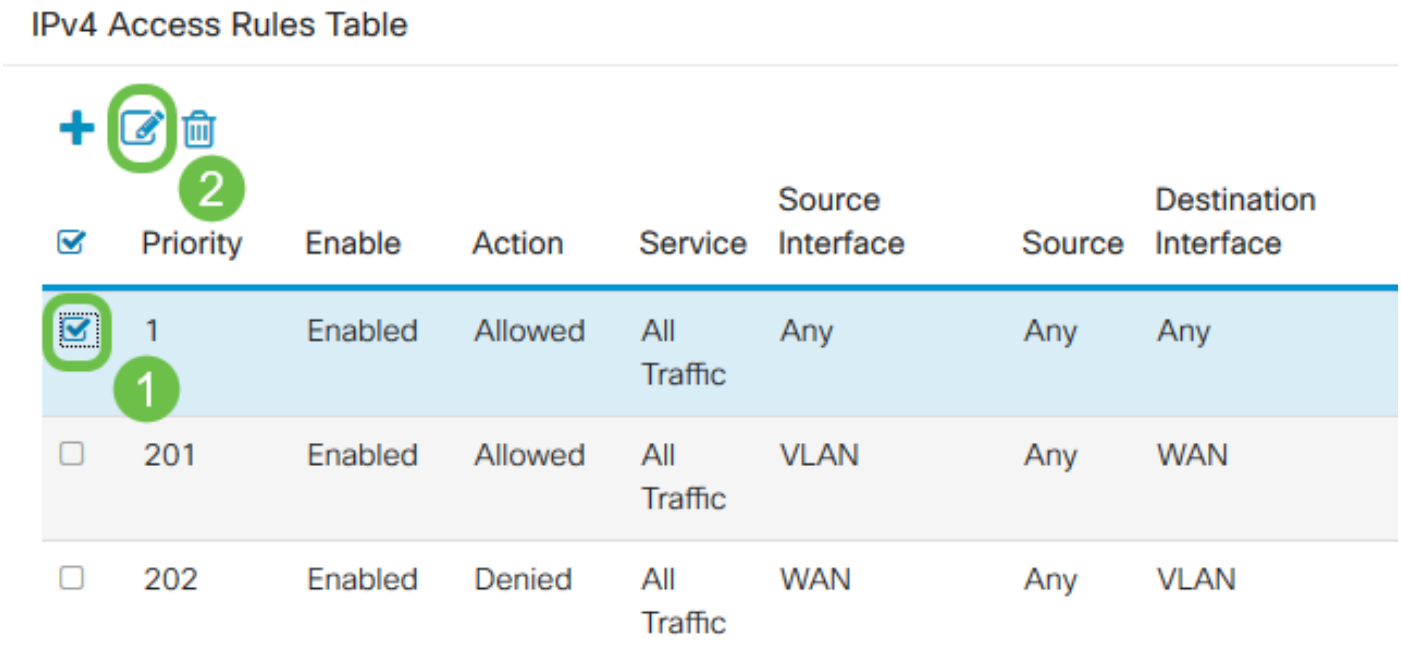


Access Rules 페이지가 나타납니다.이 페이지에는 각각 IPv4 및 IPv6에 대한 액세스 규칙 목록과 해당 특성이 포함된 테이블이 있습니다.여기에서 새 액세스 규칙을 추가하거나, 기존 규칙을 수정하거나, 기존 규칙을 제거할 수 있습니다.

액세스 규칙 추가/수정

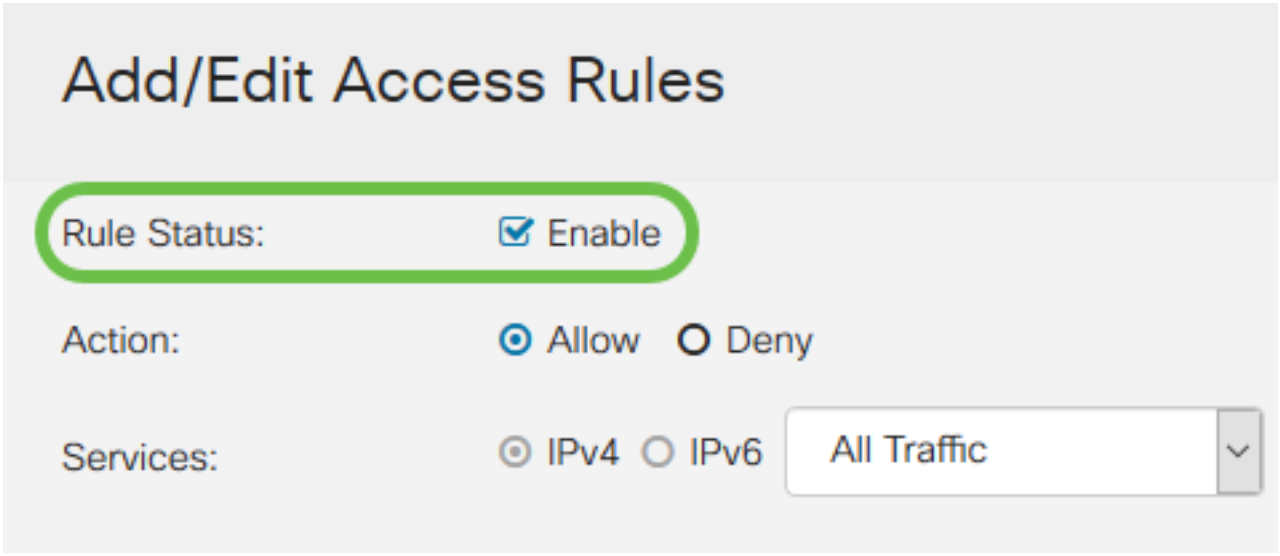
2단계. 새 액세스 규칙을 추가하려면 규칙을 적용할 프로토콜에 따라 IPv4 Access Rules 또는 IPv6 Access Rules 테이블에 추가할 파란색 아이콘을 클릭합니다.이 경우 IPv4가 사용됩니다.

기존 항목을 수정하려면 수정할 액세스 규칙 옆의 확인란을 선택합니다.그런 다음 해당 테이블의 맨 위에 있는 파란색 편집 아이콘을 선택합니다.한 번에 하나의 규칙만 선택하여 편집할 수 있습니다.

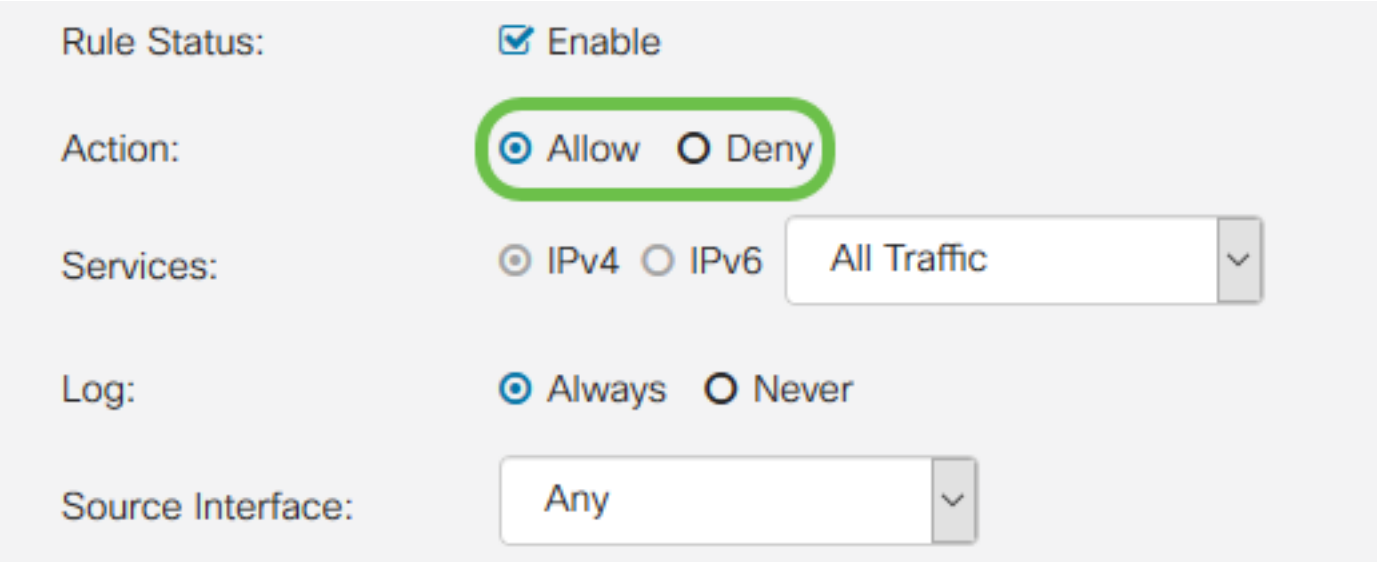


Add/*Edit Access Rules* 페이지가 나타납니다.

3단계. Rule Status(규칙 상태)의 확인란을 선택/선택 취소하여 작업 중에 액세스 규칙을 활성화 또는 비활성화합니다.이 기능은 나중에 적용하기 위해 저장하려는 액세스 규칙이 있는 경우 유용합니다.

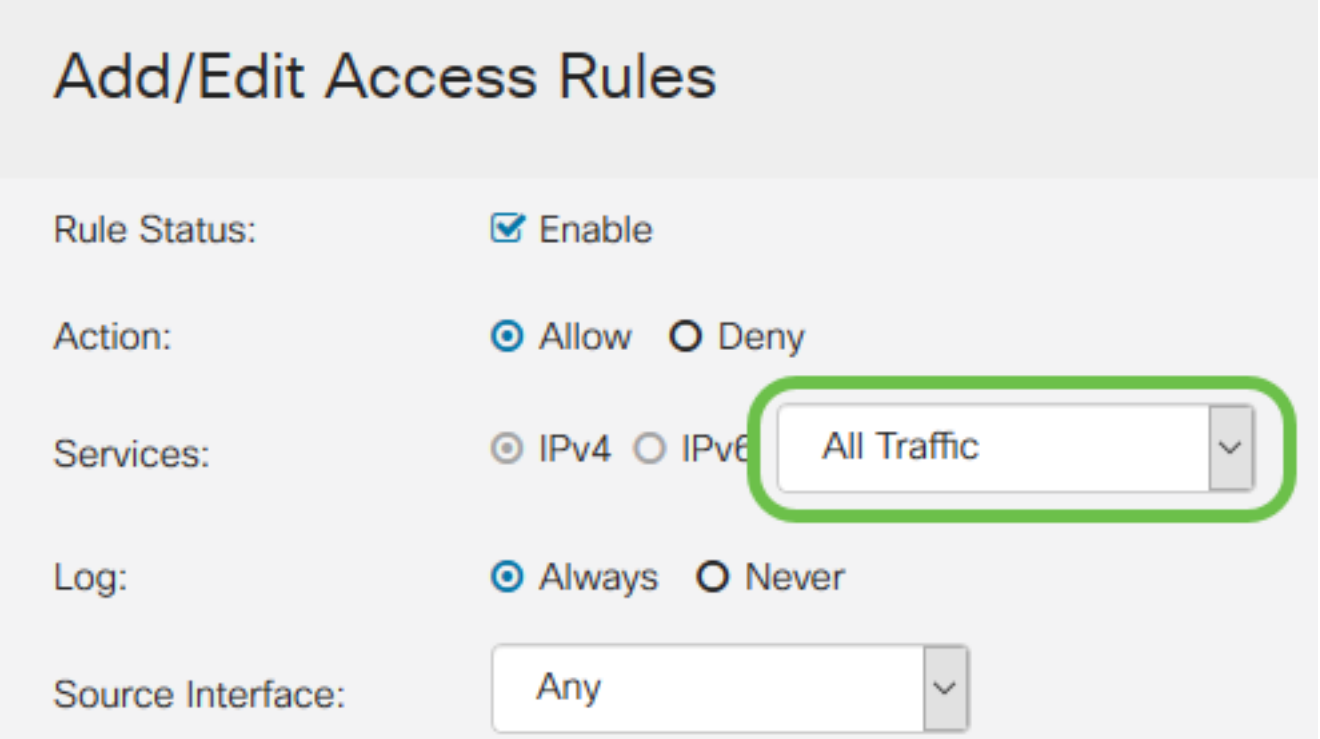


4단계. *Action* 필드에서 규칙이 수신 네트워크 트래픽에 대한 액세스를 허용할지 아니면 거부할지를 선택합니다.



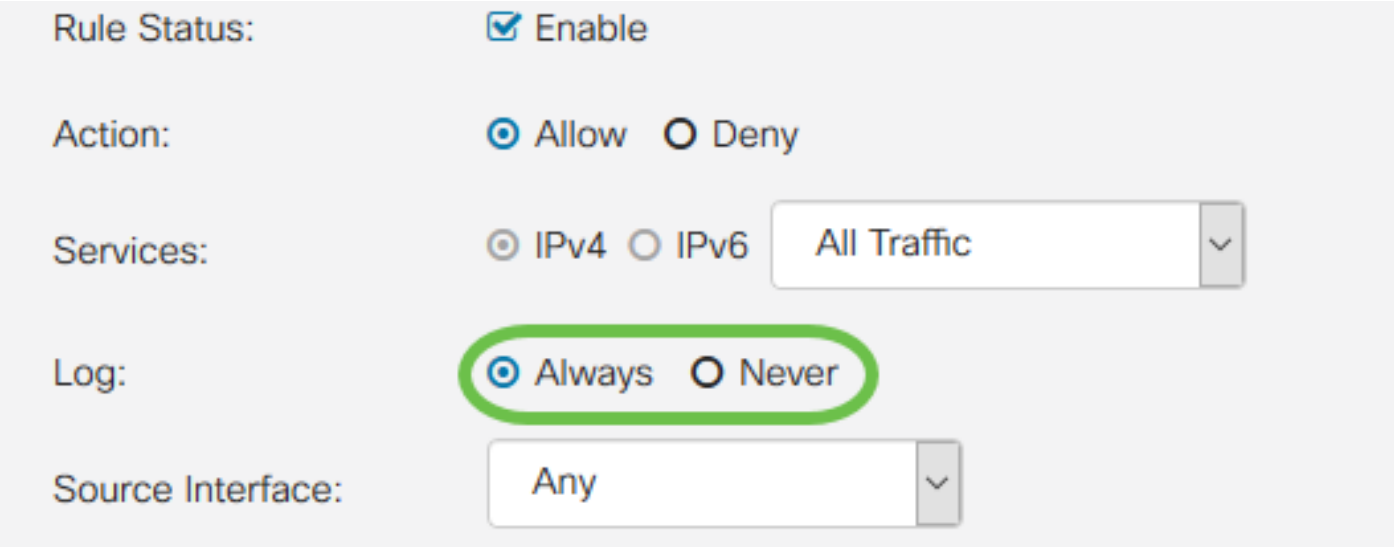
참고:바람직하지 않은 트래픽만 거부하려는 대신 수신하려는 트래픽만 허용하는 액세스 규칙을 설정하는 것이 최상의 보안입니다.그러면 알려지지 않은 위협으로부터 네트워크를 더 잘 보호할 수 있습니다.

5단계. *서비스* 필드의 드롭다운 메뉴에서 액세스 규칙을 적용할 네트워크 서비스 유형을 선택합니다.

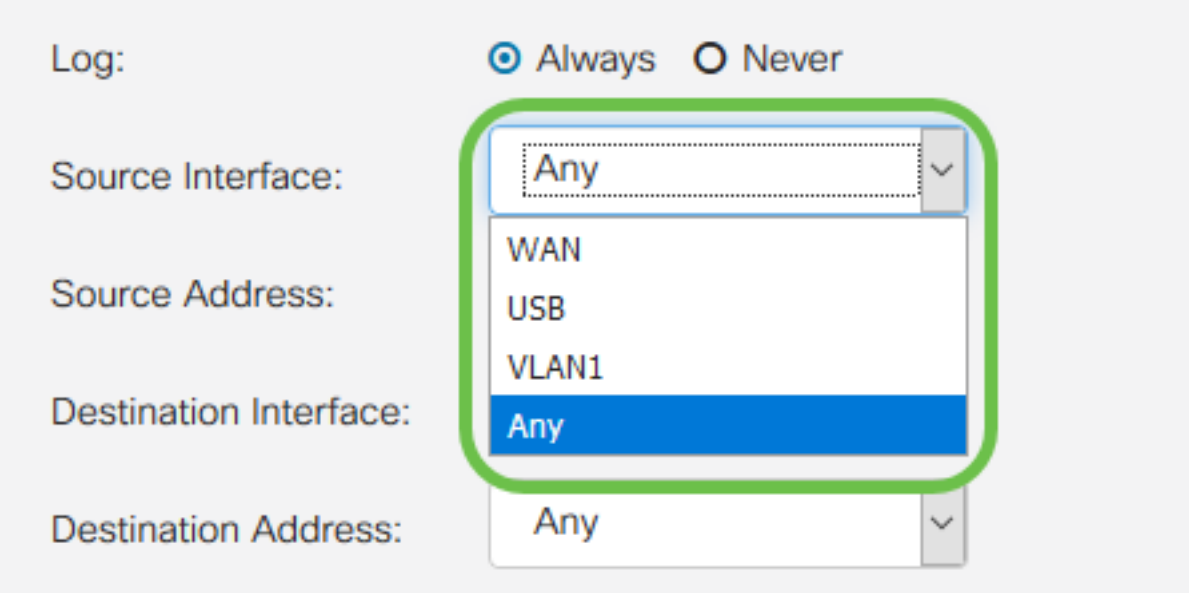


참고:IPv4 또는 IPv6 라디오 버튼은 Access *Rules* 페이지에서 액세스 규칙을 적용하도록 선택한 테이블에 따라 자동으로 선택됩니다.

6단계. *Log* 필드에서 네트워크에 들어오는 패킷이 적용된 규칙과 일치하면 라우터가 로그 메시지를 생성할지 여부를 선택합니다.



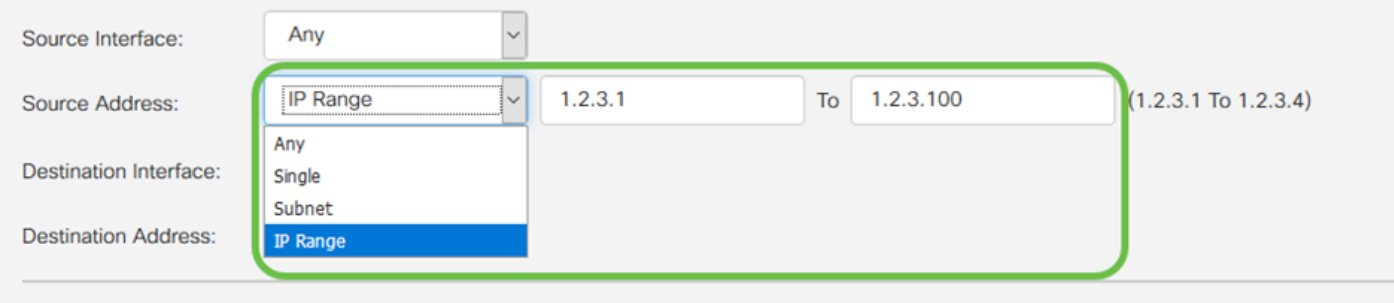
7단계. Source *Interface* 드롭다운 목록에서 액세스 규칙이 적용할 수신 패킷의 네트워크 인터페이스를 선택합니다.



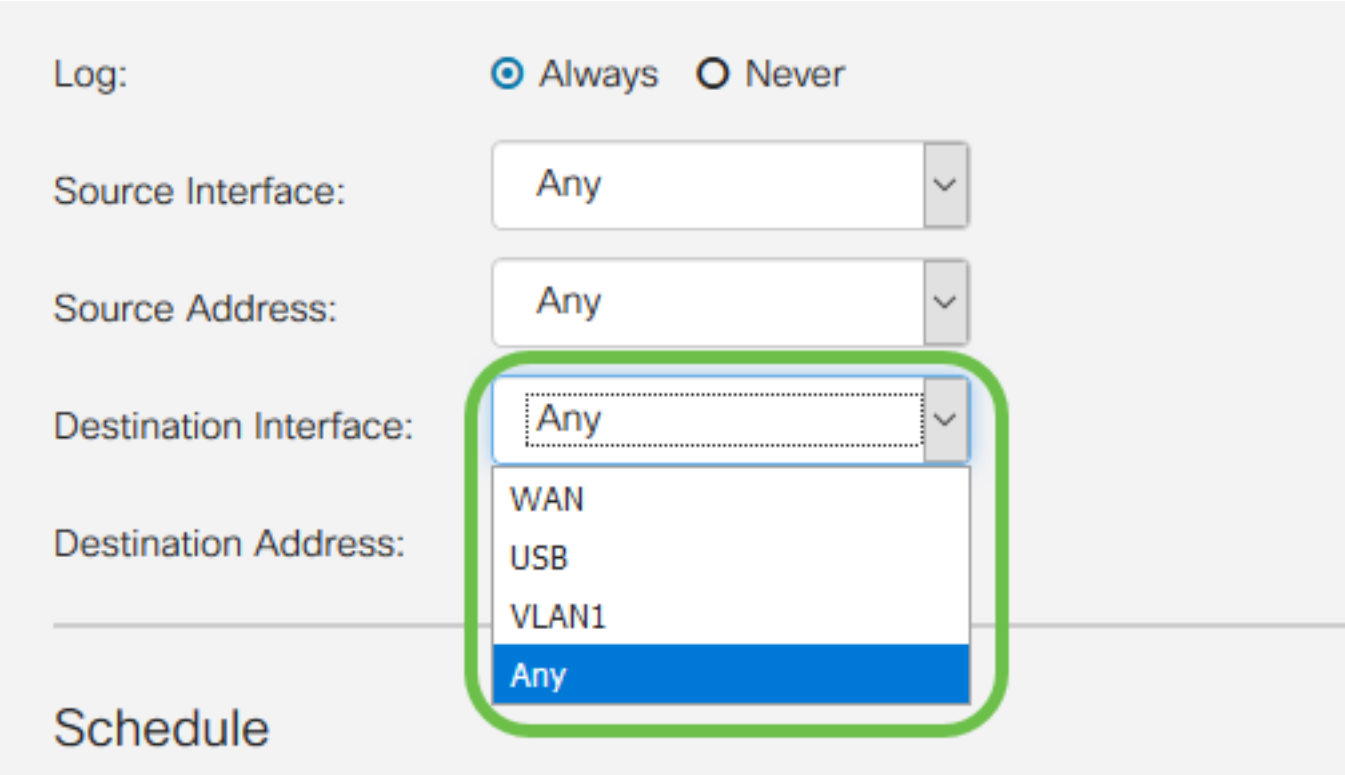
8단계. Source *Address* 드롭다운 목록에서 액세스 규칙이 적용할 수신 주소의 유형을 선택합니다.옵션은 다음과 같습니다.

- Any - 수신 IP 주소에 규칙이 적용됩니다.
- 단일 - 규칙이 정의된 단일 IP 주소에 적용됩니다.
- 서브넷 - 규칙이 네트워크의 정의된 서브넷에 적용됩니다.
- IP 범위 - 정의된 IP 주소 범위에 규칙이 적용됩니다.

참고:단일, 서브넷 또는 IP 범위를 선택하면 주소 세부 정보를 입력할 수 있는 드롭다운 메뉴 오른쪽에 해당 필드가 나타납니다.이 예에서는 시연할 IP 범위를 입력합니다.



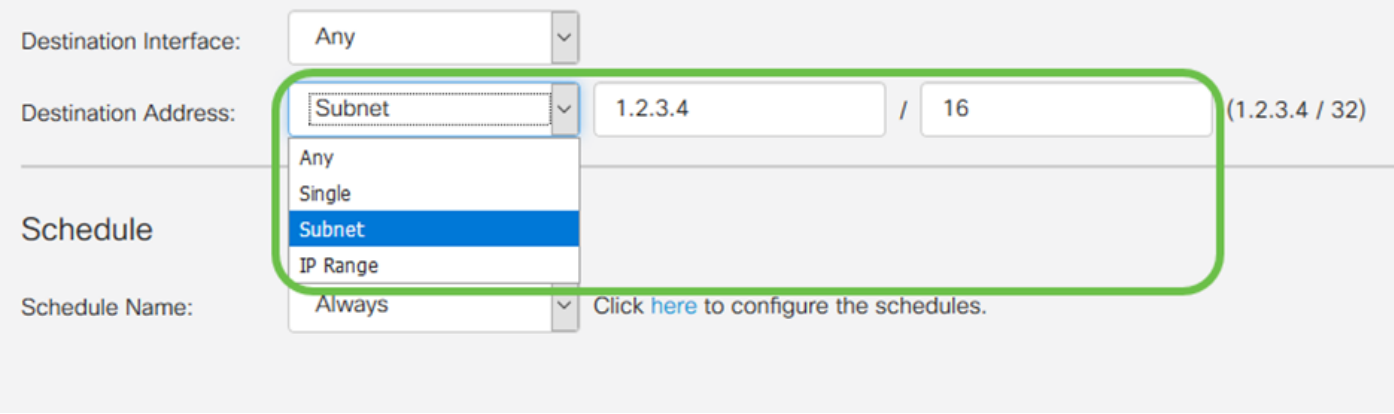
9단계. Destination *Interface* 드롭다운 목록에서 액세스 규칙이 적용할 발신 패킷의 네트워크 인터페이스를 선택합니다.



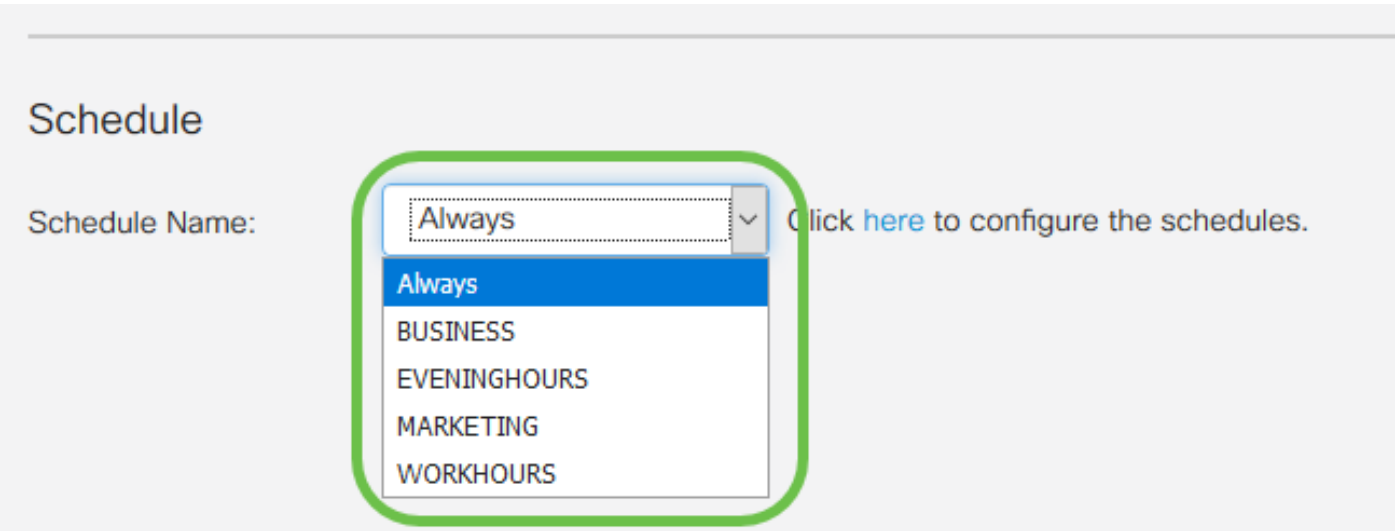
10단계. Destination *Address* 드롭다운 목록에서 액세스 규칙이 적용할 발신 주소의 유형을 선택합니다.옵션은 다음과 같습니다.

- Any - 모든 발신 IP 주소에 규칙이 적용됩니다.
- 단일 - 규칙이 정의된 단일 IP 주소에 적용됩니다.
- 서브넷 - 규칙이 네트워크의 정의된 서브넷에 적용됩니다.
- IP 범위 - 정의된 IP 주소 범위에 규칙이 적용됩니다.

참고:단일, 서브넷 또는 IP 범위를 선택하면 주소 세부 정보를 입력할 수 있는 드롭다운 메뉴 오른쪽에 해당 필드가 나타납니다.이 예에서는 서브넷을 입력하여 시연합니다.



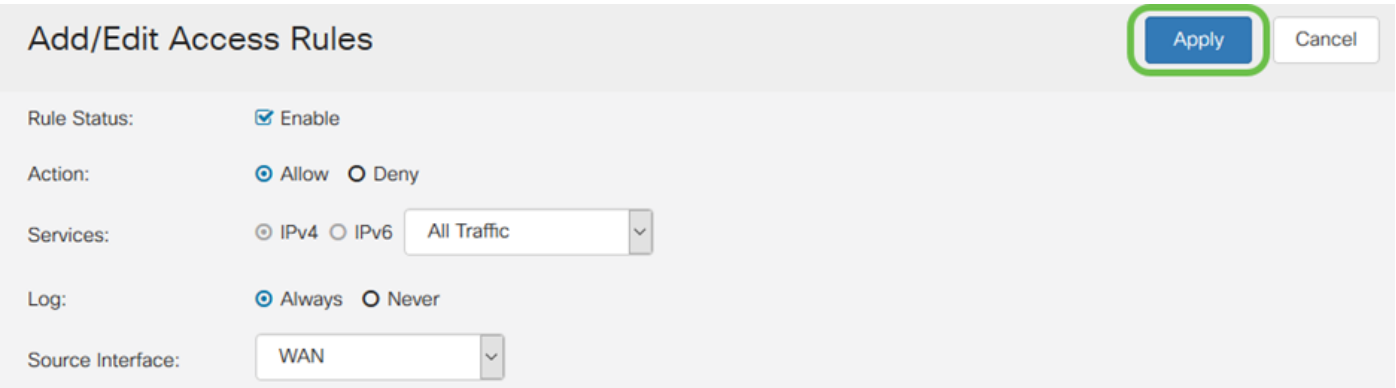
11단계. *Schedule Name* 드롭다운 목록에서 액세스 규칙을 적용할 시간 스케줄을 선택합니다.



참고:보안을 강화하기 위해 업무 시간에 중요하지 않은 네트워크 액세스를 제한하여 비즈니스가 작동하지 않을 때 원치 않는 연결이 거부되도록 하는 것이 좋습니다.

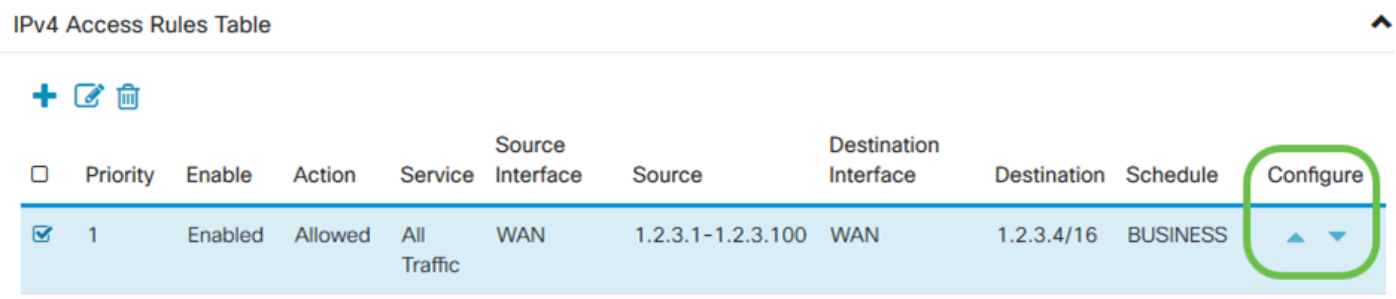
참고:액세스 규칙에 대한 예약 시간을 구성하려면 *Schedule Name* 드롭다운 오른쪽의 링크를 클릭합니다.이러한 일정을 구성하는 방법에 대한 자세한 내용은 여기에서 확인할 수 있습니다.

12단계. 액세스 규칙 컨피그레이션에 만족하면 Apply(**적용)를** 클릭하여 확인합니다.

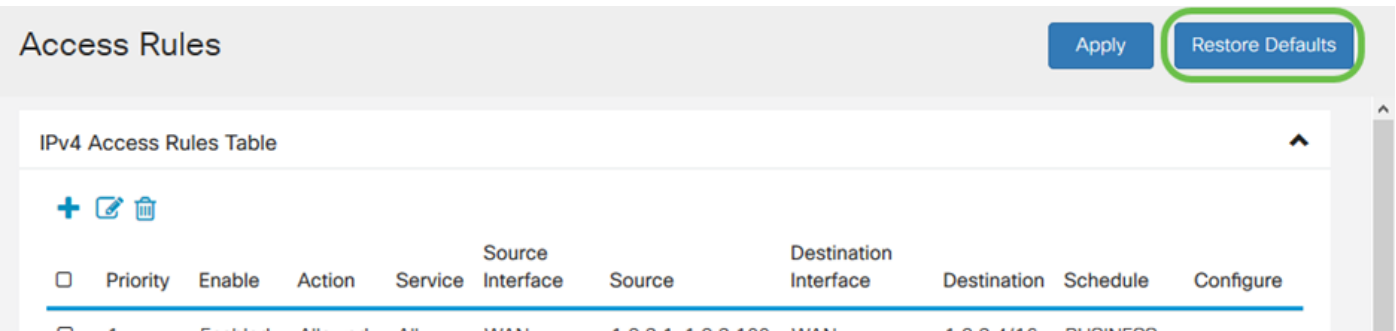


이제 기본 *Access Rules* 페이지로 돌아갑니다.

참고:새 액세스 규칙이 생성되면 목록의 맨 아래에 우선 순위가 지정됩니다.즉, 액세스 규칙이 특정 매개변수에 대해 다른 규칙과 충돌하면 우선순위가 더 높은 규칙의 제한이 우선합니다.우선 순위에서 규칙을 위 또는 아래로 이동하려면 Configure 열에 있는 파란색 화살표를 사용할 수 있습니다.

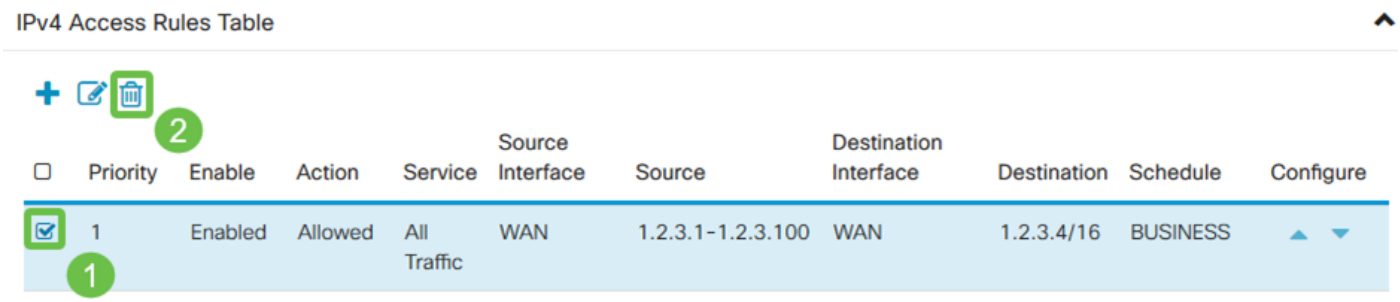


13단계(선택 사항). 액세스 규칙 목록을 기본값으로 되돌리려면 페이지 오른쪽 상단 모서리에서 **Restore Defaults**를 클릭합니다.



액세스 규칙 제거

14단계. 목록에서 액세스 규칙을 제거하려면 제거할 해당 규칙의 확인란을 선택하면 됩니다.그런 다음 목록의 맨 위에 있는 파란색 휴지통 아이콘을 선택합니다.여러 액세스 규칙 항목을 한 번에 제거할 수 있습니다.



서비스 관리

서비스 관리를 사용하면 포트 번호, 프로토콜 및 기타 세부사항을 기준으로 기존 네트워크 서비스를 추가하거나 수정할 수 있습니다.이러한 네트워크 서비스는 액세스 규칙을 구성할 때 서비스 드롭다운에서 사용할 수 있습니다.서비스 관리 목록의 컨피그레이션 메뉴를 통해 액세스 규칙에 적용할 수 있는 맞춤형 서비스를 생성하여 네트워크에 들어오는 트래픽을 보다 세밀하게 제어할 수 있습니다.서비스 관리 구성 방법에 대한 자세한 내용을 보려면 여기를 클릭하십시오.

결론

적절하게 적용되는 액세스 규칙은 WAN 연결을 보호하는 데 유용한 툴입니다.위 설명서와 관련 사례를 통해 RV160x 또는 RV260x 라우터에 대한 보안 액세스 규칙을 올바르게 구성하는 데 필요한 모든 사항을 포함해야 합니다.