RV315W VPN 라우터의 액세스 제어 컨피그레이션

목표

액세스 제어 컨피그레이션을 사용하면 특정 IP 주소에 대한 액세스를 제한할 수 있습니다.제한을 사용자 지정하는 다양한 옵션이 있습니다.시간, 요일, IP 주소, 물리적 포트 및 프로토콜 유형은 액세스 제어 정책에 대한 일부 사용자 지정 기능의 예입니다.

이 문서에서는 RV315W VPN 라우터에서 액세스 제어를 활용하고 구성하는 방법에 대해 설명합니다.

적용 가능한 장치

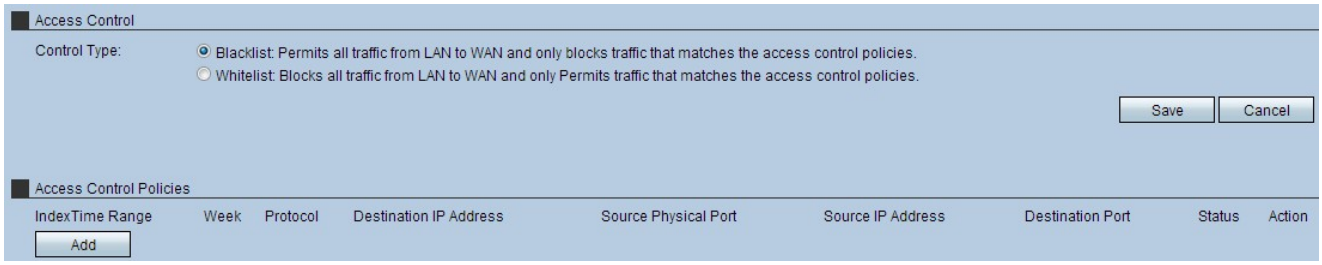
·RV315W

소프트웨어 버전

•1.01.03

구성 관리

1단계. 웹 구성 유틸리티에 로그인하고 **보안 > 액세스 제어를** 선택합니다.Access *Control* 페이지가 열립니다.



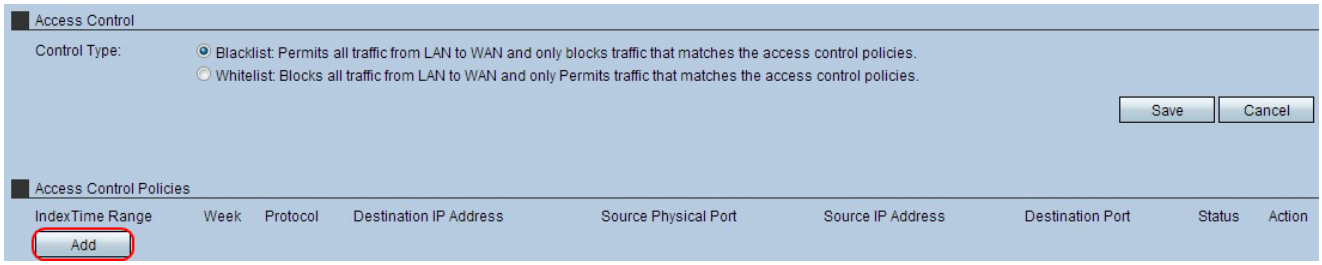
2단계. 제어 유형 필드에서 차단 목록 또는 허용 목록 라디오 버튼을 클릭합니다.

·차단 목록 — 이 옵션은 액세스 제어 설정을 통해 차단된 트래픽을 제외하고 LAN에서 WAN으로 향하는 모든 트래픽을 허용합니다.

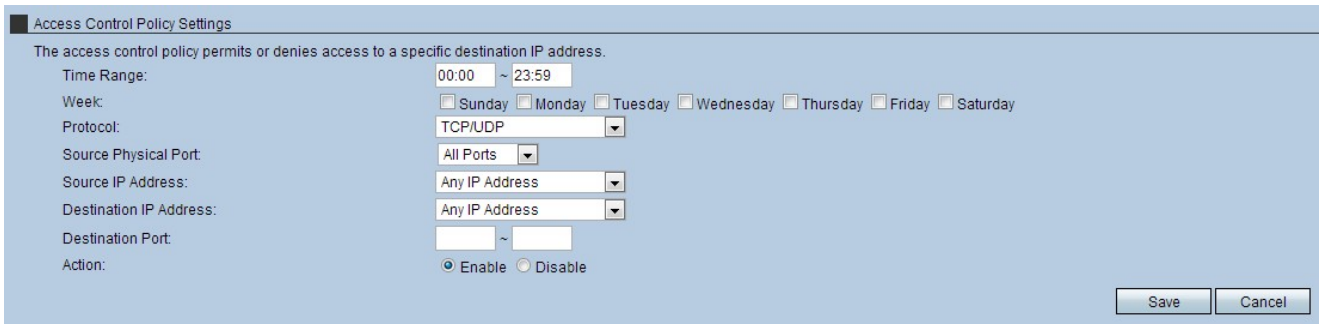
·허용 목록 — 이 옵션은 액세스 제어 설정을 통해 허용되는 트래픽을 제외하고 LAN에서 WAN으로의 모든 트래픽을 차단합니다.

자세한 내용은 용어집을 참조하십시오.

3단계. 설정을 적용하려면 **저장**을 클릭합니다.



4단계. **Add**(추가)를 클릭하여 새 액세스 제어 정책을 추가합니다.Access *Control Policy Settings(액세스 제어 정책 설정*) 페이지가 열립니다.



5단계. 시간 범위 필드에 범위를 입력합니다.이 옵션은 액세스 제어 정책이 적용되는 시간입니다.

6단계. 액세스를 허용하거나 제한할 요일을 선택합니다.이 옵션은 액세스 제어 정책이 적용되는 요일입니다.

7단계. Protocol 드롭다운 목록에서 액세스 제어가 적용되는 프로토콜을 선택합니다.

·TCP — 이 프로토콜은 애플리케이션에서 네트워크로 데이터를 전송하는 데 사용됩니다.TCP는 일반적으로 정보 전송이 완료되어야 하고 패킷이 삭제되지 않는 애플리케이션에 사용됩니다.

·UDP — 이 프로토콜은 IP(Internet Protocol)를 기반으로 하는 클라이언트/서버 네트워크 애플리케이션을 위한 것입니다. 이 프로토콜의 주요 목적은 라이브 애플리케이션을 위한 것입니다.(VOIP, 게임 등)

·TCP/UDP — TCP와 UDP를 모두 활용하려면 이 프로토콜을 선택합니다.이것이 기본 프로토콜입니다.

·ICMP — 이 프로토콜은 오류 메시지를 전송하며 네트워크에서 오류 처리를 담당합니다.네트워크에서 패킷 전달에 문제가 있을 경우 이 프로토콜을 사용하여 알림을 받습니다.

·HTTP — 이 프로토콜은 웹 서버와 브라우저 간에 안전한 통신을 제공합니다.서버와 브라우저 간에 패킷을 안전하게 전송해야 하는 경우 이 프로토콜을 사용합니다.

·FTP — 이 프로토콜은 컴퓨터 간에 파일을 전송합니다.여러 디바이스 간에 파일을 교환할 때 이 프로토콜을 선택합니다.

·SMTP — 이 프로토콜은 이메일 전송을 처리합니다.전자 메일을 교환할 때 이 프로토콜을 선택합니다.

·POP3 — 이 프로토콜은 이메일과 관련하여 SMTP와 결합됩니다.POP3는 전자 메일 서버에서 개인 컴퓨터로 전자 메일을 다운로드합니다.전자 메일을 다운로드할 때 이 프로토콜을 선택합니다.

8단계. Source Physical Port(소스 물리적 포트) 드롭다운 목록에서 액세스 제어가 적용되는

포트를 선택합니다.

9단계. Source IP Address 드롭다운 목록에서 액세스 제어가 적용되는 IP 주소를 선택합니다.

·모든 IP 주소 — 모든 IP 주소를 허용하거나 거부하려면 이 옵션을 선택합니다.이 옵션에 대해 enable 또는 disable 라디오 버튼을 선택합니다.

·단일 IP 주소 — 개별 IP 주소를 허용하거나 거부하려면 이 옵션을 선택합니다.Source IP Address 필드에 해당 IP 주소를 입력합니다.

·IP 주소 범위 — 선택한 범위를 기준으로 IP 주소를 허용하거나 거부하려면 이 옵션을 선택합니다.첫 번째 및 두 번째 Source IP Address 필드에 해당 IP 주소 범위를 입력합니다.

10단계. Destination IP Address 드롭다운 목록에서 액세스 제어가 적용되는 IP 주소를 선택합니다.

·모든 IP 주소 — 모든 IP 주소를 허용하거나 거부하려면 이 옵션을 선택합니다.이 옵션에 대한 enable 또는 disable 라디오 버튼을 클릭합니다.

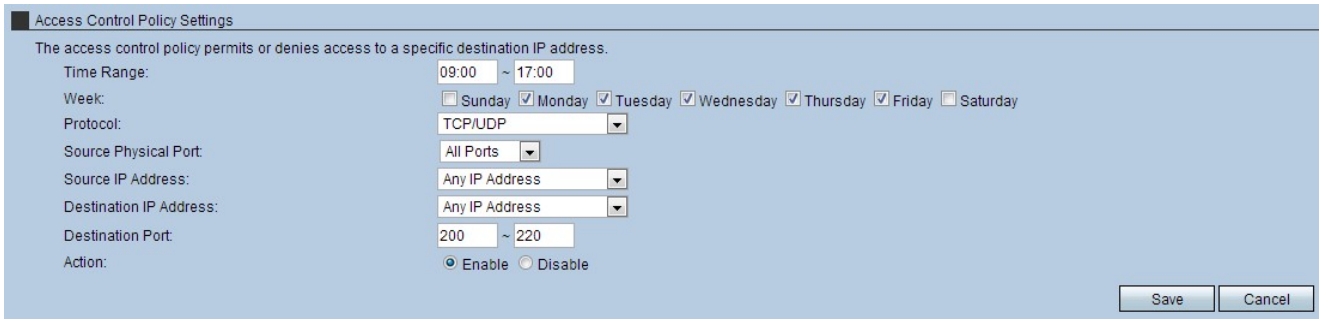
·단일 IP 주소 — 개별 IP 주소를 허용하거나 거부하려면 이 옵션을 선택합니다.Destination IP Address 필드에 해당 IP 주소를 입력합니다.

·IP 주소 범위 — 선택한 범위를 기준으로 IP 주소를 허용하거나 거부하려면 이 옵션을 선택합니다.첫 번째 및 두 번째 Destination IP Address 필드에 해당 IP 주소 범위를 입력합니다.

11단계. Destination Port 필드에 액세스 제어가 적용되는 프로토콜 또는 애플리케이션의 포트 범위를 입력합니다.

12단계. 액세스 제어 정책을 활성화하려면 **Enable** 라디오 버튼을 클릭합니다.

13단계. 설정을 적용하려면 **저장**을 클릭합니다.



14단계. (선택 사항) 액세스 제어 정책을 삭제하려면 Action 헤더 아래의 휴지통 아이콘을 클릭합니다.

15단계. (선택 사항) 액세스 제어 정책을 수정하려면 작업 헤더 아래의 봉투 아이콘을 클릭합니다.