RV160 및 RV260 라우터에서 세션 시간 초과 설정 구성

목표

세션 시간 초과 기능은 특정 세션이 닫히기 전에 유휴 상태로 유지할 수 있는 시간을 정의합니다.따라서 유휴 상태일 때 세션에서 로그아웃하여 네트워크에 원치 않는 액세스를 가질 가능성도 제한됩니다.

세션 시간 초과 설정을 구성하는 것도 시간이 걸리는 컨피그레이션을 수행하는 경우 유리하므로 세션 시간 제한을 훨씬 더 오래 설정할 수 있습니다.이렇게 하면 세션 시간이 초과되어 관리자가 전체 컨피그레이션을 다시 수행해야 하는 상황을 방지할 수 있습니다.

이 문서의 목적은 RV160 및 RV260 라우터에서 세션 시간 제한 설정을 구성하는 방법을 보여주는 것입니다.

적용 가능한 디바이스

- RV160
- RV260

소프트웨어 버전

- 1.0.00.13

세션 시간 초과 구성

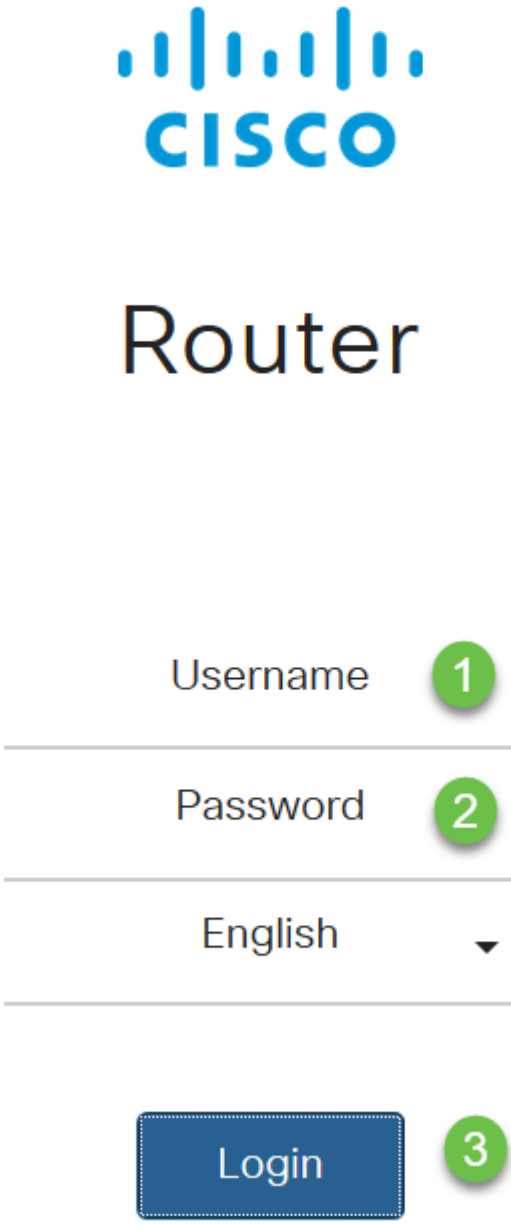
Session Timeout 섹션에서 TCP(Transmission Control Protocol)/UDP(User Datagram Protocol)/ICMP(Internet Control Message Protocol) 흐름에 대한 세션 시간 제한 및 최대 동시 연결을 구성할 수 있습니다.

TCP와 UDP는 인터넷 프로토콜 제품군의 핵심 프로토콜인 전송 프로토콜입니다.TCP와 UDP는 모두 TCP/IP 모델의 전송 레이어에서 작동합니다.TCP는 신뢰할 수 있는 연결을 설정하기 위해 3방향 핸드셰이크를 사용하는 반면 UDP는 TCP와 비교할 때 안정적이지만 빠릅니다.ICMP는 오류를 보고하고 알리는 데 사용되는 네트워크 레이어 프로토콜이며 네트워크 검색에 사용됩니다.

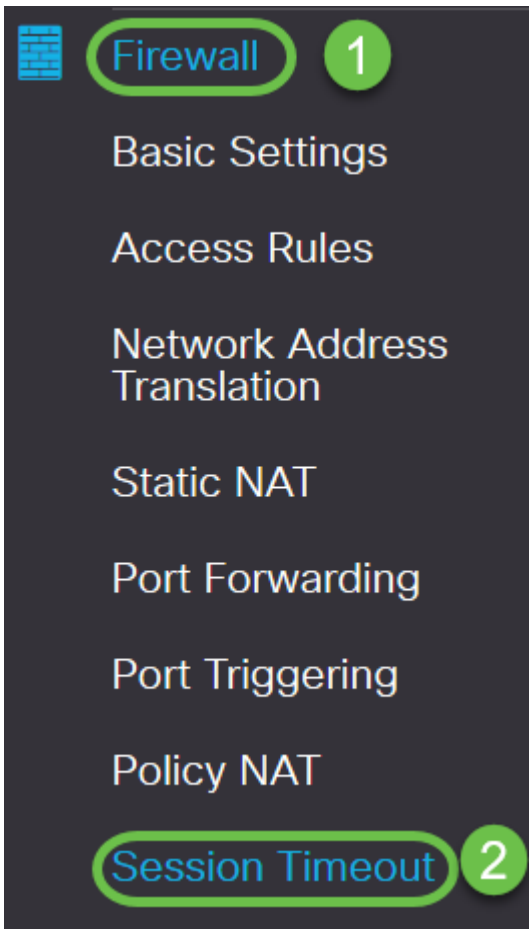
세션 시간 초과는 TCP/UDP/ICMP 세션이 유휴 기간 후 시간 초과에 걸리는 시간입니다.세션 시간 초과를 구성하려면 다음 단계를 수행합니다.

1단계. 웹 구성 유틸리티에 로그인합니다.

참고:이 문서에서는 RV260을 사용하여 세션 시간 제한을 구성합니다.구성은 사용 중인 모델에 따라 달라질 수 있습니다.



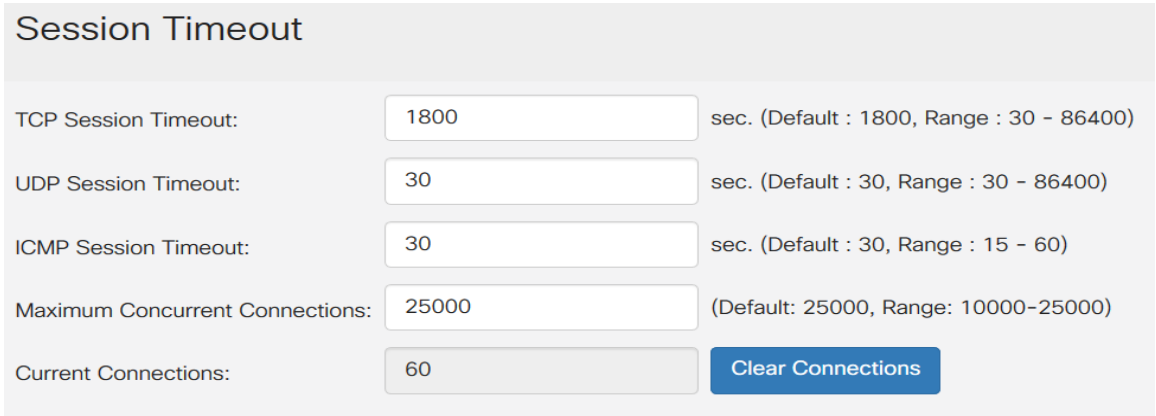
2단계. Firewall(**방화벽**) > **Session Timeout(세션 시간 초과)을 클릭합니다**.



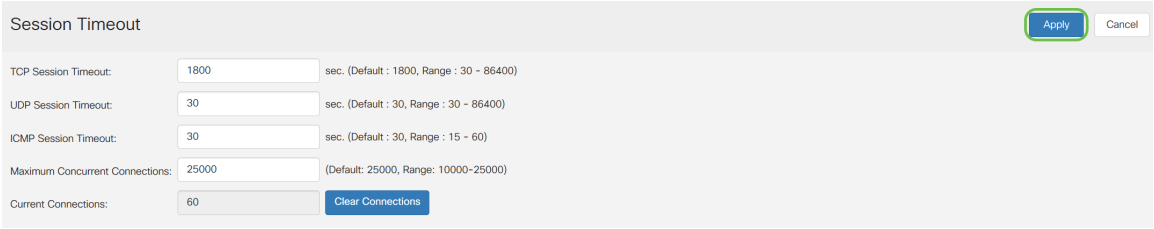
3단계. 다음을 입력합니다.

- *TCP 세션 시간 제한*:TCP 세션에 대한 시간 제한 값을 초 단위로 입력합니다.이 기간 후에 비활성 TCP 세션이 세션 테이블에서 제거됩니다(기본값 1800, 범위 30~86400).
- *UDP 세션 시간 제한*:UDP 세션에 대한 시간 제한 값을 초 단위로 입력합니다.이 기간이 지나면 비활성 UDP 세션이 세션 테이블에서 제거됩니다(기본값 30, 범위 30~86400).
- *ICMP 세션 시간 제한*:ICMP 세션에 대한 시간 제한 값을 초 단위로 입력합니다.비활성 ICMP 세션은 이 기간이 지나면 세션 테이블에서 제거됩니다(기본값 30, 범위 15~60).
- *최대 동시 연결 수*:허용되는 최대 동시 연결 수를 입력합니다(기본값 25000, 범위 10000~25000).
- *현재 연결*:현재 연결 수를 표시합니다.
- *연결 지우기*:현재 연결을 지우려면 클릭합니다.

참고:RV160의 경우 기본 최대 동시 연결 수는 15000이고 범위는 10000 - 15000입니다.



4단계. Apply(적용)를 **클릭합니다.**



이제 RV160 및 RV260 라우터에서 Session Timeout Settings(세션 시간 초과 설정)를 성공적으로 구성했어야 합니다.