RV132W 또는 RV134W VPN Router에 공격 방지 구성

목표

Attack Protection을 사용하면 검색, 플러딩 및 에코 스톰과 같은 일반적인 유형의 공격으로부터 네트워크를 보호할 수 있습니다. 라우터에 기본적으로 Attack Protection(공격 보호)이 활성화되어 있지만, 매개변수를 조정하여 네트워크에서 탐지할 수 있는 공격에 더 민감하고 대응력을 높이도록 할 수 있습니다.

이 문서에서는 RV132W 및 RV134W VPN Router에서 공격 보호를 구성하는 방법을 보여 줍니다.

적용 가능한 장치

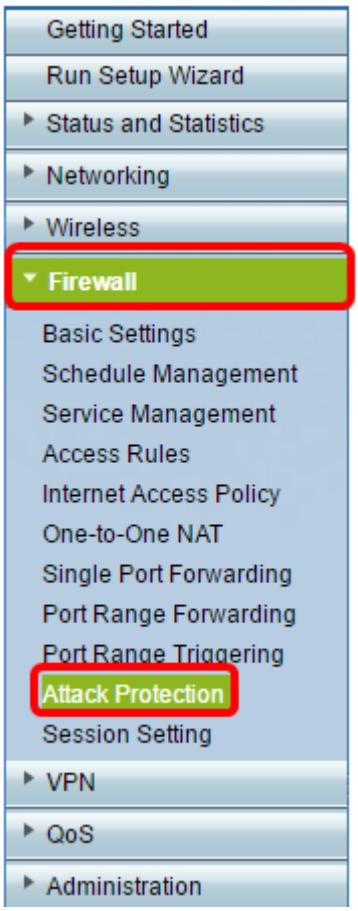
- RV 132W
- RV134W

소프트웨어 버전

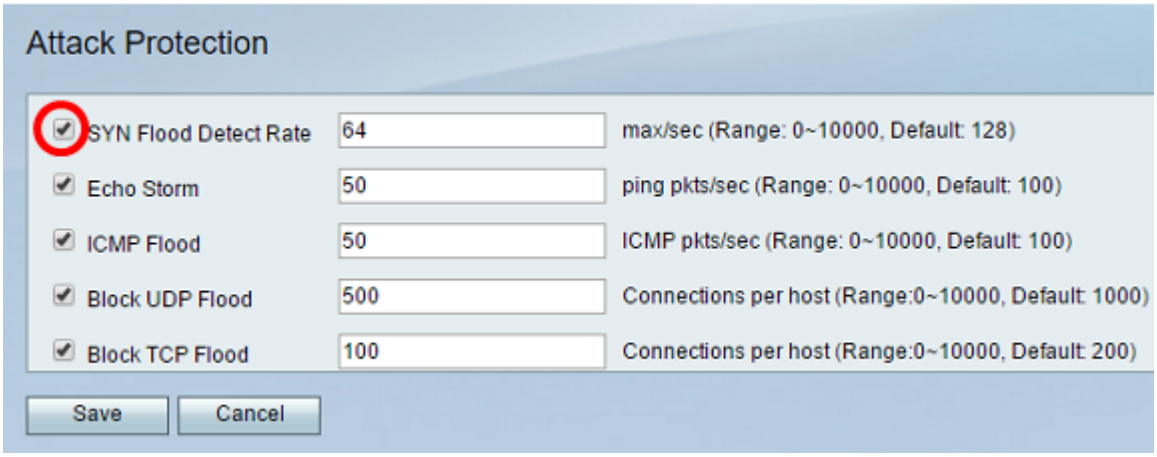
- 1.0.0.17 — RV132W
- 1.0.0.24 — RV134W

공격 보호 구성

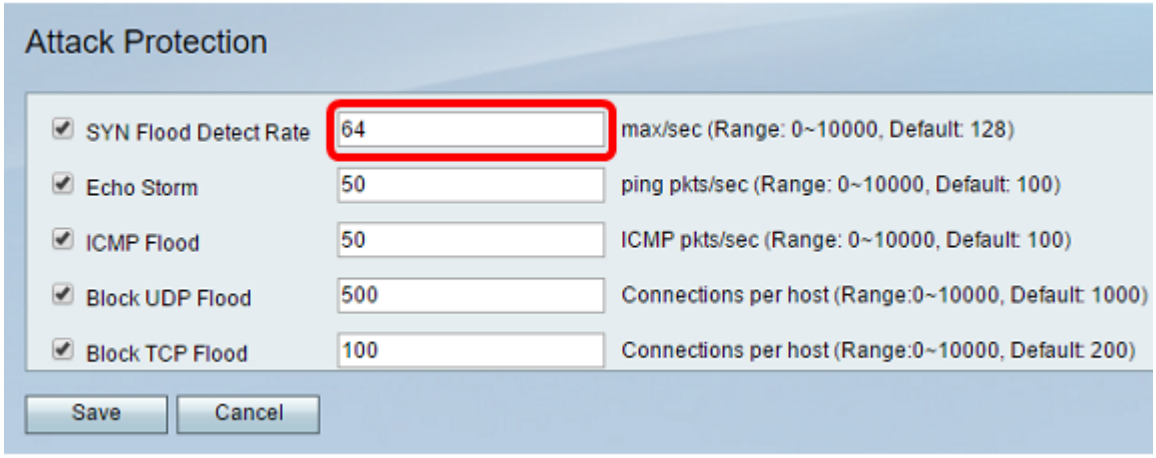
1단계. 웹 기반 유틸리티에 로그인하고 **Firewall > Attack Protection**을 선택합니다.



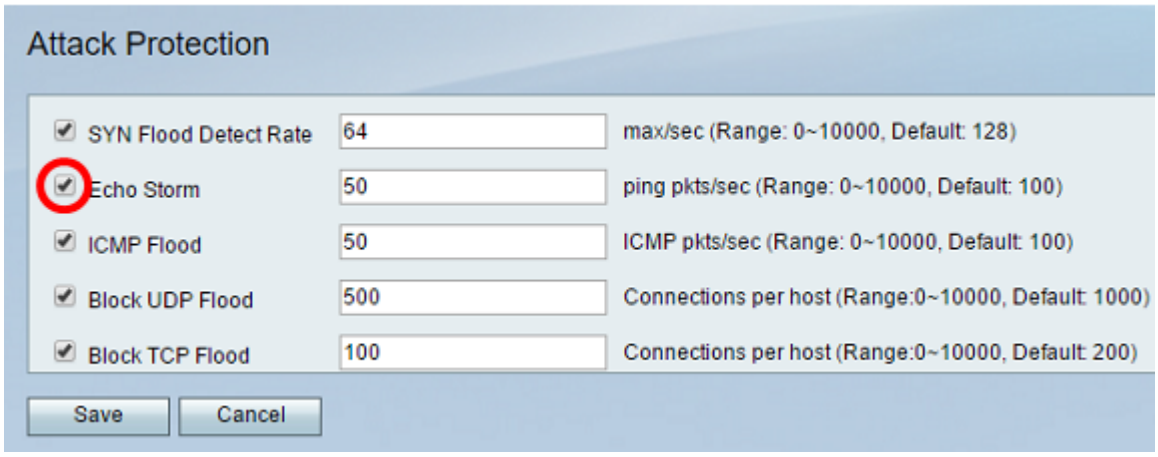
2단계. SYN Flood Detect Rate(SYN 플러드 탐지 속도) 확인란이 선택되어 있는지 확인하여 기능이 활성 상태인지 확인합니다. 기본적으로 선택되어 있습니다.



3단계. SYN Flood Detect Rate(SYN 플러드 *탐지 속도) 필드에 값을* 입력합니다. 기본값은 초당 128개의 SYN 패킷입니다. 0에서 10000 사이의 값을 입력할 수 있습니다. 보안 어플라이언스에서 SYN 플러드 침입 여부를 확인하게 하는 초당 SYN 패킷 수입니다. 값이 0이면 SYN 플러드 탐지 기능이 비활성화되었음을 나타냅니다. 이 예에서 입력한 값은 64입니다. 이는 어플라이언스가 SYN 플러드 침입을 초당 64개의 SYN 패킷으로만 탐지하므로 기본 컨피그레이션보다 더 민감하게 만든다는 것을 의미합니다.

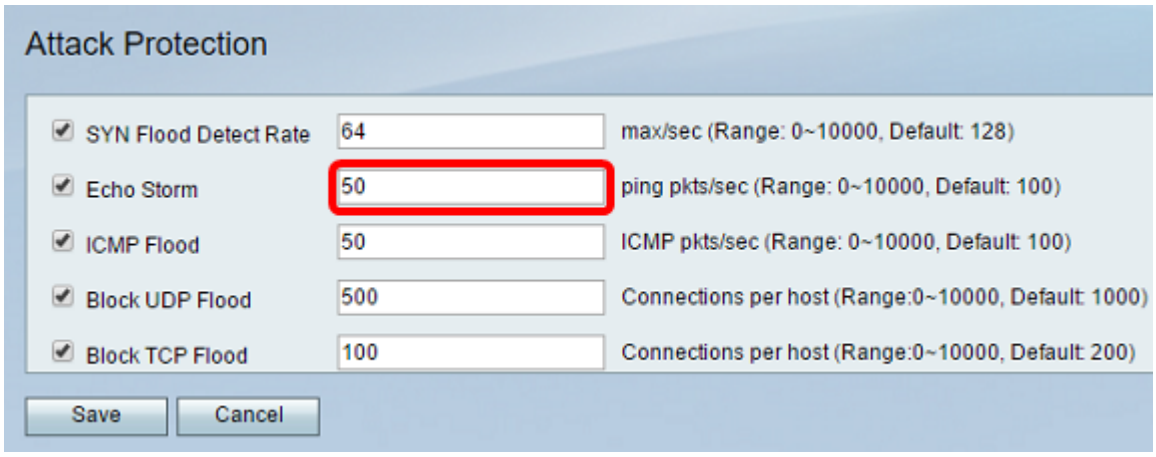


4단계. Echo Storm(에코 스톰) 확인란이 선택되어 있는지 확인하여 기능이 활성화되어 있는지 확인합니다. 기본적으로 선택되어 있습니다.

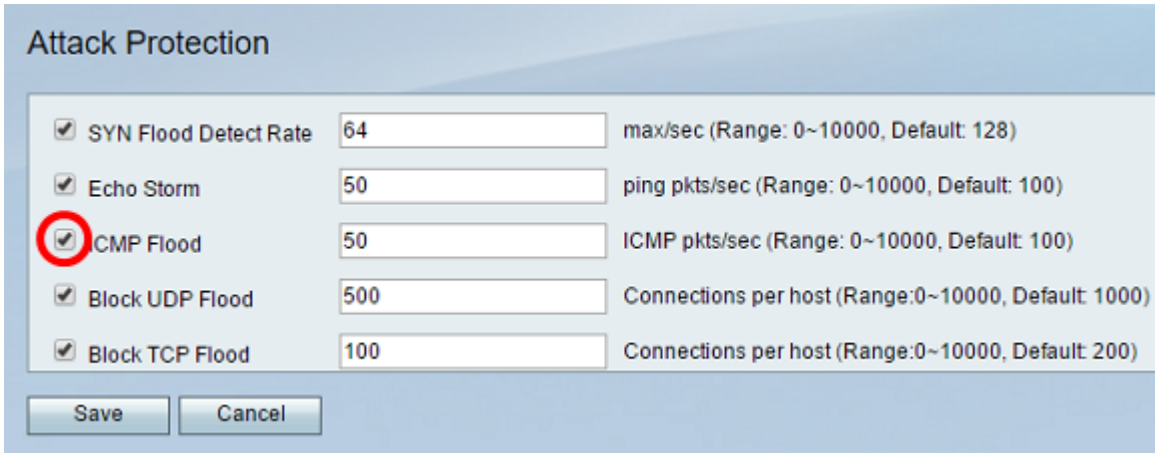


5단계. Echo Storm(에코 스톰) 필드에 *값을* 입력합니다. 기본값은 초당 100ping입니다. 0에서 10000 사이의 값을 입력할 수 있습니다. 보안 어플라이언스에서 에코 스톰 침입 이벤트가 발생하는지 확인하게 하는 초당 ping 수입니다. 값이 0이면 에코 스톰 기능이 비활성화되었음을 나타냅니다.

참고: 이 예에서 어플라이언스는 Echo Storm 이벤트를 초당 50ping으로만 탐지합니다.

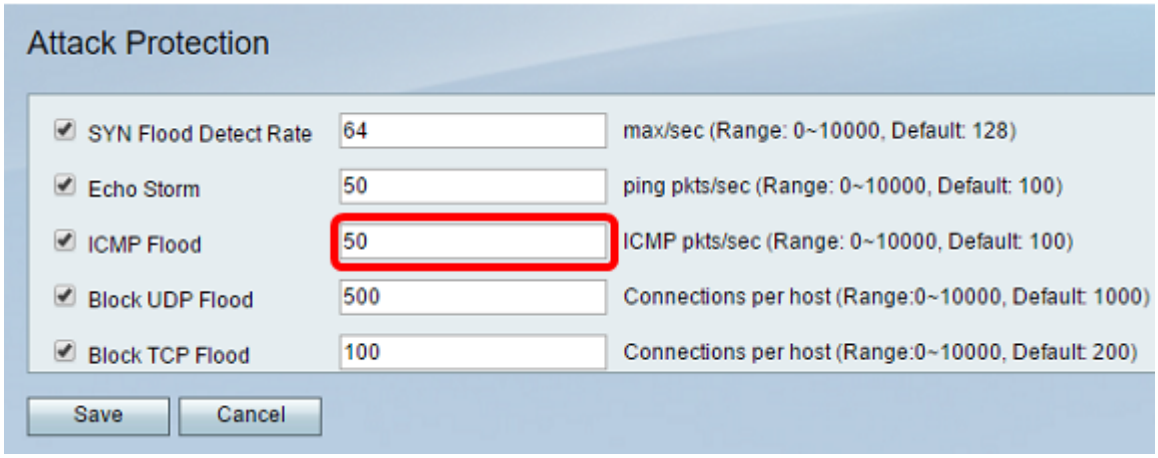


6단계. ICMP(Internet Control Message Protocol) 플러드 확인란이 선택되어 있는지 확인하여 기능이 활성화되어 있는지 확인합니다. 이 기능은 기본적으로 선택되어 있습니다.

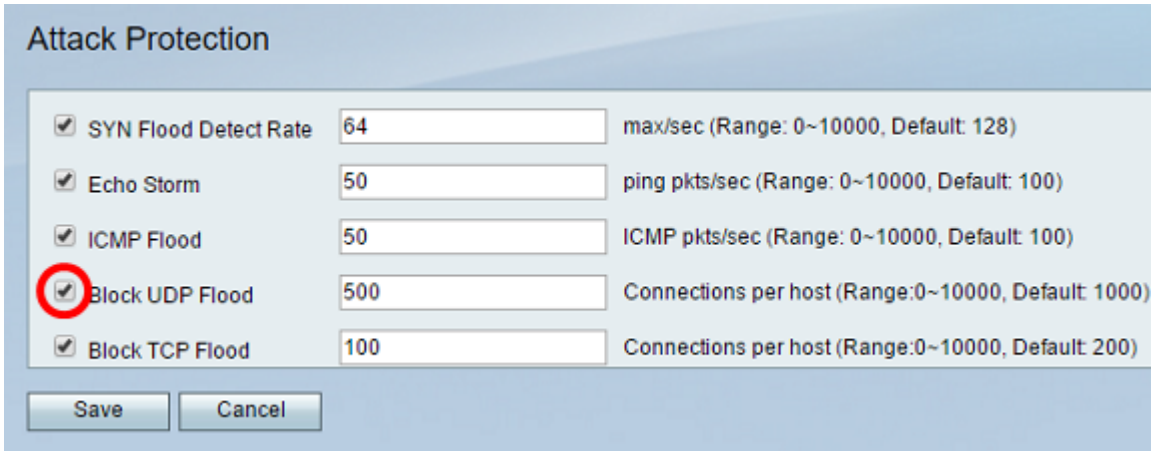


7단계. *ICMP* Flood 필드에 숫자 *값을* 입력합니다. 기본값은 초당 100개의 ICMP 패킷입니다. 0에서 10000 사이의 값을 입력할 수 있습니다. 보안 어플라이언스에서 ICMP 플러드 침입 이벤트가 발생하는지 확인하게 하는 초당 ICMP 패킷 수입니다. 값이 0이면 ICMP 플러드 기능이 비활성화되었음을 나타냅니다.

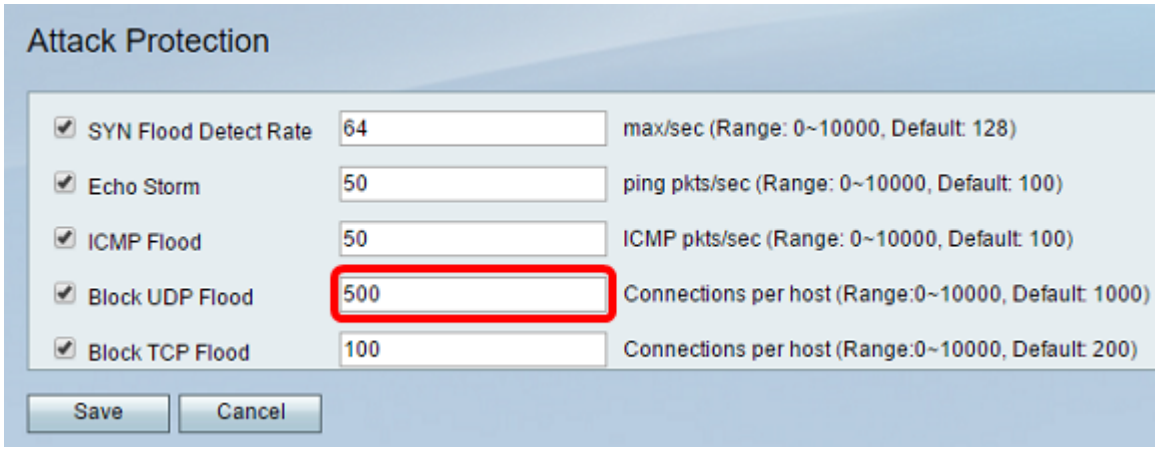
참고: 이 예에서 입력한 값은 50이므로 기본 설정보다 ICMP 플러딩에 더 민감합니다.



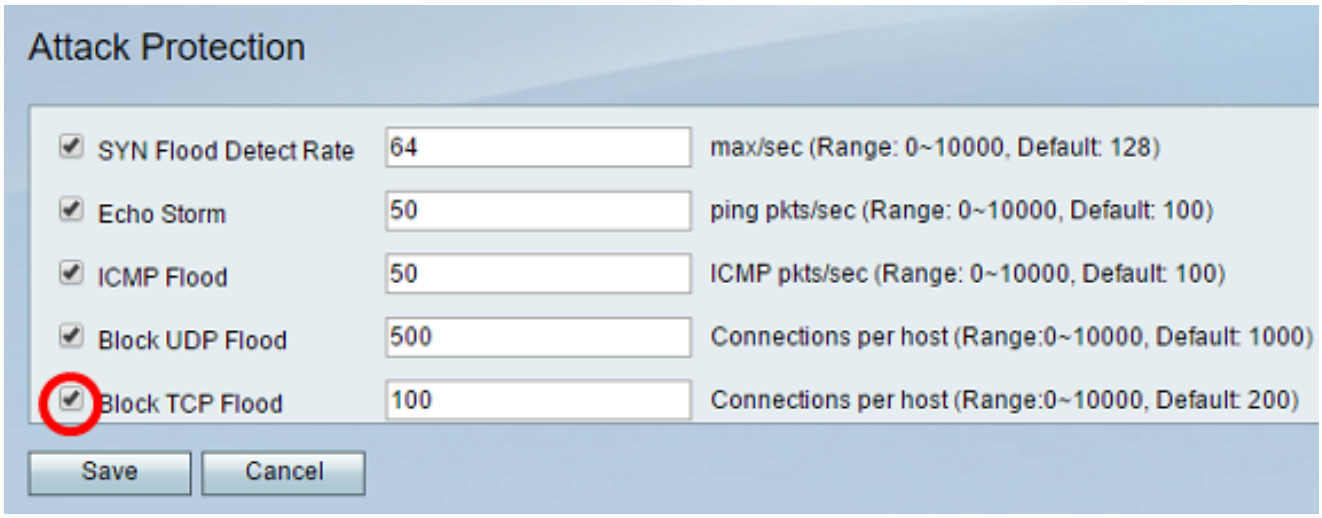
8단계. Block UDP Flood(UDP 플러드 차단) 확인란이 선택되어 있는지 확인하여 기능이 활성 상태인지 확인하고, 보안 어플라이언스가 LAN(Local Area Network)의 단일 컴퓨터에서 초당 150개 이상의 활성 UDP(사용자 데이터그램 프로토콜) 연결을 동시에 수락하지 못하도록 합니다. 이 옵션은 기본적으로 선택되어 있습니다.



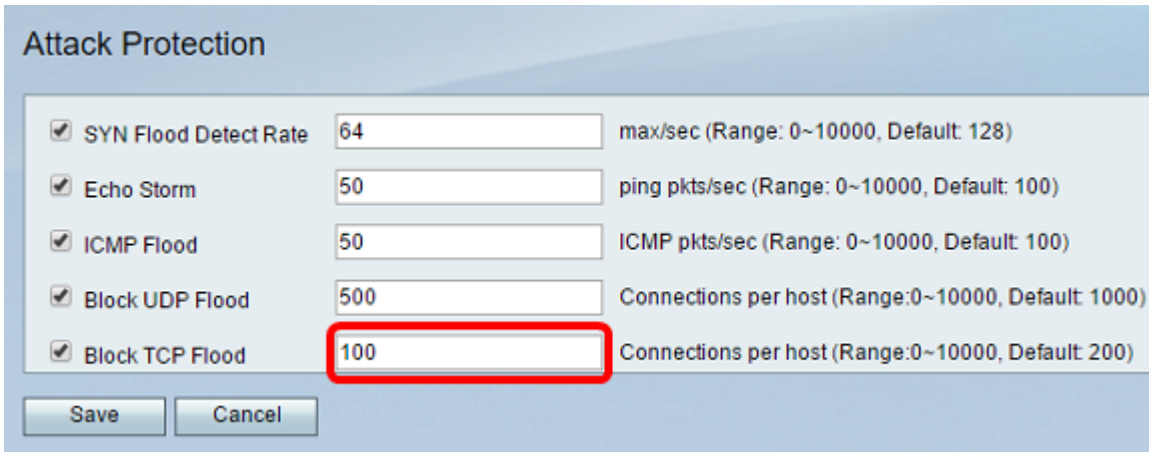
9단계. Block UDP Flood(UDP 플러드 차단) 필드에 0~10000*의 값을* 입력합니다. 기본값은 1000입니다. 이 예에서 입력한 값은 500이므로 더 민감합니다.



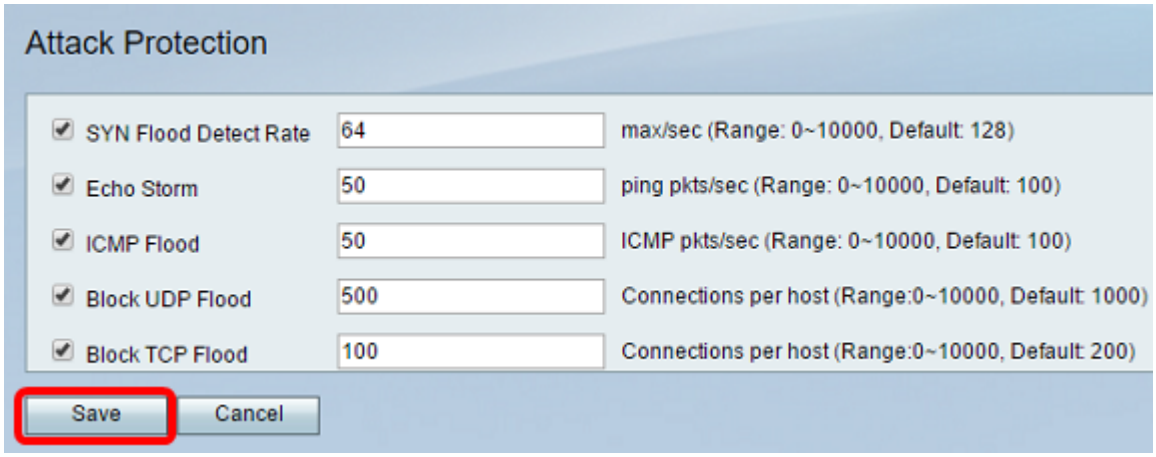
10단계. Block TCP Flood(TCP 플러드 차단) 확인란을 선택하여 유효하지 않은 모든 TCP(Transmission Control Protocol) 패킷을 삭제합니다. 이 옵션은 기본적으로 선택되어 있습니다.



11단계. SYN 플러드 공격으로부터 네트워크를 보호하려면 *Block TCP Flood(TCP 플러드* 차단) 필드에 0~10000의 값을 입력합니다. 기본값은 200입니다. 이 예제에서는 100을 입력하여 더 민감하게 만듭니다.



12단계. 저장을 **클릭합니다**.



이제 RV132W 또는 RV134W 라우터에 공격 보호를 성공적으로 구성했어야 합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.