RV320 및 RV325 라우터의 기본 방화벽 구성

목표

이 문서에서는 RV32x VPN Router Series에서 기본 방화벽 설정을 구성하는 방법에 대해 설명합니다.

방화벽은 네트워크를 안전하게 유지하기 위해 설계된 기능 집합입니다.라우터는 강력한 하드웨어 방화벽으로 간주됩니다.이는 라우터가 모든 인바운드 트래픽을 검사하고 원치 않는 패킷을 삭제할 수 있기 때문입니다.네트워크 방화벽은 외부의 악성 액세스로부터 내부 컴퓨터 네트워크(가정, 학교, 비즈니스 인트라넷)를 보호합니다.네트워크 방화벽은 내부 사용자의 외부 액세스를 제한하도록 구성할 수도 있습니다.

적용 가능한 디바이스

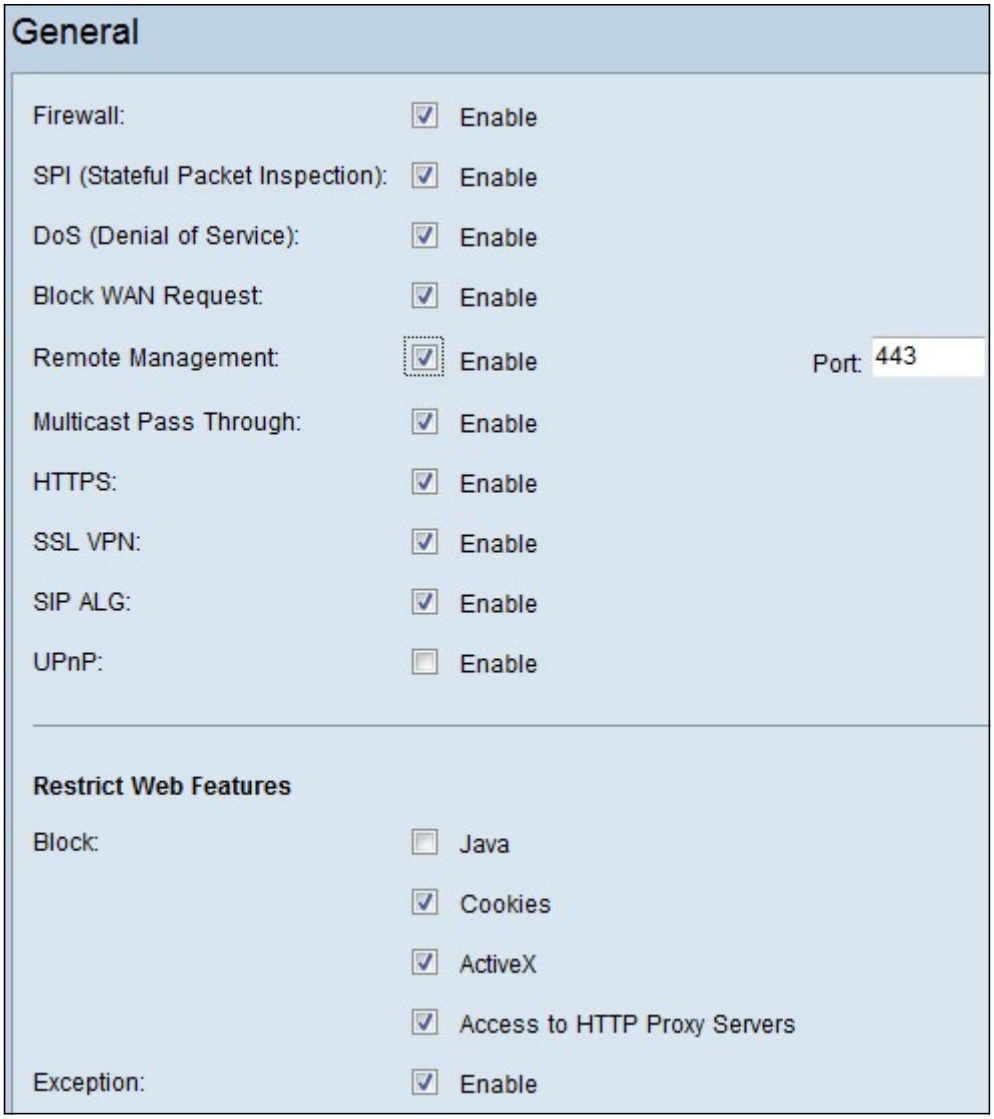
- RV320 Dual WAN VPN Router
- RV325 Gigabit Dual WAN VPN Router

소프트웨어 버전

- v1.1.0.09

기본 설정

1단계. 웹 구성 유틸리티에 로그인하고 **Firewall > General**을 선택합니다.[*일반 사항*] 페이지가 열립니다.



2단계. 요구 사항에 따라 활성화하려는 기능**에** 해당하는 활성화 확인란을 선택합니다.

- 방화벽 — 라우터 방화벽을 해제(비활성화)하거나, 특정 유형의 네트워크 트래픽을 필터링(방화벽 규칙이라고 함)할 수 있습니다. 방화벽을 사용하여 모든 수신 및 발신 트래픽을 필터링하고 기반으로 할 수 있습니다.
- SPI(Stateful Packet Inspection) — TCP 스트림 및 UDP 통신 같은 네트워크 연결의 상태를 모니터링합니다. 방화벽은 서로 다른 연결 유형에 대해 합법적인 패킷을 구별합니다.알려진 활성 연결과 일치하는 패킷만 방화벽에서 허용되며 다른 모든 패킷은 거부됩니다.
- DoS(서비스 거부) — DDoS(Distributed Denial of Service) 공격으로부터 네트워크를 보호하는 데 사용됩니다.DDoS 공격은 네트워크의 리소스를 사용할 수 없게 되는 지점까지 네트워크를 플러딩하는 것입니다.RV320은 DoS 보호를 사용하여 원치 않는 패킷의 제한 및 제거를 통해 네트워크를 보호합니다.
- Block WAN Request(WAN 요청 차단) - WAN 포트에서 라우터에 대한 모든 ping 요청을 차단합니다.
- 원격 관리 — 원격 WAN 네트워크에서 라우터에 액세스할 수 있습니다.
  - 포트 — 원격으로 관리할 포트 번호를 입력합니다.
- Multicast Pass Through — IP 멀티캐스트 메시지가 디바이스를 통과하도록 허용합니다.
- HTTPS(Hypertext Transfer Protocol Secure) — 컴퓨터 네트워크를 통한 안전한 통신을 위한 통신 프로토콜입니다.클라이언트와 서버에서 양방향 암호화를 제공합니다.
- SSL VPN — 라우터를 통해 SSL VPN 연결을 허용합니다.
- SIP ALG — SIP ALG는 NAPT(Network Address and Port Translation)를 사용할 때 방화벽의

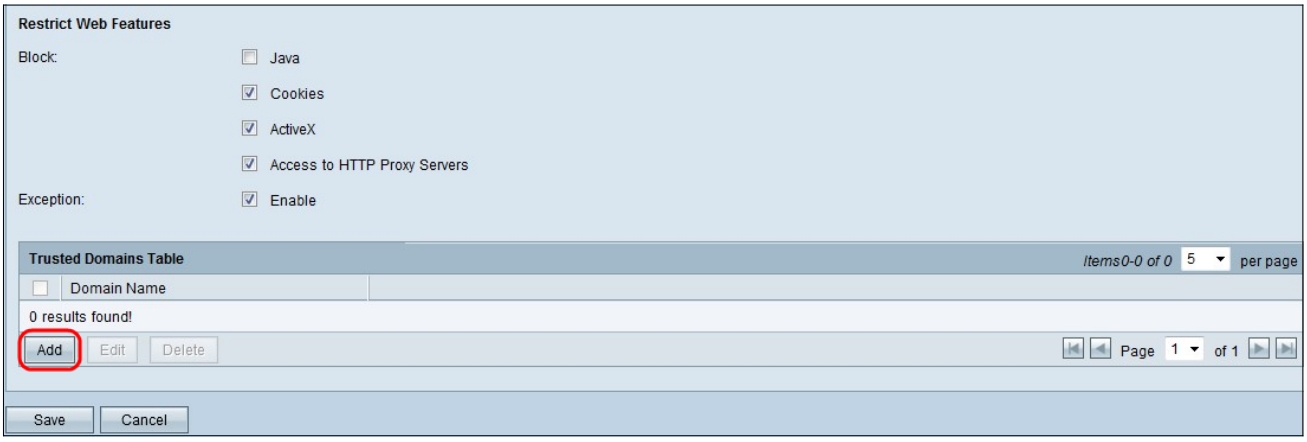
사설 및 공용, 사설 측으로 이동하는 Voice-over-IP 트래픽을 허용하는 기능을 제공합니다 .NAPT는 가장 일반적인 네트워크 주소 변환 유형입니다.
- UPnP(Universal Plug and Play) — 라우터와 통신할 수 있는 디바이스를 자동으로 검색할 수 있습니다.

3단계. 요구 사항에 따라 차단할 기능에 해당하는 **사용** 확인란을 선택합니다.

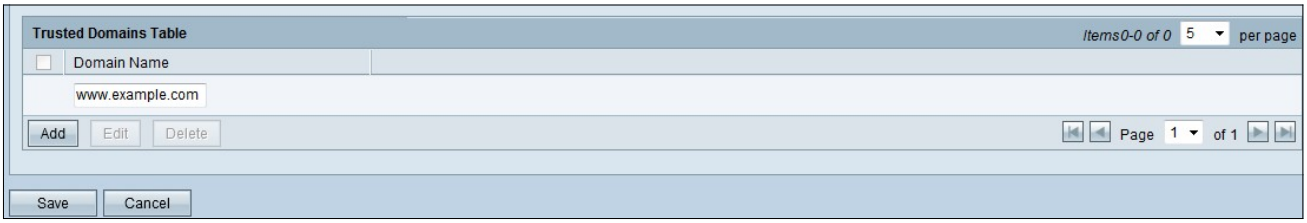
- Java — 이 확인란을 선택하면 Java 애플릿이 다운로드 및 실행되지 않습니다.Java는 많은 웹 사이트에서 사용되는 공통 프로그래밍 언어입니다.그러나 악의적인 목적을 위해 만들어진 Java 애플릿은 네트워크에 보안 위협이 될 수 있습니다.다운로드되면 적대적인 Java 애플릿이 네트워크 리소스를 악용할 수 있습니다.
- 쿠키 — 쿠키는 사용자 정보를 저장하기 위해 웹 사이트에 의해 생성됩니다.쿠키는 사용자의 웹 기록을 추적하여 개인 정보 침해로 이어질 수 있습니다.
- ActiveX — ActiveX는 많은 웹 사이트에서 사용되는 애플릿 유형입니다.일반적으로 안전하지만 컴퓨터에 악성 ActiveX 애플릿이 설치되면 사용자가 할 수 있는 모든 작업을 수행할 수 있습니다.운영 체제에 유해한 코드를 삽입하거나 보안 인트라넷을 검색하거나 암호를 변경하거나 문서를 검색하고 보낼 수 있습니다.
- HTTP 프록시 서버에 액세스 — 프록시 서버는 두 개별 네트워크 간에 링크를 제공하는 서버입니다.악성 프록시 서버는 로그인 또는 비밀번호와 같이 암호화되지 않은 데이터를 기록할 수 있습니다.
- 예외 — 선택한 기능(Java, Cookies, ActiveX 또는 HTTP 프록시 서버에 대한 액세스)을 허용하되 구성된 트러스트된 도메인에서 선택되지 않은 모든 기능을 제한합니다.신뢰할 수 있고 신뢰할 수 있는 네트워크에 액세스할 수 있는 도메인입니다.외부 도메인의 사용자가 네트워크 리소스에 액세스할 수 있도록 하는 신뢰할 수 있는 도메인을 설정할 수 있습니다.이 옵션을 비활성화하면 신뢰할 수 있는 도메인에서 모든 기능을 허용합니다.

참고:시간 절약 모드: 예외 확인란을 선택하지 않은 경우 4단계를 건너뜁니다.

4단계. Add(추가)를 클릭하고 새 Trusted Domain(신뢰할 수 있는 도메인)을 입력한 다음 Save(저장)를 클릭하여 신뢰할 수 있는 도메인을 생성합니다.

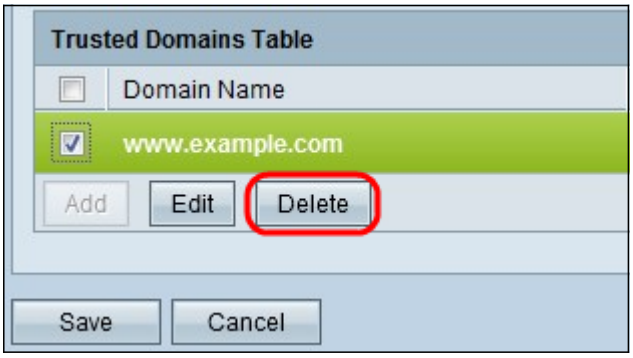


5단계. Save(저장)를 클릭하여 변경 사항을 업데이트합니다.



6단계. (선택 사항) Trusted Domain의 이름을 수정하려면 편집할 트러스트된 도메인의 확인란을 선택하고 Edit(편집)를 클릭한 다음 도메인 이름을 편집하고 Save(저장)를 클릭합니다.

7단계. (선택 사항) Trusted Domain(신뢰할 수 있는 도메인) 목록에서 도메인을 삭제하려면 삭제할 트러스트된 도메인의 확인란을 선택하고 Delete(삭제)를 클릭합니다.



이 문서와 관련된 비디오 보기...

여기를 클릭하여 Cisco의 다른 기술 대화를 확인하십시오.