RV34x Series 라우터에서 기본 방화벽 설정 구성

목표

이 문서의 목적은 RV34x Series Router에서 기본 방화벽 설정을 구성하는 방법을 설명하는 것입니다.

소개

방화벽의 주요 목적은 미리 결정된 규칙 집합에 따라 데이터 패킷을 분석하고 허용해야 하는지 여부를 결정하여 수신 및 발신 네트워크 트래픽을 제어하는 것입니다.인바운드 데이터의 필터링을 허용하는 기능으로 인해 라우터는 강력한 하드웨어 방화벽으로 간주됩니다.네트워크 방화벽은 보안 및 신뢰로 간주되는 내부 네트워크와 일반적으로 보안 및 신뢰 할 수 없는 것으로 간주되는 인터넷과 같은 외부 인터네트워크 사이에 브리지를 구축합니다.

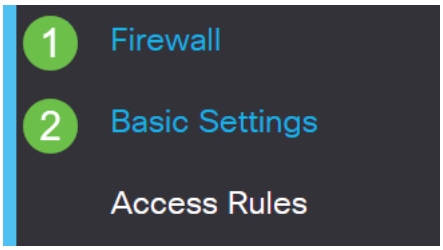
적용 가능한 디바이스 | 펌웨어 버전

- RV34x 시리즈 | 1.0.03.21 **(최신 버전 다운로드)**

기본 방화벽 설정 구성

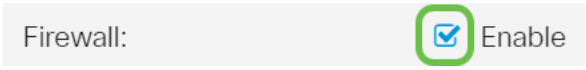
1단계

Web User Interface(UI)에 로그인하고 Firewall(방화벽) **>Basic Settings(기본 설정)를** 선택합니다.



2단계

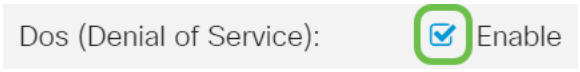
Enable Firewall(방화벽 **활성화**) 확인란을 선택하여 방화벽 기능을 활성화합니다.기본적으로 활성화되어 있습니다.



3단계

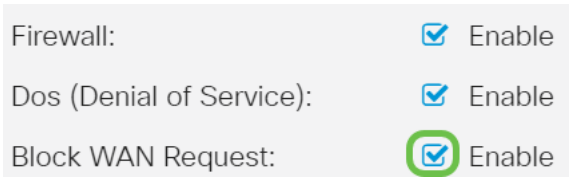
DoS 공격으로부터 네트워크를 보호하려면 Enable Dos (Denial of Service) 확인란을 선

택합니다.기본적으로 활성화되어 있습니다.



4단계

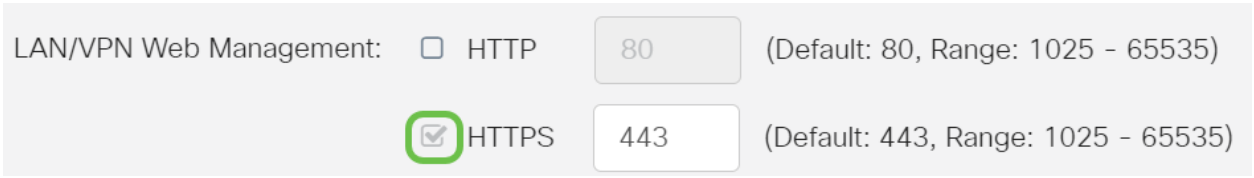
RV34x Series Router에 대한 ping 요청을 거부하려면 Enable Block WAN Request 확인란을 선택합니다.기본적으로 활성화되어 있습니다.



5단계

LAN/VPN Web Management(LAN/VPN 웹 관리) 영역에서 **HTTP** 및/또는 **HTTPS** 확인란을 선택하여 이러한 프로토콜의 트래픽을 활성화합니다.이 예에서는 HTTPS 확인란이 선택됩니다.

- HTTP — Hyper Text Transfer Protocol은 인터넷에서 사용되는 데이터 전송 프로토콜입니다.
- HTTPS — Hyper Text Transfer Protocol Secure는 보안 강화를 위해 패킷을 암호화하는 HTTP의 보안 버전입니다.

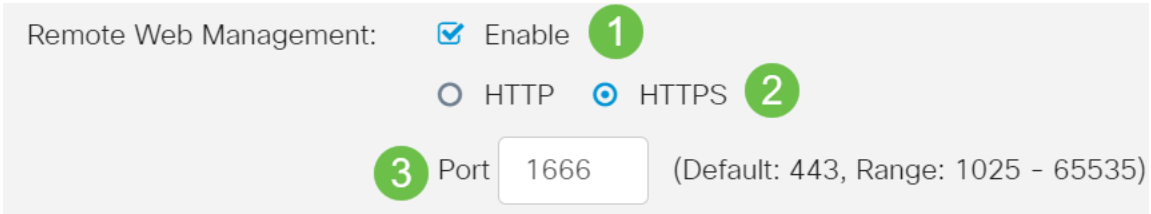


6단계(선택 사항)

원격 관리를 **활성화하려면** Enable Remote Web Management 확인란을 선택합니다.그렇지 않으면 8단계로 건너뜁니다.

라디오 버튼을 선택하여 방화벽에 연결하는 데 사용되는 프로토콜 유형을 선택합니다.옵션은 **HTTP** 및 **HTTPS입니다**.

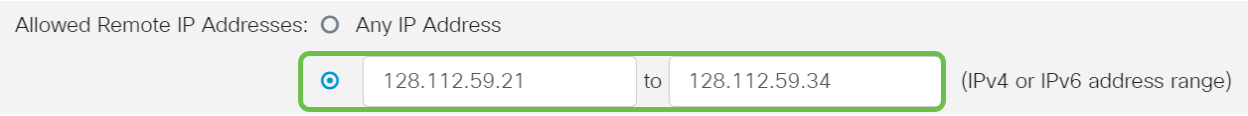
1025에서 65535 사이의 포트 번호를 입력하여 원격 관리가 가능합니다.기본값은 443입니다. 이 예에서는 1666이 사용됩니다.



7단계

Allowed Remote IP Addresses(허용된 원격 IP 주소) 영역에서 라디오 버튼을 선택하여 IP 주소가 원격으로 네트워크에 액세스하도록 허용하거나 IPv4 또는 IPv6 주소 범위를

지정합니다.이 예에서는 IP 범위가 선택되었습니다.이 예에서 시작 IP 주소는 128.112.59.21이고 끝 IP 주소는 128.112.59.34입니다.



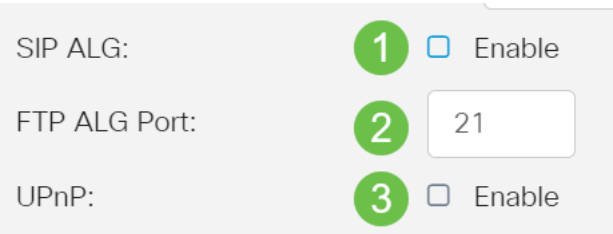
8단계(선택 사항)

Enable SIP **ALG(SIP** ALG) 확인란을 선택하여 SIP(Session Initiation Protocol) ALG(Application Layer Gateway)가 방화벽을 통과하도록 합니다.SIP 패킷이 방화벽을 통과하도록 이 기능을 활성화할 수 있습니다.SIP 패킷은 음성 트래픽의 연결을 시작하는 데 사용됩니다.VoIP 공급자가 다른 NAT(Network Address Translation) 접근 프로토콜을 사용하는 경우 이 기능을 사용하지 않도록 설정할 수 있습니다. 이는 기본 설정입니다.

FTP ALG Port(FTP ALG 포트) 필드에서 SIP ALG의 FTP(File Transfer Protocol) 포트를 지정합니다.기본값은 21입니다.

UPnP(Universal Plug and Play)를 활성화하려면 Enable UPnP 확인란을 선택합니다. 이 기능은 기본적으로 비활성화되어 있습니다.

이 예에서는 이러한 옵션이 비활성화되어 있습니다.



9단계(선택 사항)

Restrict Web Feature(웹 기능 제한) 영역에서 Block(차단) 영역에서 차단할 웹 기능 유형의 확인란을 선택합니다.이러한 확인란은 기본적으로 비활성화되어 있습니다.옵션은 다음과 같습니다.

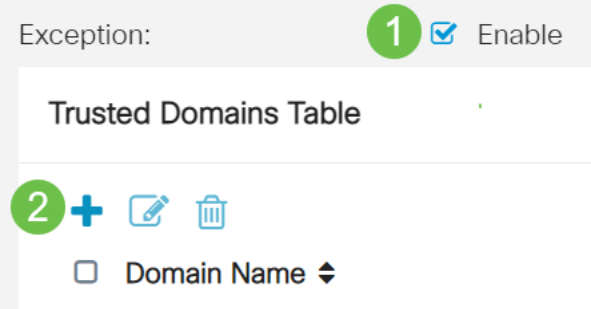
Java — 이 유형의 웹 요소를 포함하는 모든 웹 요소가 차단됩니다.이 설정은 Java 기반 웹 공격을 방지하는 데 도움이 됩니다.
쿠키 — 쿠키는 웹 사이트에서 해당 쿠키에 액세스하는 사용자를 파악하는 데 도움이 되도록 컴퓨터에 저장되는 데이터입니다. 쿠키를 차단하면 악의적인 쿠키가 데이터에 액세스하지 못하게 될 수 있습니다.
ActiveX — Microsoft에서 개발한 플러그인으로서 검색 환경을 개선합니다.이를 차단하면 악의적인 ActiveX 플러그인이 네트워크 장치를 손상시키는 것을 방지할 수 있습니다.
프록시 HTTP 서버에 액세스 — HTTP 프록시 서버는 최종 사용자의 세부 정보를 해커로부터 숨깁니다.고객은 중개인이 되어 인터넷에 직접 액세스하지 않습니다.그러나 로컬 사용자가 WAN 프록시 서버에 액세스할 수 있는 경우, 라우터에서 콘텐츠 필터를 중심으로 라우터에 의해 차단된 인터넷 사이트에 액세스하는 방법을 찾을 수 있습니다.

이 예에서는 확인란이 비활성화되어 있습니다.

11단계(선택 사항)

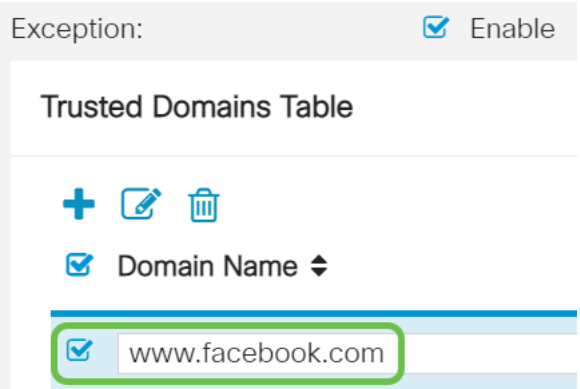
Java, Cookies, ActiveX 또는 Access to HTTP Proxy Servers(HTTP 프록시 서버에 대한 액세스)와 같은 선택한 웹 기능만 허용하고 나머지는 모두 제한하려면 Enable Exception(예외 **활성화**) 확인란을 선택합니다.기본적으로 비활성화되어 있습니다.이 예에서는 비활성화된 상태로 유지됩니다.

Trusted Domains Table(신뢰할 수 있는 도메인 테이블)에서 **추가 아이콘**을 클릭하여 네트워크에서 액세스할 수 있거나 신뢰할 수 있는 도메인을 추가합니다.



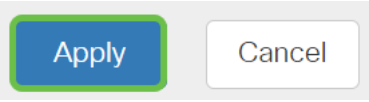
12단계

Domain *Name* 필드에 네트워크에 대한 액세스 권한을 부여할 도메인 이름을 입력합니다.이 예에서는 www.facebook.com가 사용됩니다.



13단계

Apply를 **클릭합니다**.



14단계(선택 사항)

컨피그레이션을 영구적으로 저장하려면 Copy/Save Configuration(컨피그레이션 복사/저장) 페이지로 이동하거나 페이지 상단에서 **저장 아이콘**을 클릭합니다.

결론

이제 RV34x Series Router에서 Basic Firewall Settings(기본 방화벽 설정)를 성공적으로 구성했어야 합니다.