RV215W의 기본 방화벽 설정 구성

목표

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.

이 문서에서는 RV215W에서 기본 방화벽 설정을 구성하는 방법에 대해 설명합니다.

적용 가능한 디바이스

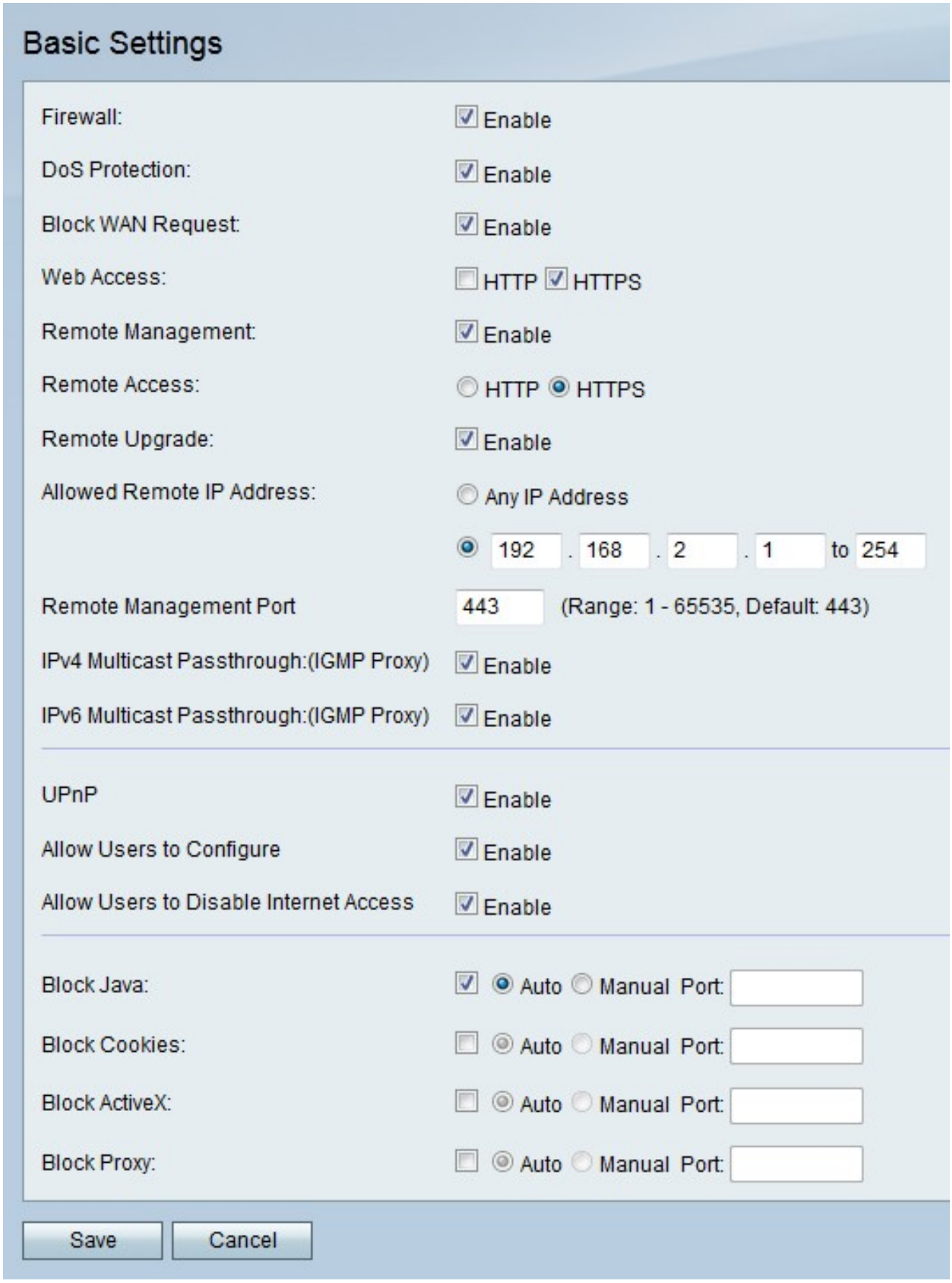
·RV215W

소프트웨어 버전

•1.1.0.5

기본 설정

1단계. 웹 구성 유틸리티에 로그인하고 **Firewall > Basic Settings**를 선택합니다.기본 *설정* 페이지가 열립니다.



2단계. RV215W에서 방화벽 컨피그레이션을 활성화하려면 Firewall(방화벽) 필드에서 Enable(활성화)을 선택합니다.

3단계. RV215W에서 DoS(서비스 거부) 보호를 활성화하려면 DoS Protection(DoS 보호) 필드에서 Enable(활성화)을 선택합니다.DoS 보호는 네트워크에서 DDoS(Distributed Denial of Service) 공격을 방지하는 데 사용됩니다.DDoS 공격은 네트워크의 리소스를 사용할 수 없게

되는 지점까지 네트워크를 플러딩하는 것입니다.RV215W는 DoS 보호를 사용하여 원치 않는 패킷의 제한 및 제거를 통해 네트워크를 보호합니다.

4단계. WAN에서 RV215W에 대한 모든 ping 요청을 차단하려면 Block WAN Request(**WAN** 요청 차단) 필드에서 Enable(활성화)을 선택합니다.

5단계. Web Access(웹 액세스) 필드에서 방화벽에 연결하는 데 사용할 수 있는 원하는 웹 액세스 유형에 해당하는 확인란을 선택합니다.

6단계. Remote Management(원격 관리) 필드에서 Enable(활성화)을 선택합니다.원격 관리를 통해 원격 WAN 네트워크에서 RV215W에 액세스할 수 있습니다.

7단계. Remote Access(원격 액세스) 필드의 원격 WAN에서 방화벽에 연결하는 데 사용할 수 있는 원하는 유형의 웹 액세스에 해당하는 라디오 버튼을 클릭합니다.

8단계. **원격** 사용자가 RV215W를 업그레이드할 수 있도록 하려면 Remote Upgrade(원격 업그레이드)를 선택합니다.

9단계. Allowed Remote IP Address(허용된 원격 IP 주소) 필드에서 RV215W에 원격으로 액세스할 수 있는 원하는 IP 주소에 해당하는 라디오 버튼을 클릭합니다.

·모든 IP 주소 — 모든 IP 주소가 허용됩니다.

·IP 주소 — 허용되는 IP 주소 범위를 입력합니다.

10단계. 원격 관리 포트 필드에 원격 액세스가 허용되는 포트를 입력합니다.원격 사용자는 원격 포트를 사용하여 디바이스에 액세스해야 합니다.

참고:원격 액세스 형식은 https://<*remote-ip*>:<*remote-port*>

11단계. IPv4 멀티캐스트 트래픽이 인터넷에서 RV215W를 통과하도록 허용하려면 IPv4 Multicast Passthrough 필드에서 Enable(활성화)을 선택합니다.IP 멀티캐스트는 단일 전송에서 지정된 수신자 그룹에 IP 데이터그램을 전송하는 데 사용되는 방법입니다.

12단계. IPv6 멀티캐스트 패스스루 필드에서 Enable(활성화)을 **선택하여** IPv6 멀티캐스트 트래픽이 인터넷에서 RV215W를 통과하도록 허용합니다.

13단계. UPnP 필드에서 Enable(활성화)을 선택하여 UPnP(Universal Plug and Play)를 활성화합니다.UPnP를 사용하면 RV215W와 통신할 수 있는 장치를 자동으로 검색할 수 있습니다.

14단계. Allow Users to Configure(사용자가 구성할 수 **있음**) 필드에서 Enable(활성화)을 선택하여 UPnP 지원 디바이스가 있는 사용자가 UPnP 포트 매핑 규칙을 구성할 수 있도록 허용합니다.포트 매핑 또는 포트 전달은 외부 호스트와 프라이빗 LAN 내에서 제공되는 서비스 간의 통신을 허용하는 데 사용됩니다.

15단계. 사용자가 장치에 대한 인터넷 액세스를 비활성화하도록 허용하려면 Allow Users to Disable Internet Access(사용자가 인터넷 액세스를 비활성화하도록 허용) 필드에서 Enable(활성화)을 선택합니다.

16단계. **Java 애플릿이** 다운로드되지 않도록 차단하려면 Block Java를 선택합니다.악의적인 목적을 위해 만들어진 Java 애플릿은 네트워크에 보안 위협이 될 수 있습니다.다운로드되면 적대적인 Java 애플릿이 네트워크 리소스를 악용할 수 있습니다.원하는 차단 방법에 해당하는 라디오 버튼을 클릭합니다.

·자동 — Java를 자동으로 차단합니다.

·수동 포트 — Java를 차단할 특정 포트를 입력합니다.

17단계. **쿠키** 차단을 선택하여 웹 사이트에서 만든 쿠키를 필터링합니다.쿠키는 이러한 사용자의 정보를 저장하기 위해 웹 사이트에 의해 생성됩니다.쿠키는 사용자의 웹 기록을 추적하여 개인 정보 침해로 이어질 수 있습니다.원하는 차단 방법에 해당하는 라디오 버튼을 클릭합니다.

·자동 — 쿠키를 자동으로 차단합니다.

·수동 포트 — 쿠키를 차단할 특정 포트를 입력합니다.

18단계. ActiveX **차단**을 선택하여 ActiveX 애플릿이 다운로드되지 않도록 차단합니다.ActiveX는 보안이 부족한 애플릿의 유형입니다.ActiveX 애플릿이 컴퓨터에 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.원하는 차단 방법에 해당하는 라디오 버튼을 클릭합니다.

·자동 — ActiveX를 자동으로 차단합니다.

·수동 포트 — ActiveX를 차단할 특정 포트를 입력합니다.

19단계. 프록시 **서버를** 차단하려면 프록시 차단을 선택합니다.프록시 서버는 두 개의 개별 네트워크 간에 링크를 제공하는 서버입니다.악성 프록시 서버는 로그인 또는 비밀번호와 같이 암호화되지 않은 데이터를 기록할 수 있습니다.원하는 차단 방법에 해당하는 라디오 버튼을 클릭합니다.

·자동 — 프록시 서버를 자동으로 차단합니다.

·수동 포트 — 프록시 서버를 차단할 특정 포트를 입력합니다.

20단계. 저장을 **클릭합니다**.