Firewall-instellingen configuratie op RV215W

Doel

Een firewall is een reeks functies die zijn ontworpen om een netwerk veilig te stellen. Een router wordt beschouwd als een sterke hardwarefirewall. Dit is te wijten aan het feit dat routers alle inkomende verkeer kunnen controleren en ongewenste pakketten kunnen drogen.

Dit artikel legt uit hoe u fundamentele firewallinstellingen op de RV215W kunt configureren.

Toepasselijke apparaten

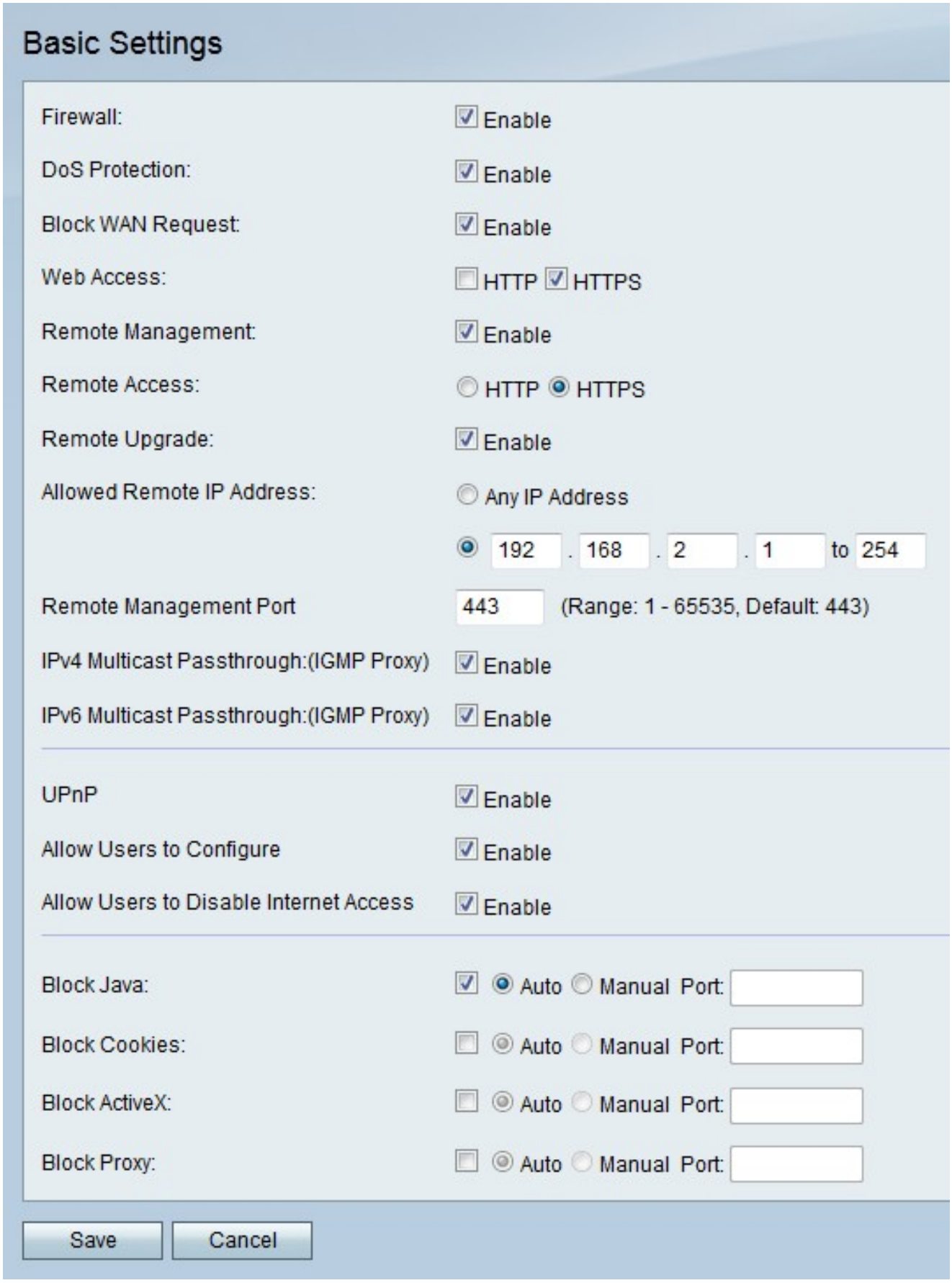
- RV215W

Softwareversie

•1.1.0.5

Basisinstellingen

Stap 1. Meld u aan bij het programma voor webconfiguratie en kies **Firewall > Basisinstellingen**. De pagina *Basisinstellingen* wordt geopend:



Stap 2. Controleer het veld Firewall in om firewallconfiguratie op RV215W **mogelijk** te maken.

Stap 3. Controleer het veld DoS **Protection** in om de bescherming tegen **Denial** of Service (DoS) op RV215W **mogelijk** te maken. Bescherm het netwerk wordt gebruikt om een netwerk van een gedistribueerde Denial of Service (DDoS) aanval te verhinderen. De aanvallen van

DDoS zijn bedoeld om een netwerk te overspoelen tot het punt waar de middelen van het netwerk niet beschikbaar worden. De RV215W gebruikt DoS-beveiliging om het netwerk te beschermen door beperkingen en verwijdering van ongewenste pakketten.

Stap 4. Controleer het veld WAN-aanvraag blokkeren om alle ping-verzoeken naar de RV215W vanuit WAN te blokkeren.

Stap 5. Controleer het aankruisvakje dat overeenkomt met het gewenste type webtoegang dat kan worden gebruikt voor een verbinding met de firewall in het veld Webtoegang.

Stap 6. Controleer het veld Afstandsbeheer inschakelen. Afstandsbeheer maakt toegang tot de RV215W mogelijk via een extern WAN-netwerk.

Stap 7. Klik op de radioknop die overeenkomt met het gewenste type webtoegang dat kan worden gebruikt voor de aansluiting op de firewall van het externe WAN in het veld Externe toegang.

Stap 8. Controleer upgrade op afstand om externe gebruikers in staat te stellen de RV215W te verbeteren.

Stap 9. Klik op de radioknop die overeenkomt met de gewenste IP-adressen die in het veld Toegestaan Remote IP-adres op afstand toegang tot de RV215W hebben.

- Alle IP-adressen zijn toegestaan.
- IP-adres - Voer een bereik in van IP-adressen die zijn toegestaan.

Stap 10. Voer een poort in waarop externe toegang is toegestaan in het veld Remote Management-poort. Een externe gebruiker moet de externe poort gebruiken om toegang tot het apparaat te krijgen.

Opmerking: Het formaat voor toegang op afstand is https://<*Remote-ip*>:<*Remote-poort*>

Stap 1. Controleer het veld IPv4-multicast passthrough in het geval om IPv4-multicast verkeer via RV215W via het internet te laten verlopen. IP multicast is een methode die wordt gebruikt om IP-datagrammen naar een aangewezen groep ontvangers in één transmissie te verzenden.

Stap 12. Controleer het veld Wachtwoord voor IPv6-multicast inschakelen om IPv6-multicast verkeer via RV215W via het internet te laten verlopen.

Stap 13. Controleer het veld UPnP in om Universal Plug and Play (UPnP) in te schakelen. UPnP maakt automatische ontdekking mogelijk van apparaten die met de RV215W kunnen communiceren.

Stap 14. Controleer de gebruikers in de Toeleveranciers om het veld te configureren om gebruikers met UPnP-kabelapparaten in staat te stellen de UPnP-poortregels te configureren. Port-mapping of poorttransport wordt gebruikt om communicatie tussen externe hosts en services mogelijk te maken die binnen een privaat LAN worden geleverd.

Stap 15. Controleer in het veld Toegang voor gebruikers toestaan om het veld Internet-toegang uit te schakelen om gebruikers de toegang tot het apparaat via het internet uit te schakelen.

Stap 16. Controleer Blok Java om te voorkomen dat er javepapieren worden gedownload. Java-applets die voor een kwaadaardige bedoeling zijn gemaakt, kunnen een

beveiligingsbedreiging voor een netwerk vormen. Wanneer je het hebt gedownload, kan een vijandige java-applet netwerkbronnen exploiteren. Klik op de radioknop die overeenkomt met de gewenste blokmethode.

- Auto — blokkeert automatisch java.
- Handmatige poort — Voer een specifieke poort in waarop u java wilt blokkeren.

Stap 17. Controleer **Cookies** op **blok** om koekjes te filteren van het creëren door een website. Cookies worden gemaakt door websites om informatie van deze gebruikers op te slaan. Cookies kunnen de webgeschiedenis van de gebruiker volgen, wat kan leiden tot een inbreuk op de privacy. Klik op de radioknop die overeenkomt met de gewenste blokmethode.

- Auto - blokkeert koekjes automatisch.
- Handmatige poort — Voer een specifieke poort in waarop je koekjes moet blokkeren.

Stap 18. Controleer **Blok ActiveX** om ActiveX-applets te blokkeren nadat u deze hebt gedownload. ActiveX is een type applet dat geen beveiliging heeft. Nadat een ActiveX-applet op een computer is geïnstalleerd, kan deze alles doen wat een gebruiker kan doen. Het kan schadelijke code in het besturingssysteem invoegen, op een beveiligd intranet surfen, een wachtwoord wijzigen of documenten herstellen en verzenden. Klik op de radioknop die overeenkomt met de gewenste blokmethode.

- Auto — Blokkeer automatisch ActiveX.
- Handmatige poort - Voer een specifieke poort in waarop u ActiveX wilt blokkeren.

Stap 19. Controleer **Blokproxy** om proxy-servers te blokkeren. Proxyservers zijn servers die een link tussen twee afzonderlijke netwerken bieden. Kwaadaardige proxy-servers kunnen alle niet-versleutelde gegevens die naar ze worden verzonden, zoals logins of wachtwoorden, opslaan. Klik op de radioknop die overeenkomt met de gewenste blokmethode.

- Auto — Blokkeer automatisch proxyservers.
- Handmatige poort — Voer een specifieke poort in waarop u proxy-servers wilt blokkeren.

Stap 20. Klik op **Opslaan**.