Access Control-configuratie voor de RV315W VPN-router

Doel

De configuratie van het toegangsbeheer staat toe om de toegang tot een specifiek IP-adres te beperken. Er zijn verschillende opties om de beperkingen aan te passen. Tijd van dag, dagen van de week, IP adressen, fysieke poort en type protocol zijn voorbeelden van enkele aanpassingseigenschappen voor het toegangsbeheerbeleid.

Dit artikel helpt uit te leggen hoe u toegangscontroles op de RV315W VPN-router kunt gebruiken en configureren.

Toepassbaar apparaat

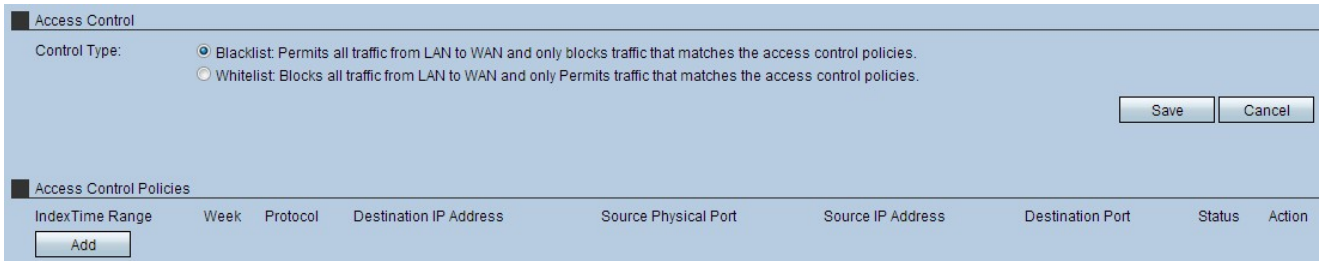
- RV315W

Softwareversie

•1.01.03

Configuratie-beheer

Stap 1. Meld u aan bij het web configuratie hulpprogramma en kies **Beveiliging > Toegangsbeheer**. De pagina *Toegangsbeheer* wordt geopend:



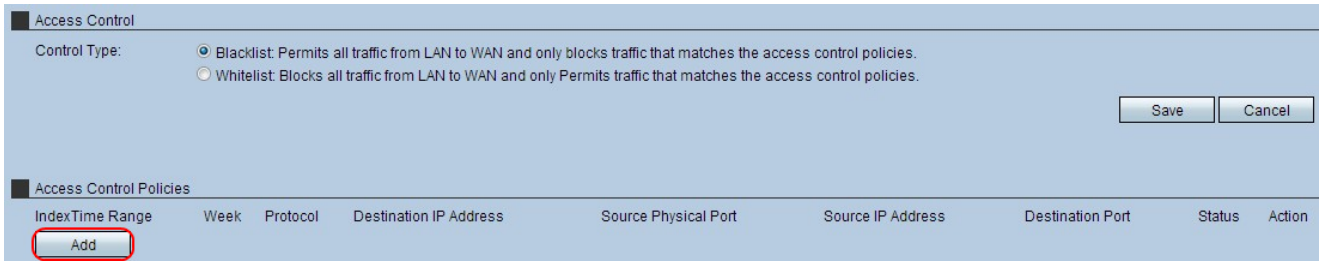
Stap 2. Klik op de lijst Blokken of de knop Lijst toestaan in het veld Type controle.

- Bloklijst - Met deze optie kunt u al het verkeer van LAN naar WAN blokkeren, behalve het verkeer dat door de toegangscontrole-instellingen is geblokkeerd.

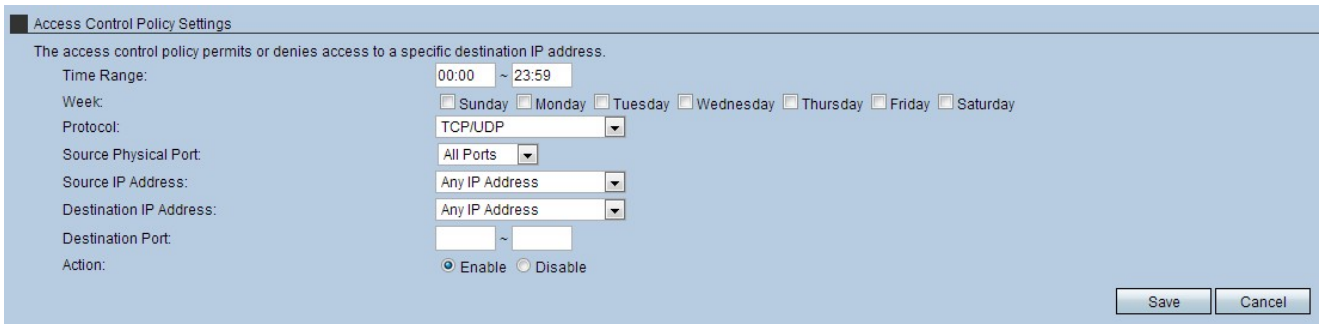
- Sta lijst toe — Deze optie blokkeert al het verkeer van LAN naar WAN, behalve het verkeer dat door de instellingen voor toegangscontrole is toegestaan.

Zie de woordenlijst voor aanvullende informatie.

Stap 3. Klik op **Save** om de instellingen toe te passen.



Stap 4. Klik op **Add** om een nieuw toegangsbeheerbeleid toe te voegen. De pagina *Instellingen toegangsbeleid* wordt geopend:



Stap 5. Voer een bereik in het veld Tijdbereik in. Deze optie is het moment waarop het beleid inzake toegangscontrole effectief is.

Stap 6. Selecteer de dagen van de week om de toegang toe te staan of te beperken. Deze optie is de dagen van de week waarin het beleid inzake toegangscontrole effectief is.

Stap 7. Kies in de vervolgkeuzelijst Protocol het protocol waarop de toegangscontrole van toepassing is.

- TCP — Dit protocol wordt gebruikt om gegevens van een toepassing naar het netwerk te verzenden. TCP wordt gewoonlijk gebruikt voor toepassingen waar de informatieoverdracht volledig moet zijn en pakketten niet worden ingetrokken.

- UDP — Dit protocol is voor client-/server-netwerktoepassingen gebaseerd op het Internet Protocol (IP). Dit protocol heeft als hoofddoel de toepassing van het protocol te vergemakkelijken. (VOIP, games enz.)

- TCP/UDP — Selecteer dit protocol om zowel TCP als UDP te gebruiken. Dit is het standaardprotocol.

- ICMP — Dit protocol verstuurt foutmeldingen en is verantwoordelijk voor foutenbehandeling in het netwerk. Gebruik dit protocol om een melding te krijgen wanneer het netwerk problemen heeft met de levering van pakketten.

- HTTP — Dit protocol biedt veilige communicatie tussen een webserver en browser. Gebruik dit protocol wanneer er een noodzaak is om pakketten veilig tussen een server en browser over te brengen.

- FTP - Dit protocol verzenden de bestanden tussen computers. Selecteer dit protocol wanneer bestanden tussen meerdere apparaten worden uitgewisseld.

- MTP — Dit protocol behandelt de verzending van e-mails. Selecteer dit protocol bij het uitwisselen van e-mails.

- POP3 — Dit protocol combineert met MTP wat betreft e-mail. POP3 downloads van een

e-mailserver naar een pc. Selecteer dit protocol bij het downloaden van e-mails.

Stap 8. Kies in de vervolgkeuzelijst Bron Physical Port de poort waarop de toegangscontrole van toepassing is.

Stap 9. Kies in de vervolgkeuzelijst Bron IP-adres het IP-adres waarop de toegangscontrole van toepassing is.

- Elk IP-adres - Kies deze optie om alle IP-adressen toe te staan of te ontkennen. Selecteer de selectieknop voor deze optie in- of uitschakelen.
- Eén IP-adres - Kies deze optie om afzonderlijke IP-adressen toe te staan of te ontkennen. Voer het toepasselijke IP-adres in het veld Bron IP-adres in.
- IP-adresbereik — Kies deze optie om IP-adressen op basis van een geselecteerd bereik toe te staan of te ontkennen. Geef het toepasselijke IP-adresbereik op in het veld eerste en tweede bron-IP-adres.

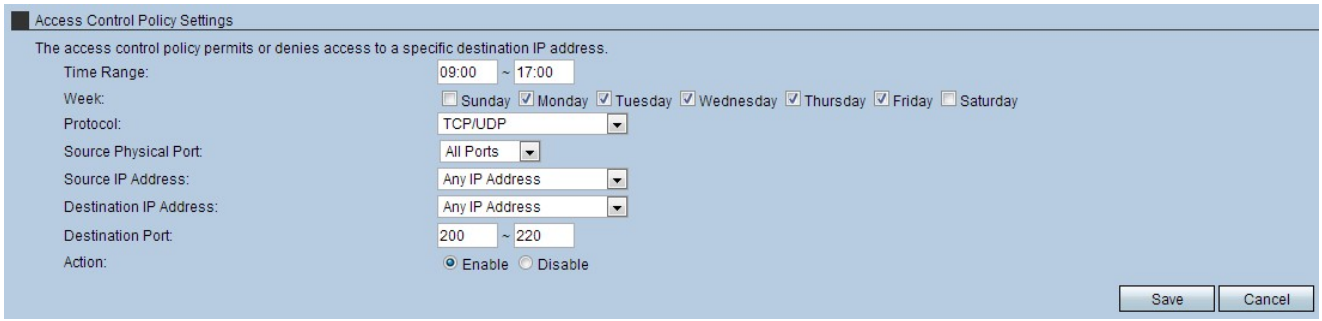
Stap 10. Kies in de vervolgkeuzelijst IP-adres van de bestemming het IP-adres waarop de toegangscontrole van toepassing is.

- Elk IP-adres - Kies deze optie om alle IP-adressen toe te staan of te ontkennen. Klik op de radioknop in- of uitschakelen voor deze optie.
- Eén IP-adres - Kies deze optie om een individueel IP-adres toe te staan of te ontkennen. Voer het toepasbare IP-adres in het veld IP-adres van de bestemming in.
- IP-adresbereik — Kies deze optie om IP-adressen op basis van een geselecteerd bereik toe te staan of te ontkennen. Geef het toepasselijke IP-adresbereik op in het veld eerste en tweede bestemming IP-adres.

Stap 11. Voer in de velden van de haven van bestemming het poortbereik in van een protocol of toepassing waarop de toegangscontrole van toepassing is.

Stap 12. Klik op de radioknop **Enable** om het toegangscontrolebeleid in te schakelen.

Stap 13. Klik op **Save** om de instellingen toe te passen.



Stap 14. (Optioneel) Klik om een toegangscontrolebeleid te verwijderen op het pictogram afval onder de kop Actie.

Stap 15. (Optioneel) Klik om een toegangscontrolebeleid te bewerken op het pictogram onder de kop Actie.