Configuratie van een IPv4-toegangsregel op RV016, RV042, RV042G en RV082 VPN-routers

Doel

Een toegangsregel helpt de router om, gebaseerd op het gebruikersvereiste, te bepalen welk verkeer mag worden doorgegeven en welk verkeer door de firewall moet worden ontkend. Dit helpt beveiliging aan de router toe te voegen.

Dit document legt de procedure uit om een toegangsregel toe te voegen of te verwijderen op de RV016-, RV042-, RV042G- en RV082 VPN-routers.

Toepasselijke apparaten

· RV016
â€¢RV042
· RV042G
· RV082

Softwareversie

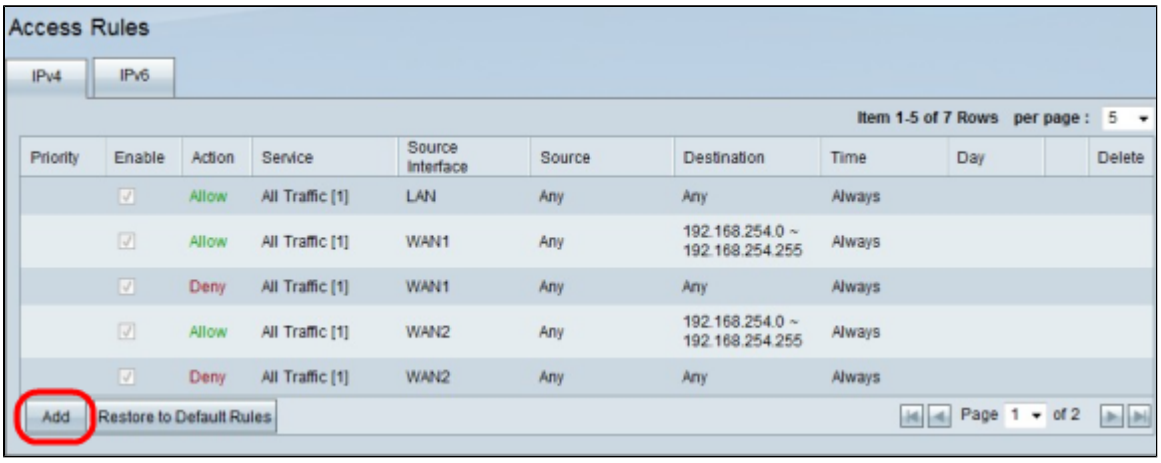
â€¢4.2.1.02

IPv4-toegangsregels beheren

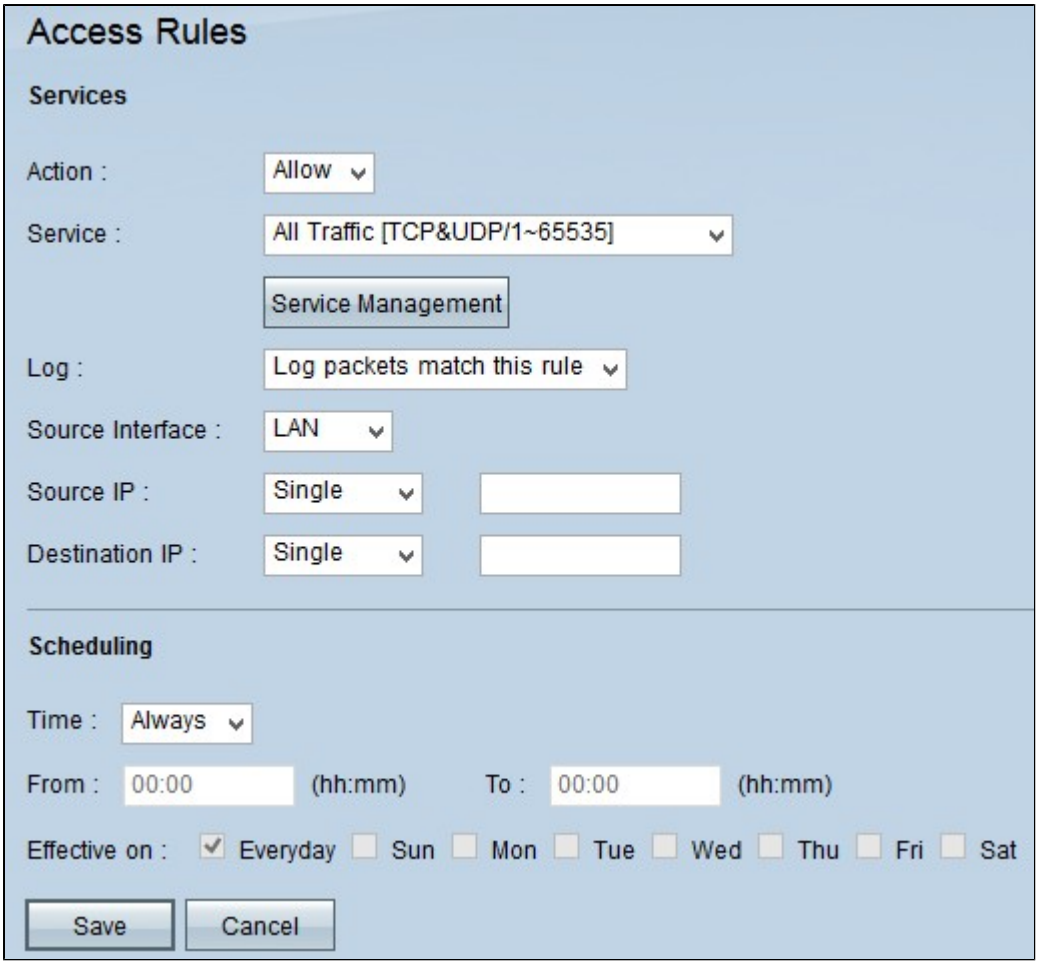
Het plannen van IPv4-toegangsregels is een optionele configuratie.

IPv4-toegangsregels toevoegen of verwijderen

Stap 1. Meld u aan bij het hulpprogramma voor webconfiguratie en kies **Firewall > Toegangsregels**. De pagina *IPv4-toegangsregels* wordt geopend. Klik op **Add** (Toevoegen).

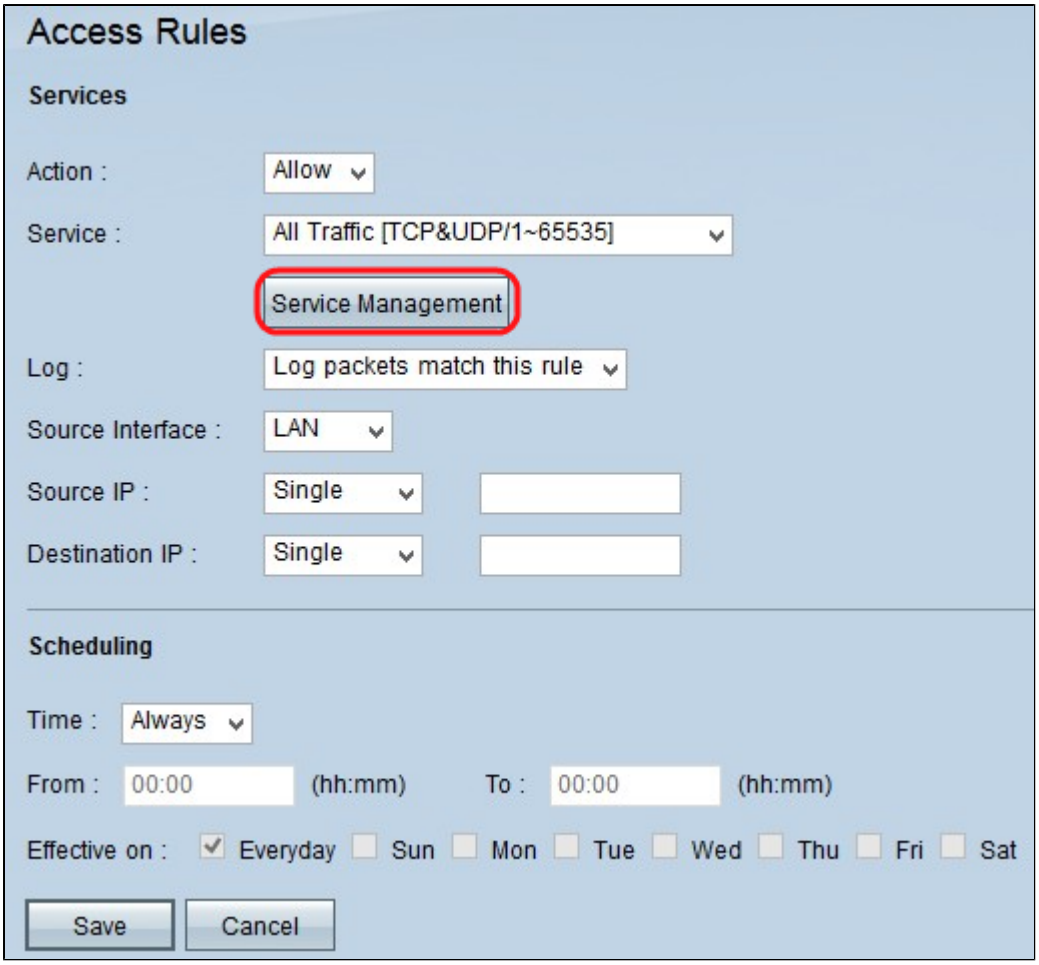


Stap 2. De *Servicepagina voor toegangsregels* wordt geopend. Selecteer in de vervolgkeuzelijst Actie de optie **Toestaan** om het verkeer toe te staan. Anders, kies **Deny** om het verkeer te ontkennen.



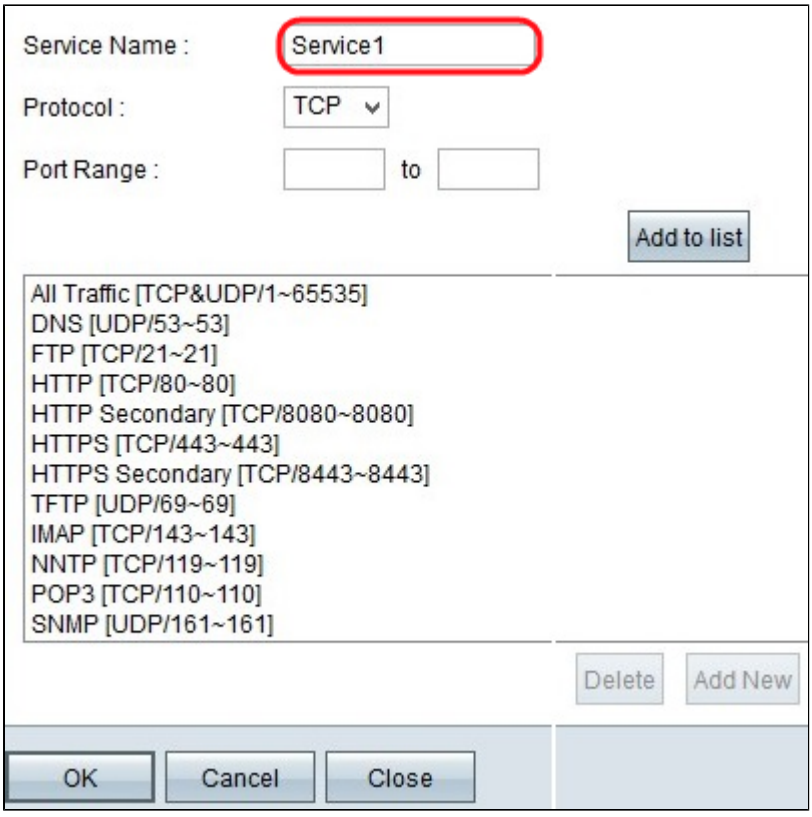
Stap 3. Kies de juiste service uit de vervolgkeuzelijst Service. Als de juiste service niet beschikbaar is, klikt u op **Servicebeheer.**

Opmerking: als de gewenste service beschikbaar is, gaat u naar Stap 6.



Stap 4.

Er verschijnt een nieuw venster. Voer een servicenaam in het veld Servicenaam in.

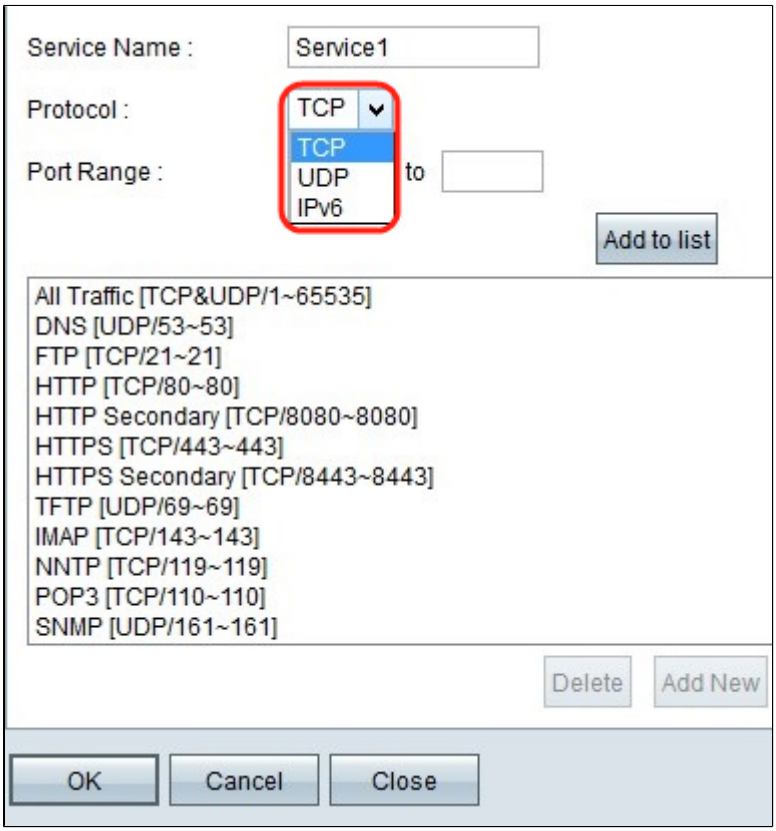


Stap 5. Kies het juiste protocoltype in de vervolgkeuzelijst Protocol.

· TCP (Transmission Control Protocol) â€" Een transportlaagprotocol dat wordt gebruikt door toepassingen die een gegarandeerde levering vereisen.

· UDP (User Datagram Protocol) â€" Gebruikt datagramsockets om host-to-host communicatie tot stand te brengen. Het is sneller dan TCP maar niet zo waarschijnlijk om succesvol te leveren.

· IPv6 (Internet Protocol versie 6) â€" Leidt internetverkeer tussen hosts in pakketten die worden gerouteerd over netwerken die door routering van adressen worden gespecificeerd.

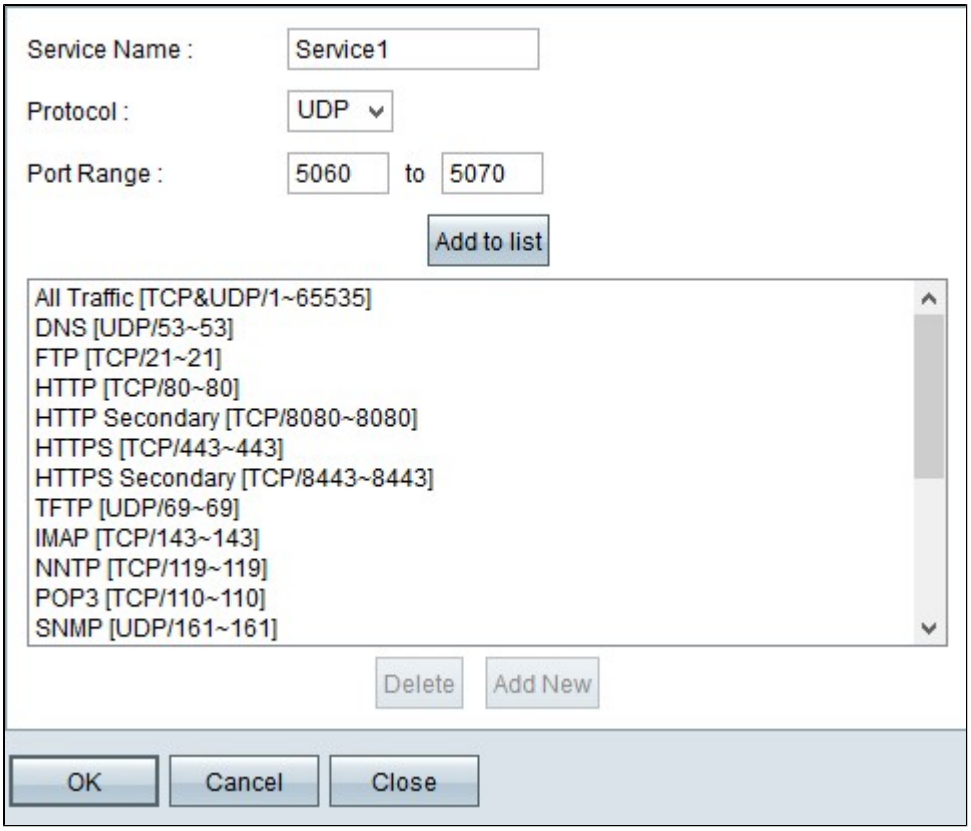


Stap 6. Voer het poortbereik in in de velden Poortbereik. Dit bereik is afhankelijk van het gekozen protocol.

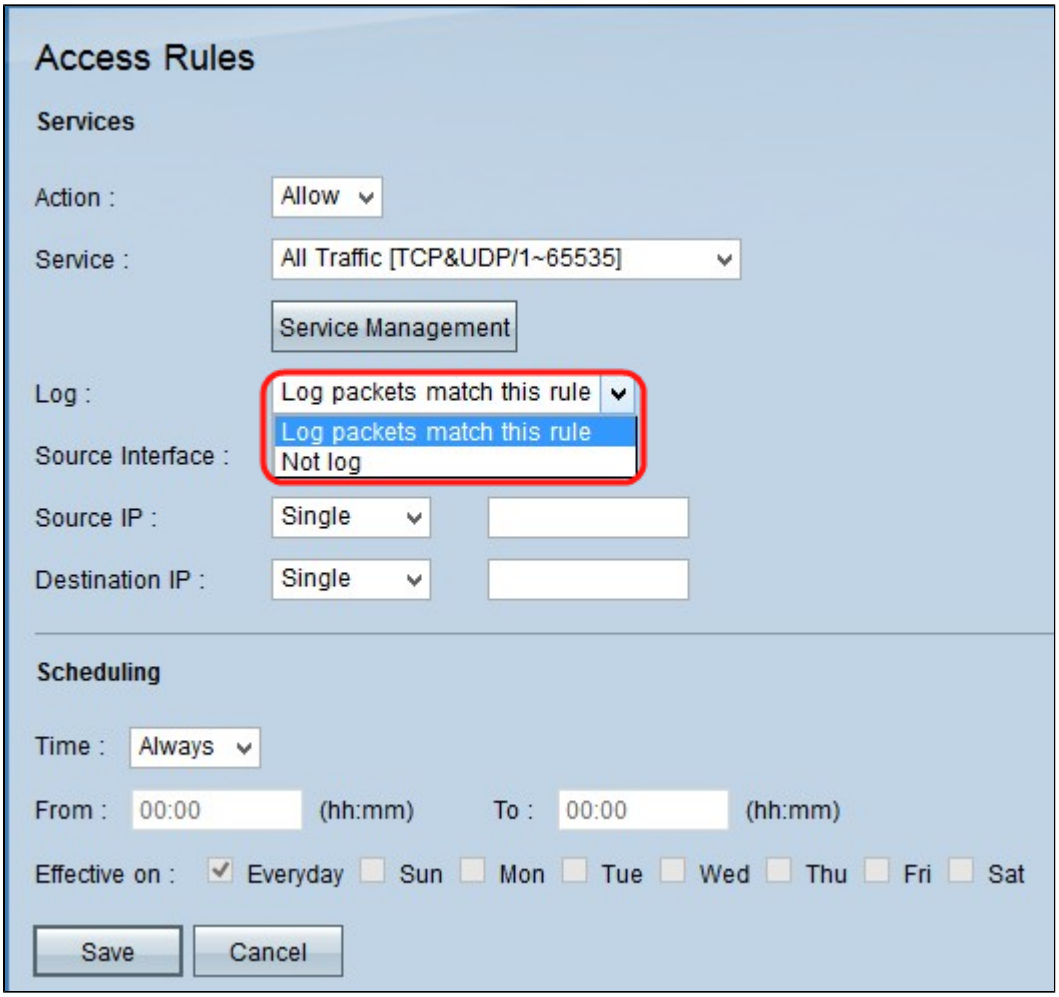
Klik op **Toevoegen aan lijst**. Hiermee wordt de Service toegevoegd aan de vervolgkeuzelijst Service.

Andere opties zijn **Verwijderen**, **Bijwerken** of **Nieuw toevoegen**.

Klik op **OK**. Hiermee wordt het venster gesloten en wordt de gebruiker teruggebracht naar de pagina *Access Rule Service*.



Stap 7. Kies in de vervolgkeuzelijst Log **pakketten** die **overeenkomen met deze regel** om de inkomende pakketten te registreren die overeenkomen met de toegangsregel. Anders, kies **Niet Loggen**.



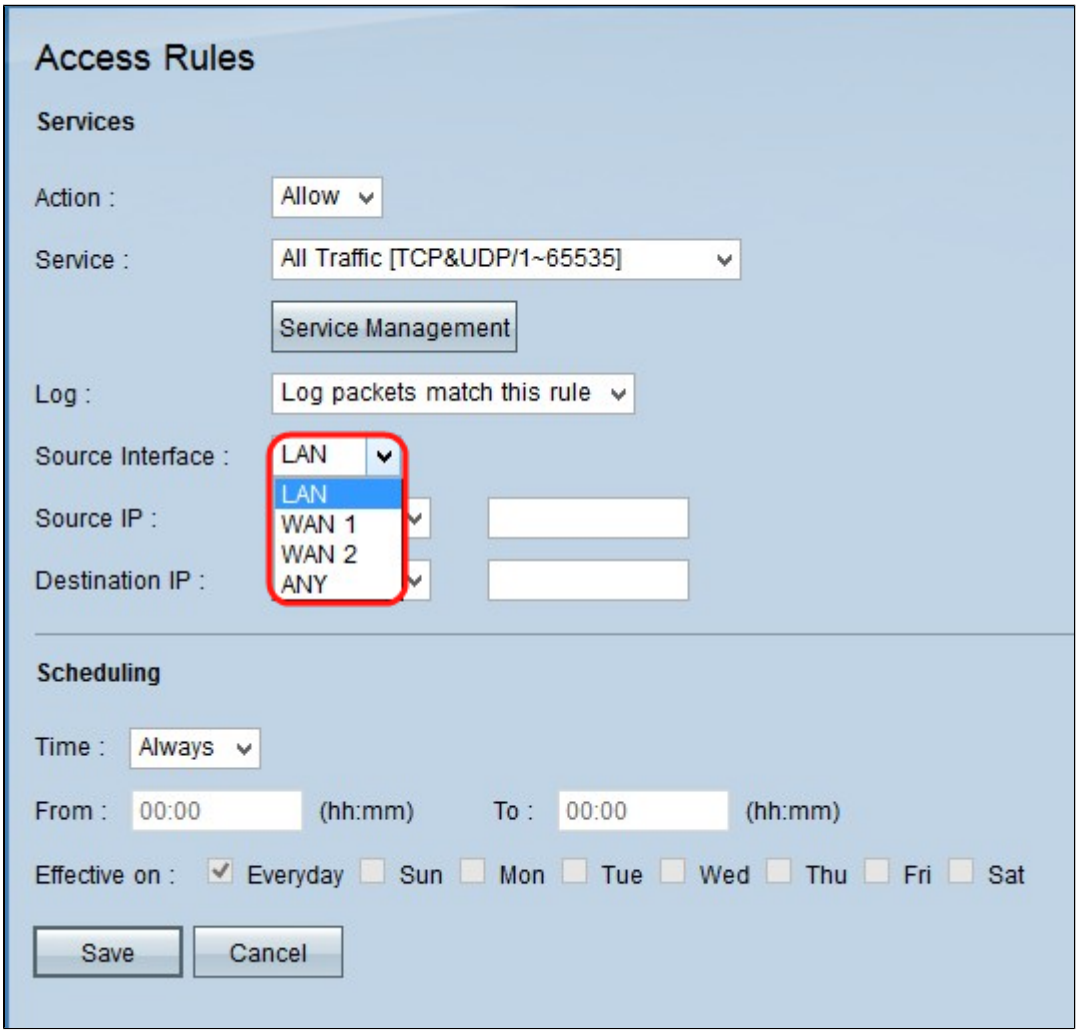
Stap 8. Kies de interface die door deze regel wordt beïnvloed uit de vervolgkeuzelijst Source Interface. De broninterface is de interface van waaruit het verkeer wordt geïnitieerd.

· LAN â€" Het lokale netwerk van de router.

· WAN1 â€" Het brede gebiedsnetwerk of het netwerk waarvan de router internet van de ISP of volgende hoprouter krijgt.

· WAN2 - hetzelfde als WAN1, behalve dat het een secundair netwerk is.

· OM HET EVEN WELKE â€" Laat om het even welke interface toe om worden gebruikt.

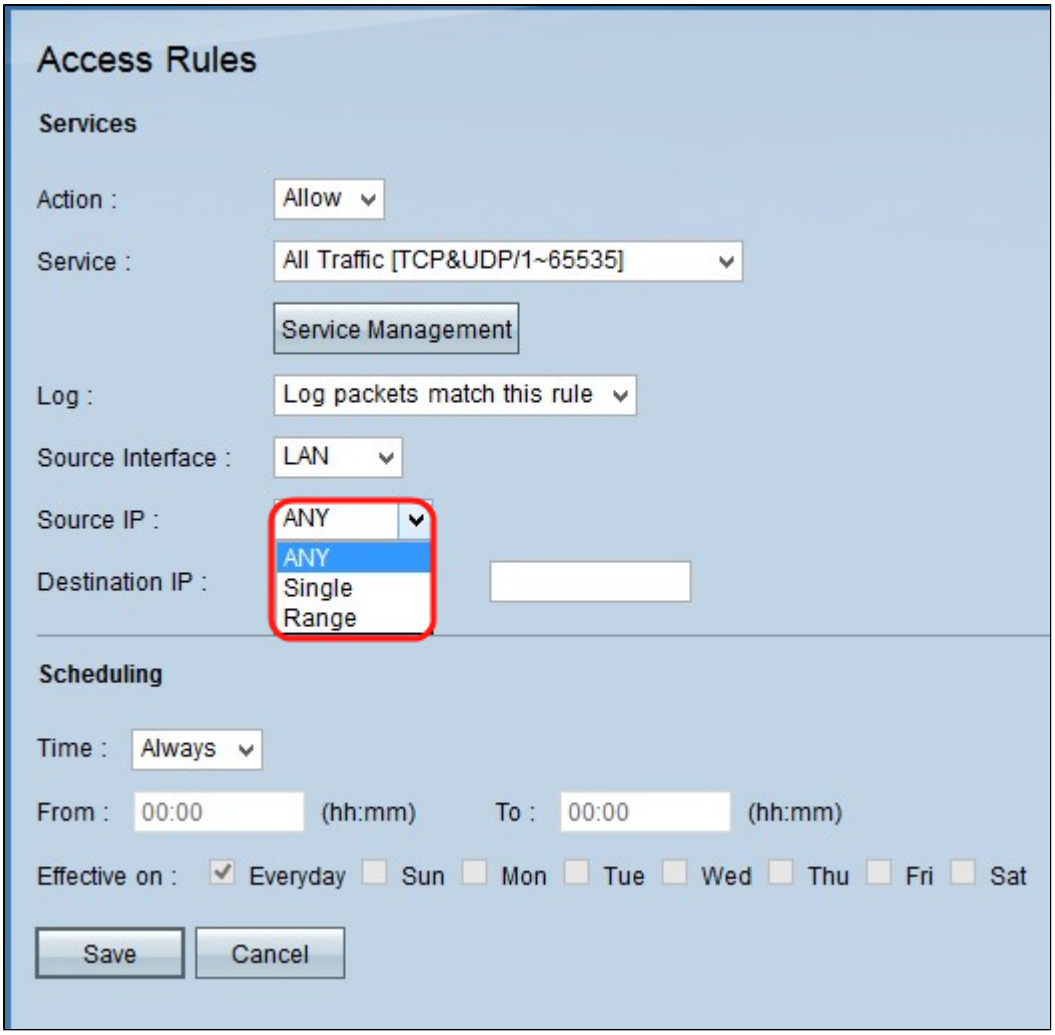


Stap 9. Kies in de vervolgkeuzelijst Bron-IP een optie om het bereik van IP-bronadressen op te geven die door de interface moeten worden toegestaan of geweigerd. De pakketten die op de interface aankomen worden geverifieerd door bron IP en bestemming IP.

· Om het even welk â€" De toegangsregel zal op al verkeer van de broninterface worden toegepast. Er zijn geen velden rechts van de vervolgkeuzelijst beschikbaar.

· Enkelvoudig â€" Toegangsregel wordt toegepast op één IP-adres vanuit de broninterface. Voer in het veld Adres het gewenste IP-adres in.

· Bereik â€" Toegangsregel wordt toegepast op een subnetnetwerk vanaf de broninterface. Voer het IP-adres en de prefixlengte in.



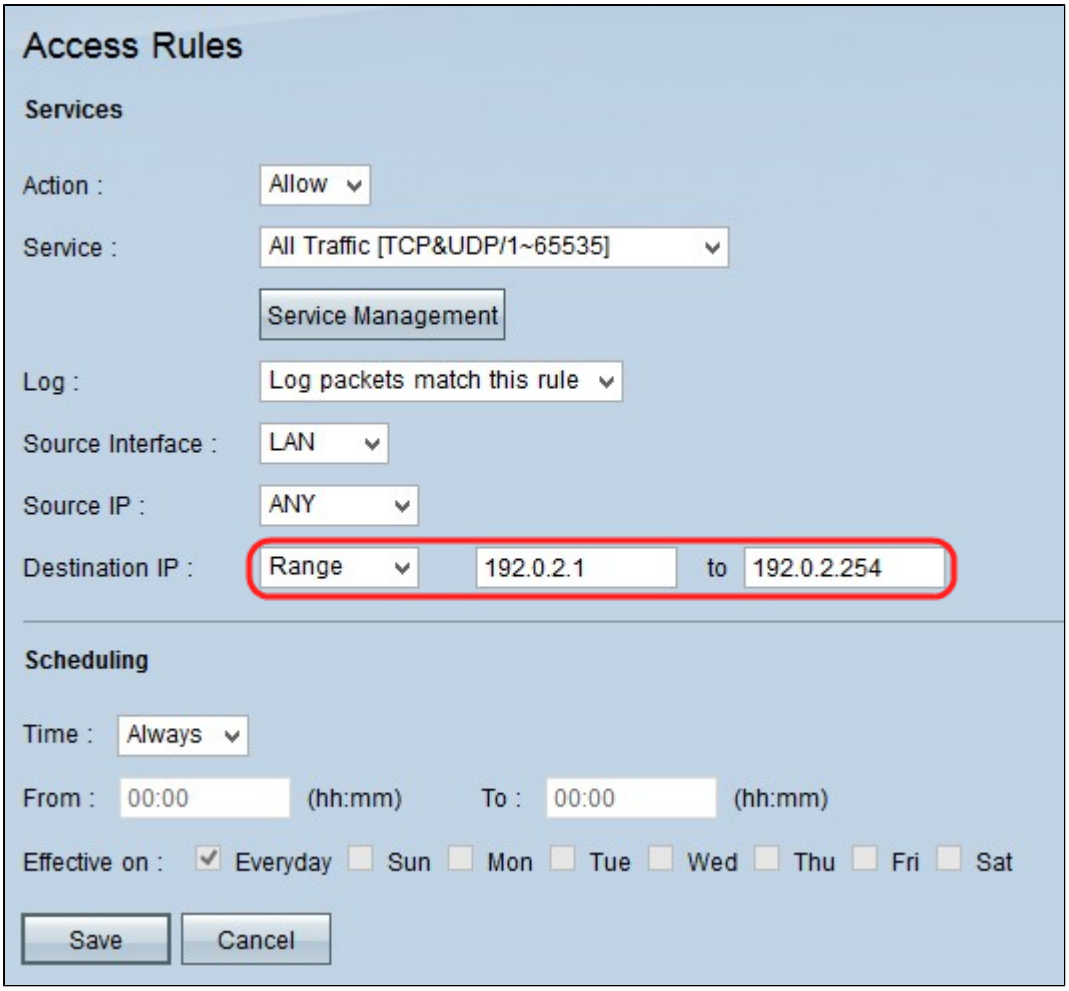
Stap 9. In de vervolgkeuzelijst Bestemming kiest u een optie om het bereik van doeladressen op te geven die moeten worden toegestaan of geweigerd door de interface. De pakketten die op de interface aankomen worden geverifieerd door bron IP en bestemming IP.

· Om het even welk â€" De toegangsregel zal op al verkeer op de bestemmingsinterface worden toegepast. Er zijn geen velden rechts van de vervolgkeuzelijst beschikbaar.

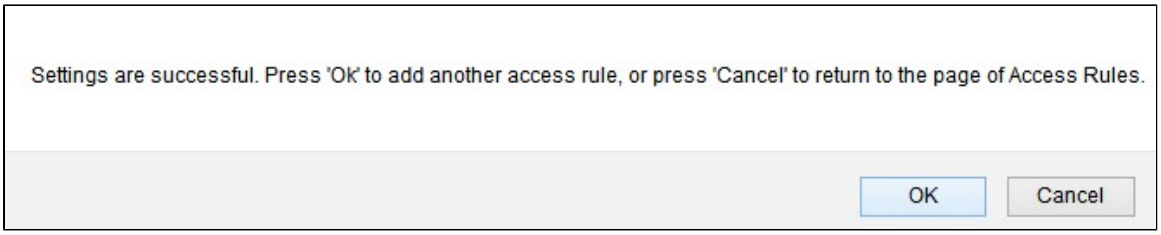
· Enkele toegangsregel wordt toegepast op één IP-adres op de doelinterface. Voer in het veld Adres het gewenste IP-adres in.

· Bereik â€" Toegangsregel wordt toegepast op een subnetnetwerk op de doelinterface. Voer het IP-adres en de prefixlengte in.

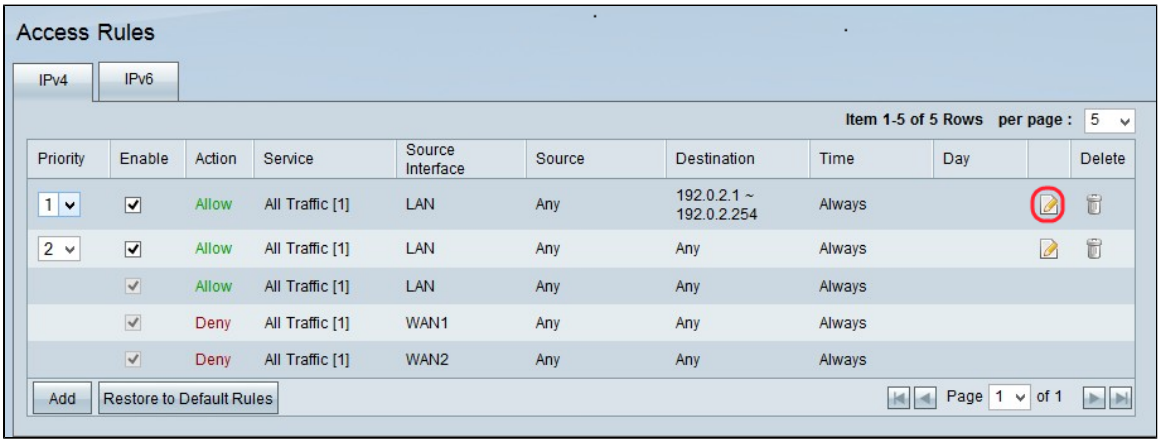
Klik op **Opslaan** om alle wijzigingen op te slaan die in de toegangsregel zijn aangebracht. Er verschijnt een bevestigingsvenster met de status van de wijzigingen die op het apparaat zijn aangebracht.



Stap 10. Klik op **OK** om een andere toegangsregel toe te voegen. Klik op **Annuleren** om de pagina *Toegangsregels* terug te keren.

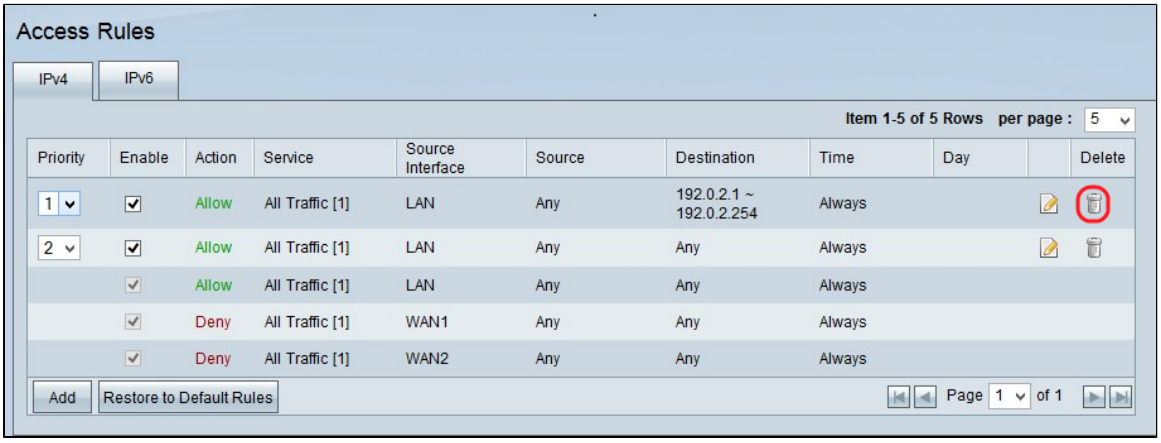


Stap 1 (optioneel). Kies de gewenste toegangsregel in de lijst en klik vervolgens op **knop Bewerken** om de configuratie van de toegangsregel te bewerken.



Stap 12 (optioneel). Kies de gewenste toegangsregels in de lijst en klik vervolgens op **Verwijderen om** de

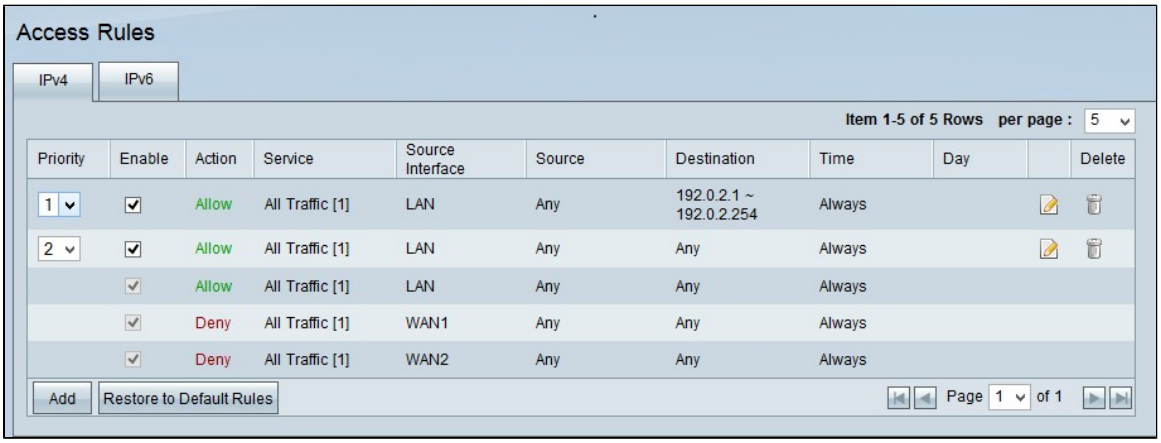
toegangsregel te verwijderen uit de lijst met toegangsregels.



IPv4-toegangsregels plannen

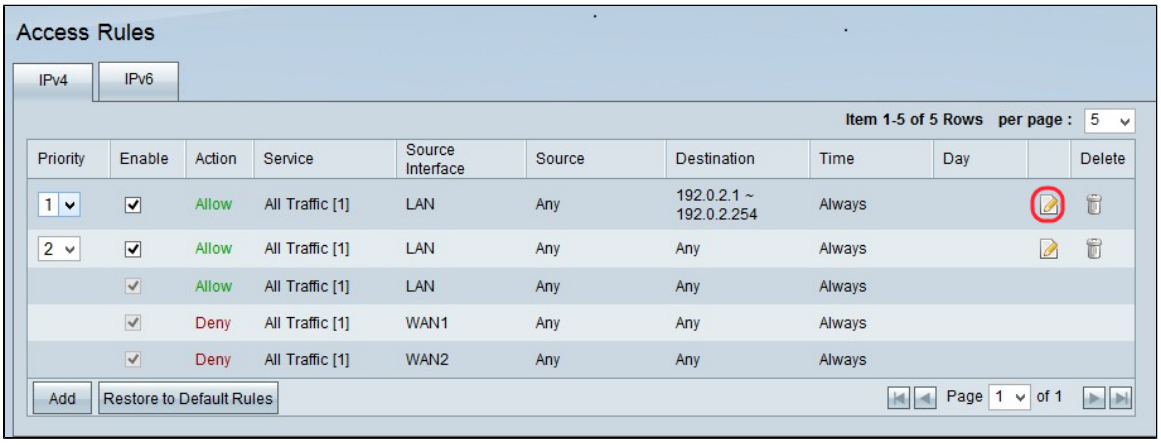
Het plannen van toegangsregels helpt om een schema te specificeren wanneer deze toegangsregels actief zijn in termen van dag en tijd. Het werkt alleen met IPv4.

Stap 1. Gebruik het hulpprogramma voor webconfiguratie en kies **Firewall > Toegangsregels**. De pagina *IPv4-toegangsregels* wordt geopend:



Stap 2. Kies de toegangsregel uit de tabel en klik op het pictogram **Bewerken** om de planningsfunctie aan die toegangsregel toe te voegen.

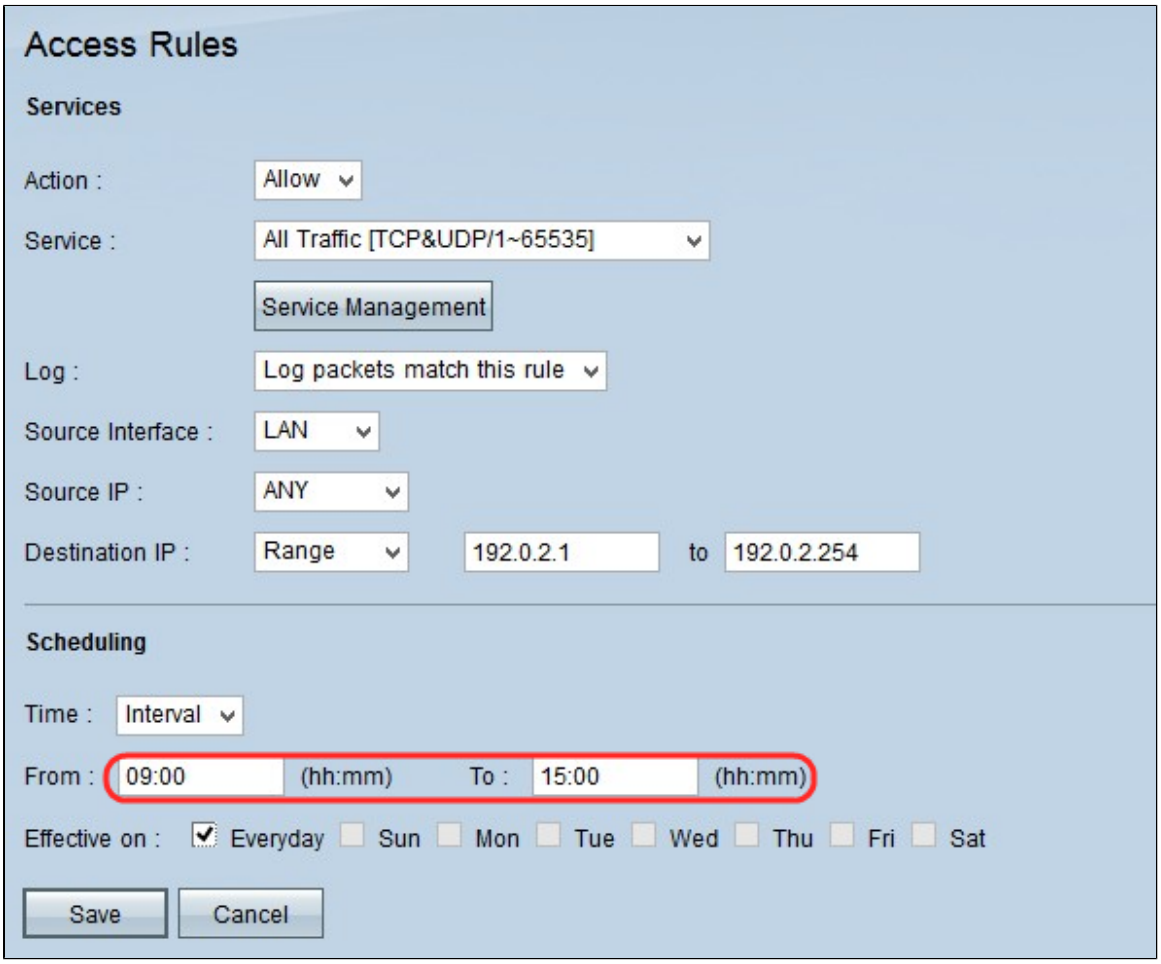
Opmerking: u kunt ook de planningsfunctie toevoegen wanneer u een nieuwe toegangsregel toevoegt.



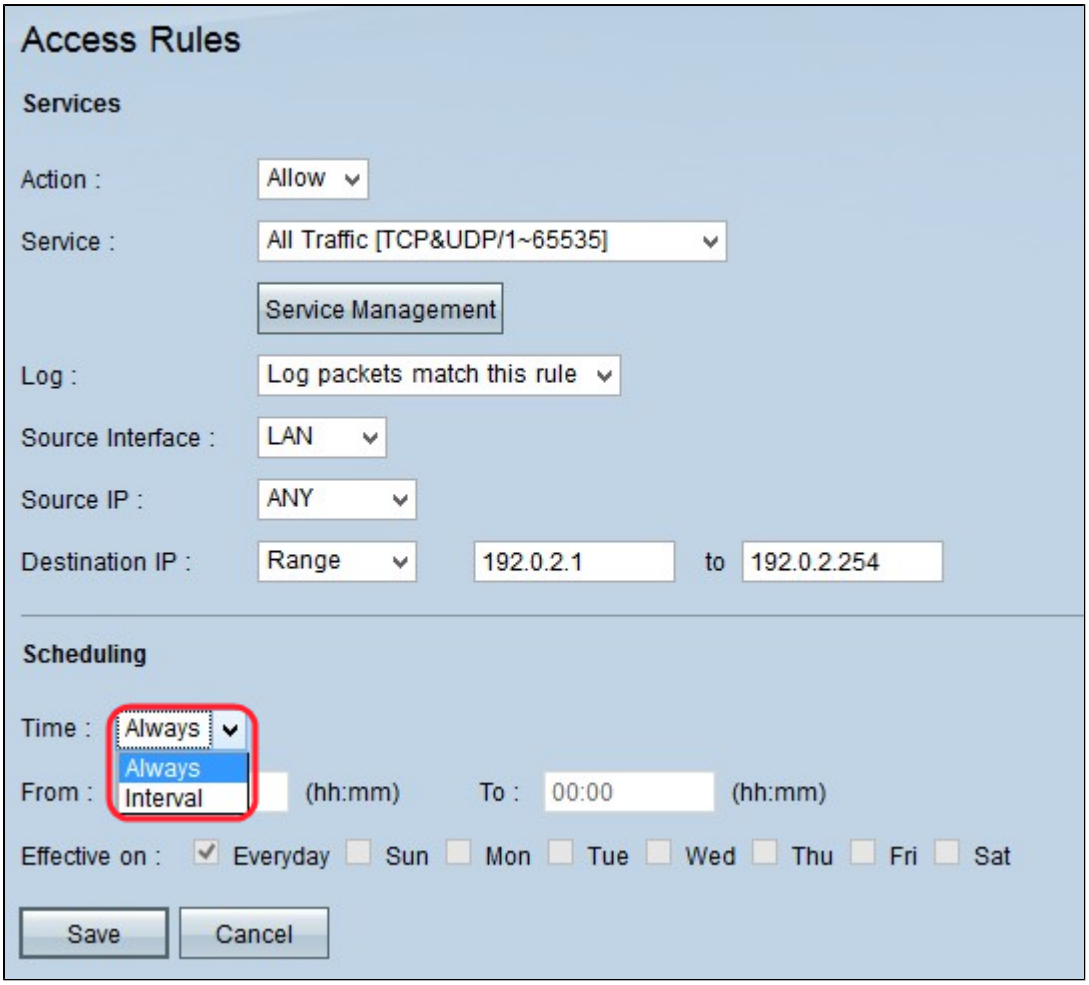
Stap 3. Kies de tijd in de vervolgkeuzelijst Tijd. Hiermee wordt aangegeven wanneer de planning moet worden gebruikt.

· Altijd â€" Toegangsregel geldt te allen tijde en op alle dagen van de week. Standaard is deze optie gekozen. Als u deze optie kiest, klikt u op *Opslaan* en naar stap 6 overslaan.

· Interval â€" Op basis van het door de gebruiker opgegeven tijdsinterval wordt de toegangsregel toegepast.

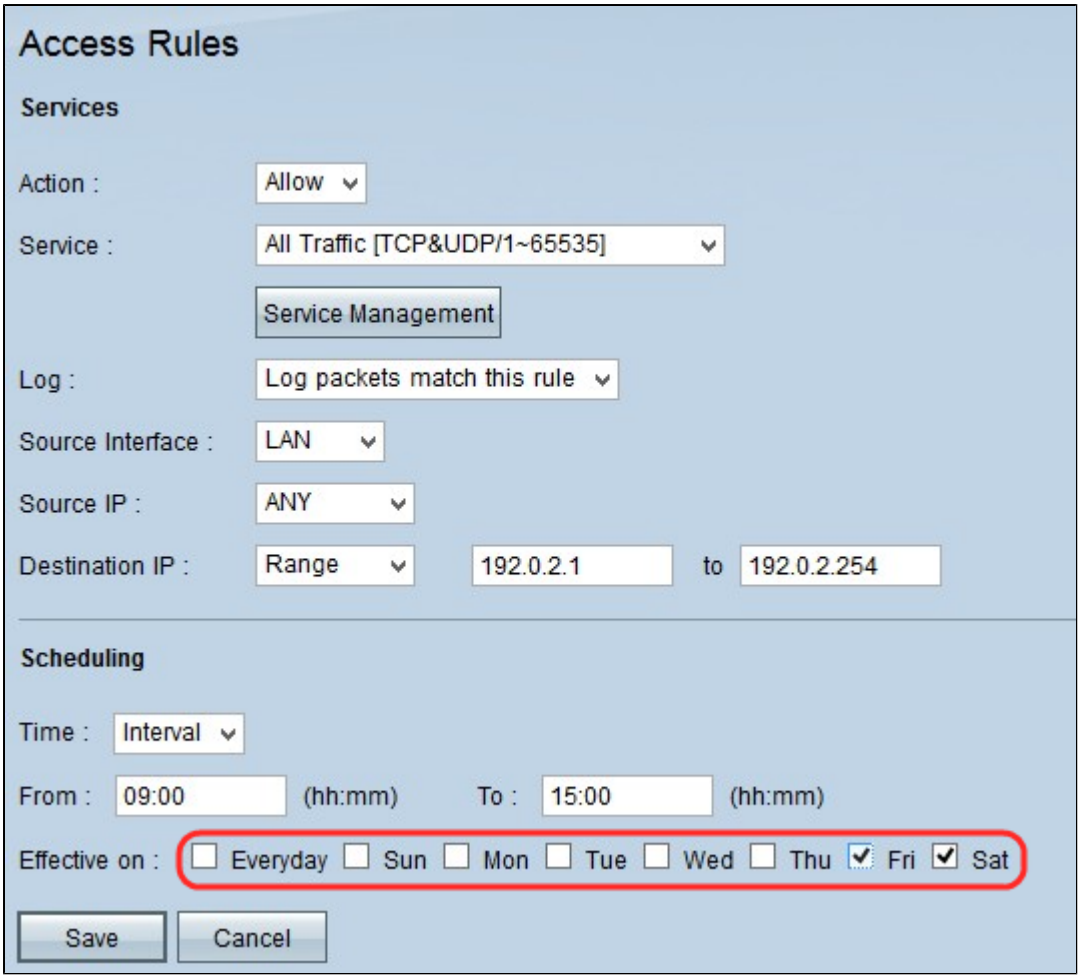


Stap 4. Voer in de velden *Van* en *Tot* het tijdsinterval in met een indeling van 24 uur waarin de toegangsregel wordt toegepast.

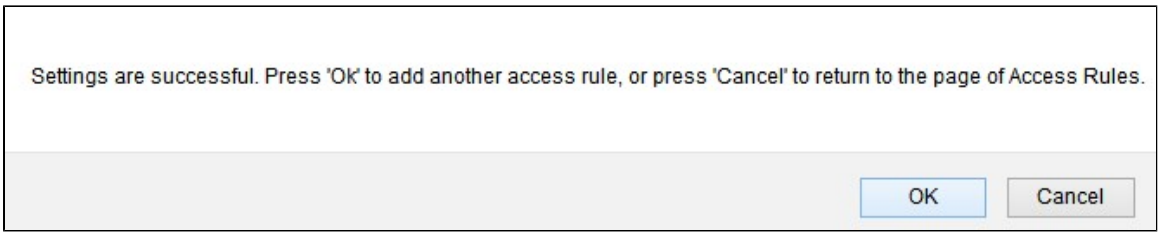


Stap 5. Schakel de selectievakjes in naast de dagen waarop u de toegangsregel wilt toepassen. De toegangsregel is alleen op de aangegeven dagen van kracht. Standaard wordt *Dagelijks* gekozen.

Klik op **Opslaan** om alle wijzigingen op te slaan die in de toegangsregel zijn aangebracht. Er wordt een bevestigingsvenster weergegeven met de status van de wijzigingen die op het apparaat zijn aangebracht.



Stap 6. Klik op **OK** om een andere toegangsregel toe te voegen. Klik op **Annuleren** om de pagina met toegangsregels terug te keren.



Conclusie

U hebt nu IPv4-toegangsregels ingesteld voor uw RV016, RV042, RV042G of RV082 VPN-router.

Als u alle ondersteuning voor deze routers wilt gebruiken, controleert u de productpagina door hier te klikken.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.