Configureer de toegangsregels voor RV160 en RV260 Series routers

Doel

Uw router is verantwoordelijk voor het ontvangen van gegevens van het externe netwerk en is de eerste verdedigingslijn wanneer deze op uw lokale netwerkbeveiliging aankomt. Door toegangsregels op uw router toe te passen, kunt u pakketten filteren die op specifieke parameters zoals IP-adres of poortnummer zijn gebaseerd. Met de onderstaande stappen helpt dit document u bij het configureren van de toegangsregels om de pakketten die uw netwerk binnendringen beter te controleren. Dit document zal ook enkele goede praktijken belichten om de toegangsregels optimaal te benutten voor de veiligheid.

Toepasselijke apparaten

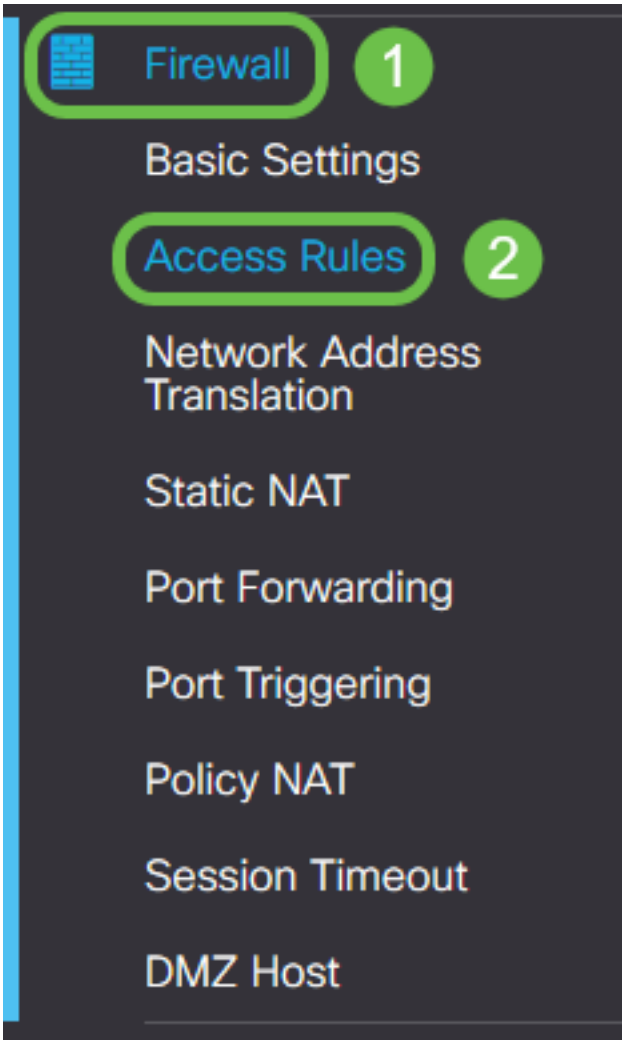
- RV160x-software
- RV260x-software

Softwareversie

- 1.0.00.13

Toegangsregels instellen

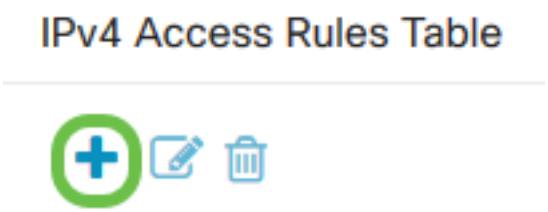
Stap 1. Selecteer in het navigatiedeelvenster aan de linkerkant van het configuratieprogramma de optie **Firewall > Toegangsregels.**



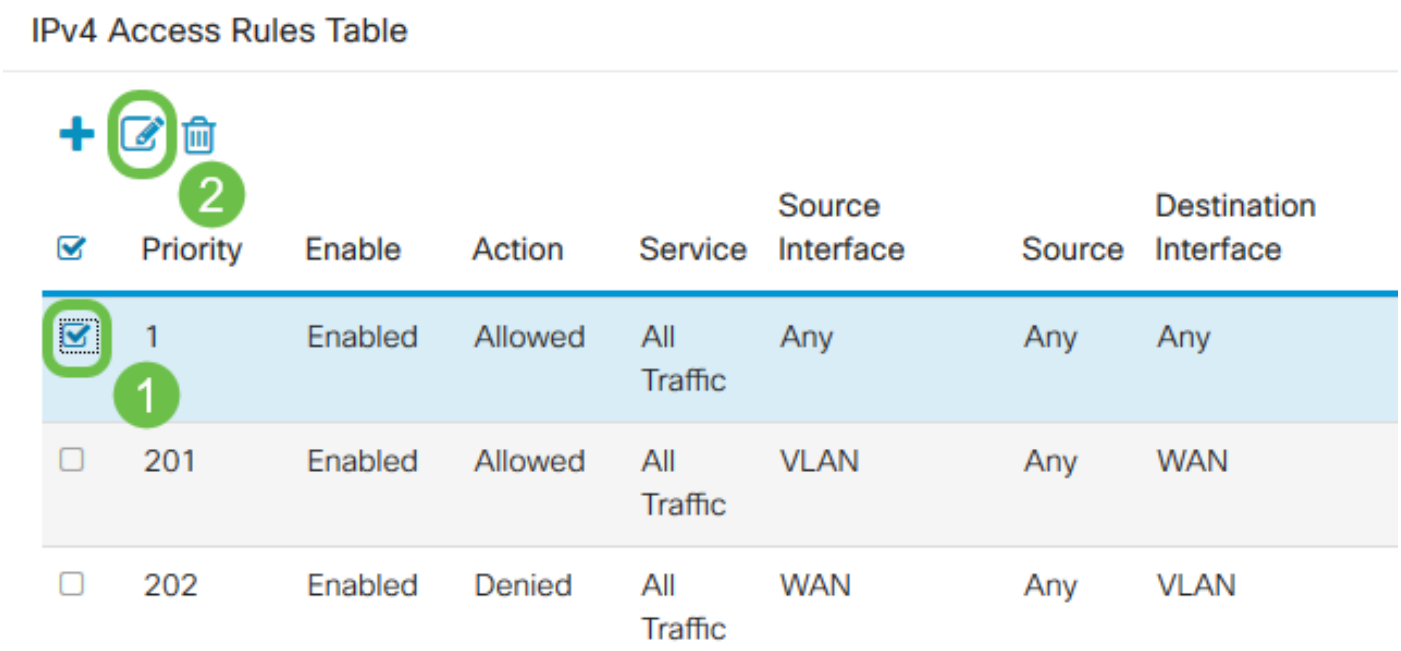
De pagina Toegangsregels wordt weergegeven. Op deze pagina zijn er tabellen met lijsten van toegangsregels en hun eigenschappen voor respectievelijk IPv4 en IPv6. Hier kunt u een nieuwe toegangsregel toevoegen, een bestaande regel bewerken of een bestaande regel verwijderen.

Een toegangsregel toevoegen/bewerken

Stap 2. Om een nieuwe toegangsregel toe te voegen, klik op het blauwe pictogram om in de tabel met IPv4-toegangsregels of IPv6-toegangsregels toe te voegen, afhankelijk van welk protocol u de regel wilt toepassen. In dit geval wordt IPv4 gebruikt.

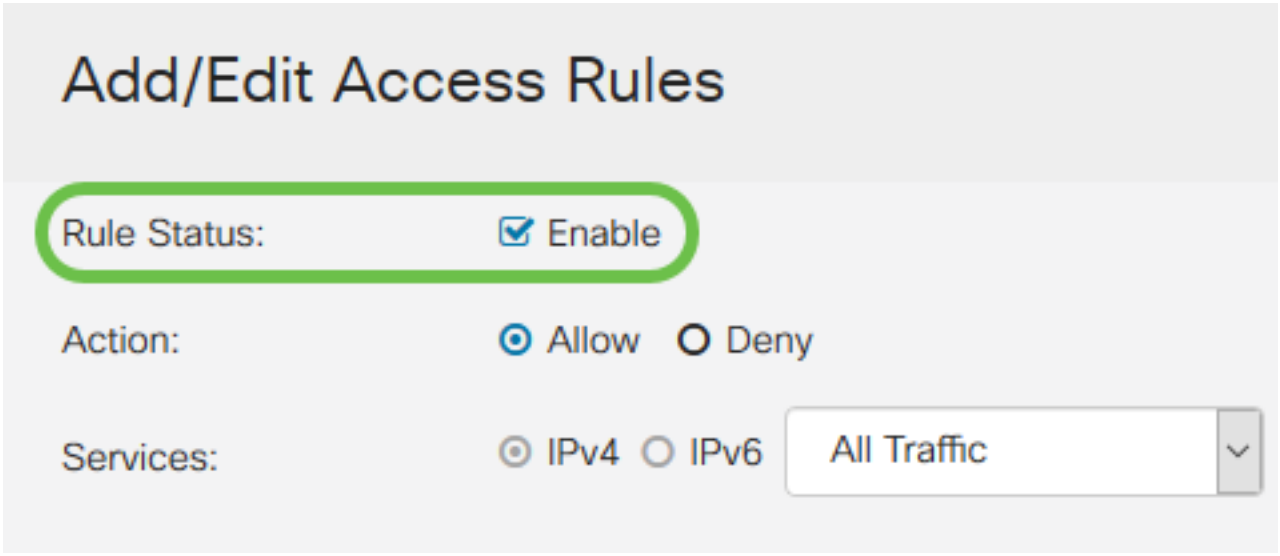


Als u een bestaande ingang wilt bewerken, selecteert u het selectieteken naast de toegangsregel die u wilt wijzigen. Selecteer vervolgens het blauwe pictogram bewerken boven in de corresponderende tabel. Er kan slechts één regel worden geselecteerd voor bewerking.

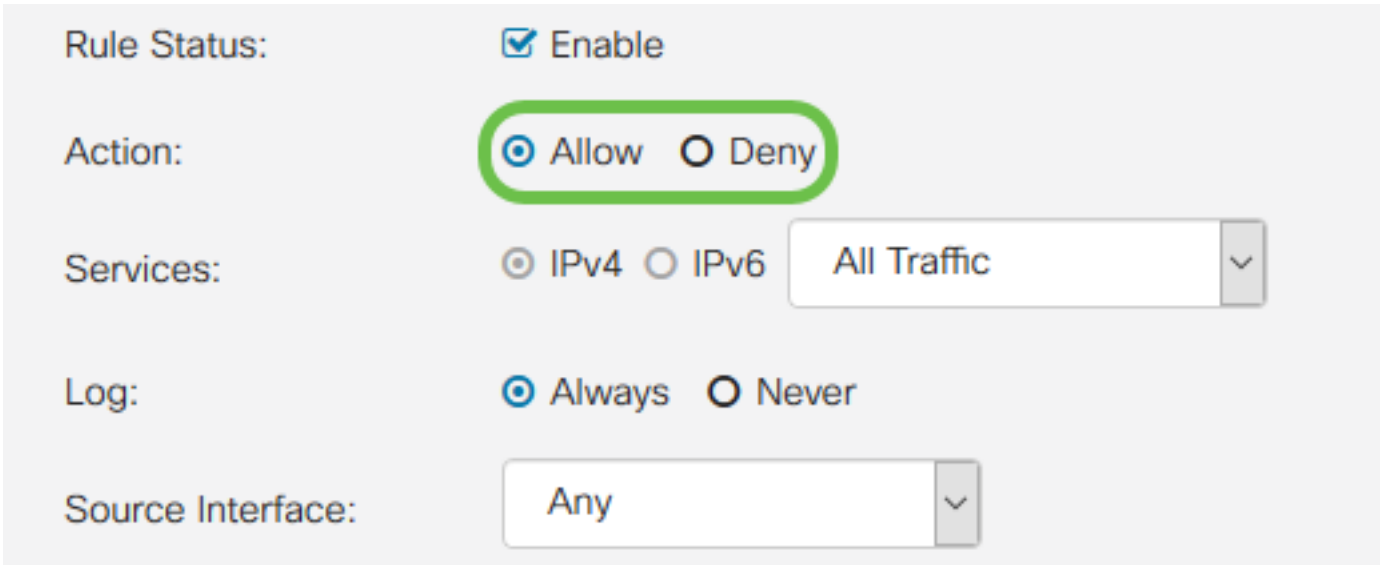


De pagina *Toegangsregels toevoegen/bewerken* wordt weergegeven.

Stap 3. Controleer/Schakel het selectieteken voor Regelstatus uit om de toegangsregel tijdens het gebruik in te schakelen of uit te schakelen. Dit is handig wanneer u een toegangsregel hebt die u wilt opslaan om deze op een latere datum toe te passen.

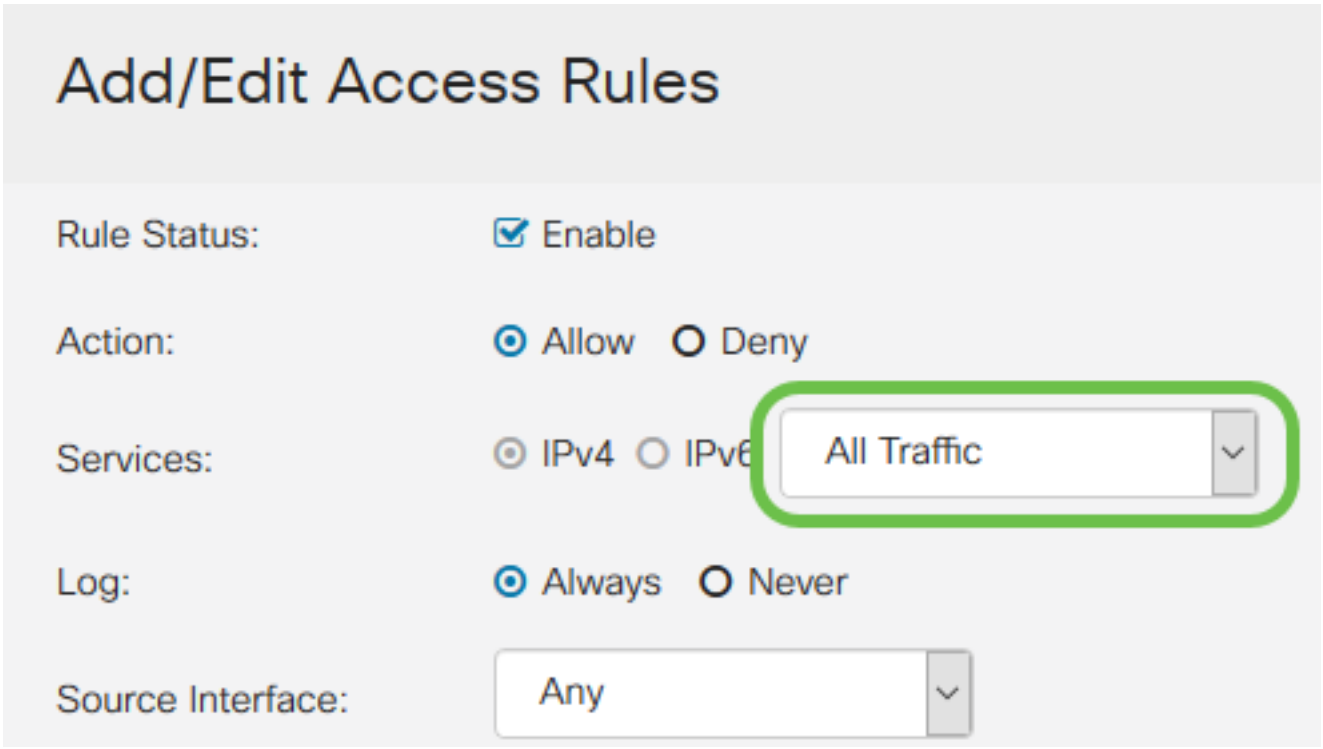


Stap 4. Van het veld *Actie* selecteert u of de regel de toegang tot het inkomende netwerkverkeer al dan niet moet toestaan.



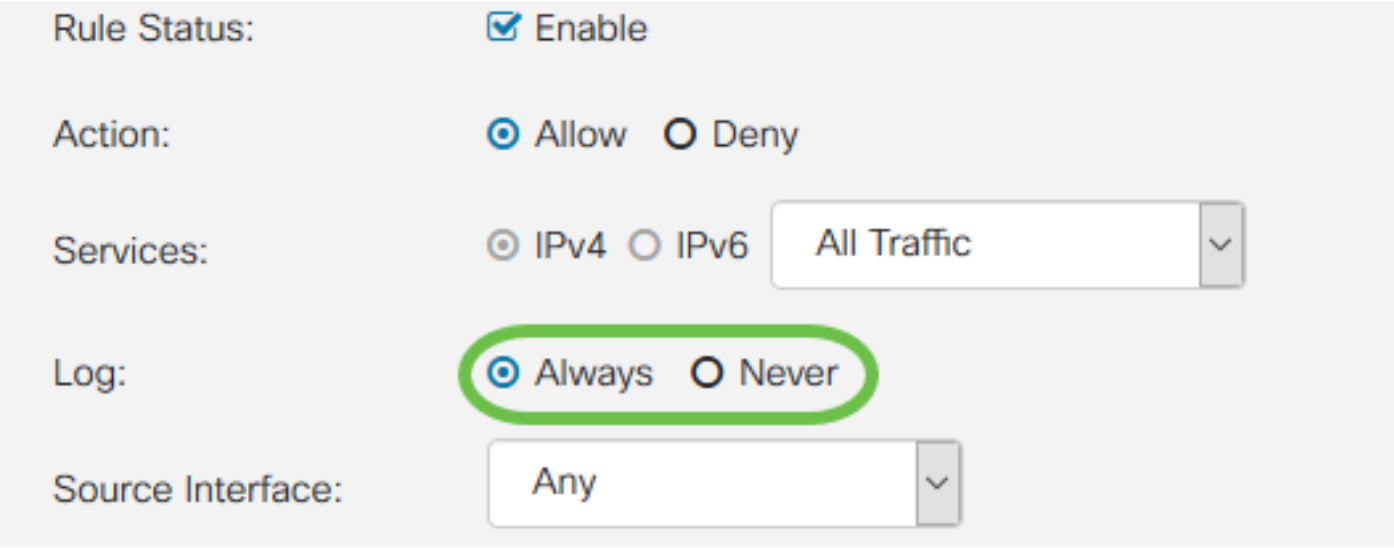
Opmerking: Het wordt voor de beste veiligheid aanbevolen om toegangsregels in te stellen die alleen het verkeer toestaan dat u verwacht te ontvangen, in plaats van alleen ongewenste verkeer te ontkennen. Dit zal uw netwerk beter beschermen tegen onbekende bedreigingen.

Stap 5. In het veld *Services* selecteert u in het vervolgkeuzemenu het type netwerkservice waarvoor u de toegangsregel wilt toepassen.

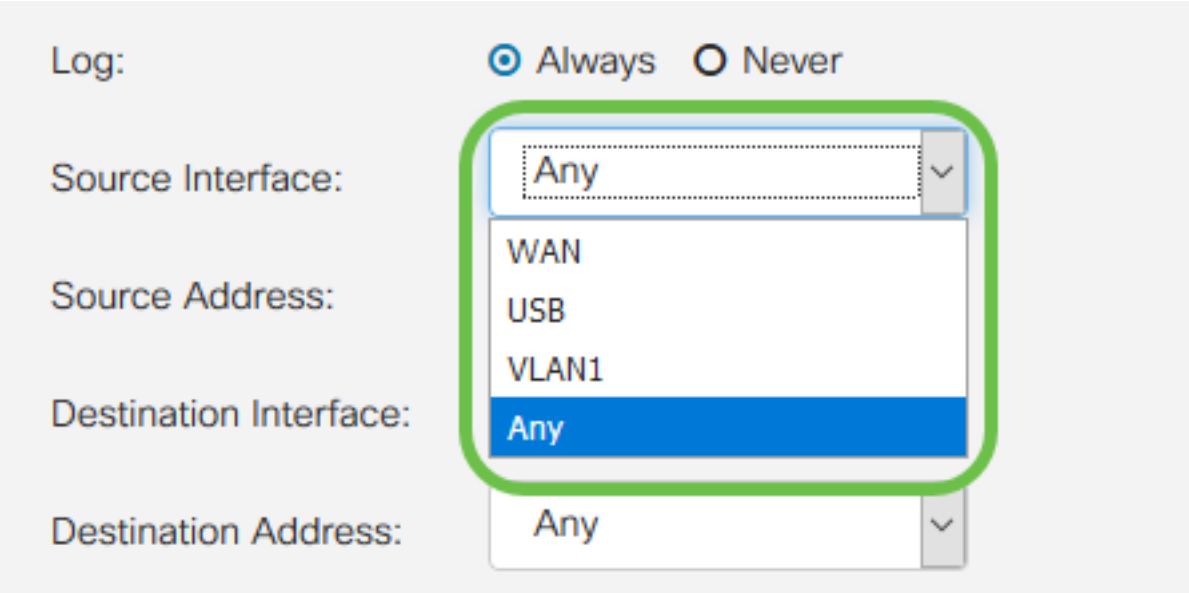


Opmerking: De radioknop IPv4 of IPv6 wordt automatisch geselecteerd op basis van de tabel waarop u hebt gekozen om de toegangsregel van de pagina *Toegangsregels* toe te passen.

Stap 6. Selecteer in het veld *Log* of u wilt dat de router een logbericht genereert nadat pakketten die uw netwerk invoeren, overeenkomen met de gebruikte regels.



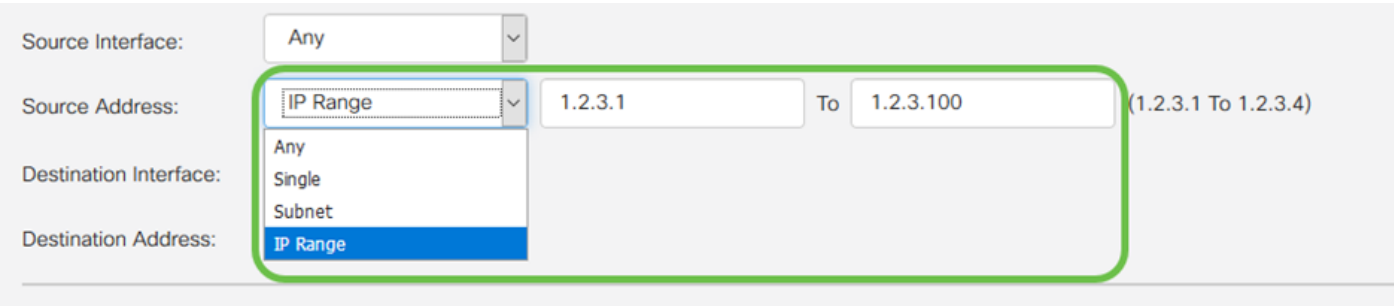
Stap 7. Selecteer in de vervolgkeuzelijst *Bron-interface* de netwerkinterface voor inkomende pakketten waarop de toegangsregel van toepassing zal zijn.



Stap 8. Selecteer in de vervolgkeuzelijst *Bron adres* het type inkomend adres waarop de toegangsregel van toepassing is. De opties zijn als volgt:

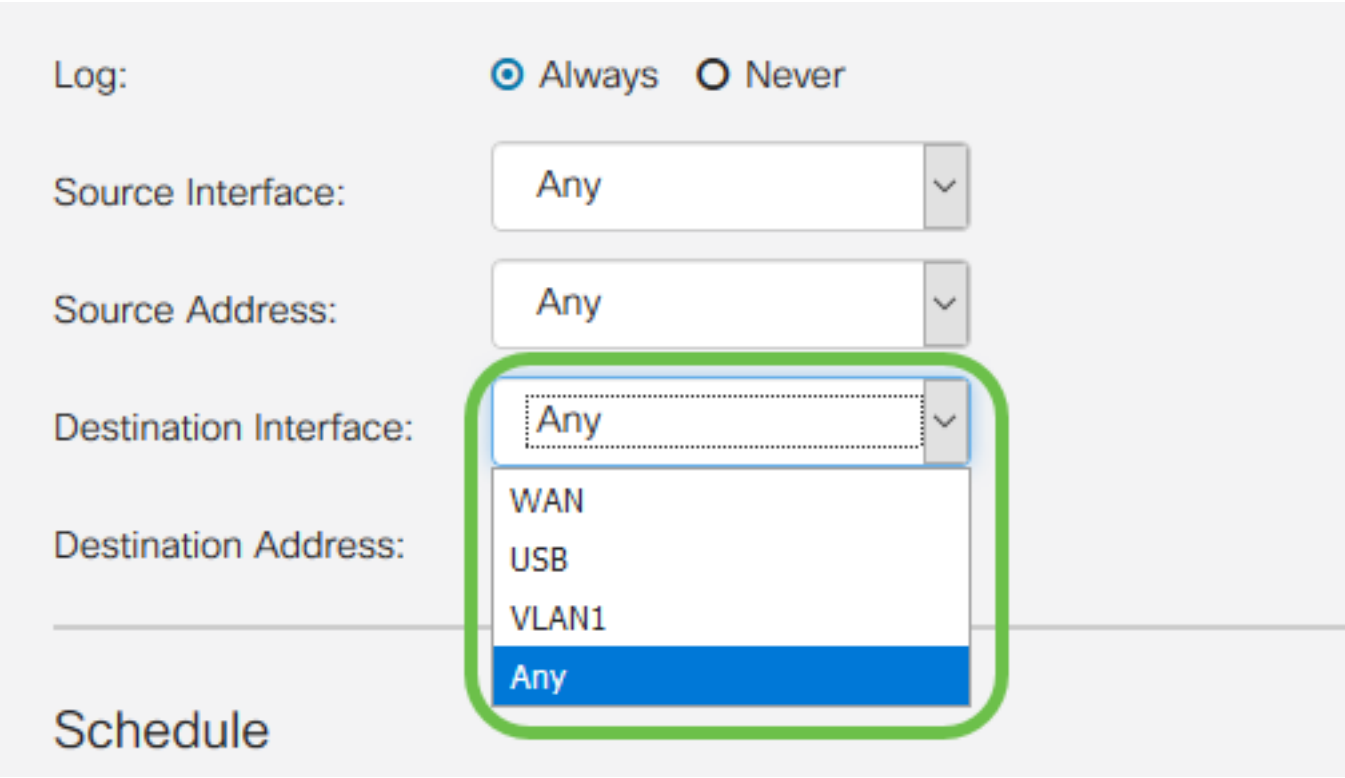
- Any- De regel wordt toegepast op alle inkomende IP-adressen
- Single - De regel zal van toepassing zijn op één bepaald IP-adres
- Subnet - De regel zal op bepaalde subnet van een netwerk van toepassing zijn
- IP-bereik - De regel is van toepassing op een gedefinieerd bereik van IP-adressen

Opmerking: Als u Single Point, Subnet of IP Range selecteert, verschijnen de bijbehorende velden rechts in het vervolgkeuzemenu waar u adresdetails kunt invoeren. In dit voorbeeld wordt een IP-bereik ingevoerd om te demonstreren.



Stap 9. Selecteer in de vervolgkeuzelijst *Bestandsinterface* de netwerkinterface voor uitgaande

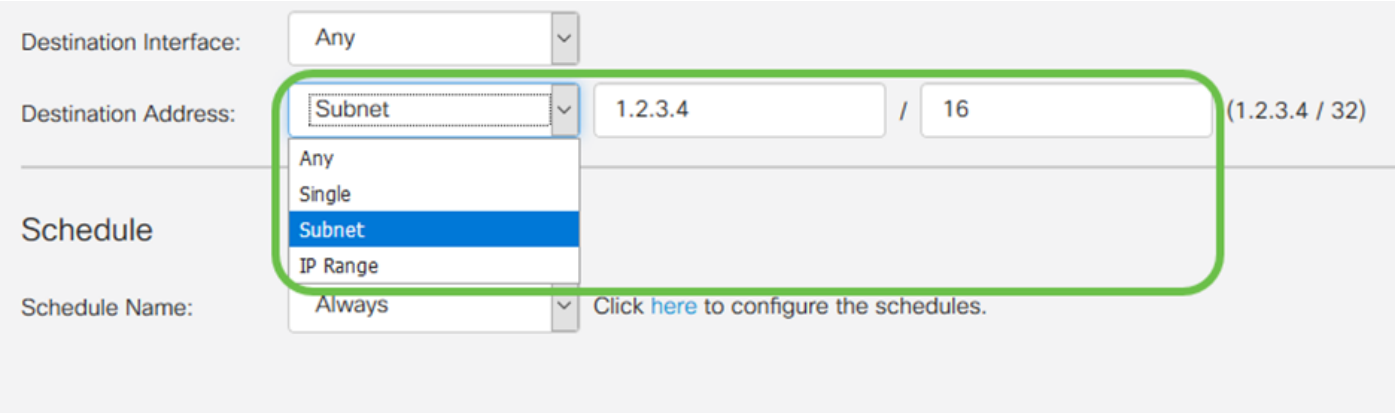
pakketten waarop de toegangsregel van toepassing zal zijn.



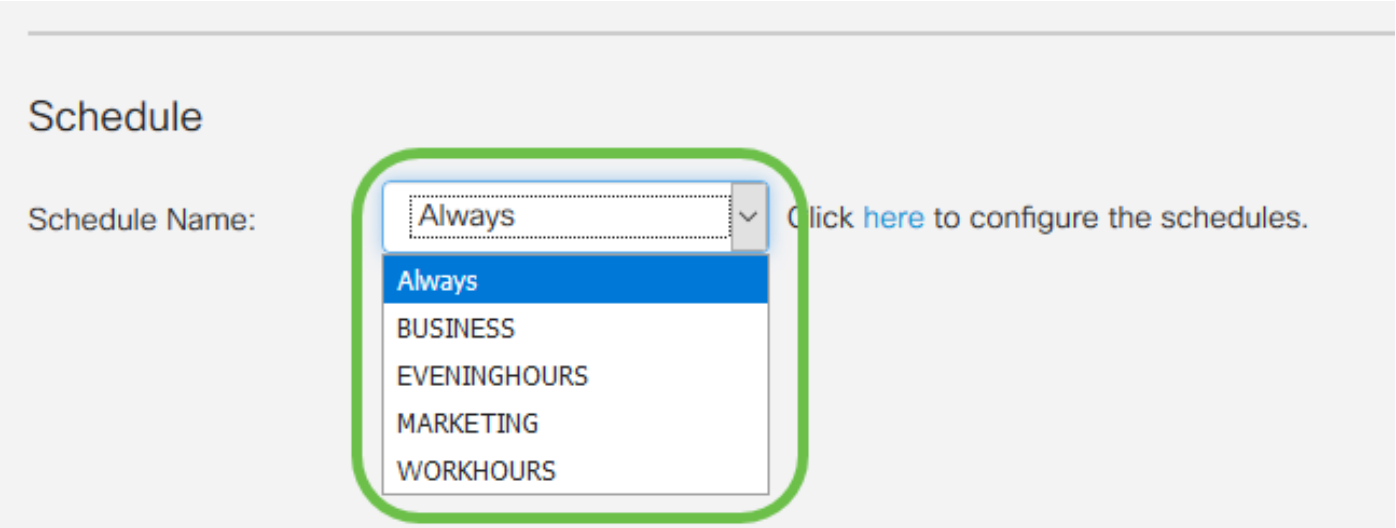
Stap 10. Selecteer in de vervolgkeuzelijst *Doeladres* het type uitgaand adres waarop de toegangsregel van toepassing is. De opties zijn als volgt:

- AnyRes - De regel wordt toegepast op alle uitgaande IP-adressen
- Single - De regel zal van toepassing zijn op één bepaald IP-adres
- Subnet - De regel zal op bepaalde subnet van een netwerk van toepassing zijn
- IP-bereik - De regel is van toepassing op een gedefinieerd bereik van IP-adressen

Opmerking: Als u Single Point, Subnet of IP Range selecteert, verschijnen de bijbehorende velden rechts in het vervolgkeuzemenu waar u adresdetails kunt invoeren. In dit voorbeeld wordt een SUBSIDIE ingevoerd om te demonstreren.



Stap 1. Selecteer in de vervolgkeuzelijst Naam *planning* het tijdschema waarop u de toegangsregel wilt toepassen.



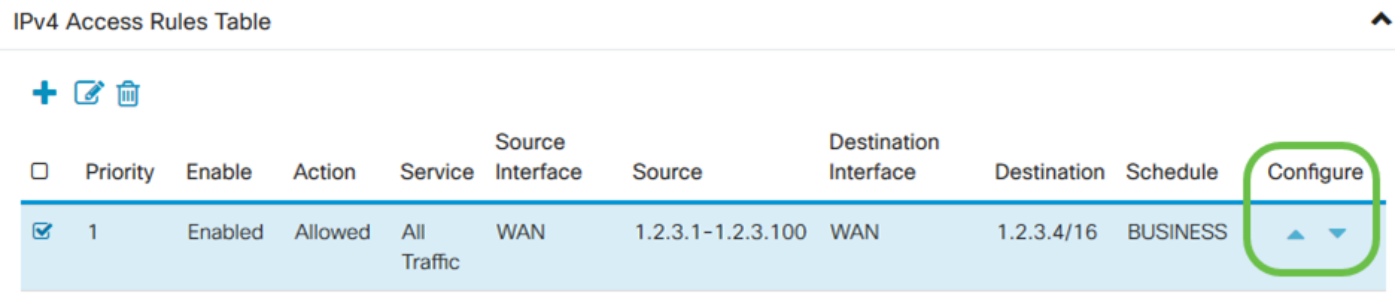
Opmerking: Voor verhoogde veiligheid, is het een beste praktijk om de niet kritieke netwerktoegang tot bedrijfsuren te beperken om te verzekeren dat ongewenste verbindingen worden ontkend wanneer uw zaken niet in werking zijn.

Opmerking: Klik op de koppeling rechts naast de vervolgkeuzelijst *Schedule Name* als u de tijden voor de toegangsregels wilt instellen. Meer informatie kan worden gevonden over hoe u deze schema's hier kunt configureren.

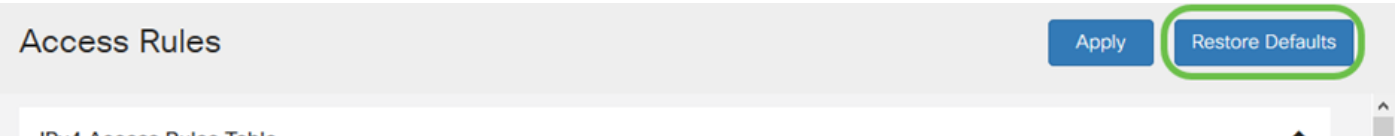
Stap 12. Wanneer u tevreden bent met de configuratie van de toegangsregel, klik op **Toepassen** om dit te bevestigen.

U wordt nu teruggestuurd naar de pagina met de hoofdregels *voor toegang*.

Opmerking: Wanneer een nieuwe toegangsregel wordt gecreëerd, wordt zijn prioriteit onderin de lijst geplaatst. Dit betekent dat als een toegangsregel op een specifieke parameter in strijd is met een andere, de beperkingen van de hogere prioriteitsregel voorrang zullen krijgen. Om een regel omhoog of omlaag in prioriteit te verplaatsen, kunt u de blauwe pijlen in de kolom Configure gebruiken.

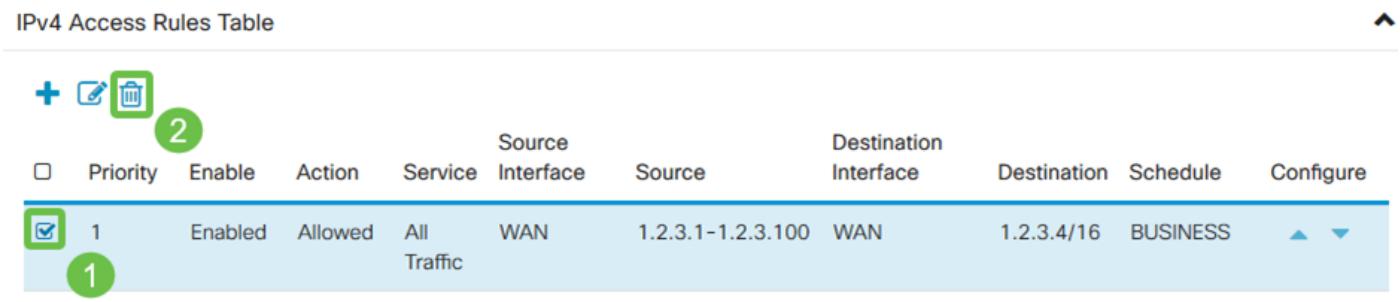


Stap 13 (optioneel). Als u de standaardinstelling van de toegangsregels wilt teruggeven, klikt u op **Standaardinstellingen herstellen** in de rechterbovenhoek van de pagina.



Een toegangsregel verwijderen

Stap 14. Als u een toegangsregel uit de lijst wilt verwijderen, selecteert u eenvoudig het vakje voor de corresponderende regel die u wilt verwijderen. Selecteer vervolgens het pictogram blauw afval boven in de lijst. Meerdere toegangsregels kunnen tegelijk worden verwijderd.



Servicebeheer

Met servicebeheer kunt u bestaande netwerkservices toevoegen of bewerken aan de hand van hun poortnummer, protocol en andere details. Deze netwerkservice is beschikbaar in de vervolgkeuzelijst Services bij het configureren van de toegangsregels. Via het configuratiemenu van de de dienstbeheerlijst kunt u aangepaste services maken die dan kunnen worden toegepast op de toegangsregels voor een fijnere controle over het verkeer dat uw netwerk ingaat. Klik hier voor meer informatie over de configuratie van het Servicebeheer.

Conclusie

Toegangsregels die op juiste wijze worden toegepast, zijn een waardevol gereedschap om de WAN-verbinding te beveiligen. Met de bovenstaande handleiding en besproken praktijken dient u alles te hebben wat u nodig hebt om de beveiligde toegangsregels voor uw RV160x- of RV260x-router correct te configureren.