Configuratie van client-naar-Site Virtual Private Network (VPN) verbinding op de RV34x Series router

Doel

In een client-to-Site Virtual Private Network (VPN) verbinding kunnen klanten van het internet zich via de server aansluiten op het netwerk van het bedrijf of LAN (Local Area Network) achter de server, maar blijven de beveiliging van het netwerk en de bronnen ervan behouden. Deze optie is zeer nuttig aangezien het een nieuwe VPN-tunnel creëert die telewerkers en zakenreizigers in staat zou stellen om toegang te krijgen tot uw netwerk door gebruik te maken van een VPN-clientsoftware zonder de privacy en de beveiliging op het spel te zetten.

Het doel van dit document is om u te tonen hoe u client-to-Site VPN-verbinding kunt configureren op de RV34x Series router.

Toepasselijke apparaten

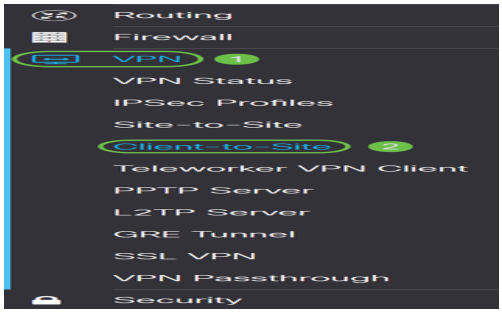
- RV34x Series

Softwareversie

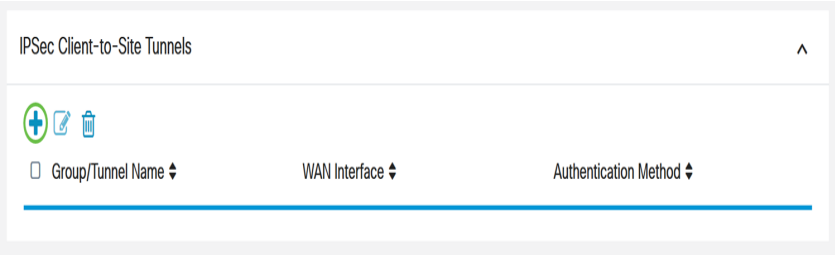
- 1.0.01.16

Client-to-Site VPN configureren

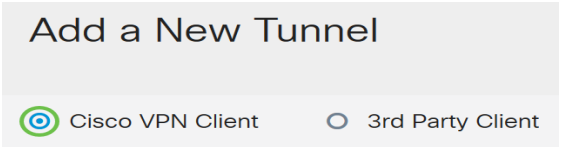
Stap 1. Meld u aan bij het op router gebaseerde hulpprogramma en kies **VPN > Client-to-Site**.



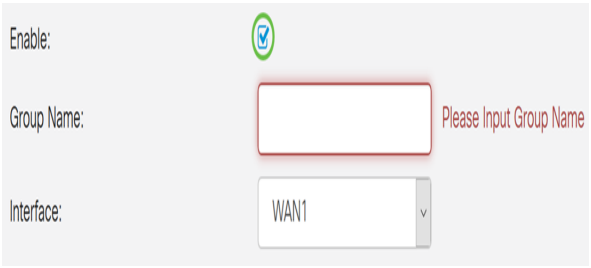
Stap 2. Klik op de knop **Add** onder de sectie client-to-Site tunnels.



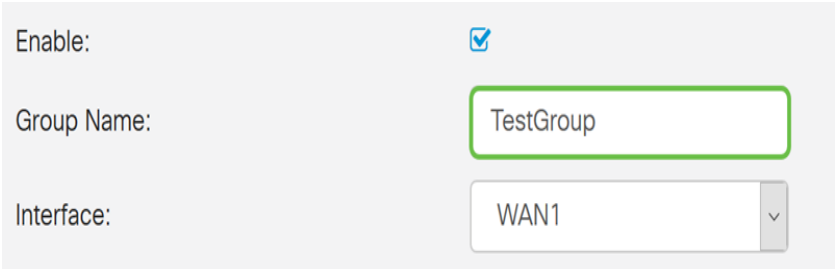
Stap 3. Klik in het gebied *Add a New Tunnel* op de radioknop van **Cisco VPN Client**.



Stap 4. Controleer het vakje **Enable** om de configuratie in te schakelen.



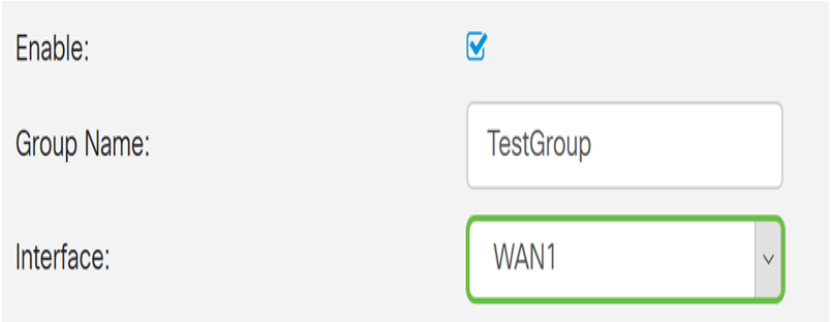
Stap 5. Voer een groepsnaam in in het daarvoor bestemde veld. Dit zal dienen als identificator voor alle leden van deze groep tijdens de onderhandelingen over de Internet Key Exchange (IKE).



Opmerking: Voer tekens in tussen A tot Z of 0 tot 9. Er zijn geen spaties en speciale tekens toegestaan voor de groepsnaam. In dit voorbeeld wordt TestGroup gebruikt.

Stap 6. Klik op de vervolgkeuzelijst om de interface te kiezen. De opties zijn:

- WAN1
- WAN2
- USB1
- USB2



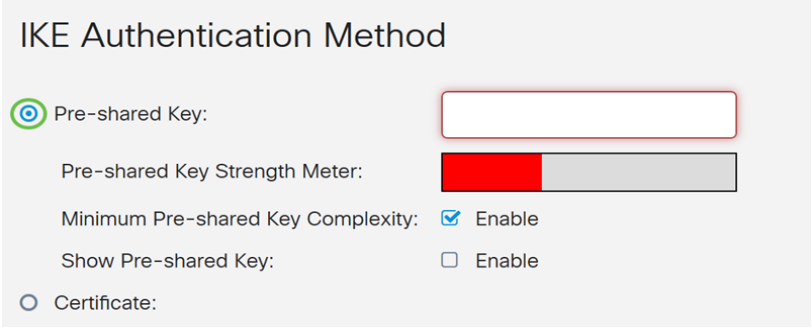
Opmerking: In dit voorbeeld wordt WAN1 geselecteerd. Dit is de standaardinstelling.

Stap 7. Kies in het gebied van de IKE-verificatiemethode een verificatiemethode die moet worden gebruikt bij IKE-onderhandelingen in de op IKE gebaseerde tunnel. De opties zijn:

- Vooraf gedeelde sleutel — IKE-peers authentiek elkaar door berekening en het verzenden van een kei aan gegevens die de Pre-Shared Key omvat. Als het

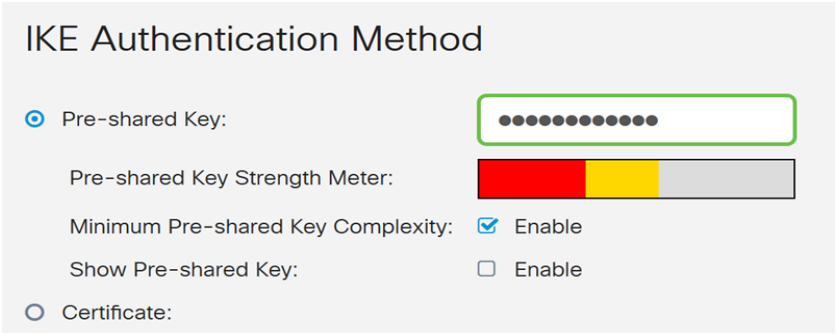
ontvangende peer in staat is om het zelfde hash onafhankelijk te creëren met gebruik van zijn Pre-gedeeld sleutel, weet het dat beide peers het zelfde geheim moeten delen en zo het andere peer authentiek te verklaren. Vooraf gedeelde toetsen schalen niet goed omdat elke IPSec-peer moet worden geconfigureerd met de Pre-Shared key van elke andere peer waarmee deze een sessie vastlegt.

- Certificaat — Het digitale certificaat is een pakket dat informatie bevat zoals een identiteitsbewijs van de houder: naam of IP-adres, de vervaldatum van het certificaat en een kopie van de openbare sleutel van de certificaathouder. De standaard digitale certificaatindeling is gedefinieerd in de X.509-specificatie. X.509 versie 3 definieert de gegevensstructuur voor certificaten.



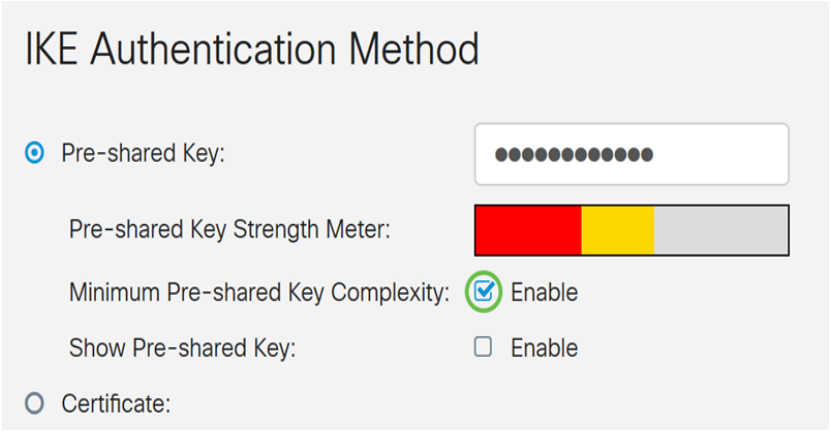
Opmerking: In dit voorbeeld wordt Pre-Shared Key geselecteerd. Dit is de standaardinstelling.

Stap 8. Voer in het daarvoor bestemde veld een vooraf gedeelde sleutel in. Dit zal de authenticatiesleutel zijn onder uw groep IKE-peers.

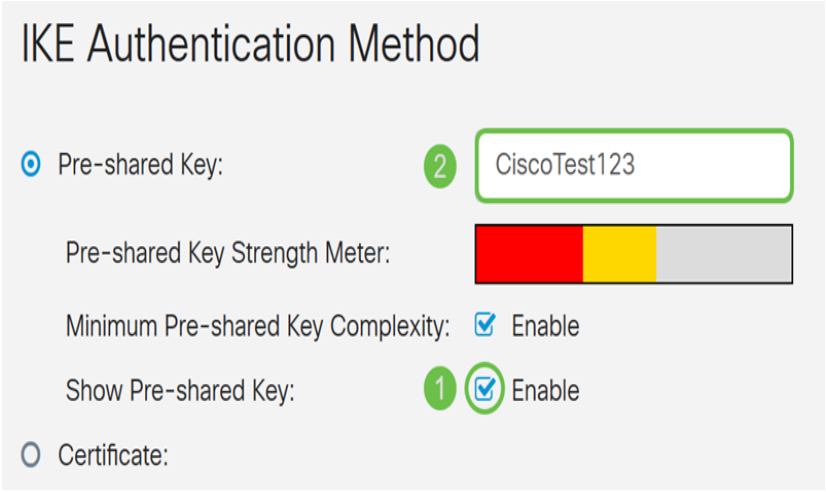


Stap 9. (Optioneel) Controleer het aanvinkvakje **Enable** for the Minimale Pre-Shared Key Complexity om de vooraf gedeelde sleutel te bekijken en de sterkte van uw toets te bepalen. De sterkte van de toets wordt als volgt gedefinieerd:

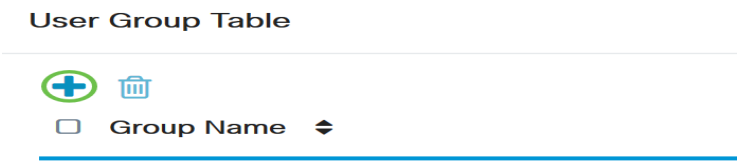
- Het wachtwoord is zwak.
- Orange— Het wachtwoord is vrij sterk.
- Groen — Het wachtwoord is sterk.



Opmerking: U kunt het aanvinkvakje **Enable** controleren in het veld *Voorgedeelde sleutel tonen* om het wachtwoord in onbewerkte tekst te controleren.

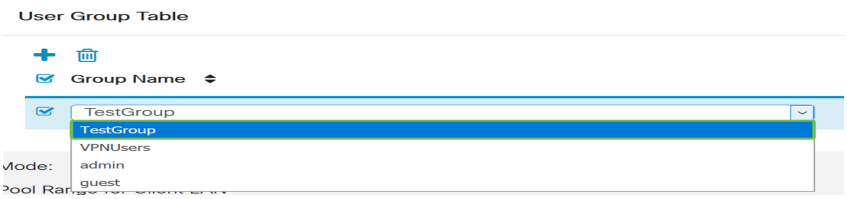


Stap 10. (Optioneel) Klik op het pictogram **plus** in de tabel van de gebruikersgroep om een groep toe te voegen.



Stap 1. (Optioneel) Kies uit de vervolgkeuzelijst of de gebruikersgroep geschikt is voor beheerder of voor gasten. Als u met gebruikersaccounts uw eigen gebruikersgroep hebt gemaakt, kunt u deze selecteren. In dit voorbeeld zullen we TestGroup selecteren.

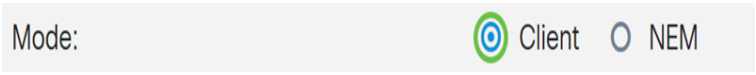
Opmerking: TestGroup is een gebruikersgroep die we in **System Configuration > Gebruikersgroepen** hebben gemaakt.



Opmerking: In dit voorbeeld wordt TestGroup gekozen. U kunt ook het vakje naast de gebruikersgroep controleren en vervolgens op de knop **Verwijderen** klikken als u een gebruikersgroep wilt verwijderen.

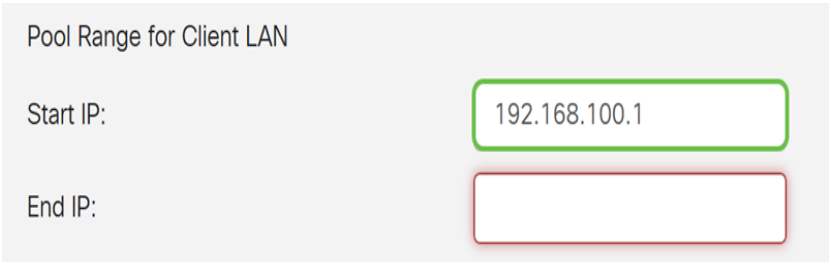
Stap 12. Klik op een radioknop om een modus te kiezen. De opties zijn:

- client - Met deze optie kan de client om een IP-adres vragen en de server levert de IP-adressen van het geconfigureerde adresbereik.
- Network Extension Mode (NEM) - Met deze optie kunnen klanten hun subnetwerk voorstellen waarvoor VPN-services moeten worden toegepast op verkeer tussen LAN achter server en subsysteem dat door client wordt voorgesteld.



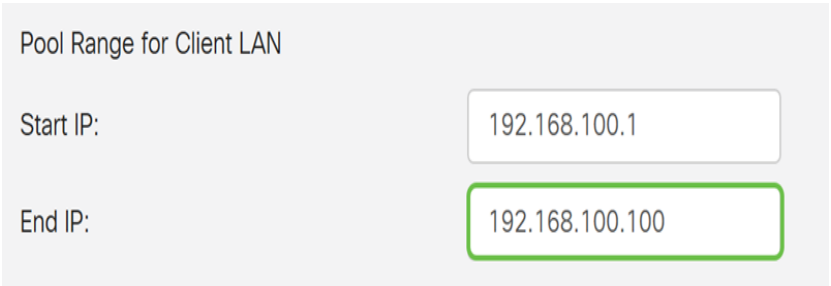
Opmerking: In dit voorbeeld wordt Client geselecteerd.

Stap 13. Voer het beginnende IP-adres in het veld *Start IP in*. Dit is het eerste IP-adres in de pool dat aan een client kan worden toegewezen.



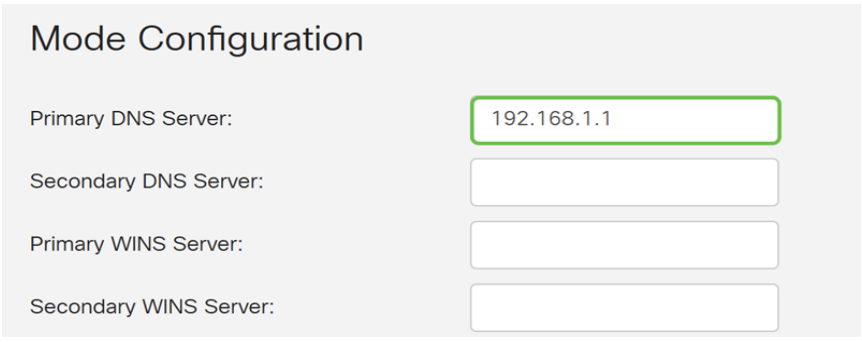
Opmerking: In dit voorbeeld wordt 192.168.100.1 gebruikt.

Stap 14. Voer het laatste IP-adres in het veld *End IP in*. Dit is het laatste IP-adres in de pool dat aan een client kan worden toegewezen.



Opmerking: In dit voorbeeld wordt 192.168.100.100 gebruikt.

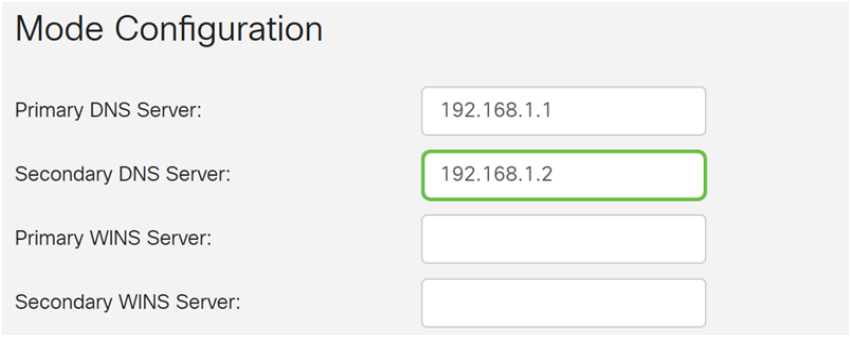
Stap 15. (Optioneel) Onder het gebied *Mode Configuration* voert u het IP-adres in van de primaire DNS-server in het daarvoor bestemde veld.



Opmerking: In dit voorbeeld wordt 192.168.1.1 gebruikt.

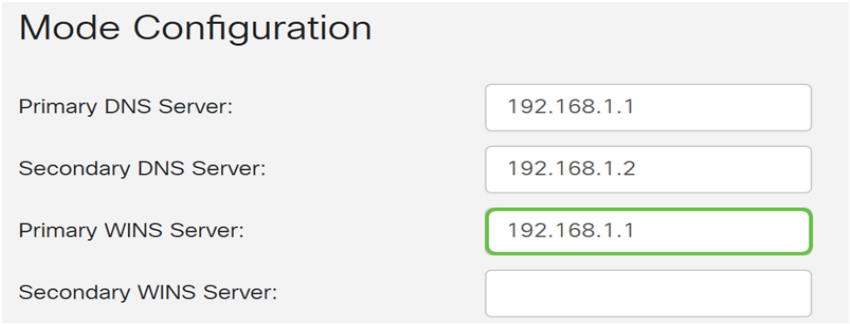
Stap 16. (Optioneel) Voer het IP-adres van de secundaire DNS-server in het daarvoor

bestemde veld.



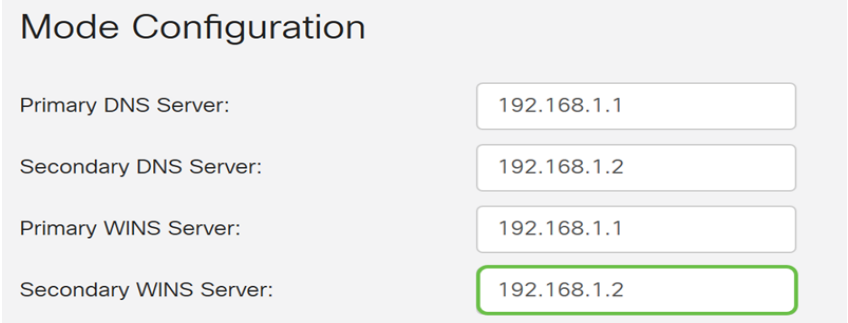
Opmerking: In dit voorbeeld wordt 192.168.1.2 gebruikt.

Stap 17. (Optioneel) Voer het IP-adres in van de primaire WINS-server in het daarvoor bestemde veld.



Opmerking: In dit voorbeeld wordt 192.168.1.1 gebruikt.

Stap 18. (Optioneel) Voer het IP-adres van de secundaire WINS-server in het daarvoor bestemde veld in.



Opmerking: In dit voorbeeld wordt 192.168.1.2 gebruikt.

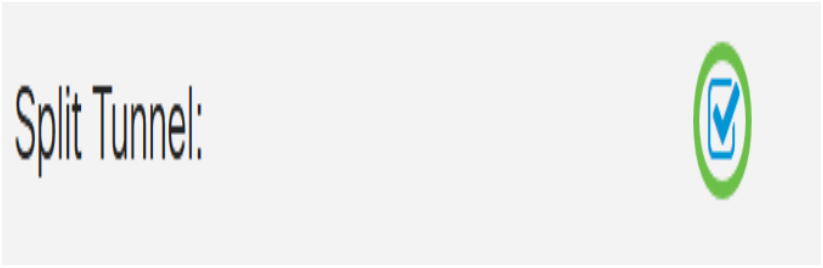
Stap 19. (Optioneel) Voer het standaarddomein in dat in het verstrekte veld op het externe netwerk moet worden gebruikt.

Opmerking: In dit voorbeeld wordt Samsung.com gebruikt.

Stap 20. (Optioneel) Voer in het veld *Backup Server 1* het IP-adres of de domeinnaam van de reserveserver in. Dit zal zijn waar het apparaat de VPN verbinding kan starten voor het geval de primaire IPSec VPN-server faalt. U kunt maximaal drie reserveservers invoeren in de daarvoor bestemde velden. De back-upserver 1 heeft de hoogste prioriteit van de drie servers en de back-upserver 3 heeft de laagste prioriteit.

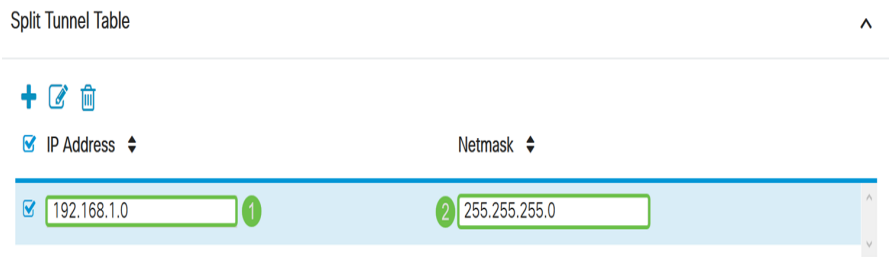
Opmerking: In dit voorbeeld wordt Bijvoorbeeld.com gebruikt voor Reserve Server 1.

Stap 21. (Optioneel) Controleer het aanvinkvakje **Split Tunnel** om gesplitste tunnel in te schakelen. Split-tunneling biedt u tegelijkertijd toegang tot de bronnen van een privaat netwerk en het internet.



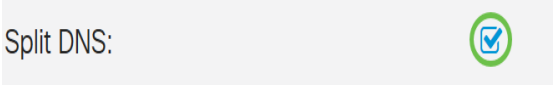
Stap 2. (Optioneel) Onder de *Tabel Split Tunnel* klikt u op het pictogram **plus** om een IP-adres voor gesplitste tunnels toe te voegen.

Stap 23. (Optioneel) Voer het IP-adres en het netmasker van de gesplitste tunnel in de daartoe bestemde velden in.

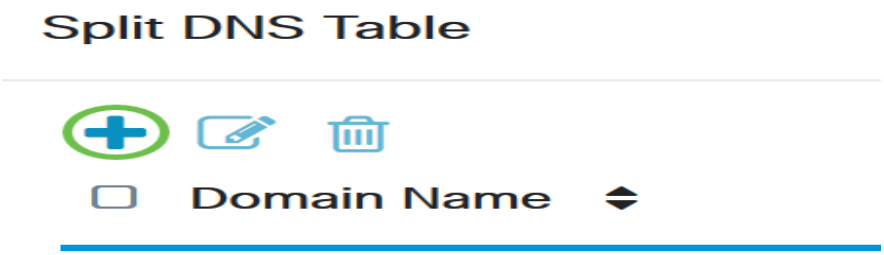


Opmerking: In dit voorbeeld worden 192.168.1.0 en 255.255.255.0 gebruikt. U kunt het vakje ook controleren en op de knoppen **Toevoegen**, **Bewerken** en **Verwijderen** verwijderen die u respectievelijk wilt toevoegen, bewerken of verwijderen.

Stap 24. (Optioneel) Controleer het selectieteken **DNS-**vakje **splitter** om gesplitste DNS in te schakelen. Met Split DNS kunt u afzonderlijke DNS-servers maken voor interne en externe netwerken om de beveiliging en privacy van netwerkbronnen te behouden.



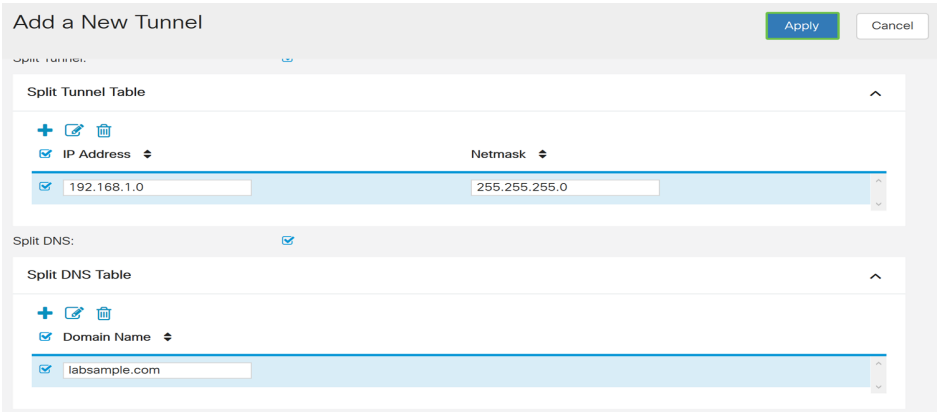
Stap 25. (Optioneel) Klik op het pictogram **plus** onder de *DNS-tabel splitsen* om een domeinnaam voor gesplitste DNS toe te voegen.



Stap 26. (Optioneel) Voer de domeinnaam van de gesplitste DNS in het daarvoor bestemde veld in.

Opmerking: In dit voorbeeld wordt labSamsung.com gebruikt. U kunt het vakje ook controleren en op de knoppen **Toevoegen**, **Bewerken** en **Verwijderen** verwijderen die u respectievelijk een gesplitste DNS wilt toevoegen, bewerken of verwijderen.

Stap 27. Klik op **Toepassen**.



Conclusie

U hebt nu een client-naar-site verbinding ingesteld op de RV34x Series router.

Klik op de volgende artikelen om meer te weten te komen over de volgende onderwerpen:

- Een VPN-client voor Teleworker configureren op de RV34x Series router

- Gebruik de GreenBow VPN-client voor een verbinding met RV34x Series router
- Een gebruikersaccount maken voor VPN-clientinstelling op de RV34x-router
- Een gebruikersgroep voor VPN-instellingen maken op de RV34x-router

Bekijk een video gerelateerd aan dit artikel...

Klik hier om andere Tech Talks uit Cisco te bekijken