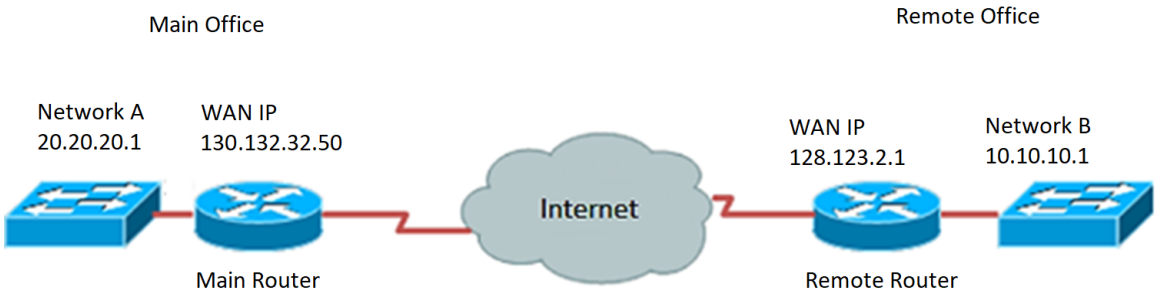
Configuratie van Virtual Private Network (VPN) Connection met de Setup-wizard op de RV34x Series router

Doel

Een Virtual Private Network (VPN)-verbinding stelt gebruikers in staat om toegang te krijgen tot, gegevens te verzenden en te ontvangen van en naar een privaat netwerk door middel van een openbaar of gedeeld netwerk zoals het internet, maar toch beveiligde verbindingen naar een onderliggende netwerkinfrastructuur te waarborgen om het particuliere netwerk en de bijbehorende bronnen te beschermen.

Een VPN-tunnel stelt een privaat netwerk in dat gegevens veilig kan verzenden met behulp van encryptie en verificatie. Bedrijven maken gebruik vooral van VPN-verbinding omdat het zowel nuttig als noodzakelijk is om hun werknemers toegang te geven tot hun privénetwerk, zelfs als ze zich niet binnen het kantoor bevinden.

VPN staat een externe host toe te handelen alsof ze zich op hetzelfde lokale netwerk bevonden. De router ondersteunt 50 tunnels. De wizard van VPN Setup maakt het mogelijk om een beveiligde verbinding te configureren voor een site-to-site IPSec-tunnel. Deze optie maakt de configuratie eenvoudig en voorkomt complexe instellingen en optionele parameters. Op deze manier kan iedereen de IPSec-tunnel snel en efficiënt opzetten.



Voordelen van het gebruik van een VPN-verbinding:

1. Gebruik van een VPN-verbinding om vertrouwelijke netwerkgegevens en -bronnen te beschermen.
2. Verleent gemak en toegankelijkheid voor externe werknemers of bedrijfsmedewerkers, aangezien zij gemakkelijk toegang zullen kunnen krijgen tot het hoofdbureau zonder fysiek aanwezig te moeten zijn en toch de beveiliging van het particuliere netwerk en zijn middelen behouden.
3. Communicatie via een VPN-verbinding biedt een hoger beveiligingsniveau dan andere methoden voor communicatie op afstand. Dankzij de geavanceerde technologie kan dit nu ook, en dus tegen ongeoorloofde toegang, het particuliere netwerk worden beschermd.
4. Feitelijke geografische locaties van de gebruikers worden beschermd en niet blootgesteld aan het publiek of gedeelde netwerken zoals het internet.
5. Het toevoegen van nieuwe gebruikers of groepen gebruikers aan het netwerk is gemakkelijk aangezien VPN's zeer aanpasbaar zijn. Het is mogelijk het netwerk te

laten groeien zonder de behoefte aan extra nieuwe componenten of gecompliceerde configuraties.

Risico's van het gebruik van VPN-verbinding:

1. Beveiligingsrisico door verkeerde configuratie. Aangezien het ontwerp en de implementatie van een VPN gecompliceerd kunnen zijn, is het nodig de taak toe te vertrouwen om de verbinding te configureren naar een zeer deskundig en ervaren professional, om er zeker van te zijn dat de beveiliging van het privénetwerk niet in gevaar komt.
2. Betrouwbaarheid. Aangezien een VPN-verbinding een internetverbinding vereist, is het belangrijk om een provider te kiezen die bewezen en getest is om uitstekende internetservice te bieden en minimaal aan geen downtime te garanderen.
3. schaalbaarheid. In een situatie waarin er nieuwe infrastructuur moet worden toegevoegd of nieuwe configuraties moeten worden ingesteld, kunnen technische problemen ontstaan door incompatibiliteit, vooral als er andere producten of verkopers bij betrokken zijn dan de producten die u al gebruikt.
4. Beveiligingsproblemen voor mobiele apparaten. Soms, wanneer u mobiele apparaten gebruikt wanneer u de VPN-verbinding start, kunnen veiligheidsproblemen ontstaan, vooral bij gebruik van draadloze verbinding. Sommige niet-geverifieerde providers vormen "gratis VPN providers" en kunnen zelfs malware op uw computer installeren. Daarom is het mogelijk om meer veiligheidsmaatregelen toe te voegen om dergelijke problemen bij het gebruik van mobiele apparaten te voorkomen.
5. Lage verbindingssnelheden. Als u een VPN-client gebruikt die gratis VPN-service biedt, kan worden verwacht dat de verbindingssnelheid zal vertragen omdat deze providers geen prioriteit geven aan verbindingssnelheden.

Het doel van dit document is om u te tonen hoe u de VPN-verbinding op de RV34x Series router kunt configureren met behulp van de Setup Wizard.

Toepasselijke apparaten

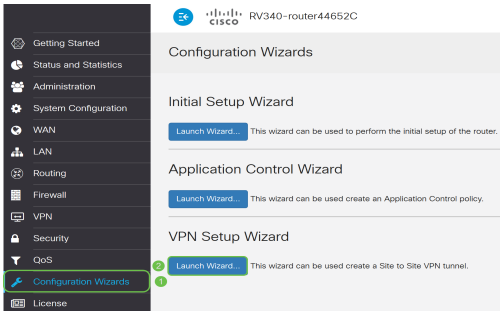
- RV34x Series

Softwareversie

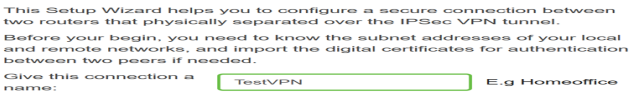
- 1.0.01.16

VPN-verbinding configureren met de installatiewizard

Stap 1. Meld u aan bij het op router gebaseerde hulpprogramma en kies de **wizard Configuration**. Klik vervolgens op **Wizard Start** onder het gedeelte *VPN Setup*.



Stap 2. Voer in het daarvoor bestemde veld een naam in om deze verbinding te identificeren.



Opmerking: In dit voorbeeld wordt TestVPN gebruikt.

Stap 3. Klik in het interfacegebied op het vervolgkeuzemenu en kies de interface die u wilt inschakelen. De opties zijn:

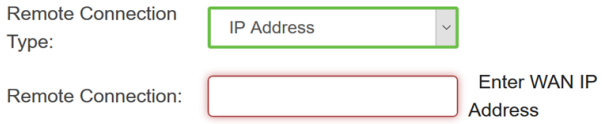
- WAN1
- WAN2
- USB1
- USB2

Opmerking: In dit voorbeeld wordt WAN1 gebruikt.

Stap 4. Klik op **Volgende**.

Stap 5. Kies het type afstandsbediening door op de vervolgkeuzelijst te klikken. De opties zijn:

- IP Address - Kies deze optie als u het IP-adres van de externe router aan het andere uiteinde van de VPN-tunnel wilt gebruiken.
- FQDN - (Full Qualified Domain Name) Kies deze optie als u de domeinnaam van de afstandsrouter aan het andere eind van de VPN-tunnel wilt gebruiken.



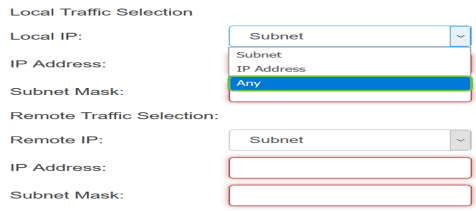
Opmerking: In dit voorbeeld, wordt het IP Adres gekozen.

Stap 6. Voer het WAN IP-adres van de afstandsbediening in en klik op **Volgende**.

Opmerking: In dit voorbeeld wordt 128.123.2.1 gebruikt.

Stap 7. Klik onder het gedeelte Local Traffic Selection Area op de vervolgkeuzelijst om de lokale IP te kiezen. De opties zijn:

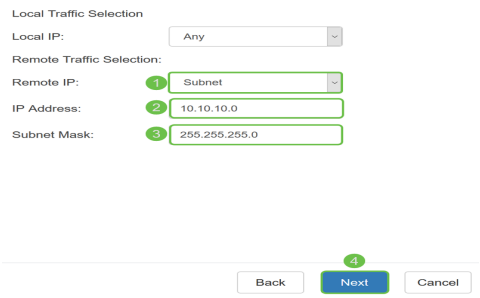
- Subnet — Kies dit als u zowel het IP-adres als het Subnet-masker van het Local Network wilt invoeren.
- IP-adres - Kies dit als u alleen het IP-adres van het lokale netwerk wilt invoeren.
- Kies dit als je een van de twee wilt.



Opmerking: In dit voorbeeld wordt AnyRes gekozen.

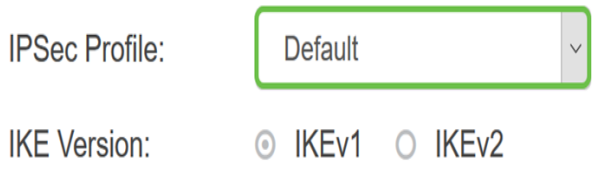
Stap 8. Klik onder het gebied voor selectie van het afstandsverkeer op de vervolgkeuzelijst om de Remote IP-telefoon te kiezen. Voer het externe IP-adres en het subnetmasker in het veld in, mits u op **Volgende** klikt. De opties zijn:

- Subnet — Kies dit als u zowel het IP-adres als het subnetmasker van het externe netwerk wilt invoeren.
- IP-adres - Kies dit als u alleen het IP-adres van het externe netwerk wilt invoeren.



Opmerking: In dit voorbeeld wordt Subnet geselecteerd. 10.10.10.0 werd ingevoerd als IP-adres en 255.255.255.0 werd ingevoerd als het subnetmasker.

Stap 9. Klik op de vervolgkeuzelijst in het gedeelte IPSec Profile om te kiezen welk profiel u wilt gebruiken.



Opmerking: In dit voorbeeld wordt standaard geselecteerd.

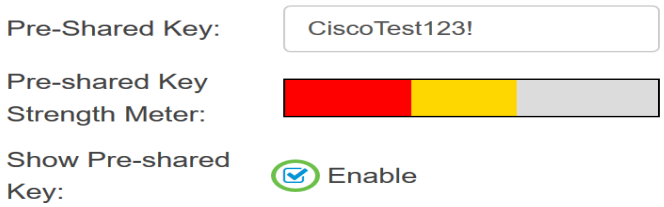
Stap 10. Voer in het veld Fase 1 Opties de vooraf gedeelde sleutel voor deze verbinding in. Dit is de pre-Shared key die wordt gebruikt om de peer van Remote Internet Key Exchange (IKE) te authentiseren. Beide uiteinden van de VPN-tunnel moeten dezelfde vooraf gedeelde toets gebruiken. Er mogen maximaal 30 tekens of hexadecimale waarden voor deze toets worden gebruikt.

Opmerking: Het is sterk geadviseerd om de pre-gedeeld sleutel regelmatig te veranderen om de veiligheid van uw VPN verbinding te handhaven.

Opmerking: De vooraf gedeelde sleutel van de Sterkte geeft de sterkte van de toets aan die u hebt ingevoerd, op basis van het volgende:

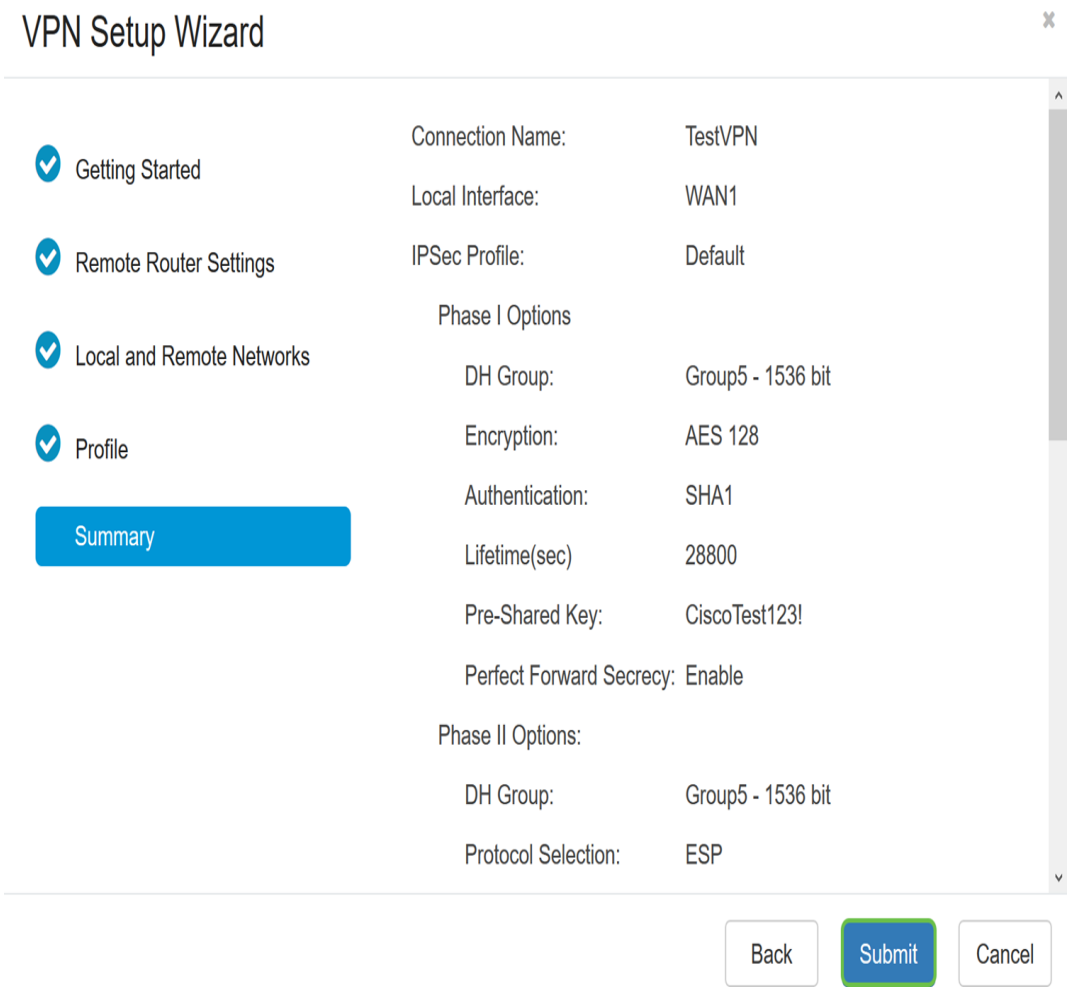
- Rood — Het wachtwoord is zwak.
- Amber — Het wachtwoord is vrij sterk.
- Groen — Het wachtwoord is sterk.

Stap 1. (Optioneel) U kunt ook het vakje Enable controleren in het vak Weergave van onbewerkte tekst om het wachtwoord in onbewerkte tekst te zien.



Stap 12. Klik op **Volgende**.  .

Stap 13. De pagina toont dan alle configuratiedetails van uw VPN-verbinding. Klik op **Inzenden**.



U hebt nu met succes een VPN-verbinding ingesteld op de RV34x Series router met behulp van de Setup-wizard. Om met succes een site-to-site VPN aan te sluiten, zult u de Setup Wizard op de afstandsrouter moeten configureren.