

# Controleer VPN-status op RV016 RV042 RV042G en RV082 VPN-routers

## Doel

Een Virtual Private Network (VPN) is een beveiligde verbinding tussen twee eindpunten. VPN maakt een beveiligde tunnel tussen deze twee eindpunten en biedt beveiliging aan het gegevensverkeer langs de tunnel. Een Virtual Private Network (VPN) is een beveiligde verbinding die binnen een netwerk of tussen netwerken wordt gemaakt. Om deze tunnel goed te laten werken, moet de VPN-configuratie aan beide zijden van de verbinding zorgvuldig worden uitgevoerd en moet bepaalde informatie overeenkomen. Het doel van dit document is uit te leggen hoe u de VPN-status kunt controleren bij RV016, RV042, RV042G en RV082 VPN-routers. VPN's dienen om verkeer tussen gespecificeerde hosts en netwerken te isoleren van het verkeer van onbevoegde hosts en netwerken.

## Toepasselijke apparaten

- RV016
- RV042
- RV042G
- RV082

## Softwareversie

4.2.1.02

## Te controleren gemeenschappelijke VPN-parameters

Om een VPN-verbinding goed te laten werken, moeten de twee uiteinden van de verbinding aan dezelfde vereisten voldoen. Wanneer er een storing is in de VPN verbinding, zijn er twee dingen die je kunt controleren die het verschil kunnen maken. Deze zijn:

- De lokale IP-adresconflicten tussen de twee VPN-endpoints.
- Er zijn verschillen in de instellingen voor versleuteling en verificatie van de twee eindpunten.

In de volgende sectie wordt uitgelegd hoe u het IP-adresschema van een VPN kunt controleren en hoe u de juiste wijzigingen kunt aanbrengen.

### Het LAN IP-adres van de router wijzigen

De LAN interface van beide uiteinden van de VPN verbinding moet deel uitmaken van een ander netwerkadres. Als beide delen tot hetzelfde netwerkadres behoren, werkt de VPN-verbinding niet. De volgende stappen verklaren hoe u wijzigingen kunt aanbrengen in uw LAN IP-adres op RV042-, RV042G- en RV082 VPN-routers.

Stap 1. Log in op het web gebaseerde configuratie hulpprogramma en kies **Setup > Netwerk**. De pagina *Netwerk* wordt geopend:

## Network

Host Name :  (Required by some ISPs)

Domain Name :  (Required by some ISPs)

### IP Mode

Mode	WAN	LAN
<input checked="" type="radio"/> IPv4 Only	IPv4	IPv4
<input type="radio"/> Dual-Stack IP	IPv4 and IPv6	IPv4 and IPv6

IPv4

IPv6

### LAN Setting



MAC Address : 64:9E:F3:88:C6:A4

Device IP Address :

Subnet Mask :

Multiple Subnet :  Enable

### WAN Setting

Interface	Connection Type	Configuration
WAN1	Obtain an IP automatically	
WAN2	Obtain an IP automatically	

### DMZ Setting

Enable DMZ

Stap 2. Voer onder LAN-instelling in het veld IP-adres apparaat een IP-adres in dat behoort tot een ander netwerkadres aan de andere kant van de VPN-verbinding.

**LAN Setting**



MAC Address : 64:9E:F3:88:C6:A4

Device IP Address :

Subnet Mask :  ▼

Multiple Subnet :

**WAN Setting**

Interface	Connection Type	Configuration
WAN1	Obtain an IP automatically	
WAN2	Obtain an IP automatically	

Stap 3. Kies in de vervolgkeuzelijst Subnetmasker het juiste subnetmasker voor uw VPN-verbinding.

Stap 4. (Optioneel) Schakel het selectievakje Enable in om het gebruik van meerdere subnetten in het veld Meervoudige subnet in te schakelen.

Stap 5. Klik op **Opslaan** om de nieuwe instellingen toe te passen.

## Controleer de security parameters van de VPN-verbinding

De beveiligingsinstellingen van de VPN-verbinding moeten aan elk uiteinde van de verbinding hetzelfde zijn. De volgende stappen leggen uit hoe u deze parameters kunt controleren op RV042-, RV042G- en RV082 VPN-routers.

Stap 1. Log in op het web gebaseerde configuratiehulpprogramma en kies **VPN > Gateway om te gateways**. De pagina *Gateway to Gateway* wordt geopend.

## Gateway To Gateway

### Add a New Tunnel

Tunnel No. 1

Tunnel Name : TestTunnel

Interface : WAN1

Enable :

### Local Group Setup

Local Security Gateway Type : IP Only

IP Address : 156.26.31.119

Local Security Group Type : Subnet

IP Address : 192.168.1.0

Subnet Mask : 255.255.255.0

### Remote Group Setup

Remote Security Gateway Type : IP Only

IP Address : 192.0.2.2

Remote Security Group Type : Subnet

IP Address : 192.168.2.0

Subnet Mask : 255.255.255.0

### IPSec Setup

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 1 - 768 bit

Phase 1 Encryption : DES

Phase 1 Authentication : MD5

Phase 1 SA Life Time : 28800 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 1 - 768 bit


Phase 2 Encryption : DES

Phase 2 Authentication : MD5

Phase 2 SA Life Time : 3600 seconds

Preshared Key : VPNkey

Minimum Preshared Key Complexity :  Enable

Preshared Key Strength Meter : 

Advanced +

Save

Cancel

Stap 2. Controleer de volgende parameters. Zorg ervoor dat beide uiteinden van de VPN-verbinding dezelfde instellingen hebben:

- Het type Local Security Group is hetzelfde als het LAN-segment van de lokale router.
- Remote Security Group Type is hetzelfde als het LAN-segment van de externe router.
- Remote Security Gateway Type is het WAN/Internet IP-adres van de externe router.
- De velden voor de IPSec-installatie moeten aan beide zijden van de VPN-tunnel overeenkomen.
- Vooraf gedeelde sleutel moet aan beide zijden van de VPN-tunnel hetzelfde zijn.

Stap 3. (Optioneel) Klik op **Advanced+** voor meer beveiligingseigenschappen. Deze instellingen moeten aan beide zijden van de verbinding hetzelfde zijn.

Stap 4. Klik op **Opslaan** om de nieuwe instellingen toe te passen als er iets is gewijzigd.

## 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.