

# Configuratie van gateway voor VPN-gateway op RV016, RV042, RV042G en RV082 VPN-routers

## Doel

Een Virtual Private Network (VPN) wordt gebruikt om een beveiligde verbinding tussen twee endpoints via een openbaar of gedeeld internet te maken, via een VPN-tunnel. Meer in het bijzonder, staat een gateway-aan-gateway VPN verbinding voor twee routers toe om veilig met elkaar te verbinden en voor een client op één eind om logisch te verschijnen alsof zij een deel van het netwerk aan het andere eind zijn. Hierdoor kunnen gegevens en hulpmiddelen gemakkelijker en veiliger over het internet worden gedeeld.

Configuratie moet op beide routers worden gedaan om een gateway-aan-gateway VPN mogelijk te maken. De configuraties die in de secties *Local Group Setup* en *Remote Group Setup* worden uitgevoerd, moeten tussen de twee routers worden omgekeerd, zodat de lokale groep van de ene de externe groep van de andere is.

Het doel van dit document is uit te leggen hoe u gateway-to-Gateway VPN kunt configureren op RV016, RV042, RV042G en RV082 VPN-Series routers.

## Toepasselijke apparaten

- RV016
- RV042
- RV042G
- RV082

## Softwareversie

- v4.2.2.08

## Gateway configureren voor gateway VPN

Stap 1. Meld u aan bij het hulpprogramma Router Configuration en kies **VPN > Gateway to Gateway**. De pagina *Gateway to Gateway* wordt geopend:

## Gateway To Gateway

### Add a New Tunnel

Tunnel No. 2

Tunnel Name :

Interface :

Enable :

---

### Local Group Setup

Local Security Gateway Type :

IP Address : 0.0.0.0

Local Security Group Type :

IP Address :

Subnet Mask :

---

### Remote Group Setup

Remote Security Gateway Type :

:

Remote Security Group Type :

IP Address :

Subnet Mask :

Om gateway te configureren naar gateway VPN moeten de volgende functies worden geconfigureerd:

1. [Voeg een nieuwe tunnel toe](#)
2. [Instellen lokale groep](#)
3. [Instellen groep op afstand](#)
4. [IPsec-instelling](#)

**Voeg een nieuwe Tunnel toe**

### Gateway To Gateway

Add a New Tunnel

Tunnel No.	2
Tunnel Name :	<input type="text" value="tunnel_new"/>
Interface :	<input type="text" value="WAN1"/>
Enable :	<input checked="" type="checkbox"/>

Tunnel Nr. is een alleen-lezen veld dat de huidige tunnel weergeeft die er gemaakt zal worden.

Stap 1. Voer een naam in voor de VPN-tunnel in het veld Naam van de Tunnel. Het hoeft niet gelijk te zijn aan de naam aan het andere uiteinde van de tunnel.

Stap 2. Kies in de vervolgkeuzelijst Interface de WAN-poort (Wide Area Network) om voor de tunnel te gebruiken.

- WAN1 — De speciale WAN-poort van de RV0XX serie VPN-routers.
- WAN2 — De WAN2/DMZ poort op de RV0X Series VPN-routers. Alleen worden weergegeven in het vervolgkeuzemenu als dit is geconfigureerd als WAN en niet als een DMZ-poort (Demilitariseert Zone).

Stap 3. (Optioneel) Schakel VPN in door het aanvinkvakje in het veld **Inschakelen** in te schakelen. VPN is standaard ingeschakeld.

## Local Group Setup

Opmerking: De configuratie voor de lokale groepsinstellingen op één router moet dezelfde zijn als de configuratie voor de instellingen van de externe groep op de andere router.

## Gateway To Gateway

**Add a New Tunnel**

Tunnel No. : 2

Tunnel Name :

Interface :

Enable :

---

**Local Group Setup**

Local Security Gateway Type :

IP Address : 0.0.0.0

Local Security Group Type :

IP Address :

Subnet Mask :

Stap 1. Kies de juiste router-identificatiemethode om een VPN-tunnel te maken uit de vervolgkeuzelijst Local Security Gateway Type.

- Alleen IP — De lokale router (deze router) wordt herkend op een statisch IP-adres. U kunt deze optie alleen kiezen als de router een statische WAN IP heeft. Het statische WAN IP-adres wordt automatisch weergegeven in het veld IP-adres.
- IP + Domain Name (FQDN)-verificatie — Toegang tot de tunnel is mogelijk door een statisch IP-adres en een geregistreerd domein. Als u deze optie kiest, voert u de naam van het geregistreerde domein in het veld Naam van het domein in. Het statische WAN IP-adres wordt automatisch weergegeven in het veld IP-adres.
- IP + E-mailadres. (USER FQDN) verificatie — toegang tot de tunnel is mogelijk door een statisch IP-adres en een e-mailadres. Als u deze optie kiest, voert u het e-mailadres in het veld E-mailadres in. Het statische WAN IP-adres wordt automatisch weergegeven in het veld IP-adres.
- Dynamische IP + Domain Name (FQDN)-verificatie — Toegang tot de tunnel is mogelijk door een dynamisch IP-adres en een geregistreerd domein. Als u deze optie kiest, voert u de naam van het geregistreerde domein in het veld Naam van het domein in.
- Dynamische IP + e-mailadres.(USER FQDN)-verificatie — Toegang tot de tunnel is mogelijk door een dynamisch IP-adres en een e-mailadres. Als u deze optie kiest, voert u het e-mailadres in het veld E-mailadres in.

Stap 2. Kies de juiste lokale LAN-gebruiker of de groep gebruikers die toegang kunnen krijgen tot de VPN-tunnel in de vervolgkeuzelijst Local Security Group. De standaardinstelling is Subnet.

- IP — Er is slechts één LAN-apparaat dat toegang heeft tot de VPN-tunnel. Als u deze optie kiest, voert u het IP-adres van het LAN-apparaat in het veld IP-adres in.
- Subnet - Alle LAN apparaten op specifieke subnetwerk kunnen tot de tunnel toegang hebben. Als u deze optie kiest, voert u het IP-adres en het subnetwerk-masker van de

LAN-apparaten in het veld IP-adres en subnetmasker in. Het standaardmasker is 255.255.255.0.

- IP-bereik: er is een bereik van LAN-apparaten om toegang te krijgen tot de tunnel. Als u deze optie kiest, voert u het begin- en eindadres in in de IP Beginnen en IP-velden Eindtijd in.

Stap 3. Klik op **Save** om de instellingen op te slaan.

## Instellen afstandsgroep

Opmerking: De configuratie voor de instellingen van de externe groep op één router moet dezelfde zijn als de configuratie voor de lokale instellingen van de groep op de andere router.

The screenshot shows a configuration interface with two main sections: 'Local Group Setup' and 'Remote Group Setup'. The 'Remote Group Setup' section is highlighted with a red border. The 'Local Group Setup' section includes fields for 'Local Security Gateway Type' (set to 'IP + Email Address(USER FQDN) Authentication'), 'Email Address' (set to 'abcd@mail.com'), 'IP Address' (set to '0.0.0.0'), 'Local Security Group Type' (set to 'IP'), and 'IP Address' (set to '192.168.1.1'). The 'Remote Group Setup' section includes fields for 'Remote Security Gateway Type' (set to 'IP Only'), 'IP Address' (empty), 'Remote Security Group Type' (set to 'Subnet'), 'IP Address' (empty), and 'Subnet Mask' (set to '255.255.255.0').

Stap 1. Kies in de vervolgkeuzelijst Type beveiligingsgateway op afstand de methode om de externe router te identificeren om de VPN-tunnel op te zetten.

- Alleen IP — Toegang tot de tunnel is mogelijk via een statische WAN IP. Als u het IP-adres van de externe router kent, kiest u IP-adres uit de vervolgkeuzelijst direct onder het veld Type security gateway en geeft u het IP-adres in. Kies IP door DNS Opgelost als u het IP-adres niet weet maar de domeinnaam wel kent en voer de domeinnaam van de router in het IP met DNS Opgeloste veld in.
- IP + Domain Name (FQDN)-verificatie — Toegang tot de tunnel is mogelijk door een statisch IP-adres en een geregistreerd domein voor de router. Als u het IP-adres van de externe router kent, kiest u IP-adres in de vervolgkeuzelijst direct onder het veld Type security gateway en geeft u het adres in. Kies IP door DNS Opgelost als u het IP-adres niet weet maar de domeinnaam wel kent en voer de domeinnaam van de router in het IP met DNS Opgeloste veld in. Voer de domeinnaam van de router in het veld Naam van het domein in, ongeacht de methode die u kiest om deze te identificeren.
- IP + E-mailadres. (USER FQDN) verificatie — toegang tot de tunnel is mogelijk door een

statisch IP-adres en een e-mailadres. Als u het IP-adres van de externe router kent, kiest u IP-adres in de vervolgkeuzelijst direct onder het veld Afstandsgateway en voert u het adres in. Kies IP door DNS Opgelost als u het IP-adres niet weet maar de domeinnaam wel kent en voer de domeinnaam van de router in het IP met DNS Opgeloste veld in. Voer het e-mailadres in het veld E-mailadres.

- Dynamische IP + Domain Name (FQDN)-verificatie — Toegang tot de tunnel is mogelijk door een dynamisch IP-adres en een geregistreerd domein. Als u deze optie kiest, voert u de naam van het geregistreerde domein in het veld Naam van het domein in.
- Dynamische IP + e-mailadres.(USER FQDN)-verificatie — Toegang tot de tunnel is mogelijk door een dynamisch IP-adres en een e-mailadres. Als u deze optie kiest, voert u het e-mailadres in het veld E-mailadres in.

Stap 2. Kies de juiste externe LAN-gebruiker of groep gebruikers die toegang kunnen krijgen tot de VPN-tunnel uit de vervolgkeuzelijst Afstandsbeveiligingsgroep.

- IP — Er kan slechts één specifiek LAN-apparaat toegang hebben tot de tunnel. Als u deze optie kiest, voert u het IP-adres van het LAN-apparaat in het veld IP-adres in.
- Subnet — Alle LAN apparaten op een specifiek netwerk kunnen tot de tunnel toegang hebben. Als u deze optie kiest, voert u het IP-adres en het subnetwerk-masker van de LAN-apparaten in het veld IP-adres en subnetmasker in.
- IP-bereik: er is een bereik van LAN-apparaten om toegang te krijgen tot de tunnel. Als u deze optie kiest, voert u het begin- en eindadres in in de IP Beginnen en IP-velden Eindtijd in.

Opmerking: De twee routers aan het eind van de tunnel kunnen niet op zelfde subnet zijn.

Stap 3. Klik op **Save** om de instellingen op te slaan.

## IPsec-instelling

**IPSec Setup**

Keying Mode :

Phase 1 DH Group :

Phase 1 Encryption :

Phase 1 Authentication :

Phase 1 SA Life Time :  seconds

Perfect Forward Secrecy :

Phase 2 DH Group :

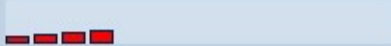
Phase 2 Encryption :

Phase 2 Authentication :

Phase 2 SA Life Time :  seconds

Preshared Key :

Minimum Preshared Key Complexity :  Enable

Preshared Key Strength Meter : 

Internet Protocol Security (IPSec) is een protocol voor de beveiliging van de internetlaag dat end-to-end beveiliging biedt door middel van verificatie en encryptie tijdens elke communicatiesessie.

Opmerking: Beide extremen van VPN moeten dezelfde methoden voor encryptie, decryptie en authenticatie hebben om goed te werken. Voer dezelfde IPSec Setup-instellingen voor beide routers in.

**IPSec Setup**

Keying Mode : IKE with Preshared key  
Manual  
IKE with Preshared key

Phase 1 DH Group : Manual  
IKE with Preshared key

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 :

Minimum Preshared Key Complexity :  Enable

Preshared Key Strength Meter :

Stap 1. Kies de juiste modus van het sleutelbeheer om beveiliging te garanderen in de vervolgkeuzelijst Keying Mode. De standaardmodus is IKE met de PreShared key.

- [Handmatig](#) - Een aangepaste veiligheidsmodus om zelf een nieuwe beveiligingssleutel te genereren en geen onderhandeling met de toets. Het is het beste om tijdens het oplossen van problemen en in een klein statisch milieu te gebruiken.
- [IKE met PreShared Key](#) — Internet Key Exchange (IKE)-protocol wordt automatisch gebruikt om een vooraf gedeelde sleutel te genereren en uit te wisselen om voor de tunnel authenticatie-communicatie tot stand te brengen.

### IPsec-instelling voor handmatige modus

**IPSec Setup**

Keying Mode : Manual

Incoming SPI : 101

Outgoing SPI : 101

Encryption : DES

Authentication : MD5

Encryption Key :

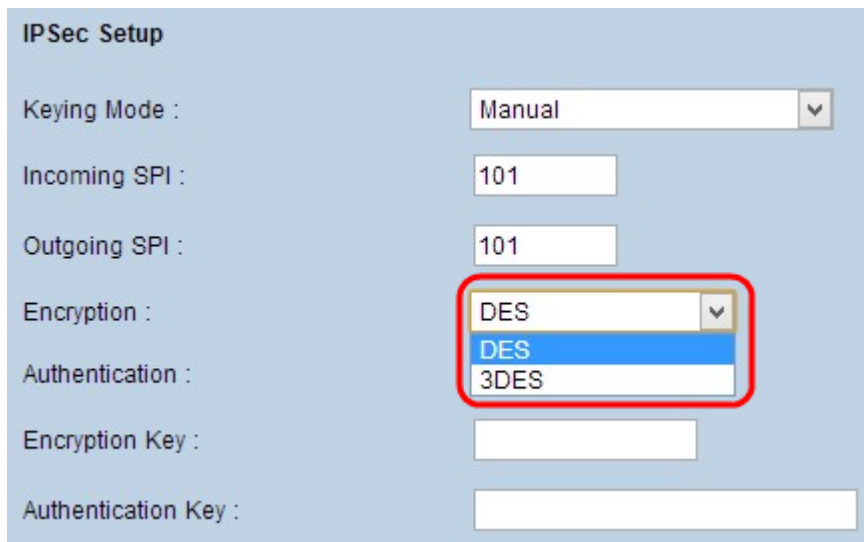
Authentication Key :



Stap 1. Voer de unieke hexadecimale waarde in voor inkomende security parameter Index (SPI) in het veld Inkomende SPI. SPI wordt in de ESP-header (Encapsulation Security Payload Protocol) toegevoegd en bepaalt de beveiliging van het inkomende pakket. U kunt een waarde van 100 tot in het veld invoeren. De inkomende SPI van de lokale router moet met de uitgaande SPI van de afstandsrouter overeenkomen.

Stap 2. Voer de unieke hexadecimale waarde in voor de uitgaande Security Parameter Index (SPI) in het veld Uitgaande SPI. U kunt een waarde van 100 tot in het veld invoeren. De uitgaande SPI van de externe router moet worden afgestemd op de inkomende SPI van de lokale router.

Opmerking: Geen twee tunnels kunnen dezelfde SPI hebben.



IPSec Setup

Keying Mode : Manual

Incoming SPI : 101

Outgoing SPI : 101

Encryption : DES

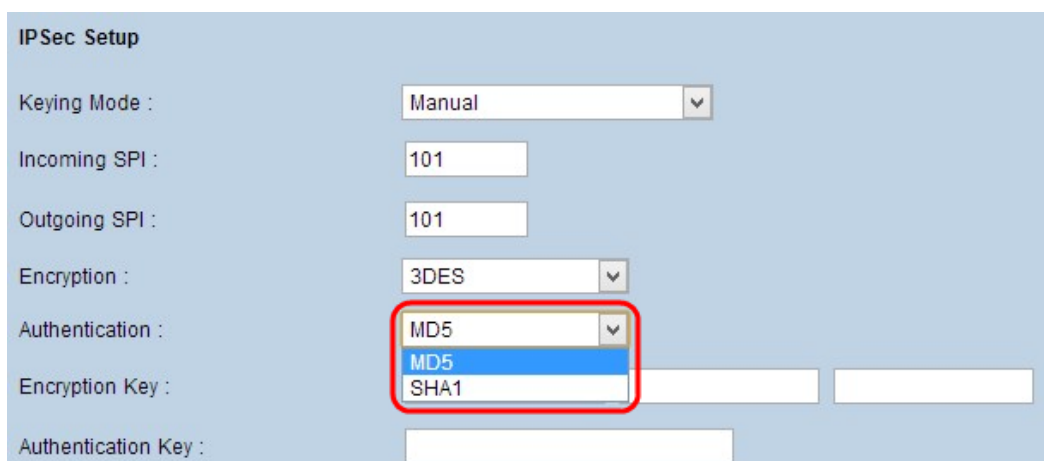
Authentication : DES

Encryption Key :

Authentication Key :

Stap 3. Kies de juiste coderingsmethode voor de gegevens in de vervolgkeuzelijst Encryptie. De aanbevolen codering is 3DES. De VPN-tunnel moet aan beide kanten dezelfde encryptiemethode toepassen.

- DES - Data Encryption Standard (DES) gebruikt een 56-bits sleutelformaat voor gegevensencryptie. DES is verouderd en mag alleen worden gebruikt als één eindpunt alleen DES ondersteunt.
- 3DES - Triple Data Encryption Standard (3DES) is een 168 bit, eenvoudige coderingsmethode. 3DES versleutelt de gegevens drie keer, waardoor er meer beveiliging is dan DES.



IPSec Setup

Keying Mode : Manual

Incoming SPI : 101

Outgoing SPI : 101

Encryption : 3DES

Authentication : MD5

Encryption Key :

Authentication Key :

Stap 4. Kies de juiste verificatiemethode voor de gegevens uit de vervolgkeuzelijst



**IPSec Setup**

Keying Mode : IKE with Preshared key

Phase 1 DH Group : **Group 1 - 768 bit**

Phase 1 Encryption : MD5

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 :

Minimum Preshared Key Complexity :  Enable

Preshared Key Strength Meter : 

Stap 1. Kies de juiste fase 1 DH-groep uit de vervolgkeuzelijst Fase 1 DH-groep. Fase 1 wordt gebruikt om de simplex, logical security association (SA) tussen de twee uiteinden van de tunnel aan te leggen ter ondersteuning van beveiligde communicatie. Diffie-Hellman (DH) is een cryptografisch zeer belangrijk uitwisselingsprotocol dat wordt gebruikt om de sterkte van de sleutel tijdens Fase 1 te bepalen en het deelt ook de geheime sleutel om de communicatie te authenticeren.

- Groep 1 - 768 bit — De laagste sterkte en de meest onveilige authenticatiegroep, maar neemt de minste tijd in beslag om de IKE-toetsen te berekenen. Deze optie heeft de voorkeur wanneer de snelheid van het netwerk laag is.
- Groep 2 - 1024 bit - Een hogere sterktesleutel en een veiliger authenticatiegroep dan groep 1, maar het kost meer tijd om de IKE-toetsen te berekenen.
- Groep 5 - 1536 bit - De hoogste sterktesleutel en de meest beveiligde authenticatiegroep. Het heeft meer tijd nodig om de IKE-toetsen te berekenen. Het is de voorkeur dat de snelheid van het netwerk hoog is.

**IPSec Setup**

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 2 - 1024 bit

Phase 1 Encryption : **DES**

Phase 1 Authentication : DES

Phase 1 SA Life Time : 3600 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 1 - 768 bit

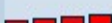
Phase 2 Encryption : DES

Phase 2 Authentication : MD5

Phase 2 SA Life Time : 3600 seconds

Preshared Key :

Minimum Preshared Key Complexity :  Enable

Preshared Key Strength Meter : 

Stap 2. Kies de juiste fase 1-encryptie om de sleutel te versleutelen uit de vervolgkeuzelijst Fase 1 Encryption. AES-128, AES-192, of AES-256 worden aanbevolen. De VPN-tunnel moet dezelfde encryptie-methode voor beide eindpunten gebruiken.

- DES - Data Encryption Standard (DES) gebruikt een 56-bits sleutelformaat voor gegevensencryptie. DES is verouderd en mag alleen worden gebruikt als één eindpunt alleen DES ondersteunt.
- 3DES - Triple Data Encryption Standard (3DES) is een 168 bit, eenvoudige coderingsmethode. 3DES versleutelt de gegevens drie keer, waardoor er meer beveiliging is dan DES.
- AES-128 — Advanced Encryption Standard (AES) is een 128-bits coderingsmethode waarmee de onbewerkte tekst door 10-cycli wordt herhaald.
- AES-192 — Advanced Encryption Standard (AES) is een 192-bits coderingsmethode waarmee de onbewerkte tekst door 12-cycli wordt herhaald. AES-192 is veiliger dan AES-128.
- AES-256 — Advanced Encryption Standard (AES) is een 256-bits coderingsmethode waarmee de onbewerkte tekst door 14-cycli wordt herhaald. AES-256 is de best beveiligde coderingsmethode.

**IPSec Setup**

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 2 - 1024 bit

Phase 1 Encryption : 3DES

Phase 1 Authentication : MD5

Phase 1 SA Life Time : 3600 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 :

Minimum Preshared Key Complexity :  Enable

Preshared Key Strength Meter : 

Stap 3. Kies de juiste fase 1-verificatiemethode in de vervolgkeuzelijst Fase 1-verificatie. De VPN-tunnel moet voor beide uiteinden dezelfde verificatiemethode gebruiken. SHA1 wordt aanbevolen.

- MD5 — Message Digest Algorithm-5 (MD5) is een 128-bits hashfunctie die bescherming biedt aan de gegevens tegen boosaardige aanvallen door de berekening van de checksum.
- SHA1 — Secure Hash Algorithm, versie 1 (SHA1) is een 160-bits hashfunctie die veiliger is dan MD5, maar u hoeft er meer tijd voor te berekenen.

**IPSec Setup**

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 2 - 1024 bit

Phase 1 Encryption : 3DES

Phase 1 Authentication : MD5

Phase 1 SA Life Time : 27800 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 :

Minimum Preshared Key Complexity :  Enable

Preshared Key Strength Meter :



Stap 4. Voer de hoeveelheid tijd in seconden in dat de toetsen Fase 1 geldig zijn en de VPN-tunnel actief blijft in het veld Fase 1 SA Life Time.

Stap 5. Controleer het vakje **Perfect Forward Security (Perfect Forward Security)** om meer bescherming aan de toetsen te bieden. Deze optie staat de router toe om een nieuwe sleutel te genereren als er een toets wordt gecompromitteerd. De versleutelde gegevens worden alleen via de gecompromitteerde toets gecompromitteerd. Dit is een aanbevolen actie omdat deze meer beveiliging biedt.



**IPSec Setup**

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 2 - 1024 bit

Phase 1 Encryption : 3DES

Phase 1 Authentication : MD5

Phase 1 SA Life Time : 27800 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 1 - 768 bit

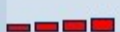
Phase 2 Encryption : 3DES

Phase 2 Authentication : MD5

Phase 2 SA Life Time : 3600 seconds

Preshared Key :

Minimum Preshared Key Complexity :  Enable

Preshared Key Strength Meter : 

Stap 6. Kies de juiste fase 2 DH-groep uit de vervolgkeuzelijst Fase 2 DH-groep. Fase 2 gebruikt Security Association en wordt gebruikt om de beveiliging van het gegevenspakket vast te stellen terwijl deze door de twee eindpunten loopt.

- Groep 1 - 768 bit - De laagste sterkte en de meest onveilige authenticatiegroep, maar neemt de minste tijd in beslag om de IKE-toetsen te berekenen. Deze optie heeft de voorkeur wanneer de snelheid van het netwerk laag is.
- Groep 2 - 1024 bit - Een hogere sterktesleutel en een veiliger authenticatiegroep dan groep 1, maar vergt meer tijd om de IKE-toetsen te berekenen.
- Groep 5 - 1536 bit - De hoogste sterktesleutel en de meest beveiligde authenticatiegroep. Het heeft meer tijd nodig om de IKE-toetsen te berekenen. Het is de voorkeur dat de snelheid van het netwerk hoog is.

**IPSec Setup**

Keying Mode :

Phase 1 DH Group :

Phase 1 Encryption :

Phase 1 Authentication :

Phase 1 SA Life Time :  seconds

Perfect Forward Secrecy :

Phase 2 DH Group :

Phase 2 Encryption :

Phase 2 Authentication :

Phase 2 SA Life Time :

Preshared Key :

Minimum Preshared Key Complexity :  Enable

Preshared Key Strength Meter :

Stap 7. Kies de juiste fase 2-encryptie om de sleutel te versleutelen uit de vervolgkeuzelijst Fase 2 Encryptie. AES-128, AES-192, of AES-256 worden aanbevolen. De VPN-tunnel moet dezelfde encryptie-methode voor beide eindpunten gebruiken.

- NULL — Er wordt geen encryptie gebruikt.
- DES - Data Encryption Standard (DES) gebruikt een 56-bits sleutelformaat voor gegevensencryptie. DES is verouderd en mag alleen worden gebruikt als één eindpunt alleen DES ondersteunt.
- 3DES - Triple Data Encryption Standard (3DES) is een 168 bit, eenvoudige coderingsmethode. 3DES versleutelt de gegevens drie keer, waardoor er meer beveiliging is dan DES.
- AES-128 — Advanced Encryption Standard (AES) is een 128-bits coderingsmethode waarmee de onbewerkte tekst door 10-cyclusherhalingen in een algoritme wordt omgezet.
- AES-192 — Advanced Encryption Standard (AES) is een 192-bits coderingsmethode waarmee de onbewerkte tekst door 12-cyclusherhalingen in een algoritme wordt omgezet. AES-192 is veiliger dan AES-128.
- AES-256 — Advanced Encryption Standard (AES) is een 256-bits coderingsmethode waarmee de onbewerkte tekst door 14-cyclusherhalingen in een algoritme wordt omgezet. AES-256 is de best beveiligde coderingsmethode.



**IPSec Setup**

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 2 - 1024 bit

Phase 1 Encryption : 3DES

Phase 1 Authentication : MD5

Phase 1 SA Life Time : 27800 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 2 - 1024 bit

Phase 2 Encryption : DES

Phase 2 Authentication : MD5

Phase 2 SA Life Time :

Preshared Key :

Minimum Preshared Key Complexity :  Enable

Preshared Key Strength Meter :

Stap 8. Kies de juiste verificatiemethode in de vervolgkeuzelijst Fase 2-verificatie. De VPN-tunnel moet voor beide eindpunten dezelfde verificatiemethode gebruiken. SHA1 wordt aanbevolen.

- MD5 — Message Digest Algorithm-5 (MD5) is een 128-bits hexadecimale hashfunctie die bescherming biedt aan de gegevens van kwaadaardige aanvallen door de berekening van de checksum.
- SHA1 — Secure Hash Algorithm, versie 1 (SHA1) is een 160-bits hashfunctie die veiliger is dan MD5, maar u hoeft er meer tijd voor te berekenen.
- Volledig - Er wordt geen echtheidscontrole gebruikt.

**IPSec Setup**

Keying Mode :

Phase 1 DH Group :

Phase 1 Encryption :

Phase 1 Authentication :

Phase 1 SA Life Time :  seconds

Perfect Forward Secrecy :

Phase 2 DH Group :

Phase 2 Encryption :

Phase 2 Authentication :

Phase 2 SA Life Time :  seconds

Preshared Key :

Minimum Preshared Key Complexity :  Enable

Preshared Key Strength Meter :

Stap 9. Voer de hoeveelheid tijd in seconden in dat de toetsen Fase 2 geldig zijn en de VPN-tunnel actief blijft in het veld Fase 2 SA Life Time.

Stap 10. Voer een toets in die eerder door de IKE-peers wordt gedeeld om de peers in het veld Voorgedeelde sleutel te authentifieren. Tot 30 hexadecimaal en teken kunnen als de voorgedeelde sleutel worden gebruikt. De VPN-tunnel moet dezelfde vooraf gedeelde toets gebruiken voor beide eindpunten.

Opmerking: Het is sterk aanbevolen om regelmatig de gedeelde sleutel tussen de IKE-peers te wijzigen, zodat VPN veilig blijft.

Stap 1. (Optioneel) Als u de sterktemeter voor de voorgedeelde toets wilt inschakelen, schakelt u het vakje **Minimale Gepineerde Key Complexity** in. Deze wordt gebruikt om de sterkte van de voorgedeelde toets door middel van kleurbalken te bepalen.

- Voorgedeelde sleutel met sterke punten — Dit toont de kracht van de voorgedeelde toets door gekleurde balken. Rood wijst op zwakke sterkte, geel op aanvaardbare sterkte en groen op sterke sterkte.

Stap 12. Klik op **Opslaan** om de instellingen op te slaan.

Opmerking: Als u de opties wilt configureren die in het gedeelte *Advanced* voor Gateway to Gateway VPN beschikbaar zijn, verwijst u naar het artikel en [vormt u Geavanceerde instellingen voor gateway naar Gateway VPN op RV016, RV042, RV042G en RV082 VPN-routers](#).

## 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.