

Een externe access tunnel (client naar gateway) instellen voor VPN-clients op RV016, RV042, RV042G en RV082 VPN-routers

Doel

In dit artikel wordt uitgelegd hoe u externe VPN-tunnels (Virtual Private Network) kunt configureren van client naar gateway op RV016, RV042, RV042G en RV082 VPN-routers met behulp van VPN-clientsoftware van derden als The Green Bow of VPN Tracker.

Inleiding

Een VPN is een privaat netwerk dat wordt gebruikt om apparaten van de externe gebruiker virtueel aan te sluiten via het openbare netwerk om beveiliging te bieden. Remote-toegangstunnel VPN is het proces dat wordt gebruikt om een VPN te configureren tussen een clientcomputer en een netwerk. De client is geconfigureerd op de desktop of laptop van de gebruikers via VPN-clientsoftware. Het biedt de gebruikers om veilig verbinding te maken met het netwerk op afstand. De client naar gateway VPN verbinding is handig voor de externe medewerkers om op afstand en veilig verbinding te maken met het kantoornetwerk.

Toepasselijke apparaten

- RV016
- RV042
- RV042G-router
- RV082

Softwareversie

- v4.2.2.08

Een VPN-tunnel configureren

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

Client To Gateway

Add a New Tunnel

Tunnel Group VPN

Tunnel No. 1

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 Client Setup

Remote Security Gateway Type : ▼

▼ :

IPSec Setup

Een nieuwe tunnel toevoegen

Stap 1. Klik op de juiste keuzerondje volgens het soort tunnel dat u wilt toevoegen.

- Tunnel - vertegenwoordigt een tunnel voor één externe gebruiker.
- Groep VPN - Vertegenwoordigt een tunnel voor een externe groep gebruikers.

Client To Gateway

Add a New Tunnel

Tunnel Group VPN

Tunnel No. : 1

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 Client Setup

Remote Security Gateway Type :

:

IPSec Setup

Het tunnelnummer is een automatisch gegenereerd veld dat het nummer van de tunnel weergeeft.

Client To Gateway

Add a New Tunnel

Tunnel Group VPN

Tunnel No. 1

Tunnel Name : tunnel_1

Interface : WAN1

Enable :

Local Group Setup

Local Security Gateway Type : IP Only

IP Address : 0.0.0.0

Local Security Group Type : Subnet

IP Address : 192.168.1.0

Subnet Mask : 255.255.255.0

Remote Client Setup

Remote Security Gateway Type : IP Only

IP Address :

IPSec Setup

Stap 2. Voer een naam in voor de tunnel in het veld Tunnelnaam.

Stap 3. Kies de juiste WAN-interface die u voor de VPN-tunnel wilt gebruiken in de vervolgkeuzelijst Interface.

Stap 4. (Optioneel) Om VPN in te schakelen, schakelt u het aankruisvakje in het veld Inschakelen in. Standaard wordt deze altijd gecontroleerd.

Lokale groep instellen

Stap 1. Kies de juiste methode voor routeridentificatie om een VPN-tunnel te maken uit de vervolgkeuzelijst *Local Security Gateway*. Sla deze stap over als u Groep VPN hebt gekozen in Stap 1 van de sectie *Een nieuwe tunnel toevoegen*.

Client To Gateway

Add a New Tunnel

Tunnel Group VPN

Tunnel No. : 1

Tunnel Name : tunnel_1

Interface : WAN1

Enable :

Local Group Setup

Local Security Gateway Type : IP Only

IP Address : [empty]

Local Security Group Type : [empty]

IP Address : 192.168.1.1

Subnet Mask : 255.255.255.0

Remote Client Setup

Remote Security Gateway Type : IP Only

IP Address : [empty]

IPSec Setup

Keying Mode : IKE with Preshared key

- IP Only - toegang tot de tunnel is mogelijk via een statisch WAN IP-adres. U kunt deze optie alleen kiezen als de router een statisch WAN IP heeft. Het statische WAN IP-adres wordt automatisch weergegeven.
- IP + Domeinnaam (FQDN) Verificatie - Toegang tot de tunnel is mogelijk via een statisch IP-adres en een geregistreerd FQDN-domein. Het statische WAN IP-adres is een automatisch gegenereerd veld.
- IP + E-mail adres (USER FQDN) verificatie - Toegang tot de tunnel is mogelijk via een statisch IP-adres en een e-mailadres. Het statische WAN IP-adres is een automatisch gegenereerd veld.
- Dynamic IP + Domain Name (FQDN) Verificatie - Toegang tot de tunnel is mogelijk via een dynamisch IP-adres en een geregistreerd domein.
- Dynamische IP + E-mail adres (USER FQDN) verificatie - Toegang tot de tunnel is mogelijk via een dynamisch IP-adres en een e-mailadres.

Stap 2. Voer in het veld Domeinnaam de naam in van het geregistreerde Volledig gekwalificeerde domein als u in Stap 1 voor de verificatie van IP + Domeinnaam (FQDN) of Dynamic IP + Domain Name (FQDN) kiest.

Stap 3. Voer het e-mailadres in het veld E-mailadres in als u in Stap 1 de optie IP + E-mail adres (USER FQDN) verificatie of Dynamic IP + E-mail adres (USER FQDN) verificatie kiest.

Stap 4. Kies de gewenste lokale LAN-gebruiker of groep gebruikers die toegang hebben tot de VPN-tunnel in de vervolgkeuzelijst Local Security Group. De standaardinstelling is Subnet.

- IP - slechts één specifiek LAN-apparaat kan toegang tot de tunnel krijgen. Als u deze optie kiest, voert u het IP-adres van het LAN-apparaat in het veld IP-adres in. Het standaard IP-adres is 192.168.1.0.

- Subnet - Alle LAN-apparaten op een specifieke subnetverbinding kunnen toegang krijgen tot de tunnel. Als u deze optie kiest, voert u het IP-adres en subnetmasker van de LAN-apparaten in het veld IP-adres en subnetmasker in. Het standaardmasker is 25.255.255.0.
- IP-bereik - Een reeks LAN-apparaten kan toegang tot de tunnel krijgen. Als u deze optie kiest, voert u het begin- en eindadres van het IP-adres in in de velden Begin IP en Einde IP in. Het standaardbereik loopt van 192.168.1.0 tot 192.168.1.254.

Client To Gateway

Add a New Tunnel

Tunnel Group VPN

Tunnel No. : 1

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 Client Setup

Remote Security Gateway Type :

:

IPSec Setup

Keying Mode :

Stap 5. Klik op **Opslaan** om de instellingen op te slaan.

Instellen externe client

Stap 1. Als u Tunnel kiest, kies de juiste client-identificatiemethode om een VPN-tunnel te maken uit de vervolgkeuzelijst *Remote Security Gateway-type*. De standaardinstelling is alleen IP. Sla deze stap over als Group VPN in Stap 1 van de sectie *Add A New Tunnel* is gekozen.

Client To Gateway

Add a New Tunnel

Tunnel Group VPN

Tunnel No. : 1

Tunnel Name :

Interface :

Enable :

Local Group Setup

Local Security Gateway Type :

IP Address :

Local Security Group Type :

IP Address :

Subnet Mask :

Remote Client Setup

Remote Security Gateway Type :

IP Address :

IPSec Setup

Keying Mode :

- IP Only - toegang tot de tunnel is alleen mogelijk via het statische WAN IP van de client. U moet het statische WAN IP van de client kennen om deze optie te gebruiken.
- IP + Domain Name (FQDN) verificatie - Toegang tot de tunnel is mogelijk via een statisch IP-adres van de client en een geregistreerd domein.
- IP + E-mail adres (USER FQDN) verificatie - Toegang tot de tunnel is mogelijk via een statisch IP-adres van de client en een e-mailadres.
- Dynamic IP + Domain Name (FQDN) Verificatie - Toegang tot de tunnel is mogelijk via een dynamisch IP-adres van de client en een geregistreerd domein.
- Dynamische IP + E-mail adres (USER FQDN) verificatie - Toegang tot de tunnel is mogelijk via een dynamisch IP-adres van de client en een e-mailadres.

Stap 2. Voer het IP-adres van de externe client in het veld *IP-adres* in als u in Stap 1 de optie *Alleen IP*, *IP + Domeinnaam (FQDN)* of *IP + E-mailadresverificatie (FQDN)* hebt gekozen.

Stap 3. Kies de gewenste optie in de vervolgkeuzelijst om het IP-adres in te voeren als u het weet of los het IP-adres op van de DNS-server als u in stap 1 de optie *IP Only* of *IP + Domain Name (FQDN)* of *IP + E-mail Address (USER FQDN) verificatie* kiest.

- IP-adres - Geeft het statische IP-adres van de externe client weer. Voer in het veld het statische IP-adres in.
- IP by DNS Resolved - Vertegenwoordigt de domeinnaam van het IP-adres dat het IP-adres automatisch via de lokale DNS-server ophalen als u het statische IP-adres van de externe client niet kent. Voer in het veld de domeinnaam van het IP-adres in.

Stap 4. Voer in het veld Domeinnaam de domeinnaam van het IP-adres in als u in Stap 1 voor *IP + Domeinnaam (FQDN) verificatie* of *Dynamic IP + Domain Name (FQDN) verificatie* kiest.

Stap 5. Voer het e-mailadres in het veld E-mailadres in als u in Stap 1 de optie *IP + E-mail adres (USER FQDN) verificatie* of *Dynamic IP + E-mail Address (USER FQDN) verificatie* kiest.

Stap 6. Als u Groep kiest, kiest u het juiste type externe client in de vervolgkeuzelijst *Externe client*. Sla deze stap over als Tunnel VPN in Stap 1 van de sectie *Een nieuwe tunnel toevoegen* is gekozen.

- Domain Name (FQDN) - Toegang tot de tunnel is mogelijk via een geregistreerd domein. Als u deze optie kiest, voert u de naam van het geregistreerde domein in het veld Domeinnaam in.
- E-mail Addr. (USER FQDN) - Toegang tot de tunnel is mogelijk via een e-mailadres van de client. Als u deze optie kiest, voert u het e-mailadres in het veld E-mailadres in.
- Microsoft XP/2000 VPN-client - Toegang tot de tunnel is mogelijk via Microsoft XP of Microsoft 2000 Windows-software. Externe gebruikers met Microsoft VPN-clientsoftware hebben toegang tot de tunnel via de software.

Client To Gateway

Add a New Group VPN

Tunnel Group VPN

Group No. 1

Tunnel Name : Tunnel_2

Interface : WAN2

Enable :

Local Group Setup

Local Security Group Type : Subnet

IP Address : 192.168.1.0

Subnet Mask : 255.255.255.0

Remote Client Setup

Remote Client : Microsoft XP/2000 VPN Client

Domain Name(FQDN)

Email Address(USER FQDN)

Microsoft XP/2000 VPN Client

IPSec Setup

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 1 - 768 bit

Stap 7. Klik op **Opslaan** om de instellingen op te slaan.

IPsec-installatie

Internet Protocol Security (IPSec) is een beveiligingsprotocol op de internetlaag dat end-to-end beveiliging biedt via verificatie en encryptie tijdens elke communicatiesessie.

Opmerking: twee uiteinden van de VPN moeten dezelfde methoden van encryptie, decryptie en verificatie hebben voor de IPSec om te werken. Ook de Perfect Forward Secrecy sleutel moet aan beide kanten van de tunnel hetzelfde zijn.

Stap 1. Kies de juiste modus voor sleutelbeheer om de beveiliging te garanderen uit de vervolgkeuzelijst *Sleutelmodus*. De standaardmodus is *IKE met een Preshared-toets*.

- Handmatig - Een aangepaste beveiligingsmodus om zelf een nieuwe beveiligingssleutel te genereren en geen onderhandeling met de sleutel. Het is het beste te gebruiken tijdens probleemoplossing en kleine statische omgeving. Als u Groep VPN kiest in Stap 1 in de sectie Een nieuwe tunnel toevoegen, wordt deze optie uitgeschakeld.
- IKE met Preshared key - Internet Key Exchange (IKE) protocol wordt gebruikt om automatisch een preshared key te genereren en te ruilen om communicatie voor de tunnel te verifiëren.

Subnet Mask : 255.255.255.0

Remote Client Setup

Remote Security Gateway Type : IP Only

IP Address : 192.168.1.2

IPSec Setup

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Manual

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 :

Advanced +

Configuratie handmatige toetsmodus

Stap 1. Voer de unieke hexadecimale waarde in voor inkomende Security Parameter Index (SPI) in het veld *Inkomende SPI*. SPI wordt meegeleverd in ESP-header (Encapsulating Security Payload Protocol) die samen de bescherming voor het inkomende pakket bepaalt. U kunt van 100 naar ffffffff gaan. De inkomende SPI van de lokale router moet overeenkomen met de uitgaande SPI van de externe router.

Stap 2. Voer in het veld *Uitgaande SPI* de unieke hexadecimale waarde in voor uitgaande Security

Parameter Index (SPI). SPI wordt meegeleverd in ESP-header (Encapsulating Security Payload Protocol) die samen de bescherming voor het uitgaande pakket bepaalt. U kunt van 100 naar ffffffff gaan. De uitgaande SPI van de externe router moet overeenkomen met de inkomende SPI van de lokale router.

Remote Client Setup

Remote Security Gateway Type : IP Only

IP Address : 192.168.1.2

IPSec Setup

Keying Mode : Manual

Incoming SPI : 100A

Outgoing SPI : 1BCD

Encryption : DES

Authentication : MD5

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 voor beide doeleinden dezelfde coderingsmethode gebruiken.

- DES - Data Encryption Standard (DES) gebruikt een 56-bits sleutelgrootte voor gegevenscodering. DES is verouderd en zou slechts moeten worden gebruikt als één eindpunt slechts DES steunt.
- 3DES - Triple Data Encryption Standard (3DES) is een 168-bits eenvoudige coderingsmethode. 3DES versleutelt de gegevens drie keer, wat meer beveiliging biedt dan DES.

IPSec Setup

Keying Mode : Manual

Incoming SPI : 100A

Outgoing SPI : 1BCD

Encryption :
 DES
 DES
 3DES

Authentication :

Encryption Key :

Authentication Key :

Stap 4. Kies de juiste verificatiemethode voor de gegevens in de vervolgkeuzelijst *Verificatie*. De aanbevolen verificatie is *SHA1* omdat deze veiliger is dan MD5. De VPN-tunnel moet voor beide doeleinden dezelfde verificatiemethode gebruiken.

- MD5 - Message Digest Algorithm-5 (MD5) vertegenwoordigt een hexadecimale hashfunctie met 32 cijfers die de gegevens tegen kwaadaardige aanvallen beschermt door middel van een checksum.

- SHA1 - Secure Hash Algorithm versie 1 (SHA1) is een 160-bits hashfunctie die veiliger is dan MD5, maar het kost meer tijd om te berekenen.

IPSec Setup

Keying Mode : Manual

Incoming SPI : 100A

Outgoing SPI : 1BCD

Encryption : DES

Authentication : MD5 (selected), MD5, SHA1

Encryption Key : [empty field]

Authentication Key : [empty field]

Stap 5. Voer de sleutel in om gegevens te versleutelen en te decrypteren in het veld *Encryption Key*. Als u in Stap 3 voor DES als coderingsmethode kiest, voert u een hexadecimale waarde van 16 cijfers in. Als u in Stap 3 3DES als coderingsmethode kiest, voert u een hexadecimale waarde van 40 cijfers in.

Stap 6. Voer een vooraf gedeelde sleutel in om het verkeer te verifiëren in het veld *Verificatiesleutel*. Als u in stap 4 MD5 als verificatiemethode kiest, voert u een hexadecimale waarde van 32 cijfers in. Als u SHA als verificatiemethode in stap 4 kiest, voert u een hexadecimale waarde van 40 cijfers in. De VPN-tunnel moet dezelfde vooraf gedeelde sleutel voor beide doeleinden gebruiken.

IPSec Setup

Keying Mode : Manual

Incoming SPI : 100A

Outgoing SPI : 1BCD

Encryption : DES

Authentication : MD5

Encryption Key : ABC12675BC0ACD

Authentication Key : AC67BCD00A12876CB

Stap 7. Klik op **Opslaan** om de instellingen op te slaan.

IKE met configuratie van voorgedeelde sleutelmodus

Stap 1. Kies de gewenste fase 1 DH-groep uit de vervolgkeuzelijst *fase 1 DH*-groep. Fase 1 wordt gebruikt om de simplex, logical security associatie (SA) tussen de twee uiteinden van de tunnel tot stand te brengen om veilige communicatie te ondersteunen. Diffie-Hellman (DH) is een cryptografisch sleuteluitwisselingsprotocol 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 sleutel en de meest onveilige authenticatie groep. Maar het kost

minder tijd om de IKE-sleutels te berekenen. Deze optie heeft de voorkeur als de netwerksnelheid laag is.

- Groep 2 - 1024 bit - De hogere sterktesleutel en veiligere verificatiegroep. Maar het heeft wat tijd nodig om de IKE-sleutels te berekenen.
- Groep 5 - 1536 bit - Vertegenwoordigt de hoogste sterktesleutel en de veiligste verificatiegroep. Het heeft meer tijd nodig om de IKE-sleutels te berekenen. De voorkeur gaat uit naar een netwerk met een hoge snelheid.

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 :

Minimum Preshared Key Complexity : Enable

Preshared Key Strength Meter :

Advanced +

Stap 2. Kies de juiste fase 1-encryptie om de sleutel uit de vervolgkeuzelijst *fase 1-encryptie* te versleutelen. 3DES wordt geadviseerd aangezien het de veiligste encryptiemethode is. De VPN-tunnel moet voor beide doeleinden dezelfde coderingsmethode gebruiken.

- DES - Data Encryption Standard (DES) gebruikt een 56-bits sleutelgrootte voor gegevenscodering. DES is verouderd en zou slechts moeten worden gebruikt als één eindpunt slechts DES steunt.
- 3DES - Triple Data Encryption Standard (3DES) is een 168-bits eenvoudige coderingsmethode. 3DES versleutelt de gegevens drie keer, wat meer beveiliging biedt dan DES.
- AES-128 - Advanced Encryption Standard (AES) is een 128-bits coderingsmethode die de onbewerkte tekst door 10 cycli en herhalingen omzet in coderingstekst.
- AES-192 - Advanced Encryption Standard (AES) is een 192-bits coderingsmethode die de onbewerkte tekst door 12 cycli en herhalingen omzet in coderingstekst. AES-192 is veiliger dan AES-128.
- AES-256 - Advanced Encryption Standard (AES) is een 256-bits coderingsmethode die de onbewerkte tekst met 14 cycli en herhalingen omzet in coderingstekst. AES-256 is de best beveiligde coderingsmethode.

IPSec Setup

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 1 - 768 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 :

Advanced +

Stap 3. Kies de juiste verificatiemethode van fase 1 uit de vervolgkeuzelijst *Fase 1-verificatie*. De VPN-tunnel moet voor beide doeleinden dezelfde verificatiemethode gebruiken.

- MD5 - Message Digest Algorithm-5 (MD5) vertegenwoordigt een hexadecimale hashfunctie met 32 cijfers die de gegevens tegen kwaadaardige aanvallen beschermt door middel van een checksum.
- SHA1 - Secure Hash Algorithm versie 1 (SHA1) is een 160-bits hashfunctie die veiliger is dan MD5, maar het kost meer tijd om te berekenen.

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 : 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 : 

Advanced +

Stap 4. Geef de hoeveelheid tijd in seconden op dat de sleutels van fase 1 geldig zijn en dat de VPN-tunnel actief blijft in het veld *Fase 1 SA-levensduur*.

Stap 5. Controleer het aanvinkvakje **Perfect Forward Secrecy** om de toetsen beter te beschermen. Deze optie staat de router toe om een nieuwe sleutel te produceren als om het even welke sleutel wordt gecompromitteerd. De versleutelde gegevens worden alleen gecompromitteerd via de gecompromitteerde sleutel. Zo verstrekt het veiligere en authenticiteit communicatie aangezien het andere sleutels hoewel een sleutel wordt gecompromitteerd beveiligd. Dit is een aanbevolen actie omdat deze meer beveiliging biedt.

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 6. Kies de juiste fase 2-DH-groep uit de vervolgkeuzelijst *fase 2-DH-groep*. Fase 2 maakt gebruik van security associatie en wordt gebruikt om de beveiliging van het gegevenspakket tijdens de gegevenspakketten die door de twee eindpunten worden doorgegeven te bepalen.

- Groep 1 - 768 bit - Vertegenwoordigt de laagste sterktesleutel en de meest onveilige verificatiegroep. Maar het heeft minder tijd nodig om de IKE-sleutels te berekenen. De voorkeur gaat uit naar een netwerk met een lage snelheid.
- Groep 2 - 1024 bit - Vertegenwoordigt een hogere sterktesleutel en een veiligere verificatiegroep. Maar het heeft wat tijd nodig om de IKE-sleutels te berekenen.
- Groep 5 - 1536 bit - Vertegenwoordigt de hoogste sterktesleutel en de veiligste verificatiegroep. Het heeft meer tijd nodig om de IKE-sleutels te berekenen. De voorkeur gaat uit naar een netwerk met een hoge snelheid.

IPSec Setup

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 2 - 1024 bit

Phase 1 Encryption : DES

Phase 1 Authentication : SHA1

Phase 1 SA Life Time : 27600 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 1 - 768 bit

Phase 2 Encryption : MD5

Phase 2 Authentication : MD5

Phase 2 SA Life Time : 3600 seconds

Preshared Key :

Minimum Preshared Key Complexity : Enable

Preshared Key Strength Meter :

Advanced +

Stap 7. Kies de juiste fase 2-encryptie om de sleutel uit de vervolgkeuzelijst *fase 2-encryptie* te versleutelen. AES-256 wordt aanbevolen omdat dit de best beveiligde coderingsmethode is. De VPN-tunnel moet voor beide doeleinden dezelfde coderingsmethode gebruiken.

- DES - Data Encryption Standard (DES) gebruikt een 56-bits sleutelgrootte voor gegevenscodering. DES is verouderd en zou slechts moeten worden gebruikt als één eindpunt slechts DES steunt.
- 3DES - Triple Data Encryption Standard (3DES) is een 168-bits eenvoudige coderingsmethode. 3DES versleutelt de gegevens drie keer, wat meer beveiliging biedt dan DES.
- AES-128 - Advanced Encryption Standard (AES) is een 128-bits coderingsmethode die de onbewerkte tekst door 10 cycli en herhalingen omzet in coderingstekst.
- AES-192 - Advanced Encryption Standard (AES) is een 192-bits coderingsmethode die de onbewerkte tekst door 12 cycli en herhalingen omzet in coderingstekst. AES-192 is veiliger dan AES-128.
- AES-256 - Advanced Encryption Standard (AES) is een 256-bits coderingsmethode die de onbewerkte tekst met 14 cycli en herhalingen omzet in coderingstekst. 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 : DES

Phase 1 Authentication : SHA1

Phase 1 SA Life Time : 27600 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 1 - 768 bit


Phase 2 Encryption : **DES**

Phase 2 Authentication : **DES**

Phase 2 SA Life Time :

Preshared Key :

Minimum Preshared Key Complexity : Enable

Preshared Key Strength Meter : 

Advanced +

Stap 8. Kies de juiste verificatiemethode uit de vervolgkeuzelijst *Fase 2-verificatie*. De VPN-tunnel moet voor beide doeleinden dezelfde verificatiemethode gebruiken.

- MD5 - Message Digest Algorithm-5 (MD5) vertegenwoordigt een hexadecimale hashfunctie met 32 cijfers die de gegevens tegen kwaadaardige aanvallen beschermt door middel van een checksum.
- SHA1 - Secure Hash Algorithm versie 1 (SHA1) is een 160-bits hashfunctie die veiliger is dan MD5, maar het kost meer tijd om te berekenen.
- Ongeldig - er wordt geen verificatiemethode gebruikt.

IPSec Setup

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 2 - 1024 bit

Phase 1 Encryption : DES

Phase 1 Authentication : SHA1

Phase 1 SA Life Time : 27600 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 :

Preshared Key :

Minimum Preshared Key Complexity : Enable

Preshared Key Strength Meter :

Advanced +

Stap 9. Geef de hoeveelheid tijd in seconden op dat de Fase 2-toetsen geldig zijn en dat de VPN-tunnel actief blijft in het veld *Fase 2 SA-levensduur*.

Stap 10. Voer een sleutel in die eerder wordt gedeeld tussen de IKE-peers om de peers in het veld *Preshared Key* te verifiëren. Tot 30 hexadecimale tekens en tekens kunnen worden gebruikt als de vooraf gedeelde sleutel. De VPN-tunnel moet dezelfde vooraf gedeelde sleutel voor beide doeleinden gebruiken.

Opmerking: het is sterk aanbevolen om de vooraf gedeelde sleutel tussen de IKE-peers vaak te wijzigen, zodat de VPN beveiligd blijft.

Stap 11. Schakel het aanvinkvakje **Minimale Preshared Key Complexity in** als u krachtmeter wilt inschakelen voor de preshared sleutel. Het wordt gebruikt om de sterkte van de vooraf gedeelde sleutel door kleurenbars te bepalen

Opmerking: *Preshared Key Strength Meter* toont de sterkte van de preshared sleutel door gekleurde balken. Rood geeft zwakke sterkte aan, geel geeft aanvaardbare sterkte aan en groen geeft sterke sterkte aan.

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

Geavanceerde IKE met configuratie van voorgedeelde sleutelmodus

Stap 1. Klik op **Advanced** om de geavanceerde instellingen voor IKE met Preshared-toets weer te geven.

Advanced

Aggressive Mode

Compress (Support IP Payload Compression Protocol(IPComp))

Keep-Alive

AH Hash Algorithm

NetBIOS Broadcast

NAT Traversal

Dead Peer Detection Interval seconds

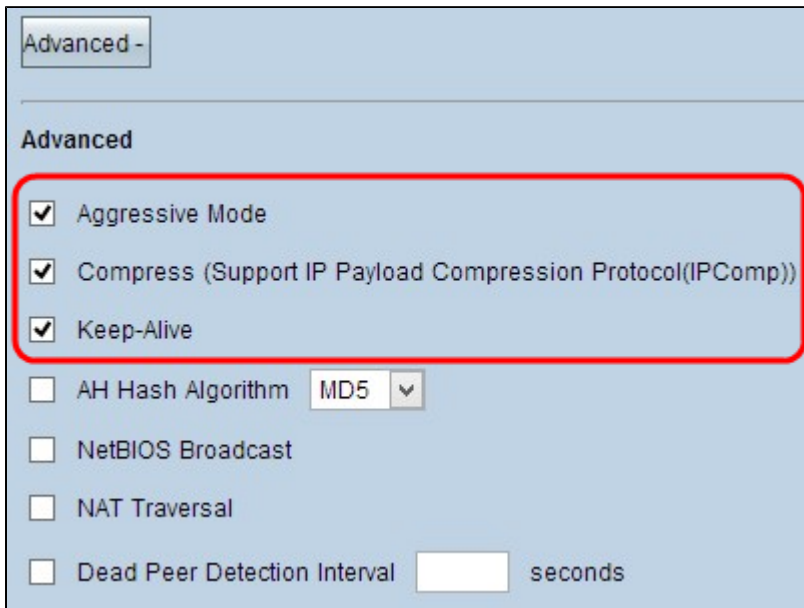
Stap 2. Schakel het selectievakje **Aggressive Mode in** als uw netwerksnelheid laag is. Dit ruilt de ID's van

de eindpunten van de tunnel in duidelijke tekst tijdens SA-verbinding (fase 1), die minder tijd vergt om te ruilen maar minder veilig is.

Opmerking: Aggressive Mode is niet beschikbaar voor groepsclient naar gateway VPN verbinding.

Stap 3. Schakel het aanvinkvakje **Compress (Support IP payload Compression Protocol (IPComp))** in als u de grootte van de IP-datagrammen wilt comprimeren. IPComp is een IP compressieprotocol dat wordt gebruikt om de grootte van IP datagram te comprimeren. IP-compressie is nuttig als de netwerksnelheid laag is en de gebruiker de gegevens snel wil verzenden zonder verlies via het langzame netwerk, maar biedt geen beveiliging.

Stap 4. Schakel het aankruisvakje **Keep-Alive in** als u altijd wilt dat de verbinding met de VPN-tunnel actief blijft. Keep Alive helpt de verbindingen onmiddellijk te herstellen als een verbinding inactief wordt.



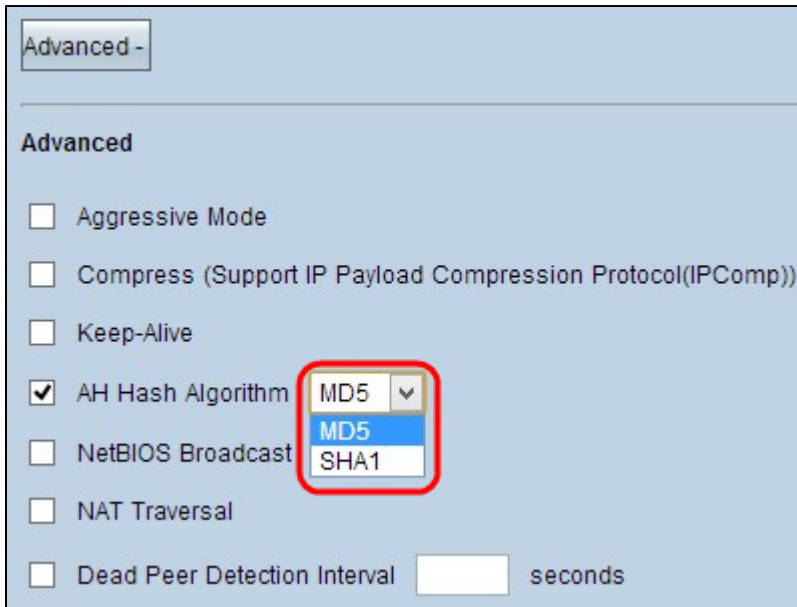
Advanced -

Advanced

- Aggressive Mode
- Compress (Support IP Payload Compression Protocol(IPComp))
- Keep-Alive
- AH Hash Algorithm MD5
- NetBIOS Broadcast
- NAT Traversal
- Dead Peer Detection Interval seconds

Stap 5. Schakel het aanvinkvakje **AH Hash Algorithm in** als u Authenticate Header (AH) wilt inschakelen. AH biedt authenticatie aan de oorspronkelijke gegevens, gegevensintegriteit door middel van checksum en bescherming in de IP-header. De tunnel zou hetzelfde algoritme moeten hebben voor beide kanten.

- MD5 - Message Digest Algorithm-5 (MD5) vertegenwoordigt een hexadecimale hashfunctie met 128 cijfers die de gegevens tegen kwaadaardige aanvallen beschermt door middel van een checksum.
- SHA1 - Secure Hash Algorithm versie 1 (SHA1) is een 160-bits hashfunctie die veiliger is dan MD5, maar het kost meer tijd om te berekenen.

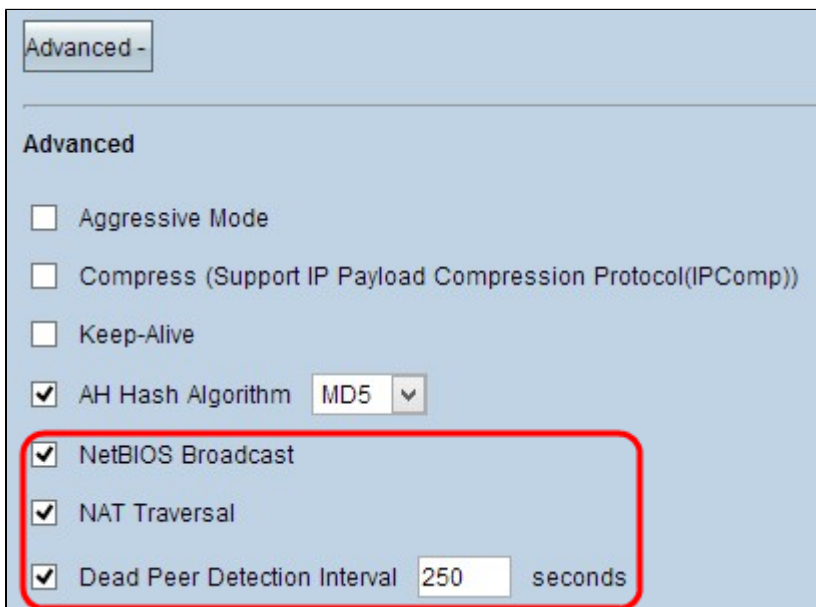


Stap 6. Controleer **NetBIOS Broadcast** als u niet-routeerbaar verkeer via de VPN-tunnel wilt toestaan. De standaardinstelling is niet ingeschakeld. NetBIOS wordt gebruikt om netwerkbronnen zoals printers, computers etc. in het netwerk te detecteren via sommige softwaretoepassingen en Windows-functies zoals Network Neighbourhood.

Stap 7. Schakel het aanvinkvakje **NAT Tradition in** als u via een openbaar IP-adres toegang tot het internet wilt hebben via uw privé LAN. Als uw VPN-router zich achter een NAT-gateway bevindt, schakelt u deze optie in om NAT-traversatie in te schakelen. Beide uiteinden van de tunnel moeten de zelfde instellingen hebben.

Stap 8. Controleer het **Dead Peer Detection Interval** om de levendigheid van de VPN-tunnel op een periodieke manier door hello of ACK te controleren. Als u dit aanvinkvakje aankruist, voert u de gewenste duur of het interval van de hello-berichten in.

Opmerking: u kunt dode peer-detectie-interval alleen configureren voor één client naar gateway-VPN-verbinding, niet voor groepsclient naar gateway-VPN-verbinding.



Stap 9. Klik op **Opslaan** om de instellingen op te slaan.

U hebt nu geleerd hoe u externe VPN-tunnels voor toegang kunt configureren van client naar gateway 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.