

Configuratie van één client voor Gateway Virtual Private Network (VPN) op RV320 en RV325 VPN-routerSeries

Doel

Het doel van dit document is om u te tonen hoe u één client aan gateway Virtual Private Network (VPN) op RV32x Series VPN-routers kunt configureren.

Inleiding

Een VPN is een privaat netwerk dat wordt gebruikt om virtueel een externe gebruiker via een openbaar netwerk aan te sluiten. Eén type VPN is een client-naar-gateway VPN. Een client-naar-gateway VPN is een verbinding tussen een externe gebruiker en het netwerk. De client is ingesteld in het gebruikersapparaat met VPN-clientsoftware. Hiermee kunnen gebruikers zich veilig op een netwerk aansluiten.

Toepasselijke apparaten

- RV320 VPN-router met dubbel WAN
- RV325 Gigabit VPN-router met dubbel WAN

Softwareversie

- v1.1.0.09

Eén client voor gateway VPN configureren

Stap 1. Meld u aan bij het web configuratieprogramma en kies **VPN > Client naar Gateway**. De pagina *Client to Gateway* wordt geopend:

Client to Gateway

Add a New Tunnel

Tunnel Group VPN Easy VPN

Tunnel No.

1

Tunnel Name:

Interface:

WAN1

Keying Mode:

IKE with Preshared key

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

:

Stap 2. Klik op de radioknop **van de Tunnel** om één tunnel voor client aan gateway VPN toe te voegen.

Client to Gateway

Add a New Tunnel

Tunnel

Group VPN

Easy VPN

Tunnel No. 1

Tunnel Name:

Interface: WAN1

Keying Mode: IKE with Preshared key

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 :

Voeg een nieuwe Tunnel toe

Client to Gateway

Add a New Tunnel

Tunnel Group VPN Easy VPN

Tunnel No. 1

Tunnel Name:

Interface: ▼

Keying Mode: ▼

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: ▼

▼ :

Opmerking: Tunnel nr. - vertegenwoordigt het aantal tunnels. Dit nummer wordt automatisch gegenereerd.

Stap 1. Voer de naam van de tunnel in in het veld *Tunnelnaam*.

Stap 2. Kies de interface waarmee de externe client naar VPN toegang heeft van de vervolgkeuzelijst *Interface*.

Client to Gateway

Add a New Tunnel

Tunnel
 Group VPN
 Easy VPN

Tunnel No. 1

Tunnel Name: tunnel_1

Interface: WAN1
WAN1
WAN2
USB1
USB2

Keying Mode:

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

Stap 3. Kies de juiste modus van het sleutelbeheer om beveiliging te garanderen in de vervolgkeuzelijst Keying Mode De standaardmodus is IKE met de PreShared key.

Client to Gateway

Add a New Tunnel

Tunnel
 Group VPN
 Easy VPN

Tunnel No. 1

Tunnel Name: tunnel_1

Interface: WAN1

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

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

De opties zijn als volgt gedefinieerd:

- Handmatig - Aangepaste beveiligingsmodus om zelf een nieuwe beveiligingssleutel te

genereren en geen onderhandeling met de toets. Het is het beste voor gebruik tijdens het oplossen van problemen of in een klein statisch milieu.

- IKE met PreShared Key - Internet Key Exchange (IKE)-protocol wordt gebruikt om automatisch een vooraf gedeelde sleutel te genereren en uit te wisselen om voor de tunnel gewaarmerkte communicatie op te zetten.
- IKE met certificaatprotocol - Internet Key Exchange (IKE)-protocol met certificaat is een veiliger methode om automatisch gedeelde sleutels te genereren en uit te wisselen om een veiliger communicatie voor de tunnel tot stand te brengen.

Stap 4. Controleer het aanvinkvakje **Enable** om client in te schakelen om VPN-poort te openen. Deze functie is standaard ingeschakeld.

Client to Gateway

Add a New Tunnel

Tunnel Group VPN Easy VPN

Tunnel No. 1

Tunnel Name: tunnel_1

Interface: WAN1

Keying Mode: IKE with Preshared key

Enable:

Local Group Setup

Local Security Gateway Type: Dynamic IP + Domain Name(FQDN) Authentication

Domain Name: domain_1

Local Security Group Type: IP

IP Address: 192.168.2.1

Stap 5. Als u de instellingen wilt opslaan die u tot nu toe hebt, klikt u op **Opslaan** om de instellingen op te slaan.

Local Group Setup

Local Group Setup met handleiding of IKE met vooraf gedeelde sleutel

Opmerking: Volg de onderstaande stappen als u Handmatig of IKE met de Gepubliceerde sleutel uit de vervolgkeuzelijst Toetsenmodus in Stap 3 van het gedeelte *Nieuwe Tunnel toevoegen*.

Stap 1. Kies de juiste router-identificatiemethode uit de vervolgkeuzelijst *Local Security Gateway* om een VPN-tunnel op te zetten.

Client to Gateway

Add a New Tunnel

Tunnel
 Group VPN
 Easy VPN

Tunnel No.

Tunnel Name:

Interface:

Keying Mode:

Enable:

Local Group Setup

Local Security Gateway Type:

IP Address:

Local Security Group Type:

IP Address:

Subnet Mask:

De opties zijn als volgt gedefinieerd:

- IP only - toegang tot de tunnel is mogelijk door een enkel statisch WAN IP. U kunt deze optie kiezen als alleen de router een statische WAN IP heeft. Het statische WAN IP-adres wordt automatisch gegenereerd.
- 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 domein in*. Het statische WAN IP-adres wordt automatisch gegenereerd.
- 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 gegenereerd.
- 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 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*.
- IP-adres - dit is het IP-adres van de WAN-interface. Het is een alleen-lezen veld.

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

Client to Gateway

Add a New Tunnel

Tunnel
 Group VPN
 Easy VPN

Tunnel No. 1

Tunnel Name: tunnel_1

Interface: WAN1

Keying Mode: IKE with Preshared key

Enable:

Local Group Setup

Local Security Gateway Type: Dynamic IP + Domain Name(FQDN) Authentication

Domain Name: domain_1

Local Security Group Type: Subnet

IP Address:

Subnet Mask: 255.255.255.0

- IP - Er is slechts één specifiek LAN-apparaat dat toegang heeft tot de tunnel. Als u deze optie kiest, specificeert u het IP-adres van het LAN-apparaat in het veld *IP-adres*. De standaard IP is 192.168.1.0.
- Subnet - Alle LAN apparaten op specifiek netwerk kunnen tot de tunnel toegang hebben. Als u deze optie kiest, voert u het IP-adres en het subnetmasker 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 tot de tunnel te krijgen. Als u deze optie kiest, specificeert u het begin- en eindadres in de velden *Start IP* en *End IP*. Het standaardbereik loopt van 192.168.1.0 tot 192.168.1.254.

Stap 3. Als u de instellingen wilt opslaan die u tot nu toe hebt, klikt u op **Omlaag** en vervolgens klikt u op **Opslaan** om de instellingen op te slaan.

Local Group Setup met IKE met certificaatnummer voor Tunnel VPN

Opmerking: Volg de onderstaande stappen als u voor IKE met certificaatnummer kiest in de vervolgkeuzelijst *Keying Mode* in Stap 3 van het gedeelte *Add a New Tunnel*.

Client to Gateway

Add a New Tunnel

Tunnel
 Group VPN
 Easy VPN

Tunnel No. 1

Tunnel Name:

Interface: ▼

Keying Mode: ▼

Enable:

Local Group Setup

Local Security Gateway Type: ▼

IP Address: 0.0.0.0

Local Certificate: ▼

Local Security Group Type: ▼

IP Address:

- Type lokale beveiligingsgateway - toegang tot de tunnel is mogelijk via IP met een certificaat.
- IP-adres - dit is het IP-adres van de WAN-interface. Het is een alleen-lezen veld.

Stap 1. Kies het juiste lokale certificaat om de router te identificeren uit de vervolgkeuzelijst *Lokaal certificaat*. Klik op **Zelfgenerator** om het certificaat automatisch te genereren of klik op **Importeren** om een nieuw certificaat te importeren.

Opmerking: om meer te weten te komen over de manier waarop automatisch certificaten kunnen worden gegenereerd, raadpleeg *Generate Certificaten op RV320 Routers*, en om te weten hoe u certificaten kunt importeren om *Mijn certificaat op RV320 Routers te configureren*.

Client to Gateway

Add a New Tunnel

Tunnel
 Group VPN
 Easy VPN

Tunnel No. 1

Tunnel Name: tunnel_1

Interface: WAN1

Keying Mode: IKE with Certificate

Enable:

Local Group Setup

Local Security Gateway Type: IP + Certificate

IP Address: 0.0.0.0

Local Certificate: 01. Issuer: 6c:20:56:c6:16:52 - Subject: 6c:20:56:c6:16:52

Local Security Group Type: IP

IP Address:

- IP
- IP
- Subnet
- IP Range

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

- IP - Er is slechts één specifiek LAN-apparaat dat toegang heeft tot de tunnel. Als u deze optie kiest, voert u het IP-adres van het LAN-apparaat in het veld IP-adres in. De standaard IP is 192.168.1.0.
- Subnet - Alle LAN apparaten op specifiek netwerk kunnen tot de tunnel toegang hebben. Als u deze optie kiest, voert u het IP-adres en het subnetmasker 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 tot de tunnel te krijgen. Als u deze optie kiest, voert u het begin- en eindadres in in de IP-beginvelden en de IP-eindvelden. Het standaardbereik loopt van 192.168.1.0 tot 192.168.1.254.

Stap 3. Als u de instellingen wilt opslaan die u tot nu toe hebt, klikt u op Omlaag en vervolgens klikt u op **Opslaan** om de instellingen op te slaan.

Instellen externe client

Remote-clientinstelling met handleiding of IKE met vooraf gedeelde toets

Opmerking: Volg de onderstaande stappen als u Handmatig of IKE met Voorgedeelde sleutel uit de vervolgkeuzelijst Keying Mode in Stap 3 van het gedeelte *Add a New Tunnel* hebt geselecteerd.

Client to Gateway

Add a New Tunnel

Tunnel
 Group VPN
 Easy VPN

Tunnel No. 1

Tunnel Name: tunnel_1

Interface: WAN1

Keying Mode: IKE with Preshared key

Enable:

Local Group Setup

Local Security Gateway Type: IP Only

IP Address: 0.0.0.0

Local Security Group Type: IP

IP Address: 192.168.2.1

Remote Client Setup

Remote Security Gateway Type: IP Only

IP Address :

IPSec Setup

Phase 1 DH Group: Group 1 - 768 bit

Stap 1. Kies de juiste client-identificatiemethode om een VPN-tunnel te maken uit de vervolgkeuzelijst *Remote Security Gateway*. De standaard is alleen IP.

- IP only - de toegang tot de tunnel is mogelijk door het statische WAN IP van de cliënt slechts. U kunt deze optie alleen kiezen als u de statische WAN IP- of domeinnaam van de client kent. Kies IP-adres in de vervolgkeuzelijst en voer het statische IP van de client in het aangrenzende veld in, of kies IP door DNS Resolved uit de vervolgkeuzelijst en voer de domeinnaam van het IP-adres in het aangrenzende veld in. Via de lokale DNS-server van het IP-adres kan de router het IP-adres automatisch ophalen.

Opmerking: Als u Handmatig kiest uit de vervolgkeuzelijst Toetsenmodus in Stap 3 in het vak Toevoegen van een nieuwe tunnelleiding door Tunnel of groep VPN, is dit de enige beschikbare optie.

- IP + Domain Name (FQDN)-verificatie - toegang tot de tunnel is mogelijk door een statisch IP-adres van de client 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. Kies IP-adres in de vervolgkeuzelijst en voer het statische IP van de client in het aangrenzende veld in, of kies IP door DNS Resolved uit de vervolgkeuzelijst en voer de domeinnaam van het IP-adres in het aangrenzende veld in. Via de lokale DNS-server van het IP-adres kan de router het IP-adres

automatisch ophalen.

- IP + E-mailadres. (USER FQDN)-verificatie - toegang tot de tunnel is mogelijk door een statisch IP-adres van de client en een e-mailadres. Als u deze optie kiest, voert u het e-mailadres in het veld E-mailadres in. Kies IP-adres in de vervolgkeuzelijst en voer het statische IP van de client in het aangrenzende veld in of kies IP met DNS opgelost in de vervolgkeuzelijst en voer de domeinnaam van het IP-adres in het aangrenzende veld in. Via de lokale DNS-server van het IP-adres kan de router het IP-adres automatisch ophalen.
- Dynamic IP + Domain Name (FQDN)-verificatie - Toegang tot de tunnel is mogelijk via een dynamisch IP-adres van de client 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 van de client en een e-mailadres. Als u deze optie kiest, voert u het e-mailadres in het veld E-mailadres in.

Stap 2. Als u de instellingen wilt opslaan die u tot nu toe hebt, klikt u op Omlaag en vervolgens klikt u op **Opslaan** om de instellingen op te slaan.

Remote Group Setup met IKE met certificaat

Opmerking: Volg de onderstaande stappen als u voor IKE met Certificaat hebt gekozen uit de vervolgkeuzelijst Keying Mode in Stap 3 van het gedeelte *Add a New Tunnel*.

Local Group Setup

Local Security Gateway Type: IP + Certificate

IP Address: 0.0.0.0

Local Certificate: 01. Issuer : 6c:20:56:c6:16:52 - Subject: 6c:20:56:c6:16:52

Self-Generator Import Certificate

Local Security Group Type: Subnet

IP Address: 192.168.3.1

Subnet Mask: 255.255.255.0

Remote Client Setup

Remote Security Gateway Type: IP + Certificate

IP Address : 192.168.3.2

Remote Certificate: 01. Issuer : 6c:20:56:c6:16:52 - Subject: 6c:20:56:c6:16:52

Import Remote Certificate Authorize CSR

- Type externe security gateway - clientidentificatie is mogelijk via IP met een certificaat om een VPN-verbinding op te zetten.

Stap 1. Kies **IP-adres** of **IP met DNS-oplossing** in de vervolgkeuzelijst.

- IP-adres - toegang tot de tunnel is alleen mogelijk via het statische WAN IP van de client. U

kunt deze optie alleen kiezen als u de statische WAN IP van de client kent. Voer het statische IP van de client in het veld *IP-adres* in.

- IP door DNS opgelost - handig als u het IP-adres van de client niet kent maar u het domein van dat IP-adres weet. Voer de domeinnaam van het IP-adres in. Via de lokale DNS-server van het IP-adres kan de router het IP-adres automatisch ophalen.

Stap 2. Kies het juiste externe certificaat in de vervolgkeuzelijst *Remote* certificaataanvraag. Klik op **Afstandscertificaat importeren** om een nieuw certificaat te importeren of klik op **CSR autoriseren** om certificaat te identificeren met een digitale tekenaanvraag.

Opmerking: Als u meer wilt weten over het importeren van een nieuw certificaat, raadpleeg *Beeld/Toevoegen Trusted SSL-certificaat op RV320-routers* en om meer te weten te komen over geautoriseerd CSR raadpleeg *CSR-certificaataanvraag (CSR) op RV320-routers*.

Stap 3. Als u de instellingen wilt opslaan die u tot nu toe hebt, klikt u op **Omlaag** en vervolgens klikt u op **Opslaan** om de instellingen op te slaan.

IPsec-instelling

IPsec-instelling met handmatige sleutel

Opmerking: Volg de onderstaande stappen als u Handmatig kiest uit de vervolgkeuzelijst *Keying Mode* in Stap 3 van het gedeelte *Add a New Tunnel*.

The screenshot shows a configuration interface for a remote client. It is divided into two main sections: "Remote Client Setup" and "IPSec Setup".

Remote Client Setup:

- Remote Security Gateway Type: IP Only (dropdown)
- IP Address: 192.168.3.2 (text input)

IPSec Setup:

- Incoming SPI: 1023ac (text input, highlighted with a red box) (Range: 100-FFFFFFFF, Default: 100)
- Outgoing SPI: 1023cb (text input, highlighted with a red box) (Range: 100-FFFFFFFF, Default: 100)
- Encryption: DES (dropdown)
- Authentication: MD5 (dropdown)
- Encryption Key: (text input) (HEX Number, DES: 16bits, 3DES: 48bits)
- Authentication Key: (text input) (HEX Number, MD5: 32bits, SHA1: 40bits)

Stap 1. Voer de unieke hexadecimale waarde in voor de inkomende Security Parameter Index (SPI) in het veld *Inkomende SPI*. De SPI wordt in de Encapsulating Security Payload Protocol (ESP)-header gedragen, die samen de security associatie (SA) voor het inkomende pakket bepaalt. Het bereik is 100 in het veld, standaard 100.

Stap 2. Voer de unieke hexadecimale waarde in voor de uitgaande Security Parameter Index (SPI) in het *uitgaande SPI*-veld. De SPI wordt opgeslagen in Encapsulation Security Payload Protocol (ESP)-header, die samen de Security Association (SA) bepaalt voor het uitgaande pakket. Het bereik is 100 in het veld, standaard 100.

Opmerking: De inkomende SPI van het aangesloten apparaat en de uitgaande SPI van het

andere uiteinde van de tunnel moeten elkaar koppelen om een tunnel tot stand te brengen.

The screenshot shows a 'Remote Client Setup' dialog box. Under the 'IPSec Setup' section, the 'Encryption' dropdown menu is open, showing 'DES' selected and '3DES' as an option. The 'Authentication' dropdown menu is also open, showing 'MD5' and 'SHA1' as options. The 'Encryption Key' and 'Authentication Key' fields are empty. The 'Remote Security Gateway Type' is set to 'IP Only' and the 'IP Address' is '192.168.3.2'. The 'Incoming SPI' is '1023ac' and the 'Outgoing SPI' is '1023cb'. The 'Save' and 'Cancel' buttons are at the bottom.

Stap 3. Kies de juiste encryptie-methode in de vervolgkeuzelijst *Encryption*. De aanbevolen codering is 3DES. De VPN-tunnel moet dezelfde coderingsmethode gebruiken voor beide eindpunten.

- DES - Data Encryption Standard (DES) is een 56-bits, oude, meer achterwaartse compatibele encryptie-methode die niet zo veilig is.
- 3DES - Triple Data Encryption Standard (3DES) is een 168 bit, eenvoudige coderingsmethode om de grootte van de sleutel te verhogen door de gegevens drie keer te versleutelen, wat meer beveiliging dan DES biedt.

The screenshot shows the same 'Remote Client Setup' dialog box. In this view, the 'Authentication' dropdown menu is open, showing 'MD5' selected and 'SHA1' as an option. The 'Encryption' dropdown menu is now closed and set to 'DES'. The 'Encryption Key' and 'Authentication Key' fields are empty. The 'Remote Security Gateway Type' is 'IP Only' and the 'IP Address' is '192.168.3.2'. The 'Incoming SPI' is '1023ac' and the 'Outgoing SPI' is '1023cb'. The 'Save' and 'Cancel' buttons are at the bottom.

Stap 4. Kies de juiste authenticatiemethode in de vervolgkeuzelijst *Verificatie*. De aanbevolen authenticatie is SHA1. De VPN-tunnel moet dezelfde authenticatiemethode gebruiken voor beide uiteinden.

- MD5 - Message Digest Algorithm-5 (MD5) staat voor de functie met 32 cijfers die een hexadecimale hashfunctie heeft, die bescherming biedt aan de gegevens tegen 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.

The screenshot shows a 'Remote Client Setup' dialog box. Under the 'IPSec Setup' section, the following fields are visible:

- Incoming SPI: 1023ac (Range: 100-FFFFFFFF, Default: 100)
- Outgoing SPI: 1023cb (Range: 100-FFFFFFFF, Default: 100)
- Encryption: DES
- Authentication: SHA1
- Encryption Key: adbc234987bc (HEX Number, DES: 16bits, 3DES: 48bits)
- Authentication Key: 233445bcfacffb (HEX Number, MD5: 32bits, SHA1: 40bits)

Buttons for 'Save' and 'Cancel' are located at the bottom of the dialog.

Stap 5. Voer de sleutel in om gegevens te versleutelen en te decrypteren in het veld *Encryption Key*. Als u DES als encryptiemethode in stap 3 hebt gekozen, moet u een 16-cijferige hexadecimale waarde invoeren. Als u 3DES als encryptiemethode in Stap 3 hebt gekozen, moet u een 40-cijferige hexadecimale waarde invoeren.

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

Stap 7. Als u de instellingen wilt opslaan die u tot nu toe hebt, klikt u op **Opslaan** om de instellingen op te slaan.

IPsec-instelling met IKE met gedeelde sleutel of IKE met certificaat

Opmerking: Volg de onderstaande stappen als u voor IKE hebt gekozen met Voorgedeelde sleutel of IKE met Certificaat van de vervolgkeuzelijst *Keying Mode* in Stap 3 van het gedeelte *Add a New Tunnel*.

Remote Client Setup

Remote Security Gateway Type: IP Only

IP Address: 192.168.3.2

IPSec Setup

Phase 1 DH Group: Group 1 - 768 bit

Phase 1 Encryption: Group 1 - 768 bit

Phase 1 Authentication: MD5

Phase 1 SA Lifetime: 28800 sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group: Group 1 - 768 bit

Phase 2 Encryption: DES

Phase 2 Authentication: MD5

Phase 2 SA Lifetime: 3600 sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key:

Preshared Key Strength Meter:

Advanced +

Stap 1. Kies de juiste Fase 1 DH-groep uit de vervolgkeuzelijst *Fase 1 DH Group*. Fase 1 wordt gebruikt om de simplex, logical security association (SA) tussen de twee uiteinden van de tunnel op te richten ter ondersteuning van veilige authentieke communicatie. Diffie-Hellman (DH) is een cryptografisch zeer belangrijk uitwisselingsprotocol dat tijdens Fase 1 verbinding wordt gebruikt om geheime sleutel te delen om communicatie te authenticeren.

- Groep 1 - 768 bit - vertegenwoordigt de laagste sterkte en de meest onveilige echtheidsgroep. Maar het heeft minder tijd nodig om de IKE-toetsen te berekenen. Het is de voorkeur dat de snelheid van het netwerk laag is.
- Groep 2 - 1024 bit - vertegenwoordigt een hogere sterkte en een veiliger authenticatiegroep. Maar het heeft wat tijd nodig om de IKE-toetsen te berekenen.
- Groep 5 - 1536 bit - vertegenwoordigt 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

Phase 1 DH Group:

Phase 1 Encryption:

- DES
- DES
- 3DES
- AES-128
- AES-192
- AES-256

Phase 1 Authentication:

Phase 1 SA Lifetime: sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group:

Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime: sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key:

Preshared Key Strength Meter:

Stap 2. Kies de juiste fase 1-encryptie om de sleutel te versleutelen uit de vervolgkeuzelijst *Fase 1 Encryption*. AES-256 wordt aanbevolen, omdat dit de best beveiligde coderingsmethode is. De VPN-tunnel moet dezelfde coderingsmethode gebruiken voor beide eindpunten.

- DES - Data Encryption Standard (DES) is 56 bit, oude encryptiemethode die niet erg veilig is.
- 3DES - Triple Data Encryption Standard (3DES) is een 168 bit, eenvoudige coderingsmethode om de grootte van de sleutel te verhogen door de gegevens drie keer te versleutelen, wat meer beveiliging dan DES biedt.
- AES-128 - Advanced Encryption Standard (AES) is 128-bits coderingsmethode waarmee de onbewerkte tekst door 10 herhalingscycli wordt getransformeerd.
- AES-192 - Advanced Encryption Standard (AES) is een 192-bits coderingsmethode waarmee de gewone tekst door 12 herhalingscycli in een algoritme wordt omgezet.
- AES-256 - Advanced Encryption Standard (AES) is 256-bits coderingsmethode waarmee de onbewerkte tekst door 14 herhalingscycli wordt getransformeerd.

IPSec Setup

Phase 1 DH Group:

Phase 1 Encryption :

Phase 1 Authentication: (highlighted with a red box)

Phase 1 SA Lifetime: sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group:

Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime: sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key:

Preshared Key Strength Meter:

Stap 3. Kies de juiste authenticatiemethode in de vervolgkeuzelijst *Fase 1-verificatie*. De VPN-tunnel moet dezelfde verificatiemethode toepassen voor beide uiteinden.

- MD5 - Message Digest Algorithm-5 (MD5) staat voor de functie met 32 cijfers die een hexadecimale hashfunctie hebben, 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.

IPSec Setup

Phase 1 DH Group:

Phase 1 Encryption:

Phase 1 Authentication:

Phase 1 SA Lifetime: sec (Range: 120-86400, Default: 28800)

Perfect Forward Security:

Phase 2 DH Group:


Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime: sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key:

Preshared Key Strength Meter: 

Stap 4. Voer de hoeveelheid tijd in in seconden, in fase 1, blijft de VPN-tunnel actief in het veld *Phase 1 SA Live*. De standaardtijd is 2800 seconden.

Stap 5. Controleer **het** vakje **Perfect Forward Security** om meer bescherming aan de toetsen te bieden. Met deze optie kunt u een nieuwe toets genereren indien er een toets wordt gecompromitteerd. De versleutelde gegevens worden alleen via de gecompromitteerde toets gecompromitteerd. Het zorgt voor meer veiligheid en authenticiteit van communicatie, omdat het andere sleutels veilig stelt, door een sleutel in gevaar te brengen. Dit is een aanbevolen actie omdat deze meer beveiliging biedt.

IPSec Setup

Phase 1 DH Group:

Phase 1 Encryption:

Phase 1 Authentication:

Phase 1 SA Lifetime: sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group:

Phase 2 Encryption:

Phase 2 SA Lifetime: sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key:

Preshared Key Strength Meter:

Stap 6. Kies de juiste fase 2 DH-groep uit de vervolgkeuzelijst *Fase 2 DH Group*. 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 tijdens Fase 1 verbinding wordt gebruikt om geheime sleutel te delen om communicatie te authentifieren.

- Groep 1 - 768 bit - vertegenwoordigt de laagste sterkte en de meest onveilige echtheidsgroep. Maar het heeft minder tijd nodig om de IKE-toetsen te berekenen. Het is de voorkeur dat de snelheid van het netwerk laag is.
- Groep 2 - 1024 bit - vertegenwoordigt een hogere sterkte en een veiliger authenticatiegroep. Maar het heeft wat tijd nodig om de IKE-toetsen te berekenen.
- Groep 5 - 1536 bit - vertegenwoordigt 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

Phase 1 DH Group:

Phase 1 Encryption:

Phase 1 Authentication:

Phase 1 SA Lifetime: sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group:

Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime: sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity:

Preshared Key:

Preshared Key Strength Meter: ■ ■ ■ ■

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

- DES - Data Encryption Standard (DES) is 56 bit, oude encryptiemethode die niet erg veilig is.
- 3DES - Triple Data Encryption Standard (3DES) is een 168 bit, eenvoudige coderingsmethode om de grootte van de sleutel te verhogen door de gegevens drie keer te versleutelen, wat meer beveiliging dan DES biedt.
- AES-128 - Advanced Encryption Standard (AES) is 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 gewone tekst door 12-cycli wordt herhaald.
- AES-256 - Advanced Encryption Standard (AES) is een 256-bits coderingsmethode waarmee de gewone tekst door 14-cycli wordt herhaald.

IPSec Setup

Phase 1 DH Group:

Phase 1 Encryption:

Phase 1 Authentication:

Phase 1 SA Lifetime: sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group:

Phase 2 Encryption:

Phase 2 Authentication: (highlighted in red box)

Phase 2 SA Lifetime: sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key:

Preshared Key Strength Meter:

Stap 8. Kies de juiste authenticatiemethode in de vervolgkeuzelijst *Fase 2-verificatie*. De VPN-tunnel moet dezelfde verificatiemethode toepassen voor beide uiteinden.

- MD5 - Message Digest Algorithm-5 (MD5) staat voor de functie met 32 cijfers die een hexadecimale hashfunctie hebben, 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.
- Nul - Er wordt geen echtheidscontrole - methode gebruikt.

IPSec Setup

Phase 1 DH Group: Group 1 - 768 bit

Phase 1 Encryption: AES-128

Phase 1 Authentication: SHA1

Phase 1 SA Lifetime: 2870 sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group: Group 2 - 1024 bit


Phase 2 Encryption: AES-128

Phase 2 Authentication: MD5

Phase 2 SA Lifetime: 350 sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key: abcd1234ght

Preshared Key Strength Meter: 

Advanced +

Stap 9. Voer de hoeveelheid tijd in in seconden, in fase 2, blijft de VPN-tunnel actief in het veld *Fase 2 SA Livetime*. De standaardtijd is 3600 seconden.

Stap 10. Controleer het aanvinkvakje **Minimale gedeelde sleutel Complexity** als u krachtmeter voor de voorgedeelde toets wilt inschakelen.

Stap 1. Voer een toets in die eerder door de IKE-peers wordt gedeeld in het veld *PreShared Key*. Tot 30 alfanumerieke tekens kunnen als voorgedeelde toets 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 veranderen zodat VPN veilig blijft.

- PreShared Key Sterker Meter - dit is de kracht van de voorgedeelde toets via gekleurde balken. Rood wijst op zwakke sterkte, geel op aanvaardbare sterkte en groen op sterke sterkte. Als u in Stap 10 van **het vak Minimale instelbare sleutel** voor **instelbare sleutel** controleert, verschijnt alleen de Gepileerde Toetsversterking.

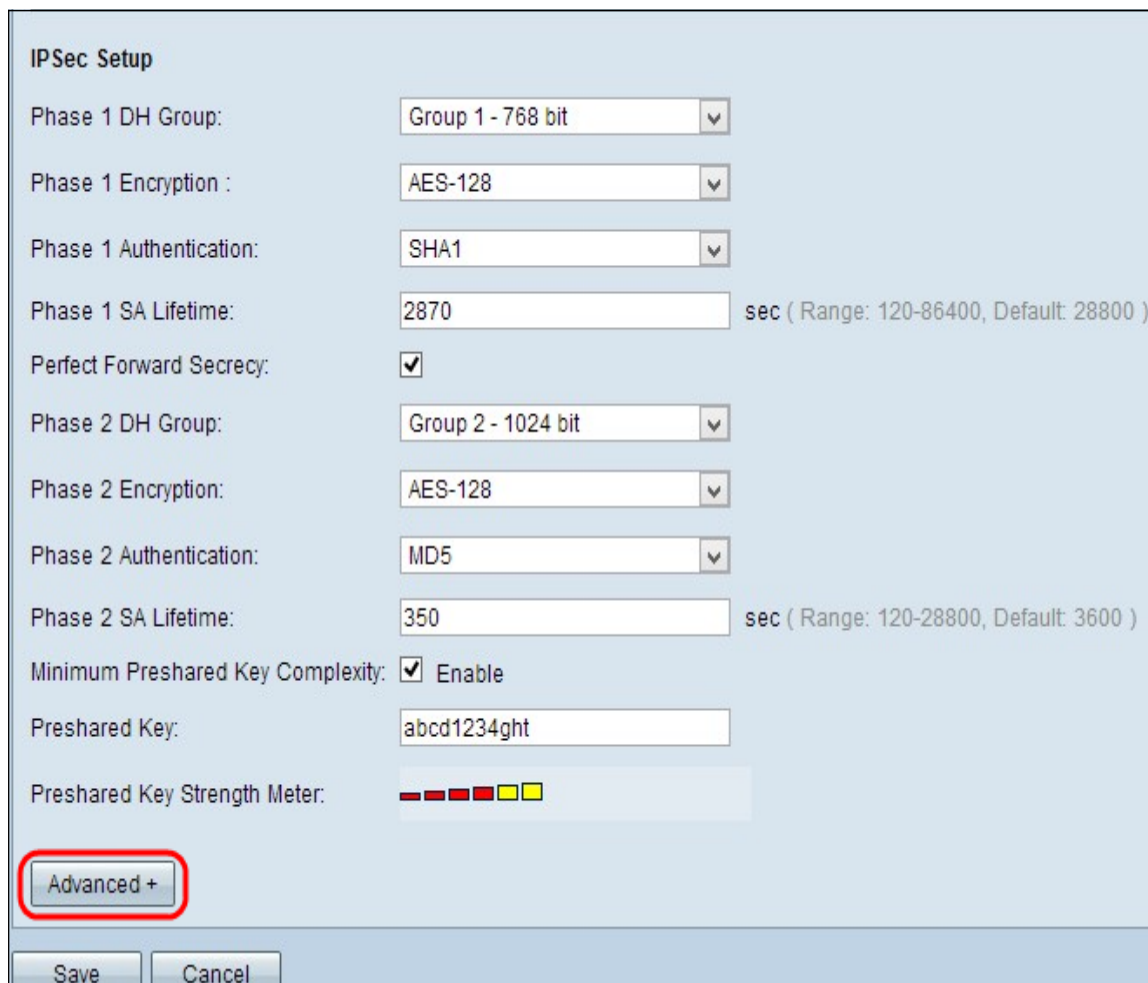
Opmerking: Als u voor IKE met PreShared Key kiest uit de vervolgkeuzelijst *Keying Mode* in Stap 3 voor *Add een sectie New Tunnel*, kunt u alleen de optie hebben om Stap 10, Stap 11 te configureren en de Gepubliceerde toetsuitbreidingsmeter te bekijken.

Stap 12. Als u de instellingen wilt opslaan die u tot nu toe hebt, klikt u op **Opslaan** om de instellingen op te slaan.

Geavanceerde setup met IKE met vooraf gedeelde sleutel of IKE met certificaat

Geavanceerde instellingen zijn alleen mogelijk voor IKE met PreShared Key en IKE met

certificeringsleutel. De handmatig ingestelde instellingen hebben geen geavanceerde instellingen.



The image shows a configuration window titled "IPSec Setup". It contains several settings for Phase 1 and Phase 2. Phase 1 settings include: Phase 1 DH Group (Group 1 - 768 bit), Phase 1 Encryption (AES-128), Phase 1 Authentication (SHA1), Phase 1 SA Lifetime (2870 sec, Range: 120-86400, Default: 28800), Perfect Forward Secrecy (checked), Phase 2 DH Group (Group 2 - 1024 bit), Phase 2 Encryption (AES-128), Phase 2 Authentication (MD5), Phase 2 SA Lifetime (350 sec, Range: 120-28800, Default: 3600), Minimum Preshared Key Complexity (checked, Enable), Preshared Key (abcd1234ght), and Preshared Key Strength Meter (a bar with four segments: two red, one yellow, one green). At the bottom left, there is a button labeled "Advanced +" which is circled in red. At the bottom of the window are "Save" and "Cancel" buttons.

Setting	Value	Notes
Phase 1 DH Group:	Group 1 - 768 bit	
Phase 1 Encryption :	AES-128	
Phase 1 Authentication:	SHA1	
Phase 1 SA Lifetime:	2870	sec (Range: 120-86400, Default: 28800)
Perfect Forward Secrecy:	<input checked="" type="checkbox"/>	
Phase 2 DH Group:	Group 2 - 1024 bit	
Phase 2 Encryption:	AES-128	
Phase 2 Authentication:	MD5	
Phase 2 SA Lifetime:	350	sec (Range: 120-28800, Default: 3600)
Minimum Preshared Key Complexity:	<input checked="" type="checkbox"/> Enable	
Preshared Key:	abcd1234ght	
Preshared Key Strength Meter:	■■■■	Strength indicator with 4 segments (2 red, 1 yellow, 1 green)

Stap 1. Klik op **Advanced** om de geavanceerde instellingen voor IKE te verkrijgen met de PreShared-toets.

Advanced

Aggressive Mode

Compress (Support IP Payload Compression Protocol(IPComp))

Keep-Alive

AH Hash Algorithm

NetBIOS Broadcast

NAT Traversal

Dead Peer Detection Interval sec (Range: 10-999, Default: 10)

Extended Authentication

IPsec Host

User Name:

Password:

Edge Device

Mode Configuration

Stap 2. Controleer het vakje **Aggressive Mode** als uw netwerksnelheid laag is. Het wisselt de ID's van de eindpunten van de tunnel in duidelijke tekst uit tijdens SA-aansluiting, hetgeen minder tijd vergt om te wisselen maar minder veilig is.

Stap 3. Controleer het vakje **Compressed (Support IP payload Compression Protocol (IPComp))** als u de grootte van IP-datagram wilt comprimeren. IPComp is een IP-compressieverhouding die wordt gebruikt om de grootte van IP-datagram te comprimeren als de netwerksnelheid laag is en de gebruiker de gegevens snel zonder verlies door het trage netwerk wil verzenden.

Stap 4. Controleer het aanvinkvakje **Houd-bewegend** vast als u altijd wilt dat de verbinding met de VPN-tunnel actief blijft. Het helpt om de verbindingen onmiddellijk te herstellen als een verbinding inactief wordt.

Stap 5. Controleer het aankruisvakje **AH Hash Algorithm** als u de Verificate Header (AH) wilt controleren. AH biedt verificatie aan gegevensoorsprong, gegevensintegriteit door middel van een checksum en de beveiliging wordt uitgebreid naar de IP-header. De tunnel zou hetzelfde algoritme moeten hebben voor beide kanten.

- MD5 - Message Digest Algorithm-5 (MD5) vertegenwoordigt de 128-cijferige hexadecimale hashfunctie, die bescherming biedt aan de gegevens tegen 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.

Stap 6. Controleer **Netoverheid Broadcast** als u niet-routeerbaar verkeer via de VPN-tunnel wilt toestaan. Dit is een ongecontroleerd standaard. Netoverheid wordt gebruikt om netwerkbronnen zoals printers, computers etc. in het netwerk te detecteren door middel van bepaalde softwaretoepassingen en Windows-functies zoals de netwerkbuurt.

Stap 7. Controleer het vakje **NAT Traversal** als u via uw openbare IP-adres het internet wilt bereiken via uw privénetwerk. NAT-verplaatsing wordt gebruikt om de privé IP-adressen van de interne systemen als openbare IP-adressen te verschijnen om de privé IP-adressen te beschermen tegen elke kwaadaardige aanval of ontdekking.

Stap 8. Controleer het **Dead Peer Detection Interval** om de levendigheid van de VPN-tunnel door hallo of ACK periodiek te controleren. Als u dit aanvinkvakje aankruist, specificeert u de duur of het interval van de gedag berichten die u wilt.

The screenshot shows the 'Advanced' configuration window for a VPN tunnel. The 'Extended Authentication' section is highlighted with a red border. It contains the following options:

- Extended Authentication
 - IPSec Host
 - User Name:
 - Password:
 - Edge Device
 - Default - Local Database (dropdown menu)
 - Add/Edit button
- Mode Configuration

At the bottom of the window are 'Save' and 'Cancel' buttons.

Stap 9. Controleer **Uitgebreide verificatie** om meer beveiliging en verificatie van de VPN-verbinding te bieden. Klik op het gewenste keuzerondje om de verificatie van de VPN-verbinding uit te breiden.

- IPsec host - uitgebreide verificatie door IPsec-host. Als u deze optie kiest, voert u de gebruikersnaam voor de IPsec-host in het veld Gebruikersnaam en een wachtwoord in het veld Wachtwoord in.
- Edge machine - uitgebreide verificatie via het randapparaat. Als u deze optie kiest, kiest u de database die het randapparaat bevat uit de vervolgkeuzelijst. Als u de database wilt toevoegen of bewerken, klikt u op **Toevoegen/Bewerken**.

Opmerking: Om meer te weten te komen over het toevoegen of bewerken van de lokale database, raadpleegt u *Gebruiker- en Domain Management Configuration op RV320-router*.

Stap 10. Controleer **Mode Configuration** om IP-adres te geven voor de inkomende tunnelaanvrager.

Opmerking: Stap 9 tot Stap 11 is beschikbaar voor de IKE PreShared Keying Mode voor Tunnel VPN.

Stap 1. Klik op **Opslaan** om de instellingen op te slaan.

Conclusie

U hebt nu de stappen geleerd om één client te configureren naar gateway-VPN op RV32x Series VPN-routers

Bekijk een video gerelateerd aan dit artikel...

[Klik hier om andere Tech Talks uit Cisco te bekijken](#)