

Configuratie van groepsclient voor Gateway Virtual Private Network (VPN) op RV320 en RV325 VPN-routerserie

Doel

Een Virtual Private Network (VPN) is een privaat netwerk dat wordt gebruikt om virtueel de apparaten van de externe gebruiker via het openbare netwerk aan te sluiten om beveiliging te bieden. Een van de typen VPN's is een client-naar-gateway VPN. Met client-to-poort kunt u verschillende takken van uw bedrijf in verschillende geografische gebieden op afstand verbinden om de gegevens tussen de gebieden beter te verzenden en ontvangen. Group VPN biedt een eenvoudige configuratie van VPN, omdat VPN-configuratie voor elke gebruiker niet meer werkt. De RV32x VPN-routerserie kan maximaal twee VPN-groepen ondersteunen.

Het doel van dit document is om uit te leggen hoe u een groepsclient kunt configureren naar VPN-gateway op RV32x Series VPN-routers.

Toepasselijke apparaten

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

Softwareversie

- v1.1.0.09

Groepsclient voor Gateway VPN

Stap 1. Meld u aan bij het hulpprogramma voor routerconfiguratie 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 **Group VPN** om een groepsclient-naar-gateway VPN toe te voegen.

Client to Gateway

Add a New Group VPN

Tunnel

Group VPN

Easy VPN

Group No. 1

Tunnel Name:

Interface:

Keying Mode: IKE with Preshared key

Enable:

Local Group Setup

Local Security Group Type:

IP Address:

Subnet Mask:

Remote Client Setup

Remote Client:

Domain Name:

Voeg een nieuwe Tunnel toe

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

Client to Gateway

Add a New Group VPN

Tunnel Group VPN Easy VPN

Group No. 1

Tunnel Name: tunnel_1

Interface: WAN1

Keying Mode: IKE with Preshared key

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: DomainName(FQDN)

Domain Name:

Opmerking: Groep nr. - vertegenwoordigt het nummer van de groep. Dit is een veld dat automatisch wordt gegenereerd.

Stap 2. Kies de juiste interface waardoor de VPN-groep met de poort verbonden is, uit de vervolgkeuzelijst *Interface*.

Client to Gateway

Add a New Group VPN

Tunnel Group VPN Easy VPN

Group No. 1

Tunnel Name: tunnel_1

Interface: WAN1
WAN1
WAN2
USB1
USB2

Keying Mode:

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: DomainName(FQDN)

Domain Name:

Stap 3. Controleer het aanvinkvakje **Enable** om de gateway-naar-gateway VPN toe te staan. Standaard is deze ingeschakeld.

Client to Gateway

Add a New Group VPN

Tunnel
 Group VPN
 Easy VPN

Group No. 1

Tunnel Name: tunnel_1

Interface: WAN1

Keying Mode: IKE with Preshared key

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: DomainName(FQDN)

Domain Name:

Opmerking: Bedieningsmodus - Hier wordt de gebruikte verificatiemodus weergegeven. IKE met PreShared Key is de enige optie, wat betekent dat het Internet Key Exchange (IKE)-protocol automatisch wordt gebruikt om een vooraf gedeelde sleutel te genereren en uit te wisselen voor het opzetten van gewaarmerkte communicatie voor de tunnel.

Stap 4. Om de instellingen op te slaan die u tot nu toe hebt en de rest standaard te laten, klikt u op **Opslaan** om de instellingen op te slaan.

Local Group Setup

Stap 1. Kies de juiste lokale LAN-gebruiker of de groep gebruikers die toegang kunnen krijgen tot de VPN-tunnel uit de vervolgkeuzelijst *Type* Local Security Group. De standaardinstelling is Subnet.

Client to Gateway

Add a New Group VPN

Tunnel
 Group VPN
 Easy VPN

Group No. 1

Tunnel Name: tunnel_1

Interface: WAN1

Keying Mode: IKE with Preshared key

Enable:

Local Group Setup

Local Security Group Type: Subnet

IP Address:

Subnet Mask: 255.255.255.0

Remote Client Setup

Remote Client: DomainName(FQDN)

Domain Name:

De beschikbare opties zijn als volgt gedefinieerd:

- IP — Er kan slechts één specifiek LAN-apparaat toegang tot de tunnel hebben. 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 specifieke subnetwerk 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 te krijgen tot de tunnel. Als u deze optie kiest, voert u de eerste en laatste IP-adressen voor het bereik in respectievelijk de velden *Start IP* en *End IP in*. Het standaardbereik loopt van 192.168.1.0 tot 192.168.1.254.

Stap 2. Om de instellingen op te slaan die u tot nu toe hebt en de rest standaard te laten, klikt u op **Opslaan** om de instellingen op te slaan.

Instellen externe client

Stap 1. Kies de juiste externe LAN-gebruiker of groep gebruikers die toegang kunnen krijgen tot de VPN-tunnel uit de vervolgkeuzelijst *Afstandsgroep security type*.

Client to Gateway

Add a New Group VPN

Tunnel
 Group VPN
 Easy VPN

Group No. 1

Tunnel Name: tunnel_1

Interface: WAN1

Keying Mode: IKE with Preshared key

Enable:

Local Group Setup

Local Security Group Type: IP

IP Address: 192.168.3.0

Remote Client Setup

Remote Client: DomainName(FQDN)

Domain Name: DomainName(FQDN)

Email Address(USER FQDN)
 Microsoft XP/2000 VPN Client

De beschikbare opties zijn als volgt gedefinieerd:

- Domain Name (FQDN)-verificatie — 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 *Naam van domein in*.
- E-mailadres. (USER FQDN) verificatie — Toegang tot de tunnel is mogelijk door een e-mailadres. 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 clientsoftware die een ingebouwde Microsoft XP of VPN-clientsoftware van 2000 is.

Stap 2. Om de instellingen op te slaan die u tot nu toe hebt en de rest standaard te laten, klikt u op **Opslaan** om de instellingen op te slaan.

IPsec-instelling

Stap 1. Kies de juiste Diffie-Hellman (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 aan te leggen ter ondersteuning van beveiligde communicatie. Diffie-Hellman is een cryptografisch zeer belangrijk uitwisselingsprotocol dat in Fase 1 verbinding wordt gebruikt om een geheime sleutel te delen om communicatie te authentifieren.

Remote Client Setup

Remote Client:

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: Enable

Preshared Key:

De beschikbare opties zijn als volgt gedefinieerd:

- Group1 (768 bit) — compileert de key het snelste, maar is de minst beveiligde.
- Group2 (1024-bits) — compileert de toets trager, maar is veiliger dan Group1.
- Groep5 (1536 bit) — Compileert de toets het langst, maar is het best veilig.

Stap 2. Kies de juiste encryptie-methode om de toets te versleutelen van de vervolgkeuzelijst *Fase 1 Encryption*. AES-128 wordt aanbevolen voor hoge security en snelle prestaties. De VPN-tunnel moet voor beide eindpunten dezelfde encryptie-methode gebruiken.

Remote Client Setup

Remote Client:

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:

De beschikbare opties zijn als volgt gedefinieerd:

- DES — Data Encryption Standard (DES) is een 56-bits oude encryptiemethode die niet erg veilig is, maar wel vereist is voor compatibiliteit met de achterzijde.
- 3DES - Triple Data Encryption Standard (3DES) is een 168-bits eenvoudige coderingsmethode die wordt gebruikt om de grootte van het bestand te vergroten, omdat de gegevens drie keer worden versleuteld. Dit biedt meer beveiliging dan DES maar minder beveiliging dan AES.
- AES-128 — Advanced Encryption Standard met 128-bits toets (AES-128) gebruikt een 128-bits toets voor AES-encryptie. AES is sneller en veiliger dan DES. In het algemeen is AES ook sneller en veiliger dan 3DES. AES-128 is sneller maar minder veilig dan AES-192 en AES-256.
- AES-192 — AES-192 gebruikt een 192-bits sleutel voor AES-encryptie. AES-1920 is langzamer maar veiliger dan AES-128 en sneller maar minder beveiligd dan AES-256.
- AES-256 — AES-256 gebruikt een 256-bits toets voor AES-encryptie. AES-256 is langzamer maar veiliger dan AES-128 en AES-192.

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

Remote Client Setup

Remote Client:

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: Enable

Preshared Key:

De beschikbare opties zijn als volgt gedefinieerd:

- MD5 — Message Digest Algorithm-5 (MD5) vertegenwoordigt 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.

Stap 4. In het veld *Fase 1 SA Life Time*, specificeert u de tijd in seconden dat de VPN-tunnel actief blijft in Fase 1. De standaardtijd is 28.800 seconden.

Remote Client Setup

Remote Client:

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: Enable

Preshared Key:

Stap 5. (Optioneel) Controleer het vakje **Perfect Forward SECURITY** om de toetsen beter te beschermen. Met deze optie kunt u een nieuwe toets genereren indien er een toets wordt gecompromitteerd. Dit is een aanbevolen actie omdat deze meer beveiliging biedt.

N.B.: Als u in Stap 5 het **programma** Perfect Forward Security verwijdert, hoeft u fase 2 DH Group niet te configureren.

Stap 6. Kies de juiste DH-groep in de vervolgkeuzelijst *Fase 2 DH Group*.

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: Enable

Preshared Key:

De beschikbare opties zijn als volgt gedefinieerd:

- Group1 (768 bit) — compileert de key het snelste, maar is de minst beveiligde.
- Group2 (1024-bits) — compileert de toets trager, maar is veiliger dan Group1.
- Groep5 (1536 bit) — Compileert de toets het langst, maar is het best veilig.

Stap 2. Kies de juiste encryptie-methode om de toets te versleutelen van de vervolgkeuzelijst *Fase 1 Encryption*. AES-128 wordt aanbevolen voor hoge security en snelle prestaties. De VPN-tunnel moet voor beide eindpunten dezelfde encryptie-methode gebruiken.

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:

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

Phase 2 Authentication:

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

Minimum Preshared Key Complexity: Enable

Preshared Key:

De beschikbare opties zijn als volgt gedefinieerd:

- DES — Data Encryption Standard (DES) is een 56-bits oude encryptiemethode die niet erg veilig is, maar wel vereist is voor compatibiliteit met de achterzijde.
- 3DES - Triple Data Encryption Standard (3DES) is een 168-bits eenvoudige coderingsmethode die wordt gebruikt om de grootte van het bestand te vergroten, omdat de gegevens drie keer worden versleuteld. Dit biedt meer beveiliging dan DES maar minder beveiliging dan AES.
- AES-128 — Advanced Encryption Standard met 128-bits toets (AES-128) gebruikt een 128-bits toets voor AES-encryptie. AES is sneller en veiliger dan DES. In het algemeen is AES ook sneller en veiliger dan 3DES. AES-128 is sneller maar minder veilig dan AES-192 en AES-256.
- AES-192 — AES-192 gebruikt een 192-bits sleutel voor AES-encryptie. AES-1920 is langzamer maar veiliger dan AES-128 en sneller maar minder beveiligd dan AES-256.
- AES-256 — AES-256 gebruikt een 256-bits toets voor AES-encryptie. AES-256 is langzamer maar veiliger dan AES-128 en AES-192.

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

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: Enable

Preshared Key:

De beschikbare opties zijn als volgt gedefinieerd:

- MD5 — Message Digest Algorithm-5 (MD5) vertegenwoordigt de hashfunctie met 128 bits, 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 9. In het veld *Fase 2 SA Live*, specificeert u de tijd in seconden dat de VPN-tunnel actief blijft in Fase 2. De standaardtijd is 3600 seconden.

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: Enable

Preshared Key:

Preshared Key Strength Meter: 

Stap 10. (Optioneel) Als u de sterktemeter voor de voorgedeelde toets wilt inschakelen, schakelt u het vakje **Minimale Gepineerde Key Complexity** in.

Opmerking: Als u het vakje **Minimale Gedeelde Key Complexity** controleert, toont de *Gedeelte Key Sterkte-meter* de sterkte van de voorgedeelde toets door gekleurde staven. Rood wijst op zwakke sterkte, geel op aanvaardbare sterkte en groen op sterke sterkte.

Stap 1. Voer de gewenste toets in het veld *Gedeelde sleutel in*. Tot 30 hexadecimale kunnen als de vooraf gedeelde 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 beveiligd blijft.

Stap 12. Om de instellingen op te slaan die u tot nu toe hebt en de rest standaard te laten, klikt u op **Opslaan** om de instellingen op te slaan.

Geavanceerde setup

Stap 1. Klik op **Advanced** om de geavanceerde instellingen te configureren.

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: Enable

Preshared Key:

Preshared Key Strength Meter:

Advanced +

Het *geavanceerde* gebied wordt weergegeven met nieuwe velden beschikbaar.

Phase 2 Authentication:

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

Minimum Preshared Key Complexity: Enable

Preshared Key:

Preshared Key Strength Meter:

Advanced -

Advanced

- Aggressive Mode
- Compress (Support IP Payload Compression Protocol(IPComp))
- Keep-Alive
- AH Hash Algorithm
- NetBIOS Broadcast
- NAT Traversal

Stap 2. (Optioneel) Controleer het vakje **Aggressive Mode** als uw netwerksnelheid laag is. De agressieve modus ruilt de ID's van de eindpunten van de tunnel in duidelijke tekst tijdens SA-verbinding, wat minder tijd nodig heeft om uit te wisselen maar minder veilig is.

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

Stap 4. (Optioneel) Controleer het aanvinkvakje **Regelmatig** als u altijd wilt dat de verbinding met de VPN-tunnel actief blijft. Houd-Alive helpt om de verbindingen direct te herstellen als een verbinding inactief wordt.

Stap 5. (Optioneel) Controleer het aanvinkvakje **AH Hash Algorithm** als u wilt dat de gegevens van oorsprong, de gegevensintegriteit en de checksum worden gecontroleerd en dat de beveiliging in de IP-header wordt uitgebreid. Kies vervolgens de juiste authenticatiemethode in de vervolgkeuzelijst. De tunnel zou hetzelfde algoritme moeten hebben voor beide kanten.

De beschikbare opties zijn als volgt gedefinieerd:

- **MD5** — Message Digest Algorithm-5 (MD5) vertegenwoordigt de hashfunctie met 128 bits, 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 het aankruisvakje **NetStart 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, enz. in het netwerk te detecteren via softwaretoepassingen en Windows-functies zoals netwerkbuurt.

Stap 7. (Optioneel) Controleer **NAT-kruisvakje** als u via uw privé-LAN-adres toegang tot het internet wilt hebben. NAT-verplaatsing wordt gebruikt om de privé IP-adressen van interne systemen aan te maken als openbare IP-adressen om de privé IP-adressen te beschermen tegen elke kwaadaardige aanval of ontdekking.

Stap 8. Klik op **Opslaan** om de instellingen op te slaan.