Gateway to Gateway Virtual Private Network (VPN) Configuration op RV320 en RV325 VPN-router Series

Doel

VPN's worden gebruikt om zeer veilige verbindingen te maken via twee eindpunten, via het openbare of gedeelde internet, door wat een VPN-tunnel wordt genoemd. Meer in het bijzonder staat een gateway-to-gateway VPN-verbinding toe voor twee routers om veilig met elkaar te verbinden en voor een client in het ene uiteinde om logischerwijs deel uit te maken van hetzelfde externe netwerk aan het andere uiteinde. Hierdoor kunnen gegevens en middelen gemakkelijker en veiliger via het internet worden gedeeld. De configuratie moet aan beide zijden van de verbinding worden uitgevoerd zodat een succesvolle verbinding van gateway-naar-gateway VPN wordt gerealiseerd. Het doel van dit artikel is om u met de configuratie van een gateway-naar-gateway VPN-verbinding op de RV32x VPN-routerserie te leiden.

Toepasselijke apparaten

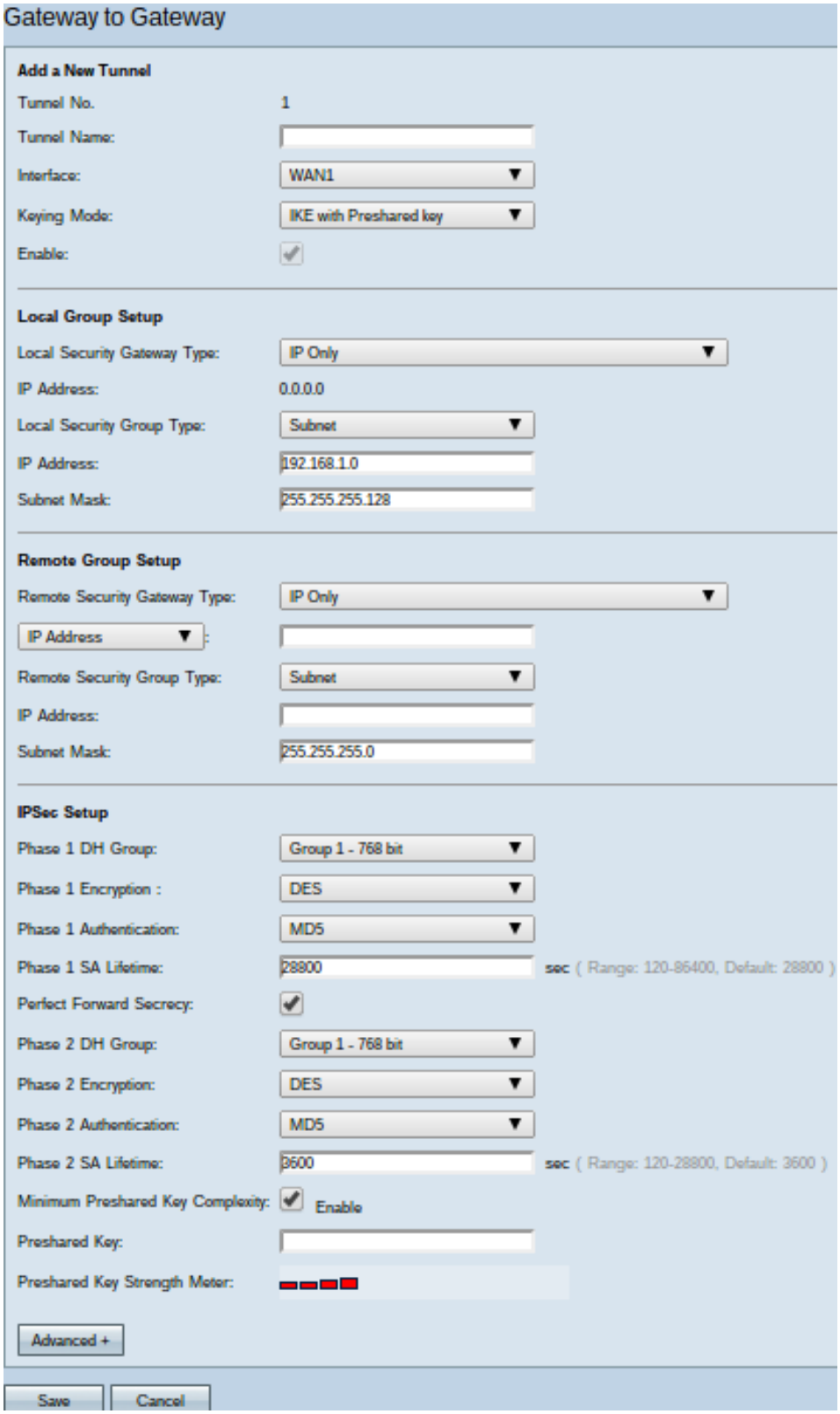
- RV320 VPN-router met dubbel WAN
- RV325 Gigabit VPN-router met dubbel WAN

Softwareversie

- v1.1.0.09

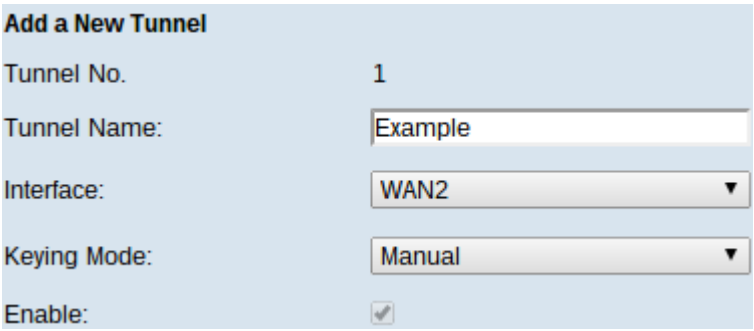
Gateway to Gateway

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



Om de VPN-verbinding naar behoren te kunnen laten werken, moeten de waarden van Internet Protocol Security (IPSec) aan beide zijden van de verbinding hetzelfde zijn. Beide zijden van de verbinding moeten behoren tot verschillende LAN's (Local Area Networks) en ten minste één van de routers moet identificeerbaar zijn door een statisch IP-adres of een dynamische DNS-hostnaam.

Voeg een nieuwe Tunnel toe



- Tunnel nr. — Hiermee wordt de huidige tunnel weergegeven die wordt aangemaakt. De router ondersteunt 100 tunnels.

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 specifieke WAN-poort van de router.

- WAN2 — De WAN2/DMZ poort op de router. Alleen worden weergegeven in het vervolgkeuzemenu als dit is geconfigureerd als WAN en niet als een DMZ-poort (Demilitariseert Zone).

- USB1 — De USB1 poort van de router. Werkt alleen als er een 3G/4G/LTE USB-dongle aan de poort is bevestigd.

- USB2 — de USB2 poort van de router. Werkt alleen als er een 3G/4G/LTE USB-dongle aan de poort is bevestigd.

Stap 3. Kies in de vervolgkeuzelijst Keying Mode de tunnelbeveiliging die u wilt gebruiken.

- Handmatig - Met deze optie kunt u de toets handmatig configureren in plaats van met de andere kant van de VPN-verbinding te onderhandelen.

- IKE met PreShared key — Kies deze optie om het Internet Key Exchange Protocol (IKE) in te schakelen, dat een beveiligingsassociatie in de VPN-tunnel instelt. IKE gebruikt een vooraf gedeelde sleutel om een externe peer te authentiseren.

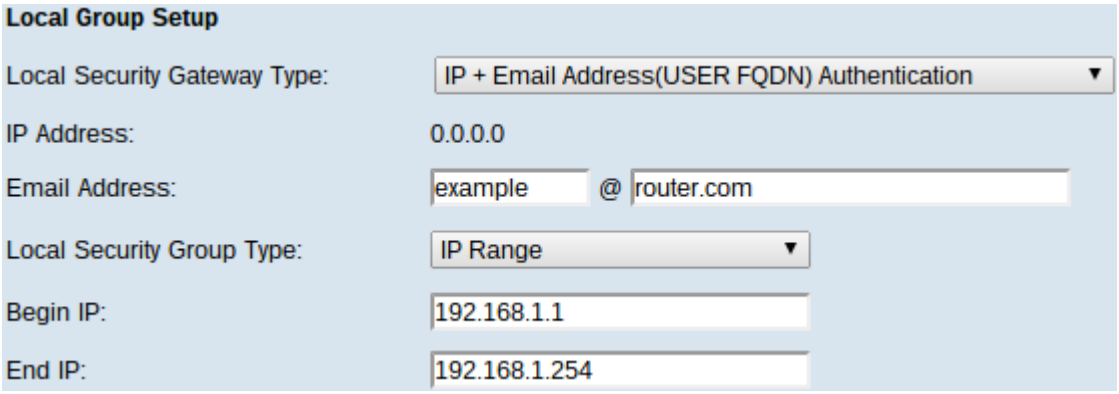
- IKE met certificaat — Kies deze optie om het Internet Key Exchange-protocol (IKE) in te schakelen met een certificaat dat een veiliger manier biedt om automatisch gedeelde sleutels te genereren en uit te wisselen, om voor de tunnel meer gewaarmerkte en beveiligde communicatie tot stand te brengen.

Stap 4. Controleer het aanvinkvakje Enable om de VPN-tunnel in te schakelen. Standaard is deze ingeschakeld.

Local Group Setup

Deze instellingen moeten overeenkomen met de instellingen "Remote Group Setup" voor de router aan het andere uiteinde van de VPN-tunnel.

Opmerking: Als de optie Handmatig of IKE met de voorgedeelde toets is geselecteerd in de vervolgkeuzelijst Keying Mode van Stap 3 of Add a New Tunnel start in Stap 1 en sla stap 2 tot en met 4 over. Als IKE met het certificaat is geselecteerd, stap 1.



Stap 1. Kies in de vervolgkeuzelijst Local Security Gateway Type de methode om de router te identificeren om de VPN-tunnel op te zetten.

- Alleen IP — Toegang tot de tunnel is alleen mogelijk via een statische WAN-IP. U kunt deze optie kiezen als alleen de router een statische WAN IP heeft. Het statische WAN IP-adres is een automatisch gegenereerd veld.

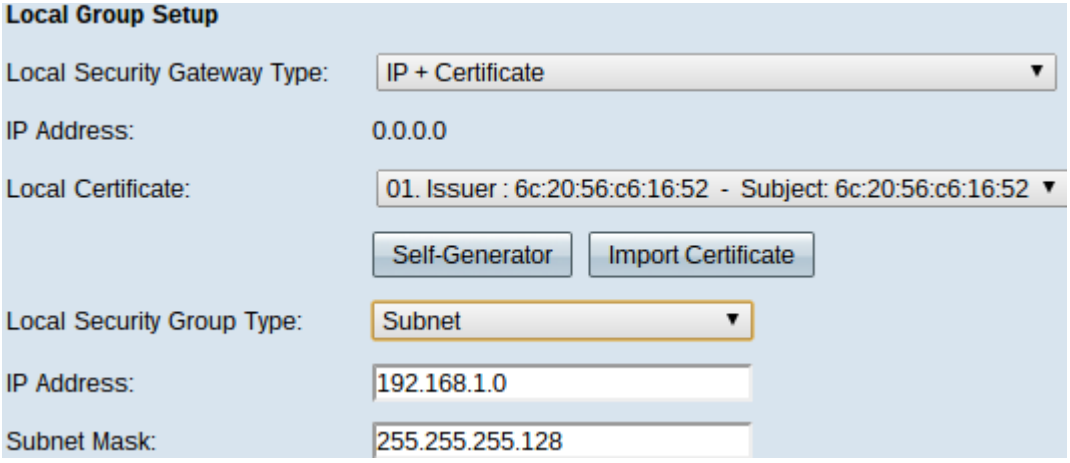
- IP + Domain Name (FQDN)-verificatie — Toegang tot de tunnel is mogelijk door een statisch IP-adres en een geregistreerd domein. Als u deze optie kiest, voert u de naam van het geregistreerde domein in het veld Naam van het domein in. Het statische WAN IP-adres is een automatisch gegenereerd veld.

- 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 is een automatisch gegenereerd veld.

- 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.

Opmerking: De volgende wijzigingen in het gebied Local Group Setup worden aangebracht bij het werken met IKE als certificaat.



De vervolgkeuzelijst Local Security Gateway Type wordt onbewerkbaar en geeft IP + certificaat weer. Dit is de LAN bron die de tunnel kan gebruiken.
Het veld IP-adres geeft het WAN IP-adres van het apparaat weer. Het kan niet door de gebruiker worden bewerkt.

Stap 2. Kies een certificaat uit de vervolgkeuzelijst Lokaal certificaat. Certificaten bieden een sterkere authenticatiebeveiliging op de VPN-verbindingen.

Stap 3. (Optioneel) Klik op de knop **Zelfgenerator** om het *venster* van *certificaatgenerator* weer te geven om certificaten te configureren en te genereren.

Stap 4. (Optioneel) Klik op de knop **Importeren** om het *venster Mijn certificaat* weer te geven om certificaten te bekijken en te configureren.

Stap 5. Kies een van de volgende opties in de vervolgkeuzelijst Local Security Group Type:

- IP-adres - Met deze optie kunt u één apparaat specificeren dat deze VPN-tunnel kan gebruiken. U hoeft alleen het IP-adres van het apparaat in het IP-adresveld in te voeren.

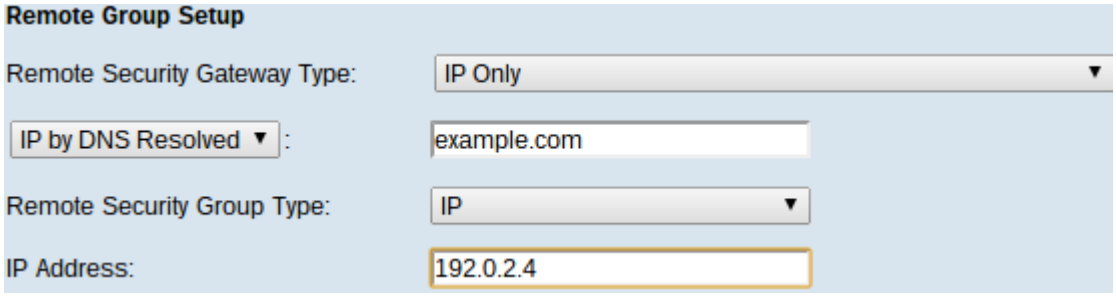
- Subnet - Kies deze optie om alle apparaten toe te staan die tot zelfde voorwerp behoren om de VPN tunnel te gebruiken. U moet het netwerk IP-adres in het veld IP-adres en het bijbehorende subnetmasker in het veld Subnetmasker invoeren.

- IP-bereik — Kies deze optie om een bereik van apparaten te specificeren dat de VPN-tunnel kan gebruiken. U moet het eerste IP-adres en het laatste IP-adres van het bereik van apparaten in het veld Beginnen IP en Eindtijd invoeren.

Instellen afstandsgroep

Deze instellingen moeten overeenkomen met de instellingen "Local Group Setup" voor de router aan het andere uiteinde van de VPN-tunnel.

Opmerking: Als Handmatig of IKE met de voorgedeelde toets is geselecteerd in de vervolgkeuzelijst Keying Mode van Stap 3 of Add a New Tunnel start in Stap 1 en sla stap 2 tot en met 5 over. Of als IKE met certificaatnummer is geselecteerd, stap 1.



Stap 1. Kies in de vervolgkeuzelijst Type afstandsbeveiliging de methode om de andere router te identificeren om de VPN-tunnel op te zetten.

- Alleen IP — Toegang tot de tunnel is alleen mogelijk via een statische WAN-IP. Als u het IP-adres van de externe router kent, kiest u IP-adres in de vervolgkeuzelijst direct onder het veld Gateway type afstandsbeveiliging 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.

- IP + Domain Name (FQDN)-verificatie — Toegang tot de tunnel is mogelijk door een statisch IP-adres en een geregistreerd domein van de router. Als u het IP-adres van de externe router kent, kiest u IP-adres in de vervolgkeuzelijst direct onder het veld Gateway type afstandsbeveiliging 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. Als u deze optie kiest, voert u de naam van het

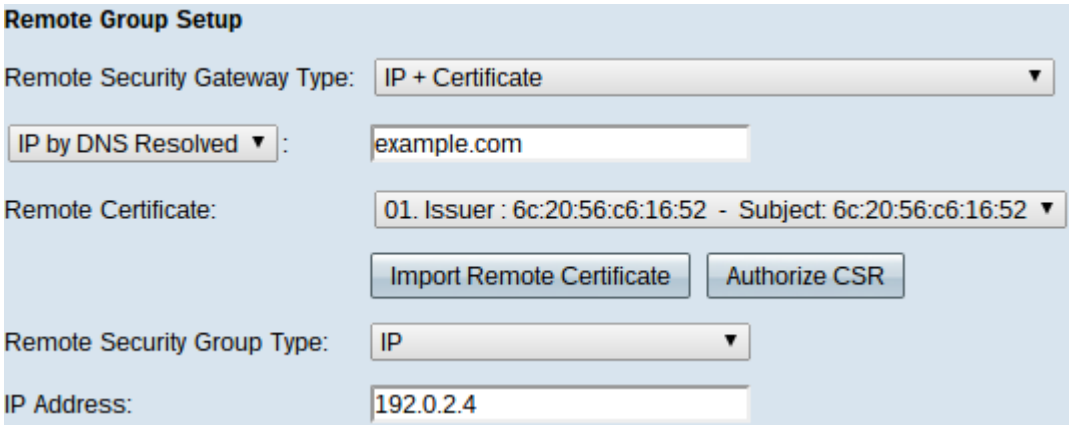
geregistreerde domein in het veld Naam van het domein in.

- 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, kies IP-adres in de vervolgkeuzelijst direct onder het veld Type Remote Security Gateway en voer 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.
Opmerking: Als beide routers dynamische IP-adressen hebben, kiest u NIET Dynamisch IP + e-mailadres voor beide gateways.

Opmerking: De volgende wijzigingen in het gebied Instellen van de Remote Group hebben een andere invloed bij het werken met IKE met Certificaat.



De vervolgkeuzelijst Afstandsbeveiligingsgateway wordt onbewerkbaar en geeft IP + certificaat weer. Dit is de LAN bron die de tunnel kan gebruiken.

Stap 2. Als u het IP-adres van de externe router kent, kiest u IP-adres in de vervolgkeuzelijst direct onder het veld Type afstandsbeveiliging 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 externe router in het IP-veld met DNS Opgeloste veld in

Stap 3. Kies een certificaat uit de vervolgkeuzelijst Afstandsbewijs. Certificaten bieden een sterkere authenticatiebeveiliging op de VPN-verbindingen.

Stap 4. (Optioneel) Klik op de knop **Afstandscertificaat importeren** om een nieuw certificaat te importeren.

Stap 5. (Optioneel) Klik op de knop **CSR** autoriseren om het certificaat te identificeren met een digitale ondertekeningsaanvraag.

Stap 6. Kies een van de volgende opties in de vervolgkeuzelijst Local Security Group Type:

- IP-adres - Met deze optie kunt u één apparaat specificeren dat deze VPN-tunnel kan gebruiken. U hoeft alleen het IP-adres van het apparaat in het IP-adresveld in te voeren.

- Subnet - Kies deze optie om alle apparaten toe te staan die tot zelfde voorwerp behoren om de VPN tunnel te gebruiken. U moet het netwerk IP-adres in het veld IP-adres en het bijbehorende subnetmasker in het veld Subnetmasker invoeren.

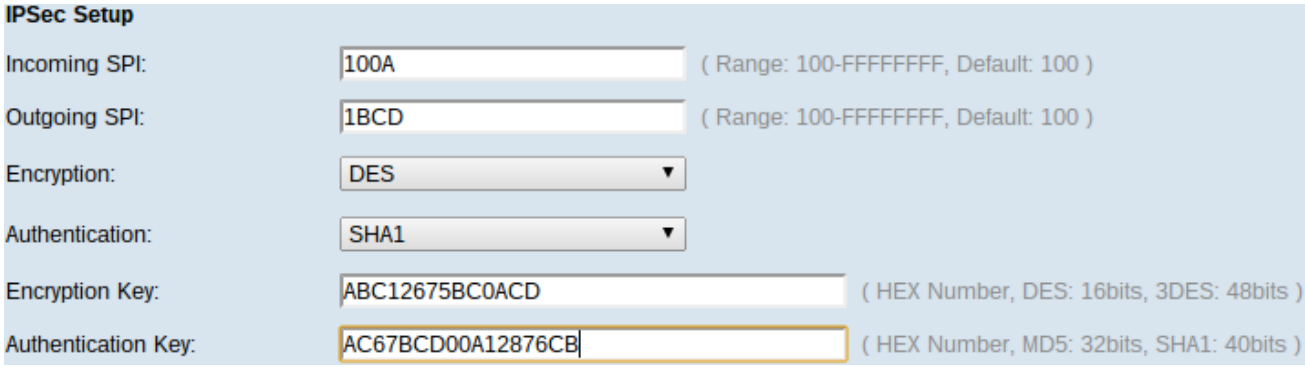
- IP-bereik — Kies deze optie om een bereik van apparaten te specificeren dat de VPN-tunnel kan gebruiken. U moet het eerste IP-adres en het laatste IP-adres van het bereik van apparaten invoeren. In het veld Beginnen IP en Eind IP.

IPsec-instelling

Om de encryptie goed te kunnen instellen tussen de twee uiteinden van de VPN-tunnel moeten beide exact dezelfde instellingen hebben. In dit geval creëert IPSec een veilige authenticatie tussen de twee apparaten. Dat gebeurt in twee fasen.

IPsec-instelling voor handmatige modus

Alleen beschikbaar indien Handmatig is geselecteerd uit de vervolgkeuzelijst Keying Mode in Stap 3 van Add a New Tunnel. Dit is een aangepaste beveiligingsmodus zodat u zelf een nieuwe beveiligingssleutel kunt genereren en niet onderhandelt met de toets. Het is het best te gebruiken tijdens het oplossen van problemen en in een klein statisch milieu.



Stap 1. Voer de unieke hexadecimale waarde in voor inkomende security parameter Index (SPI) in het veld Inkomende SPI. SPI wordt geleverd in Encapsulation Security Payload (ESP) Protocol-header, die samen de beveiliging van het inkomende pakket bepaalt. Je kunt van 100 naar FFFFFFFF gaan.

Stap 2. Voer de unieke hexadecimale waarde in voor SPI in het veld Uitgaande SPI. SPI wordt in de ESP-header opgeslagen, die samen de beveiliging van het uitgaande pakket bepaalt. Je kunt van 100 naar FFFFFFFF gaan.

Opmerking: De inkomende en uitgaande SPI moeten aan beide uiteinden met elkaar overeenkomen om een tunnel tot stand te brengen.

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

- DES — DES (Data Encryption Standard) is een 56-bits oude, meer achterwaartse compatibele coderingsmethode die niet zo veilig is als moeilijk te breken.

- 3DES - 3DES (Triple Data Encryption Standard) is een 168 bit, eenvoudige encryptiemethode om de grootte van de sleutel te verhogen door de gegevens drie keer te versleutelen, wat meer beveiliging dan DES biedt.

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 — MD5 (Message Digest Algorithm-5) staat voor de functie met 32 cijfers hexadecimale hash, die bescherming biedt aan de gegevens tegen kwaadaardige aanvallen door de berekening van de checksum.

- SHA1 — SHA1 (Secure Hash Algorithm, versie 1) is een 160-bits hashfunctie die veiliger is dan MD5.

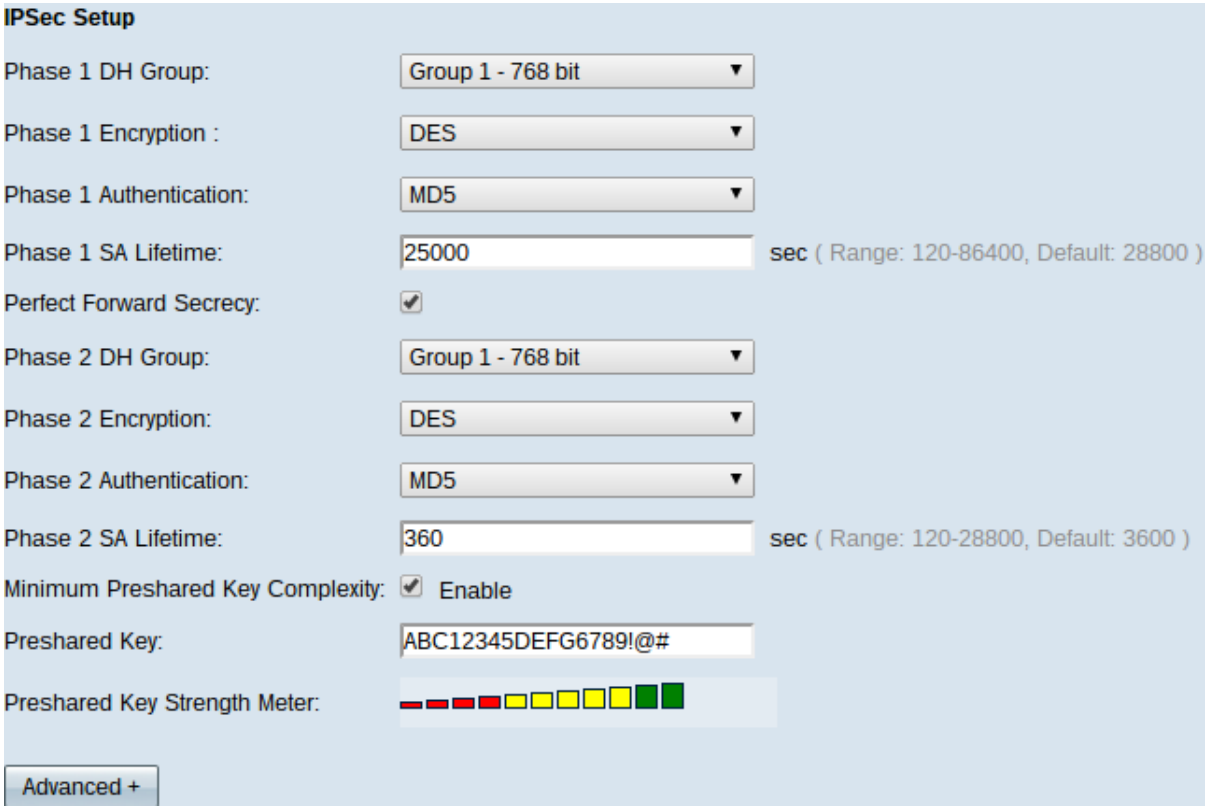
Stap 5. Voer de sleutel in om gegevens te versleutelen en te decrypteren in het veld Encryption Key. Als u DES als encryptiemethode in Stap 3 kiest, voer dan een 16-cijferige hexadecimale waarde in. Als u in Stap 3 3DES als encryptiemethode kiest, typt u een hexadecimale waarde van 40 cijfers.

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

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

IPsec-instelling voor IKE met gedeelde sleutel

Alleen beschikbaar als IKE met de modus PreShared is geselecteerd uit de vervolgkeuzelijst Keying Mode in Stap 3 van Add a New Tunnel.



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 in te stellen ter ondersteuning van beveiligde communicatie. Diffie-Hellman

(DH) is een cryptografietoepassingssleutelprotocol dat tijdens Fase 1 verbinding wordt gebruikt om een geheime sleutel te delen om communicatie te authentiseren.

- Groep 1 - 768 bit - vertegenwoordigt de hoogste sterktesleutel en de best 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.

- Groep 2 - 1024 bit - vertegenwoordigt een hogere sterkte en een veiliger authenticatiegroep. Het heeft tijd nodig om de IKE-toetsen te berekenen.

- Groep 5 - 1536 bit - vertegenwoordigt de laagste sterkte en de meest onveilige echtheidsgroep. Het heeft minder tijd nodig om de IKE-toetsen te berekenen. Het is de voorkeur dat de snelheid van het netwerk laag is.

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 coderingsmethode gebruiken voor beide eindpunten.

- DES — Data Encryption Standard (DES) is 56-bits, oude encryptiemethode die in de huidige wereld niet erg veilig is.

- 3DES - Triple Data Encryption Standard (3DES) is een 168-bits, eenvoudige coderingsmethode om de grootte van de sleutel te verhogen door de gegevens drie keer te versleutelen, wat meer beveiliging biedt dan DES.

- AES-128 — Advanced Encryption Standard (AES) is een 128-bits coderingsmethode waarmee de onbewerkte tekst door 10 cycli wordt herhaald.

- AES-192 — Is 192-bits coderingsmethode die de onbewerkte tekst door 12 cycli in een algoritme omzet.

- AES-256 — is een 256-bits coderingsmethode die de gewone tekst door 14-cycli in een algoritme omzet.

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

- MD5 — Message Digest Algorithm-5 (MD5) vertegenwoordigt een hexadecimale hashfunctie met 32 cijfers die bescherming biedt aan de gegevens tegen boosaardige aanvallen door de berekening van de checksum.

- SHA1 — Een 160-bits hashfunctie die veiliger is dan MD5.

Stap 4. Voer de hoeveelheid tijd in seconden in die de VPN-tunnel actief blijft in het veld Fase 1 SA Life Time.

Stap 5. Controleer het vakje Perfect Forward Security (Gebiedsgeheim) om de toetsen beter te beschermen. 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.

Stap 6. Kies de juiste fase 2 DH-groep uit de vervolgkeuzelijst Fase 2 DH-groep. Fase 1

wordt gebruikt om de simplex, logical Security Association (SA) tussen de twee uiteinden van de tunnel in te stellen ter ondersteuning van beveiligde communicatie. 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 hoogste sterktesleutel en de best 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.

- Groep 2 - 1024 bit - vertegenwoordigt een hogere sterkte en een veiliger authenticatiegroep. Het heeft tijd nodig om de IKE-toetsen te berekenen.

- Groep 5 - 1536 bit - vertegenwoordigt de laagste sterkte en de meest onveilige echtheidsgroep. Het heeft minder tijd nodig om de IKE-toetsen te berekenen. Het is de voorkeur dat de snelheid van het netwerk laag is.

Opmerking: Aangezien er geen nieuwe toets wordt gegenereerd, hoeft u fase 2 DH Group niet te configureren als u in stap 5 het programma Perfect Forward Security verwijdert.

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 coderingsmethode gebruiken voor beide eindpunten.

- DES — DES is een 56-bits oude encryptiemethode die niet erg veilig is in de huidige wereld.

- 3DES — 3DES is een 168-bits eenvoudige coderingsmethode om de grootte van de sleutel te vergroten door de gegevens drie keer te versleutelen, wat meer beveiliging biedt dan DES.

- AES-128 — AES is een 128-bits coderingsmethode die de onbewerkte tekst door 10-cycli in een coderingsmethode omzet.

- AES-192 — Is 192-bits coderingsmethode die de onbewerkte tekst door 12 cycli in een algoritme omzet.

- AES-256 — is een 256-bits coderingsmethode die de gewone tekst door 14-cycli in een algoritme omzet.

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

- MD5 — MD5 staat voor een hexadecimale hashfunctie van 32 cijfers die bescherming biedt tegen de gegevens van een kwaadaardige aanval door middel van de berekening van de checksum.

- SHA1 — Secure Hash Algorithm, versie 1 (SHA1), is een 160-bits hashfunctie die veiliger is dan MD5.

- Volledig - Er wordt geen echtheidscontrole gebruikt.

Stap 9. Voer de hoeveelheid tijd in seconden in die de VPN-tunnel actief blijft in het veld Fase 2 SA Life Time.

Stap 10. Controleer het aankruisvakje 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 is gedeeld in het veld Voorgedeelde sleutel. Tot 30 hexadecimale en tekens kunnen worden gebruikt als een voorgedeelde toets. De VPN-tunnel moet dezelfde vooraf gedeelde toets gebruiken voor beide eindpunten.

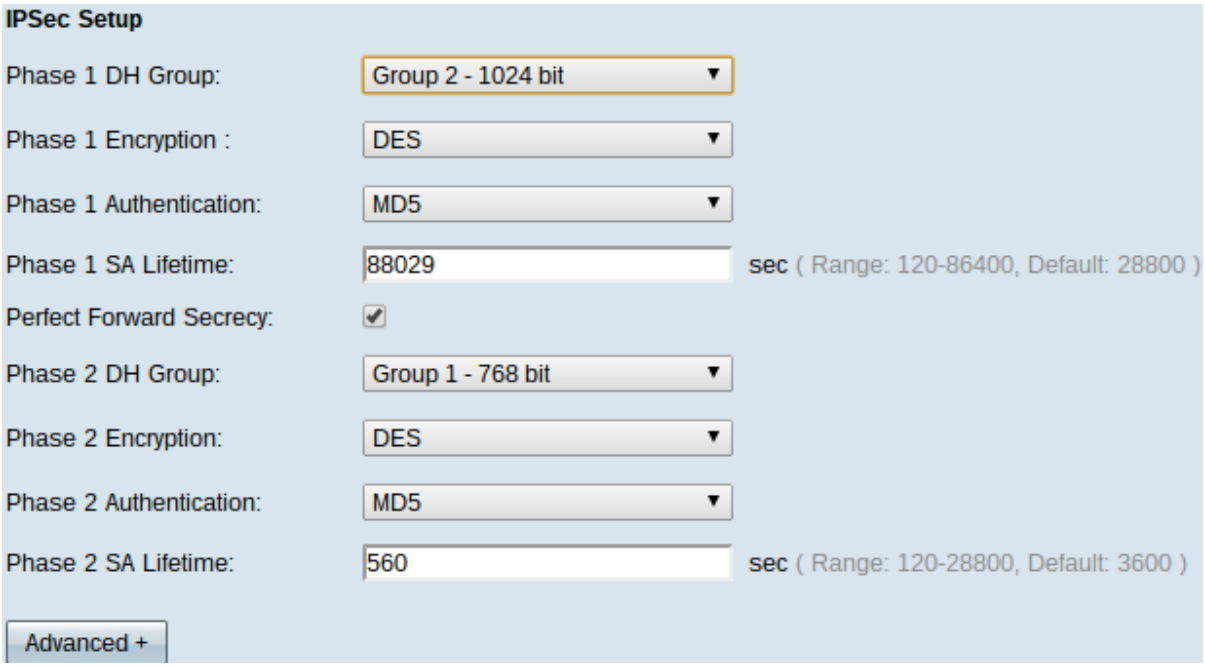
Opmerking: Het is sterk aanbevolen om regelmatig de gedeelde sleutel tussen de IKE-peers te veranderen zodat VPN veilig blijft.

De PreShared Key Sterker Meter toont de kracht van de voorgedeelde toets door middel van kleurenbalken. 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.

IPsec-instelling voor IKE met certificaat

Alleen beschikbaar als IKE met certificaatnummer is geselecteerd in de vervolgkeuzelijst Eindmodus van Stap 3 van Add a New Tunnel.



Stap 1. Kies de juiste fase 1 DH-groep uit de vervolgkeuzelijst Fase 1 DH-groep. Fase 1 wordt gebruikt om de simplex, logical SA (Security Association) tussen de twee uiteinden van de tunnel in te stellen ter ondersteuning van beveiligde communicatie. 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 hoogste sterktesleutel en de best beveiligde authenticatiegroep. Maar het heeft meer tijd nodig om de IKE-toetsen te berekenen. Het is de voorkeur dat de snelheid van het netwerk hoog 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 laagste sterkte en de meest onveilige echtheidsgroep. Het heeft minder tijd nodig om de IKE-toetsen te berekenen. Het is de voorkeur dat de snelheid van het netwerk laag is.

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 coderingsmethode gebruiken voor beide eindpunten.

- DES — DES is een 56-bits oude encryptiemethode die niet erg veilig is in de huidige wereld.
- 3DES — 3DES is een 168-bits eenvoudige coderingsmethode om de grootte van de sleutel te vergroten door de gegevens drie keer te versleutelen, wat meer beveiliging biedt dan DES.
- AES-128 — AES is een 128-bits coderingsmethode die de onbewerkte tekst door 10-cycli in een coderingsmethode omzet.
- AES-192 — Is 192-bits coderingsmethode die de onbewerkte tekst door 12 cycli in een algoritme omzet.
- AES-256 — is een 256-bits coderingsmethode die de gewone tekst door 14-cycli in een algoritme omzet.

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

- MD5 — MD5 staat voor een hexadecimale hashfunctie van 32 cijfers die bescherming biedt tegen de gegevens van een kwaadaardige aanval door middel van de berekening van de checksum.
- SHA1 — Een 160-bits hashfunctie die veiliger is dan MD5.

Stap 4. Voer de hoeveelheid tijd in seconden in die de VPN-tunnel actief blijft in het veld Fase 1 SA Life Time.

Stap 5. Controleer het vakje Perfect Forward Security (Gebiedsgeheim) om de toetsen beter te beschermen. 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 veilige en echt gewaarmerkte communicatie, omdat het andere sleutels veilig stelt wanneer een andere sleutel gecompromitteerd wordt. Dit is een aanbevolen actie omdat deze meer beveiliging biedt.

Stap 6. Kies de juiste fase 2 DH-groep uit de vervolgkeuzelijst Fase 2 DH-groep. Fase 1 wordt gebruikt om de simplex, logical SA tussen de twee uiteinden van de tunnel in te stellen om veilige communicatie te ondersteunen. 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 hoogste sterktesleutel en de best beveiligde authenticatiegroep. Maar het heeft meer tijd nodig om de IKE-toetsen te berekenen. Het is de voorkeur dat de snelheid van het netwerk hoog 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 laagste sterkte en de meest onveilige echtheidsgroep. Het heeft minder tijd nodig om de IKE-toetsen te berekenen. Het is de voorkeur dat de snelheid van het netwerk laag is.

Opmerking: Aangezien er geen nieuwe toets wordt gegenereerd, hoeft u fase 2 DH Group niet te configureren als u in Stap 5 het programma Perfect Forward Security niet hebt ingeschakeld.

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 coderingsmethode gebruiken voor beide eindpunten.

- DES — DES is een 56-bits oude encryptiemethode die niet erg veilig is in de huidige wereld.
- 3DES — 3DES is een 168-bits eenvoudige coderingsmethode om de grootte van de sleutel te vergroten door de gegevens drie keer te versleutelen, wat meer beveiliging biedt dan DES.
- AES-128 — AES is een 128-bits coderingsmethode die de onbewerkte tekst door 10-cycli in een coderingsmethode omzet.
- AES-192 — Is 192-bits coderingsmethode die de onbewerkte tekst door 12 cycli in een algoritme omzet.
- AES-256 — is een 256-bits coderingsmethode die de gewone tekst door 14-cycli in een algoritme omzet.

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

- MD5 — MD5 staat voor een hexadecimale hashfunctie van 32 cijfers die bescherming biedt tegen de gegevens van een kwaadaardige aanval door middel van de berekening van de checksum.
- SHA1 — SHA1 is een 160 bit hash-functie die veiliger is dan MD5.
- Volledig - Er wordt geen echtheidscontrole gebruikt.

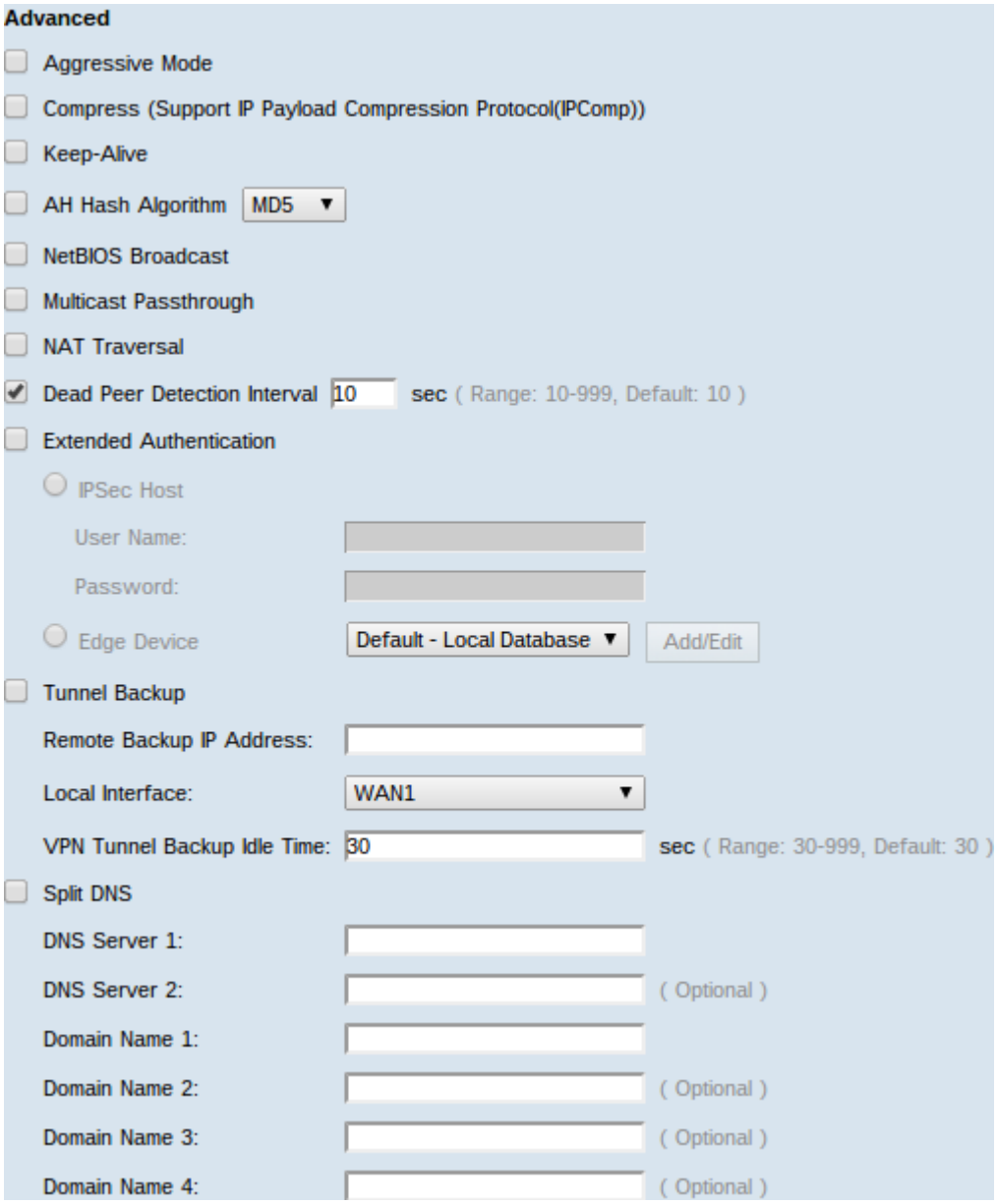
Stap 9. Voer de hoeveelheid tijd in seconden in die de VPN-tunnel actief blijft in het veld Fase 2 SA Life Time.

Stap 10. Klik op **Opslaan** om de instellingen op te slaan.

(Optioneel) IPSec Advanced Setup voor IKE met certificaatmodel en IKE met gedeelde sleutel

De geavanceerde opties zijn beschikbaar indien IKE met Certificaat of IKE met Vooraf ingestelde toets is geselecteerd uit de vervolgkeuzelijst Keying Mode in Stap 3 van Add a New Tunnel. Deze instellingen zijn ook beschikbaar voor beide typen bevestigingsmodi.

Stap 1. Klik op de knop **Advanced+** om de geavanceerde IPSec-opties weer te geven.



Stap 2. Controleer het vakje Aggressief 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 Comprimeer (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-actief 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 aanvinkvakje AH Hash Algorithm als u het vakje 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 — MD5 staat voor een hexadecimale hashfunctie van 128 cijfers die bescherming biedt tegen de gegevens van een kwaadaardige aanval door middel van de berekening van de checksum.

- SHA1 — SHA1 is een 160 bit hash-functie 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. Als uw VPN-router achter een NAT-gateway staat, schakelt u het vakje in om NAT-verplaatsing in te schakelen. Network adresomzetting (NAT) stelt gebruikers met privé LAN-adressen in staat om toegang te krijgen tot internetbronnen door een publiekelijk routeerbaar IP-adres als bronadres te gebruiken. Voor inkomende verkeer heeft de NAT-gateway echter geen automatische methode om het openbare IP-adres naar een bepaalde bestemming op het particuliere LAN te vertalen. Deze kwestie belemmert succesvolle IPSec-uitwisselingen. NAT-omkering stelt deze inkomende vertaling in. Aan beide uiteinden van de tunnel moet dezelfde instelling worden gebruikt.

Stap 8. Controleer het Dead Peer Detection Interval om de levendigheid van de VPN-tunnel door hallo of ACK op een periodieke manier te controleren. Als u dit aanvinkvakje aankruist, specificeert u de duur of de tussenpoos in seconden van de hallo-berichten die u wilt.

Stap 9. Controleer Uitgebreide verificatie om een gebruikersnaam en wachtwoord voor IPSec-host te gebruiken om VPN-clients te authentiseren of om de database te gebruiken die in Gebruikersbeheer is gevonden. Dit moet in beide apparaten mogelijk zijn om te kunnen werken. Klik op de radioknop **IPSec Host** om IPSec-host en -gebruikersnaam te gebruiken en voer de gebruikersnaam en het wachtwoord in het veld Gebruikersnaam en het veld Wachtwoord in. Of klik op het radioknop **Edge Devices** om een database te gebruiken. Kies de gewenste database in de vervolgkeuzelijst Edge-apparaat.

Stap 10. Controleer het aanvinkvakje voor back-up van Tunnel om tunnelback-up mogelijk te maken. Deze optie is beschikbaar bij controle van het onderdeelprogramma van de peer. Deze functie stelt het apparaat in staat om de VPN-tunnel opnieuw op te zetten via een alternatieve WAN-interface of IP-adres.

- Remote Backup IP-adres - een alternatieve IP-telefoon voor de afstandsbediening. Voer het in voor WAN IP dat al is ingesteld voor de externe gateway in dit veld.

- Lokale interface - de WAN-interface die wordt gebruikt om de verbinding opnieuw op te zetten. Kies de gewenste interface in de vervolgkeuzelijst.

- VPN Tunnel back-up-tijd - De tijd die is gekozen voor het gebruik van de reservetuning als de primaire tunnel niet is aangesloten. Geef het in seconden op.

Stap 1. Controleer het vakje Split DNS-controle om gesplitste DNS in te schakelen. Met deze functie kunt u DNS-aanvraag naar een bepaalde DNS-server verzenden op basis van gespecificeerde domeinnamen. Voer de DNS-servernamen in in de velden DNS-server 1 en DNS-server 2 en voer de domeinnamen in de velden Domain Name # in.

Stap 12. Klik op **Save** om het apparaat te configureren.