Geavanceerde instellingen voor gateway naar gateway VPN configureren op RV016-, RV042-, RV042G- en RV082 VPN-routers

Doel

Een Virtual Private Network (VPN) is een privaat netwerk dat wordt gebruikt om apparaten van de externe gebruiker virtueel aan te sluiten via een openbaar netwerk om beveiliging te bieden. Meer specifiek, staat een gateway-to-gateway VPN verbinding voor twee routers toe om veilig met elkaar en voor een cliënt in één eind te verbinden om logisch gezien om deel van het zelfde verre netwerk op het andere eind te lijken. Hierdoor kunnen gegevens en bronnen gemakkelijker en veiliger worden gedeeld via het internet. Aan beide zijden van de verbinding moet een identieke configuratie worden uitgevoerd om een succesvolle gateway-to-gateway VPN-verbinding tot stand te brengen.

Advanced Gateway to Gateway VPN-configuratie biedt de flexibiliteit om optionele configuraties te configureren zodat de VPN-tunnel gebruiksvriendelijker is voor de VPN-gebruikers. De geavanceerde opties zijn alleen beschikbaar voor IKE met de toetsmodus Preshared. De geavanceerde instellingen moeten aan beide zijden van de VPN-verbinding hetzelfde zijn.

Het doel van dit document is u te tonen hoe u geavanceerde instellingen kunt configureren voor gateway naar gateway VPN-tunnel op RV016, RV042, RV042G en RV082 VPN-routers.

Opmerking: Als u meer wilt weten over de configuratie van een gateway voor Gateway VPN, raadpleegt u het artikel *Configuration of Gateway to Gateway VPN op RV016, RV042, RV042G en RV082 VPN-routers.*

Toepasselijke apparaten

· RV016
â€¢RV042
· RV042G
· RV082

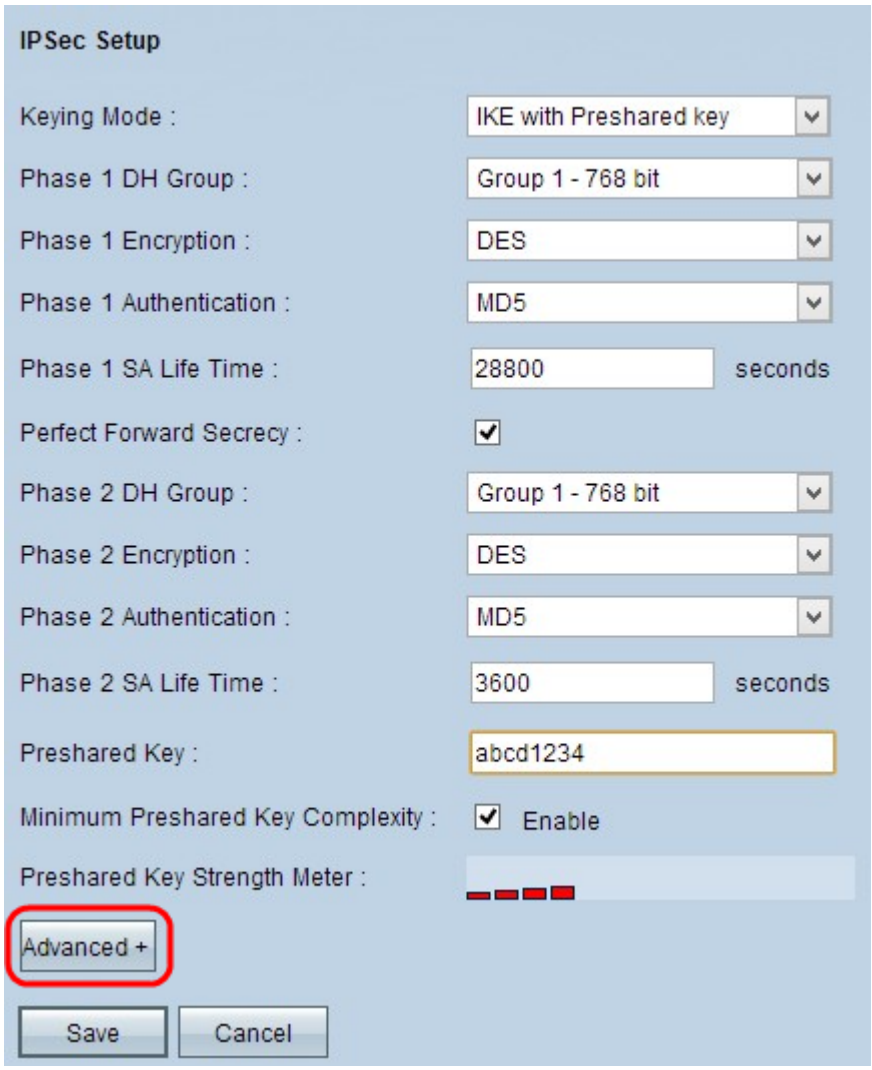
Softwareversie

· v4.2.2.08

Configuratie van geavanceerde instellingen voor Gateway to Gateway VPN

Stap 1. Log in op het hulpprogramma voor routerconfiguratie en kies **VPN > Gateway to Gateway**. De pagina *Gateway to Gateway* wordt geopend:

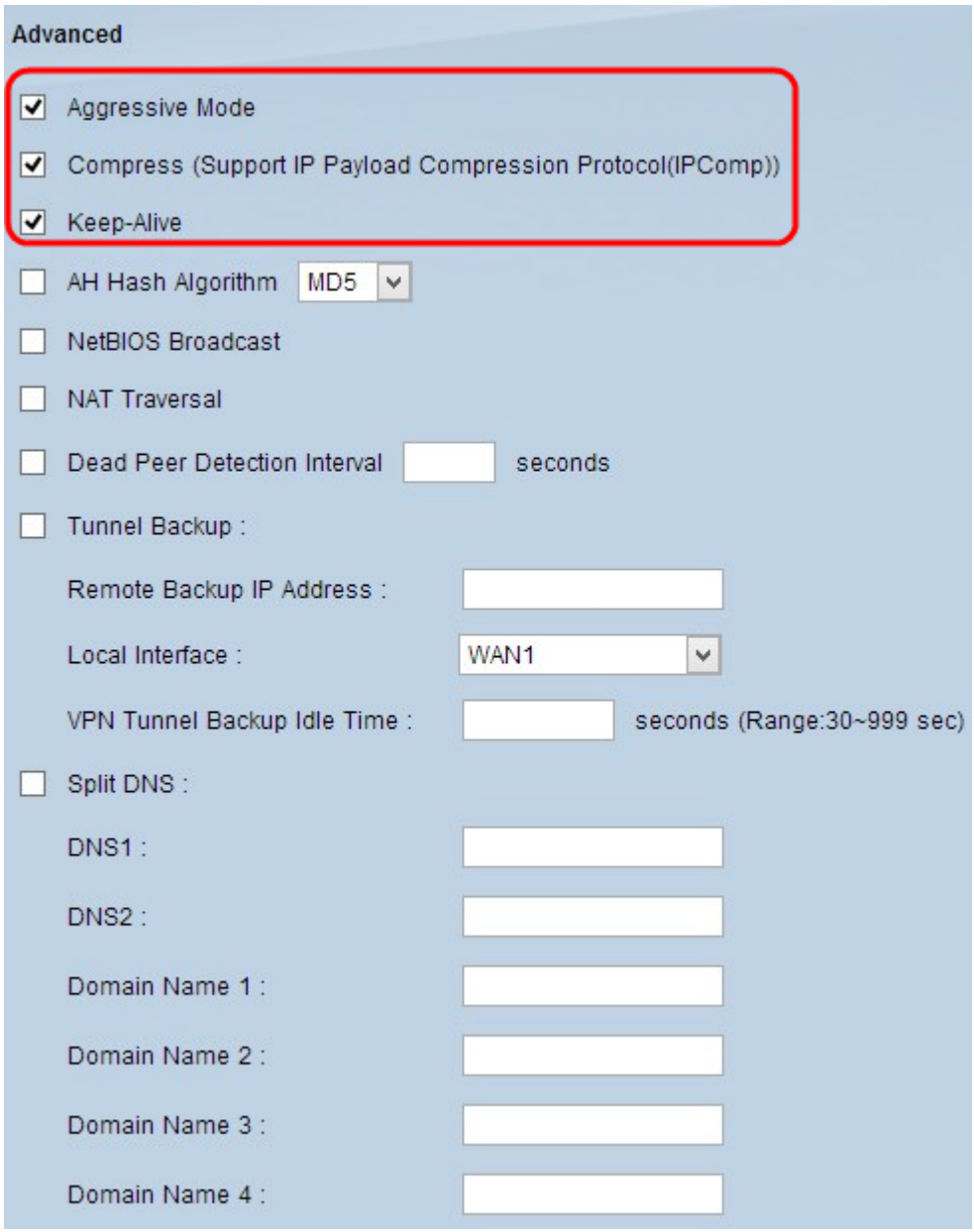
Stap 2. Blader naar beneden naar de sectie *IPSec Setup* en klik op **Advanced +**. Het gebied *Advanced* verschijnt:



Stap 3. Schakel het selectievakje **Aggressive Mode in** als uw netwerksnelheid laag is. Dit ruilt de ID's van de eindpunten van de tunnel in duidelijke tekst tijdens SA-verbinding (fase 1), die minder tijd vergt om te ruilen maar minder veilig is.

Stap 4. Schakel het aanvinkvakje **Compress (Support IP payload Compression Protocol (IPComp)** in als u de grootte van de IP-datagrammen wilt comprimeren. IPComp is een IP-compressieprotocol dat wordt gebruikt om de grootte van IP-datagrammen te comprimeren. IP-compressie is nuttig als de netwerksnelheid laag is en de gebruiker de gegevens snel wil verzenden zonder verlies via het langzame netwerk, maar biedt geen beveiliging.

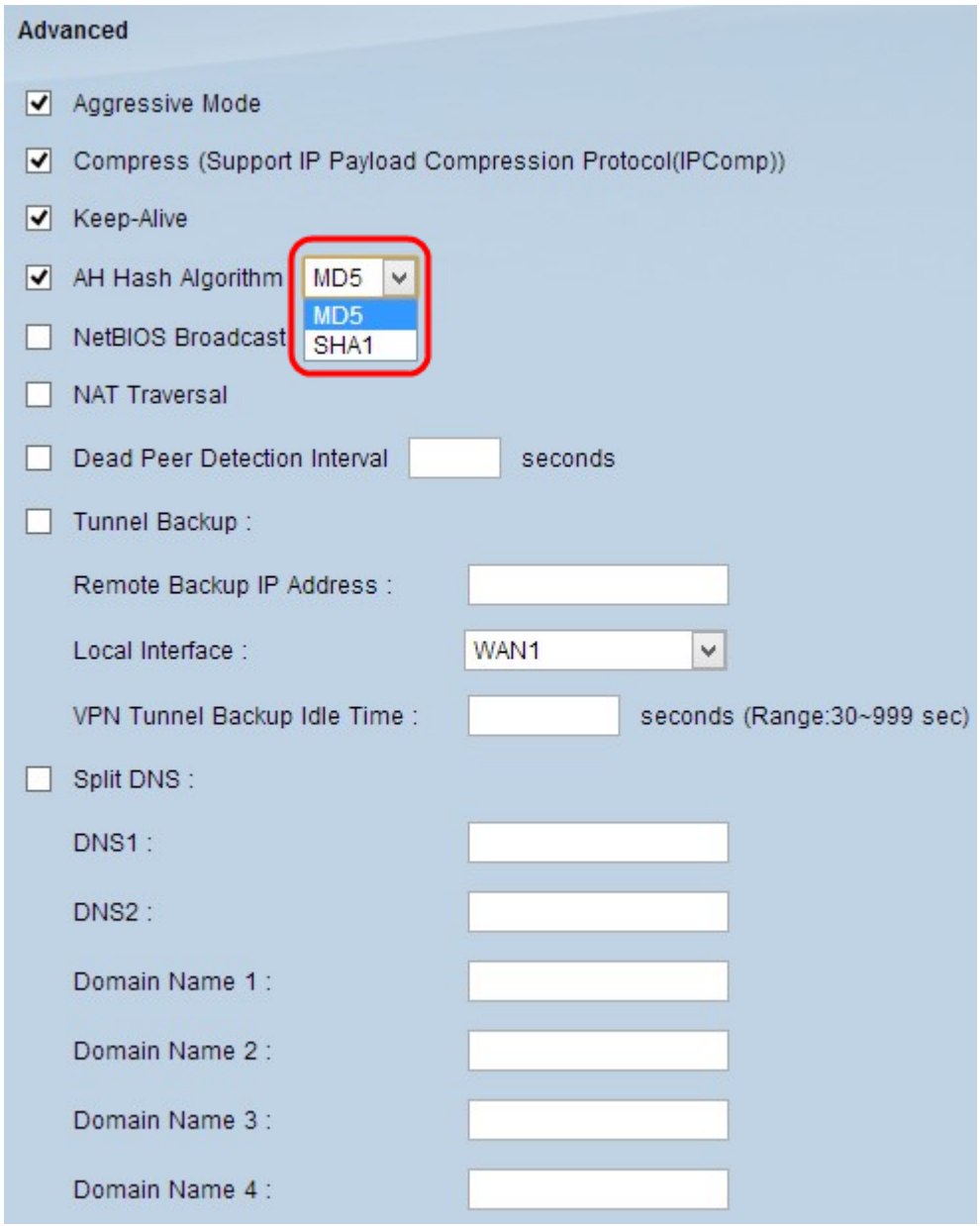
Stap 5. Schakel het aankruisvakje **Keep-Alive in** als u altijd wilt dat de verbinding met de VPN-tunnel actief blijft. Keep-Alive helpt de verbindingen onmiddellijk te herstellen als een verbinding inactief wordt.



Stap 6. Schakel het aanvinkvakje **AH Hash Algorithm in** als u Authenticate Header (AH) wilt inschakelen. AH biedt authenticatie aan de oorspronkelijke gegevens, gegevensintegriteit door middel van checksum en bescherming in de IP-header. De tunnel zou hetzelfde algoritme voor beide kanten moeten hebben.

· MD5 â€" Message Digest Algorithm-5 (MD5) is een hexadecimale hashfunctie met 128 cijfers die de gegevens tegen kwaadaardige aanvallen beschermt door middel van een checksum.

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

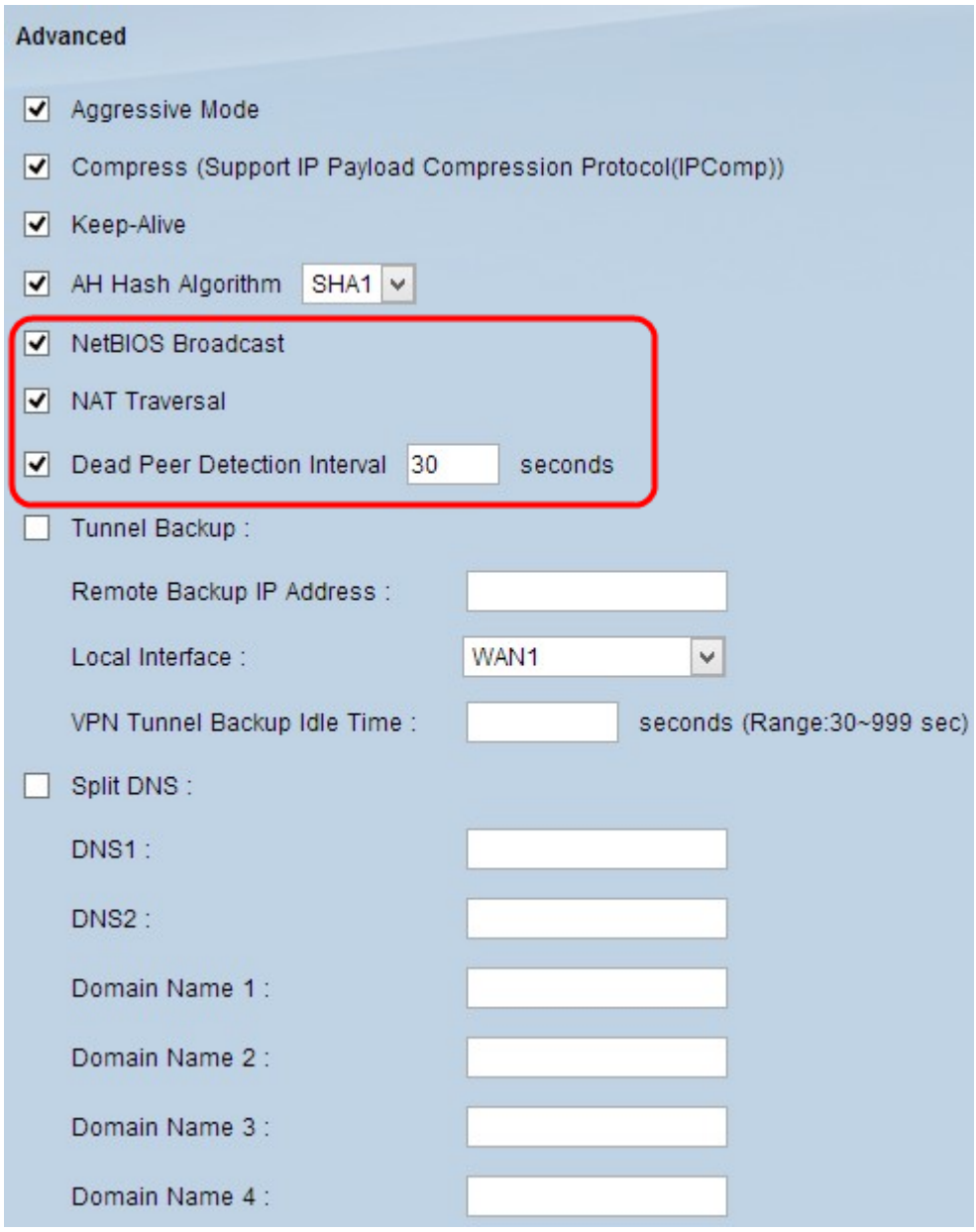


Stap 7. Schakel het aanvinkvakje **NetBIOS Broadcast in** als u niet-routeerbaar verkeer via de VPN-tunnel wilt toestaan. De standaardinstelling is niet ingeschakeld. NetBIOS wordt gebruikt om netwerkbronnen zoals printers en computers in het netwerk te detecteren via bepaalde softwaretoepassingen en Windows-functies zoals Network Neighbourhood.

Stap 8. Schakel het aanvinkvakje **NAT Tradition in** als u via een openbaar IP-adres toegang tot het internet wilt krijgen via uw privé LAN. Als uw VPN-router zich achter een NAT-gateway bevindt, schakelt u deze optie in om NAT-traversatie in te schakelen. Beide uiteinden van de tunnel moeten de zelfde instellingen hebben.

Stap 9. Controleer het **Dead Peer Detection Interval** om de levendigheid van de VPN-tunnel op een periodieke manier door hello of ACK te controleren. Als u dit aanvinkvakje aankruist, voert u het interval (in seconden) in tussen de hello-berichten.

Opmerking: als u het interval voor detectie van dode peers niet controleert, gaat u naar stap 11.

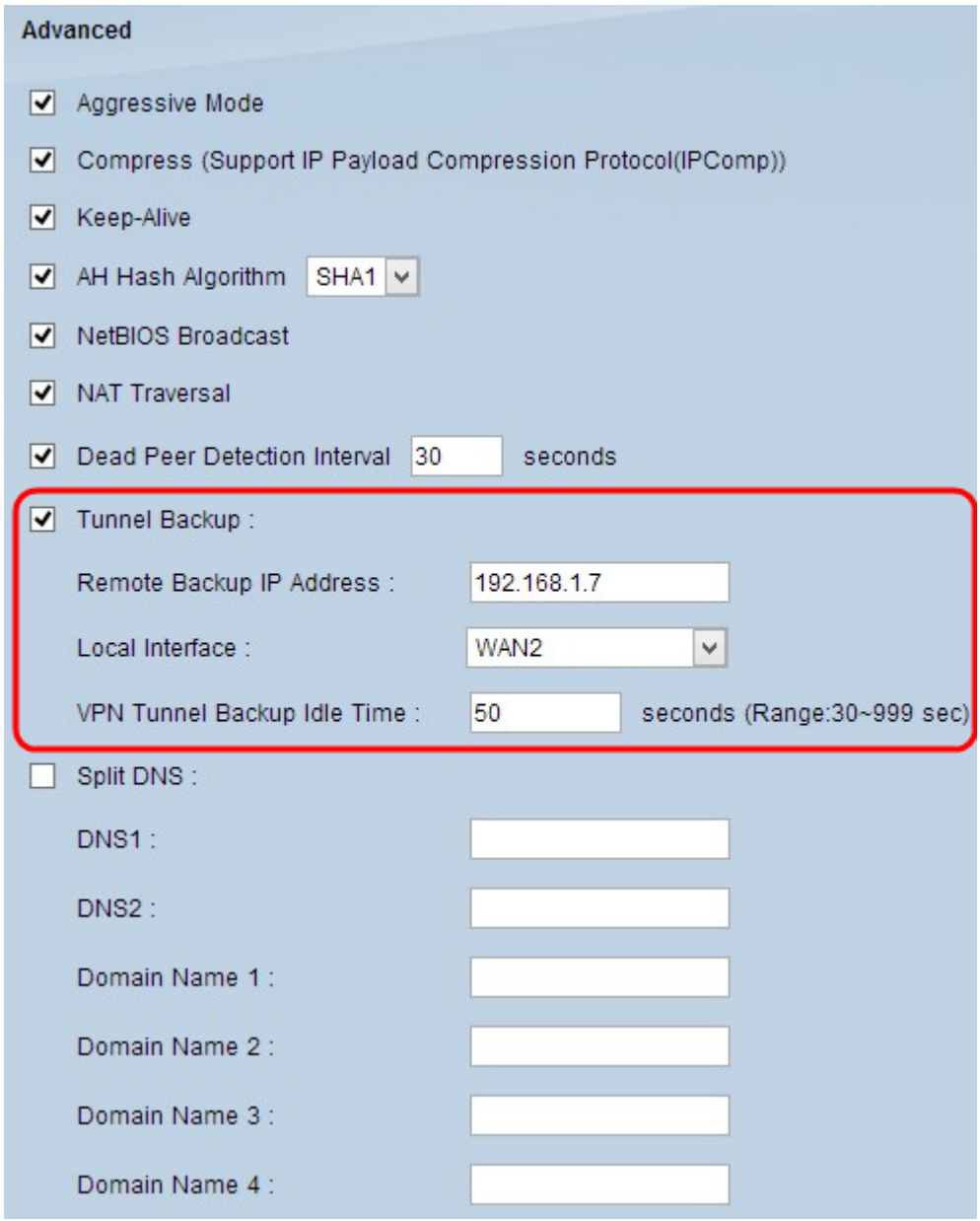


Stap 10. Controleer het aanvinkvakje **Tunnel Backup** om tunnelback-up in te schakelen. Deze optie is alleen beschikbaar als het Dead Peer Detection Interval is ingeschakeld. Met deze functie kan het apparaat de VPN-tunnel opnieuw instellen via een alternatieve lokale WAN-interface of een extern IP-adres.

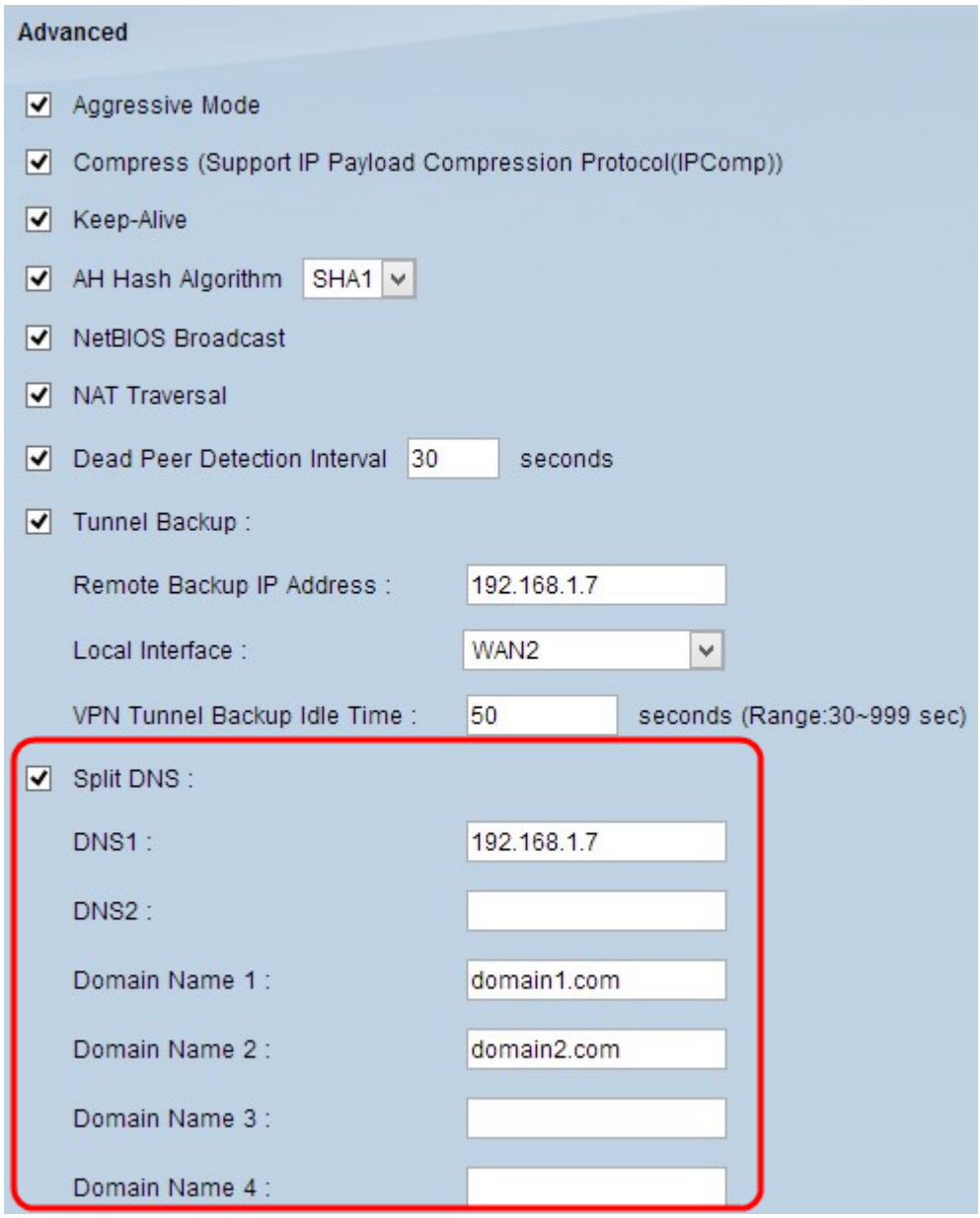
· IP-adres voor externe back-up â€" Voer een ander IP-adres voor de externe gateway in of voer het IP-adres van WAN in dat al was ingesteld voor de externe gateway in dit veld.

· Lokale interface â€" De WAN-interface die wordt gebruikt om de verbinding te herstellen. Kies de gewenste interface uit de vervolgkeuzelijst.

· VPN Tunnel back-up inactiviteitstijd â€" Voer de tijd (in seconden) in die de primaire tunnel moet verbinden voordat de back-uptunnel wordt gebruikt.



Stap 11. Controleer het aankruisvakje **Split DNS** om gesplitste DNS in te schakelen. Split DNS maakt het mogelijk om verzoeken voor specifieke domeinnamen te behandelen door een andere DNS server dan gewoonlijk wordt gebruikt. Wanneer de router een DNS-verzoek van de client ontvangt, controleert het het DNS-verzoek en komt overeen met de domeinnaam en stuurt het verzoek naar die specifieke DNS-server.



Stap 12. Voer in het *DNS1*-veld het IP-adres van de DNS-server in. Als er een andere DNS-server is, voert u het IP-adres van de DNS-server in het veld *DNS2 in*.

Stap 13. Voer in de velden *Domain Name 1* de domeinnamen in via *Domain Name 4*. Verzoeken voor deze domeinnamen worden verwerkt door de DNS-servers die in Stap 12 zijn gespecificeerd.

Stap 14. Klik op **Opslaan** om de wijzigingen op te slaan.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.