Configuration des paramètres avancés du VPN passerelle à passerelle sur les routeurs VPN RV016, RV042, RV042G et RV082

Objectif

Un réseau privé virtuel (VPN) est un réseau privé utilisé pour connecter virtuellement des périphériques de l'utilisateur distant via un réseau public afin d'assurer la sécurité. Plus précisément, une connexion VPN de passerelle à passerelle permet à deux routeurs de se connecter entre eux en toute sécurité et à un client situé à une extrémité de faire logiquement partie du même réseau distant situé à lâ€™autre extrémité. Les données et les ressources peuvent ainsi être partagées plus facilement et en toute sécurité sur Internet. Une configuration identique doit être effectuée des deux côtés de la connexion pour qu'une connexion VPN de passerelle à passerelle soit établie.

La configuration VPN passerelle à passerelle avancée offre la flexibilité de configurer des configurations facultatives pour le tunnel VPN afin d'être plus convivial pour les utilisateurs VPN. Les options avancées ne sont disponibles que pour IKE avec le mode clé prépartagée. Les paramètres avancés doivent être identiques des deux côtés de la connexion VPN.

L'objectif de ce document est de vous montrer comment configurer des paramètres avancés pour le tunnel VPN passerelle à passerelle sur les routeurs VPN RV016, RV042, RV042G et RV082.

Remarque : si vous souhaitez en savoir plus sur la configuration d'un VPN passerelle à passerelle, reportez-vous à l'article *Configuration du VPN passerelle à passerelle sur les routeurs VPN RV016, RV042, RV042G et RV082.*

Périphériques pertinents

â€¢RV016
â€¢RV042
â€¢RV042G
â€¢RV082

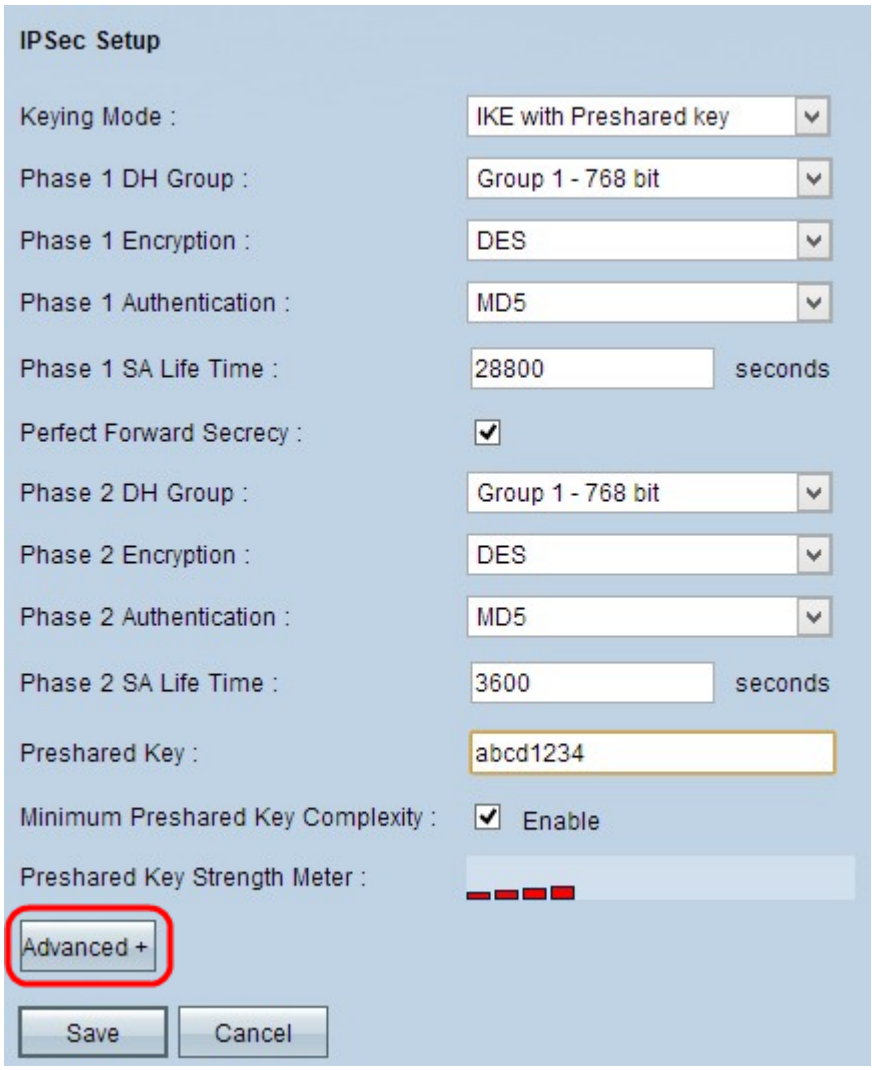
Version du logiciel

â€¢v 4.2.2.08

Configuration des paramètres avancés pour le VPN passerelle à passerelle

Étape 1. Connectez-vous à l'utilitaire de configuration du routeur et choisissez **VPN > Gateway To Gateway**. La page *Gateway To Gateway* s'ouvre :

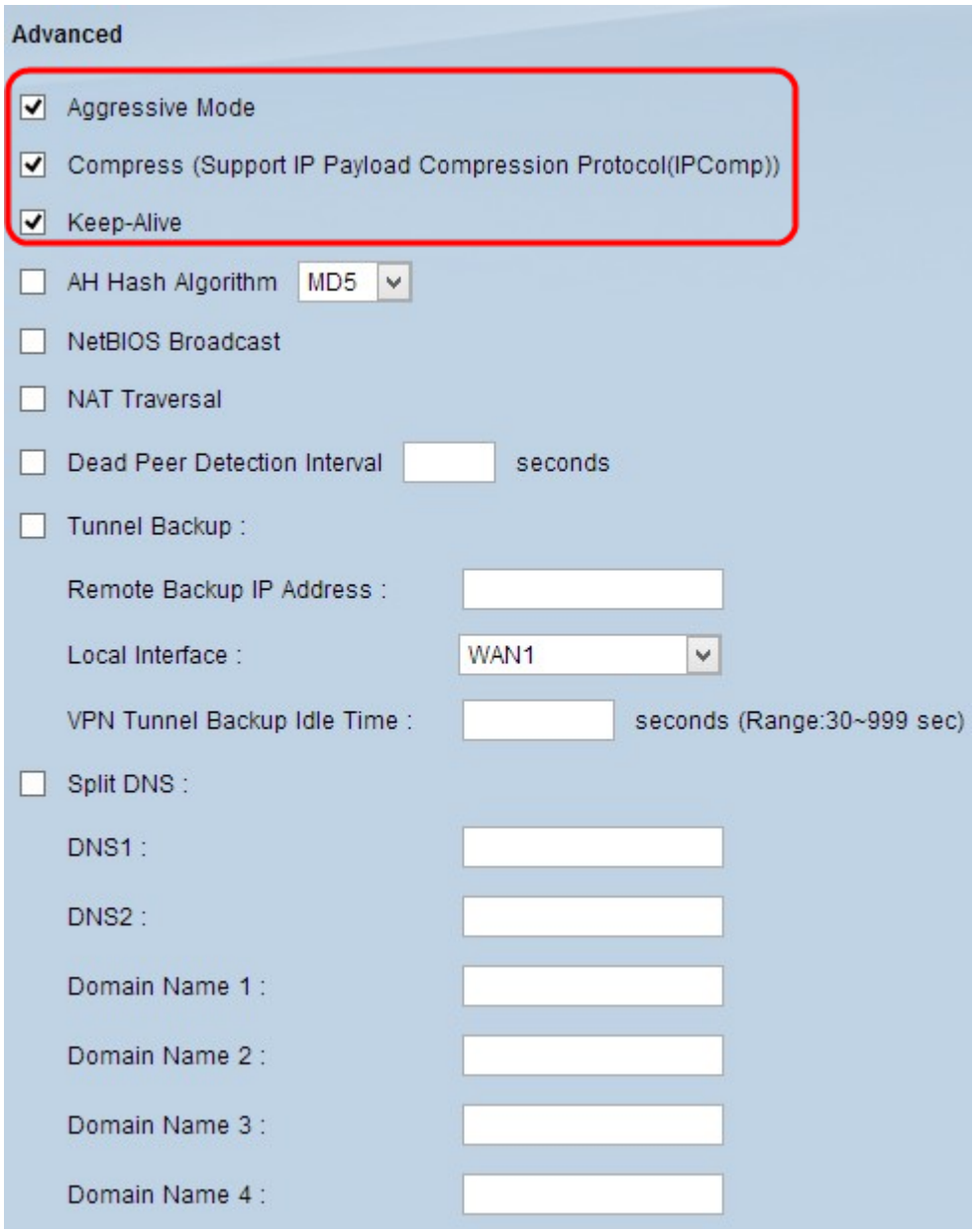
Étape 2. Faites défiler jusqu'à la section *IPSec Setup* et cliquez sur **Advanced +**. La zone *Avancé* apparaît :



Étape 3. Activez la case à cocher Aggressive Mode (mode agressif) si votre débit de réseau est faible. Cela permet dâ€™échanger les ID des points finaux du tunnel en texte clair pendant la connexion de SA (phase 1), ce qui nécessite moins de temps dâ€™échange, mais qui est moins sécurisé.

Étape 4. Cochez la case **Compress (Support IP Payload Compression Protocol (IPComp))** si vous voulez compresser la taille des datagrammes IP. IPComp est un protocole de compression IP utilisé pour compresser la taille des datagrammes IP. La compression IP est utile si la vitesse du réseau est faible et que lâ€™utilisateur souhaite transmettre rapidement les données sans aucune perte via le réseau lent, mais elle nâ€™offre pas de sécurité.

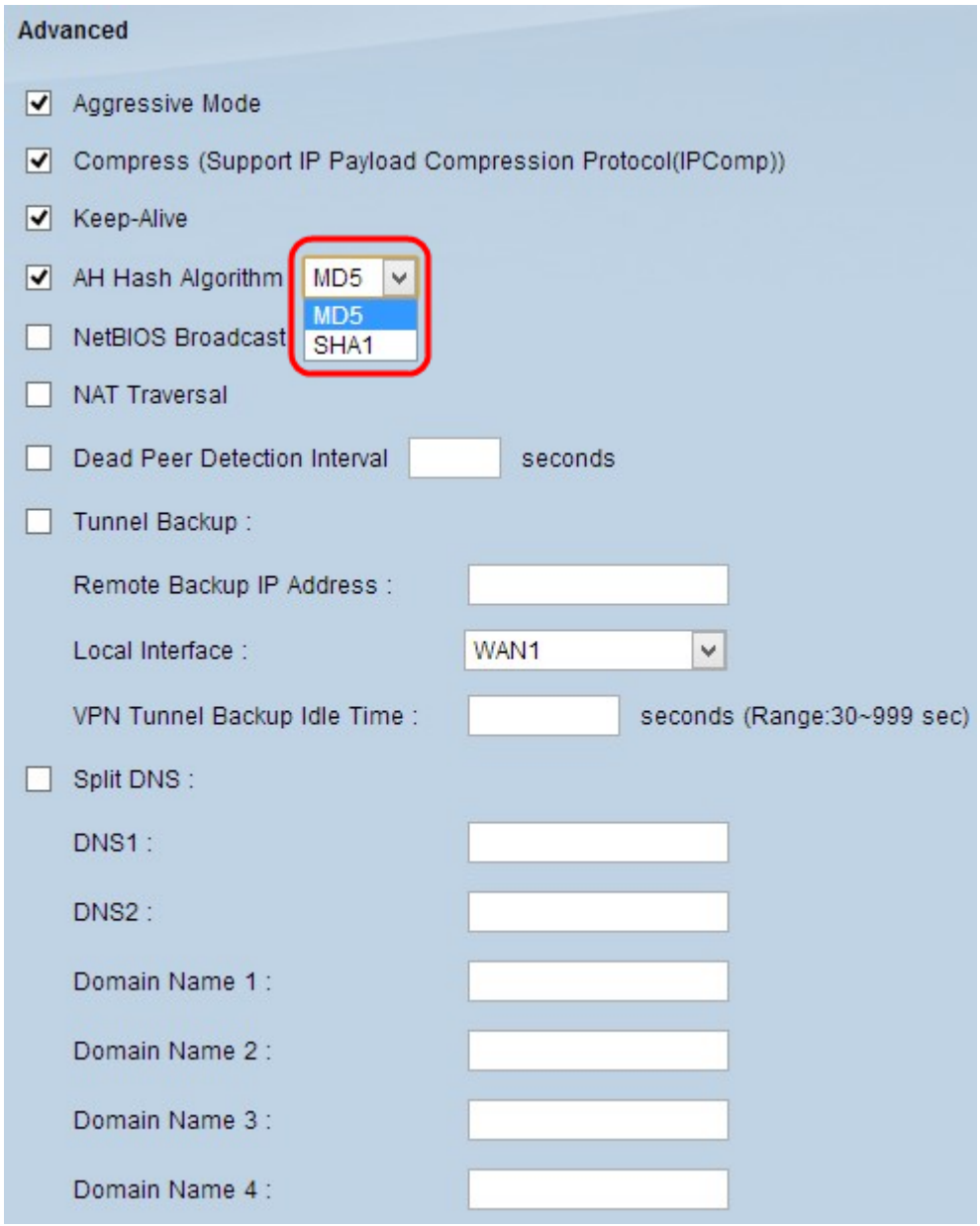
Étape 5. Cochez la case **Keep-Alive** si vous voulez toujours que la connexion du tunnel VPN reste active. Keep-Alive permet de rétablir les connexions immédiatement si une connexion devient inactive.



Étape 6. Activez la case à cocher de lâ€™algorithme de hachage AH (AH Hash Algorithm) si vous souhaitez activer lâ€™en-tête dâ€™authentification (Authenticate Header, AH). AH permet dâ€™authentifier les données dâ€™origine, lâ€™intégrité des données via la somme de contrôle et la protection dans lâ€™en-tête IP. Le tunnel doit avoir le même algorithme pour les deux côtés.

· MD5 â€” Message Digest Algorithm-5 (MD5) est une fonction de hachage hexadécimal à 128 chiffres qui protège les données contre les attaques malveillantes par le calcul de la somme de contrôle.

· SHA1 : l'algorithme de hachage sécurisé version 1 (SHA1) est une fonction de hachage 160 bits plus sécurisée que MD5, mais dont le calcul prend plus de temps.

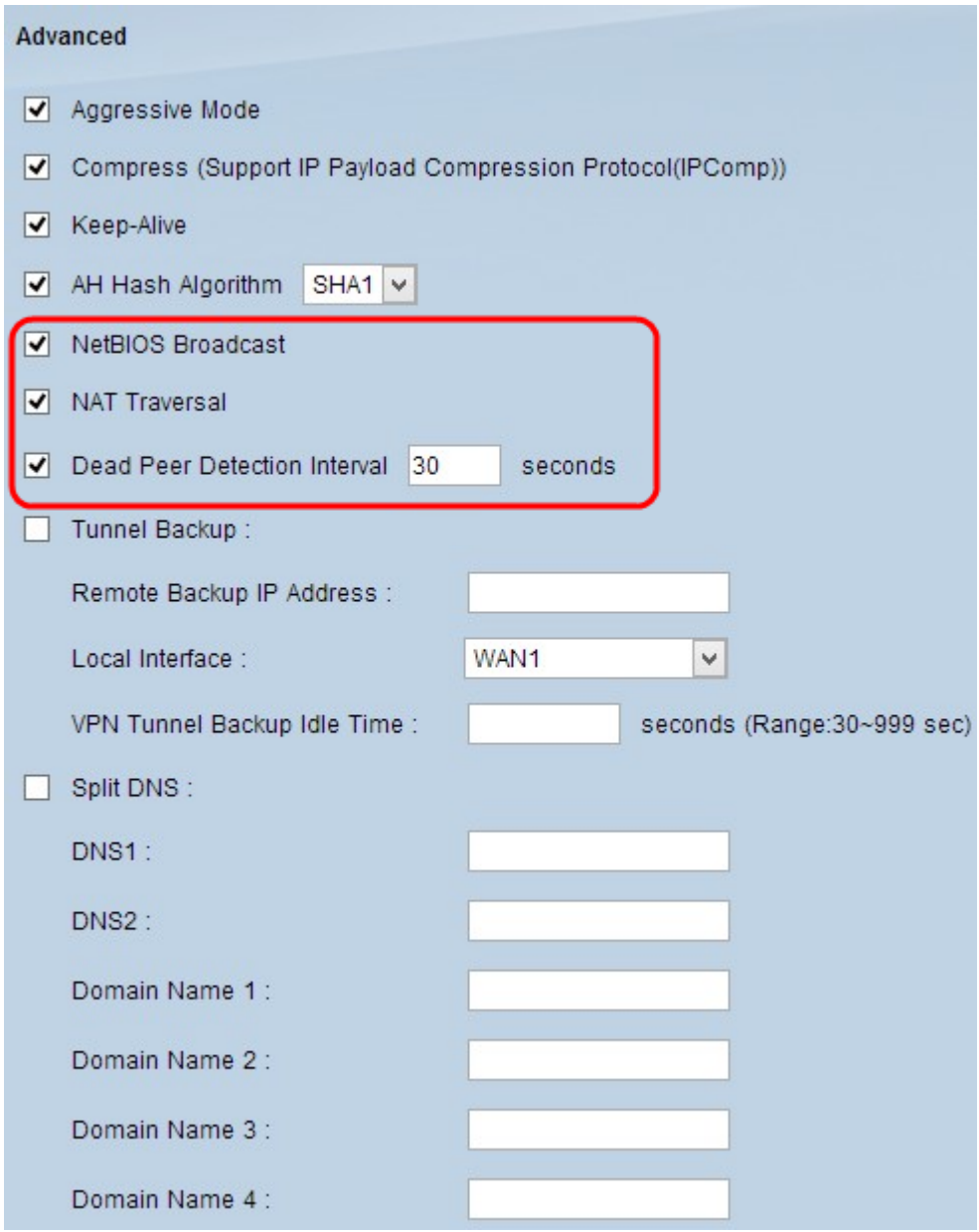


Étape 7. Cochez la case **NetBIOS Broadcast** si vous voulez autoriser le trafic non routable à travers le tunnel VPN. La case est décochée par défaut. NetBIOS est utilisé pour détecter les ressources réseau telles que les imprimantes et les ordinateurs du réseau par le biais de certaines applications logicielles et de fonctionnalités Windows telles que le Voisinage réseau.

Étape 8. Cochez la case **NAT Traversal** si vous voulez accéder à Internet depuis votre LAN privé via une adresse IP publique. Si votre routeur VPN se trouve derrière une passerelle NAT, cochez cette case pour activer la traversée NAT. Les deux extrémités du tunnel doivent avoir les mêmes paramètres.

Étape 9. Cochez la case Dead Peer Detection Interval (intervalle de détection des homologues inactifs) pour vérifier lâ€™activité du tunnel VPN via des messages Hello ou ACK, de manière régulière. Si vous cochez cette case, entrez l'intervalle (en secondes) entre les messages Hello.

Remarque : si vous ne cochez pas la case Intervalle de détection des homologues morts, passez à l'étape 11.

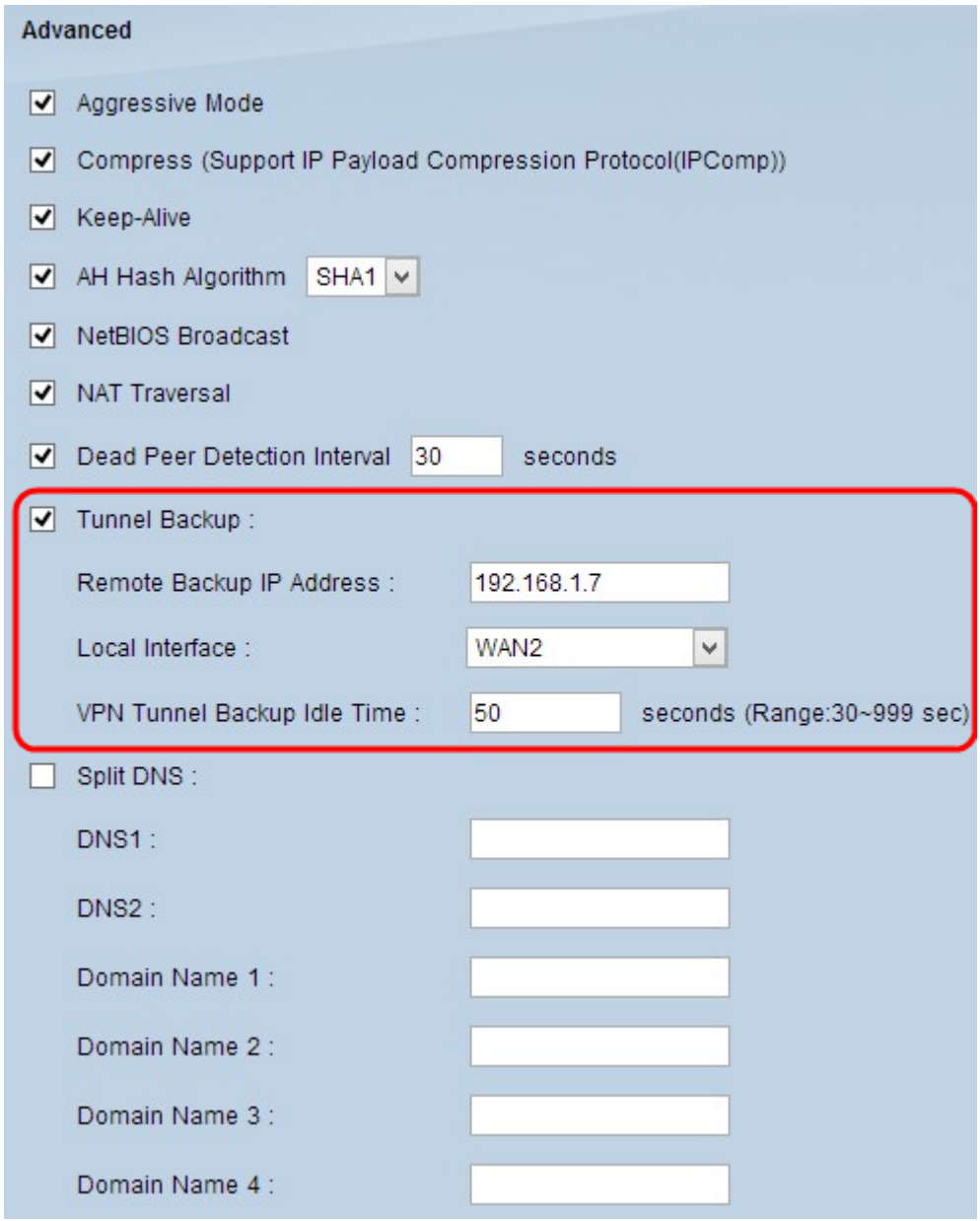


Étape 10. Cochez la case **Tunnel Backup** pour activer la sauvegarde de tunnel. Cette fonctionnalité n'est disponible que lorsque l'intervalle de détection des homologues morts a été vérifié. Cette fonctionnalité permet au périphérique de rétablir le tunnel VPN via une autre interface WAN locale ou une adresse IP distante.

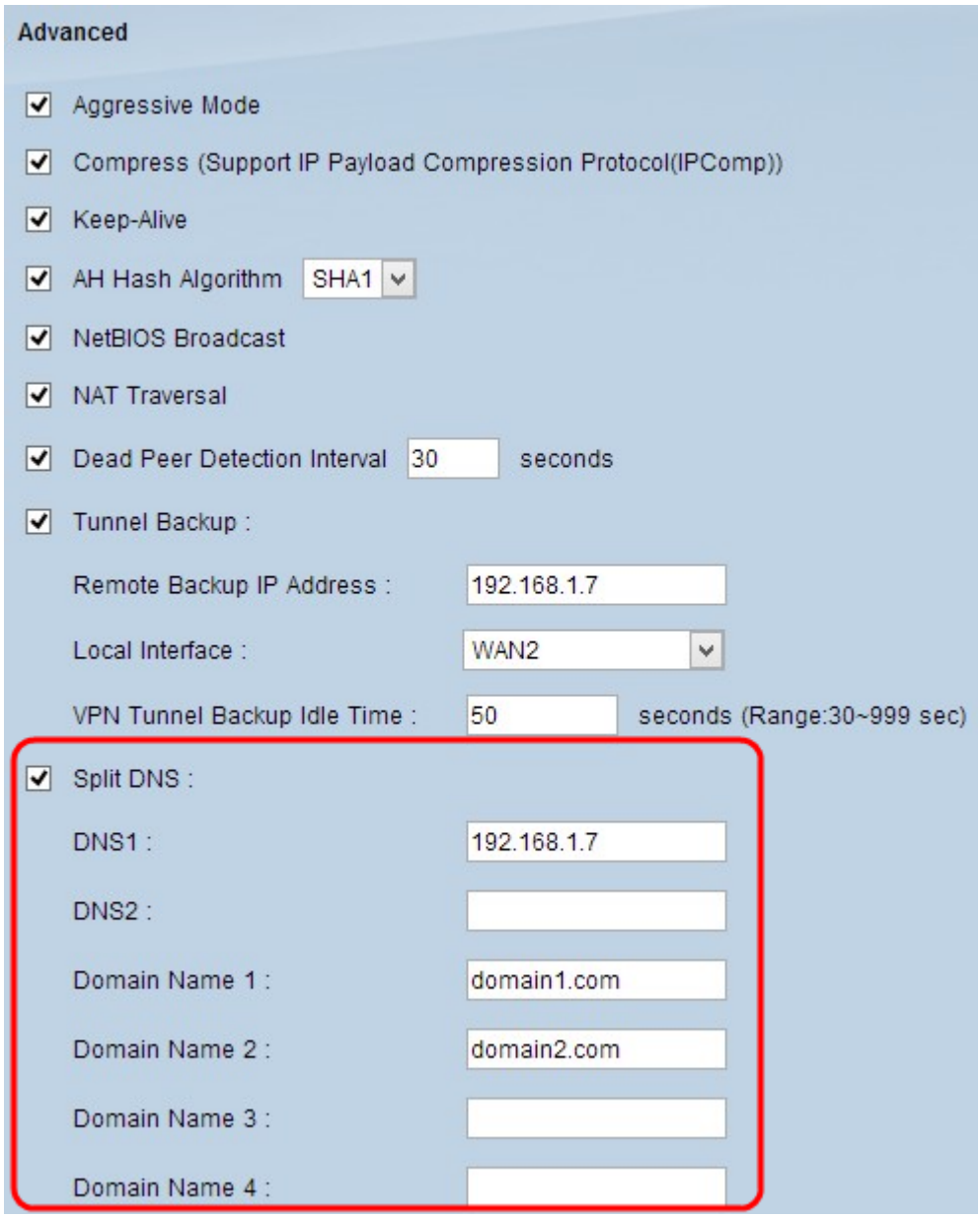
· Remote Backup IP Address : saisissez une autre adresse IP pour la passerelle distante ou saisissez l'adresse IP WAN déjà définie pour la passerelle distante dans ce champ.

· Local Interface : interface WAN utilisée pour rétablir la connexion. Sélectionnez l'interface souhaitée dans la liste déroulante.

· VPN Tunnel Backup Idle Time : saisissez la durée (en secondes) de connexion du tunnel principal avant l'utilisation du tunnel de secours.



Étape 11. Cochez la case **Split DNS** pour activer le DNS partagé. Le DNS fractionné permet aux demandes de noms de domaine spécifiés d'être traitées par un serveur DNS différent de celui habituellement utilisé. Lorsque le routeur reçoit une requête DNS du client, il vérifie la requête DNS et la fait correspondre au nom de domaine, puis envoie la requête à ce serveur DNS spécifique.



Étape 12. Saisissez l'adresse IP du serveur DNS dans le champ *DNS1*. S'il y a un autre serveur DNS, entrez l'adresse IP du serveur DNS dans le champ *DNS2*.

Étape 13. Saisissez les noms de domaine dans les champs *Domain Name 1* à *Domain Name 4*. Les demandes de ces noms de domaine seront traitées par les serveurs DNS spécifiés à l'étape 12.

Étape 14. Cliquez sur **Save** pour enregistrer vos modifications.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.