# Configurer un tunnel dâ€™accès à distance (client vers passerelle) pour les clients VPN sur les routeurs VPN RV016, RV042, RV042G et RV082

## Objectif

Cet article explique comment configurer le tunnel VPN dâ€™accès à distance (Virtual Private Network) entre le client et la passerelle sur les routeurs VPN RV016, RV042, RV042G et RV082 à lâ€™aide dâ€™un logiciel client VPN tiers en tant que client GreenBow ou dispositif de suivi VPN.

## Introduction

Un VPN est un réseau privé qui est utilisé pour connecter virtuellement des périphériques de lâ€™utilisateur distant via le réseau public pour en assurer la sécurité. Le tunnel dâ€™accès à distance VPN est le processus utilisé pour configurer un VPN entre un ordinateur client et un réseau. Le client est configuré dans le bureau ou lâ€™ordinateur portable des utilisateurs via le logiciel client VPN. Il permet aux utilisateurs de se connecter en toute sécurité au réseau à distance. La connexion VPN client à passerelle est utile pour permettre aux employés distants de se connecter au réseau de lâ€™entreprise à distance et de manière sécurisée.

## Périphériques pertinents

- RV016
- RV042
- RV042G
- RV082

## Version du logiciel

- v 4.2.2.08

## Configuration dâ€™un tunnel VPN

Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez **VPN > Client to Gateway.** La *page Client to Gateway sâ€™ouvre :*


## Ajouter un nouveau tunnel

Étape 1. Sélectionnez la case d'option appropriée en fonction du type de tunnel que vous souhaitez ajouter.

- Tunnel : représente un tunnel pour un seul utilisateur distant.
- Group VPN : représente un tunnel pour un groupe dâ€™utilisateurs distants.


Le numéro de tunnel (Tunnel Number) est un champ généré automatiquement qui affiche le numéro du tunnel.

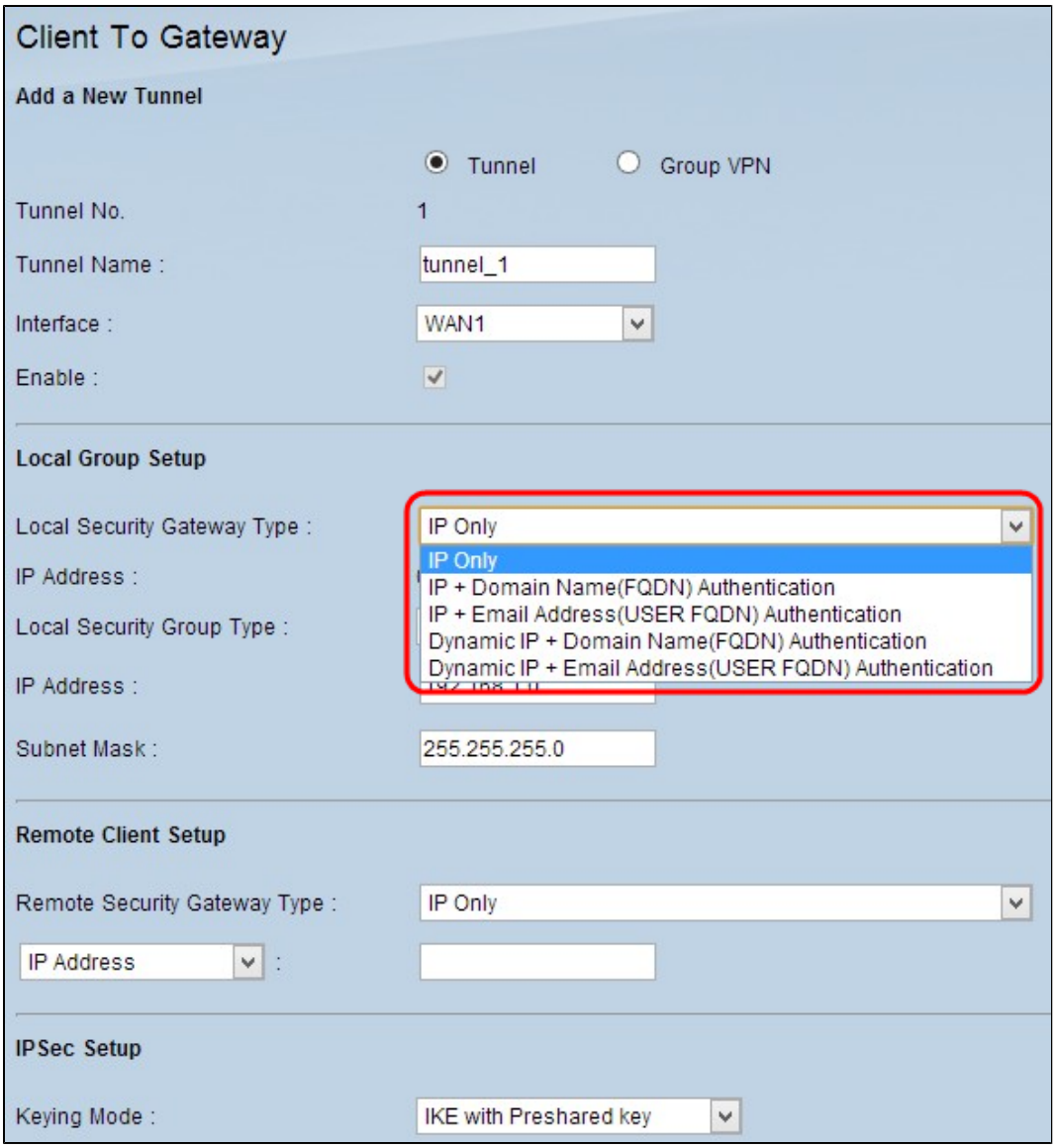

Étape 2. Entrez un nom pour le tunnel dans le champ Tunnel Name.

Étape 3. Sélectionnez l'interface WAN appropriée à utiliser pour le tunnel VPN dans la liste déroulante Interface.

Étape 4. (Facultatif) Pour activer le VPN, cochez la case dans le champ Enable (activer). Par défaut, elle est toujours cochée.

## Configuration du groupe local

Étape 1. Choisissez la méthode d'identification de routeur appropriée pour établir un tunnel VPN dans la liste déroulante *Local Security Gateway*. Ignorez cette étape si vous avez choisi le VPN de groupe à *lâ€™étape 1 de* la section Ajouter un nouveau tunnel.



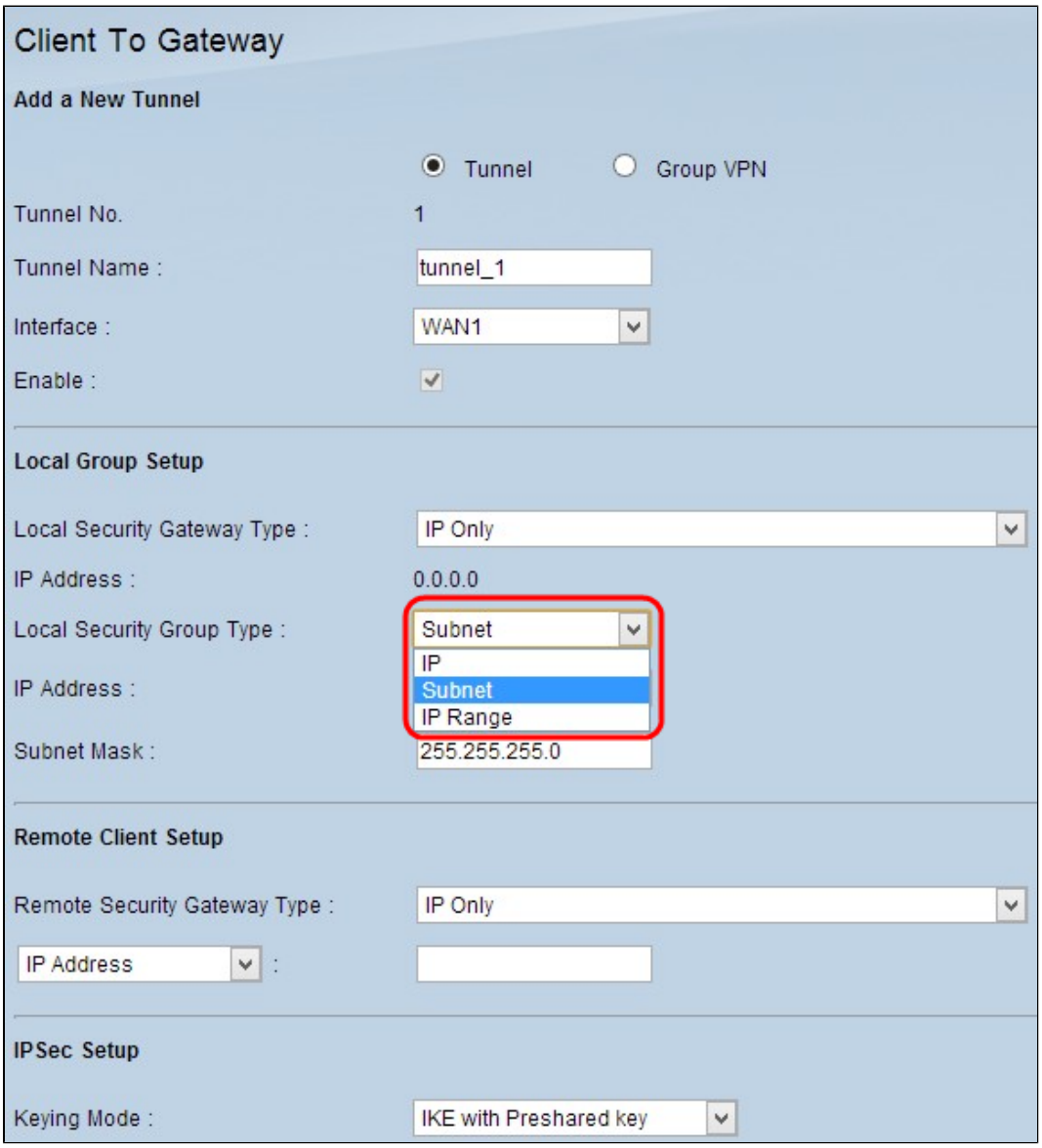

- IP Only : lâ€™accès au tunnel est possible via une adresse IP WAN statique. Vous pouvez sélectionner cette option uniquement si le routeur dispose dâ€™une adresse IP WAN statique. Lâ€™adresse IP WAN statique apparaît automatiquement.
- IP + Domain Name(FQDN) Authentication : il est possible dâ€™accéder au tunnel par le biais dâ€™une adresse IP statique et dâ€™un domaine de nom de domaine complet (FQDN) enregistré. Lâ€™adresse IP WAN statique est un champ généré automatiquement.
- IP + E-mail Address(USER FQDN) Authentication : lâ€™accès au tunnel est possible via une adresse IP statique et une adresse courriel. Lâ€™adresse IP WAN statique est un champ généré automatiquement.
- Authentification Dynamic IP + nom de domaine (FQDN) : lâ€™accès au tunnel est possible via une adresse IP dynamique et un domaine enregistré.
- Dynamic IP + E-mail Address(USER FQDN) Authentication : lâ€™accès au tunnel est possible via une adresse IP dynamique et une adresse courriel.

Étape 2. Entrez le nom du domaine complet enregistré dans le champ Domain Name si vous choisissez *IP + Domain Name (FQDN) Authentication* ou *Dynamic IP + Domain Name (FQDN) Authentication* à l'étape 1.

Étape 3. Saisissez l'adresse e-mail dans le champ Email Address (Adresse e-mail) si vous choisissez *IP + E-mail Address (USER FQDN) Authentication (Authentification IP + adresse e-mail dynamique)* ou *Dynamic IP + E-mail Address (USER FQDN) Authentication (Authentification IP + adresse e-mail dynamique)* à l'étape 1.

Étape 4. Choisissez l'utilisateur ou le groupe d'utilisateurs LAN local approprié qui peut accéder au tunnel VPN dans la liste déroulante *Local Security Group*. La valeur par défaut est « Subnet » (sous-réseau).

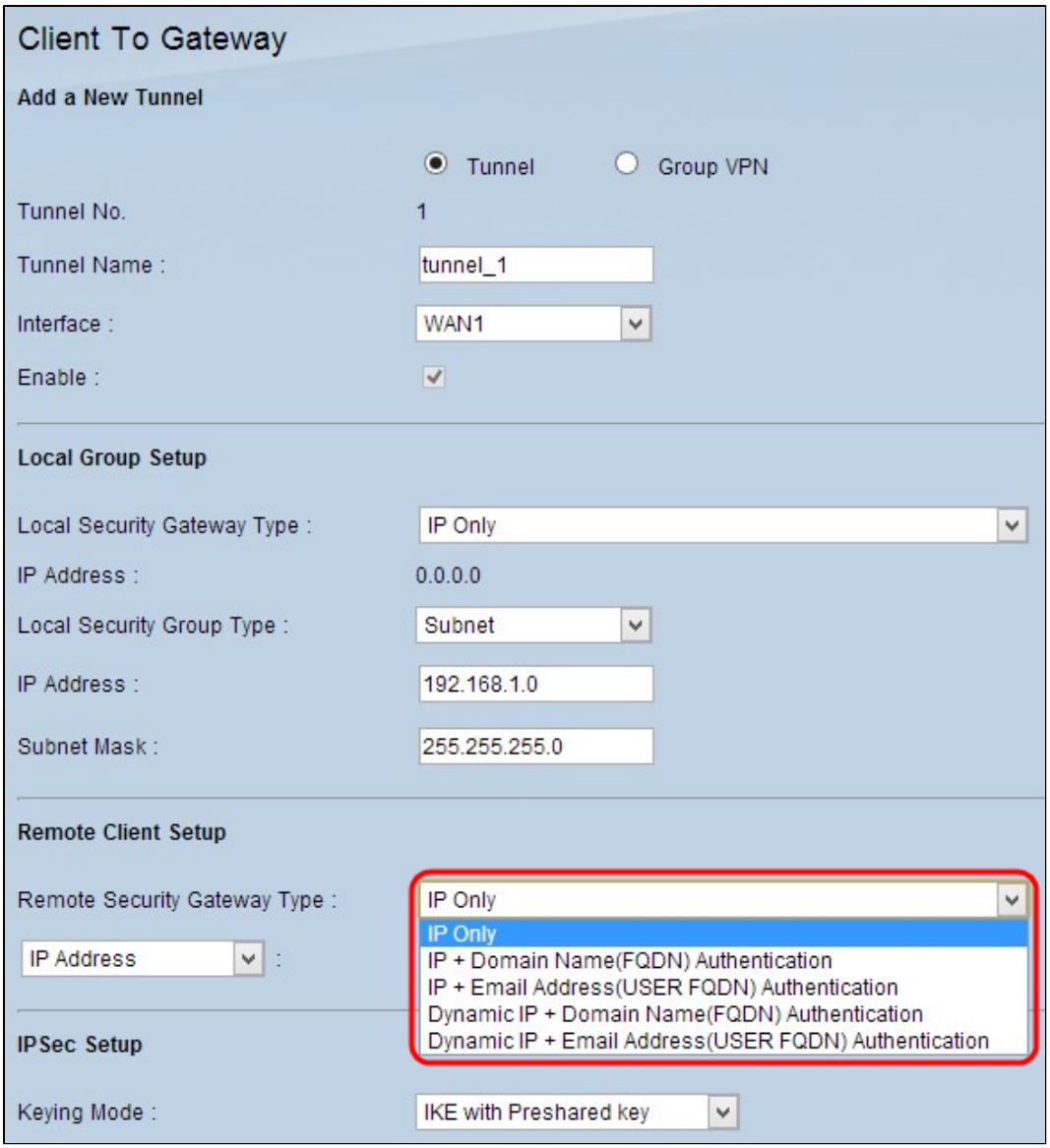
- IP : un seul périphérique LAN spécifique peut accéder au tunnel. Si vous choisissez cette option, saisissez lâ€™adresse IP de lâ€™appareil LAN dans le champ IP Address (adresse IP). Lâ€™adresse IP par défaut est 192.168.1.0.
- Subnet : tous les périphériques LAN dâ€™un sous-réseau spécifique peuvent accéder au tunnel. Si vous choisissez cette option, saisissez lâ€™adresse IP et le masque de sous-réseau des appareils LAN dans les champs IP Address (adresse IP) et Subnet Mask (masque de sous-réseau) respectivement. Le masque par défaut est 255.255.255.0.
- IP Range : un éventail dâ€™appareils LAN peuvent accéder au tunnel. Si vous choisissez cette option, saisissez lâ€™adresse IP de début et de fin respectivement dans les champs Begin IP (adresse IP de début) et End IP (adresse IP de fin). La plage par défaut est comprise entre 192.168.1.0 et 192.168.1.254.




Étape 5. Cliquez sur **Save pour enregistrer les paramètres.**

## Configuration du client distant

Étape 1. Si vous choisissez Tunnel, sélectionnez la méthode dâ€™identification du client appropriée pour établir un tunnel VPN dans la liste déroulante *Remote Security Gateway Type (type de passerelle de sécurité à distance)*. La valeur par défaut est IP Only (IP seulement). Ignorez cette étape si le VPN de groupe a été choisi à lâ€™étape 1 de la section pour ajouter un nouveau tunnel (*Add A New Tunnel* ).




- IP Only : lâ€™accès au tunnel est possible via lâ€™IP WAN statique du client seulement. Vous devez connaître lâ€™adresse IP WAN statique du client pour utiliser cette option.
- IP + Domain Name(FQDN) Authentication : il est possible dâ€™accéder au tunnel par le biais dâ€™une adresse IP statique du client et dâ€™un domaine enregistré.
- IP + E-mail Address(USER FQDN) Authentication : lâ€™accès au tunnel est possible via lâ€™adresse IP statique du client et une adresse courriel.
- Dynamic IP + Domain Name(FQDN) Authentication : il est possible dâ€™accéder au tunnel par le biais dâ€™une adresse IP dynamique du client et dâ€™un domaine enregistré.
- Dynamic IP + E-mail Address(USER FQDN) Authentication : lâ€™accès au tunnel est possible via lâ€™adresse IP dynamique du client et une adresse courriel.

Étape 2. Entrez l'adresse IP du client distant dans le champ *IP Address* si vous avez choisi *IP Only*, *IP + Domain Name (FQDN) ou IP + E-mail Address (User FQDN) Authentication* à l'étape 1.

Étape 3. Choisissez l'option appropriée dans la liste déroulante pour entrer l'adresse IP si vous la connaissez ou résolvez l'adresse IP à partir du serveur DNS si vous choisissez *IP Only* ou *IP + Domain Name (FQDN) Authentication* ou *IP + E-mail Address (USER FQDN) Authentication* à l'étape 1.

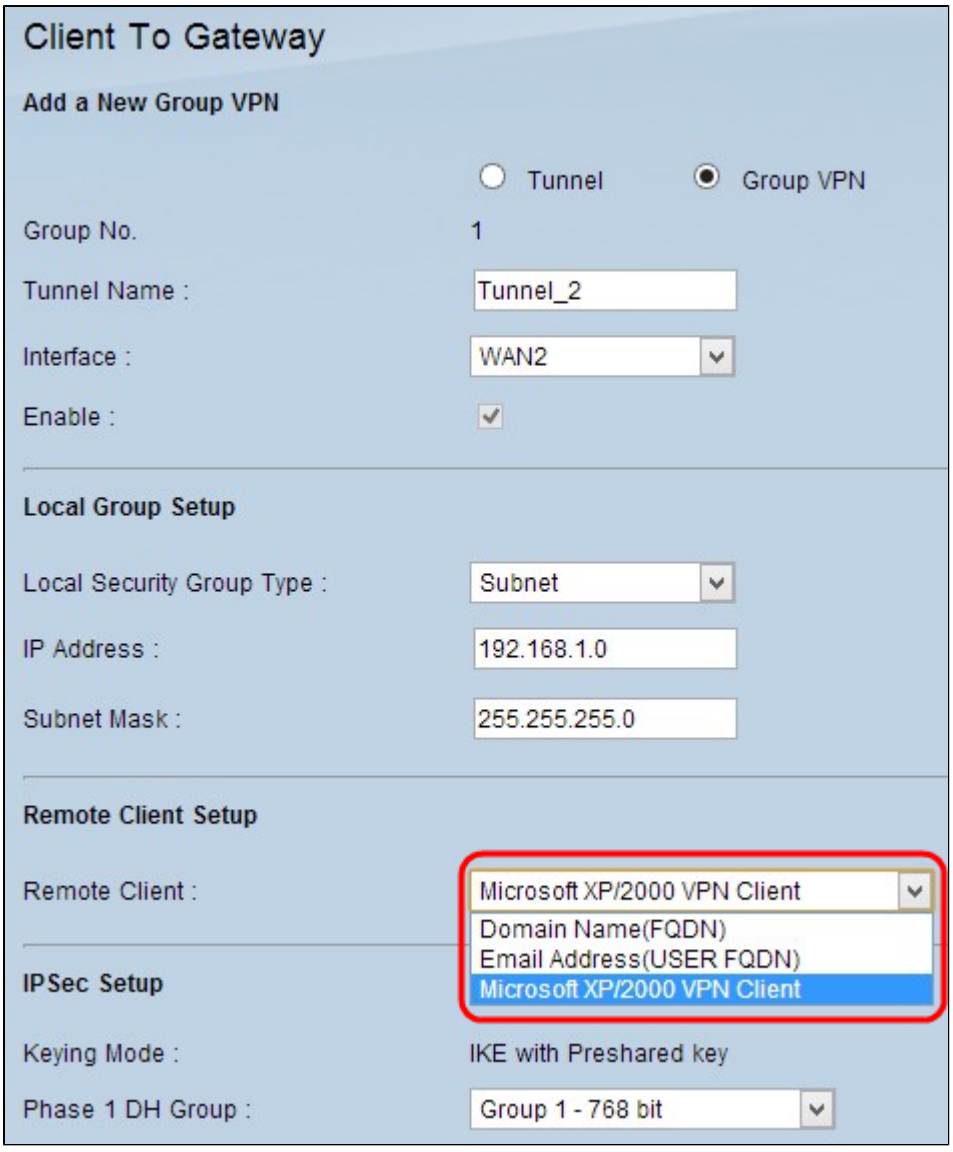
- IP Address : représente lâ€™adresse IP statique du client distant. Saisissez lâ€™adresse IP statique dans le champ.
- IP by DNS Resolved : représente le nom de domaine de lâ€™adresse IP qui récupère automatiquement lâ€™adresse IP via le serveur DNS local si vous ne connaissez pas lâ€™adresse IP statique du client distant. Entrez le nom de domaine de lâ€™adresse IP dans le champ.

Étape 4. Entrez le nom de domaine de l'adresse IP dans le champ Domain name si vous choisissez *IP + Domain Name (FQDN) Authentication* ou *Dynamic IP + Domain Name (FQDN) Authentication* à l'étape 1.

Étape 5. Saisissez l'adresse e-mail dans le champ Email Address (Adresse e-mail) si vous choisissez *IP + E-mail Address (USER FQDN) Authentication (Authentification IP + Adresse e-mail dynamique)* ou *Dynamic IP + E-mail Address (USER FQDN) Authentication (Authentification IP + Adresse e-mail dynamique)* à l'étape 1.

Étape 6. Si vous choisissez Group, sélectionnez le type de client distant approprié dans la liste déroulante de client distant (*Remote Client).* Ignorez cette étape si le VPN de tunnel a été choisi à lâ€™étape 1 de la section pour ajouter un nouveau tunnel (*Add A New Tunnel* ).

- Domain Name (FQDN) Authentication : il est possible dâ€™accéder au tunnel par le biais dâ€™un domaine enregistré. Si vous choisissez cette option, saisissez le nom du domaine enregistré dans le champ Domain Name (nom de domaine).
- Adresse e-mail (USER FQDN) : l'accès au tunnel est possible via l'adresse e-mail du client. Si vous choisissez cette option, saisissez lâ€™adresse courriel dans le champ Email Address.
- Microsoft XP/2000 VPN Client : lâ€™accès au tunnel est possible via le logiciel Windows Microsoft XP ou Microsoft 2000. Les utilisateurs distants disposant du logiciel client VPN de Microsoft peuvent accéder au tunnel via le logiciel.




Étape 7. Cliquez sur **Save pour enregistrer les paramètres.**

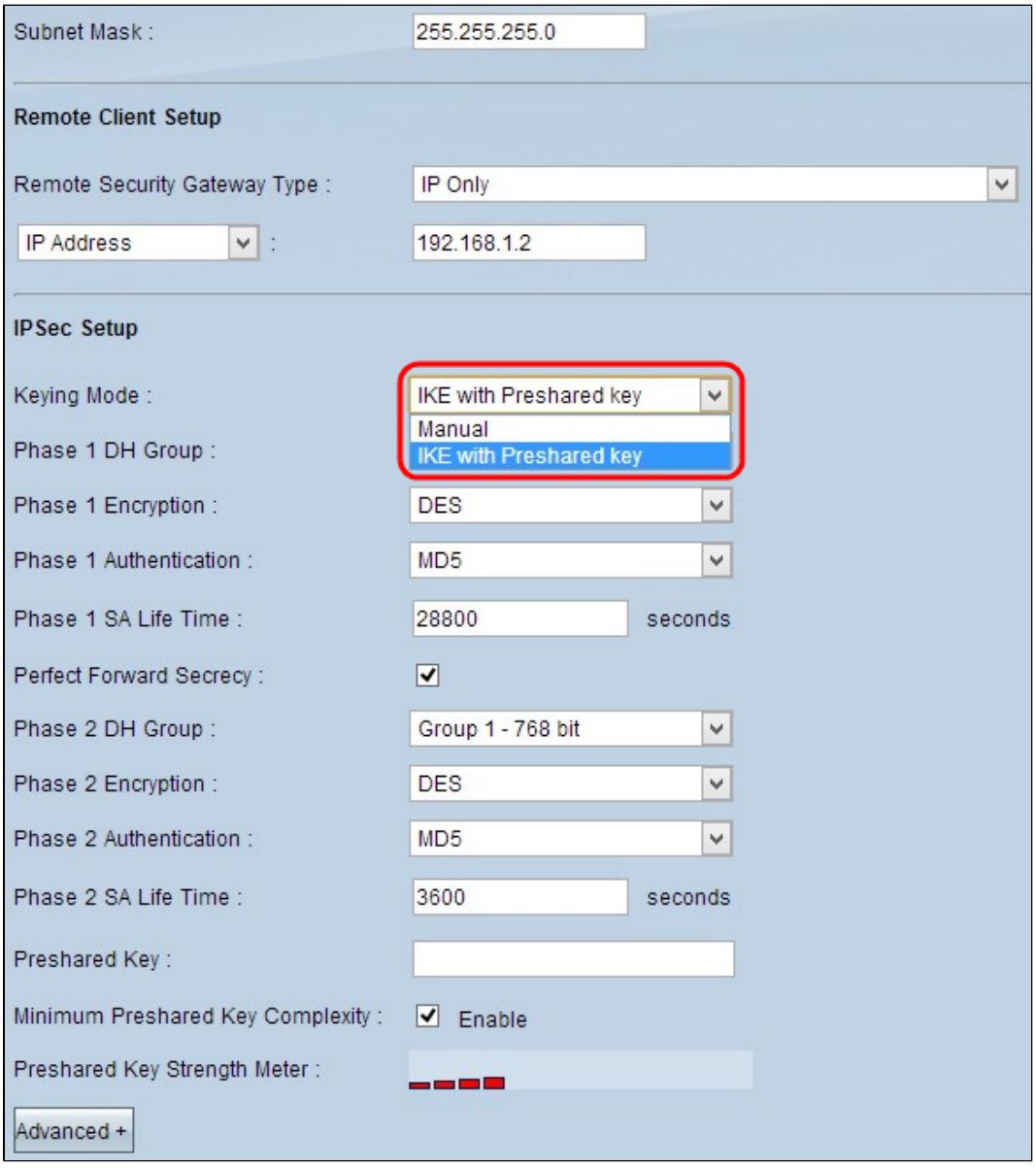
## Configuration IPSec

Le protocole IPSec (Internet Protocol Security) est un protocole de sécurité pour les couches Internet qui offre une sécurité de bout en bout via lâ€™authentification et le chiffrement pendant toute session de communication.

**Remarque :** les deux extrémités du VPN doivent disposer des mêmes méthodes de cryptage, de décryptage et d'authentification pour que l'IPSec fonctionne. La clé de secret de transfert parfait doit également être identique des deux côtés du tunnel.

Étape 1. Choisissez le mode de gestion des clés approprié pour garantir la sécurité dans la liste déroulante *Keying Mode*. Le mode par défaut *IKE with Preshared key*.

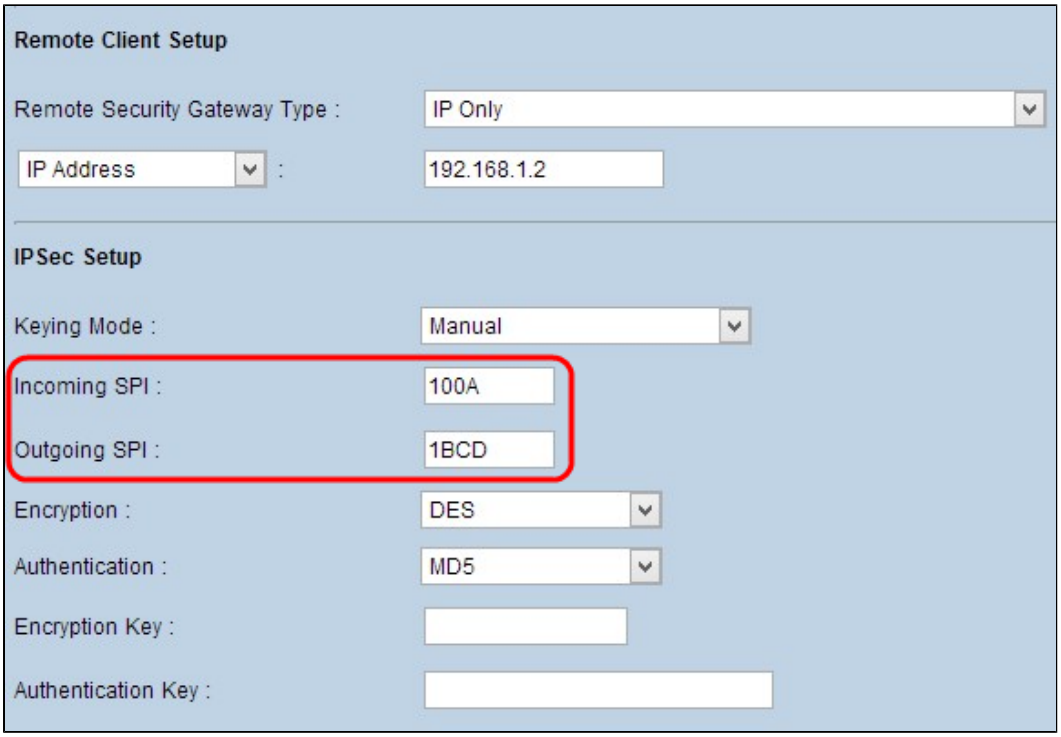
- Manuel : il sâ€™agit dâ€™un mode de sécurité personnalisé qui permet de générer soi-même une nouvelle clé de sécurité et dâ€™éviter toute négociation avec la clé. Il est conseillé dâ€™utiliser ce mode pendant un dépannage et dans des petits environnements statiques. Si vous sélectionnez le VPN de groupe à lâ€™étape 1 dans la section pour ajouter un nouveau tunnel (Add A New Tunnel), cette option est désactivée.
- IKE with Preshared key : le protocole IKE (Internet Key Exchange) est utilisé pour générer et échanger automatiquement une clé prépartagée afin dâ€™établir lâ€™authentification des communications pour le tunnel.




**Configuration manuelle du mode de gestion de clés**

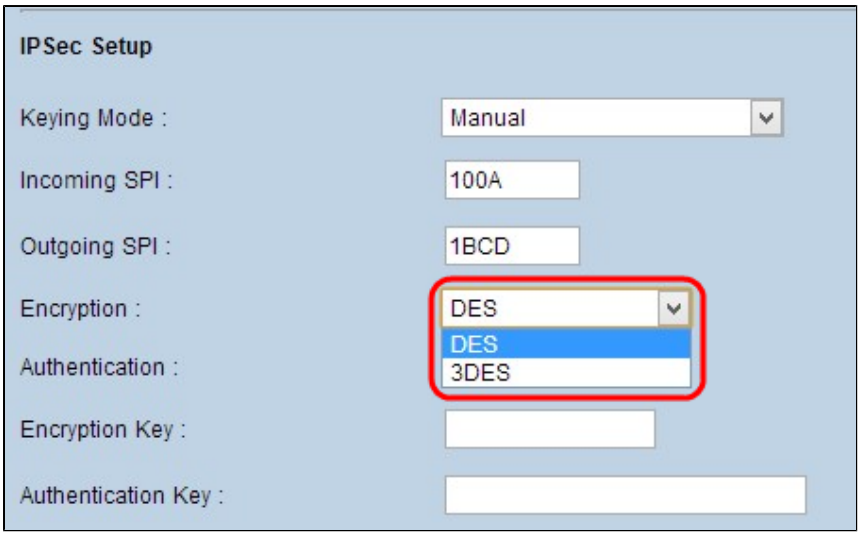
Étape 1. Entrez la valeur hexadécimale unique de l'index de paramètres de sécurité (SPI) entrant dans le champ *SPI entrant*. Le SPI est transporté dans lâ€™en-tête ESP (Encapsulating Security Payload Protocol), qui détermine la protection du paquet entrant. Vous pouvez saisir de 100 à ffffffff. Le SPI entrant du routeur local doit correspondre au SPI sortant du routeur distant.

Étape 2. Entrez la valeur hexadécimale unique de l'index de paramètres de sécurité (SPI) sortant dans le champ *SPI sortant*. Le SPI est transporté dans lâ€™en-tête ESP (Encapsulating Security Payload Protocol), qui détermine la protection du paquet sortant. Vous pouvez saisir de 100 à ffffffff. Le SPI sortant du routeur distant doit correspondre au SPI entrant du routeur local.



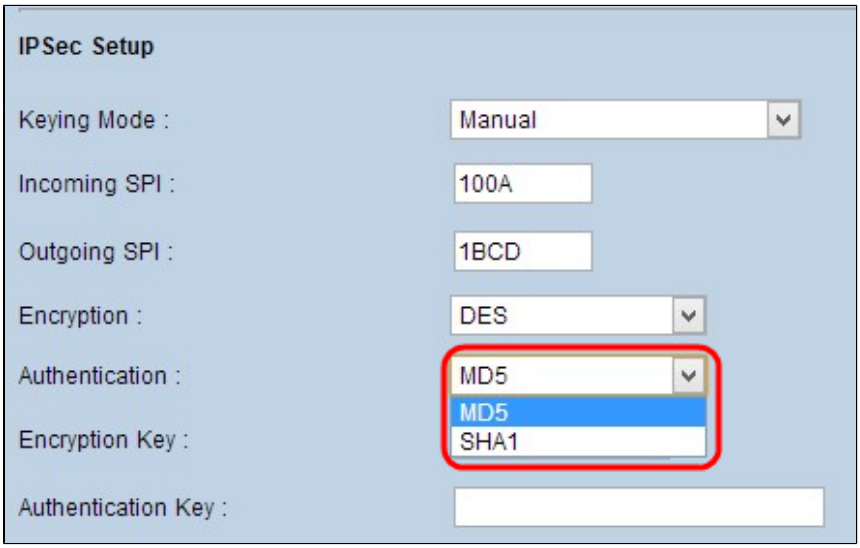

Étape 3. Choisissez la méthode de cryptage appropriée pour les données dans la liste déroulante *Encryption*. Le chiffrement recommandé est *3DES*. Le tunnel VPN doit utiliser la même méthode de chiffrement pour ses deux extrémités.

- DES : la norme DES (Data Encryption Standard) utilise une taille de clé de 56 bits pour le cryptage des données. DES est obsolète et ne doit être utilisée que si un terminal prend uniquement en charge cette norme.
- 3DES (Triple Data Encryption Standard) : la norme 3DES (Triple Data Encryption Standard) est une méthode de cryptage simple de 168 bits. Le chiffrement 3DES chiffre les données trois fois, ce qui améliore la sécurité par rapport à la norme DES.



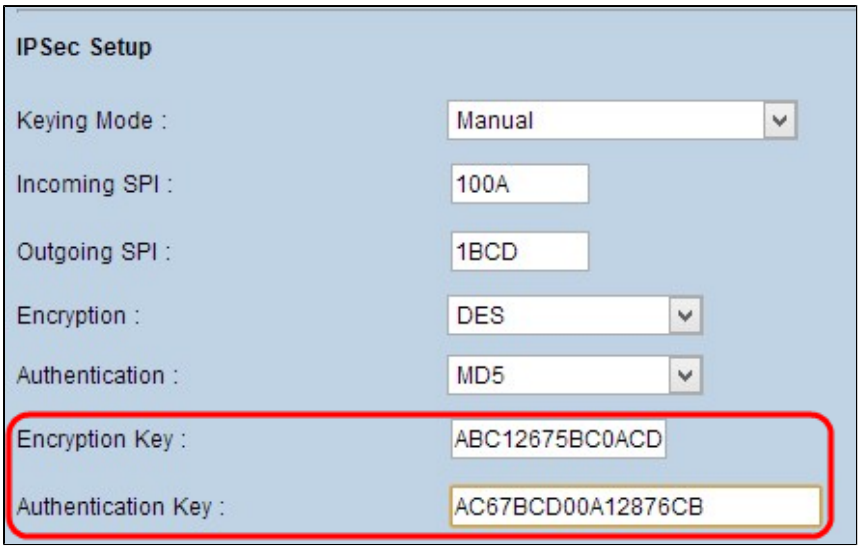

Étape 4. Choisissez la méthode d'authentification appropriée pour les données dans la liste déroulante *Authentification*. Lâ€™authentification recommandée est *SHA1, car elle est plus sécurisée que la méthode MD5*. Le tunnel VPN doit utiliser la même méthode dâ€™authentification pour ses deux extrémités.

- MD5 : l'algorithme MD5 (Message Digest Algorithm-5) représente une fonction de hachage hexadécimale à 32 chiffres qui protège les données contre les attaques malveillantes par le calcul de la somme de contrôle.
- SHA1 - Secure Hash Algorithm version 1 (SHA1) est une fonction de hachage 160 bits plus sécurisée que MD5, mais dont le calcul prend plus de temps.




Étape 5. Saisissez la clé de cryptage et de décryptage des données dans le champ *Encryption Key*. Si vous choisissez la méthode de chiffrement DES, à lâ€™étape 3, saisissez une valeur hexadécimale de 16 chiffres. Si vous choisissez la méthode de chiffrement 3DES, à lâ€™étape 3, saisissez une valeur hexadécimale de 40 chiffres.

Étape 6. Entrez une clé pré-partagée pour authentifier le trafic dans le champ *Authentication Key*. Si vous choisissez la méthode dâ€™authentification MD5, à lâ€™étape 4, saisissez une valeur hexadécimale de 32 chiffres. Si vous choisissez la méthode dâ€™authentification SHA, à lâ€™étape 4, saisissez une valeur hexadécimale de 40 chiffres. Le tunnel VPN doit utiliser la même clé prépartagée pour ses deux extrémités.

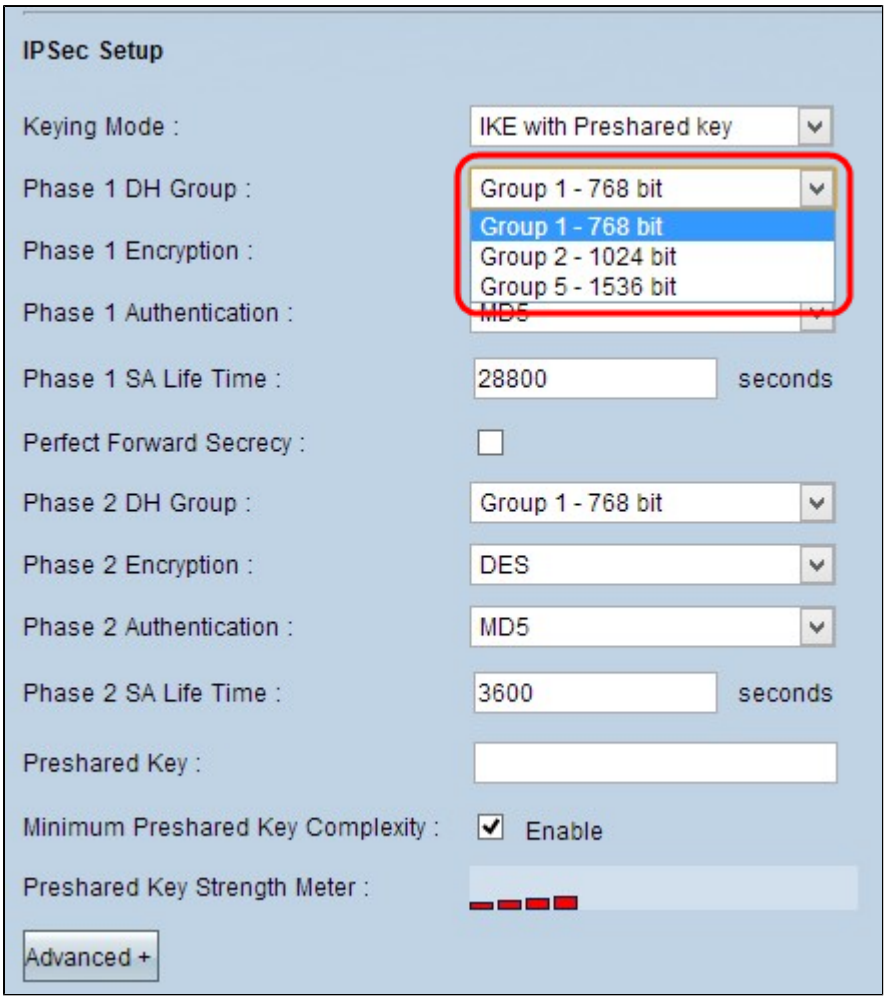



Étape 7. Cliquez sur **Save pour enregistrer les paramètres.**

**IKE avec configuration du mode de la clé prépartagée**

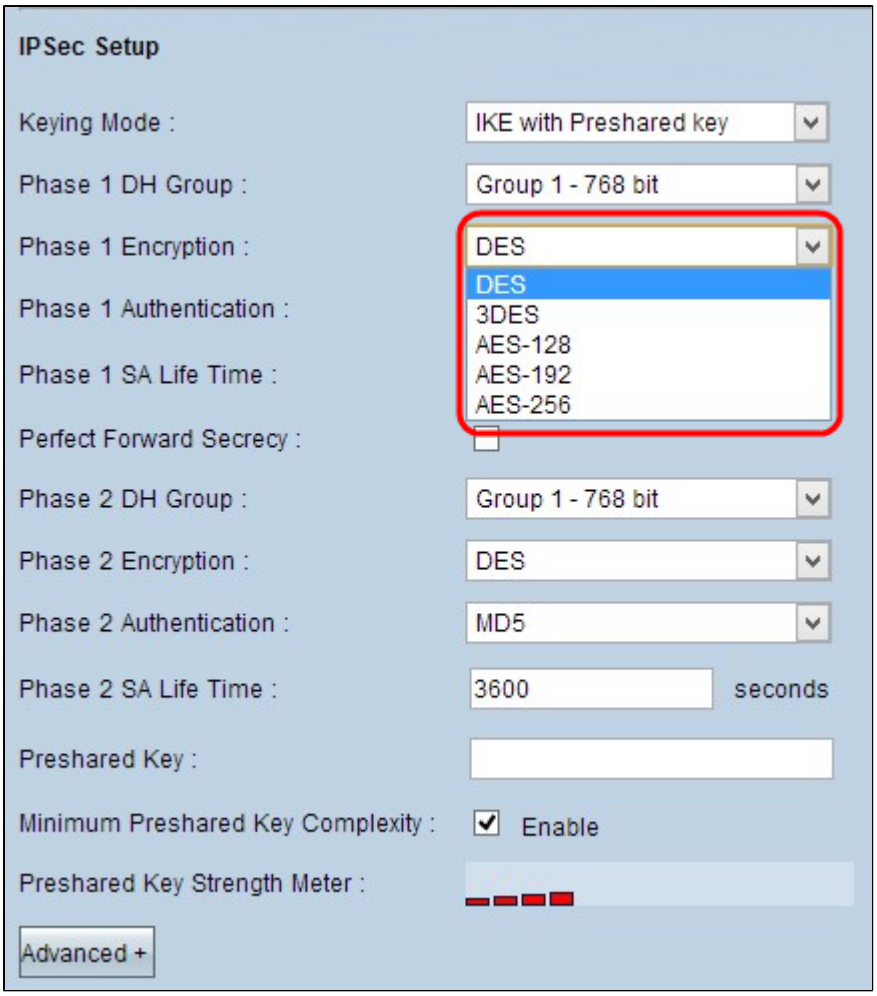
Étape 1. Sélectionnez le groupe DH de phase 1 approprié dans la liste déroulante *Groupe DH de phase 1*. La phase 1 est utilisée pour établir le simplex, lâ€™association de sécurité logique (SA) entre les deux extrémités du tunnel afin de prendre en charge la communication sécurisée de lâ€™authentification. Le protocole Diffie-Hellman (DH) est un protocole dâ€™échange de clés cryptographiques utilisé pour déterminer la puissance de la clé au cours de la phase 1 et il permet aussi de partager la clé secrète pour authentifier la communication.

- Groupe 1, 768 bits : la clé de puissance la plus basse et le groupe dâ€™authentification le moins sécurisé. Mais il faut moins de temps pour calculer les clés IKE. Cette option est préférable si le débit du réseau est faible.
- Groupe 2, 1024 bits : la clé de puissance supérieure, un groupe dâ€™authentification plus sécurisé. Mais il faut un certain temps pour calculer les clés IKE.
- Groupe 5, 1536 bits : la clé la plus puissante et le groupe dâ€™authentification le mieux sécurisé. Il faut plus de temps pour calculer les clés IKE. Cette option est préférable si le débit du réseau est élevé.



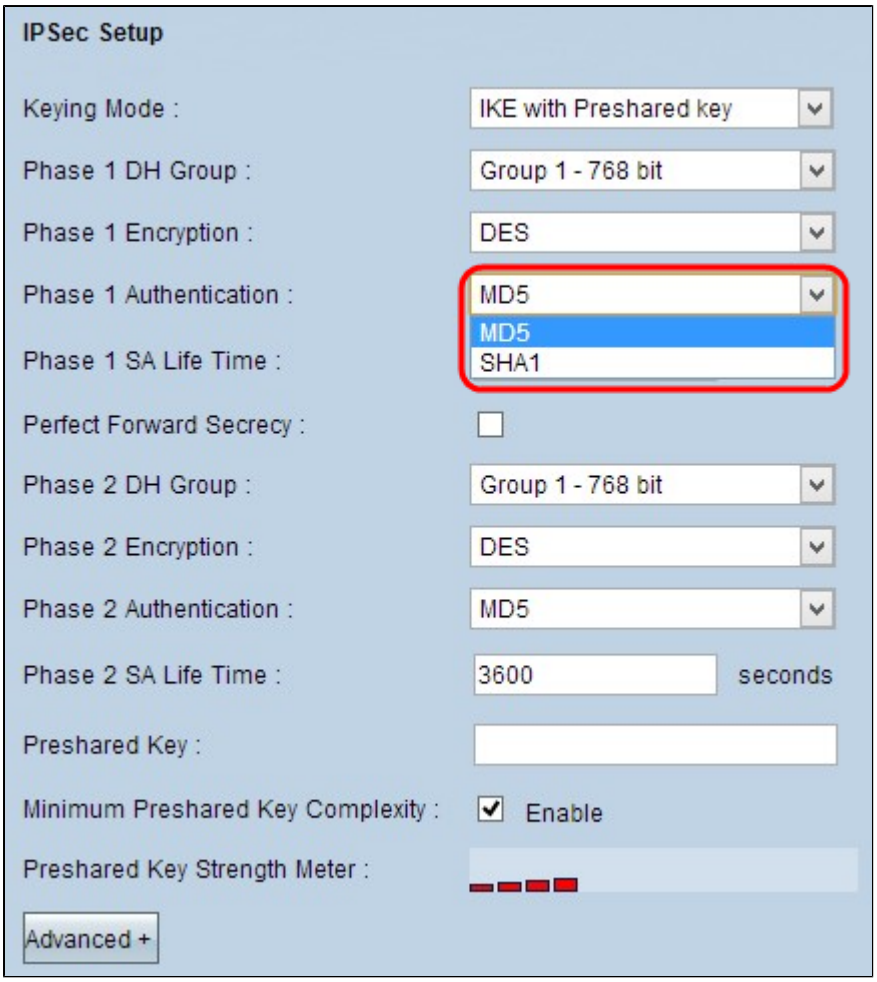

Étape 2. Choisissez le chiffrement de phase 1 approprié pour chiffrer la clé dans la liste déroulante *Cryptage de phase 1*. La méthode 3DES est recommandée, car il sâ€™agit de la méthode de chiffrement la mieux sécurisée. Le tunnel VPN doit utiliser la même méthode de chiffrement pour ses deux extrémités.

- DES : la norme DES (Data Encryption Standard) utilise une taille de clé de 56 bits pour le cryptage des données. DES est obsolète et ne doit être utilisée que si un terminal prend uniquement en charge cette norme.
- 3DES (Triple Data Encryption Standard) : la norme 3DES (Triple Data Encryption Standard) est une méthode de cryptage simple de 168 bits. Le chiffrement 3DES chiffre les données trois fois, ce qui améliore la sécurité par rapport à la norme DES.
- AES-128 - Advanced Encryption Standard (AES) est une méthode de cryptage à 128 bits qui transforme le texte brut en texte chiffré par 10 cycles de répétition.
- AES-192 - Advanced Encryption Standard (AES) est une méthode de cryptage 192 bits qui transforme le texte brut en texte chiffré par 12 cycles de répétition. AES-192 est plus sécurisée que AES-128.
- AES-256 - Advanced Encryption Standard (AES) est une méthode de cryptage de 256 bits qui transforme le texte brut en texte chiffré par 14 cycles de répétition. AES-256 est la méthode de chiffrement la plus sécurisée.



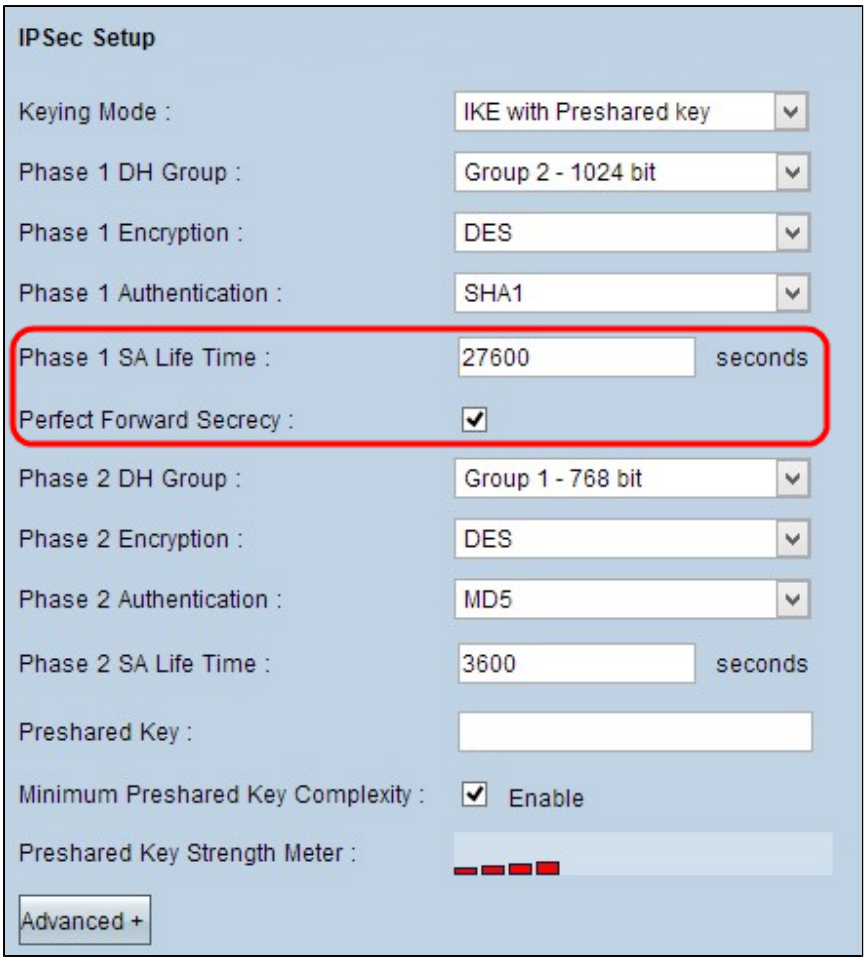

Étape 3. Sélectionnez la méthode d'authentification de phase 1 appropriée dans la liste déroulante *Authentification de phase 1*. Le tunnel VPN doit utiliser la même méthode dâ€™authentification pour ses deux extrémités.

- MD5 : l'algorithme MD5 (Message Digest Algorithm-5) représente une fonction de hachage hexadécimale à 32 chiffres qui protège les données contre les attaques malveillantes par le calcul de la somme de contrôle.
- SHA1 - Secure Hash Algorithm version 1 (SHA1) est une fonction de hachage 160 bits plus sécurisée que MD5, mais dont le calcul prend plus de temps.



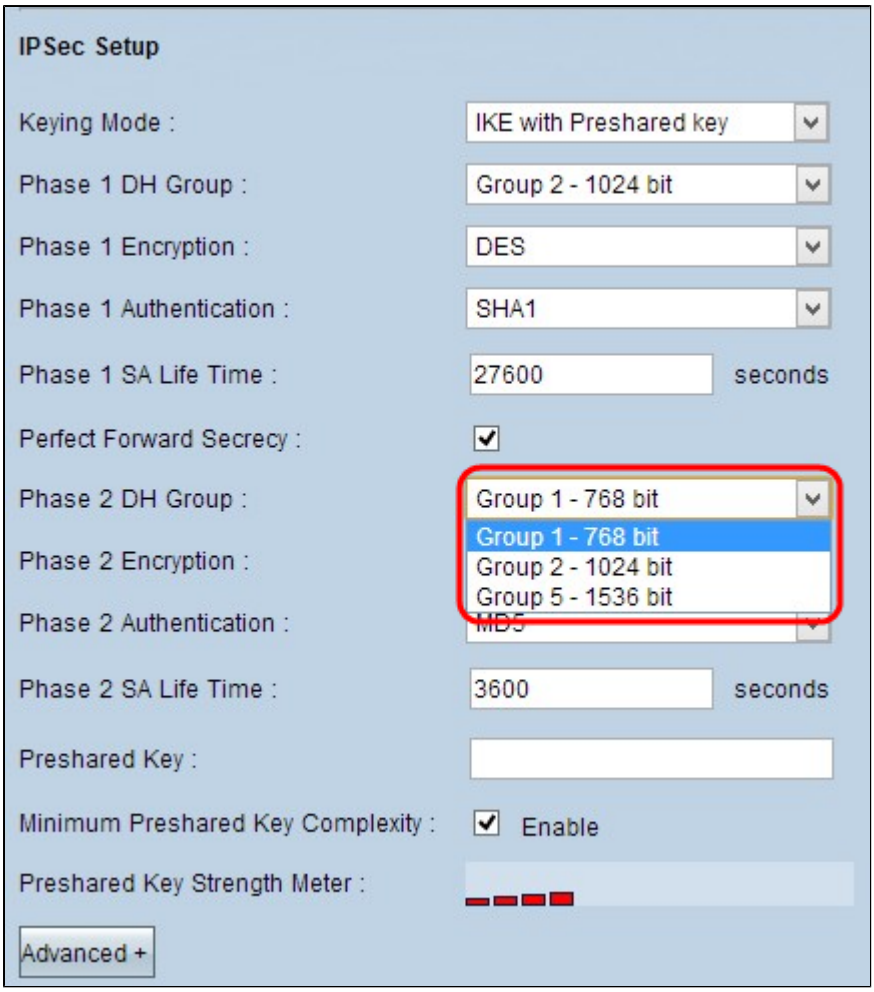

Étape 4. Saisissez la durée en secondes pendant laquelle les clés de la phase 1 sont valides et le tunnel VPN reste actif dans le champ *Phase 1 SA Life Time*.

Étape 5. Activez la case à cocher de confidentialité de transfert parfaite (**Perfect Forward Secrecy) pour assurer une meilleure protection des clés.** Cette option permet au routeur de générer une nouvelle clé si une clé est compromise. Les données chiffrées sont uniquement compromises par le biais de la clé compromise. Par conséquent, cela assure donc une communication plus sécurisée et authentifiée en sécurisant dâ€™autres clés, même si une clé est compromise. Il sâ€™agit dâ€™une action recommandée, car elle fournit plus de sécurité.



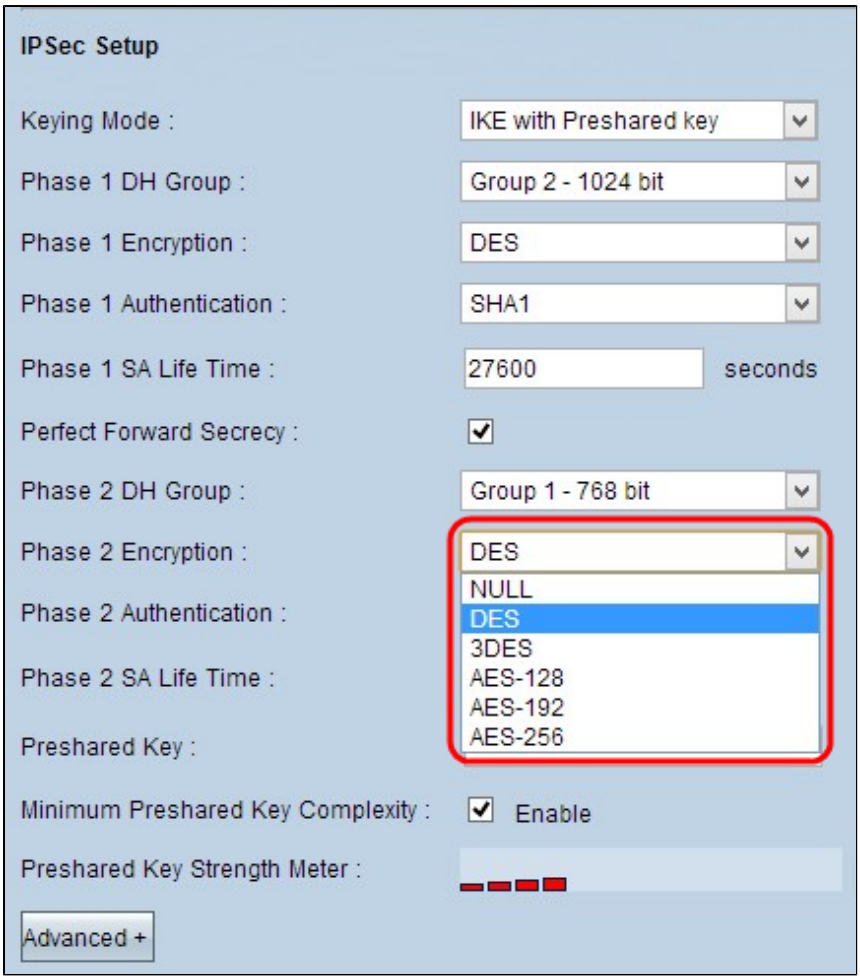

Étape 6. Sélectionnez le groupe DH de phase 2 approprié dans la liste déroulante *Groupe DH de phase 2*. La phase 2 fait appel à lâ€™association de sécurité et permet de déterminer la sécurité du paquet de données pendant que les paquets de données transitent entre les deux points de terminaison.

- Groupe 1, 768 bits : représente la clé de puissance la plus basse et le groupe dâ€™authentification le moins sécurisé. Mais il faut moins de temps pour calculer les clés IKE. Cette option est préférable si le débit du réseau est faible.
- Groupe 2, 1024 bits : représente la clé de puissance supérieure, un groupe dâ€™authentification plus sécurisé. Mais il faut un certain temps pour calculer les clés IKE.
- Groupe 5, 1536 bits : la clé la plus puissante et le groupe dâ€™authentification le mieux sécurisé. Il faut plus de temps pour calculer les clés IKE. Cette option est préférable si le débit du réseau est élevé.



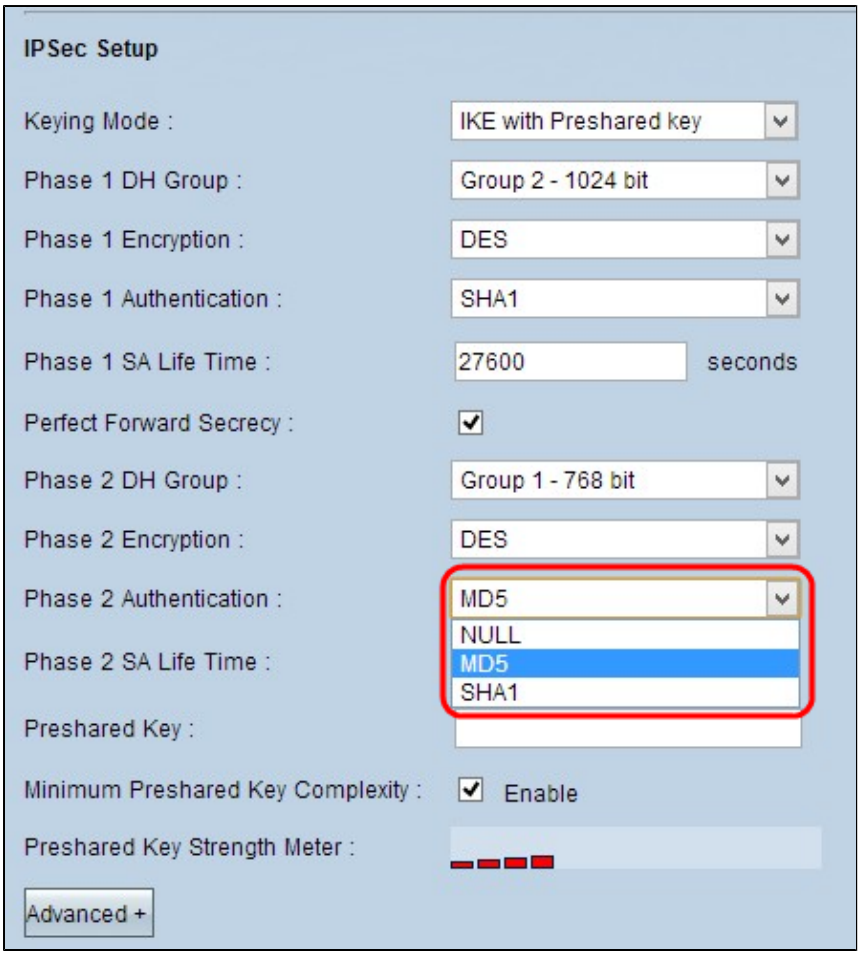

Étape 7. Choisissez le chiffrement de phase 2 approprié pour chiffrer la clé dans la liste déroulante *Cryptage de phase 2*. La méthode AES-256 est recommandée, car il sâ€™agit de la méthode de chiffrement la mieux sécurisée. Le tunnel VPN doit utiliser la même méthode de chiffrement pour ses deux extrémités.

- DES : la norme DES (Data Encryption Standard) utilise une taille de clé de 56 bits pour le cryptage des données. DES est obsolète et ne doit être utilisée que si un terminal prend uniquement en charge cette norme.
- 3DES (Triple Data Encryption Standard) : la norme 3DES (Triple Data Encryption Standard) est une méthode de cryptage simple de 168 bits. Le chiffrement 3DES chiffre les données trois fois, ce qui améliore la sécurité par rapport à la norme DES.
- AES-128 - Advanced Encryption Standard (AES) est une méthode de cryptage à 128 bits qui transforme le texte brut en texte chiffré par 10 cycles de répétition.
- AES-192 - Advanced Encryption Standard (AES) est une méthode de cryptage 192 bits qui transforme le texte brut en texte chiffré par 12 cycles de répétition. AES-192 est plus sécurisée que AES-128.
- AES-256 - Advanced Encryption Standard (AES) est une méthode de cryptage de 256 bits qui transforme le texte brut en texte chiffré par 14 cycles de répétition. AES-256 est la méthode de chiffrement la plus sécurisée.




Étape 8. Sélectionnez la méthode d'authentification appropriée dans la liste déroulante *Phase 2 Authentication*. Le tunnel VPN doit utiliser la même méthode dâ€™authentification pour ses deux extrémités.

- MD5 : l'algorithme MD5 (Message Digest Algorithm-5) représente une fonction de hachage hexadécimale à 32 chiffres qui protège les données contre les attaques malveillantes par le calcul de la somme de contrôle.
- SHA1 - Secure Hash Algorithm version 1 (SHA1) est une fonction de hachage 160 bits plus sécurisée que MD5, mais dont le calcul prend plus de temps.
- Null : aucune méthode dâ€™authentification nâ€™est utilisée.



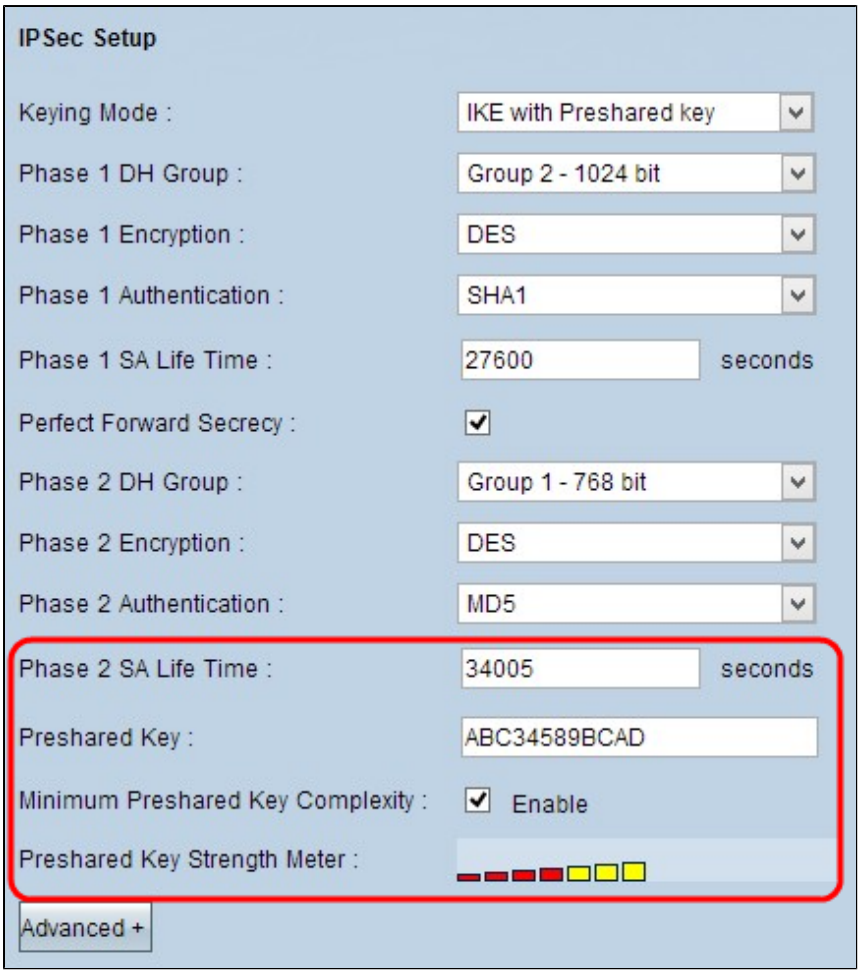

Étape 9. Saisissez la durée en secondes pendant laquelle les clés de la phase 2 sont valides et le tunnel VPN reste actif dans le champ *Phase 2 SA Life Time*.

Étape 10. Entrez une clé qui est partagée précédemment entre les homologues IKE pour authentifier les homologues dans le champ *Clé pré-partagée*. Il est possible dâ€™utiliser jusquâ€™à 30 caractères hexadécimaux et autres caractères comme clé prépartagée. Le tunnel VPN doit utiliser la même clé prépartagée pour ses deux extrémités.

**Remarque :** il est fortement recommandé de changer fréquemment la clé pré-partagée entre les homologues IKE afin que le VPN reste sécurisé.

Étape 11. Activez la case à cocher **Minimum Preshared Key Complexity (complexité minimale des clés prépartagées) si vous souhaitez activer la mesure de force pour la clé prépartagée.** La mesure est utilisée pour déterminer la puissance de la clé prépartagée par le biais de barres de couleur

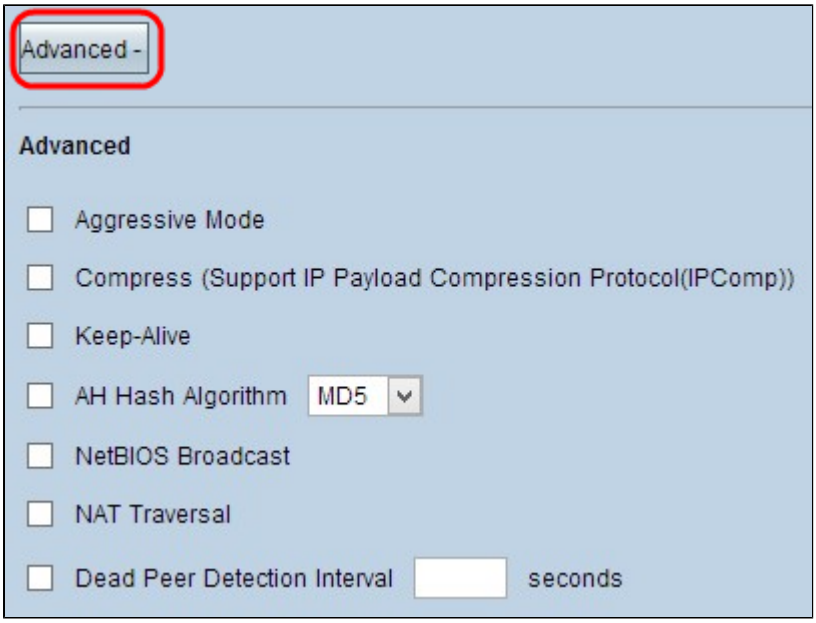
**Remarque** : le *mesureur de force de la clé pré-partagée* indique la force de la clé pré-partagée à travers des barres colorées. La couleur rouge indique une puissance faible, la couleur jaune, une puissance acceptable et le vert, une puissance élevée.




Étape 12. Cliquez sur **Save pour enregistrer les paramètres.**

**Paramètres avancés dâ€™IKE avec configuration du mode de la clé prépartagée**

Étape 1. Cliquez sur **Advanced** pour afficher les paramètres avancés de IKE avec clé pré-partagée.



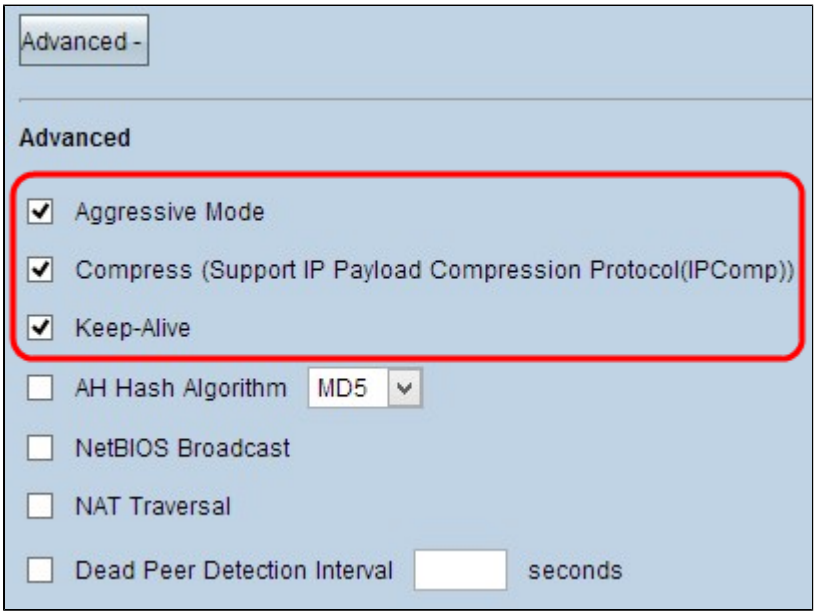

Étape 2. Activez la case à cocher **Aggressive Mode (mode agressif) si votre débit de réseau est faible.**

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.

**Remarque : le** mode agressif n'est pas disponible pour la connexion VPN de groupe client à passerelle.

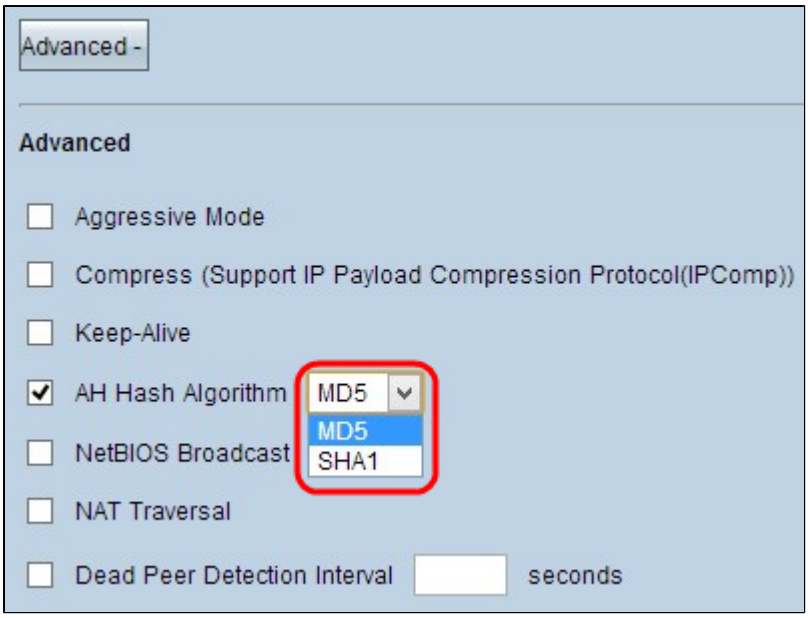
Étape 3. Cochez la case **Compress (Support IP Payload Compression Protocol (IPComp))** si vous voulez compresser la taille des datagrammes IP. IPComp est un protocole de compression IP utilisé pour comprimer la taille du datagramme IP. La compression IP est utile si la vitesse du réseau est faible et que lâ€™utilisateur souhaite transmettre rapidement les données sans aucune perte via le réseau lent, mais elle nâ€™offre pas de sécurité.

Étape 4. Cochez la case **Keep-Alive si vous souhaitez toujours que la connexion du tunnel VPN demeure active.** Lâ€™option Keep Alive permet de rétablir immédiatement les connexions si une connexion devient inactive.




Étape 5. 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 ses deux côtés.

- MD5 - Message Digest Algorithm-5 (MD5) représente une fonction de hachage hexadécimale à 128 chiffres qui protège les données contre les attaques malveillantes par le calcul de la somme de contrôle.
- SHA1 - Secure Hash Algorithm version 1 (SHA1) est une fonction de hachage 160 bits plus sécurisée que MD5, mais dont le calcul prend plus de temps.

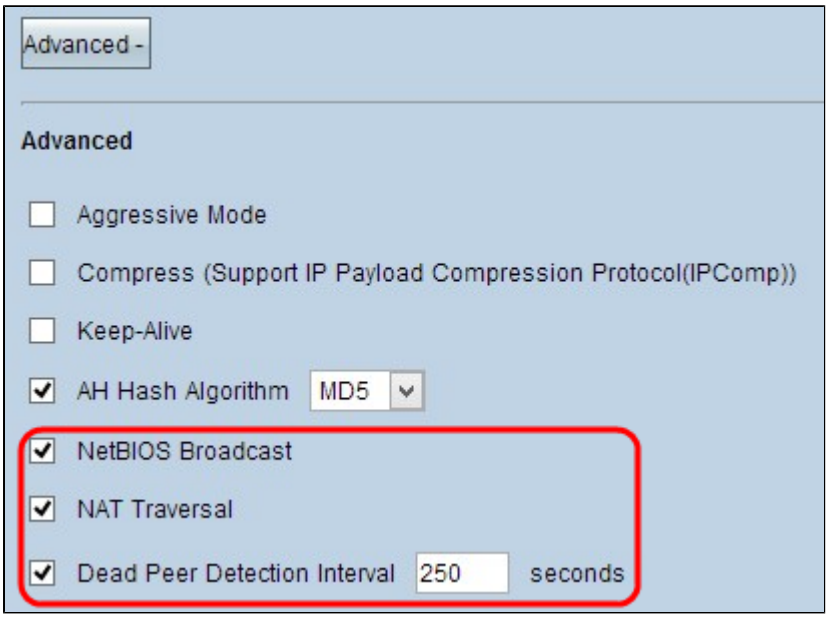



Étape 6. Vérifiez la diffusion NetBIOS (**NetBIOS Broadcast) si vous souhaitez autoriser le trafic non routable via le tunnel VPN.** La case est décochée par défaut. NetBIOS est utilisé pour détecter les ressources réseau, telles que les imprimantes, les ordinateurs, etc. dans le réseau, via certaines applications logicielles et des fonctionnalités Windows telles que le voisinage réseau.

Étape 7. Cochez la case de la traversée NAT (**NAT Traversal) si vous souhaitez accéder à Internet depuis votre LAN privé par le biais dâ€™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 8. 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, saisissez la durée souhaitée ou lâ€™intervalle souhaité pour les messages Hello.

**Remarque :** vous pouvez configurer l'intervalle de détection d'homologue mort uniquement pour une connexion VPN de client à passerelle unique, et non pour une connexion VPN de client à passerelle de groupe.




Étape 9. Cliquez sur **Save pour enregistrer les paramètres.**

Vous avez maintenant appris à configurer le tunnel VPN dâ€™accès à distance entre le client et la passerelle sur les routeurs VPN RV016, RV042, RV042G et RV082.

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.