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

Objectif

Un réseau privé virtuel (VPN) est utilisé pour établir une connexion sécurisée entre deux points d'extrémité sur un Internet public ou partagé, via ce que l'on appelle un tunnel VPN. 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 d'apparaître logiquement comme s'il faisait partie du réseau situé à l'autre extrémité. Les données et les ressources peuvent ainsi être partagées plus facilement et en toute sécurité sur Internet.

La configuration doit être effectuée sur les deux routeurs pour activer un VPN de passerelle à passerelle. Les configurations effectuées dans les sections Local Group Setup et Remote Group Setup doivent être inversées entre les deux routeurs afin que le groupe local de l'un soit le groupe distant de l'autre.

L'objectif de ce document est d'expliquer comment configurer un VPN passerelle-à-passerelle sur des routeurs VPN RV016, RV042, RV042G et RV082.

Périphériques pertinents

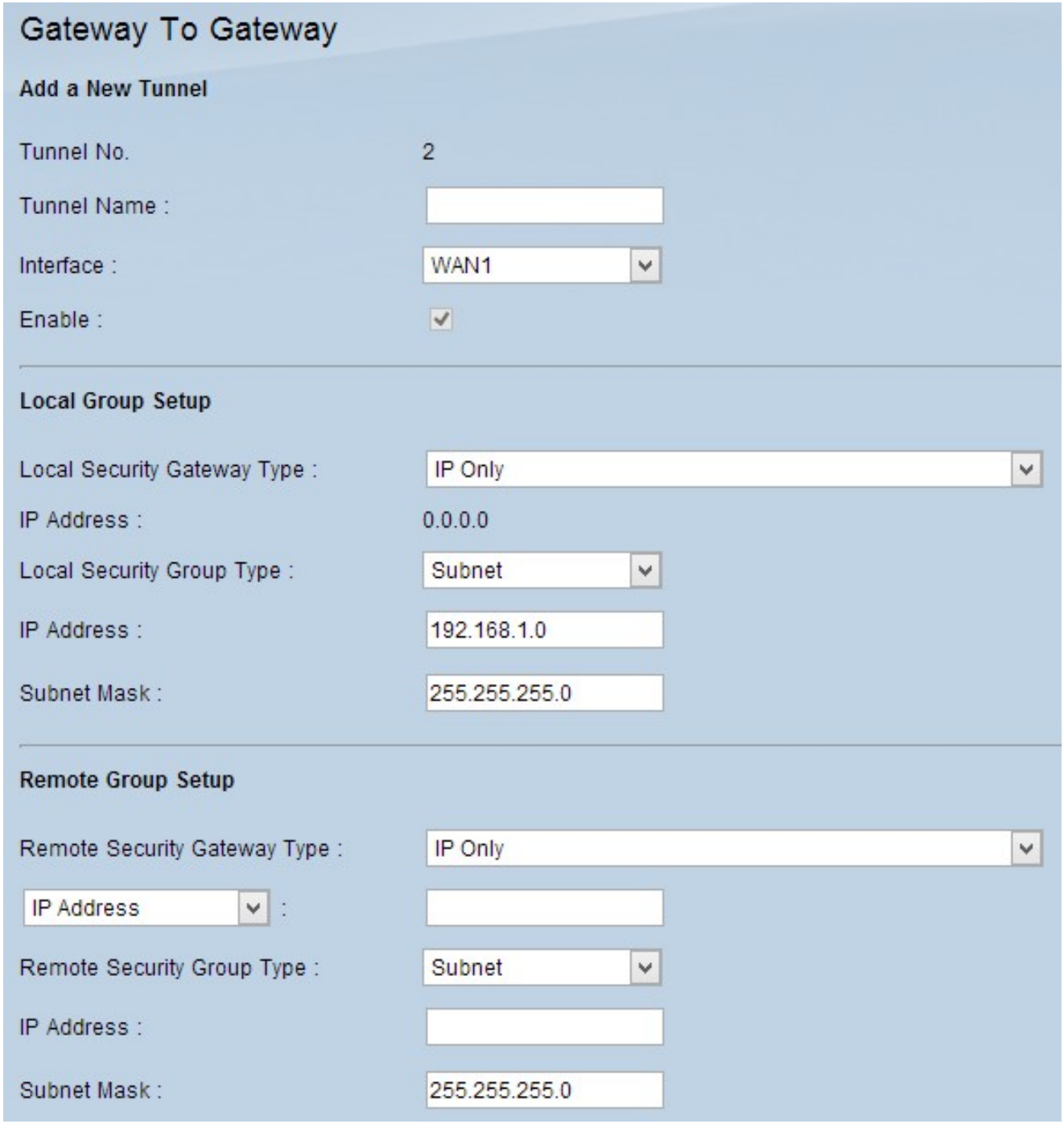
- RV016
- RV042
- RV042G
- RV082

Version du logiciel

- v 4.2.2.08

Configuration du 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 :



Pour configurer la passerelle vers le VPN de passerelle, les fonctionnalités suivantes doivent être configurées :

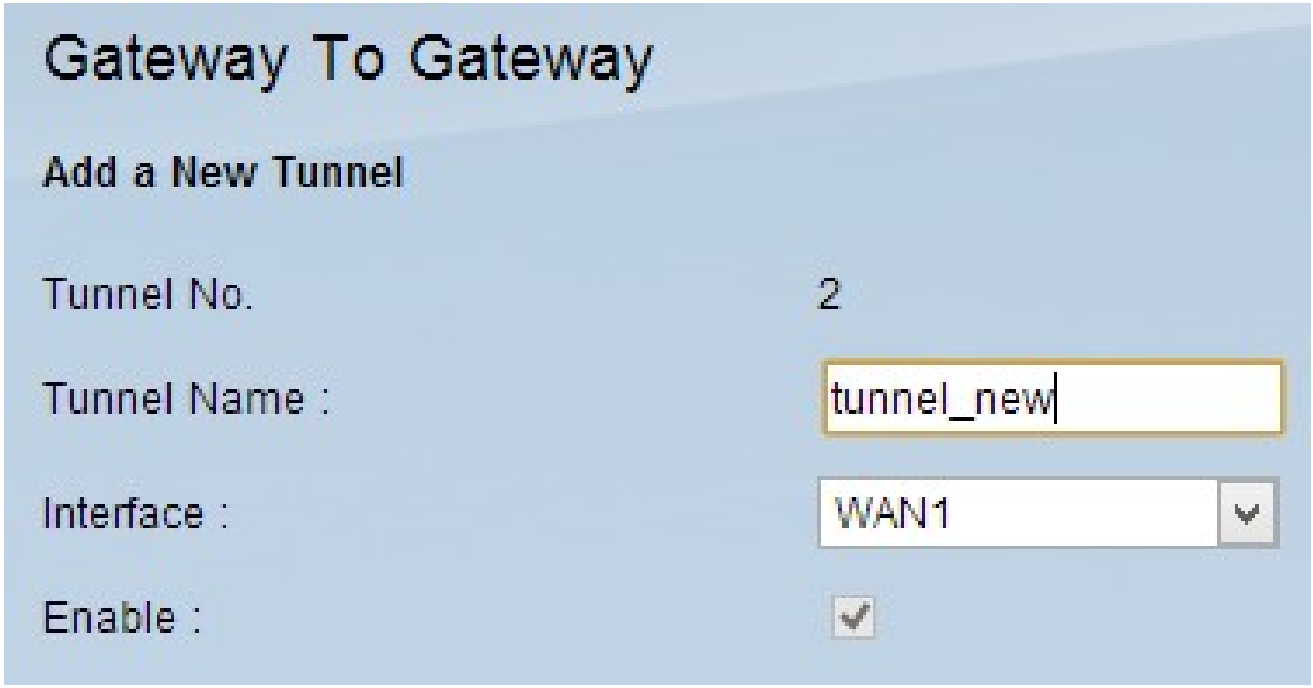
1. Ajouter un nouveau tunnel

2. Configuration du groupe local

3. Configuration du groupe distant

4. Configuration IPSec

Ajouter un nouveau tunnel



Tunnel No. est un champ en lecture seule qui affiche le tunnel en cours de création.

Étape 1. Entrez un nom pour le tunnel VPN dans le champ Tunnel Name. Il ne doit pas nécessairement correspondre au nom utilisé à l'autre extrémité du tunnel.

Étape 2. Dans la liste déroulante Interface, sélectionnez le port de réseau étendu (WAN) à utiliser pour le tunnel.

· WAN1 : port WAN dédié des routeurs VPN de la gamme RV0XX.

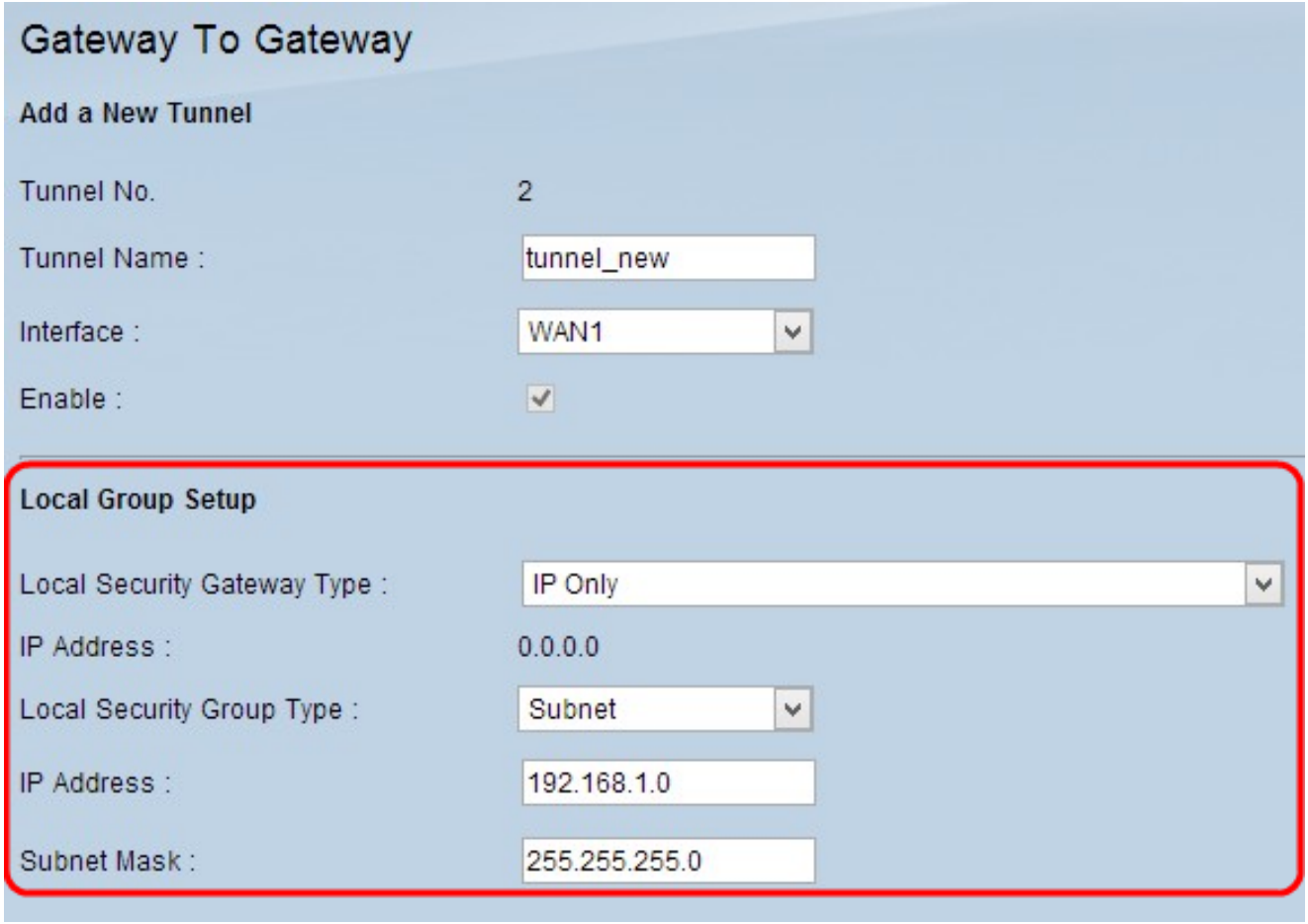
· WAN2 : port WAN2/DMZ des routeurs VPN de la gamme RV0XX. S'affiche uniquement dans le menu déroulant s'il a été configuré en tant que WAN et non en tant que port DMZ (Demilitarize Zone).

Étape 3. (Facultatif) Pour activer le VPN, cochez la case dans le champ Enable (activer). Le

VPN est activé par défaut.

Configuration du groupe local

Remarque : la configuration de la configuration du groupe local sur un routeur doit être identique à celle de la configuration du groupe distant sur l'autre routeur.



Étape 1. Choisissez la méthode d'identification de routeur appropriée pour établir un tunnel VPN dans la liste déroulante Local Security Gateway Type.

· IP Only : le routeur local (ce routeur) est reconnu par une adresse IP statique. Vous ne pouvez choisir cette option que si le routeur a une adresse IP WAN statique. L'adresse IP WAN statique apparaît automatiquement dans le champ IP Address (Adresse IP).

· Authentification IP + Domain Name (FQDN) - L'accès au tunnel est possible via une adresse IP statique et un domaine enregistré. Si vous choisissez cette option, saisissez le nom du domaine enregistré dans le champ Domain Name (nom de domaine). L'adresse IP WAN statique apparaît automatiquement dans le champ IP Address (Adresse IP).

· IP + E-mail Addr.(USER FQDN) Authentication : l'accès au tunnel est possible via une adresse IP statique et une adresse e-mail. Si vous choisissez cette option, saisissez l’adresse courriel dans le champ Email Address. L'adresse IP WAN statique apparaît automatiquement dans le champ IP Address (Adresse IP).

· Authentification IP dynamique + nom de domaine (FQDN) - L'accès au tunnel est possible via une adresse IP dynamique et un domaine enregistré. Si vous choisissez cette option, saisissez le nom du domaine enregistré dans le champ Domain Name (nom de domaine).

· Dynamic IP + Email Addr.(USER FQDN) Authentication : l'accès au tunnel est possible via une adresse IP dynamique et une adresse e-mail. Si vous choisissez cette option, saisissez l’adresse courriel dans le champ Email Address.

Étape 2. Sélectionnez l'utilisateur ou le groupe d'utilisateurs LAN local approprié pouvant accéder au tunnel VPN dans la liste déroulante Local Security Group. La valeur par défaut est « Subnet » (sous-réseau).

· IP : un seul périphérique LAN peut accéder au tunnel VPN. Si vous choisissez cette option, saisissez l’adresse IP de l’appareil LAN dans le champ IP Address (adresse IP).

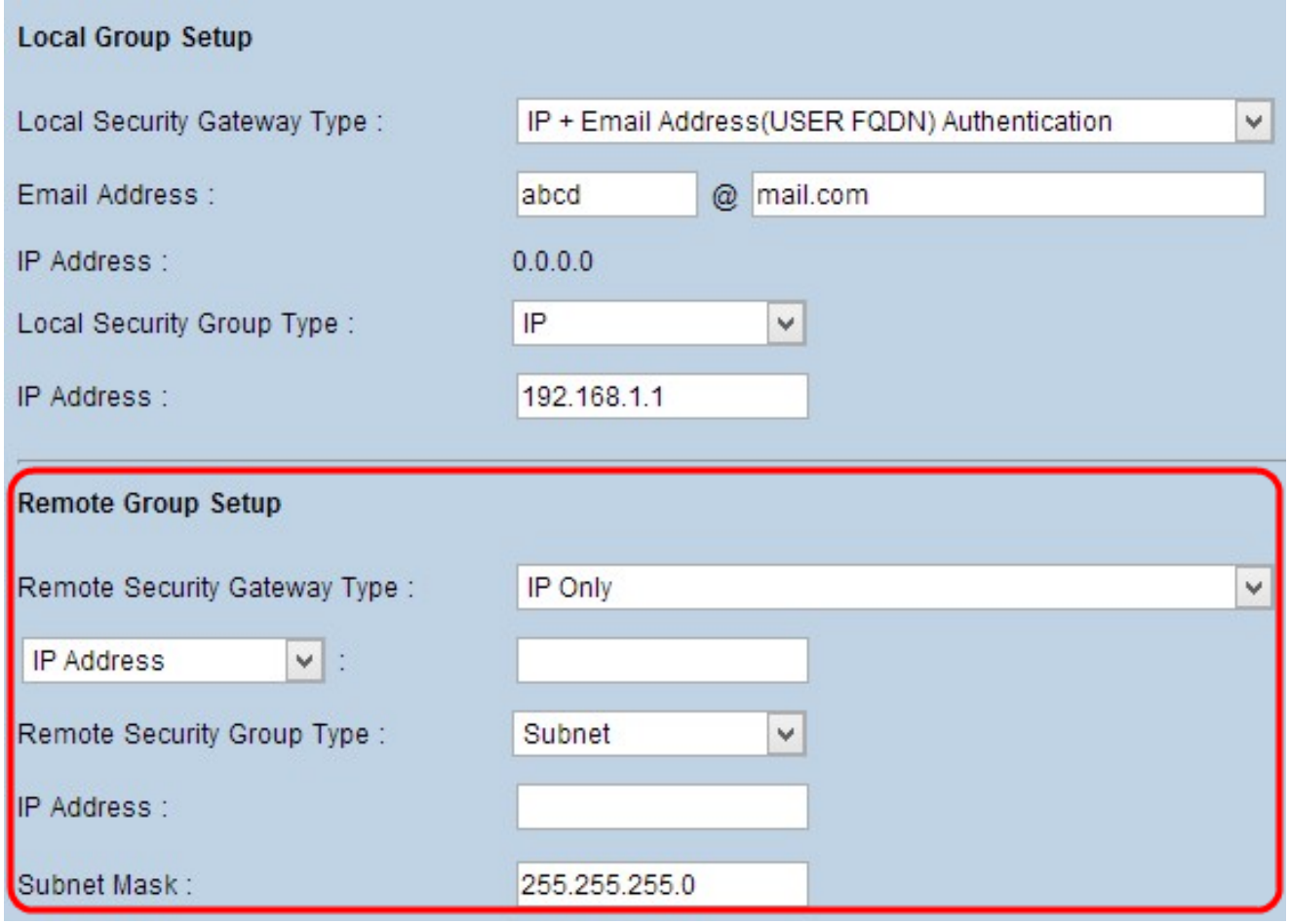
· Subnet : tous les périphériques LAN d'un sous-réseau spécifique peuvent accéder au tunnel. Si vous choisissez cette option, entrez l'adresse IP et le masque de sous-réseau des périphériques LAN dans les champs IP Address et Subnet Mask, respectivement. Le masque par défaut est 255.255.255.0.

· Plage IP : une plage de périphériques LAN peut accéder au tunnel. Si vous choisissez cette option, saisissez l’adresse IP de début et de fin respectivement dans les champs Begin IP (adresse IP de début) et End IP (adresse IP de fin).

Étape 3. Cliquez sur Save pour enregistrer les paramètres.

Configuration du groupe distant

Remarque : la configuration de la configuration du groupe distant sur un routeur doit être identique à celle de la configuration du groupe local sur l'autre routeur.



Étape 1. Dans la liste déroulante Remote Security Gateway Type, choisissez la méthode d'identification du routeur distant pour établir le tunnel VPN.

· IP Only : l'accès au tunnel est possible via une adresse IP WAN statique. Si vous connaissez l'adresse IP du routeur distant, choisissez IP address (Adresse IP) dans la liste déroulante située directement sous le champ Remote Security Gateway Type (Type de passerelle de sécurité distante) et saisissez l'adresse IP. Choisissez IP by DNS Resolved si vous ne connaissez pas l'adresse IP mais le nom de domaine et entrez le nom de domaine du routeur dans le champ IP by DNS Resolved.

· Authentification IP + Domain Name (FQDN) - L'accès au tunnel est possible via une adresse IP statique et un domaine enregistré pour le routeur. Si vous connaissez l'adresse IP du routeur distant, choisissez IP address (Adresse IP) dans la liste déroulante située directement sous le champ Remote Security Gateway Type (Type de passerelle de sécurité distante) et saisissez l'adresse. Choisissez IP by DNS Resolved si vous ne connaissez pas l'adresse IP mais le nom de domaine et entrez le nom de domaine du routeur dans le champ IP by DNS Resolved. Saisissez le nom de domaine du routeur dans le champ Domain Name, quelle que soit la méthode choisie pour l'identifier.

· IP + Email Addr.(USER FQDN) Authentication : l'accès au tunnel est possible via une adresse IP statique et une adresse e-mail. Si vous connaissez l'adresse IP du routeur

distant, choisissez IP address dans la liste déroulante située directement sous le champ Remote Security Gateway Type et saisissez l'adresse. Choisissez IP by DNS Resolved si vous ne connaissez pas l'adresse IP mais le nom de domaine et entrez le nom de domaine du routeur dans le champ IP by DNS Resolved. Saisissez l'adresse e-mail dans le champ Adresse e-mail.

· Authentification IP dynamique + nom de domaine (FQDN) - L'accès au tunnel est possible via une adresse IP dynamique et un domaine enregistré. Si vous choisissez cette option, saisissez le nom du domaine enregistré dans le champ Domain Name (nom de domaine).

· Dynamic IP + Email Addr.(USER FQDN) Authentication : l'accès au tunnel est possible via une adresse IP dynamique et une adresse e-mail. Si vous choisissez cette option, saisissez l'adresse courriel dans le champ Email Address.

Étape 2. Sélectionnez l'utilisateur ou le groupe d'utilisateurs du réseau local distant qui peut accéder au tunnel VPN dans la liste déroulante Remote Security Group Type.

· IP : un seul périphérique LAN spécifique peut accéder au tunnel. Si vous choisissez cette option, saisissez l'adresse IP de l'appareil LAN dans le champ IP Address (adresse IP).

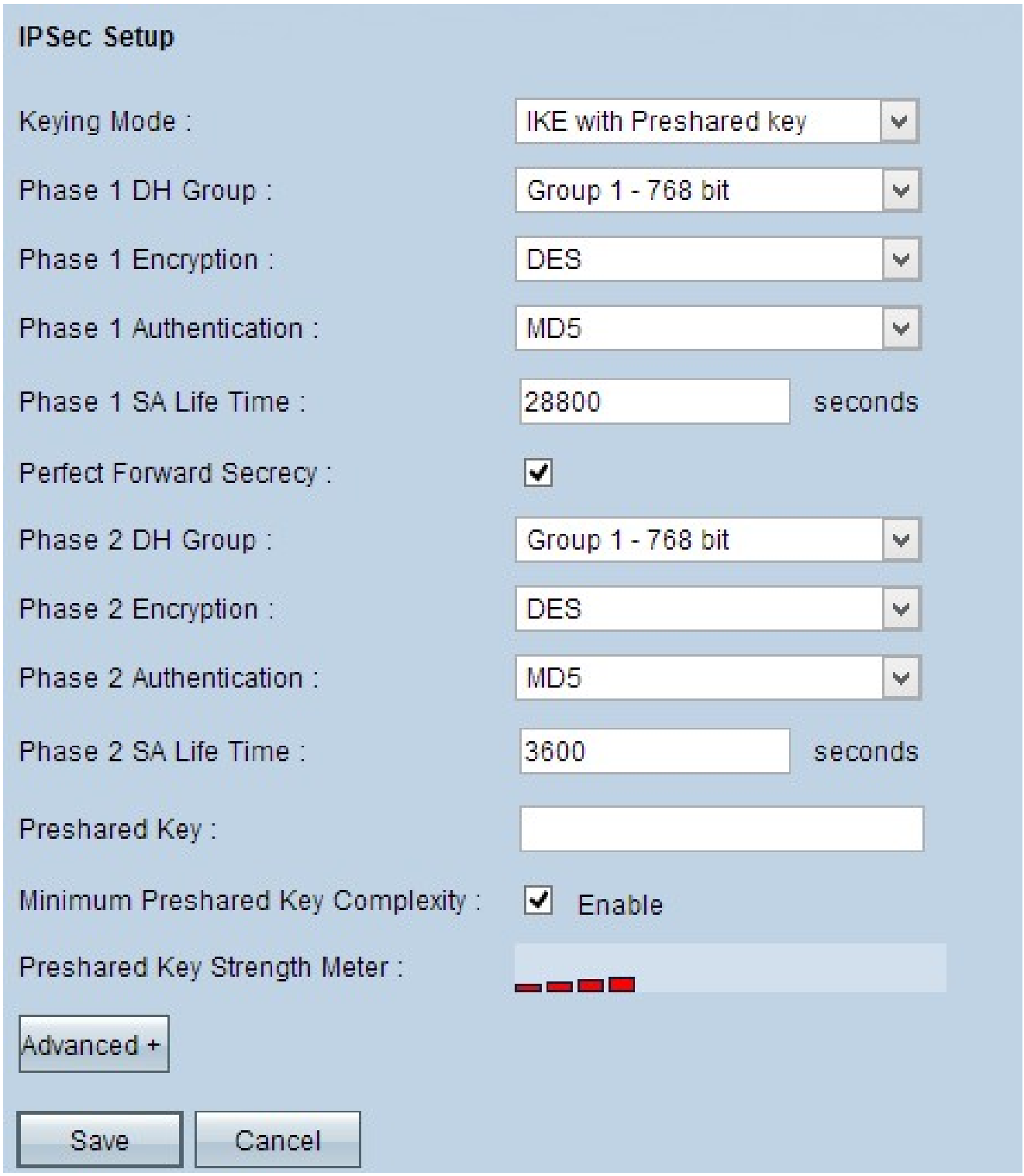
· Subnet : tous les périphériques LAN d'un sous-réseau spécifique peuvent accéder au tunnel. Si vous choisissez cette option, entrez l'adresse IP et le masque de sous-réseau des périphériques LAN dans les champs IP Address et Subnet Mask, respectivement.

· Plage IP : une plage de périphériques LAN peut accéder au tunnel. Si vous choisissez cette option, saisissez l'adresse IP de début et de fin respectivement dans les champs Begin IP (adresse IP de début) et End IP (adresse IP de fin).

Remarque : les deux routeurs situés aux extrémités du tunnel ne peuvent pas se trouver sur le même sous-réseau.

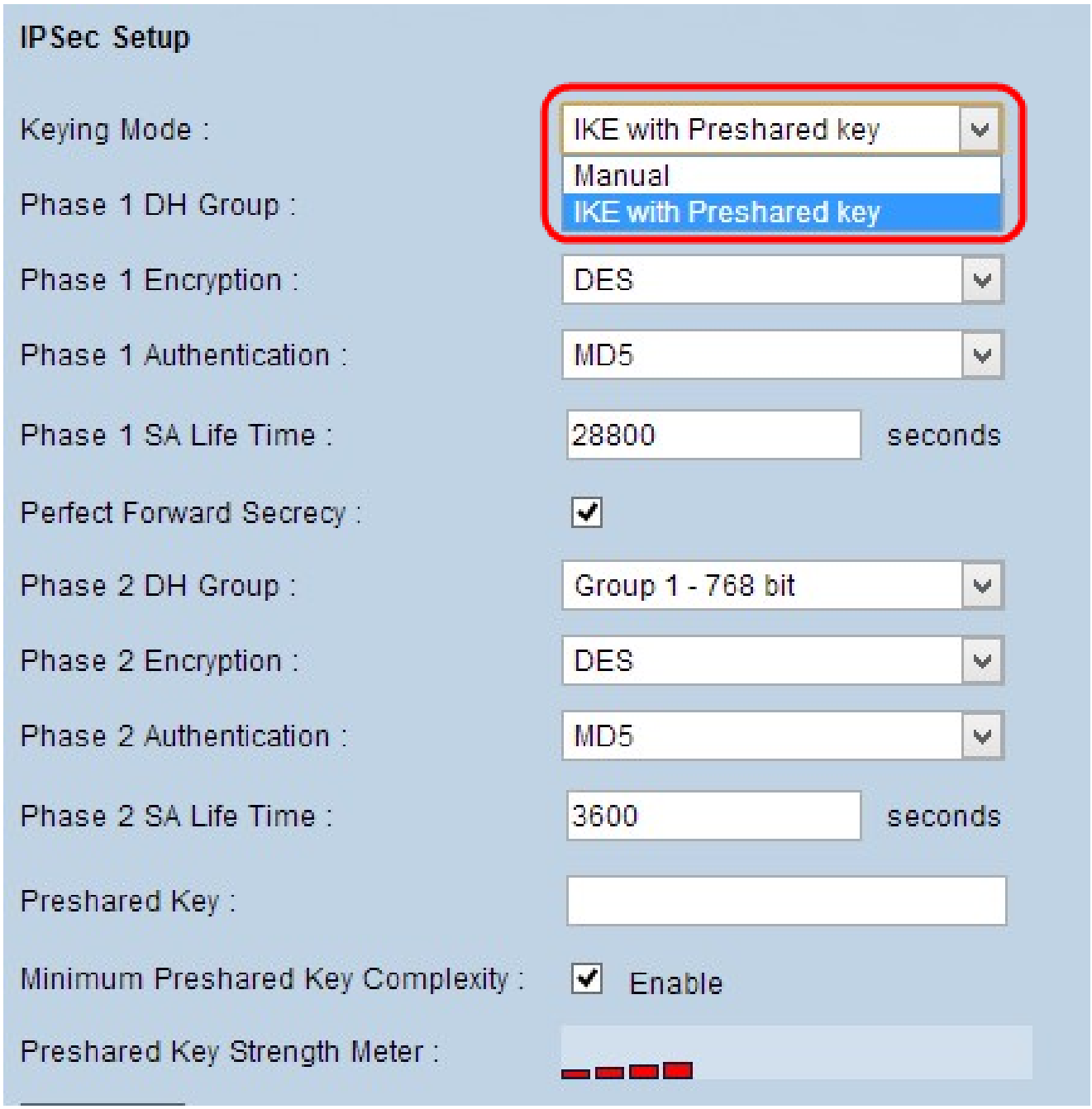
Étape 3. Cliquez sur Save pour enregistrer les paramètres.

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 l'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 fonctionner correctement. Entrez les mêmes paramètres de configuration IPSec pour les deux routeurs.

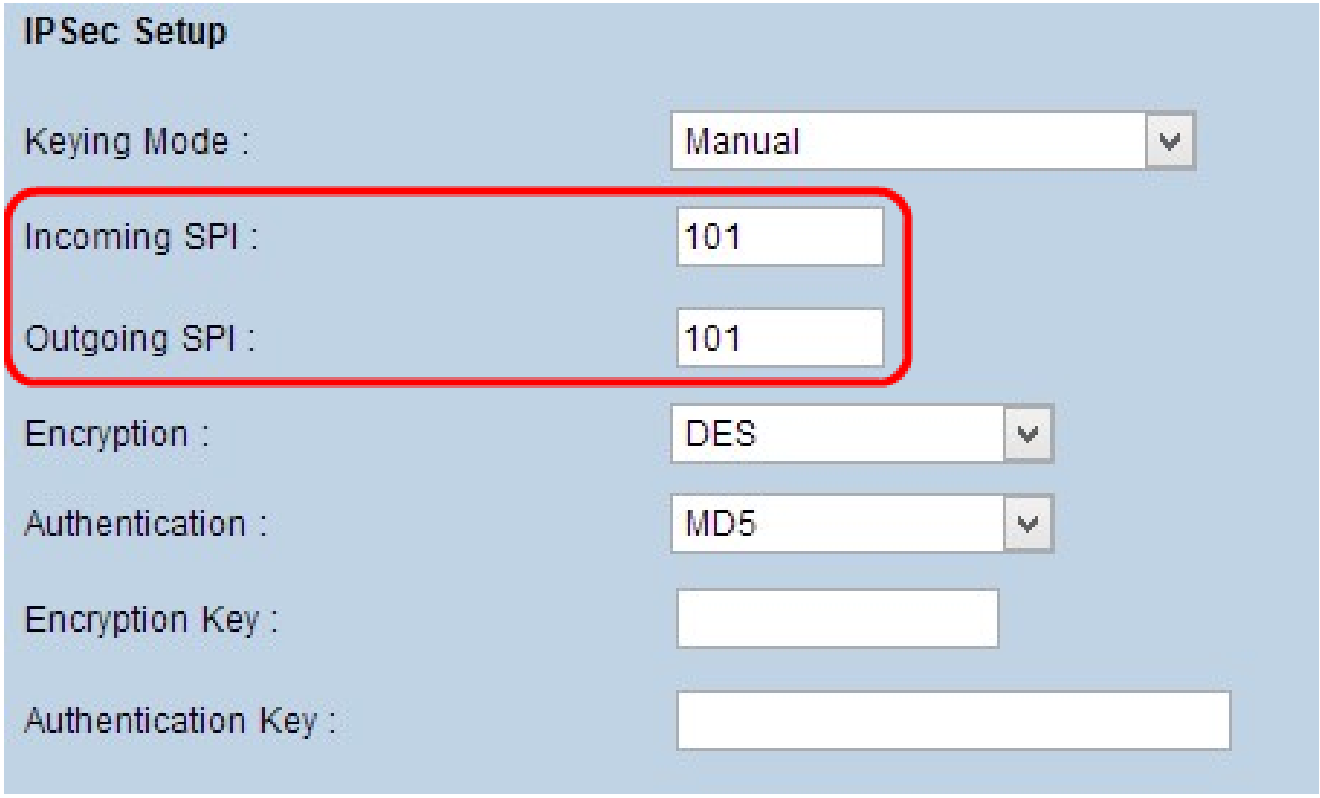


Étape 1. Sélectionnez le mode de gestion des clés approprié pour garantir la sécurité dans la liste déroulante Mode de frappe. Le mode par défaut IKE with Preshared key.

· Manuel — Mode de sécurité personnalisé pour générer une nouvelle clé de sécurité par vous-même et aucune négociation avec la clé. Il s'agit de la meilleure solution à utiliser lors du dépannage et dans un environnement statique de petite taille.

· IKE avec clé pré-partagée — Le protocole IKE (Internet Key Exchange) est utilisé pour générer et échanger automatiquement une clé pré-partagée afin d'établir une communication d'authentification pour le tunnel.

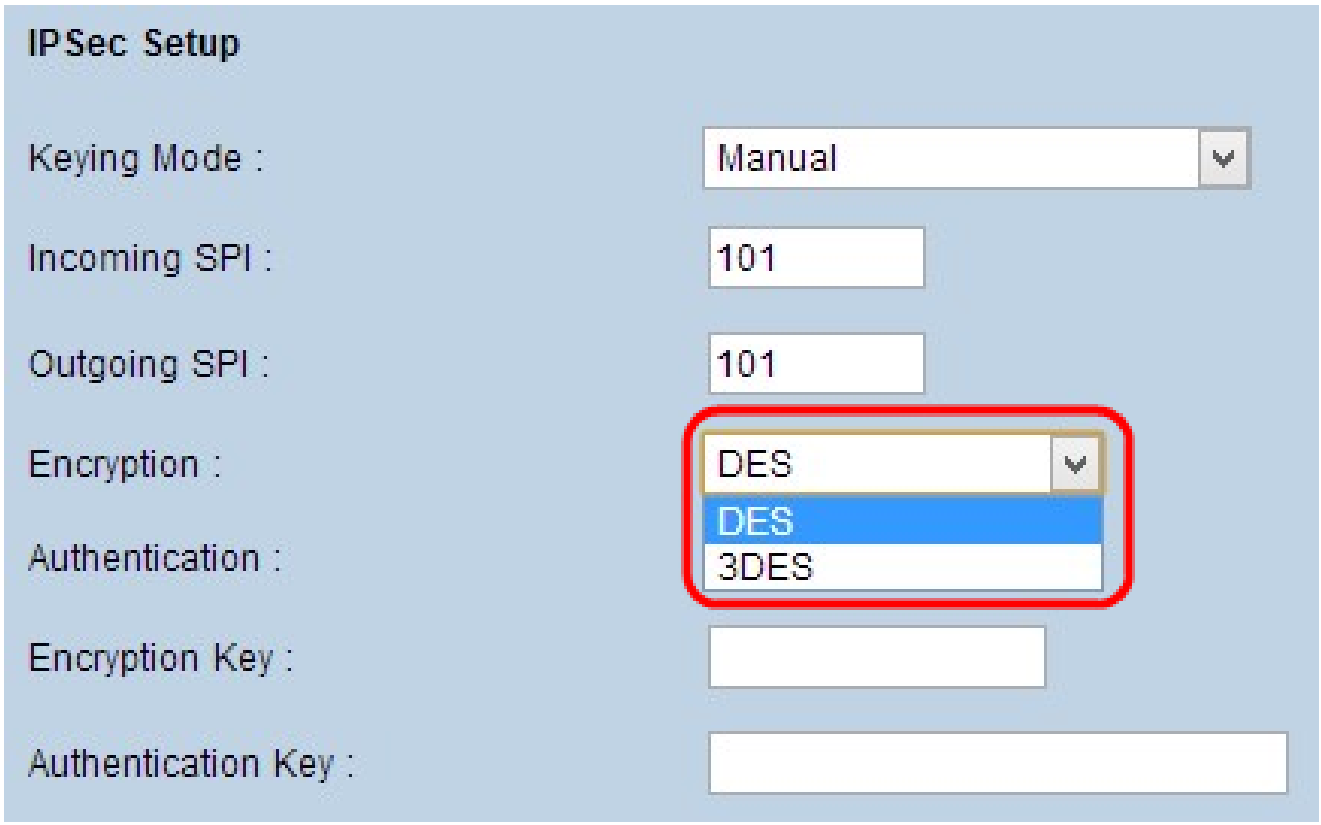
Configuration IPSec pour le mode de frappe manuelle



Étape 1. Saisissez la valeur hexadécimale unique de l'index des paramètres de sécurité (SPI) entrant dans le champ SPI entrant. SPI est transporté dans l'en-tête ESP (Encapsulating Security Payload Protocol) et détermine la protection du paquet entrant. Vous pouvez entrer une valeur comprise entre 100 et 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. Vous pouvez entrer une valeur comprise entre 100 et ffffffff. Le SPI sortant du routeur distant doit correspondre au SPI entrant du routeur local.

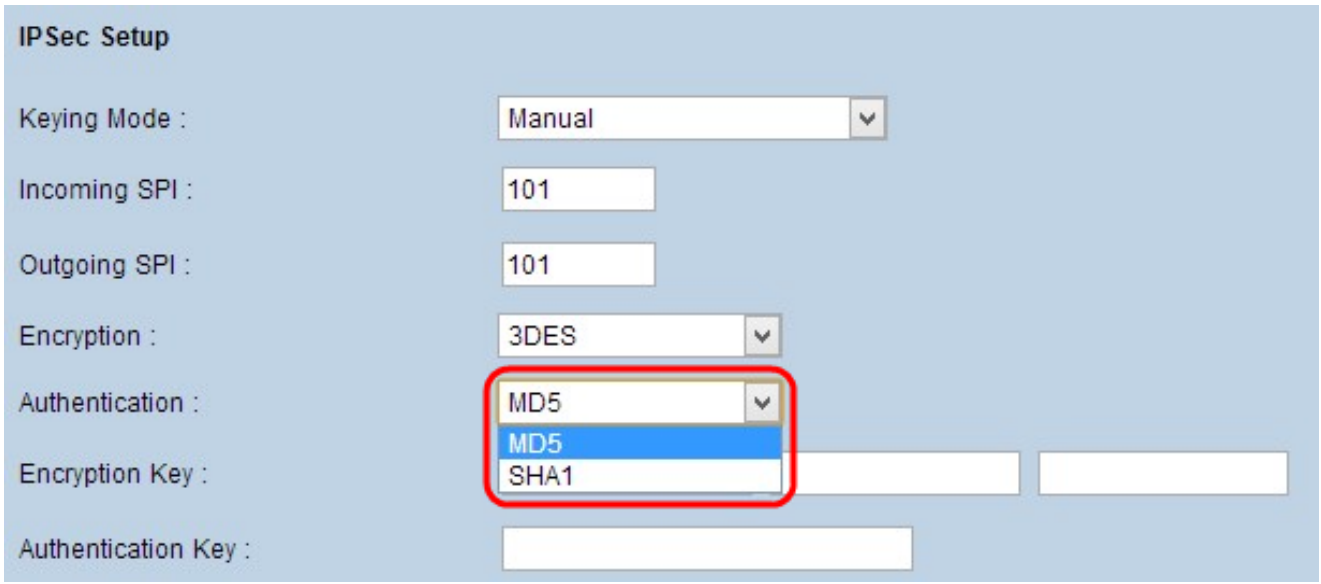
Remarque : deux tunnels ne peuvent pas avoir le même SPI.



Étape 3. Sélectionnez la méthode de cryptage appropriée pour les données dans la liste déroulante Encryption (Cryptage). Le chiffrement recommandé est 3DES. Le tunnel VPN doit utiliser la même méthode de cryptage aux deux extrémités.

· DES — Data Encryption Standard (DES) 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.

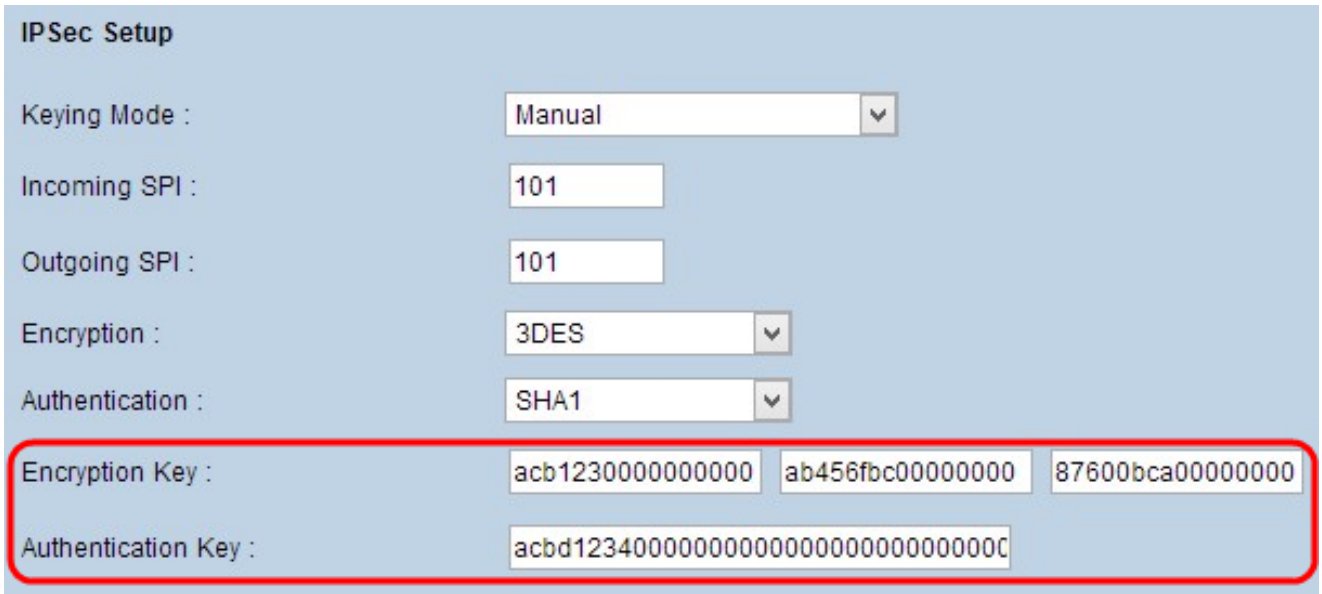
· 3DES - La norme 3DES (Triple Data Encryption Standard) est une méthode de cryptage simple de 168 bits. Le chiffrement 3DES chiffre les données trois fois, ce qui améliore la sécurité par rapport à la norme DES.



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

· MD5 — Message Digest Algorithm-5 (MD5) est une fonction de hachage de 128 bits 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.



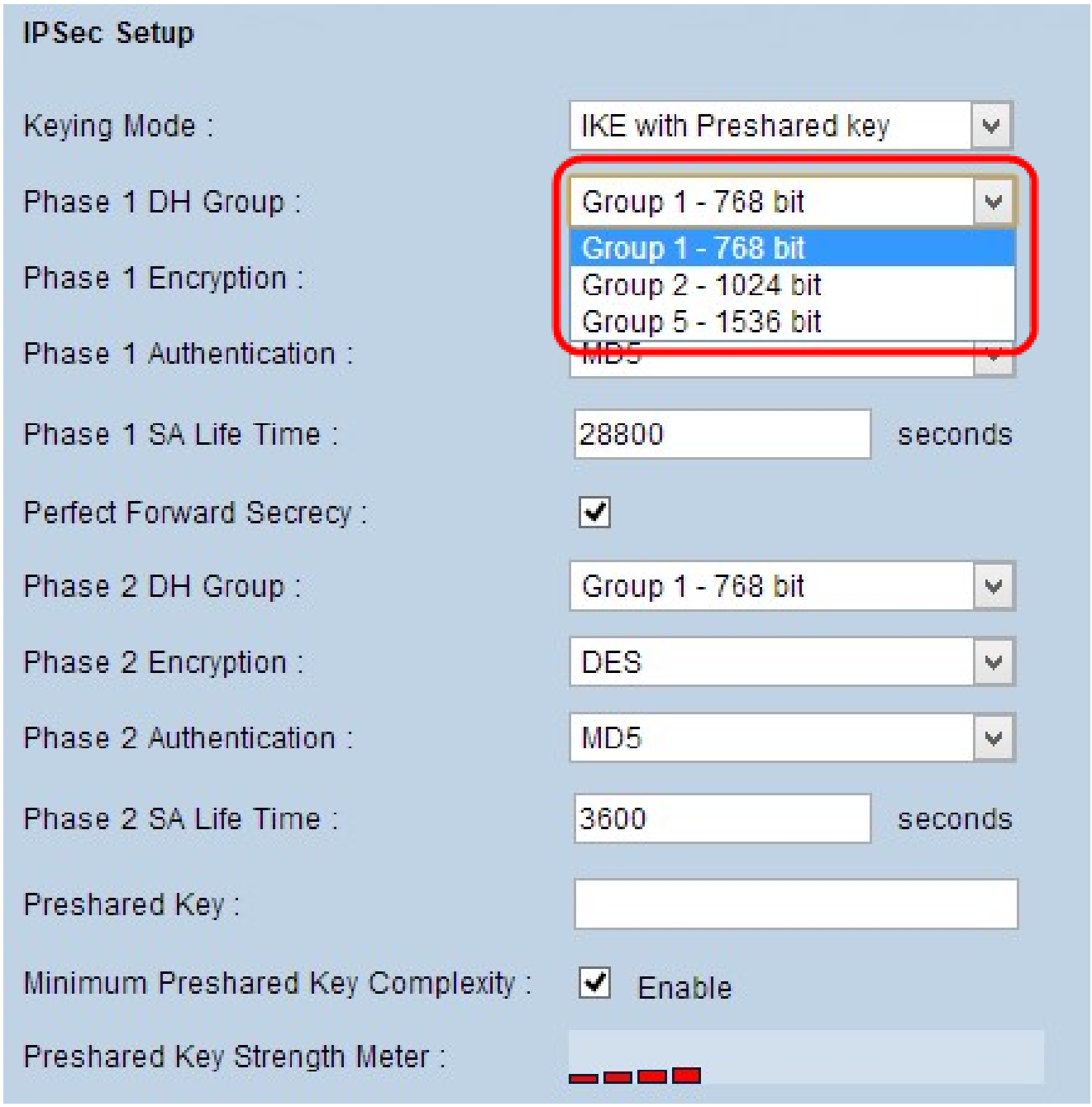
Étape 5. Saisissez la clé de chiffrement et de déchiffrement des données dans le champ Encryption Key (Clé de chiffrement). Si vous choisissez la méthode de chiffrement DES, à

l’étape 3, saisissez une valeur hexadécimale de 16 chiffres. Si vous choisissez la méthode de chiffrement 3DES, à l’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 d’authentification MD5, à l’étape 4, saisissez une valeur hexadécimale de 32 chiffres. Si vous choisissez SHA1 comme méthode d'authentification à l'étape 4, entrez une valeur hexadécimale de 40 chiffres. Si vous n'ajoutez pas assez de chiffres, des zéros seront ajoutés à la fin jusqu'à ce qu'il y ait assez de chiffres. Le tunnel VPN doit utiliser la même clé pré-partagée pour les deux extrémités.

Étape 7. Cliquez sur Save pour enregistrer les paramètres.

IKE avec configuration du mode de la clé prépartagée

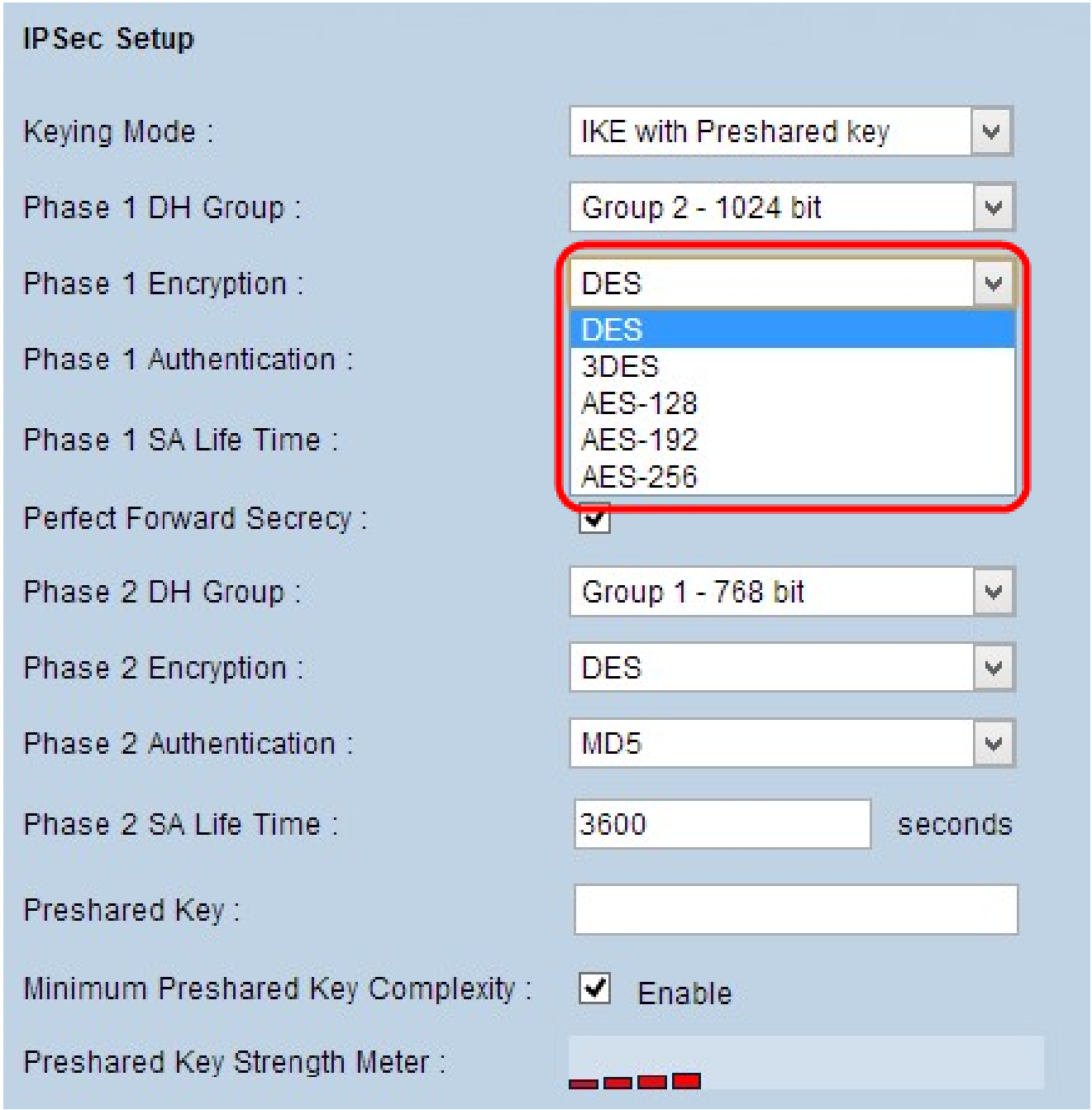


Étape 1. Sélectionnez le groupe DH de phase 1 approprié dans la liste déroulante Groupe DH de phase 1. La phase 1 est utilisée pour établir le simplex, l'association de sécurité logique (SA) entre les deux extrémités du tunnel afin de prendre en charge la communication sécurisée de l'authentification. Le protocole Diffie-Hellman (DH) est un protocole d'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 la moins puissante et le groupe d'authentification le moins sécurisé, mais dont le calcul des clés IKE prend le moins de temps. Cette option est préférable si le débit du réseau est faible.

· Groupe 2 - 1024 bits - Clé de plus grande puissance et groupe d'authentification plus sécurisé que le groupe 1, mais le calcul des clés IKE prend plus de temps.

· Groupe 5 - 1536 bits - Clé de plus grande puissance et groupe d'authentification le plus sécurisé. Il faut plus de temps pour calculer les clés IKE. Cette option est préférable si le débit du réseau est élevé.



Étape 2. Sélectionnez le chiffrement de phase 1 approprié pour chiffrer la clé dans la liste déroulante Chiffrement de phase 1. AES-128, AES-192 ou AES-256 sont recommandés. Le tunnel VPN doit utiliser la même méthode de chiffrement pour ses deux extrémités.

· DES — Data Encryption Standard (DES) utilise une taille de clé de 56 bits pour le

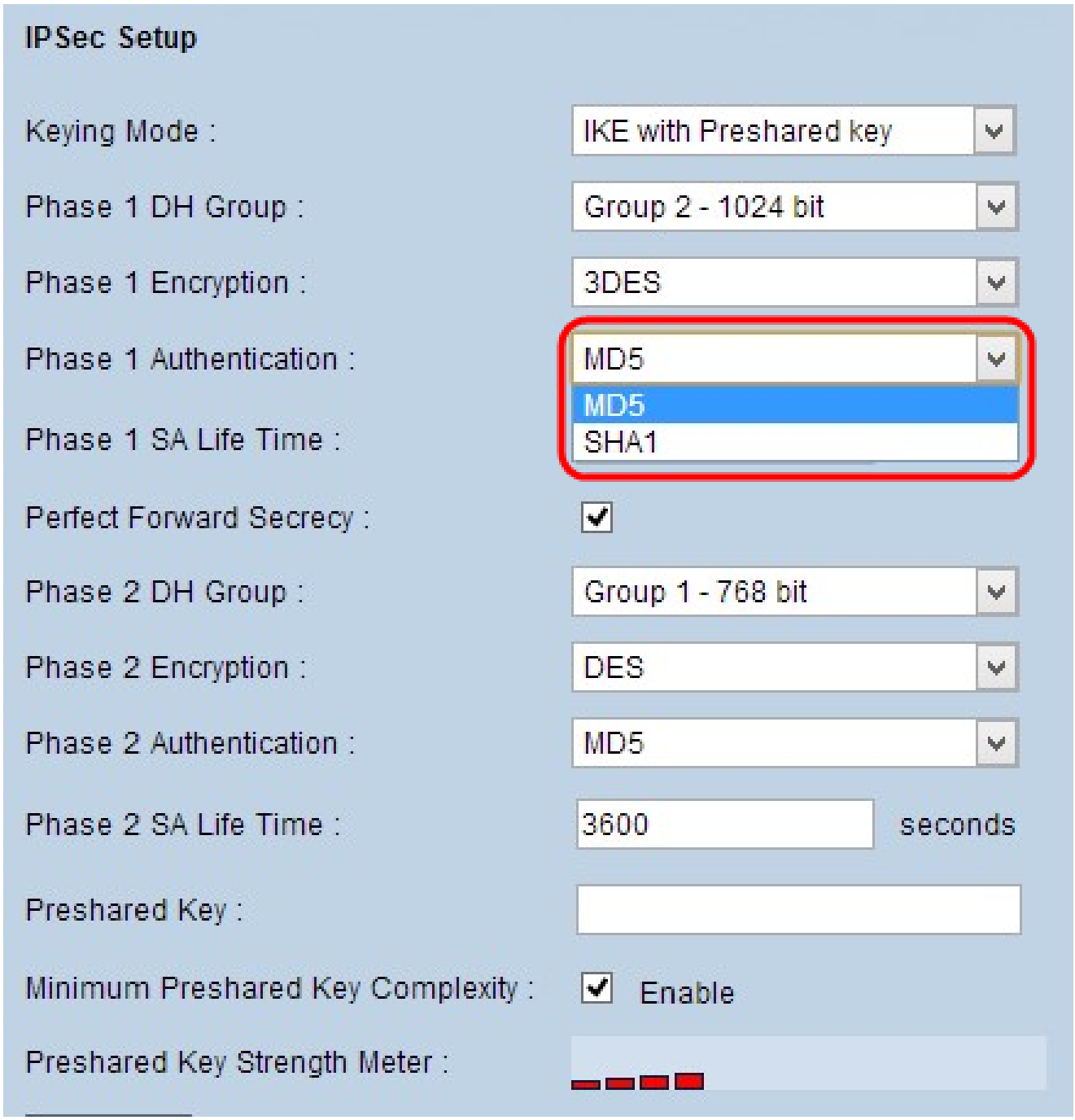
cryptage des données. DES est obsolète et ne doit être utilisée que si un terminal prend uniquement en charge cette norme.

· 3DES - 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 à 192 bits qui transforme le texte brut en texte chiffré par 12 cycles de répétition. AES-192 est plus sécurisée que AES-128.

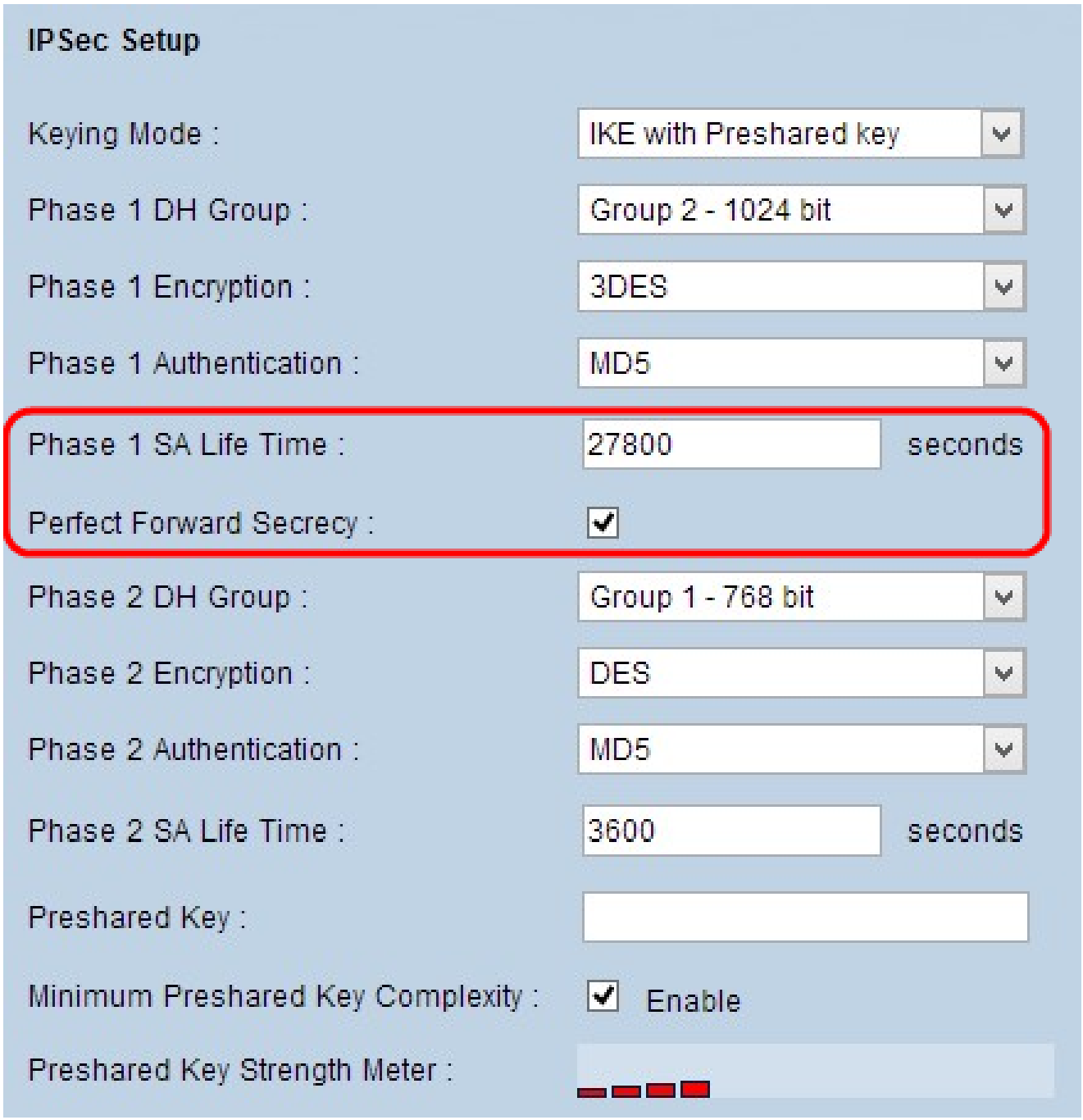
· AES-256 - Advanced Encryption Standard (AES) est une méthode de cryptage à 256 bits qui transforme le texte brut en texte chiffré par 14 cycles de répétition. AES-256 est la méthode de chiffrement la plus sécurisée.



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 d'authentification pour ses deux extrémités. SHA1 est recommandé.

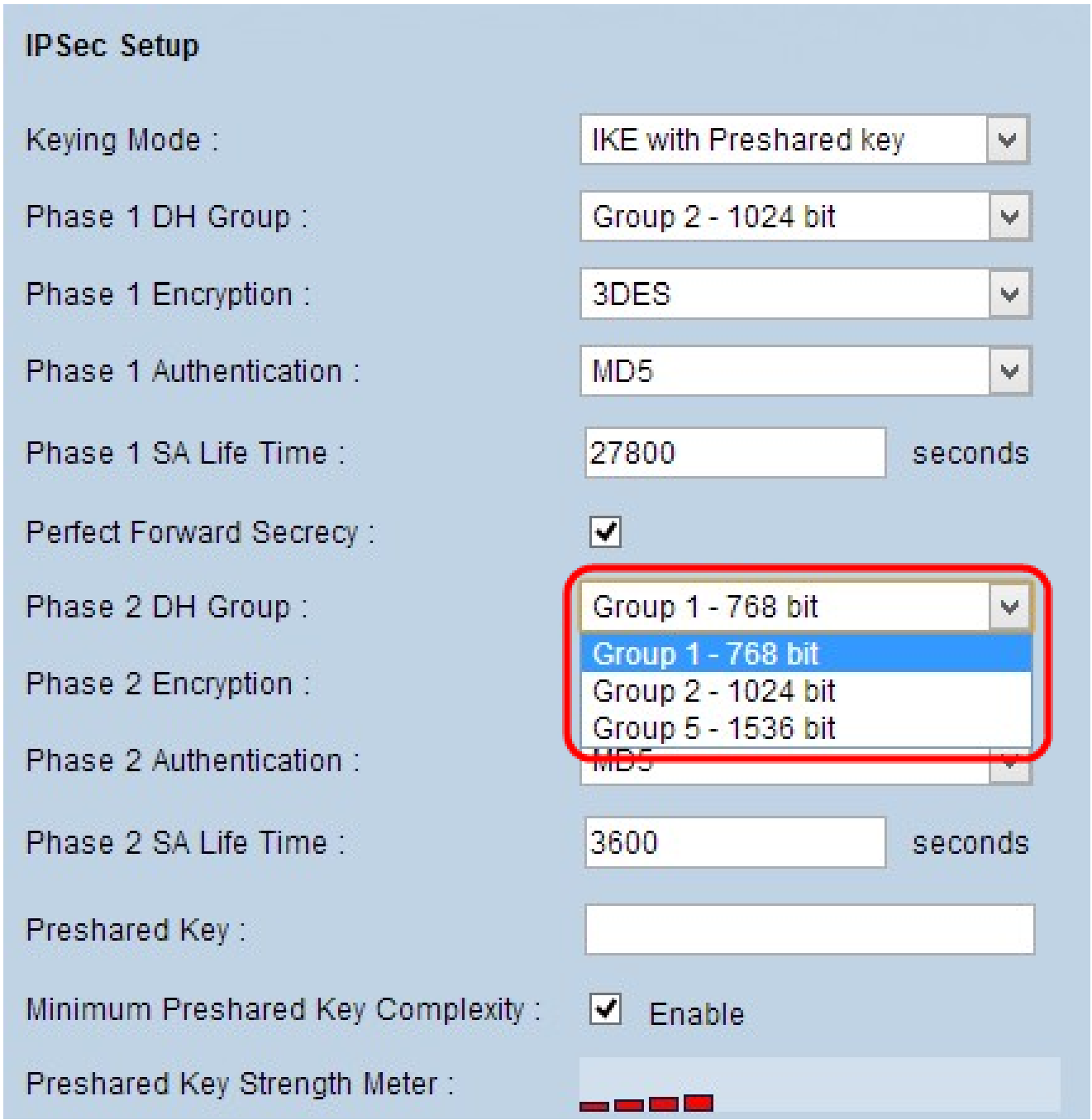
· MD5 — Message Digest Algorithm-5 (MD5) est une fonction de hachage de 128 bits qui protège les données contre les attaques malveillantes par le calcul de la somme de contrôle.

· 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 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. Il s'agit d'une action recommandée, car elle fournit plus de sécurité.

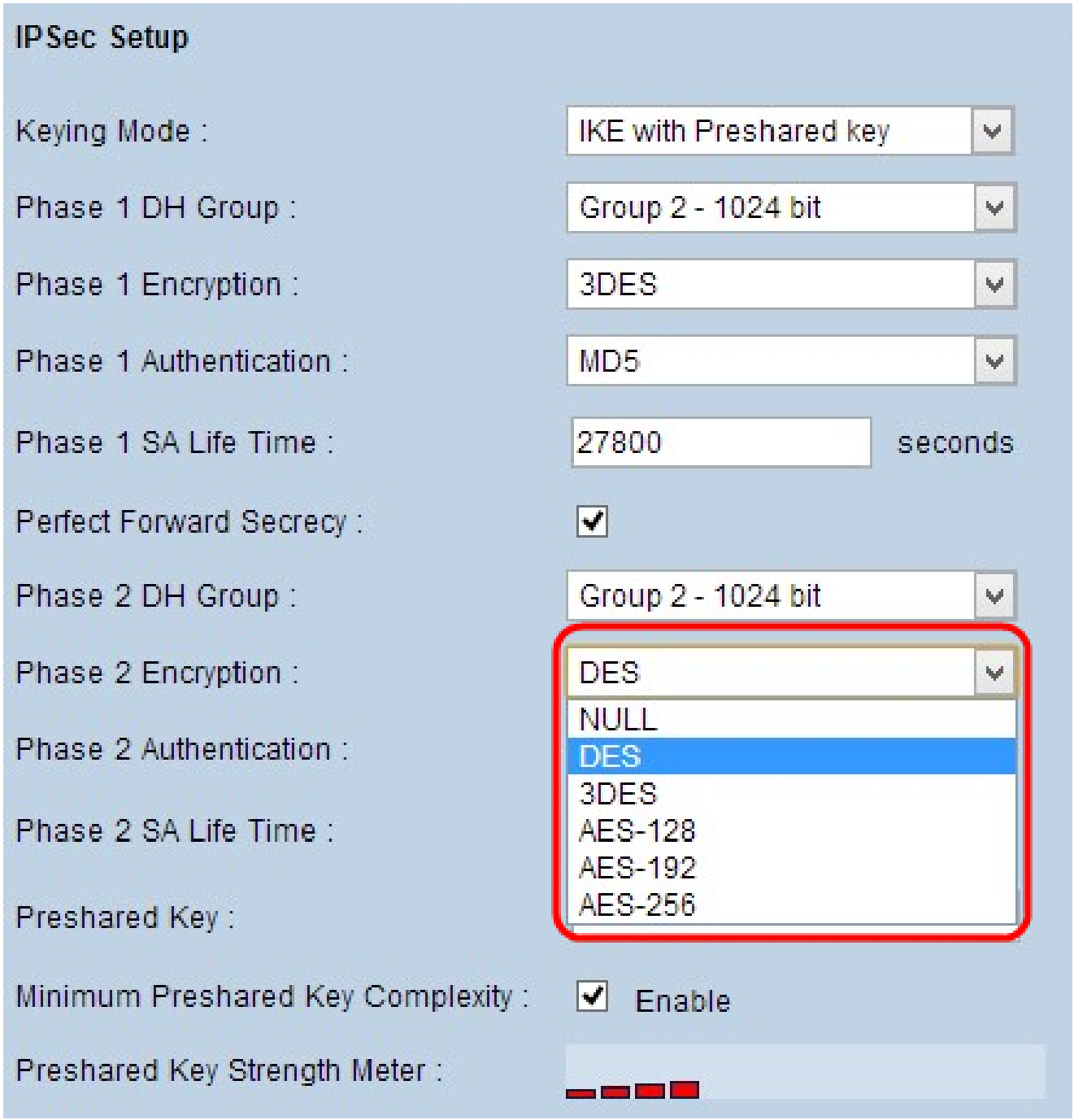


Étape 6. Sélectionnez le groupe DH de phase 2 approprié dans la liste déroulante Groupe DH de phase 2. La phase 2 utilise l'association de sécurité et permet de déterminer la sécurité du paquet de données lorsqu'il passe par les deux points d'extrémité.

· Groupe 1 - 768 bits : la clé de plus faible puissance et le groupe d'authentification le moins sécurisé, mais le calcul des clés IKE prend le moins de temps. Cette option est préférable si le débit du réseau est faible.

· Groupe 2 - 1024 bits - Clé de plus grande puissance et groupe d'authentification plus sécurisé que le groupe 1, mais le calcul des clés IKE prend plus de temps.

· Groupe 5 - 1536 bits - Clé de plus grande puissance et groupe d'authentification le plus sécurisé. Il faut plus de temps pour calculer les clés IKE. Cette option est préférable si le débit du réseau est élevé.



Étape 7. Sélectionnez le chiffrement de phase 2 approprié pour chiffrer la clé dans la liste déroulante Chiffrement de phase 2. AES-128, AES-192 ou AES-256 sont recommandés. Le tunnel VPN doit utiliser la même méthode de chiffrement pour ses deux extrémités.

· NULL : aucun chiffrement n'est utilisé.

· DES — Data Encryption Standard (DES) utilise une taille de clé de 56 bits pour le

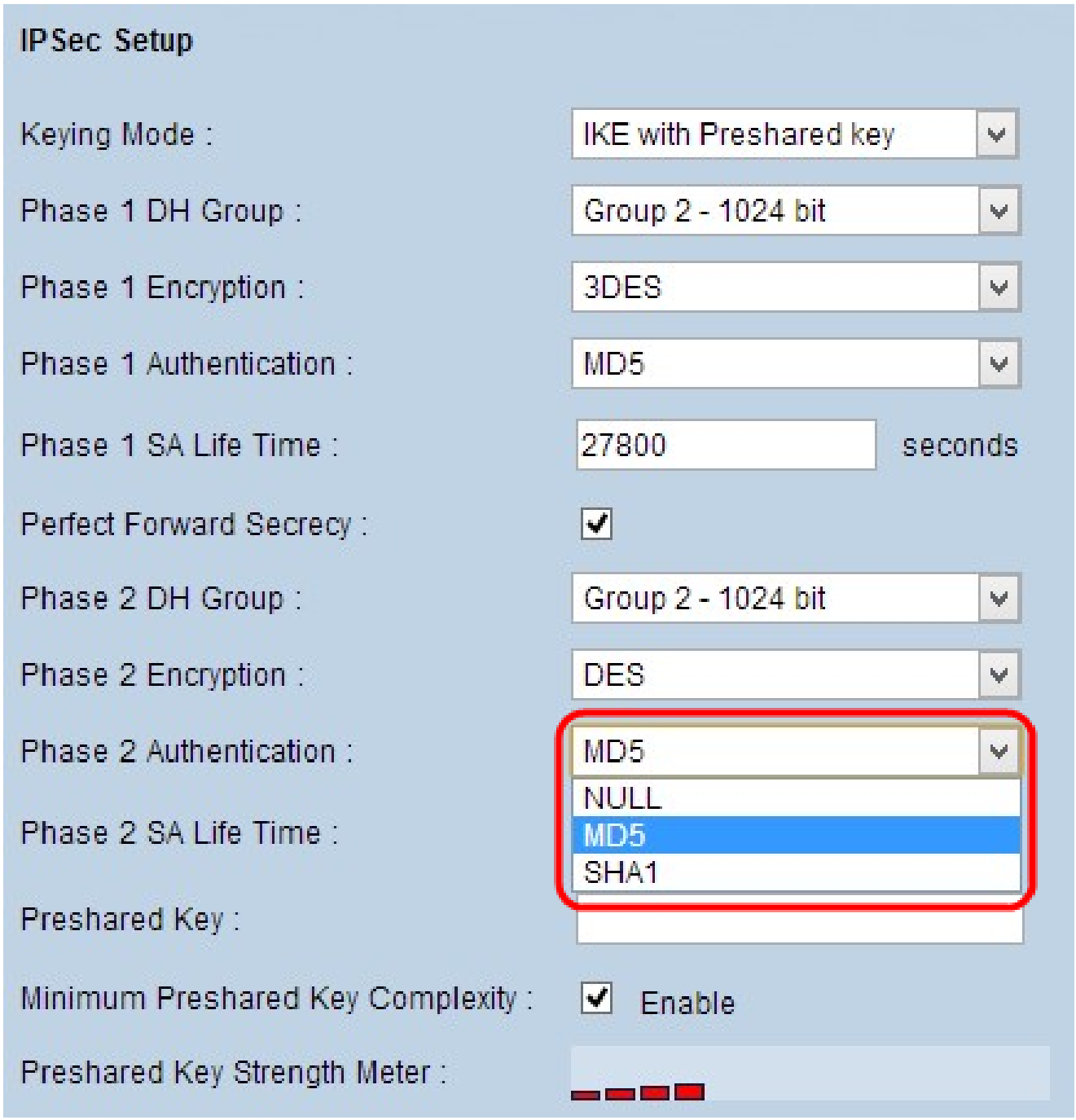
cryptage des données. DES est obsolète et ne doit être utilisée que si un terminal prend uniquement en charge cette norme.

· 3DES - 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 sécurisé que AES-128.

· AES-256 - Advanced Encryption Standard (AES) est une méthode de cryptage à 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.

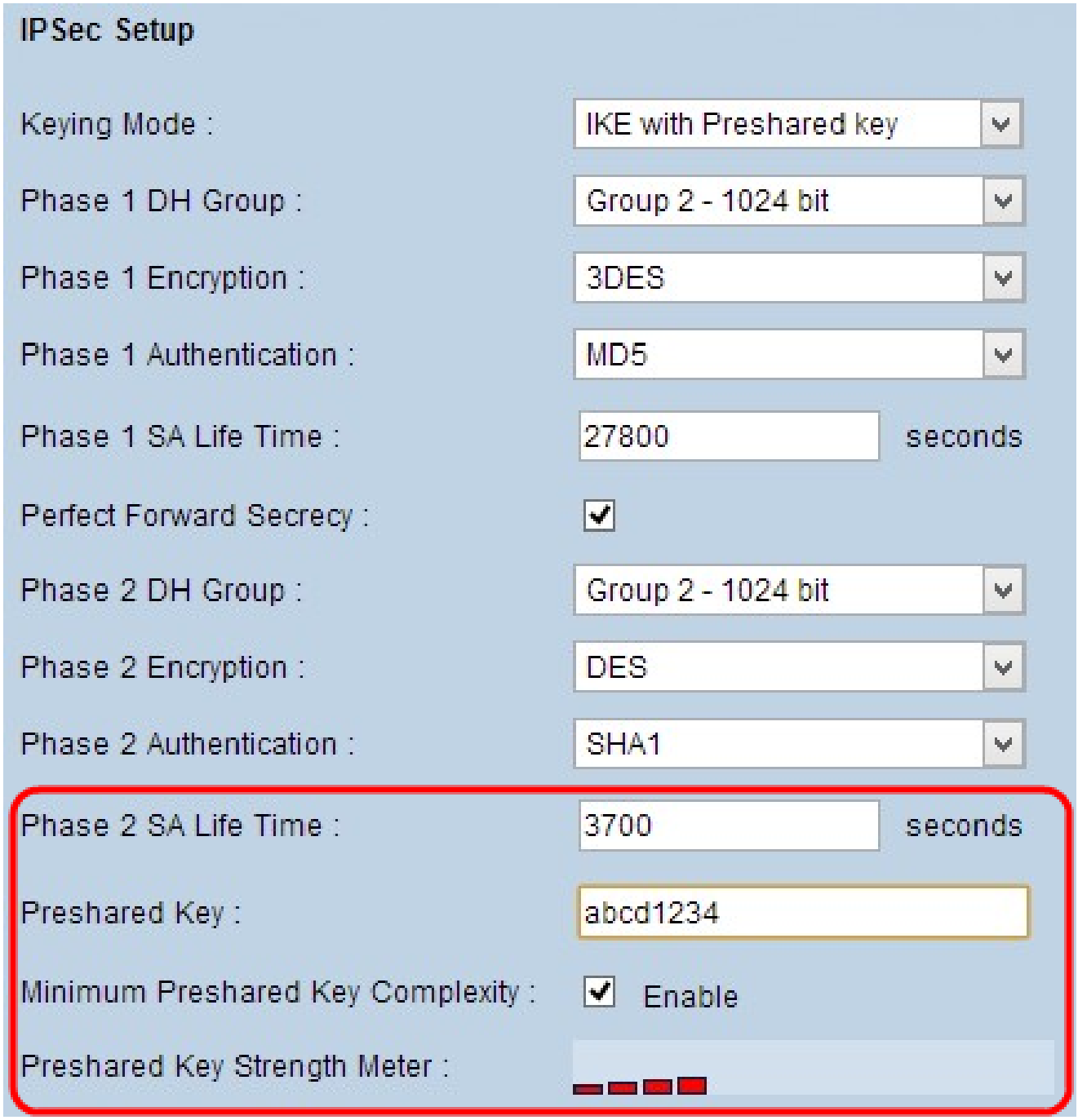


Étape 8. Sélectionnez la méthode d'authentification appropriée dans la liste déroulante Phase 2 Authentication. Le tunnel VPN doit utiliser la même méthode d'authentification pour ses deux extrémités. SHA1 est recommandé.

· MD5 — Message Digest Algorithm-5 (MD5) est une fonction de hachage hexadécimal de 128 bits 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.

· Null : aucune méthode d'authentification n'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 a été partagée précédemment entre les homologues IKE pour authentifier les homologues dans le champ Clé pré-partagée. Il est possible d'utiliser jusqu'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. (Facultatif) Si vous souhaitez activer la jauge de puissance pour la clé pré-partagée, cochez la case Complexité minimale de la clé pré-partagée. Il permet de déterminer la puissance de la clé pré-partagée à l'aide de barres de couleur.

· Preshared Key Strength Meter : indique la force de la clé prépartagée à l'aide de barres colorées. Le rouge indique une résistance faible, le jaune indique une résistance acceptable et le vert indique une résistance forte.

Étape 12. Cliquez sur Save pour enregistrer les paramètres.

Remarque : si vous souhaitez configurer les options disponibles dans la section Advanced pour Gateway to Gateway VPN, reportez-vous à l'article Configure Advanced Settings for Gateway to Gateway VPN 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.