Configuration d'un seul client vers un réseau privé virtuel de passerelle (VPN) sur les gammes de routeurs RV320 et RV325 VPN

Objectif

L'objectif de ce document est de vous montrer comment configurer un client unique pour la passerelle VPN (Virtual Private Network) sur les routeurs VPN de la gamme RV32x.

Introduction

Un VPN est un réseau privé utilisé pour connecter virtuellement un utilisateur distant via un réseau public. Un type de VPN est un VPN client-passerelle. Un VPN client-passerelle est une connexion entre un utilisateur distant et le réseau. Le client est configuré dans le périphérique de l'utilisateur avec le logiciel client VPN. Il permet aux utilisateurs de se connecter à distance à un réseau en toute sécurité.

Périphériques pertinents

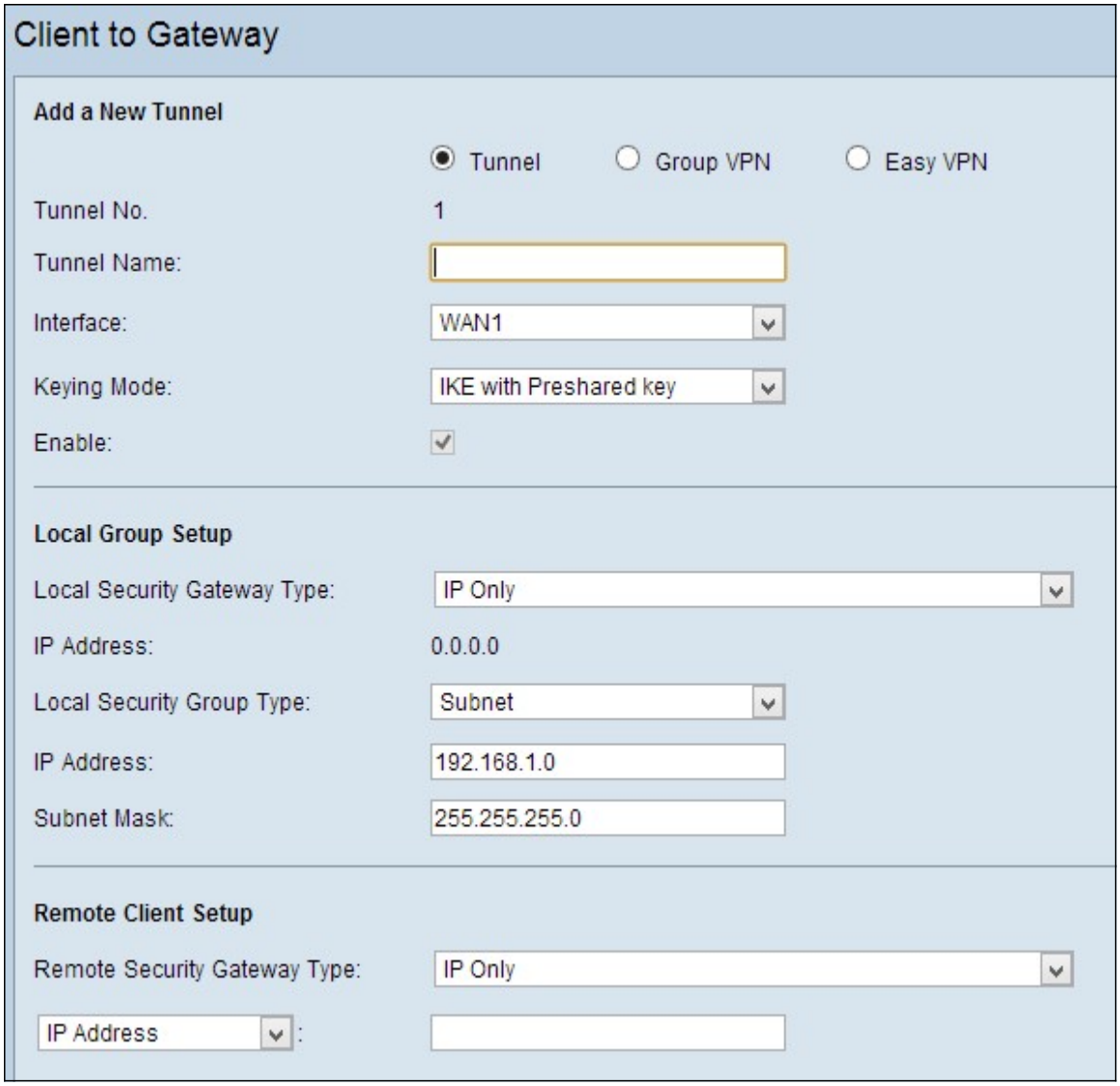
- Routeur VPN double WAN RV320
- Routeur VPN double WAN Gigabit RV325

Version du logiciel

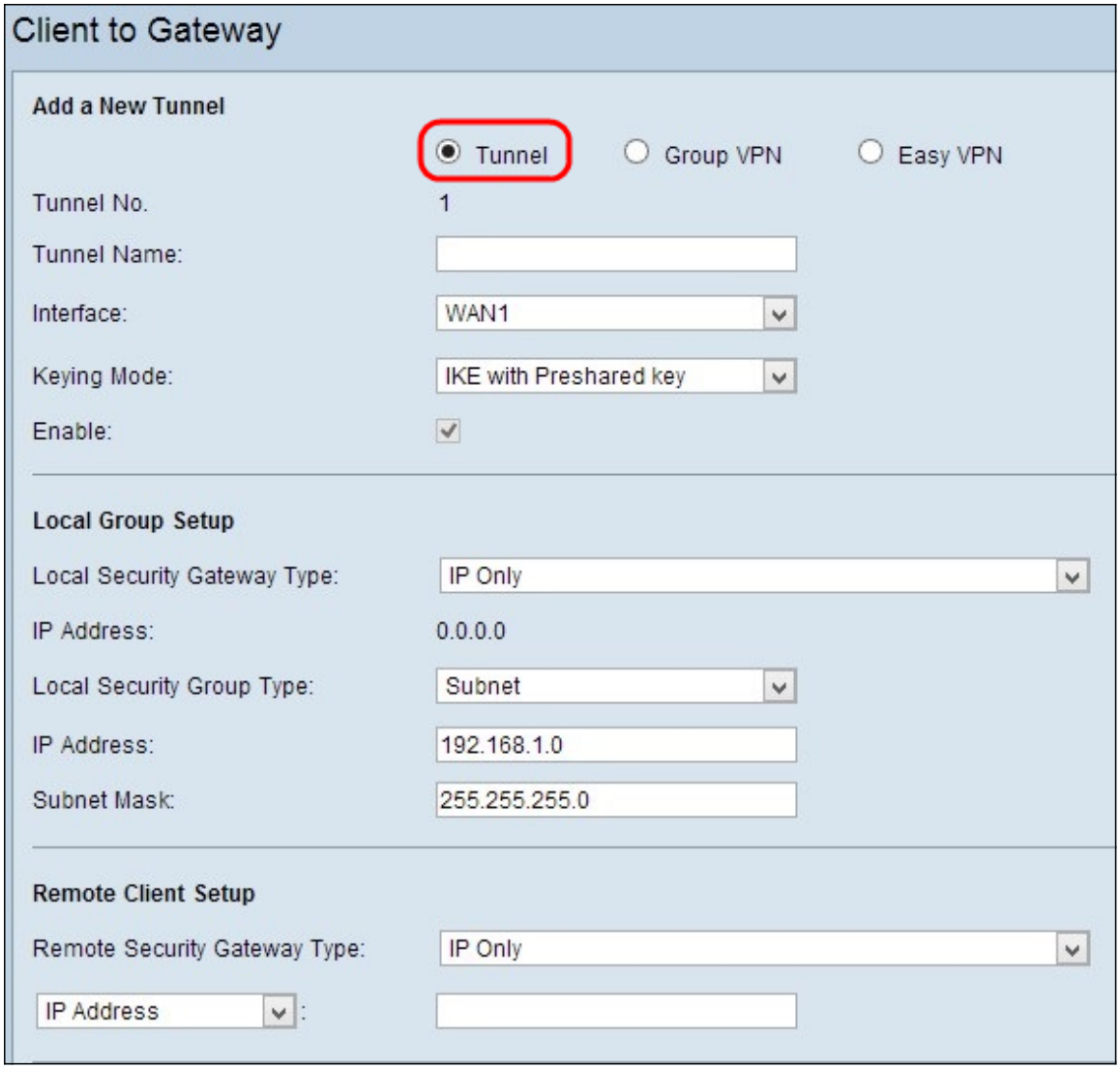
- v 1.1.0.09

Configuration d'un client unique vers un VPN de passerelle

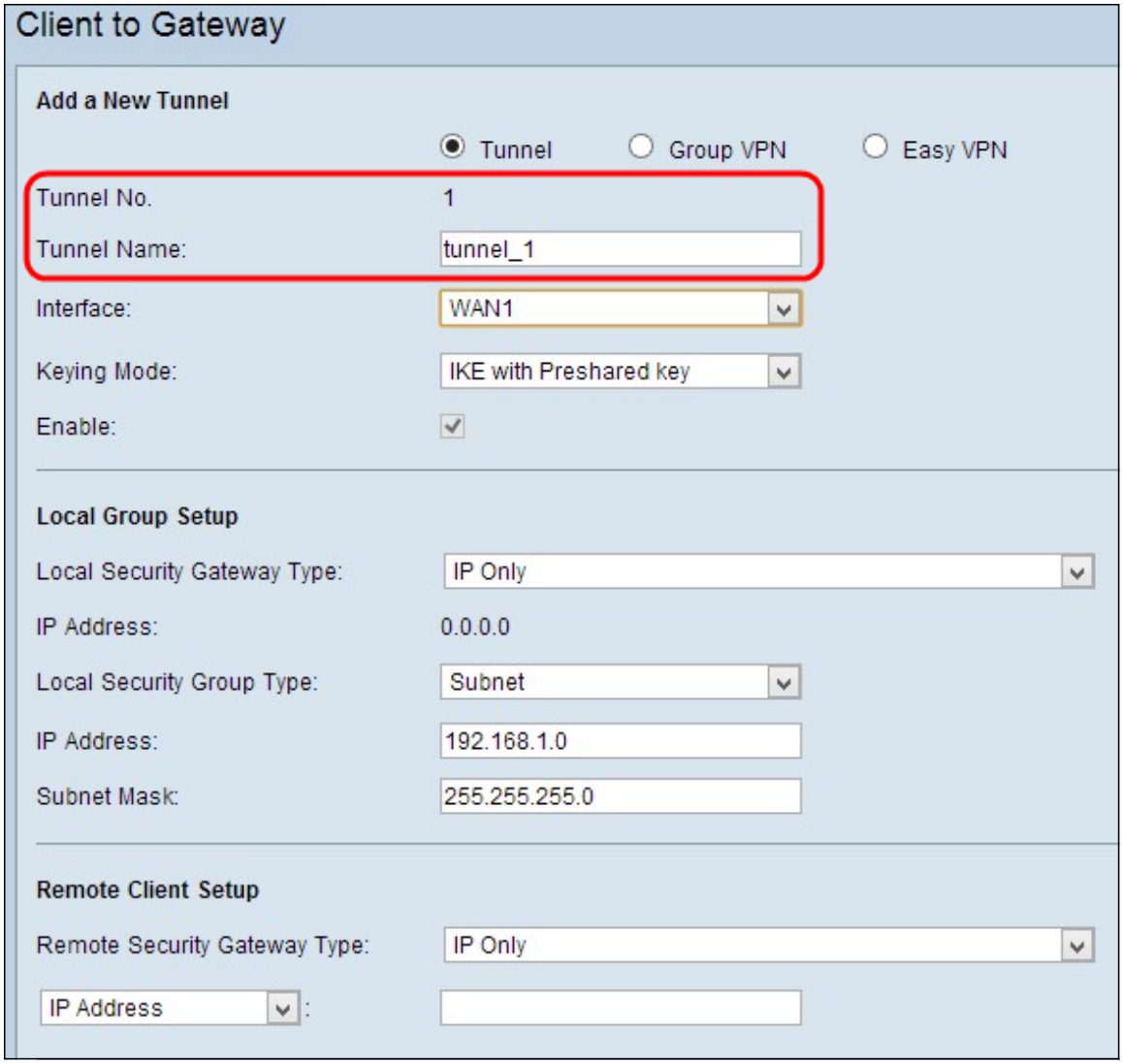
Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez **VPN > Client to Gateway**. La *page Client to Gateway s'ouvre :*



Étape 2. Cliquez sur la case d'option **Tunnel** pour ajouter un tunnel unique pour le VPN client à passerelle.



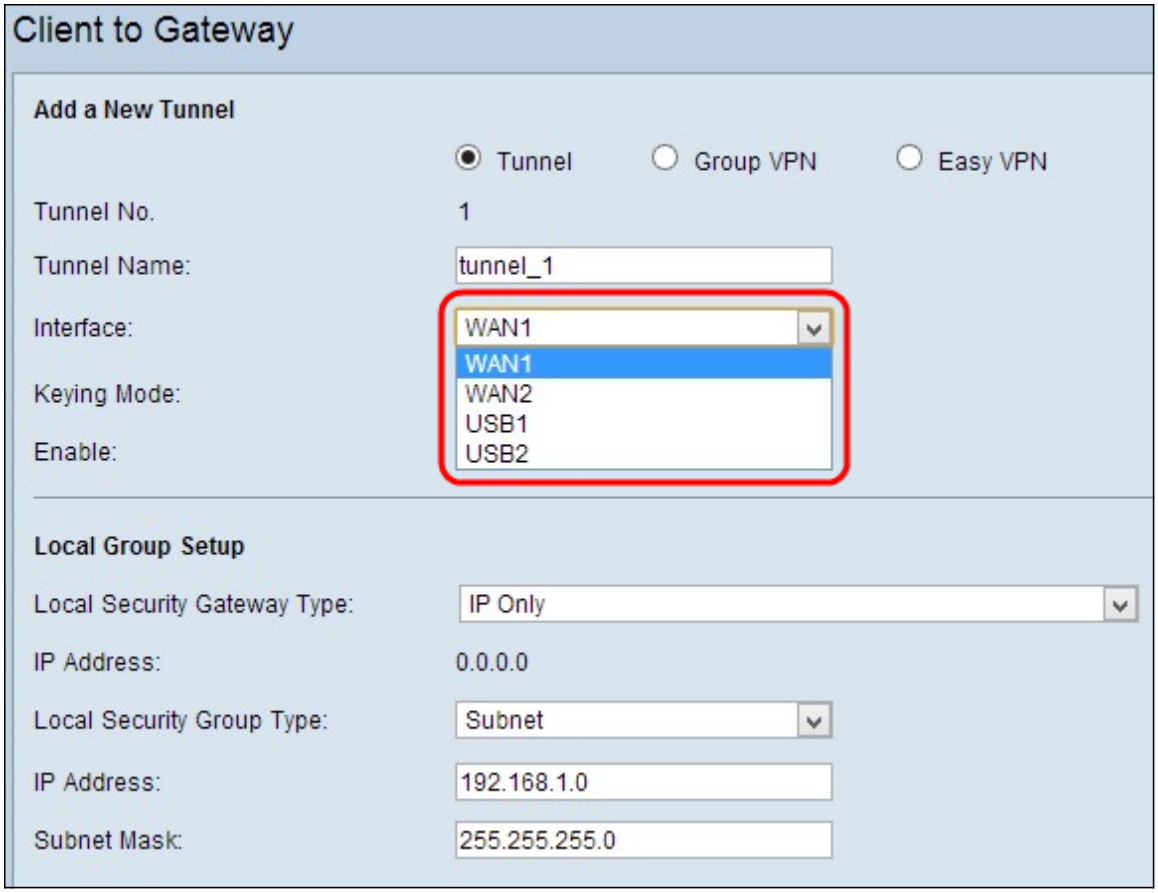
Ajouter un nouveau tunnel



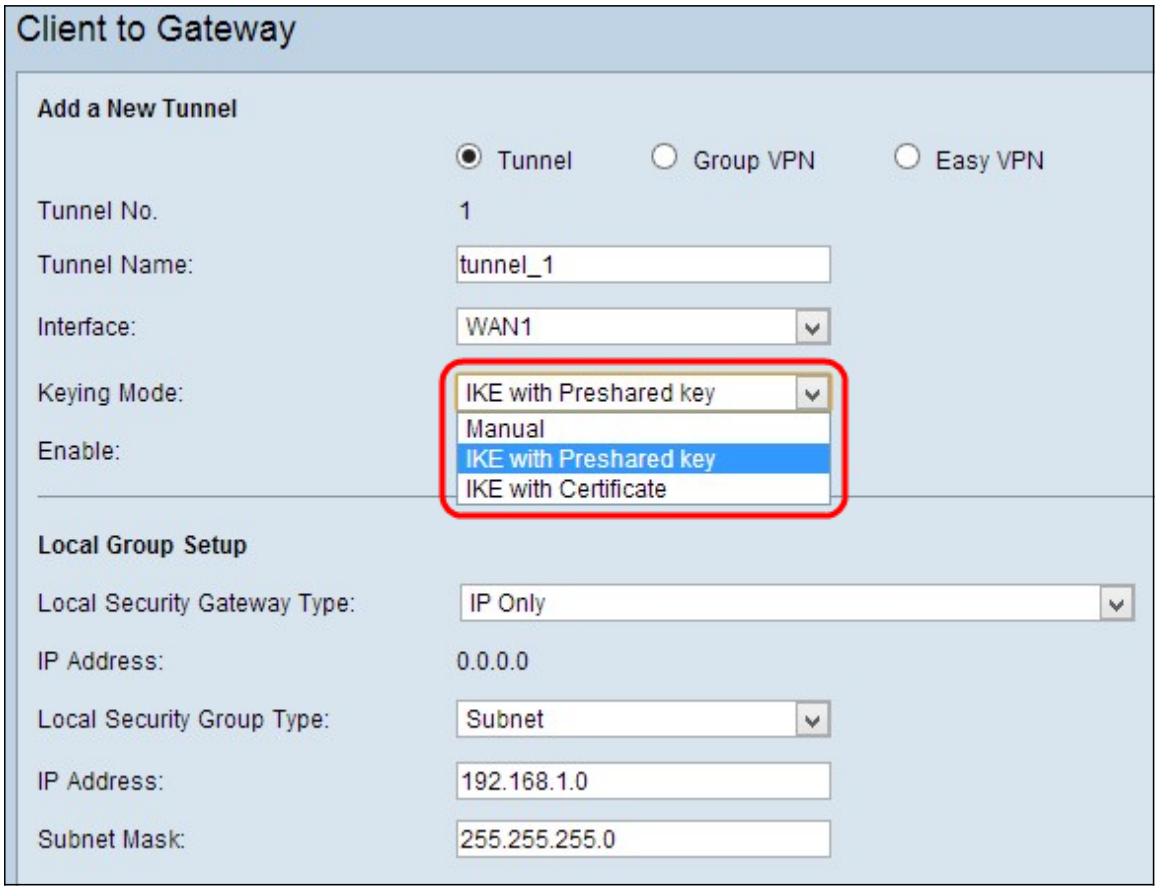
Note: Tunnel No : représente le numéro du tunnel. Ce numéro est généré automatiquement.

Étape 1. Entrez le nom du tunnel dans le champ *Nom du tunnel*.

Étape 2. Choisissez l'interface par laquelle le client distant accède au VPN dans la liste déroulante *Interface*.



Étape 3. Choisissez le mode de gestion des clés approprié pour assurer la sécurité dans la liste déroulante *Mode de clé*. Le mode par défaut IKE with Preshared key.



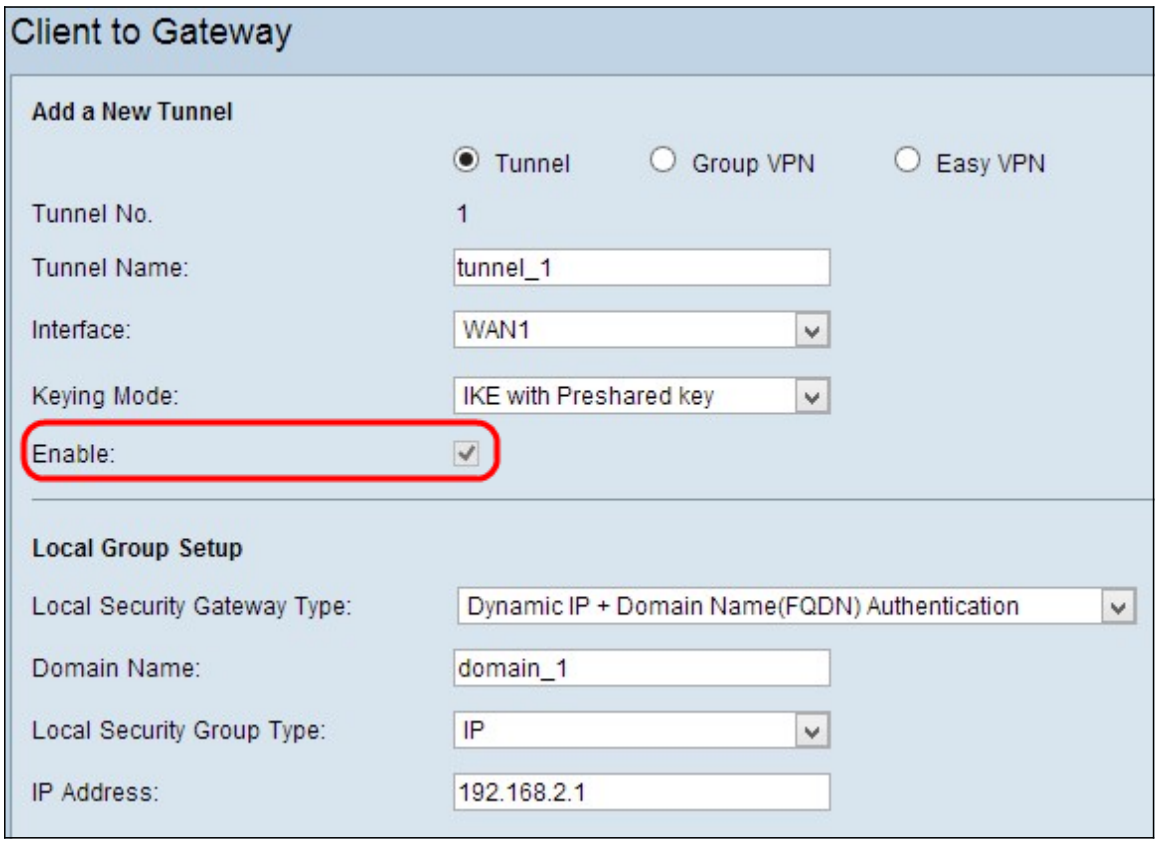
Les options sont définies comme suit :

- Manual (Manuel) : mode de sécurité personnalisé permettant de générer une nouvelle clé de

sécurité par vous-même et de ne pas négocier avec la clé. Il est préférable de l'utiliser lors du dépannage ou dans un petit environnement statique.

- IKE avec clé prépartagée : le protocole IKE (Internet Key Exchange) est utilisé pour générer et échanger automatiquement une clé prépartagée afin d'établir une communication authentifiée pour le tunnel.
- IKE avec certificat - Le protocole IKE (Internet Key Exchange) avec certificat est une méthode plus sécurisée pour générer et échanger automatiquement des clés pré-partagées afin d'établir une communication plus sécurisée pour le tunnel.

Étape 4. Cochez la case **Activer** pour activer le VPN client-passerelle. Il est activé par défaut.



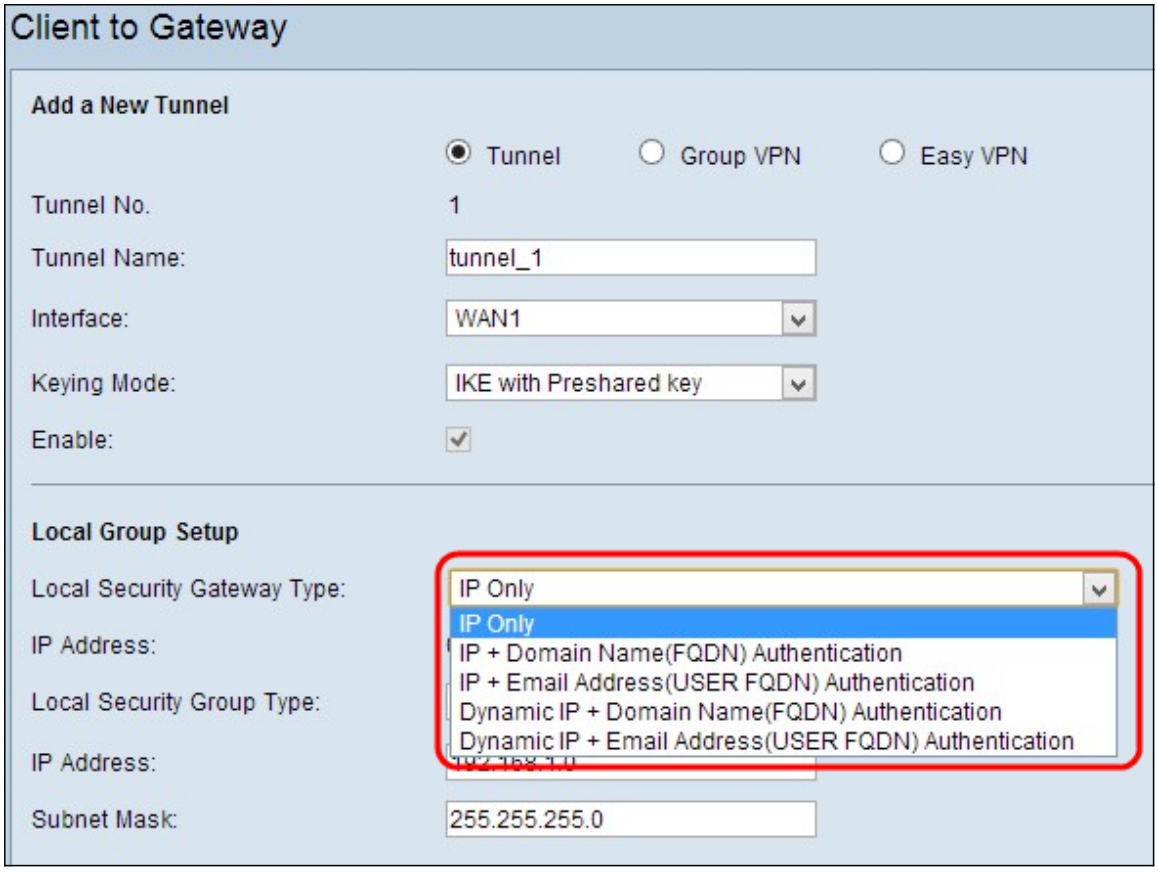
Étape 5. Si vous souhaitez enregistrer les paramètres que vous avez déjà, faites défiler la page vers le bas et cliquez sur **Enregistrer** pour enregistrer les paramètres.

Configuration du groupe local

Configuration de groupe local avec manuel ou IKE avec clé prépartagée

Note: Suivez les étapes ci-dessous si vous avez sélectionné Manual ou IKE with Preshared key dans la liste déroulante *Keying Mode* de l'étape 3 de la section *Add a New Tunnel*.

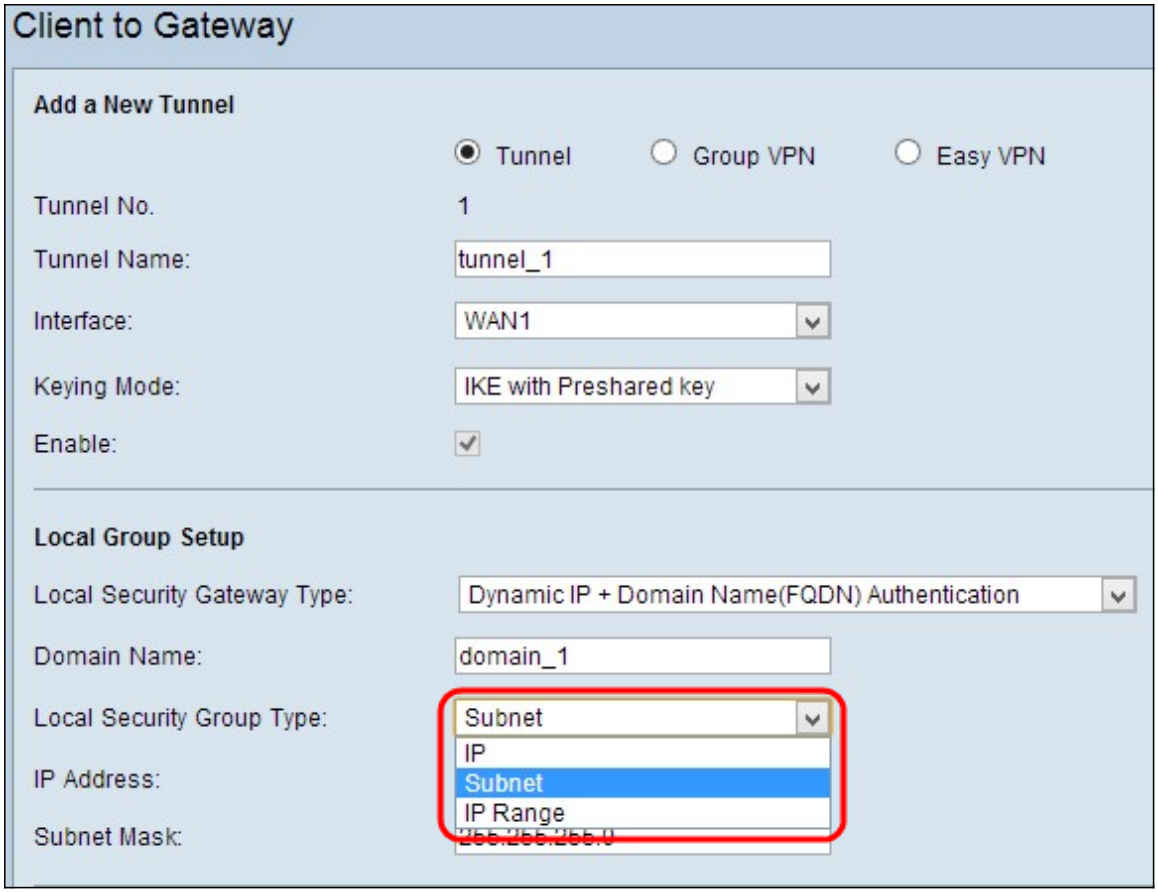
Étape 1. Choisissez la méthode d'identification de routeur appropriée dans la liste déroulante *Passerelle de sécurité locale* pour établir un tunnel VPN.



Les options sont définies comme suit :

- IP Only (IP uniquement) : l'accès au tunnel est possible via une adresse IP WAN statique uniquement. Vous pouvez choisir cette option si seul le routeur possède une adresse IP WAN statique. L'adresse IP WAN statique est générée automatiquement.
- 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 est générée automatiquement.
- Authentification IP + E-mail Addr. (USER FQDN) : 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 est générée automatiquement.
- Authentification FQDN (Dynamic IP + Domain Name) : 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).
- Authentification FQDN (Dynamic IP + E-mail Addr.) (USER FQDN) : 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.
- IP Address (Adresse IP) : adresse IP de l'interface WAN. Il s'agit d'un champ en lecture seule.

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

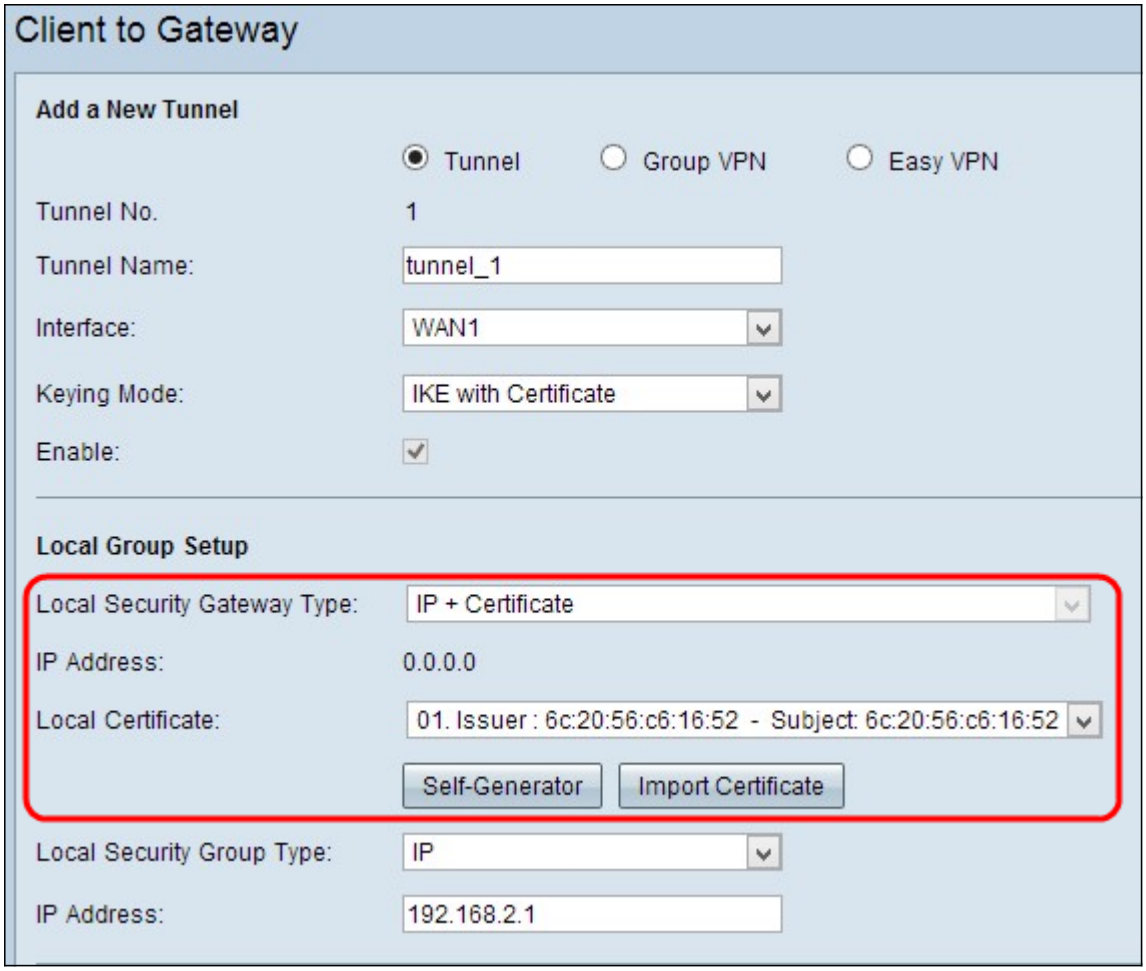


- IP : un seul périphérique LAN spécifique peut accéder au tunnel. Si vous choisissez cette option, saisissez l'adresse IP de l'appareil LAN dans le champ IP Address (adresse IP). L'adresse IP par défaut est 192.168.1.0.
- Sous-réseau : tous les périphériques LAN d'un sous-réseau spécifique peuvent accéder au tunnel. Si vous choisissez cette option, saisissez l'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.
- Plage IP : une gamme de périphériques LAN peut accéder au tunnel. Si vous choisissez cette option, entrez l'adresse IP de début et de fin dans les champs *Start IP* et *End IP* respectivement. La plage par défaut est comprise entre 192.168.1.0 et 192.168.1.254.

Étape 3. Si vous souhaitez enregistrer les paramètres que vous avez déjà, faites défiler la page vers le bas et cliquez sur **Enregistrer** pour enregistrer les paramètres.

Configuration de groupe local avec IKE avec certificat pour VPN de tunnel

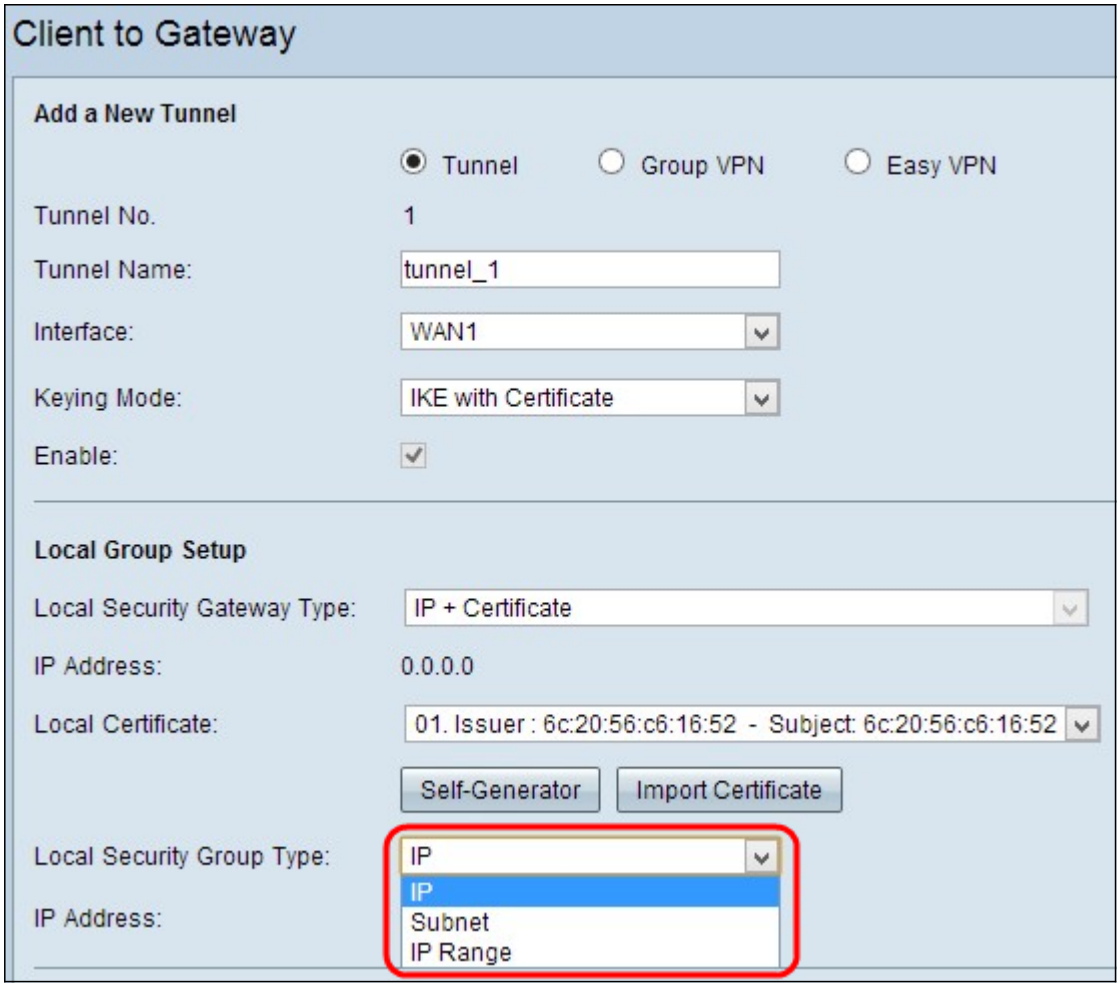
Note: Suivez les étapes ci-dessous si vous avez sélectionné IKE with Certificate dans la liste déroulante *Keying Mode* de l'étape 3 de la section *Add a New Tunnel*.



- Local Security Gateway Type (Type de passerelle de sécurité locale) : l'accès au tunnel est possible via IP avec un certificat.
- IP Address (Adresse IP) : adresse IP de l'interface WAN. Il s'agit d'un champ en lecture seule.

Étape 1. Choisissez le certificat local approprié pour identifier le routeur dans la liste déroulante *Certificat local*. Cliquez sur **Auto-générateur** pour générer automatiquement le certificat ou cliquez sur **Importer le certificat** pour importer un nouveau certificat.

Remarque : pour en savoir plus sur la génération automatique de certificats, reportez-vous à *Générer des certificats sur des routeurs RV320*, et pour savoir comment importer des certificats, reportez-vous à *Configurer mon certificat sur des routeurs RV320*.



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

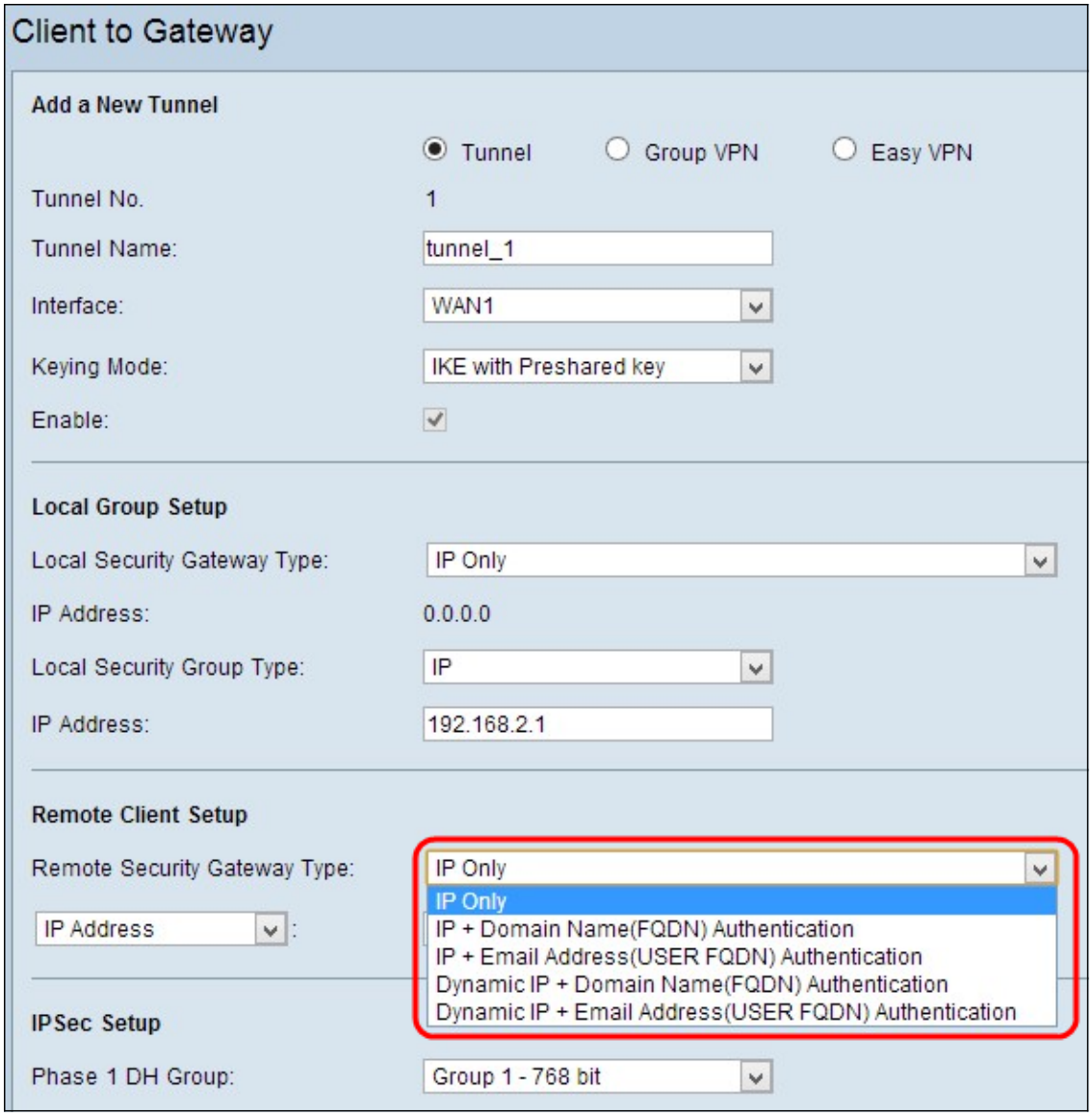
- IP : un seul périphérique LAN spécifique peut accéder au tunnel. Si vous choisissez cette option, saisissez l'adresse IP de l'appareil LAN dans le champ IP Address (adresse IP). L'adresse IP par défaut est 192.168.1.0.
- Subnet : tous les périphériques LAN d'un sous-réseau spécifique peuvent accéder au tunnel. Si vous choisissez cette option, saisissez l'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 d'appareils LAN peuvent accéder au tunnel. Si vous choisissez cette option, entrez respectivement les adresses IP de début et de fin dans les champs IP de début et IP de fin. La plage par défaut est comprise entre 192.168.1.0 et 192.168.1.254.

Étape 3. Si vous souhaitez enregistrer les paramètres que vous avez déjà, faites défiler la page vers le bas et cliquez sur **Enregistrer** pour enregistrer les paramètres.

Configuration du client distant

Configuration du client distant avec manuel ou IKE avec clé prépartagée

Remarque : suivez les étapes ci-dessous si vous avez sélectionné Manual ou IKE with Preshared Key dans la liste déroulante *Keying Mode* de l'étape 3 de la section *Add a New Tunnel*.



Étape 1. Choisissez la méthode d'identification du client appropriée pour établir un tunnel VPN dans la liste déroulante *Remote Security Gateway*. La valeur par défaut est IP Only (IP seulement).

- IP Only : l'accès au tunnel est possible via l'IP WAN statique du client seulement. Vous ne pouvez choisir cette option que si vous connaissez l'adresse IP ou le nom de domaine WAN statique du client. Choisissez IP Address dans la liste déroulante et saisissez l'adresse IP statique du client dans le champ adjacent, ou choisissez IP by DNS Resolved dans la liste déroulante et saisissez le nom de domaine de l'adresse IP dans le champ adjacent. Par l'intermédiaire du serveur DNS local de l'adresse IP, le routeur peut récupérer l'adresse IP automatiquement.

  Note: Si vous choisissez Manual dans la liste déroulante *Keying Mode* de l'étape 3 de la section Add a New Tunnel Through Tunnel ou Group VPN, ce sera la seule option disponible.

- IP + Domain Name(FQDN) Authentication : il est possible d'accéder au tunnel par le biais d'une adresse IP statique du client et d'un domaine enregistré. Si vous choisissez cette option, saisissez le nom du domaine enregistré dans le champ Domain Name (nom de domaine). Choisissez IP Address dans la liste déroulante et saisissez l'adresse IP statique du

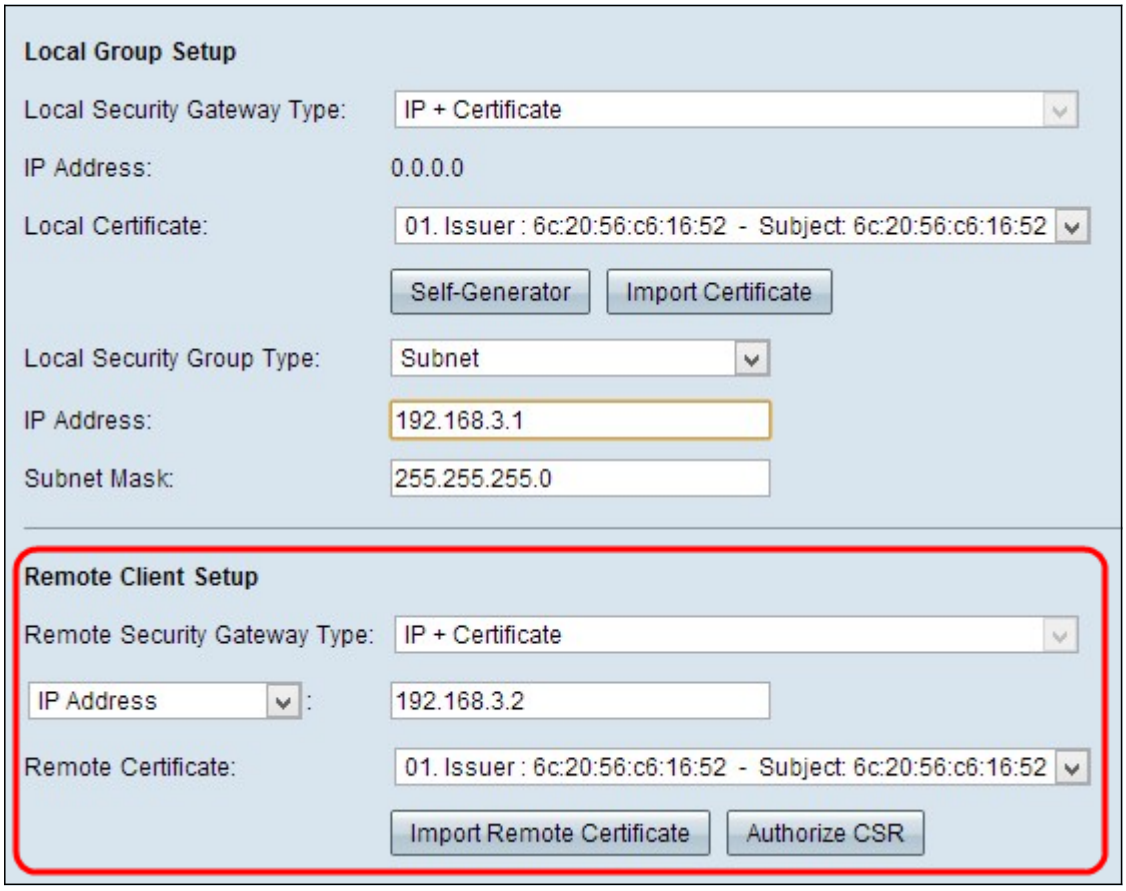
client dans le champ adjacent, ou choisissez IP by DNS Resolved dans la liste déroulante et saisissez le nom de domaine de l'adresse IP dans le champ adjacent. Par l'intermédiaire du serveur DNS local de l'adresse IP, le routeur peut récupérer l'adresse IP automatiquement.

- Authentification IP + E-mail Addr. (USER FQDN) : l'accès au tunnel est possible via une adresse IP statique du client et une adresse e-mail. Si vous choisissez cette option, saisissez l'adresse courriel dans le champ Email Address. Choisissez IP Address dans la liste déroulante et saisissez l'adresse IP statique du client dans le champ adjacent, ou choisissez IP by DNS Resolved dans la liste déroulante et saisissez le nom de domaine de l'adresse IP dans le champ adjacent. Par l'intermédiaire du serveur DNS local de l'adresse IP, le routeur peut récupérer l'adresse IP automatiquement.
- Dynamic IP + Domain Name(FQDN) Authentication : il est possible d'accéder au tunnel par le biais d'une adresse IP dynamique du client et d'un domaine enregistré. Si vous choisissez cette option, saisissez le nom du domaine enregistré dans le champ Domain Name (nom de domaine).
- Authentification FQDN (Dynamic IP + E-mail Addr.) (USER FQDN) : l'accès au tunnel est possible via une adresse IP dynamique du client et une adresse e-mail. Si vous choisissez cette option, saisissez l'adresse courriel dans le champ Email Address.

Étape 2. Si vous souhaitez enregistrer les paramètres que vous avez déjà, faites défiler la page vers le bas et cliquez sur **Enregistrer** pour enregistrer les paramètres.

Configuration du groupe distant avec IKE avec certificat

Remarque : suivez les étapes ci-dessous si vous avez choisi IKE avec certificat dans la liste déroulante *Keying Mode* de l'étape 3 de la section *Add a New Tunnel*.



- Remote Security Gateway Type (Type de passerelle de sécurité à distance) : l'identification du client est possible via IP avec un certificat pour établir une connexion VPN.

Étape 1. Choisissez **IP Address** ou **IP by DNS Resolved** dans la liste déroulante.

- Adresse IP : l'accès au tunnel est possible via l'adresse IP WAN statique du client uniquement. Vous pouvez choisir cette option uniquement si vous connaissez l'adresse IP WAN statique du client. Entrez l'adresse IP statique du client dans le champ *Adresse IP*.
- IP By DNS Resolved : utile si vous ne connaissez pas l'adresse IP du client mais que vous connaissez le domaine de cette adresse IP. Saisissez le nom de domaine de l'adresse IP. Par l'intermédiaire du serveur DNS local de l'adresse IP, le routeur peut récupérer l'adresse IP automatiquement.

Étape 2. Choisissez le certificat distant approprié dans la liste déroulante *Certificat distant*. Cliquez sur **Importer un certificat distant** pour importer un nouveau certificat ou cliquez sur **Autoriser le CSR** pour identifier le certificat avec une demande de signature numérique.

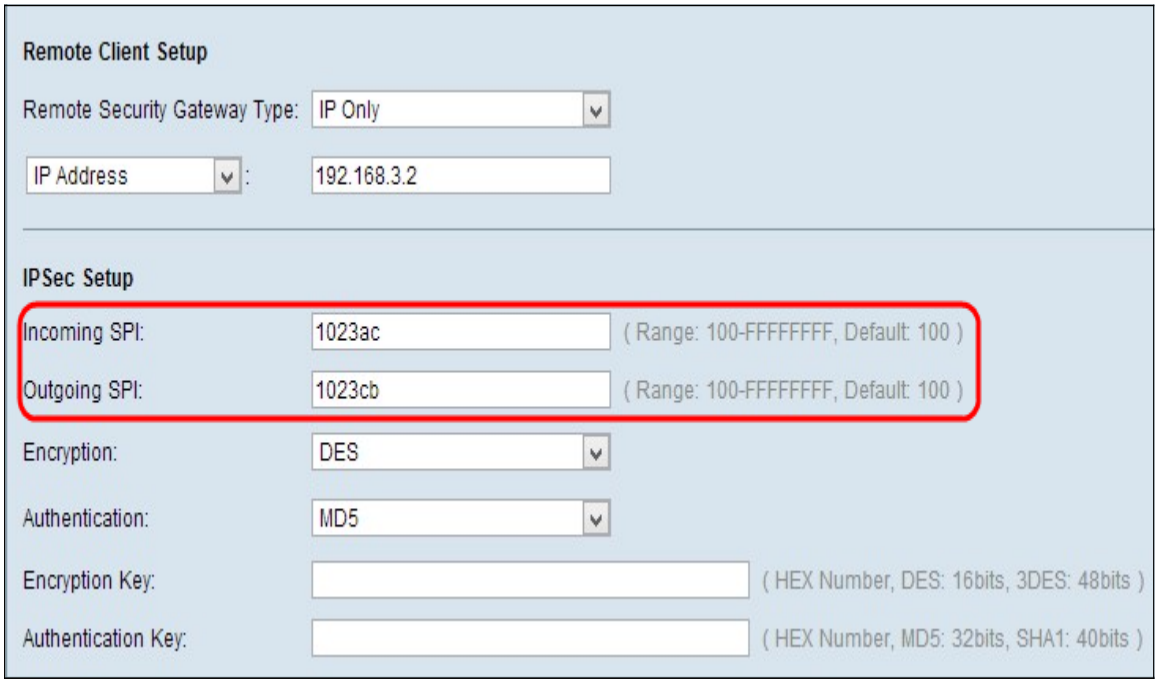
Note: Pour en savoir plus sur l'importation d'un nouveau certificat, reportez-vous à *Afficher/Ajouter un certificat SSL approuvé sur les routeurs RV320*, et pour en savoir plus sur le CSR autorisé, reportez-vous à *Demande de signature de certificat (CSR) sur les routeurs RV320*.

Étape 3. Si vous souhaitez enregistrer les paramètres que vous avez déjà, faites défiler la page vers le bas et cliquez sur **Enregistrer** pour enregistrer les paramètres.

Configuration IPSec

Configuration IPSec avec clé manuelle

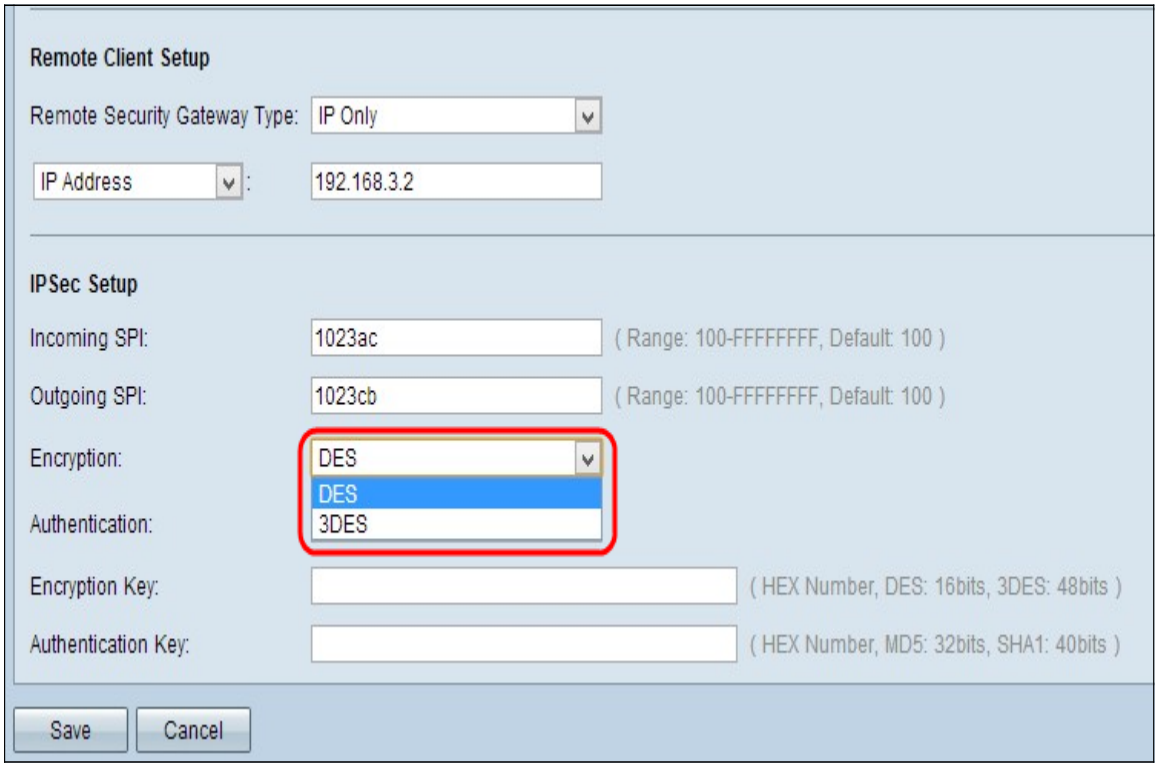
Remarque : Suivez les étapes ci-dessous si vous avez sélectionné Manual dans la liste déroulante *Keying Mode* de l'étape 3 de la section *Add a New Tunnel*.



Étape 1. Entrez la valeur hexadécimale unique pour l'index de paramètre de sécurité entrant (SPI) dans le champ *SPI entrant*. Le SPI est transporté dans l'en-tête ESP (Encapsulating Security Payload Protocol), qui détermine ensemble l'association de sécurité (SA) du paquet entrant. La plage est comprise entre 100 et ffffff, la valeur par défaut étant 100.

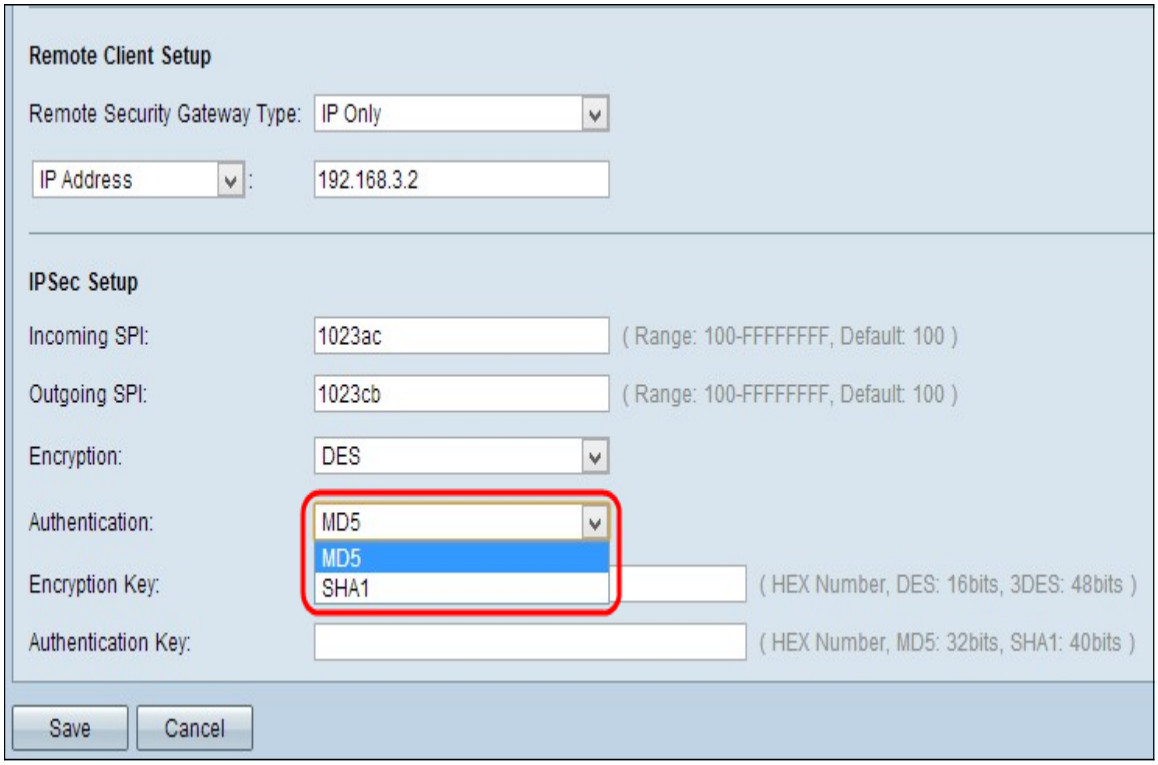
Étape 2. Entrez la valeur hexadécimale unique de l'index de paramètre de sécurité sortant (SPI) dans le champ *SPI sortant*. Le SPI est transporté dans l'en-tête ESP (Encapsulating Security Payload Protocol) qui détermine ensemble l'association de sécurité (SA) pour le paquet sortant. La plage est comprise entre 100 et ffffff, la valeur par défaut étant 100.

Note: Le SPI entrant du périphérique connecté et le SPI sortant de l'autre extrémité du tunnel doivent correspondre les uns aux autres pour établir un tunnel.



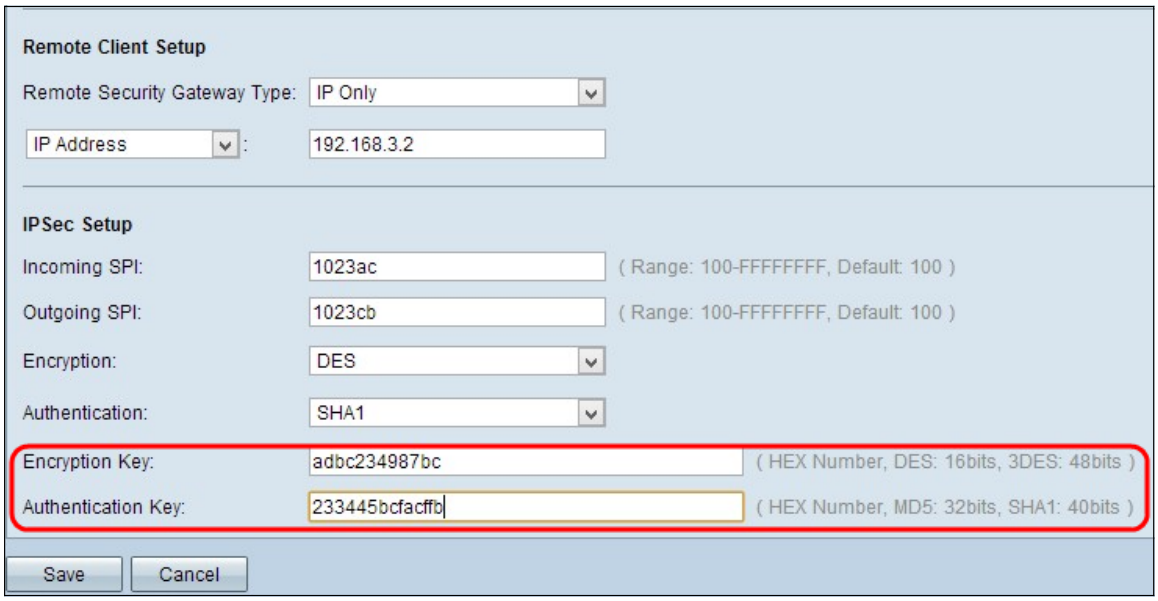
Étape 3. Choisissez la méthode de chiffrement appropriée dans la liste déroulante *Cryptage* . Le chiffrement recommandé est 3DES. Le tunnel VPN doit utiliser la même méthode de chiffrement pour ses deux extrémités.

- DES - Data Encryption Standard (DES) est une méthode de cryptage 56 bits, ancienne et plus rétrocompatible, qui n'est pas aussi sécurisée.
- 3DES - La norme 3DES (Triple Data Encryption Standard) est une méthode de cryptage simple de 168 bits qui permet d'augmenter la taille de la clé en cryptant les données trois fois, ce qui renforce la sécurité par rapport à DES.



Étape 4. Choisissez la méthode d'authentification appropriée dans la liste déroulante *Authentification*. L'authentification recommandée est SHA1. Le tunnel VPN doit utiliser la même méthode d'authentification pour ses deux extrémités.

- MD5 - L'algorithme MD5 (Message Digest Algorithm-5) représente une fonction de hachage hexadécimal 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 de 160 bits plus sécurisée que MD5.



Étape 5. Entrez la clé pour chiffrer et déchiffrer les données dans le champ *Clé de chiffrement*. Si vous avez choisi DES comme méthode de cryptage à l'étape 3, saisissez une valeur hexadécimale à 16 chiffres. Si vous avez choisi 3DES comme méthode de cryptage à l'étape 3, saisissez une valeur hexadécimale à 40 chiffres.

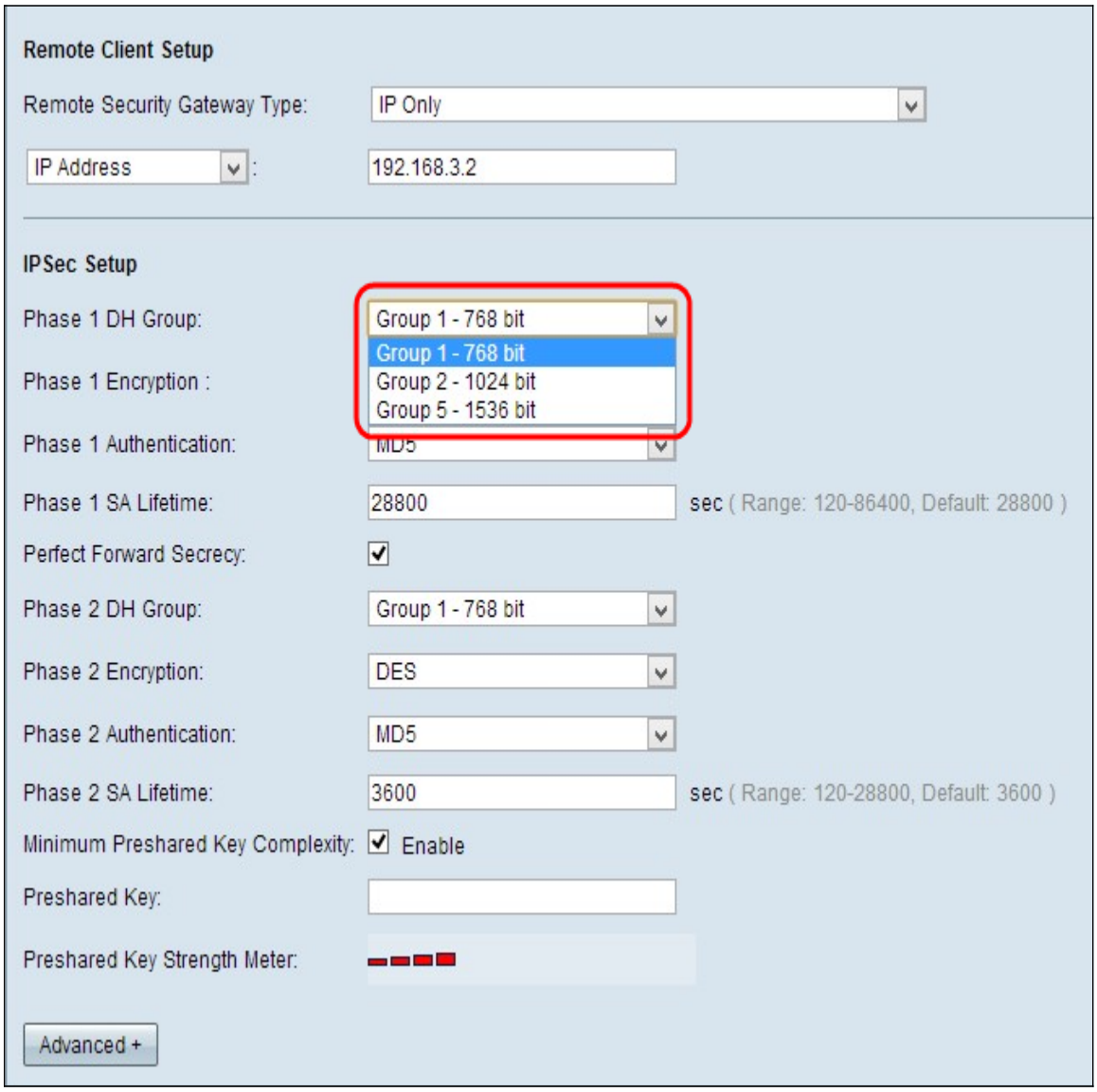
Étape 6. Entrez une clé pré-partagée pour authentifier le trafic dans le champ *Clé*

d'authentification. Si vous choisissez la méthode d'authentification MD5, à l'étape 4, saisissez une valeur hexadécimale de 32 chiffres. Si vous choisissez la méthode d'authentification SHA, à l'étape 4, saisissez une valeur hexadécimale de 40 chiffres. Le tunnel VPN doit utiliser la même clé prépartagée pour ses deux extrémités.

Étape 7. Si vous souhaitez enregistrer les paramètres que vous avez déjà, faites défiler la page vers le bas et cliquez sur **Enregistrer** pour enregistrer les paramètres.

Configuration IPSec avec IKE avec clé prépartagée ou IKE avec certificat

Remarque : suivez les étapes ci-dessous si vous avez choisi IKE avec clé prépartagée ou IKE avec certificat dans la liste déroulante *Keying Mode* de l'étape 3 de la section *Ajouter un nouveau tunnel*.

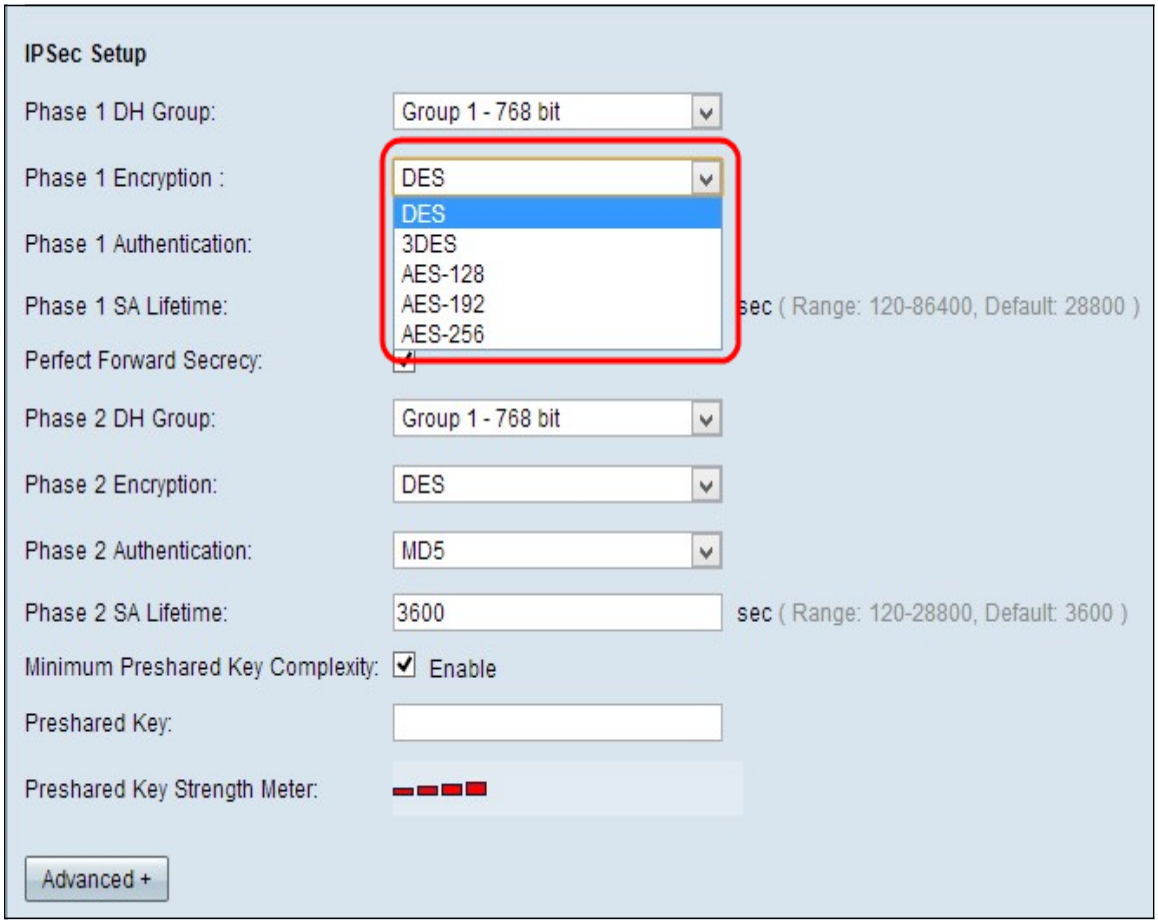


Étape 1. Choisissez le groupe DH de phase 1 approprié dans la liste déroulante *Phase 1 DH* Group. La phase 1 sert à établir l'association de sécurité logique (SA) simplex entre les deux extrémités du tunnel afin de prendre en charge les communications authentiques sécurisées. Diffie-Hellman (DH) est un protocole d'échange de clé cryptographique utilisé lors de la connexion de phase 1 pour partager une clé secrète afin d'authentifier la communication.

- Groupe 1, 768 bits : représente la clé de puissance la plus basse et le groupe

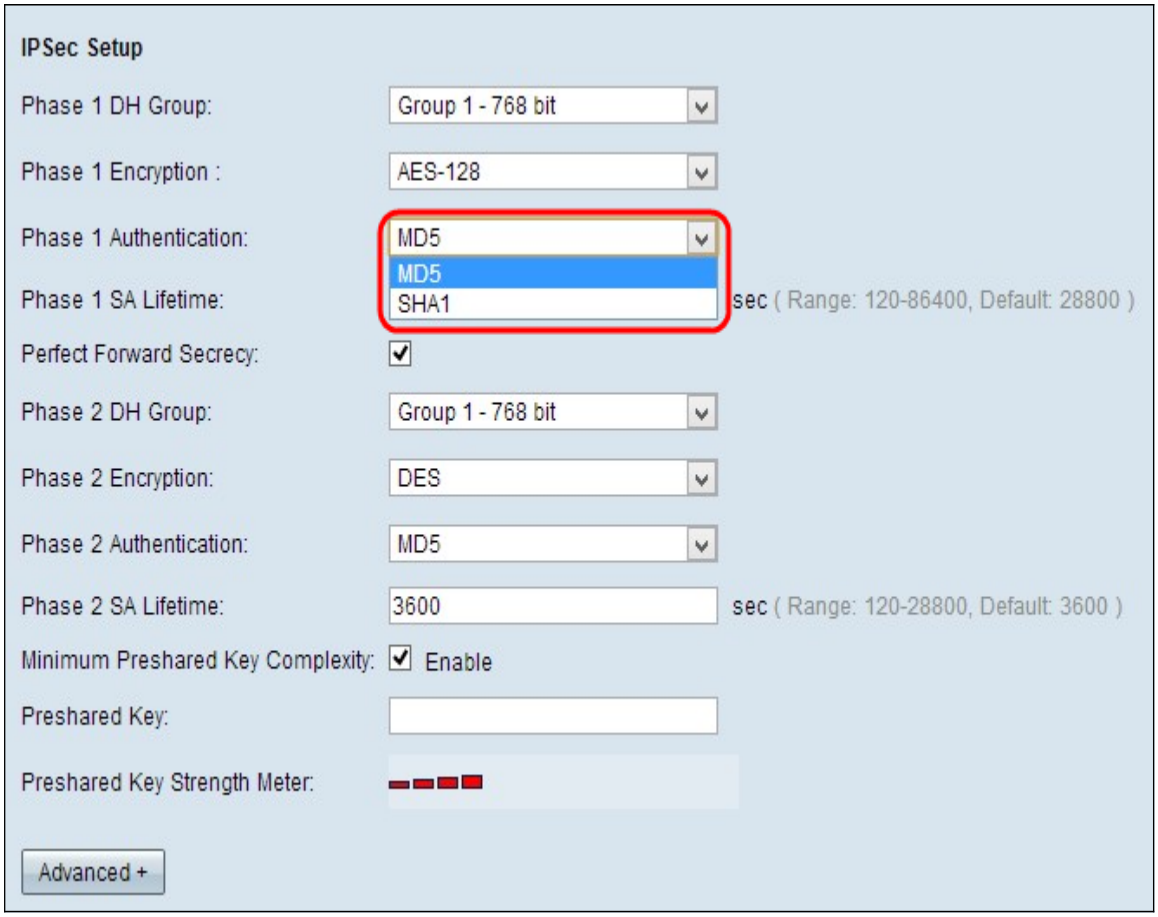
d’authentification le moins sécurisé. Mais il faut moins de temps pour calculer les clés IKE. Cette option est préférable si le débit du réseau est faible.

- Groupe 2, 1024 bits : représente la clé de puissance supérieure, un groupe d’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 d’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.



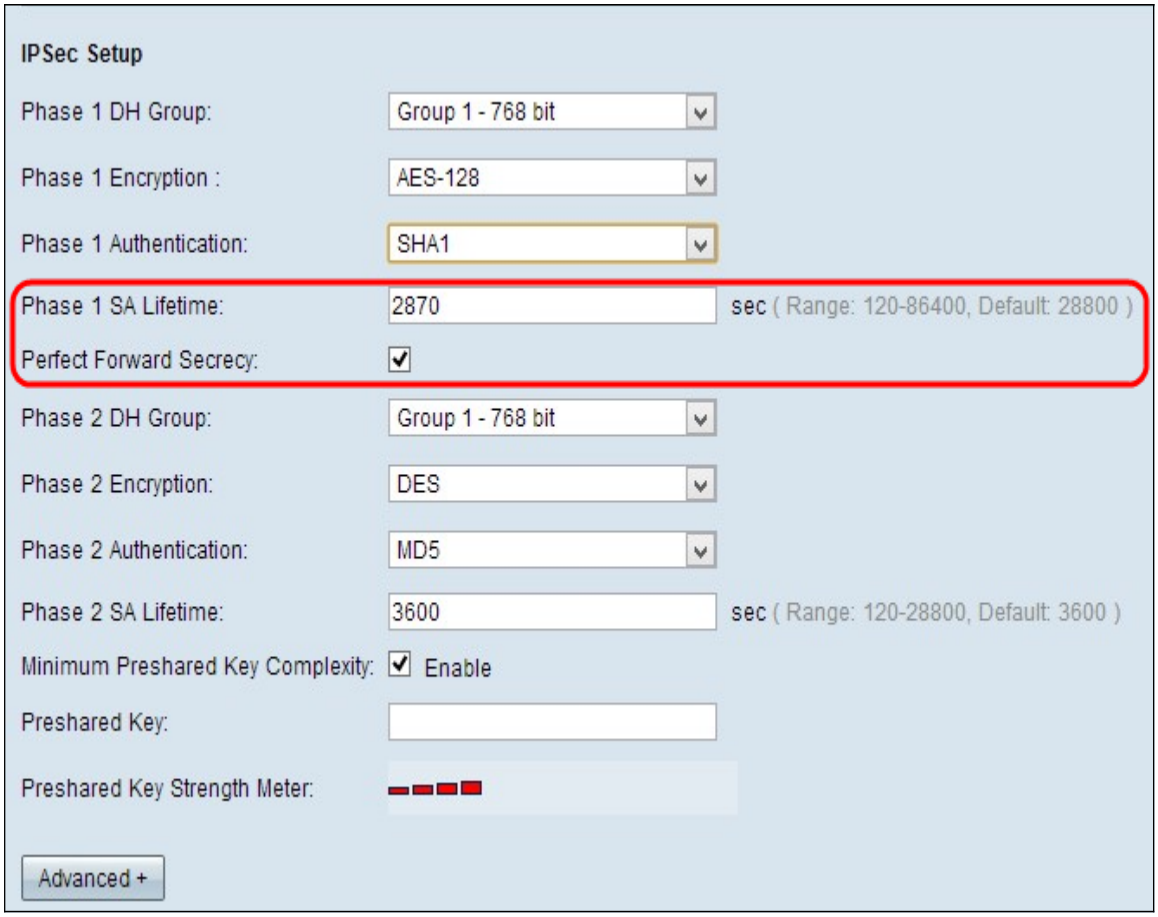
Étape 2. Choisissez le chiffrement de phase 1 approprié pour chiffrer la clé dans la liste déroulante *Phase 1 Encryption*. La méthode AES-256 est recommandée, car il s’agit de la méthode de chiffrement la mieux sécurisée. Le tunnel VPN doit utiliser la même méthode de chiffrement pour ses deux extrémités.

- DES - Data Encryption Standard (DES) est une méthode de cryptage 56 bits, ancienne méthode de cryptage qui n'est pas très sécurisée.
- 3DES - La norme 3DES (Triple Data Encryption Standard) est une méthode de cryptage simple de 168 bits qui permet d'augmenter la taille de la clé en cryptant les données trois fois, ce qui renforce la sécurité par rapport à DES.
- AES-128 - La norme AES (Advanced Encryption Standard) est une méthode de cryptage de 128 bits qui transforme le texte brut en texte chiffré en 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 en 12 cycles de répétition.
- AES-256 - Advanced Encryption Standard (AES) est une méthode de cryptage 256 bits qui transforme le texte brut en texte chiffré en 14 cycles de répétition.



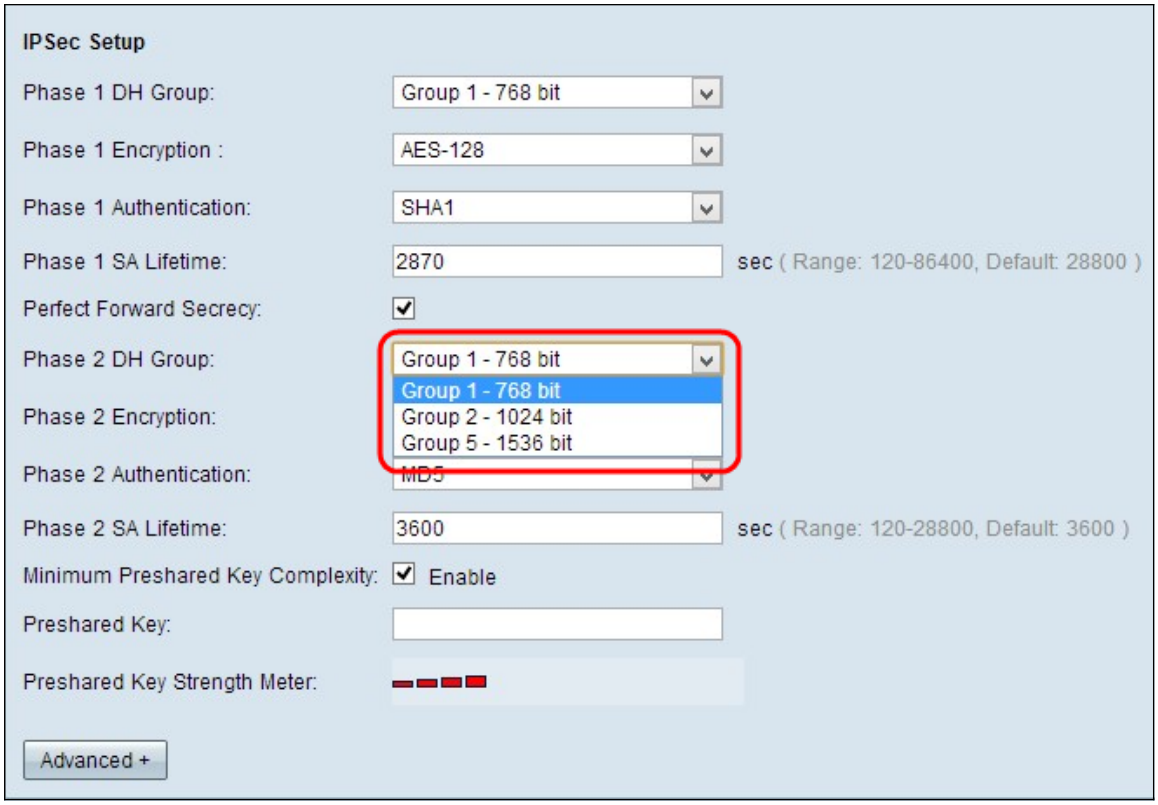
Étape 3. Choisissez la méthode d'authentification appropriée dans la liste déroulante *Authentification de phase 1*. Le tunnel VPN doit utiliser la même méthode d'authentification pour ses deux extrémités.

- MD5 - L'algorithme MD5 (Message Digest Algorithm-5) représente une fonction de hachage hexadécimal 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 de 160 bits plus sécurisée que MD5.



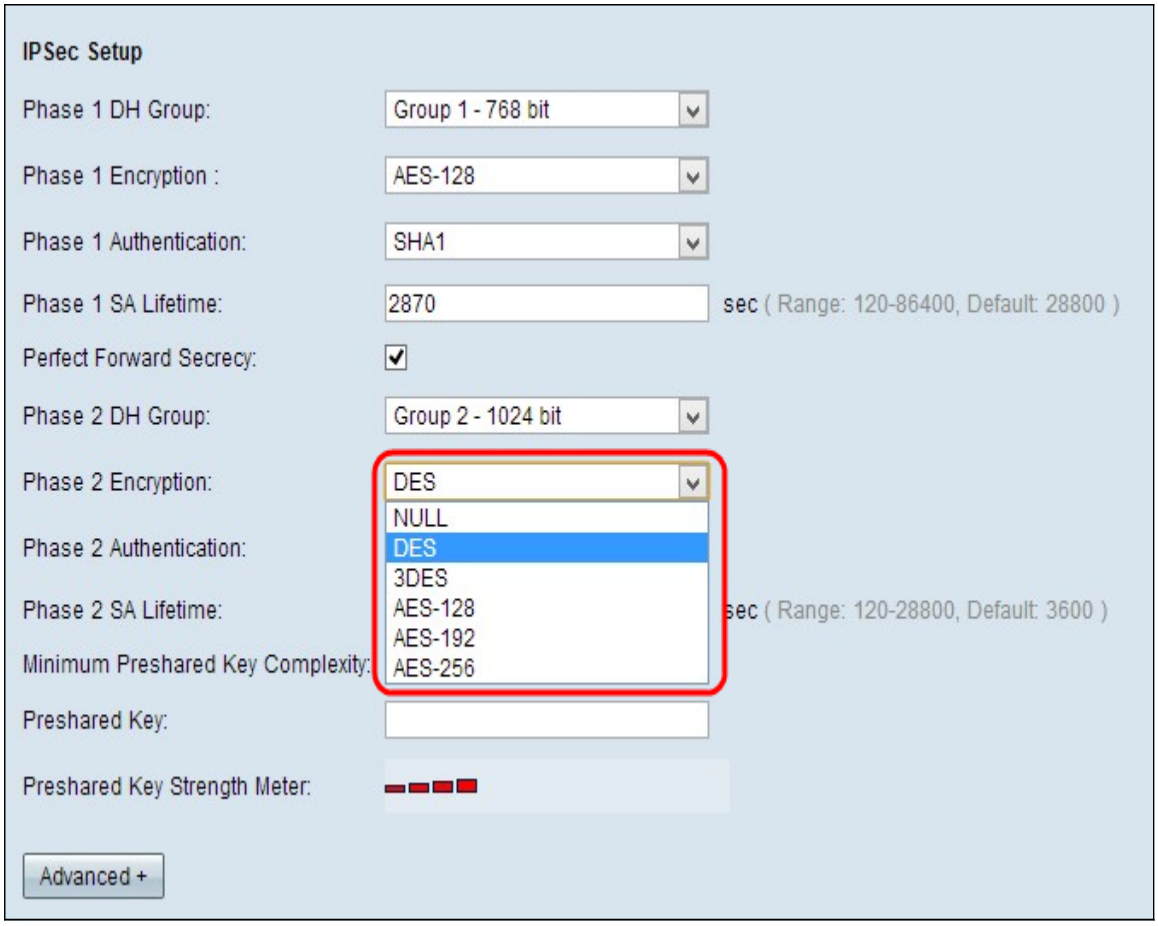
Étape 4. Entrez la durée en secondes, dans la phase 1, le tunnel VPN reste actif dans le champ *Durée de vie de l'association de sécurité de phase 1*. La durée par défaut est de 28 800 secondes.

Étape 5. Cochez la case **Perfect Forward Secrecy** pour fournir une protection accrue aux clés. Cette option permet 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 d'autres clés, même si une clé est compromise. Il s'agit d'une action recommandée, car elle fournit plus de sécurité.



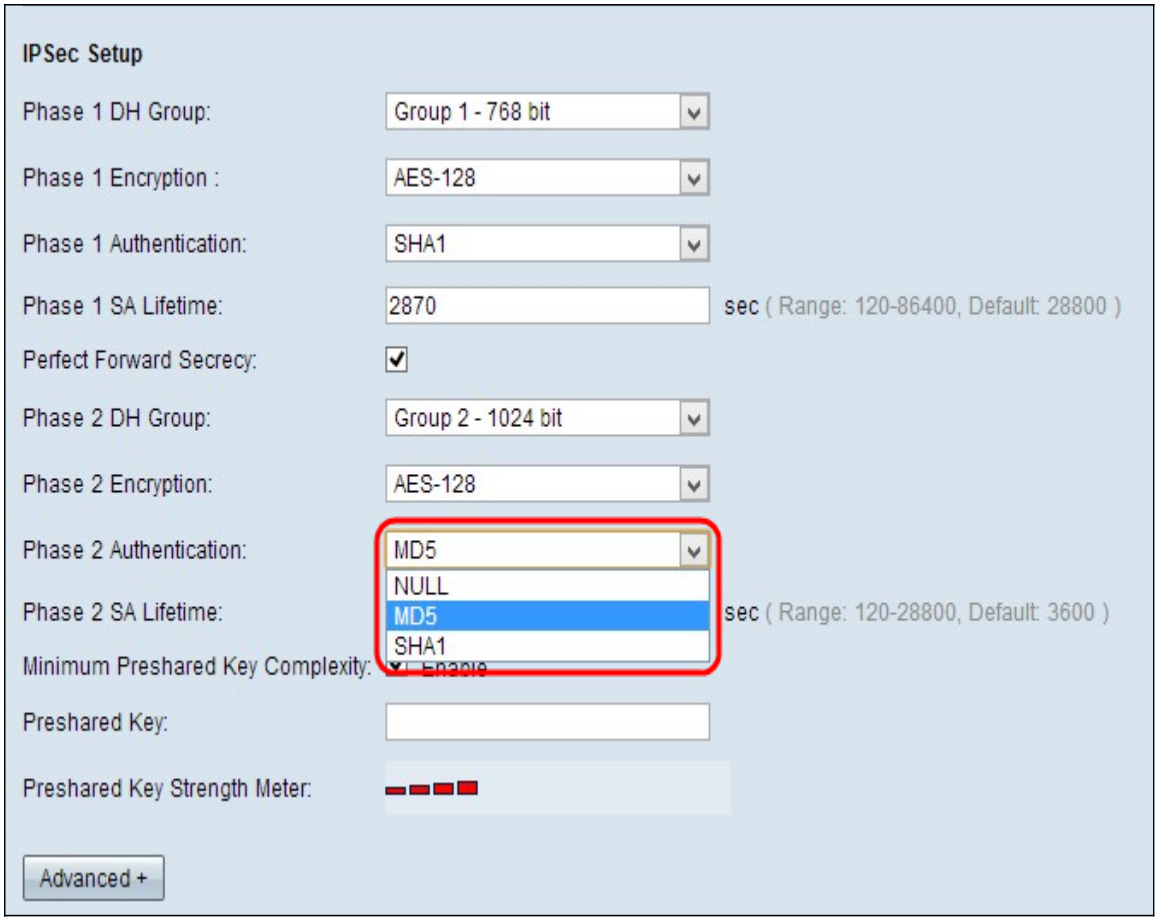
Étape 6. Choisissez le groupe DH de phase 2 approprié dans la liste déroulante *Groupe DH de phase 2*. La phase 1 est utilisée pour établir le simplex, l'association de sécurité logique (SA) entre les deux extrémités du tunnel afin de prendre en charge la communication sécurisée de l'authentification. Diffie-Hellman (DH) est un protocole d'échange de clé cryptographique utilisé lors de la connexion de phase 1 pour partager une clé secrète afin d'authentifier la communication.

- Groupe 1, 768 bits : représente la clé de puissance la plus basse et le groupe d'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 d'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 d'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.



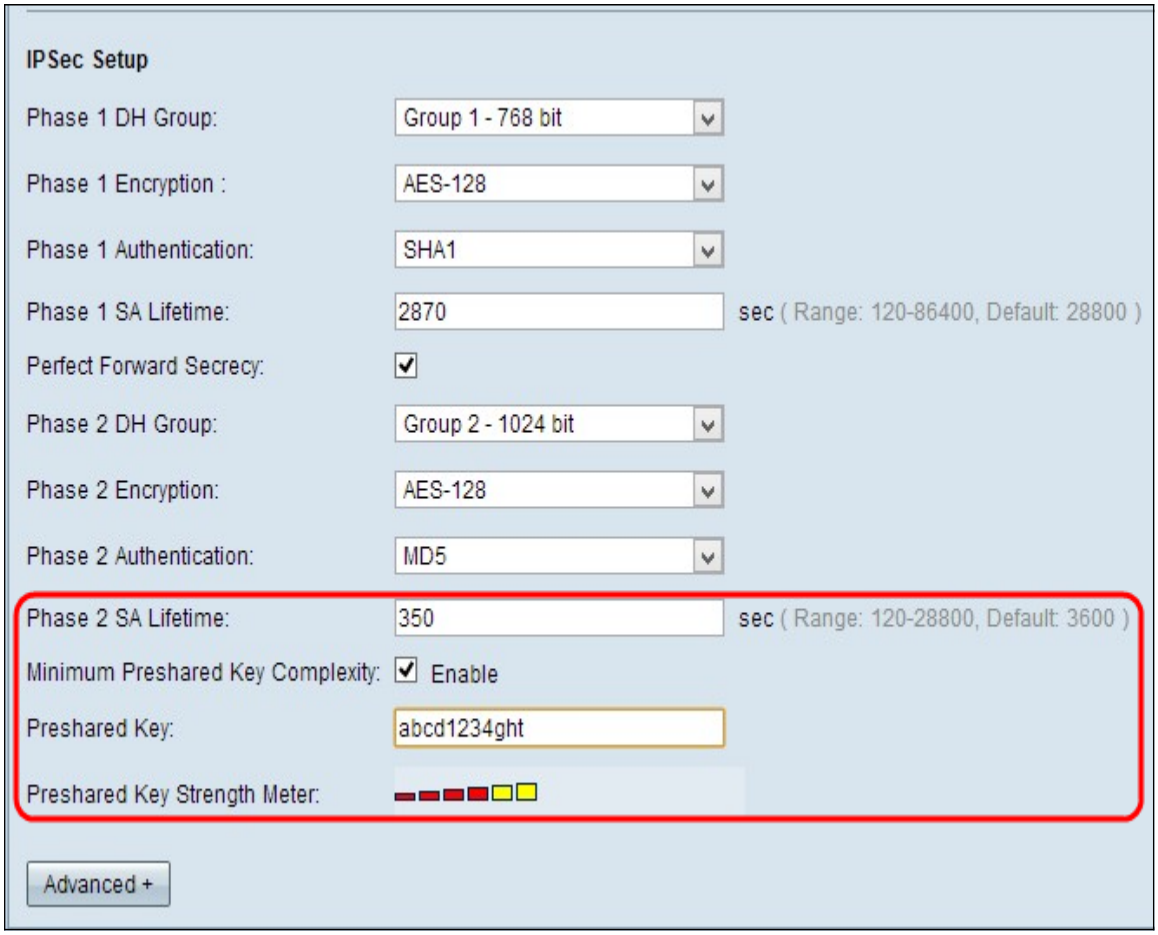
Étape 7. Choisissez le chiffrement de phase 2 approprié pour chiffrer la clé dans la liste déroulante *Phase 2 Encryption*. La méthode AES-256 est recommandée, car il s'agit de la méthode de chiffrement la mieux sécurisée. Le tunnel VPN doit utiliser la même méthode de chiffrement pour ses deux extrémités.

- DES - Data Encryption Standard (DES) est une méthode de cryptage 56 bits, ancienne méthode de cryptage qui n'est pas très sécurisée.
- 3DES - La norme 3DES (Triple Data Encryption Standard) est une méthode de cryptage simple de 168 bits qui permet d'augmenter la taille de la clé en cryptant les données trois fois, ce qui renforce la sécurité par rapport à DES.
- AES-128 - La norme AES (Advanced Encryption Standard) est une méthode de cryptage de 128 bits qui transforme le texte brut en texte chiffré à l'aide de répétitions de 10 cycles.
- AES-192 - Advanced Encryption Standard (AES) est une méthode de cryptage 192 bits qui transforme le texte brut en texte chiffré à l'aide de répétitions de 12 cycles.
- AES-256 - Advanced Encryption Standard (AES) est une méthode de cryptage 256 bits qui transforme le texte brut en texte chiffré à l'aide de répétitions de 14 cycles.



Étape 8. Choisissez la méthode d'authentification appropriée dans la liste déroulante *Authentification de phase 2*. Le tunnel VPN doit utiliser la même méthode d’authentification pour ses deux extrémités.

- MD5 - L'algorithme MD5 (Message Digest Algorithm-5) représente une fonction de hachage hexadécimal 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 de 160 bits plus sécurisée que MD5.
- Null : aucune méthode d’authentification n’est utilisée.



Étape 9. Entrez la durée en secondes, dans la phase 2, le tunnel VPN reste actif dans le champ Durée de vie de l'*AS de phase 2*. La durée par défaut est de 3 600 secondes.

Étape 10. 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.**

Étape 11. Entrez une clé précédemment partagée entre les homologues IKE dans le champ *Clé prépartagée*. Jusqu'à 30 caractères alphanumériques peuvent être utilisés comme clé prépartagée. Le tunnel VPN doit utiliser la même clé prépartagée pour ses deux extrémités.

Note: Il est fortement recommandé de modifier fréquemment la clé pré-partagée entre les homologues IKE afin que le VPN reste sécurisé.

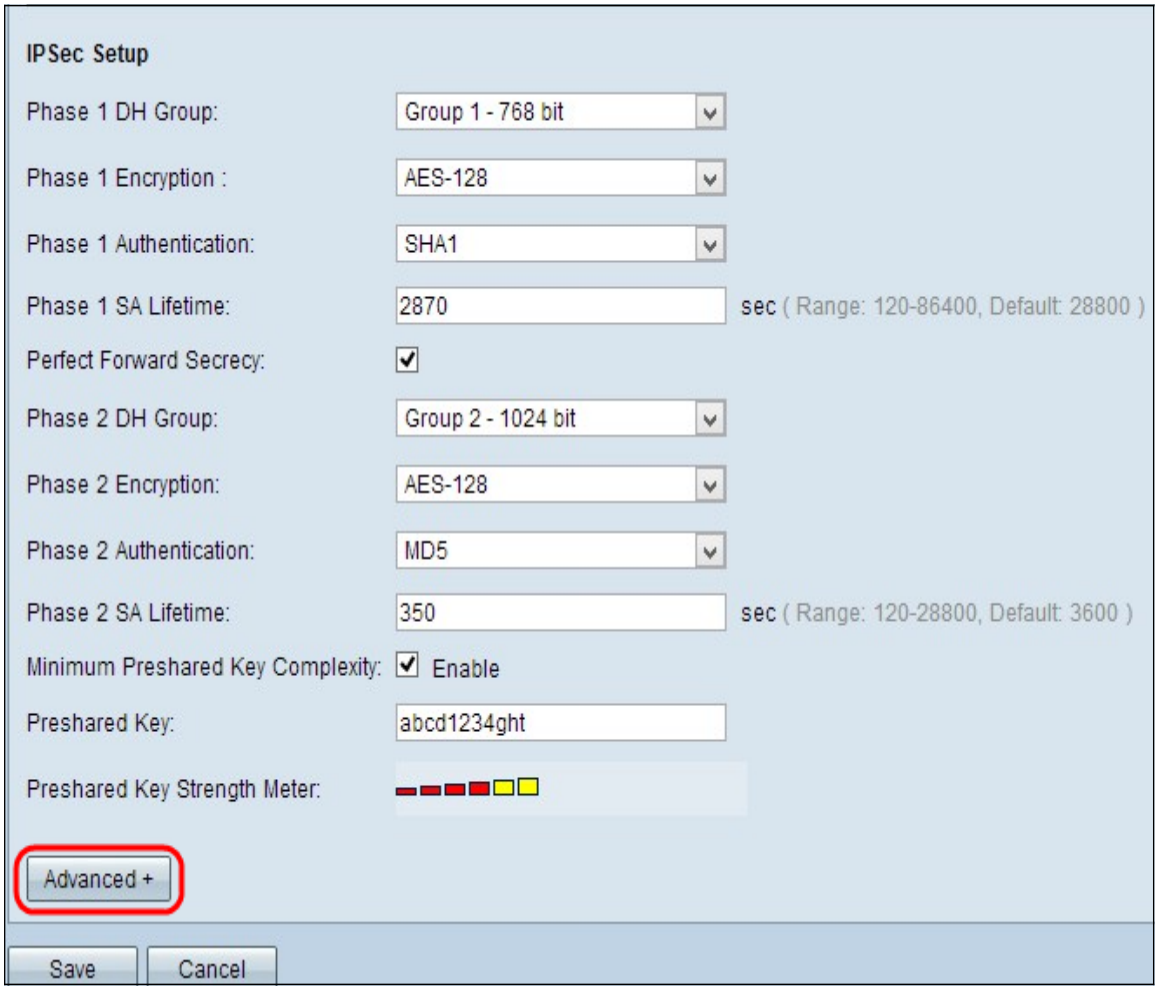
- Compteur de force de la clé prépartagée : indique la force de la clé prépartagée par des barres colorées. La couleur rouge indique une puissance faible, la couleur jaune, une puissance acceptable et le vert, une puissance élevée. Si vous cochez la case **Complexité de clé prépartagée minimale** à l'étape 10 de la section Configuration IPSec, seul le paramètre de force de clé prépartagée apparaît.

Note: Si vous choisissez IKE with Preshared Key dans la liste déroulante *Keying Mode* de l'étape 3 pour *ajouter un nouveau tunnel* dans la section, vous pouvez uniquement configurer l'étape 10, étape 11 et afficher le paramètre Preshared Key Strength Meter.

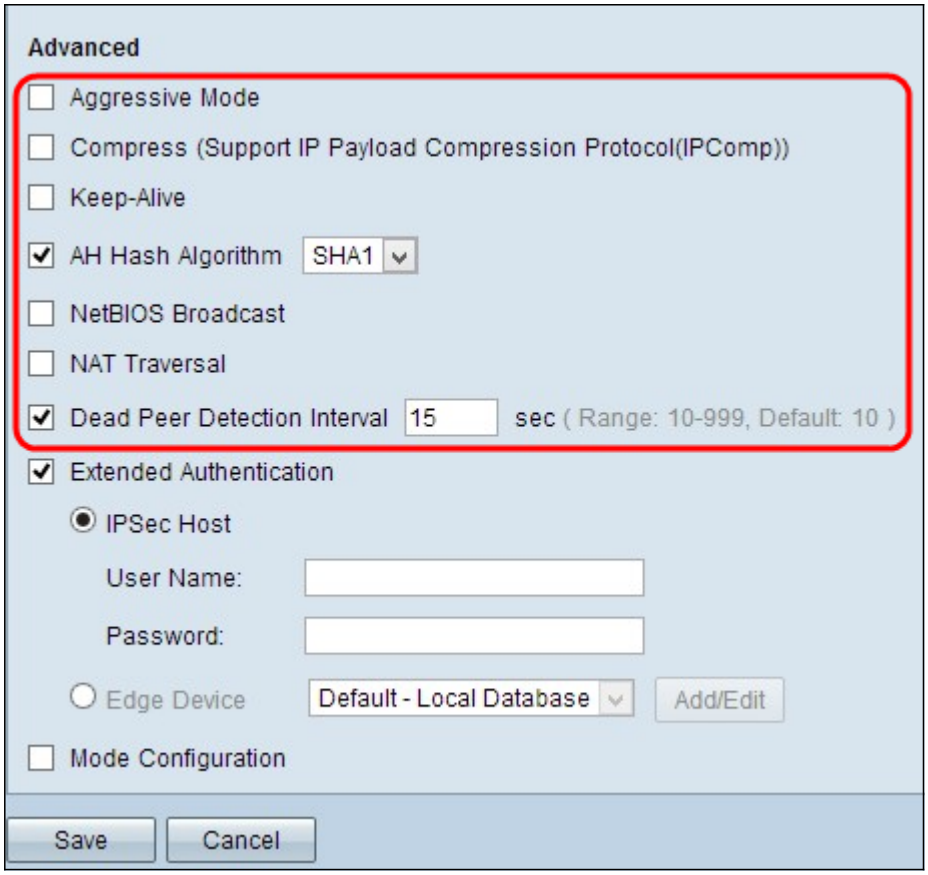
Étape 12. Si vous souhaitez enregistrer les paramètres que vous avez déjà, faites défiler la page vers le bas et cliquez sur **Enregistrer** pour enregistrer les paramètres.

Configuration avancée avec IKE avec clé prépartagée ou IKE avec certificat

Les paramètres avancés ne sont possibles que pour IKE avec clé prépartagée et IKE avec clé de certification. Le paramètre de clé Manual ne comporte aucun paramètre avancé.



Étape 1. Cliquez sur **Avancé** pour obtenir les paramètres avancés pour IKE avec la clé prépartagée.



Étape 2. Activez la case à cocher **Aggressive Mode (mode agressif) si votre débit de réseau est faible.** Il échange les ID des points d'extrémité du tunnel en texte clair pendant la connexion SA, ce qui nécessite moins de temps pour échanger mais moins de sécurité.

Étape 3. Cochez la case **Compress (Support IP Payload Compression Protocol (IPComp))** si vous voulez compresser la taille du datagramme IP. IPComp est un protocole de compression IP utilisé pour compresser la taille du datagramme IP, si la vitesse du réseau est faible et que l'utilisateur souhaite transmettre rapidement les données sans perte via le réseau lent.

Étape 4.Cochez la case **Keep-Alive** si vous voulez toujours que la connexion du tunnel VPN reste active. Il permet de rétablir immédiatement les connexions si une connexion devient inactive.

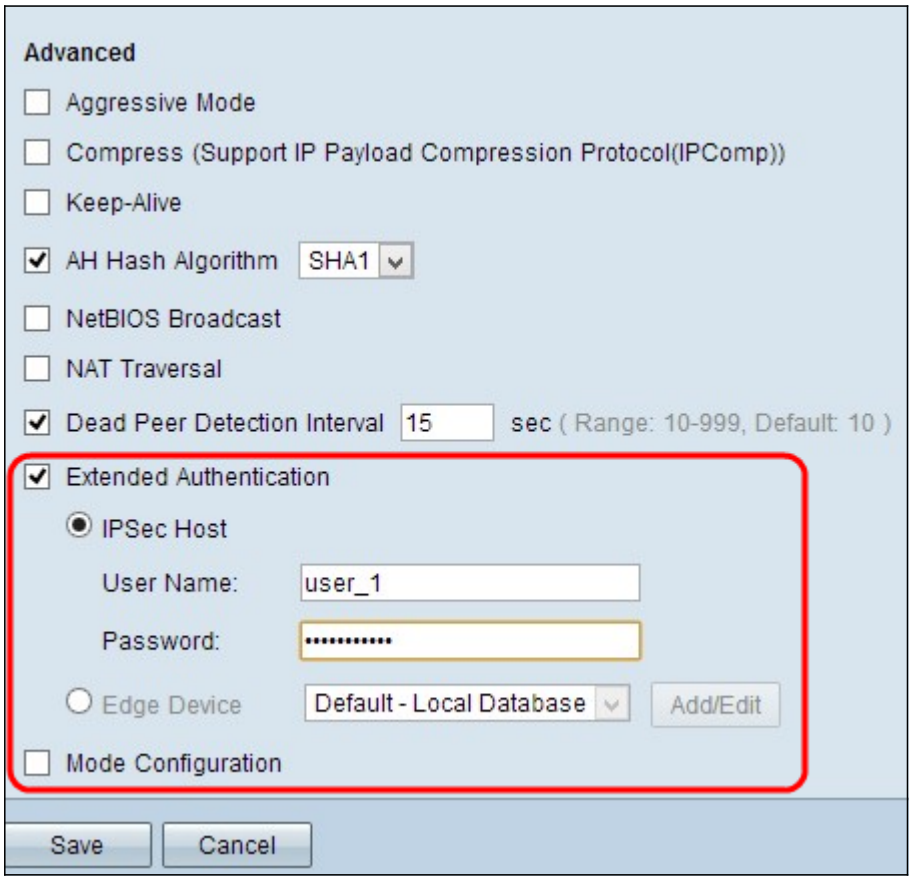
Étape 5. Cochez la case **Algorithme de hachage AH** si vous voulez authentifier l'en-tête Authentifier (AH). AH assure l'authentification à l'origine des données, l'intégrité des données via la somme de contrôle et la protection est étendue à l'en-tête IP. Le tunnel doit avoir le même algorithme pour les deux côtés.

- MD5 - L'algorithme MD5 (Message Digest Algorithm-5) représente 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 - Secure Hash Algorithm version 1 (SHA1) est une fonction de hachage de 160 bits plus sécurisée que MD5.

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 **NAT Traversal** si vous souhaitez accéder à Internet à partir de votre réseau local privé via une adresse IP publique. La traversée NAT est utilisée pour afficher les adresses IP privées des systèmes internes en tant qu'adresses IP publiques afin de protéger les adresses IP privées contre toute attaque ou découverte malveillante.

Étape 8. Cochez la case **Dead Peer Detection Interval** (intervalle de détection des homologues inactifs) pour vérifier l'activité du tunnel VPN via des messages Hello ou ACK, de manière régulière. Si vous cochez cette case, entrez la durée ou l'intervalle des messages Hello souhaités.



Étape 9. Cochez **Extended Authentication** pour fournir plus de sécurité et d'authentification à la connexion VPN. Cliquez sur la case d'option appropriée pour étendre l'authentification de la connexion VPN.

- Hôte IPSec : authentification étendue via l'hôte IPSec. Si vous choisissez cette option, saisissez le nom d'utilisateur de l'hôte IPSec dans le champ User Name (Nom d'utilisateur) et un mot de passe dans le champ Password (Mot de passe).
- Périphérique de périphérie : authentification étendue via le périphérique de périphérie. Si vous choisissez cette option, choisissez la base de données qui contient le périphérique de périphérie dans la liste déroulante. Pour ajouter ou modifier la base de données, cliquez sur **Ajouter/Modifier**.

Note: Pour en savoir plus sur l'ajout ou la modification de la base de données locale, reportez-vous à *Configuration de la gestion des utilisateurs et des domaines sur le routeur RV320*.

Étape 10. Cochez **Configuration du mode** pour fournir l'adresse IP du demandeur de tunnel entrant.

Note: Les étapes 9 à 11 sont disponibles pour le mode de clé pré-partagée IKE pour le VPN

de tunnel.

Étape 11. Cliquez sur **Save pour enregistrer les paramètres.**

Conclusion

Vous avez maintenant appris les étapes de configuration d'un client unique vers un VPN de passerelle sur les routeurs VPN de la gamme RV32x

Afficher une vidéo relative à cet article...

Cliquez ici pour afficher d'autres présentations techniques de Cisco