# Configurer un profil de sécurité IPSec (Internet Protocol Security) sur un routeur de la gamme RV34x

## Objectif

IPSec (Internet Protocol Security) fournit des tunnels sécurisés entre deux homologues, tels que deux routeurs. Les paquets considérés comme sensibles et qui doivent être envoyés via ces tunnels sécurisés, ainsi que les paramètres qui doivent être utilisés pour protéger ces paquets sensibles, doivent être définis en spécifiant les caractéristiques de ces tunnels. Ensuite, lorsque l'homologue IPsec voit un paquet aussi sensible, il configure le tunnel sécurisé approprié et envoie le paquet par ce tunnel à l'homologue distant.

Quand IPsec est mis en oeuvre dans un pare-feu ou un routeur, il fournit une sécurité forte qui peut être appliquée à tout le trafic traversant le périmètre. Le trafic au sein d'une entreprise ou d'un groupe de travail n'entraîne pas de surcharge liée au traitement de la sécurité.

L'objectif de ce document est de vous montrer comment configurer le profil IPSec sur un routeur de la gamme RV34x.

## Périphériques pertinents

- Gamme RV34x

## Version du logiciel

- 1.0.1.16

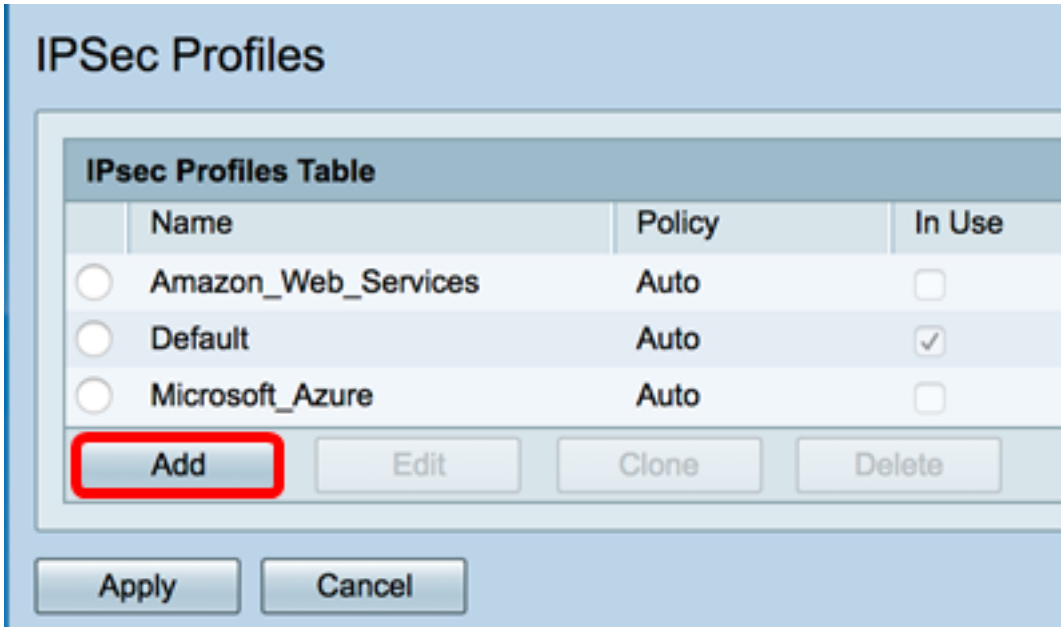
## Configurer le profil IPSec

### Créer un profil IPSec

Étape 1. Connectez-vous à l'utilitaire Web du routeur et choisissez **VPN > IPSec Profiles**.


Étape 2. Le tableau Profils IPsec affiche les profils existants. Cliquez sur **Ajouter** pour créer

un nouveau profil.




Étape 3. Créez un nom pour le profil dans le champ *Nom du profil*. Le nom du profil ne doit contenir que des caractères alphanumériques et un trait de soulignement (_) pour les caractères spéciaux.

**Note:** Dans cet exemple, IPSec_VPN est utilisé comme nom de profil IPSec.


Étape 4. Cliquez sur une case d'option pour déterminer la méthode d'échange de clés que le profil utilisera pour s'authentifier. Les options sont les suivantes :

- Auto : les paramètres de stratégie sont définis automatiquement. Cette option utilise une stratégie IKE (Internet Key Exchange) pour l'intégrité des données et les échanges de clés de chiffrement. Si cette option est sélectionnée, les paramètres de configuration de la zone Paramètres de stratégie automatique sont activés. Cliquez ici pour configurer les paramètres Auto.
- Manual : cette option vous permet de configurer manuellement les clés pour le cryptage et l'intégrité des données pour le tunnel VPN (Virtual Private Network). Si cette option est sélectionnée, les paramètres de configuration de la zone Manual Policy Parameters sont activés. Cliquez ici pour configurer les paramètres manuels.

**Note:** Dans cet exemple, Auto a été sélectionné.


## Configuration des paramètres automatiques

Étape 1. Dans la zone Options de phase 1, sélectionnez le groupe Diffie-Hellman (DH) approprié à utiliser avec la clé de phase 1 dans la liste déroulante Groupe DH. Diffie-Hellman est un protocole d'échange de clés cryptographiques utilisé dans la connexion pour échanger des ensembles de clés pré-partagés. La force de l'algorithme est déterminée par des bits. Les options sont les suivantes :

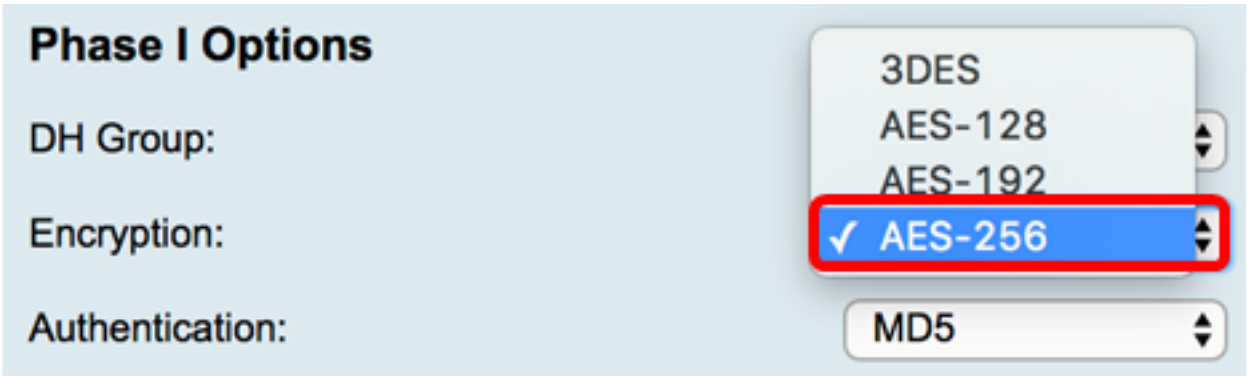
- Group2 - 1024 bit : calcule la clé plus lentement, mais est plus sécurisé que Group1.
- Group5 - 1536-bit : calcule la clé la plus lente, mais la plus sécurisée.

**Note:** Dans cet exemple, le bit Group2-1024 est choisi.


Étape 2. Dans la liste déroulante Encryption (Cryptage), sélectionnez la méthode de cryptage appropriée pour chiffrer et déchiffrer les données utiles ESP (Encapsulating Security Payload) et ISAKMP (Internet Security Association and Key Management Protocol). Les options sont les suivantes :

- 3DES - Triple Data Encryption Standard.
- AES-128 — Advanced Encryption Standard utilise une clé de 128 bits.
- AES-192 — Advanced Encryption Standard utilise une clé 192 bits.
- AES-256 — Advanced Encryption Standard utilise une clé de 256 bits.

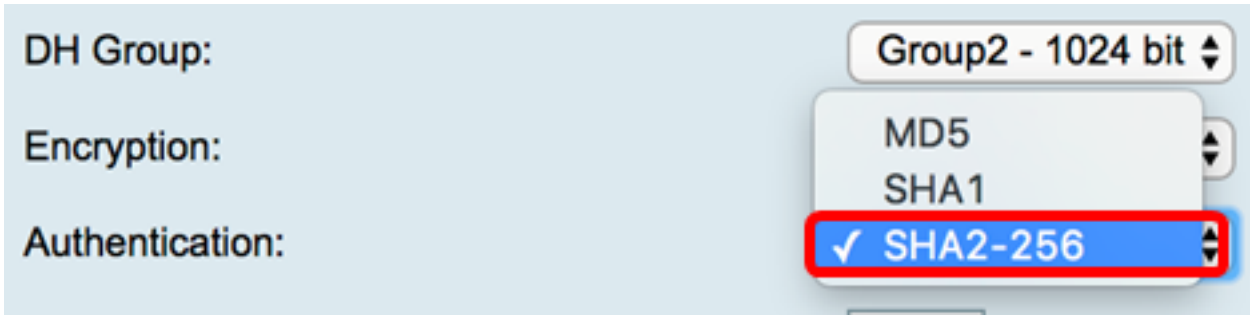
**Remarque :** AES est la méthode standard de cryptage sur DES et 3DES pour ses performances et sa sécurité accrues. L'élargissement de la clé AES améliorera la sécurité grâce à des performances directes. Dans cet exemple, AES-256 est choisi.




Étape 3. Dans le menu déroulant Authentification, choisissez une méthode d'authentification qui déterminera comment ESP et ISAKMP sont authentifiés. Les options sont les suivantes :

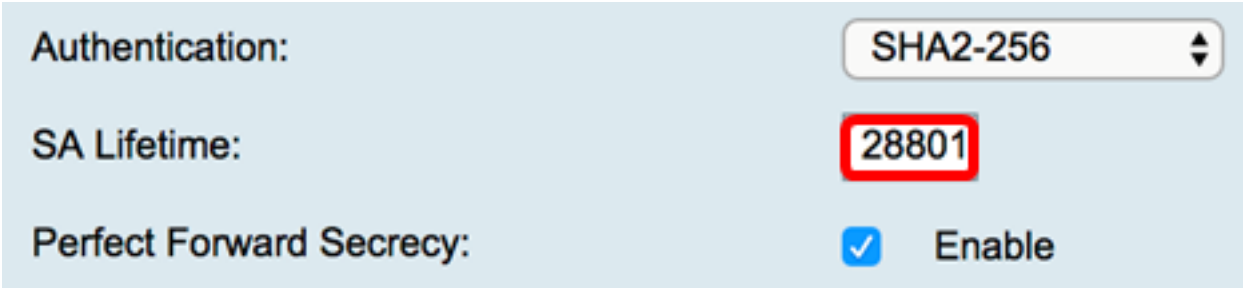
- MD5 — L'algorithme Message Digest a une valeur de hachage de 128 bits.
- SHA-1 — L'algorithme de hachage sécurisé a une valeur de hachage de 160 bits.
- SHA2-256 — Algorithme de hachage sécurisé avec une valeur de hachage de 256 bits.

**Remarque :** MD5 et SHA sont deux fonctions de hachage cryptographique. Ils prennent une donnée, la compactent et créent une sortie hexadécimale unique qui n'est généralement pas reproductible. Dans cet exemple, SHA2-256 est sélectionné.

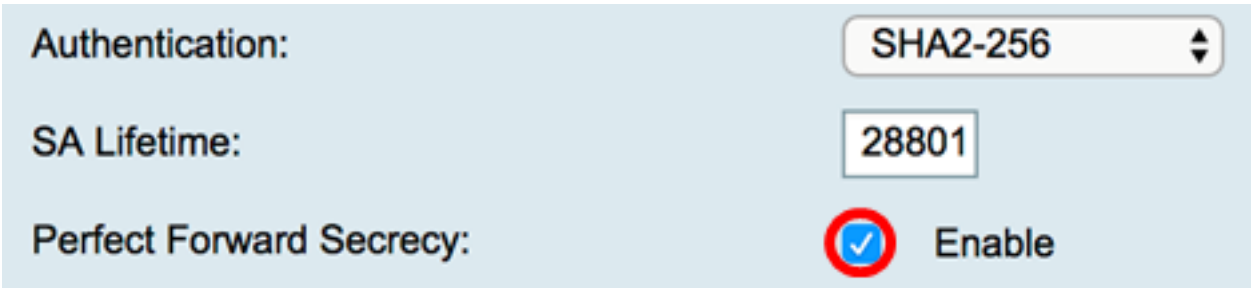



Étape 4. Dans le champ *Durée de vie de la SA*, saisissez une valeur comprise entre 120 et 86 400. Il s'agit de la durée pendant laquelle l'association de sécurité IKE (Internet Key Exchange) restera active dans cette phase. La valeur par défaut est 28800.

**Note:** Dans cet exemple, 28801 est utilisé.

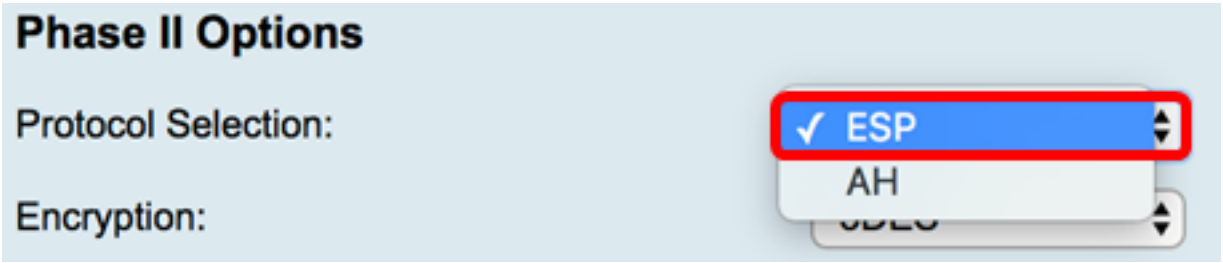



Étape 5. (Facultatif) Cochez la case **Enable Perfect Forward Secrecy** pour générer une nouvelle clé pour le chiffrement et l'authentification du trafic IPSec.




Étape 6. Dans le menu déroulant Sélection de protocole de la zone Options de phase II, sélectionnez un type de protocole à appliquer à la deuxième phase de la négociation. Les options sont les suivantes :

- ESP — Si vous choisissez cette option, passez à l'étape 7 pour choisir une méthode de chiffrement sur la façon dont les paquets ESP seront cryptés et décryptés. Protocole de sécurité qui fournit des services de confidentialité des données et des services d'authentification des données facultatifs, ainsi que des services anti-relecture. ESP encapsule les données à protéger.
- AH - Authentication Header (AH) est un protocole de sécurité qui fournit l'authentification des données et des services facultatifs d'anti-relecture. AH est incorporé dans les données à protéger (datagramme IP complet). Passez à l'étape 8 si vous avez choisi cette option.




Étape 7. Si ESP a été choisi à l'étape 6, choisissez la méthode de chiffrement appropriée pour chiffrer et déchiffrer ESP et ISAKMP dans la liste déroulante Encryption (Cryptage). Les options sont les suivantes :

- 3DES - Triple Data Encryption Standard.
- AES-128 — Advanced Encryption Standard utilise une clé de 128 bits.
- AES-192 — Advanced Encryption Standard utilise une clé 192 bits.
- AES-256 — Advanced Encryption Standard utilise une clé de 256 bits.

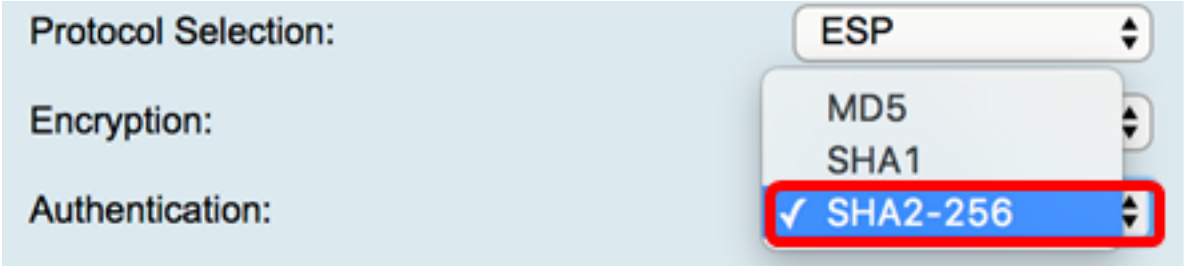
**Note:** Dans cet exemple, AES-256 est choisi.


Étape 8. Dans le menu déroulant Authentification, choisissez une méthode d'authentification qui déterminera comment ESP et ISAKMP sont authentifiés. Les options sont les suivantes :

- MD5 — L'algorithme Message Digest a une valeur de hachage de 128 bits.

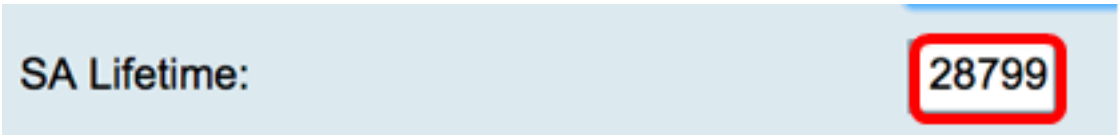
- SHA-1 — L'algorithme de hachage sécurisé a une valeur de hachage de 160 bits.
- SHA2-256 — Algorithme de hachage sécurisé avec une valeur de hachage de 256 bits.

**Note:** Dans cet exemple, SHA2-256 est utilisé.




Étape 9. Dans le champ *Durée de vie de la SA*, saisissez une valeur comprise entre 120 et 28 800. Il s'agit de la durée pendant laquelle l'association de sécurité IKE restera active dans cette phase. La valeur par défaut est 3600.

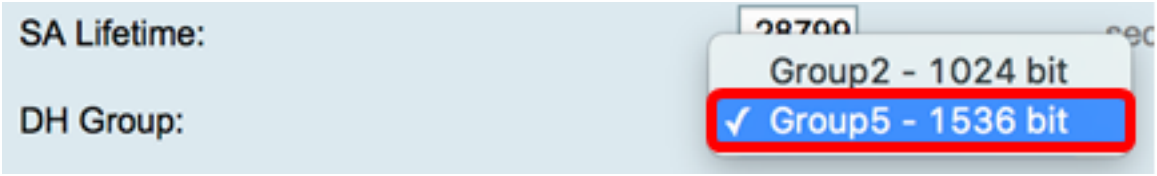
**Note:** Dans cet exemple, 28799 est utilisé.

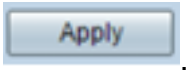



Étape 10. Dans la liste déroulante Groupe DH, sélectionnez le groupe Diffie-Hellman (DH) approprié à utiliser avec la clé dans la phase 2. Les options sont les suivantes :

- Group2 - 1024 bit : calcule la clé plus lentement, mais est plus sécurisé que Group1.
- Group5 - 1536 bit - Calcule la clé la plus lente, mais la plus sécurisée.

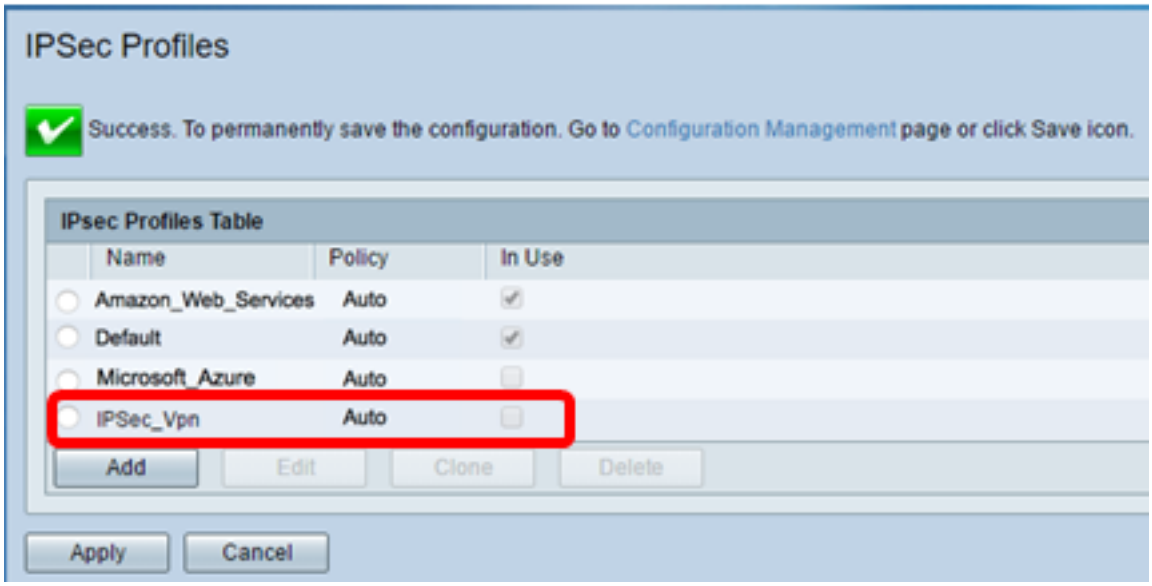
**Note:** Dans cet exemple, Group5 - 1536 bit est sélectionné.




Étape 11. Cliquez sur 

.

**Note:** Vous allez revenir à la table Profils IPSec et le profil IPSec nouvellement créé doit apparaître.




Étape 12. (Facultatif) Pour enregistrer définitivement la configuration, accédez à la page Copier/Enregistrer la configuration ou cliquez sur l' 

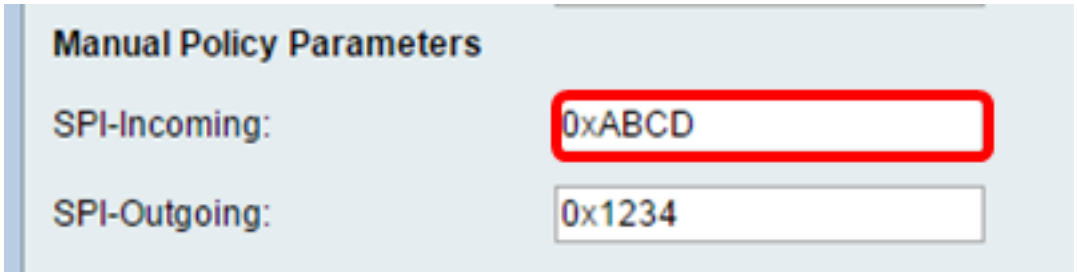
icône située dans la partie supérieure de la page.

Vous devez maintenant avoir correctement configuré un profil IPSec automatique sur un routeur de la gamme RV34x.

## Configuration des paramètres manuels

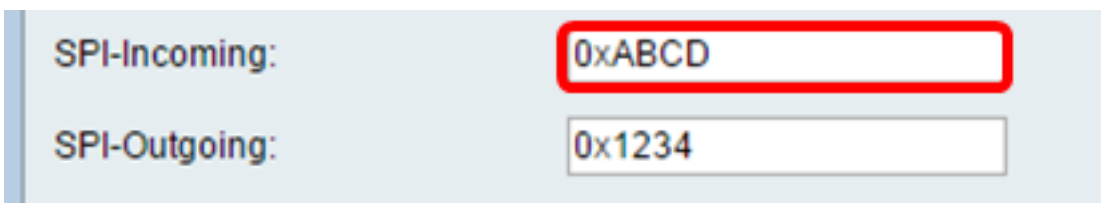
Étape 1. Dans le champ *SPI-Incoming*, saisissez un nombre hexadécimal compris entre 100 et FFFFFF pour la balise SPI (Security Parameter Index) pour le trafic entrant sur la connexion VPN. La balise SPI est utilisée pour distinguer le trafic d'une session du trafic d'autres sessions.

**Note:** Pour cet exemple, 0xABCD est utilisé.



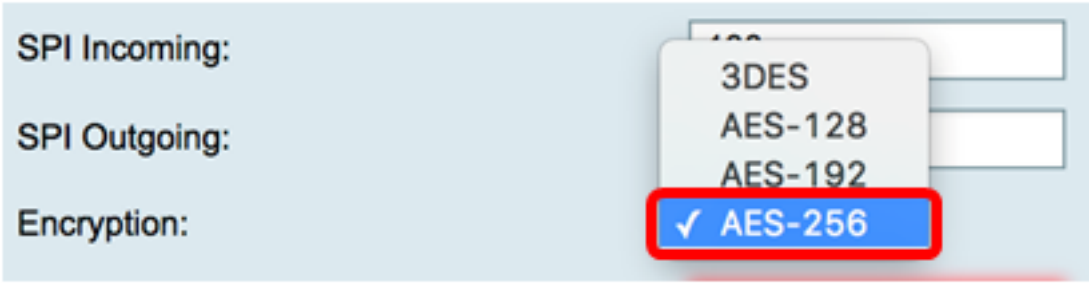

Étape 2. Dans le champ *SPI-Sortant*, saisissez un nombre hexadécimal compris entre 100 et FFFFFF pour la balise SPI du trafic sortant sur la connexion VPN.

**Note:** Pour cet exemple, 0x1234 est utilisé.




Étape 3. Sélectionnez une option dans la liste déroulante Cryptage. Les options sont 3DES, AES-128, AES-192 et AES-256.

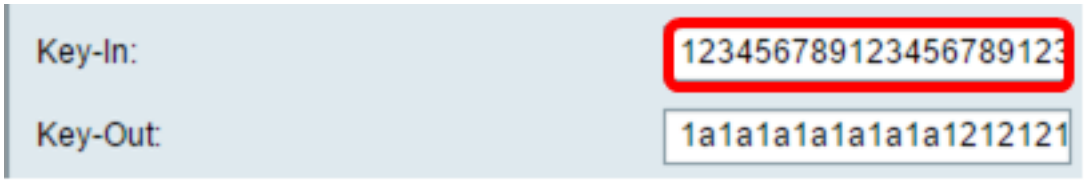
**Note:** Dans cet exemple, AES-256 est choisi.




Étape 4. Dans le champ *Key-In*, saisissez une clé pour la stratégie entrante. La longueur de la clé dépend de l'algorithme choisi à l'étape 3.

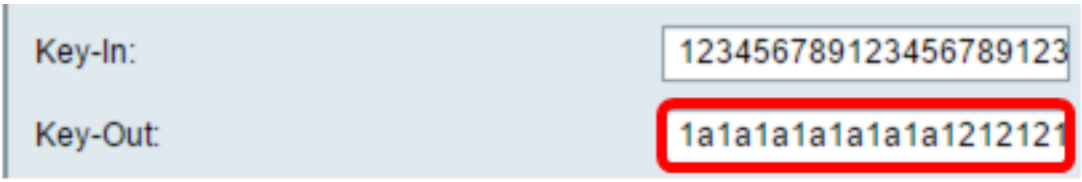
- 3DES utilise une clé de 48 caractères.
- L'AES-128 utilise une clé de 32 caractères.
- AES-192 utilise une clé de 48 caractères.
- L'AES-256 utilise une clé de 64 caractères.

**Note:** Dans cet exemple, 12345678912345678912 3... est utilisé.




Étape 5. Dans le champ *Clé sortante*, saisissez une clé pour la stratégie sortante. La longueur de la clé dépend de l'algorithme choisi à l'étape 3.

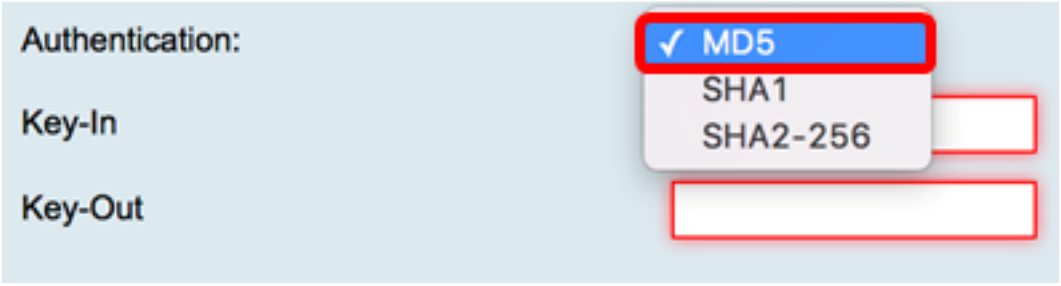
**Note**: Dans cet exemple, 1a1a1a1a1a1a1a121212... est utilisé.




Étape 6. Sélectionnez une option dans la liste déroulante Manual Integrity Algorithm.

- MD5 : utilise une valeur de hachage de 128 bits pour l'intégrité des données. MD5 est moins sécurisé mais plus rapide que SHA-1 et SHA2-256.
- SHA-1 : utilise une valeur de hachage de 160 bits pour l'intégrité des données. SHA-1 est plus lent mais plus sécurisé que MD5, et SHA-1 est plus rapide mais moins sécurisé que SHA2-256.
- SHA2-256 : utilise une valeur de hachage de 256 bits pour l'intégrité des données. SHA2-256 est plus lent mais plus sûr que MD5 et SHA-1.

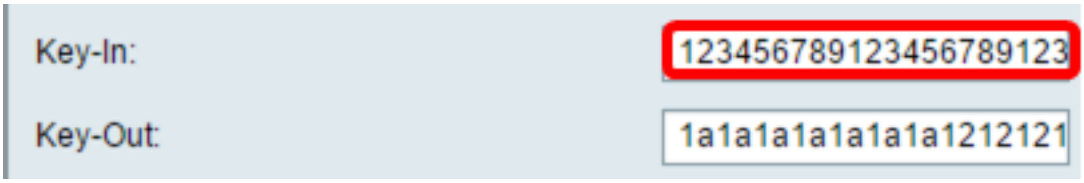
**Note:** Dans cet exemple, MD5 est sélectionné.




Étape 7. Dans le *champ Key-In*, saisissez une clé pour la stratégie entrante. La longueur de la clé dépend de l'algorithme choisi à l'étape 6.

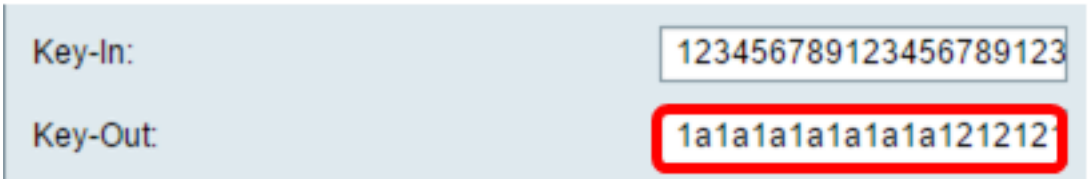
- MD5 utilise une clé de 32 caractères.
- SHA-1 utilise une clé de 40 caractères.
- SHA2-256 utilise une clé de 64 caractères.

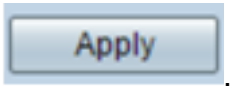
**Note:** Dans cet exemple, 12345678912345678912345... est utilisé.




Étape 8. Dans le *champ Clé sortante*, saisissez une clé pour la stratégie sortante. La longueur de la clé dépend de l'algorithme choisi à l'étape 6.

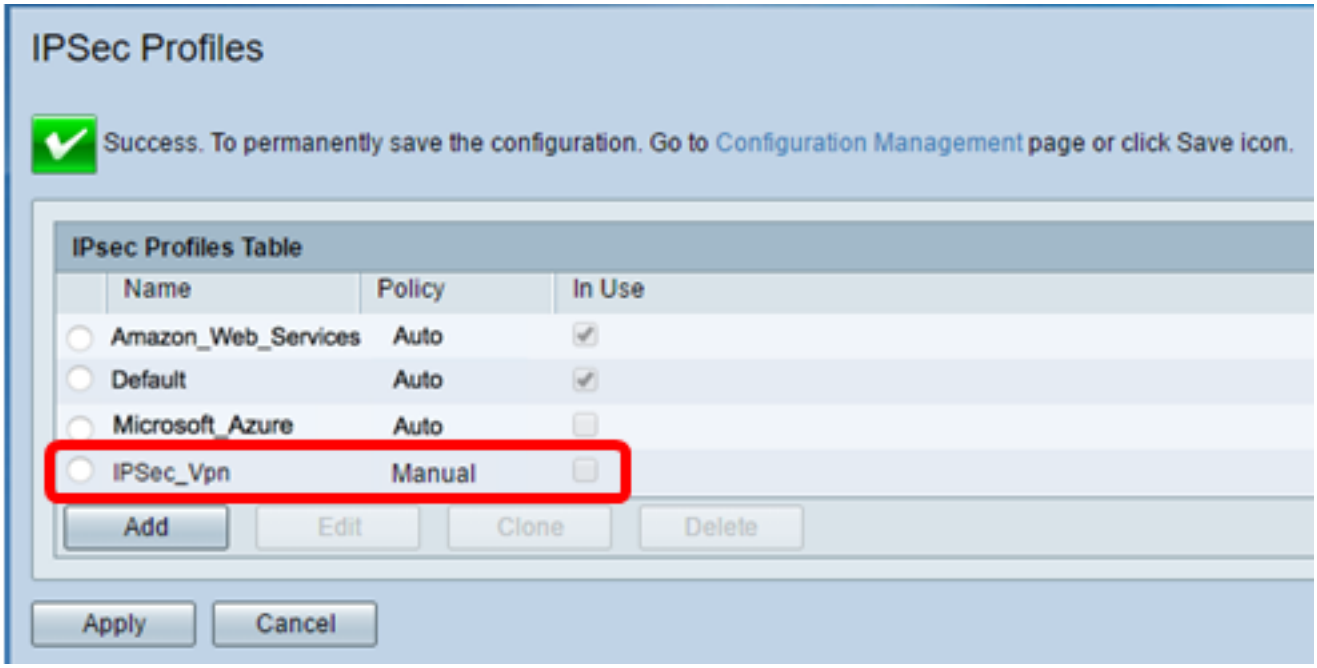
**Note:** Dans cet exemple, 1a1a1a1a1a1a1a121212... est utilisé.




Étape 9. Cliquez sur 

.

**Note:** Vous allez revenir à la table Profils IPSec et le profil IPSec nouvellement créé doit apparaître.




Étape 10. (Facultatif) Pour enregistrer définitivement la configuration, accédez à la page Copier/Enregistrer la configuration ou cliquez sur l' 

icône située dans la partie supérieure de la page.

Vous devez maintenant avoir correctement configuré un profil IPSec manuel sur un routeur de la gamme RV34x.