Configuration d'un serveur VPN IPSec sur RV130 et RV130W

Objectif

VPN IPSec (Virtual Private Network, réseau privé virtuel) vous permet d'obtenir un accès à distance sécurisé aux ressources de l'entreprise en établissant un tunnel crypté sur Internet.

L'objectif de ce document est de vous montrer comment configurer un serveur VPN IPSec sur RV130 et RV130W.

Note: Pour plus d'informations sur la façon de configurer un serveur VPN IPSec avec le client VPN logiciel Shrew sur RV130 et RV130W, référez-vous à l'article *Utiliser le client VPN logiciel Shrew avec le serveur VPN IPSec sur RV130 et RV130W*.

Périphériques pertinents

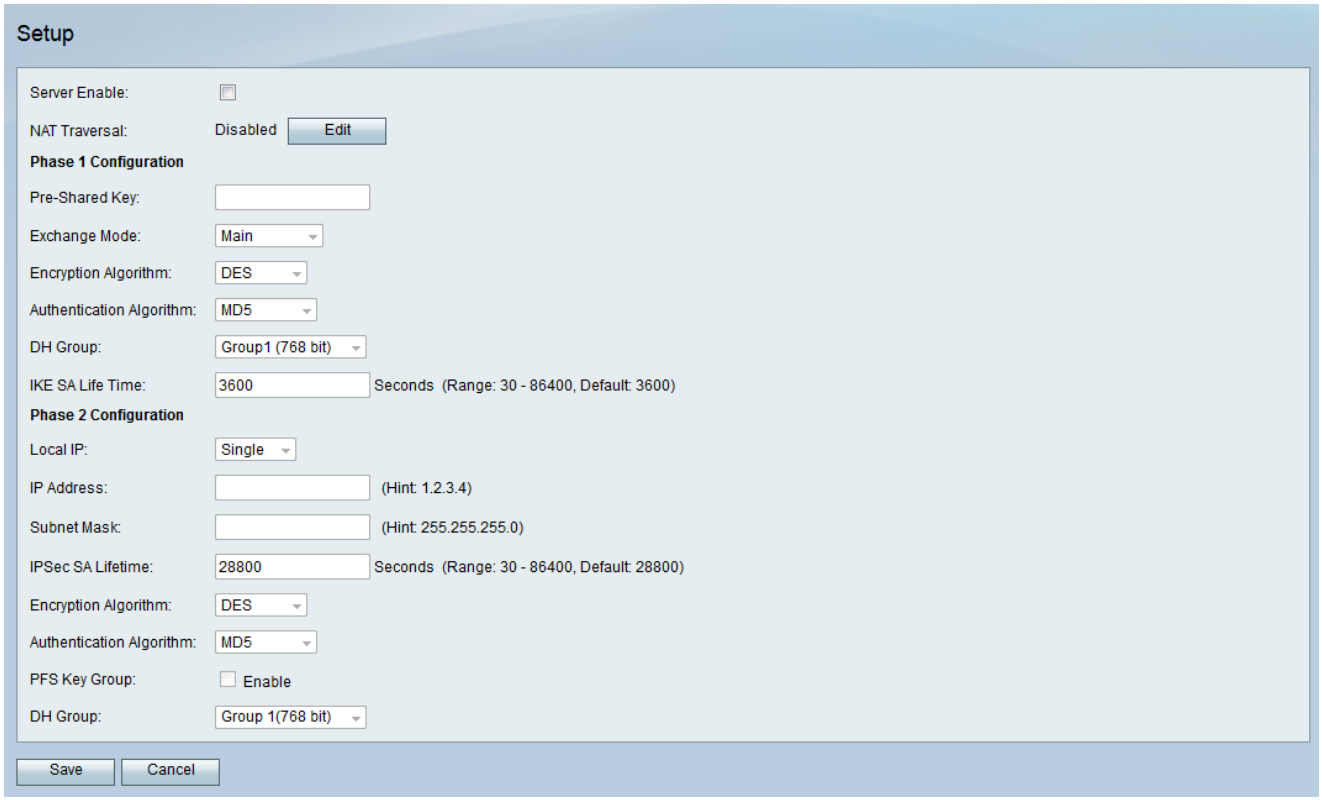
·Pare-feu VPN sans fil N RV130W
· Pare-feu VPN RV130

Version du logiciel

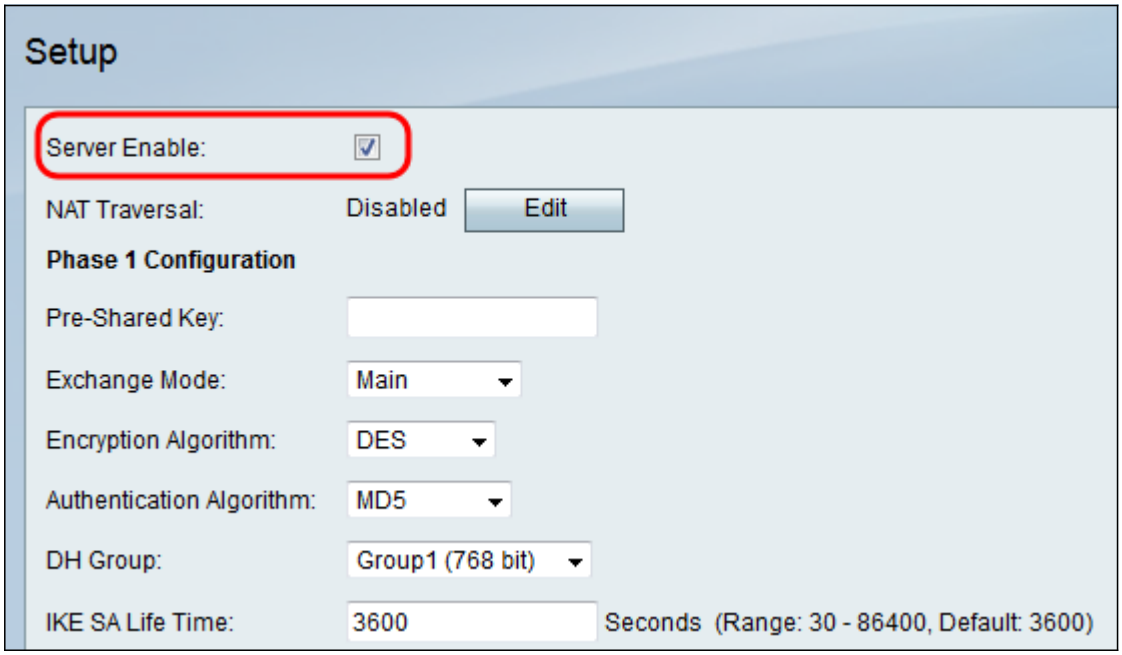
•v 1.0.1.3

Configuration du serveur VPN IPSec

Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez **VPN > IPSec VPN Server > Setup**. La page Setup s'ouvre.

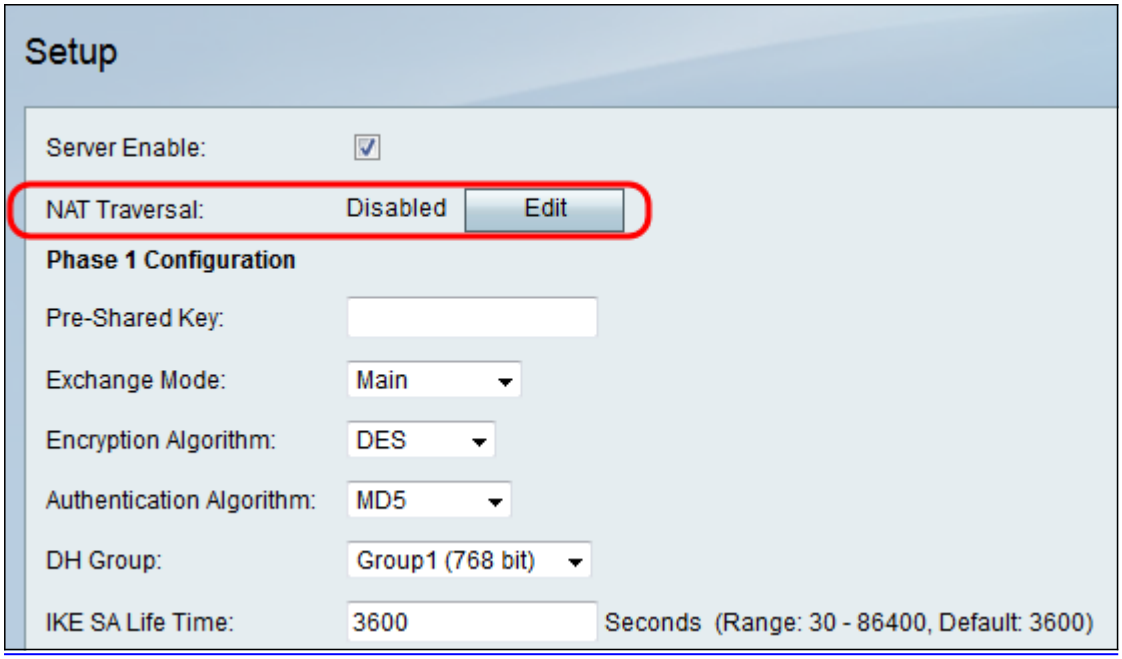


Étape 2. Cochez la case **Server Enable** pour activer le certificat.

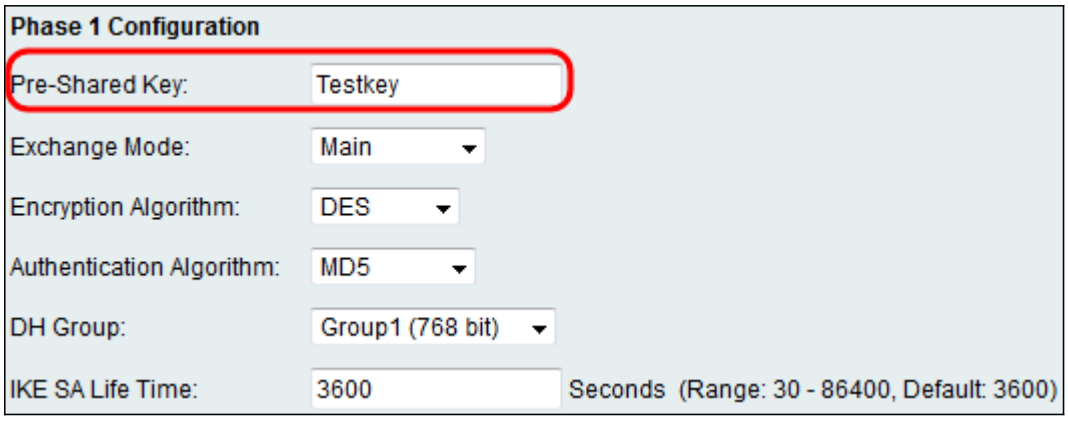


Étape 3. (Facultatif) Si votre routeur VPN ou client VPN est derrière une passerelle NAT, cliquez sur **Edit** pour configurer la traversée NAT. Sinon, laissez NAT Traversal désactivé.

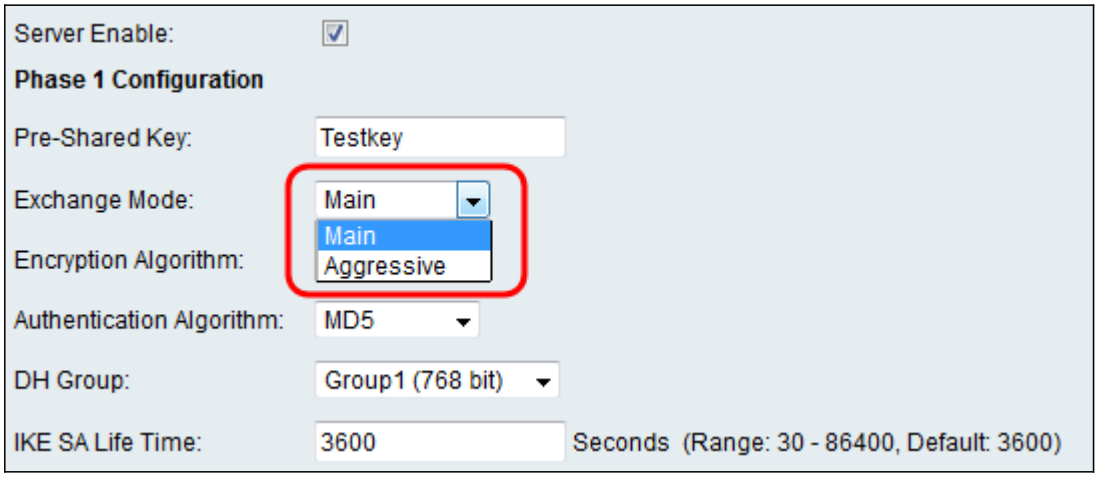
Note: Pour plus d'informations sur la façon de configurer les paramètres de traversée NAT, référez-vous à *Paramètres de stratégie IKE (Internet Key Exchange) sur les routeurs VPN RV130 et RV130W*.



Étape 4. Entrez une clé de 8 à 49 caractères qui sera échangée entre votre périphérique et le terminal distant dans le champ *Pre-Shared Key*.

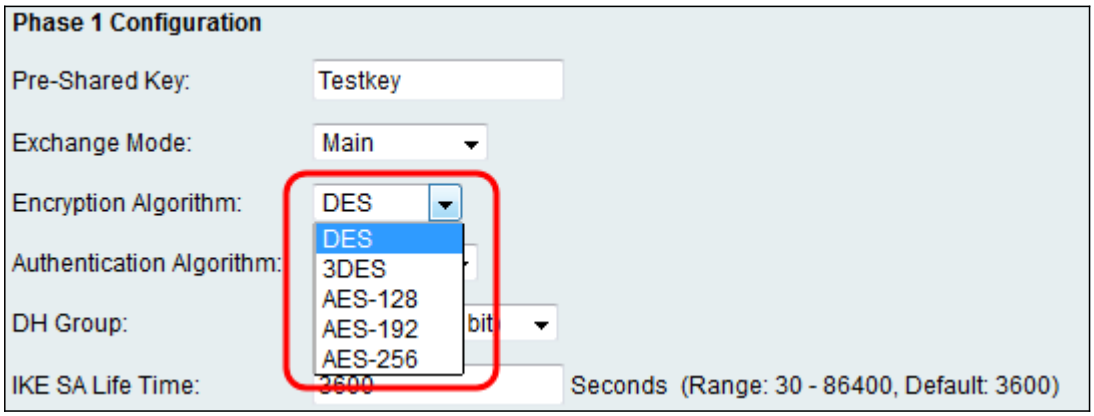


Étape 5. Dans la liste déroulante *Exchange Mode*, sélectionnez le mode de connexion VPN IPSec. **Main** est le mode par défaut. Cependant, si la vitesse de votre réseau est faible, choisissez le mode **Aggressive**.



Note: Le mode agressif échange les ID des points d'extrémité du tunnel en texte clair pendant la connexion, ce qui nécessite moins de temps pour l'échange mais est moins sécurisé.

Étape 6. Dans la liste déroulante **Encryption Algorithm**, choisissez la méthode de cryptage appropriée pour crypter la clé pré-partagée dans Phase 1. AES-128 est recommandé pour sa sécurité élevée et ses performances rapides.Le tunnel VPN doit utiliser la même méthode de cryptage pour ses deux extrémités.



Les options disponibles sont définies comme suit :

·DES — Data Encryption Standard (DES) est une ancienne méthode de chiffrement de 56 bits qui n'est pas très sûre, mais qui peut être requise pour la rétrocompatibilité.

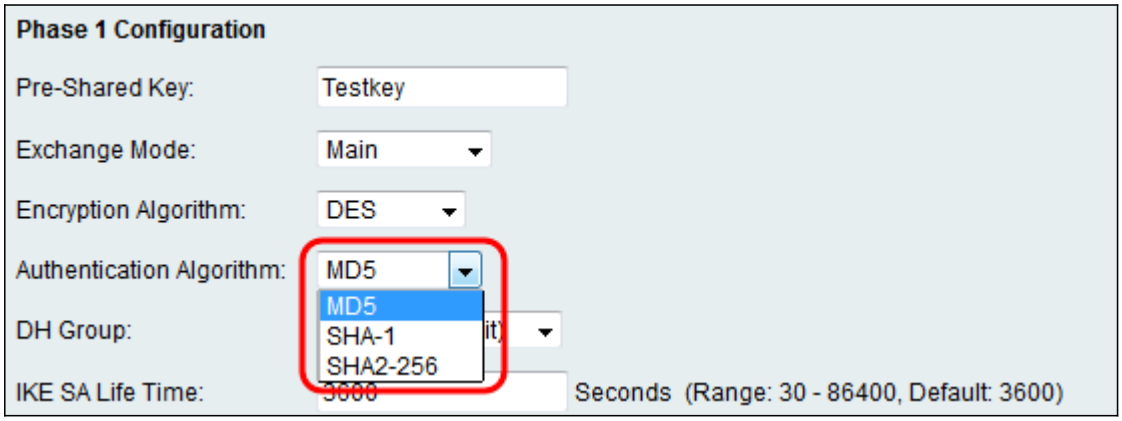
·3DES - La norme 3DES (Triple Data Encryption Standard) est une méthode de chiffrement simple de 168 bits utilisée pour augmenter la taille de la clé, car elle chiffre les données trois fois. Cela offre plus de sécurité que DES, mais moins de sécurité que AES.

·AES-128 - Advanced Encryption Standard avec clé 128 bits (AES-128) utilise une clé 128 bits pour le cryptage AES. AES est plus rapide et plus sécurisé que DES. En général, AES est également plus rapide et plus sécurisé que 3DES. AES-128 est plus rapide mais moins sécurisé que AES-192 et AES-256.

·AES-192 : AES-192 utilise une clé de 192 bits pour le cryptage AES. AES-192 est plus lent mais plus sécurisé que AES-128, et plus rapide mais moins sécurisé que AES-256.

·AES-256 - AES-256 utilise une clé de 256 bits pour le cryptage AES. AES-256 est plus lent mais plus sécurisé que AES-128 et AES-192.

Étape 7. Dans la liste déroulante *Authentication Algorithm*, choisissez la méthode d'authentification appropriée pour déterminer comment les paquets d'en-tête du protocole ESP (Encapsulating Security Payload) sont validés dans la phase 1. Le tunnel VPN doit utiliser la même méthode d'authentification pour les deux extrémités de la connexion.



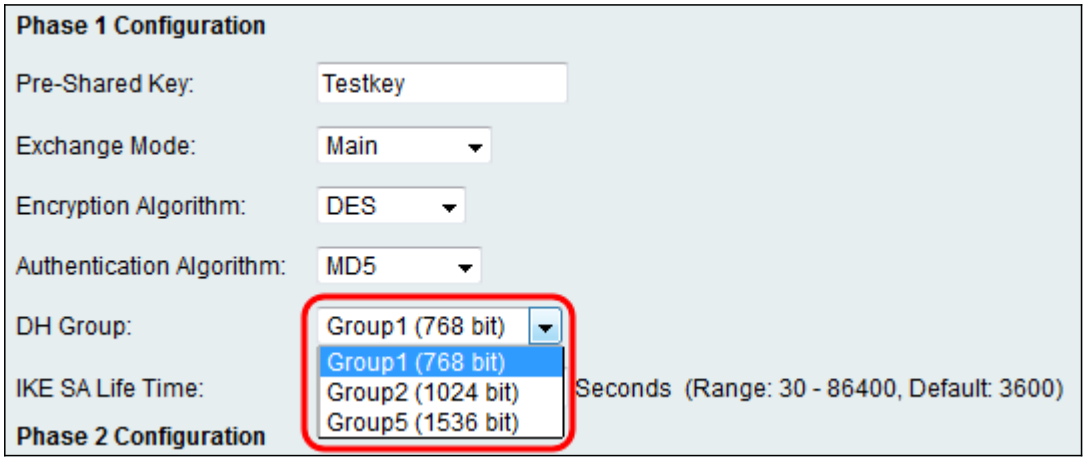
Les options disponibles sont définies comme suit :

·MD5 : MD5 est un algorithme de hachage unidirectionnel qui produit un condensé de 128 bits. MD5 calcule plus rapidement que SHA-1, mais est moins sécurisé que SHA-1. MD5 n'est pas recommandé.

·SHA-1 : SHA-1 est un algorithme de hachage unidirectionnel qui produit un condensé de 160 bits. SHA-1 calcule plus lentement que MD5, mais est plus sécurisé que MD5.

·SHA2-256 — Spécifie l'algorithme de hachage sécurisé SHA2 avec le condensé 256 bits.

Étape 8. Dans la liste déroulante *DH Group*, sélectionnez le groupe Diffie-Hellman (DH) approprié à utiliser avec la clé dans la phase 1. Diffie-Hellman est un protocole d'échange de clés cryptographiques qui est utilisé dans la connexion pour échanger des ensembles de clés pré-partagées. La puissance de l'algorithme est déterminée par les bits.



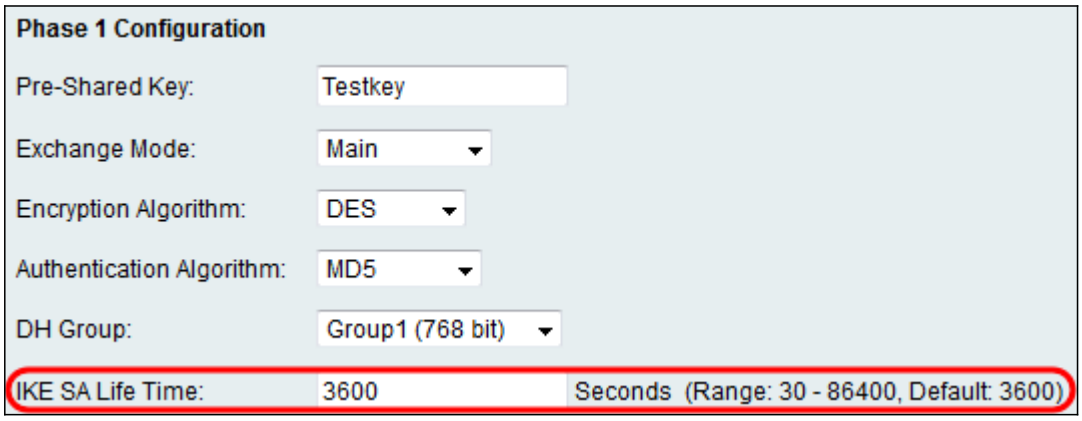
Les options disponibles sont définies comme suit :

·Group1 (768 bits) - Calcule la clé la plus rapide, mais la moins sûre.

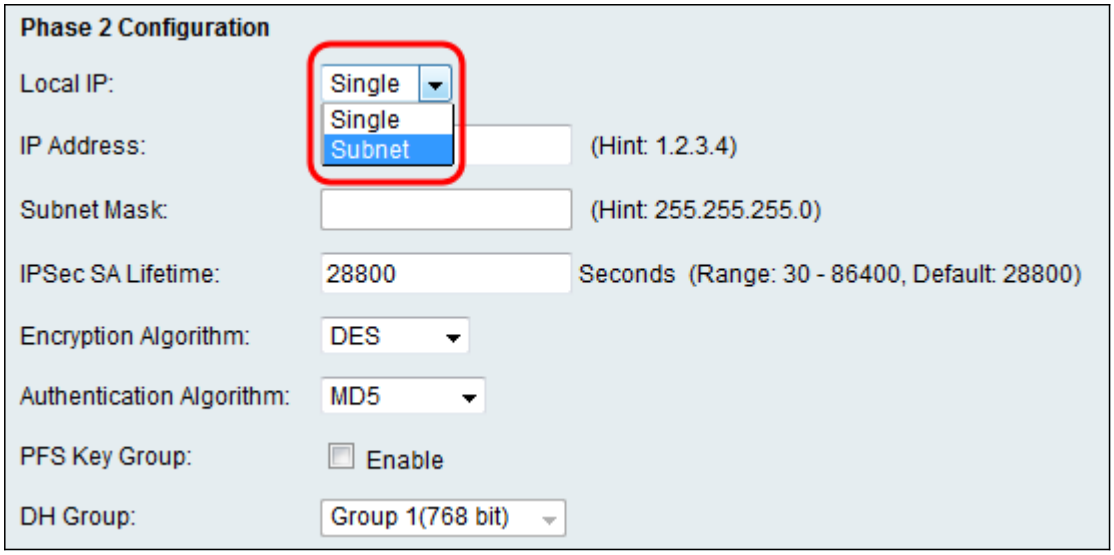
·Group2 (1024 bits) : calcule la clé plus lentement, mais est plus sécurisé que Group1.

·Group5 (1536 bits) : calcule la clé le plus lentement, mais en toute sécurité.

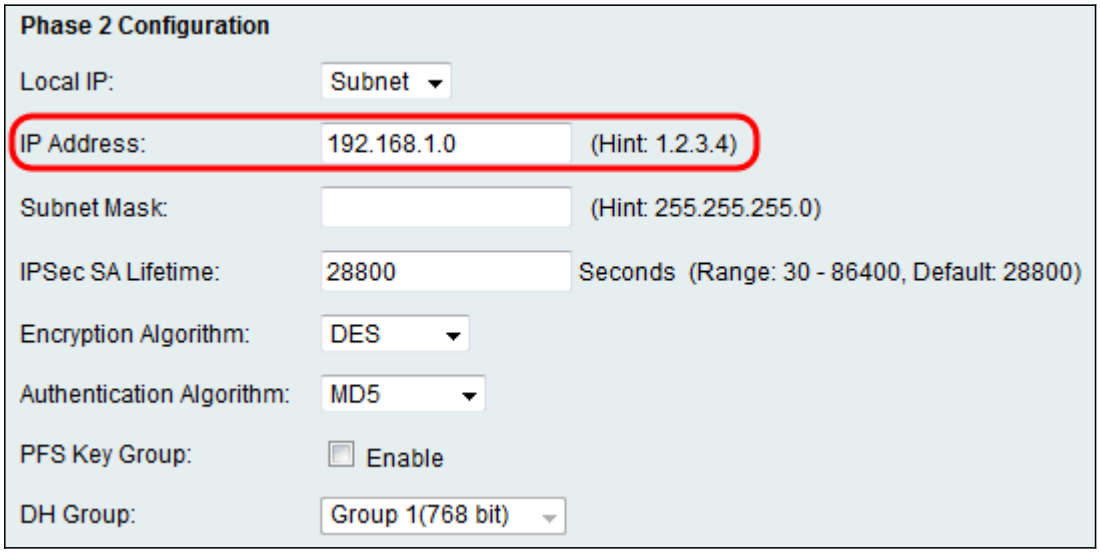
Étape 9. Dans le champ *IKE SA Life Time*, saisissez la durée, en secondes, pendant laquelle la clé IKE automatique est valide. Une fois ce délai écoulé, une nouvelle clé est négociée automatiquement.



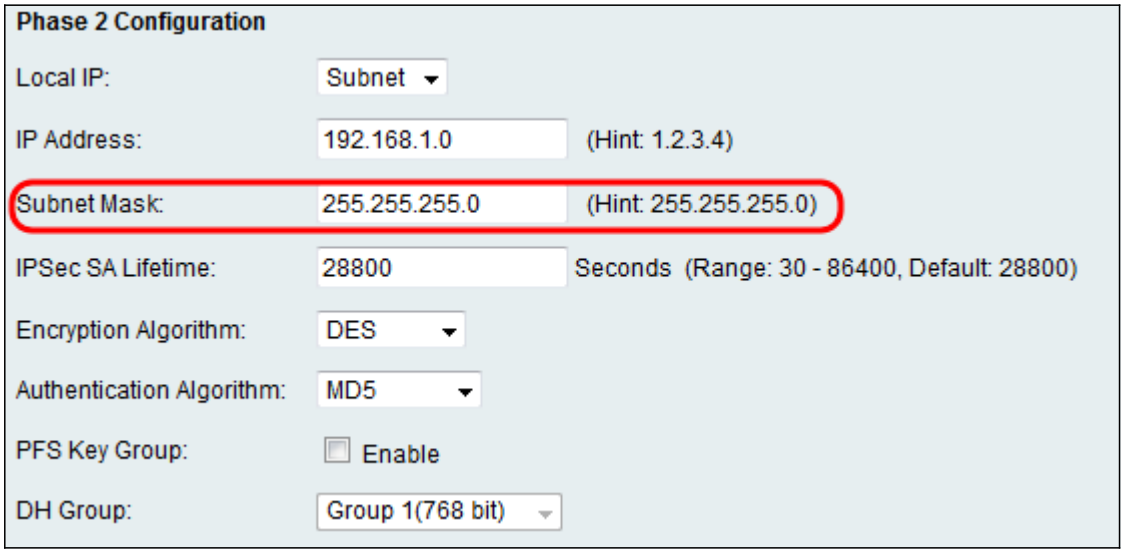
Étape 10. Dans la liste déroulante *Local IP*, sélectionnez **Single** si vous souhaitez qu'un seul utilisateur local du réseau local accède au tunnel VPN, ou sélectionnez **Subnet** si vous souhaitez que plusieurs utilisateurs puissent y accéder.



Étape 11. Si **Subnet** a été choisi à l'étape 10, entrez l'adresse IP réseau du sous-réseau dans le champ IP Address. Si **Single** a été choisi à l'étape 10, entrez l'adresse IP de l'utilisateur unique et passez à l'étape 13.

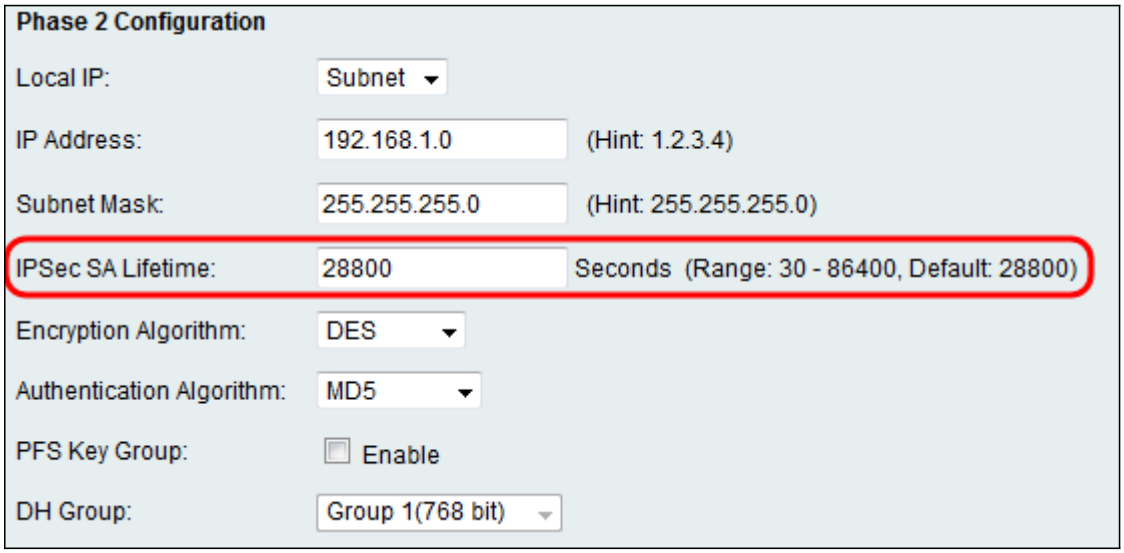


Étape 12. (Facultatif) Si **Subnet** a été choisi à l'étape 10, entrez le masque de sous-réseau du réseau local dans le champ *Subnet Mask*.

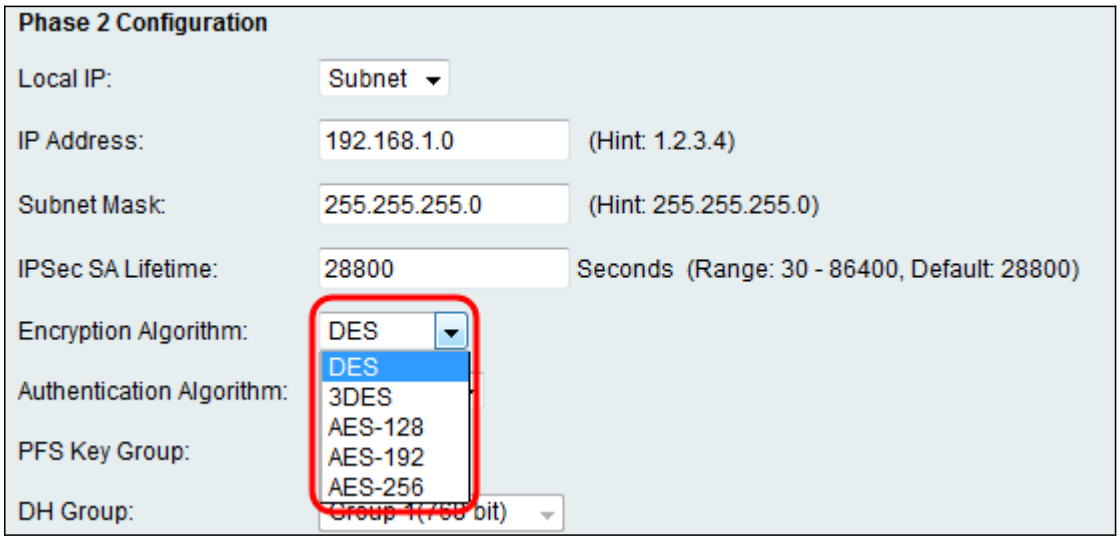


Étape 13. Dans le champ *IPSec SA Lifetime*, entrez la durée en secondes pendant laquelle

la connexion VPN reste active dans la phase 2. Une fois cette durée expirée, l'association de sécurité IPSec pour la connexion VPN est renégociée.



Étape 14. Dans la liste déroulante *Encryption Algorithm*, choisissez la méthode de cryptage appropriée pour crypter la clé pré-partagée dans Phase 2. AES-128 est recommandé pour sa sécurité élevée et ses performances rapides.Le tunnel VPN doit utiliser la même méthode de cryptage pour ses deux extrémités.



Les options disponibles sont définies comme suit :

·DES — Data Encryption Standard (DES) est une ancienne méthode de chiffrement de 56 bits qui est la moins sûre, mais qui peut être requise pour la rétrocompatibilité.

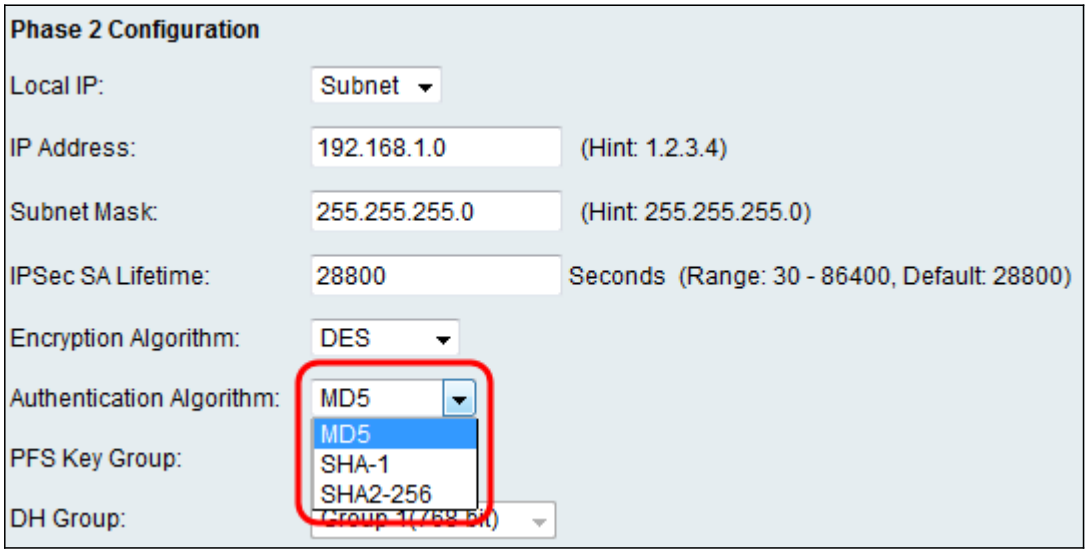
·3DES - La norme 3DES (Triple Data Encryption Standard) est une méthode de chiffrement simple de 168 bits utilisée pour augmenter la taille de la clé, car elle chiffre les données trois fois. Cela offre plus de sécurité que DES, mais moins de sécurité que AES.

·AES-128 - Advanced Encryption Standard avec clé 128 bits (AES-128) utilise une clé 128 bits pour le cryptage AES. AES est plus rapide et plus sécurisé que DES. En général, AES est également plus rapide et plus sécurisé que 3DES. AES-128 est plus rapide mais moins sécurisé que AES-192 et AES-256.

·AES-192 : AES-192 utilise une clé de 192 bits pour le cryptage AES. AES-192 est plus lent mais plus sécurisé que AES-128, et plus rapide mais moins sécurisé que AES-256.

·AES-256 - AES-256 utilise une clé de 256 bits pour le cryptage AES. AES-256 est plus lent mais plus sécurisé que AES-128 et AES-192.

Étape 15. Dans la liste déroulante *Authentication Algorithm*, choisissez la méthode d'authentification appropriée pour déterminer comment les paquets d'en-tête du protocole ESP (Encapsulating Security Payload) sont validés au cours de la phase 2. Le tunnel VPN doit utiliser la même méthode d'authentification pour ses deux extrémités.



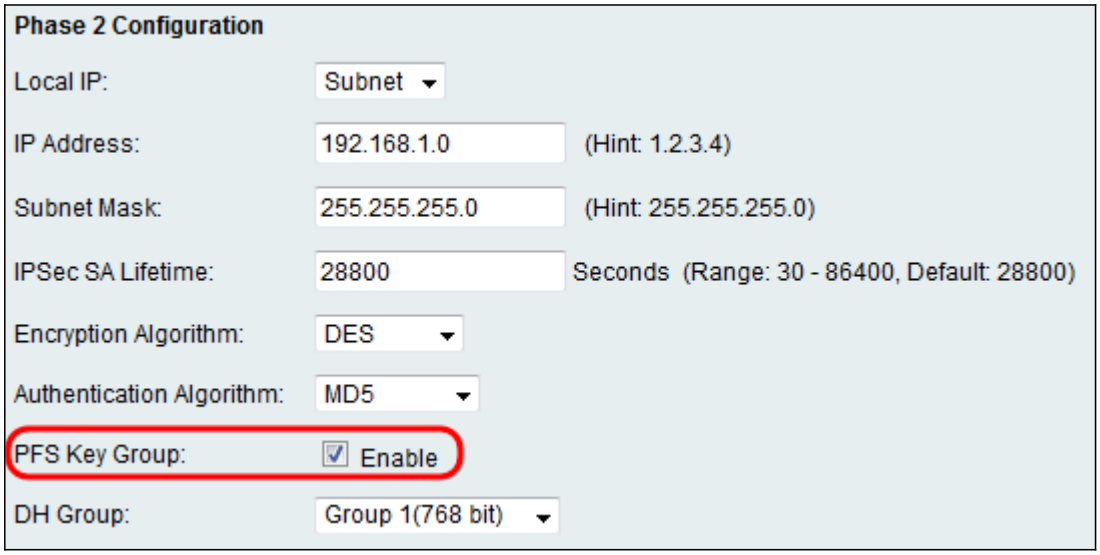
Les options disponibles sont définies comme suit :

·MD5 : MD5 est un algorithme de hachage unidirectionnel qui produit un condensé de 128 bits. MD5 calcule plus rapidement que SHA-1, mais est moins sécurisé que SHA-1. MD5 n'est pas recommandé.

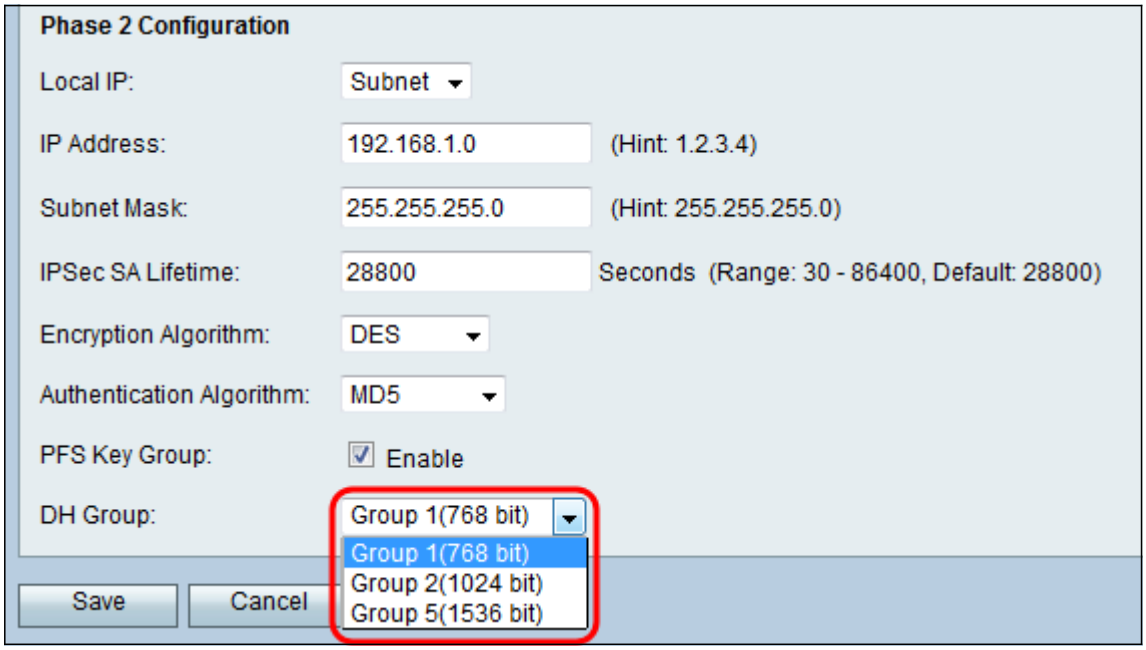
·SHA-1 : SHA-1 est un algorithme de hachage unidirectionnel qui produit un condensé de 160 bits. SHA-1 calcule plus lentement que MD5, mais est plus sécurisé que MD5.

·SHA2-256 — Spécifie l'algorithme de hachage sécurisé SHA2 avec le condensé 256 bits.

Étape 16. (Facultatif) Dans le champ *PFS Key Group*, cochez la case **Enable**. PFS (Perfect Forward Secrecy) crée une couche de sécurité supplémentaire pour la protection de vos données en garantissant une nouvelle clé DH dans la Phase 2. Le processus est effectué au cas où la clé DH générée dans la Phase 1 serait compromise en cours de transfert.



Étape 17. Dans la liste déroulante *Groupe DH*, sélectionnez le groupe Diffie-Hellman (DH) approprié à utiliser avec la clé de la phase 2.



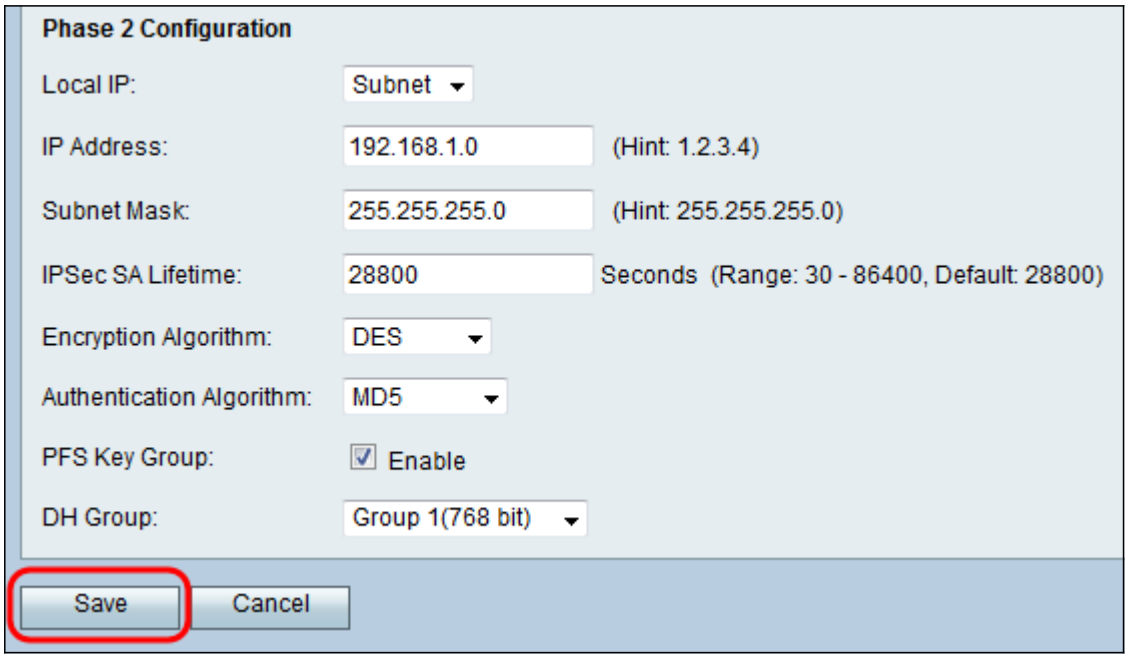
Les options disponibles sont définies comme suit :

·Group1 (768 bits) - Calcule la clé la plus rapide, mais la moins sûre.

·Group2 (1024 bits) : calcule la clé plus lentement, mais est plus sécurisé que Group1.

·Group5 (1536 bits) : calcule la clé le plus lentement, mais en toute sécurité.

Étape 18. Cliquez sur **Save** pour enregistrer vos paramètres.



Pour plus d'informations, consultez la documentation suivante :

- Fiche technique du routeur RV130 : explique les fonctionnalités VPN des routeurs de la gamme RV130
- Page produit RV130 - inclut des liens vers tous les articles RV130 de Cisco

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.