Configuration du client VPN logiciel Shrew avec les routeurs RV160 et RV260

Objectif

L'objectif de ce document est de vous montrer comment configurer les paramètres nécessaires pour connecter le client VPN logiciel Shrew via les routeurs de la gamme RV160 ou RV260.

Présentation des bases du VPN

Un réseau privé virtuel (VPN) est un excellent moyen de connecter des utilisateurs distants à un réseau sécurisé. Il établit une connexion chiffrée sur un réseau moins sécurisé comme Internet.

Un tunnel VPN établit un réseau privé qui peut envoyer des données en toute sécurité à l'aide du chiffrement et de l'authentification. Les bureaux d'entreprise utilisent souvent une connexion VPN, car il est à la fois utile et nécessaire de permettre à leurs employés d'accéder à leurs ressources internes, même s'ils se trouvent à l'extérieur du bureau.

Le routeur RV160 prend en charge jusqu'à 10 tunnels VPN et le routeur RV260 jusqu'à 20.

Cet article décrit les étapes nécessaires à la configuration du routeur RV160/RV260 et du client VPN logiciel Shrew. Vous apprendrez à créer un groupe d'utilisateurs, un compte d'utilisateur, un profil IPsec et un profil client-à-site. Sur le client VPN logiciel Shrew, vous apprendrez à configurer les onglets Général, Client, Résolution de noms, Authentification, Phase 1 et Phase 2.

Quels sont les avantages et les inconvénients d'un VPN ?

Les réseaux privés virtuels permettent d'aborder des scénarios d'utilisation réelle communs à de nombreux secteurs et types d'entreprise. Le tableau ci-dessous présente certains des avantages et des inconvénients de l'utilisation d'un VPN.

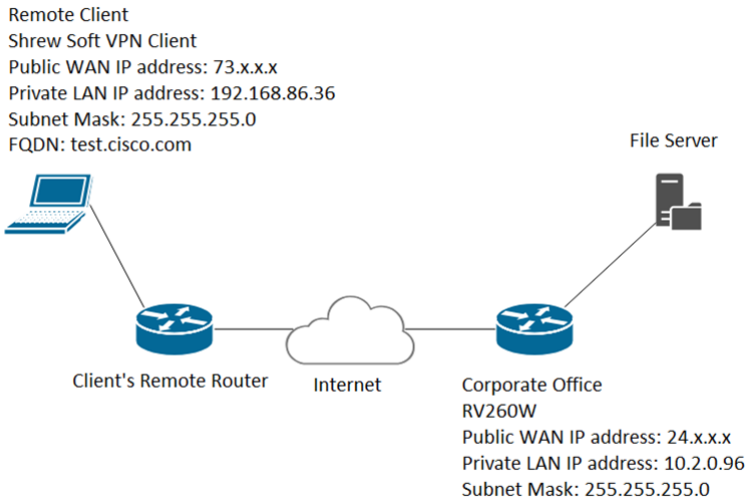
Avantages	Cons
Fournit des communications, une commodité et une accessibilité sécurisées avec des droits d'accès adaptés aux utilisateurs individuels, tels que les employés, les sous-traitants ou les partenaires.	La vitesse de connexion peut être lente. Un chiffrement plus fort demande du temps et des ressources pour garantir l'anonymat et la sécurité. Le chiffrement du trafic réseau nécessite généralement un peu plus de surcharge. Vous pouvez peut-être trouver deux fournisseurs VPN qui maintiennent une bonne vitesse de connexion tout en gardant l'anonymat et la sécurité, mais ils

	sont généralement des services payants.
Améliore la productivité en étendant le réseau et les applications de l'entreprise.	Risque potentiel de sécurité dû à des erreurs de configuration. La conception et la mise en oeuvre d'un VPN peuvent être compliquées. Il est nécessaire de confier à un professionnel expérimenté la configuration de votre VPN pour s'assurer que votre réseau ne sera pas compromis.
Réduit les coûts de communication et augmente la flexibilité.	Si une situation se produit lorsqu'il est nécessaire d'ajouter une nouvelle infrastructure ou un nouvel ensemble de configurations, des problèmes techniques peuvent survenir en raison de l'incompatibilité, en particulier s'il s'agit de produits ou de fournisseurs différents autres que ceux que vous utilisez déjà.
L'emplacement géographique réel des utilisateurs est protégé et n'est pas exposé aux réseaux publics ou partagés comme Internet.	
Protection des données et des ressources réseau confidentielles.	
Un VPN permet d'ajouter de nouveaux utilisateurs ou un groupe d'utilisateurs sans avoir à ajouter de composants supplémentaires ou une configuration compliquée.	

Topologie

Il s’agit d’une topologie simple du réseau.

Note: L'adresse IP WAN publique a été effacée.



Périphériques pertinents

- RV160
- RV260

Version du logiciel

- 1.0.0.xx (RV160 et RV260)
- 2.2.1 est recommandé car 2.2.2 peut rencontrer des problèmes de connectivité avec nos routeurs (Téléchargement du client VPN logiciel Shrew)

Table des matières

1. Création de groupes d'utilisateurs
2. Création de comptes utilisateur
3. Configuration du profil IPsec
4. Configuration de client à site
5. Configuration du client VPN logiciel Shrew
6. Client VPN logiciel Shrew : Onglet Général
7. Client VPN logiciel Shrew : Onglet Client
8. Client VPN logiciel Shrew : Onglet Résolution de nom
9. Client VPN logiciel Shrew : Onglet Authentification
10. Client VPN logiciel Shrew : Onglet Phase 1
11. Client VPN logiciel Shrew : Onglet Phase 2

12. Client VPN logiciel Shrew : Connexion

13. Conseils de dépannage de la connexion VPN

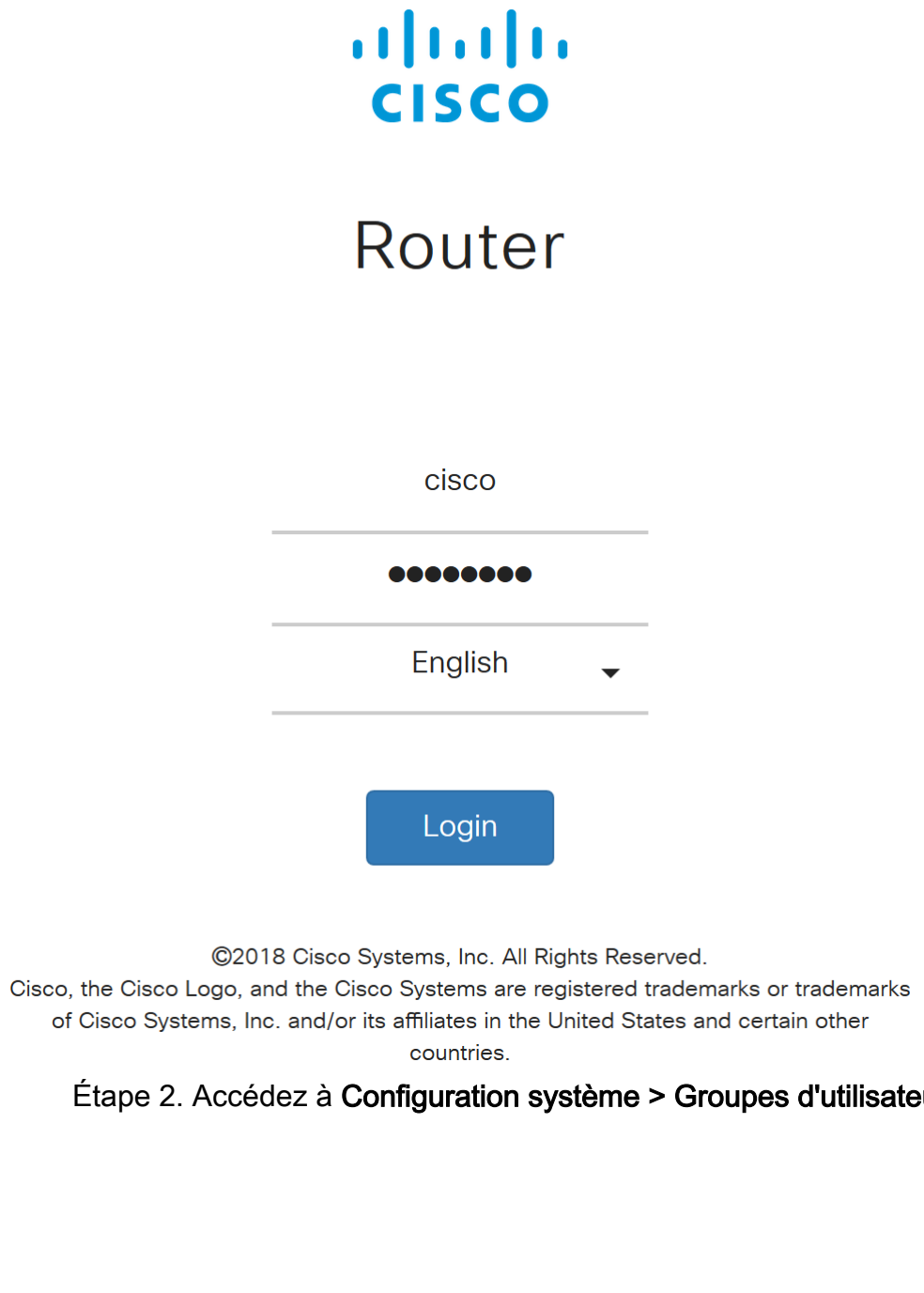
14. Vérification

15. Conclusion

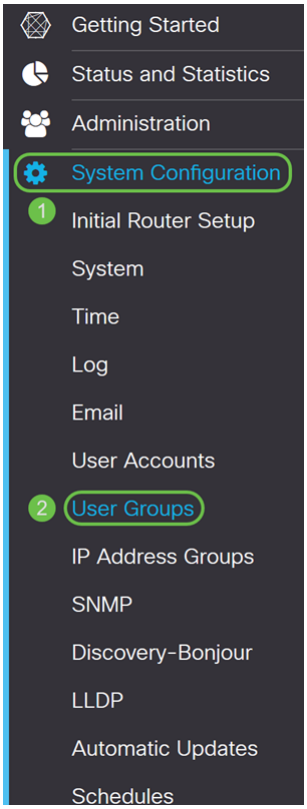
Création de groupes d'utilisateurs

Remarque importante : Laissez le compte d'administrateur par défaut dans le groupe d'administrateurs et créez un nouveau compte d'utilisateur et un nouveau groupe d'utilisateurs pour Shrew Soft. Si vous déplacez votre compte d'administrateur vers un autre groupe, vous vous empêcherez de vous connecter au routeur.

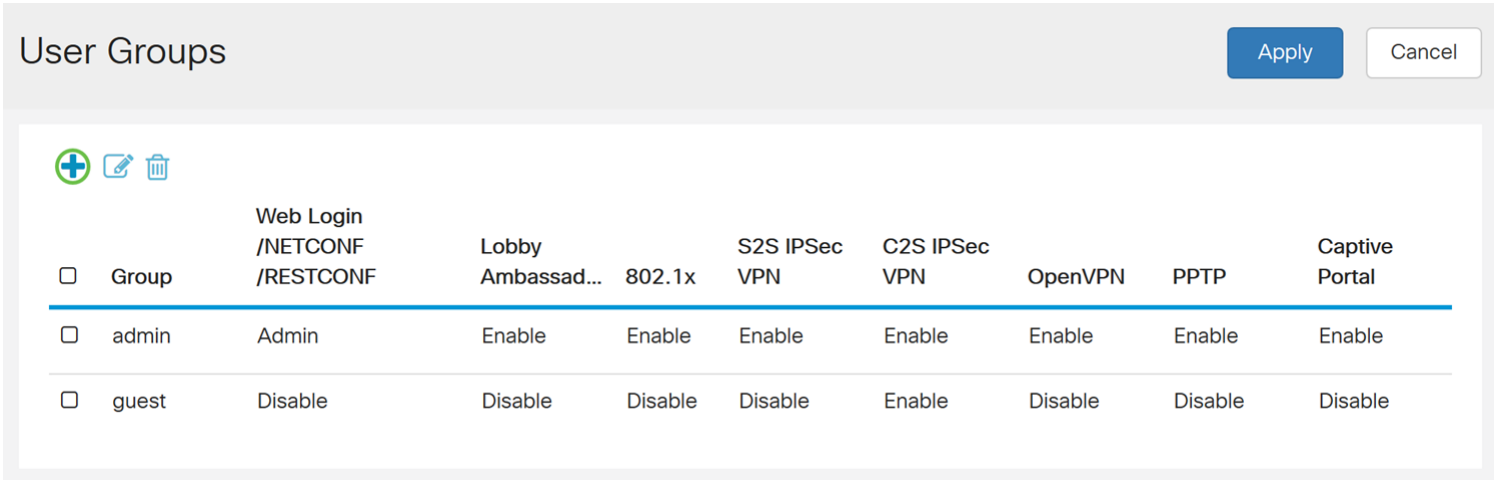
Étape 1. Connectez-vous à la page de configuration Web.



Étape 2. Accédez à **Configuration système > Groupes d'utilisateurs**.

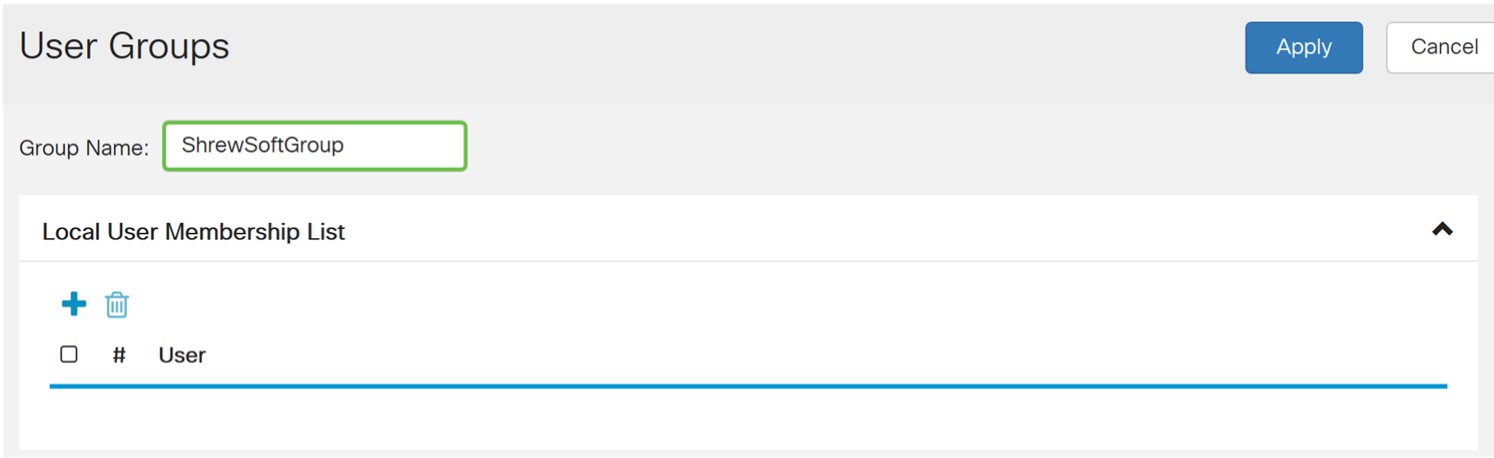


Étape 3. Cliquez sur l'icône **plus** pour ajouter un nouveau groupe d'utilisateurs.

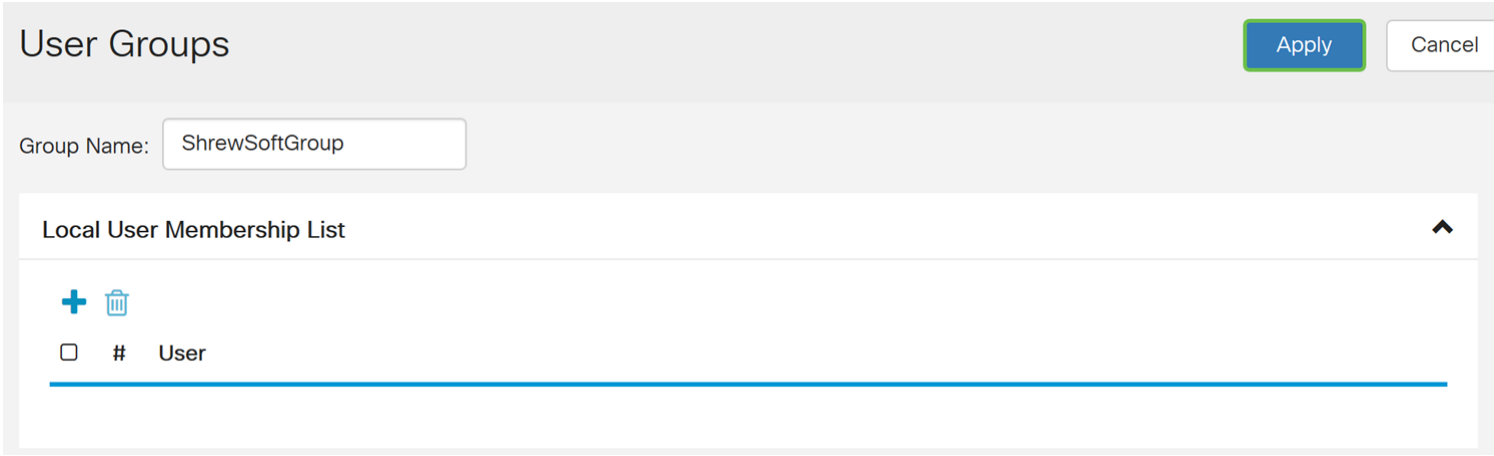


Étape 4. Entrez un nom pour le groupe dans le champ *Nom du groupe*.

Nous utiliserons **ShrewSoftGroup** comme exemple.

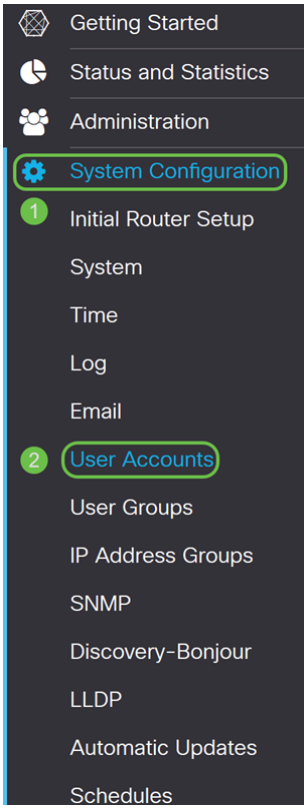


Étape 5. Appuyez sur **Apply** pour créer un nouveau groupe.

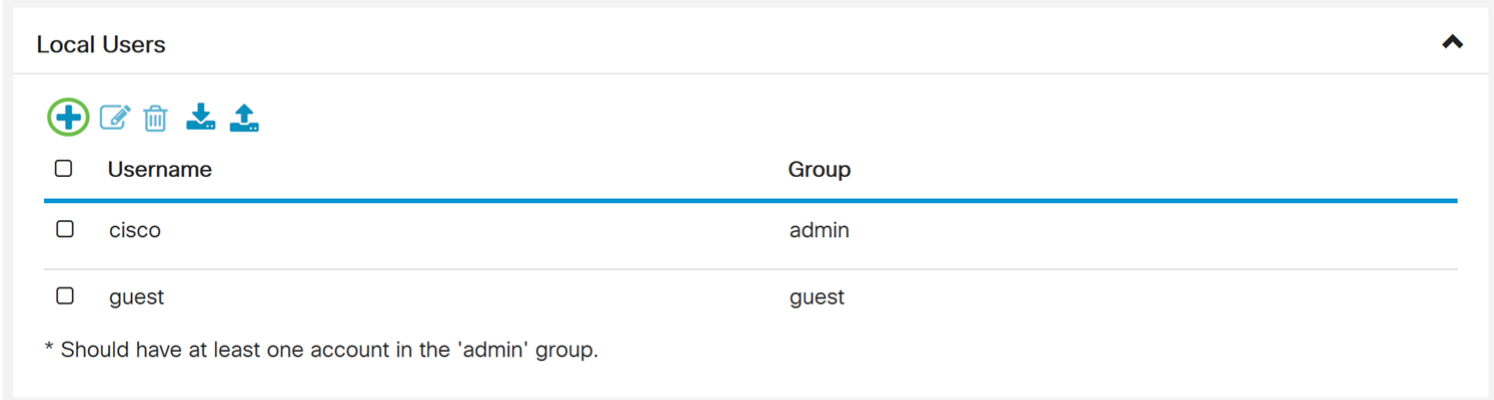


Création de comptes utilisateur

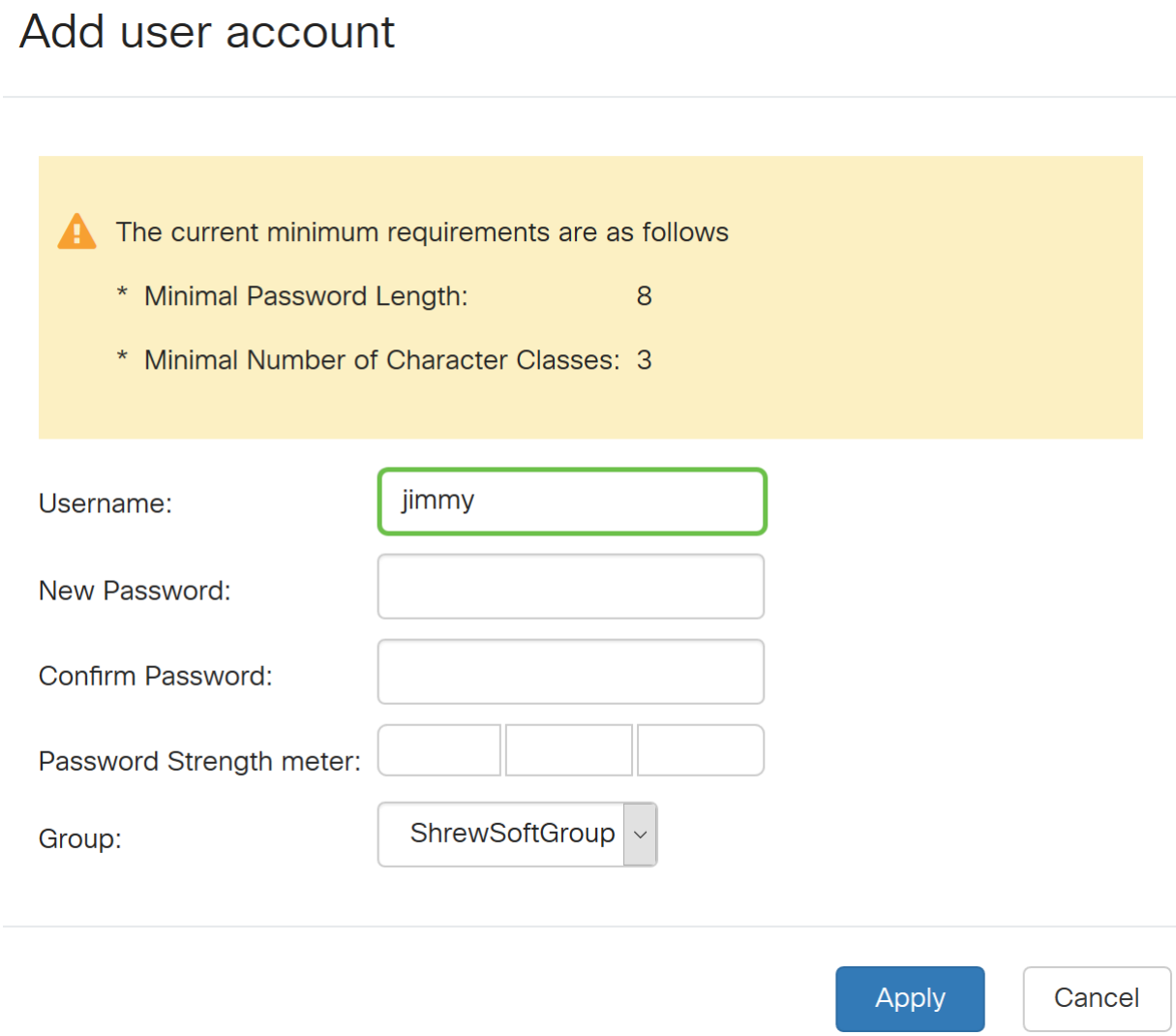
Étape 1. Accédez à **Configuration système > Comptes d'utilisateurs**.



Étape 2. Faites défiler jusqu'au tableau *Utilisateurs locaux* et appuyez sur l'icône **plus** pour ajouter un nouvel utilisateur.

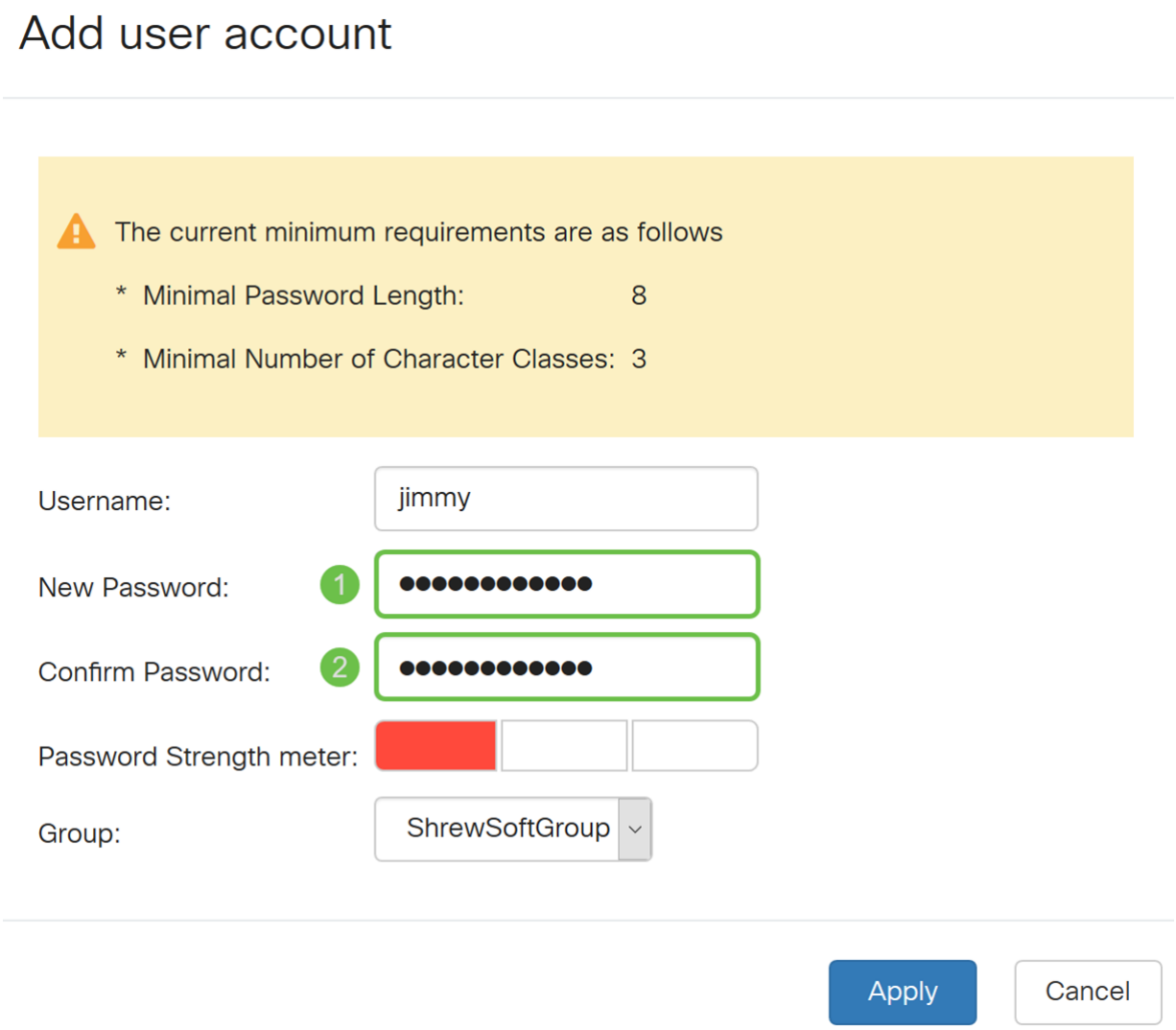


Étape 3. La page *Ajouter des comptes d'utilisateurs* s'ouvre. Entrez un nom d'utilisateur pour l'utilisateur.

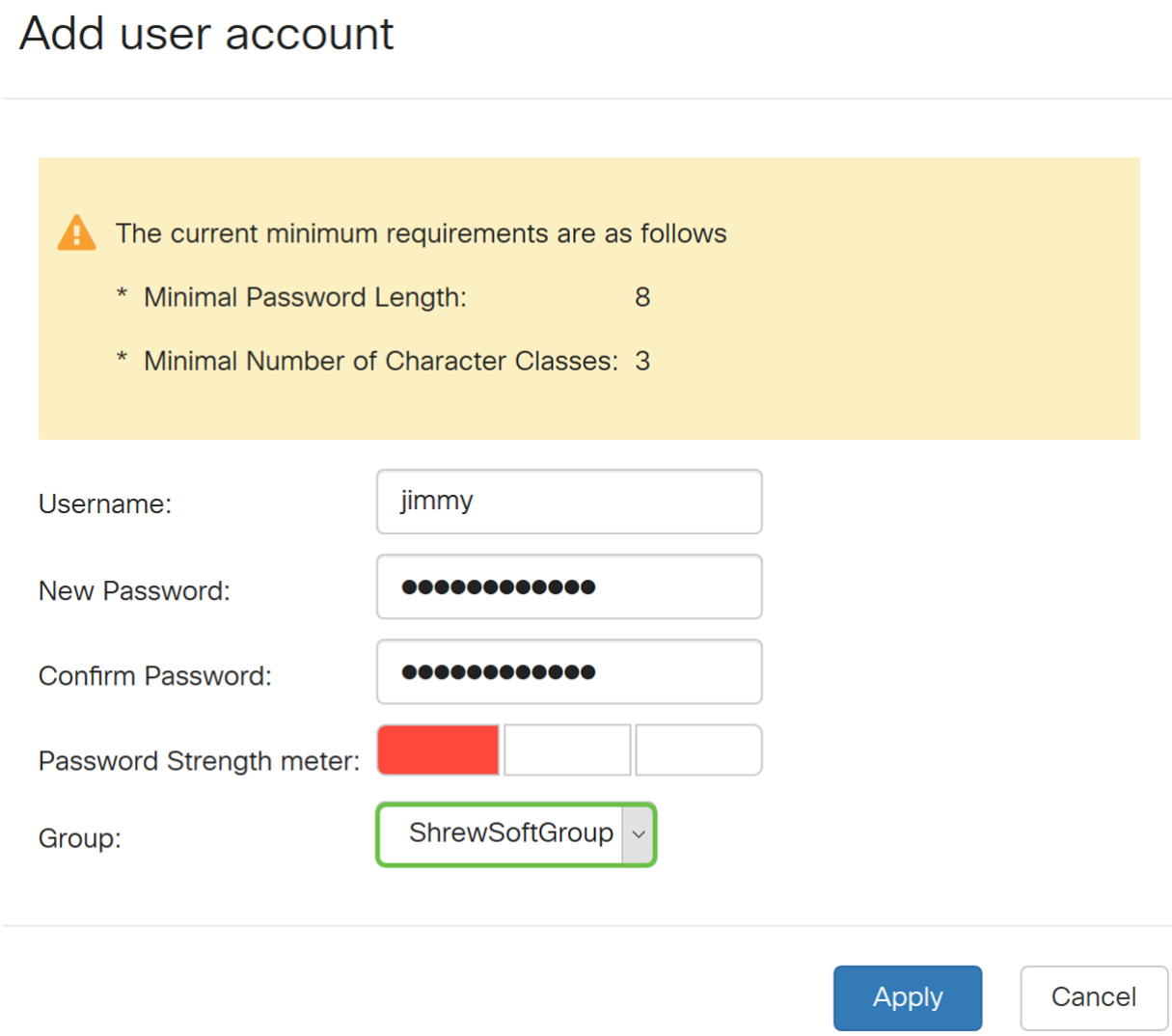


Étape 4. Entrez un mot de passe dans le champ *Nouveau mot de passe*. Entrez à nouveau le même mot de passe dans le champ *Confirmer le mot de passe*. Dans cet exemple, nous utiliserons **CiscoTest123** comme mot de passe.

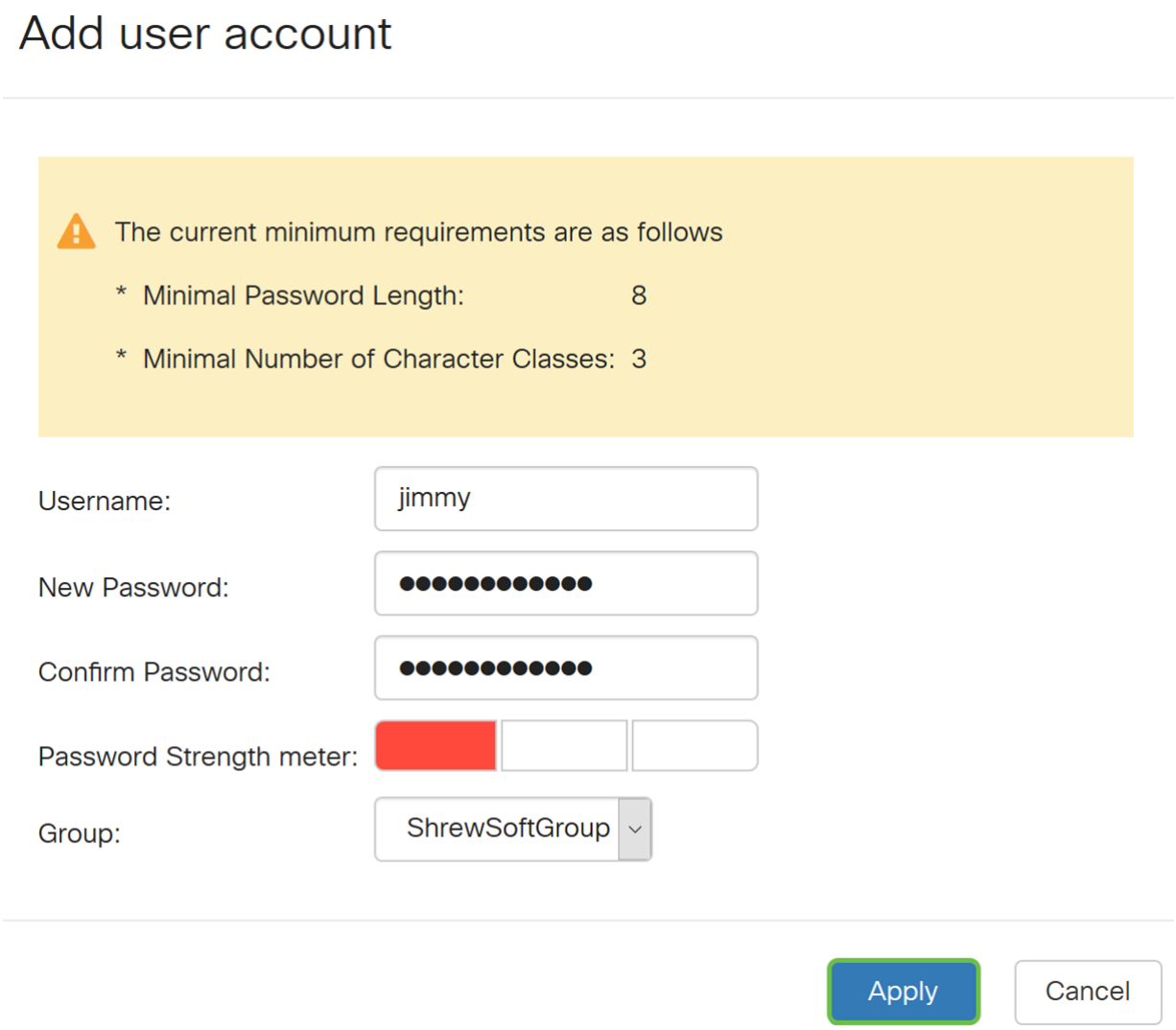
Note: Le mot de passe utilisé ici est un exemple. Il est recommandé de rendre votre mot de passe plus complexe.



Étape 5. Dans la liste déroulante *Groupe*, sélectionnez un groupe dans lequel l'utilisateur doit se trouver.

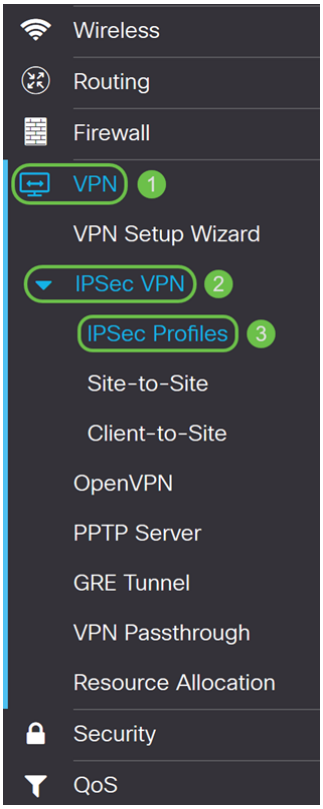


Étape 6. Appuyez sur **Apply** pour créer un compte d'utilisateur.



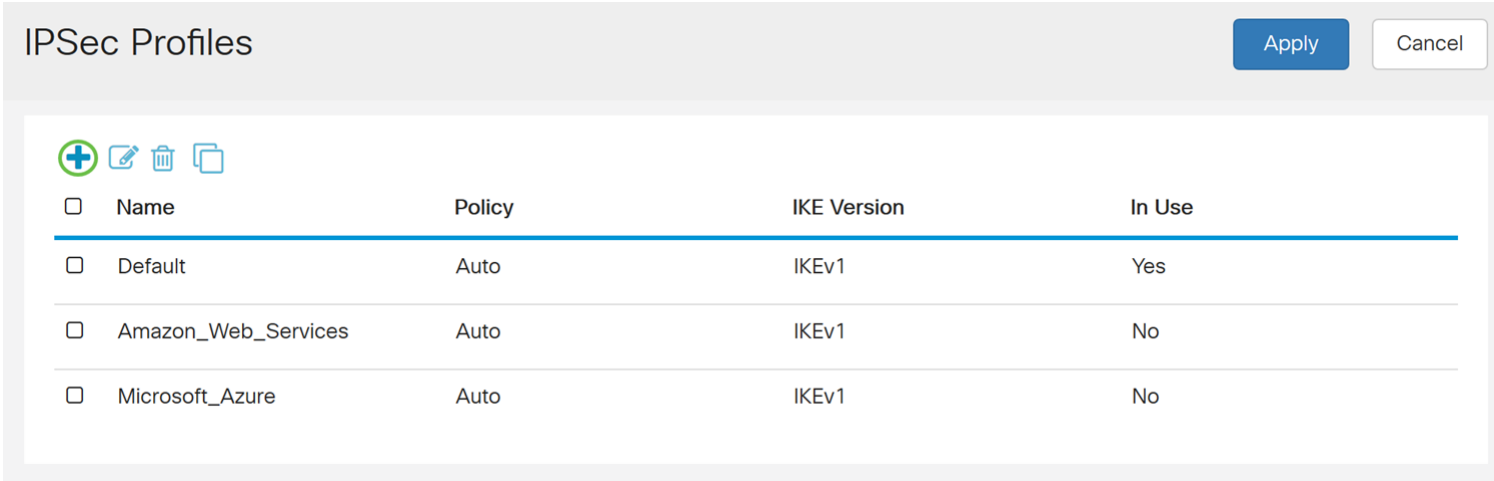
Configuration du profil IPsec

Étape 1. Accédez à **VPN > IPSec VPN > IPSec Profiles**.

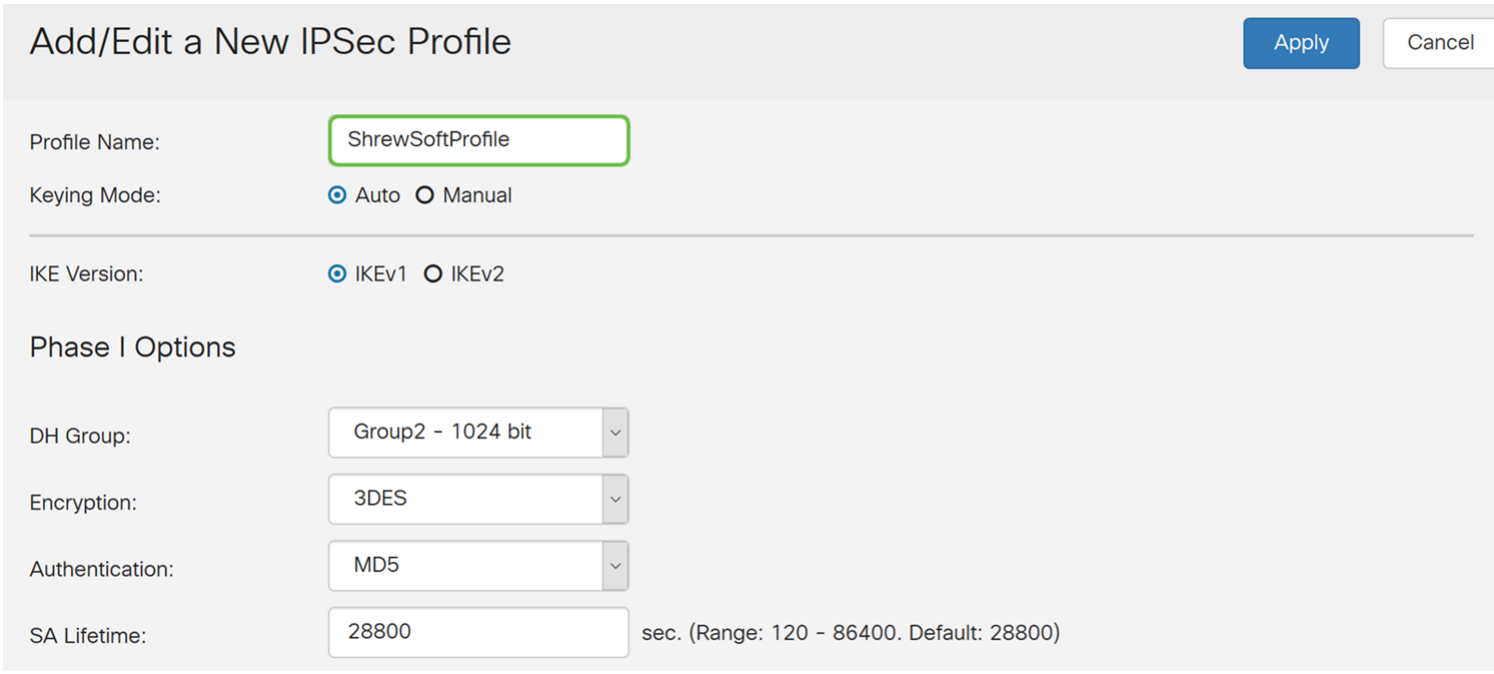


Note: Pour plus d'informations sur la configuration des profils IPsec, cliquez sur le lien pour consulter l'article : [Configuration des profils IPsec (mode de sélection automatique) sur les routeurs RV160 et RV260]

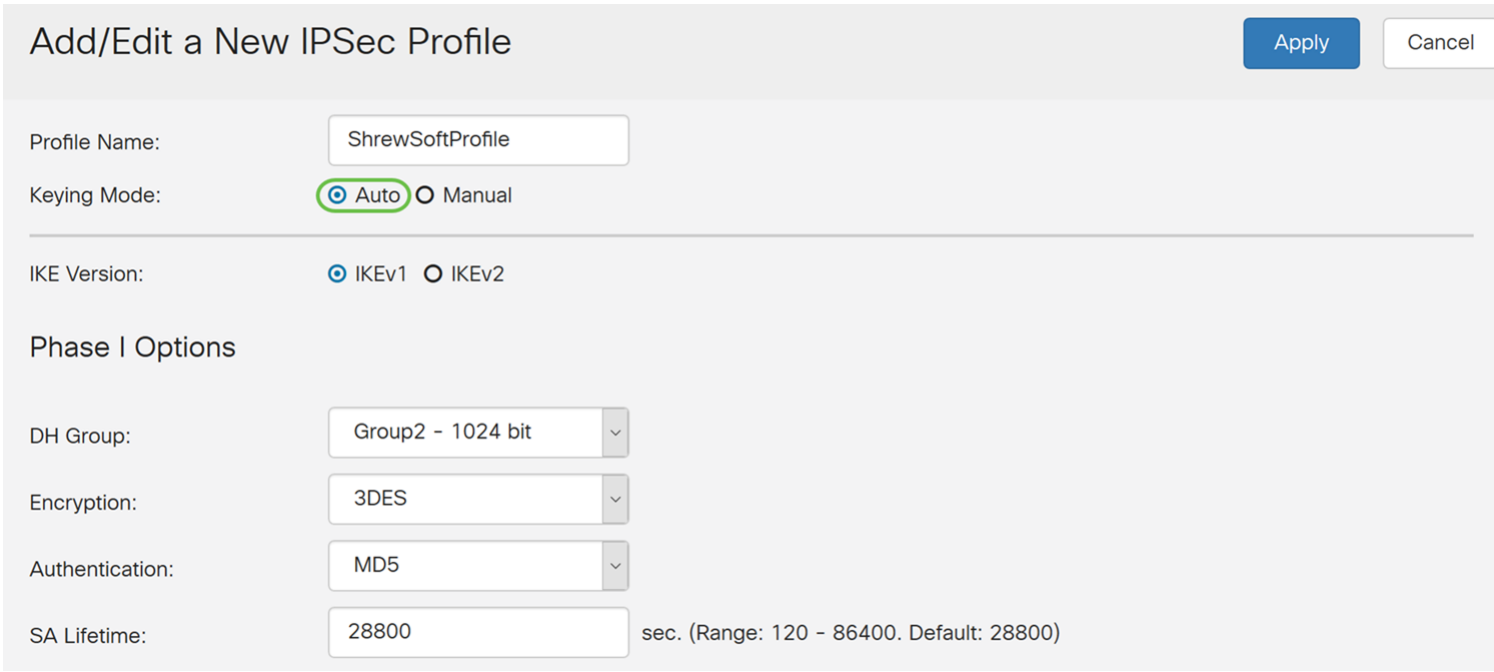
Étape 2. Cliquez sur l'icône **plus** pour ajouter un nouveau profil IPsec.



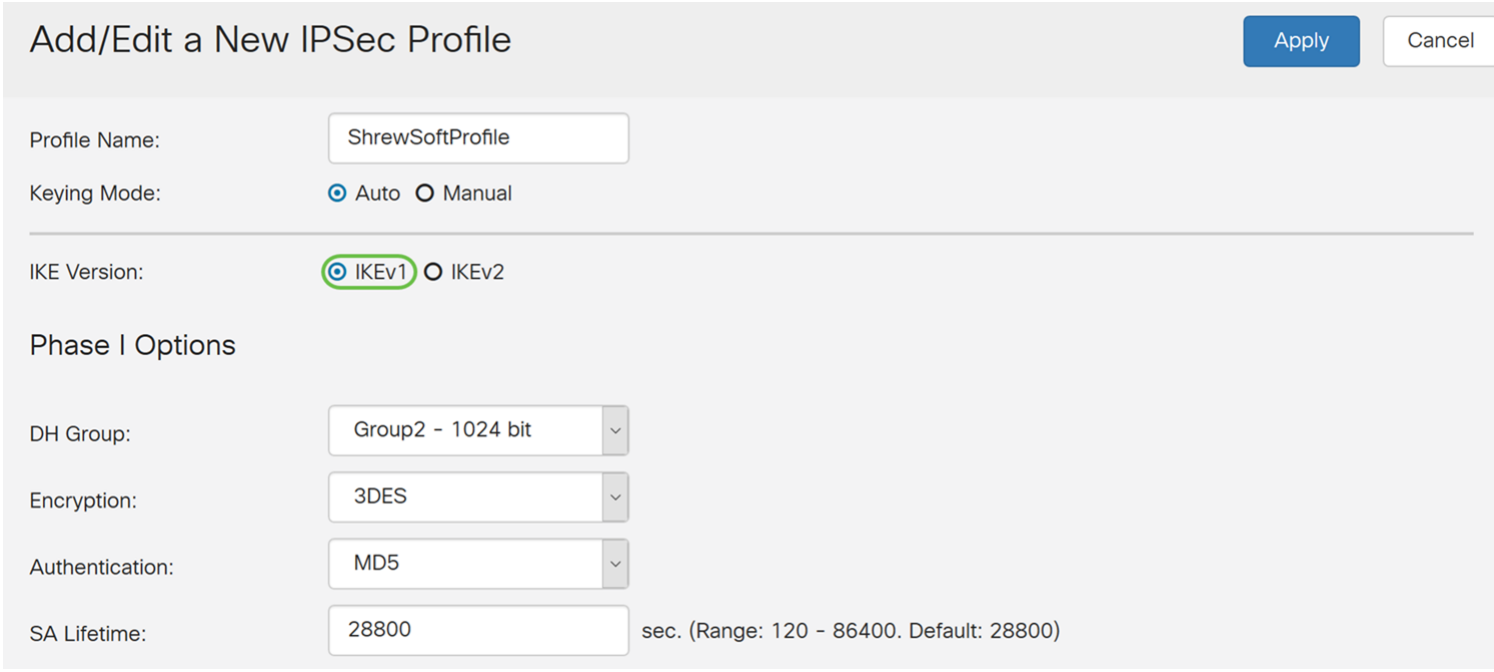
Étape 3. Entrez un nom pour le profil dans le champ *Nom du profil*. Nous allons entrer **ShrewSoftProfile** comme nom de profil.



Étape 4. Sélectionnez **Auto** pour *le mode Clé*.



Étape 5. Sélectionnez **IKEv1** ou **IKEv2** comme *version IKE*. Dans cet exemple, IKEv1 a été sélectionné.



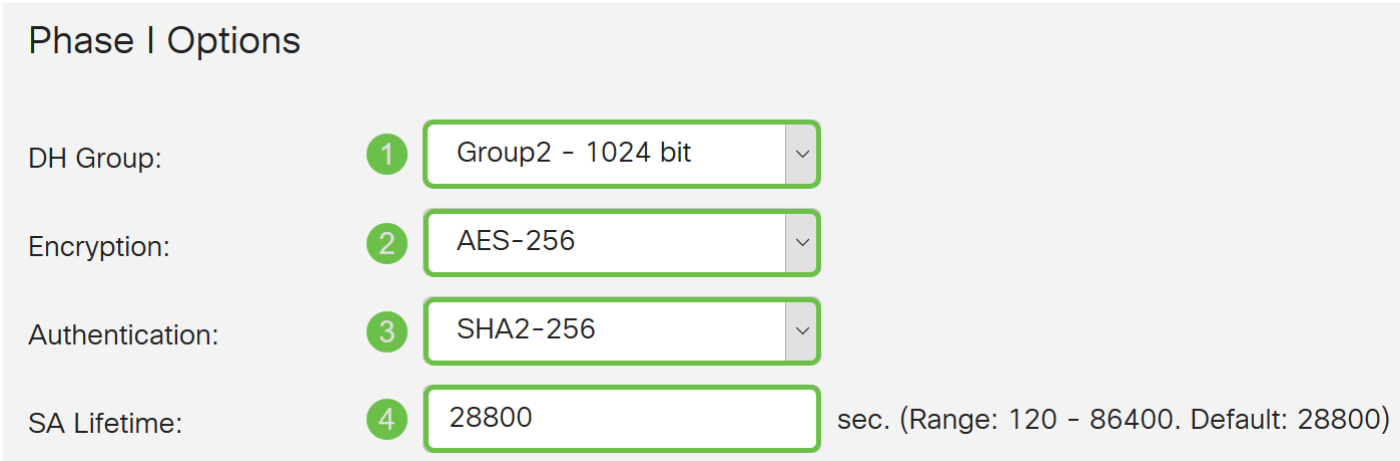
Étape 6. Dans la section *Options de phase I*, voici ce que nous avons configuré pour cet article.

Groupe DH : **Groupe2 - 1 024 bits**

Chiffrement : **AES-256**

Authentification: **SHA2-256**

Durée de vie du SA : **28800**



Étape 7. Dans le cadre des *options de phase II*, voici ce que nous avons configuré pour cet article.

Sélection de protocole : **ESP**

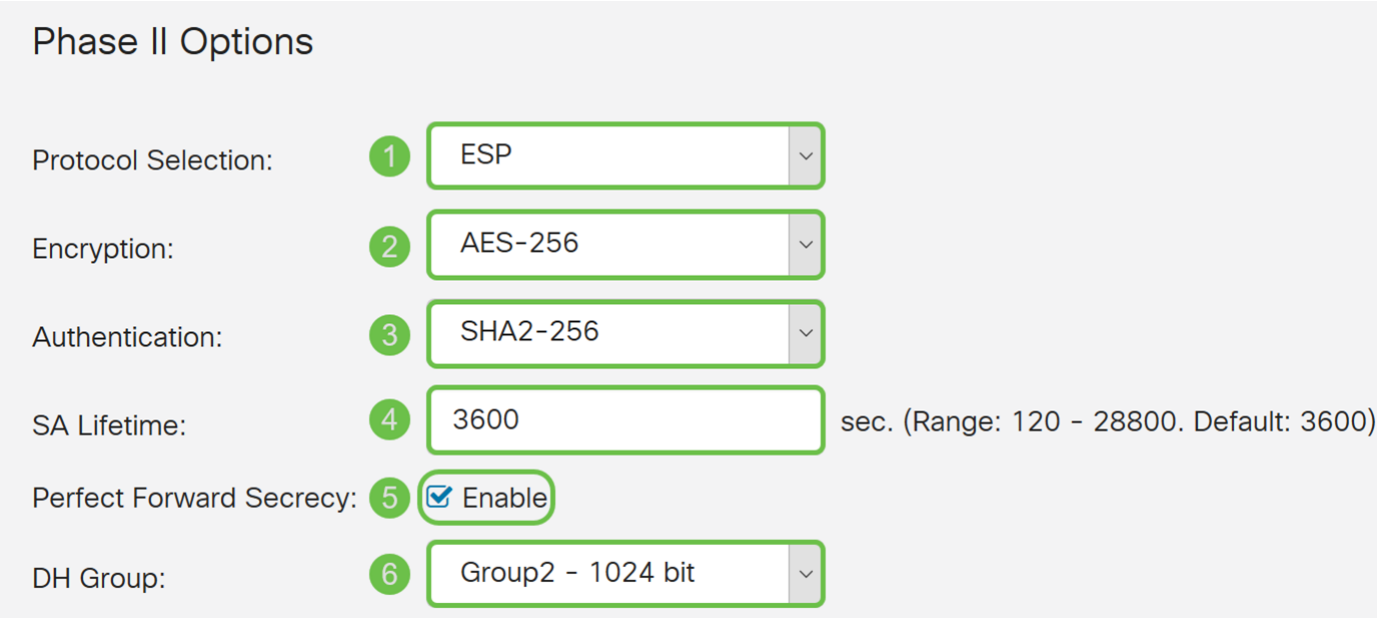
Chiffrement : **AES-256**

Authentification: **SHA2-256**

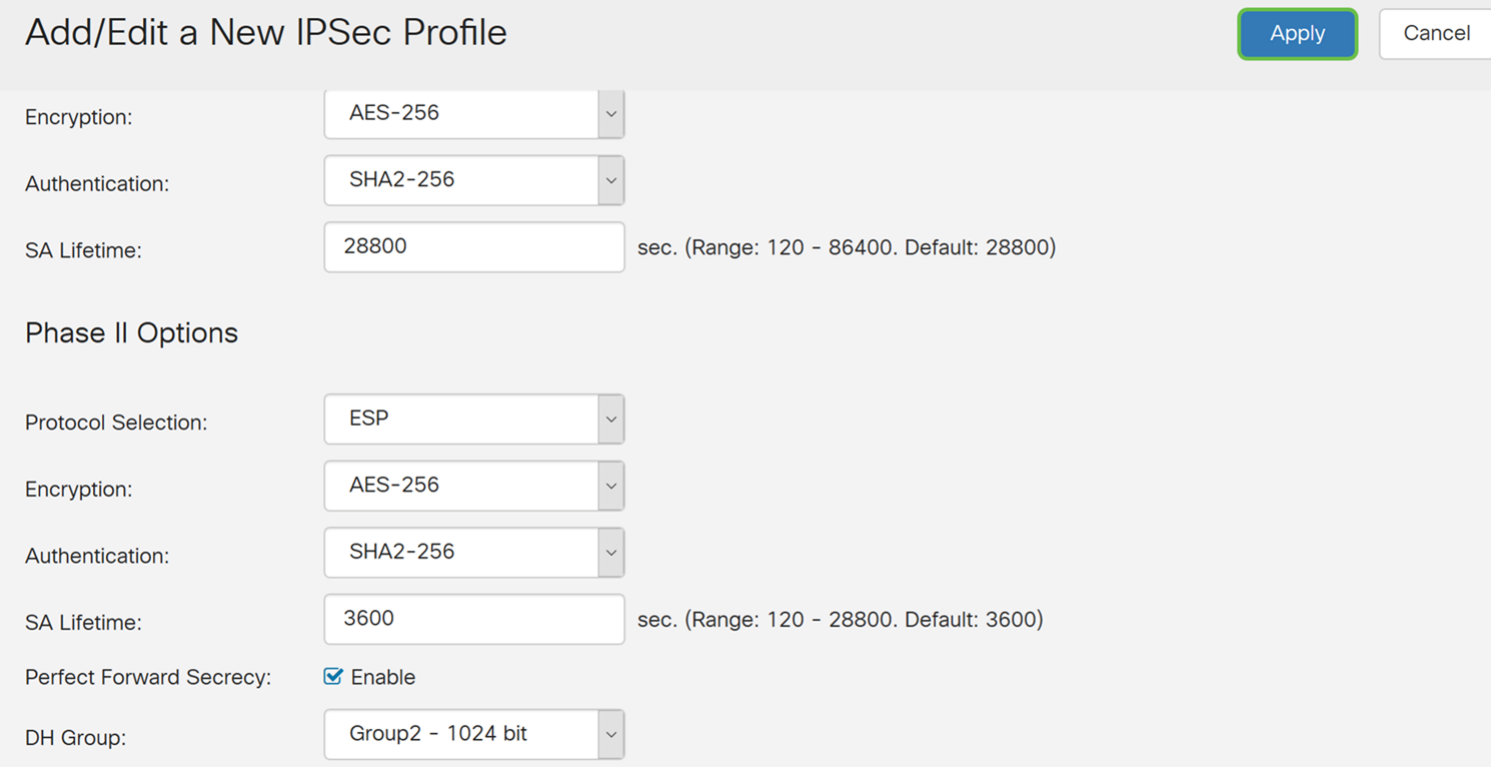
Durée de vie du SA : **3600**

Secret de transmission parfait : **Activée**

Groupe DH : **Groupe2 - 1 024 bits**

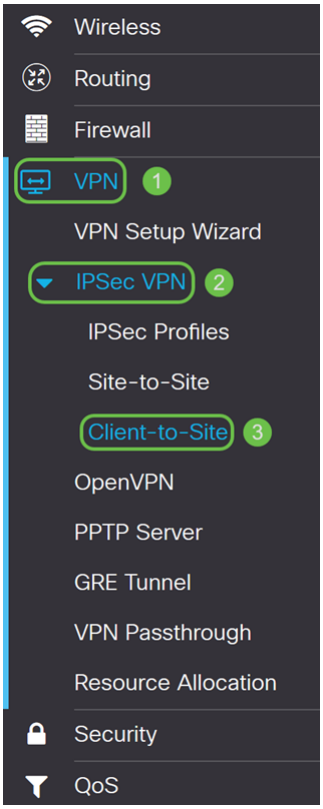


Étape 8. Cliquez sur **Apply** pour créer votre nouveau profil IPsec.

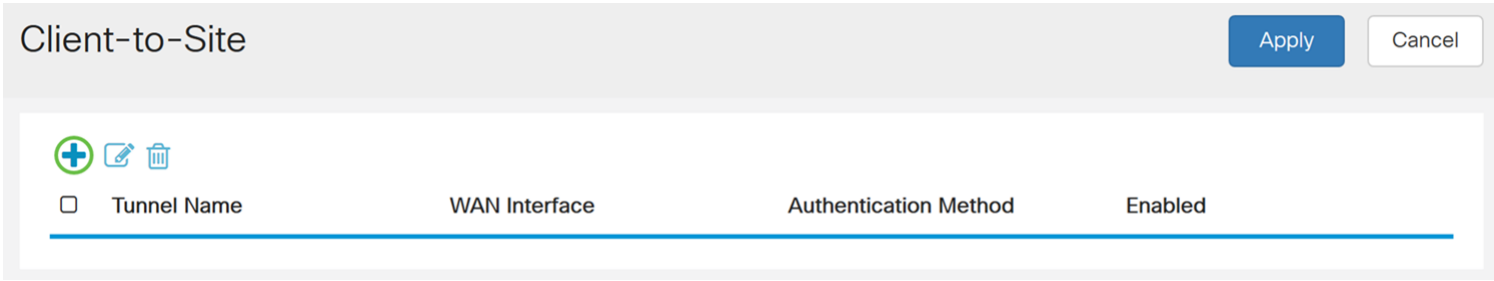


Configuration de client à site

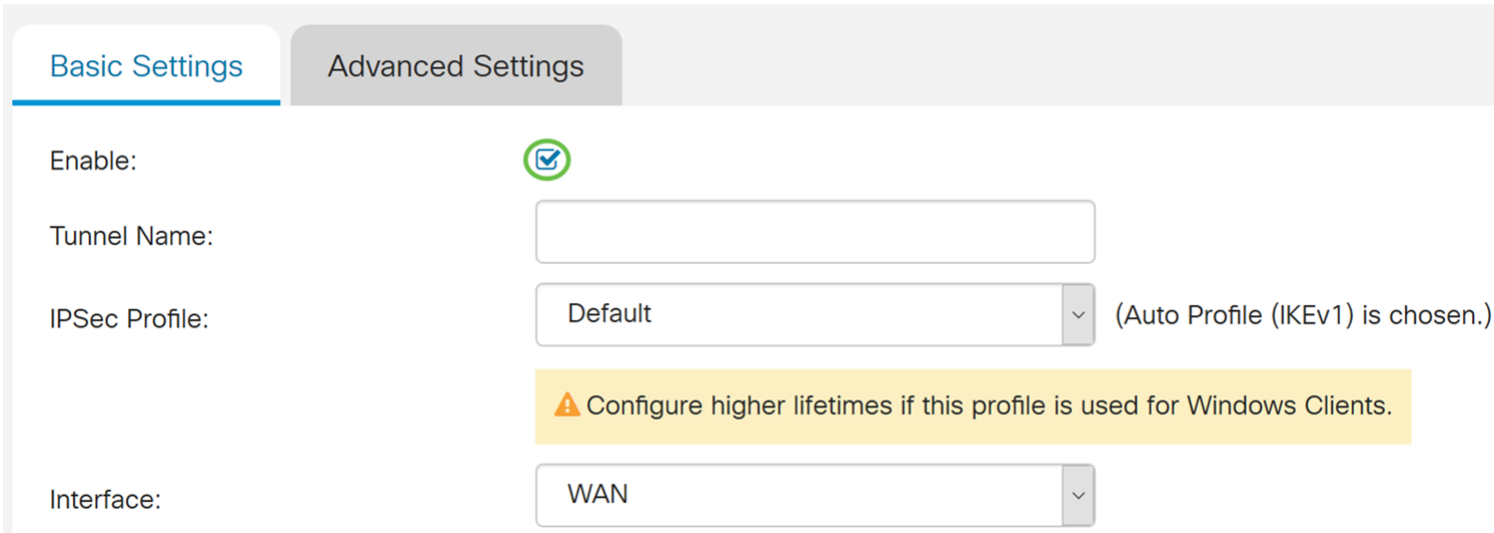
Étape 1. Accédez à **VPN > IPSec VPN > Client-to-Site**.



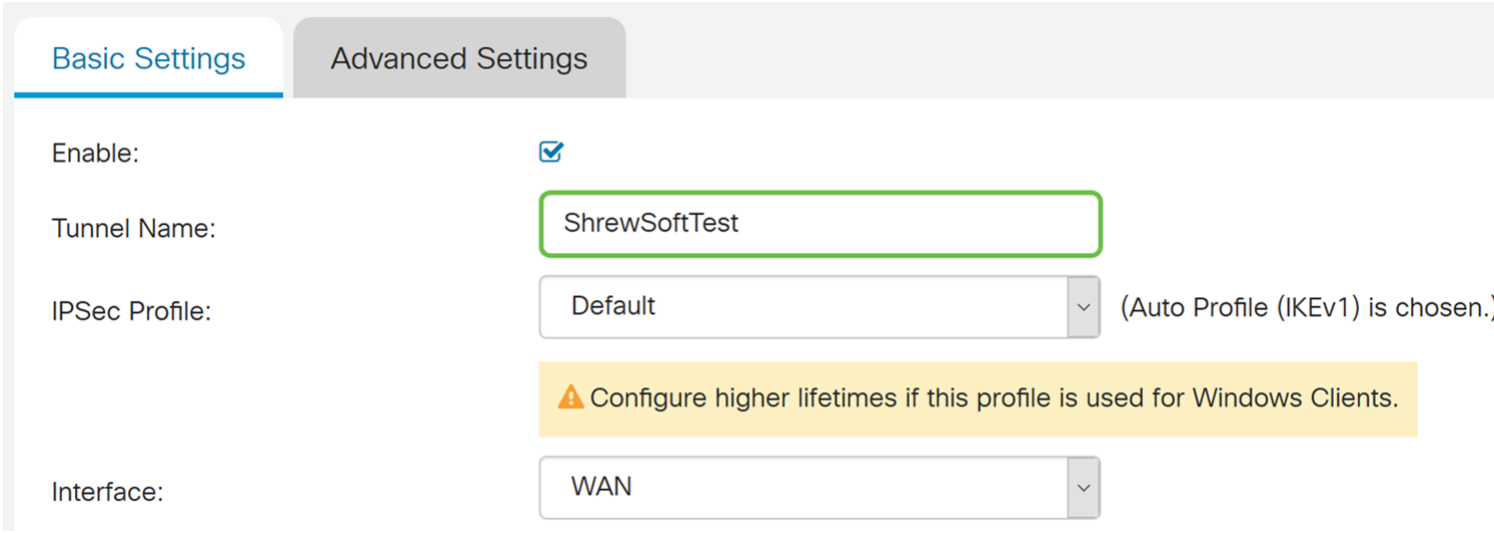
Étape 2. Cliquez sur l'icône **plus** pour ajouter un nouveau tunnel.



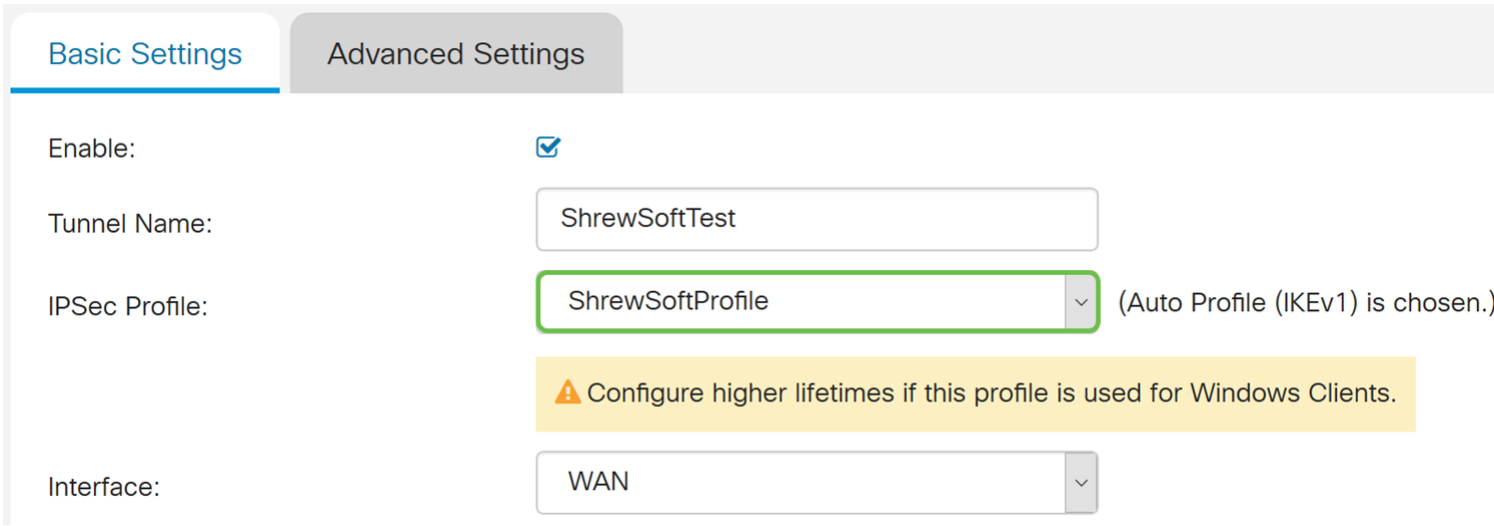
Étape 3. Cochez la case **Activer** pour activer le tunnel.



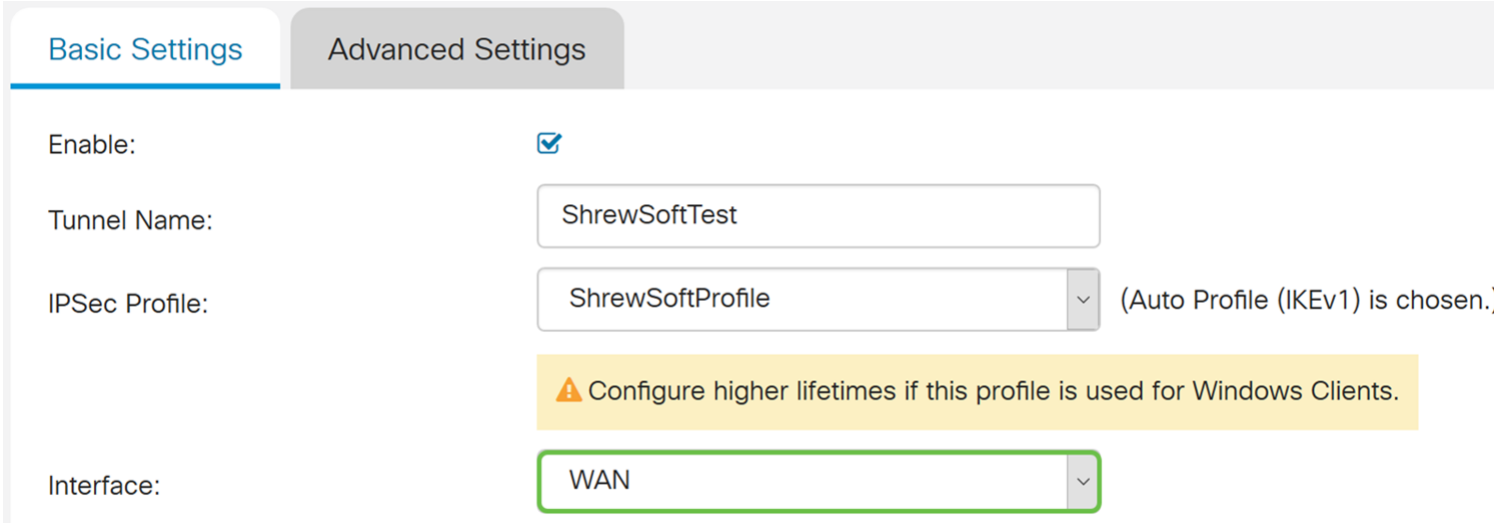
Étape 4. Entrez un nom pour le tunnel dans le champ *Nom du tunnel*.



Étape 5. Dans la liste déroulante *Profil IPSec*, sélectionnez un profil à utiliser. Nous allons sélectionner ShrewSoftProfile qui a été créé dans la section précédente : [Configuration du profil IPsec].



Étape 6. Dans la liste déroulante *Interface*, sélectionnez l'interface à utiliser. Nous utiliserons le **WAN** comme interface pour connecter le tunnel.

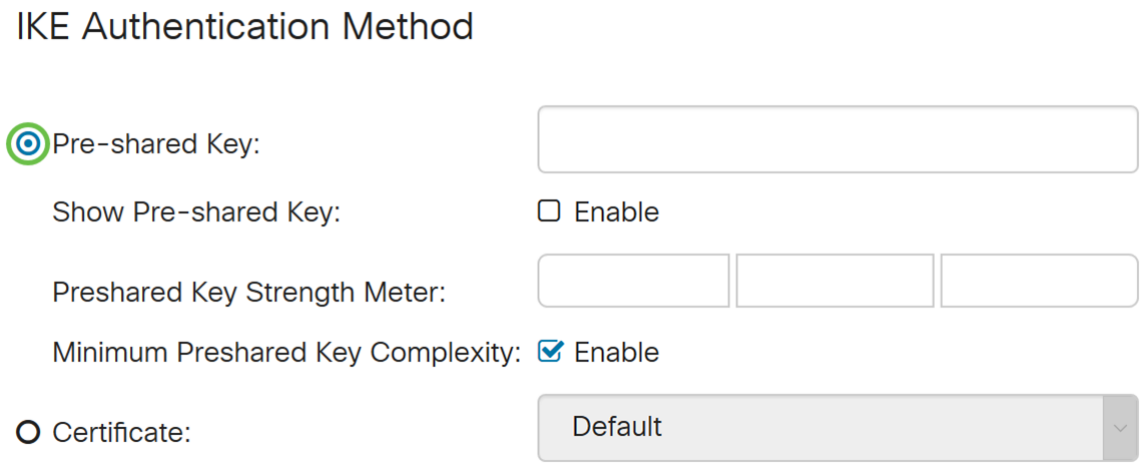


Étape 7. Dans la section *Méthode d'authentification IKE*, sélectionnez *Clé prépartagée* ou *Certificat*. Nous utiliserons la **clé pré-partagée** comme méthode d'authentification IKE.

Note: Les homologues IKE s'authentifient mutuellement en calculant et en envoyant un hachage de données comportant la clé pré-partagée. Si l'homologue récepteur est capable

de créer le même hachage indépendamment à l'aide de sa clé pré-partagée, il sait que les deux homologues doivent partager le même secret, authentifiant ainsi l'autre homologue. Les clés pré-partagées ne s'adaptent pas correctement, car chaque homologue IPsec doit être configuré avec les clés pré-partagées de tous les autres homologues avec lesquels il établit une session.

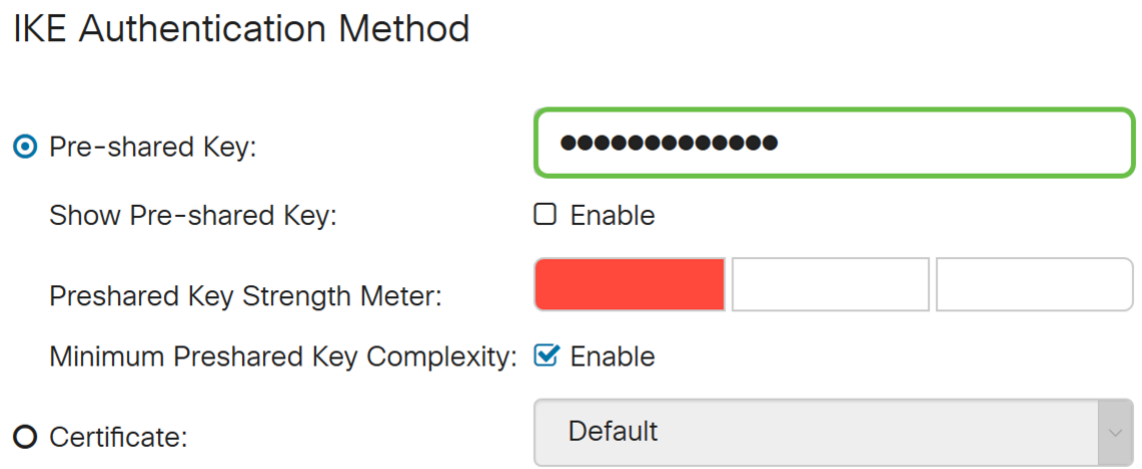
Le certificat utilise un certificat numérique qui contient des informations telles que le nom, ou l'adresse IP, le numéro de série, la date d'expiration du certificat et une copie de la clé publique du titulaire du certificat.



Étape 8. Saisissez la clé prépartagée que vous souhaitez utiliser pour l'authentification. La clé pré-partagée peut être ce que vous voulez qu'elle soit. La clé pré-partagée configurée sur le client VPN logiciel Shrew devra être identique à celle que vous avez configurée ici.

Dans cet exemple, nous allons utiliser **CiscoTest123 !** comme clé pré-partagée.

Note: La clé pré-partagée entrée ici est un exemple. Il est recommandé d'entrer une clé pré-partagée plus complexe.



Étape 9. Sélectionnez l'*identificateur local* dans la liste déroulante. Les options suivantes sont définies comme suit :

- Local WAN IP : cette option utilise l'adresse IP de l'interface WAN (Wide Area Network) de la passerelle VPN.

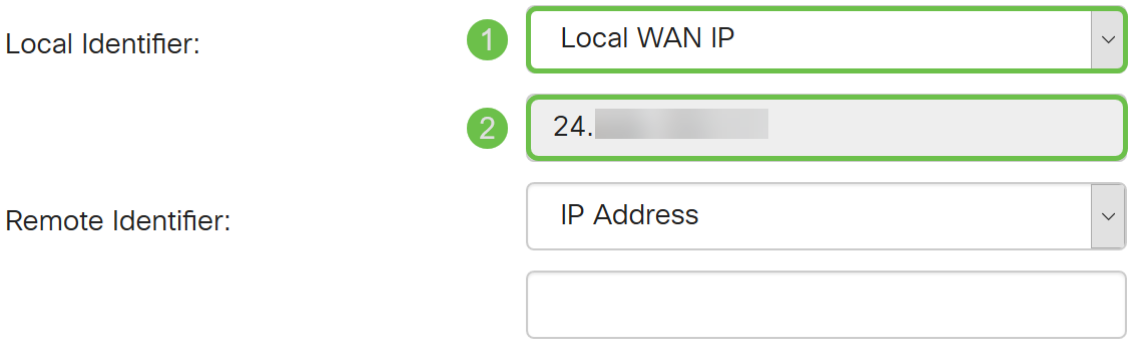
- IP Address : cette option vous permet de saisir manuellement une adresse IP pour la connexion VPN. Vous devez saisir l'adresse IP WAN du routeur sur le site (bureau).

• FQDN : cette option utilise le nom de domaine complet (FQDN) du routeur lors de l'établissement de la connexion VPN.

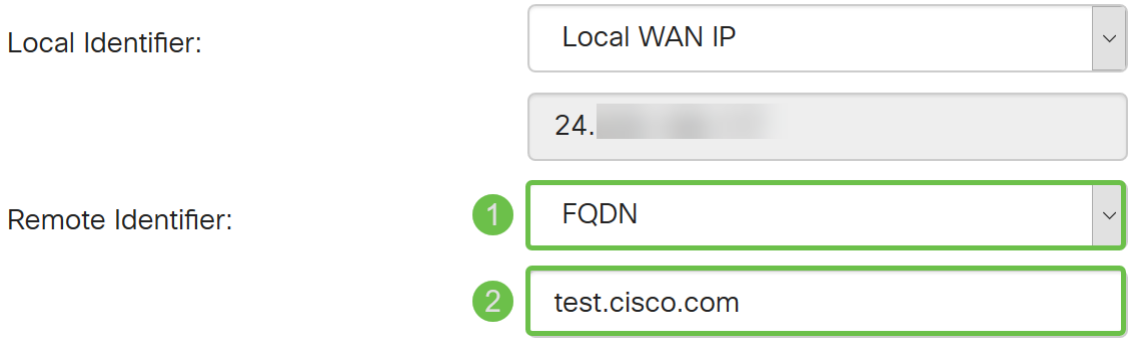
• User FQDN - Cette option vous permet d'utiliser un nom de domaine complet pour un utilisateur spécifique sur Internet.

Dans cet exemple, nous allons sélectionner **Local WAN IP** comme notre identificateur local.

Note: L'adresse IP WAN locale du routeur est automatiquement renseignée.

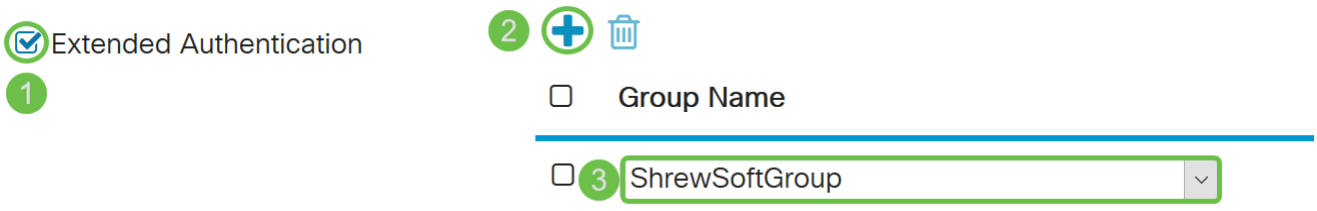


Étape 10. Dans la liste déroulante *Remote Identifier*, sélectionnez **IP Address**, **FQDN** ou **User FQDN**. Saisissez ensuite la réponse appropriée à partir de ce que vous avez sélectionné. Dans cet exemple, nous allons sélectionner **FQDN** et entrer **test.cisco.com**.



Étape 11. Cochez la case **Extended Authentication** pour l'activer. Cela fournira un niveau d'authentification supplémentaire qui exigera des utilisateurs distants qu'ils saisissent leurs informations d'identification avant d'obtenir l'accès au VPN.

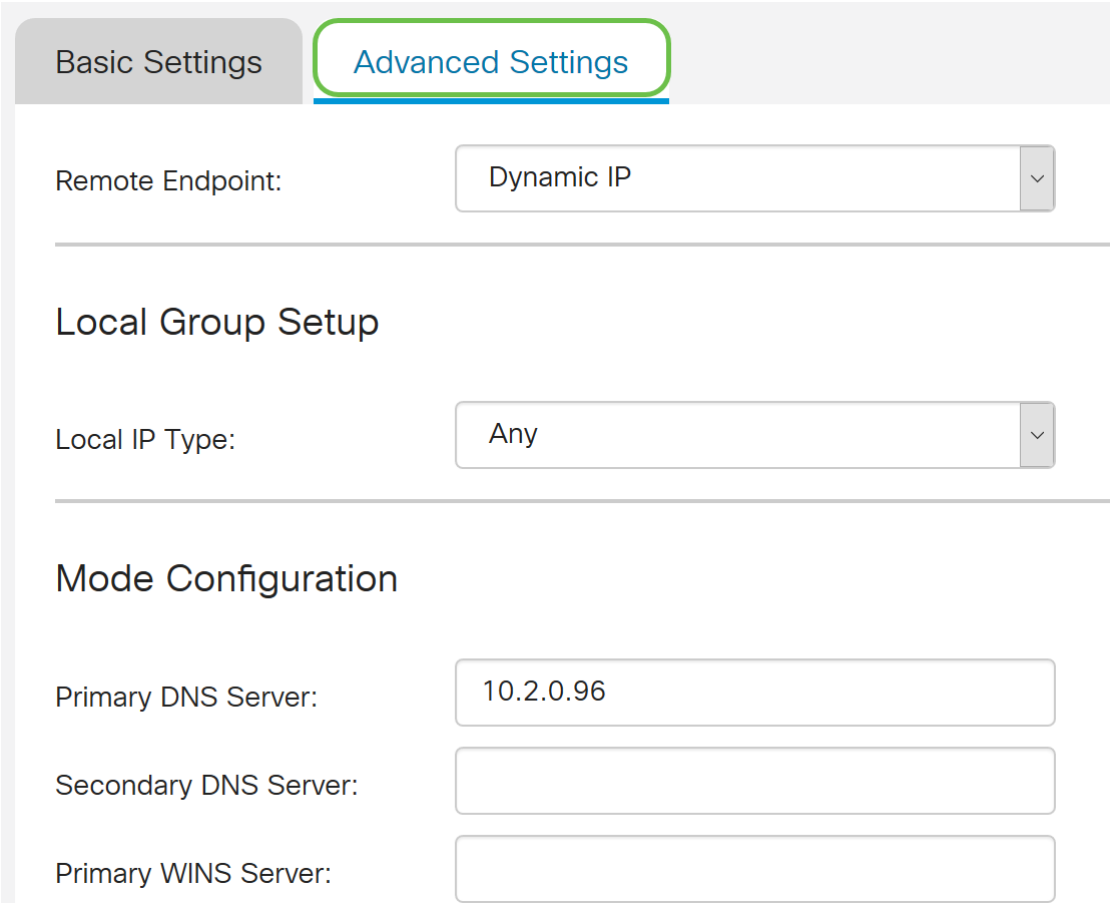
Si vous avez activé l'*authentification étendue*, cliquez sur l'icône **plus** pour ajouter un groupe d'utilisateurs. Sélectionnez le groupe dans la liste déroulante à utiliser pour l'authentification étendue. Nous sélectionnerons **ShrewSoftGroup** comme groupe.



Étape 12. Dans la *plage du pool pour le réseau local du client*, saisissez la plage d'adresses IP qui peuvent être attribuées à un client VPN dans le champ *Start IP* and *End IP*. Il doit s'agir d'un pool d'adresses qui ne se chevauchent pas avec les adresses de site.

Nous allons entrer **10.2.1.1** comme *IP de début* et **10.2.1.254** comme *IP de fin*.

Étape 13. (Facultatif) Cliquez sur l'onglet **Paramètres avancés**.



Étape 14. (Facultatif) Vous pouvez spécifier ici l'adresse IP du point de terminaison distant. Dans ce guide, nous allons utiliser **Dynamic IP**, car l'adresse IP du client final n'est pas fixe.

Vous pouvez également spécifier quelles ressources internes seront disponibles dans la *configuration du groupe local*.

Si vous sélectionnez **Any**, toutes les ressources internes seront disponibles.

Vous pouvez également choisir d'utiliser les serveurs DNS et WINS internes. Pour cela, vous devez les spécifier sous *Configuration du mode*.

Vous avez également la possibilité d'utiliser le tunnel complet ou partagé et le DNS partagé.

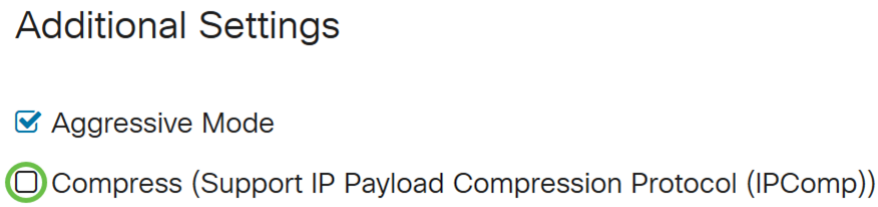
Faites défiler jusqu'à *Paramètres supplémentaires*. Cochez la case **Mode agressif** pour activer le mode agressif. Le mode agressif est lorsque la négociation pour l'association de sécurité IKE est compressée en trois paquets avec toutes les données de l'association de sécurité requises pour être transmises par l'initiateur. La négociation est plus rapide, mais ils ont une vulnérabilité d'identités d'échange en texte clair.

Note: Informations supplémentaires pour le mode principal et le mode agressif, reportez-vous à la section : Mode Principal Vs Mode Agressif

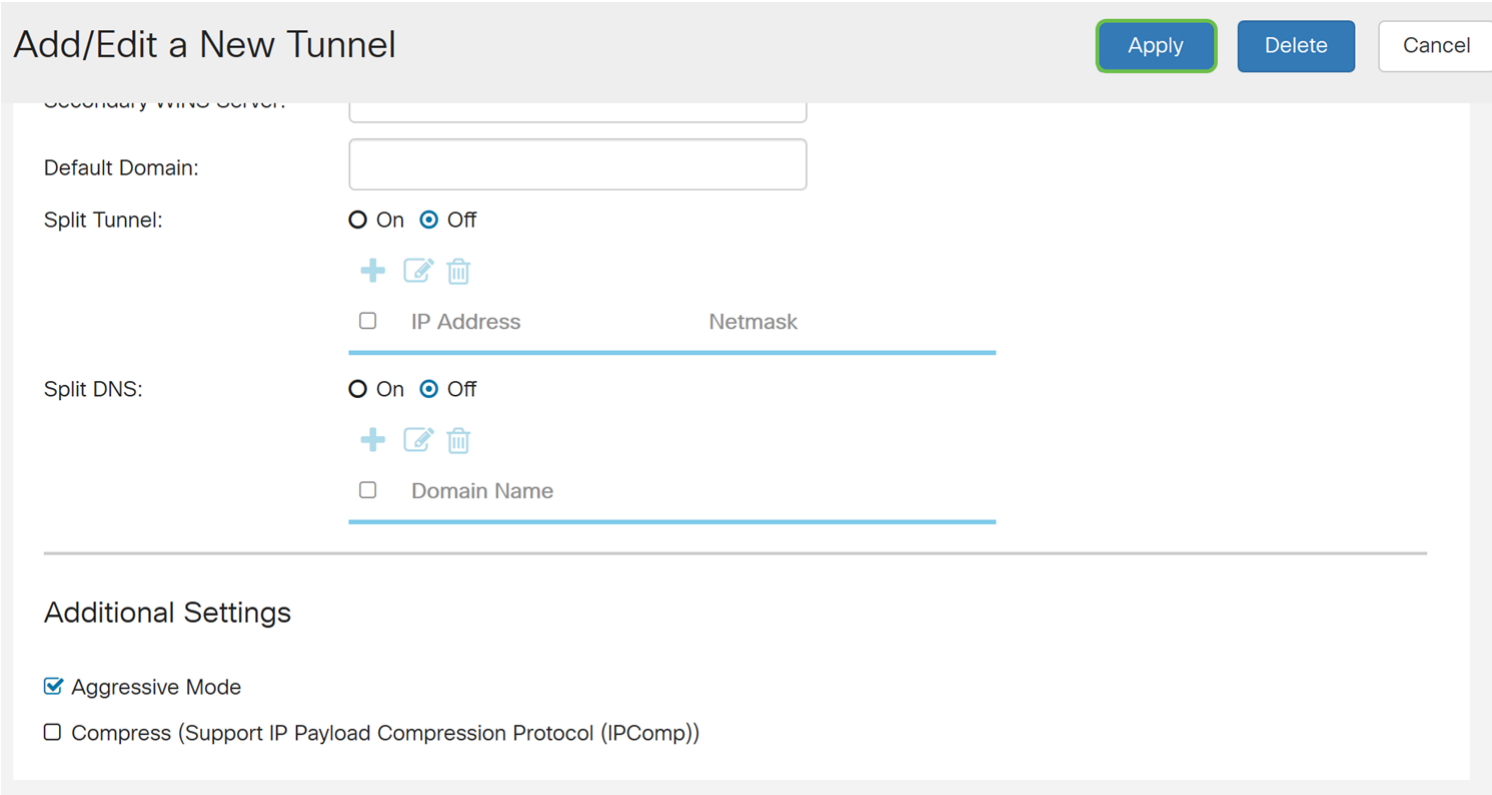
Dans cet exemple, nous allons activer le **mode agressif**.

Étape 15. (Facultatif) Cochez la case **Compress (Support IP Payload Compression Protocol (IPComp))** pour permettre au routeur de proposer la compression lorsqu'il démarre une connexion. Il s'agit d'un protocole qui réduit la taille des datagrammes IP. Si le répondeur rejette cette proposition, le routeur n'implémente pas la compression. Lorsque le routeur est le répondeur, il accepte la compression, même si la compression n'est pas activée.

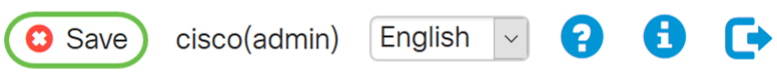
Nous laisserons *Compress* sans contrôle.



Étape 16. Cliquez sur **Apply** pour ajouter le nouveau tunnel.

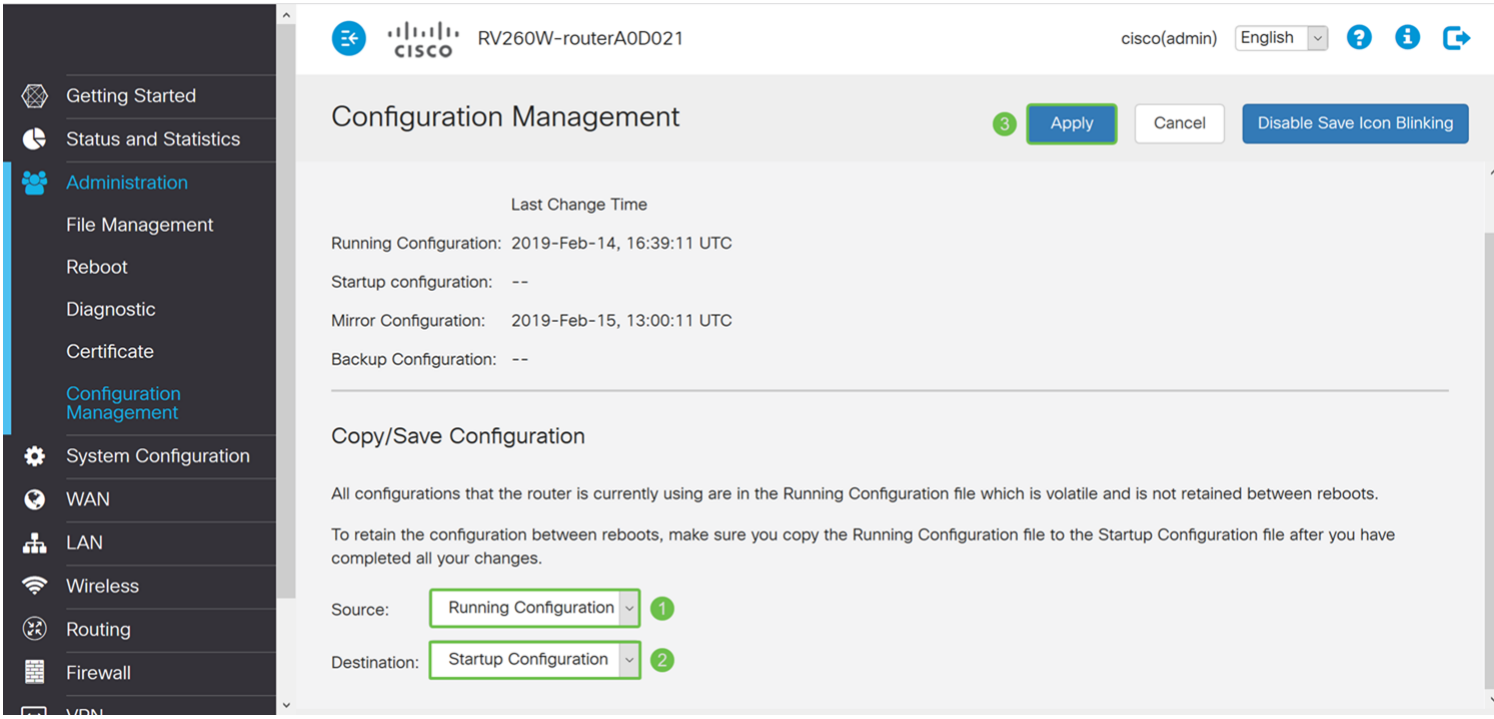


Étape 17. Cliquez sur l'icône **Enregistrer** clignotante en haut de la page de configuration Web.



Étape 18. La page *Configuration Management* s'affiche. Dans la section Copier/enregistrer la configuration, assurez-vous que le champ *Source* a **Configuration en cours** et que le

champ *Destination a* **Configuration de démarrage**. Appuyez ensuite sur **Apply**. Toutes les configurations actuellement utilisées par le routeur se trouvent dans le fichier de configuration en cours, qui est volatile et qui n'est pas conservé entre les redémarrages. La copie du fichier de configuration en cours dans le fichier de configuration initiale conserve votre configuration entre les redémarrages.

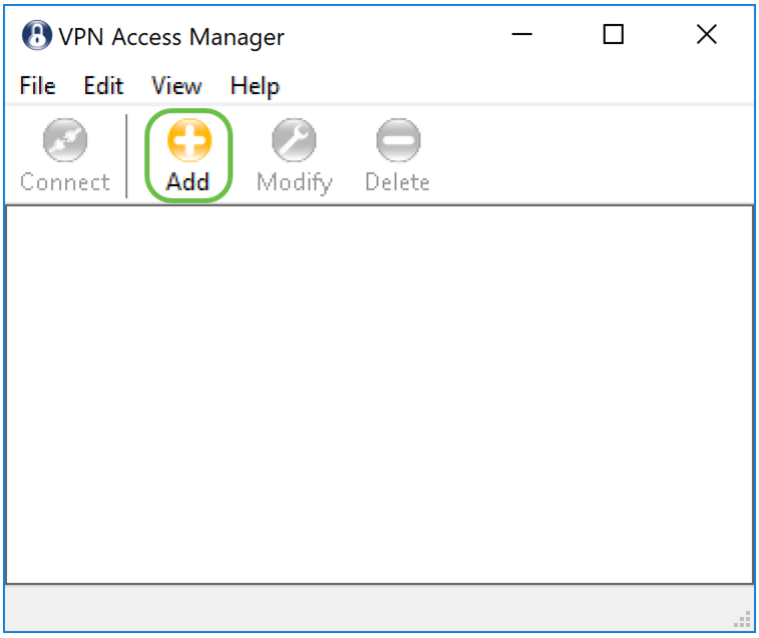


Configuration du client VPN logiciel Shrew

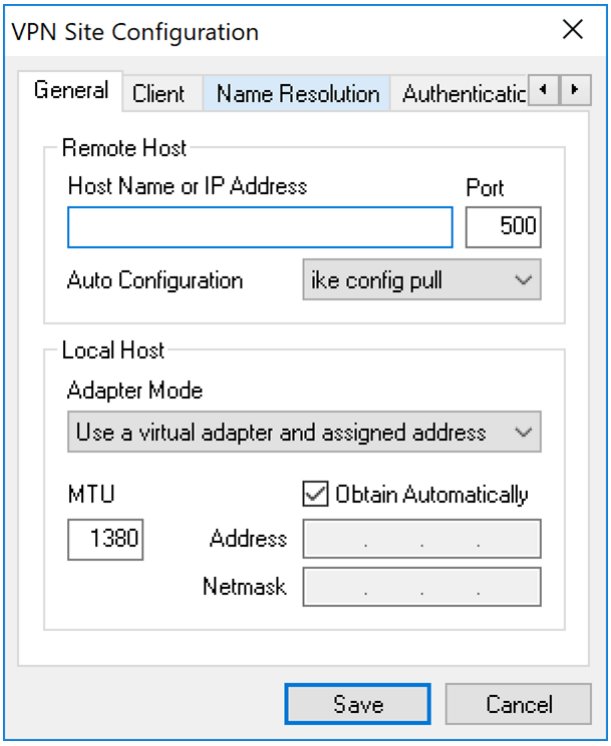
Si vous n'avez pas téléchargé le client VPN Shrew Soft, n'hésitez pas à télécharger le client en cliquant sur ce lien : Shrew Soft VPN Client pour Windows. Nous utiliserons l'édition standard. Si vous avez déjà téléchargé le client VPN logiciel Shrew, n'hésitez pas à passer à la première étape.

Client VPN logiciel Shrew : Onglet Général

Étape 1. Ouvrez Shrew VPN Access Manager et cliquez sur **Add** pour ajouter un nouveau profil.

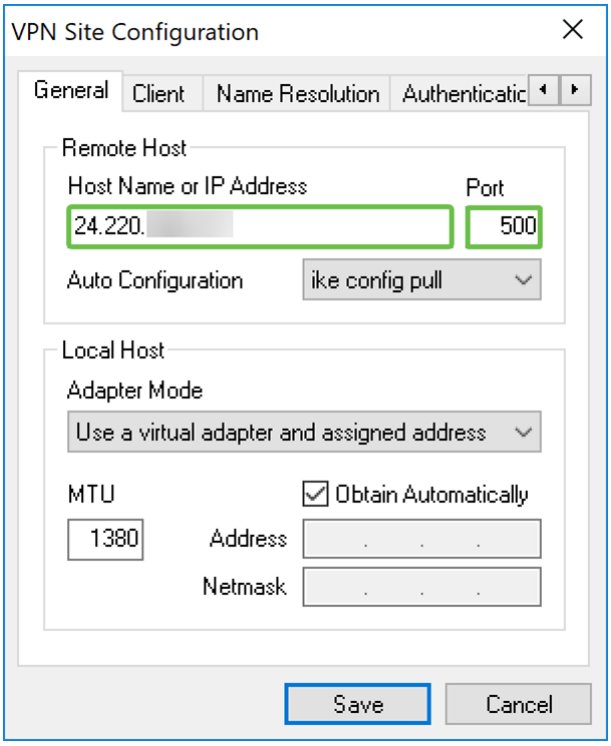


La fenêtre *Configuration du site VPN* apparaît.



Étape 2. Dans la section *Hôte distant* sous l'onglet *Général*, saisissez le nom d'hôte public ou l'adresse IP du réseau auquel vous essayez de vous connecter. Dans cet exemple, nous allons entrer l'adresse IP WAN du routeur RV160/RV260 sur site pour configurer la connexion.

Note: Assurez-vous que le numéro de port est défini sur la valeur par défaut 500. Pour que le VPN fonctionne, le tunnel utilise le port UDP 500 qui doit être configuré pour permettre le transfert du trafic ISAKMP au niveau du pare-feu.



Étape 3. Dans la liste déroulante *Configuration automatique*, sélectionnez une option. Les options disponibles sont définies comme suit :

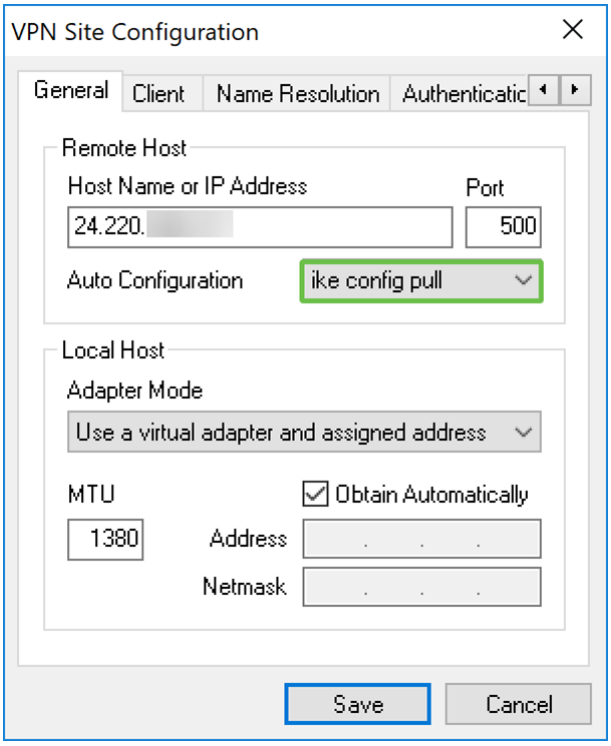
- **Désactivé** - Désactive toute configuration automatique du client

- **Ike Config Pull** - Permet de définir des requêtes à partir d'un ordinateur par le client. Avec la prise en charge de la méthode d'extraction par l'ordinateur, la requête retourne une liste des paramètres pris en charge par le client.

- **Ike Config Push** - Permet à un ordinateur d'offrir des paramètres au client tout au long du processus de configuration. Avec la prise en charge de la méthode push par l'ordinateur, la requête retourne une liste des paramètres pris en charge par le client.

- **DHCP Over IPsec** - Permet au client de demander des paramètres à l'ordinateur via DHCP sur IPsec.

Dans cet exemple, nous allons sélectionner **comme config pull**.

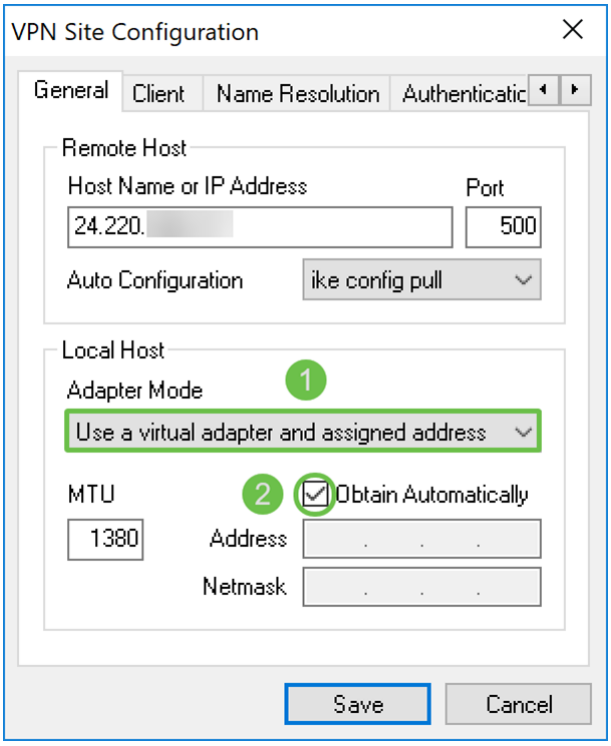


Étape 4. Dans la section *Hôte local*, sélectionnez **Utiliser un adaptateur virtuel et une adresse attribuée** dans la liste déroulante *Mode adaptateur* et cochez la case **Obtenir automatiquement**. Les options disponibles sont définies comme suit :

- **Utiliser une carte virtuelle et une adresse attribuée** - Permet au client d'utiliser une carte virtuelle avec une adresse spécifiée comme source de ses communications IPsec.

- **Utiliser une carte virtuelle et une adresse aléatoire** : permet au client d'utiliser une carte virtuelle avec une adresse aléatoire comme source de ses communications IPsec.

- **Utiliser une carte existante et une adresse actuelle** : permet au client d'utiliser uniquement sa carte physique existante avec son adresse actuelle comme source de ses communications IPsec.



Client VPN logiciel Shrew : Onglet Client

Étape 1. Cliquez sur l'onglet *Client*. Dans la liste déroulante *NAT Traversal*, sélectionnez le même paramètre que celui que vous avez configuré sur le routeur RV160/RV260 pour NAT Traversal. Les options de menu NAT (Network Address Traversal) disponibles sont définies comme suit :

- **Désactivé** - Les extensions de protocole NAT ne seront pas utilisées.

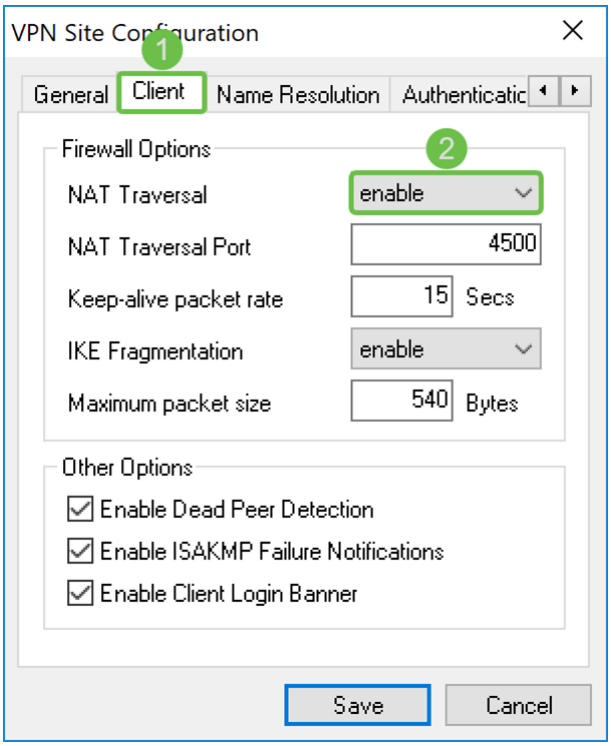
- **Activé** - Les extensions de protocole NAT ne seront utilisées que si la passerelle VPN indique la prise en charge pendant les négociations et si la NAT est détectée.

- **Force-Draft** - La version provisoire des extensions de protocole NAT sera utilisée, que la passerelle VPN indique ou non la prise en charge pendant les négociations ou que la NAT soit détectée.

- **Force-RFC** - La version RFC du protocole NATT sera utilisée, que la passerelle VPN indique ou non la prise en charge lors des négociations ou que la NAT soit détectée.

- **Force-Cisco-UDP** - Forcer l'encapsulation UDP pour les clients VPN sans NAT.

Dans ce document, nous allons sélectionner **enable** pour NAT Traversal et laisser *NAT Traversal Port* et *Keep-alive packet rate* comme valeur par défaut.



Étape 2. Dans la liste déroulante *Fragmentation IKE*, sélectionnez **Désactiver**, **Activer** ou **Force**. Les options sont définies comme suit :

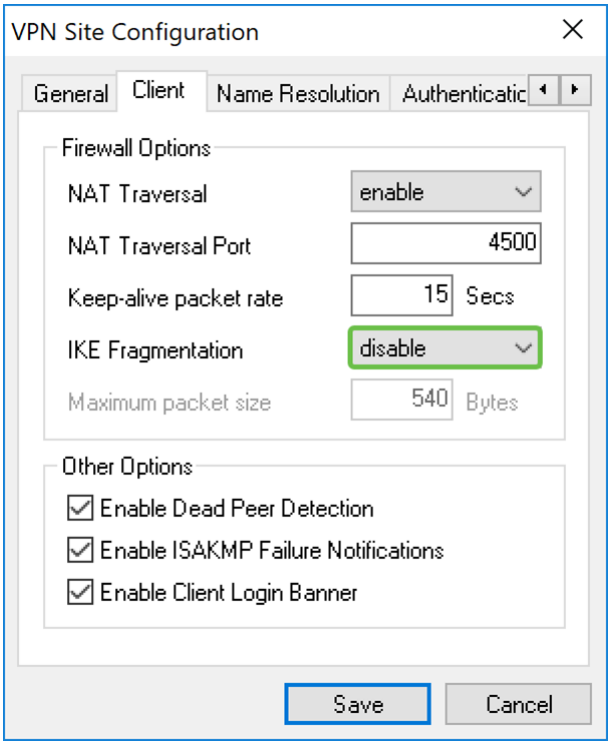
- **Disable** - L'extension du protocole de fragmentation IKE ne sera pas utilisée.

- **Enable** - L'extension du protocole de fragmentation IKE ne sera utilisée que si la passerelle VPN indique la prise en charge pendant les négociations.

- **Force** - L'extension du protocole de fragmentation IKE sera utilisée, que la passerelle VPN

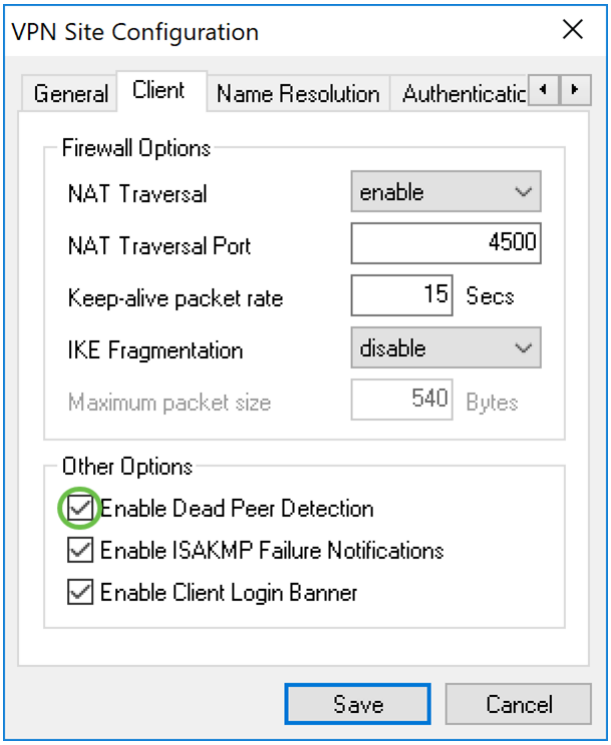
indique ou non la prise en charge lors des négociations.

Nous avons sélectionné **disable** pour *la fragmentation IKE*.



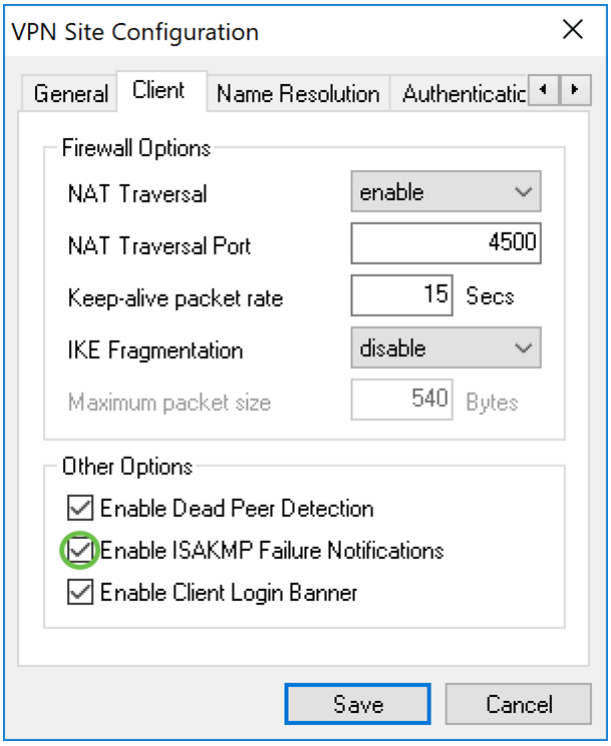
Étape 3. Cochez la case **Enable Dead Peer Detection** pour activer le protocole Dead Peer Detection. Si cette option est activée, elle ne sera utilisée que si le routeur la prend en charge. Cela permet au client et au routeur de vérifier l'état du tunnel pour détecter lorsqu'un côté n'est plus en mesure de répondre. Cette option est activée par défaut.

Dans cet exemple, nous allons laisser Dead Peer Detection cochée.



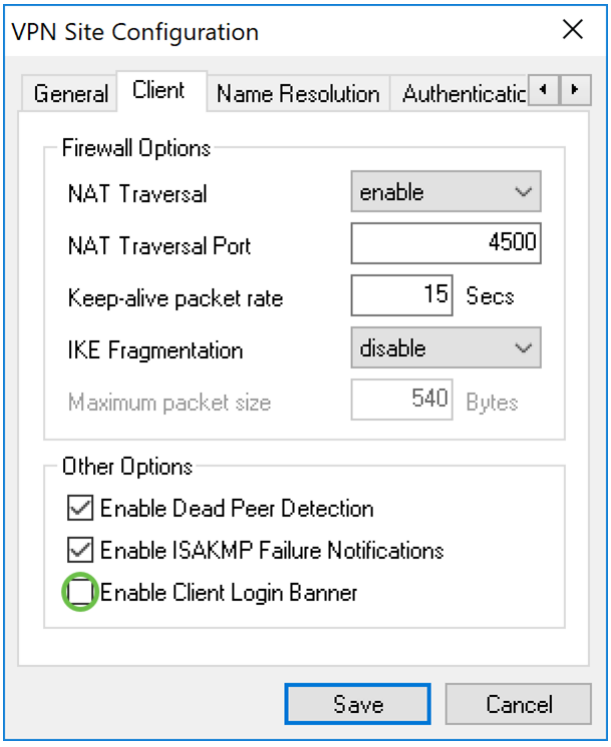
Étape 4. Cochez la case **Activer la notification d'échec ISAKMP** pour activer la notification d'échec ISAKMP à partir du démon IPsec du client VPN. Ceci est activé par défaut.

Dans cet exemple, nous allons laisser ISAKMP Failure Notification cochée.



Étape 5. Désélectionnez la **bannière Activer la connexion client** pour la désactiver. Une fois le tunnel établi avec le routeur, une bannière de connexion s'affiche. Le routeur doit prendre en charge l'échange de transactions et être configuré pour transférer une bannière de connexion au client. Cette valeur est activée par défaut.

Nous désélectionnerons la bannière de connexion du client.



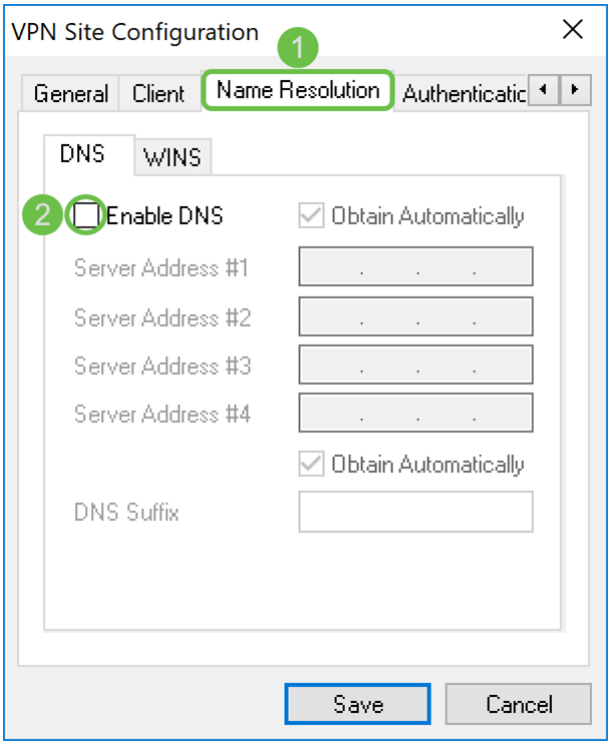
Client VPN logiciel Shrew : Onglet Résolution de nom

Étape 1. Cliquez sur l'onglet *Résolution de noms*, puis cochez la case **Activer DNS** si vous voulez activer DNS. Si des paramètres DNS spécifiques ne sont pas requis pour la configuration de votre site, décochez la case **Activer DNS**.

Si *Enable DNS* est coché et que votre passerelle distante est configurée pour prendre en

charge Configuration Exchange, la passerelle peut fournir les paramètres DNS automatiquement. Si ce n'est pas le cas, vérifiez que la case **Obtenir automatiquement** est décochée et entrez manuellement une adresse de serveur DNS valide.

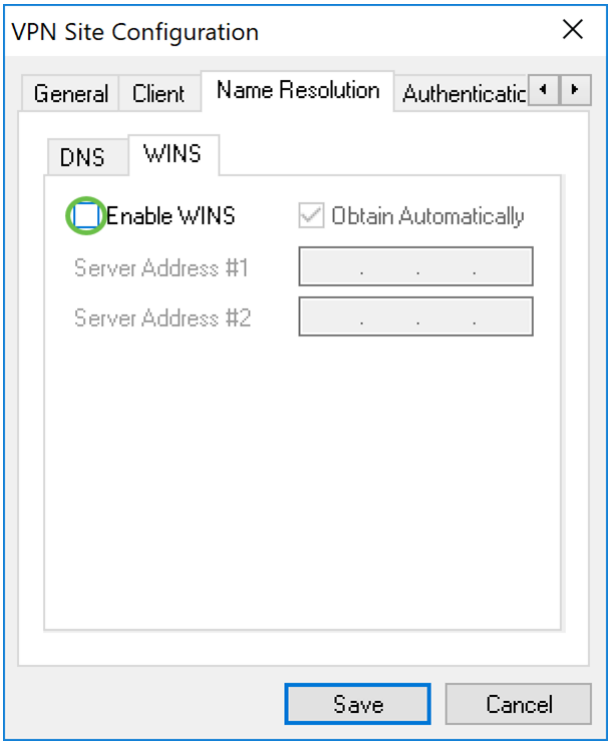
Dans cet exemple, **Enable DNS** est décoché.



Étape 2. Cochez la case **Activer WINS** si vous voulez activer le serveur de noms Internet Windows (WINS). Si votre passerelle distante est configurée pour prendre en charge Configuration Exchange, la passerelle peut fournir automatiquement les paramètres WINS. Si ce n'est pas le cas, vérifiez que la case **Obtenir automatiquement** est décochée et entrez manuellement une adresse de serveur WINS valide.

Note: En fournissant des informations de configuration WINS, un client peut résoudre les noms WINS à l'aide d'un serveur situé dans le réseau privé distant. Cela est utile lorsque vous tentez d'accéder aux ressources réseau Windows distantes à l'aide d'un nom de chemin d'accès à la Convention de noms unifiés. Le serveur WINS appartient généralement à un contrôleur de domaine Windows ou à un serveur Samba.

Dans cet exemple, **Enable WINS** est décoché.



Client VPN logiciel Shrew : Onglet Authentification

Étape 1. Cliquez sur l'onglet *Authentication*, puis sélectionnez **Mutual PSK + XAuth** dans la liste déroulante *Authentication Method*. Les options disponibles sont définies comme suit :

- **RSA hybride + XAuth** - Les informations d'identification du client ne sont pas nécessaires. Le client authentifie la passerelle. Les informations d'identification seront sous la forme de fichiers de certificat PEM ou PKCS12 ou de type de fichier de clé.

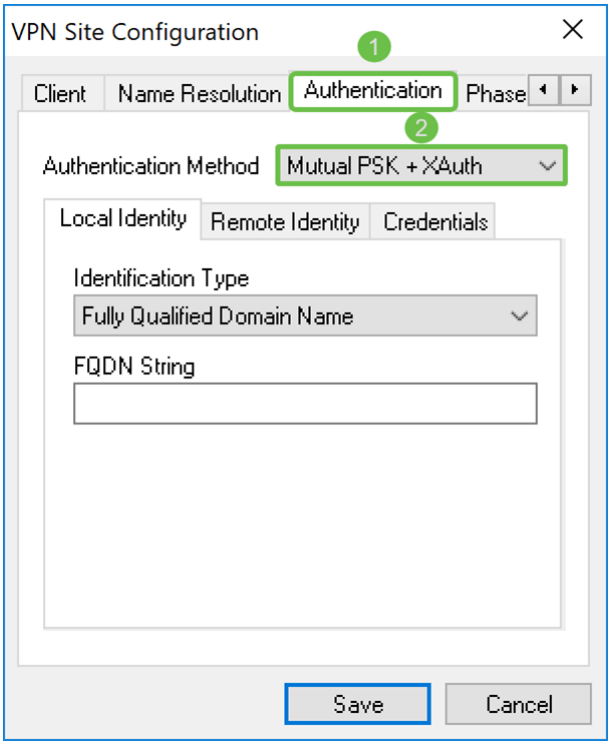
- **GRP hybride + XAuth** - Les informations d'identification du client ne sont pas nécessaires. Le client authentifie la passerelle. Les informations d'identification seront sous la forme d'un fichier de certificat PEM ou PKCS12 et d'une chaîne secrète partagée.

- **RSA mutuel + XAuth** - Le client et la passerelle ont tous deux besoin d'informations d'identification pour s'authentifier. Les informations d'identification seront sous la forme de fichiers de certificat ou de type de clé PEM ou PKCS12.

- **Mutual PSK + XAuth** - Le client et la passerelle ont tous deux besoin d'informations d'identification pour s'authentifier. Les informations d'identification seront sous la forme d'une chaîne secrète partagée.

- **RSA mutuel** - Le client et la passerelle ont tous deux besoin d'informations d'identification pour s'authentifier. Les informations d'identification seront sous la forme de fichiers de certificat ou de type de clé PEM ou PKCS12.

- **PSK mutuel** - Le client et la passerelle ont tous deux besoin d'informations d'identification pour s'authentifier. Les informations d'identification seront sous la forme d'une chaîne secrète partagée.



Étape 2. Dans l'onglet *Identité locale*, sélectionnez le type d'identification, puis saisissez la chaîne appropriée dans le champ vide. Les options suivantes sont définies comme suit :

- **Any** - Cette option n'est acceptée que dans l'onglet Remote Identity. Le client accepte tout type d'ID et toute valeur. Il convient d'utiliser cette méthode avec prudence car elle contourne une partie du processus d'identification IKE de phase 1.

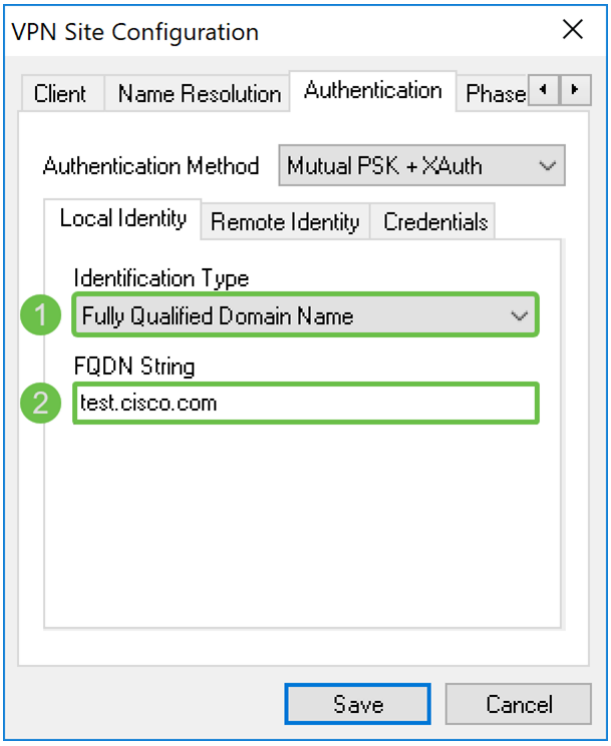
- **Fully Qualified Domain Name** - Cette option vous permet de fournir une chaîne FQDN sous la forme d'une chaîne de domaine DNS. Par exemple, " " cisco.com serait une valeur acceptable. Le client autorise uniquement la sélection de cette option si un mode d'authentification PSK est utilisé.

- **Nom de domaine complet de l'utilisateur** - Vous devez fournir une chaîne de nom de domaine complet de l'utilisateur sous la forme d'une chaîne user@domain. Par exemple, " dave@cisco.com " serait une valeur acceptable. Le client autorise uniquement la sélection de cette option si un mode d'authentification PSK est utilisé.

- **IP Address** - Lorsque l'adresse IP est sélectionnée, la case *Utiliser une adresse hôte locale détectée* est automatiquement cochée par défaut. Cela signifie que la valeur sera automatiquement déterminée. Décochez la case si vous souhaitez utiliser une adresse autre que l'adresse de l'adaptateur utilisée pour communiquer avec la passerelle du client. Ensuite, entrez une chaîne d'adresse spécifique. Le client autorise uniquement la sélection de cette option si un mode d'authentification PSK est utilisé.

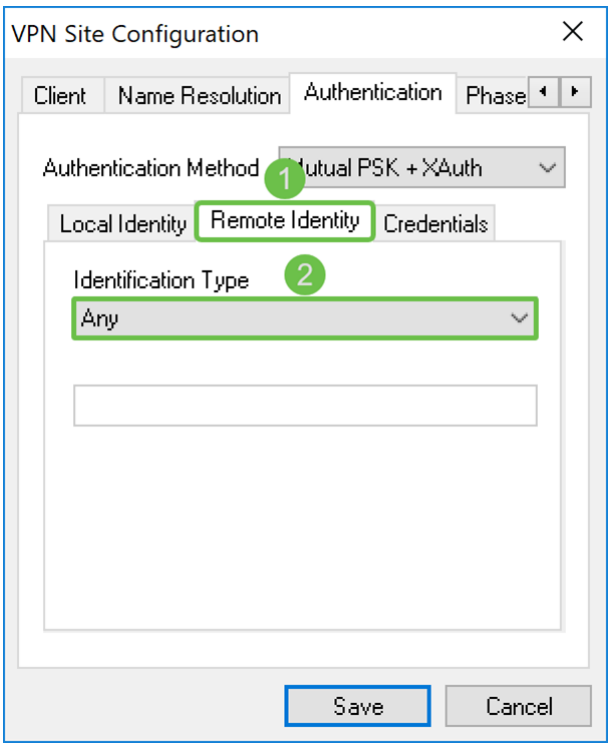
- **Key Identifier** - Lorsque cette option est sélectionnée, vous devez fournir une chaîne d'identificateur.

Dans cet exemple, nous allons sélectionner **Fully Qualified Domain Name** et entrer **test.cisco.com** dans le champ *FQDN String*.



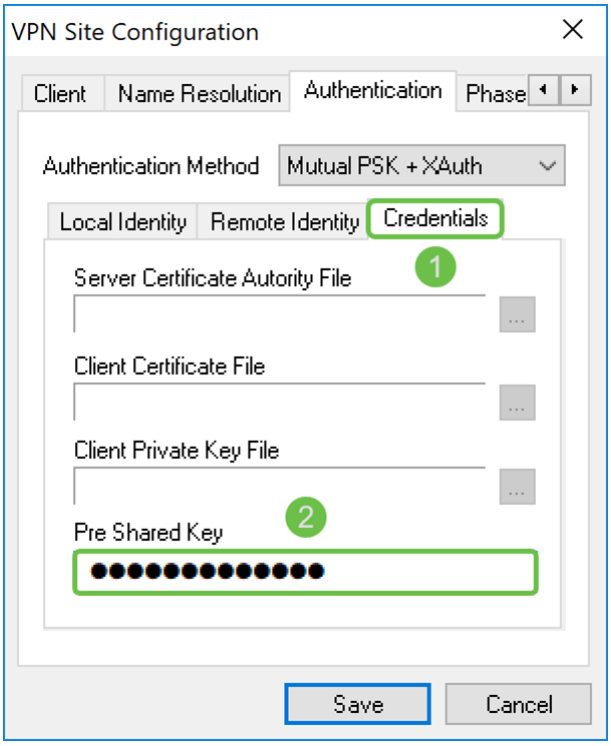
Étape 3. Cliquez sur l'onglet *Identité distante* et sélectionnez le type d'identification. Les options disponibles sont les suivantes : Tout, nom de domaine complet, nom de domaine complet de l'utilisateur, adresse IP ou identificateur de clé.

Dans ce document, nous utiliserons **Any** comme type d'identification.



Étape 4. Cliquez sur l'onglet *Informations d'identification* et saisissez la même clé prépartagée que celle que vous avez configurée sur le routeur RV160/RV260.

Nous allons entrer **CiscoTest123 !** dans le champ *Clé prépartagée*.



Client VPN logiciel Shrew : Onglet Phase 1

Étape 1. Cliquez sur l'onglet *Phase 1*. Configurez les paramètres suivants pour qu'ils aient les mêmes paramètres que ceux que vous avez configurés pour le routeur RV160/RV260.

Les paramètres de Shrew Soft doivent correspondre à la configuration RV160/RV260 que vous avez sélectionnée au cours de la phase 1. Dans ce document, les paramètres de Shrew Soft seront définis comme suit :

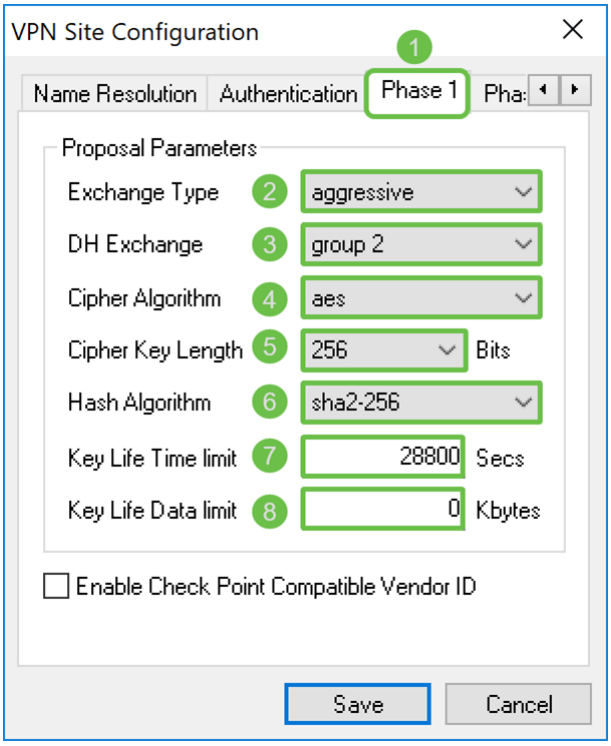
- Type d'échange : **agressif**
- échange DH : **groupe 2**
- Algorithme de chiffrement : **aes**

Longueur • de la clé de chiffrement : **256**

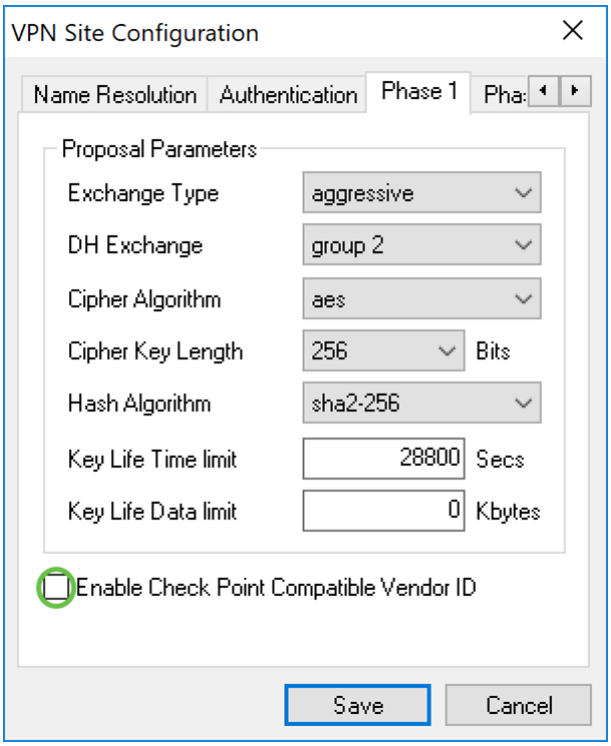
- algorithme de hachage : **sha2-256**

Durée de vie de la clé : **28800**

- Limite de données sur la durée de vie des clés : **0**



Étape 2. (Facultatif) Si votre passerelle propose un ID de fournisseur compatible Cisco lors des négociations de phase 1, cochez la case **Activer l'ID de fournisseur compatible Check Point**. Si le portail ne propose pas d'ID de fournisseur compatible Cisco ou si vous n'êtes pas sûr, ne cochez pas cette case. Nous ne cocherons pas la case.



Client VPN logiciel Shrew : Onglet Phase 2

Étape 1. Cliquez sur l'onglet *Phase 2*. Configurez les paramètres suivants pour qu'ils aient les mêmes paramètres que ceux que vous avez configurés pour le routeur RV160/RV260.

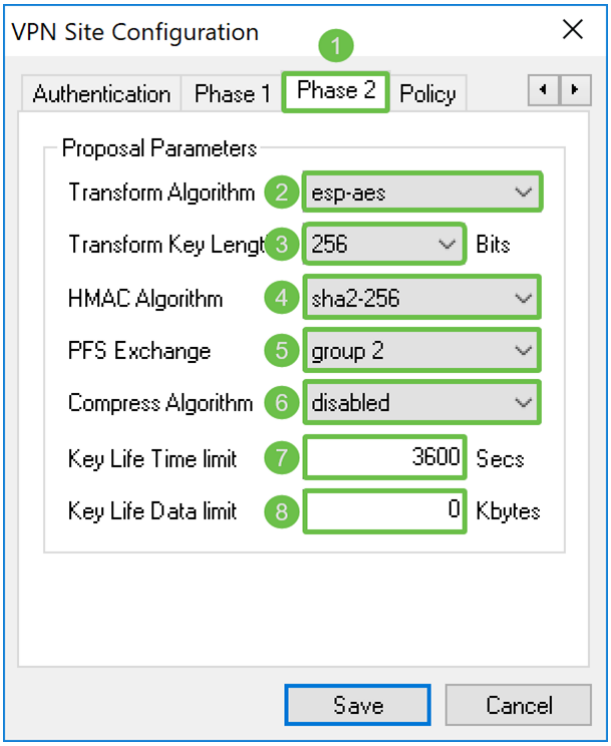
Les paramètres doivent correspondre à la configuration RV160/260 de la phase 2 comme suit :

- Algorithme de transformation : **esp-aes**

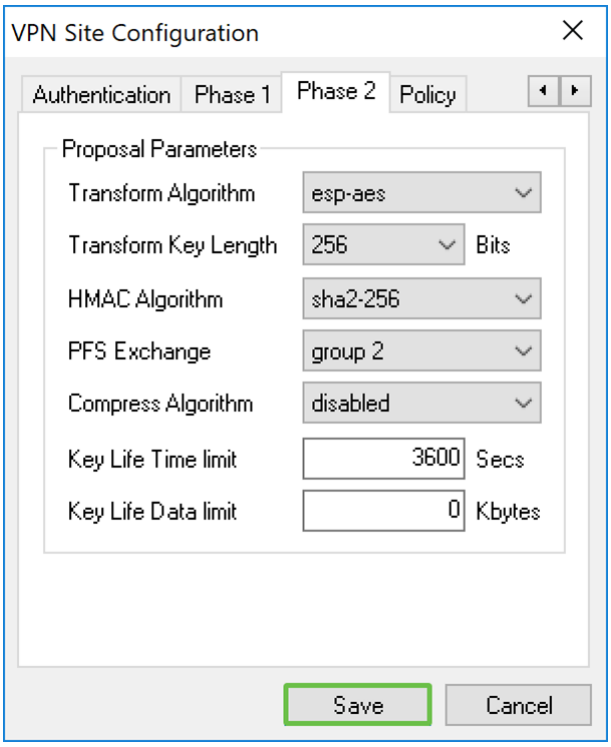
- Longueur de la clé de transformation : **256**
- Algorithme HMAC : **sha2-256**
- échange PFS : **groupe 2**
- Algorithme de compression : **désactivé**

Durée de vie de la clé : **3600**

- Limite de données sur la durée de vie des clés : **0**



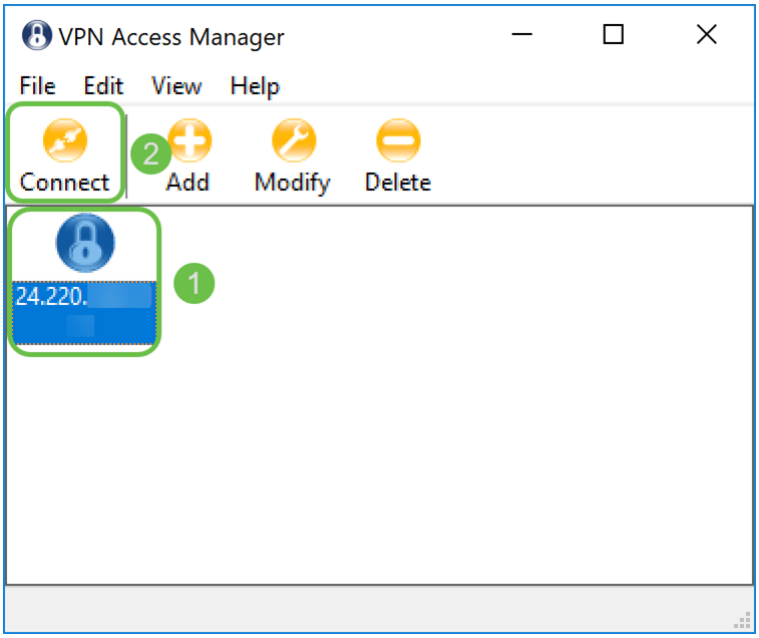
Étape 2. Appuyez sur le bouton **Enregistrer** en bas de la page pour enregistrer votre configuration.



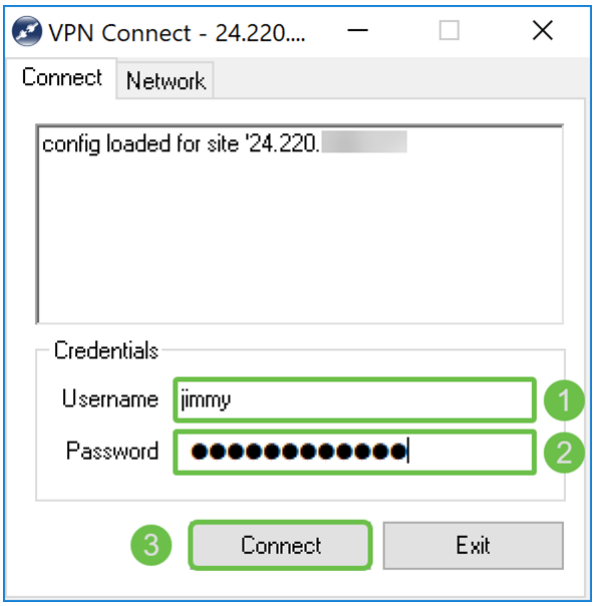
Client VPN logiciel Shrew : Connexion

Étape 1. Dans le *VPN Access Manager*, sélectionnez le profil VPN que vous venez de créer. Appuyez ensuite sur **Connect**.

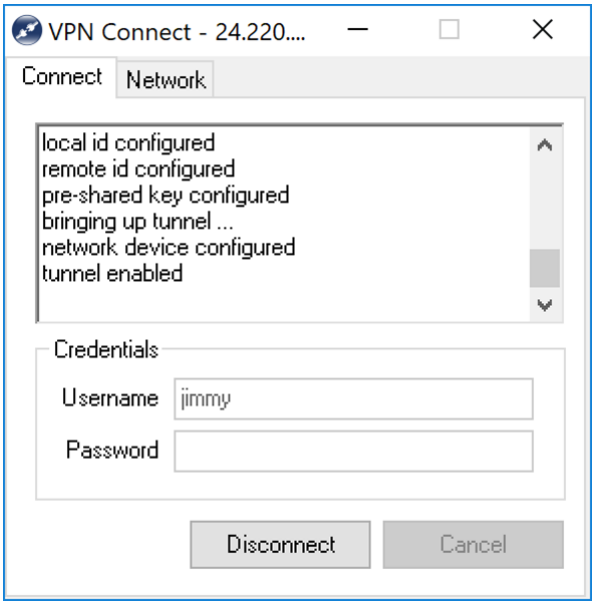
Note: Si vous souhaitez renommer le profil VPN, cliquez dessus avec le bouton droit de la souris et sélectionnez **Renommer**. Une partie de l'adresse IP du profil est floue pour protéger ce réseau.



Étape 2. Une fenêtre *VPN Connect* apparaît. Entrez le nom d'utilisateur et le mot de passe créés dans la section *Création d'un compte d'utilisateur*. Appuyez ensuite sur **Connect**.

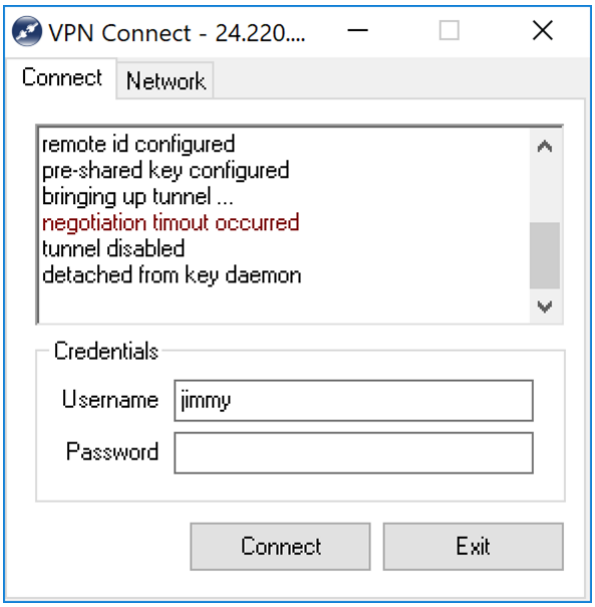


Étape 3. Après avoir appuyé sur *Connect*, les informations de configuration sont transmises au démon IKE avec une demande de communication. Différents messages de l'état de la connexion s'affichent dans la fenêtre de sortie. Si la connexion réussit, vous recevrez un message indiquant que “ périphérique réseau configuré ” et “ tunnel activé ”. Le bouton *Connexion* devient un bouton *Déconnexion*.

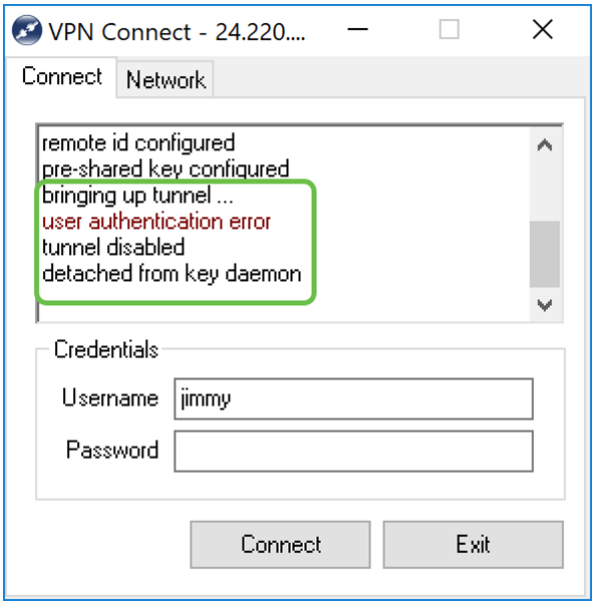


Conseils de dépannage de la connexion VPN

Si vous recevez des messages d'erreur qui disent que “ délai de négociation s'est ”, “ tunnel a désactivé ” et “ détaché du ” de démon clé. Vous pouvez vérifier deux fois votre configuration sur votre routeur et le client VPN logiciel Shrew pour vous assurer qu'ils correspondent.

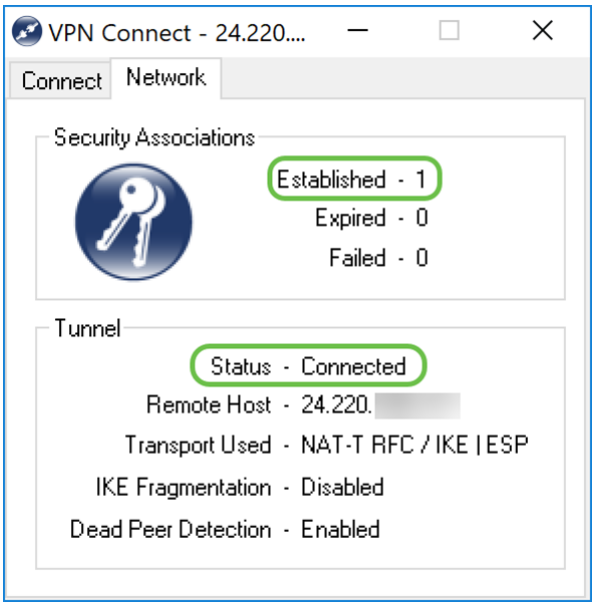


Si vous recevez un message d'erreur qui indique, “ erreur d'authentification de l'utilisateur ” alors cela signifie que vous avez entré le mauvais mot de passe pour ce nom d'utilisateur. Vérifiez deux fois les informations d'identification de l'utilisateur et assurez-vous qu'elles sont correctement configurées et entrées.

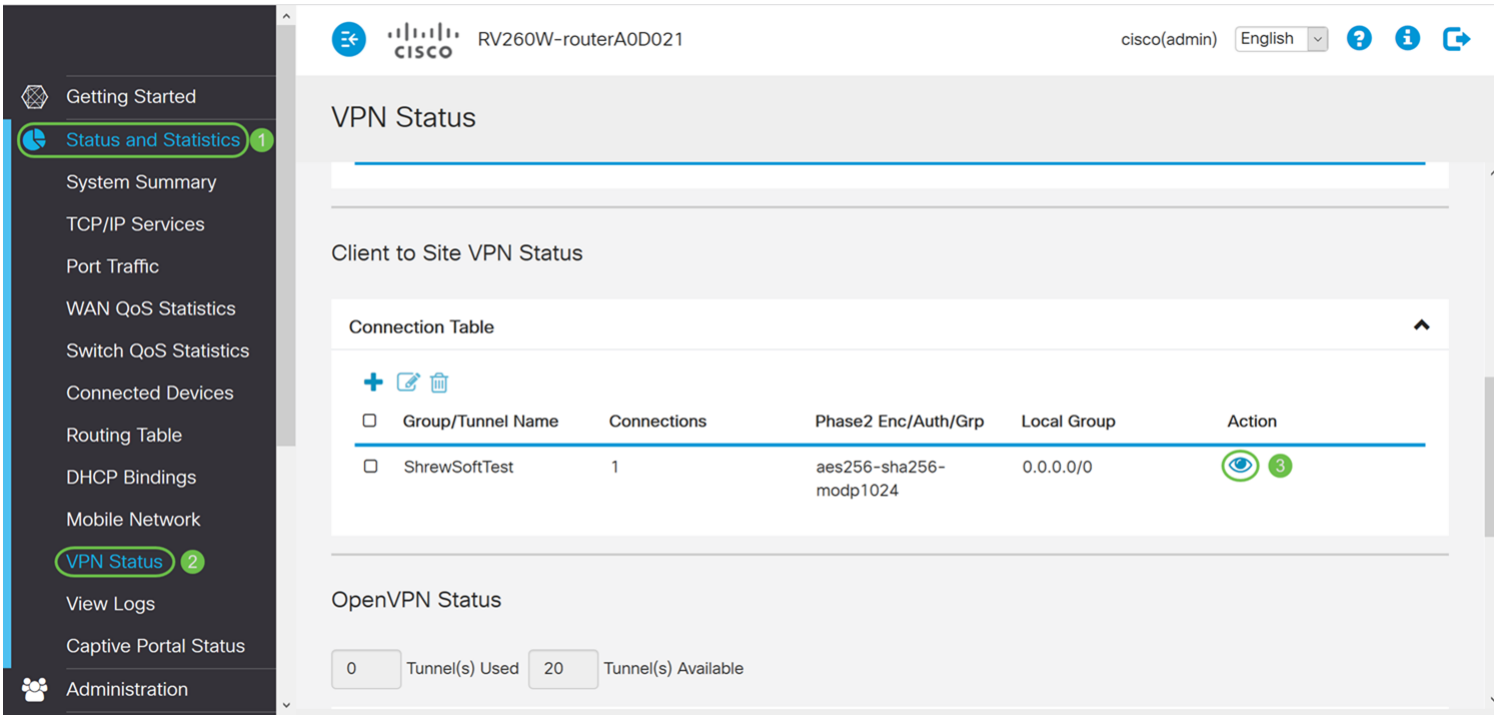


Vérification

Étape 1. Cliquez sur l'onglet *Réseau* de la fenêtre *Connexion VPN*. Dans cet onglet, vous devez être en mesure d'afficher les statistiques réseau actuelles de la connexion. Sous la section *Tunnel*, vous devriez voir *Connected* comme état.

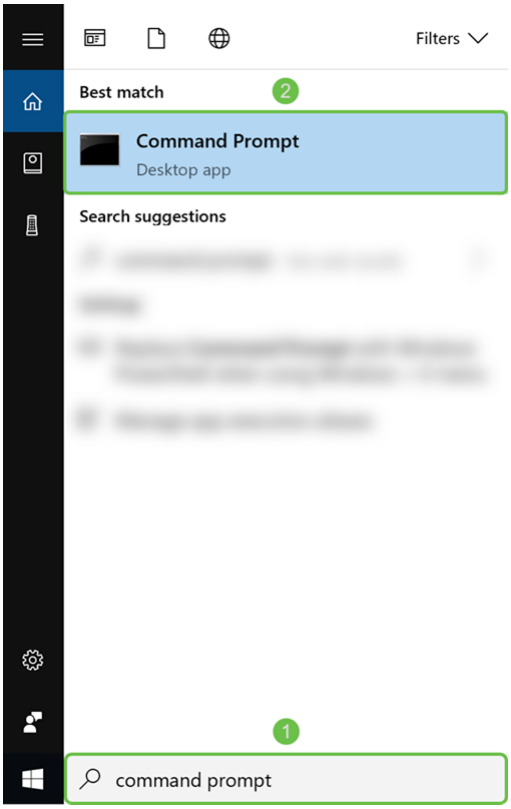


Étape 2. Sur votre routeur, accédez à **Status and Statistics > VPN Status**. Dans la page *VPN Status*, faites défiler jusqu'à la section *Client to Site VPN Status*. Dans cette section, vous pouvez afficher toutes les connexions client-à-site. Cliquez sur l'icône **oeil** pour afficher plus de détails.



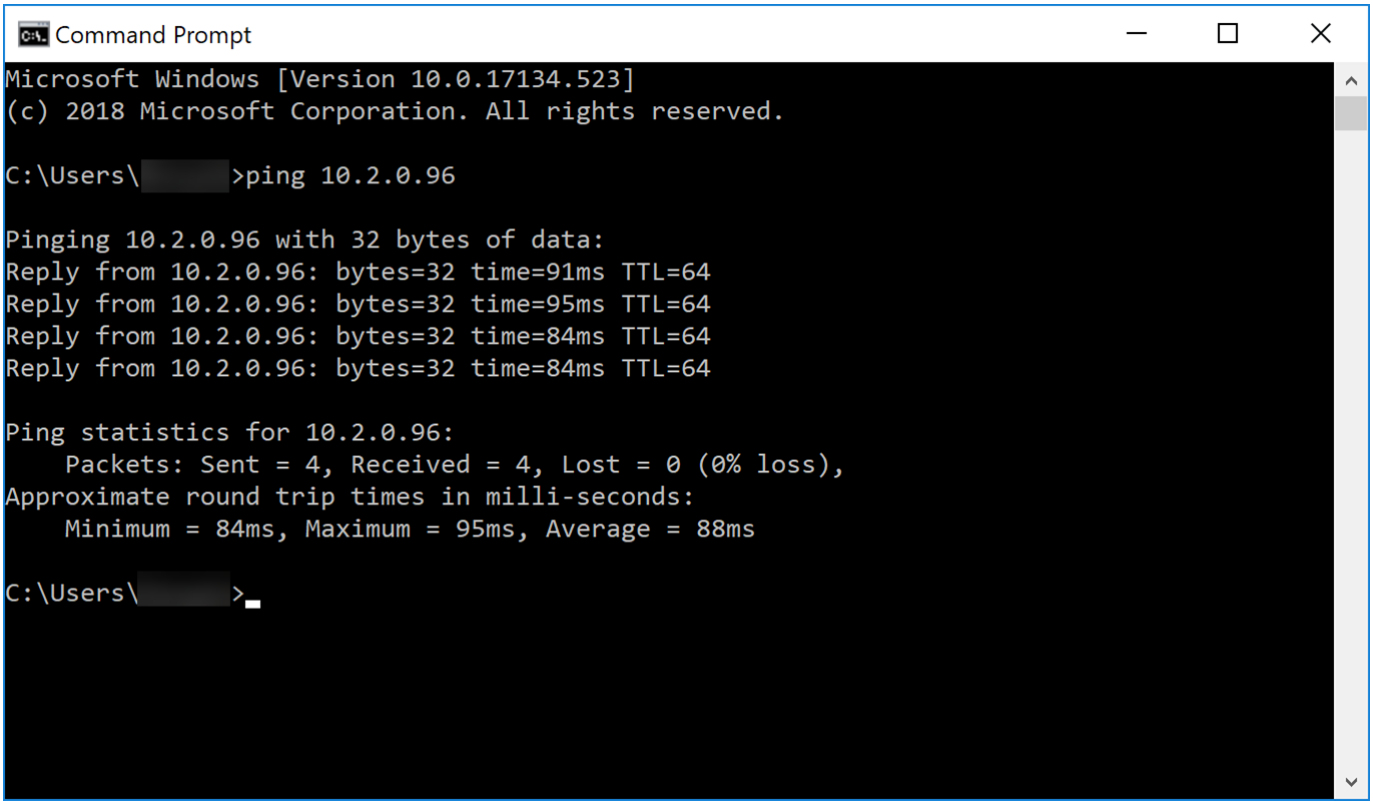
Étape 3. Accédez à la barre de recherche de votre barre des tâches et recherchez **Invite de commandes**.

Note: Les instructions suivantes sont utilisées sur un système d'exploitation Windows 10. Cela peut varier en fonction du système d'exploitation que vous utilisez.



Étape 4. Tapez la commande sans les guillemets, “ **ping [*adresse IP privée du routeur*]** ” mais saisissez l'adresse IP privée au lieu des mots. Vous devriez pouvoir envoyer une requête ping à l’adresse IP privée du routeur.

Dans cet exemple, nous allons taper dans **ping 10.2.0.96**. 10.2.0.96 est l’adresse IP privée de notre routeur.



Conclusion

Vous devez maintenant avoir correctement connecté votre client VPN logiciel Shrew à RV160 ou RV260.