Configuration du client VPN logiciel Shrew pour la connexion au routeur de la gamme RV34X

Objectif

L'objectif de ce document est de montrer comment utiliser le client VPN logiciel Shrew pour se connecter à un routeur de la gamme RV340.

Vous pouvez télécharger la dernière version du logiciel client VPN Shrew Soft ici :

https://www.shrew.net/download/vpn

Périphériques pertinents | Version du logiciel

RV340 | 1.0.3.17 (Télécharger la dernière version)

RV340W | 1.0.3.17 (Télécharger la dernière version)

RV345 | 1.0.3.17 (Télécharger la dernière version)

RV345P | 1.0.3.17 (Télécharger la dernière version)

Introduction/Cas d'utilisation

Le VPN IPSec (Virtual Private Network) vous permet d'obtenir des ressources distantes en toute sécurité en établissant un tunnel crypté sur Internet. Les routeurs de la gamme RV34X fonctionnent comme des serveurs VPN IPSEC et prennent en charge le client VPN logiciel Shrew. Ce guide vous indique comment configurer votre routeur et le client logiciel Shrew pour sécuriser une connexion à un VPN.

Ce document comporte deux parties :

Configuration du routeur de la gamme RV340

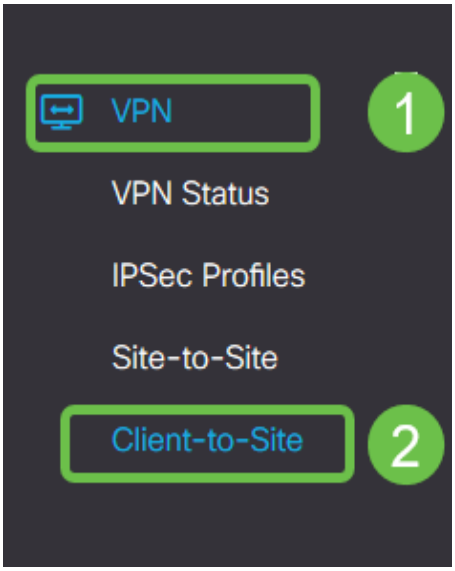
Configurer le client VPN logiciel Shrew

Configurez le routeur de la gamme RV34X :

Nous commencerons par configurer le **VPN client à site** sur le RV34x

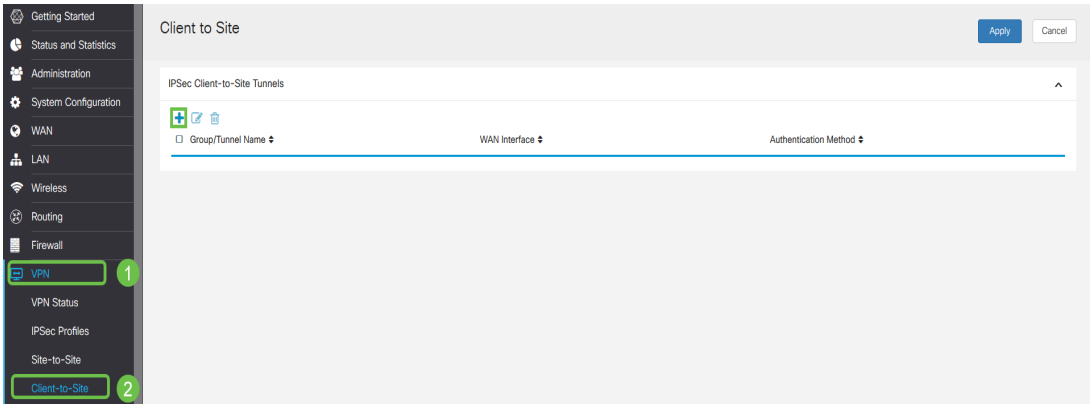
Étape 1

Dans **VPN > Client-to-Site**,



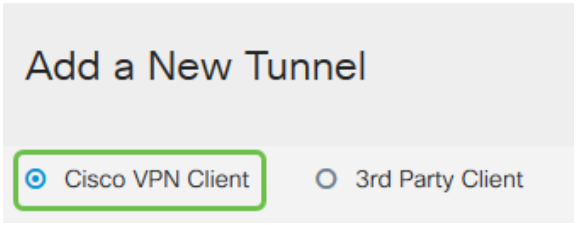
Étape 2

Ajouter un profil VPN **client à site**



Étape 3

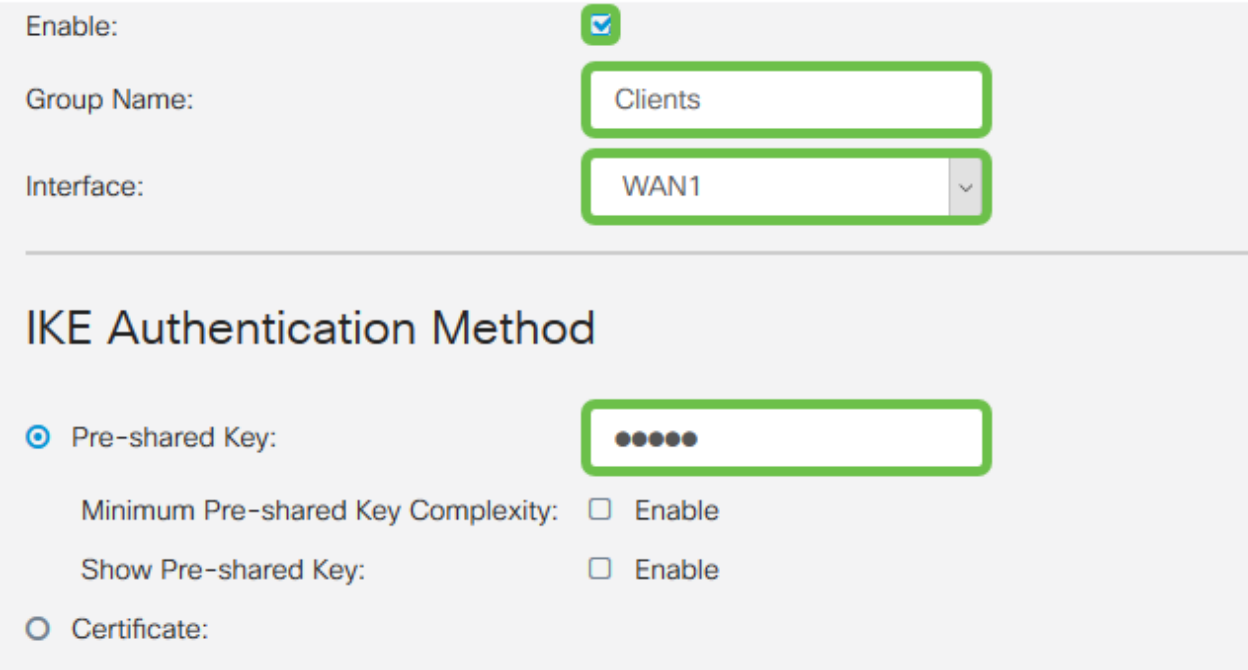
Sélectionnez l'option **Client VPN Cisco**.



Étape 4

Cochez la case **Enable** pour activer le profil de client VPN. Nous allons également configurer le *nom de groupe*, sélectionner l'**interface WAN** et saisir une **clé prépartagée**.

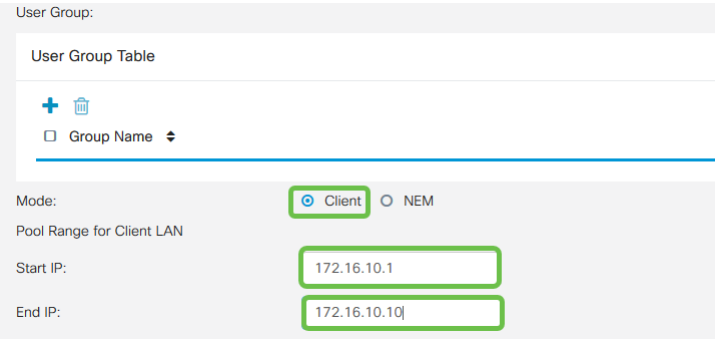
Note: Notez le ***nom du groupe*** et la *clé pré-partagée* car ils seront utilisés ultérieurement lors de la configuration du client.



Étape 5

Laissez la **table Groupe d'utilisateurs** vide pour le moment. Il s'agit du *groupe d'utilisateurs* sur le routeur, mais nous ne l'avons pas encore configuré. Assurez-vous que le **mode** est défini sur **Client**. Entrez la **plage de pools pour le réseau local du client**. Nous utiliserons 172.16.10.1 à 172.16.10.10.

Note: La plage de pools doit utiliser un sous-réseau unique qui n'est pas utilisé ailleurs sur le réseau.



Étape 6

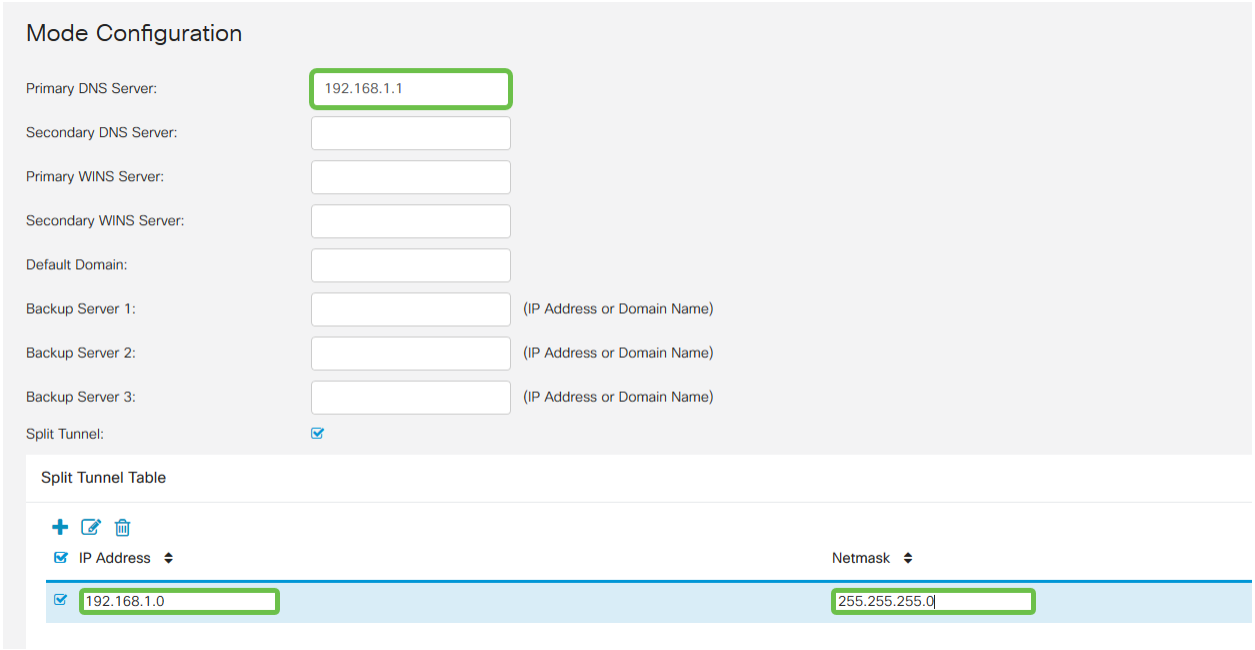
Voici où nous configurons les paramètres **de configuration du mode**. Voici les paramètres que nous allons utiliser :

Serveur DNS principal : Si vous avez un serveur DNS interne ou souhaitez utiliser un serveur DNS externe, vous pouvez le saisir ici. Sinon, la valeur par défaut est l'adresse IP LAN RV340. Nous utiliserons la valeur par défaut dans notre exemple.

Tunnel fractionné : Cochez cette case pour activer la tunnellisation fractionnée. Ceci est utilisé pour spécifier le trafic qui passera par le tunnel VPN. Nous allons utiliser le tunnel partagé

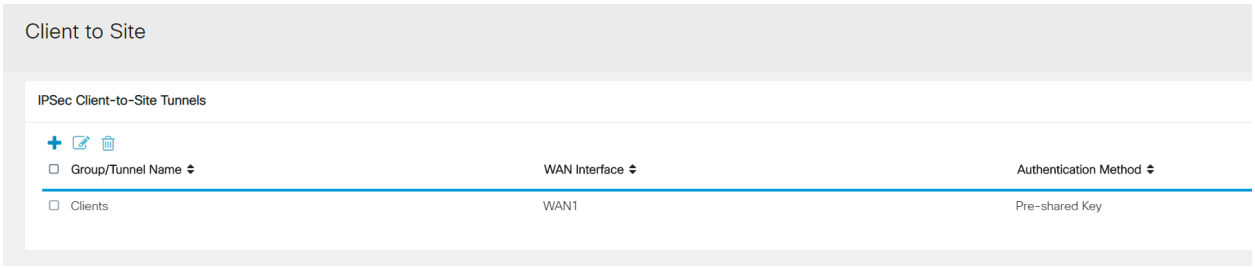
dans notre exemple.

Table de tunnel partagée : Entrez les réseaux auxquels le client VPN doit avoir accès via le VPN. Cet exemple utilise le réseau local RV340.



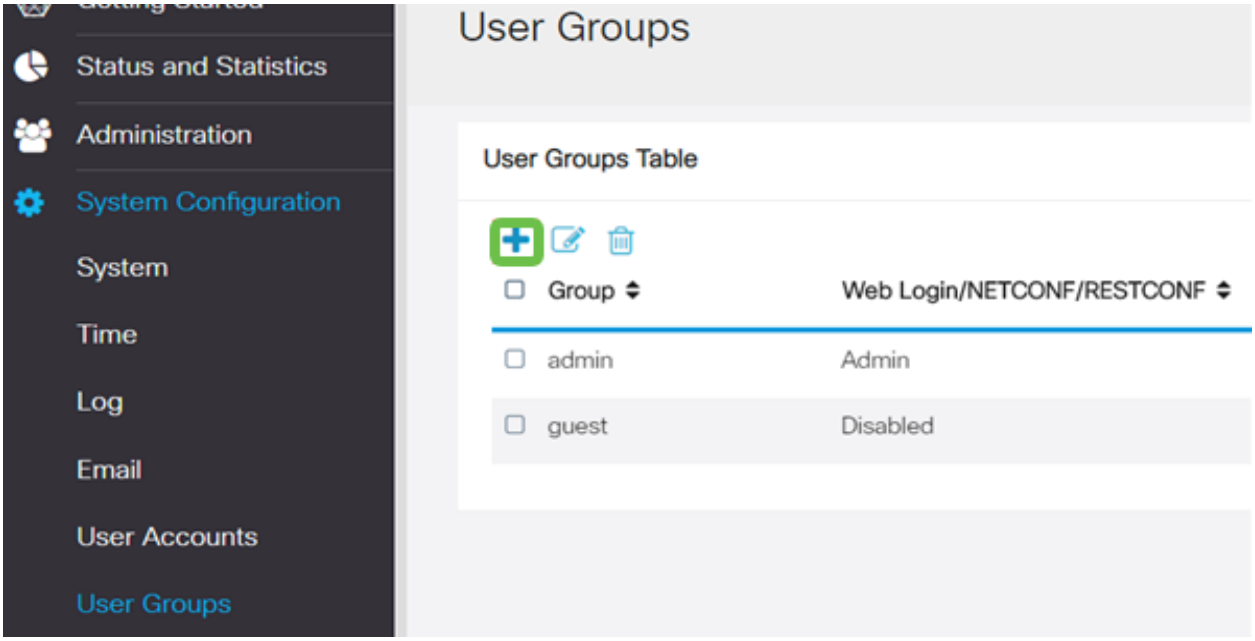
Étape 7

Après avoir cliqué sur **Enregistrer**, nous pouvons voir le profil dans la liste **Groupes client à site IPSec**.



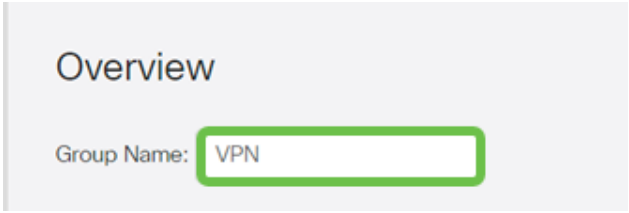
Étape 8

Nous allons maintenant configurer un **groupe d'utilisateurs** à utiliser pour authentifier les utilisateurs du client VPN. Dans **Configuration du système > Groupes d'utilisateurs,** cliquez sur **'+'** pour ajouter un groupe d'utilisateurs.



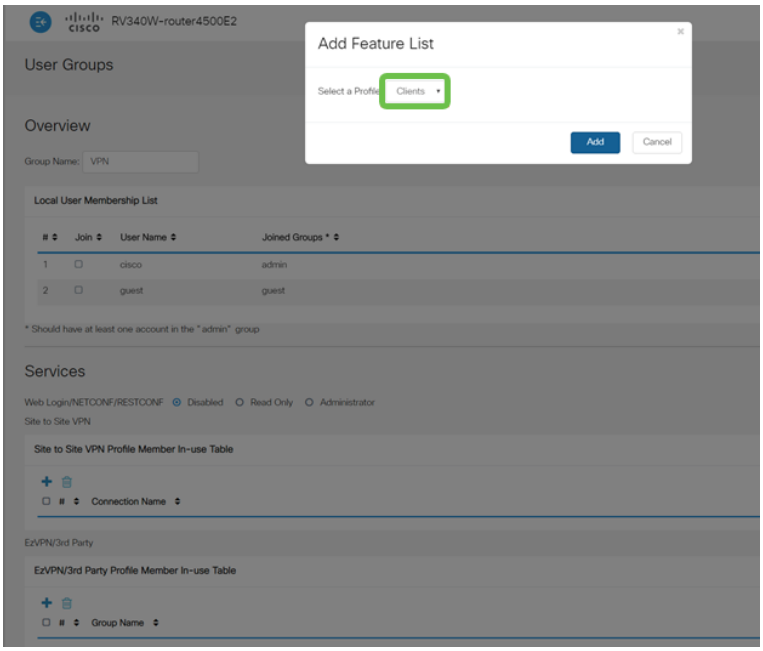
Étape 9

Entrez un **nom de groupe**.



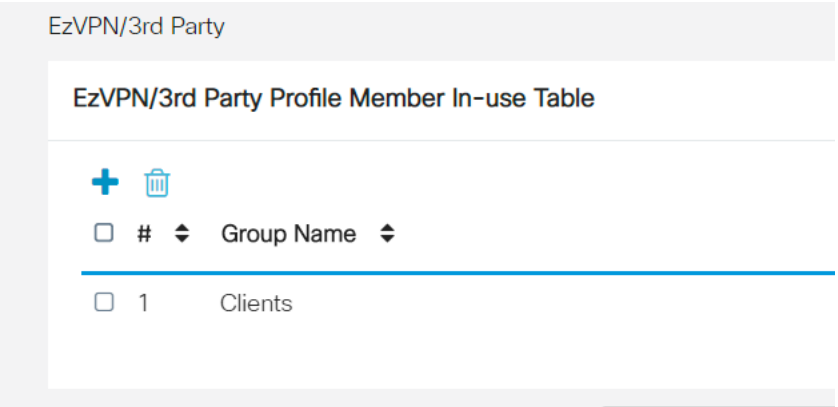
Étape 10

Dans la section **Services** > **EzVPN/tiers**, cliquez sur **Ajouter** pour lier ce groupe d'utilisateurs au **profil client-site** que nous avons configuré précédemment.



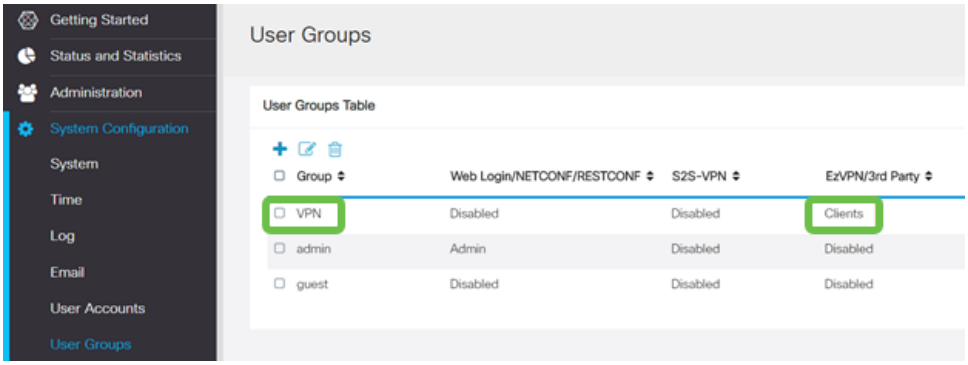
Étape 11

Vous devriez maintenant voir le nom du groupe **client-site** dans la liste pour **EzVPN/tiers**



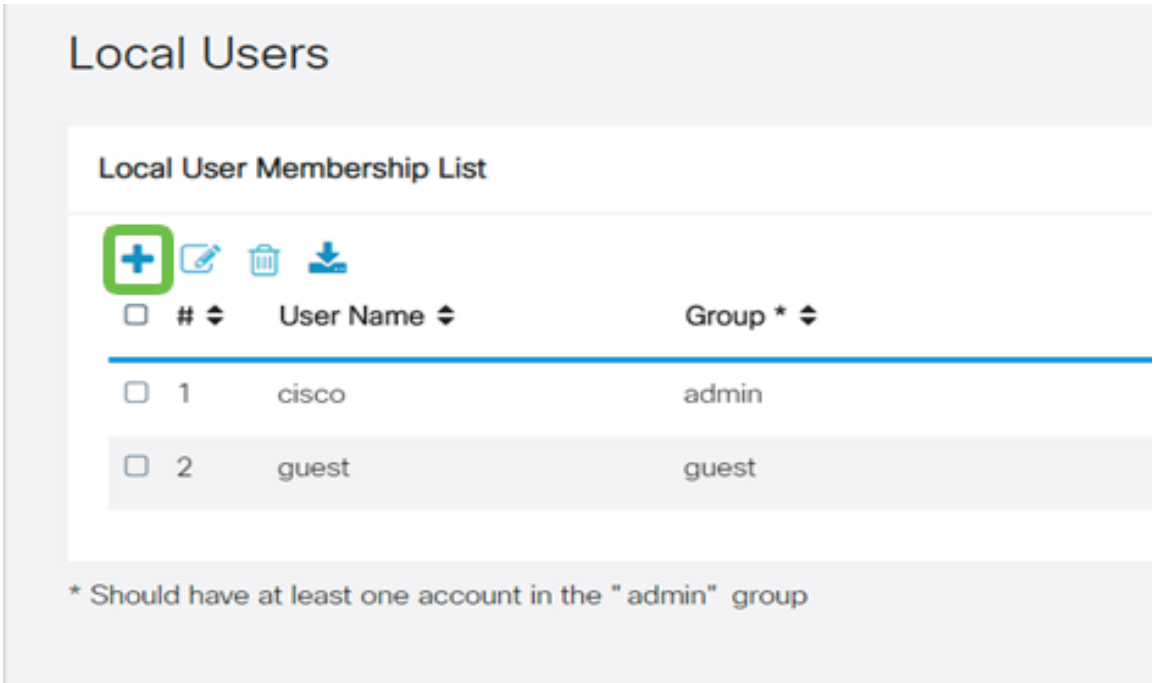
Étape 12

Après avoir **appliqué** la configuration du groupe d'utilisateurs, vous la verrez dans la liste **Groupes d'utilisateurs** et vous verrez que le nouveau groupe d'utilisateurs sera utilisé avec le profil client-site que nous avons créé précédemment.



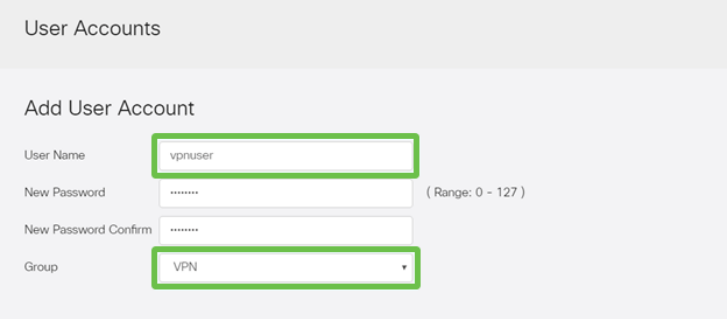
Étape 13

Nous allons maintenant configurer un nouvel utilisateur dans **Configuration système > Comptes d'utilisateurs**. Cliquez sur **'+'** pour créer un nouvel utilisateur.



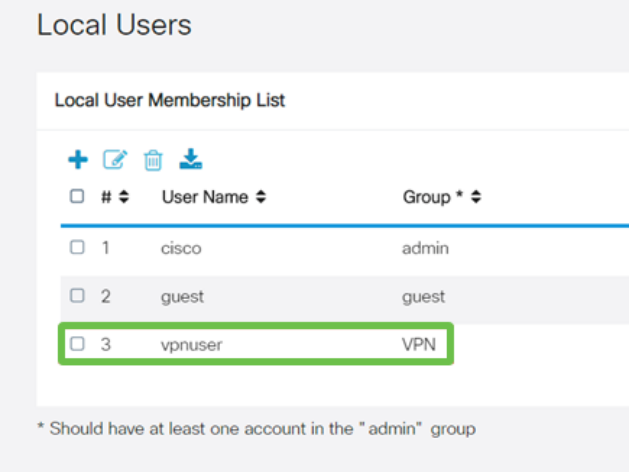
Étape 14

Entrez le nouveau **nom d'utilisateur** ainsi que le **nouveau mot de passe**. Vérifiez que le **groupe** est défini sur le nouveau **groupe d'utilisateurs** que nous venons de configurer. Cliquez sur **Apply** lorsque vous avez terminé.



Étape 15

Le nouvel **utilisateur** apparaîtra dans la liste des **utilisateurs locaux**.



La configuration du routeur de la gamme RV340 est terminée. Nous allons maintenant configurer le client VPN logiciel Shrew.

Configurer le client VPN ShrewSoft

Nous allons maintenant configurer le client VPN logiciel Shrew.

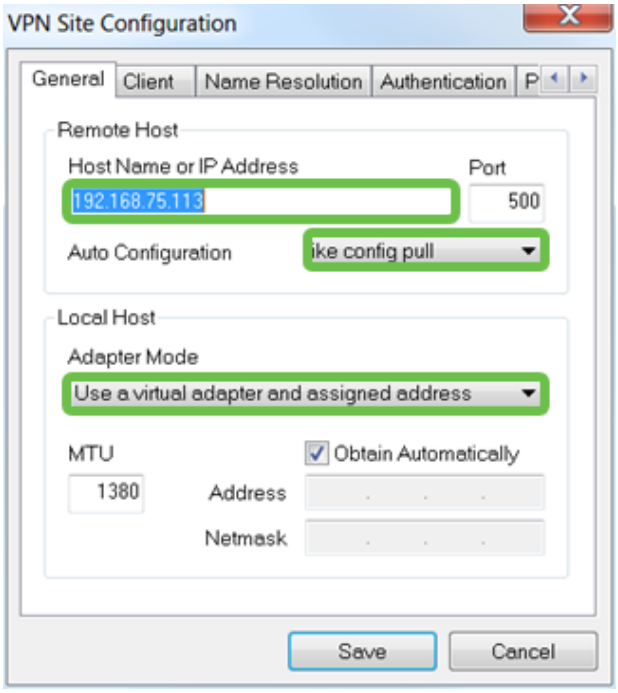
Étape 1

Ouvrez le *Gestionnaire d'accès VPN* ShrewSoft et cliquez sur **Ajouter** pour ajouter un profil. Dans la fenêtre *Configuration du site VPN* qui s'affiche, configurez l'onglet **Général** :

Nom d'hôte ou adresse IP : Utiliser l'adresse IP WAN (ou le nom d'hôte du routeur RV340)

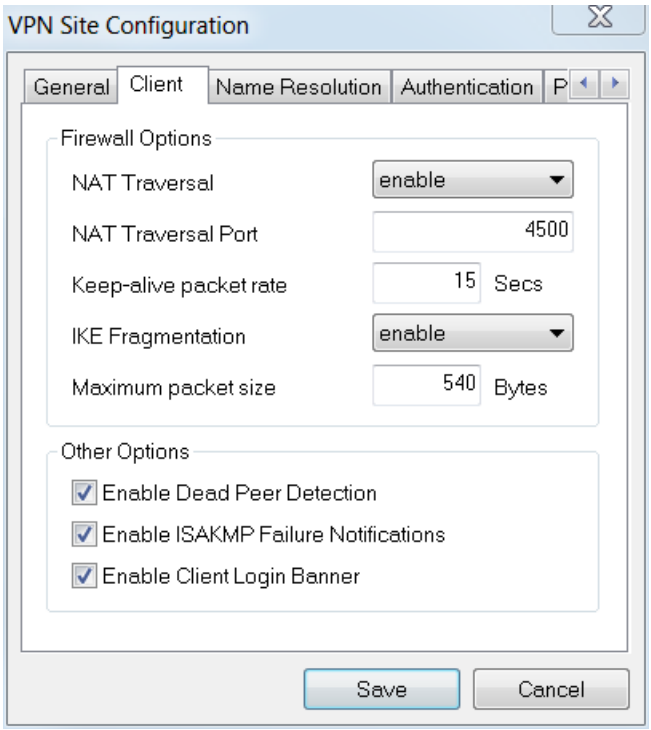
Configuration automatique : Sélectionner **comme configuration pull**

Mode adaptateur : Sélectionnez **Utiliser une carte virtuelle et l'adresse attribuée**



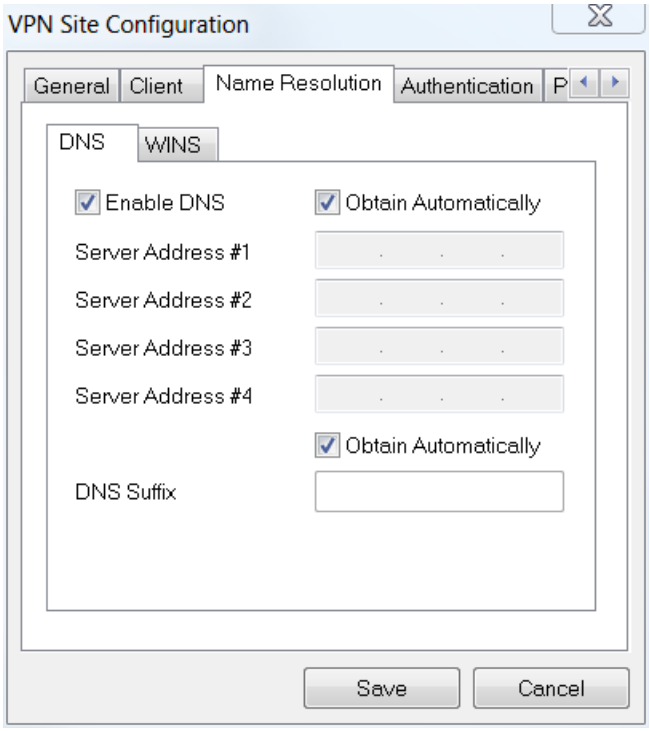
Étape 2

Configurez l'onglet **Client**. Nous utiliserons simplement les paramètres par défaut.



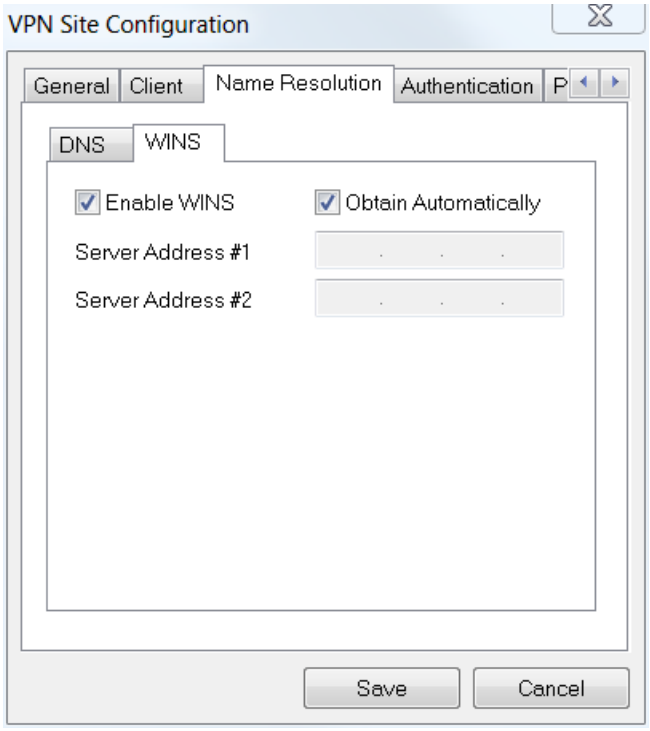
Étape 3

Dans l'onglet **Résolution de noms > DNS**, cochez la case **Activer DNS** et laissez les cases **Obtenir automatiquement** cochées.



Étape 4

Dans l'onglet **Résolution de noms > WINS**, cochez la case **Activer WINS** et laissez la case **Obtenir automatiquement** cochée.

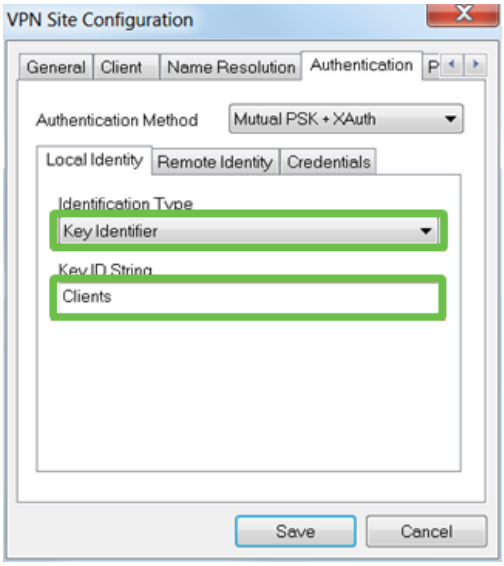


Étape 5

Configurez l'onglet **Authentification > Identité locale** :

Type d'identification : Sélectionner **l'identificateur de clé**

Chaîne d'ID de clé : Entrez le **nom du groupe** configuré sur le RV34x



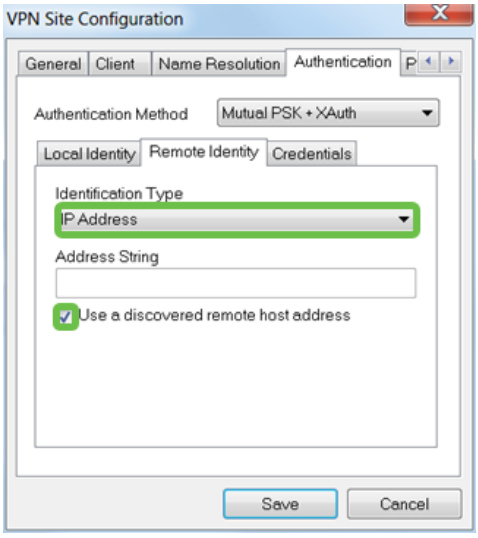
Étape 6

Dans l'onglet **Authentification > Identité distante**, nous laisserons les paramètres par défaut.

Type d'identification : Adresse IP

Chaîne d'adresses : <vierge>

Utilisez une zone **d'adresse d'hôte distant découverte** : Coché

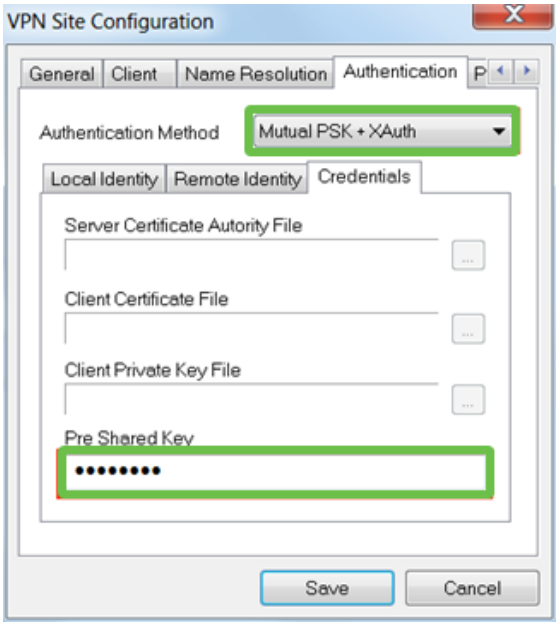


Étape 7

Dans l'onglet **Authentification > Informations d'identification**, configurez les éléments suivants :

Méthode d'authentification : Sélectionner **PSK mutuel + XAuth**

Clé pré-partagée : Entrez la **clé prépartagée** configurée dans le profil client RV340



Étape 8

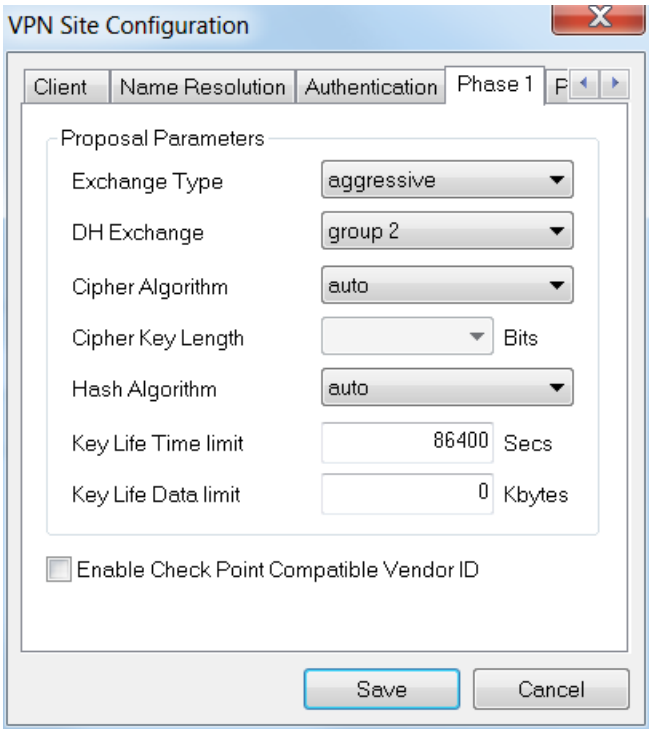
Pour l'onglet **Phase 1**, les paramètres par défaut restent en place :

Type d'échange : Agressif

Échange DH : groupe 2

Algorithme de chiffrement : « Auto »

Algorithme de hachage : « Auto »



Étape 9

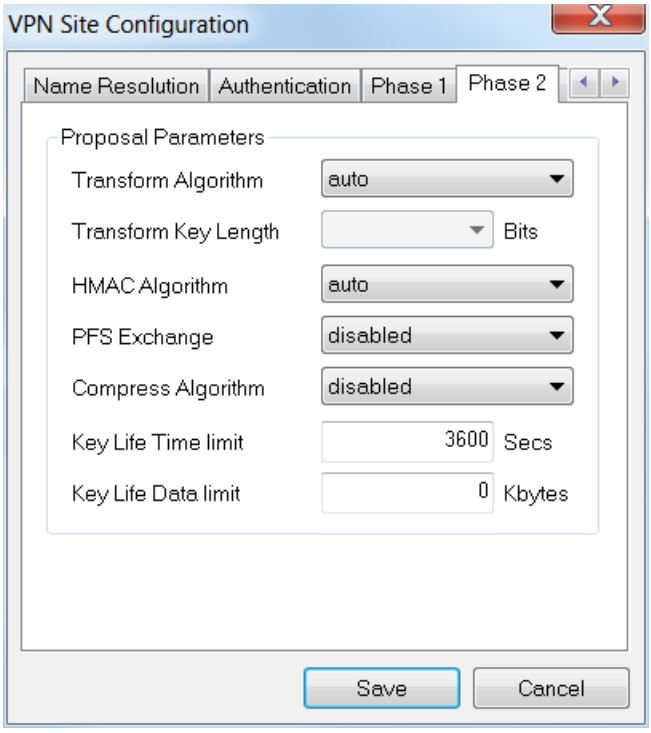
Nous utiliserons également les valeurs par défaut de l'onglet **Phase 2** :

Algorithme de transformation : « Auto »

Algorithme HMAC : « Auto »

Échange PFS : Désactivé

Algorithme de compression : Désactivé



Étape 10

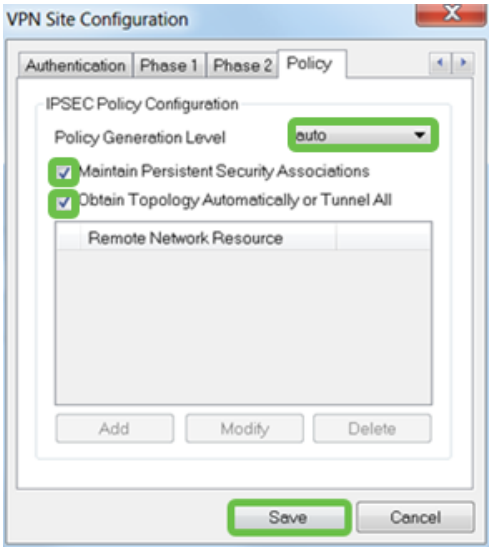
Pour l'onglet **Stratégie**, nous utiliserons les paramètres suivants :

Niveau de génération de stratégie : « Auto »

Tenir À Jour Les Associations De Sécurité Persistantes : Coché

Obtenir la topologie automatiquement ou Tunnel All : Coché

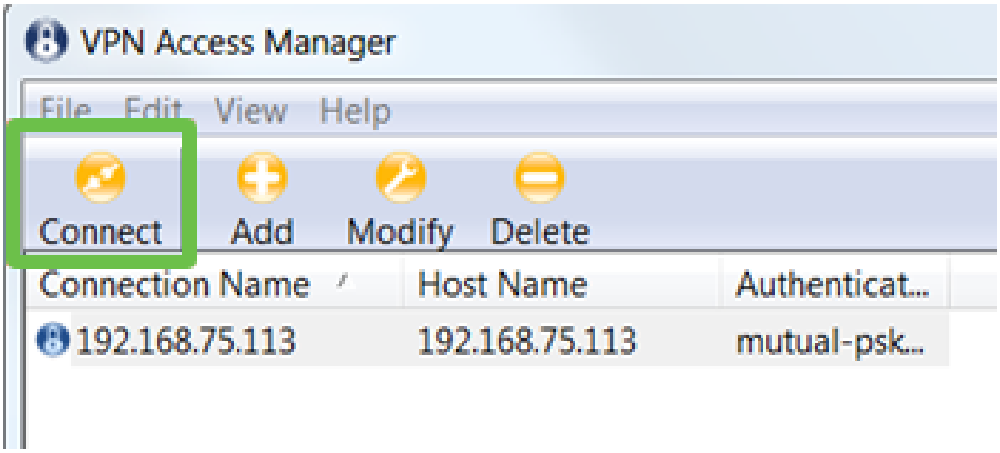
Puisque nous avons configuré la **tunnellisation partagée** sur le RV340, nous n'avons pas besoin de le configurer ici.



Une fois terminé, cliquez sur **Save** (enregistrer).

Étape 11

Nous sommes maintenant prêts à tester la connexion. Dans *VPN Access Manager*, mettez en surbrillance le profil de connexion et cliquez sur le bouton **Connect**.



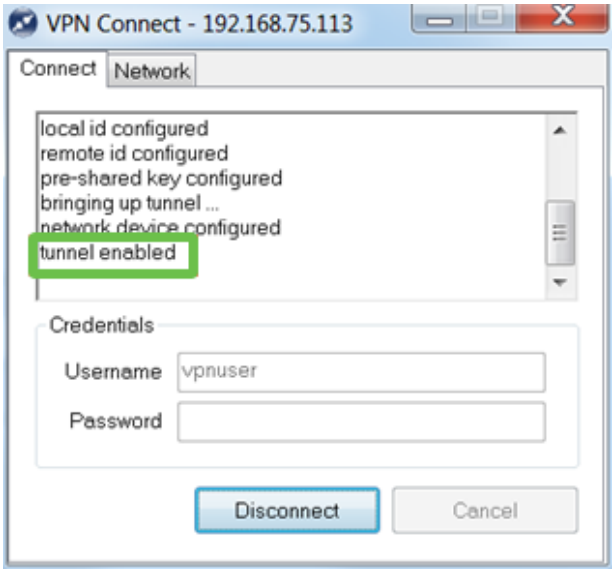
Étape 12

Dans la fenêtre **VPN Connect** qui apparaît, entrez le **nom d'utilisateur** et le **mot de passe** à l'aide des informations d'identification du **compte d'utilisateur** que nous avons créé sur le RV340 (étapes 13 et 14).

Lorsque vous avez terminé, cliquez sur **Connect**.

Étape 13

Vérifiez que le tunnel est connecté. Le **tunnel** doit être **activé**.



Conclusion

Là, vous êtes maintenant configuré pour vous connecter à votre réseau via VPN.