

Utiliser le client VPN logiciel Shrew pour se connecter au serveur VPN IPSec sur les modèles RV130 et RV130W

Objectif

VPN IPSec (Virtual Private Network, réseau privé virtuel) vous permet d'obtenir des ressources distantes en toute sécurité en établissant un tunnel chiffré sur Internet.

Les routeurs RV130 et RV130W fonctionnent comme des serveurs VPN IPSec et prennent en charge le client VPN logiciel Shrew.

Veillez à télécharger la dernière version du logiciel client.

·Shrew Soft (<https://www.shrew.net/download/vpn>)

Note: Pour réussir la configuration du client VPN logiciel Shrew avec un serveur VPN IPSec, vous devez d'abord configurer le serveur VPN IPSec. Pour plus d'informations sur la façon de faire ceci, référez-vous à l'article [Configuration d'un serveur VPN IPSec sur RV130 et RV130W](#).

L'objectif de ce document est de vous montrer comment utiliser le client VPN logiciel Shrew pour se connecter à un serveur VPN IPSec sur les routeurs RV130 et RV130W.

Périphériques pertinents

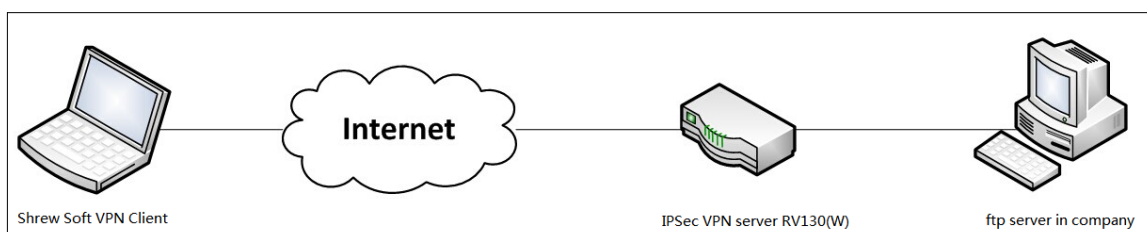
- Pare-feu VPN sans fil N RV130W
- Pare-feu VPN RV130

Configuration système nécessaire

- Systèmes 32 ou 64 bits
- Windows 2000, XP, Vista ou Windows 7/8

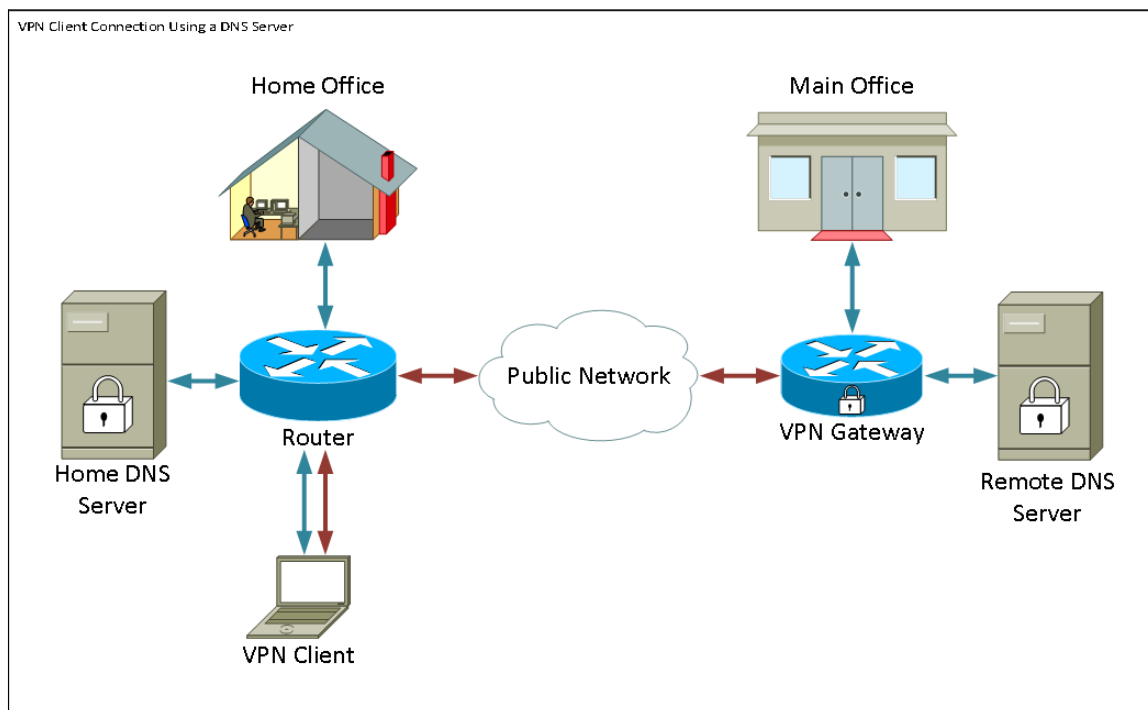
Topologie

Une topologie de niveau supérieur est illustrée ci-dessous pour illustrer les périphériques impliqués dans une configuration client à site Shrewsoft.



Un organigramme plus détaillé illustrant le rôle des serveurs DNS dans un environnement

réseau de petite entreprise est présenté ci-dessous.



Version du logiciel

•1.0.1.3

Configuration du client VPN logiciel Shrew

Configuration VPN IPsec et configuration utilisateur

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

Setup

Server Enable:

NAT Traversal: Disabled

Phase 1 Configuration

Pre-Shared Key:

Exchange Mode:

Encryption Algorithm:

Authentication Algorithm:

DH Group:

IKE SA Life Time: Seconds (Range: 30 - 86400, Default: 3600)

Phase 2 Configuration

Local IP:

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

IPSec SA Lifetime: Seconds (Range: 30 - 86400, Default: 28800)

Encryption Algorithm:


Authentication Algorithm:

PFS Key Group: Enable

DH Group:

Étape 2 : vérification de la configuration du serveur VPN IPsec pour le routeur RV130 Si le serveur VPN IPsec n'est pas configuré ou mal configuré, référez-vous à [Configuration d'un serveur VPN IPsec sur RV130 et RV130W](#) et cliquez sur **Save**.

Setup

 Configuration settings have been saved successfully

Server Enable:

NAT Traversal: Disabled

Phase 1 Configuration

Pre-Shared Key:

Exchange Mode:

Encryption Algorithm:

Authentication Algorithm:

DH Group:

IKE SA Life Time: Seconds (Range: 30 - 86400, Default: 3600)

Phase 2 Configuration

Local IP:

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

IPSec SA Lifetime: Seconds (Range: 30 - 86400, Default: 28800)

Encryption Algorithm:

Authentication Algorithm:

PFS Key Group: Enable

DH Group:

Note: Les paramètres ci-dessus sont un exemple de configuration de serveur VPN IPSec RV130/RV130W. Les paramètres sont basés sur le document [Configuration of an IPSec VPN Server on RV130 and RV130W](#), et seront mentionnés dans les étapes suivantes.

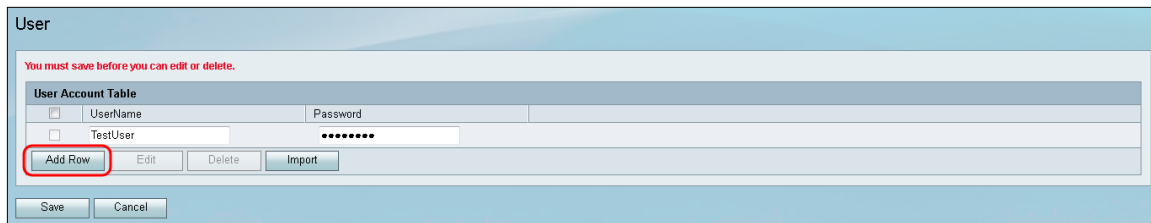
Étape 3. Accédez à **VPN > IPSec VPN Server > User**. La page *User* s'affiche.

User

User Account Table

<input type="checkbox"/>	UserName	Password
<input type="checkbox"/>	No data to display	

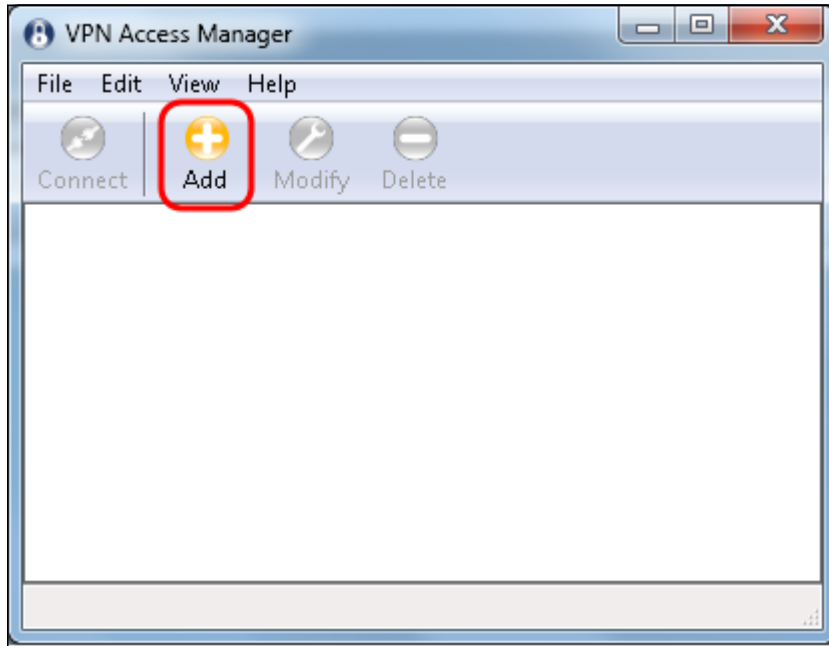
Étape 4. Cliquez sur **Add Row** pour ajouter des comptes d'utilisateurs, utilisés pour authentifier les clients VPN (Extended Authentication), et entrez le nom d'utilisateur et le mot de passe souhaités dans les champs fournis.



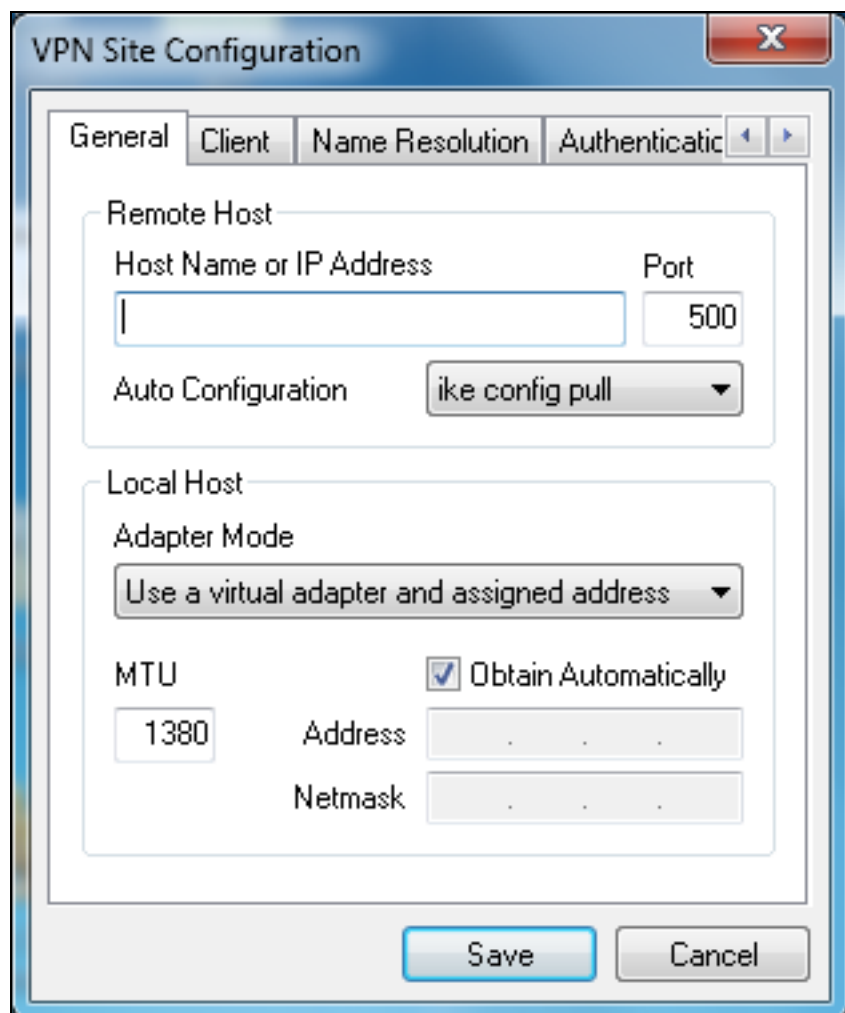
Étape 5. Cliquez sur **Save** pour enregistrer les paramètres.

Configuration du client VPN

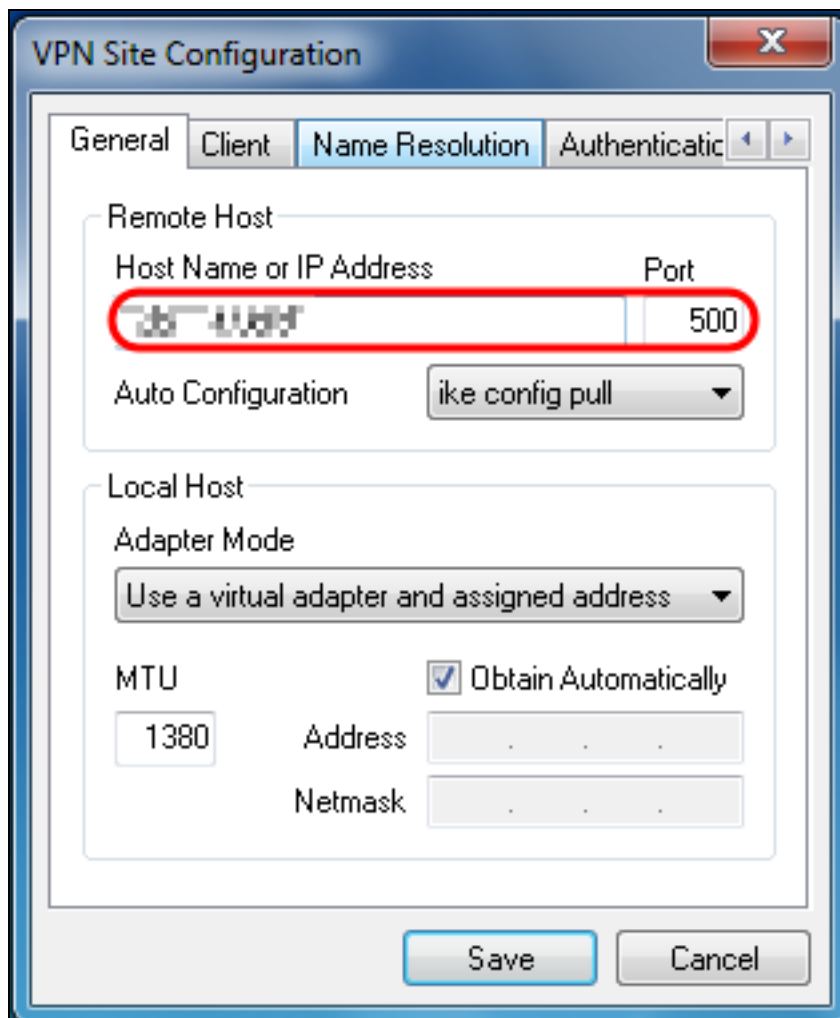
Étape 1. Ouvrez Shrew VPN Access Manager et cliquez sur **Add** pour ajouter un profil.



La fenêtre *VPN Site Configuration* s'affiche.

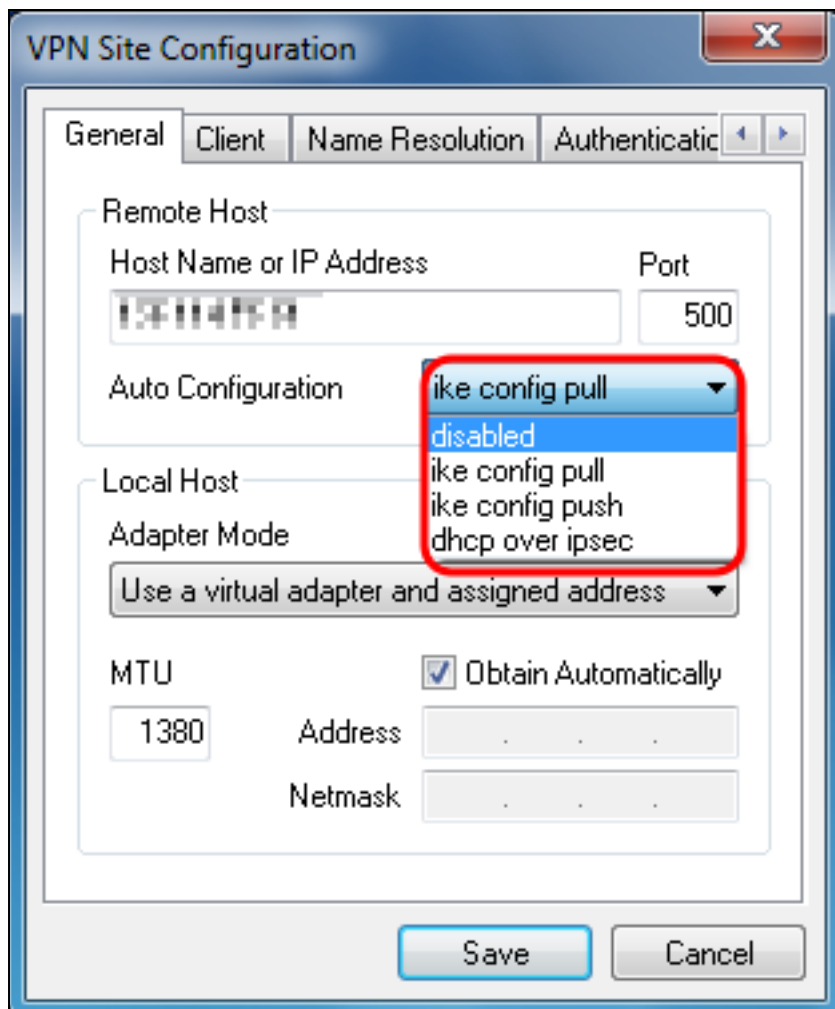


Étape 2. Dans la section *Remote Host* sous l'onglet *General*, entrez le nom d'hôte ou l'adresse IP publique du réseau auquel vous essayez de vous connecter.



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

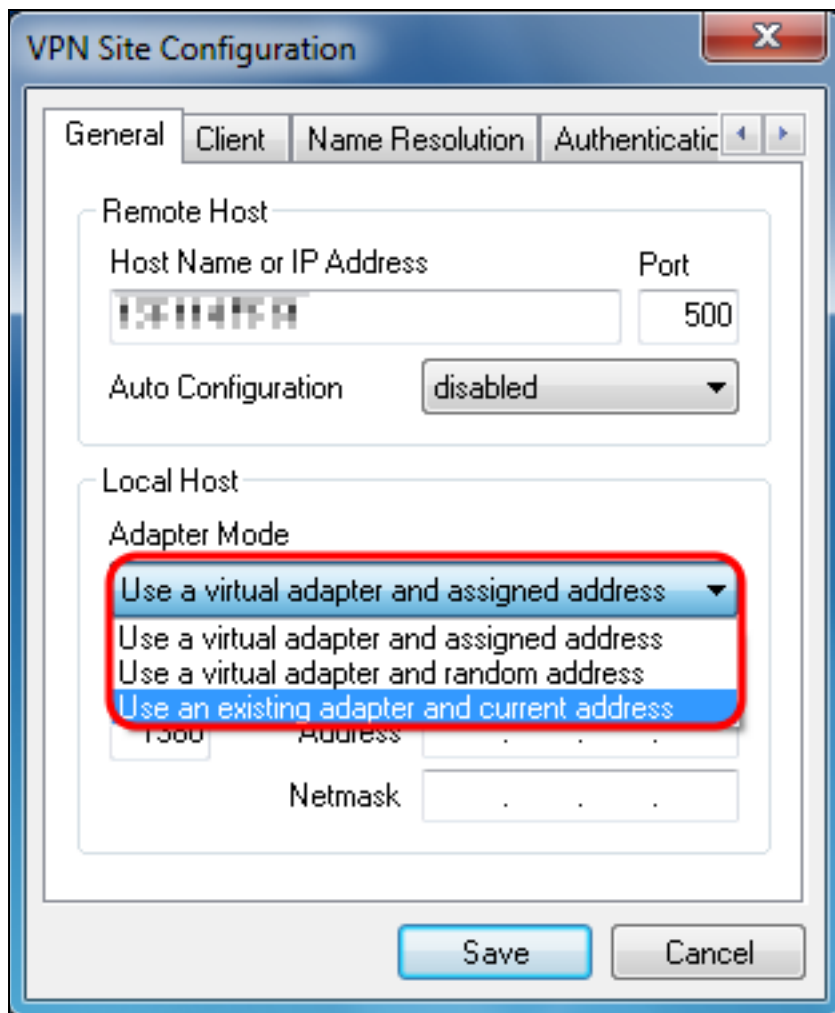
Étape 3. Dans la liste déroulante *Configuration automatique*, sélectionnez **disabled**.



Les options disponibles sont définies comme suit :

- Disabled : désactive toutes les configurations client automatiques.
- IKE Config Pull : permet au client de définir les requêtes d'un ordinateur. Avec la prise en charge de la méthode Pull par l'ordinateur, la demande renvoie une liste de paramètres pris en charge par le client.
- IKE Config Push : permet à un ordinateur de proposer 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 renvoie une liste de paramètres pris en charge par le client.
- DHCP sur IPsec : permet au client de demander des paramètres à l'ordinateur via DHCP sur IPsec.

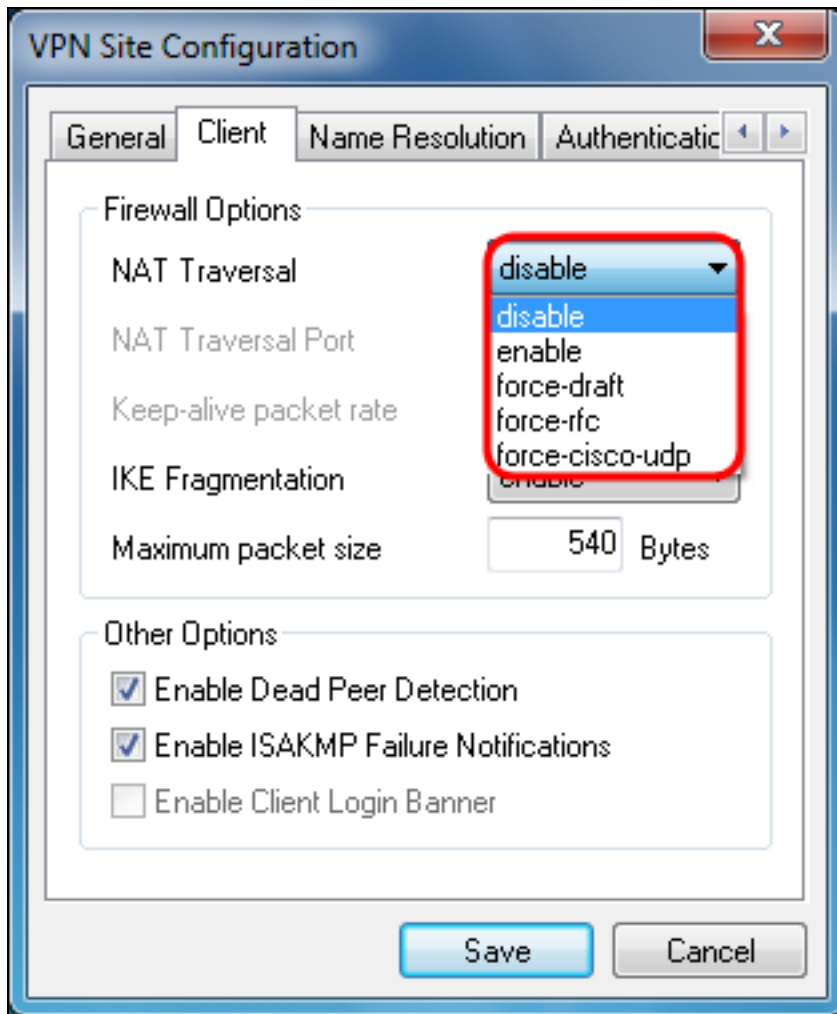
Étape 4. Dans la section *Local Host*, choisissez **Use an existing adapter and current address** dans la liste déroulante *Adapter Mode*.



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 pour ses communications IPsec.
- Use a virtual adapter and random address : permet au client d'utiliser une carte virtuelle avec une adresse aléatoire comme source de ses communications IPsec.
- Use an existing adapter and current address : permet au client d'utiliser uniquement sa carte physique existante avec son adresse actuelle comme source pour ses communications IPsec.

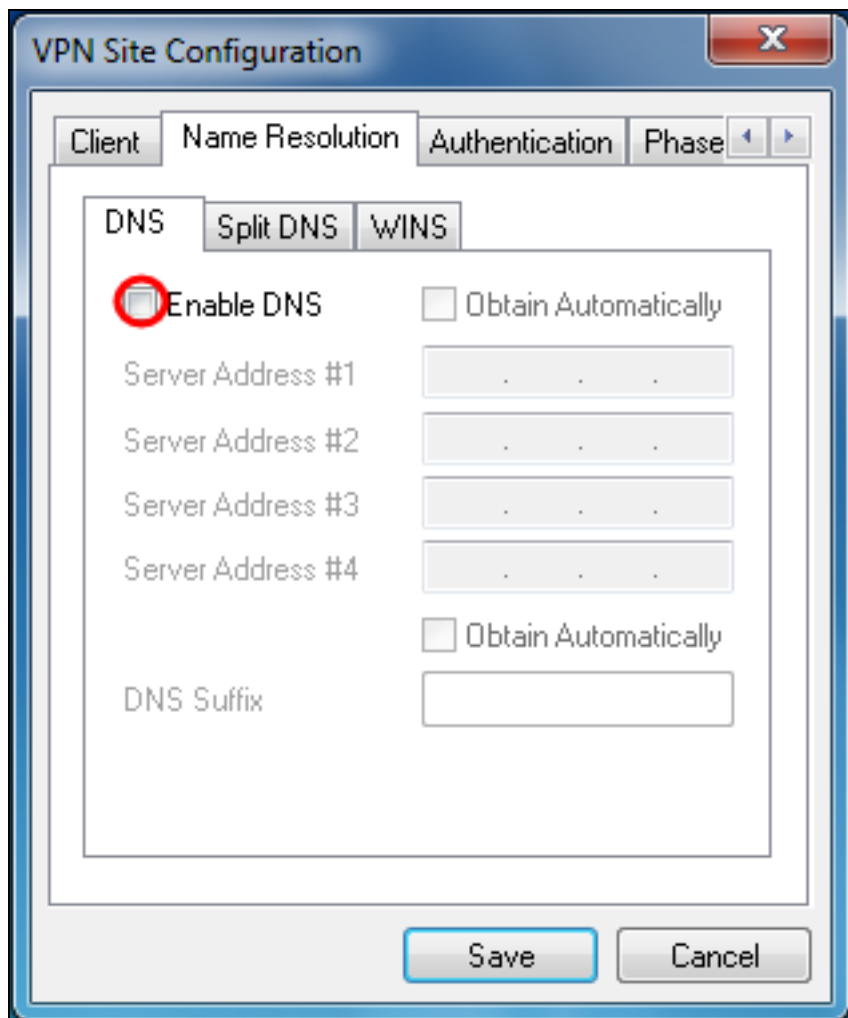
Étape 5. Cliquez sur l'onglet *Client*. Dans la liste déroulante *NAT Traversal*, sélectionnez le même paramètre que vous avez configuré sur le RV130/RV130W pour NAT Traversal dans l'article [Configuration d'un serveur VPN IPsec sur RV130 et RV130W](#).



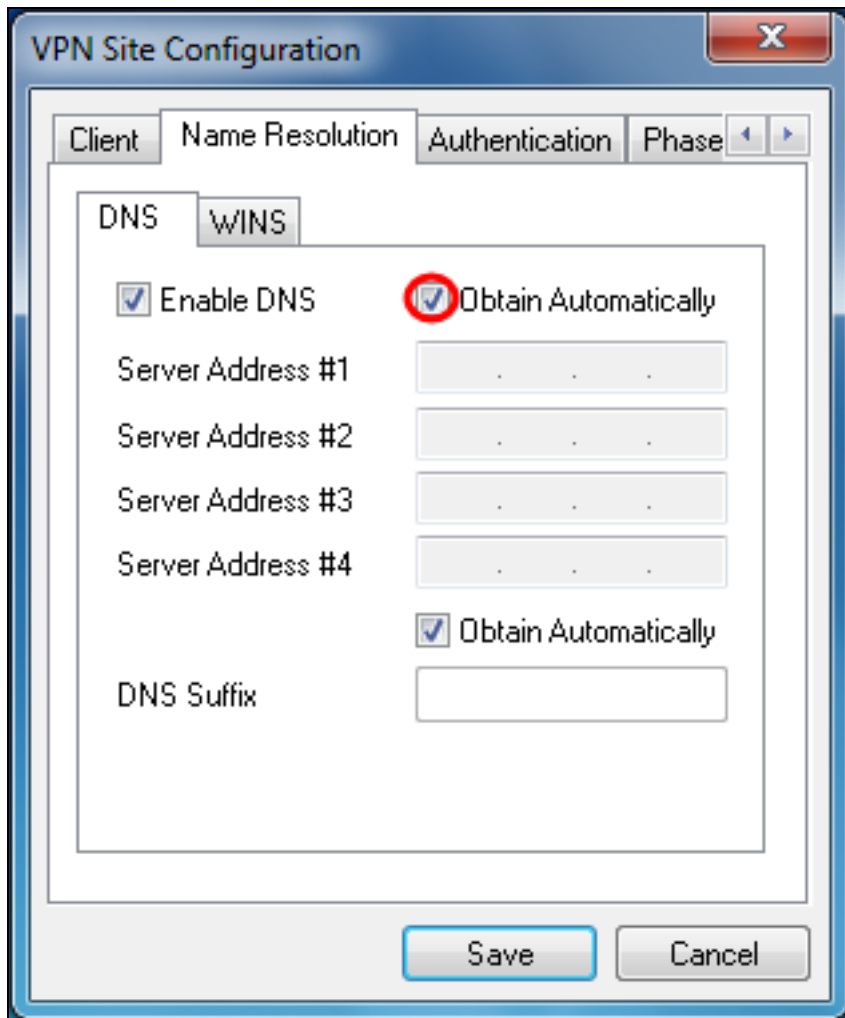
Les options de menu NAT (Network Address Translation Traversal) disponibles sont définies comme suit :

- Disable : les extensions du protocole NAT ne seront pas utilisées.
- Enable : les extensions du protocole NAT ne seront utilisées que si la passerelle VPN indique la prise en charge pendant les négociations et que la NAT est détectée.
- Forcer-Draft : la version préliminaire des extensions du protocole NAT sera utilisée, que la passerelle VPN indique une prise en charge lors des négociations ou que la NAT soit détectée ou non.
- Force-RFC : la version RFC du protocole NAT sera utilisée, que la passerelle VPN indique une prise en charge lors des négociations ou que la NAT soit détectée ou non.
- Force-Cisco-UDP — Force l'encapsulation UDP pour les clients VPN sans NAT.

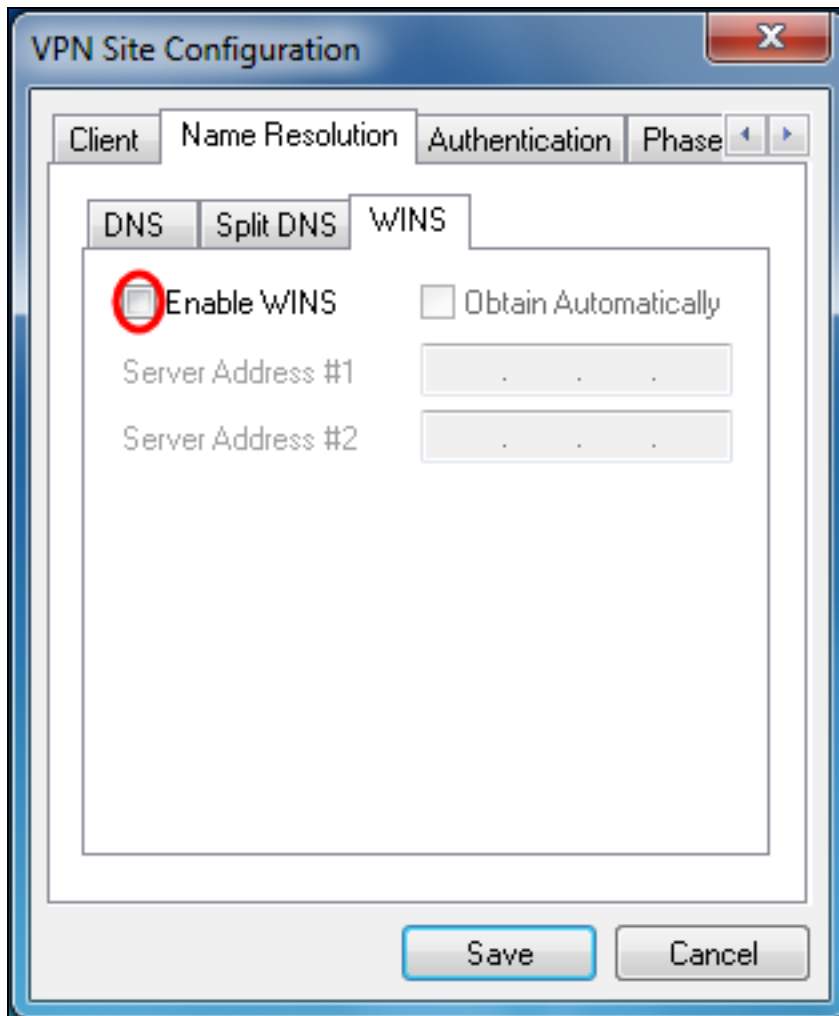
Étape 6. Cliquez sur l'onglet *Name Resolution*, et cochez la case **Enable DNS** si vous souhaitez activer DNS. Si des paramètres DNS spécifiques ne sont pas requis pour la configuration de votre site, décochez la case **Enable DNS**.



Étape 7. (Facultatif) Si votre passerelle distante est configurée pour prendre en charge l'échange de configuration, la passerelle peut fournir automatiquement les paramètres DNS. Si ce n'est pas le cas, vérifiez que la case **Obtain Automatically** est décochée et entrez manuellement une adresse de serveur DNS valide.

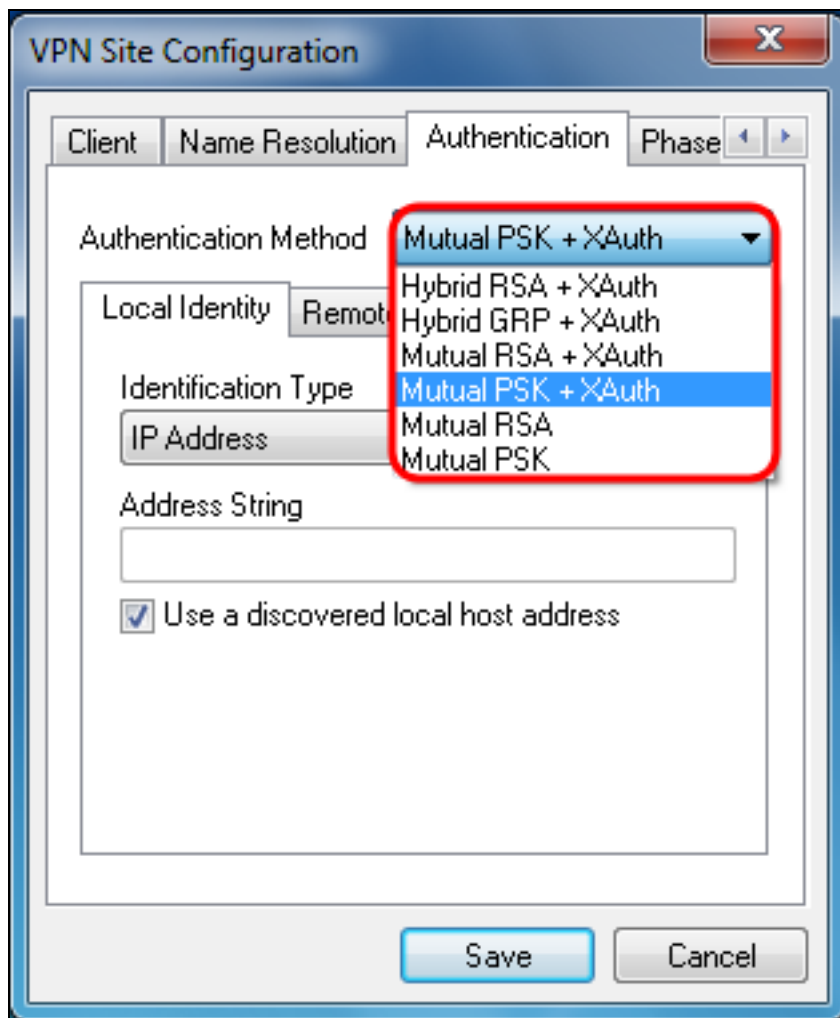


Étape 8. (Facultatif) Cliquez sur l'onglet *Résolution de noms*, cochez la case **Activer WINS** si vous souhaitez activer le serveur de noms Internet Windows (WINS). Si votre passerelle distante est configurée pour prendre en charge l'échange de configuration, elle peut fournir automatiquement les paramètres WINS. Si ce n'est pas le cas, vérifiez que la case à cocher **Obtain Automatically** est désactivée et entrez manuellement une adresse de serveur WINS valide.



Note: En fournissant des informations de configuration WINS, un client pourra résoudre les noms WINS à l'aide d'un serveur situé sur le réseau privé distant. Cela est utile lorsque vous tentez d'accéder à des ressources réseau Windows distantes à l'aide d'un nom de chemin de convention d'attribution de noms uniforme. Le serveur WINS appartient généralement à un contrôleur de domaine Windows ou à un serveur Samba.

Étape 9. Cliquez sur l'onglet *Authentication* et sélectionnez **Mutual PSK + XAuth** dans la liste déroulante *Authentication Method*.

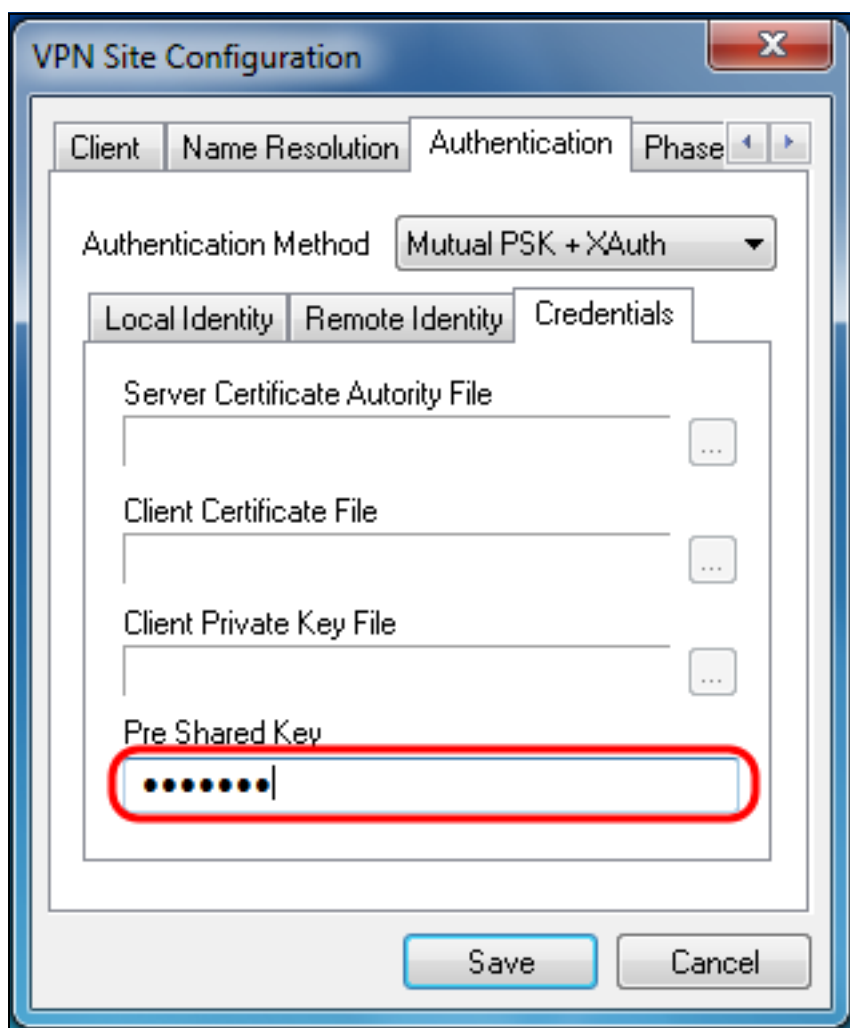


Les options disponibles sont définies comme suit :

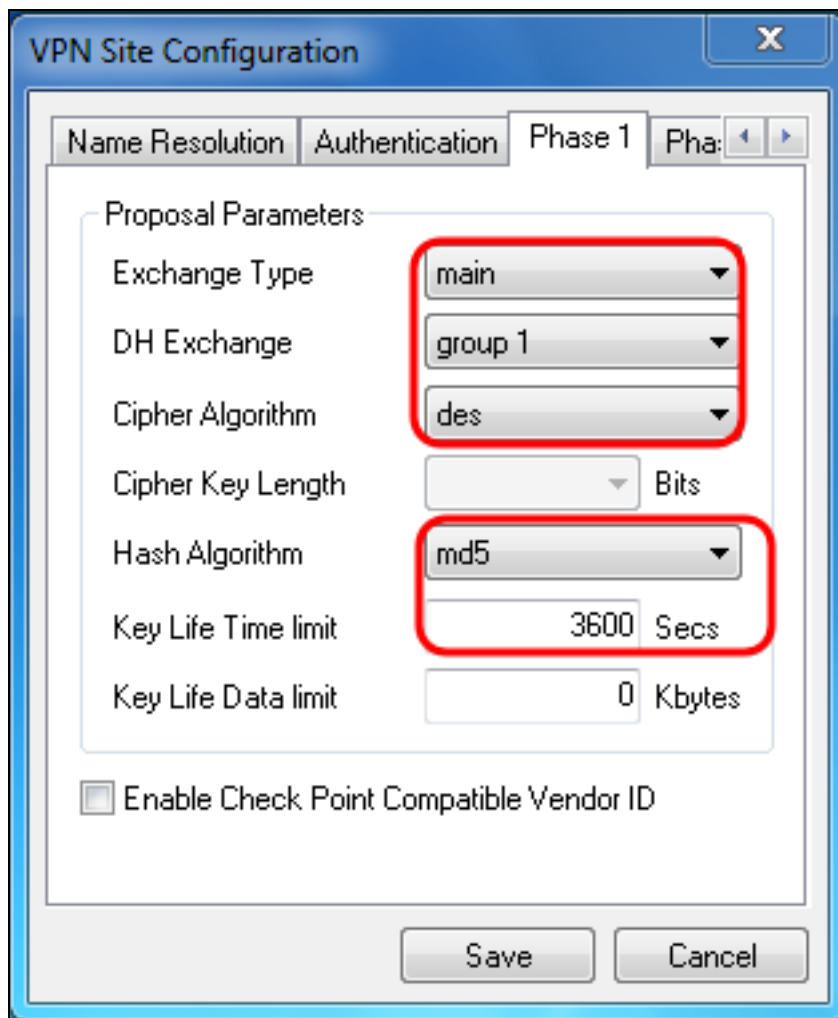
- RSA hybride + XAuth — Les informations d'identification du client ne sont pas nécessaires. Le client authentifie la passerelle. Les informations d'identification se présentent sous la forme de fichiers de certificats PEM ou PKCS12 ou de fichiers de clés.
- Hybrid GRP + XAuth — Les informations d'identification du client ne sont pas nécessaires. Le client authentifie la passerelle. Les informations d'identification se présentent 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 se présentent sous la forme de fichiers de certificat PEM ou PKCS12 ou de type de clé.
- PSK mutuel + XAuth - Le client et la passerelle ont tous deux besoin d'informations d'identification pour s'authentifier. Les informations d'identification prennent 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 se présentent sous la forme de fichiers de certificat PEM ou PKCS12 ou de type de clé.
- PSK mutuel : le client et la passerelle ont tous deux besoin d'informations d'identification pour s'authentifier. Les informations d'identification prennent la forme d'une chaîne secrète partagée.

Étape 10. Dans la section *Authentication*, cliquez sur le sous-onglet *Credentials* et entrez la

même clé pré-partagée que vous avez configurée sur la page *IPsec VPN Server Setup* dans le champ *Pre Shared Key*.



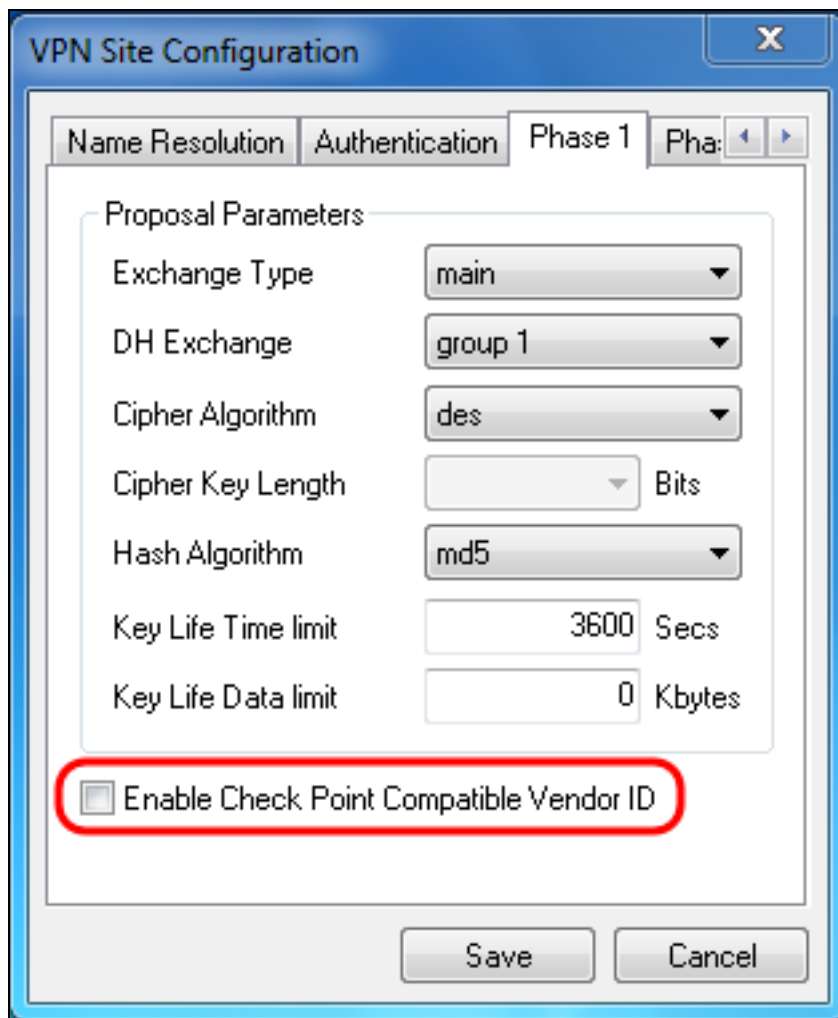
Étape 11. Cliquez sur l'onglet *Phase 1*. Configurez les paramètres suivants pour qu'ils soient identiques à ceux que vous avez configurés pour le RV130/RV130W à l'[étape 2 de la section Configuration utilisateur du serveur VPN IPsec](#) de ce document.



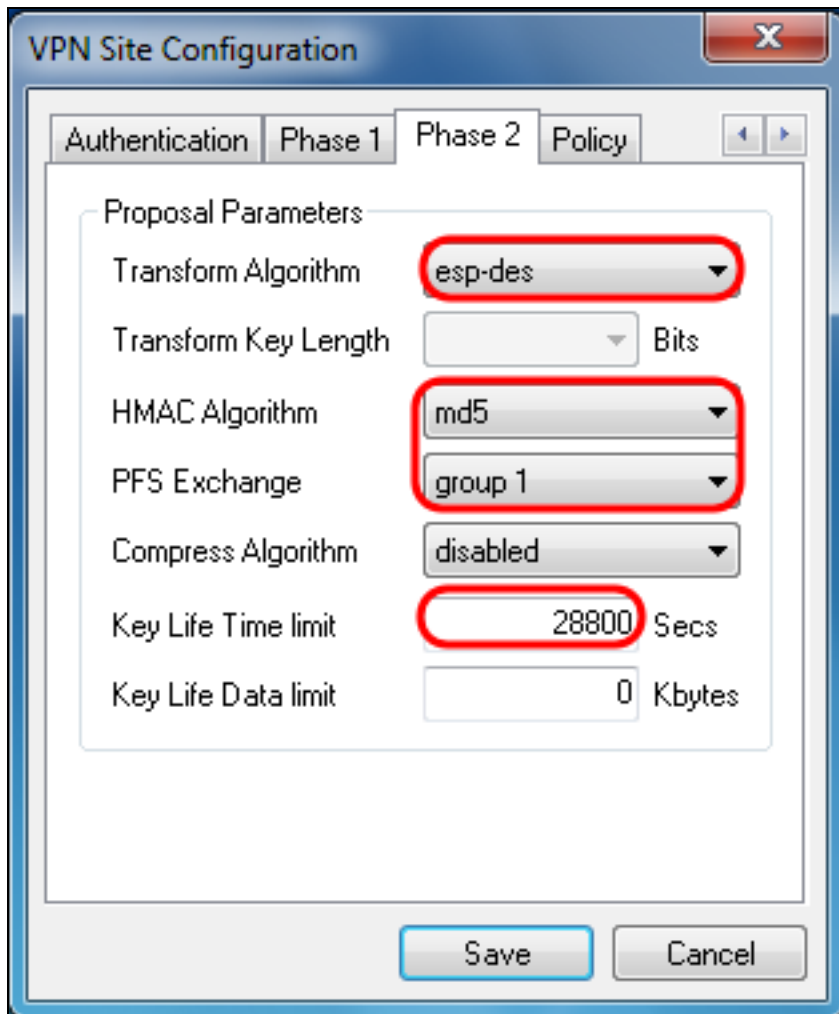
Les paramètres de Shrew Soft doivent correspondre aux configurations RV130/RV130W de la phase 1, comme suit :

- « Exchange Type » doit correspondre à « Exchange Mode ».
- « DH Exchange » doit correspondre à « DH Group ».
- « Algorithme de chiffrement » doit correspondre à « Algorithme de chiffrement ».
- « Hash Algorithm » doit correspondre à « Authentication Algorithm ».

Étape 12. (Facultatif) Si votre passerelle propose un ID fournisseur compatible Cisco lors des négociations de la phase 1, cochez la case **Enable Check Point Compatible Vendor ID**. Si la passerelle ne fonctionne pas ou si vous n'êtes pas sûr, ne cochez pas cette case.



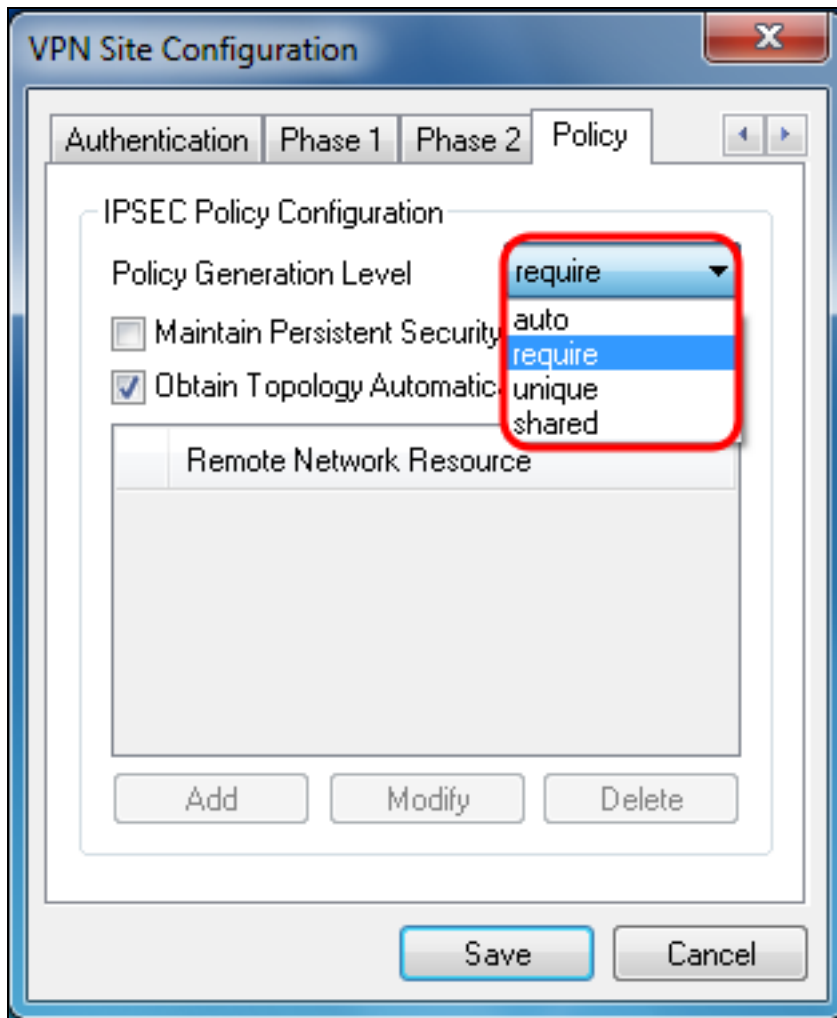
Étape 13. Cliquez sur l'onglet *Phase 2*. Configurez les paramètres suivants pour qu'ils soient identiques à ceux que vous avez configurés pour le RV130/RV130W à l'[étape 2 de la section Configuration utilisateur du serveur VPN IPSec](#) de ce document.



Les paramètres de Shrew Soft doivent correspondre aux configurations RV130/RV130W de la phase 2, comme suit :

- « Algorithme de transformation » doit correspondre à « Algorithme de chiffrement ».
- « Algorithme HMAC » doit correspondre à « Algorithme d'authentification ».
- « PFS Exchange » doit correspondre à « DH Group » si le groupe de clés PFS est activé sur le RV130/RV130W. Sinon, sélectionnez **disabled**.
- « Key Life Time limit » doit correspondre à « IPsec SA Lifetime ».

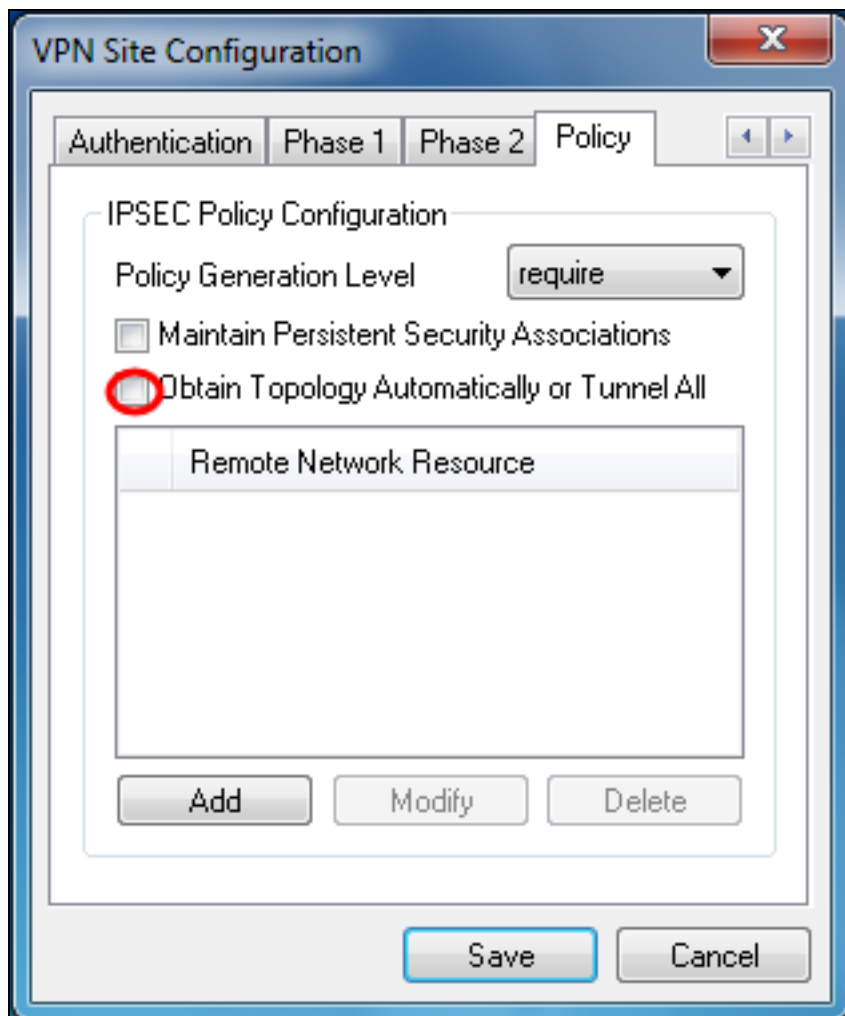
Étape 14. Cliquez sur l'onglet *Policy* et sélectionnez **require** dans la liste déroulante *Policy Generation Level*. L'option *Policy Generation Level* modifie le niveau dans lequel les stratégies IPsec sont générées. Les différents niveaux fournis dans la liste déroulante correspondent aux comportements de négociation de l'association de sécurité IPsec implémentés par différentes implémentations de fournisseurs.



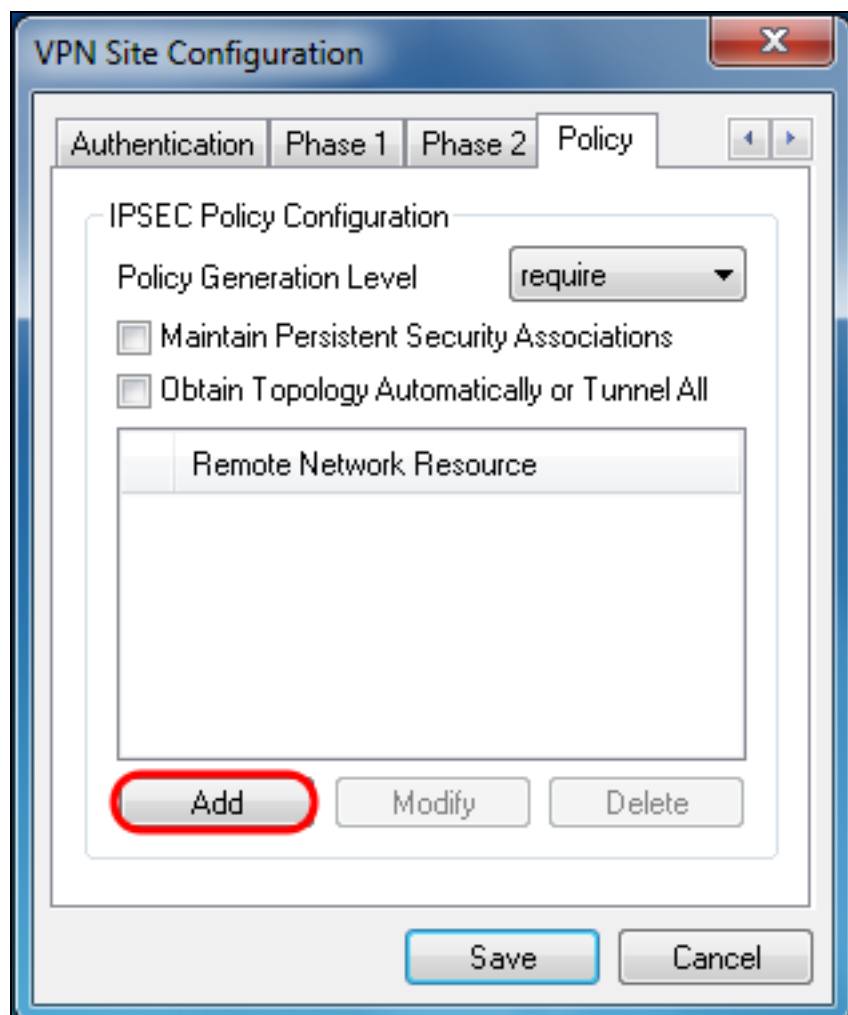
Les options disponibles sont définies comme suit :

- Auto : le client détermine automatiquement le niveau de stratégie IPsec approprié.
- Require : le client ne négociera pas une association de sécurité (SA) unique pour chaque stratégie. Les stratégies sont générées en utilisant l'adresse publique locale comme ID de stratégie locale et les ressources réseau distantes comme ID de stratégie distante. La proposition de phase2 utilise les ID de stratégie lors de la négociation.
- Unique : le client négociera une association de sécurité unique pour chaque stratégie.
- Partagé - Les politiques sont générées au niveau requis. La proposition de phase 2 utilise l'ID de stratégie locale comme ID local et Any (0.0.0.0/0) comme ID distant pendant la négociation.

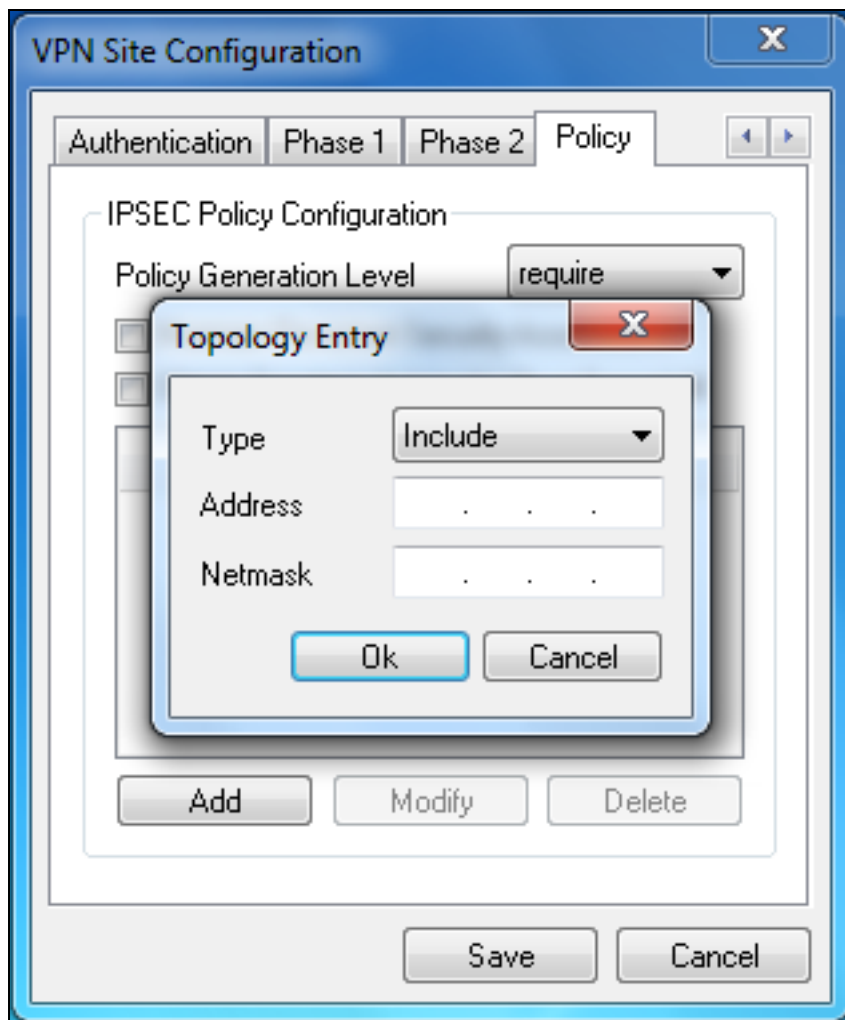
Étape 15. Désactivez la case à cocher **Obtenir la topologie automatiquement ou Tunnel All**. Cette option modifie la configuration des stratégies de sécurité pour la connexion. Une fois désactivée, la configuration manuelle doit être effectuée. Lorsque cette option est activée, la configuration automatique est effectuée.



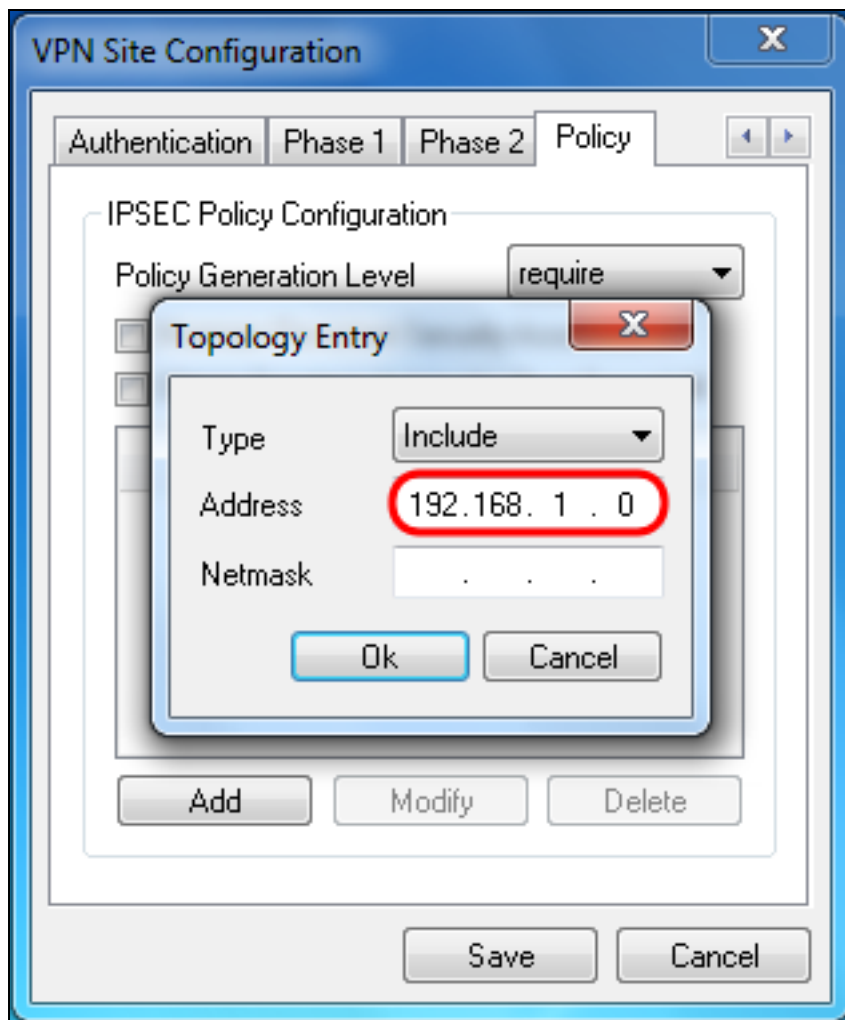
Étape 16. Cliquez sur **Add** afin d'ajouter la ressource de réseau distant à laquelle vous voulez vous connecter. Les ressources réseau distantes incluent l'accès à distance au bureau, les ressources de service, les lecteurs réseau et le courrier électronique sécurisé.



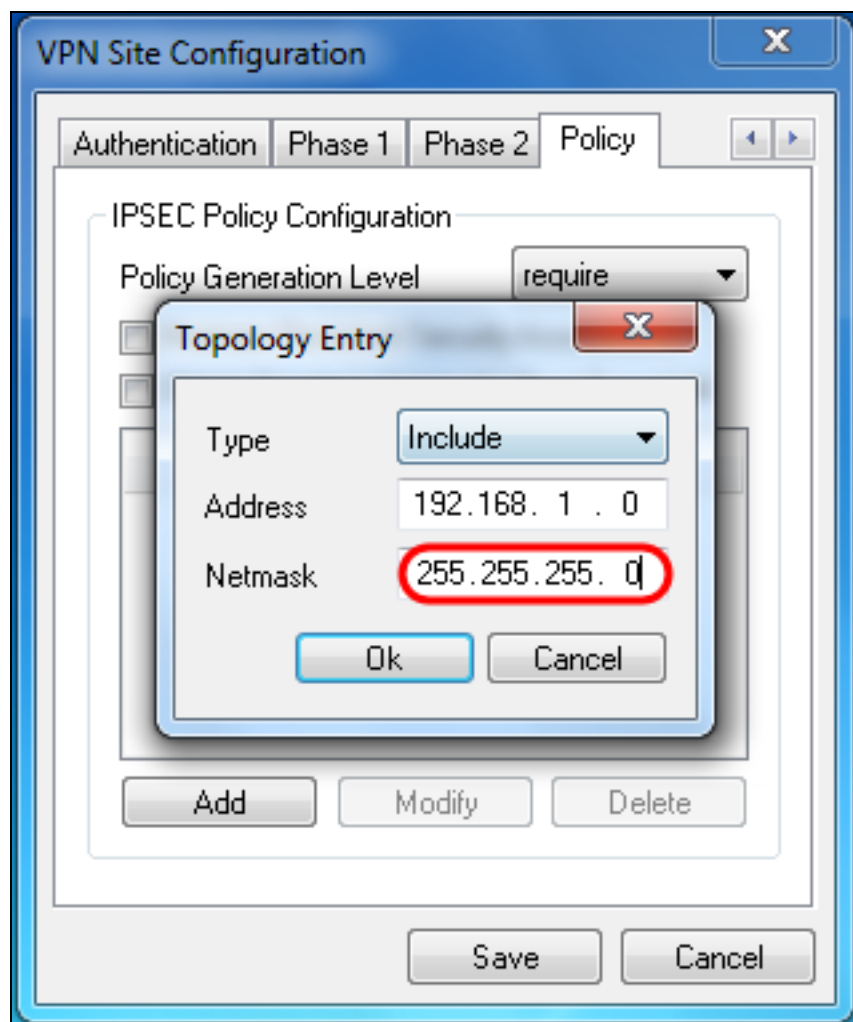
La fenêtre *Topology Entry* s'affiche :



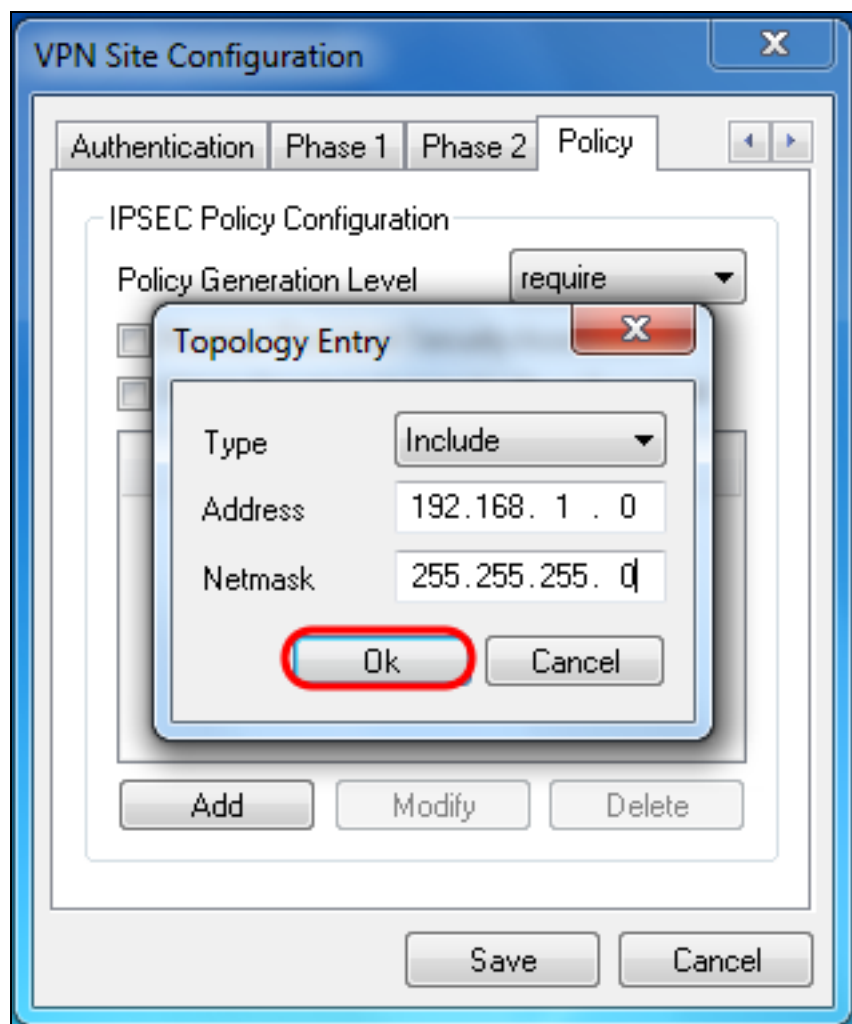
Étape 17. Dans le champ *Address*, entrez l'ID de sous-réseau du routeur RV130/RV130W. L'adresse doit correspondre au champ *IP Address* à l'[étape 2 de la section *IPSec VPN Server Setup and User Configuration*](#) de ce document.



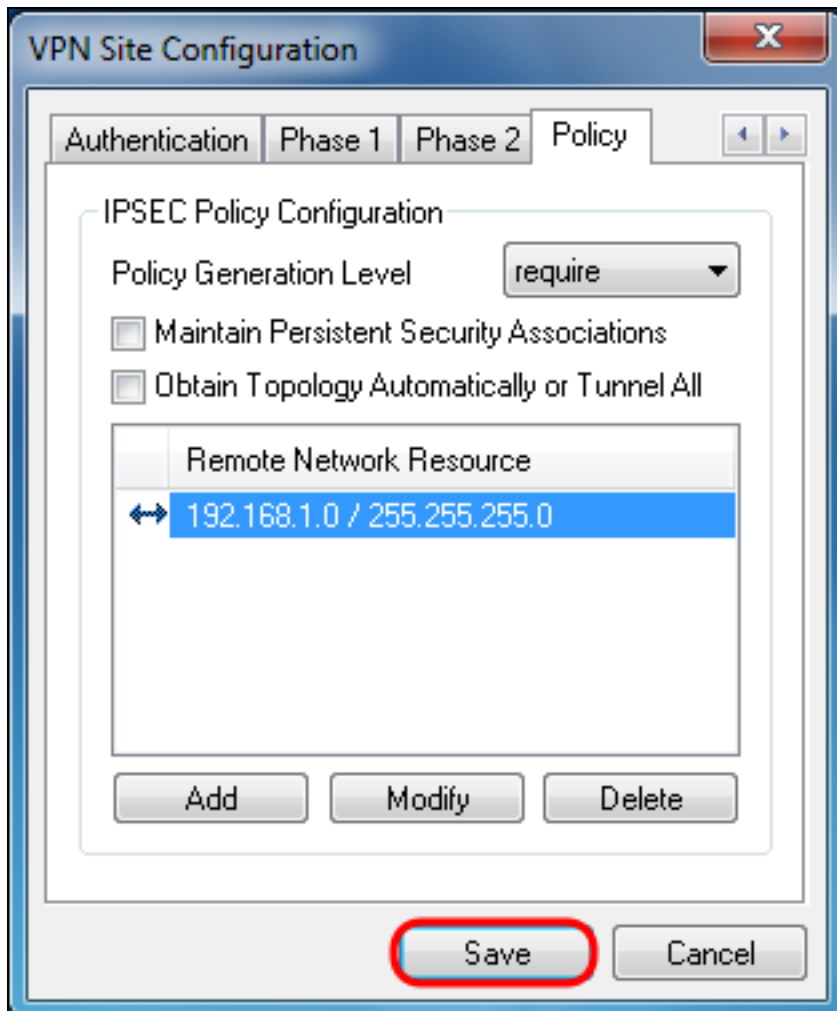
Étape 18. Dans le champ *Netmask*, entrez le masque de sous-réseau du réseau local du routeur RV130/RV130W. Le masque de réseau doit correspondre au champ *Subnet Mask* de l'[étape 2 de la](#) section [IPSec VPN Server User Configuration](#) de ce document.



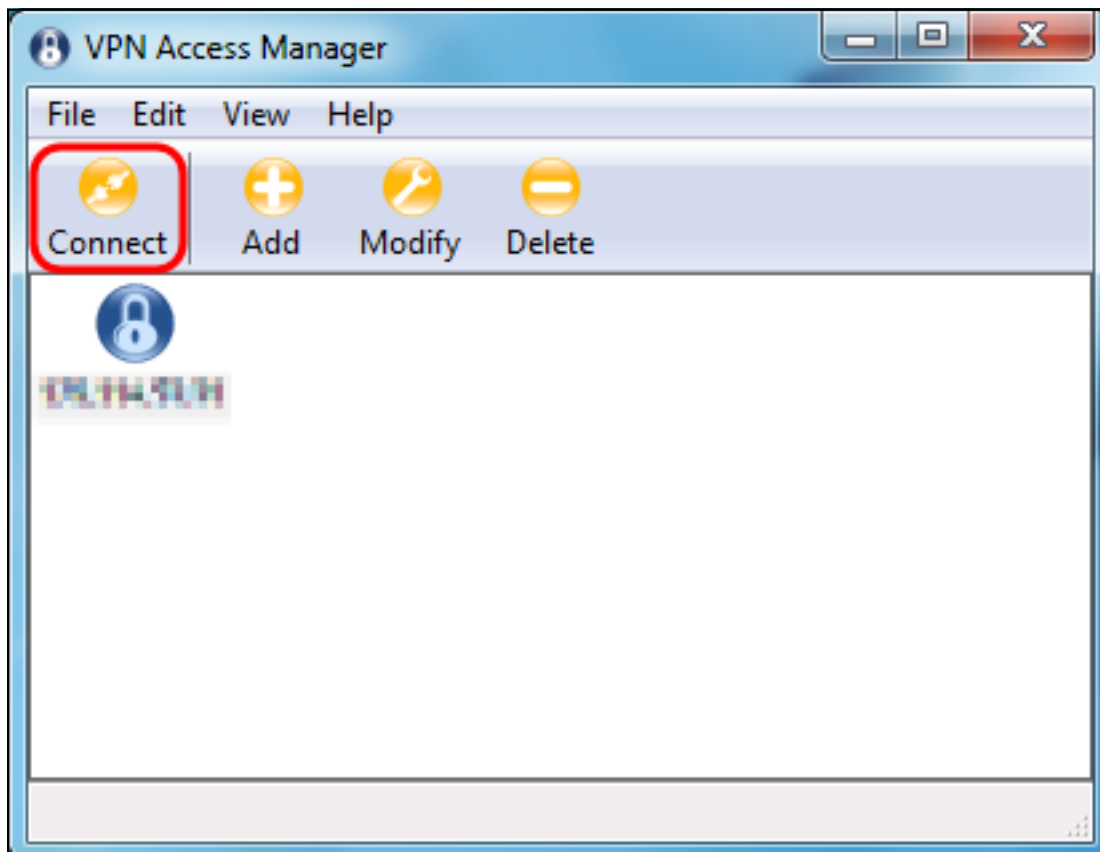
Étape 19. Cliquez sur **Ok** pour terminer l'ajout de la ressource de réseau distant.



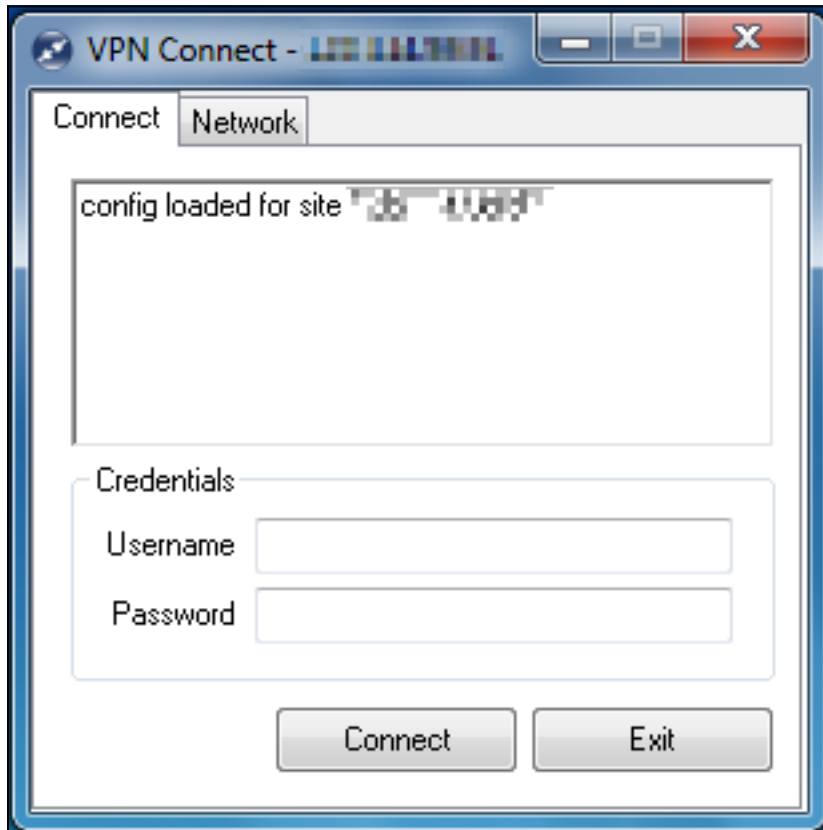
Étape 20. Cliquez sur **Save** pour enregistrer vos configurations pour vous connecter au site VPN.



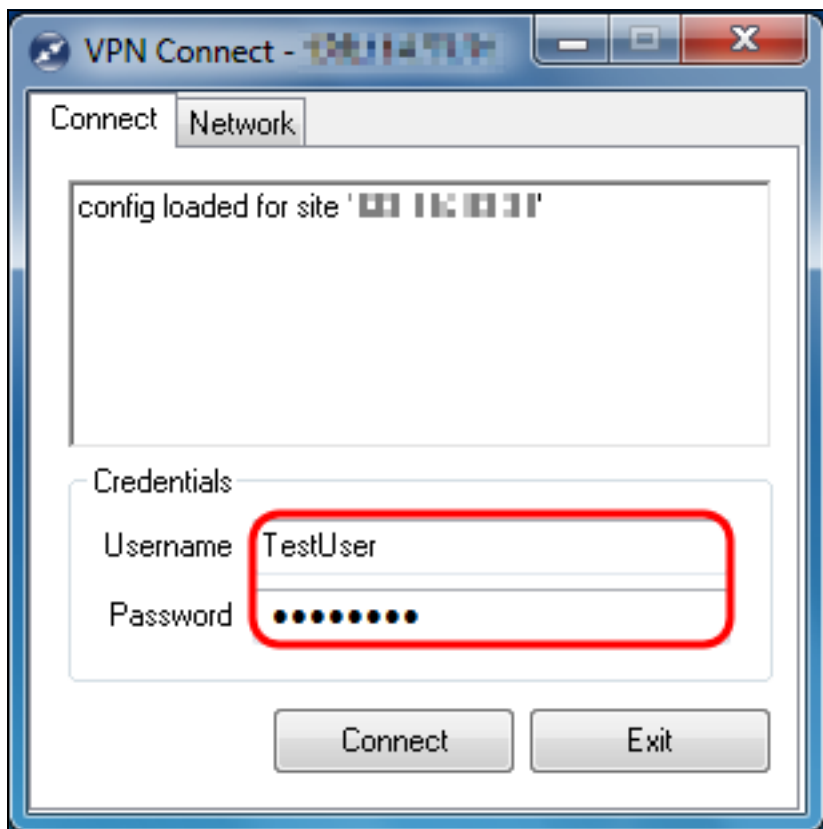
Étape 21. Revenez à la fenêtre *VPN Access Manager* pour sélectionner le site VPN que vous avez configuré, et cliquez sur le bouton **Connect**.



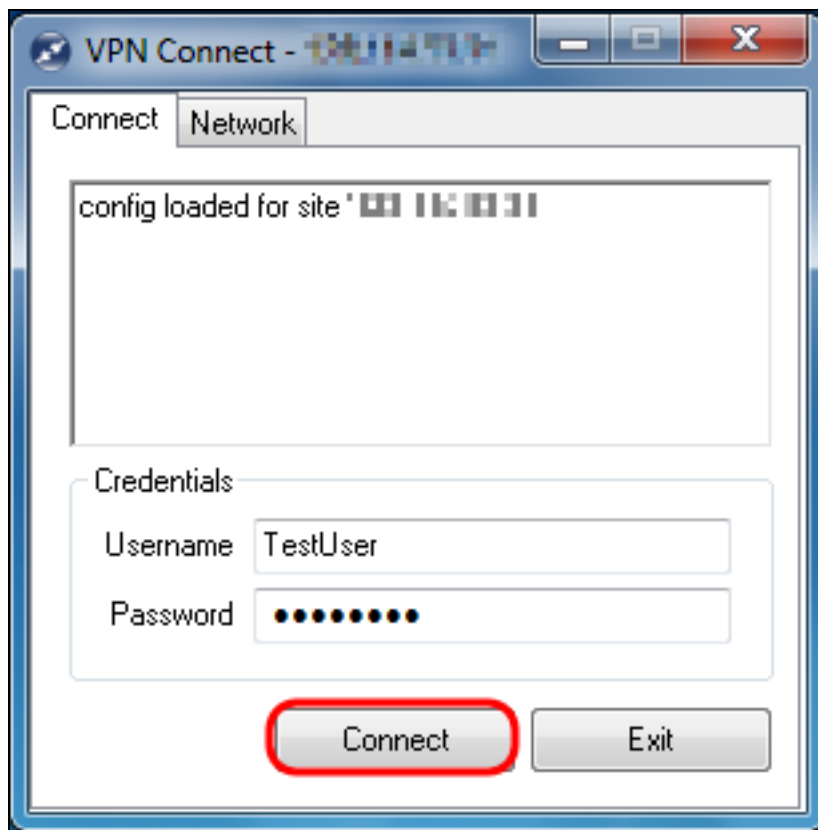
La fenêtre *VPN Connect* s'affiche.



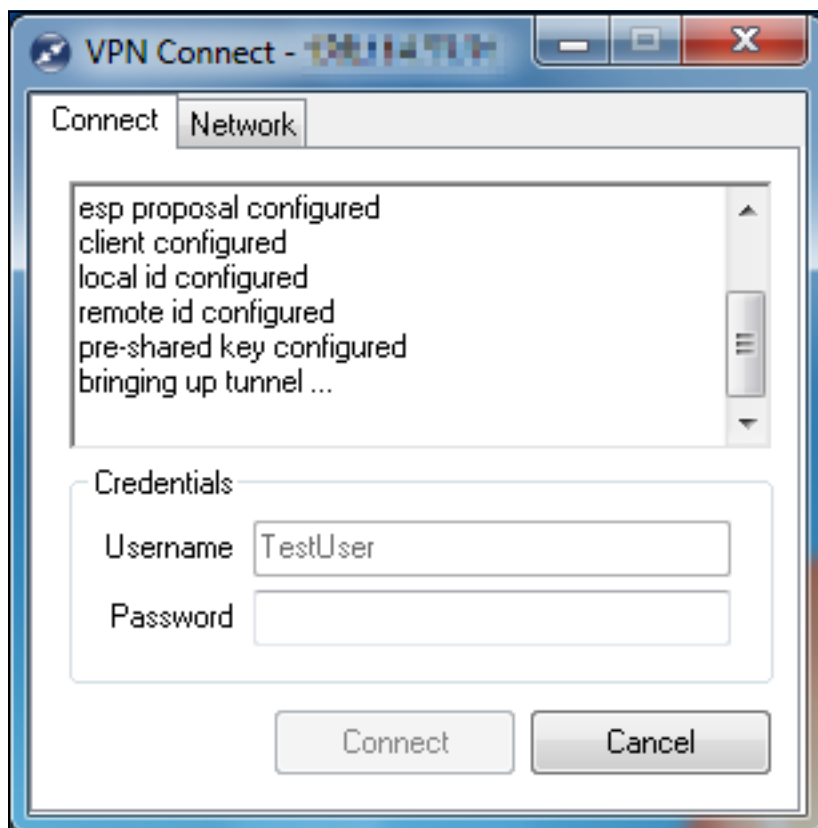
Étape 22. Dans la section *Credentials*, entrez le nom d'utilisateur et le mot de passe du compte que vous avez configuré à l'[étape 4 de la section IPsec VPN Server User Configuration](#) de ce document.

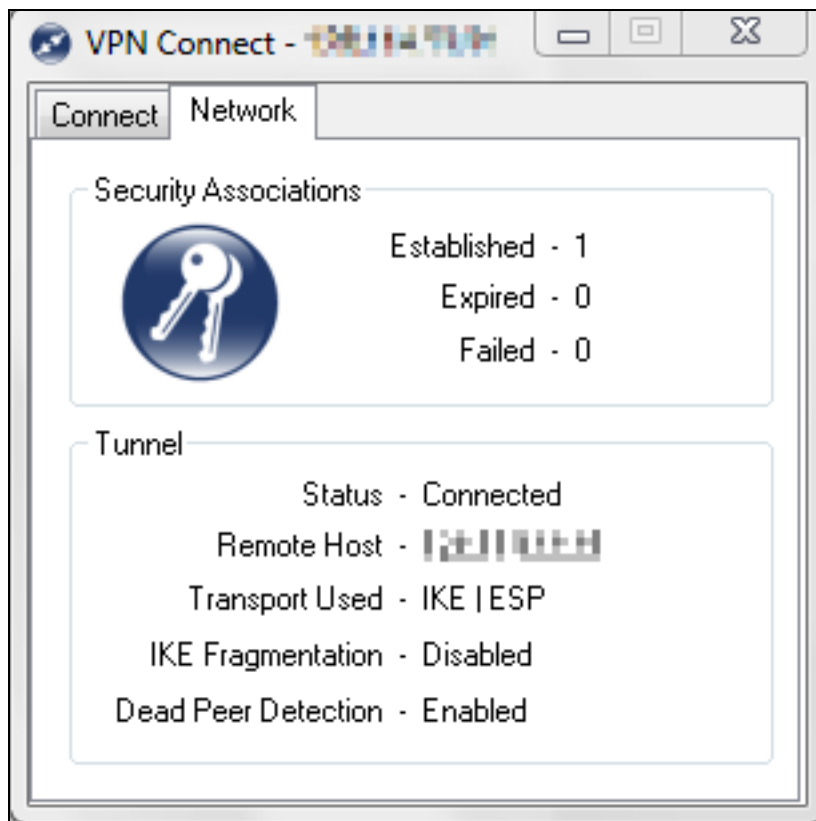


Étape 23. Cliquez sur **Connect** to VPN into the RV130/RV130W.



Le tunnel VPN IPsec est établi et le client VPN peut accéder à la ressource derrière le LAN RV130/RV130W.





[Voir une vidéo liée à cet article...](#)

[Cliquez ici pour afficher d'autres présentations techniques 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.