Configuration du client VPN Shrew sur les routeurs VPN RV042, RV042G et RV082 via Windows

Objectif

Un réseau privé virtuel (VPN) est une méthode permettant aux utilisateurs distants de se connecter virtuellement à un réseau privé sur Internet. Un VPN Client to Gateway connecte le bureau ou l'ordinateur portable d'un utilisateur à un réseau distant à l'aide d'un logiciel client VPN. Les connexions VPN de client à passerelle sont utiles pour les employés distants qui souhaitent se connecter en toute sécurité au réseau du bureau à distance. Shrew VPN Client est un logiciel configuré sur un périphérique hôte distant qui fournit une connectivité VPN facile et sécurisée.

L'objectif de ce document est de vous montrer comment configurer Shrew VPN Client pour un ordinateur qui se connecte à un routeur VPN RV042, RV042G ou RV082.

Remarque : ce document suppose que vous avez déjà téléchargé le client VPN Shrew sur l'ordinateur Windows. Sinon, vous devez configurer une connexion VPN client-passerelle avant de pouvoir commencer à configurer le VPN Shrew. Pour en savoir plus sur la façon de configurer le VPN client-passerelle, référez-vous à Configurer un tunnel d'accès à distance (client-passerelle) pour les clients VPN sur les routeurs VPN RV042, RV042G et RV082.

Périphériques pertinents

- RV042
- RV042G
- RV082

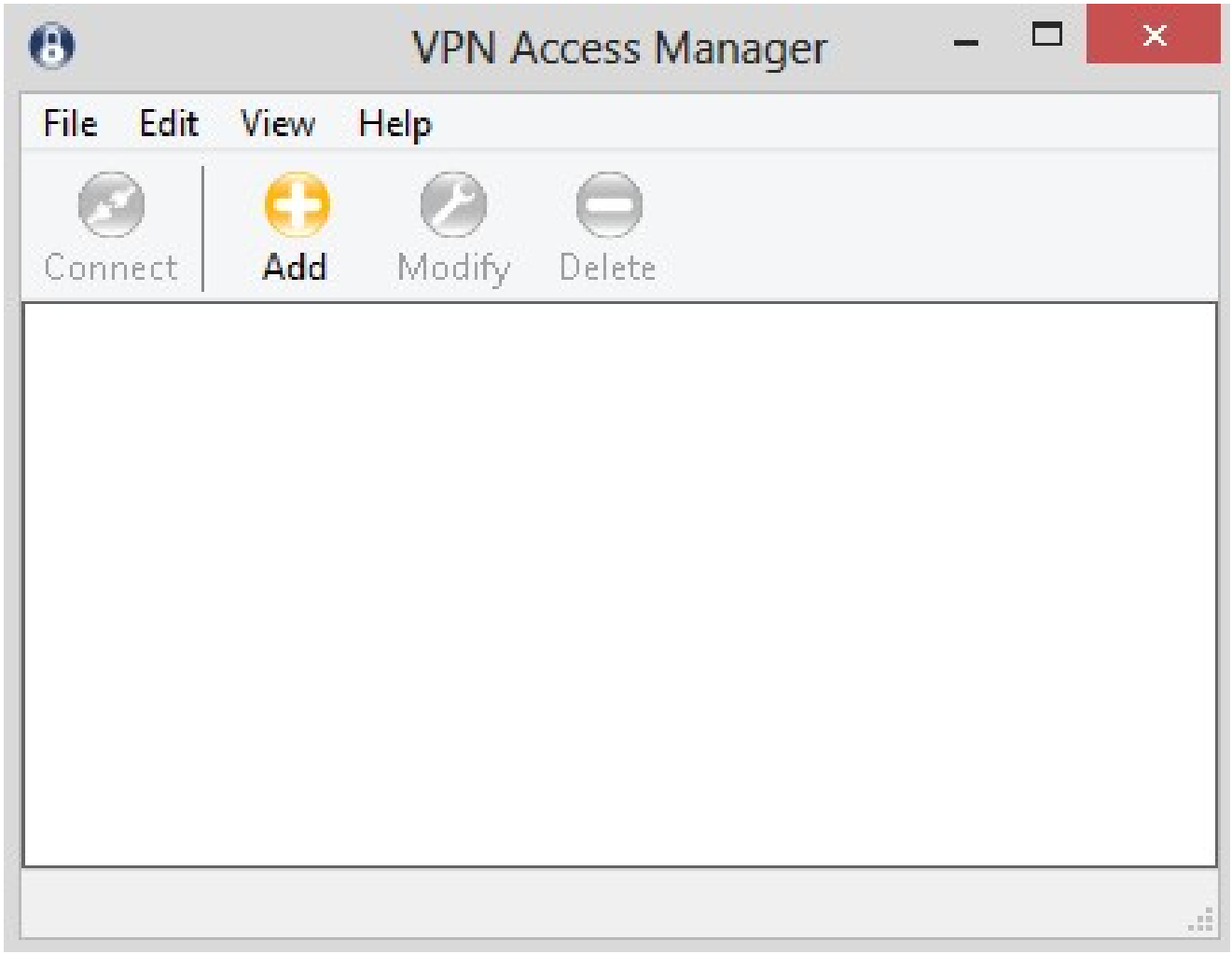
Version du logiciel

- v 4.2.2.08

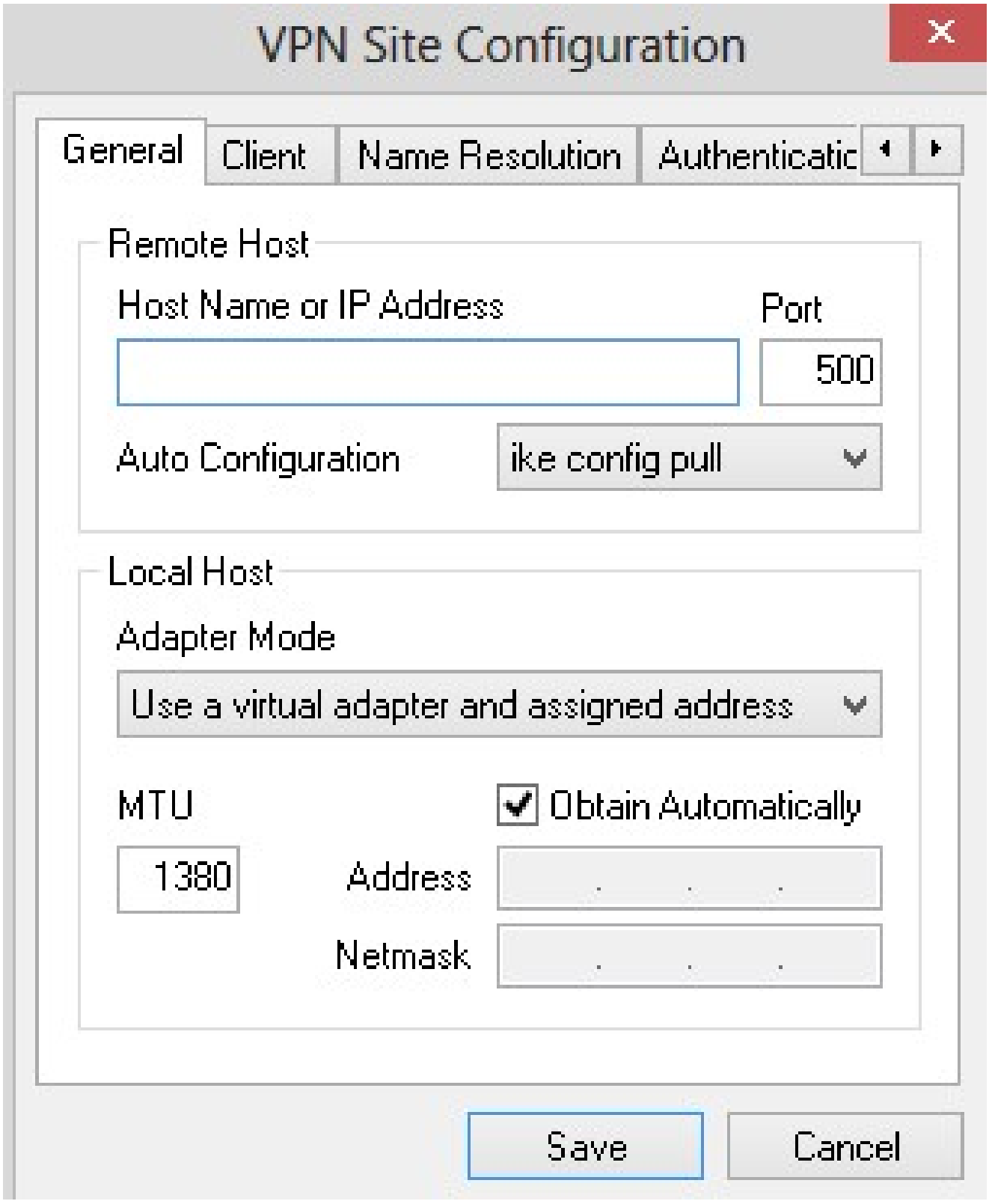
Configuration de la connexion du client VPN Shrew sous

Windows

Étape 1. Cliquez sur le programme Shrew VPN Client sur l'ordinateur et ouvrez-le. La fenêtre Shrew Soft VPN Access Manager s'ouvre :

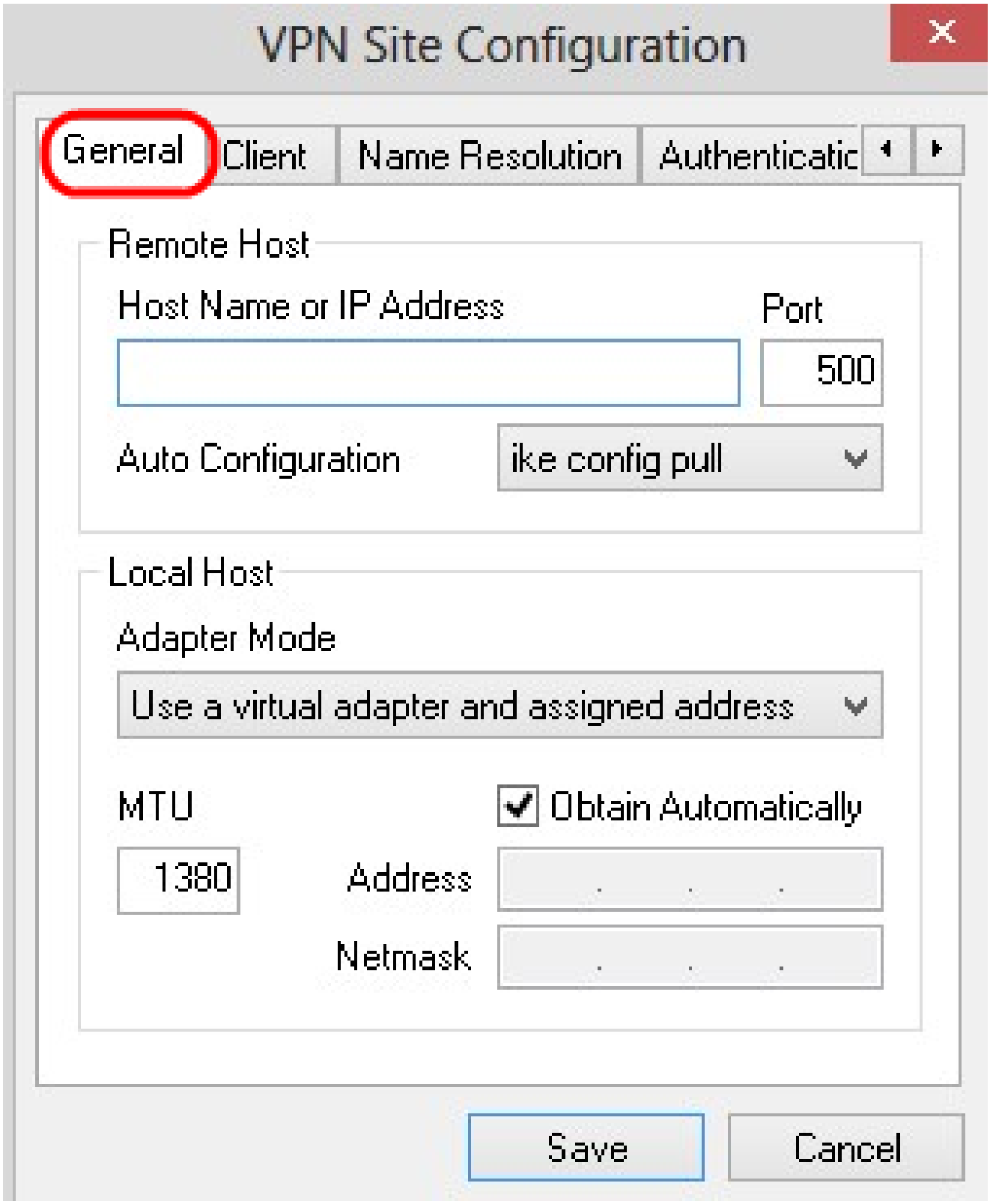


Étape 2. Cliquez sur Add. La fenêtre VPN Site Configuration s'affiche :



Configuration générale

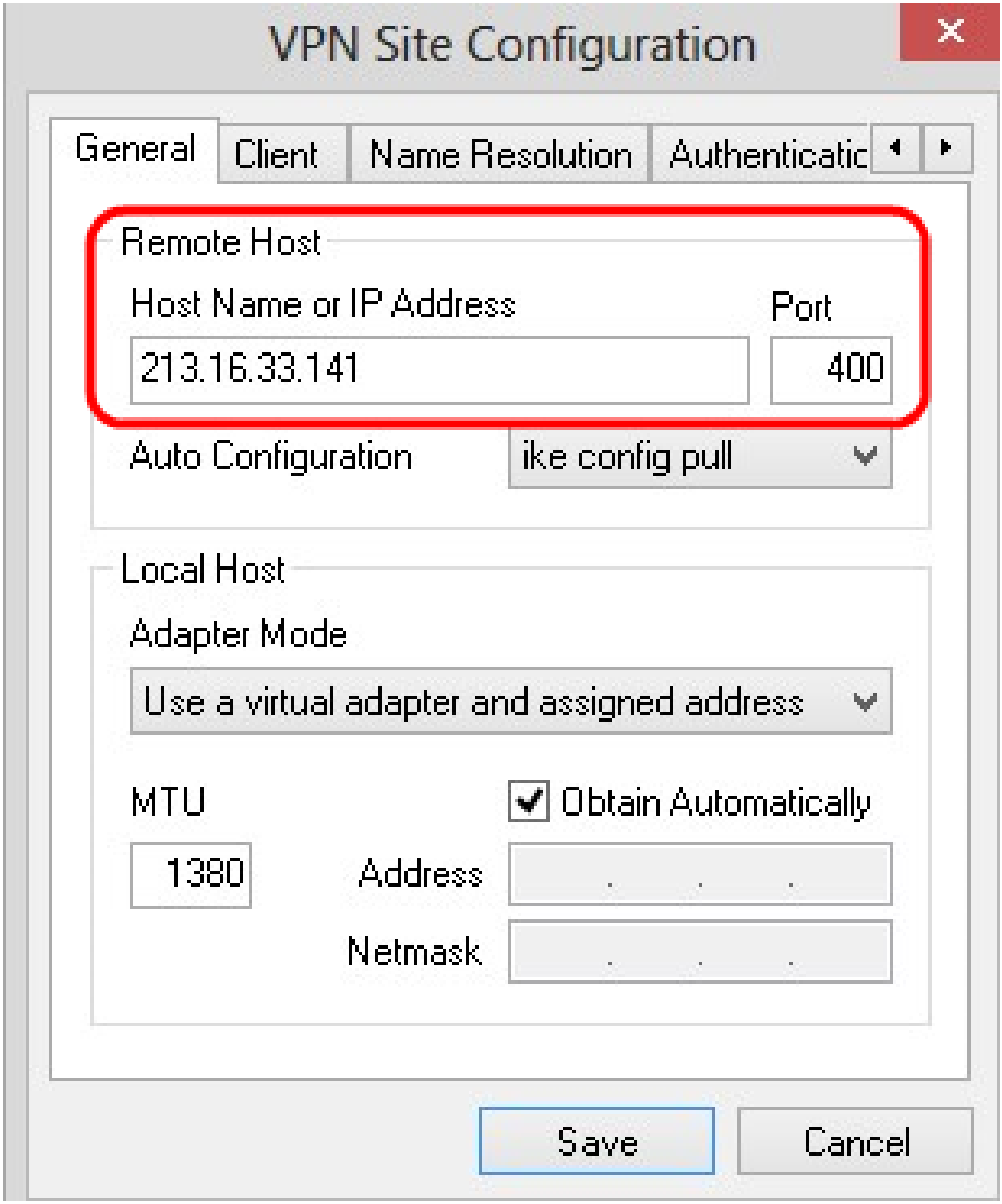
Étape 1. Cliquez sur l’onglet General (Général).



Remarque : la section Général est utilisée pour configurer les adresses IP des hôtes distants et locaux. Ils servent à définir les paramètres réseau de la connexion du client à la passerelle.

Étape 2. Dans le champ Host Name or IP Address, entrez l'adresse IP de l'hôte distant, qui est l'adresse IP du WAN configuré.

Étape 3. Dans le champ Port, saisissez le numéro du port à utiliser pour la connexion. Le numéro de port utilisé dans l'exemple illustré est 400.



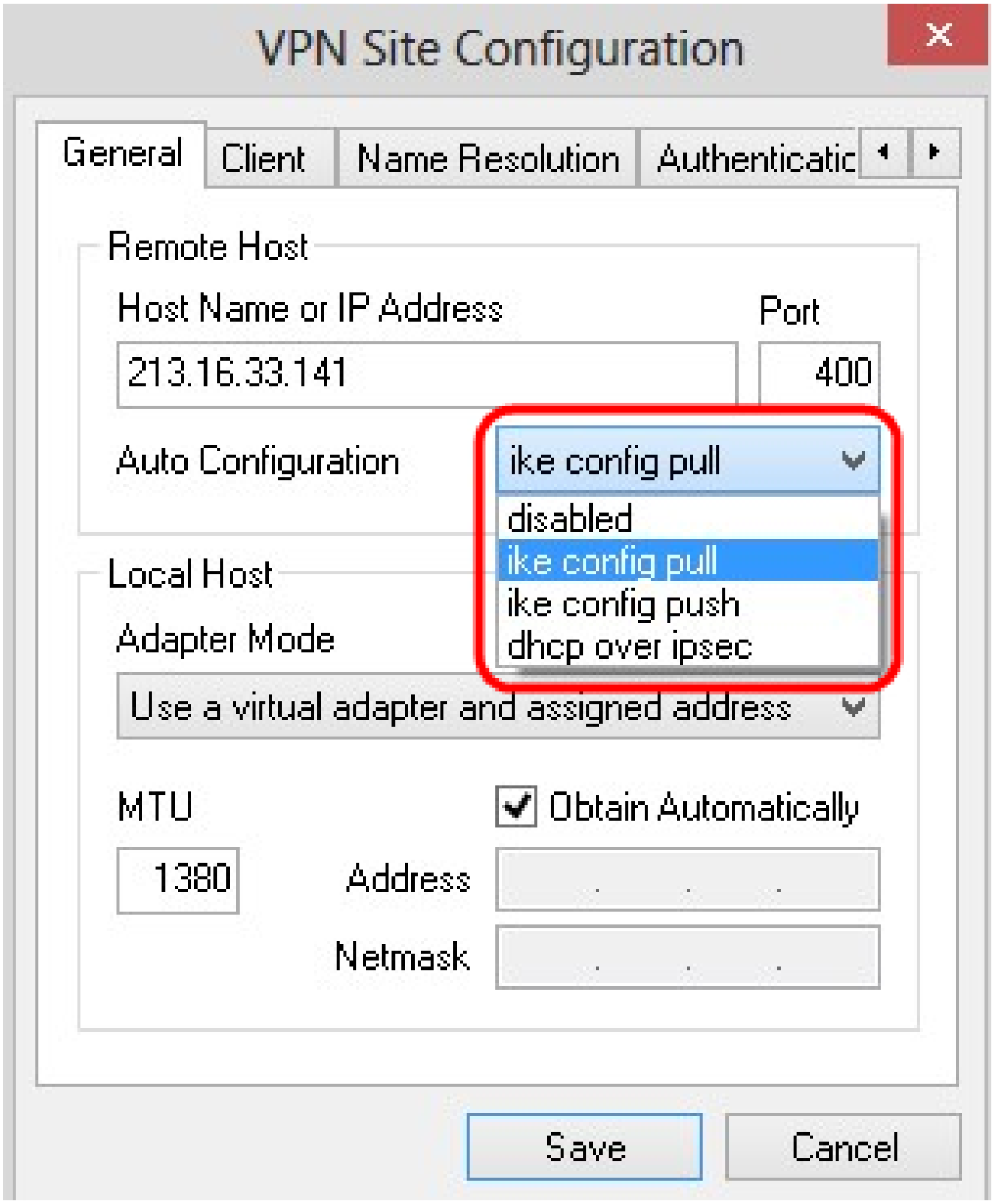
Étape 4. Dans la liste déroulante Auto Configuration, sélectionnez la configuration souhaitée.

· Disabled : l'option 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.

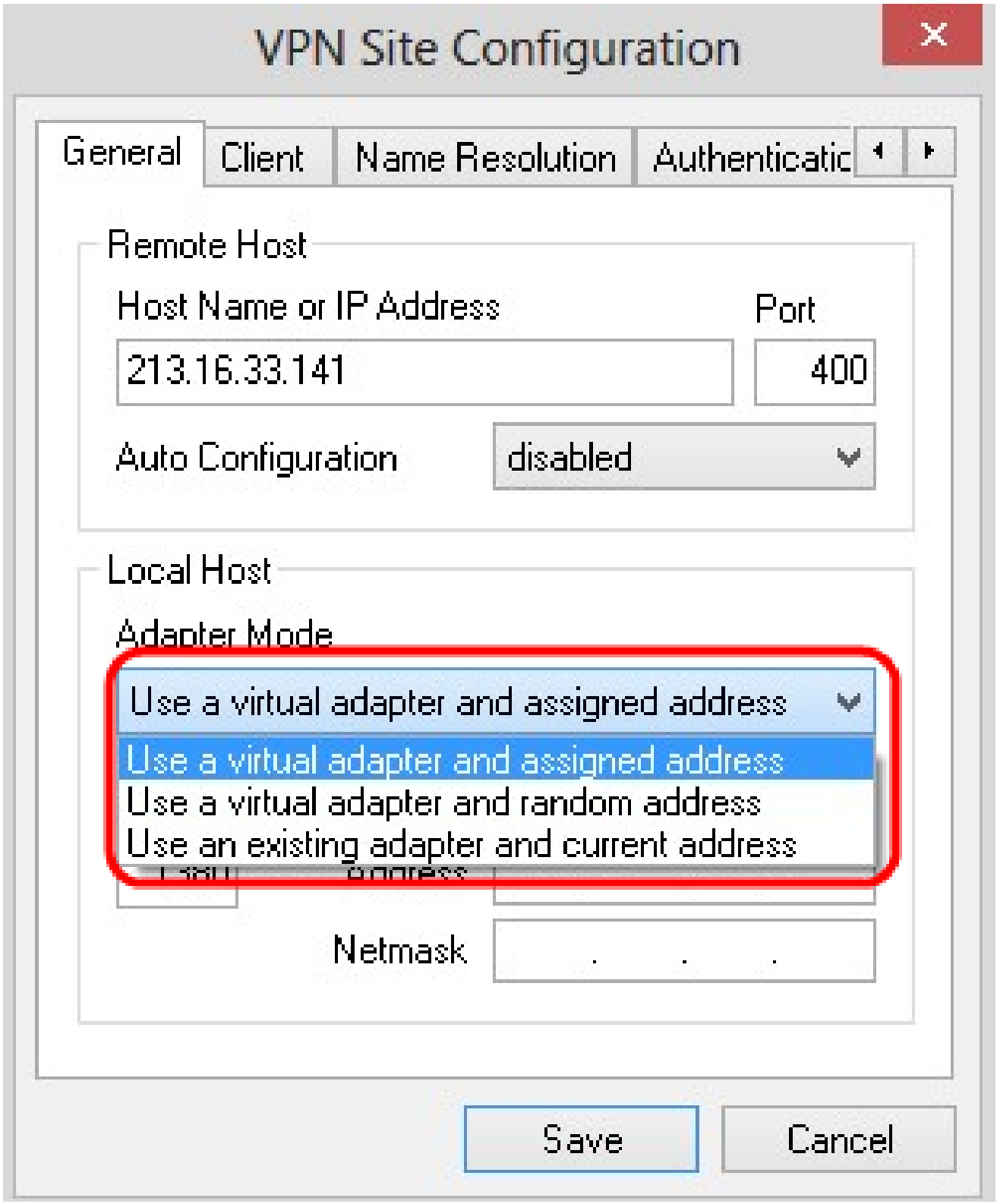


Étape 5. Dans la liste déroulante Adapter Mode, sélectionnez le mode de carte souhaité pour l'hôte local en fonction de la configuration automatique.

· Use a Virtual Adapter and Assigned Address : permet au client d'utiliser une carte virtuelle avec une adresse spécifiée.

· Use a Virtual Adapter and Random Address : permet au client d'utiliser une carte virtuelle avec une adresse aléatoire.

· Use an Existing Adapter and Current Address : utilise une carte existante et son adresse. Aucune information supplémentaire ne doit être saisie.

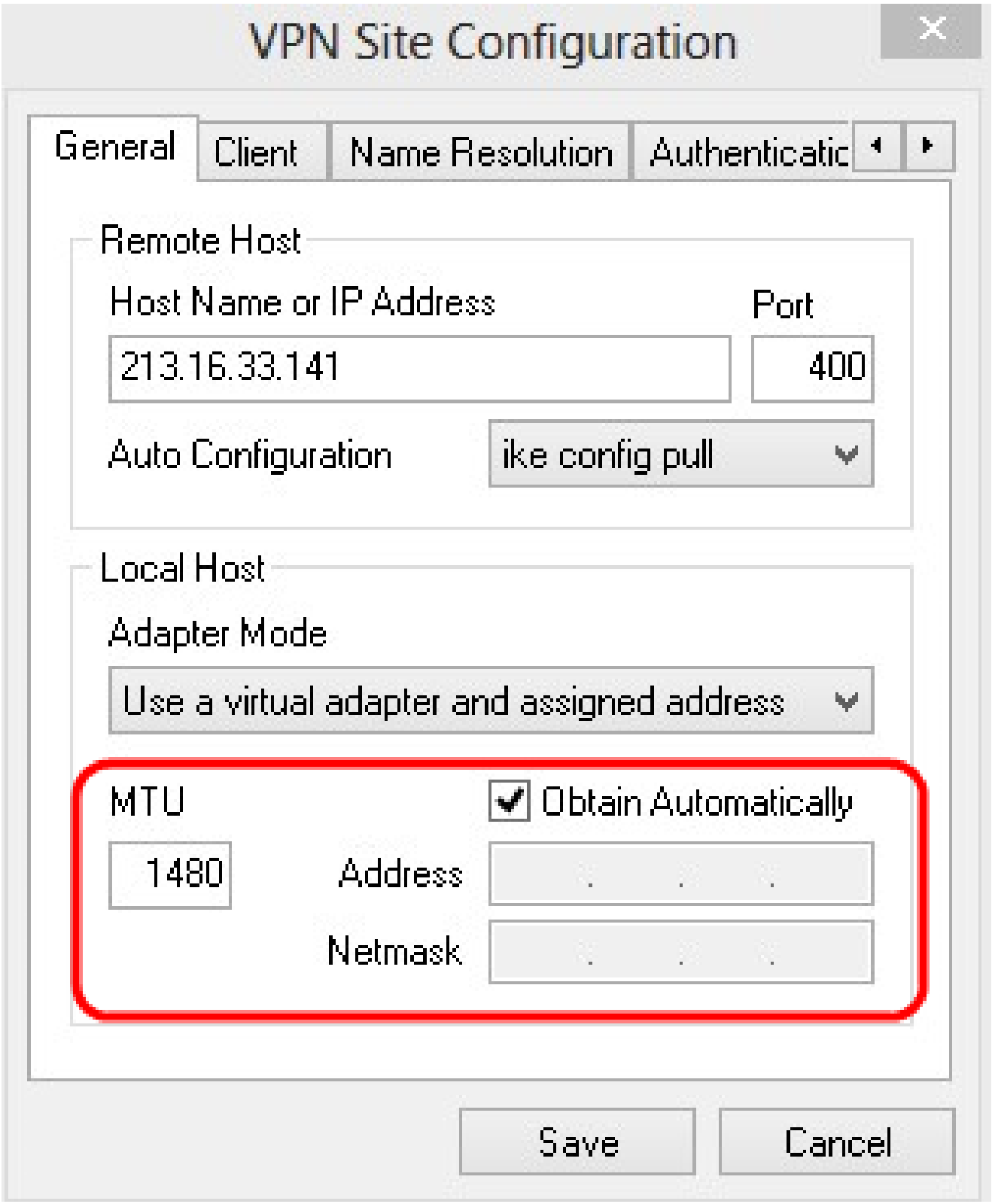


Étape 6. Saisissez l'unité de transmission maximale (MTU) dans le champ MTU si vous avez sélectionné Use a Virtual Adapter and Assigned Address dans la liste déroulante Adapter Mode à l'étape 5. L'unité de transmission maximale permet de résoudre les problèmes de fragmentation IP. La valeur par défaut est 1380.

Étape 7. (Facultatif) Pour obtenir l’adresse et le masque de sous-réseau automatiquement via le serveur DHCP, cochez la case Obtain Automatically. Cette option n'est pas disponible pour toutes les configurations.

Étape 8. Saisissez l'adresse IP du client distant dans le champ Address si vous avez choisi Use a Virtual Adapter and Assigned Address dans la liste déroulante Adapter Mode à l'étape 5.

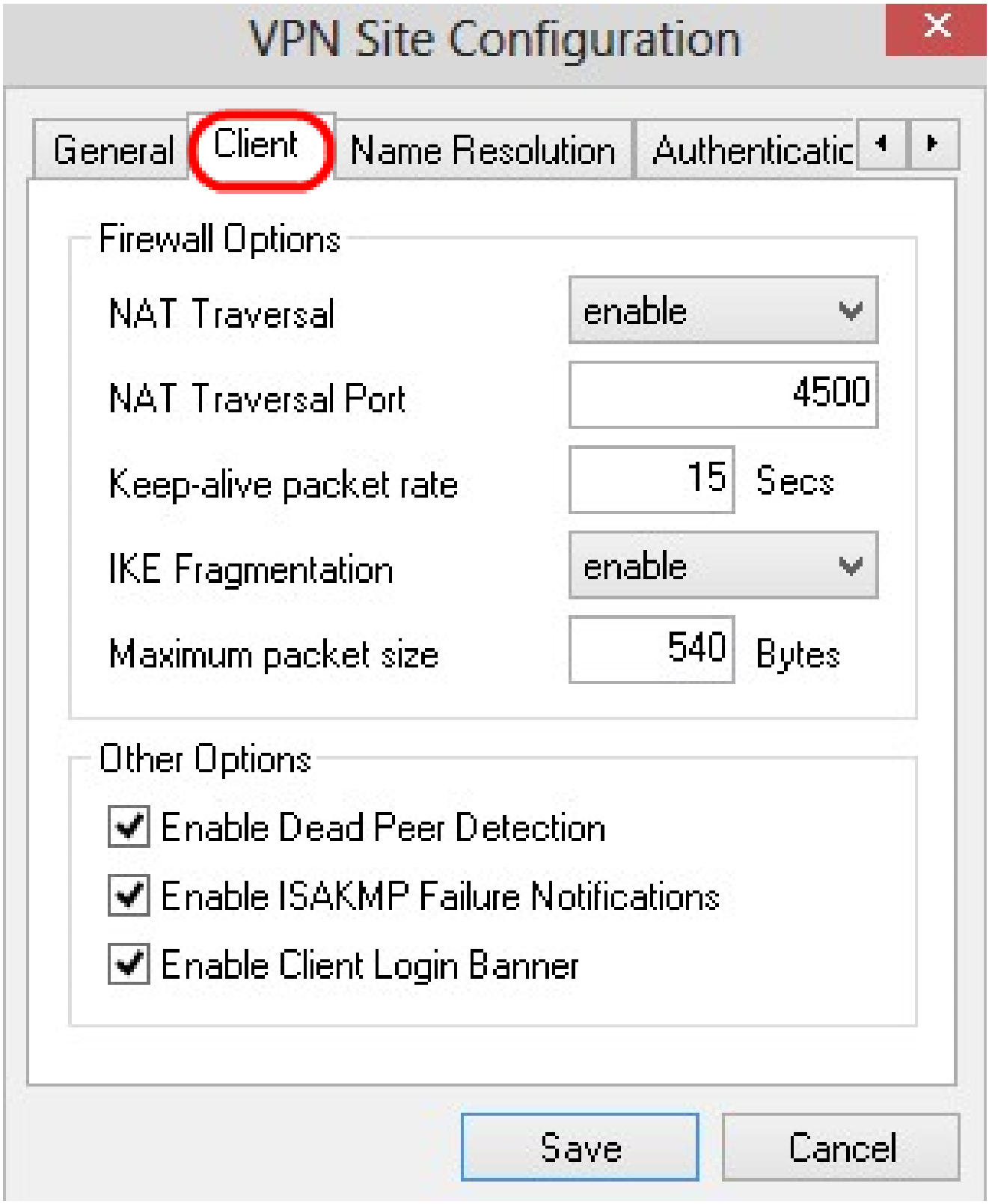
Étape 9. Entrez le masque de sous-réseau de l'adresse IP du client distant dans le champ Netmask si vous avez choisi Use a Virtual Adapter and Assigned Address dans la liste déroulante Adapter Mode à l'étape 5.



Étape 10. Cliquez sur Save pour enregistrer les paramètres.

Configuration du client

Étape 1. Cliquez sur l'onglet Client.



Remarque : dans la section Client, vous pouvez configurer les options de pare-feu, Dead Peer Detection et ISAKMP (Internet Security Association and Key Management Protocol) Failure Notifications. Les paramètres définissent les options de configuration qui sont configurées manuellement et celles qui sont obtenues automatiquement.

Étape 2. Choisissez l'option de traversée NAT (Network Address Translation) appropriée

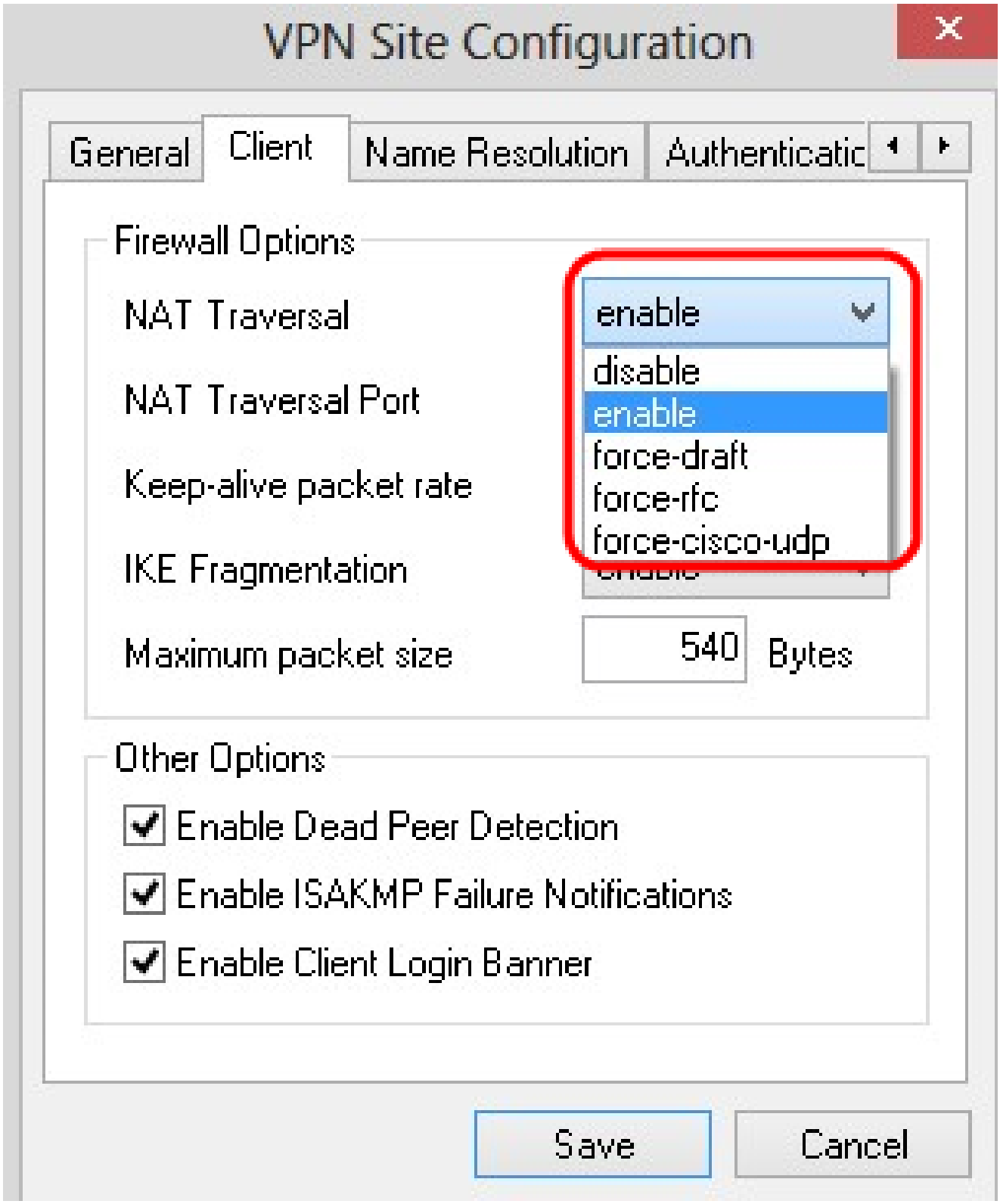
dans la liste déroulante NAT Traversal.

· Disable : le protocole NAT est désactivé.

· Enable : la fragmentation IKE n'est utilisée que si la passerelle indique la prise en charge par le biais de négociations.

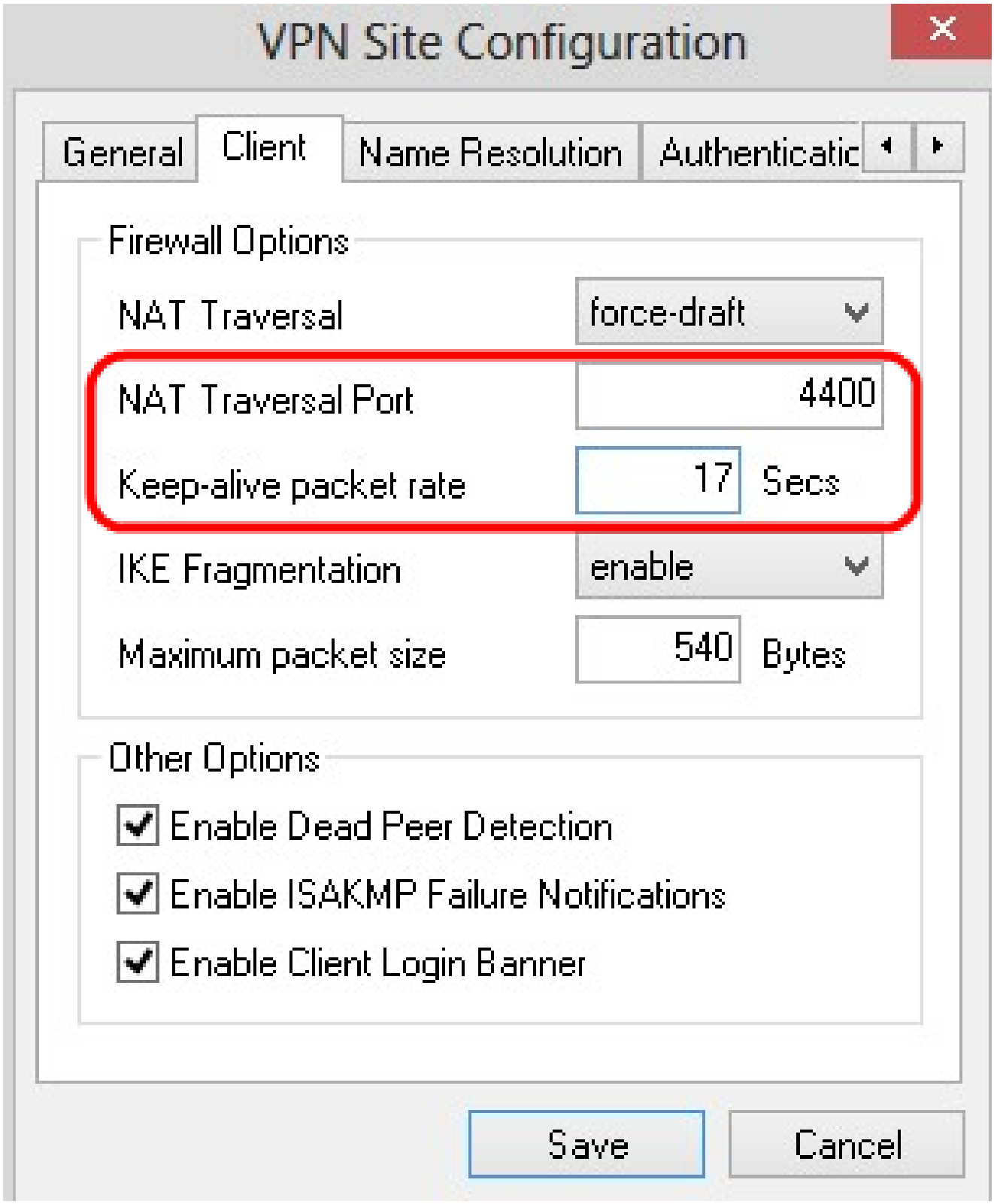
· Force Draft : version préliminaire du protocole NAT. Elle est utilisée si la passerelle indique la prise en charge par la négociation ou la détection de la NAT.

· Force RFC : version RFC du protocole NAT. Elle est utilisée si la passerelle indique la prise en charge par la négociation ou la détection de la NAT.



Étape 3. Saisissez le port UDP de la NAT dans le champ NAT Traversal Port. La valeur par défaut est 4500.

Étape 4. Dans le champ Taux de paquets de maintien de la connexion, entrez une valeur pour le taux auquel les paquets de maintien de la connexion sont envoyés. La valeur est mesurée en secondes. La valeur par défaut est de 30 secondes.

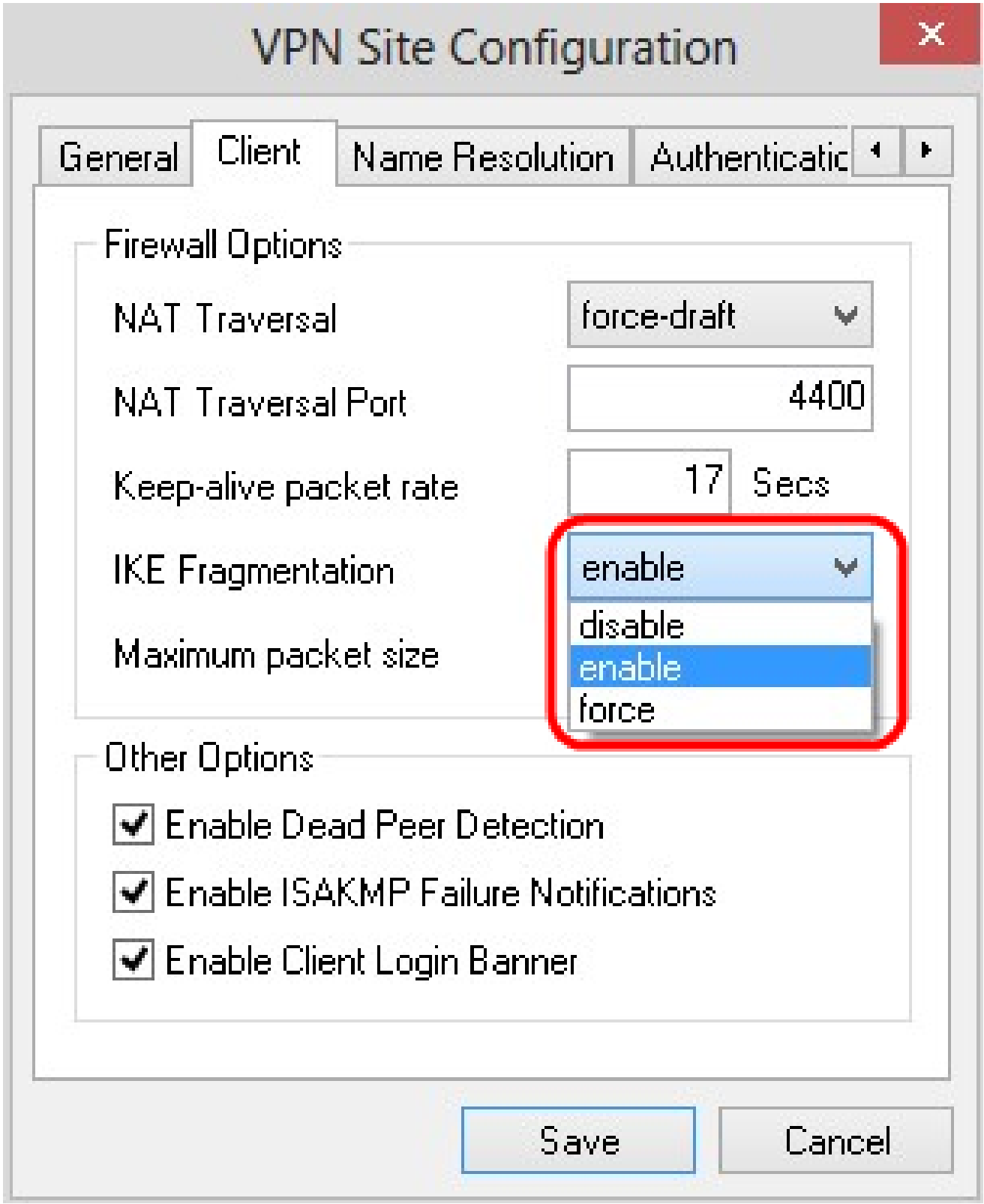


Étape 5. Dans la liste déroulante Fragmentation IKE, sélectionnez l'option appropriée.

· Disable : la fragmentation IKE n'est pas utilisée.

· Enable : la fragmentation IKE n'est utilisée que si la passerelle indique la prise en charge par le biais de négociations.

· Force : la fragmentation IKE est utilisée indépendamment des indications ou de la détection.

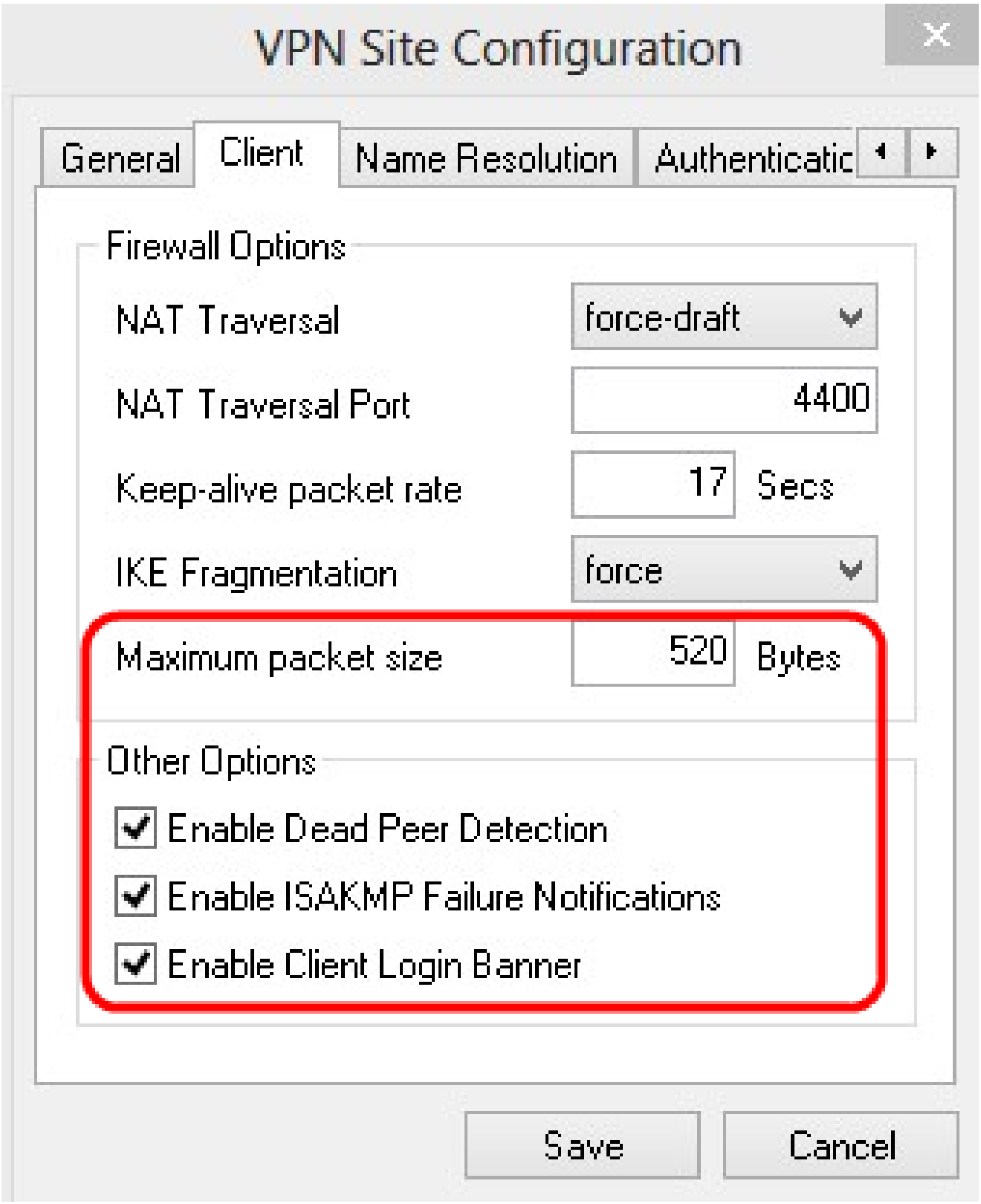


Étape 6. Entrez la taille maximale du paquet dans le champ Taille maximale du paquet en octets. Si la taille du paquet est supérieure à la taille maximale, la fragmentation IKE est effectuée. La valeur par défaut est 540 octets.

Étape 7. (Facultatif) Pour permettre à l’ordinateur et au client de détecter si l’autre n’est plus en mesure de répondre, cochez la case Enable Dead Peer Detection.

Étape 8. (Facultatif) Pour envoyer des notifications d’échec par le client VPN, cochez la case Enable ISAKMP Failure Notifications.

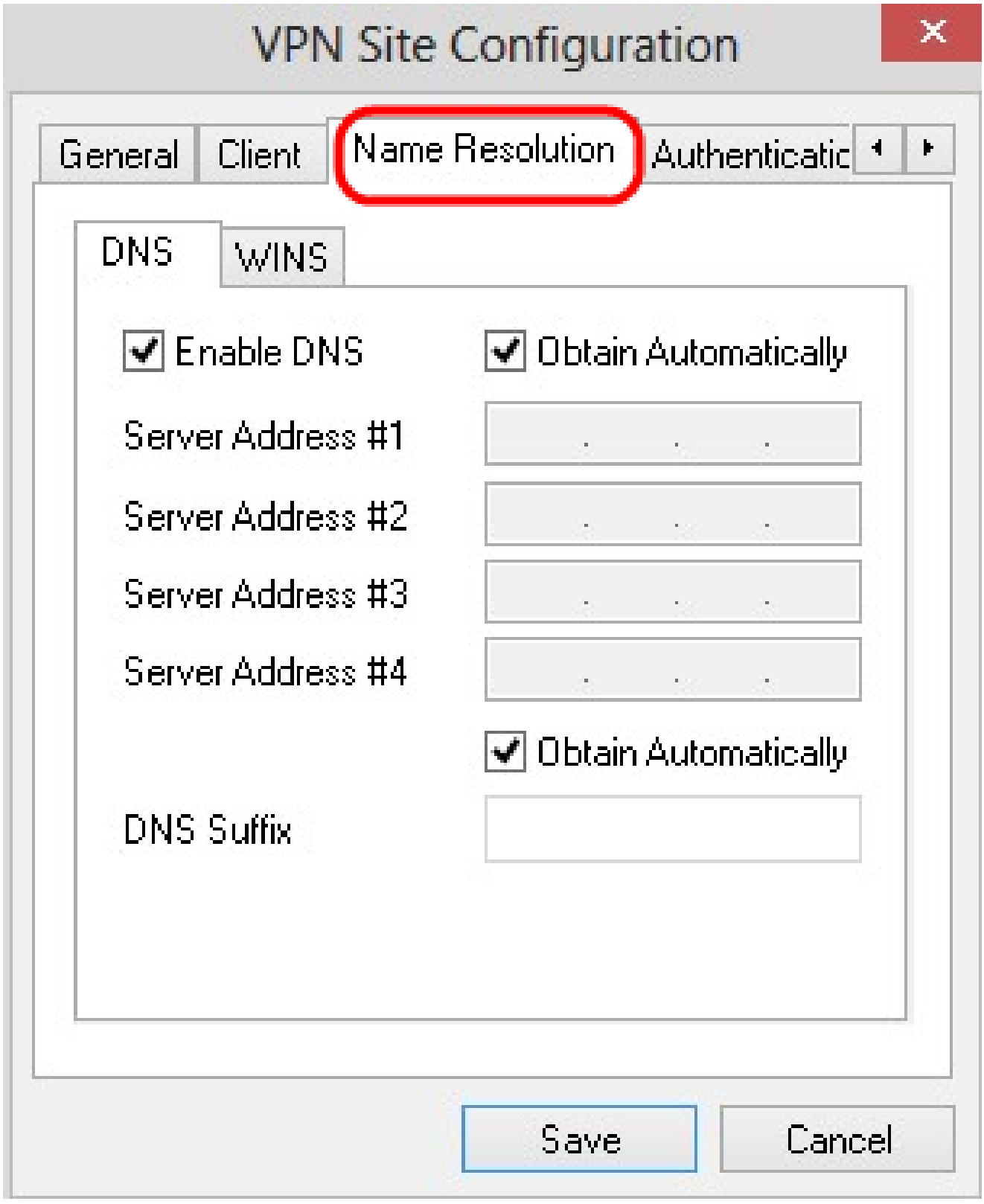
Étape 9. (Facultatif) Pour afficher une bannière de connexion par le client lorsque la connexion est établie avec la passerelle, cochez la case Enable Client Login.



Étape 10. Cliquez sur Save pour enregistrer les paramètres.

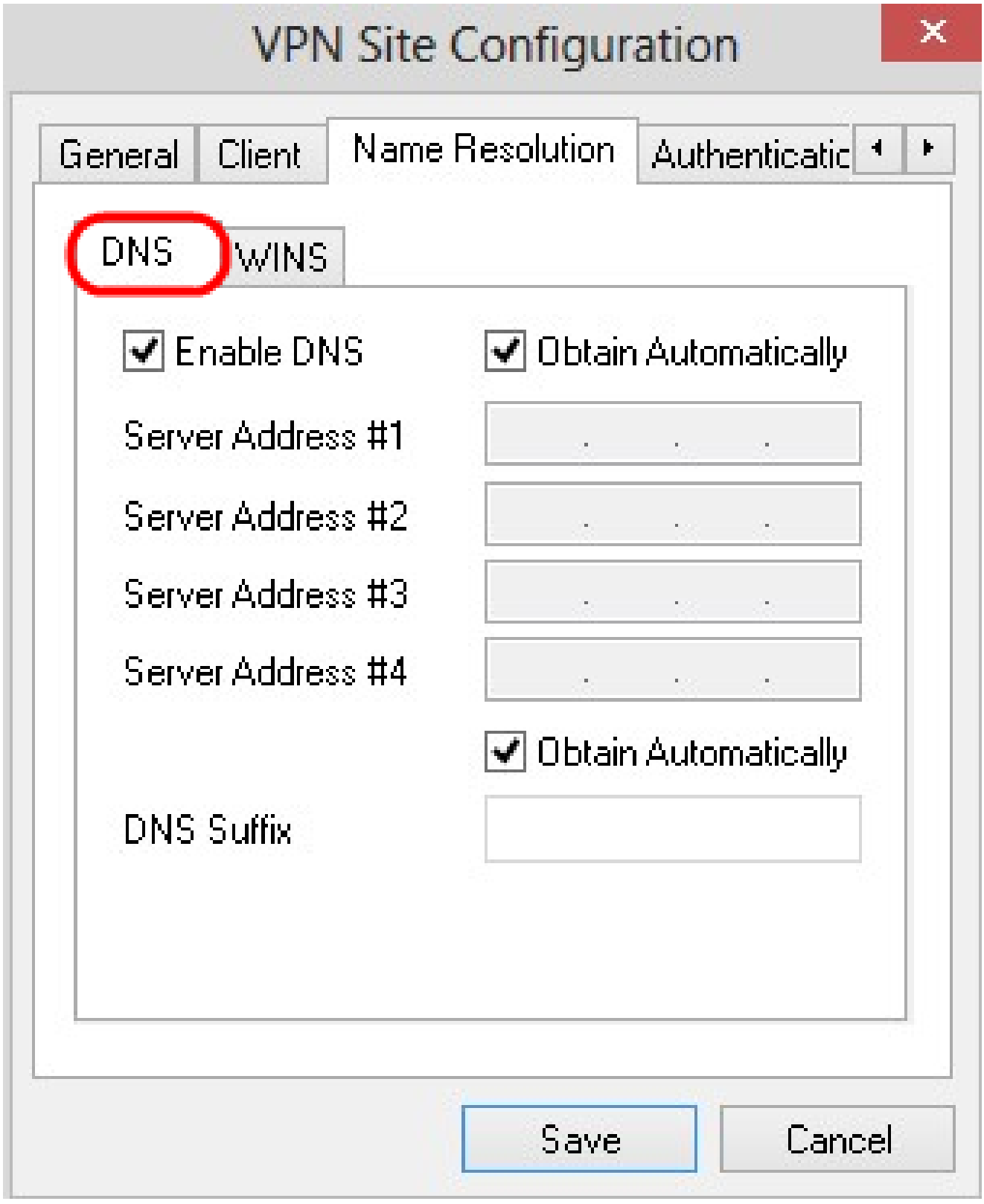
Configuration de résolution de noms

Étape 1. Cliquez sur l'onglet Résolution de nom.



Remarque : la section Résolution de noms est utilisée pour configurer les paramètres DNS (Domain Name System) et WIN (Windows Internet Name Service).

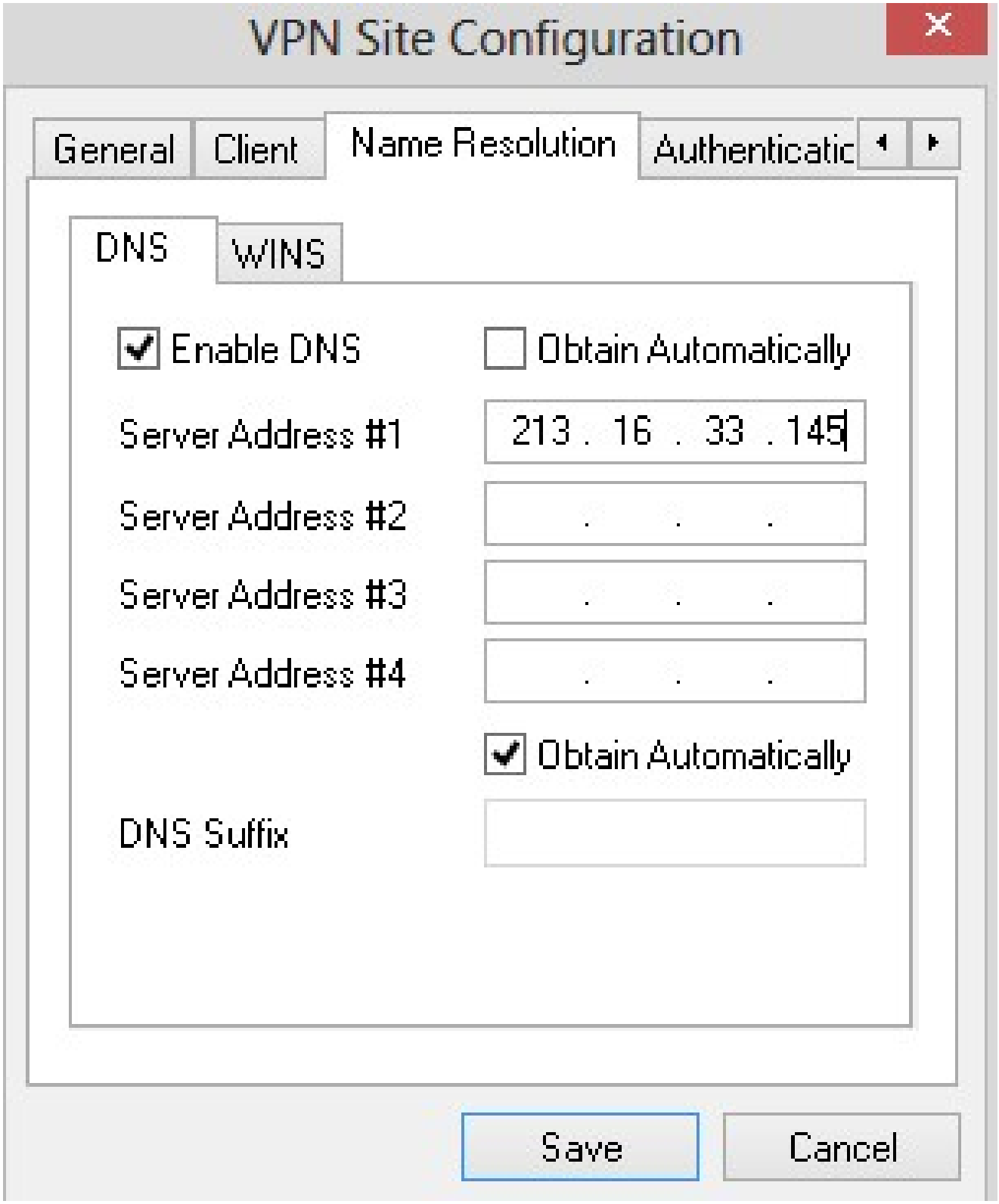
Étape 2. Cliquez sur l'onglet DNS.



Étape 3. Cochez Enable DNS pour activer le système de noms de domaine (DNS).

Étape 4. (Facultatif) Pour obtenir l'adresse du serveur DNS automatiquement, cochez la case Obtain Automatically (Obtenir automatiquement). Si cette option est choisie, passez à l'étape 6.

Étape 5. Saisissez l'adresse du serveur DNS dans le champ Server Address #1. S'il existe un autre serveur DNS, saisissez l'adresse de ces serveurs dans les champs Server Address restants.

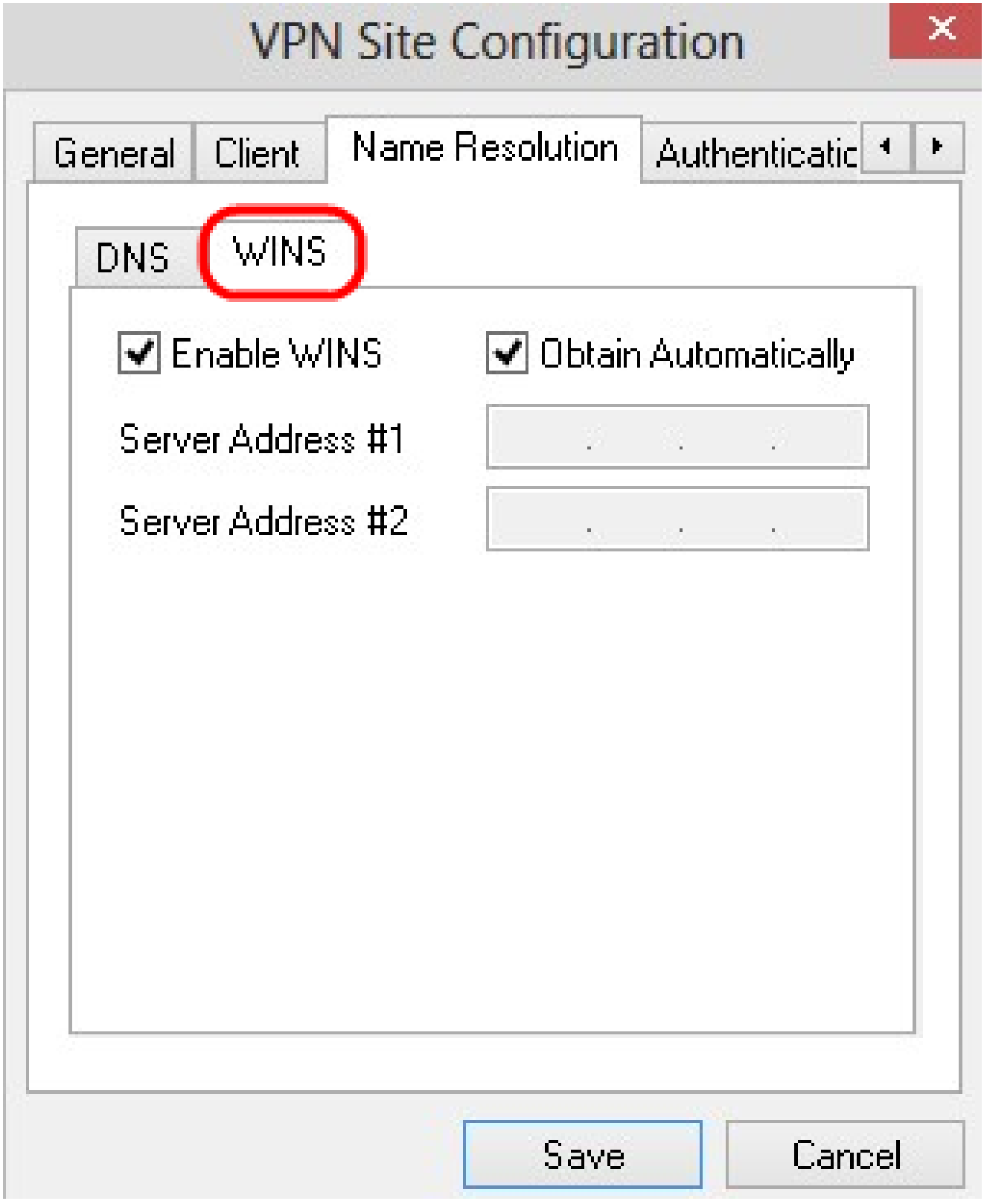


Étape 6. (Facultatif) Pour obtenir le suffixe du serveur DNS automatiquement, cochez la case Obtain Automatically . Si cette option est choisie, passez à l’étape 8.

Étape 7. Saisissez le suffixe du serveur DNS dans le champ Suffixe DNS.

Étape 8. Cliquez sur Save pour enregistrer les paramètres.

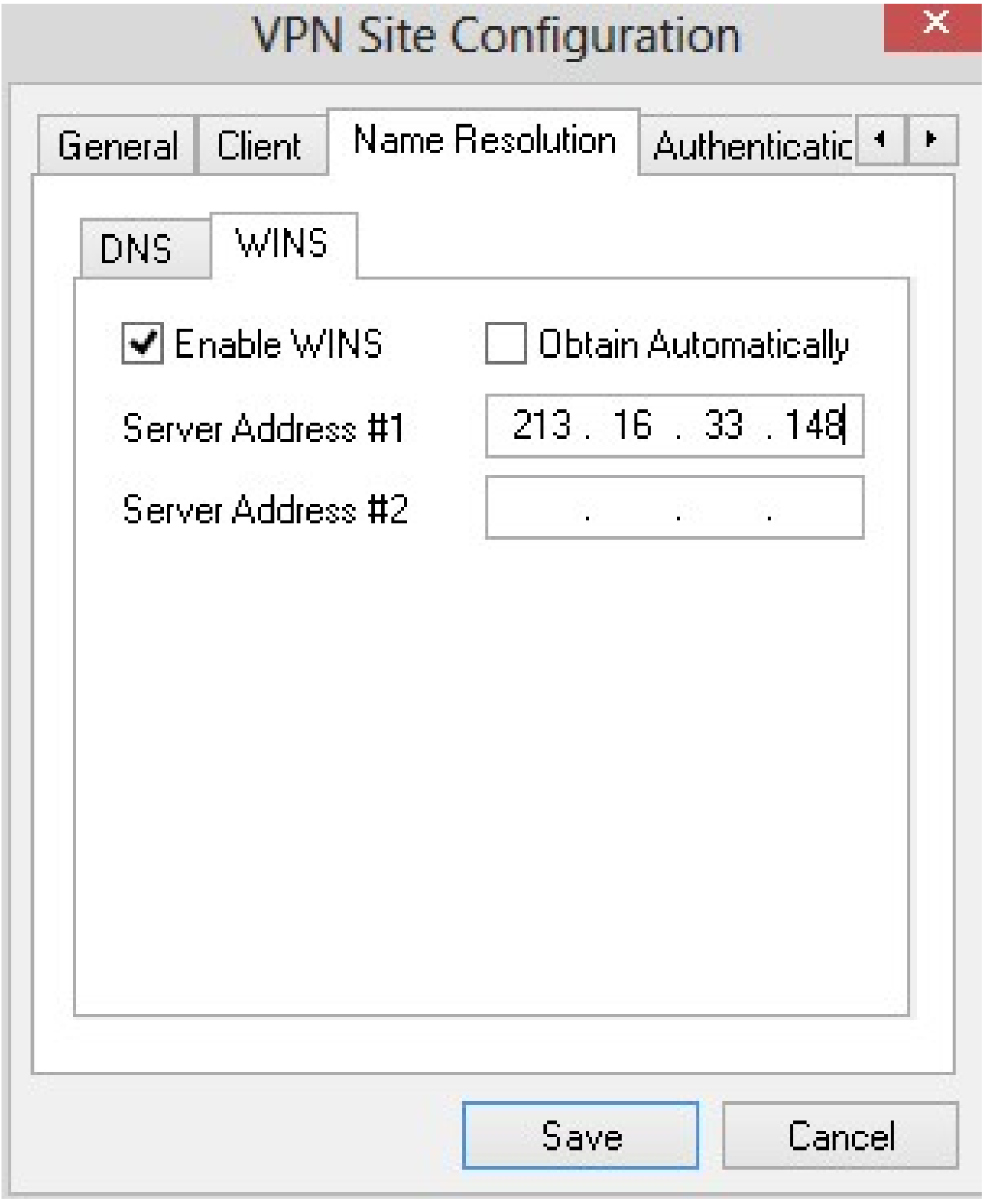
Étape 9. Cliquez sur l'onglet WINS.



Étape 10. Cochez Enable WINS pour activer Windows Internet Name Server (WINS).

Étape 11. (Facultatif) Pour obtenir l’adresse du serveur DNS automatiquement, cochez la case Obtain Automatically . Si cette option est choisie, passez à l’étape 13.

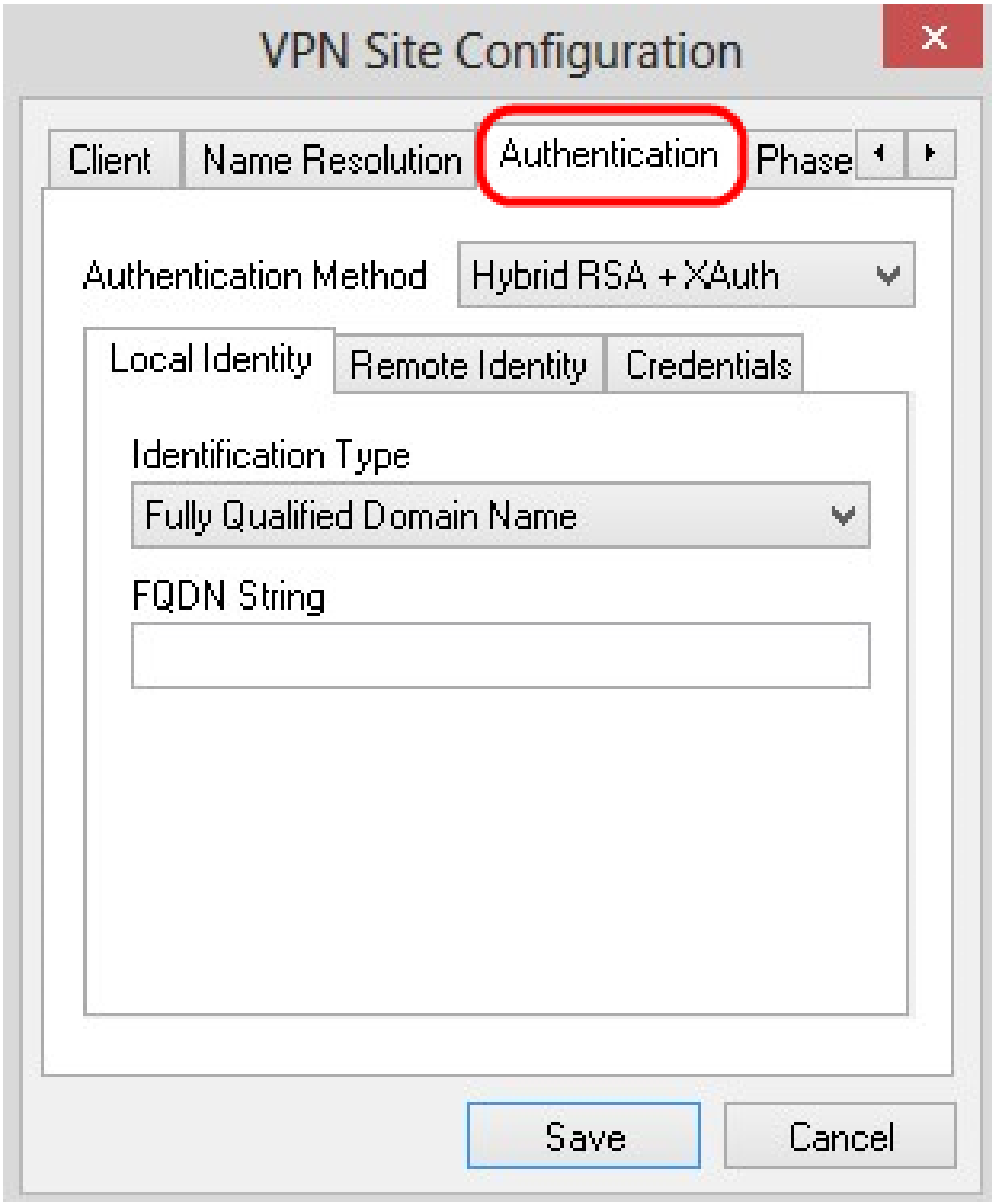
Étape 12. Entrez l'adresse du serveur WINS dans le champ Server Address #1. S'il existe d'autres serveurs DNS, entrez l'adresse de ces serveurs dans les champs Server Address restants.



Étape 13. Cliquez sur Save pour enregistrer les paramètres.

Authentification

Étape 1. Cliquez sur l'onglet Authentification.



Remarque : dans la section Authentication, vous pouvez configurer les paramètres pour que le client gère l'authentification lorsqu'il tente d'établir une SA ISAKMP.

Étape 2. Sélectionnez la méthode d'authentification appropriée dans la liste déroulante Authentication Method.

· 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.

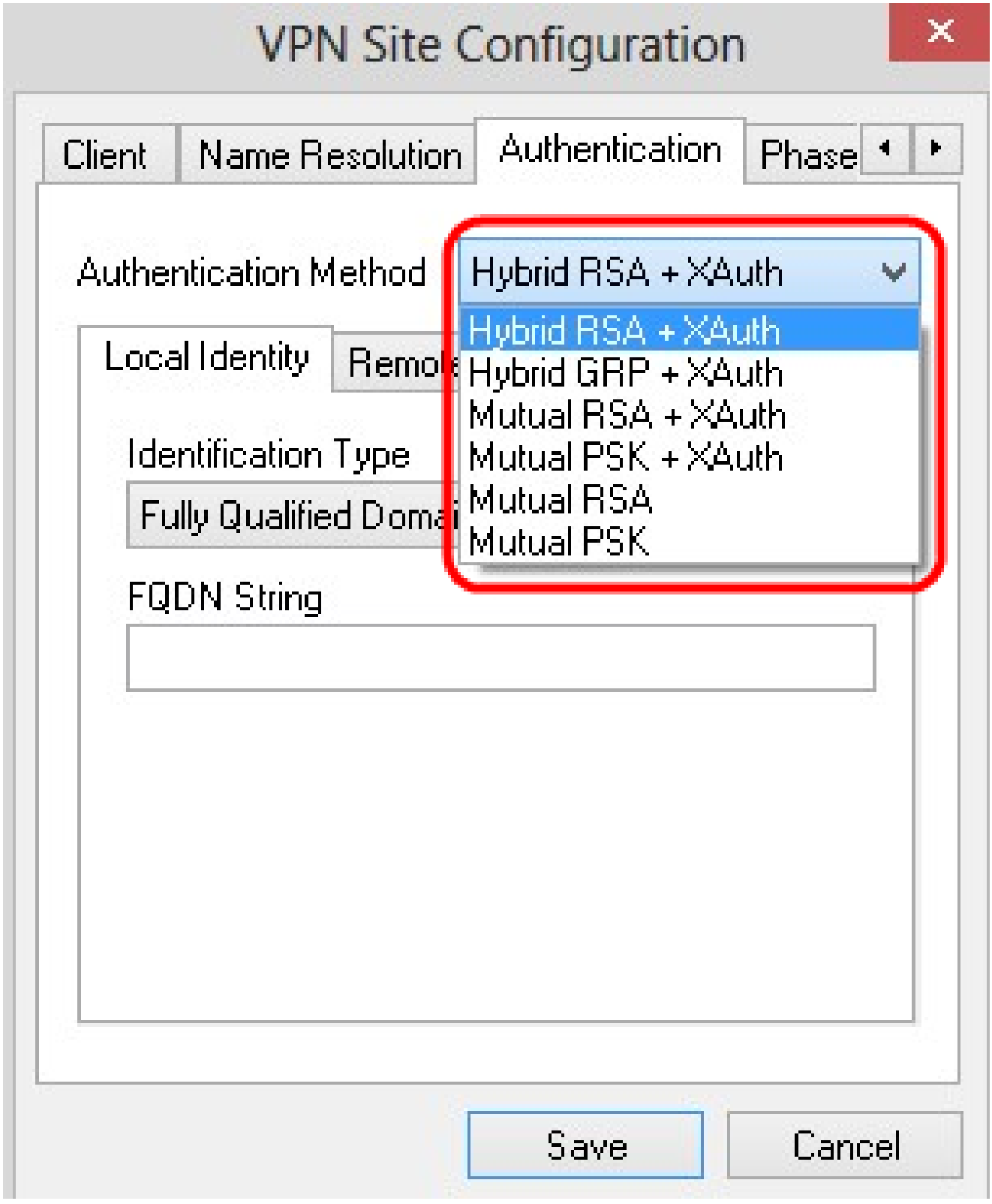
· Hybrid GRP + XAuth — Les informations d'identification du client ne sont pas nécessaires. Le client authentifie la passerelle. Les informations d'identification se présentent sous la forme d'un fichier de certificat PEM ou PKCS12 et d'une chaîne secrète partagée.

· 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 + XAuth mutuels : 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.

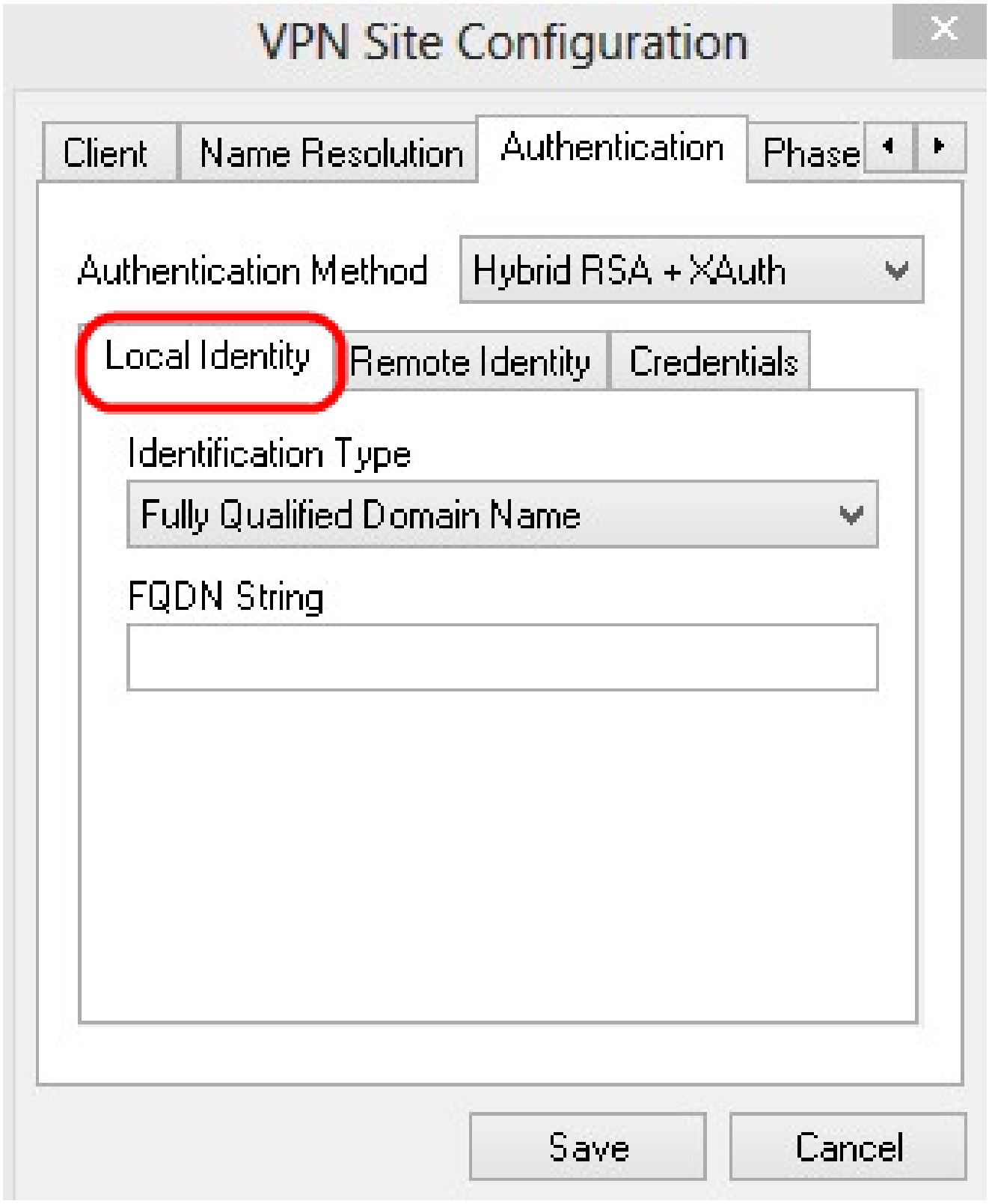
· RSA mutuel : le client et la passerelle ont tous deux besoin d'informations d'identification pour s'authentifier. Les informations d'identification se présentent sous la forme de fichiers de certificat PEM ou PKCS12 ou de type de clé.

· 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.



Configuration de l'identité locale

Étape 1. Cliquez sur l'onglet Identité locale.



Remarque : l'identité locale définit l'ID envoyé à la passerelle pour vérification. Dans la section Identité locale, le type d'identification et la chaîne FQDN (Fully Qualified Domain Name) sont configurés pour déterminer comment l'ID est envoyé.

Étape 2. Sélectionnez l'option d'identification appropriée dans la liste déroulante Type d'identification. Toutes les options ne sont pas disponibles pour tous les modes

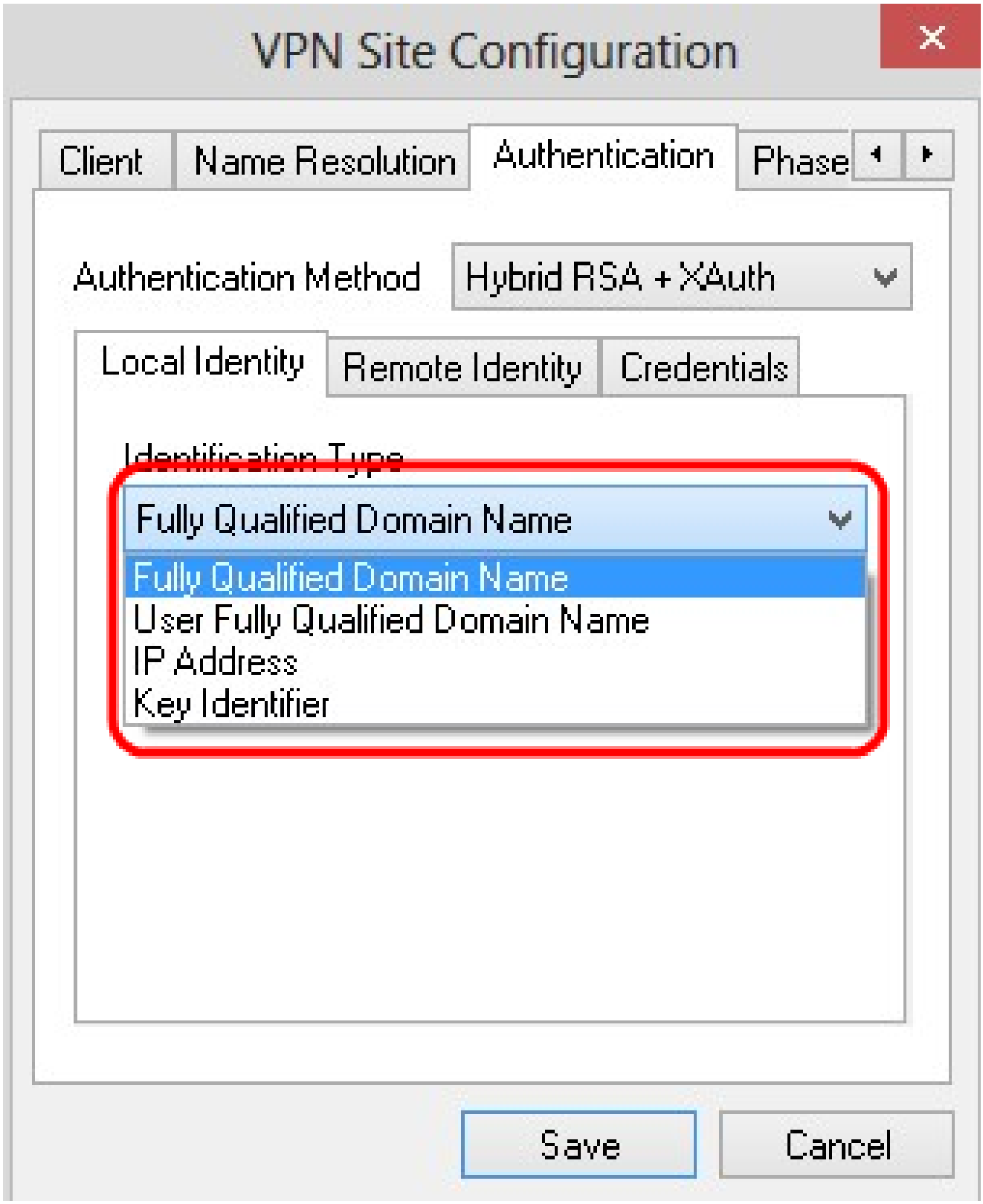
d'authentification.

· Nom de domaine complet : l'identification client de l'identité locale est basée sur un nom de domaine complet. Si vous choisissez cette option, suivez l'étape 3, puis passez à l'étape 7.

· User Fully Qualified Domain Name : l'identification client de l'identité locale est basée sur le nom de domaine complet de l'utilisateur. Si vous choisissez cette option, suivez l'étape 4, puis passez à l'étape 7.

· Adresse IP : l'identification du client de l'identité locale est basée sur l'adresse IP. Si vous cochez Utiliser une adresse d'hôte local découverte, l'adresse IP est découverte automatiquement. Si vous choisissez cette option, suivez l'étape 5, puis passez à l'étape 7.

· Identificateur de clé — L'identification du client local est établie à partir d'un identificateur de clé. Si vous choisissez cette option, suivez les étapes 6 et 7.



Étape 3. Entrez le nom de domaine complet en tant que chaîne DNS dans le champ FQDN String.

Étape 4. Entrez le nom de domaine complet de l'utilisateur en tant que chaîne DNS dans le champ UFQDN String.

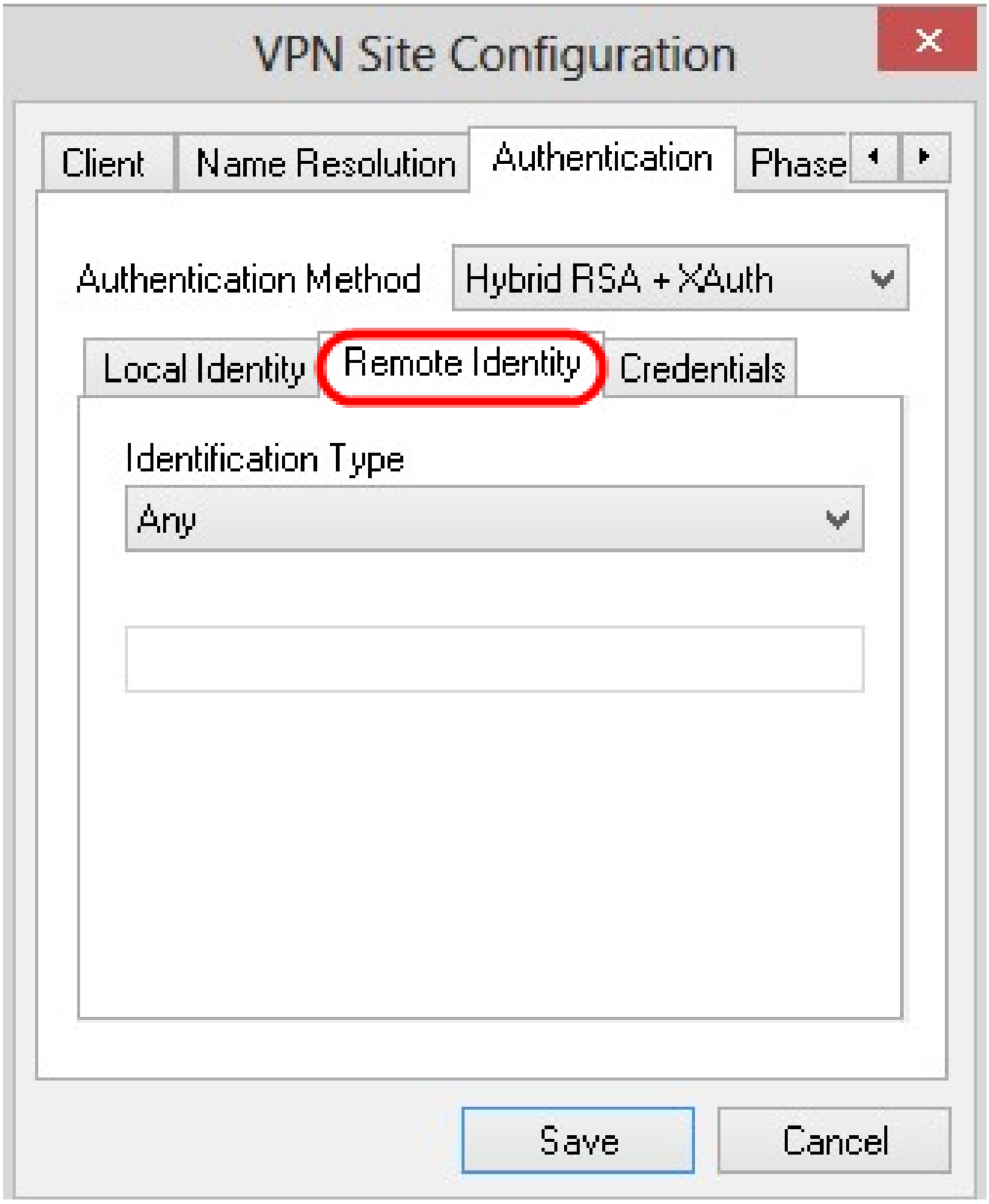
Étape 5. Saisissez l'adresse IP dans le champ UFQDN String.

Étape 6. Entrez l'identificateur de clé pour identifier le client local dans la chaîne d'ID de clé.

Étape 7. Cliquez sur Save pour enregistrer les paramètres.

Configuration de l'identité distante

Étape 1. Cliquez sur l'onglet Identité distante.



Remarque : Remote Identity vérifie l'ID à partir de la passerelle. Dans la section Identité distante, le type d'identification est configuré pour déterminer comment l'ID est vérifié.

Étape 2. Sélectionnez l'option d'identification appropriée dans la liste déroulante Type d'identification.

· Any : le client distant peut accepter n'importe quelle valeur ou n'importe quel ID à authentifier.

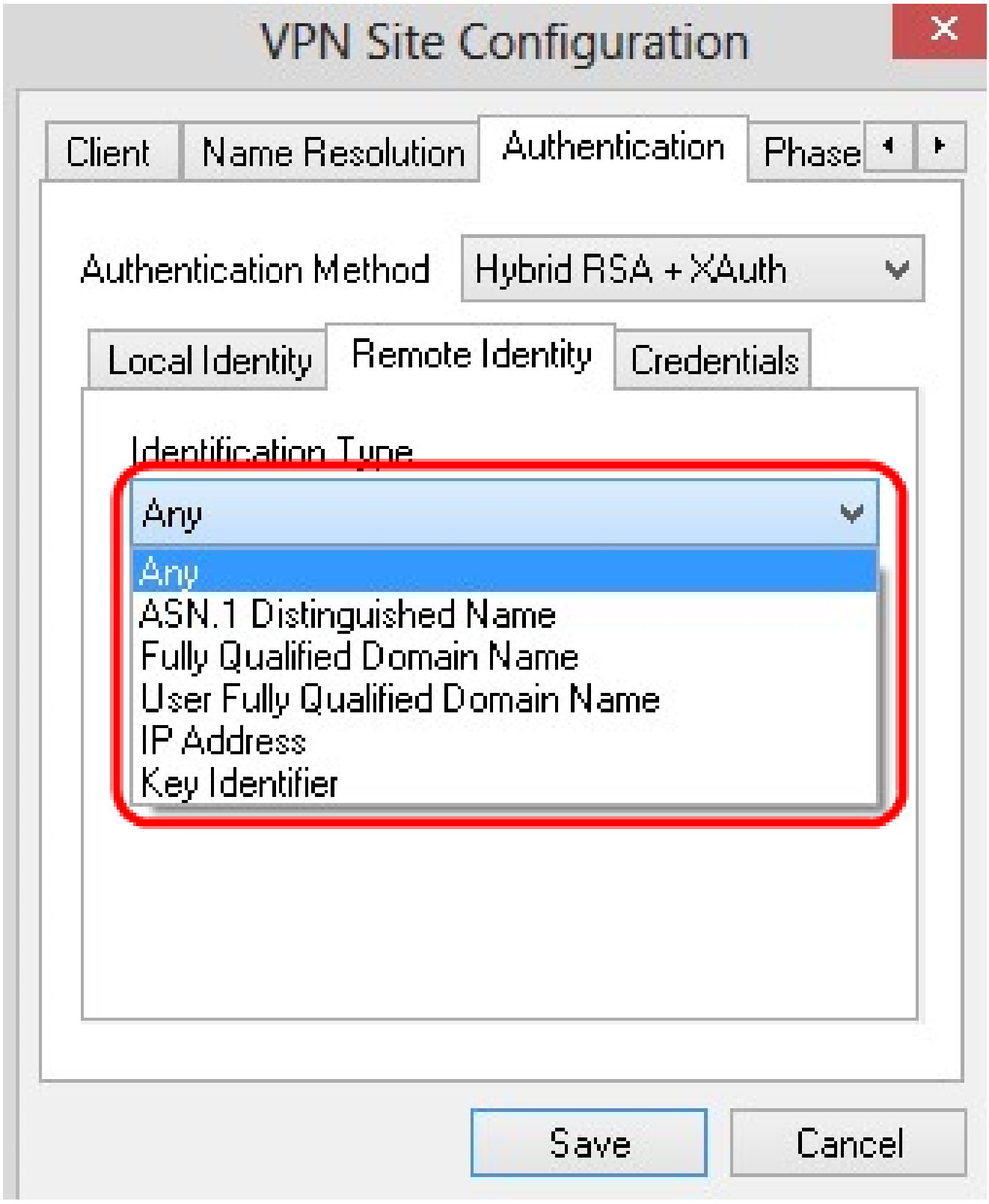
· ASN.1 Distinguished Name : le client distant est automatiquement identifié à partir d'un fichier de certificat PEM ou PKCS12. Vous ne pouvez choisir cette option que si vous choisissez une méthode d'authentification RSA à l'étape 2 de la section Authentification. Cochez la case Utiliser l'objet dans le certificat reçu mais ne le comparez pas à une valeur spécifique pour recevoir automatiquement le certificat. Si vous choisissez cette option, suivez l'étape 3, puis passez à l'étape 8.

· Nom de domaine complet : l'identification client de l'identité distante est basée sur le nom de domaine complet. Vous ne pouvez choisir cette option que si vous choisissez une méthode d'authentification PSK à l'étape 2 de la section Authentification. Si vous choisissez cette option, suivez l'étape 4, puis passez à l'étape 8.

· User Fully Qualified Domain Name : l'identification client de l'identité distante est basée sur le nom de domaine complet de l'utilisateur. Vous ne pouvez choisir cette option que si vous choisissez une méthode d'authentification PSK à l'étape 2 de la section Authentification. Si vous choisissez cette option, suivez l'étape 5, puis passez à l'étape 8.

· Adresse IP : l'identification du client de l'identité distante est basée sur l'adresse IP. Si vous cochez Utiliser une adresse d'hôte local découverte, l'adresse IP est découverte automatiquement. Si vous choisissez cette option, suivez l'étape 6, puis passez à l'étape 8.

· Identificateur de clé — L'identification du client distant est fondée sur un identificateur de clé. Si vous choisissez cette option, suivez les étapes 7 et 8.



Étape 3. Entrez la chaîne DN ASN.1 dans le champ Chaîne DN ASN.1.

Étape 4. Entrez le nom de domaine complet sous forme de chaîne DNS dans le champ FQDN String.

Étape 5. Entrez le nom de domaine complet de l'utilisateur en tant que chaîne DNS dans le

champ UFQDN String.

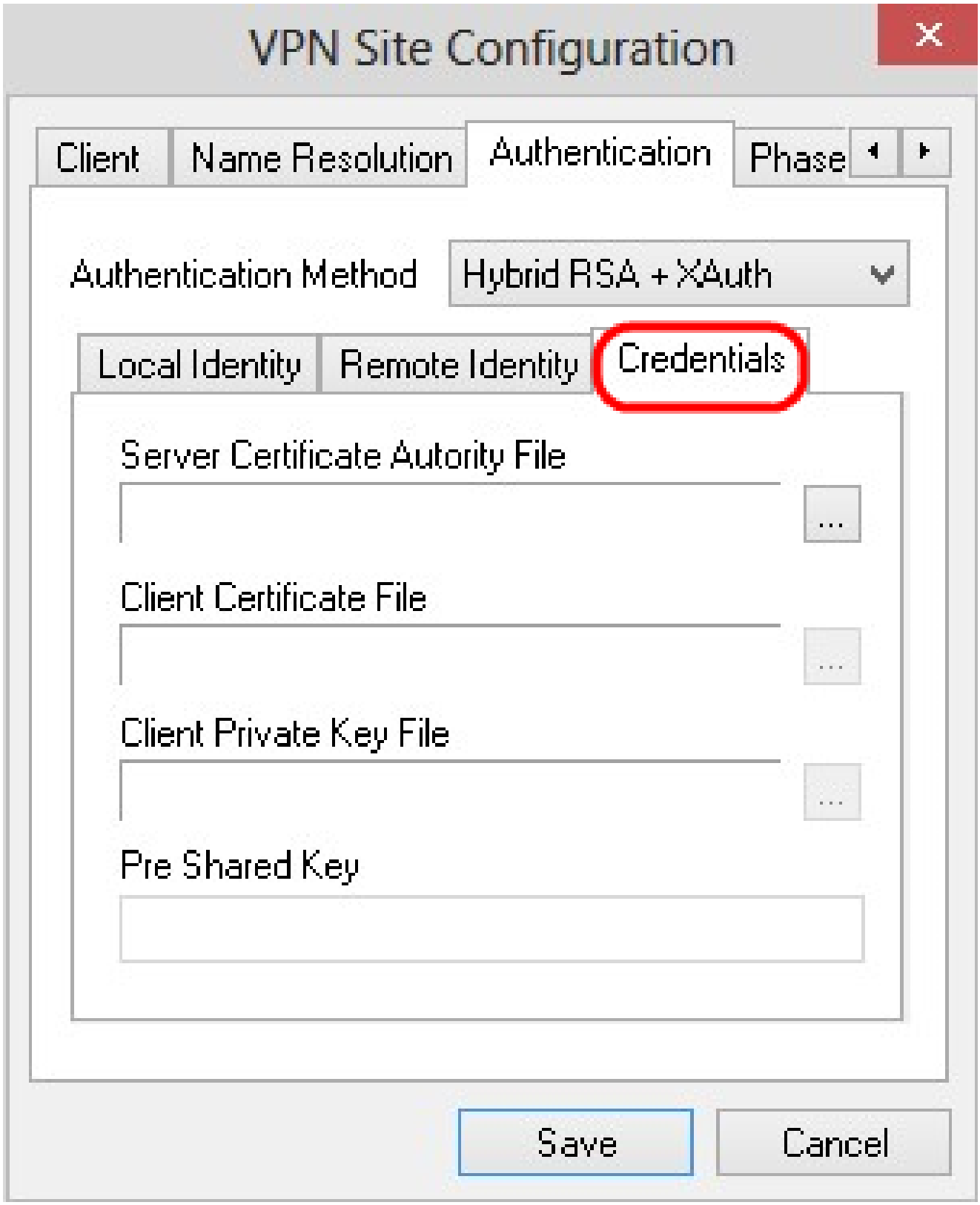
Étape 6. Saisissez l'adresse IP dans le champ UFQDN String.

Étape 7. Entrez l'identificateur de clé permettant d'identifier le client local dans le champ Key ID String.

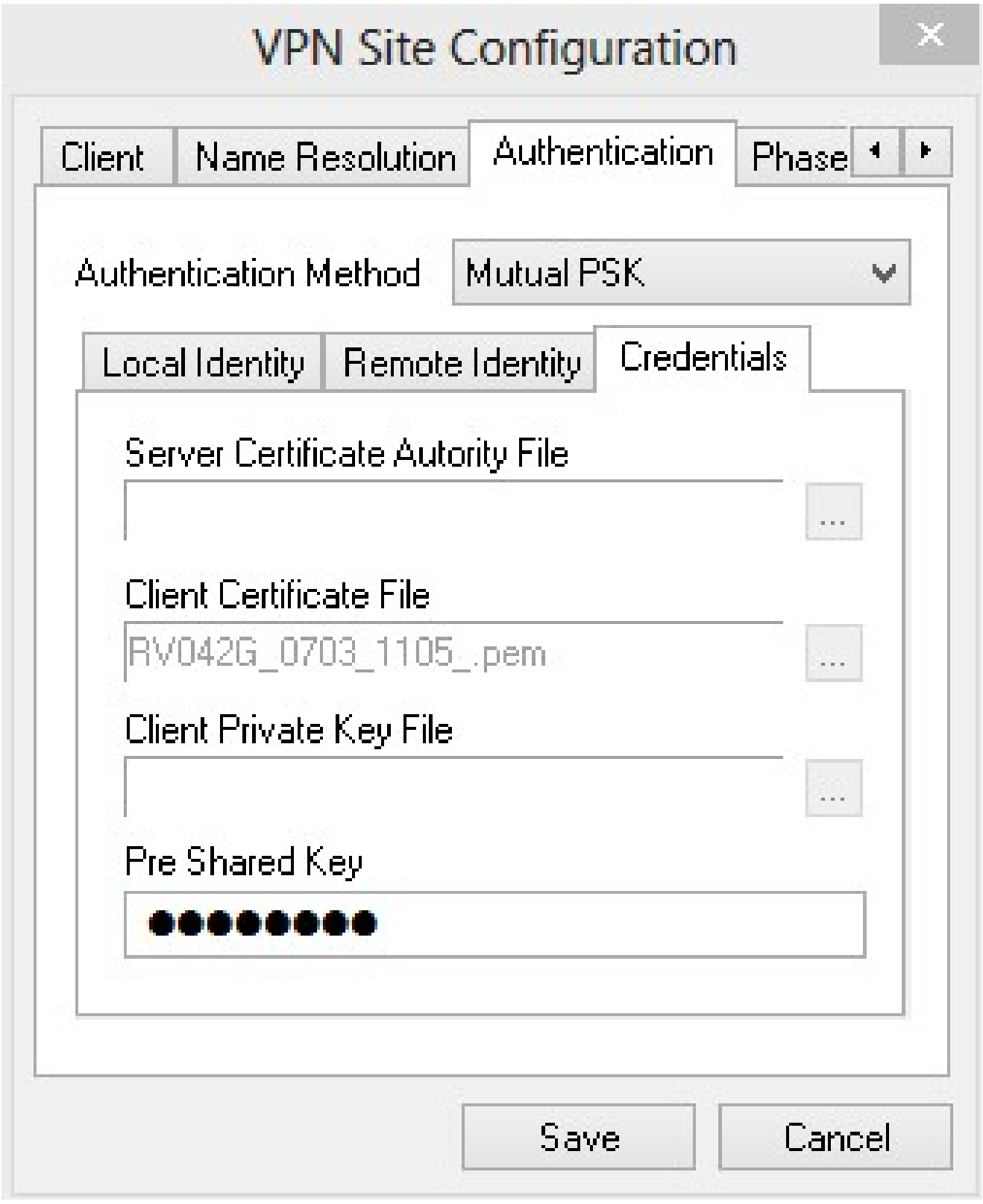
Étape 8. Cliquez sur Save pour enregistrer les paramètres.

Configuration des informations d'identification

Étape 1. Cliquez sur l'onglet Informations d'identification.



Remarque : dans la section Informations d'identification, la clé prépartagée est configurée.



Étape 2. Pour choisir le fichier de certificat de serveur, cliquez sur l'icône ... en regard du champ Server Certificate Authority File et choisissez le chemin où vous avez enregistré le fichier de certificat de serveur sur votre PC.

Étape 3. Pour choisir le fichier de certificat client, cliquez sur l'icône ... en regard du champ Fichier de certificat client et choisissez le chemin où vous avez enregistré le fichier de

certificat client sur votre PC.

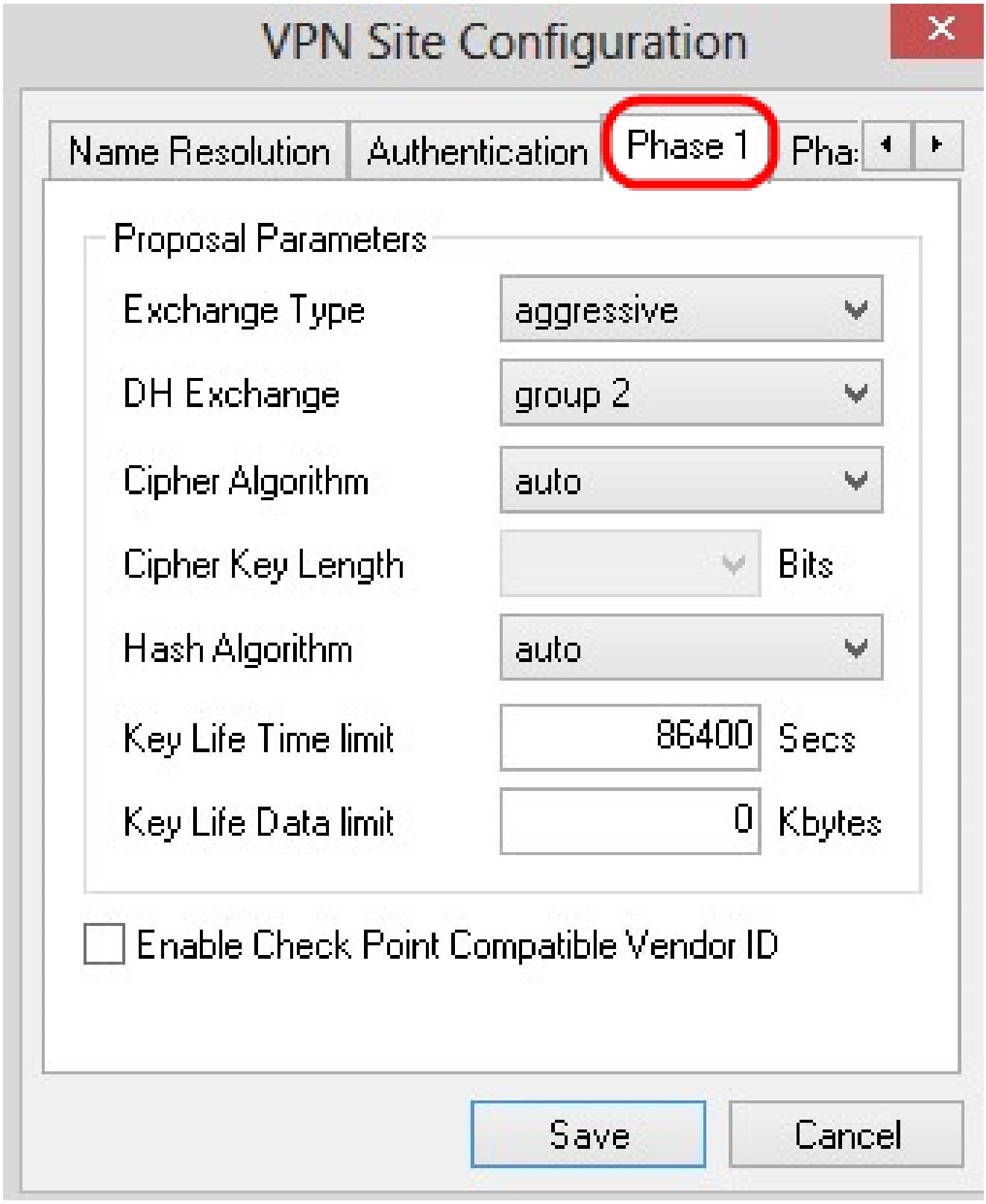
Étape 4. Pour choisir le fichier de clé privée du client, cliquez sur l'icône ... en regard du champ Client Private Key File et choisissez le chemin où vous avez enregistré le fichier de clé privée du client sur votre PC.

Étape 5. Saisissez la clé pré-partagée dans le champ PreShared Key. Il doit s'agir de la même clé que celle utilisée lors de la configuration du tunnel.

Étape 6. Cliquez sur Save pour enregistrer les paramètres.

Configuration de la phase 1

Étape 1. Cliquez sur l'onglet Phase 1.

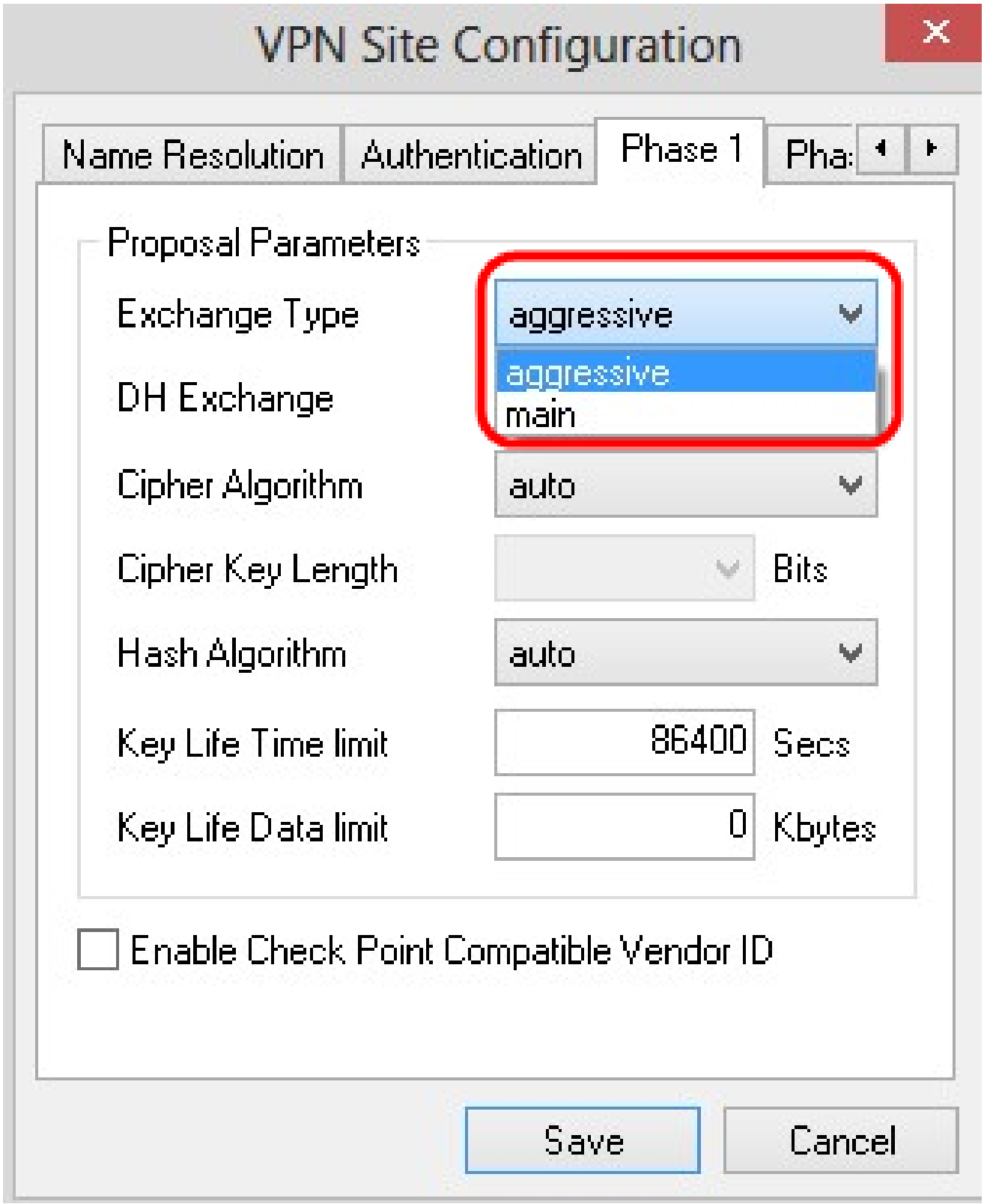


Remarque : dans la section Phase 1, vous pouvez configurer les paramètres de sorte qu'une SA ISAKMP avec la passerelle client puisse être établie.

Étape 2. Sélectionnez le type d'échange de clé approprié dans la liste déroulante Type d'échange.

· Principal — L'identité des pairs est protégée.

· Agressif — L'identité des pairs n'est pas sécurisée.



Étape 3. Dans la liste déroulante DH Exchange, choisissez le groupe approprié qui a été choisi lors de la configuration de la connexion VPN.

Étape 4. Dans la liste déroulante Algorithme de chiffrement, choisissez l'option appropriée qui a été choisie lors de la configuration de la connexion VPN.

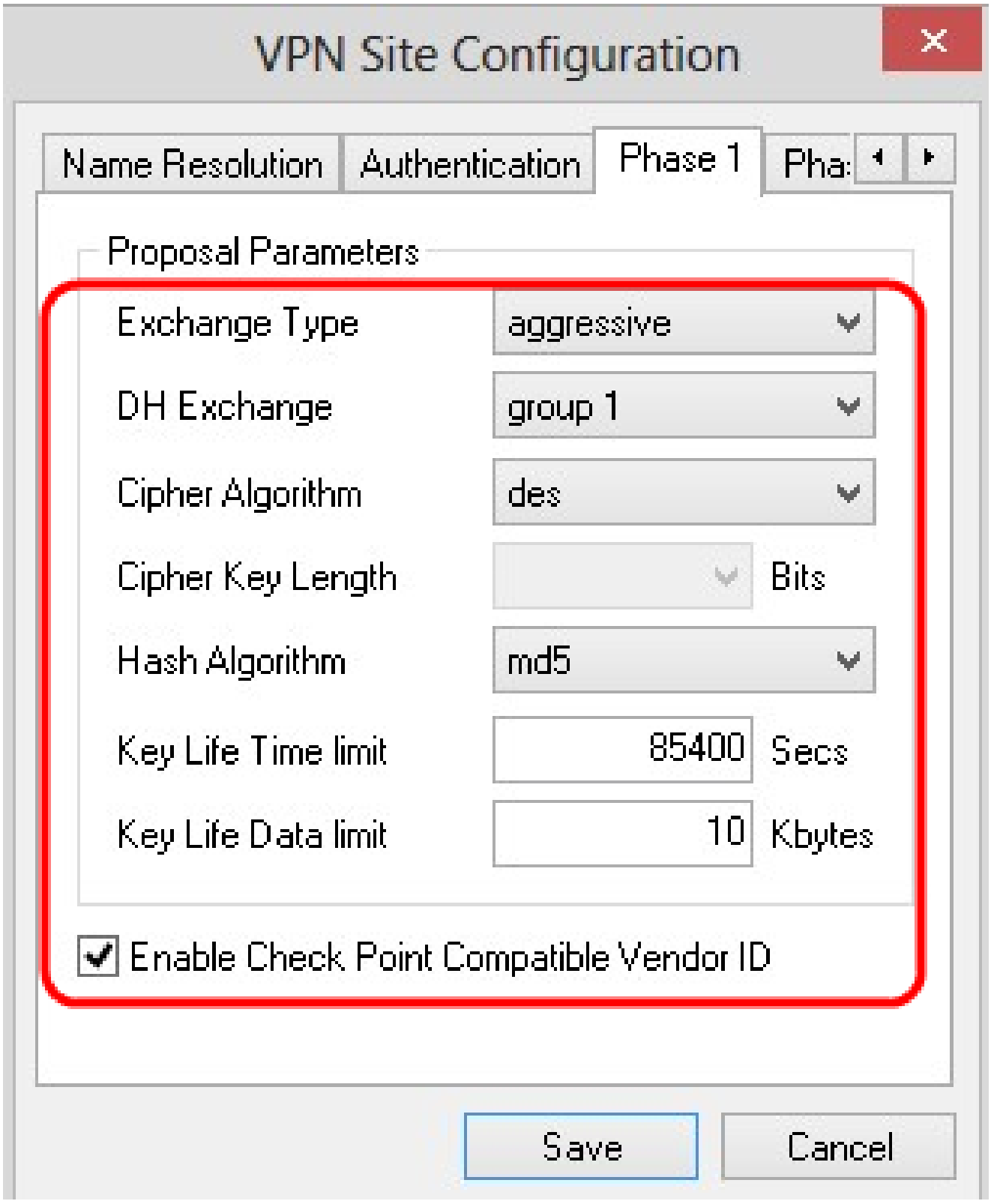
Étape 5. Dans la liste déroulante Cipher Key Length, choisissez l'option qui correspond à la longueur de clé de l'option qui a été choisie lors de votre configuration de la connexion VPN.

Étape 6. Dans la liste déroulante Hash Algorithm, choisissez l'option qui a été choisie lors de votre configuration de la connexion VPN.

Étape 7. Dans le champ Key Life Time limit, saisissez la valeur utilisée pendant votre configuration de la connexion VPN.

Étape 8. Dans le champ Key Life Data limit, saisissez la valeur en kilo-octets à protéger. La valeur par défaut est 0, ce qui désactive la fonction.

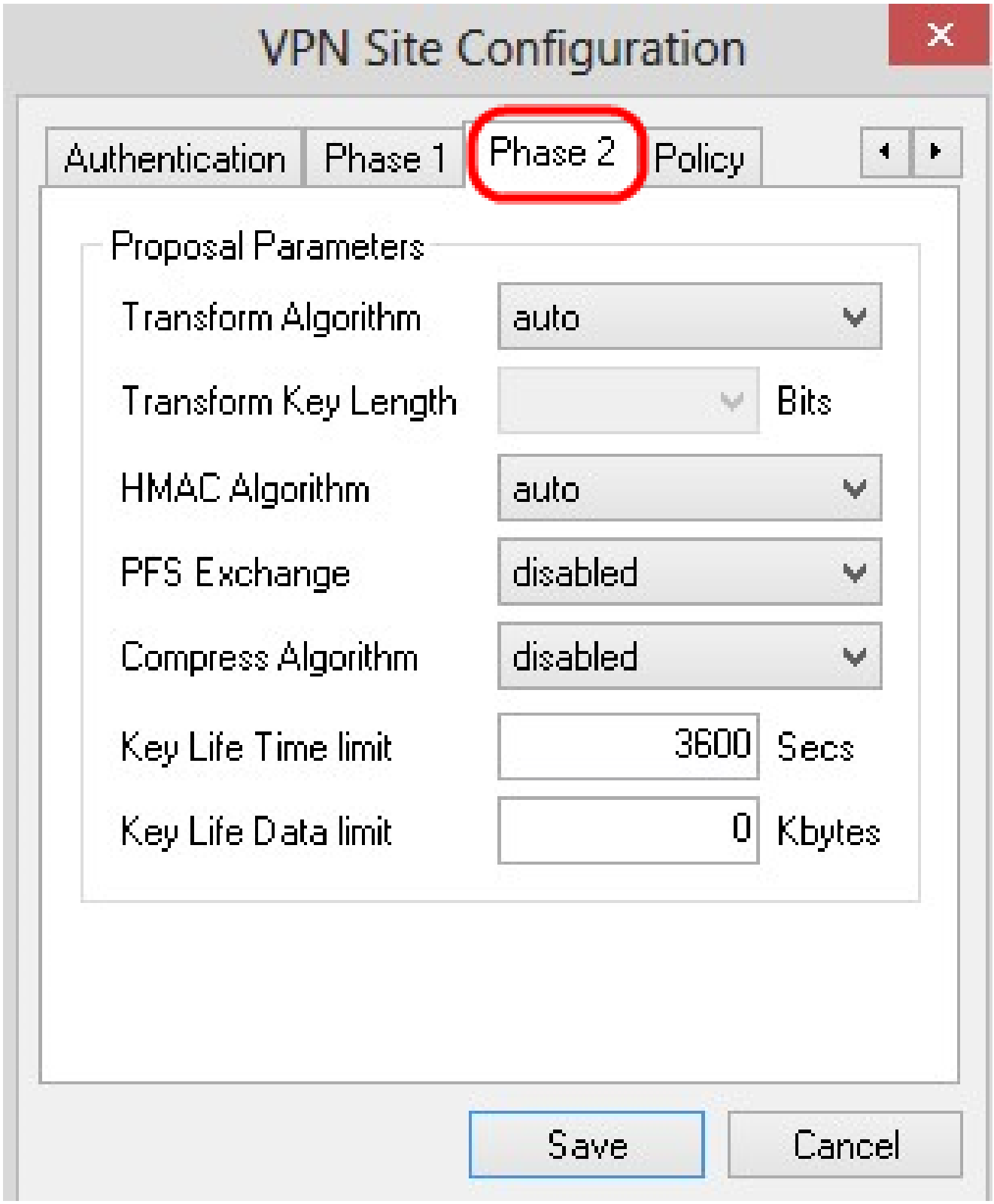
Étape 9. (Facultatif) Cochez la case Enable Check Point Compatible Vendor ID.



Étape 10. Cliquez sur Save pour enregistrer les paramètres.

Configuration de la phase 2

Étape 1. Cliquez sur l'onglet Phase 2.



Remarque : dans la section Phase 2, vous pouvez configurer les paramètres de sorte qu'une SA IPsec avec la passerelle client distante puisse être établie.

Étape 2. Dans la liste déroulante Transform Algorithm, choisissez l'option qui a été choisie lors de la configuration de la connexion VPN.

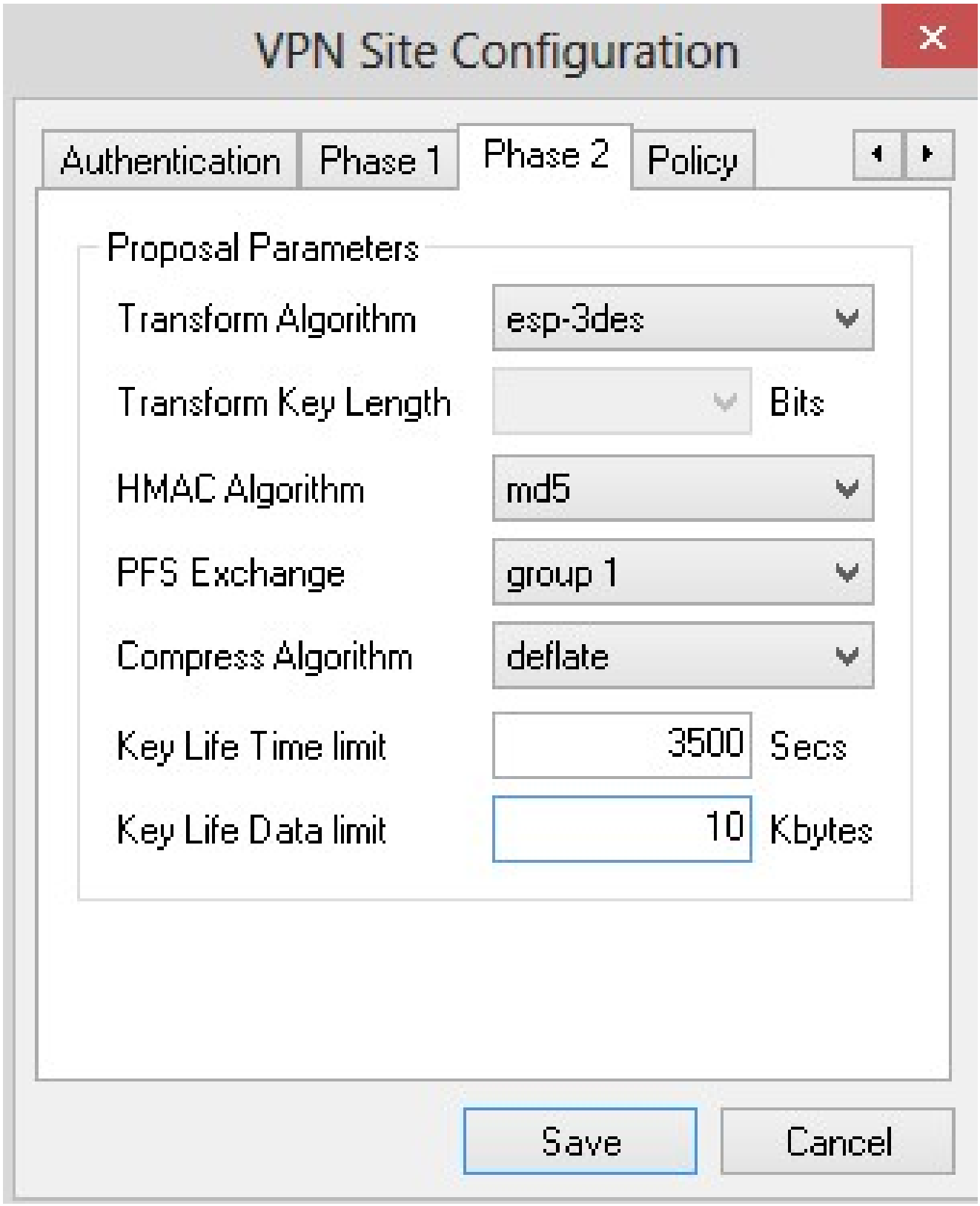
Étape 3. Dans la liste déroulante Transform Key Length, choisissez l'option qui correspond à la longueur de clé de l'option qui a été choisie lors de la configuration de la connexion VPN.

Étape 4. Dans la liste déroulante HMAC Algorithm, choisissez l'option qui a été choisie lors de la configuration de la connexion VPN.

Étape 5. Dans la liste déroulante PFS Exchange, choisissez l'option qui a été choisie lors de la configuration de la connexion VPN.

Étape 6. Dans le champ Key Life Time limit, saisissez la valeur utilisée pendant la configuration de la connexion VPN.

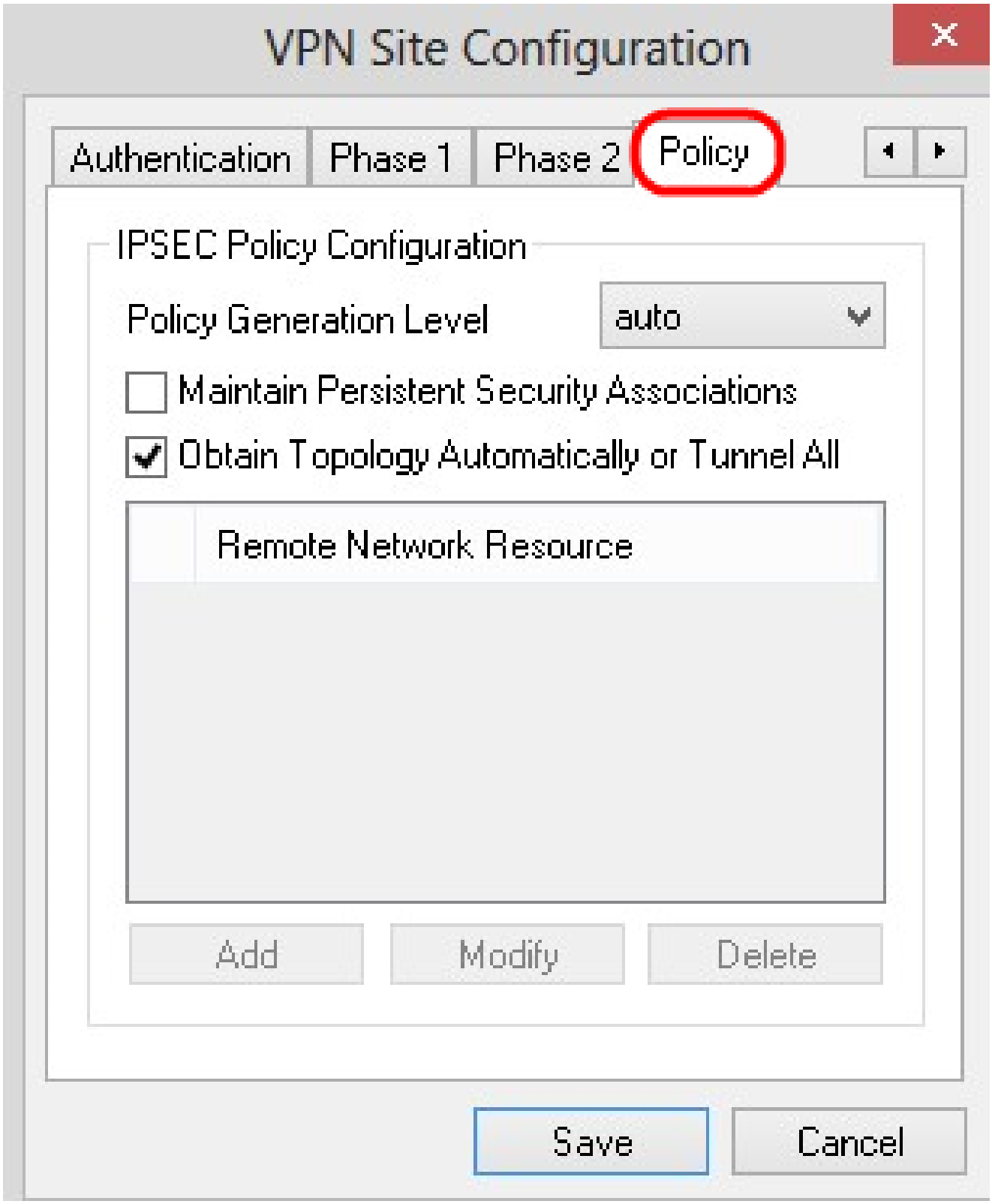
Étape 7. Dans le champ Limite de données de durée de vie des clés, saisissez la valeur en kilo-octets à protéger. La valeur par défaut est 0, ce qui désactive la fonction.



Étape 8. Cliquez sur Save pour enregistrer les paramètres.

Configuration des stratégies

Étape 1. Cliquez sur l'onglet Policy.



Remarque : dans la section Stratégie, la stratégie IPSEC est définie, ce qui est nécessaire pour que le client communique avec l'hôte pour la configuration du site.

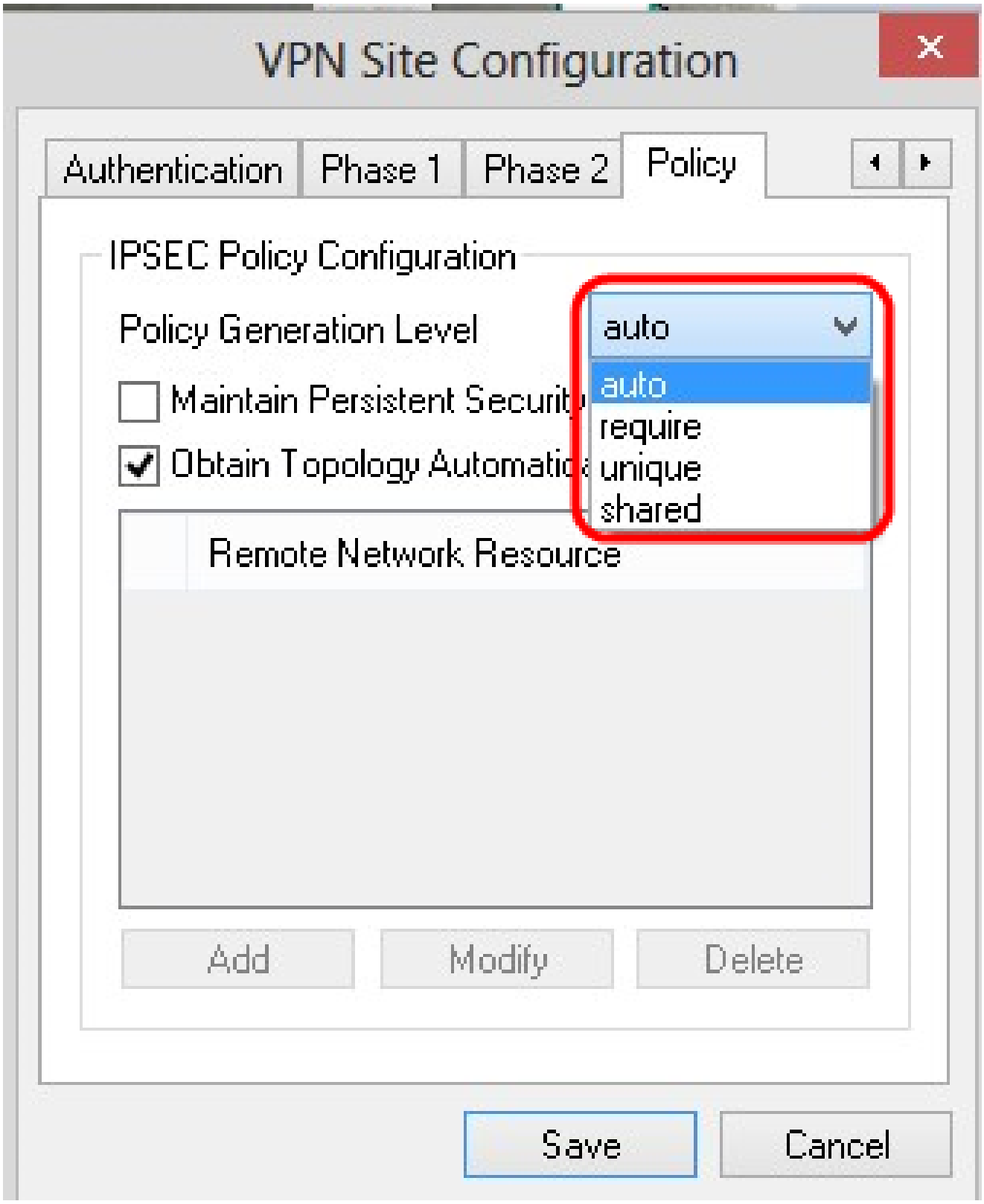
Étape 2. Dans la liste déroulante Niveau de génération de la stratégie, sélectionnez l'option appropriée.

· Auto : le niveau de stratégie IPsec nécessaire est déterminé automatiquement.

· Require : une association de sécurité unique pour chaque stratégie n'est pas négociée.

· Unique : une association de sécurité unique pour chaque stratégie est négociée.

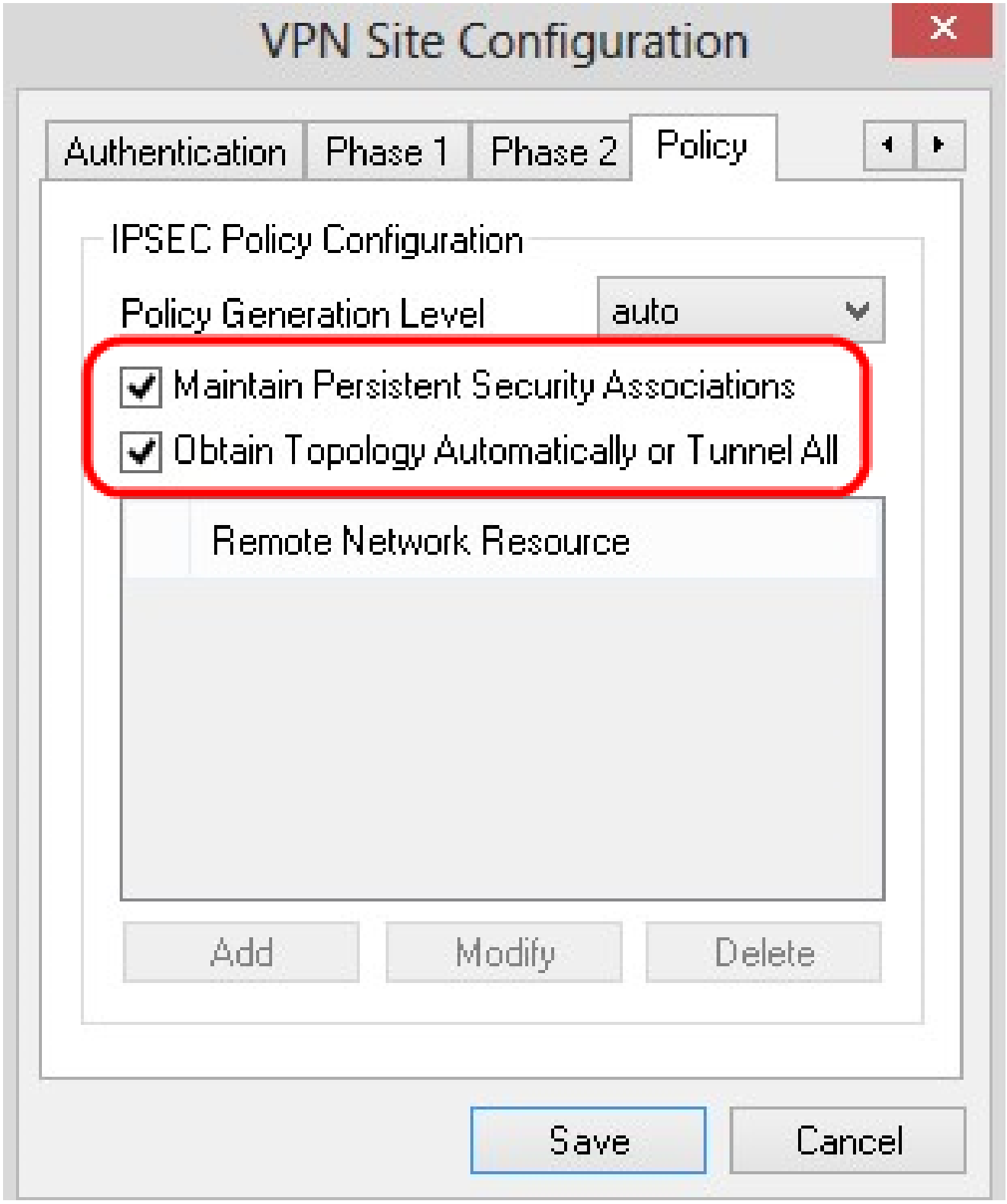
· Partagée — La politique appropriée est élaborée au niveau nécessaire.



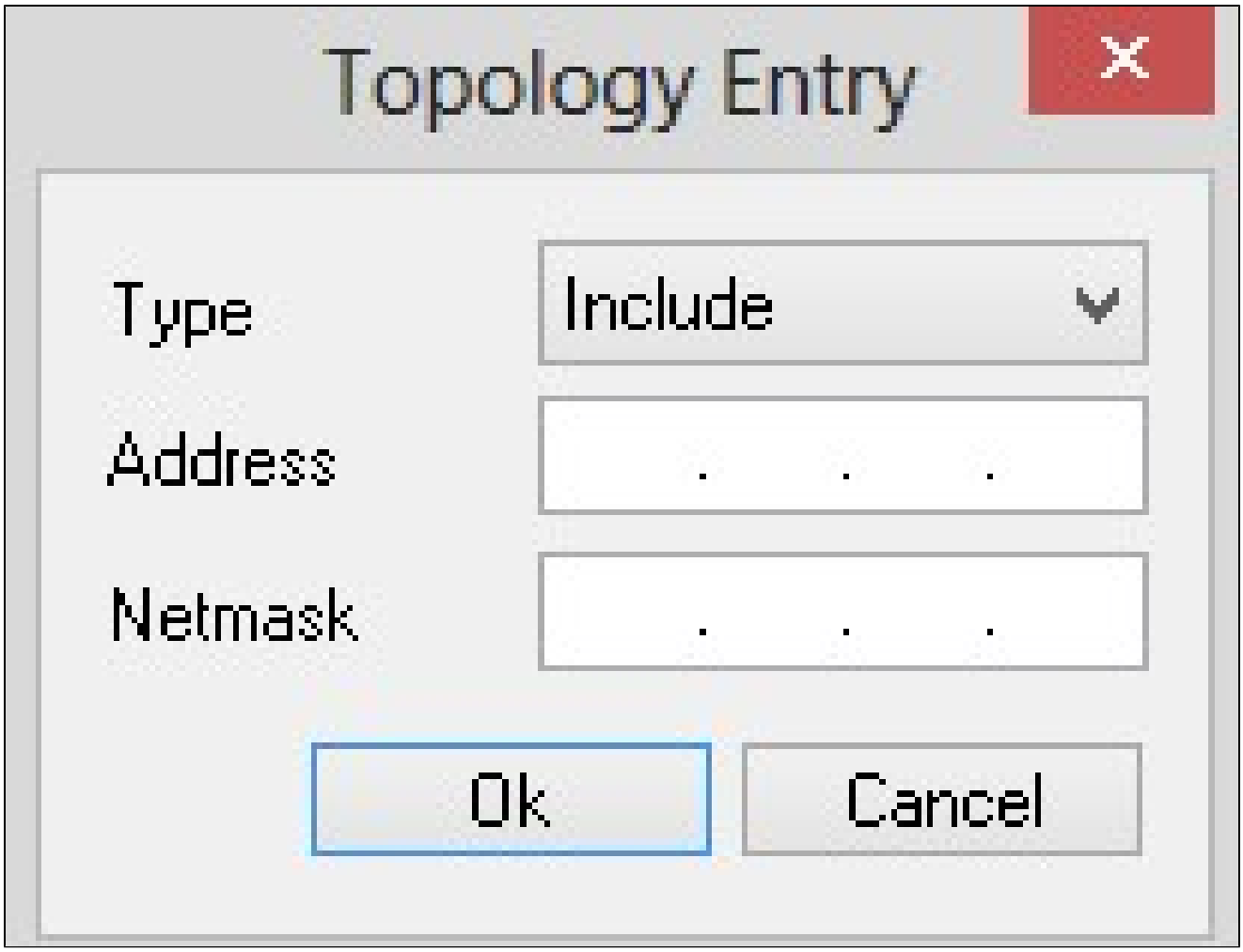
Étape 3. (Facultatif) Pour modifier les négociations IPSec, cochez la case Maintenir les associations de sécurité persistantes. Si cette option est activée, la négociation est effectuée pour chaque stratégie directement après la connexion. Si cette option est désactivée, la négociation est effectuée en fonction des besoins.

Étape 4. (Facultatif) Pour recevoir une liste de réseaux fournie automatiquement par le

périphérique ou pour envoyer tous les paquets au routeur RV0XX par défaut, cochez la case Obtain Topology Automatically ou Tunnel All. Si cette case n'est pas cochée, la configuration doit être effectuée manuellement. Si cette case est cochée, passez à l'étape 10.



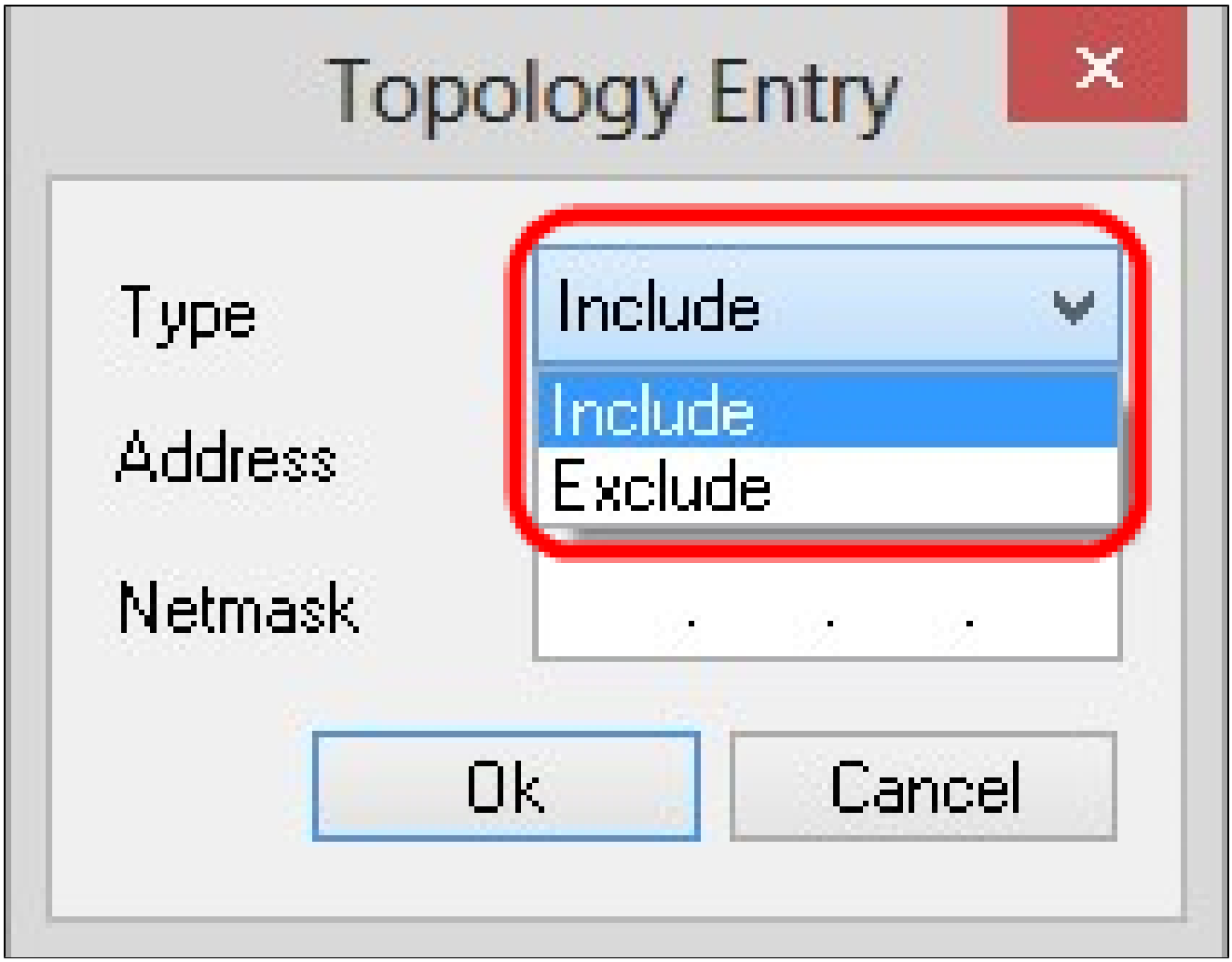
Étape 5. Cliquez sur Add pour ajouter une entrée de topologie dans la table. La fenêtre Topology Entry s'affiche.



Étape 6. Dans la liste déroulante Type, sélectionnez l'option appropriée.

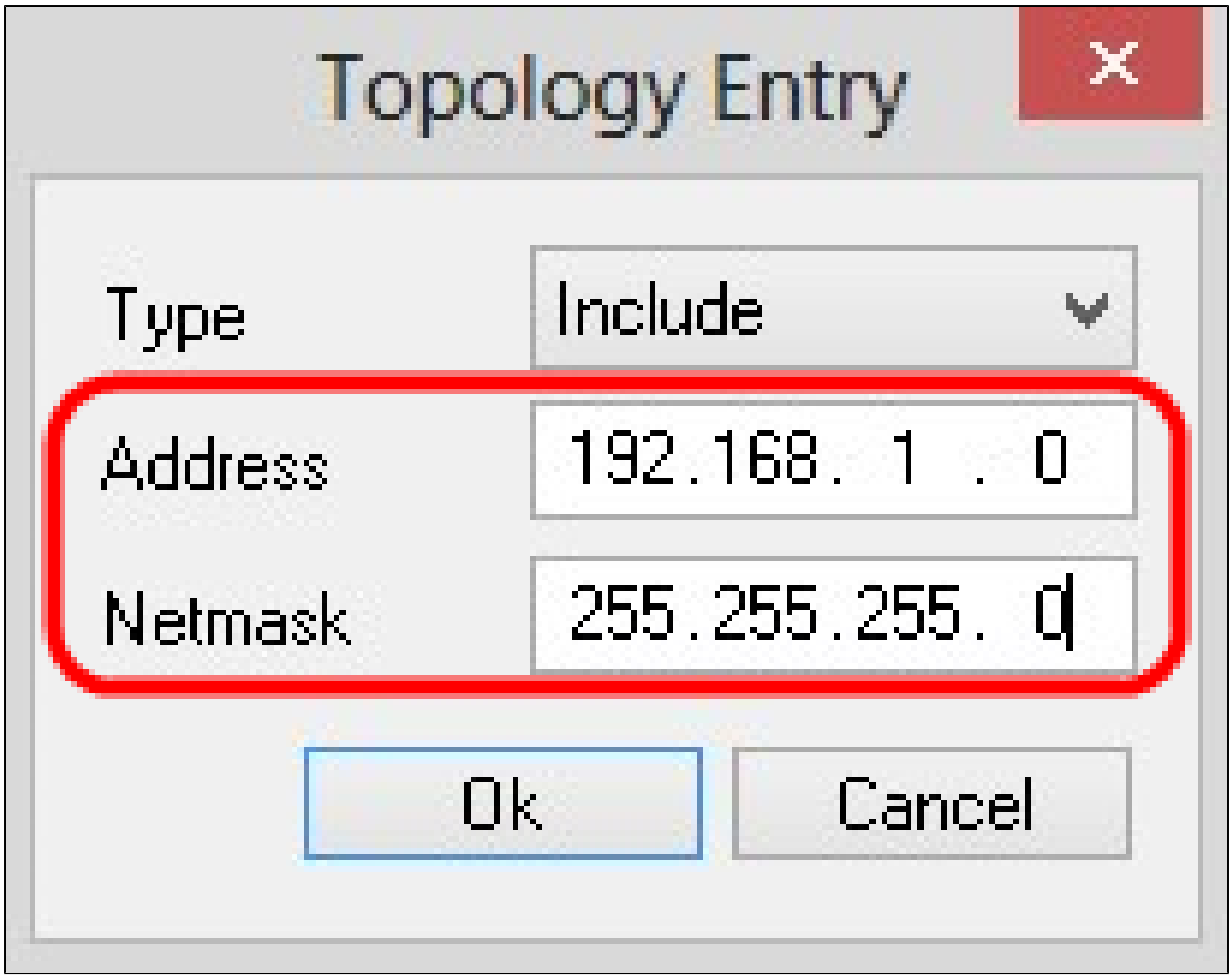
· Include : le réseau est accessible via une passerelle VPN.

· Exclure : le réseau est accessible via la connectivité locale.

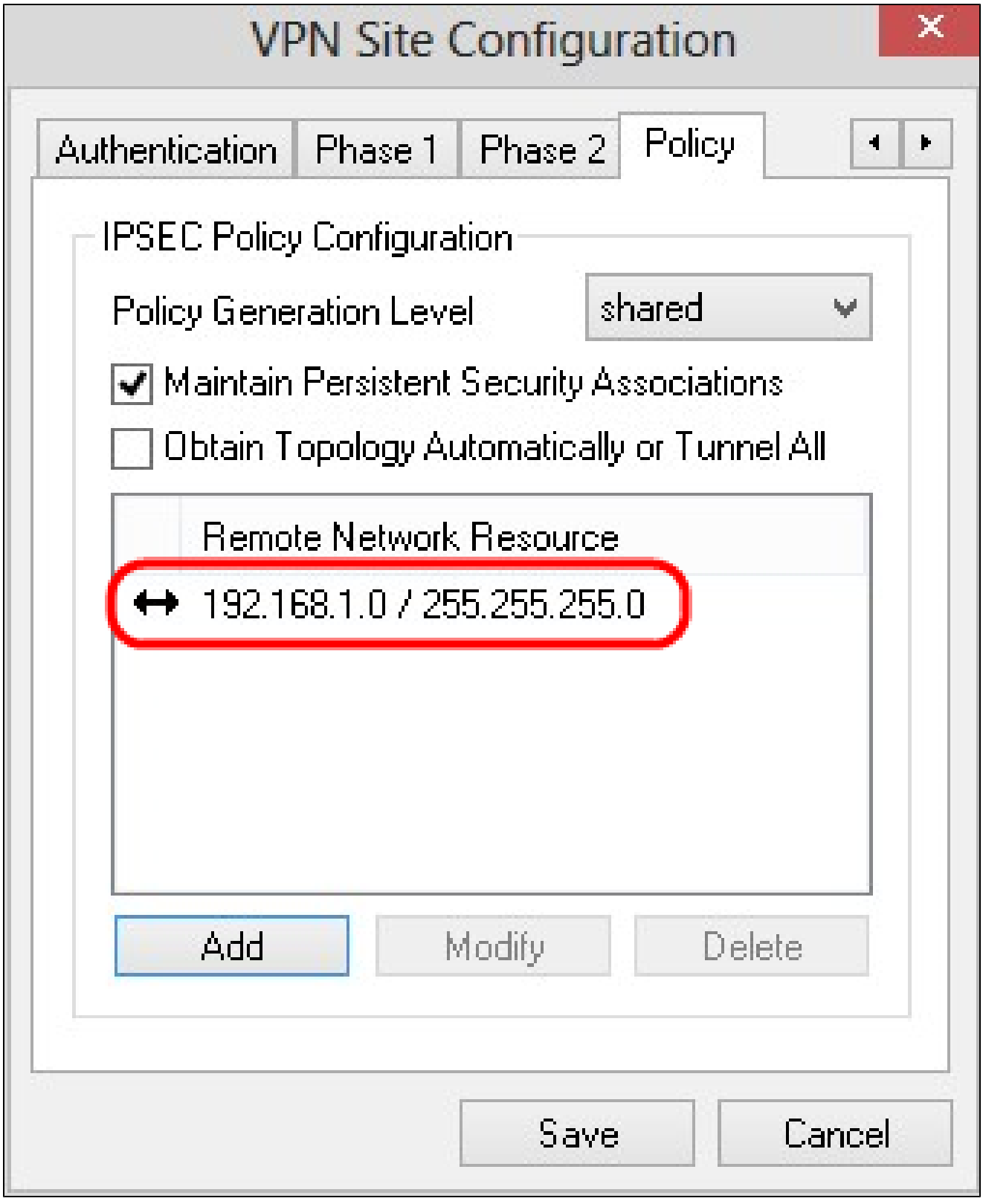


Étape 7. Dans le champ Address, saisissez l'adresse IP du RV0XX.

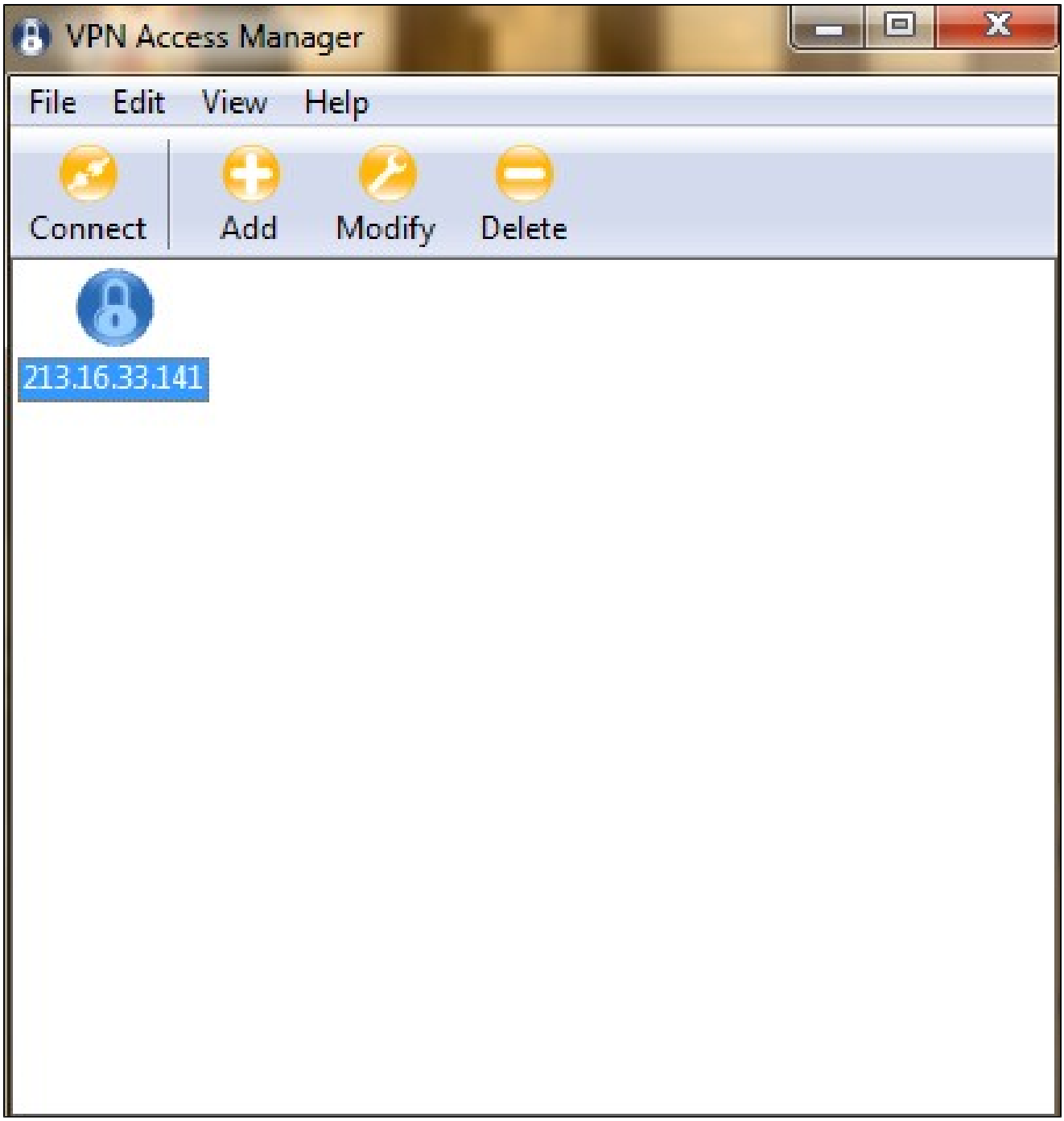
Étape 8. Dans le champ Netmask, saisissez l'adresse de masque de sous-réseau du périphérique.



Étape 9. Click OK. L'adresse IP et l'adresse de masque de sous-réseau du routeur RV0XX sont affichées dans la liste des ressources du réseau distant.



Étape 10. Cliquez sur Save, ce qui ramène l'utilisateur à la fenêtre VPN Access Manager où la nouvelle connexion VPN est affichée.

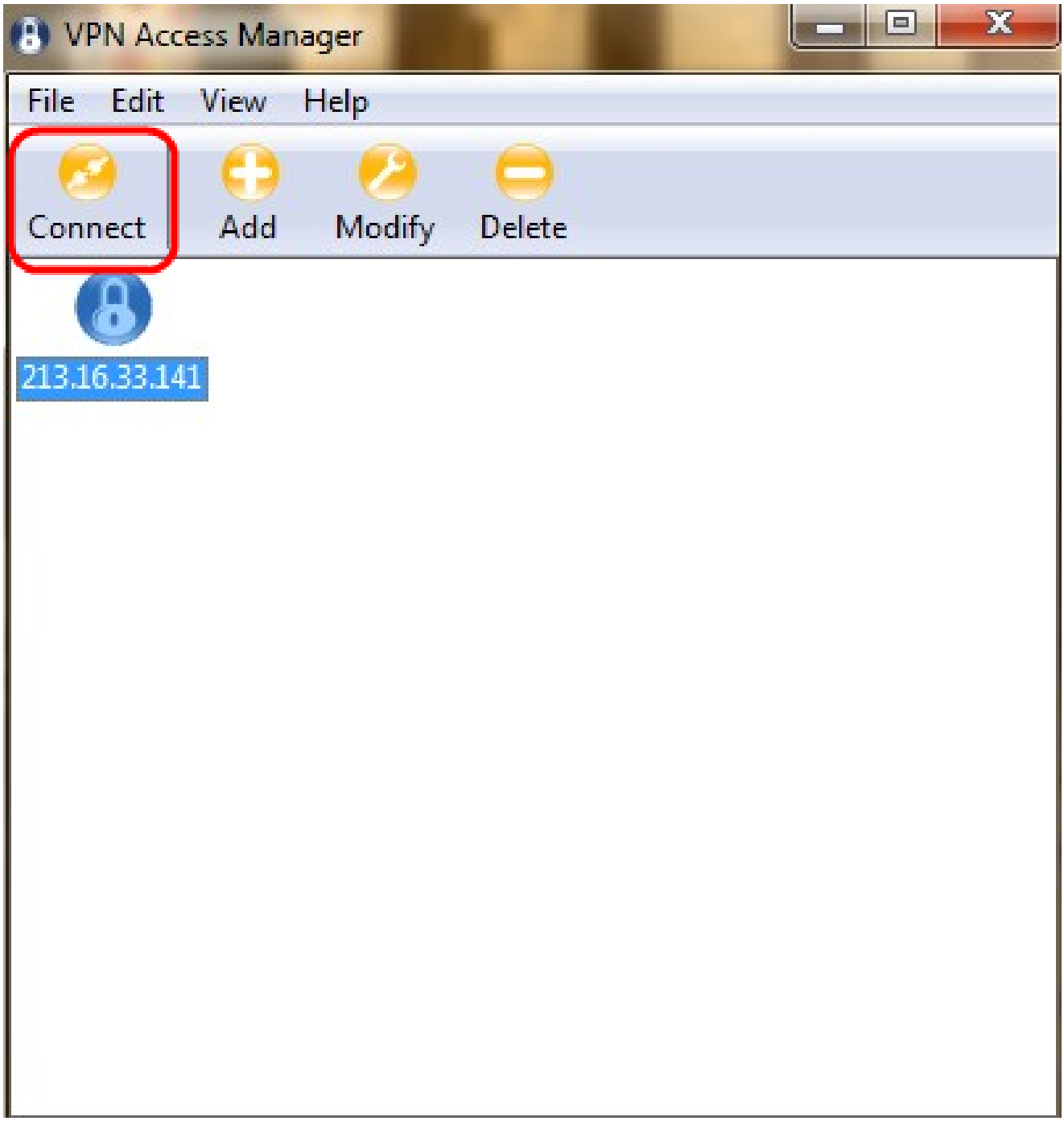


Connecter

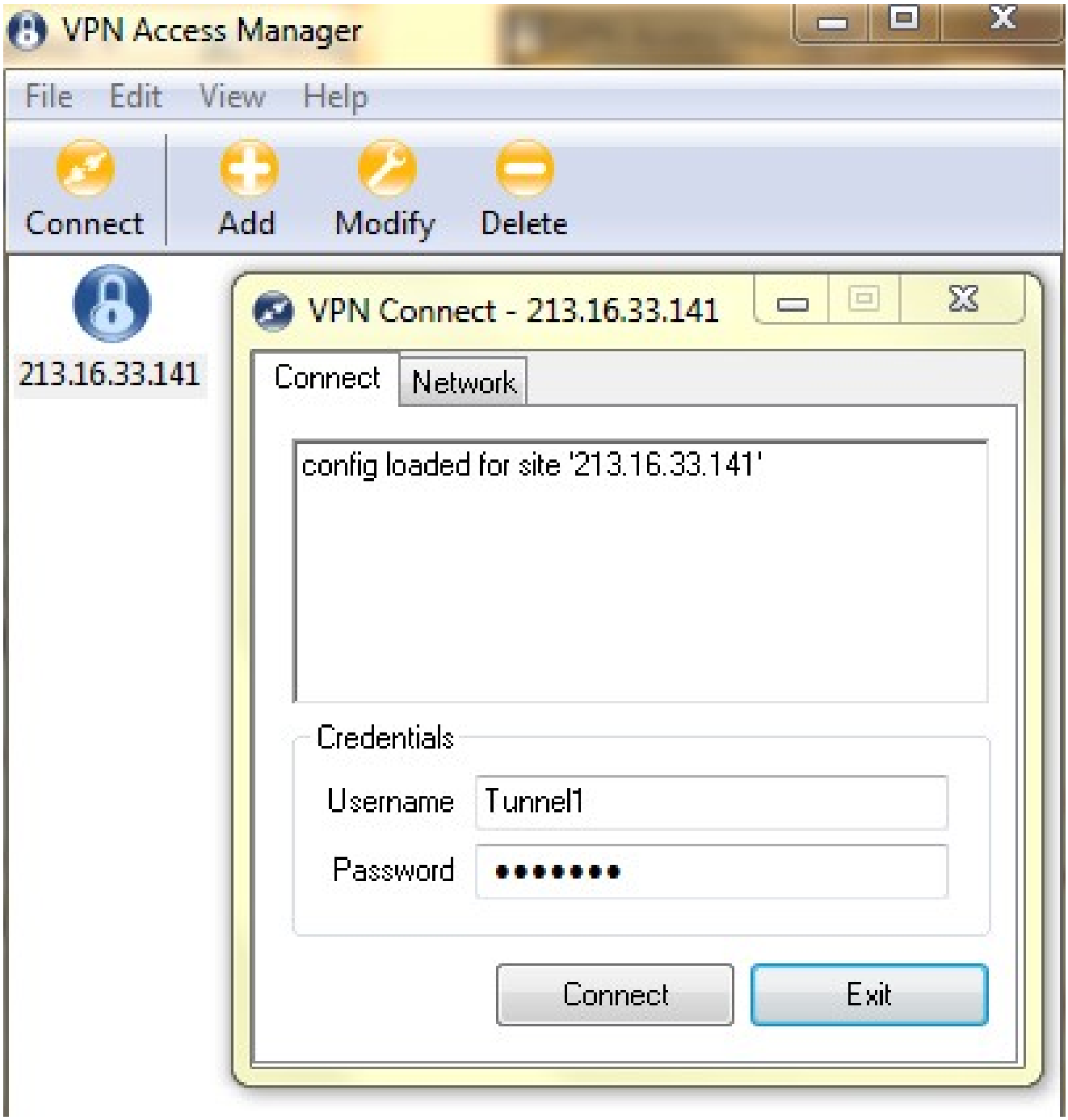
Cette section explique comment configurer la connexion VPN une fois tous les paramètres configurés. Les informations de connexion requises sont les mêmes que l'accès client VPN configuré sur le périphérique.

Étape 1. Cliquez sur la connexion VPN souhaitée.

Étape 2. Cliquez sur Connect.



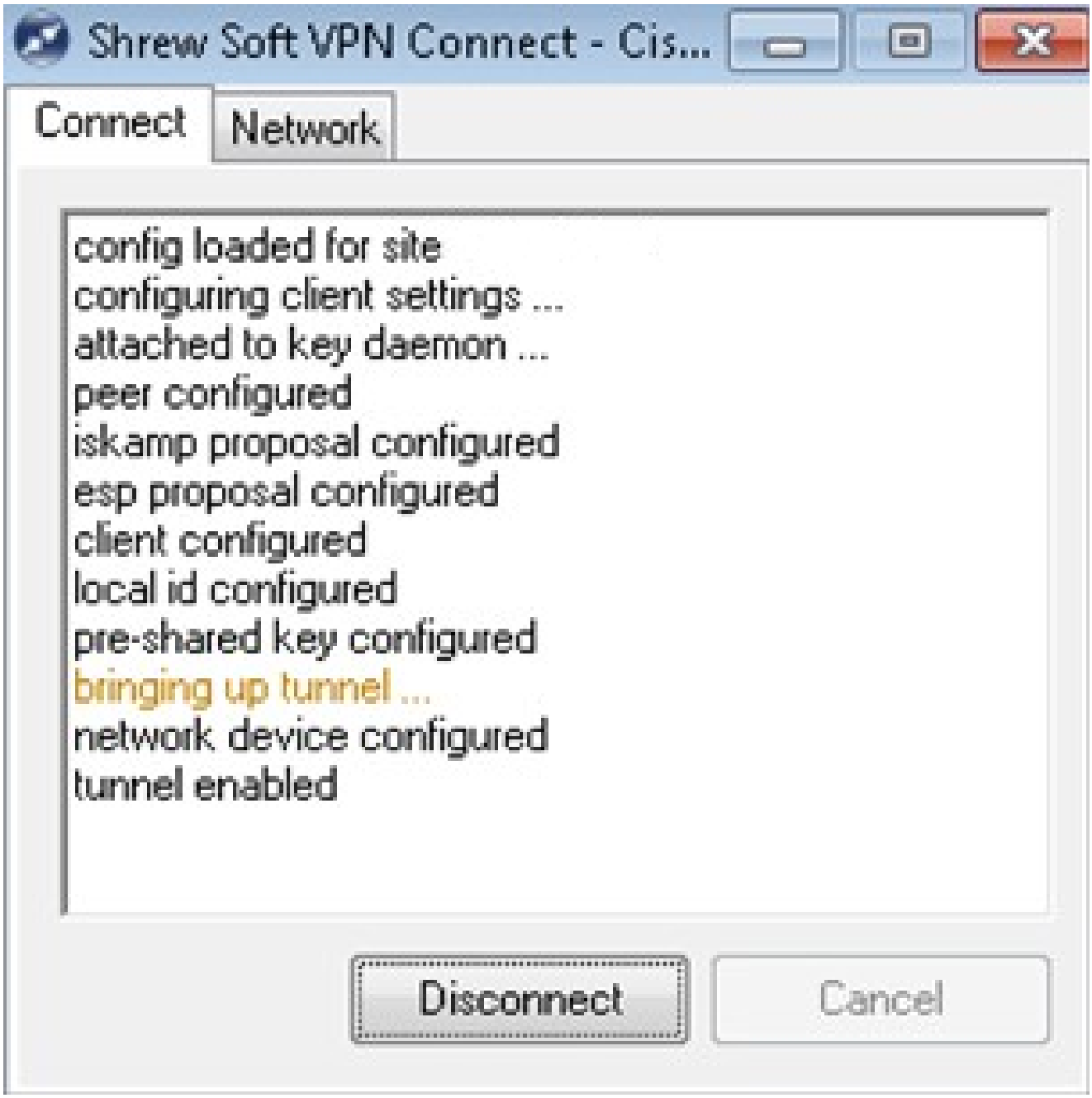
La fenêtre VPN Connect apparaît :



Étape 3. Saisissez le nom d'utilisateur du VPN dans le champ Username.

Étape 4. Saisissez le mot de passe du compte d'utilisateur VPN dans le champ Password.

Étape 5. Cliquez sur Connect. La fenêtre Shrew Soft VPN Connect apparaît :



Étape 6. (Facultatif) Pour désactiver la connexion, cliquez sur Disconnect.

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.