WindowsをRV042、RV042G、およびRV082 VPNルータでのShrew VPN Clientの設定

目的

バーチャルプライベートネットワーク(VPN)は、リモートユーザがインターネット経由でプライベートネットワークに仮想的に接続するための方法です。クライアントからゲートウェイへのVPNは、VPNクライアントソフトウェアを使用して、ユーザのデスクトップまたはラップトップをリモートネットワークに接続します。クライアントからゲートウェイへのVPN接続は、オフィスのネットワークにリモートから安全に接続したいリモートの従業員に役立ちます。Shrew VPN Clientは、リモートホストデバイスに設定されたソフトウェアで、簡単で安全なVPN接続を提供します。

このドキュメントの目的は、RV042、RV042G、またはRV082 VPNルータに接続するコンピュータにShrew VPN Clientを設定する方法を示すことです。

注：このドキュメントでは、WindowsコンピュータにShrew VPN Clientがすでにダウンロードされていることを前提としています。そうでない場合は、Shrew VPNの設定を開始する前に、クライアントからゲートウェイへのVPN接続を設定する必要があります。クライアントからゲートウェイへのVPNの設定方法の詳細については、『RV042、RV042G、およびRV082 VPNルータでのVPNクライアント用のリモートアクセストンネル（クライアントからゲートウェイ）のセットアップ』を参照してください。

適用可能なデバイス

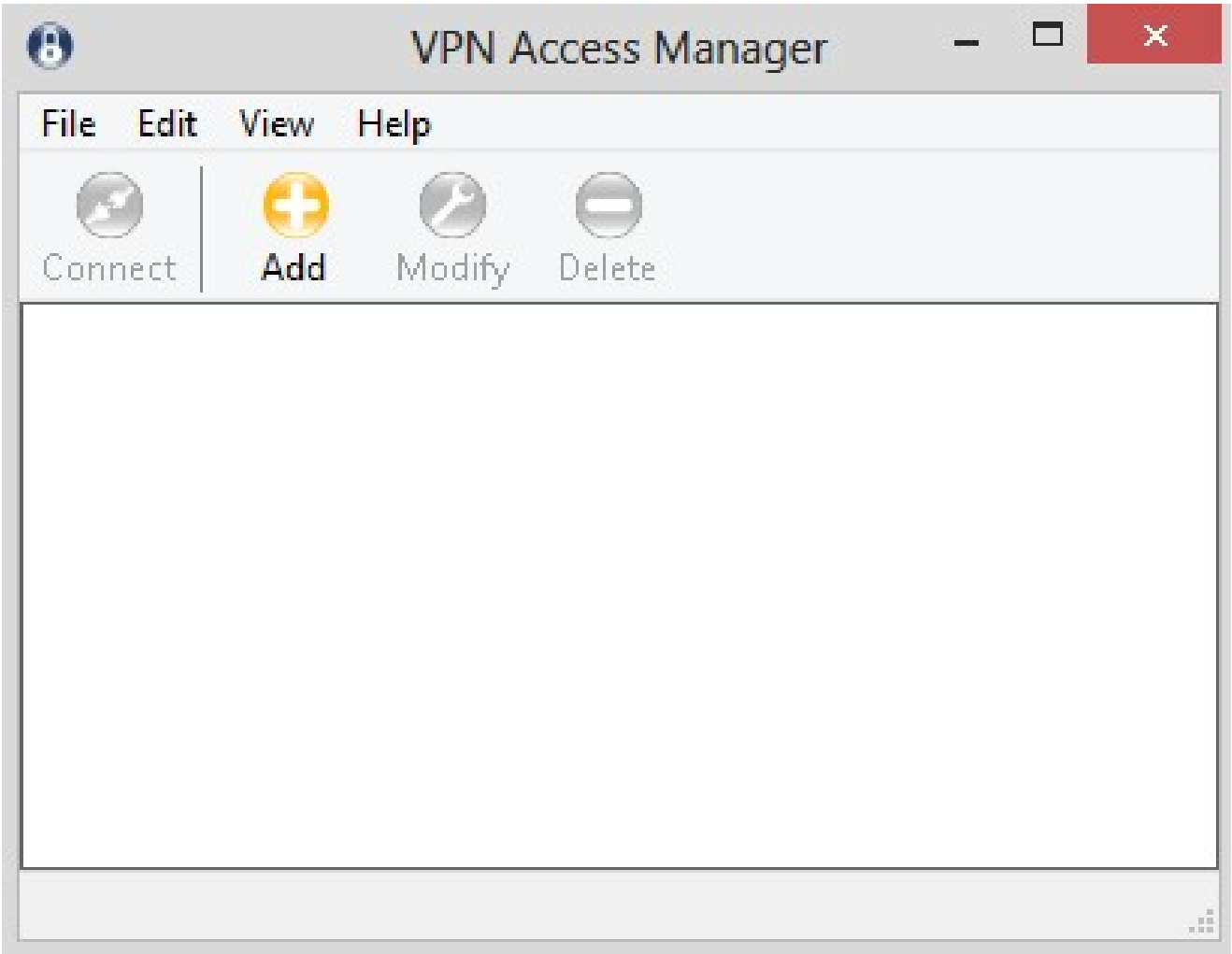
- RV042
- RV042G
- RV082

[Software Version]

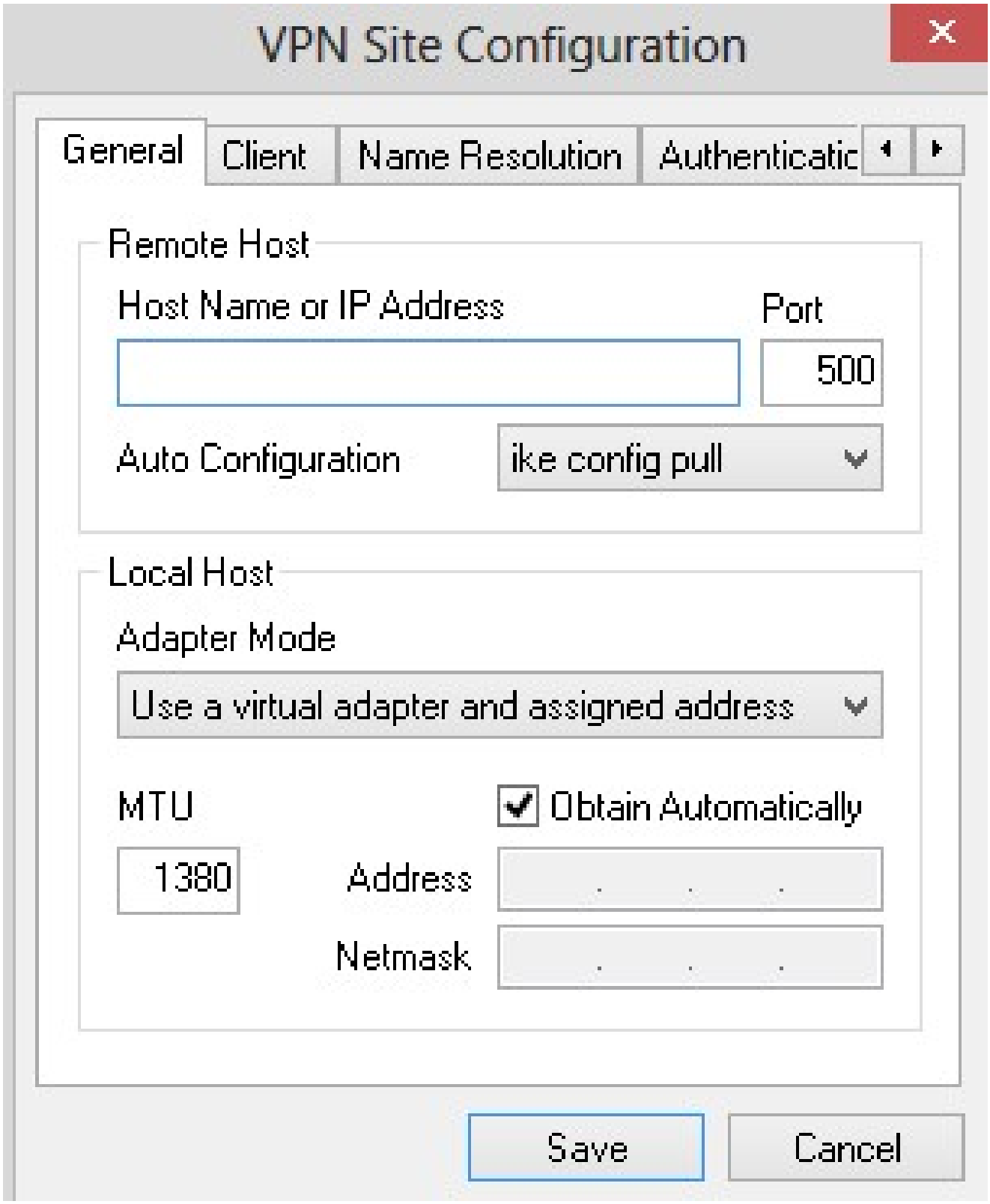
- v4.2.2.08

WindowsでのShrew VPN Client接続の設定

ステップ 1：コンピュータでShrew VPN Clientプログラムをクリックして開きます。Shrew Soft VPN Access Managerウィンドウが開きます。

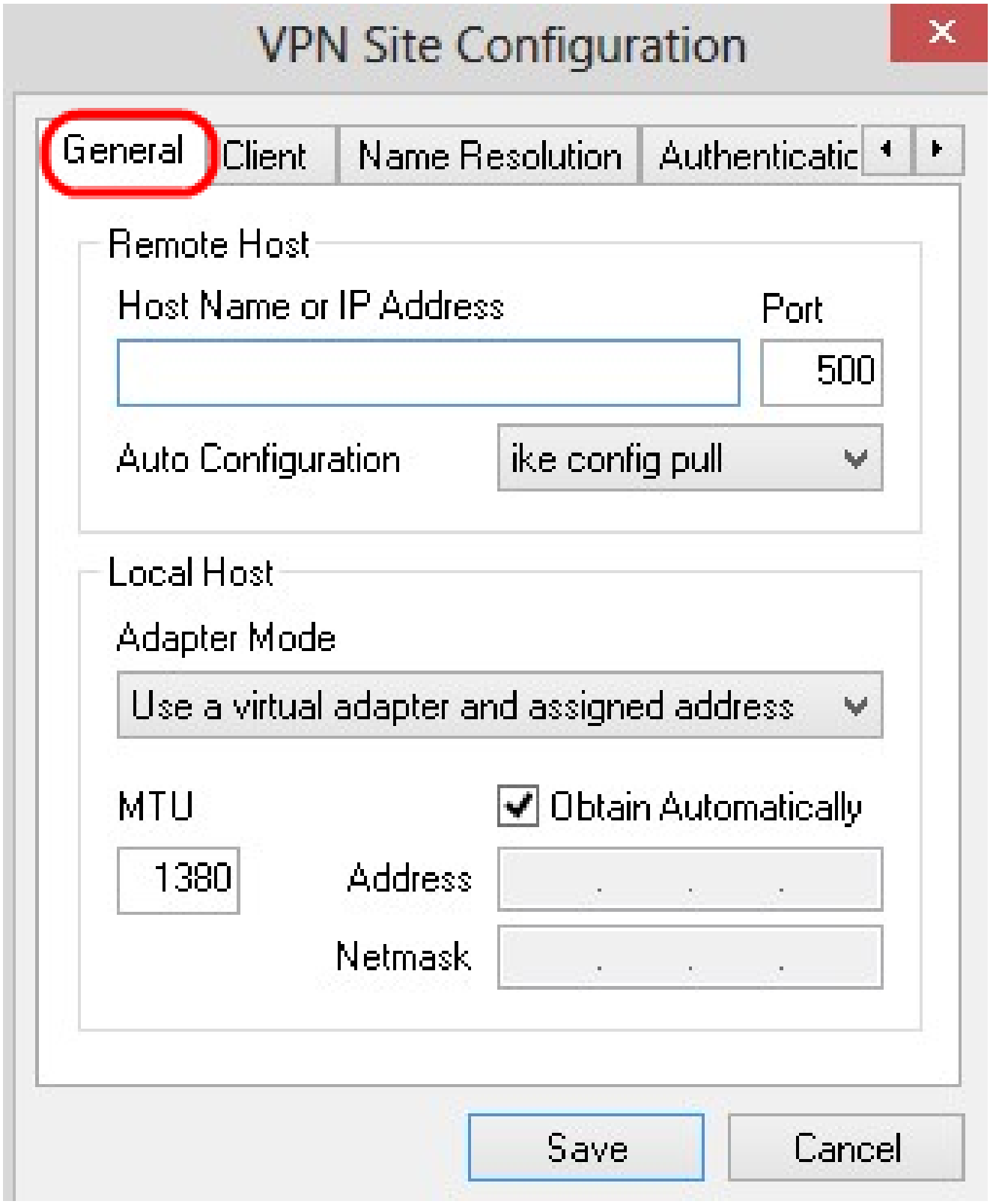


ステップ 2：[Add] をクリックします。VPN Site Configurationウィンドウが表示されます。



一般的な設定

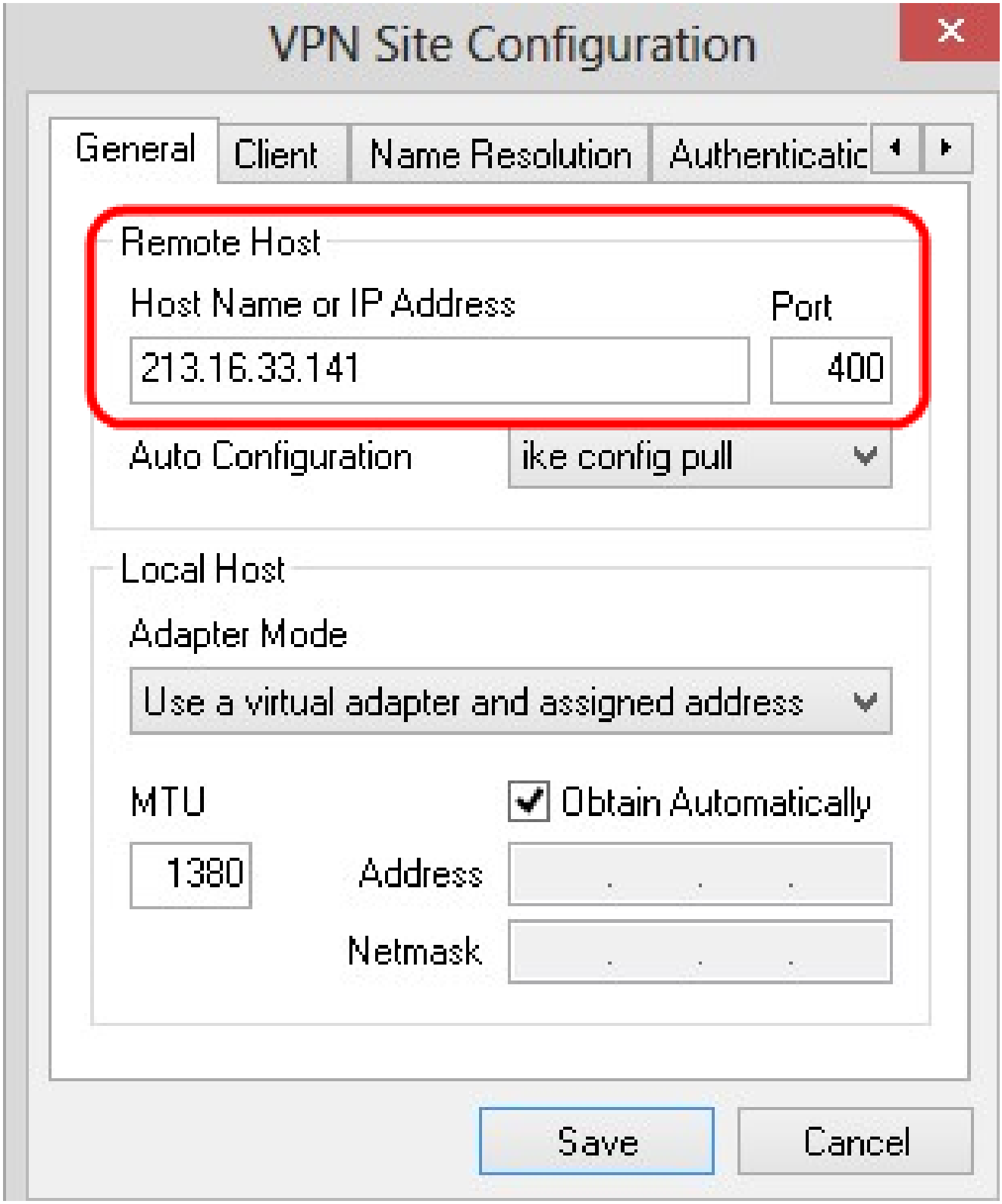
ステップ 1：[General]タブをクリックします



注：「General」セクションは、リモートおよびローカルホストのIPアドレスを設定するために使用します。これらは、クライアントからゲートウェイへの接続のネットワークパラメータを定義するために使用されます。

ステップ 2：Host Name or IP Addressフィールドに、設定されたWANのIPアドレスであるリモートホストのIPアドレスを入力します。

ステップ 3：Portフィールドに、接続に使用するポート番号を入力します。図の例で使用されているポート番号は400です。



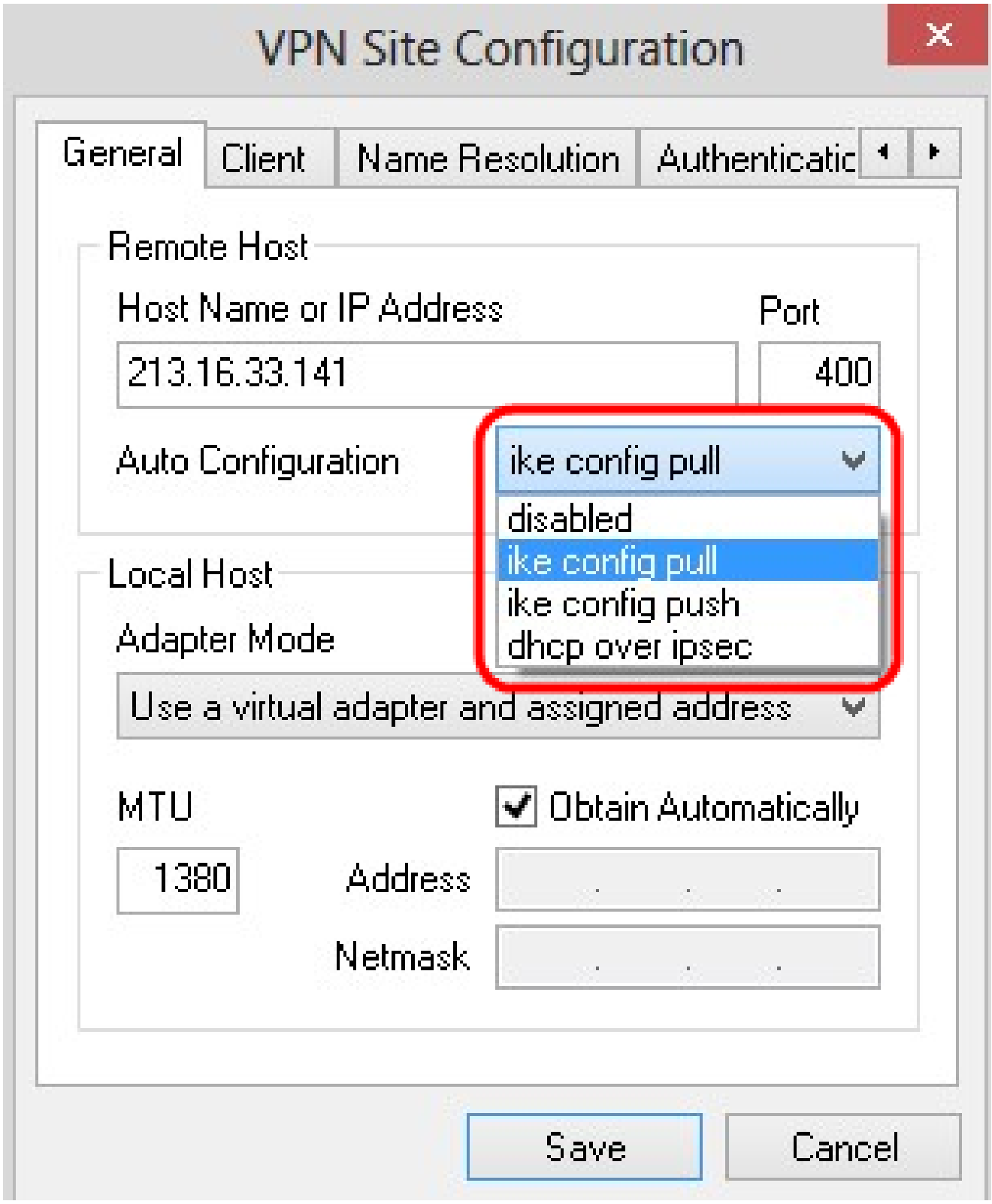
ステップ 4：Auto Configurationドロップダウンリストから、必要な設定を選択します。

- Disabled:disabledオプションは、自動クライアント設定を無効にします。

・ IKE Config Pull：クライアントによるコンピュータからの設定要求を許可します。コンピュータによるPullメソッドのサポートにより、要求はクライアントでサポートされている設定のリストを返します。

・ IKE Config Push：設定プロセスを通じて設定をクライアントに提供する機会をコンピュータに与えます。コンピュータによるPushメソッドのサポートにより、要求はクライアントでサポートされている設定のリストを返します。

・ DHCP Over IPSec:DHCP over IPSecを使用してコンピュータに設定を要求する機会をクライアントに与えます。

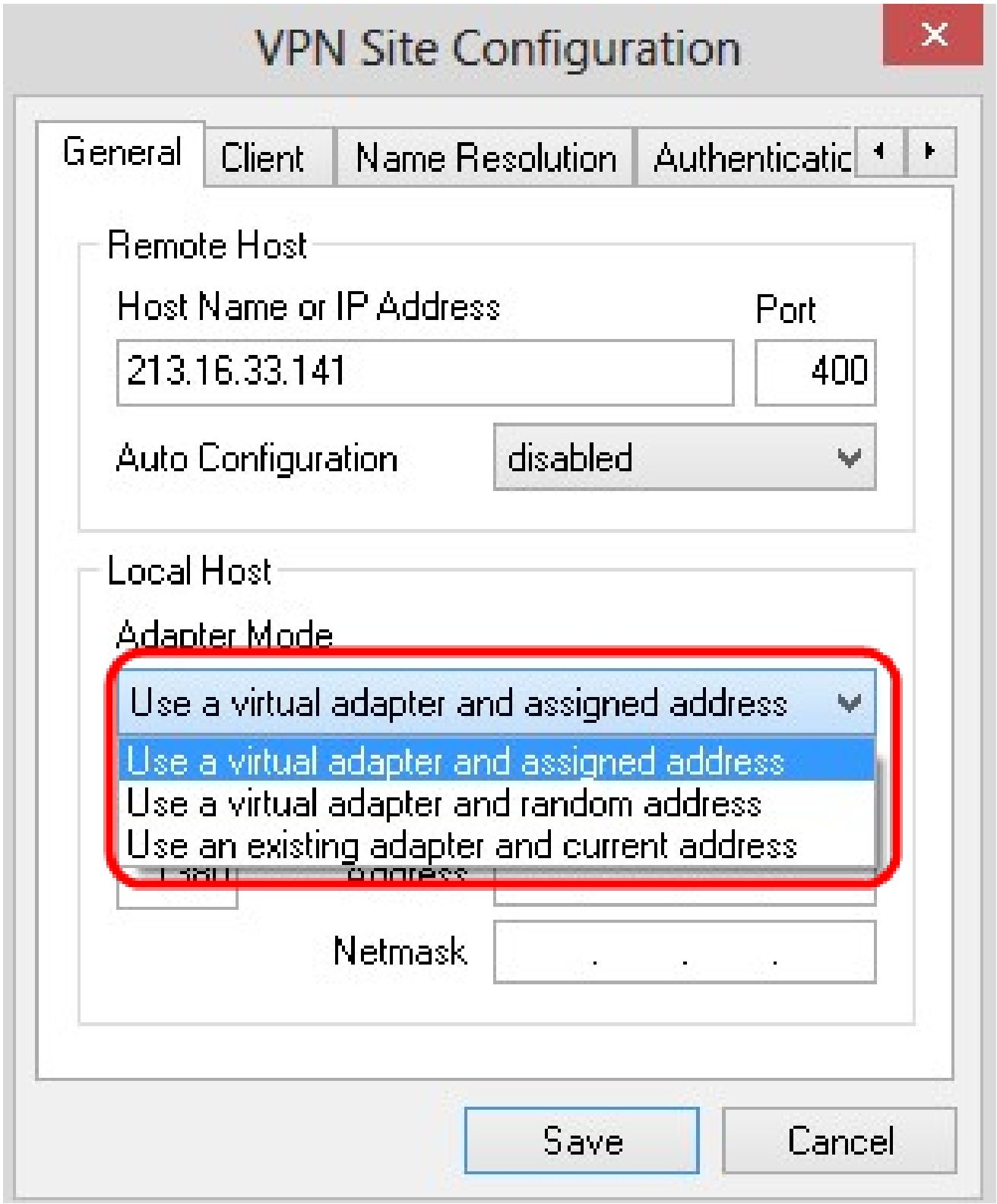


ステップ 5：Adapter Modeドロップダウンリストから、Auto Configurationに基づいてローカルホストに対する適切なアダプタモードを選択します。

・ Use a Virtual Adapter and Assigned Address：クライアントが、指定されたアドレスを持つ仮想アダプタを使用できるようにします。

・ Use a Virtual Adapter and Random Address：クライアントがランダムアドレスの仮想アダプタを使用できるようにします。

・既存のアダプタと現在のアドレスを使用 – 既存のアダプタとそのアドレスを使用します。追加の情報を入力する必要はありません。

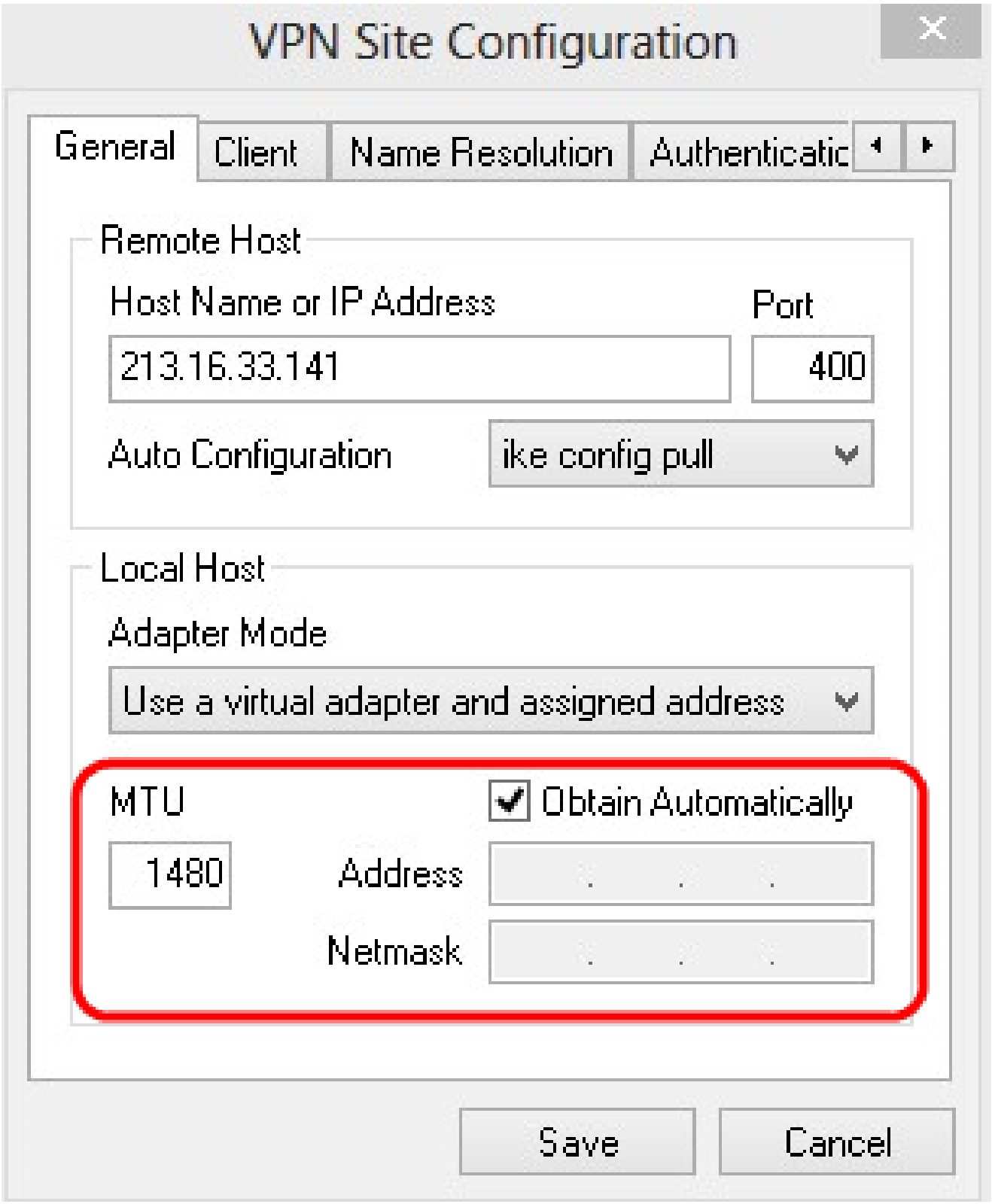


手順 6：ステップ5のAdapter Modeドロップダウンリストから**Use a Virtual Adapter and Assigned Address**を選択した場合は、MTUフィールドに最大伝送ユニット(MTU)を入力します。最大伝送ユニット(MTU)は、IPフラグメンテーションの問題の解決に役立ちます。デフォルト値は 1380 です。

ステップ7: (オプション) DHCPサーバからアドレスとサブネットマスクを自動的に取得するには、**Obtain Automatically**チェックボックスにチェックマークを付けます。このオプションは、一部の設定では使用できません。

ステップ 8：ステップ5のAdapter Modeドロップダウンリストで**Use a Virtual Adapter and Assigned Address**を選択した場合は、Addressフィールドにリモートクライアントの**IP**アドレスを入力します。

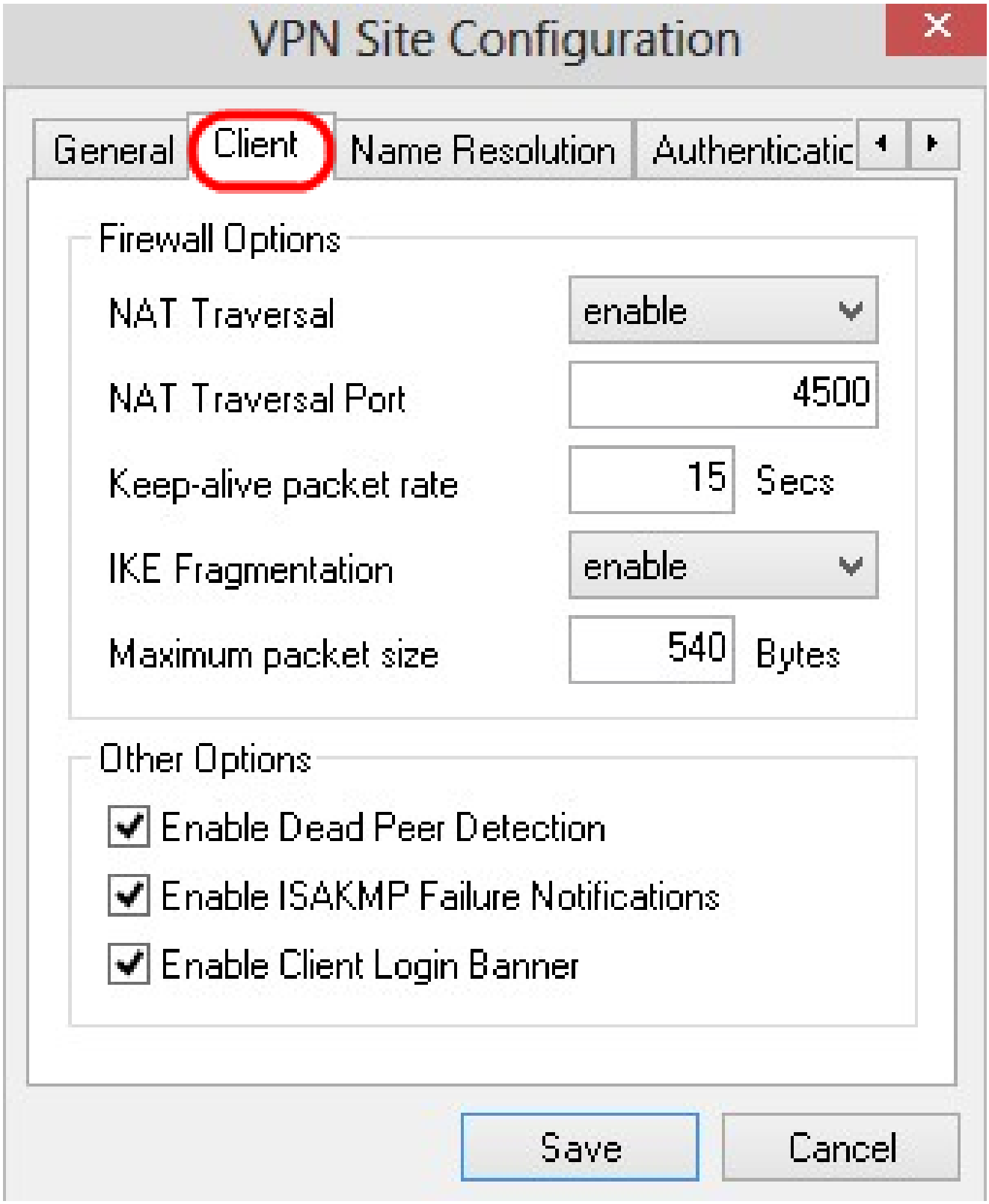
ステップ 9：ステップ5のAdapter Modeドロップダウンリストで**Use a Virtual Adapter and Assigned Address**を選択した場合は、Netmaskフィールドにリモートクライアントの**IP**アドレスのサブネットマスクを入力します。



ステップ 10：[Save] をクリックして、設定を保存します。

クライアントの設定

ステップ 1：Clientタブをクリックします。



注：「クライアント」セクションでは、ファイアウォールオプション、デッドピア検出、およびISAKMP(Internet Security Association and Key Management Protocol)障害通知を設定できます。この設定では、手動で設定する設定オプションと、自動的に取得する設定オプションを定義します。

ステップ 2：NAT Traversalドロップダウンリストから、適切なNAT(Network Address

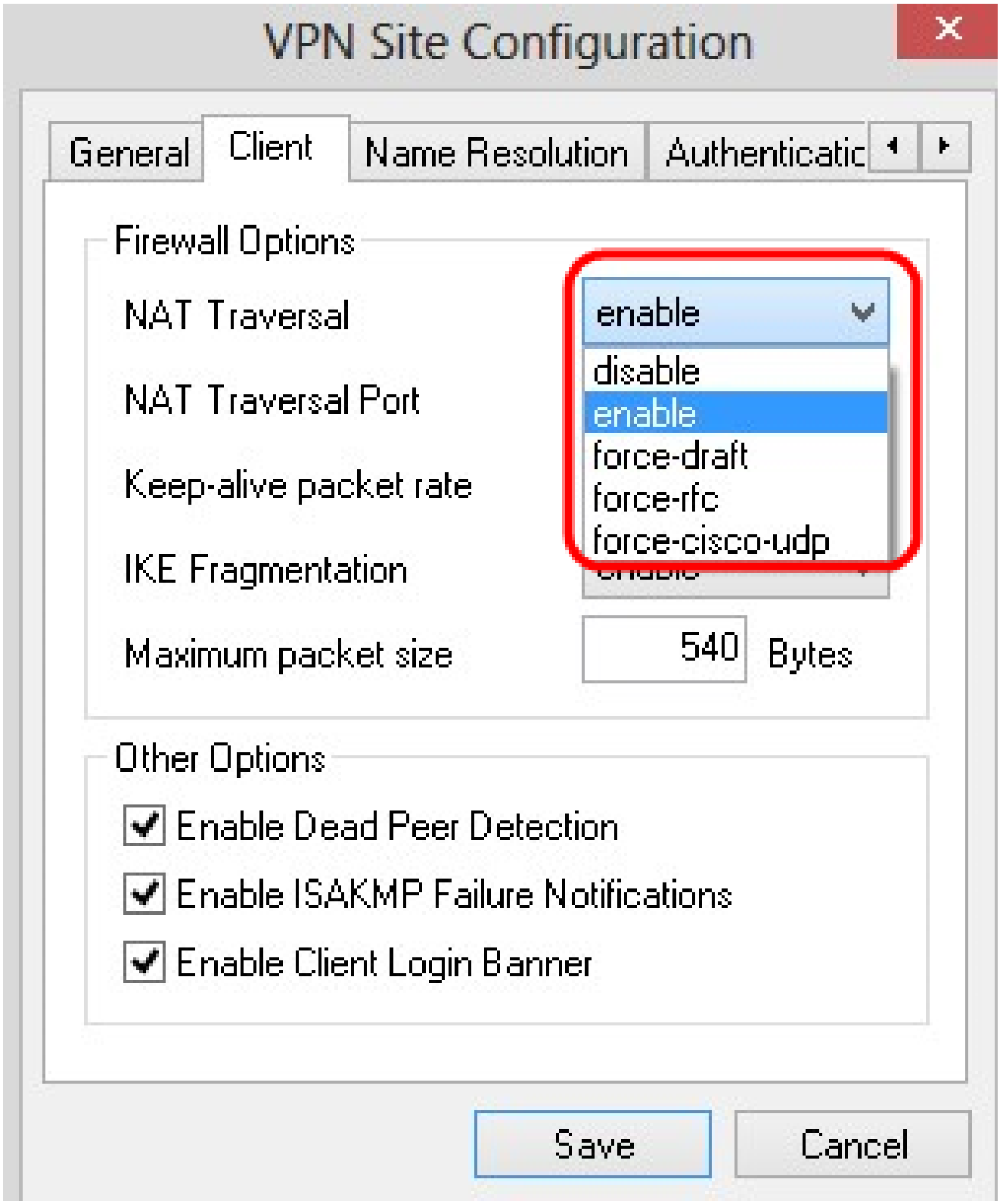
Translation)トラバーサルオプションを選択します。

・ Disable:NATプロトコルが無効です。

・ Enable:IKEフラグメンテーションは、ゲートウェイがネゴシエーションを通じてサポートを示す場合にのみ使用されます。

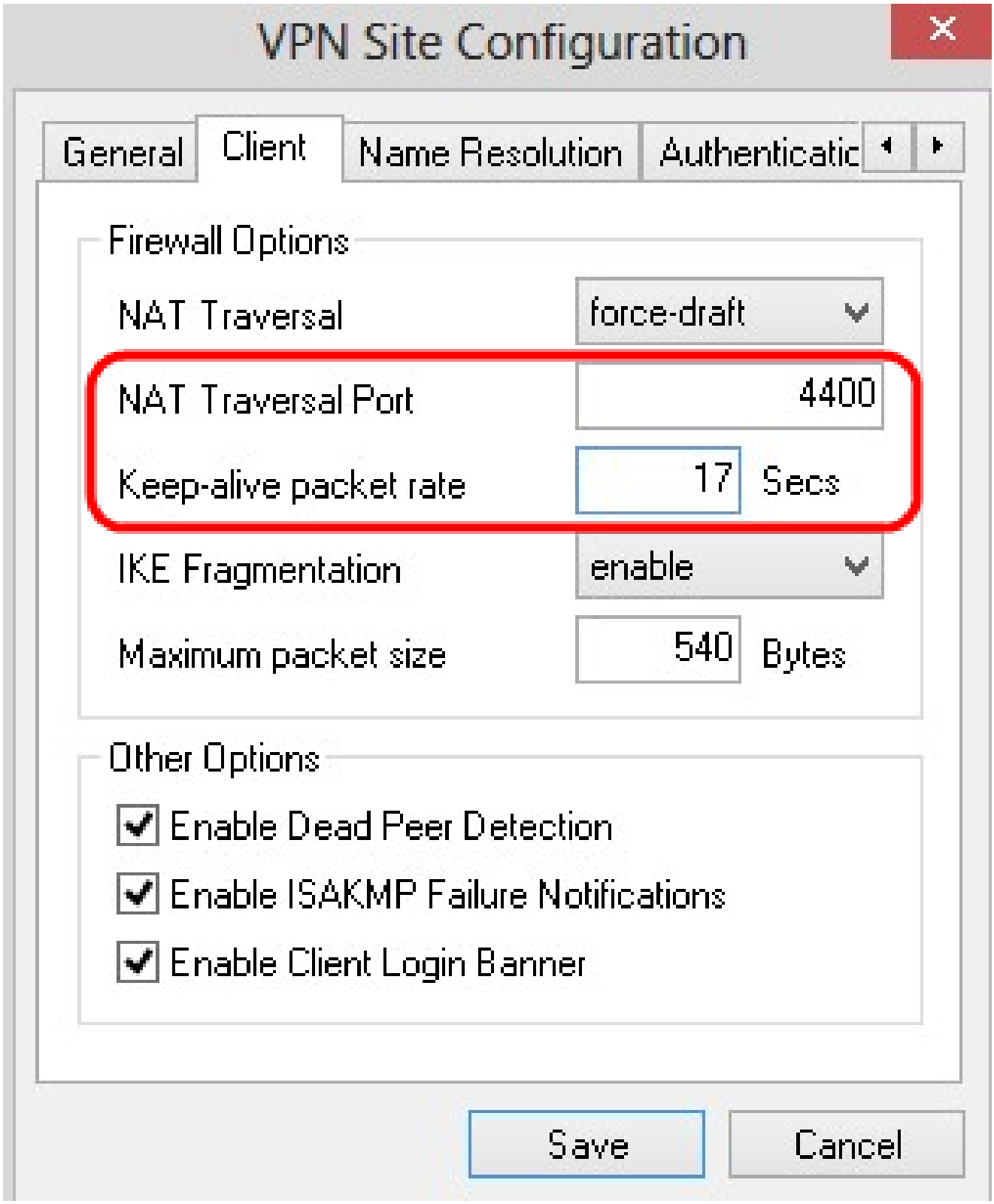
・ Force Draft:NATプロトコルのドラフトバージョン。これは、ゲートウェイがネゴシエーションまたはNATの検出によってサポートを示す場合に使用されます。

・ Force RFC:NATプロトコルのRFCバージョン。これは、ゲートウェイがネゴシエーションまたはNATの検出によってサポートを示す場合に使用されます。



ステップ 3：NAT Traversal PortフィールドにNATのUDPポートを入力します。デフォルト値は 4500 です。

ステップ 4：Keep-alive packet rateフィールドに、キープアライブパケットが送信されるレートの値を入力します。この値は秒単位で測定されます。デフォルト値は 30 秒です。

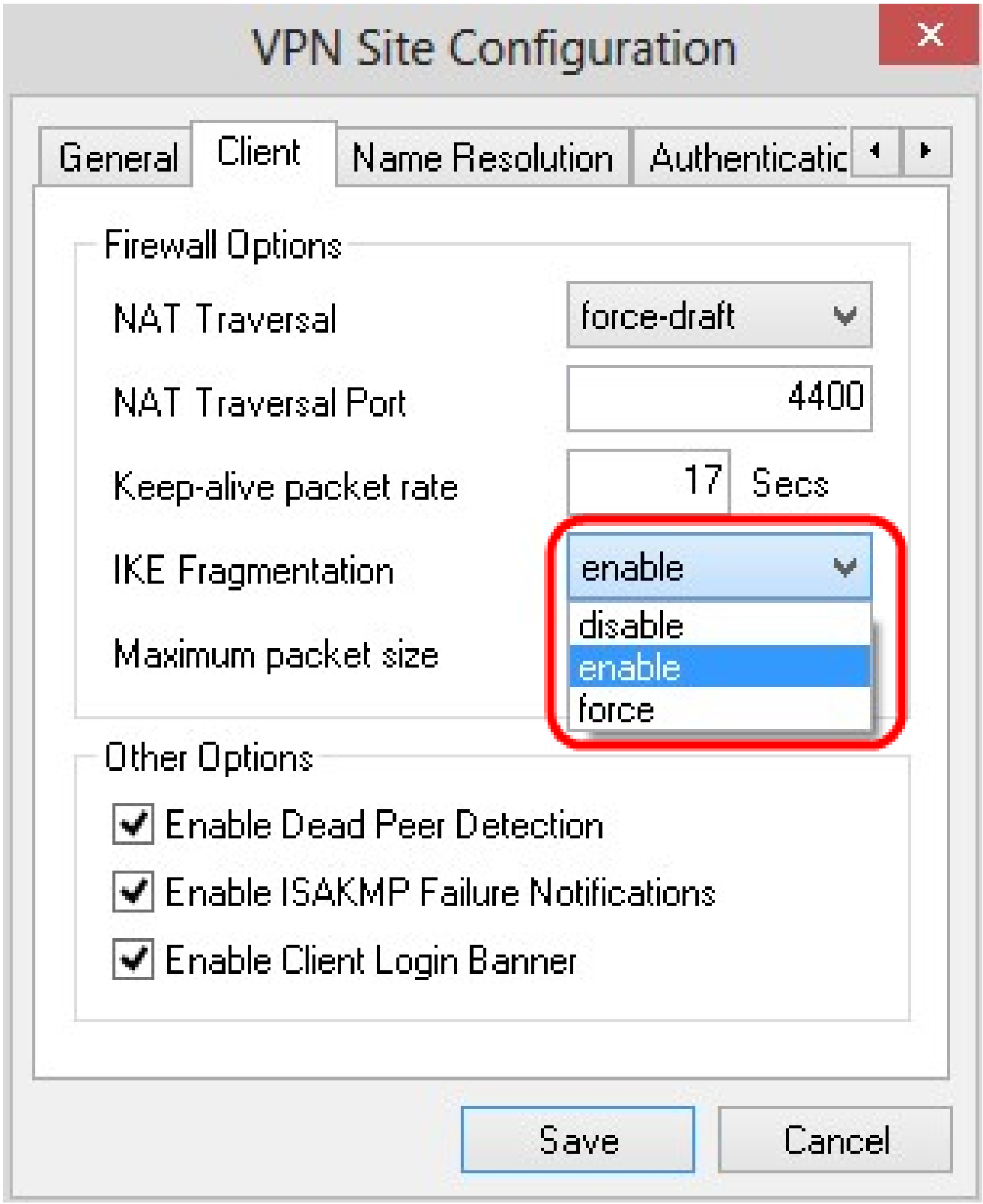


ステップ 5：IKE Fragmentationドロップダウンリストで、適切なオプションを選択します。

- Disable:IKEフラグメンテーションは使用されません。
- Enable:IKEフラグメンテーションは、ゲートウェイがネゴシエーションを通じてサポー

トを示す場合にのみ使用されます。

・ Force:IKEフラグメンテーションは、表示または検出に関係なく使用されます。



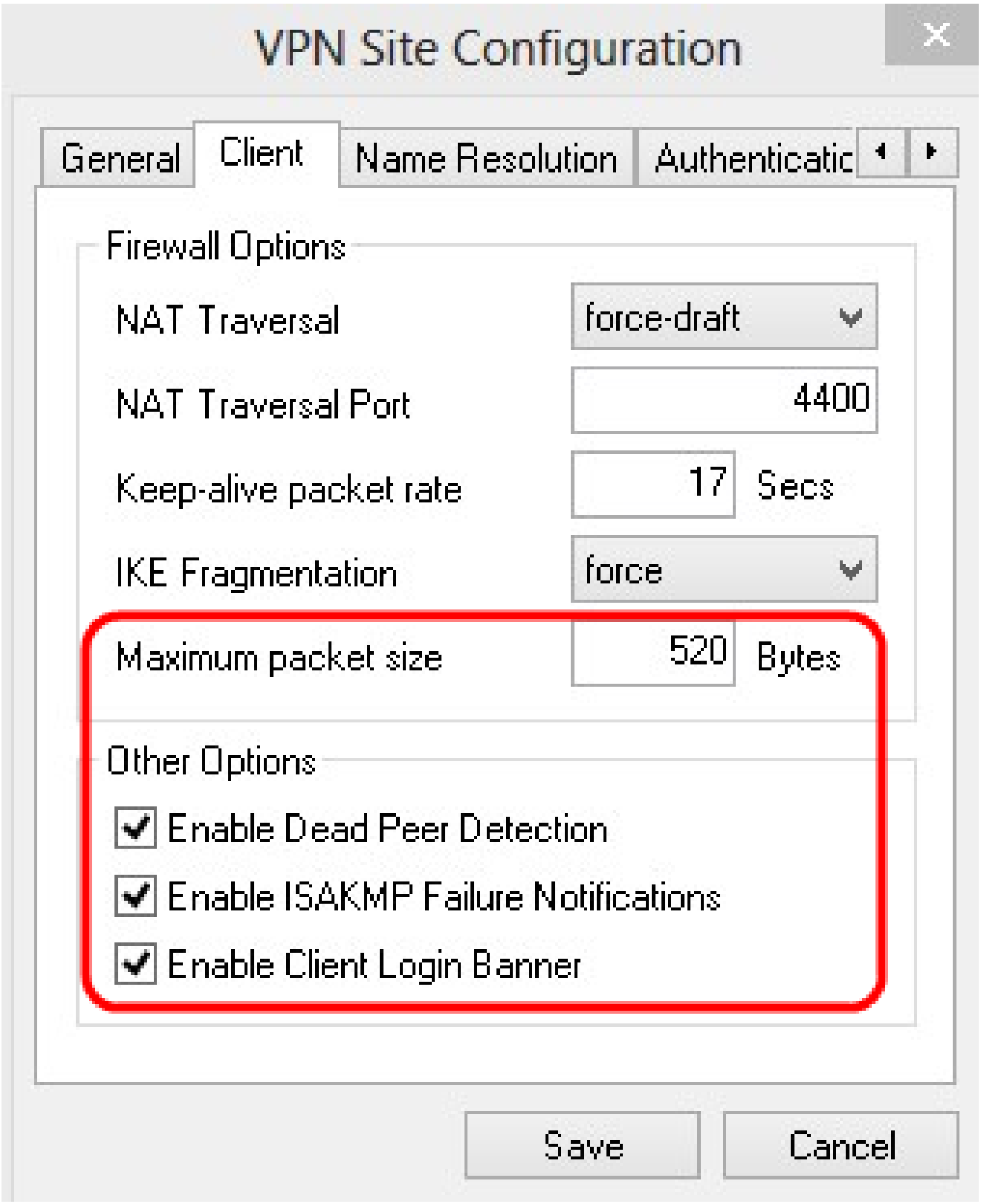
手順 6：最大パケットサイズをMaximum packet sizeフィールドにバイト単位で入力します。パケットサイズが最大パケットサイズよりも大きい場合、IKEフラグメンテーションが実

行されます。デフォルト値は540バイトです。

ステップ7: (オプション) コンピュータとクライアントが相手側が応答できなくなったことを検出できるようにするには、Enable Dead Peer Detectionチェックボックスにチェックマークを入れます。

ステップ8: (オプション) VPN Clientによって障害通知を送信するには、Enable ISAKMP Failure Notificationsチェックボックスにチェックマークを付けます。

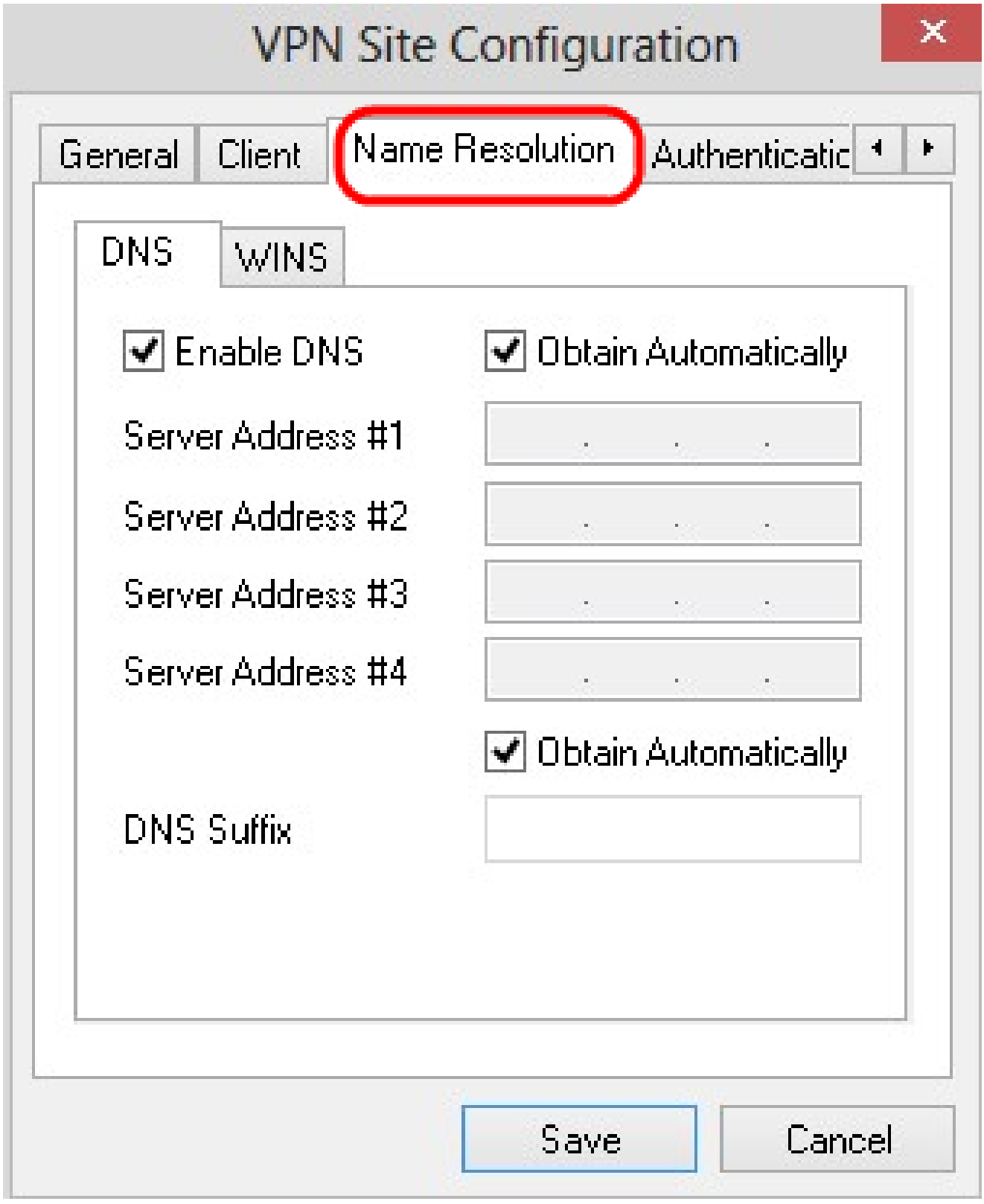
ステップ9: (オプション) ゲートウェイとの接続が確立されたときにクライアントがログインバナーを表示するには、Enable Client Loginチェックボックスにチェックマークを付けます。



ステップ 10：[Save] をクリックして、設定を保存します。

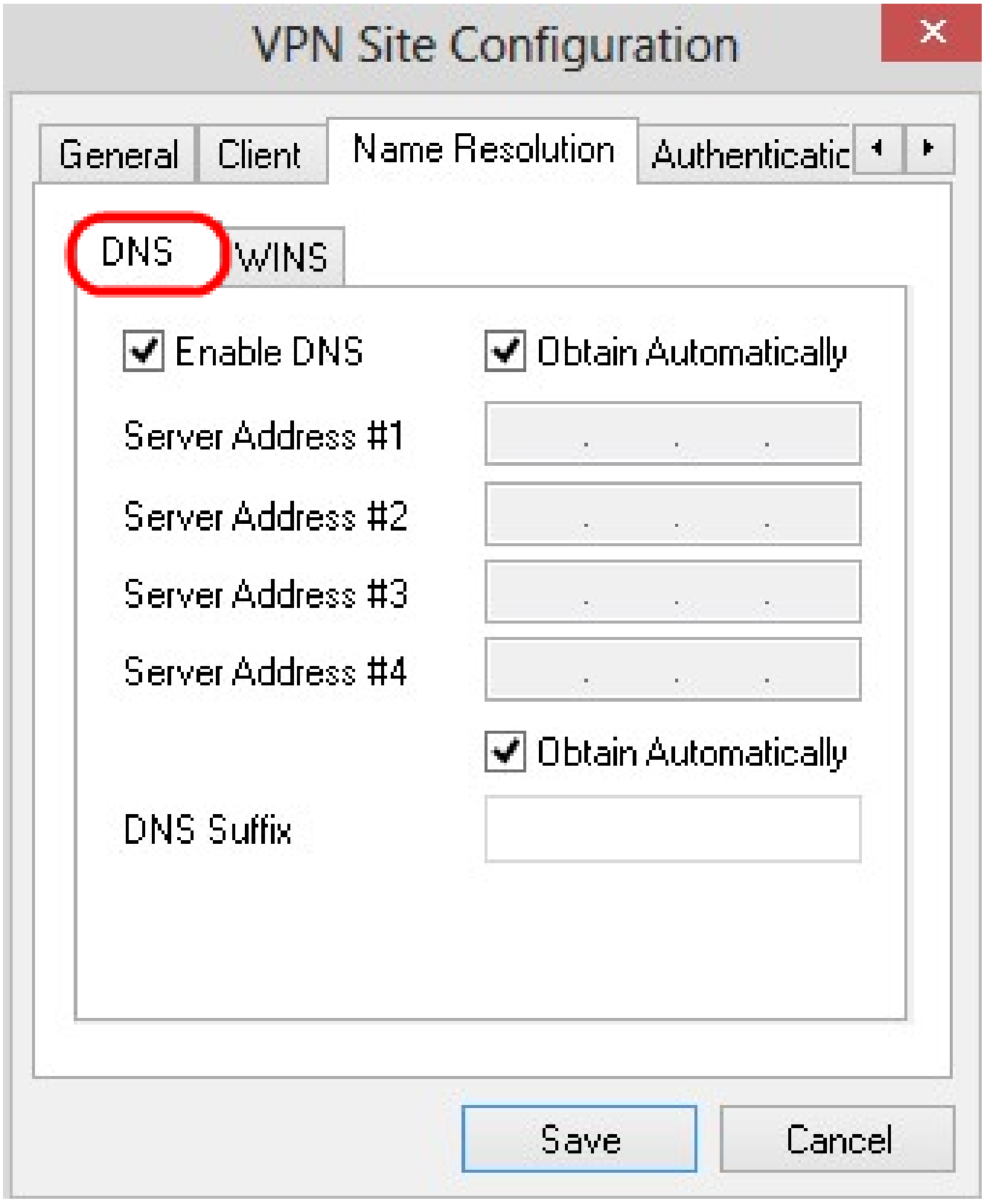
名前解決の設定

ステップ 1：Name Resolutionタブをクリックします。



注： Name Resolutionセクションは、DNS（ドメインネームシステム）とWIN(Windows Internet Name Service)の設定に使用されます。

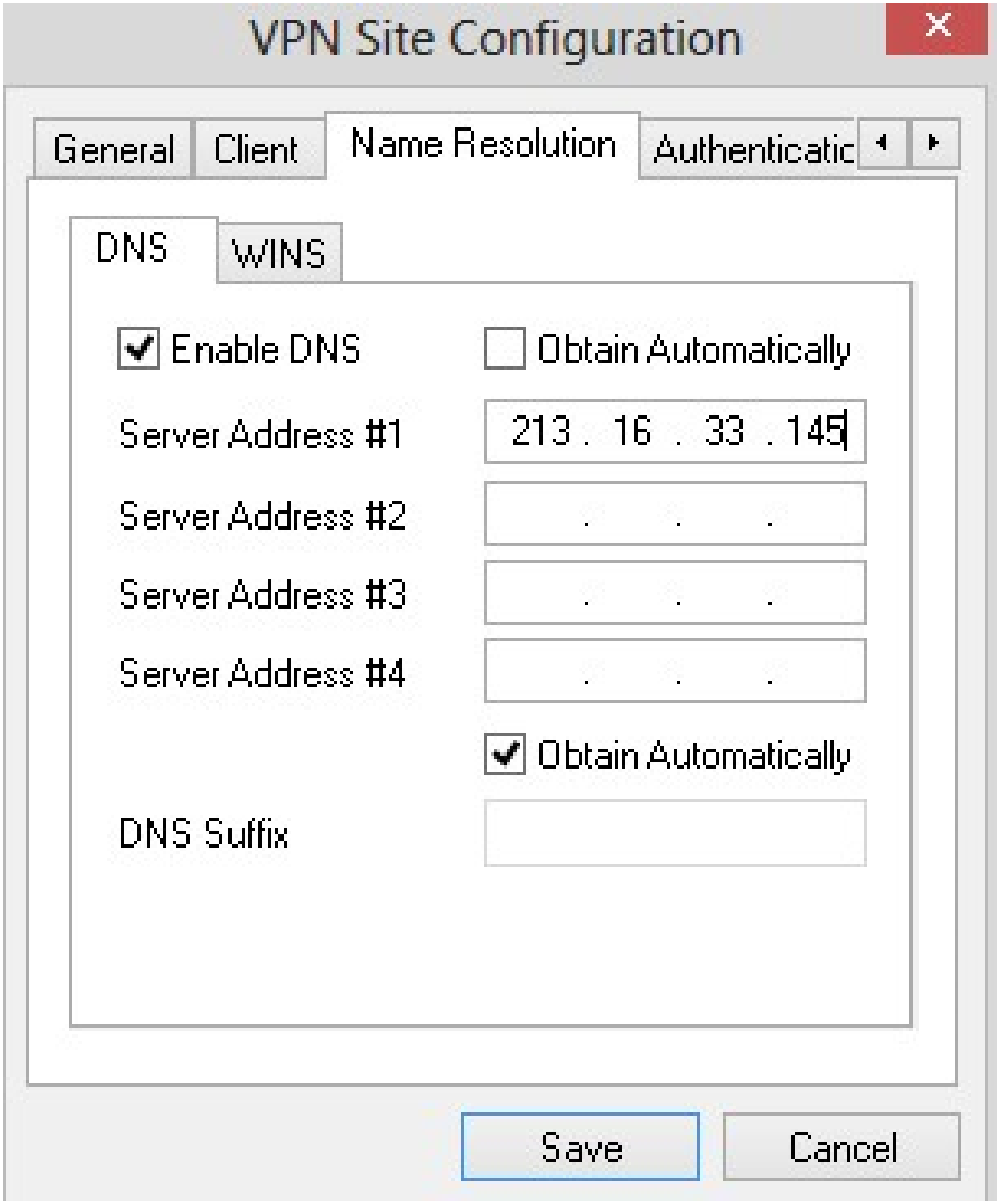
ステップ 2：DNSタブをクリックします。



ステップ 3：ドメインネームシステム(DNS)を有効にするには、Enable DNSにチェックマークを付けます。

ステップ4:（オプション）DNSサーバアドレスを自動的に取得するには、Obtain Automaticallyチェックボックスにチェックマークを付けます。このオプションを選択した場合は、ステップ6に進みます。

ステップ 5：Server Address #1フィールドにDNSサーバアドレスを入力します。別のDNSサーバがある場合は、残りのServer Addressフィールドにそれらのサーバのアドレスを入力します。

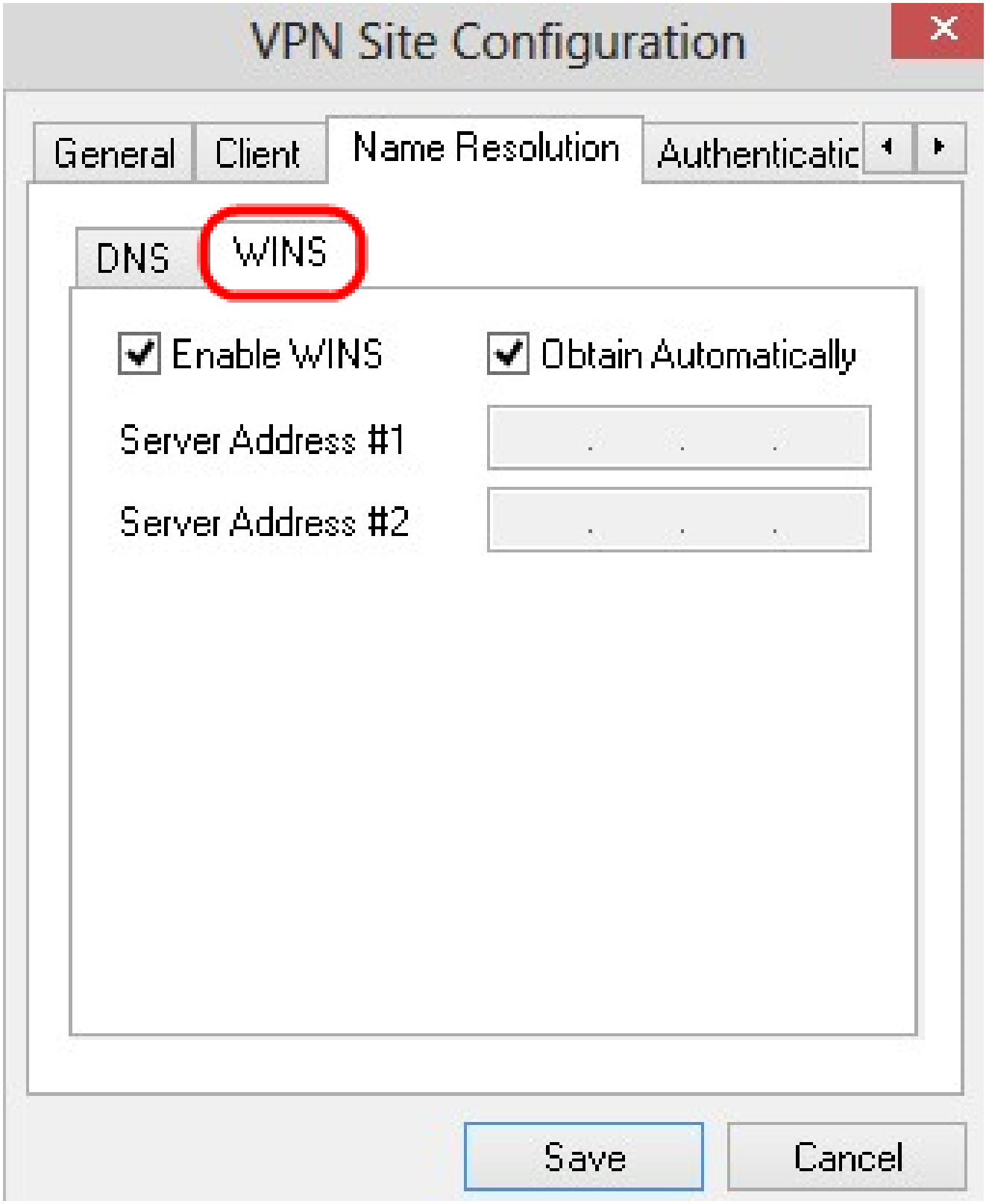


ステップ6:（オプション）DNSサーバのサフィックスを自動的に取得するには、Obtain Automaticallyチェックボックスにチェックマークを付けます。このオプションを選択した場合は、ステップ8に進みます。

手順 7：DNS SuffixフィールドにDNSサーバのサフィクスを入力します。

ステップ 8：[Save] をクリックして、設定を保存します。

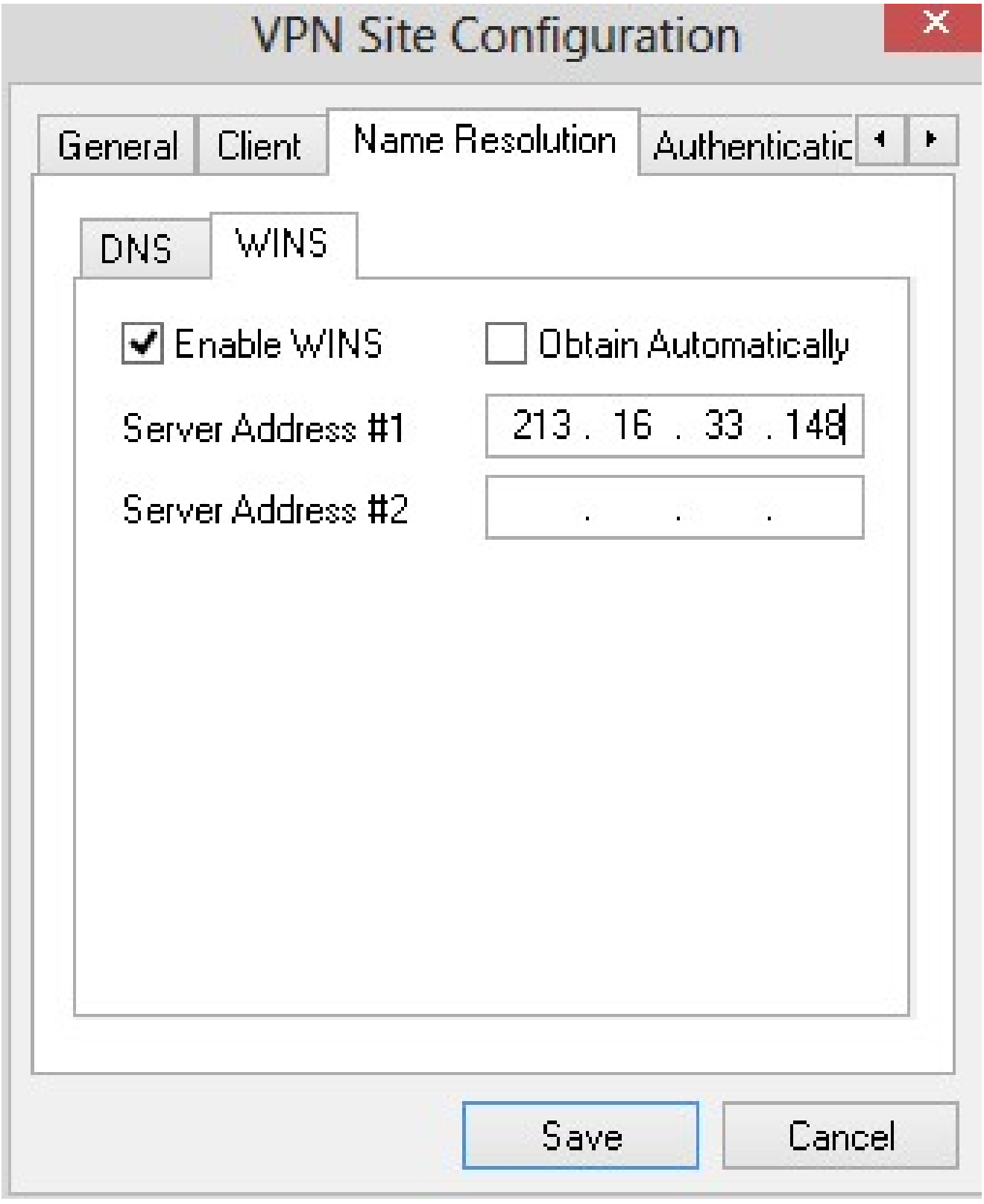
ステップ 9：WINSタブをクリックします。



ステップ 10：Windows Internet Name Server（WINS；インターネットネームサーバ）をイネーブルにするには、Enable WINSにチェックマークを付けます。

ステップ11:（オプション）DNSサーバアドレスを自動的に取得するには、Obtain Automaticallyチェックボックスにチェックマークを付けます。このオプションを選択する場合は、ステップ13に進みます。

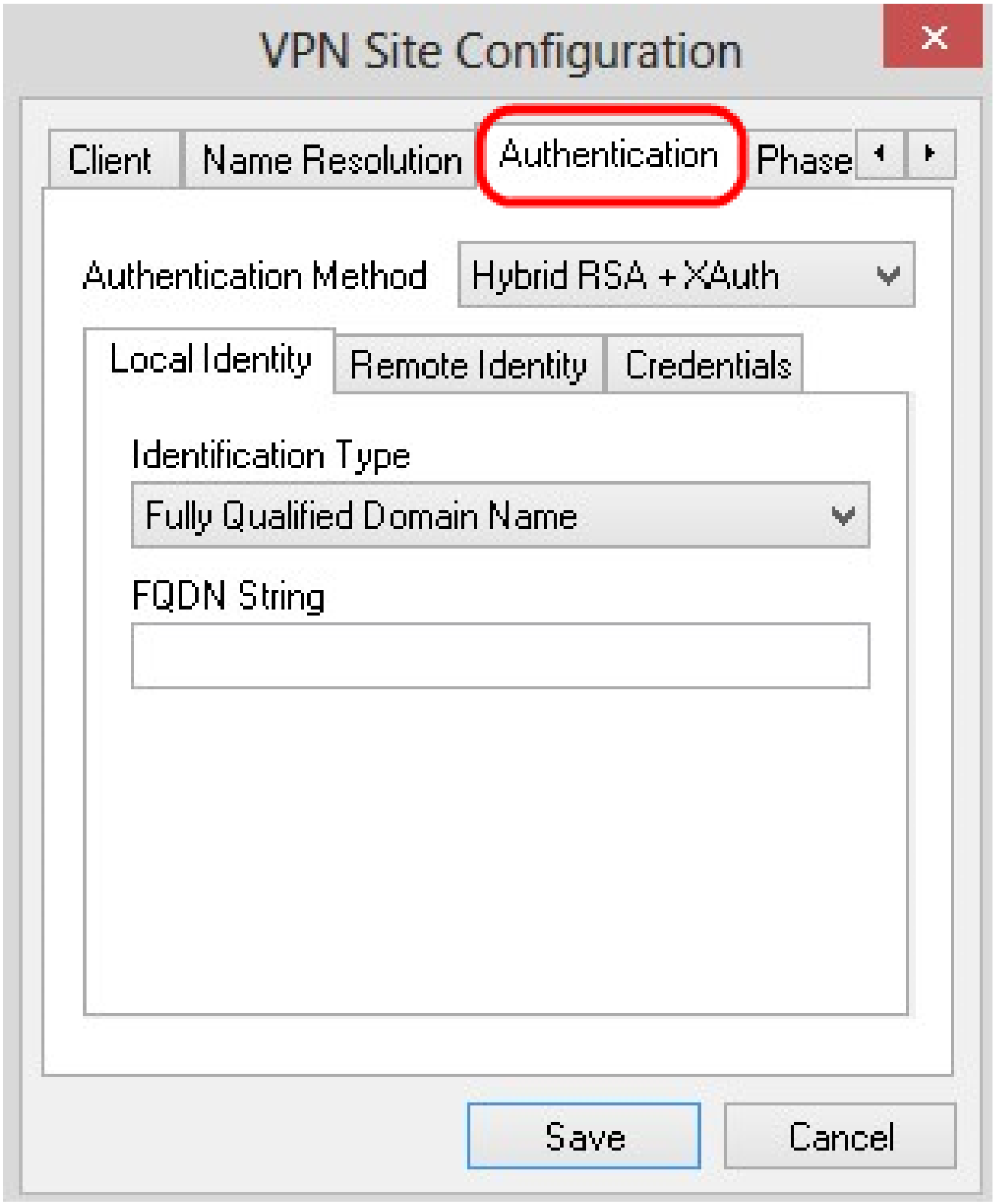
ステップ 12Server Address #1フィールドにWINSサーバのアドレスを入力します。他のDNSサーバがある場合は、残りのServer Addressフィールドにそれらのサーバのアドレスを入力します。



ステップ 13[Save] をクリックして、設定を保存します。

[Authentication]

ステップ 1：[Authentication] タブをクリックします。



注：「認証」セクションでは、ISAKMP SAを確立しようとする際に認証を処理するようにクライアントのパラメータを設定できます。

ステップ 2：Authentication Methodドロップダウンリストから、適切な認証方式を選択します。

・ RSA + XAuthのハイブリッド：クライアントクレデンシャルは必要ありません。クライアントはゲートウェイを認証します。クレデンシャルは、PEMまたはPKCS12証明書ファイル、あるいはキーファイルタイプの形式になります。

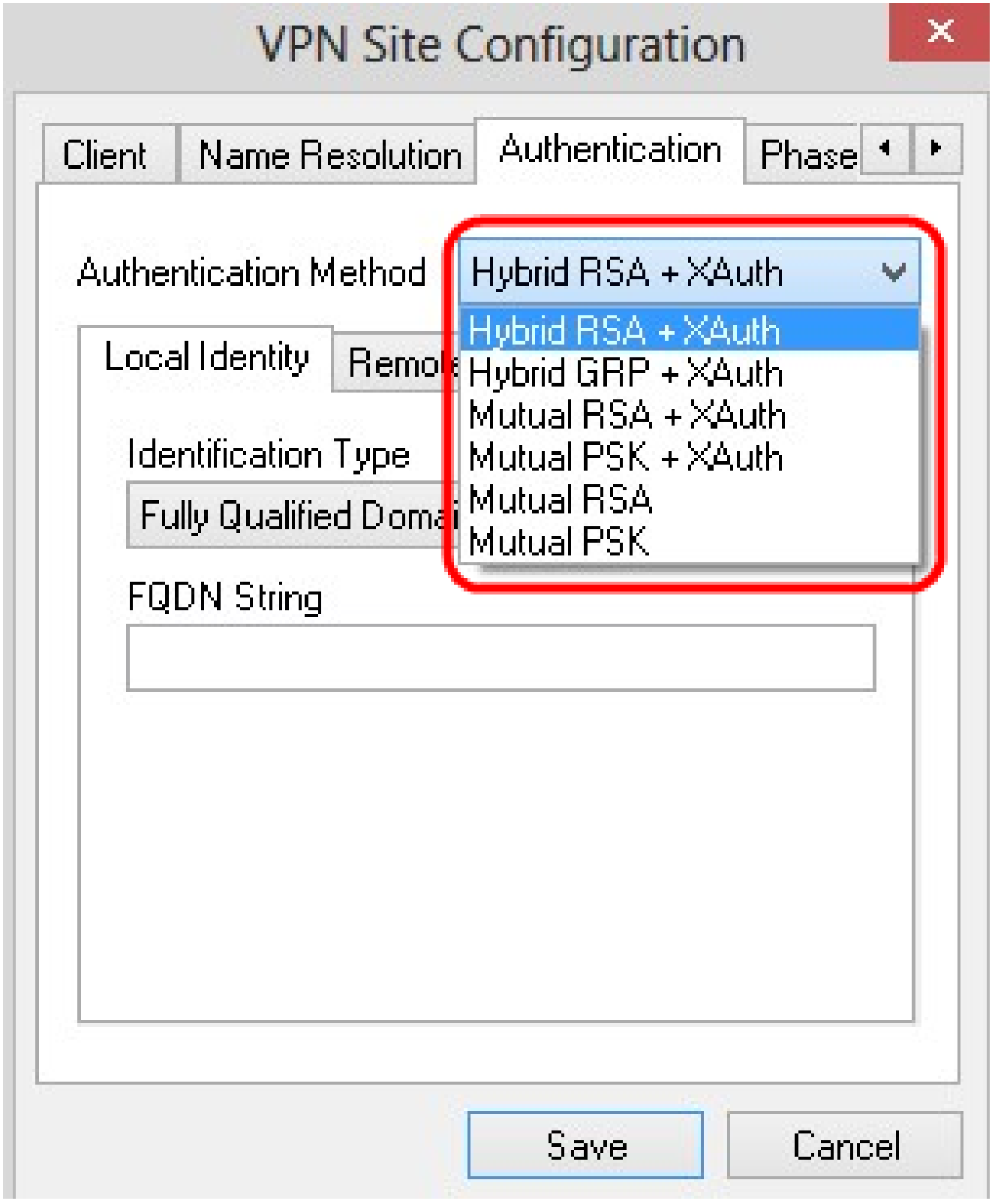
・ ハイブリッドGRP + XAuth：クライアントクレデンシャルは必要ありません。クライアントはゲートウェイを認証します。クレデンシャルは、PEMまたはPKCS12証明書ファイルと共有秘密文字列の形式になります。

・ 相互RSA + XAuth ：クライアントとゲートウェイの両方が認証にクレデンシャルを必要とする。クレデンシャルは、PEMまたはPKCS12証明書ファイルまたはキータイプの形式になります。

・ 相互PSK + XAuth：クライアントとゲートウェイの両方が認証にクレデンシャルを必要とします。クレデンシャルは、共有秘密文字列の形式になります。

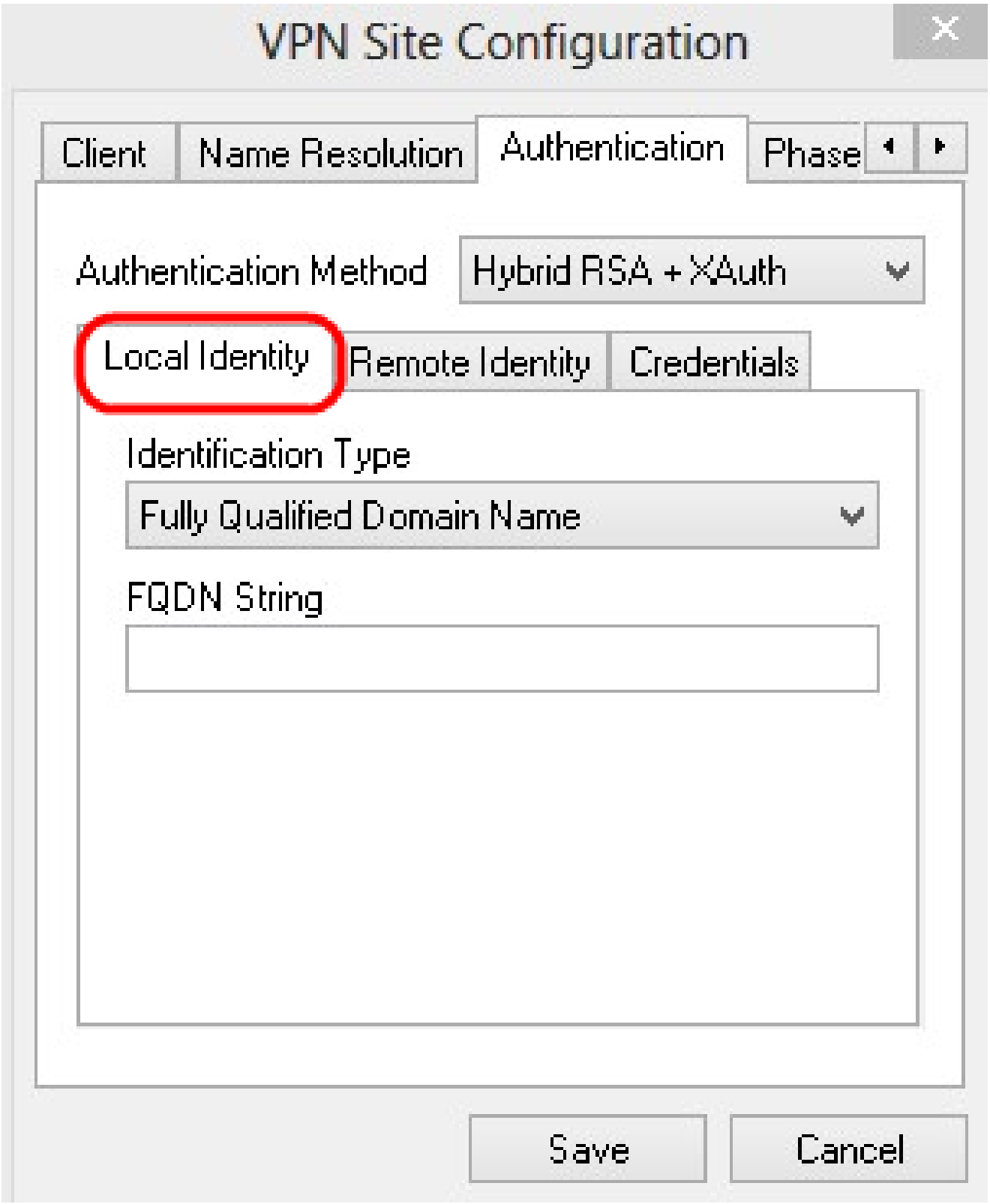
・ 相互RSA：クライアントとゲートウェイの両方が認証にクレデンシャルを必要とする。クレデンシャルは、PEMまたはPKCS12証明書ファイルまたはキータイプの形式になります。

・ 双方向PSK：クライアントとゲートウェイの両方が認証にクレデンシャルを必要とします。クレデンシャルは、共有秘密文字列の形式になります。



ローカルIDの設定

ステップ 1：Local Identityタブをクリックします。



注：ローカルIDは、検証のためにゲートウェイに送信されるIDを設定します。Local Identityセクションでは、IDの送信方法を決定するために、IDタイプ(ID)とFQDN（完全修飾ドメイン名）文字列が設定されます。

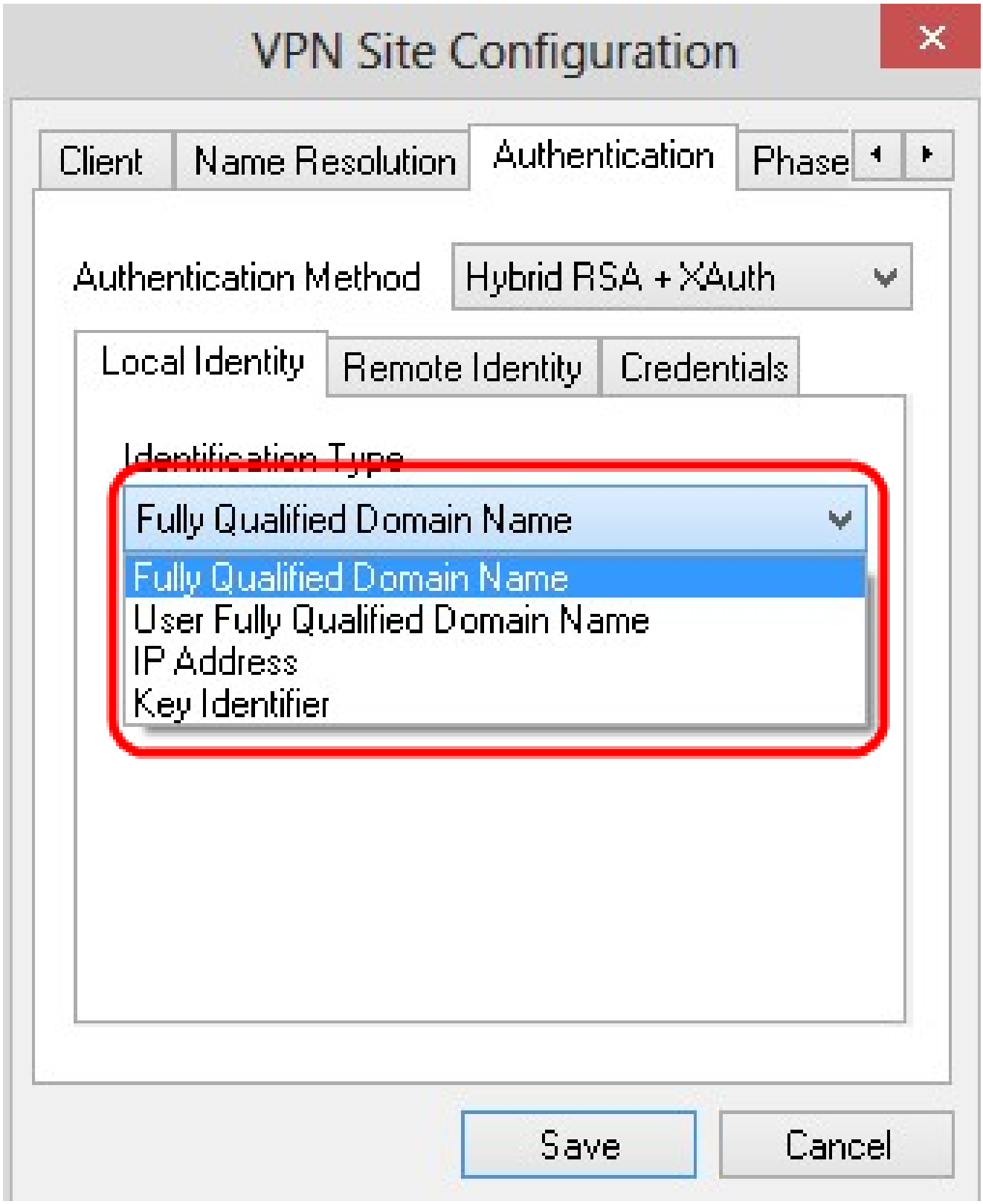
ステップ 2：Identification Typeドロップダウンリストから、適切な識別オプションを選択します。すべての認証モードですべてのオプションを使用できるわけではありません。

・ 完全修飾ドメイン名：ローカルIDのクライアントIDは、完全修飾ドメイン名に基づきます。このオプションを選択する場合は、ステップ3に従い、ステップ7に進みます。

・ ユーザーの完全修飾ドメイン名：ローカルIDのクライアントIDは、ユーザーの完全修飾ドメイン名に基づきます。このオプションを選択する場合は、ステップ4に従い、ステップ7に進みます。

・ IPアドレス：ローカルIDのクライアントIDはIPアドレスに基づきます。Use a discovered local host addressにチェックマークを入れると、IPアドレスは自動的に検出されます。このオプションを選択する場合は、ステップ5に従い、ステップ7に進みます。

・ Key Identifier：ローカルクライアントのクライアントIDは、キーIDに基づいて識別されます。このオプションを選択する場合は、ステップ6とステップ7に従ってください。



ステップ 3：FQDN Stringフィールドに、DNS文字列として完全修飾ドメイン名(FQDN)を入力します。

ステップ 4：UFQDN Stringフィールドに、DNS文字列としてユーザの完全修飾ドメイン名(FQDN)を入力します。

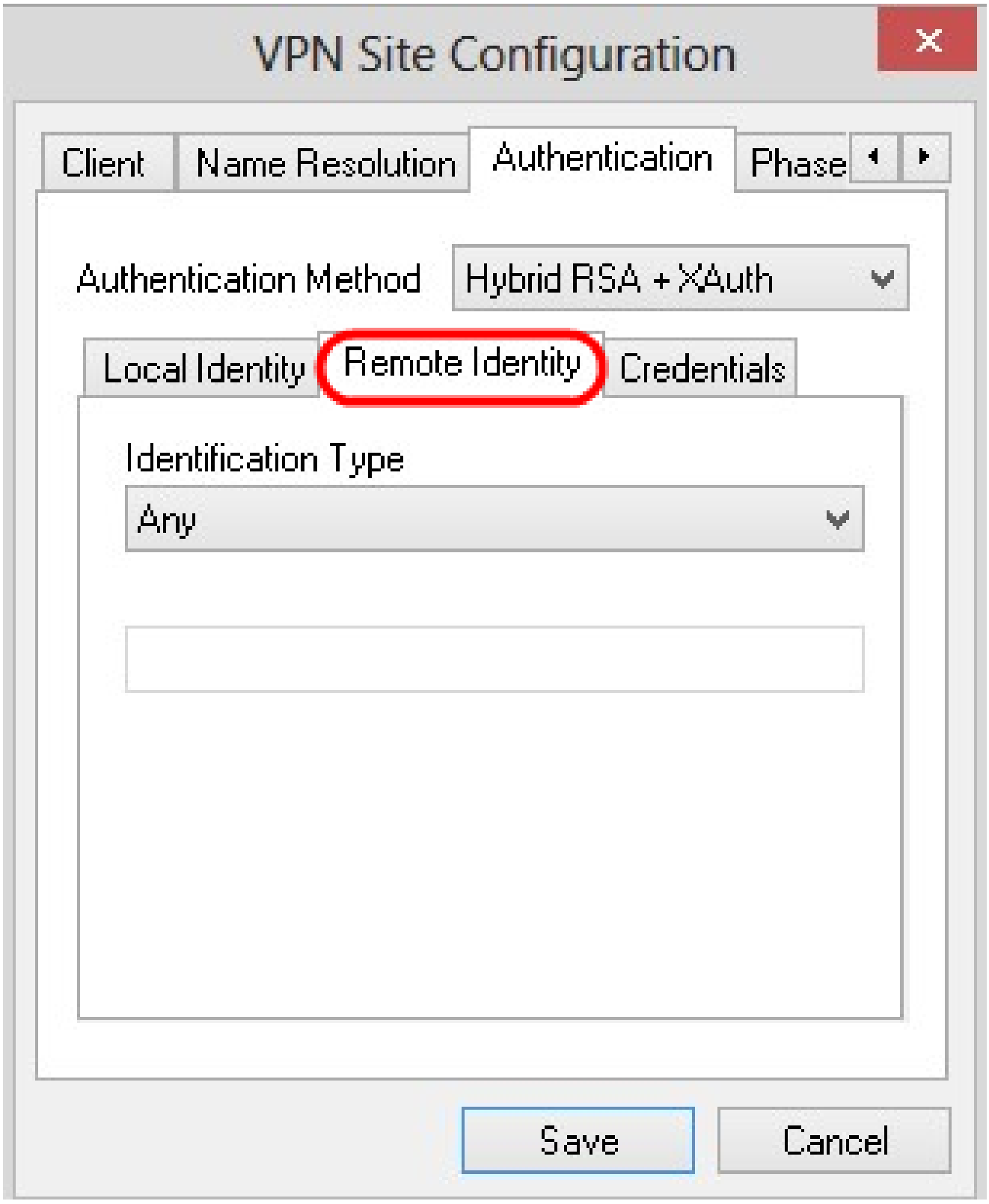
ステップ 5：UFQDN StringフィールドにIPアドレスを入力します。

手順 6：ローカルクライアントを識別するキーIDをKey ID Stringに入力します。

手順 7：[Save] をクリックして、設定を保存します。

リモートIDの設定

ステップ 1：Remote Identityタブをクリックします。



注：リモートIDはゲートウェイからIDを確認します。「リモートID」セクションでは、IDの確認方法を決定するためにIDタイプが設定されます。

ステップ 2：Identification Typeドロップダウンリストから、適切な識別オプションを選択します。

・ Any：リモートクライアントは、認証する任意の値またはIDを受け入れることができます。

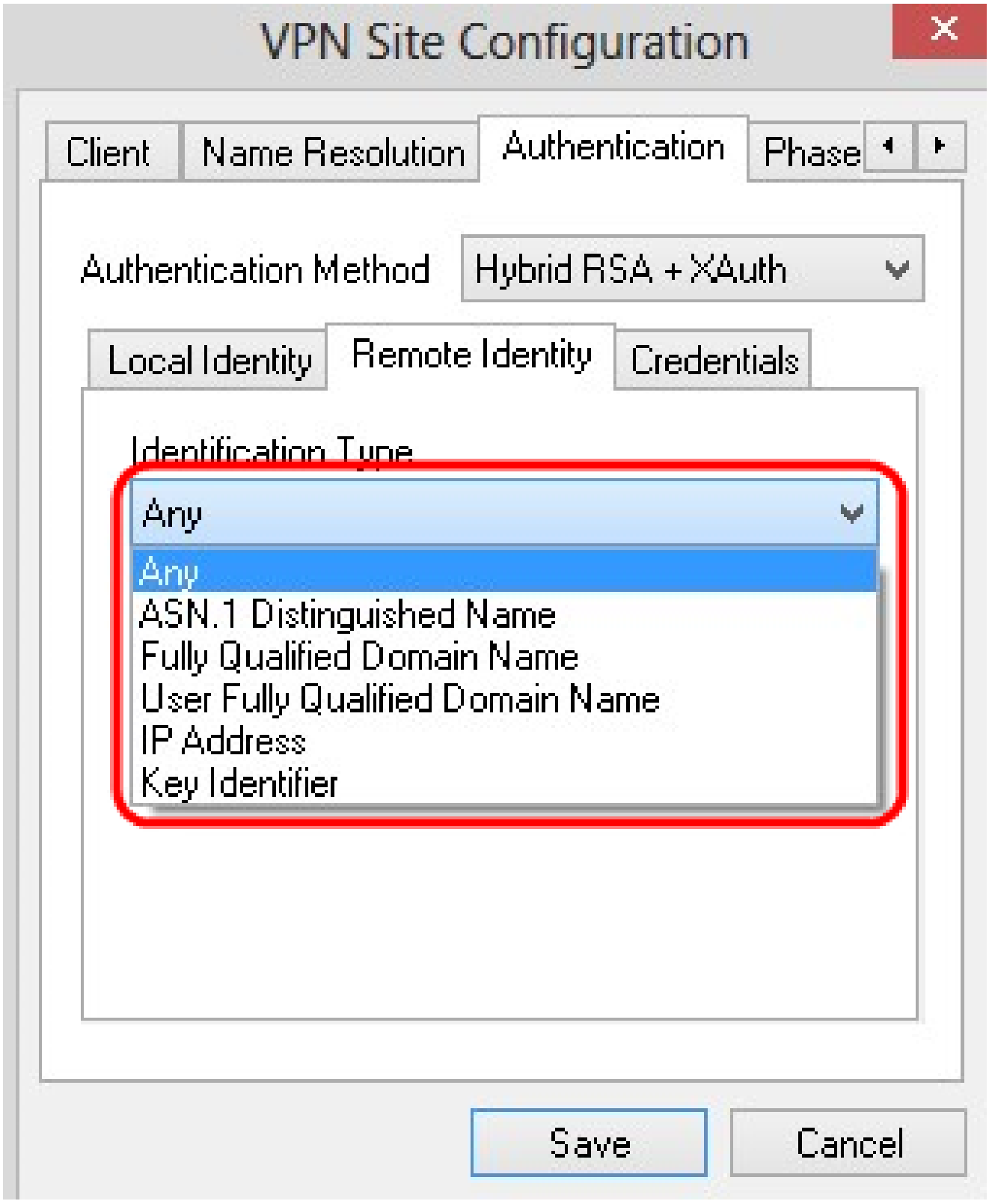
・ ASN.1 Distinguished Name：リモートクライアントはPEMまたはPKCS12証明書ファイルから自動的に識別されます。このオプションを選択できるのは、「認証」セクションのステップ2でRSA認証方式を選択した場合だけです。証明書を自動的に受信するには、Use the subject in the received certificate but don't compare it with a specific valueチェックボックスにチェックマークを付けます。このオプションを選択する場合は、ステップ3に従い、ステップ8に進みます。

・ 完全修飾ドメイン名：リモートIDのクライアントIDは完全修飾ドメイン名に基づきます。このオプションを選択できるのは、「認証」セクションのステップ2でPSK認証方式を選択した場合だけです。このオプションを選択する場合は、ステップ4に従い、ステップ8に進みます。

・ ユーザーの完全修飾ドメイン名：リモートIDのクライアントIDは、ユーザーの完全修飾ドメイン名に基づきます。このオプションを選択できるのは、「認証」セクションのステップ2でPSK認証方式を選択した場合だけです。このオプションを選択する場合は、ステップ5に従い、ステップ8に進みます。

・ IPアドレス：リモート・アイデンティティのクライアントIDはIPアドレスに基づきます。Use a discovered local host addressにチェックマークを入れると、IPアドレスは自動的に検出されます。このオプションを選択する場合は、ステップ6に従い、ステップ8に進みます。

・ Key Identifier：リモートクライアントのクライアントIDは、キーIDに基づいて識別されます。このオプションを選択する場合は、ステップ7とステップ8に従ってください。



ステップ 3：ASN.1 DN StringフィールドにASN.1 DN文字列を入力します。

ステップ 4：FQDN StringフィールドにDNS文字列として完全修飾ドメイン名(FQDN)を入力します。

ステップ 5：UFQDN Stringフィールドに、DNS文字列としてユーザの完全修飾ドメイン名

(FQDN)を入力します。

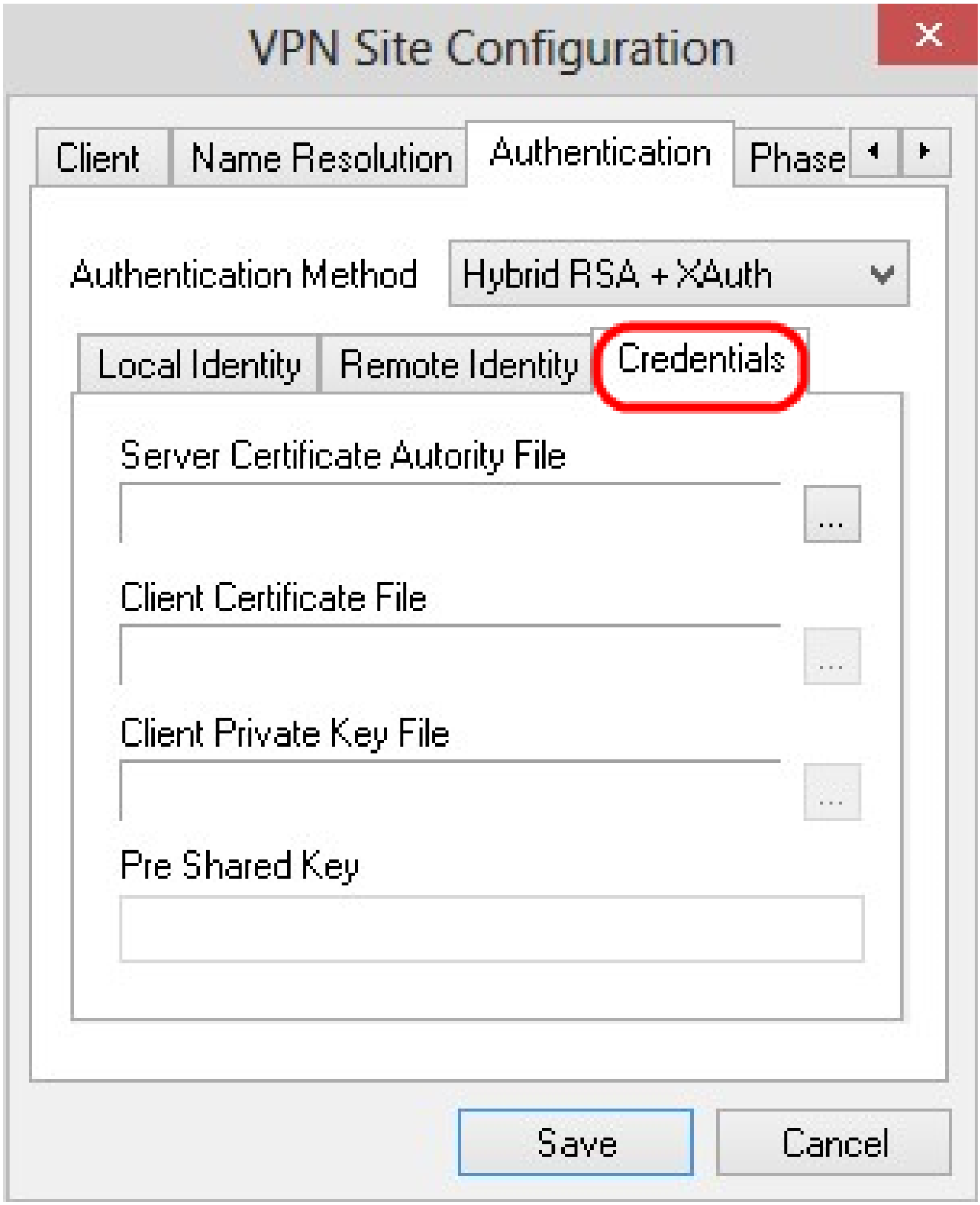
手順 6：UFQDN StringフィールドにIPアドレスを入力します。

手順 7：ローカルクライアントを識別するキーIDをKey ID Stringフィールドに入力します。

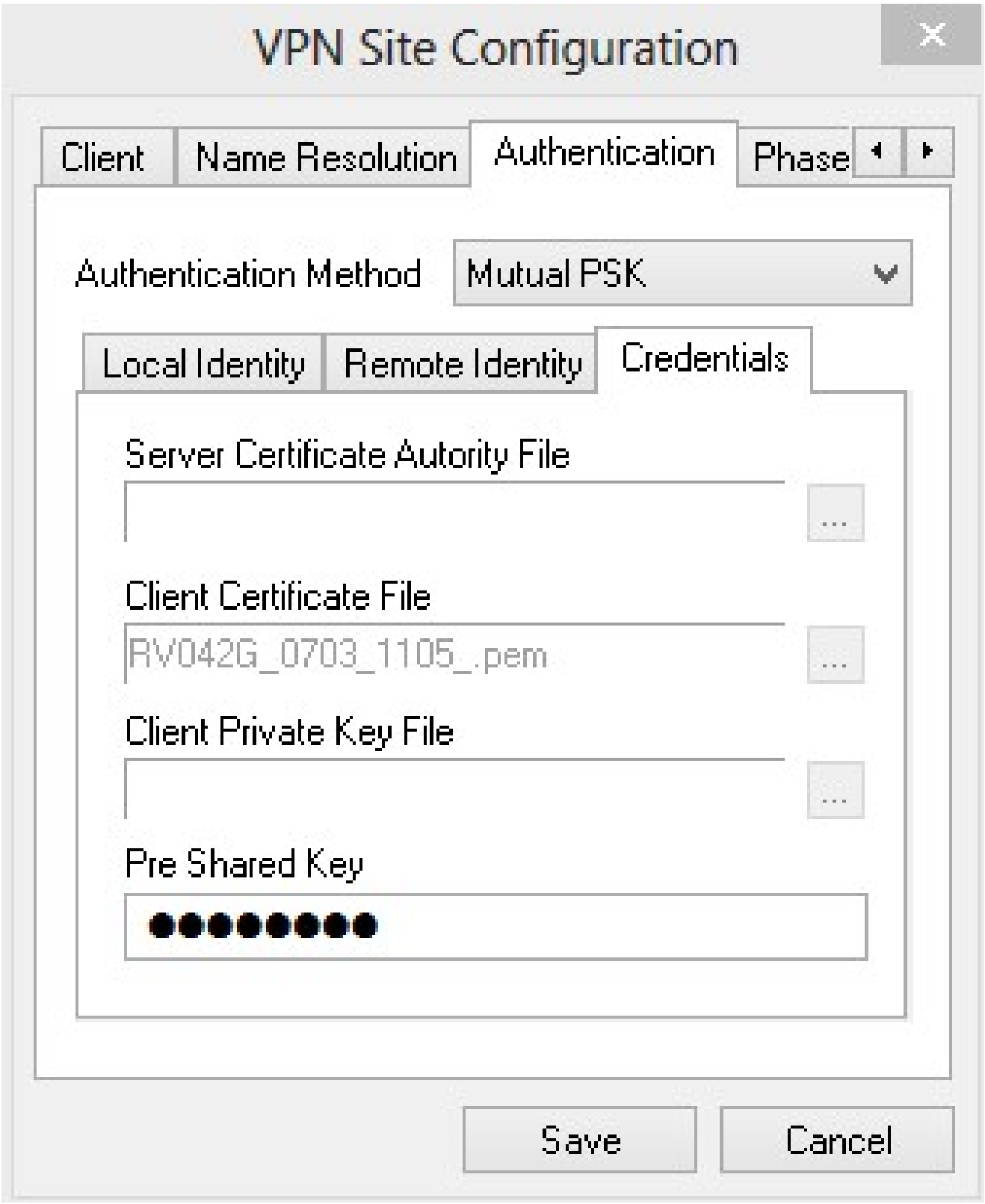
ステップ 8：[Save] をクリックして、設定を保存します。

クレデンシャルの設定

ステップ 1：Credentialsタブをクリックします。



注：クレデンシャルセクションで、事前共有キーが設定されています。



ステップ 2：サーバ証明書ファイルを選択するには、Server Certificate Authority Fileフィールドの横にある...アイコンをクリックし、PC上のサーバ証明書ファイルを保存したパスを選択します。

ステップ 3：クライアント証明書ファイルを選択するには、Client Certificate Fileフィールドの横にある...アイコンをクリックし、PC上でクライアント証明書ファイルを保存したパス

を選択します。

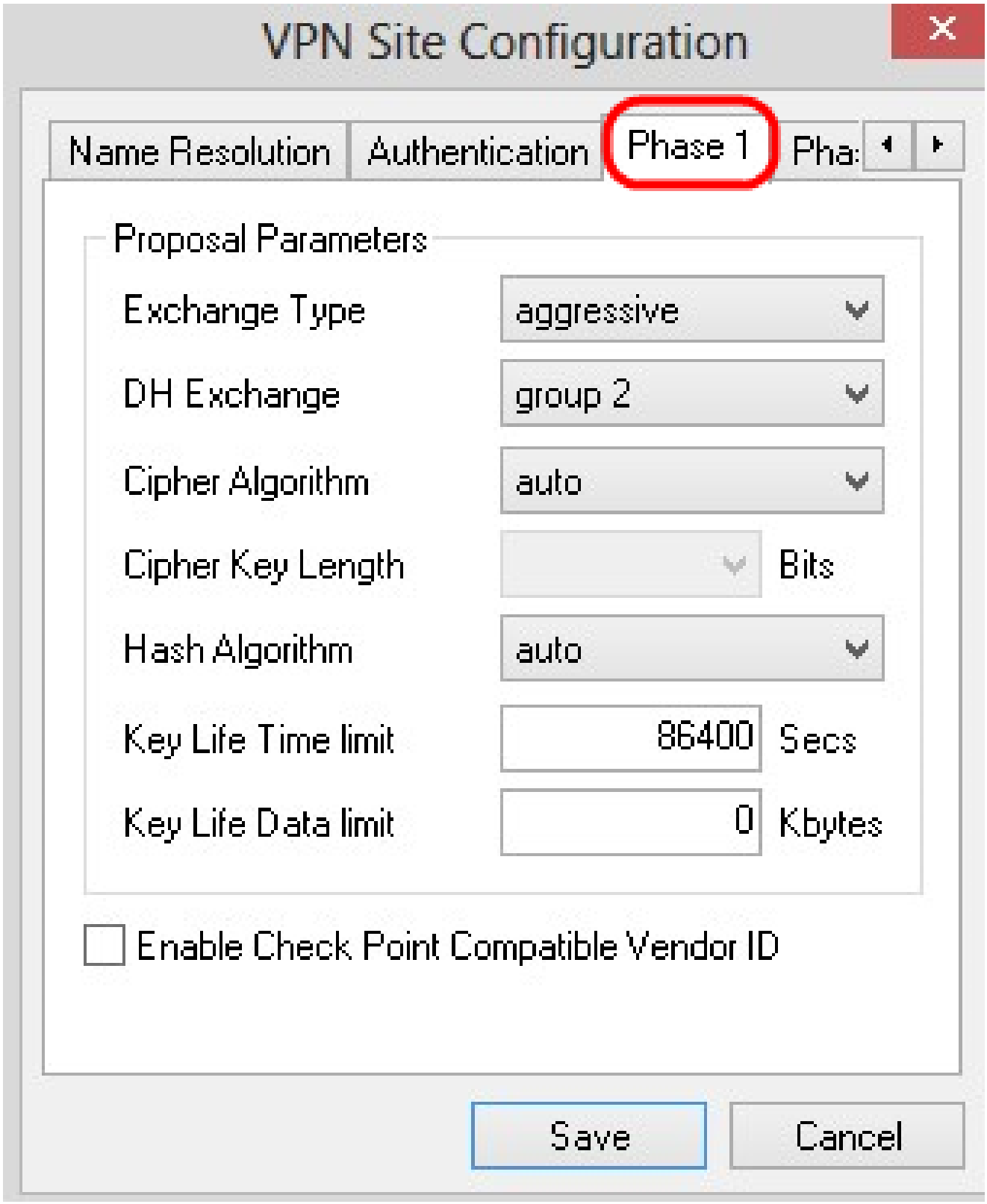
ステップ 4： クライアント秘密キーファイルを選択するには、Client Private Key Fileフィールドの横にある...アイコンをクリックし、PCでクライアント秘密キーファイルを保存したパスを選択します。

ステップ 5：PreShared Keyフィールドに事前共有キーを入力します。これは、トンネルの設定時に使用するキーと同じである必要があります。

手順 6：[Save] をクリックして、設定を保存します。

フェーズ 1 の設定

ステップ 1：Phase 1タブをクリックします。

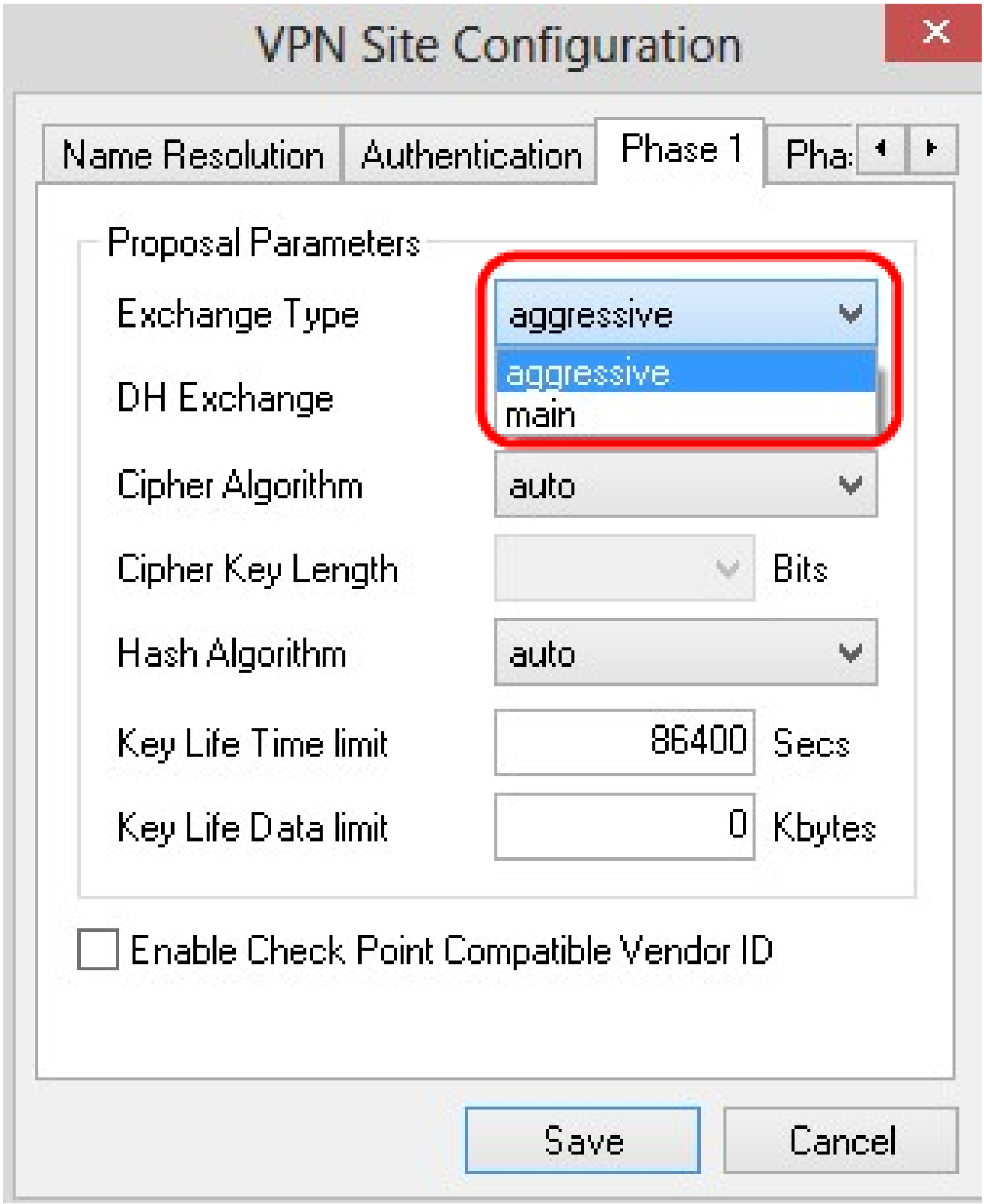


注：「フェーズ1」セクションでは、クライアントゲートウェイとのISAKMP SAを確立できるようにパラメータを設定できます。

ステップ 2：Exchange Typeドロップダウンリストから、適切なキー交換タイプを選択します。

・ Main：ピアのIDが保護されます。

・ アグレッシブ：ピアのIDは保護されません。



ステップ 3：DH Exchangeドロップダウンリストで、VPN接続の設定時に選択した適切なグループを選択します。

ステップ 4：Cipher Algorithmドロップダウンリストで、VPN接続の設定中に選択された適切なオプションを選択します。

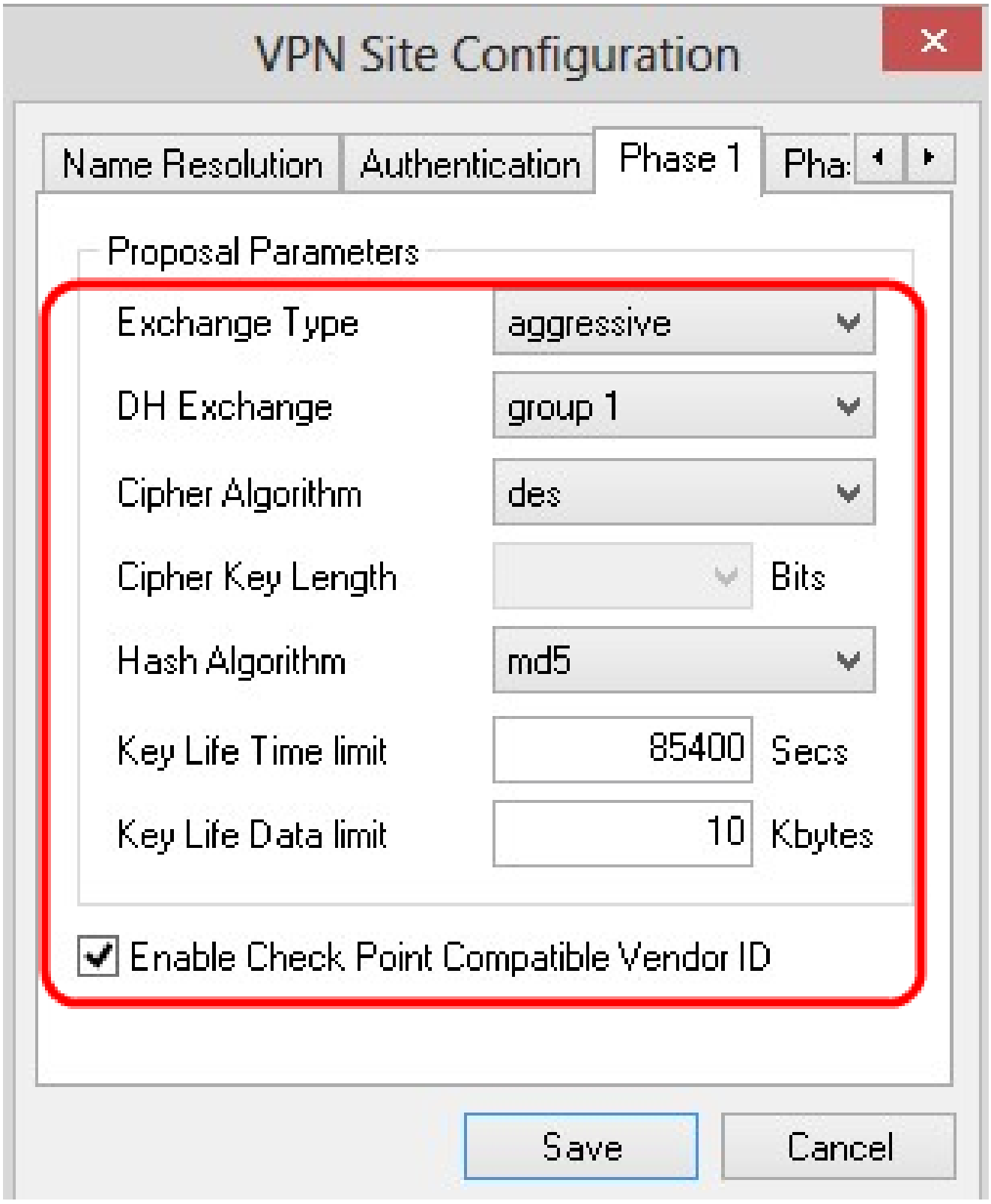
ステップ 5：Cipher Key Lengthドロップダウンリストで、VPN接続の設定時に選択したオプションのキー長と一致するオプションを選択します。

手順 6：Hash Algorithmドロップダウンリストで、VPN接続の設定時に選択したオプションを選択します。

手順 7：Key Life Time Limitフィールドに、VPN接続の設定時に使用した値を入力します。

ステップ 8：Key Life Data Limitフィールドに、保護する値をKB単位で入力します。デフォルト値は0で、この機能はオフになります。

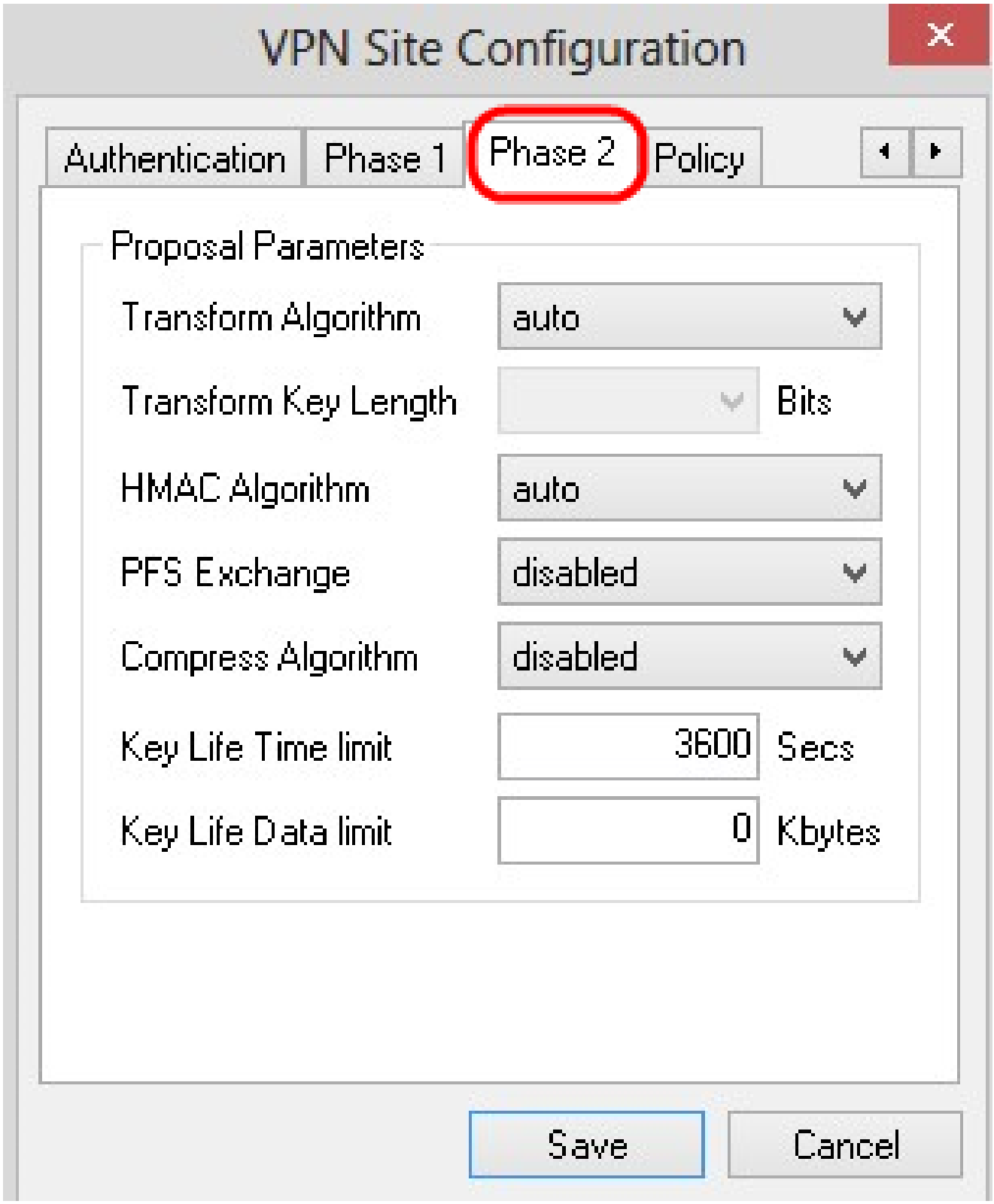
ステップ9:（オプション）Enable Check Point Compatible Vendor IDチェックボックスにチェックマークを付けます。



ステップ 10：[Save] をクリックして、設定を保存します。

フェーズ 2 の設定

ステップ 1：Phase 2タブをクリックします。



注：「フェーズ2」セクションでは、リモートクライアントゲートウェイとのIPsec SAを確立できるようにするためのパラメータを設定できます。

ステップ 2：Transform Algorithmドロップダウンリストで、VPN接続の設定時に選択されたオプションを選択します。

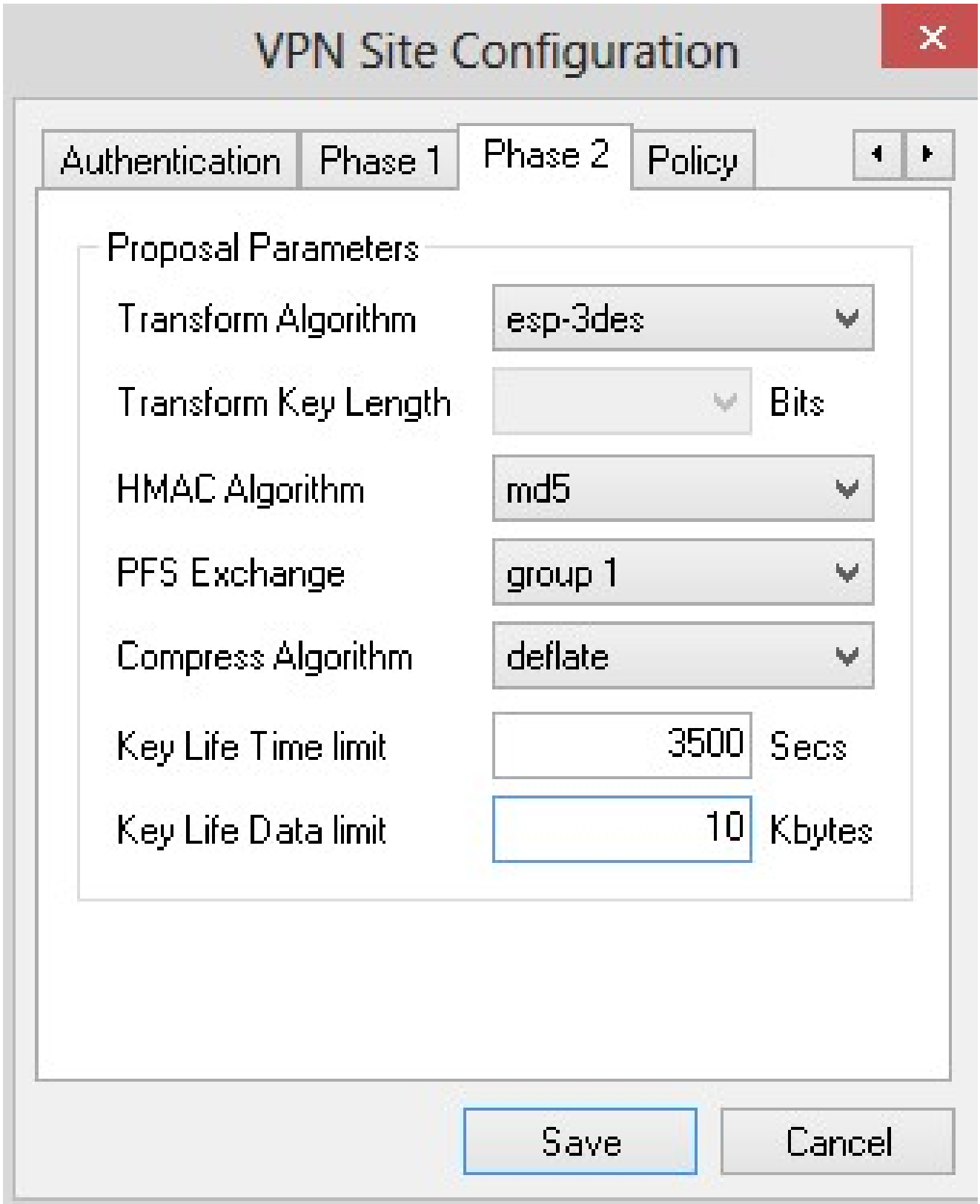
ステップ 3：Transform Key Lengthドロップダウンリストで、VPN接続の設定時に選択されたオプションのキー長と一致するオプションを選択します。

ステップ 4：HMAC Algorithmドロップダウンリストで、VPN接続の設定時に選択されたオプションを選択します。

ステップ 5：PFS Exchangeドロップダウンリストで、VPN接続の設定中に選択されたオプションを選択します。

手順 6：Key Life Time limitフィールドに、VPN接続の設定時に使用する値を入力します。

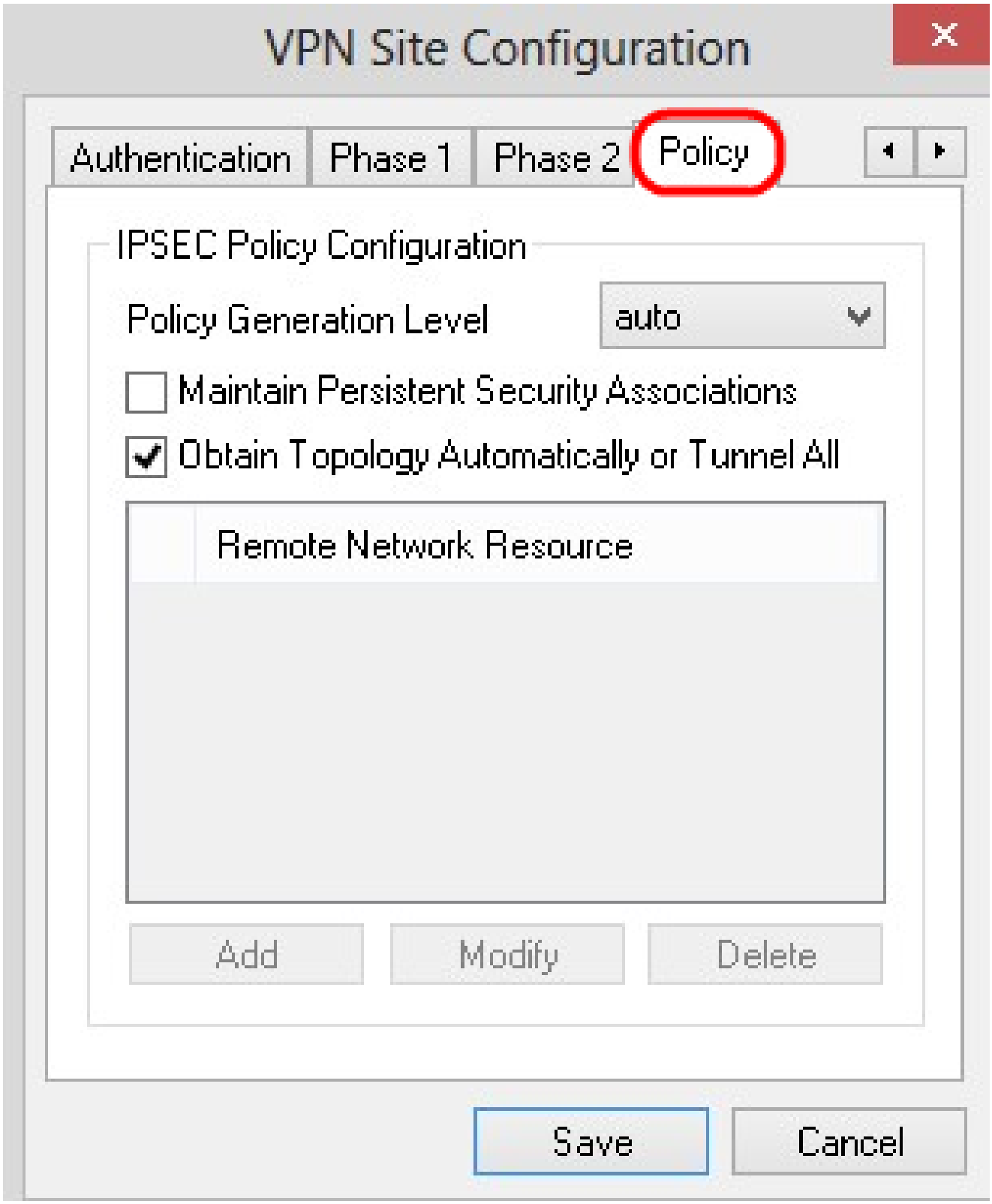
手順 7：Key Life Data limitフィールドに、保護する値をKB単位で入力します。デフォルト値は0で、この機能はオフになります。



ステップ 8：[Save] をクリックして、設定を保存します。

ポリシーの設定

ステップ1:Policyタブをクリックします。



注：「ポリシー」セクションで、IPSECポリシーが定義されています。これは、クライアントがサイト設定のためにホストと通信するために必要です。

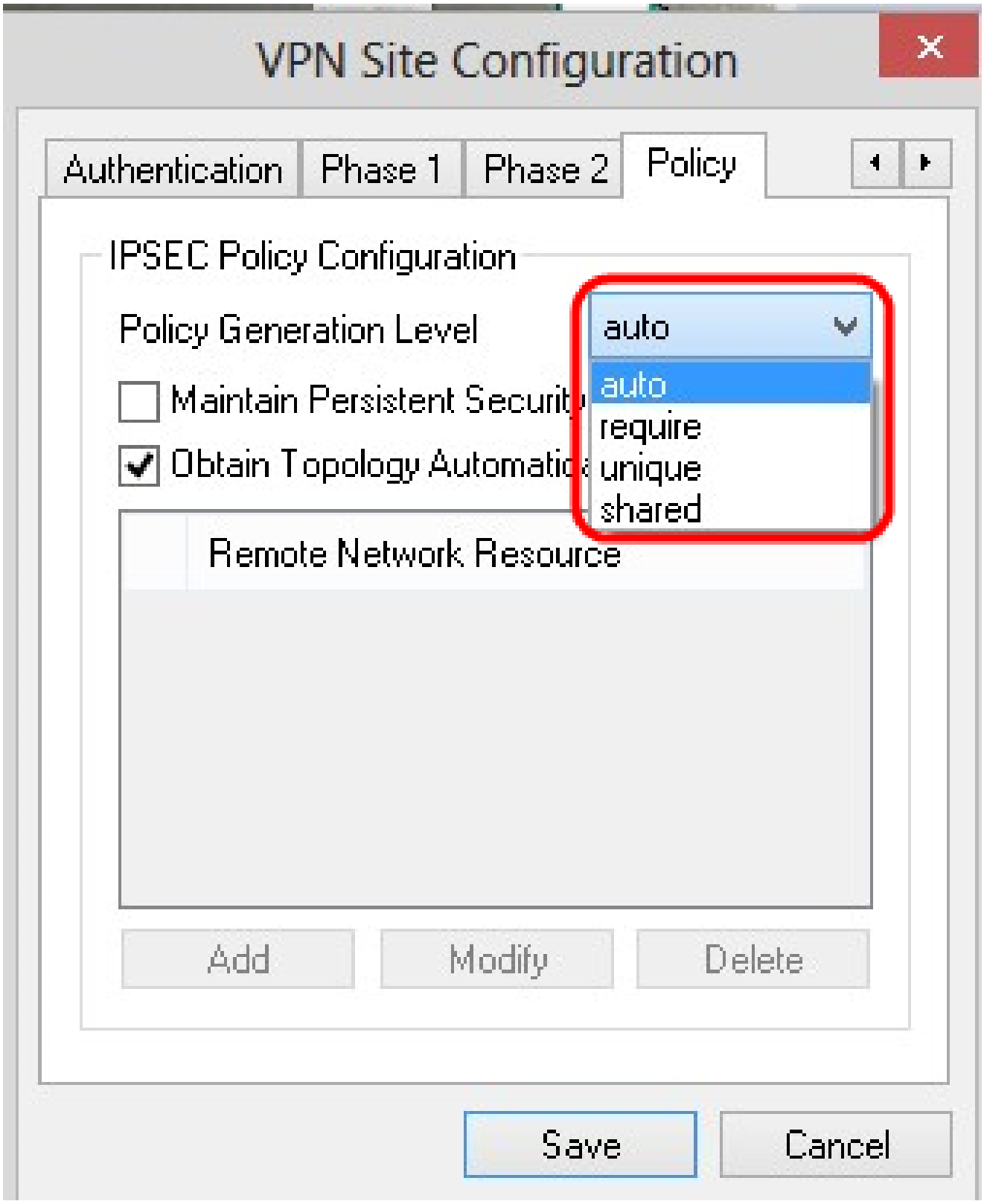
ステップ 2：Policy Generation Levelドロップダウンリストで、適切なオプションを選択します。

・ Auto：必要なIPSecポリシーレベルが自動的に決定されます。

・ Require：各ポリシーの一意のセキュリティ・アソシエーションはネゴシエートされません。

・ Unique：各ポリシーに対する一意のセキュリティ・アソシエーションがネゴシエートされます。

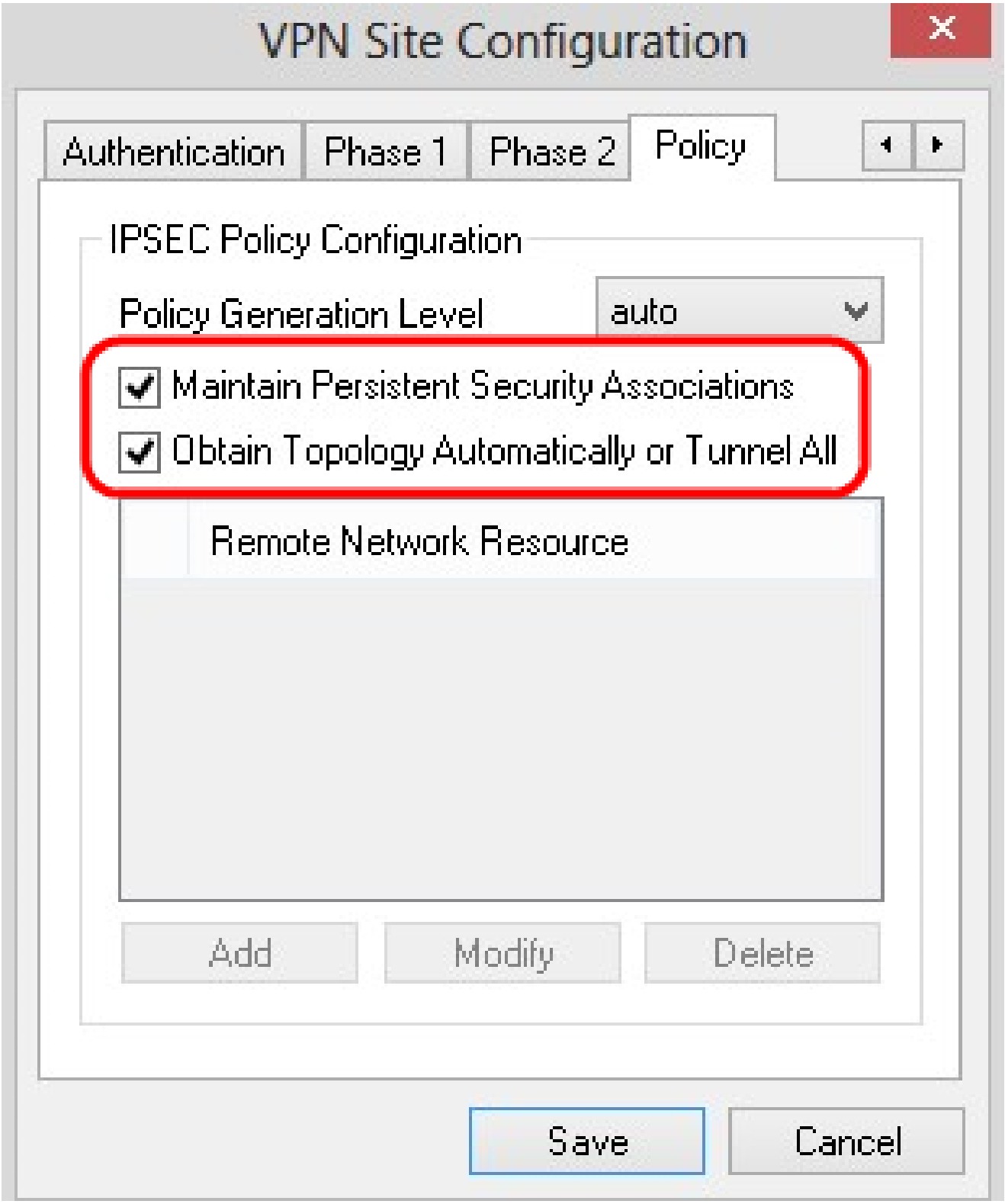
・ 共有：適切なポリシーが必要なレベルで生成されます。



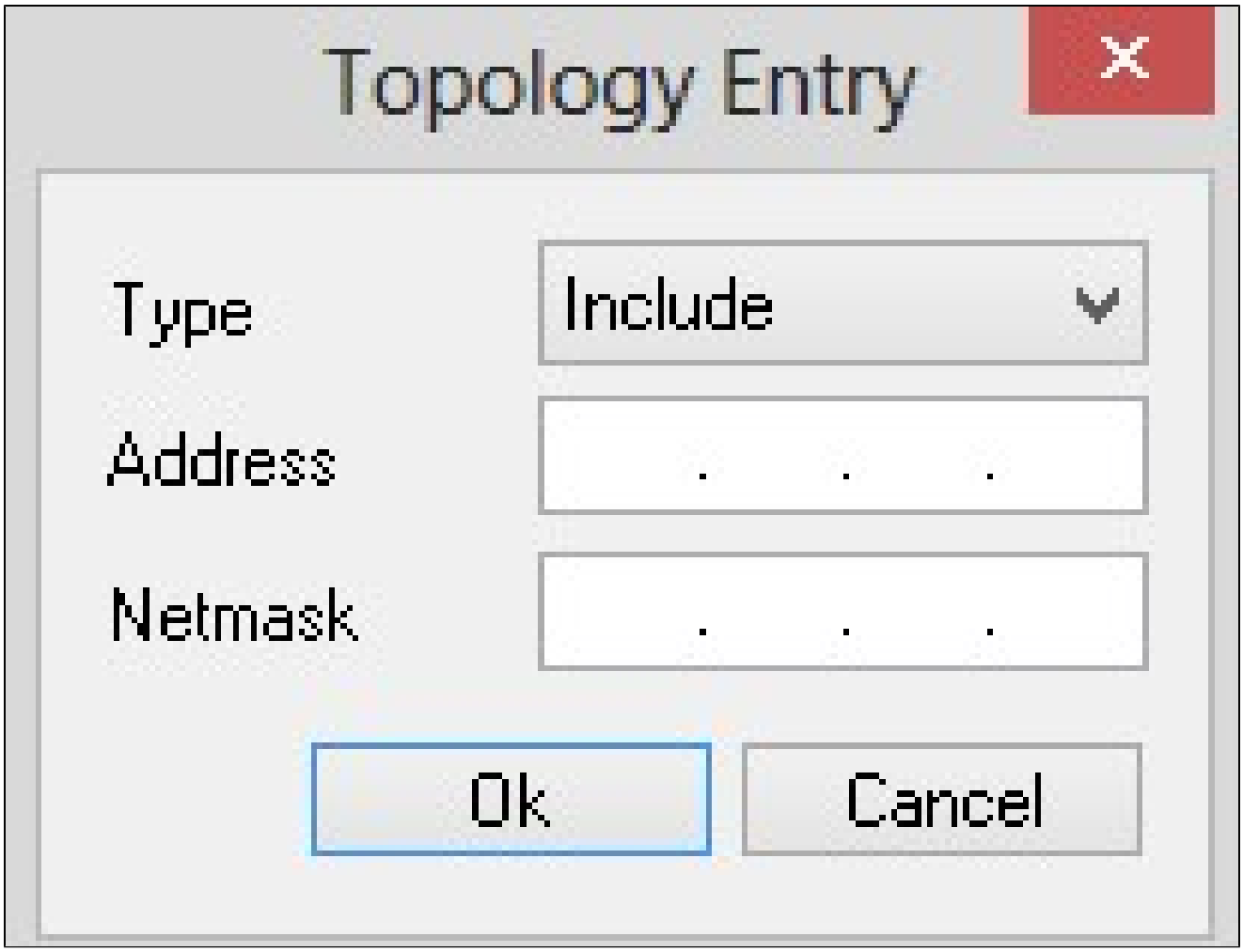
ステップ3: (オプション) IPSecネゴシエーションを変更するには、Maintain Persistent Security Associationsチェックボックスにチェックマークを付けます。有効にすると、ネゴシエーションは接続後に各ポリシーに対して直接行われます。無効にした場合、ネゴシエーションは必要に応じて行われます。

ステップ4: (オプション) デバイスから自動的に提供されたネットワークリストを受信する

か、デフォルトですべてのパケットをRV0XXに送信するには、Obtain Topology AutomaticallyまたはTunnel Allチェックボックスをオンにします。オフの場合、設定は手動で行う必要があります。オンになっている場合は、ステップ10に進みます。

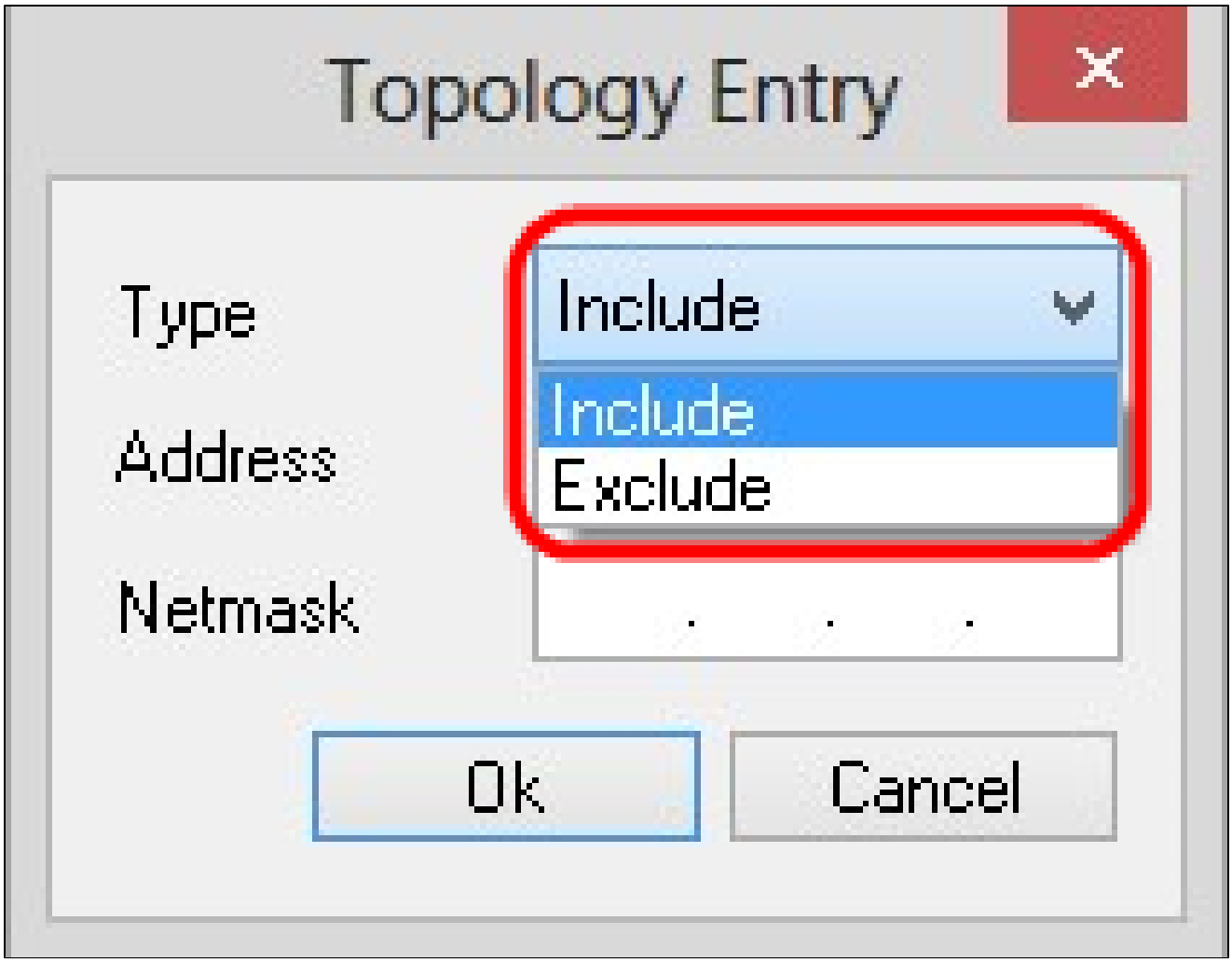


ステップ 5：Addをクリックして、トポロジエントリをテーブルに追加します。Topology Entryウィンドウが表示されます。



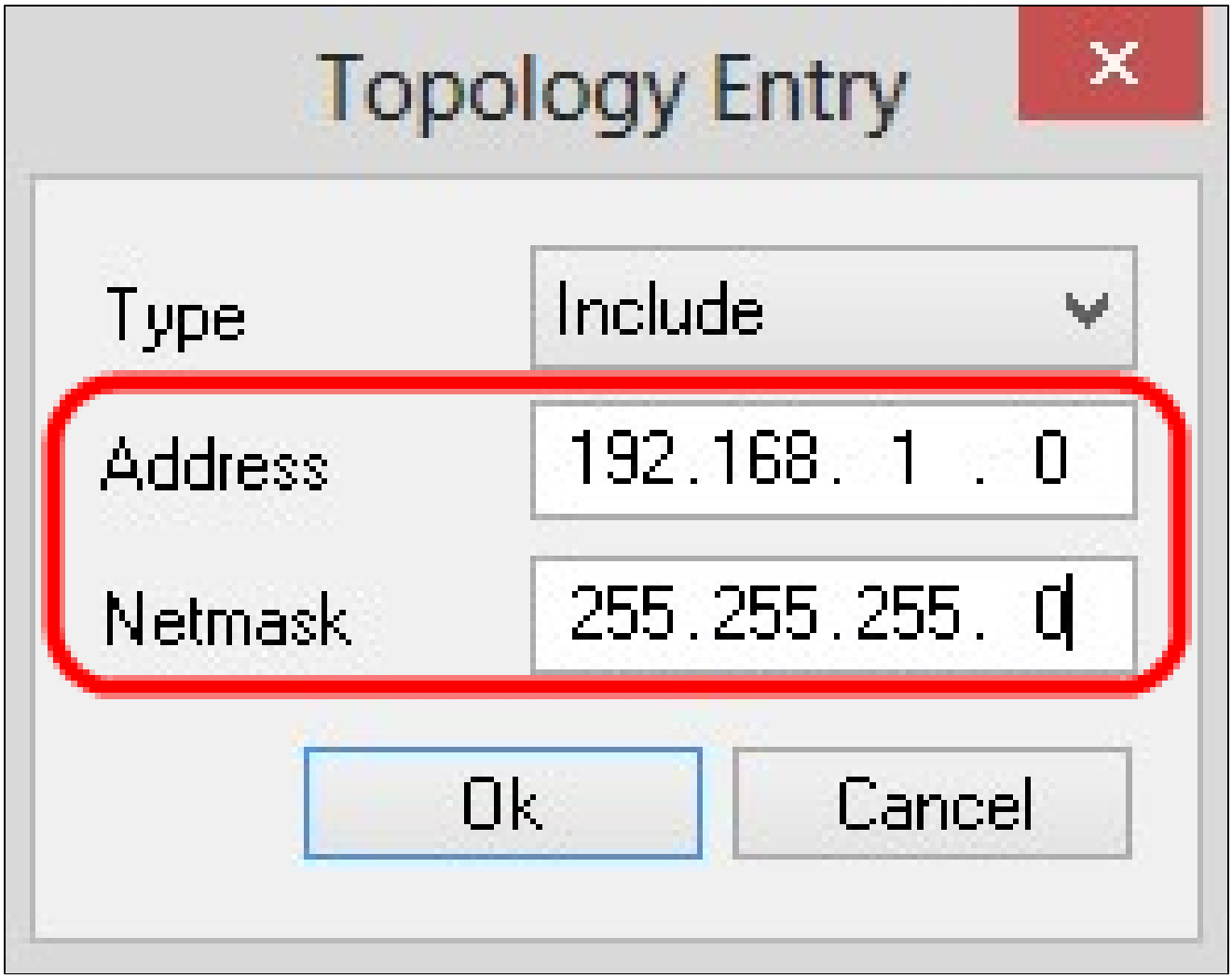
手順 6：Typeドロップダウンリストで、適切なオプションを選択します。

- Include：ネットワークはVPNゲートウェイを介してアクセスされます。
- 除外：ネットワークはローカル接続を介してアクセスされます。

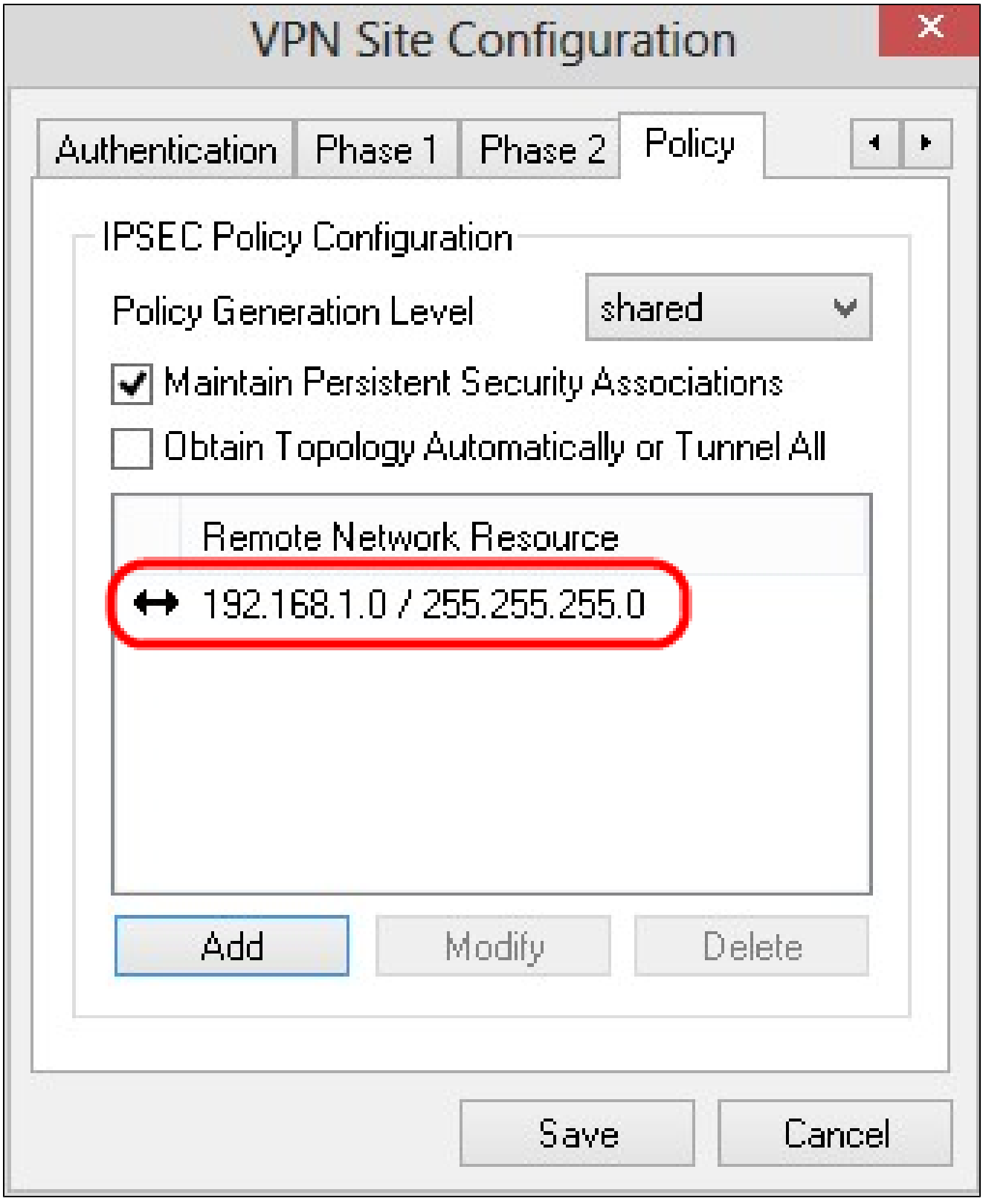


手順 7：Addressフィールドに、RV0XXのIPアドレスを入力します。

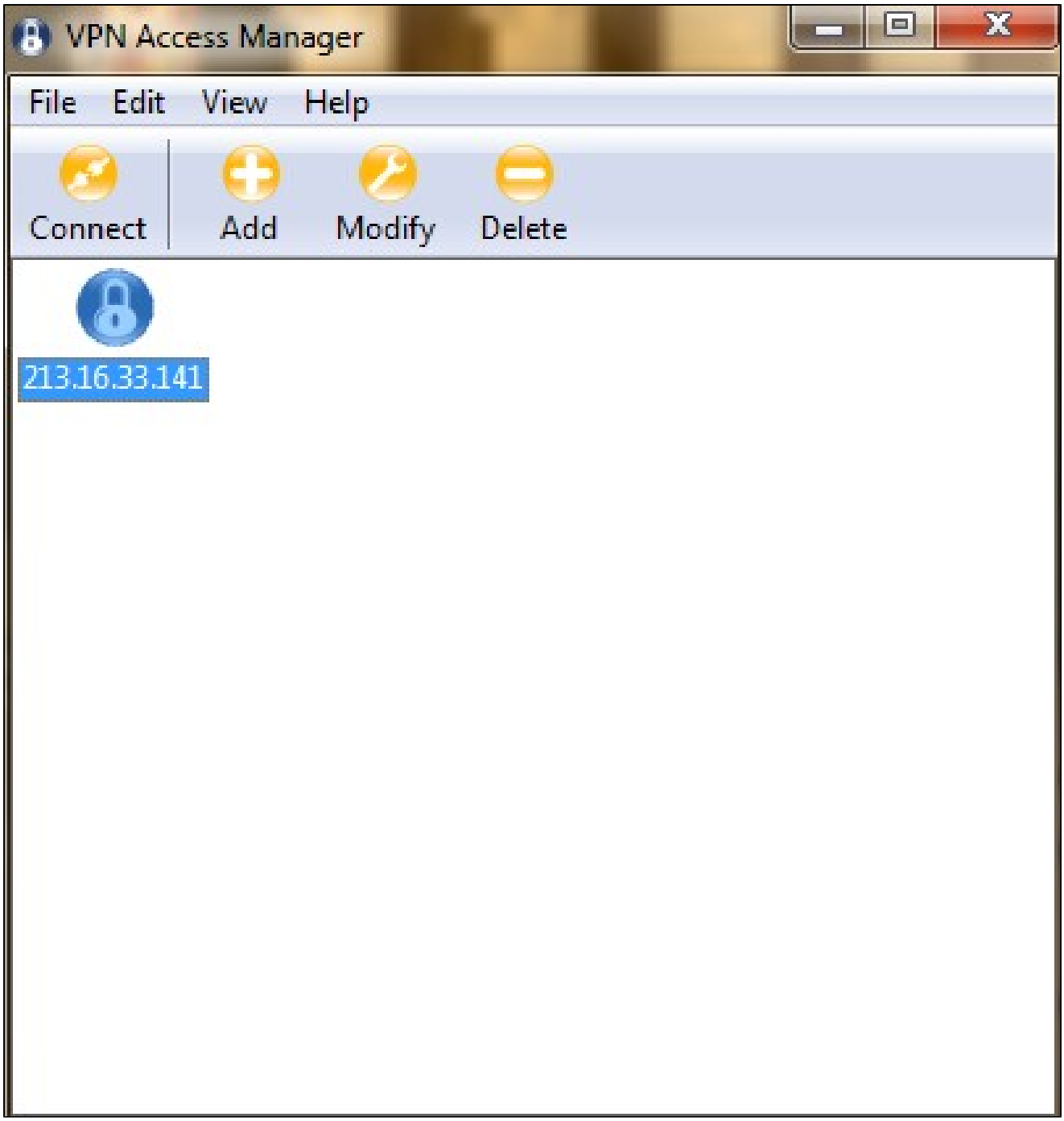
ステップ 8：Netmaskフィールドに、デバイスのサブネットマスクのアドレスを入力します。



ステップ 9 : [OK] をクリックします。RV0XXのIPアドレスとサブネットマスクアドレスがリモートネットワークリソースのリストに表示されます。



ステップ 10：Saveをクリックします。ユーザはVPN Access Managerウィンドウに戻り、新しいVPN接続が表示されます。

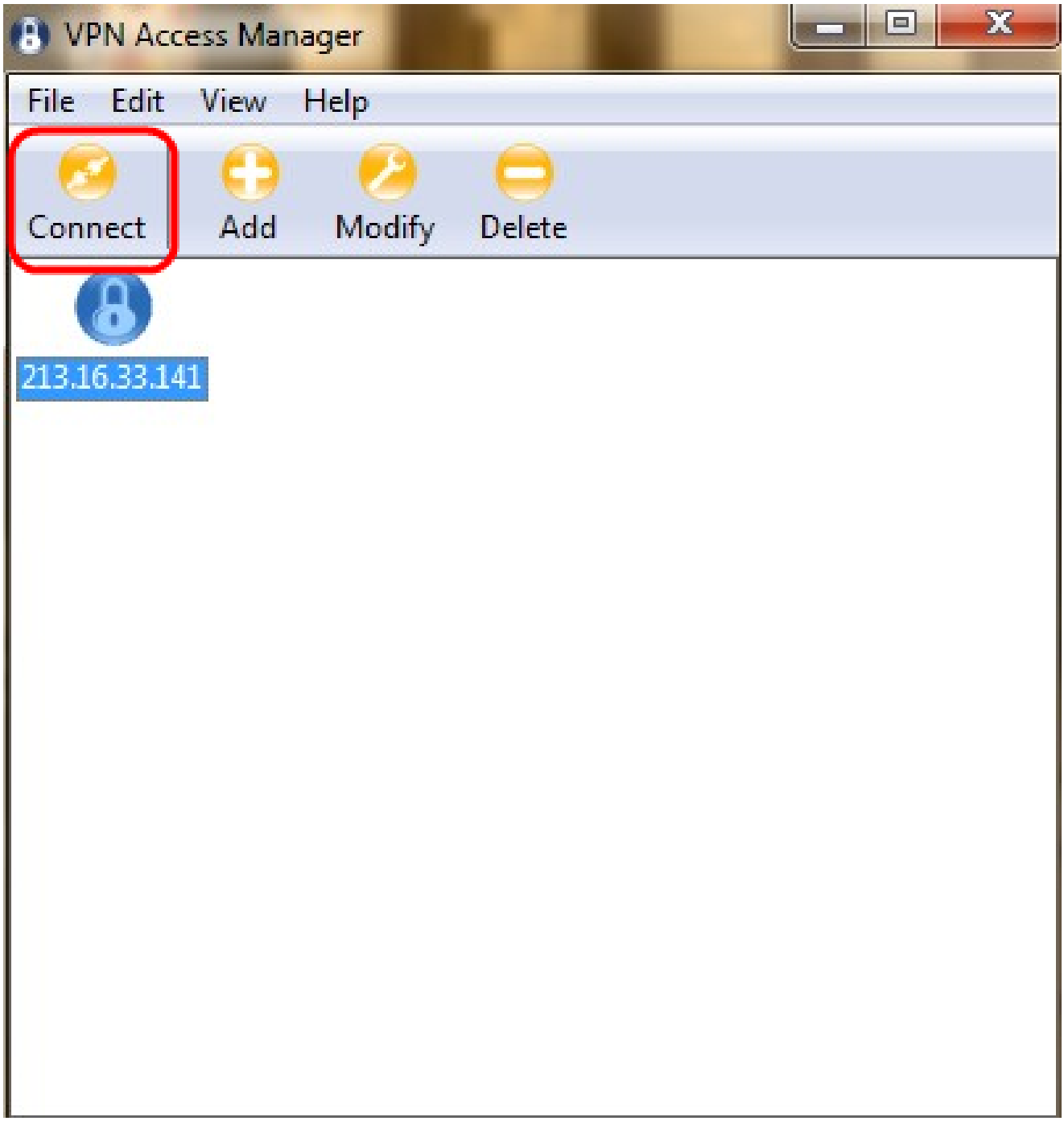


[Connect]

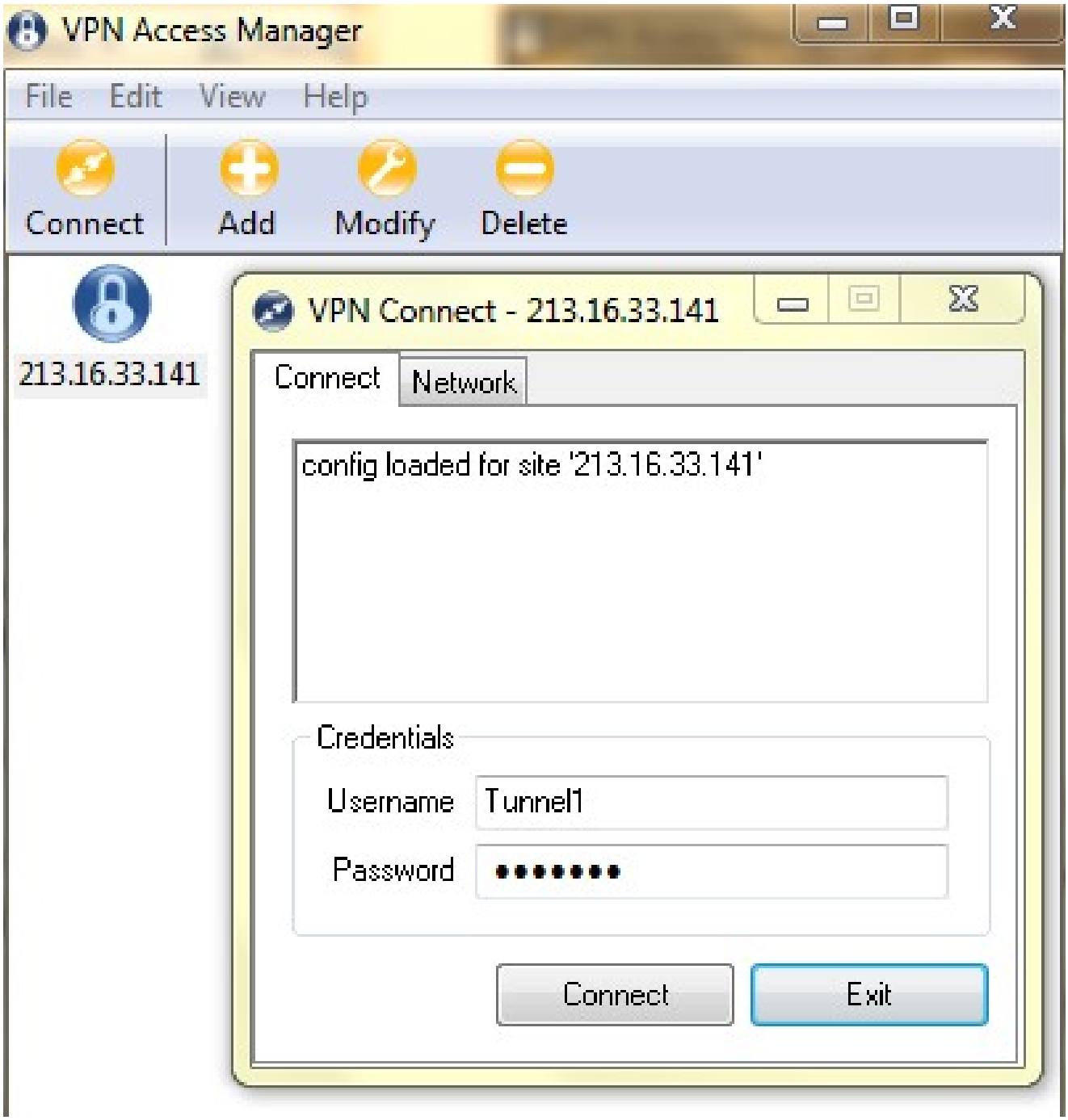
このセクションでは、すべての設定が完了した後にVPN接続をセットアップする方法について説明します。必要な口グイン情報は、デバイスで設定されているVPN Client Accessと同じです。

ステップ 1：目的のVPN接続をクリックします。

ステップ 2：[Connect] をクリックします。



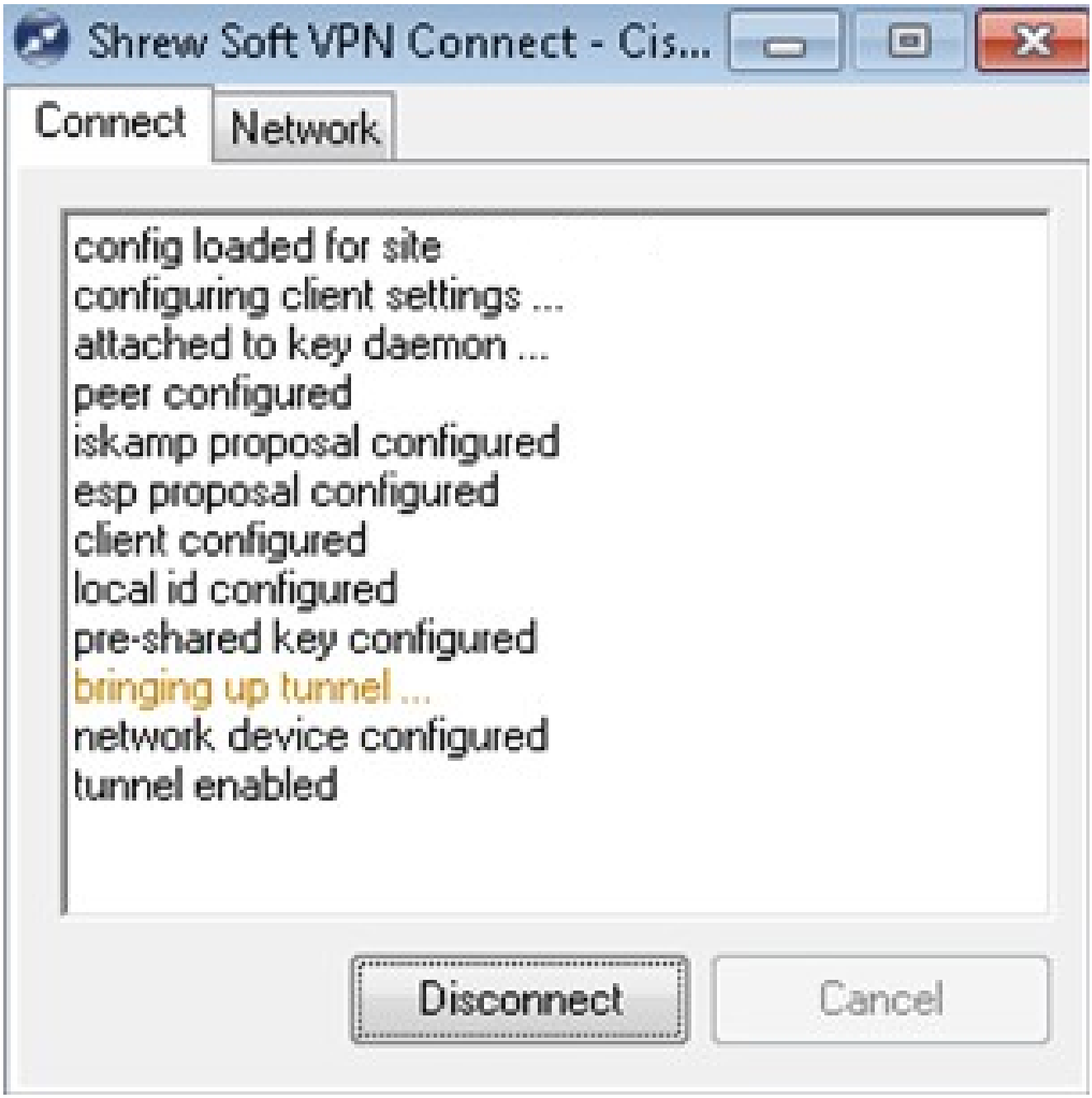
VPN Connectウィンドウが表示されます。



ステップ 3：UsernameフィールドにVPNのユーザ名を入力します。

ステップ 4：VPNユーザアカウントのパスワードをPasswordフィールドに入力します。

ステップ 5：[Connect] をクリックします。Shrew Soft VPN Connectウィンドウが表示されます。



ステップ6:（オプション）接続を無効にするには、Disconnectをクリックします。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。