

# Windowsを介した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、簡単に安全な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

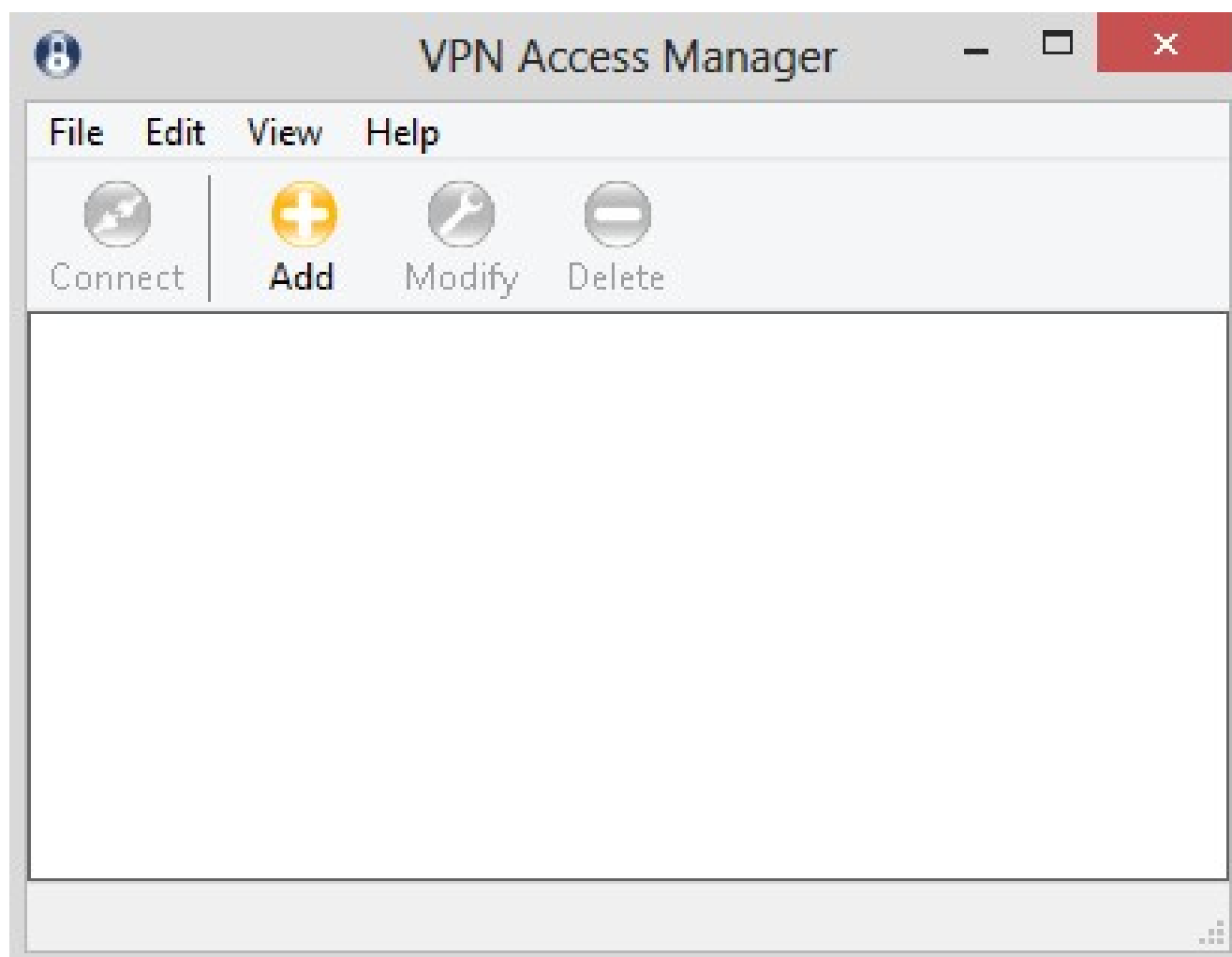
- ・ RV042
- ・ RV042G
- ・ RV082

## [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。

## VPN Site Configuration ✕

General Client Name Resolution Authentication ◀ ▶

Remote Host

Host Name or IP Address	Port
<input type="text"/>	<input type="text" value="500"/>

Auto Configuration  ▼

Local Host

Adapter Mode

▼

MTU   Obtain Automatically

Address	<input type="text" value="."/> <input type="text" value="."/> <input type="text" value="."/>
Netmask	<input type="text" value="."/> <input type="text" value="."/> <input type="text" value="."/>

### 一般的な設定

ステップ 1 : [General]タブをクリックします

## VPN Site Configuration X

General Client Name Resolution Authenticatic ◀ ▶

### Remote Host

Host Name or IP Address	Port
<input type="text"/>	<input type="text" value="500"/>
Auto Configuration	<input type="text" value="ike config pull"/> ▼

### Local Host

Adapter Mode

▼

MTU	<input type="text" value="1380"/>	<input checked="" type="checkbox"/>	Obtain Automatically
	Address	<input type="text" value="."/> <input type="text" value="."/> <input type="text" value="."/>	
	Netmask	<input type="text" value="."/> <input type="text" value="."/> <input type="text" value="."/>	

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。

The image shows a 'VPN Site Configuration' dialog box with a red 'X' close button in the top right corner. The 'General' tab is selected. The 'Remote Host' section is highlighted with a red rounded rectangle. It contains two input fields: 'Host Name or IP Address' with the value '213.16.33.141' and 'Port' with the value '400'. Below this is an 'Auto Configuration' dropdown menu set to 'ike config pull'. The 'Local Host' section is also visible, with 'Adapter Mode' set to 'Use a virtual adapter and assigned address', 'MTU' set to '1380', and 'Obtain Automatically' checked. 'Address' and 'Netmask' fields are empty. At the bottom are 'Save' and 'Cancel' buttons.

Remote Host	
Host Name or IP Address	Port
213.16.33.141	400
Auto Configuration	ike config pull

Local Host	
Adapter Mode	Use a virtual adapter and assigned address
MTU	<input checked="" type="checkbox"/> Obtain Automatically
1380	Address
	Netmask

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。

## VPN Site Configuration ✕

GeneralClientName ResolutionAuthenticatic◀▶

Remote Host

Host Name or IP Address	Port
213.16.33.141	400

Auto Configuration

- ike config pull ▼
- disabled
- ike config pull
- ike config push
- dhcp over ipsec

Local Host

Adapter Mode

Use a virtual adapter and assigned address▼

MTU   Obtain Automatically

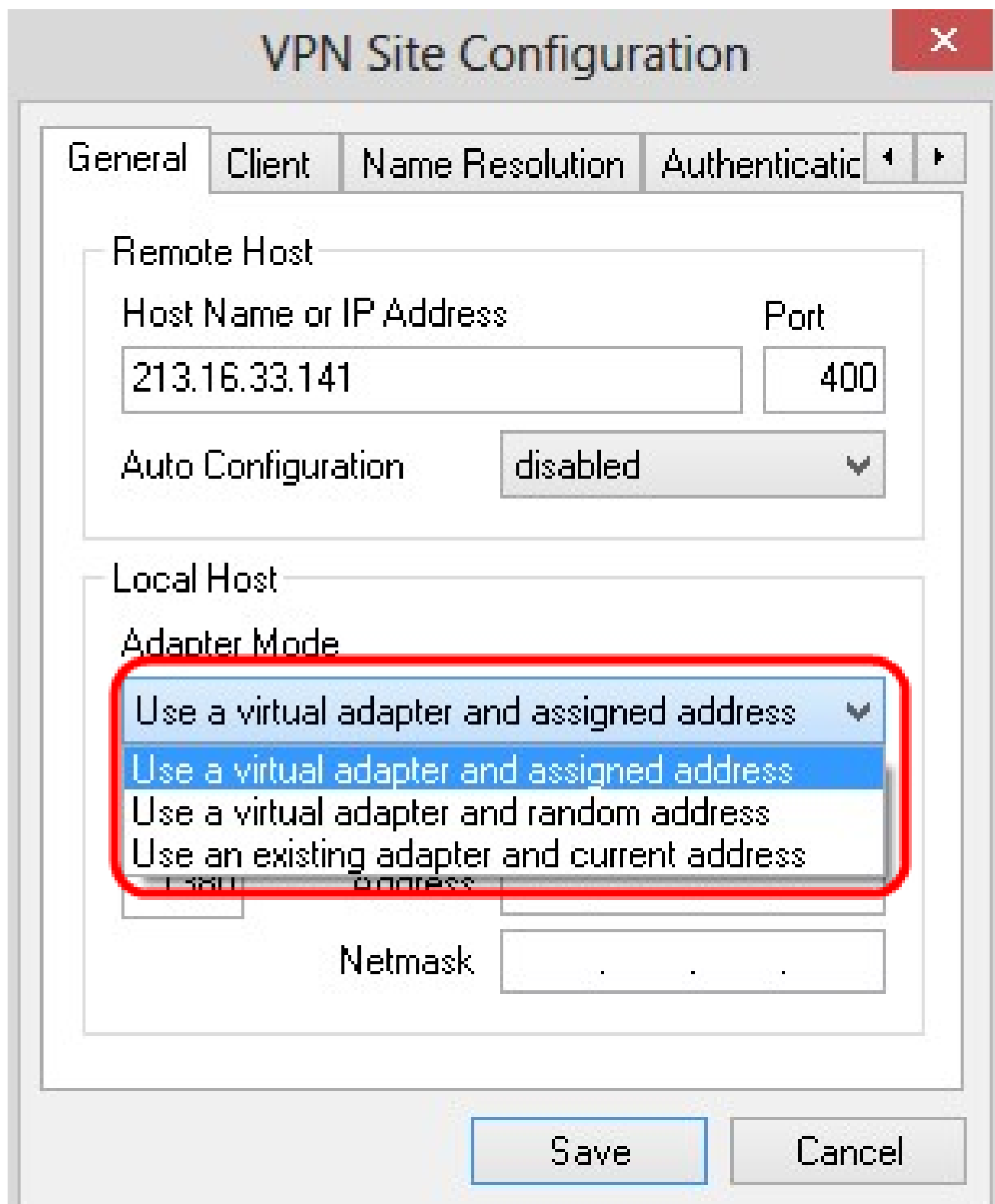
Address 

Netmask

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。



The image shows a 'VPN Site Configuration' dialog box with a red close button in the top right corner. The dialog has four tabs: 'General', 'Client', 'Name Resolution', and 'Authenticatic'. The 'General' tab is selected. It contains two main sections: 'Remote Host' and 'Local Host'. In the 'Remote Host' section, there are fields for 'Host Name or IP Address' (containing '213.16.33.141') and 'Port' (containing '400'). Below these is a dropdown for 'Auto Configuration' set to 'disabled'. The 'Local Host' section has a dropdown for 'Adapter Mode' which is open, showing four options: 'Use a virtual adapter and assigned address' (selected), 'Use a virtual adapter and assigned address', 'Use a virtual adapter and random address', and 'Use an existing adapter and current address'. Below the dropdown is a 'Netmask' field with three dots. At the bottom of the dialog are 'Save' and 'Cancel' buttons.

### VPN Site Configuration

General Client Name Resolution Authenticatic

Remote Host

Host Name or IP Address Port

213.16.33.141 400

Auto Configuration disabled

Local Host

Adapter Mode

- Use a virtual adapter and assigned address
- Use a virtual adapter and assigned address
- Use a virtual adapter and random address
- Use an existing adapter and current address

Netmask . . .

Save Cancel



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。

## VPN Site Configuration ✕

GeneralClientName ResolutionAuthenticatic◀▶

Remote Host

Host Name or IP Address	Port
<input type="text" value="213.16.33.141"/>	<input type="text" value="400"/>

Auto Configuration  ▼

Local Host

Adapter Mode

▼

MTU	<input type="text" value="1480"/>		<input checked="" type="checkbox"/> Obtain Automatically
	Address	<input type="text" value="."/> . .	
	Netmask	<input type="text" value="."/> . .	

Save

Cancel

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。

## VPN Site Configuration X

General Client Name Resolution Authenticatic ◀ ▶

### Firewall Options

NAT Traversal	<input type="text" value="enable"/>
NAT Traversal Port	<input type="text" value="4500"/>
Keep-alive packet rate	<input type="text" value="15"/> Secs
IKE Fragmentation	<input type="text" value="enable"/>
Maximum packet size	<input type="text" value="540"/> Bytes

### Other Options

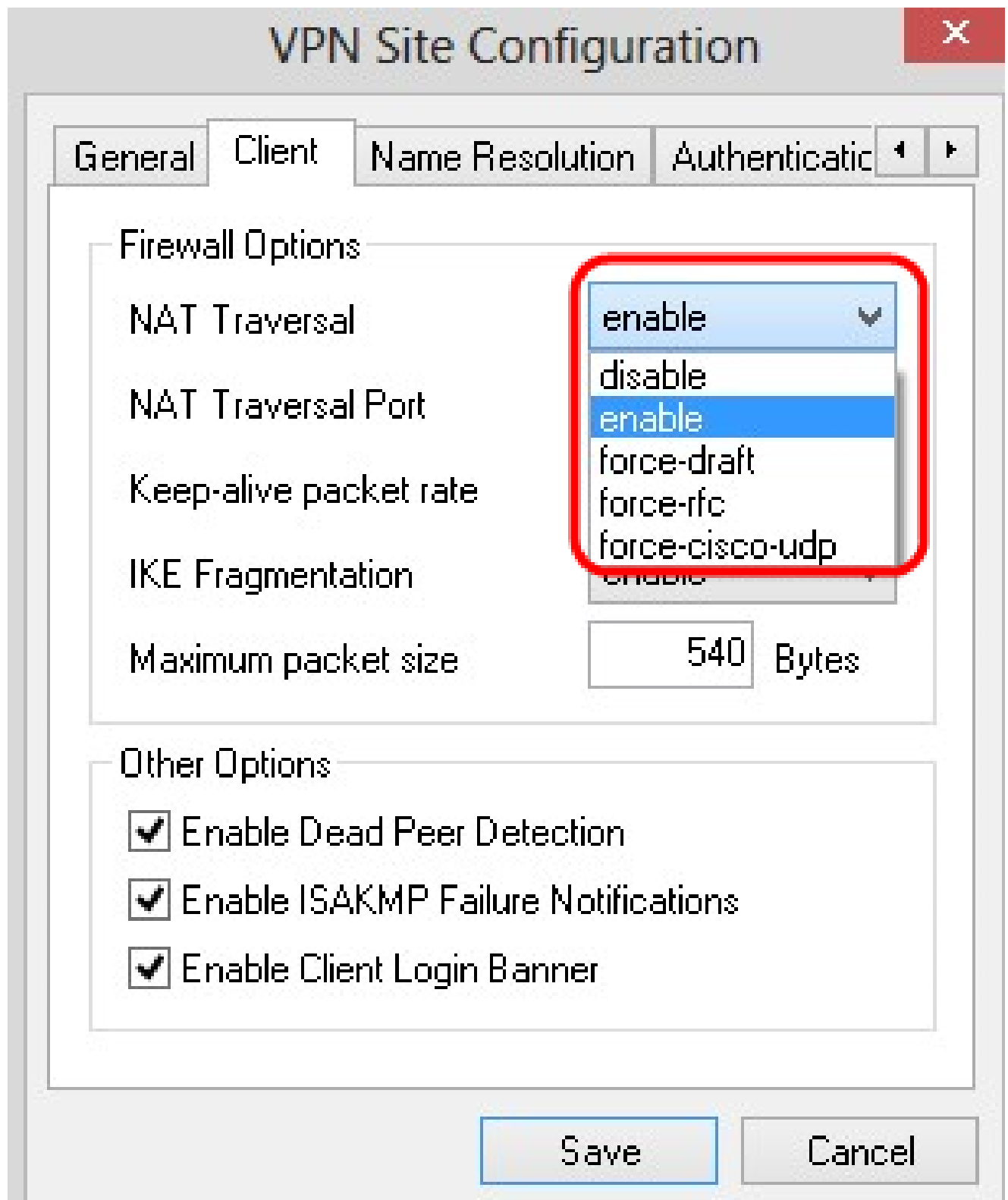
- Enable Dead Peer Detection
- Enable ISAKMP Failure Notifications
- Enable Client Login Banner

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。

## VPN Site Configuration ✕

GeneralClientName ResolutionAuthenticatic◀▶

**Firewall Options**

NAT Traversal	<input type="text" value="force-draft"/>
NAT Traversal Port	<input type="text" value="4400"/>
Keep-alive packet rate	<input type="text" value="17"/> Secs
IKE Fragmentation	<input type="text" value="enable"/>
Maximum packet size	<input type="text" value="540"/> Bytes

**Other Options**

- Enable Dead Peer Detection
- Enable ISAKMP Failure Notifications
- Enable Client Login Banner

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。

The image shows a 'VPN Site Configuration' dialog box with the 'Client' tab selected. The 'Firewall Options' section contains the following settings:

- NAT Traversal: force-draft
- NAT Traversal Port: 4400
- Keep-alive packet rate: 17 Secs
- IKE Fragmentation: enable (highlighted in a red box)
- Maximum packet size: (empty)

The 'Other Options' section has three checked checkboxes:

- Enable Dead Peer Detection
- Enable ISAKMP Failure Notifications
- Enable Client Login Banner

At the bottom, there are 'Save' and 'Cancel' buttons.

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。



## VPN Site Configuration ✕

General Client Name Resolution Authenticatic ◀ ▶

**Firewall Options**

NAT Traversal	<input type="text" value="force-draft"/>
NAT Traversal Port	<input type="text" value="4400"/>
Keep-alive packet rate	<input type="text" value="17"/> Secs
IKE Fragmentation	<input type="text" value="force"/>
Maximum packet size	<input type="text" value="520"/> Bytes

**Other Options**

- Enable Dead Peer Detection
- Enable ISAKMP Failure Notifications
- Enable Client Login Banner

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。

**VPN Site Configuration** ✕

General Client **Name Resolution** Authenticatic ◀ ▶

DNS WINS

Enable DNS  Obtain Automatically

Server Address #1

Server Address #2

Server Address #3

Server Address #4

Obtain Automatically

DNS Suffix

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。

## VPN Site Configuration

✕

GeneralClientName ResolutionAuthenticatic◀▶

**DNS**WINS

Enable DNS

Obtain Automatically

Server Address #1

Server Address #2

Server Address #3

Server Address #4

Obtain Automatically

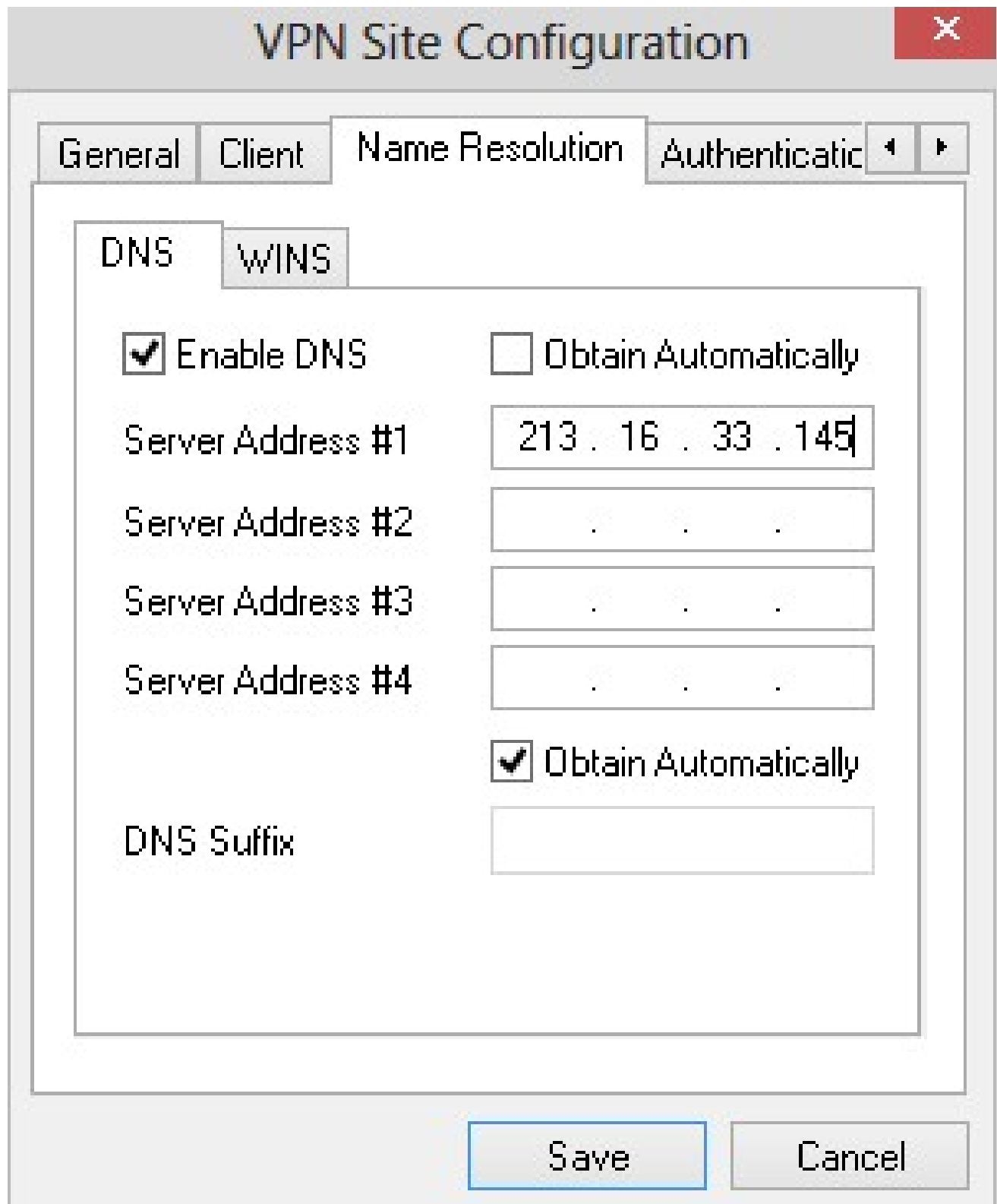
DNS Suffix

SaveCancel

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。



The image shows a 'VPN Site Configuration' dialog box with a red close button in the top right corner. The 'Name Resolution' tab is selected, and within it, the 'DNS' sub-tab is active. The 'WINS' sub-tab is also visible. The 'Enable DNS' checkbox is checked, and the 'Obtain Automatically' checkbox is unchecked. The 'Server Address #1' field contains the IP address '213 . 16 . 33 . 145'. The 'Server Address #2', 'Server Address #3', and 'Server Address #4' fields are empty and contain three dots. The 'Obtain Automatically' checkbox at the bottom is checked. The 'DNS Suffix' field is empty. At the bottom of the dialog are 'Save' and 'Cancel' buttons.

Field	Value
Enable DNS	<input checked="" type="checkbox"/>
Obtain Automatically	<input type="checkbox"/>
Server Address #1	213 . 16 . 33 . 145
Server Address #2	. . .
Server Address #3	. . .
Server Address #4	. . .
Obtain Automatically (bottom)	<input checked="" type="checkbox"/>
DNS Suffix	

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。

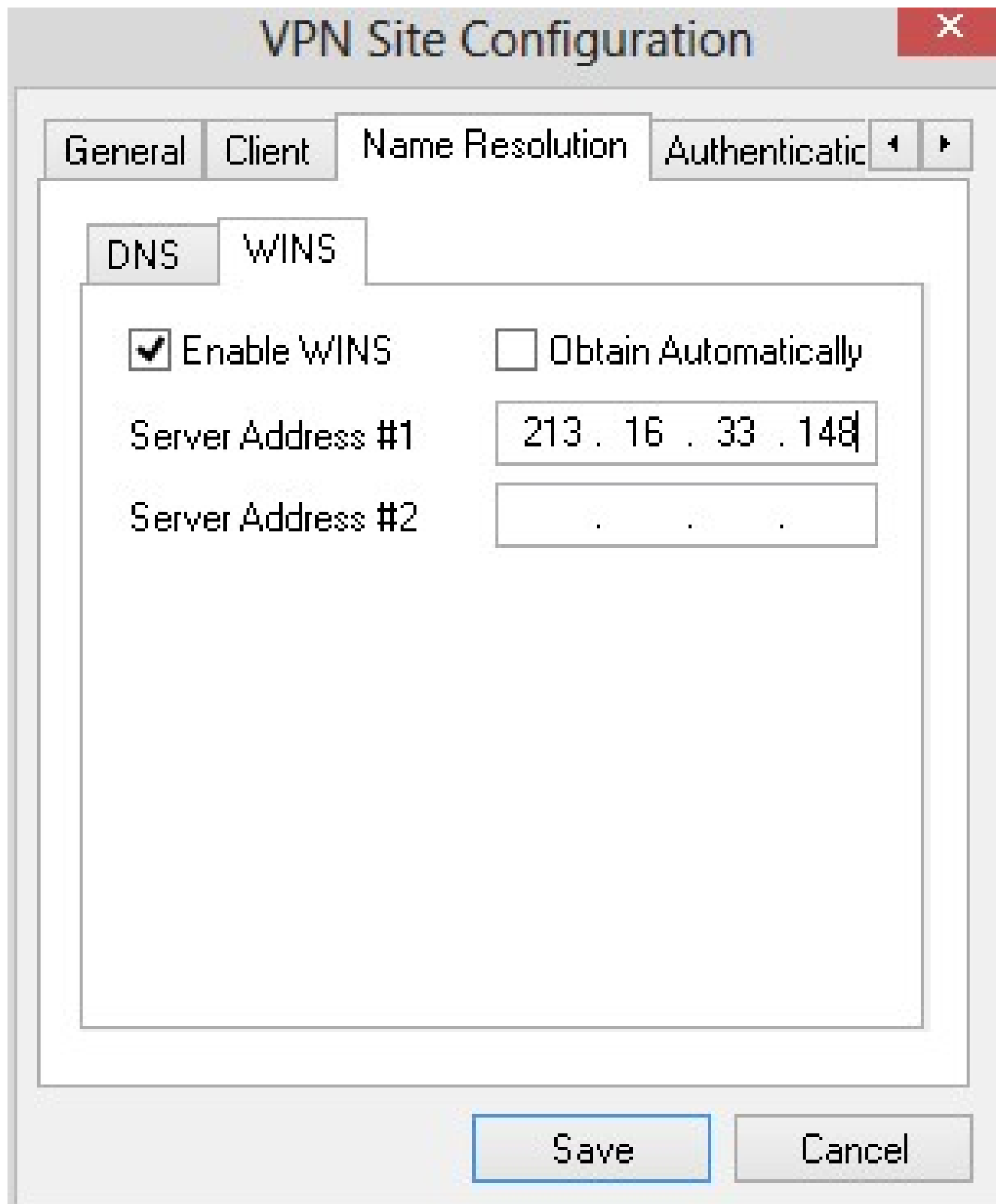
ステップ 9 : WINSタブをクリックします。

The image shows a screenshot of the 'VPN Site Configuration' dialog box. The title bar at the top reads 'VPN Site Configuration' and has a red close button on the right. Below the title bar are four tabs: 'General', 'Client', 'Name Resolution', and 'Authenticatic'. The 'Name Resolution' tab is selected. Inside this tab, there are two sub-tabs: 'DNS' and 'WINS'. The 'WINS' sub-tab is selected and highlighted with a red circle. Below the sub-tabs, there are two checked checkboxes: 'Enable WINS' and 'Obtain Automatically'. Underneath these are two input fields labeled 'Server Address #1' and 'Server Address #2', each containing three dots. At the bottom of the dialog box are two buttons: 'Save' and 'Cancel'.

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。

## VPN Site Configuration ✕

ClientName ResolutionAuthenticationPhase ◀ ▶

Authentication Method Hybrid RSA + XAuth ▼

Local IdentityRemote IdentityCredentials

Identification Type

Fully Qualified Domain Name ▼

FQDN String

Save

Cancel

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。

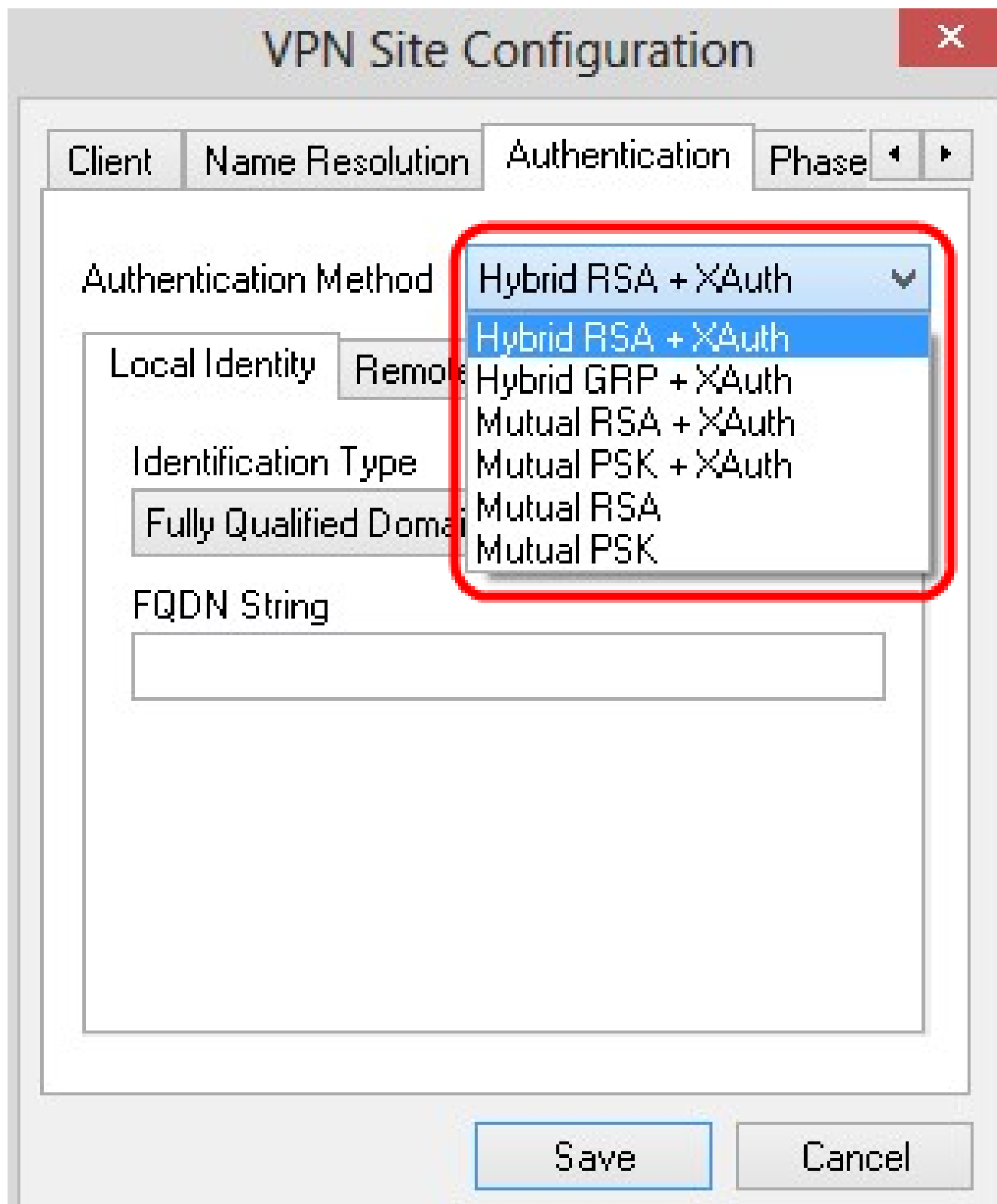
- ・ ハイブリッドGRP + XAuth：クライアントクレデンシャルは必要ありません。クライアントはゲートウェイを認証します。クレデンシャルは、PEMまたはPKCS12証明書ファイルと共有秘密文字列の形式になります。

- ・ 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。

## VPN Site Configuration

✕

Client | Name Resolution | Authentication | Phase ◀ ▶

Authentication Method Hybrid RSA + XAuth ▼

Local Identity | Remote Identity | Credentials

Identification Type

Fully Qualified Domain Name ▼

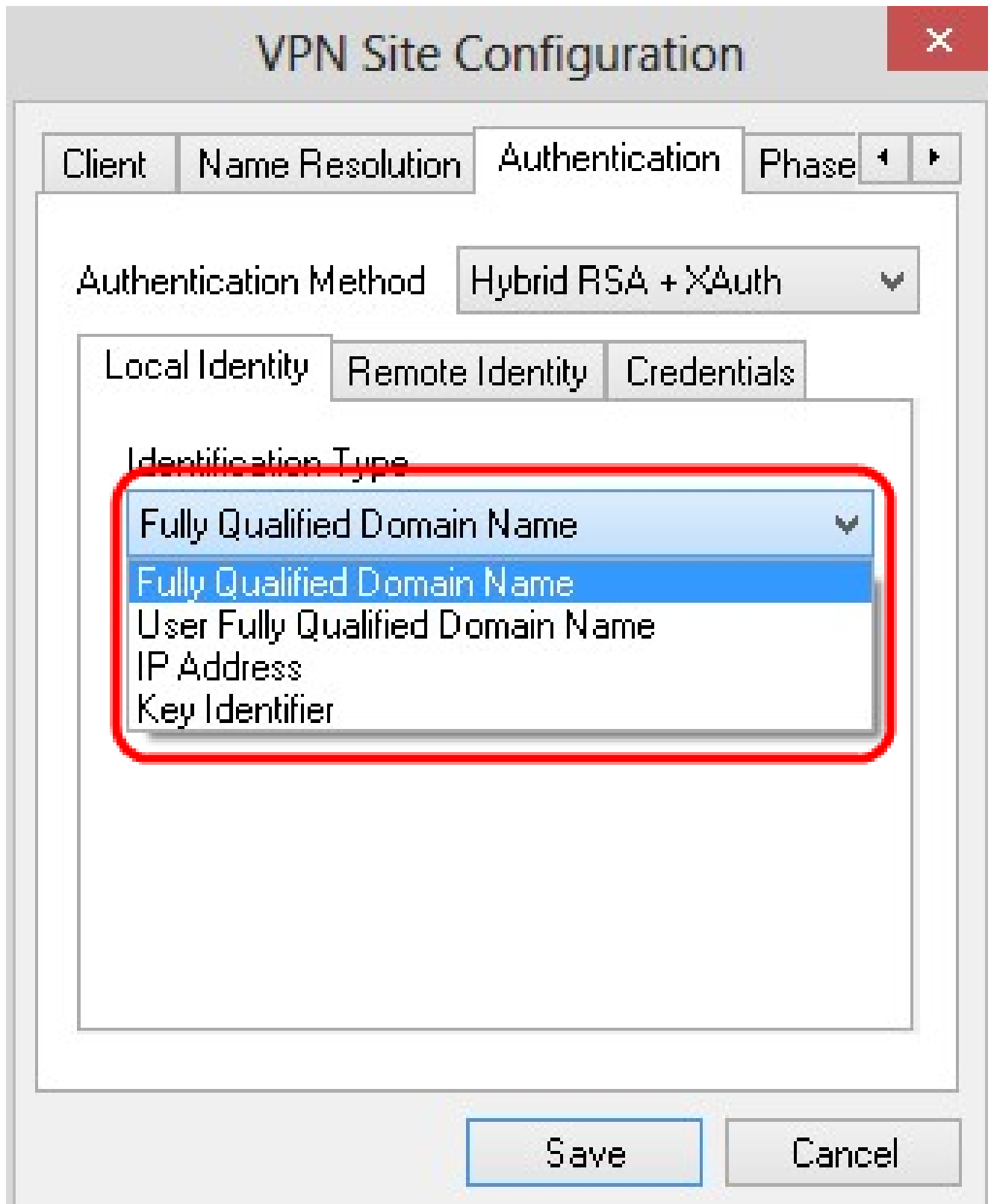
FQDN String

Save Cancel

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。

### VPN Site Configuration ✕

ClientName ResolutionAuthenticationPhase ◀ ▶

Authentication Method Hybrid RSA + XAuth ▼

Local IdentityRemote IdentityCredentials

Identification Type  
Any ▼

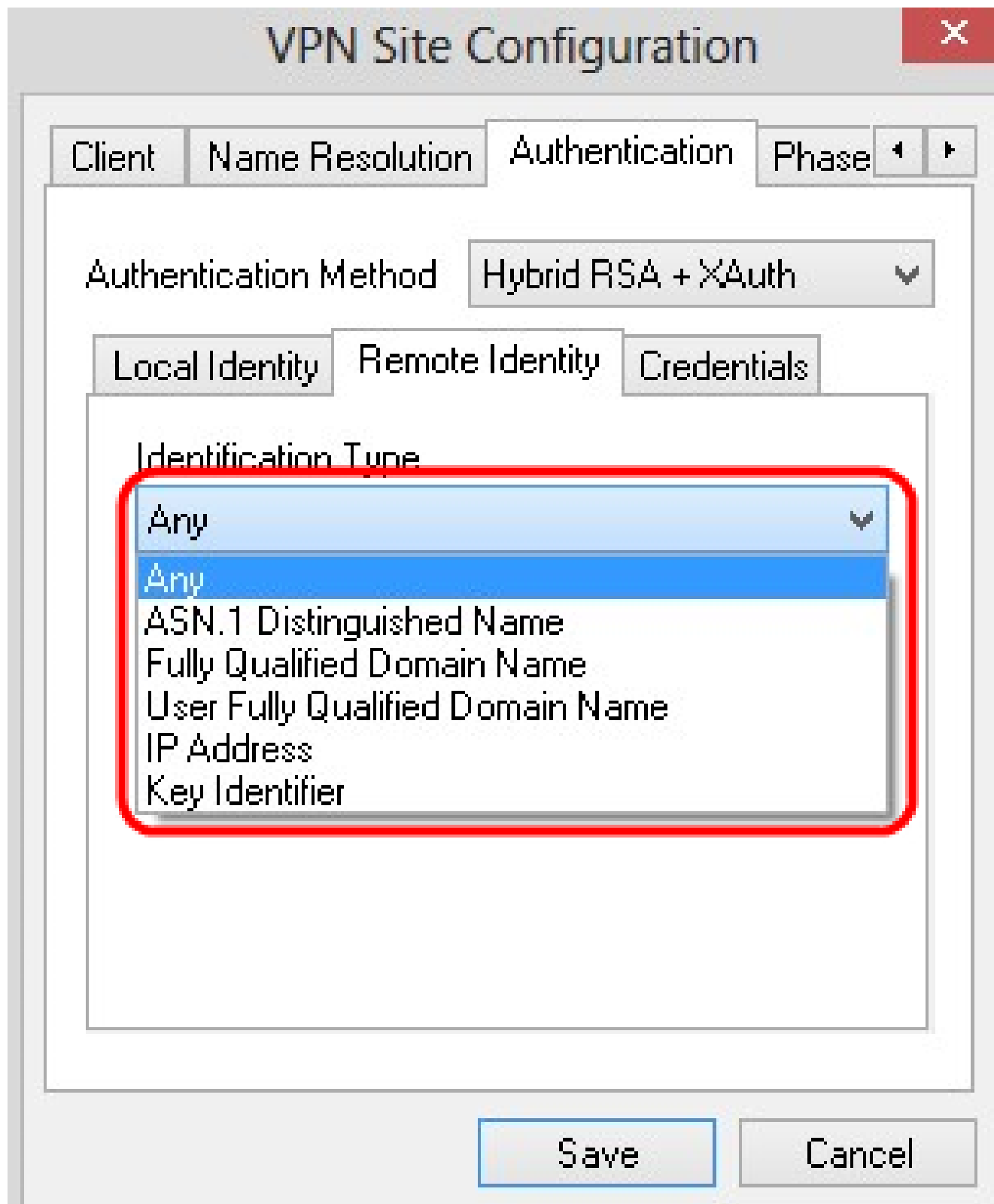
SaveCancel

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。

## VPN Site Configuration

✕

---

ClientName ResolutionAuthenticationPhase

Authentication Method Hybrid RSA + XAuth

Local IdentityRemote IdentityCredentials

Server Certificate Authority File ...

Client Certificate File ...

Client Private Key File ...

Pre Shared Key

SaveCancel

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。

## VPN Site Configuration

✕

---

ClientName ResolutionAuthenticationPhase

Authentication Method: Mutual PSK

Local IdentityRemote IdentityCredentials

Server Certificate Authority File

...

Client Certificate File

...

Client Private Key File

...

Pre Shared Key

SaveCancel

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。

## VPN Site Configuration

✕

---

Name ResolutionAuthenticationPhase 1Pha: ◀ ▶

Proposal Parameters

Exchange Type	aggressive ▼
DH Exchange	group 2 ▼
Cipher Algorithm	auto ▼
Cipher Key Length	▼ Bits
Hash Algorithm	auto ▼
Key Life Time limit	86400 Secs
Key Life Data limit	0 Kbytes

Enable Check Point Compatible Vendor ID

SaveCancel

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。

VPN Site Configuration

Name Resolution Authentication Phase 1 Pha: ◀ ▶

Proposal Parameters

Exchange Type aggressive

DH Exchange aggressive

Cipher Algorithm auto

Cipher Key Length Bits

Hash Algorithm auto

Key Life Time limit 86400 Secs

Key Life Data limit 0 Kbytes

Enable Check Point Compatible Vendor ID

Save Cancel

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。



### VPN Site Configuration

✕

Name ResolutionAuthenticationPhase 1Phase 2

Proposal Parameters

Exchange Type	aggressive	▼
DH Exchange	group 1	▼
Cipher Algorithm	des	▼
Cipher Key Length		▼ Bits
Hash Algorithm	md5	▼
Key Life Time limit	85400	Secs
Key Life Data limit	10	Kbytes

Enable Check Point Compatible Vendor ID

SaveCancel

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。

## VPN Site Configuration

✕

AuthenticationPhase 1Phase 2Policy◀▶

Proposal Parameters

Transform Algorithm	auto ▼
Transform Key Length	▼ Bits
HMAC Algorithm	auto ▼
PFS Exchange	disabled ▼
Compress Algorithm	disabled ▼
Key Life Time limit	3600 Secs
Key Life Data limit	0 Kbytes

SaveCancel

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。

## VPN Site Configuration ✕

AuthenticationPhase 1Phase 2Policy◀ ▶

**Proposal Parameters**

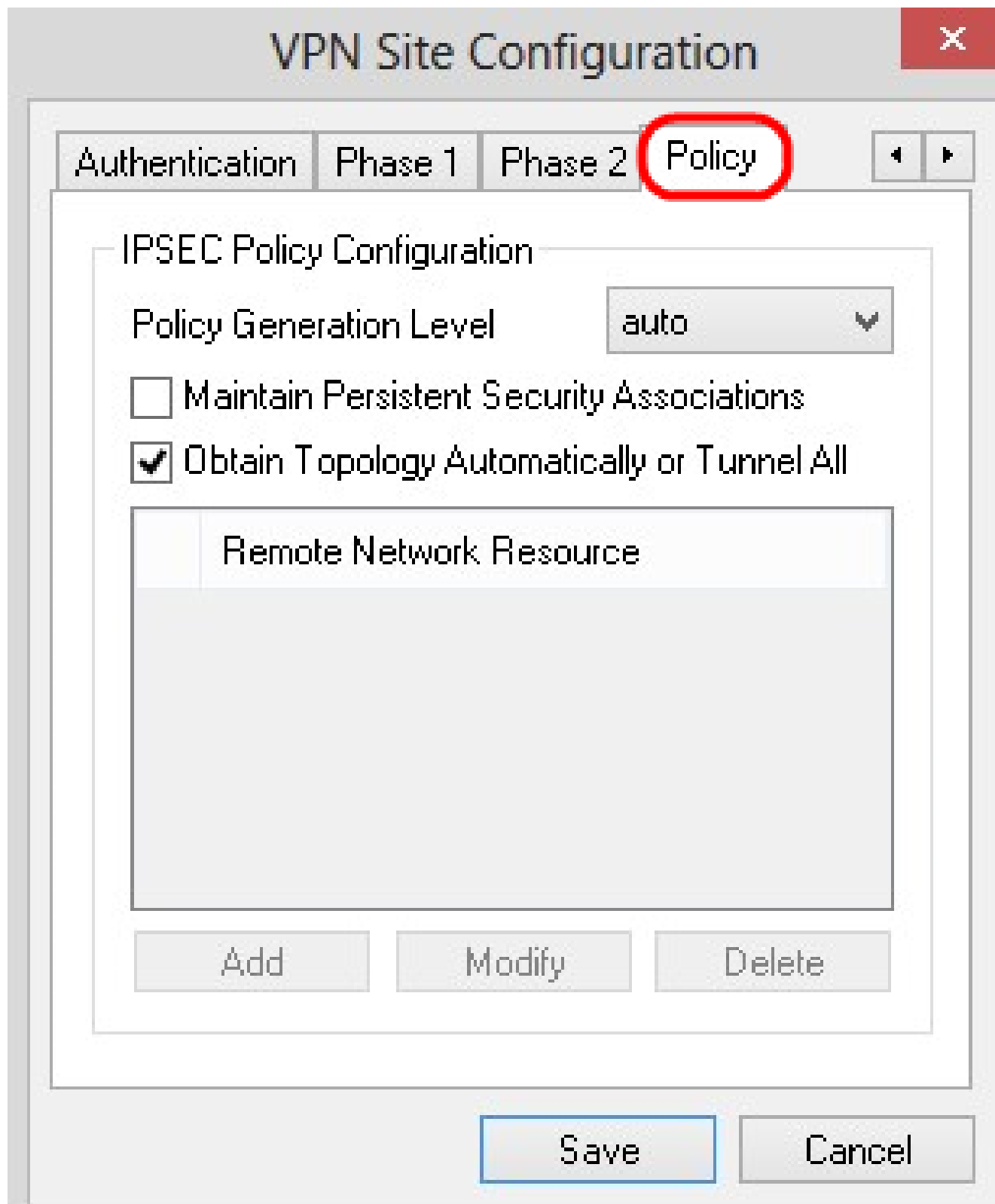
Transform Algorithm	esp-3des ▼
Transform Key Length	▼ Bits
HMAC Algorithm	md5 ▼
PFS Exchange	group 1 ▼
Compress Algorithm	deflate ▼
Key Life Time limit	3500 Secs
Key Life Data limit	10 Kbytes

SaveCancel

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

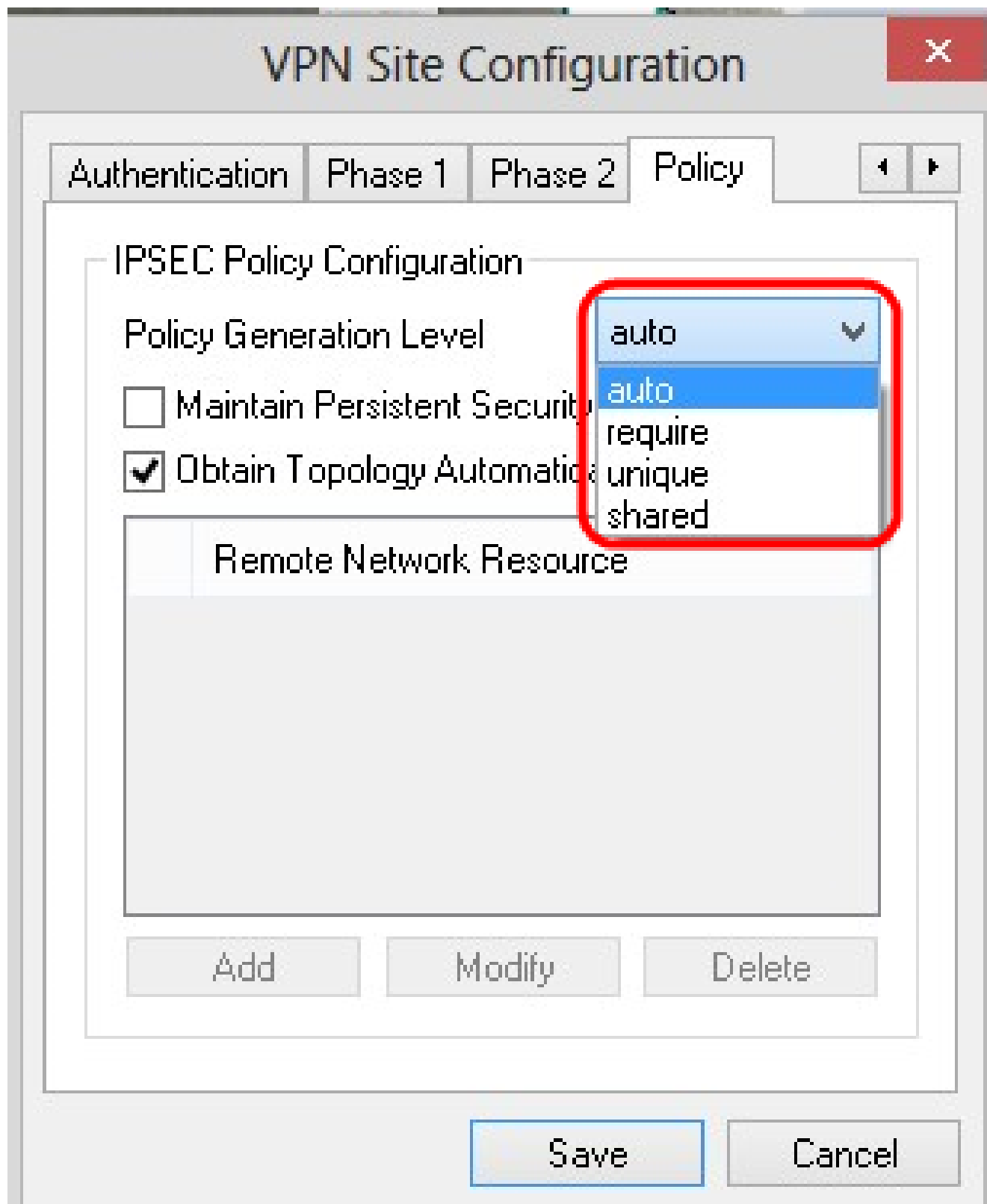
ステップ1:Policyタブをクリックします。



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。

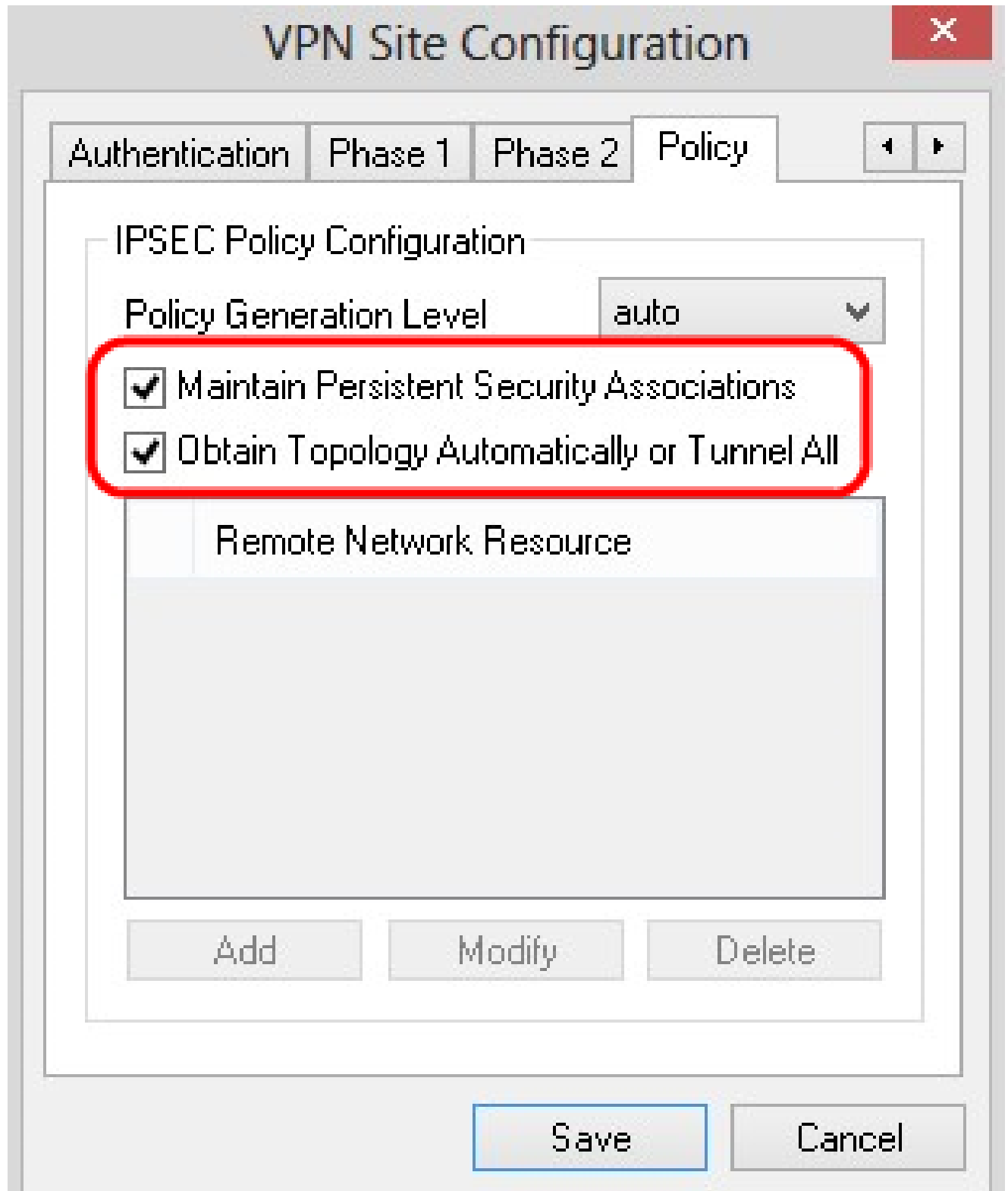
- ・ Auto : 必要なIPSecポリシーレベルが自動的に決定されます。
- ・ Require : 各ポリシーの一意のセキュリティ・アソシエーションはネゴシエートされません。
- ・ Unique : 各ポリシーに対する一意のセキュリティ・アソシエーションがネゴシエートされます。
- ・ 共有 : 適切なポリシーが必要なレベルで生成されます。



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。



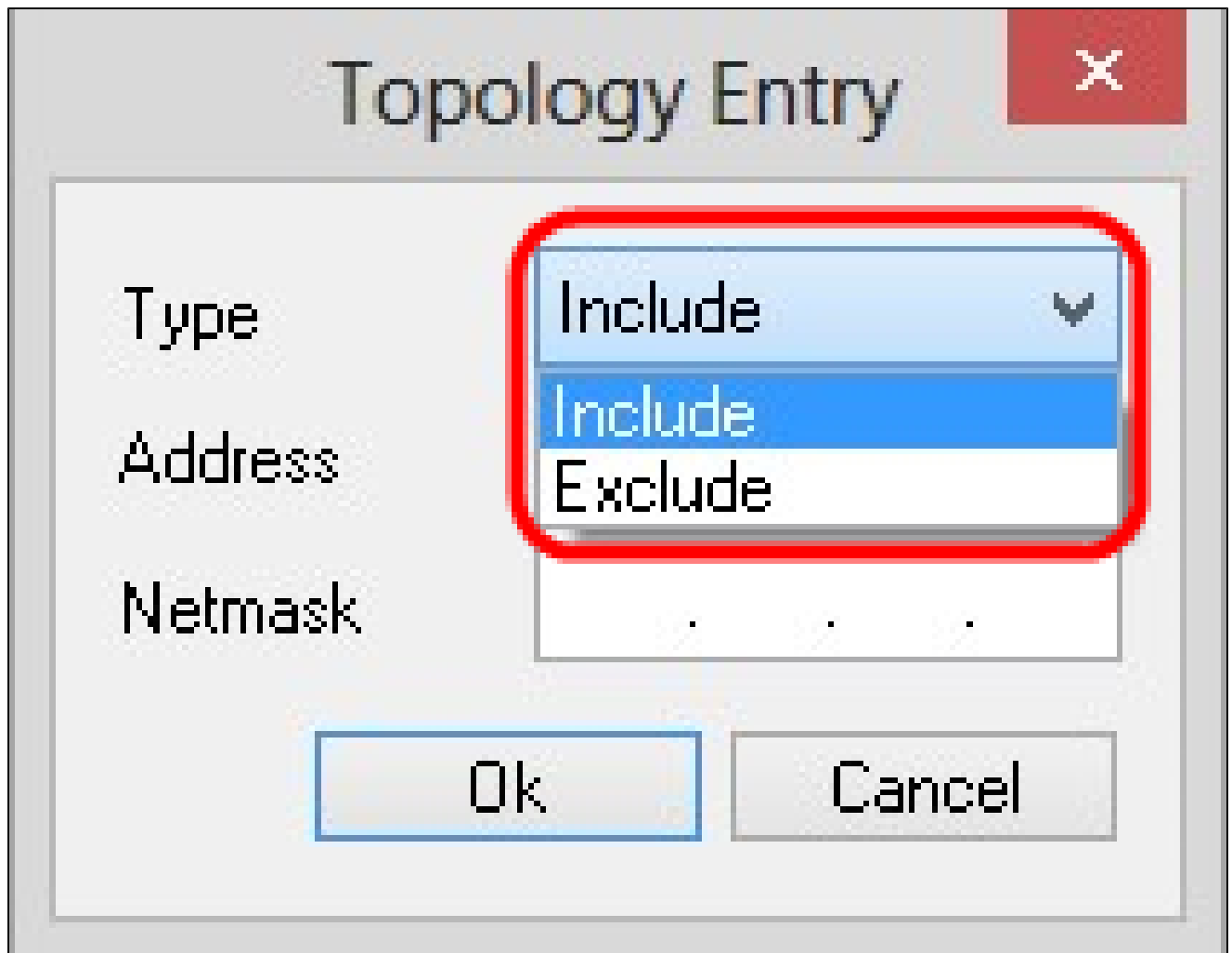
ステップ 5 : Addをクリックして、トポロジエントリをテーブルに追加します。Topology Entryウィンドウが表示されます。



The image shows a dialog box titled "Topology Entry". It contains three input fields: "Type" (a dropdown menu currently showing "Include"), "Address" (a text field with a dotted placeholder), and "Netmask" (a text field with a dotted placeholder). At the bottom of the dialog are two buttons: "Ok" and "Cancel".

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。

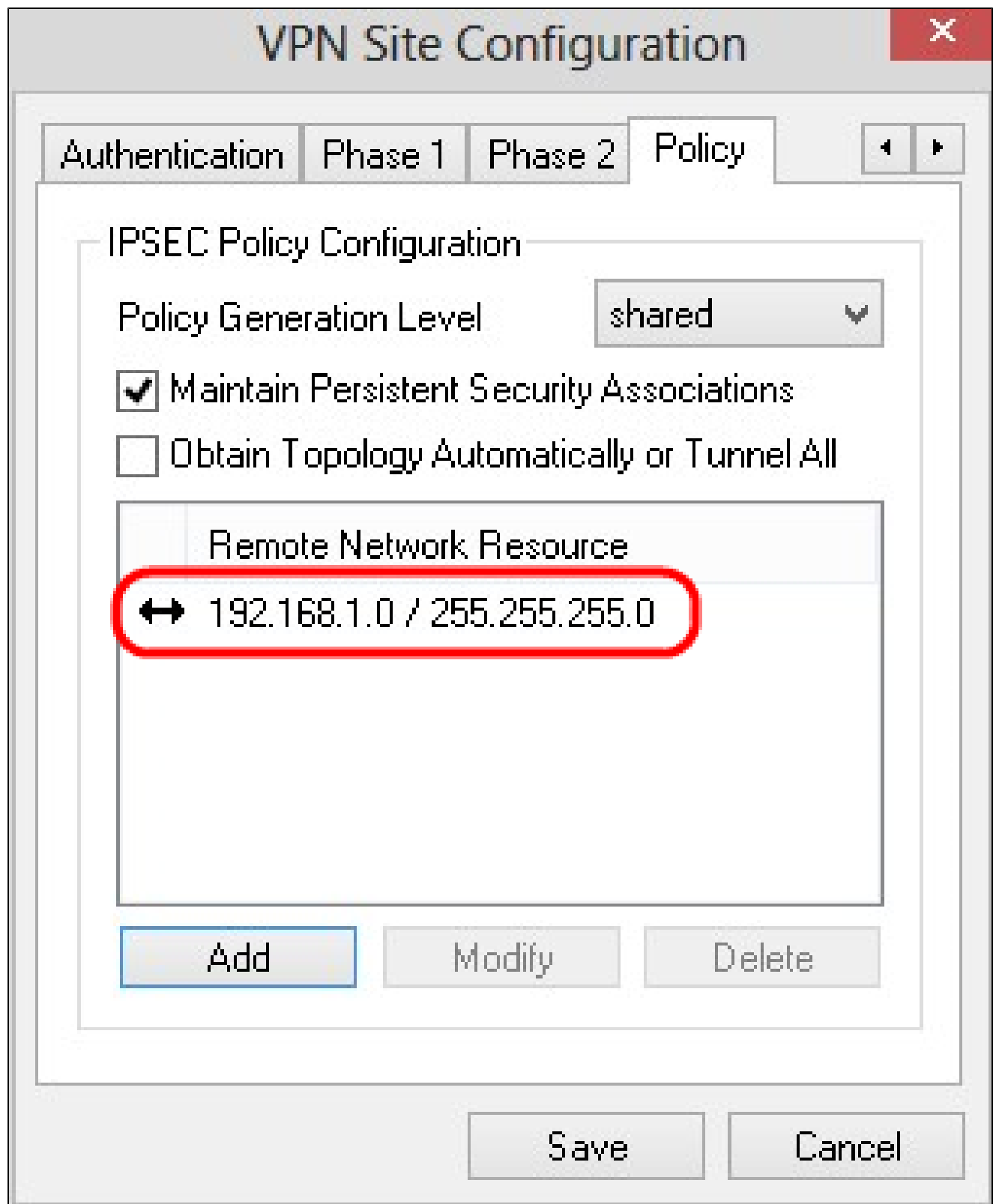
ステップ 8 : Netmaskフィールドに、デバイスのサブネットマスクのアドレスを入力します。  
。

# Topology Entry X

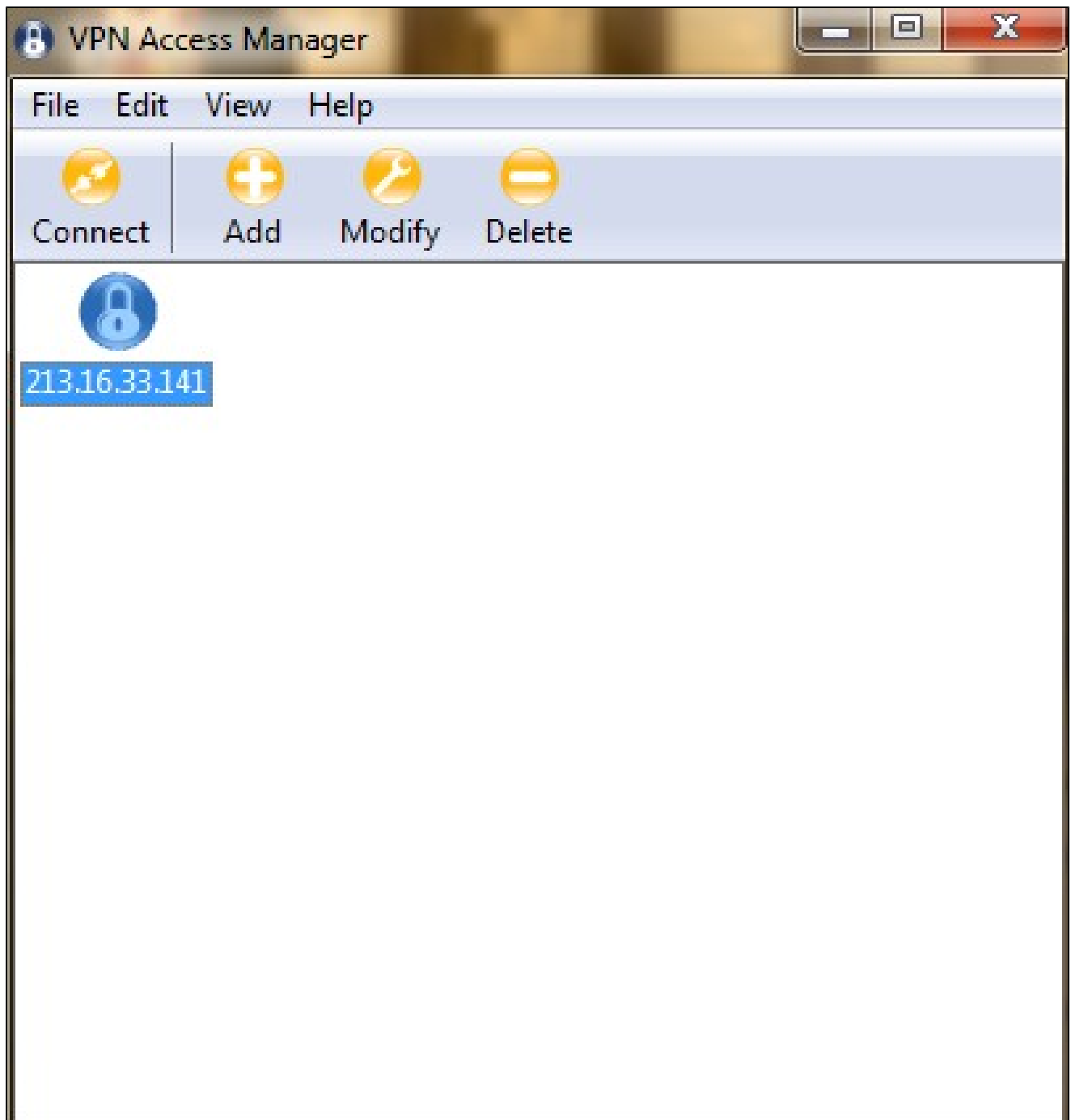
Type	Include <span style="float: right;">▼</span>
Address	192.168.1.0
Netmask	255.255.255.0

OkCancel

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。

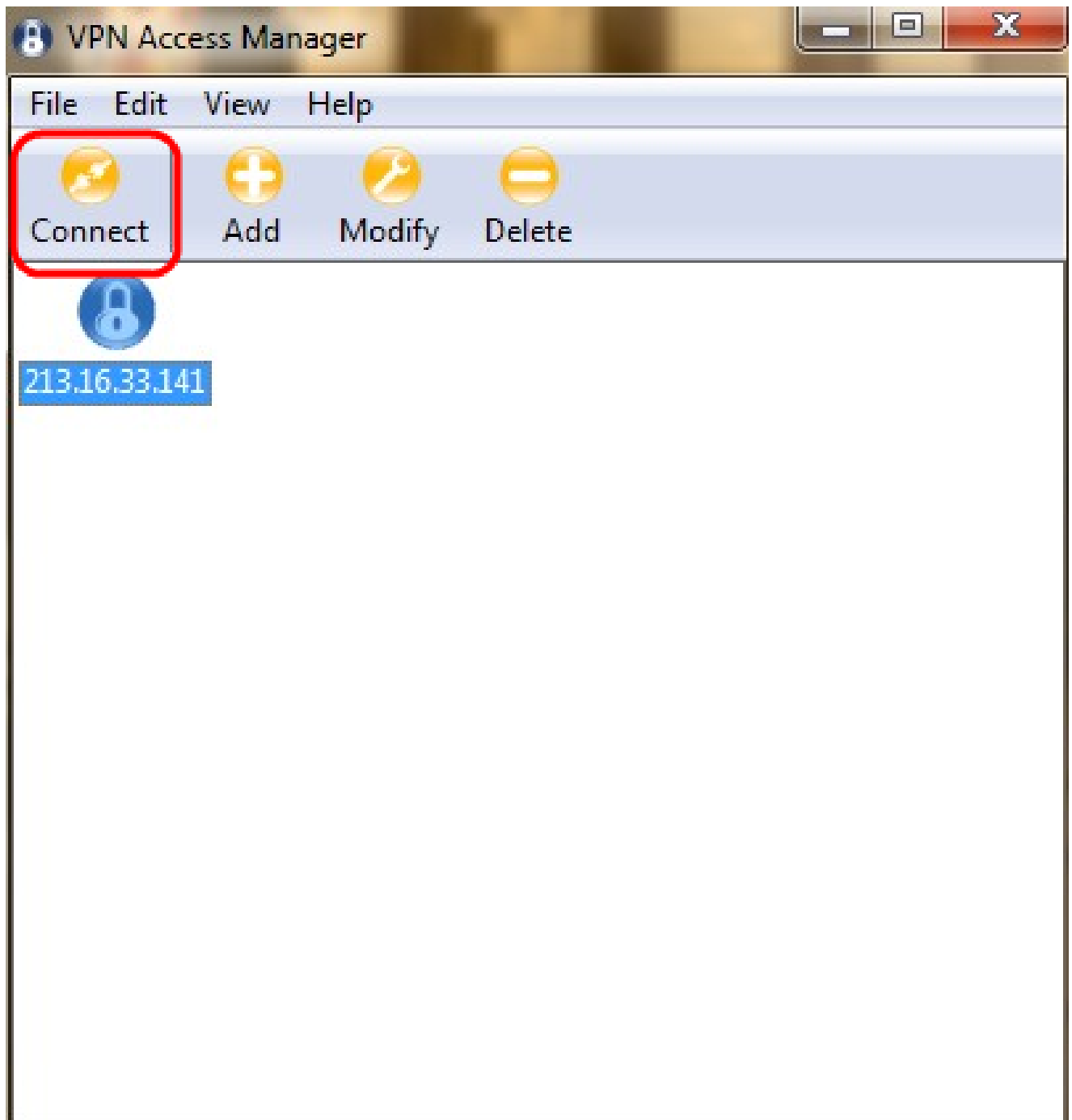


## [Connect]

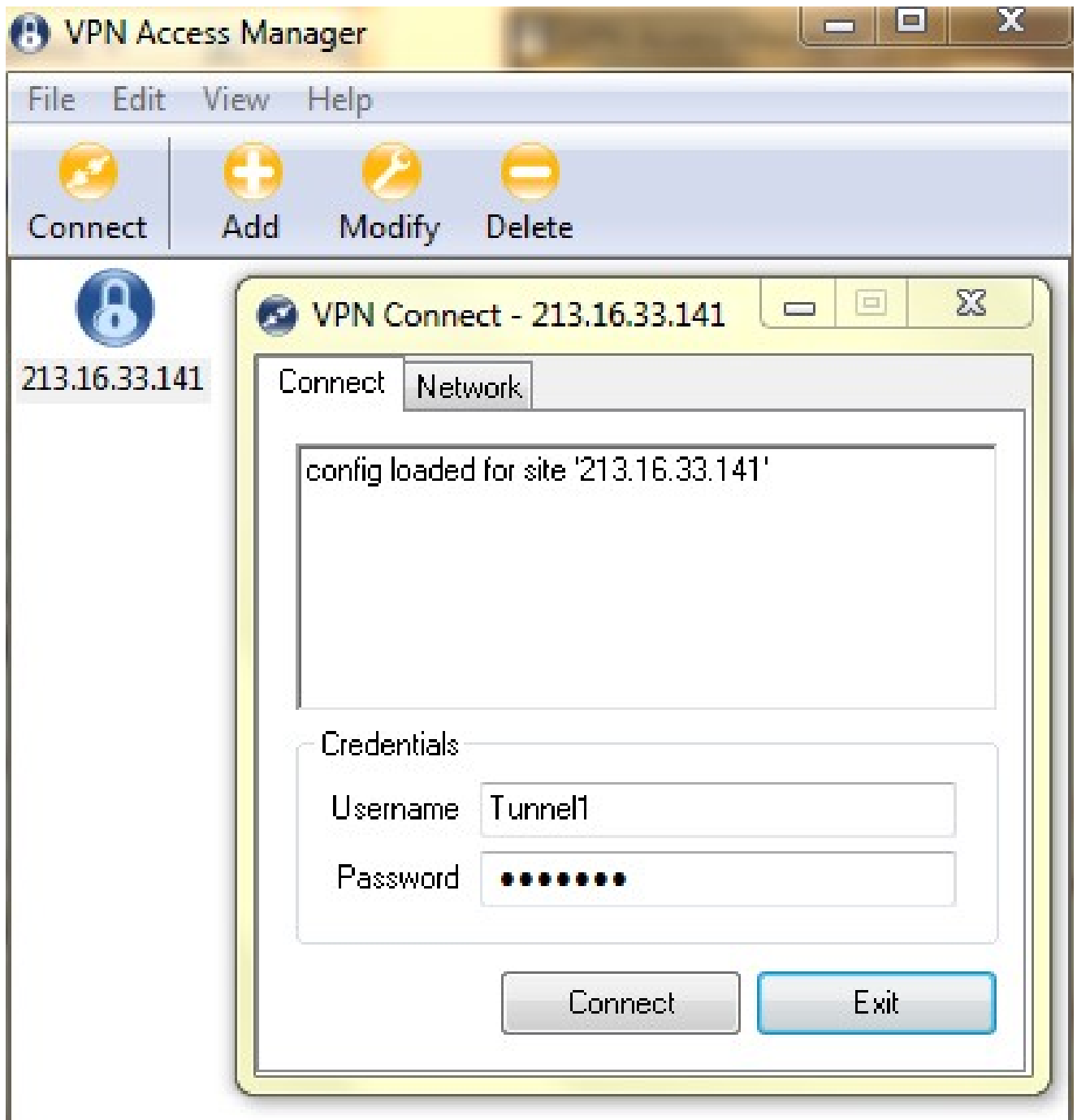
このセクションでは、すべての設定が完了した後にVPN接続をセットアップする方法について説明します。必要なログイン情報は、デバイスで設定されているVPN Client Accessと同じです。

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。



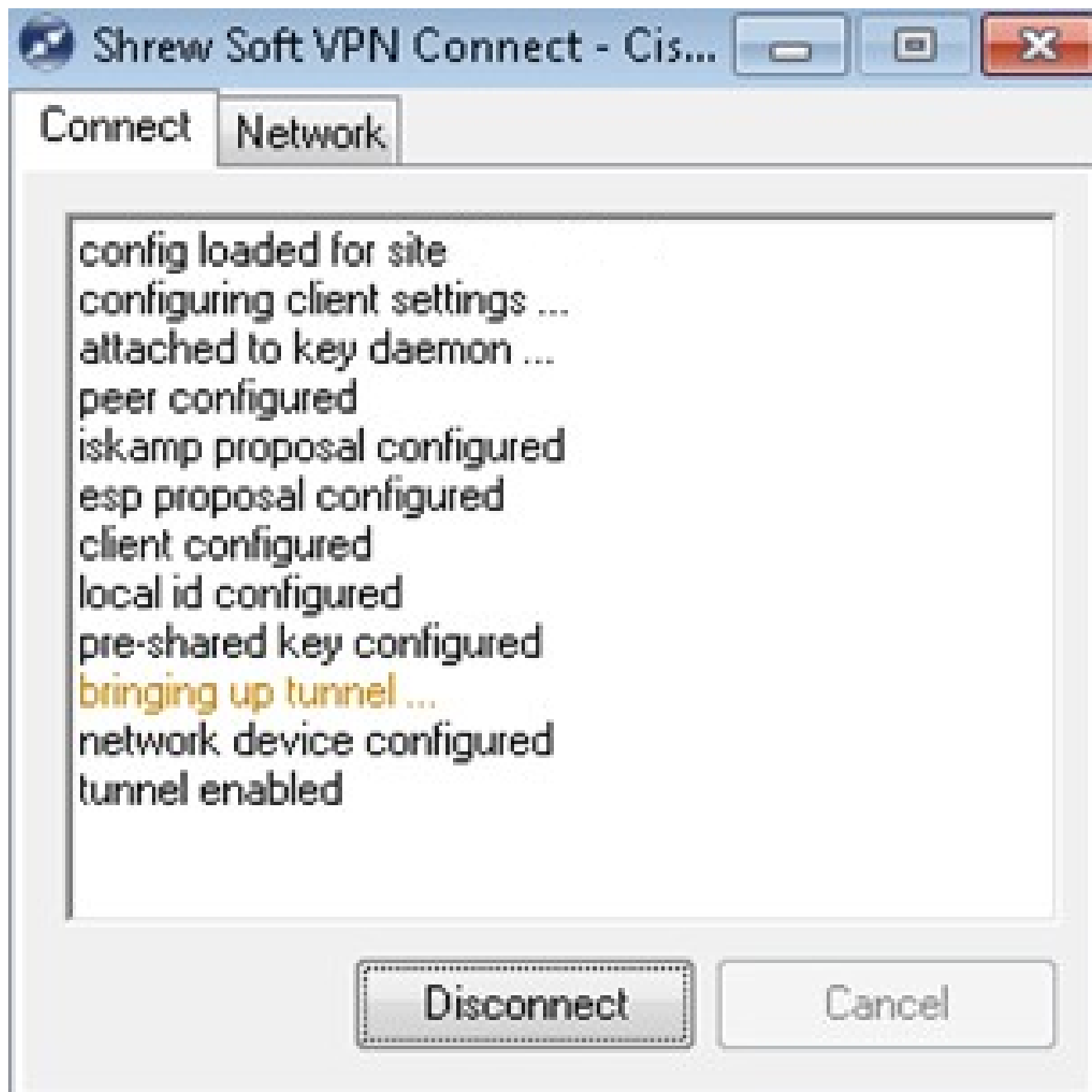
VPN Connectウィンドウが表示されます。



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。