

通过Windows在RV042、RV042G和RV082 VPN路由器上配置Shrew VPN客户端

目标

虚拟专用网络(VPN)是远程用户通过Internet以虚拟方式连接到专用网络的方法。客户端到网关VPN使用VPN客户端软件将用户的台式机或笔记本电脑连接到远程网络。客户端到网关VPN连接对于想要远程安全地连接到办公室网络的远程员工非常有用。Shrew VPN Client是在远程主机设备上配置的软件，可提供简单和安全的VPN连接。

本文档的目的是向您展示如何为连接到RV042、RV042G或RV082 VPN路由器的计算机配置Shrew VPN Client。

注意：本文档假定您已经在Windows计算机上下载了Shrew VPN客户端。否则，在开始配置精简VPN之前，需要配置客户端到网关VPN连接。有关如何配置客户端到网关VPN的详细信息，请参阅[为RV042、RV042G和RV082 VPN路由器上的VPN客户端设置远程访问隧道（客户端到网关）](#)。

适用设备

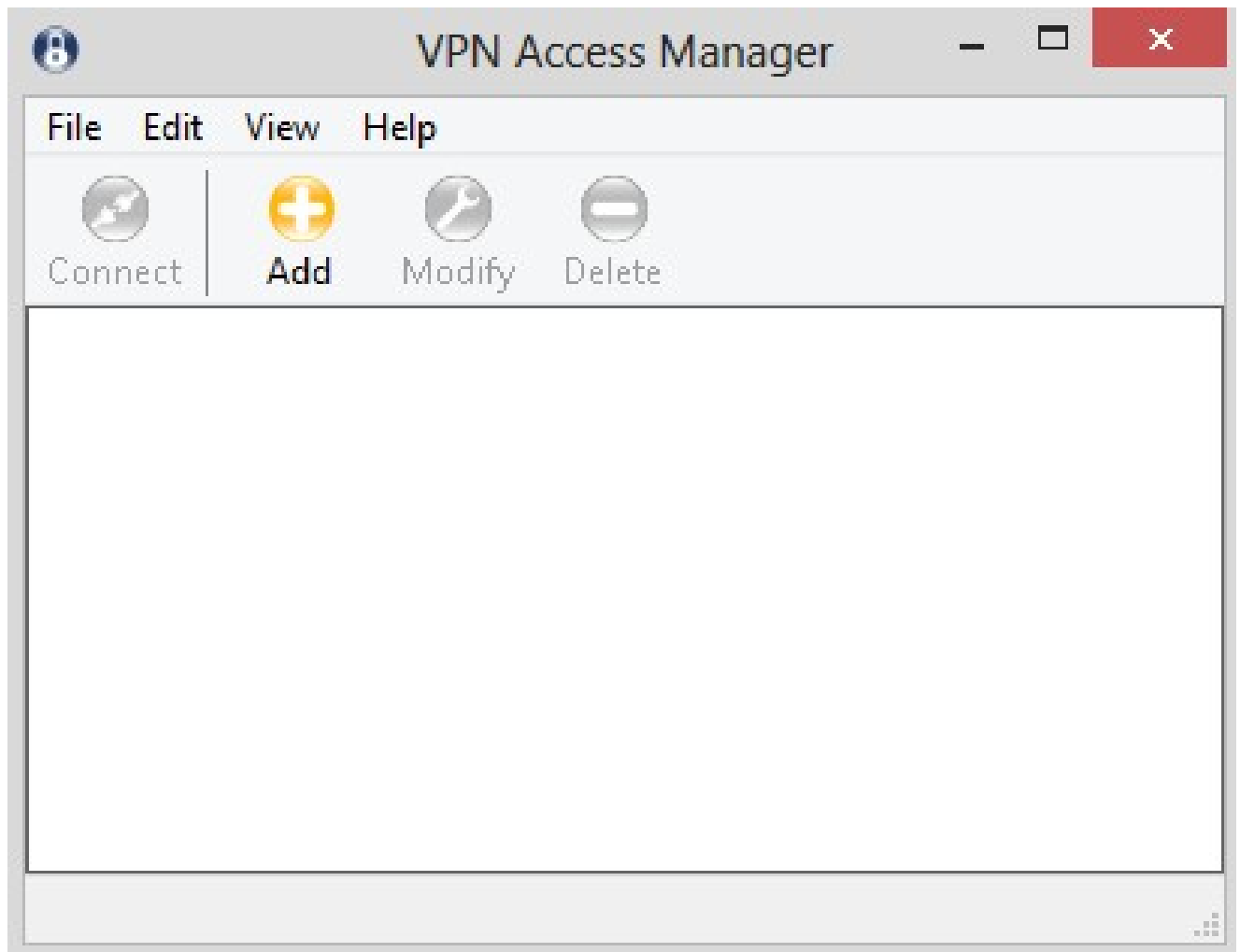
- RV042
- RV042G
- RV082

软件版本

- v4.2.2.08

在Windows上配置共享VPN客户端连接

步骤1:单击计算机上的Shrew VPN Client程序并打开它。Shrew Soft VPN Access Manager窗口打开：



第二步：单击 Add。出现VPN Site Configuration窗口：

VPN Site Configuration X

GeneralClientName ResolutionAuthenticatic◀▶

Remote Host

Host Name or IP Address	Port
	500
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	. . .

SaveCancel

一般配置

步骤1:点击常规选项卡。

VPN Site Configuration ✕

GeneralClientName ResolutionAuthenticatic◀▶

Remote Host

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

Auto Configuration ▼

Local Host

Adapter Mode

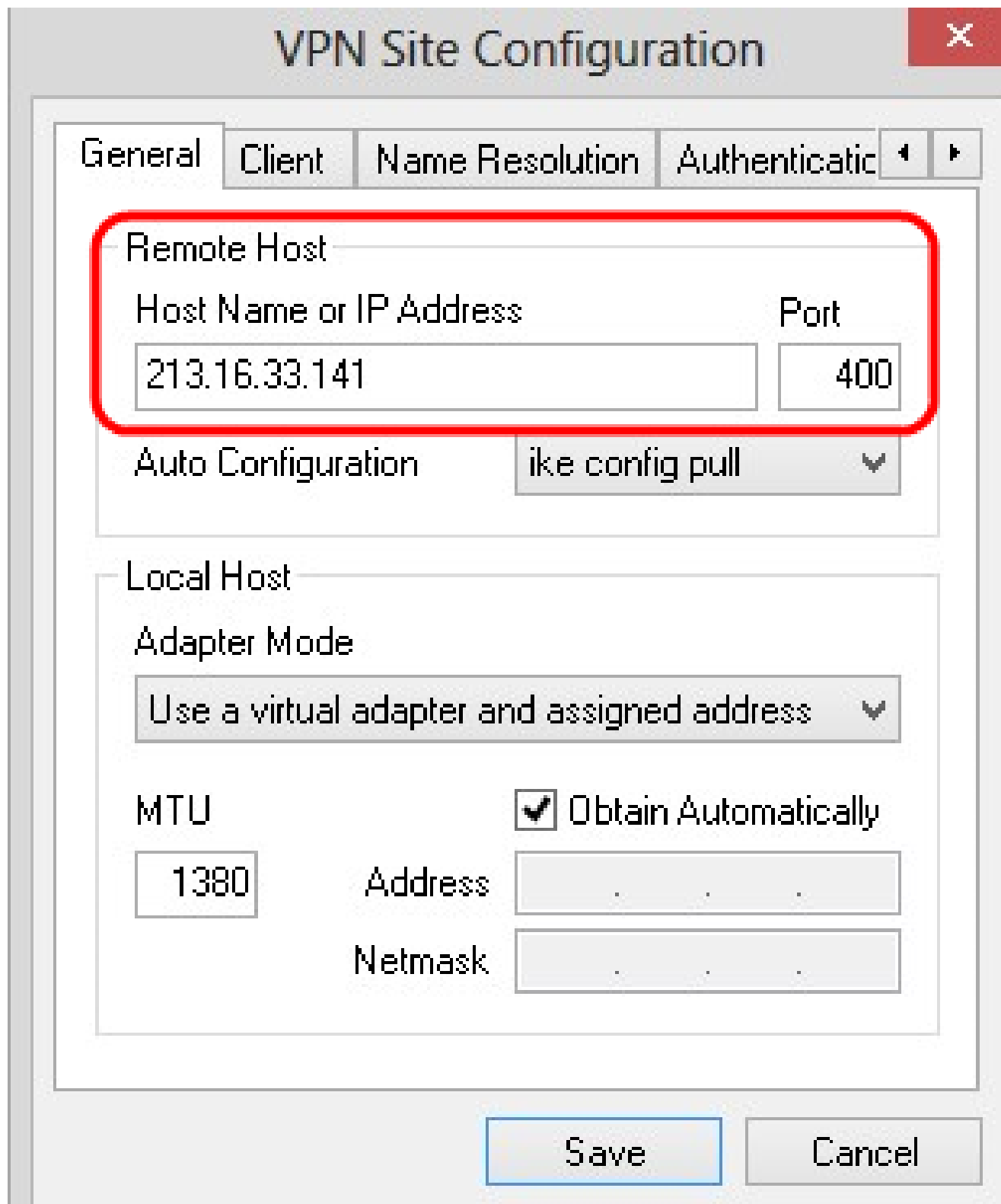
▼

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

注意：General部分用于配置远程和本地主机IP地址。这些参数用于定义客户端到网关连接的网络参数。

第二步：在Host Name or IP Address字段中，输入远程主机IP地址，即已配置WAN的IP地址。

第三步：在Port字段中，输入要用于连接的端口号。图中所示示例中使用的端口号为400。



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, and the 'Remote Host' section is highlighted with a red rounded rectangle. This section contains two input fields: 'Host Name or IP Address' with the value '213.16.33.141' and 'Port' with the value '400'. Below these is an 'Auto Configuration' dropdown menu set to 'ike config pull'. The 'Local Host' section below it includes an 'Adapter Mode' dropdown set to 'Use a virtual adapter and assigned address', an 'MTU' input field with '1380', and a checked checkbox for 'Obtain Automatically'. There are also empty input fields for 'Address' and 'Netmask'. At the bottom of the dialog are 'Save' and 'Cancel' buttons.

第四步：从Auto Configuration下拉列表中，选择所需的配置。

·禁用 — 禁用选项禁用任何自动客户端配置。

- IKE Config Pull — 允许客户端从计算机设置请求。在计算机支持Pull方法的情况下，请求返回客户端支持的设置列表。
- IKE Config Push — 使计算机有机会在整个配置过程中向客户端提供设置。在计算机支持Push方法的情况下，请求返回客户端支持的设置列表。
- DHCP Over IPsec — 使客户端有机会通过DHCP over IPsec从计算机请求设置。

VPN Site Configuration

General Client Name Resolution Authenticatic

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

1380

Obtain Automatically

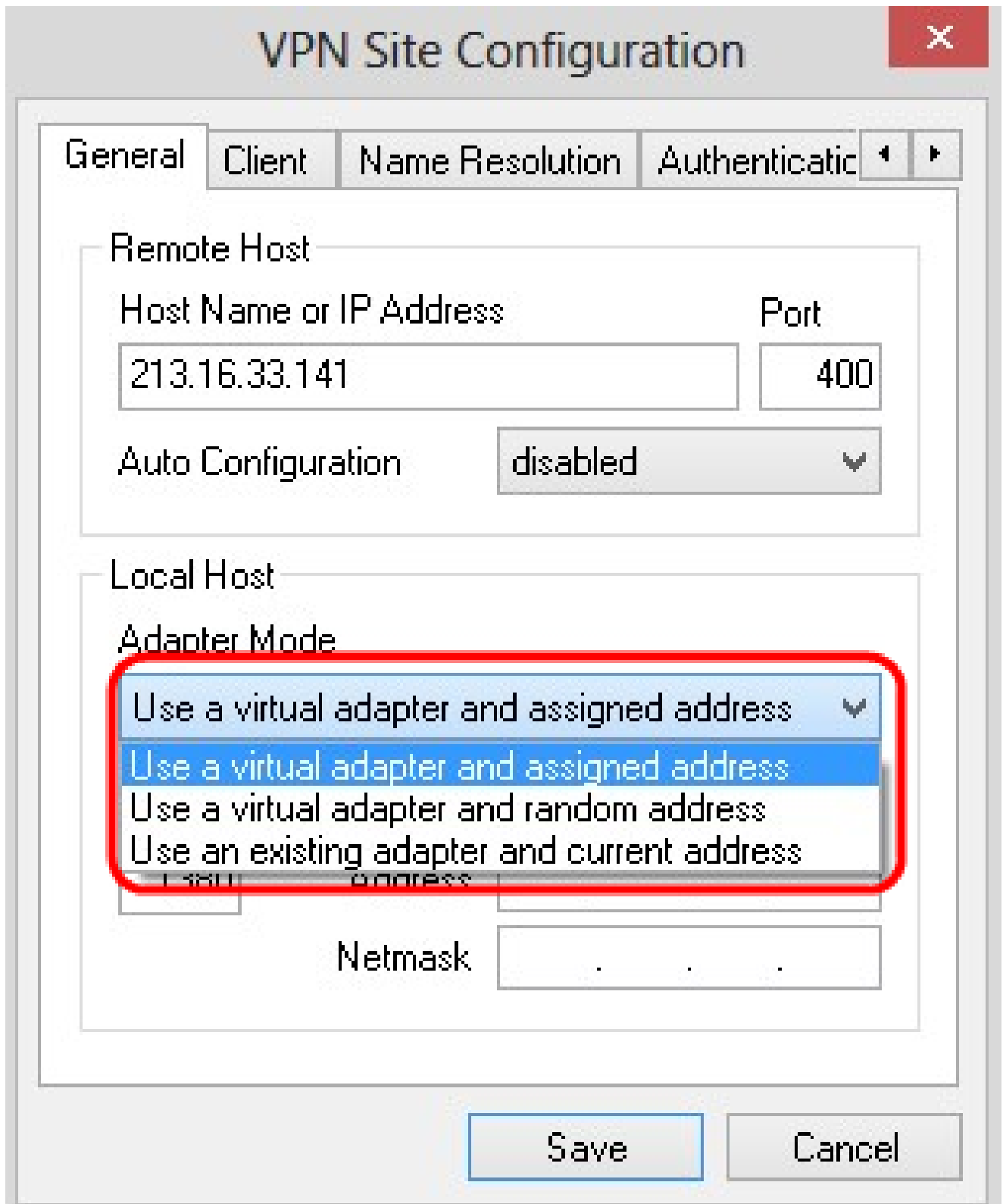
Address

Netmask

Save Cancel

第五步：从Adapter Mode下拉列表中，根据Auto Configuration为本地主机选择所需的适配器模式。

- 使用虚拟适配器和分配的地址 — 允许客户端使用具有指定地址的虚拟适配器。
- 使用虚拟适配器和随机地址 — 允许客户端使用具有随机地址的虚拟适配器。
- 使用现有适配器和当前地址 — 使用现有适配器及其地址。不需要输入其他信息。



第六步：如果在步骤5的适配器模式下拉列表中选择使用虚拟适配器和分配的地址，请在MTU字段中输入最大传输单位(MTU)。最大传输单元有助于解决IP分段问题。默认值为1380。

步骤7. (可选) 要通过DHCP服务器自动获取地址和子网掩码，请选中Obtain Automatically复选框。此选项不适用于所有配置。

步骤 8如果在Address字段中输入远程客户端的IP地址(如果从Adapter Mode下拉列表中选择Use a Virtual Adapter and Assigned Address)。

步骤 9如果在Netmask字段中选择了Use a Virtual Adapter and Assigned Address，则在Adapter Mode下拉列表中，在Netmask字段中输入远程客户端IP地址的子网掩码。

VPN Site Configuration

General Client Name Resolution Authenticatic

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 1480 Obtain Automatically

Address . . .

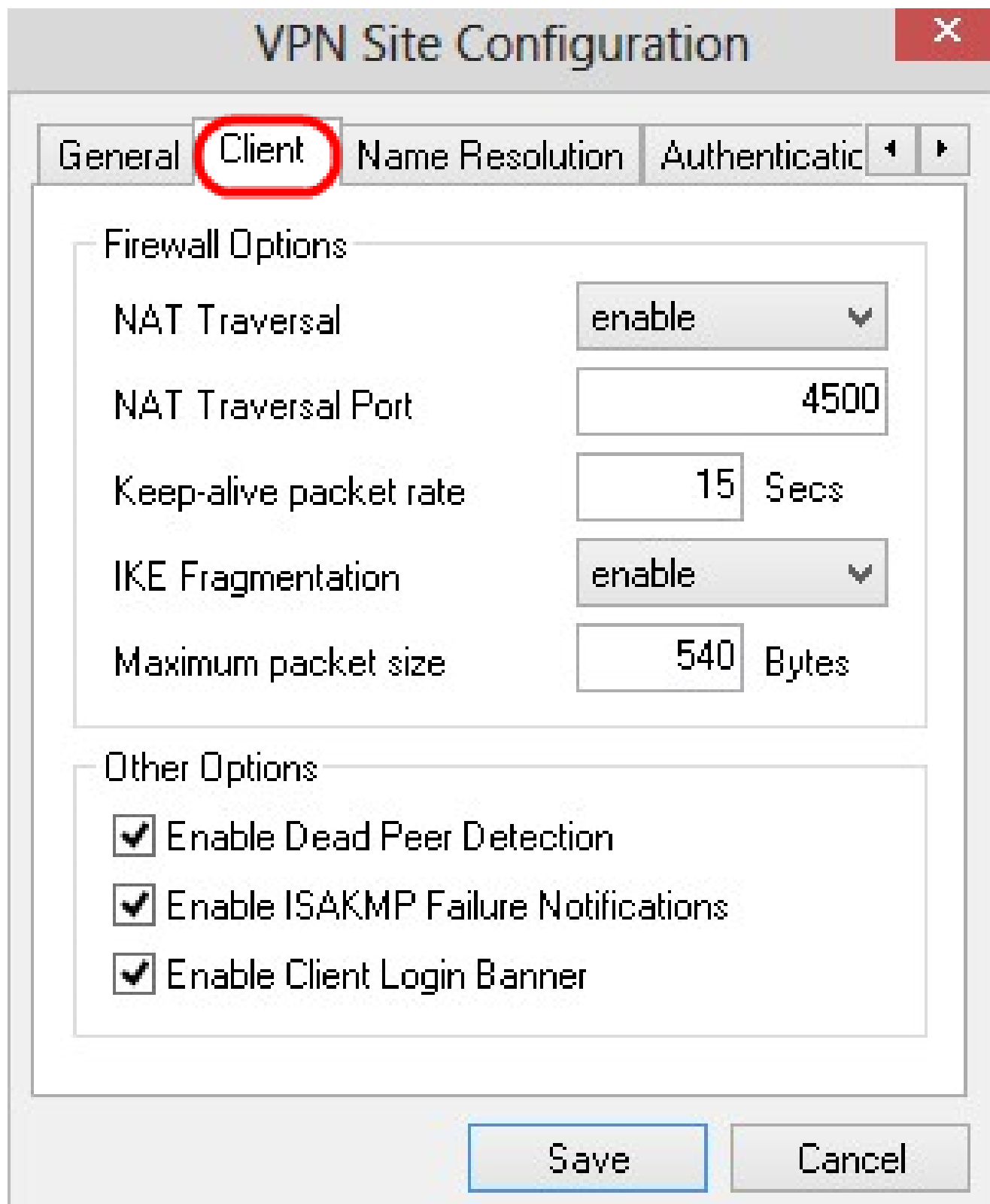
Netmask . . .

Save Cancel

步骤 10 点击 Save (保存) ，以保存设置。

客户端配置

步骤1:单击Client选项卡。



The image shows a screenshot of the "VPN Site Configuration" dialog box. The "Client" tab is selected and highlighted with a red circle. The dialog box contains two sections: "Firewall Options" and "Other Options".

Firewall Options:

NAT Traversal	enable
NAT Traversal Port	4500
Keep-alive packet rate	15 Secs
IKE Fragmentation	enable
Maximum packet size	540 Bytes

Other Options:

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

At the bottom of the dialog box, there are two buttons: "Save" and "Cancel".

注意：在Client部分，可以配置防火墙选项、失效对等体检测和ISAKMP（Internet安全关联和密钥管理协议）故障通知。这些设置定义了手动配置的配置选项和自动获取的配置选项。

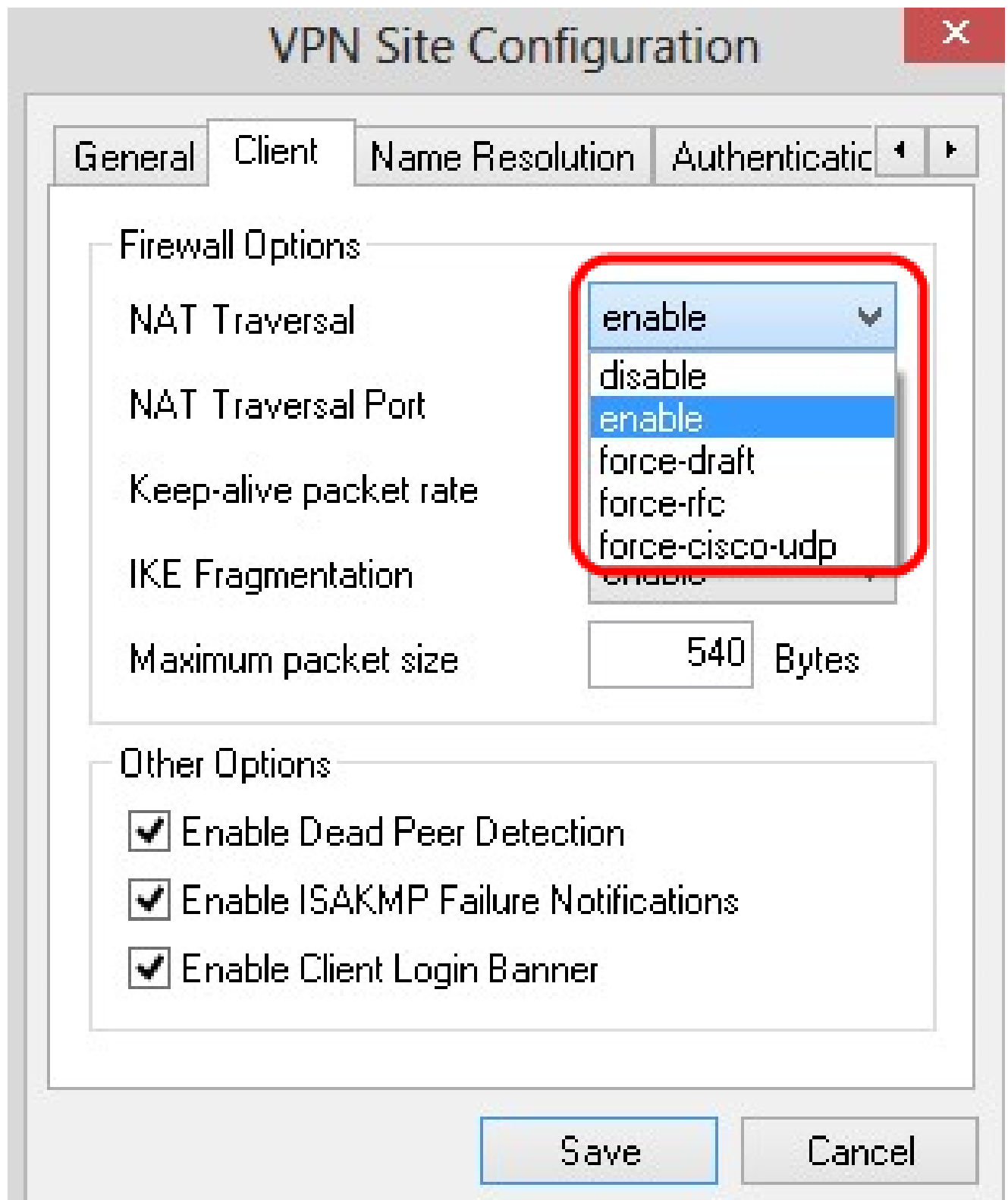
第二步：从NAT Traversal下拉列表中选择适当的NAT（网络地址转换）遍历选项。

- 禁用 — NAT协议已禁用。

- 启用 — 仅当网关通过协商指示支持时才使用IKE分段。

- Force Draft - NAT协议的草稿版本。如果网关通过协商或检测NAT来表示支持，则使用此命令。

- 强制RFC - NAT协议的RFC版本。如果网关通过协商或检测NAT来表示支持，则使用此命令。



第三步：在NAT Traversal Port字段中输入NAT的UDP端口。默认值为 4500。

第四步：在Keep-alive packet rate字段中，输入发送保持连接数据包的速率值。该值以秒为单位计算。默认值为 30 秒。

VPN Site Configuration ✕

GeneralClientName ResolutionAuthenticatic◀▶

Firewall Options

NAT Traversal	force-draft ▼
NAT Traversal Port	4400
Keep-alive packet rate	17 Secs
IKE Fragmentation	enable ▼
Maximum packet size	540 Bytes

Other Options

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

SaveCancel

第五步：在IKE Fragmentation下拉列表中，选择适当的选项。

·禁用 — 不使用IKE分段。

·启用 — 仅当网关通过协商指示支持时才使用IKE分段。

·强制 — 无论指示或检测如何，都使用IKE分段。

The image shows a 'VPN Site Configuration' dialog box with a red close button in the top right corner. The 'Client' tab is selected. Under the 'Firewall Options' section, the 'NAT Traversal' dropdown is set to 'force-draft', 'NAT Traversal Port' is 4400, and 'Keep-alive packet rate' is 17 Secs. The 'IKE Fragmentation' dropdown is open, showing options: 'enable' (selected), 'disable', 'enable', and 'force'. The 'Maximum packet size' field is empty. Under the 'Other Options' section, three checkboxes are checked: 'Enable Dead Peer Detection', 'Enable ISAKMP Failure Notifications', and 'Enable Client Login Banner'. At the bottom, there are 'Save' and 'Cancel' buttons.

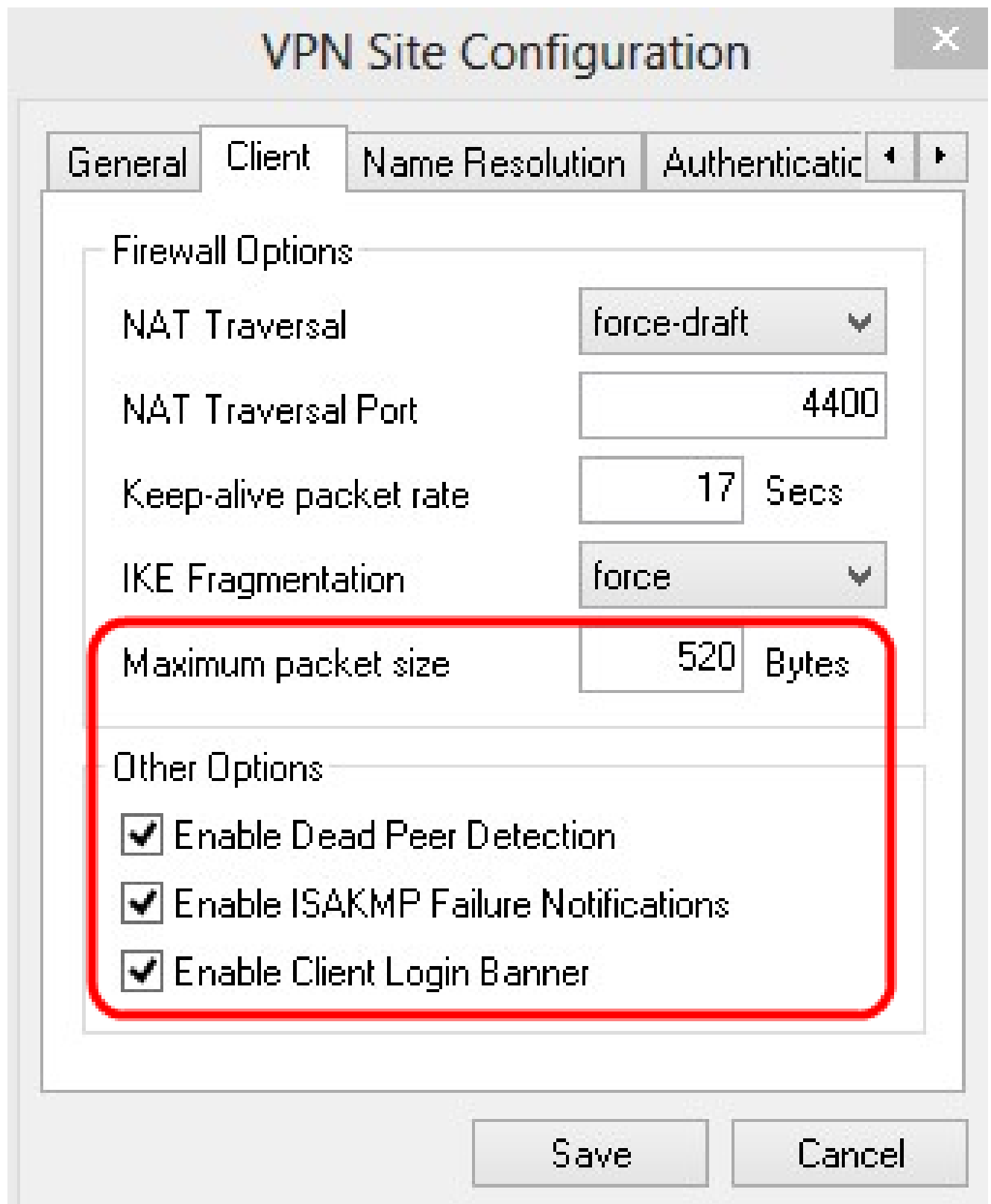
第六步：在Maximum packet size字段中输入最大数据包大小（以字节为单位）。如果数据包大小大于最大数据包大小，则执行IKE分段。默认值为 540 字节。

步骤7. (可选) 要允许计算机和客户端检测何时另一个无法响应，请选中Enable Dead Peer

Detection复选框。

步骤8. (可选) 要通过VPN客户端发送故障通知，请选中Enable ISAKMP Failure Notifications复选框。

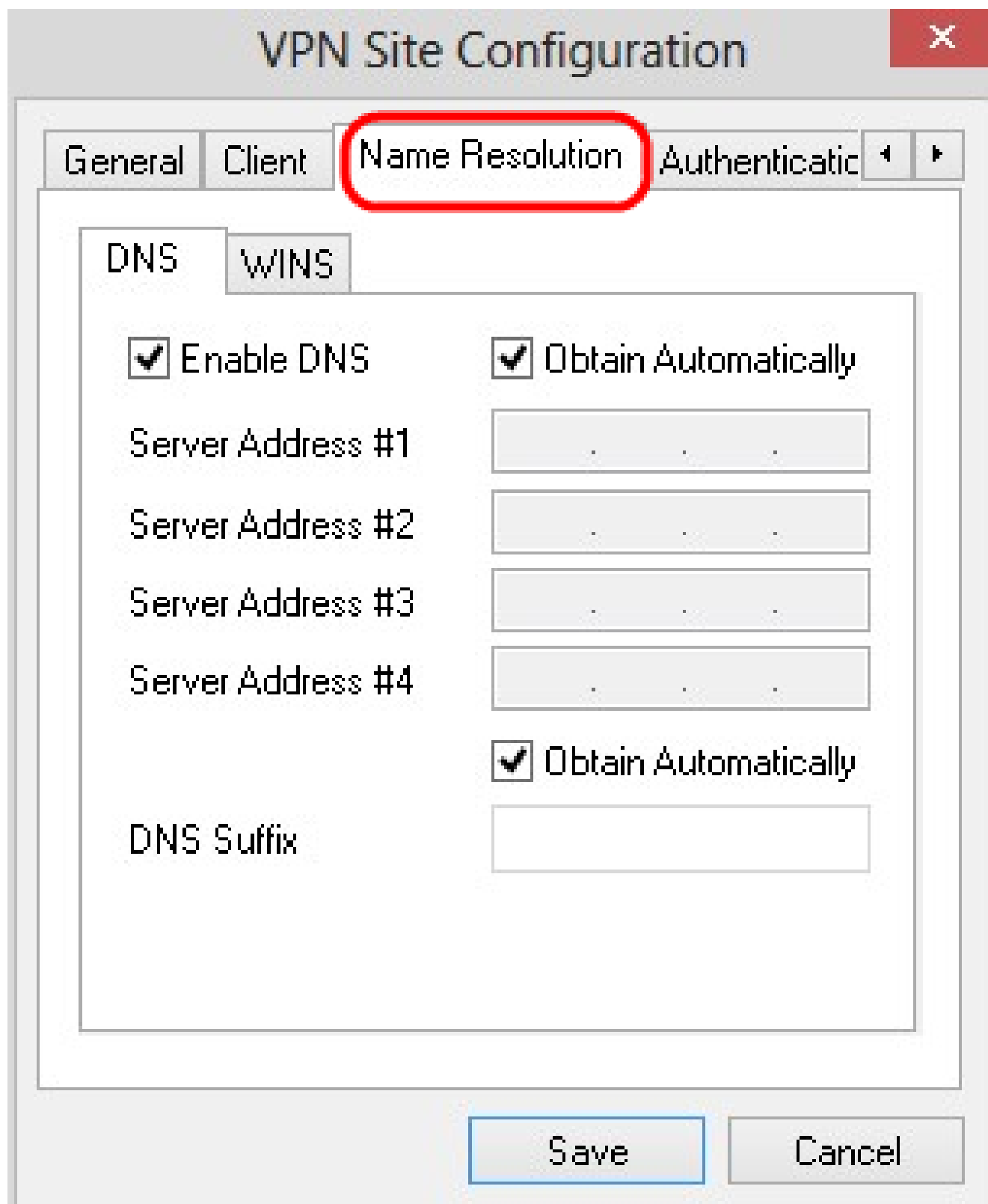
步骤9. (可选) 要在与网关建立连接时由客户端显示登录提示，请选中Enable Client Login复选框。



步骤 10 点击 Save (保存) ， 以保存设置。

名称解析配置

步骤 1: 点击 Name Resolution 选项卡。



注意：名称解析部分用于配置DNS（域名系统）和WIN（Windows Internet名称服务）设置。

第二步：点击DNS选项卡。

VPN Site Configuration X

GeneralClientName ResolutionAuthenticatic◀▶

DNSWINS

Enable DNS

Obtain Automatically

Server Address #1

Server Address #2

Server Address #3

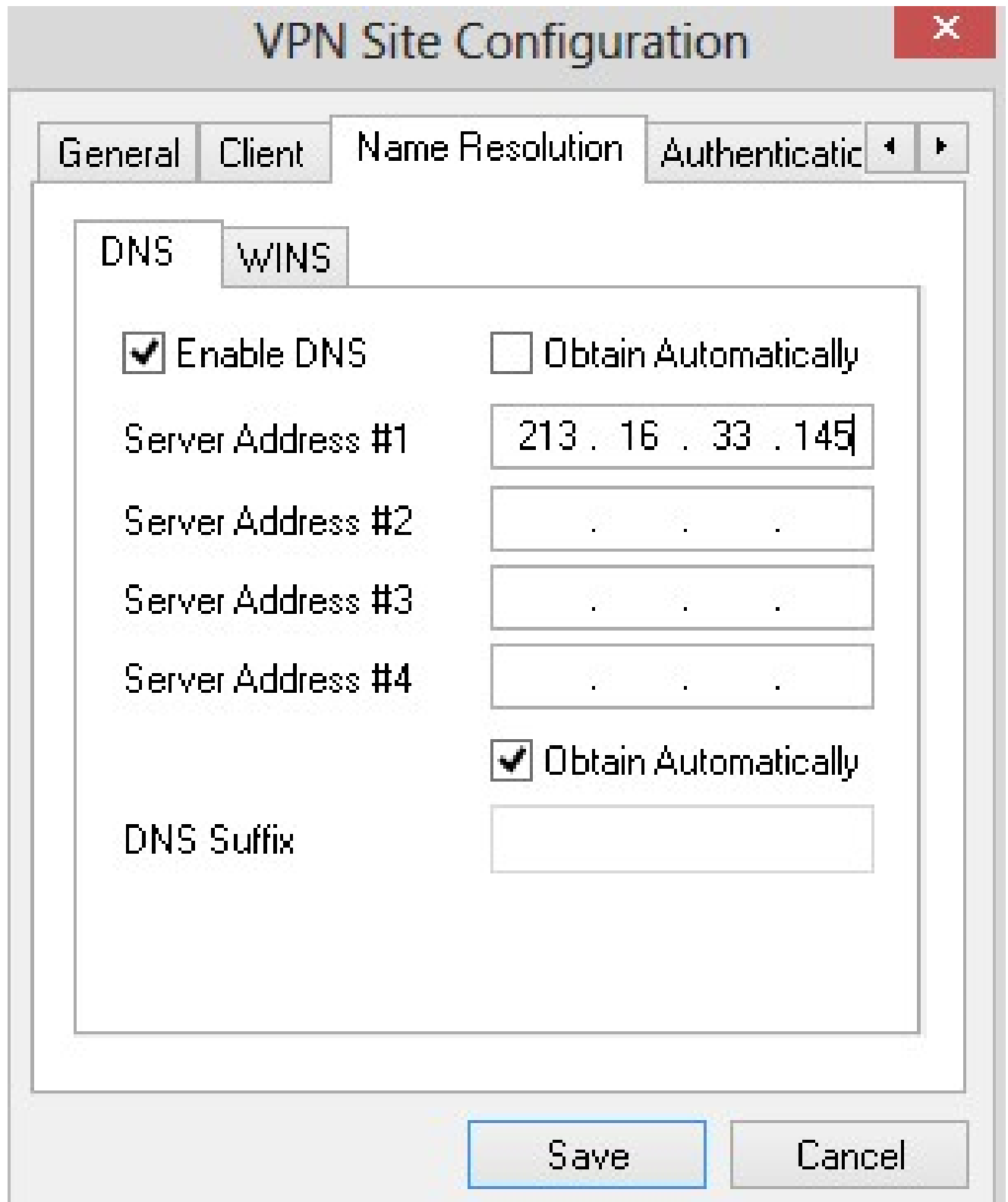
Server Address #4

Obtain Automatically

DNS Suffix

SaveCancel

Server Address字段中输入这些服务器的地址。



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. The 'Obtain Automatically' checkbox is unchecked. The 'Server Address #1' field contains '213 . 16 . 33 . 145'. The 'Server Address #2', 'Server Address #3', and 'Server Address #4' fields are empty. The 'Obtain Automatically' checkbox is checked. The 'DNS Suffix' field is empty. At the bottom, there 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	<input checked="" type="checkbox"/>
DNS Suffix	

步骤6. (可选) 要自动获取DNS服务器的后缀，请选中Obtain Automatically复选框。如果选择此选项，请跳至步骤8。

步骤 7.在DNS后缀字段中输入DNS服务器后缀。

步骤 8 点击 Save (保存) ，以保存设置。

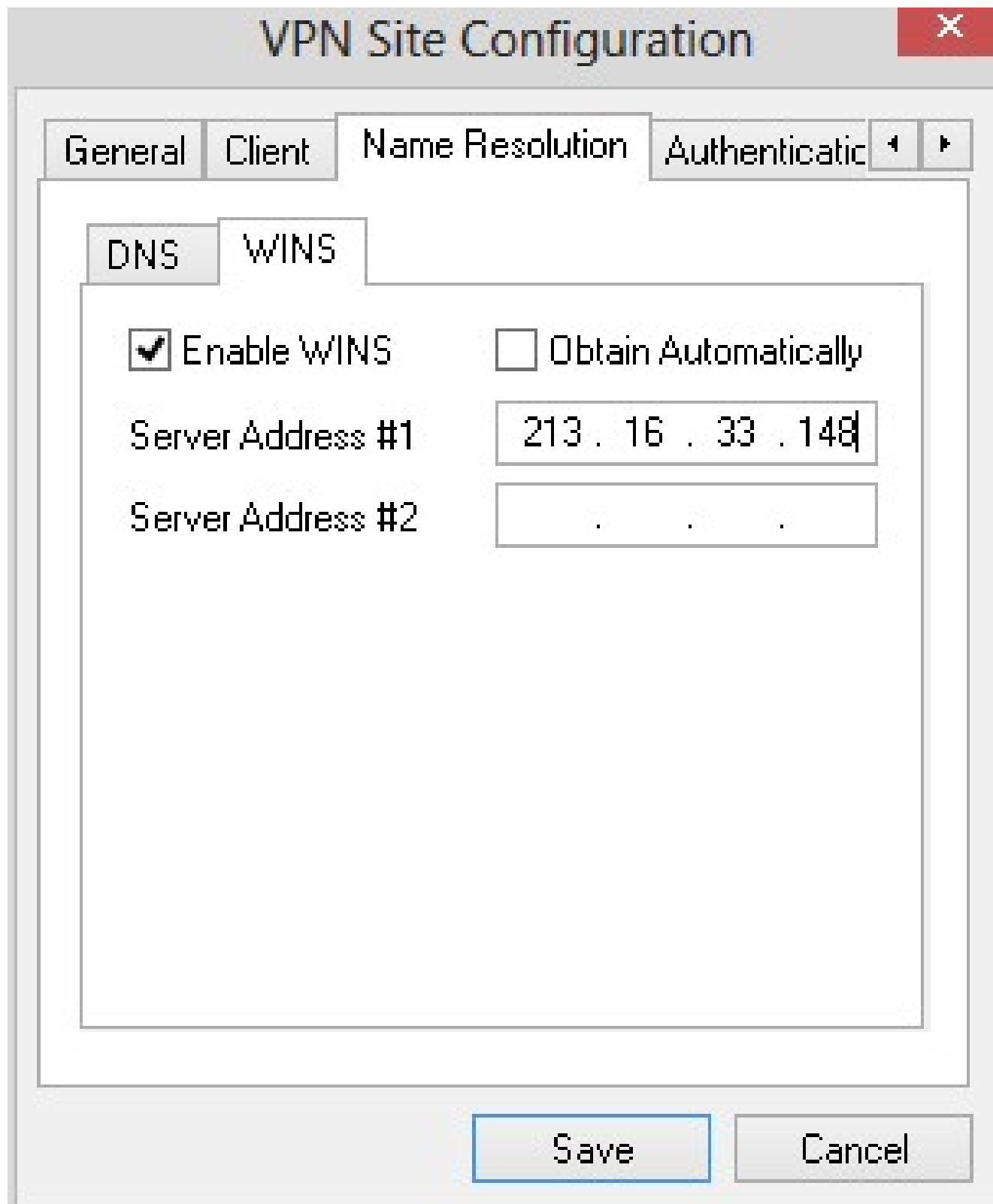
步骤 9 单击 WINS 选项卡。



步骤 10 选中 Enable WINS 以启用 Windows Internet Name Server (WINS)。

步骤11. (可选) 要自动获取DNS服务器地址，请选中Obtain Automatically 复选框。如果选择此选项，请跳至步骤13。

步骤 12在Server Address #1字段中输入WINS服务器的地址。如果有其他DNS服务器，在其余的Server Address字段中输入这些服务器的地址。



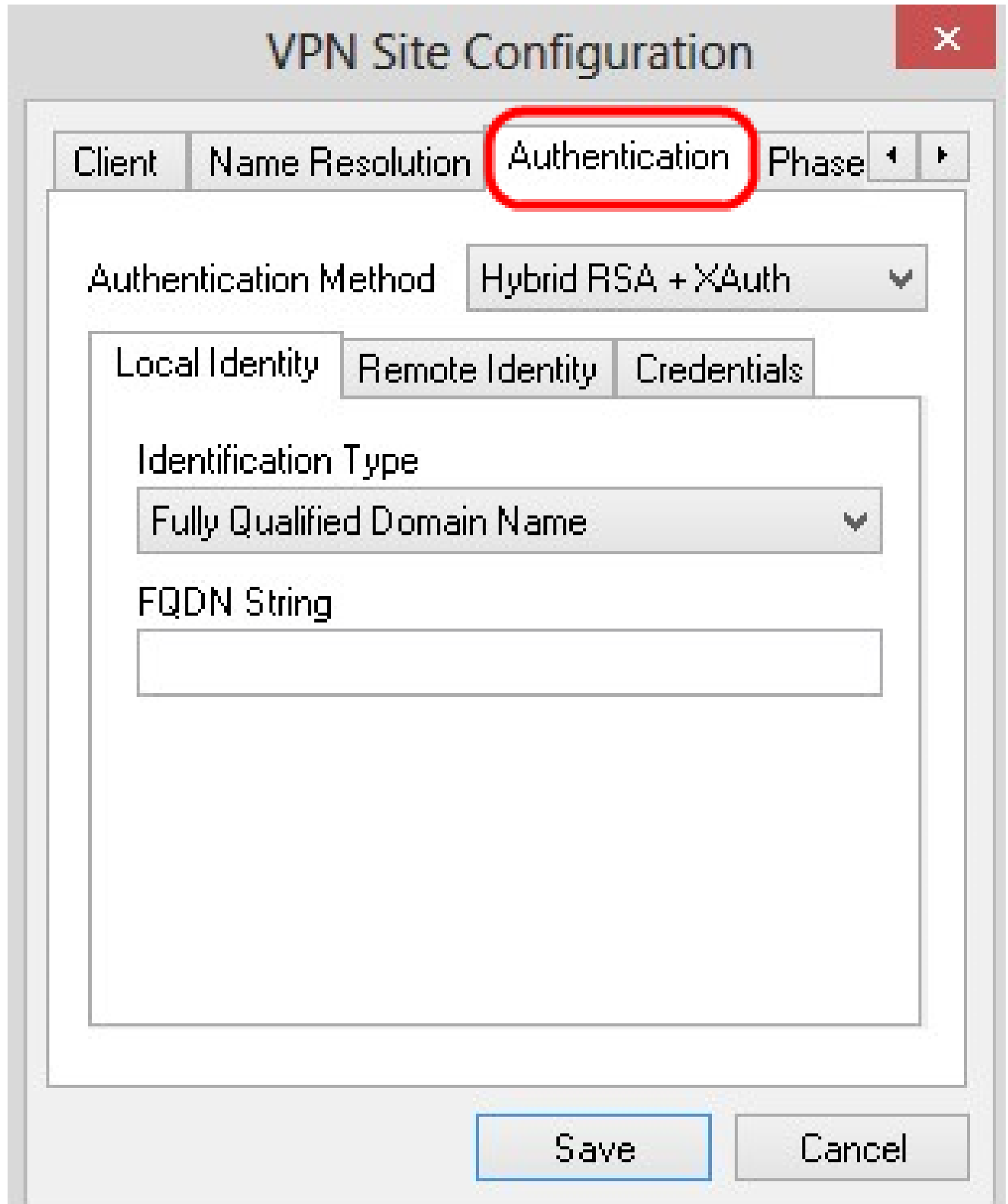
The image shows a screenshot of the "VPN Site Configuration" dialog box. The "Name Resolution" tab is selected, and the "WINS" sub-tab is active. The "Enable WINS" checkbox is checked, and the "Obtain Automatically" checkbox is unchecked. The "Server Address #1" field contains the IP address "213 . 16 . 33 . 148". The "Server Address #2" field contains three dots ". . .". At the bottom of the dialog, there are "Save" and "Cancel" buttons.

Field	Value
Enable WINS	<input checked="" type="checkbox"/>
Obtain Automatically	<input type="checkbox"/>
Server Address #1	213 . 16 . 33 . 148
Server Address #2	. . .

步骤 13 点击 Save (保存) ，以保存设置。

身份验证

步骤1:单击 Authentication 选项卡。



The image shows a screenshot of the "VPN Site Configuration" dialog box. The title bar at the top reads "VPN Site Configuration" and includes a red close button with a white "X" icon. Below the title bar is a tabbed interface with four tabs: "Client", "Name Resolution", "Authentication", and "Phase". The "Authentication" tab is currently selected and is highlighted with a red rectangular border. Below the tabs, the "Authentication Method" is set to "Hybrid RSA + XAuth" in a dropdown menu. Underneath, there are three sub-tabs: "Local Identity", "Remote Identity", and "Credentials". The "Local Identity" sub-tab is active, showing an "Identification Type" dropdown menu set to "Fully Qualified Domain Name" and an empty text input field labeled "FQDN String". At the bottom of the dialog box, there are two buttons: "Save" and "Cancel".

注意：在Authentication部分，您可以配置参数，使客户端在尝试建立ISAKMP SA时处理身份验证。

第二步：从Authentication Method下拉列表中选择适当的身份验证方法。

·混合RSA +扩展验证 — 不需要客户端凭证。客户端将对网关进行身份验证。凭证将采用PEM或PKCS12证书文件或密钥文件类型的形式。

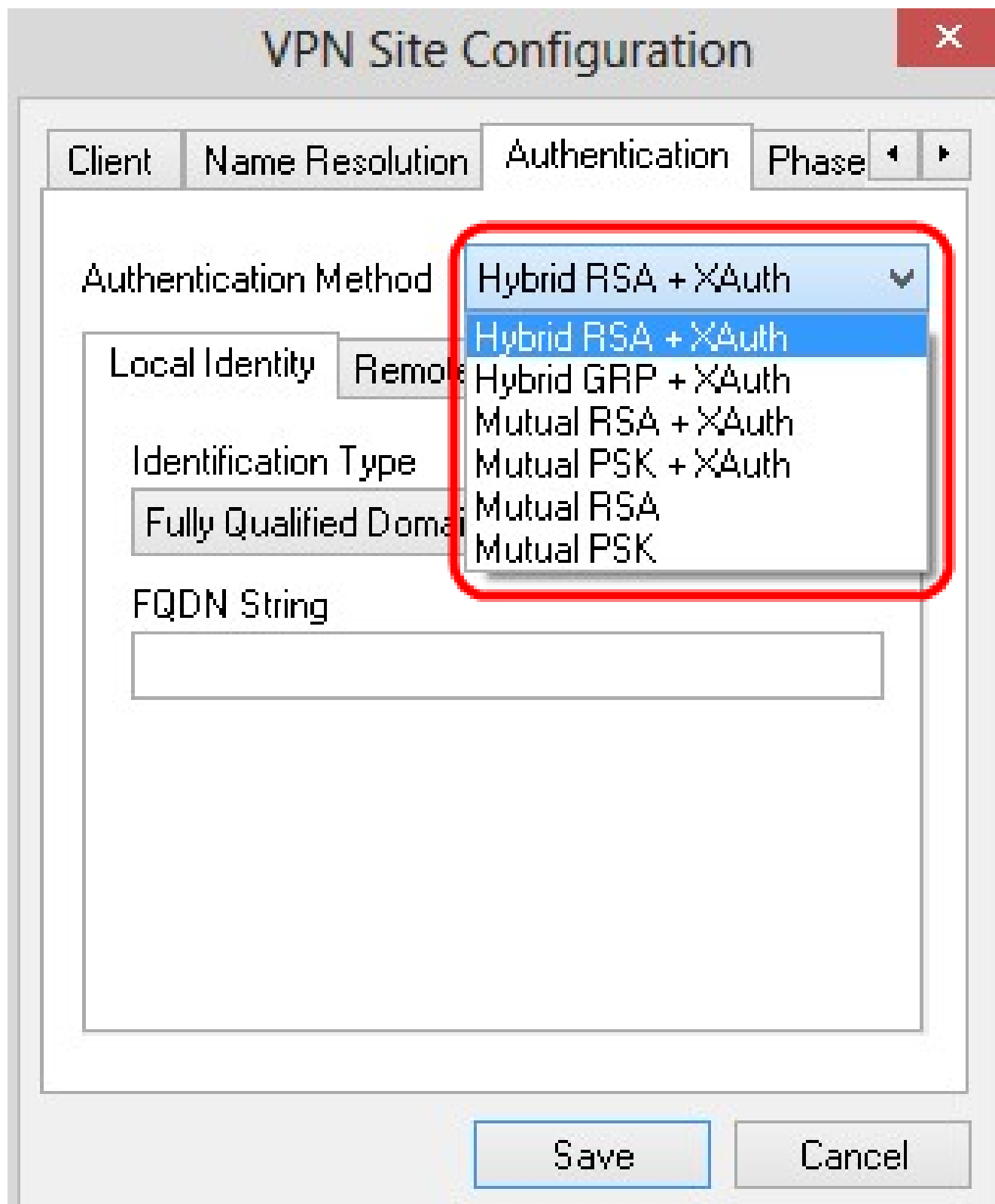
·混合GRP +扩展验证 — 不需要客户端凭证。客户端将对网关进行身份验证。凭证将采用PEM或PKCS12证书文件和共享密钥字符串的形式。

·双方RSA +扩展验证 — 客户端和网关都需要凭据进行身份验证。凭证将采用PEM或PKCS12证书文件或密钥类型的形式。

·双向PSK +扩展验证 — 客户端和网关都需要凭证进行身份验证。凭据将采用共享密钥字符串的形式。

·双向RSA — 客户端和网关都需要凭据进行身份验证。凭证将采用PEM或PKCS12证书文件或密钥类型的形式。

·双向PSK — 客户端和网关都需要凭证进行身份验证。凭据将采用共享密钥字符串的形式。



本地身份配置

步骤1:单击Local Identity选项卡。

VPN Site Configuration X

ClientName ResolutionAuthenticationPhase ◀ ▶

Authentication Method Hybrid RSA + XAuth ▼

Local Identity

Remote Identity

Credentials

Identification Type

Fully Qualified Domain Name ▼

FQDN String

Save

Cancel

注意：本地身份设置发送到网关进行验证的ID。在Local Identity部分中，配置标识类型和FQDN（完全限定域名）字符串以确定ID的发送方式。

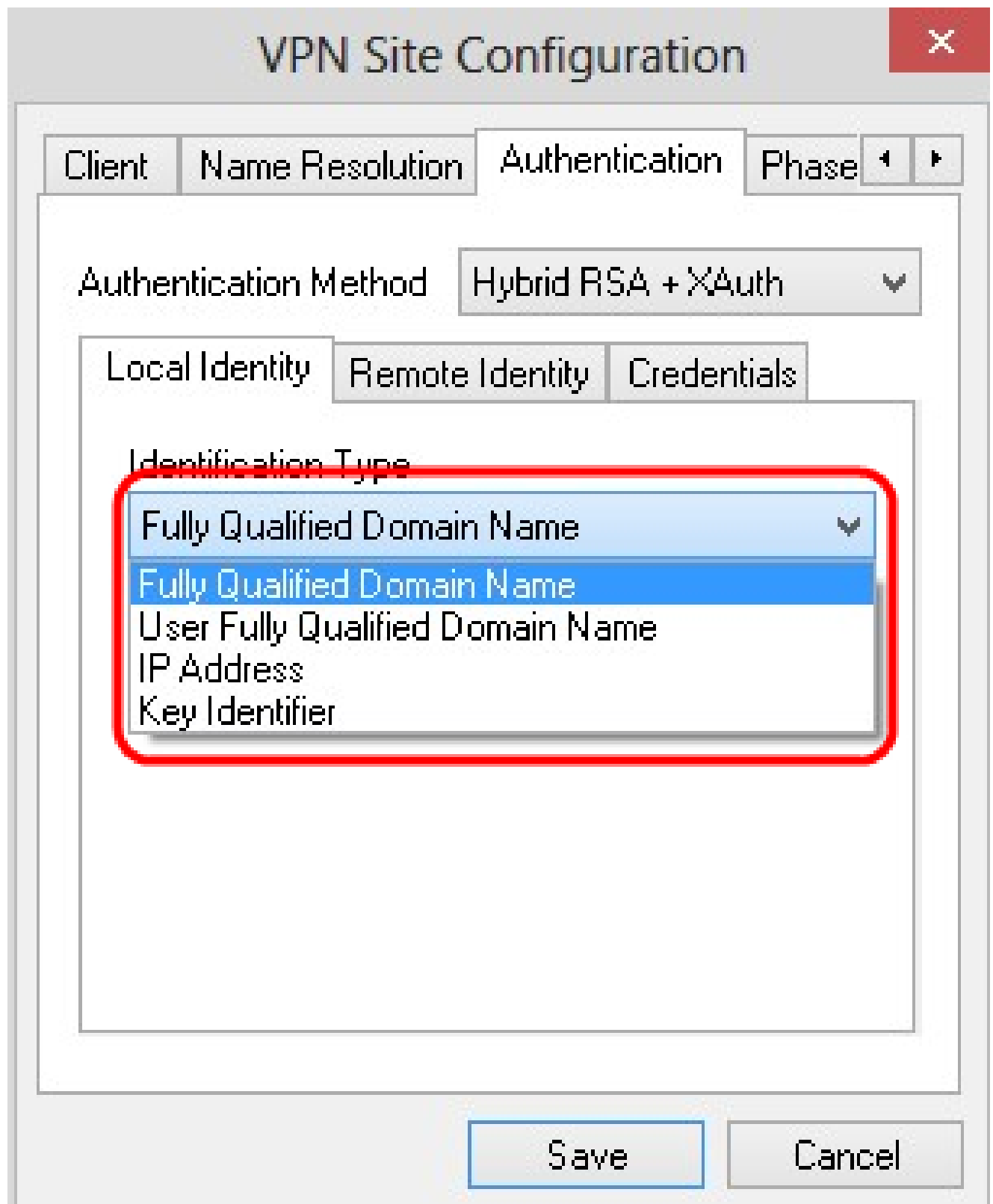
第二步：从Identification Type下拉列表中选择相应的标识选项。并非所有选项对所有身份验证模式都可用。

·完全限定域名 — 本地身份的客户端标识基于完全限定域名。如果选择此选项，请执行步骤3，然后跳至步骤7。

·用户完全限定域名 — 本地身份的客户端标识基于用户完全限定域名。如果选择此选项，请执行步骤4，然后跳至步骤7。

·IP地址 — 本地身份的客户端标识基于IP地址。如果选中Use a discovered local host address，则会自动发现IP地址。如果选择此选项，请执行步骤5，然后跳至步骤7。

·密钥标识符 — 根据密钥标识符标识本地客户端的客户端标识符。如果选择此选项，请执行步骤6和步骤7。



第三步：在FQDN字符串字段中输入完全限定域名作为DNS字符串。

第四步：在UFQDN String字段中输入用户完全限定的域名作为DNS字符串。

第五步：在UFQDN字符串字段中输入IP地址。

第六步：在Key ID String中输入用于标识本地客户端的密钥标识符。

步骤 7. 点击 Save (保存) ，以保存设置。

远程身份配置

步骤1:单击Remote Identity选项卡。

VPN Site Configuration ✕

ClientName ResolutionAuthenticationPhase ◀ ▶

Authentication Method Hybrid RSA + XAuth

Local IdentityRemote IdentityCredentials

Identification Type

Any

SaveCancel

注意：远程身份会验证来自网关的ID。在远程身份部分中，标识类型配置为确定ID的验证方式。

第二步：从Identification Type下拉列表中选择相应的标识选项。

- Any — 远程客户端可以接受任何值或ID进行身份验证。

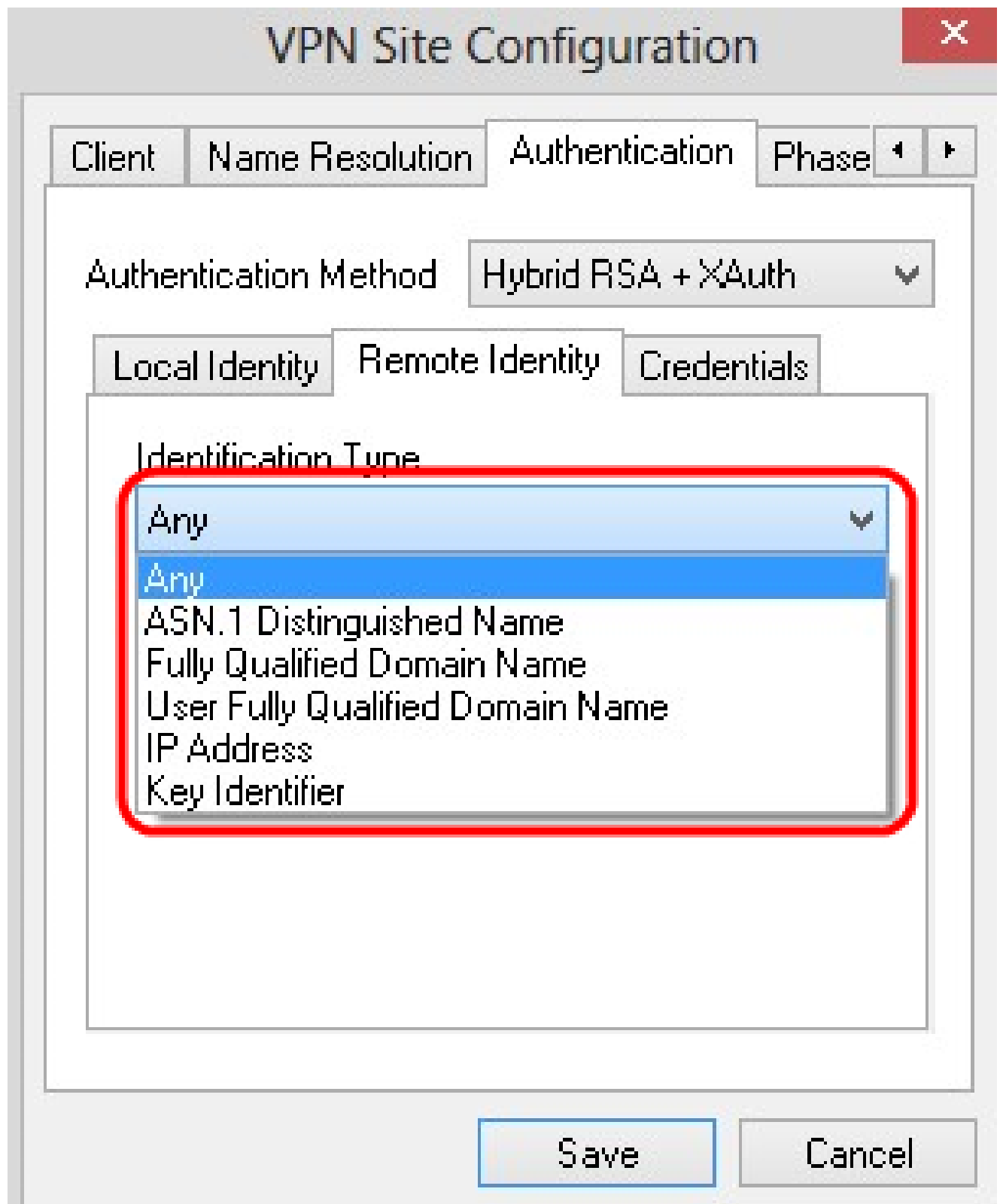
· ASN.1可分辨名称 — 从PEM或PKCS12证书文件自动识别远程客户端。只有在Authentication部分的第2步中选择RSA身份验证方法时，才能选择此选项。选中Use the subject in the received certificate but don't compare it with a specific value复选框以自动接收证书。如果选择此选项，请执行步骤3，然后跳至步骤8。

· 完全限定域名 — 远程身份的客户端标识基于完全限定域名。只有在Authentication部分的第2步中选择PSK身份验证方法时，才能选择此选项。如果选择此选项，请执行步骤4，然后跳至步骤8。

· 用户完全限定域名 — 远程身份的客户端标识基于用户完全限定域名。只有在Authentication部分的第2步中选择PSK身份验证方法时，才能选择此选项。如果选择此选项，请执行步骤5，然后跳至步骤8。

· IP地址 — 远程身份的客户端标识基于IP地址。如果选中Use a discovered local host address，则会自动发现IP地址。如果选择此选项，请执行步骤6，然后跳至步骤8。

· 密钥标识符 — 基于密钥标识符来标识远程客户端的客户端标识符。如果选择此选项，请执行步骤7和步骤8。



第三步：在ASN.1 DN String字段中输入ASN.1 DN字符串。

第四步：在FQDN字符串字段中输入完全限定域名作为DNS字符串。

第五步：在UFQDN字符串字段中输入用户完全限定域名作为DNS字符串。

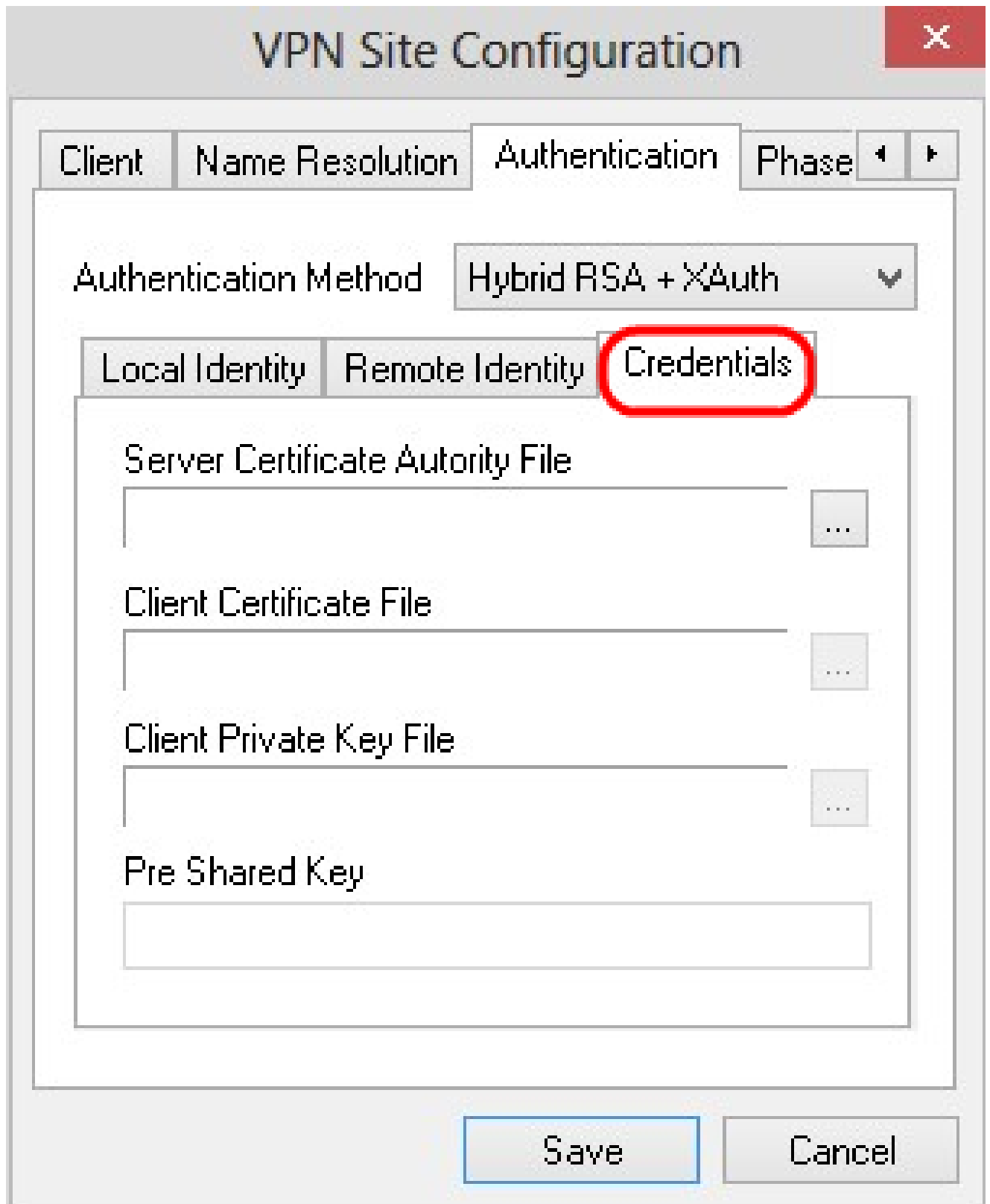
第六步：在UFQDN字符串字段中输入IP地址。

步骤 7.在Key ID String字段中输入用于标识本地客户端的密钥标识符。

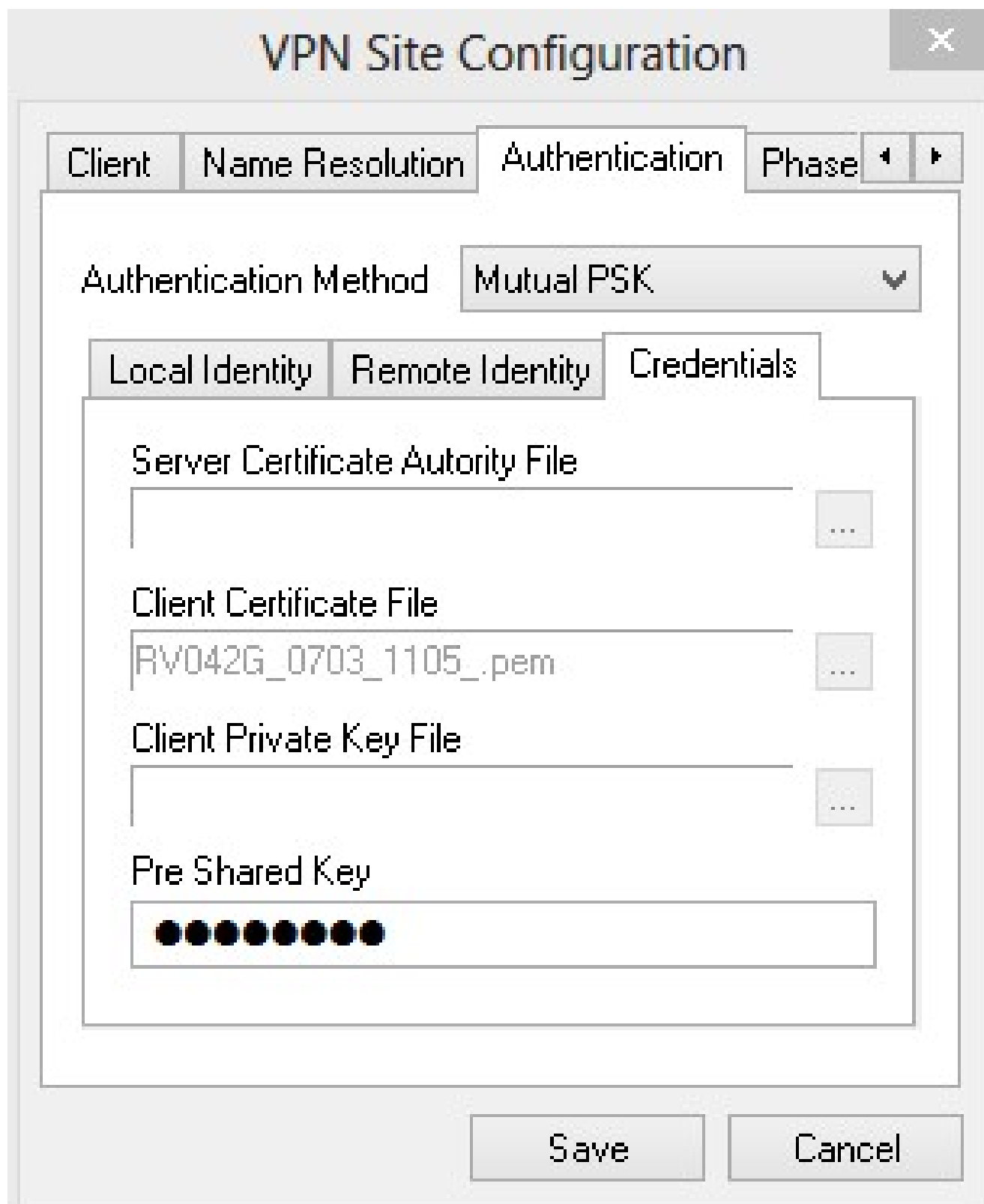
步骤 8点击 Save (保存) ，以保存设置。

凭证配置

步骤1:单击Credentials选项卡。



注意：在Credentials部分，配置预共享密钥。



第二步：要选择Server Certificate File，请点击Server Certificate Authority File字段旁边的...图标，然后选择您在PC上保存服务器证书文件的路径。

第三步：要选择Client Certificate File，请点击Client Certificate File字段旁边的...图标，然后选择您在PC上保存客户端证书文件的路径。

第四步：要选择Client Private Key File，请点击Client Private Key File字段旁边的...图标，然后选择在PC中保存客户端私钥文件的路径。

第五步：在PreShared Key字段中输入预共享密钥。此密钥应与您在配置隧道时使用的密钥相同。

第六步：点击 Save（保存），以保存设置。

第1阶段配置

步骤1:单击Phase 1选项卡。

VPN Site Configuration X

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

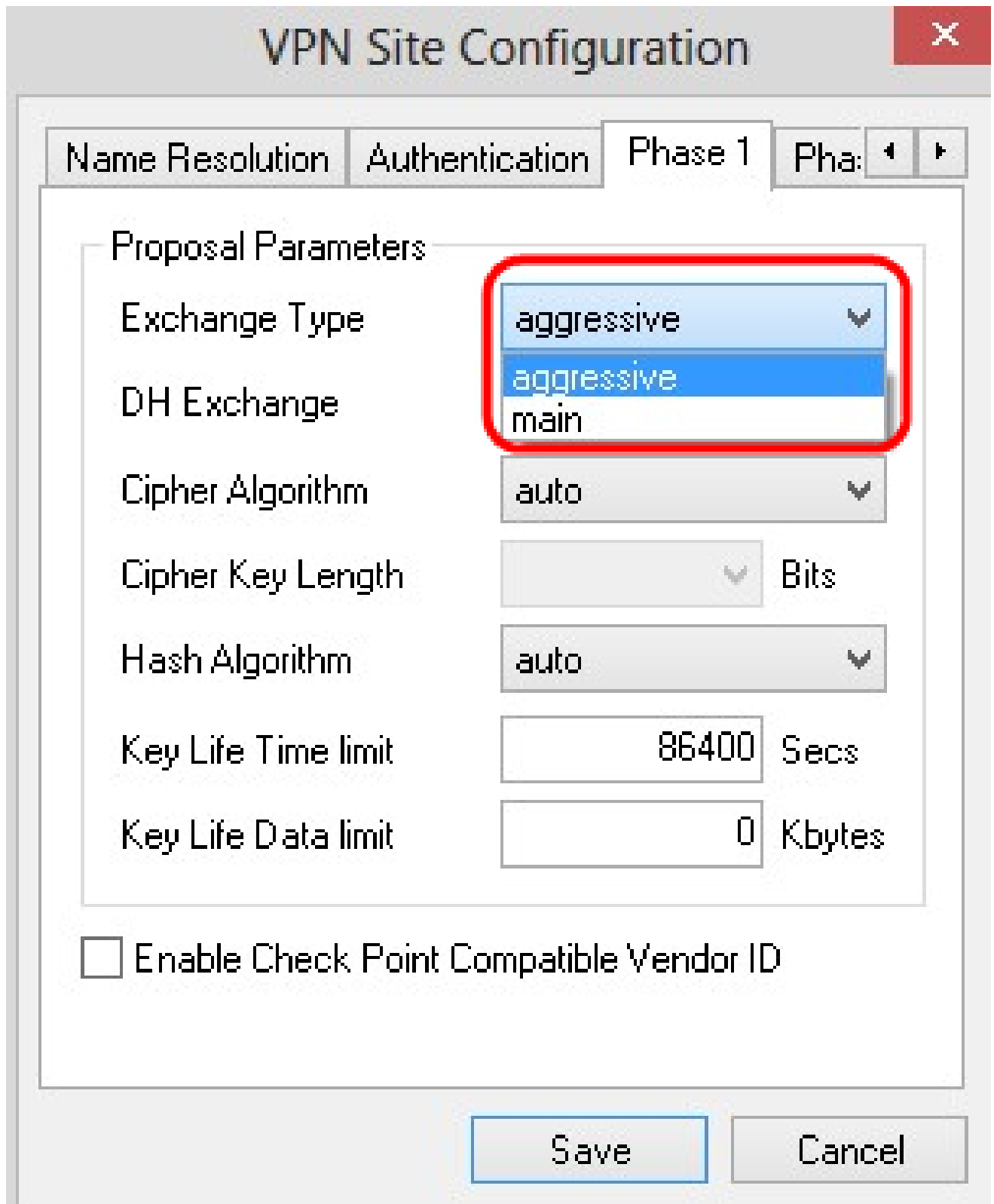
SaveCancel

注意：在Phase 1部分，您可以配置参数，以便可以建立带有客户端网关的ISAKMP SA。

第二步：从Exchange Type下拉列表中选择适当的密钥交换类型。

·主要 — 对等体的身份受到保护。

·攻击性 — 对等体的身份不安全。



The image shows a 'VPN Site Configuration' dialog box with a red close button in the top right corner. The 'Phase 1' tab is selected. Under 'Proposal Parameters', the 'Exchange Type' dropdown menu is open, showing 'aggressive' (highlighted) and 'main' options. Other settings include 'Cipher Algorithm' set to 'auto', 'Key Life Time limit' set to 86400 Secs, and 'Key Life Data limit' set to 0 Kbytes. There is an unchecked checkbox for 'Enable Check Point Compatible Vendor ID' and 'Save' and 'Cancel' buttons at the bottom.

Parameter	Value
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

第三步：在DH Exchange下拉列表中，选择在VPN连接配置期间选择的相应组。

第四步：在Cipher Algorithm下拉列表中，选择在VPN连接配置期间选择的适当选项。

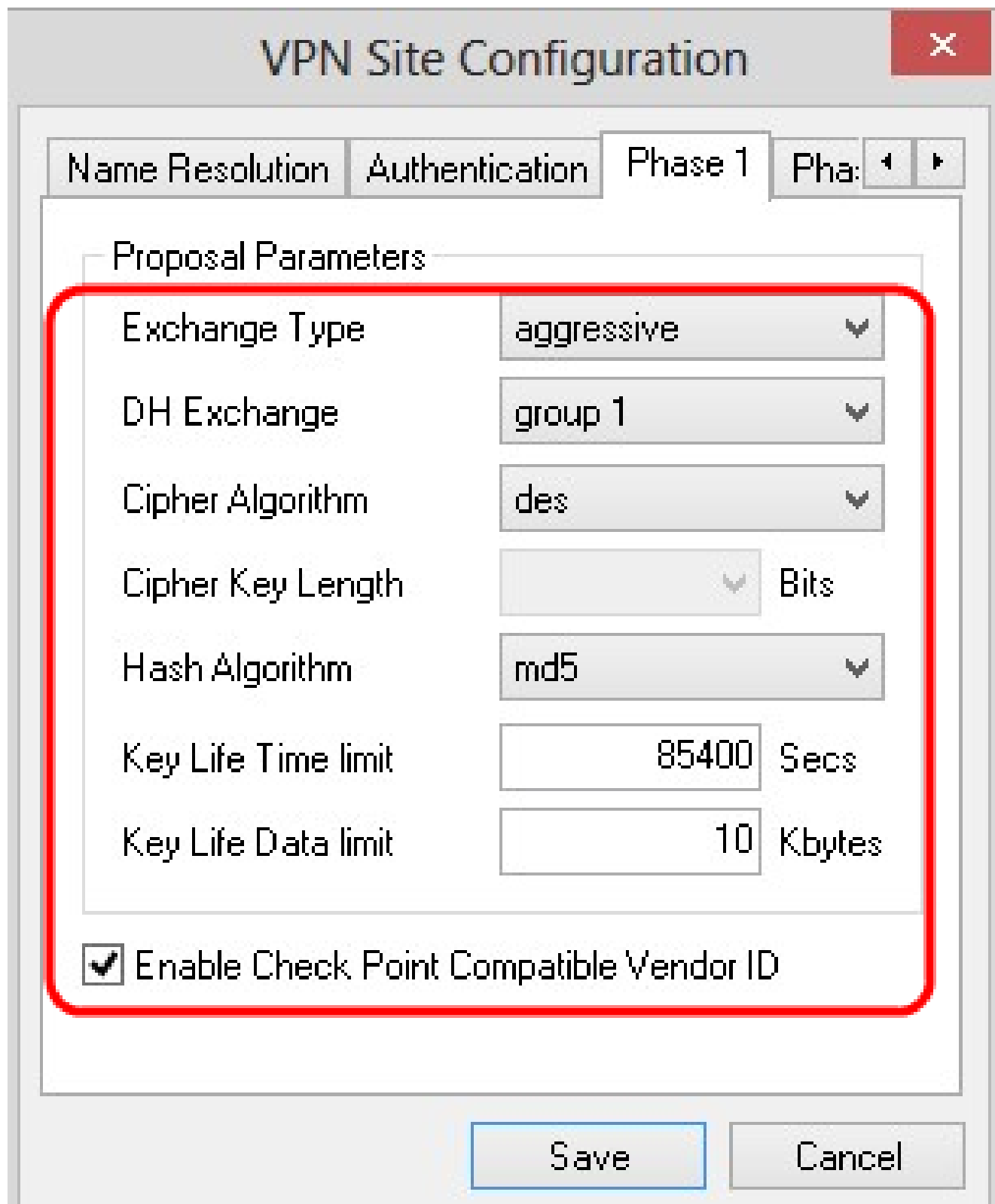
第五步：在Cipher Key Length下拉列表中，选择与配置VPN连接时选择的选项的密钥长度匹配的选项。

第六步：在Hash Algorithm下拉列表中，选择在配置VPN连接时选择的选项。

步骤 7.在Key Life Time limit字段中，输入在配置VPN连接期间使用的值。

步骤 8在Key Life Data limit字段中，输入要保护的值得值（以千字节为单位）。默认值为0，表示关闭该功能。

步骤9.（可选）选中Enable Check Point Compatible Vendor ID复选框。



步骤 10 点击 Save (保存) ， 以保存设置。

第2阶段配置

步骤1:单击Phase 2选项卡。

VPN Site Configuration

✕

AuthenticationPhase 1Phase 2Policy◀▶

Proposal Parameters

Transform Algorithm	<input type="text" value="auto"/>
Transform Key Length	<input type="text" value=""/> Bits
HMAC Algorithm	<input type="text" value="auto"/>
PFS Exchange	<input type="text" value="disabled"/>
Compress Algorithm	<input type="text" value="disabled"/>
Key Life Time limit	<input type="text" value="3600"/> Secs
Key Life Data limit	<input type="text" value="0"/> Kbytes

注意：在Phase 2部分中，您可以配置参数，以便可以建立具有远程客户端网关的IPsec SA。

第二步：在Transform Algorithm下拉列表中，选择在VPN连接配置期间选择的选项。

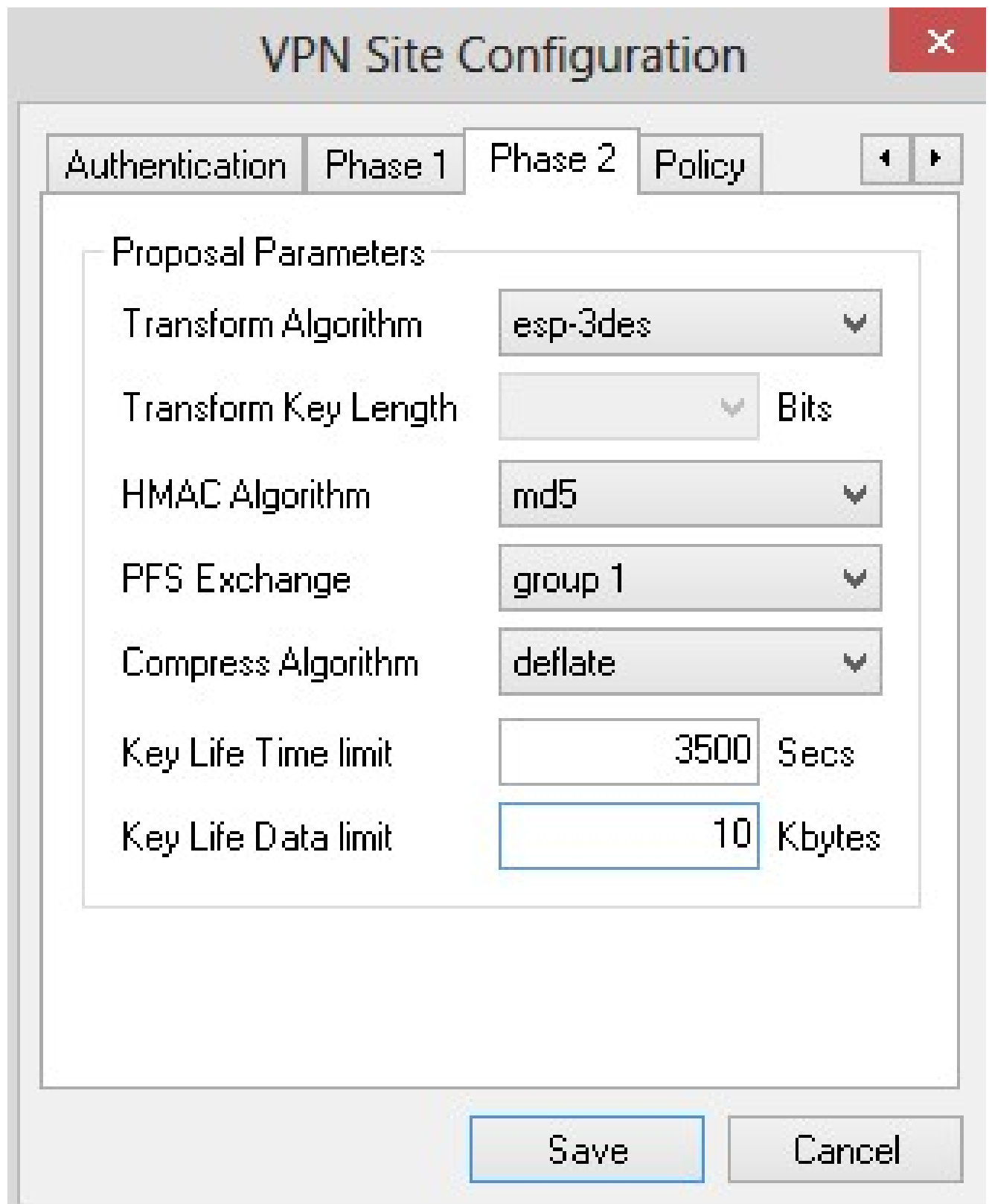
第三步：在Transform Key Length下拉列表中，选择与VPN连接配置期间选择的选项的密钥长度匹配的选项。

第四步：在HMAC Algorithm下拉列表中，选择在VPN连接配置期间选择的选项。

第五步：在PFS Exchange下拉列表中，选择在VPN连接配置期间选择的选项。

第六步：在Key Life Time limit字段中，输入在配置VPN连接期间使用的值。

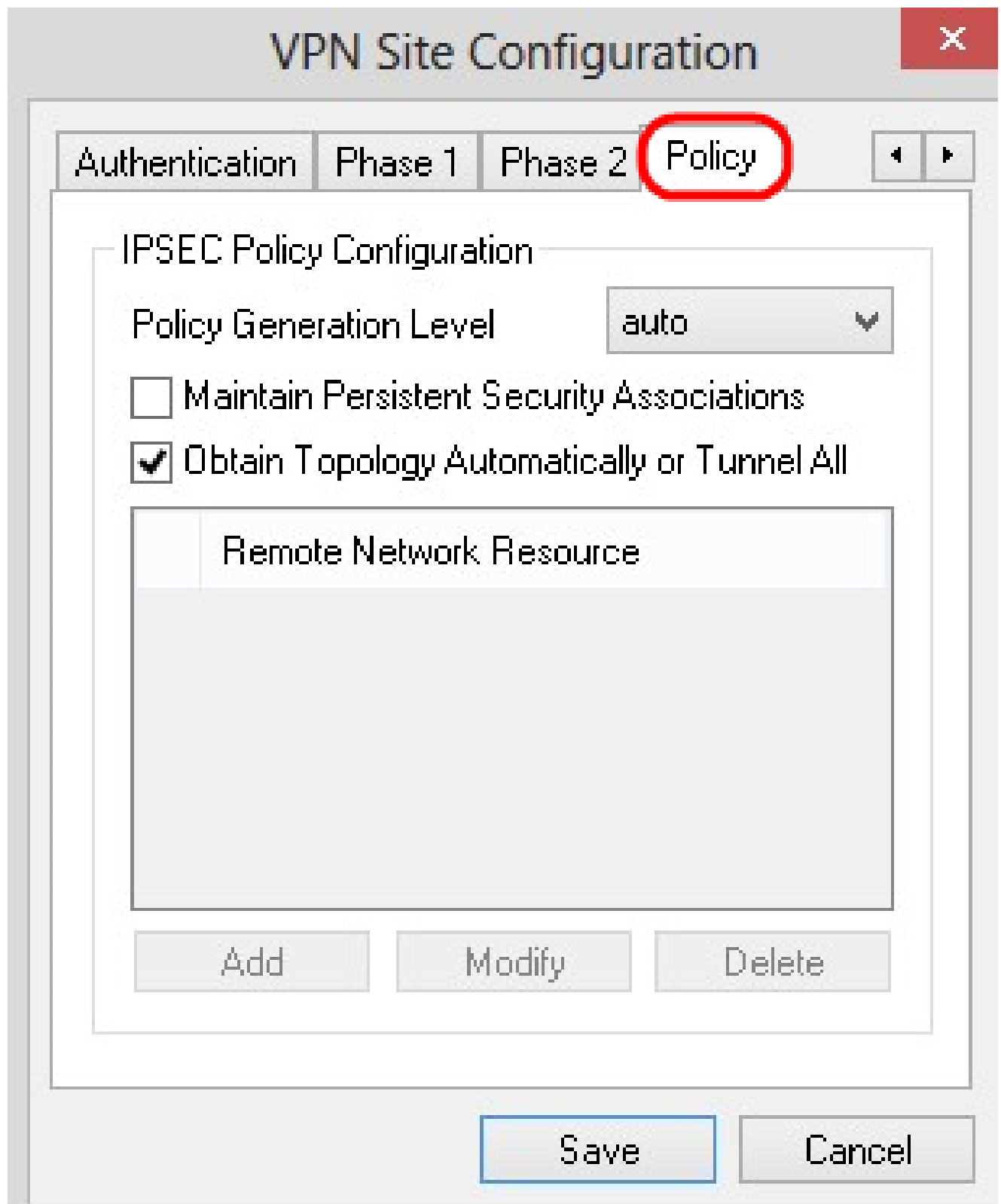
步骤 7.在Key Life Data limit字段中，输入要保护的值得值（以千字节为单位）。默认值为0，表示关闭该功能。



步骤 8 点击 Save (保存) ，以保存设置。

策略配置

步骤 1. 单击 Policy 选项卡。



注意：在Policy部分中，定义了IPSEC策略，客户端需要该策略才能与主机进行通信以进行站点配置。

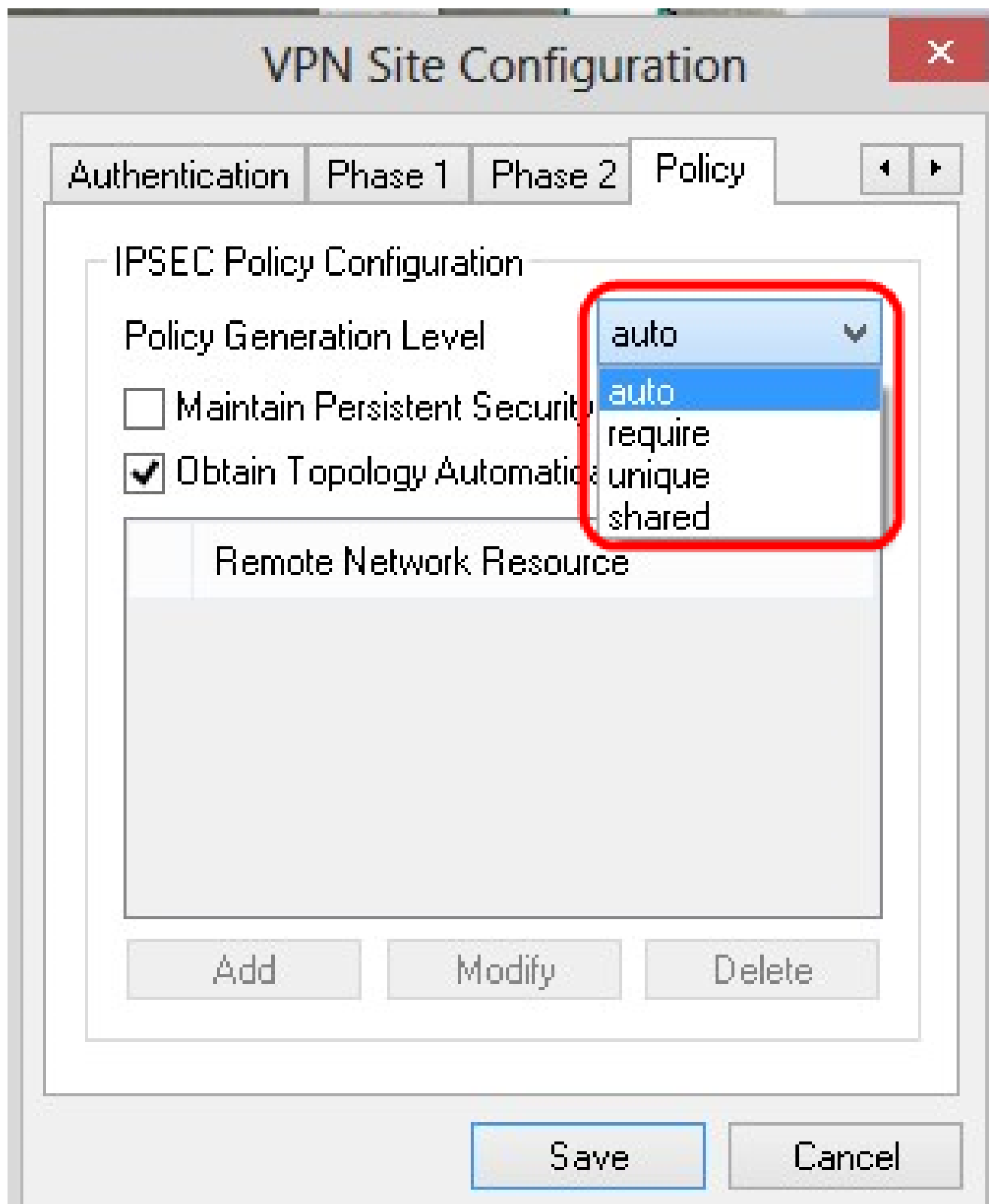
第二步：在Policy Generation Level下拉列表中，选择适当的选项。

- 自动 — 自动确定必要的IPsec策略级别。

·需要 — 不协商每个策略的唯一安全关联。

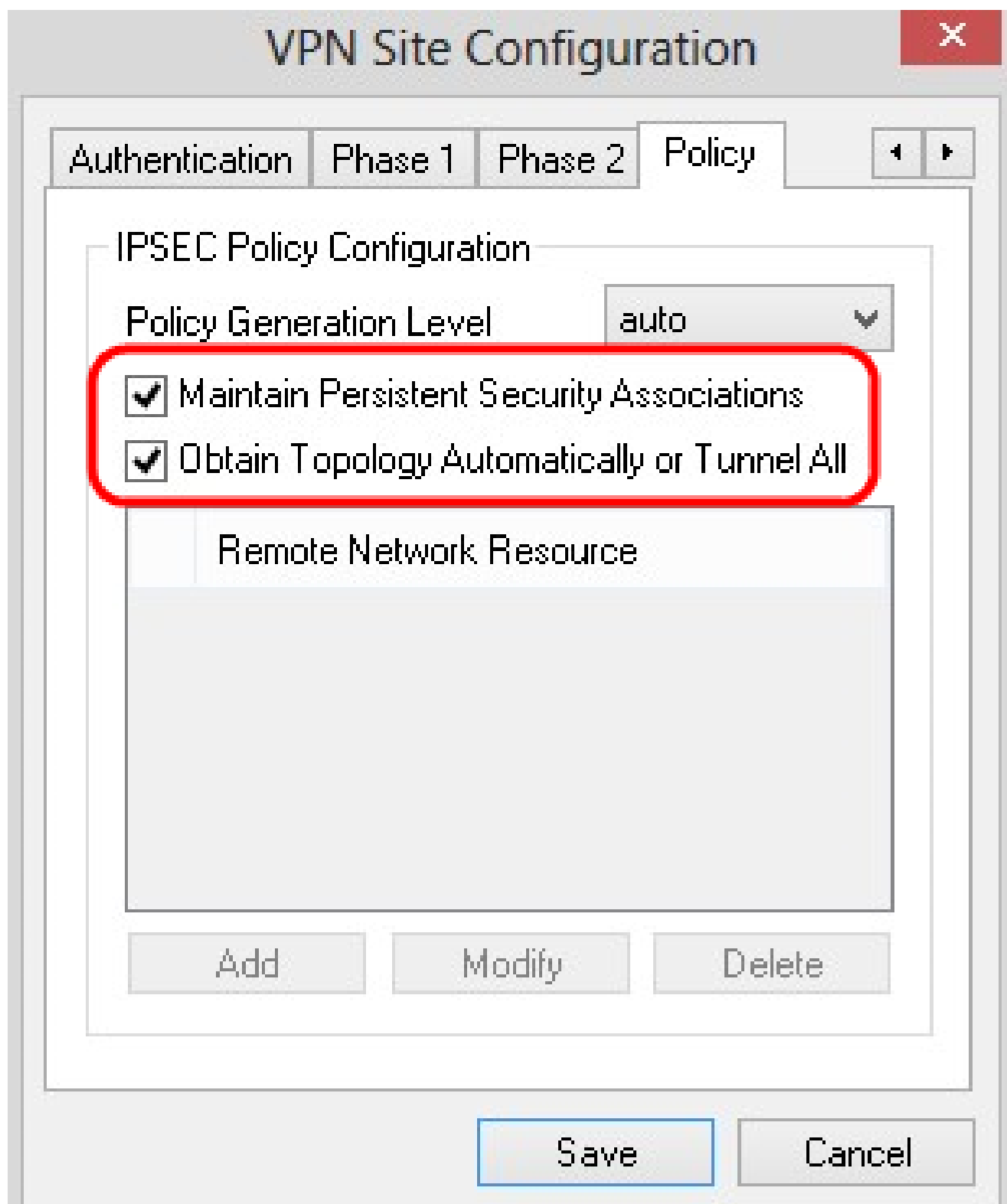
·唯一 — 协商每个策略的唯一安全关联。

·共享 — 在必要的级别生成适当的策略。

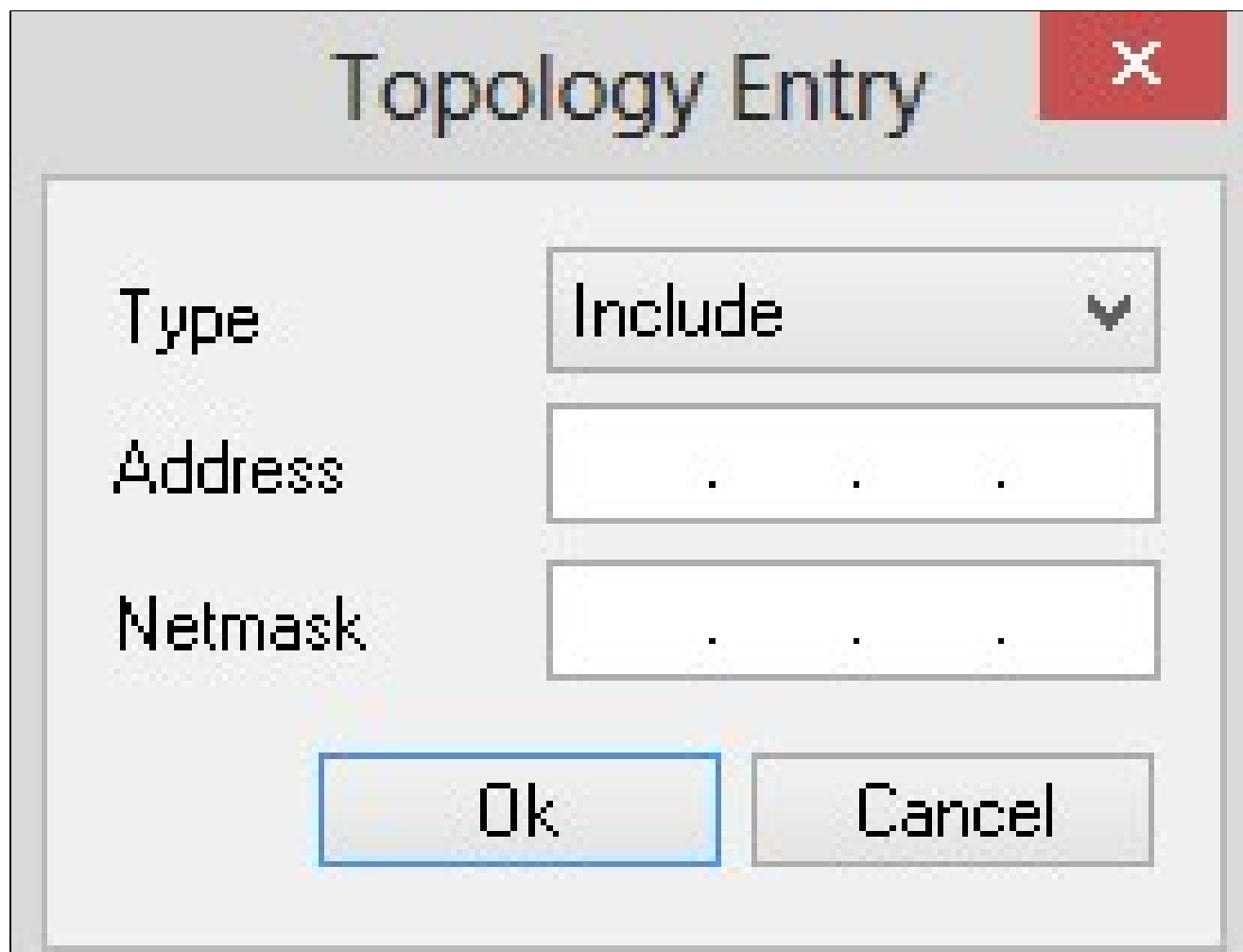


步骤3. (可选) 要更改IPSec协商, 请选中Maintain Persistent Security Associations复选框。如果启用, 则直接在连接后为每个策略进行协商。如果禁用, 则根据需要进行协商。

步骤4. (可选) 要从设备接收自动提供的网络列表, 或要将所有数据包默认发送到RV0XX, 请选中Obtain Topology Automatically or Tunnel All复选框。如果未选中, 则必须手动执行配置。如果选中此复选框, 请跳至步骤10。



第五步：单击Add将拓扑条目添加到表中。出现Topology Entry窗口。

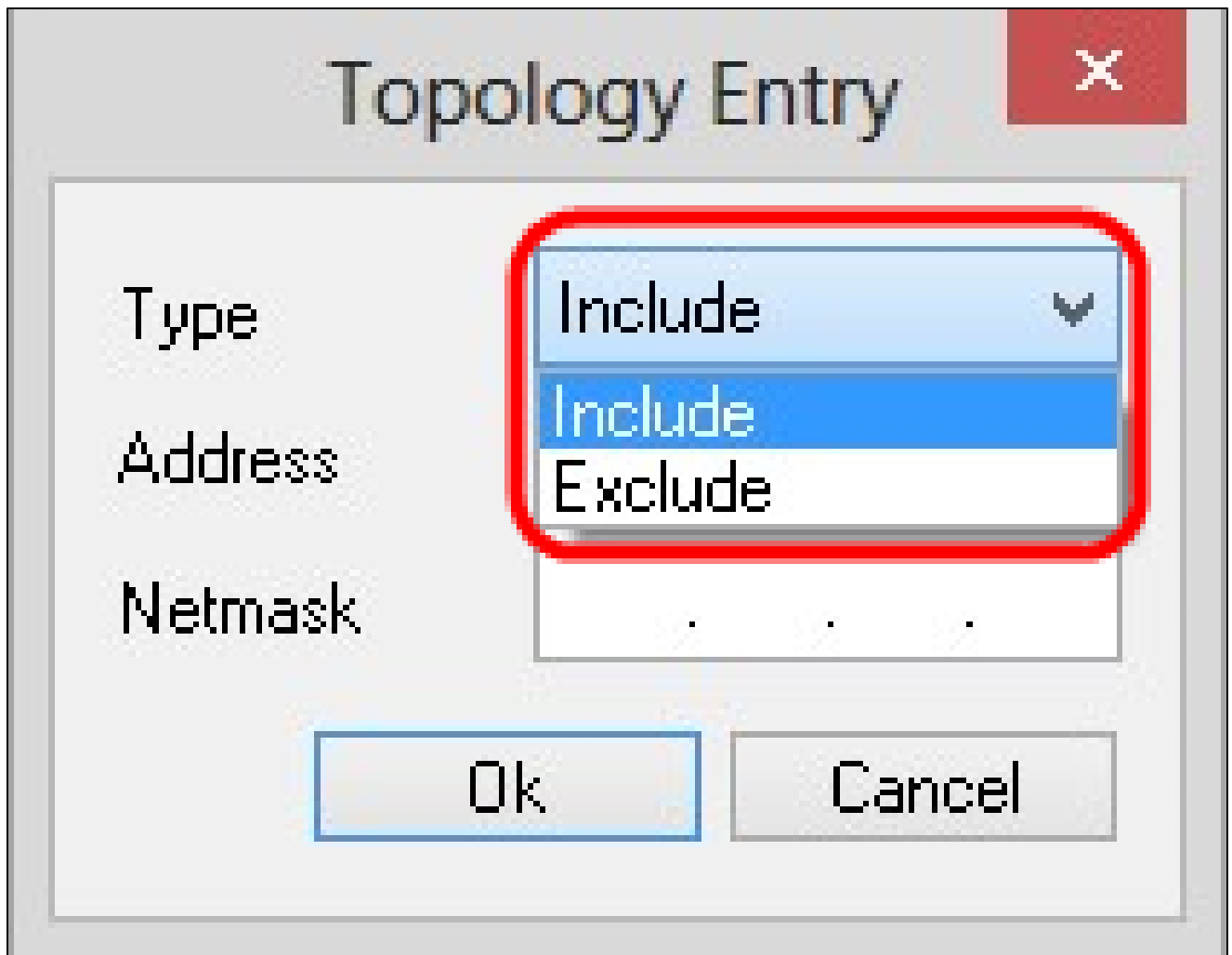


The image shows a dialog box titled "Topology Entry" with a close button (X) in the top right corner. The dialog contains three input fields: "Type" with a dropdown menu showing "Include", "Address" with a text box containing three dots, and "Netmask" with a text box containing three dots. At the bottom are "Ok" and "Cancel" buttons.

第六步：在Type下拉列表中，选择适当的选项。

·包括 — 通过VPN网关访问网络。

·排除 — 通过本地连接访问网络。



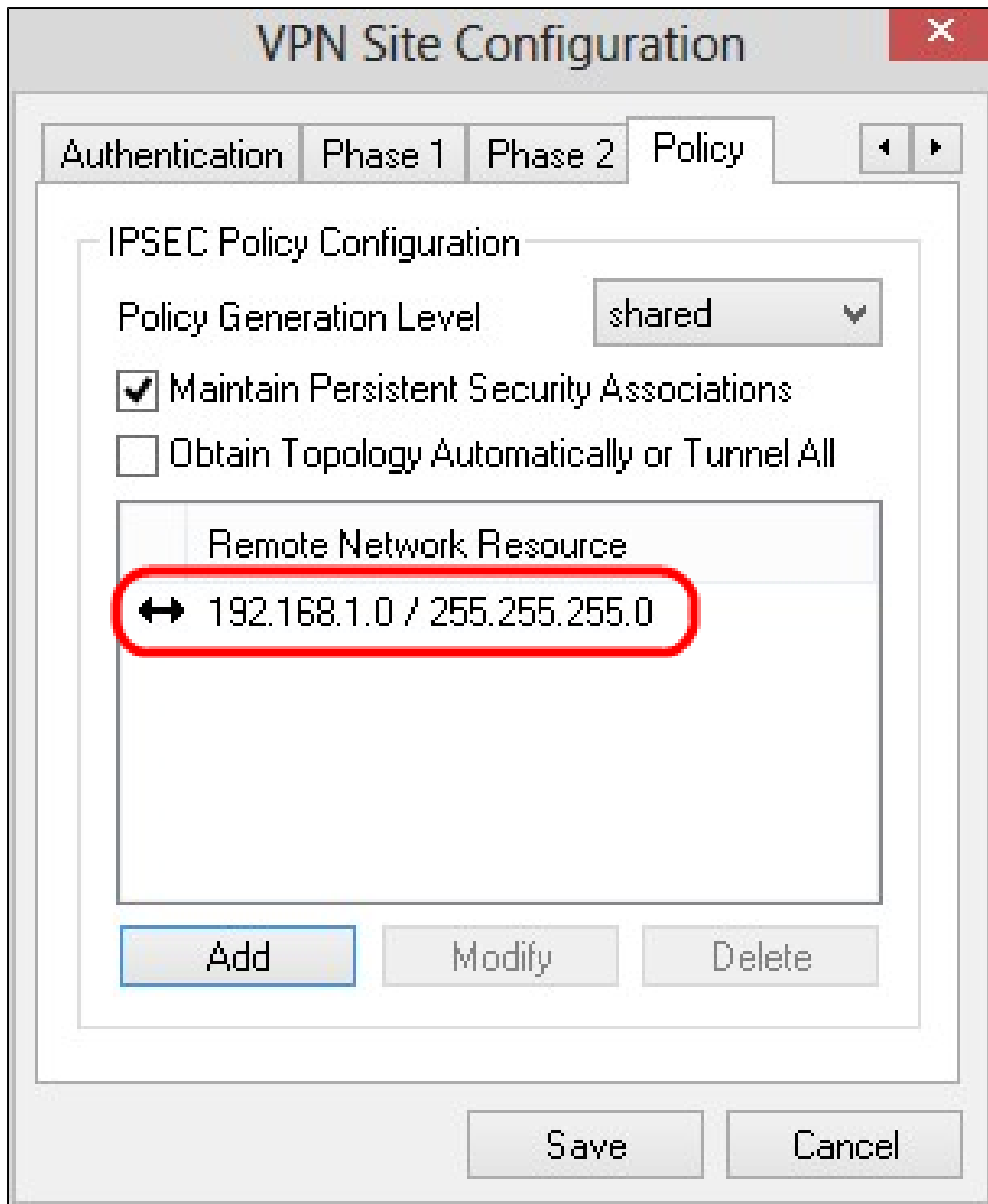
步骤 7.在Address字段中，输入RV0XX的IP地址。

步骤 8在Netmask字段中，输入设备的子网掩码地址。

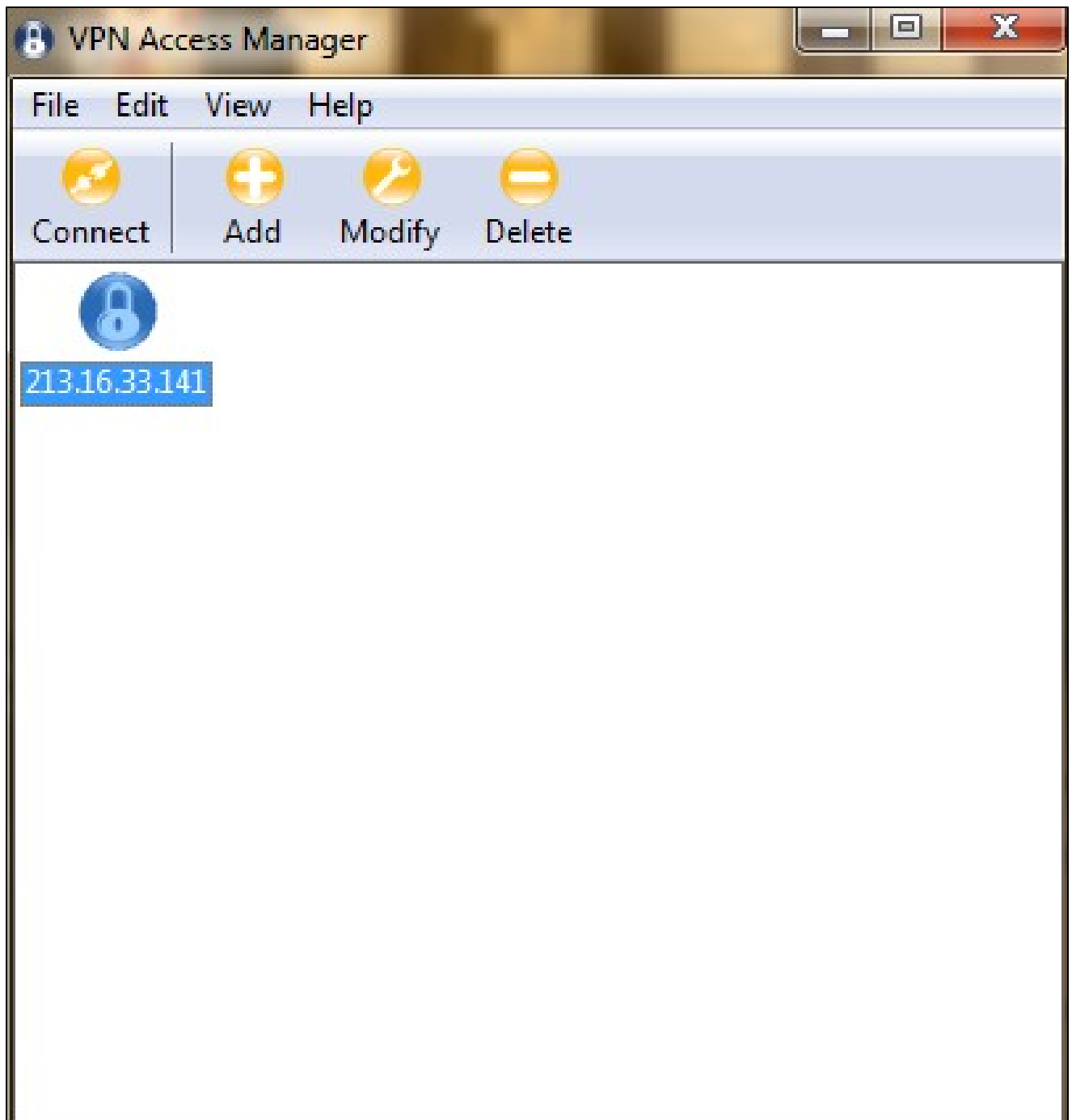
Topology Entry ✕

Type	Include ▼
Address	192.168.1.0
Netmask	255.255.255.0

步骤 9 Click OK. RV0XX的IP地址和子网掩码地址显示在Remote Network Resource列表中。



步骤 10单击Save，这会将用户返回到显示新VPN连接的VPN Access Manager窗口。

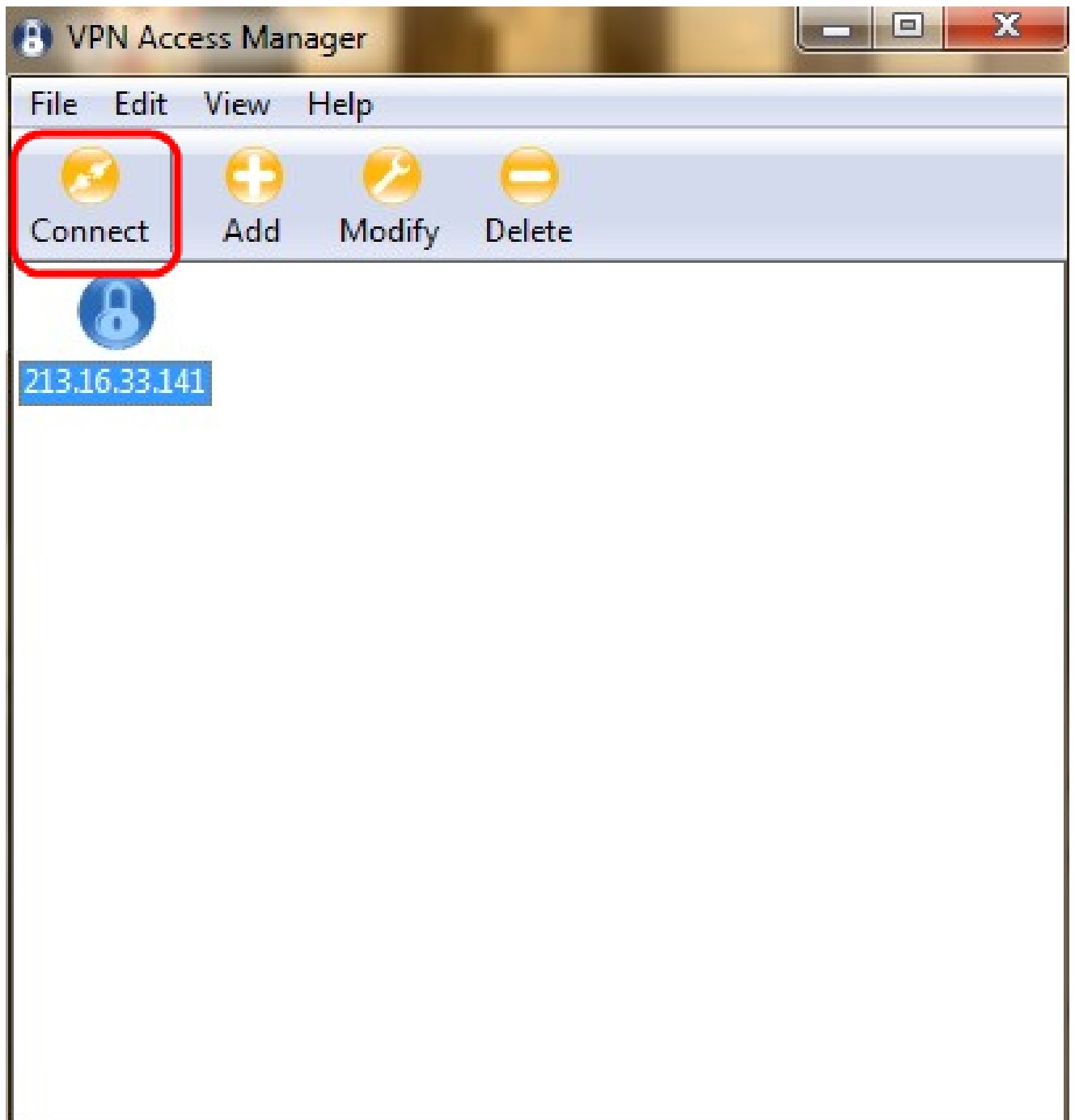


连接

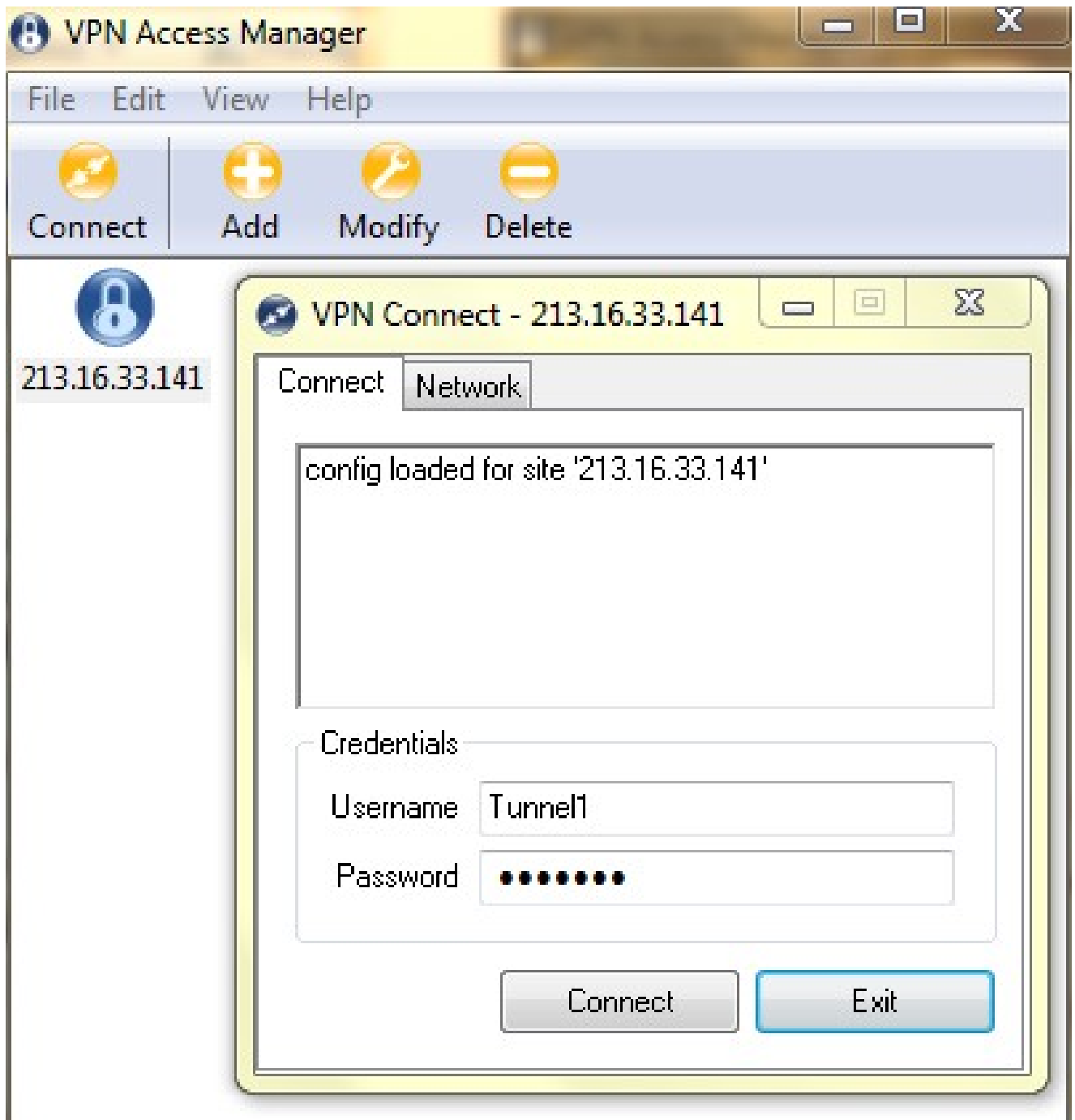
本节介绍如何在配置所有设置后设置VPN连接。所需的登录信息与设备上配置的VPN客户端访问信息相同。

步骤1:单击所需的VPN连接。

第二步：单击 Connect。



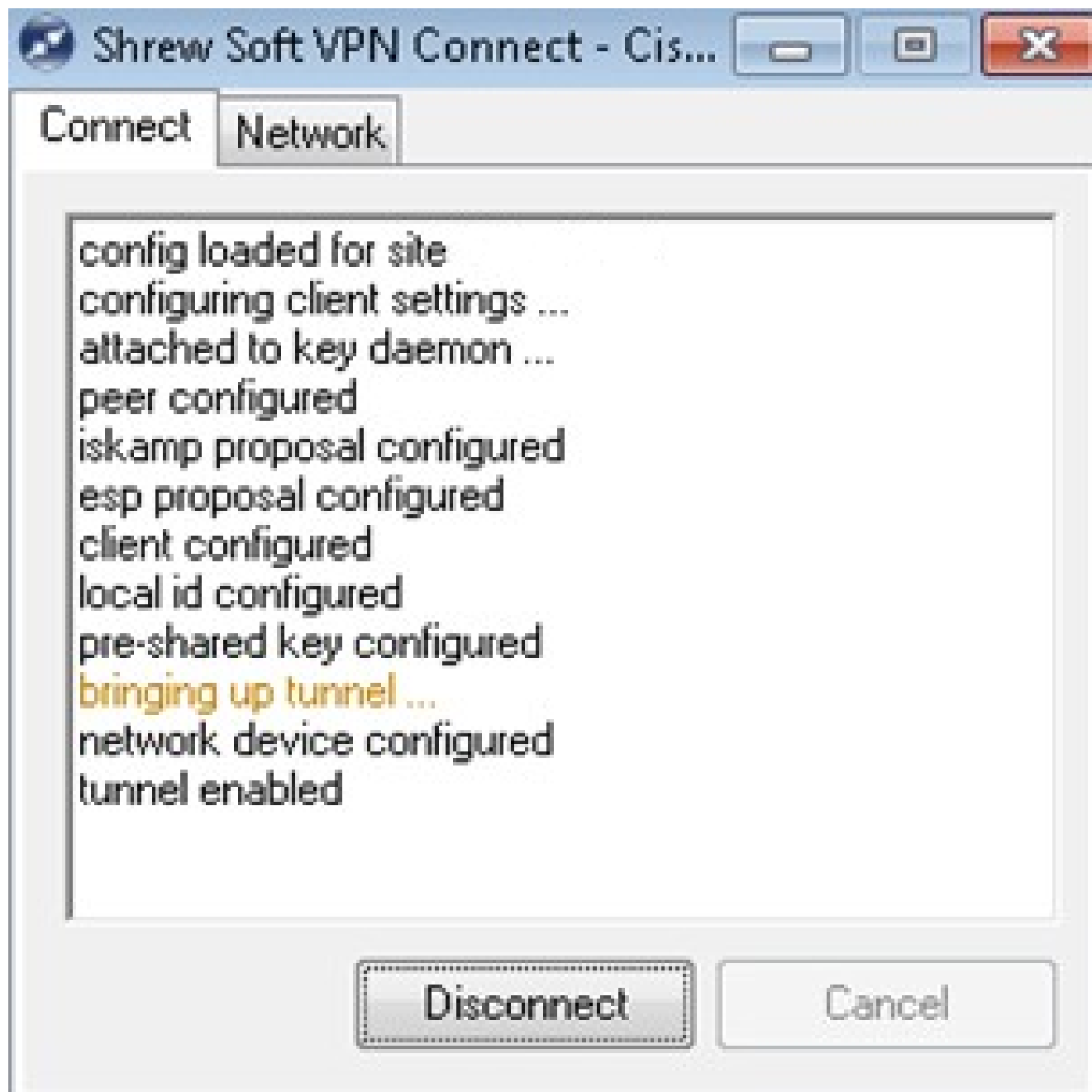
出现VPN Connect窗口：



第三步：在用户名字段中输入VPN的用户名。

第四步：在密码字段中输入VPN用户帐户的密码。

第五步：单击 Connect。出现Shrew Soft VPN Connect窗口：



步骤6. (可选) 要禁用连接，请单击Disconnect。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。