

在RV130和RV130W上使用Shrew Soft VPN Client连接IPSec VPN Server

目标

通过IPSec VPN (虚拟专用网络) ，您可以通过建立互联网上的加密隧道安全地获取远程资源。

RV130和RV130W用作IPSec VPN服务器，支持Shrew Soft VPN客户端。

确保下载最新版本的客户端软件。

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

注意：要成功设置和配置带有IPSec VPN服务器的Shrew Soft VPN客户端，您需要首先配置IPSec VPN服务器。有关如何执行此操作的信息，请参阅[在RV130和RV130W上配置IPSec VPN服务器](#)一文。

本文档的目的是向您展示如何使用Shrew Soft VPN客户端连接到RV130和RV130W上的IPSec VPN服务器。

适用设备

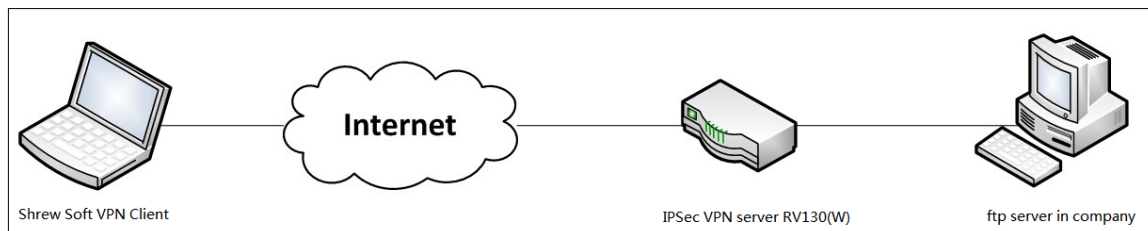
- RV130W Wireless-N VPN防火墙
- RV130 VPN防火墙

系统要求

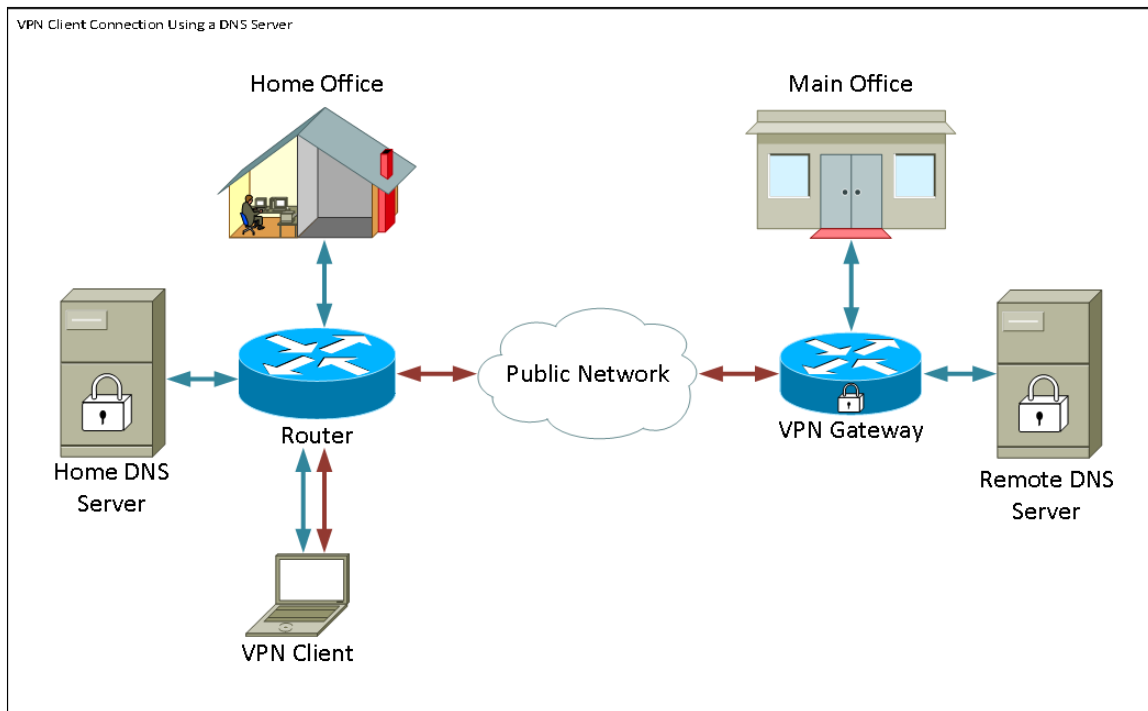
- 32或64位系统
- Windows 2000、XP、Vista或Windows 7/8

拓扑

下面显示了一个顶级拓扑，说明Shrewsoft客户端到站点配置中涉及的设备。



下面是一个更详细的流程图，说明DNS服务器在小型企业网络环境中的作用。



软件版本

•1.0.1.3

设置共享软件VPN客户端

IPSec VPN设置和用户配置

步骤1.登录到Web配置实用程序并选择VPN > IPSec VPN Server > Setup。将打开 *Setup* 页面

。

Setup

Server Enable:

NAT Traversal: Disabled

Phase 1 Configuration

Pre-Shared Key:

Exchange Mode:

Encryption Algorithm:

Authentication Algorithm:

DH Group:

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

Phase 2 Configuration

Local IP:

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

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

Encryption Algorithm:


Authentication Algorithm:

PFS Key Group: Enable

DH Group:

步骤2. 验证是否已正确配置RV130的IPSec VPN服务器。如果IPSec VPN服务器未配置或配置错误，请参阅[在RV130和RV130W上配置IPSec VPN服务器](#)，然后单击**保存**。

Setup

 Configuration settings have been saved successfully

Server Enable:

NAT Traversal: Disabled

Phase 1 Configuration

Pre-Shared Key:

Exchange Mode:

Encryption Algorithm:

Authentication Algorithm:

DH Group:

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

Phase 2 Configuration

Local IP:

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

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

Encryption Algorithm:

Authentication Algorithm:

PFS Key Group: Enable

DH Group:

注意：以上设置是RV130/RV130W IPSec VPN服务器配置的示例。这些设置基于文档[在RV130和RV130W上配置IPSec VPN服务器](#)，在后续步骤中将参考这些设置。

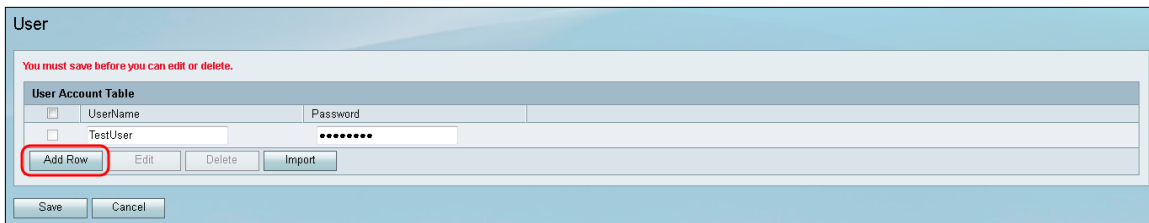
步骤3.导航到VPN > IPSec VPN Server > User。系统将显示User页面。

User

User Account Table

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

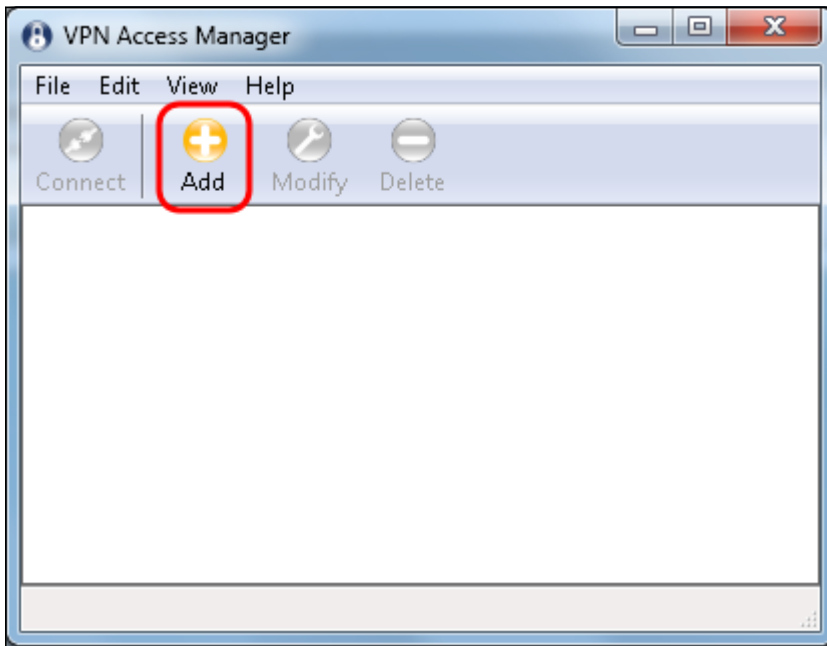
第4步：单击Add Row以添加用于对VPN客户端进行身份验证（扩展身份验证）的用户帐户，并在提供的字段中输入所需的用户名和密码。



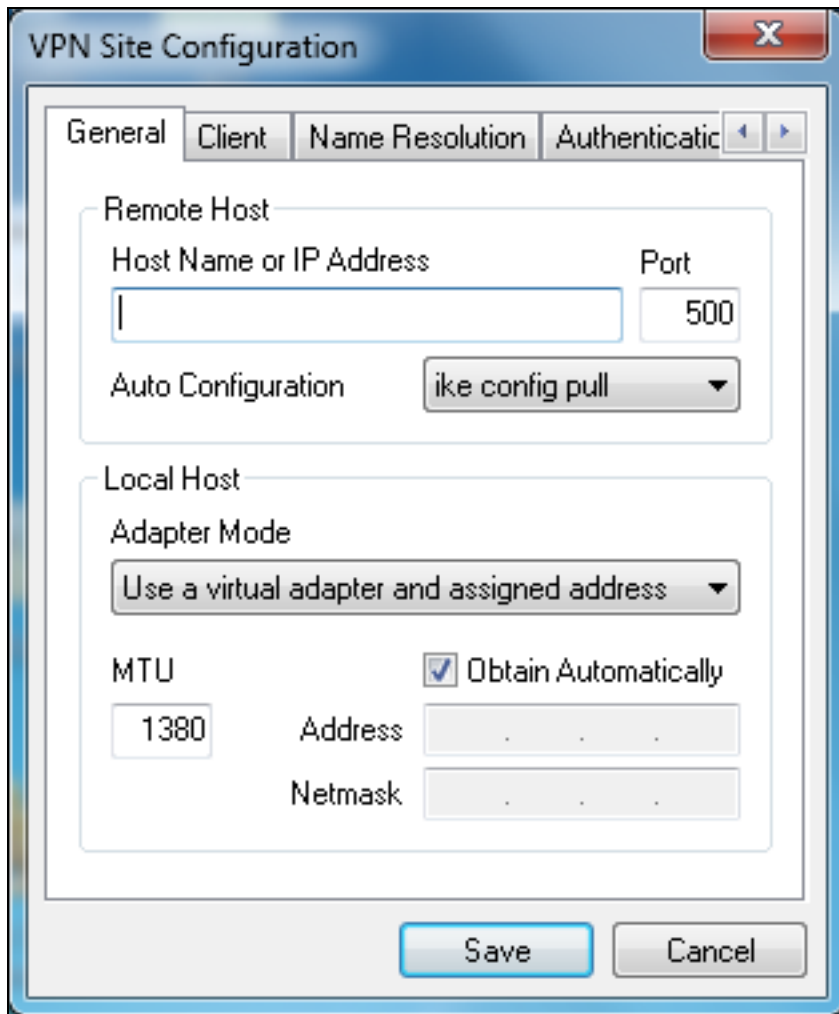
第 5 步： 点击 **Save** (保存) ， 以保存设置。

VPN 客户端配置

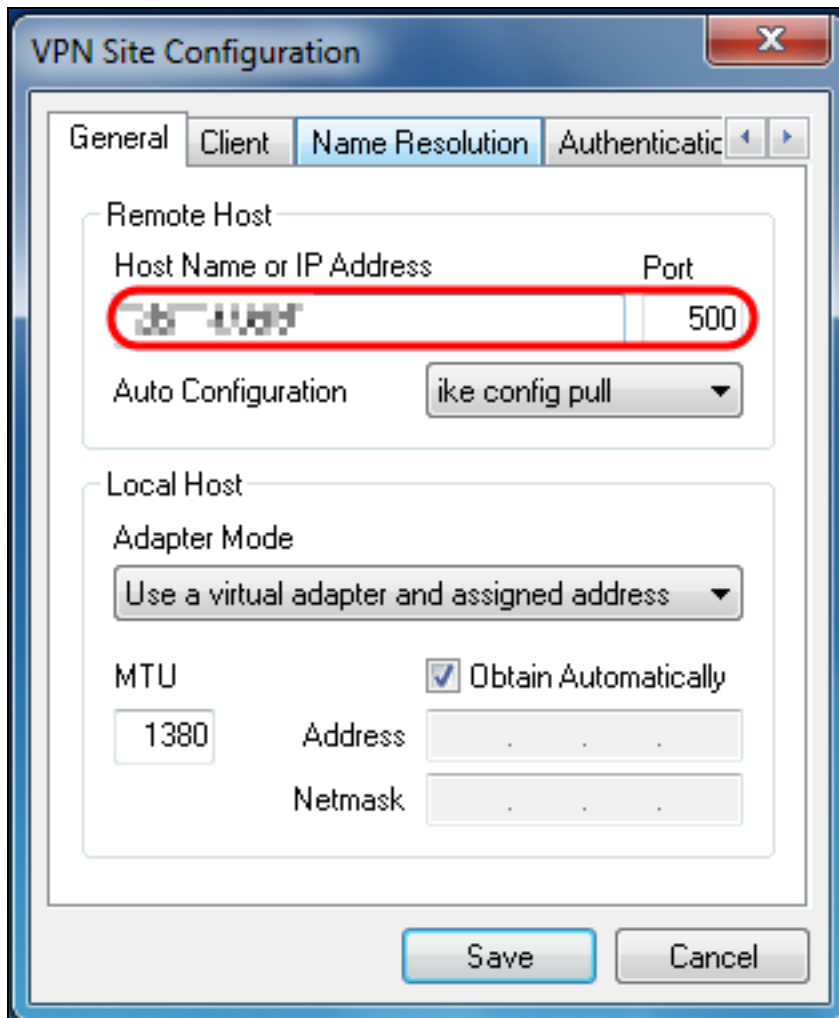
步骤1. 打开Shrew VPN Access Manager并单击**Add**添加配置文件。



出现 *VPN Site Configuration* 窗口。

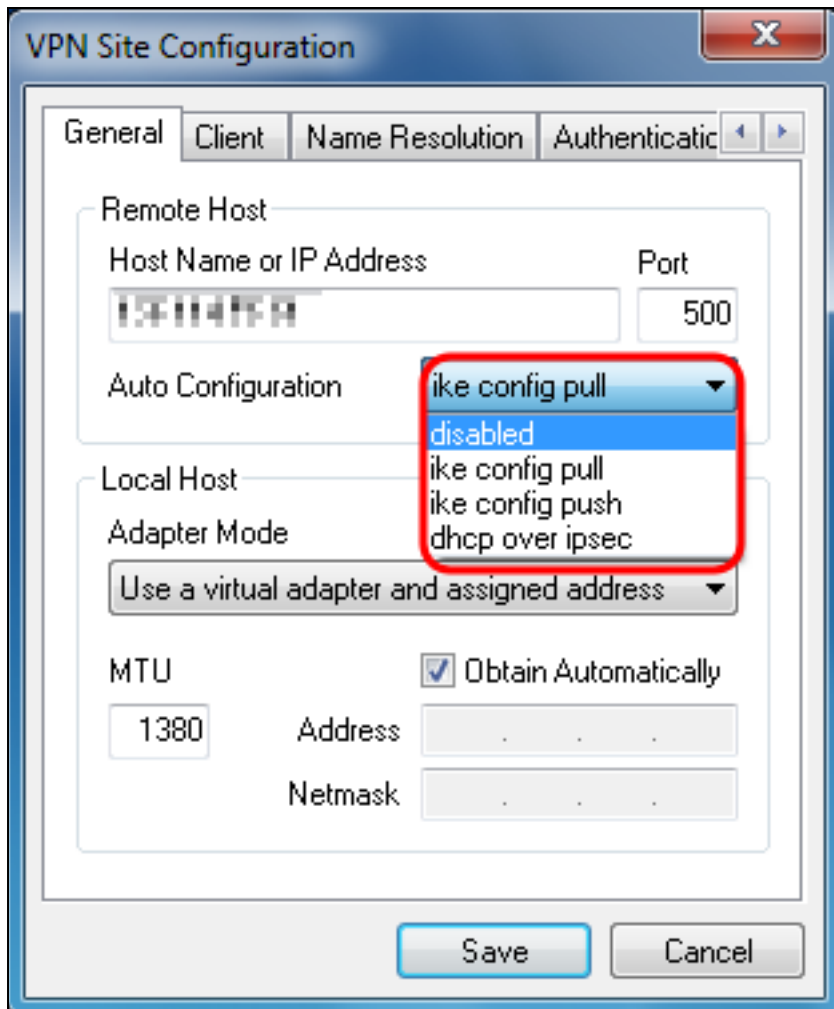


步骤2.在 *General* 选项卡下的 *Remote Host* 部分中，输入尝试连接的网络的公有主机名或IP地址。



注意：确保端口号设置为默认值500。为了使VPN正常工作，隧道使用UDP端口500，该端口应设置为允许在防火墙上转发ISAKMP流量。

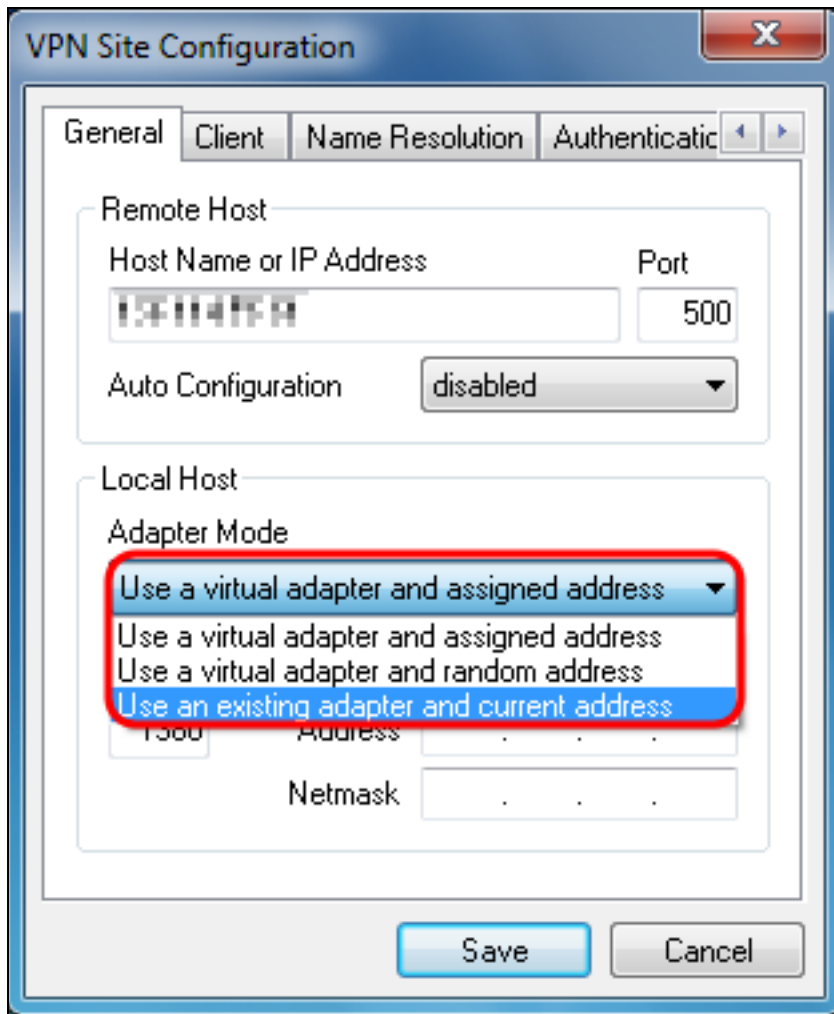
步骤3.在*Auto Configuration*下拉列表中，选择**disabled**。



可用选项定义如下：

- 已禁用 — 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。

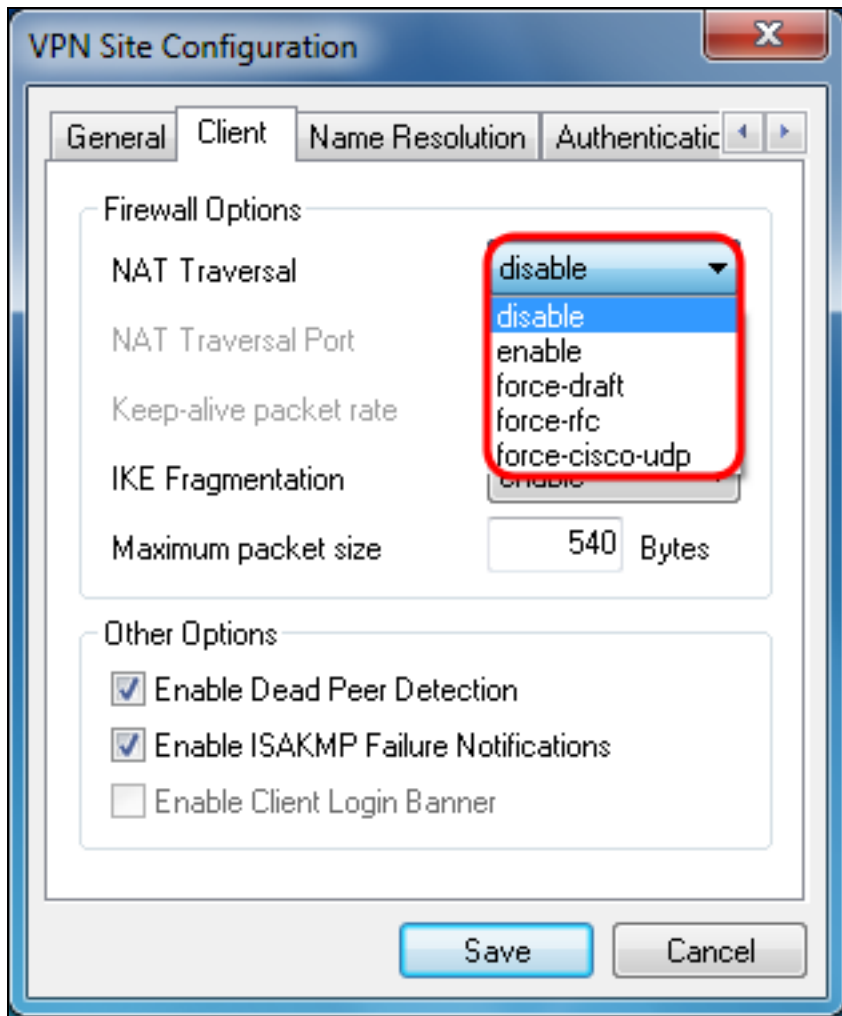
步骤4.在*Local Host*部分中，在*Adapter Mode*下拉列表中选择**Use an existing adapter and current address**。



可用选项定义如下：

- 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作为其IPsec通信的源。
- 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作为其IPsec通信的源。
- 使用现有适配器和当前地址 — 允许客户端仅使用其现有物理适配器（其当前地址作为其IPsec通信的源）。

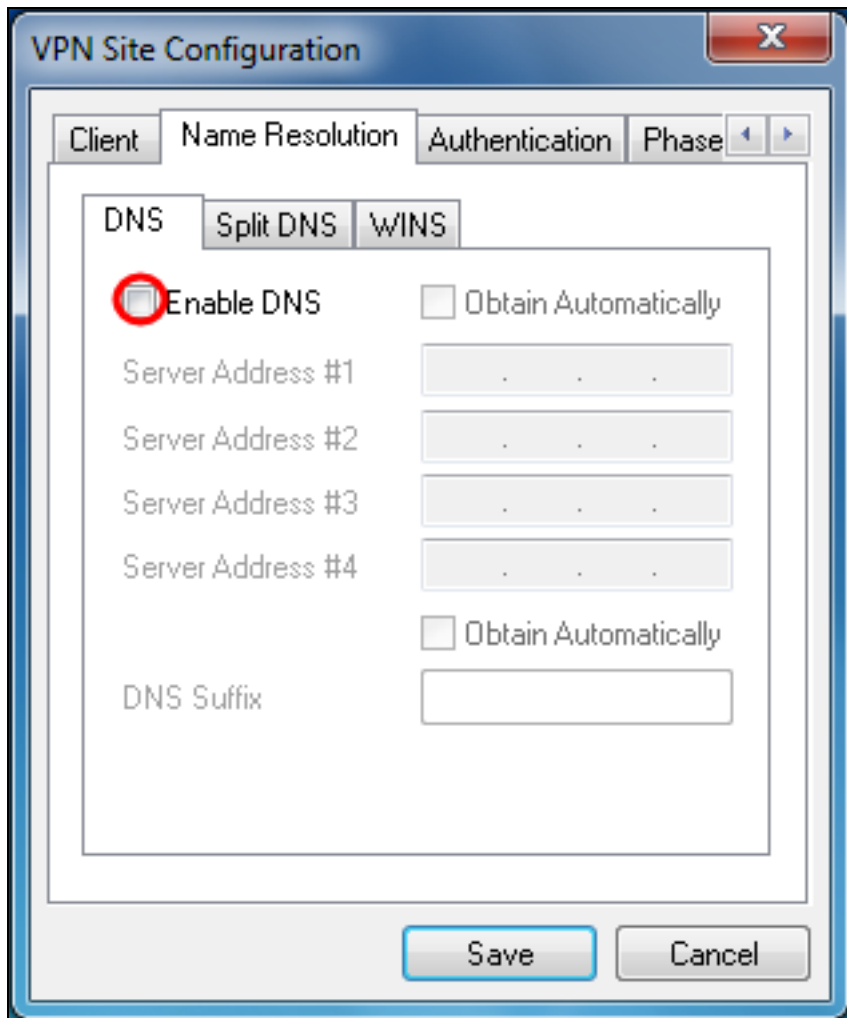
步骤5.单击Client选项卡。在NAT Traversal下拉列表中，选择[RV130和RV130W上的IPsec VPN服务器配置](#)一文中的RV130/RV130W上为NAT Traversal配置的同设置。



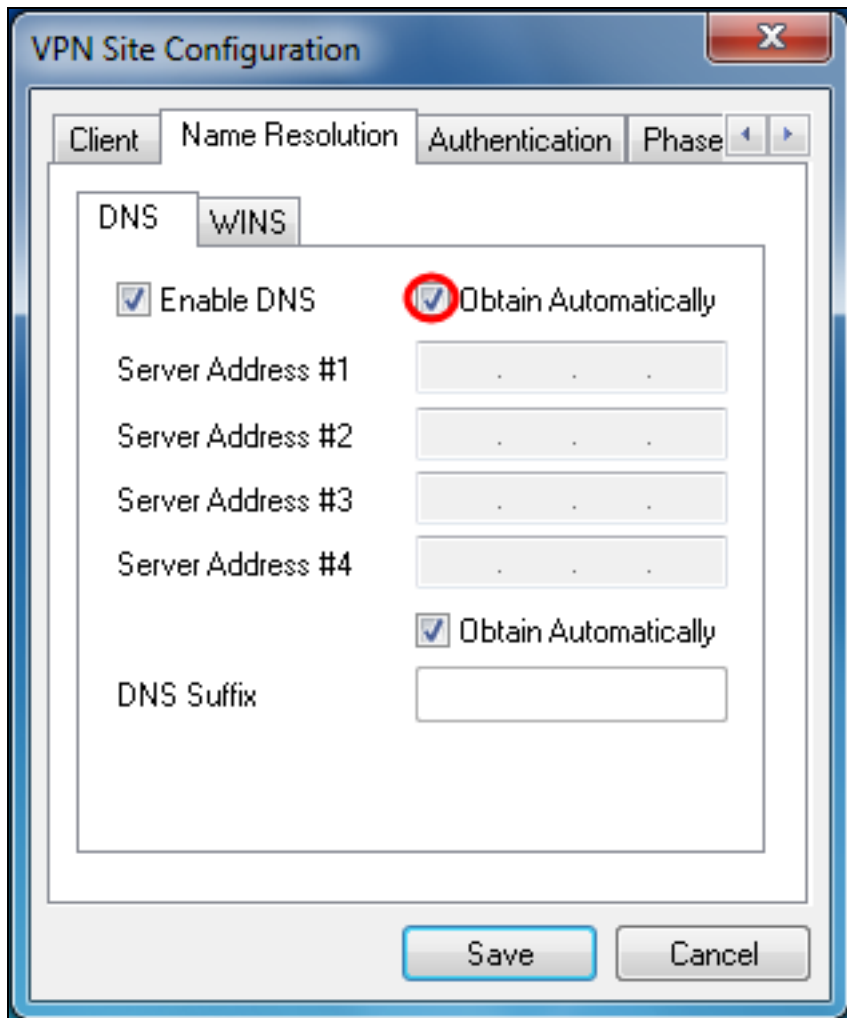
可用的Network Address Translation Traversal(NAT)菜单选项定义如下：

- 禁用 — 将不使用NAT协议扩展。
- 启用 — 只有当VPN网关在协商期间指示支持并且检测到NAT时，才会使用NAT协议扩展。
- Force-Draft — 将使用NAT协议扩展的Draft版本，而不论VPN网关是否在协商期间表示支持或检测到NAT。
- Force-RFC — 将使用NAT协议的RFC版本，而不论VPN网关是否在协商期间表示支持或检测到NAT。
- Force-Cisco-UDP — 为没有NAT的VPN客户端强制UDP封装。

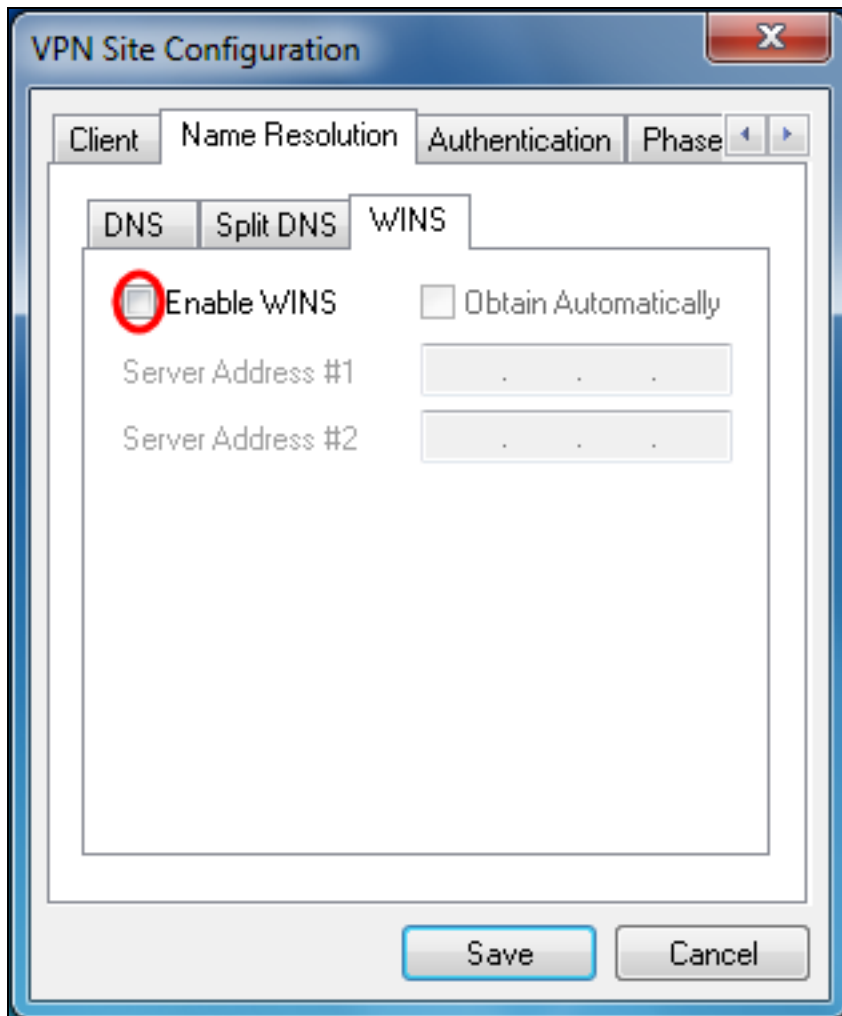
步骤6.单击*Name Resolution*选项卡，如果要启用DNS，请选中**Enable DNS**复选框。如果站点配置不需要特定DNS设置，请取消选中**Enable DNS**复选框。



步骤7. (可选) 如果您的远程网关配置为支持配置交换，则网关能够自动提供DNS设置。否则，请验证**Obtain Automatically**复选框是否已取消选中，并手动输入有效的DNS服务器地址。

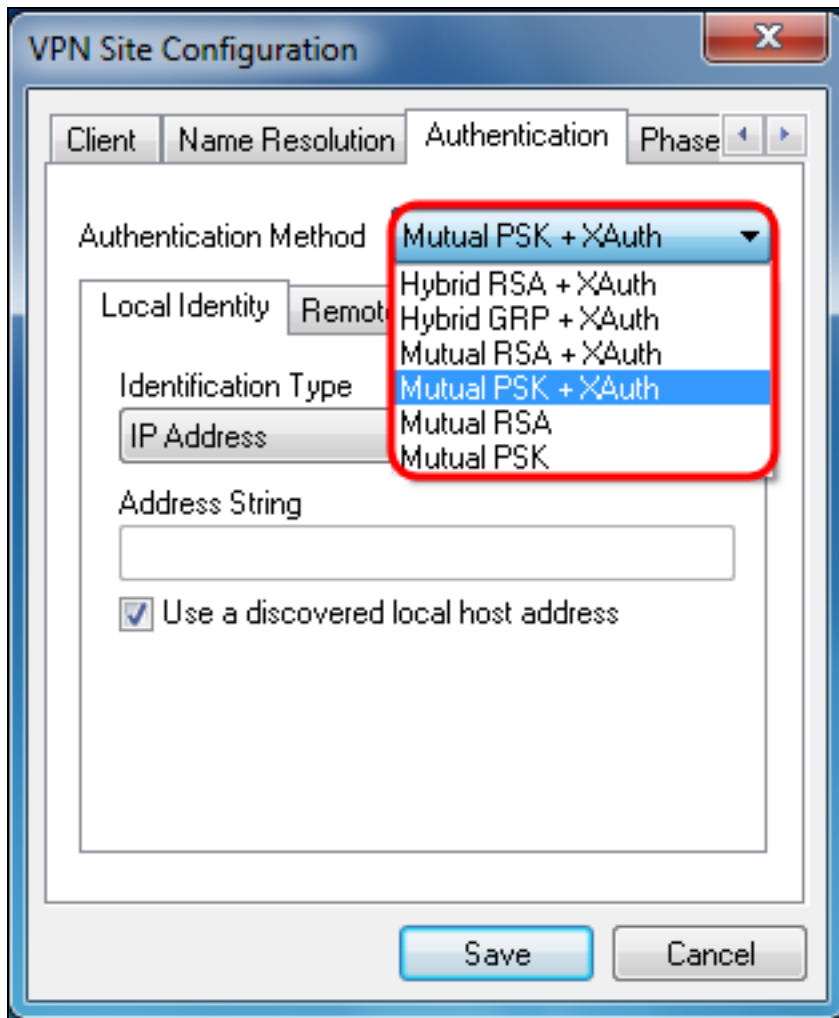


步骤8. (可选) 单击 *Name Resolution* 选项卡，如果要启用 Windows Internet Name Server (WINS)，请选中 **Enable WINS** 复选框。如果您的远程网关配置为支持配置交换，则该网关能够自动提供 WINS 设置。否则，请验证 **Obtain Automatically** 复选框是否已取消选中，并手动输入有效的 WINS 服务器地址。



注意：通过提供WINS配置信息，客户端将能够使用位于远程专用网络中的服务器解析WINS名称。这在尝试使用统一命名约定路径名访问远程Windows网络资源时非常有用。WINS服务器通常属于Windows域控制器或Samba服务器。

步骤9.单击*Authentication*选项卡，然后在**Authentication Method**下拉列表中选择**Mutual PSK + XAuth**。



可用选项定义如下：

·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。

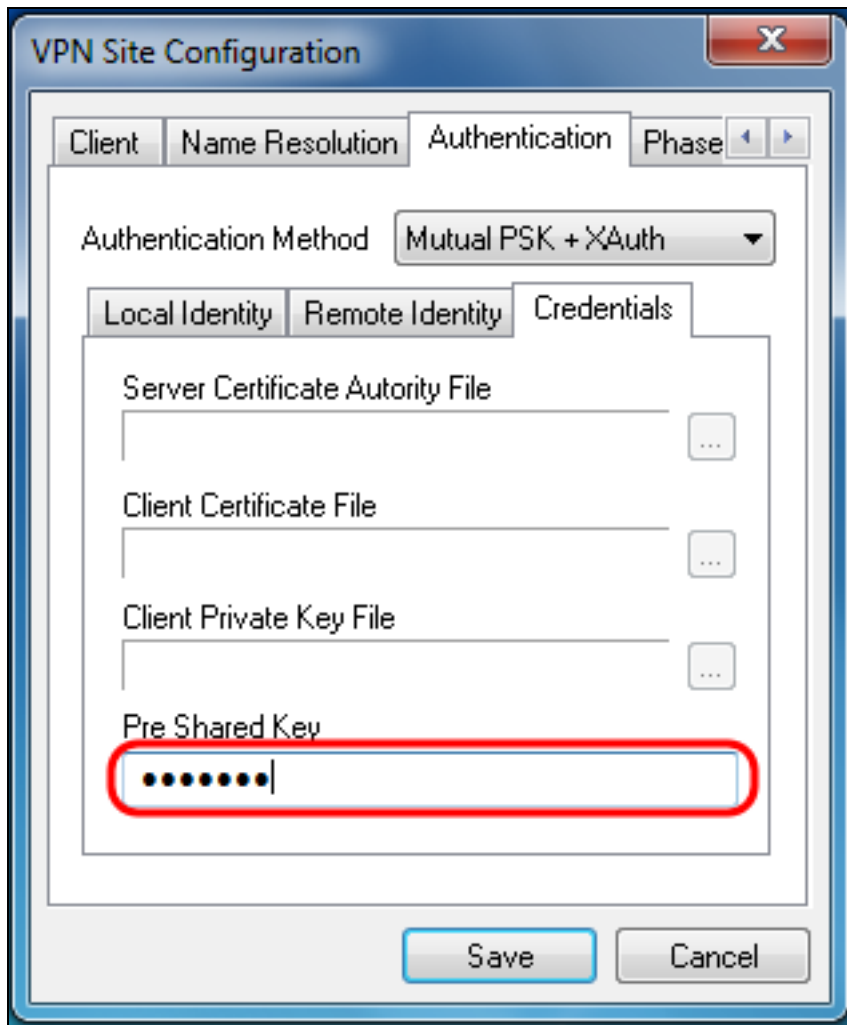
·双方RSA + 扩展验证 — 客户端和网关都需要凭据进行身份验证。凭证将采用PEM或 PKCS12证书文件或密钥类型的形式。

·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。

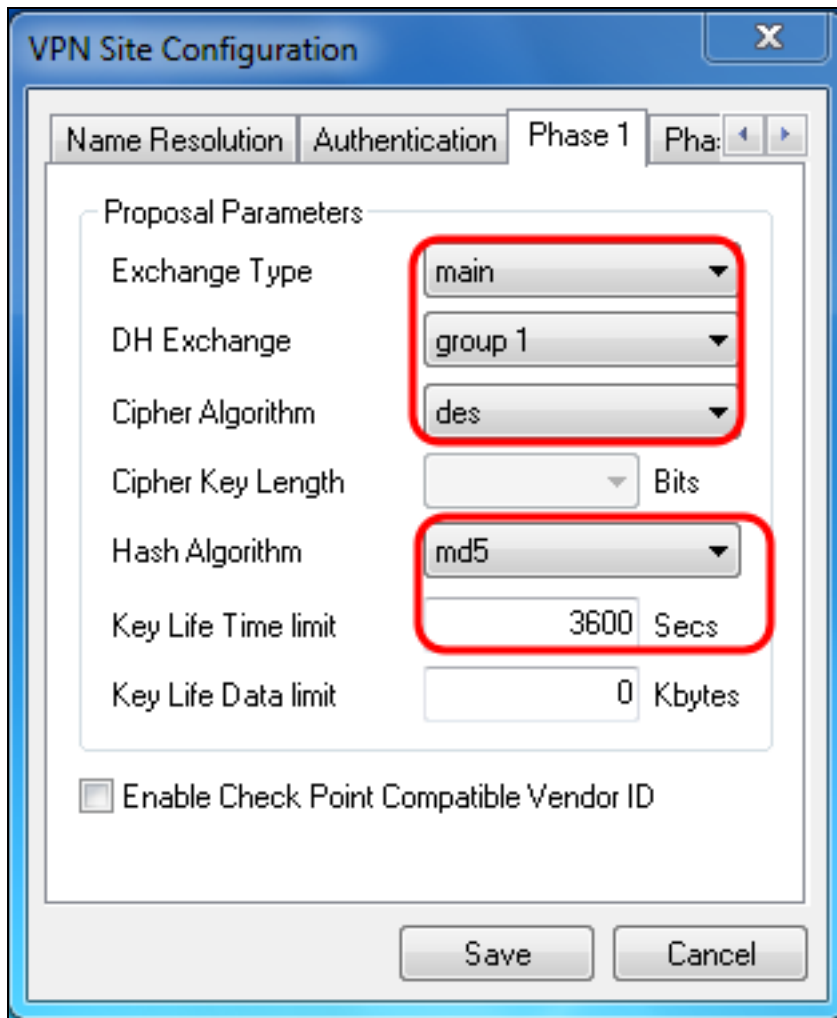
·双向RSA — 客户端和网关都需要凭据进行身份验证。凭证将采用PEM或PKCS12证书文件或密钥类型的形式。

·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。

步骤10.在Authentication部分中，单击Credentials子选项卡，然后在Pre Shared Key字段中输入您在IPsec VPN Server Setup页上配置的同一无共享密钥。



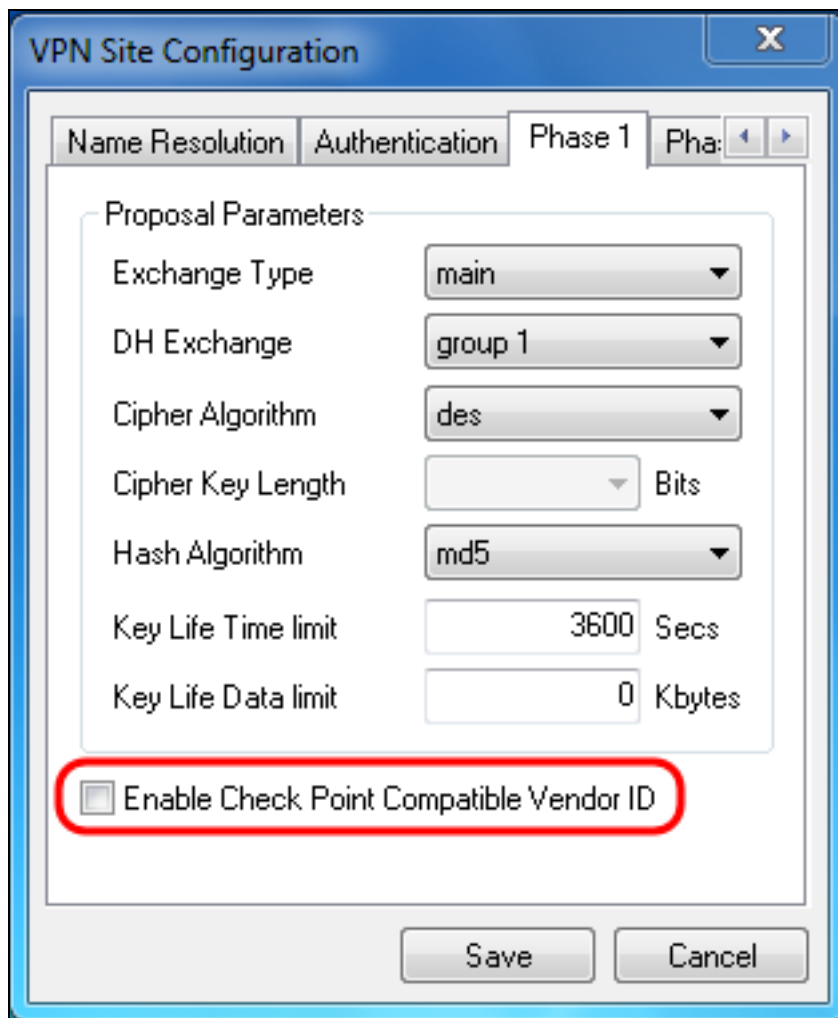
步骤11. 点击 *Phase 1* 选项卡。配置以下参数，使其与本文档的 [IPSec VPN服务器用户配置第2步中](#) 为 RV130/RV130W 配置的设置相同。



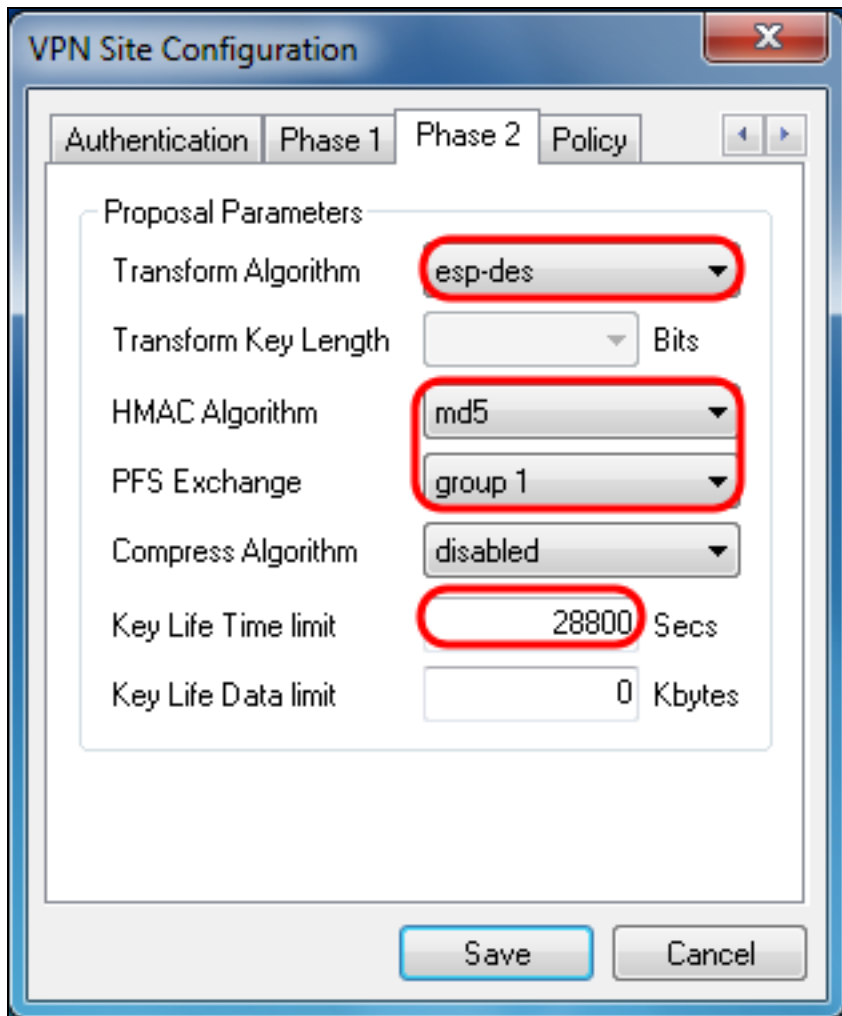
Shrew Soft中的参数应与阶段1中的RV130/RV130W配置匹配，如下所示：

- “Exchange Type”应与“Exchange Mode”匹配。
- “DH交换”应与“DH组”匹配。
- “密码算法”应与“加密算法”匹配。
- “哈希算法”应与“身份验证算法”匹配。

步骤12. (可选) 如果您的网关在第1阶段协商期间提供思科兼容供应商ID，请选中**Enable Check Point Compatible Vendor ID**复选框。如果网关没有或您不确定，请取消选中此复选框。



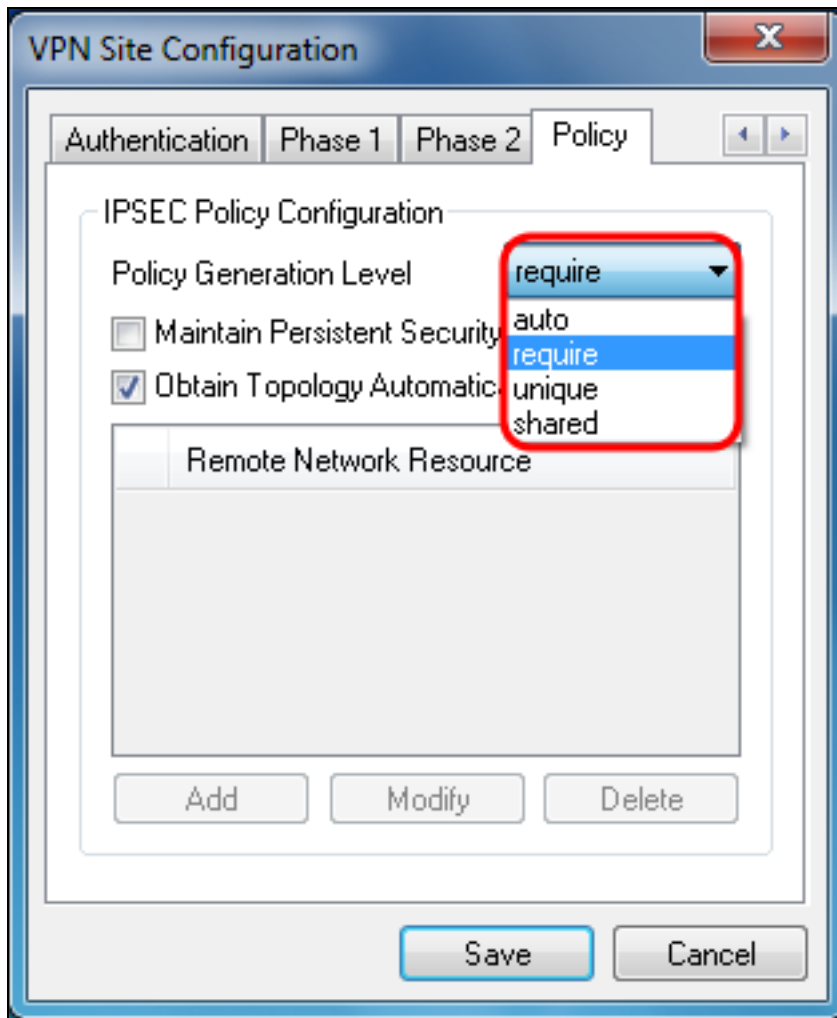
步骤13. 点击 *Phase 2* 选项卡。配置以下参数，使其与本文档的 [IPSec VPN服务器用户配置第2步中](#) 为 RV130/RV130W 配置的设置相同。



Shrew Soft中的参数应匹配第2阶段中的RV130/RV130W配置，如下所示：

- “转换算法”应与“加密算法”匹配。
- “HMAC算法”应与“身份验证算法”匹配。
- PFS Exchange应该与“DH组”匹配（如果在RV130/RV130W上启用了PFS密钥组）。否则，请选择**disabled**。
- “Key Life Time Limit”应与“IPSec SA Lifetime”匹配。

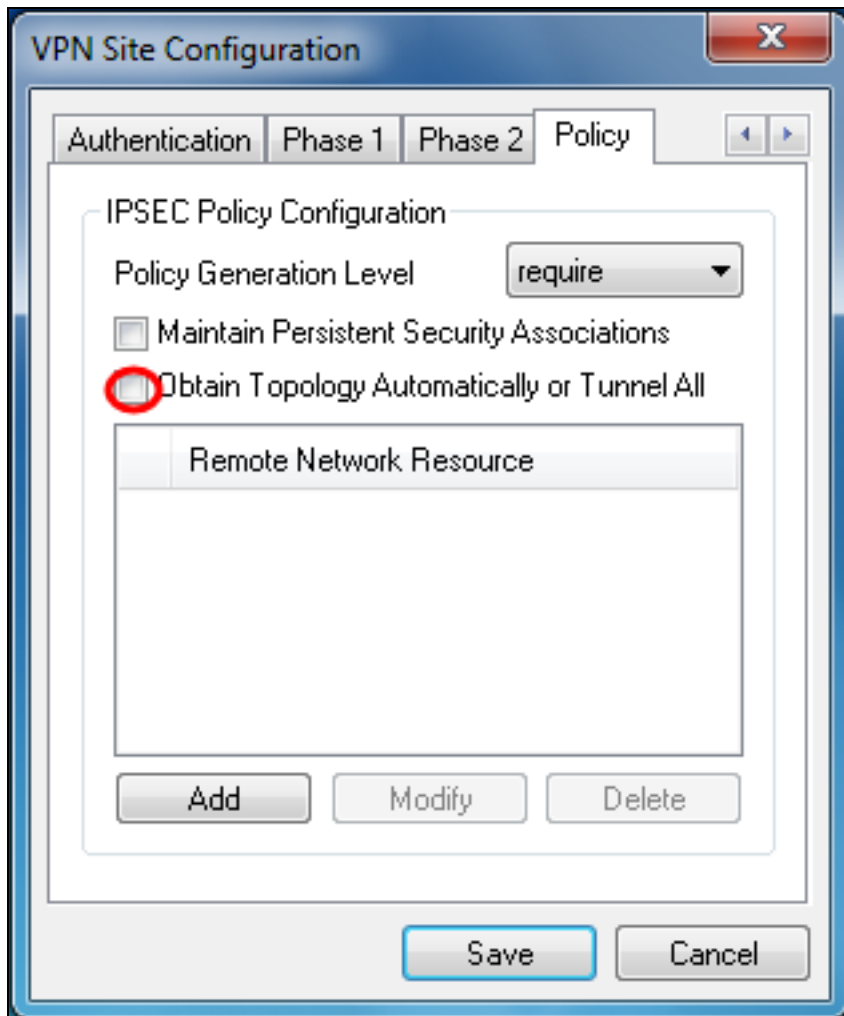
步骤14. 点击 *Policy* 选项卡，并在 **Policy Generation Level** 下拉列表中选择 **require**。 *Policy Generation Level* 选项修改生成IPsec策略的级别。下拉列表中提供的不同级别映射到由不同供应商实施的IPSec SA协商行为。



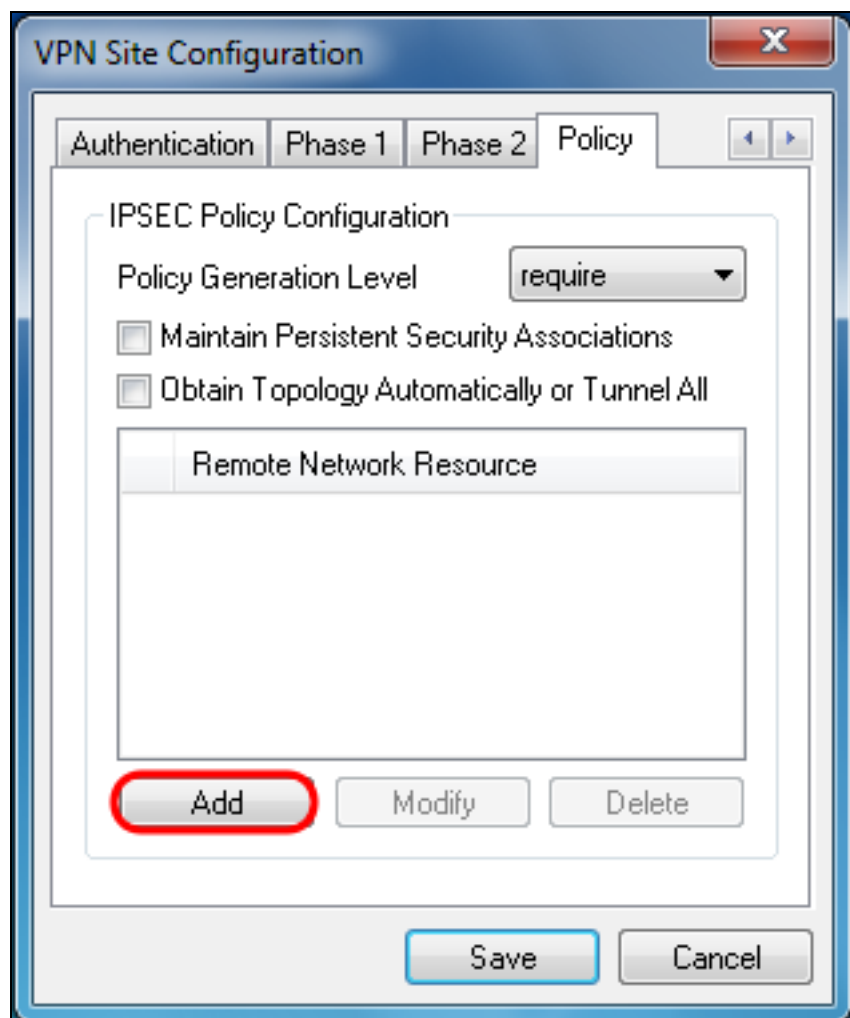
可用选项定义如下：

- Auto — 客户端将自动确定适当的IPSec策略级别。
- 需要 — 客户端不会为每个策略协商唯一的安全关联(SA)。使用本地公有地址作为本地策略ID，使用远程网络资源作为远程策略ID来生成策略。第2阶段建议将在协商期间使用策略ID。
- 唯一 — 客户端将为每个策略协商唯一SA。
- 共享 — 在所需级别生成策略。第2阶段建议将在协商期间使用本地策略ID作为本地ID，使用任意(0.0.0.0/0)作为远程ID。

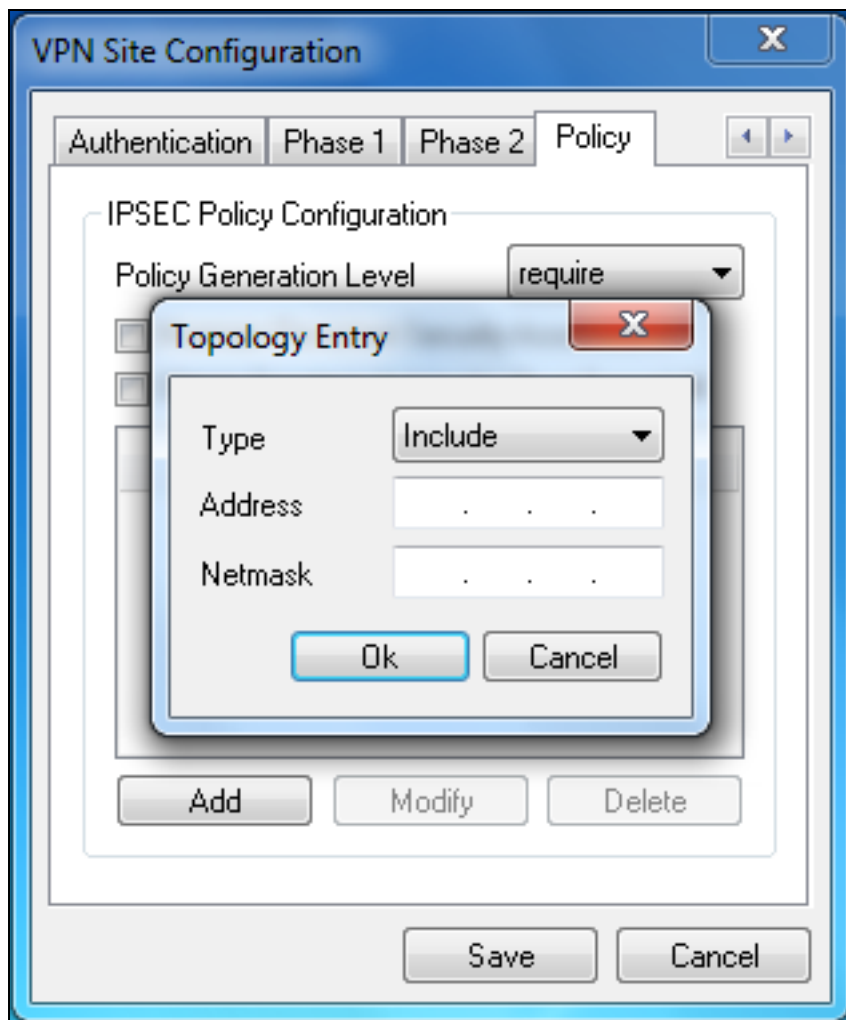
步骤15.取消选中**Obtain Topology Automatically or Tunnel All**复选框。此选项修改为连接配置安全策略的方式。禁用时，必须执行手动配置。启用后，执行自动配置。



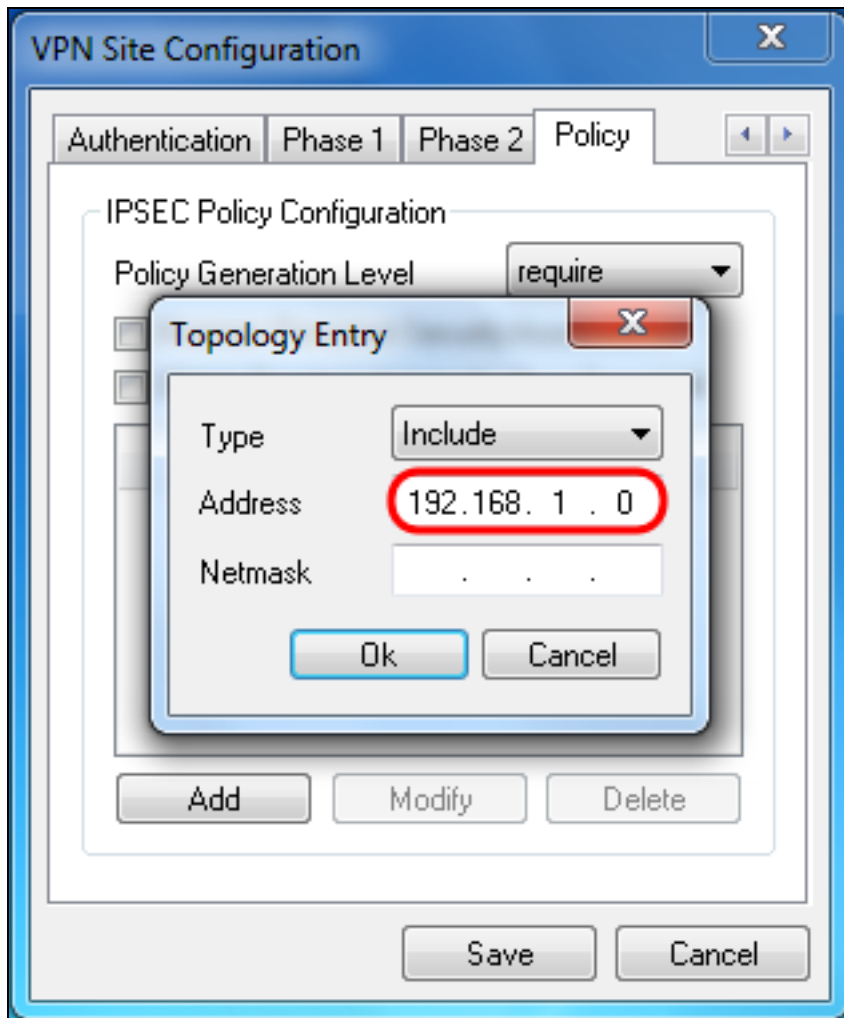
步骤16.单击**Add**以添加要连接的远程网络资源。远程网络资源包括远程桌面访问、部门资源、网络驱动器和安全电子邮件。



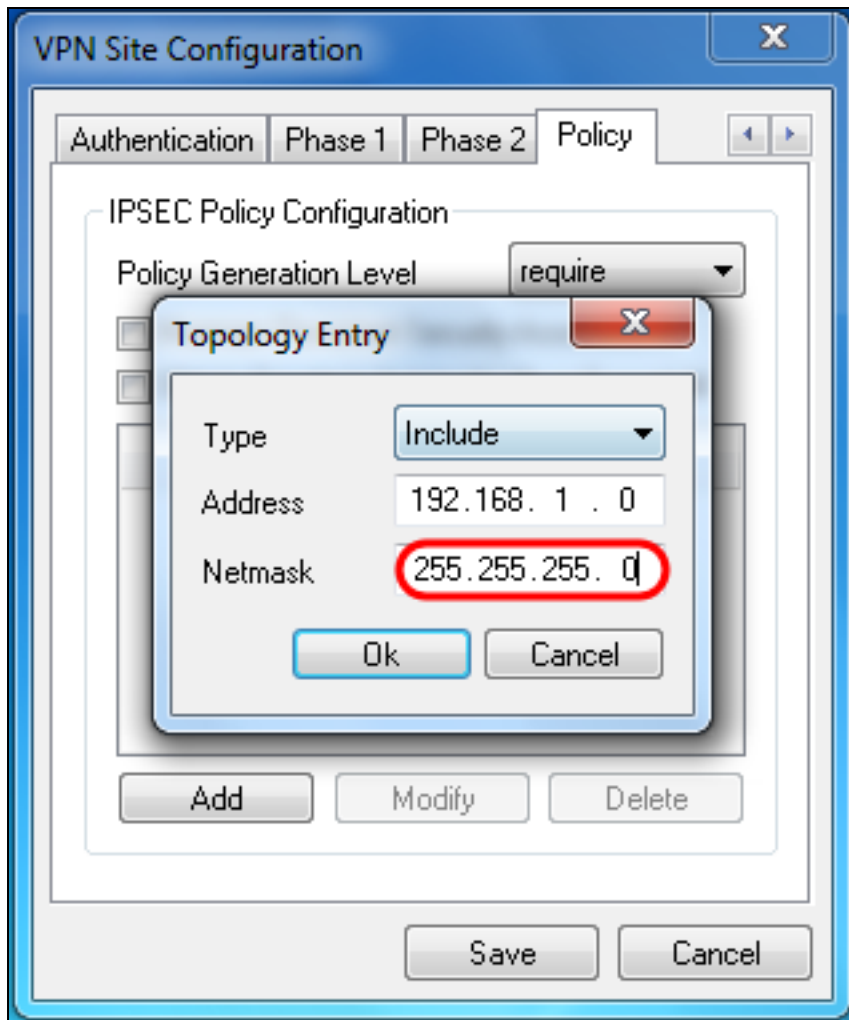
出现 *Topology Entry* 窗口：



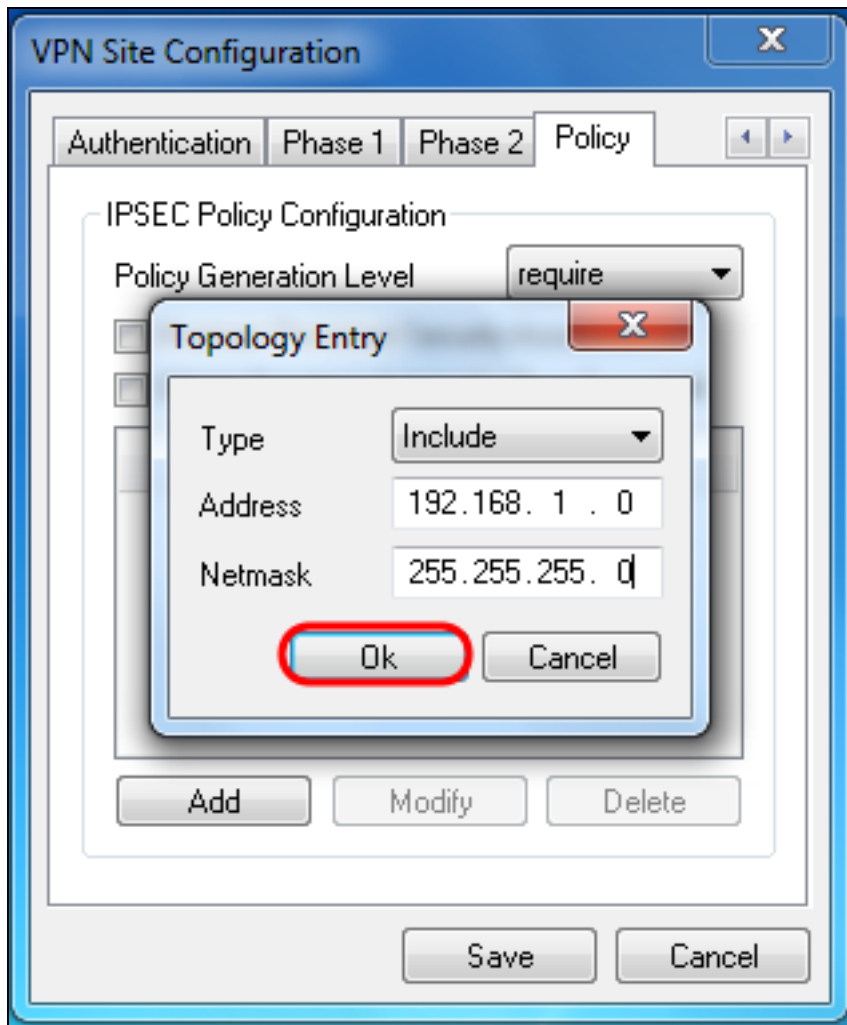
步骤17.在地址字段中，输入RV130/RV130W的子网ID。地址应与本文档的[IPSec VPN服务器设置和用户配置](#)部分的[步骤2](#)中的IP地址字段匹配。



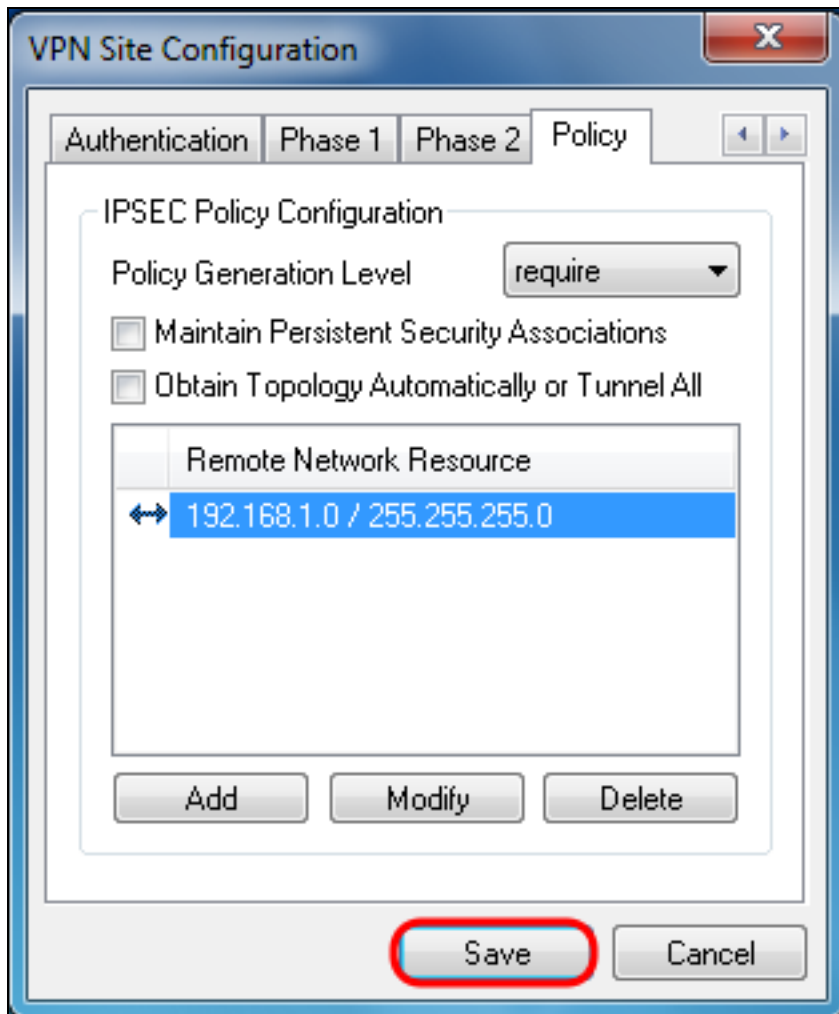
步骤18.在Netmask字段中，输入RV130/RV130W本地网络的子网掩码。网络掩码应与本文档 [IPSec VPN服务器用户配置](#)部分的 [步骤2](#)中的子网掩码字段匹配。



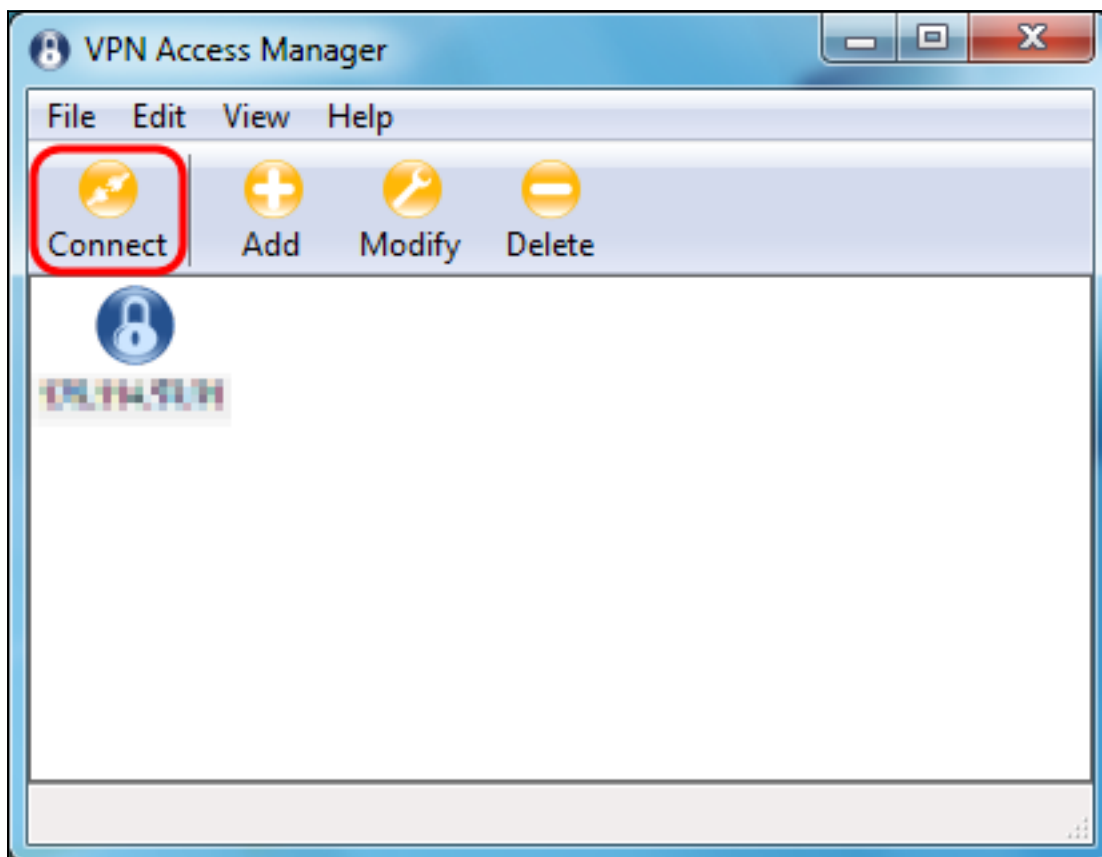
步骤19.单击**确定**完成远程网络资源的添加。



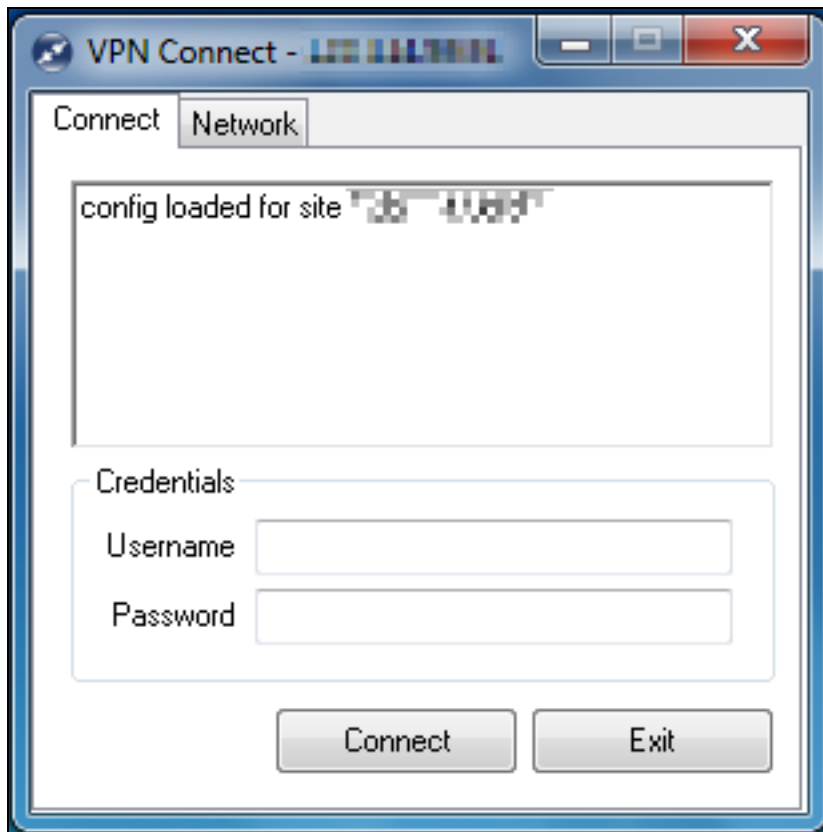
步骤20. 单击**Save**保存要连接到VPN站点的配置。



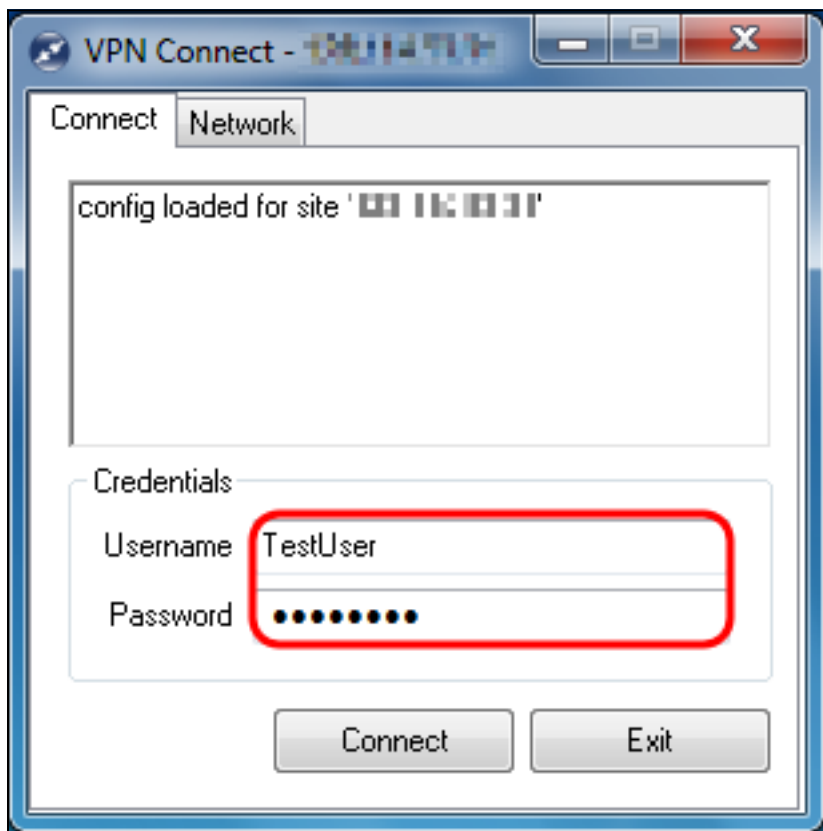
步骤21.返回VPN Access Manager窗口以选择配置的VPN站点，然后单击Connect按钮。



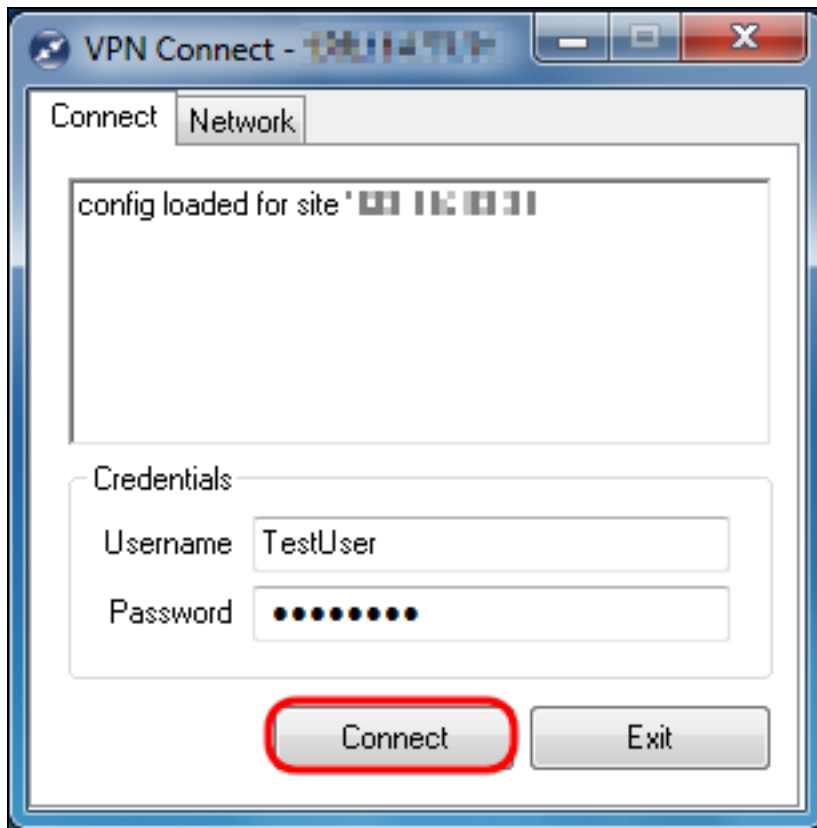
出现VPN Connect窗口。



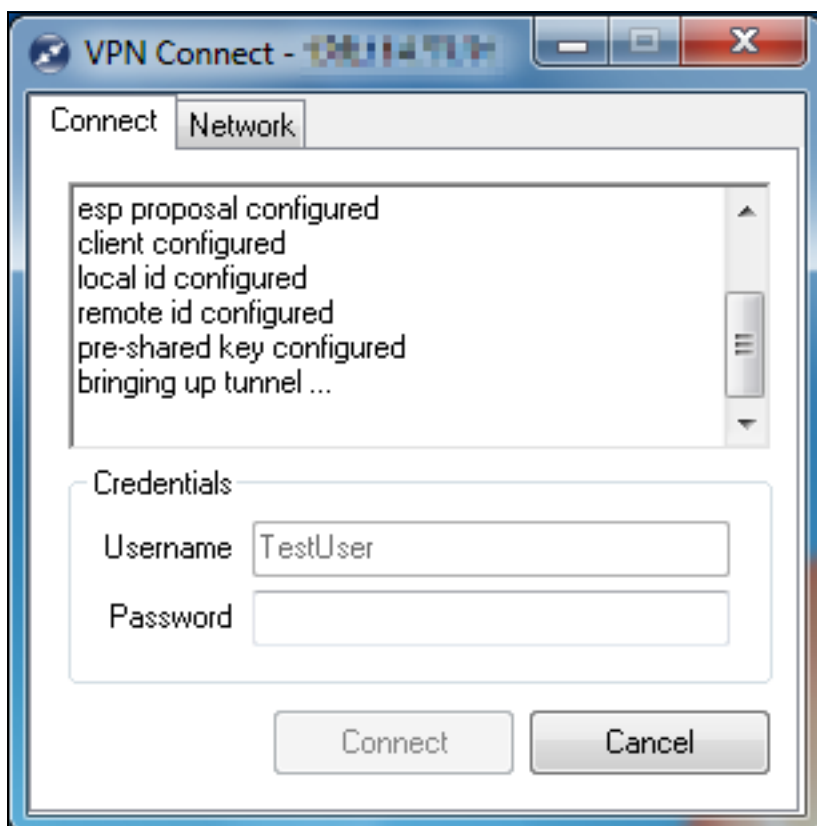
步骤22.在凭证部分，输入您在本文档的[IPSec VPN服务器用户配置](#)部分的[步骤4](#)中设置的帐户的用户名和密码。

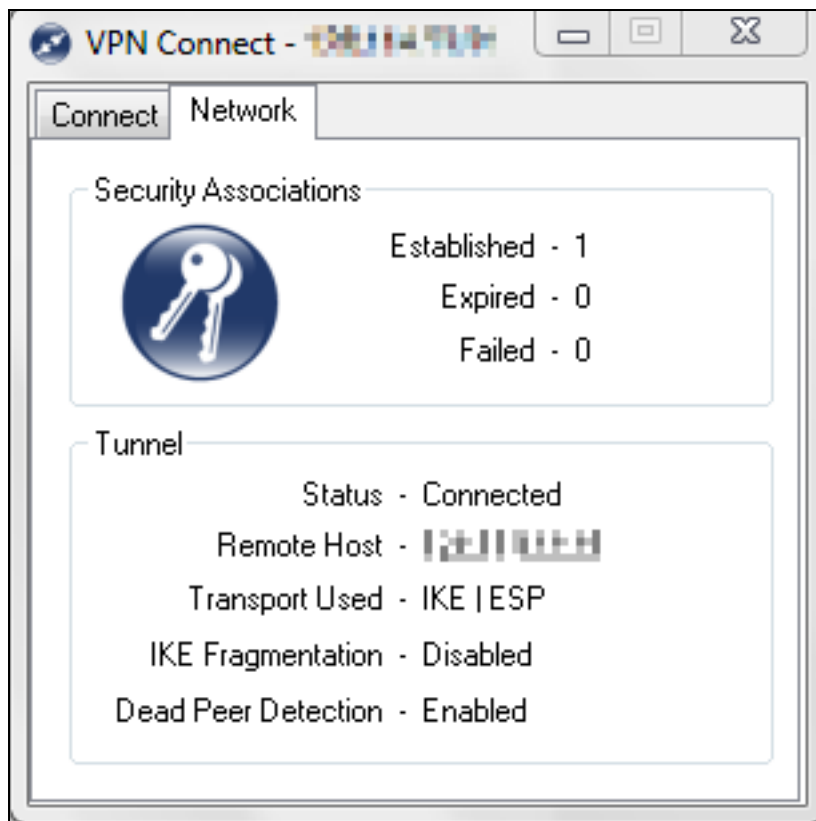


步骤23.单击**Connect** to VPN into the RV130/RV130W。



IPSec VPN隧道已建立，VPN客户端可以访问RV130/RV130W LAN后面的资源。





[查看与本文相关的视频.....](#)

[单击此处查看思科的其他技术对话](#)

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）。