

Shrew Soft VPN Clientを使用したRV130およびRV130W上のIPSec VPNサーバとの接続

目的

IPSec VPN (バーチャルプライベートネットワーク) を使用すると、インターネット上に暗号化されたトンネルを確立して、リモートリソースを安全に取得できます。

RV130およびRV130WはIPSec VPNサーバとして動作し、Shrew Soft VPNクライアントをサポートします。

クライアントソフトウェアの最新リリースをダウンロードしてください。

- ・ Shrew Soft(<https://www.shrew.net/download/vpn>)

注：IPSec VPNサーバを使用してShrew Soft VPN Clientを正常にセットアップおよび設定できるようにするには、まずIPSec VPNサーバを設定する必要があります。この方法の詳細については、『[RV130およびRV130WでのIPSec VPNサーバの設定](#)』を参照してください。

このドキュメントの目的は、Shrew Soft VPN Clientを使用してRV130およびRV130W上のIPSec VPNサーバに接続する方法を示すことです。

該当するデバイス

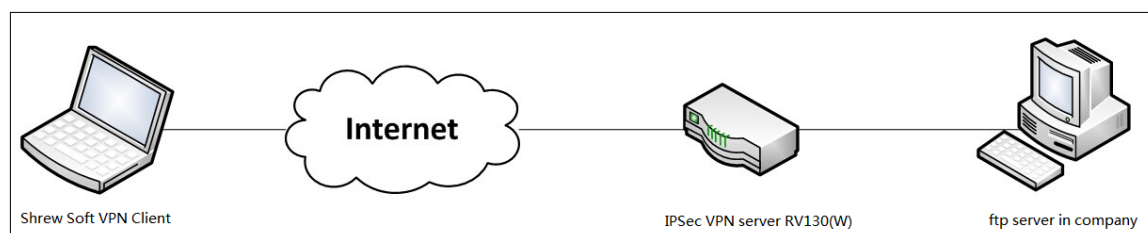
- ・ RV130W Wireless-N VPNファイアウォール
- ・ RV130 VPNファイアウォール

システム要件

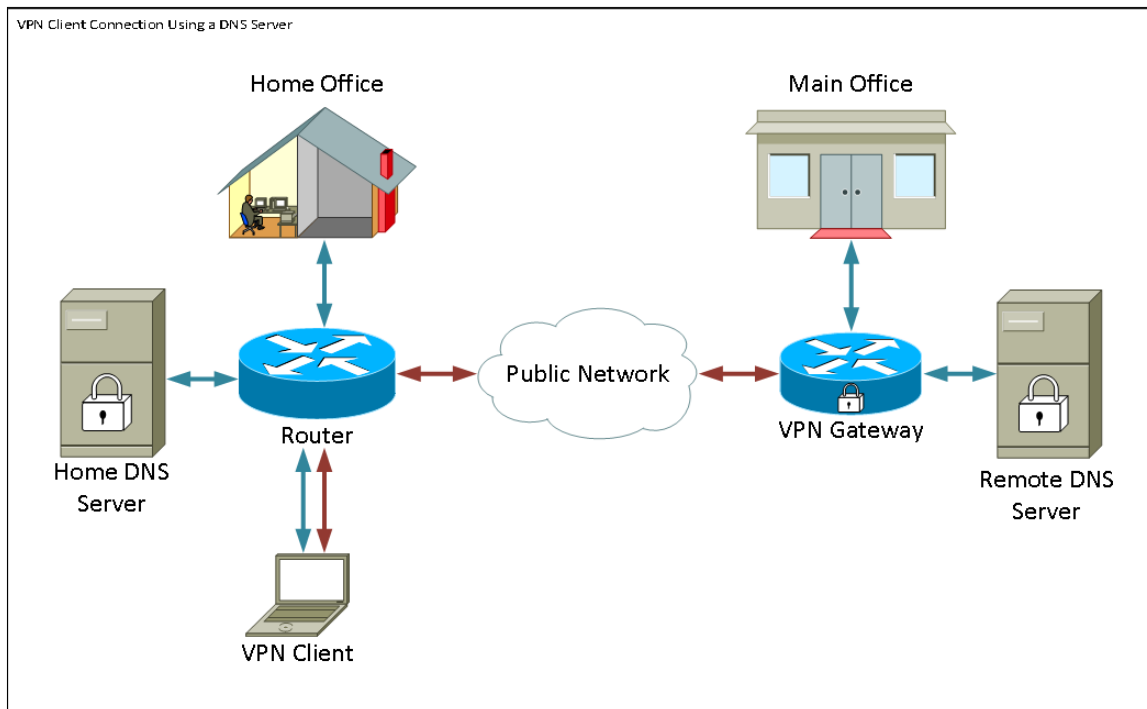
- ・ 32または64ビットシステム
- ・ Windows 2000、XP、VistaまたはWindows 7/8

トポロジ

次に、ShareSoftのクライアントとサイト間の設定に関するデバイスを示すトップレベルトポロジを示します。



小規模企業のネットワーク環境におけるDNSサーバの役割を示すより詳細なフローチャートを次に示します。



[Software Version]

•1.0.1.3

Shrew Soft VPN Clientのセットアップ

IPSec VPNのセットアップとユーザ設定

ステップ1: Web設定ユーティリティにログインし、[VPN] > [IPSec VPN Server] > [Setup] を選択します。[Setup] ページが開きます。

Setup

Server Enable:

NAT Traversal: Disabled

Phase 1 Configuration

Pre-Shared Key: Testkey

Exchange Mode: Main

Encryption Algorithm: DES

Authentication Algorithm: MD5

DH Group: Group1 (768 bit)

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

Phase 2 Configuration

Local IP: Subnet

IP Address: 192.168.1.0 (Hint: 1.2.3.4)

Subnet Mask: 255.255.255.0 (Hint: 255.255.255.0)

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

Encryption Algorithm: DES


Authentication Algorithm: MD5

PFS Key Group: Enable

DH Group: Group 1(768 bit)

[ステップ2](#):RV130のIPSec VPNサーバが正しく設定されていることを確認します。IPSec VPNサーバが設定されていない、または誤って設定されている場合は、『[RV130およびRV130WでのIPSec VPNサーバの設定](#)』を参照し、[Save] をクリックします。

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:

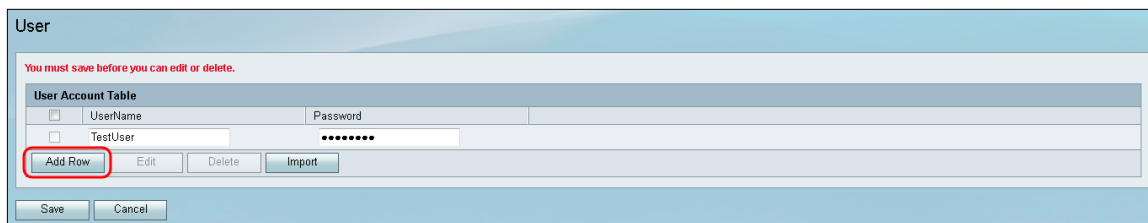
注：上記の設定は、RV130/RV130W IPSec VPNサーバの設定例です。設定は、ドキュメント『[RV130およびRV130WでのIPSec VPNサーバの設定](#)』に基づいており、以降の手順で参照します。

ステップ3:[VPN] > [IPSec VPN Server] > [User] に移動します。[User] ページが表示されます。

User

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

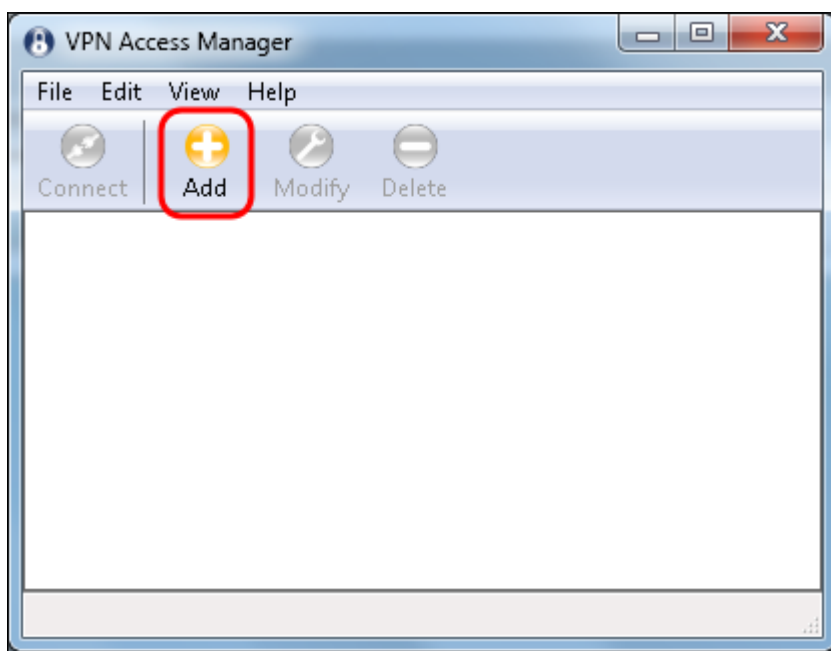
ステップ4:[Add Row] をクリックしてユーザアカウントを追加し、VPNクライアントの認証（拡張認証）に使用して、表示されるフィールドに必要なユーザ名とパスワードを入力します。



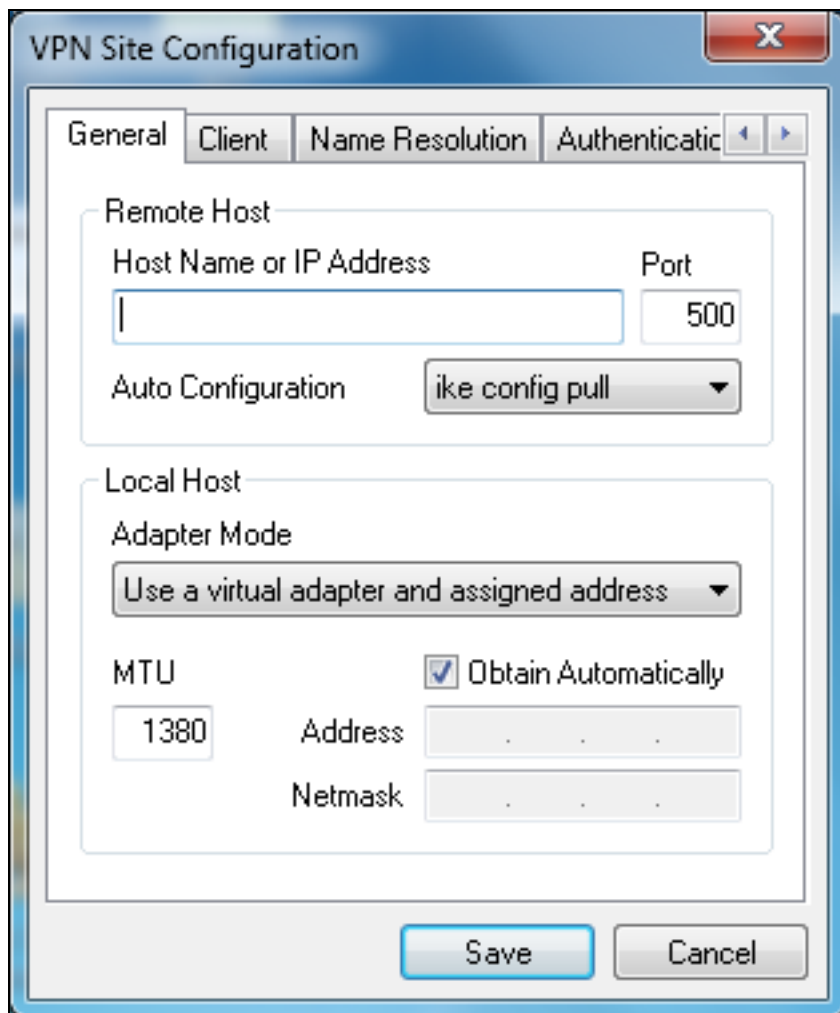
ステップ5:[Save] をクリックして設定を保存します。

VPN Client の設定

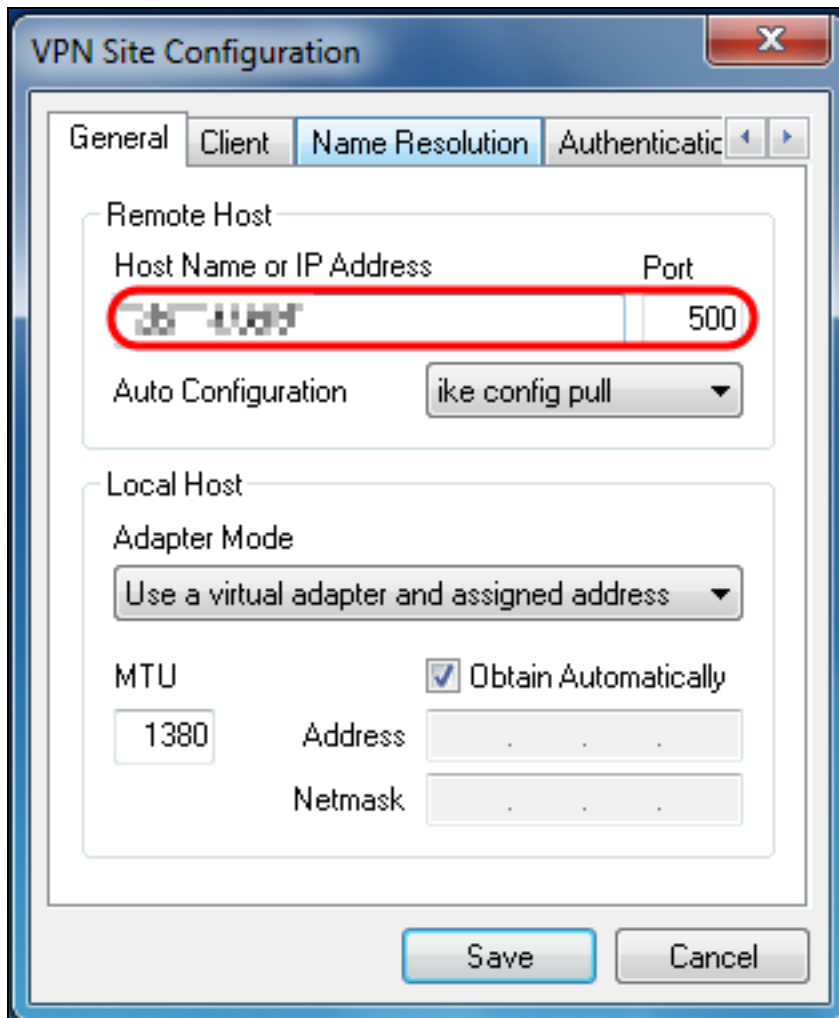
ステップ1:Share VPN Access Managerを開き、[Add] をクリックしてプロファイルを追加します。



[VPN Site Configuration] ウィンドウが表示されます。

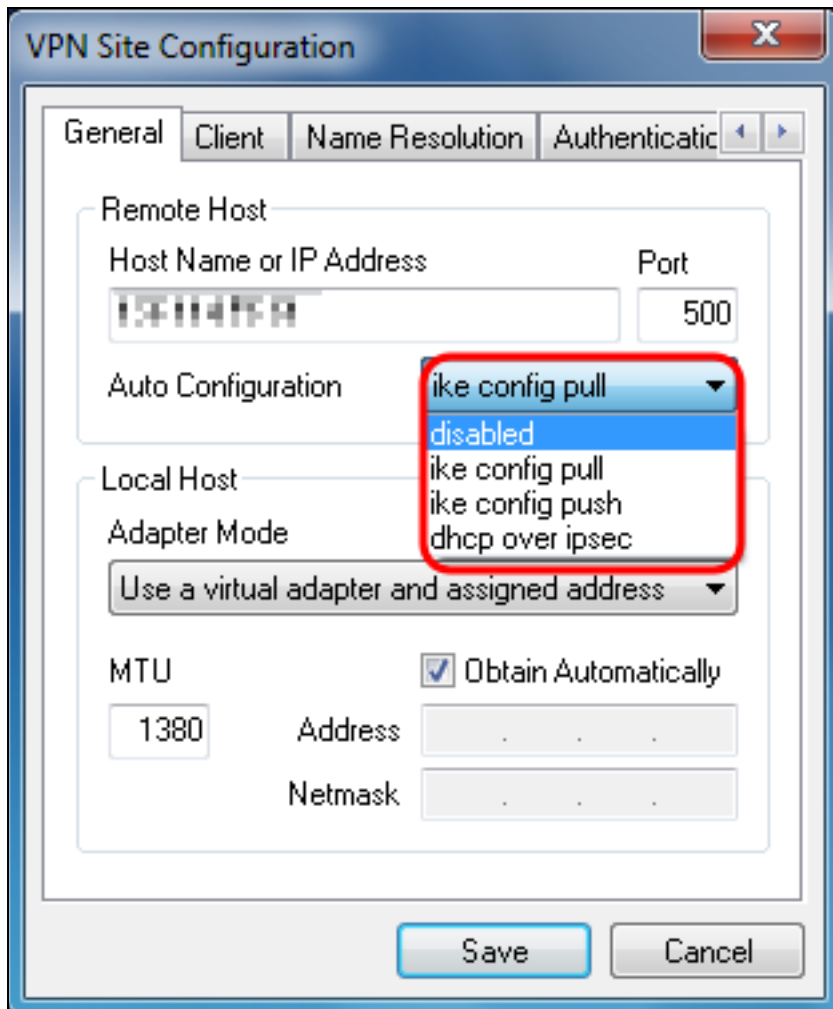


ステップ2:[General] タブの[Remote Host] セクションで、接続するネットワークのパブリックホスト名またはIPアドレスを入力します。



注：ポート番号がデフォルト値の500に設定されていることを確認します。VPNが機能するには、トンネルはUDPポート500を使用します。このポートは、ISAKMPトラフィックがファイアウォールで転送されるように設定する必要があります。

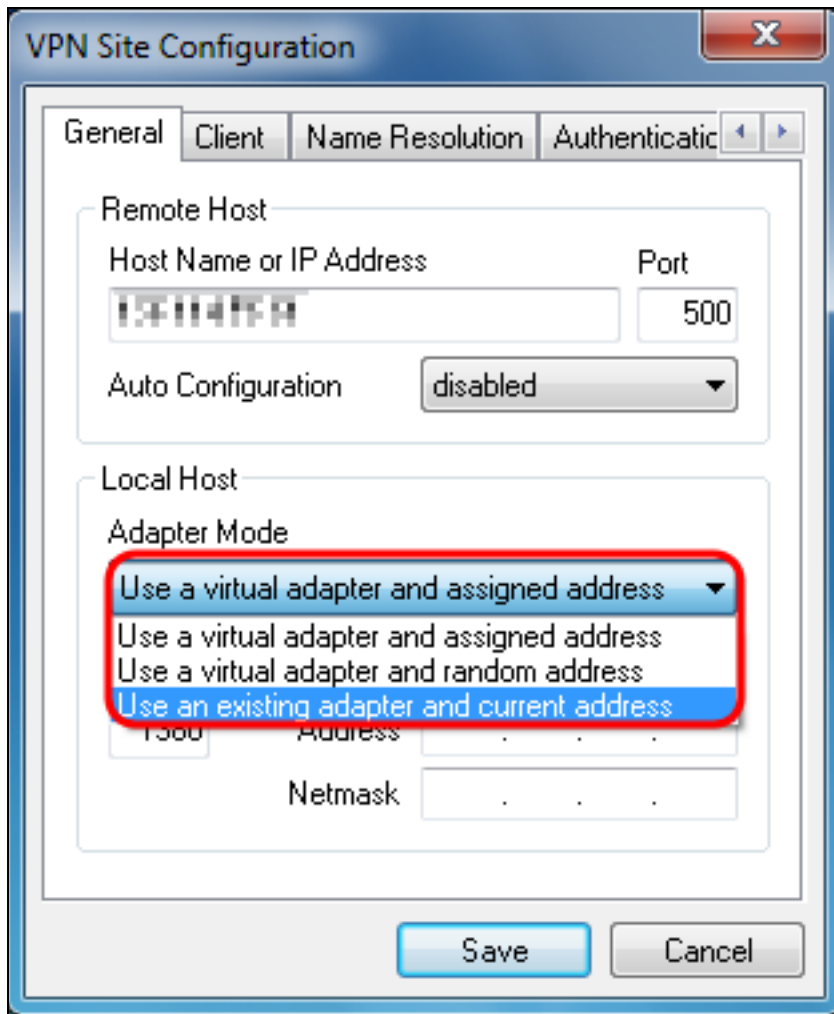
ステップ3:[Auto Configuration] ドロップダウンリストで、[disabled] を選択します。



使用可能なオプションは次のように定義されています。

- ・ Disabled : 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がサポートす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がサポートする設定のリストを返します。
- ・ DHCP Over IPsec : クライアントがDHCP over IPsecを使用してコンピュータに設定を要求できるようにします。

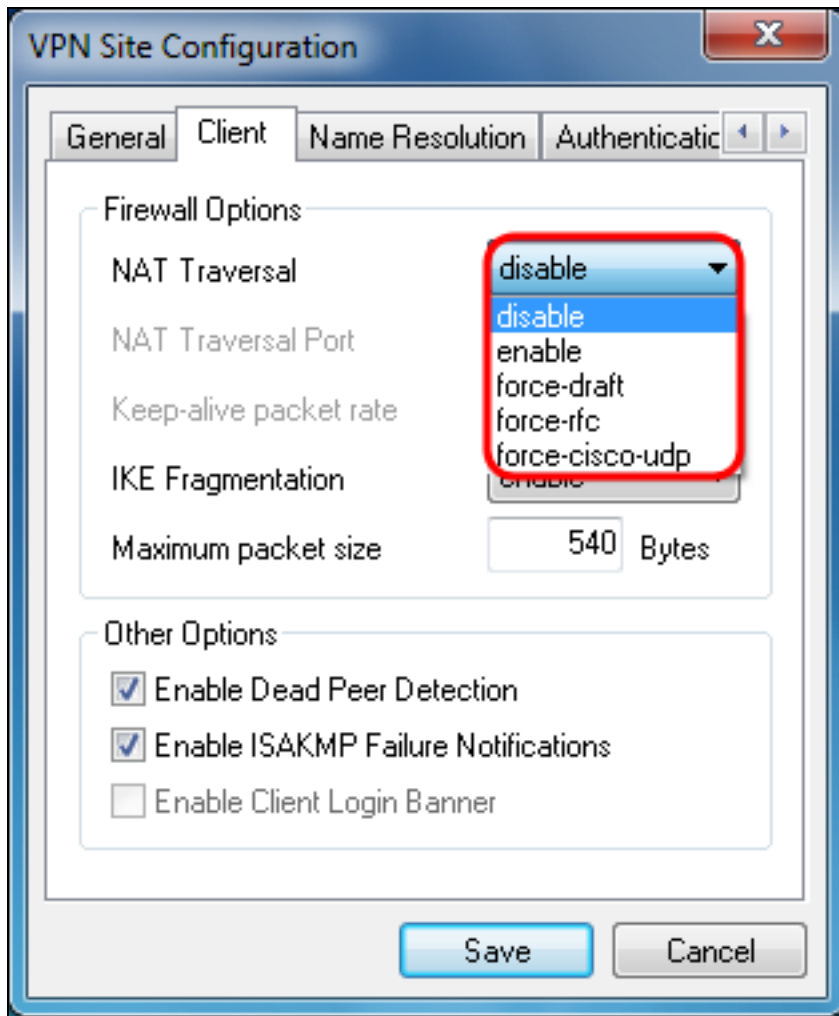
ステップ4:[Local Host] セクションで、[Adapter Mode] ドロップダウンリストから[Use an existing adapter and current address] を選択します。



使用可能なオプションは次のように定義されています。

- ・ 仮想アダプタと割り当てられたアドレスを使用する：クライアントが、指定されたアドレスをIPsec通信の送信元とする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、ランダムアドレスを持つ仮想アダプタをIPsec通信の送信元として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する：現在のアドレスをIPsec通信の送信元とする既存の物理アダプタのみをクライアントが使用できるようにします。

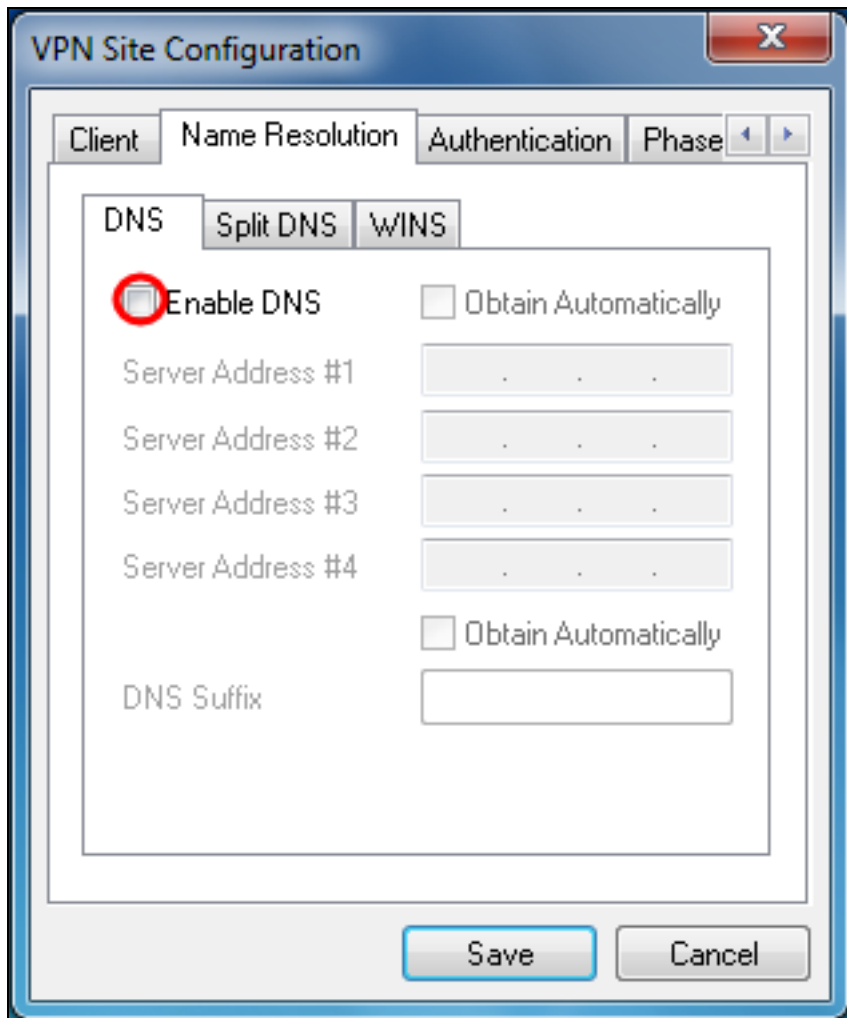
ステップ5:[Client] タブをクリックします。[NAT Traversal] ドロップダウンリストで、『[RV130およびRV130WでのIPSec VPNサーバの設定](#)』のNATトラバーサル用にRV130/RV130Wで設定したものと同一設定を選択します。



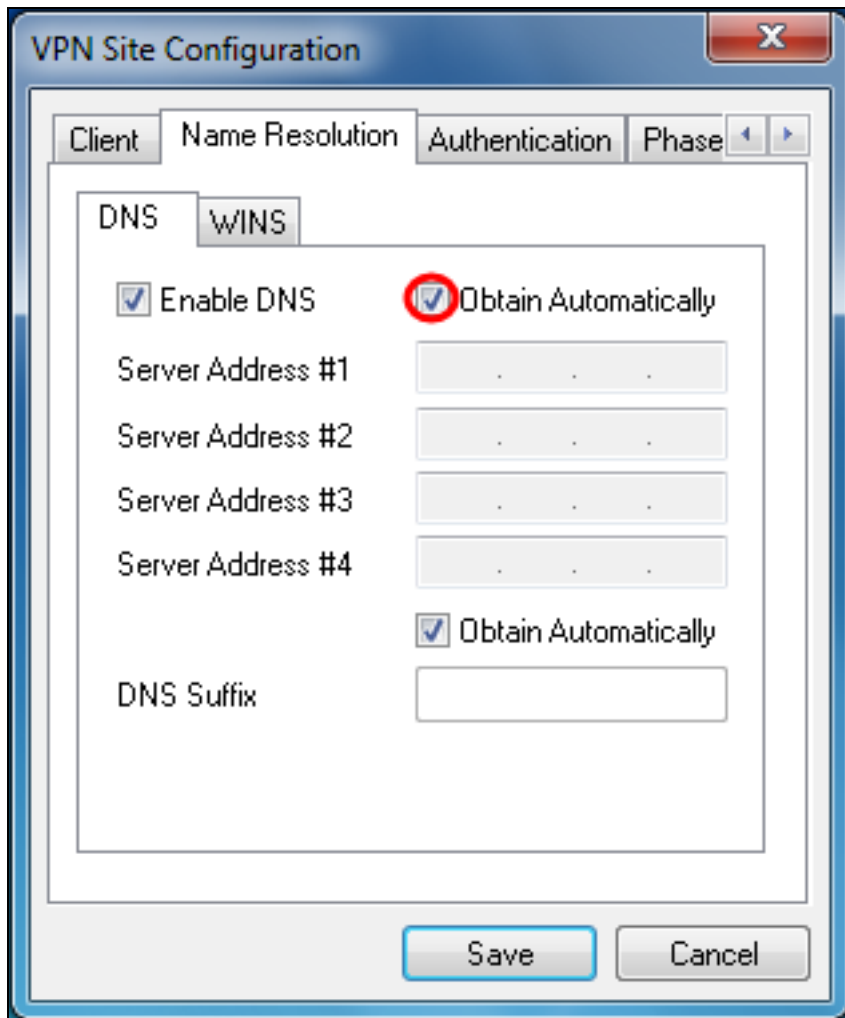
使用可能なNetwork Address Translation Traversal(NATT)メニューオプションは、次のように定義されています。

- ・ Disable:NATプロトコル拡張は使用されません。
- ・ Enable:NATプロトコル拡張は、ネゴシエーション中にVPNゲートウェイがサポートを示し、NATが検出された場合にのみ使用されます。
- ・ Force-Draft:VPNゲートウェイがネゴシエーション中にサポートを示すか、NATが検出されるかにかかわらず、NATプロトコル拡張のドラフトバージョンが使用されます。
- ・ Force-RFC:NATプロトコルのRFCバージョンは、VPNゲートウェイがネゴシエーション中のサポートを示すか、NATが検出されるかにかかわらず使用されます。
- ・ Force-Cisco-UDP:NATを使用しないVPNクライアントのUDPカプセル化を強制します。

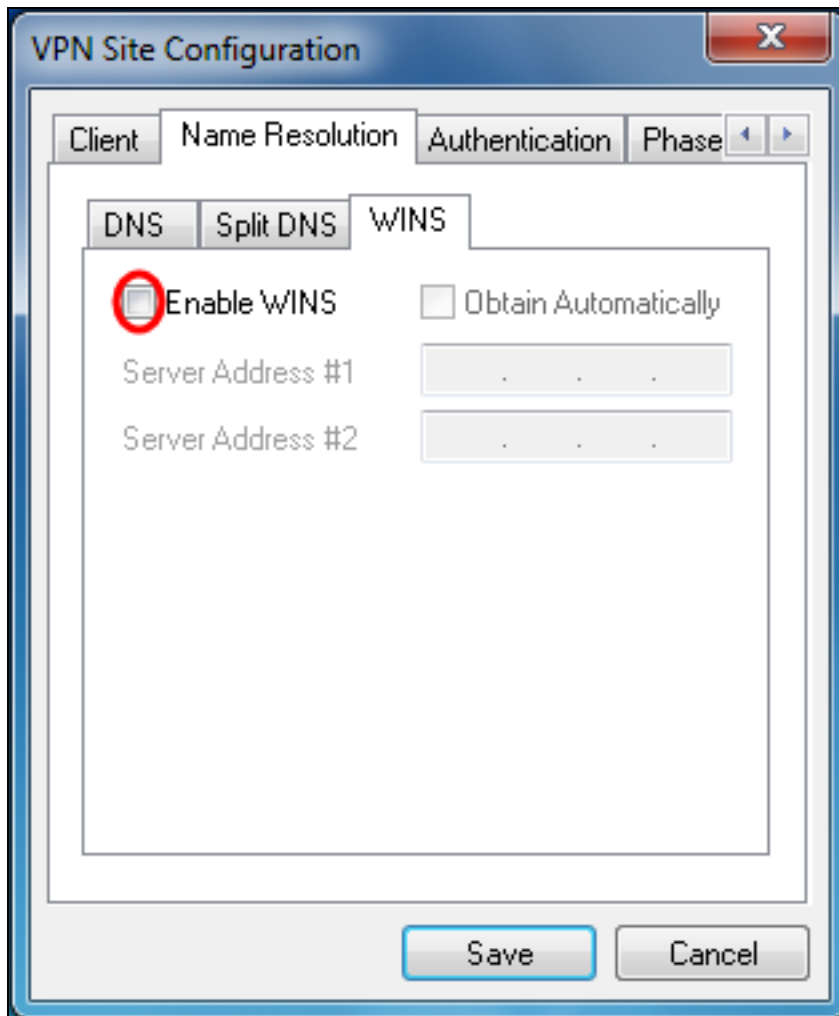
ステップ6:DNSを有効にする場合は、[Name Resolution] タブをクリックし、[Enable DNS] チェックボックスをオンにします。サイト設定に特定のDNS設定が必要ない場合は、[Enable DNS] チェックボックスをオフにします。



ステップ7 (オプション) リモートゲートウェイがConfiguration Exchangeをサポートするように設定されている場合、ゲートウェイは自動的にDNS設定を提供できます。そうでない場合は、[Obtain Automatically] チェックボックスがオフになっていることを確認し、有効なDNSサーバアドレスを手動で入力します。

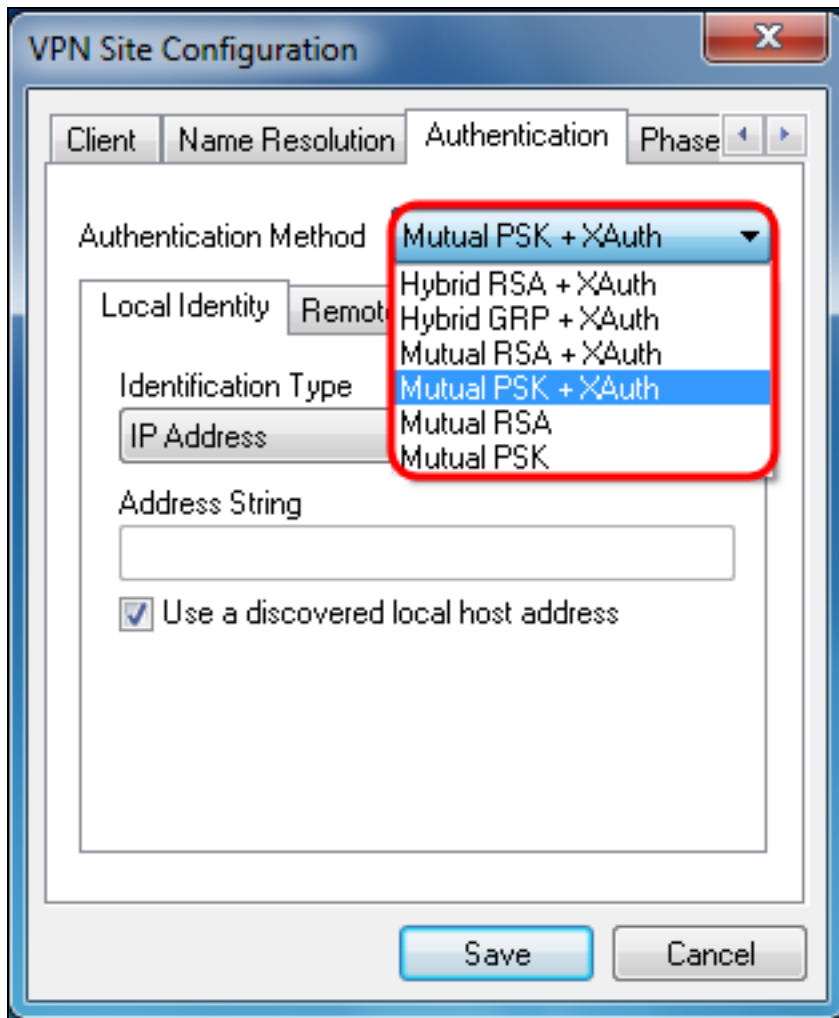


ステップ8: (オプション) Windows Internet Name Server(WINS)を有効にするには、[Name Resolution] タブをクリックし、[Enable WINS] チェックボックスをオンにします。Configuration Exchangeをサポートするようにリモートゲートウェイが構成されている場合、ゲートウェイは自動的にWINS設定を提供できます。そうでない場合は、[Obtain Automatically] チェックボックスがオフになっていることを確認し、有効なWINSサーバアドレスを手動で入力します。



注：WINS構成情報を提供することにより、クライアントはリモートプライベートネットワークにあるサーバを使用してWINS名を解決できます。これは、Uniform Naming Conventionのパス名を使用してリモートWindowsネットワークリソースにアクセスしようとする場合に便利です。WINSサーバは通常、WindowsドメインコントローラまたはSambaサーバに属します。

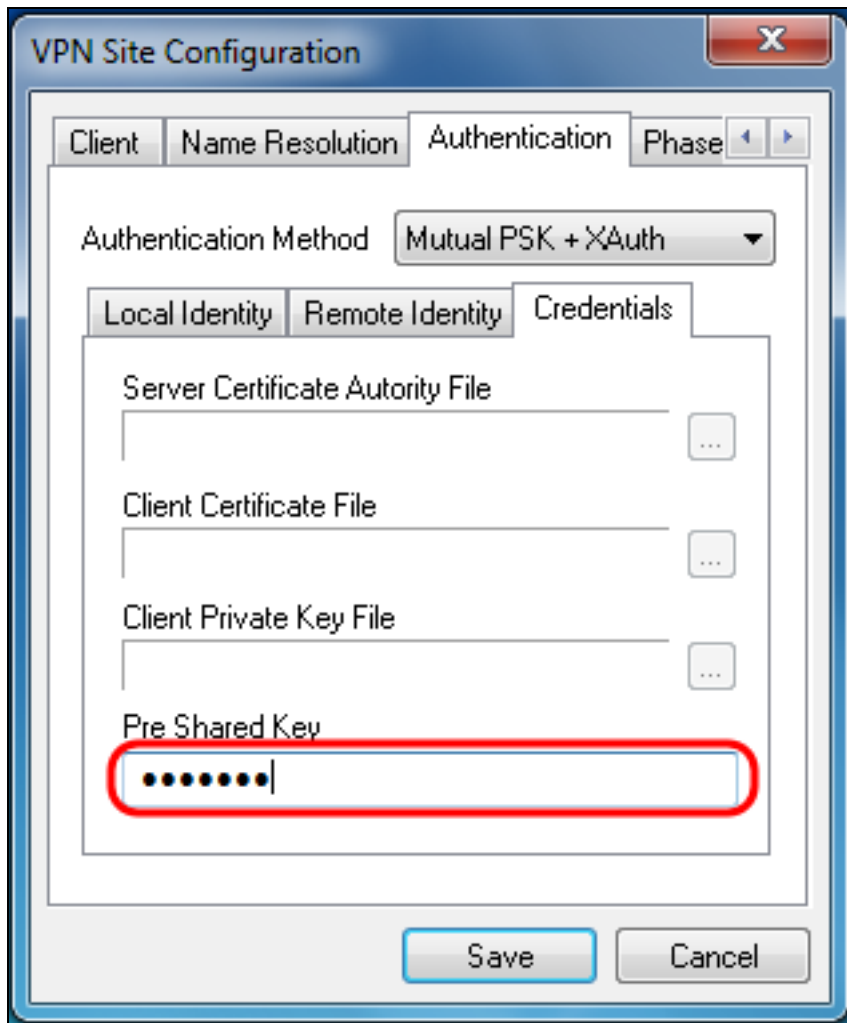
ステップ9:[Authentication] タブをクリックし、[Authentication Method] ドロップダウンリストで[Mutual PSK + XAuth] を選択します。



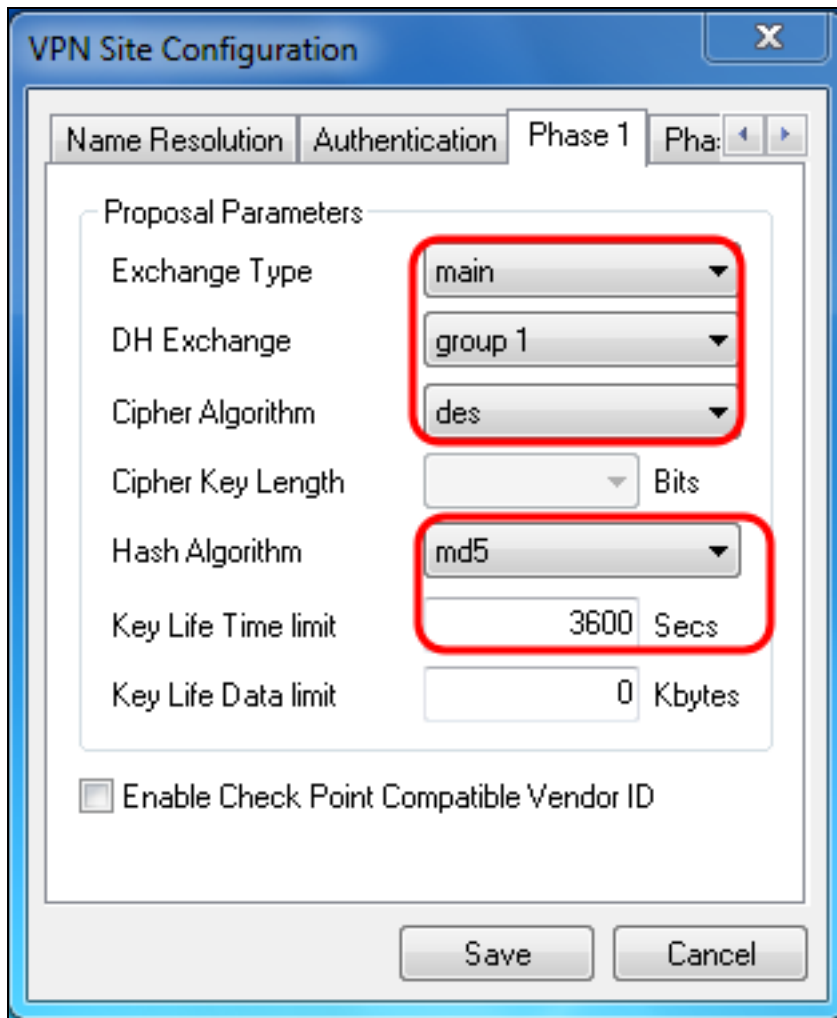
使用可能なオプションは次のように定義されています。

- ・ RSAとXAuthのハイブリッド：クライアント・クレデンシャルは不要です。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証明書ファイルまたはキーファイルタイプの形式になります。
- ・ Hybrid 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ストリングの形式になります。
- ・ 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する。クレデンシャルは、共有秘密ストリングの形式になります。
- ・ 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のためにクレデンシャルを必要とします。クレデンシャルは、共有秘密ストリングの形式になります。

ステップ10:[Authentication] セクションで、[Credentials] サブタブをクリックし、[IPsec VPN Server Setup] ページで設定したのと同じ事前共有キーを[Pre Shared Key] フィールドに入力します。



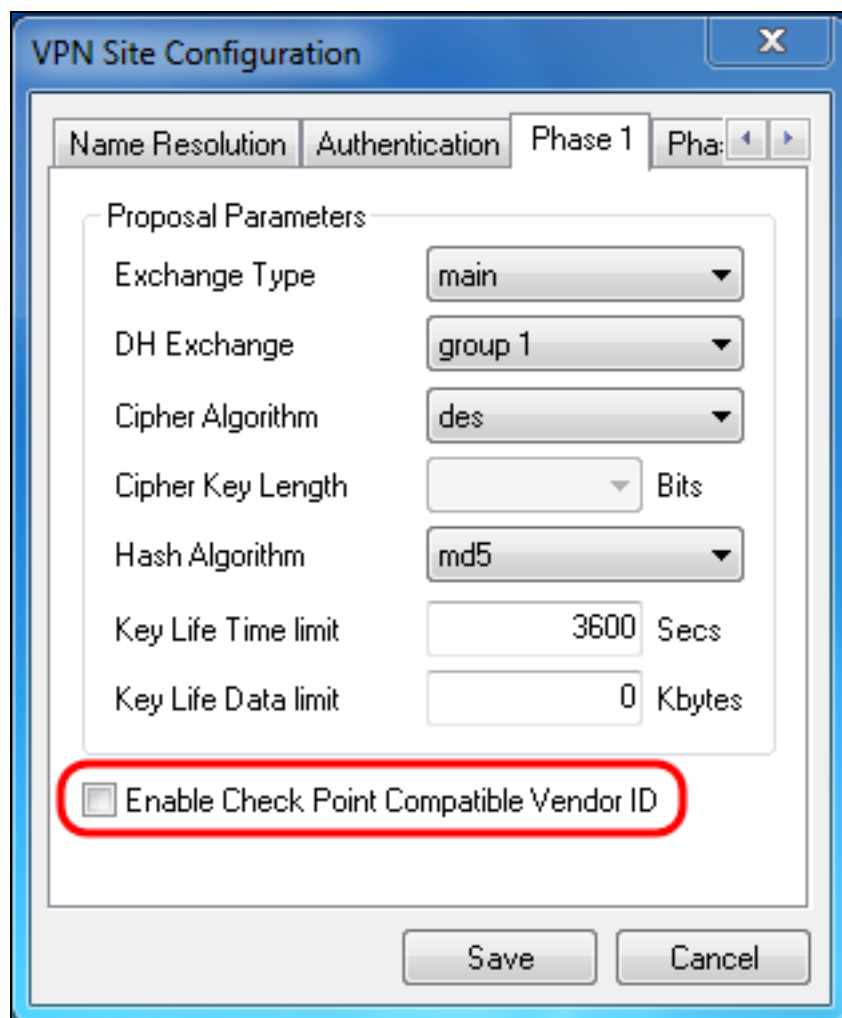
ステップ11:[Phase 1] タブをクリックします。このドキュメントの「[IPSec VPNサーバユーザ設定](#)」セクションの[ステップ2](#)で設定したRV130/RV130Wと同じ設定になるように、次のパラメータを設定します。



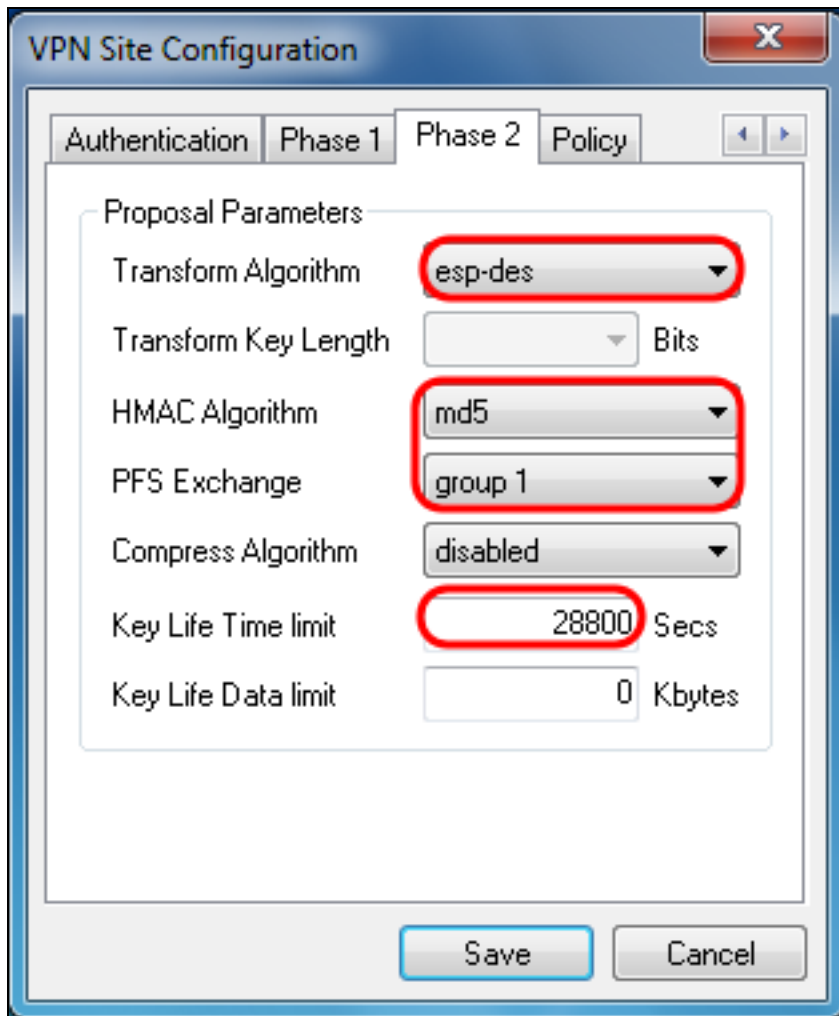
Shrew Softのパラメータは、次のようにフェーズ1のRV130/RV130W設定と一致する必要があります。

- ・ 「Exchange Type」は「Exchange Mode」と一致する必要があります。
- ・ 「DH Exchange」は「DH Group」と一致している必要があります。
- ・ 暗号アルゴリズムは暗号アルゴリズムと一致すること。
- ・ ハッシュアルゴリズムは認証アルゴリズムと一致する必要があります。

ステップ12: (オプション) フェーズ1ネゴシエーション中にゲートウェイがシスコ互換のベンダーIDを提供する場合は、[Enable Check Point Compatible Vendor ID] チェックボックスをオンにします。ゲートウェイが表示されない場合、または不明な場合は、チェックボックスをオフのままにします。



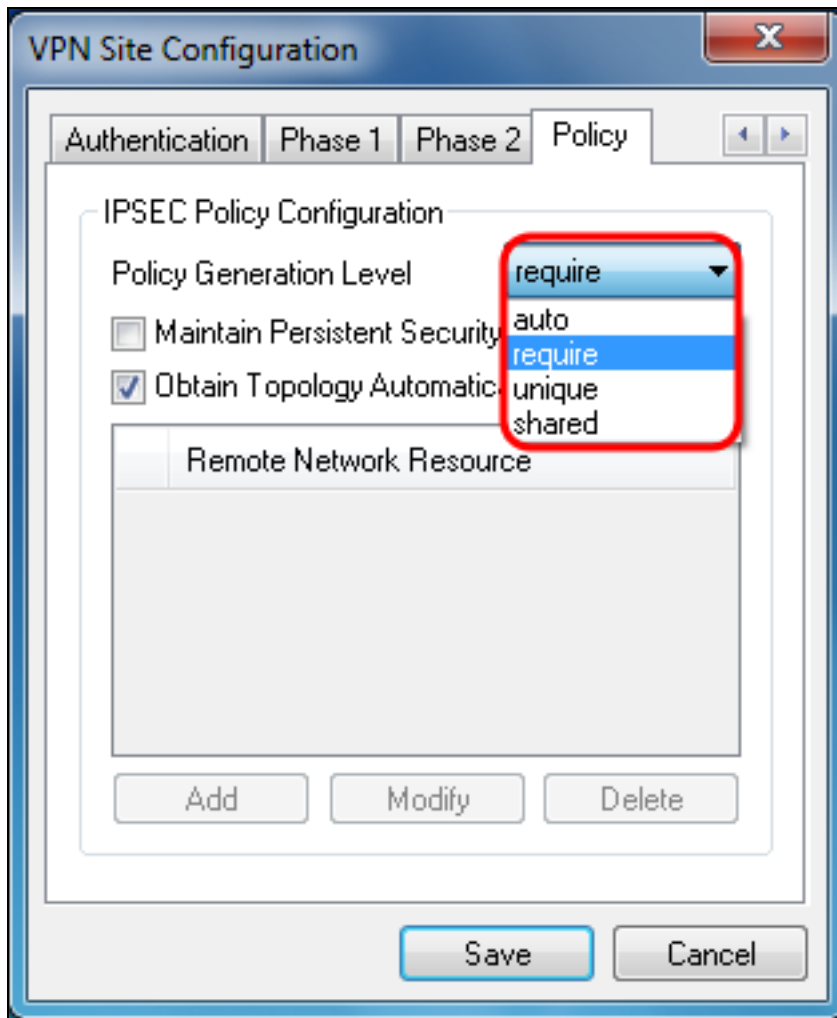
ステップ13:[Phase 2] タブをクリックします。このドキュメントの「[IPSec VPNサーバユーザ設定](#)」セクションの[ステップ2](#)で設定したRV130/RV130Wと同じ設定になるように、次のパラメータを設定します。



Shrew Softのパラメータは、次のようにフェーズ2のRV130/RV130W設定と一致する必要があります。

- ・ 「変換アルゴリズム」は「暗号化アルゴリズム」と一致する必要があります。
- ・ 「HMACアルゴリズム」は「認証アルゴリズム」と一致する必要があります。
- ・ RV130/RV130WでPFSキーグループが有効になっている場合、「PFS Exchange」は「DH Group」と一致する必要があります。そうでない場合は、**disabled**を選択します。
- ・ 「Key Life Time limit」は「IPSec SA Lifetime」と一致する必要があります。

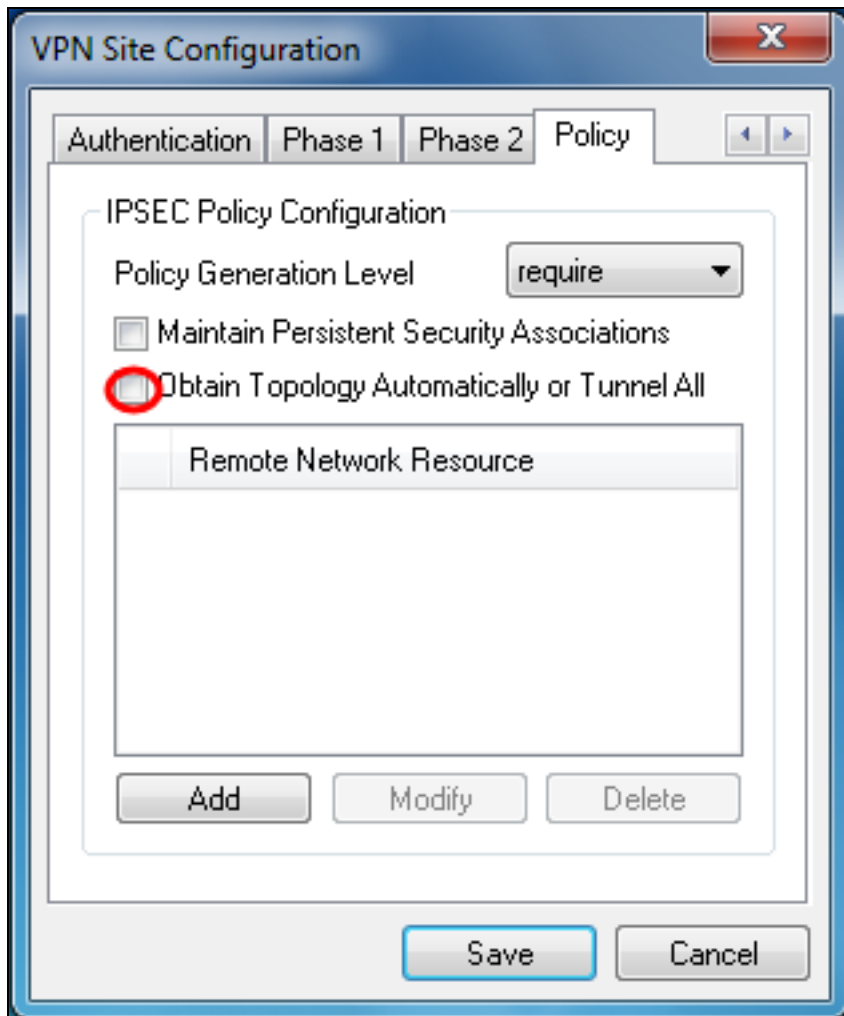
ステップ14:[Policy] タブをクリックし、[Policy Generation Level] ドロップダウンリストで [require] を選択します。[Policy Generation Level] オプションでは、IPSecポリシーが生成されるレベルを変更します。ドロップダウンリストに表示されるさまざまなレベルは、さまざまなベンダーの実装によって実装されるIPSec SAネゴシエーション動作に対応します。



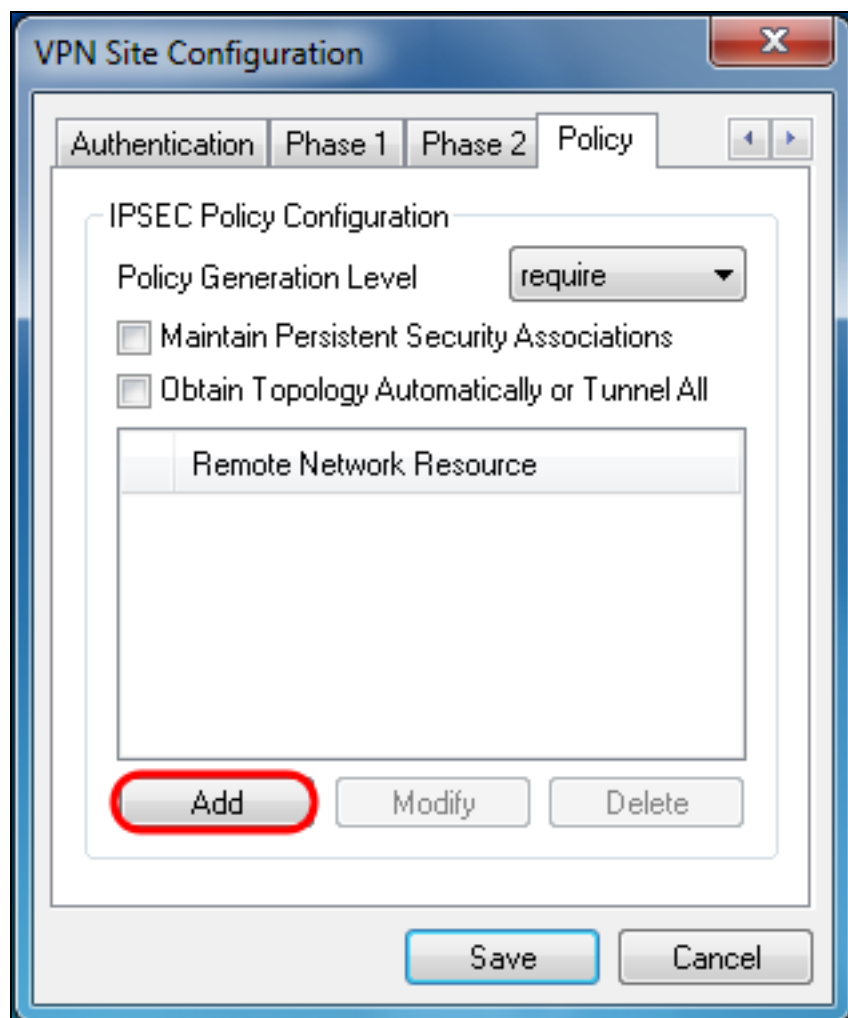
使用可能なオプションは次のように定義されています。

- ・ Auto : クライアントは適切なIPSecポリシーレベルを自動的に決定します。
- ・ Require : クライアントは、ポリシーごとに一意のセキュリティアソシエーション (SA)をネゴシエートしません。ポリシーは、ローカルパブリックアドレスをローカルポリシーIDとして使用し、リモートネットワークリソースをリモートポリシーIDとして使用して生成されます。フェーズ2の提案では、ネゴシエーション中にポリシーIDを使用します。
- ・ Unique : クライアントはポリシーごとに一意のSAをネゴシエートします。
- ・ 共有 : ポリシーは必要なレベルで生成されます。フェーズ2の提案では、ネゴシエーション時に、ローカルポリシーIDをローカルIDとして使用し、Any(0.0.0.0/0)をリモートIDとして使用します。

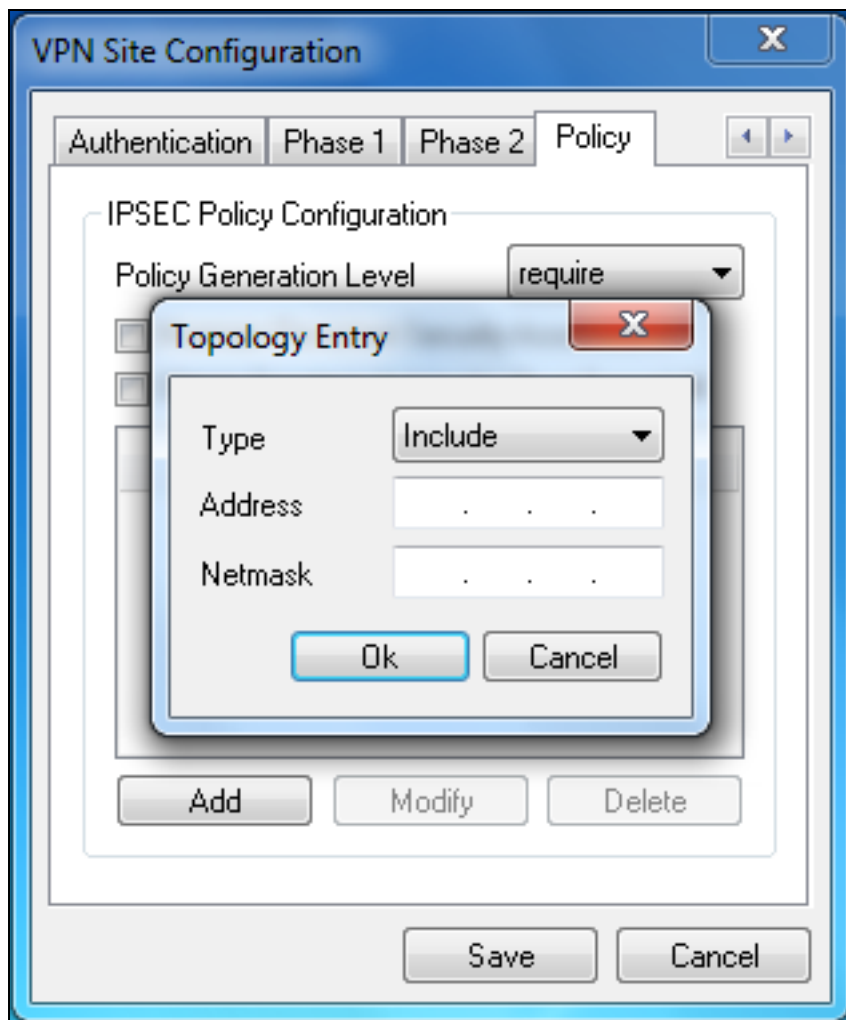
ステップ15:[Obtain Topology Automatically or Tunnel All] チェックボックスをオフにします。このオプションは、接続に対するセキュリティポリシーの設定方法を変更します。無効の場合は、手動設定を実行する必要があります。有効にすると、自動設定が実行されます。



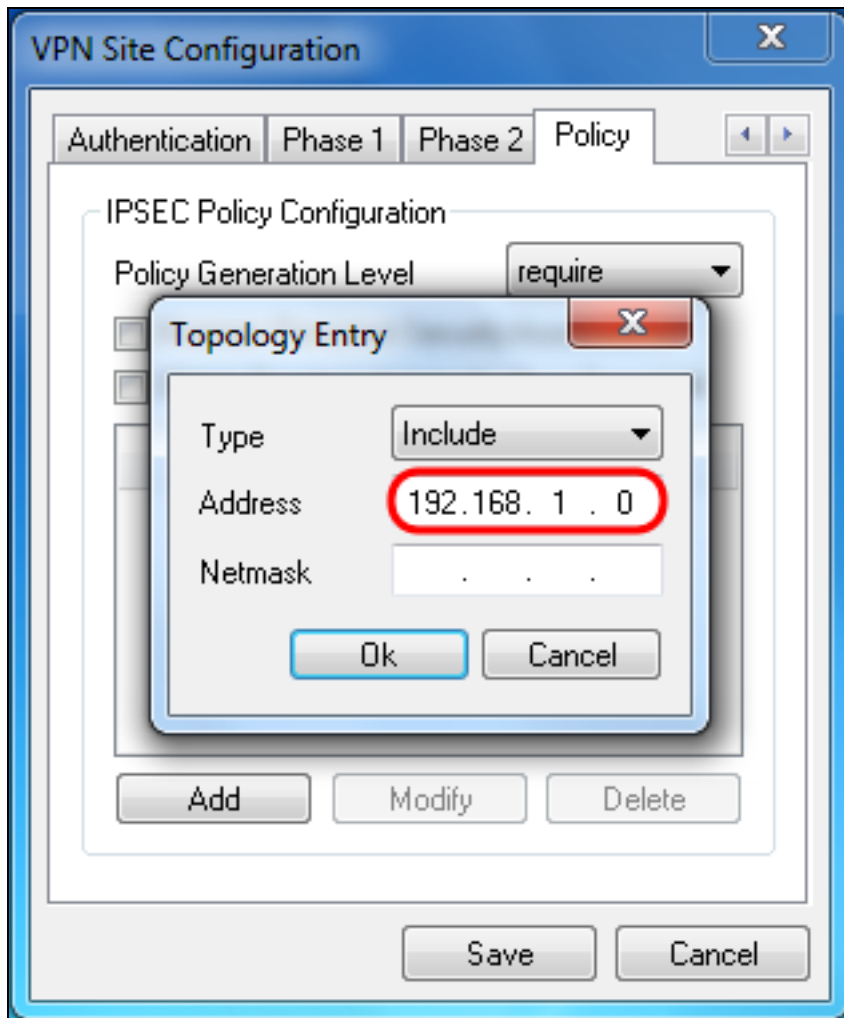
ステップ16:[Add] をクリックして、接続先のリモートネットワークリソースを追加します。リモートネットワークリソースには、リモートデスクトップアクセス、部門リソース、ネットワークドライブ、および安全な電子メールが含まれます。



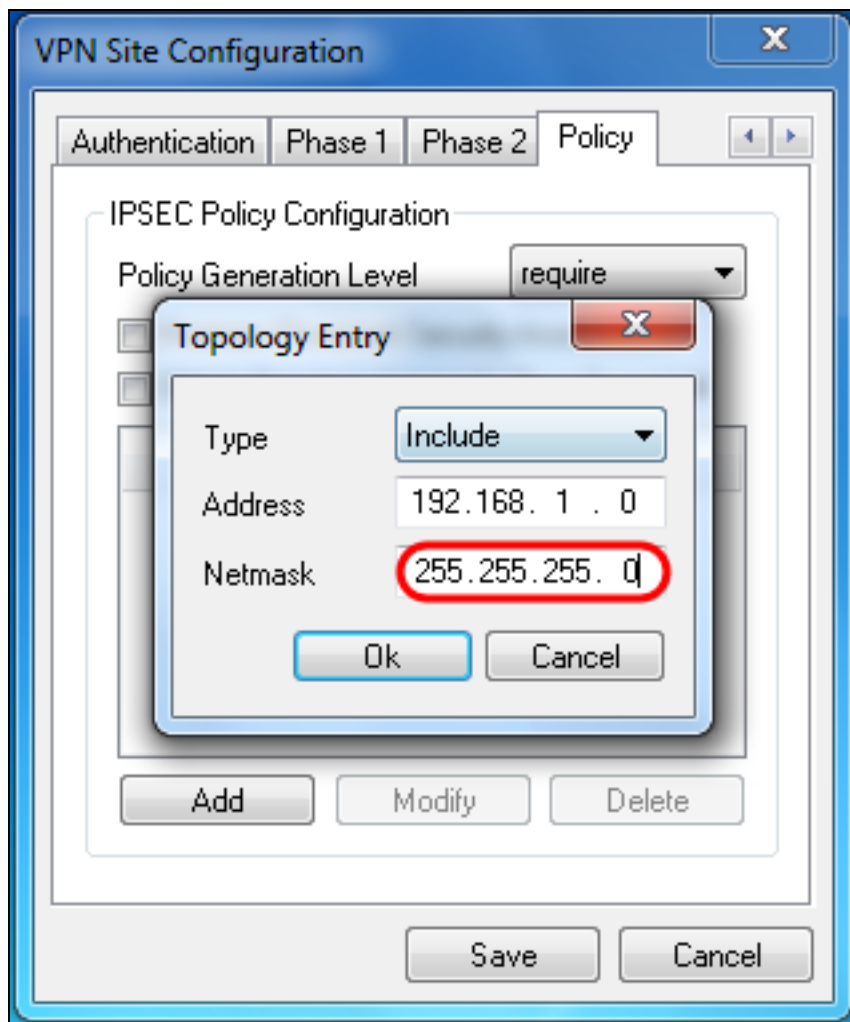
[Topology Entry] ウィンドウが表示されます。



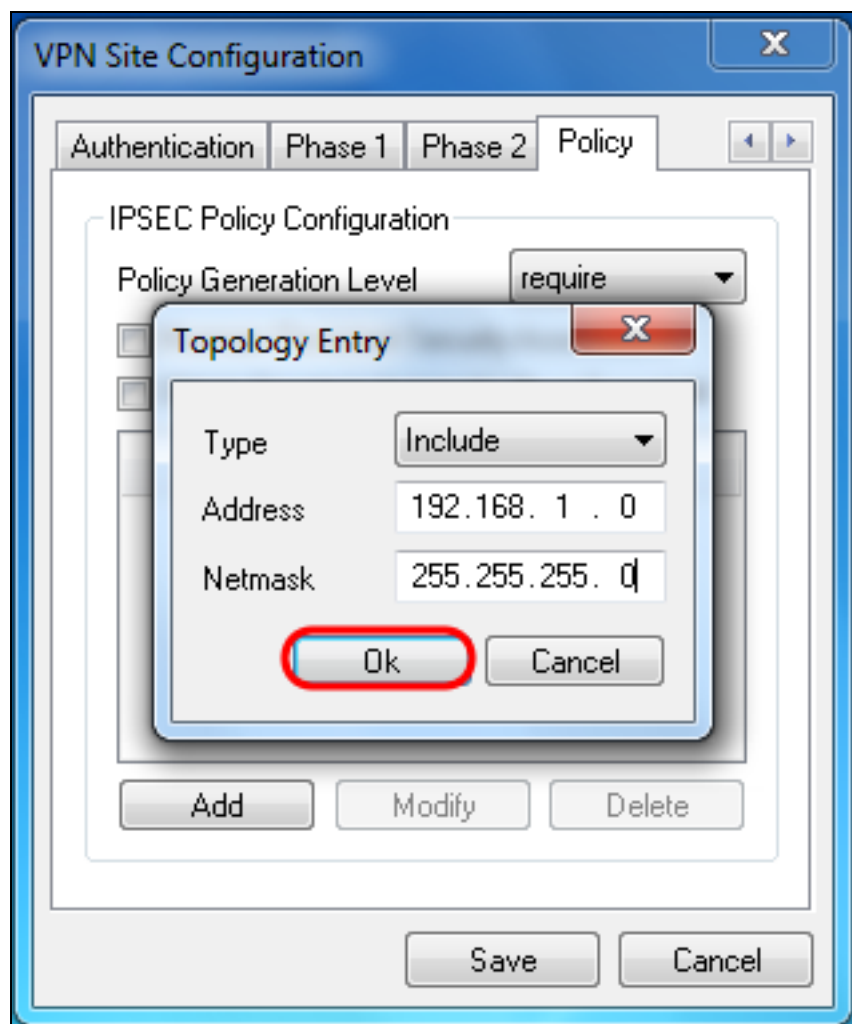
ステップ17:[Address] フィールドに、RV130/RV130WのサブネットIDを入力します。このアドレスは、このドキュメントの「IPSec VPNサーバのセットアップとユーザの設定」セクションの[ステップ2](#)にある「[IPアドレス](#)」フィールドと一致している必要があります。



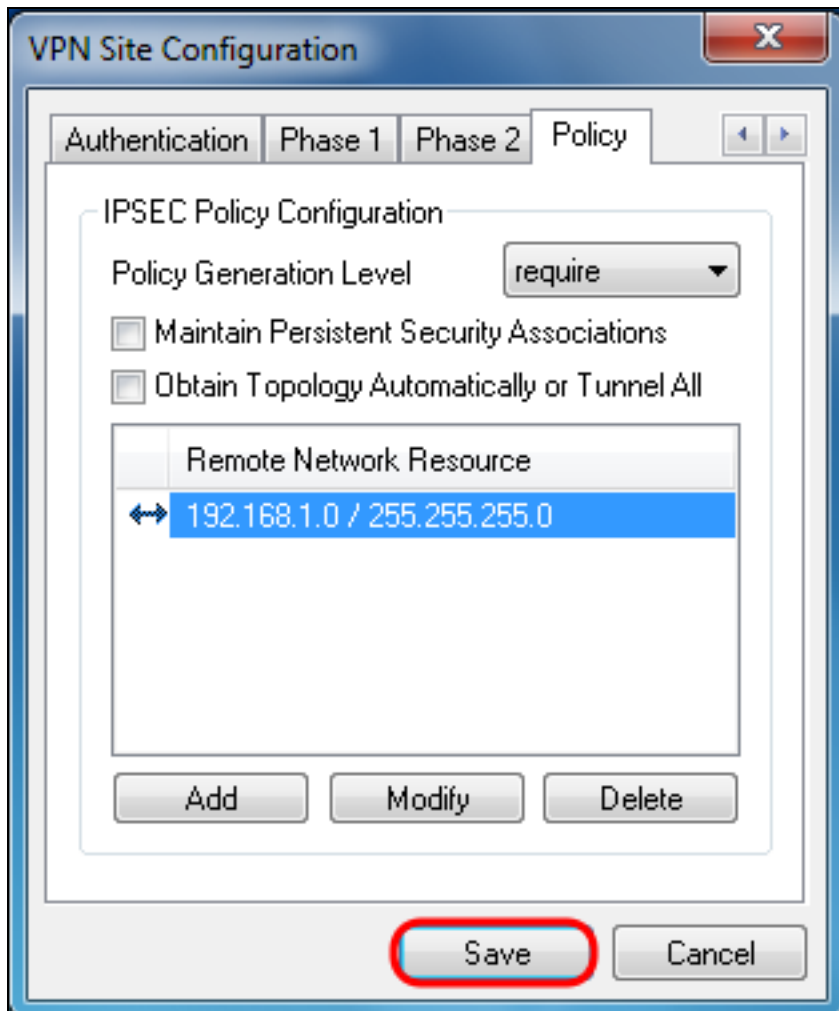
ステップ18:[Netmask] フィールドに、RV130/RV130Wのローカルネットワークのサブネットマスクを入力します。このネットマスクは、このドキュメントの「IPSec VPNサーバユーザ設定」セクションの[ステップ2](#)の「[サブネットマスク](#)」フィールドと一致している必要があります。



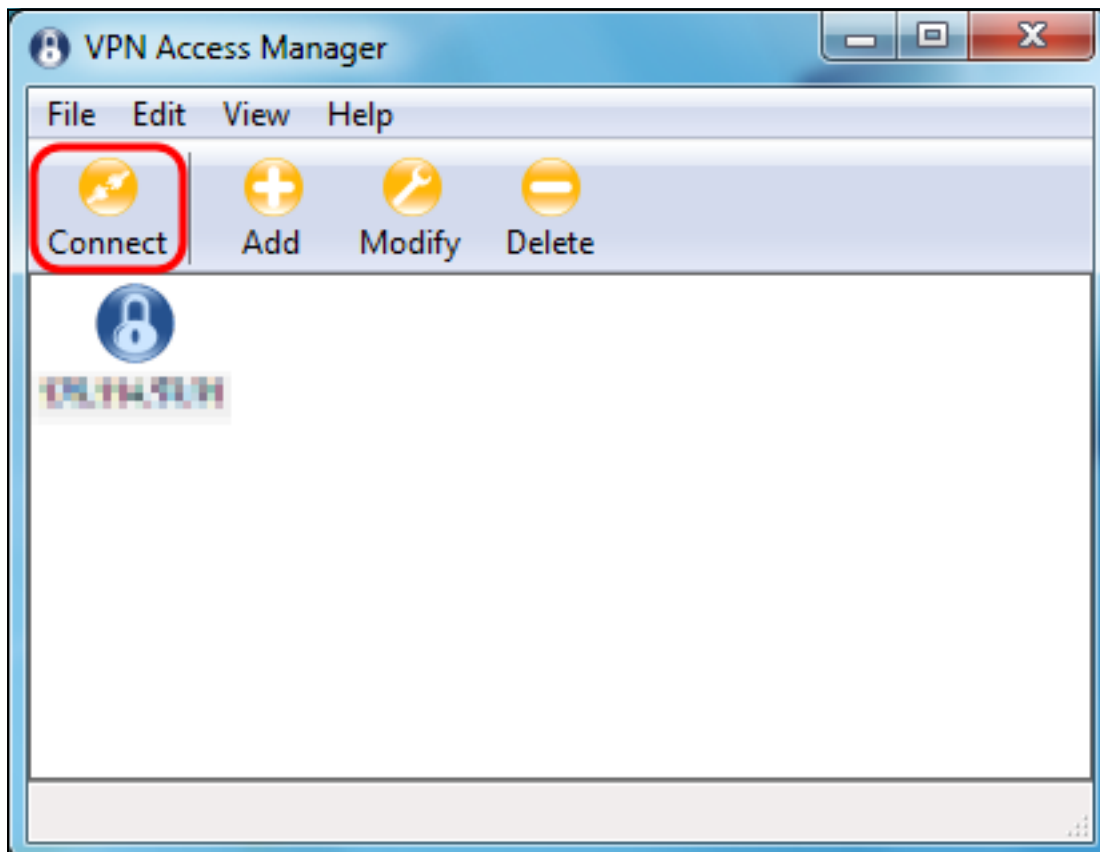
ステップ19:[OK] をクリックして、リモートネットワークリソースの追加を終了します。



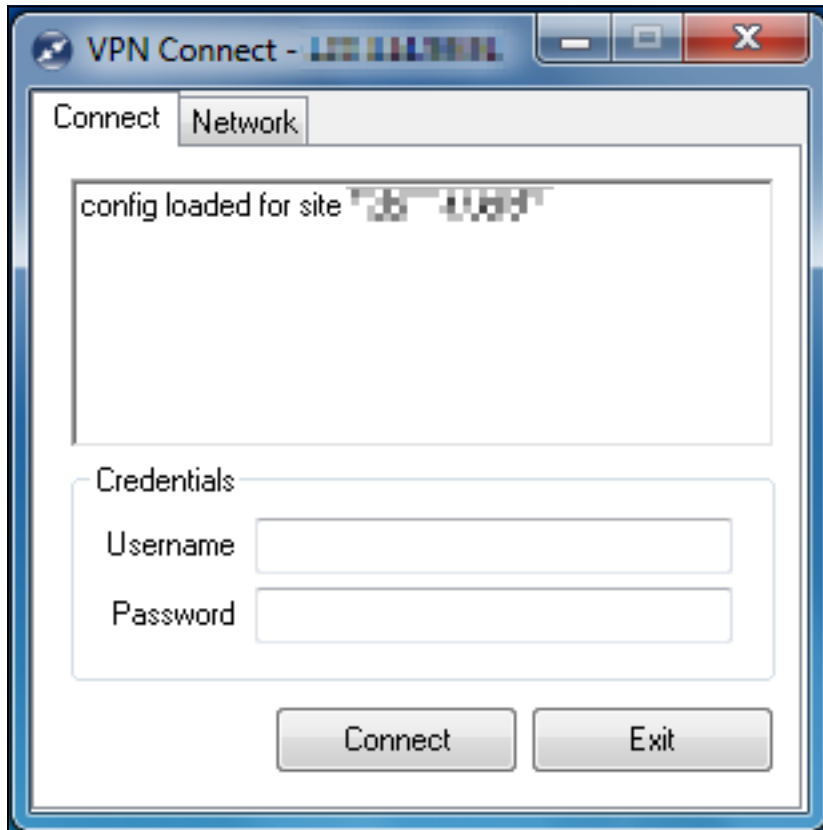
ステップ20:[Save] をクリックして、VPNサイトに接続するための設定を保存します。



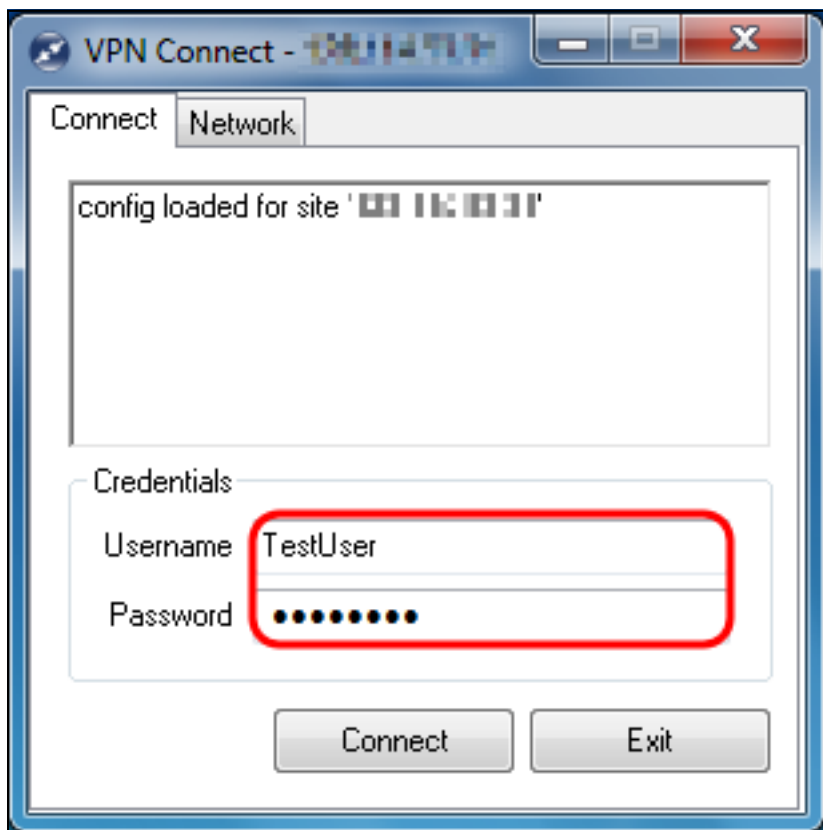
ステップ21:[VPN Access Manager] ウィンドウに戻り、設定したVPNサイトを選択し、[Connect] ボタンをクリックします。



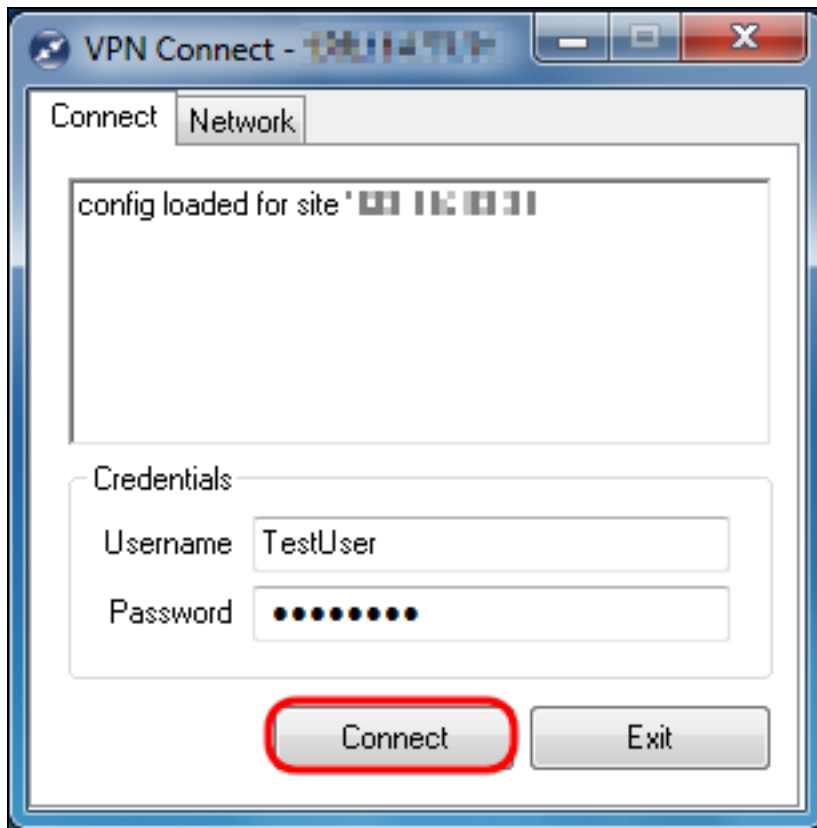
[VPN Connect] ウィンドウが表示されます。



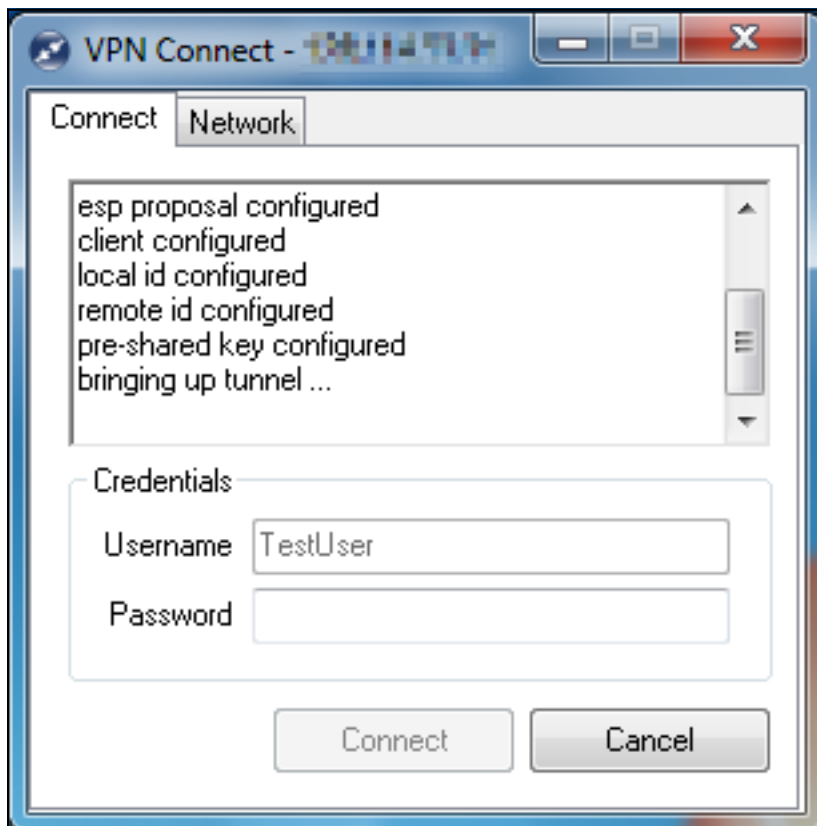
ステップ22:[Credentials] セクションで、このドキュメントの「[IPSec VPNサーバユーザ設定](#)」セクションの[ステップ4](#)で設定したアカウントのユーザ名とパスワードを入力します。

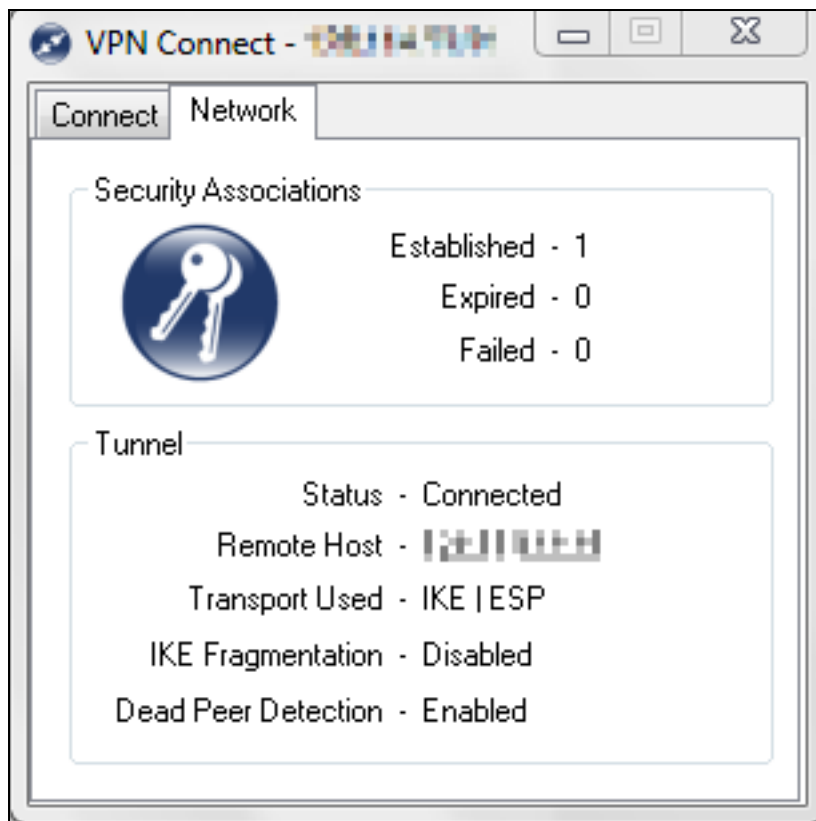


ステップ23:[Connect to VPN into the RV130/RV130W] をクリックします。



IPSec VPNトンネルが確立され、VPNクライアントはRV130/RV130W LANの背後にあるリソースにアクセスできます。





[この記事に関連するビデオを見る...](#)

シスコのその他の技術に関する講演を表示するには、[ここをクリックしてください。](#)

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。