Use o cliente Soft VPN Shrew para se conectar com o servidor VPN IPSec no RV130 e RV130W

Objetivo

A VPN IPSec (Virtual Private Network) permite que você obtenha recursos remotos com segurança, estabelecendo um túnel criptografado na Internet.

O RV130 e o RV130W funcionam como servidores VPN IPSec e suportam o cliente Shrew Soft VPN.

Faça o download da versão mais recente do software cliente.

·Shrew Soft (https://www.shrew.net/download/vpn)

Note: Para poder instalar e configurar com êxito o cliente Shrew Soft VPN com um servidor VPN IPSec, você precisa primeiro configurar o servidor VPN IPSec. Para obter informações sobre como fazer isso, consulte o artigo *Configuração de um Servidor VPN IPSec em RV130 e RV130W.*

O objetivo deste documento é mostrar como usar o cliente Soft VPN Shrew para se conectar com um IPSec VPN Server no RV130 e RV130W.

Dispositivos aplicáveis

·Firewall VPN Wireless-N RV130W

·Firewall VPN RV130

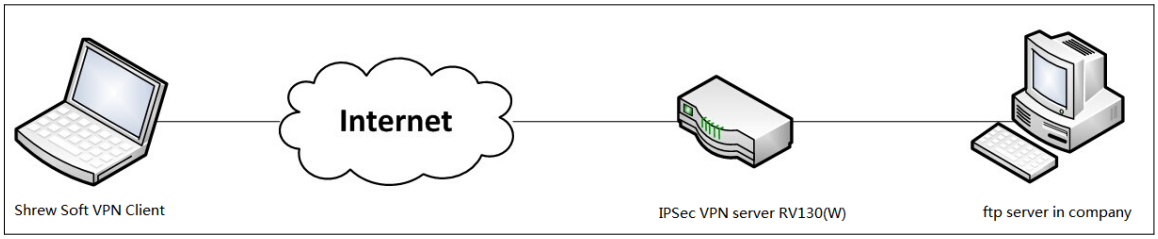
Requisitos do sistema

·Sistemas de 32 ou 64 bits

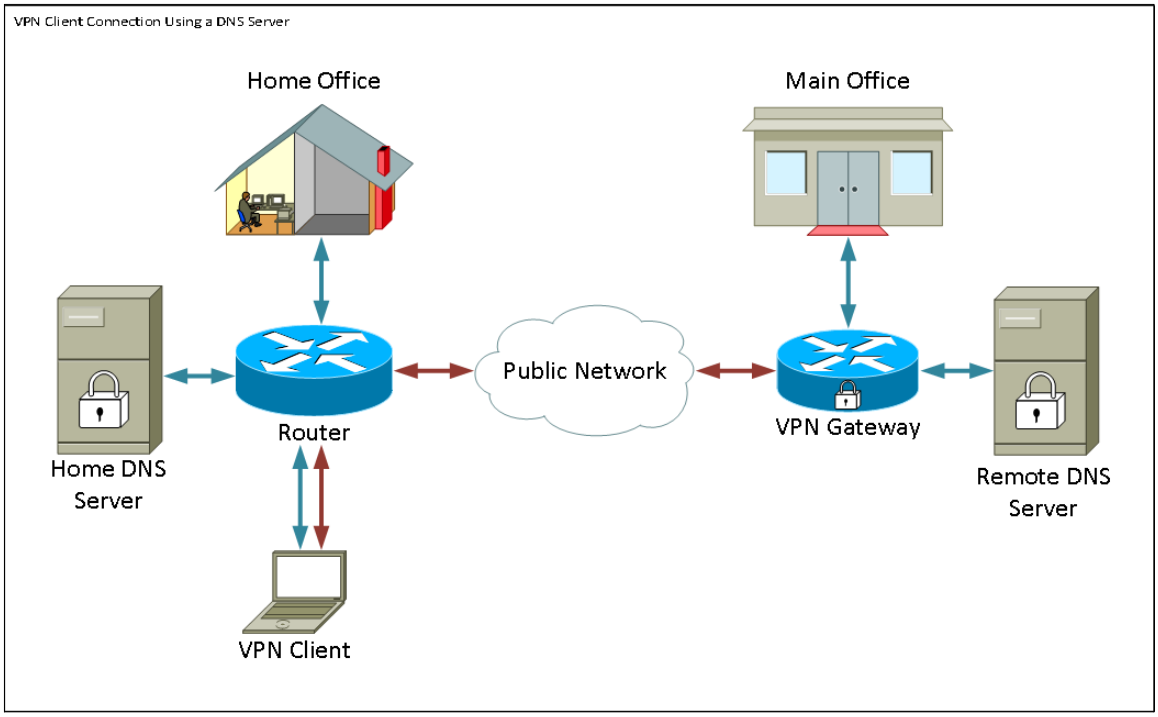
·Windows 2000, XP, Vista ou Windows 7/8

Topologia

Uma topologia de nível superior é mostrada abaixo, ilustrando os dispositivos envolvidos em uma configuração de cliente para site da Shrewsoft.



Um fluxograma mais detalhado que ilustra a função dos servidores DNS em um ambiente de rede de pequenas empresas é mostrado abaixo.



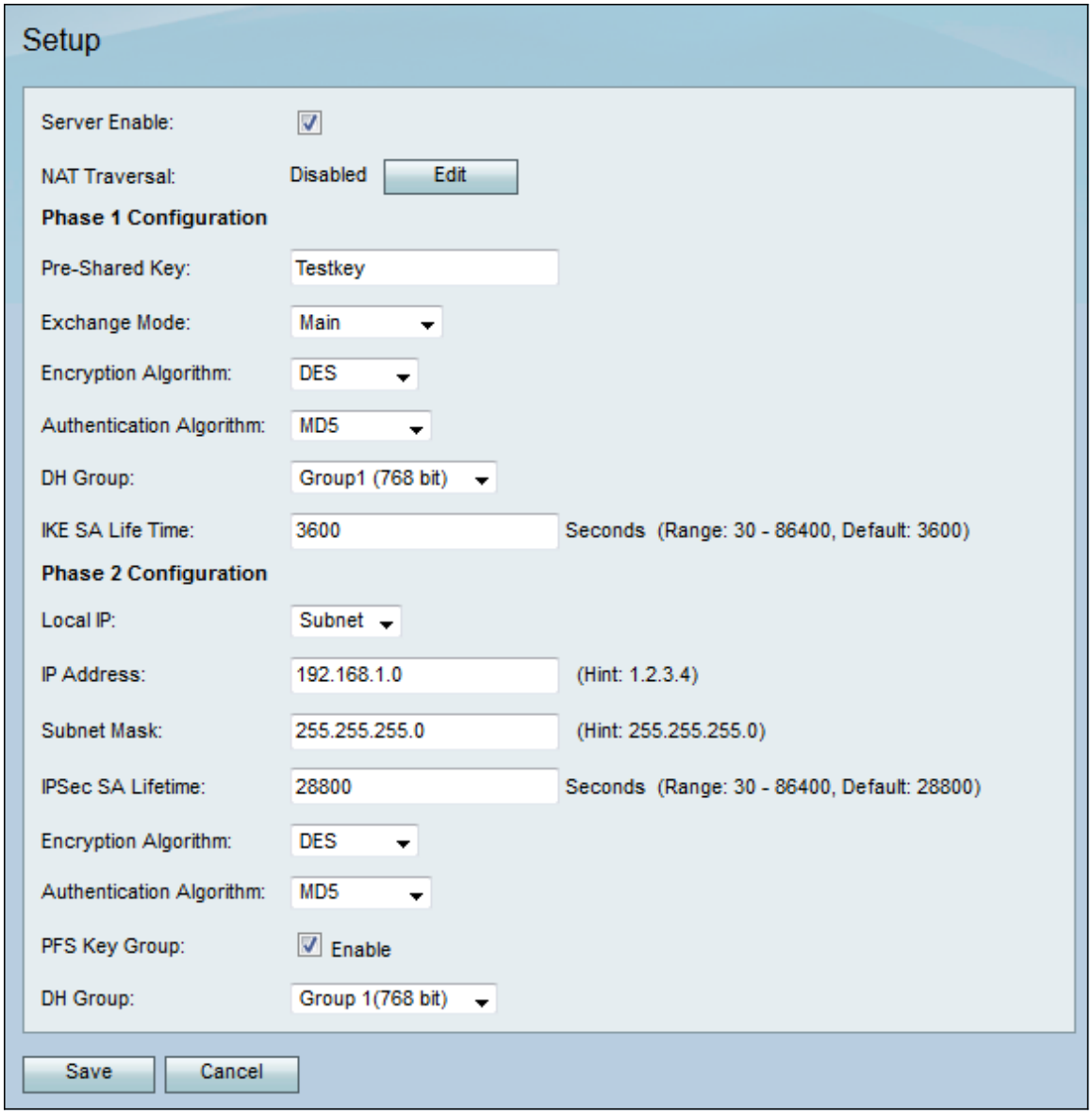
Versão de software

- 1.0.1.3

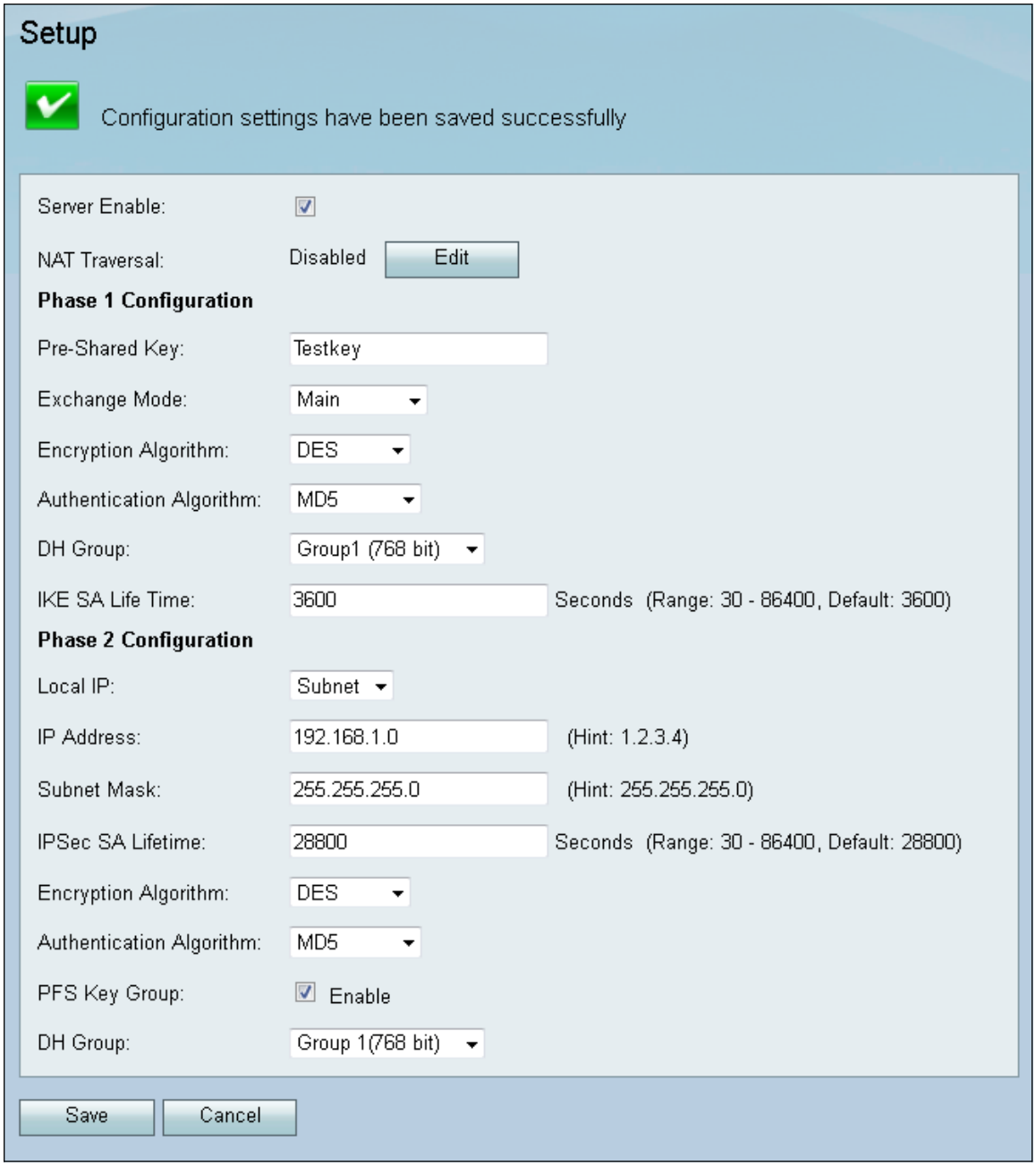
Configuração do cliente Soft VPN Shrew

Configuração de IPSec VPN e de usuário

Etapa 1. Inicie a sessão no utilitário de configuração da Web e selecione **VPN > IPSec VPN Server > Setup**. A página *Setup* é aberta.

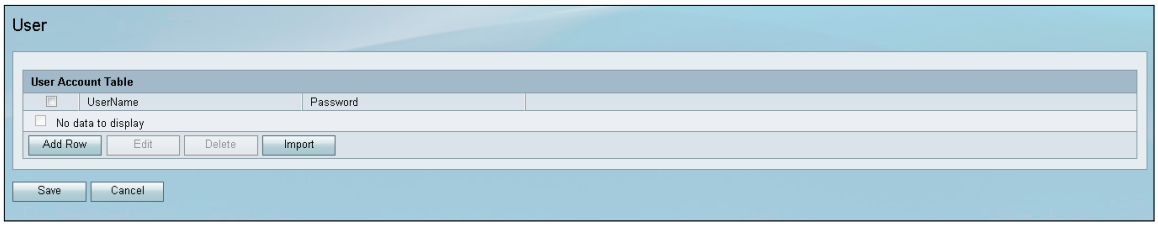


Etapa 2. Verifique se o servidor VPN IPSec para o RV130 está configurado corretamente. Se o Servidor VPN IPSec não estiver configurado ou estiver configurado incorretamente, consulte *Configuração de um Servidor VPN IPSec em RV130 e RV130W* e clique em **Salvar** .

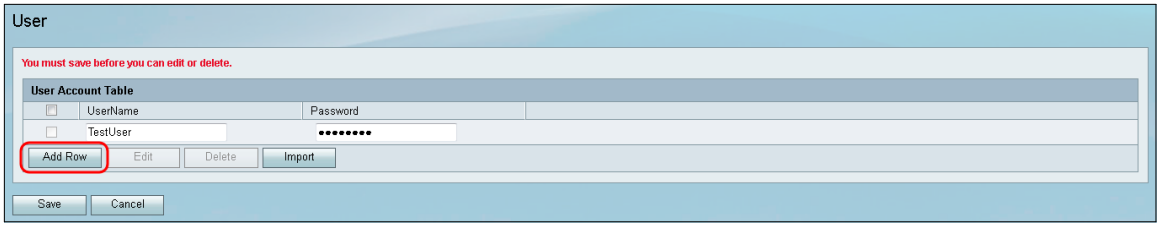


Note: As configurações acima são um exemplo de uma configuração de servidor VPN IPSec RV130/RV130W. As configurações são baseadas no documento *Configuração de um servidor VPN IPSec em RV130 e RV130W,* e serão mencionadas nas etapas subsequentes.

Etapa 3. Navegue até **VPN > IPSec VPN Server > User**. A página *User* é exibida.



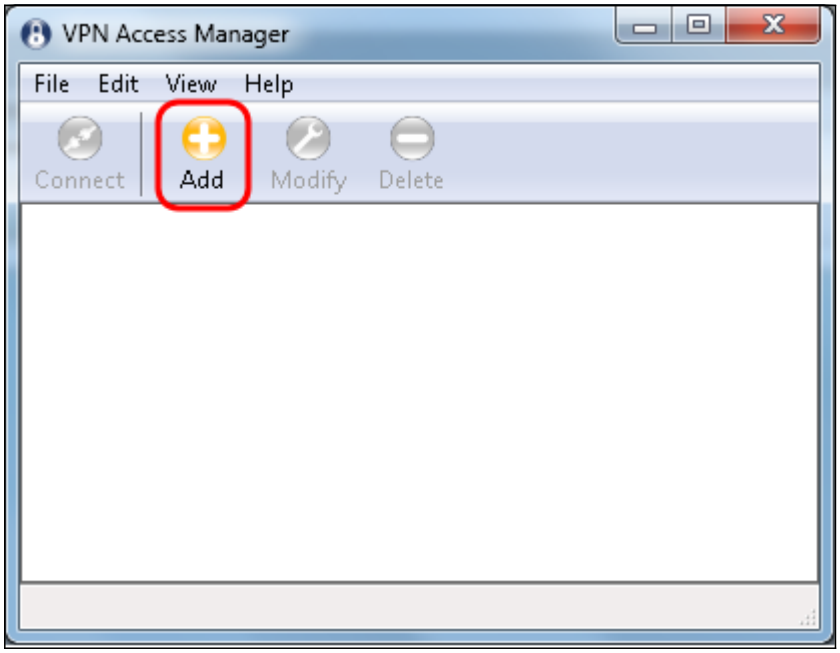
Etapa 4. Clique em **Add Row** para adicionar contas de usuário, usadas para autenticar os clientes VPN (Extended Authentication) e insira o nome de usuário e a senha desejados nos campos fornecidos.



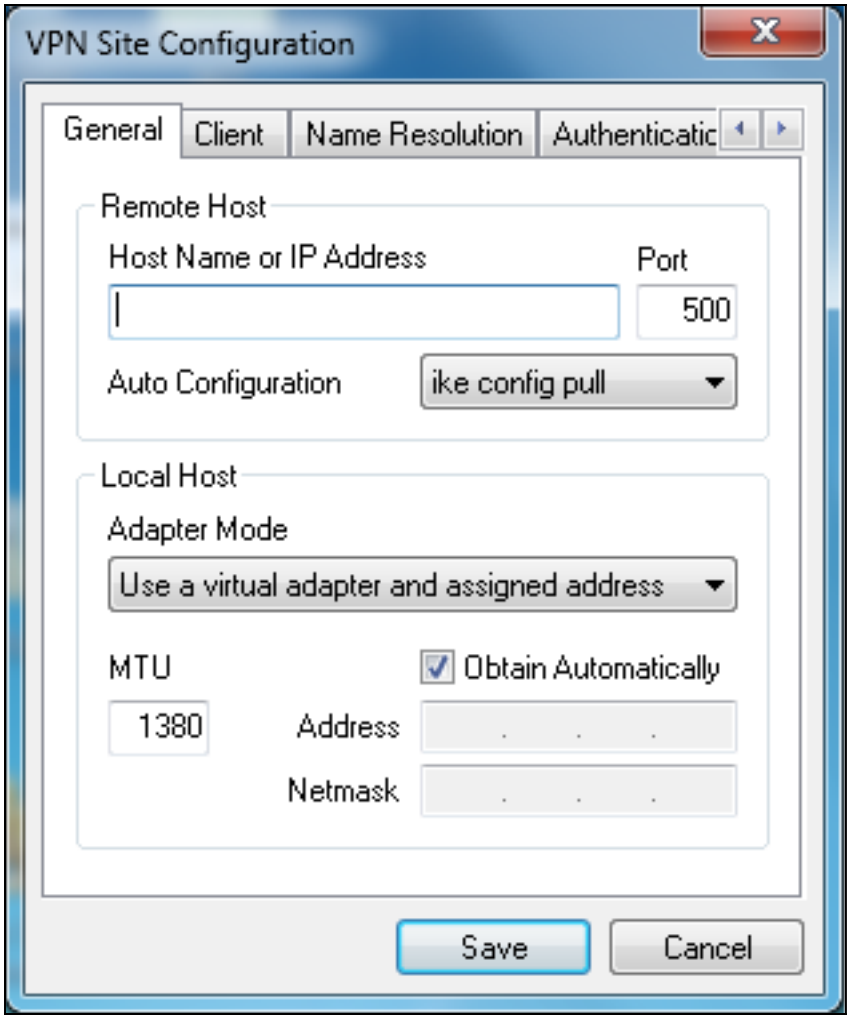
Etapa 5. Clique em **Save** (Salvar) para salvar as configurações.

Configuração de cliente de VPN

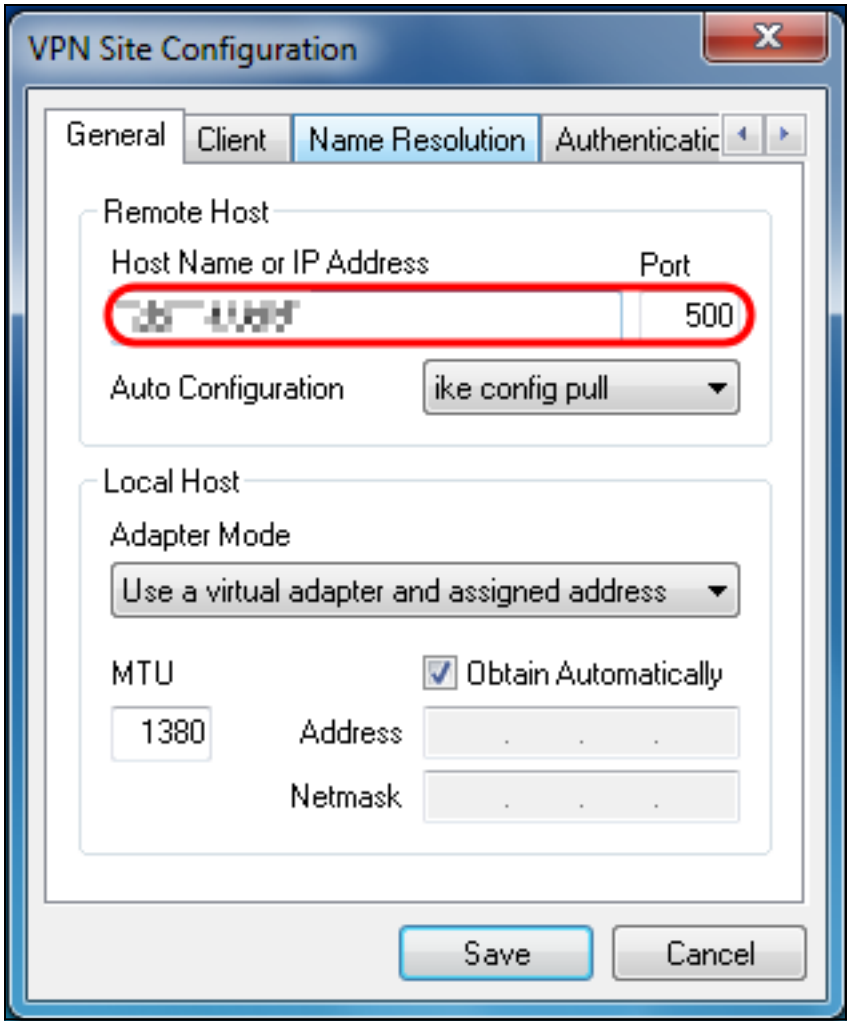
Etapa 1. Abra o Shrew VPN Access Manager e clique em **Add** para adicionar um perfil.



A janela *VPN Site Configuration* é exibida.

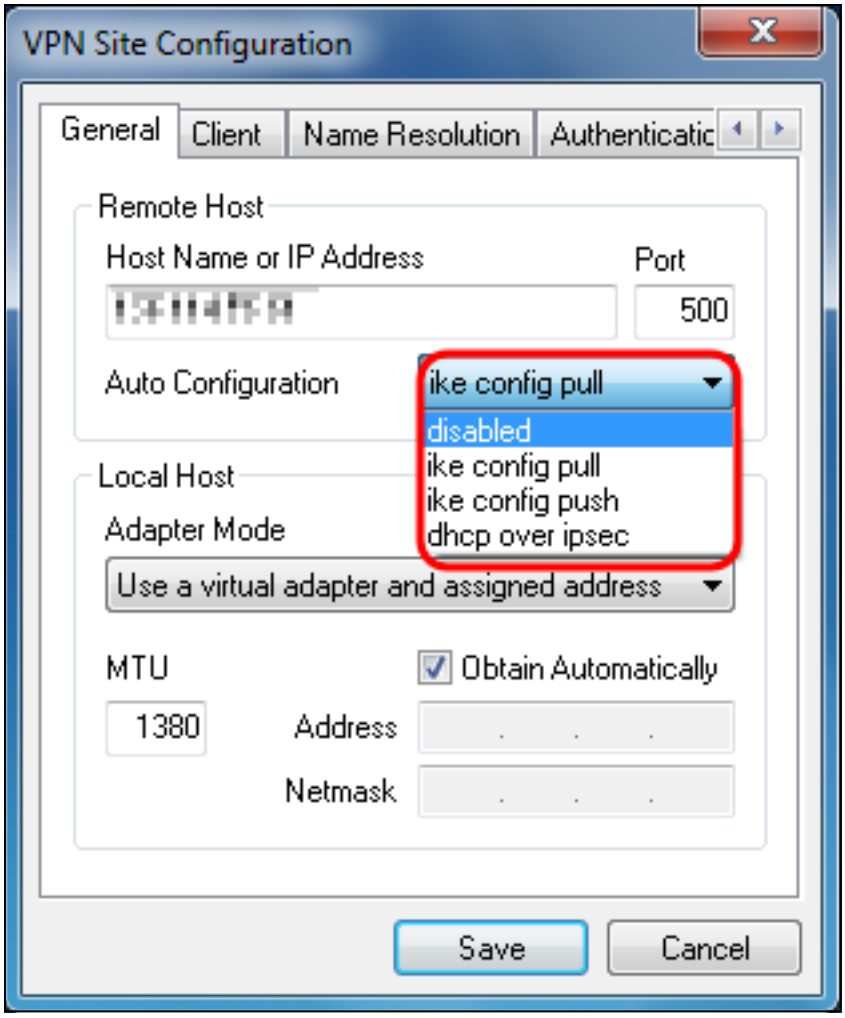


Etapa 2. Na seção *Host remoto* na guia *Geral*, digite o nome do host público ou o endereço IP da rede à qual você está tentando se conectar.



Note: Verifique se o número da porta está definido com o valor padrão de 500. Para que a VPN funcione, o túnel usa a porta UDP 500, que deve ser definida para permitir que o tráfego ISAKMP seja encaminhado no firewall.

Etapa 3. Na lista suspensa *Configuração automática*, escolha **desativado**.



As opções disponíveis são definidas da seguinte forma:

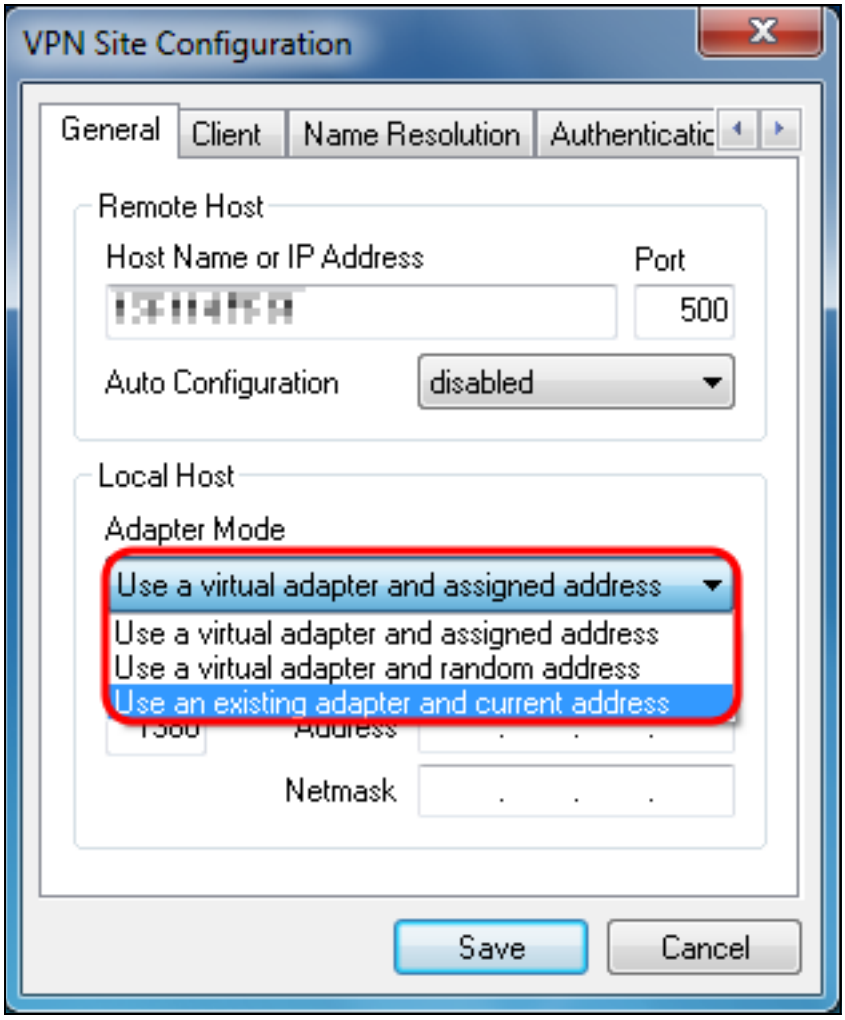
·Disabled — desativa todas as configurações automáticas do cliente.

·IKE Config Pull — Permite configurar solicitações de um computador pelo cliente. Com o suporte do método Pull pelo computador, a solicitação retorna uma lista de configurações suportadas pelo cliente.

·IKE Config Push — Oferece a um computador a oportunidade de oferecer configurações ao cliente por meio do processo de configuração. Com o suporte do método Push pelo computador, a solicitação retorna uma lista de configurações suportadas pelo cliente.

·DHCP sobre IPSec — Oferece ao cliente a oportunidade de solicitar configurações do computador por meio de DHCP sobre IPSec.

Etapa 4. Na seção *Host local*, escolha **Usar um adaptador existente e o endereço atual** na lista suspensa *Modo de adaptador*.



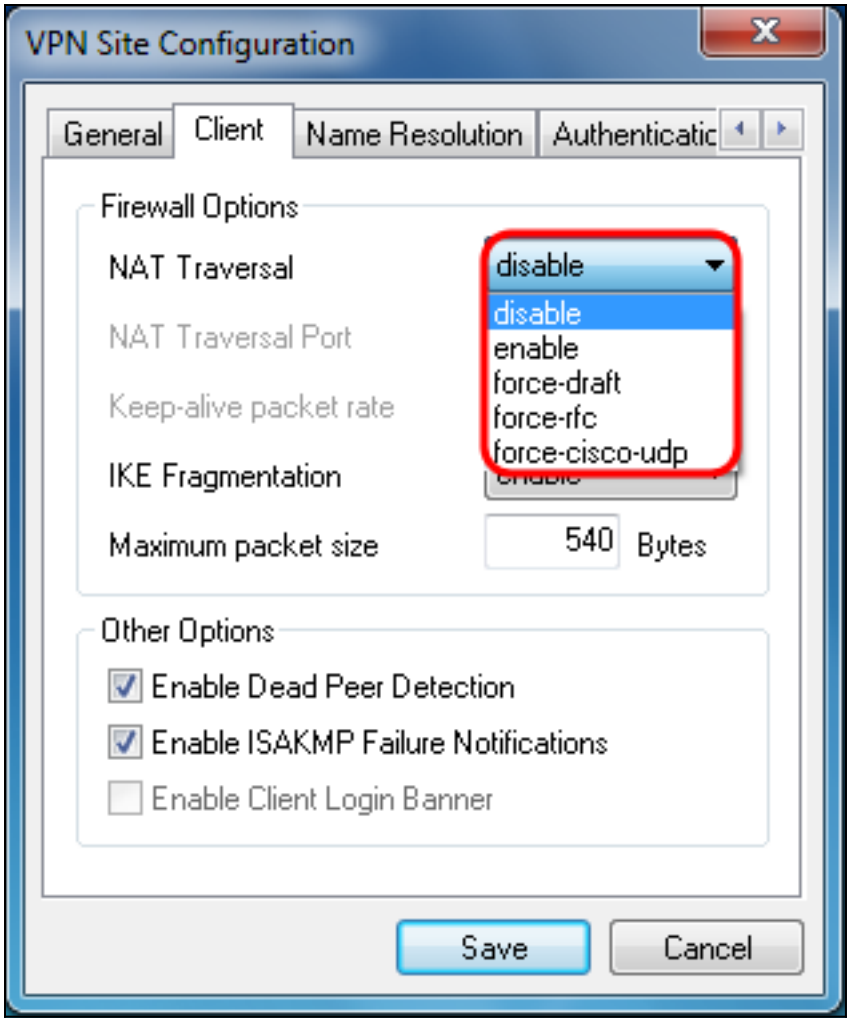
As opções disponíveis são definidas da seguinte forma:

·Usar um adaptador virtual e endereço atribuído — Permite que o cliente use um adaptador virtual com um endereço especificado como a origem para suas comunicações IPsec.

·Usar um adaptador virtual e endereço aleatório — Permite que o cliente use um adaptador virtual com um endereço aleatório como origem para suas comunicações IPsec.

·Usar um adaptador existente e o endereço atual — Permite que o cliente use apenas seu adaptador físico existente com seu endereço atual como a origem para suas comunicações IPsec.

Etapa 5. Clique na guia *Client*. Na lista suspensa *NAT Traversal*, selecione a mesma configuração que você configurou no RV130/RV130W para NAT Traversal no artigo *Configuração de um servidor VPN IPSec no RV130 e RV130W.*



As opções de menu NATT (Network Address Translation Traversal) disponíveis são definidas da seguinte forma:

·Disable — As extensões de protocolo NATT não serão usadas.

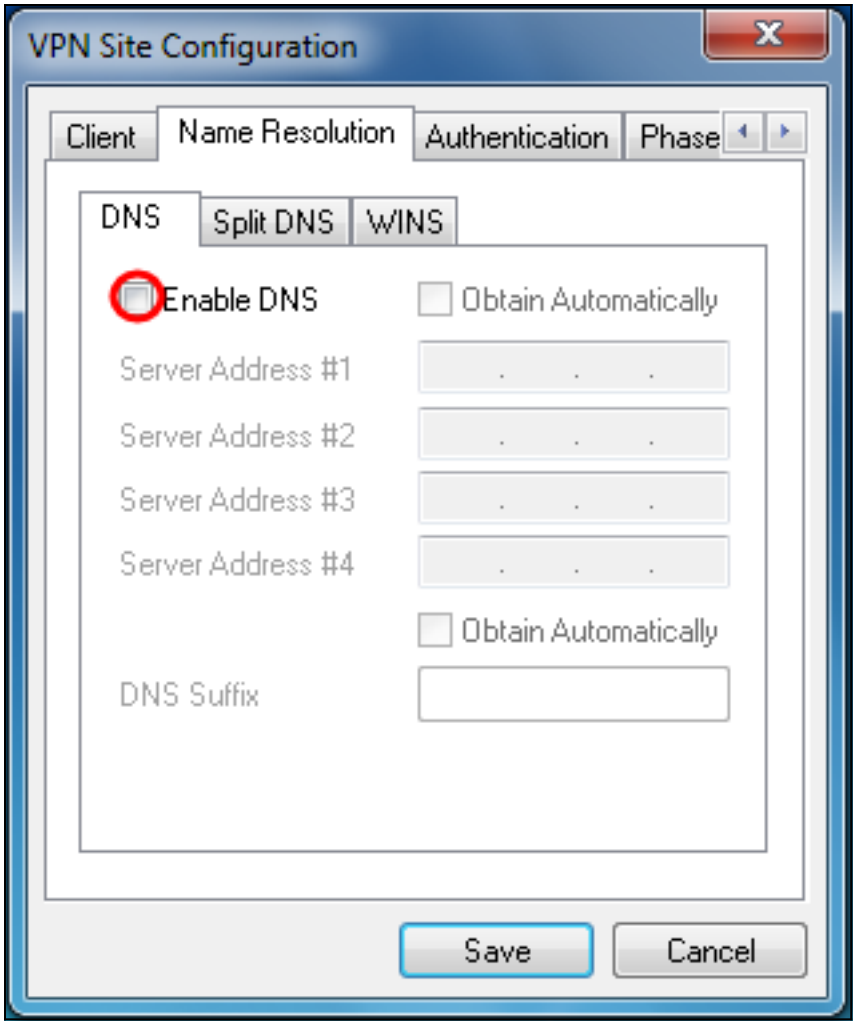
·Habilitar — As extensões de protocolo NAT serão usadas somente se o Gateway VPN indicar suporte durante as negociações e se o NAT for detectado.

·Forçar Rascunho — A versão Rascunho das extensões do protocolo NAT será usada independentemente de o Gateway VPN indicar ou não suporte durante as negociações ou se o NAT for detectado.

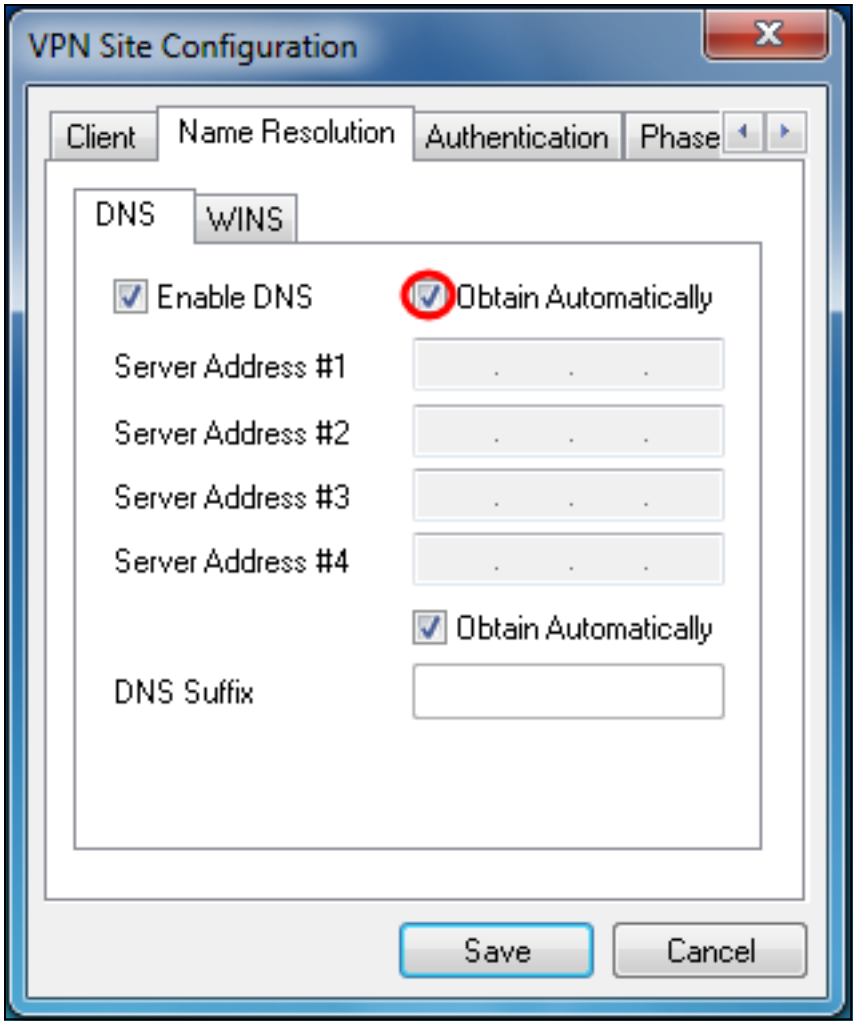
·Force-RFC — A versão RFC do protocolo NAT será usada independentemente de o Gateway VPN indicar ou não suporte durante as negociações ou se o NAT for detectado.

·Force-Cisco-UDP — Force o encapsulamento UDP para clientes VPN sem NAT.

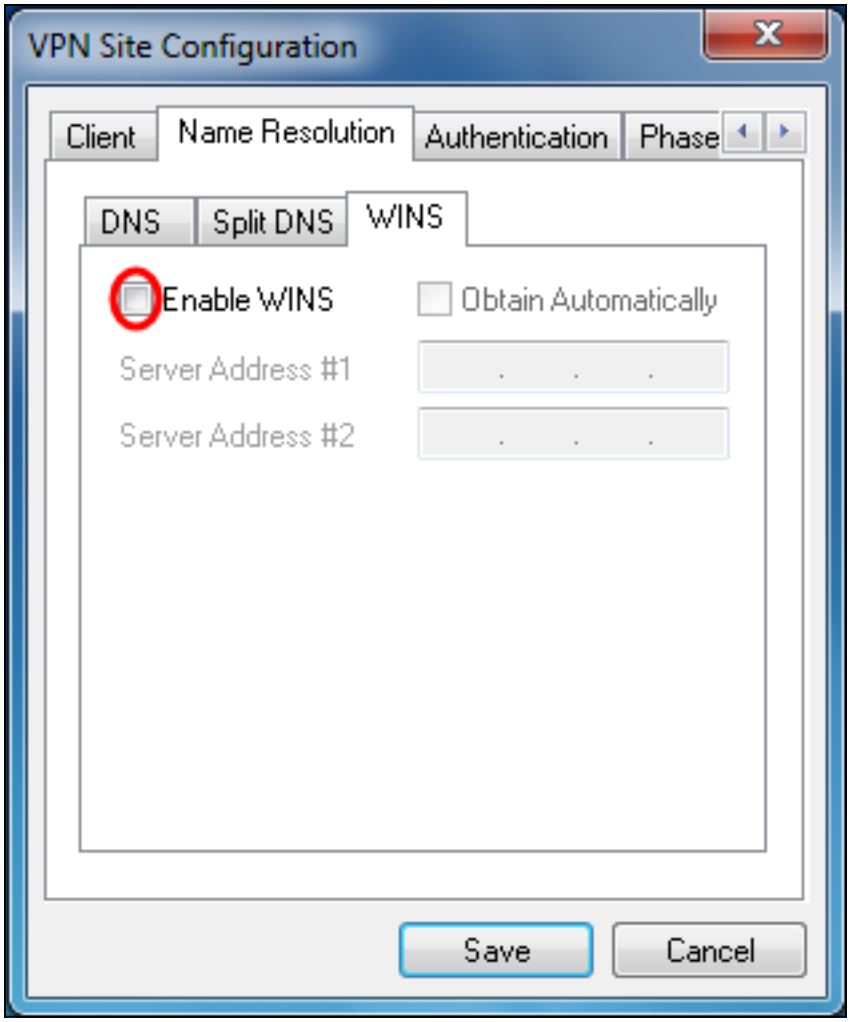
Etapa 6. Clique na guia *Name Resolution* e marque a caixa de seleção **Enable DNS** se desejar habilitar o DNS. Se configurações específicas de DNS não forem necessárias para a configuração do seu site, desmarque a caixa de seleção **Habilitar DNS**.



Etapa 7. (Opcional) Se o seu gateway remoto estiver configurado para suportar o Configuration Exchange, o gateway é capaz de fornecer configurações DNS automaticamente. Caso contrário, verifique se a caixa de seleção **Obter automaticamente** está desmarcada e insira manualmente um endereço de servidor DNS válido.

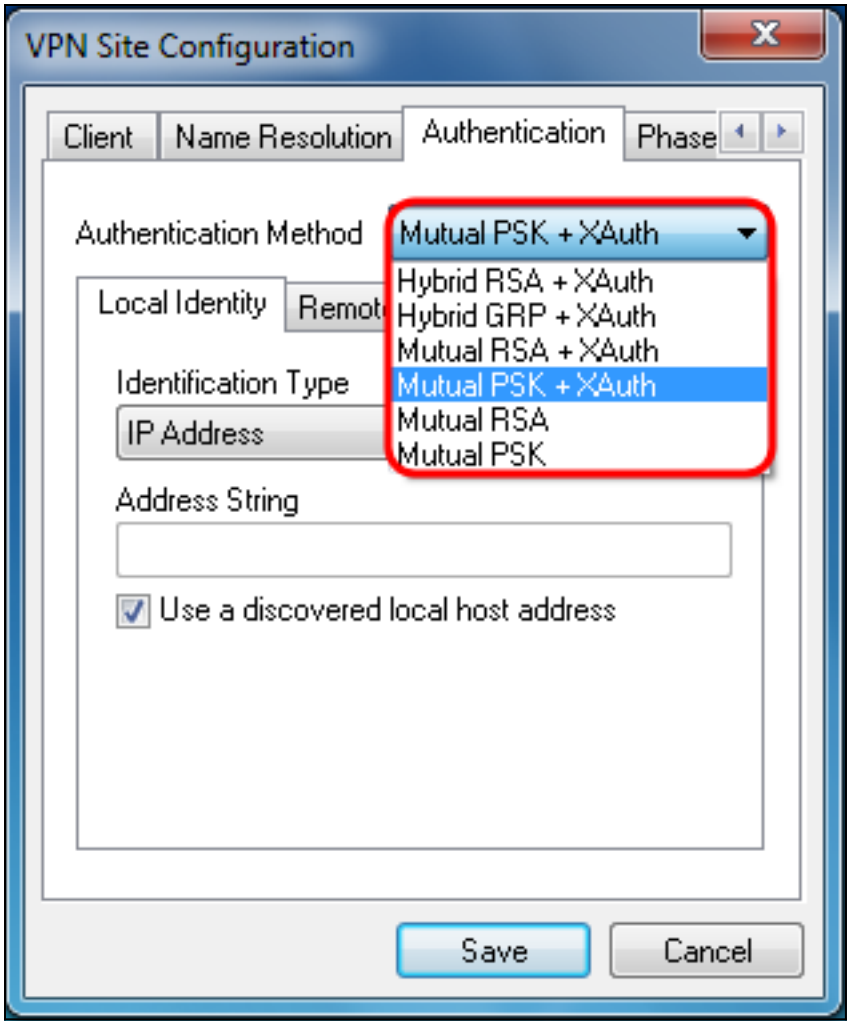


Etapa 8. (Opcional) Clique na guia *Resolução de nomes*, marque a caixa de seleção **Habilitar WINS** se quiser habilitar o Windows Internet Name Server (WINS). Se o gateway remoto estiver configurado para suportar o Configuration Exchange, o gateway poderá fornecer as configurações do WINS automaticamente. Caso contrário, verifique se a caixa de seleção **Obter automaticamente** está desmarcada e insira manualmente um endereço de servidor WINS válido.



Note: Ao fornecer informações de configuração do WINS, um cliente poderá resolver nomes WINS usando um servidor localizado na rede privada remota. Isso é útil ao tentar acessar recursos de rede do Windows remotos usando um nome de caminho Uniform Naming Convention. O servidor WINS normalmente pertenceria a um controlador de domínio do Windows ou a um servidor Samba.

Etapa 9. Clique na guia *Authentication* e selecione **Mutual PSK + XAuth** na lista suspensa *Authentication Method*.



As opções disponíveis são definidas da seguinte forma:

·RSA + XAuth híbrido — a credencial do cliente não é necessária. O cliente autenticará o gateway. As credenciais estarão na forma de arquivos de certificado PEM ou PKCS12 ou tipo de arquivos de chave.

·GRP híbrido + XAuth — A credencial do cliente não é necessária. O cliente autenticará o gateway. As credenciais estarão na forma de arquivo de certificado PEM ou PKCS12 e uma string secreta compartilhada.

·RSA + XAuth mútuos — o cliente e o gateway precisam de credenciais para se autenticarem. As credenciais estarão na forma de arquivos de certificado PEM ou PKCS12 ou tipo de chave.

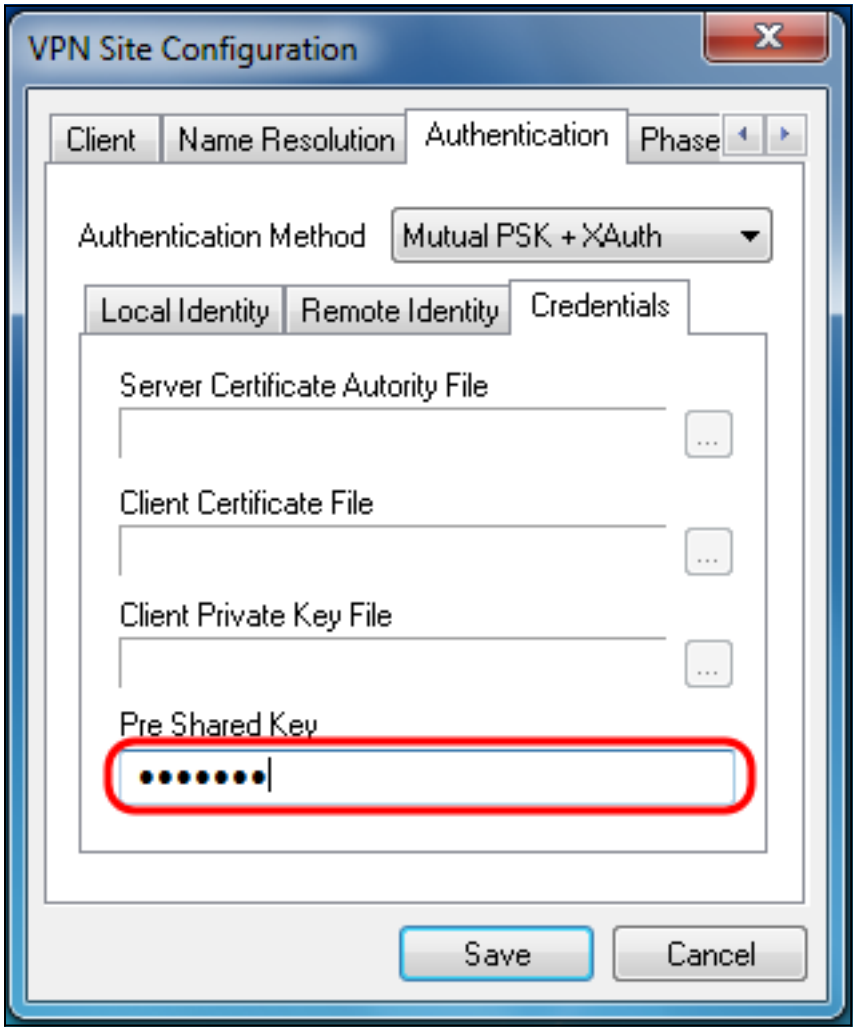
·PSK mútuo + XAuth — tanto o cliente como o gateway precisam de credenciais para se autenticarem. As credenciais terão a forma de uma cadeia de caracteres secreta compartilhada.

·RSA mútuo — tanto o cliente quanto o gateway precisam de credenciais para autenticação. As credenciais estarão na forma de arquivos de certificado PEM ou PKCS12 ou tipo de chave.

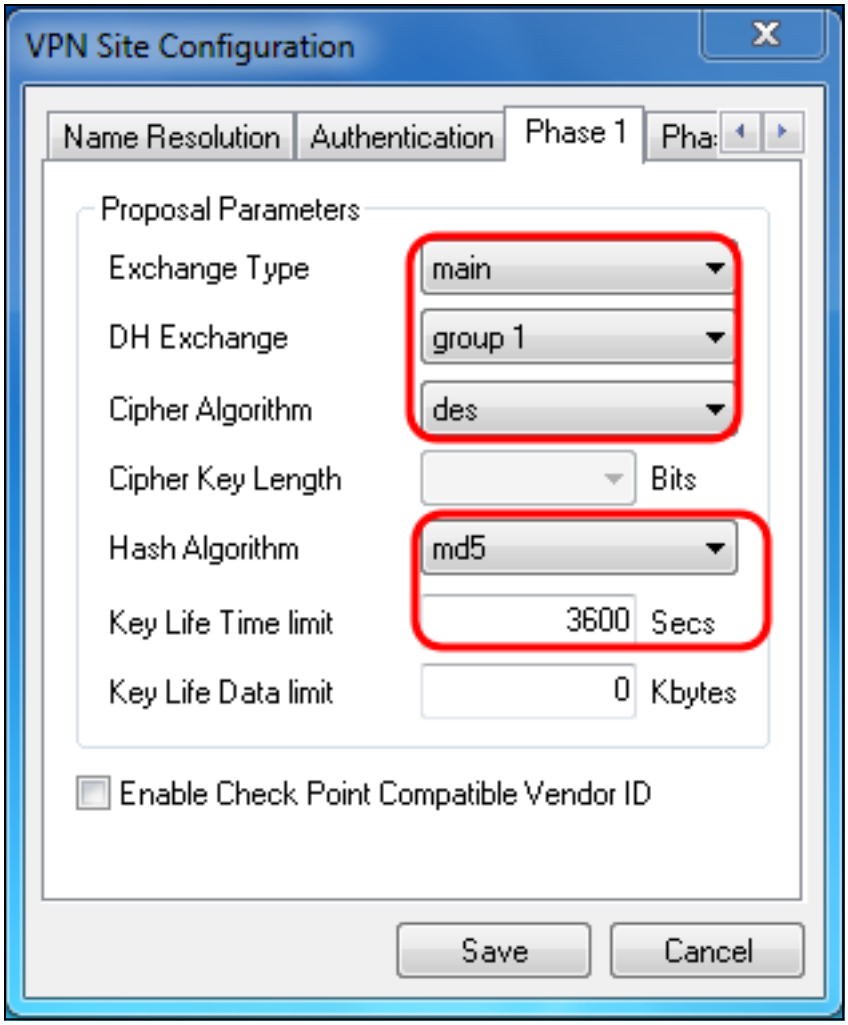
·PSK mútuo — tanto o cliente quanto o gateway precisam de credenciais para se autenticarem. As credenciais terão a forma de uma cadeia de caracteres secreta compartilhada.

Etapa 10. Na seção *Authentication*, clique na subguia *Credentials* e insira a mesma chave

pré-compartilhada que você configurou na página *IPsec VPN Server Setup* no campo *Pre Shared Key*.



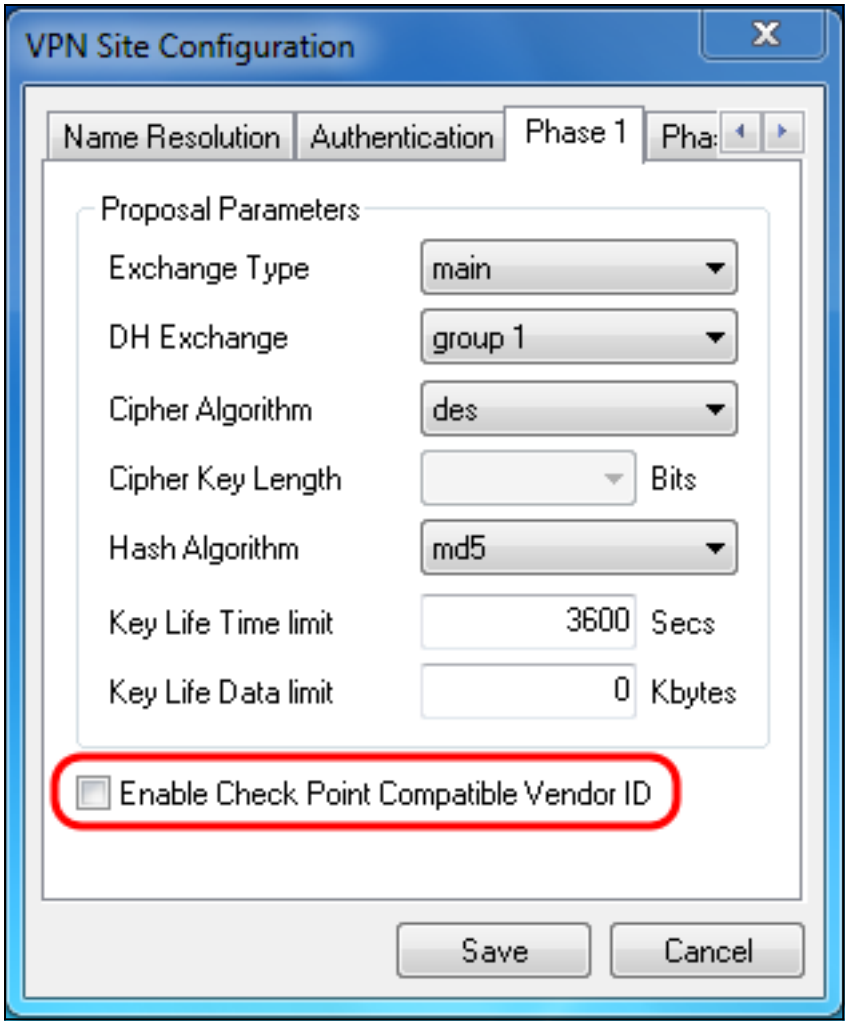
Etapa 11. Clique na guia *Fase 1*. Configure os parâmetros a seguir para ter as mesmas configurações que você definiu para o RV130/RV130W na Etapa 2 da seção *Configuração de Usuário do Servidor VPN IPSec* deste documento.



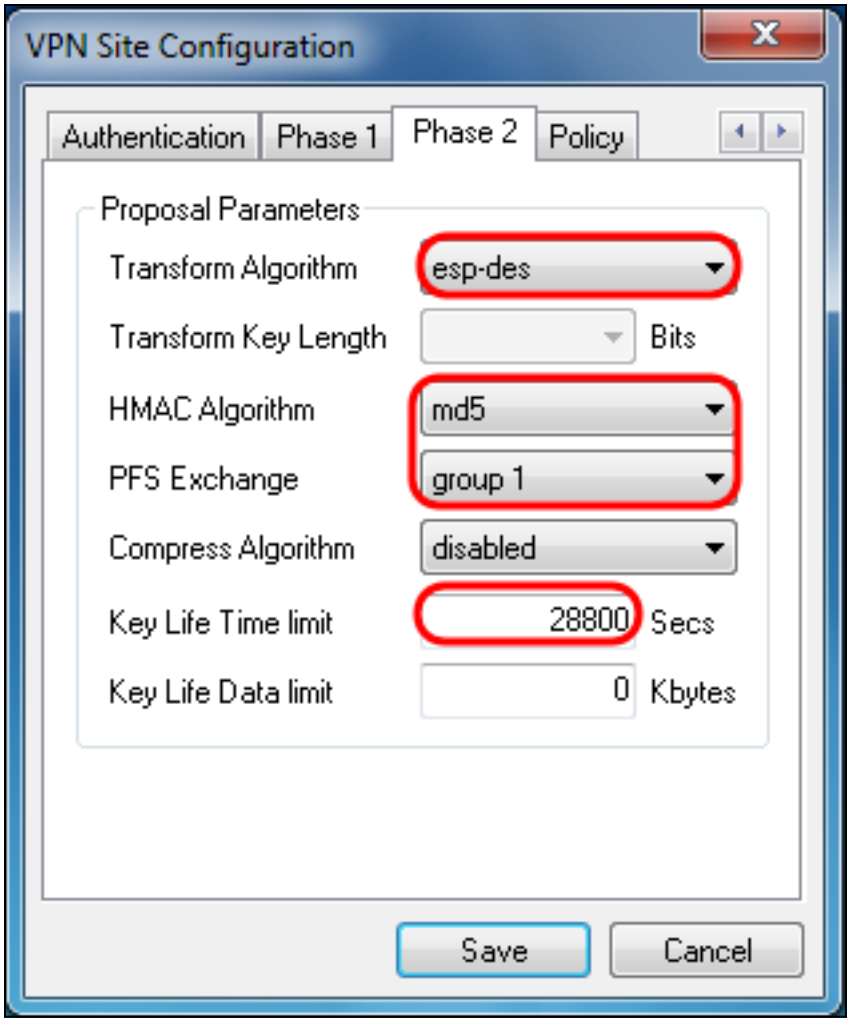
Os parâmetros em Shrew Soft devem corresponder às configurações de RV130/RV130W na Fase 1 da seguinte forma:

- "Tipo de troca" deve corresponder a "Modo de troca".
- "DH Exchange" deve corresponder a "DH Group".
- "Algoritmo de cifra" deve corresponder a "Algoritmo de criptografia".
- "Hash Algorithm" deve corresponder a "Authentication Algorithm".

Etapa 12. (Opcional) Se o seu gateway oferecer uma ID de fornecedor compatível com Cisco durante as negociações da fase 1, marque a caixa de seleção **Habilitar ID de fornecedor compatível com Check Point**. Se o gateway não funcionar ou se você não tiver certeza, deixe a caixa de seleção desmarcada.



Etapa 13. Clique na guia *Fase 2*. Configure os parâmetros a seguir para ter as mesmas configurações que você definiu para o RV130/RV130W na Etapa 2 da seção *Configuração de Usuário do Servidor VPN IPSec* deste documento.



Os parâmetros em Shrew Soft devem corresponder às configurações de RV130/RV130W na Fase 2 da seguinte forma:

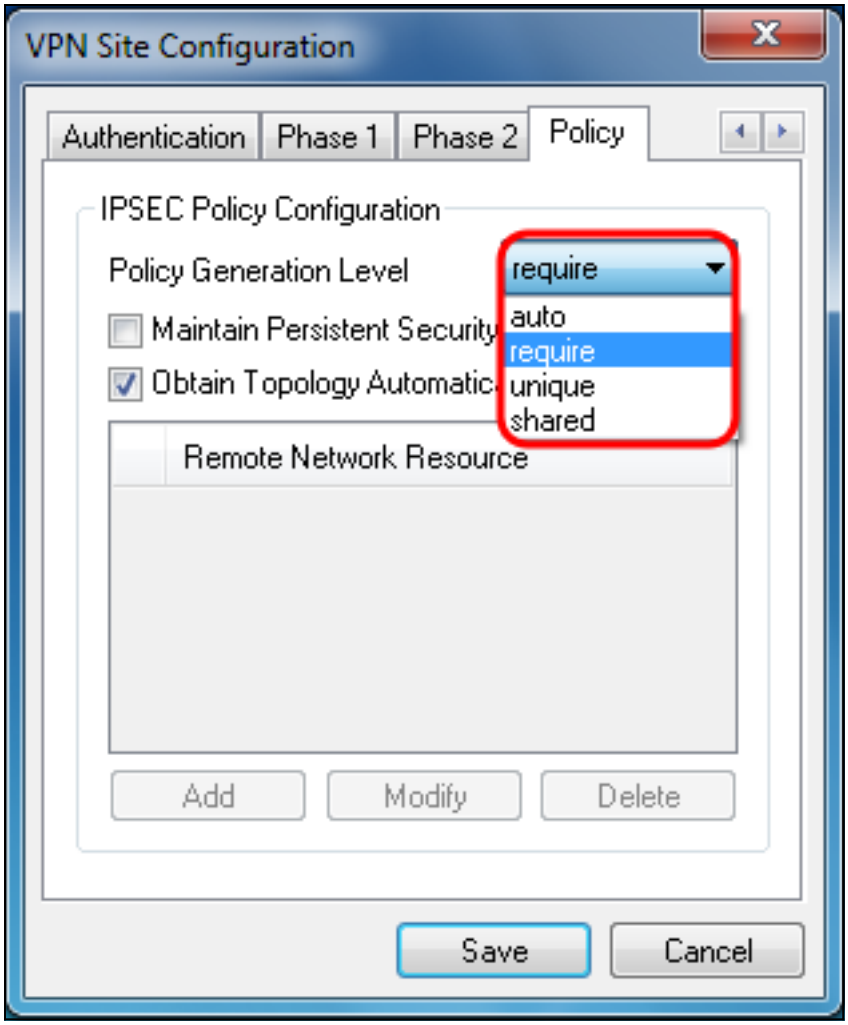
·"Transform Algorithm" deve corresponder a "Encryption Algorithm".

·"Algoritmo HMAC" deve corresponder a "Algoritmo de autenticação".

·PFS Exchange" deve corresponder a "DH Group" se o PFS Key Group estiver habilitado no RV130/RV130W. Caso contrário, selecione **disabled**.

·O "Key Life Time limit" deve corresponder ao "IPSec SA Lifetime".

Etapa 14. Clique na guia *Policy* e selecione **require** na lista suspensa *Policy Generation Level*. A opção *Policy Generation Level* modifica o nível no qual as políticas IPsec são geradas. Os diferentes níveis fornecidos na lista suspensa mapeiam os comportamentos de negociação de SA do IPSec implementados por implementações de fornecedores diferentes.



As opções disponíveis são definidas da seguinte forma:

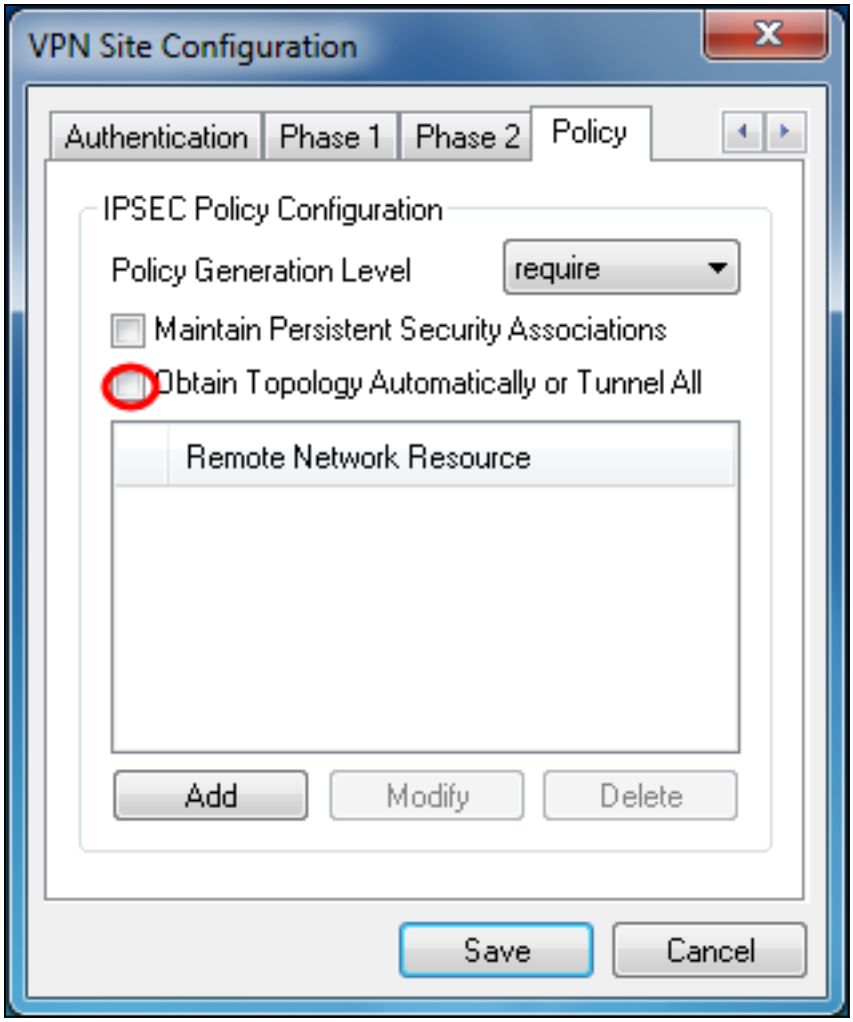
·Automático — O cliente determinará automaticamente o nível de política de IPSec apropriado.

·Exigir — O cliente não negociará uma SA (Security Association, associação de segurança) exclusiva para cada política. As políticas são geradas usando o endereço público local como a ID da política local e os Recursos de rede remota como a ID da política remota. A proposta da fase 2 usará as IDs de política durante a negociação.

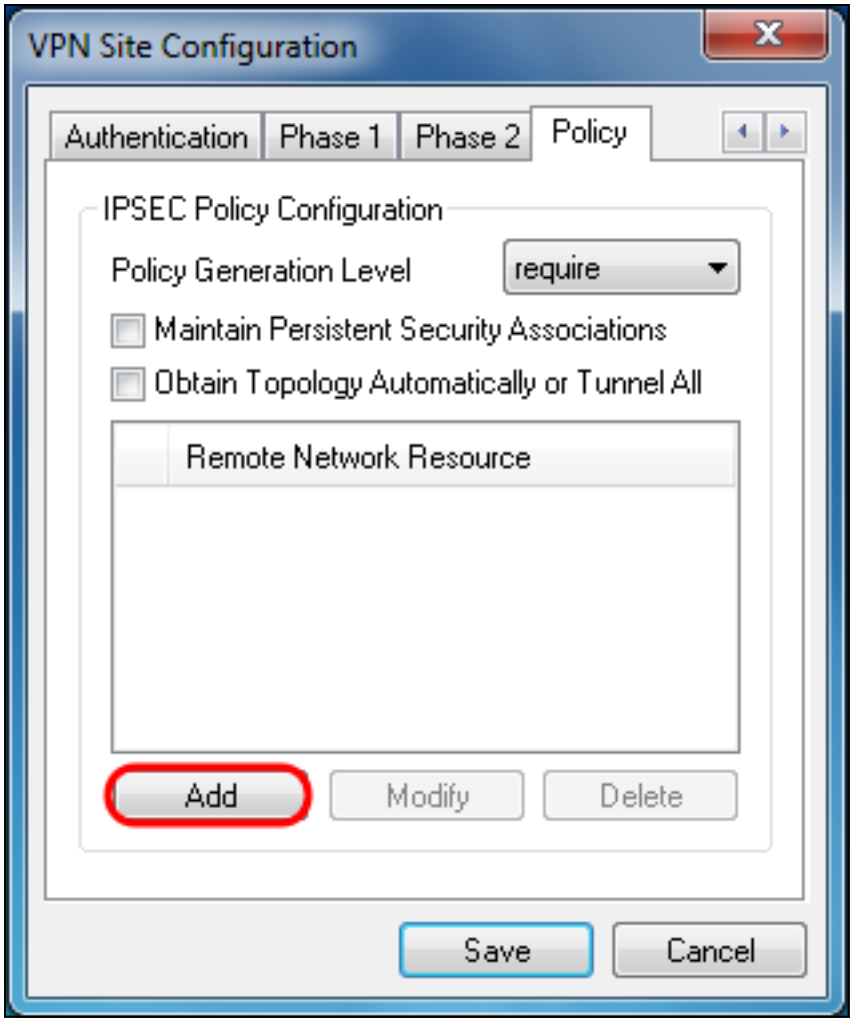
·Exclusivo — O cliente negociará um SA exclusivo para cada política.

·Compartilhado - As políticas são geradas no nível exigido. A proposta da fase 2 usará a ID da política local como a ID local e Qualquer (0.0.0.0/0) como a ID remota durante a negociação.

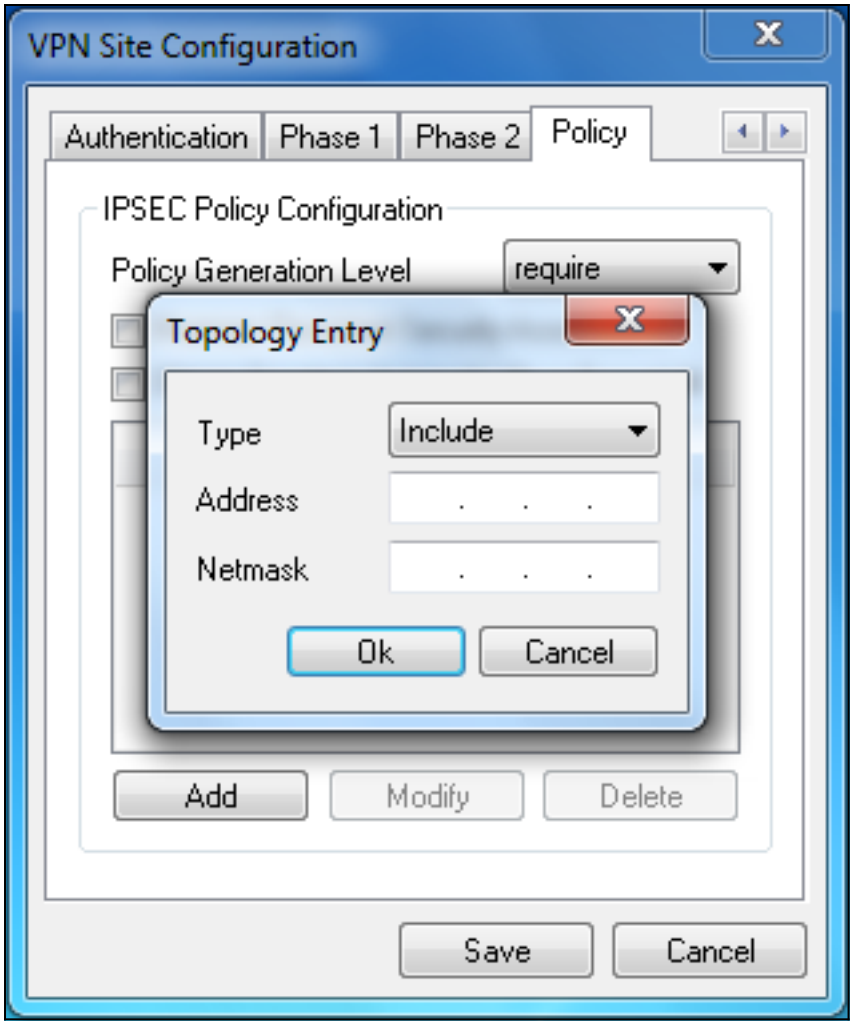
Etapa 15. Desmarque a caixa de seleção **Obter topologia automaticamente ou Encapsular tudo**. Essa opção modifica a forma como as políticas de segurança são configuradas para a conexão. Quando desativada, a configuração Manual deve ser executada. Quando ativada, a configuração Automática é executada.



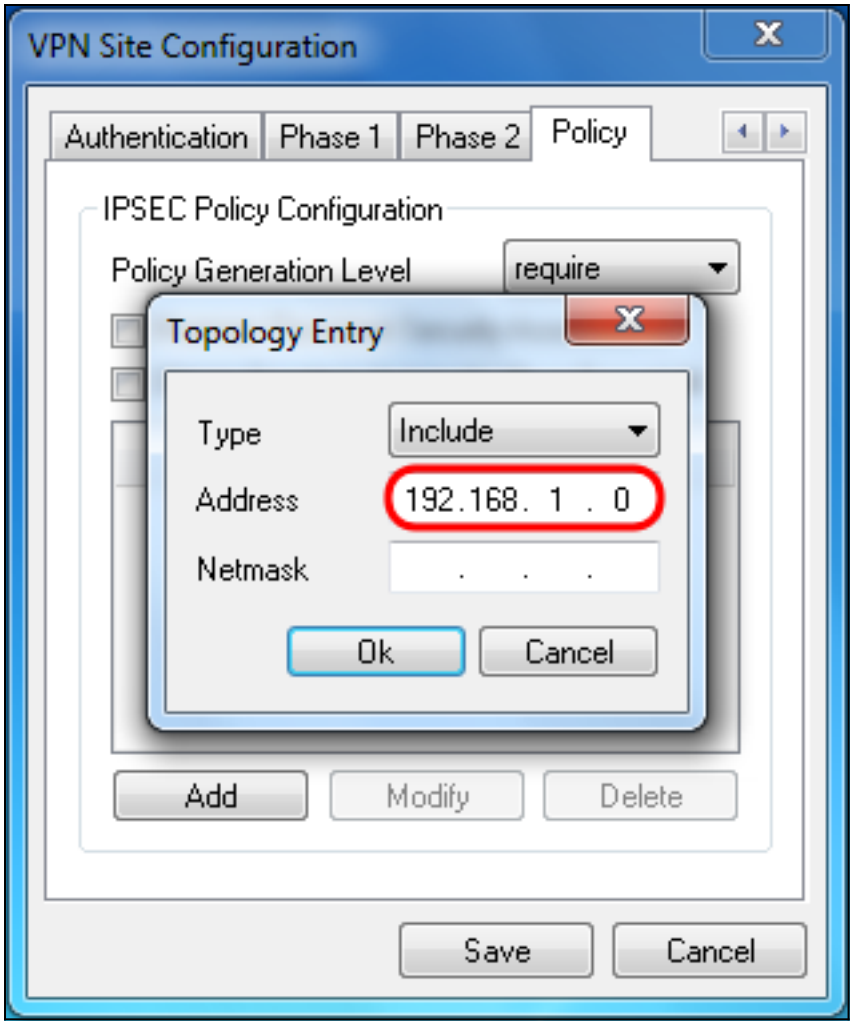
Etapa 16. Clique em **Add** para adicionar o recurso de rede remota ao qual você deseja se conectar. Os recursos de rede remota incluem acesso remoto ao desktop, recursos departamentais, unidades de rede e correio eletrônico protegido.



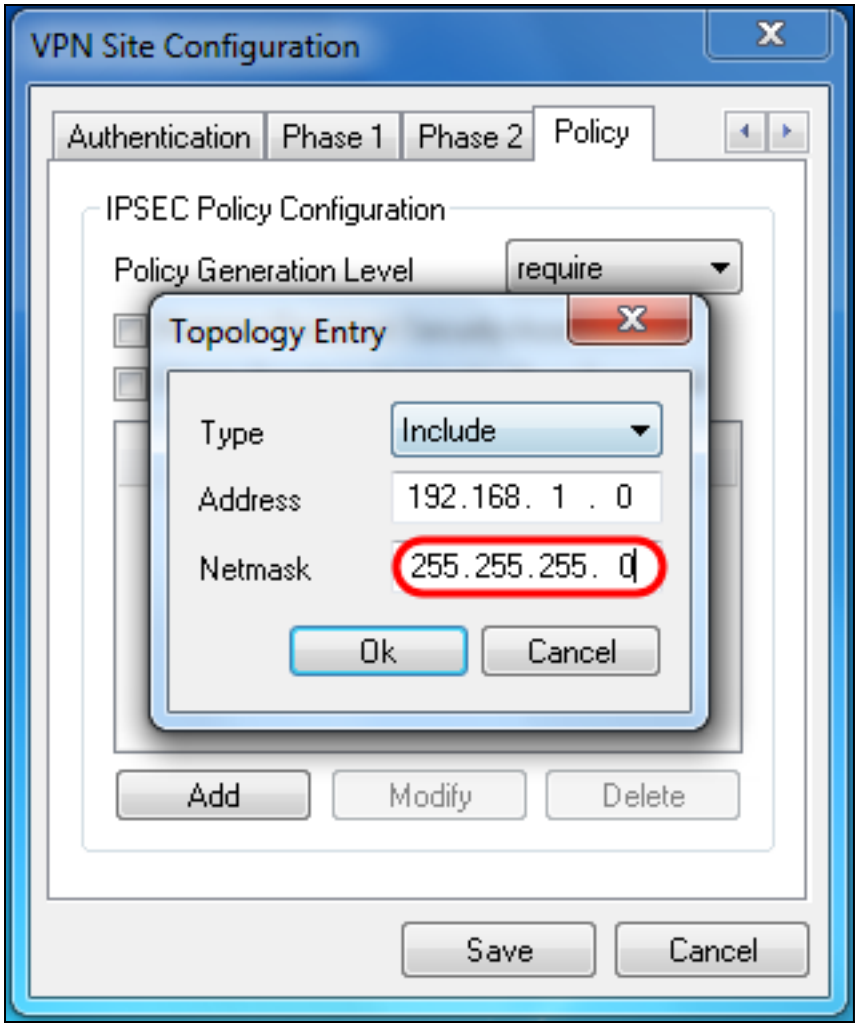
A janela *Topology Entry* é exibida:



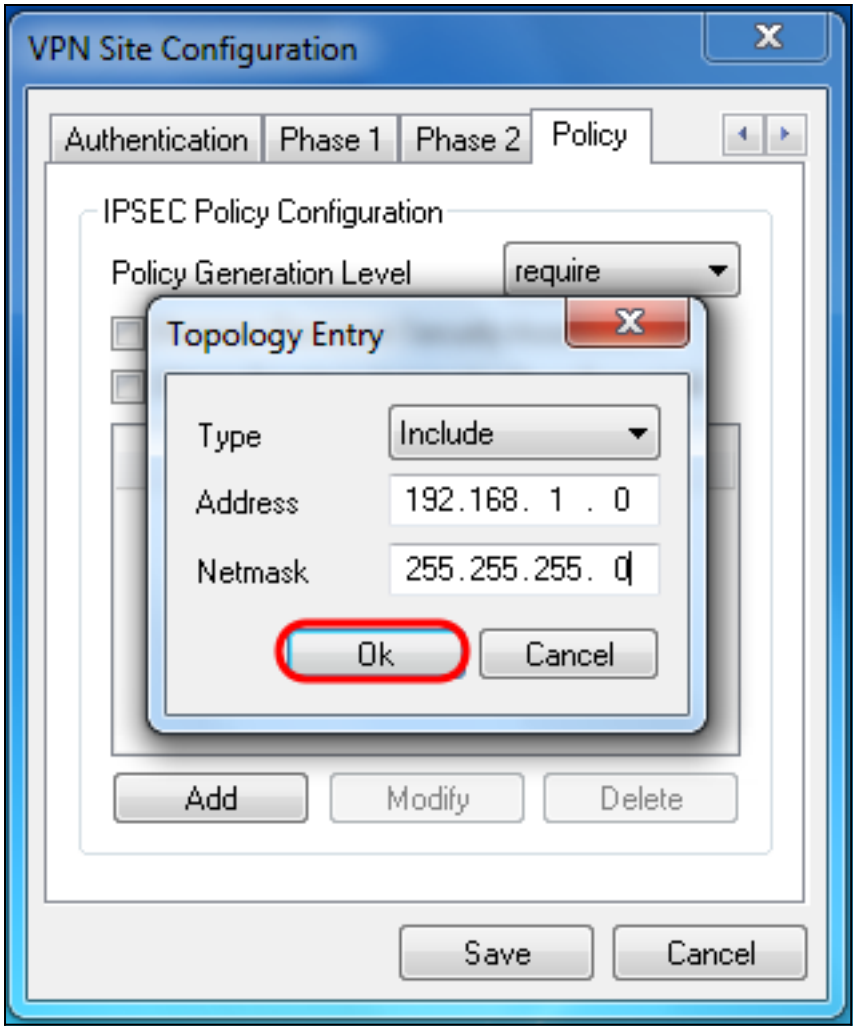
Etapa 17. No campo *Endereço*, digite o ID da sub-rede do RV130/RV130W. O endereço deve corresponder ao campo *IP Address* na Etapa 2 da seção IPSec VPN Server Setup and User Configuration deste documento.



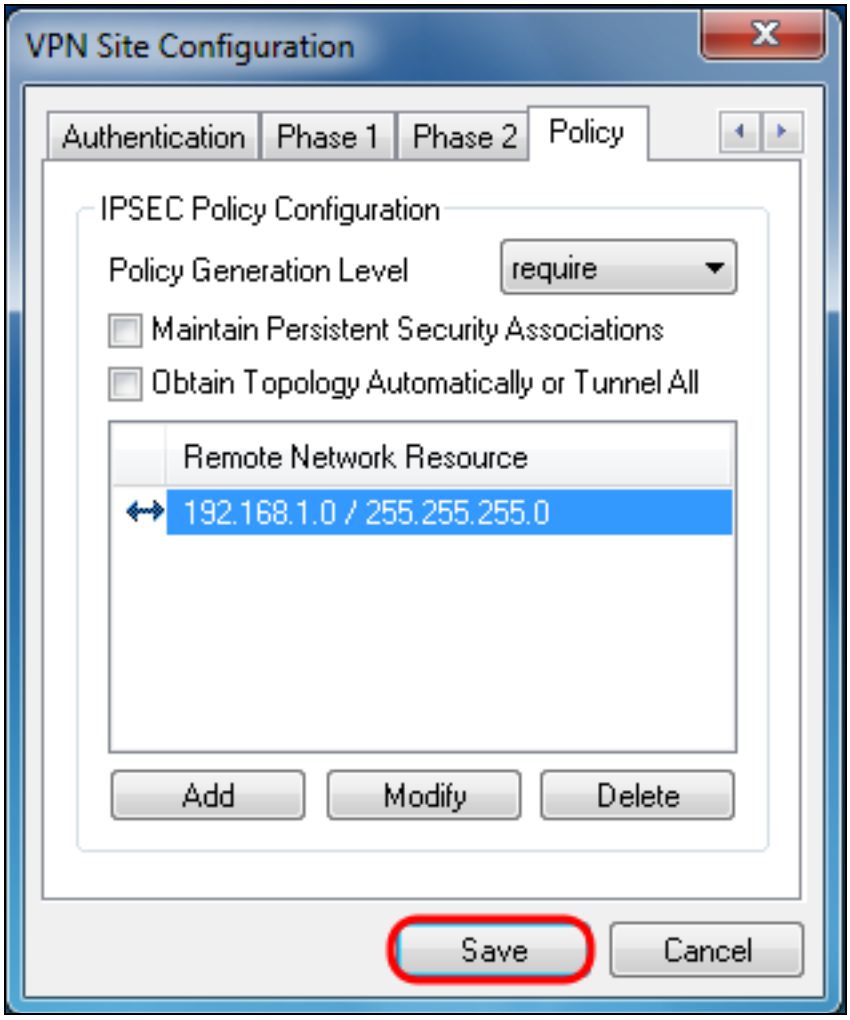
Etapa 18. No campo *Netmask*, insira a máscara de sub-rede da rede local do RV130/RV130W. A máscara de rede deve corresponder ao campo *Subnet Mask* na Etapa 2 da seção IPSec VPN Server User Configuration deste documento.



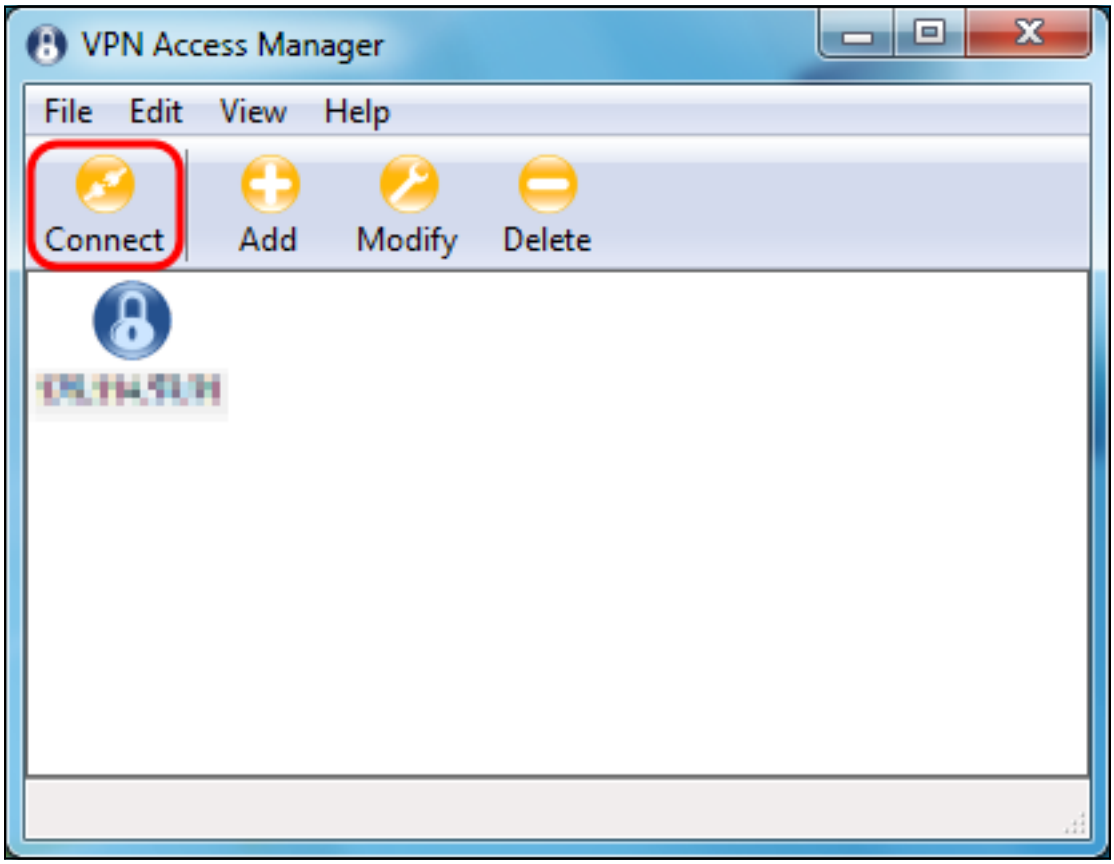
Etapa 19. Clique em **Ok** para terminar de adicionar o recurso de rede remota.



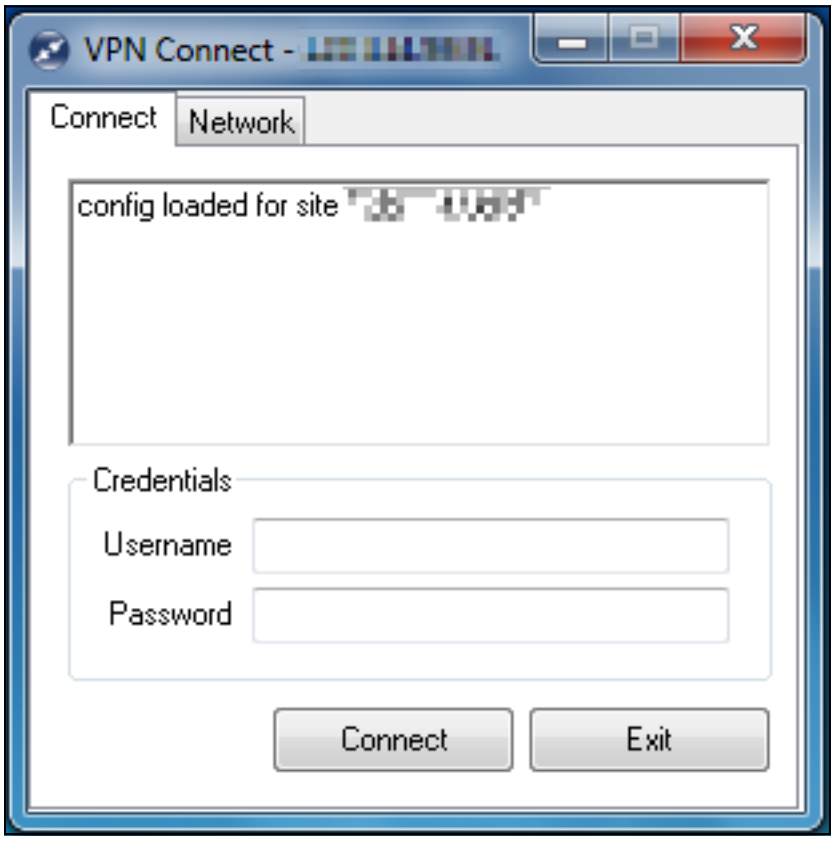
Etapa 20. Clique em **Save** para salvar suas configurações para se conectar ao site VPN.



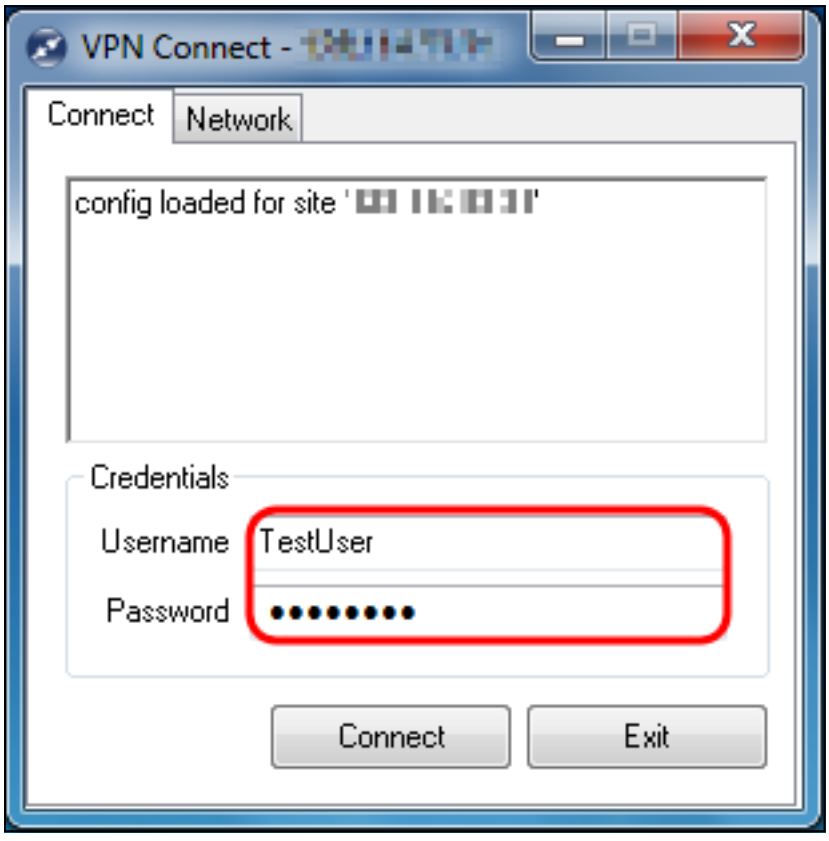
Etapa 21. Retorne à janela *VPN Access Manager* para selecionar o site VPN que você configurou e clique no botão **Connect**.



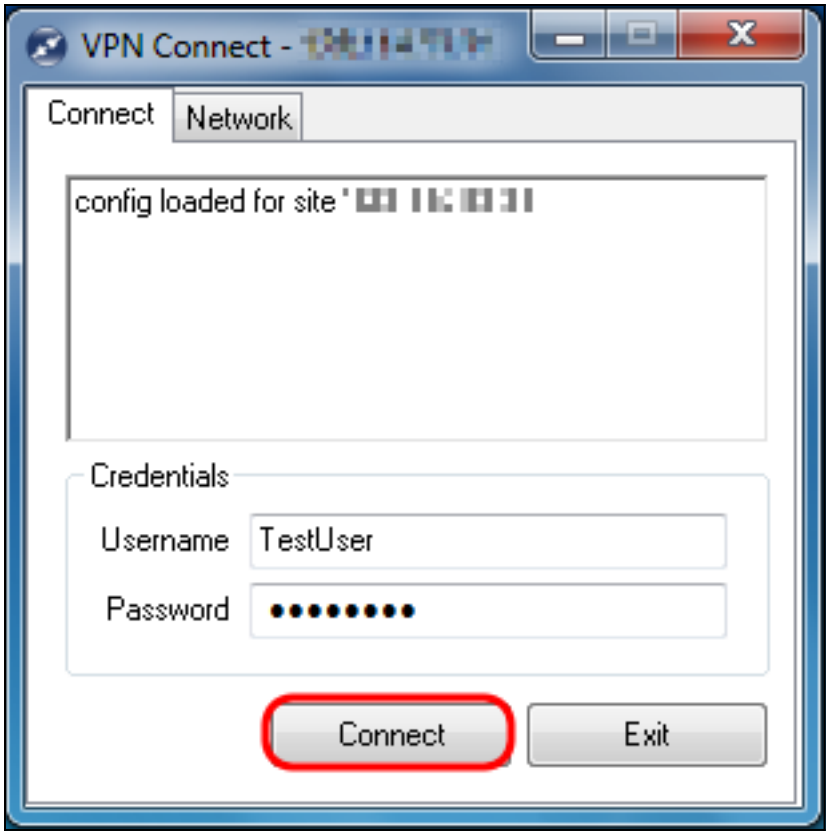
A janela *VPN Connect* é exibida.



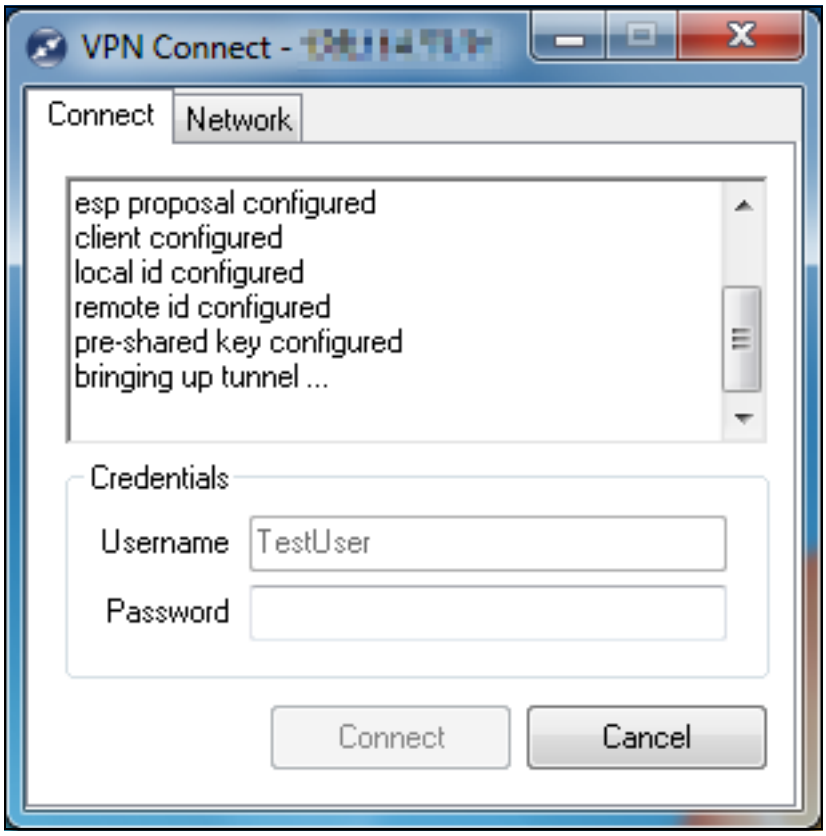
Etapa 22. Na seção *Credenciais*, digite o nome de usuário e a senha da conta que você configurou na Etapa 4 da seção Configuração de Usuário do Servidor VPN IPSec deste documento.

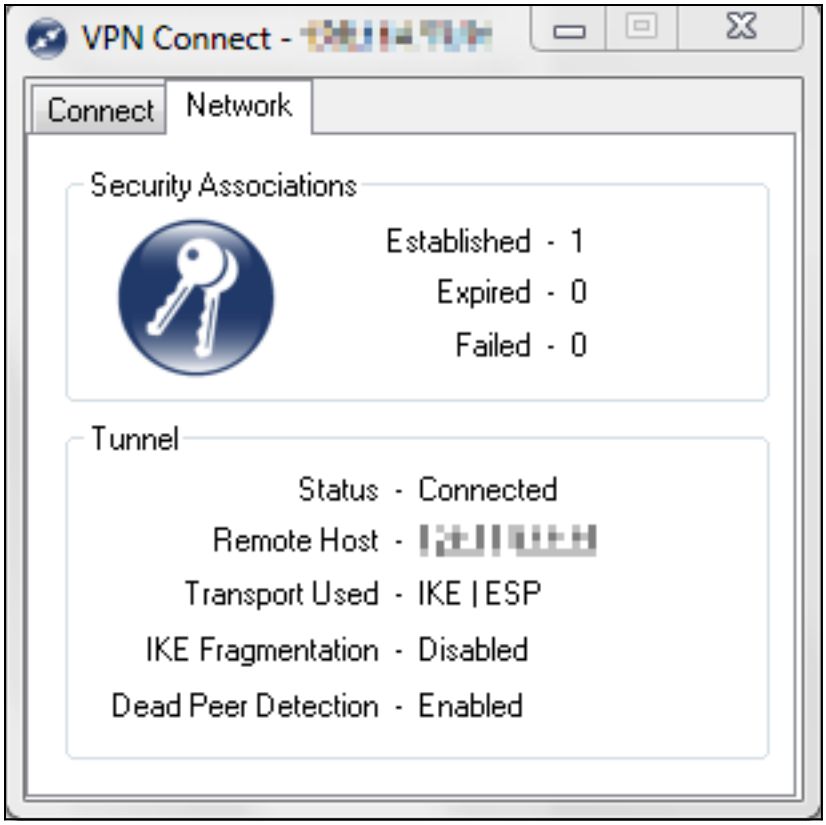


Etapa 23. Clique em **Connect** to VPN no RV130/RV130W.



O túnel VPN IPSec é estabelecido e o cliente VPN pode acessar o recurso atrás da LAN RV130/RV130W.





Exibir um vídeo relacionado a este artigo...

Clique aqui para ver outras palestras técnicas da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.