

Configuração do Shrew VPN Client em RV042, RV042G e RV082 VPN Routers através do Windows

Objetivo

Uma VPN (Virtual Private Network) é um método para que os usuários remotos se conectem virtualmente a uma rede privada pela Internet. Uma VPN Cliente a Gateway conecta o desktop ou laptop de um usuário a uma rede remota usando o software cliente VPN. As conexões VPN de cliente para gateway são úteis para funcionários remotos que desejam se conectar remotamente com segurança à rede do escritório. O Shrew VPN Client é um software configurado em um dispositivo de host remoto que fornece conectividade VPN fácil e segura.

O objetivo deste documento é mostrar como configurar o Shrew VPN Client para um computador que se conecta a um RV042, RV042G ou RV082 VPN Router.

Nota: Este documento pressupõe que você já fez o download do Shrew VPN Client no computador Windows. Caso contrário, você precisará configurar uma conexão VPN de cliente para gateway antes de começar a configurar a VPN de show. Para saber mais sobre como configurar o cliente para a VPN de gateway, consulte [Configurar um túnel de acesso remoto \(cliente para gateway\) para clientes VPN nos roteadores VPN RV042, RV042G e RV082](#).

Dispositivos aplicáveis

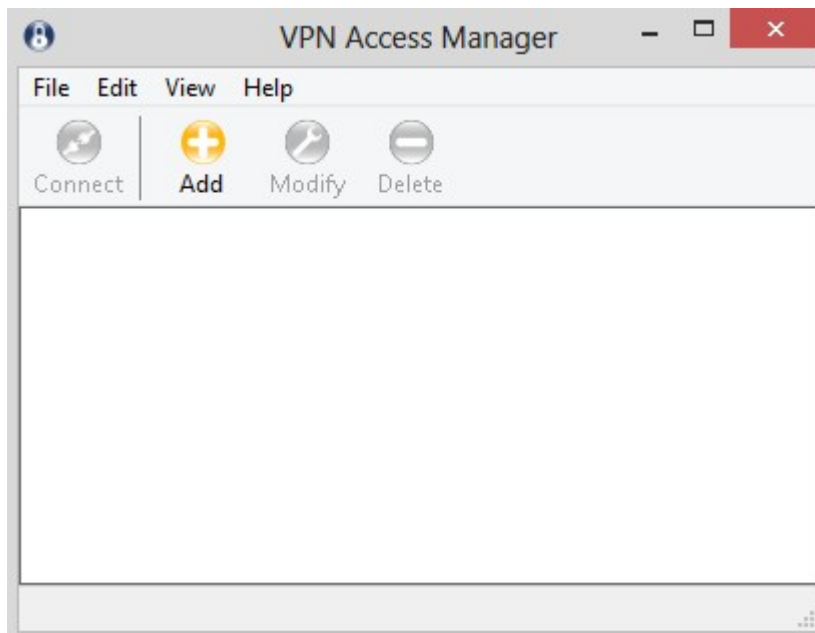
- RV042
- RV042G
- RV082

Versão de software

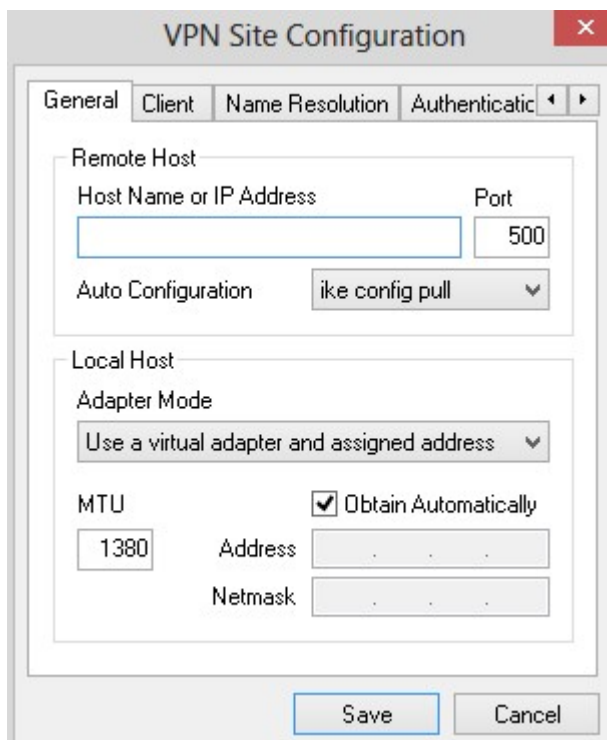
- v4.2.2.08

Configurar a conexão do cliente VPN Shrew no Windows

Etapa 1. Clique no **programa Shrew VPN Client** no computador e abra-o. A janela *Shrew Soft VPN Access Manager* é aberta:

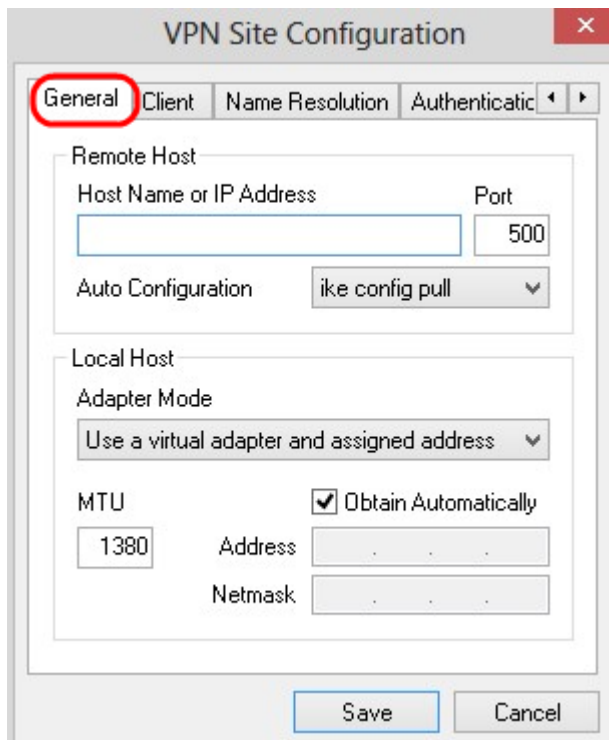


Etapa 2. Clique em Add. A janela *VPN Site Configuration* é exibida:



Configuração geral

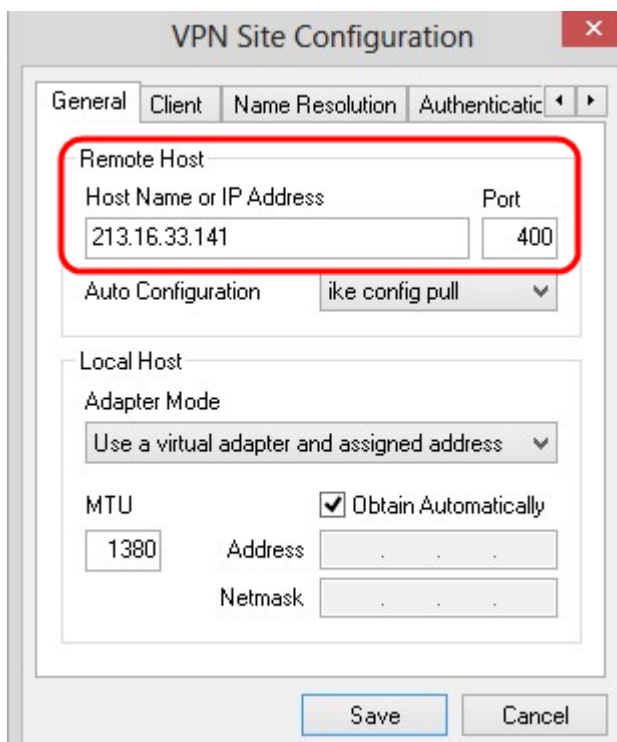
Etapa 1. Clique na guia Geral.



Note: A seção *Geral* é usada para configurar os endereços IP dos hosts remotos e locais. Eles são usados para definir os parâmetros de rede para a conexão Cliente-Gateway.

Etapa 2. No campo *Nome do host ou Endereço IP*, insira o endereço IP do host remoto, que é o endereço IP da WAN configurada.

Etapa 3. No campo *Porta*, insira o número da porta a ser usada para a conexão. O número da porta usada no exemplo mostrado na figura é 400.



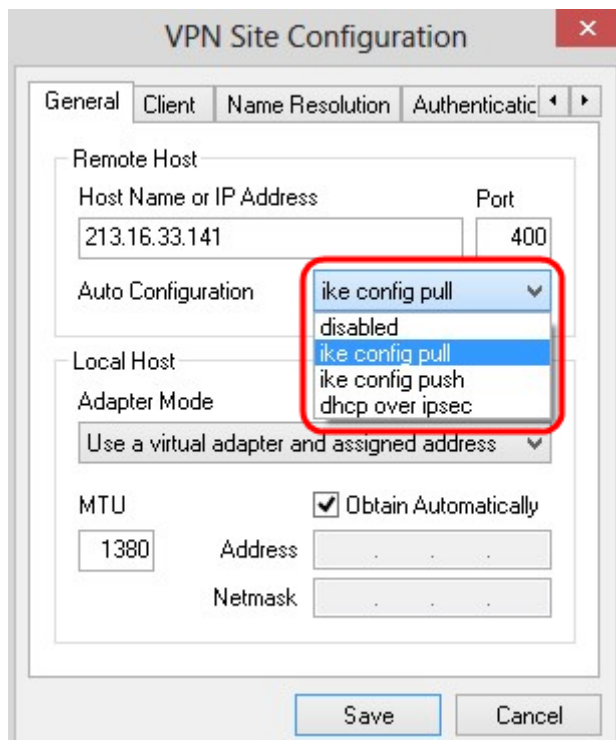
Etapa 4. Na lista suspensa *Configuração automática*, escolha a configuração desejada.

Desabilitado — A opção desabilitada desabilita todas as configurações automáticas do cliente.

IKE Config Pull — Permite definir solicitações de um computador pelo cliente. Com o suporte do método Receber 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 através do processo de configuração. Com o suporte do método Push pelo computador, a solicitação retorna uma lista de configurações suportadas pelo cliente.

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

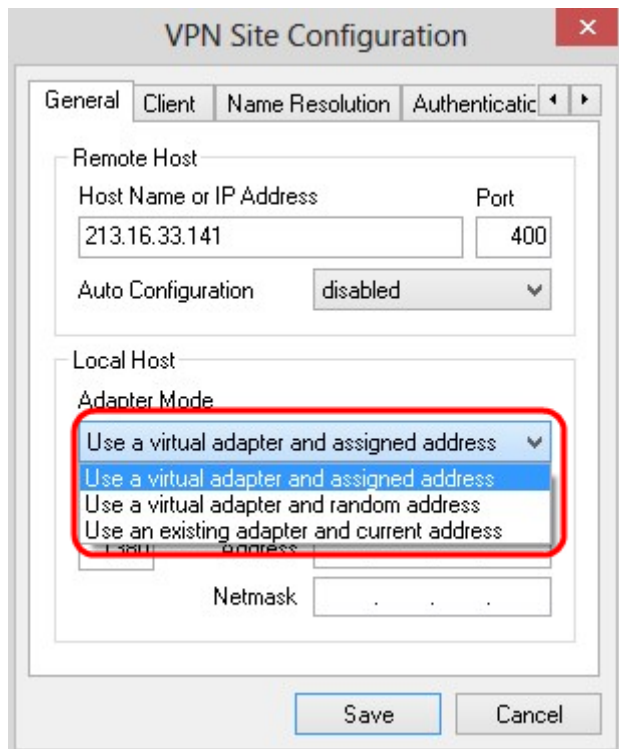


Etapa 5. Na lista suspensa *Modo do adaptador*, escolha o modo de adaptador desejado para o host local com base na Configuração automática.

Usar um adaptador virtual e um endereço atribuído — Permite que o cliente use um adaptador virtual com um endereço especificado.

Usar um adaptador virtual e um endereço aleatório — Permite que o cliente use um adaptador virtual com endereço aleatório.

Usar um adaptador existente e um endereço atual — Usa um adaptador existente e seu endereço. Não é necessário inserir nenhuma informação adicional.



Etapa 6. Insira a MTU (Maximum Transmission Unit, unidade máxima de transmissão) no campo *MTU* se escolher **Usar um adaptador virtual e um endereço atribuído** na lista suspensa *Modo do adaptador* na Etapa 5. A unidade máxima de transmissão ajuda a resolver problemas de fragmentação de IP. O valor padrão é 1380.

Passo 7. (Opcional) Para obter o endereço e a máscara de sub-rede automaticamente pelo servidor DHCP, marque a caixa de seleção **Obter automaticamente**. Esta opção não está disponível para todas as configurações.

Etapa 8. Insira o endereço IP do cliente remoto no campo *Address (Endereço)* se escolher **Use a Virtual Adapter and Assigned Address (Usar adaptador virtual e endereço atribuído)** na lista suspensa *Adapter Mode (Modo adaptador)* na Etapa 5.

Etapa 9. Insira a máscara de sub-rede do endereço IP do cliente remoto no campo *Máscara de rede* se escolher **Usar um adaptador virtual e um endereço atribuído** na lista suspensa *Modo do adaptador* na Etapa 5.

The screenshot shows the 'VPN Site Configuration' dialog box with the 'General' tab selected. The 'Remote Host' section contains 'Host Name or IP Address' (213.16.33.141) and 'Port' (400). The 'Auto Configuration' dropdown is set to 'ike config pull'. The 'Local Host' section has 'Adapter Mode' set to 'Use a virtual adapter and assigned address'. The 'MTU' field is set to '1480' and has a checked checkbox for 'Obtain Automatically'. The 'Address' and 'Netmask' fields are empty. 'Save' and 'Cancel' buttons are at the bottom.

Etapa 10. Clique em **Save (Salvar)** para salvar as configurações.

Configuração do Cliente

Etapa 1. Clique na guia **Cliente**.

The screenshot shows the 'VPN Site Configuration' dialog box with the 'Client' tab selected. The 'Firewall Options' section includes 'NAT Traversal' (enable), 'NAT Traversal Port' (4500), 'Keep-alive packet rate' (15 Secs), 'IKE Fragmentation' (enable), and 'Maximum packet size' (540 Bytes). The 'Other Options' section has three checked checkboxes: 'Enable Dead Peer Detection', 'Enable ISAKMP Failure Notifications', and 'Enable Client Login Banner'. 'Save' and 'Cancel' buttons are at the bottom.

Observação: na seção *Cliente*, você pode configurar as opções Firewall, Dead Peer Detection e ISAKMP (Internet Security Association and Key Management Protocol) Failure Notifications. As configurações definem quais opções de configuração são configuradas manualmente e quais são obtidas automaticamente.

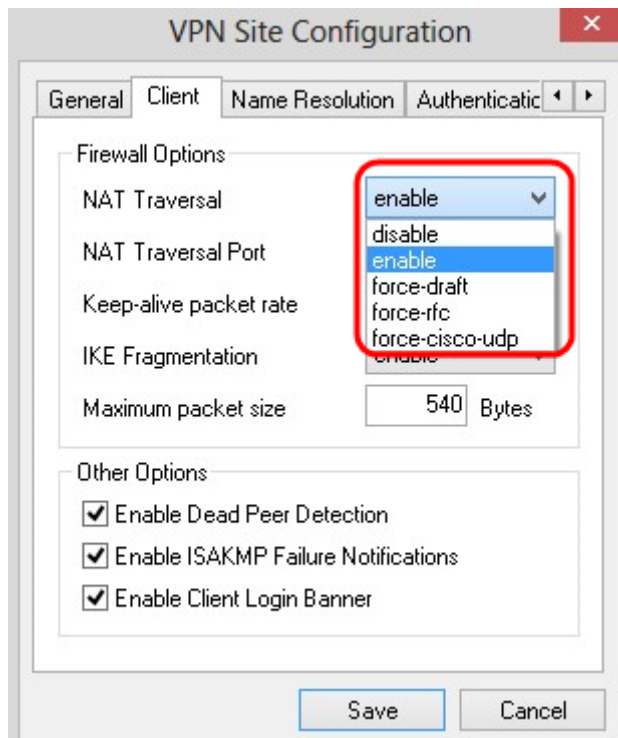
Etapa 2. Escolha a opção de passagem NAT (Network Address Translation, Conversão de endereço de rede) apropriada na lista suspensa *NAT Traversal*.

Desabilitar — O protocolo NAT está desabilitado.

Ativar — A fragmentação IKE só é usada se o gateway indicar suporte através de negociações.

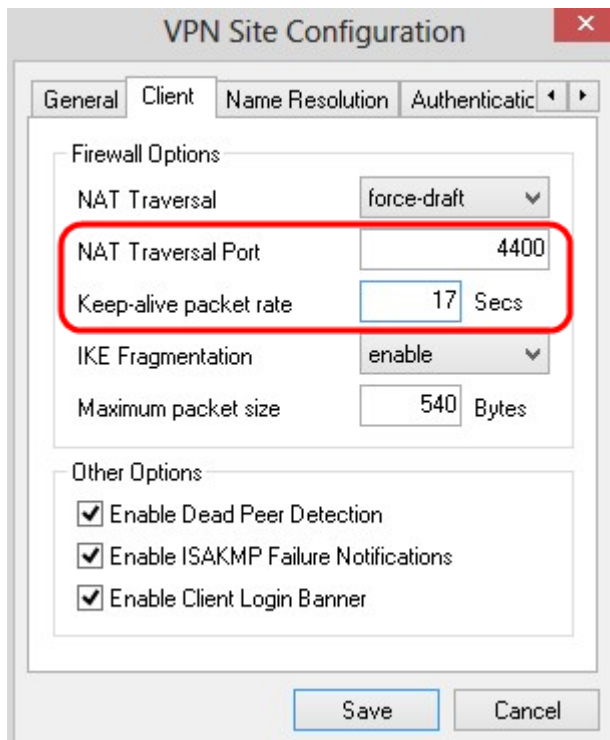
Force Draft — A versão preliminar do protocolo NAT. É usado se o gateway indicar suporte através da negociação ou detecção do NAT.

Force RFC — A versão RFC do protocolo NAT. É usado se o gateway indicar suporte através da negociação ou detecção do NAT.



Etapa 3. Insira a porta UDP para o NAT no campo *Porta de passagem NAT*. O valor padrão é 4500.

Etapa 4. No campo *Keep-alive packet rate*, insira um valor para a taxa de envio dos pacotes de manutenção de atividade. O valor é medido em segundos. O valor padrão é de 30 segundos.

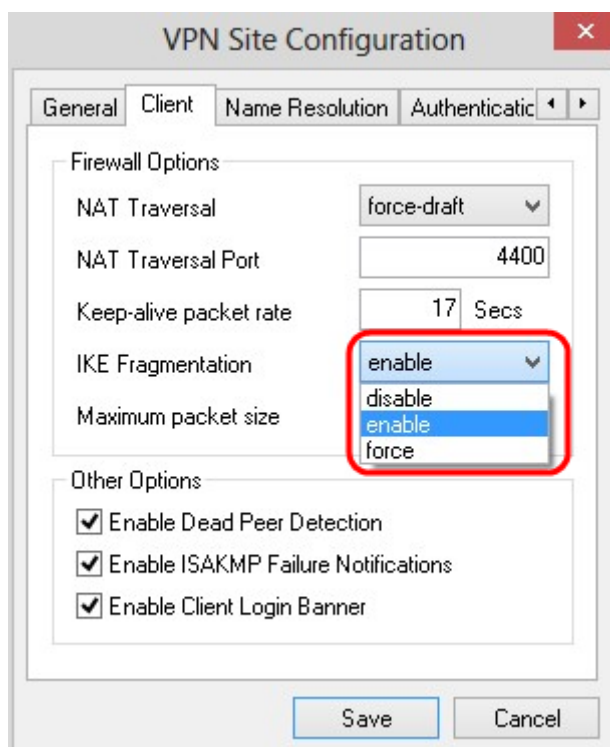


Etapa 5. Na lista suspensa *IKE Fragmentation*, escolha a opção apropriada.

Desabilitar — A fragmentação IKE não é usada.

Ativar — A fragmentação IKE só é usada se o gateway indicar suporte através de negociações.

Force - IKE fragmentation is is used independente das indicações ou da detecção.



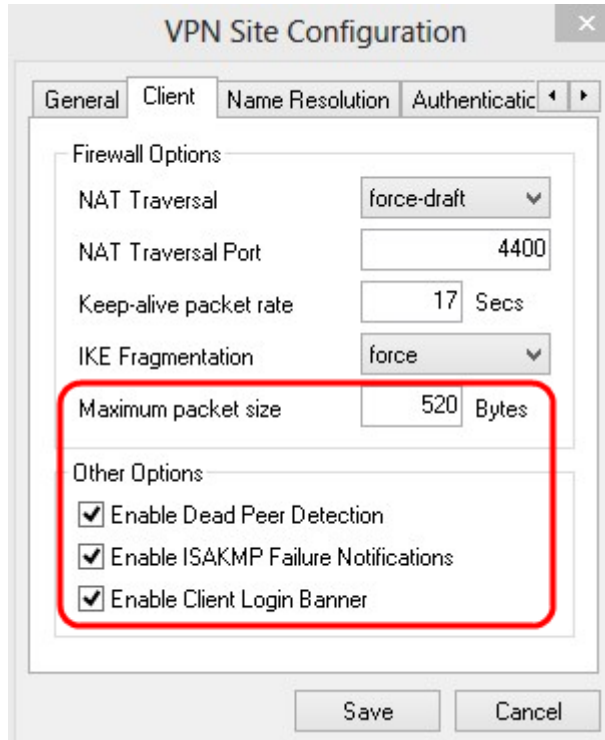
Etapa 6. Insira o tamanho máximo do pacote no campo *Tamanho máximo do pacote* em Bytes. Se o tamanho do pacote for maior que o tamanho máximo do pacote, a fragmentação IKE será executada. O valor padrão é 540 bytes.

Passo 7. (Opcional) Para permitir que o computador e o cliente detectem quando o outro

não puder mais responder, marque a caixa de seleção **Habilitar detecção de peer inoperante**.

Etapa 8. (Opcional) Para enviar notificações de falha pelo cliente VPN, marque a caixa de seleção **Habilitar notificações de falha de ISAKMP**.

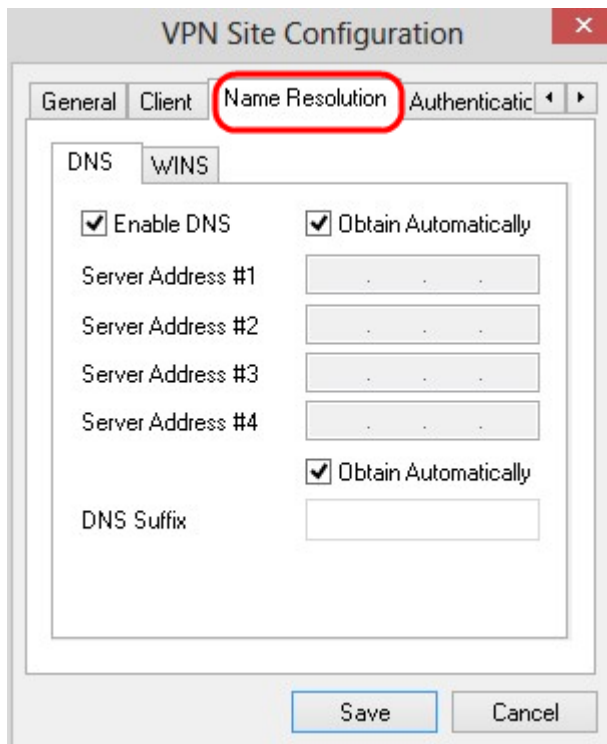
Etapa 9. (Opcional) Para mostrar um banner de login do cliente quando a conexão é estabelecida com o gateway, marque a caixa de seleção **Ativar login do cliente**.



Etapa 10. Clique em **Save (Salvar)** para salvar as configurações.

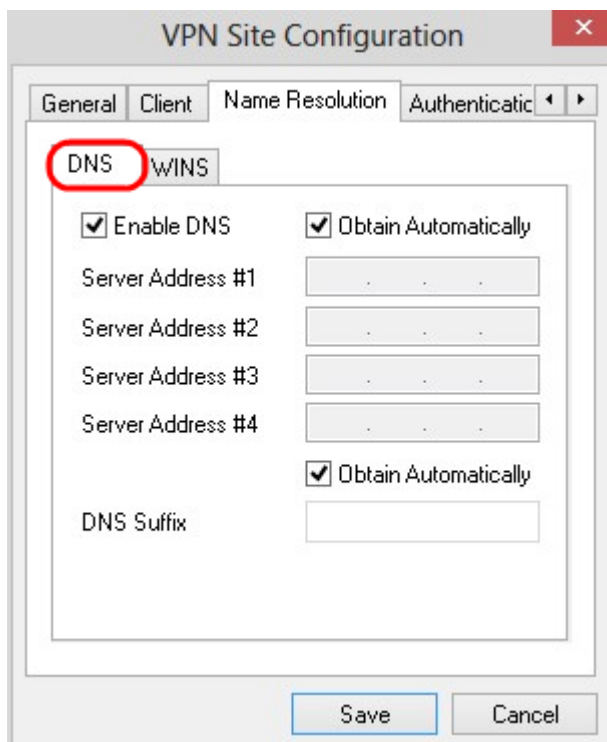
Configuração da resolução de nome

Etapa 1. Clique na guia **Resolução de nomes**.



Note: A seção *Resolução de Nomes* é usada para configurar as configurações de DNS (Domain Name System) e WIN (Windows Internet Name Service).

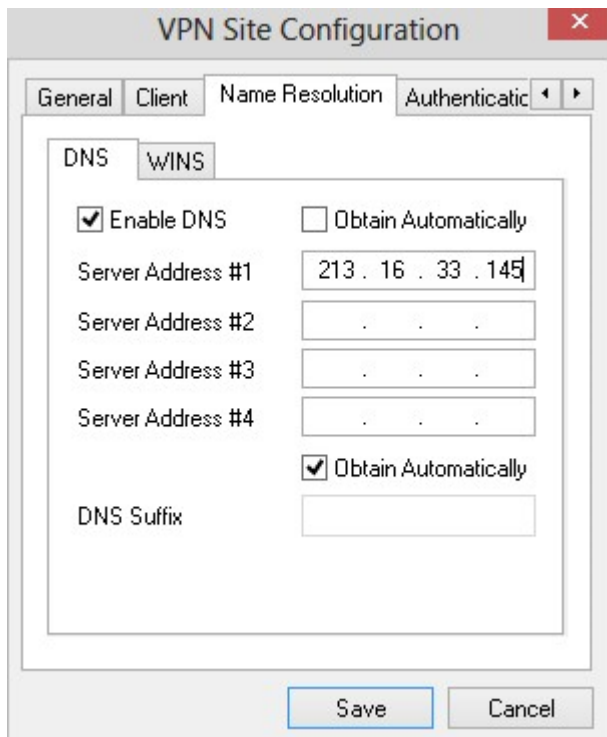
Etapa 2. Clique na guia **DNS**.



Etapa 3. Marque **Habilitar DNS** para habilitar o Domain Name System (DNS).

Etapa 4. (Opcional) Para obter o endereço do servidor DNS automaticamente, marque a caixa de seleção **Obter automaticamente**. Se você escolher essa opção, vá para a Etapa 6.

Etapa 5. Digite o endereço do servidor DNS no campo *Server Address #1* (*Endereço do servidor nº 1*). Se houver outro servidor DNS, insira o endereço desses servidores nos campos *Server Address* restantes.

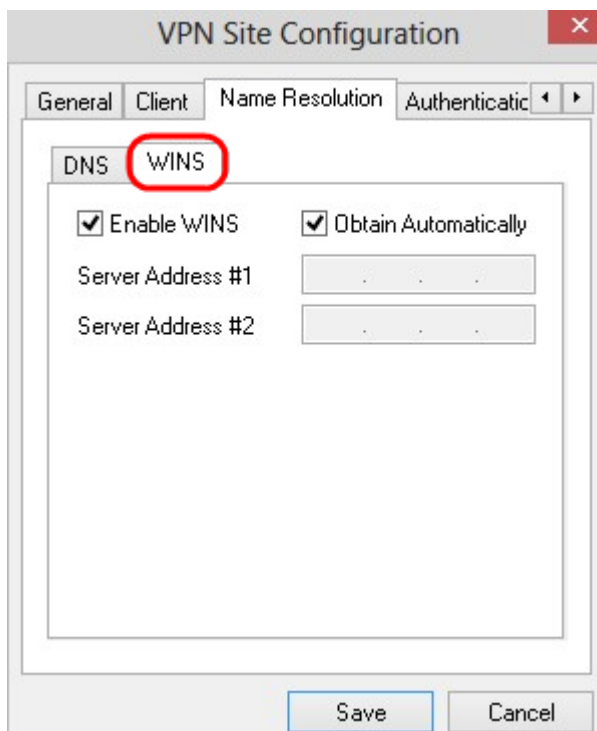


Etapa 6. (Opcional) Para obter o sufixo do servidor DNS automaticamente, marque a caixa de seleção **Obter automaticamente**. Se você escolher essa opção, vá para a Etapa 8.

Passo 7. Digite o sufixo do servidor DNS no campo *Sufixo DNS*.

Etapa 8. Clique em **Save (Salvar)** para salvar as configurações.

Etapa 9. Clique na guia **WINS**.



Etapa 10. Marque **Habilitar WINS** para habilitar o Windows Internet Name Server (WINS).

Etapa 11. (Opcional) Para obter o endereço do servidor DNS automaticamente, marque a caixa de seleção **Obter automaticamente**. Se você escolher essa opção, vá para a Etapa 13.

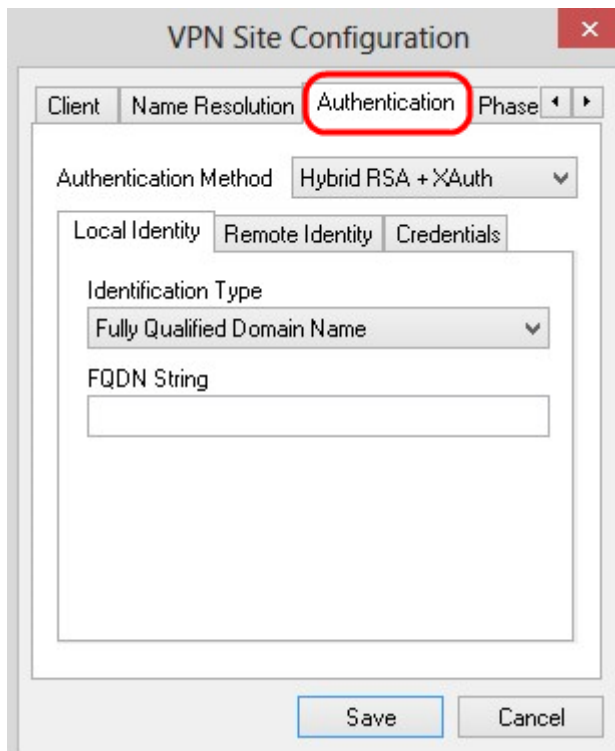
Etapa 12. Digite o endereço do servidor WINS no campo *Server Address #1* (*Endereço do servidor nº 1*). Se houver outros servidores DNS, insira o endereço desses servidores nos campos *Server Address* restantes.



Etapa 13. Clique em Save (Salvar) para salvar as configurações.

Autenticação

Etapa 1. Clique na guia **Autenticação**.



Observação: na seção *Autenticação*, você pode configurar os parâmetros para que o cliente manipule a autenticação quando tentar estabelecer uma SA ISAKMP.

Etapa 2. Escolha o método apropriado de autenticação na lista suspensa *Método de autenticação*.

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

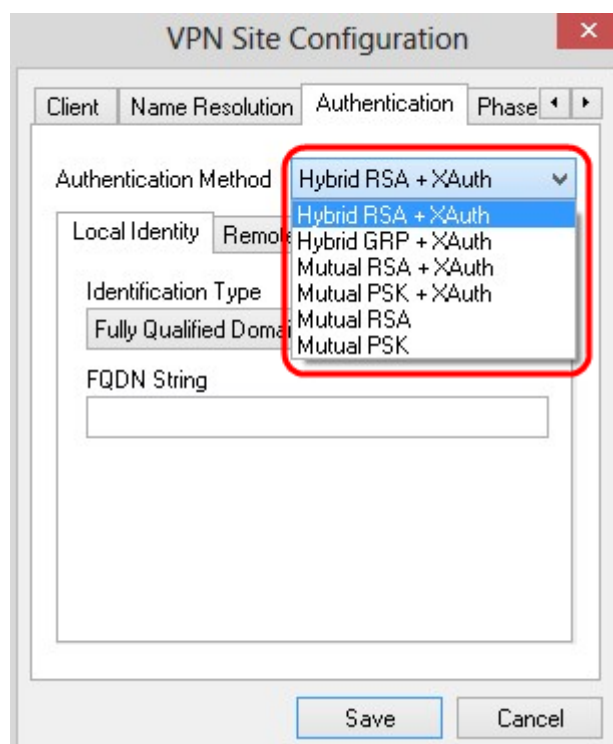
Hybrid GRP + XAuth — A credencial do cliente não é necessária. O cliente autenticará o gateway. As credenciais estarão na forma de arquivo de certificado PEM ou PKCS12 e uma cadeia de caracteres secreta compartilhada.

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

PSK + XAuth mútua — O cliente e o gateway precisam de credenciais para autenticação. As credenciais serão na forma de uma cadeia de caracteres secreta compartilhada.

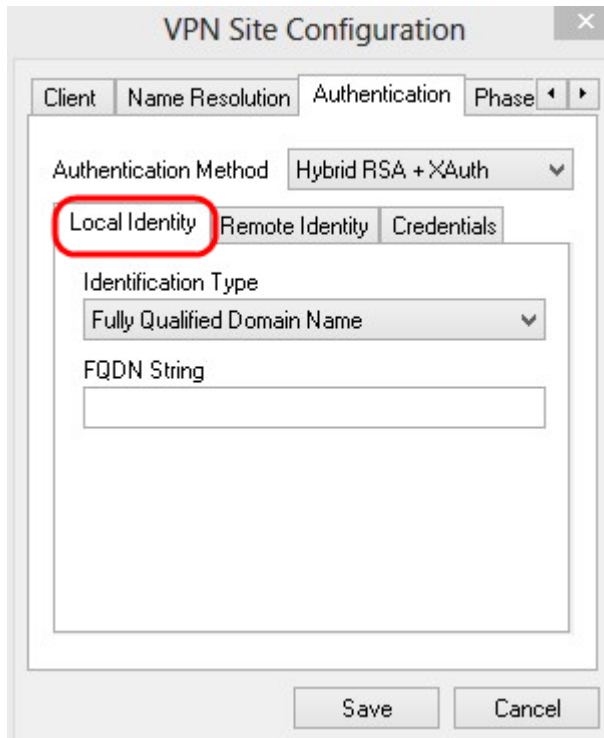
RSA mútuo — o cliente e o gateway precisam de credenciais para autenticação. As credenciais estarão na forma de arquivos de certificado PEM ou PKCS12 ou tipo de chave.

PSK mútuo — O cliente e o gateway precisam de credenciais para autenticação. As credenciais serão na forma de uma cadeia de caracteres secreta compartilhada.



Configuração de identidade local

Etapa 1. Clique na guia **Identidade local**.



Observação: a identidade local define o ID que é enviado ao Gateway para verificação. Na seção *Identidade local*, o Tipo de identificação e a String FQDN (Nome de domínio totalmente qualificado) são configurados para determinar como a ID é enviada.

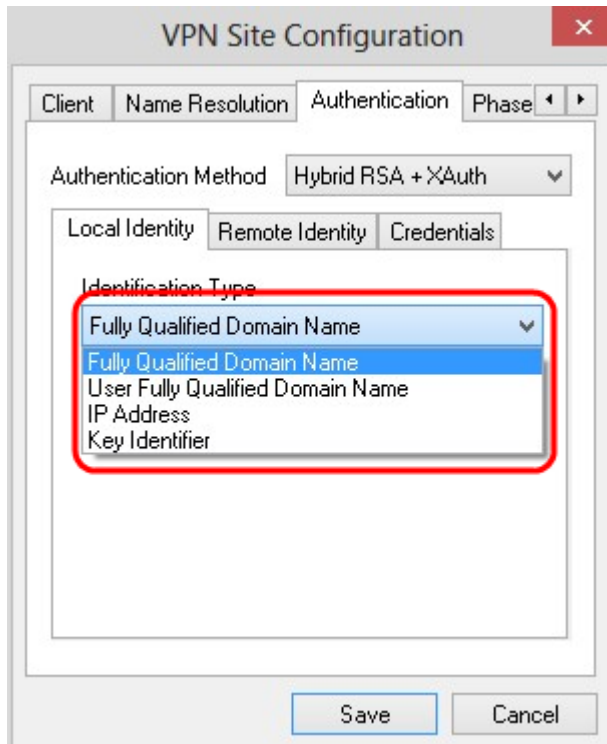
Etapa 2. Escolha a opção de identificação apropriada na lista suspensa *Tipo de identificação*. Nem todas as opções estão disponíveis para todos os modos de autenticação.

Nome de domínio totalmente qualificado — A identificação do cliente da identidade local é baseada em um nome de domínio totalmente qualificado. Se você escolher essa opção, siga a Etapa 3 e vá para a Etapa 7.

Nome de domínio totalmente qualificado do usuário — A identificação do cliente da identidade local é baseada no Nome de domínio totalmente qualificado do usuário. Se você escolher essa opção, siga a Etapa 4 e vá para a Etapa 7.

Endereço IP — A identificação do cliente da identidade local é baseada no endereço IP. Se você marcar **Usar um endereço de host local descoberto**, o endereço IP será descoberto automaticamente. Se você escolher essa opção, siga a Etapa 5 e vá para a Etapa 7.

Identificador de chave — A identificação do cliente local é identificada com base em um identificador de chave. Se você escolher essa opção, siga as etapas 6 e 7.



Etapa 3. Digite o nome de domínio totalmente qualificado como string DNS no campo *String FQDN*.

Etapa 4. Digite o nome de domínio totalmente qualificado do usuário como cadeia de caracteres DNS no campo *String UFQDN*.

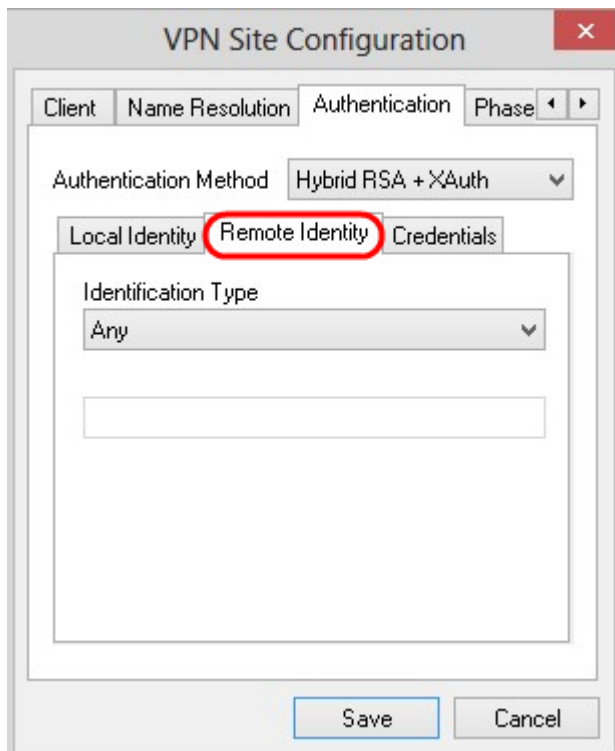
Etapa 5. Digite o endereço IP no campo *String UFQDN*.

Etapa 6. Introduza o identificador de chave para identificar o cliente local na *Cadeia de Identificação de Chave*.

Passo 7. Clique em **Save (Salvar)** para salvar as configurações.

Configuração da identidade remota

Etapa 1. Clique na guia **Remote Identity (Identidade remota)**.



Observação: a identidade remota verifica a ID do Gateway. Na seção *Identidade remota*, o Tipo de identificação é configurado para determinar como a ID é verificada.

Etapa 2. Escolha a opção de identificação apropriada na lista suspensa *Tipo de identificação*.

Any — O cliente remoto pode aceitar qualquer valor ou ID para autenticar.

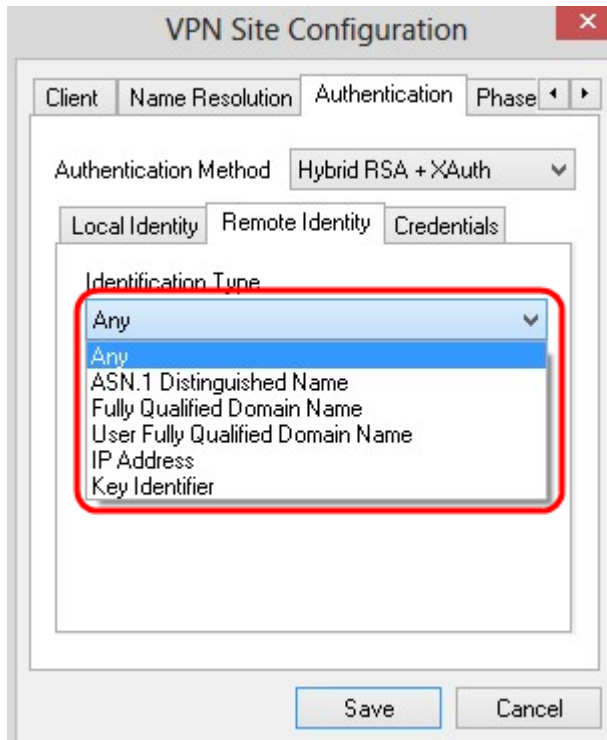
ASN.1 Distinguished Name — O cliente remoto é identificado automaticamente a partir de um arquivo de certificado PEM ou PKCS12. Você só poderá escolher essa opção se escolher um método de autenticação RSA na Etapa 2 da seção *Autenticação*. Marque a caixa de seleção **Usar o assunto no certificado recebido, mas não compare com um valor específico** para receber o certificado automaticamente. Se você escolher essa opção, siga a Etapa 3 e vá para a Etapa 8.

Nome de domínio totalmente qualificado — A identificação do cliente da identidade remota é baseada no Nome de domínio totalmente qualificado. Você só poderá escolher essa opção se escolher um método de autenticação PSK na Etapa 2 da seção *Autenticação*. Se você escolher essa opção, siga a Etapa 4 e vá para a Etapa 8.

Nome de domínio totalmente qualificado do usuário — A identificação do cliente da identidade remota é baseada no Nome de domínio totalmente qualificado do usuário. Você só poderá escolher essa opção se escolher um método de autenticação PSK na Etapa 2 da seção *Autenticação*. Se você escolher essa opção, siga a Etapa 5 e vá para a Etapa 8.

Endereço IP — A identificação do cliente da identidade remota é baseada no endereço IP. Se você marcar **Usar um endereço de host local descoberto**, o endereço IP será descoberto automaticamente. Se você escolher essa opção, siga a Etapa 6 e vá para a Etapa 8.

Identificador de Chave — A identificação do cliente remoto é identificada com base em um identificador de chave. Se você escolher essa opção, siga as etapas 7 e 8.



Etapa 3. Digite a string de DN ASN.1 no campo *String de DN ASN.1*.

Etapa 4. Digite o nome de domínio totalmente qualificado como uma string DNS no campo *FQDN String*.

Etapa 5. Digite o nome de domínio totalmente qualificado do usuário como cadeia de caracteres DNS no campo *String UFQDN*.

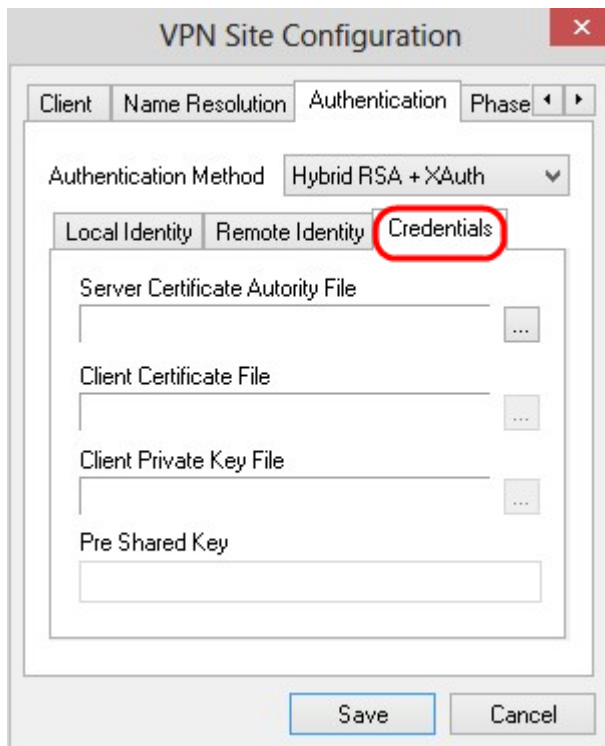
Etapa 6. Insira o endereço IP no campo *String UFQDN*.

Passo 7. Insira o identificador da chave para identificar o cliente local no campo *Cadeia de Caracteres da ID da Chave*.

Etapa 8. Clique em Save (Salvar) para salvar as configurações.

Configuração de credenciais

Etapa 1. Clique na guia **Credenciais**.



Observação: na seção *Credenciais*, a chave pré-compartilhada está configurada.



Etapa 2. Para escolher o Arquivo de certificado do servidor, clique em ... ao lado do campo *Server Certificate Authority File* e escolha o caminho onde você salvou o Server Certificate File em seu PC.

Etapa 3. Para escolher o arquivo de certificado do cliente, clique em ... ao lado do campo *Arquivo de certificado do cliente* e escolha o caminho em que você salvou o Arquivo de certificado do cliente em seu PC.

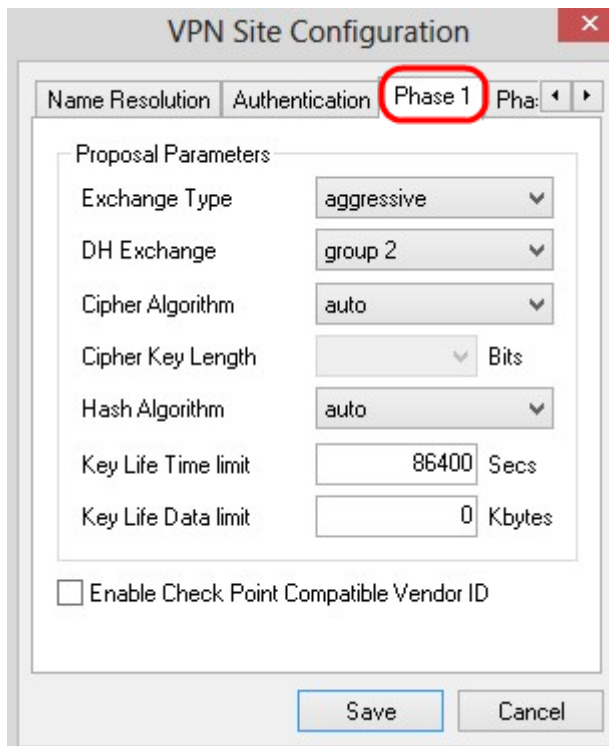
Etapa 4. Para escolher o arquivo de chave privada do cliente, clique em ... ao lado do campo *Arquivo de Chave Privada do Cliente* e escolha o caminho onde você salvou o Arquivo de Chave Privada do Cliente em seu PC.

Etapa 5. Insira a chave pré-compartilhada no campo *PreShared Key*. Essa deve ser a mesma chave que você usa durante a configuração do túnel.

Etapa 6. Clique em **Save (Salvar)** para salvar as configurações.

Configuração da fase 1

Etapa 1. Clique na guia **Fase 1**.

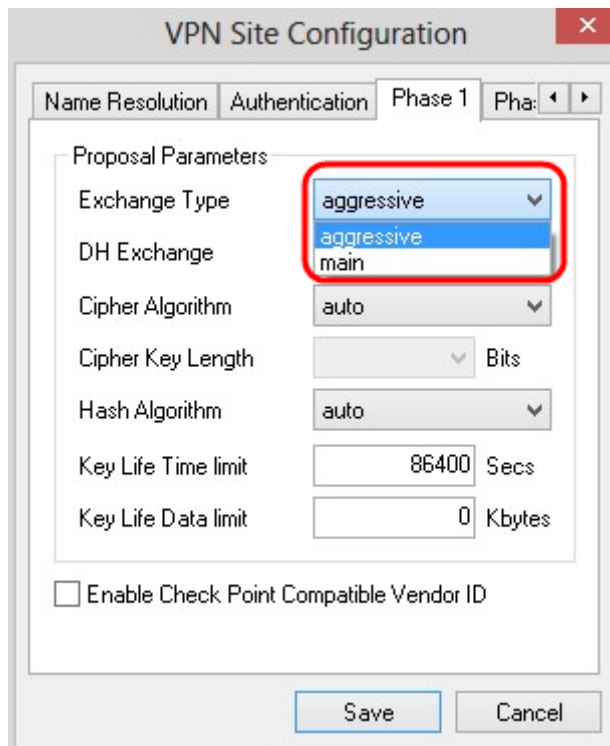


Note: Na seção *Fase 1*, você pode configurar os parâmetros de modo que um SA ISAKMP com o gateway do cliente possa ser estabelecido.

Etapa 2. Escolha o tipo de troca de chave apropriado na lista suspensa *Tipo de troca*.

Principal — A identidade dos pares está protegida.

Agressivo - A identidade dos pares não está protegida.



Etapa 3. Na lista suspensa *DH Exchange*, escolha o grupo apropriado que foi escolhido durante a configuração da conexão VPN.

Etapa 4. Na lista suspensa *Cipher Algorithm*, escolha a opção apropriada que foi escolhida durante a configuração da conexão VPN.

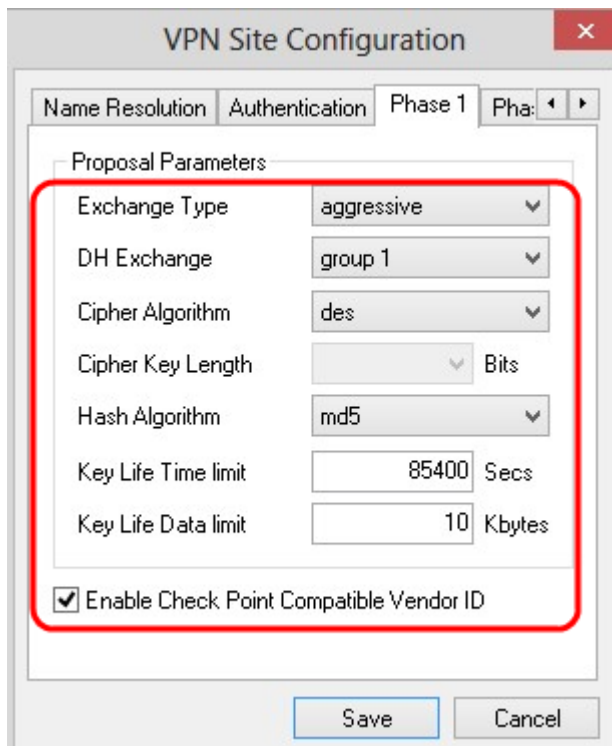
Etapa 5. Na lista suspensa *Comprimento da chave do cifrador*, escolha a opção que corresponde ao comprimento da chave da opção escolhida durante a configuração da Conexão VPN.

Etapa 6. Na lista suspensa *Hash Algorithm*, escolha a opção que foi escolhida durante a configuração da conexão VPN.

Passo 7. No campo *Key Life Time limit*, insira o valor usado durante a configuração da conexão VPN.

Etapa 8. No campo *Key Life Data limit*, insira o valor em kilobytes a serem protegidos. O valor padrão é 0, que desativa o recurso.

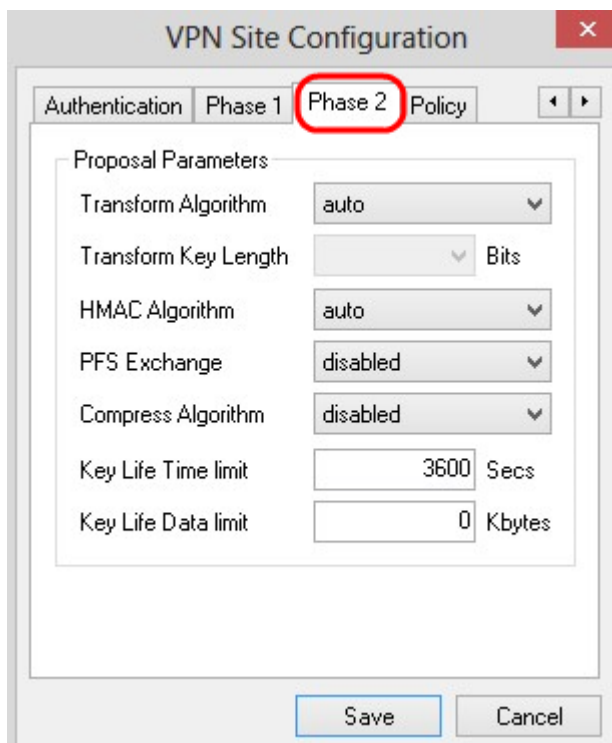
Etapa 9. (Opcional) Marque a caixa de seleção **Enable Check Point Compatible Vendor ID**.



Etapa 10. Clique em **Save (Salvar)** para salvar as configurações.

Configuração da fase 2

Etapa 1. Clique na guia **Fase 2**.



Observação: na seção *Fase 2*, você pode configurar os parâmetros de modo que uma SA IPsec com o gateway cliente remoto possa ser estabelecida.

Etapa 2. Na lista suspensa *Transform Algorithm*, escolha a opção escolhida durante a configuração da conexão VPN.

Etapa 3. Na lista suspensa *Transform Key Length*, escolha a opção que corresponde ao

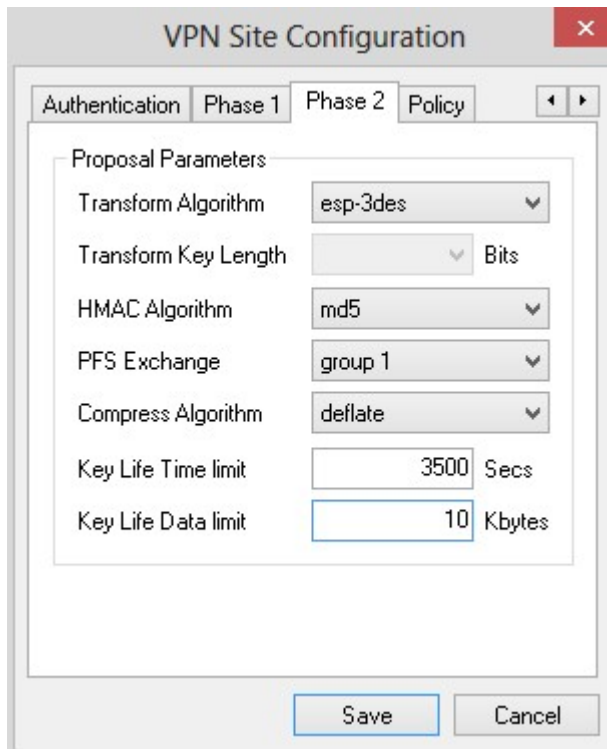
comprimento da chave da opção escolhida durante a configuração da conexão VPN.

Etapa 4. Na lista suspensa *HMAC Algorithm*, escolha a opção escolhida durante a configuração da conexão VPN.

Etapa 5. Na lista suspensa *PFS Exchange*, escolha a opção que foi escolhida durante a configuração da conexão VPN.

Etapa 6. No campo *Key Life Time limit*, insira o valor usado durante a configuração da conexão VPN.

Passo 7. No campo *Key Life Data limit*, insira o valor em kilobytes a serem protegidos. O valor padrão é 0, que desativa o recurso.



The image shows a screenshot of the "VPN Site Configuration" dialog box. The dialog has a title bar with a close button (X) and a tabbed interface with tabs for "Authentication", "Phase 1", "Phase 2", and "Policy". The "Phase 1" tab is selected. Below the tabs is a "Proposal Parameters" section containing several configuration options:

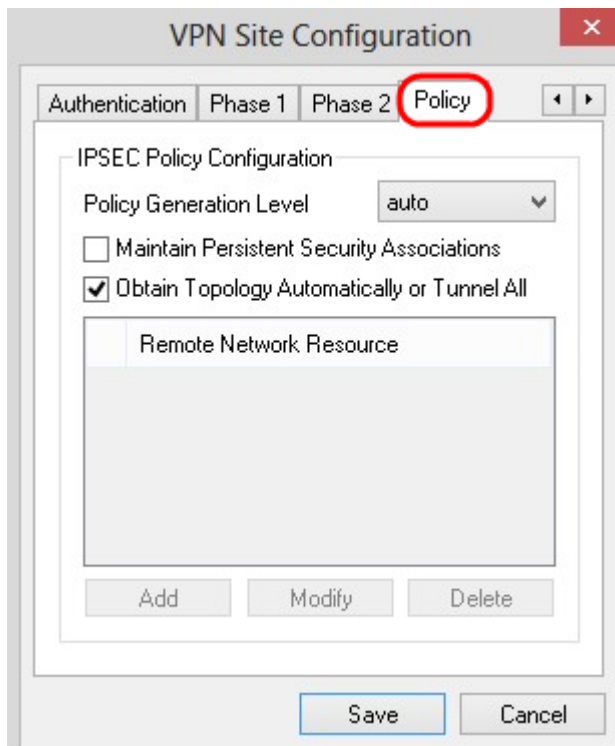
- Transform Algorithm: esp-3des
- Transform Key Length: (dropdown menu) Bits
- HMAC Algorithm: md5
- PFS Exchange: group 1
- Compress Algorithm: deflate
- Key Life Time limit: 3500 Secs
- Key Life Data limit: 10 Kbytes

At the bottom of the dialog are "Save" and "Cancel" buttons.

Etapa 8. Clique em **Save (Salvar)** para salvar as configurações.

Configuração de política

Etapa 1. Clique na guia **Política**.



Observação: na seção *Política*, a Política IPSEC é definida, que é necessária para o cliente se comunicar com o host para a configuração do site.

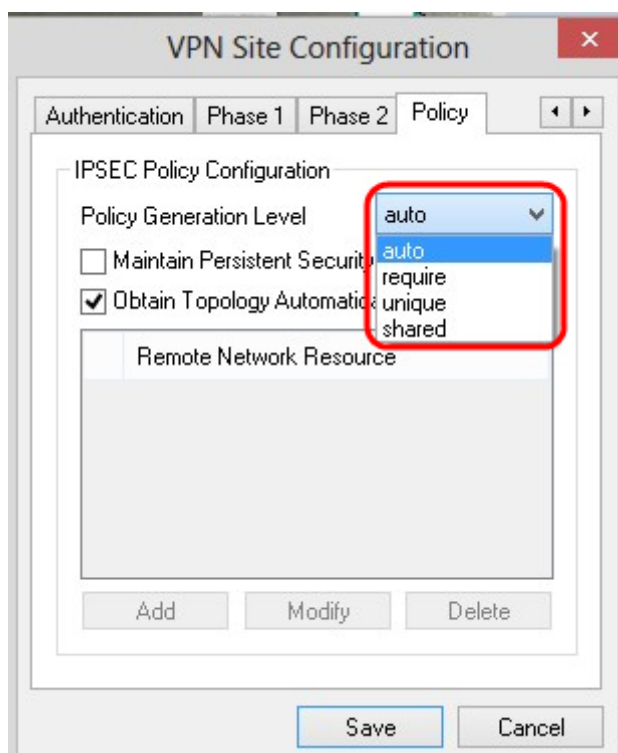
Etapa 2. Na lista suspensa *Nível de geração de política*, escolha a opção apropriada.

Automático — O nível de política IPsec necessário é determinado automaticamente.

Exigir — Uma associação de segurança exclusiva para cada política não é negociada.

Exclusivo — uma associação de segurança exclusiva para cada política é negociada.

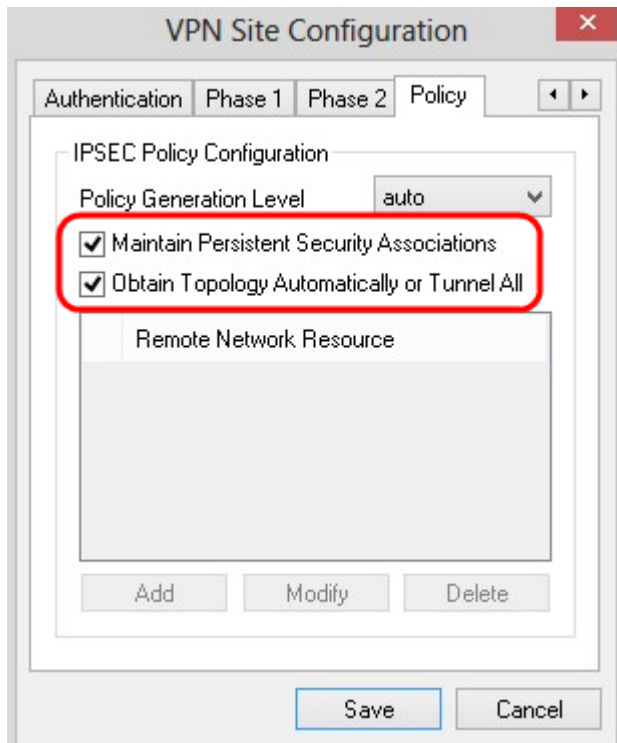
Compartilhado — A política apropriada é gerada no nível necessário.



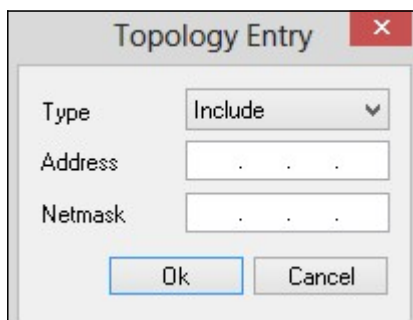
Etapa 3. (Opcional) Para alterar as negociações de IPsec, marque a caixa de seleção

Manter associações de segurança persistentes. Se habilitado, a negociação é feita para cada política diretamente após a conexão. Se desativada, a negociação é feita com base na necessidade.

Etapa 4. (Opcional) Para receber automaticamente uma lista de redes do dispositivo ou para enviar todos os pacotes para o RV0XX por padrão, marque a caixa de seleção **Obter topologia automaticamente ou Túnel tudo**. Se desmarcada, a configuração deve ser executada manualmente. Se esta opção estiver marcada, vá para a Etapa 10.



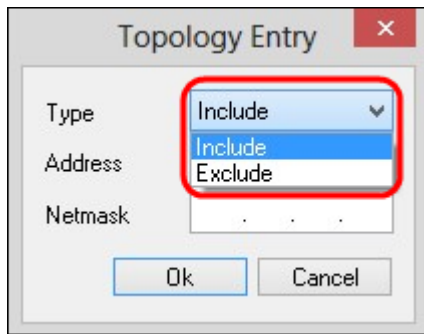
Etapa 5. Clique em **Adicionar** para adicionar uma entrada de Topologia à tabela. A janela *Topology Entry* é exibida.



Etapa 6. Na lista suspensa *Tipo*, escolha a opção apropriada.

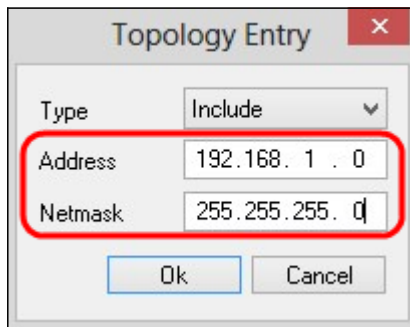
Incluir — A rede é acessada por meio de um gateway VPN.

Excluir — A rede é acessada por meio da conectividade local.

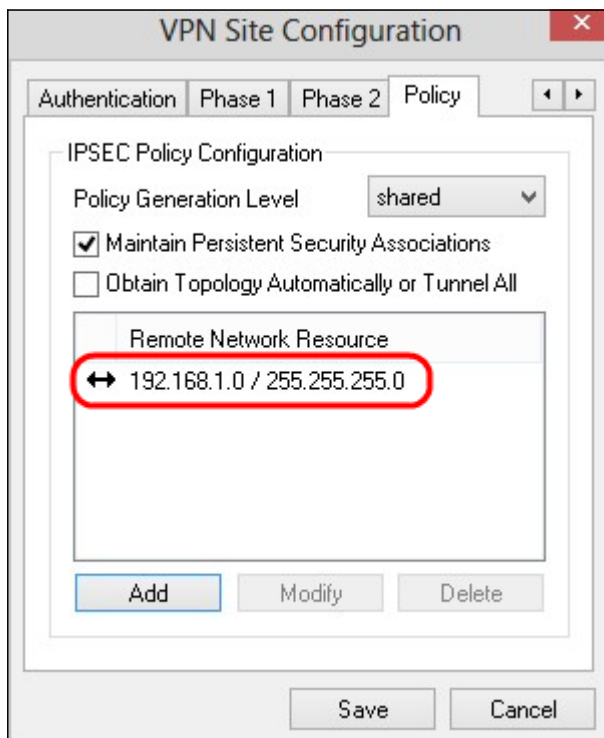


Passo 7. No campo *Address (Endereço)*, insira o endereço IP do RV0XX.

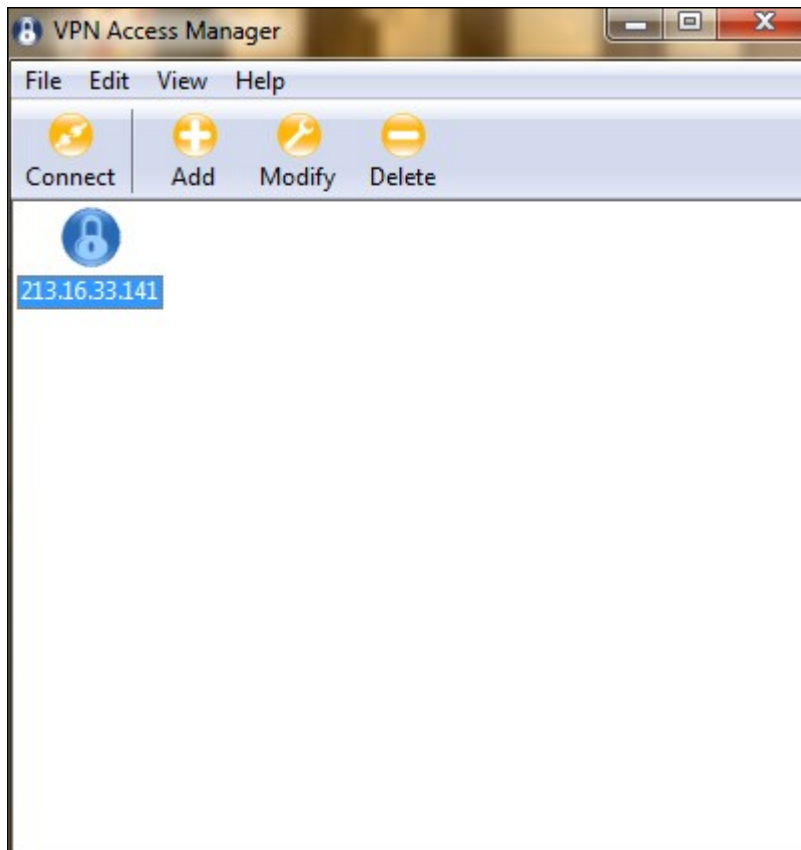
Etapa 8. No campo *Máscara de rede*, insira o endereço da máscara de sub-rede do dispositivo.



Etapa 9. Click **OK**. O endereço IP e o endereço da máscara de sub-rede do RV0XX são exibidos na lista de Recursos de Rede Remota.



Etapa 10. Clique em **Save**, que retorna o usuário para a janela *VPN Access Manager* onde a nova conexão VPN é exibida.

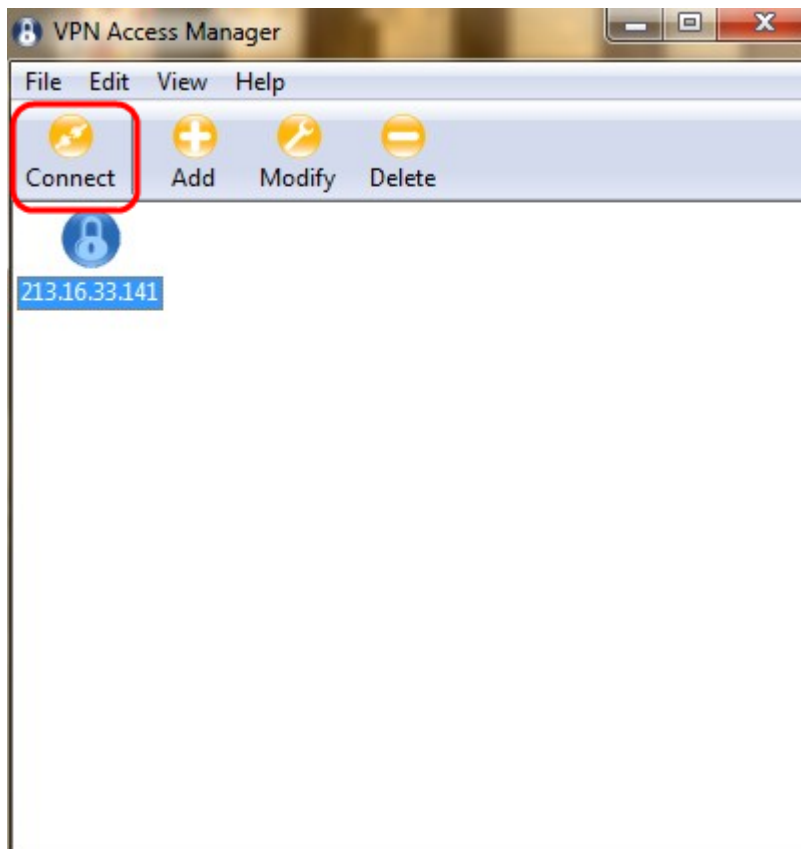


CONNECT

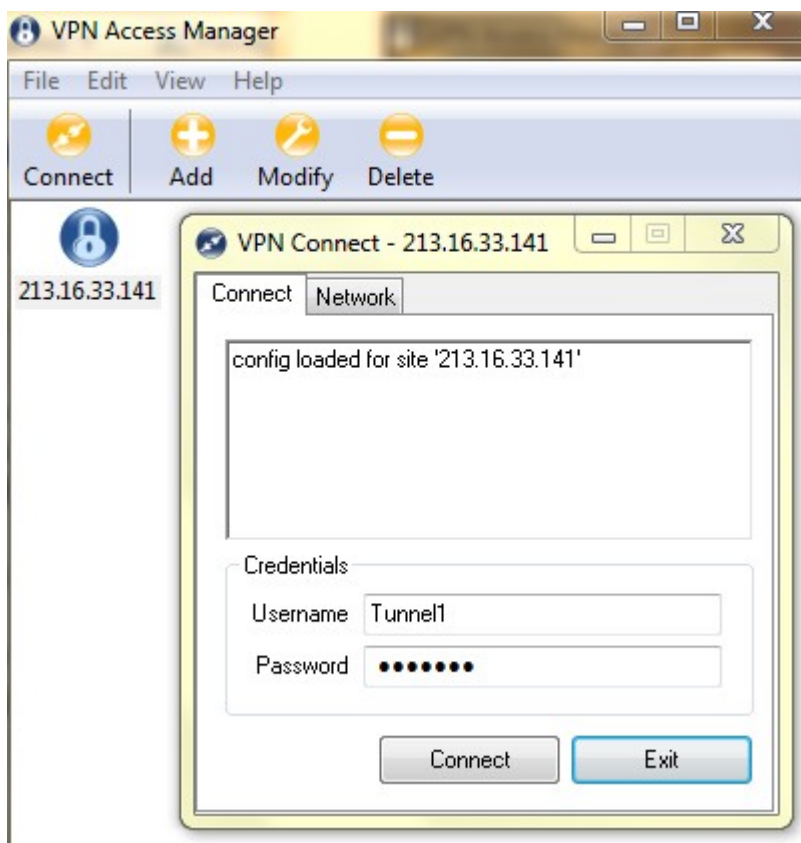
Esta seção explica como configurar a conexão VPN depois que todas as configurações forem configuradas. As informações de login necessárias são as mesmas do VPN Client Access configurado no dispositivo.

Etapa 1. Clique na conexão VPN desejada.

Etapa 2. Clique em Conectar.



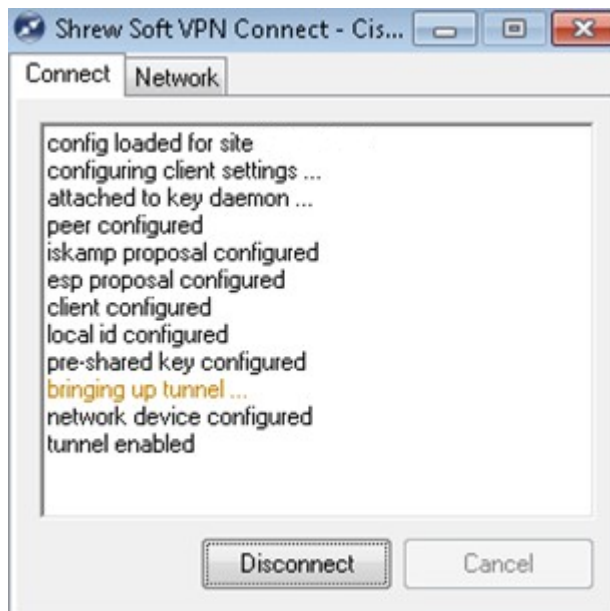
A janela *VPN Connect* é exibida:



Etapa 3. Digite o nome de usuário da VPN no campo *Nome de usuário*.

Etapa 4. Digite a senha para a conta de usuário VPN no campo *Senha*.

Etapa 5. Clique em Conectar. A janela *Shrew Soft VPN Connect* é exibida:



Etapa 6. (Opcional) Para desabilitar a conexão, clique em **Desconectar**.

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.