Configurando o Shrew Soft VPN Client com RV160 e RV260

Objetivo

O objetivo deste documento é mostrar como configurar as configurações necessárias para conectar o cliente VPN Shrew Soft via RV160 ou RV260 Series Routers.

Introdução aos conceitos básicos de VPN

Uma VPN (Virtual Private Network) é uma excelente maneira de conectar usuários remotos a uma rede segura. Ele estabelece uma conexão criptografada em uma rede menos segura como a Internet.

Um túnel VPN estabelece uma rede privada que pode enviar dados com segurança usando criptografia e autenticação. Os escritórios corporativos frequentemente usam uma conexão VPN, pois ela é útil e necessária para permitir que seus funcionários tenham acesso a seus recursos internos, mesmo que eles estejam fora do escritório.

O roteador RV160 suporta até 10 túneis VPN, e o RV260 suporta até 20.

Este artigo o guiará pelas etapas necessárias para configurar o roteador RV160/RV260 e o cliente Shrew Soft VPN. Você aprenderá como criar um grupo de usuários, uma conta de usuário, um perfil IPsec e um perfil Cliente a Site. No cliente Shrew Soft VPN, você aprenderá como configurar as guias Geral, Cliente, Resolução de Nomes, Autenticação, Fase 1 e Fase 2.

Quais são os prós e contras se eu quiser usar uma VPN?

As VPNs abordam cenários de casos de uso reais comuns a muitos setores e tipos de negócios. A tabela abaixo mostra alguns dos prós e contras do uso de uma VPN.

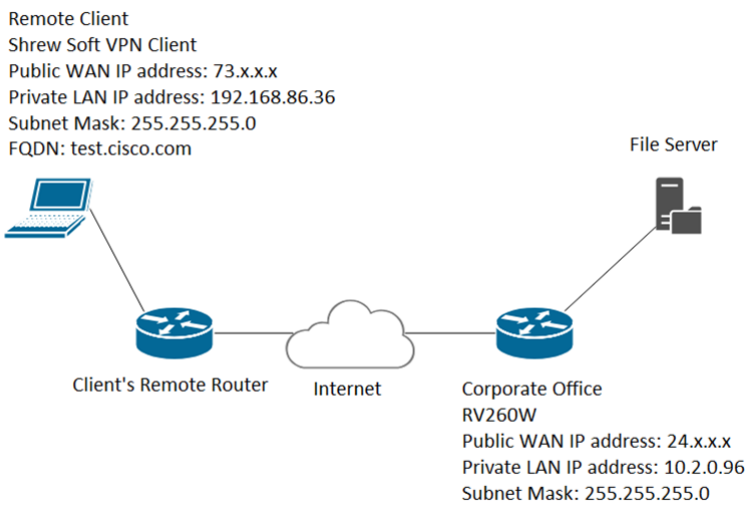
Pros	Cons
Fornece comunicações seguras, conveniência e acessibilidade com direitos de acesso personalizados para usuários individuais, como funcionários, contratados ou parceiros.	A velocidade da conexão pode ser lenta. A criptografia mais forte requer tempo e recursos para garantir o anonimato e a segurança. A criptografia do tráfego de rede geralmente exige um pouco mais de sobrecarga. Você pode encontrar alguns provedores de VPN que mantêm uma boa velocidade de conexão enquanto mantém o anonimato e a segurança, mas geralmente são serviços pagos.
Aumenta a produtividade	Possível risco à segurança devido

estendendo a rede corporativa e os aplicativos.	a configurações incorretas. Projetar e implementar uma VPN pode ser complicado. É necessário confiar a um profissional experiente para configurar sua VPN para garantir que sua rede não seja comprometida.
Reduz os custos de comunicação e aumenta a flexibilidade.	Se ocorrer uma situação em que haja necessidade de adicionar uma nova infraestrutura ou um novo conjunto de configurações, problemas técnicos podem surgir devido à incompatibilidade, especialmente se envolver produtos ou fornecedores diferentes daqueles que você já está usando.
A localização geográfica real dos usuários é protegida e não exposta a redes públicas ou compartilhadas como a Internet.	
Protege dados e recursos de rede confidenciais.	
Uma VPN permite que novos usuários ou um grupo de usuários sejam adicionados sem a necessidade de componentes adicionais ou de uma configuração complicada.	

Topologia

Essa é uma topologia simples da rede.

Note: O endereço IP público da WAN foi apagado.



Dispositivos aplicáveis

- RV160
- RV260

Versão de software

- 1.0.0.xx (RV160 e RV260)
- 2.2.1 é recomendado, pois 2.2.2 pode ter problemas de conectividade com nossos roteadores (Shrew Soft VPN Client Download)

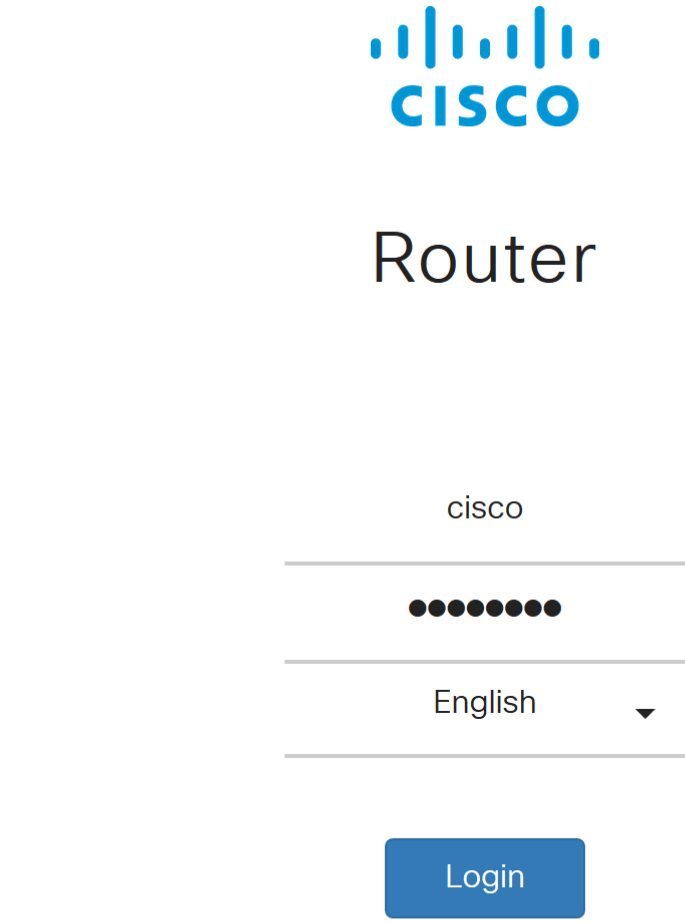
Table Of Contents

Criando grupos de usuários

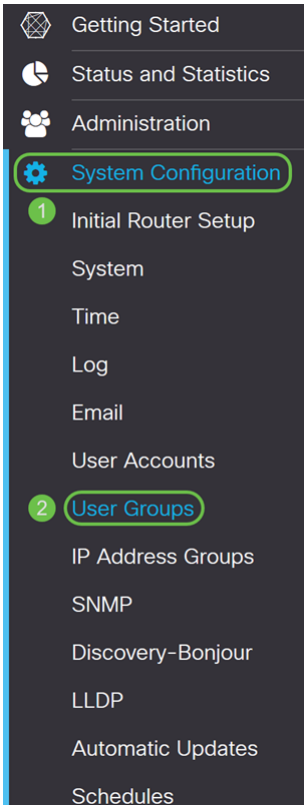
Nota importante: Deixe a conta de administrador padrão no grupo de administração e crie uma nova conta de usuário e um novo grupo de usuários para Shrew Soft. Se você mover

sua conta de administrador para um grupo diferente, você impedirá que você faça login no roteador.

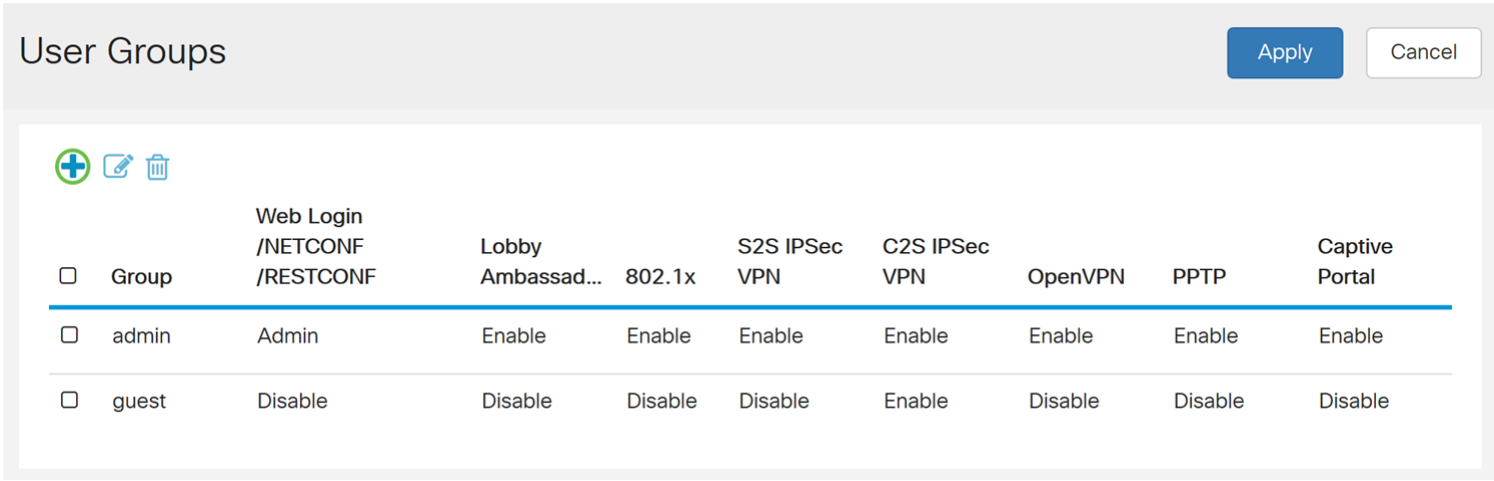
Etapa 1. Faça login na página de configuração da Web.



Etapa 2. Navegue até **Configuração do sistema > Grupos de usuários**.

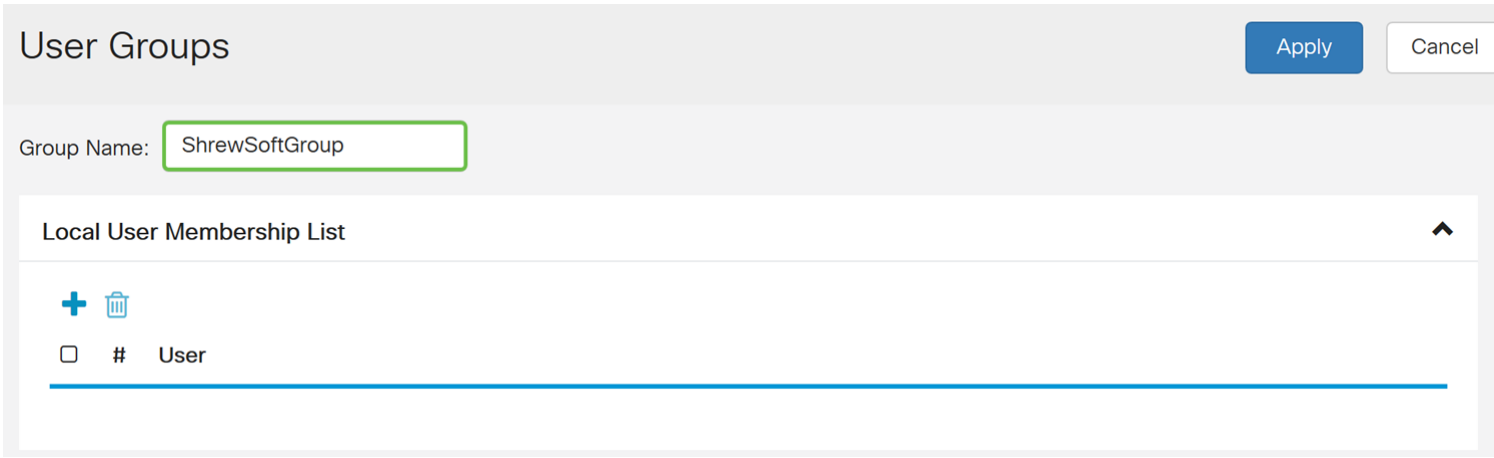


Etapa 3. Clique no ícone **de mais** para adicionar um novo grupo de usuários.

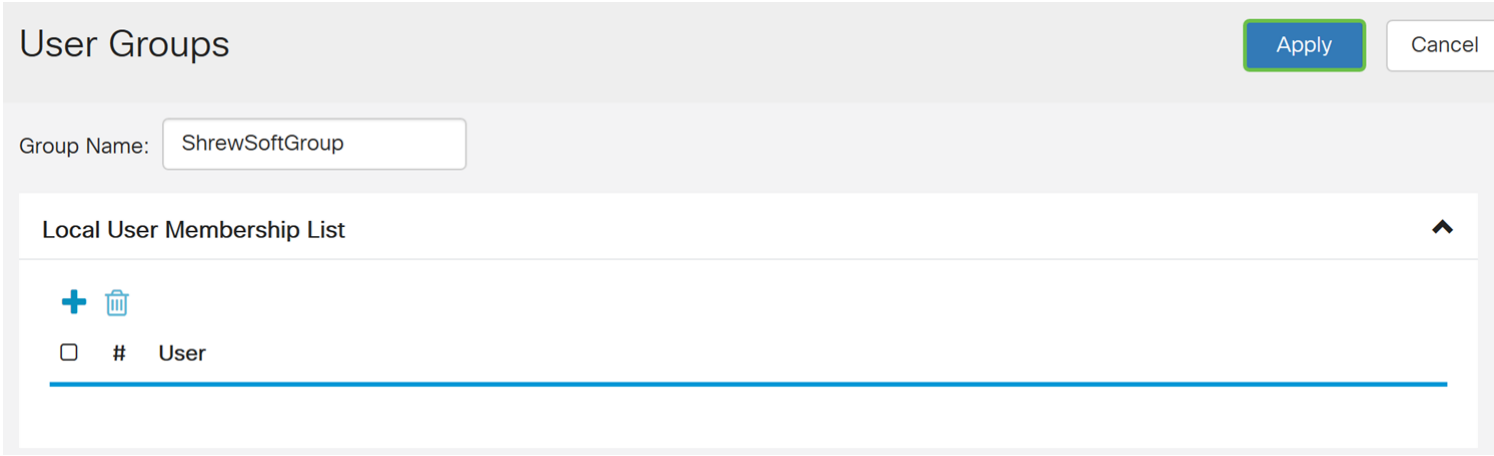


Etapa 4. Digite um nome para o grupo no campo *Nome do grupo*.

Usaremos **ShrewSoftGroup** como exemplo.

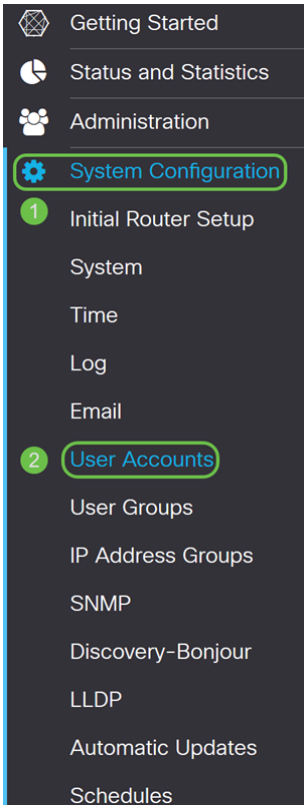


Etapa 5. Pressione **Apply** para criar um novo grupo.

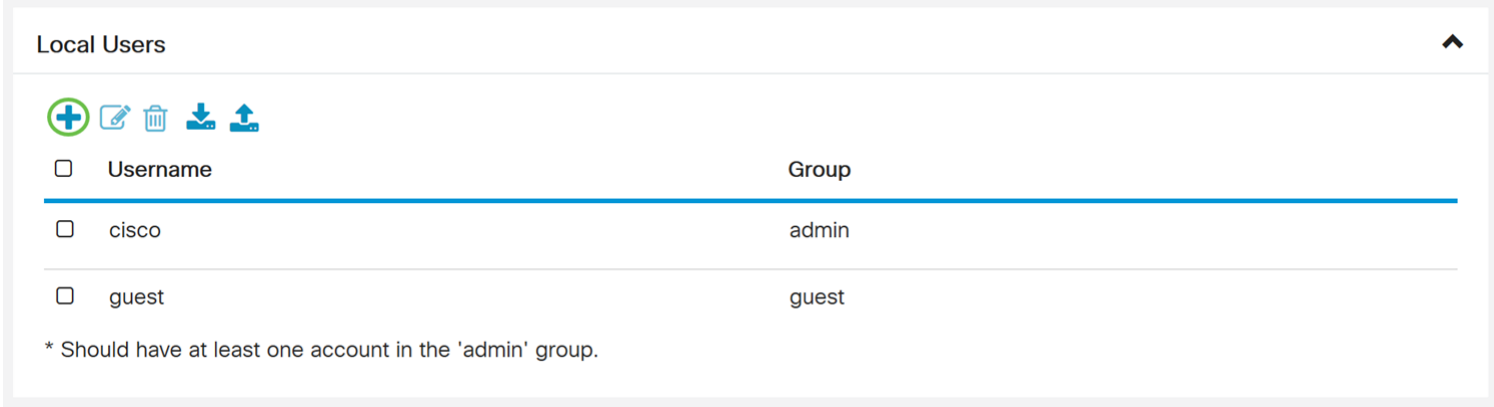


Criando contas de usuário

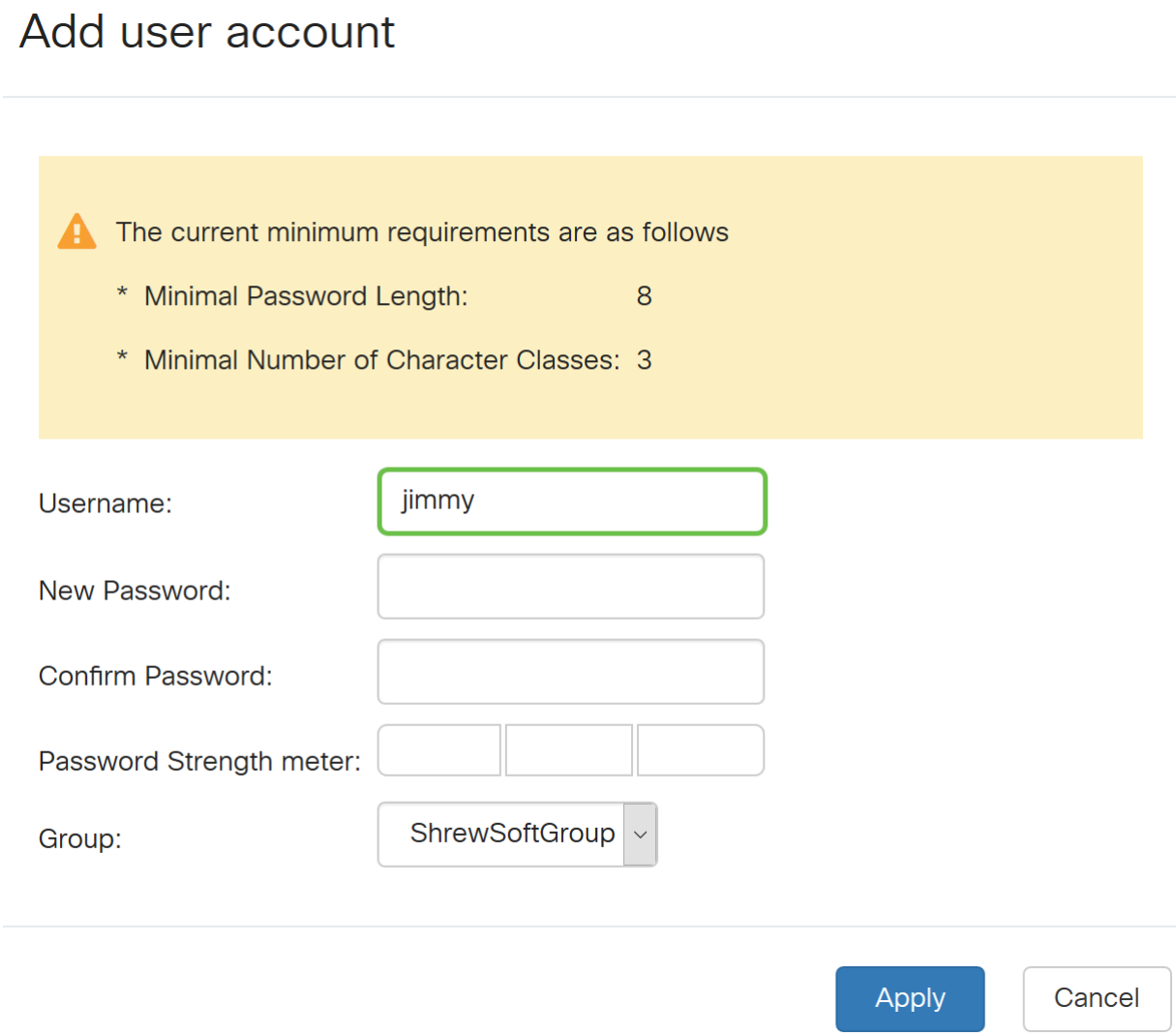
Etapa 1. Navegue até **Configuração do sistema > Contas de usuário**.



Etapa 2. Role para baixo até a tabela *Usuários locais* e pressione o ícone **mais** para adicionar um novo usuário.

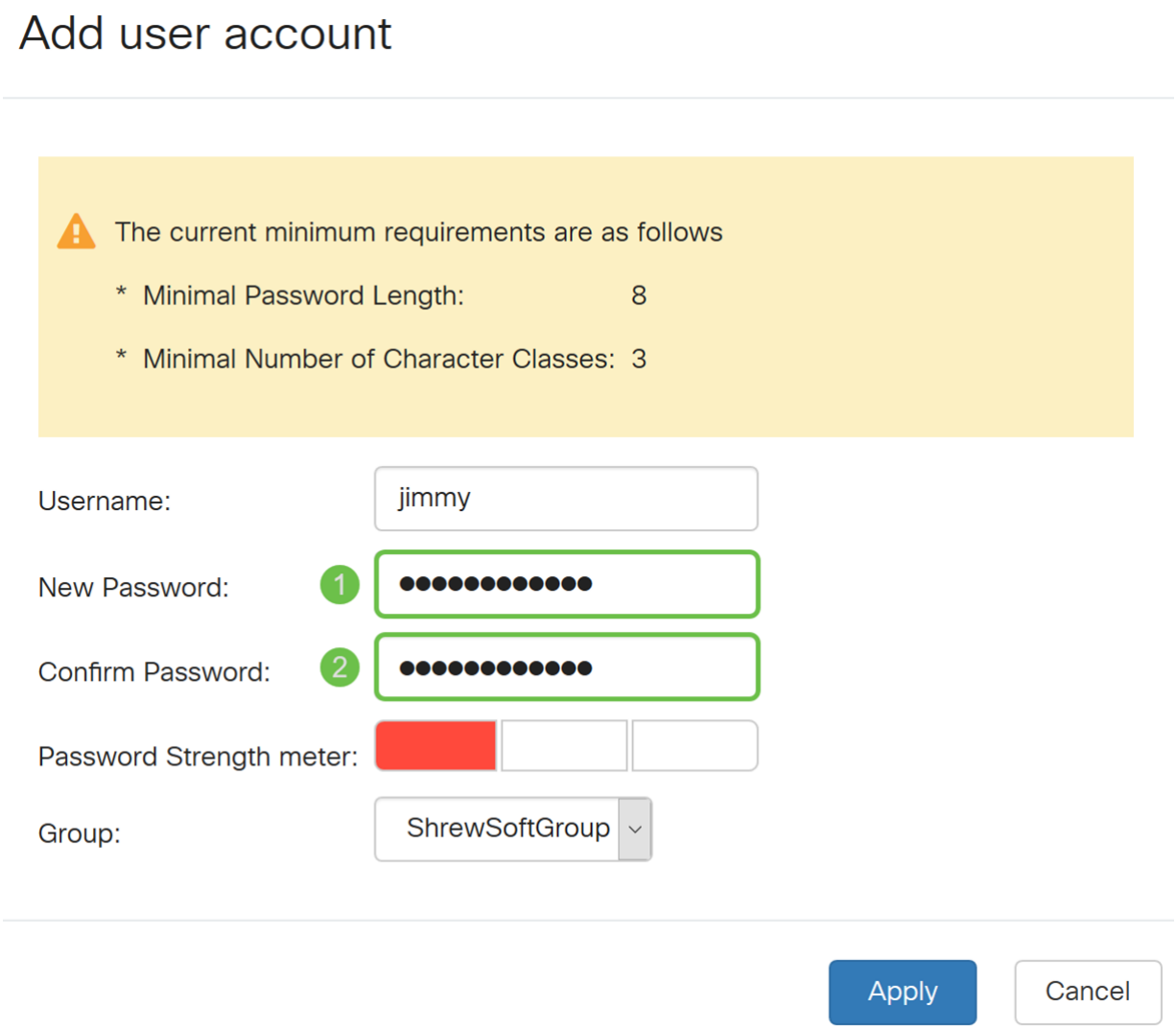


Etapa 3. A página *Adicionar contas de usuário* é aberta. Digite um nome de usuário para o usuário.

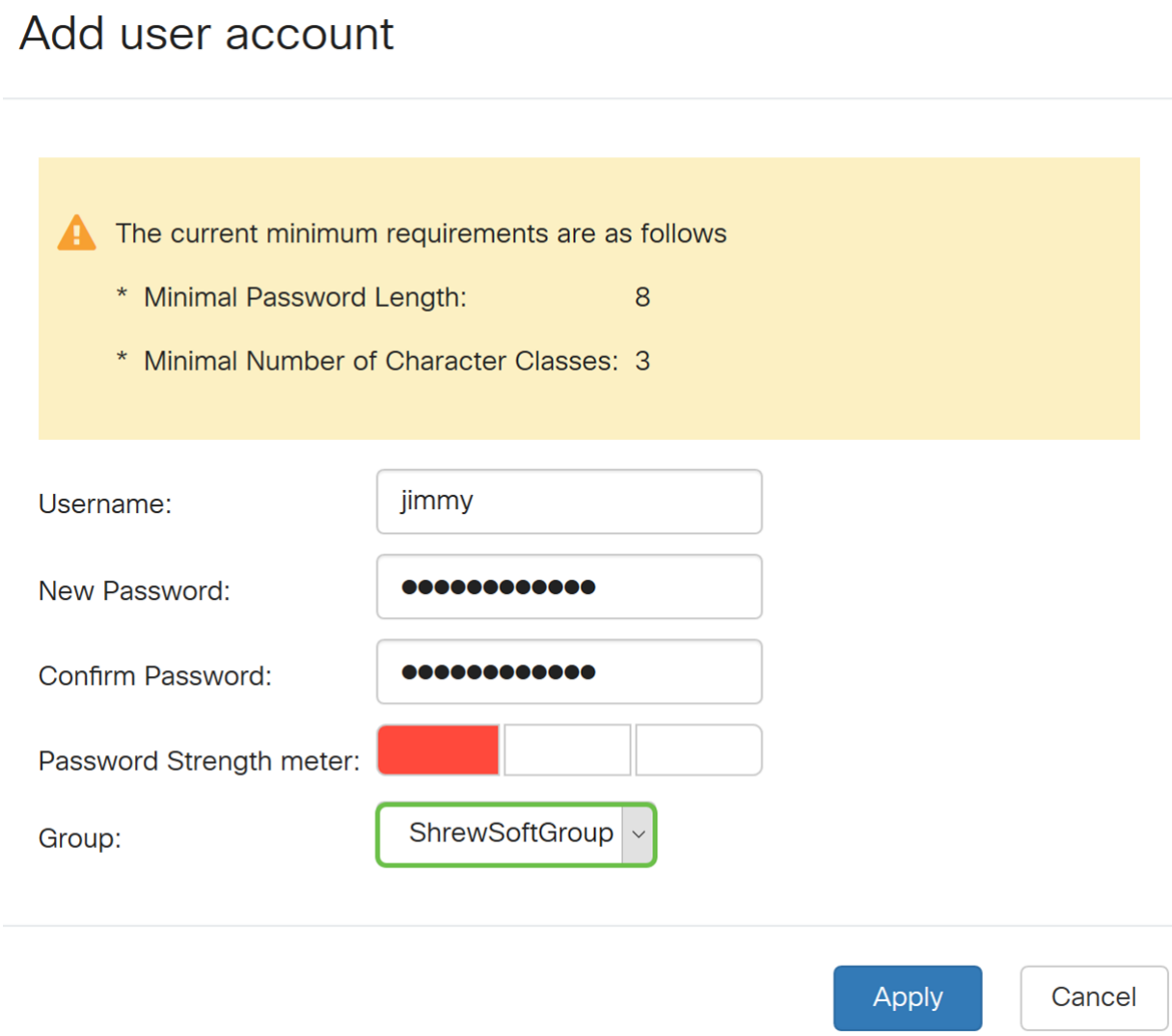


Etapa 4. Digite uma senha no campo *Nova senha*. Digite novamente a mesma senha no campo *Confirmar senha*. Neste exemplo, usaremos **CiscoTest123** como senha.

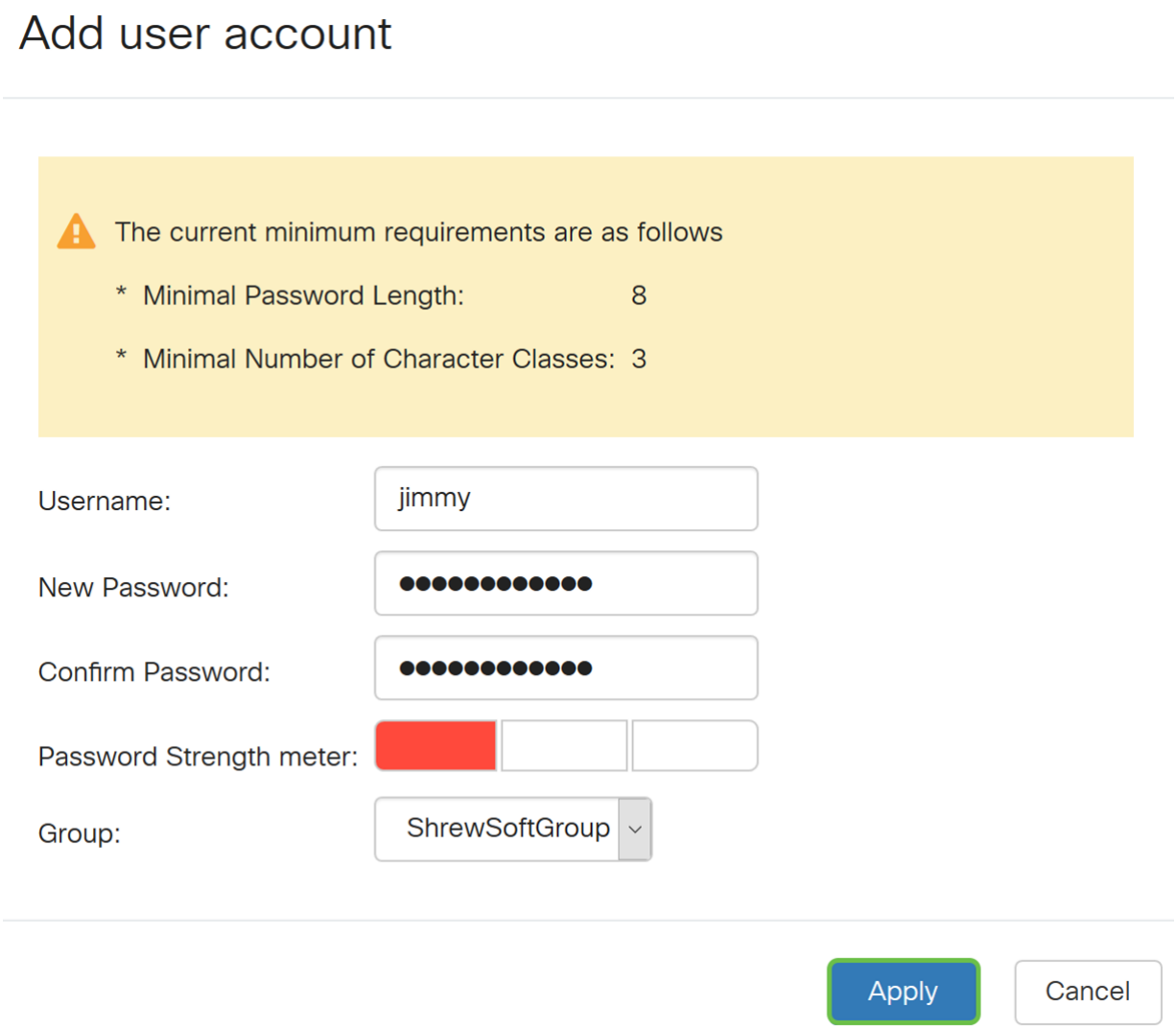
Note: A senha usada aqui é um exemplo. Recomenda-se tornar sua senha mais complexa.



Etapa 5. Na lista suspensa *Grupo*, selecione um grupo no qual deseja que o usuário esteja.

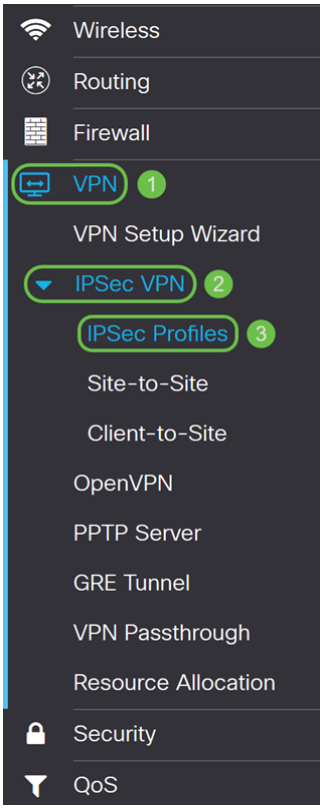


Etapa 6. Pressione **Apply** para criar uma nova conta de usuário.



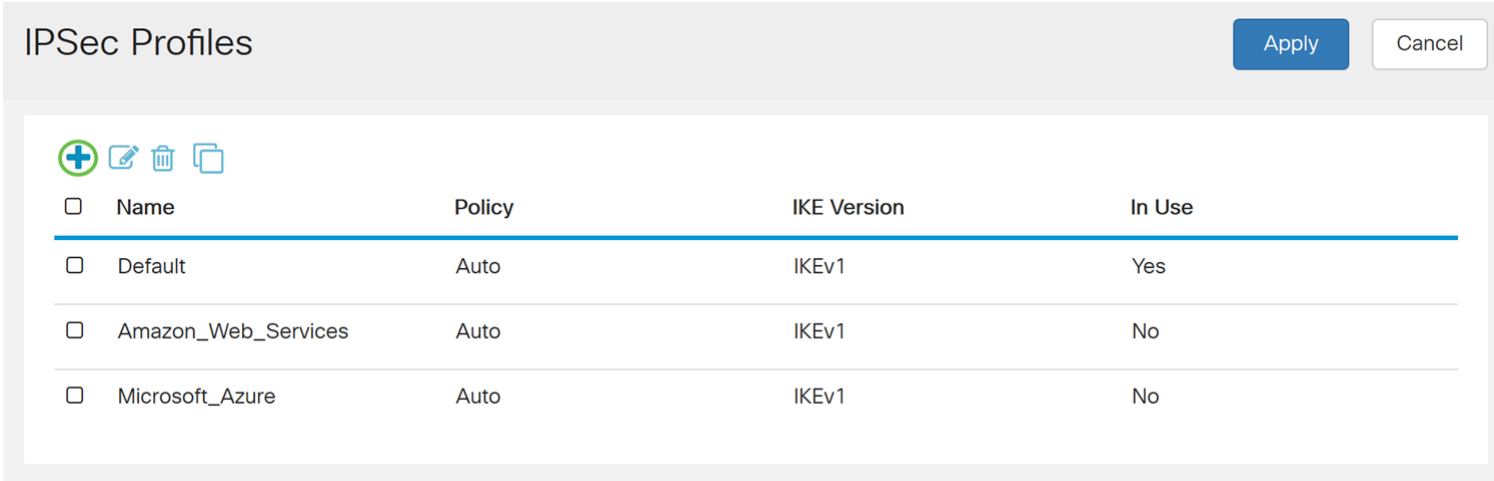
Configurando o perfil IPsec

Etapa 1. Navegue até **VPN > IPSec VPN > IPSec Profiles**.

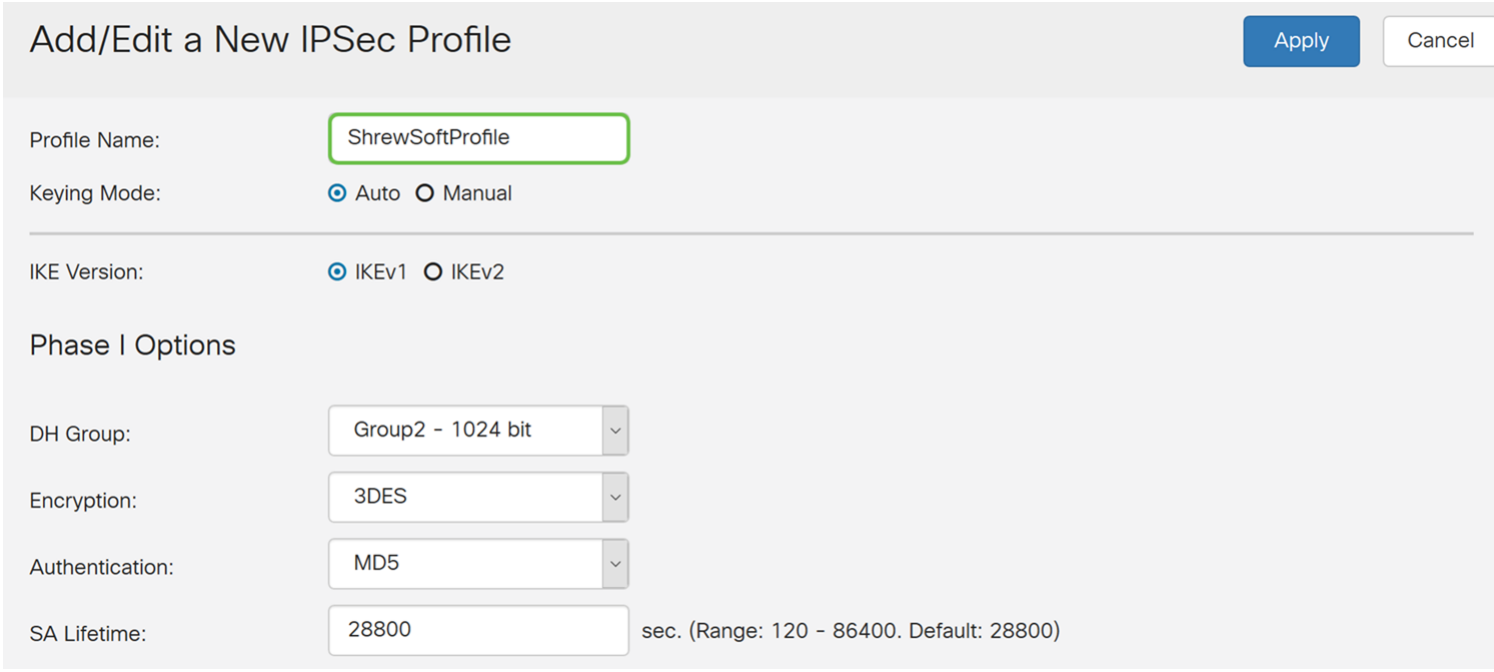


Note: Para obter mais explicações sobre como configurar perfis IPsec, clique no link para ver o artigo: [Configurando perfis IPsec (modo de chaveamento automático) no RV160 e RV260]

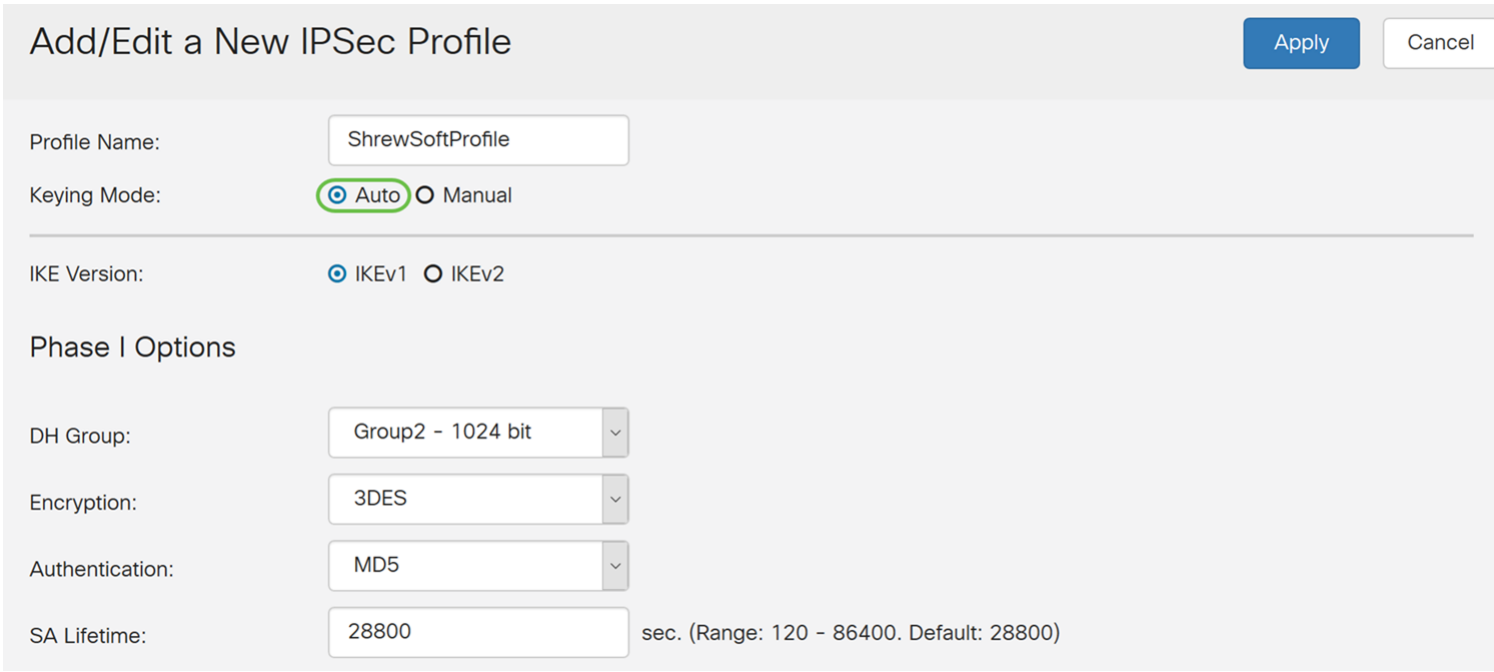
Etapa 2. Clique no ícone **de mais** para adicionar um novo perfil IPsec.



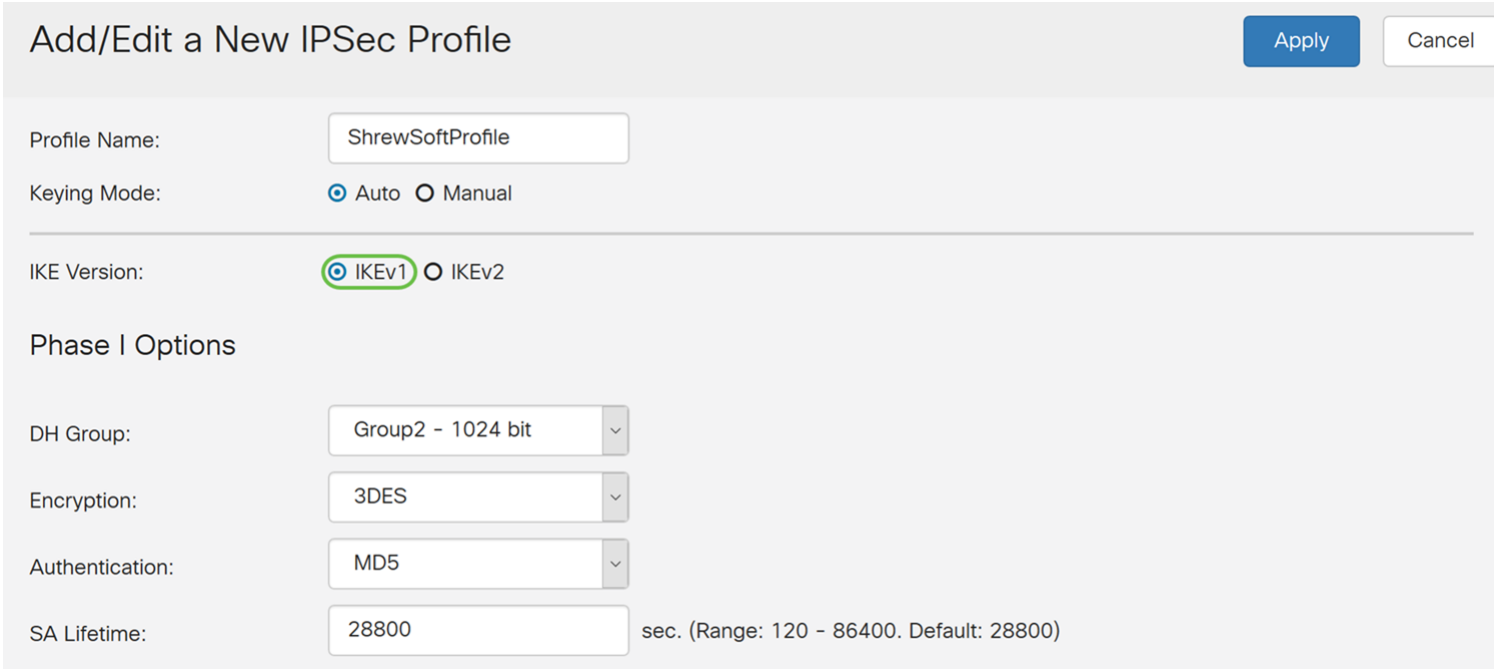
Etapa 3. Digite um nome para o perfil no campo *Nome do perfil*. Vamos introduzir **ShrewSoftProfile** como o nosso nome de perfil.



Etapa 4. Selecione **Auto** para o *modo de chave*.



Etapa 5. Selecione **IKEv1** ou **IKEv2** como a *versão IKE*. Neste exemplo, IKEv1 foi selecionado.



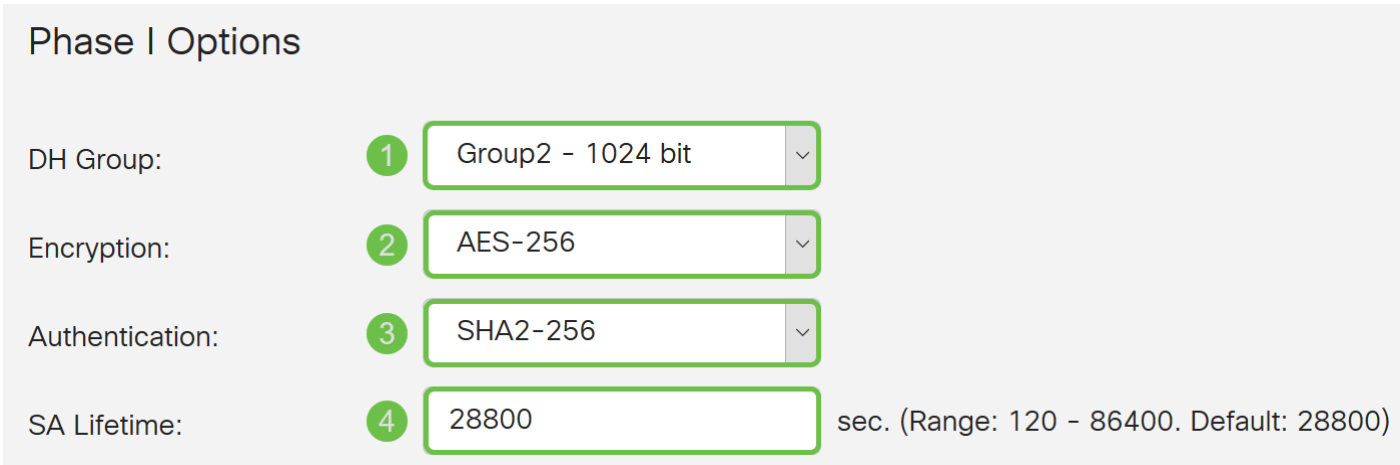
Etapa 6. Na seção *Opções da Fase I*, isso é o que configuramos para este artigo.

Grupo DH: **Grupo2 - 1024 bits**

Criptografia: **AES-256**

Autenticação: **SHA2-256**

Vida útil do SA: **28800**



Etapa 7. Nas *Opções da Fase II*, isso é o que configuramos para este artigo.

Seleção de protocolo: **ESP**

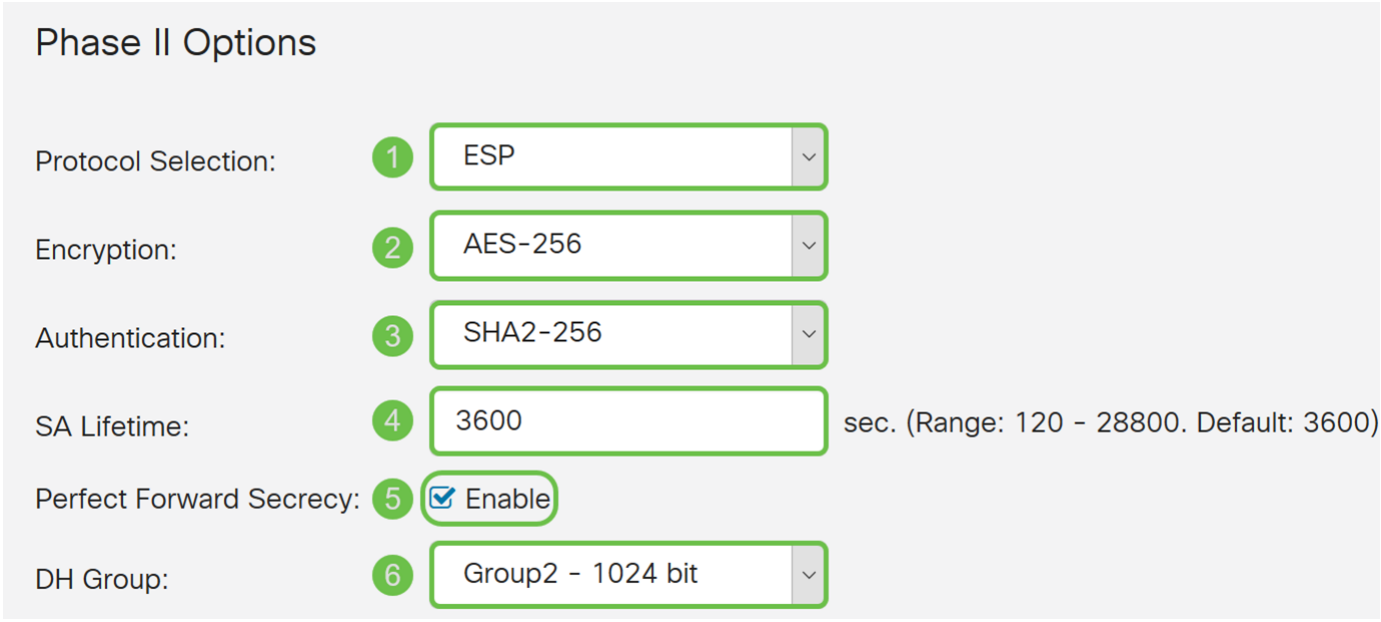
Criptografia: **AES-256**

Autenticação: **SHA2-256**

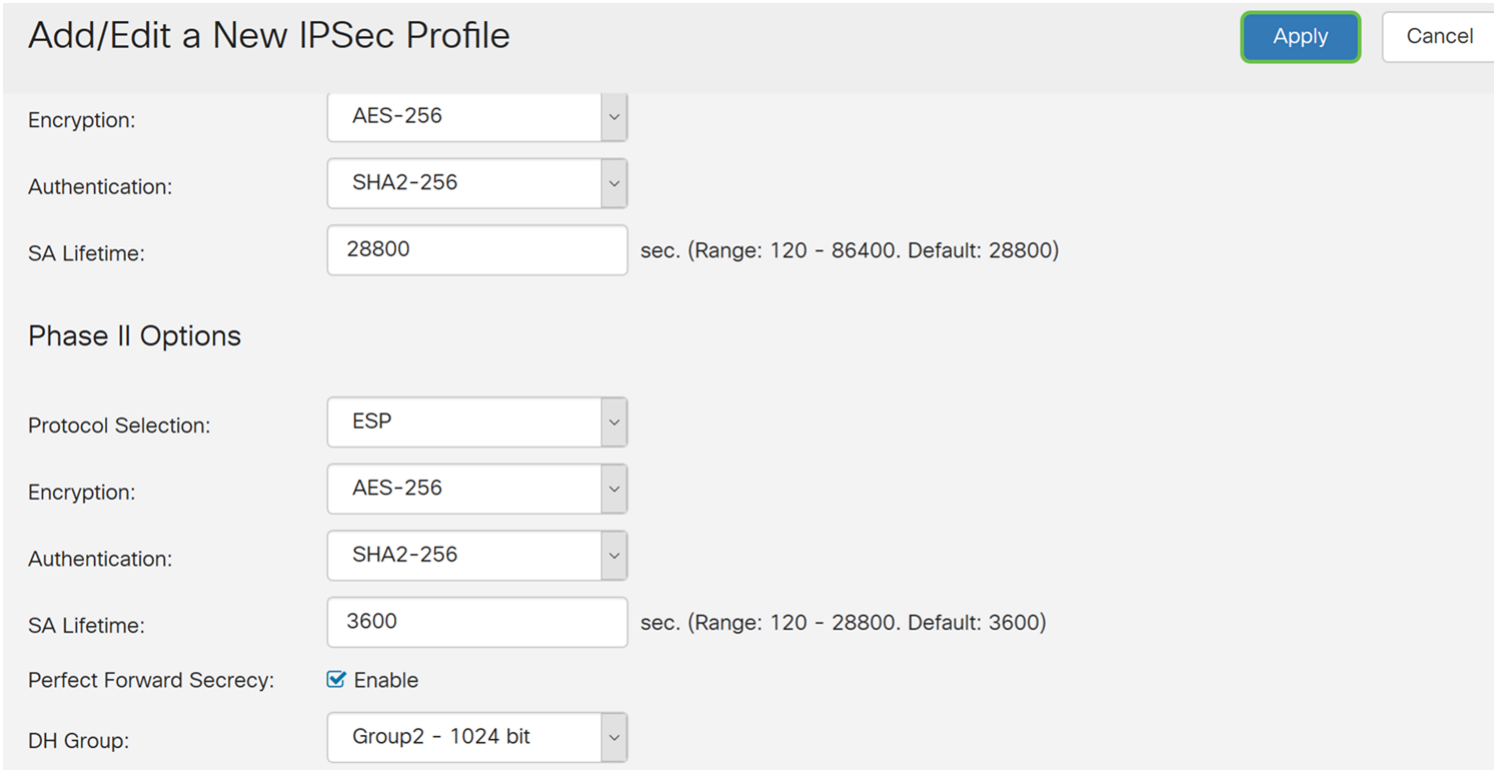
Vida útil do SA: **3600**

Segredo de encaminhamento perfeito: **Habilitado**

Grupo DH: **Grupo2 - 1024 bits**

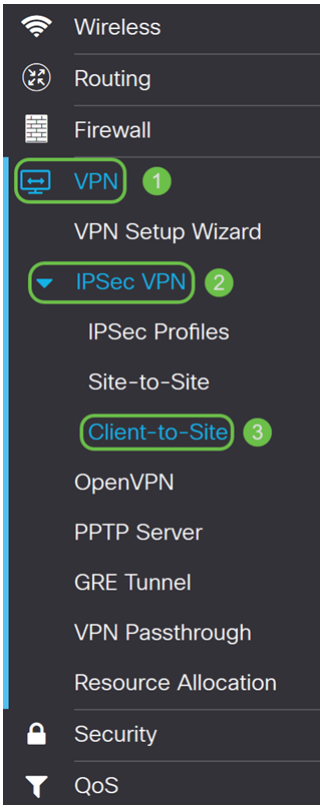


Etapa 8. Clique em **Apply** para criar seu novo perfil IPsec.

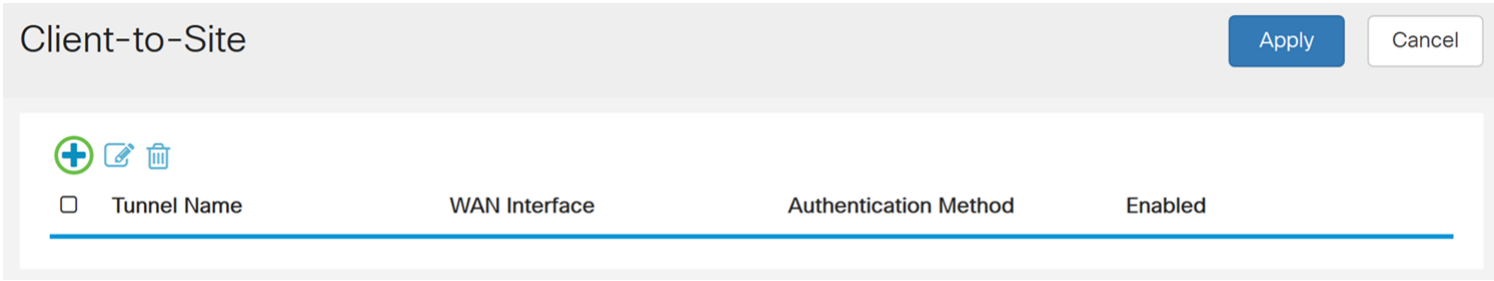


Configurando cliente para site

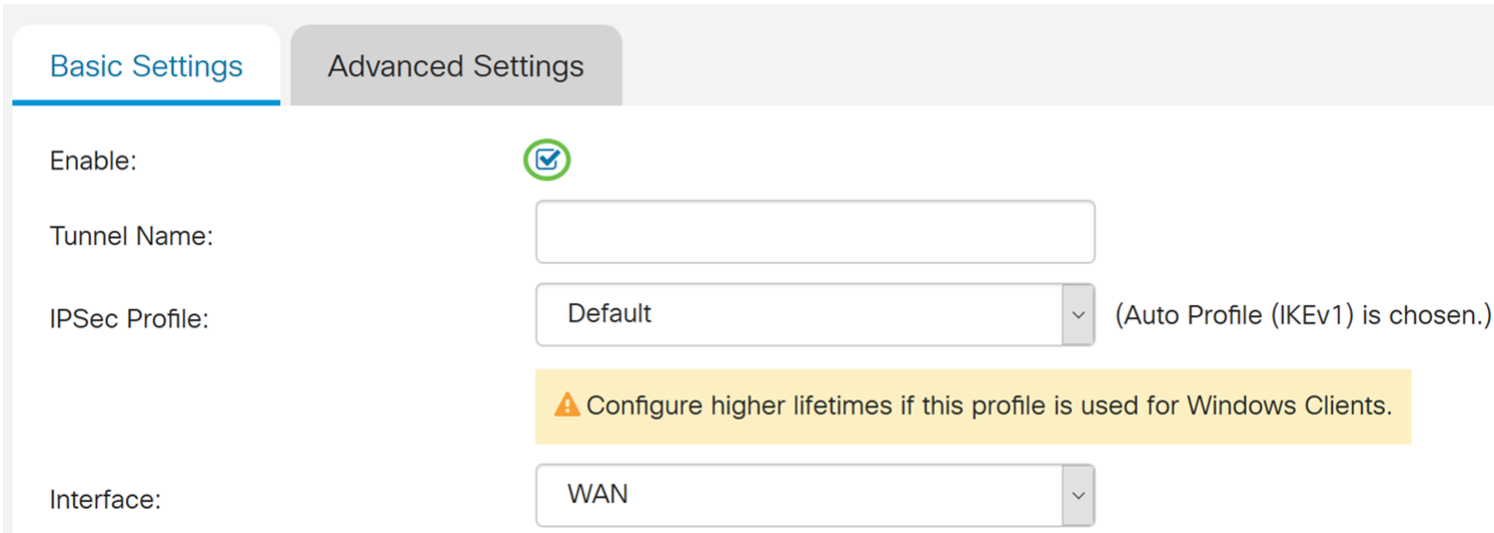
Etapa 1. Navegue para **VPN > IPSec VPN > Cliente para Site**.



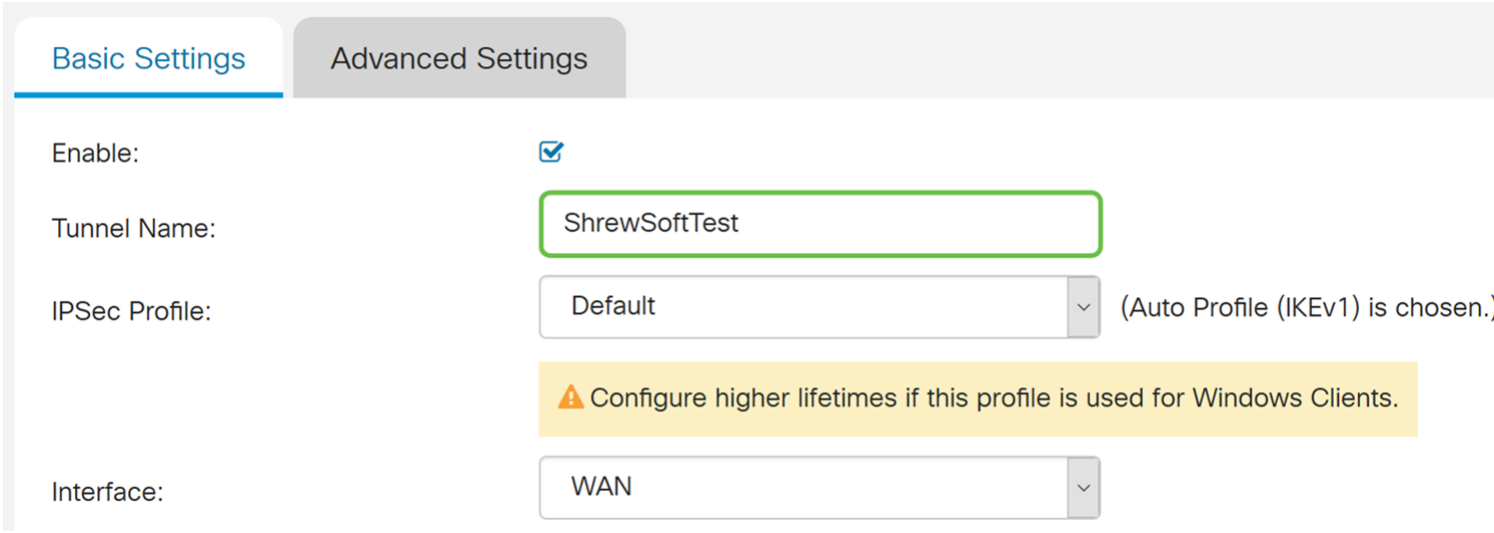
Etapa 2. Clique no ícone **de mais** para adicionar um novo túnel.



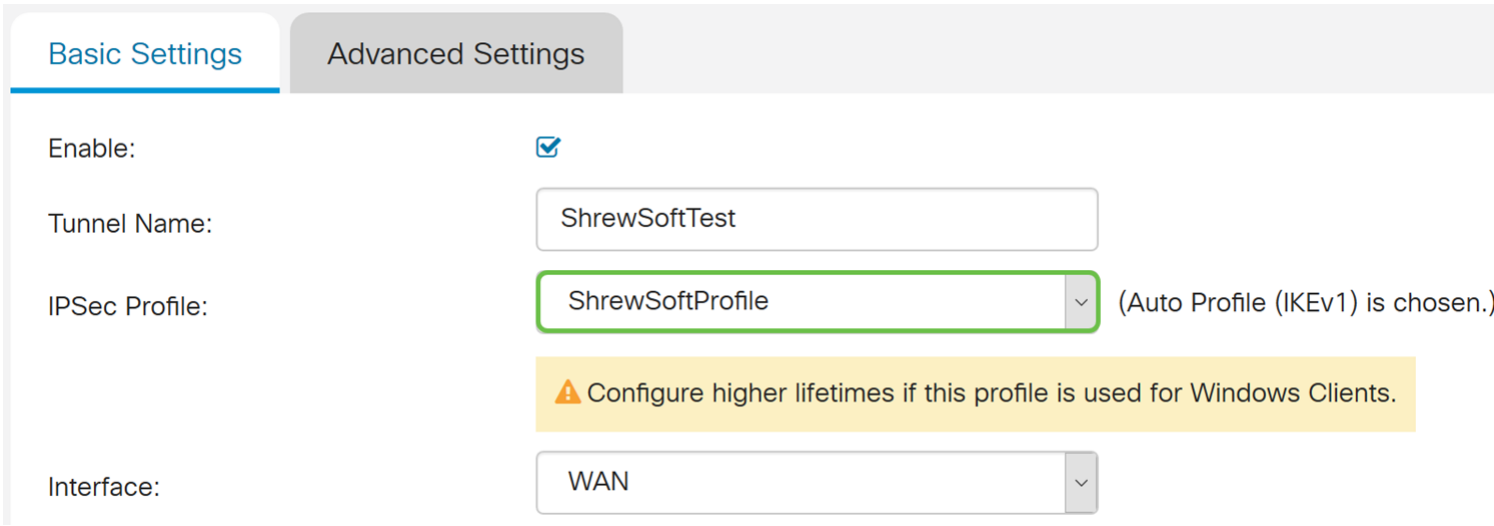
Etapa 3. Marque a caixa de seleção **Habilitar** para habilitar o túnel.



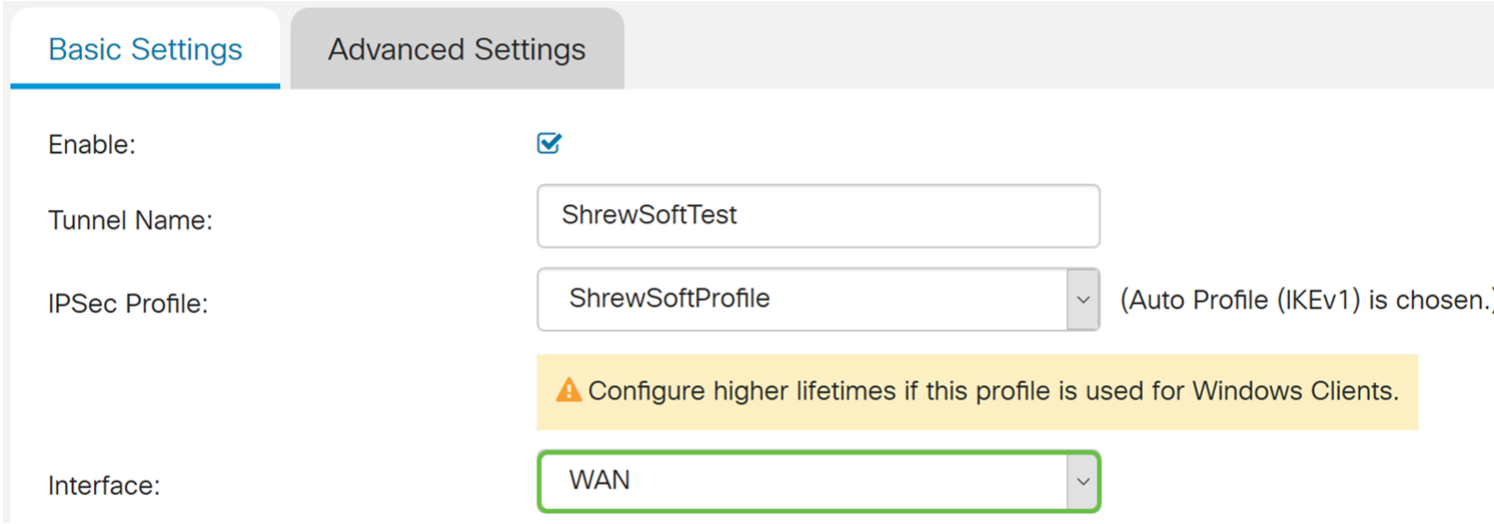
Etapa 4. Digite um nome para o túnel no campo *Nome do túnel*.



Etapa 5. Na lista suspensa *Perfil de IPSec*, selecione um perfil que deseja usar. Selecionaremos ShrewSoftProfile que foi criado na seção anterior: Configurando o perfil IPsec.



Etapa 6. Na lista suspensa *Interface*, selecione a interface que deseja usar. Usaremos a **WAN** como nossa interface para conectar o túnel.

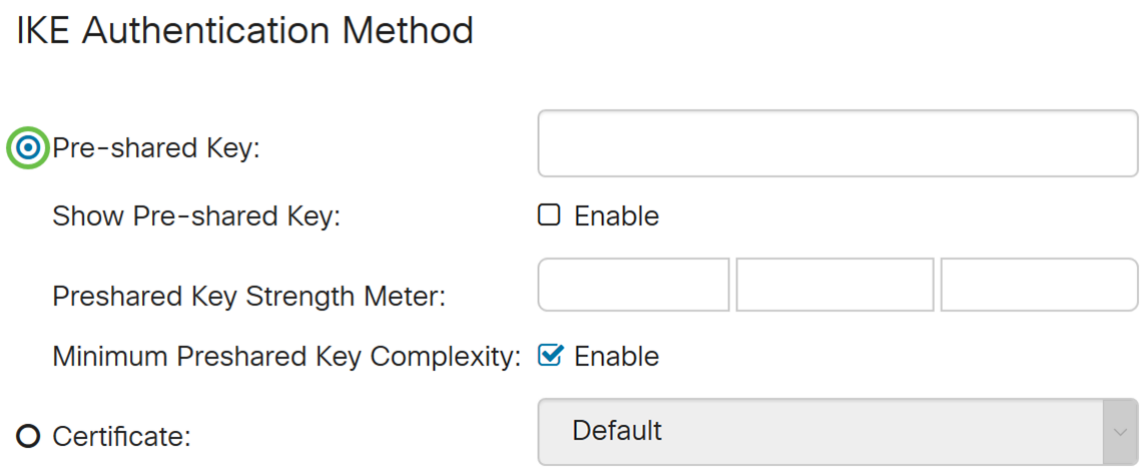


Passo 7. Na seção *Método de autenticação IKE*, selecione *Chave pré-compartilhada* ou *Certificado*. Usaremos a **chave pré-compartilhada** como nosso método de autenticação IKE.

Note: Os pares IKE autenticam-se através da computação e do envio de um hash chaveado de dados que inclui a chave pré-compartilhada. Se o peer receptor for capaz de criar o

mesmo hash independentemente usando sua chave pré-compartilhada, ele saberá que ambos os pares devem compartilhar o mesmo segredo, autenticando o outro peer. As chaves pré-compartilhadas não escalam bem porque cada peer IPsec deve ser configurado com as chaves pré-compartilhadas de todos os outros pares com os quais estabelece uma sessão.

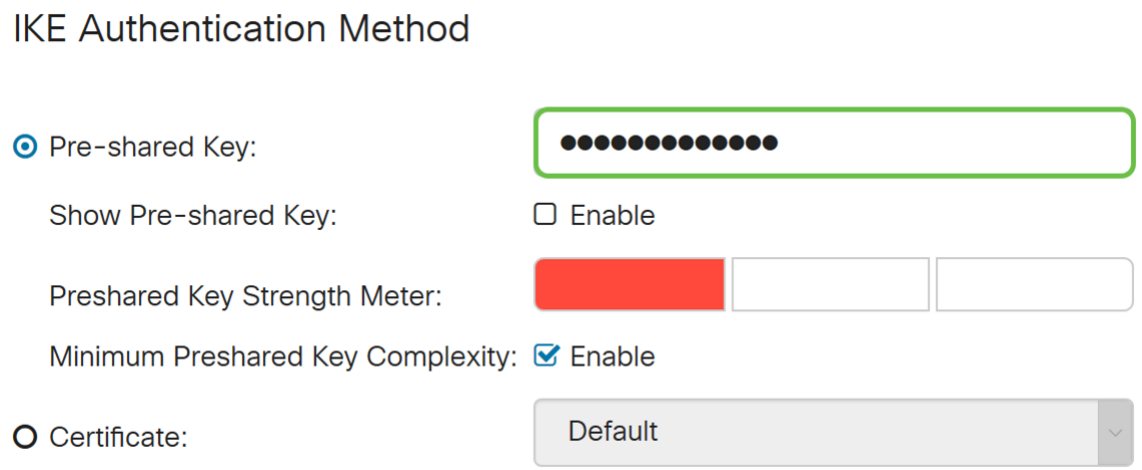
O certificado usa um certificado digital que contém informações como o nome, ou endereço IP, número de série, data de expiração do certificado e uma cópia da chave pública do portador do certificado.



Etapa 8. Digite a chave pré-compartilhada que deseja usar para autenticar. A chave pré-compartilhada pode ser o que você quiser. A chave pré-compartilhada configurada no cliente Shrew Soft VPN terá que ser a mesma aqui quando você configurá-la.

Neste exemplo, usaremos o **CiscoTest123!** como a chave pré-compartilhada.

Note: A chave pré-compartilhada que foi inserida aqui é um exemplo. É recomendável inserir uma chave pré-compartilhada mais complexa.



Etapa 9. Selecione o *Identificador local* na lista suspensa. As seguintes opções são definidas como:

IP da WAN local • - Esta opção usa o endereço IP da interface da rede de longa distância (WAN) do gateway VPN

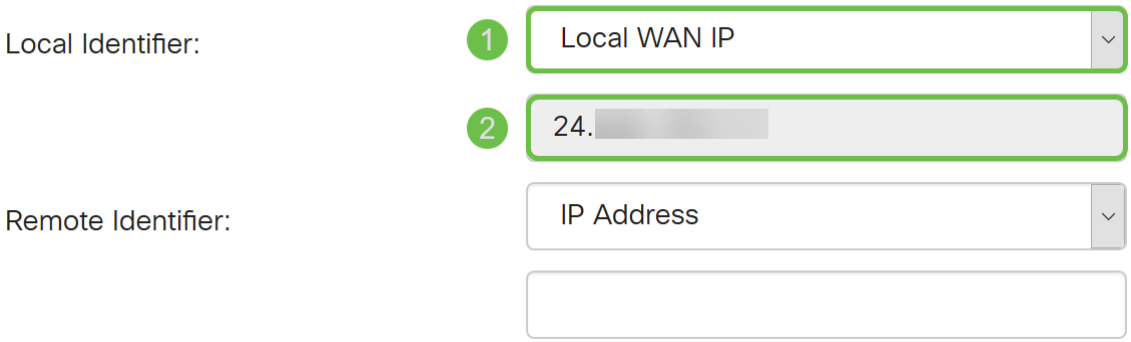
• Endereço IP - Esta opção permite inserir manualmente um endereço IP para a conexão VPN. Você precisaria digitar o endereço IP da WAN do roteador no local (escritório).

- FQDN - Essa opção usará o FQDN (Fully Qualified Domain Name, nome de domínio totalmente qualificado) do roteador ao estabelecer a conexão VPN.

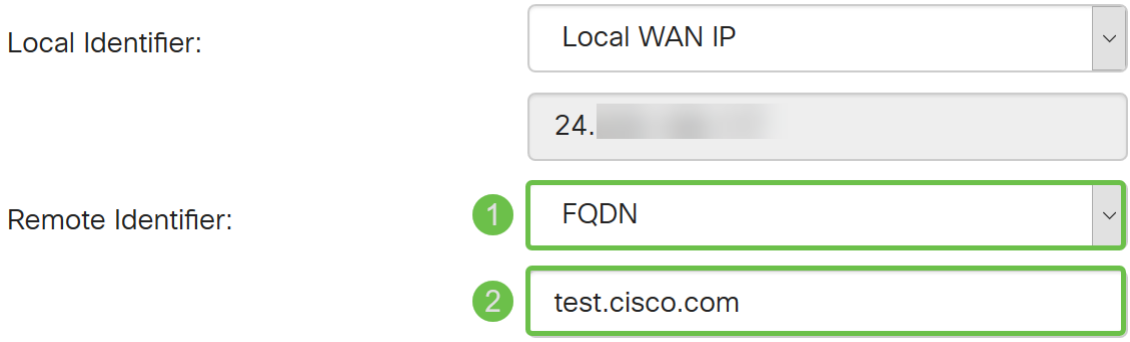
- FQDN do usuário - Essa opção permite que você use um nome de domínio completo para um usuário específico na Internet.

Neste exemplo, selecionaremos **IP de WAN local** como nosso identificador local.

Note: O IP da WAN local do roteador será preenchido automaticamente.

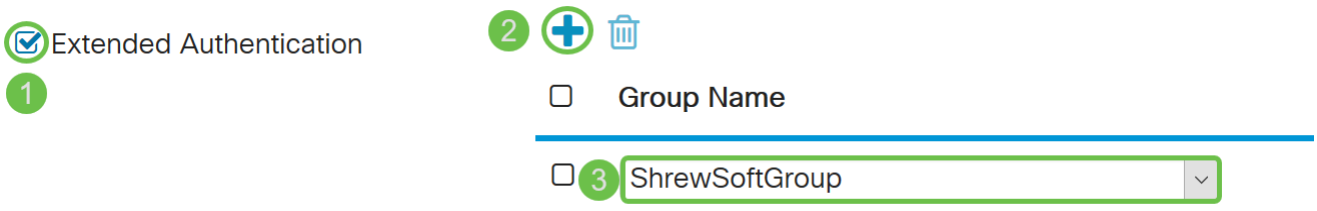


Etapa 10. Na lista suspensa *Identificador remoto*, selecione **Endereço IP**, **FQDN** ou **FQDN do usuário**. Em seguida, insira a resposta apropriada do que você selecionou. Neste exemplo, selecionaremos o **FQDN** e inseriremos **test.cisco.com**.



Etapa 11. Marque a caixa de seleção **Extended Authentication** para habilitar. Isso fornecerá um nível adicional de autenticação que exigirá que os usuários remotos digitem suas credenciais antes de receberem acesso à VPN.

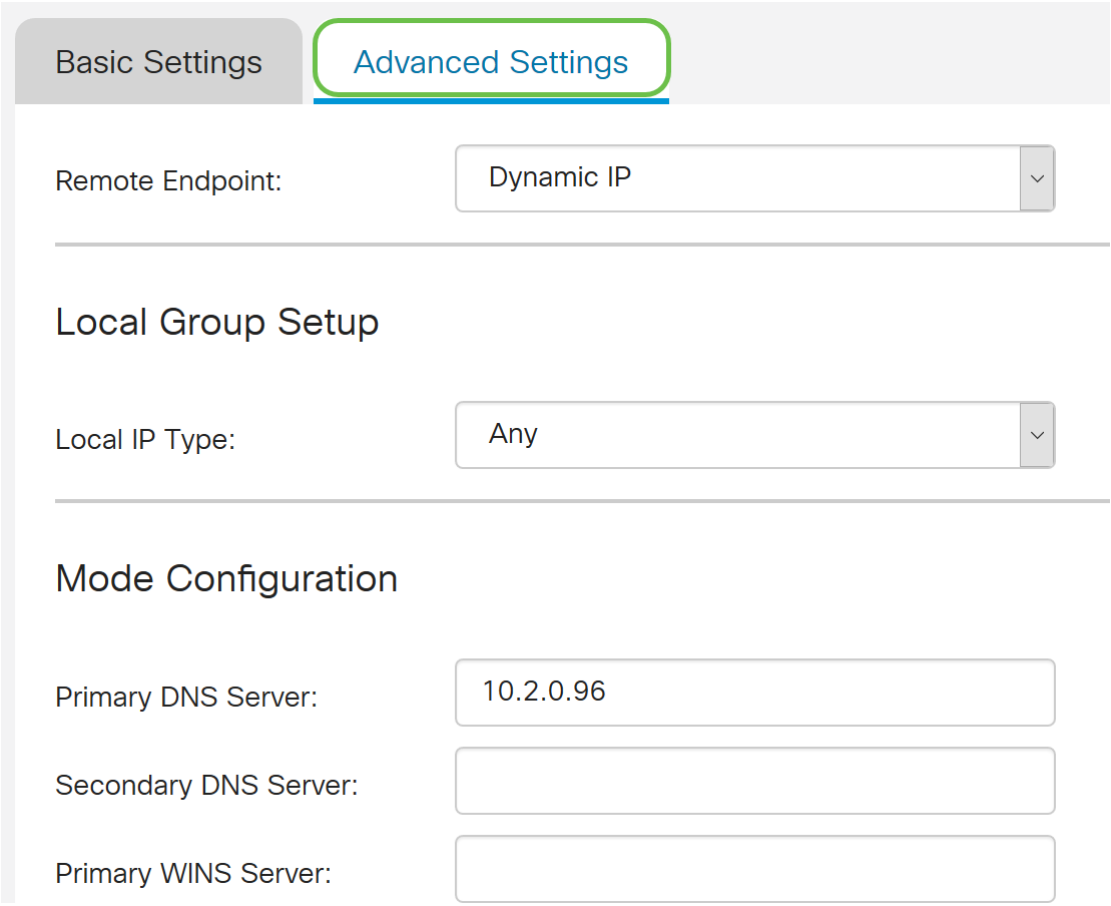
Se você habilitou a *Autenticação Estendida*, clique no ícone **de mais** para adicionar um grupo de usuários. Selecione o grupo na lista suspensa que deseja usar para autenticação estendida. Vamos selecionar **ShrewSoftGroup** como o grupo.



Etapa 12. No *Intervalo de pool para LAN de cliente*, insira o intervalo de endereços IP que podem ser atribuídos a um cliente VPN no campo *IP inicial* e *IP final*. Isso precisa ser um pool de endereços que não se sobreponha aos endereços do site.

Entraremos em **10.2.1.1** como nosso *IP inicial* e **10.2.1.254** como nosso *IP final*.

Etapa 13. (Opcional) Clique na guia **Configurações avançadas**.



Etapa 14. (Opcional) Aqui você pode especificar o endereço IP do ponto de extremidade remoto. Neste guia, usaremos **IP dinâmico**, pois o endereço IP do cliente final não é fixo.

Você também pode especificar quais recursos internos estarão disponíveis na *Configuração do grupo local*.

Se você selecionar **Qualquer**, todos os recursos internos estarão disponíveis.

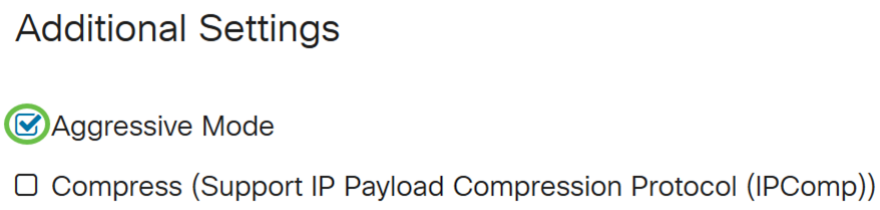
Você também pode optar por usar servidores DNS internos e WINS. Para isso, você precisa especificá-los em *Configuração do modo*.

Você também tem a possibilidade de usar o túnel completo ou dividido e o DNS dividido.

Role para baixo até *Additional Settings (Configurações adicionais)*. Marque a caixa de seleção **Modo agressivo** para ativar o modo Agressivo. O modo agressivo é quando a negociação para SA IKE é compactada em três pacotes com todos os dados exigidos pela SA a serem passados pelo iniciador. A negociação é mais rápida, mas eles têm uma vulnerabilidade de trocar identidades em texto claro.

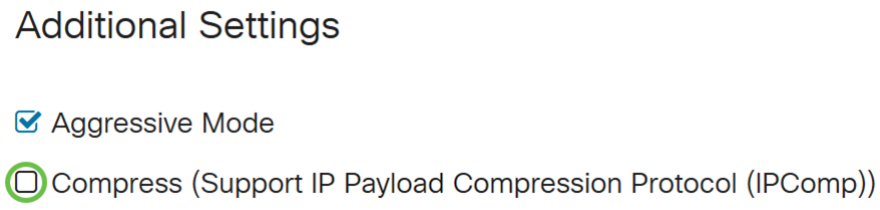
Note: Informações adicionais sobre o modo principal versus o modo agressivo, consulte: Modo Principal Vs Modo Agressivo

Neste exemplo, habilitaremos o **Modo agressivo**.

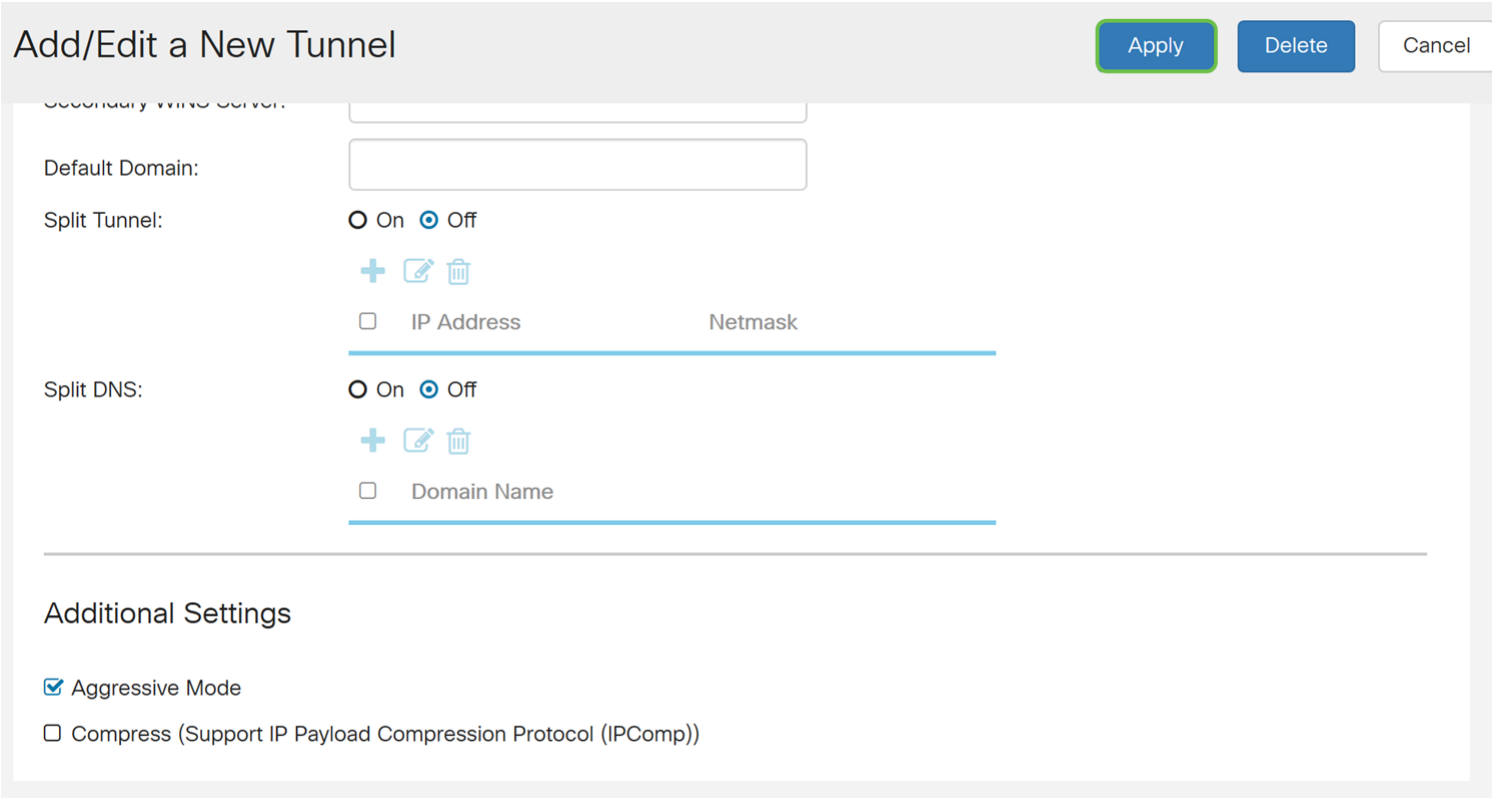


Etapa 15. (Opcional) Marque a caixa de seleção **Compress (Support IP Payload Compression Protocol (IPComp))** para permitir que o roteador proponha a compactação quando inicia uma conexão. Esse é um protocolo que reduz o tamanho dos datagramas IP. Se o respondente rejeitar esta proposta, o roteador não implementará a compactação. Quando o roteador é o respondente, ele aceita a compactação, mesmo que a compactação não esteja habilitada.

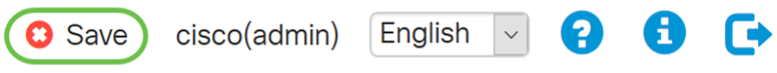
Vamos deixar a *Compress* desmarcada.



Etapa 16. Clique em **Apply** para adicionar o novo túnel.

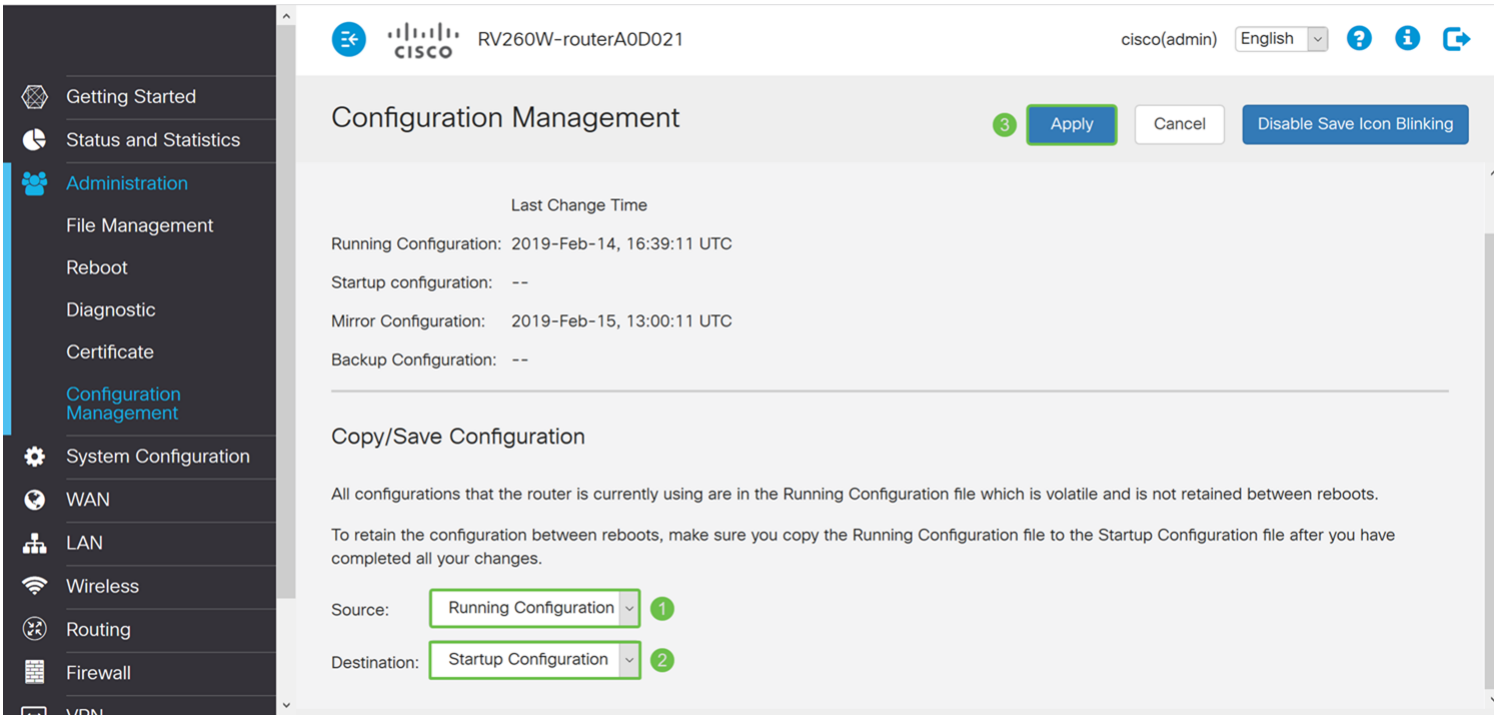


Etapa 17. Clique no ícone **Save** piscando na parte superior da página de configuração da Web.



Etapa 18. A página *Gerenciamento de configuração* é aberta. Na seção Copiar/salvar

configuração, verifique se o campo *Origem* tem **Configuração em Execução** e *Destino* possui **Configuração de Inicialização**. Em seguida, pressione **Apply (Aplicar)**. Todas as configurações que o roteador está usando no momento estão no arquivo Running Configuration, que é volátil e não é retido entre as reinicializações. Copiar o arquivo de configuração atual para o arquivo de configuração de inicialização manterá sua configuração entre as reinicializações.

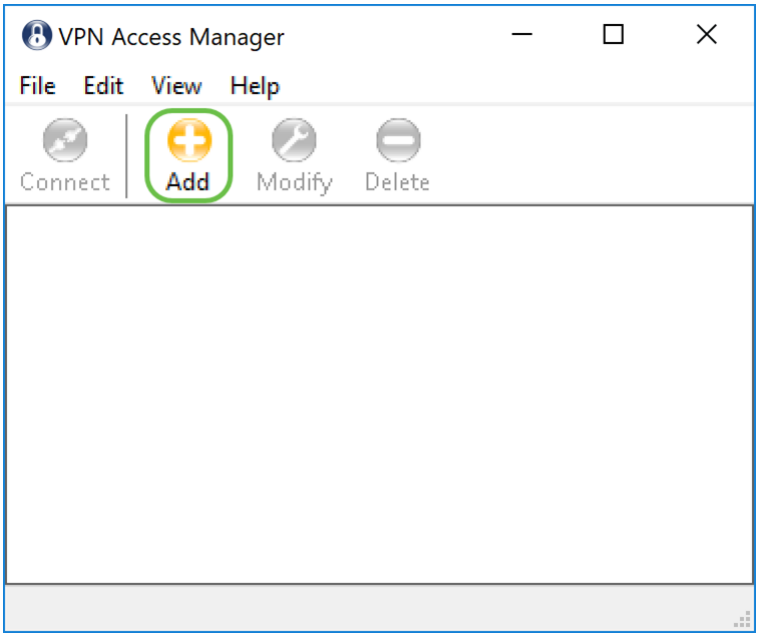


Configurando o Shrew Soft VPN Client

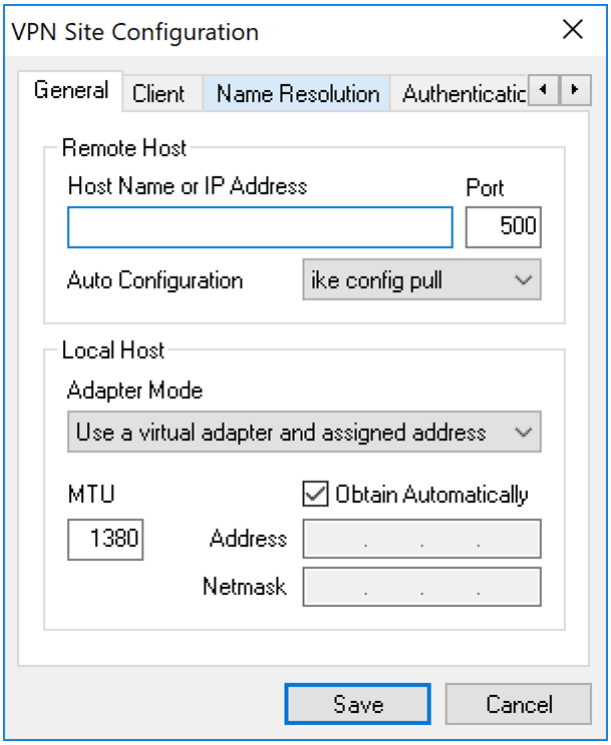
Se ainda não tiver feito o download do cliente Shrew Soft VPN, sinta-se à vontade para fazer o download do cliente clicando neste link: Mostrar o software cliente VPN para Windows. Usaremos a edição padrão. Se você já fez o download do cliente Shrew Soft VPN, sinta-se à vontade para prosseguir para a primeira etapa.

Shrew Soft VPN Client: Guia Geral

Etapa 1. Abra o Gerenciador de acesso VPN de tela e clique em **Adicionar** para adicionar um novo perfil.

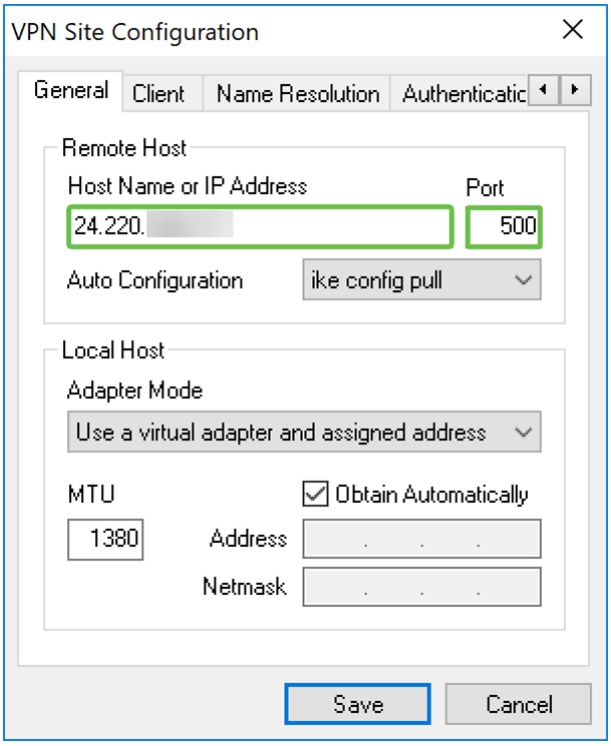


A janela *VPN Site Configuration* é exibida.



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. Neste exemplo, vamos inserir o endereço IP da WAN do RV160/RV260 no local para configurar a conexão.

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*, selecione uma opção. As opções disponíveis são definidas da seguinte forma:

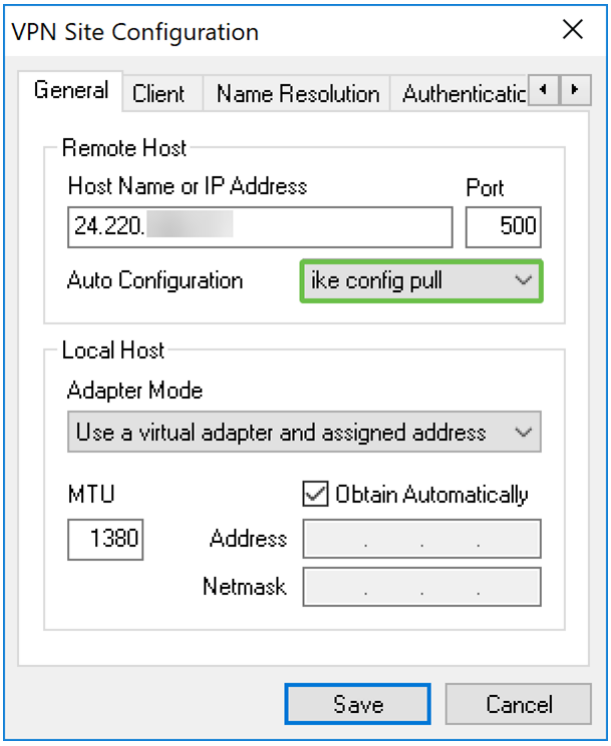
- **Desativado** - desativa qualquer configuração automática de cliente

- **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** - Dá 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 sobre IPsec** - Dá ao cliente a oportunidade de solicitar configurações do computador por DHCP sobre IPsec.

Neste exemplo, selecionaremos **como configuração pull**.

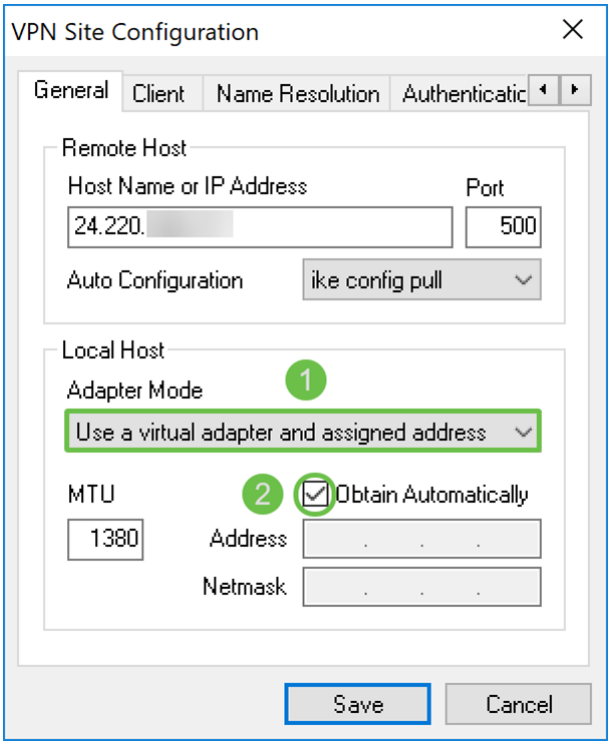


Etapa 4. Na seção *Local Host*, escolha **Usar um adaptador virtual e endereço atribuído** na lista suspensa *Modo do adaptador* e marque a caixa de seleção **Obter automaticamente**. As opções disponíveis são definidas da seguinte forma:

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

- **Usar um adaptador virtual e um 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 um endereço atual** - Permite que o cliente use somente seu adaptador físico existente com seu endereço atual como origem de suas comunicações IPsec.



Shrew Soft VPN Client: Guia Cliente

Etapa 1. Clique na guia *Cliente*. Na lista suspensa *NAT Traversal*, selecione a mesma configuração que você configurou no RV160/RV260 para NAT Traversal. As opções de menu Network Address Traversal (NATT) disponíveis são definidas da seguinte forma:

- **Desativado** - As extensões do protocolo NATT não serão usadas.

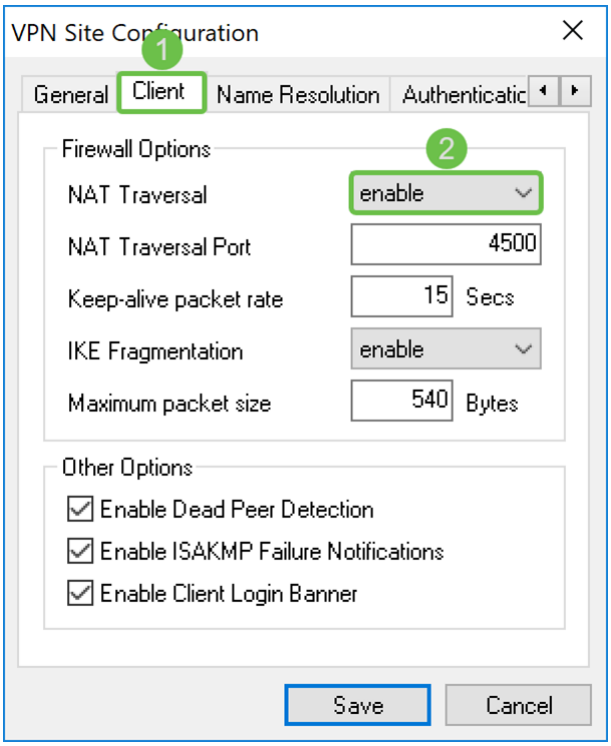
- **Habilitado** - As extensões do protocolo NAT só serão usadas se o Gateway VPN indicar suporte durante as negociações e se o NAT for detectado.

- **Force-Draft** - A versão de rascunho das extensões do protocolo NAT será usada independentemente de o Gateway VPN indicar ou não suporte durante as negociações ou de o NAT ser detectado.

- **Force-RFC** - A versão RFC do protocolo NAT será usada independentemente de o gateway de VPN indicar ou não suporte durante as negociações ou de a NAT ser detectada.

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

Neste documento, selecionaremos **enable** para NAT Traversal e deixaremos *NAT Traversal Port* e *Keep-alive packet rate* como valor padrão.



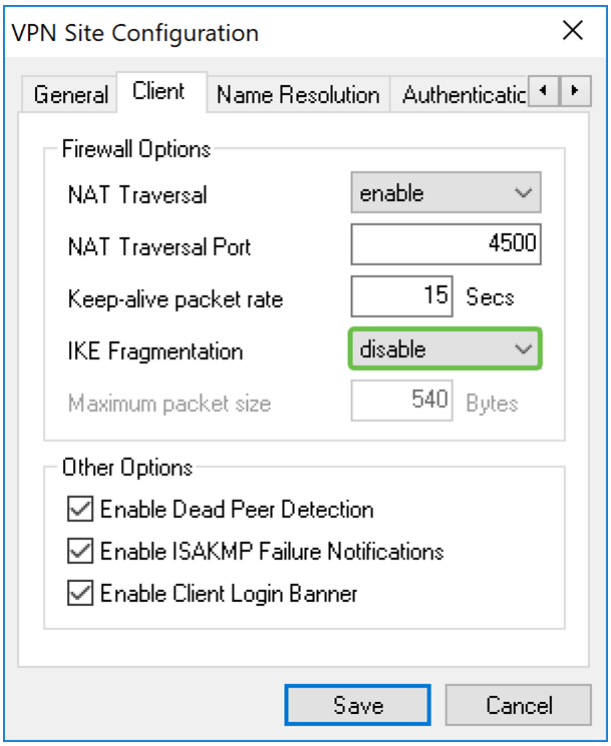
Etapa 2. Na lista suspensa *IKE Fragmentation*, selecione **Disable**, **Enable** ou **Force**. As opções são definidas da seguinte forma:

- **Disable** - A extensão do protocolo IKE Fragmentation não será usada.

- **Enable** - A extensão do protocolo IKE Fragmentation só será usada se o gateway VPN indicar suporte durante as negociações.

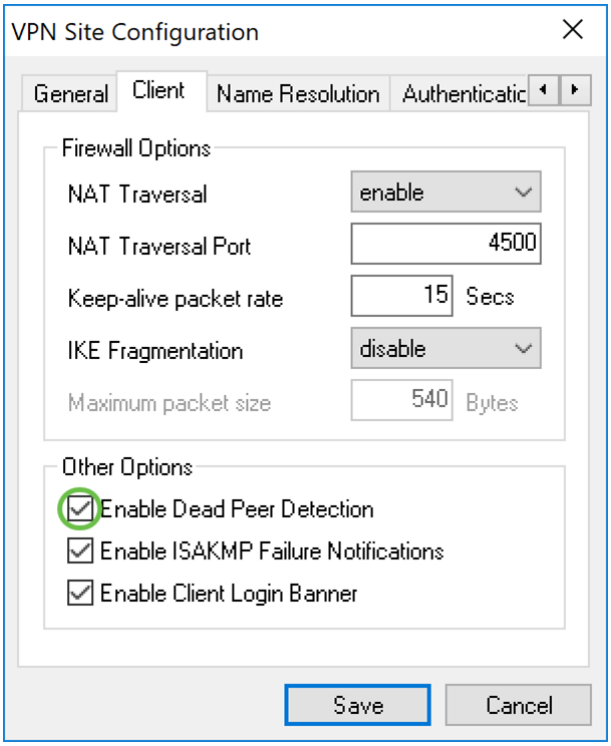
- **Force** - A extensão do protocolo IKE Fragmentation será usada independentemente de o VPN Gateway indicar ou não suporte durante as negociações.

Selecionamos **desabilitar** para *fragmentação IKE*.



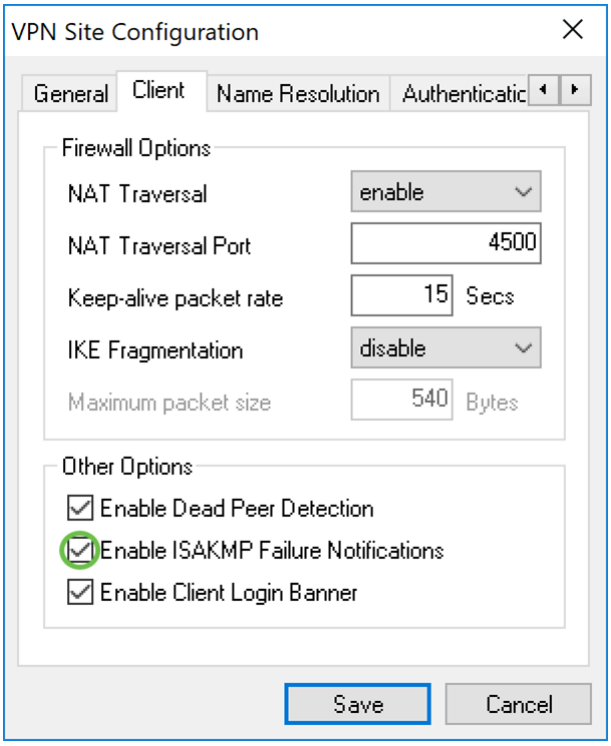
Etapa 3. Marque a caixa de seleção **Habilitar detecção de peer inoperante** para habilitar o protocolo Dead Peer Detection. Se essa opção estiver ativada, ela só será usada se o roteador a suportar. Isso permite que o cliente e o roteador verifiquem o status do túnel para detectar quando um lado não puder mais responder. Essa opção está habilitada por padrão.

Neste exemplo, deixaremos Dead Peer Detection marcada.



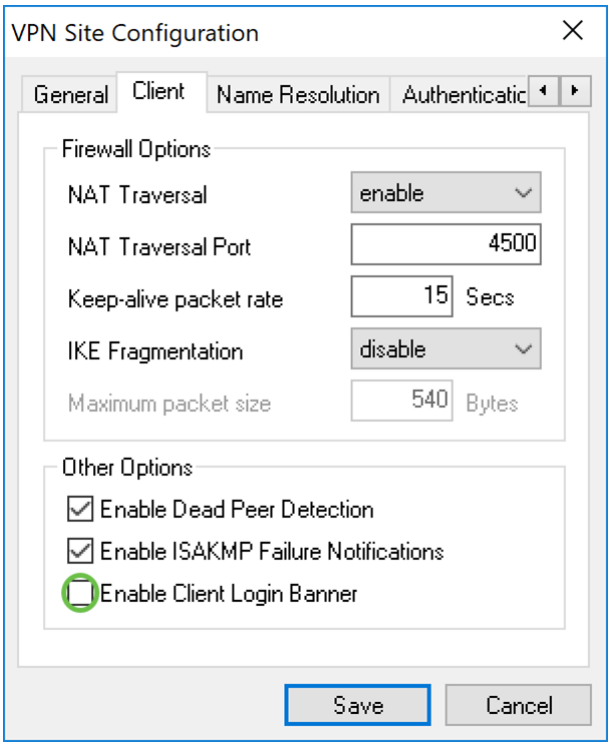
Etapa 4. Marque a caixa de seleção **Enable ISAKMP Failure Notification** para habilitar a notificação de falha ISAKMP do daemon IPsec do VPN Client. Iss está habilitado por padrão.

Neste exemplo, deixaremos ISAKMP Failure Notification marcada.



Etapa 5. Desmarque a opção **Enable Client Login Banner** para desativá-la. Isso exibirá um banner de login depois que o túnel for estabelecido com o roteador. O roteador deve suportar o Transaction Exchange e também deve ser configurado para encaminhar um banner de login ao cliente. Esse valor é ativado por padrão.

Vamos desmarcar a faixa de login do cliente.



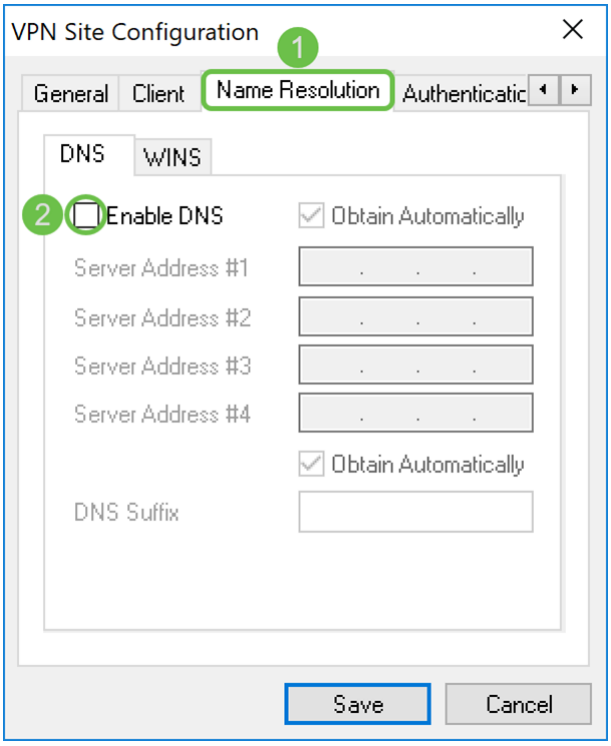
Shrew Soft VPN Client: Guia Resolução de nome

Etapa 1. Clique na guia *Resolução de nome* e marque a caixa de seleção **Habilitar DNS** se desejar habilitar o DNS. Se não forem necessárias configurações de DNS específicas para a configuração do seu site, desmarque a caixa de seleção **Habilitar DNS**.

Se *Enable DNS* estiver marcado e o gateway remoto estiver configurado para suportar o

Configuration Exchange, o gateway poderá fornecer as configurações de DNS automaticamente. Caso contrário, verifique se a caixa de seleção **Obter automaticamente** está desmarcada e insira manualmente um endereço de servidor DNS válido.

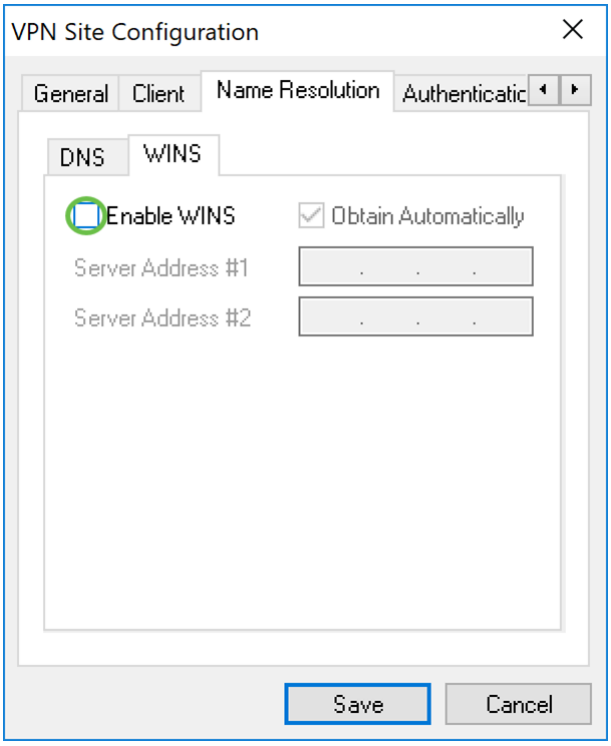
Neste exemplo, **Ativar DNS** está desmarcada.



Etapa 2. Marque a caixa de seleção **Habilitar WINS** se desejar habilitar o Windows Internet Name Server (WINS). Se o gateway remoto estiver configurado para suportar o Configuration Exchange, ele poderá fornecer as configurações 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 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 remoto 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.

Neste exemplo, **Ativar WINS** está desmarcada.



Shrew Soft VPN Client: Guia Autenticação

Etapa 1. Clique na guia *Authentication* e selecione **Mutual PSK + XAuth** na lista suspensa *Authentication Method*. As opções disponíveis são definidas da seguinte forma:

- **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.

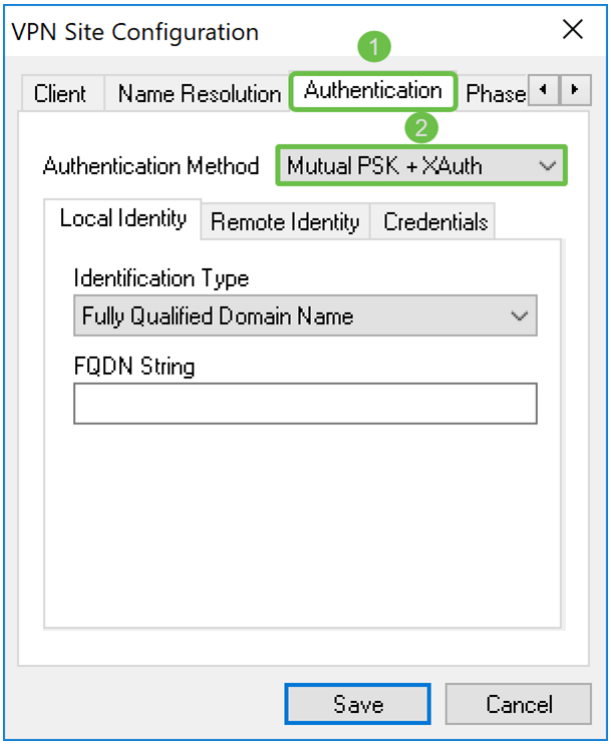
- **GRP híbrido + XAuth** - A credencial do cliente não é necessária. O cliente autenticará o gateway. As credenciais estarão na forma de arquivo de certificado PEM ou PKCS12 e uma cadeia de caracteres secreta compartilhada.

- **RSA + XAuth** - 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** - O cliente e o gateway precisam de credenciais para autenticação. As credenciais serão na forma de uma cadeia de caracteres secreta compartilhada.

- **RSA mútuo** - Tanto o cliente como o gateway precisam de credenciais para autenticação. As credenciais estarão na forma de arquivos de certificado PEM ou PKCS12 ou tipo de chave.

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



Etapa 2. Na guia *Identidade local*, selecione o tipo de identificação e insira a string apropriada no campo vazio. As seguintes opções são definidas como:

- **Qualquer** - Isso só é aceito na guia Remote Identity (Identidade remota). O cliente aceitará qualquer tipo de ID e valor. Isso deve ser usado com cuidado, pois ele ignora parte do processo de identificação da fase 1 do IKE.

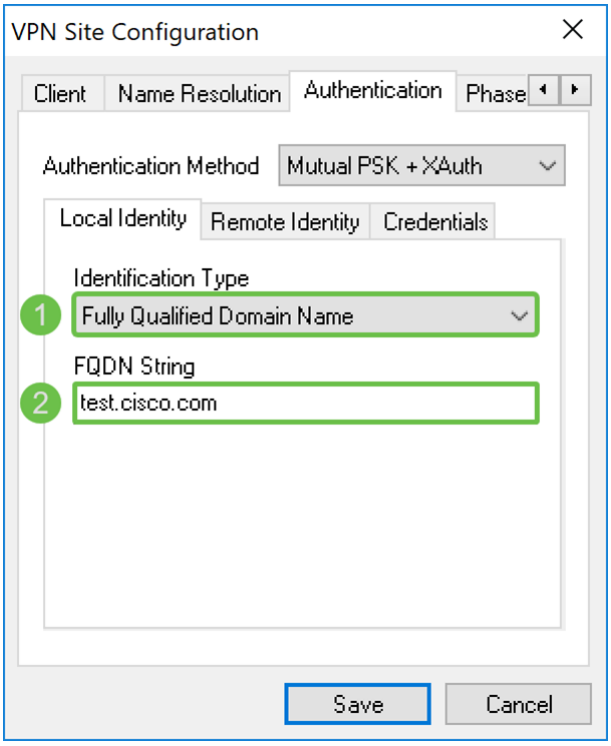
- **Nome de domínio totalmente qualificado** - Esta opção, você deve fornecer uma string FQDN na forma de uma string de domínio DNS. Por exemplo, "cisco.com" seria um valor aceitável. O cliente só permitiria que essa opção fosse selecionada se um modo de autenticação PSK estivesse sendo usado.

- **Nome de domínio totalmente qualificado do usuário** - Você deve fornecer uma string FQDN do usuário na forma de uma string user@domain. Por exemplo, "dave@cisco.com" seria um valor aceitável. O cliente só permitiria que essa opção fosse selecionada se um modo de autenticação PSK estivesse sendo usado.

- **Endereço IP** - Quando o endereço IP é selecionado, a caixa de seleção *Usar um endereço de host local descoberto* é marcada automaticamente por padrão. Isso significa que o valor será automaticamente determinado. Desmarque a caixa de seleção se quiser usar um endereço diferente do endereço do adaptador usado para se comunicar com o gateway cliente. Em seguida, insira uma string de endereço específica. O cliente só permitirá que essa opção seja selecionada se um modo de autenticação PSK estiver sendo usado.

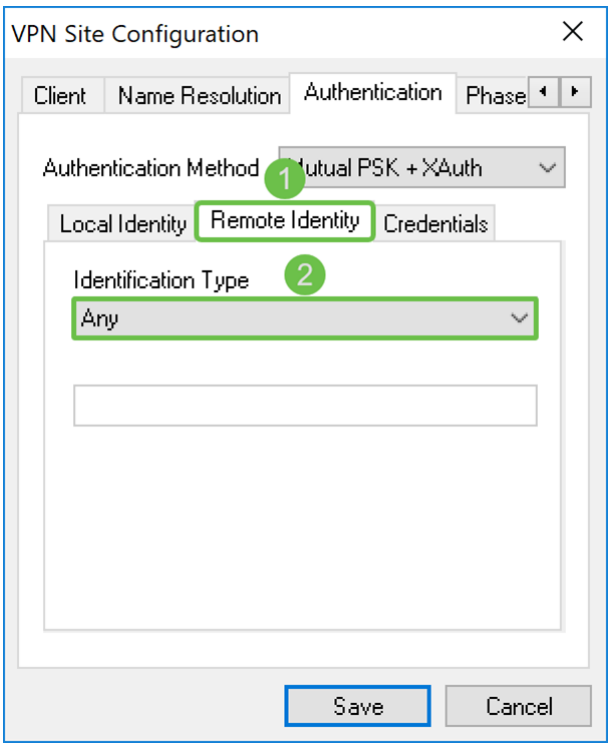
- **Identificador de Chave** - Quando esta opção é selecionada, você deve fornecer uma string de identificador.

Neste exemplo, selecionaremos **Nome de domínio totalmente qualificado** e inseriremos **test.cisco.com** no campo *String de FQDN*.



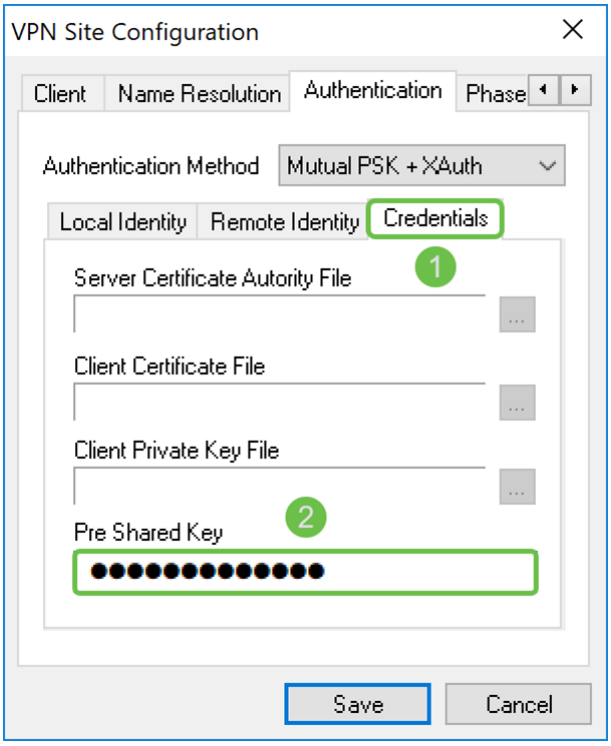
Etapa 3. Clique na guia *Remote Identity* e selecione o tipo de identificação. As opções incluem: Qualquer nome de domínio totalmente qualificado, nome de domínio totalmente qualificado do usuário, endereço IP ou identificador de chave.

Neste documento, usaremos **Qualquer** como nosso tipo de identificação.



Etapa 4. Clique na guia *Credenciais* e insira a mesma chave pré-compartilhada configurada no RV160/RV260.

Entraremos no **CiscoTest123!** no campo *Pre Shared Key*.



Shrew Soft VPN Client: Guia Fase 1

Etapa 1. Clique na guia *Fase 1*. Configure os parâmetros a seguir para ter as mesmas configurações que você configurou para o RV160/RV260.

Os parâmetros no Shrew Soft devem corresponder à configuração RV160/RV260 selecionada na Fase 1. Neste documento, os parâmetros em Shrew Soft serão definidos como:

Tipo • Exchange: **agressivo**

Troca • DH: **grupo 2**

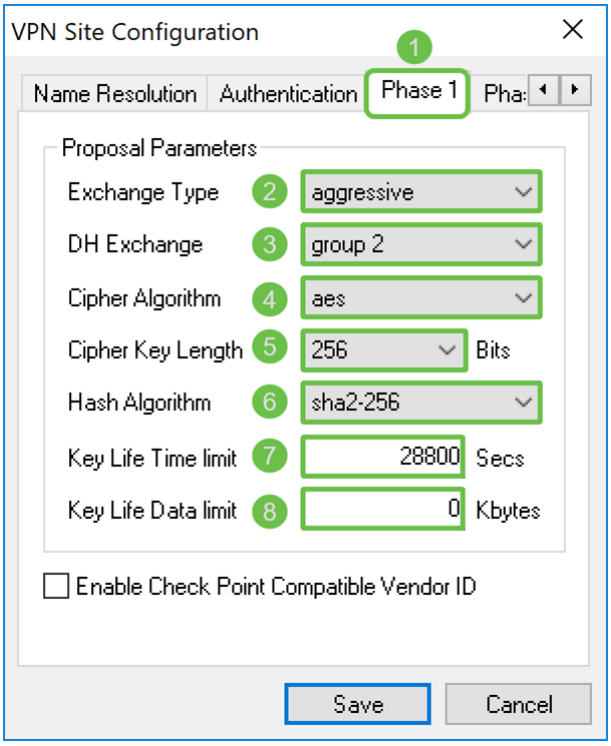
Algoritmo de cifra •: **aes**

Comprimento da chave da cifra •: **256**

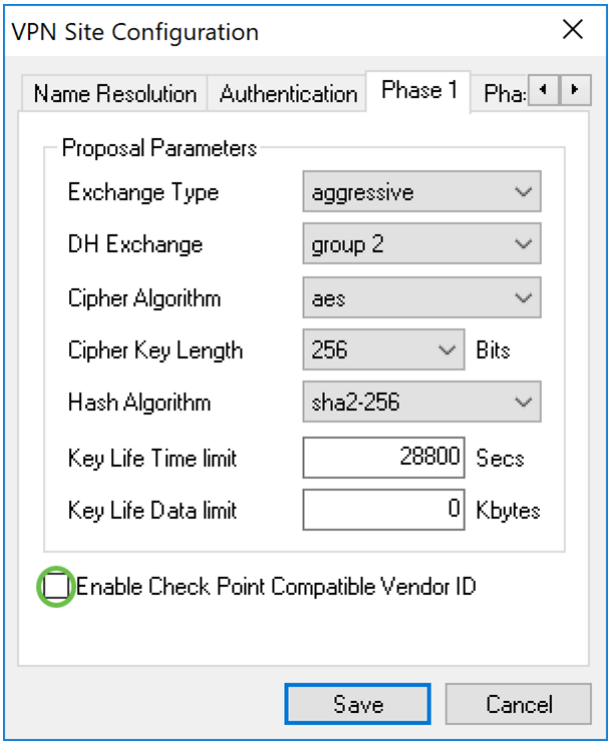
Algoritmo • Hash: **sha2-256**

Limite de tempo de vida principal •: **28800**

Limite • de dados de vida útil: **0**



Etapa 2. (Opcional) Se o gateway oferecer uma ID de fornecedor compatível com a Cisco durante as negociações da fase 1, marque a caixa de seleção **Enable Check Point Compatible Vendor ID**. Se a porta não oferecer uma ID de fornecedor compatível com a Cisco ou se você não tiver certeza, deixe a caixa de seleção desmarcada. Vamos deixar a caixa de seleção desmarcada.



Shrew Soft VPN Client: Guia Fase 2

Etapa 1. Clique na guia *Fase 2*. Configure os parâmetros a seguir para ter as mesmas configurações que você configurou para o RV160/RV260.

Os parâmetros devem corresponder à configuração RV160/260 na Fase 2 da seguinte forma:

Algoritmo •: **esp-aes**

• Comprimento da Chave: **256**

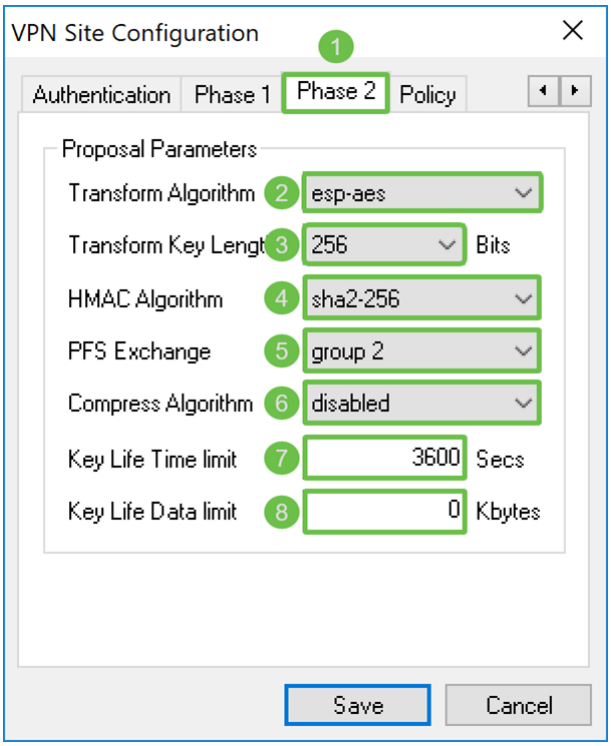
Algoritmo • HMAC: **sha2-256**

Troca • PFS: **grupo 2**

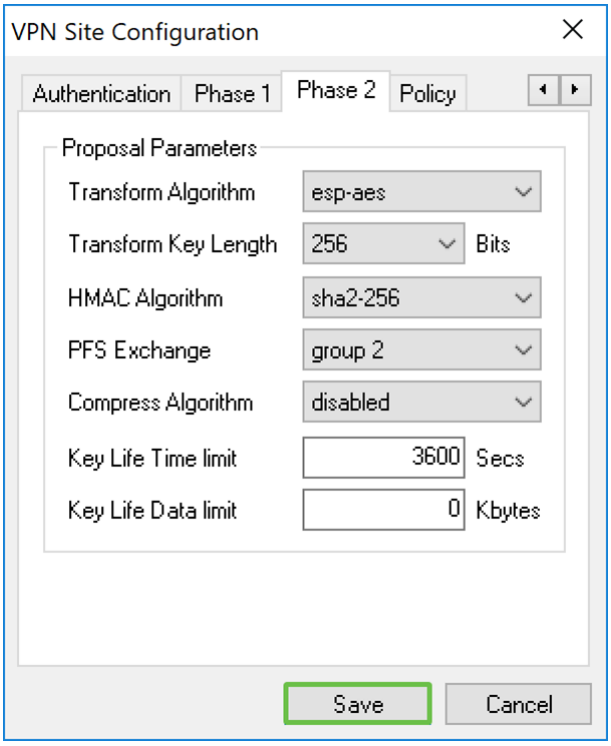
Algoritmo • Compress: **Desabilitado**

Limite de tempo de vida principal •: **3600**

Limite • de dados de vida útil: **0**



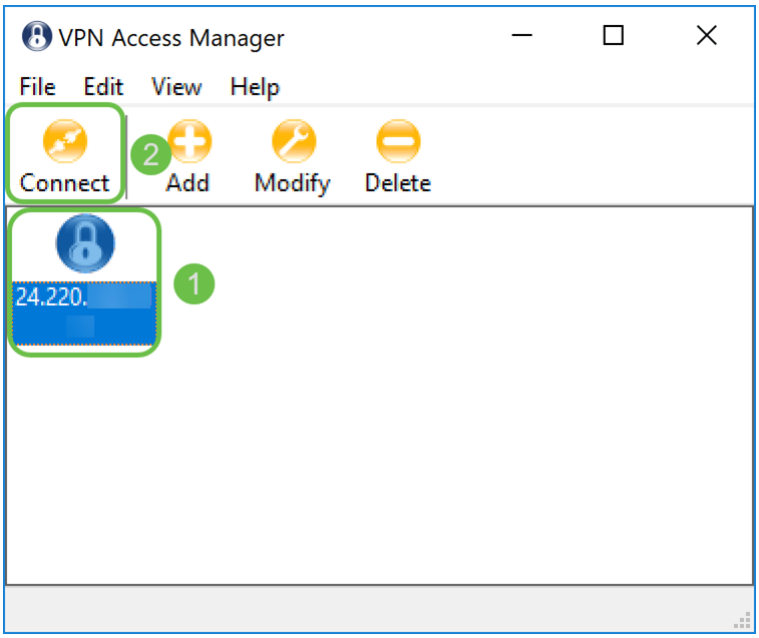
Etapa 2. Pressione o botão **Save (Salvar)** na parte inferior da página para salvar sua configuração.



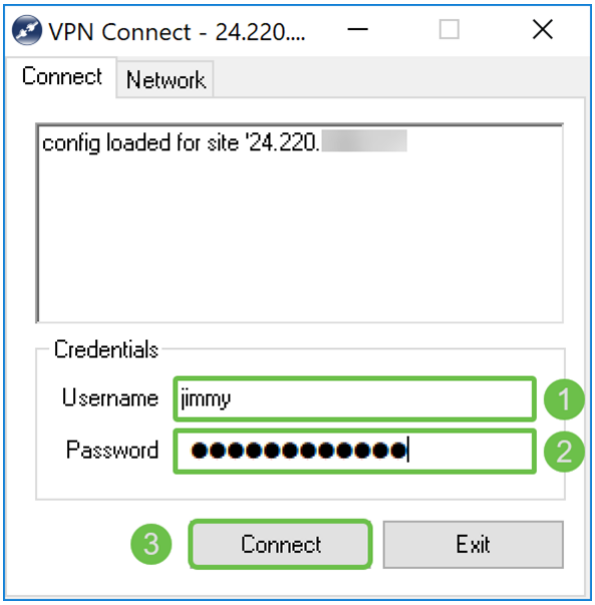
Shrew Soft VPN Client: Conectando

Etapa 1. No *VPN Access Manager*, selecione o perfil de VPN que acabou de criar. Em seguida, pressione **Connect (Conectar)**.

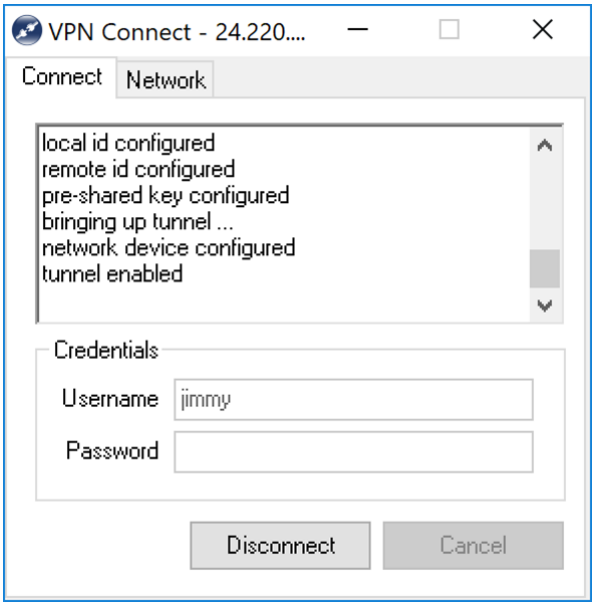
Note: Se desejar renomear o perfil da VPN, clique com o botão direito do mouse nele e selecione **Renomear**. Parte do endereço IP no perfil é desfocada para proteger essa rede.



Etapa 2. Uma janela *VPN Connect* é exibida. Digite o nome de usuário e a senha que foram criados na seção *Criando conta de usuário*. Em seguida, pressione **Connect (Conectar)**.

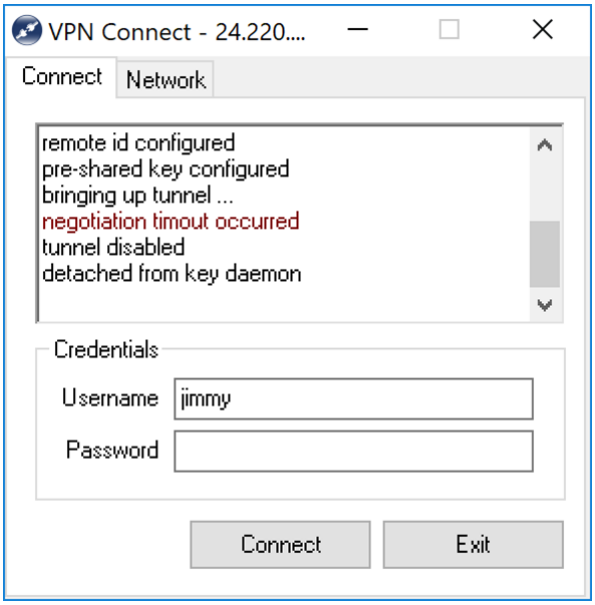


Etapa 3. Depois de pressionar *Connect*, as informações de configuração são passadas para o Daemon IKE juntamente com uma solicitação para se comunicar. Mensagens diferentes do estado da conexão são exibidas na janela de saída. Se a conexão for bem-sucedida, você receberá uma mensagem que diz, "dispositivo de rede configurado" e "túnel ativado". O botão *Connection* será alterado para um botão *Disconnect*.

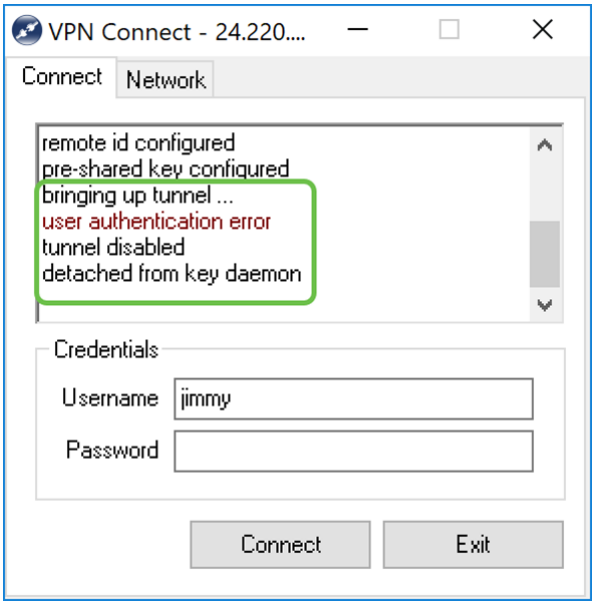


Dicas de solução de problemas de conexão VPN

Se você receber mensagens de erro que dizem: "timeout de negociação ocorreu", "tunnel disabled" e "desconectado do daemon chave". Você pode verificar duas vezes sua configuração no roteador e no cliente Shrew Soft VPN para garantir que eles correspondam.

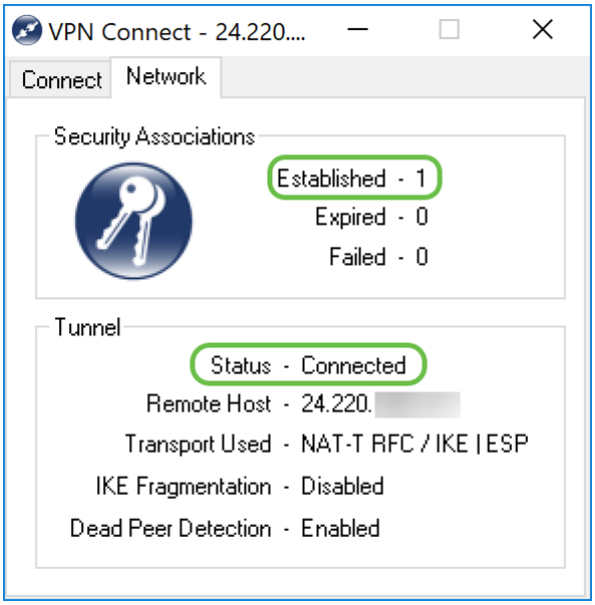


Se você receber uma mensagem de erro que diz "erro de autenticação de usuário", significa que você inseriu a senha incorreta para esse nome de usuário. Verifique duas vezes as credenciais do usuário e certifique-se de que estejam corretamente configuradas e inseridas.

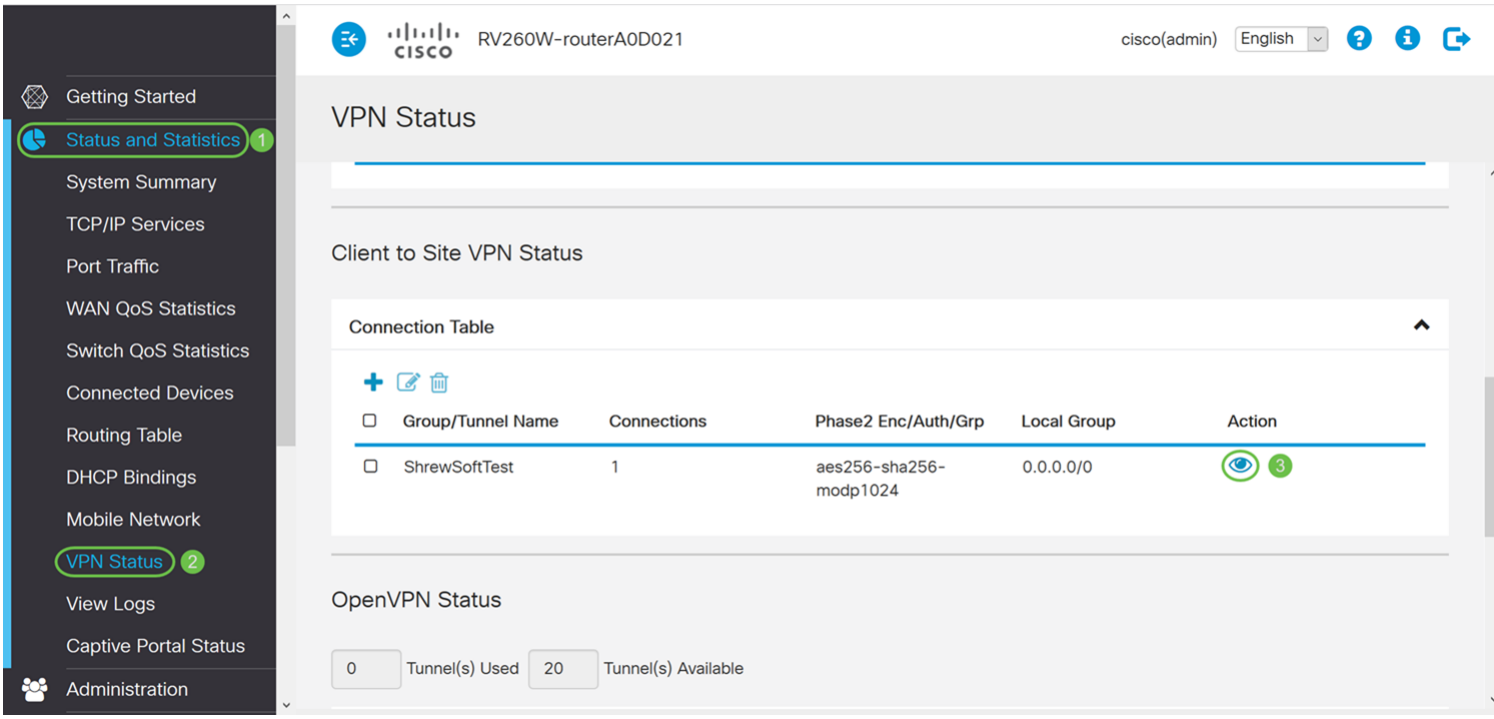


Verificação

Etapa 1. Clique na guia *Rede* na janela *VPN connect*. Nessa guia, você deve ser capaz de exibir as estatísticas atuais da rede para a conexão. Na seção *Túnel*, você deve ver *Connected* como o status.

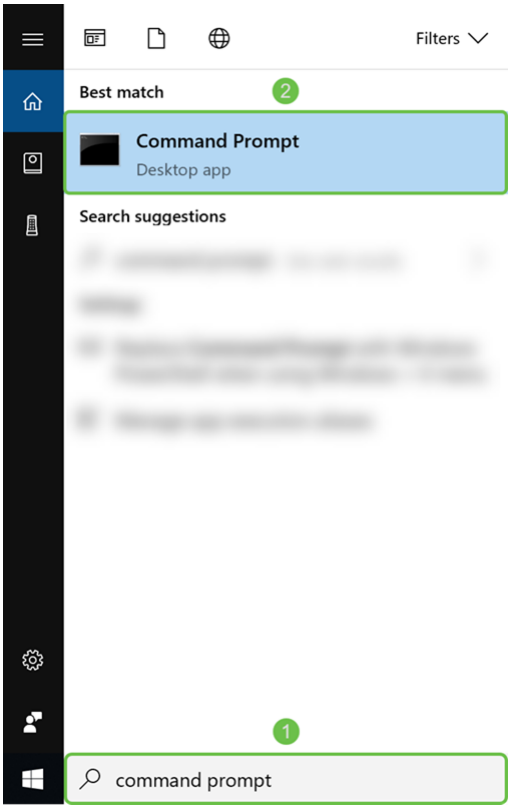


Etapa 2. No roteador, navegue para **Status and Statistics > VPN Status**. Na página *VPN Status*, role para baixo até a seção *Client to Site VPN Status*. Nesta seção, você pode visualizar todas as conexões Cliente-Site. Clique no ícone **de olho** para ver mais detalhes.



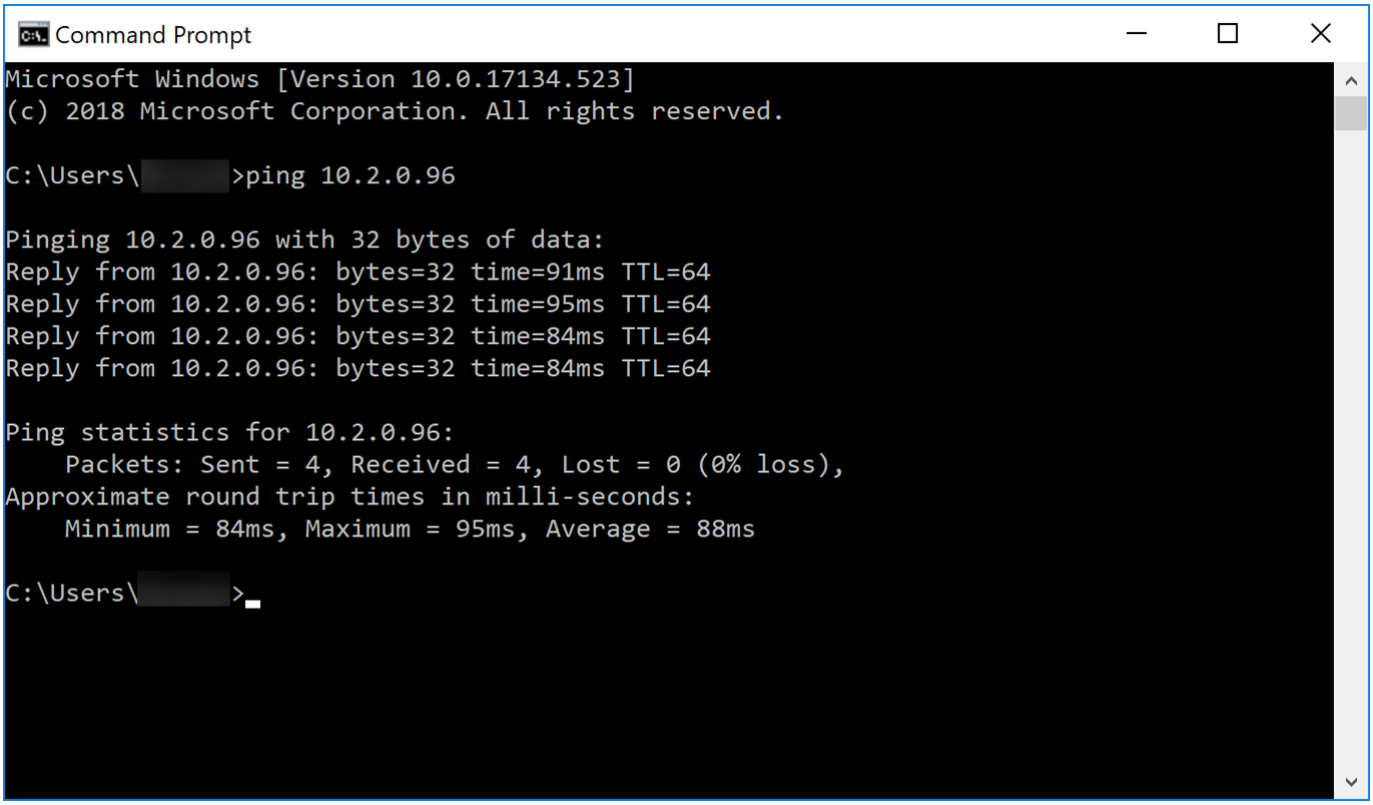
Etapa 3. Navegue até a barra de pesquisa na barra de tarefas e procure **Command Prompt**.

Note: As instruções a seguir são usadas em um sistema operacional Windows 10. Isso pode variar dependendo do sistema operacional que você está usando.



Etapa 4. Digite o comando sem aspas, "**ping [*private IP address of the router*]**" (**ping [*endereço IP privado do roteador*]**), mas insira o endereço IP privado em vez das palavras. Você deve conseguir fazer ping com êxito no endereço IP privado do roteador.

Neste exemplo, vamos digitar **ping 10.2.0.96**. 10.2.0.96 é o endereço IP privado do roteador.



Conclusão

Agora você deve ter conectado com êxito seu cliente Shrew Soft VPN com RV160 ou RV260.