# Configurar e usar o cliente VPN IPsec GreenBow para se conectar aos roteadores RV160 e RV260

## Objetivo

O objetivo deste documento é configurar e usar o cliente VPN IPsec do GreenBow para se conectar aos roteadores RV160 e RV260.

## Introduction

Uma conexão VPN (Virtual Private Network) permite que os usuários acessem, enviem e recebam dados de e para uma rede privada por meio de uma rede pública ou compartilhada, como a Internet, mas ainda garantindo uma conexão segura com uma infraestrutura de rede subjacente para proteger a rede privada e seus recursos.

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 à sua rede privada mesmo que estejam fora do escritório.

A VPN permite que um host remoto, ou cliente, atue como se estivesse localizado na mesma rede local. O roteador RV160 suporta até 10 túneis VPN, e o RV260 suporta até 20. Uma conexão VPN pode ser configurada entre o roteador e um endpoint depois que o roteador tiver sido configurado para conexão com a Internet. O cliente VPN depende inteiramente das configurações do roteador VPN para poder estabelecer uma conexão. As configurações devem corresponder exatamente ou não podem se comunicar.

O GreenBow VPN Client é um aplicativo de cliente VPN de terceiros que possibilita que um dispositivo host configure uma conexão segura para o túnel IPsec de cliente para site com os roteadores das séries RV160 e RV260.

## Benefícios do uso de uma conexão VPN

Usar uma conexão VPN ajuda a proteger dados e recursos confidenciais da rede.

Ele oferece conveniência e acessibilidade para funcionários remotos ou corporativos, já que eles poderão acessar facilmente o escritório principal sem ter que estar fisicamente presente e ainda assim manter a segurança da rede privada e seus recursos.

A comunicação usando uma conexão VPN fornece um nível mais alto de segurança comparado a outros métodos de comunicação remota. Um algoritmo de criptografia avançado torna isso possível, protegendo a rede privada de acesso não autorizado.

As localizações geográficas reais dos usuários são protegidas e não expostas a redes públicas ou compartilhadas como a Internet.

Uma VPN permite que novos usuários ou um grupo de usuários sejam adicionados sem a necessidade de componentes adicionais ou de uma configuração complicada.

# Riscos do uso de uma conexão VPN

Pode haver riscos à segurança devido a configurações incorretas. Como o projeto e a implementação de uma VPN podem ser complicados, é necessário confiar a tarefa de configurar a conexão a um profissional altamente qualificado e experiente para garantir que a segurança da rede privada não seja comprometida.

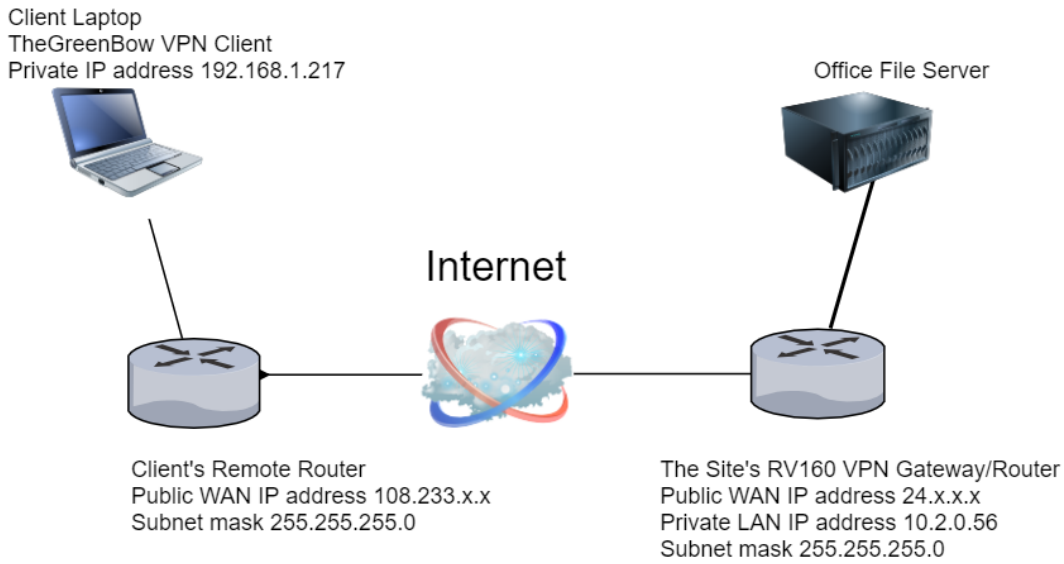
Pode ser menos confiável. Como uma conexão VPN requer uma conexão com a Internet, é importante ter um provedor com uma reputação comprovada e testada para fornecer um excelente serviço de Internet e garantir um tempo de inatividade mínimo ou nulo.

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.

Velocidades de conexão lentas podem ocorrer. Se você estiver usando um cliente VPN que fornece serviço VPN gratuito, é de esperar que sua conexão também seja lenta, já que esses provedores não priorizam as velocidades de conexão. Neste artigo, usaremos um terceiro pago para eliminar esse problema.

# Topologia básica da rede cliente-local

Este é o layout básico da rede para configuração. Os endereços IP da WAN pública foram parcialmente turvos ou estão mostrando um **x** no lugar dos números reais para proteger esta rede de ataques.




Este artigo abordará as etapas necessárias para configurar o roteador RV160 ou RV260 no local para o seguinte:

- Um grupo de usuários — **VPNUsers**
- Contas de usuário (um ou mais usuários) que terão acesso como cliente
- Um perfil IPsec — **TheGreenBow**
- Um perfil cliente-local — **cliente**
- Você também verá como visualizar o status da VPN no site quando o cliente estiver

conectado

**Note:** Você pode usar qualquer nome para o Grupo de usuários, Perfil IPsec e Perfil cliente-local. Os nomes listados são apenas exemplos.

Este artigo também explica as etapas que cada cliente deve seguir para configurar a VPN TheGreenBow em seu computador:

- Baixe e configure o software cliente VPN GreenBow
- Defina as configurações das fases 1 e 2 para o cliente
- Iniciar e verificar uma conexão VPN como um cliente

É essencial que cada configuração no roteador no local corresponda às configurações do cliente. Se a sua configuração não levar a uma conexão VPN bem-sucedida, verifique todas as configurações para garantir que elas correspondam. O exemplo mostrado neste artigo é apenas uma maneira de configurar a conexão.

# Table Of Contents



# Dispositivos aplicáveis

- RV160
- RV260

# Versão de software

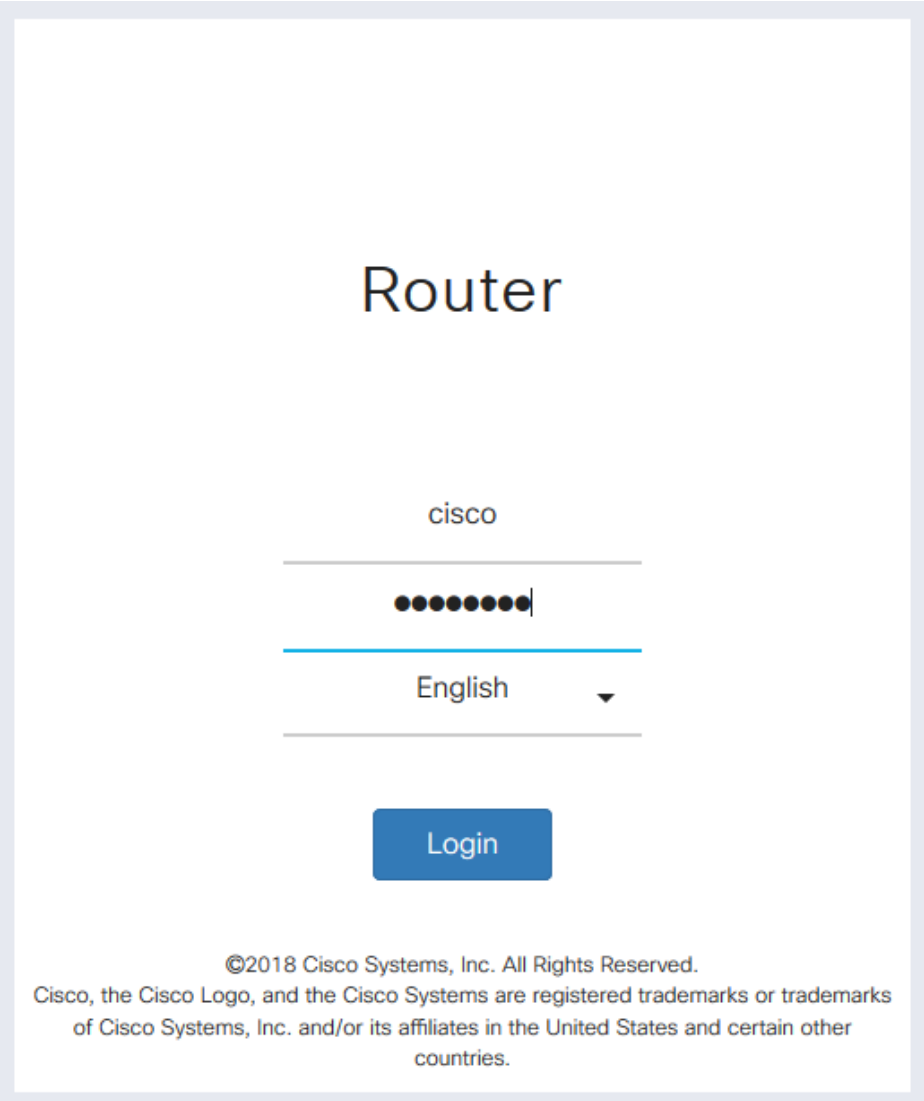
- 1.0.00.15

# Configurar o VPN Client no site do roteador RV160 ou RV260

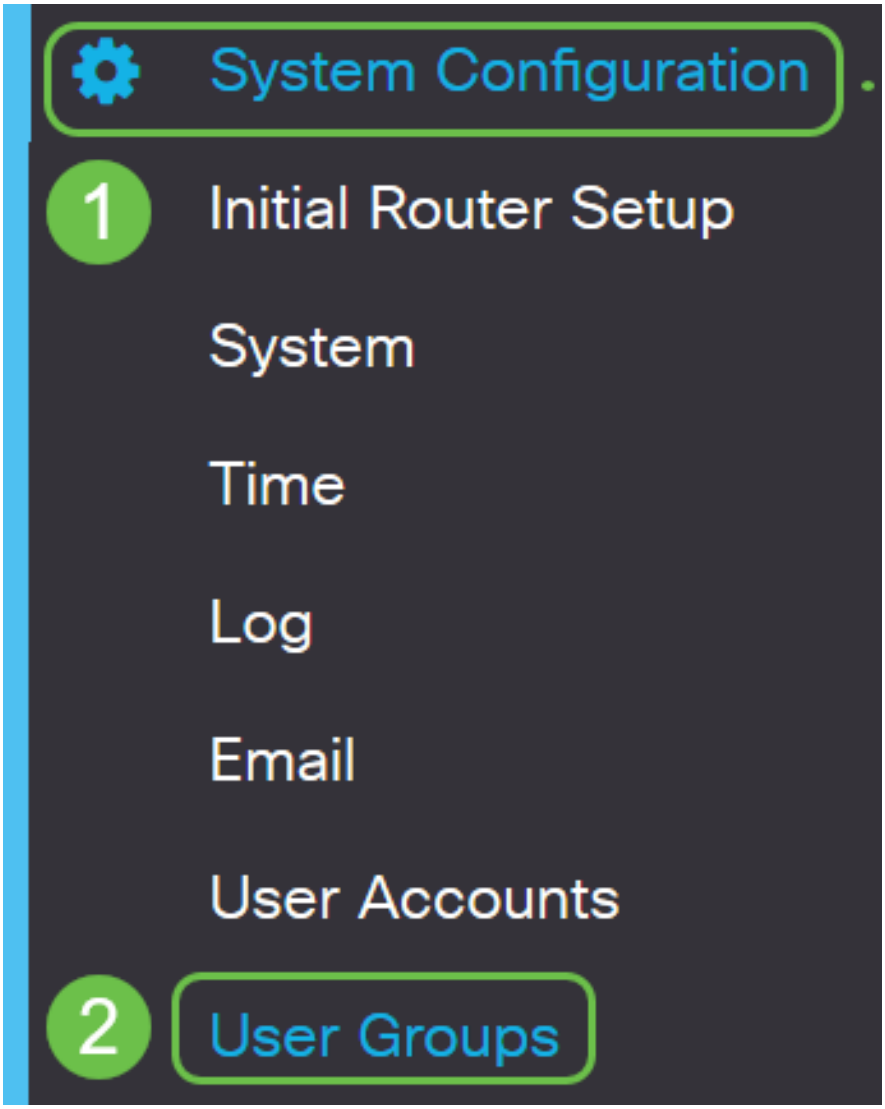
## Criar um grupo de usuários

**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 o TheGreenBow. Se você mover sua conta de administrador para um grupo diferente, você impedirá que você faça login no roteador.

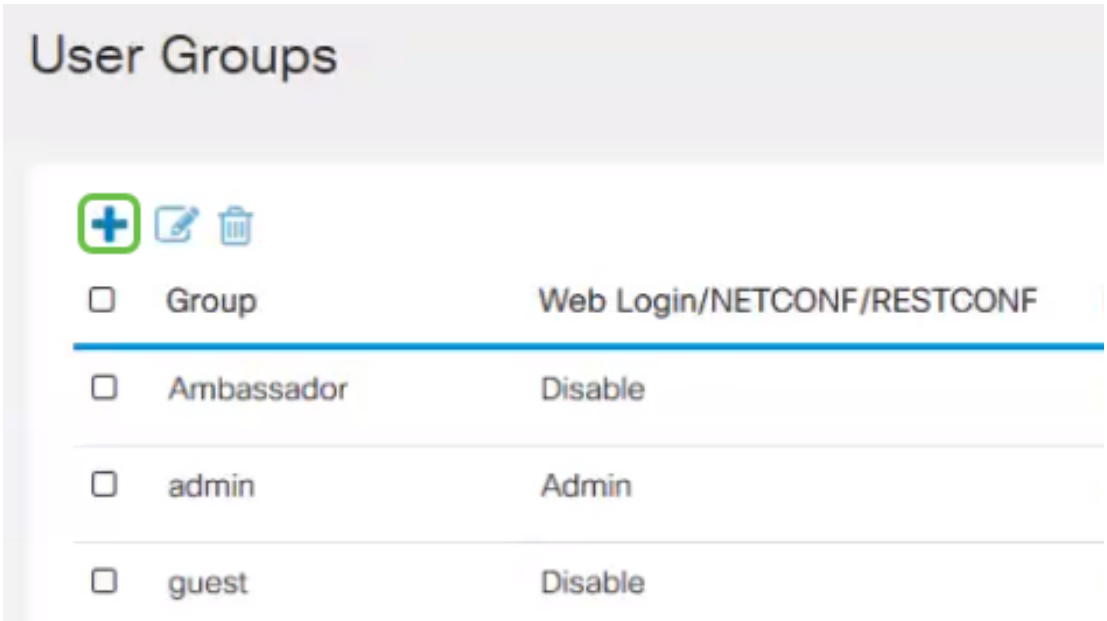
Etapa 1. Faça login no utilitário baseado na Web do roteador.



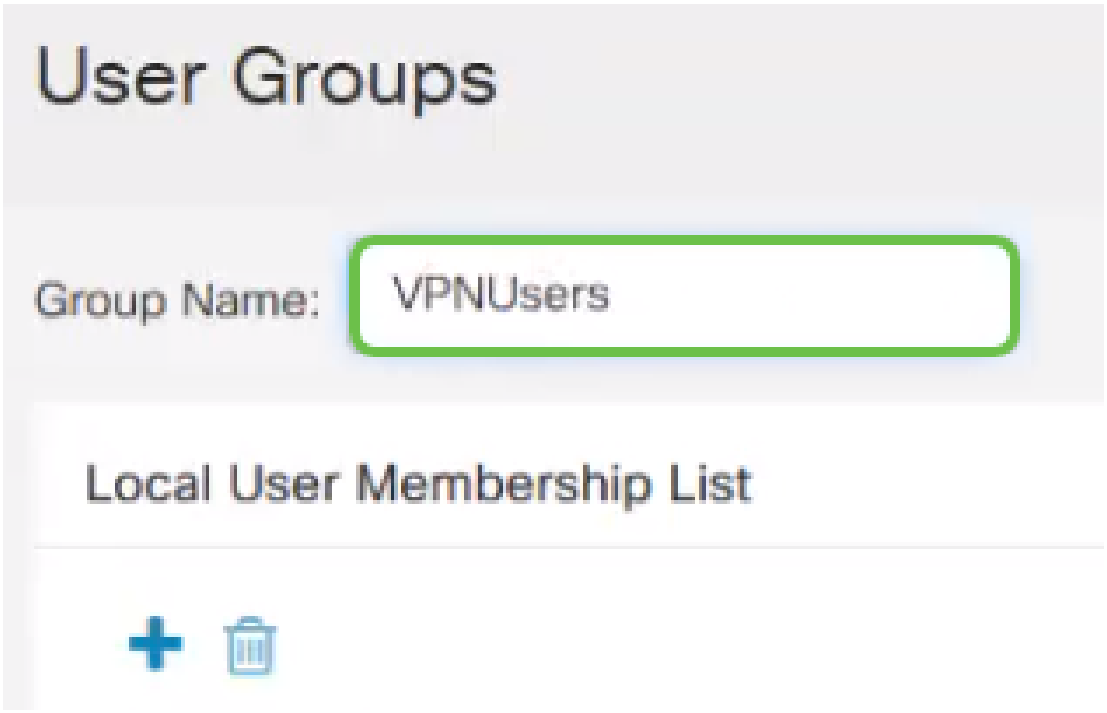

Etapa 2. Selecione **Configuração do sistema > Grupos de usuários**.



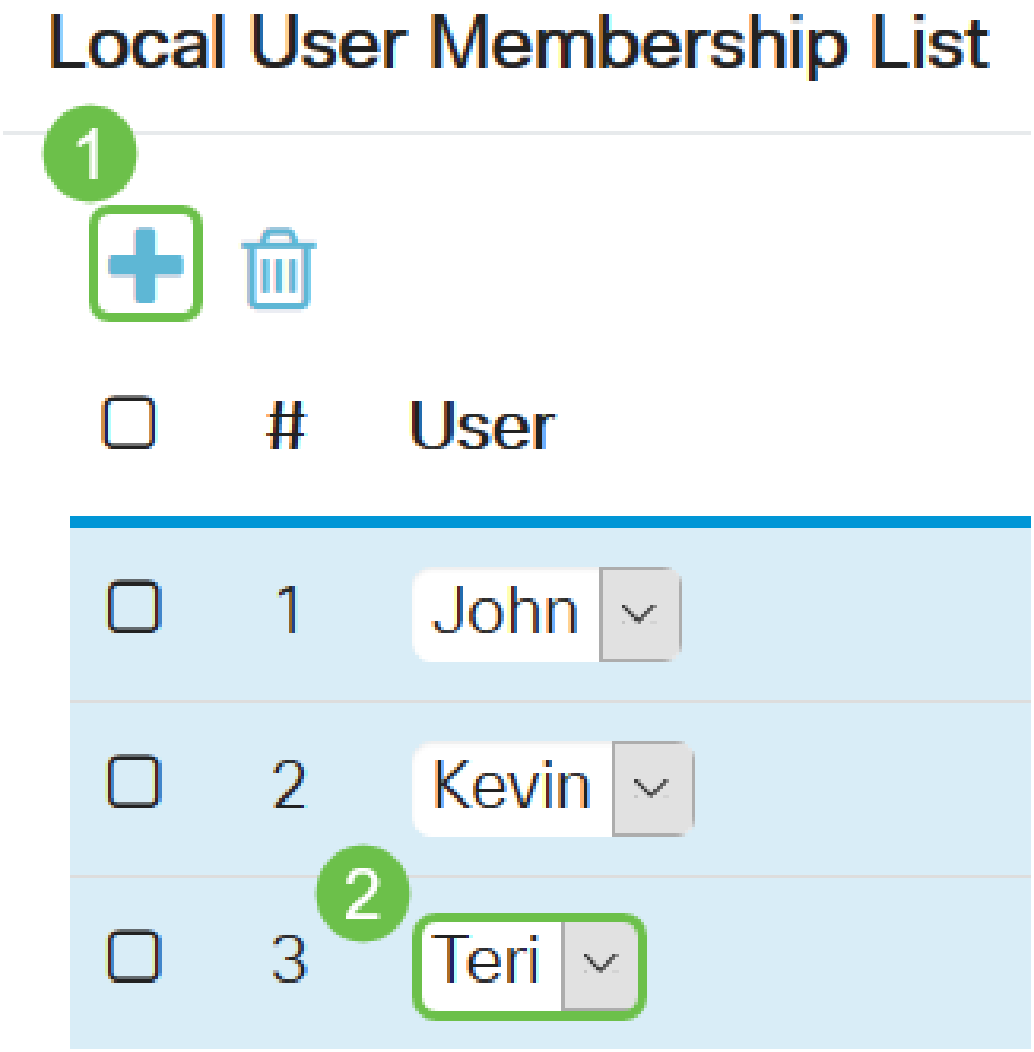

Etapa 3. Clique no ícone **de mais** para adicionar um grupo de usuários.




Etapa 4. Na área Visão geral, insira o nome do grupo no campo *Nome do grupo*.



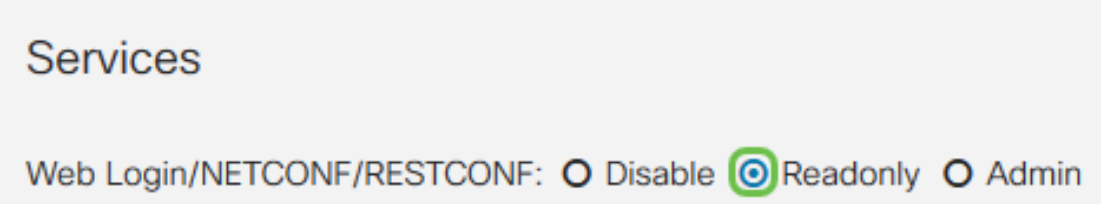

Etapa 5. Em *Lista de membros de usuários locais*, clique no ícone **de mais** e selecione o usuário na lista suspensa. Para adicionar mais, pressione o ícone **de mais** novamente e selecione outro membro a ser adicionado. Os membros só podem fazer parte de um grupo. Se você ainda não tiver todos os usuários inseridos, poderá adicionar mais na seção Criar uma conta de usuário.



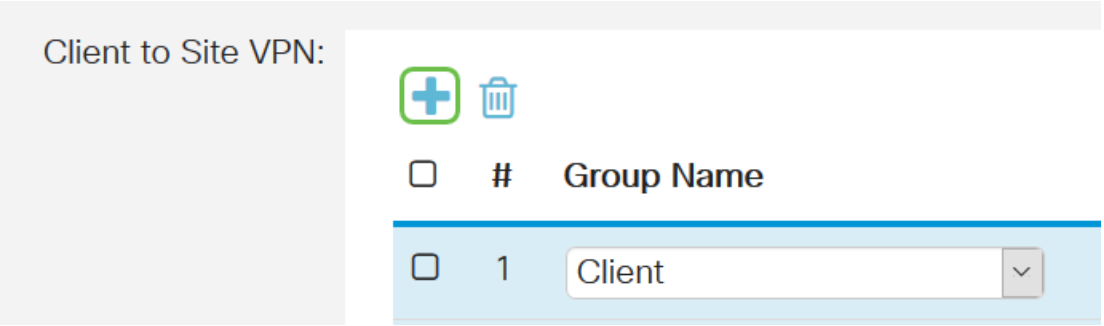

Etapa 6. Em *Serviços*, escolha uma permissão a ser concedida aos usuários do grupo. As opções

são:

- Desativado — Essa opção significa que os membros do grupo não têm permissão para acessar o utilitário baseado na Web por meio de um navegador.
- Somente leitura — Essa opção significa que os membros do grupo só podem ler o status do sistema depois de fazer login. Eles não podem editar nenhuma das configurações.
- Admin — Essa opção dá aos membros do grupo privilégios de leitura e gravação e pode configurar o status do sistema.



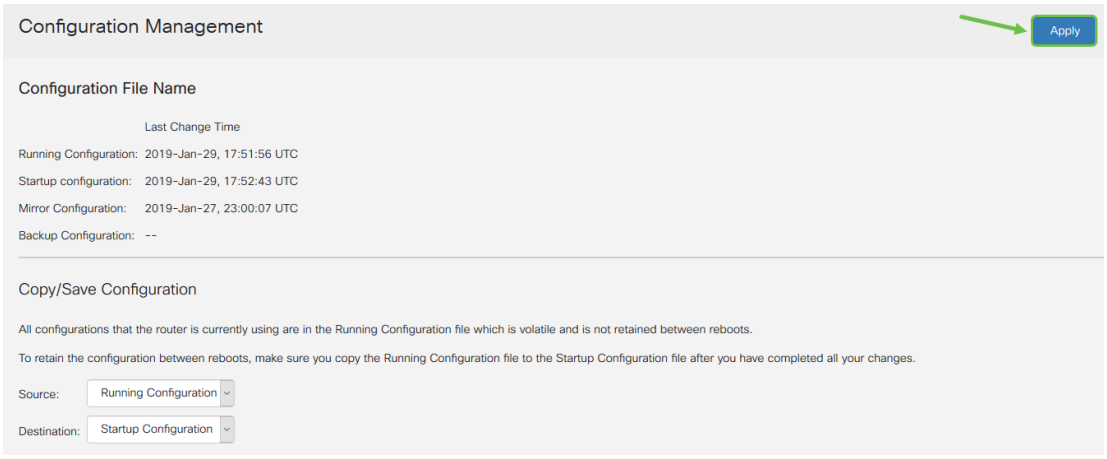

Passo 7. Clique no ícone de **mais** para adicionar uma VPN cliente a site existente. Se você não tiver configurado isso, poderá encontrar informações neste artigo na seção Criar um perfil cliente-local.




Etapa 8. Clique em Apply.


Etapa 9. Click **Save**.


Etapa 10. Clique em **Apply** novamente para salvar a configuração atual na configuração de inicialização.

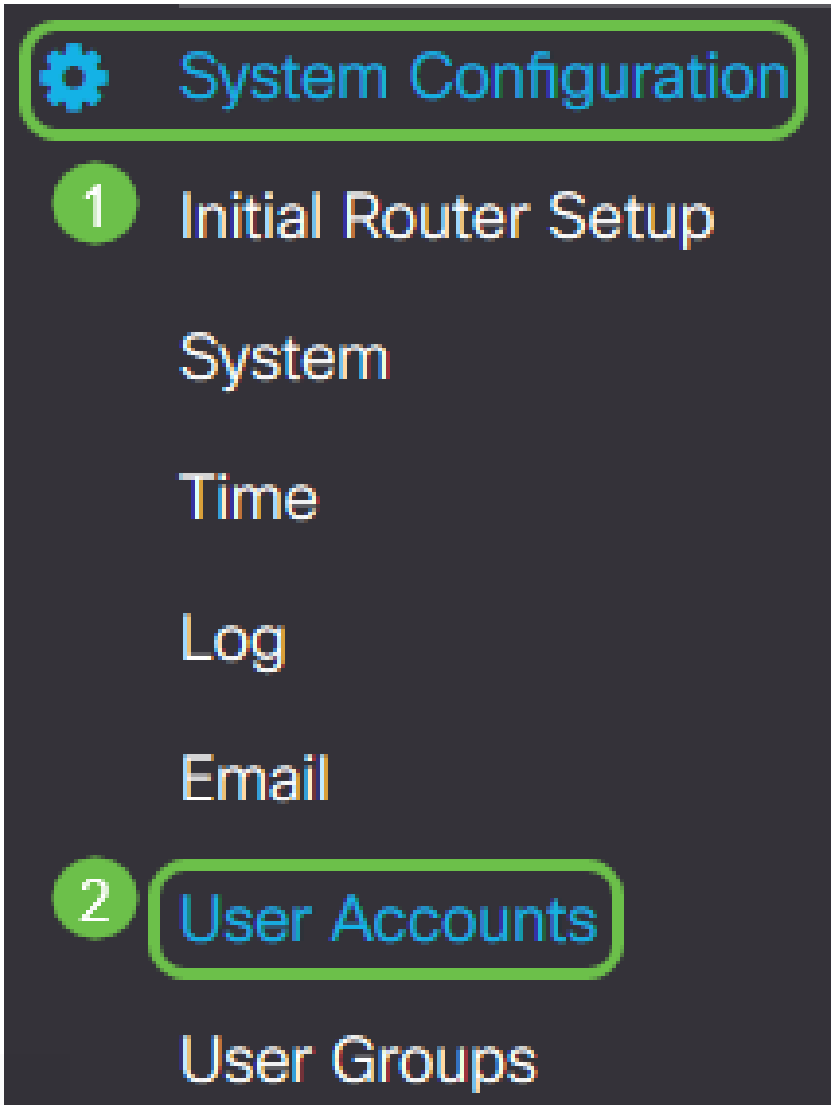



Etapa 11. Quando você receber a confirmação, clique em **OK**.

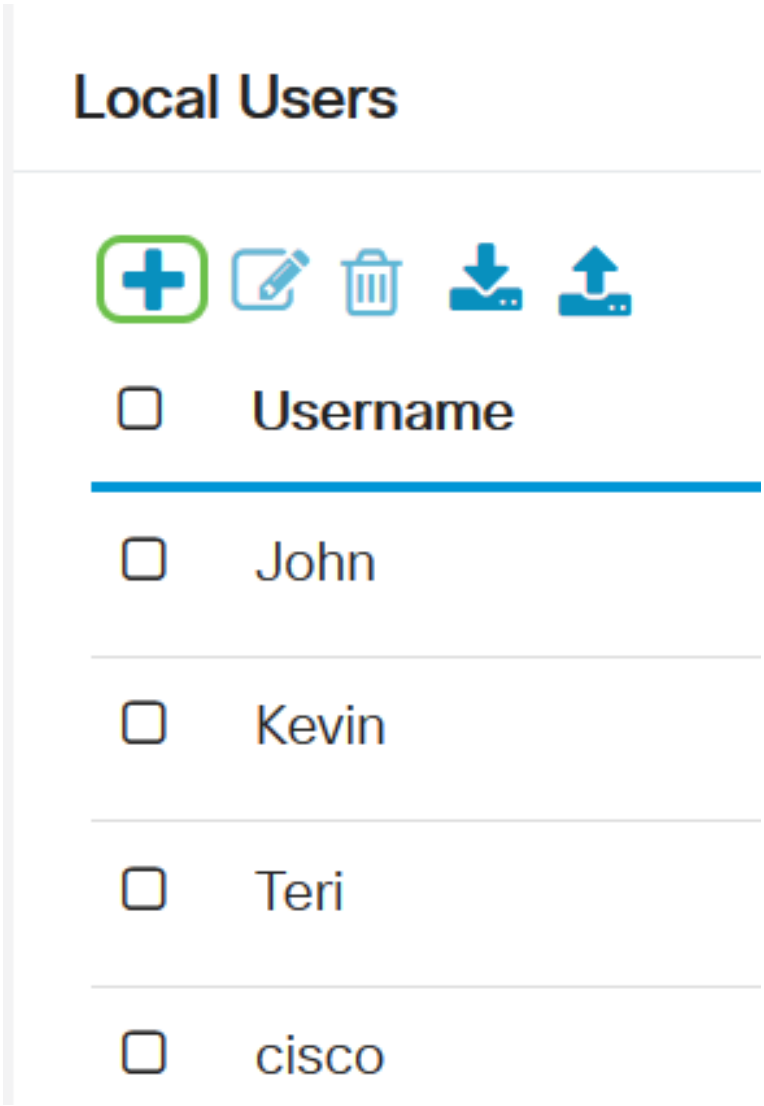

Agora você deve ter criado com êxito um grupo de usuários no RV160 ou RV260 Series Router.

## Criar uma conta de usuário

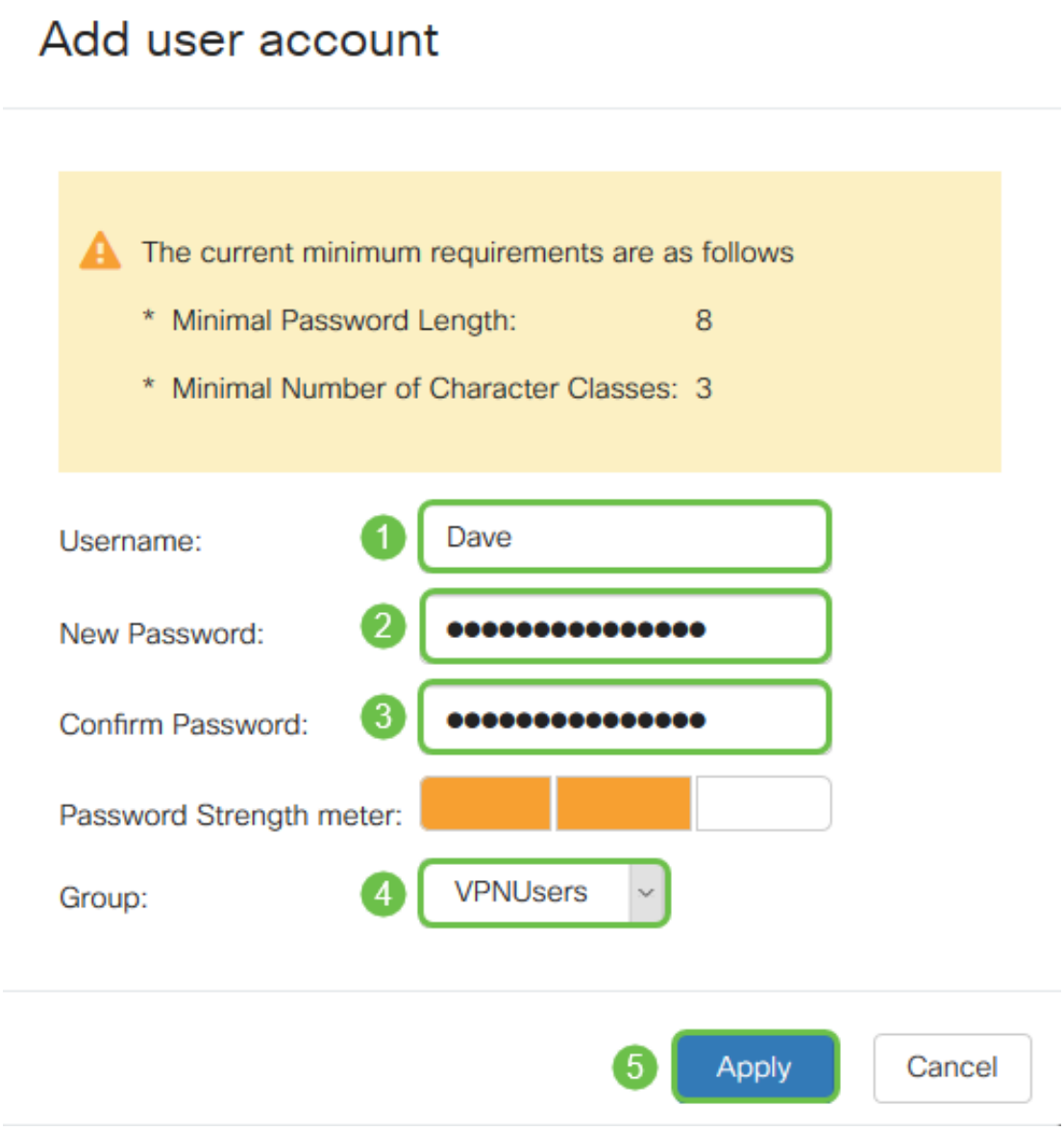
Etapa 1. Faça login no utilitário baseado na Web do roteador e escolha **Configuração do sistema > Contas de usuário**.




Etapa 2. Na área *Usuários locais*, clique no ícone **adicionar**.



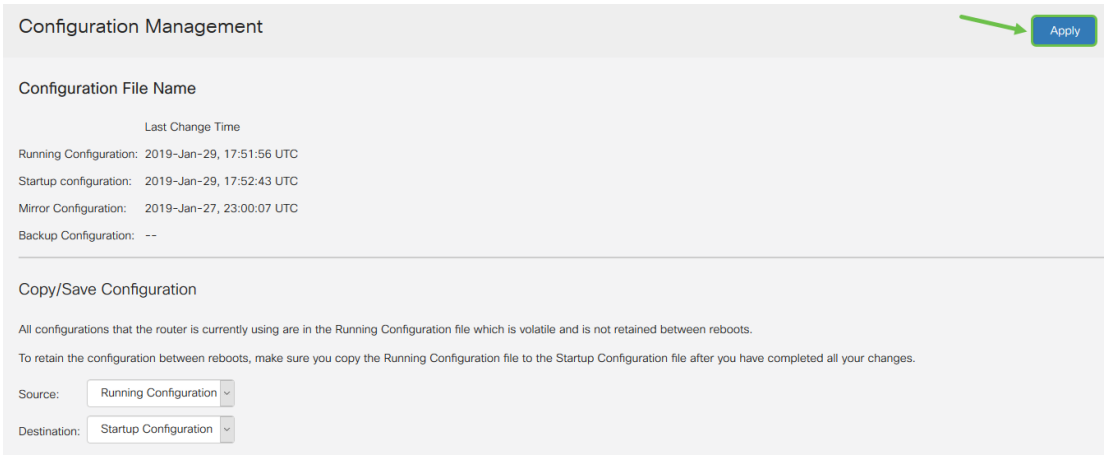

Etapa 3. Insira um nome para o usuário no campo *Nome de usuário*, a senha e o grupo ao qual deseja adicionar o usuário no menu suspenso. Clique em Apply.




**Note:** Quando o cliente configura o cliente TheGreenBow em seu computador, ele faz login com o mesmo nome de usuário e senha.

Etapa 4. Click **Save**.


Etapa 5. Clique em **Apply** novamente para salvar a configuração atual na configuração de inicialização.



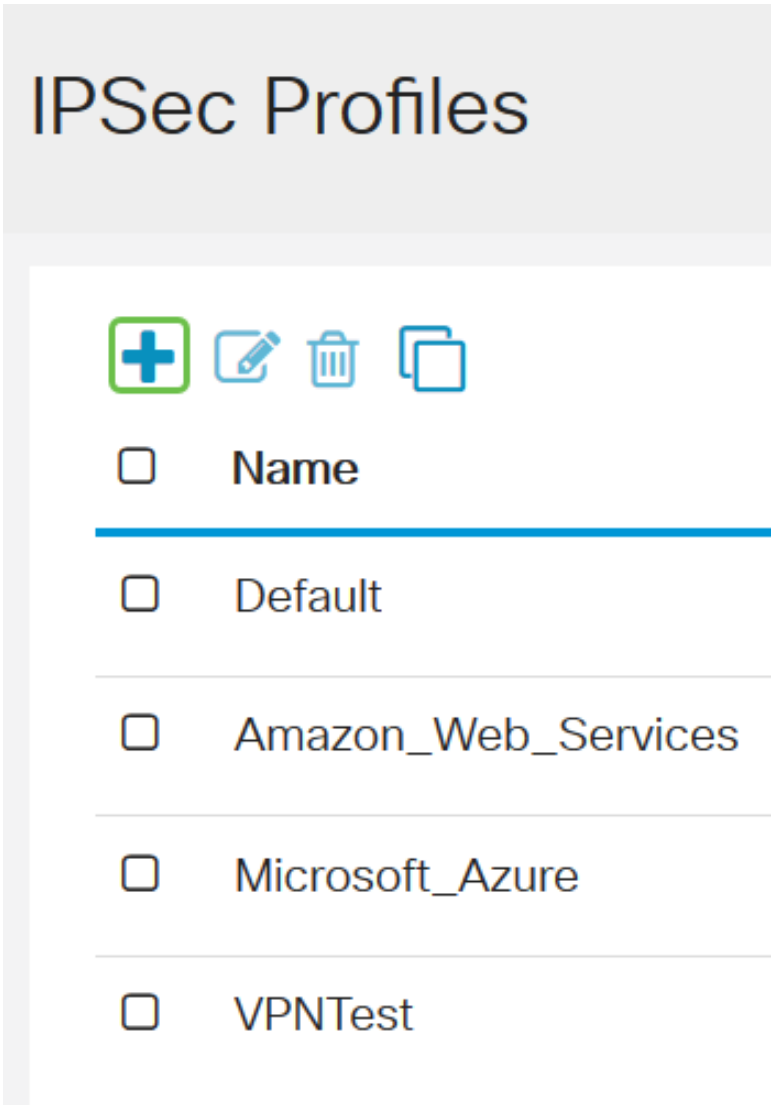

Etapa 6. Quando você receber a confirmação, clique em **OK**.


Agora você deve ter criado uma conta de usuário no roteador RV160 ou RV260.

## Configurar perfil IPsec

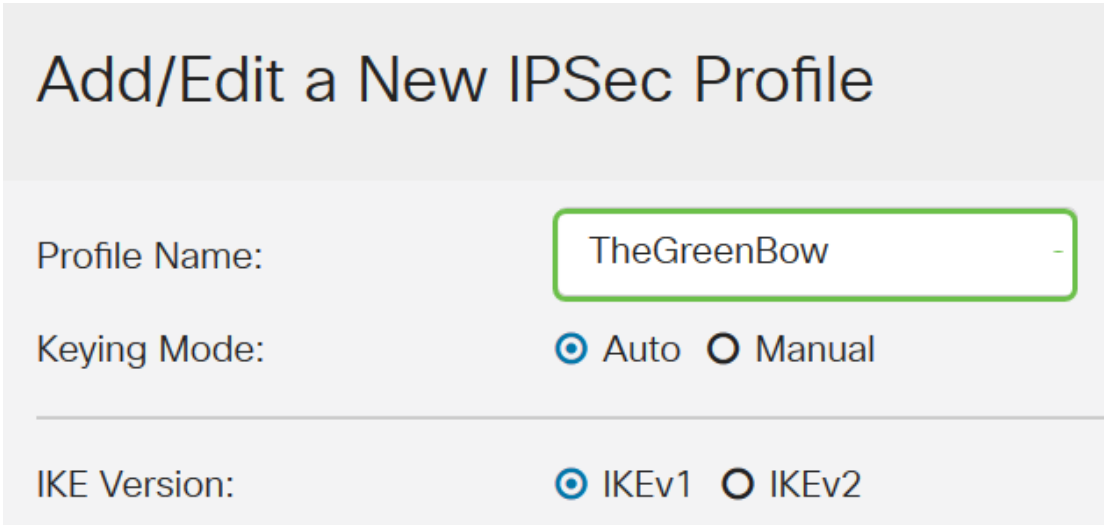
Etapa 1. Faça login no utilitário baseado na Web do roteador RV160 ou RV260 e escolha **VPN > IPSec VPN > Perfis IPSec**.


Etapa 2. A Tabela de perfis IPSec mostra os perfis existentes. Clique no ícone **de mais** para criar um novo perfil.




**Note:** Amazon_Web_Services, Default e Microsoft_Azure são perfis padrão.

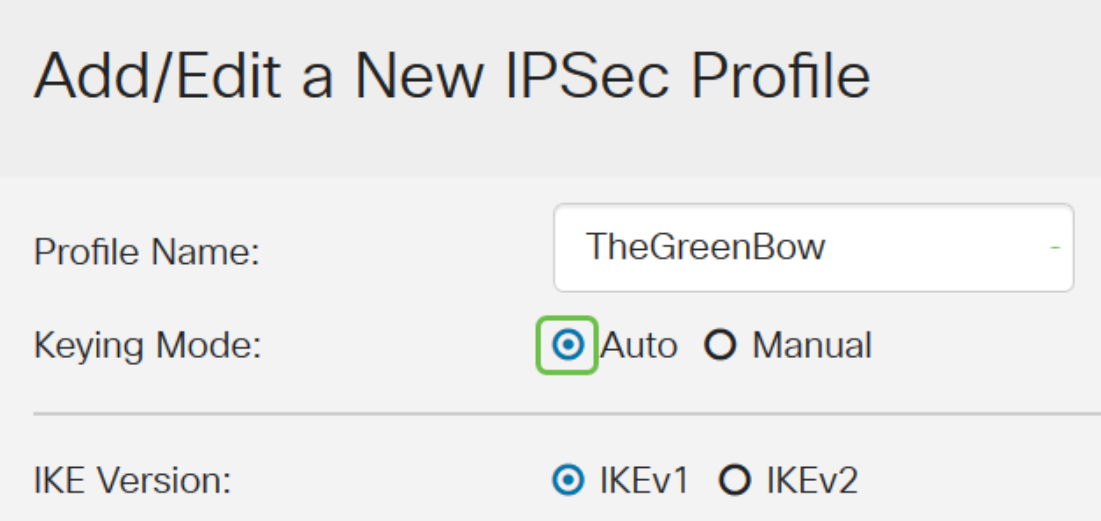
Etapa 3. Crie um nome para o perfil no campo *Nome do perfil*. O nome do perfil deve conter apenas caracteres alfanuméricos e um sublinhado (_) para caracteres especiais.




Etapa 4. Clique em um botão de opção para determinar o método de troca de chaves que o perfil usará para autenticar. As opções são:

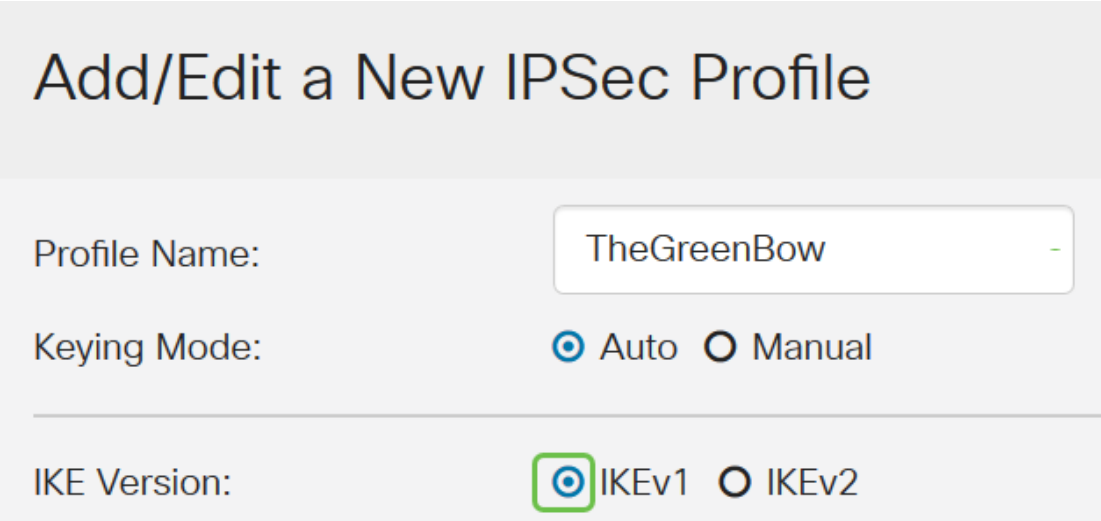
- Automático — Os parâmetros de política são definidos automaticamente. Esta opção usa uma política de Internet Key Exchange (IKE) para troca de chaves de criptografia e integridade de dados. Se isso for selecionado, as configurações na área Parâmetros de

política automática serão ativadas.
- Manual — Esta opção permite que você configure manualmente as chaves para criptografia e integridade de dados para o túnel VPN. Se isso for selecionado, as configurações na área Parâmetros de política manual serão ativadas. Isso não é muito usado.




**Note:** Para este exemplo, **Auto** foi escolhido.

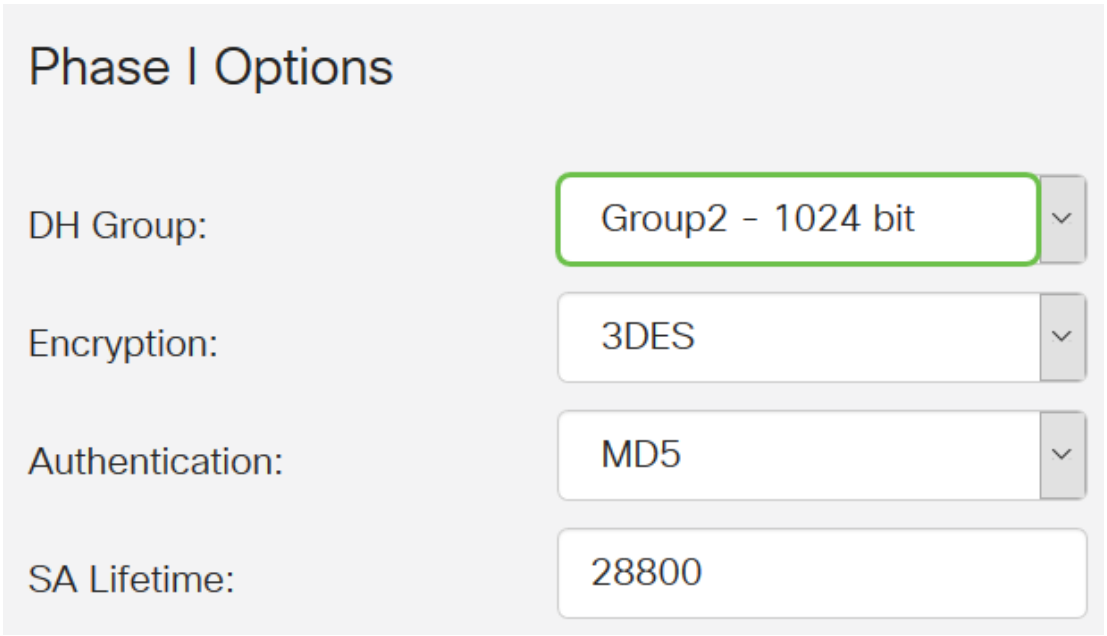
Etapa 5. Selecione a versão IKE. Certifique-se de que ao configurar o TheGreenBow no lado do cliente, a mesma versão é selecionada.




## Defina as configurações das fases 1 e 2

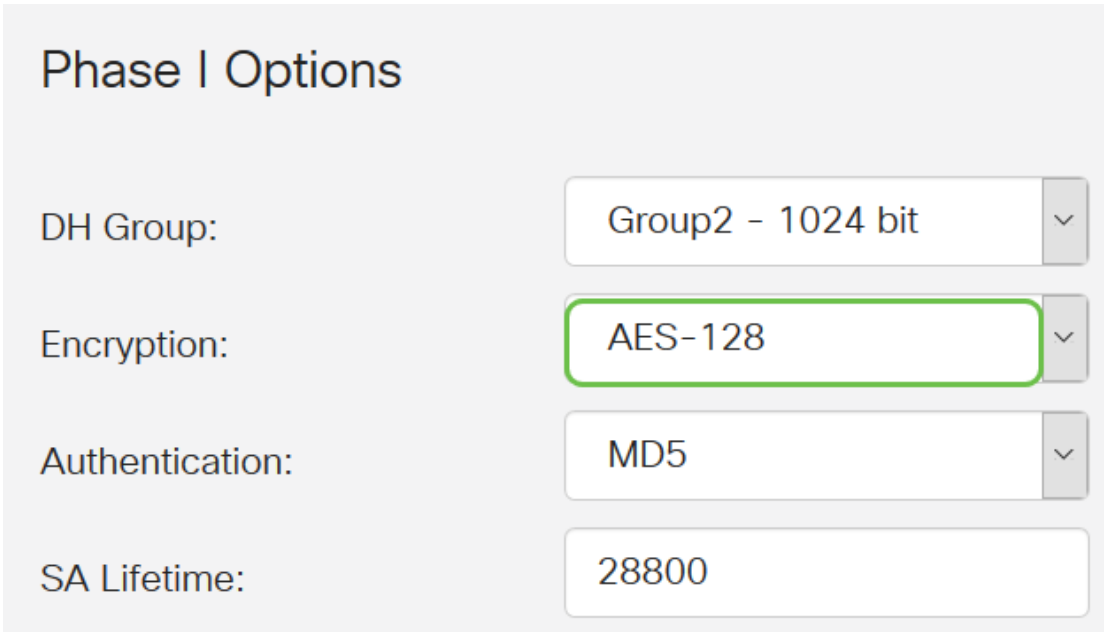
Etapa 1. Na área Opções da Fase 1, escolha o grupo Diffie-Hellman (DH) apropriado a ser usado com a chave na Fase 1 na lista suspensa *Grupo DH*. Diffie-Hellman é um protocolo de troca de chave criptográfica que é usado na conexão para trocar conjuntos de chaves pré-compartilhadas. A força do algoritmo é determinada por bits. As opções são:

- Grupo2-1024 bits — Essa opção computa a chave mais lentamente, mas é mais segura que o Grupo 1.
- Grupo5-1536 bits — Essa opção computa a chave mais lentamente, mas é a mais segura.




Etapa 2. Na lista suspensa *Criptografia*, escolha um método de criptografia para criptografar e descriptografar o ESP (Encapsulating Security Payload) e o ISAKMP (Internet Security Association and Key Management Protocol). As opções são:

- 3DES — Triple Data Encryption Standard (Padrão triplo de criptografia de dados). Não recomendado. Use-o somente se for necessário para compatibilidade com versões anteriores, pois é vulnerável a alguns ataques de "colisão de bloqueio".
- AES-128 — O Advanced Encryption Standard usa uma chave de 128 bits. O Advanced Encryption Standard (AES) é um algoritmo criptográfico projetado para ser mais seguro que o DES. O AES usa um tamanho de chave maior que garante que a única abordagem conhecida para descriptografar uma mensagem é que um invasor tente todas as chaves possíveis.
- AES-192 — O Advanced Encryption Standard usa uma chave de 192 bits.
- AES-256 — O Advanced Encryption Standard usa uma chave de 256 bits. Esta é a opção de criptografia mais segura.



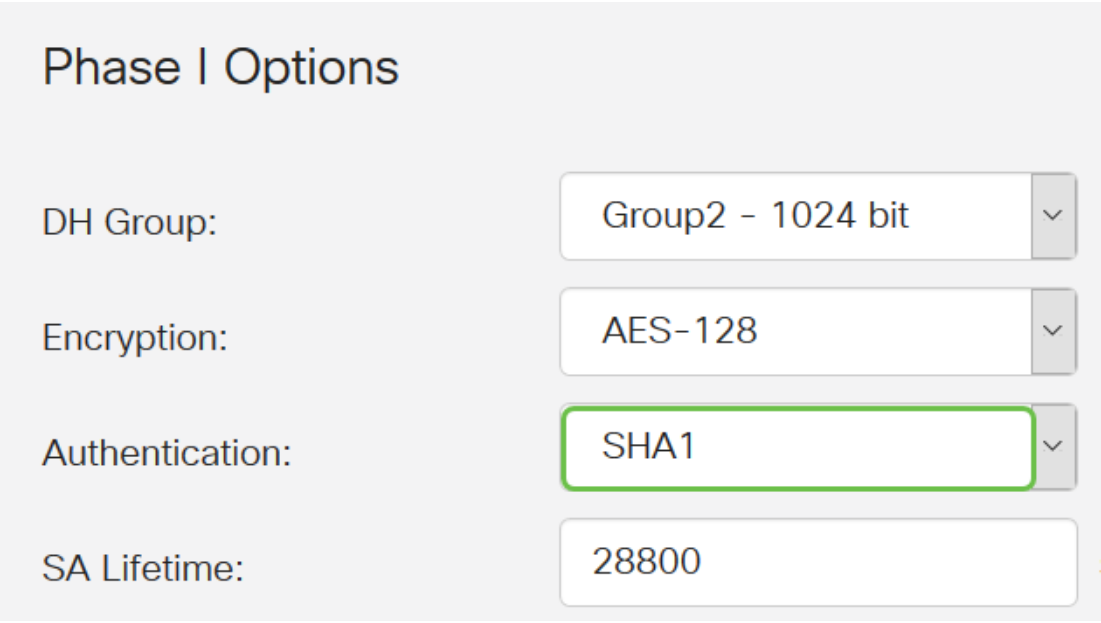

**Note:** O AES é o método padrão de criptografia sobre DES e 3DES por seu maior desempenho e segurança. O aumento da chave AES aumentará a segurança com uma queda no desempenho.

Etapa 3. Na lista suspensa *Autenticação*, escolha um método de autenticação que determinará

como o ESP e o ISAKMP são autenticados. As opções são:

- MD5 — O algoritmo Message-Digest tem um valor de hash de 128 bits.
- SHA-1 — O algoritmo de hash seguro tem um valor de hash de 160 bits.
- SHA2-256 — Algoritmo Hash Seguro com um valor hash de 256 bits. Esse é o algoritmo mais seguro e recomendado.

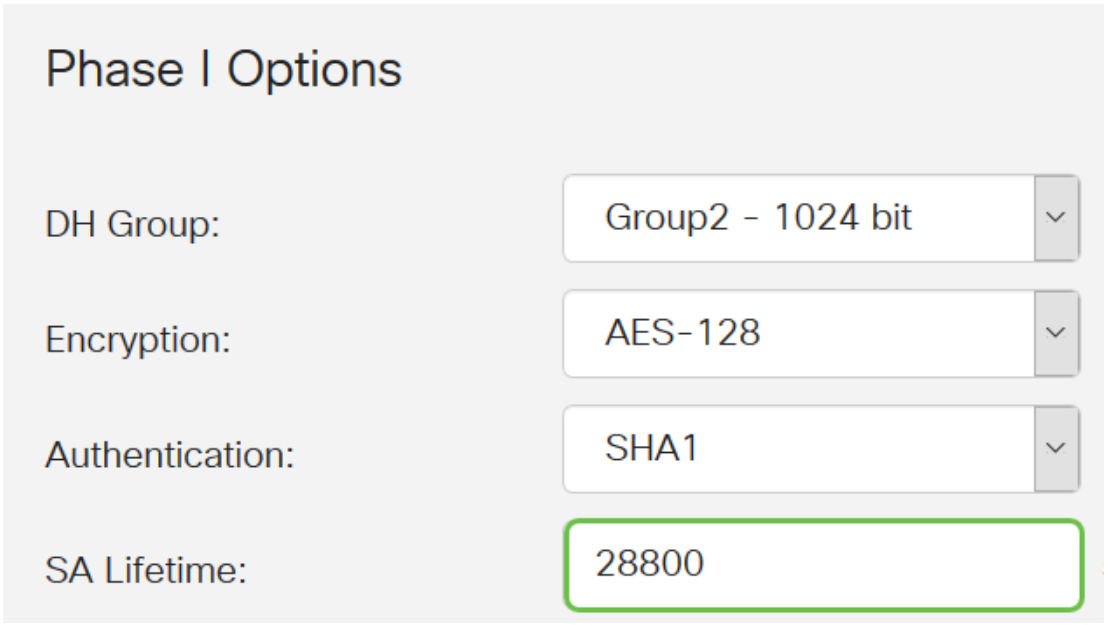
**Note:** Certifique-se de que ambas as extremidades do túnel VPN usem o mesmo método de autenticação.




**Note:** MD5 e SHA são funções de hash criptográfico. Eles pegam um pedaço de dados, compactam-no e criam uma saída hexadecimal exclusiva que normalmente não pode ser reproduzida. Neste exemplo, SHA1 é escolhido.

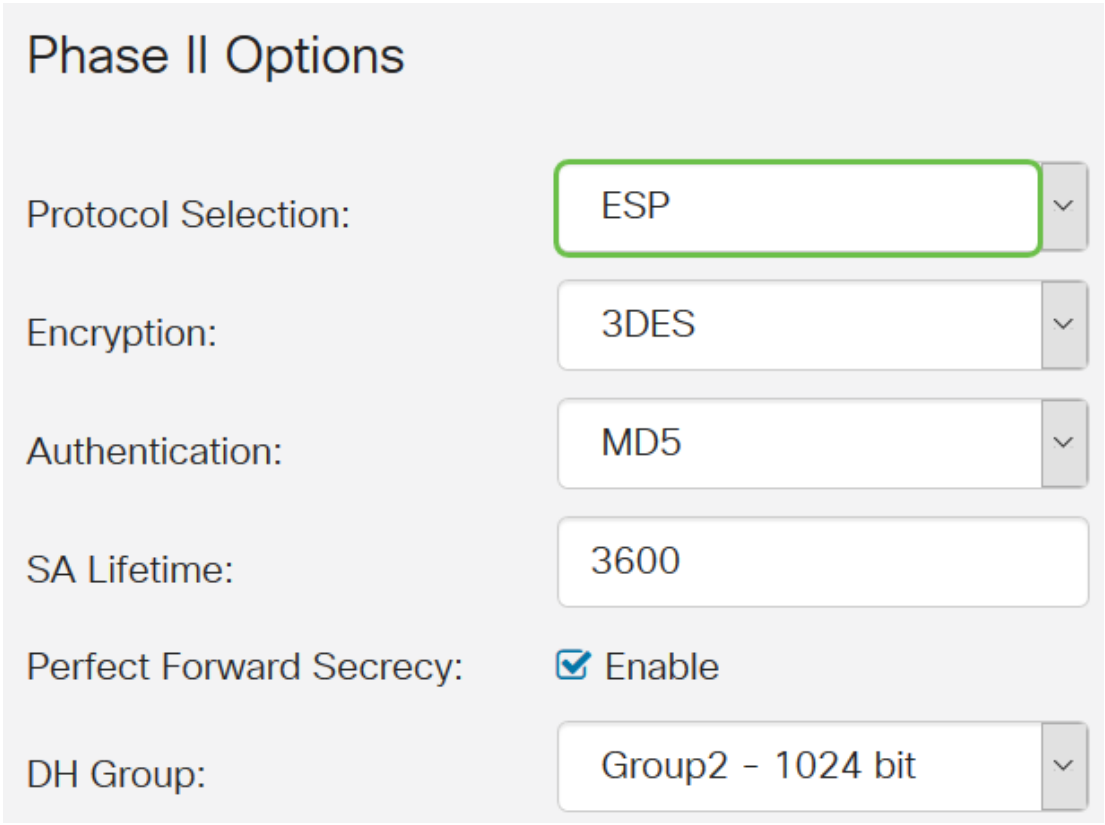
Etapa 4. No campo *Vida útil do SA*, insira um valor entre 120 e 86400. O valor padrão é 28800. O *SA Lifetime (Sec)* informa a quantidade de tempo, em segundos, em que um SA IKE está ativo nesta fase. Uma nova associação de segurança (SA) é negociada antes do tempo de vida expirar para garantir que uma nova SA esteja pronta para ser usada quando a antiga expirar. O padrão é 28800 e o intervalo é de 120 a 86400. Usaremos 28800 segundos como o tempo de vida da SA para a Fase I.

**Note:** Recomenda-se que a sua SA Lifetime na Fase I seja mais longa que a sua SA Lifetime de Fase II. Se você tornar sua Fase I mais curta que a Fase II, então terá que renegociar o túnel para frente e para trás frequentemente ao contrário do túnel de dados. O túnel de dados é o que precisa de mais segurança, então é melhor ter a vida na Fase II para ser mais curta que na Fase I.




Etapa 5. Na lista suspensa *Seleção de protocolo* na área Opções da Fase II, escolha um tipo de protocolo para aplicar à segunda fase da negociação. As opções são:

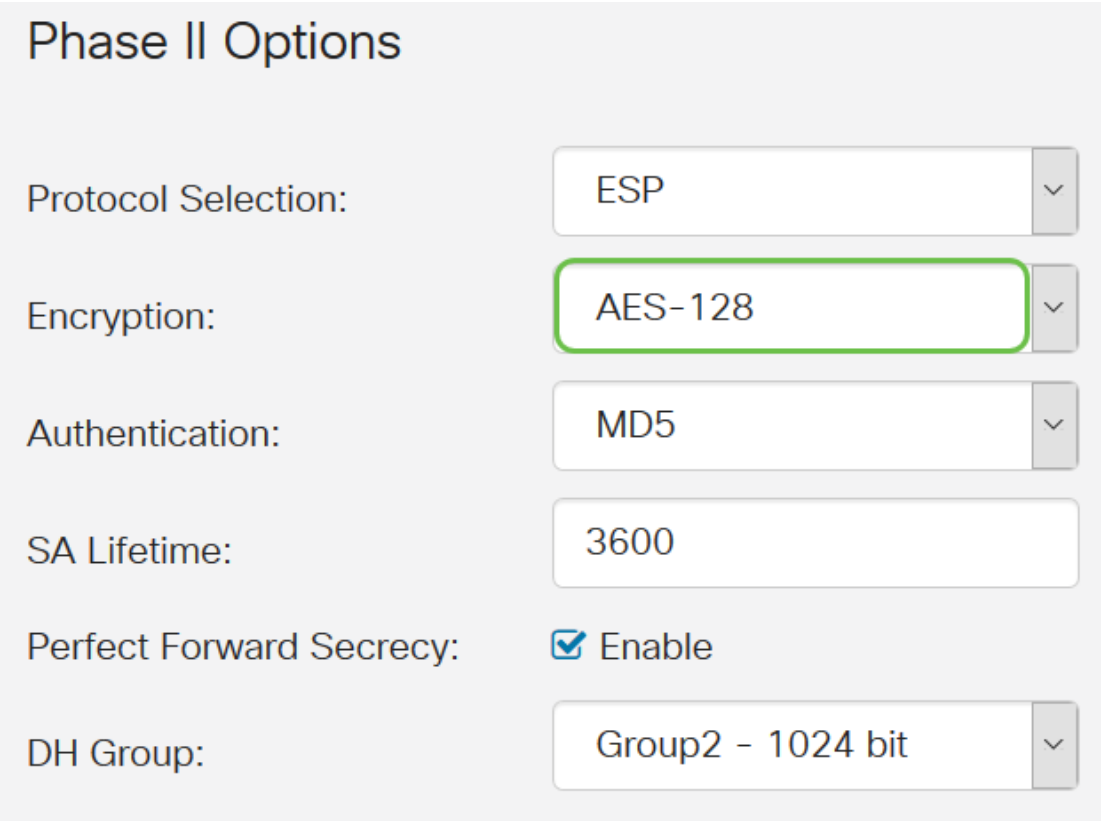
- ESP — Essa opção também é conhecida como Encapsulating Security Payload. Esta opção encapsula os dados a serem protegidos. Se esta opção for escolhida, vá para a Etapa 6 para escolher um método de criptografia.
- AH — Essa opção também é conhecida como Authentication Header (AH). É um protocolo de segurança que fornece autenticação de dados e serviço antirreprodução opcional. AH está incorporado no datagrama IP a ser protegido. Se esta opção for escolhida, vá para a Etapa 7.




Etapa 6. Se o ESP tiver sido escolhido na Etapa 6, escolha uma *Criptografia*. As opções são:

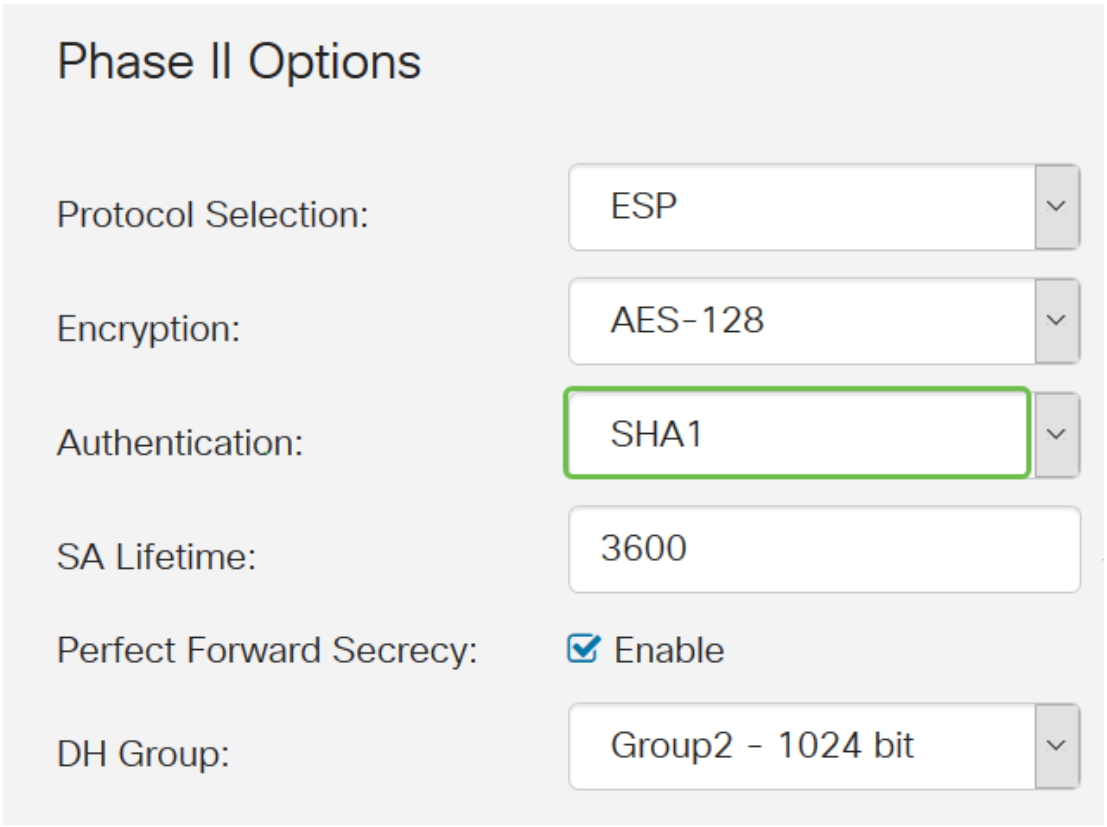
- 3DES — Triple Data Encryption Standard
- AES-128 — O Advanced Encryption Standard usa uma chave de 128 bits.

- AES-192 — O Advanced Encryption Standard usa uma chave de 192 bits.
- AES-256 — O Advanced Encryption Standard usa uma chave de 256 bits.

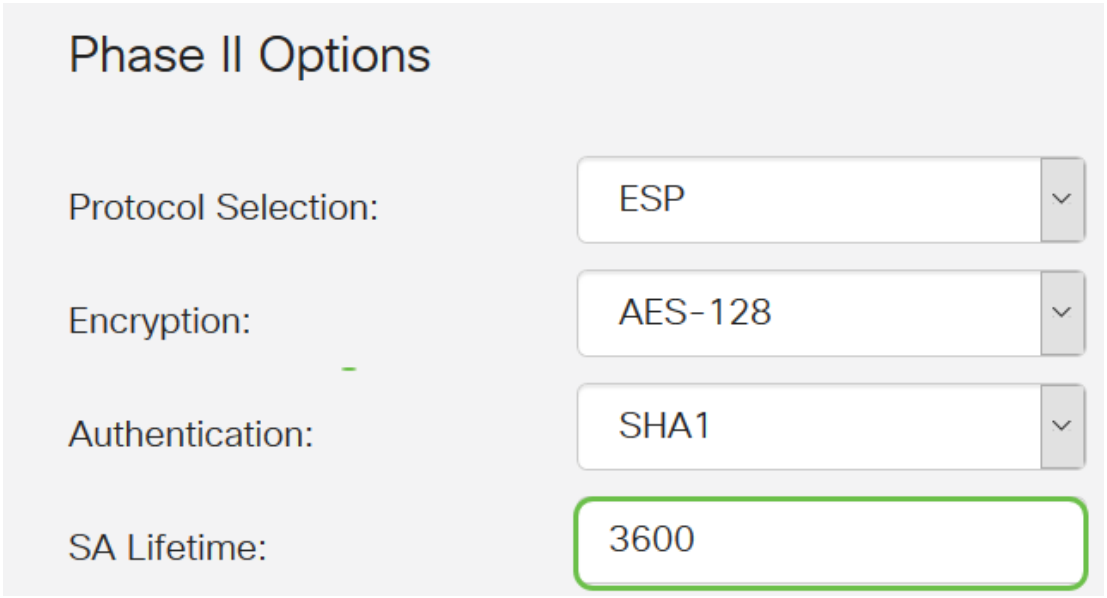



Passo 7. Na lista suspensa *Autenticação*, escolha um método de autenticação que determinará como o ESP e o ISAKMP são autenticados. As opções são:

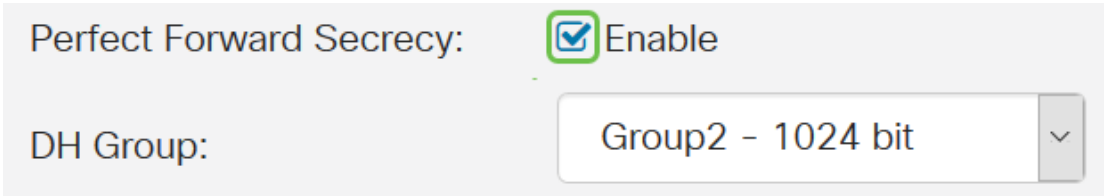
- MD5 — O algoritmo Message-Digest tem um valor de hash de 128 bits.
- SHA-1 — O algoritmo de hash seguro tem um valor de hash de 160 bits.
- SHA2-256 — Algoritmo Hash Seguro com um valor hash de 256 bits.




Etapa 8. No campo *Vida útil do SA*, insira um valor entre 120 e 28800. Este é o período de tempo durante o qual o SA do IKE permanecerá ativo nesta fase. O valor padrão é 3600.

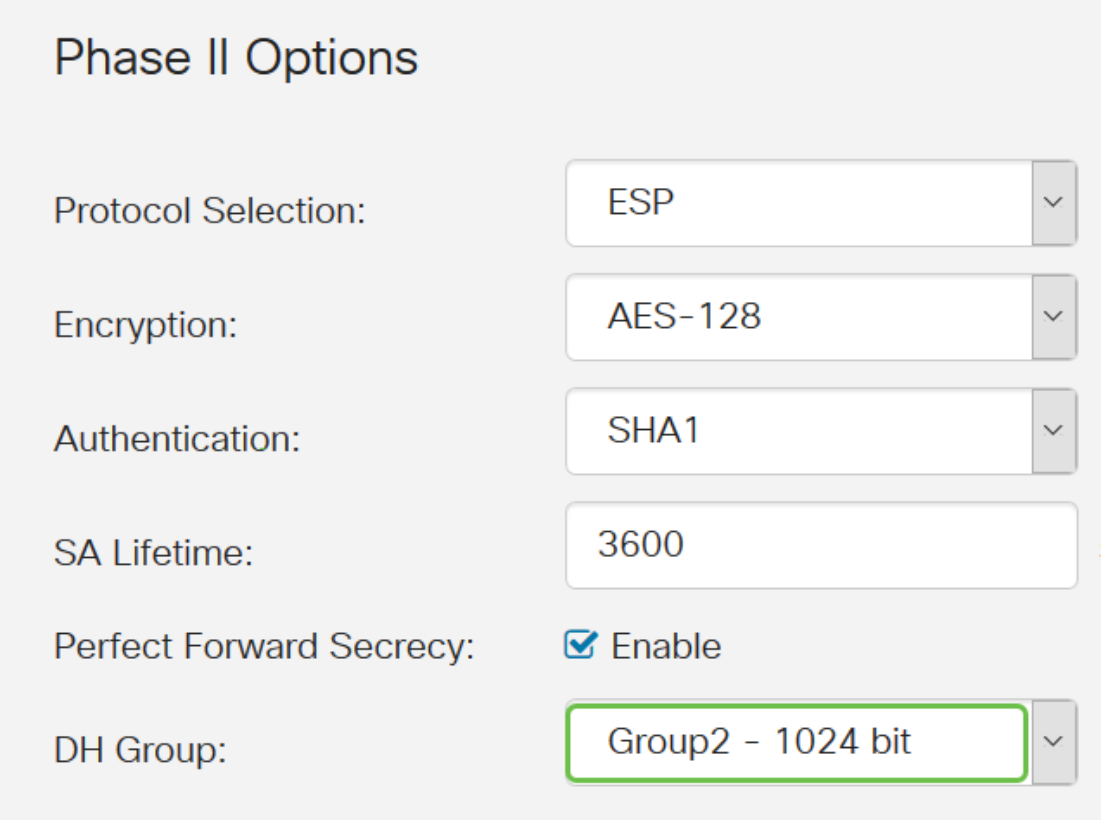



Etapa 9. (Opcional) Marque a caixa de seleção **Habilitar** segredo de encaminhamento perfeito para gerar uma nova chave para a criptografia e autenticação de tráfego IPsec. O Perfect Forward Secsecret é usado para melhorar a segurança das comunicações transmitidas pela Internet usando criptografia de chave pública. Marque a caixa para habilitar esse recurso ou desmarque a caixa para desabilitar esse recurso. Este recurso é recomendado.

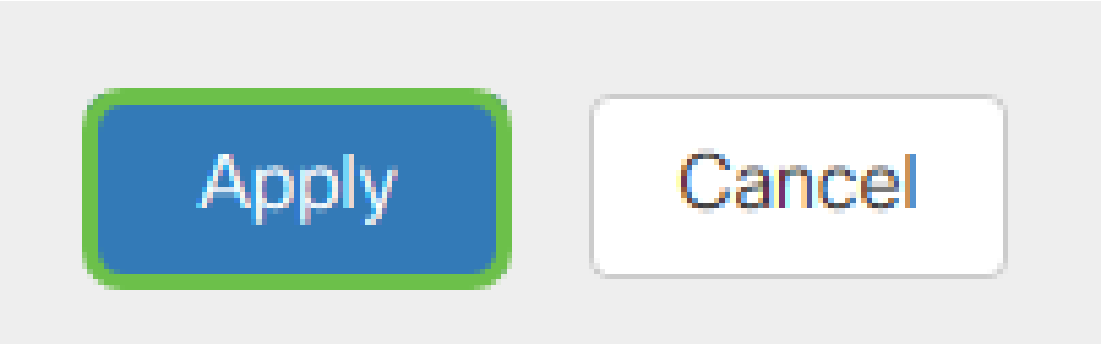



Etapa 10. Na lista suspensa *Grupo DH*, escolha um grupo DH a ser usado com a chave na Fase 2. As opções são:

- Grupo2-1024 bits — Essa opção computa a chave mais rapidamente, mas é menos segura.
- Grupo5-1536 bits — Essa opção computa a chave mais lentamente, mas é a mais segura.

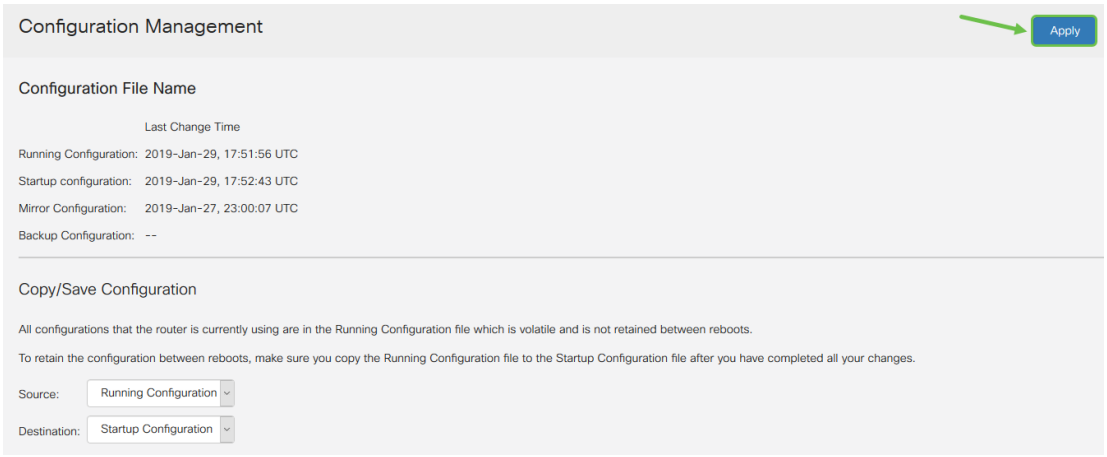



Etapa 11. Clique em Apply.

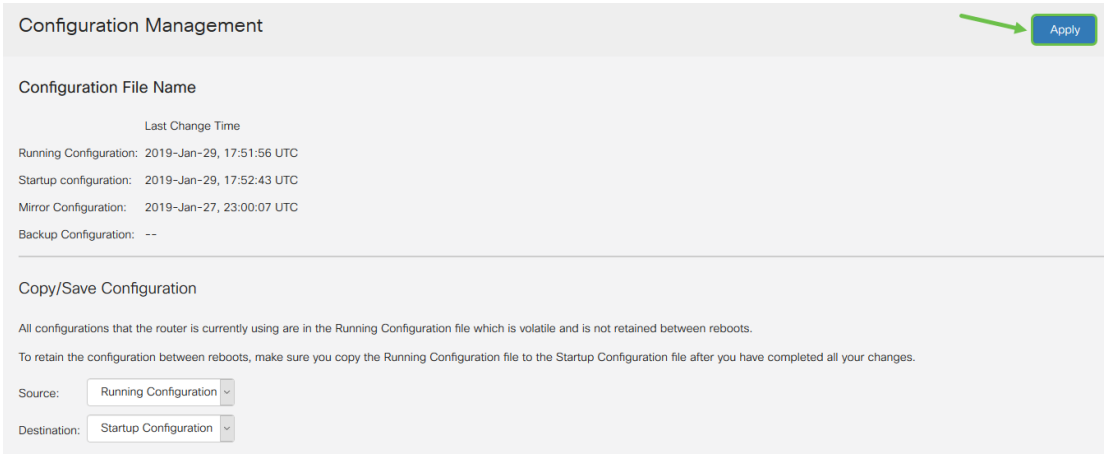



Etapa 12. Clique em **Salvar** para salvar a configuração permanentemente.


Etapa 13. Clique em **Apply** novamente para salvar a configuração atual na configuração de inicialização.



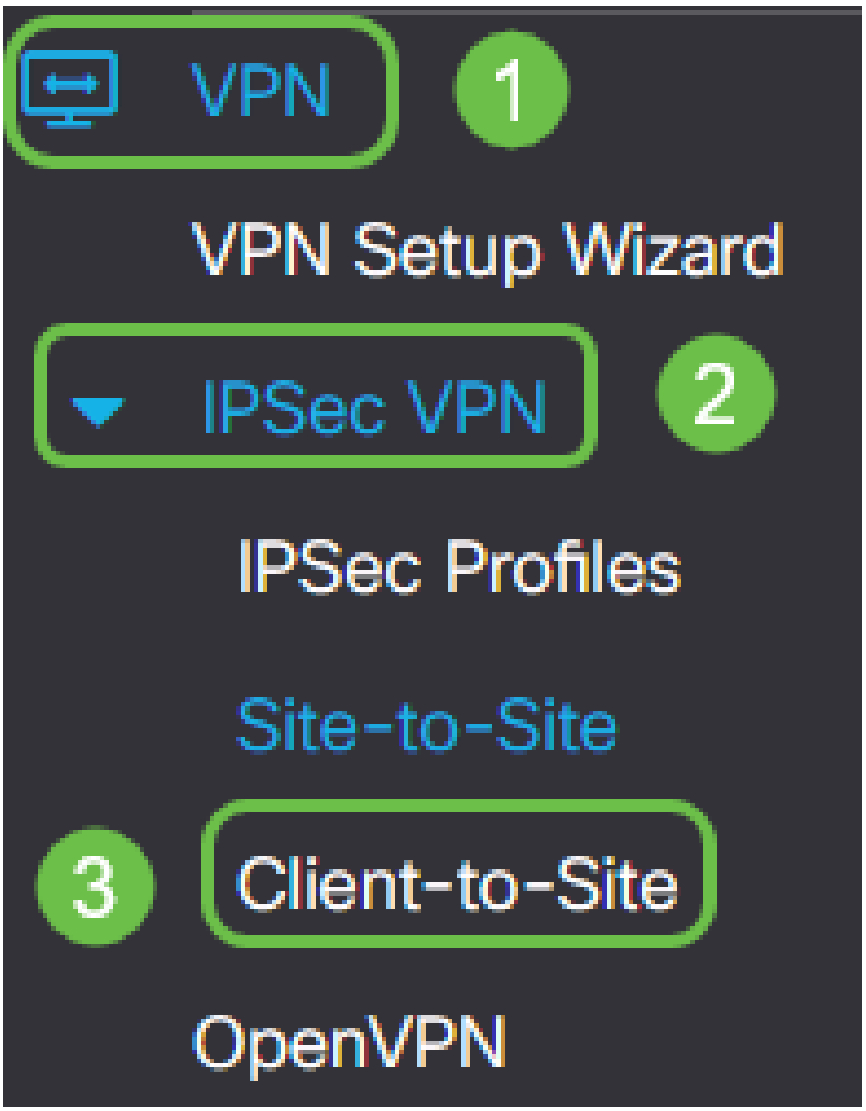

Etapa 14. Quando você receber a confirmação, clique em **OK**.



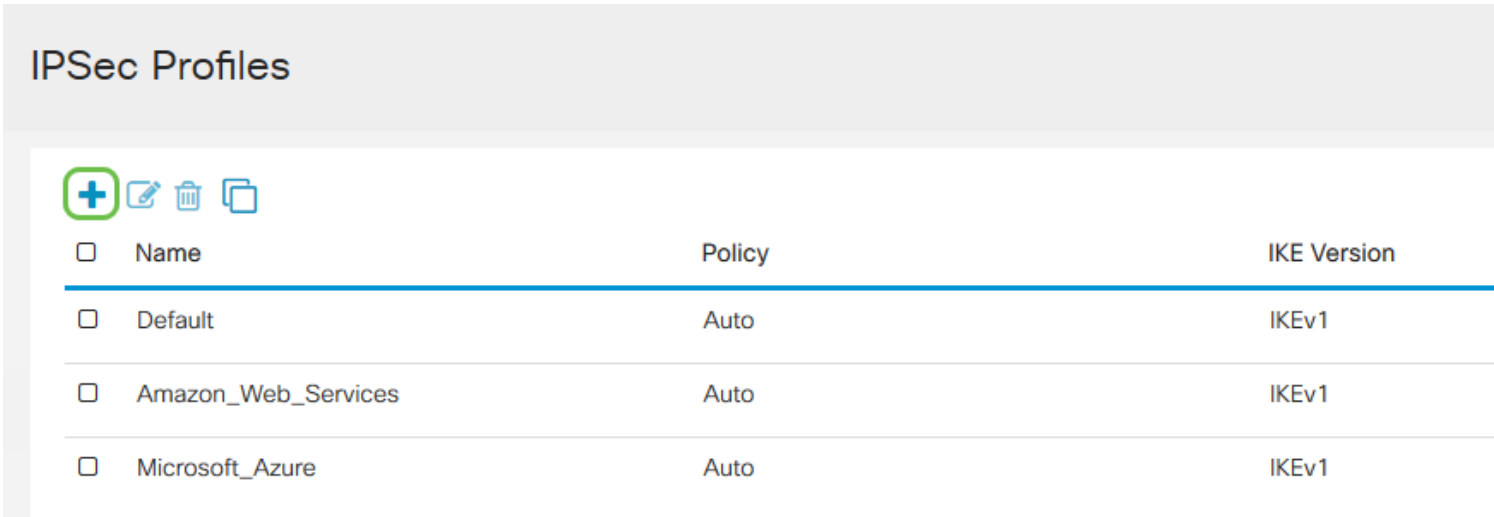

Agora você deve ter configurado com êxito um perfil IPsec no roteador RV160 ou RV260.

## Criar um perfil cliente-local

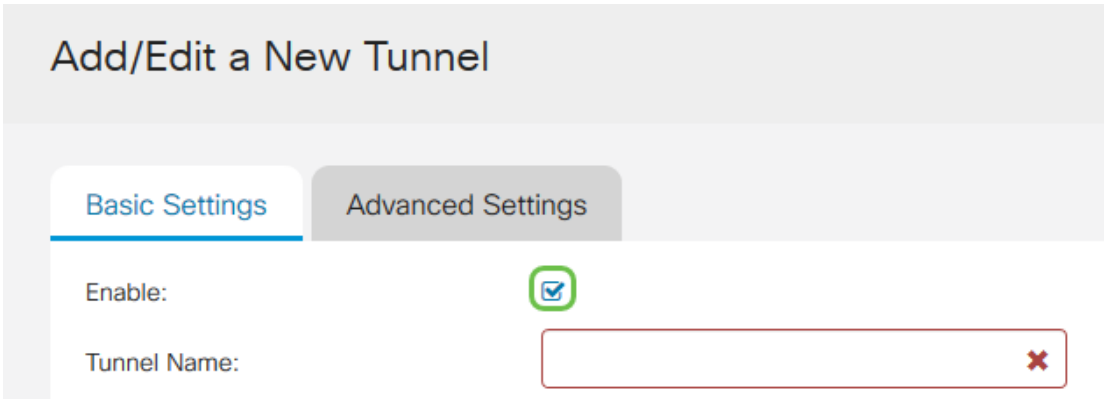
Etapa 1. Escolha **VPN > IPSec VPN > Cliente a Site** .



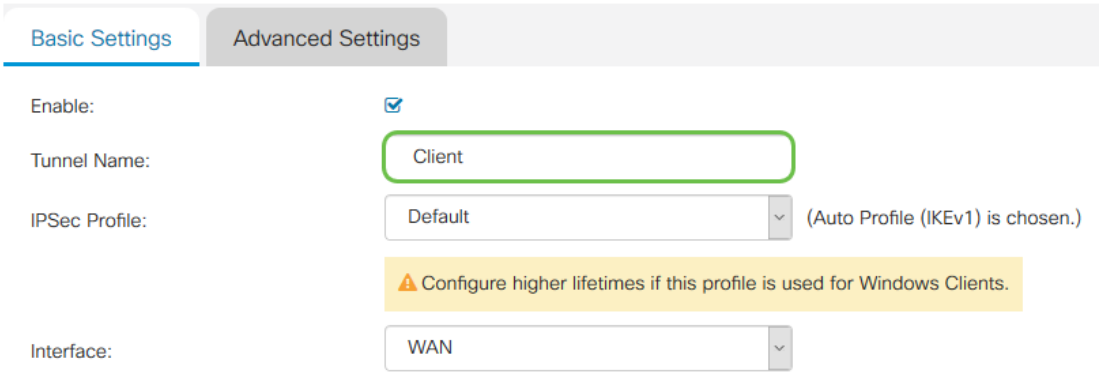

Etapa 2. Clique no ícone **de mais**.



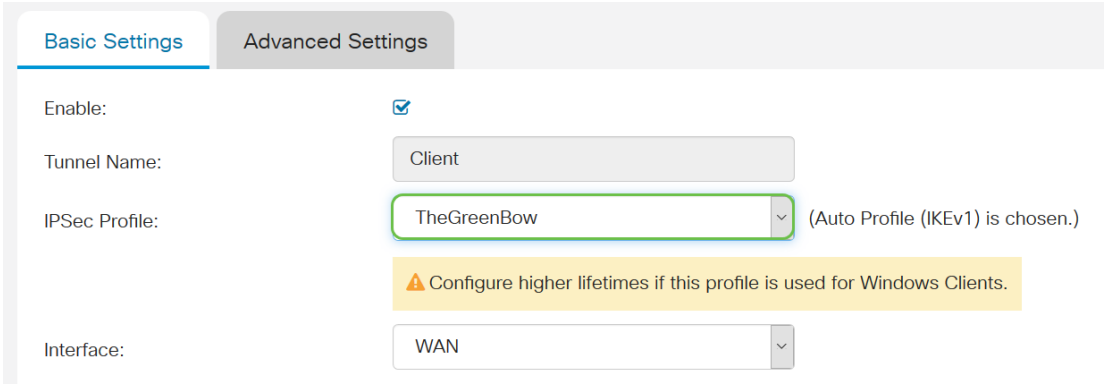

Etapa 3. Na guia Basic Settings (Configurações básicas), marque a caixa de seleção **Enable** para garantir que o perfil VPN esteja ativo.



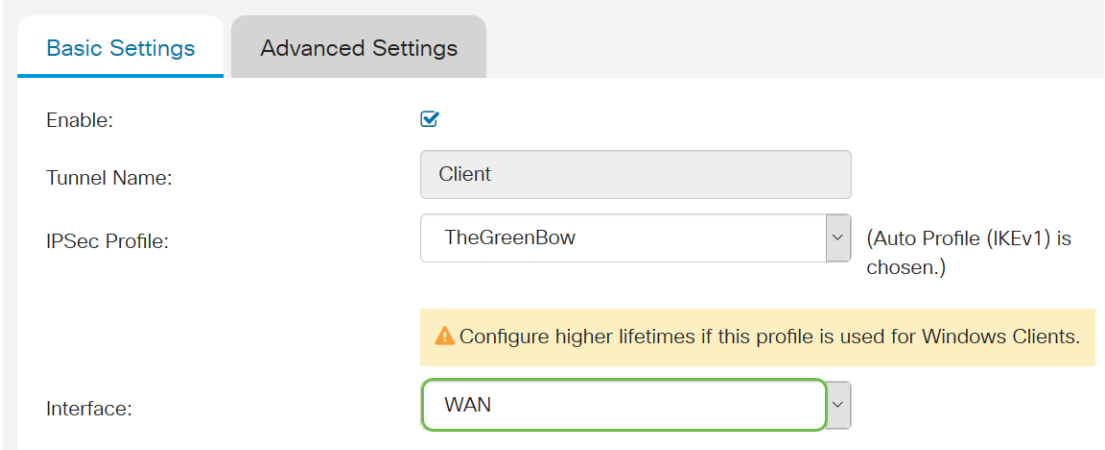

Etapa 4. Digite um nome para a conexão VPN no campo *Nome do túnel*.




Etapa 5. Escolha o perfil IPsec a ser usado na lista suspensa *IPsec*.




Etapa 6. Escolha a Interface na lista suspensa *Interface*.



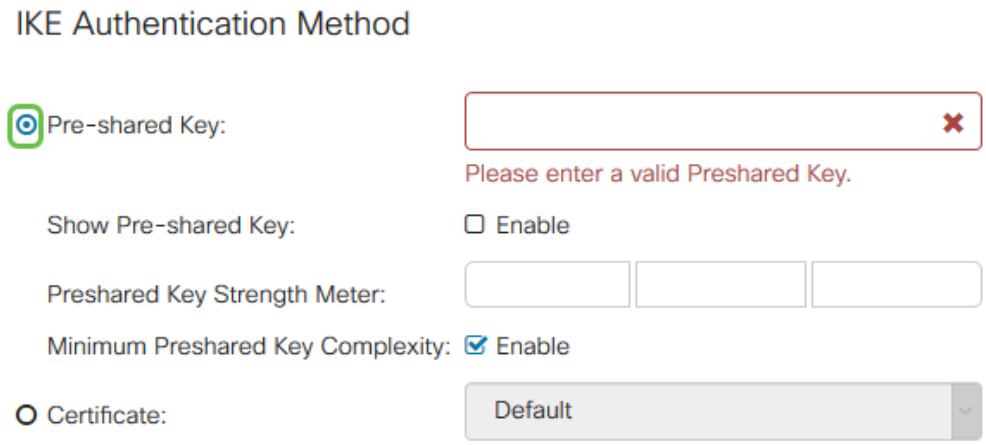

**Note:** As opções dependem do modelo do roteador que você está usando. Neste exemplo, a WAN é escolhida.

Passo 7. Escolha um método de autenticação IKE. As opções são:

- Pre-shared Key — Essa opção nos permitirá usar uma senha compartilhada para a

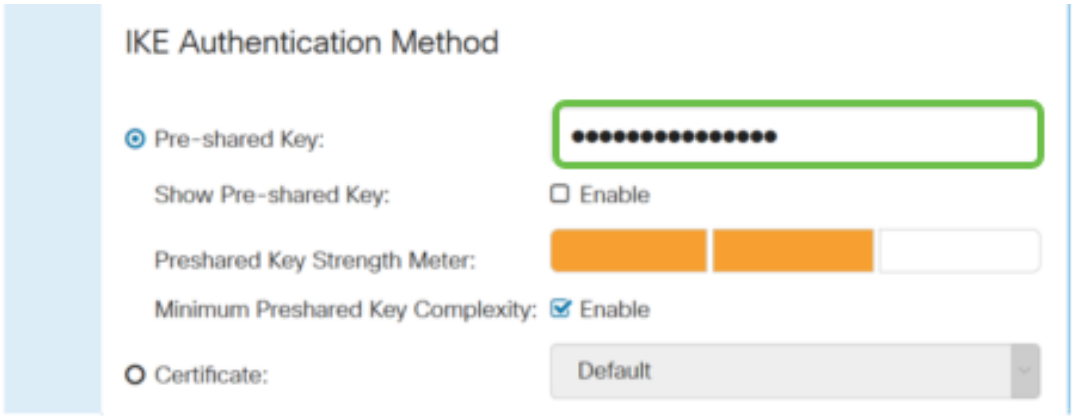
conexão VPN.

- Certificado — Esta opção usa um certificado digital que contém informações como nome, endereço IP, número de série, data de expiração do certificado e uma cópia da chave pública do portador do certificado.

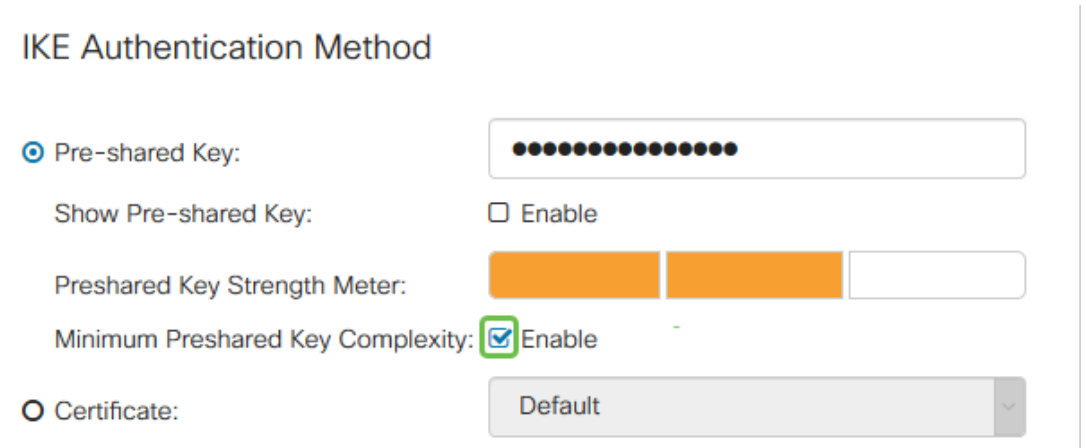



**Note:** Uma chave pré-compartilhada pode ser o que você quiser que ela seja, apenas precisa corresponder no site e com o cliente quando eles configuram o cliente TheGreenBow em seu computador.

Etapa 8. Digite a senha da conexão no campo *Pre-shared Key*.

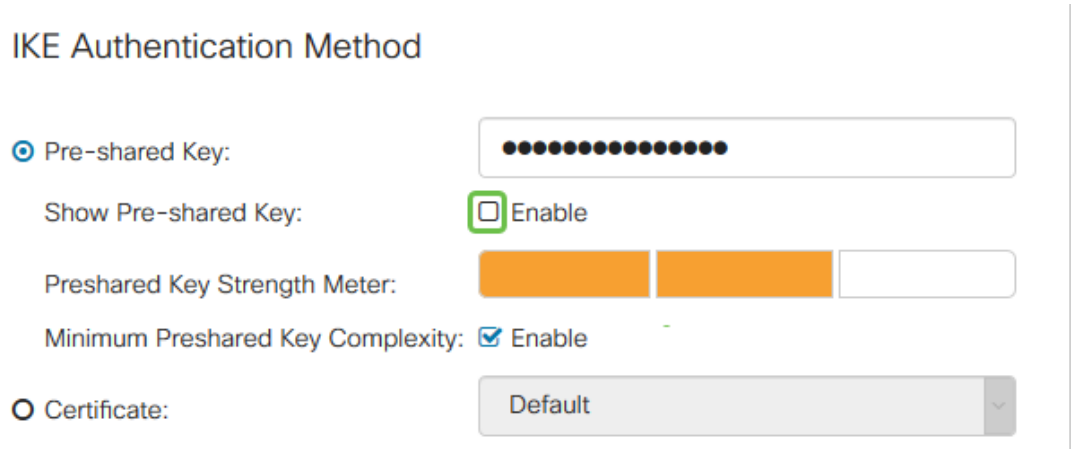



Etapa 9. (Opcional) Desmarque a caixa de seleção *Minimum Pre-shared Key Complexity* **Enable** para poder usar uma senha simples.




**Note:** Neste exemplo, a Complexidade Mínima de Chave Pré-compartilhada é deixada habilitada.

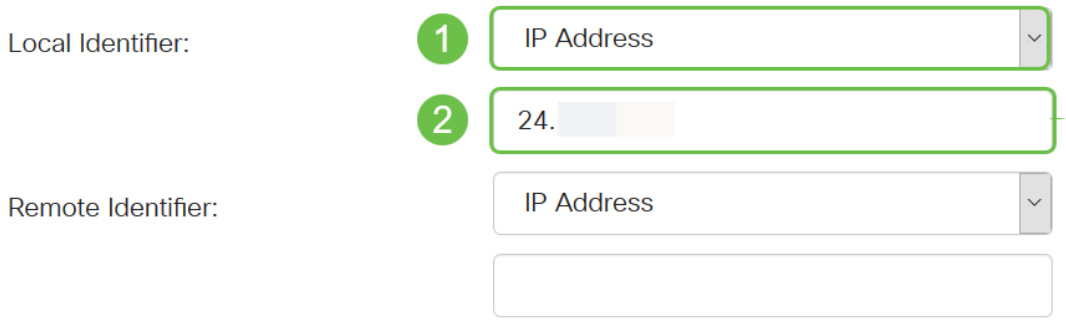
Etapa 10. (Opcional) Marque a caixa de seleção *Show Pre-shared Key* **Enable** para mostrar a senha em texto simples.




**Note:** Neste exemplo, a opção Mostrar chave pré-compartilhada é deixada desabilitada.

Etapa 11. Escolha um identificador local na lista suspensa *Identificador local*. As opções são:

- Local WAN IP — Essa opção usa o endereço IP da interface de rede de longa distância (WAN) do gateway VPN.
- Endereço IP — Essa opção permite inserir manualmente um endereço IP para a conexão VPN. Esse é o endereço IP da WAN do roteador no local (escritório).
- FQDN — Essa opção também é conhecida como Nome de domínio totalmente qualificado (FQDN). Ele permite que você use um nome de domínio completo para um computador específico na Internet.
- FQDN do usuário — Essa opção permite que você use um nome de domínio completo para um usuário específico na Internet.



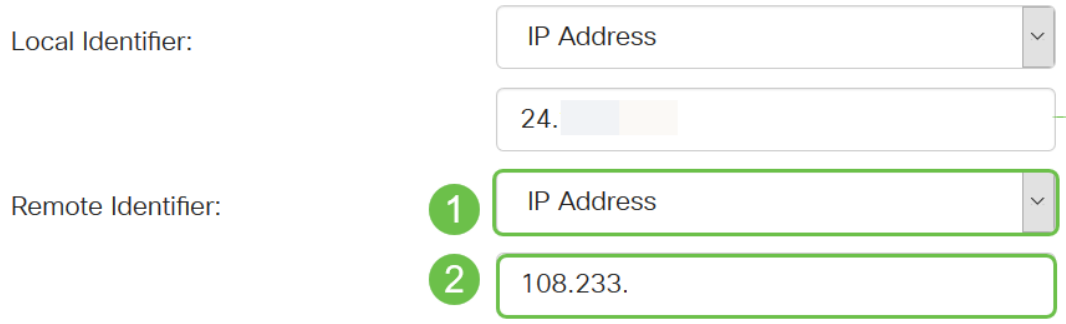

**Note:** Neste exemplo, o endereço IP é escolhido e o endereço IP da WAN do roteador no local é inserido. Neste exemplo, 24.x.x.x foi inserido. O endereço completo foi desfocado para fins de privacidade.

Etapa 12. Escolha um identificador para o host remoto. As opções são:

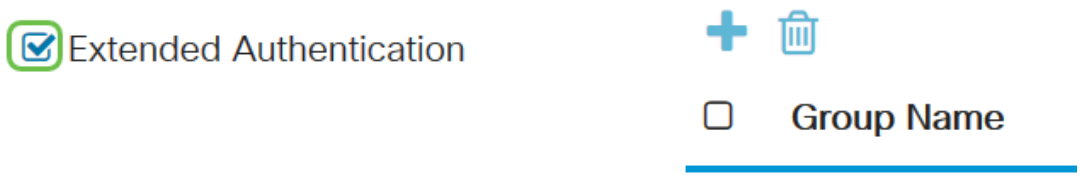
- Endereço IP — Essa opção usa o endereço IP WAN do cliente VPN. Para descobrir o endereço IP da WAN, você pode digitar "qual é meu IP" no seu navegador da Web. Este é o endereço IP do cliente.
- FQDN — Nome de domínio totalmente qualificado. Esta opção permite que você use um nome de domínio completo para um computador específico na Internet.
- FQDN do usuário — Essa opção permite que você use um nome de domínio completo para um usuário específico na Internet.

**Note:** Neste exemplo, o endereço IP é escolhido e o endereço IPv4 atual do roteador no local do cliente é inserido. Isso pode ser determinado fazendo uma pesquisa de "Qual é meu endereço IP" no seu navegador da Web. Esse endereço pode ser alterado para que, se você tiver problemas para se conectar após uma configuração bem-sucedida, essa possa ser uma área a ser verificada

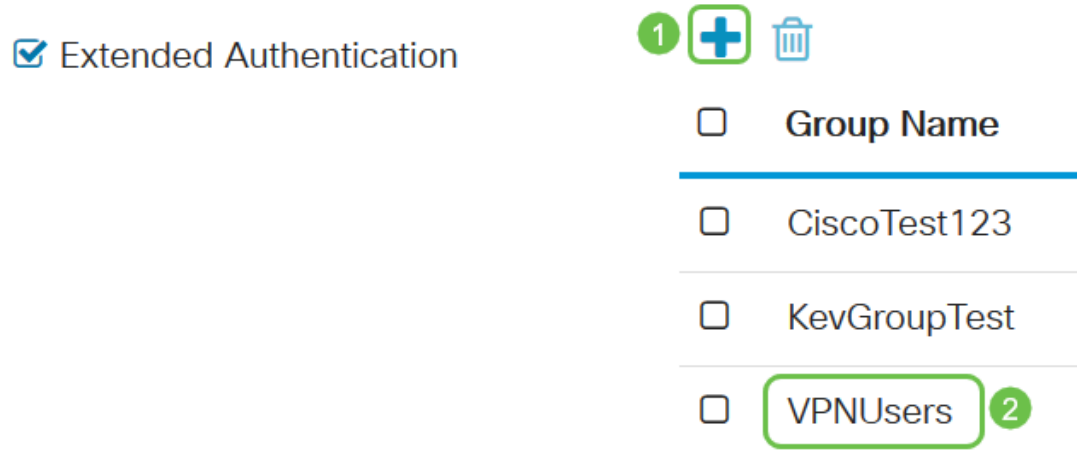
e alterada no cliente e no site.




Etapa 13. (Opcional) Marque a caixa de seleção **Autenticação Estendida** para ativar o recurso. Quando ativada, isso fornecerá um nível adicional de autenticação que exigirá que os usuários remotos digitem suas credenciais antes de receberem acesso à VPN.



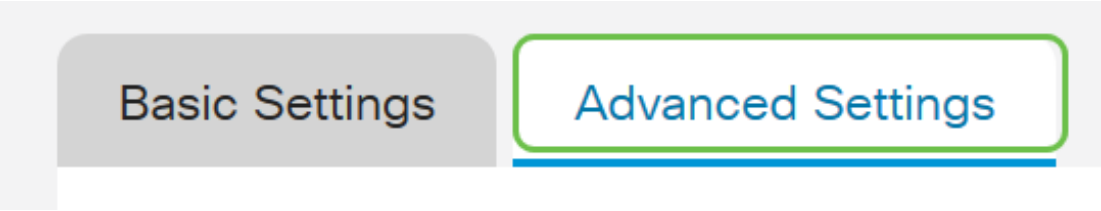

Etapa 14. (Opcional) Escolha o grupo que usará autenticação estendida clicando no ícone **mais** e selecione o usuário na lista suspensa.



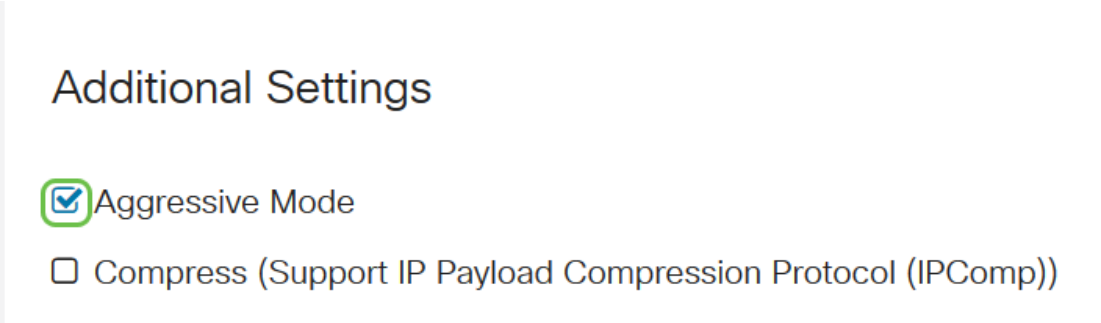

**Note:** Neste exemplo, **VPNUsers** é escolhido.

Etapa 15. Em *Pool Range for Client LAN*, insira o primeiro IP e o endereço IP final que podem ser atribuídos a um cliente VPN. Isso precisa ser um pool de endereços que não se sobreponha aos endereços do site. Elas podem ser chamadas de interfaces virtuais. Se você receber uma mensagem de que uma interface virtual precisa ser alterada, é aqui que você corrigirá isso.


Etapa 16. Selecione a guia **Advanced Settings (Configurações avançadas)**.

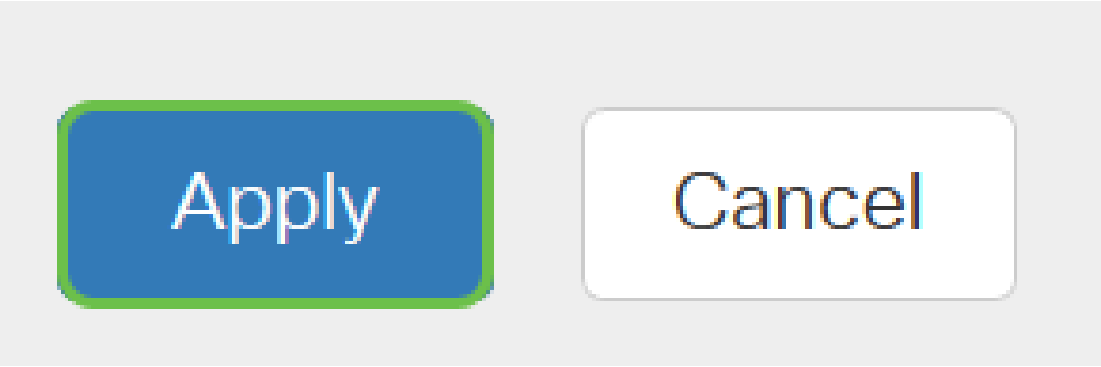



Etapa 17. (Opcional) Role para baixo até a parte inferior da página e selecione **Modo agressivo**. O recurso Modo agressivo permite especificar atributos de túnel RADIUS para um peer de segurança IP (IPsec) e iniciar uma negociação de modo agressivo de Internet Key Exchange (IKE) com o túnel. Para obter mais informações sobre o Modo agressivo vs. Modo principal, clique aqui.

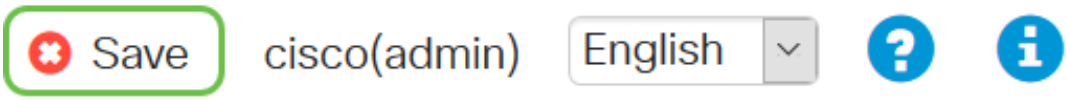



**Note:** A caixa de seleção Compress permite que o roteador proponha a compactação quando inicia uma conexão. Esse protocolo reduz o tamanho dos datagramas IP. Se o respondente rejeitar esta proposta, o roteador não implementará a compactação. Quando o roteador é o respondente, ele aceita a compactação, mesmo que a compactação não esteja habilitada. Se você habilitar esse recurso para esse roteador, precisaria habilitá-lo no roteador remoto (a outra extremidade do túnel). Neste exemplo, a *Compress* ficou desmarcada.

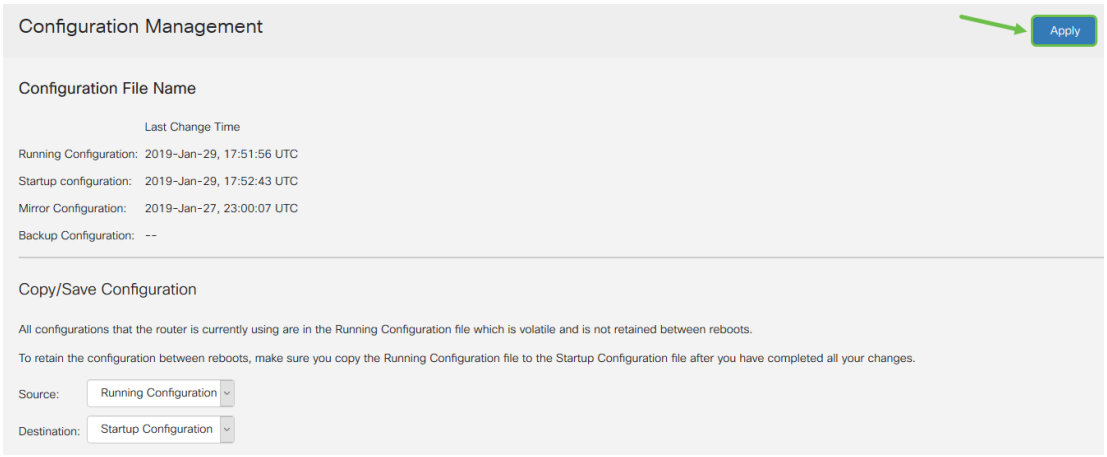
Etapa 18. Clique em Apply.



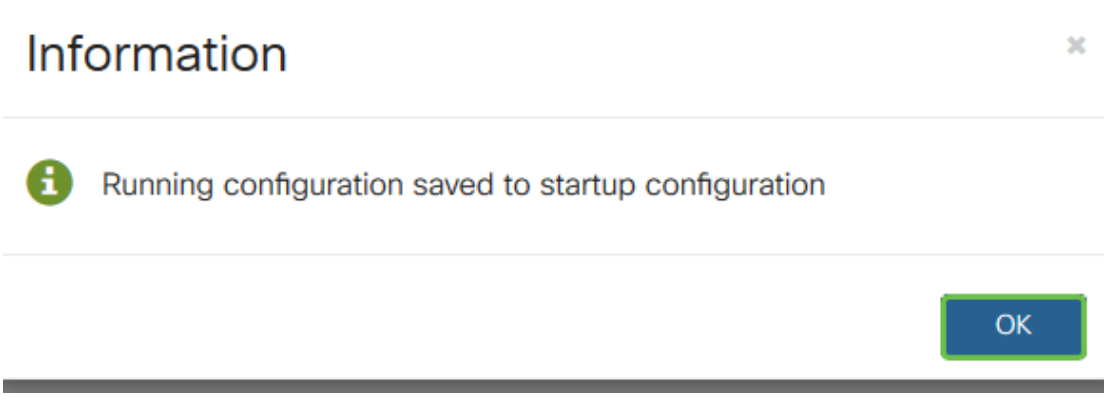

Etapa 19. Click **Save**.




Etapa 20. Clique em **Apply** novamente para salvar a configuração atual na configuração de inicialização.




Etapa 21. Quando você receber a confirmação, clique em **OK**.




Agora você deve ter configurado o túnel cliente-local no roteador para o cliente VPN do GreenBow.

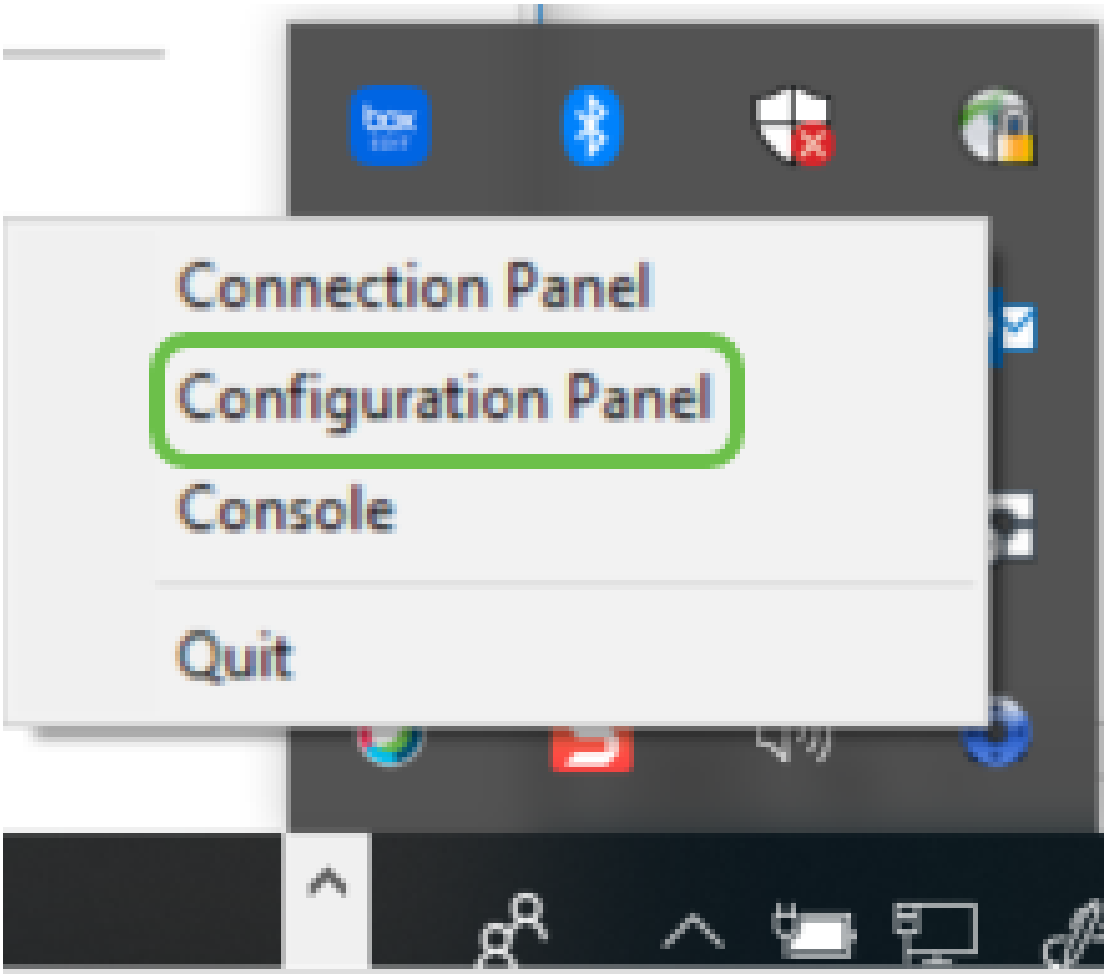
# Configurar o cliente VPN GreenBow no computador do trabalhador remoto

## Definir configurações da Fase 1

Para baixar a versão mais recente do software do cliente VPN IPsec do TheGreenBow, clique aqui.

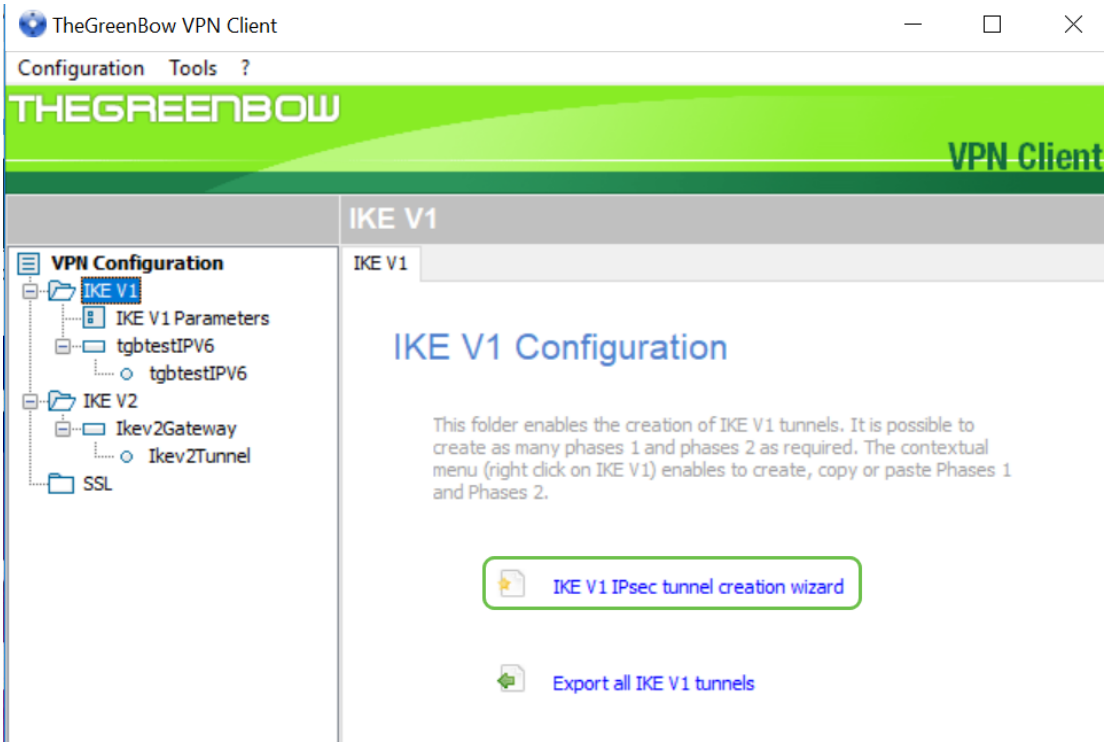
Etapa 1. Clique com o botão direito do mouse no ícone GreenBow VPN Client. Ele está localizado no canto inferior direito da barra de tarefas.

Etapa 2. Selecione **Painel de configuração**.



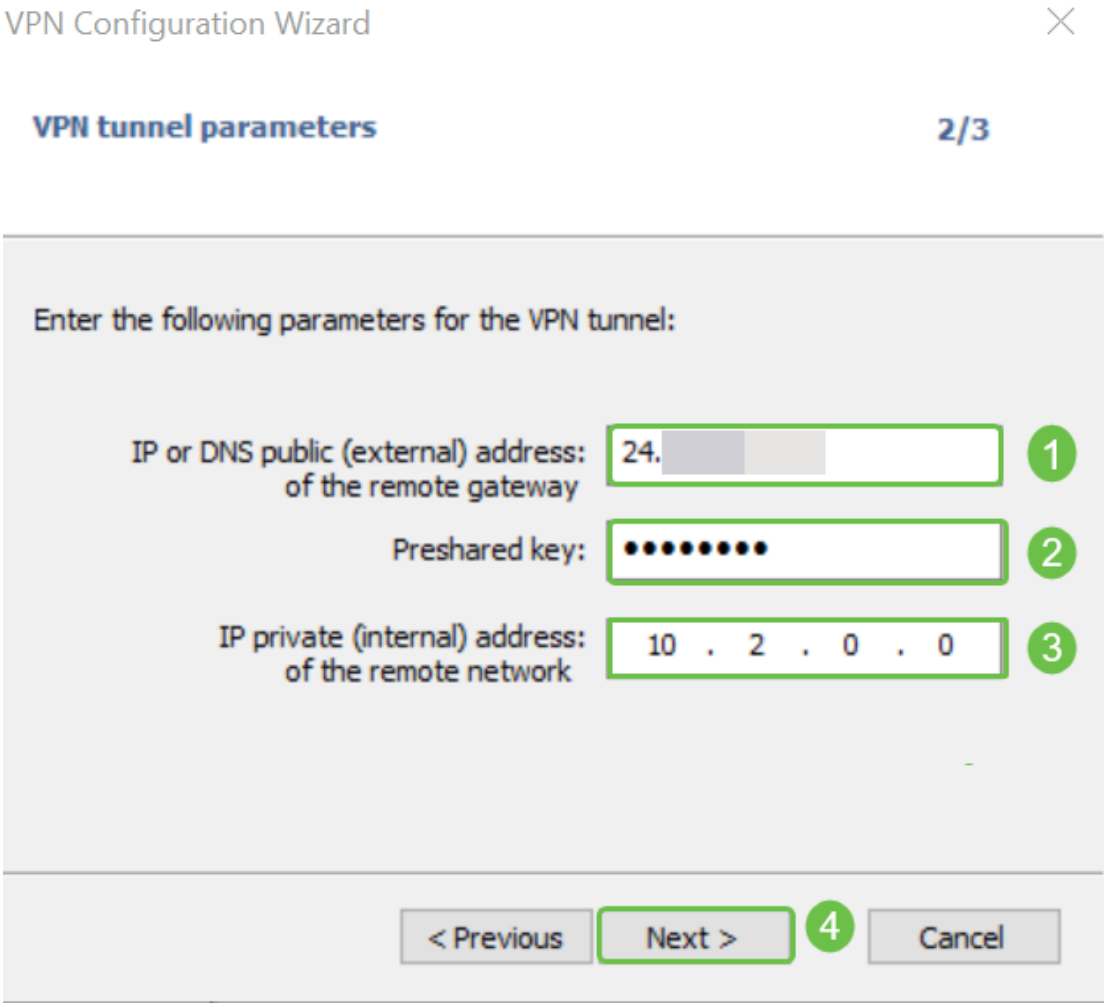

**Note:** Este é um exemplo em um computador Windows. Isso pode variar dependendo do software usado.

Etapa 3. Selecione o **assistente de criação de túnel IPsec IKE V1**.

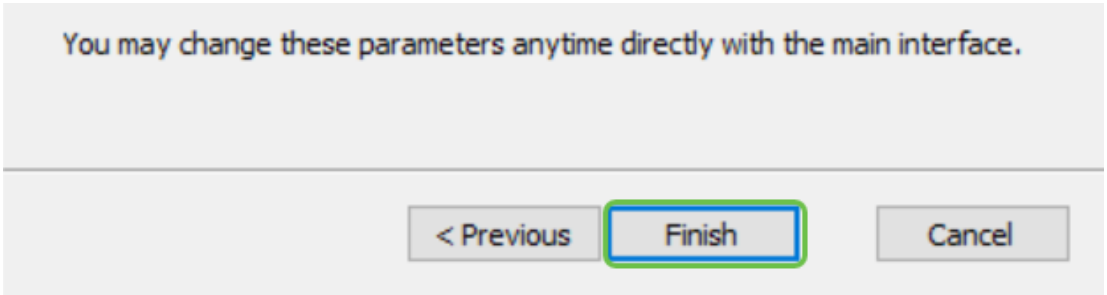



**Note:** Neste exemplo, o IKE Versão 1 está sendo configurado. Se quiser configurar o IKE Versão 2, siga as mesmas etapas, mas clique com o botão direito do mouse na pasta IKE V2. Você também precisaria selecionar IKEv2 para o perfil IPsec no roteador no site.

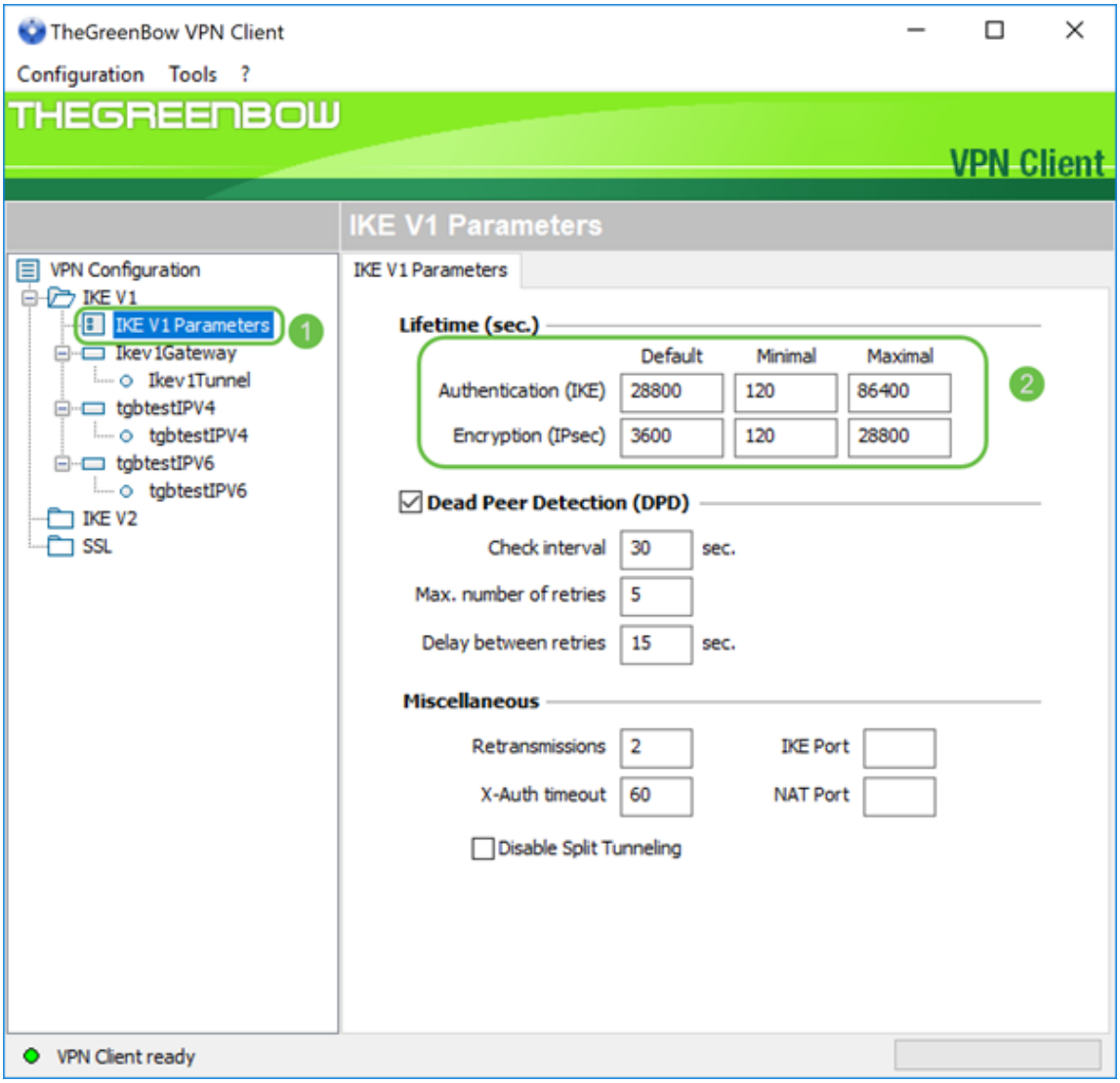
Etapa 4. Preencha o endereço IP da WAN pública do roteador no local (escritório) onde o servidor de arquivos está localizado, a chave pré-compartilhada e o endereço interno privado da rede remota no local. Clique em Next. Neste exemplo, o site é 24.x.x.x. Os últimos três octetos (conjuntos de números neste endereço IP) foram substituídos por um x para proteger essa rede. Você deve digitar o endereço IP completo.



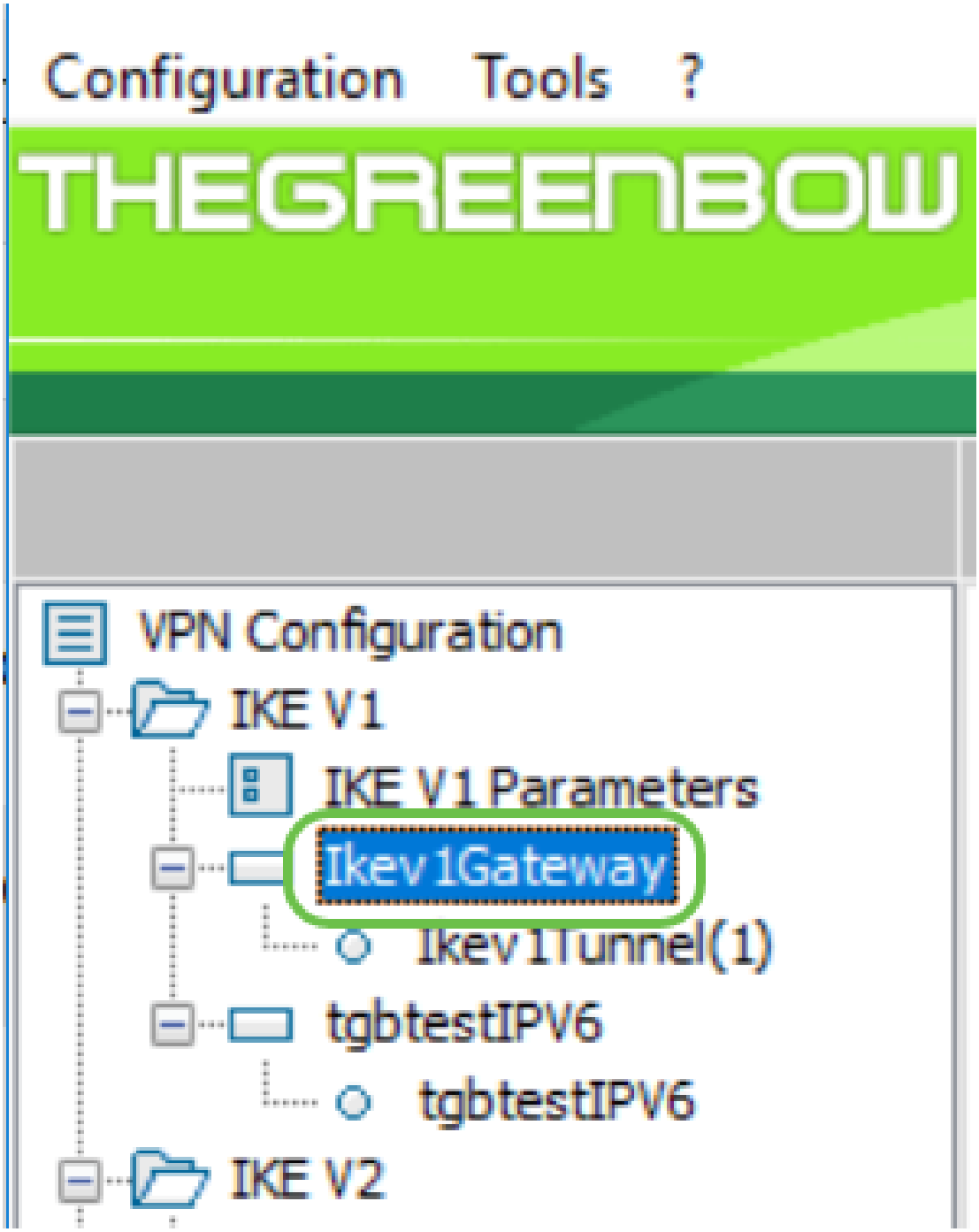

Etapa 5. Clique em Finish.



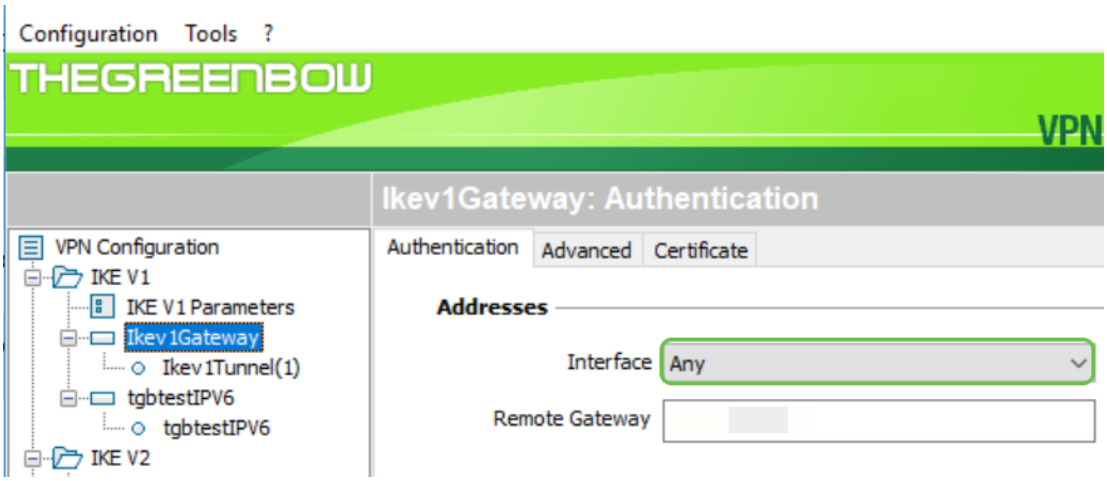

Etapa 6 (Opcional) Você pode alterar os parâmetros IKE V1. O tempo de vida padrão, mínimo e máximo do GreenBow pode ser ajustado. Nesse local, você pode inserir qualquer intervalo do tempo de vida que o roteador aceitar.



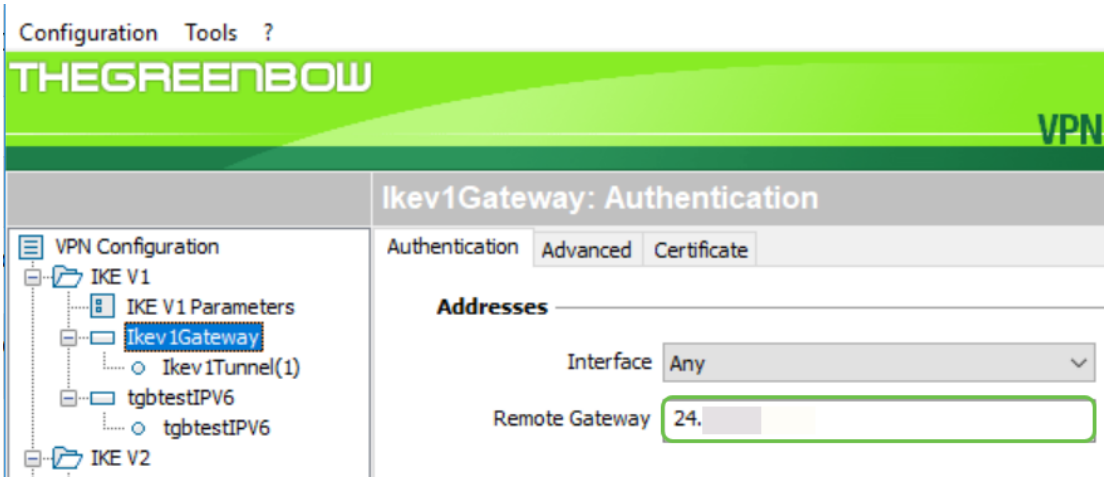

Passo 7. Clique no gateway que você criou.




Etapa 8. Na guia *Authentication* em *Addresses* você verá uma lista suspensa de endereços locais. Você pode escolher um ou selecionar **Qualquer**, conforme mostrado abaixo.

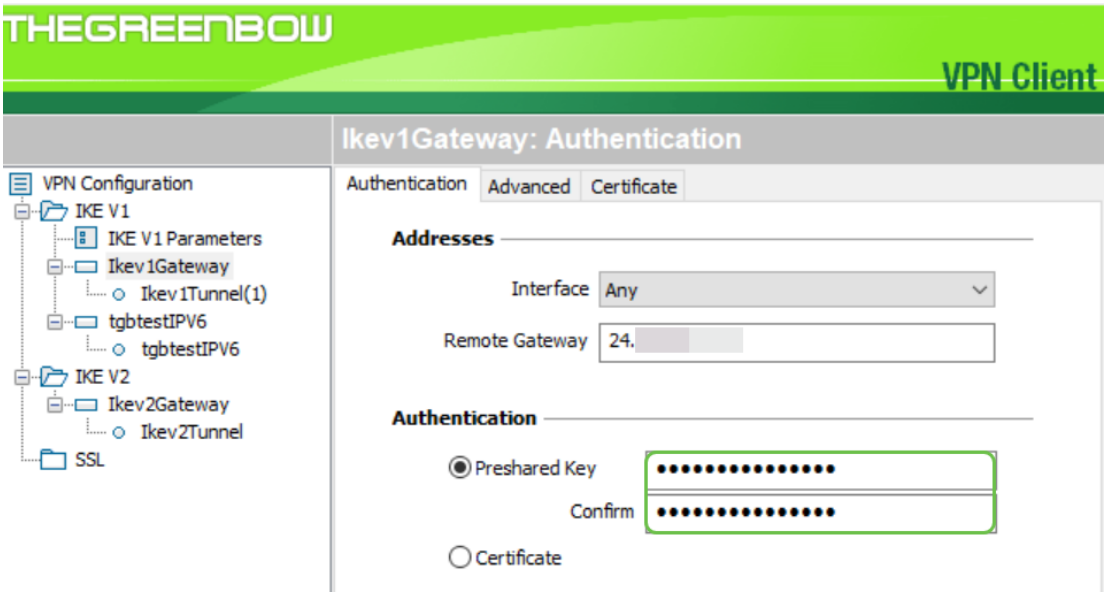



Etapa 9. Digite o endereço do gateway remoto no campo *Gateway remoto*. Pode ser um endereço IP ou um nome DNS. Esse é o endereço do endereço IP público do roteador no local (escritório).



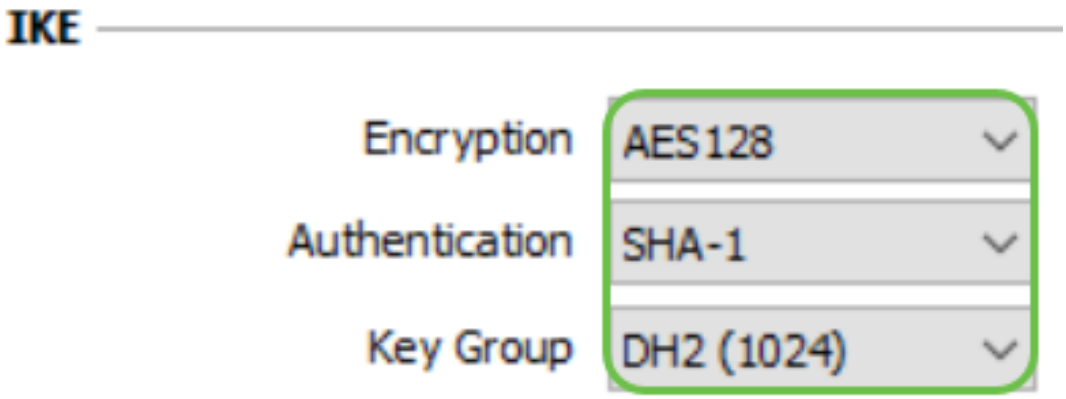

Etapa 10. Em *Authentication*, escolha o tipo de autenticação. As opções são:

- Presshared Key — (Chave pré-compartilhada) Essa opção permitirá que o usuário use uma senha configurada no gateway VPN. A senha deve ser combinada pelo usuário para poder estabelecer um túnel VPN.
- Certificado — Esta opção utilizará um certificado para concluir o handshake entre o VPN Client e o VPN Gateway.

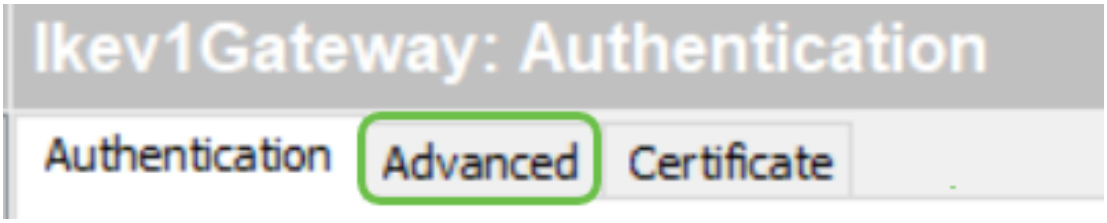



**Note:** Neste exemplo, a chave pré-compartilhada configurada no roteador foi inserida e confirmada.

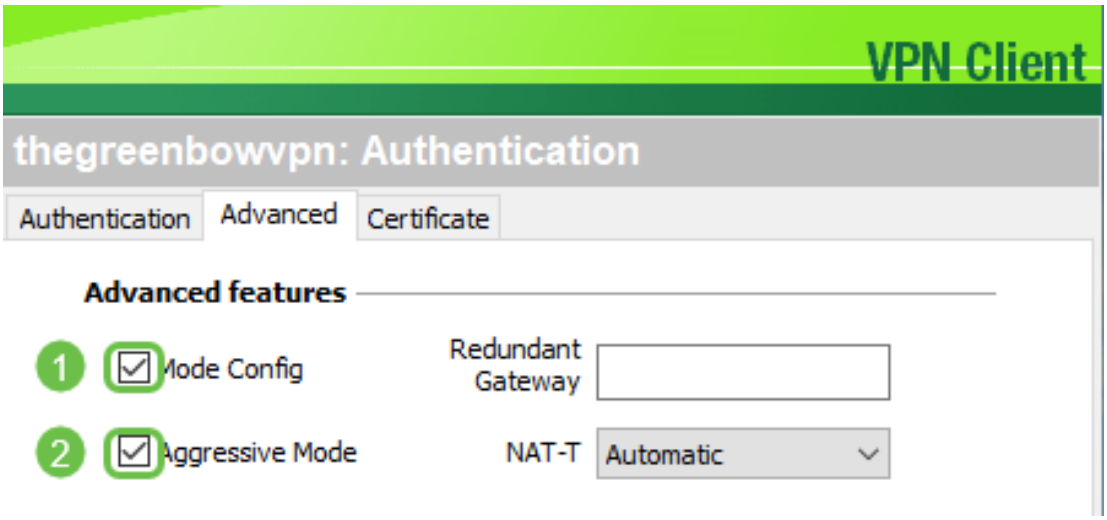
Etapa 11. Em *IKE*, defina as configurações de Criptografia, Autenticação e Grupo de Chave para corresponder à configuração do roteador.




Etapa 12. Clique na guia Advanced.

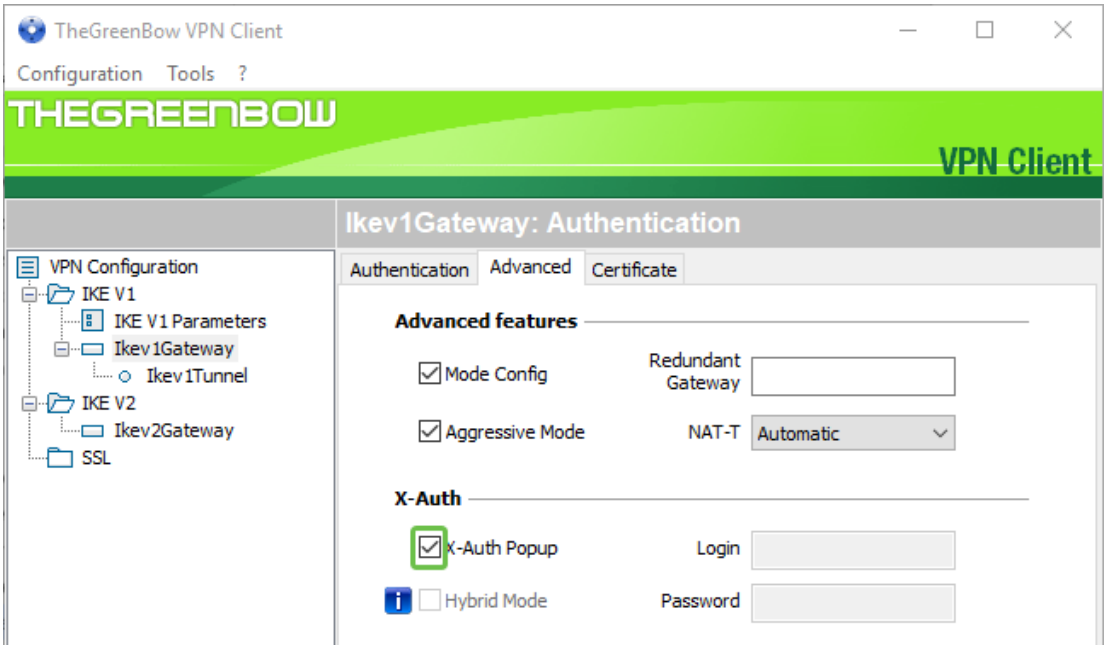



Etapa 13. Em Advanced features (Recursos avançados), marque a caixa de seleção **Mode Config** e **Aggressive Mode**. O Modo Agressivo foi selecionado no RV160 no perfil Cliente-Site deste exemplo. Deixe a configuração NAT-T como Automático.

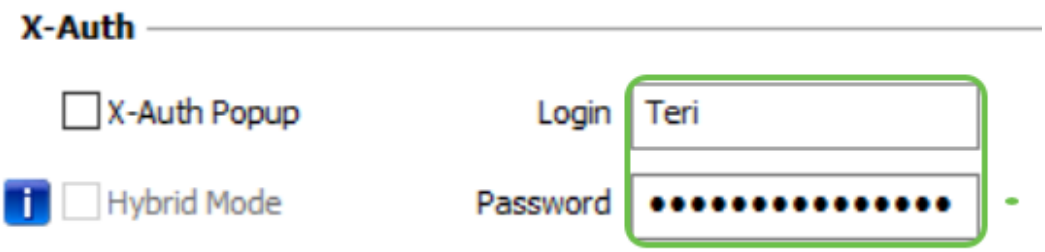



**Note:** Com o modo Config ativado, o GreenBow VPN Client irá extrair as configurações do gateway VPN para tentar estabelecer um túnel. O NAT-T torna o estabelecimento de uma conexão mais rápido.

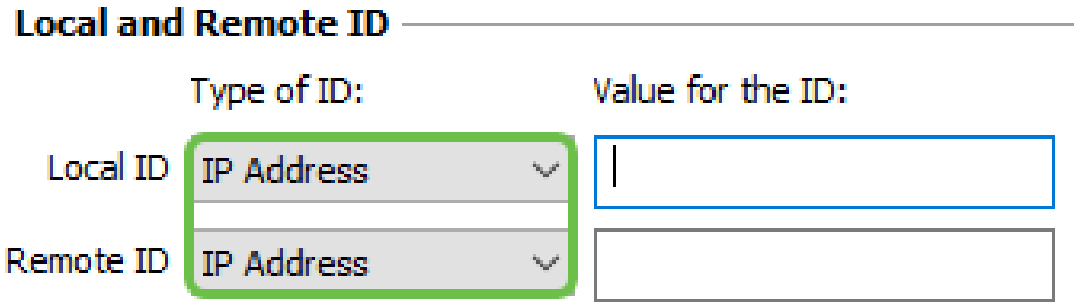
Etapa 14. (Opcional) Em *X-Auth*, você pode marcar a caixa de seleção **X-Auth Popup** para puxar automaticamente a janela de login ao iniciar uma conexão. A janela de login é onde o usuário insere suas credenciais para poder concluir o túnel.




Etapa 15. (Opcional) Se você não selecionar *X-Auth Popup*, insira seu nome de usuário no campo *Login*. Este é o nome de usuário que foi inserido quando uma conta de usuário foi criada no gateway VPN e na senha no site.

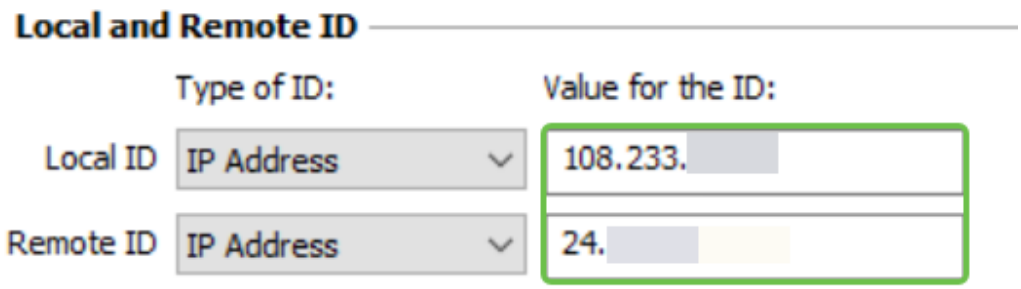



Etapa 16. Em *ID local e remota*, defina o ID local e o ID remoto para corresponder às configurações do gateway VPN.

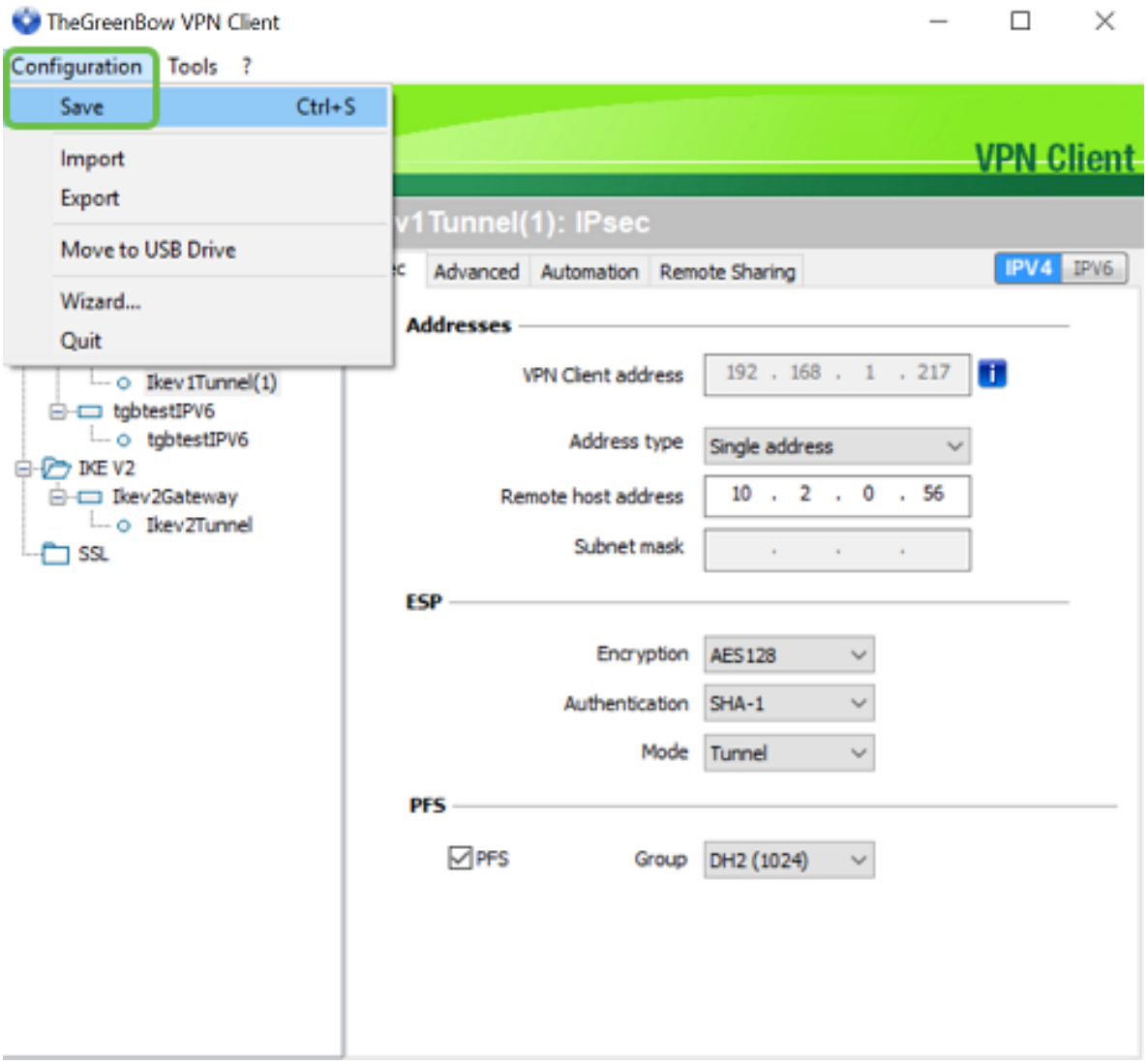



**Note:** Neste exemplo, a ID local e a ID remota estão definidas como Endereço IP para corresponder às configurações do gateway VPN RV160 ou RV260.

Etapa 17. Em *Valor da ID*, insira a ID local e a ID remota nos respectivos campos. O ID local é o endereço IP da WAN do cliente. Isso pode ser encontrado fazendo uma pesquisa na Web para "What is my IP" (O que é meu IP). O ID remoto é o endereço IP da WAN do roteador no local.

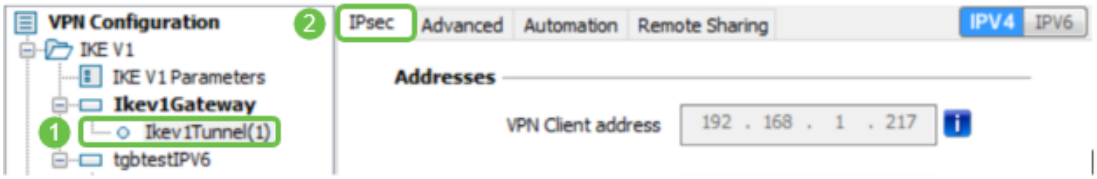



Etapa 18. Clique em **Configuração** e escolha **Salvar**.



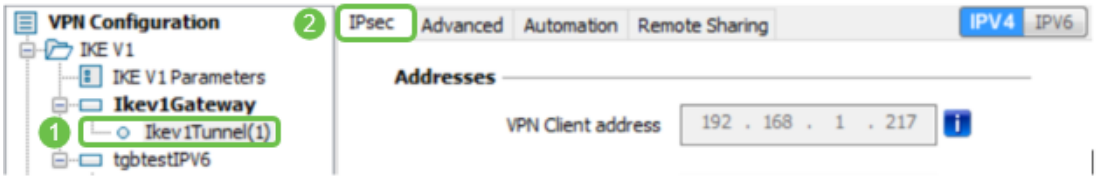

## Definir configurações de túnel

Etapa 1. Clique no **Túnel IKev11** (o seu nome pode ser diferente) e na guia **IPsec**. O endereço do VPN Client é preenchido automaticamente se você selecionou Mode Config nas configurações avançadas do Ikev1Gateway. Exibe o endereço IP local do computador/laptop no local remoto.



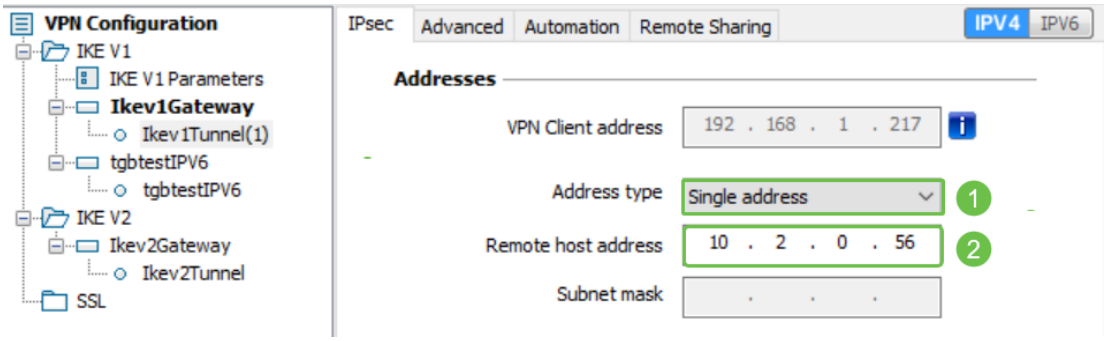

Etapa 2. Escolha o tipo de endereço que o cliente VPN pode acessar na lista suspensa *Tipo de endereço*. Pode ser um único endereço, intervalo de endereços ou um endereço de sub-rede. O

padrão, endereço de sub-rede, inclui automaticamente o endereço do VPN Client (o endereço IP local do computador), o endereço de LAN remota e a máscara de sub-rede. Se o Endereço único ou o Intervalo de endereços estiver selecionado, esses campos precisarão ser preenchidos manualmente. Digite o endereço de rede que deve ser acessado pelo túnel VPN no campo *Endereço LAN Remoto* e a máscara de sub-rede da rede remota no campo *Máscara de sub-rede*.

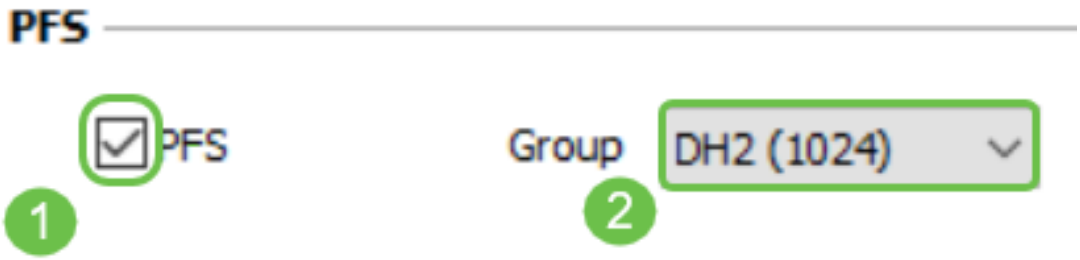



**Note:** Neste exemplo, foi escolhido o endereço único e inserido o endereço IP local do roteador no local.

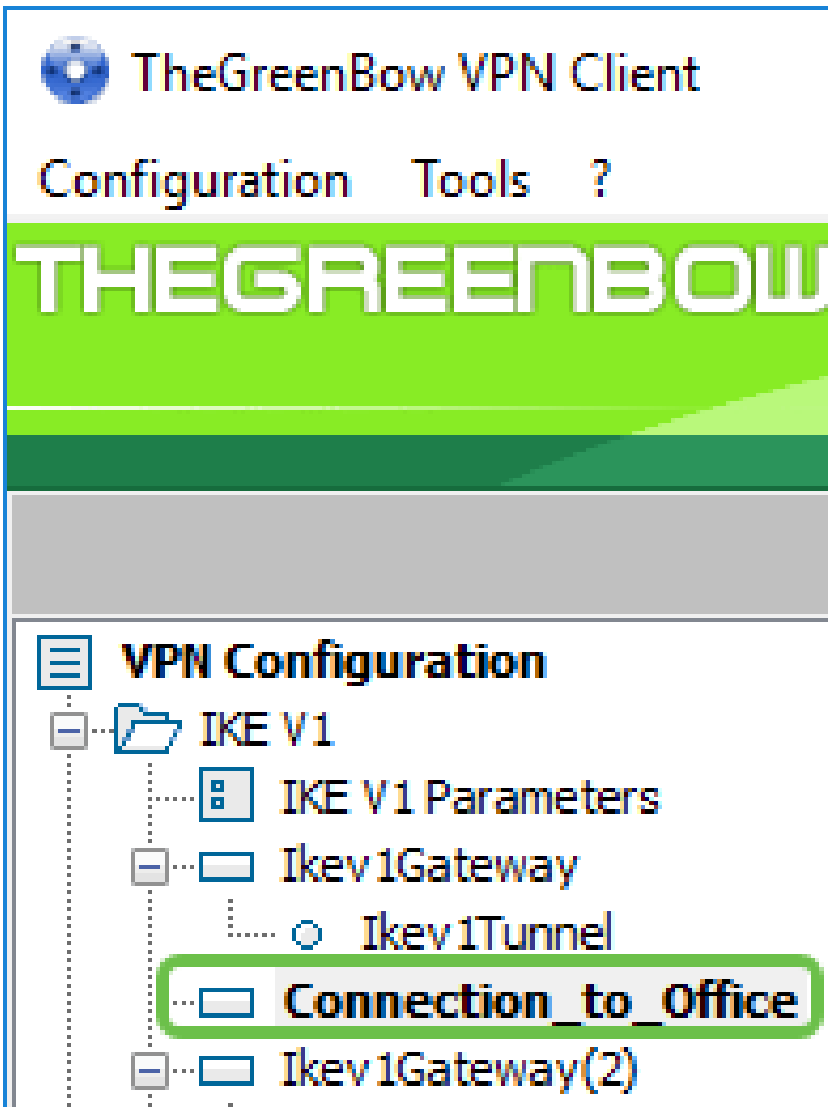
Etapa 3. Em *ESP*, defina Encryption, Authentication e Mode para corresponder às configurações do gateway VPN no site (escritório).



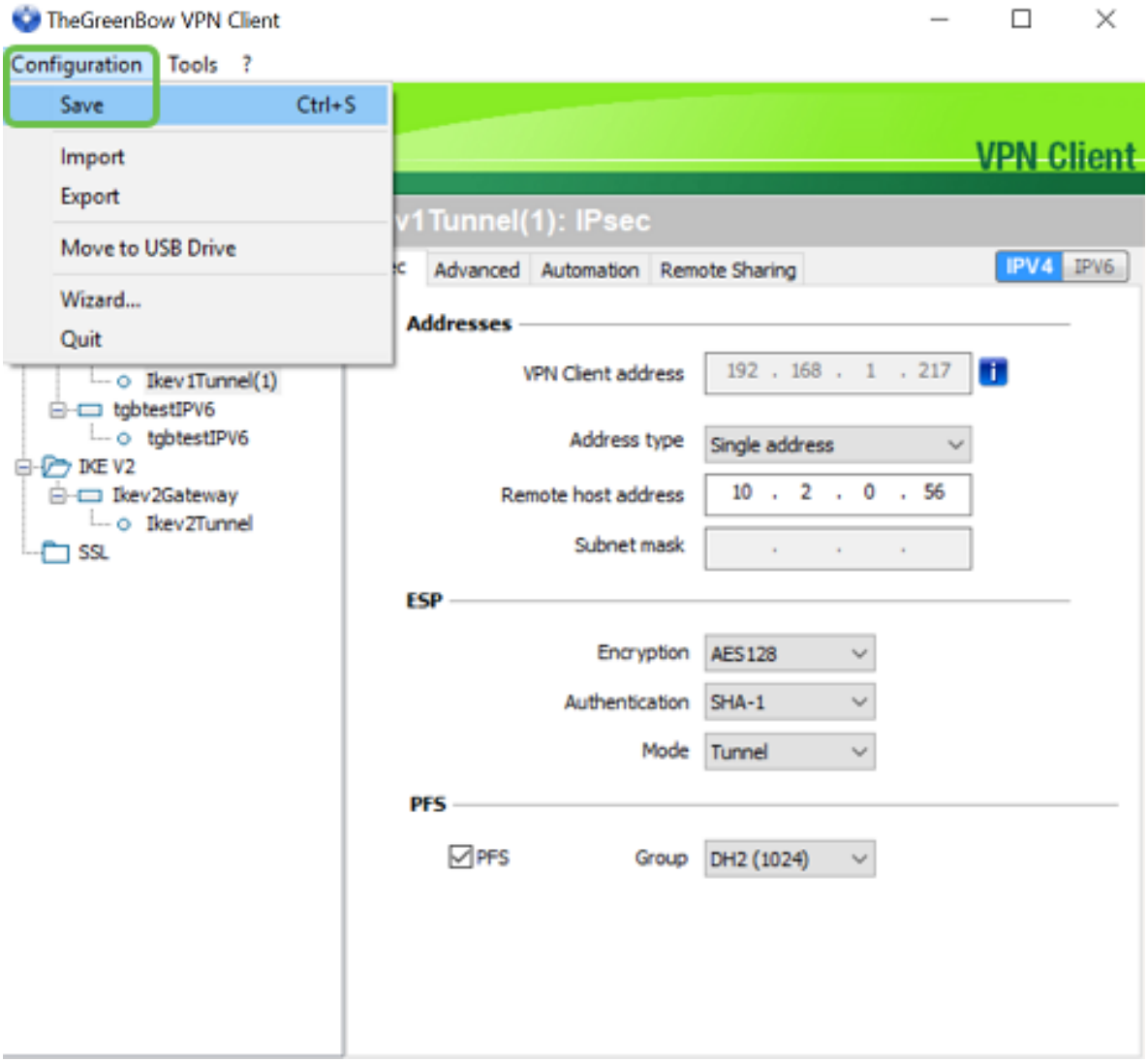

Etapa 4. (Opcional) Em *PFS*, marque a caixa de seleção **PFS** para ativar o Perfect Forward Secret (PFS). O PFS gera chaves aleatórias para criptografar a sessão. Selecione uma configuração de grupo PFS na lista suspensa *Grupo*. Se estiver ativado no roteador, ele também deve ser ativado aqui.




Etapa 5. (Opcional) Clique com o botão direito do mouse no nome do Gateway Ikev1e clique na seção renomear se desejar renomeá-lo.



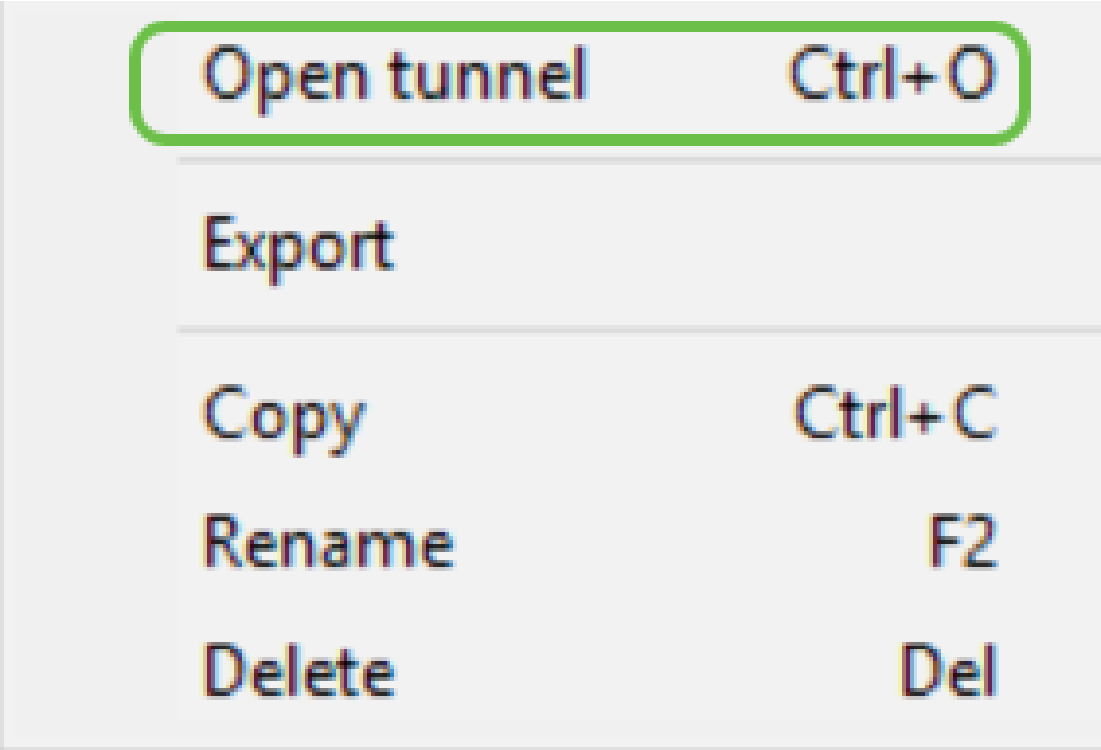

Etapa 6. Clique em **Configuração** e escolha **Salvar**.




Agora você deve ter configurado com êxito o cliente VPN TheGreenBow para se conectar ao roteador RV160 ou RV260 através da VPN.

## Iniciar uma conexão VPN como um cliente

Etapa 1. Como o GreenBow está aberto, você pode clicar com o botão direito do mouse no túnel e selecionar **Abrir túnel para iniciar uma conexão**.

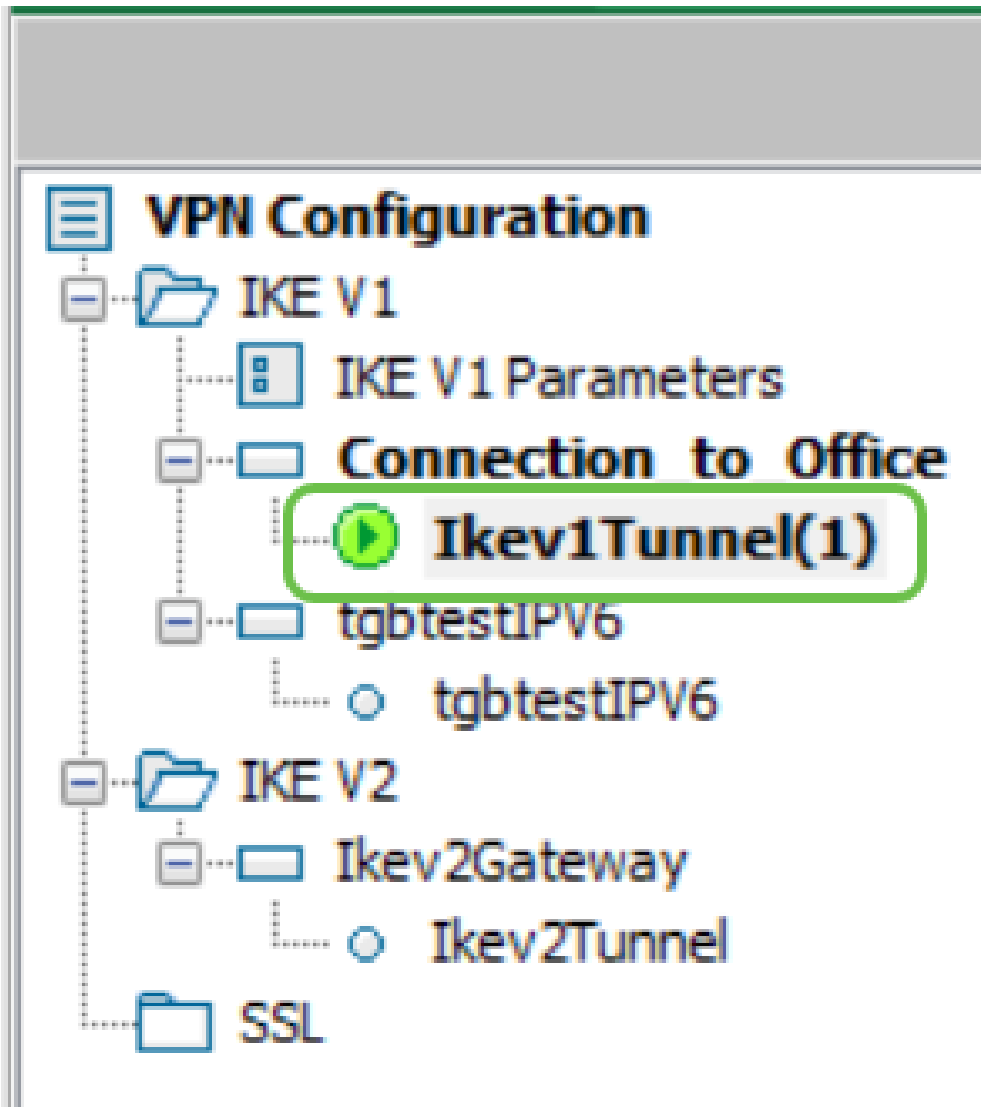



**Note:** Você também pode abrir um túnel clicando duas vezes nele.

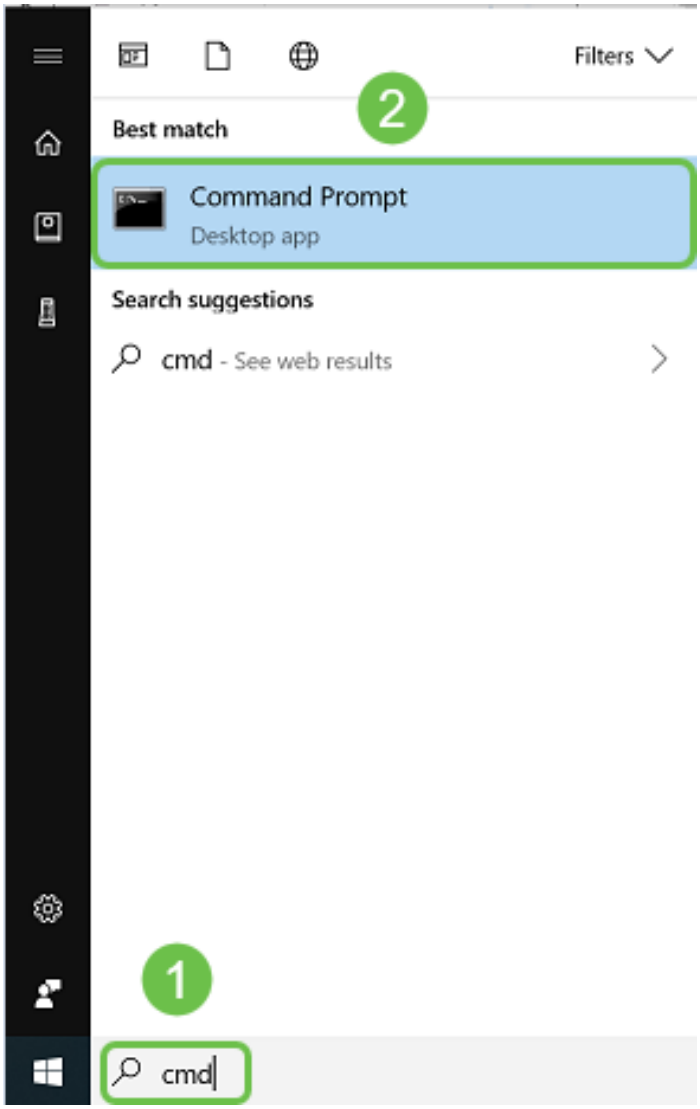
Etapa 2. (Opcional) Se você estiver iniciando uma nova sessão e tiver fechado o TheGreenBow, clique no ícone **TheGreenBow VPN Client** no lado direito da tela.

Etapa 3. (Opcional) Esta etapa só é necessária se você estiver configurando uma nova sessão e tiver seguido a Etapa 2. Escolha a conexão VPN que você precisa usar e clique em **ABRIR**. A conexão VPN deve ser iniciada automaticamente.

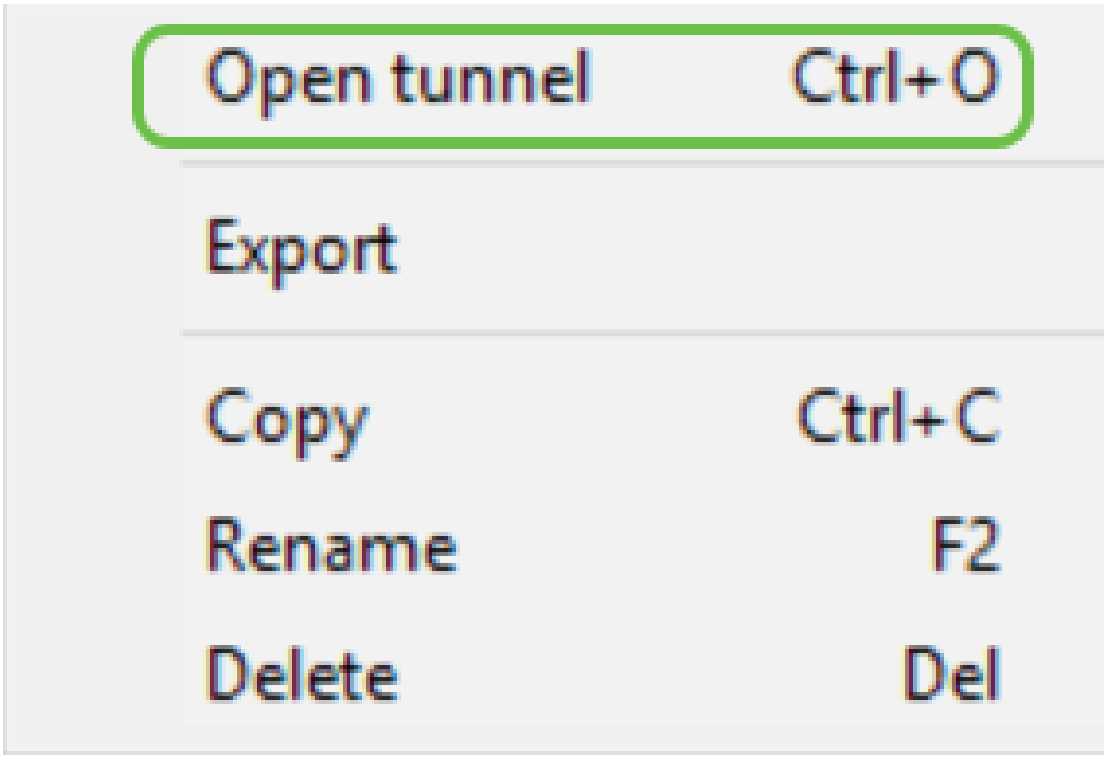

Etapa 4. Quando o túnel está conectado, um círculo verde aparecerá ao lado do túnel. Se você vir um ponto de exclamação, poderá clicar nele para localizar o erro.




Etapa 5. (Opcional) Para verificar se você está conectado, acesse o prompt de comando do computador cliente.



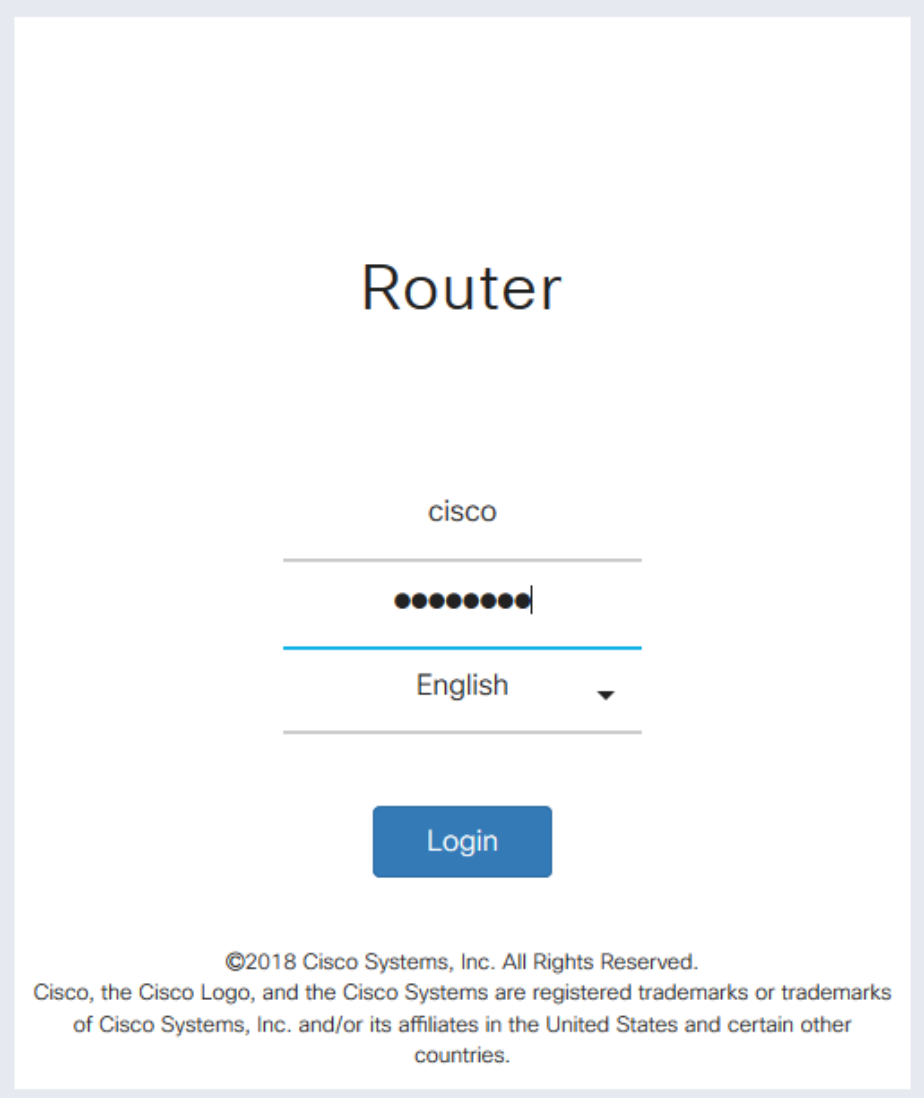

Etapa 6. (Opcional) Insira ping e, em seguida, o endereço IP da LAN privada do roteador no local. Se você receber respostas, estará conectado.



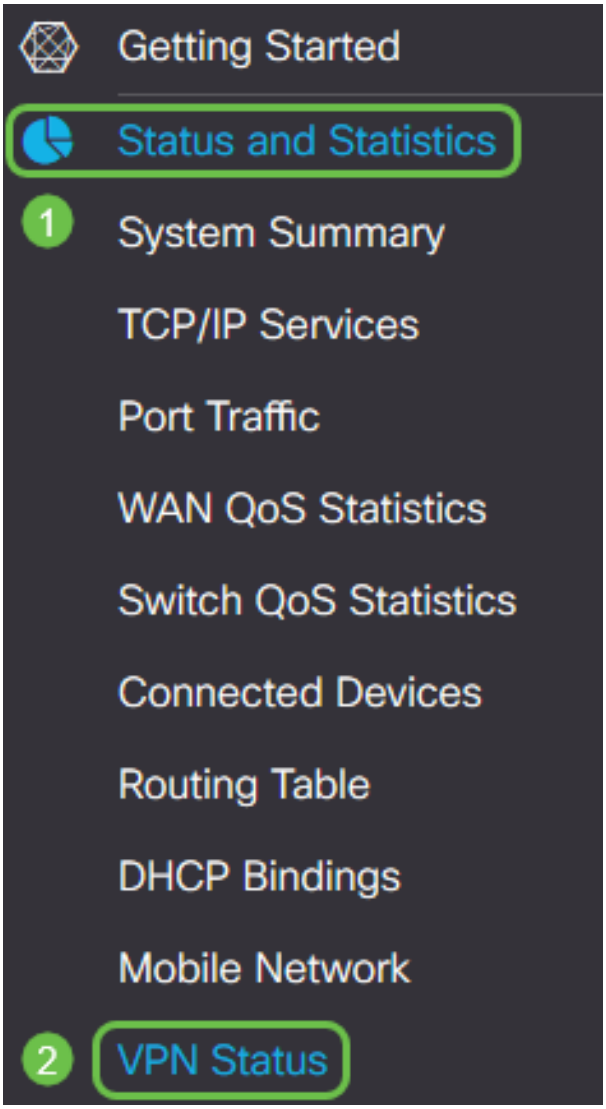

## Verificar o status da VPN

## Verifique o status da VPN no local

Etapa 1. Faça login no utilitário baseado na Web do gateway VPN do RV160 ou RV260.




Etapa 2. Escolha **Status e Statistics > VPN Status**.

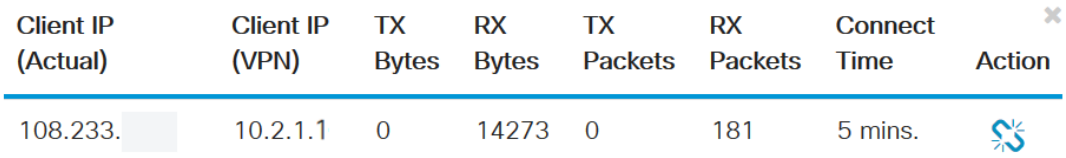



Etapa 3. Em *Client-to-Site Tunnel Status*, verifique a coluna *Connections* da *Connection Table*. Você deve ver a conexão VPN confirmada.


Etapa 4. Clique no ícone **ocular** para ver mais detalhes.


Etapa 5. Os detalhes do Status da VPN de Cliente para Site são mostrados aqui. Você observará o endereço IP da WAN do cliente, o endereço IP local que foi atribuído do pool de endereços que foi configurado na configuração. Ele também mostra bytes e pacotes enviados e recebidos, bem

como o tempo de conexão. Se quiser desconectar o cliente, clique no ícone azul **de cadeia quebrada** em *Action*. Clique no **x** no canto superior direito para fechar após a inspeção.



| Client IP (Actual) | Client IP (VPN) | TX Bytes | RX Bytes | TX Packets | RX Packets | Connect Time | Action |
|---|---|---|---|---|---|---|---|
| 108.233. | 10.2.1.1 | 0 | 14273 | 0 | 181 | 5 mins. | |

# Conclusão

Agora você deve ter configurado e verificado com êxito a conexão VPN no roteador RV160 ou RV260 e o cliente VPN do TheGreenBow configurado para se conectar ao roteador através da VPN também.