Usar o GreenBow VPN Client para se conectar ao RV34x Series Router

Aviso especial: Estrutura de licenciamento – Firmware versões 1.0.3.15 e posteriores. No futuro, o AnyConnect cobrará apenas pelas licenças do cliente.

Para obter informações adicionais sobre o licenciamento do AnyConnect nos roteadores da série RV340, consulte o artigo AnyConnect Licensing for the RV340 Series Routers.

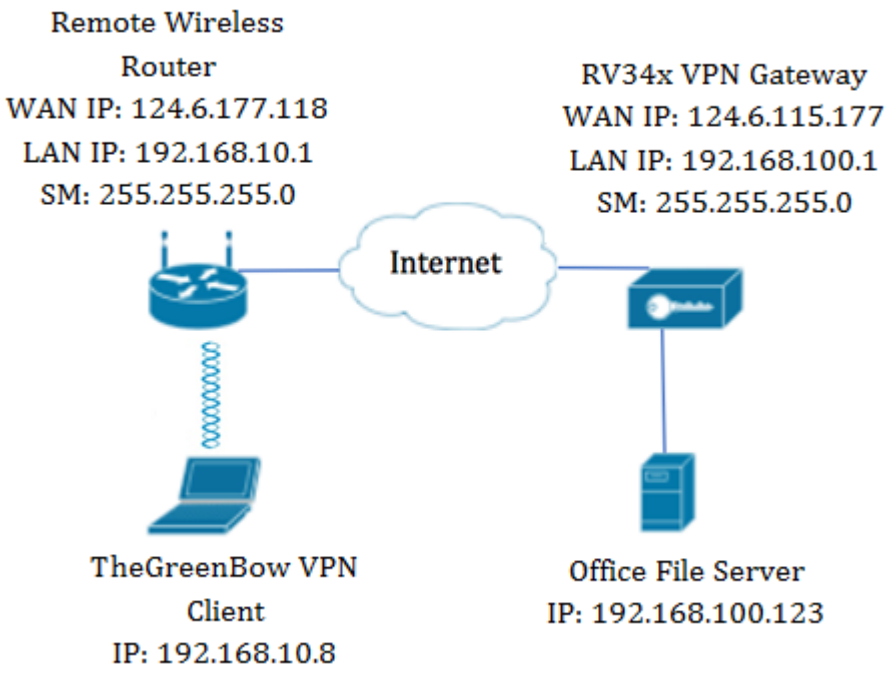
Introduction

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 usam principalmente a 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 atue como se estivesse localizado na mesma rede local. O roteador suporta até 50 túneis. 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.

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 site para site com o RV34x Series Router.



No diagrama, o computador se conectará ao servidor de arquivos no escritório fora de sua rede para acessar seus recursos. Para fazer isso, o cliente VPN do GreenBow no computador será configurado de forma que ele retire as configurações do gateway VPN RV34x.

Benefícios do uso de uma conexão VPN

1. Usar uma conexão VPN ajuda a proteger dados e recursos confidenciais da rede.
2. 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.
3. A comunicação usando uma conexão VPN fornece um nível mais alto de segurança comparado a outros métodos de comunicação remota. O nível avançado de tecnologia hoje em dia torna isso possível, protegendo assim a rede privada de acesso não autorizado.
4. A localização geográfica real dos usuários é protegida e não exposta a redes públicas ou compartilhadas, como a Internet.
5. Adicionar novos usuários ou grupos de usuários à rede é fácil, pois as VPNs são facilmente escaláveis. É possível fazer a rede crescer sem a necessidade de componentes adicionais ou configuração complicada.

Riscos do uso de uma conexão VPN

1. Risco de segurança devido a configuração incorreta. 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.
2. Confiabilidade. 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.
3. Escalabilidade. Se se tratar de uma situação em que há 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.
4. Problemas de segurança para dispositivos móveis. Ao iniciar a conexão VPN em um dispositivo móvel, podem surgir problemas de segurança especialmente quando o dispositivo móvel está conectado à rede local sem fio.
5. Velocidades de conexão lentas. 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.

Pré-requisitos para usar o cliente VPN GreenBow

Os itens a seguir devem ser configurados primeiro no roteador VPN e serão aplicados ao cliente VPN TheGreenBow clicando aqui para estabelecer uma conexão.

1. Criar um perfil cliente-local no gateway de VPN
2. Crie um grupo de usuários no gateway de VPN
3. Criar conta de usuário no gateway de VPN
4. Criar um perfil IPSec no gateway de VPN
5. Defina as configurações de Fase I e Fase II no gateway de VPN

Dispositivos aplicáveis

- Série RV34x

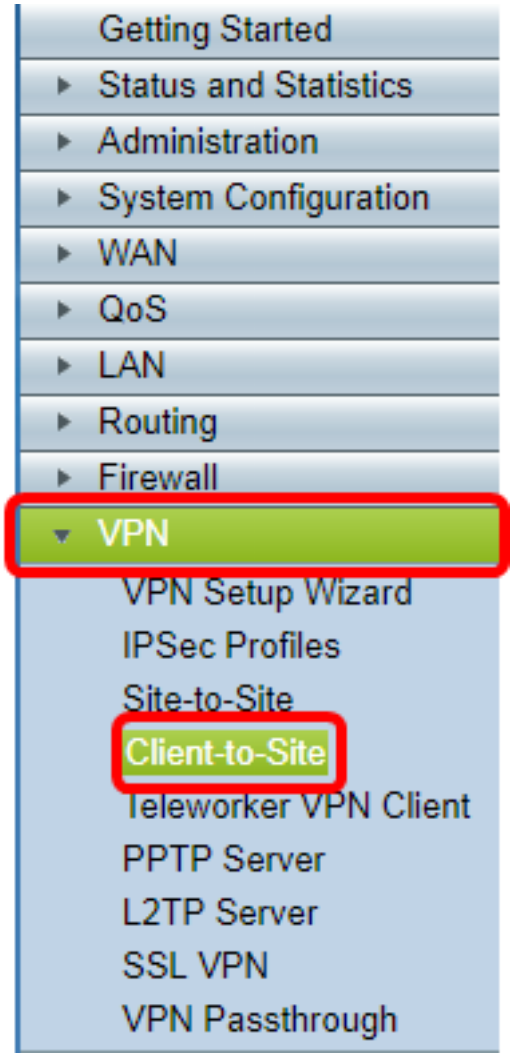
Versão de software

- 1.0.01.17

Usar o cliente GreenBow VPN

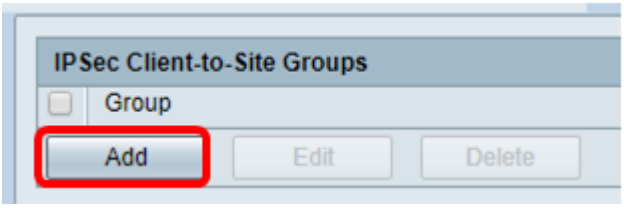
Crie um perfil cliente-local no roteador

Etapa 1. Faça login no utilitário baseado na Web do RV34x Router e escolha **VPN > Cliente para Site**.



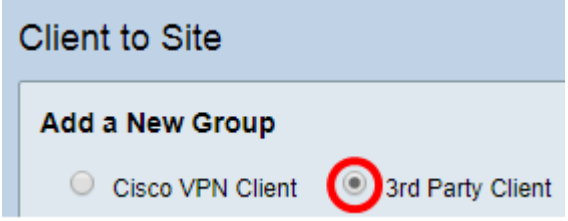
Note: As imagens neste artigo são obtidas do RV340 Router. As opções podem variar, dependendo do modelo do dispositivo.

Etapa 2. Clique em Add.



Etapa 3. Clique em **Cliente terceirizado**.

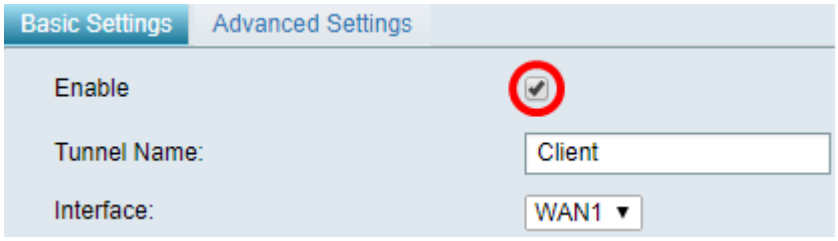
Note: O AnyConnect é um exemplo de um Cisco VPN Client, enquanto o GreenBow VPN Client é um exemplo de um VPN Client de terceiros.



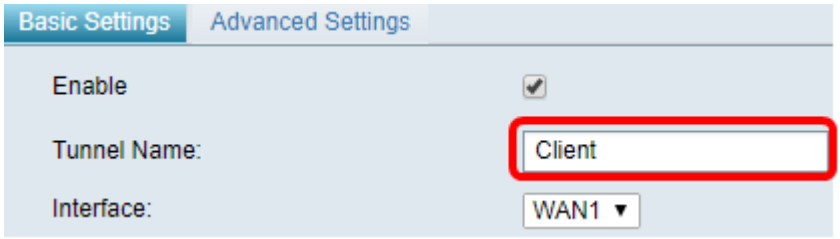
Note: Neste exemplo, o cliente de terceiros é escolhido.

Etapa 4. Na guia Basic Settings (Configurações básicas), marque a caixa de seleção **Enable**

para garantir que o perfil VPN esteja ativo.

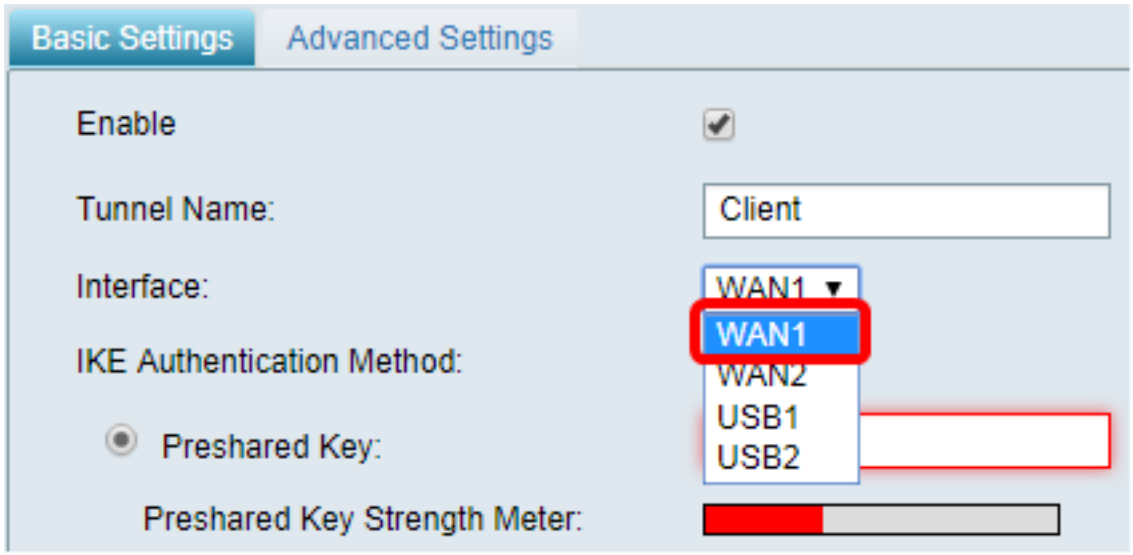


Etapa 5. Digite um nome para a conexão VPN no campo *Nome do túnel*.



Note: Neste exemplo, **Cliente** é inserido.

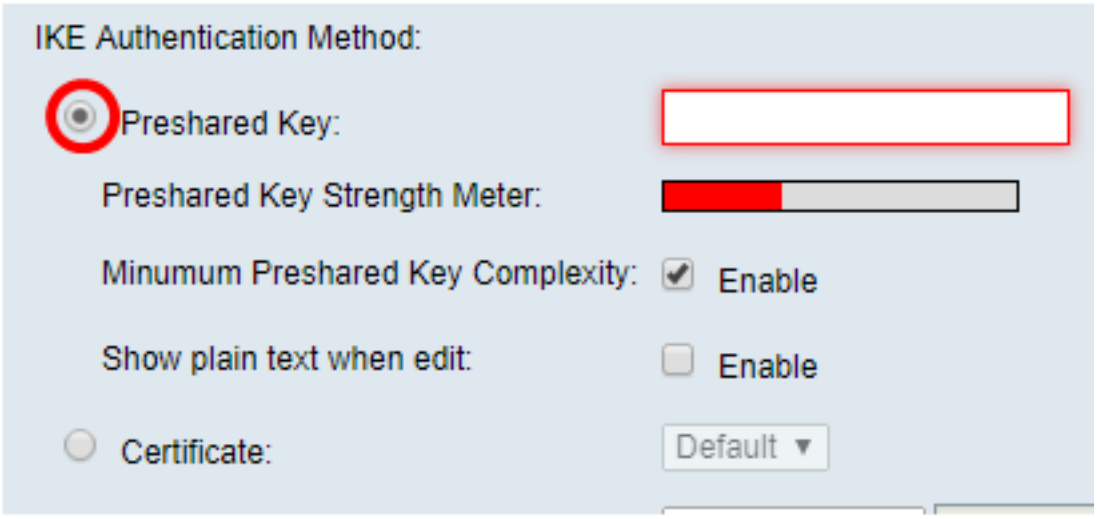
Etapa 6. Escolha a Interface a ser usada na lista suspensa Interface. As opções são WAN1, WAN2, USB1 e USB2 que usarão a interface correspondente no roteador para a conexão VPN.



Note: As opções dependem do modelo do roteador que você está usando. Neste exemplo, a WAN1 é escolhida.

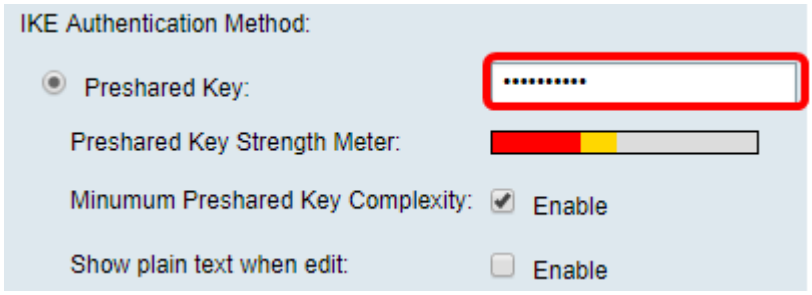
Passo 7. Escolha um método de autenticação IKE. As opções são:

- Presshared Key — (Chave pré-compartilhada) 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.

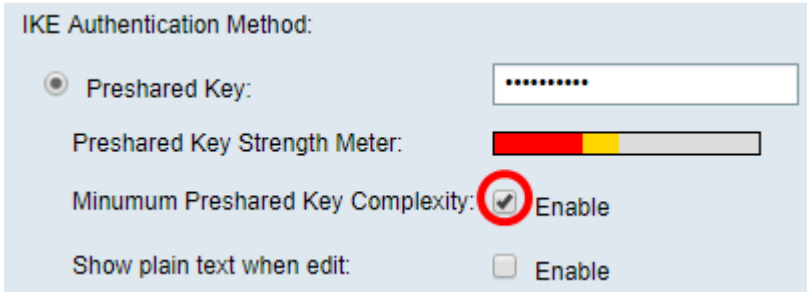


Note: Neste exemplo, a chave pré-compartilhada é escolhida.

Etapa 8. Digite a senha da conexão no campo *Presshared Key*.

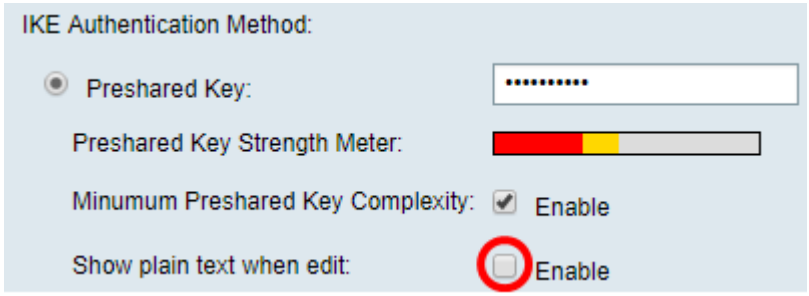


Etapa 9. (Opcional) Desmarque a caixa de seleção **Habilitar** complexidade mínima de chave pré-compartilhada para poder usar uma senha simples.



Note: Neste exemplo, a Complexidade mínima de chave pré-compartilhada é deixada habilitada.

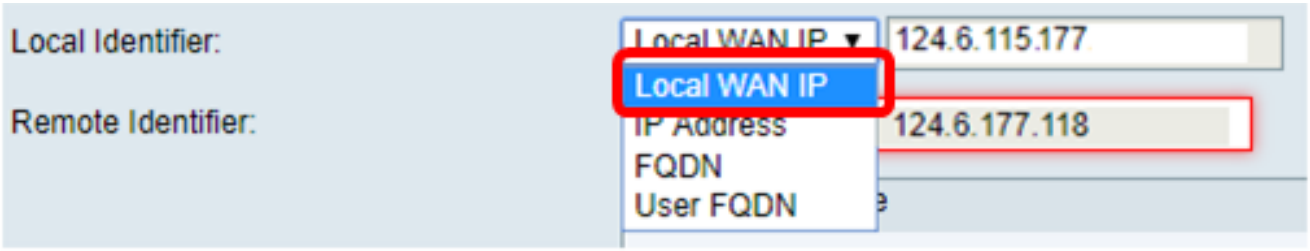
Etapa 10. (Opcional) Marque a caixa de seleção Mostrar texto sem formatação ao editar **Habilitar** para mostrar a senha em texto sem formatação.



Note: Neste exemplo, Mostrar texto sem formatação quando a edição é deixada desabilitada.

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

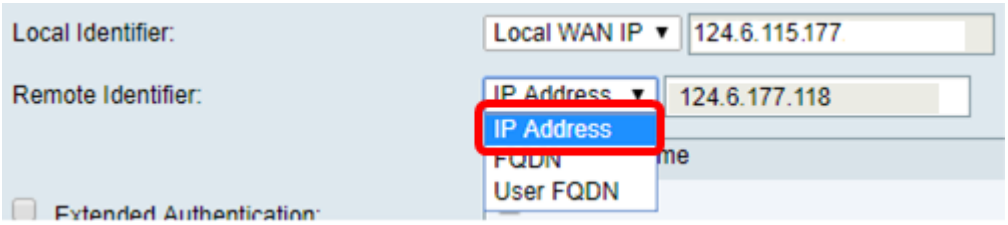
- Local WAN IP — Essa opção usa o endereço IP da interface de rede de longa distância (WAN) do gateway VPN.
- Endereço IP — Essa opção permite inserir manualmente um endereço IP para a conexão VPN.
- FQDN — Essa opção também é conhecida como Nome de domínio totalmente qualificado (FQDN). Ele permite 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, Local WAN IP é escolhido. Com essa opção, o IP da WAN local é detectado automaticamente.

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

- Endereço IP — Essa opção usa o endereço IP WAN do cliente VPN.
- FQDN — Essa 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.

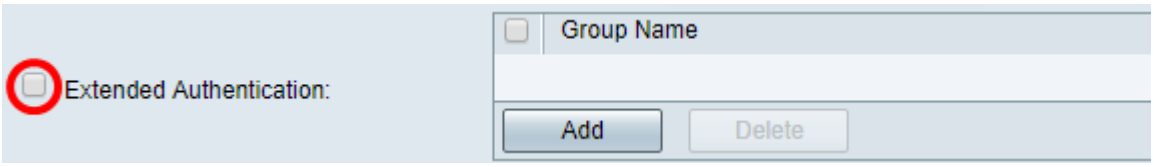


Note: Neste exemplo, Endereço IP é escolhido.

Etapa 13. Insira o identificador remoto no campo *Identificador remoto*.

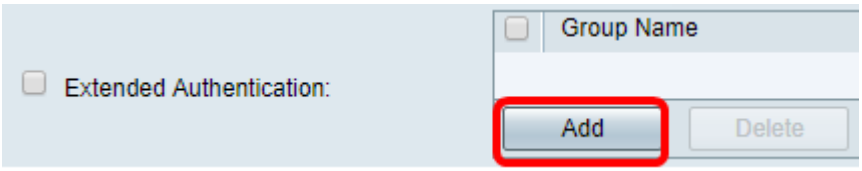
Note: Neste exemplo, 124.6.115.177 é inserido.

Etapa 14. (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.

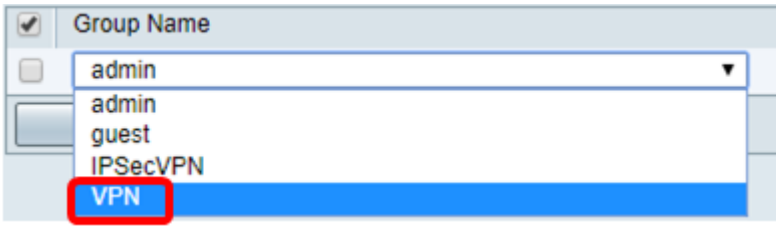


Note: Neste exemplo, a Autenticação Estendida é deixada desmarcada.

Etapa 15. Em Nome do grupo, clique em **Adicionar**.



Etapa 16. Escolha o grupo que usará autenticação estendida na lista suspensa Nome do grupo.



Note: Neste exemplo, a VPN é escolhida.

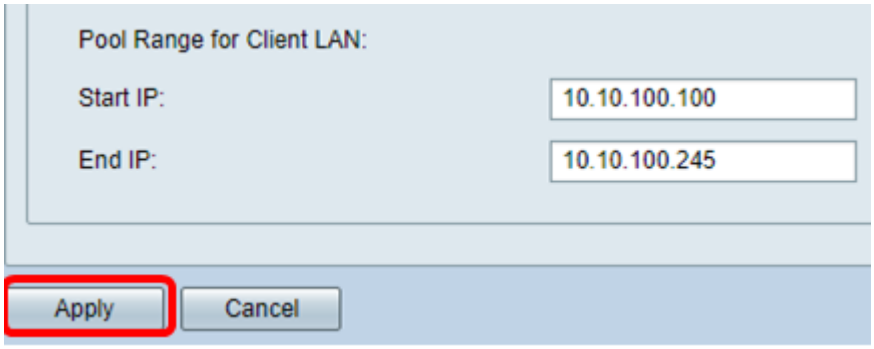
Etapa 17. Em Pool Range for Client LAN, insira o primeiro endereço IP que pode ser atribuído a um cliente VPN no campo *Start IP*.

Note: Neste exemplo, 10.10.100.100 é inserido.

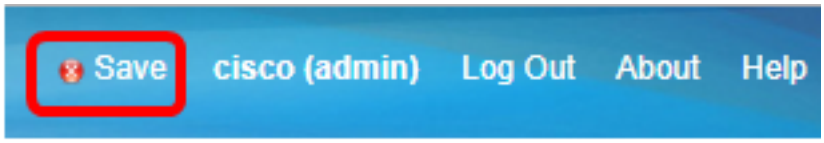
Etapa 18. Insira o último endereço IP que pode ser atribuído a um cliente VPN no campo *End IP*.

Note: Neste exemplo, 10.10.100.245 é inserido.

Etapa 19. Clique em Apply.



Etapa 20. Click **Save**.

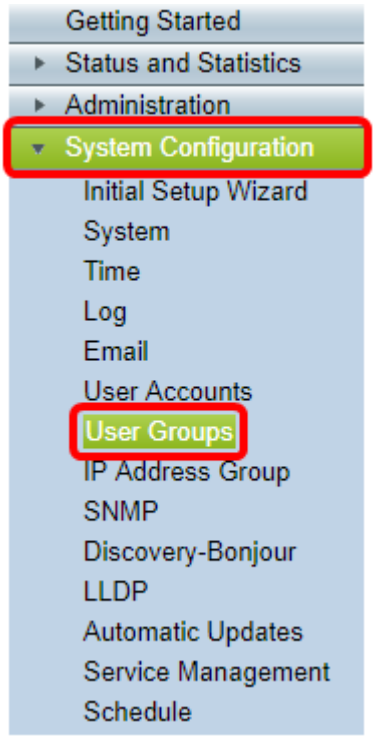


Agora você deve ter configurado o perfil cliente-local no roteador para o cliente VPN do GreenBow.

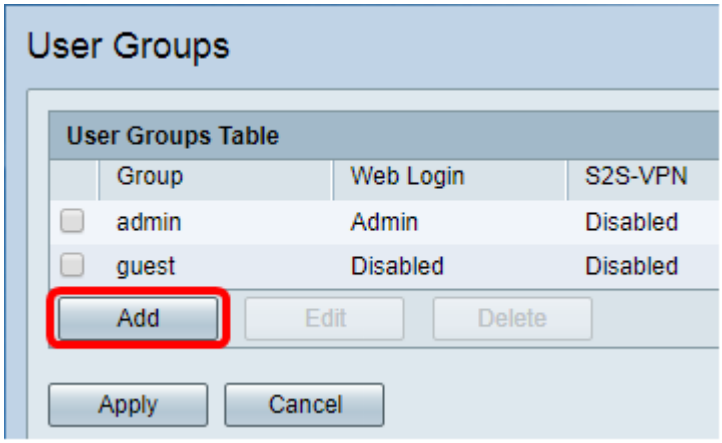
Criar um grupo de usuários

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

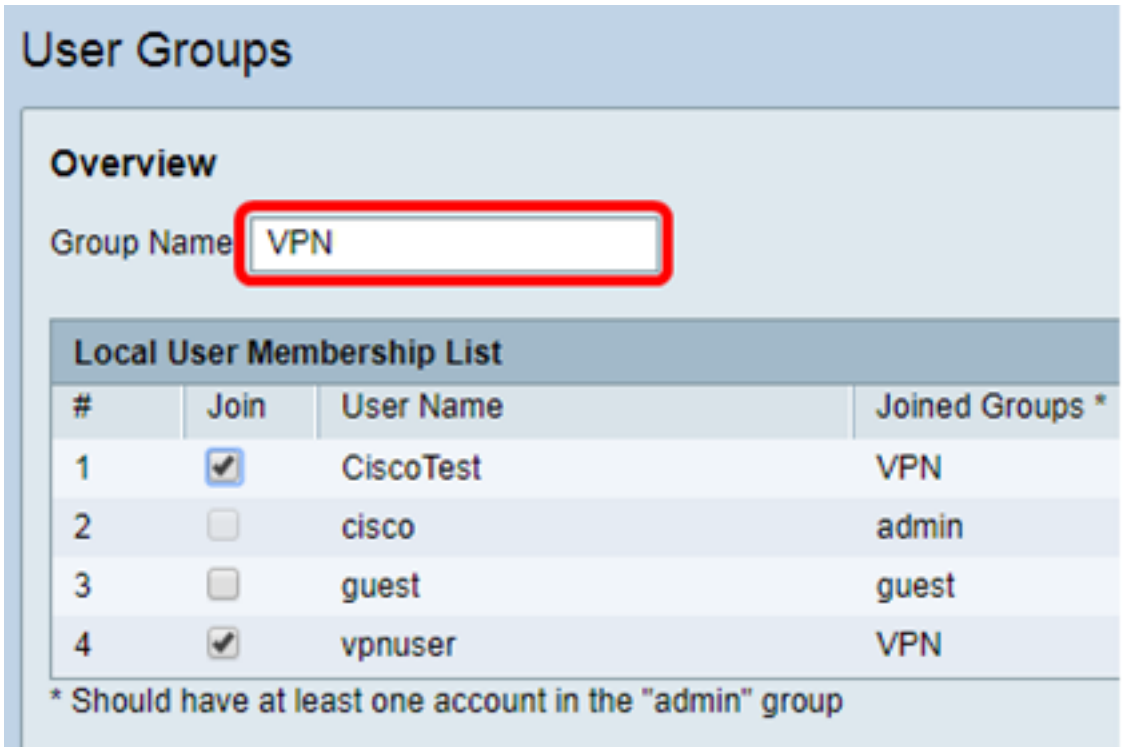
Note: As imagens neste artigo são de um roteador RV340. As opções podem variar dependendo do modelo do dispositivo.



Etapa 2. Clique em **Adicionar** para adicionar um grupo de usuários.

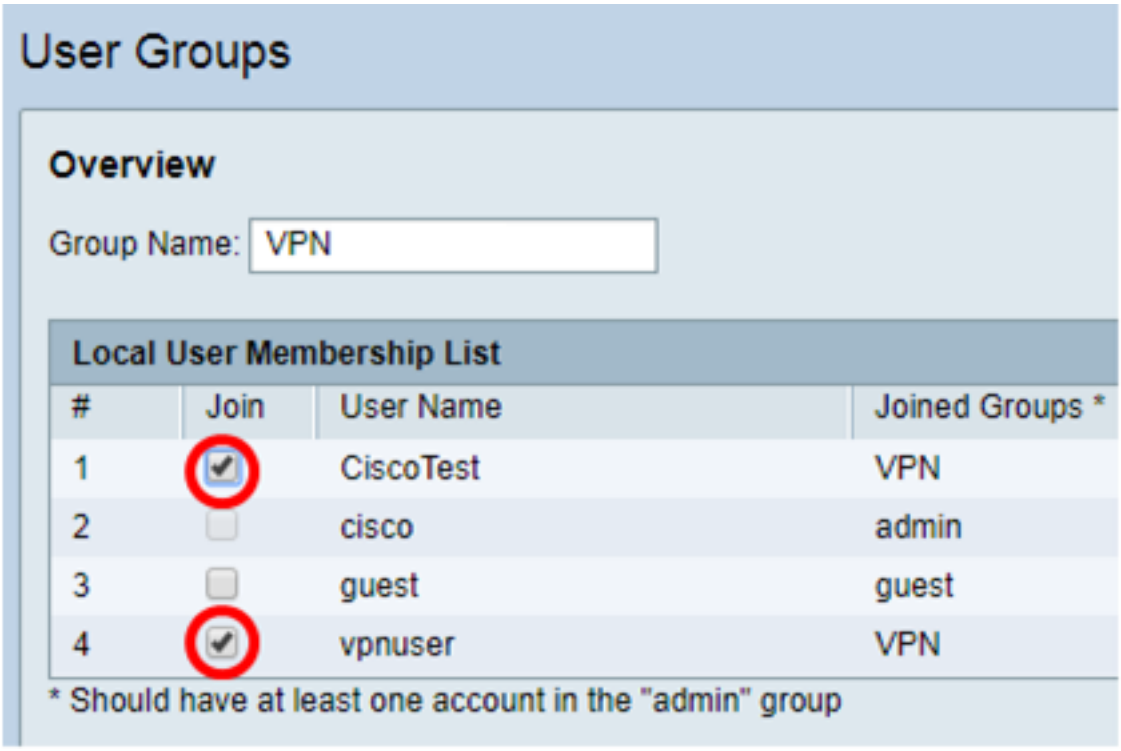


Etapa 3. Na área Visão geral, insira o nome do grupo no campo *Nome do grupo*.



Note: Neste exemplo, a VPN é usada.

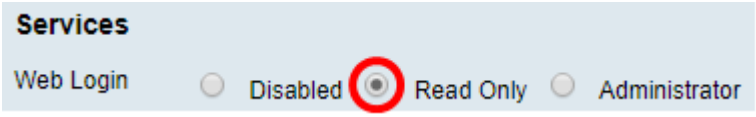
Etapa 4. Em Lista de associação local, marque as caixas de seleção dos nomes de usuário que precisam estar no mesmo grupo.



Note: Neste exemplo, CiscoTest e vpnuser são escolhidos.

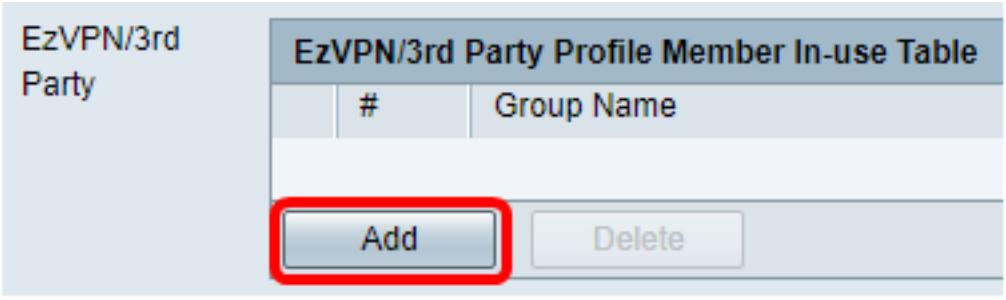
Etapa 5. Em Serviços, escolha uma permissão a ser concedida aos usuários do grupo. As opções são:

- Desativado — Essa opção significa que os membros do grupo não têm permissão para acessar o utilitário baseado na Web por meio de um navegador.
- Read Only (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.
- Administrador — Essa opção dá aos membros do grupo privilégios de leitura e gravação e pode configurar o status do sistema.

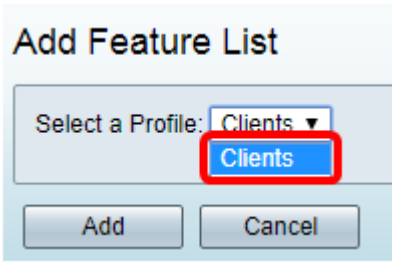


Note: Neste exemplo, somente leitura é escolhido.

Etapa 6. Na Tabela em uso do membro do perfil EzVPN/Terceiros, clique em **Adicionar**.

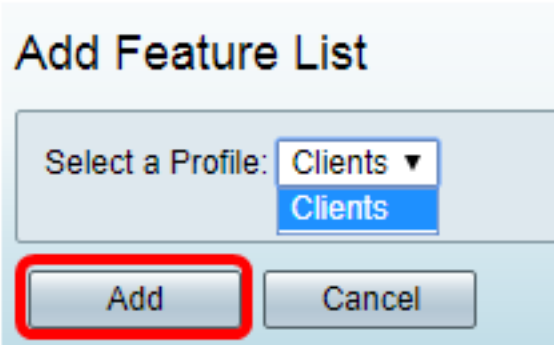


Passo 7. Escolha um perfil na lista suspensa Selecionar um perfil. As opções podem variar, dependendo dos perfis que foram configurados no gateway VPN.

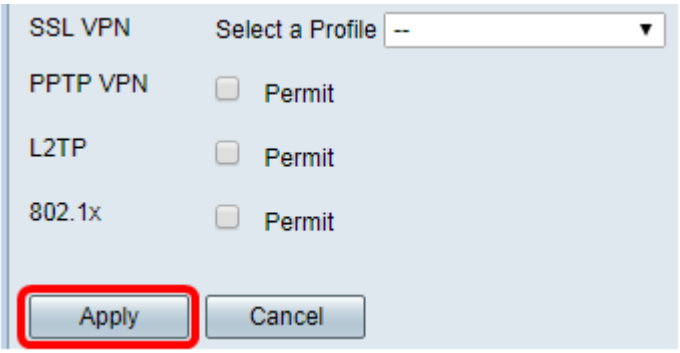


Note: Neste exemplo, Clientes são escolhidos.

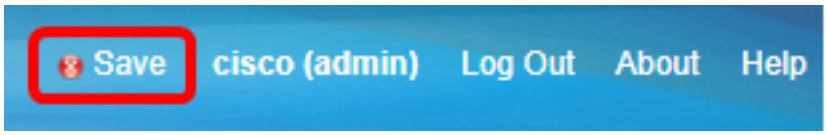
Etapa 8. Clique em Add.



Etapa 9. Clique em Apply.



Etapa 10. Click **Save**.

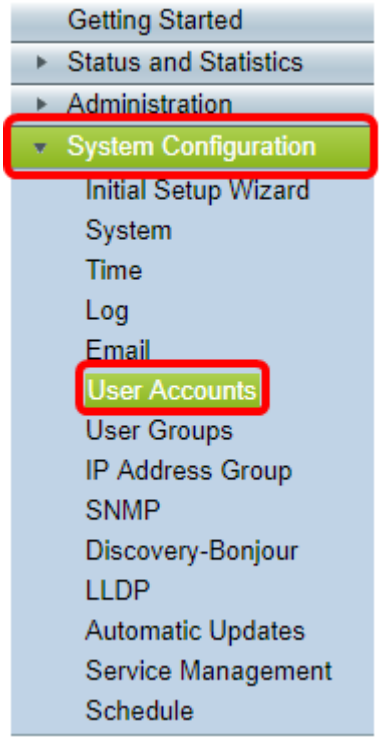


Agora você deve ter criado com êxito um grupo de usuários no RV34x Series Router.

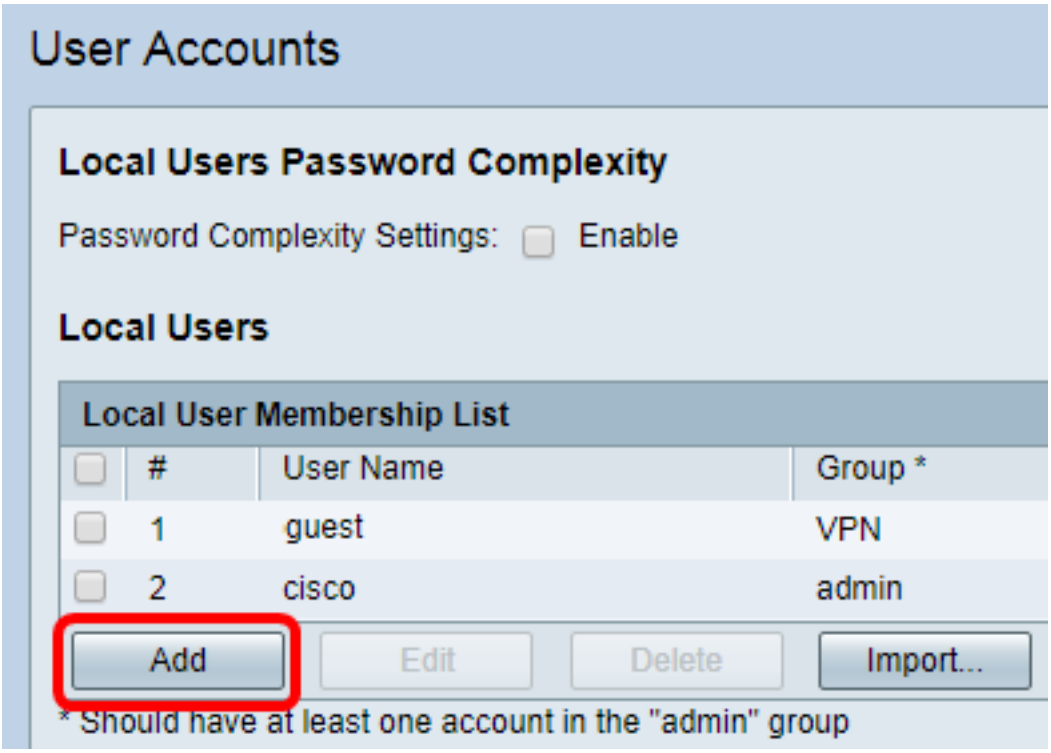
Criar uma conta de usuário

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

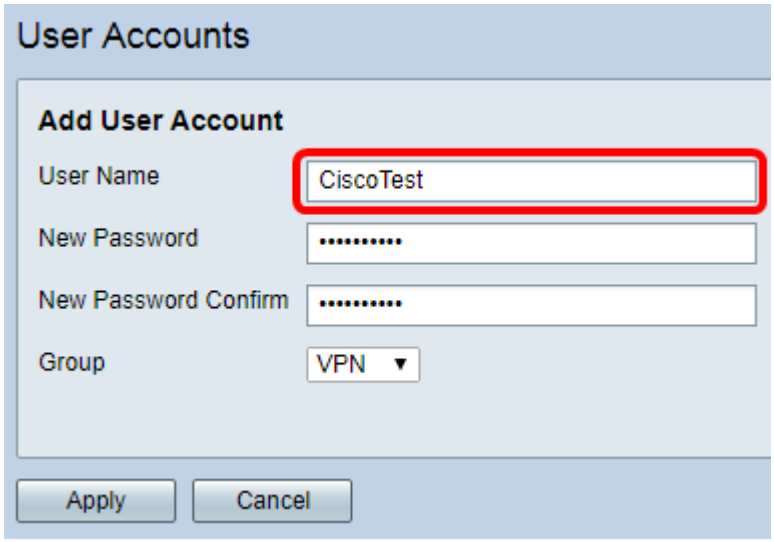
Note: As imagens neste artigo são obtidas de um roteador RV340. As opções podem variar dependendo do modelo do dispositivo.



Etapa 2. Na área Lista de associação de usuário local, clique em **Adicionar**.

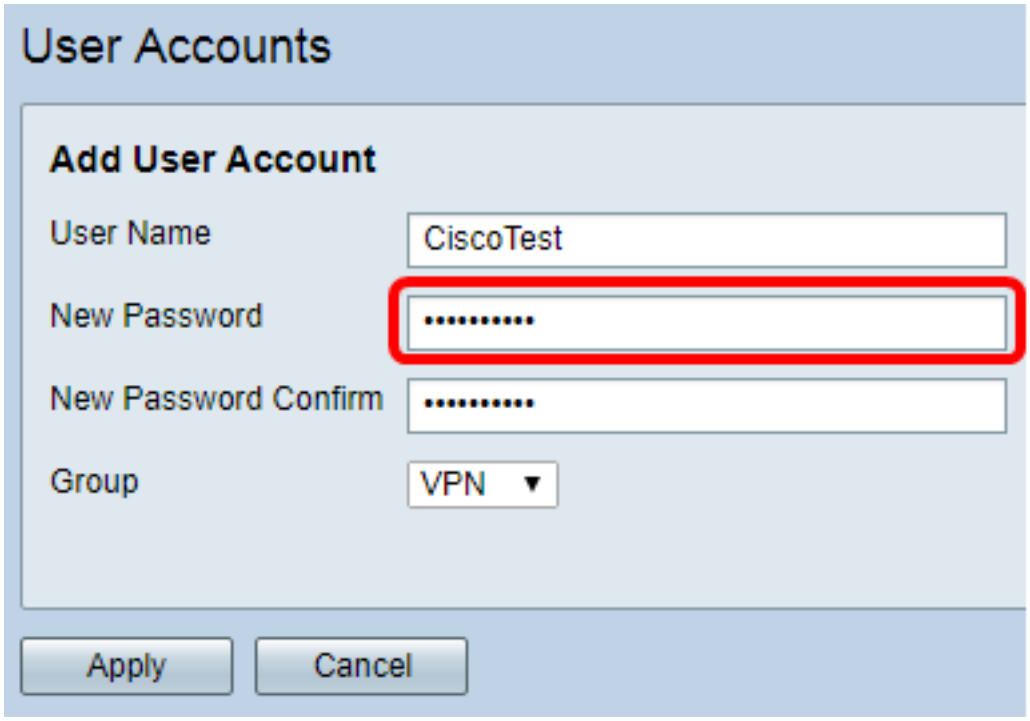


Etapa 3. Digite um nome para o usuário no campo *Nome de usuário*.

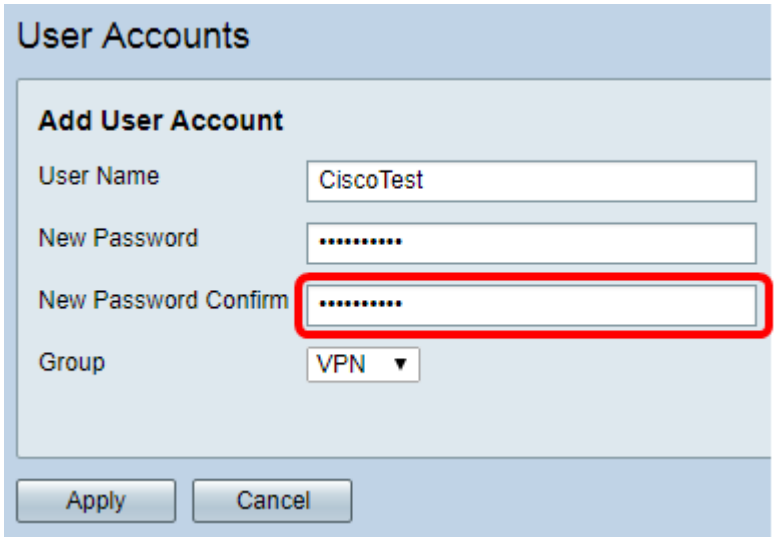


Note: Neste exemplo, o CiscoTest é inserido.

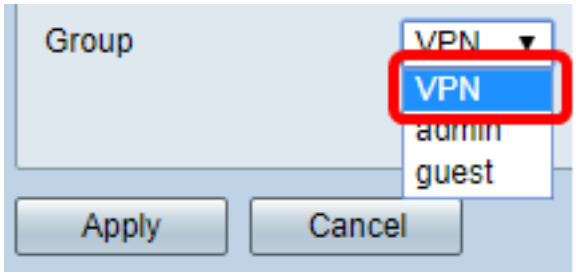
Etapa 4. Digite a senha do usuário no campo *Nova senha*.



Etapa 5. Confirme a senha na caixa *Nova confirmação de senha*.

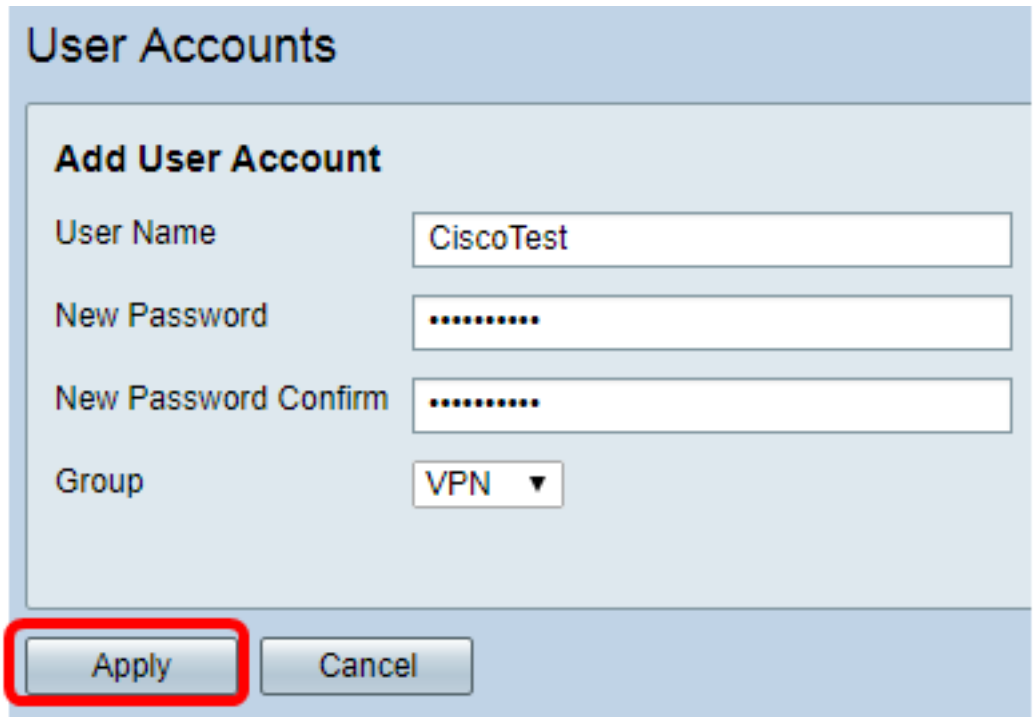


Etapa 6. Escolha um grupo na lista suspensa Grupo. Este é o grupo ao qual o usuário será associado.

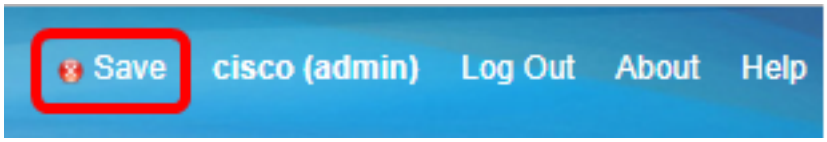


Note: Neste exemplo, a VPN é escolhida.

Passo 7. Clique em Apply.



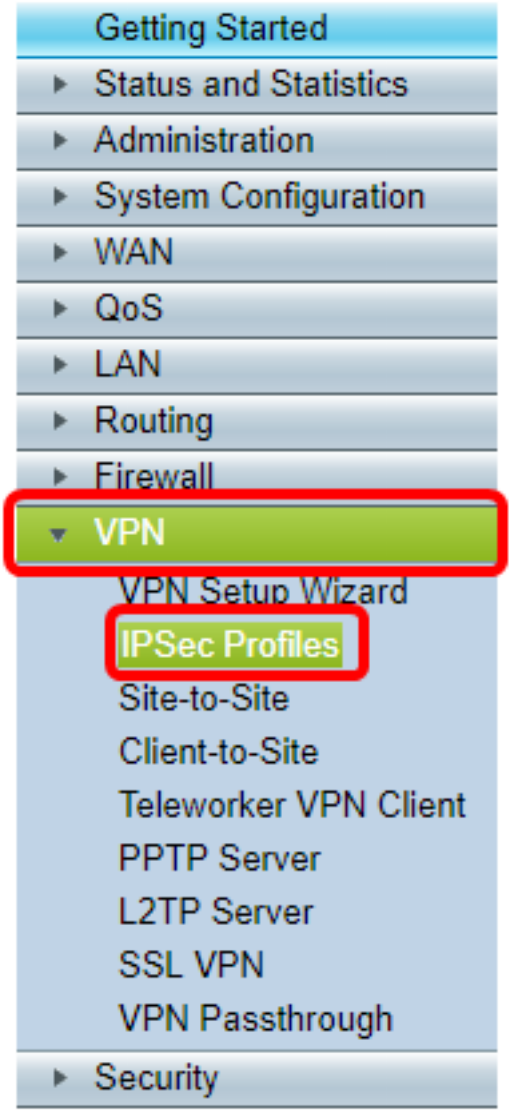
Etapa 8. Click **Save**.



Agora, você deve ter criado uma conta de usuário no seu RV34x Series Router.

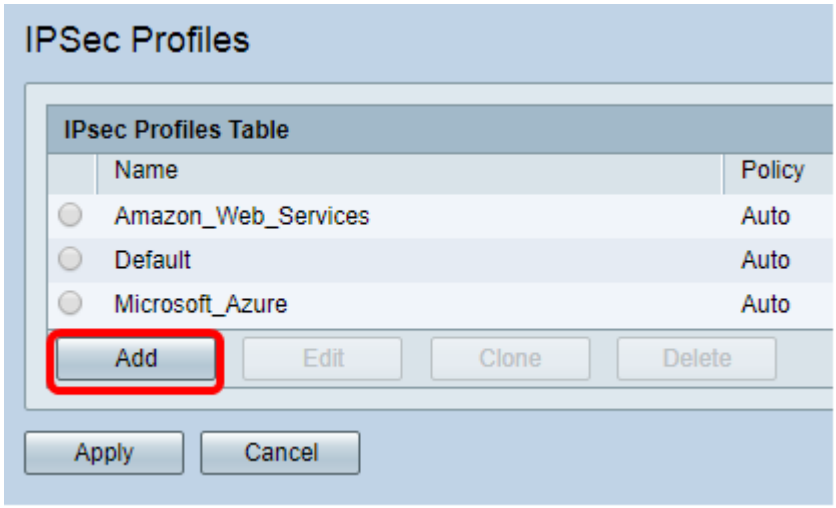
Configurar perfil de IPSec

Etapa 1. Faça login no utilitário baseado na Web do roteador RV34x e escolha **VPN > IPSec Profiles**.



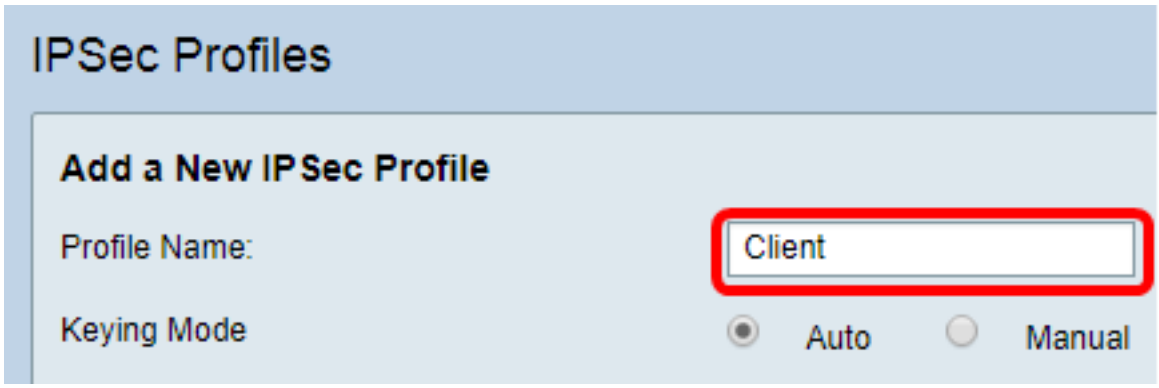
Note: As imagens neste artigo são obtidas do RV340 Router. As opções podem variar dependendo do modelo do dispositivo.

Etapa 2. A Tabela de perfis IPSec mostra os perfis existentes. Clique em **Adicionar** para criar um novo perfil.



Note: Amazon_Web_Services, Default e Microsoft_Azure são perfis padrão.

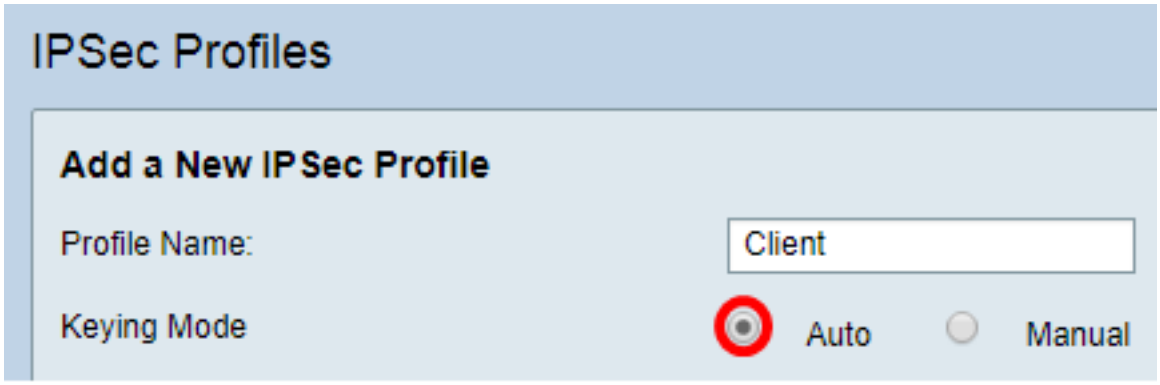
Etapa 3. Crie um nome para o perfil no campo *Nome do perfil*. O nome do perfil deve conter apenas caracteres alfanuméricos e um sublinhado (_) para caracteres especiais.



Note: Neste exemplo, Cliente é inserido.

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. Se esta opção for escolhida, vá para Configurar as configurações automáticas.
- 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. Se esta opção for selecionada, vá para Configurar configurações manuais.



Note: Para este exemplo, Auto foi escolhido.

[Definir as configurações da Fase I e da Fase II]

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.

Note: Neste exemplo, o bit Group5-1536 é escolhido.

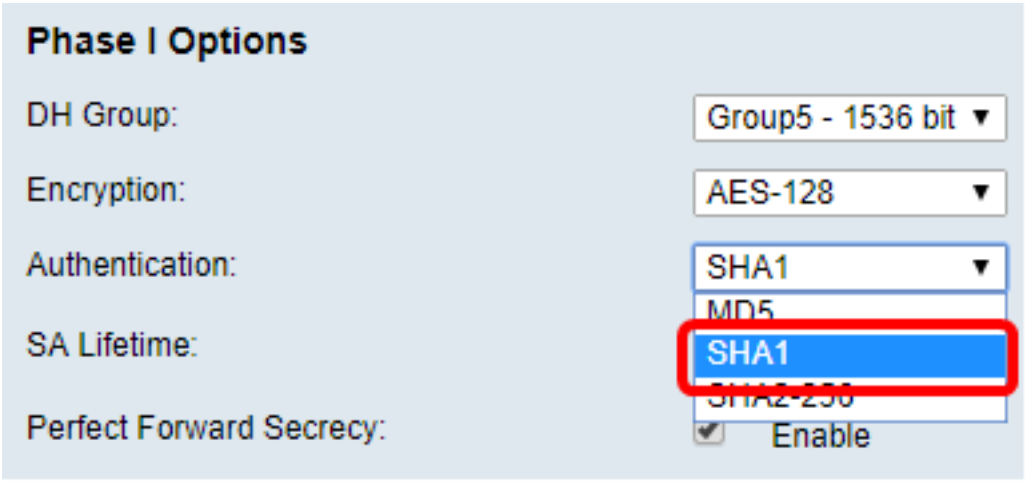
Etapa 2. Na lista suspensa Criptografia, escolha um método de criptografia para criptografar e descriptografar o Payload de Segurança de Encapsulamento (ESP - Encapsulating Security Payload) e o ISAKMP (Internet Security Association and Key Management Protocol). As opções são:

- 3DES — Triple Data Encryption Standard (Padrão triplo de criptografia de dados).
- 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.

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. Neste exemplo, AES-128 é escolhido.

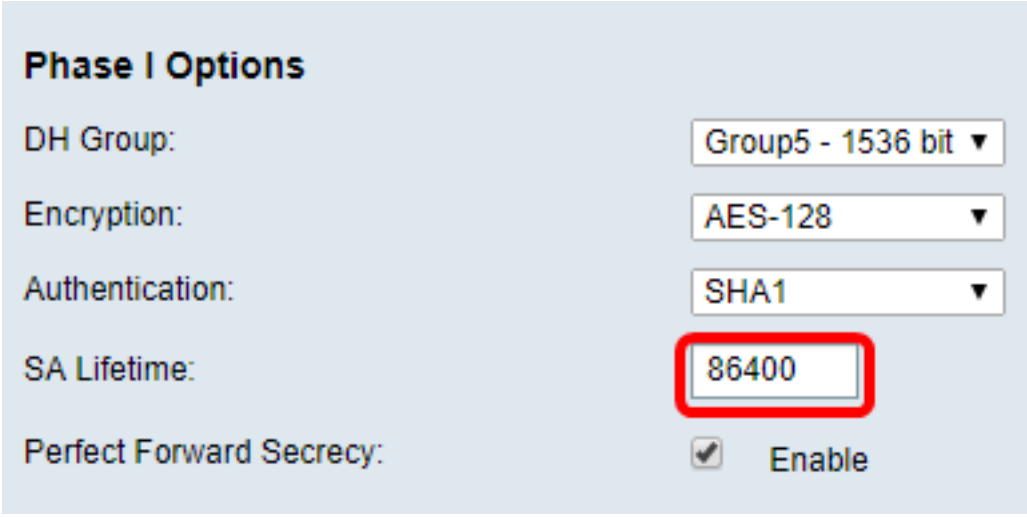
Etapa 3. Na lista suspensa Autenticação, escolha um método de autenticação que determinará como o ESP e o ISAKMP são autenticados. As opções são:

- 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.



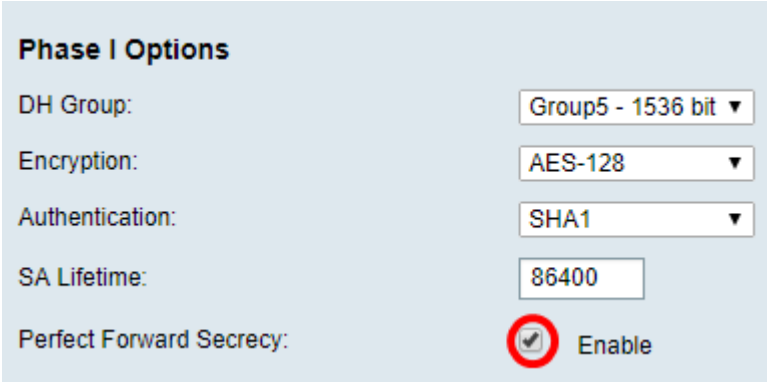
Note: MD5 e SHA são funções de hash criptográfico. Eles pegam um pedaço de dados, compactam-no e criam uma saída hexadecimal exclusiva que normalmente não pode ser reproduzida. Neste exemplo, SHA1 é escolhido.

Etapa 4. No campo *Vida útil do SA*, insira um valor entre 120 e 86400. Esse é o período de tempo durante o qual a Associação de Segurança (SA) do Internet Key Exchange (IKE) permanecerá ativa na fase. O valor padrão é 28800.



Note: Neste exemplo, 86400 é inserido.

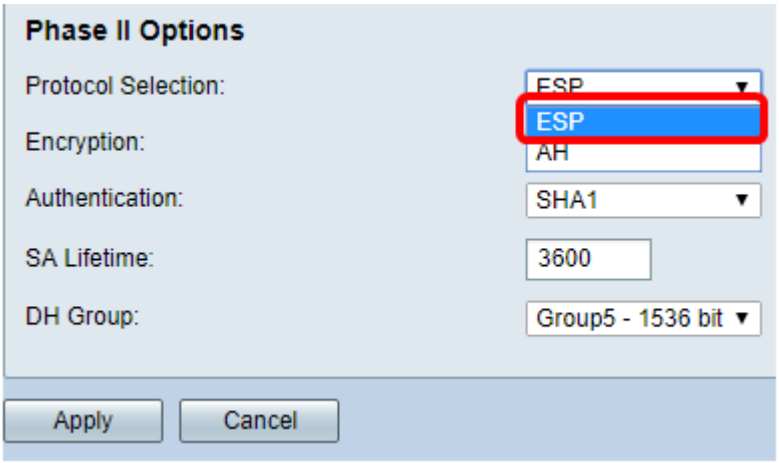
Etapa 5. (Opcional) Marque a caixa de seleção **Habilitar** segredo de encaminhamento perfeito para gerar uma nova chave para a criptografia e autenticação de tráfego IPSec.



Note: Neste exemplo, o segredo de encaminhamento perfeito está ativado.

Etapa 6. 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:

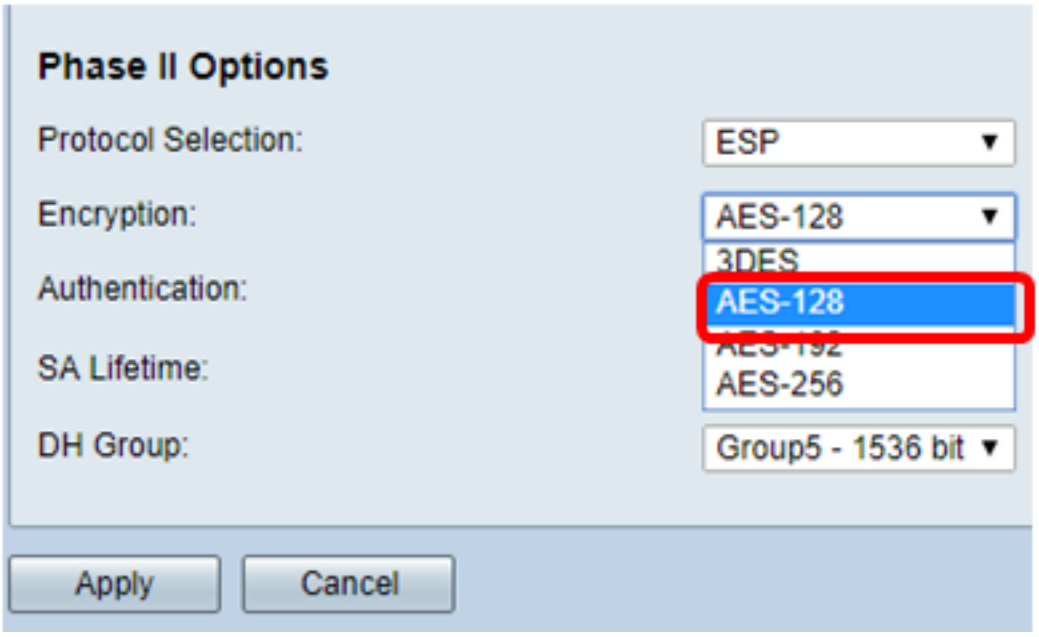
- ESP — Essa opção encapsula os dados a serem protegidos. Se esta opção for escolhida, vá para a Etapa 7 para escolher um método de criptografia.
- AH — Essa opção também é conhecida como Authentication Header (AH). É um protocolo de segurança que fornece autenticação de dados e serviço antirreprodução opcional. AH está incorporado no datagrama IP a ser protegido. Se esta opção for escolhida, vá para a Etapa 8.



Note: Neste exemplo, o ESP é escolhido.

Passo 7. Se o ESP tiver sido escolhido na Etapa 6, escolha um método de autenticação que determinará como o ESP e o ISAKMP são autenticados. As opções são:

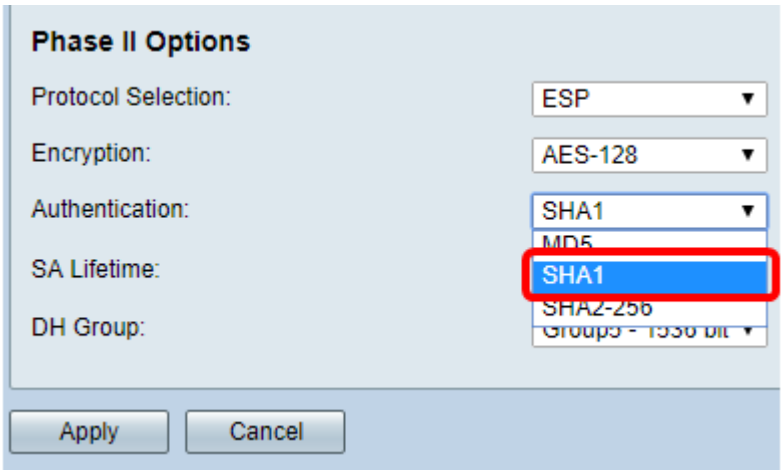
- 3DES — Triple Data Encryption Standard
- AES-128 — O Advanced Encryption Standard usa uma chave de 128 bits.
- AES-192 — O Advanced Encryption Standard usa uma chave de 192 bits.
- AES-256 — O Advanced Encryption Standard usa uma chave de 256 bits.



Note: Neste exemplo, AES-128 é escolhido.

Etapa 8. 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.

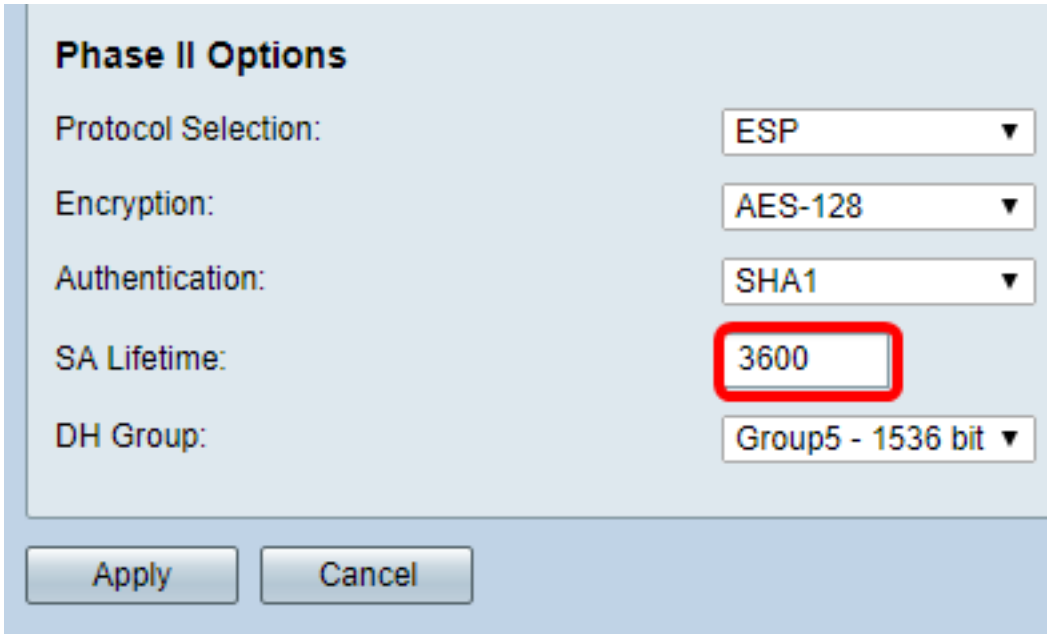


Note: Neste exemplo, SHA1 é escolhido.

Etapa 9. 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.

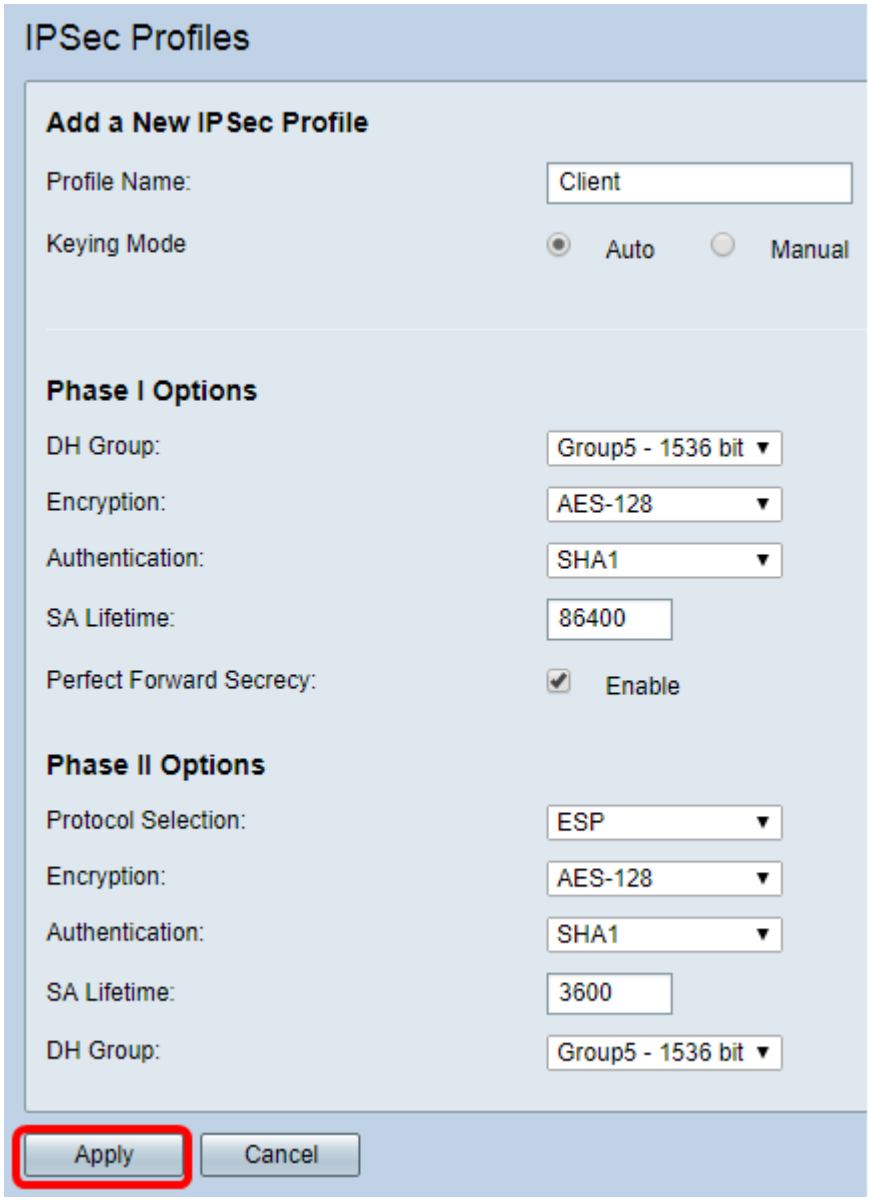
Etapa 10. Na lista suspensa Grupo DH, escolha um grupo DH a ser usado com a chave na Fase 2. As opções são:

- Grupo2-1024 bits — Essa opção calcula a chave mais lentamente, mas é mais segura que o Grupo1.
- Grupo5-1536 bits — Essa opção computa a chave mais lentamente, mas é a mais segura.

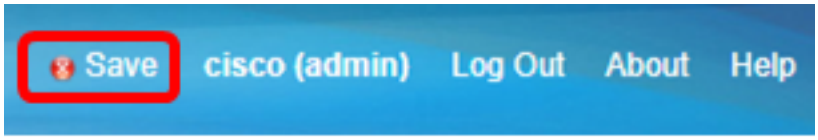


Note: Neste exemplo, 3600 é inserido.

Etapa 11. Clique em Apply.



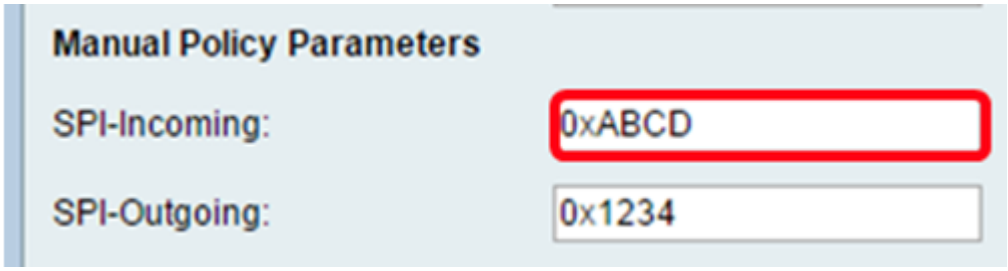
Etapa 12. Clique em **Salvar** para salvar a configuração permanentemente.



Agora você deve ter configurado com êxito um perfil de IPSec automático em seu RV34x Series Router.

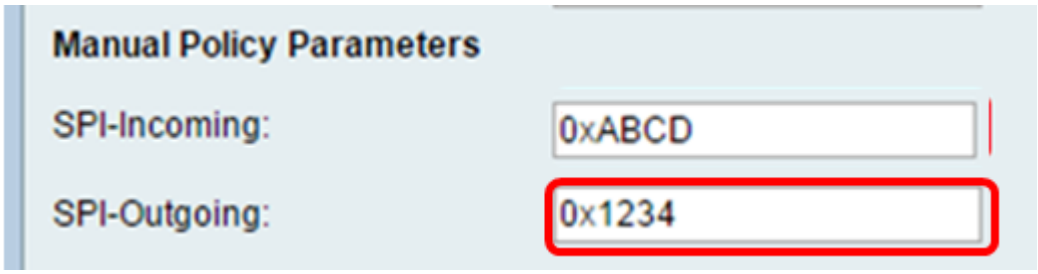
Defina as configurações manuais

Etapa 1. No campo *SPI-Entrada*, insira um valor hexadecimal de 100 a FFFFFF para a tag Security Parameter Index (SPI) para o tráfego de entrada na conexão VPN. A marca SPI é usada para distinguir o tráfego de uma sessão do tráfego de outras sessões.



Note: Neste exemplo, 0xABCD é inserido.

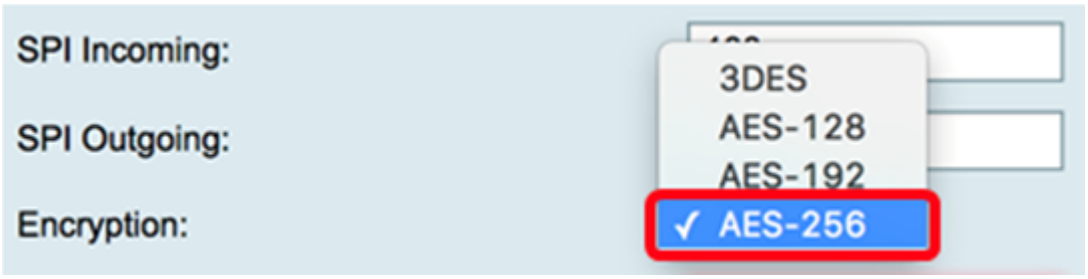
Etapa 2. No campo *SPI-Saída*, insira um valor hexadecimal de 100 a FFFFFF para a marca SPI para tráfego de saída na conexão VPN.



Note: Neste exemplo, 0x1234 é inserido.

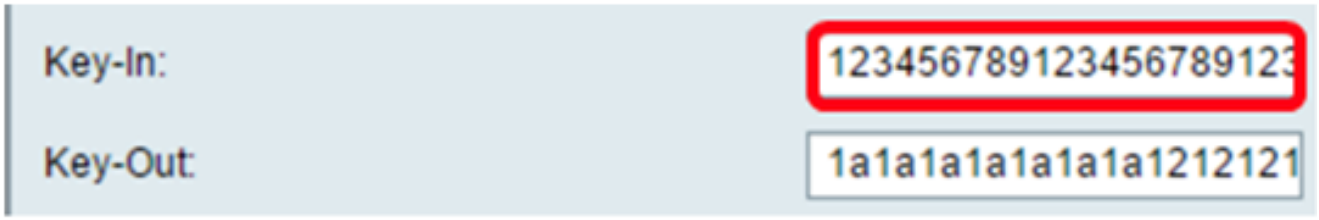
Etapa 3. Escolha um valor de criptografia na lista suspensa. As opções são:

- 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.



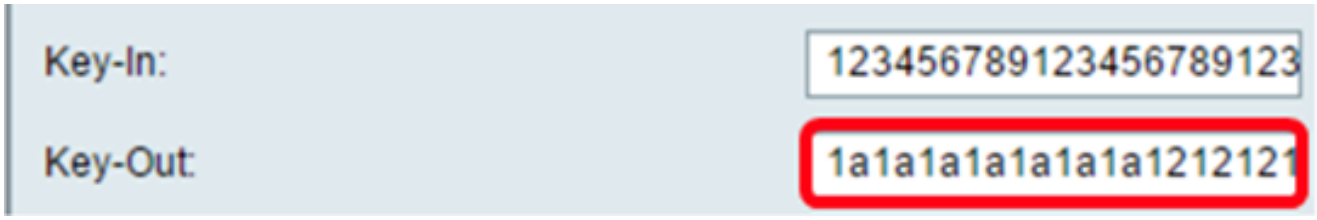
Note: Neste exemplo, AES-256 é escolhido.

Etapa 4. No campo *Key-In*, insira uma chave para a política de entrada. O comprimento da chave dependerá do algoritmo escolhido na Etapa 3.



Note: Neste exemplo, 123456789123456789123... é inserido.

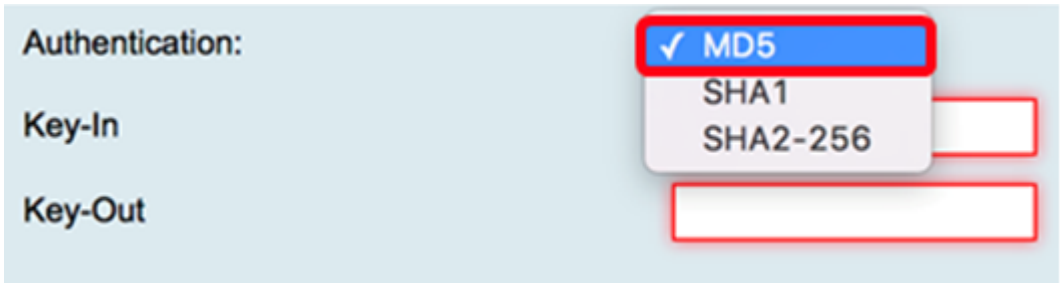
Etapa 5. No campo *Key-Out*, insira uma chave para a política de saída. O comprimento da chave dependerá do algoritmo escolhido na Etapa 3.



Note: Neste exemplo, 1a1a1a1a1a1a1a12121212... é inserido.

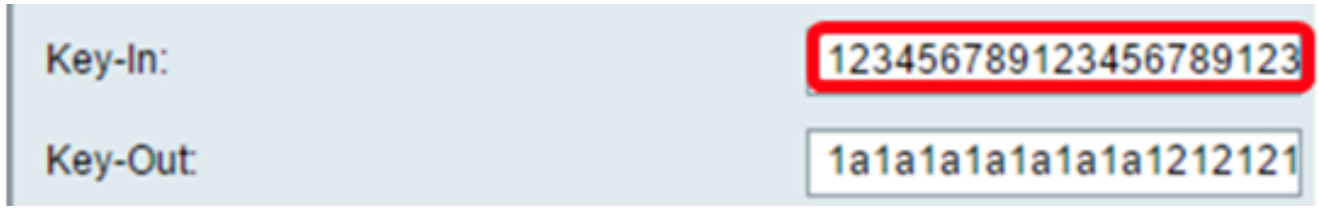
Etapa 6. Escolha um método de autenticação na lista suspensa Autenticação. As opções são:

- 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.



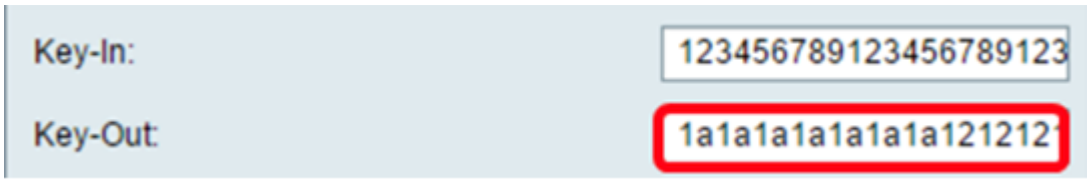
Note: Neste exemplo, MD5 é escolhido.

Passo 7. No campo *Key-In*, insira uma chave para a política de entrada. O comprimento da chave dependerá do algoritmo escolhido na Etapa 6.

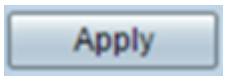


Note: Neste exemplo, 123456789123456789123... é inserido.

Etapa 8. No campo *Key-Out*, insira uma chave para a política de saída. O comprimento da chave dependerá do algoritmo escolhido na Etapa 6.

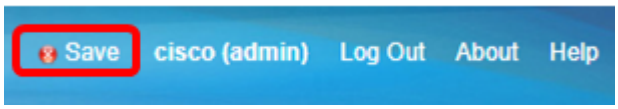


Note: Neste exemplo, 1a1a1a1a1a1a1a12121212... é inserido.

Etapa 9. Clique em 

.

Etapa 10. Clique em **Salvar** para salvar a configuração permanentemente.

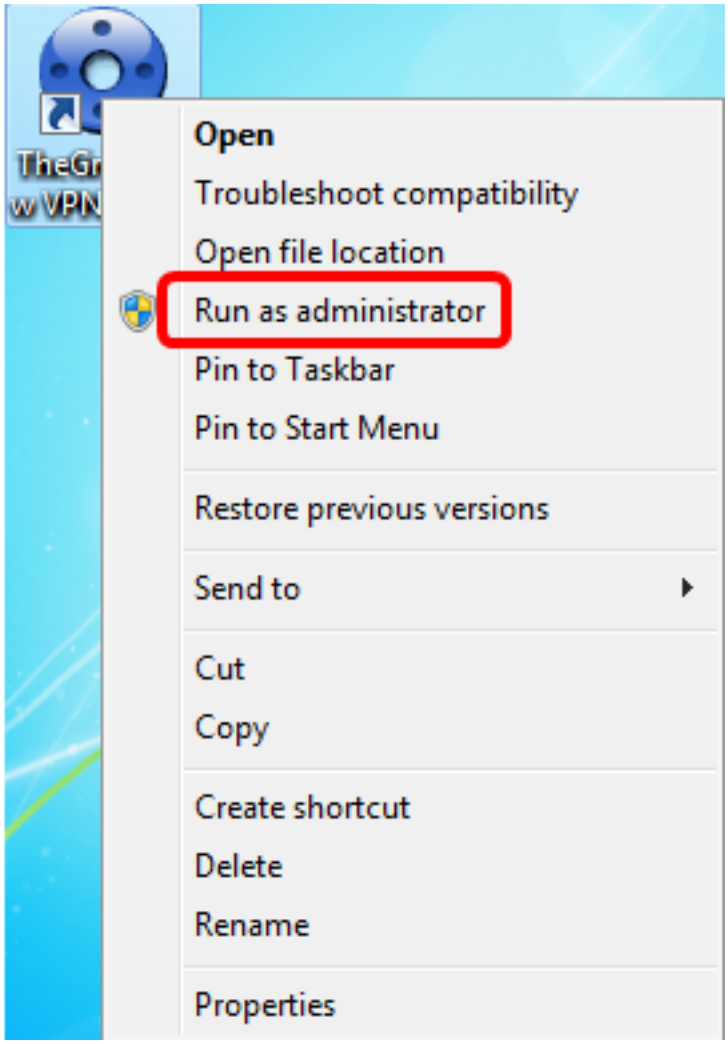


Agora você deve ter configurado com êxito um perfil de IPSec manual em um roteador RV34x Series.

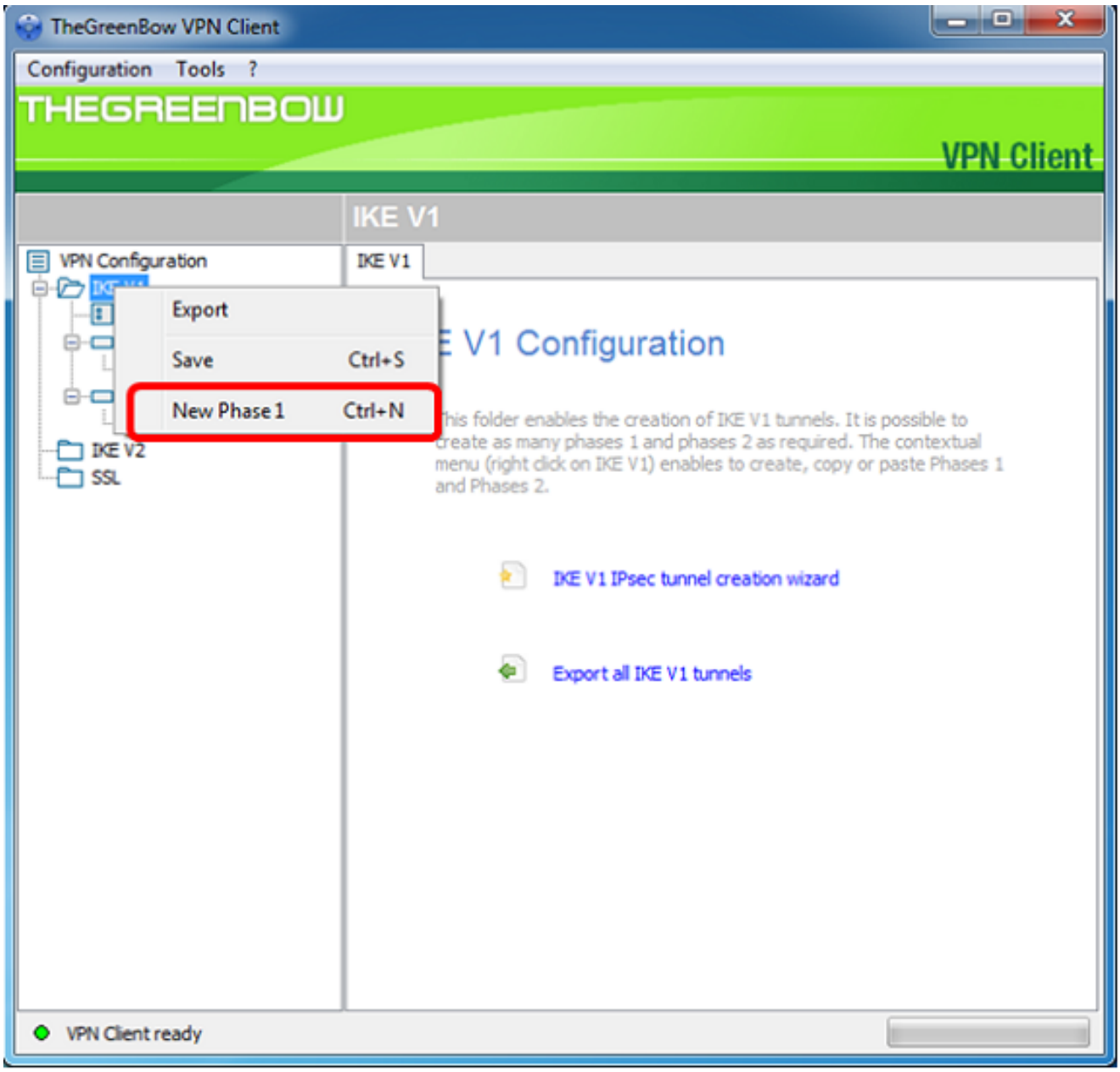
Configurar o software cliente GreenBow VPN

Definir configurações da Fase 1

Etapa 1. Clique com o botão direito do mouse no ícone GreenBow VPN Client e escolha **Executar como administrador**.

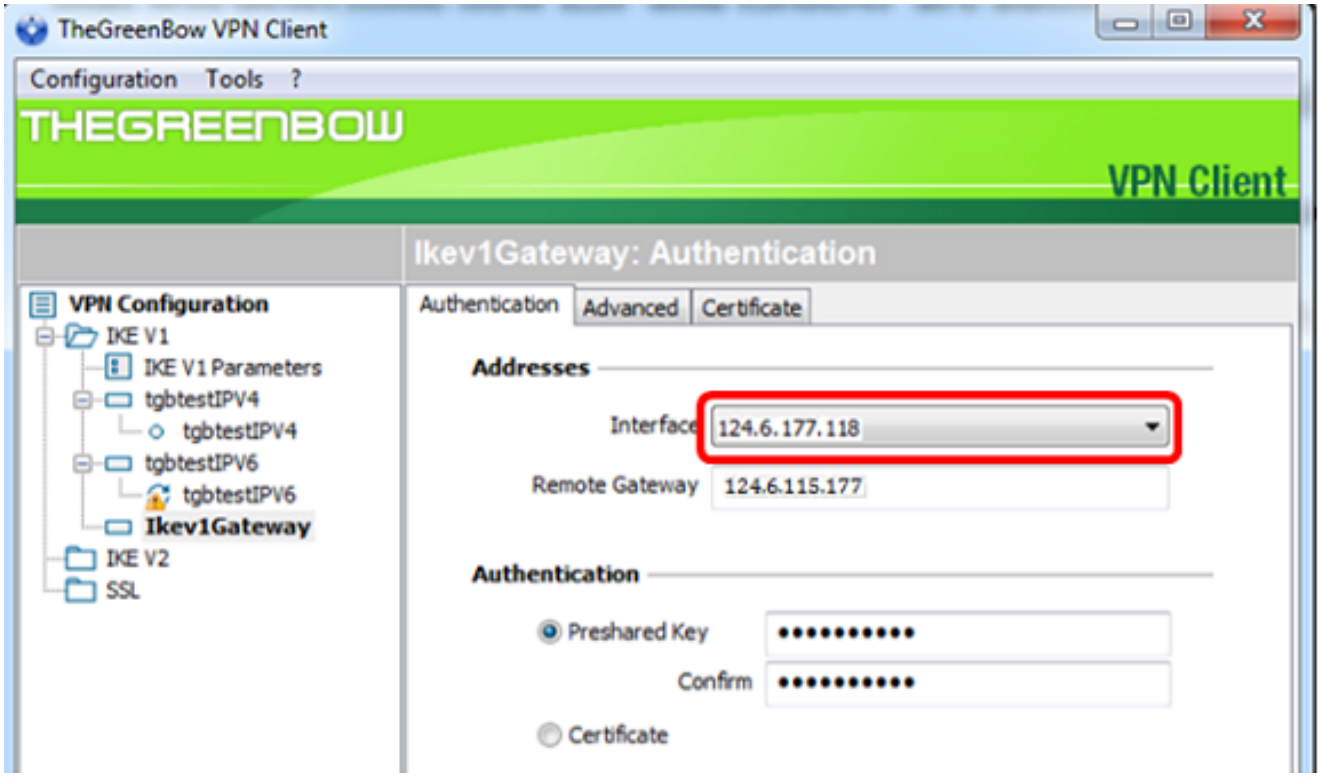


Etapa 2. No painel esquerdo em Configuração de VPN, clique com o botão direito do mouse em **IKE V1** e escolha **Nova Fase 1**.



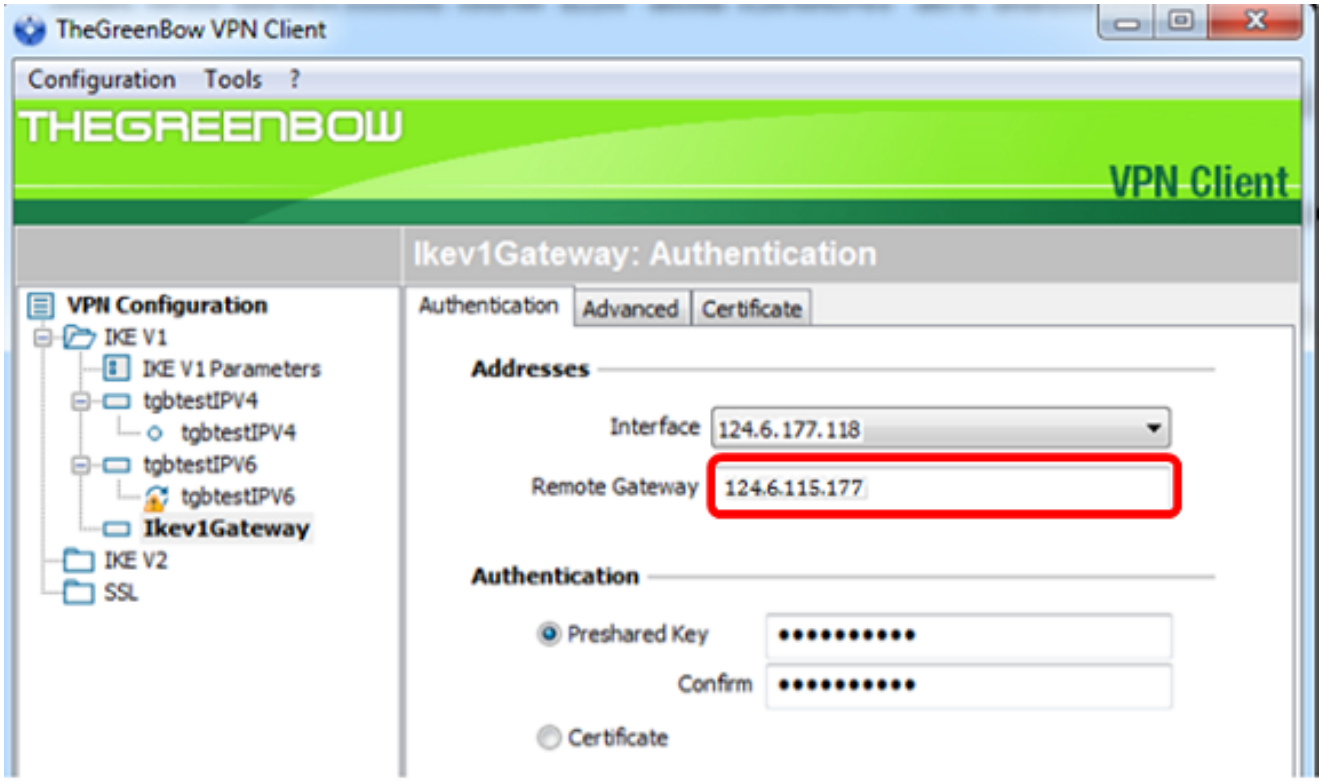
Etapa 3. Na guia Authentication (Autenticação) em Addresses (Endereços), verifique se o endereço IP na área Interface é igual ao endereço IP da WAN do computador onde o GreenBow VPN Client está instalado.

Note: Neste exemplo, o endereço IP é 124.6.177.118.



Etapa 4. Insira o endereço do gateway remoto no campo *Gateway remoto*.

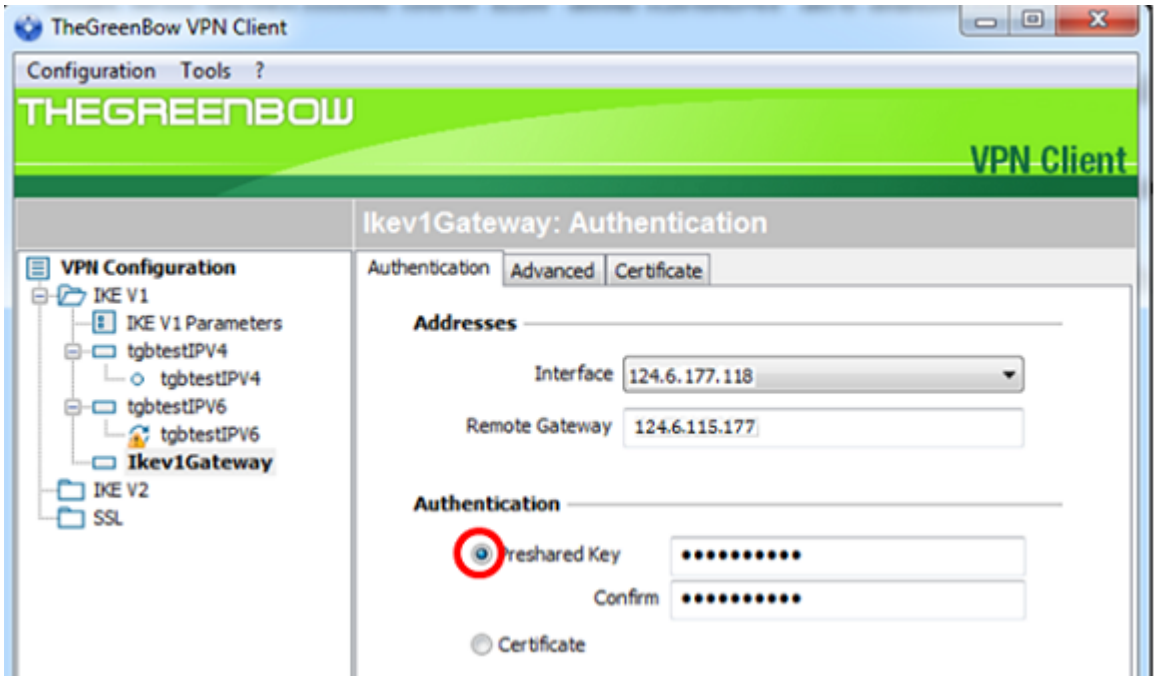
Note: Neste exemplo, o endereço IP do roteador RV34x remoto é 124.6.115.177.



Etapa 5. Em Authentication (Autenticação), escolha o tipo de autenticação. As opções são:

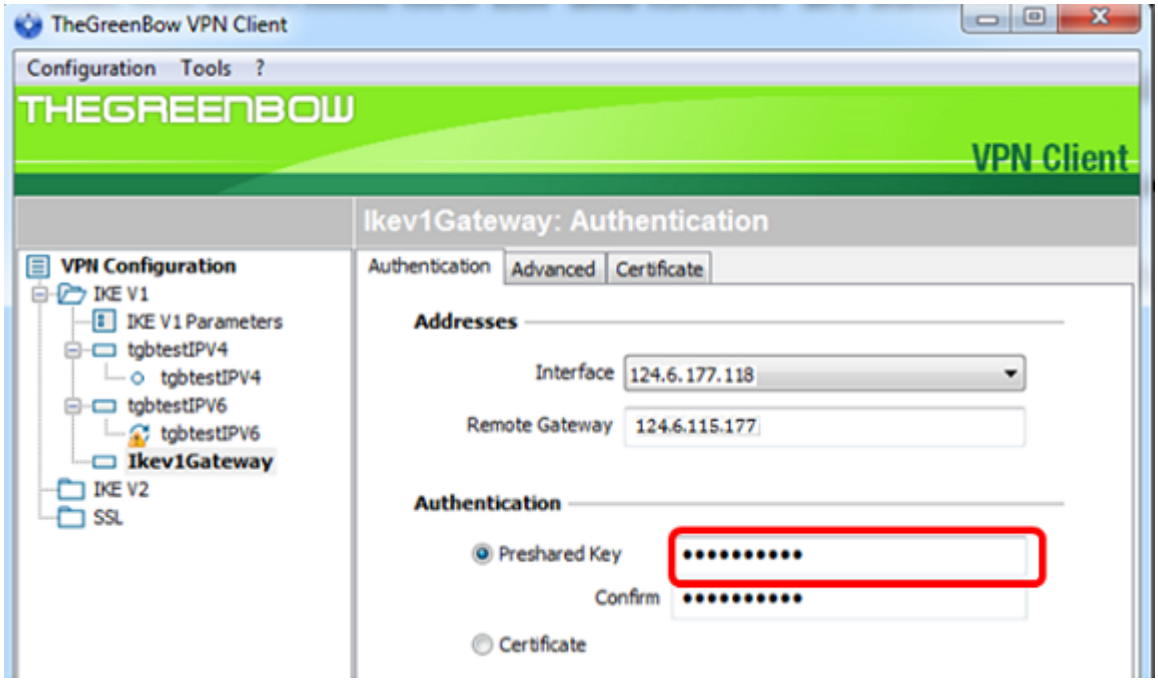
- Presshared Key — (Chave pré-compartilhada) Essa opção permitirá que o usuário use uma senha configurada no gateway VPN. A senha deve ser combinada pelo usuário para poder estabelecer um túnel VPN.
- Certificado — Esta opção utilizará um certificado para concluir o handshake entre o VPN

Client e o VPN Gateway.

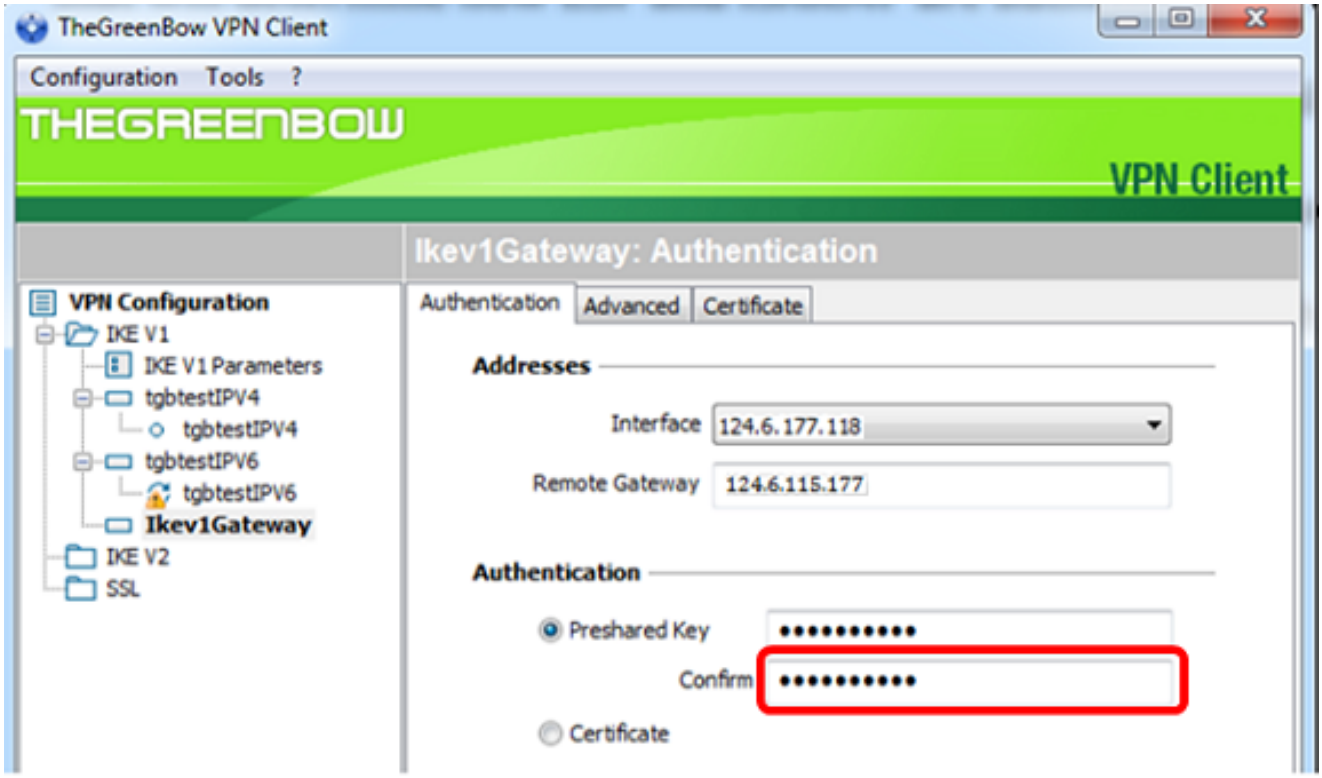


Note: Neste exemplo, a chave pré-compartilhada é escolhida para corresponder à configuração do RV34x VPN Gateway.

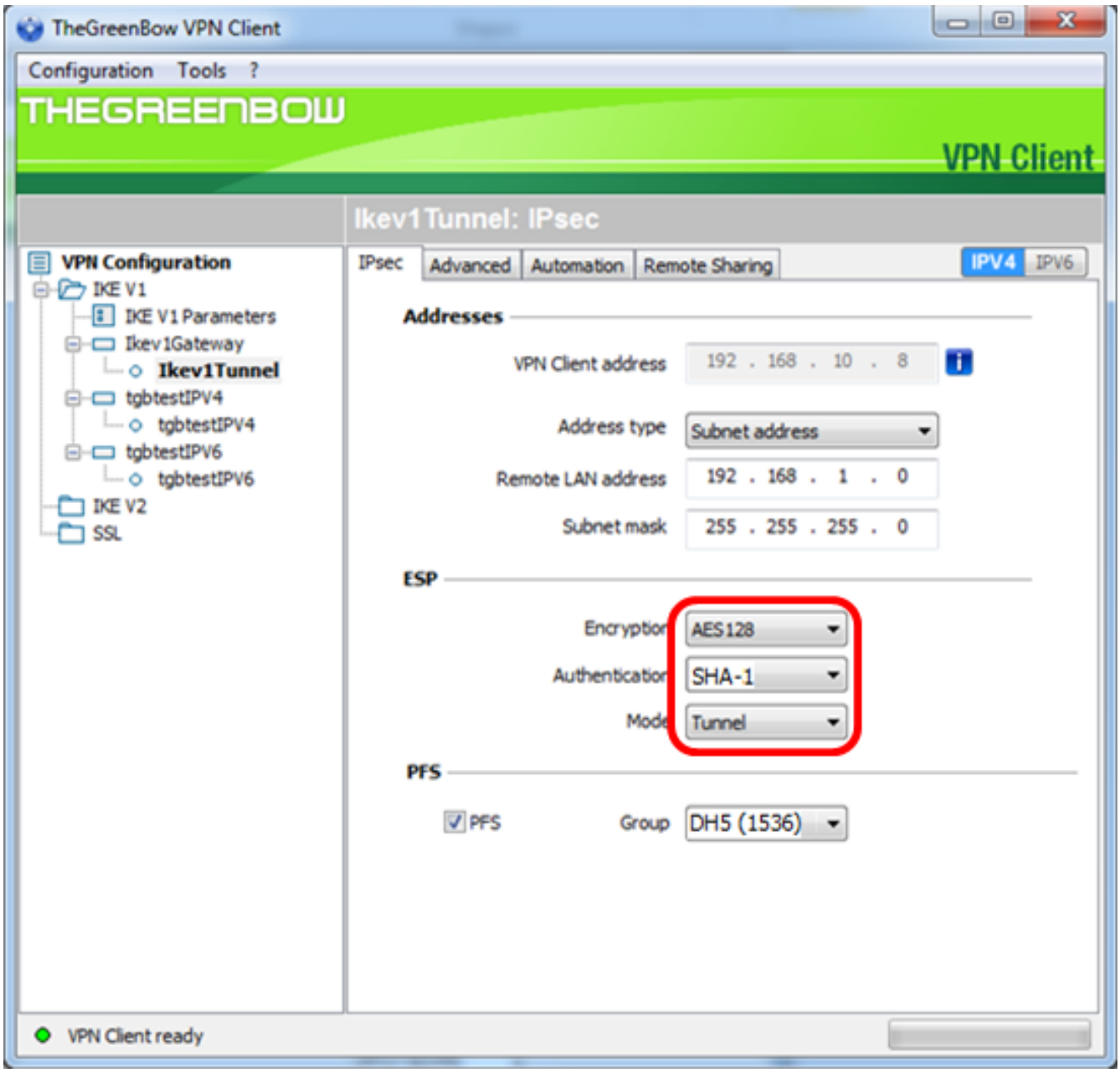
Etapa 6. Insira a chave pré-compartilhada configurada no roteador.



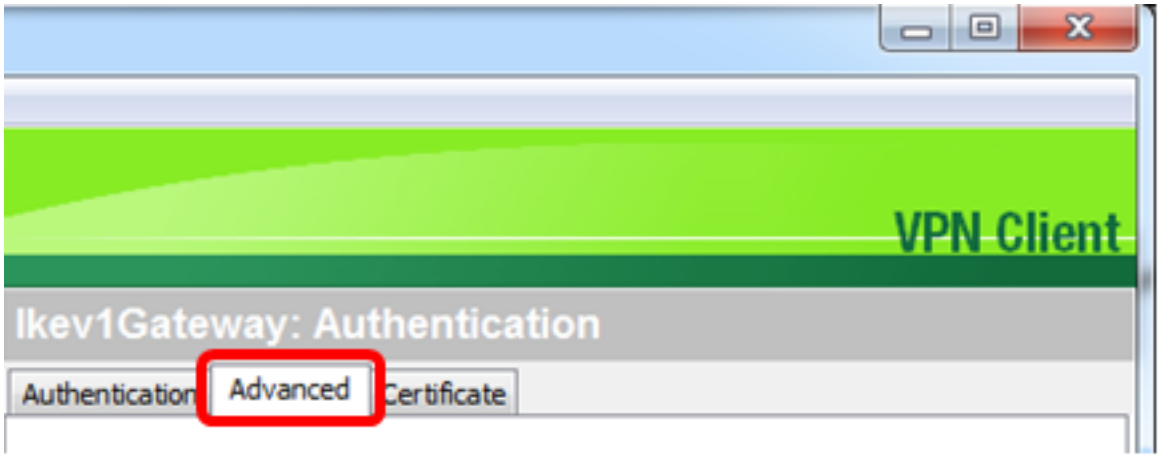
Passo 7. Digite a mesma chave pré-compartilhada no campo *Confirmar*.



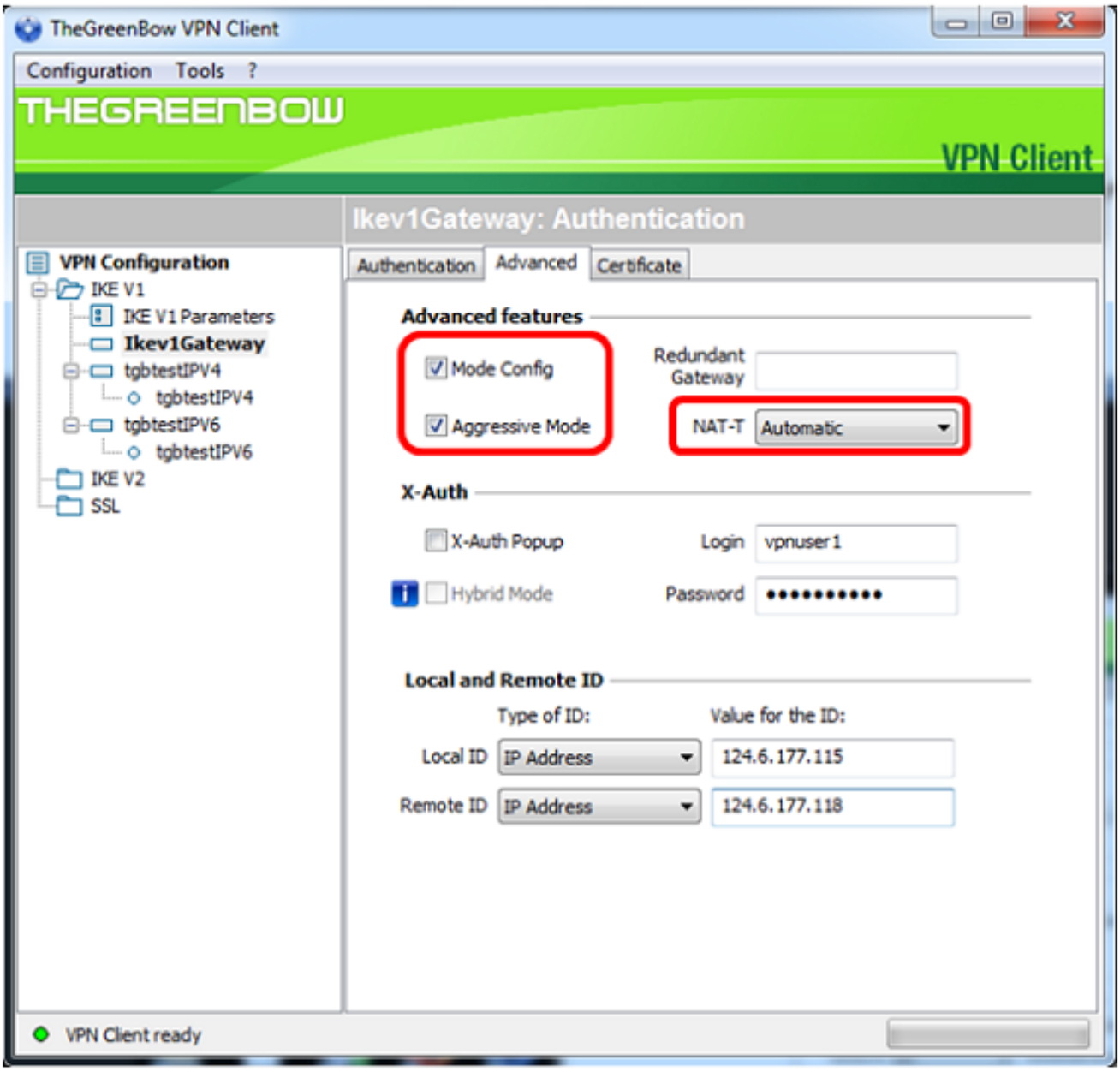
Etapa 8. Em IKE, defina as configurações de Criptografia, Autenticação e Grupo de Chave para corresponder à configuração do roteador.



Etapa 9. Clique na guia Advanced.

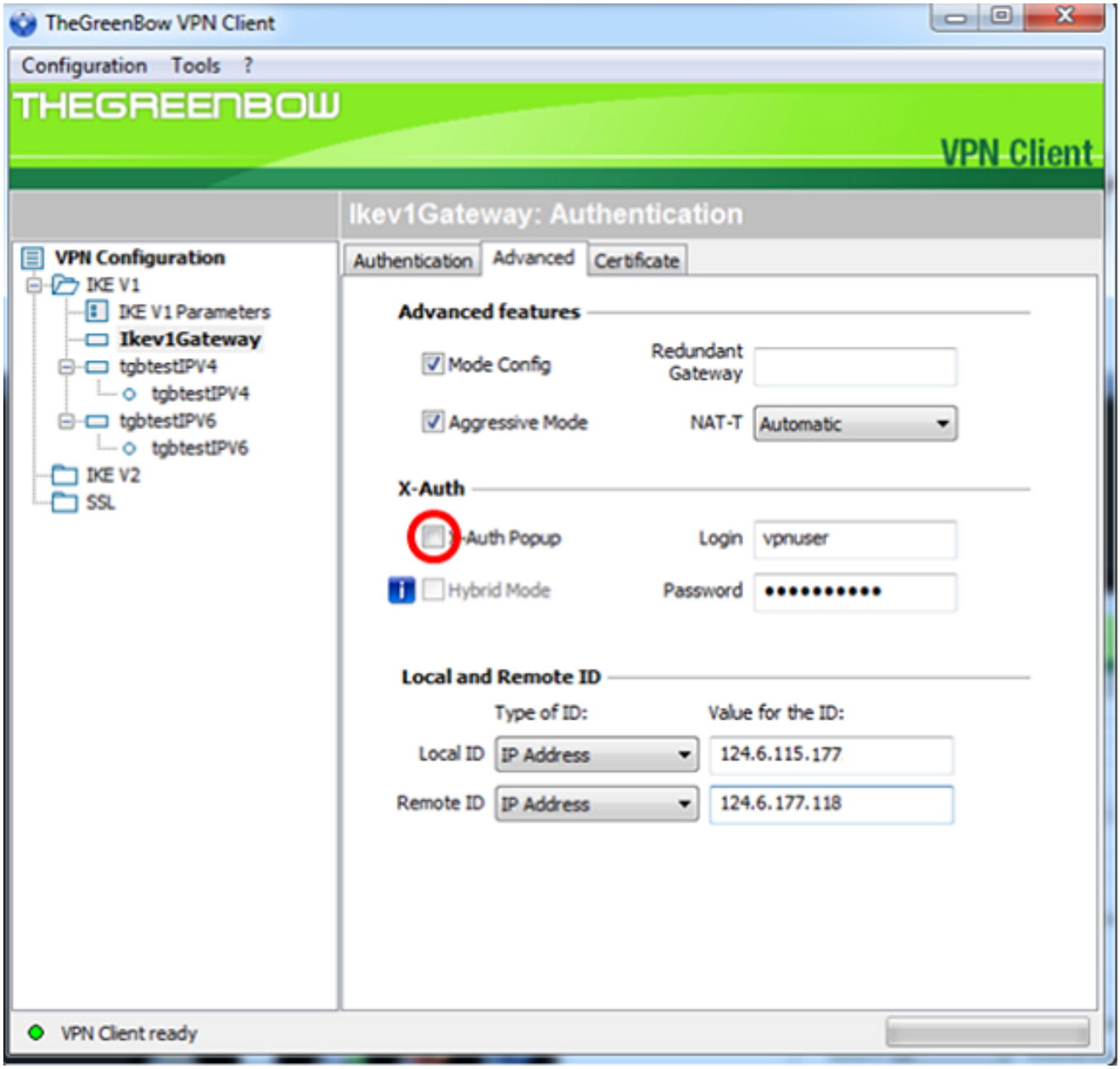


Etapa 10. (Opcional) Em Recursos avançados, marque as caixas de seleção **Mode Config** e **Aggressive Mode** e defina a configuração NAT-T como Automatic (Automático).



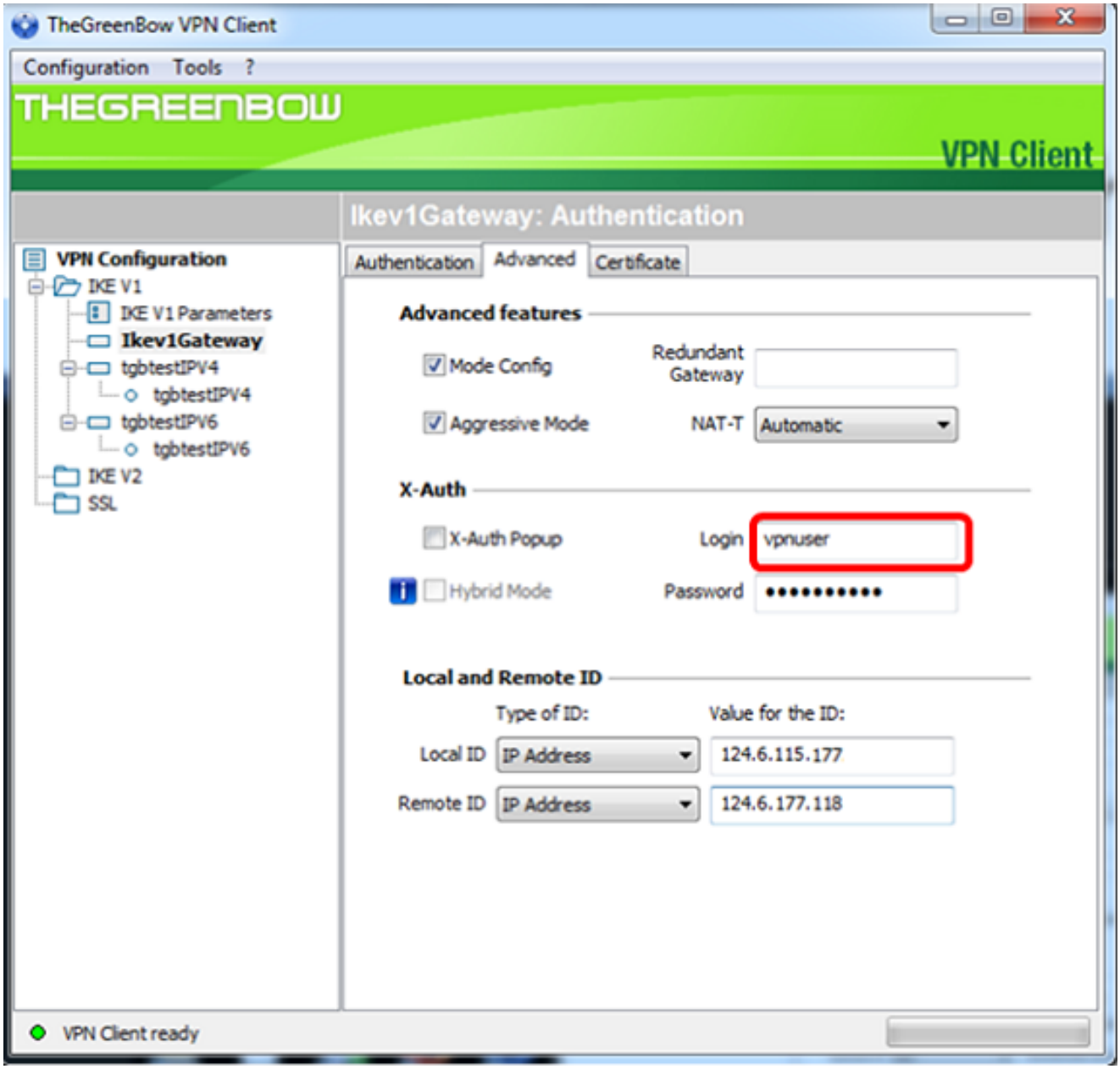
Note: Com o modo Config ativado, o GreenBow VPN Client irá extrair as configurações do gateway VPN para tentar estabelecer um túnel enquanto habilita o modo agressivo e o NAT-T torna o estabelecimento de uma conexão mais rápido.

Etapa 11. (Opcional) Em X-Auth, marque 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.

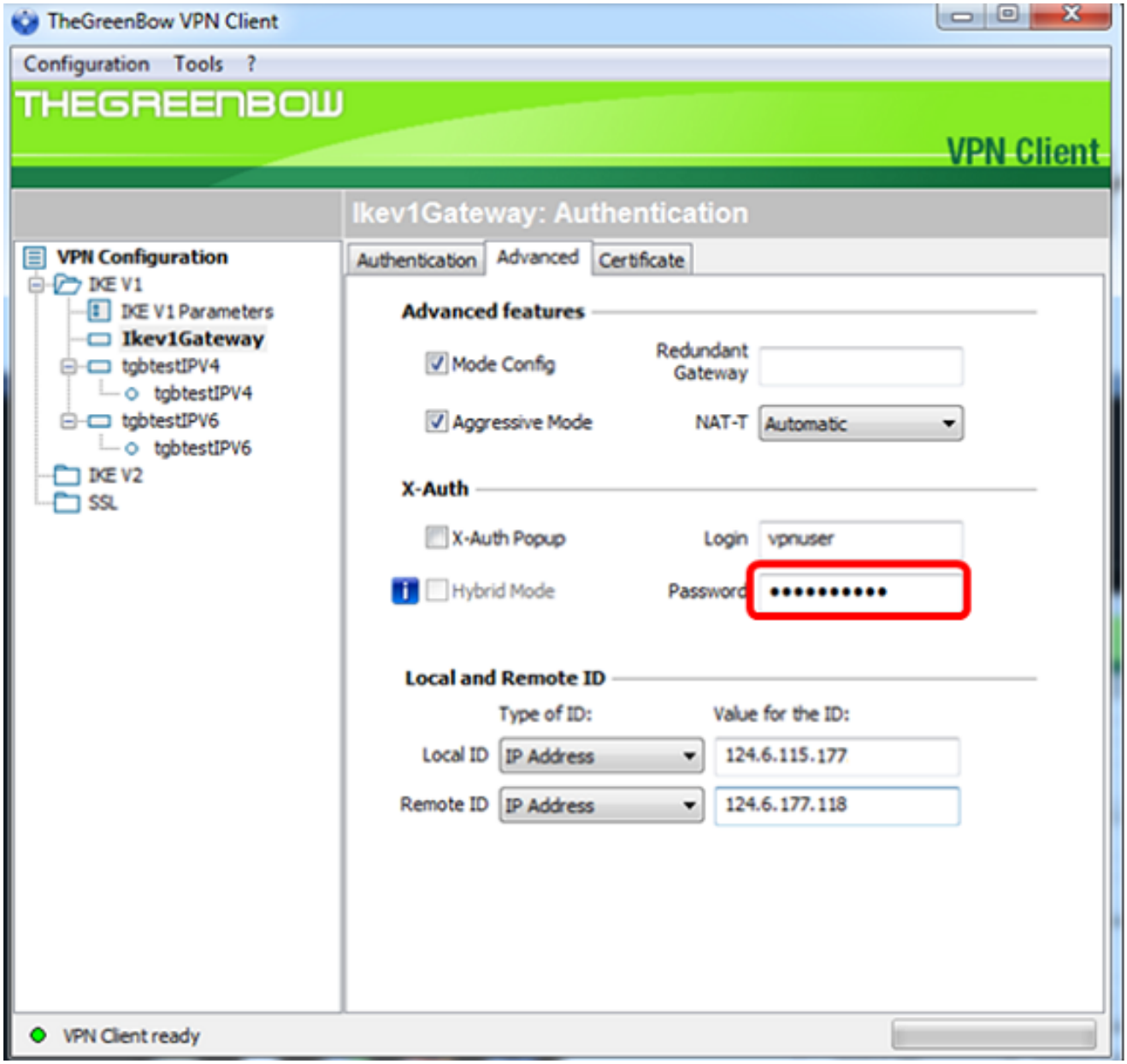


Note: Neste exemplo, o Pop-up X-Auth não está marcado.

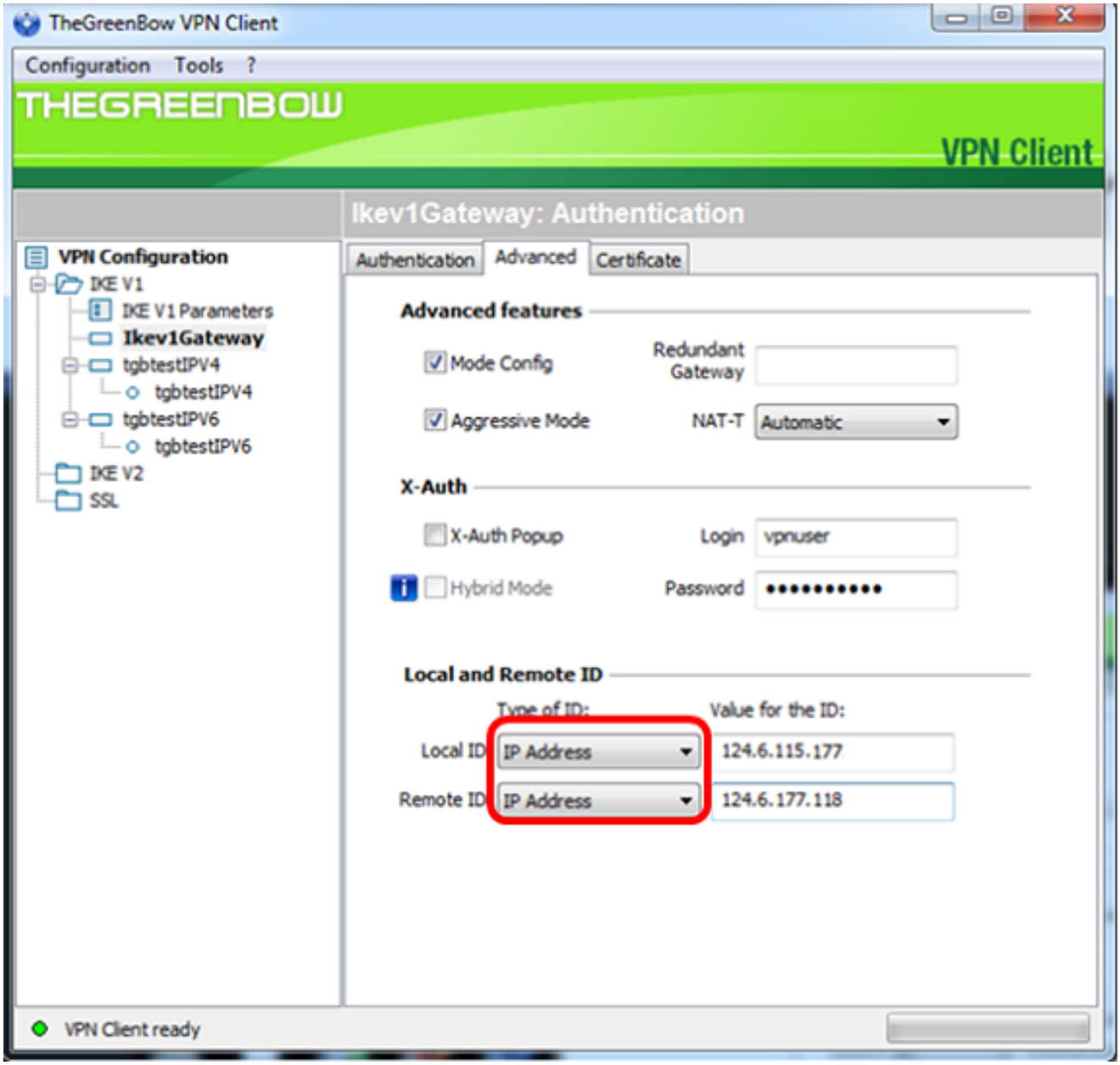
Etapa 12. Digite seu nome de usuário no campo *Login*. Este é o nome de usuário configurado para criar um grupo de usuários no gateway VPN.



Etapa 13. Digite sua senha no campo Senha.

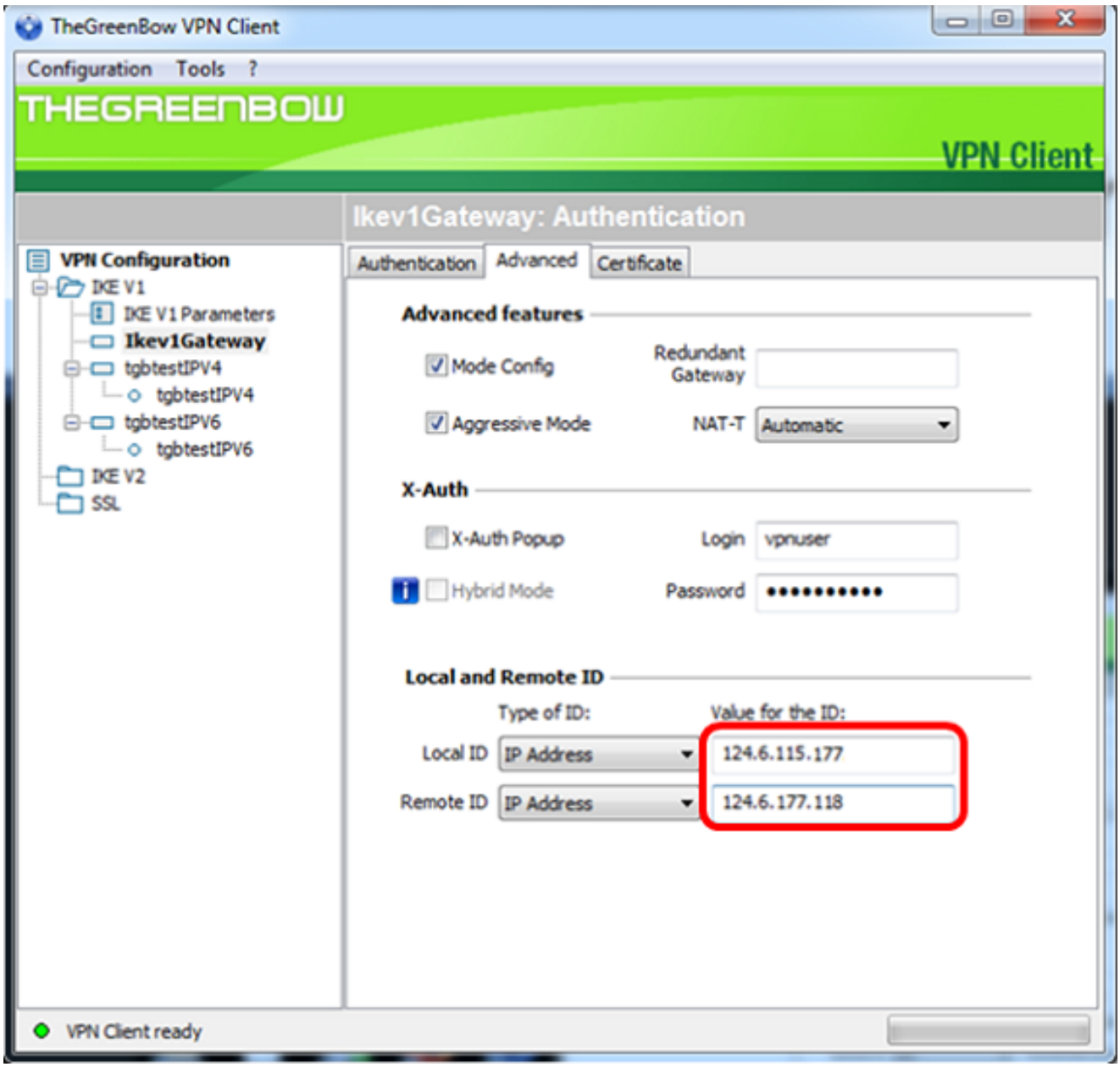


Etapa 14. Em Local and Remote ID (ID local e remota), defina o Local ID e o Remote ID para corresponder às configurações do gateway VPN.

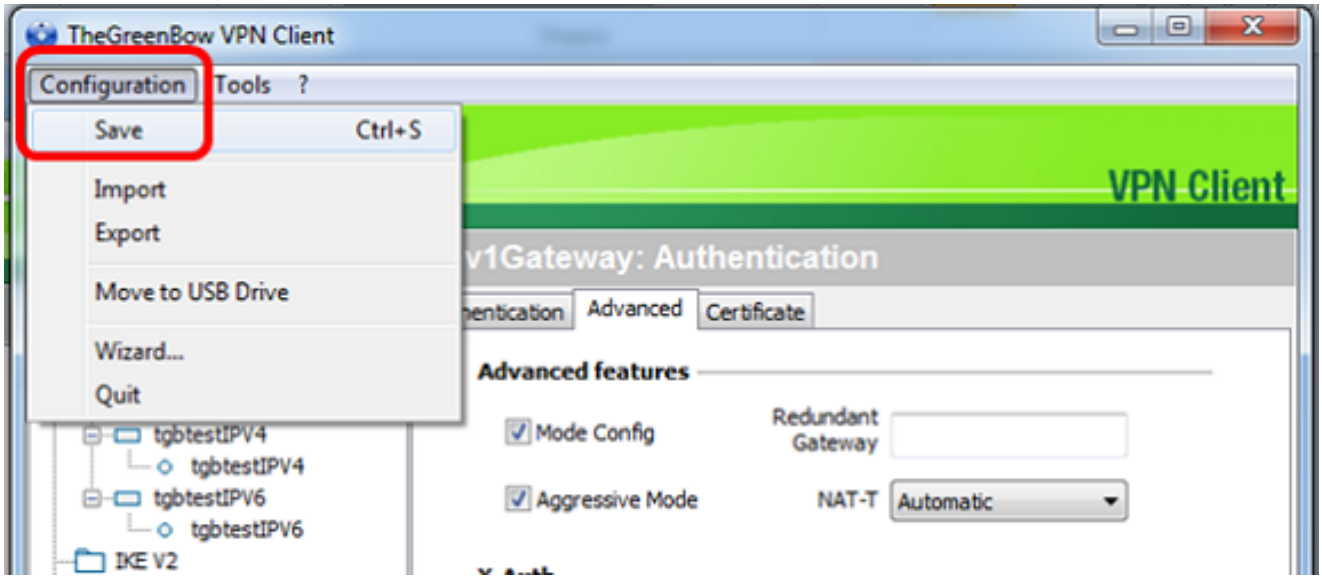


Note: Neste exemplo, a ID local e a ID remota estão definidas como Endereço IP para corresponder às configurações do gateway VPN RV34x.

Etapa 15. Em Valor para o ID, insira o ID local e o ID remoto em seus respectivos campos.

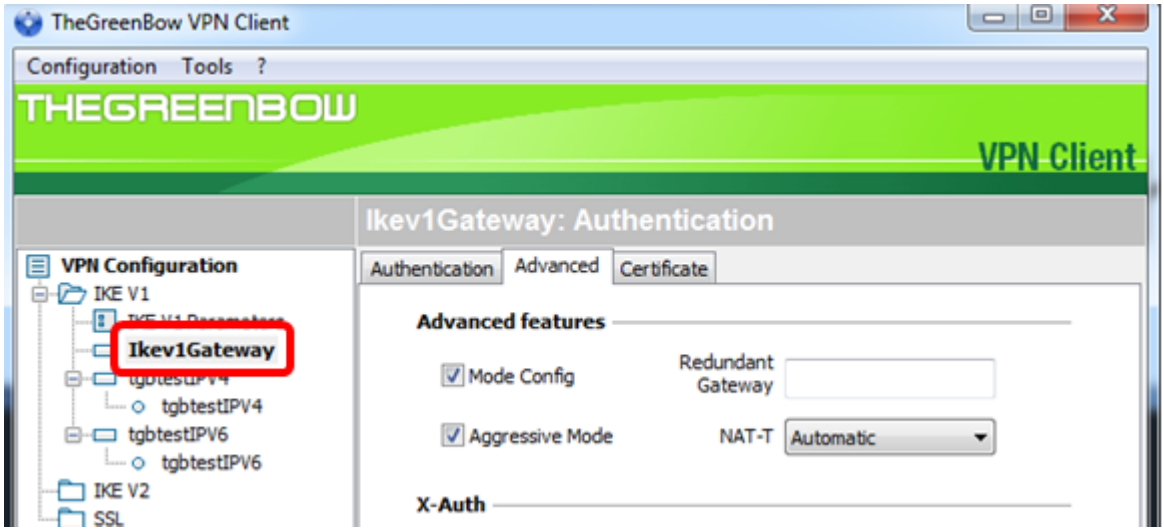


Etapa 16. Clique em **Configuration > Save** para salvar as configurações.

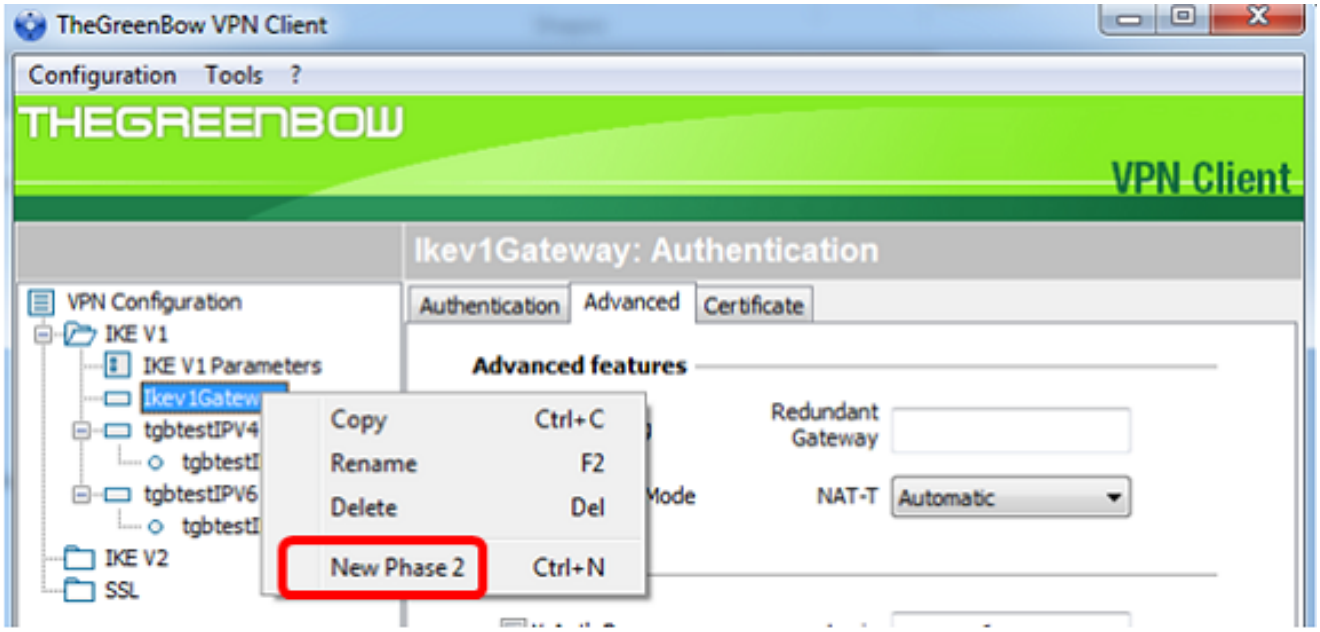


Definir configurações da fase 2

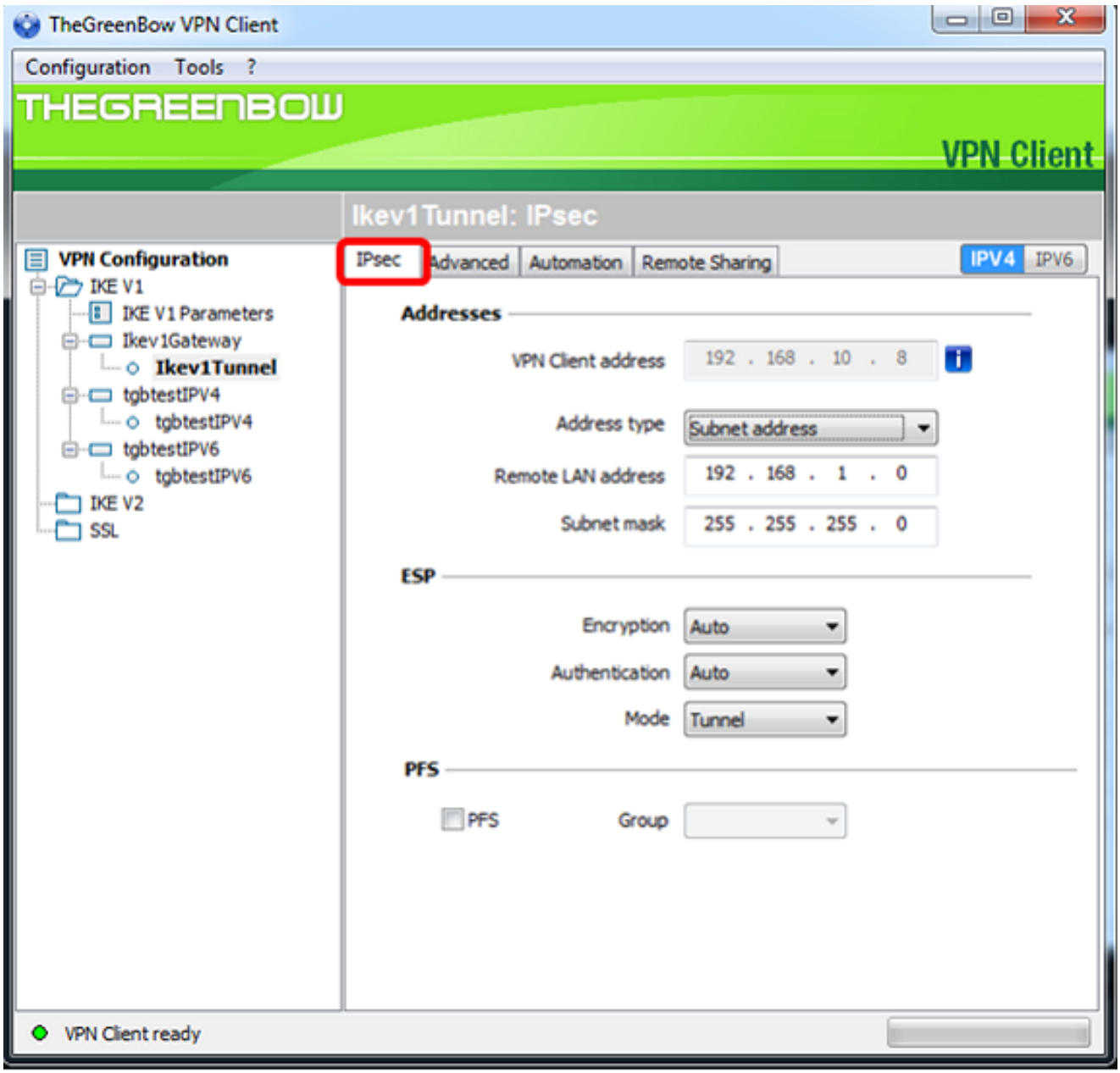
Etapa 1. Clique com o botão direito do mouse em **Ikev1** Gateway.



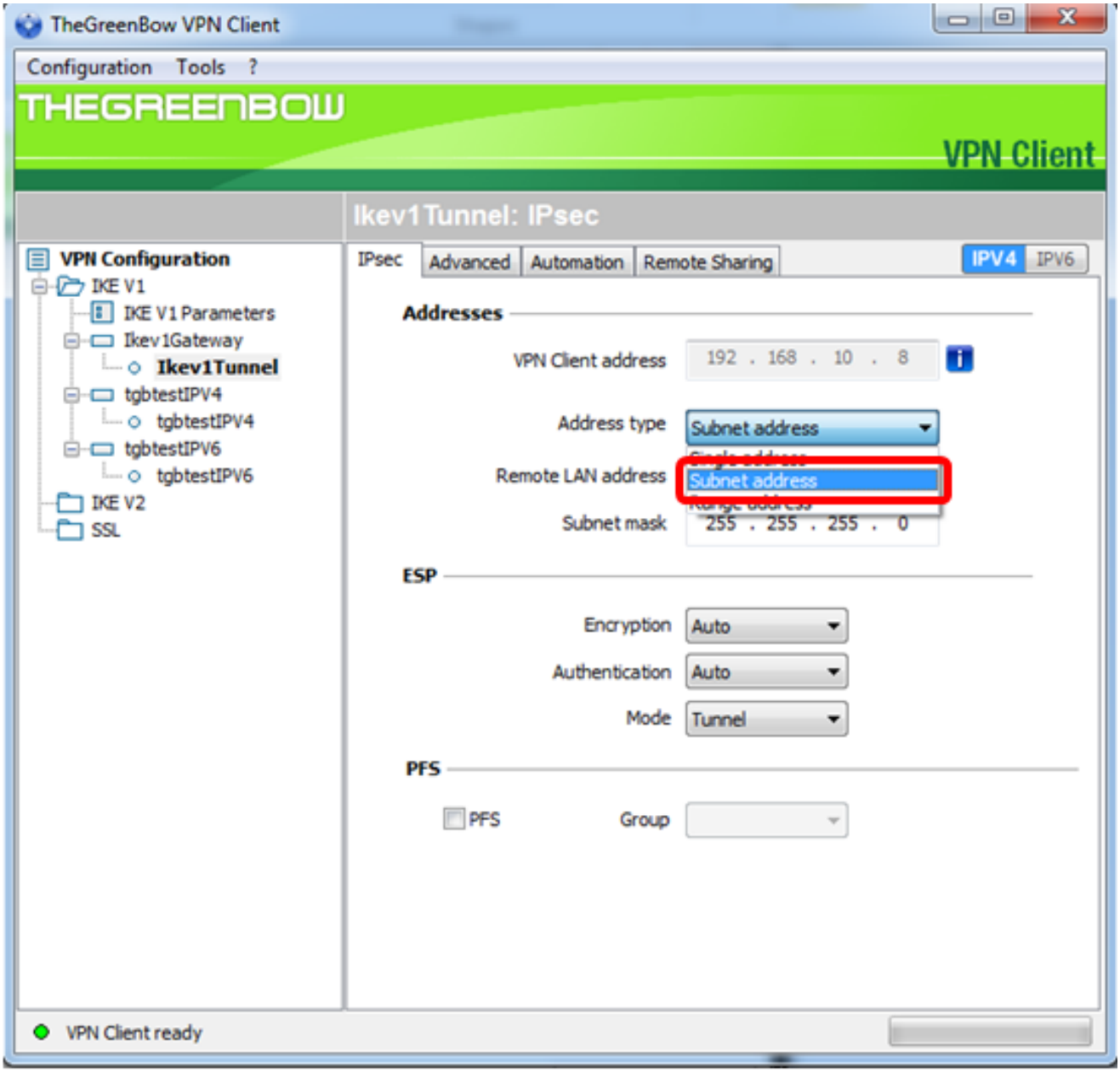
Etapa 2. Escolha **Nova Fase 2**.



Etapa 3. Clique na guia **IPsec**.

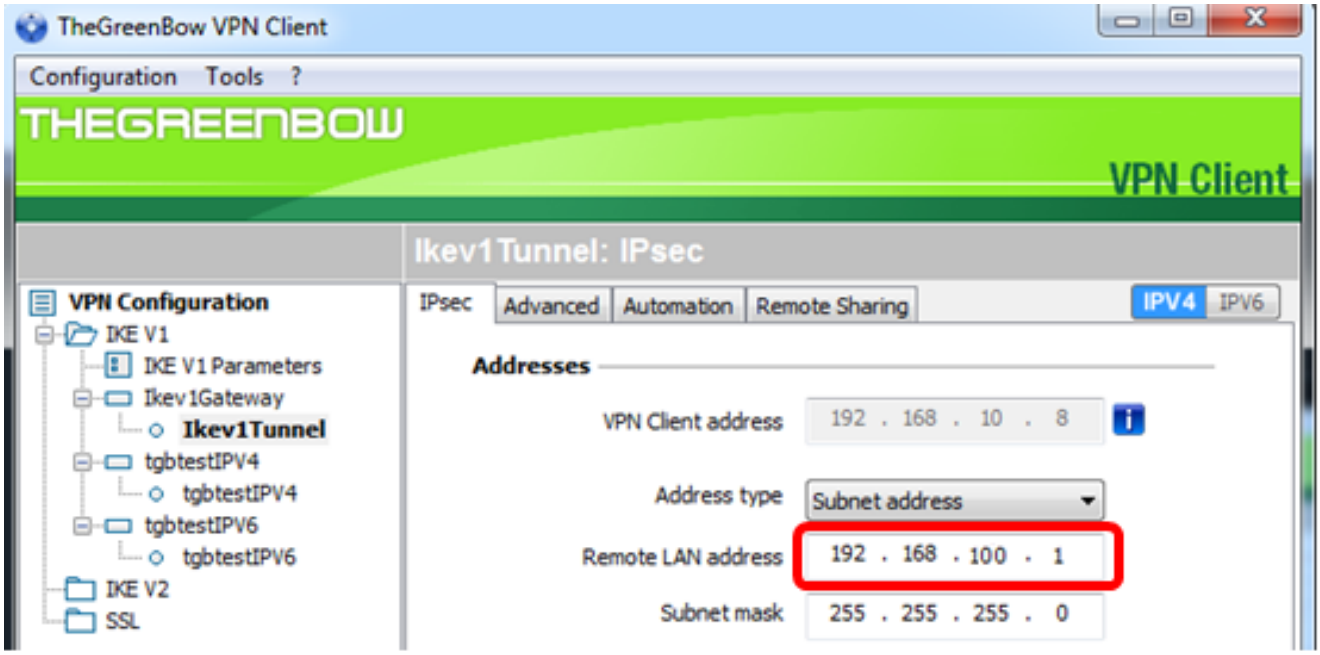


Etapa 4. Escolha o tipo de endereço que o cliente VPN pode acessar na lista suspensa Tipo de endereço.



Note: Neste exemplo, o endereço de sub-rede é escolhido.

Etapa 5. Digite o endereço de rede que deve ser acessado pelo túnel VPN no campo *Endereço LAN Remoto*.

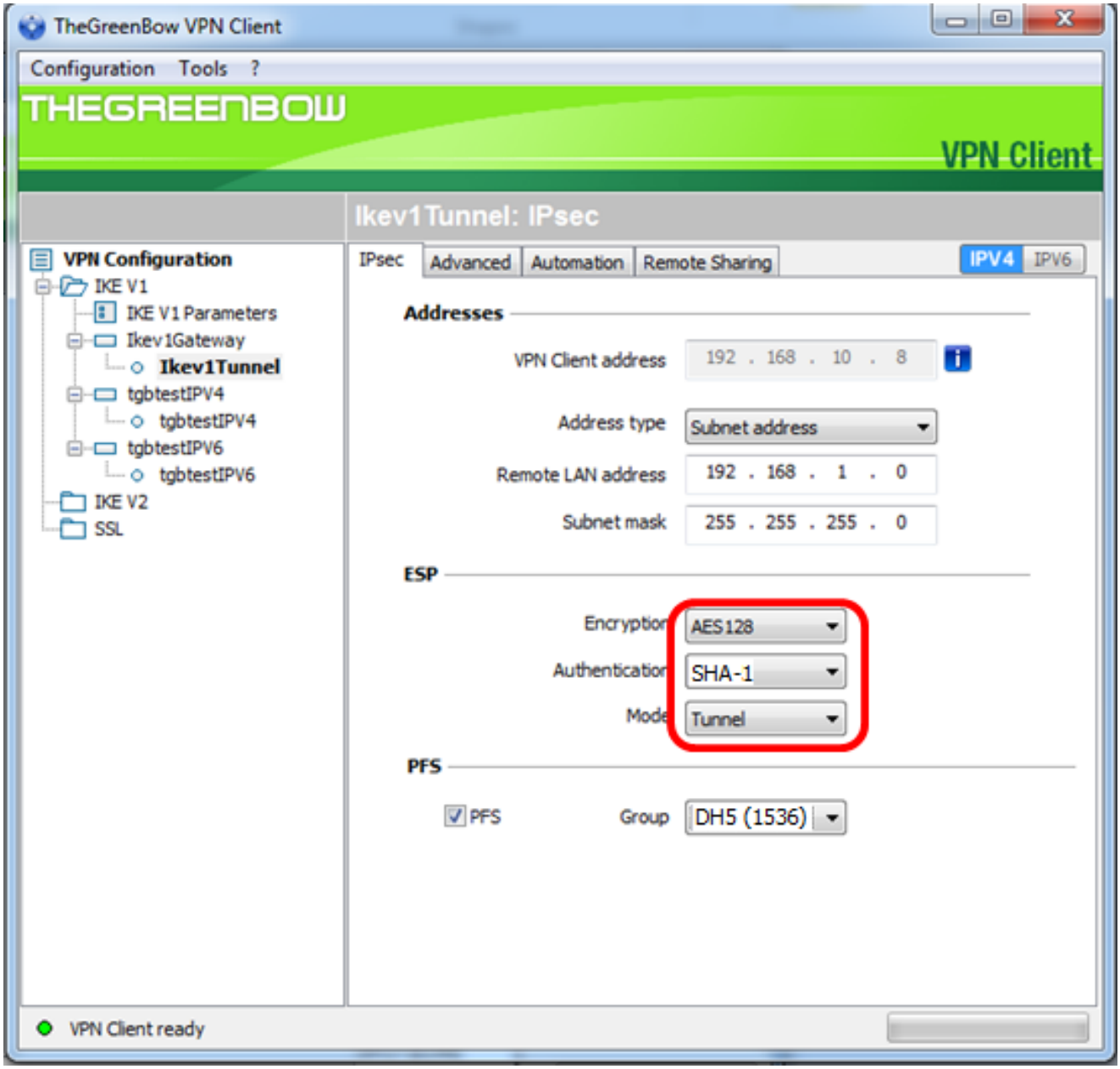


Note: Neste exemplo, 192.168.100.1 é inserido.

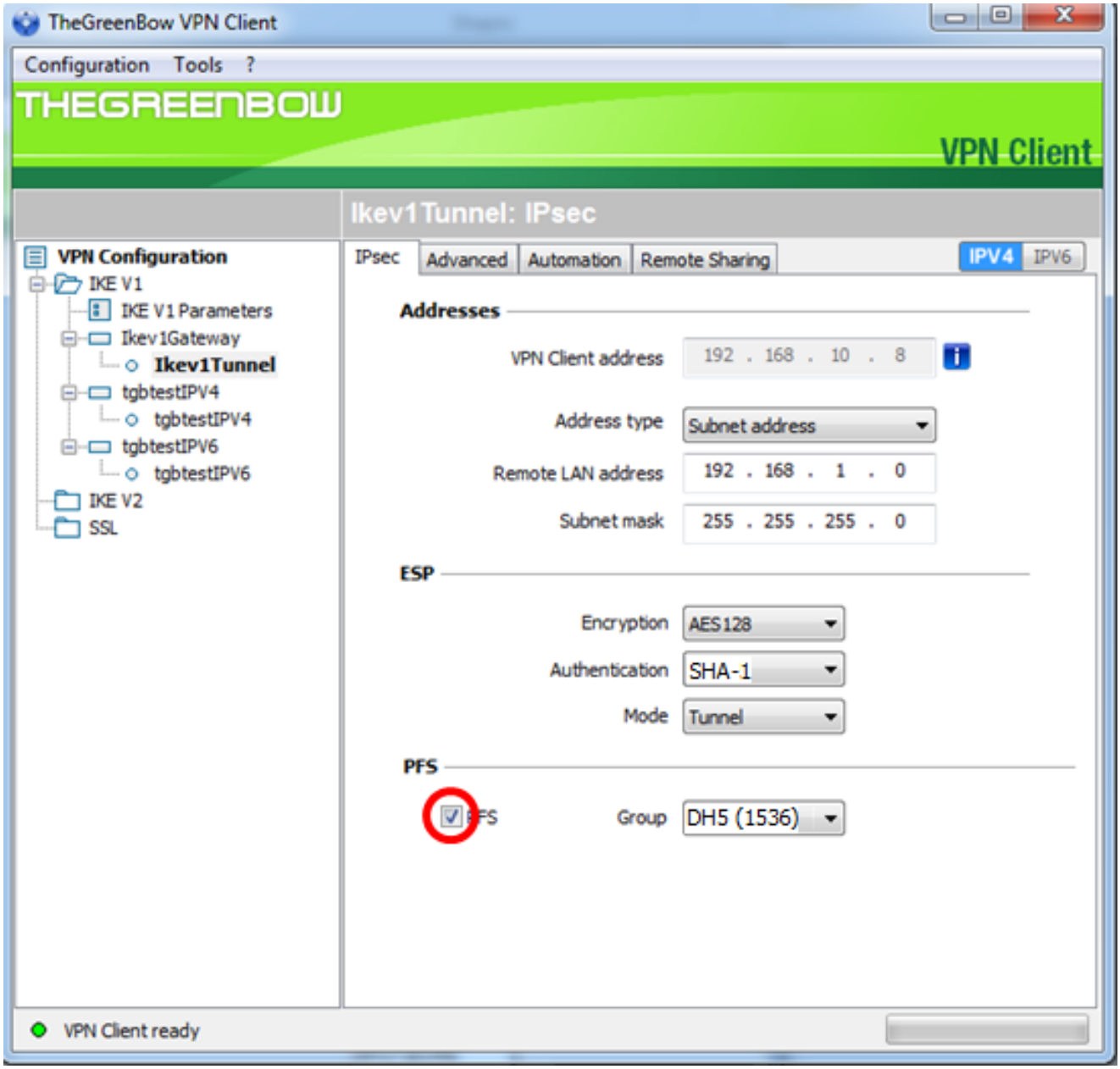
Etapa 6. Insira a máscara de sub-rede da rede remota no campo *Máscara de sub-rede*.

Note: Neste exemplo, 255.255.255.0 é inserido.

Passo 7. Em ESP, defina Encryption, Authentication e Mode para corresponder às configurações do gateway VPN.

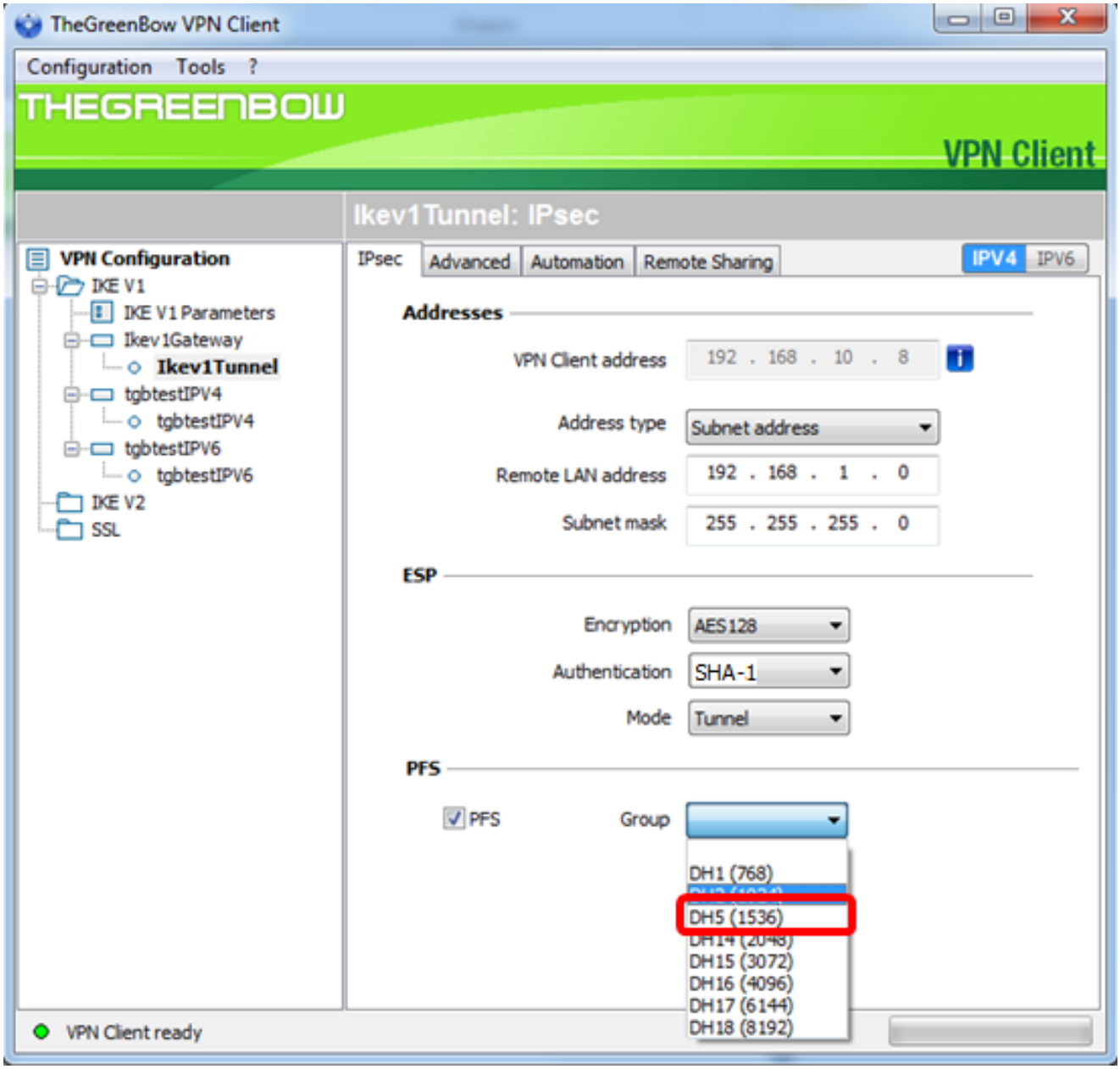


Etapa 8. (Opcional) Em PFS, marque a caixa de seleção **PFS** para ativar o Perfect Forward Secret (PFS). O PFS gera chaves aleatórias para criptografar a sessão.

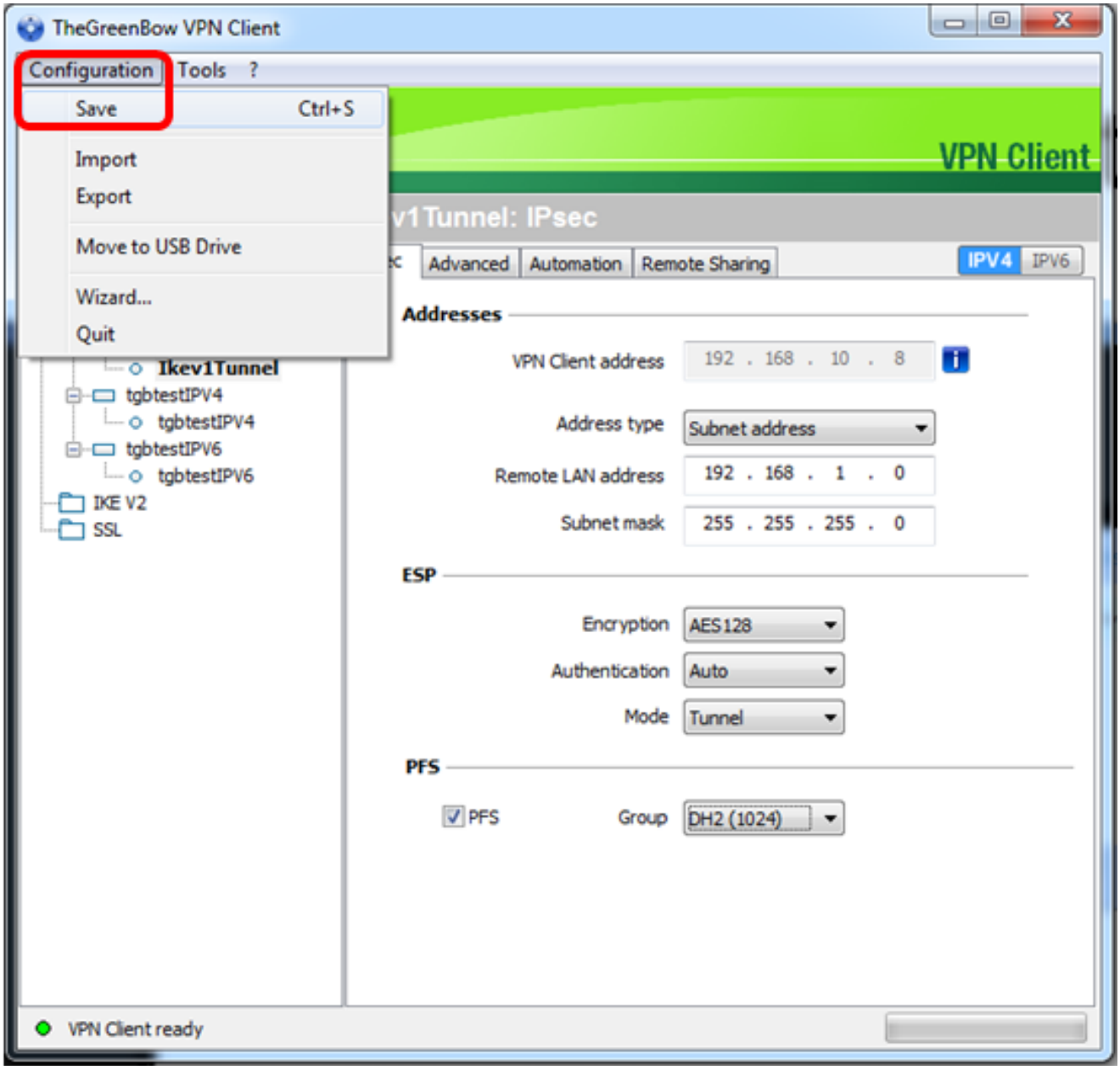


Etapa 9. Escolha uma configuração de grupo PFS na lista suspensa Grupo.

Note: Neste exemplo, DH5 (1536) é escolhido para corresponder à configuração do Grupo DH do roteador.



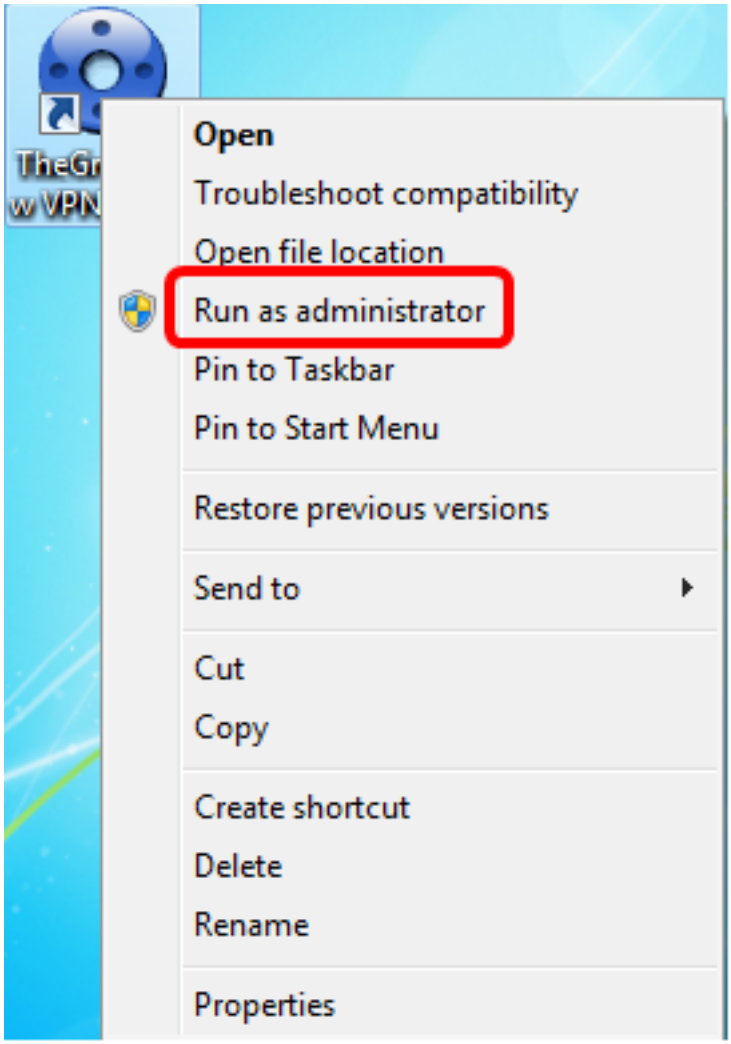
Etapa 10. Clique com o botão direito do mouse em **Configuração** e escolha Salvar.



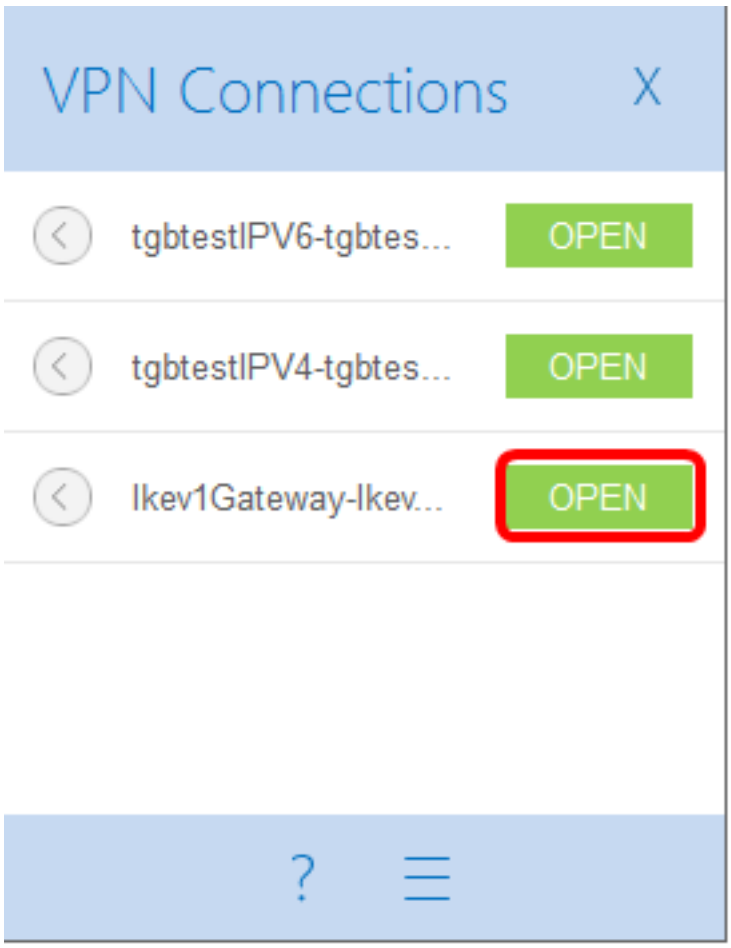
Agora você deve ter configurado com êxito o cliente VPN do GreenBow para se conectar ao roteador RV34x Series através da VPN.

Iniciar uma conexão VPN

Etapa 1. Clique com o botão direito do mouse em O cliente VPN GreenBow e escolha **Executar como administrador**.



Etapa 2. Escolha a conexão VPN que você precisa usar e clique em **ABRIR**. A conexão VPN deve ser iniciada automaticamente.

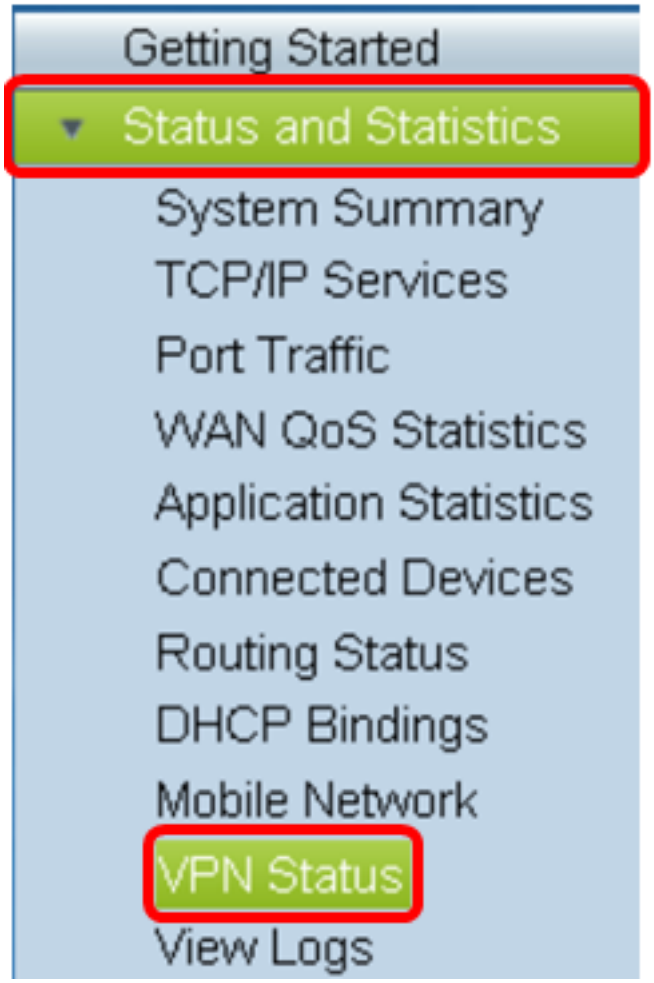


Note: Neste exemplo, o Gateway Ikev1configurado foi escolhido.

Verifique o status da VPN

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

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



Etapa 3. Em Client-to-Site Tunnel Status (Status do túnel de cliente para site), verifique a coluna Connections (Conexões) da Connection Table (Tabela de conexões).

Note: Neste exemplo, uma conexão VPN foi estabelecida.

Agora você deve ter verificado com êxito o status da conexão VPN no RV34x Series Router. O GreenBow VPN Client agora está configurado para se conectar ao roteador através da VPN.