OpenVPN em um roteador RV160 e RV260

Objetivo

O objetivo deste artigo é guiá-lo pela configuração do OpenVPN em seu roteador RV160 ou RV260, bem como pela configuração do cliente VPN do OpenVPN em seu computador.

Dispositivos aplicáveis

- RV160
- RV260

Versão de software

- 1.0.00.15

Table Of Contents

Introduction

O OpenVPN é um aplicativo gratuito e de código aberto que pode ser configurado e usado para uma VPN (Virtual Private Network). Ele usa uma conexão cliente-servidor para fornecer comunicações seguras entre um servidor e um local de cliente remoto pela Internet.

O OpenVPN usa o OpenSSL para criptografia de UDP e TCP para transmissão de tráfego. Uma VPN fornece um túnel seguro de proteção, que é menos vulnerável a hackers, pois criptografa os dados enviados do seu computador através da conexão VPN. Por exemplo, se você estiver usando WiFi em um lugar público, como em um aeroporto, ele impedirá que seus dados, transações e consultas sejam vistos por outros usuários. Assim como o HTTPS, ele criptografa os dados enviados entre dois pontos finais.

Uma das etapas mais importantes na configuração do OpenVPN é obter um certificado de uma autoridade de certificação (CA). É usado para autenticação. Os certificados são adquiridos de qualquer número de sites de terceiros. É uma forma oficial de provar que seu site é seguro. Essencialmente, a AC é uma fonte confiável que verifica se você é uma empresa legítima e se pode ser confiável. Para o OpenVPN, você só precisa de um certificado de nível inferior a um custo mínimo. Você recebe check-out do CA e, depois que ele verificar suas informações, ele emitirá o certificado para você. Este certificado pode ser baixado como um arquivo em seu computador. Você pode então ir para o roteador (ou servidor VPN) e carregá-lo lá. Observe que os clientes não precisam de um certificado para usar o OpenVPN; ele é apenas para verificação através do roteador.

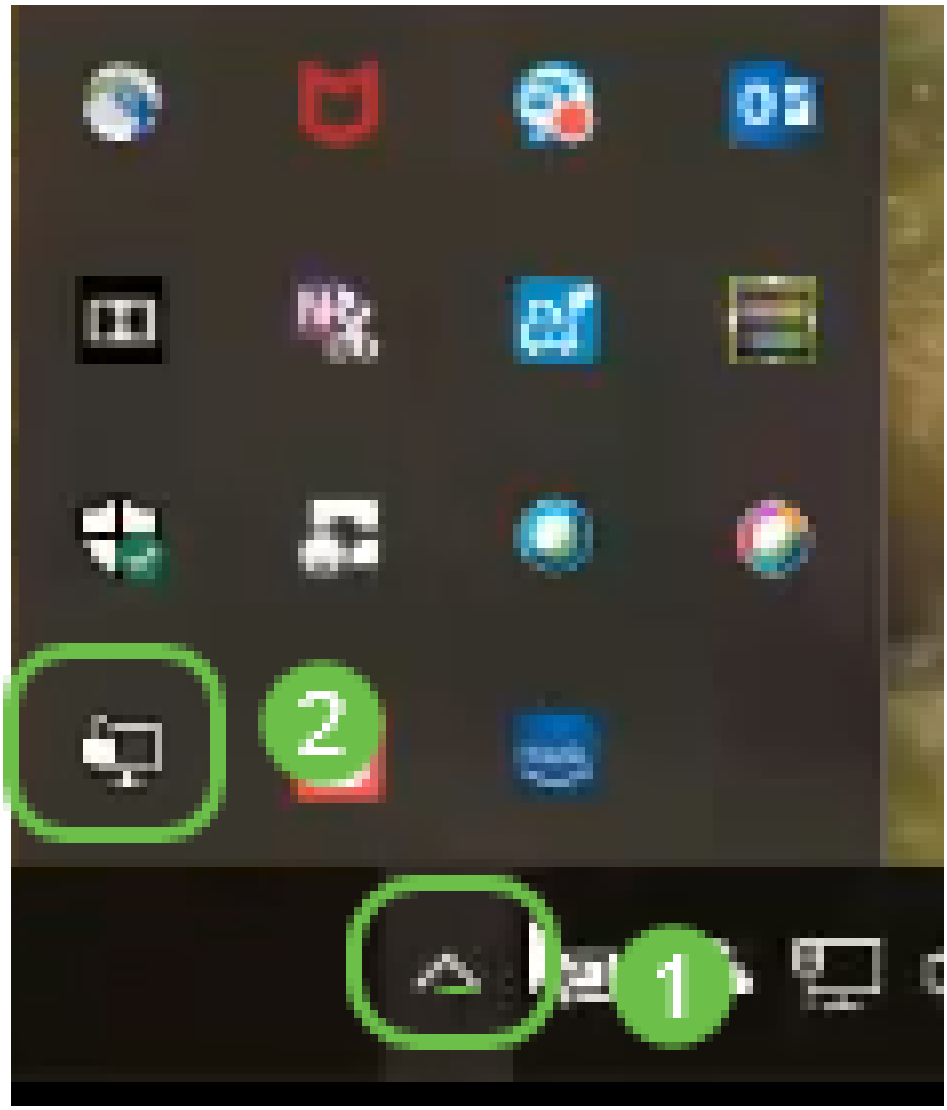
Prerequisites

Instale o aplicativo OpenVPN no sistema. Clique aqui para ir para o site OpenVPN.

Para obter mais informações sobre o OpenVPN e respostas a muitas perguntas que você possa ter, clique aqui.

Note: Essa configuração é específica para o Windows 10.

Depois que o OpenVPN estiver instalado, o aplicativo deverá aparecer em sua área de trabalho ou como um pequeno ícone no lado direito da barra de tarefas. Os clientes OpenVPN também precisarão disso instalado.



Certifique-se de que você tenha a hora correta do sistema em todos os dispositivos. A hora

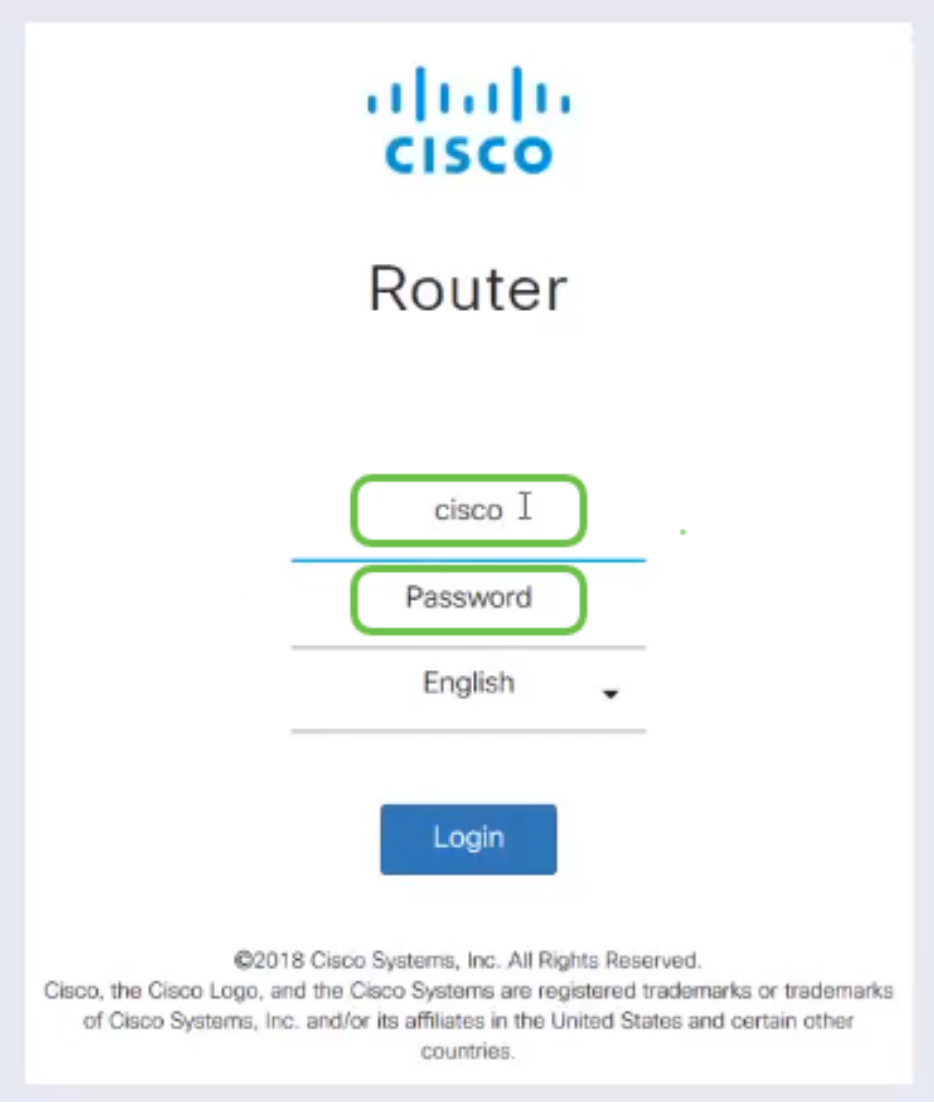
apropriada do sistema deve ser completamente sincronizada no roteador antes da criação de um certificado. Isso é feito automaticamente, mas se você encontrar problemas, esse é um bom lugar para verificar.

Configuração de uma demonstração do OpenVPN em um roteador RV160/RV260

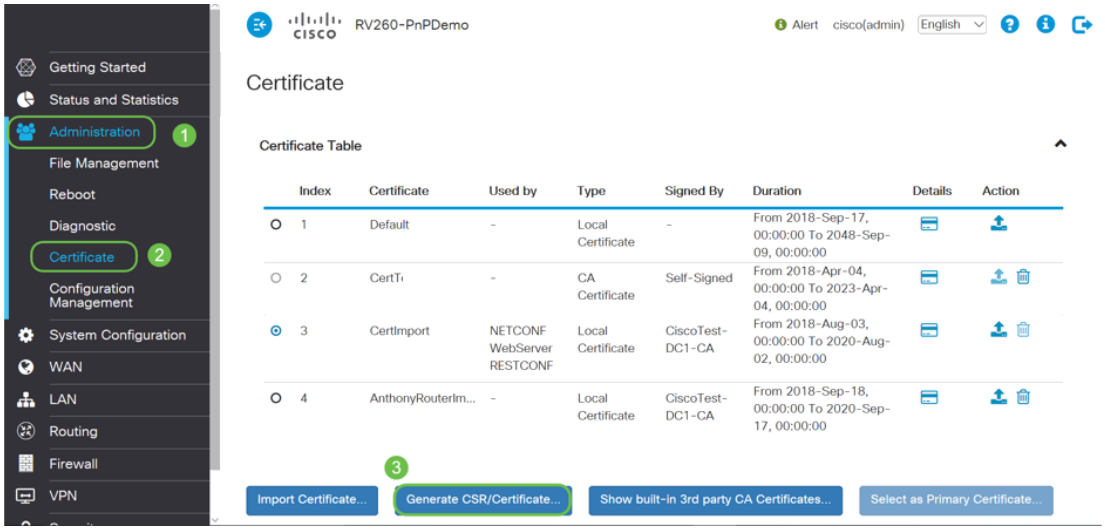
Se quiser experimentar o OpenVPN antes de pagar uma CA, você pode criar um certificado autoassinado. Essa é uma maneira sem custo de ver se o OpenVPN é algo que você gostaria de implantar para sua empresa. Se você já sabe que deseja comprar uma CA, pode pular esta seção do artigo e ir diretamente para Setting up OpenVPN on a RV160/RV260 Router.

Etapa 1. Faça login no roteador usando suas credenciais. O nome de usuário e a senha padrão são *cisco*.

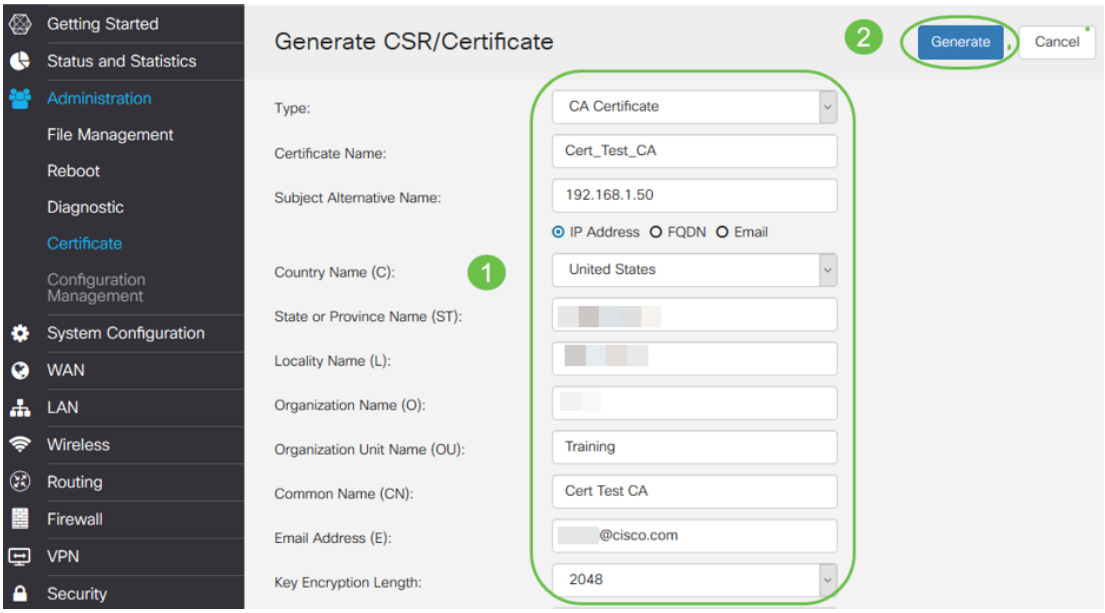
Note: É altamente recomendável alterar todas as senhas para algo mais complexo. Caso contrário, é como deixar a chave na porta trancada.



Etapa 2. É obrigatório que você obtenha um certificado no roteador. Navegue até **Administration** > **Certificate** > **Generate CSR/Certificate...** Esta é a forma de criar a solicitação de um certificado.



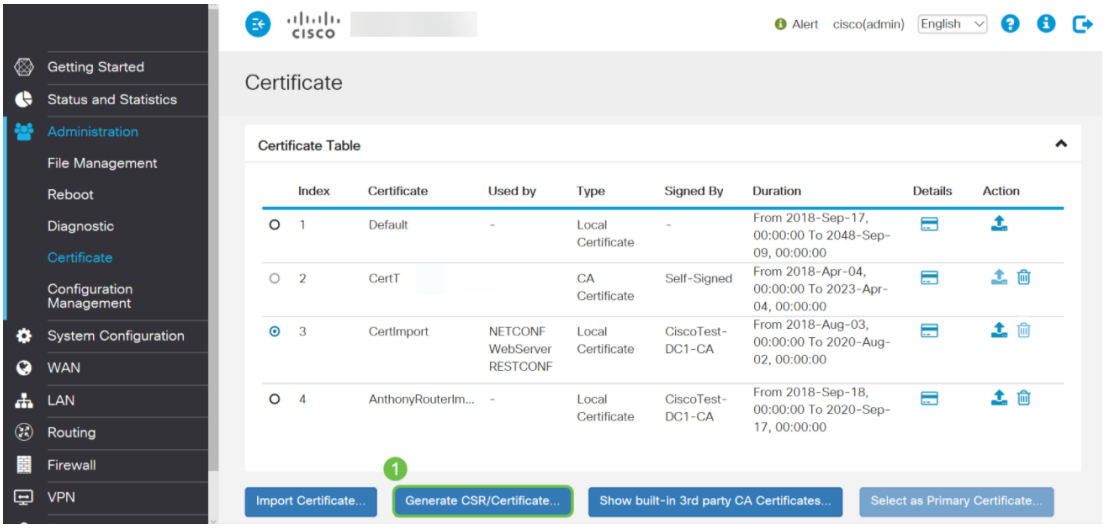
Etapa 3. Solicitar um *certificado CA*.



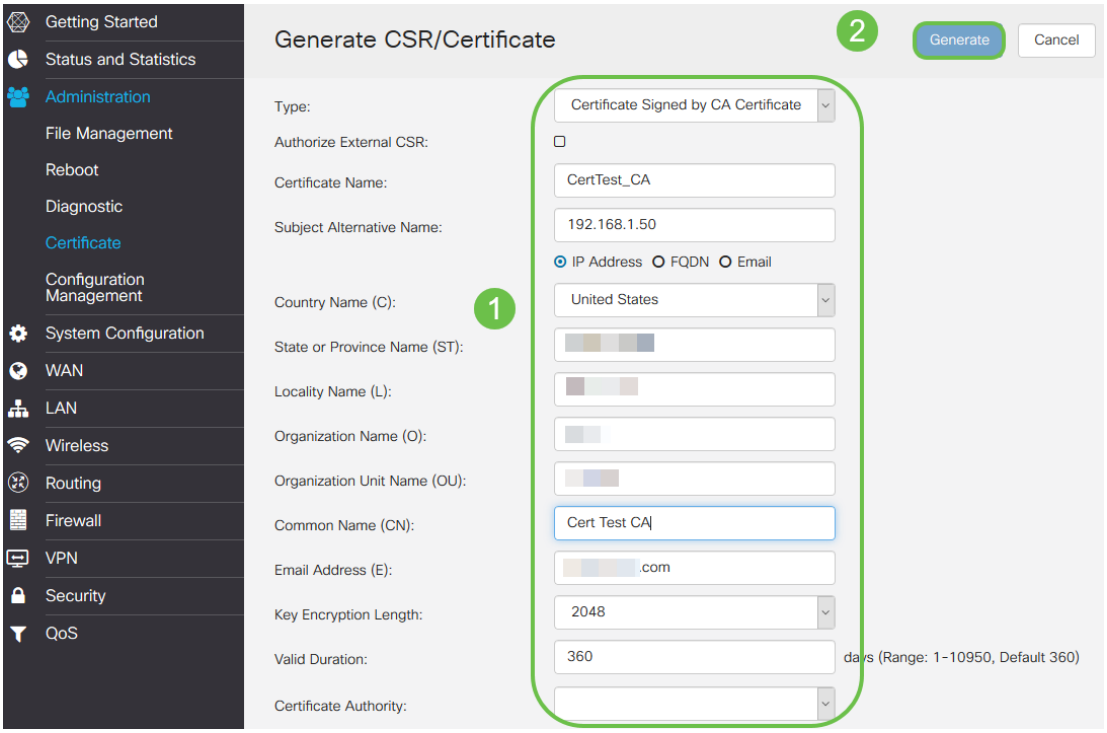
- Selecione *Certificado CA* no menu suspenso
- Inserir um nome de certificado
- Insira o endereço IP, o FQDN (Fully Qualified Domain Name, nome de domínio totalmente qualificado) ou o e-mail. Digitar o endereço IP é a escolha mais comum.
- Digite seu país
- Digite seu estado
- Insira seu nome de localidade, geralmente sua cidade
- Digite seu nome de organização
- Insira o nome da unidade da empresa
- Digite seu endereço de e-mail
- Insira o tamanho da criptografia de chave, 2048 é recomendado

Clique no botão superior direito **Gerar**.

Etapa 4. Você também precisa de um certificado de servidor. Este *certificado assinado pelo certificado CA* será assinado pelo certificado CA que acabou de criar.



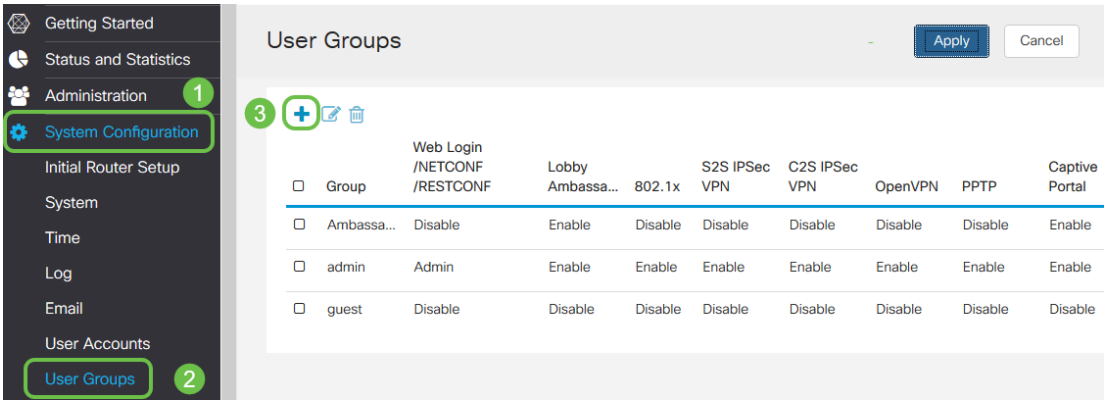
Etapa 5. Solicitar um *certificado assinado pelo certificado CA*.



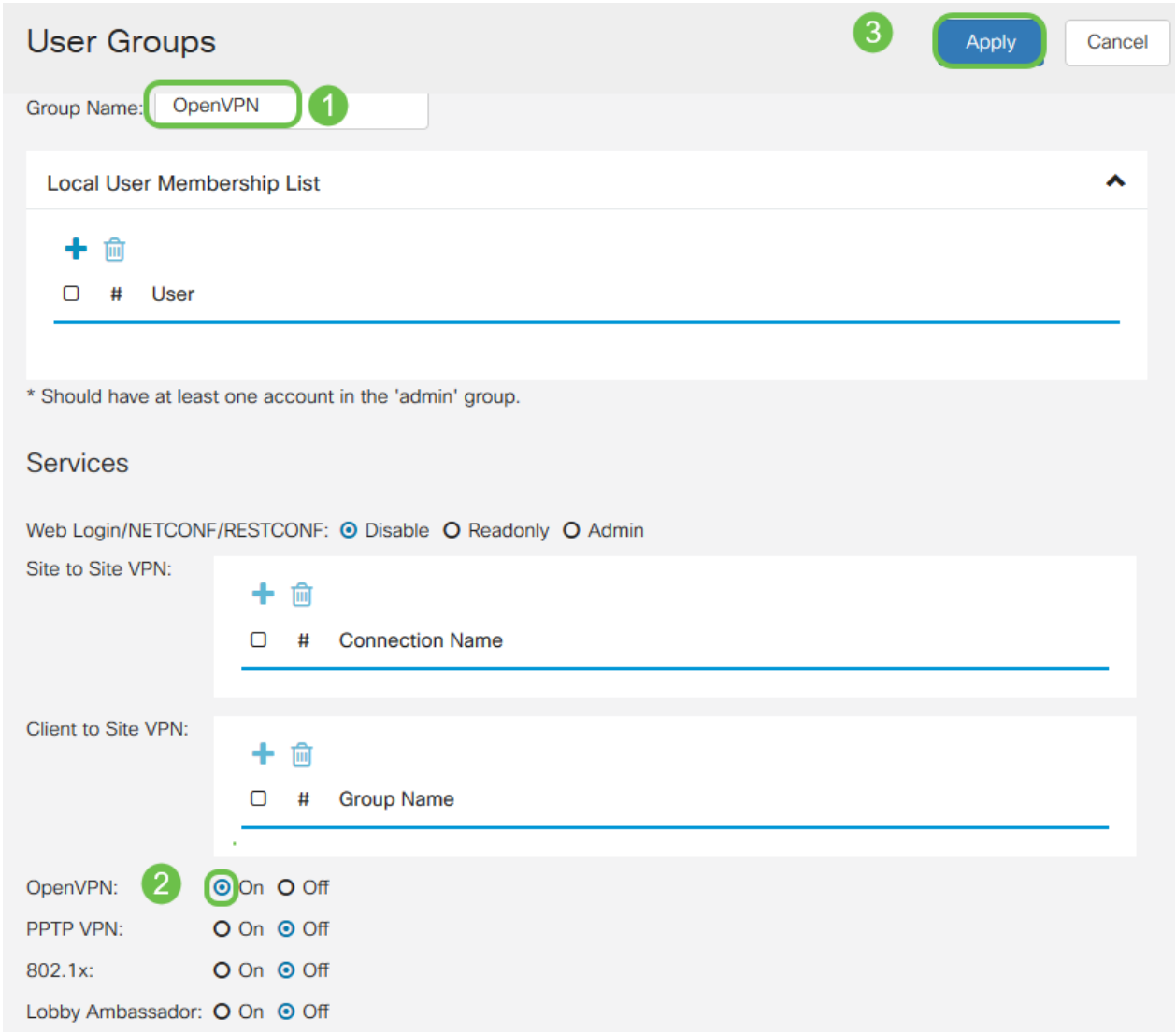
- Selecione *Solicitação de assinatura de certificado* no menu suspenso
- Inserir um nome de certificado
- Insira o endereço IP, o FQDN (Fully Qualified Domain Name, nome de domínio totalmente qualificado) ou o e-mail. Digitar o endereço IP é a escolha mais comum.
- Digite seu país
- Digite seu estado
- Insira seu nome de localidade, geralmente sua cidade
- Digite seu nome de organização
- Insira o nome da unidade da empresa
- Digite seu endereço de e-mail
- Insira o tamanho da criptografia de chave, 2048 é recomendado
- Escolha a autoridade de certificação apropriada no menu suspenso

Clique no botão superior direito **Gerar**.

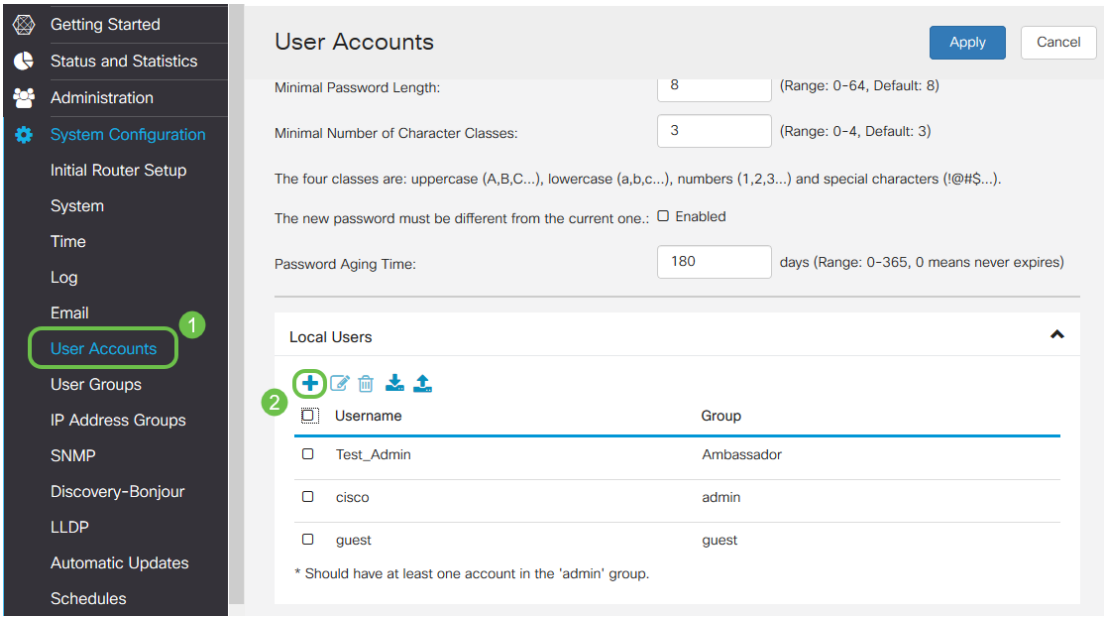
Etapa 6. Navegue até **Configuração do sistema > Grupos de usuários**. Selecione o ícone **de mais** para adicionar o novo grupo.



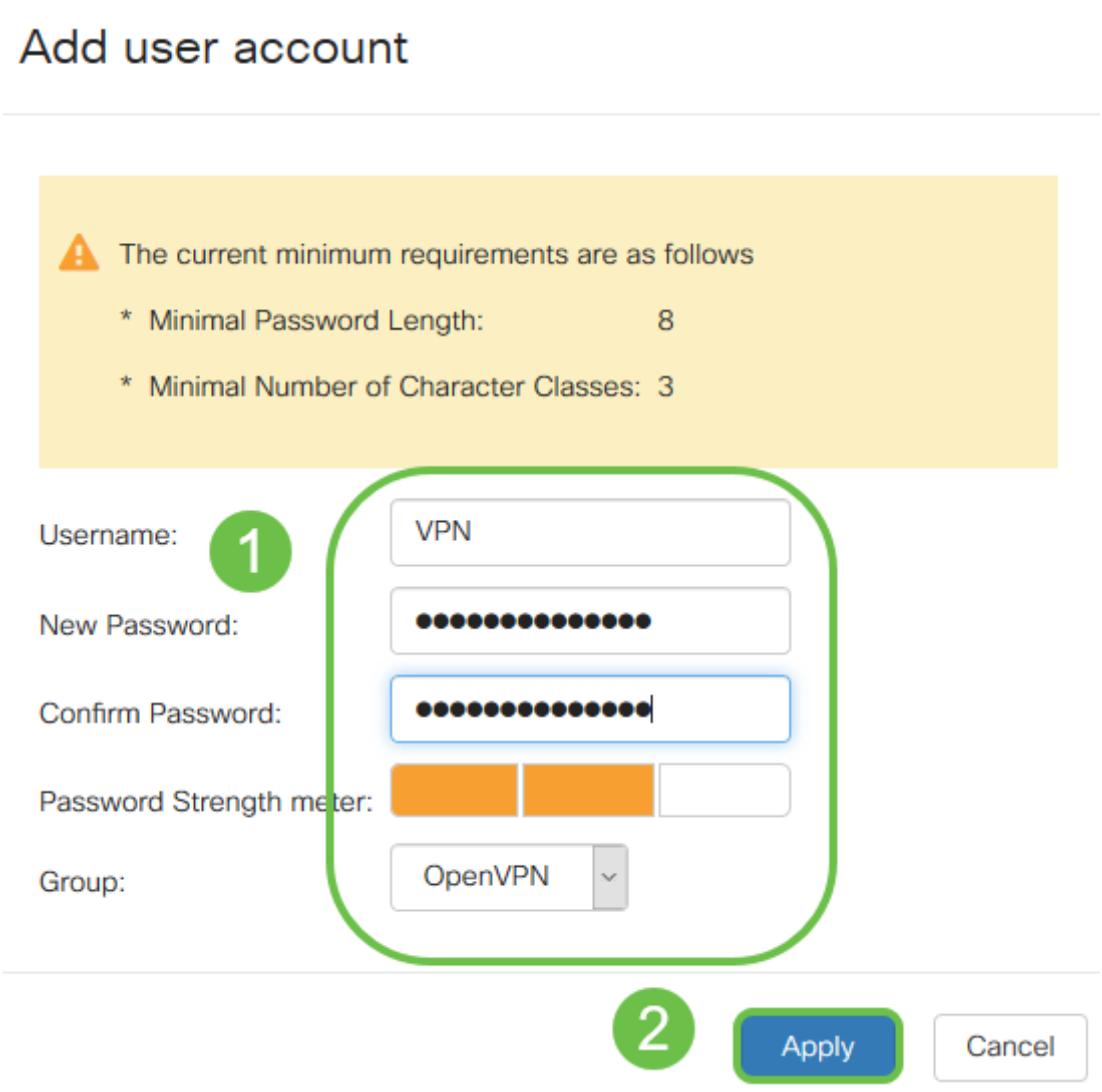
Passo 7. Digite o nome do Grupo e clique em *On* para o botão de opção para ativar o OpenVPN. Clique em Apply.



Etapa 8. Navegue no menu Configuração do sistema e clique em **Contas de usuário**. Em Usuários locais, clique no ícone **de mais**.

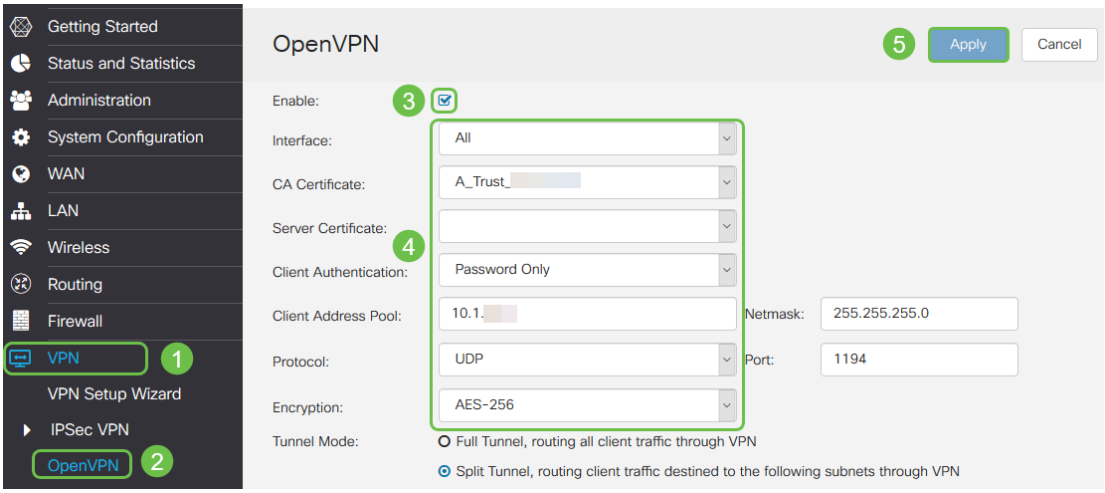


Etapa 9. Preencha as informações abaixo. Selecione OpenVPN no menu suspenso. Clique em Apply.



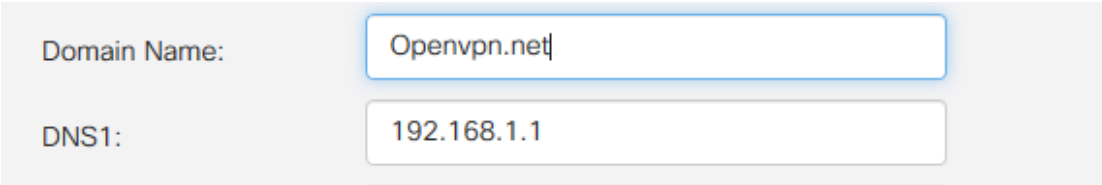
Todas as dependências estão completas e o roteador agora pode ser configurado para OpenVPN.

Etapa 10. Navegue até **VPN > OpenVPN**. A página OpenVPN é aberta. Preencha cada caixa na página, certificando-se de selecionar os certificados criados anteriormente no menu suspenso.



- Marque a caixa *Enable (Habilitar)*. Selecione a Interface que permitirá o tráfego. Nesse caso, uma rede de longa distância (WAN) e selecione um certificado de autoridade de certificação (CA).
- Selecione o *certificado CA* no menu suspenso
- Selecione o certificado do servidor baixado no menu suspenso
- Selecione *Autenticação de cliente*. Se você selecionar Senha, eles precisam se autenticar com uma senha. Se você selecionar Senha + Certificado, o cliente também deverá ter um certificado. Isso é mais seguro, mas aumenta o custo da VPN, pois eles precisariam comprar uma CA separada.
- Digite o *pool de endereços de cliente*. Escolha um endereço IP em uma sub-rede de rede que não seja usada em nenhum outro lugar da empresa. Você seleciona os intervalos reservados e escolhe um intervalo que não seja usado em nenhum outro lugar.
- Escolha a forma de *Criptografia*. Certifique-se de que a criptografia seja igual à do cliente. DES e 3DES não são recomendados e devem ser usados apenas para compatibilidade com versões anteriores.
- Escolha Dividir túnel se quiser especificar apenas qual tráfego passa pela VPN. Para uma VPN, é necessário um túnel dividido. *O Modo de Túnel Completo* é selecionado em outras situações em que você deseja que todo o tráfego do cliente passe pela VPN.

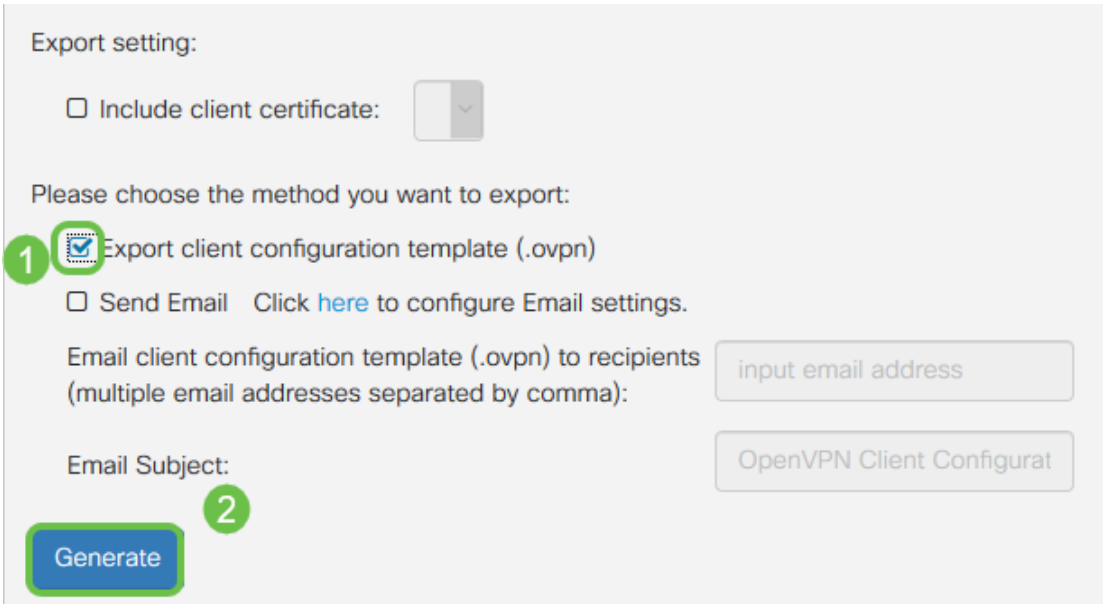
Etapa 11. Role a página para baixo e preencha o *Domain Name* e o *DNS1*.



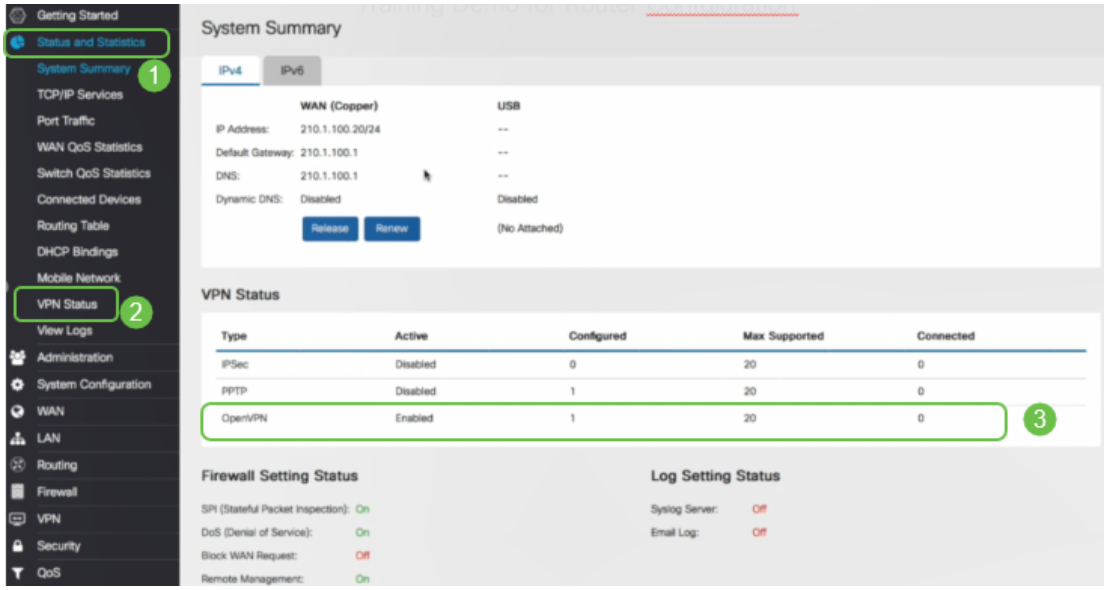
Nota: O endereço IP DNS1 pode ser um servidor DNS interno dedicado, o mesmo endereço IP do gateway padrão fornecido pelo ISP (Provedor de serviços de Internet), em uma máquina virtual ou um servidor DNS confiável na Internet.

Etapa 12. Clique em **Apply** para salvar a configuração no roteador.

Etapa 13. Fique na mesma página e role mais adiante. Gere o modelo de configuração a ser instalado no cliente OpenVPN. Este arquivo tem uma extensão *.ovpn* e será usado pelo cliente OpenVPN. Marque a caixa para *Exportar modelo de configuração de cliente (.ovpn)* e clique em **Gerar**. Isso faz o download do arquivo no computador.



Etapa 14. Navegue até **Status e Statistics** > **VPN Status**. Você pode rolar para baixo para obter informações mais detalhadas.



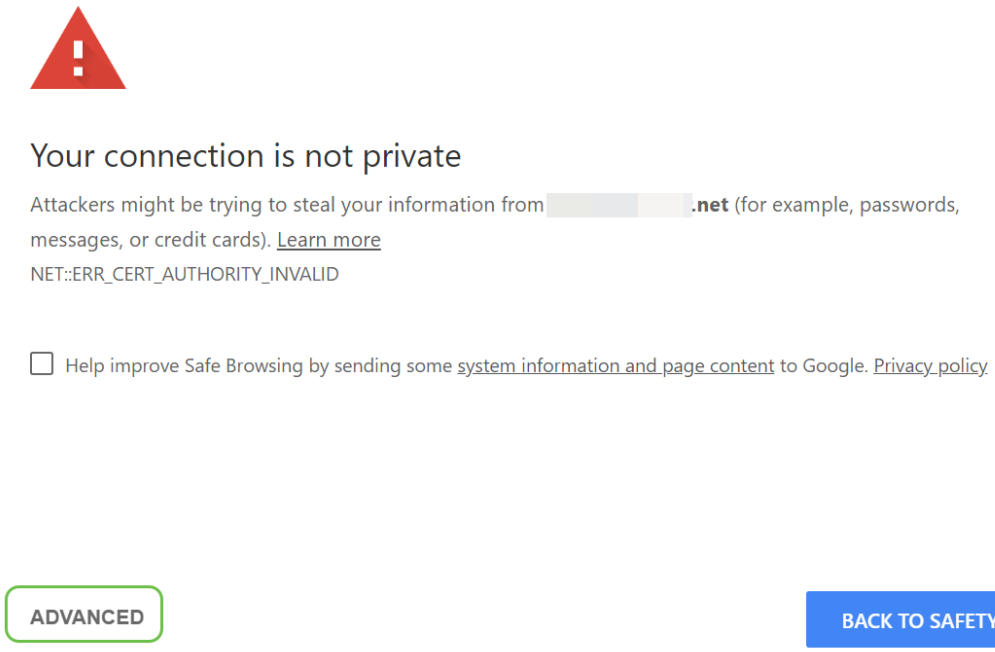
A próxima seção deste artigo é importante para revisão, pois explica como fazer login com um certificado autoassinado.

Fazendo login com um certificado autoassinado após configurar o OpenVPN de demonstração

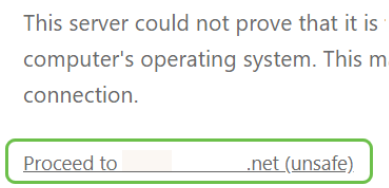
Ao fazer logon com um certificado autoassinado, você poderá ver um pop-up de aviso quando tentar fazer logon. Você precisará clicar em Avançado, Continuar, Confiar ou em outra opção, dependendo do seu navegador para continuar.

Nesse ponto, você pode receber um aviso de que não é seguro. Você pode optar por continuar, adicionar exceção ou avançado. Isso varia de acordo com o navegador da Web.

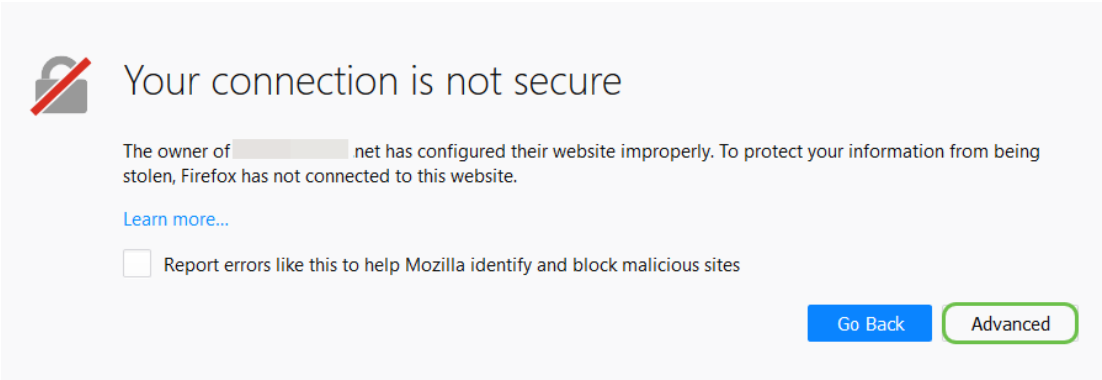
Neste exemplo, o Chrome foi usado para um navegador da Web. Esta mensagem é exibida; clique em **Avançado**.



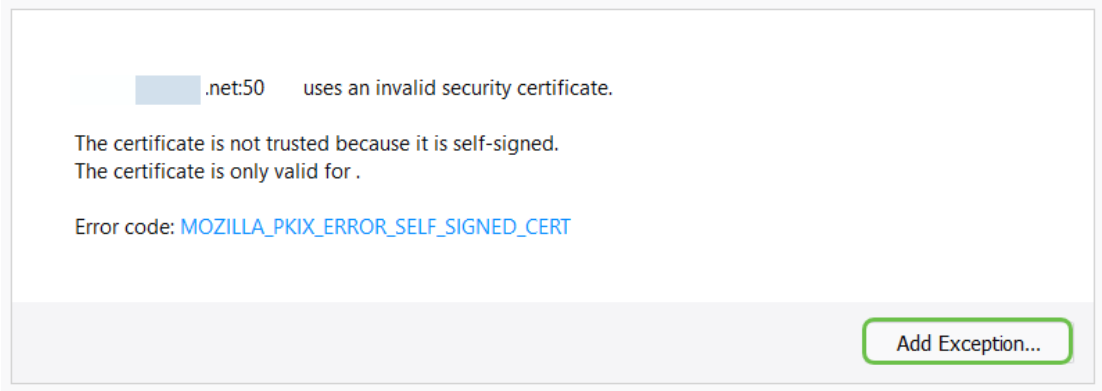
Uma nova tela será aberta e você precisará clicar em **Prosseguir para seu site.net (não seguro)**



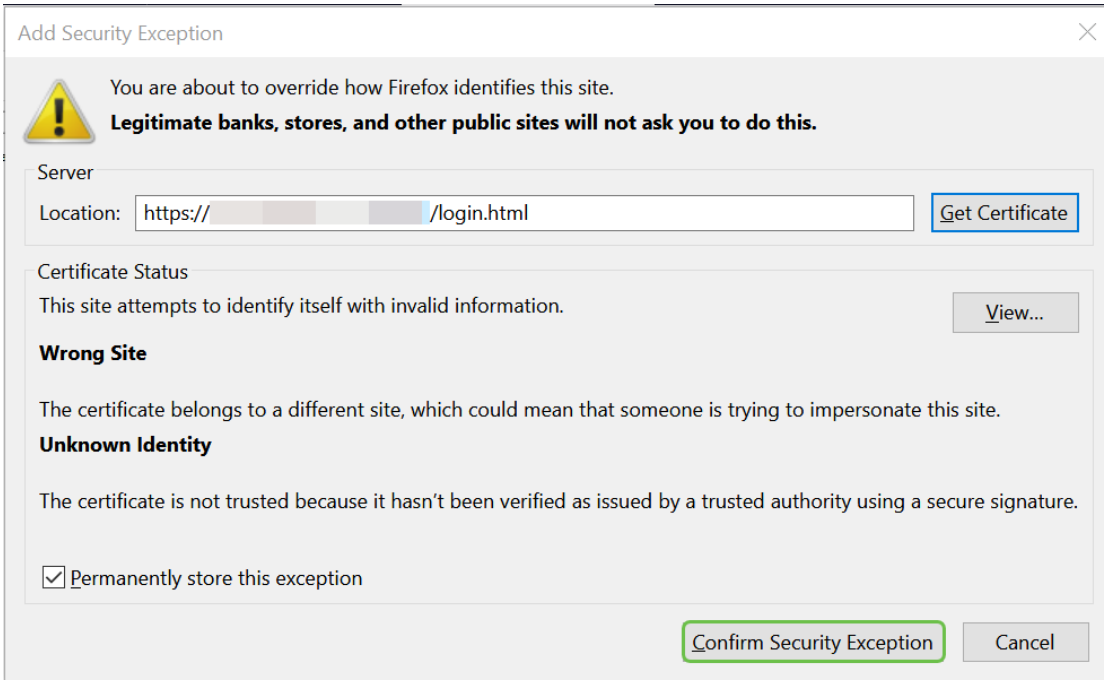
Aqui está um exemplo de como acessar o aviso do dispositivo ao usar o Firefox como um navegador da Web. Clique em **Avançado**.



Clique em **Adicionar exceção...**



Finalmente, você terá que clicar em **Confirmar exceção de segurança.**



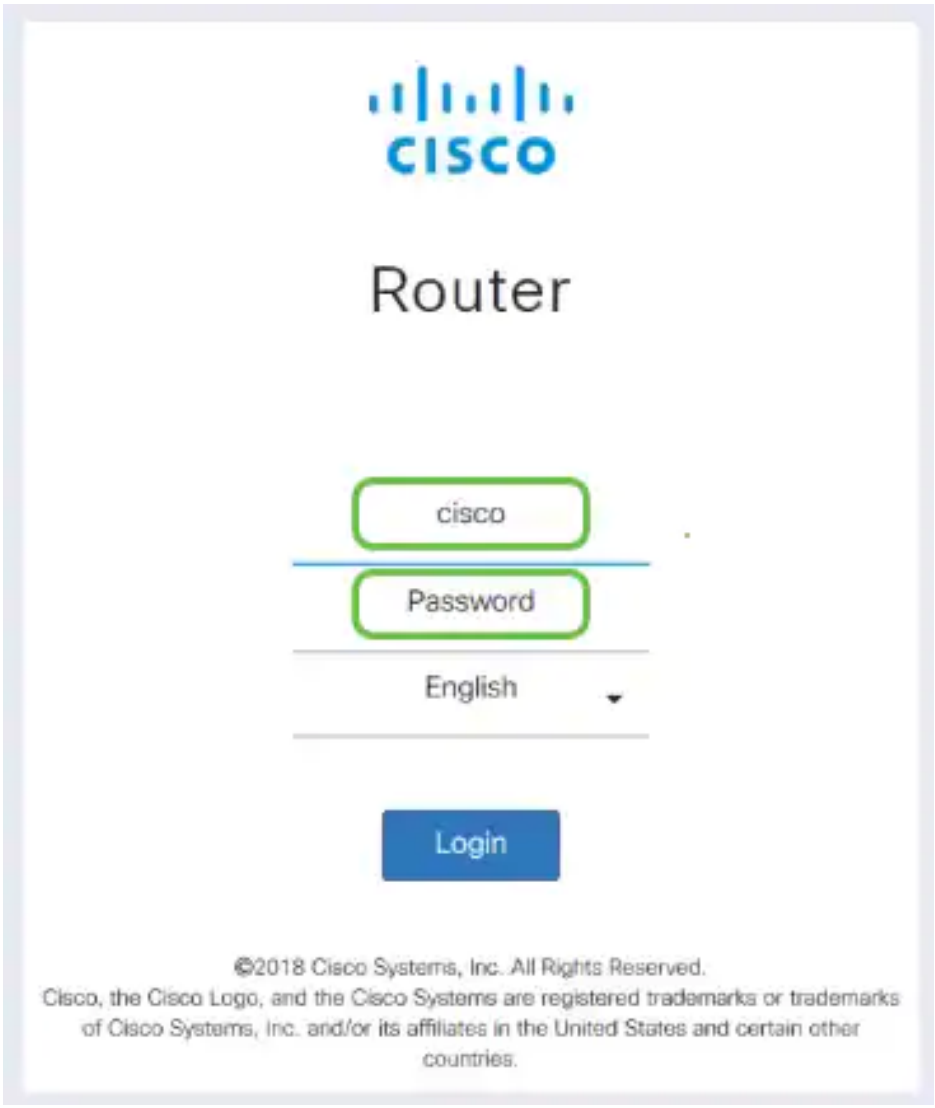
O roteador agora está configurado com todos os parâmetros necessários para suportar uma conexão de cliente OpenVPN. Como você já fez o download do modelo de configuração do cliente para seu dispositivo, o que termina em *.ovpn*, você pode prosseguir para a seção Configuração do OpenVPN Client em Computador. Se decidir implantar o OpenVPN para sua empresa, você poderá seguir as etapas desta próxima seção.

Configurando o OpenVPN em um roteador RV160/RV260

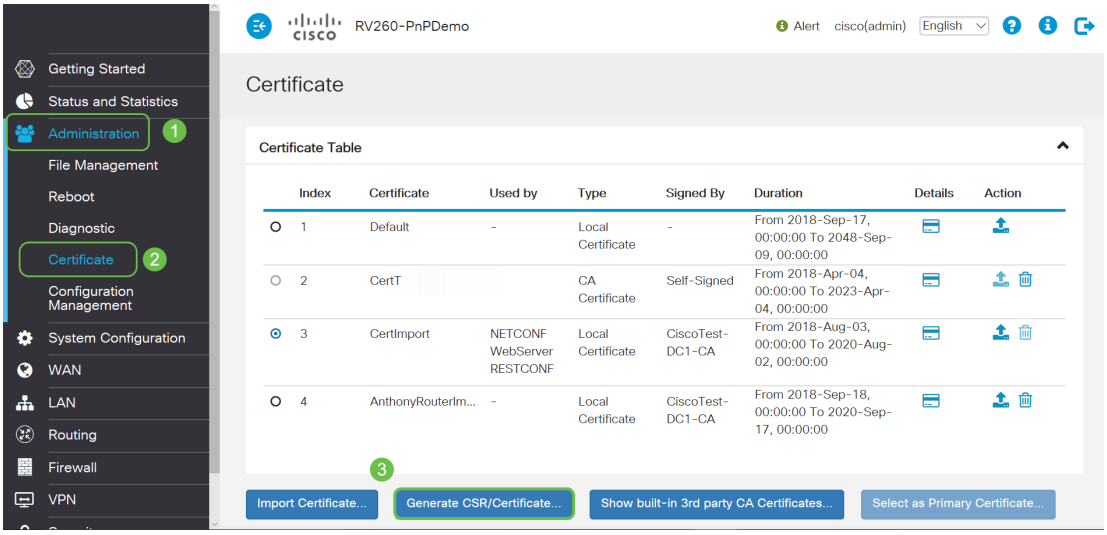
Este é um processo mais complicado, pois envolve obter uma CA de terceiros, que custa dinheiro. Você também precisa enviar o modelo de configuração do cliente VPN, terminando em *.ovpn*, para que todos os clientes possam configurar seu dispositivo. Os clientes precisam de várias configurações iguais às do roteador para se comunicarem. A melhor parte é que, por um custo mínimo, você e seus funcionários podem usar a Internet e conduzir negócios com mais segurança.

Etapa 1. Faça login no roteador usando suas credenciais. O nome de usuário e a senha padrão são *cisco*.

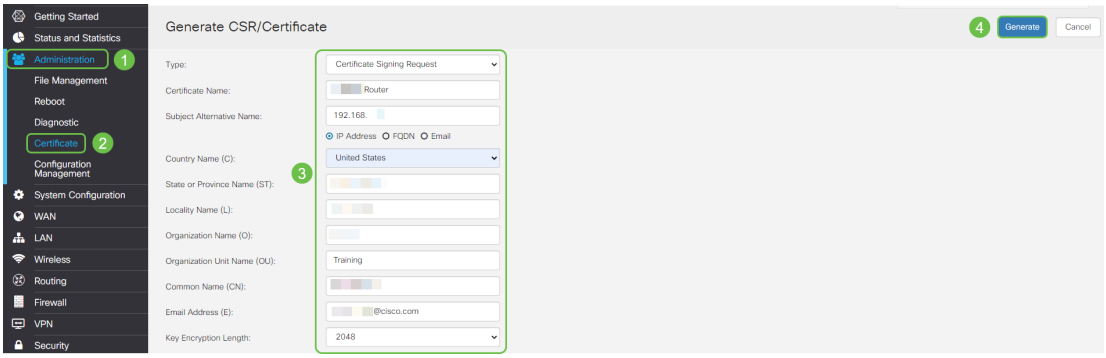
Note: É altamente recomendável alterar todas as senhas para algo mais complexo. Caso contrário, é como deixar a chave na porta trancada.



Etapa 2. É obrigatório que você obtenha um certificado. Navegue até **Administration > Certificate > Generate CSR/Certificate...** Esta é a forma de criar a solicitação de um certificado.



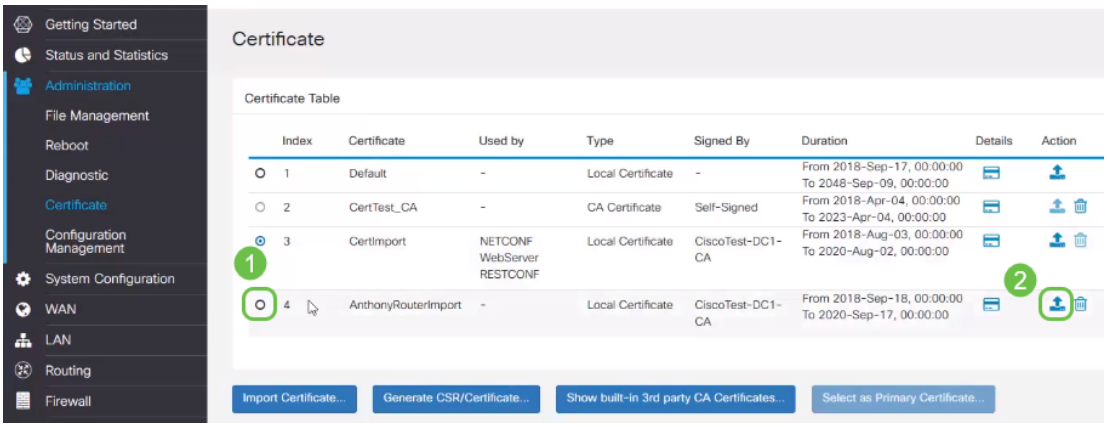
Etapa 3. Solicitar um *certificado assinado pelo certificado CA*. Isso pode ser encontrado navegando para **Administração > Certificado**.



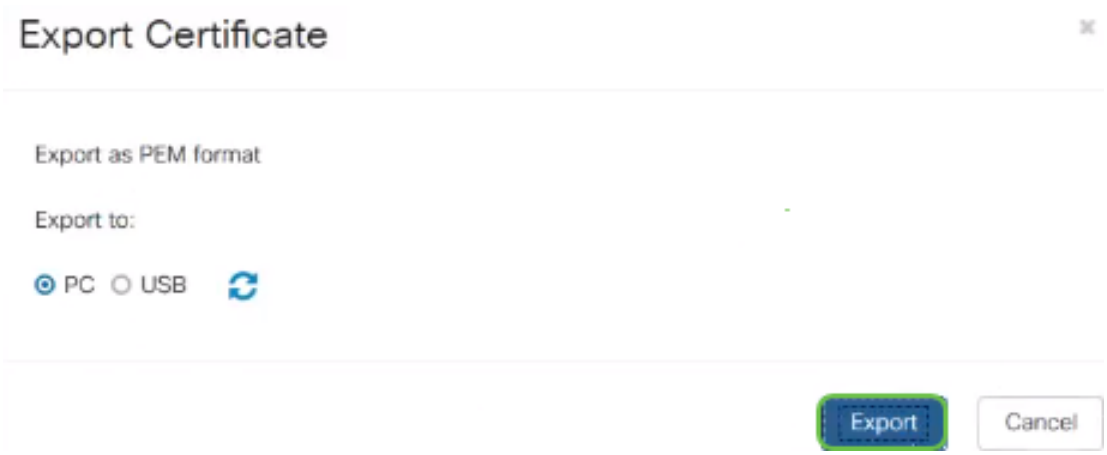
- Selecione *Solicitação de assinatura de certificado* no menu suspenso
- Inserir um nome de certificado
- Insira o endereço IP, o FQDN (Fully Qualified Domain Name, nome de domínio totalmente qualificado) ou o e-mail. Digitar o endereço IP é a escolha mais comum.
- Digite seu país
- Digite seu estado
- Insira seu nome de localidade, geralmente sua cidade
- Digite seu nome de organização
- Insira o nome da unidade da empresa
- Digite seu endereço de e-mail
- Insira o tamanho da criptografia de chave, 2048 é recomendado

Clique no botão superior direito **Gerar**

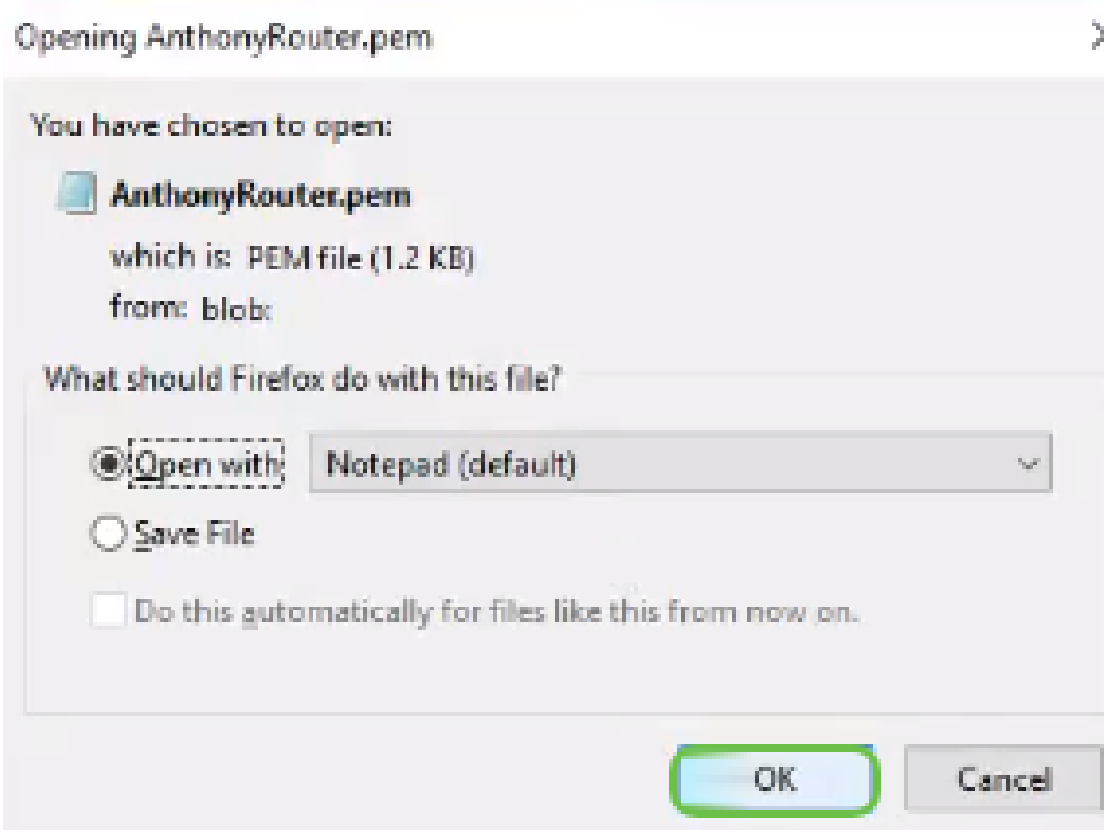
Etapa 4. Selecione Exportar clicando na seta para cima em Ação.



Etapa 5. Esta tela será exibida. Clique em **Exportar**.



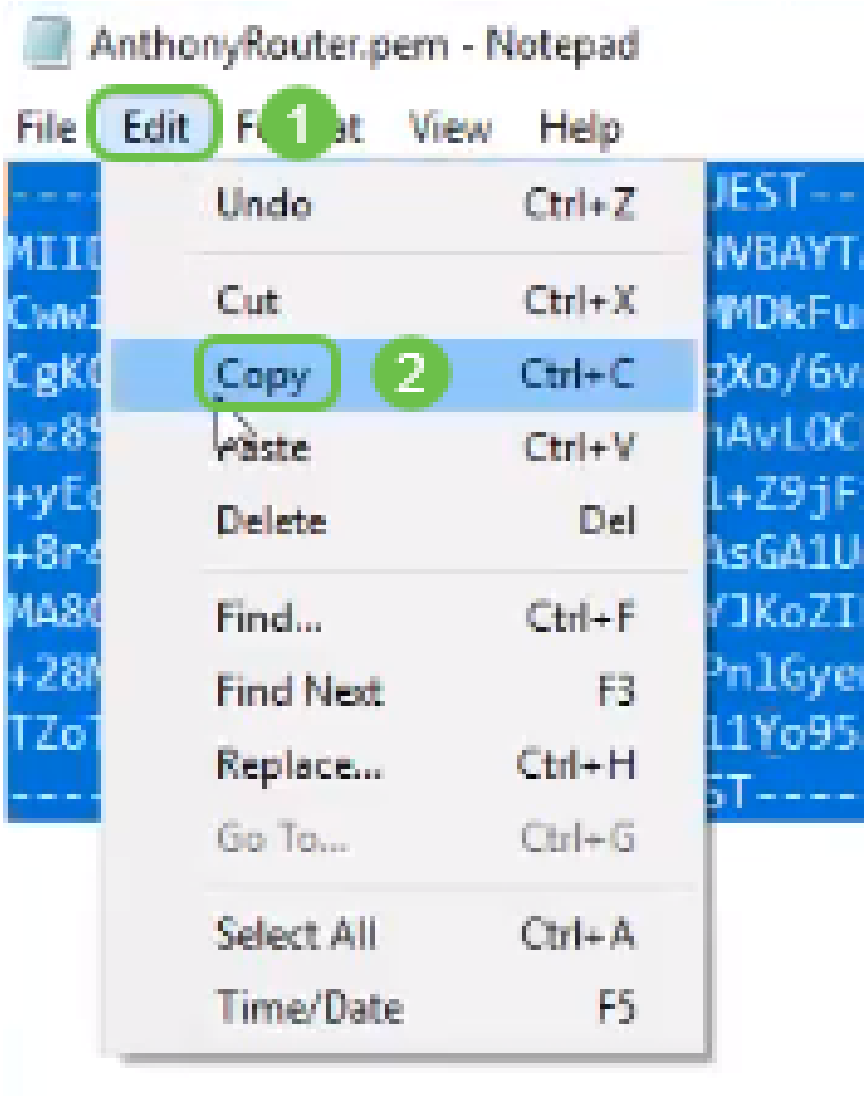
Etapa 6. Selecione *Abrir com e Bloco de notas* (padrão) no menu suspenso. Click **OK**.



Passo 7. Um arquivo XML será aberto.

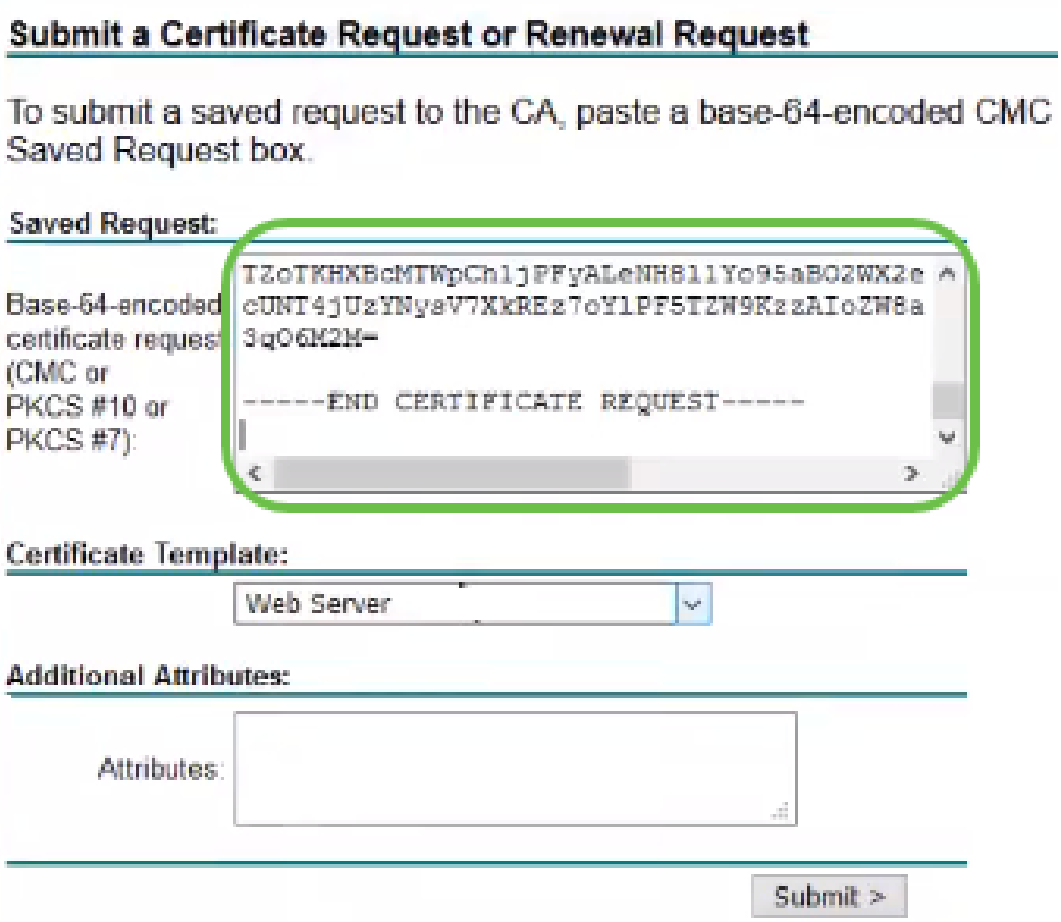
Note: Verifique se BEGIN CERTIFICATE REQUEST e END CERTIFICATE REQUEST estão em suas próprias linhas, conforme mostrado acima.

Etapa 8. Na parte superior da tela, clique em **Editar** e selecione **Copiar** no menu suspenso.

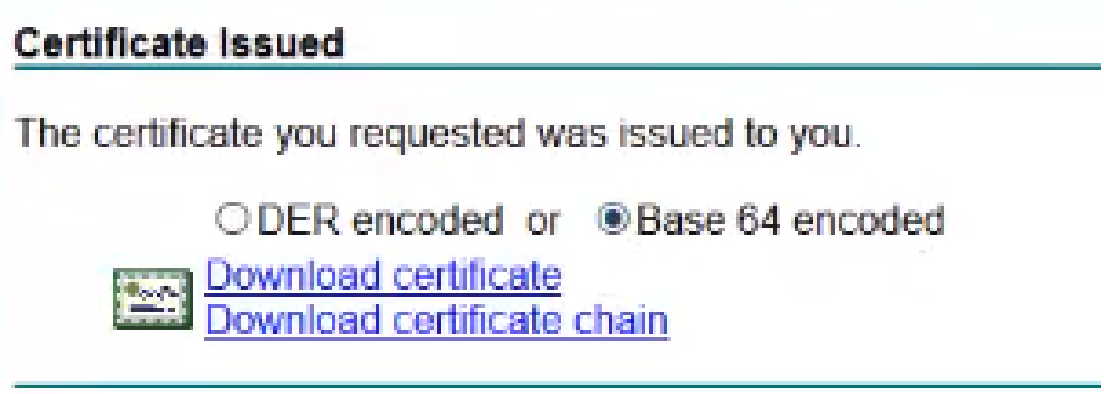


Etapa 9. Escolha um site de terceiros confiável para fazer a solicitação de certificado. Você precisará colar o arquivo XML copiado como parte da solicitação.

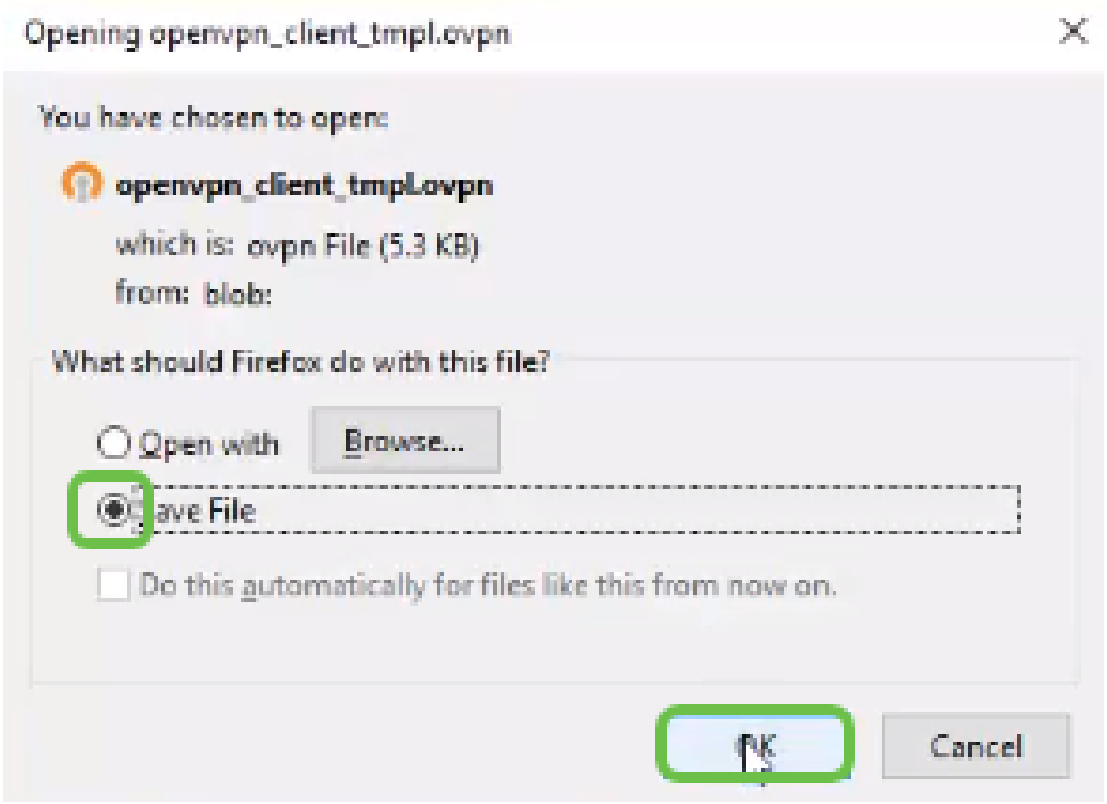
Note: Se você tiver um servidor de certificado interno em sua rede, poderá usá-lo, no entanto, isso não é comum.



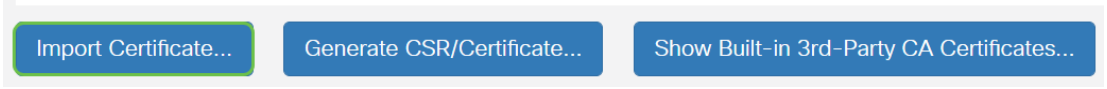
Etapa 10. Depois de verificar, você pode escolher *Baixar certificado*.



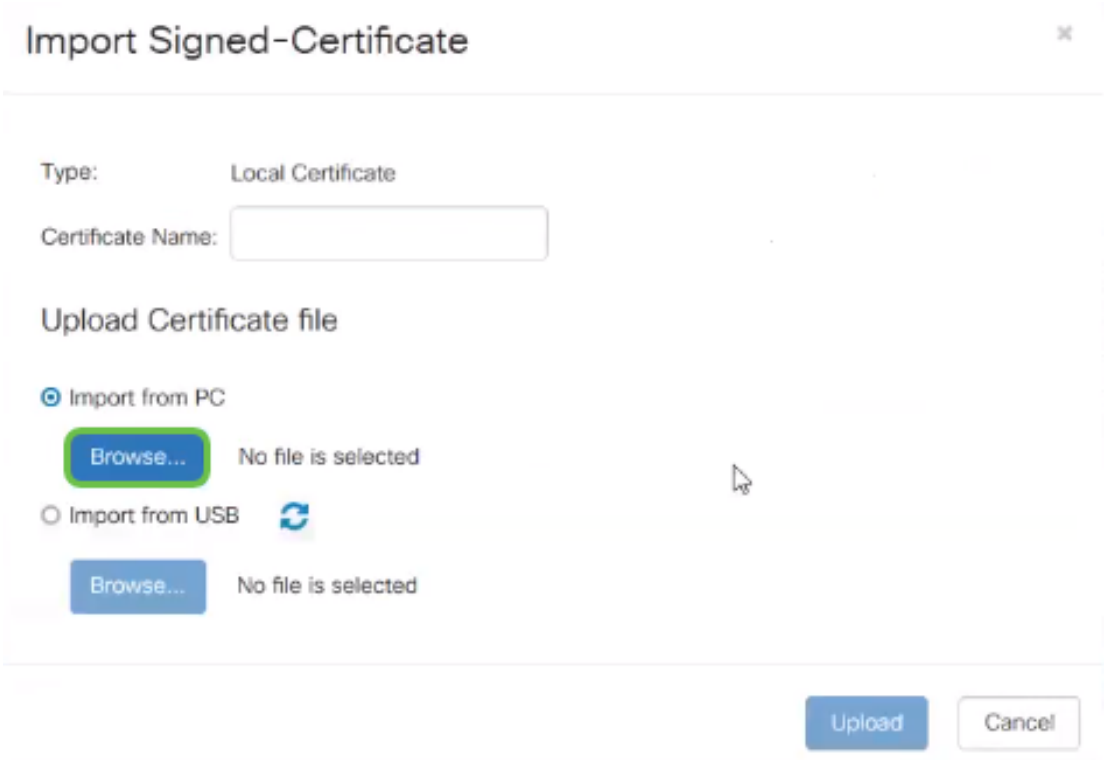
Etapa 11. Clique no botão de opção para *Salvar arquivo* e clique em **OK**.



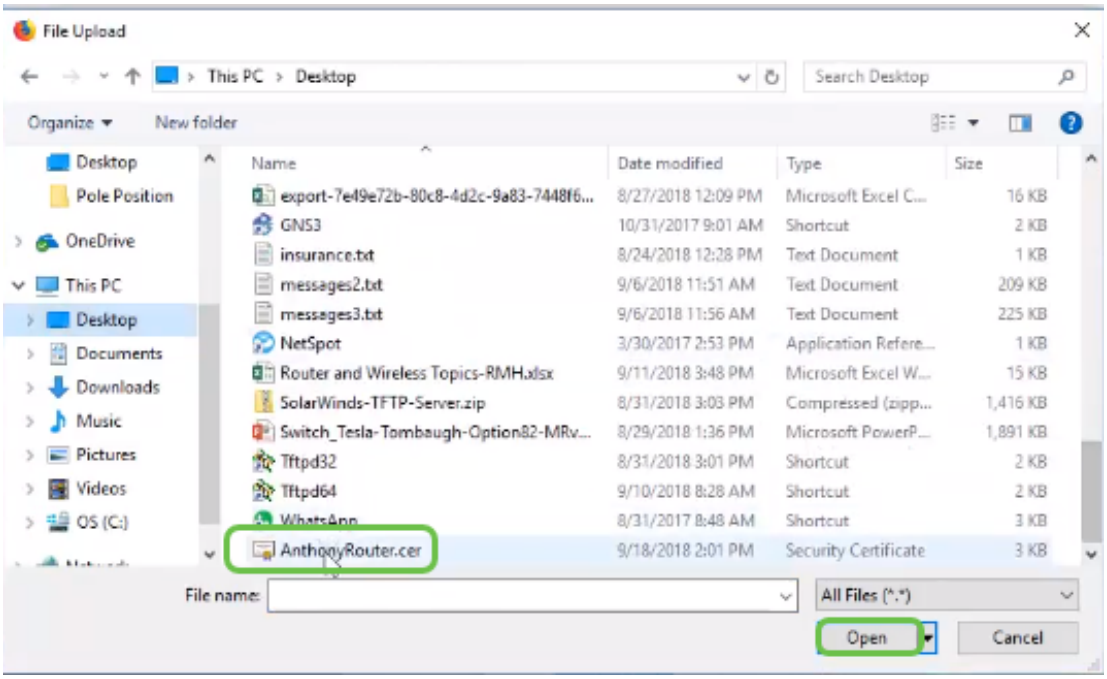
Etapa 12. Depois de salvá-lo, selecione o botão de opção do certificado e clique no ícone **de seta para baixo**.



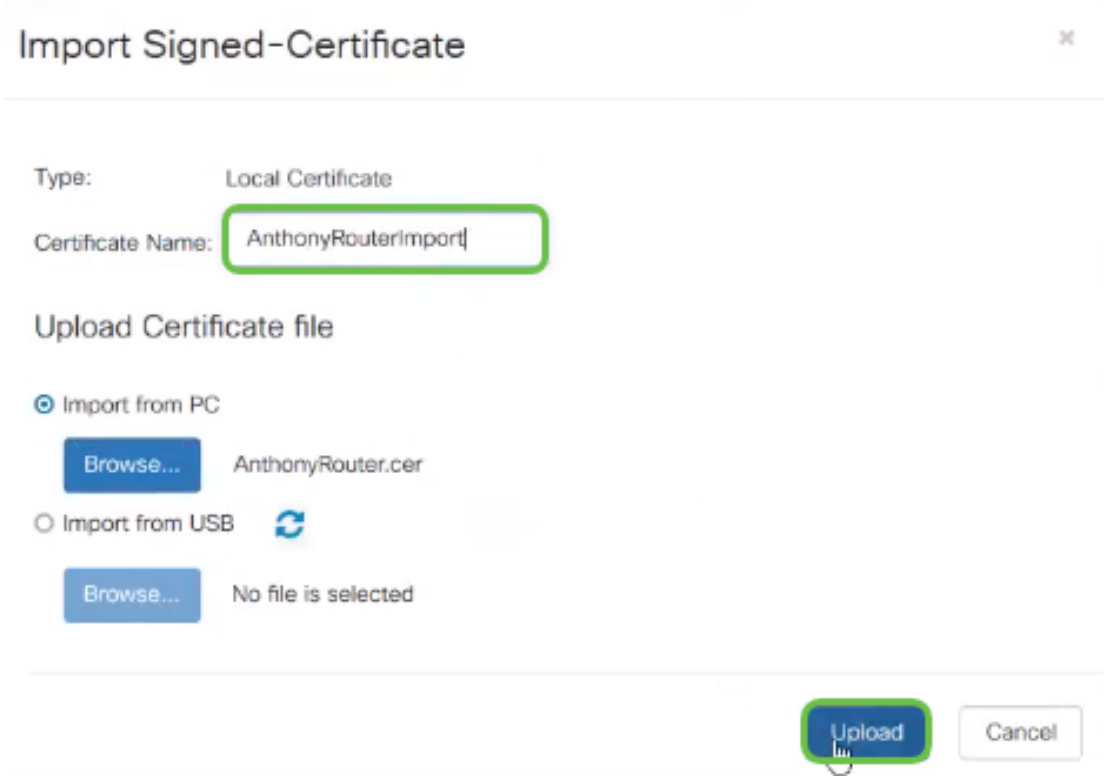
Etapa 13. Esta tela abrirá. Selecione **Procurar....**



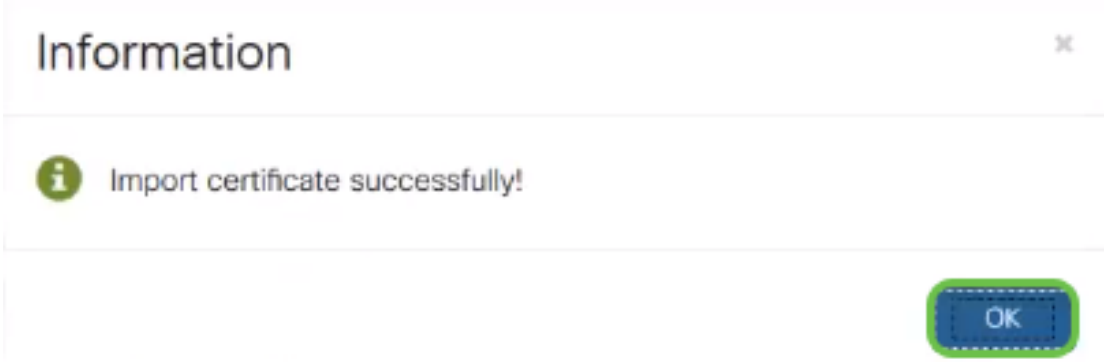
Etapa 14. Escolha o arquivo do certificado e clique em **Abrir**.



Etapa 15. Digite o *Nome do certificado* a importar e clique em **Carregar**.

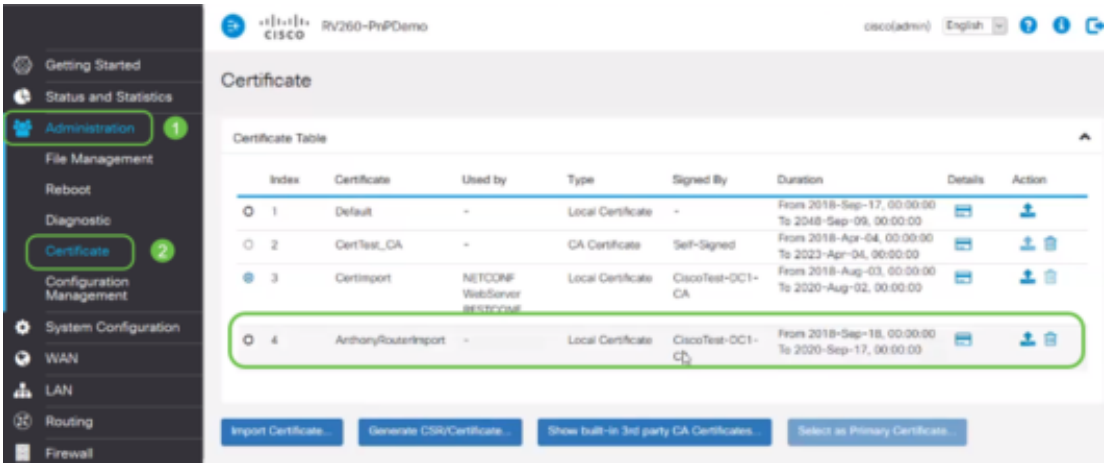


Etapa 16. Você receberá uma notificação de que o certificado foi importado com êxito. Click **OK**.

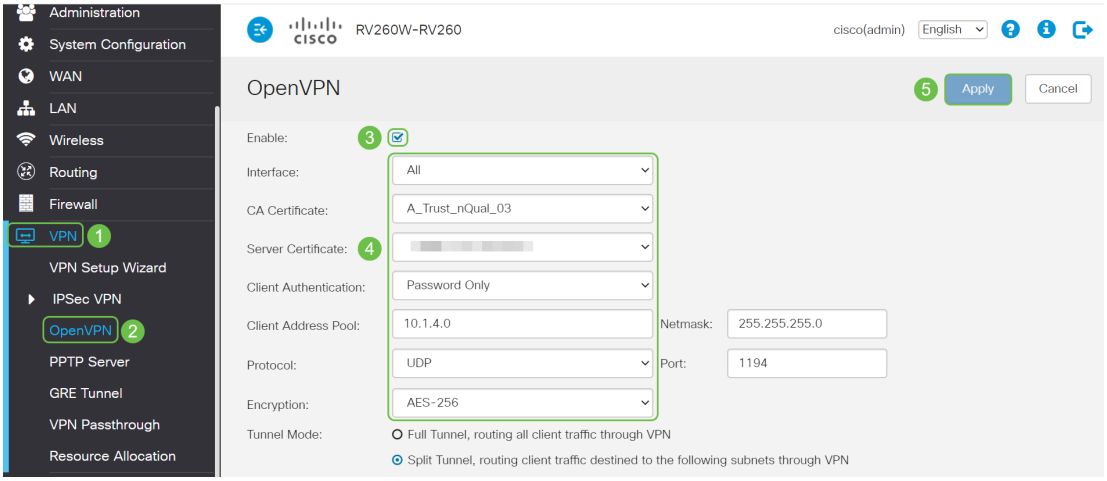


Etapa 17. Navegue até **Administração > Certificado**. O certificado foi carregado.

Note: Neste exemplo, foi usado um servidor de certificado local.



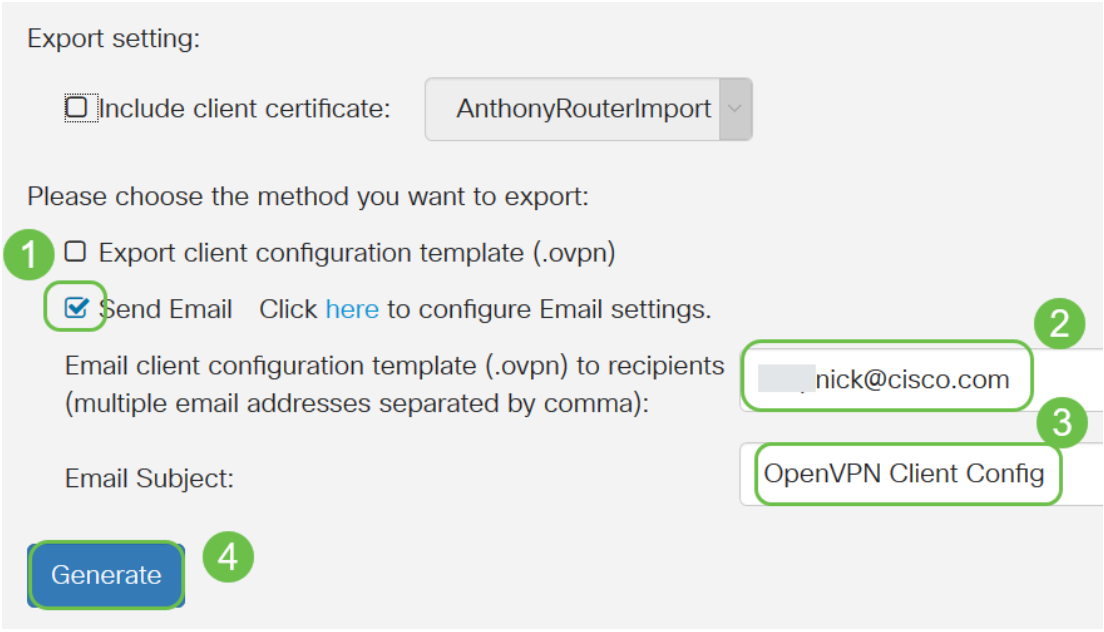
Etapa 18. Navegue até **VPN > OpenVPN**. A página OpenVPN é aberta. Preencha o seguinte com suas informações.



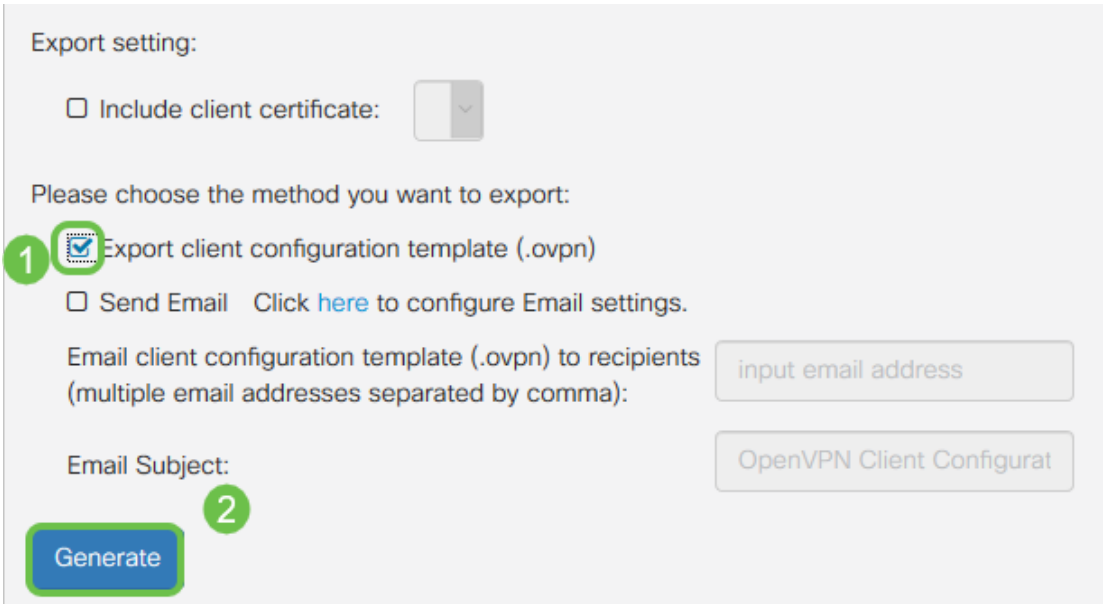
- Marque a caixa *Enable (Habilitar)*. Selecione a Interface que permitirá o tráfego. Nesse caso, uma rede de longa distância (WAN) e selecione um certificado de autoridade de certificação (CA)
- Selecione o *certificado CA* no menu suspenso
- Selecione o *certificado do servidor* baixado no menu suspenso
- Selecione *Autenticação de cliente*. Se você selecionar Senha, eles precisam se autenticar com uma senha. Se você selecionar Senha + Certificado, o cliente também deverá ter um certificado. Isso é mais seguro, mas aumenta o custo da VPN, pois eles precisariam comprar uma CA separada.
- Digite o *pool de endereços de cliente*. Escolha um endereço IP em uma sub-rede de rede que não seja usada em nenhum outro lugar da empresa. Você seleciona os intervalos reservados e escolhe um intervalo que não seja usado em nenhum outro lugar.
- Escolha a forma de *Criptografia*. Certifique-se de que a criptografia seja igual à do cliente. DES e 3DES não são recomendados e devem ser usados apenas para compatibilidade com versões anteriores.
- Escolha o *Modo de Túnel Completo* se quiser que todo o tráfego do cliente passe pelo túnel VPN ou Split se quiser especificar apenas qual tráfego passa pela VPN
- O endereço IP *DNS1* pode ser um servidor DNS interno dedicado, o mesmo endereço IP do gateway padrão fornecido pelo ISP (Provedor de serviços de Internet), em uma máquina virtual ou um servidor DNS confiável na Internet.

Clique em **Apply** para salvar a configuração.

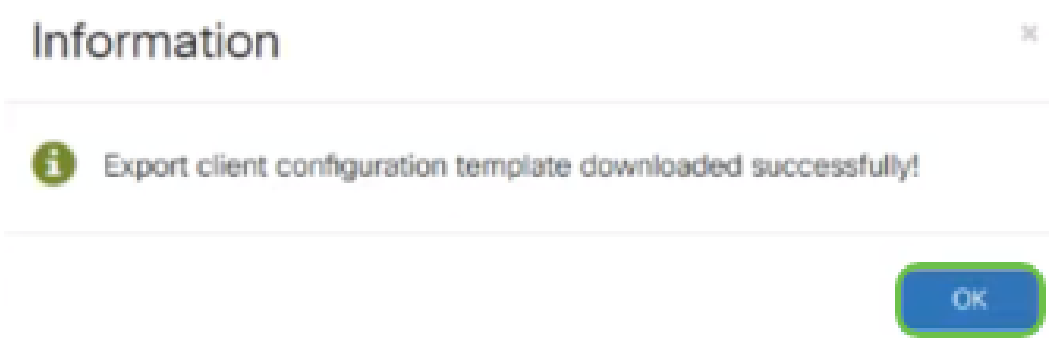
Etapa 19 (Opção 1). Você pode enviar esta configuração por e-mail para o cliente. Marque a caixa *Enviar e-mail*. Digite um endereço de e-mail. Adicione um título de assunto para o e-mail. Clique em **Gerar**.



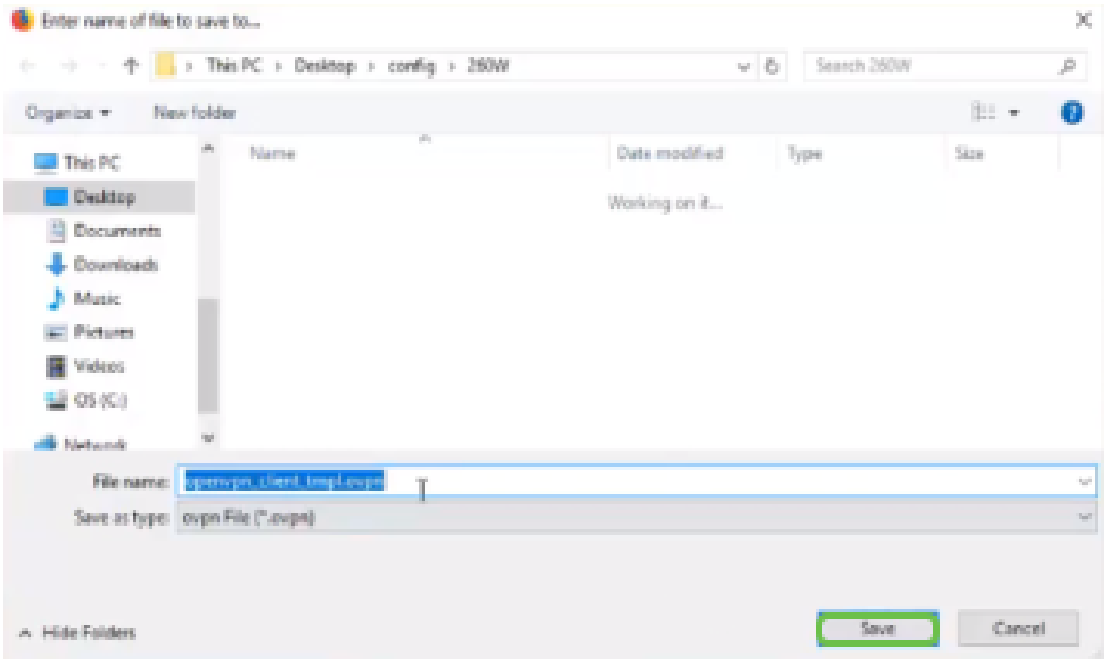
Etapa 20. (Opção 2). Selecione *Exportar modelo de configuração de cliente (.ovpn)* e clique em **Gerar**.



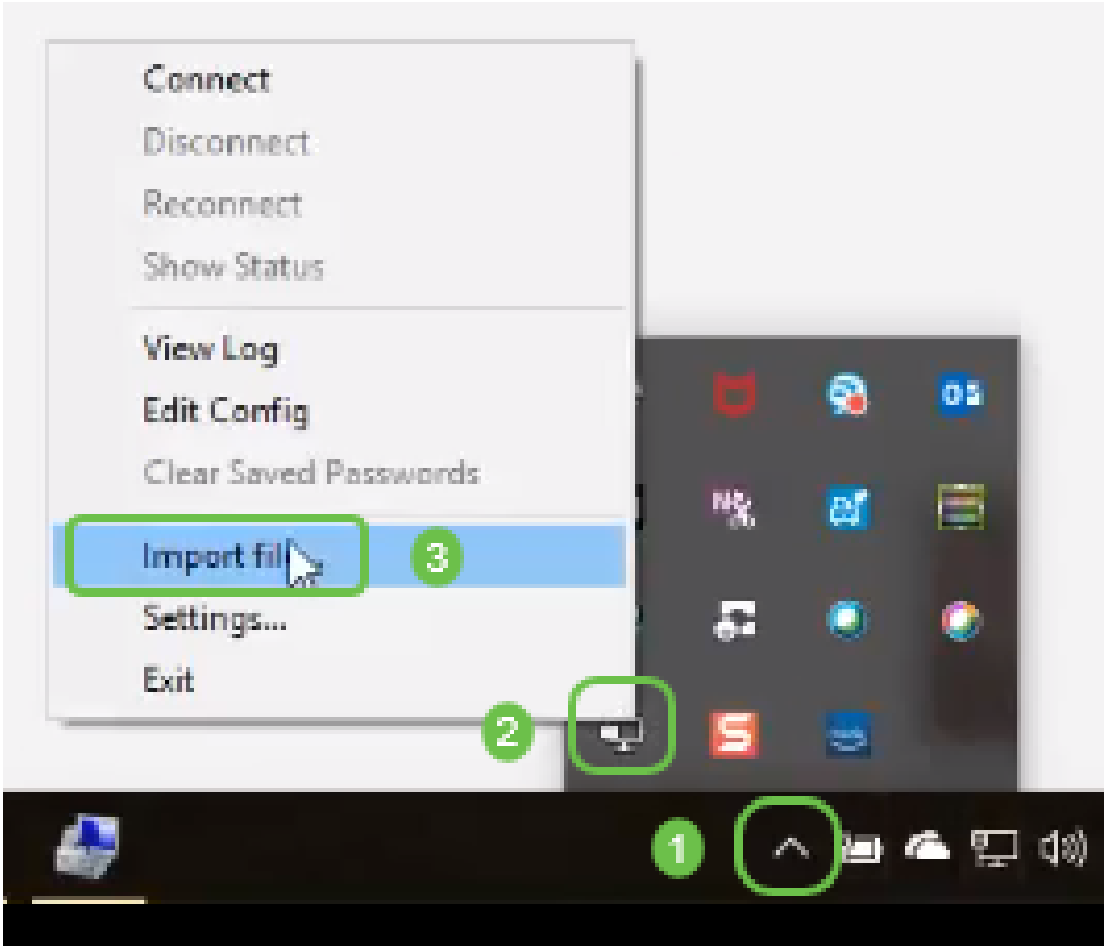
Etapa 21. Você receberá a confirmação de que foi bem-sucedido. Click **OK**.



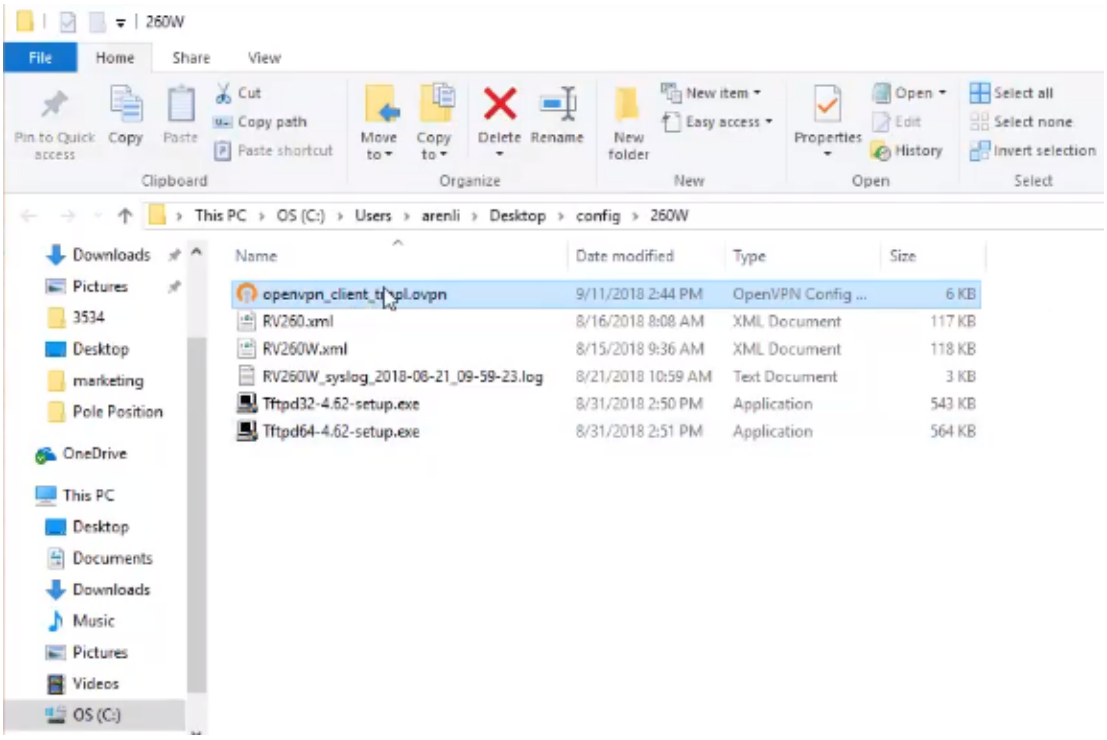
Etapa 22. Click **Save**.



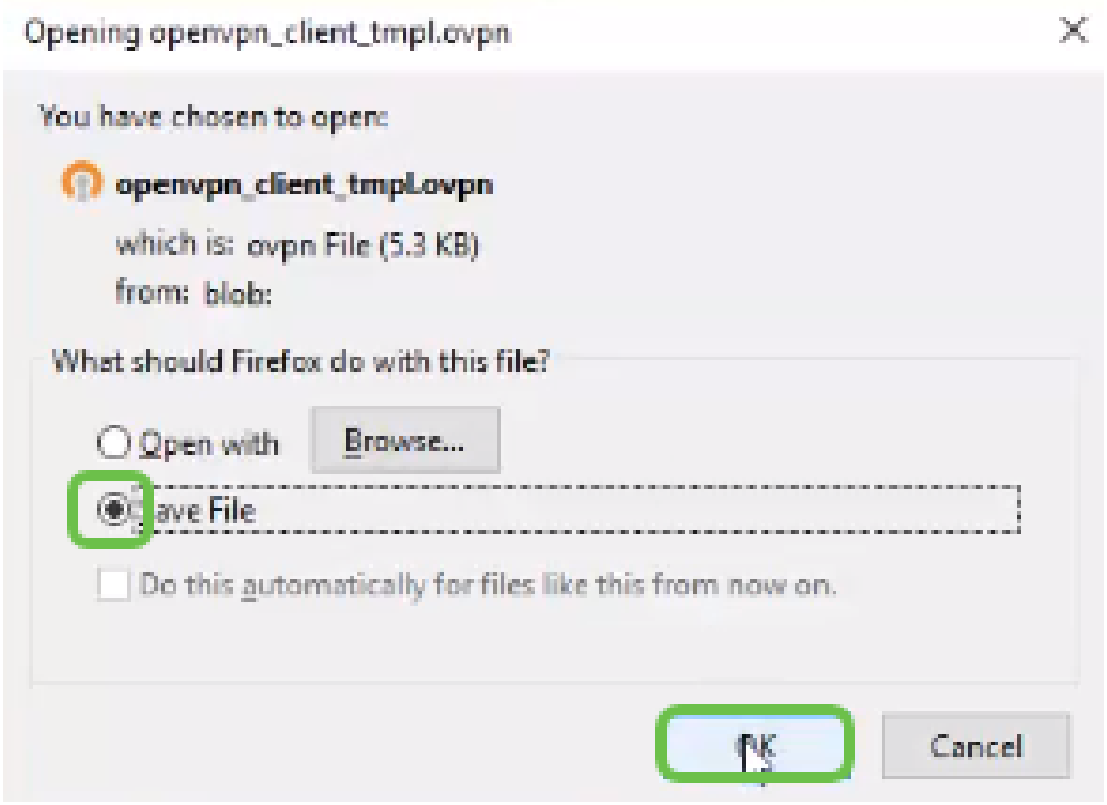
Etapa 23. Na parte inferior direita da área de trabalho e clique para abrir o OpenVPN. Clique com o botão direito do mouse para abrir o menu suspenso. Clique em *Importar arquivo*.



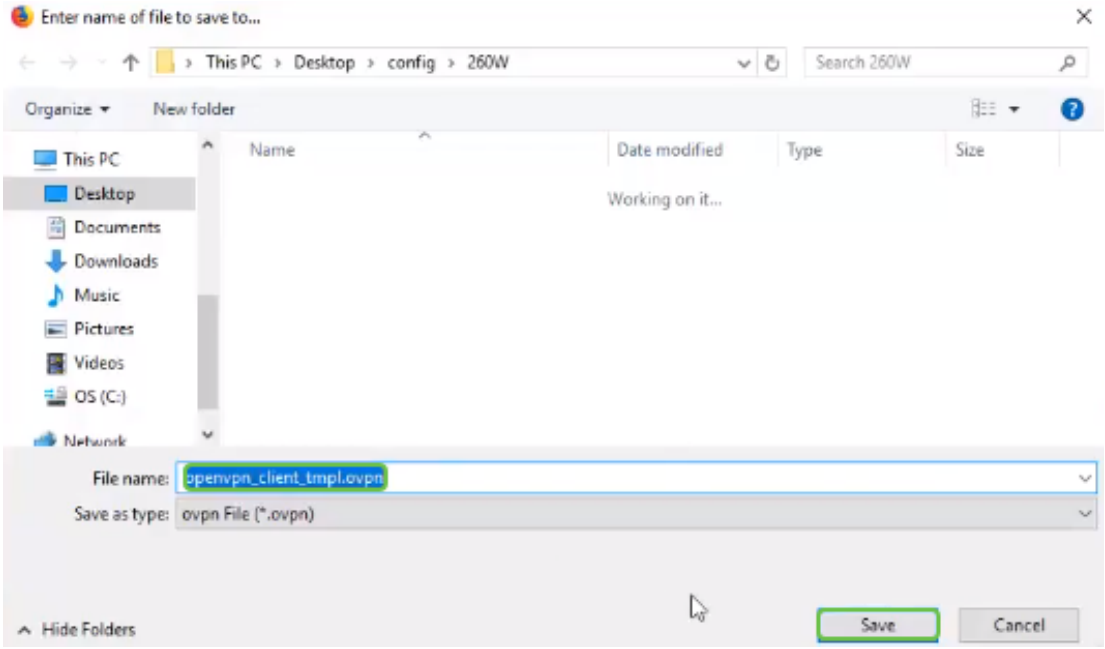
Etapa 24. Selecione o arquivo OpenVPN que termina em *.ovpn*.



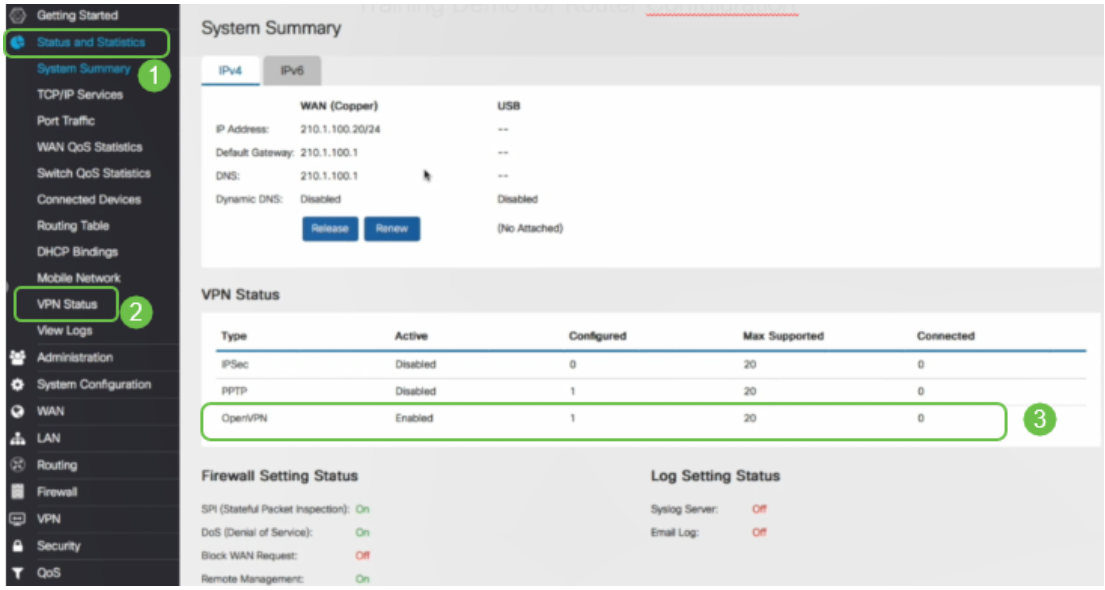
Etapa 25. Clique no botão de opção *Save File (Salvar arquivo)* e clique em **OK**.



Etapa 26. Altere o nome do arquivo se você escolher, mas deixe *.ovpn* no final do nome do arquivo. Click **Save**.



Etapa 27. Navegue até **Status e Statistics > VPN Status**. Você pode rolar para baixo para obter informações mais detalhadas.



O roteador agora está configurado com todos os parâmetros necessários para suportar uma conexão de OpenVPN Client para sua avaliação pessoal.

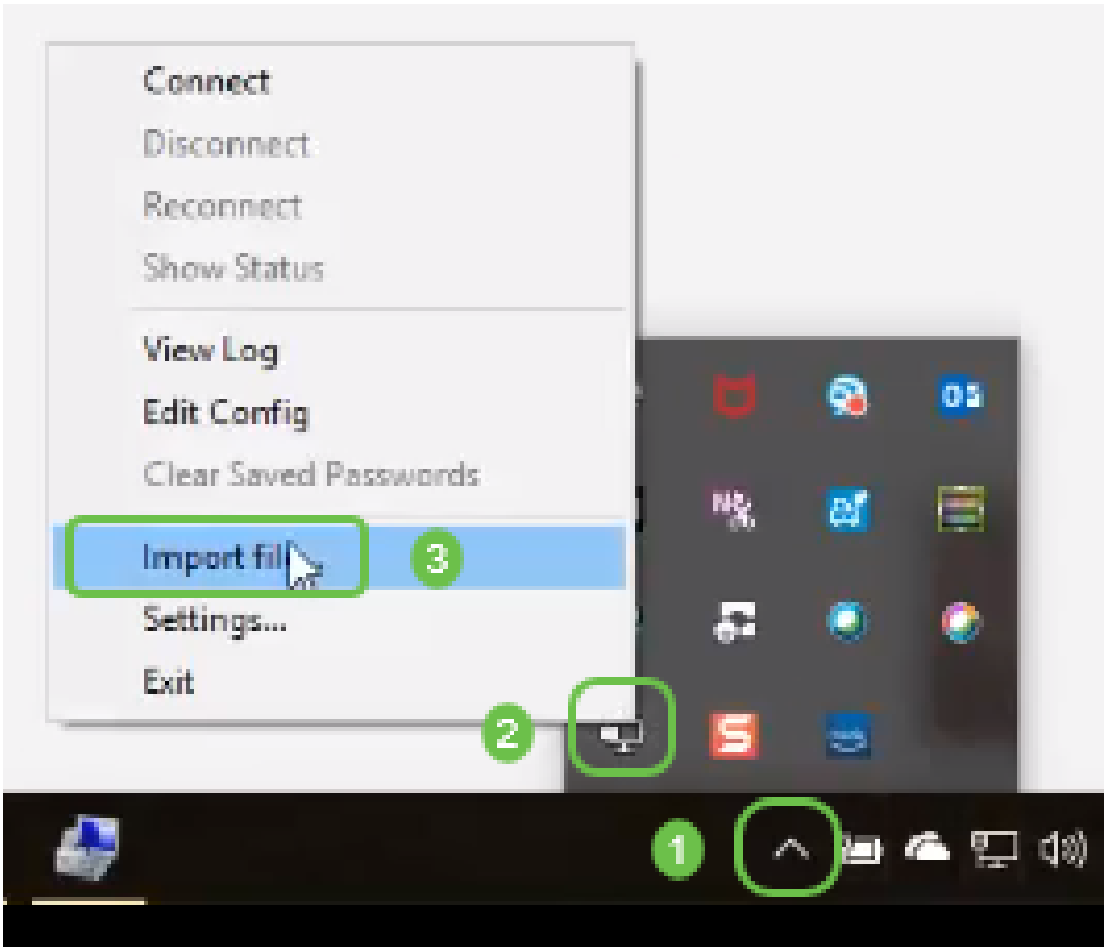
Configuração do OpenVPN Client no Computador

Cada cliente OpenVPN precisa executar as seguintes tarefas como pré-requisito:

- Baixe o aplicativo OpenVPN em seu dispositivo.
- Abra e salve o arquivo de configuração enviado nas etapas 19 a 22 da seção anterior. O arquivo de configuração termina em *.ovpn*.

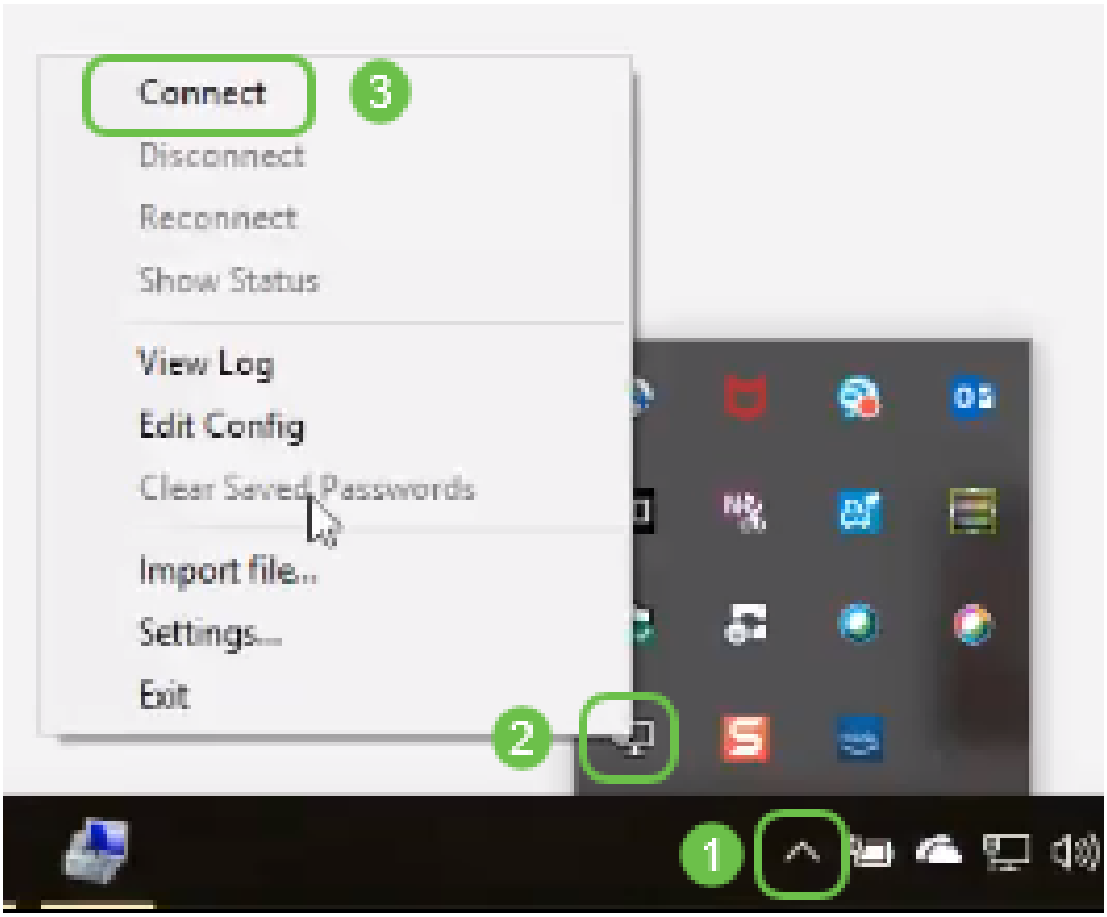
Note: Esta configuração é especificamente para o Windows 10.

Etapa 1. Navegue até o ícone de seta na parte inferior direita da área de trabalho e clique para abrir o ícone OpenVPN. Clique com o botão direito do mouse e selecione *Importar arquivo*.

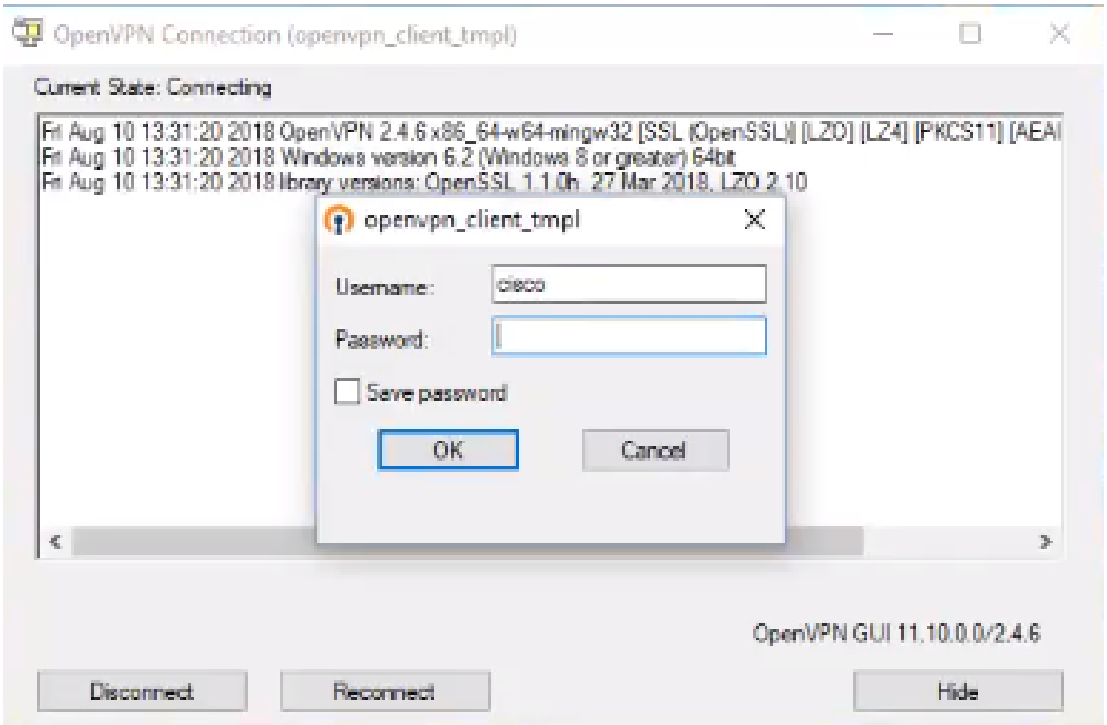


Note: O ícone está preto e branco, indicando que não está em execução no momento. Quando estiver em execução, o ícone aparecerá em cores.

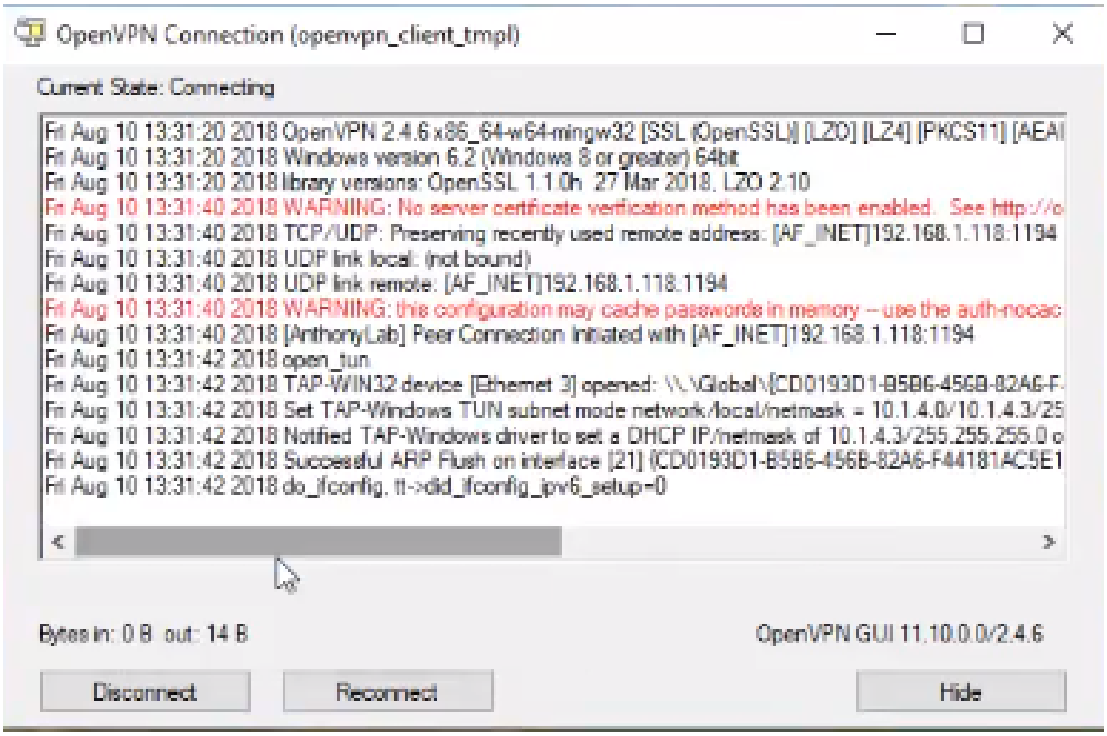
Etapa 2. Clique na *seta para cima*. Clique no ícone OpenVPN. Clique com o botão direito do mouse e selecione *Connect* no menu suspenso.



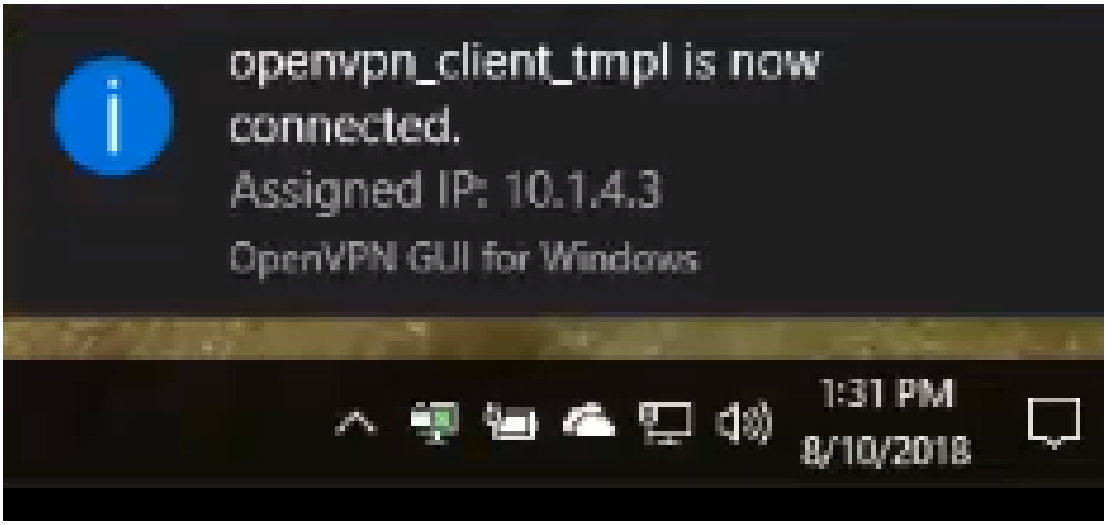
Etapa 3. Digite o nome de usuário e a senha.



Etapa 4. A janela mostrará a conexão do OpenVPN com alguns dados de log.

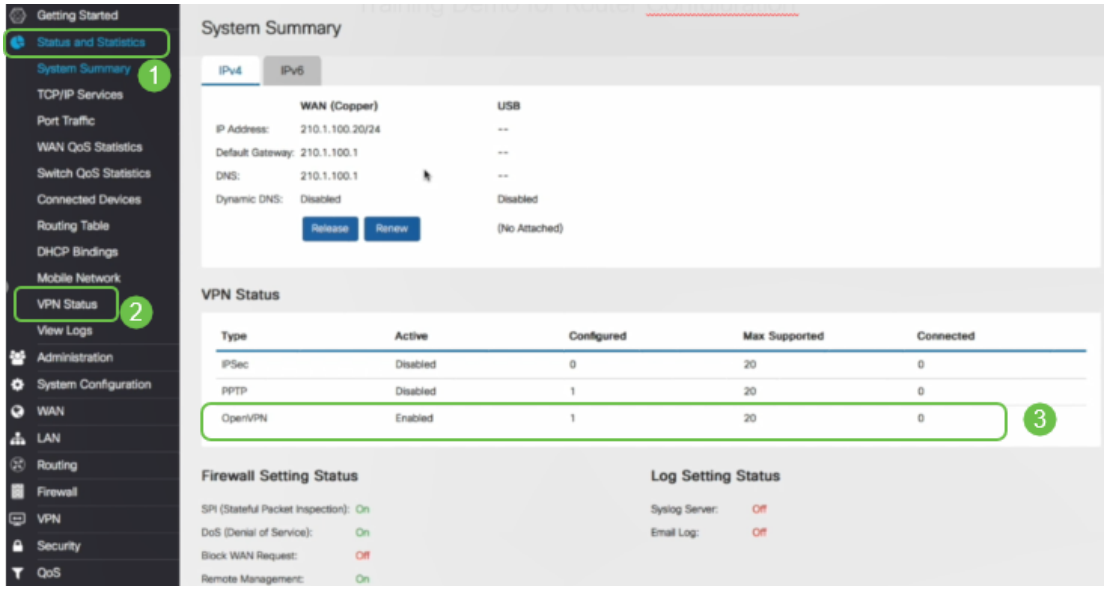


Etapa 5. Um log do sistema deve alertar que há uma conexão.



Etapa 6. O cliente VPN deve ser capaz de fazer com segurança o túnel de informações de entrada e saída por meio do OpenVPN. Isso pode ser definido para se conectar automaticamente nas configurações do OpenVPN.

Passo 7. O administrador pode confirmar o Status da VPN navegando até **Status and Statistics** > **VPN Status** no roteador.



Conclusão

Agora você deve ter instalado com êxito o OpenVPN no roteador RV160 ou RV260 e no site do cliente VPN.

Para discussões da comunidade sobre o OpenVPN, clique aqui e procure o OpenVPN.

Exibir um vídeo relacionado a este artigo...

Clique aqui para ver outras palestras técnicas da Cisco