Configurando a VPN site a site no RV160 e RV260

Objetivo

O objetivo deste documento é criar uma VPN site a site nos roteadores das séries RV160 e RV260.

Introduction

Uma rede virtual privada (VPN) é uma excelente maneira de conectar funcionários remotos a uma rede segura. Uma VPN permite que um host remoto atue como se estivesse conectado à rede protegida no local. Em uma VPN site a site, o roteador local em um local se conecta a um roteador remoto através de um túnel VPN. Esse túnel encapsula dados com segurança usando técnicas de criptografia e autenticação padrão do setor para proteger os dados enviados.

Observe que quando você está configurando VPN site a site, as sub-redes de Rede Local (LAN) em ambos os lados do túnel não podem estar na mesma rede. Por exemplo, se a LAN do Site A usar a sub-rede 192.168.***1***.x/24, o Site B não poderá usar a mesma sub-rede. O site B precisa usar uma sub-rede diferente como 192.168.***2***.x/24.

Para configurar um túnel corretamente, insira as configurações correspondentes (invertendo local e remoto) ao configurar os dois roteadores. Suponha que esse roteador esteja identificado como Roteador A. Insira suas configurações na seção Local Group Setup (Configuração do grupo local) ao inserir as configurações para o outro roteador (Roteador B) na seção Remote Group Setup (Configuração do grupo remoto). Ao configurar o outro roteador (Roteador B), insira suas configurações na seção Local Group Setup (Configuração do grupo local) e insira as configurações do Roteador A na Remote Group Setup (Configuração do grupo remoto).

Abaixo está uma tabela da configuração do Roteador A e do Roteador B, destacada em negrito, estão os parâmetros que são o inverso do roteador oposto. Todos os outros parâmetros restantes são configurados da mesma forma. Neste documento, configuraremos o roteador local usando o Roteador A.

Campos	Roteador A (local) Endereço IP da WAN: 140.x.x.x Endereço IP local: 192.168.2.0/24	Roteador B (remoto) Endereço IP da WAN: 145.x.x.x Endereço IP local: 10.1.1.0/24
Nome da conexão	**VPNTest**	**VPNTestB**
Perfil de IPSec	**HomeOffice (Tem a mesma configuração que o RemoteOffice)**	**RemoteOffice (Tem a mesma configuração que HomeOffice)**
Interface	WAN	WAN
Ponto Final Remoto	**IP estático: 145.x.x.x**	**IP estático: 140.x.x.x**
Método de autenticação IKE	Chave pré-compartilhada Chave pré-compartilhada: Teste Cisco123!	Chave pré-compartilhada Chave pré-compartilhada: Teste Cisco123!
Tipo de	IP WAN local	IP WAN local

identificador local		
Identificador local	**140.x.x.x**	**145.x.x.x**
Tipo de IP local	Sub-rede	Sub-rede
Endereço IP local	**192.168.2.0**	**10.1.1.0**
Máscara de sub-rede local	255.255.255.0	255.255.255.0
Tipo de identificador remoto	IP WAN remoto	IP WAN remoto
Identificador remoto	**145.x.x.x**	**140.x.x.x**
Tipo de IP remoto	Sub-rede	Sub-rede
Endereço IP remoto	**10.1.1.0**	**192.168.2.0**
Máscara de sub-rede remota	255.255.255.0	255.255.255.0
Modo agressivo	Desabilitado	Desabilitado

Para saber como configurar o perfil IPsec, consulte o artigo sobre: Configurando perfis IPSec (modo de chaveamento automático) no RV160 e RV260.

Para configurar a VPN site a site usando o assistente de configuração, consulte o artigo sobre: Configurando o Assistente de configuração de VPN no RV160 e RV260.

Dispositivos aplicáveis

- RV160
- RV260

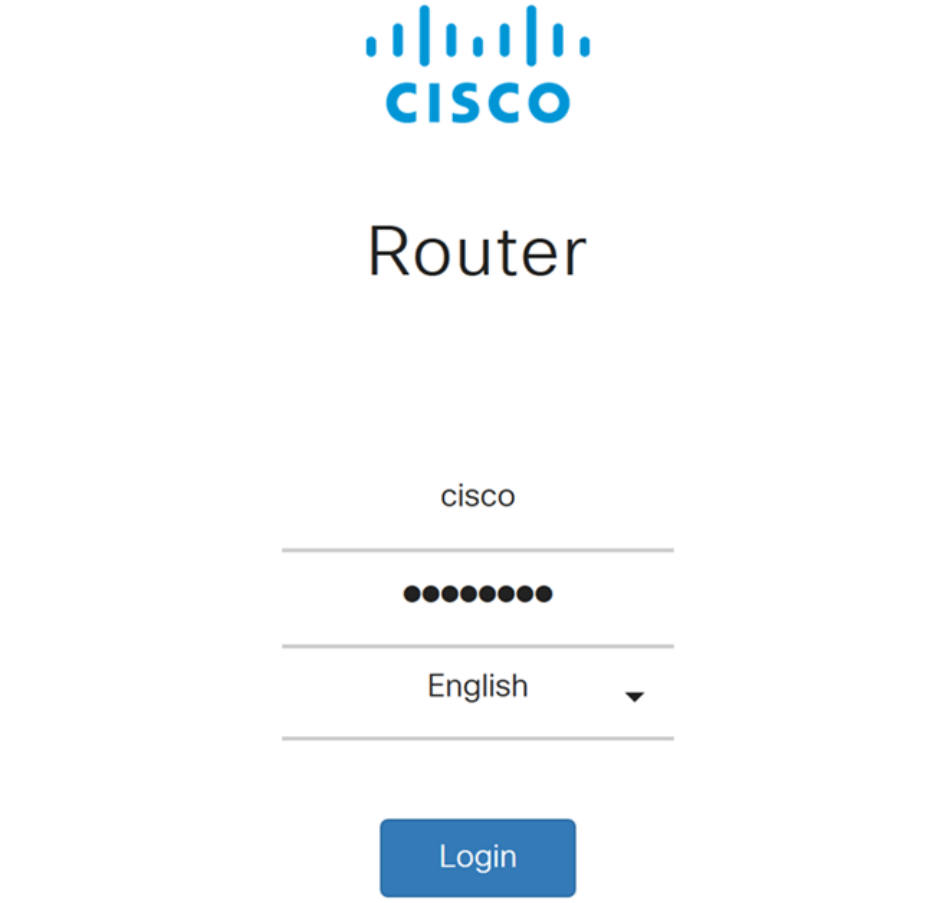
Versão de software

- 1.0.00.13

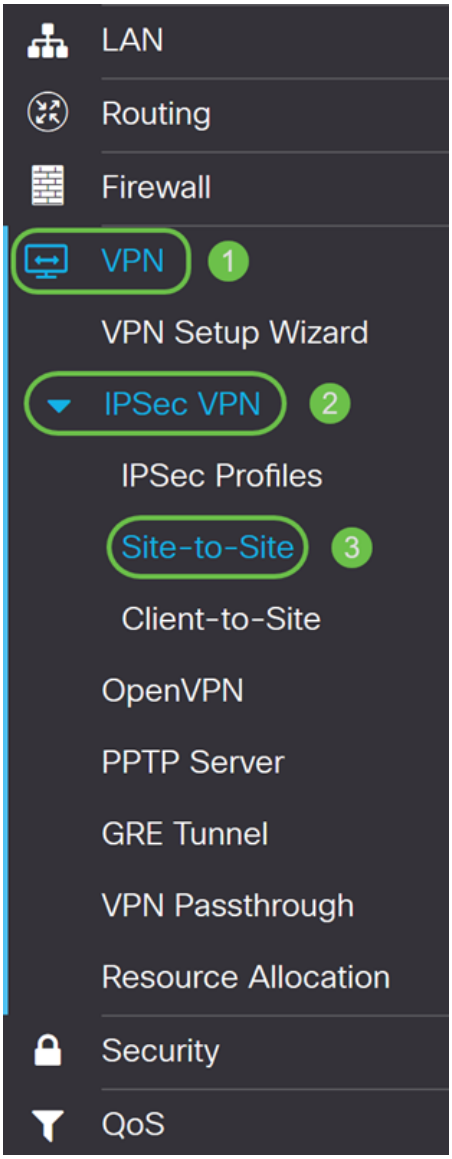
Configurando a conexão VPN site a site - Roteador A

Etapa 1. Faça login na página de configuração da Web do roteador A.

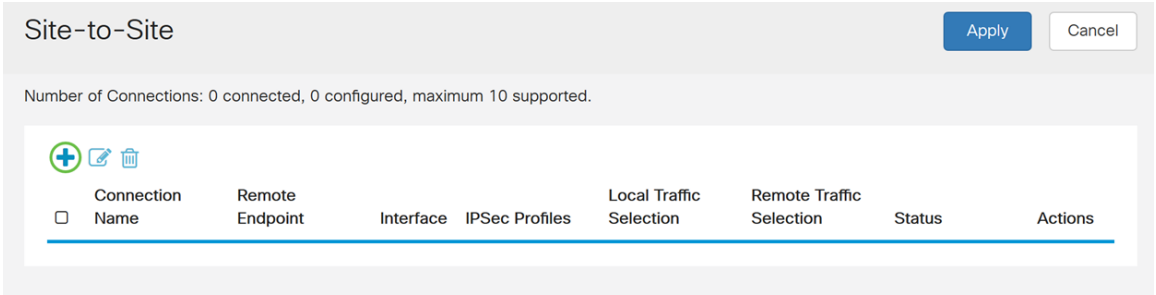
Note: Usaremos RV160 para ambos os roteadores.



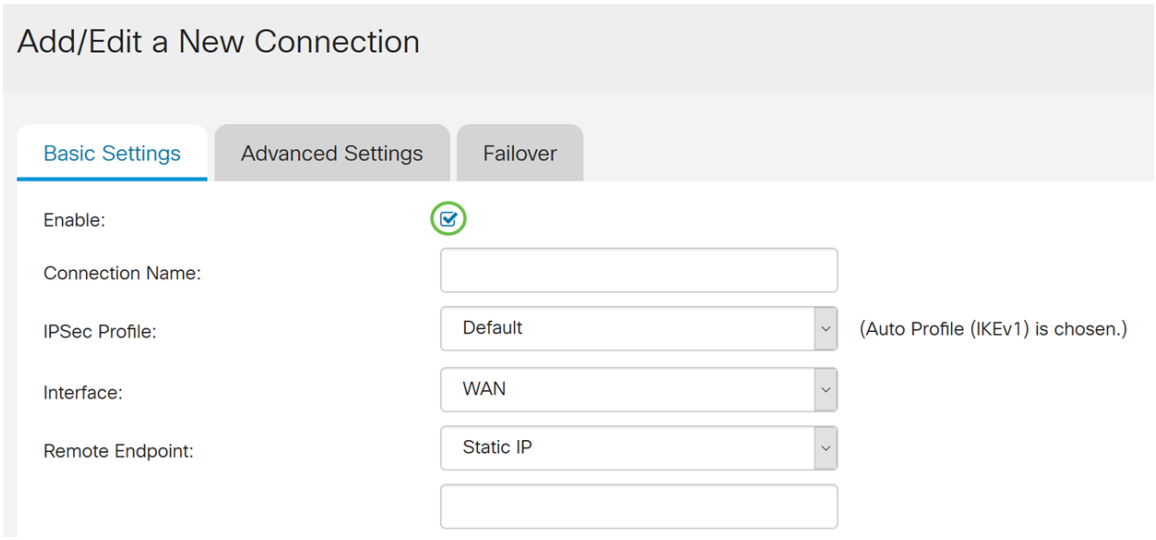
Etapa 2. Navegue até **VPN > IPSec VPN > Site-to-Site**.



Etapa 3. Clique no botão **adicionar** para adicionar uma nova conexão VPN Site a Site.

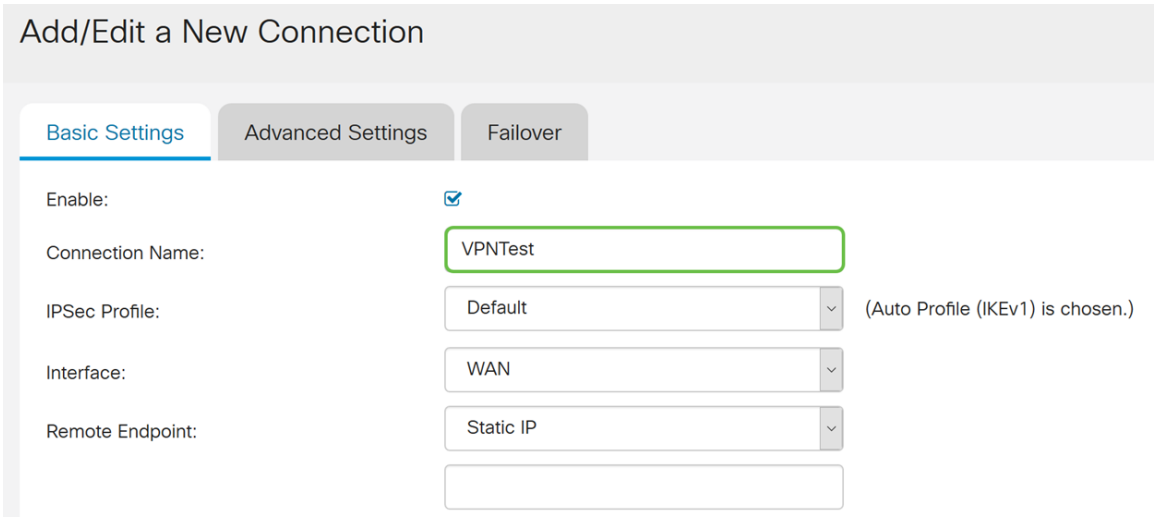


Etapa 4. Marque **Habilitar** para habilitar a configuração. Iss está habilitado por padrão.



Etapa 5. Insira um nome de conexão para o túnel VPN. Essa descrição é para fins de referência e não precisa corresponder ao nome usado na outra extremidade do túnel.

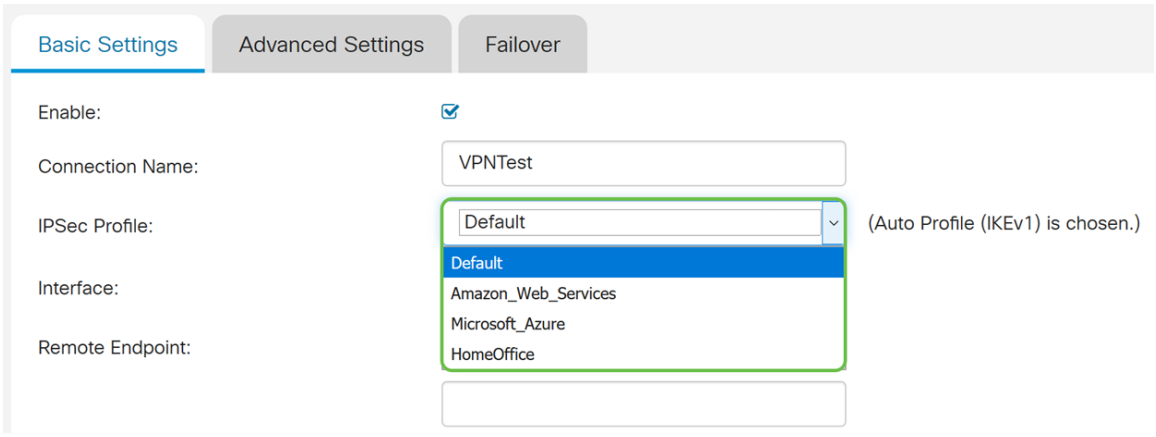
Neste exemplo, vamos inserir **VPNTest** como nosso nome de conexão.



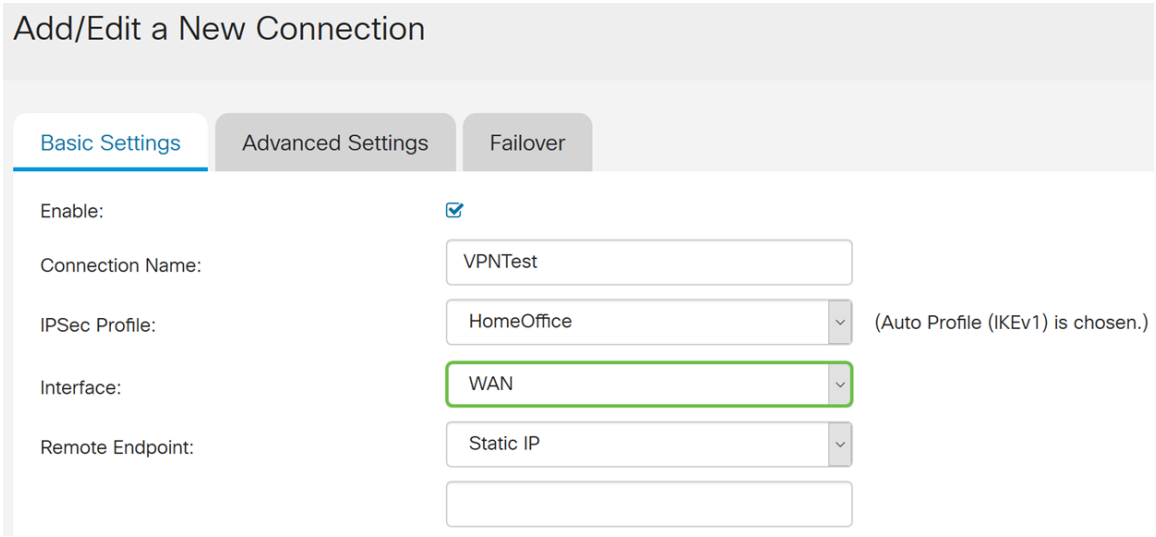
Etapa 6. Se você criou um novo perfil de IPsec ou deseja usar um pré-criado (Amazon_Web_Services, Microsoft_Azure), selecione o perfil de IPsec que deseja usar para a VPN. O padrão - perfil automático é escolhido por padrão. O perfil IPsec é a configuração central no IPsec que define os algoritmos como criptografia, autenticação e grupo Diffie-Hellman (DH) para a negociação da Fase I e da Fase II.

Para este exemplo, selecionaremos **HomeOffice** como nosso perfil IPsec.

Note: Para saber mais sobre como criar um perfil IPsec, consulte o artigo: Configurando perfis IPSec (modo de chaveamento automático) no RV160 e RV260.

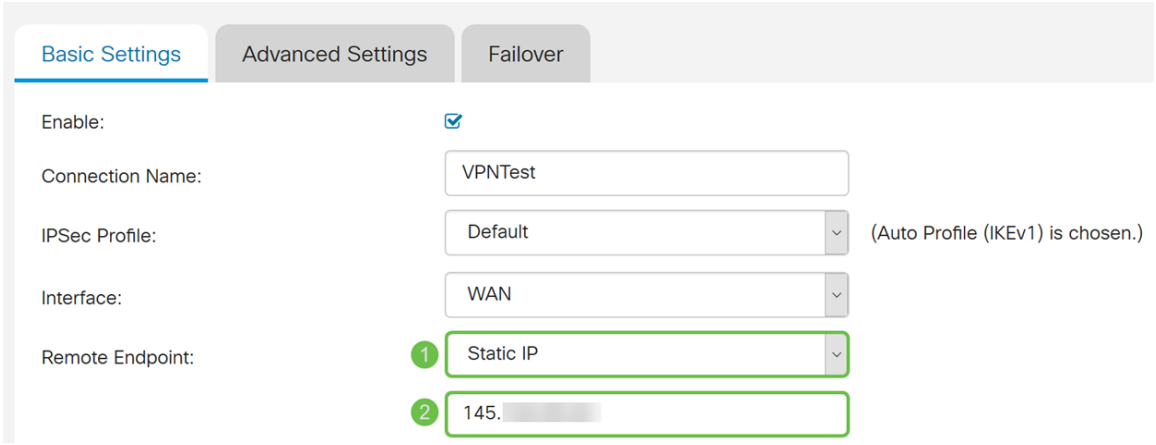


Passo 7. No campo *Interface*, selecione a interface usada para o túnel. Neste exemplo, usaremos a **WAN** como interface.



Etapa 8. Selecione **IP estático**, **Nome de domínio totalmente qualificado (FQDN)** ou **IP dinâmico** para o *endpoint remoto*. Digite o endereço IP ou FQDN do endpoint remoto com base na sua seleção.

Selecionamos o **IP estático** e inserimos em nosso endereço IP de endpoint remoto.



Configurando o método de autenticação IKE

Etapa 1. Selecione **Pre-shared Key** ou **Certificate**. Para esta demonstração, selecionaremos a **chave pré-compartilhada** como nosso método de autenticação IKE.

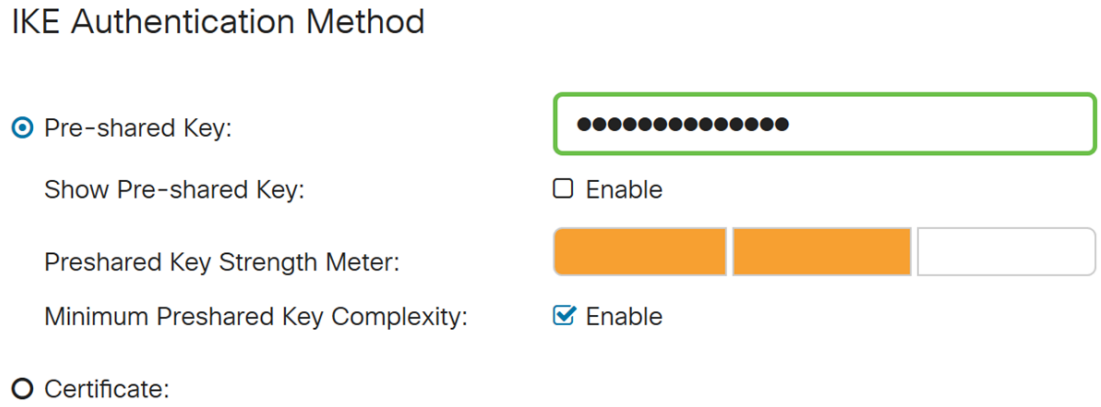
Os pares IKE autenticam-se uns aos outros através da computação e do envio de hash chaveado de dados que inclui a chave pré-partilhada. Se o peer receptor for capaz de criar o mesmo hash independentemente usando sua chave pré-compartilhada, ele saberá que

ambos os pares devem compartilhar o mesmo segredo, autenticando o outro peer. As chaves pré-compartilhadas não escalam bem porque cada peer IPsec deve ser configurado com a chave pré-compartilhada de cada outro peer com o qual estabelece uma sessão.

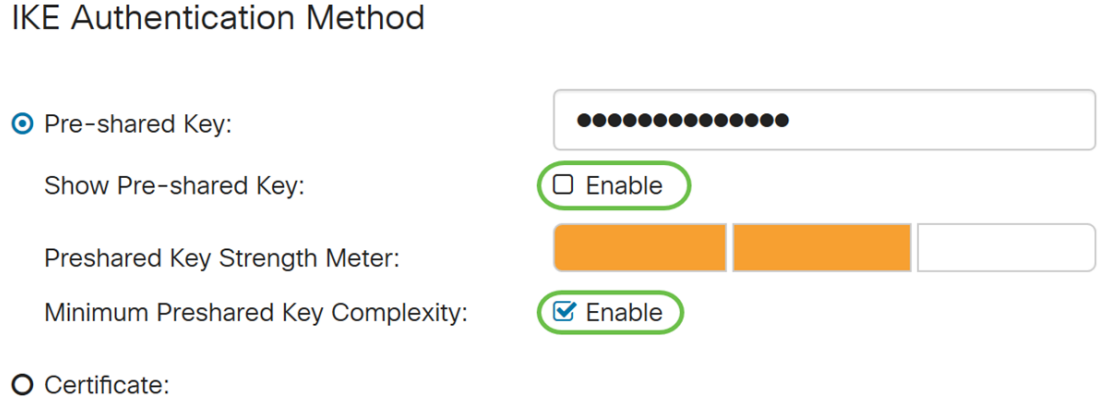
O certificado digital é um pacote que contém informações como a identificação de um portador de certificado: nome ou endereço IP, número de série do certificado, data de expiração do certificado e uma cópia da chave pública do portador do certificado. O formato padrão do certificado digital é definido na especificação X.509. A versão 3 do X.509 define a estrutura de dados para os certificados. Se tiver selecionado **Certificado**, certifique-se de que o certificado assinado foi importado em **Administração > Certificado**. Selecione o certificado na lista suspensa para local e remoto.

Etapa 2. No campo *Pre-shared Key*, insira uma chave pré-compartilhada.

Note: Certifique-se de que o roteador remoto use a mesma chave pré-compartilhada.

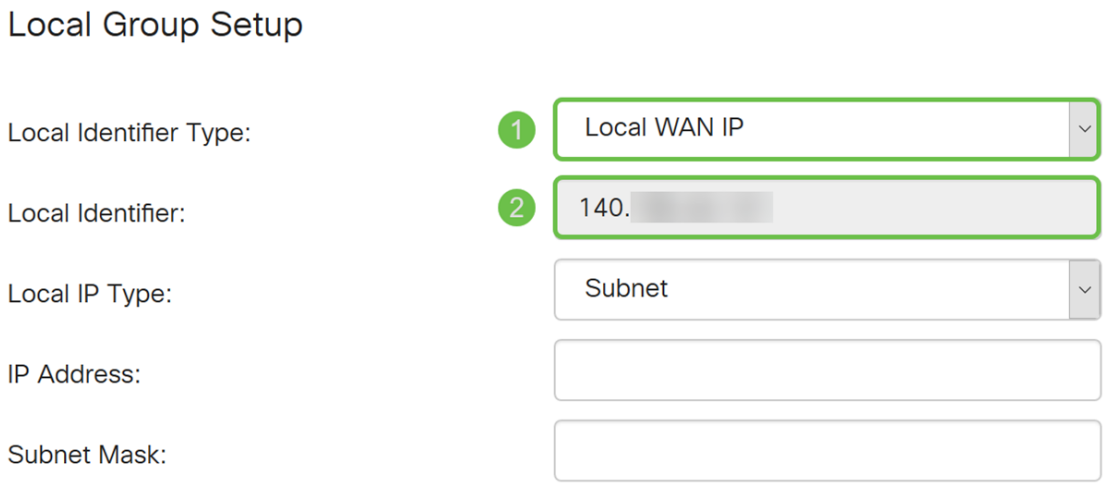


Etapa 3. Marque a caixa de seleção **Habilitar** se quiser exibir a chave pré-compartilhada. O *Medidor de força da chave pré-compartilhada* mostra a força da chave pré-compartilhada através de barras coloridas. Marque **Enable (Habilitar)** para habilitar a complexidade mínima de chave pré-compartilhada. Em seguida, vá para a seção *Para configuração de grupo local* .



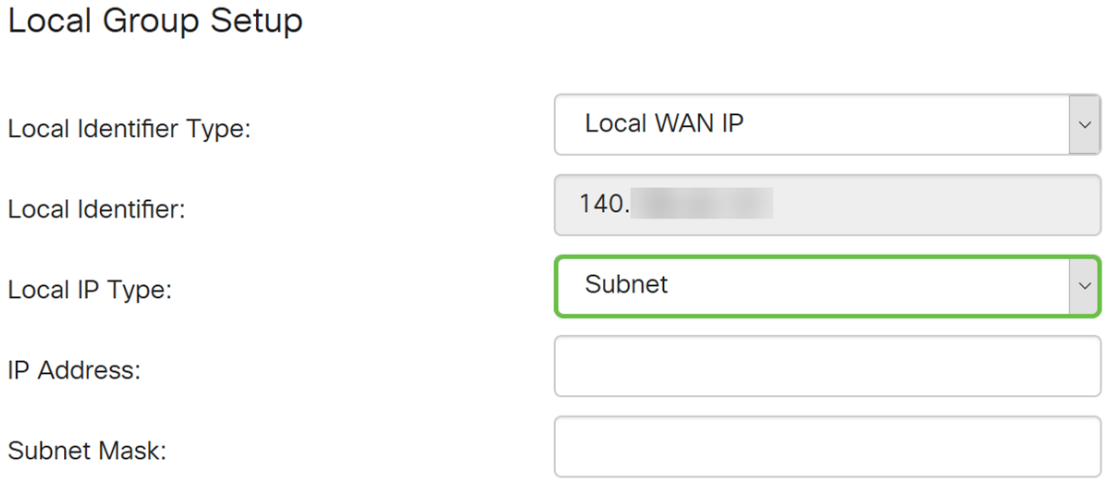
Para configuração de grupo local

Etapa 1. Selecione **Local WAN IP**, **IP Address**, **Local FQDN** ou **Local User FQDN** na lista suspensa. Insira o nome do identificador ou o endereço IP com base na sua seleção. Se você selecionou o **IP da WAN local**, o endereço IP da WAN do roteador deve ser inserido automaticamente.



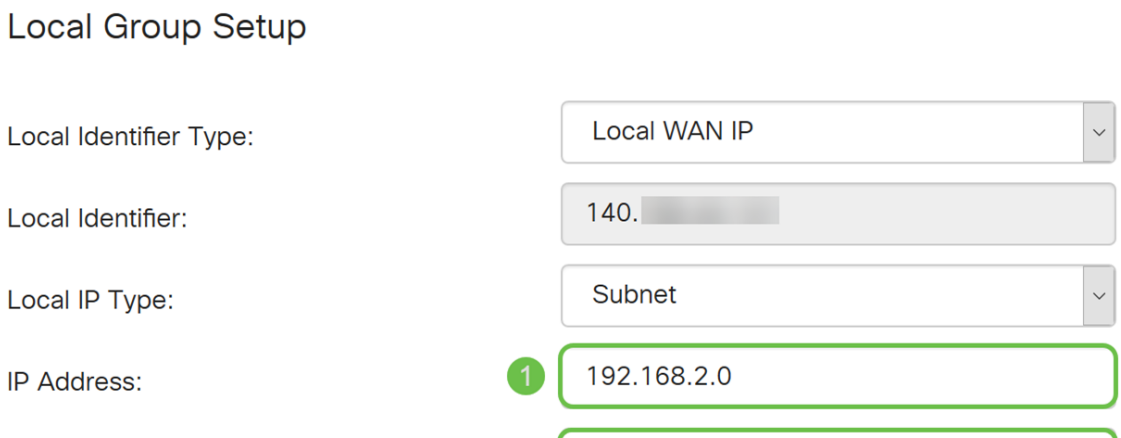
Etapa 2. Para o Tipo de IP Local, selecione Sub-rede, Única, **Qualquer**, **Grupo IP** ou **Interface GRE** na lista suspensa.

Neste exemplo, a **Sub-rede** foi escolhida.



Etapa 3. Insira o endereço IP do dispositivo que pode usar este túnel. Em seguida, insira a máscara de sub-rede.

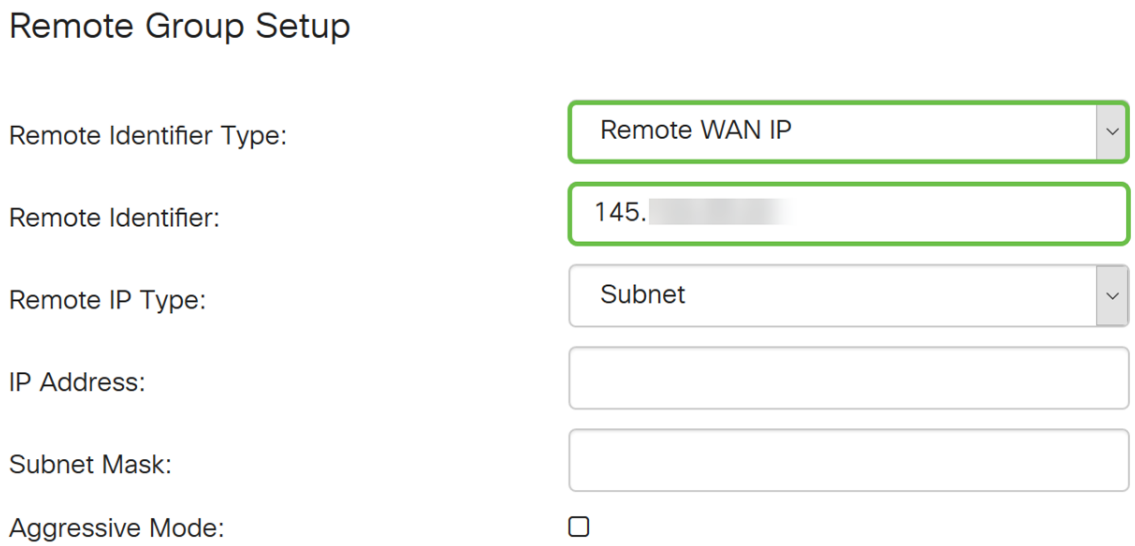
Para esta demonstração, vamos inserir **192.168.2.0** como nosso endereço IP local e **255.255.255.0** para a máscara de sub-rede.



Configuração do grupo remoto

Etapa 1. Selecione **Remote WAN IP**, **Remote FQDN** ou **Remote User FQDN** na lista suspensa. Insira o nome do identificador ou o endereço IP com base na sua seleção.

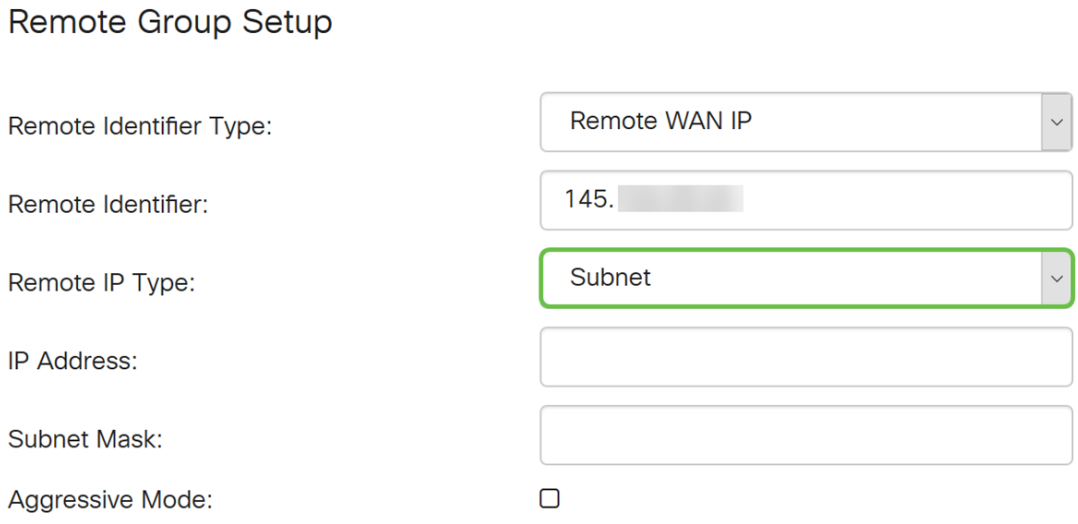
Selecionamos o **IP da WAN remota** como nosso *Tipo de Identificador Remoto* e inserimos o endereço IP do roteador remoto.



Etapa 2. Selecione Sub-rede, **Única**, **Qualquer Grupo IP** na lista suspensa Tipo de IP Remoto.

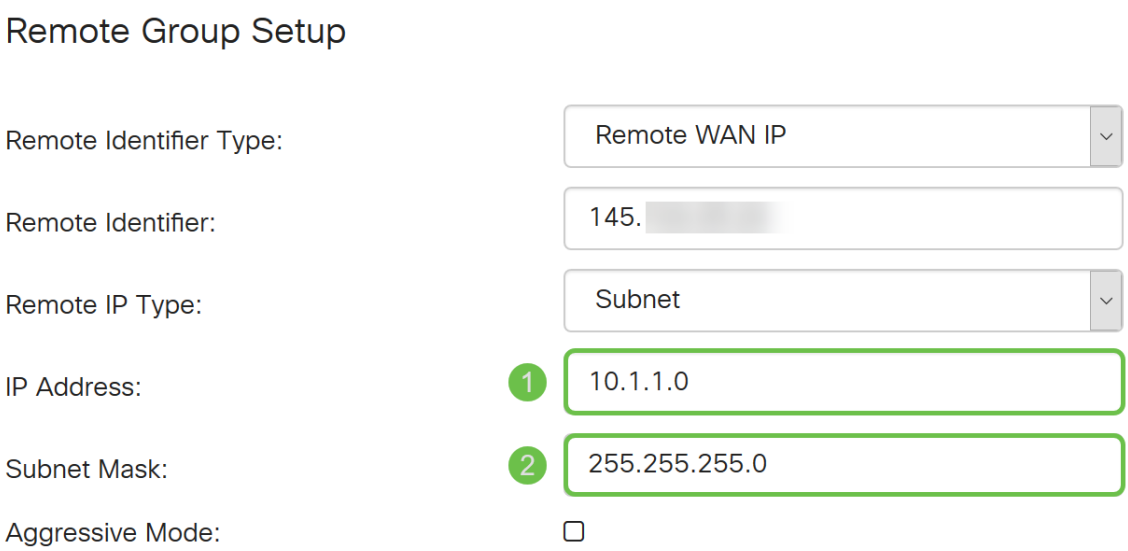
Neste exemplo, selecionaremos **Sub-rede**.

Note: Se você tiver selecionado Grupo IP como seu tipo IP remoto, uma janela pop-up para criar um novo grupo IP será exibida.



Etapa 3. Insira o endereço IP local remoto e a máscara de sub-rede do dispositivo que pode usar esse túnel.

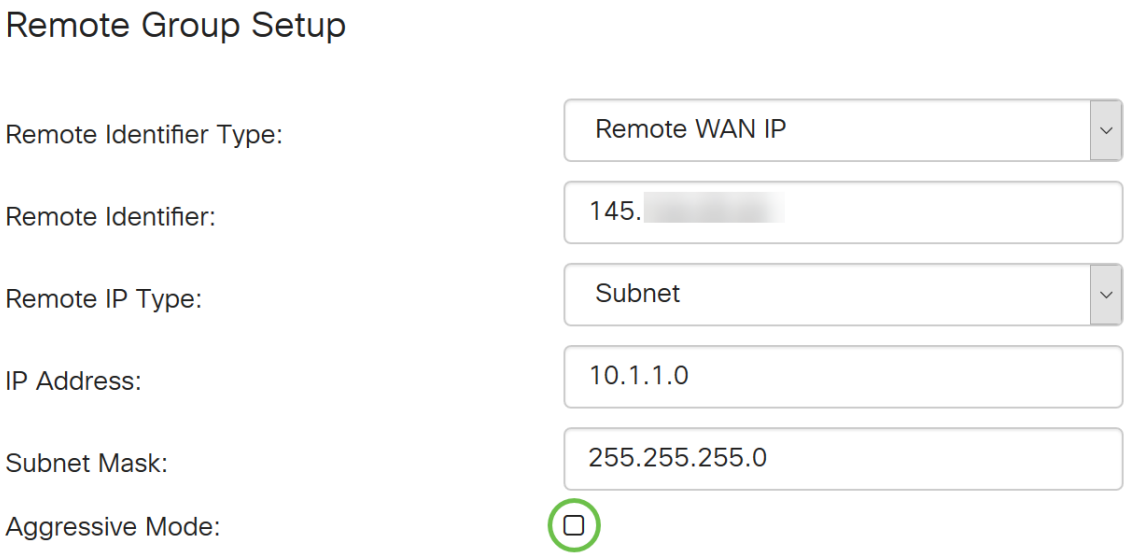
Nós inserimos **10.1.1.0** para o endereço IP local remoto que pode usar esse túnel e a máscara de sub-rede de **255.255.255.0**.



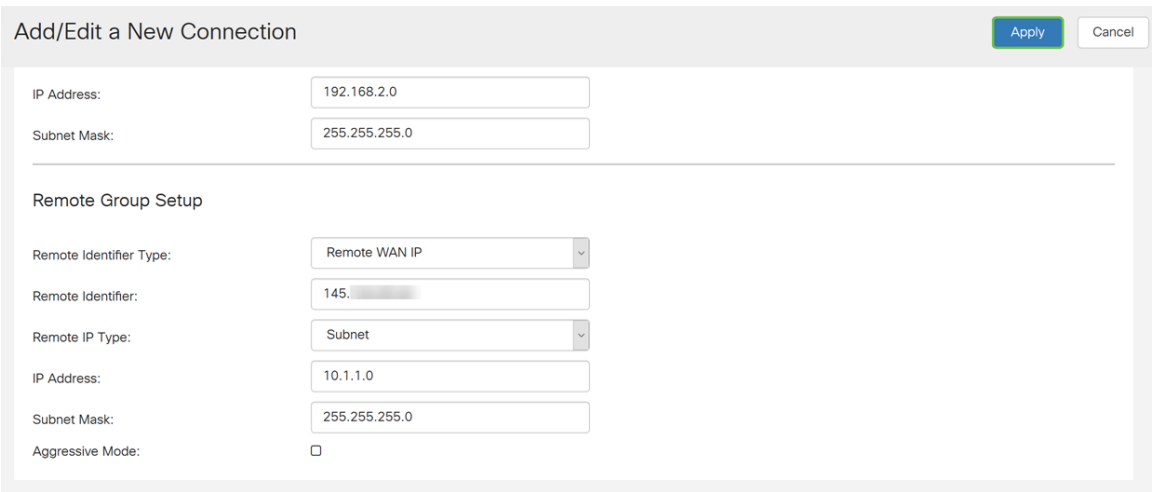
Etapa 4. Marque a caixa para ativar o modo agressivo. O modo agressivo é quando a negociação para SA IKE é compactada em três pacotes com todos os dados exigidos pela SA a serem passados pelo iniciador. A negociação é mais rápida, mas eles têm uma vulnerabilidade de trocar identidades em texto claro.

Neste exemplo, nós o deixaremos desmarcado.

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



Etapa 5. Clique em **Apply** para criar uma nova conexão VPN site a site.

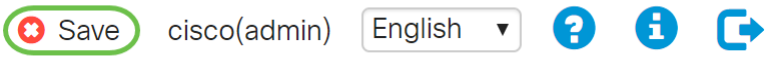


Conclusão

Agora você deve ter adicionado com êxito uma nova conexão VPN de site a site para o roteador local. Você precisaria configurar seu roteador remoto (Roteador B) usando as informações inversas.

Todas as configurações que o roteador está usando no momento estão no arquivo Running Configuration, que é volátil, no sentido de que não é retido entre as reinicializações.

Etapa 1. Na parte superior da página, clique no botão **Salvar** para navegar até o *Gerenciamento de configuração* para salvar sua configuração atual na configuração de inicialização. Isso serve para manter a configuração entre as reinicializações.



Etapa 2. No Gerenciamento de configuração, verifique se a *fonte* está **executando a configuração** e se o *destino* está **iniciando a configuração**. Em seguida, pressione **Apply** para salvar sua configuração atual na configuração de inicialização. Todas as configurações que o roteador está usando no momento estão no arquivo Running Configuration, que é volátil e não é retido entre as reinicializações. Copiar o arquivo de configuração atual para o arquivo de configuração de inicialização manterá toda a configuração entre as reinicializações.