Configurar a conectividade da rede virtual privada (VPN) do AnyConnect no roteador da série RV34x

Objetivo

O objetivo deste documento é mostrar como configurar a conectividade VPN do AnyConnect no roteador RV34x Series.

Vantagens de usar o AnyConnect Secure Mobility Client:

1. Conectividade segura e persistente
2. Segurança persistente e aplicação de políticas
3. Implantável a partir do Adaptive Security Appliance (ASA) ou de Sistemas de Implantação de Software Corporativo
4. Personalizável e traduzível
5. Fácil configuração
6. Suporta IPSec (Internet Protocol Security) e SSL (Secure Sockets Layer)
7. Suporta o protocolo Internet Key Exchange versão 2.0 (IKEv2.0)

Introduction

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

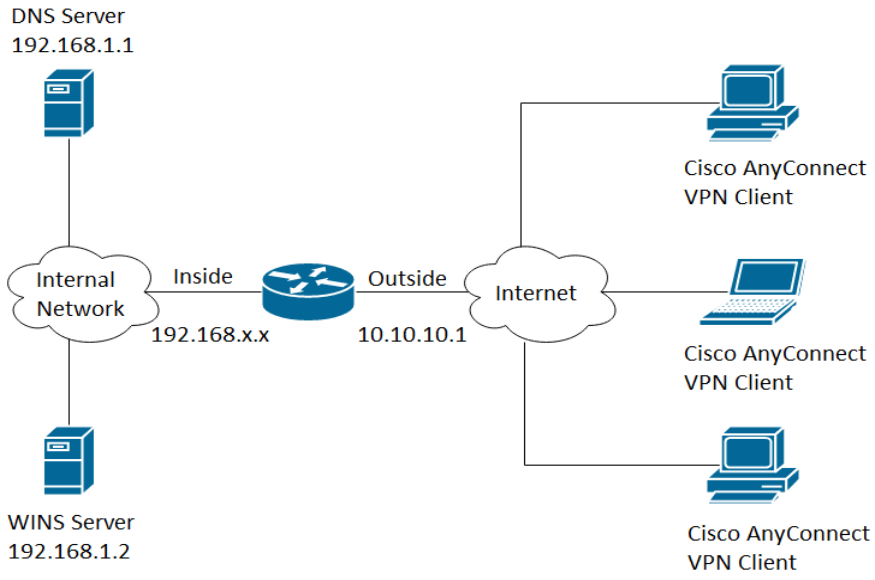
Um cliente VPN é um software instalado e executado em um computador que deseja se conectar à rede remota. Esse software cliente deve ser configurado com a mesma configuração do servidor VPN, como o endereço IP e as informações de autenticação. Essas informações de autenticação incluem o nome de usuário e a chave pré-compartilhada que será usada para criptografar os dados. Dependendo da localização física das redes a serem conectadas, um cliente VPN também pode ser um dispositivo de hardware. Isso geralmente acontece se a conexão VPN for usada para conectar duas redes que estão em locais separados.

O Cisco AnyConnect Secure Mobility Client é um aplicativo de software para conexão com uma VPN que funciona em vários sistemas operacionais e configurações de hardware. Este aplicativo de software possibilita que recursos remotos de outra rede se tornem acessíveis como se o usuário estivesse diretamente conectado à sua rede, mas de uma forma segura. O Cisco AnyConnect Secure Mobility Client oferece uma nova maneira inovadora de proteger usuários móveis em plataformas baseadas em computador ou de smartphone, fornecendo uma experiência mais contínua e sempre protegida para usuários finais e aplicação de política abrangente para o administrador de TI.

No roteador RV34x, começando com a versão do firmware 1.0.3.15 e avançando, o licenciamento do AnyConnect não é necessário. Haverá uma cobrança somente para licenças de cliente.

Para obter informações adicionais sobre o licenciamento do AnyConnect nos roteadores da série RV340, consulte o artigo sobre: licenciamento do AnyConnect para os roteadores da série RV340

.



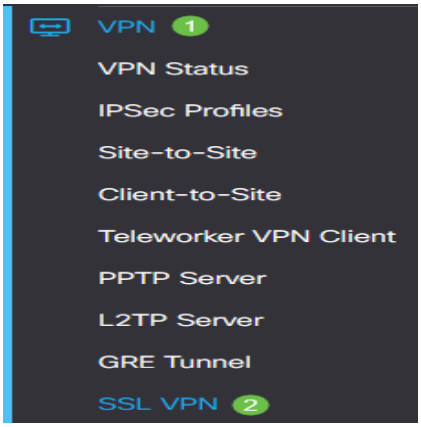
Dispositivos aplicáveis | Versão do firmware

- Cisco AnyConnect Secure Mobility Client | 4.4 (Download mais recente)
- Série RV34x | 1.0.03.15 (Baixe o mais recente)

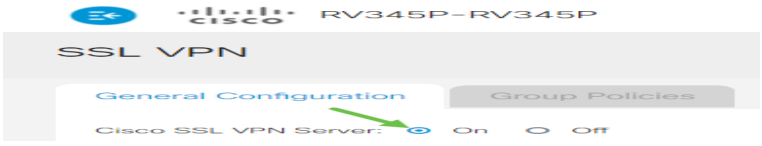
Configurar a conectividade do AnyConnect VPN no RV34x

Configure a VPN SSL no RV34x

Etapa 1. Acesse o utilitário baseado na Web do roteador e escolha **VPN > SSL VPN**.



Etapa 2. Clique no botão de opção **On** para habilitar o Cisco SSL VPN Server.



Configurações de Gateway Obrigatórias

As seguintes definições de configuração são obrigatórias:

Etapa 3. Escolha a Interface do gateway na lista suspensa. Esta será a porta que será usada para

passar o tráfego através dos Túneis VPN SSL. As opções são:

- WAN1
- WAN2
- USB1
- USB2

Observação: neste exemplo, WAN1 é escolhida.

Etapa 4. Insira o número da porta usada para o gateway VPN SSL no campo *Gateway Port*, variando de 1 a 65535.

Observação: neste exemplo, 8443 é usado como o número da porta.

Etapa 5. Escolha o Arquivo de certificado na lista suspensa. Este certificado autentica os usuários que tentam acessar o recurso de rede através dos túneis VPN SSL. A lista suspensa contém um certificado padrão e os certificados que são importados.

Observação: neste exemplo, Default é escolhido.

Etapa 6. Insira o endereço IP do pool de endereços do cliente no campo *Client Address Pool*. Este pool será o intervalo de endereços IP que serão alocados para clientes VPN remotos.

Nota: Certifique-se de que o intervalo de endereços IP não se sobreponha a nenhum dos endereços IP na rede local.

Observação: neste exemplo, 192.168.0.0 é usado.

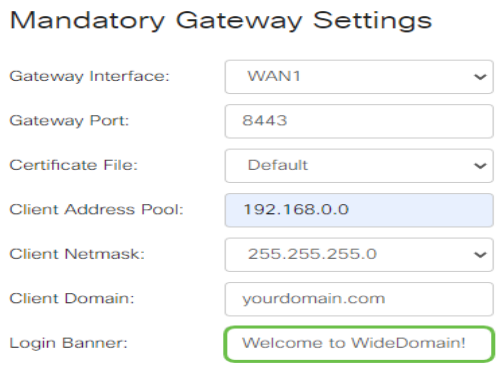
Passo 7. Escolha a Máscara de rede do cliente na lista suspensa.

Observação: neste exemplo, 255.255.255.128 é escolhido.

Etapa 8. Digite o nome de domínio do cliente no campo *Domínio do cliente*. Este será o nome de domínio que deve ser enviado aos clientes VPN SSL.

Observação: neste exemplo, WideDomain.com é usado como o nome de domínio do cliente.

Etapa 9. Insira o texto que apareceria como banner de login no campo *Banner de login*. Este será o banner que será exibido toda vez que um cliente fizer login.

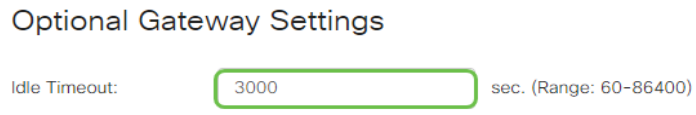


Observação: neste exemplo, Bem-vindo ao Widedomain! é usado como o banner de login.

Configurações opcionais do gateway

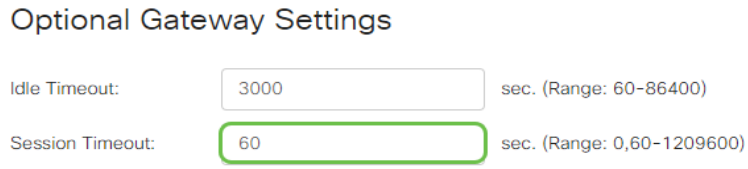
As seguintes definições de configuração são opcionais:

Etapa 1. Insira um valor em segundos para o intervalo de tempo limite ocioso de 60 a 86400. Esta será a duração de tempo durante a qual a sessão VPN SSL poderá permanecer ociosa.



Observação: neste exemplo, 3000 é usado.

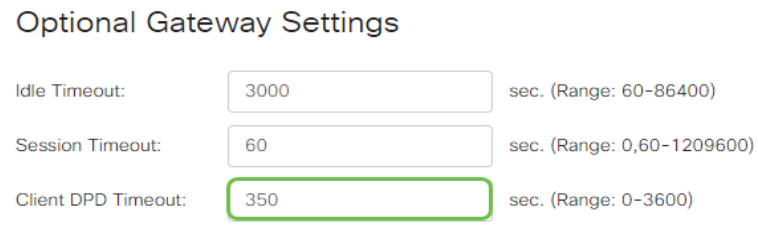
Etapa 2. Insira um valor em segundos no campo *Tempo limite da sessão*. Este é o tempo que leva para que a sessão do Transmission Control Protocol (TCP) ou do User Datagram Protocol (UDP) expire após o tempo ocioso especificado. O intervalo é de 60 a 1209600.



Observação: neste exemplo, 60 é usado.

Etapa 3. Insira um valor em segundos no campo *ClientDPD Timeout*, variando de 0 a 3600. Esse valor especifica o envio periódico de mensagens HELLO/ACK para verificar o status do túnel VPN.

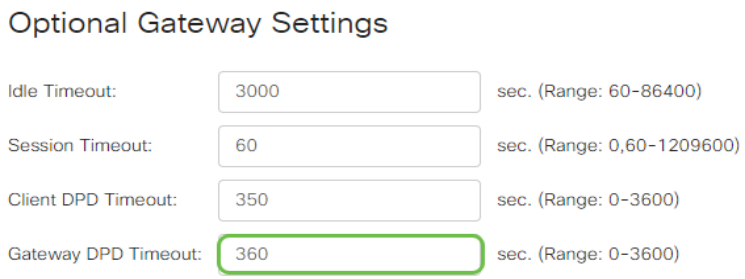
Observação: esse recurso deve ser habilitado em ambas as extremidades do túnel VPN.



Observação: neste exemplo, 350 é usado.

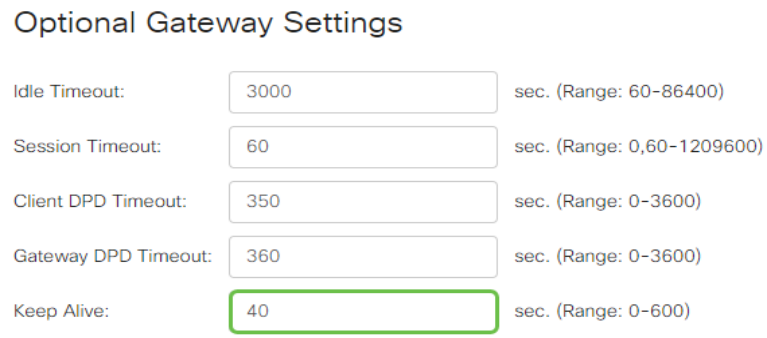
Etapa 4. Insira um valor em segundos no campo *GatewayDPD Timeout*, variando de 0 a 3600. Esse valor especifica o envio periódico de mensagens HELLO/ACK para verificar o status do túnel VPN.

Observação: esse recurso deve ser habilitado em ambas as extremidades do túnel VPN.



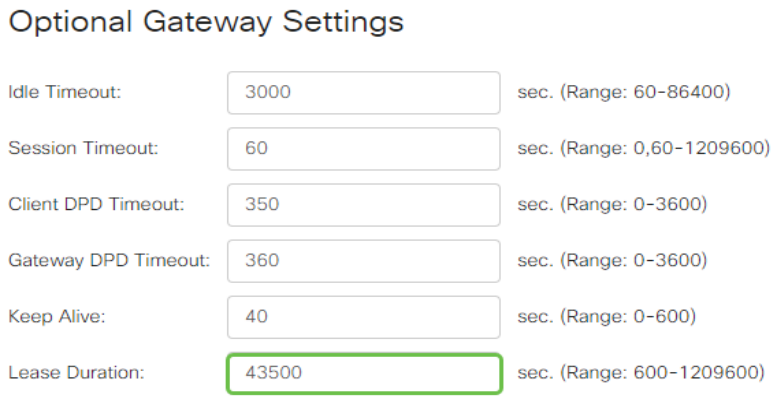
Observação: neste exemplo, 360 é usado.

Etapa 5. Insira um valor em segundos no campo *Keep Alive* variando de 0 a 600. Esse recurso garante que o roteador esteja sempre conectado à Internet. Ele tentará restabelecer a conexão VPN se ela for descartada.



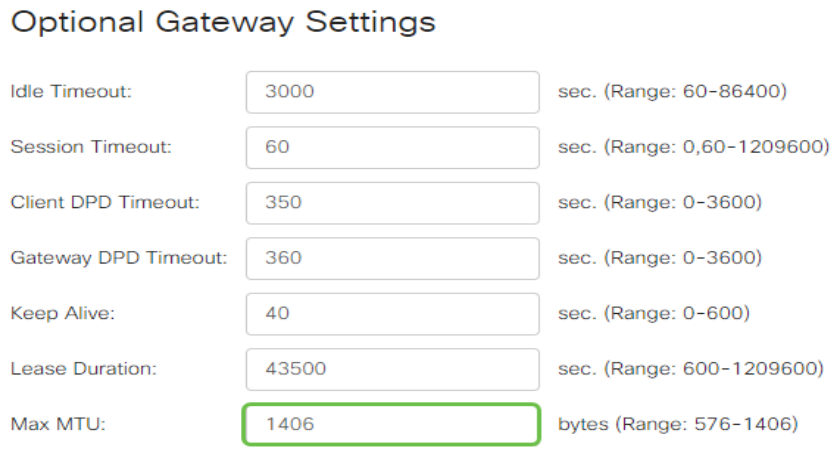
Observação: neste exemplo, 40 é usado.

Etapa 6. Insira um valor em segundos para a duração do túnel a ser conectado no campo *Lease Duration*. O intervalo é de 600 a 1209600.



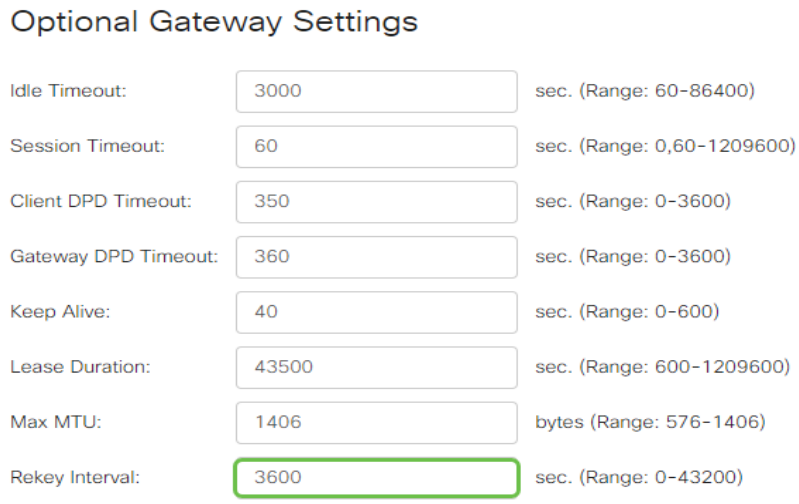
Observação: neste exemplo, 43500 é usado.

Passo 7. Insira o tamanho do pacote em bytes que pode ser enviado pela rede. O intervalo é de 576 a 1406.



Observação: neste exemplo, 1406 é usado.

Etapa 8. Insira o tempo do intervalo de retransmissão no campo *Rekey Interval*. O recurso Rechavear permite que as chaves SSL renegociem após o estabelecimento da sessão. O intervalo é de 0 a 43200.

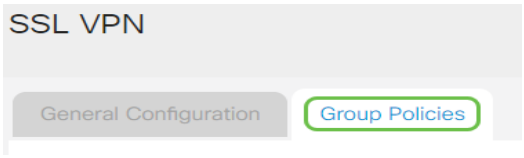


Observação: neste exemplo, 3600 é usado.

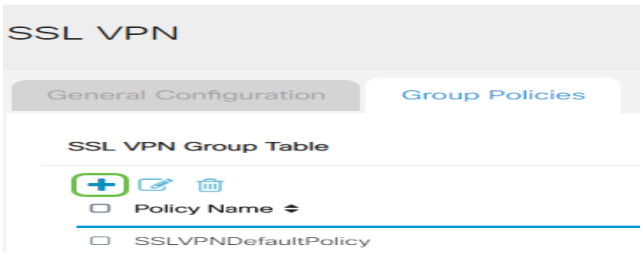
Etapa 9. Clique em Apply.

Configurar Políticas de Grupo

Etapa 1. Clique na guia **Group Policies**.



Etapa 2. Clique no botão **Add** na tabela de grupos VPN SSL para adicionar uma política de grupo.

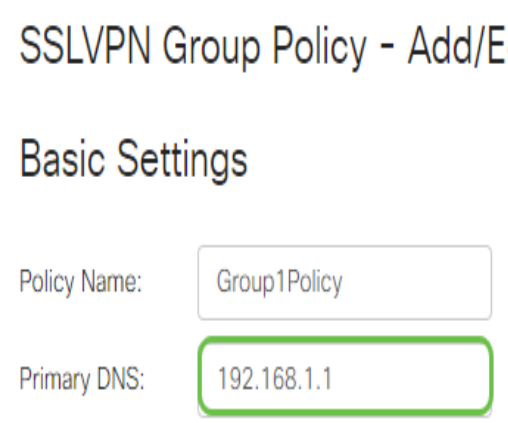


Nota: A tabela Grupo VPN SSL mostrará a lista de políticas de grupo no dispositivo. Você também pode editar a primeira política de grupo na lista, que se chama SSLVPNDefaultPolicy. Esta é a política padrão fornecida pelo dispositivo.

Etapa 3. Insira o nome da política de sua preferência no campo *Policy Name*.

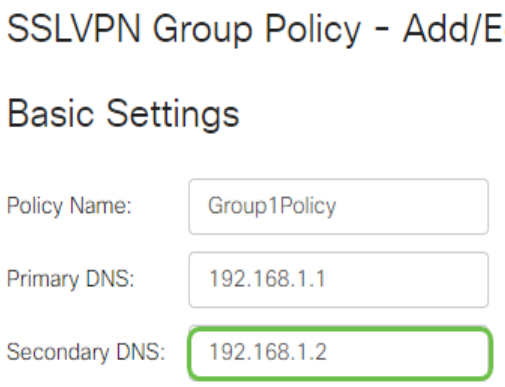
Observação: neste exemplo, a Política de Grupo 1 é usada.

Etapa 4. Insira o endereço IP do DNS primário no campo fornecido. Por padrão, esse endereço IP já é fornecido.



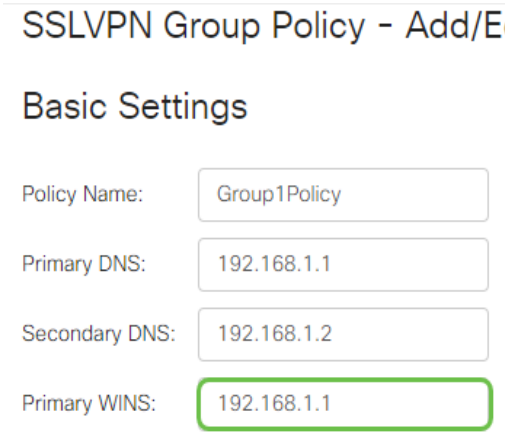
Observação: neste exemplo, 192.168.1.1 é usado.

Etapa 5. (Opcional) Insira o endereço IP do DNS secundário no campo fornecido. Isso servirá como backup em caso de falha do DNS primário.



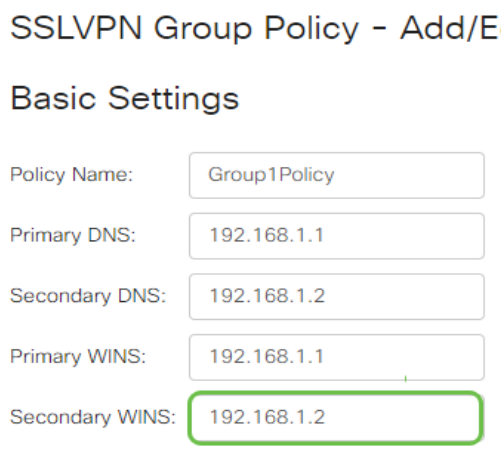
Observação: neste exemplo, 192.168.1.2 é usado.

Etapa 6. (Opcional) Insira o endereço IP do WINS primário no campo fornecido.



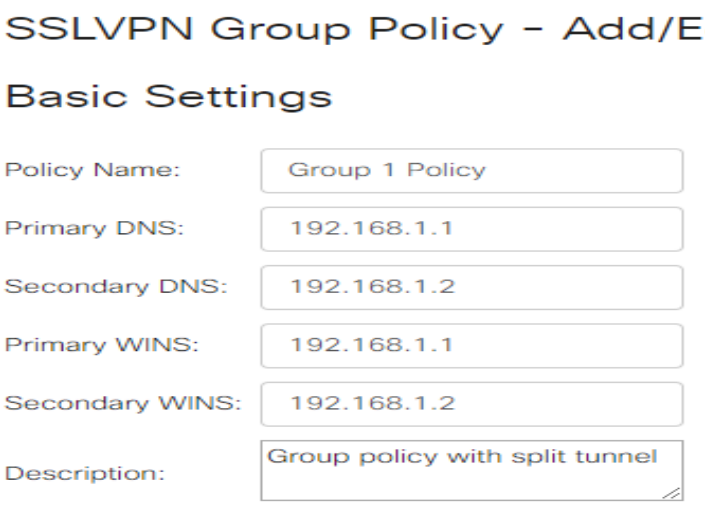
Observação: neste exemplo, 192.168.1.1 é usado.

Etapa 7. (Opcional) Insira o endereço IP do WINS secundário no campo fornecido.



Observação: neste exemplo, 192.168.1.2 é usado.

Etapa 8. (Opcional) Digite uma descrição da política no campo *Description*.



Observação: neste exemplo, a Política de Grupo com túnel dividido é usada.

Etapa 9. (Opcional) Clique em um botão de opção para escolher a Diretiva de Proxy do IE para habilitar as configurações de proxy do Microsoft Internet Explorer (MSIE) para estabelecer o túnel VPN. As opções são:

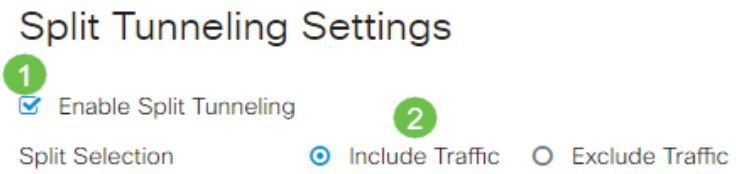
- Nenhum - Permite que o navegador não use configurações de proxy.
- Automático - Permite que o navegador detecte automaticamente as configurações de proxy.
- Bypass-local - Permite que o navegador ignore as configurações de proxy definidas no usuário remoto.
- Desabilitado - Desabilita as configurações de proxy MSIE.

Observação: neste exemplo, Disabled (Desativado) é escolhido. Essa é a configuração padrão.

Etapa 10. (Opcional) Na área Split Tunneling Settings, marque a caixa de seleção **Enable Split Tunneling** para permitir que o tráfego destinado à Internet seja enviado sem criptografia diretamente para a Internet. O Encapsulamento Completo envia todo o tráfego para o dispositivo final, onde é então roteado para os recursos de destino, eliminando a rede corporativa do

caminho para o acesso à Web.

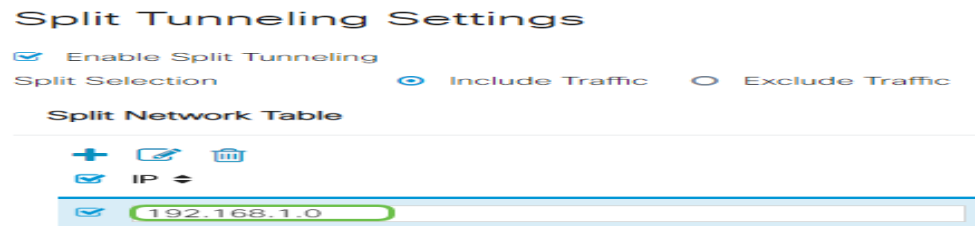
Etapa 11. (Opcional) Clique em um botão de opção para escolher se deseja incluir ou excluir o tráfego ao aplicar o tunelamento dividido.



Observação: neste exemplo, Incluir tráfego é escolhido.

Etapa 12. Na Tabela Dividir Rede, clique no botão **Adicionar** para adicionar a exceção Dividir Rede.

Etapa 13. Insira o endereço IP da rede no campo fornecido.



Observação: neste exemplo, 192.168.1.0 é usado.

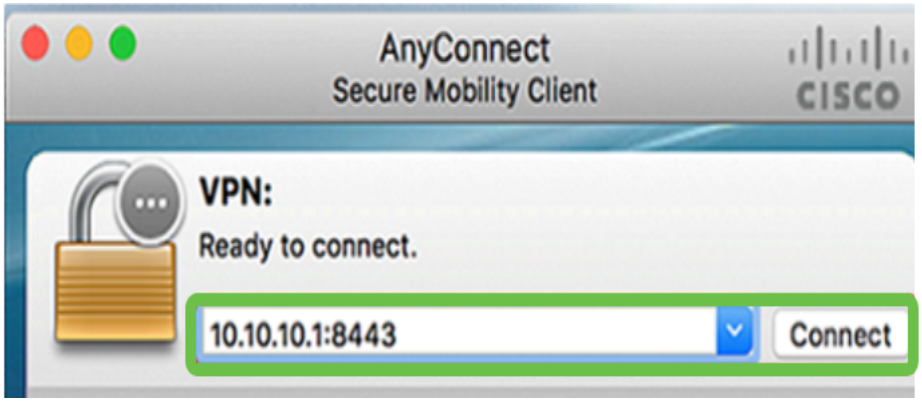
Etapa 14. Na Tabela DNS dividida, clique no botão **Adicionar** para adicionar a exceção DNS dividida.

Etapa 15. Insira o nome de domínio no campo fornecido e clique em **Aplicar**.

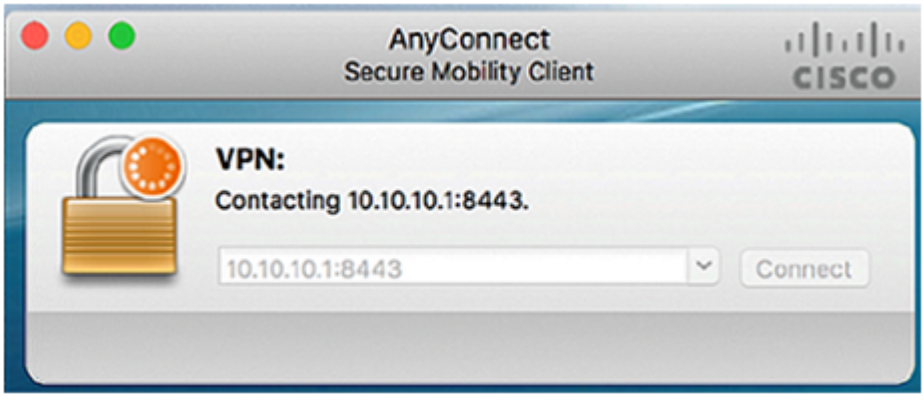
Verificar a conectividade do AnyConnect VPN

Etapa 1. Clique no ícone **AnyConnect Secure Mobility Client**.

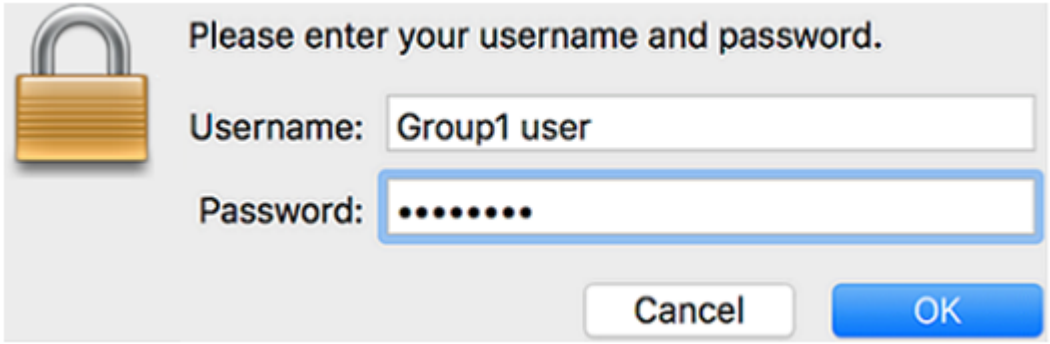
Etapa 2. Na janela AnyConnect Secure Mobility Client, insira o endereço IP do gateway e o número da porta do gateway separados por dois-pontos (:) e clique em **Connect**.



Observação: neste exemplo, 10.10.10.1:8443 é usado. O software agora mostrará que está entrando em contato com a rede remota.

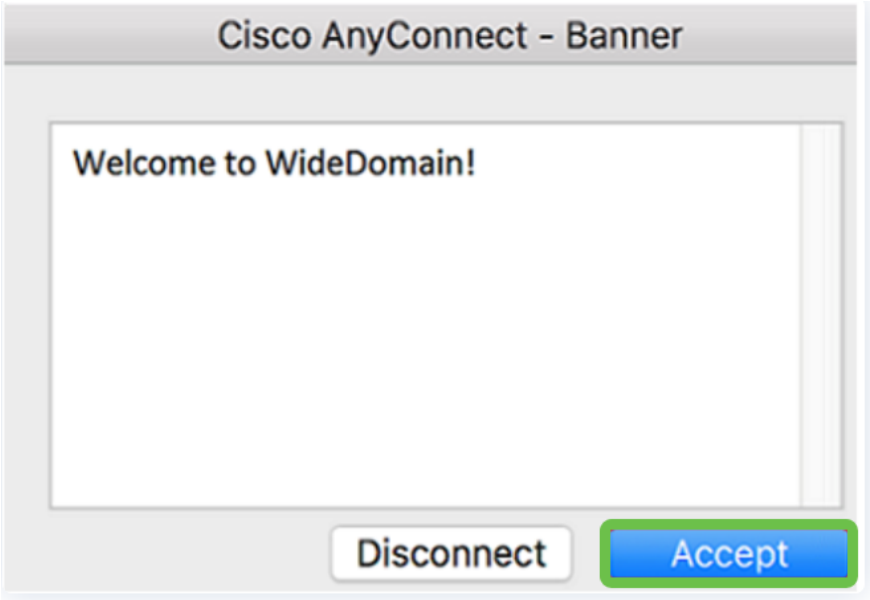


Etapa 3. Insira o nome de usuário e a senha do servidor nos respectivos campos e clique em **OK**.

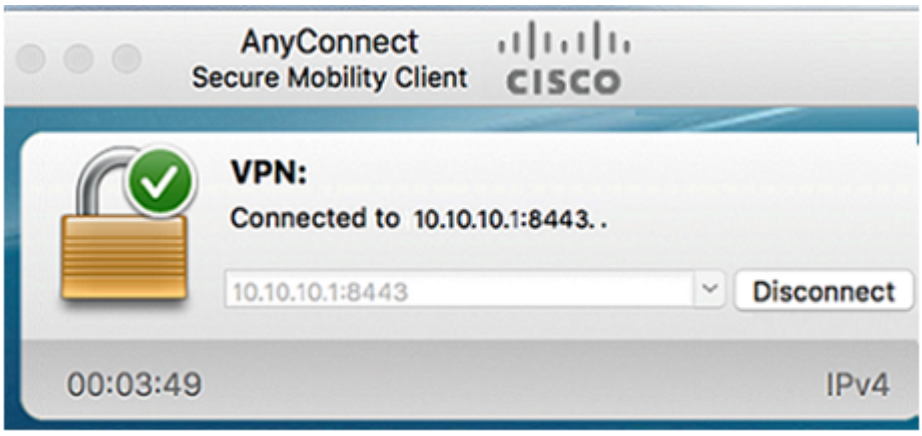


Observação: neste exemplo, o usuário Group1 é usado como o nome de usuário.

Etapa 4. Assim que a conexão for estabelecida, o banner de login será exibido. Clique em **Aceitar**.



A janela do AnyConnect deve indicar agora a conexão VPN bem-sucedida com a rede.



Etapa 5. (Opcional) Para se desconectar da rede, clique em **Desconectar**.

Agora você deve ter configurado com êxito a conectividade do AnyConnect VPN usando um RV34x Series Router.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.