

Configurar a conexão VPN (Virtual Private Network, rede virtual privada) cliente-local no roteador série RV34x

Objetivo

Em uma conexão VPN (Client-to-Site Virtual Private Network), os clientes da Internet podem se conectar ao servidor para acessar a rede corporativa ou LAN (Local Area Network) atrás do servidor, mas ainda mantêm a segurança da rede e seus recursos. Esse recurso é muito útil, pois cria um novo túnel VPN que permite que funcionários remotos e viajantes a negócios acessem sua rede usando um software cliente VPN sem comprometer a privacidade e a segurança.

O objetivo deste documento é mostrar a você como configurar a conexão VPN de cliente para site no RV34x Series Router.

Dispositivos aplicáveis

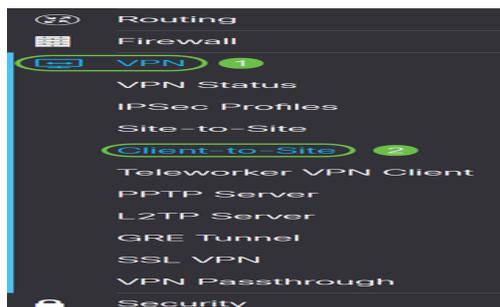
- Série RV34x

Versão de software

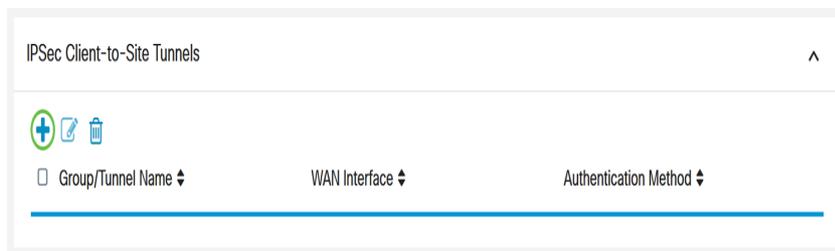
- 1.0.01.16

Configurar VPN Cliente a Site

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



Etapa 2. Clique no botão **Add** na seção IPsec Client-to-Site Tunnel.



Etapa 3. Na área *Add a New Tunnel*, clique no botão de opção **Cisco VPN Client**.

Add a New Tunnel

Cisco VPN Client 3rd Party Client

Etapa 4. Marque a caixa de seleção **Habilitar** para habilitar a configuração.

Enable:

Group Name: Please Input Group Name

Interface:

Etapa 5. Insira um nome de grupo no campo fornecido. Isso servirá como identificador para todos os membros deste grupo durante as negociações do Internet Key Exchange (IKE).

Enable:

Group Name:

Interface:

Note: Insira caracteres entre A e Z ou 0 a 9. Espaços e caracteres especiais não são permitidos para o nome do grupo. Neste exemplo, TestGroup é usado.

Etapa 6. Clique na lista suspensa para escolher a Interface. As opções são:

- WAN1
- WAN2
- USB1
- USB2

Enable:

Group Name:

Interface:

Note: Neste exemplo, a WAN1 é escolhida. Essa é a configuração padrão.

Passo 7. Na área Método de autenticação IKE, escolha um método de autenticação a ser usado em negociações IKE em túnel baseado em IKE. As opções são:

- Chave pré-compartilhada — Os colegas IKE autenticam-se ao computar e enviam um hash chaveado de dados que inclui a Chave pré-compartilhada. 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 são escaláveis bem porque cada peer de IPSec deve ser configurado com a chave pré-compartilhada de todos os outros pares com os quais estabelece uma sessão.

- Certificado — O certificado digital é um pacote que contém informações como uma identidade de certificado do portador: nome ou endereço IP, a data de expiração do número de série 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.

IKE Authentication Method

Pre-shared Key:

Pre-shared Key Strength Meter:

Minimum Pre-shared Key Complexity: Enable

Show Pre-shared Key: Enable

Certificate:

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

Etapa 8. Insira uma chave pré-compartilhada no campo fornecido. Esta será a chave de autenticação entre seu grupo de pares IKE.

IKE Authentication Method

Pre-shared Key:

Pre-shared Key Strength Meter:

Minimum Pre-shared Key Complexity: Enable

Show Pre-shared Key: Enable

Certificate:

Etapa 9. (Opcional) Marque a caixa de seleção **Habilitar** para a Complexidade Mínima de Chave Pré-compartilhada para visualizar o Medidor de Força da Chave Pré-compartilhada e determinar a força da sua chave. A força da chave é definida da seguinte forma:

- Vermelho— A senha está fraca.
- Laranja— A senha é bastante forte.
- Verde — A senha é forte.

IKE Authentication Method

Pre-shared Key:

Pre-shared Key Strength Meter:

Minimum Pre-shared Key Complexity: Enable

Show Pre-shared Key: Enable

Certificate:

Note: Você pode marcar a caixa de seleção **Habilitar** no campo *Mostrar chave pré-compartilhada* para verificar sua senha em texto simples.

IKE Authentication Method

Pre-shared Key: 2

Pre-shared Key Strength Meter:

Minimum Pre-shared Key Complexity: Enable

Show Pre-shared Key: 1 Enable

Certificate:

Etapa 10. (Opcional) Clique no ícone **de mais** na tabela Grupo de usuários para adicionar um grupo.

User Group Table

Group Name

Etapa 11. (Opcional) Escolha na lista suspensa se o grupo de usuários é para admin ou para convidados. Se você criou seu próprio grupo de usuários com contas de usuário, poderá selecioná-lo. Neste exemplo, selecionaremos TestGroup.

Note: TestGroup é um grupo de usuários que criamos em **Configuração do sistema > Grupos de usuários**.

User Group Table

Group Name

TestGroup

Mode: VPNUsers
 admin
 guest

Note: Neste exemplo, TestGroup é escolhido. Você também pode marcar a caixa ao lado do grupo de usuários e clicar no botão **Excluir** se quiser excluir um grupo de usuários.

Etapa 12. Clique em um botão de opção para escolher um modo. As opções são:

- Cliente — Esta opção permite que o cliente solicite um endereço IP e o servidor forneça os endereços IP do intervalo de endereços configurado.
- Network Extension Mode (NEM) — Essa opção permite que os clientes proponham sua sub-rede para a qual os serviços VPN precisam ser aplicados no tráfego entre a LAN atrás do servidor e a sub-rede proposta pelo cliente.

Mode: Client NEM

Note: Neste exemplo, Cliente é escolhido.

Etapa 13. Insira o endereço IP inicial no campo *Start IP (IP inicial)*. Esse será o primeiro endereço IP no pool que pode ser atribuído a um cliente.

Pool Range for Client LAN

Start IP:

End IP:

Note: Neste exemplo, 192.168.100.1 é usado.

Etapa 14. Insira o endereço IP final no campo *End IP*. Esse será o último endereço IP no pool que pode ser atribuído a um cliente.

Pool Range for Client LAN

Start IP:

End IP:

Note: Neste exemplo, 192.168.100.100 é usado.

Etapa 15. (Opcional) Na área *Configuração do modo*, insira o endereço IP do servidor DNS primário no campo fornecido.

Mode Configuration

Primary DNS Server:

Secondary DNS Server:

Primary WINS Server:

Secondary WINS Server:

Note: Neste exemplo, 192.168.1.1 é usado.

Etapa 16. (Opcional) Insira o endereço IP do servidor DNS secundário no campo fornecido.

Mode Configuration

Primary DNS Server:	<input type="text" value="192.168.1.1"/>
Secondary DNS Server:	<input type="text" value="192.168.1.2"/>
Primary WINS Server:	<input type="text"/>
Secondary WINS Server:	<input type="text"/>

Note: Neste exemplo, 192.168.1.2 é usado.

Etapa 17. (Opcional) Insira o endereço IP do servidor WINS principal no campo fornecido.

Mode Configuration

Primary DNS Server:	<input type="text" value="192.168.1.1"/>
Secondary DNS Server:	<input type="text" value="192.168.1.2"/>
Primary WINS Server:	<input type="text" value="192.168.1.1"/>
Secondary WINS Server:	<input type="text"/>

Note: Neste exemplo, 192.168.1.1 é usado.

Etapa 18. (Opcional) Insira o endereço IP do servidor WINS secundário no campo fornecido.

Mode Configuration

Primary DNS Server:	<input type="text" value="192.168.1.1"/>
Secondary DNS Server:	<input type="text" value="192.168.1.2"/>
Primary WINS Server:	<input type="text" value="192.168.1.1"/>
Secondary WINS Server:	<input type="text" value="192.168.1.2"/>

Note: Neste exemplo, 192.168.1.2 é usado.

Etapa 19. (Opcional) Insira o domínio padrão a ser usado na rede remota no campo fornecido.

Default Domain:	<input type="text" value="sample.com"/>	
Backup Server 1:	<input type="text"/>	(IP Address or Domain Name)
Backup Server 2:	<input type="text"/>	(IP Address or Domain Name)
Backup Server 3:	<input type="text"/>	(IP Address or Domain Name)

Note: Neste exemplo, sample.com é usado.

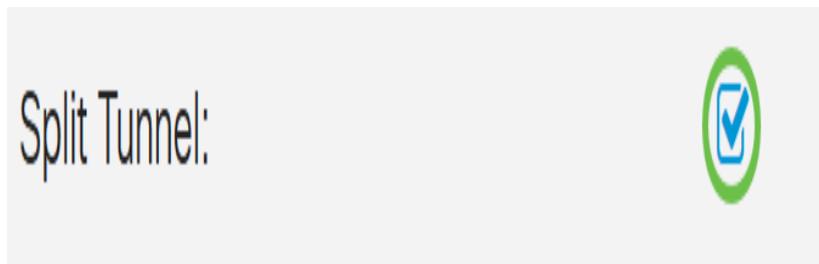
Etapa 20. (Opcional) No campo *Backup Server 1*, insira o endereço IP ou o nome de domínio do servidor de backup. Será aqui que o dispositivo poderá iniciar a conexão VPN

caso o servidor VPN IPSec principal falhe. Você pode inserir até três servidores de backup nos campos fornecidos. O Backup Server 1 tem a prioridade mais alta entre os três servidores e o Backup Server 3 tem a mais baixa.

Default Domain:	<input type="text" value="sample.com"/>	
Backup Server 1:	<input type="text" value="example.com"/>	(IP Address or Domain Name)
Backup Server 2:	<input type="text"/>	(IP Address or Domain Name)
Backup Server 3:	<input type="text"/>	(IP Address or Domain Name)

Note: Neste exemplo, Example.com é usado para o Backup Server 1.

Etapa 21. (Opcional) Marque a caixa de seleção **Dividir túnel** para ativar o túnel dividido. O tunelamento dividido permite acessar os recursos de uma rede privada e da Internet ao mesmo tempo.



Etapa 22. (Opcional) Em *Split Tunnel Table*, clique no ícone **plus** para adicionar um endereço IP para o split tunnel.

Split Tunnel Table



Etapa 23. (Opcional) Insira o endereço IP e a máscara de rede do túnel dividido nos campos fornecidos.

Split Tunnel Table ^

<input checked="" type="checkbox"/>	<input type="text" value="192.168.1.0"/>	<input type="text" value="255.255.255.0"/>
-------------------------------------	--	--

Note: Neste exemplo, 192.168.1.0 e 255.255.255.0 são usados. Você também pode marcar a caixa e clicar nos botões **Add**, **Edit** e **Delete** para adicionar, editar ou excluir um túnel dividido, respectivamente.

Etapa 24. (Opcional) Marque a caixa de seleção **Dividir DNS** para ativar o DNS dividido. O DNS dividido permite criar servidores DNS separados para redes internas e externas para manter a segurança e a privacidade dos recursos da rede.

Split DNS:



Etapa 25. (Opcional) Clique no ícone **de mais** na *Tabela DNS dividida* para adicionar um nome de domínio para DNS dividido.

Split DNS Table



Domain Name

Etapa 26. (Opcional) Insira o nome de domínio do DNS dividido no campo fornecido.

Split DNS Table



Domain Name

labsample.com

Note: Neste exemplo, labsample.com é usado. Você também pode marcar a caixa e clicar nos botões **Add**, **Edit** e **Delete** para adicionar, editar ou excluir um DNS dividido, respectivamente.

Etapa 27. Clique em Apply.

Add a New Tunnel Apply Cancel

Split Tunnel Table

<input checked="" type="checkbox"/> IP Address	Netmask
<input checked="" type="checkbox"/> 192.168.1.0	255.255.255.0

Split DNS:

Split DNS Table

<input checked="" type="checkbox"/> Domain Name
<input checked="" type="checkbox"/> labsample.com

Conclusão

Agora você deve ter configurado com êxito a conexão cliente-local no RV34x Series Router.

Clique nos seguintes artigos para saber mais sobre os seguintes tópicos:

- [Configurar um cliente de VPN de trabalhador remoto no roteador RV34x Series](#)
- [Usar o GreenBow VPN Client para se conectar ao RV34x Series Router](#)
- [Crie uma conta de usuário para a configuração do cliente VPN no roteador RV34x](#)
- [Crie um grupo de usuários para a configuração de VPN no roteador RV34x](#)

Exibir um vídeo relacionado a este artigo...

[Clique aqui para ver outras palestras técnicas da Cisco](#)