

# Configurar configurações de servidor do protocolo de transporte da camada 2 (L2TP) em um roteador do RV34x Series

## Objetivo

O protocolo Layer 2 Tunneling Protocol (L2TP) estabelece um Virtual Private Network (VPN) que permite que os host remotos conectem a um outro através de um túnel seguro. Não fornece nenhuma criptografia ou confidencialidade por si só mas confia em um protocolo de codificação que passe dentro do túnel para fornecer a privacidade.

Uma de suas vantagens mais grandes do L2TP é que cifra o processo de autenticação, em que faz mais difícil para que alguém “escute” em sua transmissão para interceptar e rachar os dados. O L2TP fornece não somente a confidencialidade mas igualmente a integridade de dados. A integridade de dados é proteção contra a alteração da data entre o tempo onde saiu do remetente e do tempo alcançou o receptor.

Este documento aponta mostrar-lhe como configurar as configurações de servidor L2TP no roteador do RV34x Series.

## Dispositivos aplicáveis

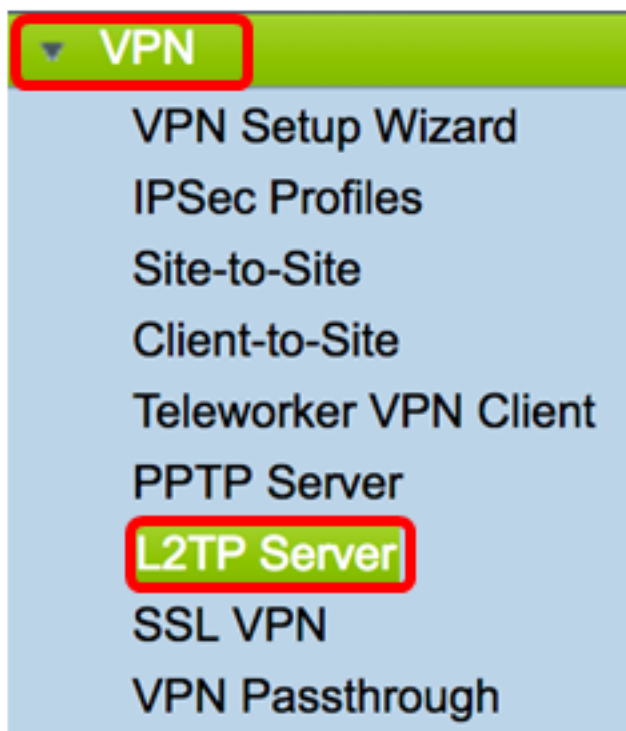
- RV34x Series

## Versão de software

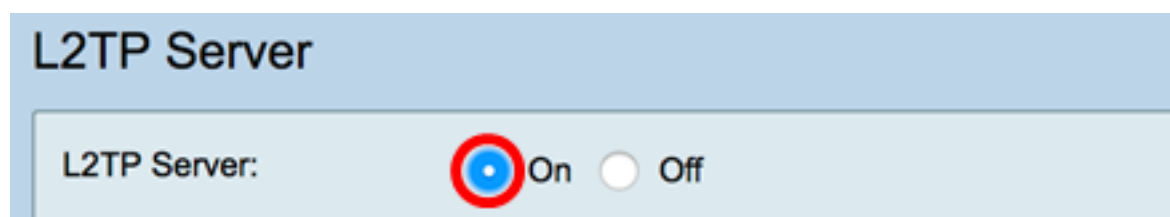
- 1.0.01.16

## Configurar o L2TP

Etapa 1. Entre à utilidade com base na Web do roteador e escolha **server VPN > L2TP**.

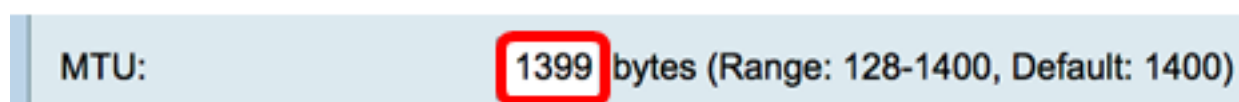


Etapa 2. Clique **sobre** o botão de rádio do server L2TP para permitir o server L2TP.



Etapa 3. Incorpore um número dentro da escala do 128 a 1400 no campo *MTU*. A unidade de transmissão máxima (MTU) define o tamanho o maior dos pacotes que uma relação pode transmitir sem a necessidade de fragmentar. O padrão é 1400.

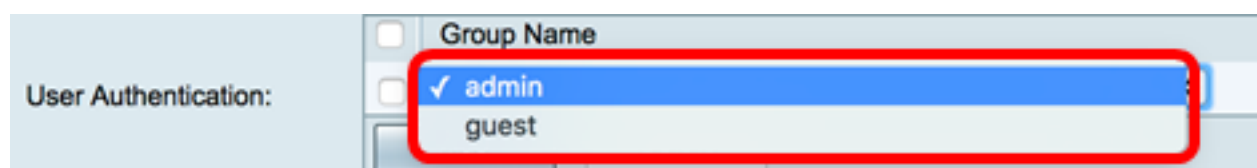
**Nota:** Para este exemplo, 1399 são usados.



Etapa 4. Na área da autenticação de usuário, o clique adiciona para um grupo adicional de escolhe um perfil de grupo onde os usuários sejam autenticados. As opções dependem sobre mesmo se um perfil de grupo tem sido configurado previamente. As opções padrão são:

- admin — Grupo do Special de privilégios ao read/write sobre ajustes
- convidado — Privilégios de leitura apenas

**Nota:** Para este exemplo, o admin é escolhido.



Etapa 5. No campo do *endereço IP de Um ou Mais Servidores Cisco ICM NT do começo*,

incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT começando do intervalo de endereço IP a ser atribuído aos usuários. Estes são endereços IP de Um ou Mais Servidores Cisco ICM NT reservados para usuários L2TP. Um máximo de 25 sessões é apoiado.

**Nota:** Para este exemplo, 10.0.1.224 é usado.

Address Pool:

Start IP Address:

Etapa 6. No campo do *endereço IP de Um ou Mais Servidores Cisco ICM NT da extremidade*, incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT do término do intervalo de endereço IP.

**Nota:** Para este exemplo, 10.0.1.254 é usado.

End IP Address:

Passo 7. No campo do *endereço IP de Um ou Mais Servidores Cisco ICM NT DNS1*, incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor DNS.

**Nota:** Para este exemplo, 192.168.1.1 é usado.

DNS1 IP Address:

Etapa 8. (opcional) no campo do *endereço IP de Um ou Mais Servidores Cisco ICM NT DNS2*, incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT do segundo servidor DNS. O padrão está vazio.

DNS2 IP Address:

Clique (opcional) de etapa 9. **sobre o** botão de rádio do IPsec para permitir a característica do IPsec para o L2TP. A segurança de protocolo do Internet (IPsec) fornece a segurança para transmissão da informação sensível sobre redes desprotegidas.

**Nota:** Se você escolheu fora, salte a [etapa 13](#).

IPSec:  On  Off

Etapa 10. Escolha um perfil do menu suspenso do perfil IPsec. As opções são:

- Amazon\_Web\_Services — Um serviço da nuvem pelas Amazonas fornecidas por Amazonas.
- Padrão — Perfil padrão
- Microsoft\_Azure — Um serviço da nuvem proporcionado por Microsoft.

**Nota:** Para este exemplo, Microsoft\_Azure é escolhido.

IPSec: Amazon\_Web\_Services  
Default  
IPSec Profile: ✓ Microsoft\_Azure

Etapa 11. No campo de *chave pré-compartilhada*, incorpore uma chave usada para autenticar ao Internet Key Exchange (IKE) um par remoto. Você pode entrar acima de 30 caracteres hexadecimais.

**Nota:** O ambas as extremidades do túnel VPN deve usar a mesma chave pré-compartilhada. Recomenda-se atualizar periodicamente a chave para maximizar a segurança do VPN.

Pre-shared Key: .....

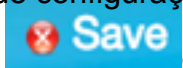
Etapa 12. (Opcional) verifique o texto simples da mostra da possibilidade quando edite a caixa de verificação para indicar a chave pré-compartilhada no texto simples.

**Nota:** Para este exemplo, o texto simples da mostra quando edite é permitido.

Pre-shared Key: @blnbb3r\$  
Show plain text when edit:  Enable  
Apply Cancel

[Etapa 13.](#) O clique **aplica-se** para salvar os ajustes.

Pre-shared Key: @blnbb3r\$  
Show plain text when edit:  Enable  
Apply Cancel

Etapa 14. (Opcional) para salvar a configuração ao arquivo de configuração de inicialização, vá à página de configuração da **cópia/salv guarda** ou clique  o ícone na parcela superior da página.

## L2TP Server



Success. To permanently save the configuration. Go to [Configuration Management](#) page or click Save icon.

L2TP Server:	<input checked="" type="radio"/> On <input type="radio"/> Off
MTU:	<input type="text" value="1399"/> bytes (Range: 128-1400, Default: 1400)
User Authentication:	<input type="checkbox"/> Group Name
	<input type="checkbox"/> admin
	<input type="button" value="Add"/> <input type="button" value="Delete"/>
Address Pool:	
Start IP Address:	<input type="text" value="10.0.1.224"/>
End IP Address:	<input type="text" value="10.0.1.254"/>
DNS1 IP Address:	<input type="text" value="192.168.1.1"/>
DNS2 IP Address:	<input type="text"/>
IPSec:	<input checked="" type="radio"/> On <input type="radio"/> Off
IPSec Profile:	<input type="text" value="Default"/>
Pre-shared Key:	<input type="text" value="*****"/>
Show plain text when edit:	<input type="checkbox"/> Enable

Você deve agora com sucesso ter configurado as configurações de servidor L2TP no roteador do RV34x Series.