

Configurer les paramètres du serveur L2TP (Layer 2 Transport Protocol) sur un routeur de la gamme RV34x

Objectif

Le protocole L2TP (Layer 2 Tunneling Protocol) établit un réseau privé virtuel (VPN) qui permet aux hôtes distants de se connecter les uns aux autres via un tunnel sécurisé. Il ne fournit pas de cryptage ni de confidentialité en lui-même, mais il s'appuie sur un protocole de cryptage qu'il transmet dans le tunnel pour assurer la confidentialité.

L2TP présente l'un de ses principaux avantages : il chiffre le processus d'authentification, ce qui rend plus difficile pour quelqu'un d'écouter votre transmission d'intercepter et de craquer les données. L2TP n'assure pas seulement la confidentialité mais aussi l'intégrité des données. L'intégrité des données est une protection contre toute modification de date entre le moment où elle a quitté l'expéditeur et le moment où elle a atteint le destinataire.

Ce document vise à vous montrer comment configurer les paramètres du serveur L2TP sur le routeur de la gamme RV34x.

Périphériques pertinents

- Gamme RV34x

Version du logiciel

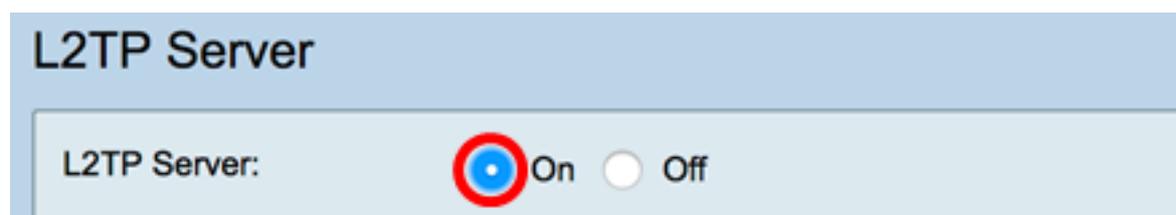
- 1.0.01.16

Configurer L2TP

Étape 1. Connectez-vous à l'utilitaire Web du routeur et choisissez **VPN > L2 TP Server**.



Étape 2. Cliquez sur la case d'option **On** L2TP Server pour activer le serveur L2TP.



Étape 3. Entrez un nombre compris entre 128 et 1400 dans le champ *MTU*. L'unité de transmission maximale (MTU) définit la plus grande taille de paquets qu'une interface peut transmettre sans avoir à fragmenter. Il est défini par défaut à 1400.

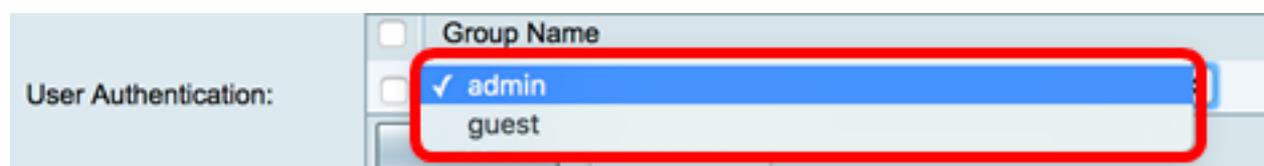
Note: Dans cet exemple, 1399 est utilisé.



Étape 4. Dans la zone Authentification utilisateur, cliquez sur Ajouter pour sélectionner un autre ensemble de profils de groupe dans lequel les utilisateurs seront authentifiés. Les options dépendent de la configuration ou non d'un profil de groupe. Les options par défaut sont les suivantes :

- admin : ensemble spécial de privilèges permettant de lire/écrire sur les paramètres
- guest : privilèges en lecture seule

Note: Dans cet exemple, admin est choisi.



Étape 5. Dans le champ *Start IP Address*, saisissez l'adresse IP de début de la plage

d'adresses IP à attribuer aux utilisateurs. Il s'agit d'adresses IP réservées aux utilisateurs L2TP. Un maximum de 25 sessions est pris en charge.

Note: Pour cet exemple, 10.0.1.224 est utilisé.



Étape 6. Dans le champ *End IP Address*, saisissez l'adresse IP de fin de la plage d'adresses IP.

Note: Pour cet exemple, 10.0.1.254 est utilisé.



Étape 7. Dans le champ *Adresse IP DNS1*, saisissez l'adresse IP du serveur DNS.

Note: Dans cet exemple, 192.168.1.1 est utilisé.



Étape 8. (Facultatif) Dans le champ *DNS2 IP Address*, saisissez l'adresse IP du deuxième serveur DNS. La valeur par défaut est vide.



Étape 9. (Facultatif) Cliquez sur la case d'option **On** IPsec pour activer la fonctionnalité IPsec pour L2TP. IPsec (Internet Protocol Security) assure la sécurité de la transmission des informations sensibles sur des réseaux non protégés.

Note: Si vous avez choisi off, passez à l'[étape 13](#).



Étape 10. Sélectionnez un profil dans le menu déroulant Profil IPsec. Les options sont les suivantes :

- Amazon_Web_Services — Service cloud d'Amazon fourni par Amazon.
- Default — Profil par défaut
- Microsoft_Azure : service cloud fourni par Microsoft.

Note: Pour cet exemple, Microsoft_Azure est sélectionné.

IPSec: Amazon_Web_Services
Default
IPSec Profile: Microsoft_Azure

Étape 11. Dans le champ *Pre-Shared Key*, saisissez une clé utilisée pour s'authentifier auprès d'un homologue IKE (Internet Key Exchange) distant. Vous pouvez saisir jusqu'à 30 caractères hexadécimaux.

Note: Les deux extrémités du tunnel VPN doivent utiliser la même clé pré-partagée. Il est recommandé de mettre à jour la clé périodiquement pour optimiser la sécurité VPN.

Pre-shared Key: [REDACTED]

Étape 12. (Facultatif) Cochez la case Activer Afficher le texte brut lors de la modification pour afficher la clé prépartagée en texte brut.

Note: Pour cet exemple, affichez le texte brut lorsque la modification est activée.

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

[Étape 13.](#) Cliquez sur **Apply** pour enregistrer les paramètres.

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

Étape 14. (Facultatif) Pour enregistrer la configuration dans le fichier de configuration initiale, accédez à la page **Copier/Enregistrer** la configuration ou cliquez sur l'  icône située dans la partie supérieure de la page.

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:	<table border="1"><tr><td><input type="checkbox"/></td><td>Group Name</td></tr><tr><td><input type="checkbox"/></td><td>admin</td></tr><tr><td><input type="button" value="Add"/></td><td><input type="button" value="Delete"/></td></tr></table>	<input type="checkbox"/>	Group Name	<input type="checkbox"/>	admin	<input type="button" value="Add"/>	<input type="button" value="Delete"/>
<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						

Vous devez maintenant avoir correctement configuré les paramètres du serveur L2TP sur le routeur de la gamme RV34x.