

RV34xシリーズルータでのレイヤ2 Transport Protocol(L2TP)サーバの設定

目的

レイヤ2トンネリングプロトコル(L2TP)は、リモートホストが安全なトンネルを介して相互に接続できるようにするバーチャルプライベートネットワーク(VPN)を確立します。暗号化や機密性は単独では提供されませんが、トンネル内で通過する暗号化プロトコルに依存してプライバシーが提供されます。

L2TPの最大の利点の1つは、認証プロセスが暗号化されることです。これにより、送信を「受信」してデータを傍受し、解読するのが困難になります。L2TPは、機密性だけでなく、データ整合性も提供します。データの整合性は、送信者から受信者に到達した時刻までの日付の変更に対する保護です。

このドキュメントでは、RV34xシリーズルータのL2TP Serverの設定方法を説明します。

該当するデバイス

- RV34xシリーズ

[Software Version]

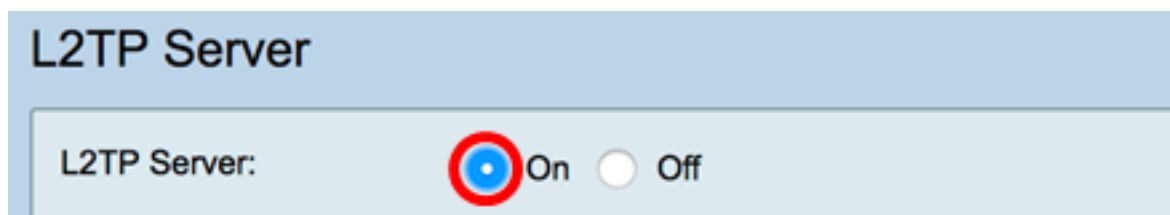
- 1.0.01.16

L2TPの設定

ステップ1：ルータのWebベースのユーティリティにログインし、[VPN] > [L2 TP Server]を選択します。

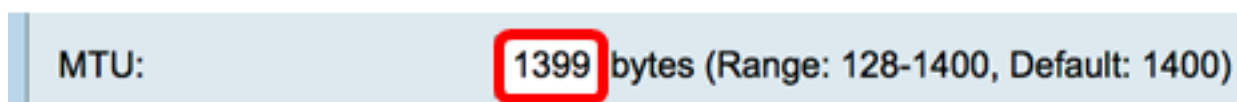


ステップ2:[L2TPサーバ上]ラジオボタンをクリックして、L2TPサーバを有効にします。



ステップ3:[MTU]フィールドに128 ~ 1400の範囲の数値を入力します。最大伝送ユニット (MTU)は、インターフェイスがフラグメント化せずに伝送できるパケットの最大サイズを定義します。デフォルト値は 1400 です。

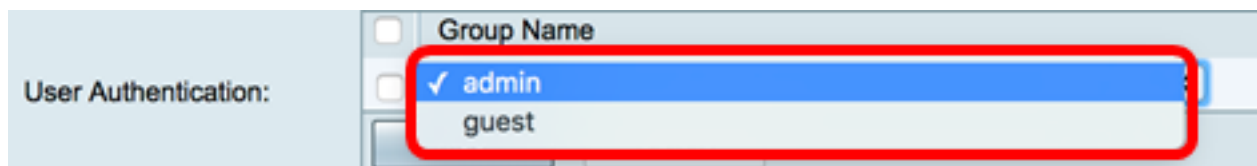
注：この例では、1399が使用されています。



ステップ4:[User Authentication (ユーザ認証)]領域で、[Add (追加)]をクリックして、ユーザが認証されるグループプロファイルを選択します。このオプションは、グループプロファイルが以前に設定されているかどうかによって異なります。デフォルトのオプションは次のとおりです。

- admin：設定の読み取り/書き込みを行う特権の特別なセット
- guest：読み取り専用権限

注：この例では、adminが選択されています。



ステップ5:[Start IP Address]フィールドに、ユーザに割り当てるIPアドレス範囲の開始IPア

ドレスを入力します。これらはL2TPユーザ用に予約されたIPアドレスです。最大25セッションをサポートします。

注：この例では、10.0.1.224が使用されています。

Address Pool:

Start IP Address:

ステップ6:[End IP Address(終了IPアドレス)]フィールドに、IPアドレス範囲の終了IPアドレスを入力します。

注：この例では、10.0.1.254が使用されています。

End IP Address:

ステップ7:[DNS1 IP Address]フィールドに、DNSサーバのIPアドレスを入力します。

注：この例では、192.168.1.1が使用されています。

DNS1 IP Address:

ステップ8: (オプション) [DNS2 IP Address]フィールドに、2番目のDNSサーバのIPアドレスを入力します。デフォルトは空白です。

DNS2 IP Address:

ステップ9: (オプション) [On IPsec]オプションボタンをクリックして、L2TPのIPsec機能を有効にします。Internet Protocol Security(IPsec)は、保護されていないネットワーク上で機密情報を伝送するためのセキュリティを提供します。

注：オフを選択した場合は、ステップ [13に進みます](#)。

IPsec: On Off

ステップ10:[IPsec Profile]ドロップダウンメニューからプロファイルを選択します。次のオプションがあります。

- Amazon_Web_Services:Amazonが提供するAmazonによるクラウドサービス。
- デフォルト：デフォルトプロファイル
- Microsoft_Azure:Microsoftが提供するクラウドサービス。

注：この例では、Microsoft_Azureが選択されています。

IPSec: Amazon_Web_Services
Default
IPSec Profile: Microsoft_Azure

ステップ11:[Pre-Shared Key (事前共有キー)]フィールドに、リモートインターネットキー交換(IKE)ピアへの認証に使用するキーを入力します。最大30文字の16進数を入力できます。

注：VPNトンネルの両端で、同じ事前共有キーを使用する必要があります。VPNセキュリティを最大化するために、キーを定期的に更新することを推奨します。

Pre-shared Key:

ステップ12: (オプション) [Enable Show plain text when edit]チェックボックスをオンにして、事前共有キーをプレーンテキストで表示します。

注：この例では、[Show plain text when edit]が有効になっています。

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

ステップ13:[Apply]をクリックし、設定を保存します。

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

ステップ14: (オプション) スタートアップコンフィギュレーションファイルにコンフィギュレーションを保存するには、「Copy/Save Configuration」ページに移動するか、ページの上にあるアイコンをクリックします  Save。

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						

これで、RV34xシリーズルータでL2TPサーバの設定が正常に完了したはずです。