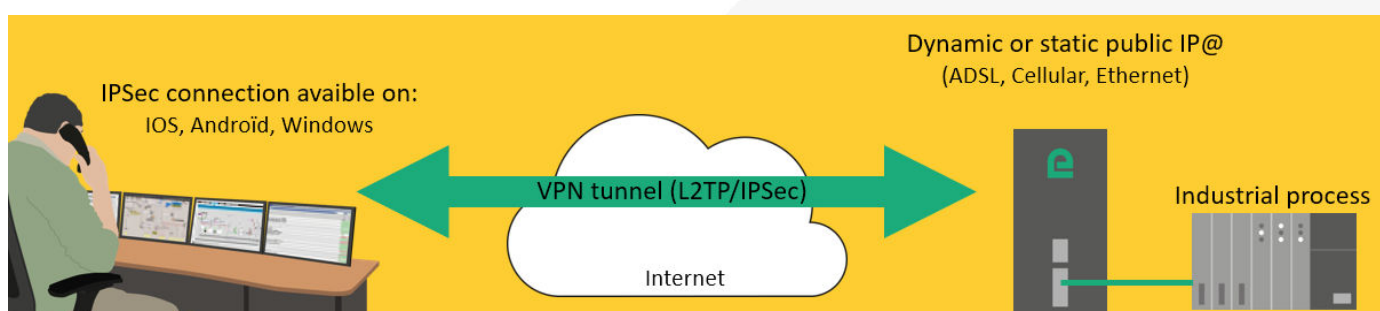


Application note

Setting an L2TP/IPSec remote connection

- Target of the solution
- Pre-requisites
- Configuration of the Etic Telecom device (RAS or IPL families)
- Configuring the Windows10 L2TP/IPSec client
- Configuring the IOS L2TP/IPSec client
- Hot line during your tests
- Virtual showroom

Latest update **09/25/2018**



1) TARGET OF THE SOLUTION

The target of this document is to explain how to configure a secured remote connection to an Etic router through the Internet without any intermediate service.

The main advantages of L2TP/IPSec tunnels are that it is fully secured and integrated on all the main OSes. This application note explains how to configure the router and the Windows or IOS client.

2) PRE-REQUISITES

- The ETIC router must have a public access from the Internet.
- For an ethernet ETIC router, the port UDP 500 and UDP 4500 should be redirected to the ETIC router.
- For a cellular ETIC router, you need to contact your provider to have a subscription that gives a public IP address.
- If you have a dynamic public IP address, you can use the EticDNS service to obtain a domain name that is automatically updated when the IP@ changes (see [Starting with Etic DNS solution](#)).

3) CONFIGURATION OF THE ETIC TELECOM DEVICE (RAS OR IPL FAMILY)

Installation and setup of the Etic Telecom device is described in the [Etic Telecom Starter kit](#).

A. ENABLING L2TP/IPSEC:

- SETUP / REMOTE ACCESS / REMOTE ACCESS SERVERS
- Check "Enable L2TP/IPSec"
- Choose a "key value" (Pre-shared key)
- "Cipher algorithm": AES
- "Message digest algorithm": SHA1



The screenshot shows the Etic Telecom web interface. The breadcrumb navigation is: > Home > Setup > Remote access > Remote access servers. The left sidebar contains a navigation menu with categories: Setup (WAN interface, LAN Interface, Remote access, Users List, Access rights, Remote access servers), Network, Security, Serial gateways, System, Diagnostics, Maintenance, About, and Alert & Display. The main content area is titled "HTTPS Application server" and has two settings: "Enable HTTPS application server" (checked) and "Enable HTTPS application server on WAN" (unchecked). Below this is the "L2TP/IPsec properties" section, which is highlighted with a red box. It contains the following settings: "Enable L2TP/IPSec" (checked), "Cipher algorithm" (AES), "Message digest algorithm" (SHA1), "Authentication method" (Pre Shared Key), and "Key value" (azertyuiop). At the bottom of this section, "Protocols allowed for authentication" are listed: PAP (unchecked), CHAP (checked), MS-CHAP (checked), and MS-CHAP v2 (checked). Below the L2TP/IPsec section is the "OpenVPN properties" section.

B. USER CREATION

- SETUP / REMOTE ACCESS / USER LIST
- Add user on user list table
- Choose a "name", "username" and "password"
- Give him Access rights to the devices you want to access



RAS-ECW-230

Documentation | EN | FR

> Home > Setup > Remote access > Users List > User Configuration

Save Cancel Page has unsaved changes

User information

Active

Full name Etic

Company

E-mail address

Phone number (International format : +33611223344)

User name etic

Password Passwords match

Password strength medium

For security reasons, choose a password longer than 8 characters with uppercase and lowercase letters, numbers and special characters

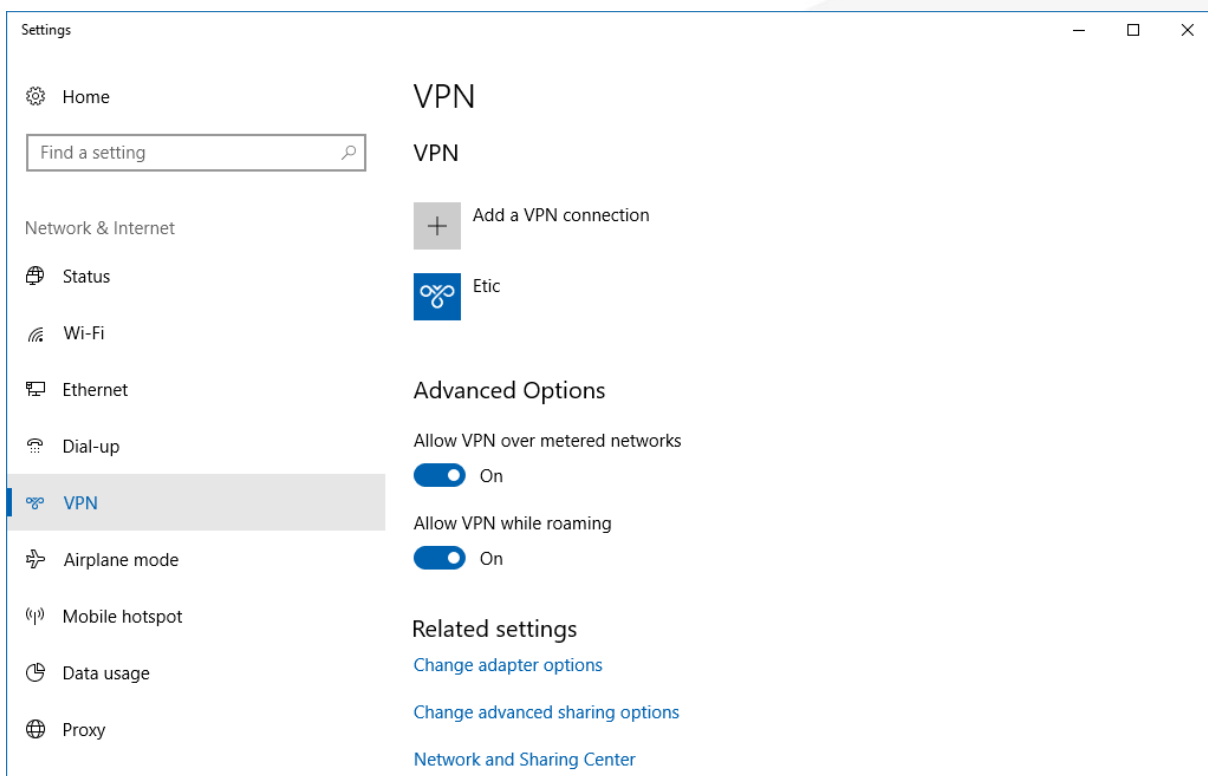
Access rights

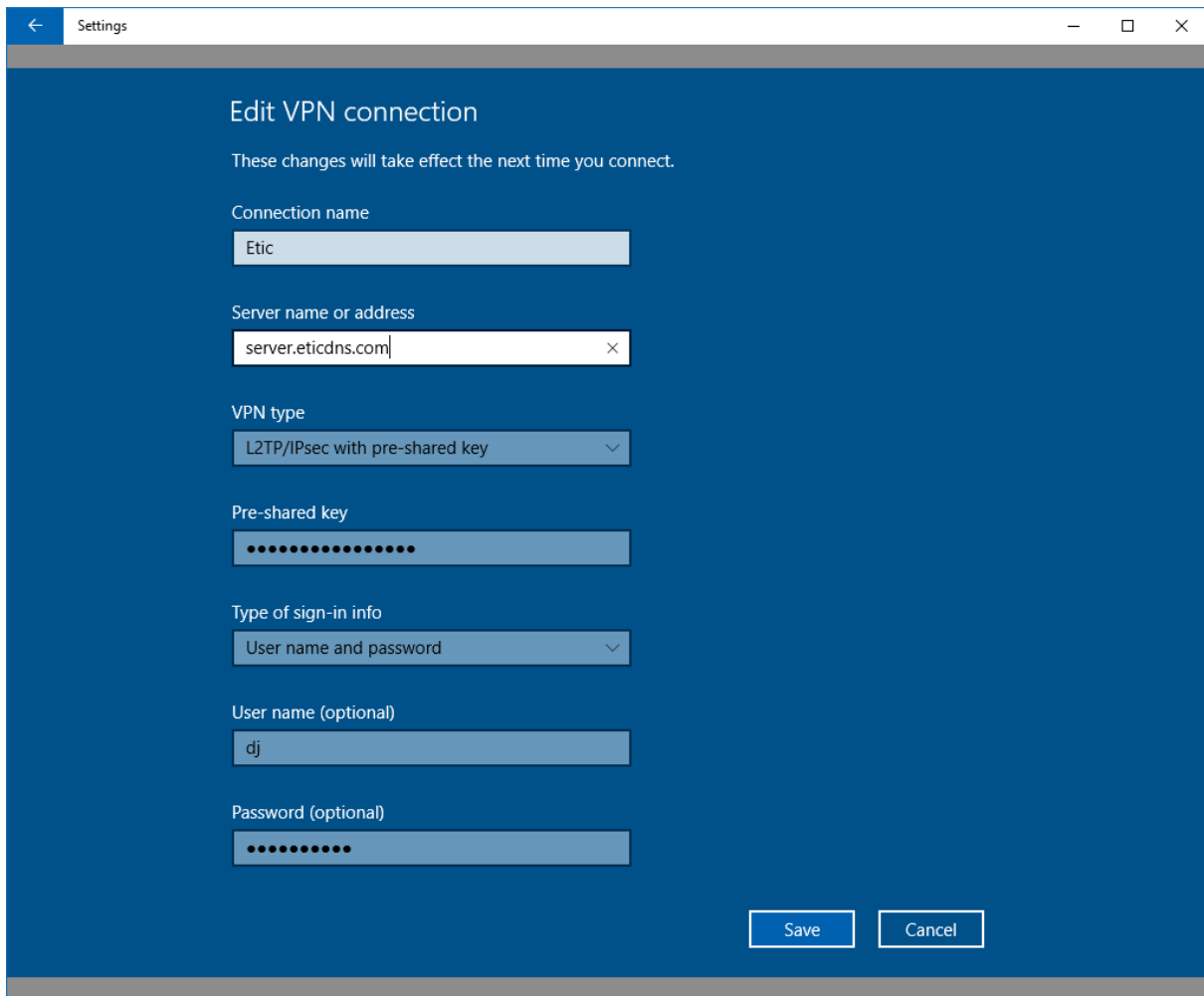
Select on the table below the devices and services the user will be authorized to access.

Authorize	Device	Services
<input checked="" type="checkbox"/>	All the devices	+ All
<input type="checkbox"/>	All devices on the LAN	+ All
<input type="checkbox"/>	All devices on the additional LAN	+ All

4) CONFIGURING WINDOWS 10 L2TP/IPSEC CLIENT

- Network & Internet settings
- Select VPN tab
- Add a VPN connection

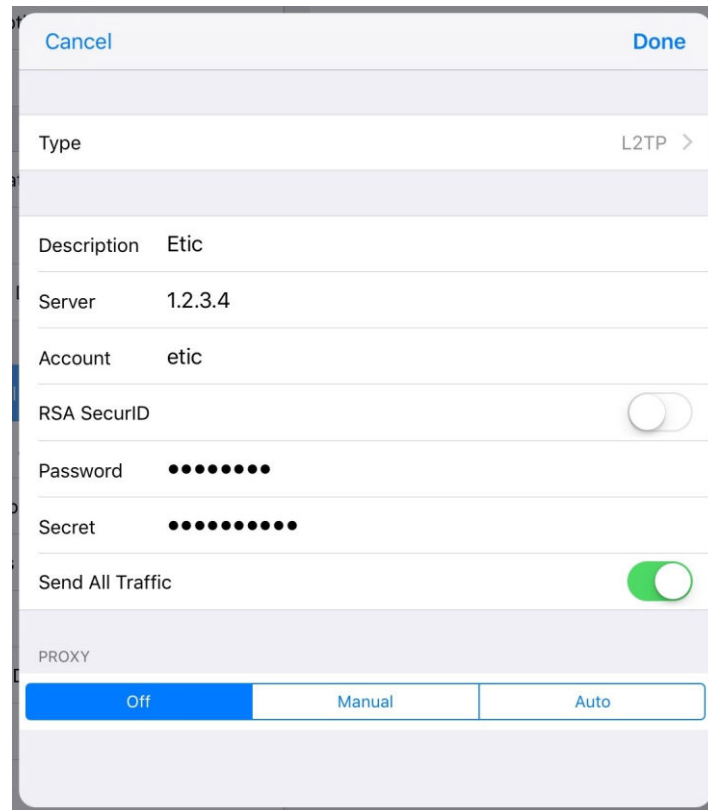




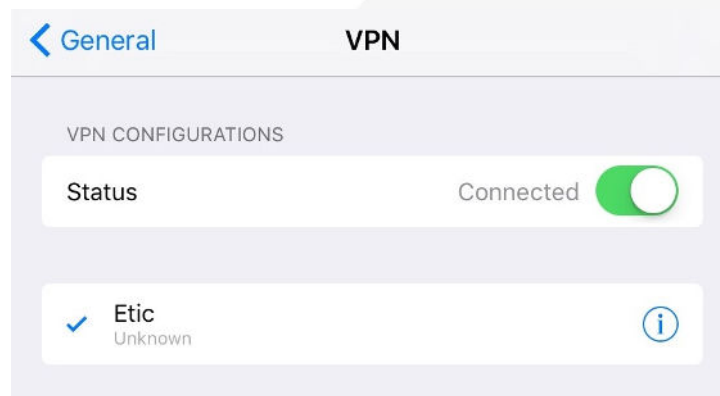
- Server name or address: Public Internet IP or domain name
- Pre-shared key: chosen on §2. A
- User name and Password: of the user created on §2. B
- Save and connect

5) CONFIGURING IOS L2TP/IPSEC CLIENT

- SETTINGS / GENERAL / VPN
- Add VPN configuration
- “Type”: L2TP
- “Server”: RAS public IP address
- “Account”: username of the user created on the RAS
- “Password”: password of the user created on the RAS



- Touch “done” button
- Slide “Status” switch to connect the VPN



6) HOT LINE SUPPORT DURING YOUR TESTS

You can contact our hotline at any time during this training phase with the Alert & Display solution at +33 4 76 04 20 05 or via hotline@etictelecom.com.

7) VIRTUAL SHOWROOM

You also have the possibility by simply logging on our website <http://www.etictelecom.com> ("Support" and then "Virtual showroom") to familiarize you with the configuration of our products.

The screenshot shows the Etic Telecom website's Virtual Showroom page. At the top, the Etic Telecom logo is on the left, and navigation links for "Who are we?", "Products", "Solutions", "Support", "News", and "Contact" are in the center. A "Customer Area" button is on the right. Below the navigation is a dark green bar with "industrial networking" on the left and "FR | EN" on the right. The main content area has a green background with the text "VIRTUAL SHOWROOM" in large yellow letters and "Access to all Etic Telecom products." below it. Underneath, there are two dropdown menus. The first, "Select a product family", lists "Machine Access Box (RAS Family)", "Router (IPL Family)", and "Ethernet Extenders (XS+ Family)". The second, "Select a product", lists "RAS-ECW / Ethernet, Wi-Fi and Cellular Machine Access Box".



13, chemin du Vieux Chêne
38240 Meylan
Tél. 04 76 04 20 00
Fax. 04 76 04 20 01
www.etictelecom.com