How To Connect a Siretta Industrial Router to a VPN Tunnel Using L2TP Protocol

General Description

An advantage of using a powerful industrial router is the ability to send and receive data securely over an encrypted connection. This offers a user the ability to keep data secure between two endpoints by allowing the connected equipment to send data across an encrypted network connection securely without any changes to the configuration of the equipment using well defined security protocols. This document explains how to connect the Siretta router family to a server over a L2TP VPN tunnel.

The Siretta range of Industrial Routers support the followings VPN protocols:

- GRE
- OpenVPN Client
- L2TP/PPTP Client
- IPSec

Before you start the process of establishing an L2TP VPN connection between a Siretta router and a server, please obtain the following details:

1. L2TP VPN Server IP address
2. L2TP User name and password

These details are available from your network administrator for your VPN server.

NOTE: If you do not have your VPN Server details to hand then you can obtain temporary test details from the following link 'http://www.vpngate.net/en/' to allow you to check the VPN functionality of the router.

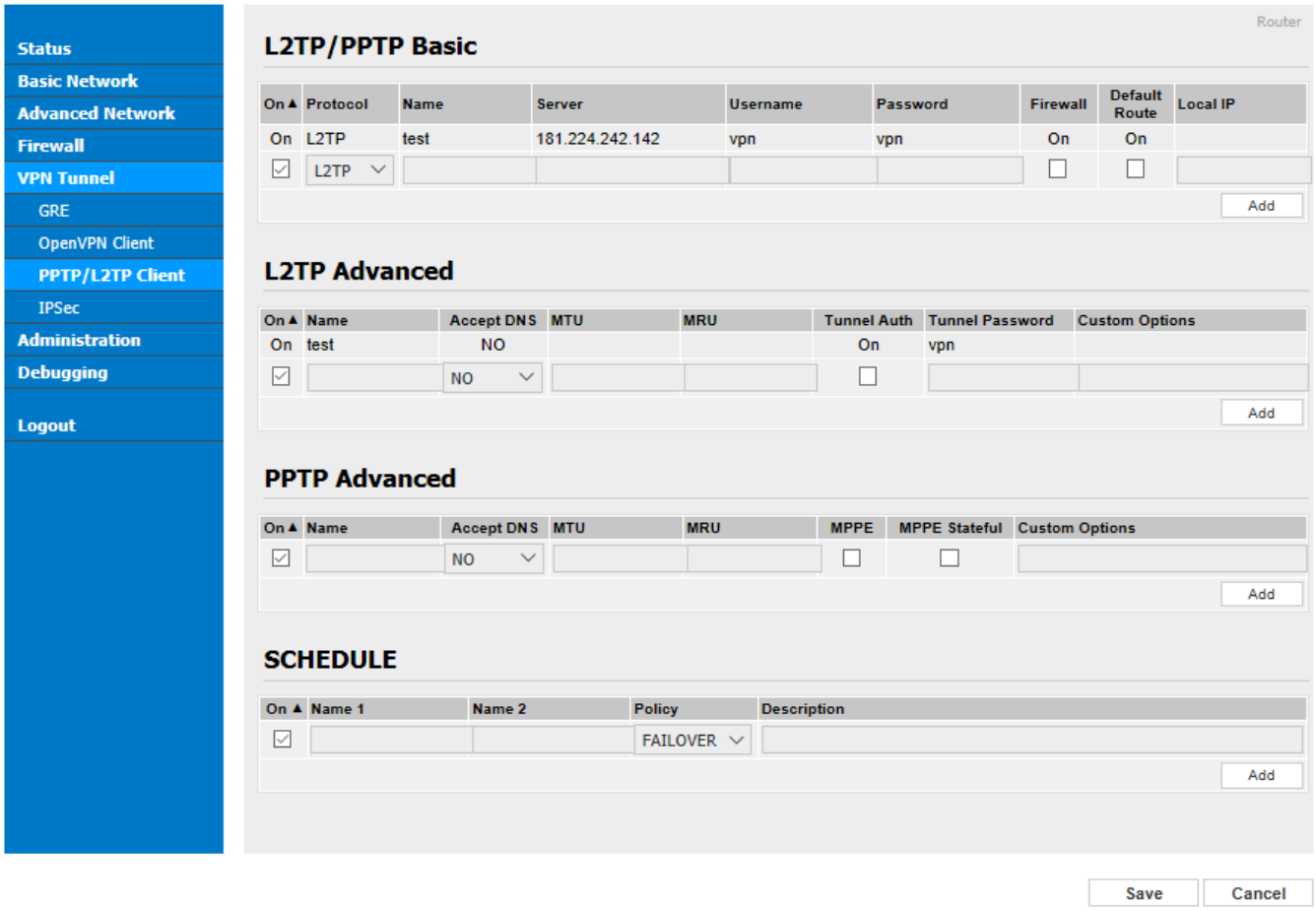
Router VPN Configuration

1) Make sure your router is connected to the internet and showing Internet status page as shown below (See Router Quick Start Guide):

2) Select the 'VPN Tunnel' tab on the left hand pane of the Siretta router web interface. Then choose 'L2TP/PPTP Client' tab and you will be presented with a number of options.

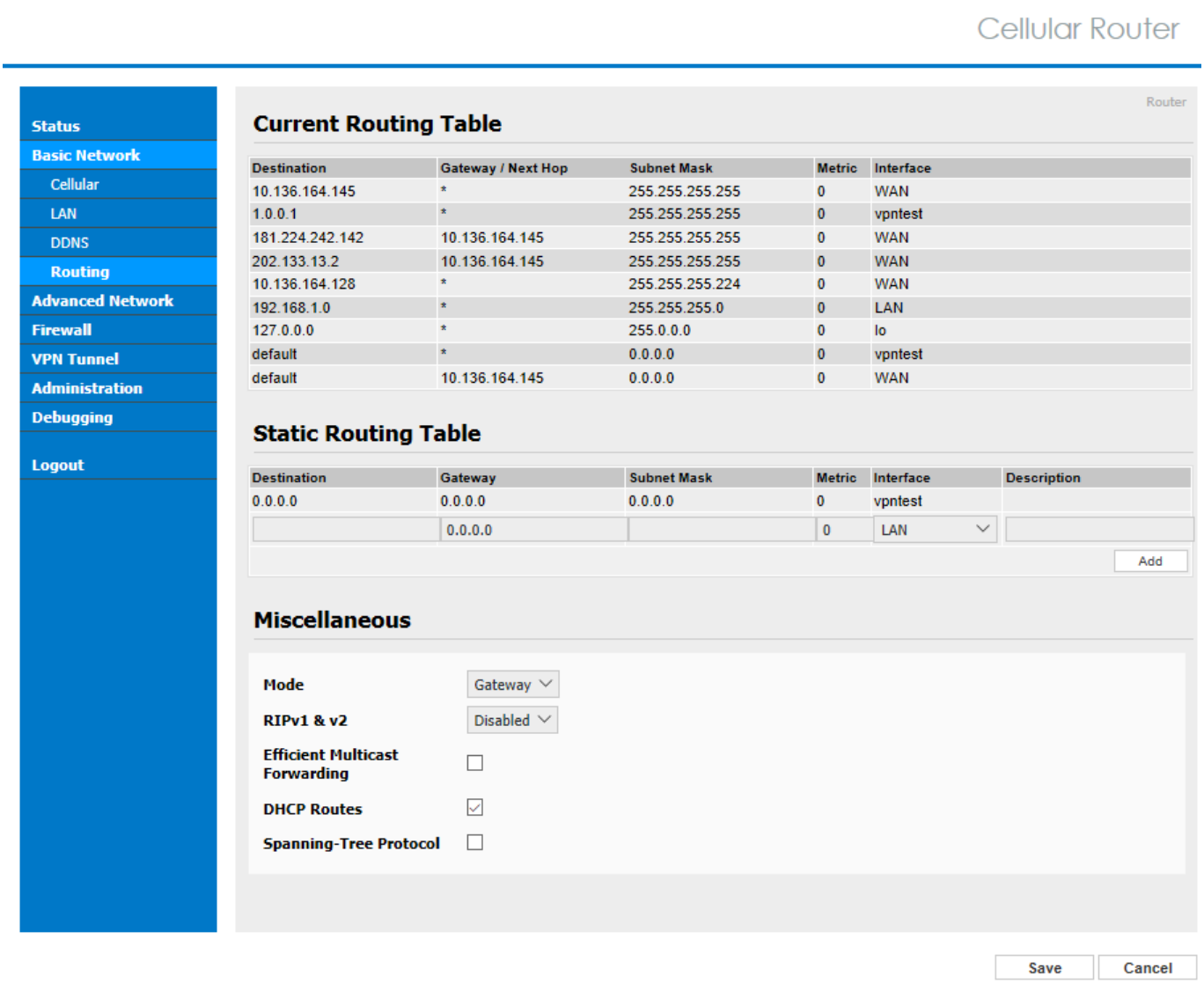
On this page you can enter the server details for the VPN connection by choosing the following:

- Under protocol click on the drop down selection and choose L2TP
- Name the connection by filling in the name field
- Enter the VPN server username under the username field
- Enter the VPN server password under the password field
- Choose if you want to enable the firewall and select the local IP address
- Click 'Add' to add the connection

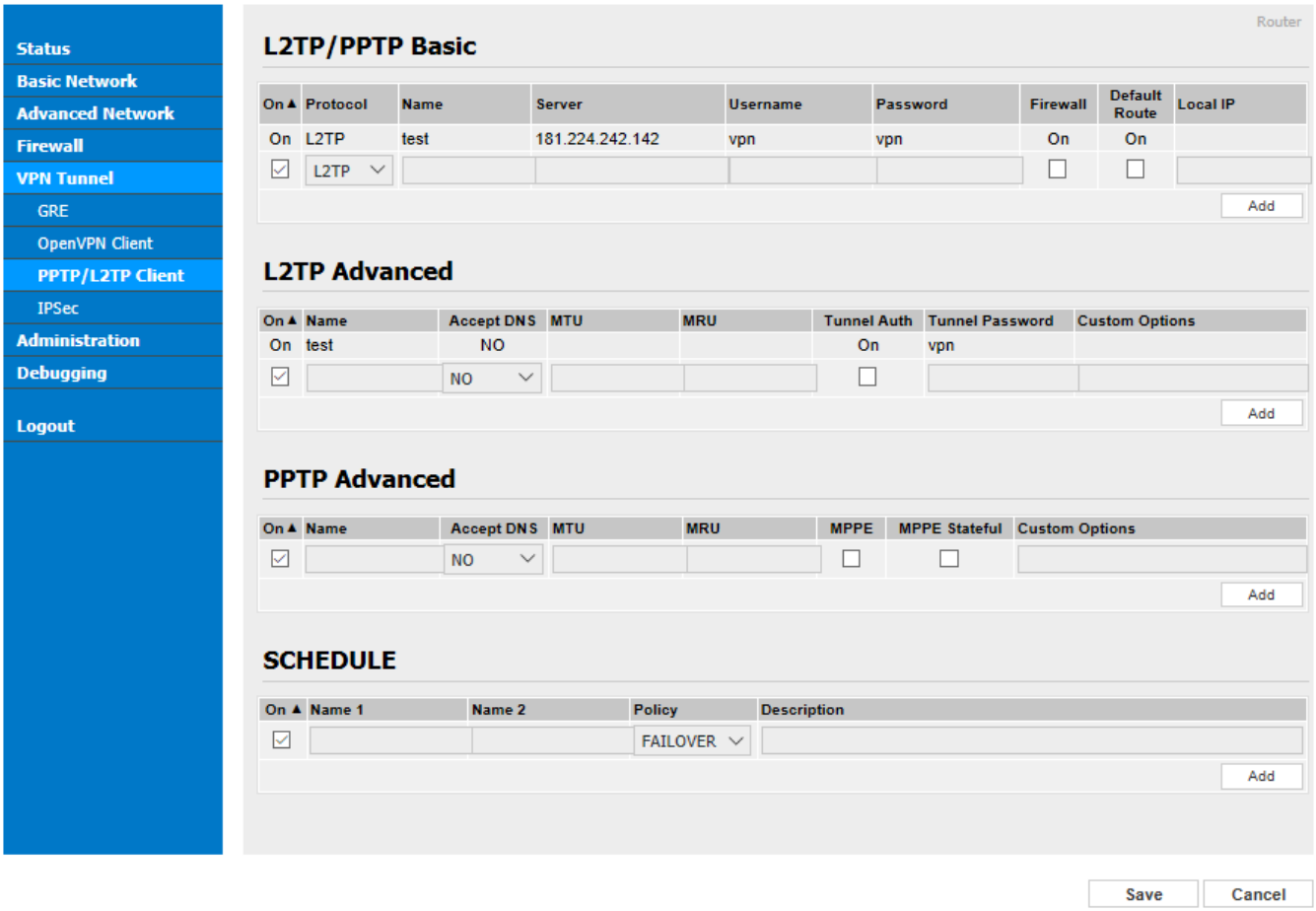


3) Select ‘Basic Network’ -> ‘Routing’ on the left hand pane to show the current routing table. In the Static Routing Table you need to add a new entry:

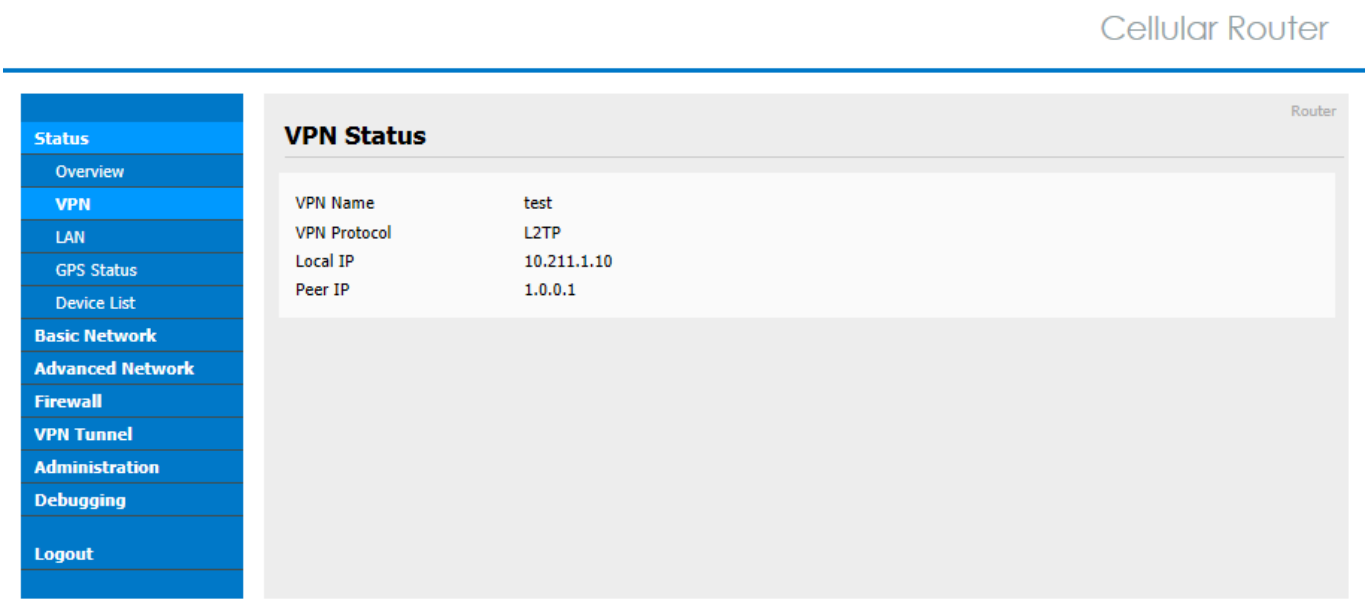
- Set ‘Destination’, ‘Gateway’, ‘Subnet Mask’ to ‘0.0.0.0’
- Set Metric to ‘0’
- Choose the VPN interface setup for the L2TP connection. (In this example the VPN connection is called ‘vpntest’ and can be selected from the dropdown menu.)
- Click ‘Add’ button
- Click ‘Save’ button



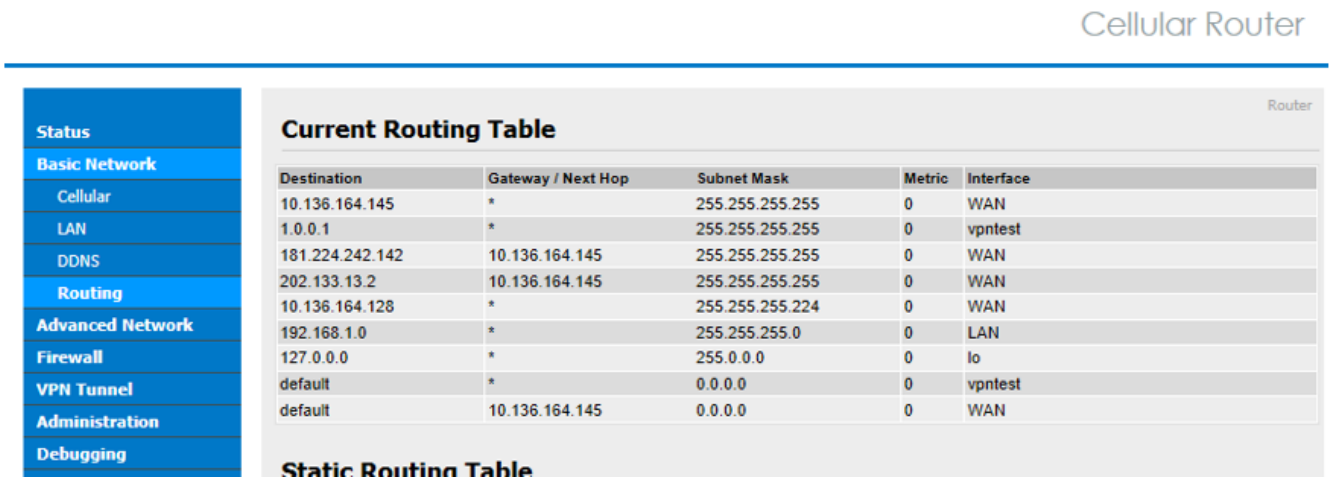
4) Select the ‘VPN Tunnel’ tab on the left pane and choose ‘L2TP/PPTP Client’ tab, you should see “Default Route” is checked to on as shown below.



5) Click on ‘Status’ -> ‘VPN’ and you will see the connection status indicating a connection between PPTP VPN server and router which is PPTP VPN client.

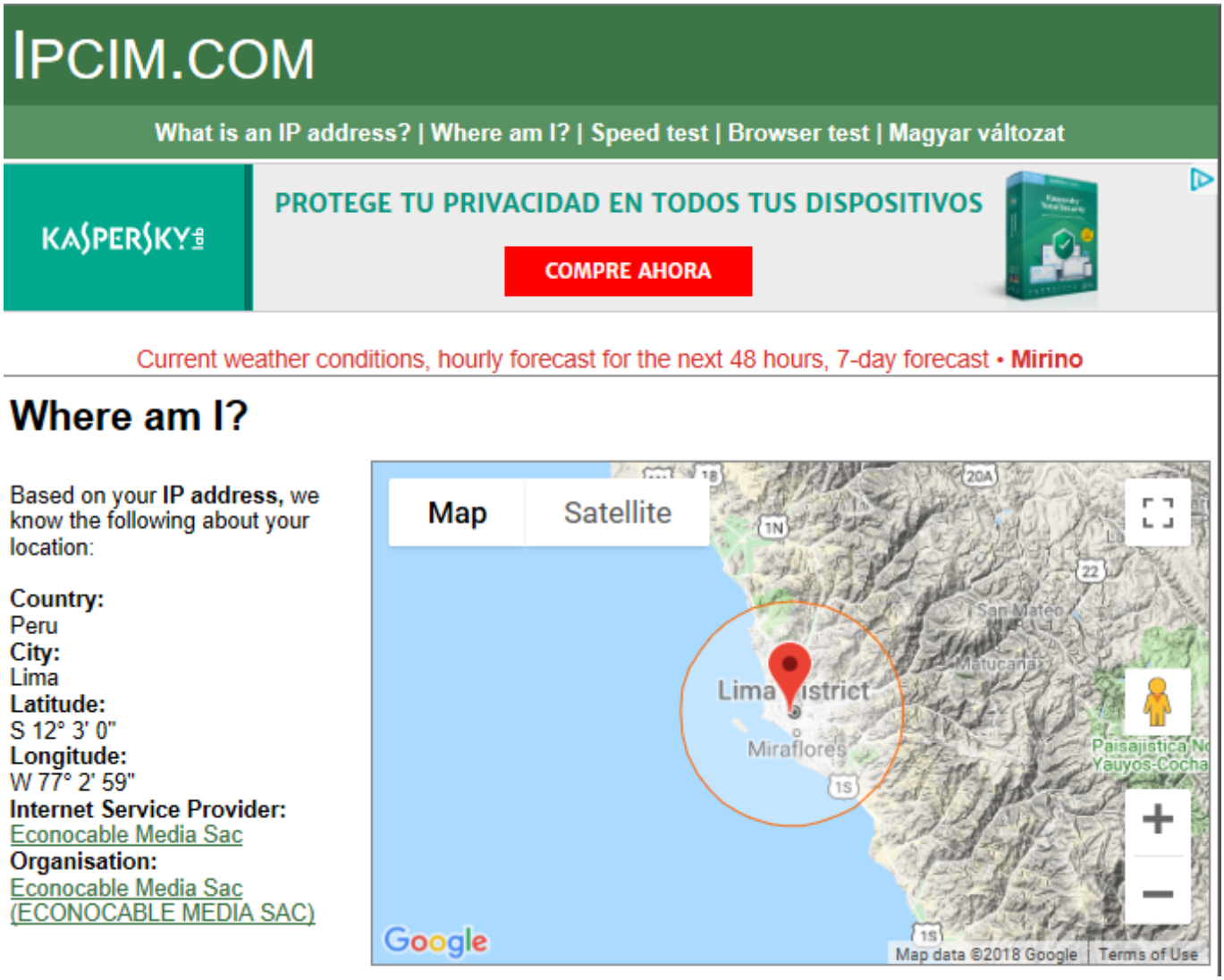


6) You can check the current routing table by selecting ‘Basic Network’ -> ‘Routing’ and you will be presented with a table showing the ‘VPN test’ connection indicating traffic through VPN tunnel.



Destination	Gateway / Next Hop	Subnet Mask	Metric	Interface
10.136.164.145	*	255.255.255.255	0	WAN
1.0.0.1	*	255.255.255.255	0	vpntest
181.224.242.142	10.136.164.145	255.255.255.255	0	WAN
202.133.13.2	10.136.164.145	255.255.255.255	0	WAN
10.136.164.128	*	255.255.255.224	0	WAN
192.168.1.0	*	255.255.255.0	0	LAN
127.0.0.0	*	255.0.0.0	0	lo
default	*	0.0.0.0	0	vpntest
default	10.136.164.145	0.0.0.0	0	WAN

7) You can open the following link https://ipcim.com/en/?p=where using the PC attached to the Router and you will be presented with the screenshot below showing your location is **Peru**. This is using the VPN server from the example.



NOTE: When you open https://ipcim.com/en/?p=where while not connected to the VPN server your exactly location will be displayed.