How to Connect a Siretta Industrial Router to a VPN Tunnel Using IPSec 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 an IPSec 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 IPSec VPN connection between a Siretta router and a server, please obtain the following details:

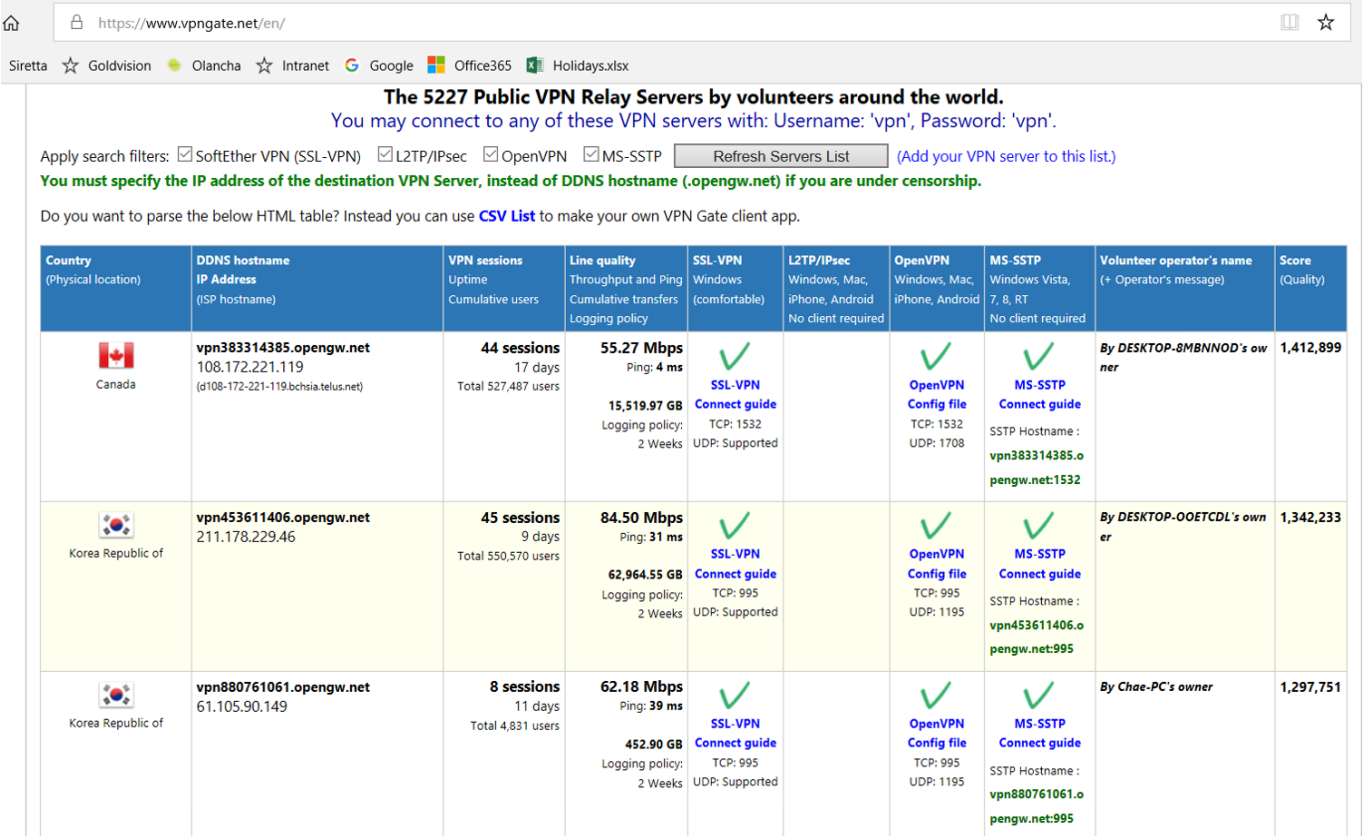
1. VPN Server IP address
2. A pre-shared key, user name and password

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.

VPN Server Details

The example shown below uses a set of temporary details, when opening this link on your web browser you will be presented with the following:



1) Check the L2TP/IPsec box then click Refresh server list. The IPsec servers list will appear as shown below:

https://www.vpngate.net/en/

ta Goldvision Olancha Intranet Google Office365 Holidays.xlsx

The 5229 Public VPN Relay Servers by volunteers around the world.

You may connect to any of these VPN servers with: Username: 'vpn', Password: 'vpn'.

Apply search filters: ☐ SoftEther VPN (SSL-VPN) ☑ L2TP/IPsec ☐ OpenVPN ☐ MS-SSTP Refresh Servers List (Add your VPN server to this list.)

You must specify the IP address of the destination VPN Server, instead of DDNS hostname (.opengw.net) if you are under censorship.

Do you want to parse the below HTML table? Instead you can use **CSV List** to make your own VPN Gate client app.

Country (Physical location)	DDNS hostname IP Address (ISP hostname)	VPN sessions Uptime Cumulative users	Line quality Throughput and Ping Cumulative transfers Logging policy	SSL-VPN Windows (comfortable)	L2TP/IPsec Windows, Mac, iPhone, Android No client required	OpenVPN Windows, Mac, iPhone, Android	MS-SSTP Windows Vista, 7, 8, RT No client required	Volunteer operator's name (+ Operator's message)	Score (Quality)
Korea Republic of	**shooran.opengw.net** 121.168.45.38	**0 sessions** 89 days Total 0 users	**21.32 Mbps** Ping: **37 ms** **0.00 GB** Logging policy: 2 Weeks	✓ SSL-VPN Connect guide TCP: 443	✓ L2TP/IPsec Connect guide	✓ OpenVPN Config file TCP: 443 UDP: 1194	✓ MS-SSTP Connect guide SSTP Hostname : **shooran.opengw.net**	***By ShooRan***	**1,196,460**
Japan	**marimo-net.opengw.net** 110.163.128.93 (mo110-163-128-93.fix.mopera.net)	**296 sessions** 6 days Total 1,753,285 users	**55.70 Mbps** Ping: **6 ms** **103,467.40 GB** Logging policy: 2 Weeks	✓ SSL-VPN Connect guide TCP: 992 UDP: Supported	✓ L2TP/IPsec Connect guide	✓ OpenVPN Config file TCP: 992 UDP: 1194	✓ MS-SSTP Connect guide SSTP Hostname : **marimo-net.opengw.net:992**	***By marimo@marimo.moe*** *E-mail: nekomiminimoe@gmail.com* *"TESTING..."*	**1,152,791**
Peru	**vpn310145142.opengw.net** 181.224.242.142	**23 sessions** 5 days Total 332,279 users	**10.81 Mbps** Ping: **31 ms** **6,453.59 GB** Logging policy: 2 Weeks	✓ SSL-VPN Connect guide TCP: 443 UDP: Supported	✓ L2TP/IPsec Connect guide	✓ OpenVPN Config file TCP: 443 UDP: 1194	✓ MS-SSTP Connect guide SSTP Hostname : **vpn310145142.opengw.net**	***By PI*** *"welcome to ponteinternet.com"*	**907,531**

2) Select and click your choice of server from the list for the detailed configuration details.

VPN Gate Public VPN Relay Servers — Academic Experiment at University of Tsukuba, Japan.

VPN Servers List What is VPN Gate How to Connect Download Join Us Forum Mirror Sites Languages

Connect to VPN Gate by Using L2TP/IPsec VPN Protocol

This document describes how to connect to a VPN Relay Server of VPN Gate by using the L2TP/IPsec VPN Client which is bundled with the operating system.

L2TP/IPsec VPN Client is built-in on Windows, Mac, iOS and Android. It is easier to configure than using OpenVPN. L2TP/IPsec VPN is recommended before you try to use OpenVPN. However, some networks or firewalls block L2TP/IPsec packets. If L2TP/IPsec fails, try OpenVPN.

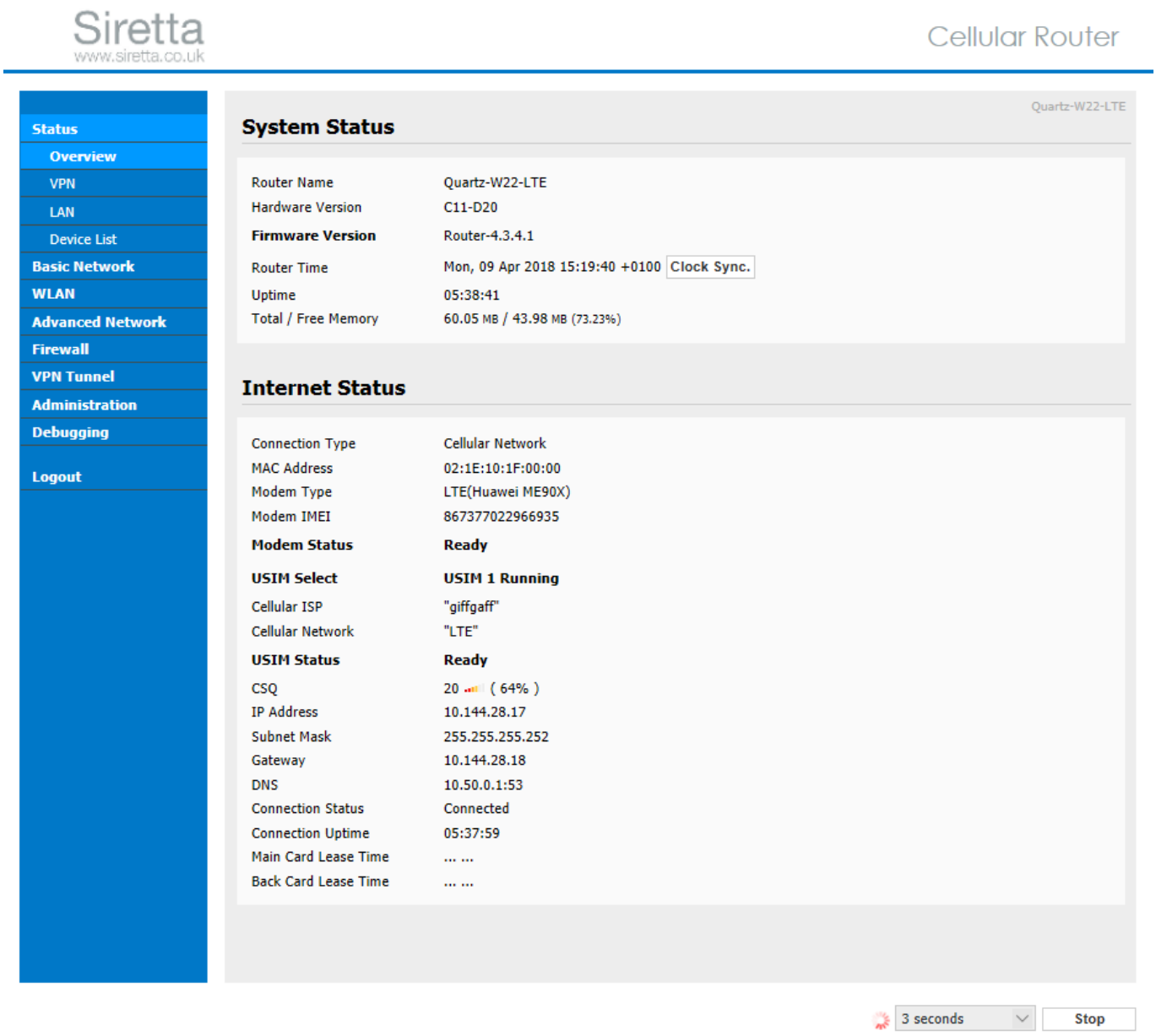
Connecting parameters for L2TP/IPsec VPN

You can quickly configure your L2TP/IPsec VPN Client by using the following parameters if you have already known how to set up.

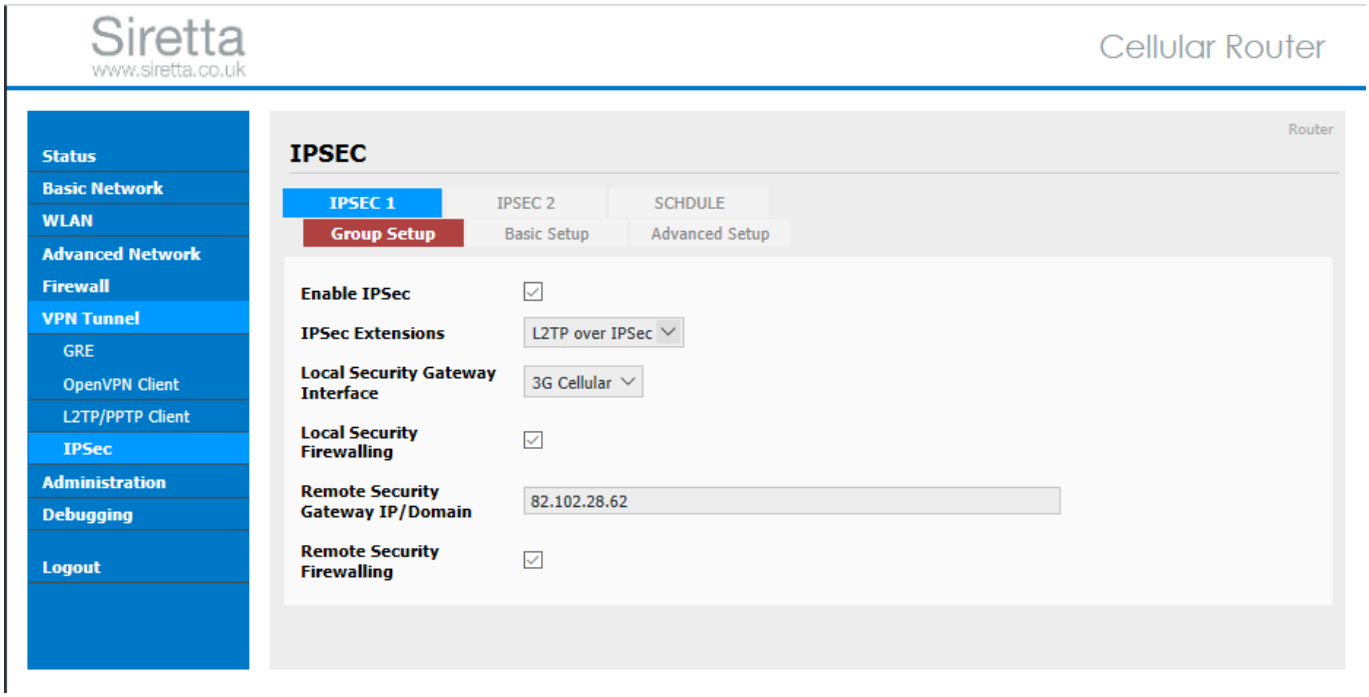
- IP Address / Hostname: **You can obtain them in Public VPN Relay Servers List page.**
  Username: **vpn**, Password: **vpn**
  Pre-shared Key (Secret): **vpn**

Router VPN Configuration

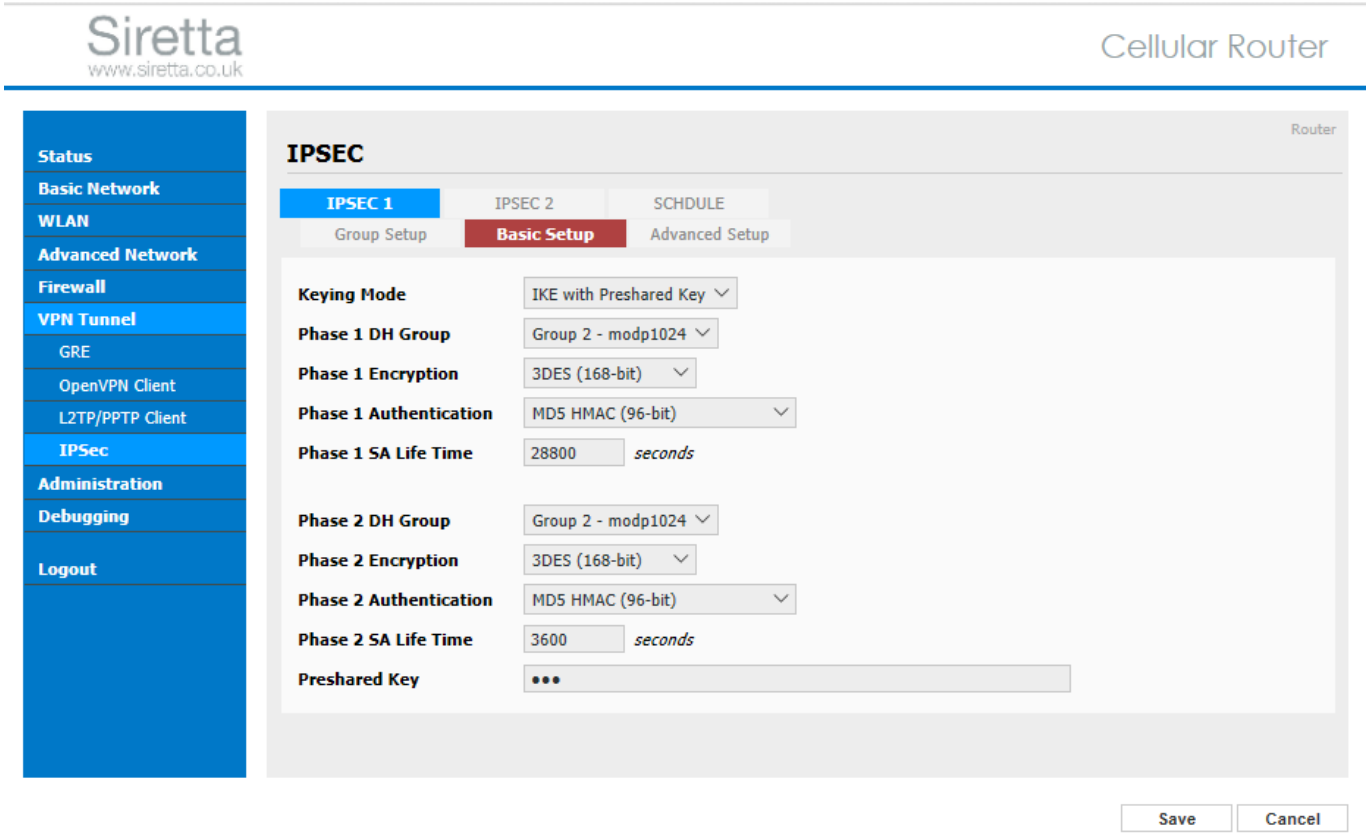
1) Make sure your Router is connected to the internet. The 'Internet Status' information should be similar to the image shown below:



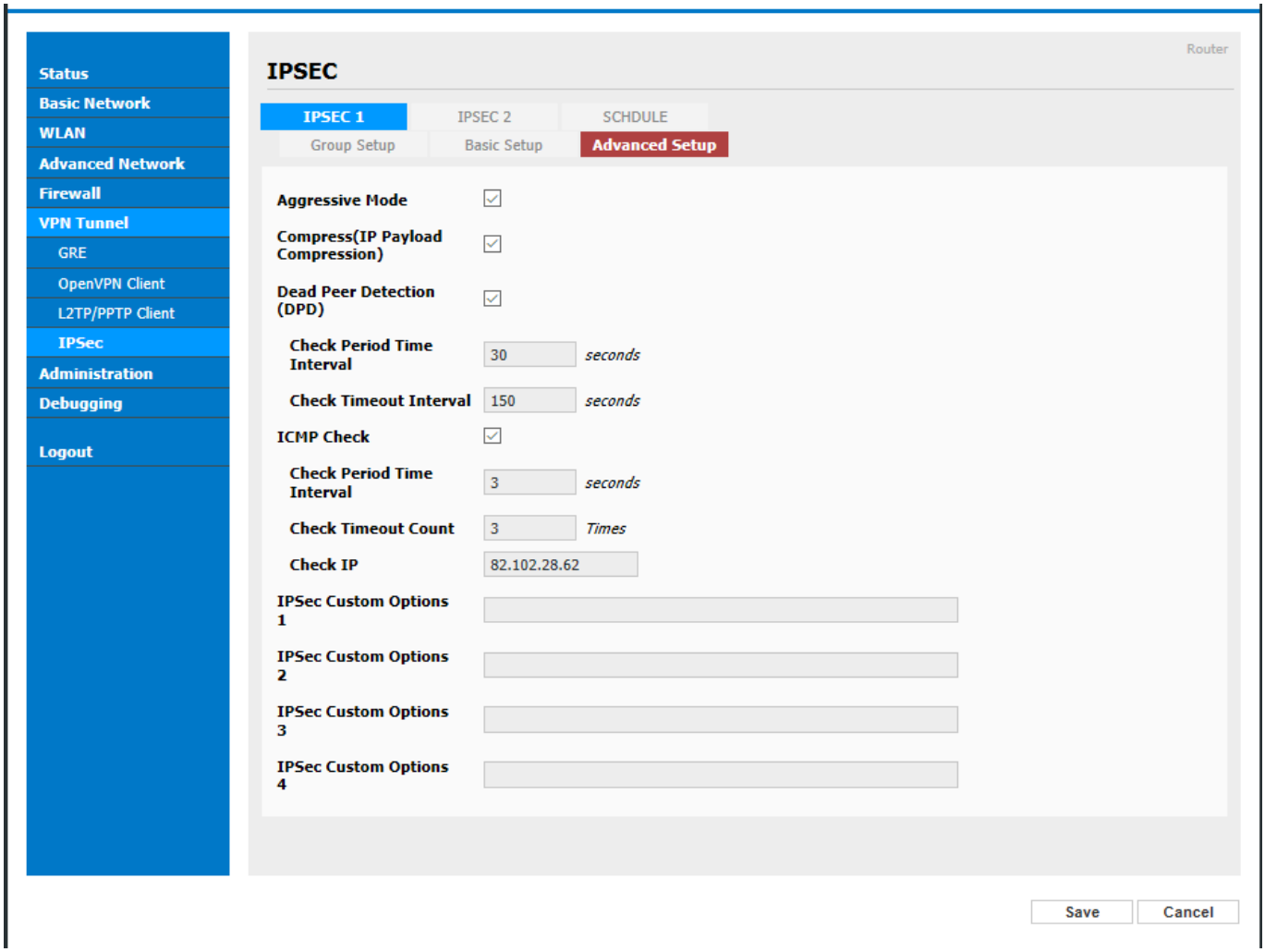
2) Select the VPN Tunnel tab on the left hand pane of the Siretta router web interface. Then select the IPSec tab and you will be presented with a number of options. On 'Group Setup' tab enter the following details for the Server IP address obtained from the VPN server list.



3) On 'Basic Setup' tab enter the Preshared Key details for VPN server obtained from the VPN server list.

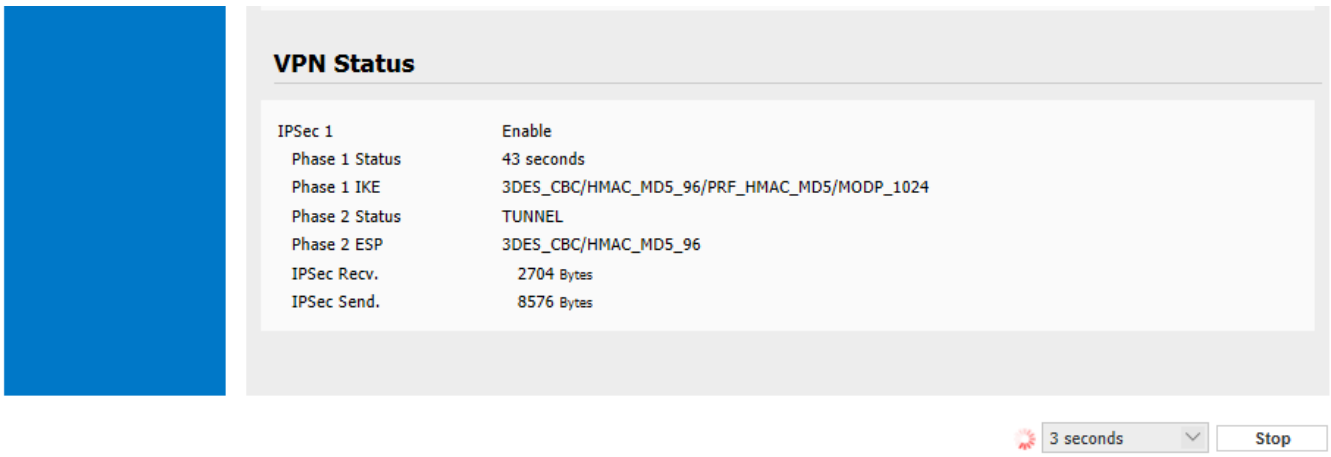


4) On 'Advanced Setup' tab select the required options for the connection to the VPN server obtained from the VPN server list.



5) Click save

6) Once you have saved the VPN connection details the router will restart some of the network services and will attempt to connect to the VPN server. Click 'Status' on the left hand menu to view the VPN connection status and see when the VPN connection is established.



Once the VPN connection has been established between the router and the VPN server, the connected equipment will be able to directly access all of the network resources of the connected server and communicate with any devices on the server's network.