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

1. OpenVPN Server IP address
2. Certificate Authority, Client Certificate and Client Key

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.

OpenVPN 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:

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

Goldvision Olancha Intranet Google Office365 Holidays.xlsx

The 5076 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)
Canada	vpn383314385.opengw.net 108.172.221.119 (d108-172-221-119.bchsia.telus.net)	26 sessions 19 days Total 535,747 users	53.44 Mbps Ping: 5 ms 15,738.52 GB Logging policy: 2 Weeks	✓ SSL-VPN Connect guide TCP: 1532 UDP: Supported		✓ OpenVPN Config file TCP: 1532 UDP: 1708	✓ MS-SSTP Connect guide SSTP Hostname : vpn383314385.opengw.net:1532	*By DESKTOP-8MBNNOD's owner*	1,402,099
Japan	vpn686053815.opengw.net 124.87.79.133 (p2044133-ipbf806souka.saitama.ocn.ne.jp)	37 sessions 7 days Total 362,312 users	88.20 Mbps Ping: 7 ms 32,056.40 GB Logging policy: 2 Weeks	✓ SSL-VPN Connect guide UDP: Supported		✓ OpenVPN Config file UDP: 1239		*By MyComputer's owner*	1,391,233
Korea Republic of	vpn453611406.opengw.net 211.178.229.46	71 sessions 11 days Total 556,313 users	72.16 Mbps Ping: 31 ms 63,405.25 GB Logging policy: 2 Weeks	✓ SSL-VPN Connect guide TCP: 995 UDP: Supported		✓ OpenVPN Config file TCP: 995 UDP: 1195	✓ MS-SSTP Connect guide SSTP Hostname : vpn453611406.opengw.net:995	*By DESKTOP-OOETCDL's owner*	1,357,833
Japan	vpn922334262.opengw.net 58.0.166.189 (ntsitm579189.sitm.nt.ngn.ppp.infoweb.ne.jp)	79 sessions 5 days Total 113,761 users	43.09 Mbps Ping: 6 ms 6,312.93 GB Logging policy: 2 Weeks	✓ SSL-VPN Connect guide TCP: 1311 UDP: Supported		✓ OpenVPN Config file TCP: 1311 UDP: 1664	✓ MS-SSTP Connect guide SSTP Hostname : vpn922334262.opengw.net:1311	*By Hirano-PC's owner*	1,278,787

1) Check the OpenVPN box then click Refresh server list, OpenVPN server lists will appear as shown below:

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)
Canada	vpn383314385.opengw.net 108.172.221.119 (d108-172-221-119.bchsia.telus.net)	26 sessions 19 days Total 535,747 users	53.44 Mbps Ping: 5 ms 15,738.52 GB Logging policy: 2 Weeks	✓ SSL-VPN Connect guide TCP: 1532 UDP: Supported		✓ OpenVPN Config file TCP: 1532 UDP: 1708	✓ MS-SSTP Connect guide SSTP Hostname : vpn383314385.opengw.net:1532	*By DESKTOP-8MBNNOD's owner*	1,402,099
Japan	vpn686053815.opengw.net 124.87.79.133 (p2044133-ipbf806souka.saitama.ocn.ne.jp)	37 sessions 7 days Total 362,312 users	88.20 Mbps Ping: 7 ms 32,056.40 GB Logging policy: 2 Weeks	✓ SSL-VPN Connect guide UDP: Supported		✓ OpenVPN Config file UDP: 1239		*By MyComputer's owner*	1,391,233
Korea Republic of	vpn453611406.opengw.net 211.178.229.46	71 sessions 11 days Total 556,313 users	72.16 Mbps Ping: 31 ms 63,405.25 GB Logging policy: 2 Weeks	✓ SSL-VPN Connect guide TCP: 995 UDP: Supported		✓ OpenVPN Config file TCP: 995 UDP: 1195	✓ MS-SSTP Connect guide SSTP Hostname : vpn453611406.opengw.net:995	*By DESKTOP-OOETCDL's owner*	1,357,833
Japan	vpn922334262.opengw.net 58.0.166.189 (ntsitm579189.sitm.nt.ngn.ppp.infoweb.ne.jp)	79 sessions 5 days Total 113,761 users	43.09 Mbps Ping: 6 ms 6,312.93 GB Logging policy: 2 Weeks	✓ SSL-VPN Connect guide TCP: 1311 UDP: Supported		✓ OpenVPN Config file TCP: 1311 UDP: 1664	✓ MS-SSTP Connect guide SSTP Hostname : vpn922334262.opengw.net:1311	*By Hirano-PC's owner*	1,278,787
Korea Republic of	shooran.opengw.net 121.168.45.38	0 sessions 89 days Total 0 users	20.15 Mbps Ping: 31 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*	1,201,725

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

Download the OpenVPN Configuration File (.ovpn file)

You can download the .ovpn file to connect this OpenVPN server.
Use one of the following .ovpn files. Refer the Hint to choose one.

You must specify IP address of the destination VPN Server, instead of DDNS hostname (.opengw.net) if you are in a big-brother country.

How to Install and Set up the OpenVPN Client

The .ovpn file which is including DDNS hostname

Destination DDNS Hostname: **vpn383314385.opengw.net**

OpenVPN Configuration File: vpn383314385.opengw.net (UDP 1708)
OpenVPN

OpenVPN Configuration File: vpn383314385.opengw.net (TCP 1532)
OpenVPN

You must specify IP address of the destination VPN Server, instead of DDNS hostname (.opengw.net) if you are in a big-brother country.

The .ovpn file which is including IP address

Destination IP Address: **108.172.221.119**

OpenVPN Configuration File: 108.172.221.119 (UDP 1708)
OpenVPN

OpenVPN Configuration File: 108.172.221.119 (TCP 1532)
OpenVPN

Configuration File

Once you have chosen a configuration file you can open the file in a text editor and you will be presented with the following information:

```
#############################################################################
# The HTTP/HTTPS proxy setting.
#
# Only if you have to use the Internet via a proxy, uncomment the below
# two lines and specify the proxy address and the port number.
# In the case of using proxy-authentication, refer the OpenVPN manual.

;http-proxy-retry
;http-proxy [proxy server] [proxy port]

#############################################################################
# The encryption and authentication algorithm.
#
# Default setting is good. Modify it as you prefer.
# When you specify an unsupported algorithm, the error will occur.
#
# The supported algorithms are as follows:
```

```
# cipher: [NULL-CIPHER] NULL AES-128-CBC AES-192-CBC AES-256-CBC BF-CBC
# CAST-CBC CAST5-CBC DES-CBC DES-EDE-CBC DES-EDE3-CBC DESX-CBC
# RC2-40-CBC RC2-64-CBC RC2-CBC
# auth: SHA SHA1 MD5 MD4 RMD160

cipher AES-128-CBC
auth SHA1

##############################################################################
# Other parameters necessary to connect to the VPN Server.
#
# It is not recommended to modify it unless you have a particular need.

resolv-retry infinite
nobind
persist-key
persist-tun
client
verb 3
#auth-user-pass

##############################################################################
# The certificate file of the destination VPN Server.
#
# The CA certificate file is embedded in the inline format.
# You can replace this CA contents if necessary.
# Please note that if the server certificate is not a self-signed, you have to
# specify the signer's root certificate (CA) here.

-----BEGIN CERTIFICATE-----
MIIF2DCCA8CgAwIBAgIQTKr5yttjb+Af907YWwOGnTANBgkqhkiG9w0BAQwFADCB
hTELMAkGA1UEBhMCR0IxGzAZBgNVBAgTEkdyZWF0ZXIgTWFuY2hlc3RlcjEQMA4G
A1UEBxMHU2FsZm9yZDEaMBgGA1UEChMRQ09NT0RPIENBIExpbWl0ZWQxKzApBgNV
BAMTIkNPTU9ETyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwHhcNMTAwMTE5
MDAwMDAwWhcNMzgwMTE4MjM1OTU5WjCBhTELMAkGA1UEBhMCR0IxGzAZBgNVBAgT
EkdyZWF0ZXIgTWFuY2hlc3RlcjEQMA4GA1UEBxMHU2FsZm9yZDEaMBgGA1UEChMR
Q09NT0RPIENBIExpbWl0ZWQxKzApBgNVBAMTIkNPTU9ETyBSU0EgQ2VydGlmaWNh
dGlvbiBBdXRob3JpdHkwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCR
6FSS0gpWsawNJN3Fz0RndJkrN6N9I3AAcbxT38T6KhKPS38QVr2fcHK3YX/JSw8X
pz3jsARh7v8Rl8f0hj4K+j5c+ZPmNHrZFGvnnLOFoIJ6dq9xkNfs/Q36nGz637CC
9BR++b7Epi9Pf5l/tfxnQ3K9DADWietrLNPtj5gcFKt+5eNu/Nio5JIk2kNrYrhV
/erBvGy2i/MOjZrkm2xpmfh4SDBF1a3hDTxFYPwyllEnvGfDyi62a+pGx8cgoLEf
Zd5ICLqkTqnyg0Y3hOvozIFIQ2dOciqbXL1MGyiKXCJ7tKuY2e7gUYPDCUZObT6Z
+pUX2nwzV0E8jVHtC7ZcryxjGt9XyD+86V3Em69FmeKjWiS0uqlWPc9vqv9JWL7w
qP/0uK3pN/u6uPQLOvnoQ0IeidiEyxPx2bvhiWC4jChWrBQdnArncevPDt09qZah
SL0896+1DSJMwBGB7FY79tOi4lu3sgQiUpWAk2nojkxl8ZEDLXB0AuqLZxUpaVIC
u9ffUGpVRr+goyhhf3DQw6KqLCGqR84onAZFdr+CGCe01a60y1Dma/RMhnEw6abf
Fobg2P9A3fvQQoh/ozM6LlweQRGBY84YcWsr7KaKtzFcOmpH4MN5WdYgGq/yapiq
crxXStJLnbsQ/LBMQeXtHT1eKJ2czL+zUdqnR+WEUwIDAQABo0IwQDAdBgNVHQ4E
FgQUu69+Aj36pvE8hI6t7jiY7NkyMtQwDgYDVR0PAQH/BAQDAgEGMA8GA1UdEwEB
/wQFMAMBAf8wDQYJKoZIhvcNAQEMBQADggIBAArx1UaEt65Ru2yyTUEUAJNMnMvl
wFTPoCWOAvn9sKIN9SCYPBMtrFaisNZ+EZLpLrqeLppysb0ZRGxhNaKatBYSaVqM
4dc+pBroLwP0rmEdEBsqpIt6xf4FpuHA1sj+nq6PK7o9mfjYcwlYRm6mnPTXJ9OV
2jeDchzTc+CiR5kDOF3VSXkAKRzH7JsgHAckaVd4sjn8OoSgtZx8jb8uk2Intzna
FxiuvTwJaP+EmzzV1gsD41eeFPfR60/IvYcjt7ZJQ3mFXLrrkguhxuhoqEwWsRqZ
```

CuhTLJK7oQkYdQxlqHvLI7cawiiFwxv/0Cti76R7CZGYZ4wUAc1oBmpjIXUDgIiK
boHGhfKppC3n9KUkEEeDys30jXlYsQab5xoq2Z0B15R97QNKyvDb6KkBPvVWmcke
jkk9u+UJueBPSZI9FoJAzMxZxuY67RIuaTxslbH9qh17f4a+Hg4yRvv7E491f0yL
S0Zj/gA0QHDBw7mh3aZw4gSzQbzpgJHqZJx64SIDqZxubw5lT2yHh17zbqD5daWb
QOhTsiedSrnAdyGN/4fy3ryM7xfft0kL0fJuMAsaDk527RH89elWsn2/x20Kk4yl
0MC2Hb46TpSi125sC8KKfPog88Tk5c0NqMuRkrF8hey1FGlmDoLnzc7ILaZRfyHB
NVOFBkpdn627G190
-----END CERTIFICATE-----

```
##############################################################################
# The client certificate file (dummy).
#
# In some implementations of OpenVPN Client software
# (for example: OpenVPN Client for iOS),
# a pair of client certificate and private key must be included on the
# configuration file due to the limitation of the client.
# So this sample configuration file has a dummy pair of client certificate
# and private key as follows.
```

-----BEGIN CERTIFICATE-----
MIICxjCCAa4CAQAwDQYJKoZIhvcNAQEFBQAwKTEaMBgGA1UEAxMRVlBOR2F0ZUNs
aWVudENlcnQxCzAJBgNVBAYTAkpQMB4XDTEzMDIxMTAzNDk0OVoXDTM3MDExOTAz
MTQwN1owKTEaMBgGA1UEAxMRVlBOR2F0ZUNsaWVudENlcnQxCzAJBgNVBAYTAkpQ
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA5h2lgQQYUjwoKYJbzVZA
5VcIGd5otPc/qZRMt0KItCFA0s9RwReNVa9fDRFLRBhcITOlv3FBcW3E8h1Us7RD
4W8GmJe8zapJnLsD39OSMRCzZJnczW4OCH1PZRZWKqDtjlNca9AF8a65jTmlDxCQ
CjntLIWk5OLLVkFt9/tScc1GDtci55ofhaNAYMPiH7V8+1g66pGHXAoWK6AQVH67
XCKJnGB5nlQ+HsMYPV/O49Ld91ZN/2tHkcaLLyNtywxVPRSsRh480jju0fcCsv6h
p/0yXnTB//mWutBGpdUlIbwiITbAmrsbYnjigRvnPqX1RNJUbi9Fp6C2c/HIFJGD
ywIDAQABMA0GCSqGSIb3DQEBBQUAA4IBAQChO5hgcw/4oWfoEFLu9kBa1B//kxH8
hQkChVNn8BRC7Y0URQitPl3DKEed9URBDdg2KOAz77bb6ENPiliD+a38UJHIRMqe
UBHhllOHIzvDhHFbaovALBQceeBzdkQxsKQESKmQmR832950UCovoyRB61UyAV7h
+mZhYPGRKXKSJI6s0Egg/Cri+Cwk4bjJfrb5hVse11yh4D9MHhwSfCOH+0z4hPUT
Fku7dGavURO5SVxMn/sL6En5D+oSeXkadHpDs+Airym2YHh15h0+jPSOoR6yiVp/
6zZeZkrN43kuS73KpKDFjfFPh8t4r1gOIjttkNcQqBccusnplQ7HJpsk
-----END CERTIFICATE-----

-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEA5h2lgQQYUjwoKYJbzVZA5VcIGd5otPc/qZRMt0KItCFA0s9R
wReNVa9fDRFLRBhcITOlv3FBcW3E8h1Us7RD4W8GmJe8zapJnLsD39OSMRCzZJnc
zW4OCH1PZRZWKqDtjlNca9AF8a65jTmlDxCQCjntLIWk5OLLVkFt9/tScc1GDtci
55ofhaNAYMPiH7V8+1g66pGHXAoWK6AQVH67XCKJnGB5nlQ+HsMYPV/O49Ld91ZN
/2tHkcaLLyNtywxVPRSsRh480jju0fcCsv6hp/0yXnTB//mWutBGpdUlIbwiITbA
mrsbYnjigRvnPqX1RNJUbi9Fp6C2c/HIFJGDywIDAQABAoIBAERV7X5AvxA8uRiK
k8SIpsD0dX1pJOMIwakUVyvc4EfN0DhKRNb4rYoSiEGTLyzLpyBc/A28Dlkm5eOY
fjzXfYkGtYi/Ftxkg3O9vcrMQ4+6i+uGHaIL2rL+s4MrfO8v1xv6+Wky33EEGCou
QiwVGRFQXnRoQ62NBCFbUNLhmXwdj1akZzLU4p5R4zA3QhdxwEIatVLt0+7owLQ3
lP8sfXhppPOXjTqMD4QkYwzPAa8/zF7acn4kryrUP7Q6PAfd0zEVqNy9ZCZ9ffho
zXedFj486IFoc5gnTp2N6jsnVj4LCGIhlVHlYGozKKFqJcQVGsHCqq1oz2zjW6LS
oRYIHgECgYEA8zZrkCwNYSXJuODJ3m/hOLVxcxgJuwXoiErWd0E42vPanjjVMhnt
KY5l8qGMJ6FhK9LYx2qCrf/E0XtUAZ2wVq3ORTyGnsMWre9tLYs55X+ZN10Tc75z
4hacbU0hqKN1HiDmsMRY3/2NaZHoy7MKnwJJBaG48l9CCTlVwMHocIECgYEA8jby
dGjxTH+6XHWNizb5SRbZxAnyEeJeRwTMh0gGzwGPpH/sZYGzyu0SySXWCnZh3Rgq
5uLlNxtrXrljZlyi2nQdQgsq2YrWUs0+zgU+22uQsZpSAftmhVrtvet6MjVjbByY

DADciEVUdJYIXk+qnFUJyeroLIkTj7WYKZ6RjksCgYBoCFIwRDeg42oK89RFmnOr
LymNAq4+2oMhsWlVb4ejWIWeAk9nc+GXUfrXszRhS01mUnU5r5ygUvRcarV/T3U7
TnMZ+I7Y4DgWRIDd51znhxIBtYV5j/C/t85HjqOkH+8b6RTkbchaX3mau7fpUfds
Fq0nhIq42fhEO8srfYYwgQKBgQCyhi1N/8taRwpk+3/IDEzQwjbfdzUkWWSDk9Xs
H/pkuRHWfTMP3flWqEYgW/LW40peW2HDq5imdV8+AgZxe/XMbaji9Lgwf1RY005n
KxaZQz7yqHupWlLGF68DPHxkZVVSagDnV/sztWX6SFsCqFVnxIXifXGC4cW5Nm9g
va8q4QKBgQCEhLVeUfdwKvkZ94g/GFz731Z2hrdVhgMZaU/u6t0V95+YezPNCQZB
wmE9Mmlbq1emDeROivjCfoGhR3kZXW1pTKlLh6ZMUQUOpptdXva8XxfoqQwa3enA
M7muBbF0XN7VO80iJPv+PmIZdEIAkpwKfi201YB+BafCIuGxIF50Vg==
-----END RSA PRIVATE KEY-----

##

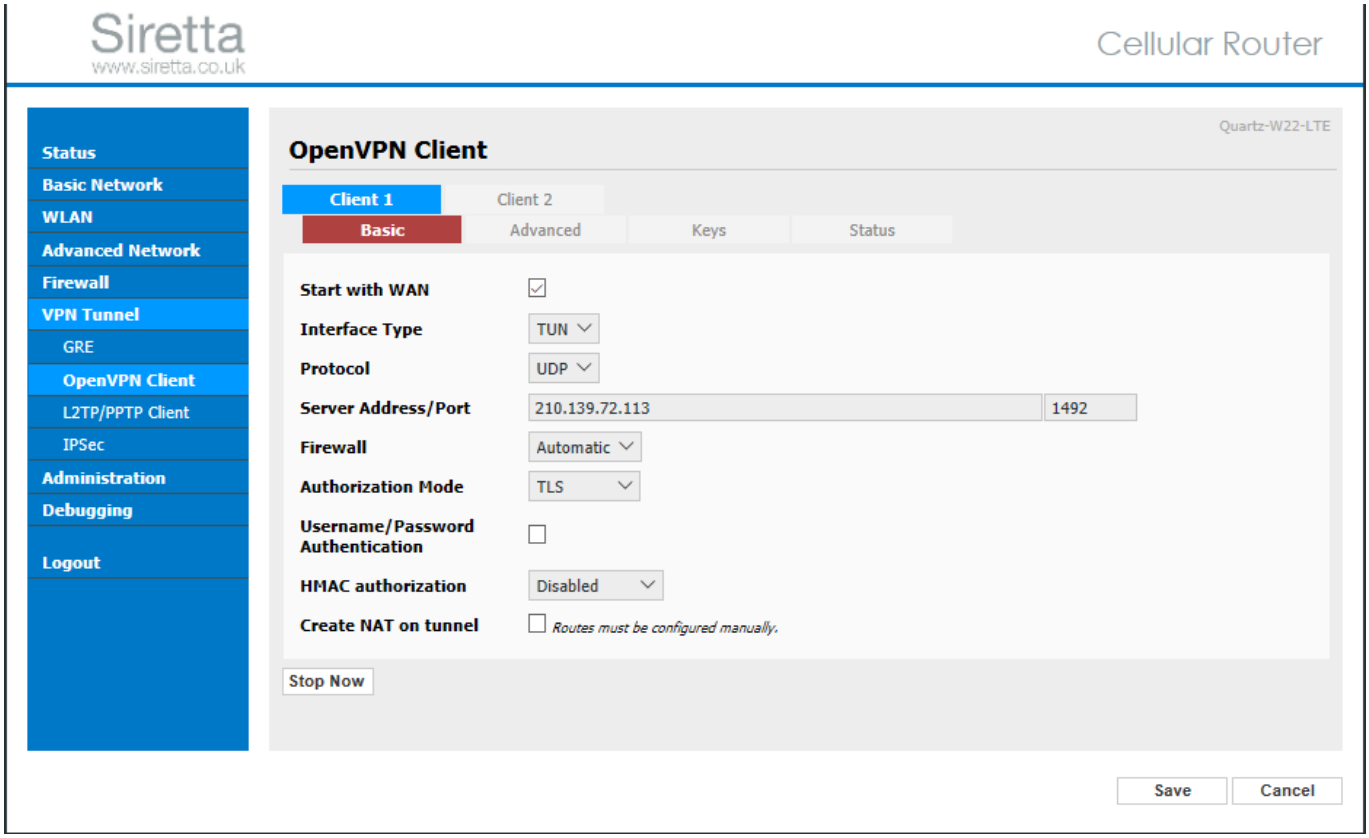
NOTE: The individual keys will be used later in the setup of the router.

Router VPN Configuration

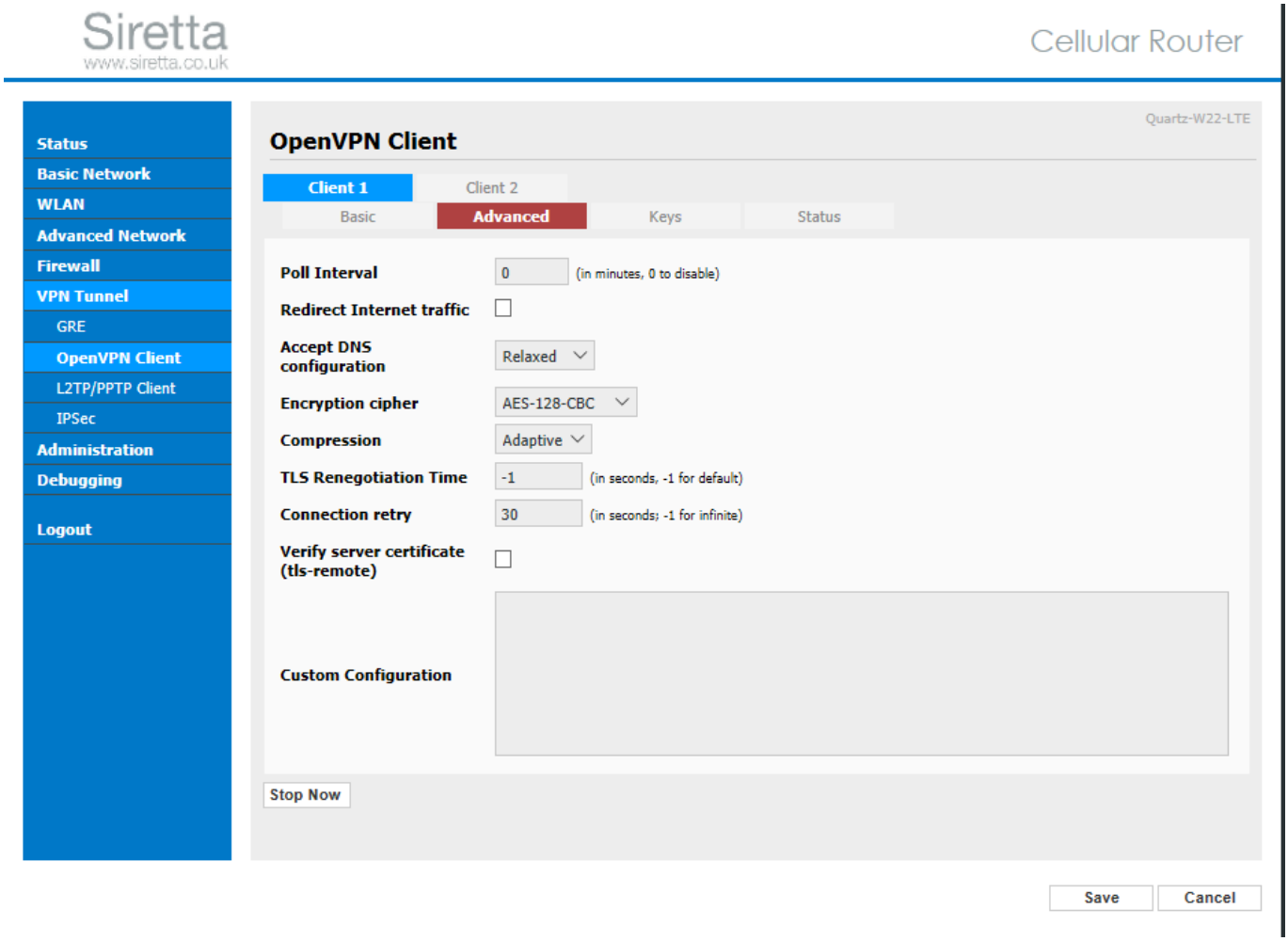
1) Make sure your Router is connected to the internet. The 'Internet Status' information should be similar to the image shown below:

2) Select the VPN tunnel tab on the left hand pane of the Siretta router web interface. Then select OpenVPN client tab and you will be presented with a number of options. On the 'Basic' tab enter the Server Address, Port Number, Firewall, Authorization Mode and Authentication options.

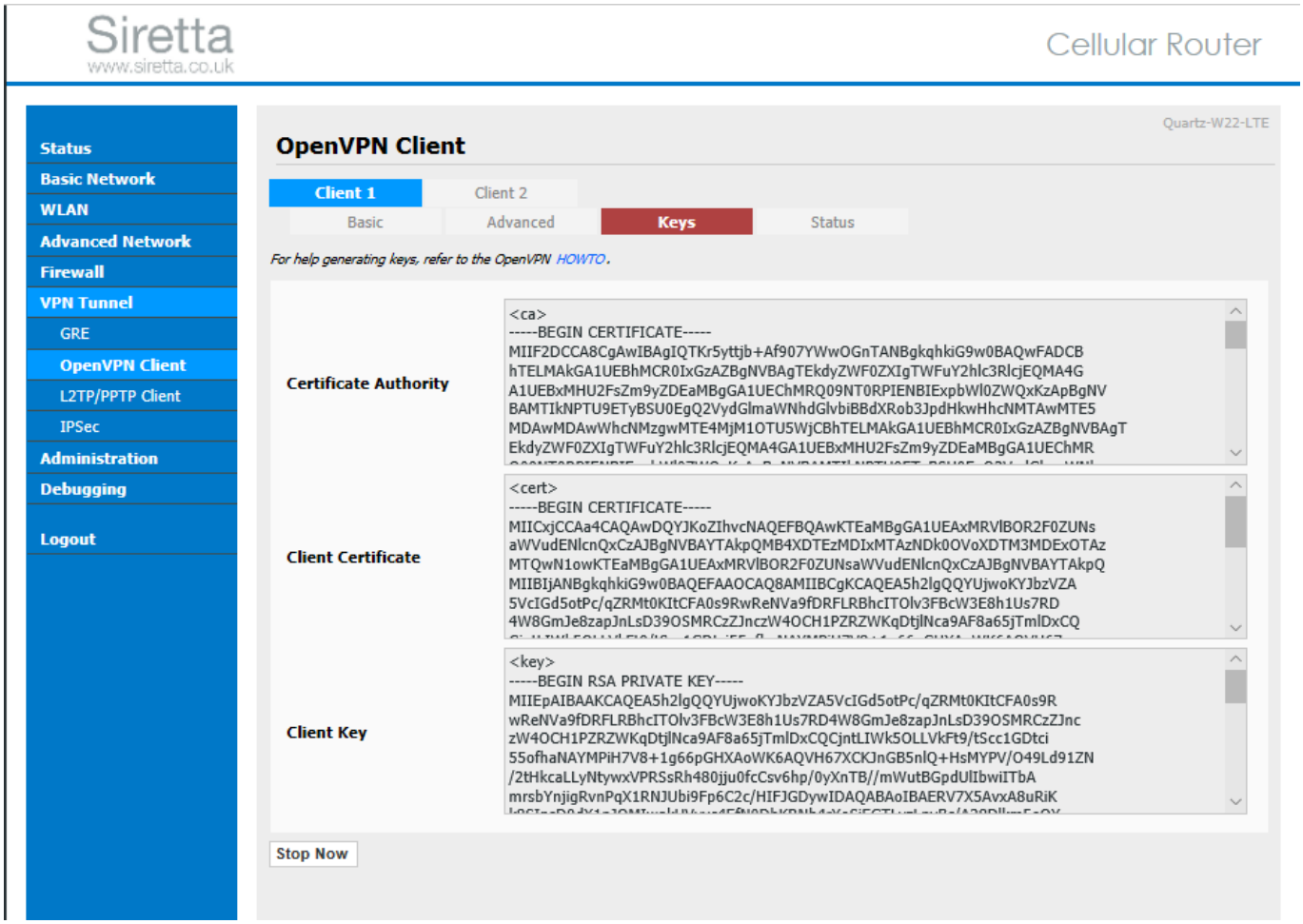
Click on save.



3) Select the 'Advanced' tab then key in your required settings. An example is shown below:

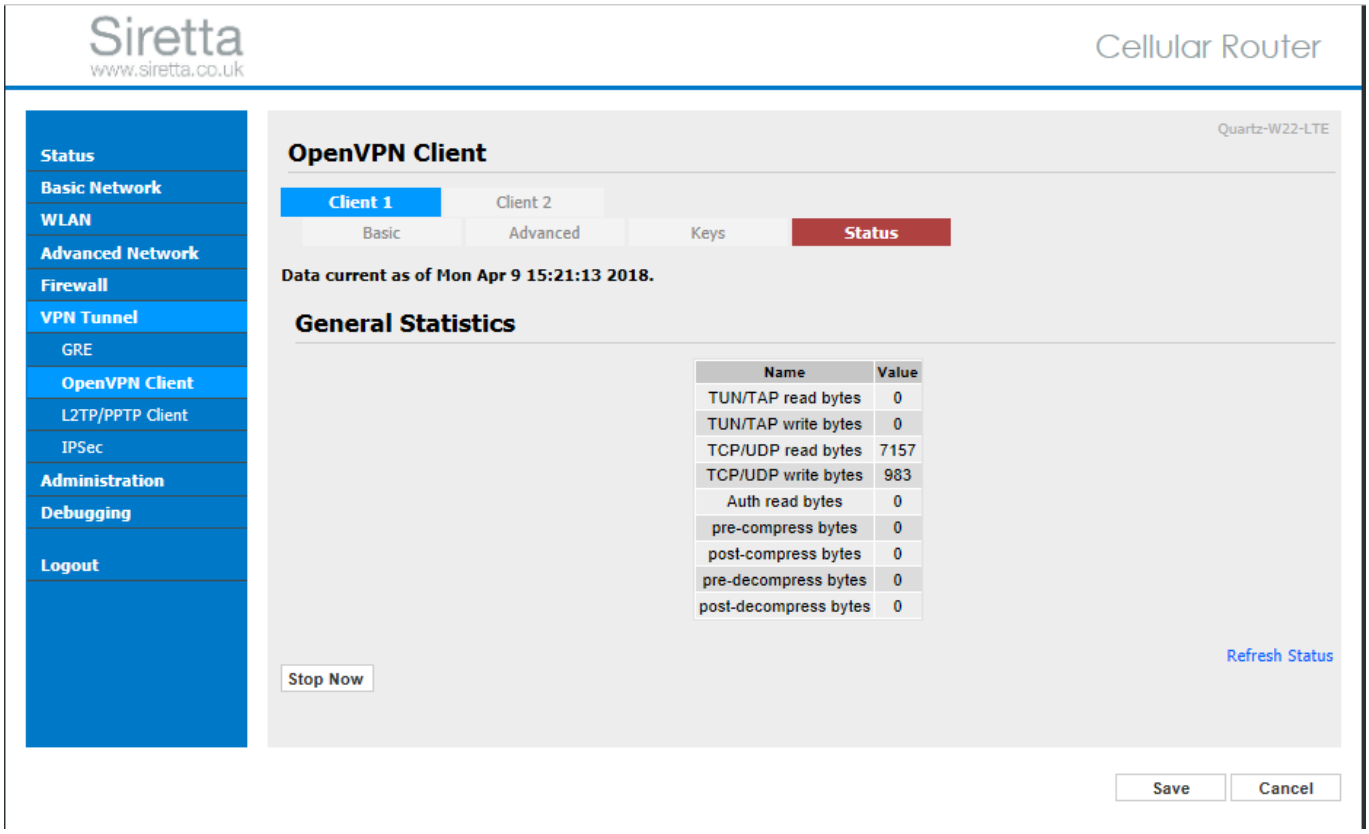


4) Select the keys tab below then enter the key details from your OpenVPN server configuration file as shown in the OpenVPN server details.

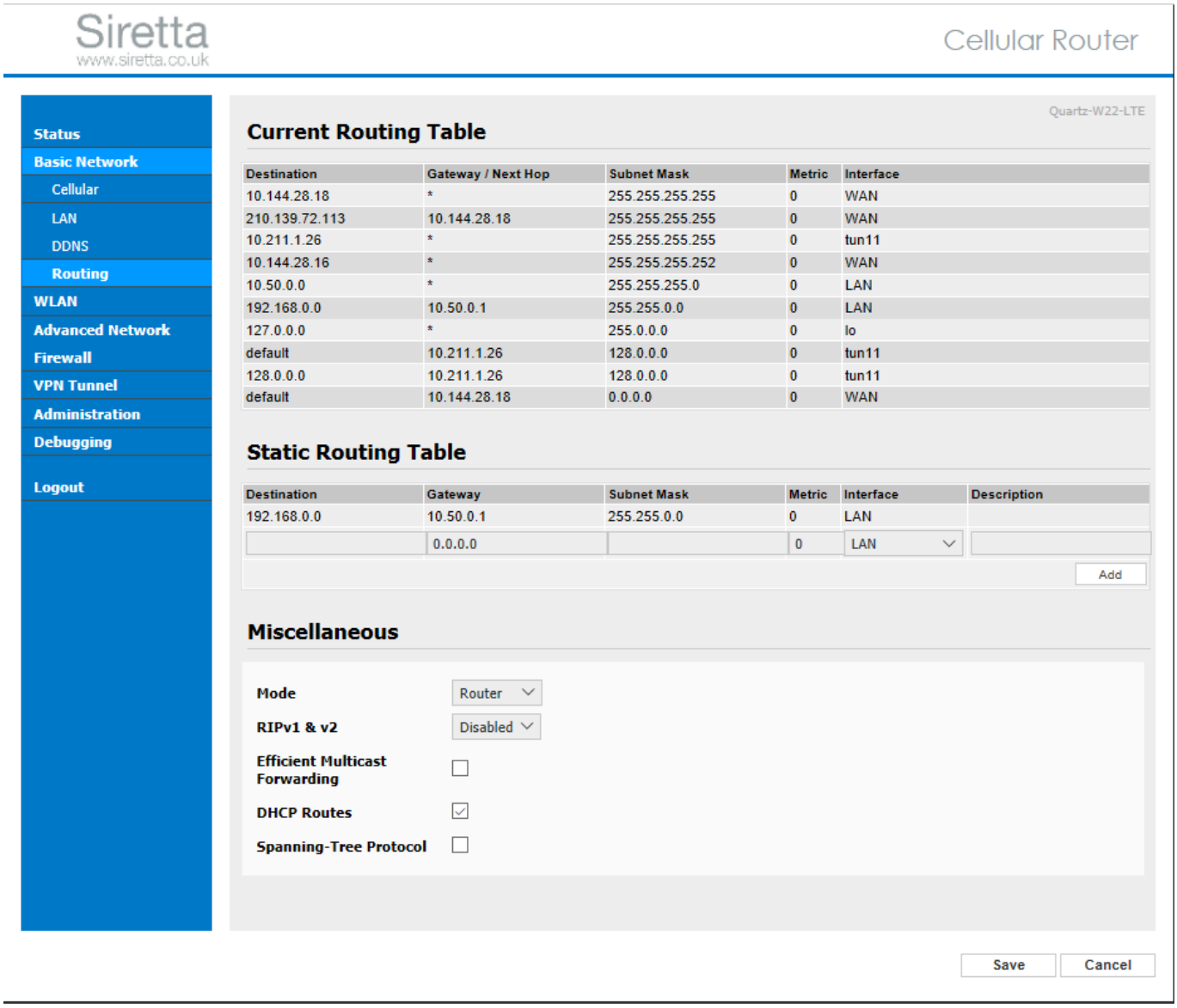


5) Once you have entered the keys, click save

6) Click start now to initiate the OpenVPN server. The client will start running and you will be connected to the OpenVPN server. You can check this by selecting the 'Status' tab:



7) You can check the router's current routing table by selecting 'Basic Network' -> 'Routing' to show the table below with tun11 indicating the connection through the VPN tunnel.



8) The two diagrams below show TCP packets on the client PC connected to the network. The first image (figure 1) shows the network connection without OpenVPN configured. The second image (figure 2) shows the network connection with OpenVPN configured.

Figure 1 - Shows more data information without the VPN

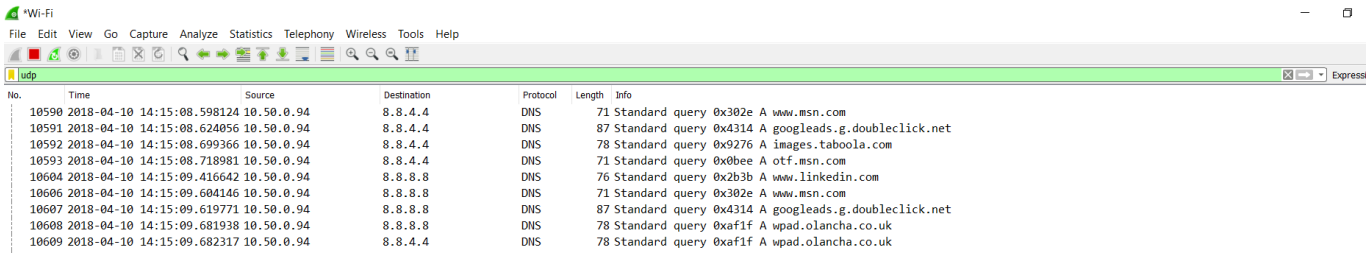
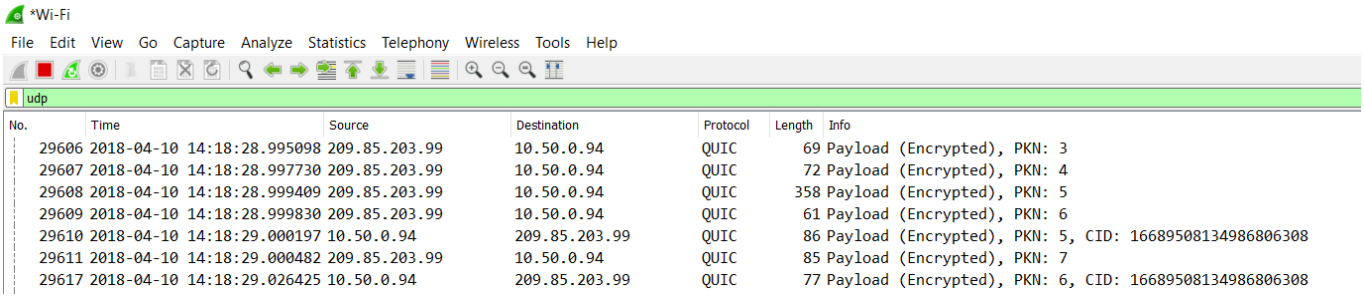


Figure 2 - Shows less data information (Encrypted) with the VPN



No.	Time	Source	Destination	Protocol	Length	Info
29606	2018-04-10 14:18:28.995098	209.85.203.99	10.50.0.94	QUIC	69	Payload (Encrypted), PKN: 3
29607	2018-04-10 14:18:28.997730	209.85.203.99	10.50.0.94	QUIC	72	Payload (Encrypted), PKN: 4
29608	2018-04-10 14:18:28.999409	209.85.203.99	10.50.0.94	QUIC	358	Payload (Encrypted), PKN: 5
29609	2018-04-10 14:18:28.999830	209.85.203.99	10.50.0.94	QUIC	61	Payload (Encrypted), PKN: 6
29610	2018-04-10 14:18:29.000197	10.50.0.94	209.85.203.99	QUIC	86	Payload (Encrypted), PKN: 5, CID: 16689508134986806308
29611	2018-04-10 14:18:29.000482	209.85.203.99	10.50.0.94	QUIC	85	Payload (Encrypted), PKN: 7
29617	2018-04-10 14:18:29.026425	10.50.0.94	209.85.203.99	QUIC	77	Payload (Encrypted), PKN: 6, CID: 16689508134986806308

NOTE: The capture was performed using Wireshark which can be downloaded from 'https://www.wireshark.org/download.html'