# Application Note 75

How to configure two Digi Transport WR Routers as OVPN Client and Server

**September 2020**

# Contents

# 1 INTRODUCTION

## 1.1 Outline

This document describes how to configure two TransPort routers as OVPN client and server.

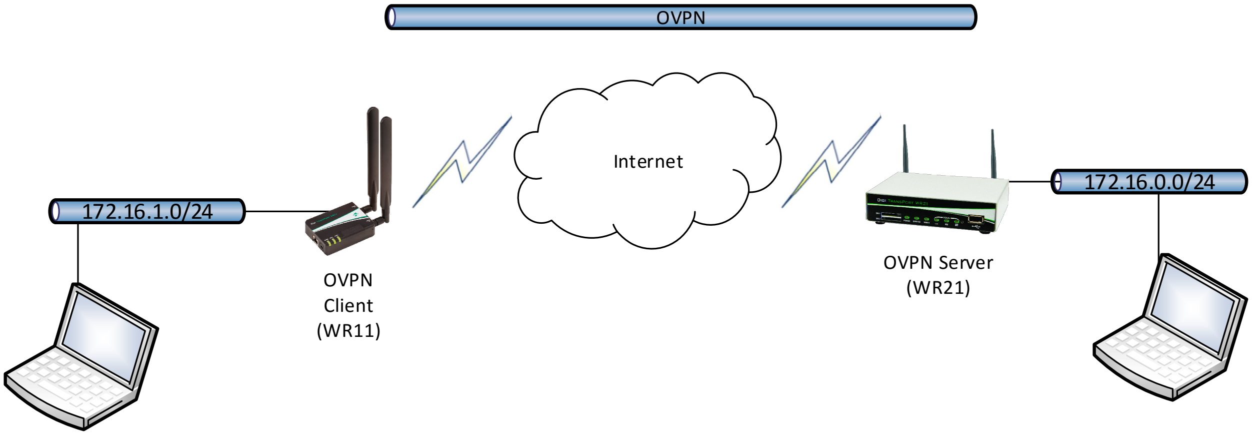
OpenVPN can be used for securely connecting a TransPort router to another one in a central office network for access to services on the LAN side of the OpenVPN server, such as corporate messaging services, file servers and print servers for example.

From the OpenVPN website:

OpenVPN is a full-featured SSL VPN which implements OSI layer 2 or 3 secure network extension using the industry standard SSL/TLS protocol, supports flexible client authentication methods based on certificates, smart cards, and/or username/password credentials, and allows user or group-specific access control policies using firewall rules applied to the VPN virtual interface. OpenVPN is not a web application proxy and does not operate through a web browser.

OpenVPN 2.0 expands on the capabilities of OpenVPN 1.x by offering a scalable client/server mode, allowing multiple clients to connect to a single OpenVPN server process over a single TCP or UDP port.

For the purposes of this application note, the following scenario will be used:



OpenVPN is certificate based, so there will be certificates on the two TransPort routers.

A PC will be needed that can be used to install the OpenVPN Easy-RSA certificate authority and create & sign the certificates.

## 1.2 Assumptions

This guide has been written for use by technically competent personnel with a good understanding of the communications technologies used in the product and of the requirements for their specific application. It also assumes a basic ability to access and navigate a Digi Transport router and configure it with basic routing functions.

This application note applies to:

**Model:** Digi Transport WR21 and WR11

**Other Compatible Models:** All Digi WR Transpost models

**Firmware versions:** 5.077 and later

**Configuration:** This Application Note assumes the devices are set to their factory default configurations. Most configuration commands are only shown if they differ from the factory default.

## 1.3 Corrections

Requests for corrections or amendments to this application note are welcome and should be addressed to: tech.support@digi.com.

Requests for new application notes can be sent to the same address.

## 1.4 Version

| Version Number | Status |
|---|---|
| 1.0 | Published (Oct 2017) |
| 1.1 | Added Publish Date, corrected links and other minor fix (Sep 2020) |

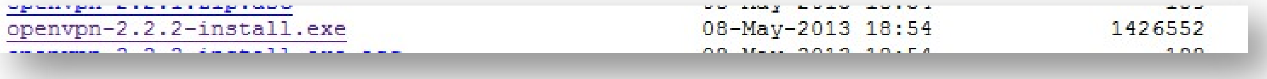
# 2 OPENVPN & EASY RSA SETUP

## 2.1 Download the OpenVPN installation package and install the software

This step should be done on a PC that will be used to create the certificates.

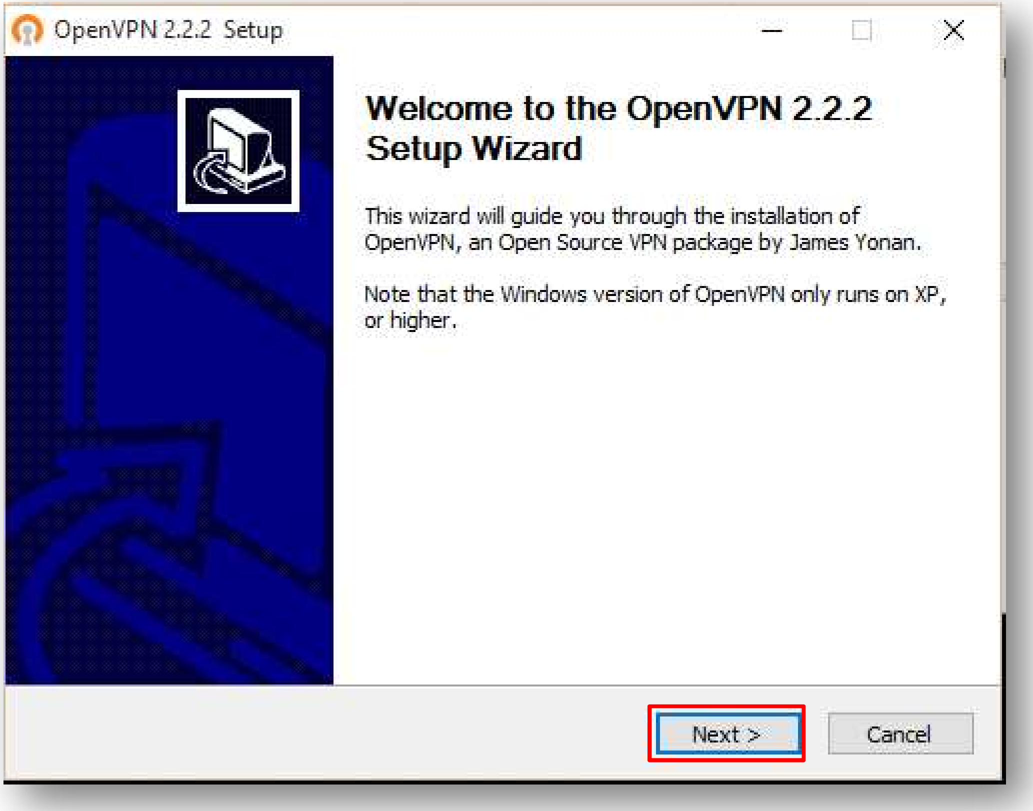
In order to download the installer, go to https://build.openvpn.net/downloads/releases/.

For this example, OpenVPN 2.2.2 version has been used:



```
openvpn-2.2.2-install.exe                          08-May-2013 18:54              1426552
```

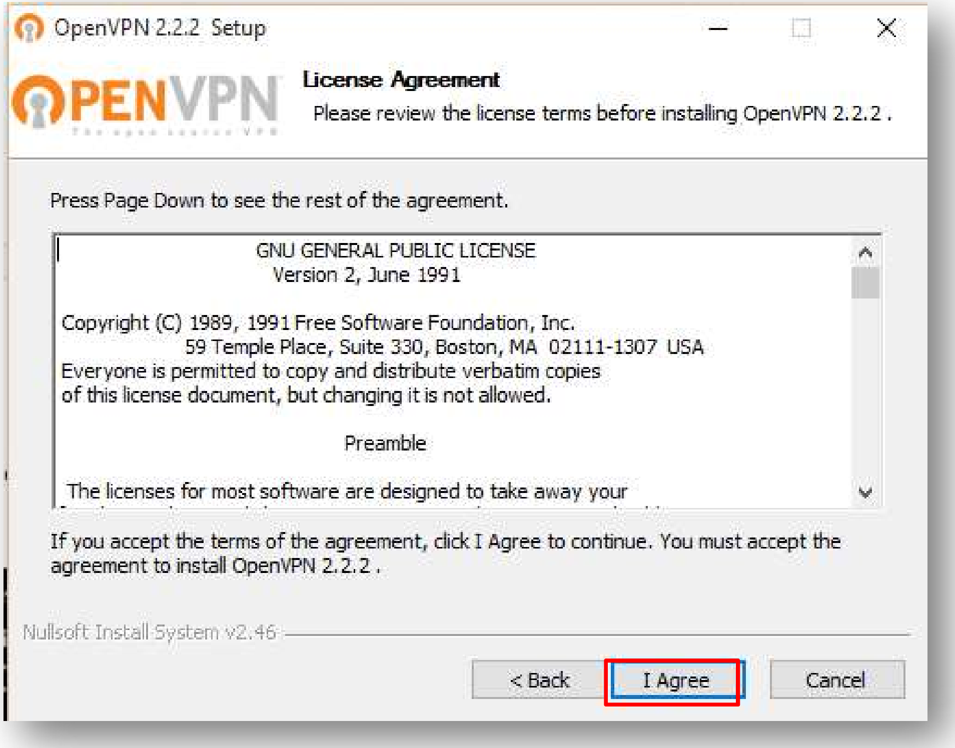
Run the installer and follow the instructions:



**Welcome to the OpenVPN 2.2.2 Setup Wizard**

This wizard will guide you through the installation of OpenVPN, an Open Source VPN package by James Yonan.

Note that the Windows version of OpenVPN only runs on XP, or higher.



OpenVPN 2.2.2 Setup

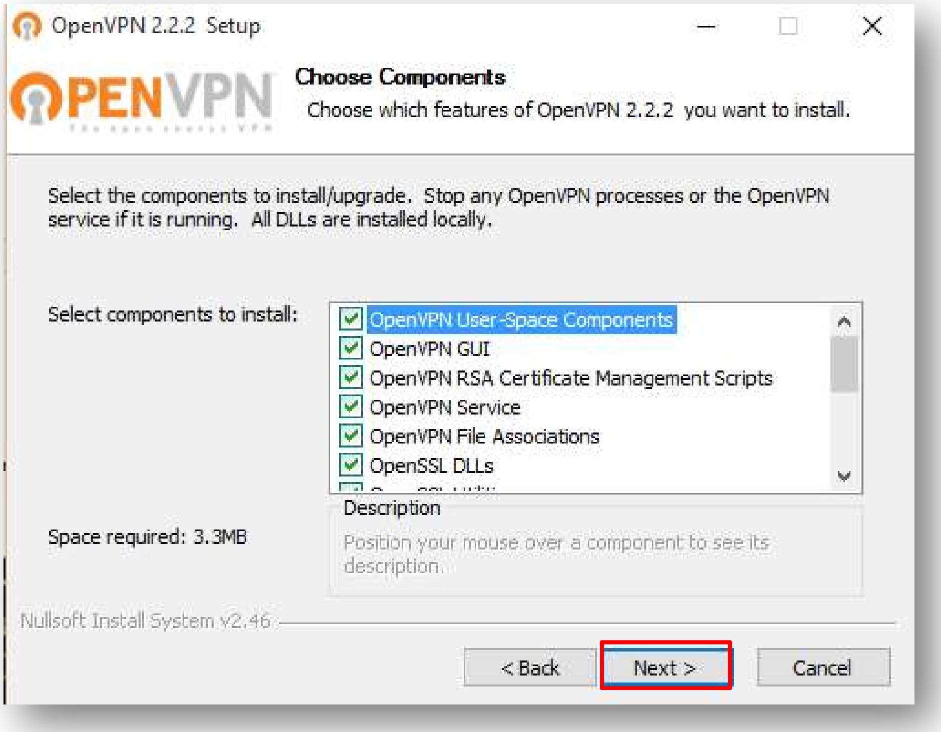
**License Agreement**

Please review the license terms before installing OpenVPN 2.2.2 .

Press Page Down to see the rest of the agreement.

```
                    GNU GENERAL PUBLIC LICENSE
                       Version 2, June 1991

 Copyright (C) 1989, 1991 Free Software Foundation, Inc.
          59 Temple Place, Suite 330, Boston, MA  02111-1307  USA
 Everyone is permitted to copy and distribute verbatim copies
 of this license document, but changing it is not allowed.

                            Preamble

  The licenses for most software are designed to take away your
```

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install OpenVPN 2.2.2 .



OpenVPN 2.2.2 Setup

**Choose Components**

Choose which features of OpenVPN 2.2.2 you want to install.

Select the components to install/upgrade. Stop any OpenVPN processes or the OpenVPN service if it is running. All DLLs are installed locally.

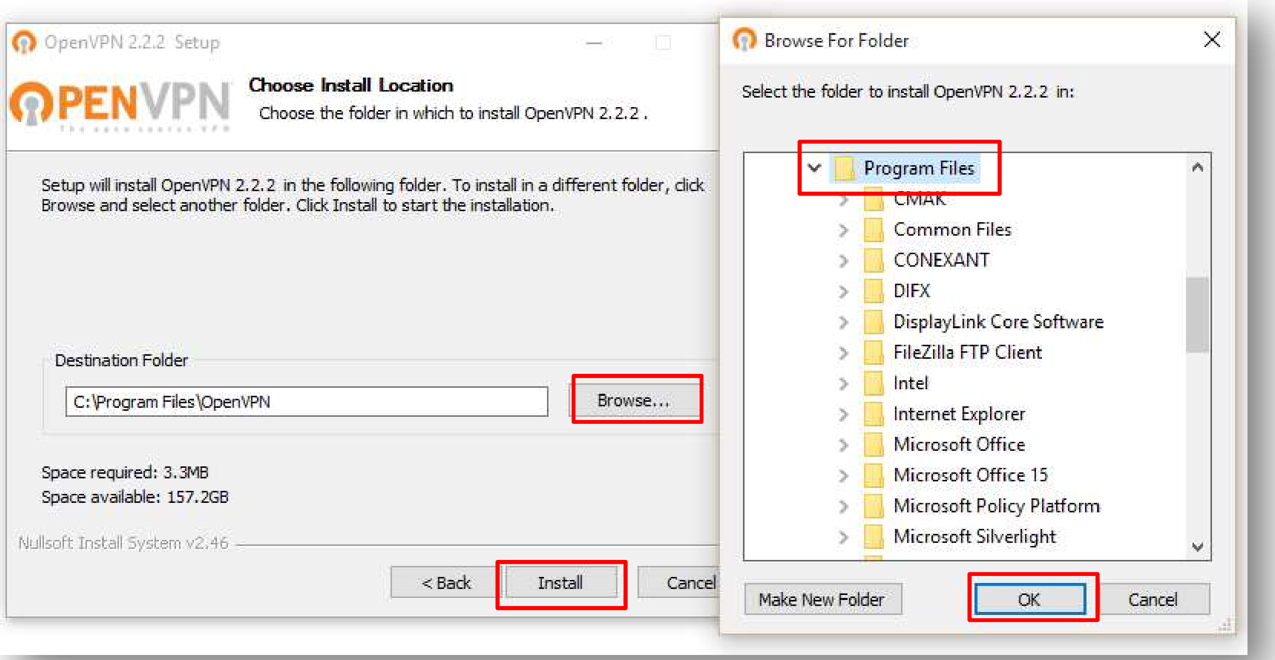
Select components to install:

- ☑ OpenVPN User-Space Components
- ☑ OpenVPN GUI
- ☑ OpenVPN RSA Certificate Management Scripts
- ☑ OpenVPN Service
- ☑ OpenVPN File Associations
- ☑ OpenSSL DLLs

Space required: 3.3MB

Description

Position your mouse over a component to see its description.



**Choose Install Location**

Choose the folder in which to install OpenVPN 2.2.2 .

Setup will install OpenVPN 2.2.2 in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.

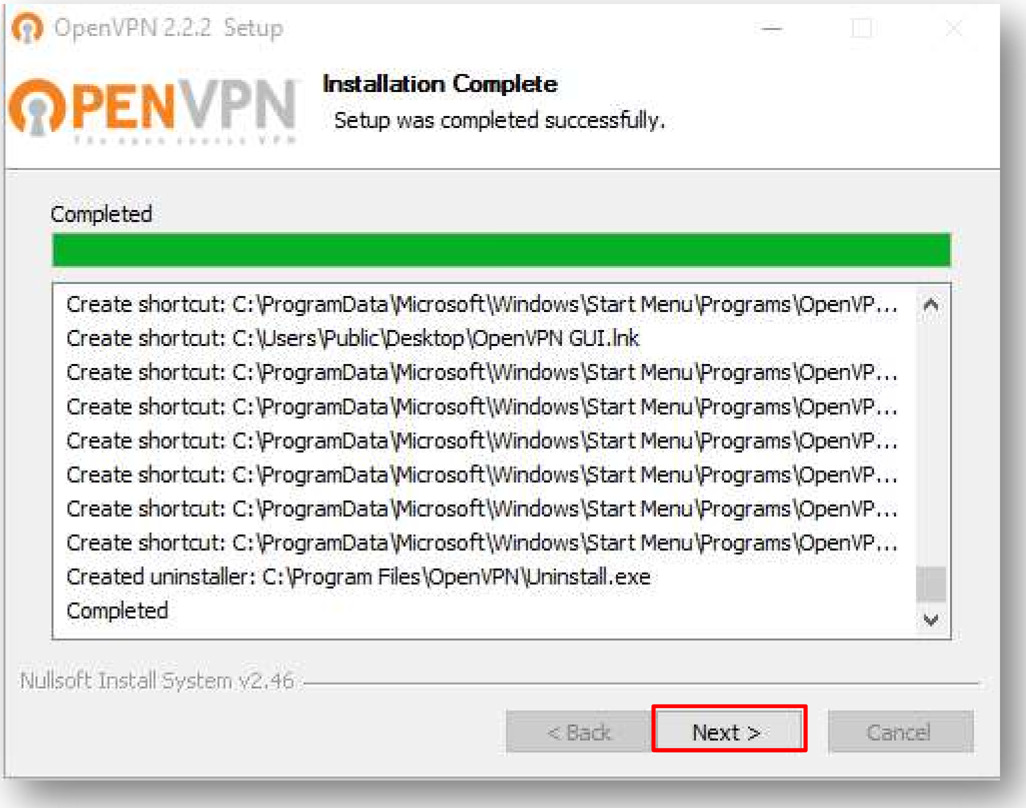
Destination Folder: C:\Program Files\OpenVPN

Space required: 3.3MB
Space available: 157.2GB

Nullsoft Install System v2.46

Select the folder to install OpenVPN 2.2.2 in:

- Program Files
  - CMAK
  - Common Files
  - CONEXANT
  - DIFX
  - DisplayLink Core Software
  - FileZilla FTP Client
  - Intel
  - Internet Explorer
  - Microsoft Office
  - Microsoft Office 15
  - Microsoft Policy Platform
  - Microsoft Silverlight



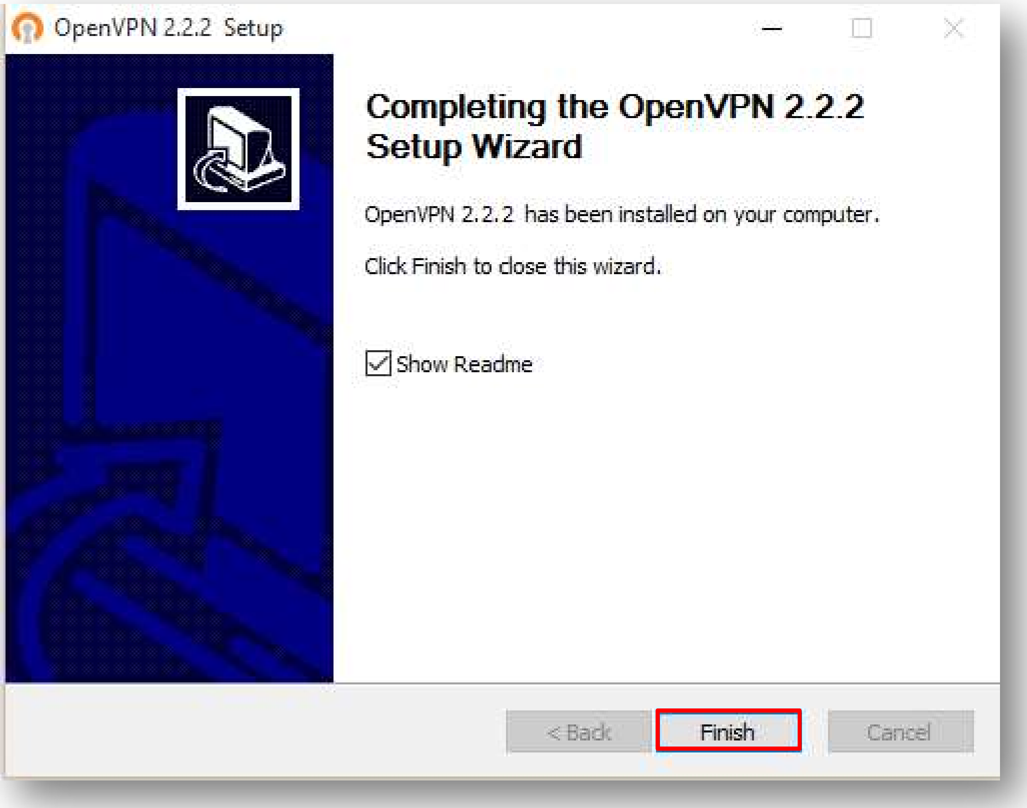
**Installation Complete**

Setup was completed successfully.

Completed

```
Create shortcut: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\OpenVP...
Create shortcut: C:\Users\Public\Desktop\OpenVPN GUI.lnk
Create shortcut: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\OpenVP...
Create shortcut: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\OpenVP...
Create shortcut: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\OpenVP...
Create shortcut: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\OpenVP...
Create shortcut: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\OpenVP...
Create shortcut: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\OpenVP...
Created uninstaller: C:\Program Files\OpenVPN\Uninstall.exe
Completed
```

Nullsoft Install System v2.46



OpenVPN 2.2.2 Setup

Completing the OpenVPN 2.2.2 Setup Wizard

OpenVPN 2.2.2 has been installed on your computer.

Click Finish to close this wizard.

☑ Show Readme

## 2.2 Setting up Certificate Authority (CA) and generating certificates and keys

The first step in building an OpenVPN 2.x configuration is to establish a PKI (public key infrastructure). The PKI consists of:

- a separate certificate (also known as a public key) and private key for the server and each client
- a master Certificate Authority (CA) certificate and key which is used to sign each of the server and client certificates.

OpenVPN supports bidirectional authentication based on certificates, meaning that the client must authenticate the server certificate and the server must authenticate the client certificate before mutual trust is established.

Both server and client will authenticate the other by first verifying that the presented certificate was signed by the master certificate authority (CA), and then by testing information in the now-authenticated certificate header, such as the certificate common name or certificate type (client or server).

This security model has a number of desirable features from the VPN perspective:

- - The server only needs its own certificate/key -- it doesn't need to know the individual certificates of every client which might possibly connect to it.
- - The server will only accept clients whose certificates were signed by the master CA certificate (which we will generate below). And because the server can perform this signature verification without needing access to the CA private key itself, it is possible for the CA key (the most sensitive key in the entire PKI) to reside on a completely different machine, even one without a network connection.
- - If a private key is compromised, it can be disabled by adding its certificate to a CRL (certificate revocation list). The CRL allows compromised certificates to be selectively rejected without requiring that the entire PKI be rebuilt.
- - The server can enforce client-specific access rights based on embedded certificate fields, such as the Common Name.

Note that the server and client clocks need to be roughly in sync or certificates might not work properly.

## 2.3 Generate the master Certificate Authority (CA) certificate & key

In this section we will generate a master CA certificate/key, a server certificate/key, and certificates/keys for the client.

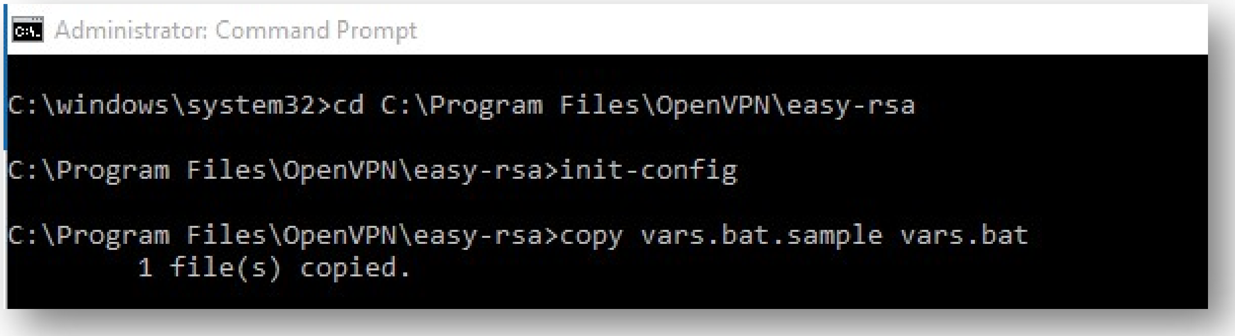
For PKI management, we will use easy-rsa 2, a set of scripts which is bundled with OpenVPN 2.2.x and earlier.

On Windows, open up a Command Prompt window and cd to **C:\Program Files\OpenVPN\easy-rsa**

Run the following batch file to copy configuration files into place (this will overwrite any preexisting vars.bat and openssl.cnf files):

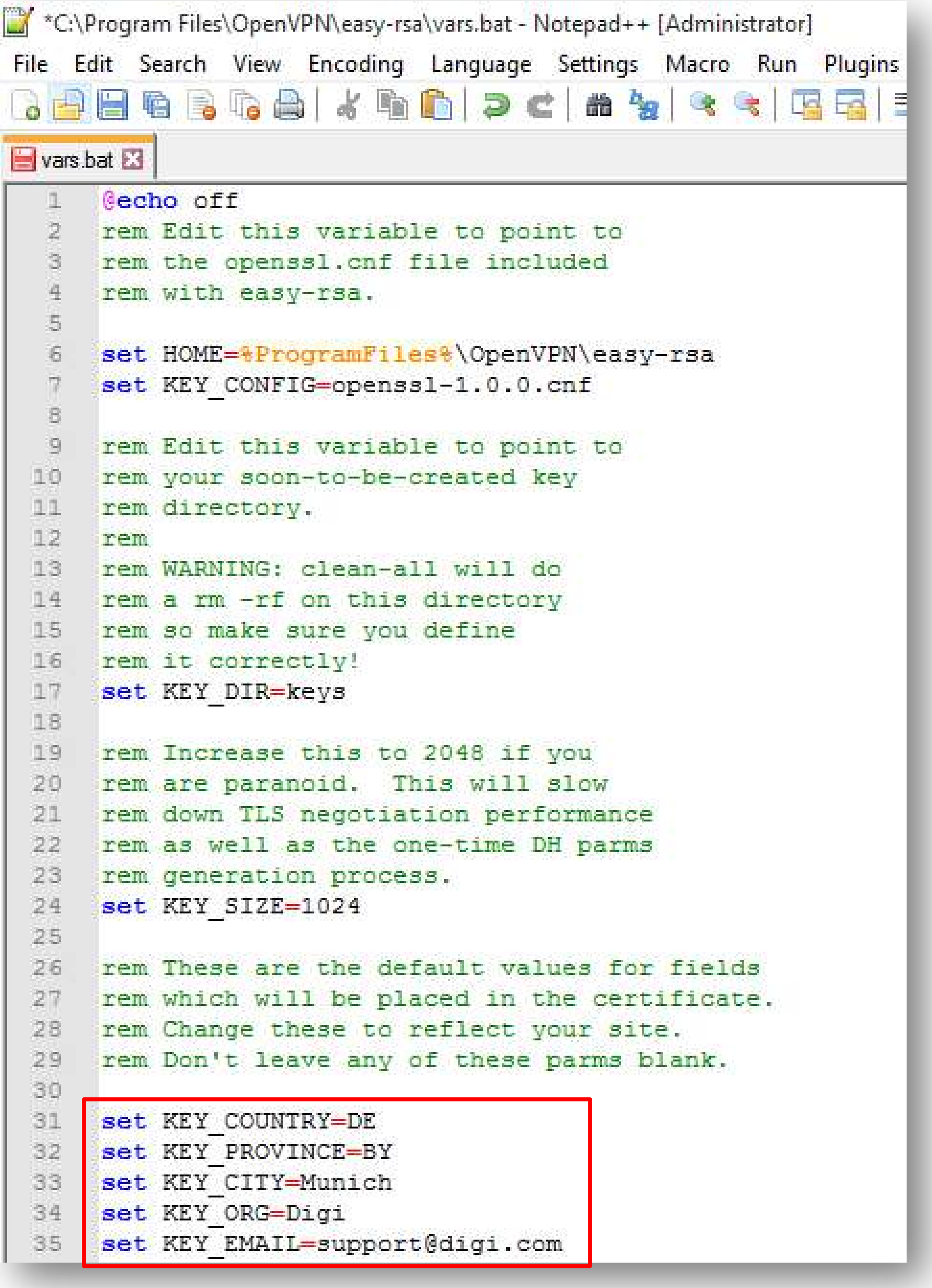
*init-config*

The output will be like the following:



```
C:\windows\system32>cd C:\Program Files\OpenVPN\easy-rsa

C:\Program Files\OpenVPN\easy-rsa>init-config

C:\Program Files\OpenVPN\easy-rsa>copy vars.bat.sample vars.bat
        1 file(s) copied.
```

Now edit the vars file (called vars.bat on Windows) and set the KEY_COUNTRY, KEY_PROVINCE, KEY_CITY, KEY_ORG, and KEY_EMAIL parameters. Don't leave any of these para meters blank:


*C:\Program Files\OpenVPN\easy-rsa\vars.bat - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins
vars.bat

```
@echo off
rem Edit this variable to point to
rem the openssl.cnf file included
rem with easy-rsa.

set HOME=%ProgramFiles%\OpenVPN\easy-rsa
set KEY_CONFIG=openssl-1.0.0.cnf

rem Edit this variable to point to
rem your soon-to-be-created key
rem directory.
rem
rem WARNING: clean-all will do
rem a rm -rf on this directory
rem so make sure you define
rem it correctly!
set KEY_DIR=keys

rem Increase this to 2048 if you
rem are paranoid.  This will slow
rem down TLS negotiation performance
rem as well as the one-time DH parms
rem generation process.
set KEY_SIZE=1024

rem These are the default values for fields
rem which will be placed in the certificate.
rem Change these to reflect your site.
rem Don't leave any of these parms blank.

set KEY_COUNTRY=DE
set KEY_PROVINCE=BY
set KEY_CITY=Munich
set KEY_ORG=Digi
set KEY_EMAIL=support@digi.com
```

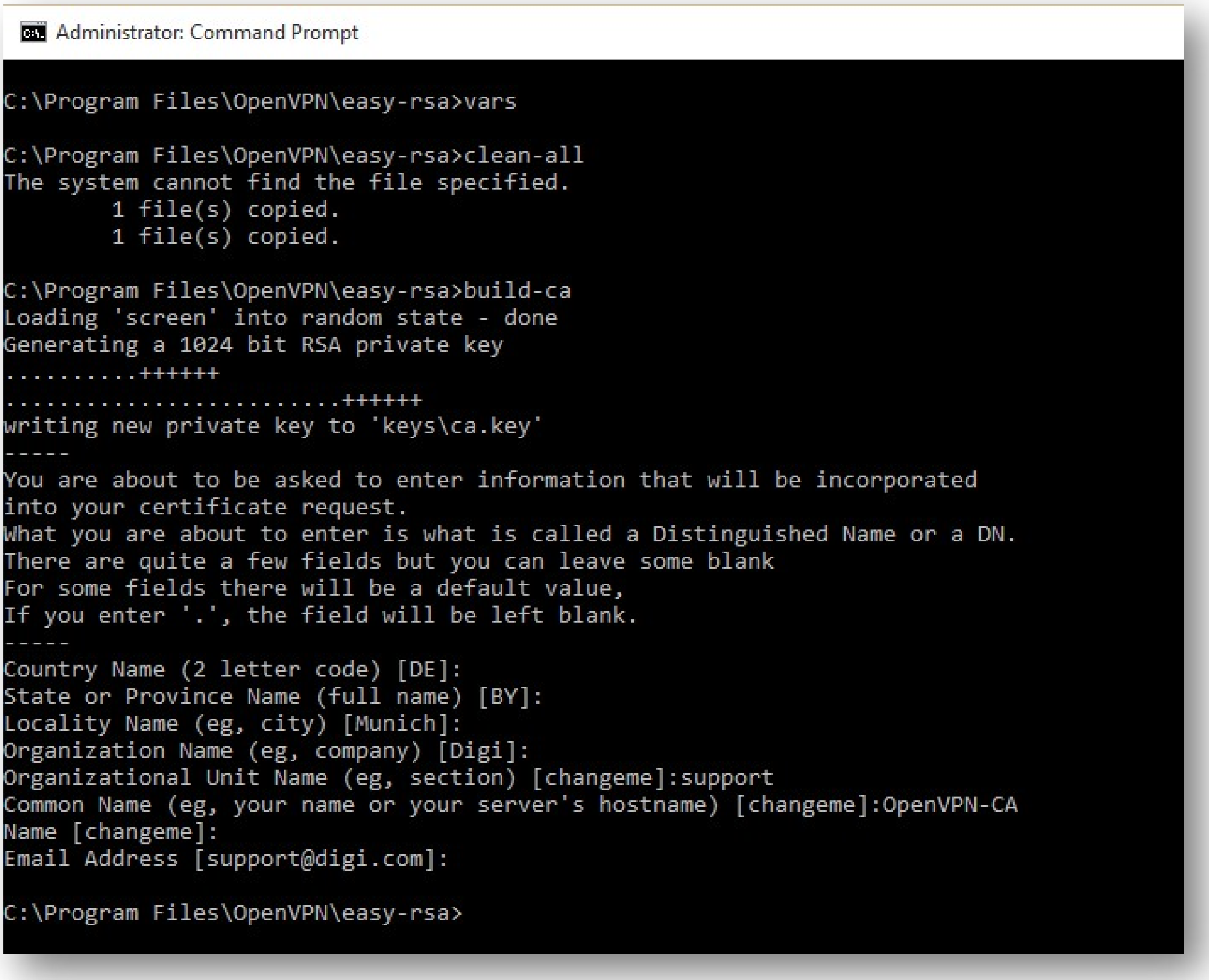
Save and close it.

Then,  in command prompt run the following to initialize the PKI:

*vars*
*clean-all*
*build-ca*

The final command (build-ca) will build the certificate authority (CA) certificate and key by invoking the interactive openssl command.

The output will be like the following:



```
C:\Program Files\OpenVPN\easy-rsa>vars

C:\Program Files\OpenVPN\easy-rsa>clean-all
The system cannot find the file specified.
        1 file(s) copied.
        1 file(s) copied.

C:\Program Files\OpenVPN\easy-rsa>build-ca
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
..........++++++
.........................++++++
writing new private key to 'keys\ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [DE]:
State or Province Name (full name) [BY]:
Locality Name (eg, city) [Munich]:
Organization Name (eg, company) [Digi]:
Organizational Unit Name (eg, section) [changeme]:support
Common Name (eg, your name or your server's hostname) [changeme]:OpenVPN-CA
Name [changeme]:
Email Address [support@digi.com]:

C:\Program Files\OpenVPN\easy-rsa>
```

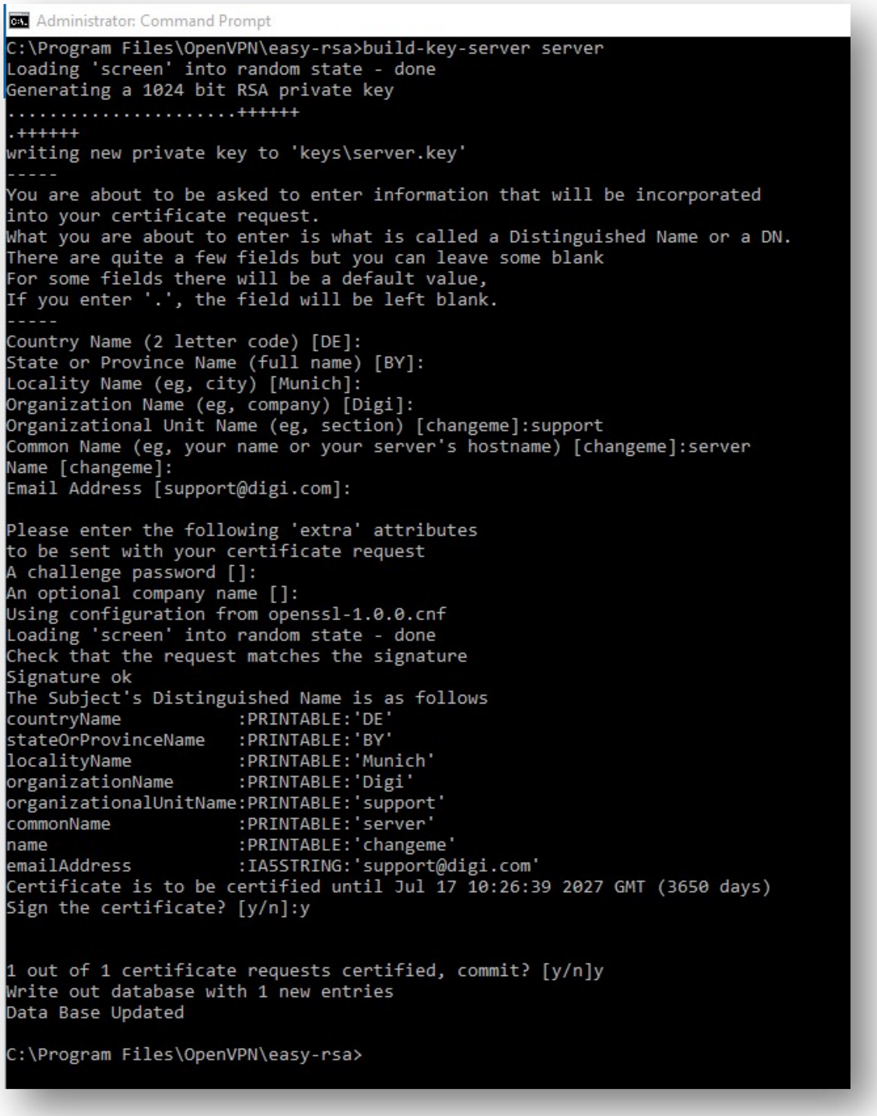
Note that in the above sequence, most queried parameters were defaulted to the values set in the vars or vars.bat files. The only parameter which must be explicitly entered is the Common Name. In the example above, OpenVPN-CA is used

### 2.3.1 Generate certificate & key for server

Next, we will generate a certificate and private key for the server

```
build-key-server server
```

As in the previous step, most parameters can be defaulted. When the Common Name is queried, enter "server". Two other queries require positive responses, "Sign the certificate? [y/n]" and "1 out of 1 certificate requests certified, commit? [y/n]".

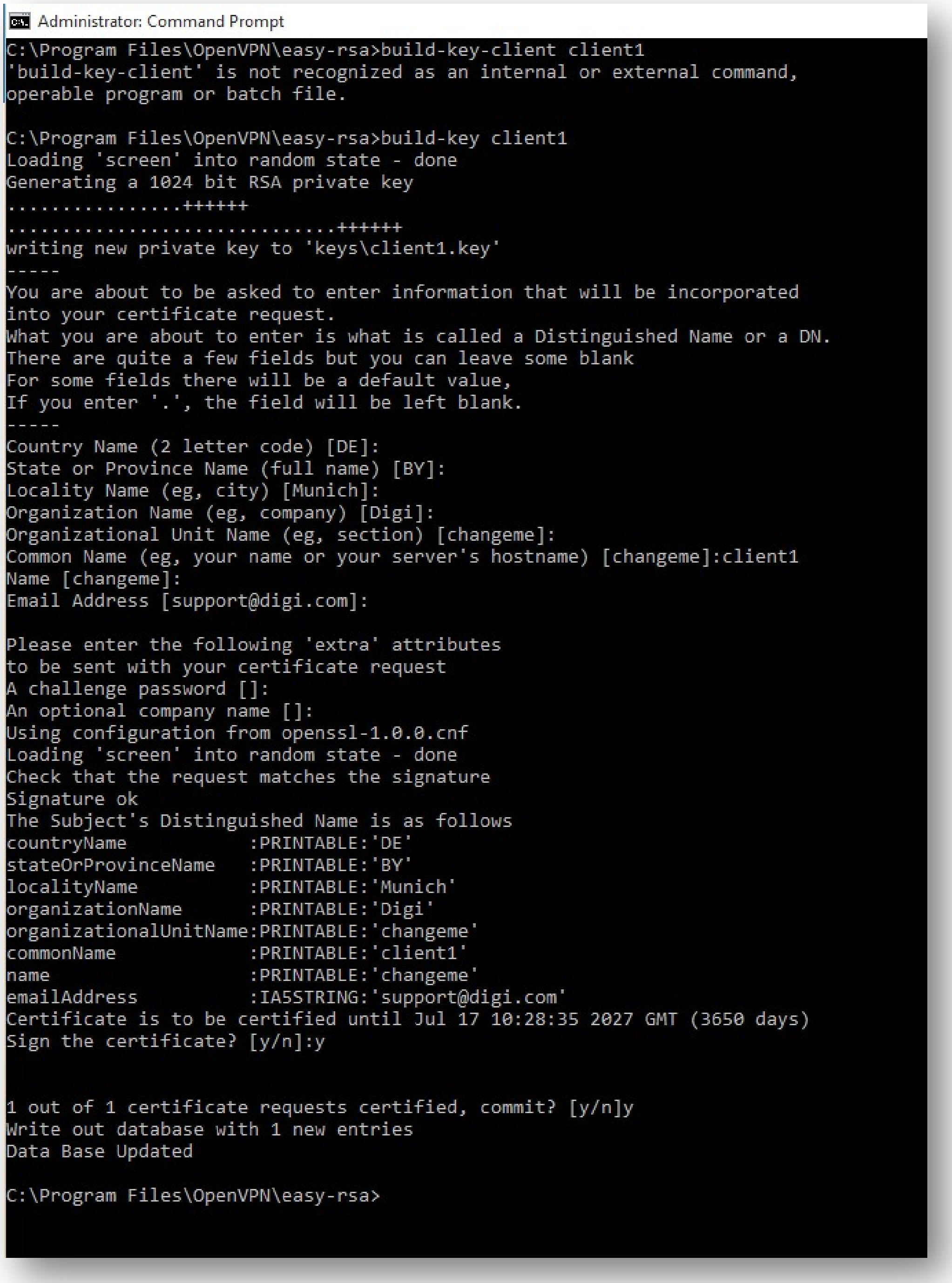


```
C:\Program Files\OpenVPN\easy-rsa>build-key-server server
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
......................++++++
.++++++
writing new private key to 'keys\server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [DE]:
State or Province Name (full name) [BY]:
Locality Name (eg, city) [Munich]:
Organization Name (eg, company) [Digi]:
Organizational Unit Name (eg, section) [changeme]:support
Common Name (eg, your name or your server's hostname) [changeme]:server
Name [changeme]:
Email Address [support@digi.com]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from openssl-1.0.0.cnf
Loading 'screen' into random state - done
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'DE'
stateOrProvinceName   :PRINTABLE:'BY'
localityName          :PRINTABLE:'Munich'
organizationName      :PRINTABLE:'Digi'
organizationalUnitName:PRINTABLE:'support'
commonName            :PRINTABLE:'server'
name                  :PRINTABLE:'changeme'
emailAddress          :IA5STRING:'support@digi.com'
Certificate is to be certified until Jul 17 10:26:39 2027 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated

C:\Program Files\OpenVPN\easy-rsa>
```

## 2.3.2 Generate certificates & keys for the client

Generating client certificates is very similar to the previous step.

**`build-key client1`**



Administrator: Command Prompt

```
C:\Program Files\OpenVPN\easy-rsa>build-key-client client1
'build-key-client' is not recognized as an internal or external command,
operable program or batch file.

C:\Program Files\OpenVPN\easy-rsa>build-key client1
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
................++++++
.............................++++++
writing new private key to 'keys\client1.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [DE]:
State or Province Name (full name) [BY]:
Locality Name (eg, city) [Munich]:
Organization Name (eg, company) [Digi]:
Organizational Unit Name (eg, section) [changeme]:
Common Name (eg, your name or your server's hostname) [changeme]:client1
Name [changeme]:
Email Address [support@digi.com]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from openssl-1.0.0.cnf
Loading 'screen' into random state - done
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'DE'
stateOrProvinceName   :PRINTABLE:'BY'
localityName          :PRINTABLE:'Munich'
organizationName      :PRINTABLE:'Digi'
organizationalUnitName:PRINTABLE:'changeme'
commonName            :PRINTABLE:'client1'
name                  :PRINTABLE:'changeme'
emailAddress          :IA5STRING:'support@digi.com'
Certificate is to be certified until Jul 17 10:28:35 2027 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated

C:\Program Files\OpenVPN\easy-rsa>
```

If you would like to password-protect your client keys, substitute the build-key-pass script.

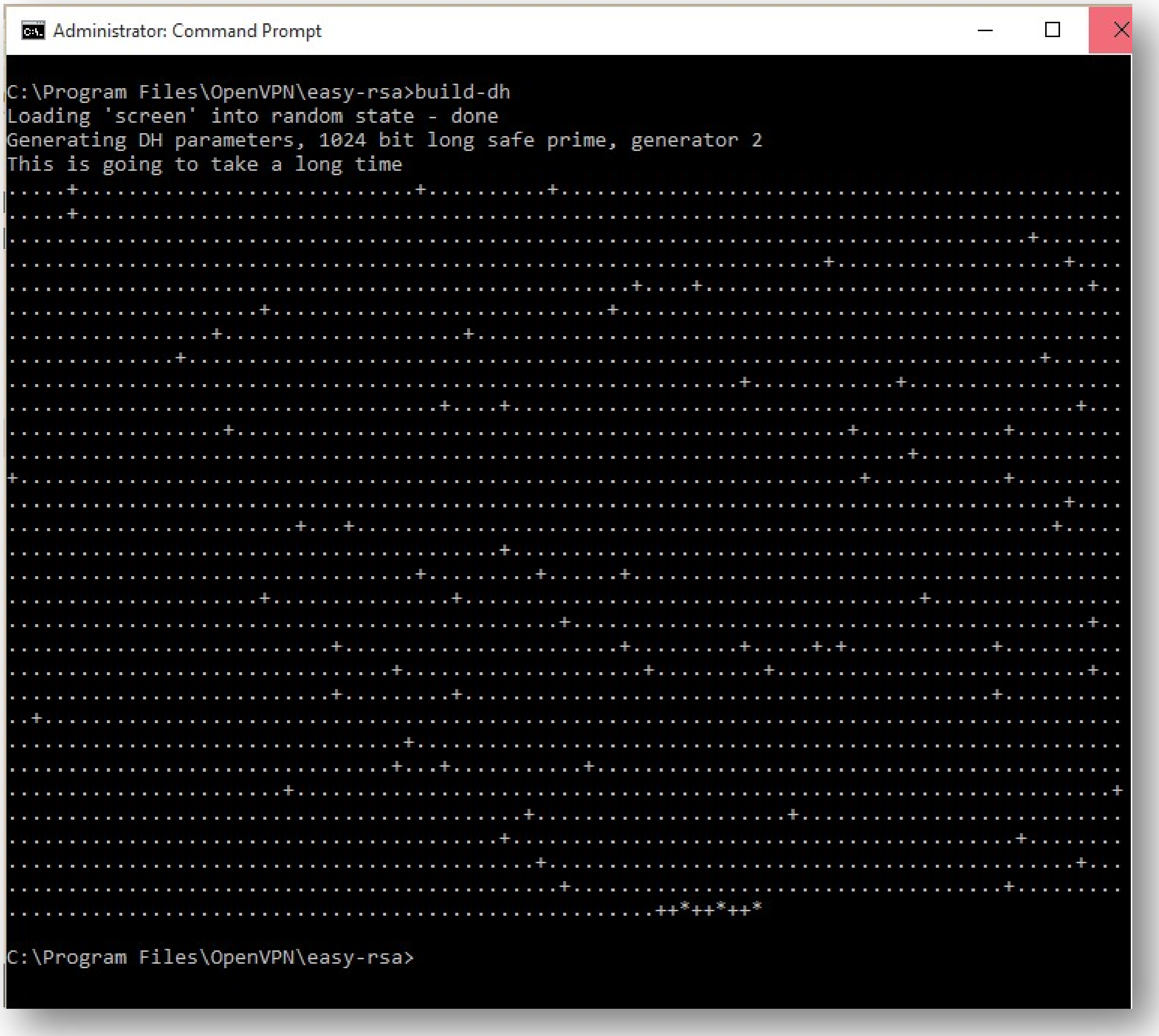
Remember that if you create Certificates and Keys for more than one client,for each client, make sure to type the appropriate Common Name when prompted, i.e. "client1", "client2", or "client3". Always use a unique common name for each client.

### 2.3.3 Generate Diffie Hellman parameters

Diffie Hellman parameters must be generated for the OpenVPN server with the following command:

```
build-dh
```

Output:



```
C:\Program Files\OpenVPN\easy-rsa>build-dh
Loading 'screen' into random state - done
Generating DH parameters, 1024 bit long safe prime, generator 2
This is going to take a long time
.....+............................+..........+...............................................
.....+.......................................................................................
.....................................................................................+.......
....................................................................+...................+....
....................................................+....+................................+..
.....................+............................+..........................................
.................+....................+......................................................
..............+.......................................................................+......
.............................................................+............+..................
....................................+....+...............................................+...
..................+...................................................+............+.........
...........................................................................+.................
+......................................................................+...........+.........
........................................................................................+....
........................+...+..........................................................+.....
.........................................+...................................................
..................................+.........+......+.........................................
.....................+...............+......................................+................
..............................................+...........................................+..
...........................+.......................+.........+.....+.+............+..........
................................+....................+.........+..........................+..
...........................+.........+............................................+..........
..+..........................................................................................
.................................+...........................................................
................................+...+...........+............................................
.......................+....................................................................+
...........................................+.....................+...........................
.........................................+..........................................+........
............................................+............................................+...
..............................................+....................................+.........
......................................................++*++*++*

C:\Program Files\OpenVPN\easy-rsa>
```

### 2.3.4 Key Files

Now we will find our newly-generated keys and certificates in the keys subdirectory. Here is an explanation of the relevant files:

| Filename | Needed By | Purpose | Secret |
|---|---|---|---|
| ca.crt | server + all clients | Root CA certificate | NO |
| ca.key | key signing machine only | Root CA key | YES |
| dh{n}.pem | server only | Diffie Hellman parameters | NO |
| server.crt | server only | Server Certificate | NO |
| server.key | server only | Server Key | YES |
| client1.crt | client1 only | Client1 Certificate | NO |
| client1.key | client1 only | Client1 Key | YES |

The final step in the key generation process is to copy all files to the machines which need them, taking care to copy secret files over a secure channel.

In this example, two TransPort routers will be considered as Client and Server.

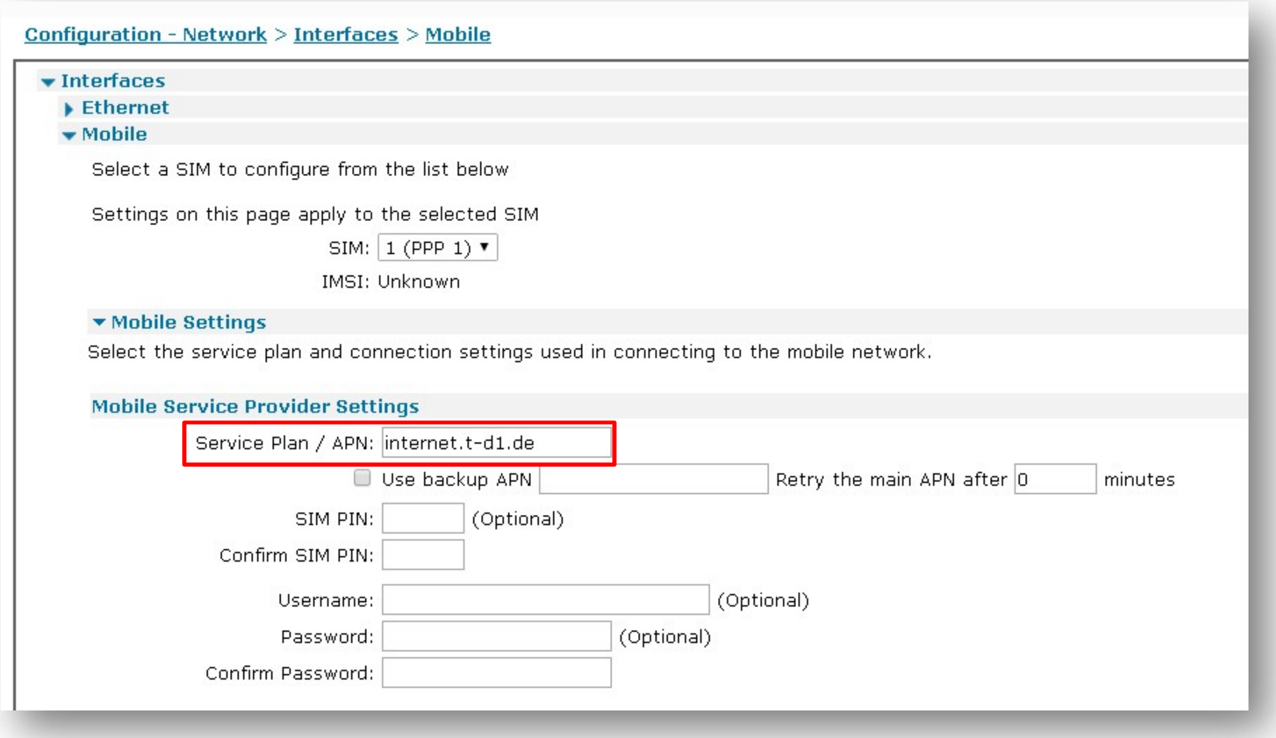
Examples on how to configure OpenVPN between a TransPort router and a different type of OpenVPN Server/Client (Windows, Ubuntu, etc) can be found at our documentation WebPage: https://www.digi.com/support/supporttype?type=documentation.

# 3 SERVER CONFIGURATION

## 3.1 WAN Interface configuration

In this example the Server has the Mobile interface as the WAN interface and it is configured as follows:

**CONFIGURATION - NETWORK > INTERFACES > MOBILE**


Configuration - Network > Interfaces > Mobile
Interfaces
Ethernet
Mobile

Select a SIM to configure from the list below

Settings on this page apply to the selected SIM

SIM: 1 (PPP 1)

IMSI: Unknown

Select the service plan and connection settings used in connecting to the mobile network.

Mobile Service Provider Settings

Service Plan / APN: internet.t-d1.de

□ Use backup APN Retry the main APN after 0 minutes

SIM PIN: (Optional)

Confirm SIM PIN:

Username: (Optional)

Password: (Optional)

Confirm Password:

Where:

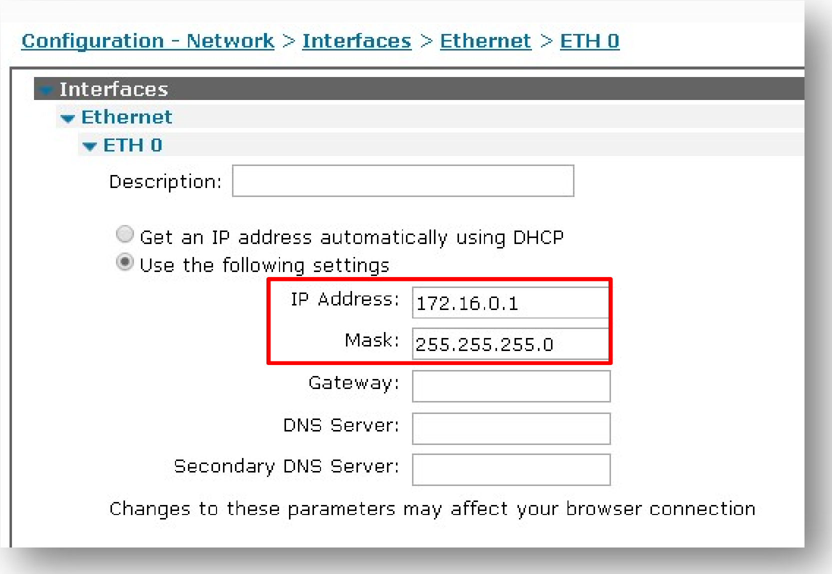
| Parameter | Setting | Description |
|---|---|---|
| Service Plan/APN | internet | Enter the APN of your mobile provider |

**Please note:** Depending on provider, a SIM PIN or Username/Password may be required. If needed, enter them in the appropriate fields.

## 3.2 LAN Interface configuration

In this example, the LAN interface is configured with a static address as follows:

**CONFIGURATION - NETWORK > INTERFACES > ETHERNET > ETH 0**



Description:

○ Get an IP address automatically using DHCP
● Use the following settings

IP Address: 172.16.0.1
Mask: 255.255.255.0
Gateway:
DNS Server:
Secondary DNS Server:

Changes to these parameters may affect your browser connection

Where:

| Parameter | Setting | Description |
|---|---|---|
| IP Address | 172.16.0.1 | Enter the IP address of the LAN interface for the router |
| Mask | 255.255.255.0 | Enter the subnet mask |

## 3.3 Transfer Certificates and Key files

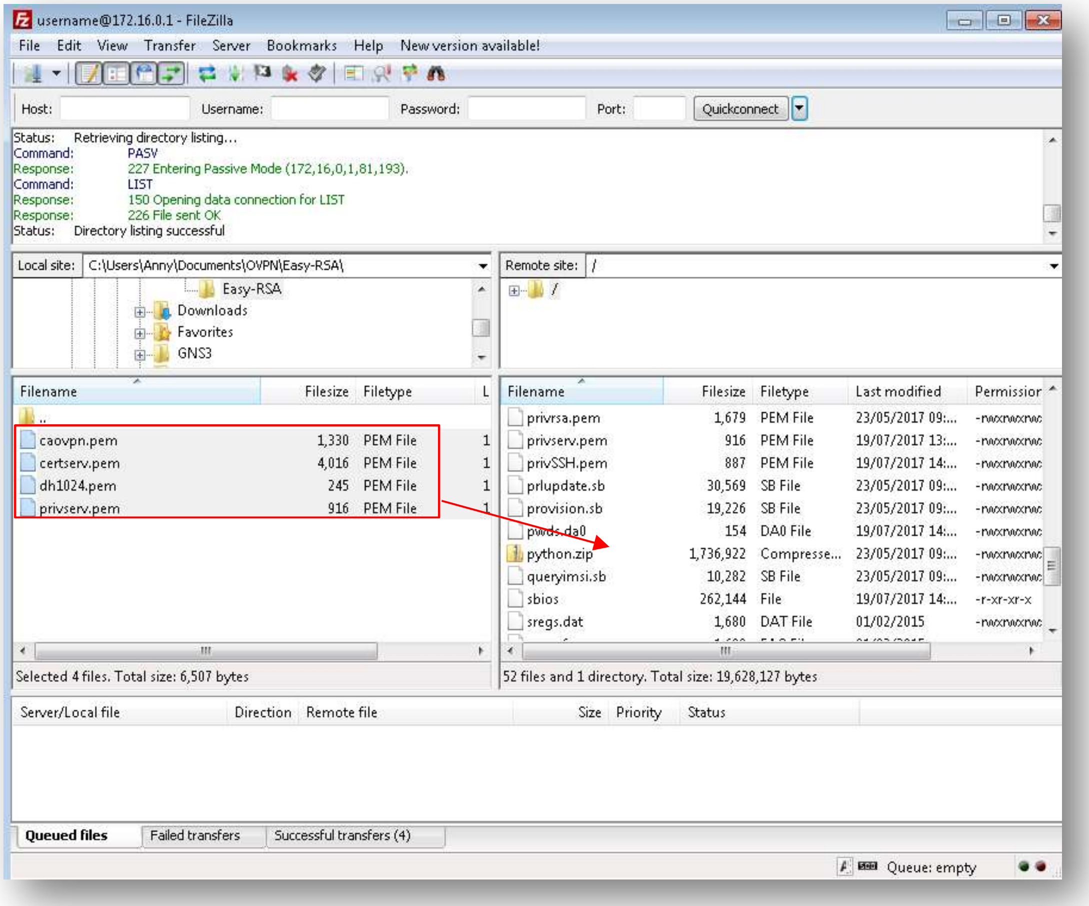
Before to transfer the Certficates and Key files on the server, they must be renamed as follows:

| Filename | Purpose | New FileName |
|---|---|---|
| ca.crt | Root CA certificate | **ca**ovpn.pem |
| server.crt | Server Certificate | **cert**serv.pem |
| server.key | Server Key | **priv**serv.pem |

The Diffie Hellman parameters file should remain unchanged.

Once done that, the files can be transferred into the Server using for example an FTP client, connected with the TransPort router with usual username and password.

Please note that you may need to change your IP on the laptop accordingly with the new IP address configured on the ETH0 of the router.



```
Status:     Retrieving directory listing...
Command:         PASV
Response:        227 Entering Passive Mode (172,16,0,1,81,193).
Command:         LIST
Response:        150 Opening data connection for LIST
Response:        226 File sent OK
Status:     Directory listing successful
```

Local site: C:\Users\Anny\Documents\OVPN\Easy-RSA\

| Filename | Filesize | Filetype | L |
|---|---|---|---|
| .. | | | |
| caovpn.pem | 1,330 | PEM File | 1 |
| certserv.pem | 4,016 | PEM File | 1 |
| dh1024.pem | 245 | PEM File | 1 |
| privserv.pem | 916 | PEM File | 1 |

Selected 4 files. Total size: 6,507 bytes

Remote site: /

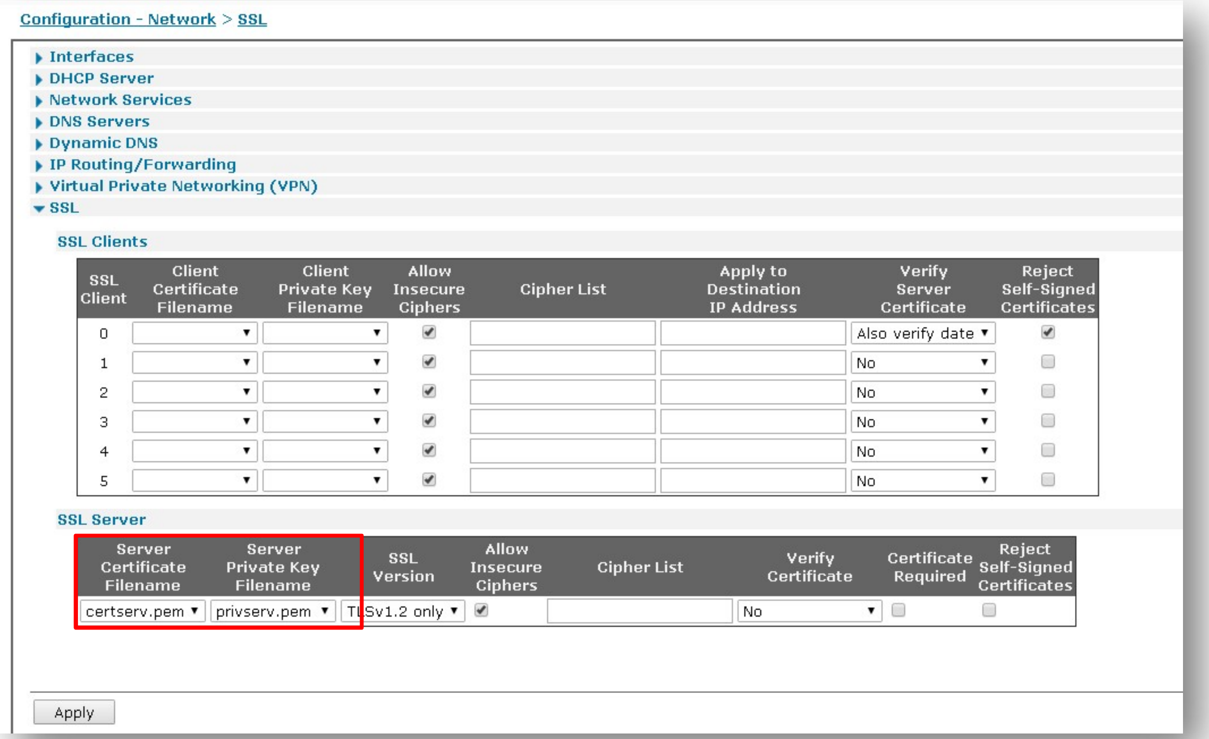
| Filename | Filesize | Filetype | Last modified | Permission |
|---|---|---|---|---|
| privrsa.pem | 1,679 | PEM File | 23/05/2017 09:... | -rwxrwxrw |
| privserv.pem | 916 | PEM File | 19/07/2017 13:... | -rwxrwxrw |
| privSSH.pem | 887 | PEM File | 19/07/2017 14:... | -rwxrwxrw |
| prlupdate.sb | 30,569 | SB File | 23/05/2017 09:... | -rwxrwxrw |
| provision.sb | 19,226 | SB File | 23/05/2017 09:... | -rwxrwxrw |
| pwds.da0 | 154 | DA0 File | 19/07/2017 14:... | -rwxrwxrw |
| python.zip | 1,736,922 | Compresse... | 23/05/2017 09:... | -rwxrwxrw |
| queryimsi.sb | 10,282 | SB File | 23/05/2017 09:... | -rwxrwxrw |
| sbios | 262,144 | File | 19/07/2017 14:... | -r-xr-xr-x |
| sregs.dat | 1,680 | DAT File | 01/02/2015 | -rwxrwxrw |

52 files and 1 directory. Total size: 19,628,127 bytes

## 3.4 SSL Certificates configuration

When the certificates have been transferred to the Server, the router needs to be configured so it knows which server certificate files to use:

**CONFIGURATION – NETWORK > SSL**



Configuration - Network > SSL

SSL Clients

| SSL Client | Client Certificate Filename | Client Private Key Filename | Allow Insecure Ciphers | Cipher List | Apply to Destination IP Address | Verify Server Certificate | Reject Self-Signed Certificates |
|---|---|---|---|---|---|---|---|
| 0 | | | ☑ | | | Also verify date | ☑ |
| 1 | | | ☑ | | | No | □ |
| 2 | | | ☑ | | | No | □ |
| 3 | | | ☑ | | | No | □ |
| 4 | | | ☑ | | | No | □ |
| 5 | | | ☑ | | | No | □ |

SSL Server

| Server Certificate Filename | Server Private Key Filename | SSL Version | Allow Insecure Ciphers | Cipher List | Verify Certificate | Certificate Required | Reject Self-Signed Certificates |
|---|---|---|---|---|---|---|---|
| certserv.pem | privserv.pem | TLSv1.2 only | ☑ | | No | □ | □ |

Where:

| Parameter | Setting | Description |
|---|---|---|
| Server Certificate Filename | certserv.pem | The file containing the server certificate is selected from this drop-down list. In this example this the one just transferred to the router. |
| Server Private Key Filename | privserv.pem | The file containing the private key that matches the above certificate is selected from this drop-down list. In this example this the one just transferred to the router. |

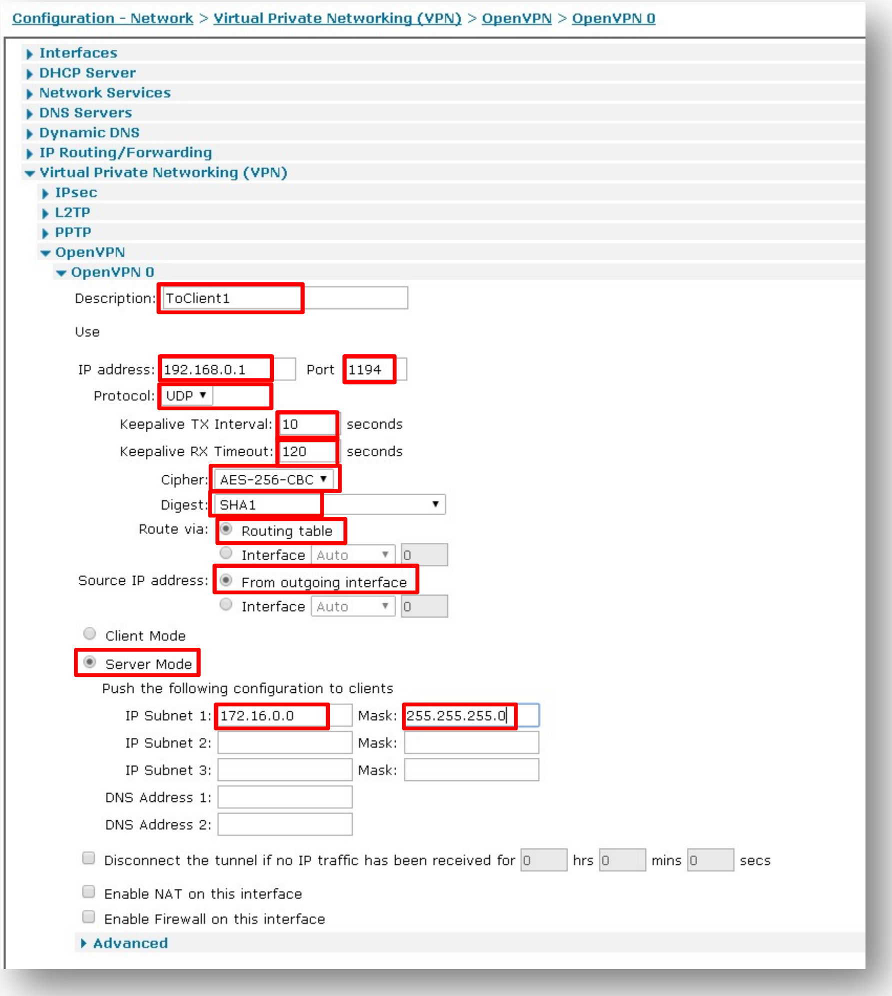
## 3.5 OpenVPN Server mode configuration

An OpenVPN interface will be configured on the TransPort router that acts as OpenVPN server. There should be as many OpenVPN interfaces configured as the number or required concurrent VPN connections. For example, if there are 10 remote users and there are likely to be 3 connected at any one time, 3 OpenVPN interfaces will be needed.

In case of multiple clients, this is not directly related to either client1 or client 2. But are a set of parameters that must match and have the correct settings for any client that tries to connect in.

In this Application Note, there is 1 remote user, so 1 OpenVPN interface will be configured:

**CONFIGURATION - NETWORK > VIRTUAL PRIVATE NETWORKING (VPN) > OPENVPN > OPENVPN 0**



Configuration - Network > Virtual Private Networking (VPN) > OpenVPN > OpenVPN 0

Description: ToClient1

Use

IP address: 192.168.0.1 Port 1194

Protocol: UDP

Keepalive TX Interval: 10 seconds

Keepalive RX Timeout: 120 seconds

Cipher: AES-256-CBC

Digest: SHA1

Route via: ● Routing table
○ Interface Auto 0

Source IP address: ● From outgoing interface
○ Interface Auto 0

○ Client Mode

● Server Mode

Push the following configuration to clients

IP Subnet 1: 172.16.0.0 Mask: 255.255.255.0

IP Subnet 2: Mask:

IP Subnet 3: Mask:

DNS Address 1:

DNS Address 2:

□ Disconnect the tunnel if no IP traffic has been received for 0 hrs 0 mins 0 secs

□ Enable NAT on this interface

□ Enable Firewall on this interface

Where:

| Parameter | Setting | Description |
|---|---|---|
| Description | OpenVPN Client 1 | Friendly name for this interface |
| IP address | 192.168.0.1 | IP address for this interface. OpenVPN interfaces use a 30 bit mask, the first address is the network address, the 2nd is the server address, the 3rd is the client address, and the 4th is the broadcast address. This address must be configured as the 2nd IP address in the block of 4. |
| Port | 1194 (default) | This is the TCP or UDP port number that the server will listen on for incoming VPN connections |
| Protocol | UDP (default) | This will either be TCP or UDP. It is up to the reader to decide which protocol to use, both the server and all clients must use the same protocol. See note below with regards to protocol choice. |
| Keepalive TX Interval | 10 | Keepalive interval: Interval between OpenVPN ping transmissions. These are required to detect the operational state of the VPN connection. |
| Keepalive RX Timeout | 120 | Keepalive timeout before VPN is marked as down: If the server hasn't received a ping from the client in the time limit specified, the tunnel will be marked as down |
| Cipher | AES-256-CBC | Encryption algorithm to use. The cipher is not negotiated during tunnel establishment. The server and all clients must be configured to use the same cipher. If the ciphers do not match, decryption errors will occur. |
| Digest | SHA1 (default) | Authentication algorithm to use. The digest is not negotiated during tunnel establishment. The server and all clients must be configured to use the same digest. If the ciphers do not match, authentication errors will occur. |
| Route via | Routing table (default) | Uses the routing table to determine the best route |
| Source IP address | From outgoing interface (default) | The IP address of the outgoing interface will be used as the source IP address |
| Server mode | Selected | Enables server mode. This should be enabled so the OpenVPN interface will answer incoming VPN connections. |
| Push IP Subnet 1 | 172.16.0.0 | Network IP address to push as a route. These parameters are used to push routing information to the remote VPN client. All subnets that can and must be accessed via the VPN tunnel should be specified here. |
| Push IP mask 1 | 255.255.255.0 | Network IP mask to push as a route. This is used in conjunction with the IP address field above |

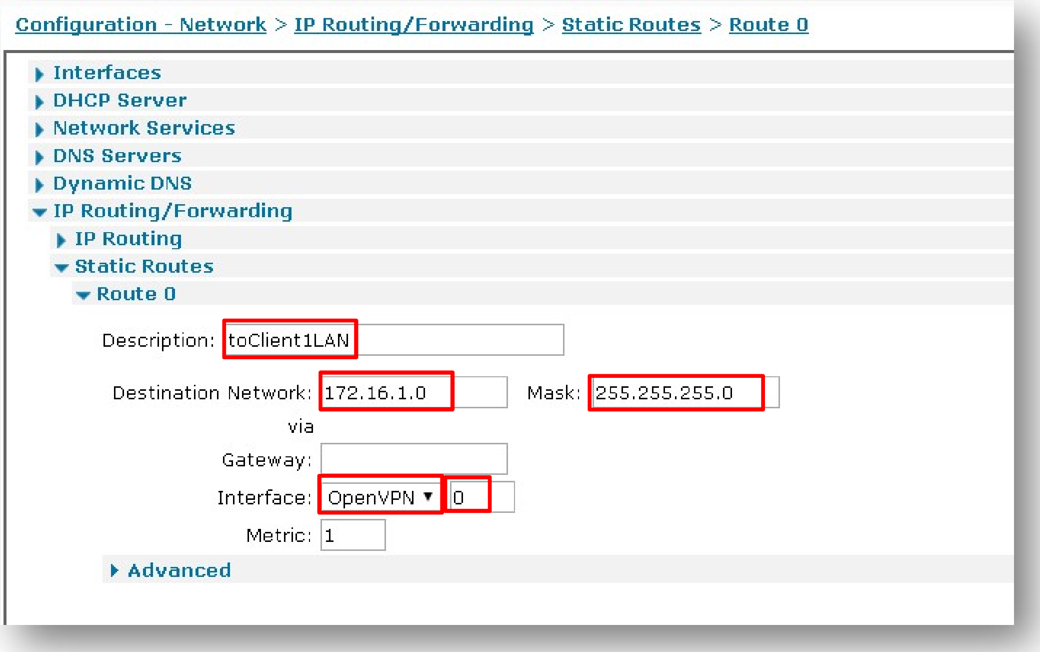
**Note regarding TCP or UDP:**

**UDP** has less protocol overhead than TCP as there is no reliability support built into UDP. A data channel packet (a packet to be tunnelled) gets encrypted and set as the payload of a UDP packet before being sent on its way. If the packet is dropped, no retransmissions of the encrypted packet will occur. It is up to the higher layers to detect that a packet has been lost and go about retransmitting. It is more difficult to detect that a peer has disconnected though, and no indication is sent to the peer if the local end closes the socket. For that reason, use of OpenVPN pings is generally required to confirm that the tunnel is still established. If no pings are received within a period of time the tunnel should be deemed to be failed and the tunnel should be torn down. A reliability layer is built into OpenVPN to ensure that control channel packets are transmitted to the remote peer. This reliability layer is used whether using TCP or UDP for the link transport.

**TCP** has higher overhead than UDP as all data is acknowledged. Also, there are issues that cause problems when transporting TCP traffic over a TCP link. This is effectively what will be occurring when a TCP stream is tunnelled through an OpenVPN tunnel configured to use TCP as the transport layer. Data transfer can get quite bogged down when retransmits start occurring. With TCP as the link transport protocol however, all traffic will get through the tunnel with no packet loss at all. When using TCP, it is much clearer when a socket has been closed by the other peer. Notifications will be delivered to the OpenVPN task that the socket has closed in a timely fashion without the need to rely on traffic through the tunnel. For this reason, there is less need to configure the peers to deliver OpenVPN pings through the data channel to confirm connectivity. With TCP, TCP keepalives can be used to keep the underlying interface connected. The bottom line is that less traffic needs to flow to confirm tunnel connectivity during times of low traffic through the tunnel.

In order to enable the router to reach the LAN of the client, a route must be configured for this subnet, with the outgoing interface being the OVPN 0 one:

## CONFIGURATION - NETWORK > IP ROUTING/FORWARDING > STATIC ROUTES > ROUTE 0



Configuration - Network > IP Routing/Forwarding > Static Routes > Route 0

Description: toClient1LAN

Destination Network: 172.16.1.0 Mask: 255.255.255.0

via

Gateway:

Interface: OpenVPN 0

Metric: 1

Where:

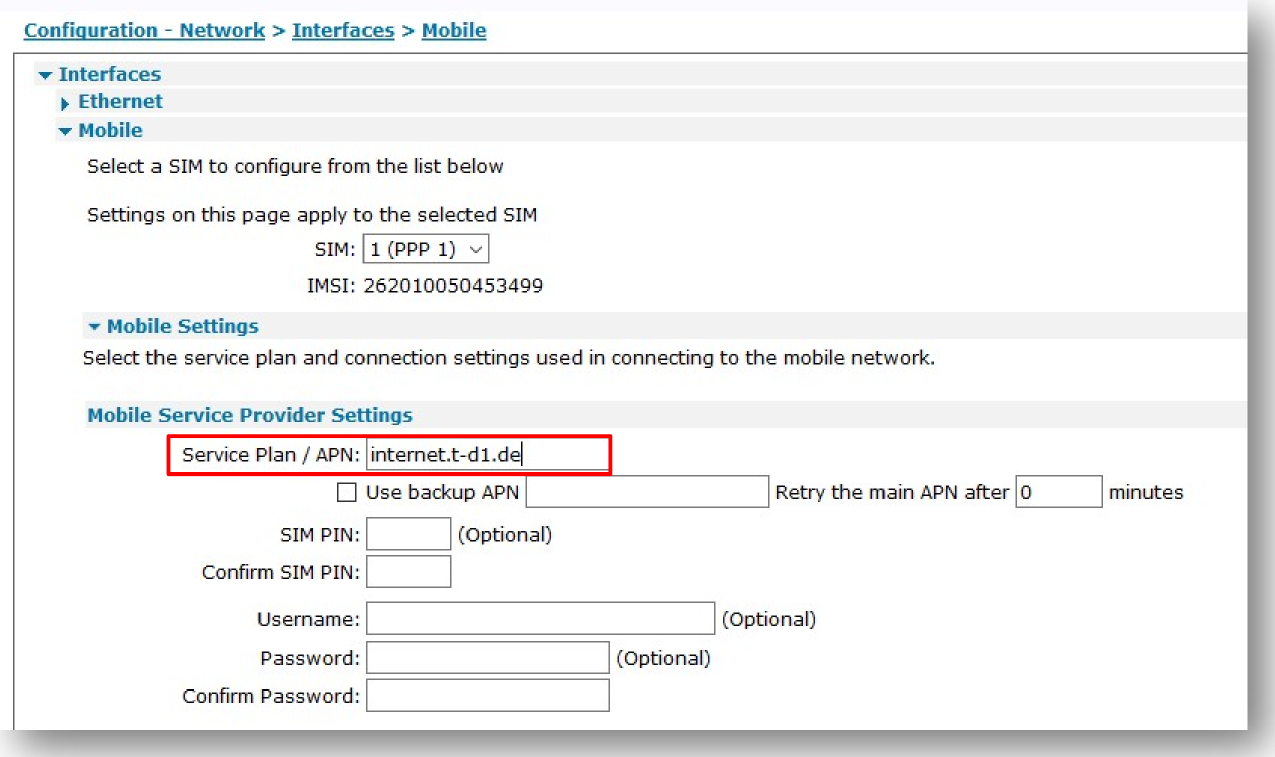
| Parameter | Setting | Description |
|---|---|---|
| Description | ToClient1LAN | Friendly name for this static route |
| Destination Network-Mask | 172.16.1.0-255.255.255.0 | The IP address of the destination subnet, network or IP address for the route. If the router receives a packet with a destination IP address that matches the Destination Network/Mask combination it will route the packet through the interface specified below. In this example, the destination subnet is the Client one. |
| Interface | OpenVPN 0 | The interface for routing the packets. Select from the drop-down list and enter the interface instance number in the adjacent text box. In this example, this is the OVPN interface just configured. |

# 4 CLIENT CONFIGURATION

## 4.1 WAN Interface configuration

In this example the Client has the Mobile interface as the WAN interface and it is configured as follows:

**CONFIGURATION - NETWORK > INTERFACES > MOBILE**



Configuration - Network > Interfaces > Mobile

Select a SIM to configure from the list below

Settings on this page apply to the selected SIM

SIM: 1 (PPP 1)

IMSI: 262010050453499

Select the service plan and connection settings used in connecting to the mobile network.

Service Plan / APN: internet.t-d1.de

☐ Use backup APN  Retry the main APN after 0 minutes

SIM PIN: (Optional)

Confirm SIM PIN:

Username: (Optional)

Password: (Optional)

Confirm Password:

Where:

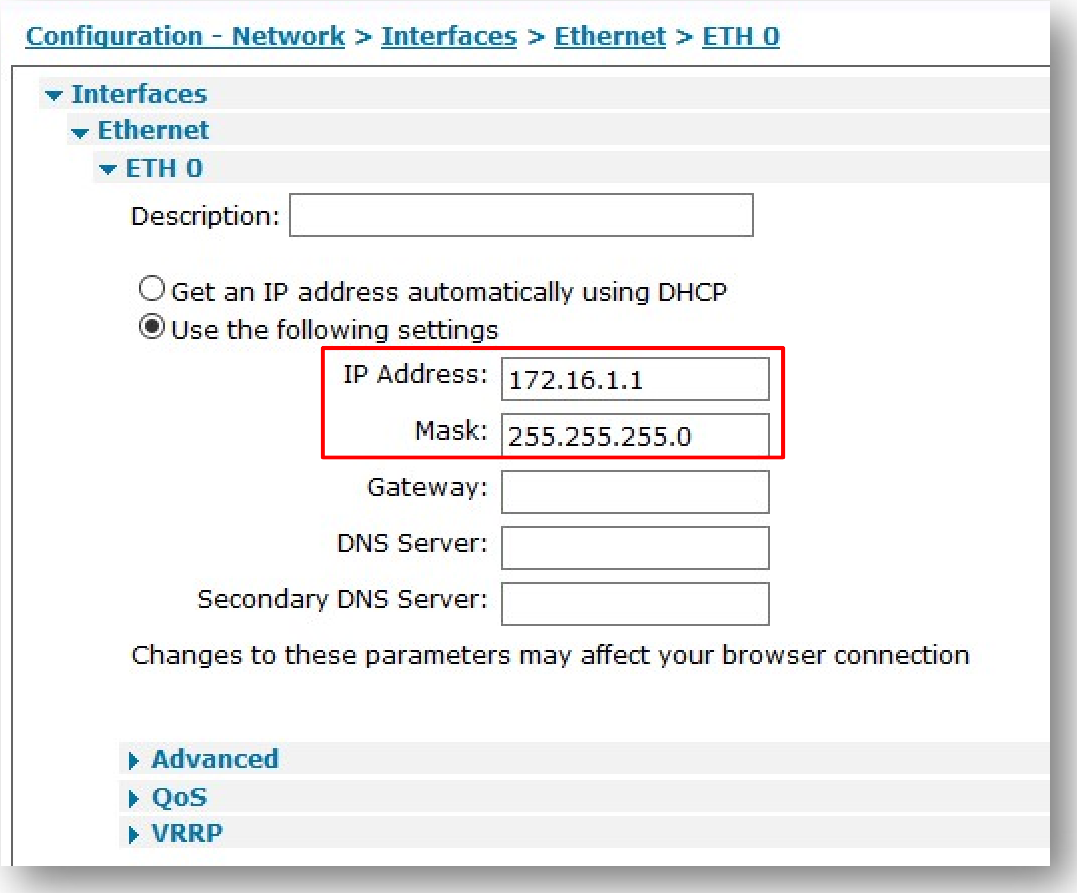
| Parameter | Setting | Description |
|---|---|---|
| Service Plan/APN | Internet.t-d1.de | Enter the APN of your mobile provider |

**Please note:** Depending on provider, a SIM PIN or Username/Password may be required. If needed, enter them in the appropriate fields.

## 4.2 LAN Interface configuration

In this example, the LAN interface is configured with a static address as follows:

**CONFIGURATION - NETWORK > INTERFACES > ETHERNET > ETH 0**



Configuration - Network > Interfaces > Ethernet > ETH 0

Description:

○ Get an IP address automatically using DHCP
● Use the following settings

IP Address: 172.16.1.1

Mask: 255.255.255.0

Gateway:

DNS Server:

Secondary DNS Server:

Changes to these parameters may affect your browser connection

Where:

| Parameter | Setting | Description |
|---|---|---|
| IP Address | 172.16.1.1 | Enter the IP address of the LAN interface for the router |
| Mask | 255.255.255.0 | Enter the subnet mask |

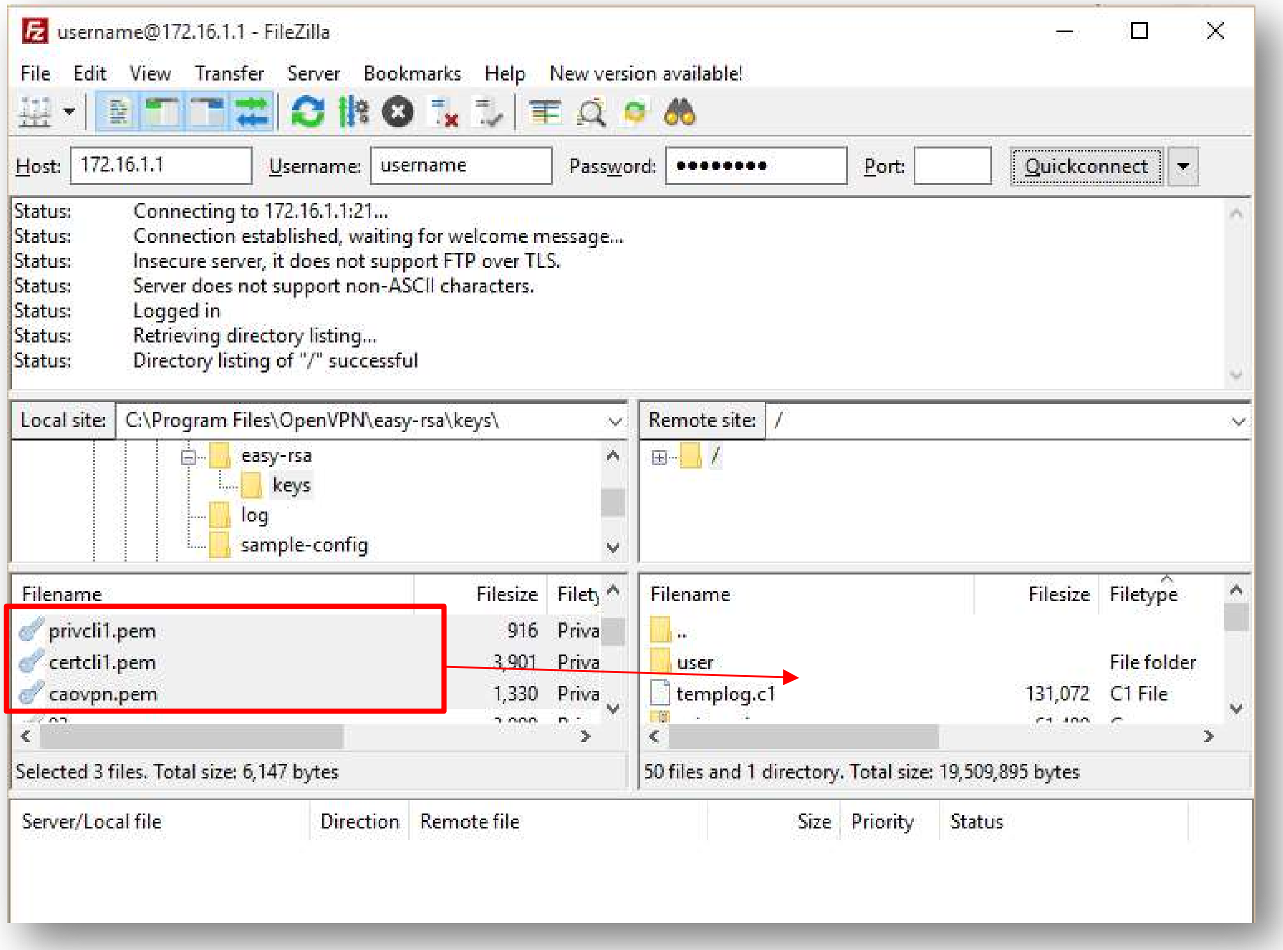
## 4.3 Transfer Certificates and Key files

Before to transfer the Certficates and Key files on the client, they must be renamed as follows:

| Filename | Purpose | New FileName |
|---|---|---|
| ca.crt | Root CA certificate | caovpn.pem |
| client1.crt | Client1 Certificate | certcli1.pem |
| client1.key | Client1 Key | privcli1.pem |

Once done that, the files can be transferred to the Client using for example an FTP client, connected with the TransPort router with usual username and password.

Please note that you may need to change your IP on the laptop accordingly with the new IP address configured on the ETH0 of the router.



Host: 172.16.1.1 Username: username Password: ••••••••• Port:

```
Status:         Connecting to 172.16.1.1:21...
Status:         Connection established, waiting for welcome message...
Status:         Insecure server, it does not support FTP over TLS.
Status:         Server does not support non-ASCII characters.
Status:         Logged in
Status:         Retrieving directory listing...
Status:         Directory listing of "/" successful
```

Local site: C:\Program Files\OpenVPN\easy-rsa\keys\

- easy-rsa
  - keys
- log
- sample-config

| Filename | Filesize | Filety |
|---|---|---|
| privcli1.pem | 916 | Priva |
| certcli1.pem | 3,901 | Priva |
| caovpn.pem | 1,330 | Priva |

Selected 3 files. Total size: 6,147 bytes

Remote site: /

| Filename | Filesize | Filetype |
|---|---|---|
| .. | | |
| user | | File folder |
| templog.c1 | 131,072 | C1 File |

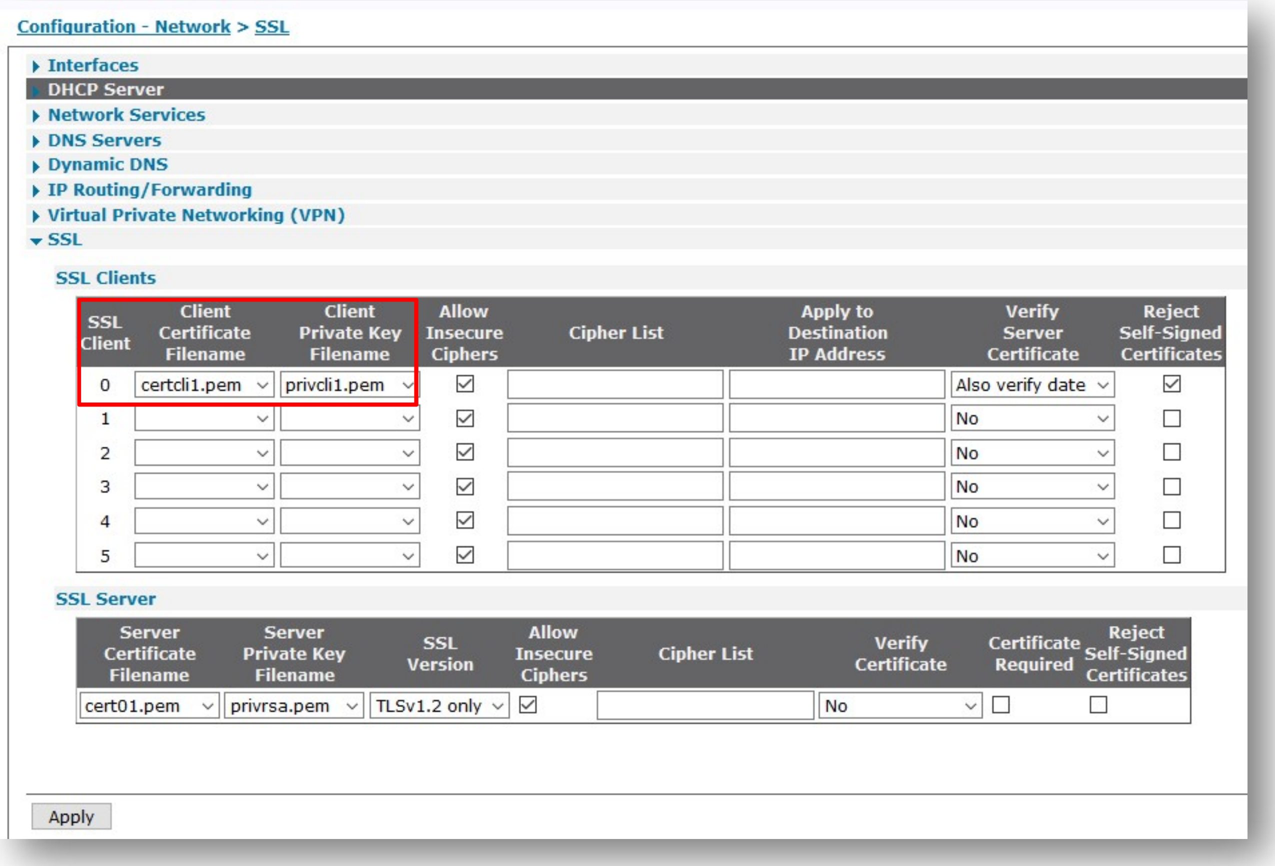
50 files and 1 directory. Total size: 19,509,895 bytes

| Server/Local file | Direction | Remote file | Size | Priority | Status |
|---|---|---|---|---|---|

## 4.4 SSL Certificates configuration

When the certificates have been transferred to the Client, the router needs to be configured so it knows which client certificate files to use:

**CONFIGURATION – NETWORK > SSL**



SSL Clients

| SSL Client | Client Certificate Filename | Client Private Key Filename | Allow Insecure Ciphers | Cipher List | Apply to Destination IP Address | Verify Server Certificate | Reject Self-Signed Certificates |
|---|---|---|---|---|---|---|---|
| 0 | certcli1.pem | privcli1.pem | ☑ | | | Also verify date | ☑ |
| 1 | | | ☑ | | | No | □ |
| 2 | | | ☑ | | | No | □ |
| 3 | | | ☑ | | | No | □ |
| 4 | | | ☑ | | | No | □ |
| 5 | | | ☑ | | | No | □ |

SSL Server

| Server Certificate Filename | Server Private Key Filename | SSL Version | Allow Insecure Ciphers | Cipher List | Verify Certificate | Certificate Required | Reject Self-Signed Certificates |
|---|---|---|---|---|---|---|---|
| cert01.pem | privrsa.pem | TLSv1.2 only | ☑ | | No | □ | □ |

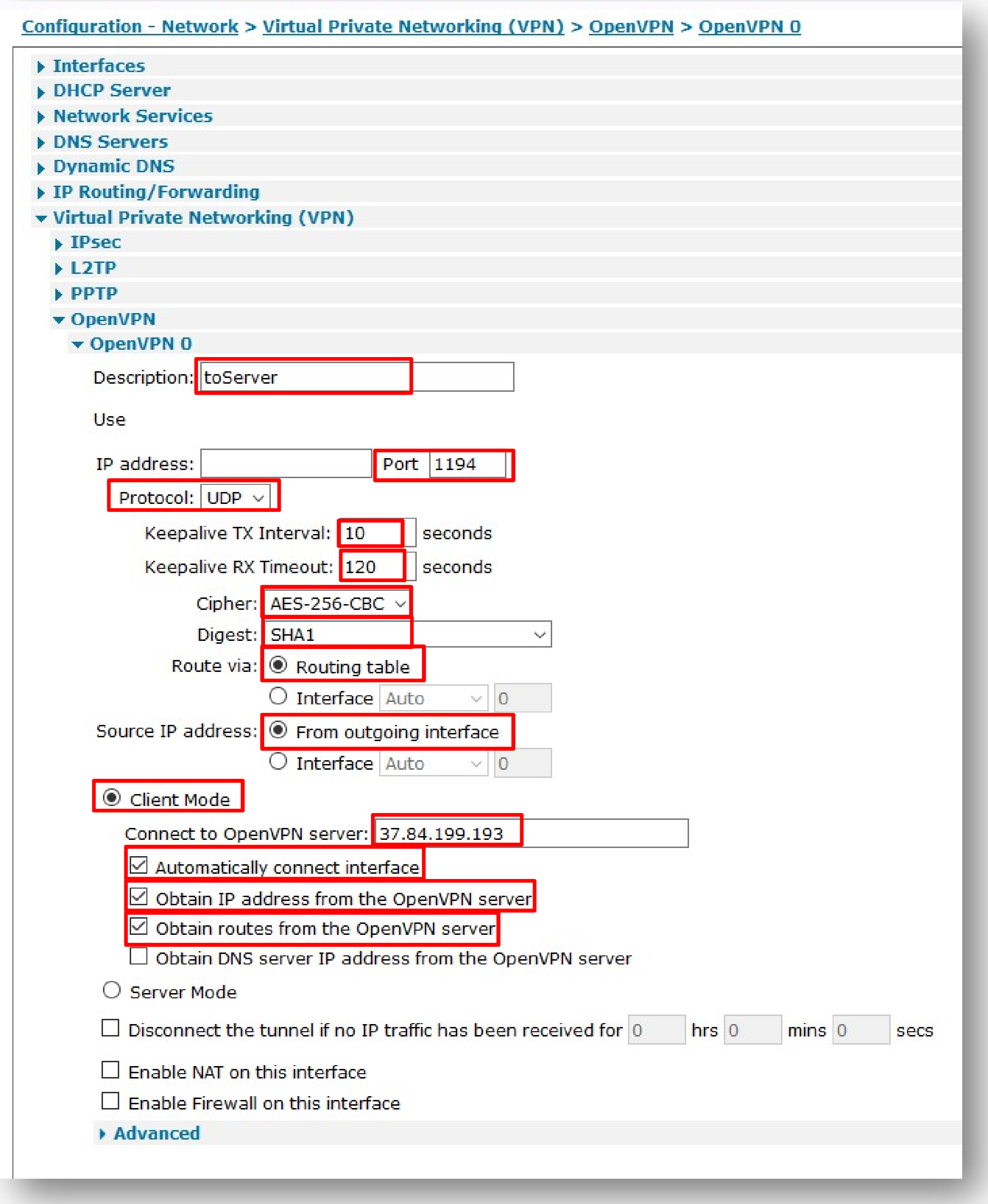
Where:

| Parameter | Setting | Description |
|---|---|---|
| Client Certificate Filename | certcli1.pem | The name of the required certificate file is selected from those available on the router's filing system from this drop-down list. In this example this the one just transferred to the router. |
| Client Private Key Filename | privcli1.pem | The name of the file that contains the private key that matches the public key stored in the above parameter, is selected from this drop-down list. In this example this the one just transferred to the router. |

## 4.5 OpenVPN Client mode configuration

An OpenVPN interface will be configured on the TransPort router that acts as OpenVPN client:

**CONFIGURATION - NETWORK > VIRTUAL PRIVATE NETWORKING (VPN) > OPENVPN > OPENVPN 0**



Description: toServer

Use

IP address: Port 1194

Protocol: UDP

Keepalive TX Interval: 10 seconds

Keepalive RX Timeout: 120 seconds

Cipher: AES-256-CBC

Digest: SHA1

Route via: ● Routing table

○ Interface Auto 0

Source IP address: ● From outgoing interface

○ Interface Auto 0

● Client Mode

Connect to OpenVPN server: 37.84.199.193

☑ Automatically connect interface

☑ Obtain IP address from the OpenVPN server

☑ Obtain routes from the OpenVPN server

☐ Obtain DNS server IP address from the OpenVPN server

○ Server Mode

☐ Disconnect the tunnel if no IP traffic has been received for 0 hrs 0 mins 0 secs

☐ Enable NAT on this interface

☐ Enable Firewall on this interface

Where:

| Parameter | Setting | Description |
|---|---|---|
| Description | toServer | Friendly name for this interface |
| Port | 1194 (default) | This is the TCP or UDP port number that the server will listen on for incoming VPN connections |
| Protocol | UDP (default) | This will either be TCP or UDP. It is up to the reader to decide which protocol to use, both the server and all clients must use the same protocol. See note with regards to protocol choice in the previous section |
| Keepalive TX Interval | 10 | Keepalive interval: Interval between OpenVPN ping transmissions. These are required to detect the operational state of the VPN connection. |
| Keepalive RX Timeout | 120 | Keepalive timeout before VPN is marked as down: If the server hasn't received a ping from the client in the time limit specified, the tunnel will be marked as down |
| Cipher | AES-256-CBC | Encryption algorithm to use. The cipher is not negotiated during tunnel establishment. The server and all clients must be configured to use the same cipher. If the ciphers do not match, decryption errors will occur. |
| Digest | SHA1 (default) | Authentication algorithm to use. The digest is not negotiated during tunnel establishment. The server and all clients must be configured to use the same digest. If the ciphers do not match, authentication errors will occur. |
| Route via | Routing table (default) | Uses the routing table to determine the best route |
| Source IP address | From outgoing interface (default) | The IP address of the outgoing interface will be used as the source IP address |
| Client Mode | Selected | Use Client mode |
| Connect to OpenVPN server | 37.84.199.193 | Public IP address of OpenVPN server |
| Automatically connect interface | ✓ | Connects to the OpenVPN server automatically, always on mode. |
| Obtain IP address from the OpenVPN server | ✓ | This interface will obtain an IP address from the OpenVPN server |
| Obtain routes from the OpenVPN server | ✓ | Routing information will be obtained from the OpenVPN server |

**Please note:**

- The "IP address" field is left blank as, in this configuration, the Client will obtain the IP address from the OpenVPN Server.
- As the routing information will be obtained automatically from the Server, there is no need to configure a static route in order to enable the Client to reach the LAN of the Server.

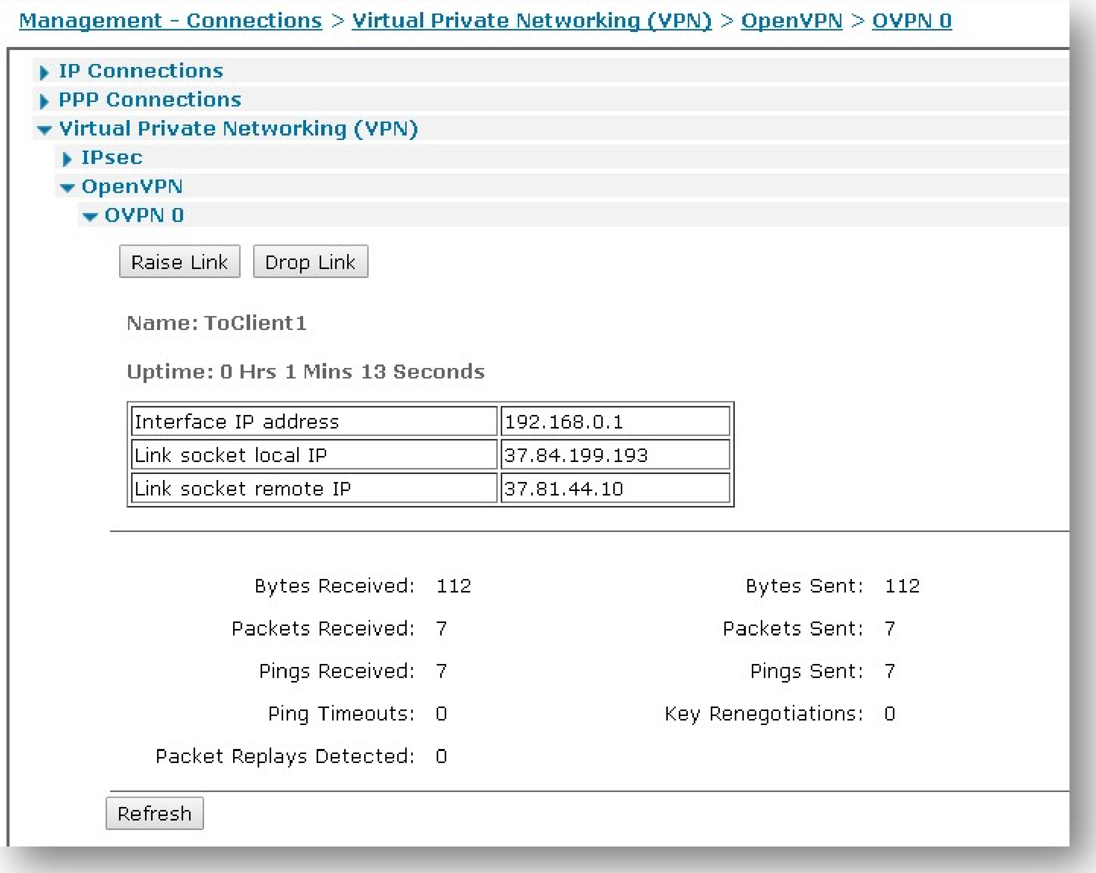
# 5 TESTING THE OPENVPN CONENCTION

## 5.1 Check Open VPN Connection

If the configuration is correct on both end routers and they are reachable to each other, the OpenVPN connection should be shown as UP on both.

Open VPN Server:

**MANAGEMENT - CONNECTIONS > VIRTUAL PRIVATE NETWORKING (VPN) > OPENVPN > OVPN 0**


Management - Connections > Virtual Private Networking (VPN) > OpenVPN > OVPN 0
IP Connections
PPP Connections
Virtual Private Networking (VPN)
IPsec
OpenVPN
OVPN 0
Raise Link
Drop Link
Refresh

Name: ToClient1

Uptime: 0 Hrs 1 Mins 13 Seconds

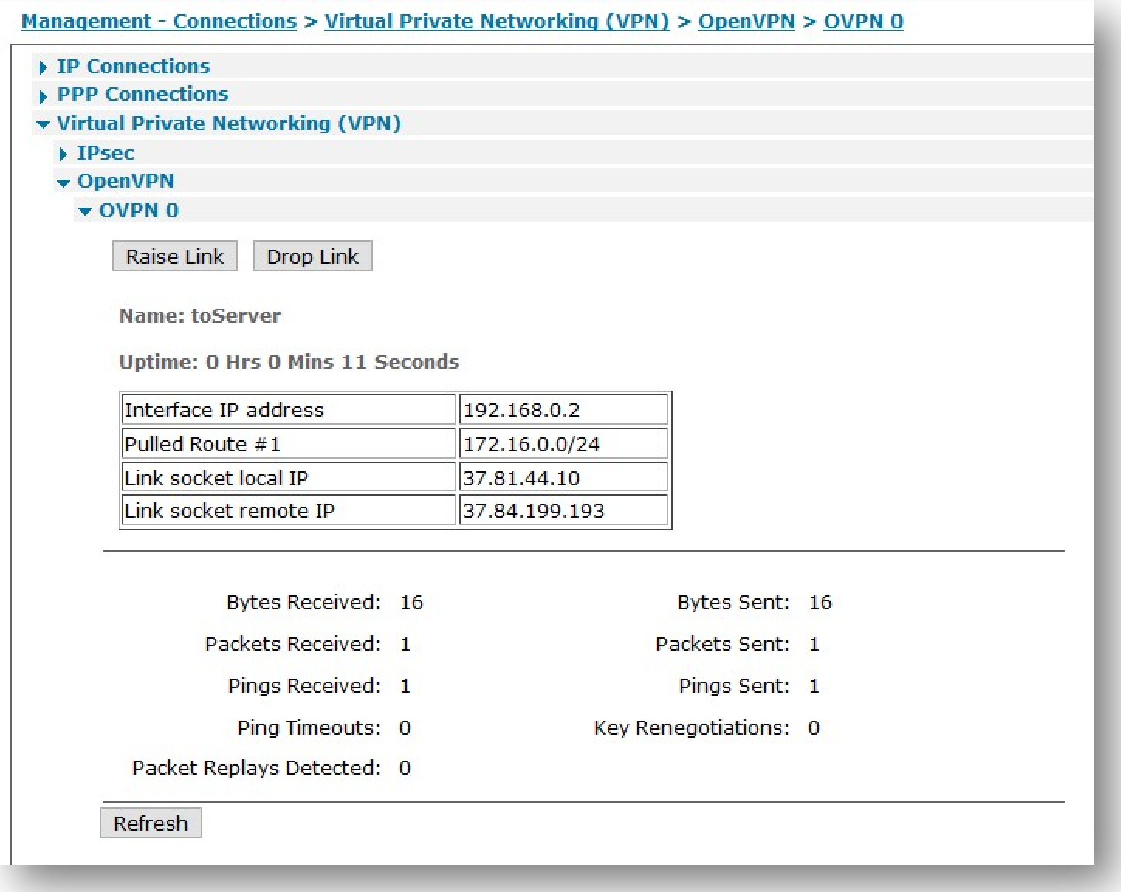
| | |
|---|---|
| Interface IP address | 192.168.0.1 |
| Link socket local IP | 37.84.199.193 |
| Link socket remote IP | 37.81.44.10 |

| | | | |
|---|---|---|---|
| Bytes Received: | 112 | Bytes Sent: | 112 |
| Packets Received: | 7 | Packets Sent: | 7 |
| Pings Received: | 7 | Pings Sent: | 7 |
| Ping Timeouts: | 0 | Key Renegotiations: | 0 |
| Packet Replays Detected: | 0 | | |

The OpenVPN connection status will show the IP address configured on the OVPN interface for the Server and, on both the client and the server, the local and remote external IPs used for the connection.

Open VPN Client:

**MANAGEMENT - CONNECTIONS > VIRTUAL PRIVATE NETWORKING (VPN) > OPENVPN > OVPN 0**


Management - Connections > Virtual Private Networking (VPN) > OpenVPN > OVPN 0
IP Connections
PPP Connections
Virtual Private Networking (VPN)
IPsec
OpenVPN
OVPN 0
Raise Link
Drop Link
Refresh

Name: toServer

Uptime: 0 Hrs 0 Mins 11 Seconds

| | |
|---|---|
| Interface IP address | 192.168.0.2 |
| Pulled Route #1 | 172.16.0.0/24 |
| Link socket local IP | 37.81.44.10 |
| Link socket remote IP | 37.84.199.193 |

| | | | |
|---|---|---|---|
| Bytes Received: | 16 | Bytes Sent: | 16 |
| Packets Received: | 1 | Packets Sent: | 1 |
| Pings Received: | 1 | Pings Sent: | 1 |
| Ping Timeouts: | 0 | Key Renegotiations: | 0 |
| Packet Replays Detected: | 0 | | |

The OpenVPN connection status on the client will also show the IP address and routing information pulled from the Server.

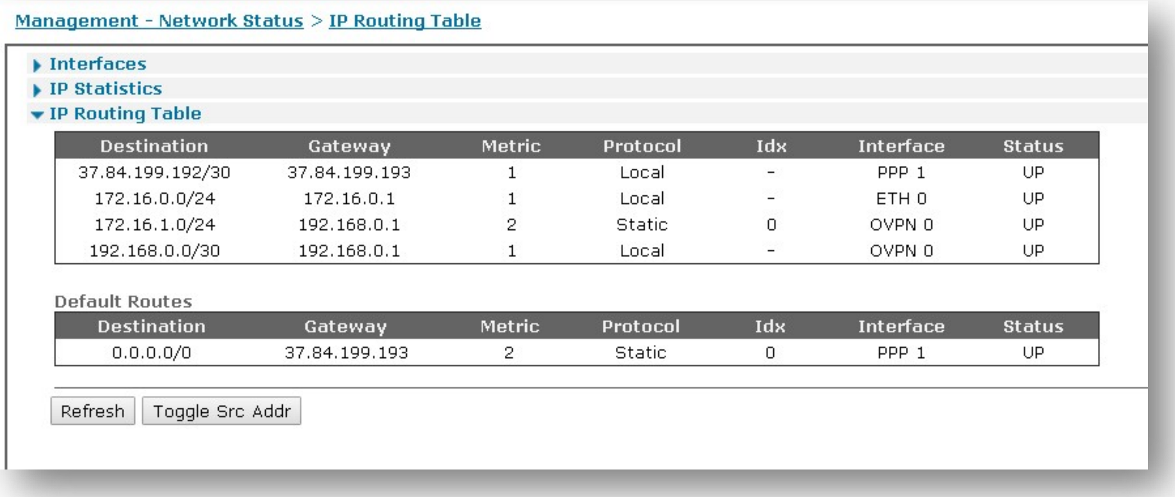
**Please note:** If the OpenVPN connection is not correctly UP please refer to the following guide to troubleshoot the issue:

## 5.2 Check the Routing Table

Once the Open VPN connection is UP, also the routing table should be changed accordingly:

Open VPN Server:

**MANAGEMENT - NETWORK STATUS > IP ROUTING TABLE**



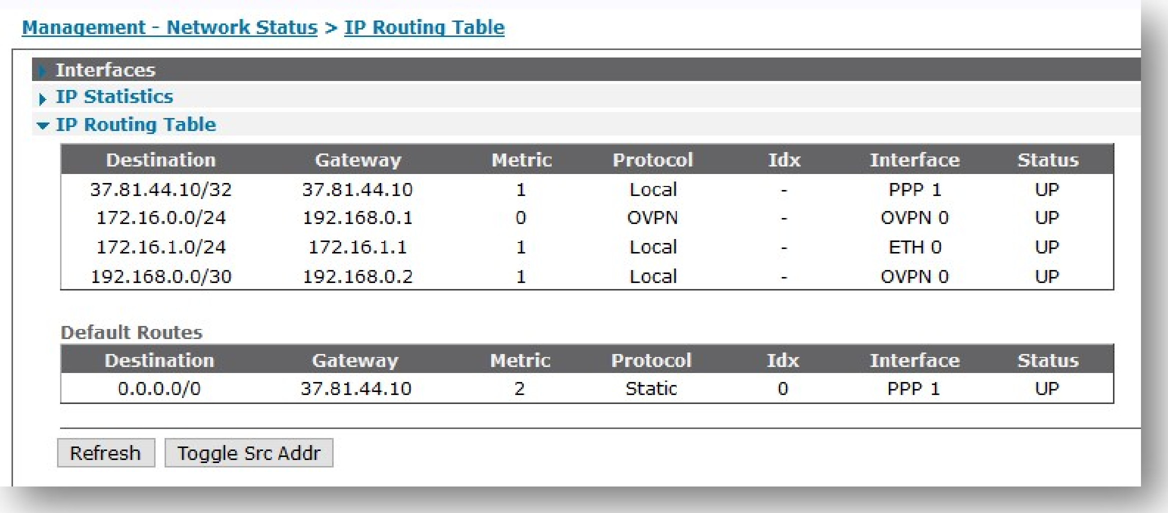
| Destination | Gateway | Metric | Protocol | Idx | Interface | Status |
|---|---|---|---|---|---|---|
| 37.84.199.192/30 | 37.84.199.193 | 1 | Local | - | PPP 1 | UP |
| 172.16.0.0/24 | 172.16.0.1 | 1 | Local | - | ETH 0 | UP |
| 172.16.1.0/24 | 192.168.0.1 | 2 | Static | 0 | OVPN 0 | UP |
| 192.168.0.0/30 | 192.168.0.1 | 1 | Local | - | OVPN 0 | UP |

Default Routes

| Destination | Gateway | Metric | Protocol | Idx | Interface | Status |
|---|---|---|---|---|---|---|
| 0.0.0.0/0 | 37.84.199.193 | 2 | Static | 0 | PPP 1 | UP |

Open VPN Client:

**MANAGEMENT - NETWORK STATUS > IP ROUTING TABLE**



| Destination | Gateway | Metric | Protocol | Idx | Interface | Status |
|---|---|---|---|---|---|---|
| 37.81.44.10/32 | 37.81.44.10 | 1 | Local | - | PPP 1 | UP |
| 172.16.0.0/24 | 192.168.0.1 | 0 | OVPN | - | OVPN 0 | UP |
| 172.16.1.0/24 | 172.16.1.1 | 1 | Local | - | ETH 0 | UP |
| 192.168.0.0/30 | 192.168.0.2 | 1 | Local | - | OVPN 0 | UP |

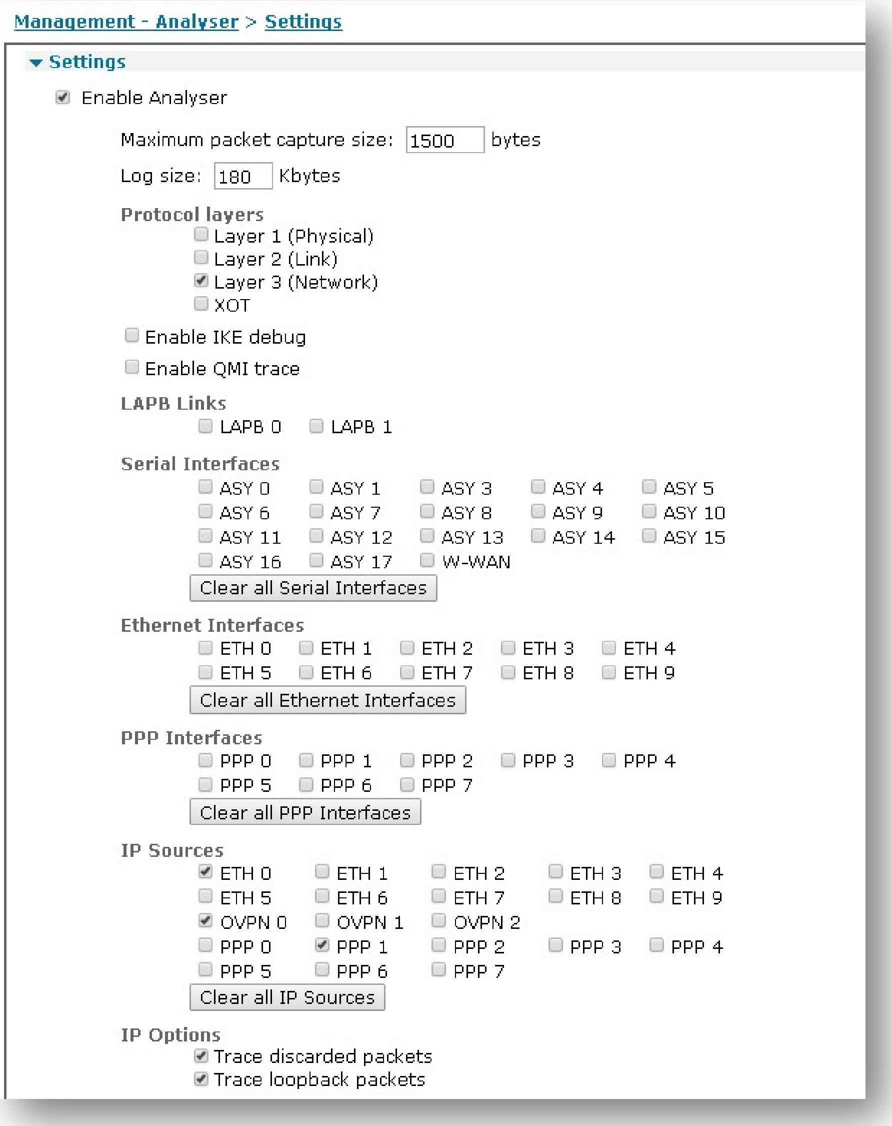
Default Routes

| Destination | Gateway | Metric | Protocol | Idx | Interface | Status |
|---|---|---|---|---|---|---|
| 0.0.0.0/0 | 37.81.44.10 | 2 | Static | 0 | PPP 1 | UP |

## 5.3 Check the Traffic

In order to check that the Traffic from the two LANs are working and passing correctly through the OpenVPN connection, the analyser can be configured to trace that traffic. In this example the trace will be taken on the Client side.

**MANAGEMENT - ANALYSER > SETTINGS**



Management - Analyser > Settings

▾ Settings

☑ Enable Analyser

Maximum packet capture size: 1500 bytes

Log size: 180 Kbytes

Protocol layers
□ Layer 1 (Physical)
□ Layer 2 (Link)
☑ Layer 3 (Network)
□ XOT

□ Enable IKE debug

□ Enable QMI trace

LAPB Links
□ LAPB 0 □ LAPB 1

Serial Interfaces
□ ASY 0 □ ASY 1 □ ASY 3 □ ASY 4 □ ASY 5
□ ASY 6 □ ASY 7 □ ASY 8 □ ASY 9 □ ASY 10
□ ASY 11 □ ASY 12 □ ASY 13 □ ASY 14 □ ASY 15
□ ASY 16 □ ASY 17 □ W-WAN
Clear all Serial Interfaces

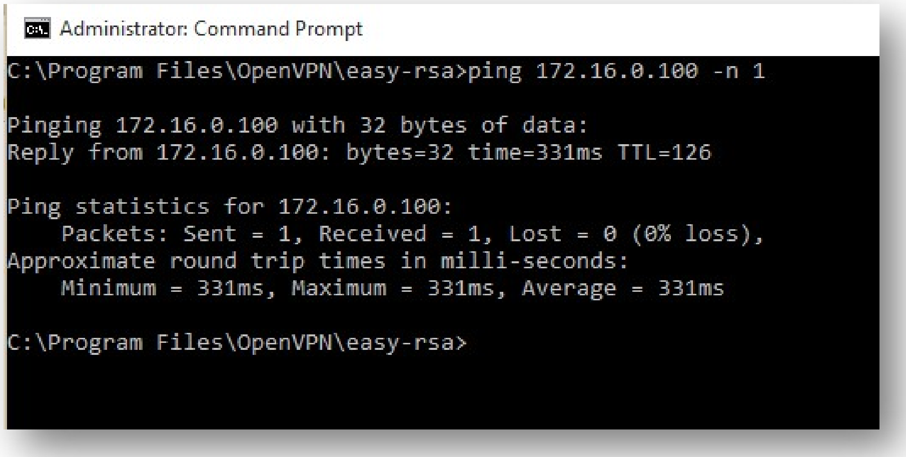
Ethernet Interfaces
□ ETH 0 □ ETH 1 □ ETH 2 □ ETH 3 □ ETH 4
□ ETH 5 □ ETH 6 □ ETH 7 □ ETH 8 □ ETH 9
Clear all Ethernet Interfaces

PPP Interfaces
□ PPP 0 □ PPP 1 □ PPP 2 □ PPP 3 □ PPP 4
□ PPP 5 □ PPP 6 □ PPP 7
Clear all PPP Interfaces

IP Sources
☑ ETH 0 □ ETH 1 □ ETH 2 □ ETH 3 □ ETH 4
□ ETH 5 □ ETH 6 □ ETH 7 □ ETH 8 □ ETH 9
☑ OVPN 0 □ OVPN 1 □ OVPN 2
□ PPP 0 ☑ PPP 1 □ PPP 2 □ PPP 3 □ PPP 4
□ PPP 5 □ PPP 6 □ PPP 7
Clear all IP Sources

IP Options
☑ Trace discarded packets
☑ Trace loopback packets

Apply the changes and make a ping from a laptop in Client LAN to a device in the Server LAN:



```
C:\Program Files\OpenVPN\easy-rsa>ping 172.16.0.100 -n 1

Pinging 172.16.0.100 with 32 bytes of data:
Reply from 172.16.0.100: bytes=32 time=331ms TTL=126

Ping statistics for 172.16.0.100:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 331ms, Maximum = 331ms, Average = 331ms

C:\Program Files\OpenVPN\easy-rsa>
```

If all is configured correctly, the ping should success, in case of need to check the, the ana.txt can be checked.

It will show like the following:

ECHO REQ arriving from the Laptop on ETH 0:

```
----------
   -----   19-7-2017  14:28:08.290   ------
   45 00 00 3C 2C C3 00 00 80 01 B4 15 AC 10 01 64     E..<,.........d
   AC 10 00 64 08 00 23 1E 00 01 2A 3D 61 62 63 64     ...d..#...*=abcd
   65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74     efghijklmnopqrst
   75 76 77 61 62 63 64 65 66 67 68 69                 uvwabcdefghi

   IP (In) From REM TO LOC       IFACE: ETH 0
   45             IP Ver:        4
                  Hdr Len:       20
   00             TOS:           Routine
                  Delay:         Normal
                  Throughput:    Normal
                  Reliability:   Normal
   00 3C          Length:        60
   2C C3          ID:            11459
   00 00          Frag Offset:   0
                  Congestion:    Normal
                                 May Fragment
                                 Last Fragment
   80             TTL:           128
   01             Proto:         ICMP
   B4 15          Checksum:      46101
   AC 10 01 64    Src IP:        172.16.1.100
   AC 10 00 64    Dst IP:        172.16.0.100
   ICMP:
   08             Type:          ECHO REQ
   00             Code:          0
   23 1E          Checksum:      7715
   ----------
```

ECHO REQ is forwarded to the OVPN interface and sent over the PPP link:

```
-----   19-7-2017  14:28:08.290   ------
45 00 00 3C 2C C3 00 00 7F 01 B5 15 AC 10 01 64     E..<,..........d
AC 10 00 64 08 00 23 1E 00 01 2A 3D 61 62 63 64     ...d..#...*=abcd
65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74     efghijklmnopqrst
75 76 77 61 62 63 64 65 66 67 68 69                 uvwabcdefghi

IP (Final) From LOC TO REM    IFACE: OVPN 0
45             IP Ver:        4
               Hdr Len:       20
00             TOS:           Routine
               Delay:         Normal
               Throughput:    Normal
               Reliability:   Normal
00 3C          Length:        60
2C C3          ID:            11459
00 00          Frag Offset:   0
               Congestion:    Normal
                              May Fragment
                              Last Fragment
7F             TTL:           127
01             Proto:         ICMP
B5 15          Checksum:      46357
AC 10 01 64    Src IP:        172.16.1.100
AC 10 00 64    Dst IP:        172.16.0.100
ICMP:
08             Type:          ECHO REQ
00             Code:          0
23 1E          Checksum:      7715
----------
-----   19-7-2017  14:28:08.290   ------
45 00 00 91 01 6A 00 00 FA 11 80 81 25 51 2C 0A     E....j......%Q,.
25 54 C7 C1 3F 9F 04 AA 00 7D 12 99 30 BA A6 46     %T..?....}..0..F
F7 B5 3F C6 D4 05 50 55 CB 72 F0 44 8F 67 7C AE     ..?...PU.r.D.g|.
15 40 44 43 F6 0F F6 0F 3C 3C F5 BA 15 49 3A 65     .@DC....<<...I:e
09 A7 70 93 62 88 CC 1C A2 25 F5 3E ED D1 C6 5B     ..p.b....%.>...[
1D A3 BE 28 1C 93 AA 95 E1 81 B4 21 60 8F 5D 02     ...(.......!`.].
AC 73 A0 95 F7 78 FB 39 DF 51 DF 33 77 E3 88 EF     .s...x.9.Q.3w...
88 E8 0B 15 35 AB E2 56 E0 21 FA C1 22 A0 C9 1C     ....5..V.!.."...
04 46 BB 9D 60 93 BB AD 77 E9 7A EF 41 8C 48 D6     .F..`...w.z.A.H.
F2                                                  .

IP (Final) From LOC TO REM    IFACE: PPP 1
45             IP Ver:        4
               Hdr Len:       20
```

```
00             TOS:           Routine
               Delay:         Normal
               Throughput:    Normal
               Reliability:   Normal
00 91          Length:        145
01 6A          ID:            362
00 00          Frag Offset:   0
               Congestion:    Normal
                              May Fragment
                              Last Fragment
FA             TTL:           250
11             Proto:         UDP
80 81          Checksum:      32897
25 51 2C 0A    Src IP:        37.81.44.10
25 54 C7 C1    Dst IP:        37.84.199.193
UDP:
3F 9F          SRC Port:      ??? (16287)
04 AA          DST Port:      ??? (1194)
00 7D          Length:        125
12 99          Checksum:      4761
----------
```

ECHO Reply received on the OVPN Interface via the PPP link:

```
-----   19-7-2017  14:28:08.620   ------
   45 00 00 91 00 DF 00 00 F4 11 87 0C 25 54 C7 C1     E...........%T..
   25 51 2C 0A 04 AA 3F 9F 00 7D BE 8B 30 F7 B9 69     %Q,...?..}..0..i
   CB 8F 11 7C 31 36 4E 1C 57 67 B8 01 8E AE 69 78     ...|16N.Wg....ix
   54 34 23 97 86 36 2E C2 F3 2A D1 CD 5E 0E CB D7     T4#..6...*..^...
   DA 7A 0B 61 62 E8 A7 94 6F 55 E6 5A E8 B6 E2 6C     .z.ab...oU.Z...l
   06 B6 E6 D0 DF 97 B0 01 0A 30 3F 63 61 98 0F 56     .........0?ca..V
   C7 D2 0A 59 99 AA 56 6E 06 77 8B 34 8D 18 DB BB     ...Y..Vn.w.4....
   A1 F9 A1 C3 BC 9F E1 21 C0 CB 7C 61 7B 5E 58 CD     .......!..|a{^X.
   20 DD 95 E3 B9 6E 2A 18 8B 5C 10 40 3D ED 93 7E      ....n*..\.@=..~
   54                                                  T

   IP (In) From REM TO LOC       IFACE: PPP 1
   45             IP Ver:        4
                  Hdr Len:       20
   00             TOS:           Routine
                  Delay:         Normal
                  Throughput:    Normal
                  Reliability:   Normal
   00 91          Length:        145
   00 DF          ID:            223
   00 00          Frag Offset:   0
                  Congestion:    Normal
                                 May Fragment
                                 Last Fragment
   F4             TTL:           244
   11             Proto:         UDP
   87 0C          Checksum:      34572
   25 54 C7 C1    Src IP:        37.84.199.193
   25 51 2C 0A    Dst IP:        37.81.44.10
   UDP:
   04 AA          SRC Port:      ??? (1194)
   3F 9F          DST Port:      ??? (16287)
   00 7D          Length:        125
   BE 8B          Checksum:      48779
   ----------
   -----   19-7-2017  14:28:08.620   ------
   45 00 00 3C 61 12 00 00 7F 01 80 C6 AC 10 00 64     E..<a..........d
   AC 10 01 64 00 00 2B 1E 00 01 2A 3D 61 62 63 64     ...d..+...*=abcd
   65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74     efghijklmnopqrst
   75 76 77 61 62 63 64 65 66 67 68 69                 uvwabcdefghi

   IP (In) From REM TO LOC       IFACE: OVPN 0
   45             IP Ver:        4
                  Hdr Len:       20
   00             TOS:           Routine
                  Delay:         Normal
                  Throughput:    Normal
                  Reliability:   Normal
   00 3C          Length:        60
   61 12          ID:            24850
   00 00          Frag Offset:   0
                  Congestion:    Normal
                                 May Fragment
                                 Last Fragment
   7F             TTL:           127
   01             Proto:         ICMP
   80 C6          Checksum:      32966
   AC 10 00 64    Src IP:        172.16.0.100
   AC 10 01 64    Dst IP:        172.16.1.100
   ICMP:
   00             Type:          ECHO REPLY
   00             Code:          0
   2B 1E          Checksum:      7723
   ----------
```

ECHO Reply is sent to the Client laptop via ETH 0:

```
-----   19-7-2017  14:28:08.620   ------
45 00 00 3C 61 12 00 00 7E 01 81 C6 AC 10 00 64     E..<a...~......d
AC 10 01 64 00 00 2B 1E 00 01 2A 3D 61 62 63 64     ...d..+...*=abcd
65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74     efghijklmnopqrst
75 76 77 61 62 63 64 65 66 67 68 69                 uvwabcdefghi

IP (Final) From LOC TO REM    IFACE: ETH 0
45             IP Ver:        4
               Hdr Len:       20
00             TOS:           Routine
               Delay:         Normal
               Throughput:    Normal
               Reliability:   Normal
00 3C          Length:        60
```

```
61 12          ID:            24850
00 00          Frag Offset:   0
               Congestion:    Normal
                              May Fragment
                              Last Fragment
7E             TTL:           126
01             Proto:         ICMP
81 C6          Checksum:      33222
AC 10 00 64    Src IP:        172.16.0.100
AC 10 01 64    Dst IP:        172.16.1.100
ICMP:
00             Type:          ECHO REPLY
00             Code:          0
2B 1E          Checksum:      7723
----------
```

# 6 CONFIGURATION FILES

## 6.1 OpenVPN Client configuration (WR11)

The config.da0 file and the hardware/firmware used on Open VPN Clientfor the purpose of this Application Note are shown below:

```
Command: config c show
Command result

eth 0 IPaddr "172.16.1.1"
eth 0 ipanon ON
lapb 0 ans OFF
lapb 0 tinact 120
lapb 1 tinact 120
lapb 3 dtemode 0
lapb 4 dtemode 0
lapb 5 dtemode 0
lapb 6 dtemode 0
ip 0 cidr ON
def_route 0 ll_ent "ppp"
def_route 0 ll_add 1
dhcp 0 IPmin "192.168.1.100"
dhcp 0 respdelms 500
dhcp 0 mask "255.255.255.0"
dhcp 0 gateway "192.168.1.1"
dhcp 0 DNS "192.168.1.1"
sntp 0 server "time.devicecloud.com"
dyndns 0 ifent "default"
ppp 0 timeout 300
ppp 1 name "W-WAN (HSPA 3G)"
ppp 1 phonenum "*98*1#"
ppp 1 IPaddr "0.0.0.0"
ppp 1 timeout 0
ppp 1 do_nat 2
ppp 1 use_modem 1
ppp 1 aodion 1
ppp 1 autoassert 1
ppp 1 ipanon ON
ppp 1 r_chap OFF
ppp 3 defpak 16
ppp 4 defpak 16
web 0 prelogin_info ON
ftpcli 0 hostname "ftp1.digi.com"
ftpcli 0 directory "support/firmware/transport/radio_module_firmware/he910d"
modemcc 0 info_asy_add 3
modemcc 0 init_str "+CGQREQ=1"
modemcc 0 init_str1 "+CGQMIN=1"
modemcc 0 apn "internet.t-d1.de"
modemcc 0 link_retries 10
modemcc 0 stat_retries 30
modemcc 0 sms_interval 1
modemcc 0 sms_access 1
modemcc 0 sms_concat 0
modemcc 0 init_str_2 "+CGQREQ=1"
modemcc 0 init_str1_2 "+CGQMIN=1"
modemcc 0 apn_2 "Your.APN.goes.here"
modemcc 0 link_retries_2 10
modemcc 0 stat_retries_2 30
modemcc 0 sms_access_2 1
modemcc 0 sms_concat_2 0
ana 0 anon ON
ana 0 l2on OFF
ana 0 l3on OFF
ana 0 xoton OFF
ana 0 lapdon 0
ana 0 lapbon 0
ana 0 loopon ON
ana 0 discardson ON
ana 0 maxdata 1500
ana 0 logsize 180
cmd 0 unitid "ss%s>"
cmd 0 cmdnua "99"
cmd 0 hostname "digi.router"
cmd 0 tremto 1200
cmd 0 rcihttp ON
user 0 access 0
user 1 name "username"
user 1 epassword "KD5lSVJDVVg="
user 1 access 0
user 2 access 0
user 3 access 0
user 4 access 0
user 5 access 0
user 6 access 0
user 7 access 0
user 8 access 0
user 9 access 0
local 0 transaccess 2
sslcli 0 certfile "certcli1.pem"
sslcli 0 keyfile "privcli1.pem"
sslcli 0 verify 10
sslsvr 0 certfile "cert01.pem"
sslsvr 0 keyfile "privrsa.pem"
ssh 0 hostkey1 "privSSH.pem"
ssh 0 nb_listen 5
ssh 0 v1 OFF
ovpn 0 descr "toServer"
ovpn 0 dest "37.84.199.193"
ovpn 0 autoup ON
ovpn 0 ipanon ON
ovpn 0 pullip ON
ovpn 0 pullroute ON
ovpn 0 pingint 10
ovpn 0 pingto 120
ovpn 0 cipher "AES-256-CBC"
```

```
cloud 0 ssl ON

Power Up Profile: 0
OK
```

```
Command: id
Command result

Digi TransPort WR11-U900-DE1-XX Ser#:319120
Software Build Ver5.2.18.3.  May 23 2017 09:43:42  1W
ARM Bios Ver 7.61u v46 360MHz B987-M995-F80-O0,0 MAC:00042d04de90
Async Driver              Revision: 1.19  Int clk
Ethernet Driver           Revision: 1.11
Firewall                  Revision: 1.0
EventEdit                 Revision: 1.0
Timer Module              Revision: 1.1
(B)USBHOST                Revision: 1.0
L2TP                      Revision: 1.10
PPTP                      Revision: 1.00
TACPLUS                   Revision: 1.00
MultiTX                   Revision: 1.00
LAPB                      Revision: 1.12
X25 Layer                 Revision: 1.19
MACRO                     Revision: 1.0
PAD                       Revision: 1.4
X25 Switch                Revision: 1.7
TPAD Interface            Revision: 1.12
TELITUPD                  Revision: 1.0
SCRIBATSK                 Revision: 1.0
BASTSK                    Revision: 1.0
PYTHON                    Revision: 1.0
CLOUDSMS                  Revision: 1.0
TCP (HASH mode)           Revision: 1.14
TCP Utils                 Revision: 1.13
PPP                       Revision: 5.2
WEB                       Revision: 1.5
SMTP                      Revision: 1.1
FTP Client                Revision: 1.5
FTP                       Revision: 1.4
IKE                       Revision: 1.0
PollANS                   Revision: 1.2
PPPOE                     Revision: 1.0
BRIDGE                    Revision: 1.1
MODEM CC (Telit 3G)       Revision: 5.2
FLASH Write               Revision: 1.2
Command Interpreter       Revision: 1.38
SSLCLI                    Revision: 1.0
OSPF                      Revision: 1.0
BGP                       Revision: 1.0
QOS                       Revision: 1.0
```

```
PWRCTRL                   Revision: 1.0
RADIUS Client             Revision: 1.0
SSH Server                Revision: 1.0
SCP                       Revision: 1.0
SSH Client                Revision: 1.0
CERT                      Revision: 1.0
LowPrio                   Revision: 1.0
Tunnel                    Revision: 1.2
OVPN                      Revision: 1.2
TEMPLOG                   Revision: 1.0
QDL                       Revision: 1.0
OK
```

## 6.2 OpenVPN Server configuration (WR21)

The config.da0 file and the hardware/firmware used on Open VPN Server for the purpose of this Application Note are shown below:

```
Command: config c show
Command result

eth 0 IPaddr "172.16.0.1"
lapb 0 ans OFF
lapb 0 tinact 120
lapb 1 tinact 120
lapb 3 dtemode 0
lapb 4 dtemode 0
lapb 5 dtemode 0
lapb 6 dtemode 0
ip 0 cidr ON
route 0 descr "toClient1LAN"
route 0 IPaddr "172.16.1.0"
route 0 ll_ent "OVPN"
def_route 0 ll_ent "ppp"
def_route 0 ll_add 1
dhcp 0 IPmin "192.168.1.100"
dhcp 0 respdelms 500
dhcp 0 mask "255.255.255.0"
dhcp 0 gateway "192.168.1.1"
dhcp 0 DNS "192.168.1.1"
sntp 0 server "time.devicecloud.com"
dyndns 0 ifent "default"
ppp 0 timeout 300
ppp 1 name "W-WAN (LTE)"
ppp 1 phonenum "*98*1#"
ppp 1 IPaddr "0.0.0.0"
ppp 1 timeout 0
ppp 1 use_modem 1
ppp 1 aodion 1
ppp 1 autoassert 1
ppp 1 r_chap OFF
ppp 3 defpak 16
ppp 4 defpak 16
web 0 prelogin_info ON
web 0 showgswiz ON
modemcc 0 info_asy_add 4
modemcc 0 init_str "+CGQREQ=1"
modemcc 0 init_str1 "+CGQMIN=1"
modemcc 0 apn "internet.t-d1.de"
modemcc 0 link_retries 10
modemcc 0 stat_retries 30
modemcc 0 sms_interval 1
modemcc 0 sms_access 1
modemcc 0 sms_concat 0
modemcc 0 init_str_2 "+CGQREQ=1"
modemcc 0 init_str1_2 "+CGQMIN=1"
modemcc 0 apn_2 "Your.APN.goes.here"
modemcc 0 link_retries_2 10
modemcc 0 stat_retries_2 30
modemcc 0 sms_access_2 1
modemcc 0 sms_concat_2 0
ana 0 l1on ON
ana 0 lapdon 0
ana 0 asyon 1
ana 0 logsize 45
cmd 0 unitid "ss%s>"
cmd 0 cmdnua "99"
cmd 0 hostname "digi.router"
cmd 0 asyled_mode 2
cmd 0 tremto 1200
cmd 0 rcihttp ON
user 0 access 0
user 1 name "username"
user 1 epassword "KD5lSVJDVVg="
user 1 access 0
user 2 access 0
user 3 access 0
user 4 access 0
user 5 access 0
user 6 access 0
user 7 access 0
user 8 access 0
user 9 access 0
local 0 transaccess 2
sslcli 0 verify 10
sslsvr 0 certfile "certserv.pem"
sslsvr 0 keyfile "privserv.pem"
ssh 0 hostkey1 "privSSH.pem"
ssh 0 nb_listen 5
ssh 0 v1 OFF
ovpn 0 descr "ToClient1"
ovpn 0 IPaddr "192.168.0.1"
ovpn 0 server ON
ovpn 0 puship "172.16.0.0"
ovpn 0 pushmask "255.255.255.0"
ovpn 0 pingint 10
ovpn 0 pingto 120
ovpn 0 cipher "AES-256-CBC"
cloud 0 ssl ON

Power Up Profile: 0
```

```
Digi TransPort WR21-U22B-DE1-XX Ser#:237416
Software Build Ver5.2.18.3.  May 23 2017 09:43:46  WW
ARM Bios Ver 7.61u v43 454MHz B987-M995-F80-O8140,0 MAC:00042d039f68
Async Driver              Revision: 1.19  Int clk
Ethernet Port Isolate Driver Revision: 1.11
Firewall                  Revision: 1.0
EventEdit                 Revision: 1.0
Timer Module              Revision: 1.1
(B)USBHOST                Revision: 1.0
L2TP                      Revision: 1.10
PPTP                      Revision: 1.00
TACPLUS                   Revision: 1.00
MODBUS                    Revision: 0.00
RealPort                  Revision: 0.00
MultiTX                   Revision: 1.00
LAPB                      Revision: 1.12
X25 Layer                 Revision: 1.19
MACRO                     Revision: 1.0
PAD                       Revision: 1.4
X25 Switch                Revision: 1.7
V120                      Revision: 1.16
TPAD Interface            Revision: 1.12
GPS                       Revision: 1.0
TELITUPD                  Revision: 1.0
SCRIBATSK                 Revision: 1.0
BASTSK                    Revision: 1.0
PYTHON                    Revision: 1.0
CLOUDSMS                  Revision: 1.0
TCP (HASH mode)           Revision: 1.14
TCP Utils                 Revision: 1.13
PPP                       Revision: 5.2
WEB                       Revision: 1.5
SMTP                      Revision: 1.1
FTP Client                Revision: 1.5
FTP                       Revision: 1.4
IKE                       Revision: 1.0
PollANS                   Revision: 1.2
PPPOE                     Revision: 1.0
BRIDGE                    Revision: 1.1
MODEM CC (Huawei LTE)     Revision: 5.2
FLASH Write               Revision: 1.2
Command Interpreter       Revision: 1.38
SSLCLI                    Revision: 1.0
OSPF                      Revision: 1.0
BGP                       Revision: 1.0
QOS                       Revision: 1.0
PWRCTRL                   Revision: 1.0
RADIUS Client             Revision: 1.0
SSH Server                Revision: 1.0
SCP                       Revision: 1.0
SSH Client                Revision: 1.0
CERT                      Revision: 1.0
LowPrio                   Revision: 1.0
Tunnel                    Revision: 1.2
```

```
OVPN                      Revision: 1.2
TEMPLOG                   Revision: 1.0
QDL                       Revision: 1.0
OK
```