Application Note

OpenVPN Client with Username & Password for RobustOS

Doc Type:	**Application Note**
Version:	**v.1.0.0**
Date:	**2016-12-26**
Status:	**Confidential**
Doc ID:	**RT_AN005_OpenVPN Client with Username & Password for RobustOS_v.1.0.0**
Author:	**Singson Chen**

Contents

Chapter 1 Introduction 2
1.1 Overview 2
1.2 Assumptions 2
1.3 Rectifications 2
1.4 Version 3
Chapter 2 Topology 4
Chapter 3 Configuration 5
3.1 OpenVPN Installation on Windows 5
3.2 Certificates Management for OpenVPN 9
3.2.1 OpenVPN Certificate 9
3.2.2 Generate OpenVPN Certificates for Server and Multiple Clients 10
3.2.3 Manage the Username/Password Script for OpenVPN 16
3.3 Configuration for Windows OpenVPN Server 17
3.3.1 Open and Edit server.ovpn file 17
3.4 R2000 Configuration 24
3.4.1 Configure Link Management 24
3.4.2 Configure Cellular WAN 25
3.4.3 Configure IP Address of LAN 27
3.4.4 Configure OpenVPN Client 29
Chapter 4 Testing 34
4.1 Network Status 34
4.2 Running the OpenVPN Software in Windows OS 35
4.3 VPN Status and Communication 36
4.4 Testing at OpenVPN Server 37
4.5 Event/Log 39
Chapter 5 Appendix 42
5.1 Firmware Version 42

Chapter 1 Introduction

1.1 Overview

RobustOS (hereinafter referred to as “the ROS”) is a new operating system for Robustel's IoT gateway released in 2015. It is a modular and open software platform which could support third party development based on SDK/API; meanwhile, it supports different routing and VPN protocols for different application scenarios. The configuration web interface of the ROS is a little different from the existing old platform of R3000 series.

OpenVPN is an open-source project with GPL license agreement, completing solution characteristics of SSL VPN and providing solutions which contain site-to-site subnet, WIFI security and enterprise remote access. OpenVPN permits to establish VPN by using pre-shared key, third party certificate or username/password for authentication.

This application note has been written for customer with a good understanding of Robustel products and a basic experience of OpenVPN. It shows customer how to configure and test the OpenVPN between the R2000 and Windows OpenVPN server through the cellular network.

This application note applies to the ROS firmware of R2000 and R3000. However, the followings will take R2000 as an example

1.2 Assumptions

The features of OpenVPN have been fully tested and this application note has been written by technically competent engineer who is familiar with the Robustel products and the application requirements.
This application note is based on:

- Product Model: Robustel GoRugged R2000, an industrial cellular VPN router
- Firmware Version: R2000_ROS_ v2.0.6
- Required Software: OpenVPN 2.2.2
- Configuration: This application note assumes the Robustel products are set to factory default. Most of configuration steps are only shown if they are different from the factory default settings.

  R2000’s cellular WAN could be dynamic or static, public or “private with NAT” IP address. OpenVPN is based on certificate, here we use username & password for authentication. It needs to install an OpenVPN Easy-RSA certificate created & signed by certificate authority on your PC. Any Easy-RSA is free and easy-to-use.

1.3 Rectifications

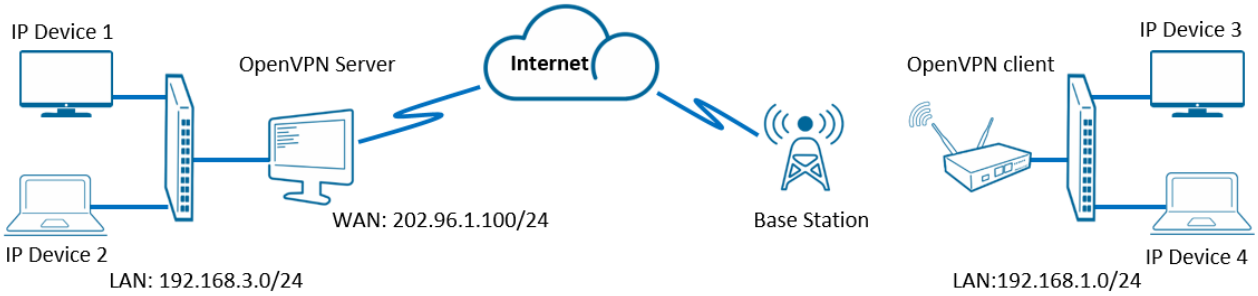
Appreciate for corrections or rectifications to this application note, and if there are any request for new application notes please email to: support@robustel.com.

1.4 Version

Updates between document versions are cumulative. Therefore, the latest document version contains all updates made to previous versions.

Release Date	Doc Version	Change Description
2016-12-23	v.1.0.0	Initial Release

Chapter 2 Topology



1. The PC runs as an OpenVPN server with a fixed public IP address and opens a specified port of OpenVPN.
2. Another R2000 works on wireless network with any kind of IP which can access the Internet and ping the WAN IP address of OpenVPN server successfully.
3. OpenVPN tunnel is established between the server and client. Multiple OpenVPN clients can connect to the same OpenVPN server.

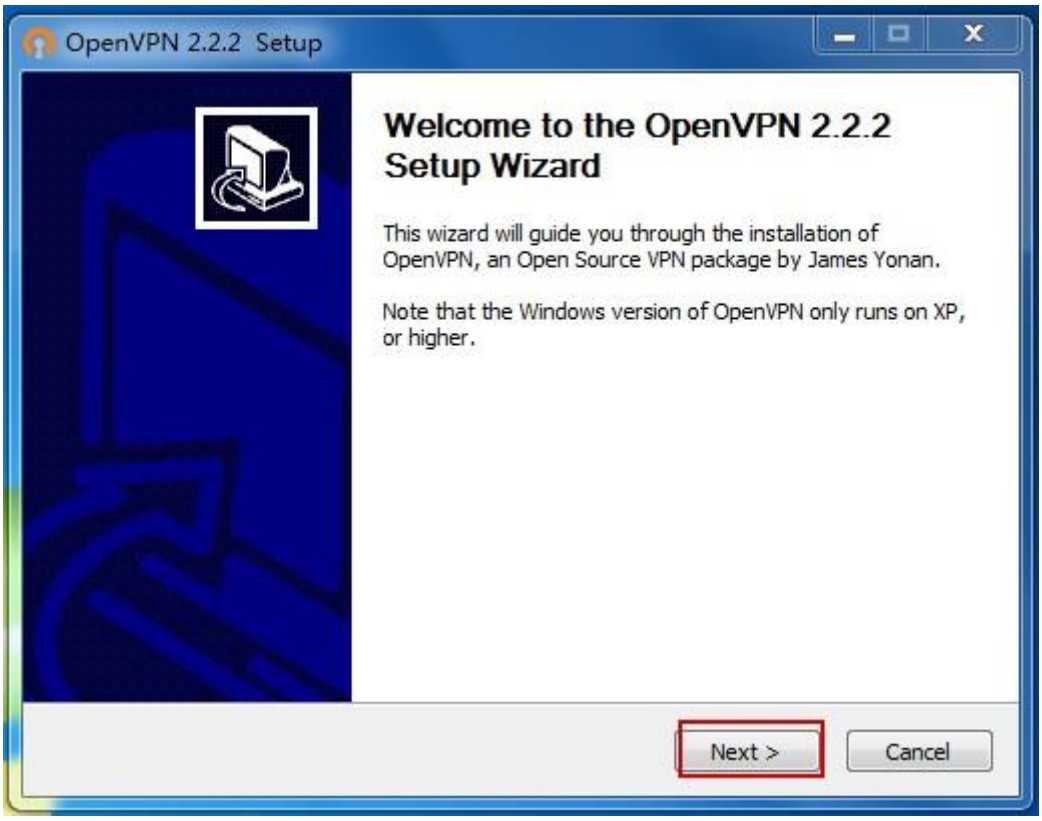
Note: *If OpenVPN server behind a Gateway Router, the Router must open the 1194 port and set up port forwarding to the internal server. 1194 is the default port number for OpenVPN negotiation.*

Chapter 3 Configuration

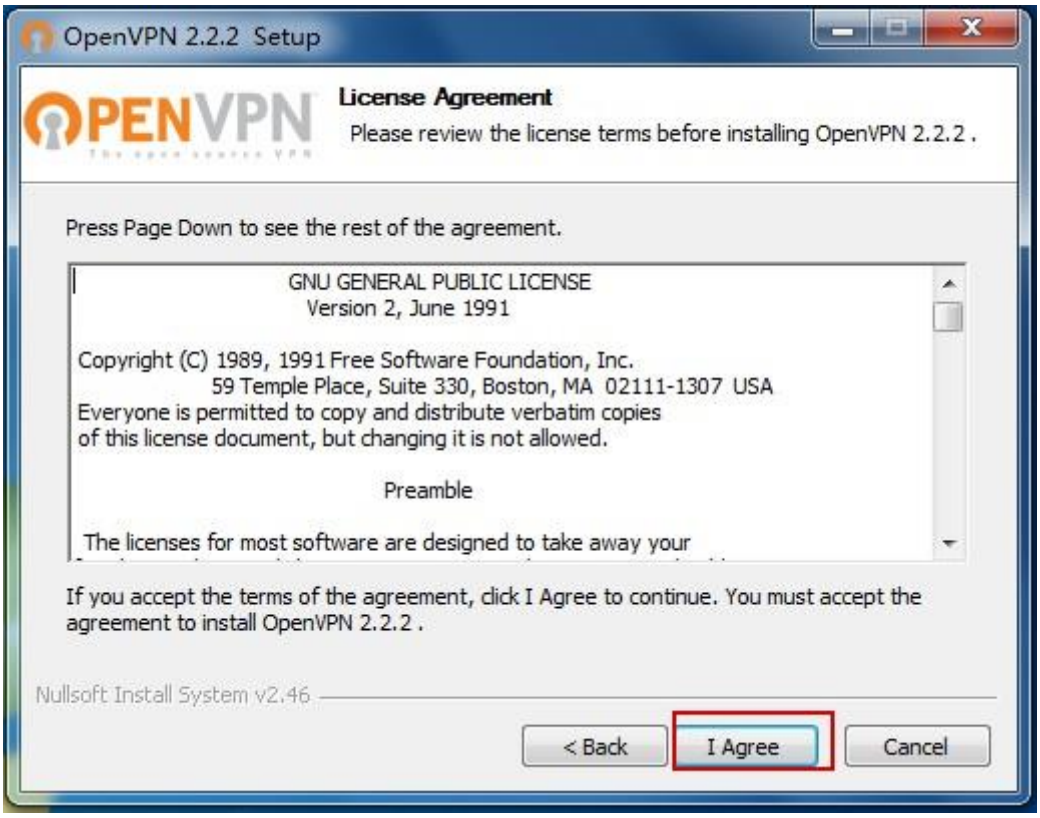
3.1 OpenVPN Installation on Windows

This step should be done on the PC which used to create certificates (the PC also can be an OpenVPN server).
Go to **http://openvpn.net/index.php** for download.

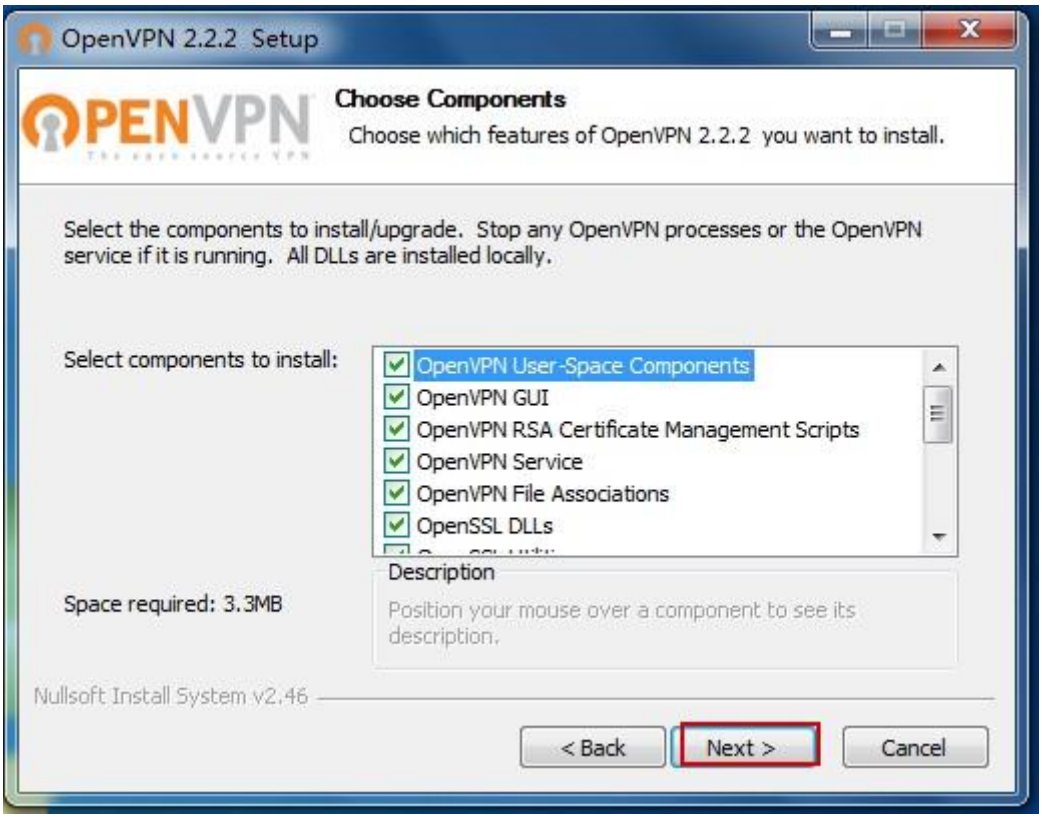
1. Download the release of Windows installer, and run the installation program.



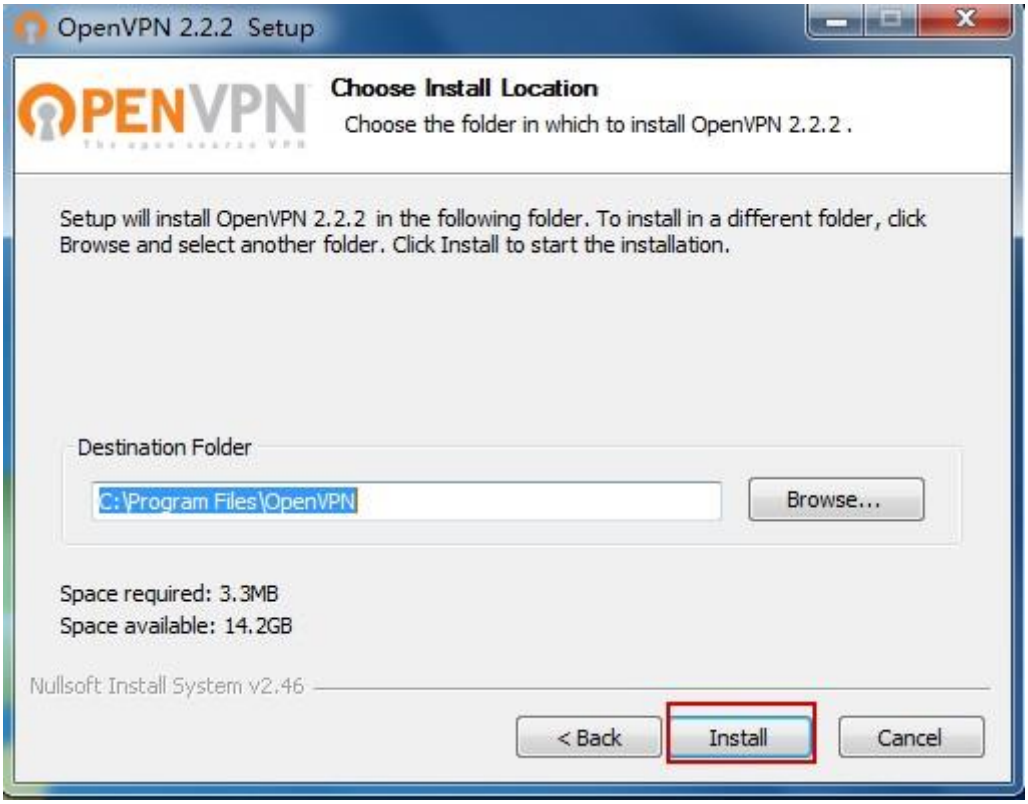
2. Agree the **License Agreement** as below.



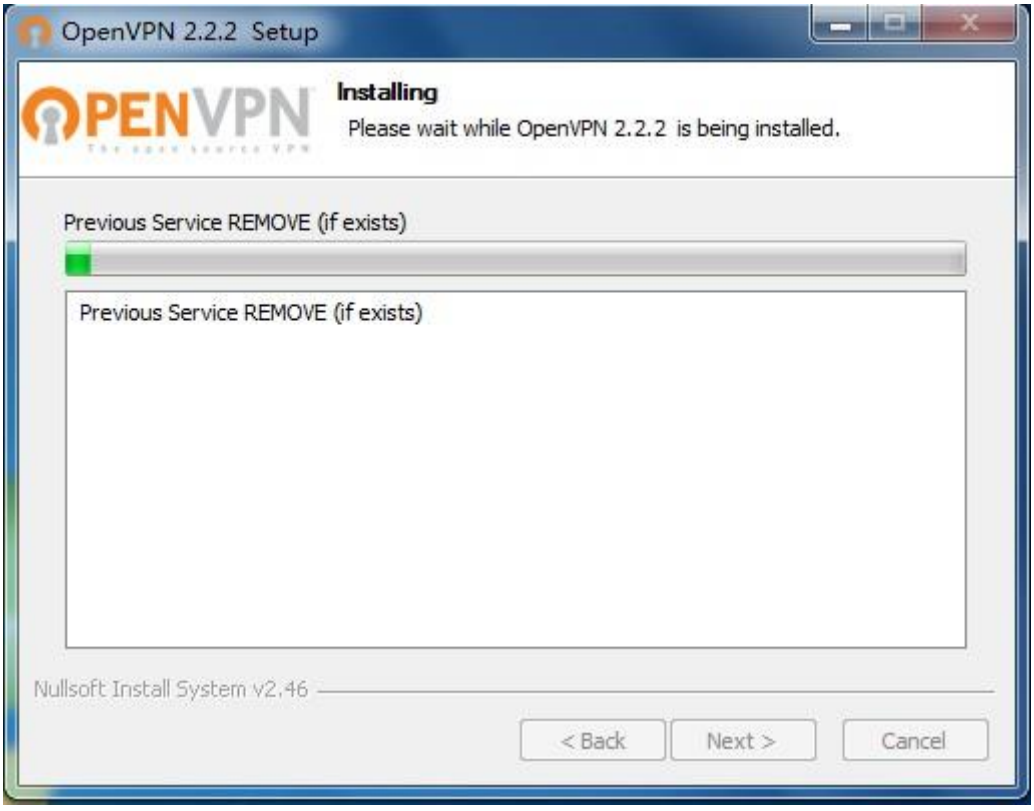
3. Select all options by default.



4. Select the installation path or save in default Destination Folder.

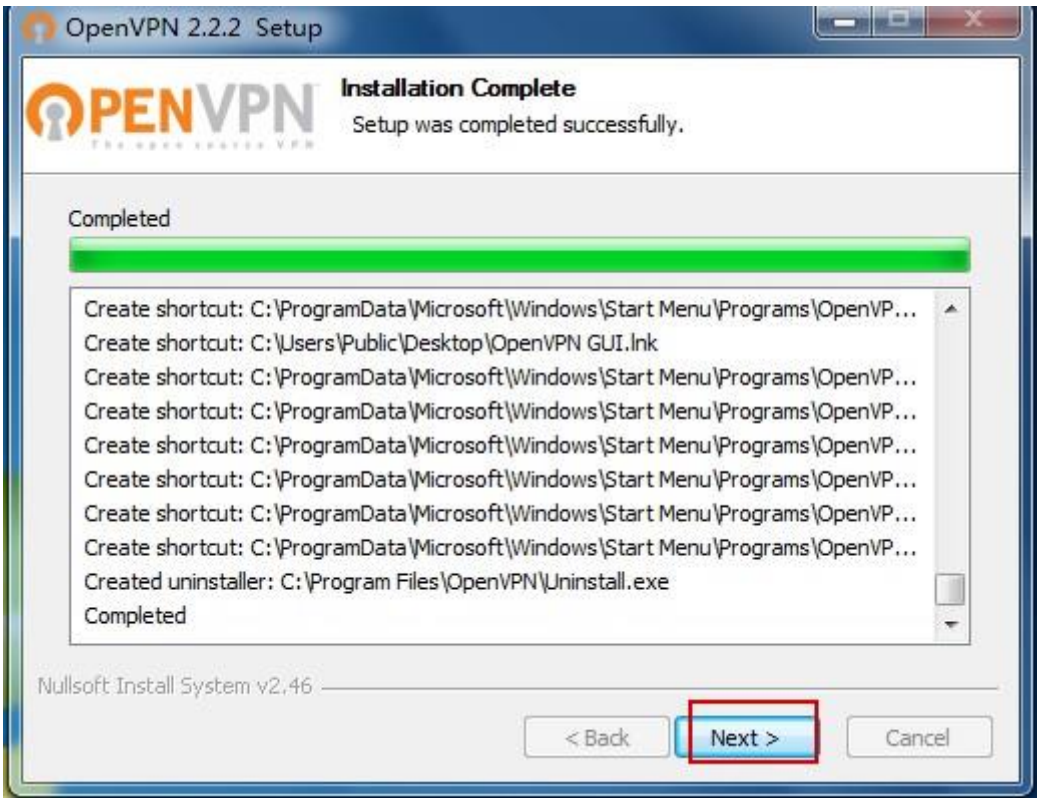


5. Wait while OpenVPN 2.2.2 is being installed.



6. Agree to install the TAP-Win32 network adapter.

7. Complete the setup.



8. Click **Finish** to complete all installation.

3.2 Certificates Management for OpenVPN

3.2.1 OpenVPN Certificate

The first step to create an OpenVPN is to establish a PKI (Public Key Infrastructure). The PKI consists of:

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

OpenVPN supports bidirectional authentication based on certificates, which means client must authenticate the server's certificate before the tunnel is established, and vice versa.

Both server and client will authenticate firstly the presented certificate signed by the master certificate authority (CA), and then test information in the now-authenticated certificate header, such as certificate common name or certificate type (client or server).

The features of OpenVPN:

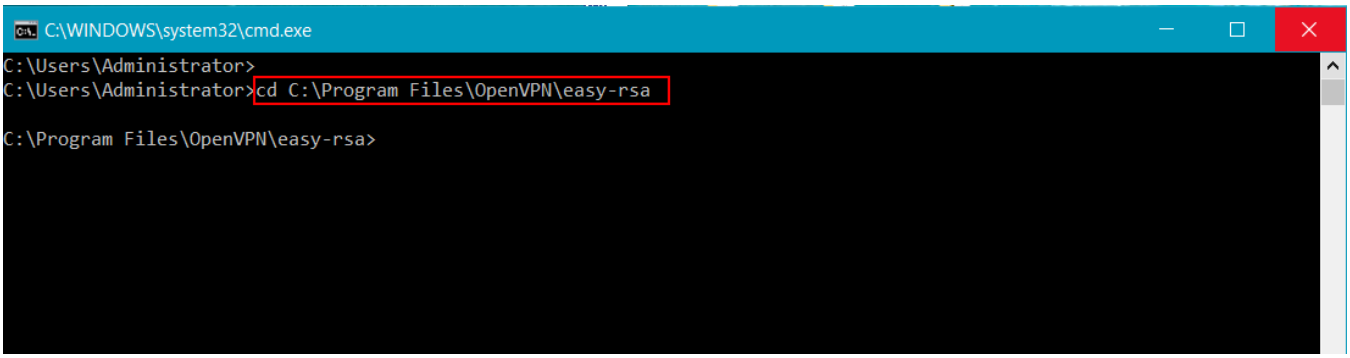
- The server only concerns its own certificate/key -- it has no need to know the individual certificates of each client.
- The server will only accept clients whose certificates is signed by the master CA certificate. Because the server can perform this signature verification without accessing the CA private key itself. We could place the CA key (the most sensitive key in the entire PKI) on a completely different machine with no Internet access.

- If a private key is compromised and not secure any more, it could be disqualified by using CRL (Certificate Revocation List). The CRL disables the compromised certificates, and does not need to rebuilt the entire PKI.
- The server can enforce client-specific access rights based on client's certificates, such as the Common Name.

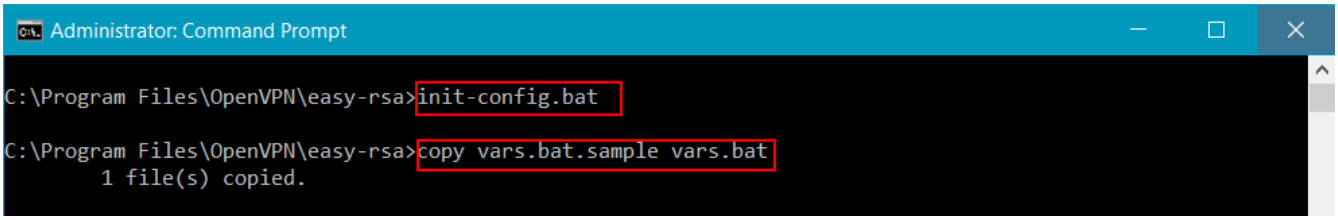
3.2.2 Generate OpenVPN Certificates for Server and Multiple Clients

In this section we will generate one master CA certificate/key, one server certificate/key and one client certificate/key.

1. For PKI management, we could pre-set the scripts bundled with OpenVPN. On Windows, open a command line interface and **cd** to **C:\Program Files\OpenVPN\easy-rsa**..



2. Run the **init-config.bat** to copy configuration files to **vars.bat** (this command would overwrite the previous vars.bat and openssl.cnf files).

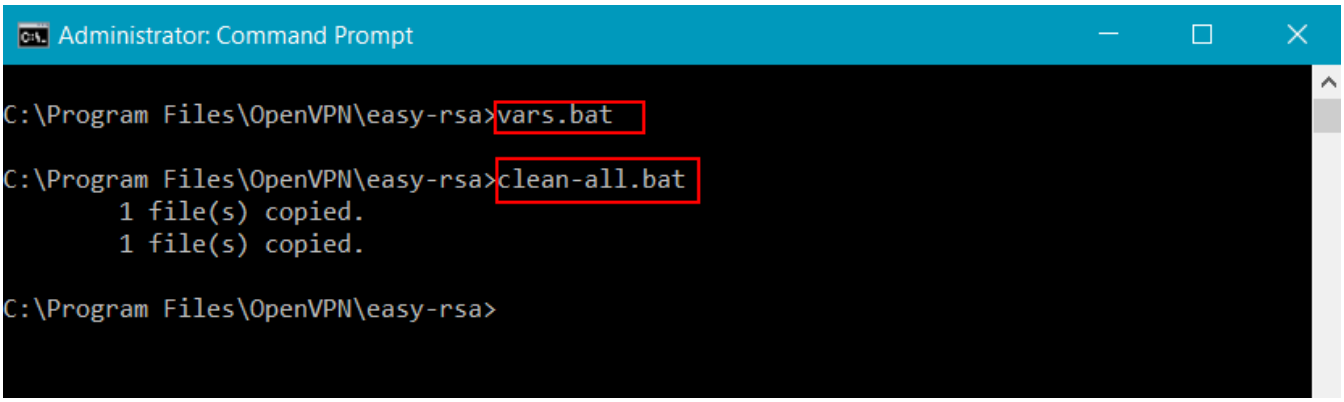


3. Edit the **vars.bat** and set the KEY_COUNTRY, KEY_PROVINCE, KEY_CITY, KEY_ORG, KEY_EMAIL parameters and so on.

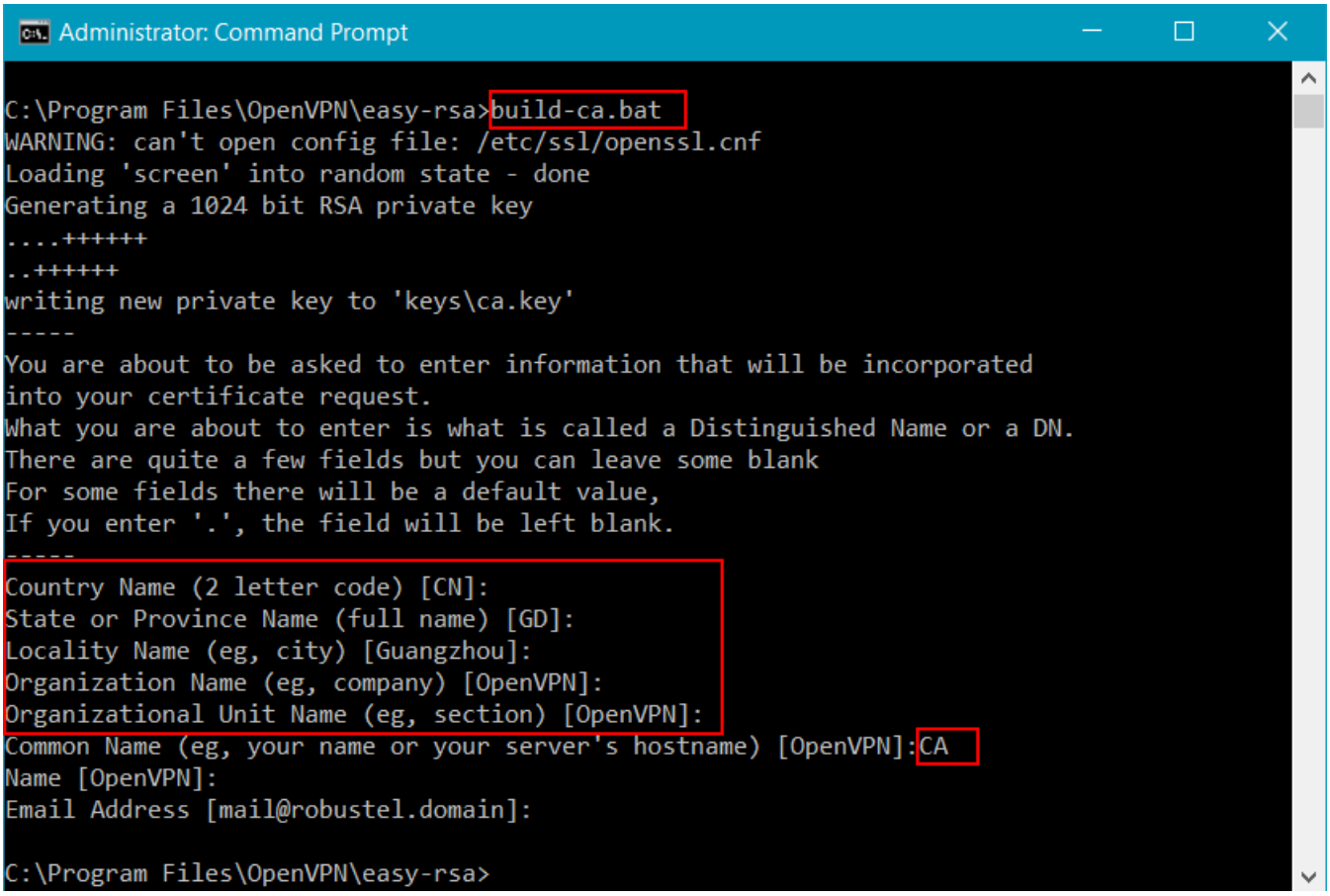
   Note: The parameters enter without any space between them.

```
@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=CN
set KEY_PROVINCE=GD
set KEY_CITY=Guangzhou
set KEY_ORG=OpenVPN
set KEY_EMAIL=mail@robustel.domain
set KEY_CN=OpenVPN
set KEY_NAME=OpenVPN
set KEY_OU=OpenVPN
set PKCS11_MODULE_PATH=changeme
set PKCS11_PIN=1234
```

4. Run the following commands to initialize the environment.

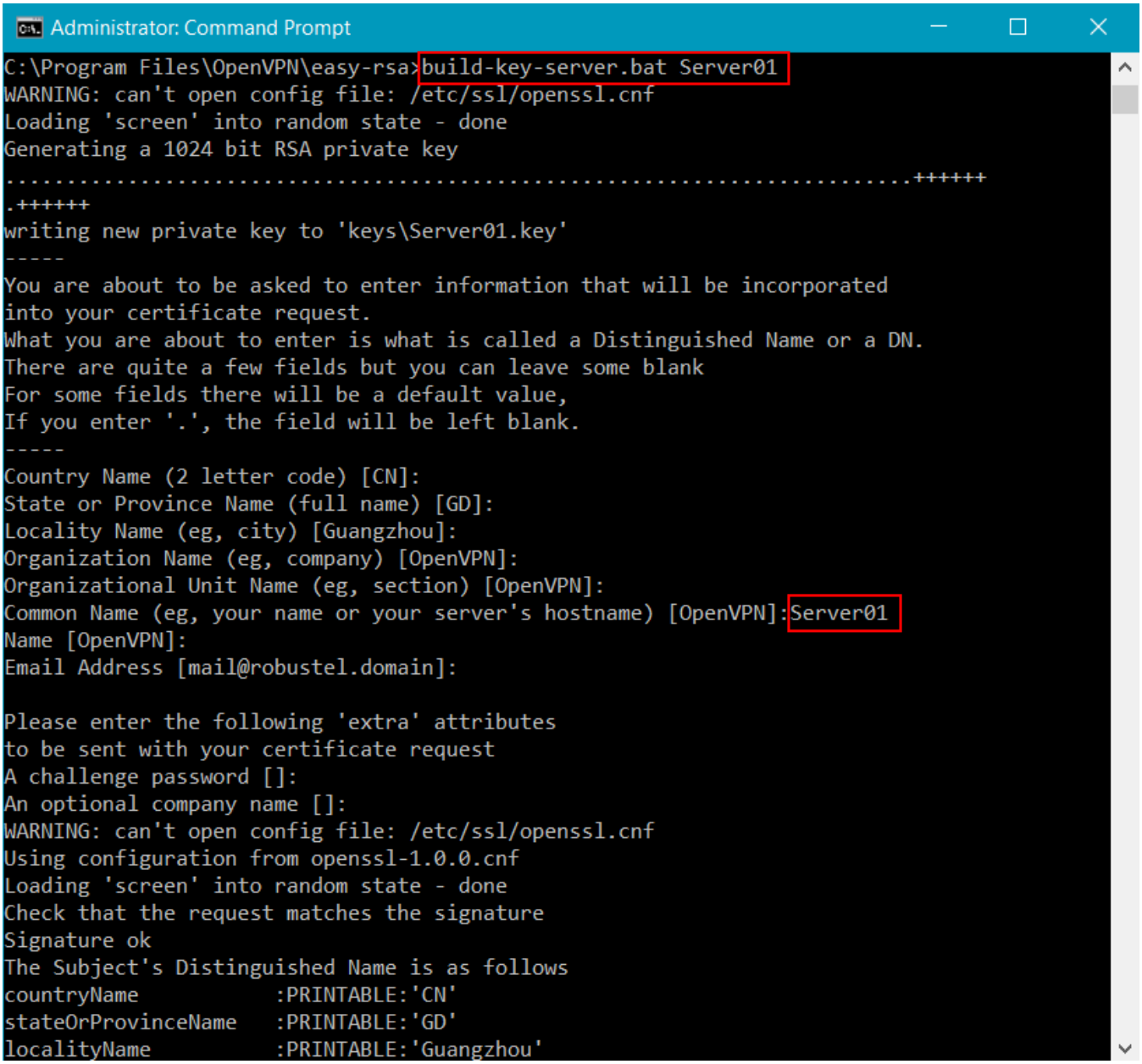


5. The command (**build-ca.bat**) will build the certificate authority(CA) certificate and the private key by invoking the interactive openssl command.



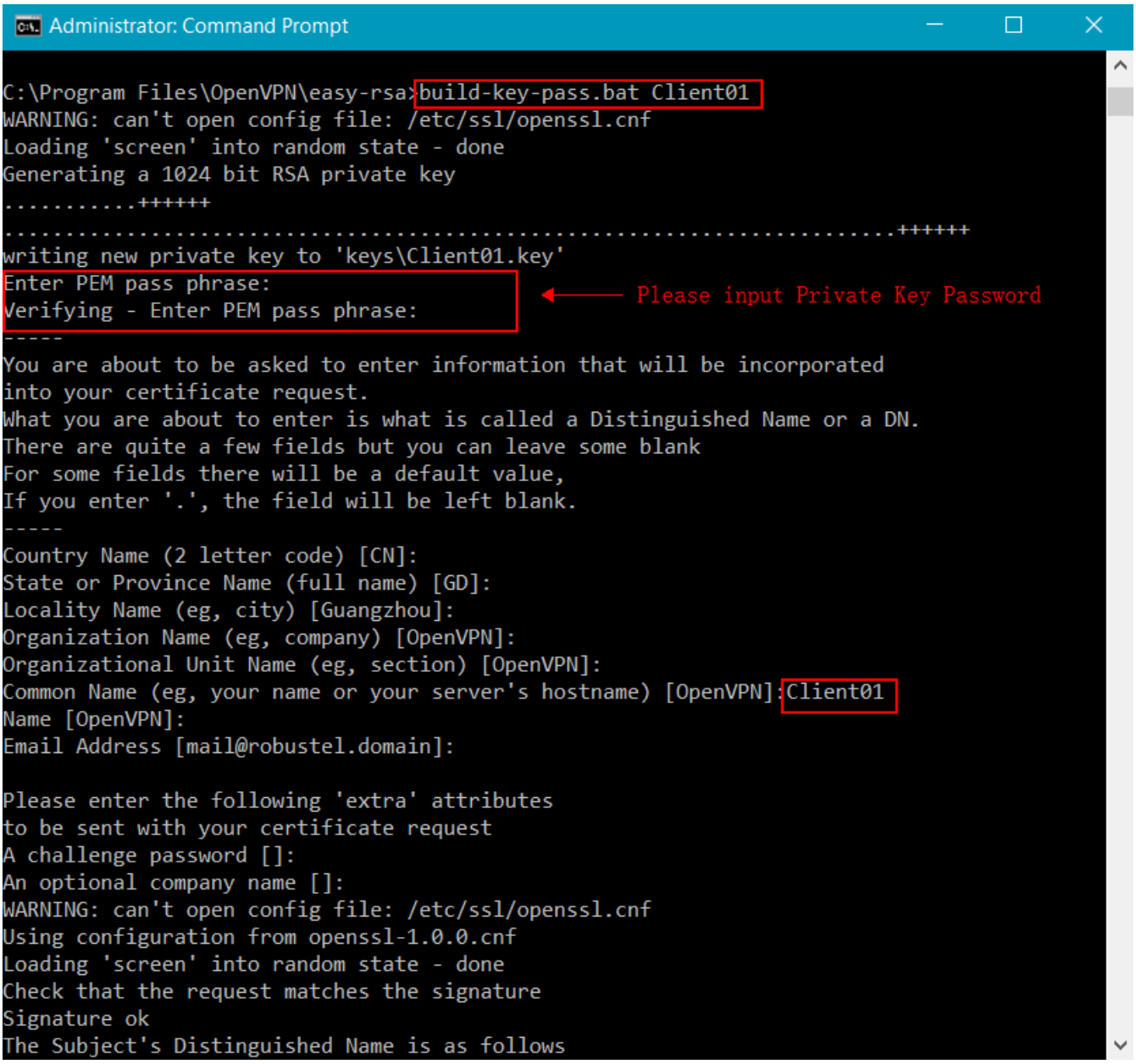
Note: *In the above sequence, most of queried parameters were defaulted to the values set in the vars.bat file. The only parameter which must be explicitly entered is the Common Name.*

6. Generate a certificate and a private key for server by using **build-key-server.bat Server01**. Enter **Server01** when the Common Name is queried.



***Note**: **Server01** in "**build-key-server.bat Server01**" is the file name of the certificate (the name of public key and private key).*

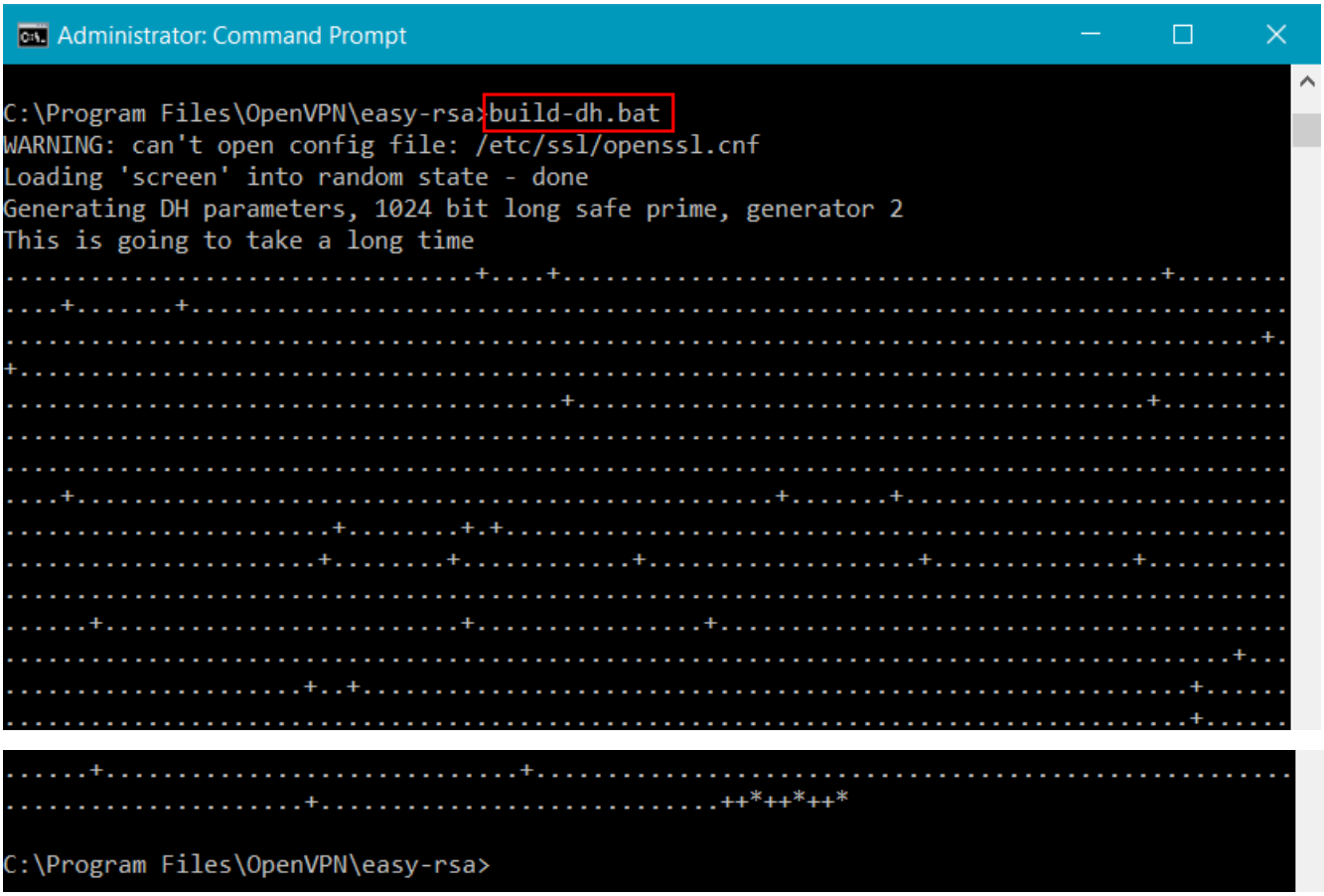
7. Generate a certificate and a private key for client by using **build-key-pass.bat Client01.** Kindly note that **pass phrase** is generated as followings. It will be necessary to help the key authentication in OpenVPN client setting. Enter **Client01** when the Common Name is queried.



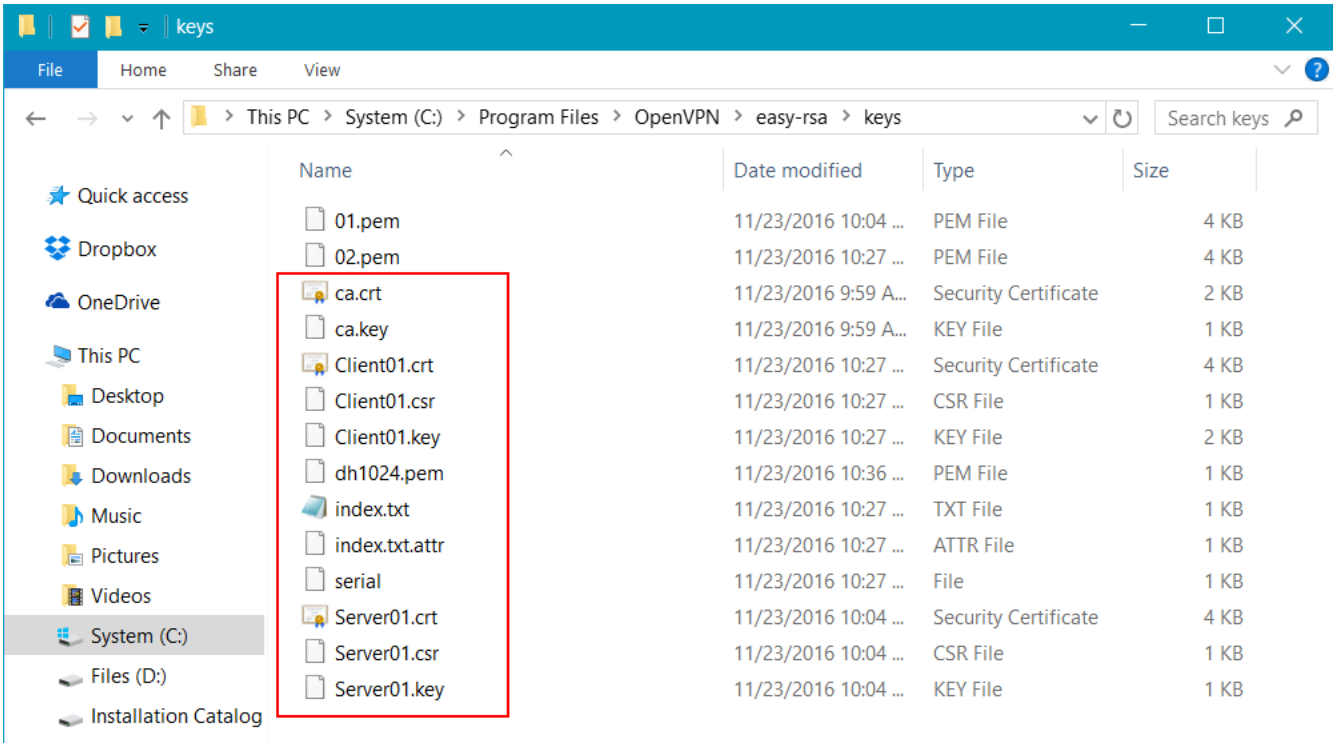
```
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'CN'
stateOrProvinceName   :PRINTABLE:'GD'
localityName          :PRINTABLE:'Guangzhou'
organizationName      :PRINTABLE:'OpenVPN'
organizationalUnitName:PRINTABLE:'OpenVPN'
commonName            :PRINTABLE:'Client01'
name                  :PRINTABLE:'OpenVPN'
emailAddress          :IA5STRING:'mail@robustel.domain'
Certificate is to be certified until Nov 21 02:27:51 2026 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>
```

***Note**: **Client01** in "**build-key-pass.bat Client01**" is the file name of the certificate(the name of public key and private key). **Always use a unique common name for each client**.*

8. Generate Diffie Hellman parameters.



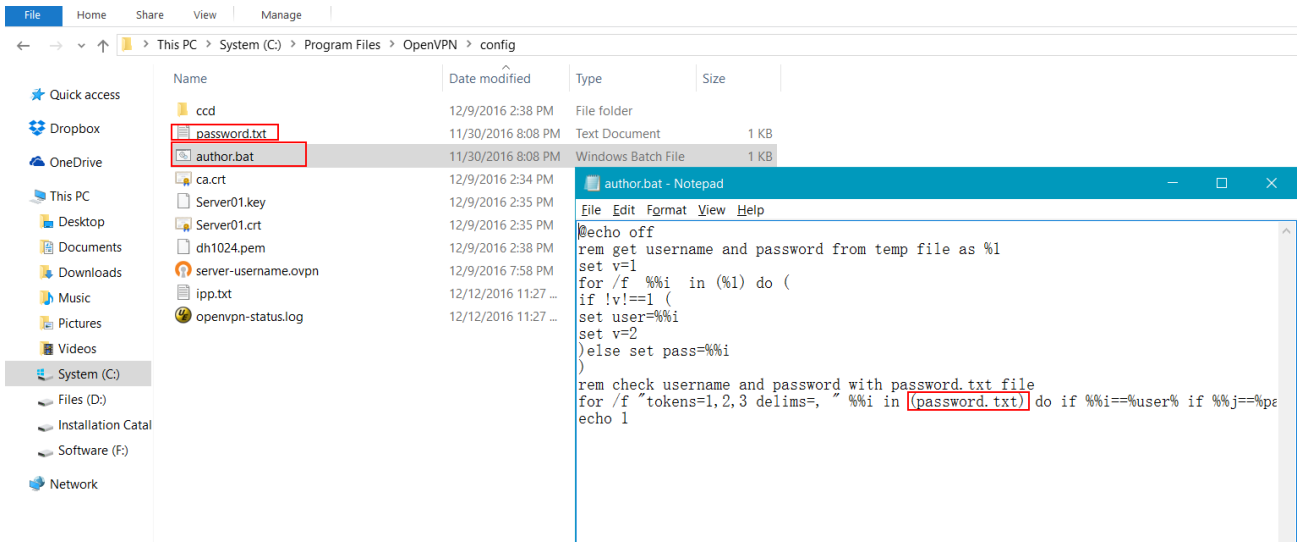
9. Now, you can view the latest generated keys and certificates in the easy-rsa\keys subdirectory.



3.2.3 Manage the Username/Password Script for OpenVPN

1. Generate one Notepad file and rename it as "**author.bat**".
   Path: C:\Program Files\OpenVPN\config

```
@echo off
rem get username and password from temp file as %1
set v=1
for /f    %%i    in (%1) do (
if !v!==1 (
set user=%%i
set v=2
)else set pass=%%i
)
rem check username and password with password.txt file
for /f "tokens=1,2,3 delims=, " %%i in (password.txt) do if %%i==%user% if %%j==%pass% if %%k==1 exit /B 0
echo 1
```



Note: *Keep the default code of scripts, and* ***password.txt*** *is the file which has registered the multiple clients' username and password.*

2. Edit file for username and password.

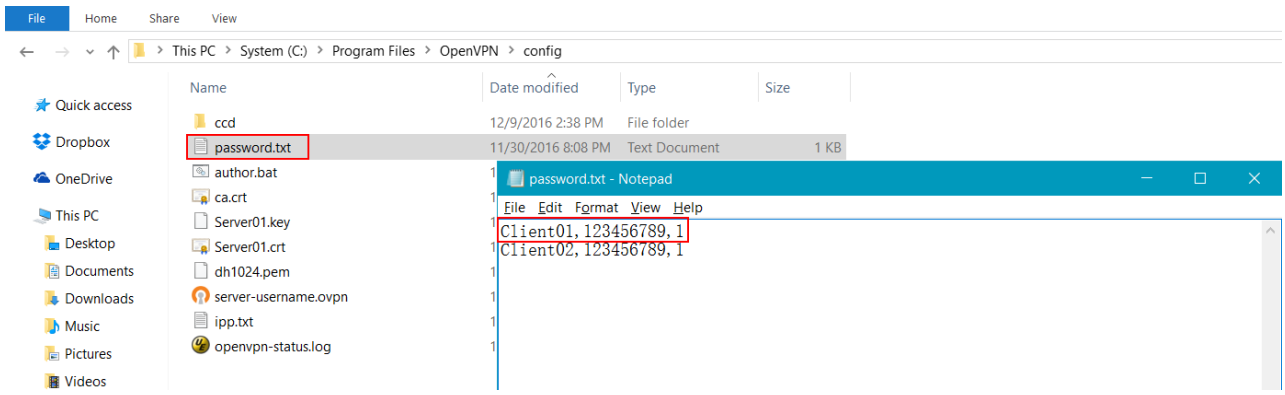
- In the configuration file and directory to create a new password.txt file. Add the content with the following format.

  Use ", "as a delimiter, format:

  The Common name, password, whether to enable (1, enable, 0, disabled)

  User1, passowrd1, 1

  User2, password2, 0

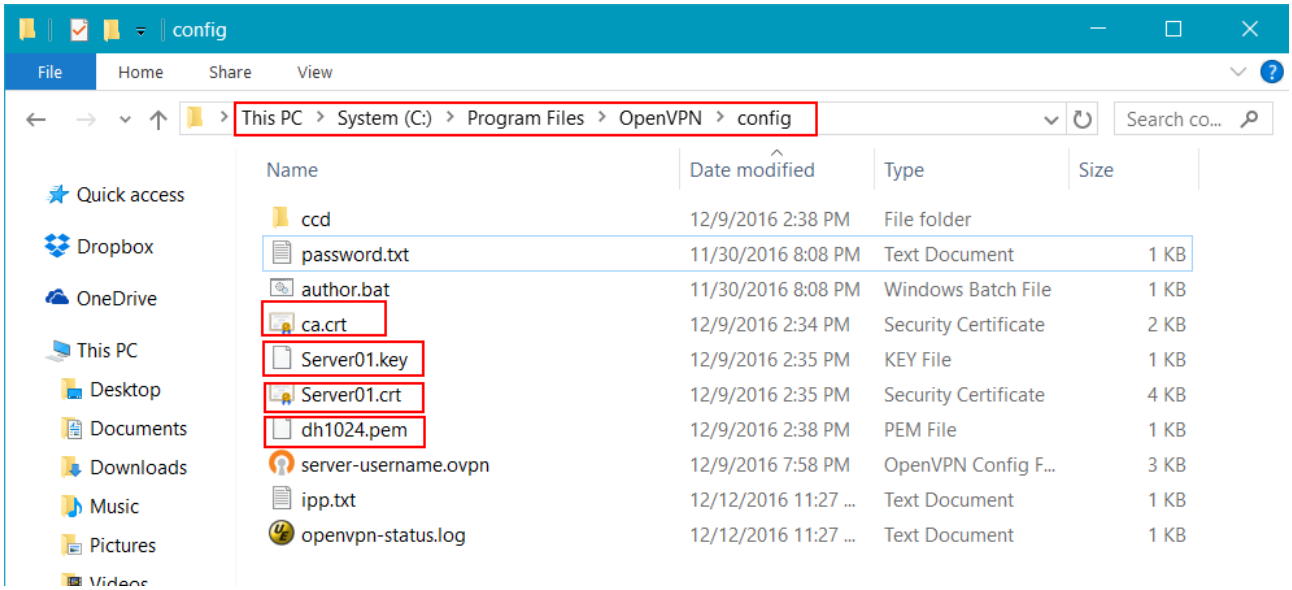


3.3 Configuration for Windows OpenVPN Server

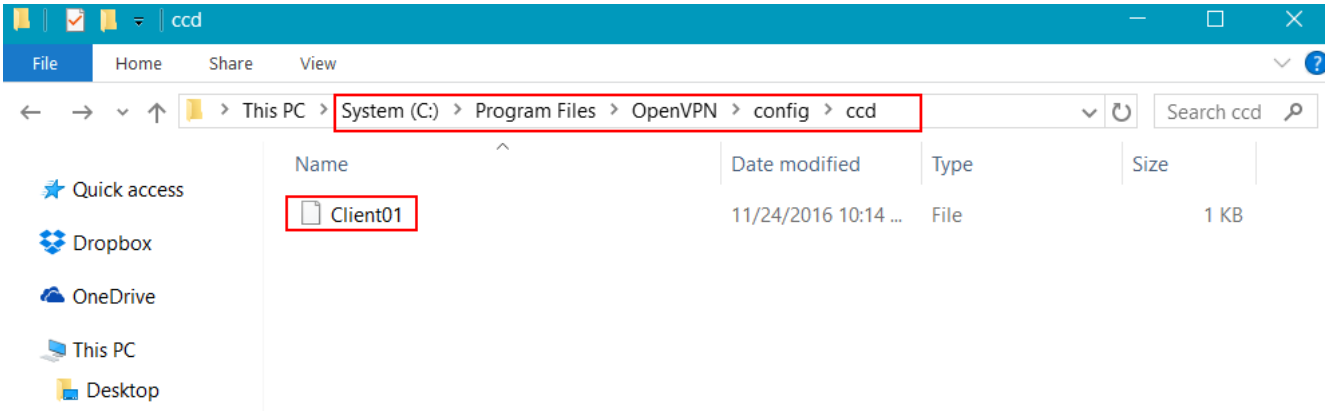
The following steps explain the configuration that needs to be done on the Windows OpenVPN Server.

3.3.1 Open and Edit server.ovpn file

1. Copy the required files to the configuration directory of OpenVPN server.
   Path: *C:\Program Files\OpenVPN\config*

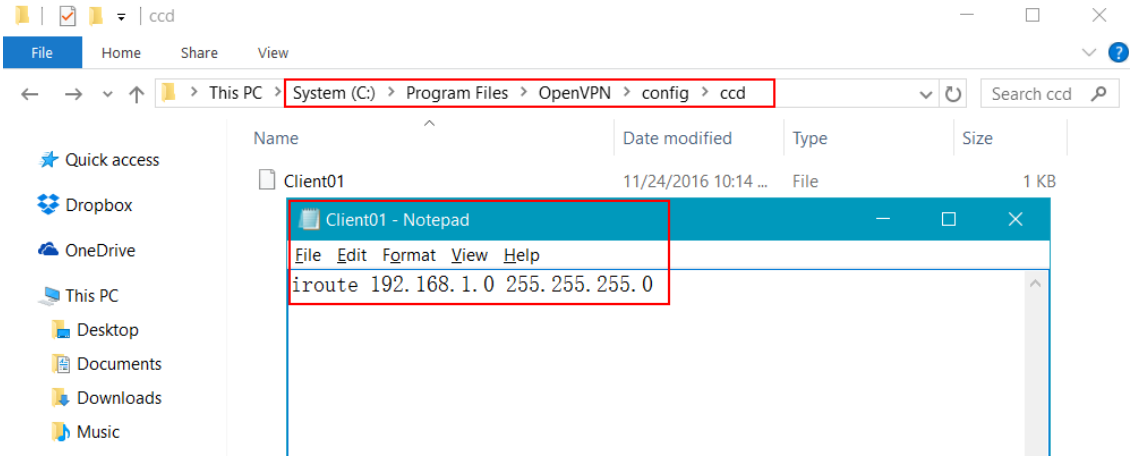


2. Assign specific IP addresses to specific clients or use the subdirectory “ccd” as the client-specific configuration files if a connecting client has a private subnet behind which should also have VPN access.
Add a new folder named “**ccd**”, create a new notepad and rename it without suffix.



Note: *“Client01” is the Common Name pre-defined in the certificate but not the file name.*

3. Edit and save the notepad.



Note: *192.168.1.0/24 is the subnet behind R2000.*

4. The configuration of the **server.ovpn**.
   Note: *The following contents marked as red have been changed from the sample configure defaults. And the extra comments are marked as blue. The server.ovpn file could be found in the Path: C:\Program Files\OpenVPN\sample-config.*

```
#########################################################
# Sample OpenVPN 2.0 config file for                    #
# multi-client server.                                  #
#                                                       #
# This file is for the server side                      #
# of a many-clients <-> one-server                      #
# OpenVPN configuration.                                #
#                                                       #
# OpenVPN also supports                                 #
# single-machine <-> single-machine                     #
# configurations (See the Examples page                 #
# on the web site for more info).                       #
#                                                       #
# This config should work on Windows                    #
# or Linux/BSD systems.    Remember on                  #
# Windows to quote pathnames and use                    #
# double backslashes, e.g.:                             #
# "C:\\Program Files\\OpenVPN\\config\\foo.key"         #
#                                                       #
# Comments are preceded with '#' or ';'                 #
#########################################################

# Which local IP address should OpenVPN
# listen on? (optional)
local 202.96.1.100

# OpenVPN working in Server mode,
# can support multiple client dynamic access at the same time.
mode server

# OpenVPN client could not provide the certificate
client-cert-not-required

# Login Name is the Common Name
username-as-common-name

# Activate login authentication, asks for the username and password
auth-user-pass-verify author.bat via-env
# Allow to execute external script
script-security 3 system
```

```
# Which TCP/UDP port should OpenVPN listen on?
# If you want to run multiple OpenVPN instances
# on the same machine, use a different port
# number for each one.    You will need to
# open up this port on your firewall.
port 1194

# TCP or UDP server?
;proto tcp
proto udp

# "dev tun" will create a routed IP tunnel,
# "dev tap" will create an ethernet tunnel.
# Use "dev tap0" if you are ethernet bridging
# and have precreated a tap0 virtual interface
# and bridged it with your ethernet interface.
# If you want to control access policies
# over the VPN, you must create firewall
# rules for the the TUN/TAP interface.
# On non-Windows systems, you can give
# an explicit unit number, such as tun0.
# On Windows, use "dev-node" for this.
# On most systems, the VPN will not function
# unless you partially or fully disable
# the firewall for the TUN/TAP interface.
;dev tap
dev tun

# Maximum Transmission Unit for OpenVPN tunnel.
# It is the identifier of the maximum size of packet,
# which is possible to transfer in a given environment.
tun-mtu 1500

# If you have fragmentation issues or misconfigured
# routers in the path which block Path MTU discovery,
# lower the TCP MSS and internally fragment non-TCP
# protocols.
fragment 1500

# SSL/TLS root certificate (ca), certificate
# (cert), and private key (key).    Each client
# and the server must have their own cert and
# key file.    The server and all clients will
# use the same ca file.
#
```

```
# See the "easy-rsa" directory for a series
# of scripts for generating RSA certificates
# and private keys.  Remember to use
# a unique Common Name for the server
# and each of the client certificates.
#
# Any X509 key management system can be used.
# OpenVPN can also use a PKCS #12 formatted key file
# (see "pkcs12" directive in man page).
ca ca.crt
cert Server01.crt
key Server01.key  # This file should be kept secret

# Diffie hellman parameters.
# Generate your own with:
#   openssl dhparam -out dh1024.pem 1024
# Substitute 2048 for 1024 if you are using
# 2048 bit keys.
dh dh1024.pem

# Configure server mode and supply a VPN subnet
# for OpenVPN to draw client addresses from.
# The server will take 10.8.0.1 for itself,
# the rest will be made available to clients.
# Each client will be able to reach the server
# on 10.8.0.1. Comment this line out if you are
# ethernet bridging. See the man page for more info.
server 10.8.0.0 255.255.255.0

# Maintain a record of client <-> virtual IP address
# associations in this file.  If OpenVPN goes down or
# is restarted, reconnecting clients can be assigned
# the same virtual IP address from the pool that was
# previously assigned.
ifconfig-pool-persist ipp.txt

# Configure server mode for ethernet bridging.
# Push routes to the client to allow it
# to reach other private subnets behind
# the server.  Remember that these
# private subnets will also need
# to know to route the OpenVPN client
# address pool (10.8.0.0/255.255.255.0)
# back to the OpenVPN server.
;push "route 192.168.10.0 255.255.255.0"
```

```
push "route 192.168.3.0 255.255.255.0"

# To assign specific IP addresses to specific
# clients or if a connecting client has a private
# subnet behind it that should also have VPN access,
# use the subdirectory "ccd" for client-specific
# configuration files (see man page for more info).

# EXAMPLE: Suppose the client
# having the certificate common name "Thelonious"
# also has a small subnet behind his connecting
# machine, such as 192.168.40.128/255.255.255.248.
# First, uncomment out these lines:
client-config-dir ccd
route 192.168.1.0 255.255.255.0

# The keepalive directive causes ping-like
# messages to be sent back and forth over
# the link so that each side knows when
# the other side has gone down.
# Ping every 10 seconds, assume that remote
# peer is down if no ping received during
# a 120 second time period.
keepalive 10 120

# For extra security beyond that provided
# by SSL/TLS, create an "HMAC firewall"
# to help block DoS attacks and UDP port flooding.
#
# Generate with:
#      openvpn --genkey --secret ta.key
#
# The server and each client must have
# a copy of this key.
# The second parameter should be '0'
# on the server and '1' on the clients.
;tls-auth ta.key 0 # This file is secret

# Select a cryptographic cipher.
# This config item must be copied to
# the client config file as well.
cipher BF-CBC               # Blowfish (default)
;cipher AES-128-CBC      # AES
;cipher DES-EDE3-CBC    # Triple-DES
```

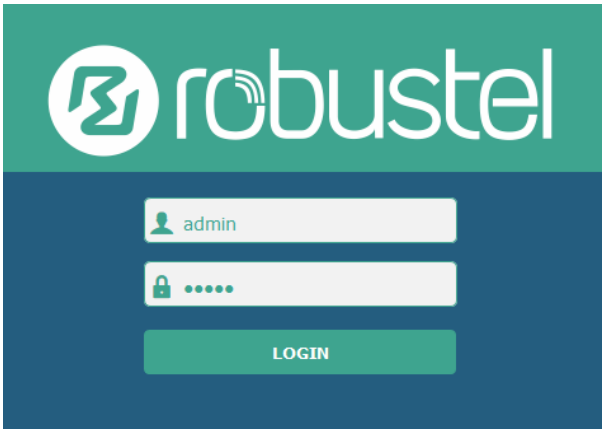
```
# Enable compression on the VPN link.
# If you enable it here, you must also
# enable it in the client config file.
comp-lzo

# The maximum number of concurrently connected
# clients we want to allow.
max-clients 100

# It's a good idea to reduce the OpenVPN
# daemon's privileges after initialization.
#
# You can uncomment this out on
# non-Windows systems.
;user nobody
;group nobody

# The persist options will try to avoid
# accessing certain resources on restart
# that may no longer be accessible because
# of the privilege downgrade.
persist-key
persist-tun

# Output a short status file showing
# current connections, truncated
# and rewritten every minute.
status openvpn-status.log

# By default, log messages will go to the syslog (or
# on Windows, if running as a service, they will go to
# the "\Program Files\OpenVPN\log" directory).
# Use log or log-append to override this default.
# "log" will truncate the log file on OpenVPN startup,
# while "log-append" will append to it.    Use one
# or the other (but not both).
;log                openvpn.log
;log-append    openvpn.log

# Set the appropriate level of log
# file verbosity.
#
# 0 is silent, except for fatal errors
# 4 is reasonable for general usage
# 5 and 6 can help to debug connection problems
```

```
# 9 is extremely verbose
verb 3

# Silence repeating messages.    At most 20
# sequential messages of the same message
# category will be output to the log.
;mute 20
```

3.4 R2000 Configuration

3.4.1 Configure Link Management

1. Install the antenna, insert the SIM cards, connect the power supply, and log-in the Web GUI of R2000.

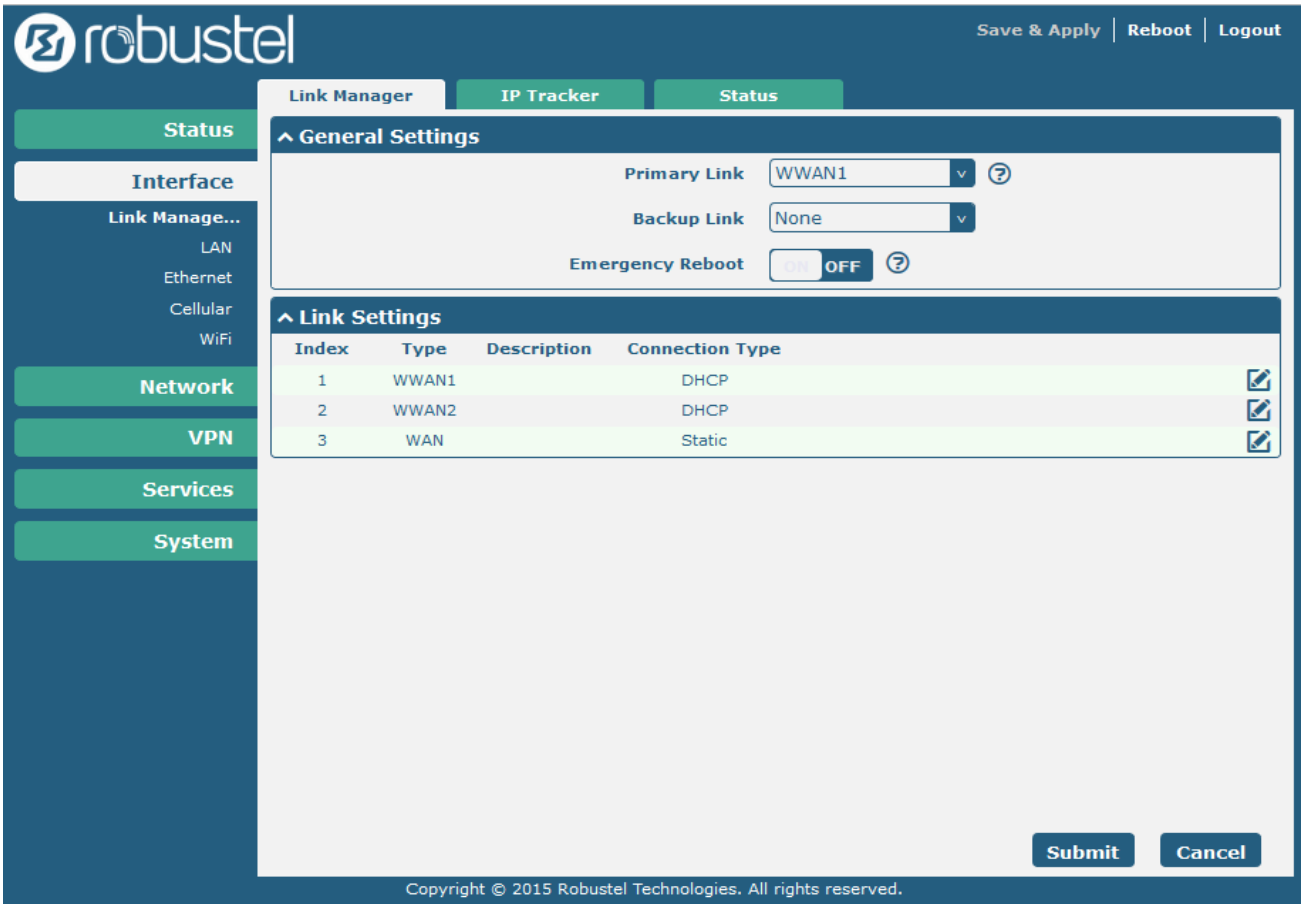


Note: You need to know the following factory settings before you have logged in the Web GUI.

Item	Description
Username	Admin
Password	Admin
ETH0	192.168.0.1/255.255.255.0, LAN Mode
ETH1	192.168.0.1/255.255.255.0, LAN Mode
DHCP Server	Enabled

2. Browse Interface > Link Management.

- Click the drop-down list of **Primary Link** and select **WWAN1**.
- Click **Submit**.
- Click **Save & Apply**.

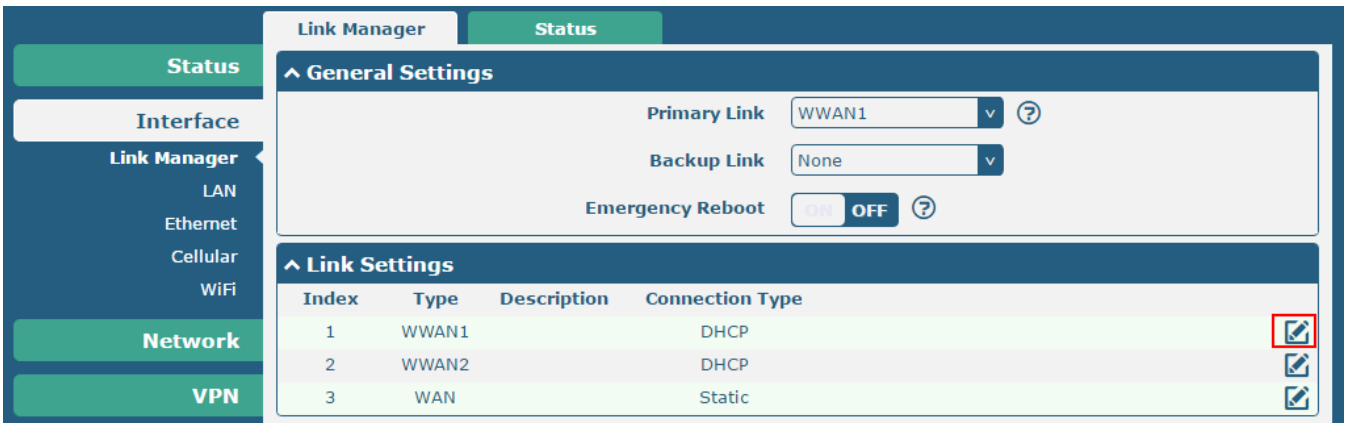


Item	Description	Setting
Primary Link	Select “WWAN1”, “WWAN2” or “WAN” as the primary connecting interface.	WWAN1

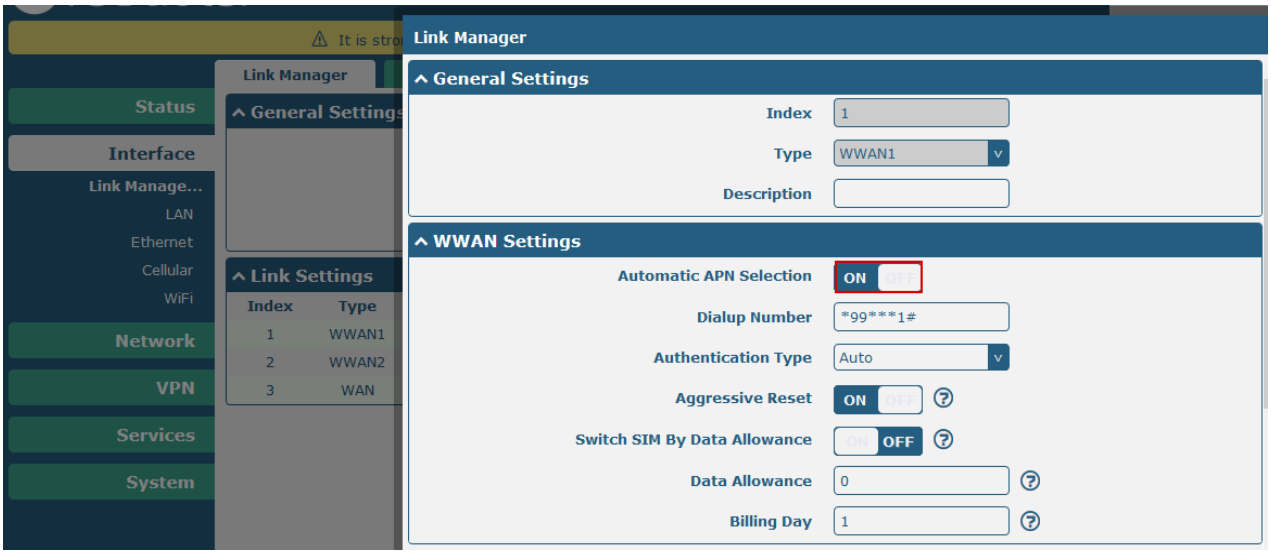
3.4.2 Configure Cellular WAN

1. Browse **Interface > Link Management > Link Settings**.

- Click the edit button of **WWAN1**.
- Enter the related parameters in **WWAN Settings**.
- Enter the related parameters in **Ping Detection Settings**.
- Click **Submit**.
- Click **Save & Apply**.

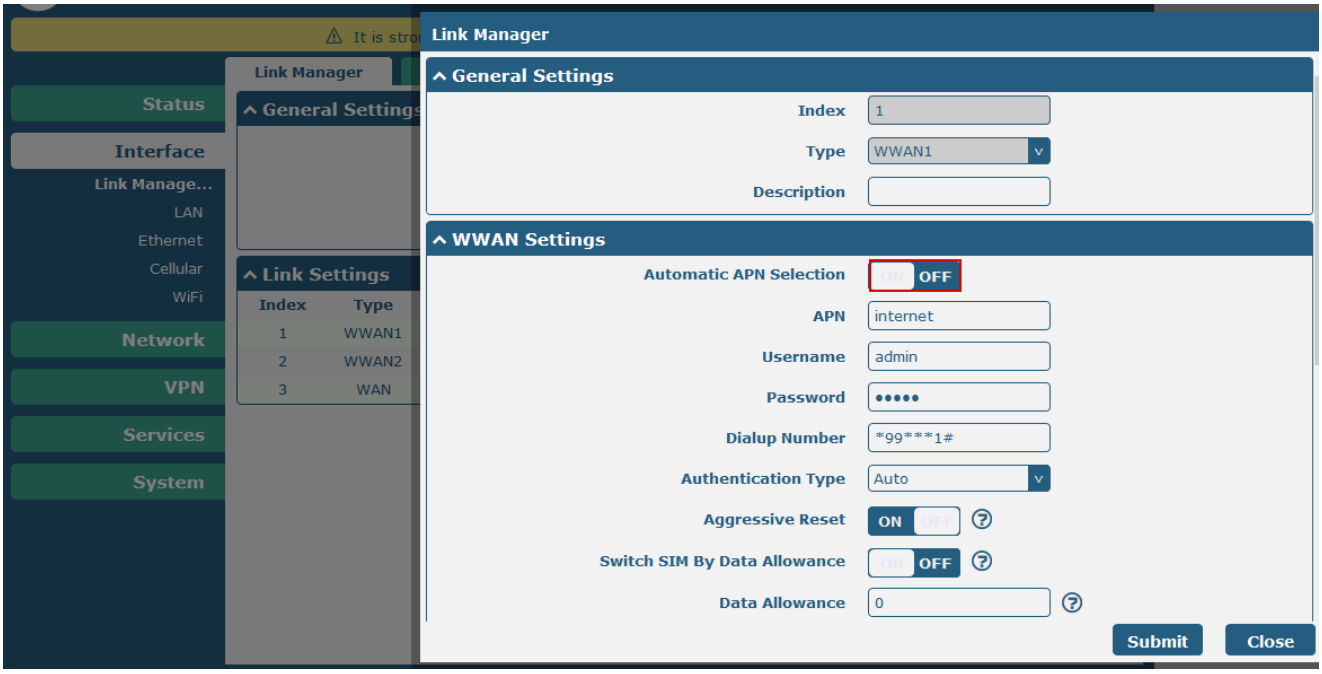


The window is displayed as below when enabling the **Automatic APN Selection**.

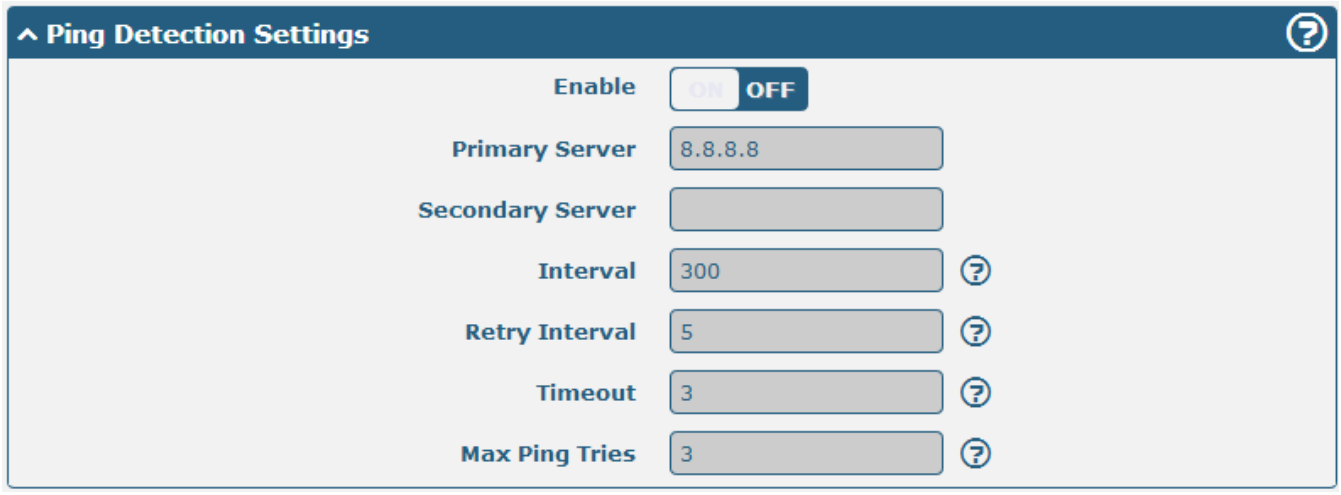


Item	Description	Setting
Dialup Number	Set the dialup number for cellular dial-up connection, provided by local ISP.	*99***1#
Data Allowance	Set the monthly data traffic limitation.	0
Billing Day	Specify the monthly billing day, and the data traffic statistics will be recalculated from this day.	1

The window is displayed as below when disabling the **Automatic APN Selection**.



Item	Description	Setting
APN	Access Point Name for cellular dial-up connection, provided by local ISP.	Internet
Username	Username for cellular dial-up connection, provided by local ISP	Null
Password	Password for cellular dial-up connection, provided by local ISP	Null

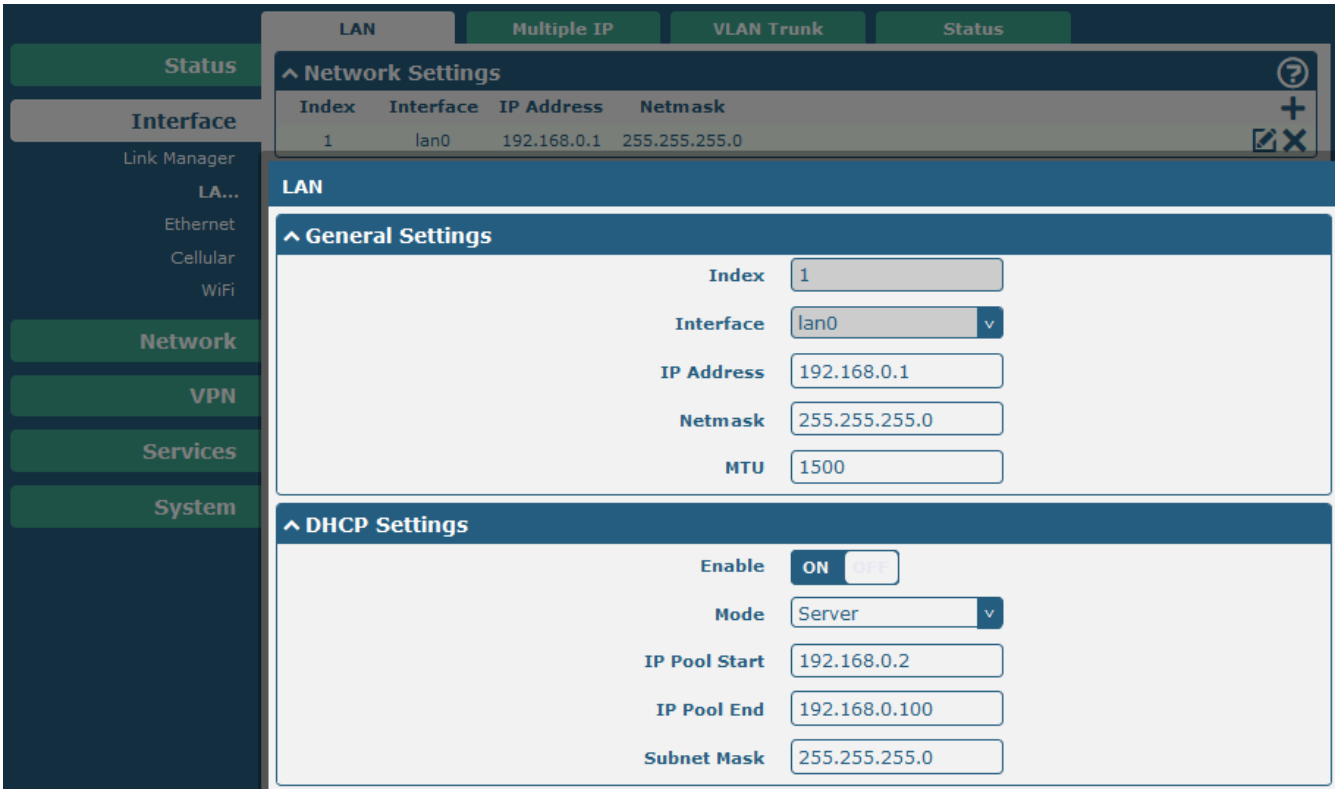


Item	Description	Setting
Enable	Click to enable the ping detection, a keepalive policy of R2000 router.	OFF
Primary Server	Router will ping this primary address/domain name to check if the current connectivity is active.	8.8.8.8
Secondary Server	Router will ping this secondary address/domain name to check if the current connectivity is active.	Null
Interval	Set the ping interval.	300
Retry Interval	Set the ping retry interval.	5
Timeout	Set the ping timeout.	3
Max Ping Tries	Switch to another link or take emergency action if max continuous ping tries reached.	3

3.4.3 Configure IP Address of LAN

1. Browse **Interface > LAN > LAN**.

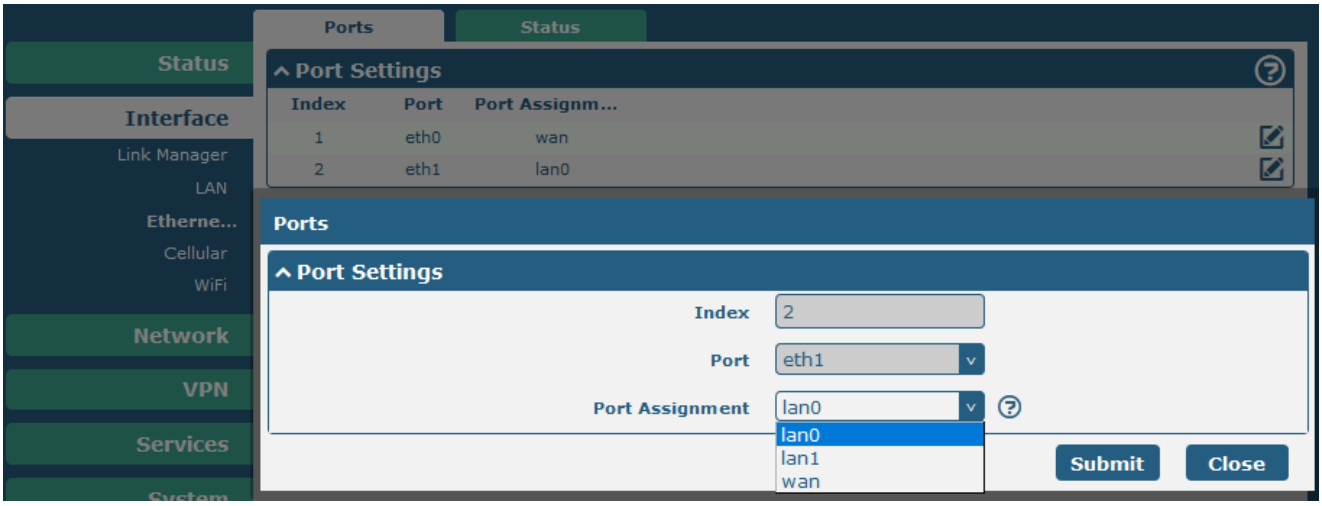
- Click the edit button of **lan0**.
- Set its **IP address** and **Netmask**, and the parameters of **DHCP Settings** are set accordingly.
- Click **Submit**.
- Click **Save & Apply**.



Item	Description	Setting
IP Address	Set the IP address of lan0.	Enter accordingly
Netmask	Set the Netmask of lan0.	Enter accordingly
MTU	Set the MTU of lan0.	1500

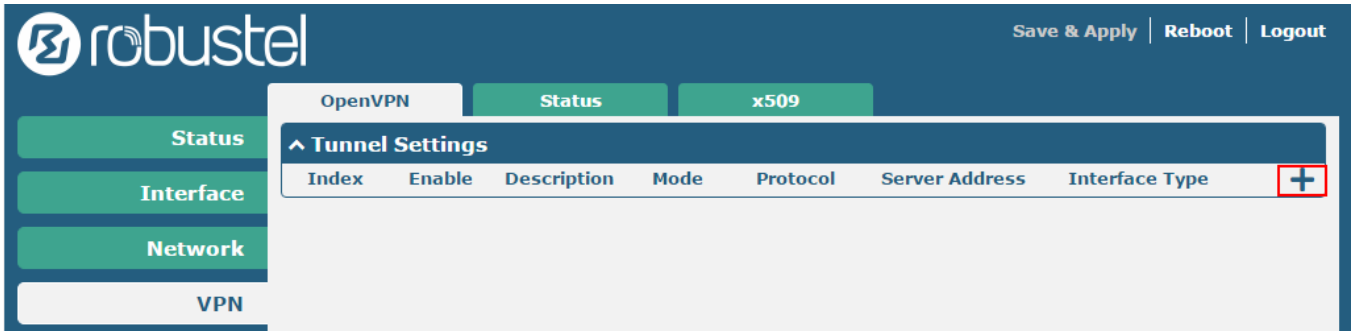
2. Browse **Interface > Ethernet > Ports**.

- Click the edit button of **eth1**.
- Assign **lan0** to the eth1 port.
- Click **Submit**.
- Click **Save & Apply**.

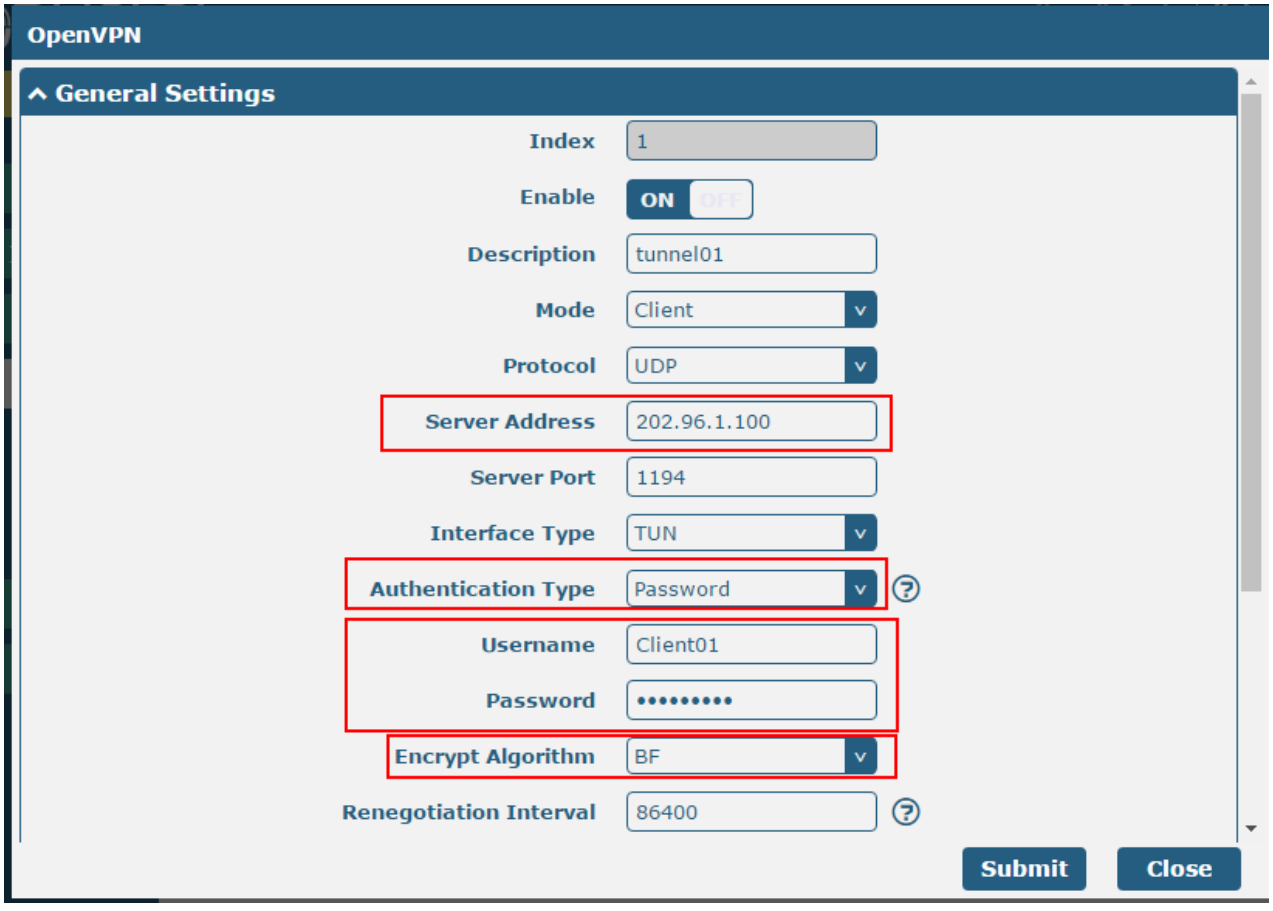


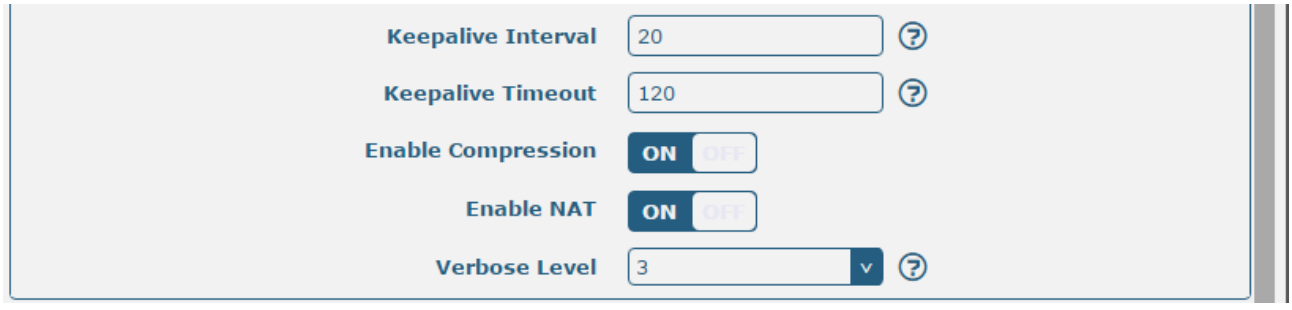
3.4.4 Configure OpenVPN Client

1. Browse **VPN > OpenVPN**, and click the add button.



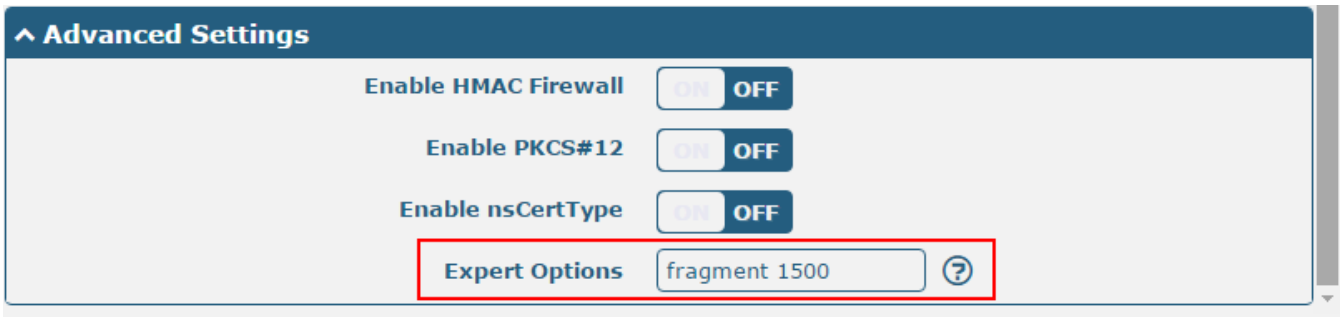
2. Configure the parameters that matched with OpenVPN server side, and click **Submit**.





Item	Description	Default
Index	Show the index of the tunnel.	1
Enable	Click to enable OpenVPN tunnel.	ON
Description	Enter some simple words about the OpenVPN Tunnel.	Null
Mode	Select from “P2P” or “Client”.	Client
Protocol	Select from “UDP” or “TCP-Client”.	UDP
Server Address	Enter the server address of OpenVPN.	Null
Server Port	Enter the server port of OpenVPN.	1194
Interface Type	Select from “TUN” or “TAP”, which are two different kinds of device interface for OpenVPN. The difference between TUN and TAP device: a TUN device is a virtual IP point-to-point device and a TAP device is a virtual Ethernet device.	TUN
Authentication Type	Select from “None”, “Preshared”, “Password”, “X509CA” or “X509CA Password”. “None” and “Preshared” type is only working in P2P mode.	None
Local IP	Define the local IP address of OpenVPN tunnel when setting P2P as the mode.	Null
Remote IP	Define the remote IP address of OpenVPN tunnel when setting P2P as the mode.	Null
Username	Username used for Authentication Type “Password” or “X509CA Password”.	Null
Password	Password used for Authentication Type “Password” or “X509CA Password”.	Null
Encrypt Algorithm	Select from “BF”, “DES”, “DES-EDE3”, “AES128”, “AES192” or “AES256”. BF: Use the BF algorithm in CBC mode and 128-bit key DES: Use the DES algorithm in CBC mode and 64-bit key DES-EDE3: Use the 3DES algorithm in CBC mode and 192-bit key AES128: Use the AES algorithm in CBC mode and 128-bit key AES192: Use the AES algorithm in CBC mode and 192-bit key AES256: Use the AES algorithm in CBC mode and 256-bit key	BF
Keepalive Interval	Set keepalive (ping) interval to check if the tunnel is active.	20
Keepalive Timeout	Trigger OpenVPN to restart after n seconds if not receiving a ping or other packets from remote.	120
Private Key Password	Password of Private Key for Authentication Type “X509CA”.	Null
Enable Compression	Enable to compress the data stream.	ON
Enable NAT	Click to enable NAT for OpenVPN. The source IP address of host behind R2000 will be disguised before accessing the remote OpenVPN client.	OFF

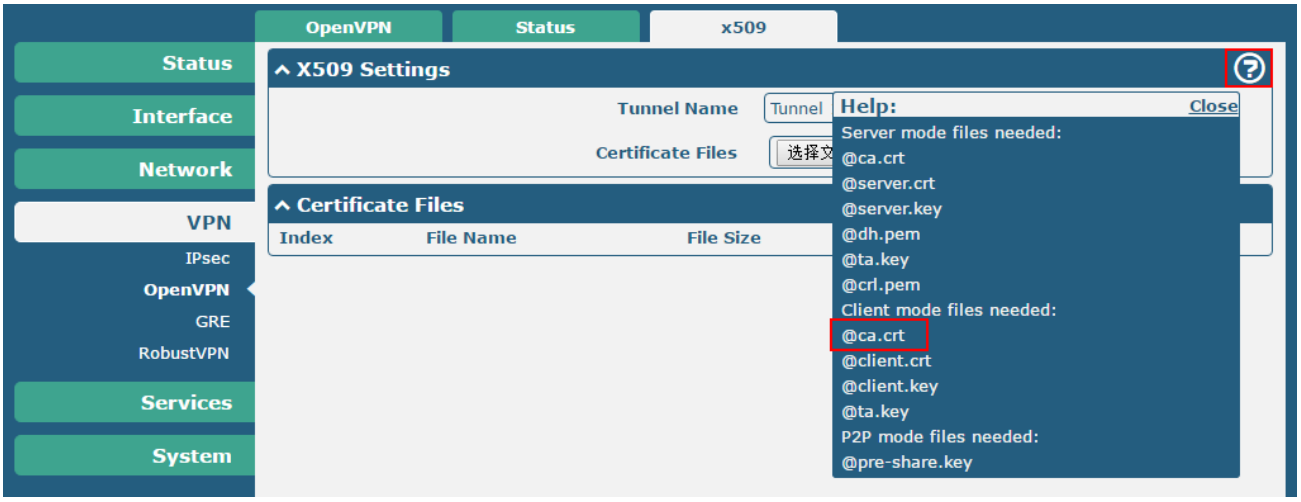
Item	Description	Default
Verbose Level	Select the level of the output log. Values range from 0 to 11. 0 -- No output except fatal errors 1 to 4 -- Normal usage range 5 -- Output R and W characters to the console for each packet read and write 6 to 11 -- Debug info range	0



Item	Description	Default
Enable HMAC Firewall	Add an additional layer of HMAC authentication on top of the TLS control channel to protect against DoS attacks.	OFF
Enable PKCS#12	Enable the PKCS#12 certificate. It is an exchange of digital certificate encryption standard, used to describe personal identity information.	OFF
Enable nsCertType	Require that peer certificate was signed with an explicit nsCertType designation of "server".	OFF
Expert Options	Enter some other options of OpenVPN in this field. Each expression can be separated by a semicolon (;).	Null

3. Import the certificate for OpenVPN.

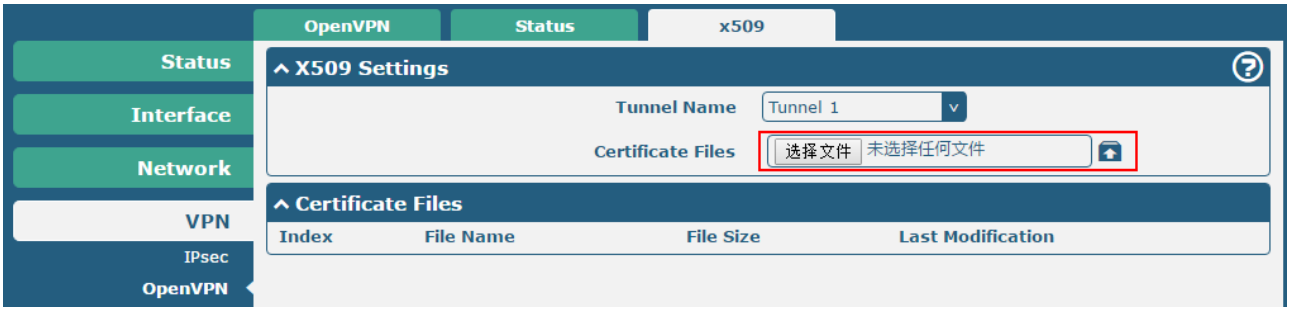
- Browse **VPN > OpenVPN > X509**.



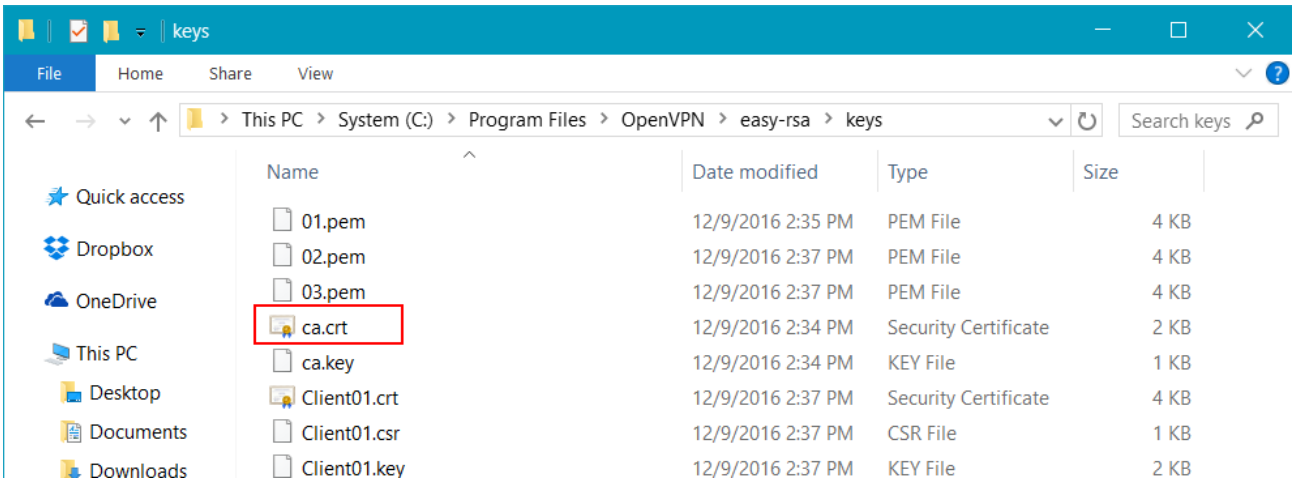
Item	Description	Setting
Select Cert Type	Select the OpenVPN client or server which the certificate used for.	Select accordingly

CA	Click “Browse” to select the correct CA file from your PC, and click “Import” to import it to the router. Click “Export” to export the CA file from the router to your PC.	Select accordingly
Public Key	Click “Browse” to select the correct Public Key file from your PC, and click “Import” to import it to the router. Click “Export” to export the Public Key A file from the router to your PC.	Select accordingly
Private Key	Click “Browse” to select the correct Private Key file from your PC, and click “Import” to import it to the router. Click “Export” to export the Private Key file from the router to your PC.	Select accordingly
DH	Click “Browse” to select the correct DH A file from your PC, and click “Import” to import it to the router. Click “Export” to export the DH file from the router to your PC.	Null
TA	Click “Browse” to select the correct TA file from your PC, and click “Import” to import it to the router. Click “Export” to export the TA file from the router to your PC.	Null
CRL	Click “Browse” to select the correct CRL file from your PC, and click “Import” to import it to the router. Click “Export” to export the CRL file from the router to your PC.	Null
Pre-Share Static Key	Click “Browse” to select the correct Pre-Share Static Key file from your PC, and click “Import” to import it to the router. Click “Export” to export the Pre-Share Static Key file from the router to your PC.	Null

4. Import the certificate, select the Tunnel Name for **Client** and click **Choose File**.

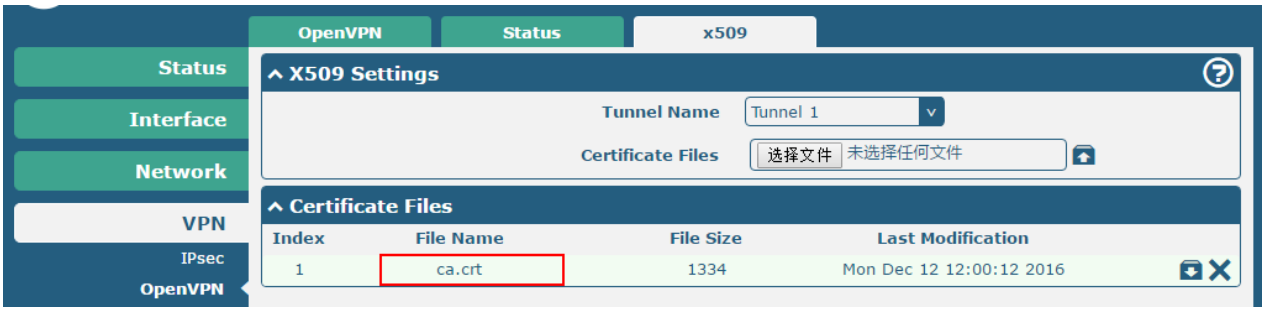


5. Select the **ca.crt** in the path C:\Program Files\OpenVPN\config



Note: *While we using Username/Password for authentication, CA is still required for the OpenVPN client, but public key and private key for client is not required.*

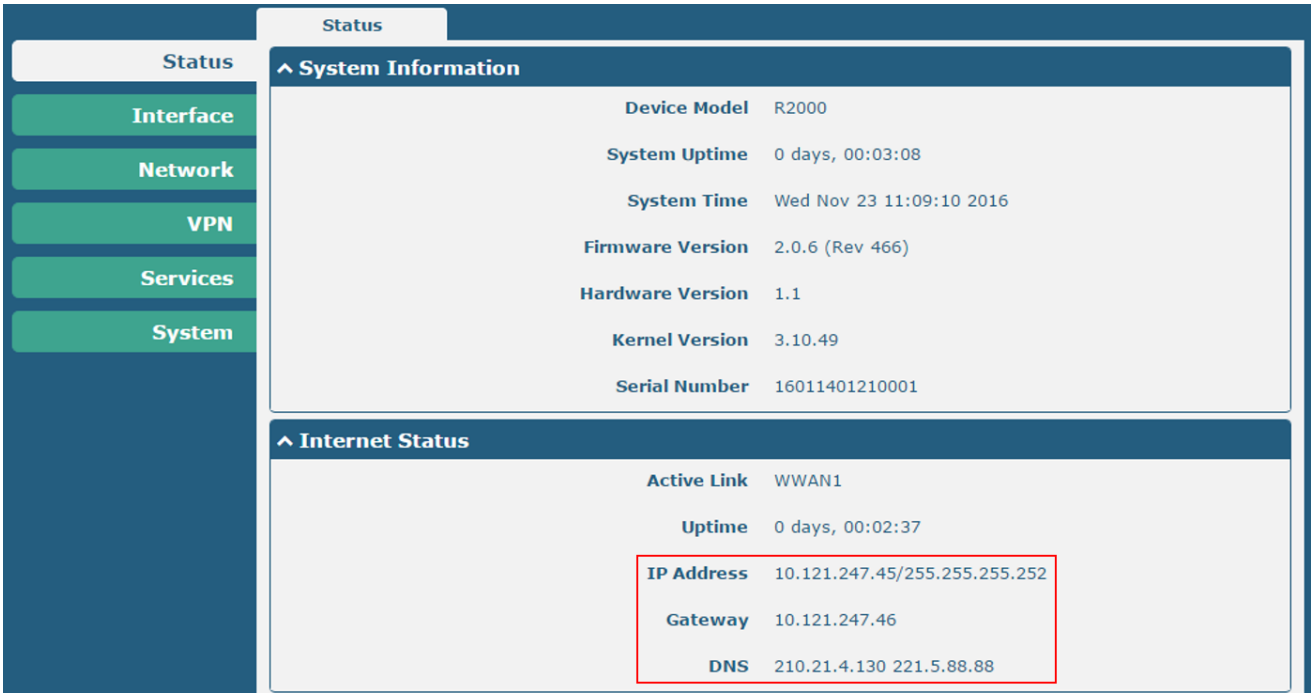
6. Click the **Save & Apply** and check the CA status.



Chapter 4 Testing

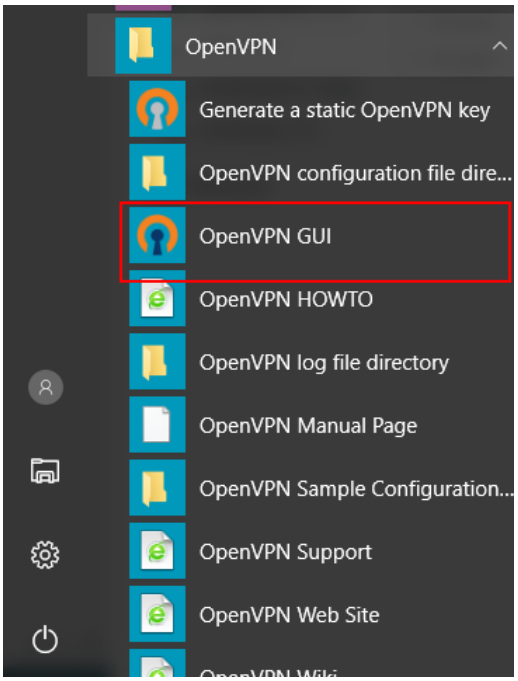
4.1 Network Status

1. Browse **Status**.
2. Check whether R2000 has obtained the assigned static IP address (the following IP is for reference only).
3. Check whether R2000 has used SIM card to register to network, dial up to get IP address and get access to the Internet.



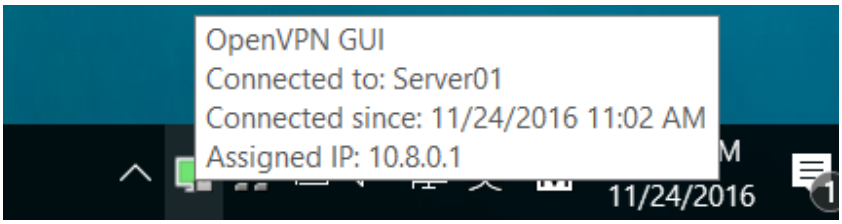
4.2 Running the OpenVPN Software in Windows OS

1. Run the OpenVPN software.



2. Check the OpenVPN icon in the system tray.

3. Double-click the icon, and the icon will turn green and prompt a notification with the assigned IP address when the OpenVPN server has successfully started.

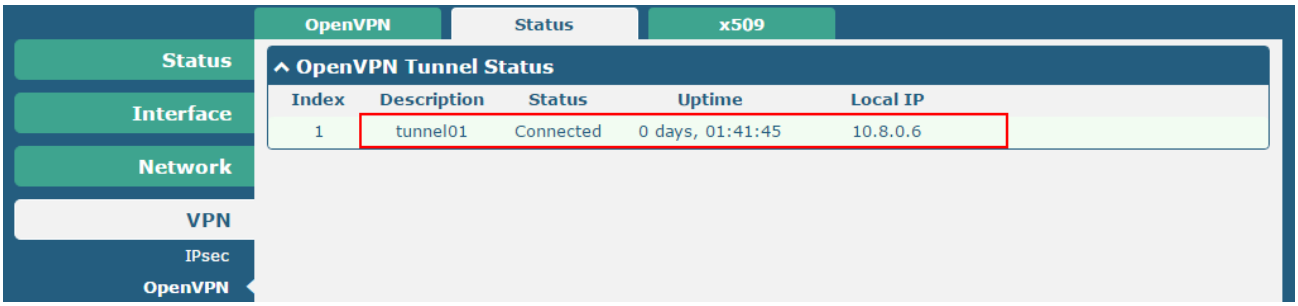


This server will now wait for the connection for OpenVPN clients.

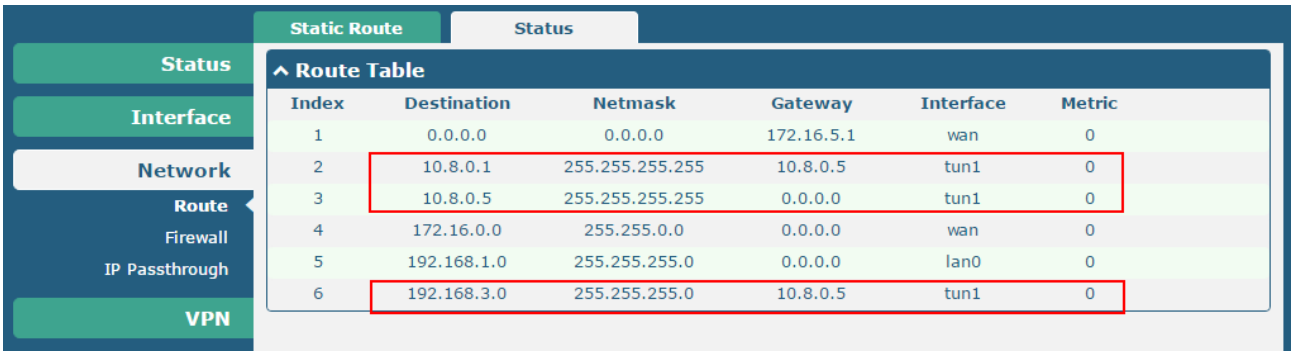
4.3 VPN Status and Communication

Browse **VPN > OpenVPN > Status**.

- Check whether R2000 has established OpenVPN tunnel with Server side.

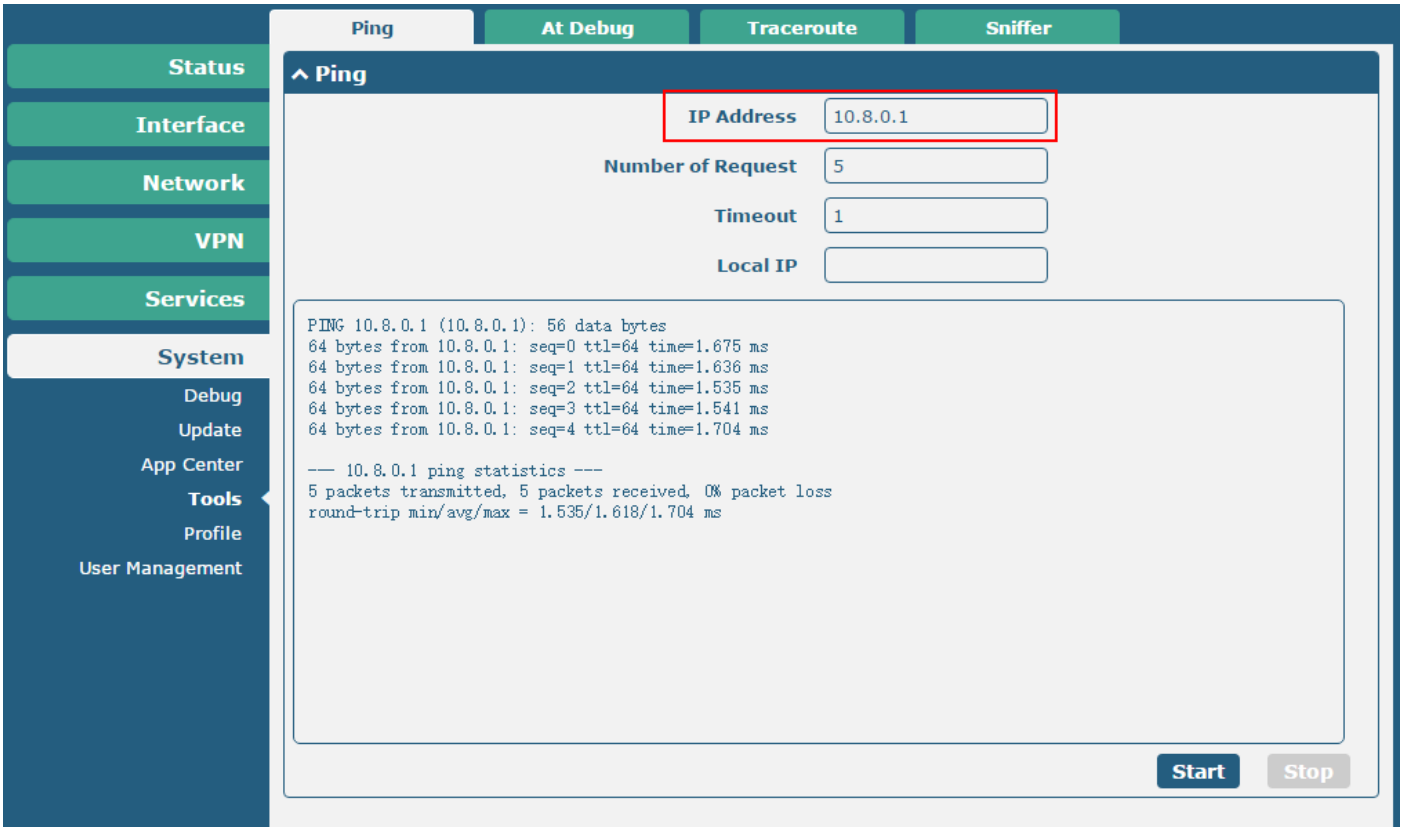


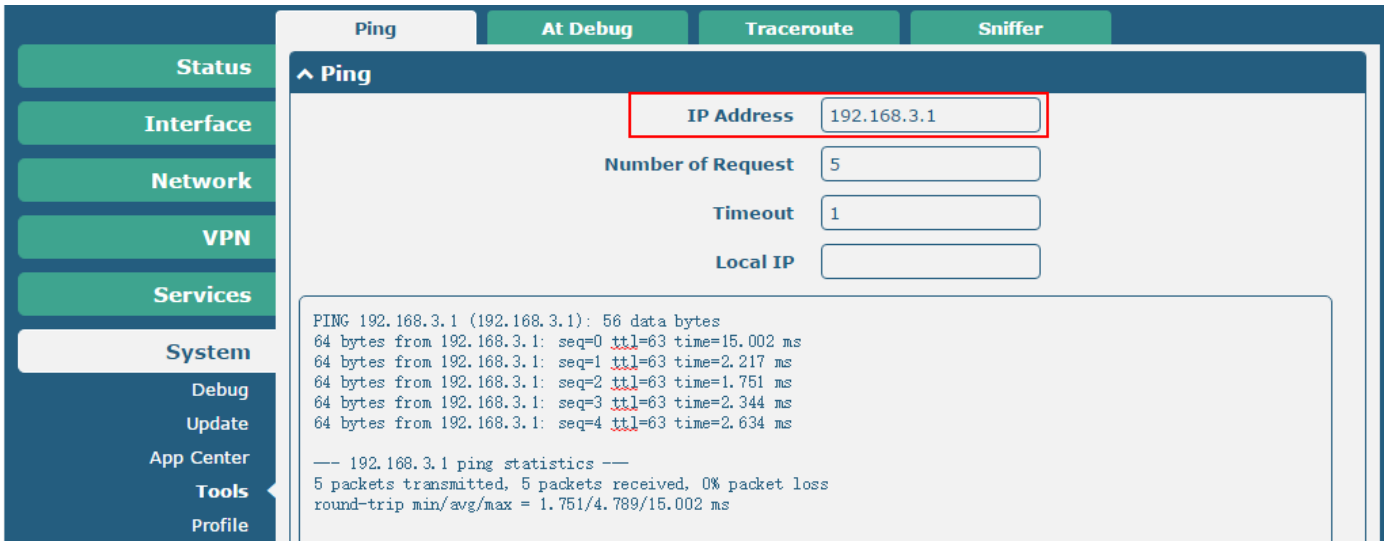
- Browse **Network > Route > Status**, and check the virtual tunnel on Route table.



- Browse **System > Tools > Ping**.

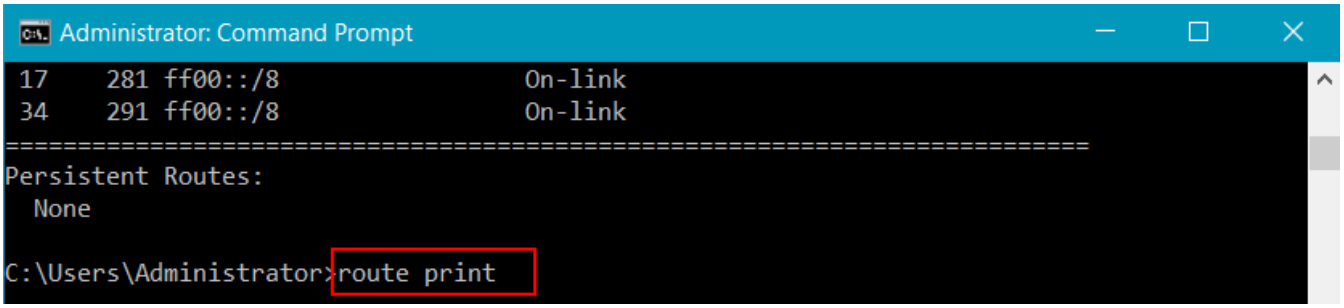
  Ping the virtual IP of OpenVPN Server and LAN IP address behind Server, got ICMP reply from remote end.



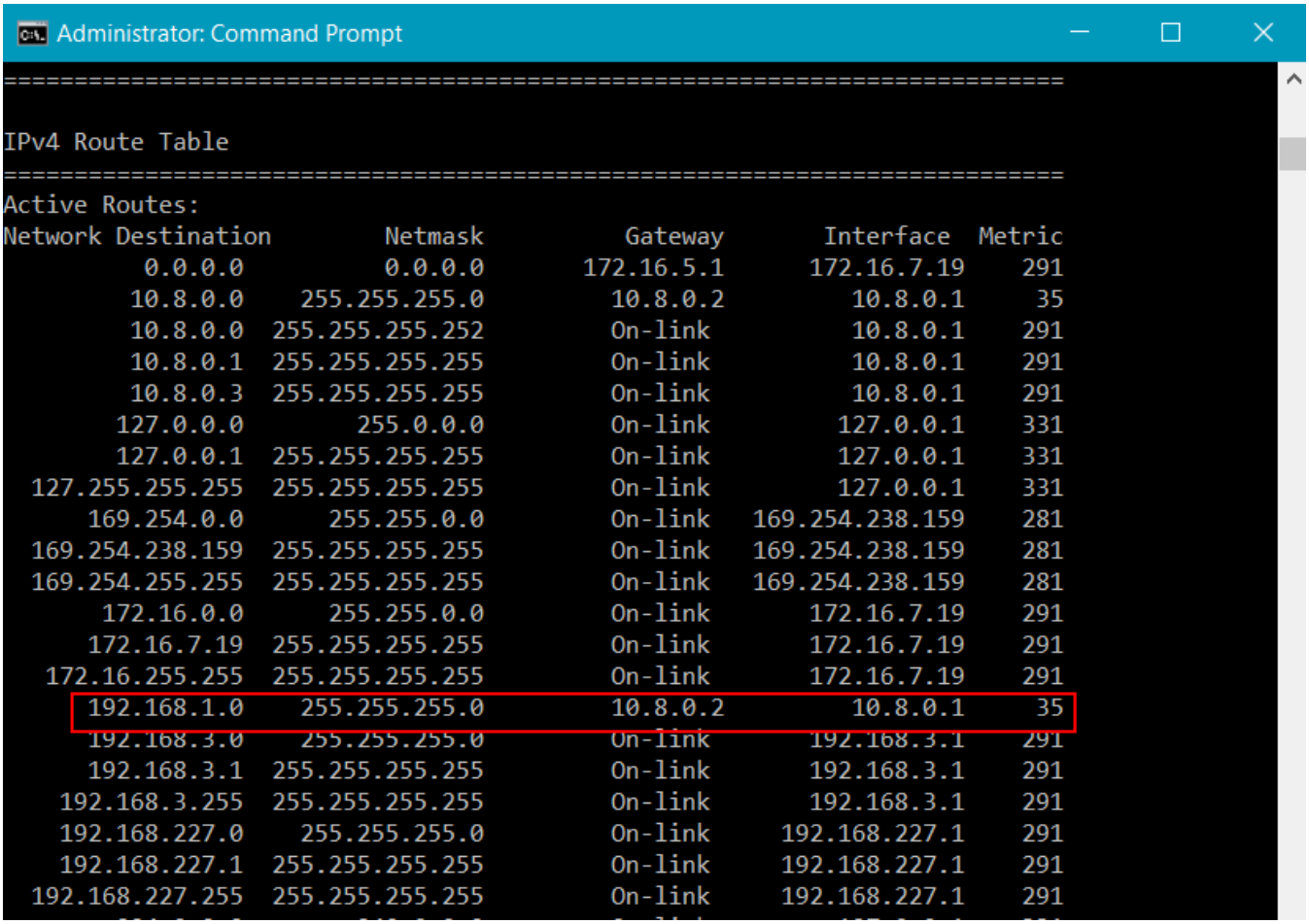


4.4 Testing at OpenVPN Server

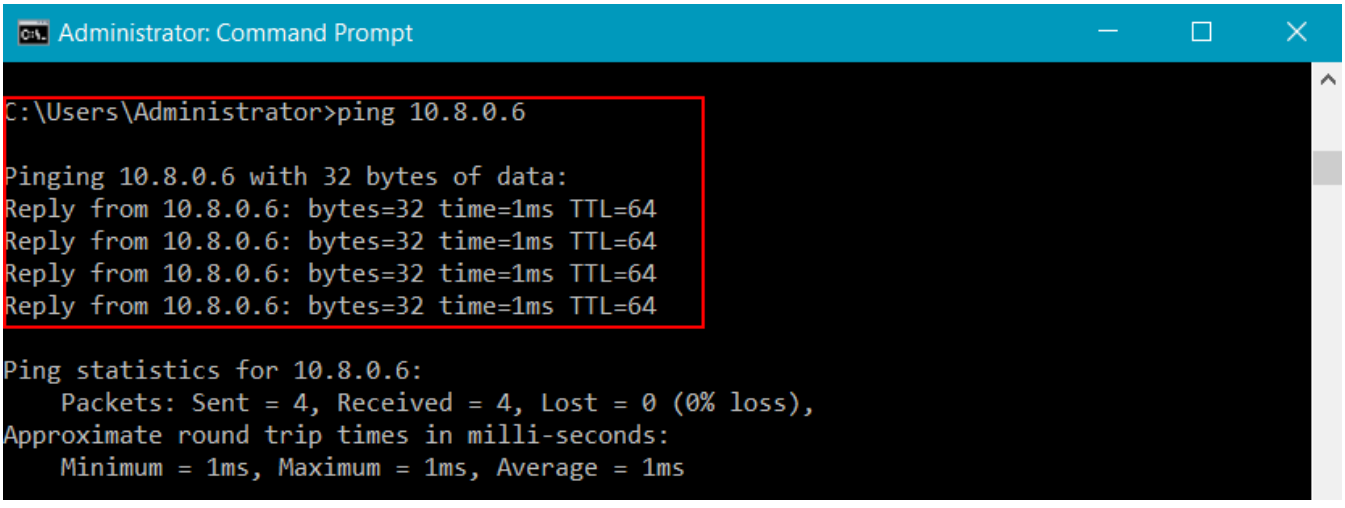
1. Run the CLI and input “route print” command to check the route-table in Windows 7.

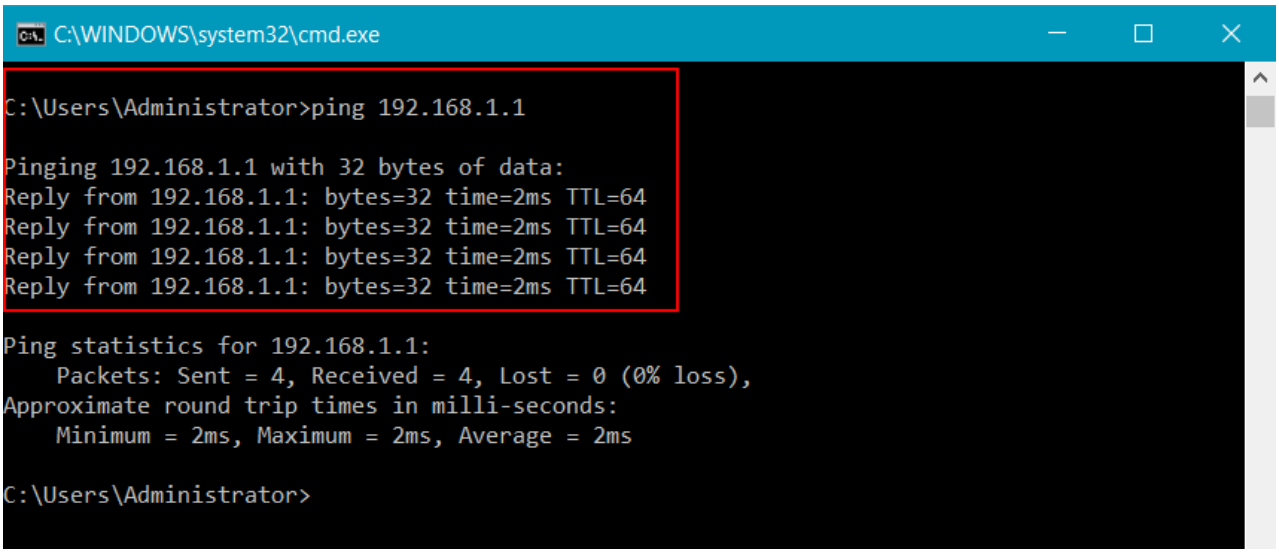


2. There is a remote subnet 192.168.1.0/24 passing through the OpenVPN tunnel.



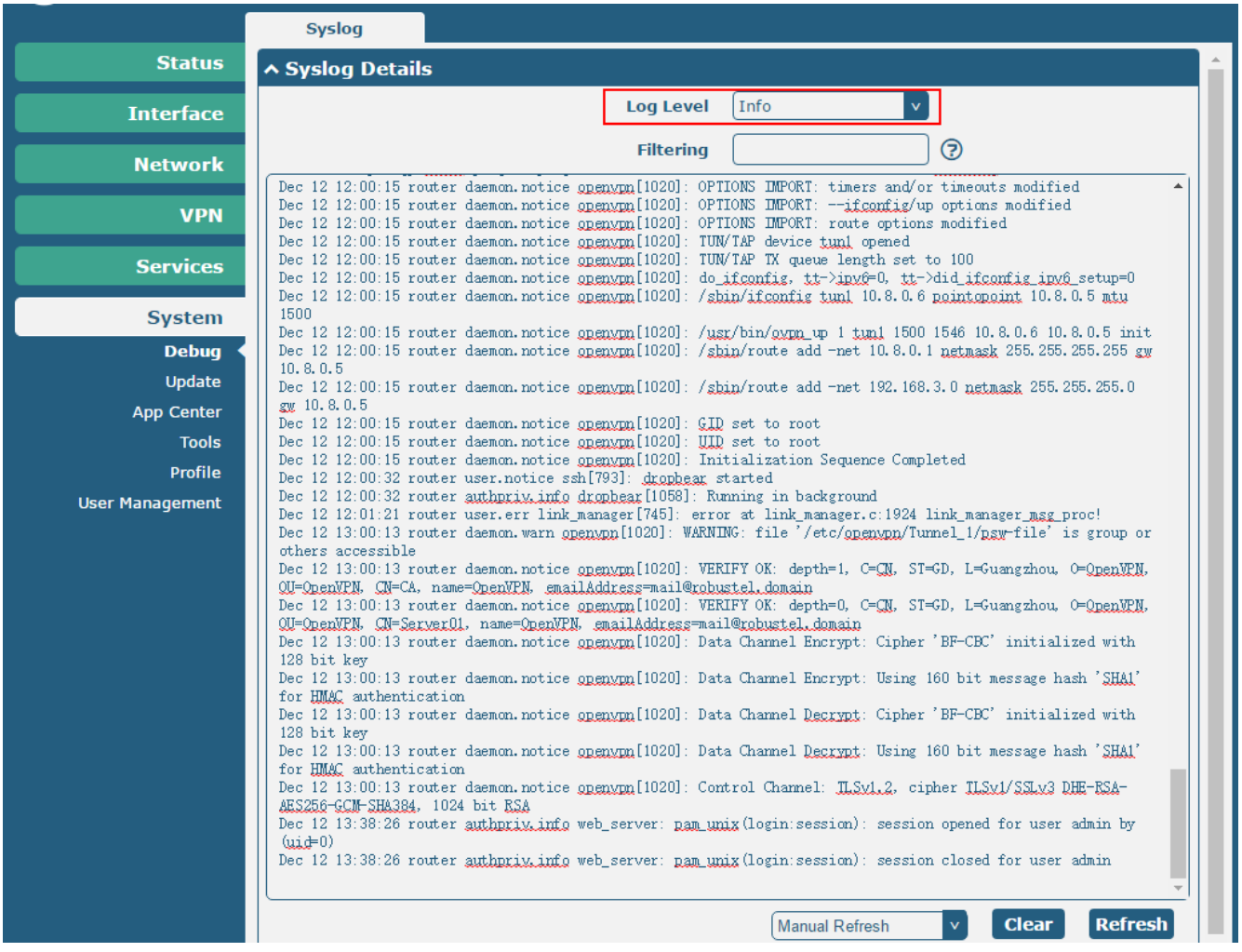
3. Ping the virtual IP of OpenVPN client and LAN IP address behind R2000, got ICMP reply from remote end.





4.5 Event/Log

Debug shows the running process and the status of R2000. Only the information is relevant to the configuration above will be explained below:



……

Dec 12 13:49:12 router user.notice init[1]: OpenVPN configure file create successfully.

Dec 12 13:49:12 router daemon.notice openvpn[1151]: OpenVPN 2.3.8 mips-ar9341-linux-uclibc [SSL (OpenSSL)] [LZO] [EPOLL] [IPv6] built on Nov 2 2016

Dec 12 13:49:12 router daemon.notice openvpn[1151]: library versions: OpenSSL 1.0.1j 15 Oct 2014, LZO 2.09

Dec 12 13:49:12 router daemon.warn openvpn[1151]: WARNING: file '/etc/openvpn/Tunnel_1/psw-file' is group or others accessible

Dec 12 13:49:12 router user.notice init[1]: OpenVPN Tunnel_1 started

Dec 12 13:49:12 router daemon.warn openvpn[1152]: WARNING: No server certificate verification method has been enabled. See http://openvpn.net/howto.html#mitm for more info.

Dec 12 13:49:12 router daemon.warn openvpn[1152]: NOTE: the current --script-security setting may allow this configuration to call user-defined scripts

Dec 12 13:49:12 router daemon.notice openvpn[1152]: Socket Buffers: R=[163840->131072] S=[163840->131072]

Dec 12 13:49:12 router daemon.notice openvpn[1152]: NOTE: UID/GID downgrade will be delayed because of --client, --pull, or --up-delay

Dec 12 13:49:12 router daemon.notice openvpn[1152]: UDPv4 link local: [undef]

Dec 12 13:49:12 router daemon.notice openvpn[1152]: UDPv4 link remote: [AF_INET]172.16.7.19:1194

Dec 12 13:49:12 router daemon.notice openvpn[1152]: TLS: Initial packet from [AF_INET]172.16.7.19:1194, sid=3e9ad251 3cadb2dd

Dec 12 13:49:12 router daemon.notice openvpn[1152]: VERIFY OK: depth=1, C=CN, ST=GD, L=Guangzhou, O=OpenVPN, OU=OpenVPN, CN=CA, name=OpenVPN, emailAddress=mail@robustel.domain

Dec 12 13:49:12 router daemon.notice openvpn[1152]: VERIFY OK: depth=0, C=CN, ST=GD, L=Guangzhou, O=OpenVPN, OU=OpenVPN, CN=Server01, name=OpenVPN, emailAddress=mail@robustel.domain

Dec 12 13:49:12 router daemon.notice openvpn[1152]: Data Channel Encrypt: Cipher 'BF-CBC' initialized with 128 bit key

Dec 12 13:49:12 router daemon.notice openvpn[1152]: Data Channel Encrypt: Using 160 bit message hash 'SHA1' for HMAC authentication

Dec 12 13:49:12 router daemon.notice openvpn[1152]: Data Channel Decrypt: Cipher 'BF-CBC' initialized with 128 bit key

Dec 12 13:49:12 router daemon.notice openvpn[1152]: Data Channel Decrypt: Using 160 bit message hash 'SHA1' for HMAC authentication

Dec 12 13:49:12 router daemon.notice openvpn[1152]: Control Channel: TLSv1.2, cipher TLSv1/SSLv3 DHE-RSA-AES256-GCM-SHA384, 1024 bit RSA

Dec 12 13:49:12 router daemon.notice openvpn[1152]: [Server01] Peer Connection Initiated with [AF_INET]172.16.7.19:1194

Dec 12 13:49:15 router daemon.notice openvpn[1152]: SENT CONTROL [Server01]: 'PUSH_REQUEST' (status=1)

Dec 12 13:49:15 router daemon.notice openvpn[1152]: PUSH: Received control message: 'PUSH_REPLY,route 10.8.0.1,topology net30,ping 10,ping-restart 120,route 192.168.3.0 255.255.255.0,ifconfig 10.8.0.6 10.8.0.5'

Dec 12 13:49:15 router daemon.notice openvpn[1152]: OPTIONS IMPORT: timers and/or timeouts modified

Dec 12 13:49:15 router daemon.notice openvpn[1152]: OPTIONS IMPORT: --ifconfig/up options modified

Dec 12 13:49:15 router daemon.notice openvpn[1152]: OPTIONS IMPORT: route options modified

Dec 12 13:49:15 router daemon.notice openvpn[1152]: TUN/TAP device tun1 opened

Dec 12 13:49:15 router daemon.notice openvpn[1152]: TUN/TAP TX queue length set to 100

Dec 12 13:49:15 router daemon.notice openvpn[1152]: do_ifconfig, tt->ipv6=0, tt->did_ifconfig_ipv6_setup=0

Dec 12 13:49:15 router daemon.notice openvpn[1152]: /sbin/ifconfig tun1 10.8.0.6 pointopoint 10.8.0.5 mtu 1500
Dec 12 13:49:15 router daemon.notice openvpn[1152]: /usr/bin/ovpn_up 1 tun1 1500 1546 10.8.0.6 10.8.0.5 init
Dec 12 13:49:15 router daemon.notice openvpn[1152]: /sbin/route add -net 10.8.0.1 netmask 255.255.255.255 gw 10.8.0.5
Dec 12 13:49:15 router daemon.notice openvpn[1152]: /sbin/route add -net 192.168.3.0 netmask 255.255.255.0 gw 10.8.0.5
Dec 12 13:49:15 router daemon.notice openvpn[1152]: GID set to root
Dec 12 13:49:15 router daemon.notice openvpn[1152]: UID set to root
Dec 12 13:49:15 router daemon.notice openvpn[1152]: Initialization Sequence Completed
……

Chapter 5 Appendix

5.1 Firmware Version

The configuration above was tested on R2000 with firmware version 2.0.6.