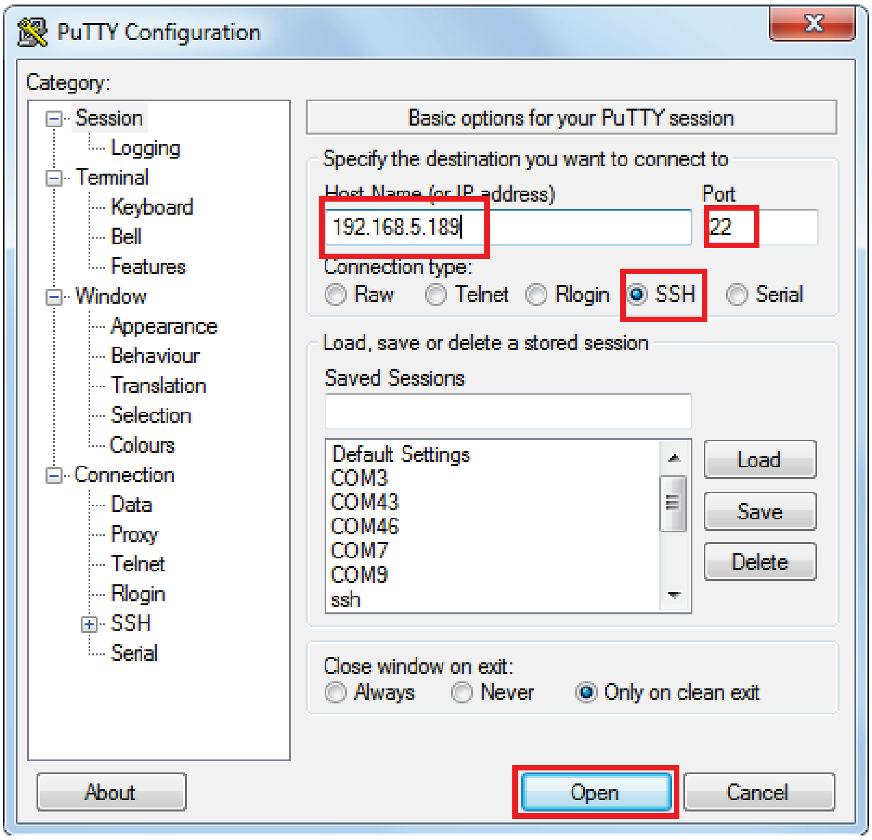
1. Open Putty, input IP address and port, select SSH as connection type, then click button “Open”.



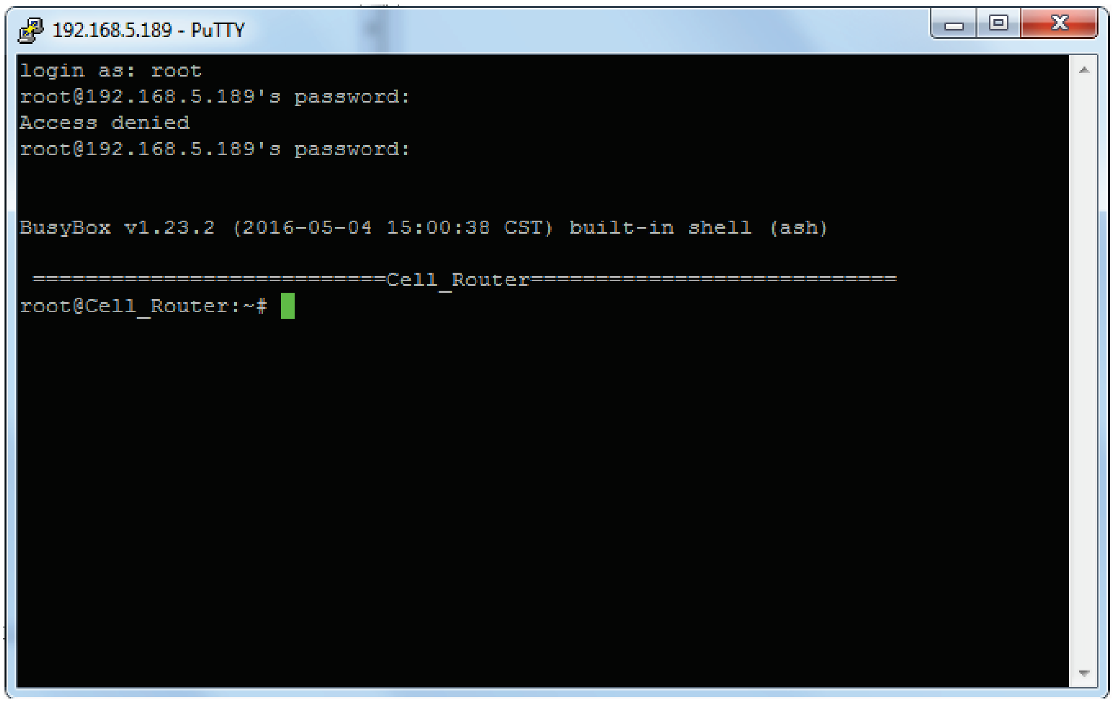
Host Name (or IP address): 192.168.5.189

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

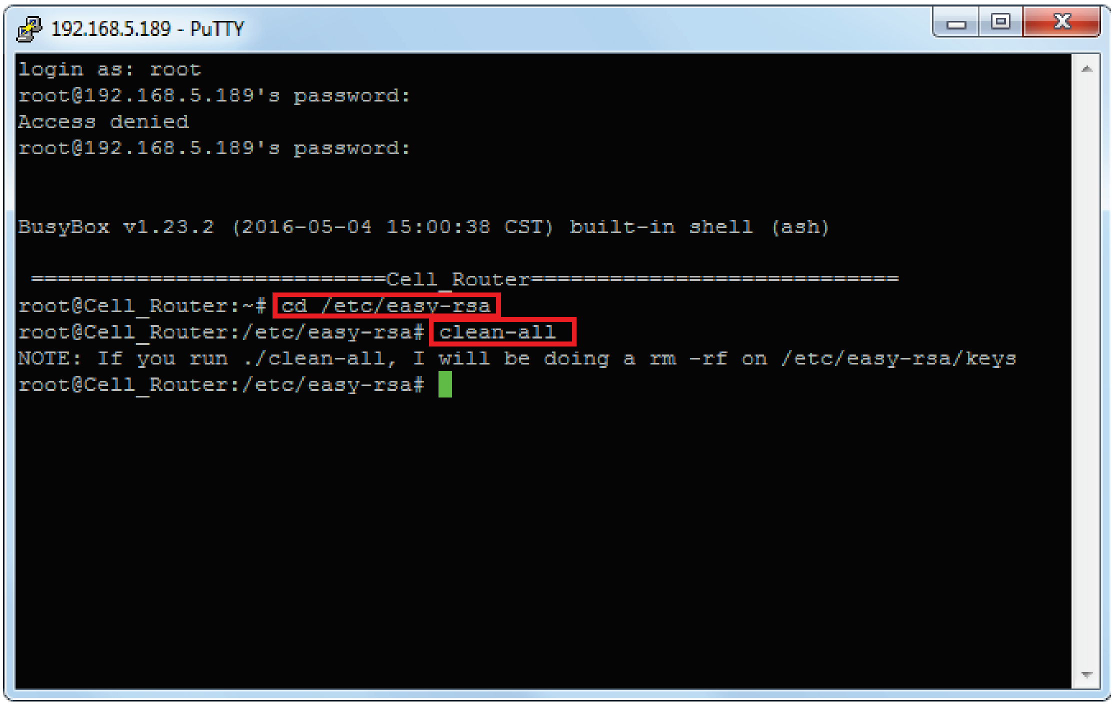
Close window on exit: ○ Always ○ Never ● Only on clean exit

2. Input username and password.



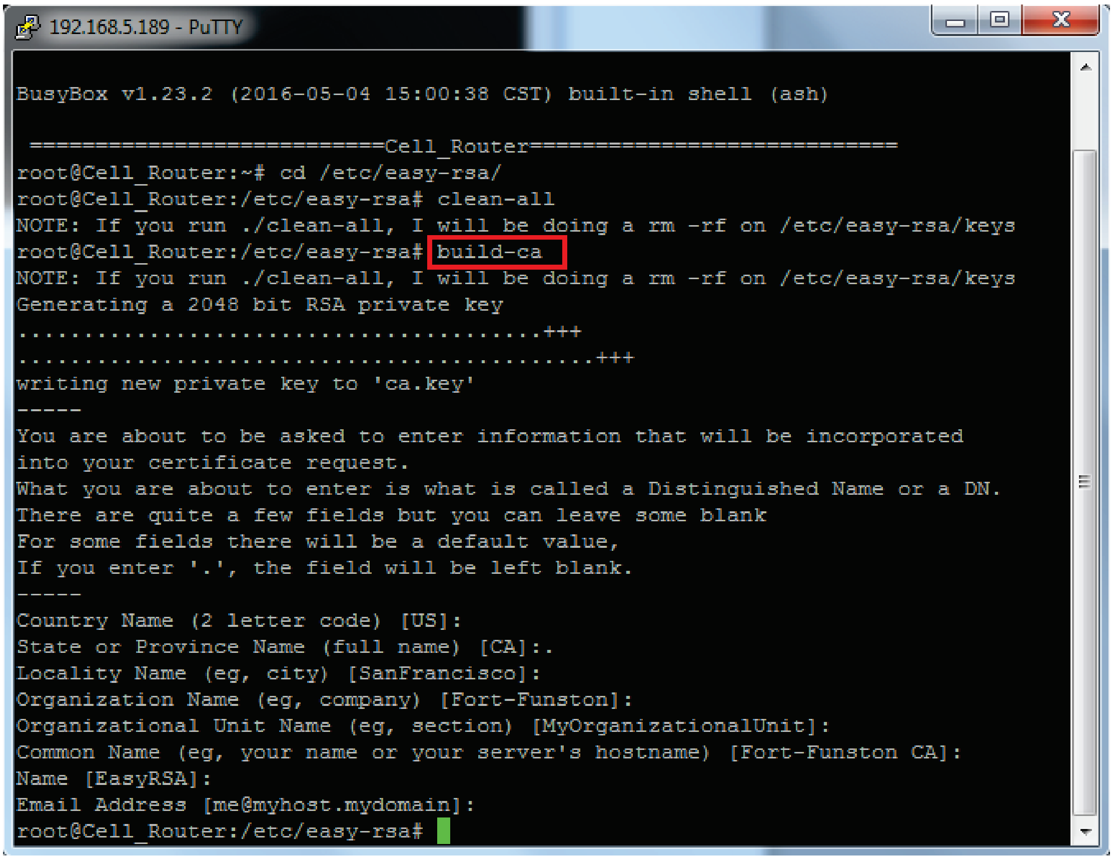
```
login as: root
root@192.168.5.189's password:
Access denied
root@192.168.5.189's password:


BusyBox v1.23.2 (2016-05-04 15:00:38 CST) built-in shell (ash)

 ===========================Cell_Router===========================
root@Cell_Router:~#
```

3. Run command “cd /etc/easy-rsa” and “clean-all”.



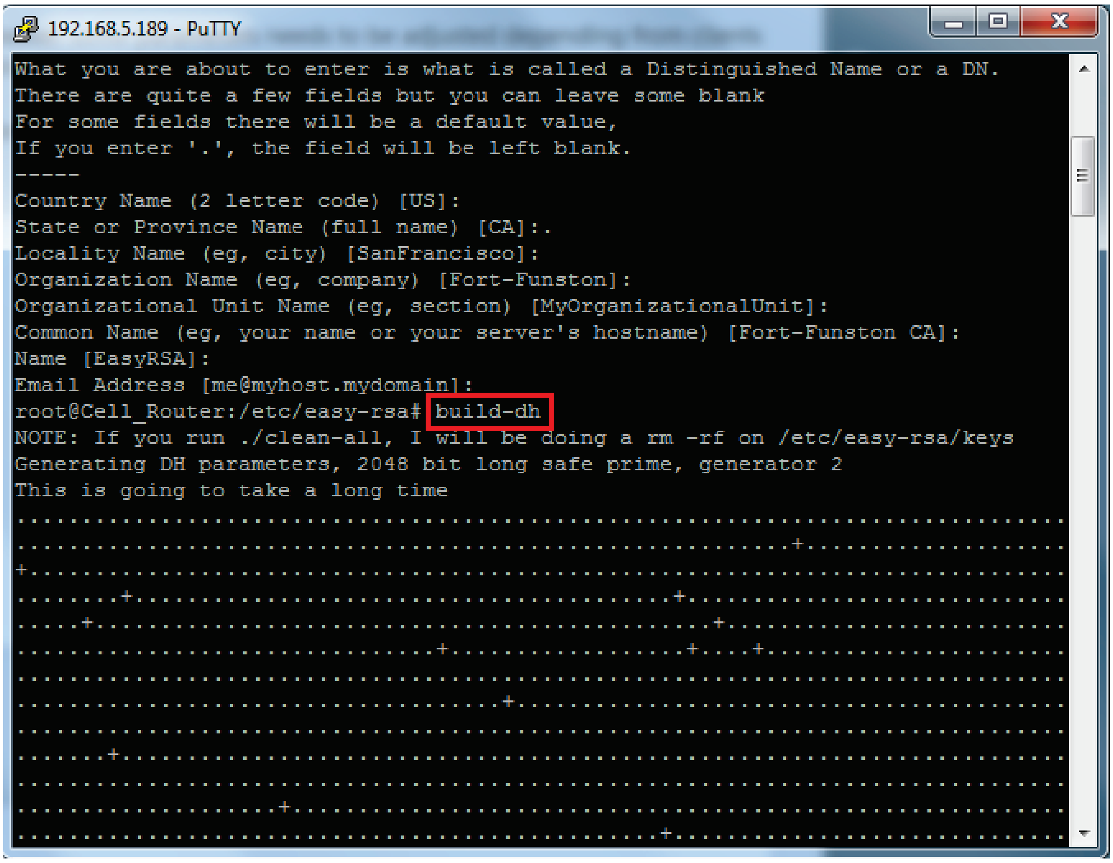
```
login as: root
root@192.168.5.189's password:
Access denied
root@192.168.5.189's password:


BusyBox v1.23.2 (2016-05-04 15:00:38 CST) built-in shell (ash)

 ===========================Cell_Router============================
root@Cell_Router:~# cd /etc/easy-rsa
root@Cell_Router:/etc/easy-rsa# clean-all
NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/easy-rsa/keys
root@Cell_Router:/etc/easy-rsa#
```

4. Run command “build-ca”.



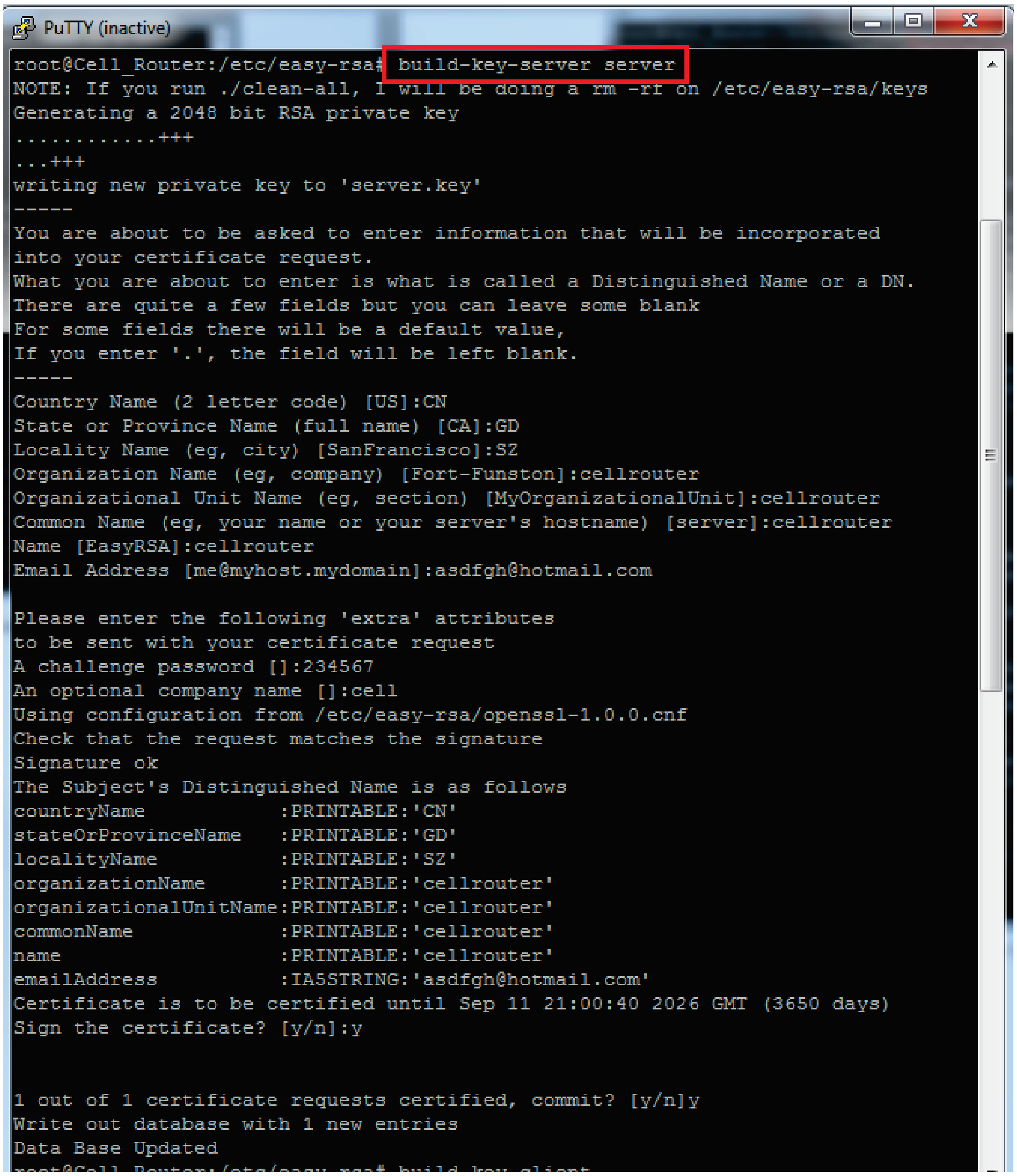
```

BusyBox v1.23.2 (2016-05-04 15:00:38 CST) built-in shell (ash)

 ===========================Cell_Router============================
root@Cell_Router:~# cd /etc/easy-rsa/
root@Cell_Router:/etc/easy-rsa# clean-all
NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/easy-rsa/keys
root@Cell_Router:/etc/easy-rsa# build-ca
NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/easy-rsa/keys
Generating a 2048 bit RSA private key
.......................................+++
...........................................+++
writing new private key to '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) [US]:
State or Province Name (full name) [CA]:.
Locality Name (eg, city) [SanFrancisco]:
Organization Name (eg, company) [Fort-Funston]:
Organizational Unit Name (eg, section) [MyOrganizationalUnit]:
Common Name (eg, your name or your server's hostname) [Fort-Funston CA]:
Name [EasyRSA]:
Email Address [me@myhost.mydomain]:
root@Cell_Router:/etc/easy-rsa#
```

5. Run command “build-dh”, this is going to take a long time. The recommend way is generate it on PC.



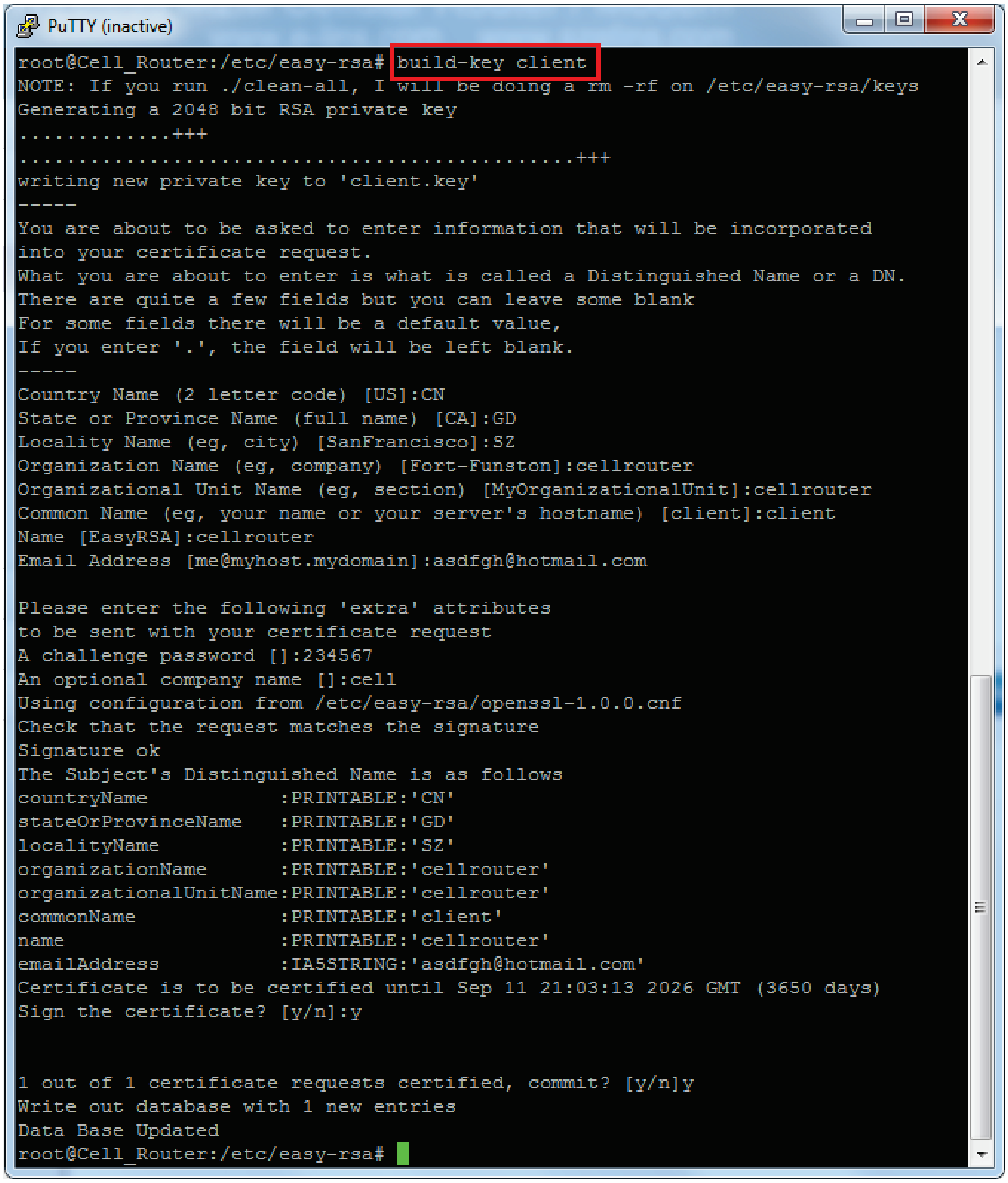
```
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [US]:
State or Province Name (full name) [CA]:.
Locality Name (eg, city) [SanFrancisco]:
Organization Name (eg, company) [Fort-Funston]:
Organizational Unit Name (eg, section) [MyOrganizationalUnit]:
Common Name (eg, your name or your server's hostname) [Fort-Funston CA]:
Name [EasyRSA]:
Email Address [me@myhost.mydomain]:
root@Cell_Router:/etc/easy-rsa# build-dh
NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/easy-rsa/keys
Generating DH parameters, 2048 bit long safe prime, generator 2
This is going to take a long time
................................................................................
...........................................................+....................
+...............................................................................
........+.........................................+.............................
.....+...............................................+..........................
................................+..................+....+.......................
................................................................................
.....................................+..........................................
................................................................................
.......+........................................................................
................................................................................
....................+...........................................................
.................................................+..............................
```

6. Run command “build-key-server server”, you can change “server” to any words you want.



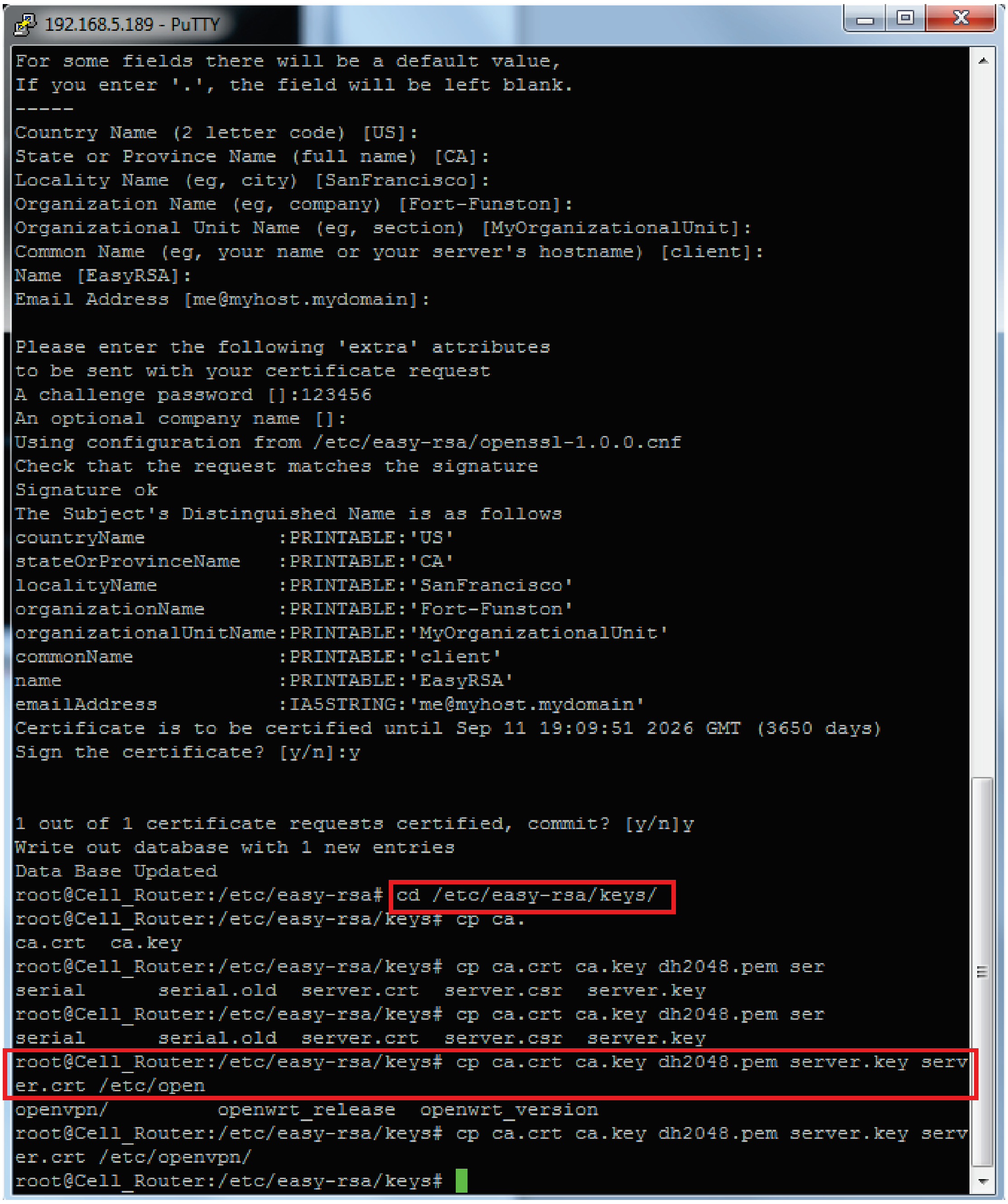
```
root@Cell_Router:/etc/easy-rsa# build-key-server server
NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/easy-rsa/keys
Generating a 2048 bit RSA private key
...........+++
...+++
writing new private key to 'server.key'
-----
You are about to be asked to enter information that will be 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) [US]:CN
State or Province Name (full name) [CA]:GD
Locality Name (eg, city) [SanFrancisco]:SZ
Organization Name (eg, company) [Fort-Funston]:cellrouter
Organizational Unit Name (eg, section) [MyOrganizationalUnit]:cellrouter
Common Name (eg, your name or your server's hostname) [server]:cellrouter
Name [EasyRSA]:cellrouter
Email Address [me@myhost.mydomain]:asdfgh@hotmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:234567
An optional company name []:cell
Using configuration from /etc/easy-rsa/openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'CN'
stateOrProvinceName   :PRINTABLE:'GD'
localityName          :PRINTABLE:'SZ'
organizationName      :PRINTABLE:'cellrouter'
organizationalUnitName:PRINTABLE:'cellrouter'
commonName            :PRINTABLE:'cellrouter'
name                  :PRINTABLE:'cellrouter'
emailAddress          :IA5STRING:'asdfgh@hotmail.com'
Certificate is to be certified until Sep 11 21:00:40 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
root@Cell_Router:/etc/easy-rsa# build-key client
```

7. Run command “build-key client”, you can change “client” to any words you want.



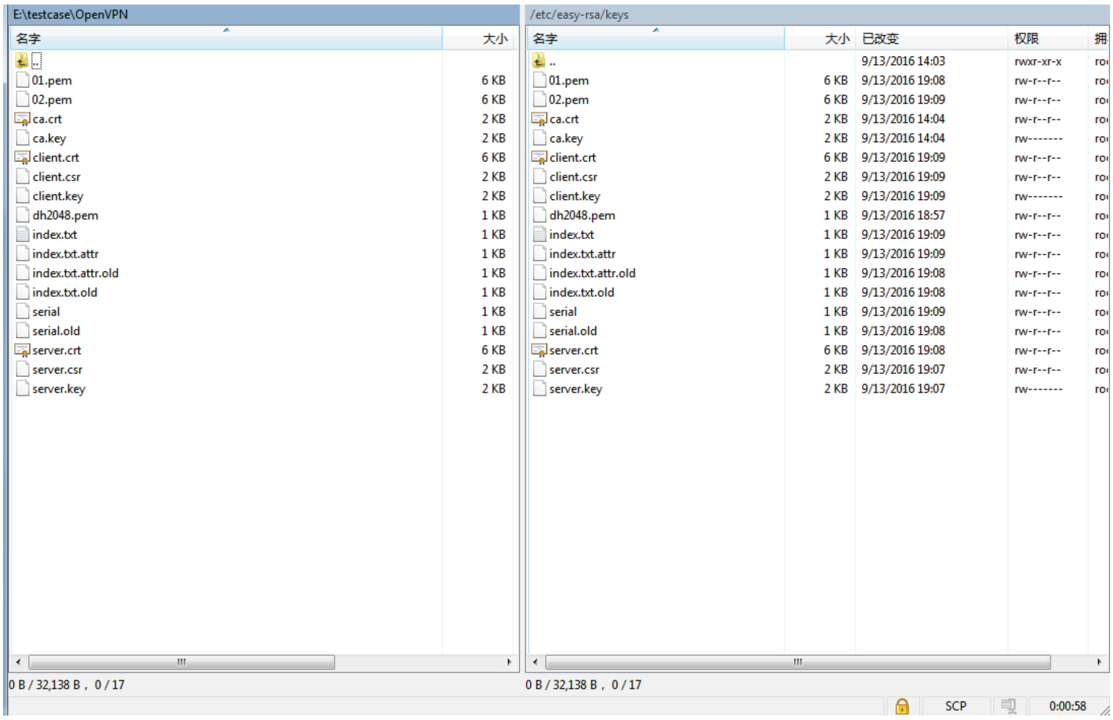
```
root@Cell_Router:/etc/easy-rsa# build-key client
NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/easy-rsa/keys
Generating a 2048 bit RSA private key
.............+++
...............................................+++
writing new private key to 'client.key'
-----
You are about to be 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) [US]:CN
State or Province Name (full name) [CA]:GD
Locality Name (eg, city) [SanFrancisco]:SZ
Organization Name (eg, company) [Fort-Funston]:cellrouter
Organizational Unit Name (eg, section) [MyOrganizationalUnit]:cellrouter
Common Name (eg, your name or your server's hostname) [client]:client
Name [EasyRSA]:cellrouter
Email Address [me@myhost.mydomain]:asdfgh@hotmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:234567
An optional company name []:cell
Using configuration from /etc/easy-rsa/openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'CN'
stateOrProvinceName   :PRINTABLE:'GD'
localityName          :PRINTABLE:'SZ'
organizationName      :PRINTABLE:'cellrouter'
organizationalUnitName:PRINTABLE:'cellrouter'
commonName            :PRINTABLE:'client'
name                  :PRINTABLE:'cellrouter'
emailAddress          :IA5STRING:'asdfgh@hotmail.com'
Certificate is to be certified until Sep 11 21:03:13 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
root@Cell_Router:/etc/easy-rsa# 
```

8. Run command “cd /etc/easy-rsa/keys/” and “cp ca.crt ca.key dh2048.pem server.key server.crt /etc/openvpn/”



```
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [US]:
State or Province Name (full name) [CA]:
Locality Name (eg, city) [SanFrancisco]:
Organization Name (eg, company) [Fort-Funston]:
Organizational Unit Name (eg, section) [MyOrganizationalUnit]:
Common Name (eg, your name or your server's hostname) [client]:
Name [EasyRSA]:
Email Address [me@myhost.mydomain]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:123456
An optional company name []:
Using configuration from /etc/easy-rsa/openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'US'
stateOrProvinceName   :PRINTABLE:'CA'
localityName          :PRINTABLE:'SanFrancisco'
organizationName      :PRINTABLE:'Fort-Funston'
organizationalUnitName:PRINTABLE:'MyOrganizationalUnit'
commonName            :PRINTABLE:'client'
name                  :PRINTABLE:'EasyRSA'
emailAddress          :IA5STRING:'me@myhost.mydomain'
Certificate is to be certified until Sep 11 19:09:51 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
root@Cell_Router:/etc/easy-rsa# cd /etc/easy-rsa/keys/
root@Cell_Router:/etc/easy-rsa/keys# cp ca.
ca.crt  ca.key
root@Cell_Router:/etc/easy-rsa/keys# cp ca.crt ca.key dh2048.pem ser
serial      serial.old  server.crt  server.csr  server.key
root@Cell_Router:/etc/easy-rsa/keys# cp ca.crt ca.key dh2048.pem ser
serial      serial.old  server.crt  server.csr  server.key
root@Cell_Router:/etc/easy-rsa/keys# cp ca.crt ca.key dh2048.pem server.key serv
er.crt /etc/open
openvpn/         openwrt_release  openwrt_version
root@Cell_Router:/etc/easy-rsa/keys# cp ca.crt ca.key dh2048.pem server.key serv
er.crt /etc/openvpn/
root@Cell_Router:/etc/easy-rsa/keys# 
```

9. Download key files to your computer by WinSCP. Login in WinSCP and copy files from router to Windows.



E:\testcase\OpenVPN

名字	大小
..	
01.pem	6 KB
02.pem	6 KB
ca.crt	2 KB
ca.key	2 KB
client.crt	6 KB
client.csr	2 KB
client.key	2 KB
dh2048.pem	1 KB
index.txt	1 KB
index.txt.attr	1 KB
index.txt.attr.old	1 KB
index.txt.old	1 KB
serial	1 KB
serial.old	1 KB
server.crt	6 KB
server.csr	2 KB
server.key	2 KB

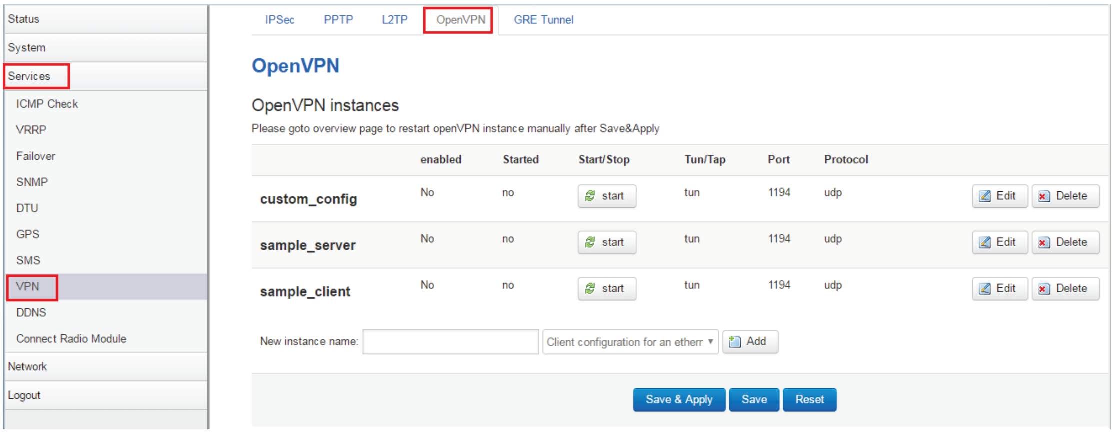
0 B / 32,138 B，0 / 17

/etc/easy-rsa/keys

名字	大小	已改变	权限	拥
..		9/13/2016 14:03	rwxr-xr-x	ro
01.pem	6 KB	9/13/2016 19:08	rw-r--r--	ro
02.pem	6 KB	9/13/2016 19:09	rw-r--r--	ro
ca.crt	2 KB	9/13/2016 14:04	rw-r--r--	ro
ca.key	2 KB	9/13/2016 14:04	rw-------	ro
client.crt	6 KB	9/13/2016 19:09	rw-r--r--	ro
client.csr	2 KB	9/13/2016 19:09	rw-r--r--	ro
client.key	2 KB	9/13/2016 19:09	rw-------	ro
dh2048.pem	1 KB	9/13/2016 18:57	rw-r--r--	ro
index.txt	1 KB	9/13/2016 19:09	rw-r--r--	ro
index.txt.attr	1 KB	9/13/2016 19:09	rw-r--r--	ro
index.txt.attr.old	1 KB	9/13/2016 19:08	rw-r--r--	ro
index.txt.old	1 KB	9/13/2016 19:08	rw-r--r--	ro
serial	1 KB	9/13/2016 19:09	rw-r--r--	ro
serial.old	1 KB	9/13/2016 19:08	rw-r--r--	ro
server.crt	6 KB	9/13/2016 19:08	rw-r--r--	ro
server.csr	2 KB	9/13/2016 19:07	rw-r--r--	ro
server.key	2 KB	9/13/2016 19:07	rw-------	ro

0 B / 32,138 B，0 / 17

10. Open management page on the router which generate keys. Click “Services” → “VPN” at left navigation bar, and then click “OpenVPN”.



OpenVPN

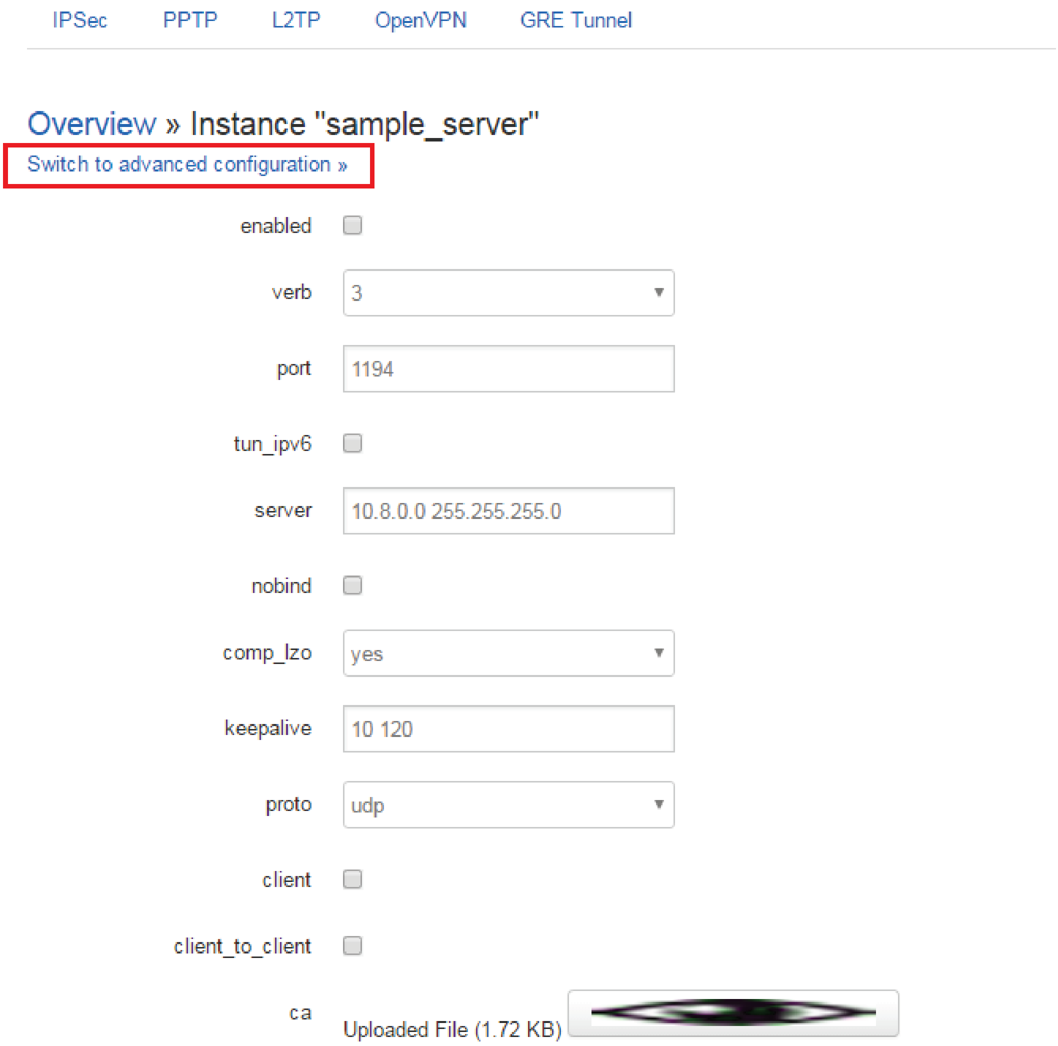
OpenVPN instances

Please goto overview page to restart openVPN instance manually after Save&Apply

	enabled	Started	Start/Stop	Tun/Tap	Port	Protocol	
custom_config	No	no	start	tun	1194	udp	Edit Delete
sample_server	No	no	start	tun	1194	udp	Edit Delete
sample_client	No	no	start	tun	1194	udp	Edit Delete

New instance name: Client configuration for an etherr Add

11. Click button “Edit” at the same line of sample_server. Then click “Switch to advanced configuration”.



Overview » Instance "sample_server"

Switch to advanced configuration »

enabled □

verb 3

port 1194

tun_ipv6 □

server 10.8.0.0 255.255.255.0

nobind □

comp_lzo yes

keepalive 10 120

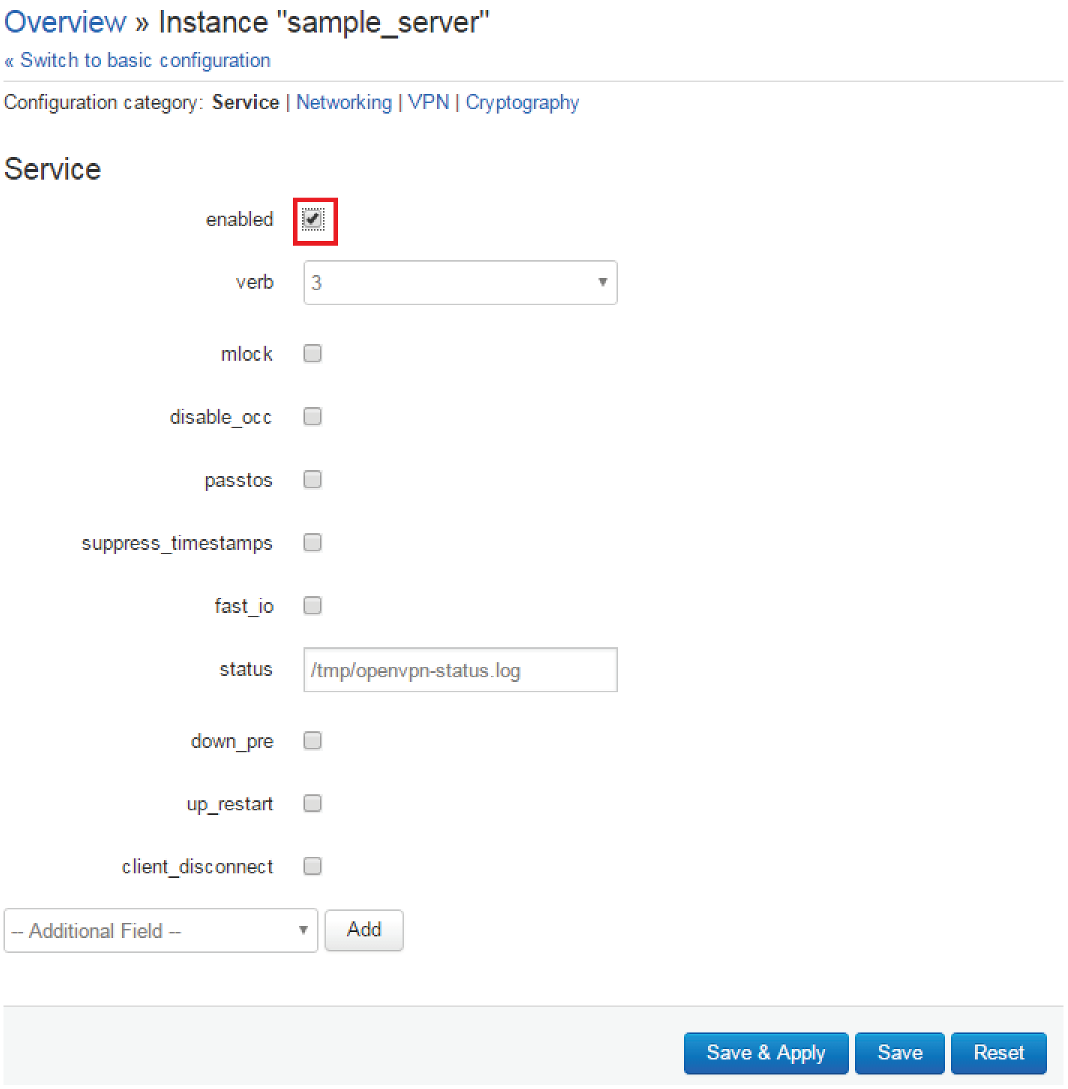
proto udp

client □

client_to_client □

ca Uploaded File (1.72 KB)

12. Click “Enable”, and press button “Save & Apply” to use the default configuration for OpenVPN server.



Overview » Instance "sample_server"

« Switch to basic configuration

Configuration category: **Service** | Networking | VPN | Cryptography

Service

enabled ☑

verb 3

mlock □

disable_occ □

passtos □

suppress_timestamps □

fast_io □

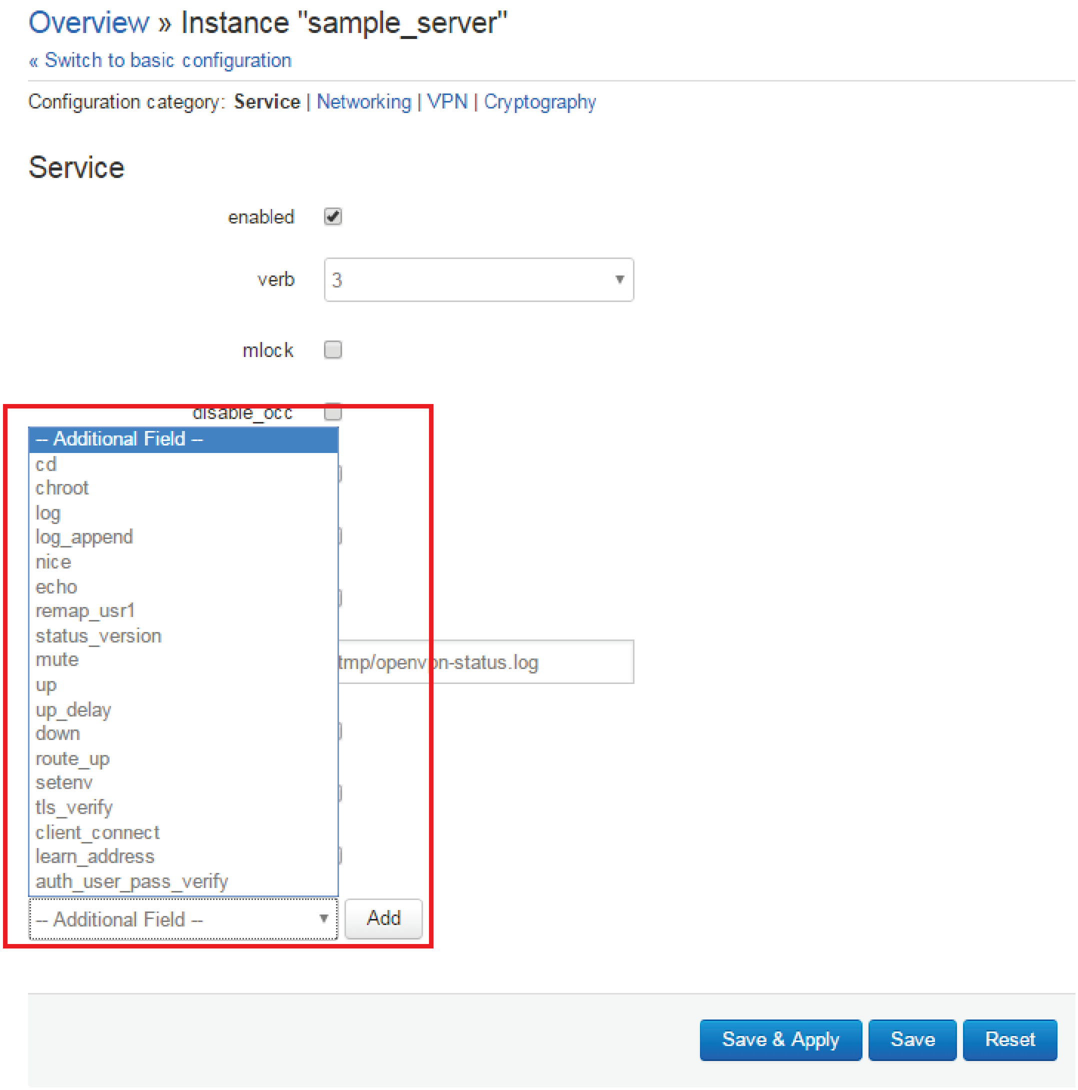
status /tmp/openvpn-status.log

down_pre □

up_restart □

client_disconnect □

13. If the default configuration is not you want, you can click "- Additional Field-" to add more fields.



Overview » Instance "sample_server"

« Switch to basic configuration

Configuration category: **Service** | Networking | VPN | Cryptography

Service

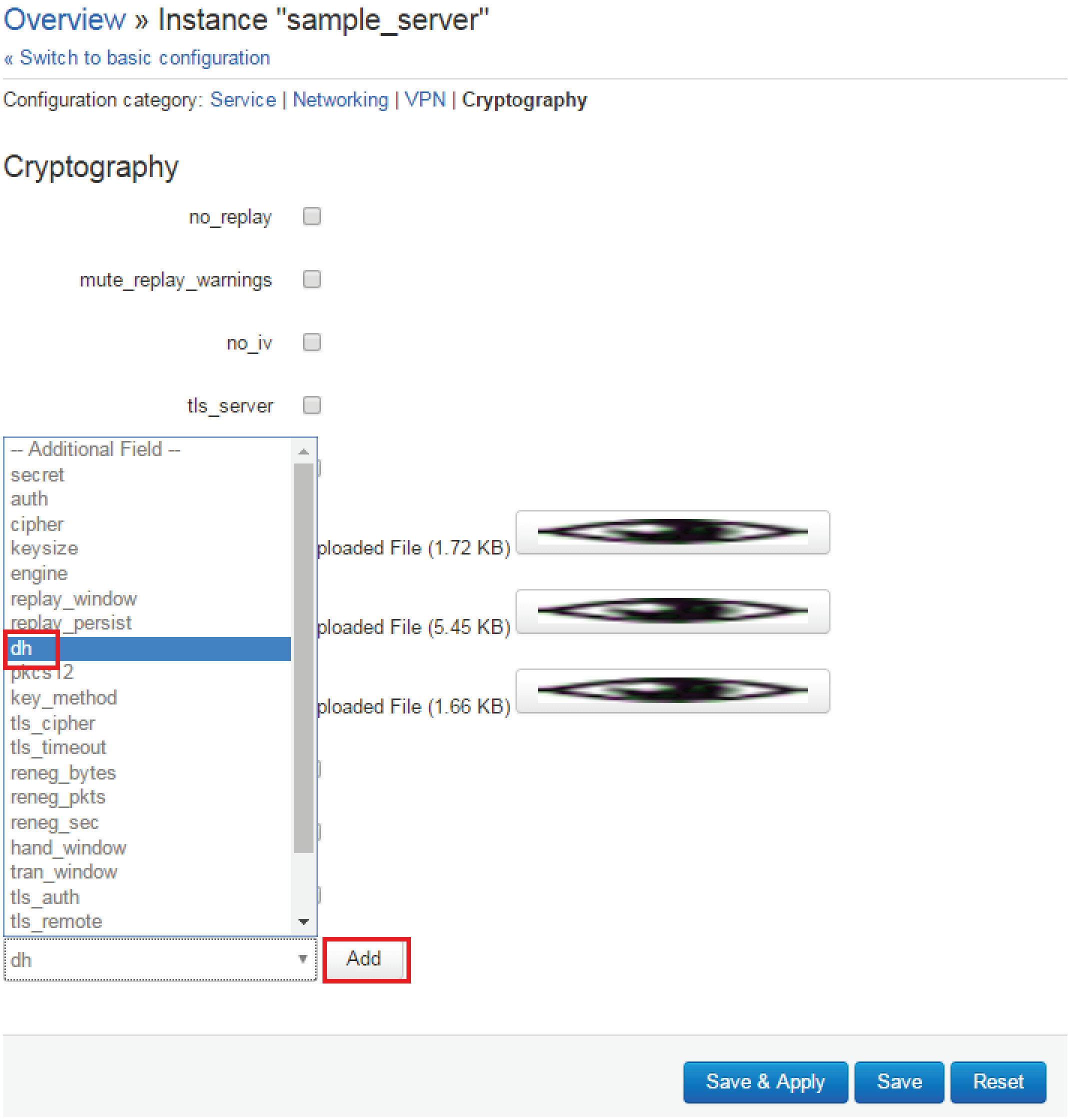
enabled ☑

verb 3

mlock □

disable_occ □

14. Switch to “Cryptography”. Click “- Additional Field -”, select “ca”(ca.crt)“dh”, then click button “Add”.



Overview » Instance "sample_server"

« Switch to basic configuration

Configuration category: Service | Networking | VPN | **Cryptography**

Cryptography

no_replay □

mute_replay_warnings □

no_iv □

tls_server □

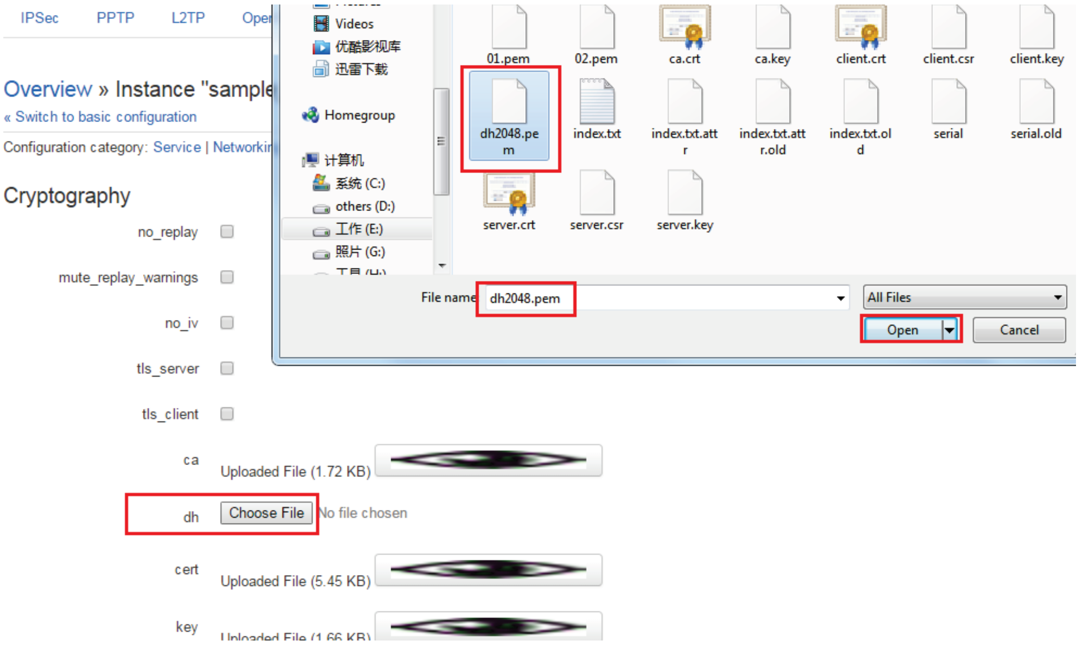
ploaded File (1.72 KB)

ploaded File (5.45 KB)

ploaded File (1.66 KB)

dh ▾ Add

15. Click button "Choose File" of dh, then select file "dh2048.pem". these key files were downloaded to windows at previous step.



Overview » Instance "sample

« Switch to basic configuration

Configuration category: Service | Networki

Cryptography

no_replay □

mute_replay_warnings □

no_iv □

tls_server □

tls_client □

ca Uploaded File (1.72 KB)

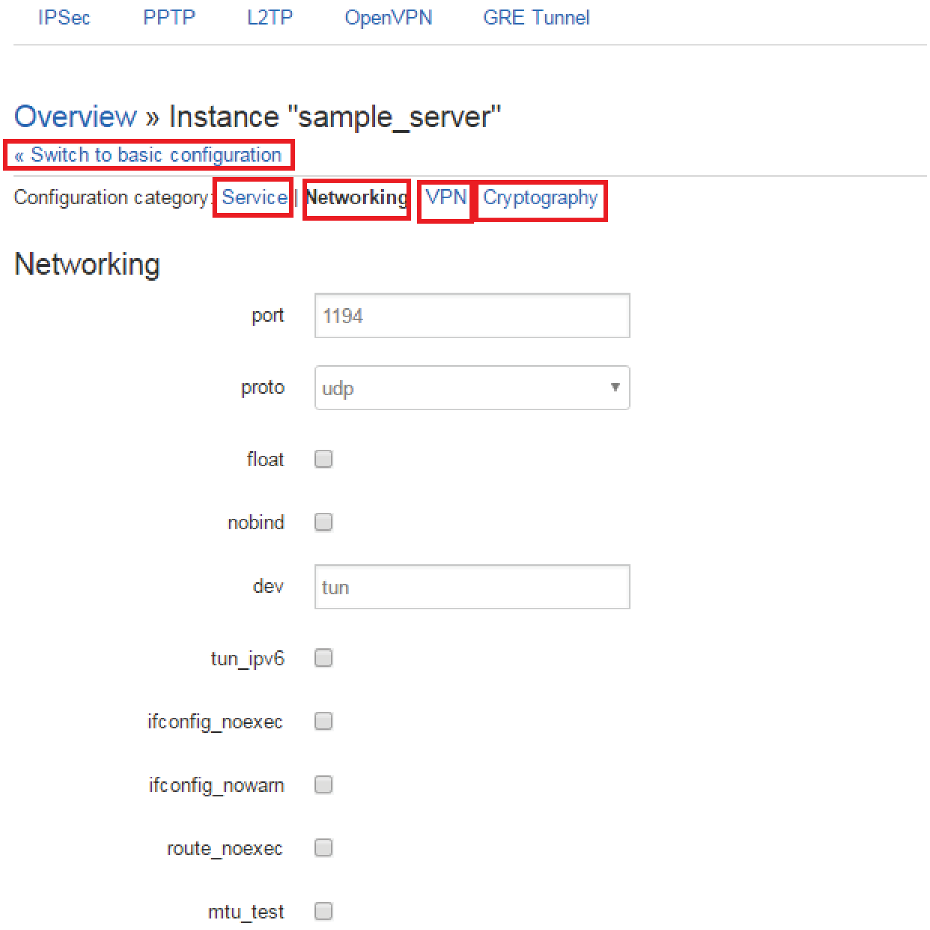
dh Choose File No file chosen

cert Uploaded File (5.45 KB)

key Uploaded File (1.66 KB)

File name dh2048.pem

16. You can switch to “Service”, “Networking”, “ VPN” and “Cryptography” to configure more. But before switching to other taboption, you must press button “Save” to avoid losing configuration



Overview » Instance "sample_server"

« Switch to basic configuration

Configuration category: Service | Networking | VPN | Cryptography

Networking

port 1194

proto udp

float □

nobind □

dev tun

tun_ipv6 □

ifconfig_noexec □

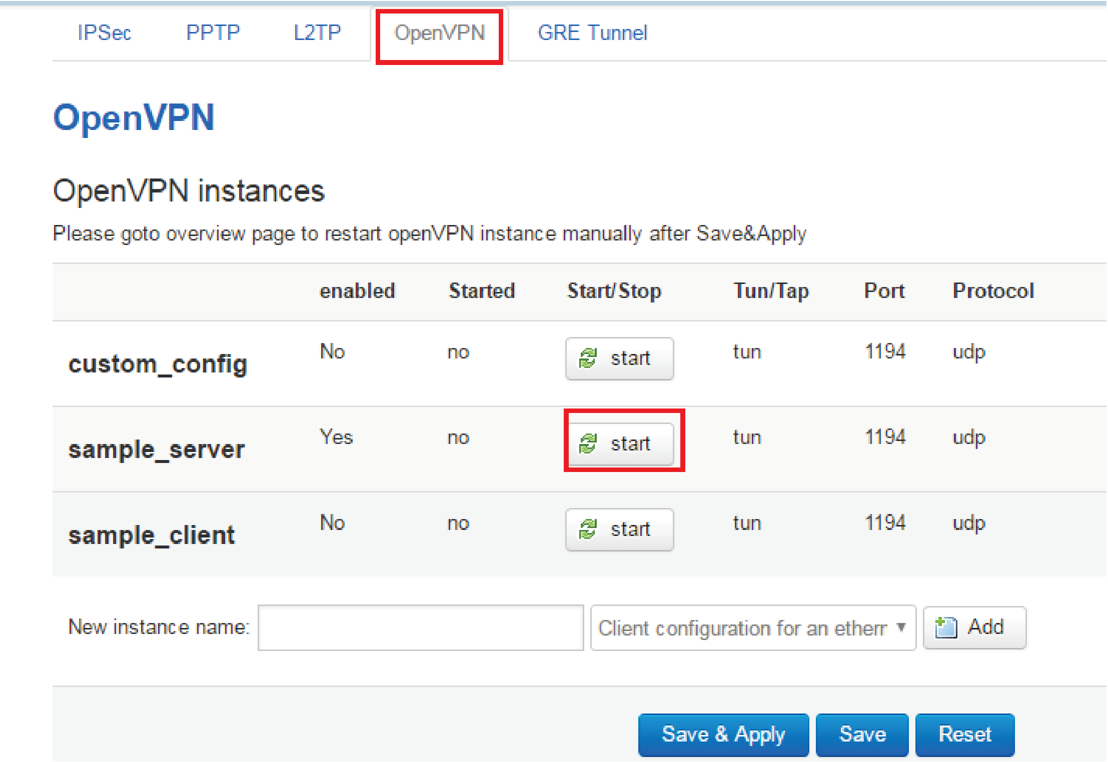
ifconfig_nowarn □

route_noexec □

mtu_test □

17. If all settings are done, click button “Save & Apply”.

18. Goto OpenVPN overview page to start sample_server by click button “start”.



OpenVPN

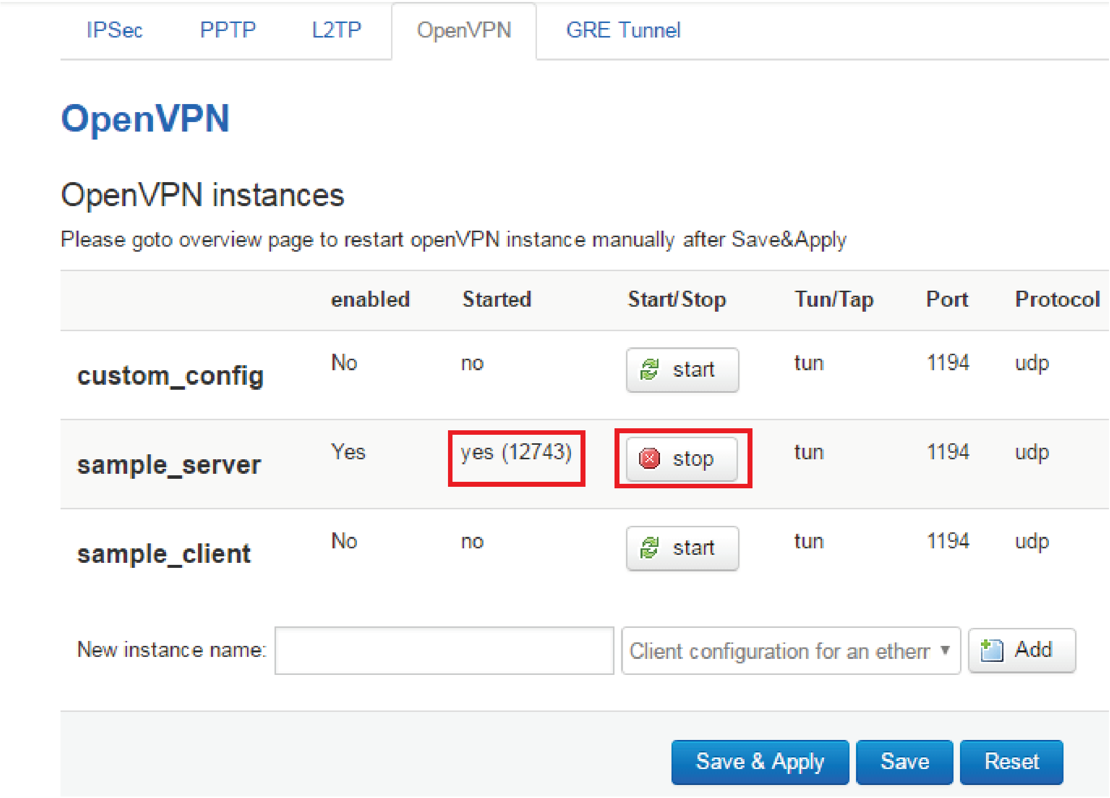
OpenVPN instances

Please goto overview page to restart openVPN instance manually after Save&Apply

	enabled	Started	Start/Stop	Tun/Tap	Port	Protocol
custom_config	No	no	start	tun	1194	udp
sample_server	Yes	no	start	tun	1194	udp
sample_client	No	no	start	tun	1194	udp

New instance name: Client configuration for an etherr

19. If “Started” is changed from “start” to “Yes(XXX)”, that means server started successfully. And you can stop it by click button “Stop”.



OpenVPN

OpenVPN instances

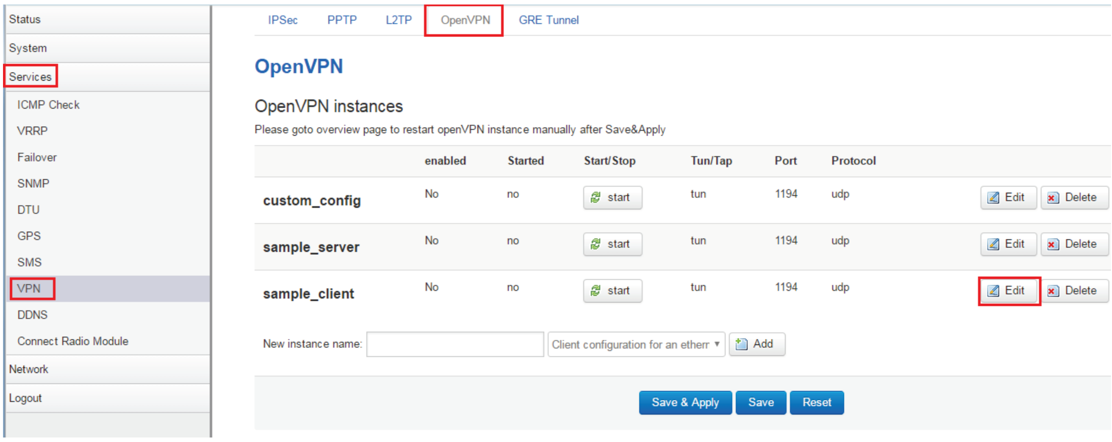
Please goto overview page to restart openVPN instance manually after Save&Apply

	enabled	Started	Start/Stop	Tun/Tap	Port	Protocol
custom_config	No	no	start	tun	1194	udp
sample_server	Yes	yes (12743)	stop	tun	1194	udp
sample_client	No	no	start	tun	1194	udp

New instance name: Client configuration for an etherr

Configuration OpenVPN client.

1. Open management page on the router which generate keys. Click "Services" → "VPN" at left navigation bar, and then click "OpenVPN". Click button "Edit" at the same line of "sample_client".



OpenVPN

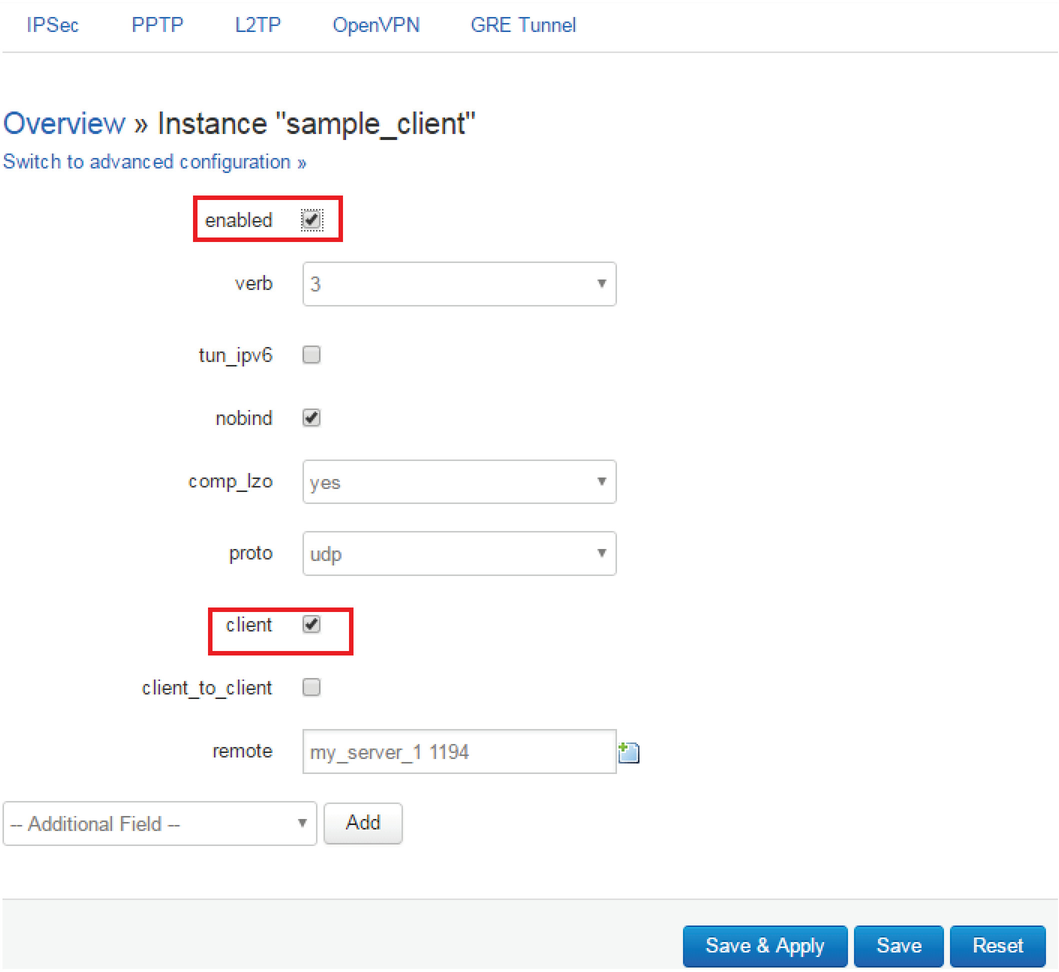
OpenVPN instances

Please goto overview page to restart openVPN instance manually after Save&Apply

	enabled	Started	Start/Stop	Tun/Tap	Port	Protocol	
custom_config	No	no	start	tun	1194	udp	Edit Delete
sample_server	No	no	start	tun	1194	udp	Edit Delete
sample_client	No	no	start	tun	1194	udp	Edit Delete

New instance name: Client configuration for an etherr ▾ Add

2. Make sure "Enable" and "Client" are checked. Then click button "Save".



Overview » Instance "sample_client"

Switch to advanced configuration »

enabled ☑

verb 3 ▾

tun_ipv6 □

nobind ☑

comp_lzo yes ▾

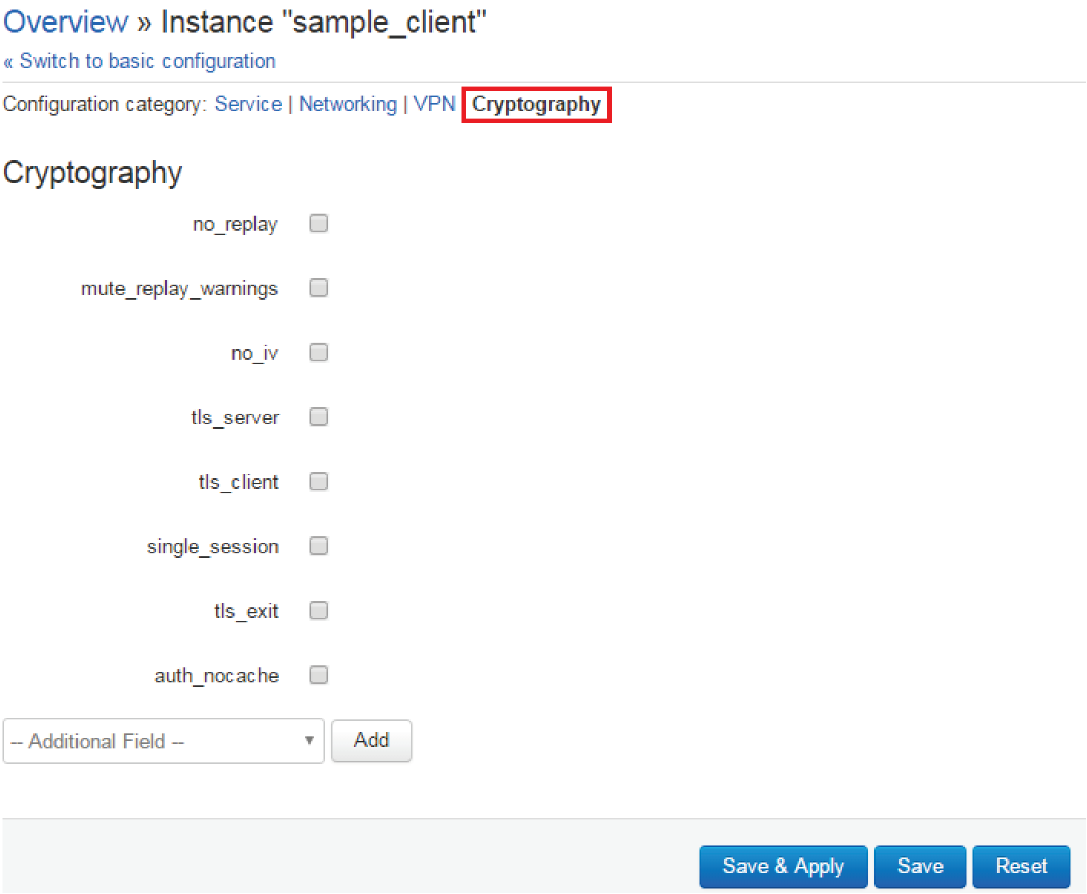
proto udp ▾

client ☑

client_to_client □

remote my_server_1 1194

3. Click "Switch to advanced configuration", and then click "Cryptography".



Overview » Instance "sample_client"

« Switch to basic configuration

Configuration category: Service | Networking | VPN | Cryptography

Cryptography

no_replay □

mute_replay_warnings □

no_iv □

tls_server □

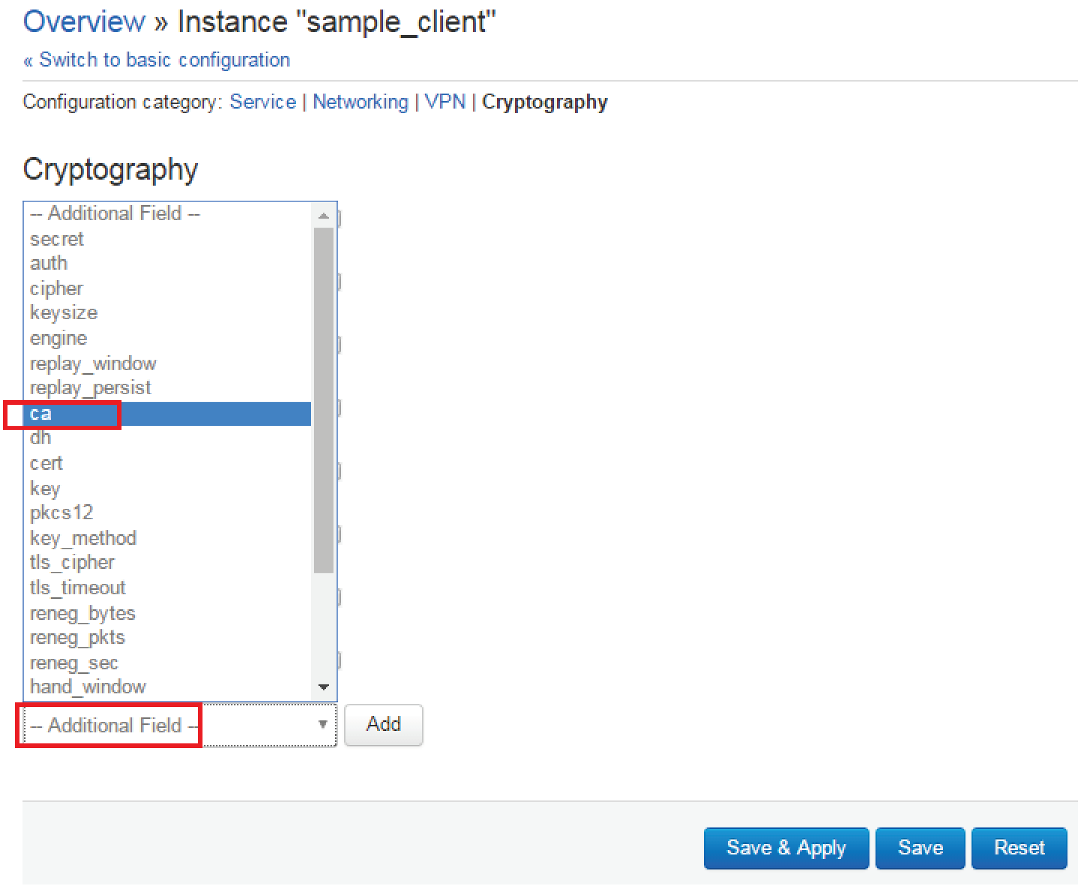
tls_client □

single_session □

tls_exit □

auth_nocache □

4. Click “- Additional Field -” then select “ca”.



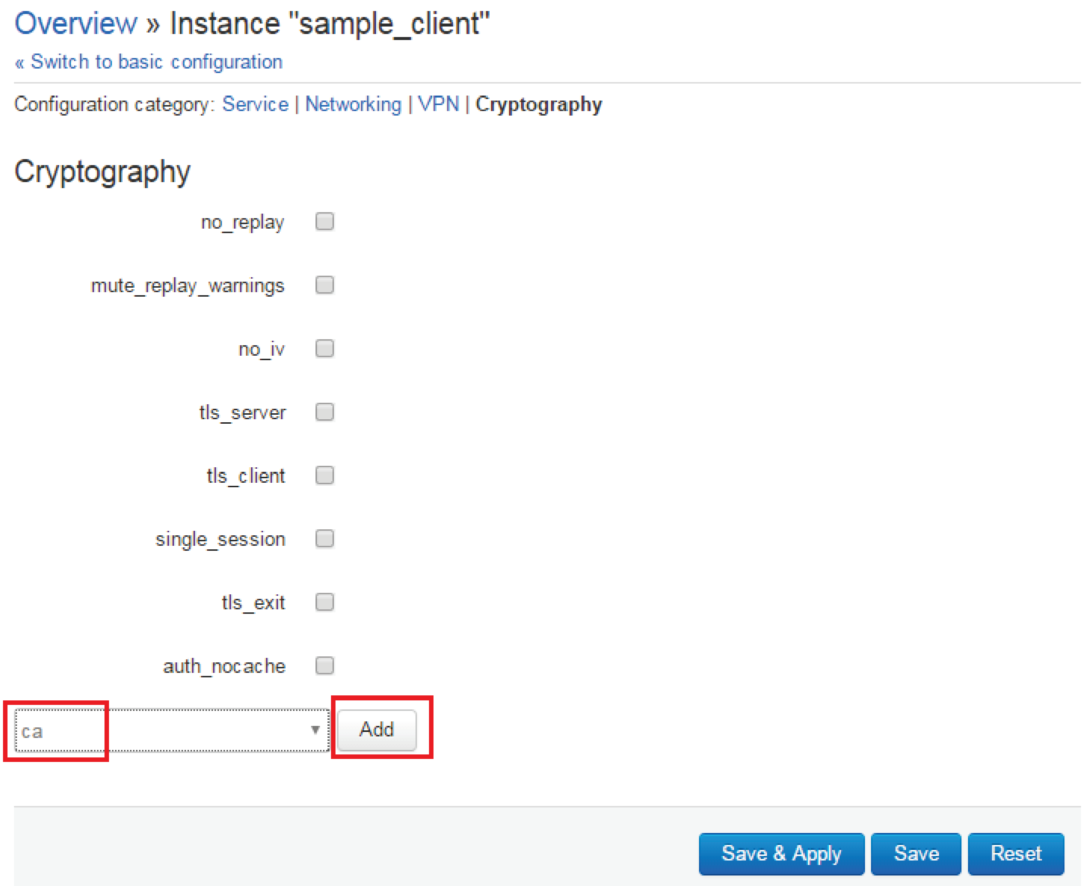
Overview » Instance "sample_client"

« Switch to basic configuration

Configuration category: Service | Networking | VPN | **Cryptography**

Cryptography

5. Click button “Add”.



Overview » Instance "sample_client"

« Switch to basic configuration

Configuration category: Service | Networking | VPN | **Cryptography**

Cryptography

no_replay □

mute_replay_warnings □

no_iv □

tls_server □

tls_client □

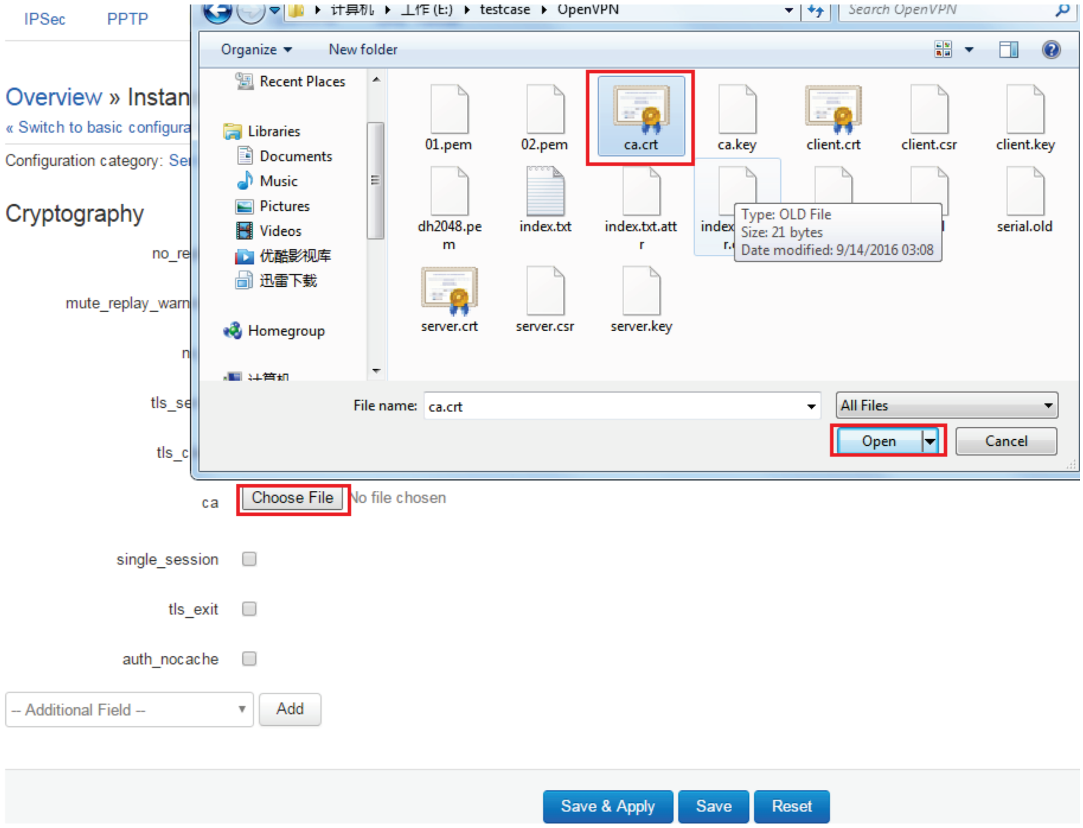
single_session □

tls_exit □

auth_nocache □

ca ▾ Add

6. Click button “Choose File” of ca, then open key files “ca.crt”. These key files were downloaded to windows by previous step.



Type: OLD File
Size: 21 bytes
Date modified: 9/14/2016 03:08

File name: ca.crt

All Files

ca Choose File No file chosen

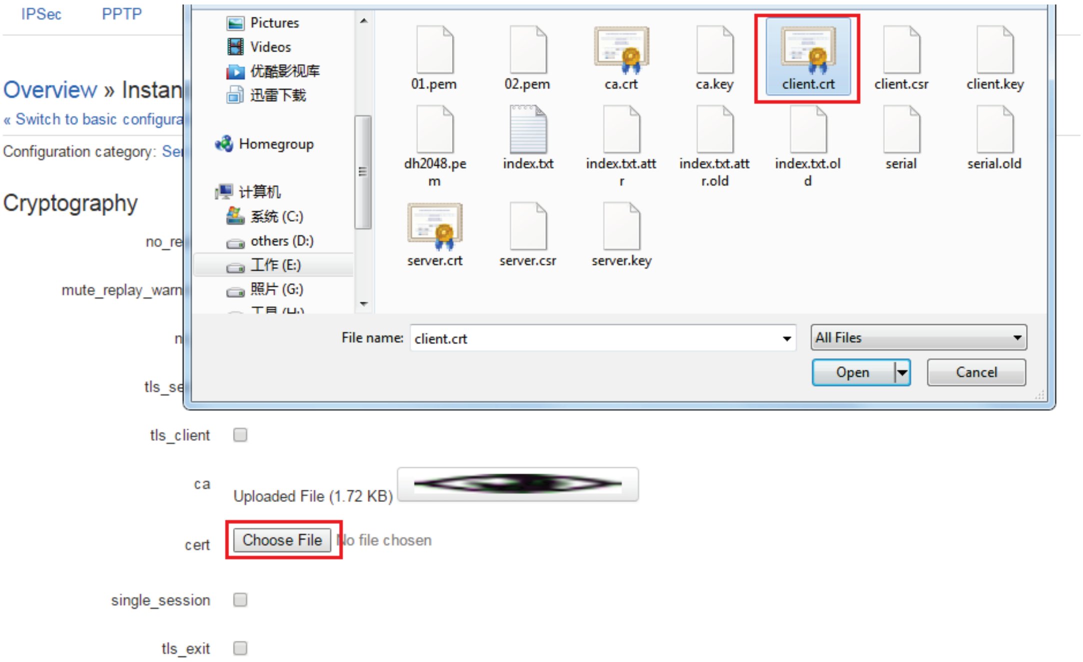
single_session □

tls_exit □

auth_nocache □

-- Additional Field -- ▾ Add

7. Add field “cert” and choose key file “client.crt”.

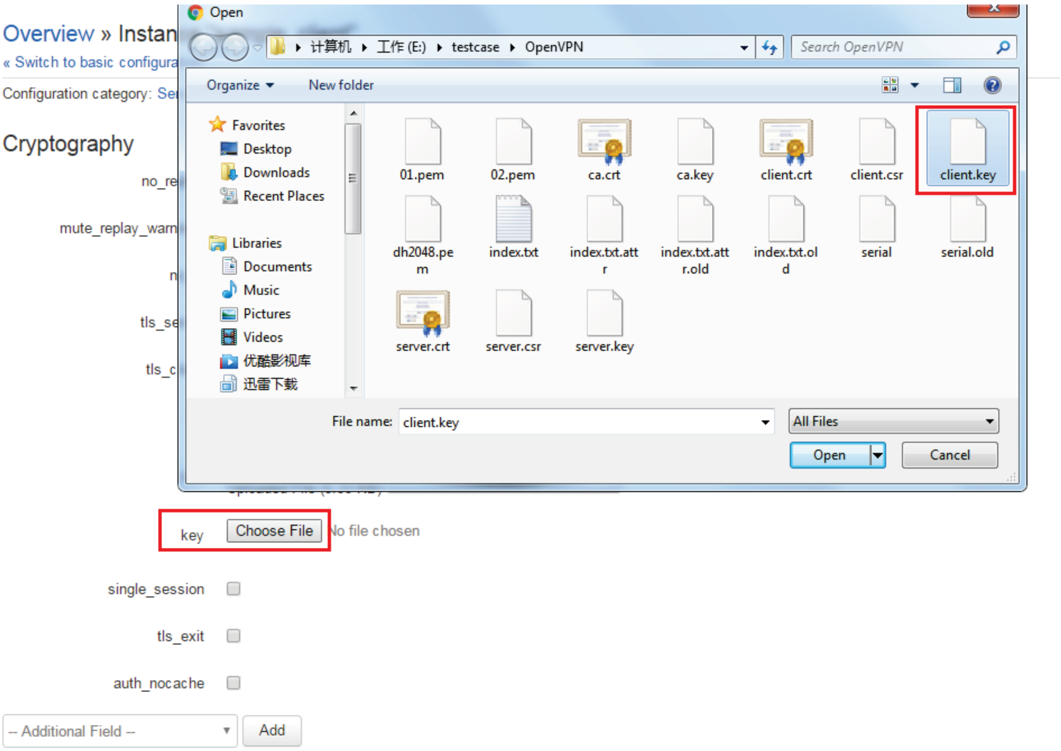


File name: client.crt

ca: Uploaded File (1.72 KB) [redacted]

cert: Choose File No file chosen

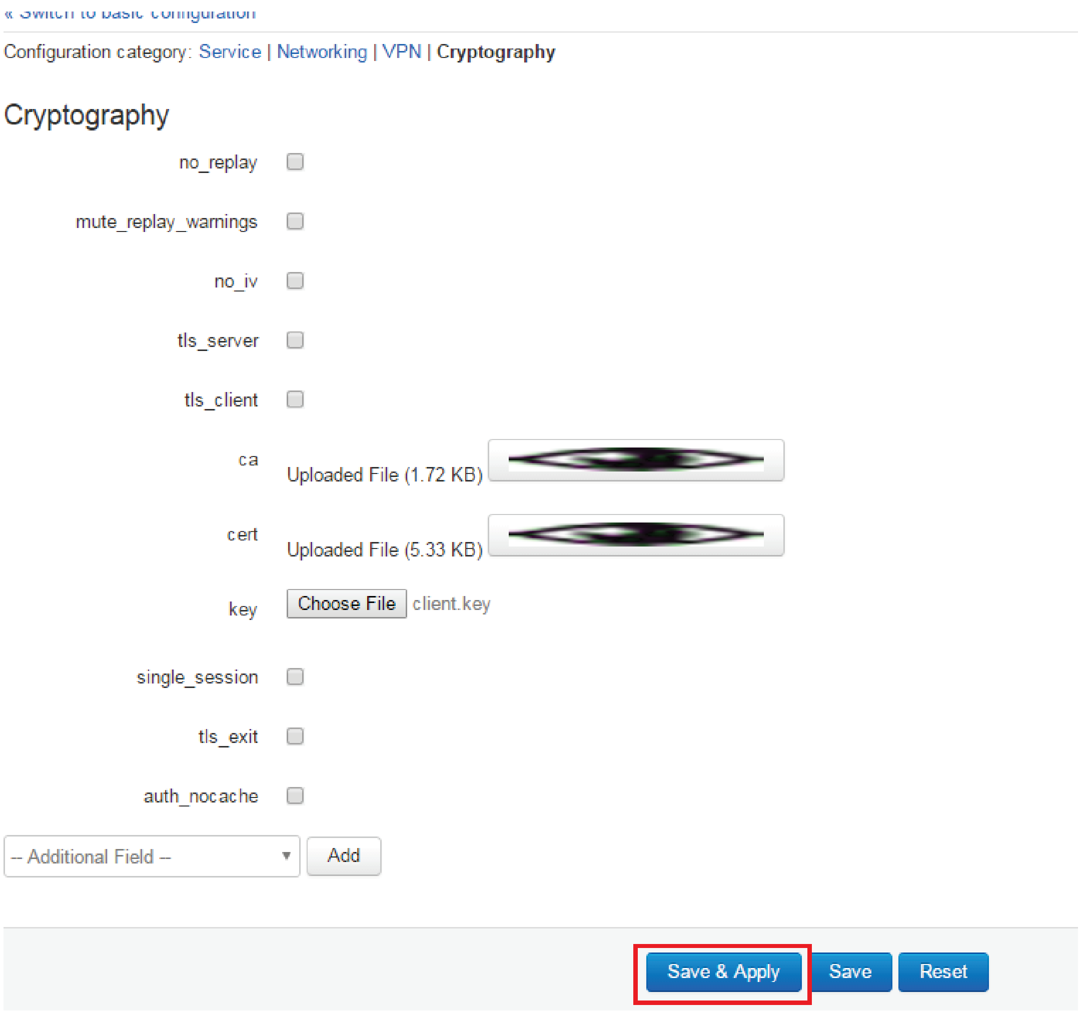
8. Add field “key” and choose key file “client.key”.



File name: client.key

key: Choose File No file chosen

9. Click button “Save & Apply” or “Save” to save configration.



« Switch to basic configuration

Configuration category: Service | Networking | VPN | **Cryptography**

Cryptography

no_replay ☐

mute_replay_warnings ☐

no_iv ☐

tls_server ☐

tls_client ☐

ca Uploaded File (1.72 KB) [redacted]

cert Uploaded File (5.33 KB) [redacted]

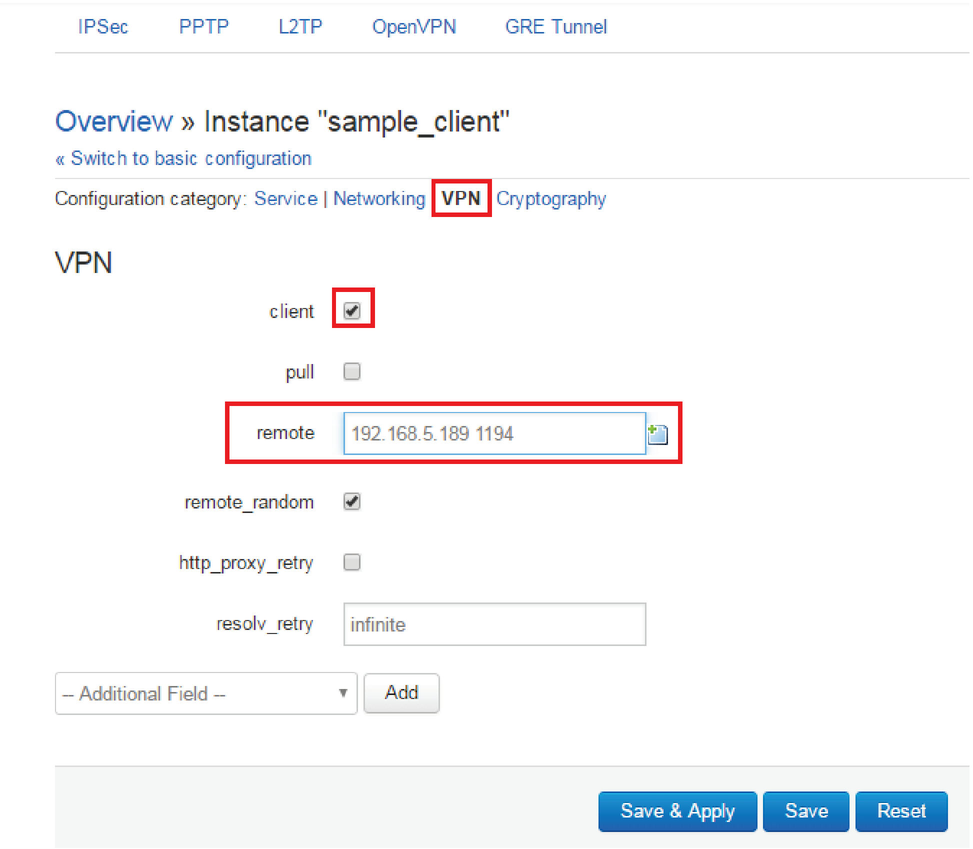
key Choose File client.key

single_session ☐

tls_exit ☐

auth_nocache ☐

10. Switch to “VPN”, modify the remote, here we have OpenVPN server on router “192.168.5.189” with port “1194”. Then click button “Save & Apply”.



Overview » Instance "sample_client"

« Switch to basic configuration

Configuration category: Service | Networking | VPN | Cryptography

VPN

client ☑

pull □

remote 192.168.5.189 1194

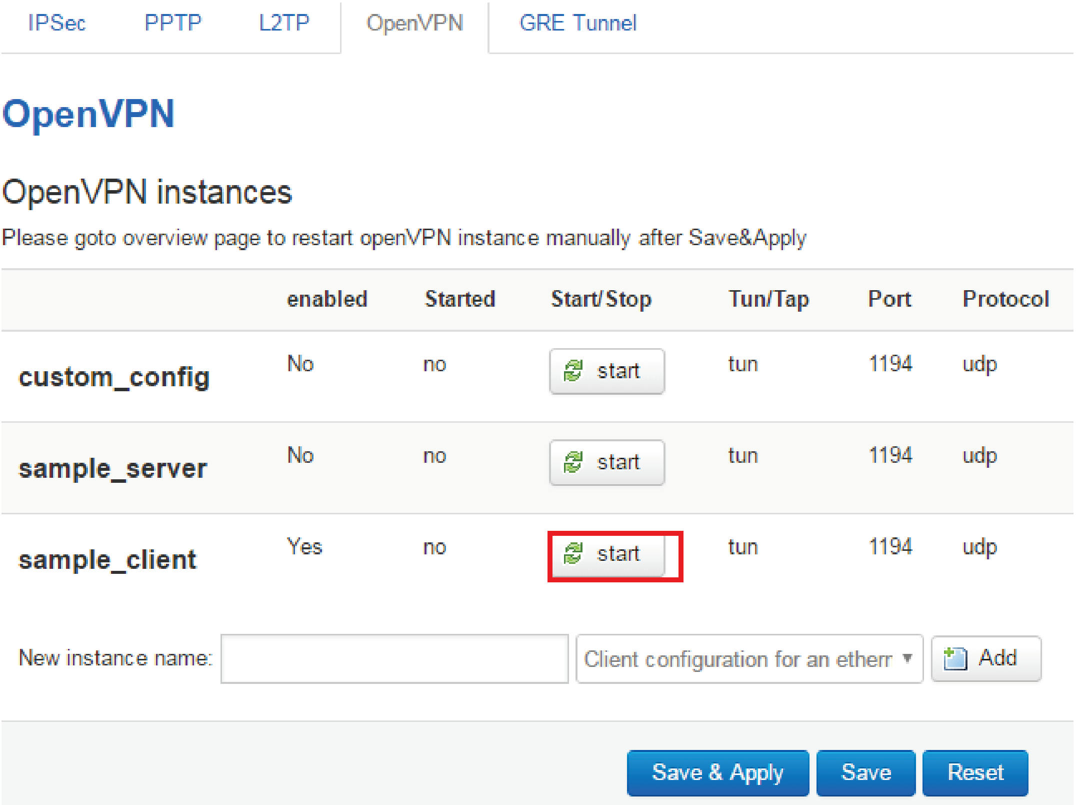
remote_random ☑

http_proxy_retry □

resolv_retry infinite

-- Additional Field --

11. Goto OpenVPN overview page to start sample_client by click button "start"



OpenVPN

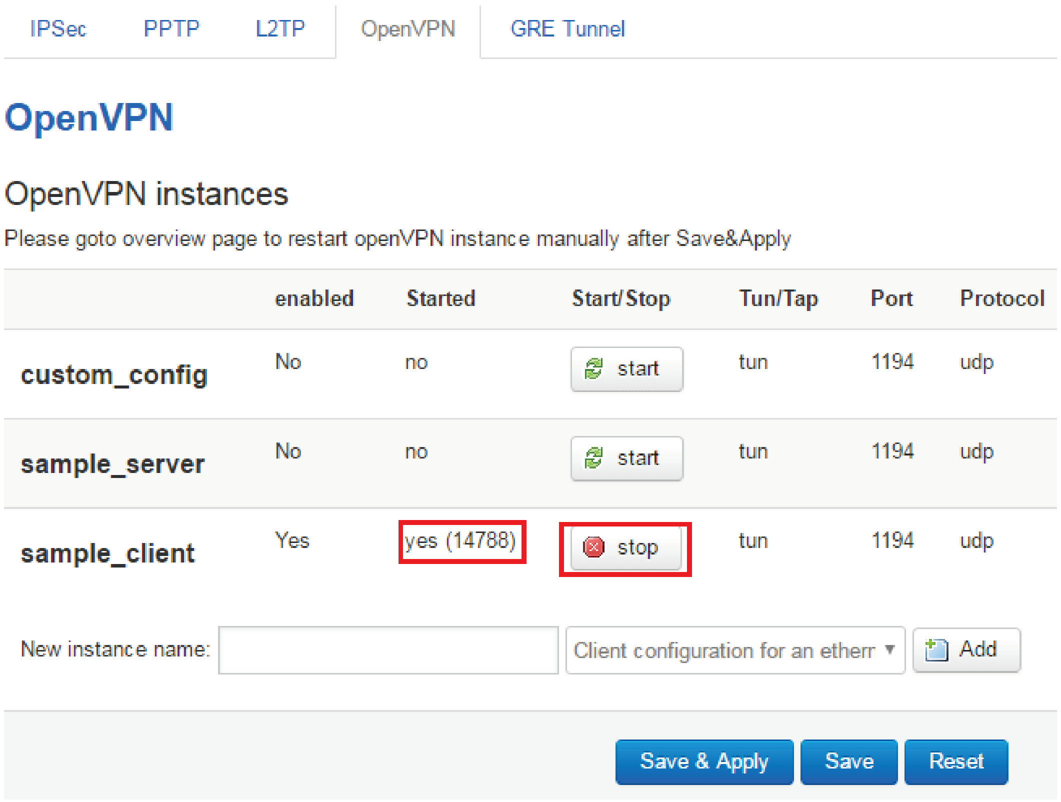
OpenVPN instances

Please goto overview page to restart openVPN instance manually after Save&Apply

	enabled	Started	Start/Stop	Tun/Tap	Port	Protocol
custom_config	No	no	start	tun	1194	udp
sample_server	No	no	start	tun	1194	udp
sample_client	Yes	no	start	tun	1194	udp

New instance name: Client configuration for an etherr

12. If "Started" is changed from "start" to "Yes(XXX)", that means server started successfully. And you can stop it by click button "Stop".



OpenVPN

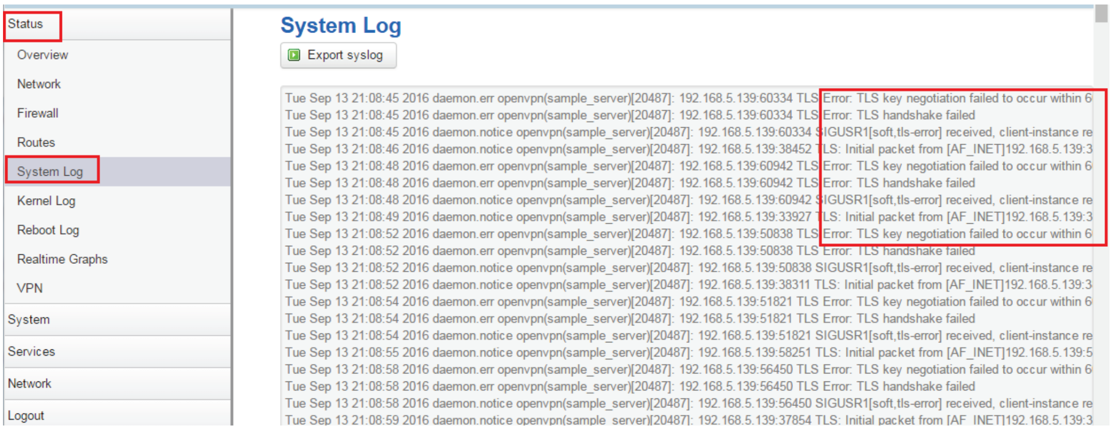
OpenVPN instances

Please goto overview page to restart openVPN instance manually after Save&Apply

	enabled	Started	Start/Stop	Tun/Tap	Port	Protocol
custom_config	No	no	start	tun	1194	udp
sample_server	No	no	start	tun	1194	udp
sample_client	Yes	yes (14788)	stop	tun	1194	udp

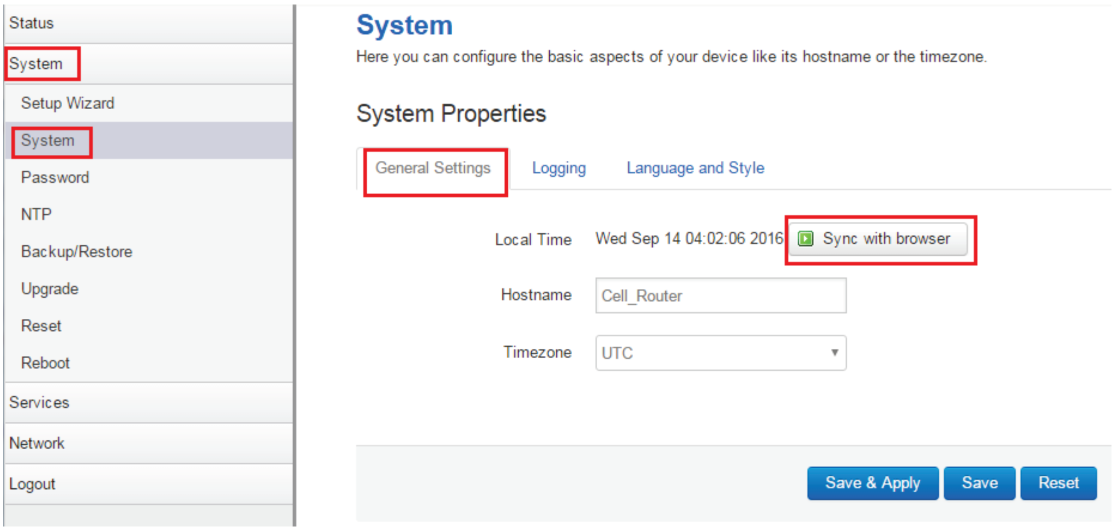
New instance name: Client configuration for an etherr

13. Check systemlog, if “Error: TLS handshake failed”, that means OpenVPN server and OpenVPN’s local time is inconsistency. Please go to “System”→”System” to Sync router’s time with browser at both side.



```
Tue Sep 13 21:08:45 2016 daemon.err openvpn(sample_server)[20487]: 192.168.5.139:60334 TLS Error: TLS key negotiation failed to occur within 6
Tue Sep 13 21:08:45 2016 daemon.err openvpn(sample_server)[20487]: 192.168.5.139:60334 TLS Error: TLS handshake failed
Tue Sep 13 21:08:45 2016 daemon.notice openvpn(sample_server)[20487]: 192.168.5.139:60334 SIGUSR1[soft,tls-error] received, client-instance re
Tue Sep 13 21:08:46 2016 daemon.notice openvpn(sample_server)[20487]: 192.168.5.139:38452 TLS: Initial packet from [AF_INET]192.168.5.139:3
Tue Sep 13 21:08:48 2016 daemon.err openvpn(sample_server)[20487]: 192.168.5.139:60942 TLS Error: TLS key negotiation failed to occur within 6
Tue Sep 13 21:08:48 2016 daemon.err openvpn(sample_server)[20487]: 192.168.5.139:60942 TLS Error: TLS handshake failed
Tue Sep 13 21:08:48 2016 daemon.notice openvpn(sample_server)[20487]: 192.168.5.139:60942 SIGUSR1[soft,tls-error] received, client-instance re
Tue Sep 13 21:08:49 2016 daemon.notice openvpn(sample_server)[20487]: 192.168.5.139:33927 TLS: Initial packet from [AF_INET]192.168.5.139:3
Tue Sep 13 21:08:52 2016 daemon.err openvpn(sample_server)[20487]: 192.168.5.139:50838 TLS Error: TLS key negotiation failed to occur within 6
Tue Sep 13 21:08:52 2016 daemon.err openvpn(sample_server)[20487]: 192.168.5.139:50838 TLS Error: TLS handshake failed
Tue Sep 13 21:08:52 2016 daemon.notice openvpn(sample_server)[20487]: 192.168.5.139:50838 SIGUSR1[soft,tls-error] received, client-instance re
Tue Sep 13 21:08:52 2016 daemon.notice openvpn(sample_server)[20487]: 192.168.5.139:38311 TLS: Initial packet from [AF_INET]192.168.5.139:3
Tue Sep 13 21:08:54 2016 daemon.err openvpn(sample_server)[20487]: 192.168.5.139:51821 TLS Error: TLS key negotiation failed to occur within 6
Tue Sep 13 21:08:54 2016 daemon.err openvpn(sample_server)[20487]: 192.168.5.139:51821 TLS Error: TLS handshake failed
Tue Sep 13 21:08:54 2016 daemon.notice openvpn(sample_server)[20487]: 192.168.5.139:51821 SIGUSR1[soft,tls-error] received, client-instance re
Tue Sep 13 21:08:55 2016 daemon.notice openvpn(sample_server)[20487]: 192.168.5.139:58251 TLS: Initial packet from [AF_INET]192.168.5.139:5
Tue Sep 13 21:08:58 2016 daemon.err openvpn(sample_server)[20487]: 192.168.5.139:56450 TLS Error: TLS key negotiation failed to occur within 6
Tue Sep 13 21:08:58 2016 daemon.err openvpn(sample_server)[20487]: 192.168.5.139:56450 TLS Error: TLS handshake failed
Tue Sep 13 21:08:58 2016 daemon.notice openvpn(sample_server)[20487]: 192.168.5.139:56450 SIGUSR1[soft,tls-error] received, client-instance re
Tue Sep 13 21:08:59 2016 daemon.notice openvpn(sample_server)[20487]: 192.168.5.139:37854 TLS: Initial packet from [AF_INET]192.168.5.139:3
```

Sync Local time with browser:



System

Here you can configure the basic aspects of your device like its hostname or the timezone.

System Properties

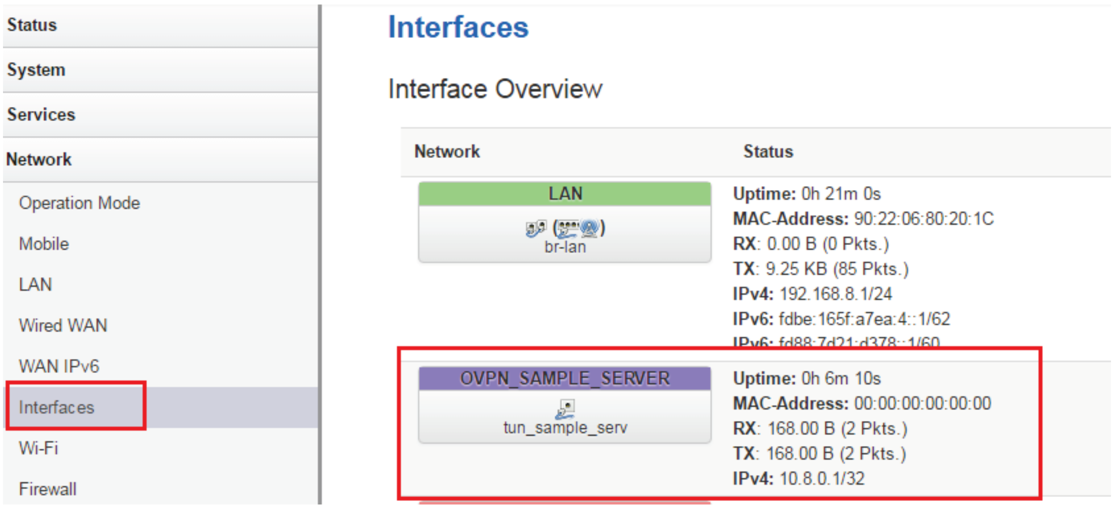
Local Time: Wed Sep 14 04:02:06 2016

Hostname: Cell_Router

Timezone: UTC

14. Now the tunnel between server and client should be setup successfully, client and server can access each other with virtual IP address 10.8.0.0/24. check the interface status at here:

    Server Side:

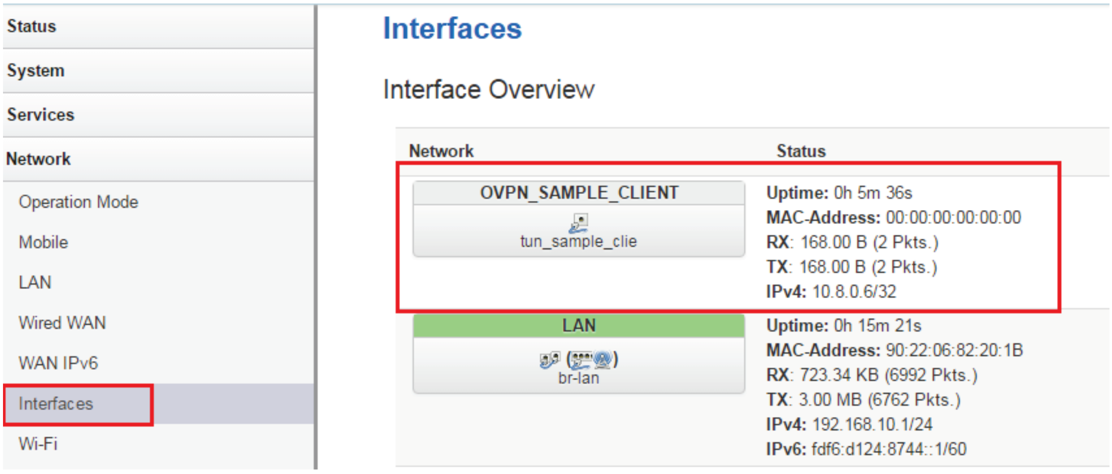


Interfaces

Interface Overview

Network	Status
LAN br-lan	**Uptime:** 0h 21m 0s **MAC-Address:** 90:22:06:80:20:1C **RX**: 0.00 B (0 Pkts.) **TX**: 9.25 KB (85 Pkts.) **IPv4:** 192.168.8.1/24 **IPv6:** fdbe:165f:a7ea:4::1/62 **IPv6:** fd88:7d21:d378::1/60
OVPN_SAMPLE_SERVER tun_sample_serv	**Uptime:** 0h 6m 10s **MAC-Address:** 00:00:00:00:00:00 **RX**: 168.00 B (2 Pkts.) **TX**: 168.00 B (2 Pkts.) **IPv4:** 10.8.0.1/32

Client side:



Interfaces

Interface Overview

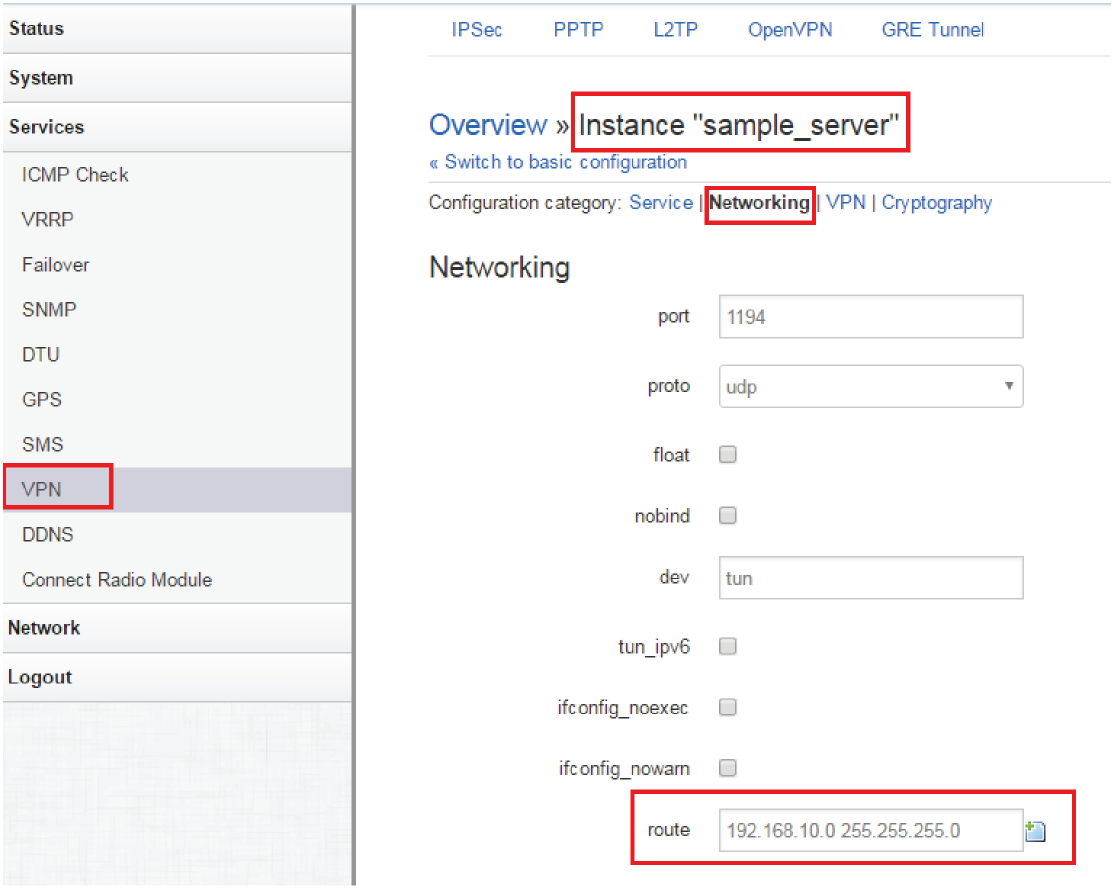
Network	Status
OVPN_SAMPLE_CLIENT tun_sample_clie	**Uptime:** 0h 5m 36s **MAC-Address:** 00:00:00:00:00:00 **RX**: 168.00 B (2 Pkts.) **TX**: 168.00 B (2 Pkts.) **IPv4:** 10.8.0.6/32
LAN br-lan	**Uptime:** 0h 15m 21s **MAC-Address:** 90:22:06:82:20:1B **RX**: 723.34 KB (6992 Pkts.) **TX**: 3.00 MB (6762 Pkts.) **IPv4:** 192.168.10.1/24 **IPv6:** fdf6:d124:8744::1/60

15. If you need to connect subnet behind server and client, we need to configure

server instance again.

Here server router subnet is 192.168.8.0/24, gateway is 192.168.8.1. Client subnet is 192.168.10.0/24, and gateway is 192.168.10.1.

16. Add route on server instance



Overview » Instance "sample_server"

« Switch to basic configuration

Configuration category: Service | Networking | VPN | Cryptography

Networking

port: 1194

proto: udp

float: □

nobind: □

dev: tun

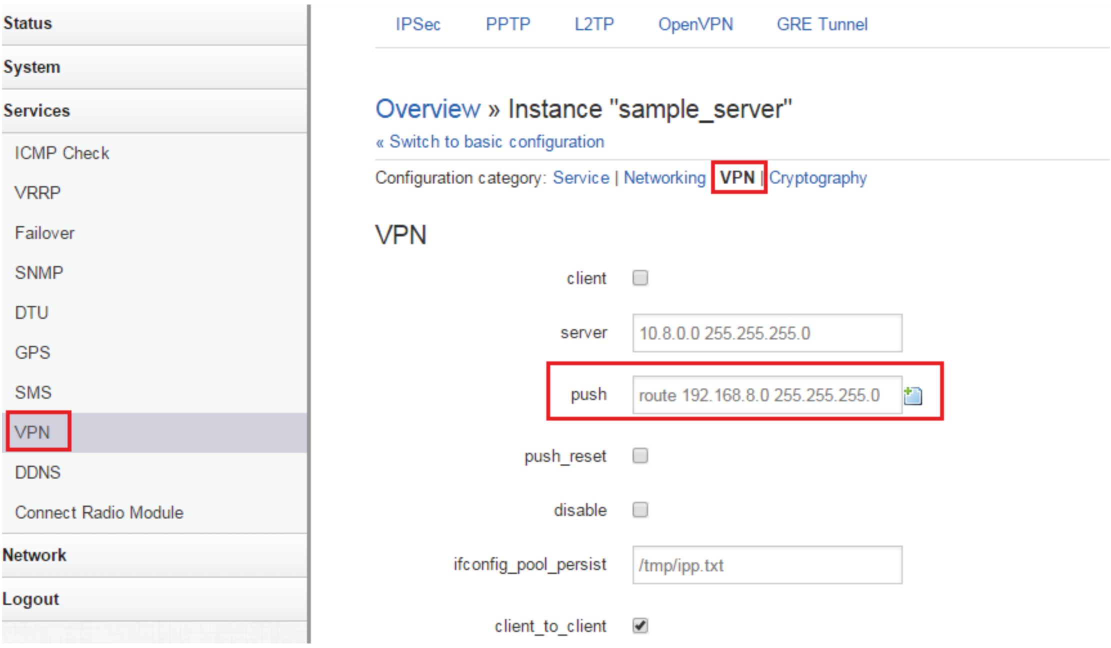
tun_ipv6: □

ifconfig_noexec: □

ifconfig_nowarn: □

route: 192.168.10.0 255.255.255.0

17. Add push on server



Overview » Instance "sample_server"

« Switch to basic configuration

Configuration category: Service | Networking | VPN | Cryptography

VPN

client: □

server: 10.8.0.0 255.255.255.0

push: route 192.168.8.0 255.255.255.0

push_reset: □

disable: □

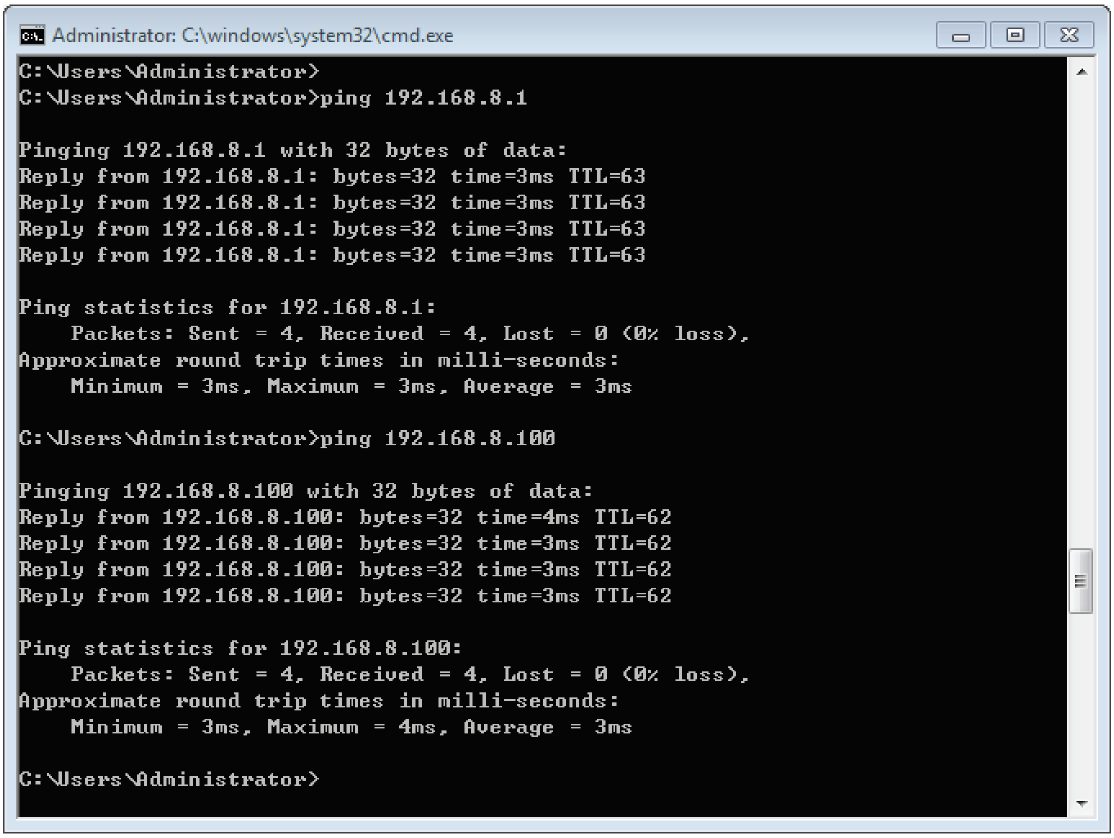
ifconfig_pool_persist: /tmp/ipp.txt

client_to_client: ☑

18. Save, then goto OpenVPN overview page to stop instance and then start this

instance.

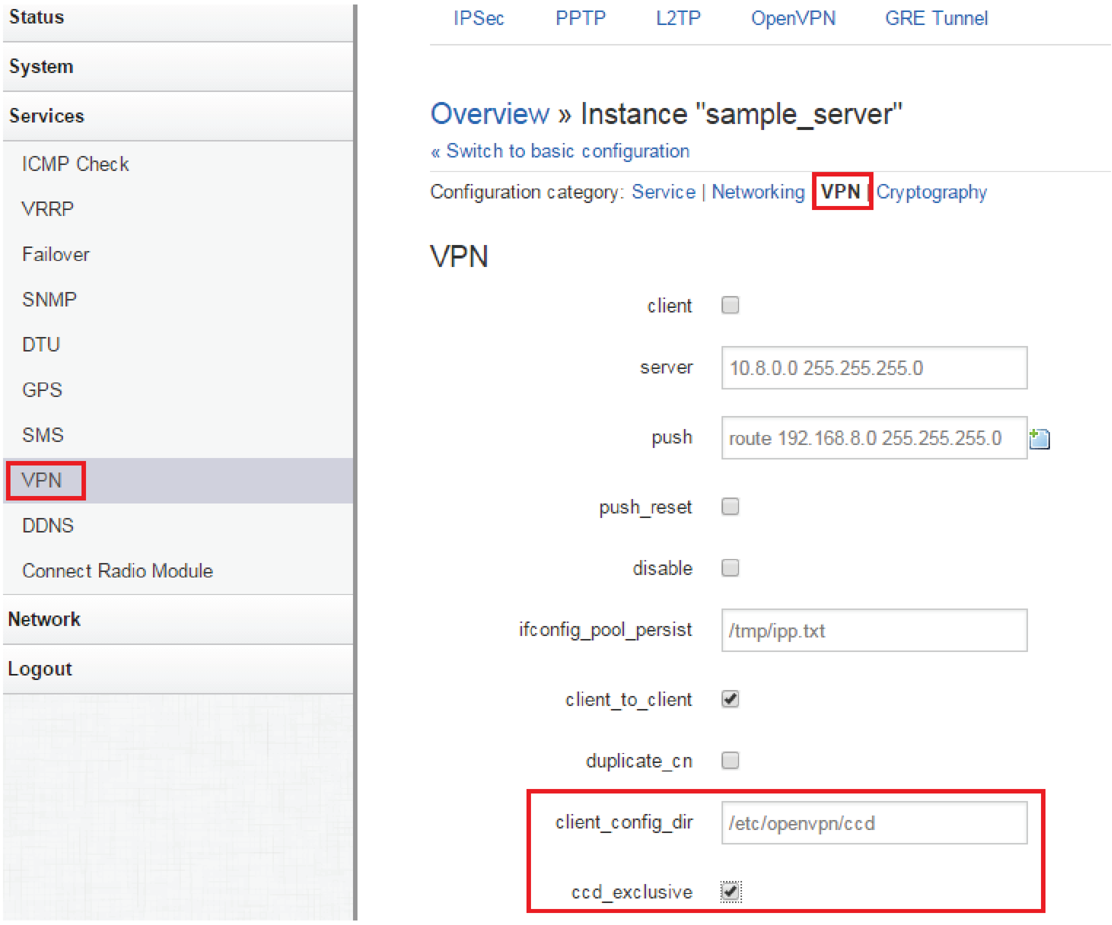
19. Ping from PC 192.168.10.171 which behind OpenVPN client.



```
C:\Users\Administrator>
C:\Users\Administrator>ping 192.168.8.1

Pinging 192.168.8.1 with 32 bytes of data:
Reply from 192.168.8.1: bytes=32 time=3ms TTL=63
Reply from 192.168.8.1: bytes=32 time=3ms TTL=63
Reply from 192.168.8.1: bytes=32 time=3ms TTL=63
Reply from 192.168.8.1: bytes=32 time=3ms TTL=63

Ping statistics for 192.168.8.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 3ms, Average = 3ms

C:\Users\Administrator>ping 192.168.8.100

Pinging 192.168.8.100 with 32 bytes of data:
Reply from 192.168.8.100: bytes=32 time=4ms TTL=62
Reply from 192.168.8.100: bytes=32 time=3ms TTL=62
Reply from 192.168.8.100: bytes=32 time=3ms TTL=62
Reply from 192.168.8.100: bytes=32 time=3ms TTL=62

Ping statistics for 192.168.8.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 4ms, Average = 3ms

C:\Users\Administrator>
```

20. If you want to ping from PC which is behind OpenVPN to the PC which is behind OpenVPN, such as ping from 192.168.8.100 to 192.168.10.171. we need to configure server again.

21. Add client_config_dir and ccd_exclusive



Overview » Instance "sample_server"

VPN

client □

server 10.8.0.0 255.255.255.0

push route 192.168.8.0 255.255.255.0

push_reset □

disable □

ifconfig_pool_persist /tmp/ipp.txt

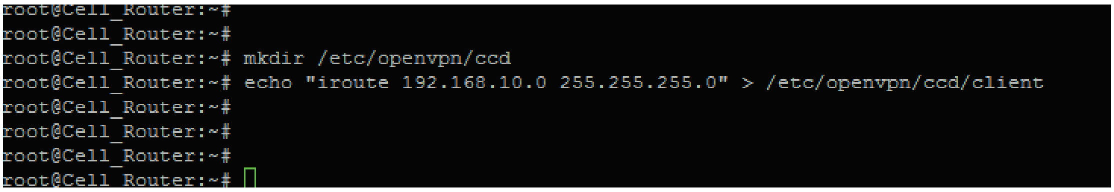
client_to_client ☑

duplicate_cn □

client_config_dir /etc/openvpn/ccd

ccd_exclusive ☑

22. Save.
23. SSH to server router, execute the follow two command



```
root@Cell_Router:~#
root@Cell_Router:~#
root@Cell_Router:~# mkdir /etc/openvpn/ccd
root@Cell_Router:~# echo "iroute 192.168.10.0 255.255.255.0" > /etc/openvpn/ccd/client
root@Cell_Router:~#
root@Cell_Router:~#
root@Cell_Router:~#
root@Cell_Router:~#
```

Path /etc/openvpn/ccd/ is client_config_dir, file name “client” is the same name in step 7. 192.168.10.0 255.255.255.0 is the subnet of client.

24. Stop server instance then start it, now ping from 192.168.8.100(server subnet) to 192.168.10.171(client subnet) should be successful. Then the site2site is complete.