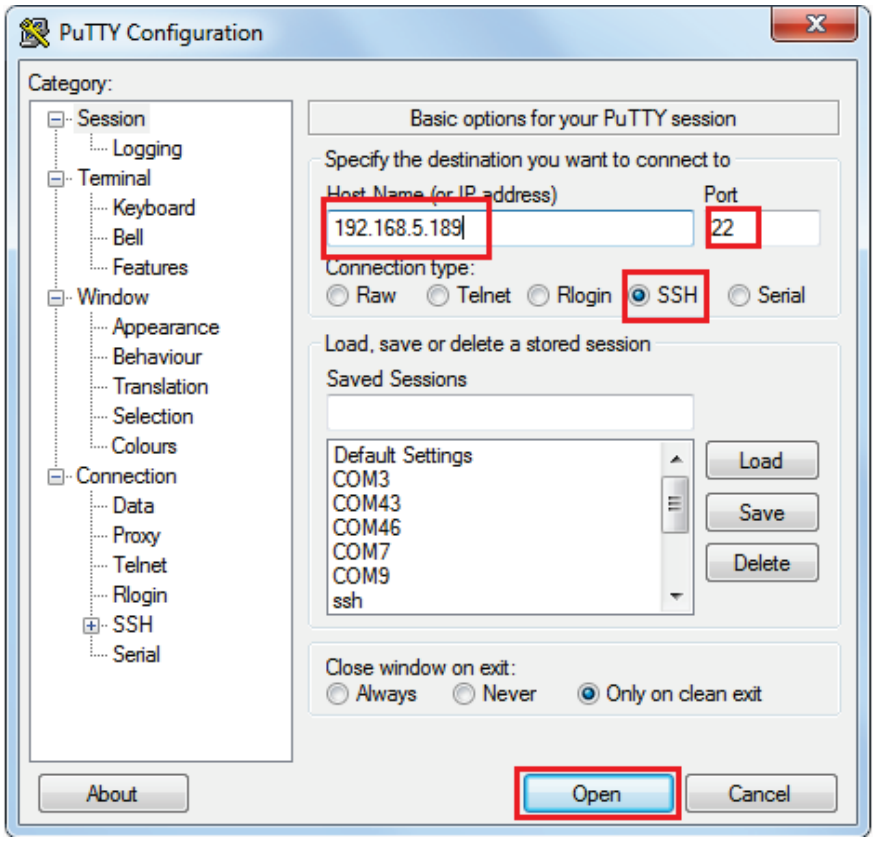
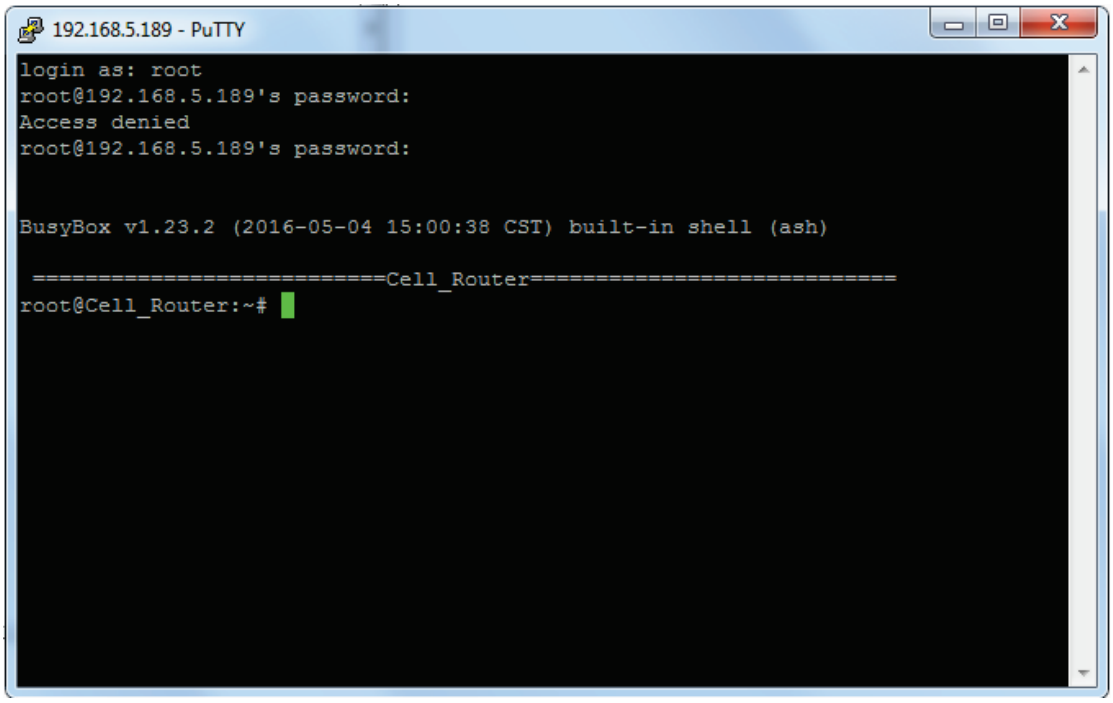
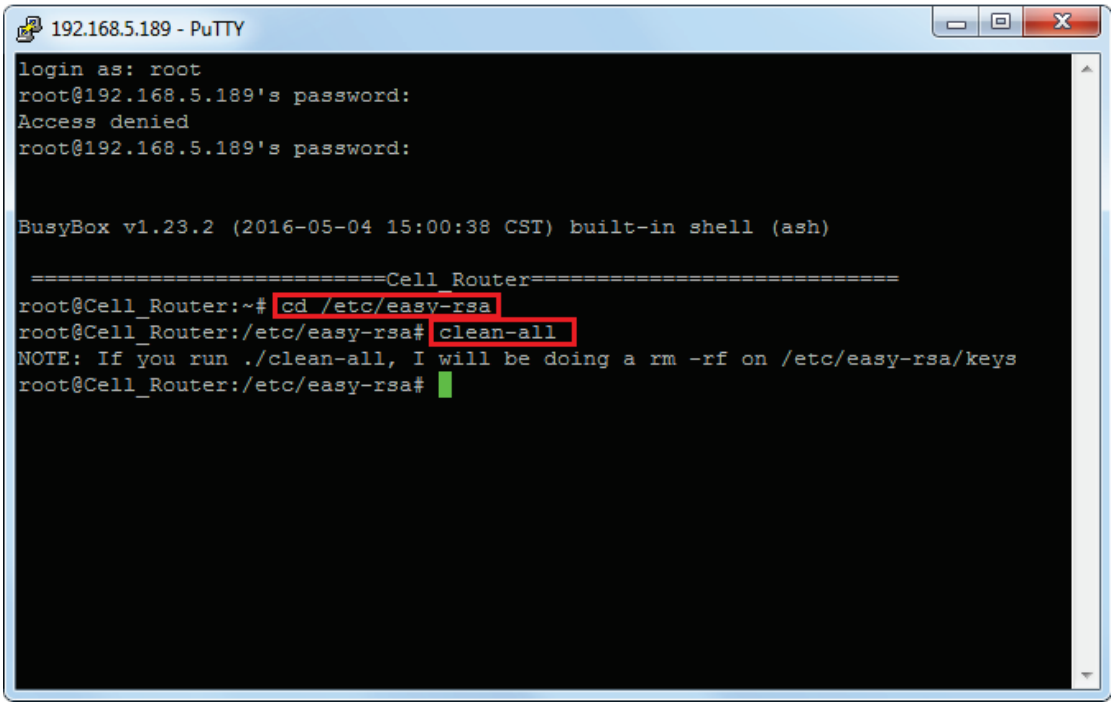
1. Open Putty, input IP address and port, select SSH as connection type, then click button “Open”.



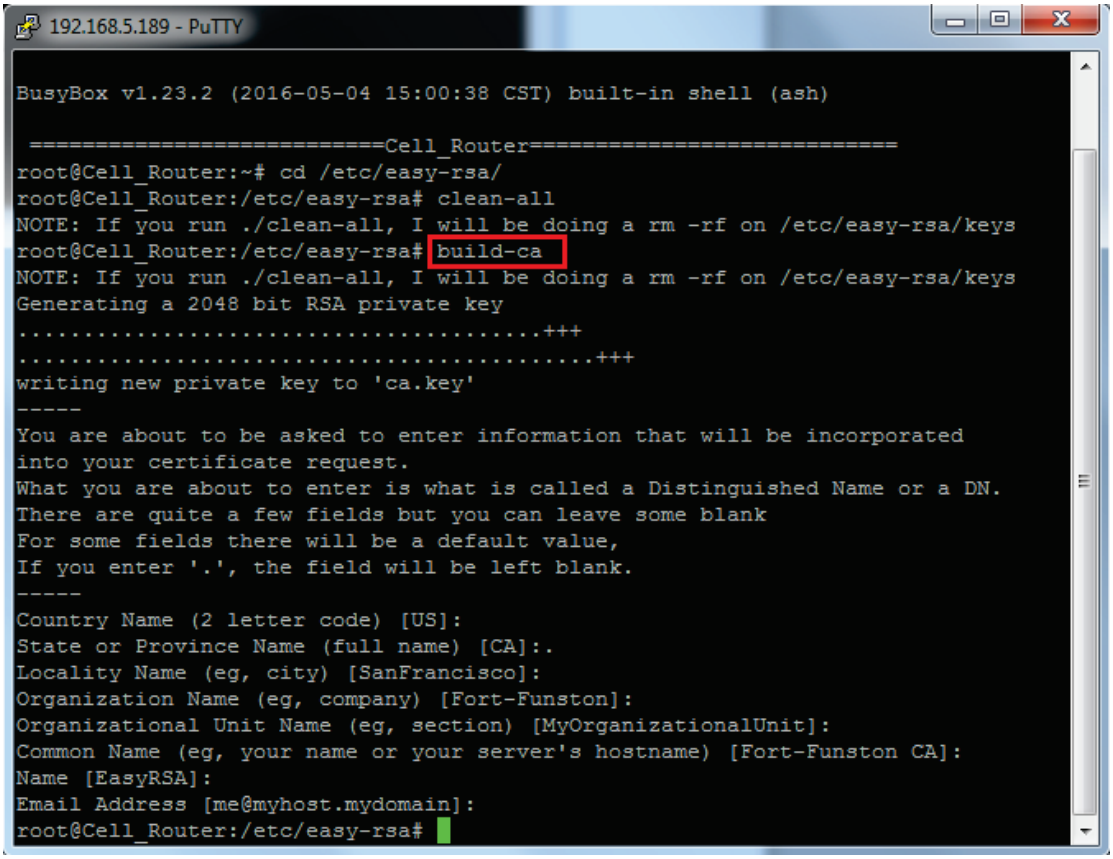
2. Input username and password.



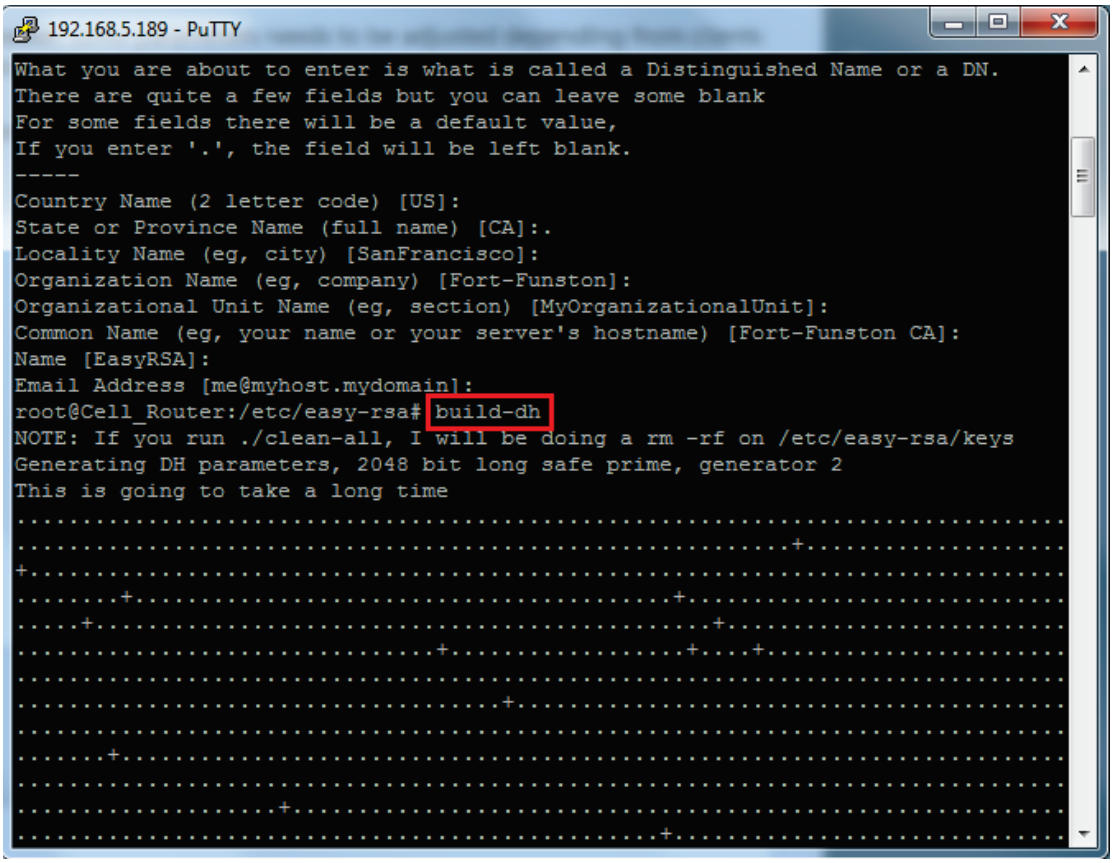
3. Run command “cd /etc/easy-rsa” and “clean-all”.



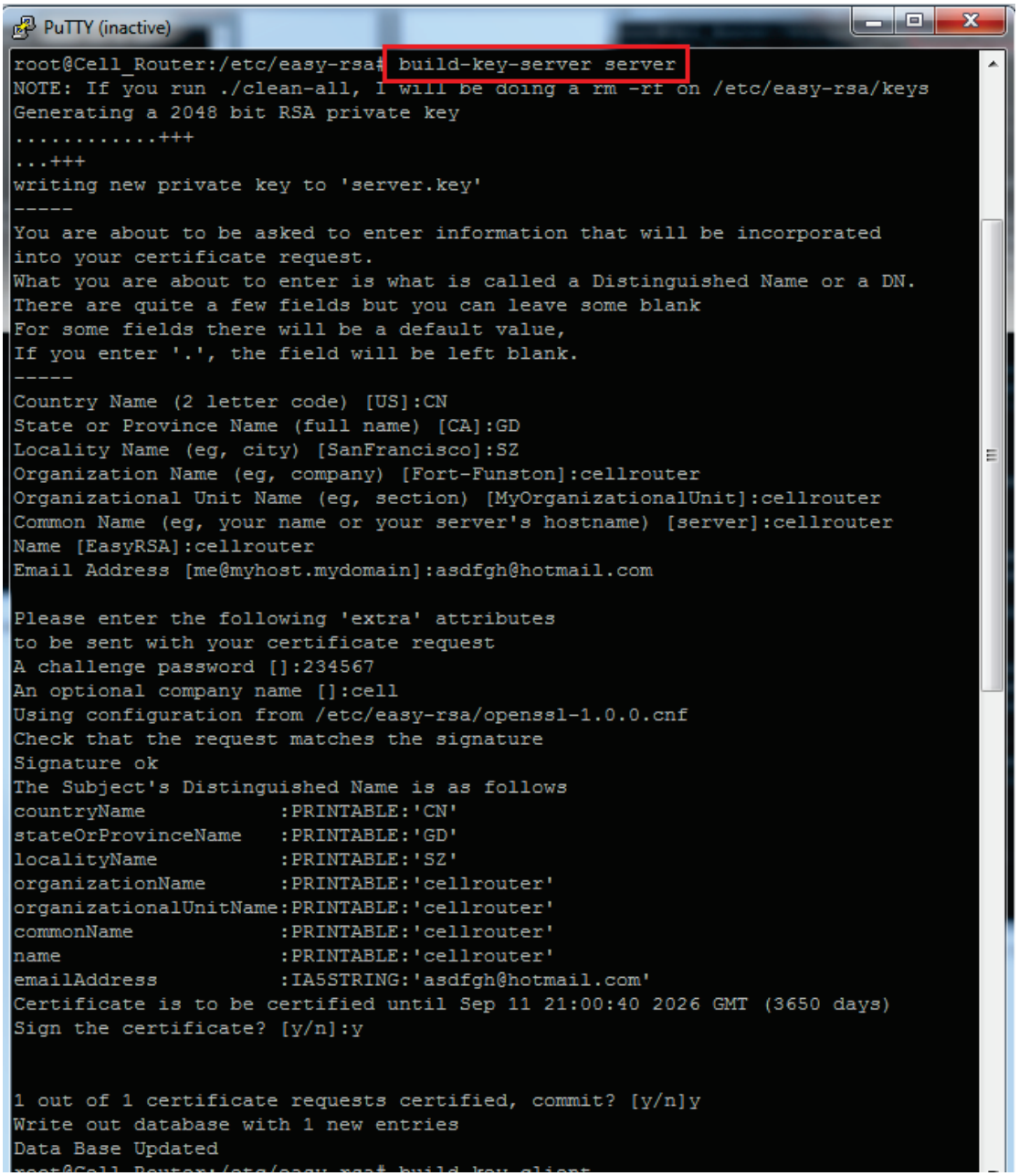
4. Run command “build-ca”.



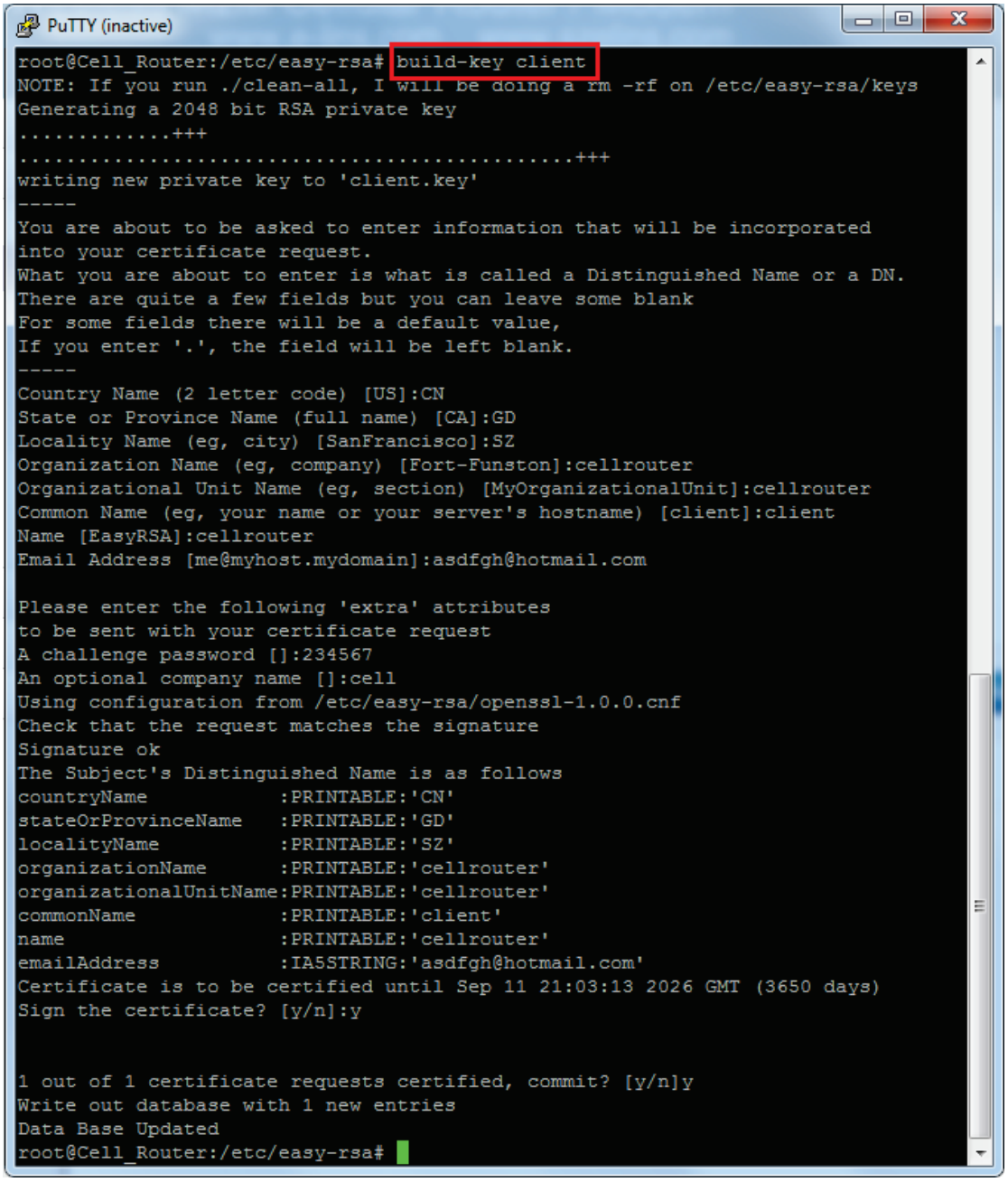
5. Run command “build-dh”, this is going to take a long time.The recommend way is generate it on PC.



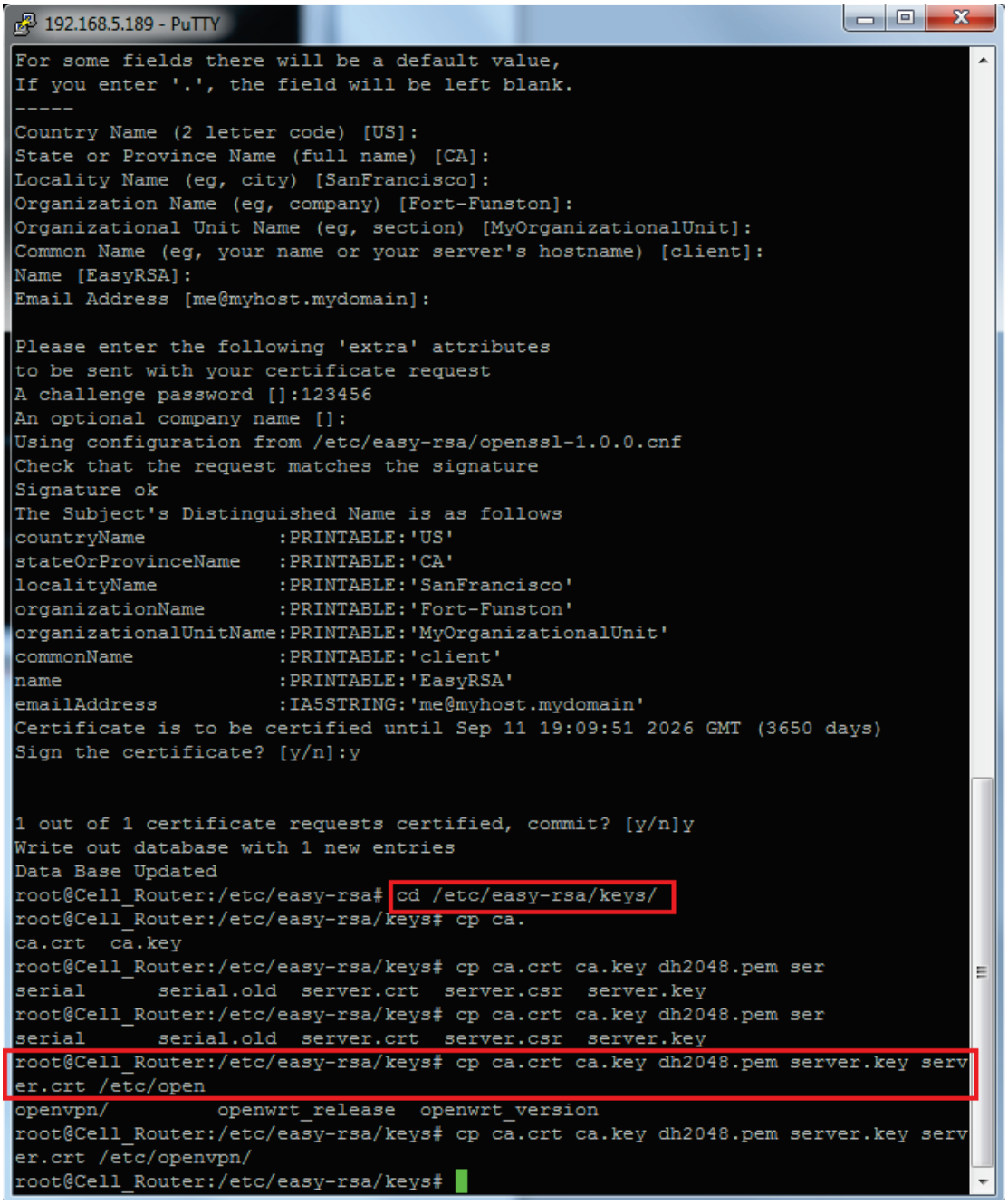
6. Run command “build-key-server server”, you can change “server” to any words you want.



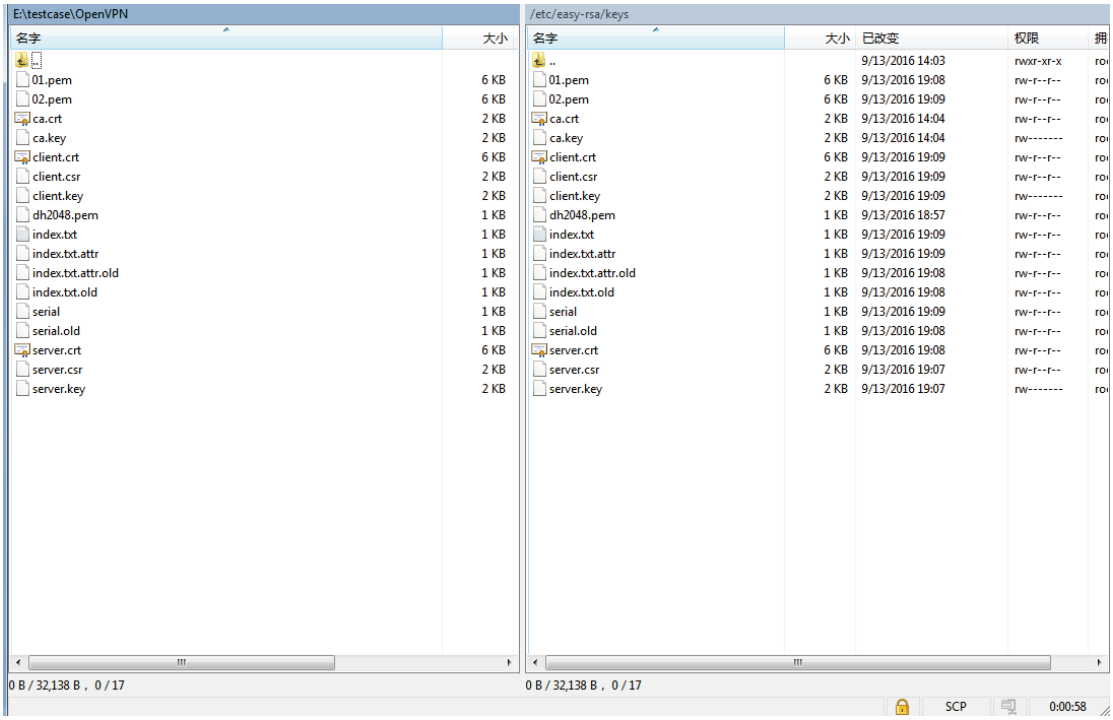
7. Run command “build-key client”,you can change “client” to any words you want.



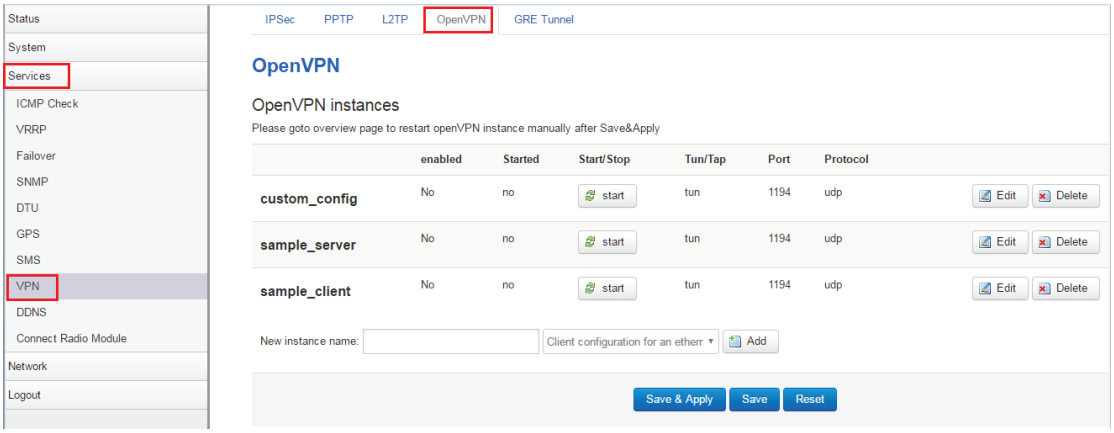
8. Run command “cd /etc/easy-rsa/keys/” and “cp ca.crt ca.key dh2048.pem server.key server.crt /etc/openvpn/”



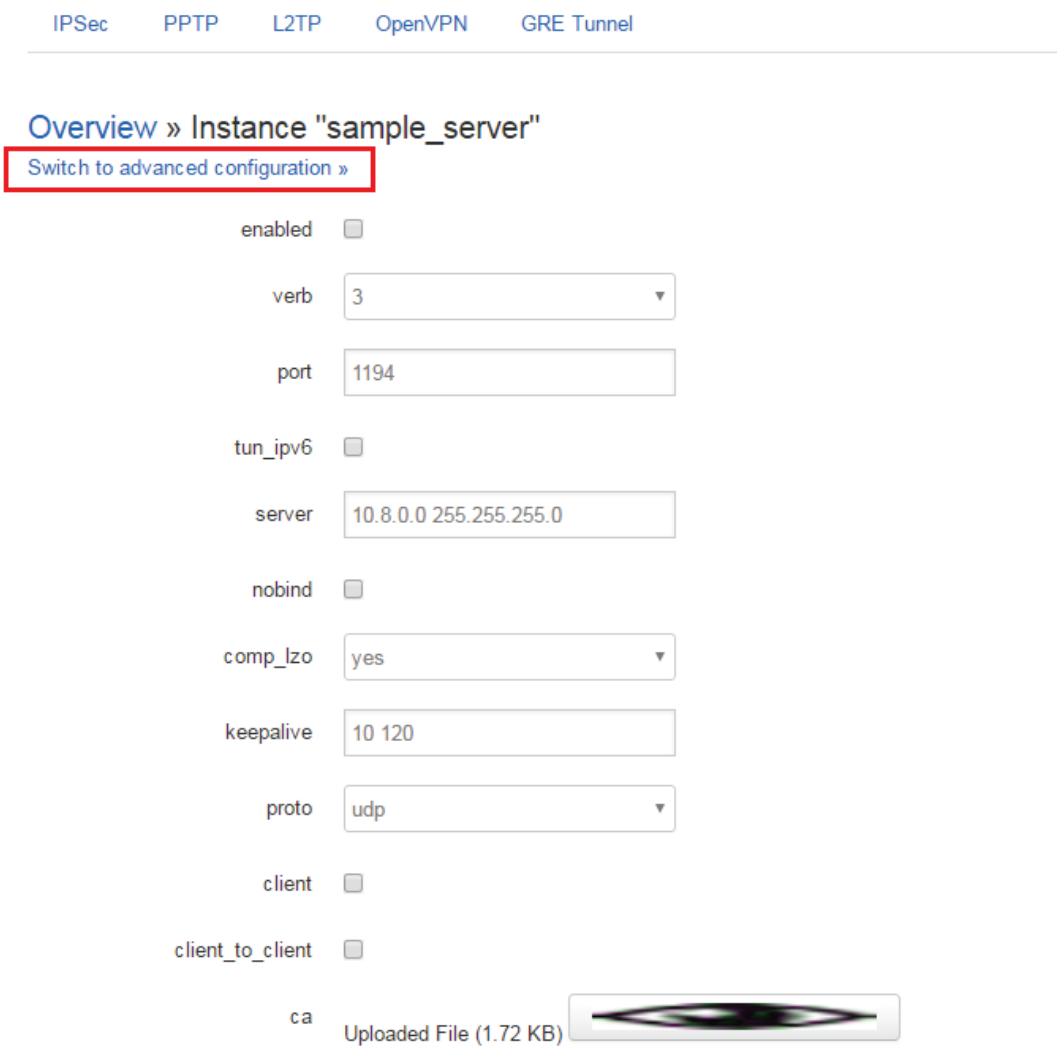
9. Download key files to your computer by WinSCP. Login in WinSCP and copy files from router to Windows.



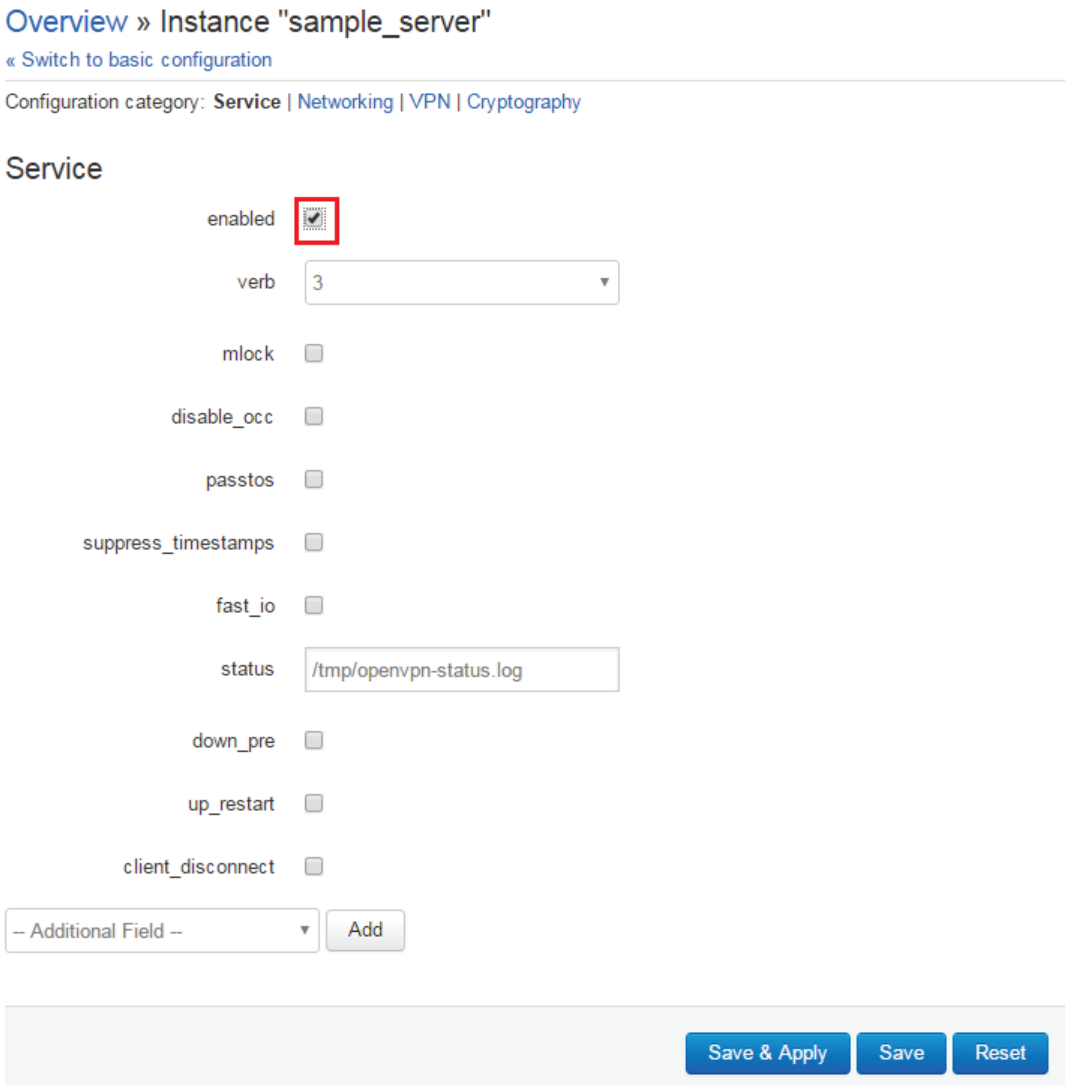
10. Open management page on the router which generate keys. Click “Services”→“VPN” at left navigation bar, and then click “OpenVPN”.



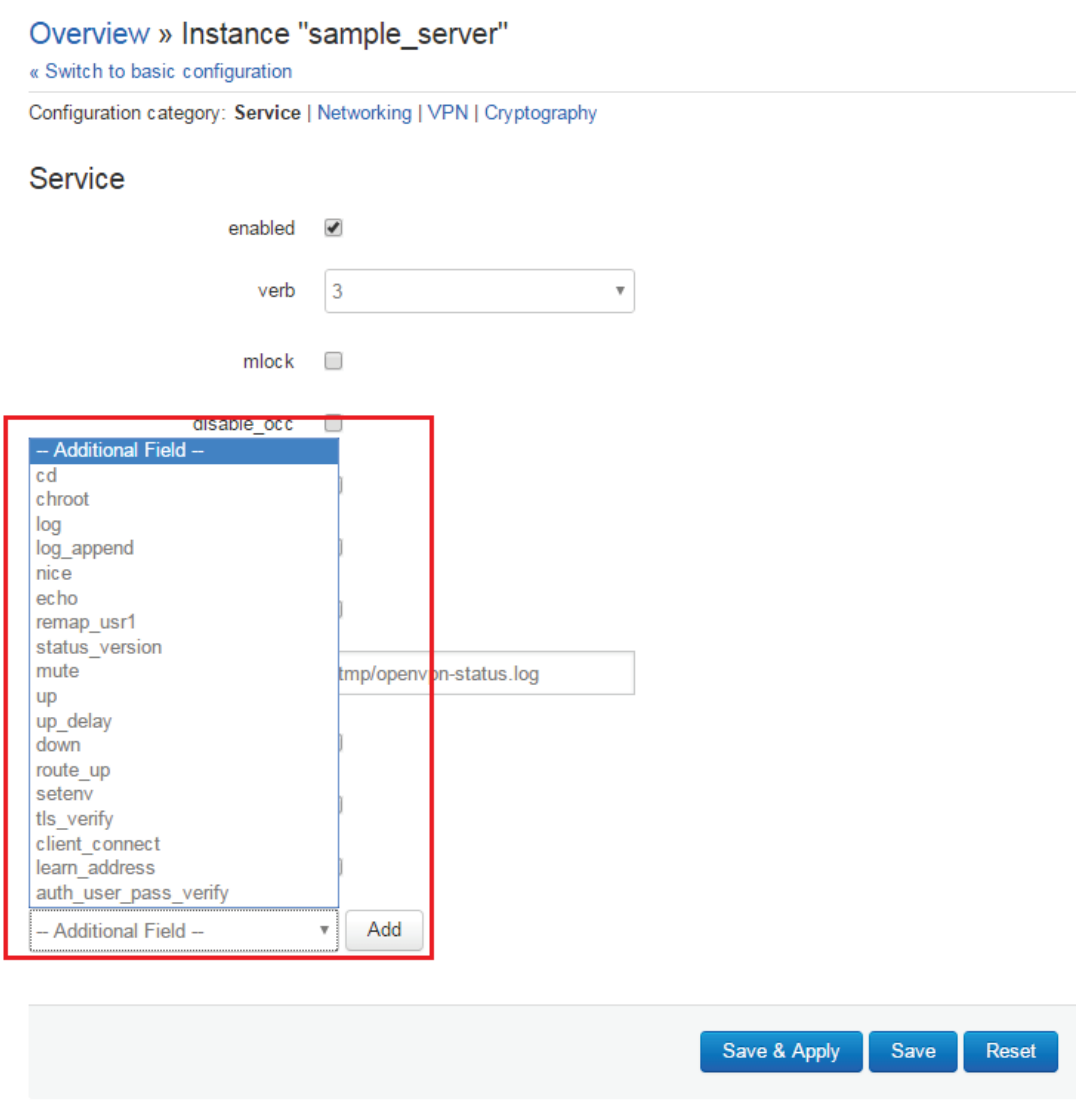
11. Click button “Edit” at the same line of sample_server. Then click “Switch to advanced configuration”.



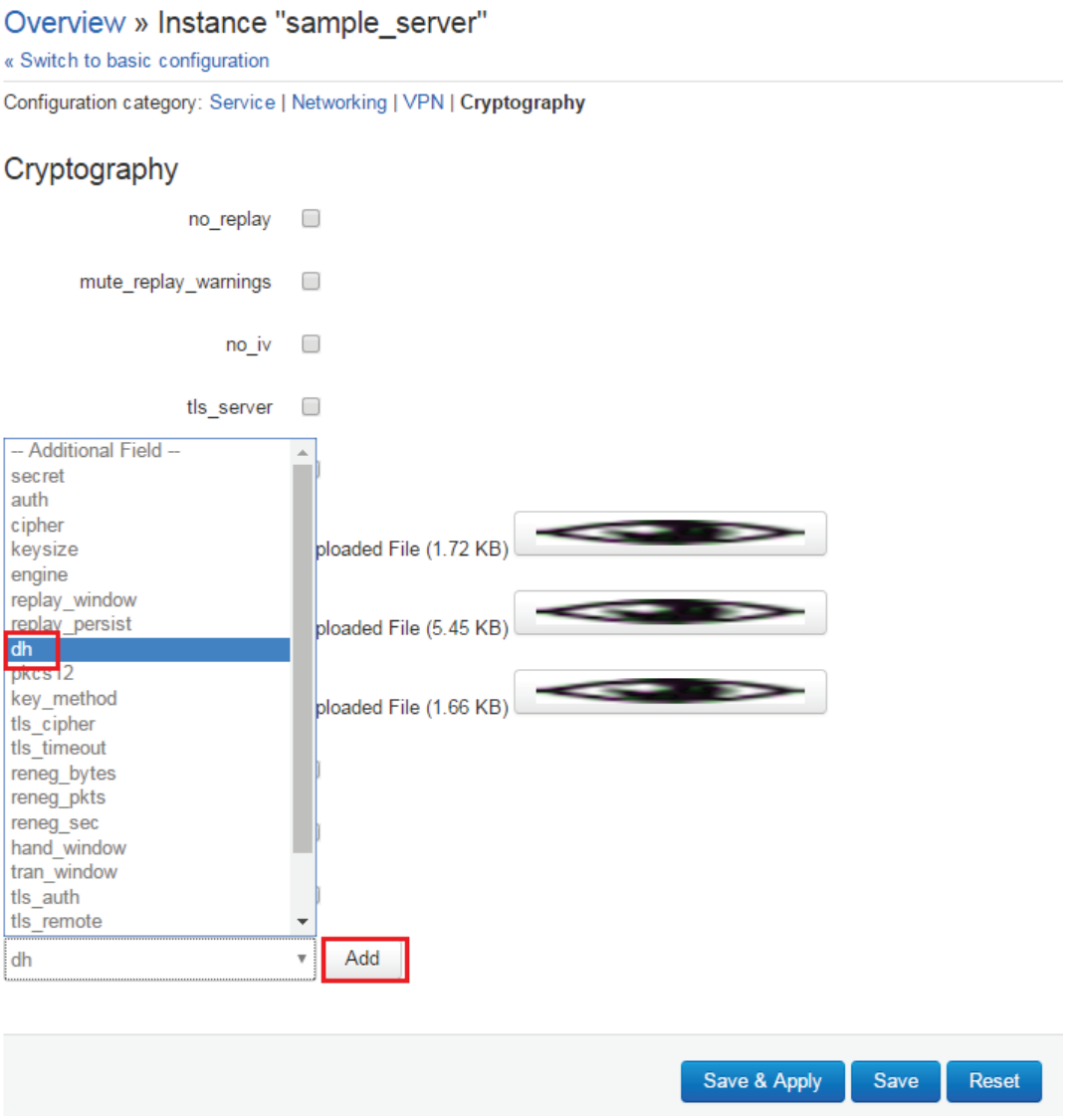
12. Click “Enable”, and press button “Save & Apply” to use the default configuration for OpenVPN server.



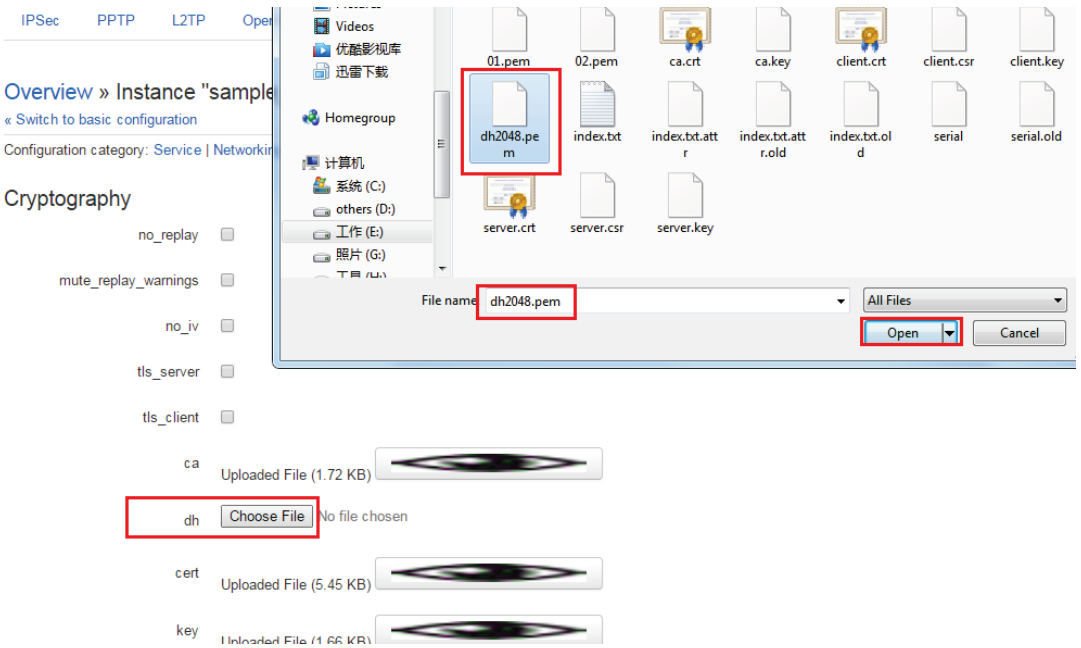
13. If the default configuration is not you want, you can click “- Additional Field-” to add more fields.



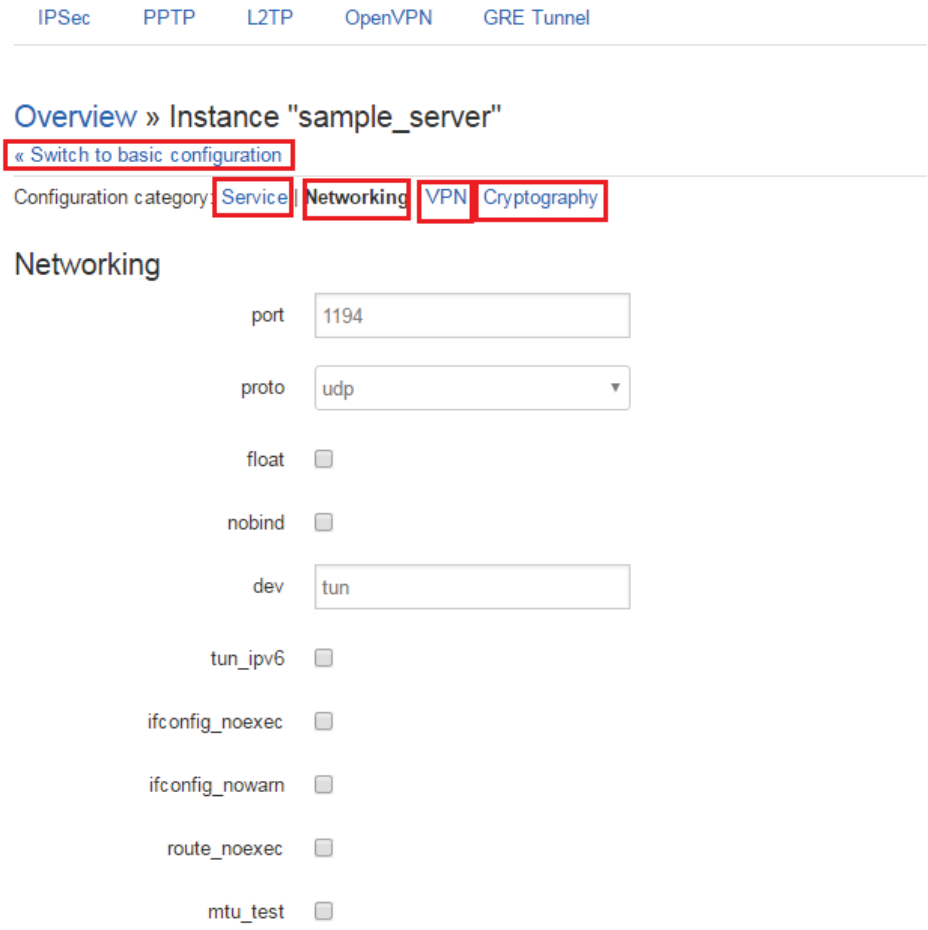
14. Switch to “Cryptography”. Click “- Additional Field -”, select “ca”(ca.crt)“dh”, then click button “Add”.



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

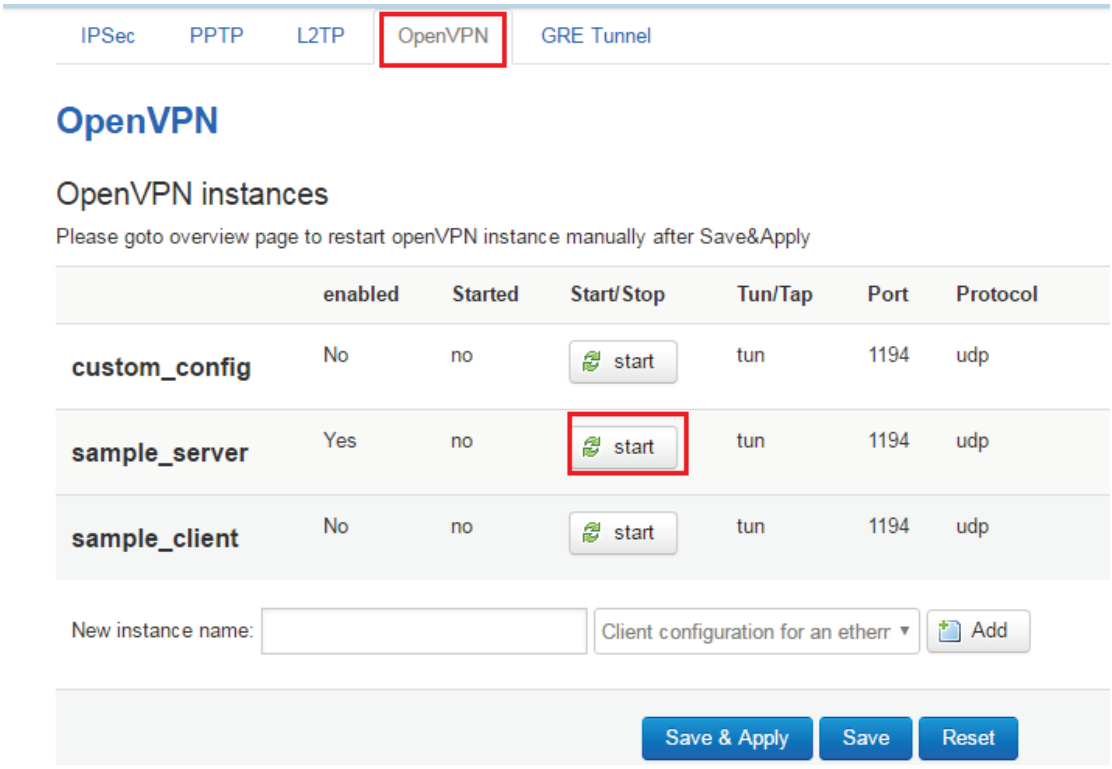


16. You can switch to “Service”, “Networking”, “ VPN” and “Cryptography” to configure more.But before switching to other taboption, you must press button “Save” to avoid losing configuration

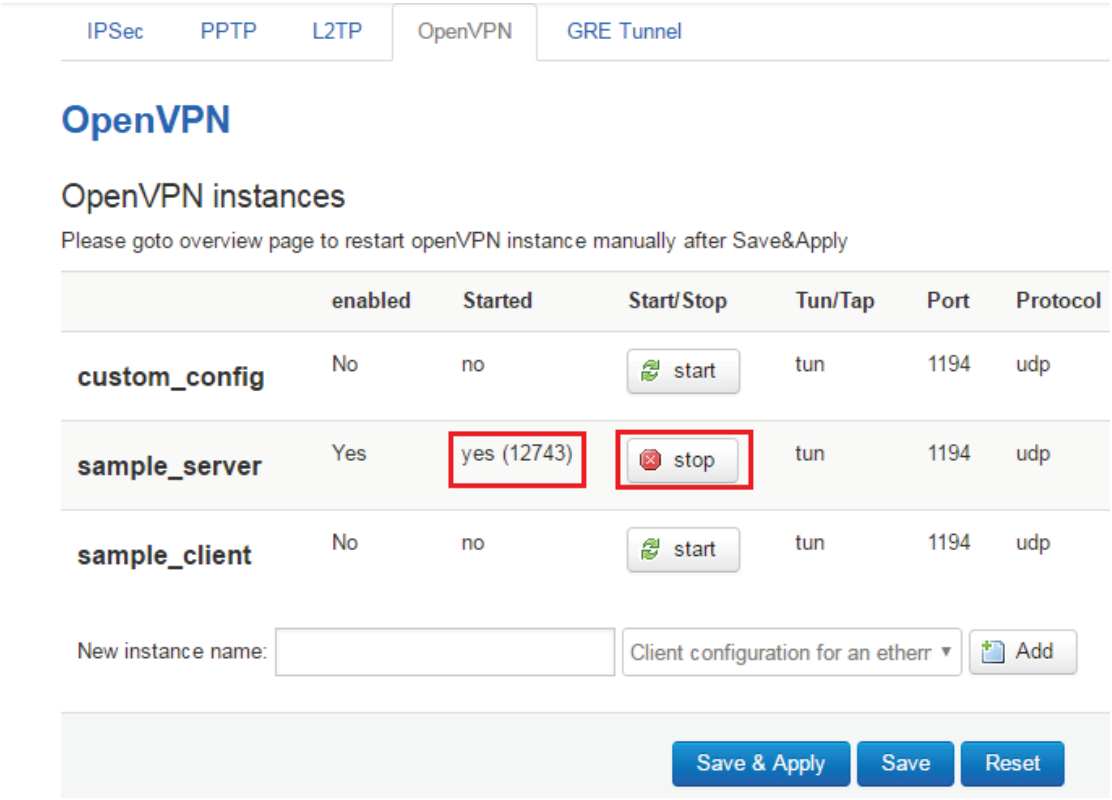


17. If all settings are done, click button “Save & Apply”.

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

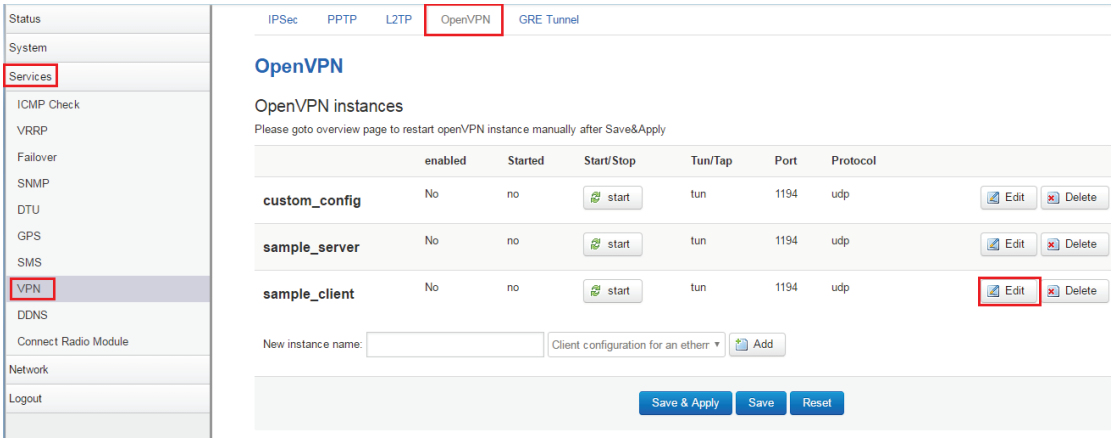


19. If “Started” is changed from “start” to “Yes(XXX)”, that means server started successfully. And you can stop it by click button “Stop”.

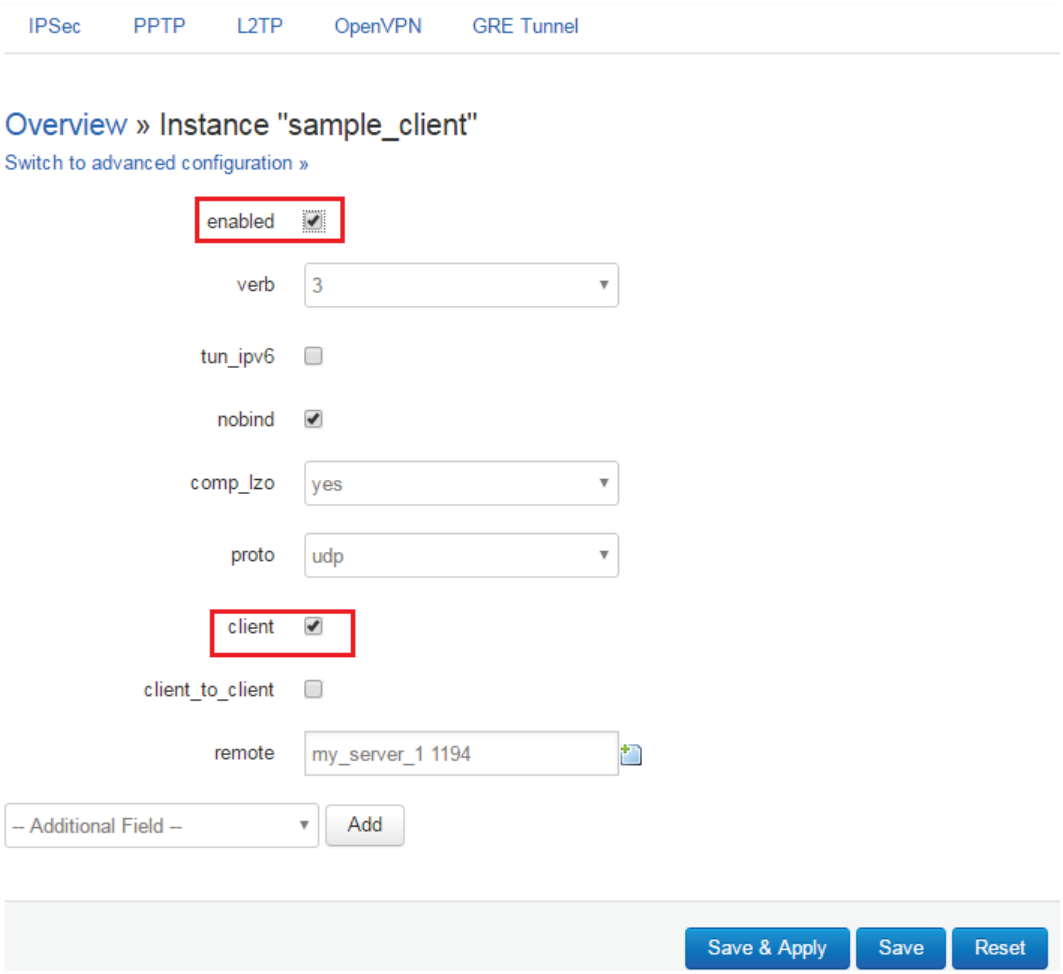


Configuration OpenVPN client.

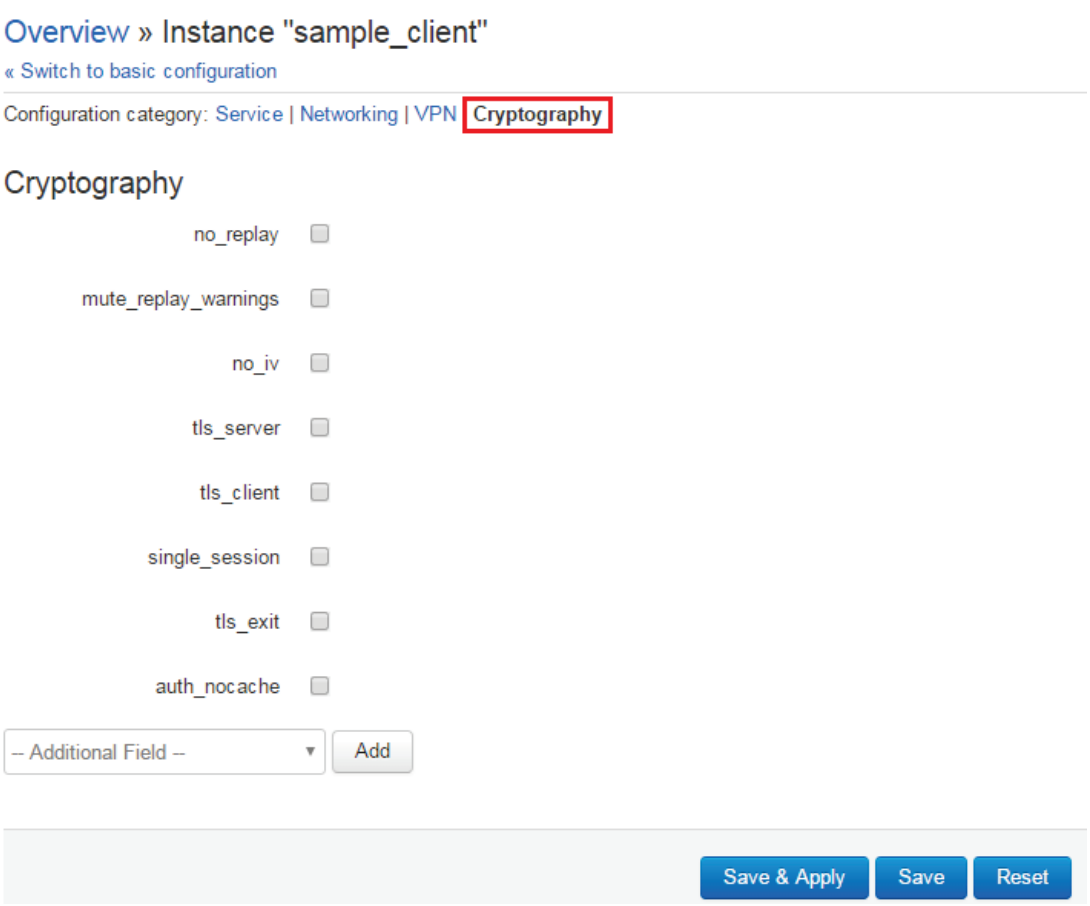
1. Open management page on the router which generate keys. Click “Services”→“VPN” at left navigation bar, and then click “OpenVPN”. Click button “Edit” at the same line of “sample_client”.



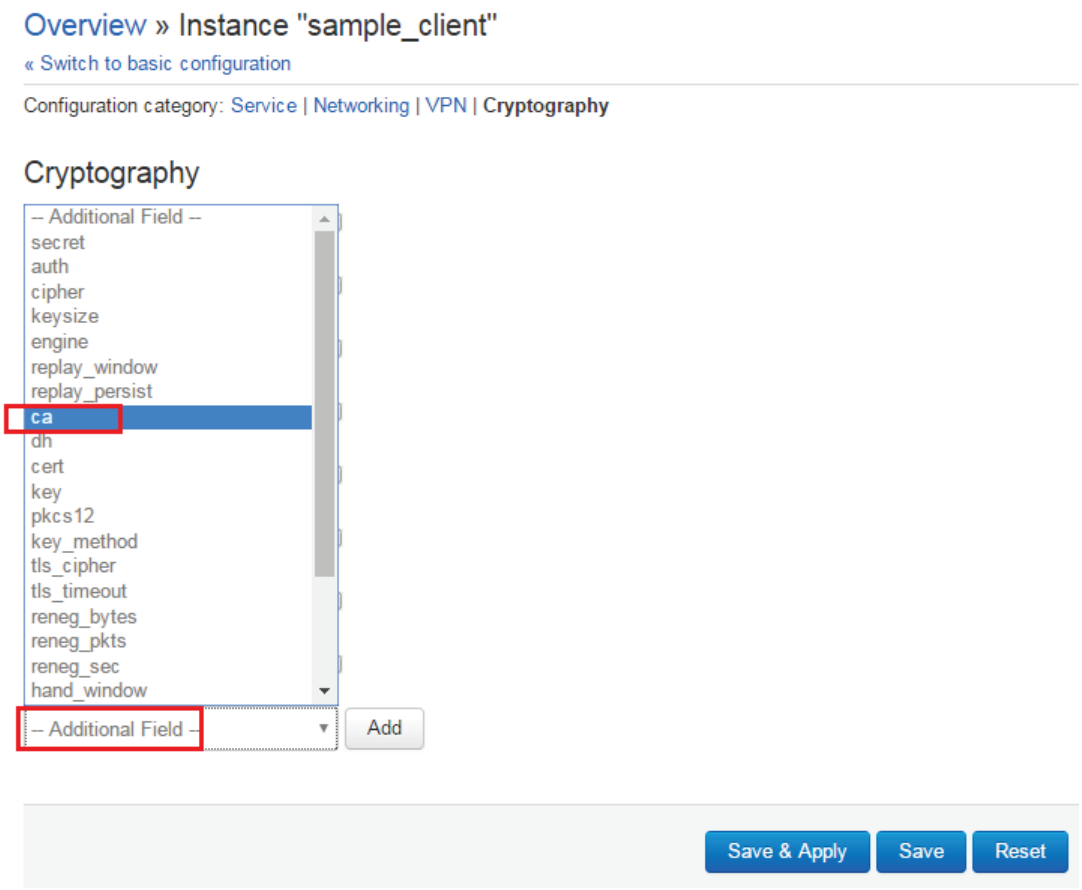
2. Make sure “Enable” and “Client” are checked.Then click button “Save”.



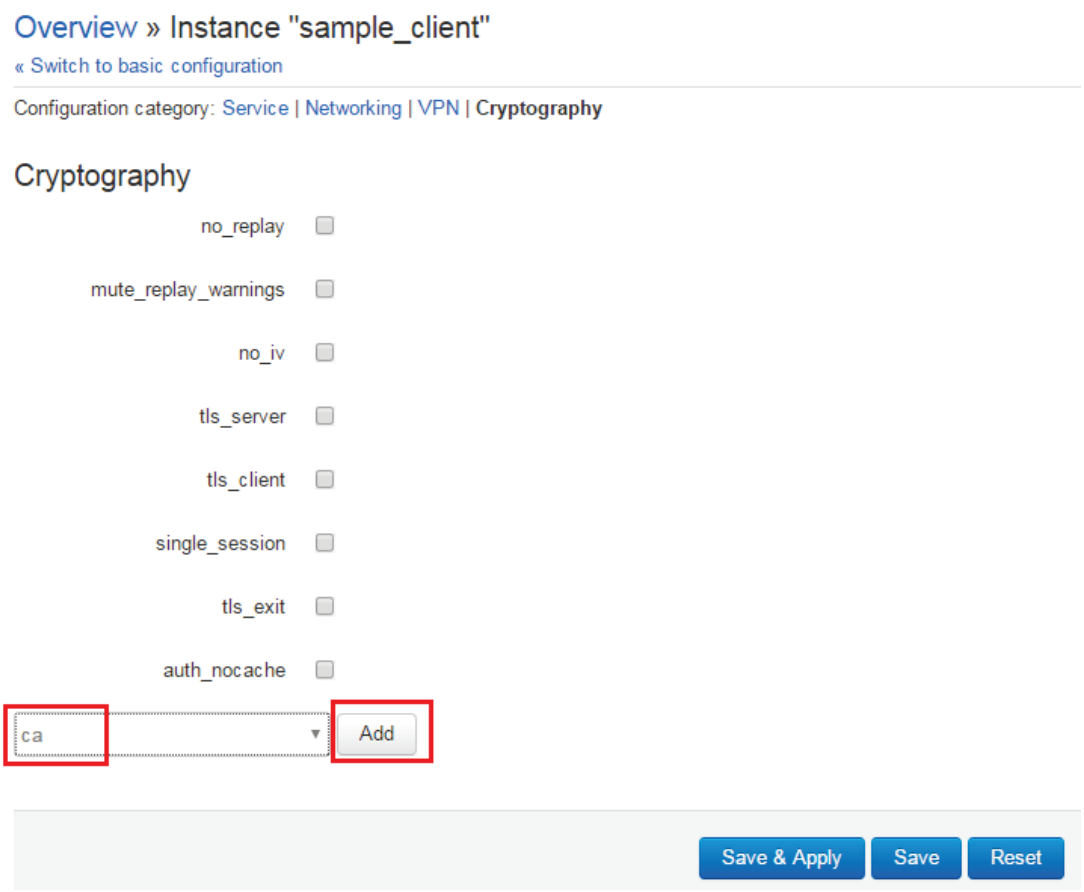
3. Click “Switch to advanced configuration”, and then click “Cryptography”.



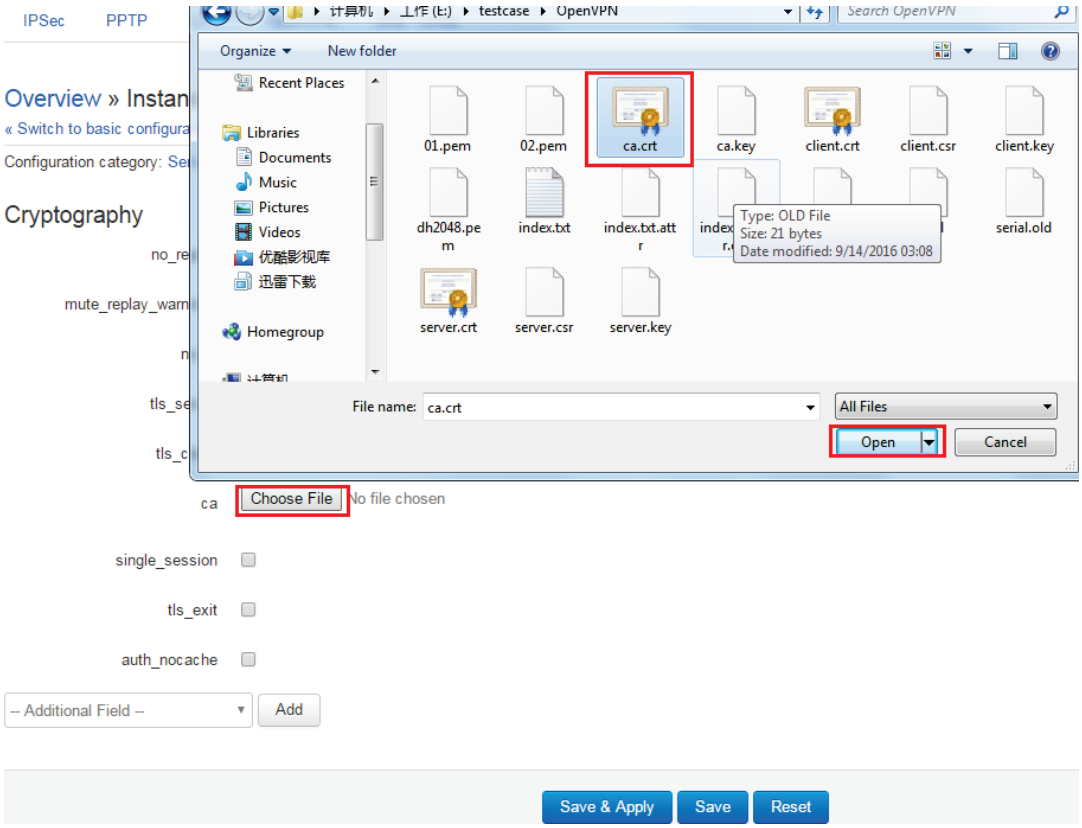
4. Click “- Additional Field -” then select “ca”.



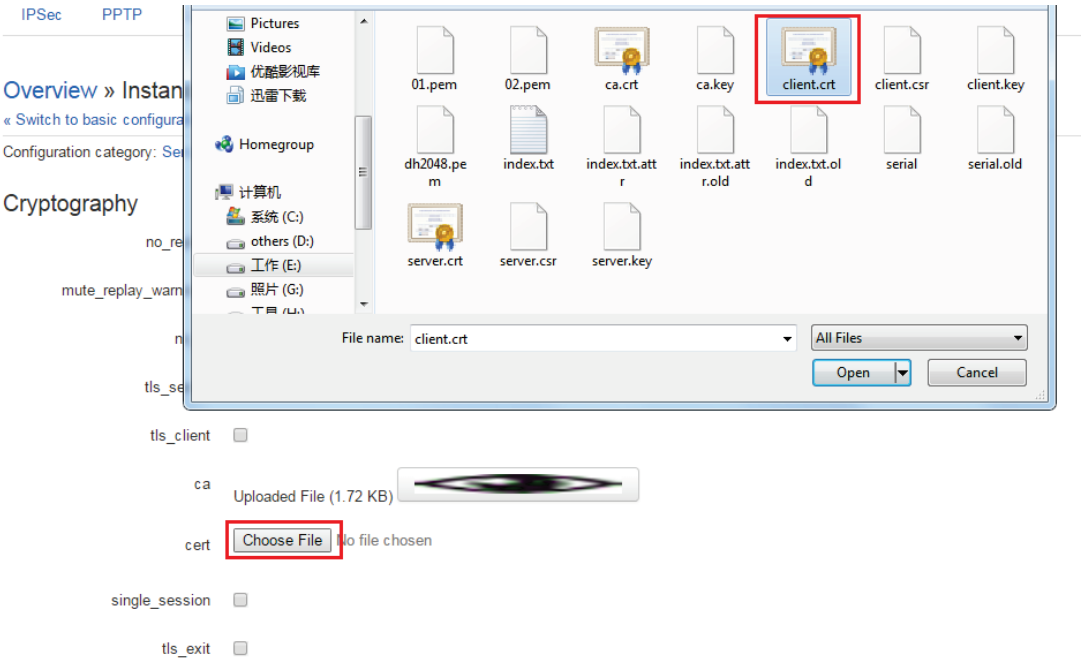
5. Click button “Add”.



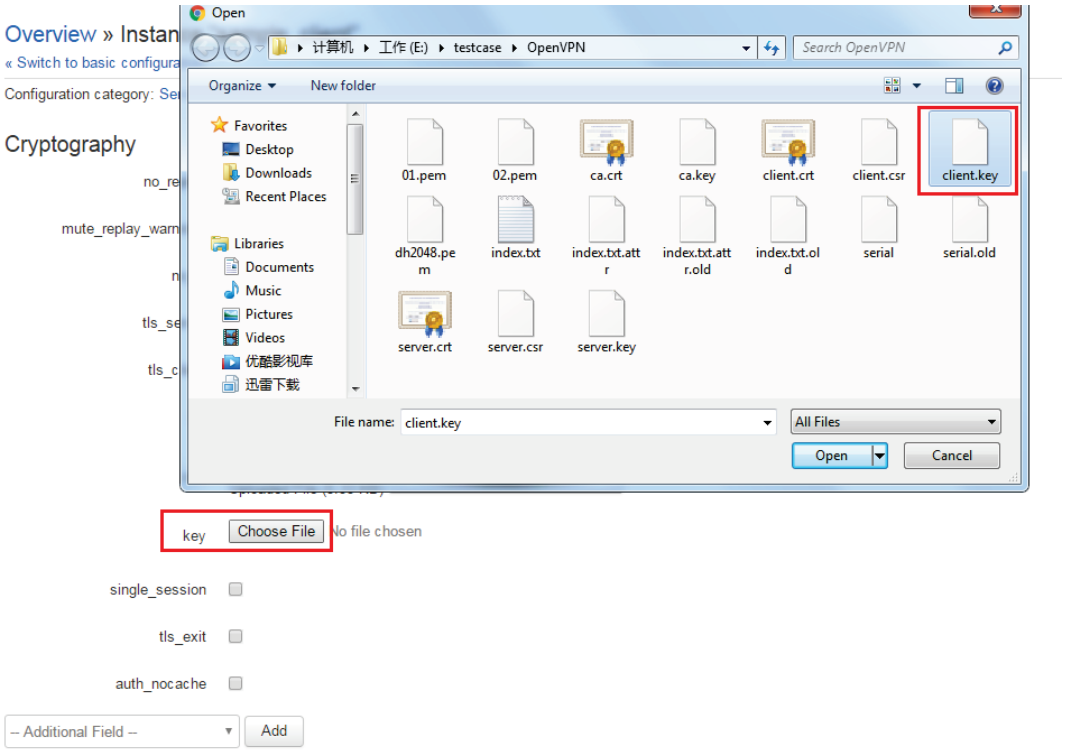
6. Click button “Choose File” of ca, then open key files “ca.crt”. These key files were downloaded to windows by previous step.



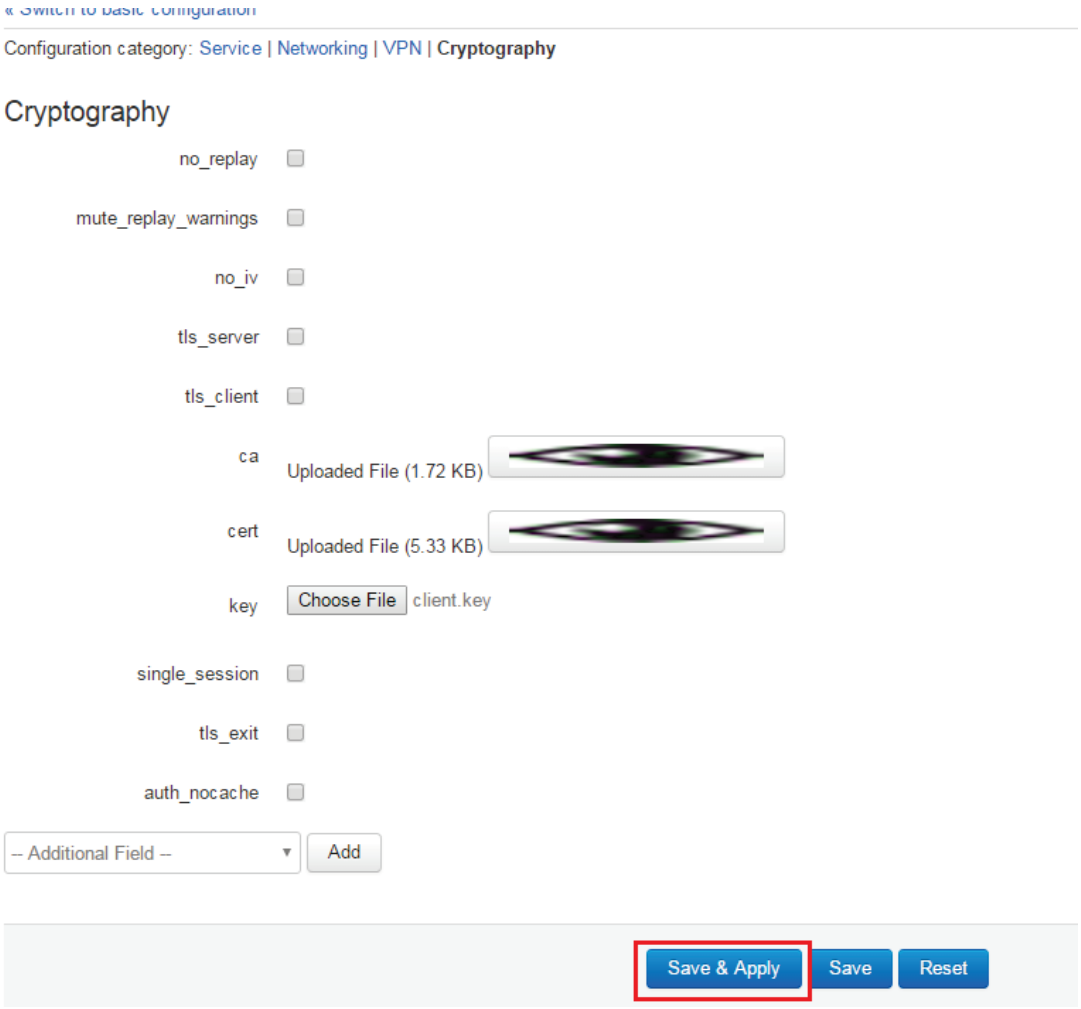
7. Add field “cert” and choose key file “client.crt”.



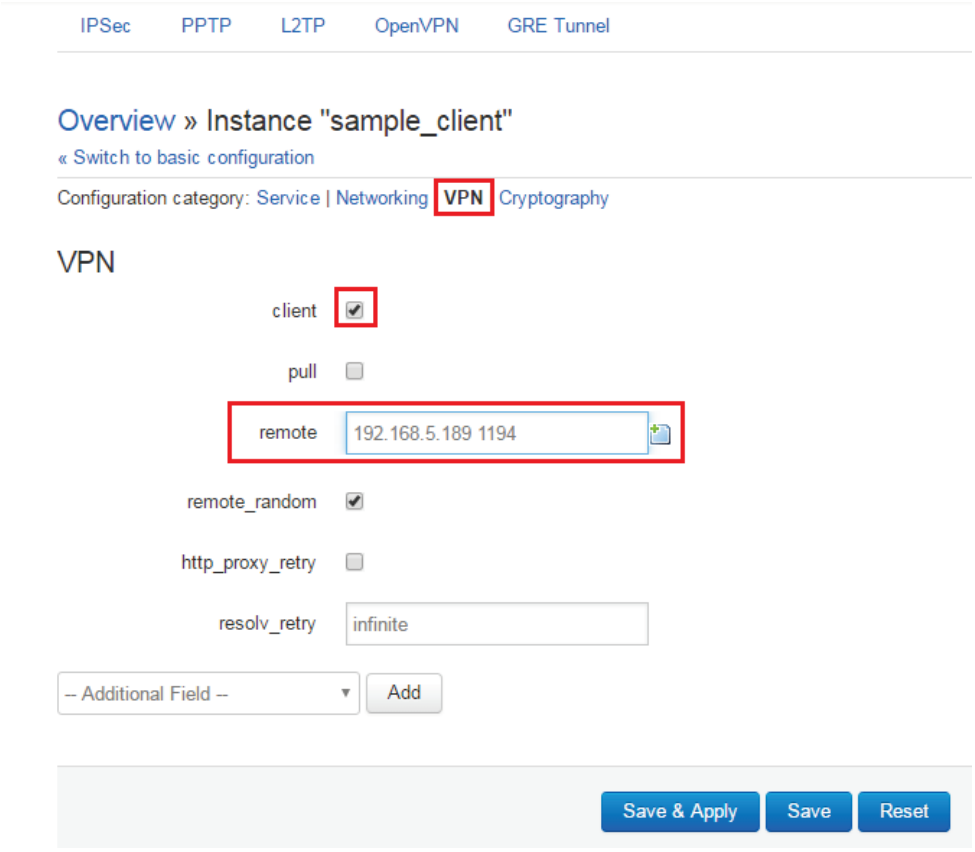
8. Add field “key” and choose key file “client.key”.



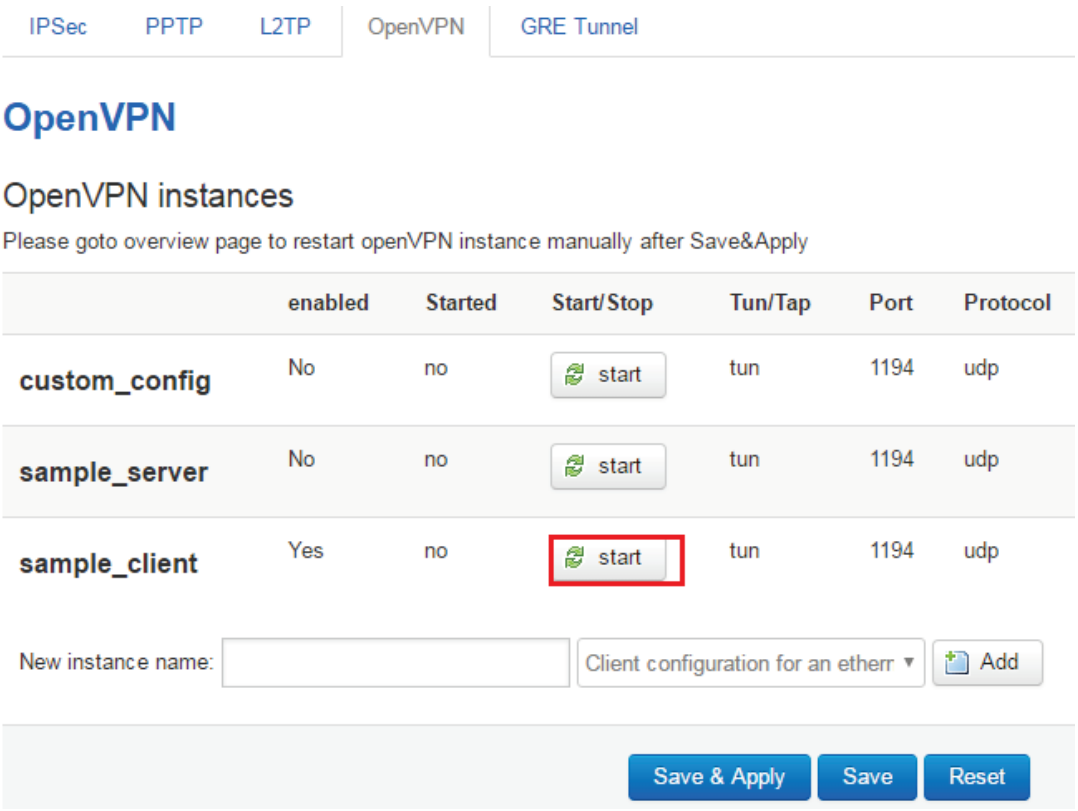
9. Click button “Save & Apply” or “Save” to save configration.



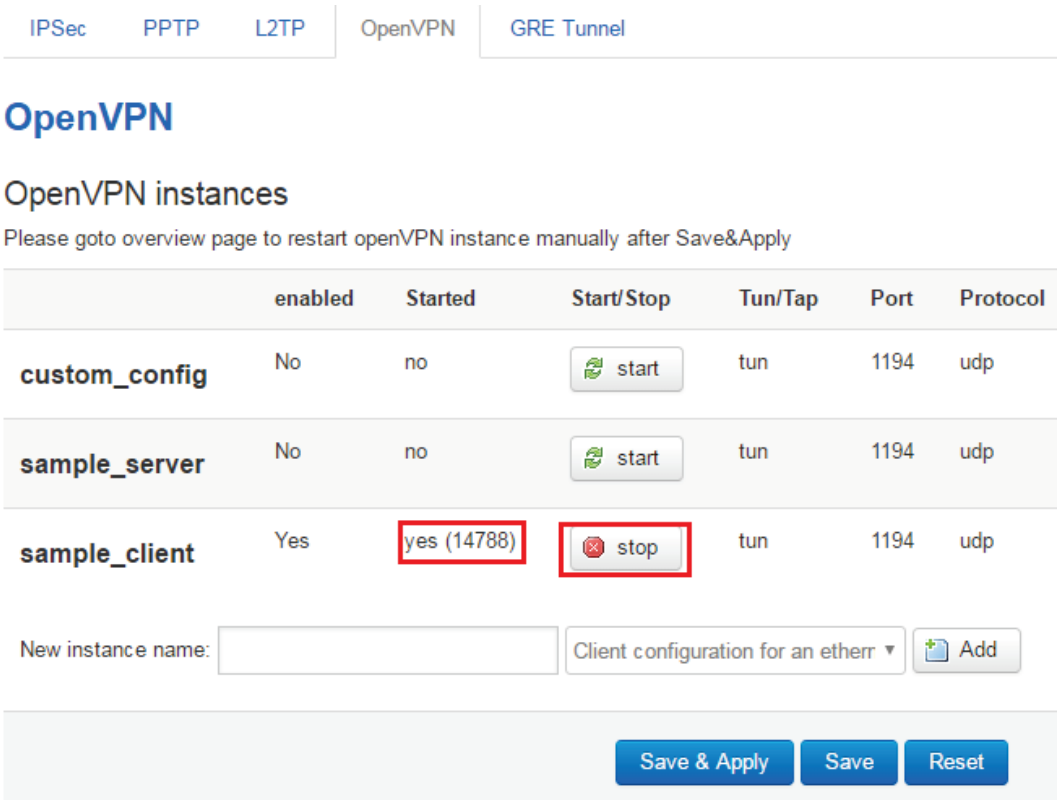
10. Switch to “VPN”, modify the remote, here we have OpenVPN server on router “192.168.5.189” with port “1194”. Then click button “Save & Apply”.



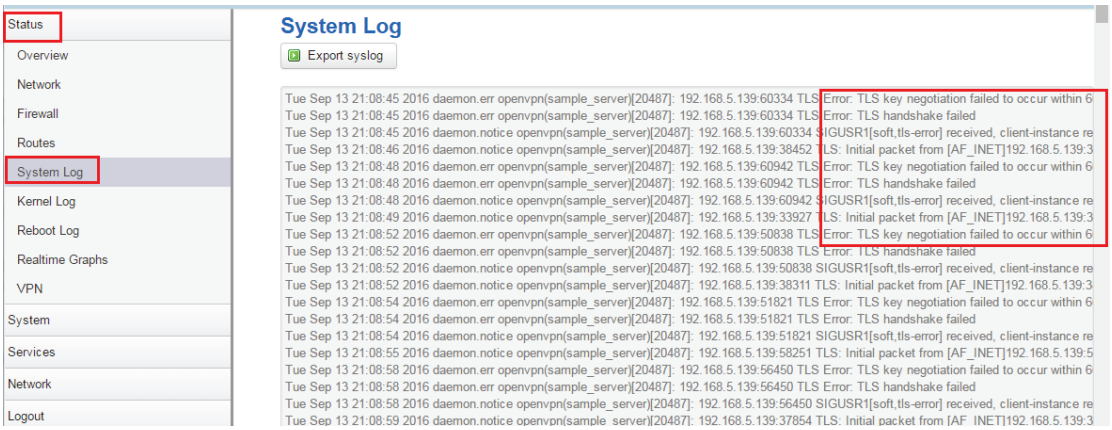
11. Goto OpenVPN overview page to start sample_client by click button “start”



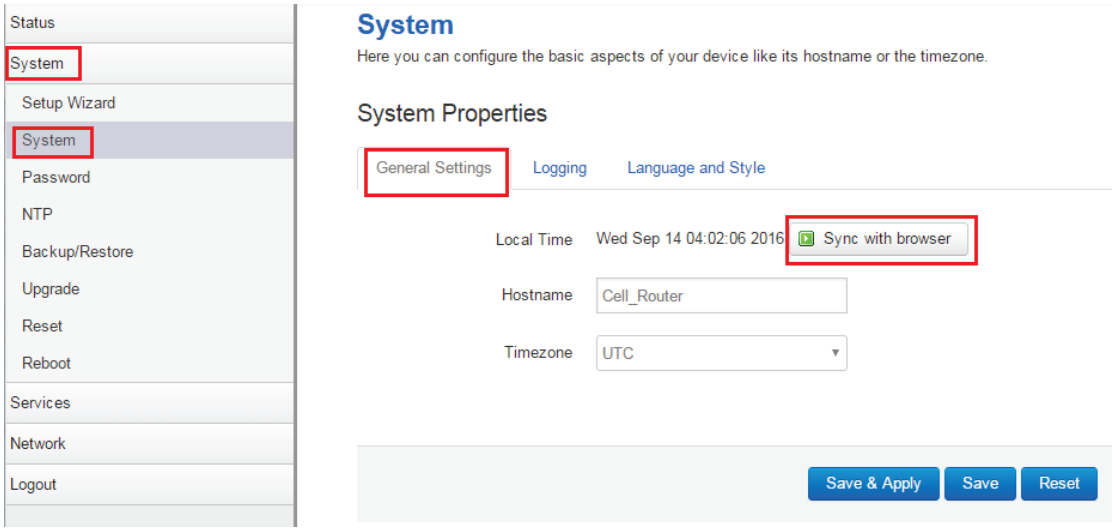
12. If “Started” is changed from “start” to “Yes(XXX)”, that means server started successfully. And you can stop it by click button “Stop”.



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.

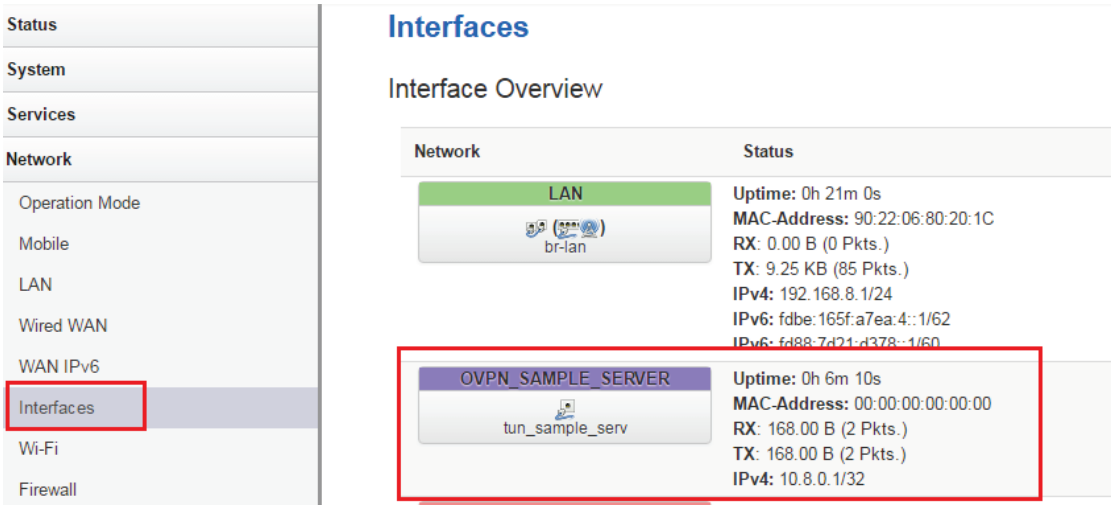


Sync Local time with browser:

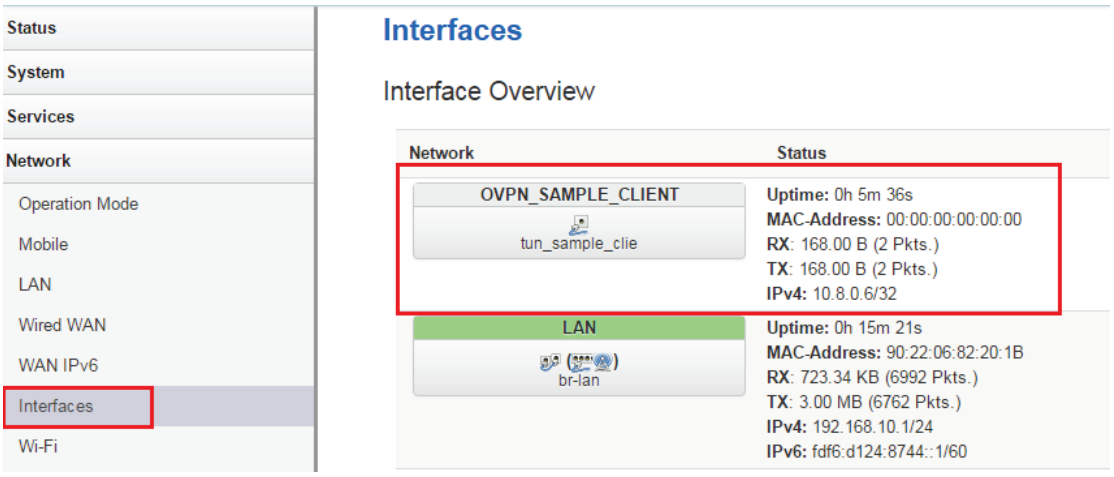


14. Now the tunnel between server and client should be setup successfully, client and server can access each other with virtual IP address 10.8.0.0/24. check the interface status at here:

    Server Side:



    Client side:

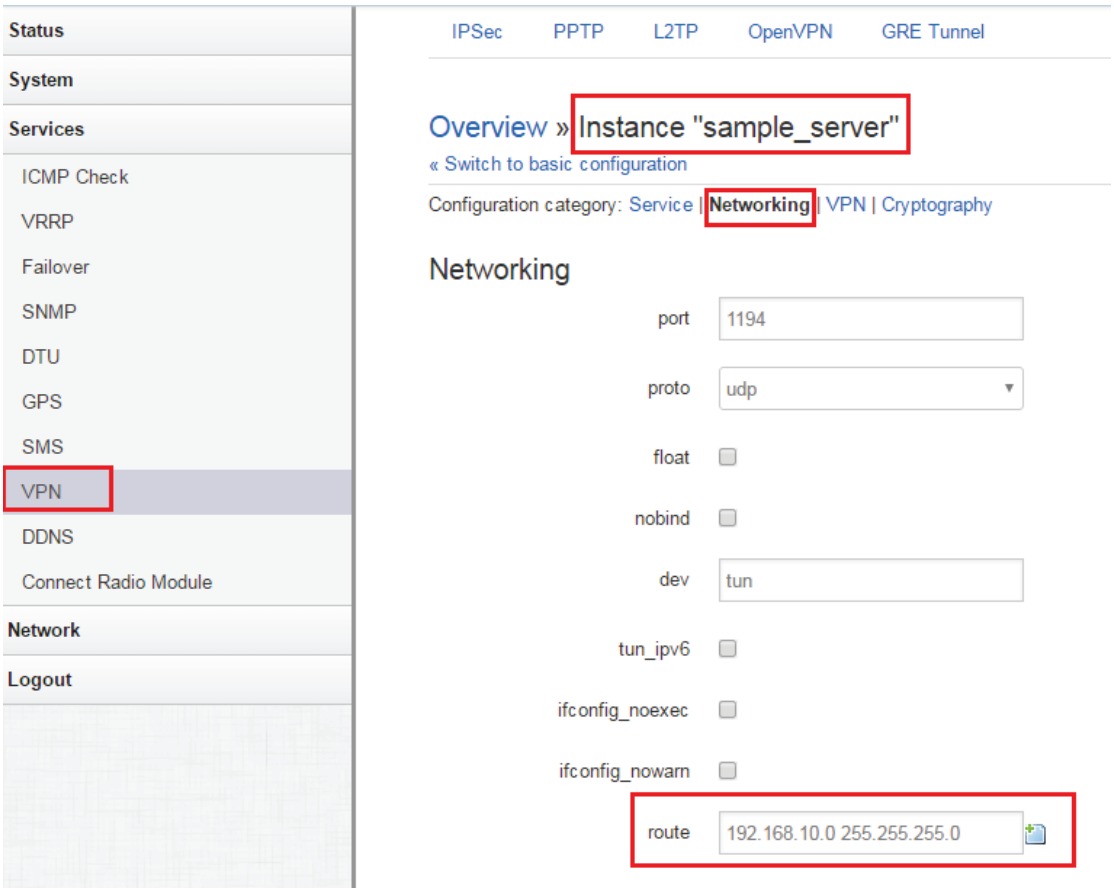


15. If you need to connect subnet behind server and client, we need to configure server

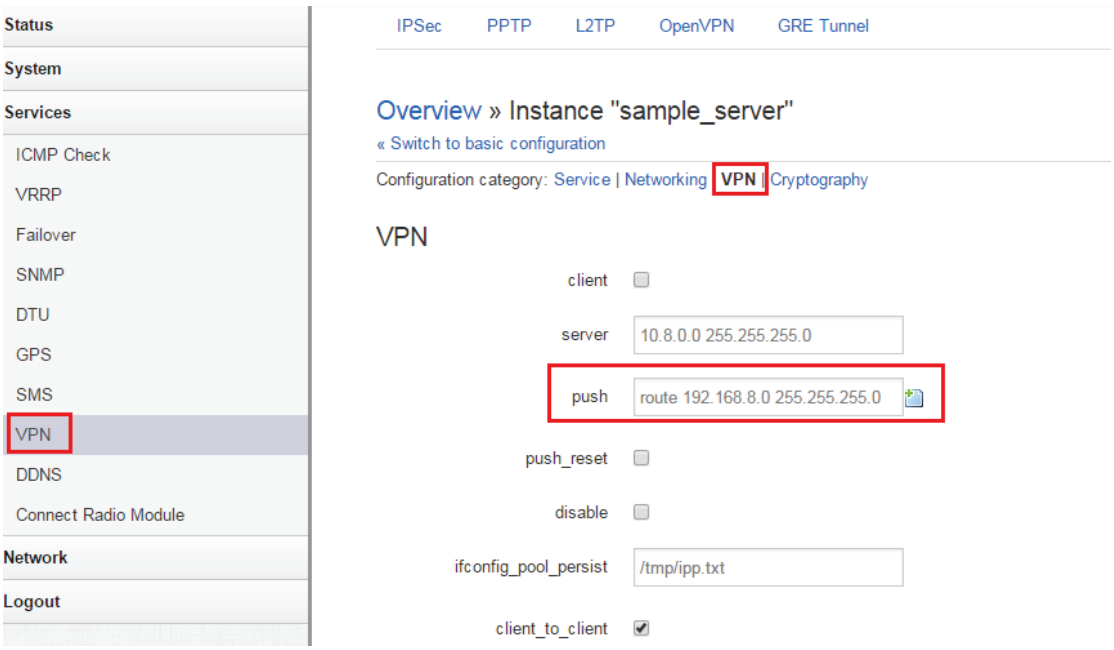
instance again.

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

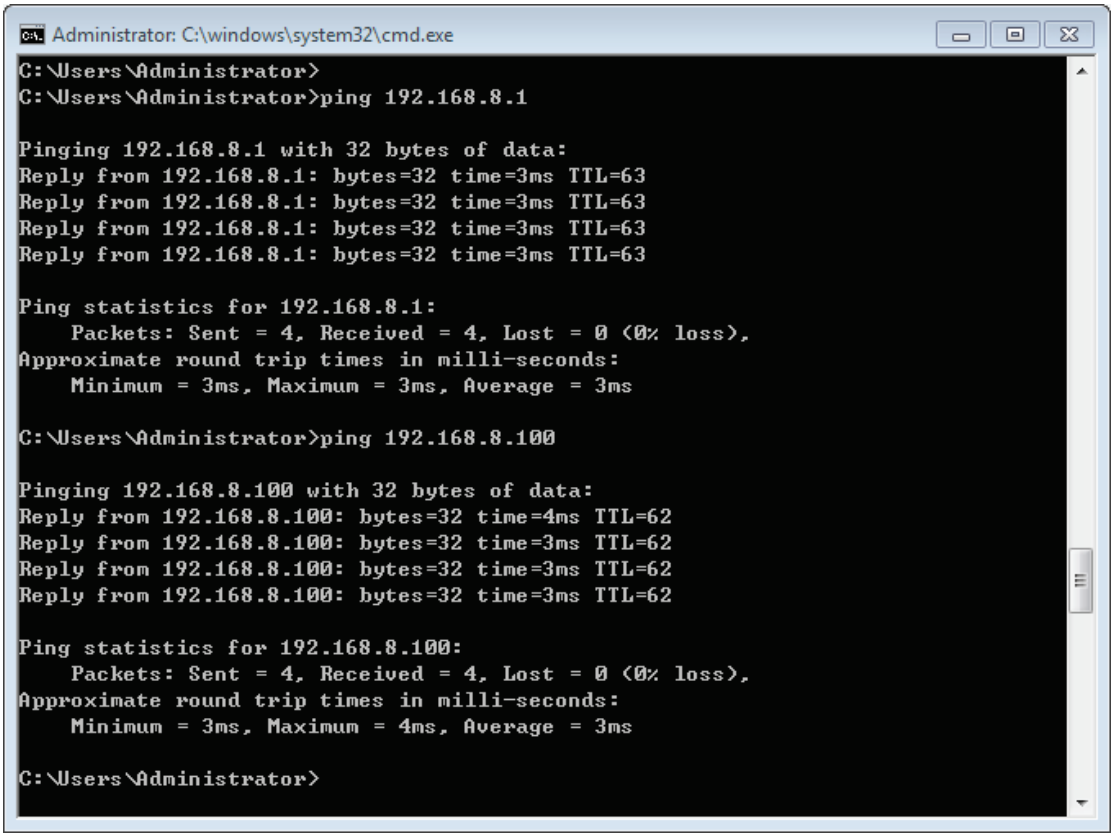


17. Add push on server

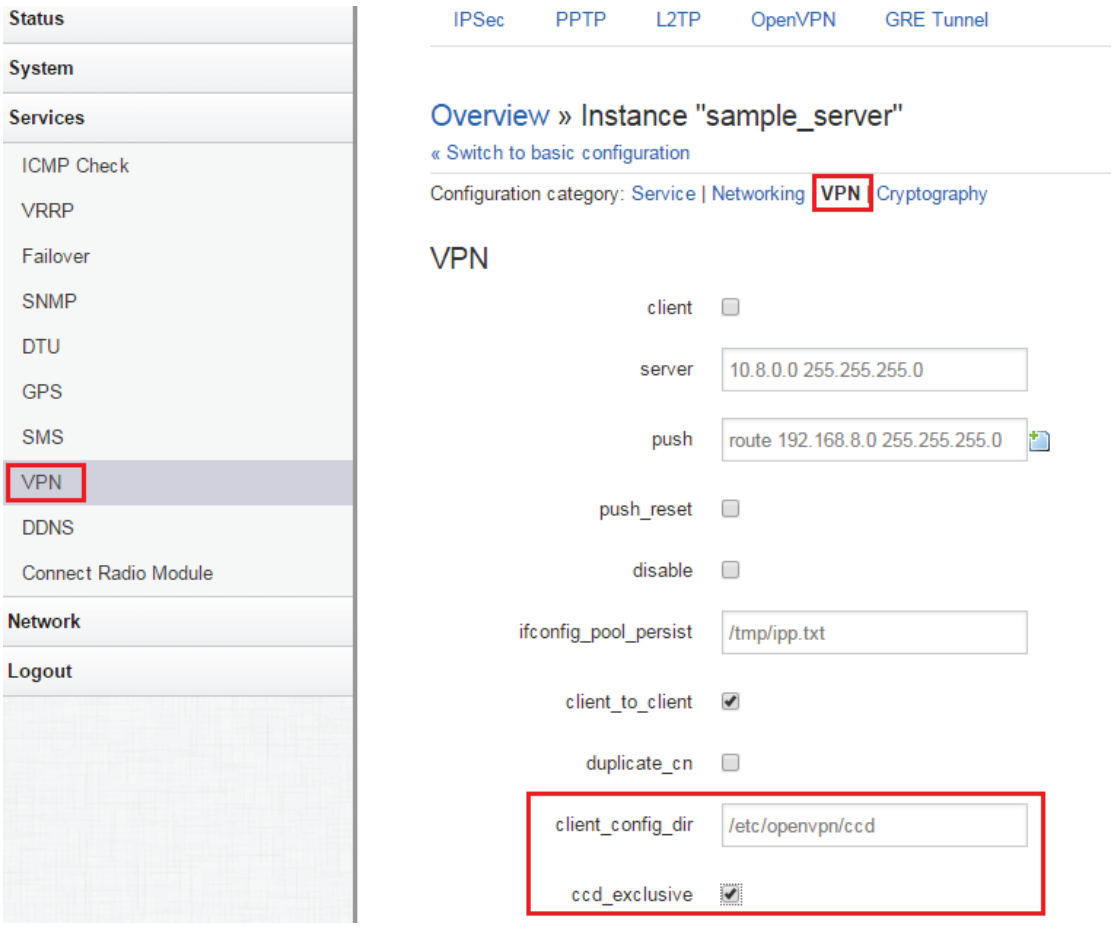


18. Save, then goto OpenVPN overview page to stop instance and then start this instance.

19. Ping from PC 192.168.10.171 which behind OpenVPN client.



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



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.