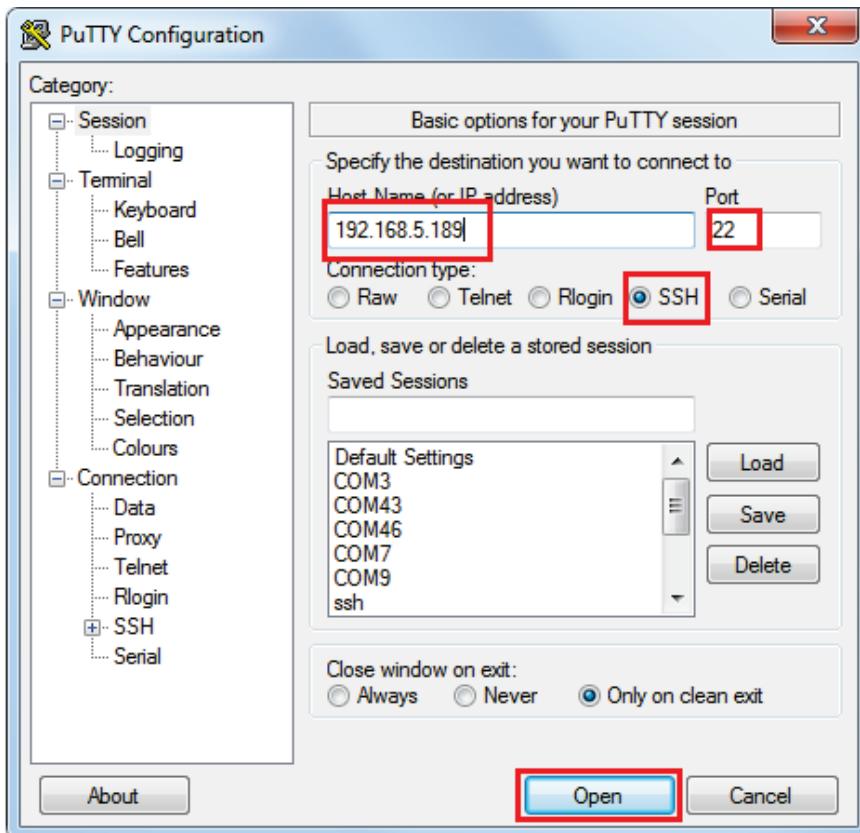


1. Open Putty, input IP address and port, select SSH as connection type, then click button “Open”.

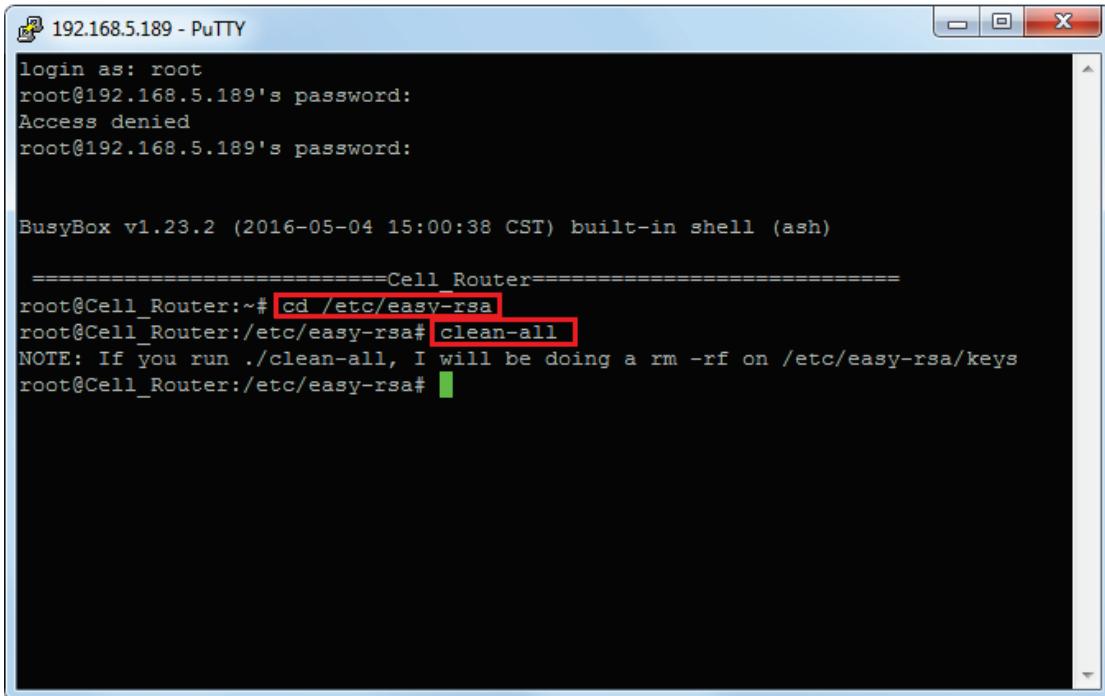


2. Input username and password.

The screenshot shows the Putty terminal window titled '192.168.5.189 - PuTTY'. The session log shows:
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".

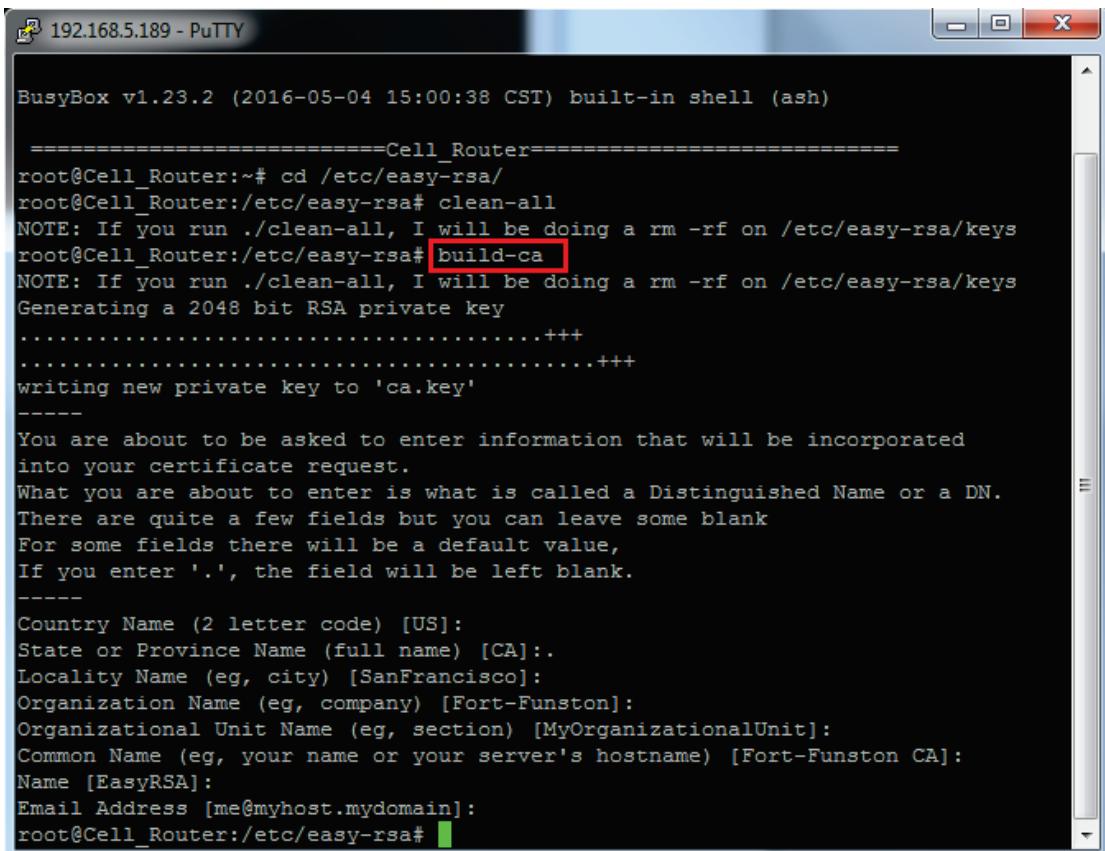


```
192.168.5.189 - PuTTY
login as: root
root@192.168.5.189's password:
Access denied
root@192.168.5.189's password:

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

=====
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#
```

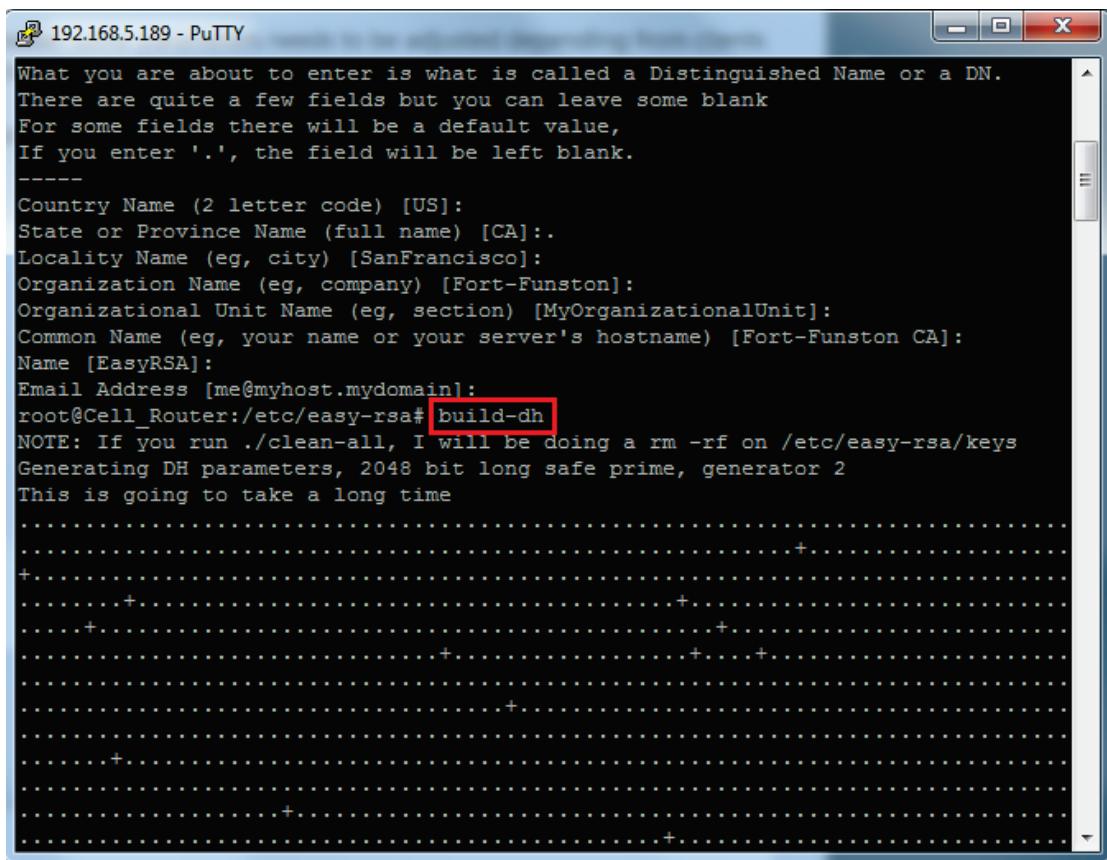
- Run command “build-ca”.



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

=====
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#
```

- 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
.....+
+.....+.....+
.....+.....+.....+
.....+.....+.....+
.....+.....+.....+
.....+.....+.....+

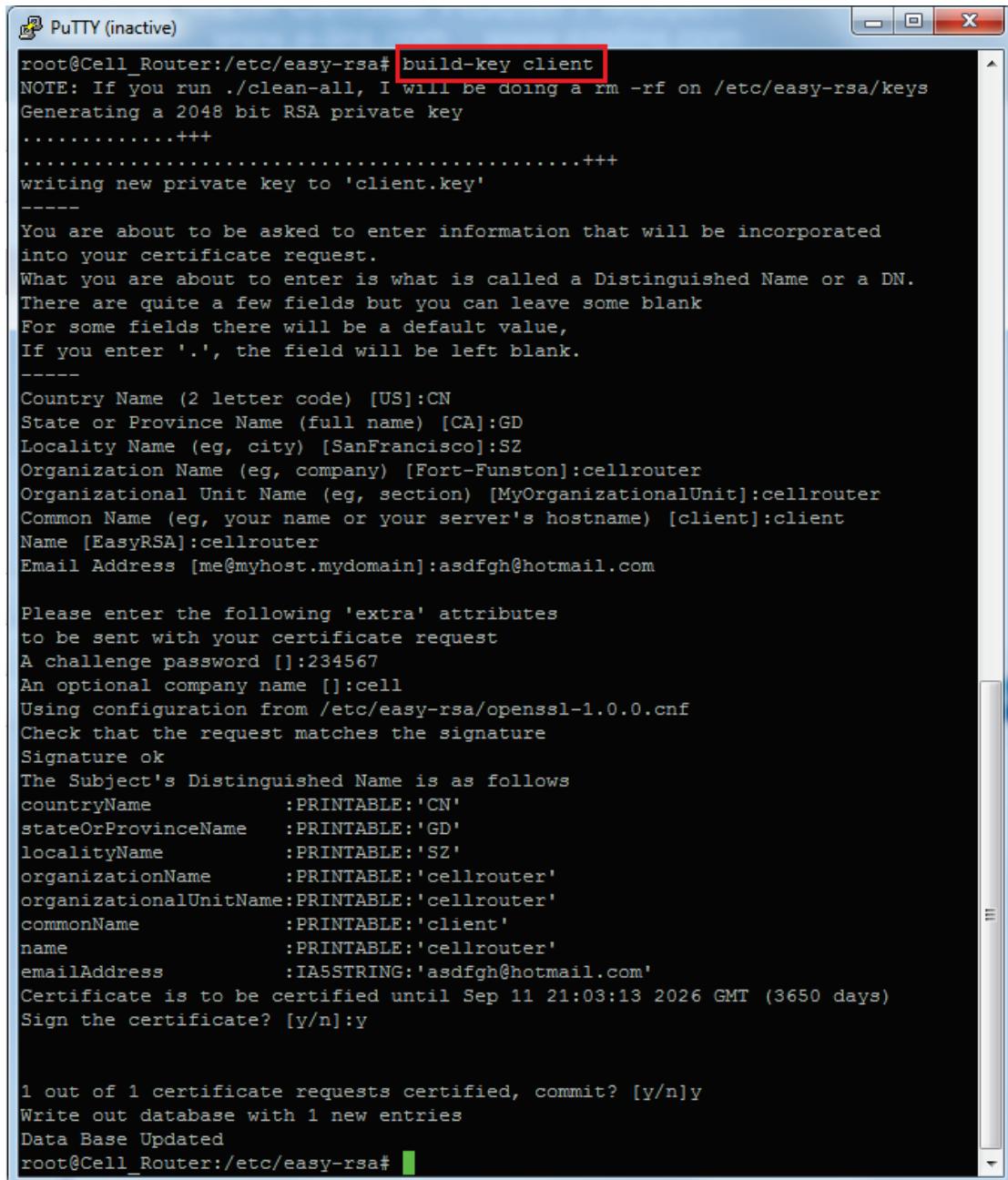
6. Run command “build-key-server server”, you can change “server” to any words you want.

```
PutTY (inactive)
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.



The screenshot shows a PuTTY terminal window titled "PutTY (inactive)". The command "build-key client" is highlighted with a red box. The terminal output is as follows:

```
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#
```

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

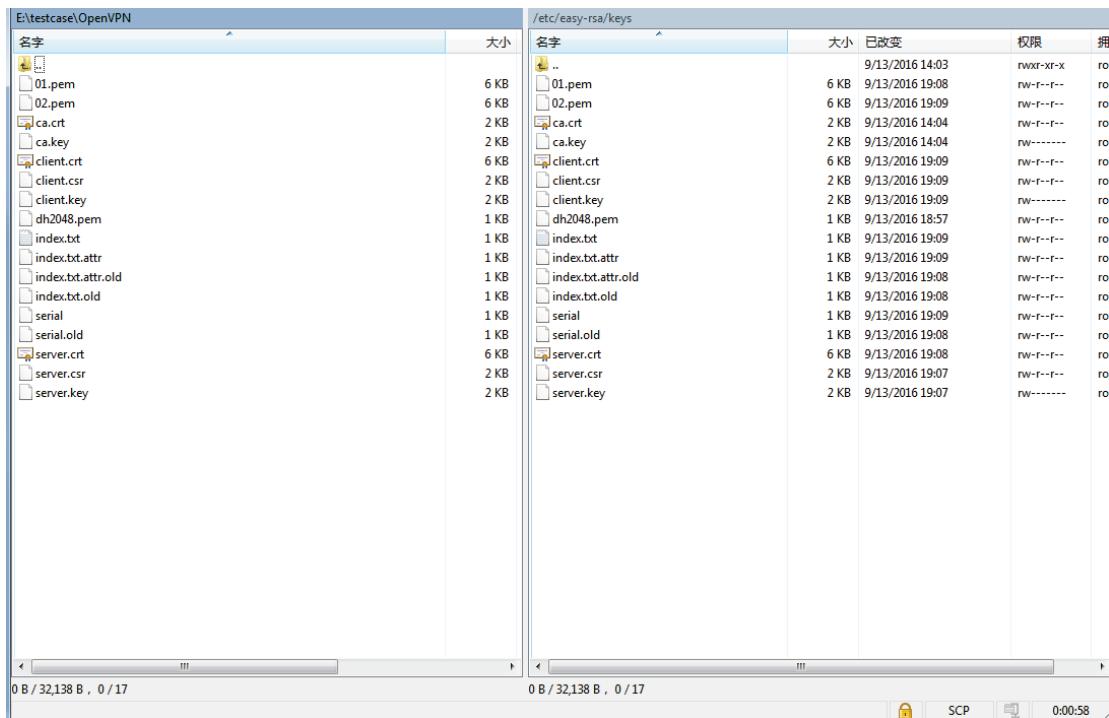
```
192.168.5.189 - PuTTY

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.



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

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

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	<input type="checkbox"/>
verb	3
port	1194
tun_ipv6	<input type="checkbox"/>
server	10.8.0.0 255.255.255.0
nobind	<input type="checkbox"/>
comp_lzo	yes
keepalive	10 120
proto	udp
client	<input type="checkbox"/>
client_to_client	<input type="checkbox"/>
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	<input checked="" type="checkbox"/>
verb	<input type="text" value="3"/> ▼
mlock	<input type="checkbox"/>
disable_occ	<input type="checkbox"/>
passtos	<input type="checkbox"/>
suppress_timestamps	<input type="checkbox"/>
fast_io	<input type="checkbox"/>
status	<input type="text" value="/tmp/openvpn-status.log"/>
down_pre	<input type="checkbox"/>
up_restart	<input type="checkbox"/>
client_disconnect	<input type="checkbox"/>
– Additional Field – ▼ Add	

[Save & Apply](#) [Save](#) [Reset](#)

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 ▾

mlock

The screenshot shows the 'Service' configuration page. At the top, there are checkboxes for 'enabled' (checked) and 'mlock' (unchecked). Below these are dropdown menus for 'verb' (set to 3) and 'disable_occ'. A large red box highlights the 'Additional Field' dropdown menu, which is open and displays a list of options: cd, chroot, log, log_append, nice, echo, remap_usr1, status_version, mute, up, up_delay, down, route_up, setenv, tls_verify, client_connect, learn_address, and auth_user_pass_verify. To the right of the dropdown, a text input field contains the value 'tmp/openvpn-status.log'. At the bottom of the dropdown menu is a button labeled 'Add'. Below the dropdown, there is a footer bar with three buttons: 'Save & Apply' (blue), 'Save' (white), and 'Reset' (white).

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

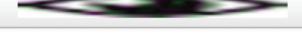
tls_server

– Additional Field –

- secret
- auth
- cipher
- keysize
- engine
- replay_window
- replay_persist
- dh** Add
- pkcs12
- key_method
- tls_cipher
- tls_timeout
- reneg_bytes
- reneg_pkts
- reneg_sec
- hand_window
- tran_window
- tls_auth
- tls_remote

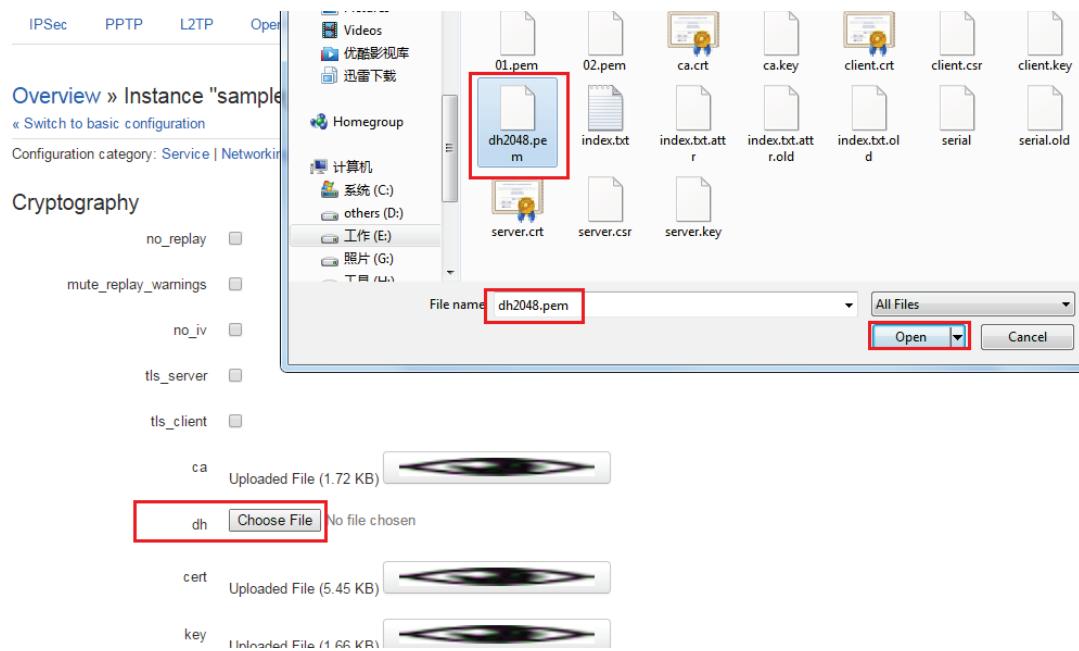
uploaded File (1.72 KB) 

uploaded File (5.45 KB) 

uploaded File (1.66 KB) 

Save & Apply **Save** **Reset**

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

The screenshot shows the 'Networking' configuration page for the 'sample_server' instance. It includes fields for 'port' (set to 1194), 'proto' (set to 'udp'), 'float' (unchecked), 'nobind' (unchecked), 'dev' (set to 'tun'), 'tun_ipv6' (unchecked), 'ifconfig_noexec' (unchecked), 'ifconfig_nowarn' (unchecked), 'route_noexec' (unchecked), and 'mtu_test' (unchecked). At the top, there are buttons for 'Switch to basic configuration', 'Save & Apply', and 'Cancel'.

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

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

The screenshot shows the OpenVPN configuration interface. At the top, there are tabs for IPSec, PPTP, L2TP, OpenVPN (which is selected and highlighted with a red box), and GRE Tunnel. Below the tabs, the title 'OpenVPN' is displayed in blue. Underneath, the heading 'OpenVPN instances' is shown, followed by a note: 'Please goto overview page to restart openVPN instance manually after Save&Apply'. A table lists three instances: 'custom_config' (disabled, no, start button), 'sample_server' (enabled, yes, start button highlighted with a red box), and 'sample_client' (disabled, no, start button). At the bottom, there are fields for 'New instance name:' and 'Client configuration for an etherr', along with 'Save & Apply', 'Save', and 'Reset' buttons.

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

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

The screenshot shows the OpenVPN configuration interface. The 'OpenVPN' tab is selected. The 'sample_server' instance's 'Started' field is highlighted with a red box and contains 'yes (12743)'. The 'Stop' button next to it is also highlighted with a red box. The other instances ('custom_config' and 'sample_client') are listed with their original settings. The bottom section includes fields for 'New instance name:', 'Client configuration for an etherr', and 'Save & Apply', 'Save', and 'Reset' buttons.

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”.

The screenshot shows the 'OpenVPN' configuration page. On the left, a sidebar lists various services: Status, System, Services (highlighted with a red box), ICMP Check, VRRP, Failover, SNMP, DTU, GPS, SMS, VPN (highlighted with a red box), DDNS, Connect Radio Module, Network, and Logout. The main area is titled 'OpenVPN' and contains a table for 'OpenVPN instances'. The table has columns: Name, enabled, Started, Start/Stop, Tun/Tap, Port, Protocol. Three instances are listed: 'custom_config' (disabled, no start button), 'sample_server' (disabled, no start button), and 'sample_client' (disabled, no start button). Below the table is a 'New instance name:' input field, a 'Client configuration for an ethernet' dropdown, and a 'Add' button. At the bottom are 'Save & Apply', 'Save', and 'Reset' buttons. The 'Edit' button for 'sample_client' is also highlighted with a red box.

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

The screenshot shows the 'Overview » Instance "sample_client"' configuration page. It includes fields for 'enabled' (checked), 'verb' (set to 3), 'tun_ipv6' (unchecked), 'nobind' (checked), 'comp_lzo' (set to yes), 'proto' (set to udp), 'client' (checked), 'client_to_client' (unchecked), 'remote' (set to my_server_1 1194), and a 'Save & Apply' button. The 'client' checkbox is highlighted with a red box.

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

– Additional Field –

- secret
- auth
- cipher
- keysize
- engine
- replay_window
- replay.persist
- ca**
- dh
- cert
- key
- pkcs12
- key.method
- tls.cipher
- tls.timeout
- reneg.bytes
- reneg.pkts
- reneg.sec
- hand.window

– Additional Field –

Save & Apply

Save

Reset

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

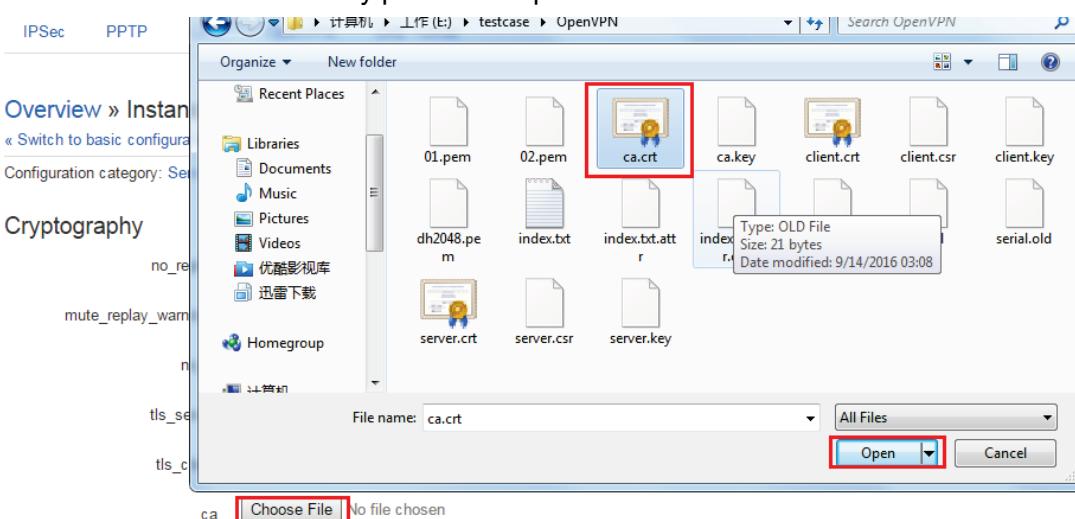


Save & Apply

Save

Reset

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



ca No file chosen

single_session

tls_exit

auth_nocache

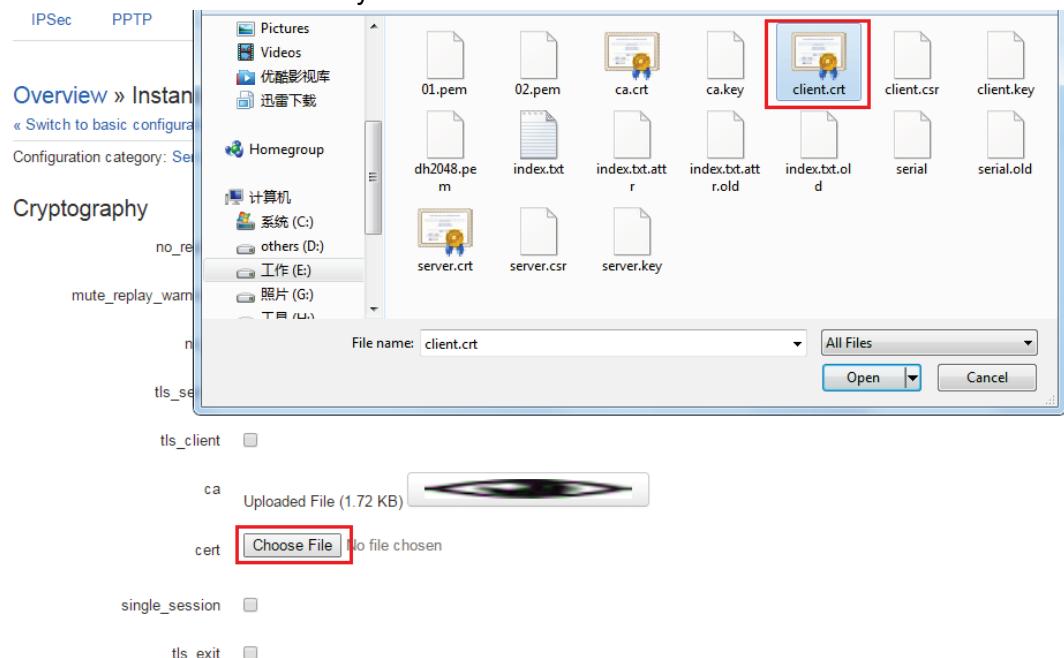


Save & Apply

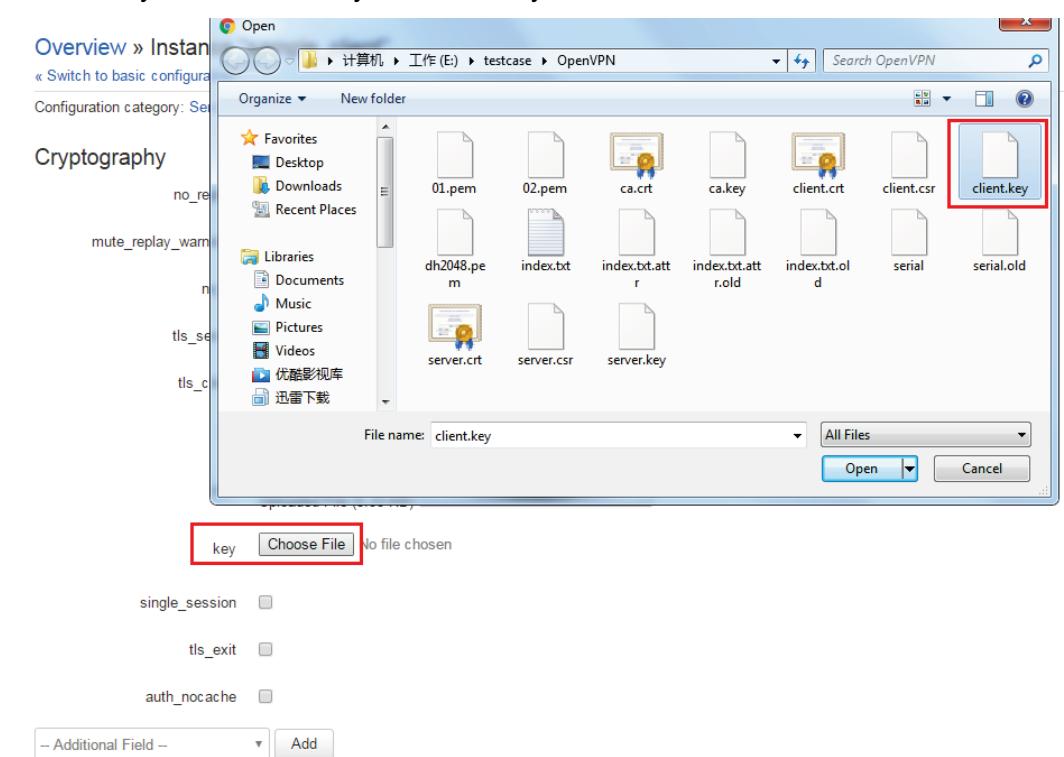
Save

Reset

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 configuration.

[« 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) 

cert Uploaded File (5.33 KB) 

key client.key

single_session

tls_exit

auth_nocache

-- Additional Field --

Save & Apply

Save

Reset

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”.

IPSec PPTP L2TP OpenVPN GRE Tunnel

Overview » Instance "sample_client"

[« Switch to basic configuration](#)

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

VPN

client

pull

remote

remote_random

http_proxy_retry

resolv_retry

– Additional Field –

Save & Apply **Save** **Reset**

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

IPSec PPTP L2TP OpenVPN GRE Tunnel

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	 <input type="button" value="start"/>	tun	1194	udp
sample_server	No	no	 <input type="button" value="start"/>	tun	1194	udp
sample_client	Yes	no	 <input checked="" type="button" value="start"/>	tun	1194	udp

New instance name:

Client configuration for an ether

Save & Apply

Save

Reset

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		tun	1194	udp
sample_server	No	no		tun	1194	udp
sample_client	Yes	yes (14788)		tun	1194	udp

New instance name: Client configuration for an etherr ▾

Save & Apply **Save** **Reset**

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.

Status

- Overview
- Network
- Firewall
- Routes
- System Log**
- Kernel Log
- Reboot Log
- Realtime Graphs
- VPN
- System
- Services
- Network
- Logout

System Log

```

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 60 seconds (the timeout), closes the connection and exits. This may be caused by a network timeout, or a failure to negotiate a cipher suite compatible between client and server.
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 rekeyed
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 60 seconds (the timeout), closes the connection and exits. This may be caused by a network timeout, or a failure to negotiate a cipher suite compatible between client and server.
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 rekeyed
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 60 seconds (the timeout), closes the connection and exits. This may be caused by a network timeout, or a failure to negotiate a cipher suite compatible between client and server.
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 rekeyed
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 60 seconds (the timeout), closes the connection and exits. This may be caused by a network timeout, or a failure to negotiate a cipher suite compatible between client and server.
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 rekeyed
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 60 seconds (the timeout), closes the connection and exits. This may be caused by a network timeout, or a failure to negotiate a cipher suite compatible between client and server.
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 rekeyed
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

General Settings (highlighted by a red box)

Local Time: Wed Sep 14 04:02:06 2016 Sync with browser (highlighted by a red box)

Hostname: Cell_Router

Timezone: UTC

Save & Apply **Save** **Reset**

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

The screenshot shows the configuration interface for a device. On the left, a sidebar lists various system and network services. The 'VPN' service is selected and highlighted with a red box. The main area shows an 'Overview' for the 'sample_server' instance. Under the 'Networking' tab, there are several configuration fields: 'port' set to 1194, 'proto' set to udp, 'float' (checkbox), 'nobind' (checkbox), 'dev' set to tun, 'tun_ipv6' (checkbox), 'ifconfig_noexec' (checkbox), 'ifconfig_nowarn' (checkbox), and a 'route' field containing 192.168.10.0 255.255.255.0, which is also highlighted with a red box.

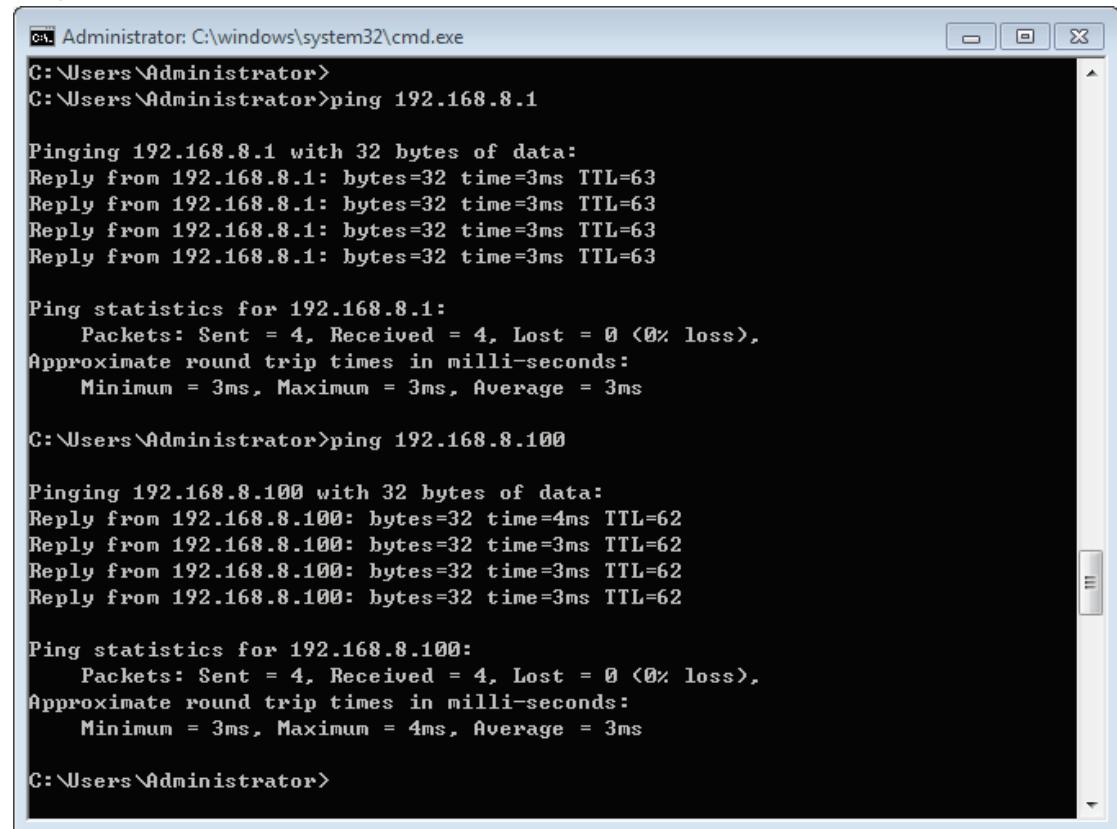
17. Add push on server

This screenshot shows the 'VPN' configuration for the 'sample_server' instance. The 'VPN' service is selected in the sidebar and highlighted with a red box. In the main configuration area, under the 'VPN' tab, there are fields for 'client' (checkbox), 'server' (10.8.0.0 255.255.255.0), 'push' (checkbox), and 'push_reset' (checkbox). The 'push' field contains route 192.168.8.0 255.255.255.0, which is highlighted with a red box. Other fields include 'disable' (checkbox), 'ifconfig_pool_persist' (/tmp/ipp.txt), and 'client_to_client' (checkbox).

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.



The screenshot shows a Windows Command Prompt window titled "Administrator: C:\windows\system32\cmd.exe". The command "ping 192.168.8.1" is run, resulting in four successful replies from the target IP. Then, "ping 192.168.8.100" is run, also resulting in four successful replies. Both pings include statistics showing 0% loss and low round-trip times (3ms to 4ms).

```
C:\Administrator: C:\windows\system32\cmd.exe
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

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

Status

System

Services

ICMP Check

VRRP

Failover

SNMP

DTU

GPS

SMS

VPN

DDNS

Connect Radio Module

Network

Logout

IPSec

PPTP

L2TP

OpenVPN

GRE Tunnel

Overview » Instance "sample_server"

« Switch to basic configuration

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

VPN

client

server

push

push_reset

disable

ifconfig_pool_persist

client_to_client

duplicate_cn

client_config_dir

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.