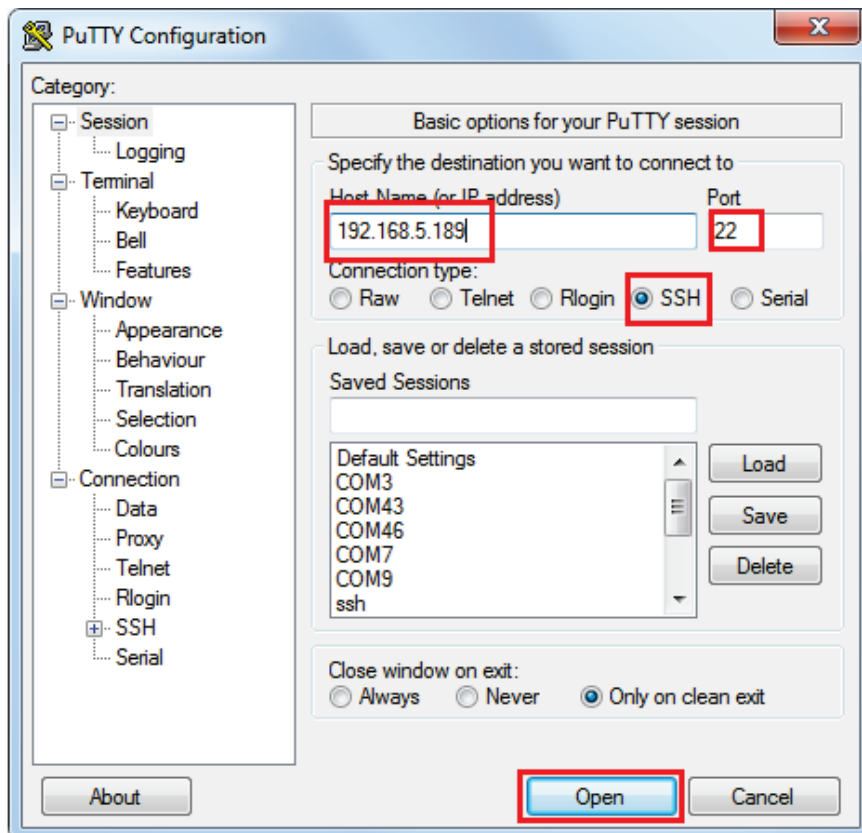
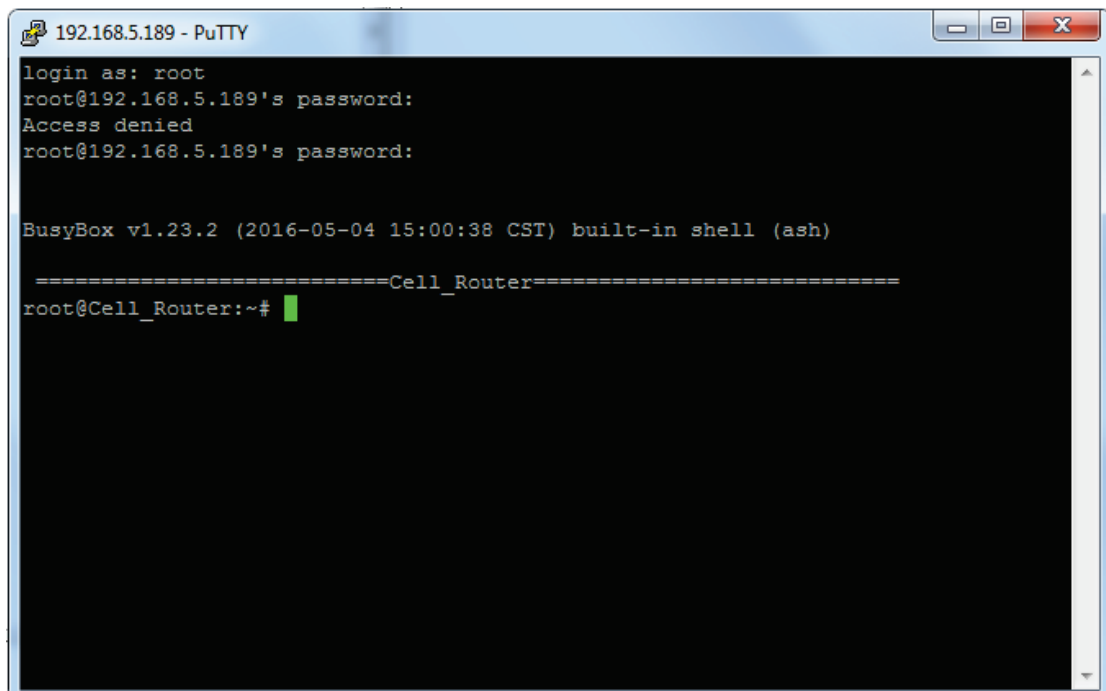


1. Open Putty, input IP address and port, select SSH as connection type, then click button "Open".



2. Input username and password.



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

```
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)

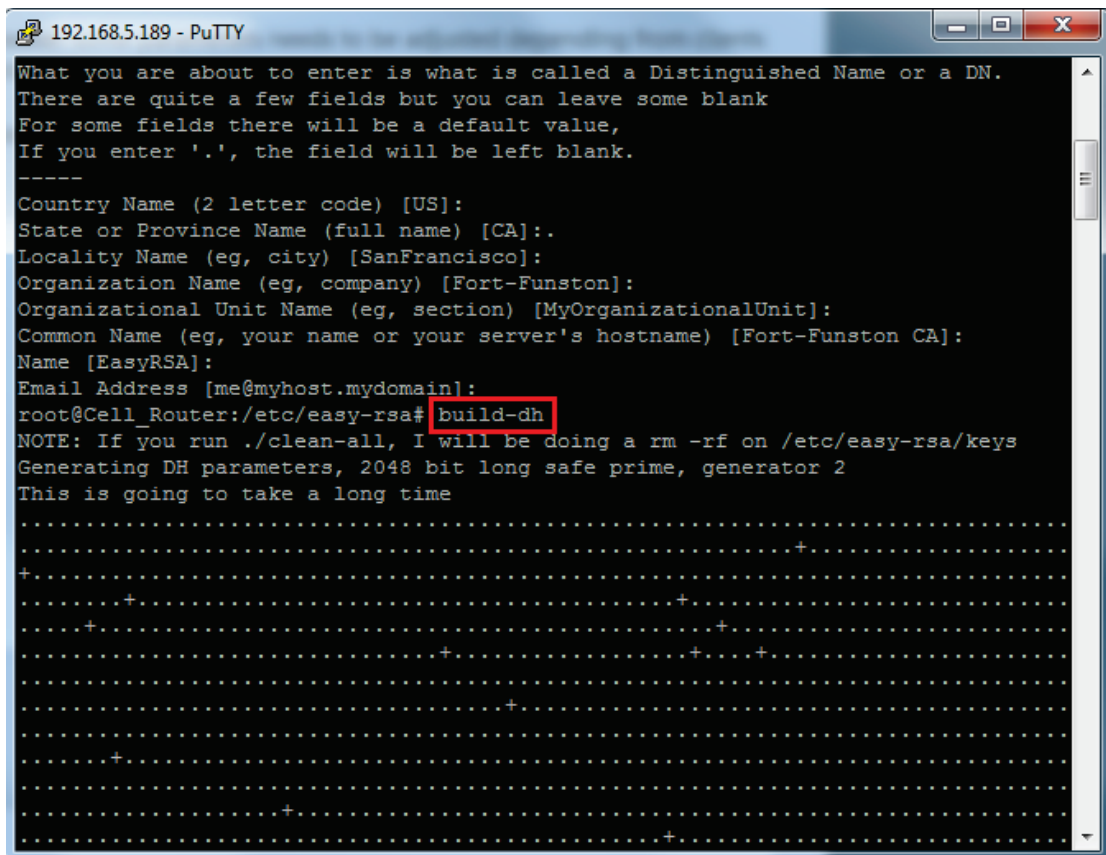
=====Cell Router=====
root@Cell_Router:~# cd /etc/easy-rsa
root@Cell_Router:/etc/easy-rsa# clean-all
NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/easy-rsa/keys
root@Cell_Router:/etc/easy-rsa#
```

4. Run command "build-ca".

```
192.168.5.189 - PuTTY
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.



```
192.168.5.189 - PuTTY
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      :IASSTRING:'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#
```

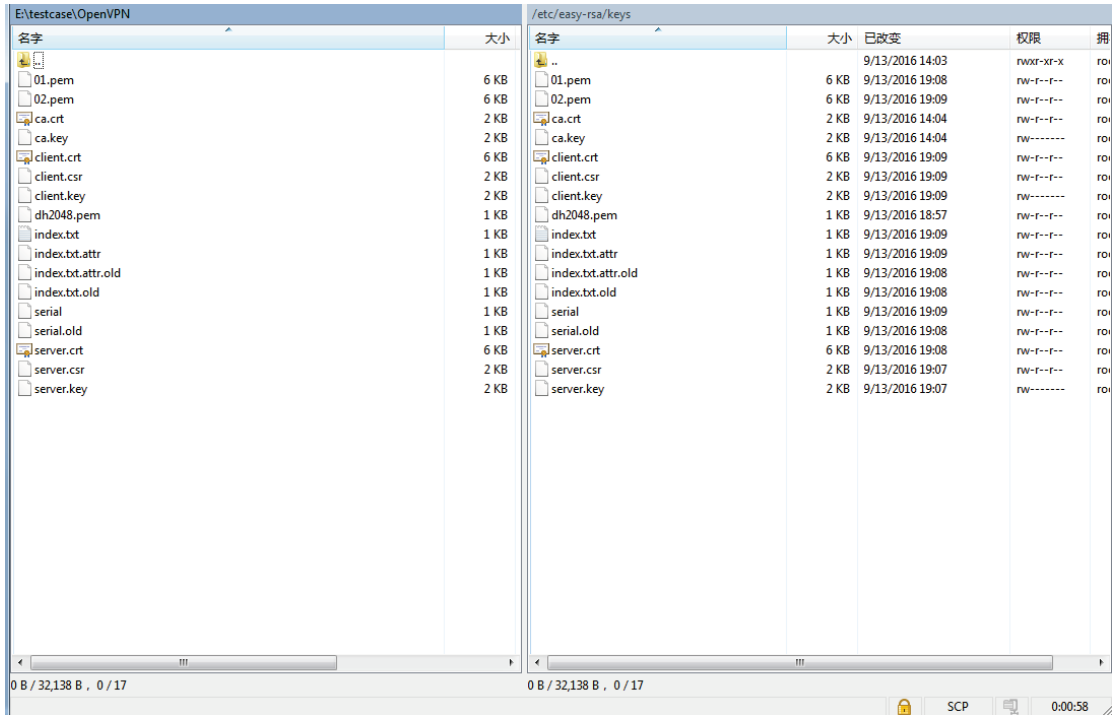
8. Run command "cd /etc/easy-rsa/keys/" and "cp ca.crt ca.key dh2048.pem server.key server.crt/etc/openssl/"

```
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]:

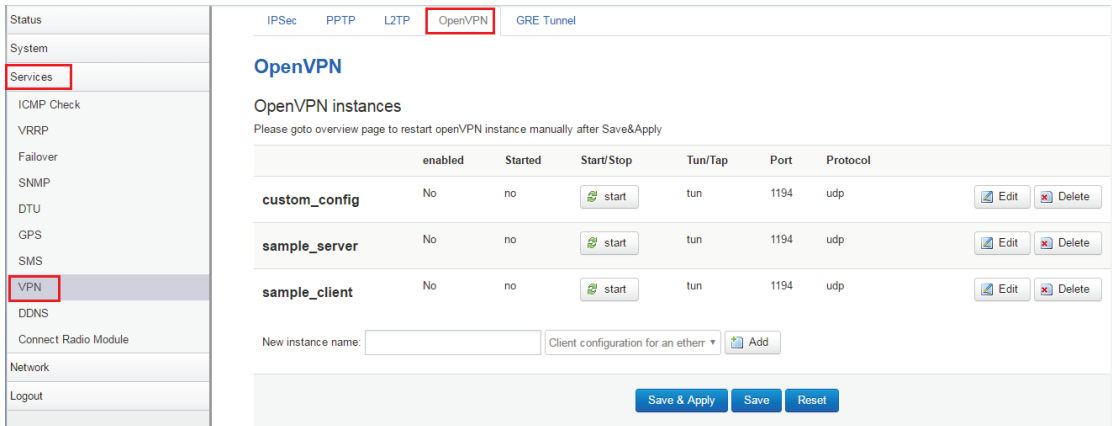
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:123456
An optional company name []:
Using configuration from /etc/easy-rsa/openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName       :PRINTABLE:'US'
stateOrProvinceName :PRINTABLE:'CA'
localityName      :PRINTABLE:'SanFrancisco'
organizationName  :PRINTABLE:'Fort-Funston'
organizationalUnitName:PRINTABLE:'MyOrganizationalUnit'
commonName        :PRINTABLE:'client'
name              :PRINTABLE:'EasyRSA'
emailAddress      :IASSTRING:'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.



- 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\_server. Then click “Switch to advanced configuration”.

## Overview » Instance "sample\_server"

[Switch to advanced configuration »](#)

enabled	<input type="checkbox"/>
verb	<input type="text" value="3"/>
port	<input type="text" value="1194"/>
tun_ipv6	<input type="checkbox"/>
server	<input type="text" value="10.8.0.0 255.255.255.0"/>
nobind	<input type="checkbox"/>
comp_lzo	<input type="text" value="yes"/>
keepalive	<input type="text" value="10 120"/>
proto	<input type="text" value="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"/>

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

disable\_occ

-- Additional Field --

- 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
- auth\_user\_pass\_verify

-- Additional Field --

Save & Apply

Save

Reset

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**
- pkcs12
- key\_method
- tls\_cipher
- tls\_timeout
- reneg\_bytes
- reneg\_pkts
- reneg\_sec
- hand\_window
- tran\_window
- tls\_auth
- tls\_remote

dh

loaded File (1.72 KB)

loaded File (5.45 KB)

loaded File (1.66 KB)

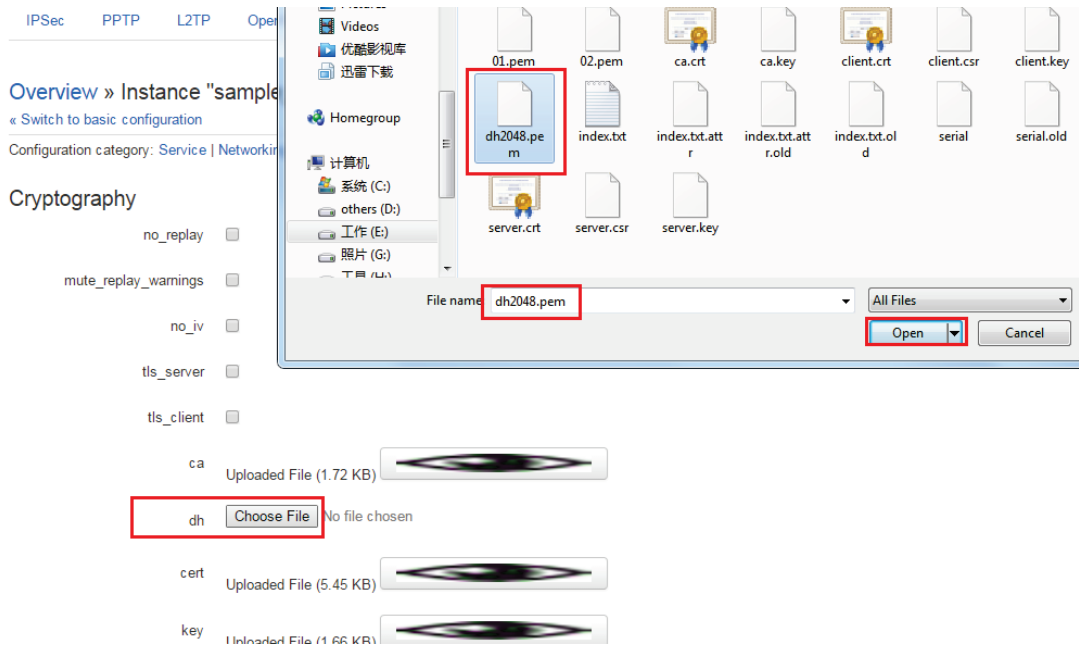
Add

Save & Apply

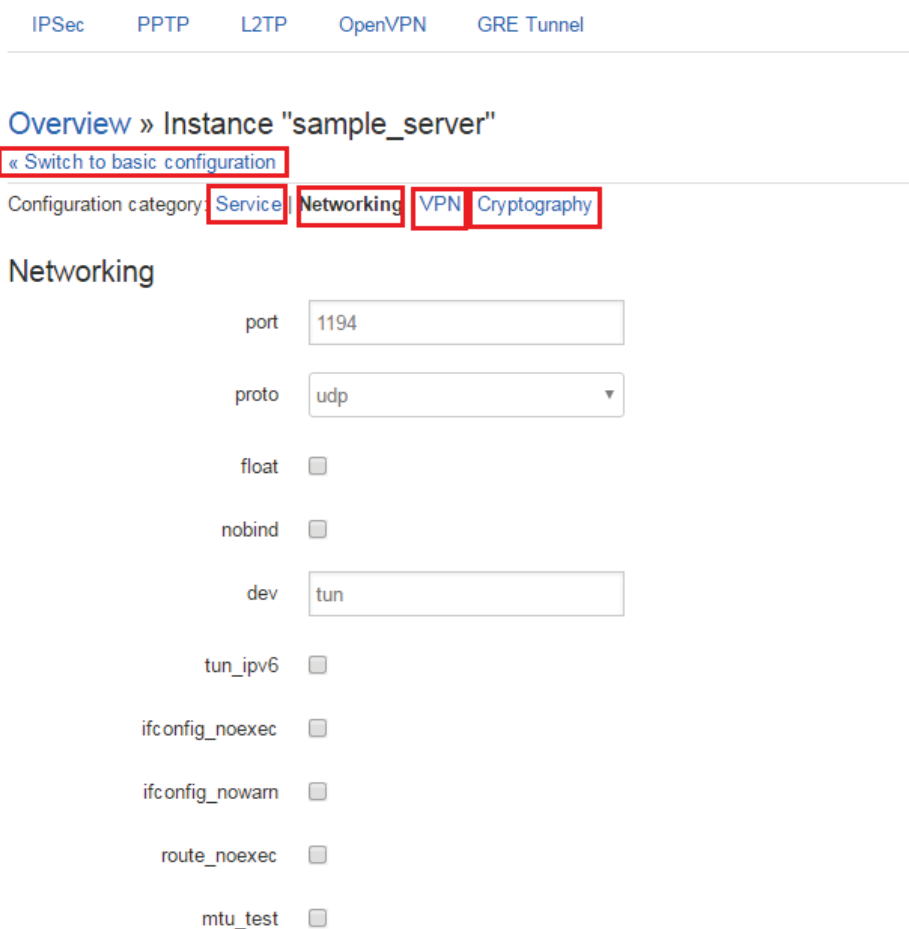
Save

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 tab option, you must press button “Save” to avoid losing configuration



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



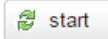
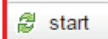
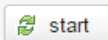
18. Goto OpenVPN overview page to start sample\_server by click button “start”.

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
<b>custom_config</b>	No	no		tun	1194	udp
<b>sample_server</b>	Yes	no		tun	1194	udp
<b>sample_client</b>	No	no		tun	1194	udp

New instance name:  Client configuration for an ethernet



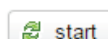
19. If “Started” is changed from “start” to “Yes(XXX)”, that means server started successfully. And you can stop it by click button “Stop”.

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
<b>custom_config</b>	No	no		tun	1194	udp
<b>sample_server</b>	Yes	yes (12743)		tun	1194	udp
<b>sample_client</b>	No	no		tun	1194	udp

New instance name:  Client configuration for an ethernet

## 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”.

	enabled	Started	Start/Stop	Tun/Tap	Port	Protocol	
custom_config	No	no	<a href="#">start</a>	tun	1194	udp	<a href="#">Edit</a> <a href="#">Delete</a>
sample_server	No	no	<a href="#">start</a>	tun	1194	udp	<a href="#">Edit</a> <a href="#">Delete</a>
sample_client	No	no	<a href="#">start</a>	tun	1194	udp	<a href="#">Edit</a> <a href="#">Delete</a>

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

enabled

verb

tun\_ipv6

nobind

comp\_lzo

proto

client

client\_to\_client

remote

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

Configuration list for 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

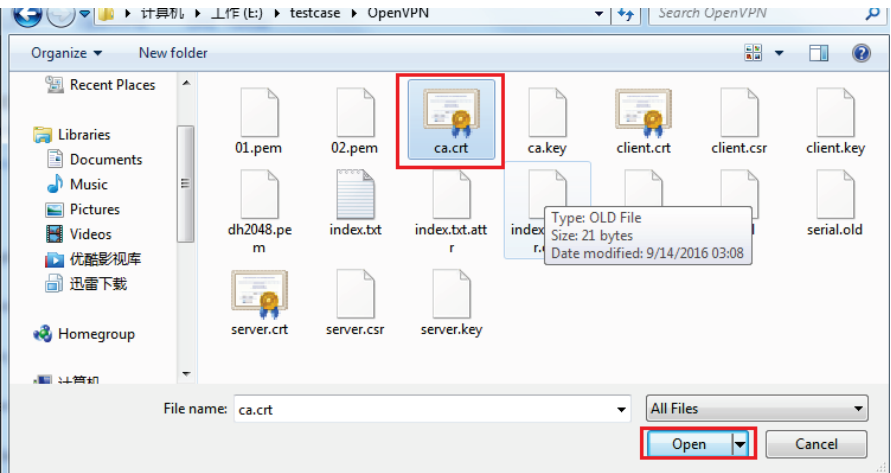
auth\_nocache

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.



The screenshot shows a Windows file explorer window titled "OpenVPN" with the path "计算机 > 工作 (E:) > testcase > OpenVPN". The file list includes: 01.pem, 02.pem, ca.crt (highlighted with a red box), ca.key, client.crt, client.csr, client.key, serial.old, dh2048.pem, index.bt, index.bt.att, index.r, server.crt, server.csr, and server.key. A tooltip for ca.crt shows: Type: OLD File, Size: 21 bytes, Date modified: 9/14/2016 03:08. The "File name" field contains "ca.crt" and the "Open" button is highlighted with a red box.

ca  No file chosen

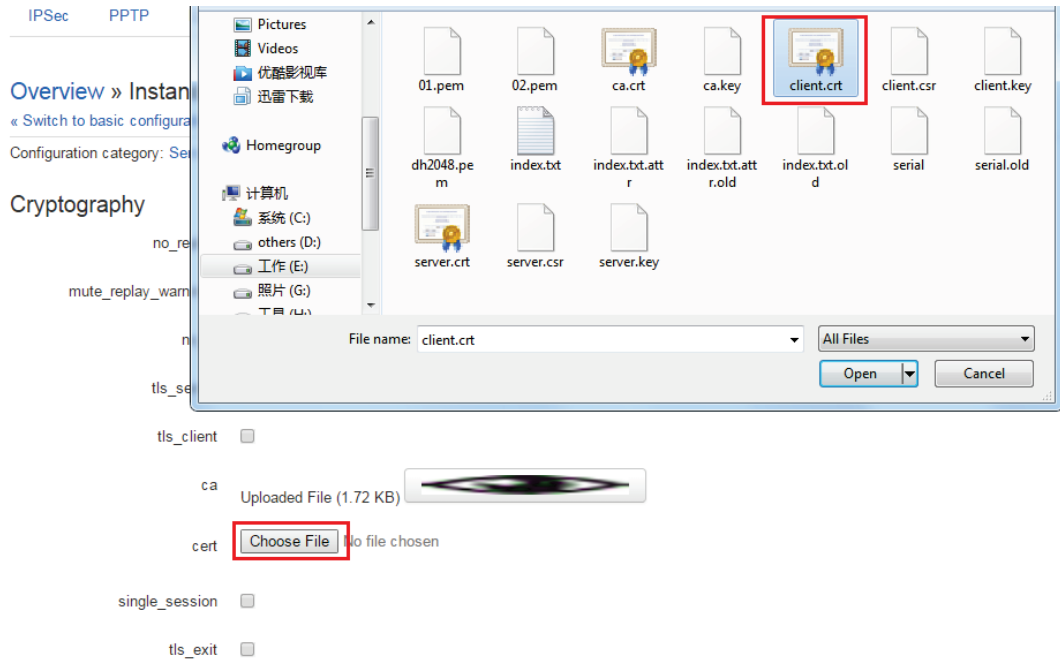
single\_session

tls\_exit

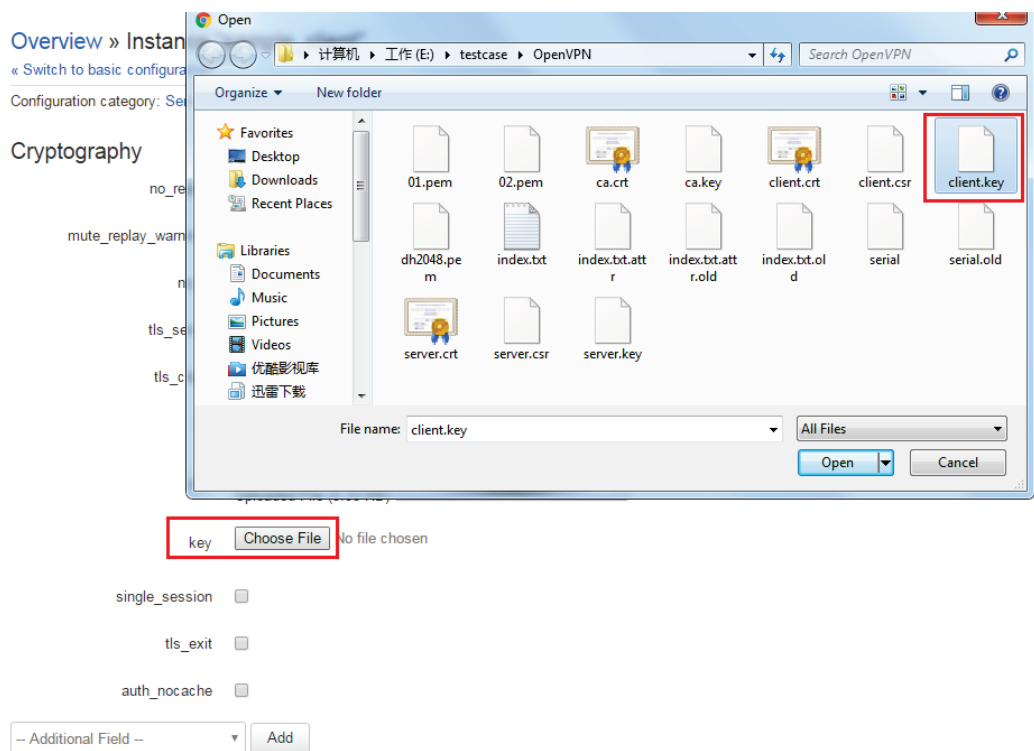
auth\_nocache

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

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 --

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

New instance name:  Client configuration for an ether:

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
<b>custom_config</b>	No	no	start	tun	1194	udp
<b>sample_server</b>	No	no	start	tun	1194	udp
<b>sample_client</b>	Yes	yes (14788)	stop	tun	1194	udp

New instance name:  Client configuration for an etherr ▾ Add

- 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 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.err 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]: 192.168.5.139:38311 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:

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

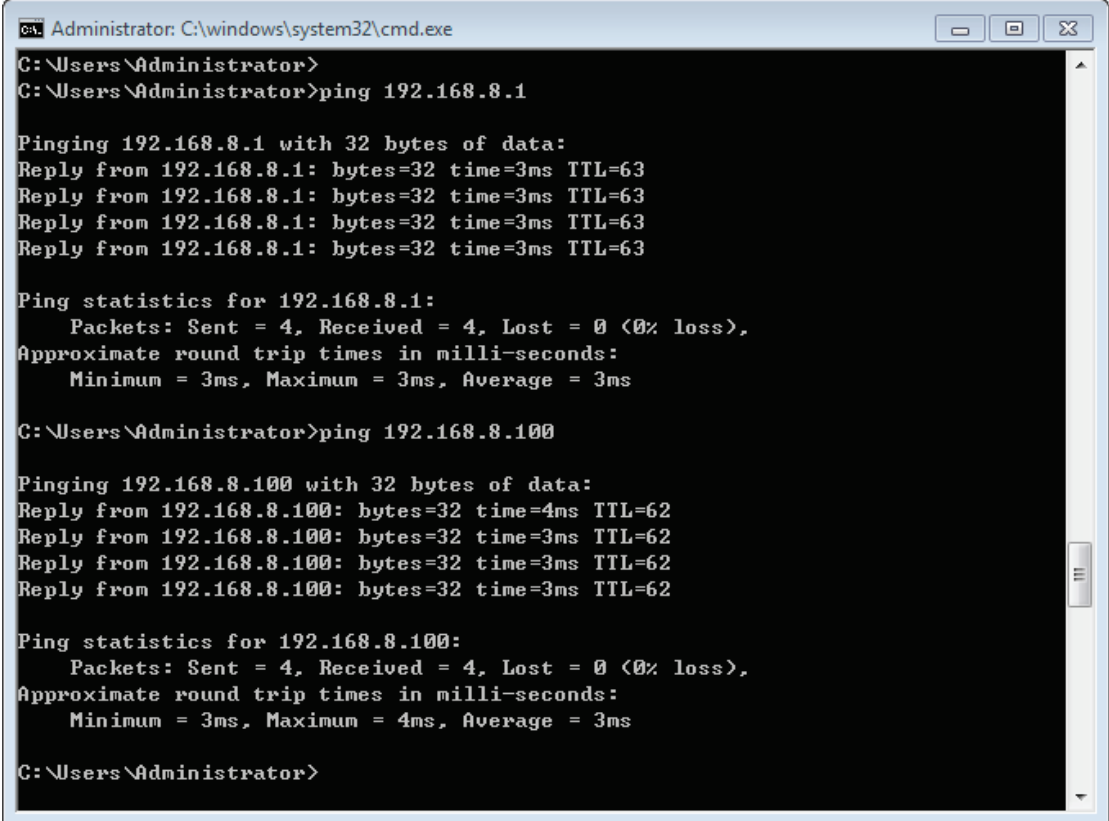
The screenshot shows the Mikrotik WinBox configuration interface for an OpenVPN instance named "sample\_server". The left sidebar has a menu with "VPN" highlighted. The main content area shows the "Networking" configuration tab. The "port" is set to 1194 and "proto" is set to "udp". A "route" field is added with the value "192.168.10.0 255.255.255.0".

17. Add push on server

The screenshot shows the Mikrotik WinBox configuration interface for the same OpenVPN instance "sample\_server". The left sidebar has "VPN" highlighted. The main content area shows the "VPN" configuration tab. The "server" field is set to "10.8.0.0 255.255.255.0". A "push" field is added with the value "route 192.168.8.0 255.255.255.0".

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.



```
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
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

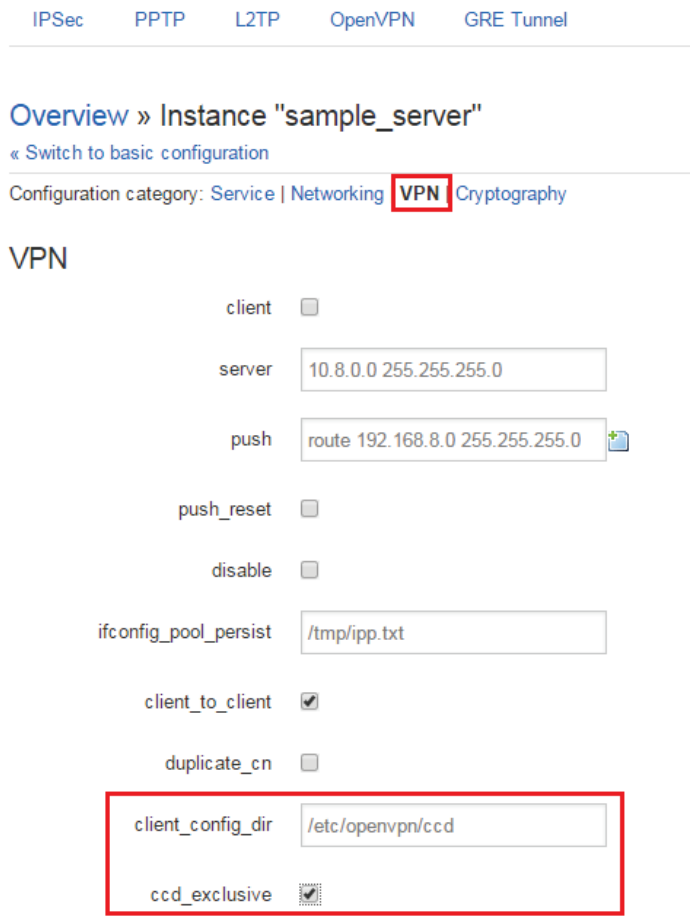
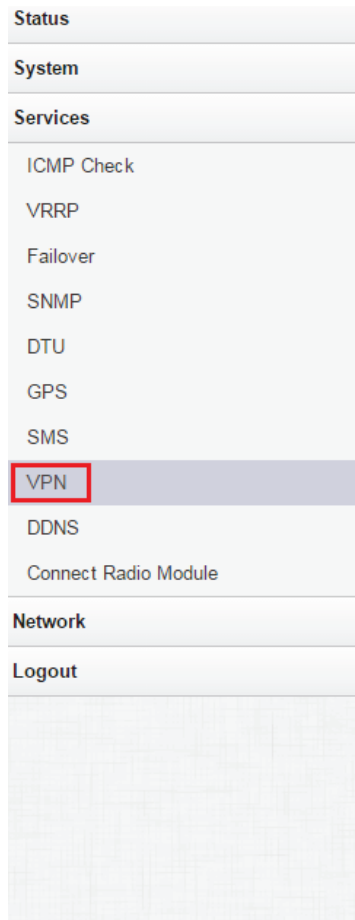
C:\Users\Administrator>ping 192.168.8.100

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



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 "route 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.