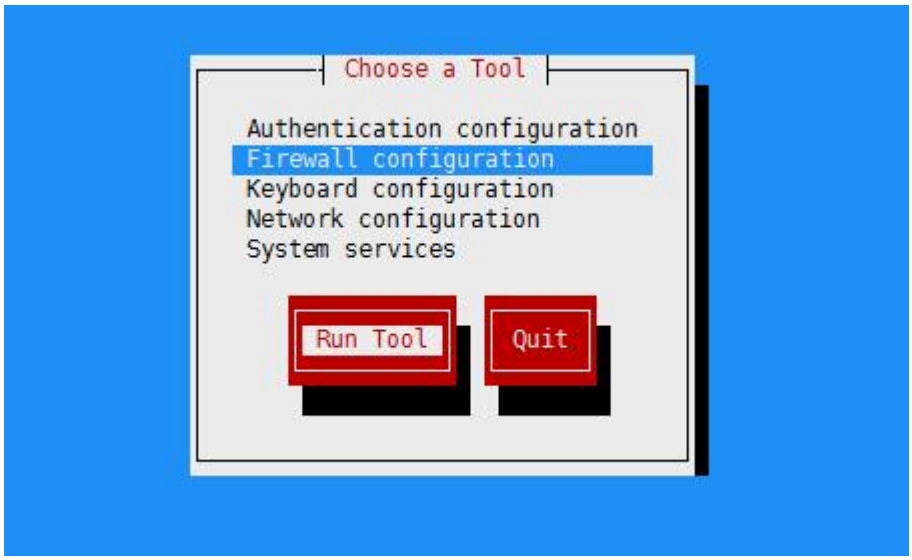
Catalogues

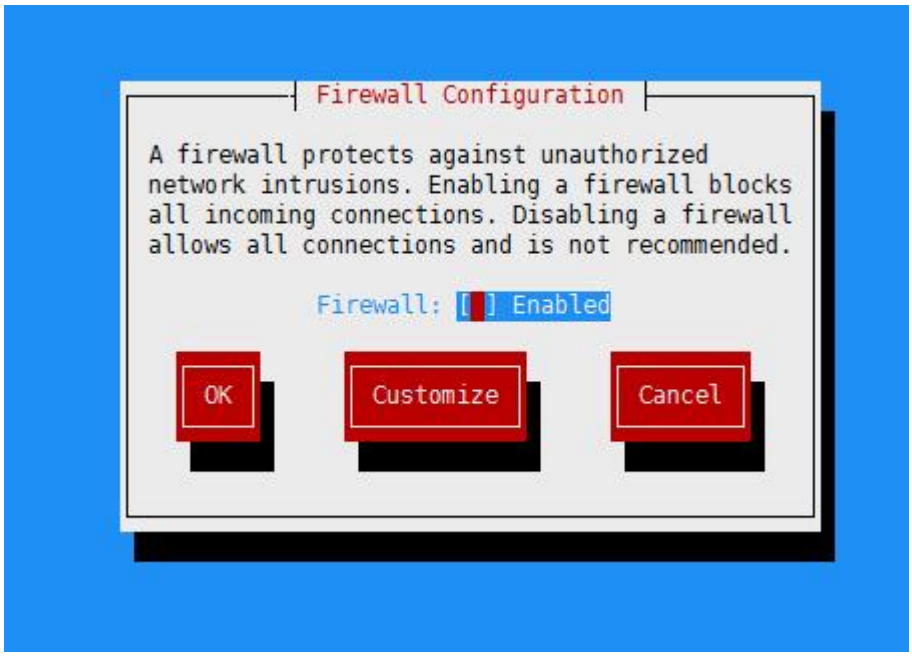
Introduction of OpenVPN Installation

Environment of Installation

Install Centos 6.5，close the firewall after installation.
Command：setup
Enter Diagram Configuration，select “Firewall configuration”.



Enter the below interface by pressing Enter，remove the selection before “enable”，Switch to OK and press Enter by using “table” key. And click “yes” to finish the configuration in the pop-up warning page.



Install gcc, openssl, lzo, pam under Centos. Input below command to finish the

installation.
Command：yum install -y gcc openssl-devel lzo-devel pam-devel

Install OpenVPN

1. Put the installation package of OpenVPN into the directory /usr/local, can it can be finished directly by SSH.
2. Extract OpenVPN
   Command：tar zxf openvpn-2.3.8.tar.gz
3. Compiling and installation for OpenVPN
   Command：
   cd openvpn-2.3.8
   Introduction：Enter the compressing directory
   ./configure
   make
   make insitall
   Above 3 commands for compile & install OpenVPN.
4. Confirm the installation is successful.
   Command：which openvpn
   The installation is successful while it shows “/usr/local/sbin/openvpn”

Produce the License

Below is how to produce the license of server & client by easy-rsa2.0

Prepare the environment for production

Put the downloaded easy-rsa-release-2.x.zip file in the directory /usr/local, and execute the below commands one by one:
Extract easy-rsa
Command：unzip -q easy-rsa-release-2.x.zip
Copy to OpenVPN directory
Command：cp -r easy-rsa-release-2.x/easy-rsa /usr/local/openvpn-2.3.8
Enter the directory
Command：/usr/local/openvpn-2.3.4/easy-rsa/2.0
Edit vars file in order to fix some variables during each generation.
Command：vi vars
Pay attention to edit the below contents, and leave others as default.
KEY_SIZE：It represents the length of the key, we setup it to 1024.
Below are some configurations for user:
KEY_COUNTRY：Country
KEY_PROVINCE：Province
KEY_CITY：City

KEY_ORG：Organization
KEY_EMAIL：Email
KEY_OU：Organization or Unit
Below are the contents which finished edit.

```
# These are the default values for fields
# which will be placed in the certificate.
# Don't leave any of these fields blank.
export KEY_COUNTRY="CN"
export KEY_PROVINCE="ShangHai"
export KEY_CITY="XuHui"
export KEY_ORG="NewRock"
export KEY_EMAIL="hyang@newrocktech.com"
export KEY_OU="MyOvpn"
```

Produce the CA License

The CA license can be used on the server and the client; however, the common name field must be unique. As a result, it cannot be applied to the server and the client that will be developed later.
Command：. ./vars
It shows the below notice：

```
[root@localhost 2.0]# . ./vars
NOTE: If you run ./clean-all, I will be doing a rm -rf on /usr/local/easy-rsa-release-2.x/easy-rsa/2.0/keys
```

Command：./clean-all
This command is only required if the key was previously produced, it is not required ifthe key is being produced for the first time.
Command：./build-ca
It shows as below：

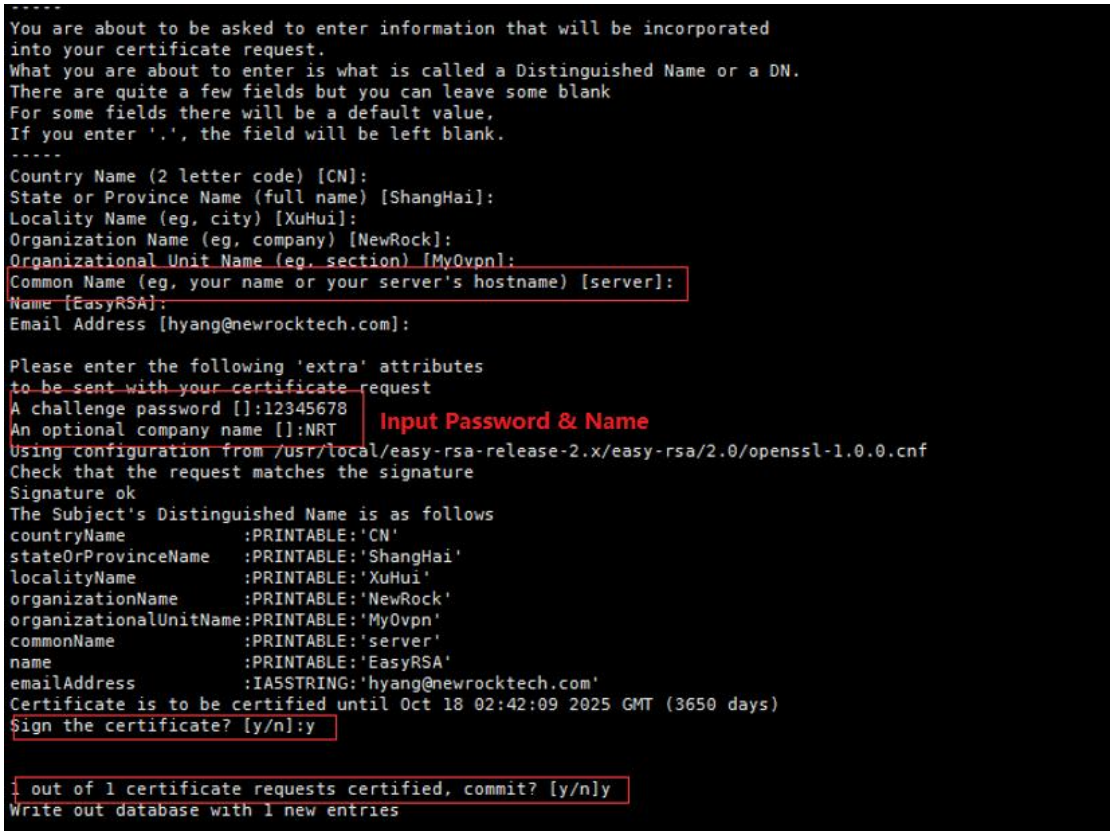
```
[root@localhost 2.0]# ./build-ca
Generating a 1024 bit RSA private key
....++++++
.....................................++++++
writing new private key to 'ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter 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) [CN]:
State or Province Name (full name) [ShangHai]:
Locality Name (eg, city) [XuHui]:
Organization Name (eg, company) [NewRock]:
Organizational Unit Name (eg, section) [MyOvpn]:
Common Name (eg, your name or your server's hostname) [NewRock CA]:
Name [EasyRSA]:
Email Address [hyang@newrocktech.com]:
```

The name must be unique here,it's NewRock CA now

Create the Server License

Command：. /build-key-server server
It appears as follows: pay attention to the uniqueness of the common name, enter the

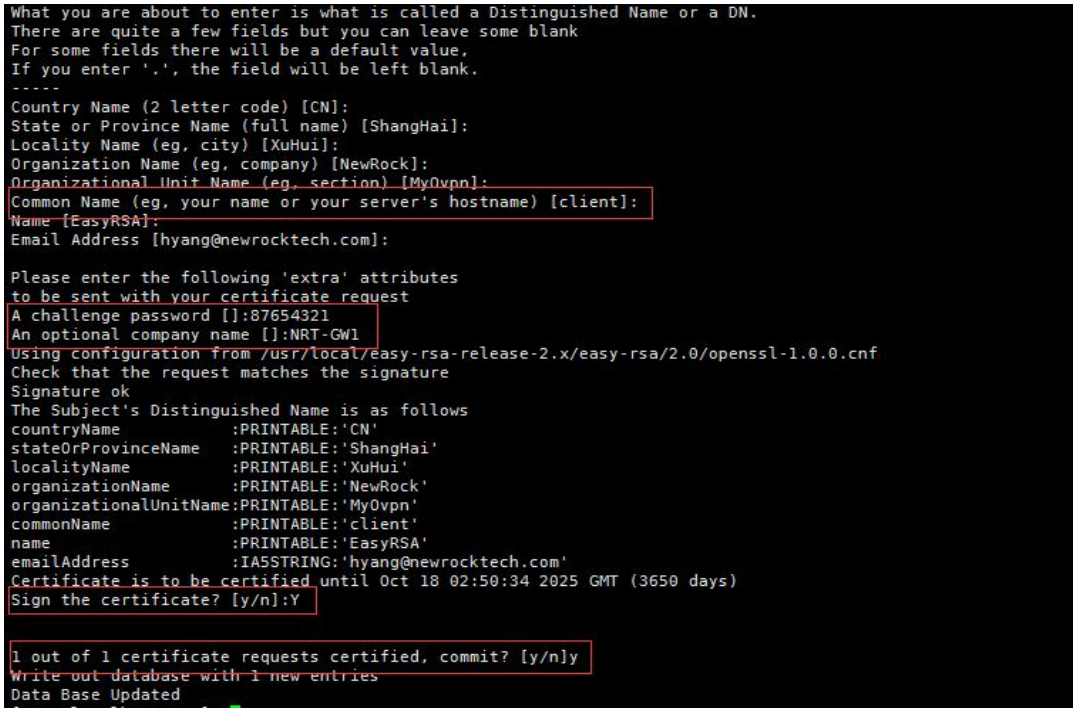
password and the company's name, and lastly hit "y" twice to complete the configuration.



Create the Client License

Command：. /build-key client

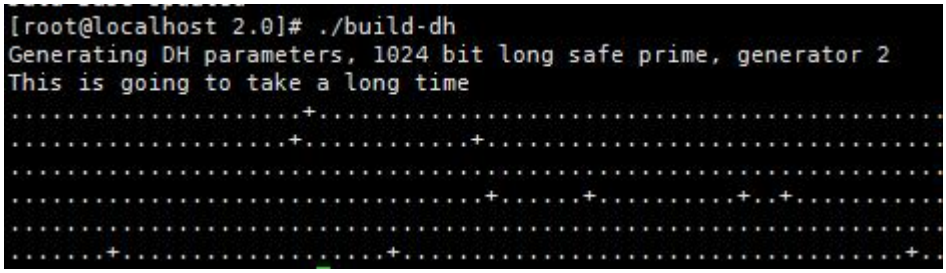
It appears as follows: pay attention to the uniqueness of the common name, enter the password and the company's name, and lastly hit "y" twice to complete the configuration.



Note: Client is the file name, if you wish to create many licenses, you can give it a random name. For example: "./build-key client2"

Create the Diffie–Hellman Key Exchange(D-H)

Additionally, we also need to create the Diffie-Hellman Key Exchange(D-H) for the server of OpenVPN, and the Diffie-Hellman Key Exchange(D-H) is a kind of safety protocol used for data encryption.
Command：./build-dh
If it shows as below, then just wait for it finishes configuration.



Create the TLS-auth Key

OpenVPN provides the TLS-auth Function, and it can defense the Dos and UDP Port flooding attacks.
Command：openvpn --genkey --secret keys/ta.key

Create the Client License again

If you want to create new client or carry out other operations, then you only need to run the command . ./vars, and then run the corresponding command, such as ./build-key client2

Details of the file

These are files which the server needs: ca.key, ca.crt, dh1024.pem, server.crt, server.key, ta.key
These are files which the client needs: ca.crt、client.crt、client.key、ta.key

Introduction of the Configuration of OpenVPN Server

Copy the licenses and key files which needed by the server to the designated directory for unified management. We create the config folder under the OpenVPN Directory to store these files.

Create the Directory

Command：
cd /usr/local/openvpn-2.3.8/
mkdir config
cd config

Copy the License and Key Files

cp /usr/local/openvpn-2.3.8/easy-rsa/2.0/keys/ca.key .
cp /usr/local/openvpn-2.3.8/easy-rsa/2.0/keys/ca.crt .
cp /usr/local/openvpn-2.3.8/easy-rsa/2.0/keys/dh1024.pem .
cp /usr/local/openvpn-2.3.8/easy-rsa/2.0/keys/server.crt .
cp /usr/local/openvpn-2.3.8/easy-rsa/2.0/keys/server.key .
cp /usr/local/openvpn-2.3.8/easy-rsa/2.0/keys/ta.key .

Sample of Copy the Server Configuration Files

Command：cp /usr/local/openvpn-2.3.8/sample/sample-config-files/server.conf

Config the Server Configuration Files

Command：vi server.conf
Introduction of Common Configuration
local 192.168.120.42 #Specify the local IP Address to be listened (because some computers with several IP Addresses), this command is optional and all IP Addresses are being listened by default.
port 1194 #Specify the Local Port which to be listened
proto udp #Specify the adopted transmission protocol, TCP or UDP can be selected
dev tun #Specify the type of created communication channel, tun or tap can be selected
ca /usr/local/openvpn-2.3.8/config/ca.crt #Specify the file route of the CA License
cert /usr/local/openvpn-2.3.8/config/server.crt #Specify the license file route of the server
key /usr/local/openvpn-2.3.8/config/server.key #Specify the private key file route of the server
dh /usr/local/openvpn-2.3.8/config/dh1024.pem #Specify the file route of the Diffie-Hellman Parameter
server 10.8.0.0 255.255.255.0 #Specify the IP Address Segment and Subnet Mask which occupied by the Virtual LAN, and the server which configured here occupies

10.8.0.1.
ifconfig-pool-persist /usr/local/openvpn-2.3.8/config/ipp.txt #After the server allocated IP to the client automatically, the client will still use the last IP Address when connecting next time (the IP which allocated for the first time is saved in ipp.txt, and it will allocate the IP which saved in it next time).
tls-auth /usr/local/openvpn-2.3.8/config/ta.key 0 #Enable TLS-auth, use ta.key to defense the attack. The second parameter of the server is 0 and the parameter of the client is 1.
keepalive 10 120 # Ping every 10 seconds, and the connection timeout is set to 120 seconds.
comp-lzo #Enable the VPN compression, if the server is enabled, then the client also must be enabled
client-to-client #Allow the connection between the clients, and the clients only can connect with the server by default
push "route 192.168.20.0 255.255.255.0" #Push the route and inform client that it can connect to 192.168.20.0 by VPN
cipher AES-128-CBC # Enable AES Encryption
persist-key
persist-tun # The persistence option can avoid accessing some resources that cannot be accessed due to the decrease of user authority while restart
status openvpn-status.log #Specify the route of the log file which record the OpenVPN status
verb 3 #Specify the level of details of the log file, you can select Level 0~9, and if the level is higher, then the contents of the log file is more detailed.

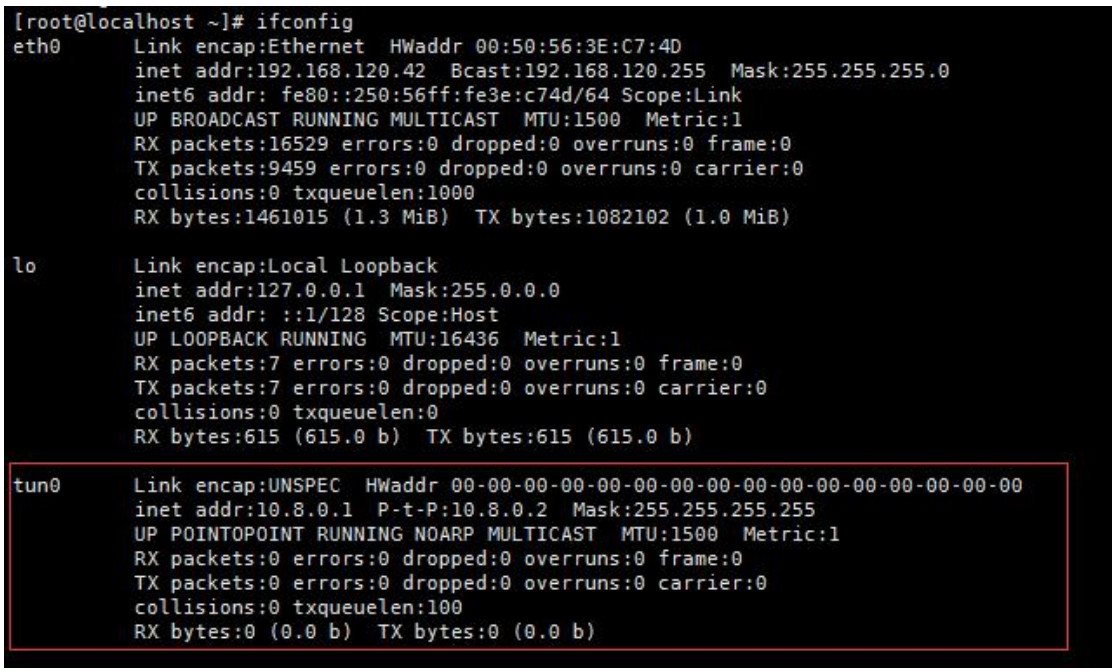
Enable the Service

Enable the OpenVPN Service

Command：/usr/local/sbin/openvpn --config /user/local/openvpn-2.3.8/config/server.conf &

Check the Status

Command：ifconfig
The configuration is successful while it shows the tun0 Virtual Network Card, as shown below:



Setup it as Power Boot

Command：echo "/usr/local/sbin/openvpn –config /user/local/openvpn-2.3.8/config/server.conf &" >>/etc/rc.local

Network Configuration for the Tun Mode

If you choose the Tun Mode while configuring the VPN Server, you will need to configure Linux and let your client to connect the network via the VPN Server.

Enable the IP Package Forwarding Function

Command：vi /etc/sysctl.conf

Change the Configuration：net.ipv4.ip_forward = 1

Use iptable Command to Config NAT Network Penetration

Command：

iptables -P FORWARD DROP

iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -j SNAT --to 192.168.120.42

iptables -A FORWARD -s 10.8.0.0/24 -j ACCEPT

Note：10.8.0.0 is the network segment which configured by the VPN，192.168.120.42 is the network segment of the VPN Server Network Card.

Reverse Routing

Command：iptables -A FORWARD -s 192.168.120.0/24 -j ACCEPT

Note：This rule means while the device of 20 Network Segment is configured with static routing 192.168.120.42, then it can access the address of VPN.

Produce the RGW4/RGW8 License of Redstone

Prepare the tool：We use the software “UltraEdit” as the sample to produce the Client Configuration File of the Redstone’s Gateway, according to the content of “The files which required by the client: ca.crt, client.crt, client.key, ta.key”, we transmit these 4 files to the Windows for backup by the transmission tools of FTP or SSH（Secure File Transfer Client）

Step 1 Create a new text file，and rename it as “client.vpn”，open and edit it by Notebook.

Step 2 Check or supplement the contents in the file.

The file contains the contents below, and they can be replaced according to the instruction by user.

```
client                          #Specify the current VPN as the Client
dev tun                         #It must be consistent with the Server
persist-tun
persist-key
cipher AES-128-CBC              #The type of encryption must be consistent with the Client
                                tls-client
tls-auth ta.key 1               #If the server setup the ta.key to defend against the Dos attack,
                                then it must be enabled by each client
remote 192.168.120.42 1194      #Specify the actual IP Address and Port No of the
                                connected Remote Server
proto tcp                       #Use TCP or UDP
comp-lzo                        #Keep consistent with the Server
passtos
ns-cert-type server             #Specify to use the Server Calibration Mode
<ca>
-----BEGIN CERTIFICATE-----
Note：Fill-in the secret key which copied from the ca.crt file here.
-----END CERTIFICATE-----
</ca>
<cert>
-----BEGIN CERTIFICATE-----
Note：Fill-in the secret key which copied from the client.crt file here.
-----END CERTIFICATE-----
</cert>
<key>
```

-----BEGIN PRIVATE KEY-----
Note：Fill-in the secret key which copied from the client.key file here. You must confirm the contents of the head & the end in accordance with the configuration which provided by the ATU-C（some of the configuration are ENCRYPTED PRIVATE KEY or others）
-----END PRIVATE KEY-----
</key>
<tls-auth>
-----BEGIN OpenVPN Static key V1-----
Note：Fill-in the secret key which copied from the ta.crt file here.
-----END OpenVPN Static key V1-----
</tls-auth>

Step 1 It must be converted to the UNIX format. For example, you can convert it from DOS format to UNIX format.

Step 2 Save the file after finished the checking and supplementation. You must save the .txt file as the client.ovpn file.

Upload this configuration file to the RGW4/RGW8 by WEB and enable the OpenVPN Function. When you open the Status Page after rebooting the gateway, you should see the content, which indicates that it connected successfully.

Fix IP Address for Every Client

Step 1 Create a new folder “client” under the “config” directory

Command：

```
cd /user/local/openvpn-2.3.8/config/
mkdir client
```

Step 2 Edit the server.conf file and change the configuration

Command：vi server.conf

Edit the below contents:

client-config-dir /usr/local/openvpn-2.3.8/config/client

Step 3 Create file under the client directory and its file name is the common name of the terminal (according to the client license which I created before; the common name is client).

Command：

```
cd /user/local/openvpn-2.3.8/config/client
vi client
```

Increase the below field after enter in

ifconfig-push 10.8.0.118 10.8.0.117

While this client is connected, then its IP Address is 10.8.0.118

Notice

1. client.ovpn integrates the client's configuration with the license and the secret key together. Therefore, the content copied by the secret key must be accurate. It is particularly important to note whether or not wording like "----BEGIN PRIVATE KEY -----" is consistent.
2. Check whether the gateway's time is correct, if the time is not synchronized, the connection will fail.
3. The OpenVPN Server may in the remote LAN, so the router shall equip with port mapping, the connection address（remote 192.168.120.42 1194 udp）of the client shall be changed to its exit IP.

List of Corresponding Software

OS：CentOS 6.5
Linux Software：openvpn2.3.8、easy-rsa2.0（Download：http://pan.baidu.com/s/1eQfPlZg）
Windows Software：UltraEdit、SSH Secure Shell