OpenVPN 基本安装 Server
sudo apt update && sudo apt install openvpn easy-rsa -y
make-cadir ~/openvpn-c
cd ~/openvpn-ca
./easyrsa init-pki
./easyrsa build-ca
./easyrsa build-server-full server nopass
./easyrsa gen-dh
openvpn --genkey secret /etc/openvpn/ta.key

生成用户 certificate key: crt key files
./easyrsa gen-req Username nopass && ./easyrsa sign-req client Username
sudo cp /usr/share/doc/openvpn/examples/sample-config-files/server.conf
/etc/openvpn/
++++++++++++++++++++++++++++++++++
修改 server.conf
Change the ca, cert, key, and dh file paths to match your generated keys. &
ta.key
ciphers----cipher AES-256-GCM
port
proto UDP #似乎比 tcp 好些
push "redirect-gateway def1 " #推送 route all client traffic through the VPN.
dev tun   #定义通道种类
topology subnet   #
server 10.8.0.0 255.255.255.0 #定义 VPN Server
 push "route 0.0.0.0 0.0.0.0"   #route Client to Server
 push "route 222.222.220.0 255.255.255.0" #Maybe not necessary
push "dhcp-option DNS 8.8.8.8"   #强制推送 DNS
push "dhcp-option DNS 222.222.220.1"   #Maybe not
duplicate-cn   #允许同一用户多链接
tls-auth /etc/openvpn/ta.key 0   #“0” 表征是 server 端
data-ciphers AES-256-GCM:AES-128-GCM   #在 ubuntu LTS 中必须 用
cipher AES-256-GCM   #在 Lite 6.0 中使用
topology---topology subnet
允许 log，压缩....   #也许有数据加密安全风险
user nobody
group nobody   必须 match ta.key
systemctl enable openvpn@server
如果修改了，在 systemctl restart openvpn@server 前， systemctl daemon-reload 一下

Maybe:
sudo chmod 600 /home/jiang/openvpn-ca/ta.key
sudo chown root:root /home/jiang/openvpn-ca/ta.key
ie: rw only to root:root
ta.key
ca.crt
server.crt
server.key
dh.pem
ALL Should be in /etc/openvpn !!!!!!!!!
If OpenVPN is running in a restricted environment, it might not be allowed to
access files in /home/.....

Use 443 TCP :
port 443
proto tcp
Enable SSL/TLS:
tls-server

tls-auth ta.key 0
Disable explicit-exit-notify 1
++++++++++++++++++++++++++++++++
Client Software:
Widows: openvpn/community-download
/home/jiang/openvpn-ca
以上两个文件+ca.crt+ta.key copy to /etc/openvpn/client
scp username@your-server-ip:/etc/openvpn/client-files/* C:\Users\
YourWindowsUser\OpenVPN\config\

++++++++++++++++++++++++++++++++++++
sudo sysctl -w net.ipv4.ip_forward=1
This maybe necessary
tun-ipv6
这才是最重要的一行，保证了 ipv6 ipv4 for VPN 优先
++++++++++++++++++++++++++++++++++
文件用途
dh.pem   Diffie-Hellman parameters for secure key exchange
server.crt Server certificate (verifies server identity)
server.key Server private key (kept secret)
ca.crt   Certificate Authority (verifies server & clients)
user1.crt   Client certificate (verifies client identity)
user1.key   Client private key (kept secret)
ta.key   TLS authentication key (prevents unauthorized access)
++++++++++++++++++++++++++++++++=
when use a mobile as a client, the ovpn file:

1
delete all 4 lines
ca
cert
key
tls-auth
2 add one line
key-direction 1
3.
merge 4 file to ovpn file
<ca>
.....
</ca>
<cert>
....
</cert>
<key>
.....
</key>
<tls-auth>
....
</tls-auth>

++
客户端模板   .ovpn file
client
dev tun
proto udp
remote blueland.com.au 997
resolv-retry infinite
nobind
persist-key
persist-tun
remote-cert-tls server
cipher AES-256-GCM

```
#tls-auth ta.key 1
key-direction 1
#ca ca.crt
#cert user1.crt
#key user1.key
#direction-gateway def1
compress lz4-v2
verb 4

++++++++++++++++++++++++++++++++++++++=
```

疑难问题

```
*****OpenVPN all data go to chain FORWARD********
so setting iptables -L FORWARD some rules is the best way to control the data
flow
```

显示 iptables List Delete

```
CHAIN as FORWARD
sudo iptables -L <CHAIN> --line-numbers -n -v
sudo iptables -D <CHAIN> <LINE_NUMBER>
```

所有 iptables 验证后永久驻留

```
Persistent the rules
sudo iptables-save > /etc/iptables/rules.v4
or
sudo netfilter-persistent save
****************************************
```

vpn 通道工作正常，可以 ping 到 10.8.0.1, 222.222.220.1,google.com

但打不开网页， 数据流显示 有 10.8.0.2 到外网的包，但没有外网到 10.8.0.2 的包

原因是 VPN 网 10.8.0.0/24 和本地网络 222.222.220.0/24 之间有防火墙

```
sudo ufw default allow FORWARD
But for safty reason
sudo ufw route allow in on AAAA out on BBBB     #避免其他应用乘机越过防火墙进入路由
ie:  sudo ufw route allow in on tun0 out on wlp1s0


Server NAT should be enabled
sudo sysctl -w net.ipv4.ip_forward=1
sysctl -p
NAT all 10.8.0.0/24 to server network interface, so that VPN data go to local
network
maybe:    iptable -A POSTROUTING -s 10.8.0.0/24 -o wlp1s0 -j MASQUERADE
display  iptable -t nat -L -v -n
****************************************
```

限制客户端访问 VPN 其他本地资源:

```
iptables -I FORWARD -s 10.8.0.0/24 -d 222.222.220.0/24 -j DROP
      (-A or -I append or insert)
display  iptable --L -v -n
************************************
```

限制客户端之间互访

```
sudo iptables -I FORWARD -i tun0 -s 10.8.0.0/24  ! -d 10.8.0.1 -j DROP


最后
rules.v4
A FORWARD -s 10.8.0.0/24 -d 10.8.0.1/32 -j ACCEPT
-A FORWARD -s 10.8.0.0/24 -d 10.8.0.0/24 -j DROP
-A FORWARD -s 10.8.0.0/24 -d 222.222.220.0/24 -j DROP

-A POSTROUTING -s 10.8.0.0/24 -o wlp1s0 -j MASQUERADE
```