安装

关闭防护墙

同步时间

线上

```
# 上传文件到服务器上
mv openvpn-install-20210524-server.sh openvpn-install.sh
chmod +x openvpn-install.sh

# 先下载好包
wget -O ~/easy-rsa.tgz https://github.com/OpenVPN/easy-
rsa/releases/download/v3.0.7/EasyRSA-3.0.7.tgz

./openvpn-install.sh
```

线下

```
# 上传文件到服务器上
mv openvpn-install-20210524-local.sh openvpn-install.sh
mv EasyRSA-3.0.7.tgz easy-rsa.tgz

chmod 777 openvpn-install.sh easy-rsa.tgz

./openvpn-install.sh
```

实际上基本上一路回车即可, 注意在dns选择和端口选择的地方需要改动

确定本机ip

```
[root@openvpn openvpn]# ./openvpn-install.sh
Welcome to the OpenVPN installer!
The git repository is available at: https://github.com/angristan/openvpn-install

I need to ask you a few questions before starting the setup.
You can leave the default options and just press enter if you are ok with them.

I need to know the IPv4 address of the network interface you want OpenVPN listening to.
Unless your server is behind NAT, it should be your public IPv4 address.
IP address: 192.168.5.66
```

确定公网ip

```
It seems this server is behind NAT. What is its public IPv4 address or hostname?
We need it for the clients to connect to the server.
Public IPv4 address or hostname: 120.78.169.170
```

是否需要使用ipv6

```
Checking for IPv6 connectivity...

Your host does not appear to have IPv6 connectivity.

Do you want to enable IPv6 support (NAT)? [y/n]: n
```

确定端口, 注意选择随机高位端口

```
What port do you want OpenVPN to listen to?
   1) Default: 1194
   2) Custom
   3) Random [49152-65535]
Port choice [1-3]: 3
Random Port:
```

确定协议: 使用udp更加稳定

```
What protocol do you want OpenVPN to use?
UDP is faster. Unless it is not available, you shouldn't use TCP.
   1) UDP
   2) TCP
Protocol [1-2]: 1
```

确定dns

使用用户自己本身的dns

```
   3) Cloudflare (Anycast: worldwide)
   4) Quad9 (Anycast: worldwide)
   5) Quad9 uncensored (Anycast: worldwide)
   6) FDN (France)
   7) DNS.WATCH (Germany)
   8) OpenDNS (Anycast: worldwide)
   9) Google (Anycast: worldwide)
   10) Yandex Basic (Russia)
   11) AdGuard DNS (Anycast: worldwide)
   12) NextDNS (Anycast: worldwide)
   13) Custom
DNS [1-12]: 2
```

确定压缩

```
Do you want to use compression? It is not recommended since the VORACLE attack make use of it.
Enable compression? [y/n]: n
```

确定自定义加密

```
Do you want to customize encryption settings?
Unless you know what you're doing, you should stick with the default parameters provided by the script.
Note that whatever you choose, all the choices presented in the script are safe. (Unlike OpenVPN's defaults)
See https://github.com/angristan/openvpn-install#security-and-encryption to learn more.

Customize encryption settings? [y/n]: n
```

回车确定安装

```
Okay, that was all I needed. We are ready to setup your OpenVPN server now.
You will be able to generate a client at the end of the installation.
Press any key to continue...
```

配置网络

我们先看到服务端配置如下:

```
port 1234
proto udp
dev tun
user nobody
group nobody
persist-key
persist-tun
keepalive 10 120
topology subnet
```

```
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt
push "dhcp-option DNS 10.8.0.1"
push "redirect-gateway def1 bypass-dhcp"
dh none
ecdh-curve prime256v1
tls-crypt tls-crypt.key
crl-verify crl.pem
ca ca.crt
cert server_zir1mGwJskPHmrcw.crt
key server_zir1mGwJskPHmrcw.key
auth SHA256
cipher AES-128-GCM
ncp-ciphers AES-128-GCM
tls-server
tls-version-min 1.2
tls-cipher TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256
client-config-dir /etc/openvpn/ccd
status /var/log/openvpn/status.log
verb 3
```

`vi /etc/openvpn/server.conf`

加上服务端ip, 去掉全部流量代理

```
#push "redirect-gateway def1 bypass-dhcp"

explicit-exit-notify 1
push "route 192.168.2.0 255.255.255.0"
push "route 192.168.3.0 255.255.255.0"
push "route 192.168.4.0 255.255.255.0"
push "route 192.168.5.0 255.255.255.0"
```

线下

```
#push "redirect-gateway def1 bypass-dhcp"

explicit-exit-notify 1
push "route 192.168.1.0 255.255.255.0"
push "route 192.168.90.0 255.255.255.0"
push "route 172.30.1.0 255.255.255.0"
```

`systemctl restart openvpn-server@server`

`systemctl status openvpn-server@server`

用户管理

添加用户

```
/data/tristan/openvpn/openvpn-install.sh
```

```
[root@openvpn openvpn]# /data/tristan/openvpn/openvpn-install.sh
Welcome to OpenVPN-install!
The git repository is available at: https://github.com/angristan/openvpn-install

It looks like OpenVPN is already installed.

What do you want to do?
   1) Add a new user
   2) Revoke existing user
   3) Remove OpenVPN
   4) Exit
Select an option [1-4]: 1
```

输入名字

```
Tell me a name for the client.
The name must consist of alphanumeric character. It may also include an underscore or a dash.
Client name:
```

```
Do you want to protect the configuration file with a password?
(e.g. encrypt the private key with a password)
   1) Add a passwordless client
   2) Use a password for the client
Select an option [1-2]: 1
```

管理

查看状态

```
systemctl status openvpn-server@server
```

重启

```
systemctl restart openvpn-server@server
```

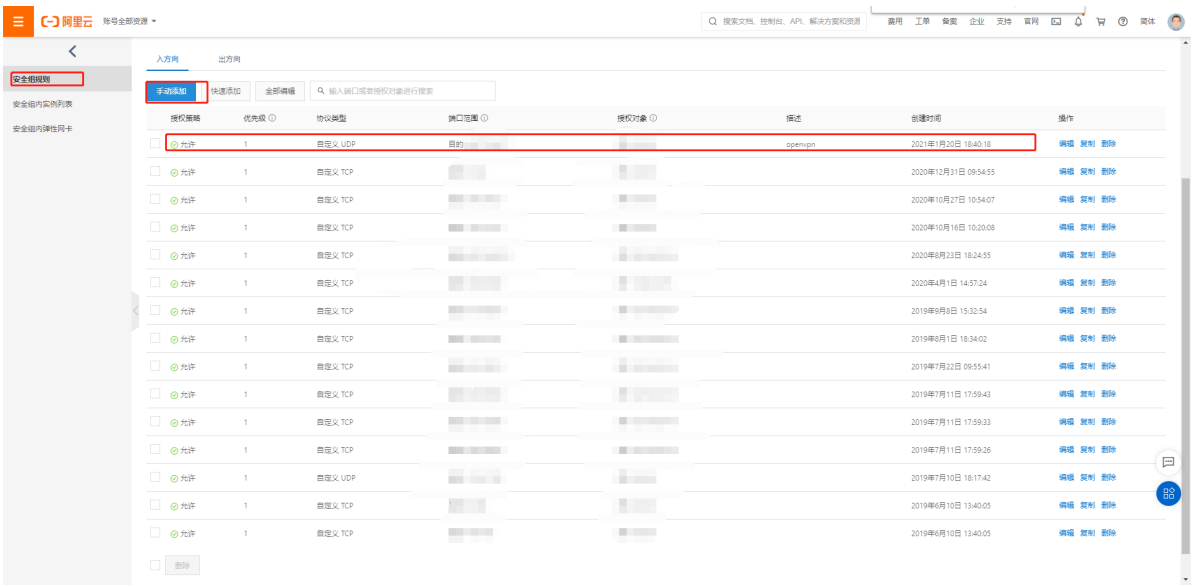
其他的按照systemctl指令即可

配置网络

协议: udp

端口范围: openvpn端口/openvpn端口

授权对象: 0.0.0.0/0



参考文档

https://github.com/angristan/openvpn-install