OpenVPN实验手册

安装OpenVPN

用这个脚本：https://github.com/angristan/openvpn-install

这个脚本可以安装OpenVPN，这个脚本是交互式的，根据提示选择VPN的端口和创建的用户名字，就能部署好。脚本会下载OpenVPN需要的文件，如果服务器只有IPv6网络会无法下载~~（我试过）~~

如果脚本当检测到已经安装，再次运行脚本，可以添加删除用户

脚本应该是会自动执行

```
systemctl enable --now openvpn-server@server.service
```

不过建议手动再执行一遍确保OpenVPN启动

之后**注意配置防火墙**，除了开放端口后还需要**开启转发**

```
# 开放端口我就不写了
# 开启地址转发
firewall-cmd --permanent --add-masquerade
firewall-cmd --reload
```

客户端连接

客户端的配置文件会被保存在服务器的`~/<用户名>.ovpn`（你需要把它下载）

Linux

Linux用户需要安装openvpn，之后运行

```
sudo openvpn <用户名>.ovpn
```

来测试连接，但是这个方法不会更新系统的DNS，会更新系统路由，正儿八经地用需要用`NetworkManager`来导入这个配置，需要安装`networkmanager-openvpn`插件

```
sudo pacman -S networkmanager-openvpn
```

之后运行

```
nmcli connection import type openvpn file <用户名>.ovpn
```

将配置导入，如果有KDE或者GNOME的话，VPN应该已经出现在连接列表了，直接用图形化像连WiFi那样连接，或者用命令行

```
nmcli connection up <用户名>
```

注意nmcli命令不需要sudo

Windows和Android

下载OpenVPN客户端，直接导入ovpn配置然后用

Windows在这里下载就行

https://openvpn.net/client-connect-vpn-for-windows/

Android去Google Play就行，需要注意，运行客户端**需要安装谷歌服务框架。**

安装后的配置

端口和DNS应该在安装脚本第一次安装的时候都配置好了，但是额外的特色配置需要改配置文件

配置文件

服务器配置文件在`/etc/openvpn/server/server.conf`，如果你用的其他的脚本，可能在`/etc/openvpn/server.conf`，客户端的配置文件会被保存在服务器的`~/<用户名>.ovpn`（你需要把它下载到OpenVPN客户端使用，导入配置）。服务器和客户端配置文件的格式都是

```
key0 value0
key1 value1
```

其中`key0`和`key1`是openvpn启动命令行传入的参数，查看man帮助

```
man openvpn
```

可以看到每一个参数都是干什么的，例如man帮助里面有这样一条

```
--keepalive interval timeout
              A helper directive designed to simplify the expression of --ping
and --ping-restart.

              This  option  can  be  used  on  both client and server side, but
it is enough to add this on the
              server side as it will push appropriate --ping and --ping-restart
options to the client.  If used
              on both server and client, the values pushed from server will
override the client local values.

              The  timeout  argument  will be twice as long on the server side.
This ensures that a timeout is
              detected on client side before the server side drops the connection
```

你往客户端配置里面写

```
keepalive 5 15
```

就可以让客户端每隔5秒ping下服务器，如果15秒（即ping了三次）没有回复，那就判定为已经掉线，开始断线重连。

几个重要的配置

服务器配置（改完记得重启服务）

显示日志（默认不存放日志，出错了调试连日志都没有，很坑）

```
log-append /var/log/openvpn.log
```

一定要注意文件`/var/log/openvpn.log`的权限，**用户nobody必须具有写权限。**

监听IPv6

```
proto udp6
```

注意，这个是监听IPv4和IPv6，写了这行之后不要在后面写`proto udp4`，如果写了，下面对于`proto`的设置会覆盖上面的，就变成只监听IPv4了。

具体proto可以选择的范围直接看man帮助，`man openvpn`，然后按`/`搜索`proto`，可以选择tcp。

给客户端设置DNS服务器

如果设置DNS为10.8.0.1

```
push "dhcp-option DNS 10.8.0.1"
```

push的意思是把后面带引号的vpn配置放在客户端执行，因此你在客户端的以ovpn为后缀的配置里面直接写上`dhcp-option DNS 10.8.0.1`的作用和你在服务器配置上写`push "dhcp-option DNS 10.8.0.1"`是一样的。

更改端口

```
port 1194
```

改完了记得把客户端的ovpn后缀的配置文件的这一行也改下。

设置keepalive

设置每3秒ping一次，9秒无响应就认定为断线

```
keepalive 3 9
```

同样，客户端配置也有这一行，如果改了服务器，客户端要一起改。

为客户端配置静态内网IP

服务器配置里面应该有这一行

```
ifconfig-pool-persist ipp.txt
```

然后你需要保证客户端至少连接过服务器一次，之后重启服务端

```
systemctl restart openvpn-server@server.service
```

（必须重启否则ipp.txt没东西）之后`/etc/openvpn/server/ipp.txt`这个文件里面写了为用户分配的内网IP，应该长这样

```
hxp,10.8.0.2
```

hxp是用户名，后面是IP，直接改后面的IP就行。**改完还需要再重启一次。**

客户端配置

断线重连

```
connect-retry 3 3
```

设置断线后每3秒重新连接一次，不要随着重连次数的增加而增加重连等待时间。

同时还建议注释掉这一行

```
;persist-tun
```

否则可能会出现重连怎么也连不上的情况（我遇到过）

使用IPv6

客户端ovpn后缀的配置应该有这一行

```
remote xxx.xxx.xxx.xxx 1194
```

xxx.xxx.xxx.xxx是服务器的IPv4地址，1194是端口（如果你用的默认端口），直接把服务器的IPv6地址复制过来，替换掉这个IPv4地址，就行。前提是服务器监听了IPv6（前面写了）。