OpenVPN 配置文件中文版

很多情况下我们不得不选择使用 openvpn 来突破一些封锁，实现自由上网，像 GFW、CMWAP 这些具有中国特色的网络文明，我们必须突破。openvpn 是最好的选择。面对 openvpn 全英文配置文件，很多朋友肯定很茫然，下面是配置文件的中文翻译版。

哪个本地 ip 地址将被 Openvpn 监听?

也可以不注明

;local a.b.c.d

哪一个 tcp/udp 端口将被监听?

如果你要在一台机器上启动多个 OpenVPN,你需要监听不同的端口

记着在防火墙那里打开这些端口

port 1194

TCP 还是 UDP 协议?

如果采用 HTTP proxy，必须使用 TCP 协议

proto udp

“dev tun” 将创建1个路由隧道

“dev tap” 将创建1个以太网隧道

如果你选择桥模式,使用 “dev tap”

如果你需要控制每个客户端的访问控制策略

你必须创建防火墙规则到 TUN/TAP 接口

在非 Windows 系统上,你可以明确该接口,如:tun0

在 Windows 上,使用”dev-node”

在大多数系统上,如果你的防火墙部分或全部禁止 TUN/TAP 接口的话,Openvpn 将可能不起作用

;dev tap

dev tun

在 Windows 上如果你更多的网络接口，你需要在网络连接控制面板上增加

TAP-Win32适配器接口名

在 XP SP2或更高系统上，你需要使 windows 防火墙对该接口不执行过滤规则

非 Windows 系统通常不需要设置这个

;dev-node MyTap

证书/key 文件指向

ca ca.crt #OpenVPN 使用的 ROOT CA，使用 build-ca 生成的，用于验证客户是证书是否合法

cert server.crt #Server 使用的证书文件

key server.key #Server 使用的证书对应的 key,该文件必须严格控制其安全性

#CRL 文件的申明，被吊销的证书链，这些证书将无法登录

;crl-verify vpncrl.pem

Diffie hellman 文件指向

如果你在建立证书时使用2048的话这里是2048

否则默认

dh dh1024.pem

给接入的 client 分配的地址段

server 192.168.80.0 255.255.255.0

维护客户端和虚拟 ip 地址联系

在 openvpn 重启时,再次连接的客户端将依然被分配和以前一样的

ip 地址

ifconfig-pool-persist ipp.txt

openvpn 桥模式用的[我不用桥模式]

配置服务器桥接模式的前提是必须将俩网卡在操作系统下先建立桥接，之后手动设置 ip 地址和子网掩码。

;server-bridge 10.8.0.4 255.255.255.0 10.8.0.50 10.8.0.100

下面这句使客户端能访问服务器后面的子网机器

比如:服务器子网网段是192.168.10.0和192.168.10.2

你需要在 openVPN 服务器端配置文件中添加下面这两句

push “route 192.168.10.0 255.255.255.0″

push “route 192.168.20.0 255.255.255.0″

使服务器子网内机器可以访问客户端子网内机器

仅用于路由模式

假设:客户端子网网段192.168.40.0

首先,在服务器配置文件中添加下面这两行

client-config-dir ccd

和 route 192.168.40.0 255.255.255.0

然后在服务器端 ccd 目录下创建一个文件,文件名是客户端的公共名

文件内容是:

iroute 192.168.40.0 255.255.255.0

;client-config-dir ccd

;route 192.168.40.0 255.255.255.0

EXAMPLE: Suppose you want to give

Thelonious a fixed VPN IP address of 10.9.0.1.

First uncomment out these lines:

;client-config-dir ccd

;route 10.9.0.0 255.255.255.252

Then add this line to ccd/Thelonious:

ifconfig-push 10.9.0.1 10.9.0.2

支持对不同客户端组执行不同的防火墙策略

这里有两种方法

(1) 运行多个 OpenVPN 守护进程, 每个对应不同的组

并且防火墙对不同的组和进程执行不同的策略

(2) (高级)创建1个动态脚本使防火墙对接入的不同客户端执行不同的策略

;learn-address ./script

下面这句使客户端所有网络通信通过 vpn

If enabled, this directive will configure

all clients to redirect their default

network gateway through the VPN, causing

all IP traffic such as web browsing and

and DNS lookups to go through the VPN

(The OpenVPN server machine may need to NAT

the TUN/TAP interface to the internet in

order for this to work properly).

CAVEAT: May break client’s network config if

client’s local DHCP server packets get routed

through the tunnel. Solution: make sure

client’s local DHCP server is reachable via

a more specific route than the default route

of 0.0.0.0/0.0.0.0.

;push “redirect-gateway”

客户端 DHCP 设置

Certain Windows-specific network settings

can be pushed to clients, such as DNS

or WINS server addresses. CAVEAT:

http://openvpn.net/faq.html#dhcpcaveats

;push “dhcp-option DNS 10.8.0.1″

;push “dhcp-option WINS 10.8.0.1″

下面这句使客户端能相互访问

否则，默认设置下客户端间不能相互访问

client-to-client

这段常用于测试用途，注释该条可实现限制一个证书在同一时刻只能有一个客户端接入

Uncomment this directive if multiple clients

might connect with the same certificate/key

files or common names. This is recommended

only for testing purposes. For production use,

each client should have its own certificate/key

pair.

IF YOU HAVE NOT GENERATED INDIVIDUAL

CERTIFICATE/KEY PAIRS FOR EACH CLIENT,

EACH HAVING ITS OWN UNIQUE “COMMON NAME”,

UNCOMMENT THIS LINE OUT.

;duplicate-cn

活动连接保时期限

The keepalive directive causes ping-like

messages to be sent back and forth over

the link so that each side knows when

the other side has gone down.

Ping every 10 seconds, assume that remote

peer is down if no ping received during

a 120 second time period.

keepalive 10 120

为防止遭到 DDoS 攻击

生成 ta.key 文件，并 cp 到服务器端和每个客户端

该文件用以下命令生成

openvpn –genkey –secret ta.key

服务器端0,客户端1

该文件要严格保护

tls-auth ta.key 0 # 服务器端是0

选择一种加密算法,Server 端和 client 端必须一样

Select a cryptographic cipher.

This config item must be copied to

the client config file as well.

;cipher BF-CBC # Blowfish (default)

;cipher AES-128-CBC # AES

;cipher DES-EDE3-CBC # Triple-DES

允许数据压缩

客户端配置文件也需要有这项

comp-lzo

最大客户端并发连接数量

;max-clients 100

#定义运行 openvpn 的用户

;user nobody

;group nobody

#通过 keepalive 检测超时后，重新启动 VPN，不重新读取 keys，保留第一次使用的 keys

persist-key

#通过 keepalive 检测超时后，重新启动 VPN，一直保持 tun 或者 tap 设备是 linkup 的，

#否则网络连接会先 linkdown 然后 linkup

persist-tun

#定期把 openvpn 的一些状态信息写到文件中，以便自己写程序计费或者进行其他操作

status openvpn-status.log

#记录日志，每次重新启动 openvpn 后删除原有的 log 信息

;log openvpn.log

#或者

#记录日志，每次重新启动 openvpn 后追加原有的 log 信息

log-append openvpn.log #[为便于管理 log 可将该项改为 /var/log/openvpn.log]

设置日志记录冗长级别

0 is silent, except for fatal errors

4 is reasonable for general usage

5 and 6 can help to debug connection problems

9 is extremely verbose

verb 3

重复日志记录限额

Silence repeating messages. At most 20

sequential messages of the same message

category will be output to the log.

mute 20