Ubuntu Server 从入门到精通

第22章：代理/VPN

代理&VPN

你看见的不是你真的看见的

- 时间、带宽、管控 都影响网络使用体验
- 作为改善技术，VPN / 代理 可以突破限制改善体验
- 代理主要提高访问速度；VPN更注重安全性
- 在某些应用场景中，作用非常相似
- 作为中间层，双向模拟（翻墙）

Proxy

你看见的不是你真的看见的

- 出国代理公司
  - 了解国外情况，讲中文，离你近
  - 代表你办理出国手续，加快你出国的进程
- 网络代理服务
  - 客户端将访问请求发给 Proxy，而非直连目标
  - 代理转发请求给目标，并将结果返回给客户端
- 正向代理
  - 提高速度、内容控制、安全
- 反向代理
  - 速度、安全、分发

Proxy

你看见的不是你真的看见的

- 安装squid
  - sudo apt install squid
- 配置
  - vi /etc/squid/squid.conf
  - acl 访问控制列表
  - acl menhu dstdomain .sina.com .163.com　　# 小心页面元素CSS、图片
  - acl xiaban time MTWHFAS 18:00-23:59
  - Mon, Tues, Wednes, tHurs, Fri, sAtur, Sun, D：工作日
  - 访问规则顺序匹配
  - http_access allow localhost
  - http_access deny all
  - http_access allow menhu xiaban

Proxy

你看见的不是你真的看见的

- 指定源地址
  - acl localnet src 10.0.0.0/24 10.0.3.0/24 10.0.5.0/24 192.168.0.1
- URL过滤
  - acl noexes url_regex -i exe$ # URL 以 exe 结尾（-i 大小写不敏感）
  - acl httpsurls url_regex -i ^https # ^ URL 起始
  - acl noporn url_regex -i sex
  - acl zipfiles url_regex -i \.zip$
- 重新加载配置文件
  - sudo kill -SIGHUP `cat /var/run/squid.pid`
- 最后一条访问规则
  - http_access deny all

Proxy

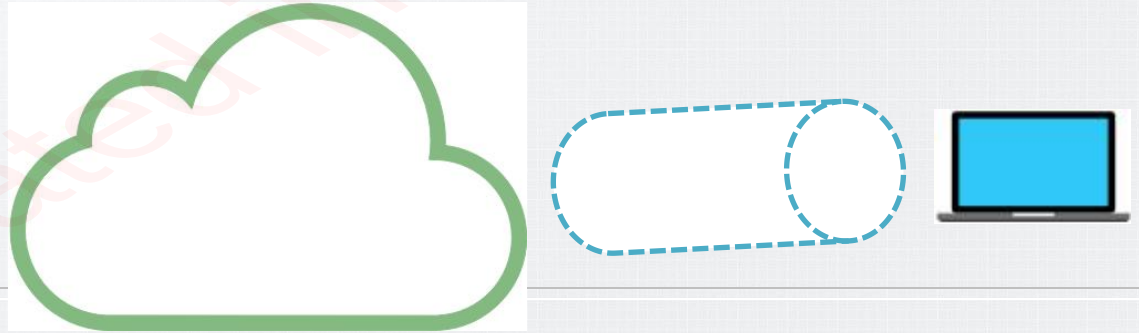
你看见的不是你真的看见的

- 代理端口
  - http_port 192.168.1.1:3128
- 不要对公网开放代理
  - 默认在所有IP上侦听代理端口
- 访问日志
  - /var/log/squid/access.log
- 缓存
  - cache_dir ufs /var/spool/squid3 100 16 256
  - refresh_pattern -i \.(gif|png|jpg|jpeg|ico)$ 3600 90% 86400 # 缓存图片

VPN

你看见的不是你真的看见的

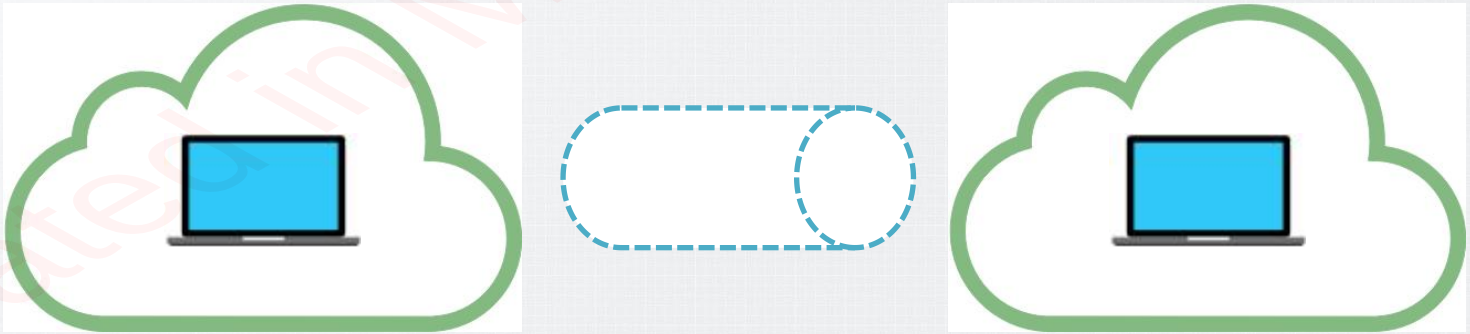
- 企业内部系统不应对外开放
  - 出差在外的企业员工需要访问公司内部系统
  - 分公司、合作商需要安全的访问指定企业内部系统
  - 专线网络费用高昂且不灵活
  - 远程访问安全性欠缺
- 虚拟专用网（VPN — Virtual Private Network）
  - 基于并不安全的网络线路，通过加密技术构建安全的信息通道（tunnel）
  - VPN 用户获得如同在内网一样的访问使用体验



VPN

你看见的不是你真的看见的

- 与Proxy相比
  - VPN 更加安全、成本高、部署难度大
  - VPN 一旦部署完成后使用简单
  - Proxy 属于一种中间层，VPN 更接近路由（对应用透明，无需设置代理）
  - VPN 更完善的认证、加密、授权控制



VPN

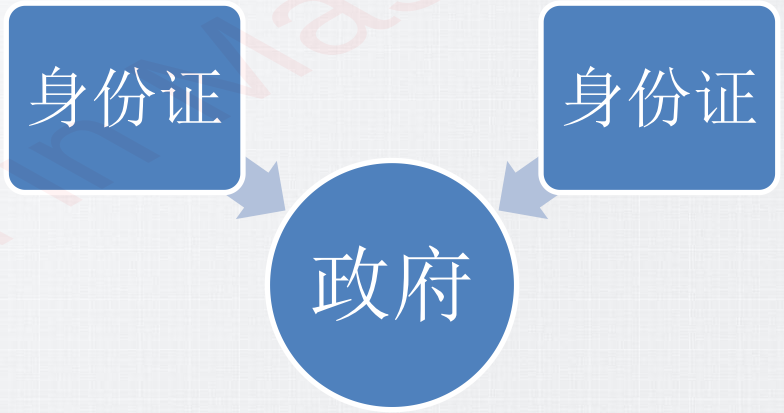
你看见的不是你真的看见的

- VPN 类型
  - PPTP
  - L2TP
  - IPSec
  - SSL
- OpenVPN
  - 全特性的开源SSL VPN
  - 跨平台 windows、linux、macox、ios、android

OpenVPN

你看见的不是你真的看见的

- OpenVPN
  - 通过非受信网络连接上网时保证安全
  - 出差员工访问企业内部系统
  - 伪装为国外地址，规避地理限制和审核（翻墙）
  - 需要（独立的）证书颁发机构CA，完成PKI架构



OpenVPN

你看见的不是你真的看见的

- 安装OpenVPN（VPN Sever）
  - sudo apt install openvpn
- 安装EasyRSA（VPN+CA Server）
  - wget https://github.com/OpenVPN/easy-rsa/releases/download/v3.0.6/EasyRSA-unix-v3.0.6.tgz
  - tar xvf EasyRSA-unix-v3.0.6.tgz
- 配置（CA）
  - cd ~/EasyRSA-v3.0.6/
  - cp vars.example vars
  - vi vars

OpenVPN

你看见的不是你真的看见的

- vi vars
  - set_var EASYRSA_REQ_COUNTRY "CN"
  - set_var EASYRSA_REQ_PROVINCE "Beijing"
  - set_var EASYRSA_REQ_CITY "BJ"
  - set_var EASYRSA_REQ_ORG "LAB"
  - set_var EASYRSA_REQ_EMAIL "admin@lab.com"
  - set_var EASYRSA_REQ_OU "IT"
- 初始化PKI架构
  - ./easyrsa init-pki

OpenVPN

你看见的不是你真的看见的

- 创建证书颁发机构，生成CA公私钥
  - ./easyrsa build-ca nopass
  - ca.crt：公钥证书，用于验证CA签名的其他证书（C/S都需要）
  - ca.key：CA的私钥，用于签名所有C/S证书（应私密保存）
  - 证书服务器在不使用时，建议关机
- 生成VPN服务器私钥和证书申请文件（VPN Server）
  - cd EasyRSA-v3.0.6/
  - ./easyrsa init-pki
  - ./easyrsa gen-req vpnserver nopass
  - pki/reqs/vpnserver.req
  - pki/private/vpnserver.key
  - sudo cp pki/private/vpnserver.key /etc/openvpn/ # 私钥

OpenVPN

你看见的不是你真的看见的

- 将证书请求文件传输至CA签发
  - scp pki/reqs/vpnserver.req yuanfh@CA_IP:/tmp
- 导入并签发VPN服务器证书（CA Server）
  - ./easyrsa import-req /tmp/vpnserver.req vpnserver
  - ./easyrsa sign-req server vpnserver # pki/issued/vpnserver.crt
  - 证书类型 server / client
- 将证书回传至vpnserver
  - scp pki/issued/vpnserver.crt yuanfh@vpnserver_ip:/tmp/ # vpnserver证书
  - scp pki/ca.crt yuanfh@vpnserver_ip:/tmp/ # CA公钥证书

OpenVPN

你看见的不是你真的看见的

- 拷贝证书文件（vpnserver）
  - sudo cp /tmp/{vpnserver.crt,ca.crt} /etc/openvpn/
- 生成Diffie-Hellman密钥（密钥交换）
  - ./easyrsa gen-dh # 生成HMAC签名（TLS完整性校验）
  - openvpn --genkey --secret ta.key
  - sudo cp ta.key /etc/openvpn/
  - sudo cp pki/dh.pem /etc/openvpn/
- 服务端证书设置全部完成

OpenVPN客户端

你看见的不是你真的看见的

- 在VPN服务器上生成客户端证书
- 使用脚本批量自动生成客户端配置文件
- 生成客户端证书密钥 / 请求文件
  - mkdir -p ~/client-configs/keys　　# 证书文件目录
  - chmod -R 700 ~/client-configs　　# 配置文件目录
  - cd ~/EasyRSA-v3.0.6/
  - ./easyrsa gen-req client1 nopass　　# client1
  - cp pki/private/client1.key ~/client-configs/keys/
  - scp pki/reqs/client1.req yuanfh@CA_ip:/tmp

OpenVPN客户端

你看见的不是你真的看见的

- 导入并签发证书（CA Server）
  - ./easyrsa import-req /tmp/client1.req client1
  - ./easyrsa sign-req client client1
  - scp pki/issued/client1.crt yuanfh@vpnserver_ip:/tmp
- 复制证书文件（VPN Server）
  - cp /tmp/client1.crt ~/client-configs/keys/
  - cp ~/EasyRSA-v3.0.6/ta.key ~/client-configs/keys/
  - sudo cp /etc/openvpn/ca.crt ~/client-configs/keys/
- 客户端证书文件准备完毕

配置OpenVPN服务

你看见的不是你真的看见的

- 服务器配置文件
  - sudo cp /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz /etc/openvpn/
  - sudo gzip -d /etc/openvpn/server.conf.gz
  - sudo vi /etc/openvpn/server.conf

```
tls-auth ta.key 0
key-direction 0
cipher AES-256-CBC
auth SHA256
dh dh2048.pem
user nobody
group nogroup
```

配置OpenVPN服务

你看见的不是你真的看见的

- 强制客户端所有流量路由至 tun0

  push "redirect-gateway def1 bypass-dhcp"
  push "dhcp-option DNS 202.106.8.20"
  push "dhcp-option DNS 8.8.8.8"

- 协议端口（可选）

  port 443
  proto tcp
  explicit-exit-notify 0

- 指定服务器证书文件

  cert vpnserver.crt
  key vpnserver.key

配置OpenVPN服务

你看见的不是你真的看见的

- 启动服务器路由功能
  - sudo vi /etc/sysctl.conf
    net.ipv4.ip_forward=1
  - sudo sysctl -p
- 确定默认路由网卡名称
  - ip route | grep default
    default via 192.168.8.2 dev **enp0s3** proto static
- 修改防火墙规则实现NAT
  - sudo vi /etc/ufw/before.rules # 优先级高于普通UFW规则

配置OpenVPN服务

你看见的不是你真的看见的

- sudo vi /etc/ufw/before.rules

```
......
#   ufw-before-output
#   ufw-before-forward
#

# START OPENVPN RULES
*nat
:POSTROUTING ACCEPT [0:0]
-A POSTROUTING -s 10.8.0.0/8 -o enp0s3 -j MASQUERADE
COMMIT
# END OPENVPN RULES
```

配置OpenVPN服务

你看见的不是你真的看见的

- sudo vi /etc/default/ufw　　# 防火墙默认开启转发包
  DEFAULT_FORWARD_POLICY="ACCEPT"
- 启动防火墙及规则
  - sudo ufw allow 1194/udp
  - sudo ufw allow OpenSSH
  - sudo ufw disable
  - sudo ufw enable
- 启动OpenVPN服务
  - sudo systemctl start openvpn@server　　# server.conf
  - sudo systemctl status openvpn@server
  - sudo systemctl enable openvpn@server
  - ip addr show tun0

客户端配置脚本

你看见的不是你真的看见的

- 配置文件模板
  - mkdir -p ~/client-configs/files　　# 配置文件存放目录
  - cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf ~/client-configs/base.conf
  - Linux 客户端有 /etc/openvpn/update-resolv-conf
  - vi ~/client-configs/base.conf

```
# script-security 2                          # 仅针对Linux客户端
# up /etc/openvpn/update-resolv-conf
# down /etc/openvpn/update-resolv-conf
```

客户端配置脚本

你看见的不是你真的看见的

- vi ~/client-configs/base.conf

```
remote vpnserver_ip 1194
proto udp
user nobody
group nogroup
#ca ca.crt
#cert client.crt
#key client.key
#tls-auth ta.key 1
cipher AES-256-CBC
auth SHA256
key-direction 1
```


客户端配置脚本

你看见的不是你真的看见的

- vi ~/client-configs/make_config.sh　　# 脚本参数为客户端标识名

```
#!/bin/bash
KEY_DIR=~/client-configs/keys
OUTPUT_DIR=~/client-configs/files
BASE_CONFIG=~/client-configs/base.conf
cat ${BASE_CONFIG} \
    <(echo -e '<ca>') \
    ${KEY_DIR}/ca.crt \
    <(echo -e '</ca>\n<cert>') \
    ${KEY_DIR}/${1}.crt \
    <(echo -e '</cert>\n<key>') \
    ${KEY_DIR}/${1}.key \
    <(echo -e '</key>\n<tls-auth>') \
    ${KEY_DIR}/ta.key \
    <(echo -e '</tls-auth>') \
    > ${OUTPUT_DIR}/${1}.ovpn
```

客户端配置脚本

你看见的不是你真的看见的

- chmod 700 ~/client-configs/make_config.sh
- cd ~/client-configs
- sudo ./make_config.sh client1
  - client1.ovpn
- 分别为每个客户端生成相应证书，然后运行脚本生成配置文件
- 将 .ovpn 配置文件拷贝至客户端
- Linux 客户端

  script-security 2
  up /etc/openvpn/update-resolv-conf
  down /etc/openvpn/update-resolv-conf

客户端配置脚本

你看见的不是你真的看见的

- Linux 客户端安装
  - sudo apt install openvpn
- Linux 客户端
  - vi client1.ovpn

    script-security 2

    up /etc/openvpn/update-resolv-conf

    down /etc/openvpn/update-resolv-conf
- CentOS 系统
  - group nobody # nogroup
- 建立VPN连接
  - sudo openvpn --config client1.ovpn >/dev/null 2>&1 &

客户端配置脚本

你看见的不是你真的看见的

- 图形化Linux VPN客户端
  - sudo apt install network-manager-openvpn-gnome
  - sudo systemctrl restart network-manager
  - 网络设置导入配置文件创建VPN连接
- 其他VPN客户端
  - Cisco Concentrator　　network-manager-vpnc
  - Cisco OpenConnect　　network-manager-openconnect
  - PPTP (Microsoft VPN)　　network-manager-pptp
  - strongSwan (for some IPsec VPNs)　　network-manager-strongswan

客户端配置脚本

你看见的不是你真的看见的

- Windows 客户端
  - https://openvpn.net/index.php/open-source/downloads.html
  - C:\Program Files\OpenVPN\config\client2.ovpn
  - 以管理员身份运行
- IOS
  - App Store 搜索 OpenVPN Connect
- Android
  - OpenVPN Connect
- MacOS
  - https://tunnelblick.net/downloads.html
  - 安装结束自动提示导入客户端配置文件

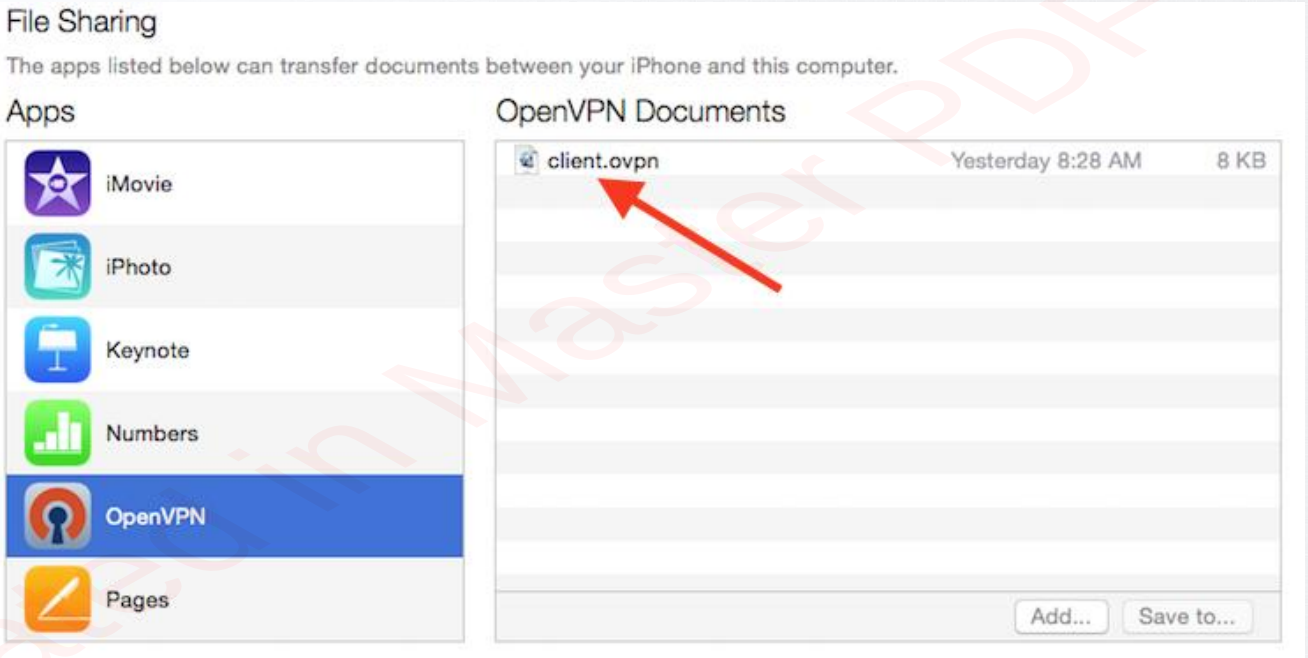
客户端配置脚本

你看见的不是你真的看见的

- Windows 客户端
  - https://openvpn.net/index.php/open-source/downloads.html
  - C:\Program Files\OpenVPN\config\client2.ovpn
  - 以管理员身份运行
- IOS
  - App Store 搜索 OpenVPN Connect
- Android
  - OpenVPN Connect
- MacOS
  - https://tunnelblick.net/downloads.html
  - 安装结束自动提示导入客户端配置文件

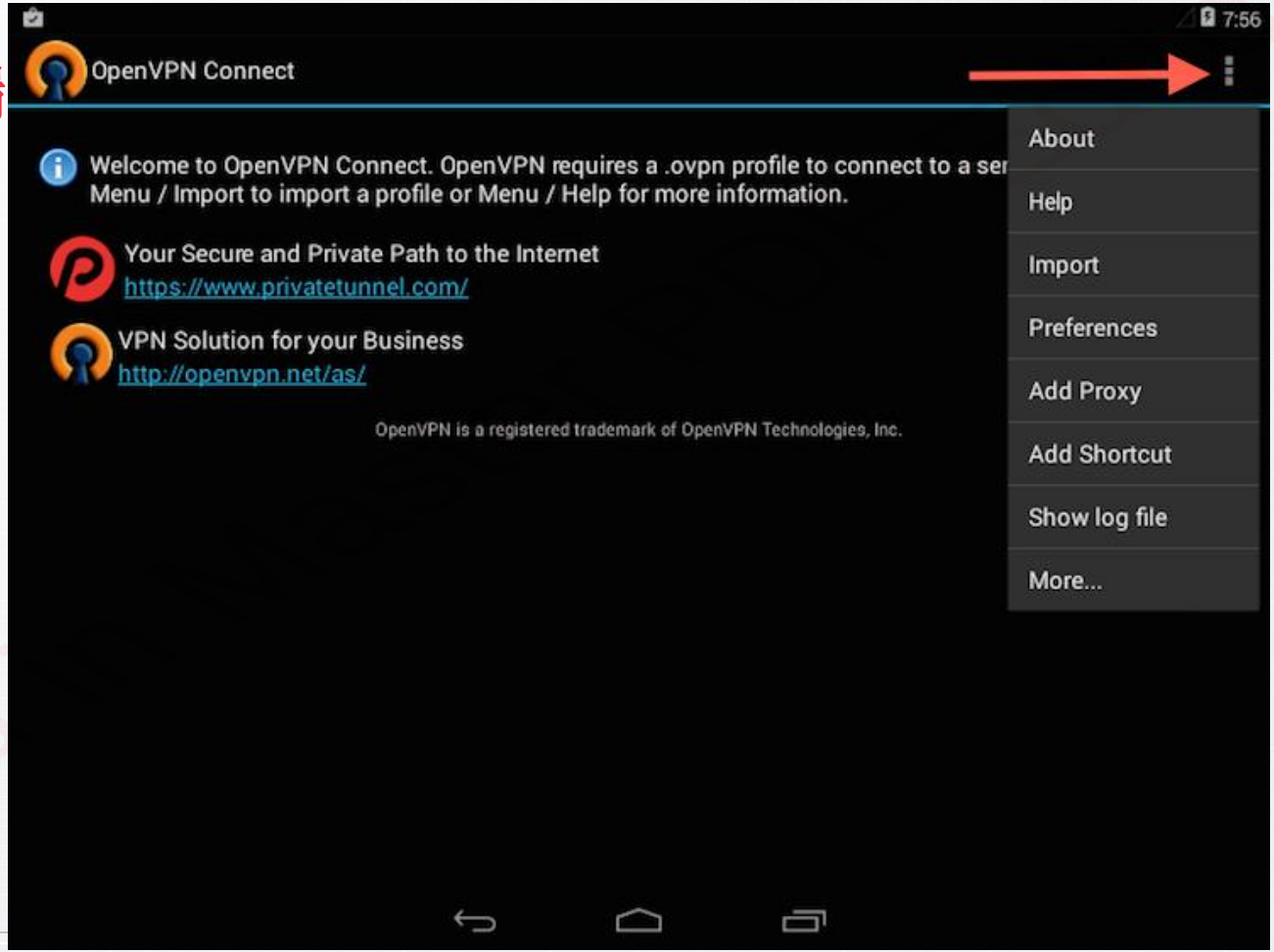
IOS客户端

你看见的不是你真的看见的



Android客户端

你看见的不是你真的看见的



撤销客户端证书

你看见的不是你真的看见的

- CA Server
  - cd EasyRSA-3.0.4/
  - ./easyrsa revoke client2
  - ./easyrsa gen-crl # 证书吊销列表 CRL（crl.pem）
  - scp /pki/crl.pem yuanfh@vpnserver_ip:/tmp
- VPN Server
  - sudo cp /tmp/crl.pem /etc/openvpn
  - sudo vi /etc/openvpn/server.conf
  - crl-verify crl.pem
  - sudo systemctl restart openvpn@server

Questions？