

# Construct a VPN by making use of OpenVPN

数据科学与计算机学院

2015 级计应

15331151

李佳

## 一、VPN 和 OpenVPN

VPN 的英文全称是“Virtual Private Network”，翻译过来就是“虚拟专用网络”。虚拟专用网络我们可以把它理解成是虚拟出来的企业内部专线。它可以通过特殊的加密的通讯协议在连接在 Internet 上的位于不同地方的两个或多个企业内部网之间建立一条专有的通讯线路。

虚拟专用网络功能是：在公用网络上建立专用网络，进行加密通讯。在企业网络中有广泛应用。VPN 网关通过对数据包的加密和数据包目标地址的转换实现远程访问。VPN 有多种分类方式，主要是按协议进行分类。VPN 可通过服务器、硬件、软件等多种方式实现。VPN 具有成本低，易于使用的特点。

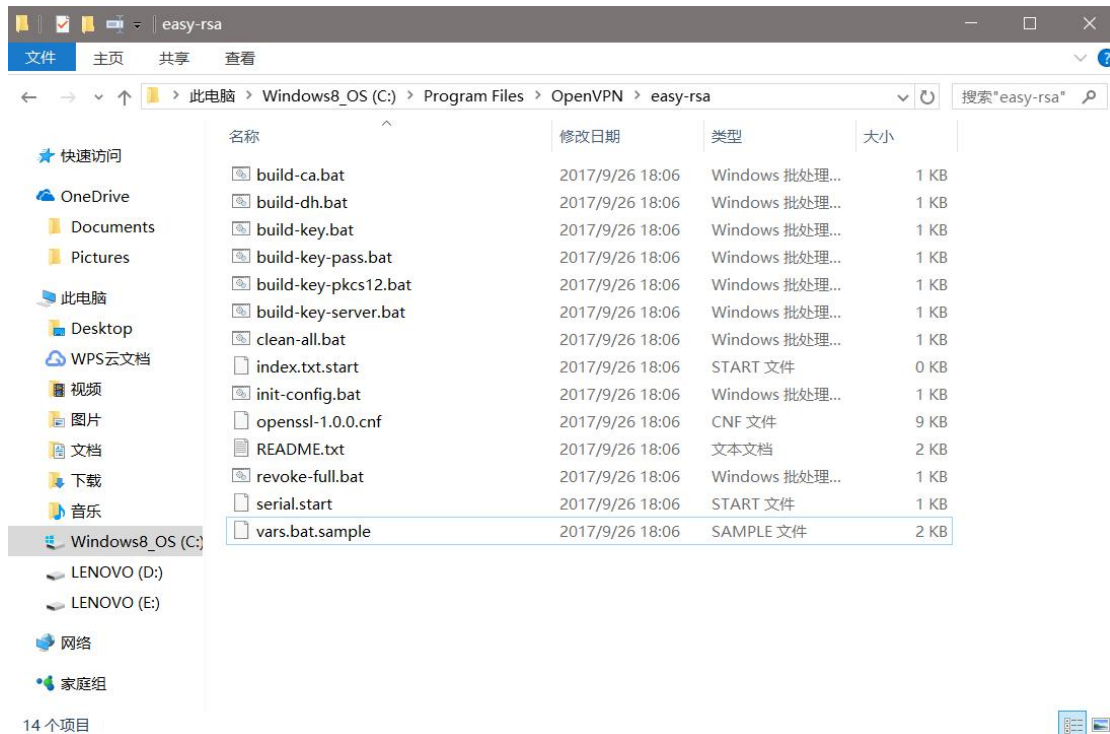
OpenVPN 是一个基于 OpenSSL 库的应用层 VPN 实现。和传统 VPN 相比，它的优点是简单易用。OpenVPN 允许参与建立 VPN 的单点使用共享金钥，电子证书，或者用户名/密码来进行身份验证。它大量使用了 OpenSSL 加密库中的 SSLv3/TLSv1 协议函数库。OpenVPN 能在 Solaris、Linux、OpenBSD、FreeBSD、NetBSD、Mac OS X 与 Windows 2000/XP/Vista 上运行，并包含了许多安全性的功能。它并不是一个基于 Web 的 VPN 软件，也不与 IPsec 及其他 VPN 软件包兼容。OpenVPN2.0 后引入了用户名/口令组合的身份验证方式，它可以省略客户端证书，但是仍有一份服务器证书需要被用作加密。

## 二、Windows10 使用 OpenVPN 配置 VPN

1. 安装 OpenVPN（官网不知道为什么上不去，可能被墙了，在 <https://www.techspot.com/>上可以下载）。



2. 修改 easy-rsa 目录下的 vars.bar.Sample 的内容，另存为 vars.bat（不是很懂为什么这些文件显示的时间都是两个月前）。



```
set KEY_COUNTRY=US
set KEY_PROVINCE=CA
set KEY_CITY=SanFrancisco
set KEY_ORG=OpenVPN
set KEY_EMAIL=mail@host.domain
set KEY_CN=changeme
set KEY_NAME=changeme
set KEY_OU=changeme
set PKCS11_MODULE_PATH=changeme
set PKCS11_PIN=1234
```

修改为下面的内容：

```
set KEY_COUNTRY=CN
set KEY_PROVINCE=GD
set KEY_CITY=GuangZhou
set KEY_ORG=SYSU_LJ
set KEY_EMAIL=1335275309@qq.com
set KEY_CN=ME
set KEY_NAME=Tomy
set KEY_OU=Lee
set PKCS11_MODULE_PATH=changeme
set PKCS11_PIN=1234
```

|                 |                 |                |      |
|-----------------|-----------------|----------------|------|
| README.txt      | 2017/9/26 18:06 | 文本文档           | 2 KB |
| revoke-full.bat | 2017/9/26 18:06 | Windows 批处理... | 1 KB |
| serial.start    | 2017/9/26 18:06 | START 文件       | 1 KB |
| vars.bat        | 2017/9/26 18:06 | Windows 批处理... | 2 KB |
| vars.bat.sample | 2017/9/26 18:06 | SAMPLE 文件      | 2 KB |

### 3. 使用命令行（管理员模式）进行初始化配置。

#### **init-config**

复制配置文件为批处理

#### **vars**

清除 key 子文件夹中的文件

#### **clean-all**

```
C:\>cd Program Files
C:\Program Files>cd OpenVPN
C:\Program Files\OpenVPN>cd easy-rsa
C:\Program Files\OpenVPN\easy-rsa>vars
C:\Program Files\OpenVPN\easy-rsa>clean-all
已复制      1 个文件。
已复制      1 个文件。
C:\Program Files\OpenVPN\easy-rsa>
```

中文(简体) - 百度输入法 全 :

### 4.生成根 CA

#### **build-ca**

```
C:\Program Files\OpenVPN\easy-rsa>build-ca
WARNING: can't open config file: /etc/ssl/openssl.cnf
Generating a 4096 bit RSA private key
.....++
.....++
writing new private key to 'keys\ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [US]:CN
State or Province Name (full name) [CA]:GD
Locality Name (eg, city) [SanFrancisco]:GuangZhou
Organization Name (eg, company) [OpenVPN]:SYSU_LJ
Organizational Unit Name (eg, section) [changeme]:ME
Common Name (eg, your name or your server's hostname) [changeme]:Tomy
Name [changeme]:Lee
Email Address [mail@host.domain]:1335275309@qq.com
C:\Program Files\OpenVPN\easy-rsa>
```

中文(简体) - 百度输入法 全 :

## build-dh

### 6.生成服务器端证书、客户端证书和 TA 证书:

生成 **server** 使用证书: **build-key-server server**

```
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:123456
An optional company name []:yServer
WARNING: can't open config file: /etc/ssl/openssl.cnf
Using configuration from openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName          :PRINTABLE:'CN'
stateOrProvinceName  :PRINTABLE:'GD'
localityName         :PRINTABLE:'GuangZhou'
organizationName     :T61STRING:'SYSU_LJ'
organizationalUnitName:PRINTABLE:'ME'
commonName           :PRINTABLE:'Tomy'
name                 :PRINTABLE:'Lee'
emailAddress         :IA5STRING:'1335275309@qq.com'
Certificate is to be certified until Nov 14 09:05:38 2027 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated

C:\Program Files\OpenVPN\easy-rsa>
```

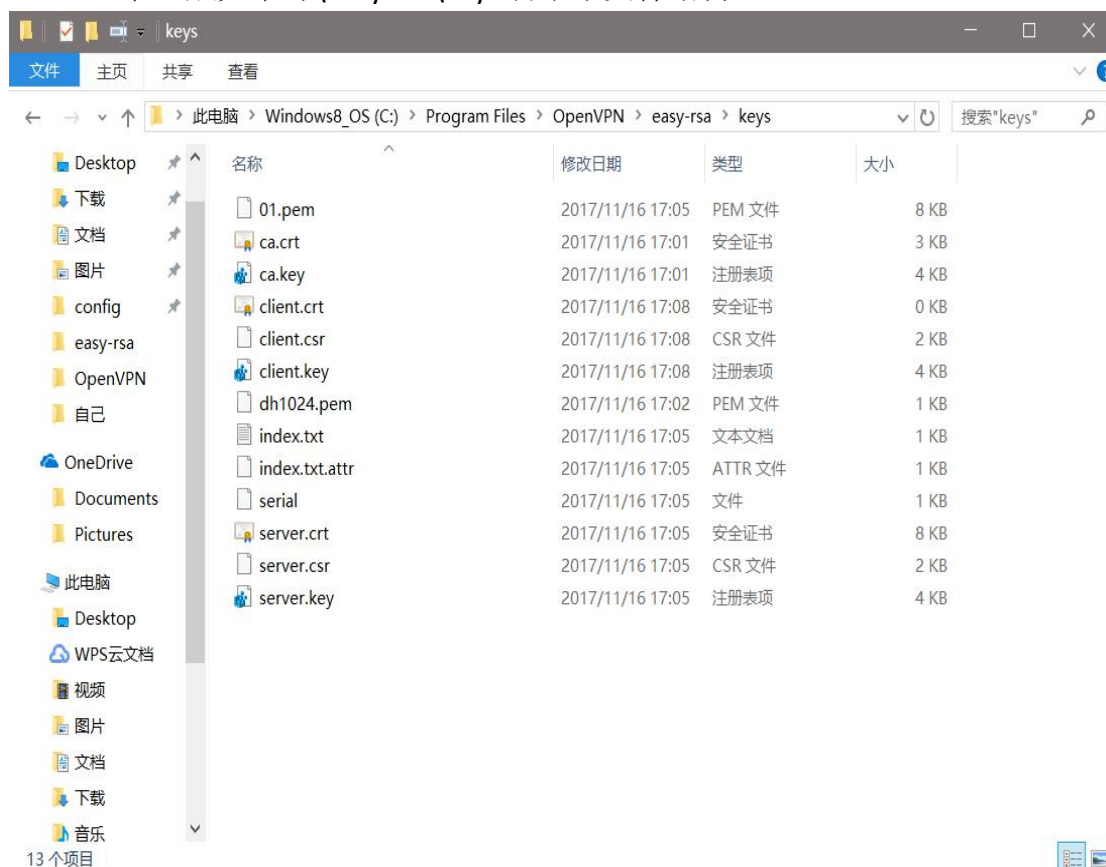


## 生成客户端证书: build-key client

```
C:\Program Files\OpenVPN\easy-rsa>build-key client
WARNING: can't open config file: /etc/ssl/openssl.cnf
Generating a 4096 bit RSA private key
.....++
.....++
writing new private key to 'keys/client.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [US]:CN
State or Province Name (full name) [CA]:GD
Locality Name (eg, city) [SanFrancisco]:GuangZhou
Organization Name (eg, company) [OpenVPN]:SYSU_LJ
Organizational Unit Name (eg, section) [changeme]:ME
Common Name (eg, your name or your server's hostname) [changeme]:Tomy
Name [changeme]:Lee
Email Address [mail@host.domain]:1335275309@qq.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:123456
An optional company name []:yClient
WARNING: can't open config file: /etc/ssl/openssl.cnf
Using configuration from openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName       :PRINTABLE:'CN'
stateOrProvinceName :PRINTABLE:'GD'
localityName      :PRINTABLE:'GuangZhou'
organizationName  :T61STRING:'SYSU_LJ'
organizationalUnitName:PRINTABLE:'ME'
commonName        :PRINTABLE:'Tomy'
name              :PRINTABLE:'Lee'
emailAddress      :IA5STRING:'1335275309@qq.com'
Certificate is to be certified until Nov 14 09:08:20 2027 GMT (3650 days)
Sign the certificate? [y/n]:y
```

## 7.证书生成完毕时\easy-rsa\keys 目录下文件结构:






## 8.服务端和客户端的配置

配置文件位于 C:\Program Files\OpenVPN\sample-config 文件夹，将 sample-config 目录下的 server.ovpn 和 client.ovpn 复制到服务端的 config 文件夹。

#### ①服务端配置(server.ovpn)

查看文件名是否匹配

```
ca ca.crt
cert server.crt
key server.key # This file should be kept secret
```

|  |                  |        |      |
|--|------------------|--------|------|
|  server.crt | 2017/11/16 17:05 | 安全证书   | 8 KB |
|  server.csr | 2017/11/16 17:05 | CSR 文件 | 2 KB |
|  server.key | 2017/11/16 17:05 | 注册表项   | 4 KB |

将配置文件中 dh dh2048.pem 修改为 dh1024.pem

```
# Diffie hellman parameters.
# Generate your own with:
# openssl dhparam -out dh2048.pem 2048
dh dh1024.pem
```




把 C:\Program Files\OpenVPN\easy-rsa\keys 目录下的 ca.crt、ca.key、server.crt、server.csr、server.key、dh1024.pem 复制到 C:\Program Files\OpenVPN\config 目录下。server 端的配置完成，点击 OpenVPN GUI 图片，点击 connect 连接，连接成功后，灰色图标变为绿色。



#### ②客户端配置(client.ovpn)，检查证书名是否匹配以及连接的 IP 地址

查看文件名是否匹配

```
ca ca.crt
cert client.crt
key client.key
```

|  |                  |        |      |
|--|------------------|--------|------|
|  client.crt | 2017/11/16 17:08 | 安全证书   | 0 KB |
|  client.csr | 2017/11/16 17:08 | CSR 文件 | 2 KB |
|  client.key | 2017/11/16 17:08 | 注册表项   | 4 KB |

修改连接服务端的 IP 地址

```
# The hostname/IP and port of the server.
# You can have multiple remote entries
# to load balance between the servers.
remote 172.18.43.69 1194
;remote my-server-2 1194
```

同上，把 C:\Program Files\OpenVPN\easy-rsa\keys 目录下的 client.csr、client.crt、client.key、ca.key、ca.crt 文件复制到客户端的 C:\Program Files\OpenVPN\config 目录下。client 端配置完成，右键小图标，启动客户端，图标变为绿色则配置成功。同上过程不再赘述。

至此，VPN 成功创建。

#### 9.检查是否连通。

验证：ping server 端的 ip 地址 10.8.0.1

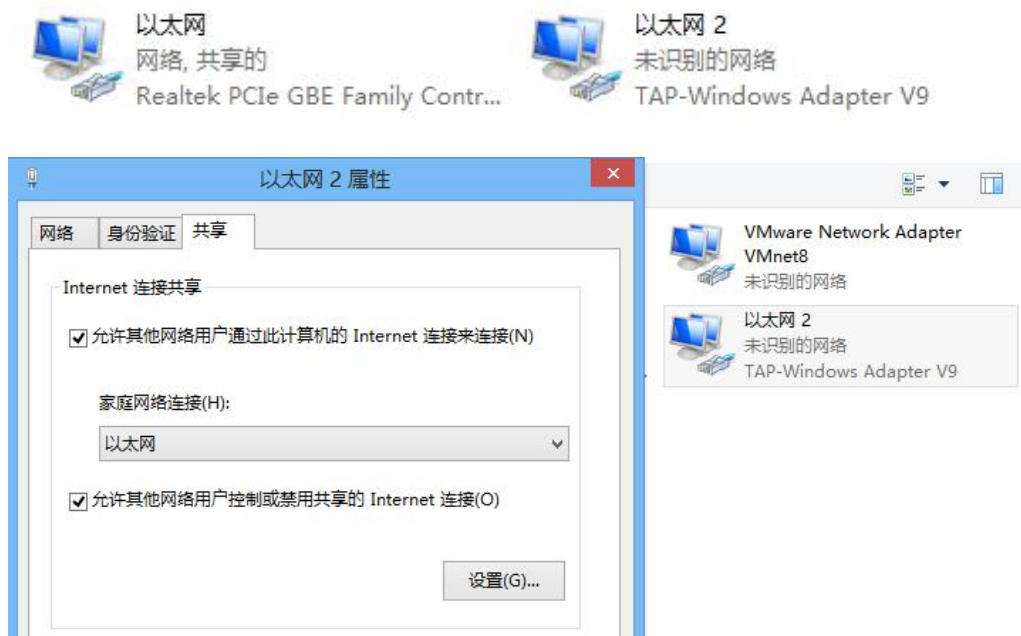
```
C:\Users\Heath>ping 10.8.0.1

正在 Ping 10.8.0.1 具有 32 字节的数据:
来自 10.8.0.1 的回复: 字节=32 时间=2ms TTL=64
来自 10.8.0.1 的回复: 字节=32 时间=2ms TTL=64
来自 10.8.0.1 的回复: 字节=32 时间=7ms TTL=64
来自 10.8.0.1 的回复: 字节=32 时间=25ms TTL=64

10.8.0.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 2ms, 最长 = 25ms, 平均 = 9ms
```

## 10. 架设 VPN 网络

client 端需要通过外网 IP 进行访问，要将网络设置为共享模式。在 server 端进行设置，server 端已创建一个新的虚拟网。



此时，VPN 搭建完成，可以使用，实验过程结束。

## 三、实验参考和总结

通过手动设置 VPN，我对专有隧道协议和虚拟网络的高安全性有了更多的认识。实验过程中遇到一些问题，比如第一次安装时未勾选安装 RSA 生成器；第一次连接时提示套接字绑定失败地址已被使用，还有在 IP 设置时的困难。经过查阅资料 and 博客，有了一定的解决。还是挺有意思的。

实验参考：

[1]Windows 下搭建 OpenVPN

<http://blog.csdn.net/qihuanfengyun/article/details/7892715>

[2]debian 下通过 vps 搭建 OpenVPN

<http://shit.name/openvpn-on-debian/>