

配置 OpenVPN 进行加密通讯

v0.1

2005-11-30

Coolc

前言.....	1
OpenVPN 软件背景小知识:.....	2
首先编译安装.....	2
生成 KEY 及证书文件。.....	3
生成 CA 证书及 key 文件.....	3
生成 server 证书和 key 文件.....	4
生成 client 证书和 key 文件.....	5
生成 Generate Diffie Hellman parameters.....	6
Key Files	6
配置 OpenVPN 文件	7
编辑 server 配置文件.....	7
Editing the client configuration files	9
初始化 VPN Server	10
启动客户端.....	11
Starting the client.....	11

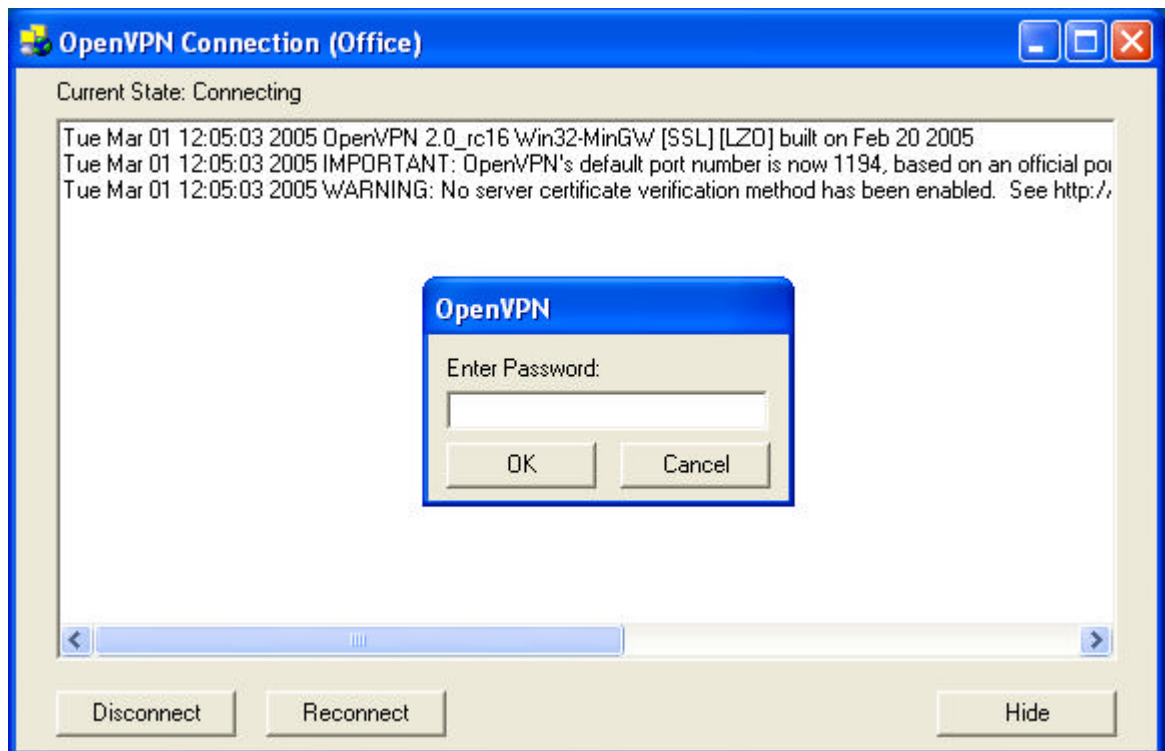
前言

Coolc 突然对 VPN 软件有了一些兴趣,找了几篇 Openvpn 的文章,感觉不够 step by step。于是索性自己做个简单教程,让大家以后自己鼓弄时也有个参考,也给自己留个备忘。主要是参考官方文档一步步作下来的,有时间的朋友还是建议去读读官方文档,这样能了解的更深入些。

OpenVPN 软件背景小知识:

优点:

- 支持多种常用应用系统。目前版本支持 Linux, Windows 2000/XP and higher, OpenBSD, FreeBSD, NetBSD, Mac OS X, and Solaris。
- 支持多种客户端连接模式。可以通过 GUI 便捷的操作



- OpenVPN 工作在 OSI layer 2 或 3 使用标准的 SSL/TLS 协议, 可以通过 certificates 或 smart cards 认证。
- 加密强度较高, 不易在传输通路上被人劫持破解信息资讯。

缺点:

使用 SSL 应用层加密, 传输效率要低于 IPSEC 传输的 VPN 软件。

首先编译安装

从官方下载 openvpn 软件, 并下载 lzo-1.08.tar.gz (vpn 传输时用到的压缩数据的库文件。) 校验通过后开始安装。按照先后顺序对 lzo 和 openvpn 进行安装。

```
./configure
make
make install
```

选择 VPN 运行模式

一般需要在配置前确认自己选择 routed 还是 bridged 模式，个人建议 routed。（除非你想要用 IPX 之类比较不常见的协议等）

选用 vpn 私有的网段 10.8.0.0/24。

生成 KEY 及证书文件。

进入 easy-rsa 目录

生成 CA 证书及 key 文件

```
#cd 2.0
#. ./vars
#./clean-all
#./build-ca
root@test02:~/openvpn/openvpn-2.0.5/easy-rsa/2.0# ./build-ca
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to '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]:
Locality Name (eg, city) [SanFrancisco]:
Organization Name (eg, company) [Fort-Funston]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [Fort-Funston CA]:OpenVPN-CA
Email Address [me@myhost.mydomain]:coolc@openvpn.net
```

生成 server 证书和 key 文件

```
./build-key-server server
root@test02:~/openvpn/openvpn-2.0.5/easy-rsa/2.0# ./build-key-server server
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'server.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]:ShenZhen
Locality Name (eg, city) [SanFrancisco]:
Organization Name (eg, company) [Fort-Funston]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [server]:
Email Address [me@myhost.mydomain]:server@openvpn.net

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /root/openvpn/openvpn-2.0.5/easy-rsa/2.0/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName          :PRINTABLE:'CN'
stateOrProvinceName  :PRINTABLE:'ShenZhen'
localityName         :PRINTABLE:'SanFrancisco'
organizationName     :PRINTABLE:'Fort-Funston'
commonName           :PRINTABLE:'server'
emailAddress         :IA5STRING:'server@openvpn.net'
Certificate is to be certified until Nov 28 08:42:32 2015 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
```

要点

- **Common Name** 填入 "server".
- "Sign the certificate? [y/n]"
- "1 out of 1 certificate requests certified, commit? [y/n]".

生成 client 证书和 key 文件

这里假设制作 3 个客户端证书。

```
./build-key client1
root@test02:~/openvpn/openvpn-2.0.5/easy-rsa/2.0# ./build-key client
Generating a 1024 bit RSA private key
.....++++++
.....++++++
writing new private key to '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]:ShenZhen
Locality Name (eg, city) [SanFrancisco]:
Organization Name (eg, company) [Fort-Funston]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [client]:client1
Email Address [me@myhost.mydomain]:client@openvpn.net
```

```
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from
/root/openvpn/openvpn-2.0.5/easy-rsa/2.0/openssl.cnf
DEBUG[load_index]: unique_subject = "yes"
Check that the request matches the signature
Signature ok
```

```
The Subject's Distinguished Name is as follows
countryName          :PRINTABLE:'CN'
stateOrProvinceName :PRINTABLE:'ShenZhen'
localityName         :PRINTABLE:'SanFrancisco'
organizationName     :PRINTABLE:'Fort-Funston'
commonName           :PRINTABLE:'client1'
emailAddress         :IA5STRING:'client@openvpn.net'
Certificate is to be certified until Nov 28 08:48:15 2015 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
```

要点

- **Common Name** 填入 "client1".
- "Sign the certificate? [y/n]"
- "1 out of 1 certificate requests certified, commit? [y/n]".

```
./build-key client2
```

略

```
./build-key client3
```

略

生成 **Generate Diffie Hellman parameters**

传输进行密钥交换时用到的交换密钥协议所需文件。

```
./build-dh
```

```
root@test02:~/openvpn/openvpn-2.0.5/easy-rsa/2.0# ./build-dh
Generating DH parameters, 1024 bit long safe prime, generator 2
This is going to take a long time
```

```
.....+.....
.....+...+.....+.....
.....
.....+.....+.....+.....
```

Key Files

生成证书和 key 文件列表，所有 .key 文件需要单独保存，不应遗留再服务器上。(其中仅有 server 上允许保留 server.key;client 上允许保留 client.key)再次生成证书时，再取出使用。Key 文件是整个加密体系的基础，一旦被获取，整个加密体系就会失效，因此需要严格保护。

Openvpn 给出了一个完整的敏感性列表。

Filename	Needed By	Purpose	Secret
ca.crt	server + all clients	Root CA certificate	NO
ca.key	key signing machine only	Root CA key	YES
dh{n}.pem	server only	Diffie Hellman parameters	NO
server.crt	server only	Server Certificate	NO
server.key	server only	Server Key	YES
client1.crt	client1 only	Client1 Certificate	NO
client1.key	client1 only	Client1 Key	YES
client2.crt	client2 only	Client2 Certificate	NO
client2.key	client2 only	Client2 Key	YES
client3.crt	client3 only	Client3 Certificate	NO
client3.key	client3 only	Client3 Key	YES

配置 OpenVPN 文件

修改软件包自带的配置文件

```
root@test02:~/openvpn/openvpn-2.0.5# cd sample-config-files/
```

编辑 server 配置文件

下面将配置一个服务器端的样例配置程序

- 生成 virtual TUN network interface (for routing)
- 在 UDP port 1194 (OpenVPN's official port number) 监听通讯
- 向客户端分发 10.8.0.0/24 的子网地址.

编辑配置文件中 ca, cert, key, and dh parameters 的文件存放路径, 指向我们刚才生成文件的位置。

```
root@test02:~/openvpn/openvpn-2.0.5/sample-config-files# cp
-r ../easy-rsa/2.0/keys/ /etc/openvpn/
```

```
root@test02:~/openvpn/openvpn-2.0.5/sample-config-files# cp
server.conf /etc/openvpn/
```

```
root@test02:~/openvpn/openvpn-2.0.5/sample-config-files# cp
client.conf /etc/openvpn/
```

```
root@test02:~/openvpn/openvpn-2.0.5/sample-config-files# cp ipp.txt
/etc/openvpn/
```

- 编译 server.conf 文件

对 server.conf 文件做如下配置修改

```
port 1194

;proto tcp

proto udp

dev tun

ca /etc/openvpn/keys/ca.crt

cert /etc/openvpn/keys/server.crt

dh /etc/openvpn/keys/dh1024.pem

server 10.8.0.0 255.255.255.0

ifconfig-pool-persist /etc/openvpn/ipp.txt

keepalive 10 120

comp-lzo

max-clients 10

user nobody
```

```
group nobody

persist-key

persist-tun

status /var/log/openvpn/openvpn-status.log

log /var/log/openvpn/openvpn.log

verb 3
```

Editing the client configuration files

- 编辑配置文件中 ca, cert, key, and dh parameters 的文件存放路径, 指向我们刚才生成文件的位置。
- comp-lzo 在客户端和服务端都已经安装

```
[root@RH-syslog-server openvpn-2.0.5]# cp sample-config-files/client.conf /etc/openldap/ openvpn/ opt/
```

```
[root@RH-syslog-server openvpn-2.0.5]# cp sample-config-files/client.conf /etc/openvpn/
```

```
[root@RH-syslog-server openvpn-2.0.5]# scp -r root@172.30.28.130:/etc/openvpn/keys /etc/openvpn/
```

- 编译 client.conf 文件

```
client

dev tun

proto udp

remote 172.30.28.103 1194

nobind

user nobody

group nobody
```

persist-key

persist-tun

ca /etc/openvpn/keys/ca.crt

cert /etc/openvpn/keys/client.crt

key /etc/openvpn/keys/client.key

comp-lzo

verb 3

初始化 VPN Server

- 初始化虚拟网卡

```
root@test02:~/openvpn# mknod /dev/net/tun c 10 200
```

```
root@test02:~/openvpn# modprobe tun
```

```
root@test02:~/openvpn# echo 1 > /proc/sys/net/ipv4/ip_forward
```

- 启动 vpn

```
root@test02:~/openvpn# openvpn /etc/openvpn/server.conf
```

- 查看日志

```
root@test02:~# tail -f /var/log/openvpn/openvpn.log
```

```
Wed Nov 30 18:08:32 2005 /sbin/route add -net 10.8.0.0 netmask 255.255.255.0 gw 10.8.0.2
```

```
Wed Nov 30 18:08:33 2005 Data Channel MTU parms [ L:1542 D:1450 EF:42 EB:135 ET:0 EL:0  
AF:3/1 ]
```

```
Wed Nov 30 18:08:33 2005 GID set to nobody
```

```
Wed Nov 30 18:08:33 2005 UID set to nobody
```

```
Wed Nov 30 18:08:33 2005 UDPv4 link local (bound): [undef]:1194
```

```
Wed Nov 30 18:08:33 2005 UDPv4 link remote: [undef]
```

```
Wed Nov 30 18:08:33 2005 MULTI: multi_init called, r=256 v=256
```

```
Wed Nov 30 18:08:33 2005 IFCONFIG POOL: base=10.8.0.4 size=62
```

```
Wed Nov 30 18:08:33 2005 IFCONFIG POOL LIST
```

```
Wed Nov 30 18:08:33 2005 Initialization Sequence Completed
```

启动客户端

Starting the client

启动客户端

```
root@test5:~# openvpn /etc/openvpn/client.conf
Wed Nov 30 19:49:06 2005 OpenVPN 2.0.5 i686-pc-linux [SSL] [LZO] built on Nov 30 2005
Wed Nov 30 19:49:06 2005 IMPORTANT: OpenVPN's default port number is now 1194, based on an official
port number assignment by IANA. OpenVPN 2.0-beta16 and earlier used 5000 as the default port.
Wed Nov 30 19:49:06 2005 WARNING: No server certificate verification method has been enabled.
See http://openvpn.net/howto.html#mitm for more info.
Wed Nov 30 19:49:06 2005 LZO compression initialized
Wed Nov 30 19:49:06 2005 Control Channel MTU parms [ L:1542 D:138 EF:38 EB:0 ET:0 EL:0 ]
Wed Nov 30 19:49:06 2005 Data Channel MTU parms [ L:1542 D:1450 EF:42 EB:135 ET:0 EL:0 AF:3/1 ]
Wed Nov 30 19:49:06 2005 Local Options hash (VER=V4): '41690919'
Wed Nov 30 19:49:06 2005 Expected Remote Options hash (VER=V4): '530fdded'
Wed Nov 30 19:49:06 2005 UDPv4 link local: [undef]
Wed Nov 30 19:49:06 2005 UDPv4 link remote: 172.30.28.102:1194
Wed Nov 30 19:49:06 2005 TLS: Initial packet from 172.30.28.102:1194, sid=f8d2337a 75be9018
Wed Nov 30 19:49:06 2005 VERIFY OK: depth=1,
/C=CN/ST=CA/L=SanFrancisco/O=Fort-Funston/CN=OpenVPN-CA/emailAddress=coolc@openvpn.net
Wed Nov 30 19:49:06 2005 VERIFY OK: depth=0,
/C=CN/ST=ShenZhen/L=SanFrancisco/O=Fort-Funston/CN=server/emailAddress=server@openvpn.net
Wed Nov 30 19:49:06 2005 Data Channel Encrypt: Cipher 'BF-CBC' initialized with 128 bit key
Wed Nov 30 19:49:06 2005 Data Channel Encrypt: Using 160 bit message hash 'SHA1' for HMAC
authentication
Wed Nov 30 19:49:06 2005 Data Channel Decrypt: Cipher 'BF-CBC' initialized with 128 bit key
Wed Nov 30 19:49:06 2005 Data Channel Decrypt: Using 160 bit message hash 'SHA1' for HMAC
authentication
Wed Nov 30 19:49:06 2005 Control Channel: TLSv1, cipher TLSv1/SSLv3 DHE-RSA-AES256-SHA, 1024 bit
RSA
Wed Nov 30 19:49:06 2005 [server] Peer Connection Initiated with 172.30.28.102:1194
Wed Nov 30 19:49:06 2005 TCP/UDP: Incoming packet rejected from 172.30.28.104:53754[2], expected
peer address: 172.30.28.102:1194 (allow this incoming source address/port by removing --remote
or adding --float)
```

确认 vpn 通讯正常

```
ping 10.8.0.1
```

```
root@test5:/etc/openvpn# ping 10.8.0.1
PING 10.8.0.1 (10.8.0.1) 56(84) bytes of data.
64 bytes from 10.8.0.1: icmp_seq=1 ttl=64 time=0.841 ms
64 bytes from 10.8.0.1: icmp_seq=2 ttl=64 time=0.333 ms
64 bytes from 10.8.0.1: icmp_seq=3 ttl=64 time=0.741 ms
```

64 bytes from 10.8.0.1: icmp_seq=4 ttl=64 time=0.902 ms

整个配置完成，可以通过此 VPN 通道进行加密传输了。 :)