Construct a VPN by making use of OpenVPN

13331233 孙中阳

VPN

VPN， 即虚拟专用网络，其目的是在公用网络上建立专用网络，进行加密通讯。

Open VPN

OpenVPN 是一个基于 OpenSSL 库的开源软件能够提供VPN服务，但更加简单易用。能在Solaris、Linux、OpenBSD、FreeBSD、NetBSD、Mac OS X与Microsoft Windows以及Android和iOS上运行，并包含了许多安全性的功能。
Open VPN的官网在国内无法访问，所以需要首先配置一个翻墙服务，以获取有关资源

Open VPN 的创建和使用

环境

ubuntu14.04.3
软件包 openvpn，easy-rsa

安装

首先建立PKI:
依次执行命令

```
mkdir /etc/openvpn/easy-rsa/
cp -r /usr/share/easy-rsa/* /etc/openvpn/easy-rsa/
```

接下来，编辑文件 `/etc/openvpn/easy-rsa/vars` ，并改写如下内容

```
export EASY_RSA='/etc/openvpn/easy-rsa'
export KEY_COUNTRY="CN"
export KEY_PROVINCE="Guangdong"
export KEY_CITY="Guangzhou"
export KEY_ORG="OpenVPN"
export KEY_EMAIL="szy@sunzhongyang.com"
export KEY_OU="OrganizationUnit"
```

随后，切换到 `/etc/openvpn/easy-rsa/` 目录下并依次执行命令

```
source ./vars
./clean-all
./build-
```

服务器证书：

首先切换到 `easy-rsa` 目录下，然后依次执行命令:

```
 ./build-key-server VPNServer
 ./build-dh
```

到此已经生成了所需的证书
接下来切换到 `keys` 目录下，并将刚刚生成的证书文件复制到 `/etc/openvpn` 目录下

客户端证书:

首先切换到 `easy-rsa` 目录下，然后执行命令：

```
./build-key client1
```

接下来切换到 `keys` 目录下，并将刚刚生成的证书文件以及 `ca.crt` 安全地复制到客户端，所需复制的文件如下：

```
/etc/openvpn/ca.crt
/etc/openvpn/easy-rsa/keys/client1.crt
/etc/openvpn/easy-rsa/keys/client1.key
```

服务器配置：

首先将 `server.conf.gz` 复制到 `/etc/openvpn` 并解压，命令如下：

```
cp /usr/share/doc/openvpn/examples/sample-config-files/serv
er.conf.gz
gzip -d /etc/openvpn/server.conf.gz
```

编辑刚刚解压出的 `server.conf` （同样是给出改动内容）：

```
ca ca.crt
cert VPNServer.crt
key VPNServer.key
```

编辑 `/etc/sysctl.conf` ，取消 `net.ipv4.ip_forward=1` 这行的注释，从而开启IP转发，然后 `reload sysctl` ，命令如下：

```
sysctl -p /etc/sysctl.conf
```

简单的服务器配置到此结束，现在可以开启服务器进行测试

客户端配置:

说明:客户端同样为 ubuntu 14.04.3, 且没有全程工作在 root 权限下
安装 openvpn，使用 `apt-get`
将前面生成的三个文件复制到 `/etc/openvpn` ,此步骤需要提权
将 `openvpn` 的示例 client 配置复制到 `/etc/openvpn` ，命令如下:

```
sudo cp /usr/share/doc/openvpn/examples/sample-config-files
/client.conf /etc/openvpn/
```

编辑（依然给出改动内容):

```
ca ca.crt
cert VPNServer.crt
key VPNServer.key
remote 192.168.1.100 11
```

(注:此处测试环境为 192.168 的局域网,服务器 IP 为 192.168.1.100, 端口为 1194)

连接与测试

开启服务端(root权限下)：

命令如下:

```
service openvpn start
```

开启后可用命令

```
ifconfig tun0
netstat –rn
```

查看网络及路由状态

开启客户端：

命令如下:

```
sudo service openvpn start
```

开启后可用命令

```
ifconfig tun0
netstat –rn
```

查看网络及路由状态

测试连通性：

使用命令 `ping 10.8.0.1` 测试连通性