Openvpn 使用及证书生成说明

版本：<1.1>

发布日期：<2017-03-12

目录

1 模块介绍

1.1 概述

虚拟专用网 VPN(virtual private network)是在公共网络中建立的安全网络连接，这个网络连接和普通意义上的网络连接不同之处在于，它采用了专有的隧道协议，实现了数据的加密和完整性的检验、用户的身份认证，从而保证了信息在传输中不被偷看、篡改、复制，从网络连接的安全性角度来看，就类似于在公共网络中建立了一个专线网络一样，只不过这个专线网络是逻辑上的而不是物理的所以称为虚拟专用网。VPN 系统包括 VPN 服务器，VPN 客户机和隧道。由于使用 Internet 进行传输相对于租用专线来说，费用极为低廉，所以 VPN 的出现使企业通过 Internet 既安全又经济的传输私有的机密信息成为可能。

我们介绍的是 Windows 操作系统中利用 OpenVPN 配置 VPN ， OpenVPN 是一个开源的第三方虚拟专用网配置工具，可以利用固有设备搭建 VPN 应用网关。

2 服务器的安装与配置

OpenVPN 是一个开源的第三方虚拟专用网配置工具，可以利用固有设备搭建 VPN 应用网关。以下将分别介绍 Ubuntu、Windows 操作系统下的服务器的部署与配置。

2.1 Ubuntu 下搭建 OpenVPN 服务器

2.1.1 安装 OpenVPN 服务器

在 Ubuntu 下输入以下命令：

sudo apt-get -y install openvpn libssl-dev openssl
sudo apt-get -y install easy-rsa

2.1.2 证书制作

按照以下步骤执行命令生成 OpenVPN 正常运行所需要的证书
初始化配置:
sudo mkdir /etc/openvpn/easy-rsa/
sudo cp -r /usr/share/easy-rsa/* /etc/openvpn/easy-rsa/
sudo su
sudo vi /etc/openvpn/easy-rsa/vars
----->按照需要可以修改证书配置如下：
export KEY_COUNTRY=”CN”
export KEY_PROVINCE=”BJ”
export KEY_CITY=”BeiJing”
export KEY_ORG=”fanvil”
export KEY_EMAIL=”fanvil@fanvil.com”
export KEY_OU=”fanvil”
export KEY_NAME=”server”

运行 vars:	source vars
如果第一次运行清空所有:	./clean-all
生成 CA 证书:	./build-ca
生成服务器证书:	./build-key-server server
生成客户端证书:	./build-key client
产生动态密码库.	./build-dh

2.2 启动服务器

服务器环境配置，将相应的证书配置文件放入指定的目录：

cp keys/ca.crt /etc/openvpn/

cp keys/server.crt keys/server.key keys/dh2048.pem /etc/openvpn

mv /etc/openvpn/dh2048.pem /etc/openvpn/dh1024.pem

cp keys/client.key keys/client.crt /etc/openvpn/

cp /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz /etc/openvpn/

cd /etc/openvpn

gzip -d server.conf.gz

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

启动服务器:

/etc/init.d/openvpn restart

2.3 Windows 下搭建 OpenVPN 服务器

2.3.1 安装 OpenVPN 服务器

在网上搜索下载 Windows 版的 OpenVpn 软件。本篇搭建使用的是 openVPN GUI

双击下载软件进行默认安装，注意勾选安装 easy-rsa 配件。默认路径是 C:\Program Files\OpenVPN。

2.3.2 证书制作

在进行操作之前，首先要进行初始化工作:

请根据自身情况修改 C:\Program Files\OPENVPN\easy-rsa\vars.bat.sample 的以下部分

set HOME=C:\Program Files\OPENVPN\easy-rsa

set KEY_COUNTRY=CN #(国家)

set KEY_PROVINCE=BEIJING #(省份)

set KEY_CITY= BEIJING #(城市)

set KEY_ORG=WINLINE #(组织)

set KEY_EMAIL=admin@winline.com.cn #(邮件地址)

上面#开始的是注释，请不要写到文件中。

以管理员权限打开 cmd 进入 DOS，执行下列命令

进入 openvpn\easy-rsa 目录:

init-config

vars

clean-all

生成根证书: build-ca（一路回车按照缺省配置生成即可）

产生动态密码库: build-dh

生成服务器证书: build-key-server server（一路回车按照缺省配置生成即可）

生成客户端证书: build-key client （一路回车按照缺省配置生成即可

2.3.3 启动服务器

生成的均密钥存放于 OpenVPN\easy-rsa\keys 目录下

将生成的证书拷贝到 OpenVPN\config 目录下

将 OpenVPN\sample-config 下的服务器配置文件拷贝到 OpenVPN\config 目录下

启动 OpenVPN 应用程序即可

2.4 服务器端配置

在 OpenVPN 的安装目录下，使用 notepad++ 打开 server.ovpn 或者 server.conf 文件查看服务器端文件示例如下:

```
port 1194        #这个端口是 IANA 为 OpenVPN 分配的指定端口，可以根据需要自行修改
proto udp        #可以选用 tcp
dev tun
ca ca.crt
cert server.crt
key server.key
dh dh1024.pem
server 10.8.0.0 255.255.255.0  #  虚拟局域网网段设置，请根据需要自行修改
ifconfig-pool-persist ipp.txt
keepalive 10 120
client-to-client
comp-lzo
max-clients 100
persist-key
persist-tun
status openvpn-status.log
verb 3
```

3 客户端使用与配置

3.1 客户端配置

这里的客户端针对的是我们支持 OpenVPN 的设备，为了让我们的话机能够连接到 OpenVPN 服务器,我们需要证书文件。

首先需要针对客户端的配置文件 client.ovpn 或者 client.conf 进行编辑修改，客户端配置文件示例如下:

```
client
dev tun
proto udp
remote 192.168.1.135 1194          #服务器域名/IP 和端口
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
cert client.crt
key client.key
comp-lzo
verb 3
```

可以结合服务器端的配置进行相关修改。

其次将我们之前制作好的客户端文件 ca.crt、client.crt、client.key 导出来在话机升级时使用。

3.2 话机使用 OpenVPN

登陆话机网页，依次点击网络->VPN，在 OpenVPN 文件栏逐个升级 client.ovpn, client.key, client.crt, ca.crt。升级完成后，OpenVPN 文件栏会有升级进入的证书文件大小显示，如下所示

3.3 开启 VPN NAT

使用方法：

话机导入 vpn 证书，开启 Enable VPN 和 Enable NAT，PC（网关需要设置为话机的 ip）连接话机 lan 口，此时 PC 能够访问话机的 VPN。

PC ping 10.8.0.10 可以 ping 通，ping www.baidu.com 也可以 ping 通（10.8.0.10 是 VPN IP 地址）

```
client
dev tun
proto udp
remote 47.93.201.71 1194
resolv-retry infinite
nobind
ca ca.crt
cert client.crt
key client.key
status /mnt/openvpn-status.log
comp-lzo
verb 3
```