

openvpn简易安装脚本-江哥架构师笔记

昨天大数据部门过来让我帮他们搭建一个vpn环境，于是拿出我写好的脚本，三五分钟帮他搭建完成，效率杠杠滴。

openvpn需求常见

有时候在家，却要访问公司内部网络 ==>在入口机器做server端

公司的云服务器只能从公司的ip访问，我需要在家访问 ==>公司服务器入口或者跳板上起一个server端，云上内网机器安装client端

把家里的虚拟机，和其他网络的内网机器打通 ==>中间要借助有外网ip的机器做server端，家里的机器和其他内网机做client端

今天的需求是：云服务器不能开放外网web端口(8080)，在公司要访问云内的10.x.x.x的私网地址的(8080端口)

程序组成

其中包括：

一个openvpn的源码压缩包

一个easy-rsa 2版本的加密用的包

一个openvpn脚本安装包 (v4.0版本)

一个openvpn客户端证书生成包 (v2.0版本)

下载地址 注：只支持centos版本



[openvpn-package-sh-v4.zip \(https://andblog.cn/files/20180829-7276301059.zip\)](https://andblog.cn/files/20180829-7276301059.zip)

openvpn_install.sh 脚本使用方法

将压缩包上传至服务器，解压，进入解压目录运行

```
]# bash openvpn_install.sh -o openvpn-2.3.17.tar.gz -e easy-rsa-2.2.0.zip
```

运行过程如图，按照提示输入信息

```
[root@zheng openvpn]# ll
total 1348
-rw-r--r-- 1 root root 58487 Nov 27 2017 easy-rsa-2.2.0.zip
-rw-r--r-- 1 root root 1292639 Nov 27 2017 openvpn-2.3.17.tar.gz
-rw-r--r-- 1 root root 4852 Jun 15 18:21 openvpn_create_client_certificate.sh
-rw-r--r-- 1 root root 15770 Jul 9 11:15 openvpn_install.sh
[root@zheng openvpn]# bash openvpn_install.sh -o openvpn-2.3.17.tar.gz -e easy-rsa-2.2.0.zip
[root@zheng openvpn]# bash openvpn_install.sh -o openvpn-2.3.17.tar.gz -e easy-rsa-2.2.0.zip
安装软件包: lzo-devel pam-devel expect ,若安装失败请检查网络连接和yum源配置
yum -y install lzo-devel pam-devel expect [ OK ]
解压 easy-rsa-2.2.0.zip [ OK ]
解压 openvpn-2.3.17.tar.gz [ OK ]

是否需要手动输入创建证书的详细信息，直接回车为不输入,键入(yes/no):
国家(countryName): cn
省份(provinceName): sh
城市(city): sh
公司(org): ali
邮箱(email): ali@ali.com
部门(section): it
名字(name): kk
唯一证书名(commonName): CA

CA证书生成 [ OK ]

输入服务器证书名(需唯一): server 证书名不要和唯一证书名CA相同即可
输入服务器证书密码(可为空):
Server 证书生成 [ OK ]

执行 ./configure --prefix=/usr/local/openvpn-2.3.17/ [ OK ]
执行 make [ OK ]
执行 make install [ OK ]
安装目录为 /usr/local/openvpn-2.3.17/ [ OK ]

生成迪菲-赫尔曼交换密钥 [ OK ]

本机地址如下:
1: lo: inet 127.0.0.1/8
2: eth0: inet 172.16.43.59/18
3: docker0: inet 172.17.0.1/16
7: vetha77dd71@if6:
输入服务端监听的ip地址: 47.106.175.98 若在云主机环境上搭建，应该填写云主机外网IP地址
Warning: 该地址不在本机网卡配置上，将默认监听本机所有地址 0.0.0.0

指定虚拟局域网占用的IP地址段和子网掩码:
例(10.0.0.0 255.255.255.0): 10.7.7.0 255.255.255.0 设置一个不和本地网络冲突的网段地址
```

```

指定虚拟局域网占用的IP地址段和子网掩码:
例(10.0.0.0 255.255.255.0): 10.7.7.0 255.255.255.0

是否需要设置客户端默认路由走openvpn网络, 直接回车为不设置, 键入(yes/no):
是否需要给客户端推送静态路由, 访问指定的网络号时走openvpn网络, 直接回车为不设置, 键入(yes/no): yes
输入静态路由的网络号和子网掩码(例: 172.16.0.0 255.255.0.0): 172.16.0.0 255.255.0.0
客户端推送静态路由 [ OK ]

是否需要开启客户端密码认证, 直接回车为不设置, 键入(yes/no): yes
开启客户端密码认证 [ OK ]

开启ip_forward转发 [ OK ]

请手动执行NAT规则: iptables -t nat -A POSTROUTING -s 10.7.7.0/24 -j SNAT --to-source 本机上网IP
账号密码配置文件为: /usr/local/openvpn-2.3.17/psw-file
测试账户和密码为: vpnTest openvpntest2018

安装配置openvpn服务端 [ OK ]

启动方法: cd /usr/local/openvpn-2.3.17/config ; /usr/local/openvpn-2.3.17/sbin/openvpn server.conf &

创建客户端证书脚本路径为: /usr/local/openvpn-2.3.17/openvpn_create_client_certificate.sh
[root@zheng openvpn]# iptables -t nat -A POSTROUTING -s 10.7.7.0/24 -j SNAT --to-source 47.106.175.98
[root@zheng openvpn]# cd /usr/local/

```

云服务器上的外网地址可能并没有配置在本地网卡上，需要填写云服务器外网IP地址

执行这条iptables才能让客户端能直接连接server端的局域网IP

服务端的启动方法注意要进入config目录，以相对路径启动。如图所示

openvpn_create_client_certificate.sh 脚本使用方法

此脚本用来生成客户端证书，安装好服务端后，这个脚本位于/usr/local/openvpn-xxx/目录下

生成客户端证书如下，运行脚本时需要指定客户端证书输出路径，本例为/tmp

```

[root@zheng openvpn]# cd /usr/local/
[root@zheng local]# ll
total 60
drwxr-xr-x. 6 root root 4096 Jun 28 14:09 aegis
drwxr-xr-x. 2 root root 4096 Nov 5 2016 bin
drwxr-xr-x. 10 root root 4096 Jun 21 16:56 cloudmonitor
drwxr-xr-x. 2 root root 4096 Nov 5 2016 etc
drwxr-xr-x. 2 root root 4096 Nov 5 2016 games
drwxr-xr-x. 2 root root 4096 Nov 5 2016 include
drwxr-xr-x. 2 root root 4096 Nov 5 2016 lib
drwxr-xr-x. 2 root root 4096 Nov 5 2016 lib64
drwxr-xr-x. 2 root root 4096 Nov 5 2016 libexec
drwxrwxr-x. 7 500 500 4096 Jun 30 23:07 node-v8.11.3-linux-x64
drwxr-xr-x. 8 root root 4096 Jul 9 11:21 openvpn-2.3.17
drwxrwsr-x. 25 root rvm 4096 Jun 29 11:24 rvm
drwxr-xr-x. 2 root root 4096 Nov 5 2016 sbin
drwxr-xr-x. 7 root root 4096 Jun 29 11:01 share
drwxr-xr-x. 2 root root 4096 Nov 5 2016 src
[root@zheng local]# cd openvpn-2.3.17/
[root@zheng openvpn-2.3.17]# ll
total 40
-rwxr--r-- 1 root root 1221 Jul 9 11:21 checkpsw.sh
drwxr-xr-x 2 root root 4096 Jul 9 11:20 config
drwxr-xr-x 5 root root 4096 Jul 9 11:19 easy-rsa
drwxr-xr-x 2 root root 4096 Jul 9 11:19 include
drwxr-xr-x 3 root root 4096 Jul 9 11:19 lib
-rw-r--r-- 1 root root 4852 Jul 9 11:21 openvpn_create_client_certificate.sh
-rw-r--r-- 1 root root 24 Jul 9 11:21 psw-file
drwxr-xr-x 2 root root 4096 Jul 9 11:19 sbin
drwxr-xr-x 4 root root 4096 Jul 9 11:19 share
[root@zheng openvpn-2.3.17]# bash openvpn_create_client_certificate.sh /tmp
运行脚本并指定客户端证书输出路径
输入客户端证书名(需唯一): kk 输入客户端证书名不要和前面的CA证书名或服务端证书名一样即可
输入客户端证书密码(可为空):
客户端证书生成 [ OK ]

client.conf listen remote 47.106.175.98 客户端连接服务端的地址

客户端文件创建于/tmp/openvpn_client_kk/ [ OK ]

linux启动方法 cd /tmp/openvpn_client_kk/config ; /tmp/openvpn_client_kk/sbin/openvpn server.conf &

windows请将/tmp/openvpn_client_kk/kk-windows-config.tar.gz解压，将其中config目录覆盖openvpn安装目录的config目录

```

linux客户端将客户端文件目录拷贝至对应主机，cd到该目录中，使用相对路径指定配置文件启动即可

windows客户端先安装 windows版openvpn安装包，再下载生成的客户端证书.tar.gz压缩包到windows，解压将里面的config目录替换openvpn安装路径下的config目录

测试ping 云服务器局域网IP

```
命令提示符
无
C:\Users\cej>ping 10.10.163.20
正在 Ping 10.10.163.20 具有 32 字节的数据:
来自 10.10.163.20 的回复: 字节=32 时间=35ms TTL=63
来自 10.10.163.20 的回复: 字节=32 时间=34ms TTL=63
10.10.163.20 的 Ping 统计信息:
    数据包: 已发送 = 2, 已接收 = 2, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 34ms, 最长 = 35ms, 平均 = 34ms
Control-C
^C
C:\Users\cej>ping 10.10.88.9
正在 Ping 10.10.88.9 具有 32 字节的数据:
来自 10.10.88.9 的回复: 字节=32 时间=86ms TTL=63
来自 10.10.88.9 的回复: 字节=32 时间=32ms TTL=63
来自 10.10.88.9 的回复: 字节=32 时间=32ms TTL=63
10.10.88.9 的 Ping 统计信息:
    数据包: 已发送 = 3, 已接收 = 3, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 32ms, 最长 = 86ms, 平均 = 50ms
Control-C
^C
C:\Users\cej>
```

路由环境分析

此脚本中有两个选择项，一是让所有网络都走openvpn，这样网络出口相当于使用了云服务器的IP出口了，连接openvpn之后，上网IP为服务器IP

二是部分网络走openvpn，此时可以达到访问云服务器内部局域网的特性

扩展配置选项

路由：

服务端推送路由规则：

```
push "route 10.0.0.0 255.0.0.0 vpn_gateway" #vpn网关
```

```
push "route 10.0.0.0 255.0.0.0 net_gateway" #本地net上网网关
```

客户端：

```
route 10.0.0.0 255.0.0.0 vpn_gateway #vpn网关
```

```
route 10.0.0.0 255.0.0.0 net_gateway #本地net上网网关
```

固定客户端IP地址

```
client-config-dir /etc/openvpn/ccd #ccd目录下对应的文件名为客户端  
证书名
```

```
/etc/openvpn/ccd/client1: ifconfig-push 10.8.0.2 10.8.0.3
```

ifconfig-push 后面是紧跟着两个连续的成组IP地址，以第一个为客户端的IP地址

其他：

```
duplicate-cn #允许一个客户端证书同时被多个终端使用
```

```
max-clients 1000 #客户端链接最大数量
```

参考文档：<http://www.kkwen.cn/index.php/archives/24/>