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机上起一个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)

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

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

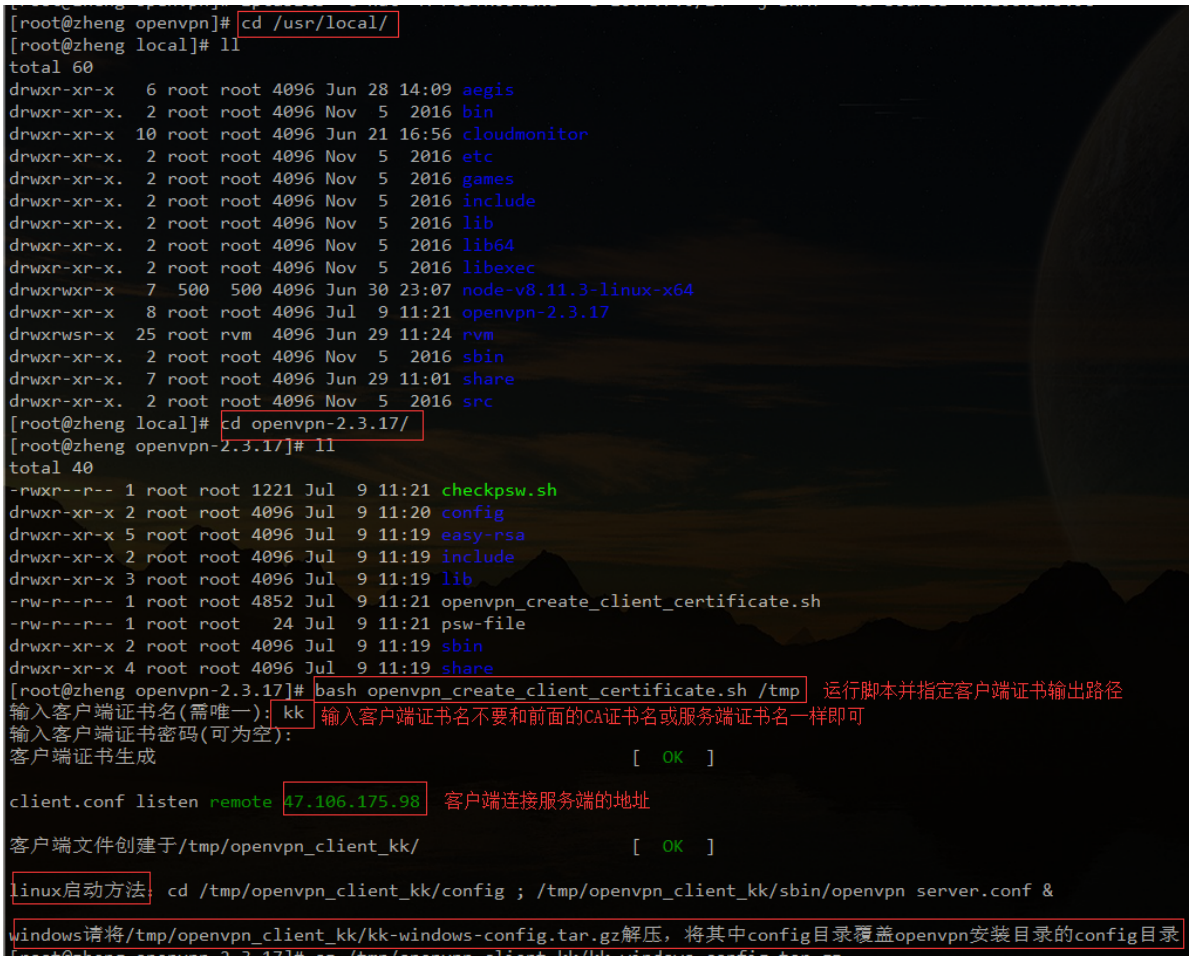
执行这条iptables才能让客户端能直接连接server端的局域网IP

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

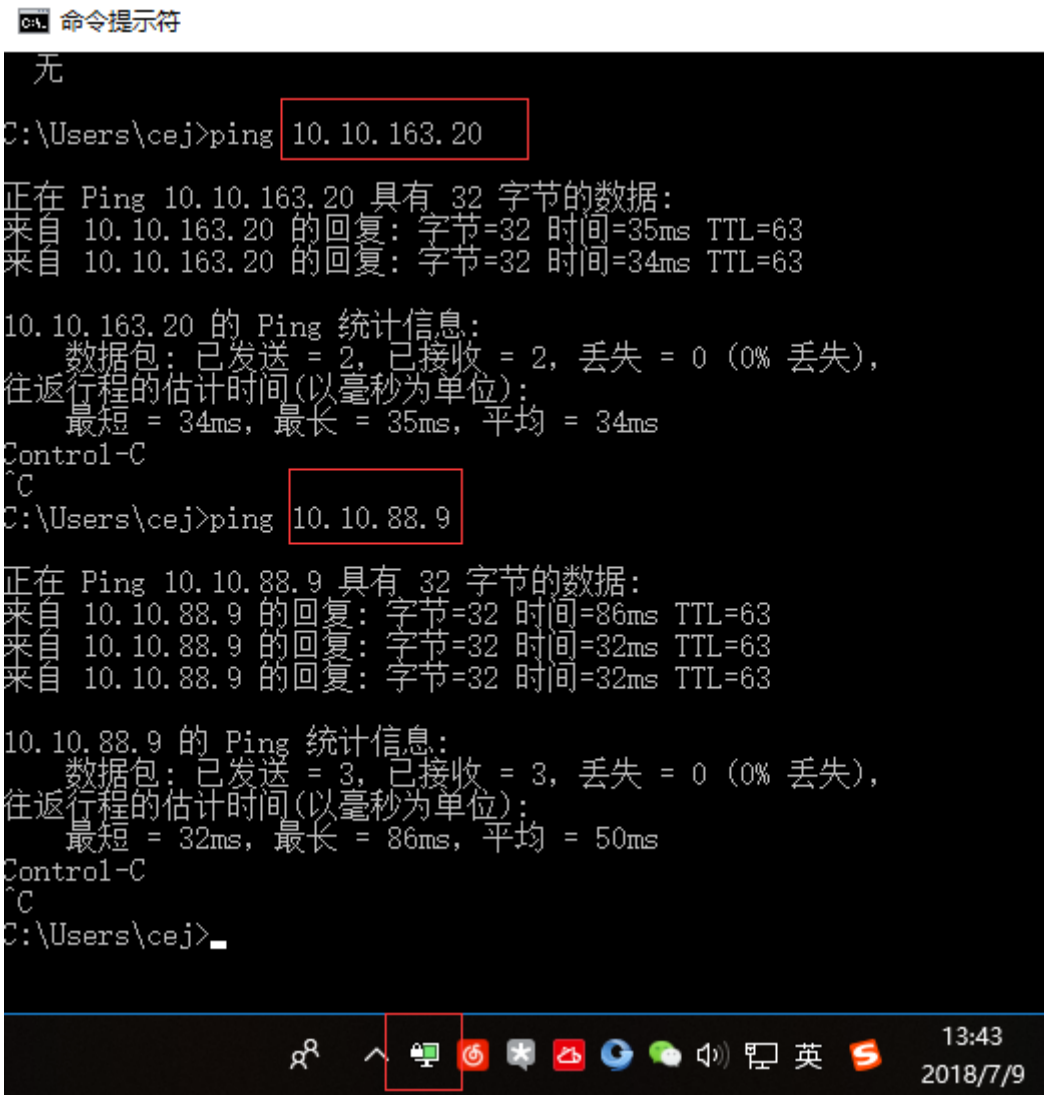
生成客户端证书如下，运行脚本时需要指定客户端证书输出路径，本例为/tmp



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



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 #cdd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地扯，以第一个为客户端的IP地扯

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/