鉴于公司现有 VPN 太坑，每次连接之后得做一些奇怪的配置才能访问外网，很麻烦，于是准备换了他，现有的是在路由上做的，这次准备用 CentOS7.4 来做一个 openvpn，不用 Debian 了，琢磨一下 CentOS 系列的，仔细的想了一下，需求有两个，一是能访问公司内部的服务器，这个是必须的，第二个就是连接 VPN 之后外网 IP 也要变成公司的，因为机房的防火墙对于 22/3389 端口有限制，只能是公司的 IP 才能去连接，就酱紫，使用 CentOS7.4X64 系统，开撸开撸。

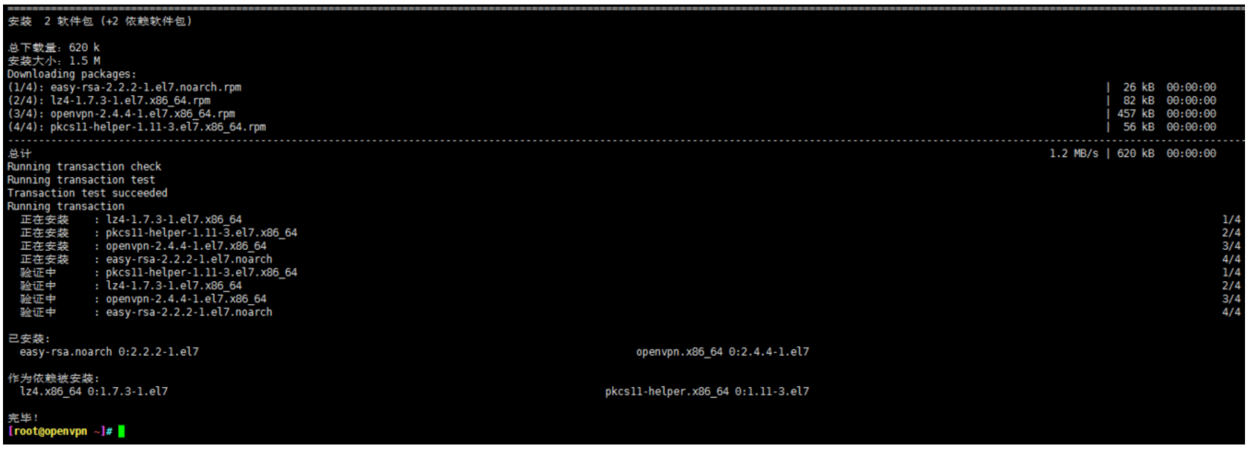
安装阶段

1. 添加源

```
[root@openvpn ~]# mv /etc/yum.repos.d/CentOS-Base.repo /etc/yum.repos.d/CentOS-Base.repo.backup
[root@openvpn ~]# wget -O /etc/yum.repos.d/CentOS-Base.repo http://mirrors.aliyun.com/repo/Centos-7.repo
[root@openvpn ~]# mv /etc/yum.repos.d/epel.repo /etc/yum.repos.d/epel.repo.backup
[root@openvpn ~]# mv /etc/yum.repos.d/epel-testing.repo /etc/yum.repos.d/epel-testing.repo.backup
[root@openvpn ~]# wget -O /etc/yum.repos.d/epel.repo http://mirrors.aliyun.com/repo/epel-7.repo
```

2. 安装 openvpn

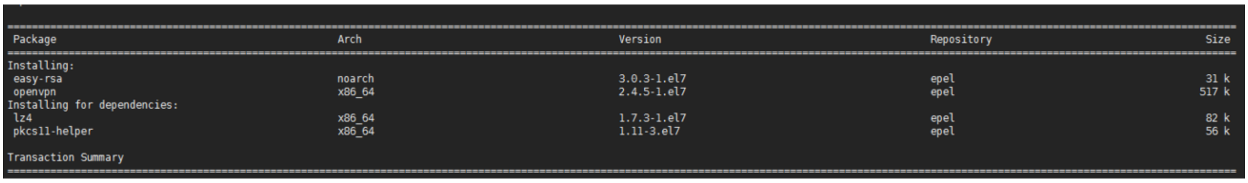
```
[root@openvpn ~]# yum -y install openvpn easy-rsa
```



```
安装  2 软件包 (+2 依赖软件包)

总下载量：620 k
安装大小：1.5 M
Downloading packages:
(1/4): easy-rsa-2.2.2-1.el7.noarch.rpm                                   |  26 kB  00:00:00
(2/4): lz4-1.7.3-1.el7.x86_64.rpm                                        |  82 kB  00:00:00
(3/4): openvpn-2.4.4-1.el7.x86_64.rpm                                    | 457 kB  00:00:00
(4/4): pkcs11-helper-1.11-3.el7.x86_64.rpm                               |  56 kB  00:00:00
------------------------------------------------------------------------------------------------
总计                                                           1.2 MB/s | 620 kB  00:00:00
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  正在安装    : lz4-1.7.3-1.el7.x86_64                                                      1/4
  正在安装    : pkcs11-helper-1.11-3.el7.x86_64                                             2/4
  正在安装    : openvpn-2.4.4-1.el7.x86_64                                                  3/4
  正在安装    : easy-rsa-2.2.2-1.el7.noarch                                                 4/4
  验证中      : pkcs11-helper-1.11-3.el7.x86_64                                             1/4
  验证中      : lz4-1.7.3-1.el7.x86_64                                                      2/4
  验证中      : openvpn-2.4.4-1.el7.x86_64                                                  3/4
  验证中      : easy-rsa-2.2.2-1.el7.noarch                                                 4/4

已安装:
  easy-rsa.noarch 0:2.2.2-1.el7                        openvpn.x86_64 0:2.4.4-1.el7

作为依赖被安装:
  lz4.x86_64 0:1.7.3-1.el7                           pkcs11-helper.x86_64 0:1.11-3.el7

完毕！
[root@openvpn ~]# 
```

生成 openvpn 必备文件

如果你安装的 easy-rsa-3.0 的版本，生成证书步骤请参考这里，2.2 的请继续向下走，判断安装的 easy-rsa 版本看下图。



```
================================================================================================
 Package                 Arch               Version                  Repository            Size
================================================================================================
Installing:
 easy-rsa                noarch             3.0.3-1.el7              epel                 31 k
 openvpn                 x86_64             2.4.5-1.el7              epel                517 k
Installing for dependencies:
 lz4                     x86_64             1.7.3-1.el7              epel                 82 k
 pkcs11-helper           x86_64             1.11-3.el7               epel                 56 k

Transaction Summary
================================================================================================
```

1. 生成证书

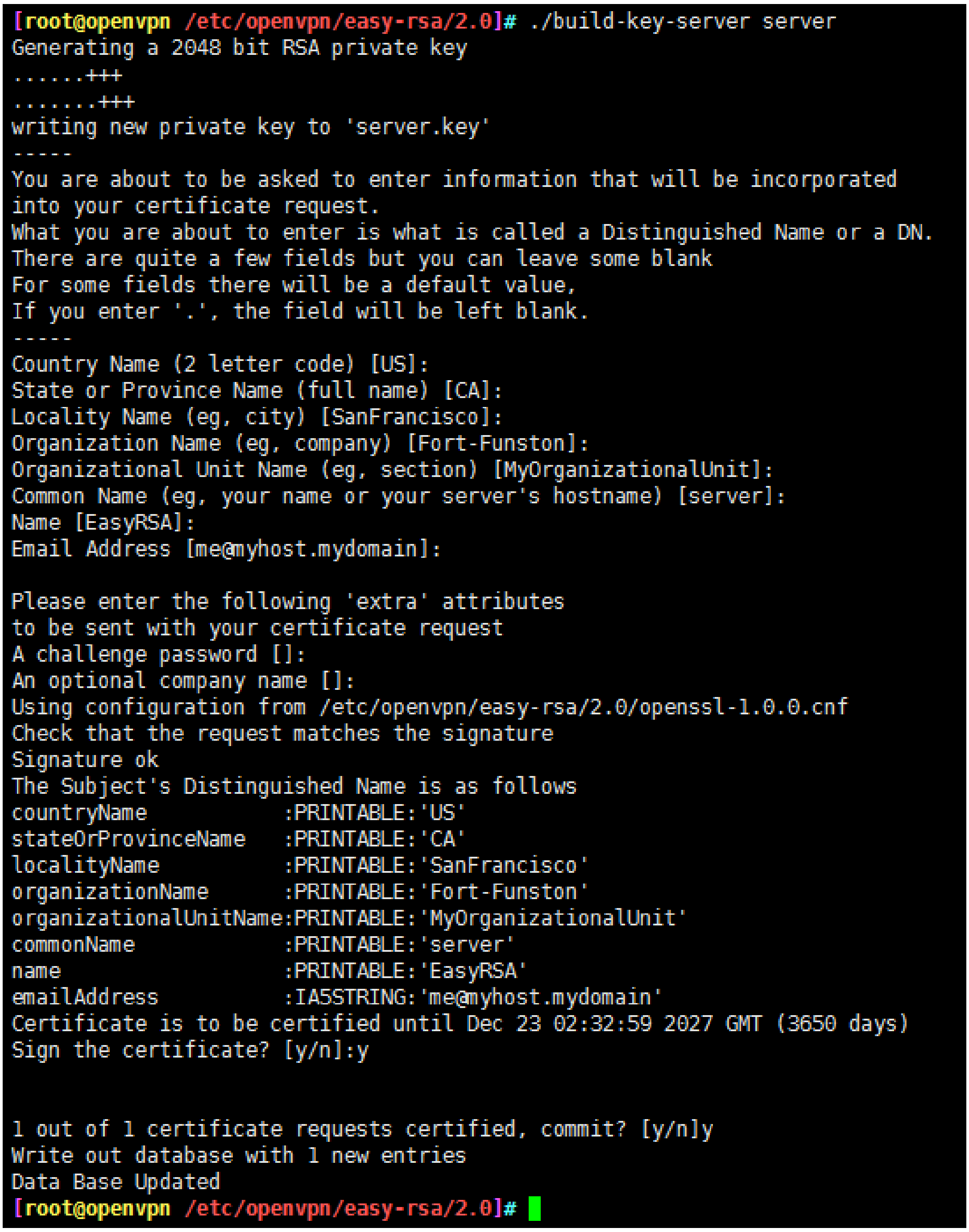
```
[root@openvpn ~]# cp -r /usr/share/easy-rsa/ /etc/openvpn/
[root@openvpn ~]# cd /etc/openvpn/easy-rsa/2.0/
[root@openvpn /etc/openvpn/easy-rsa/2.0]# source vars
NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/openvpn/easy-r
sa/2.0/keys
[root@openvpn /etc/openvpn/easy-rsa/2.0]# ./clean-all
[root@openvpn /etc/openvpn/easy-rsa/2.0]# ./build-ca
```

一路回车 y 即可

2. 生成服务器端证书和秘钥

```
[root@openvpn /etc/openvpn/easy-rsa/2.0]# ./build-key-server server
```

一路回车 Y 即可。

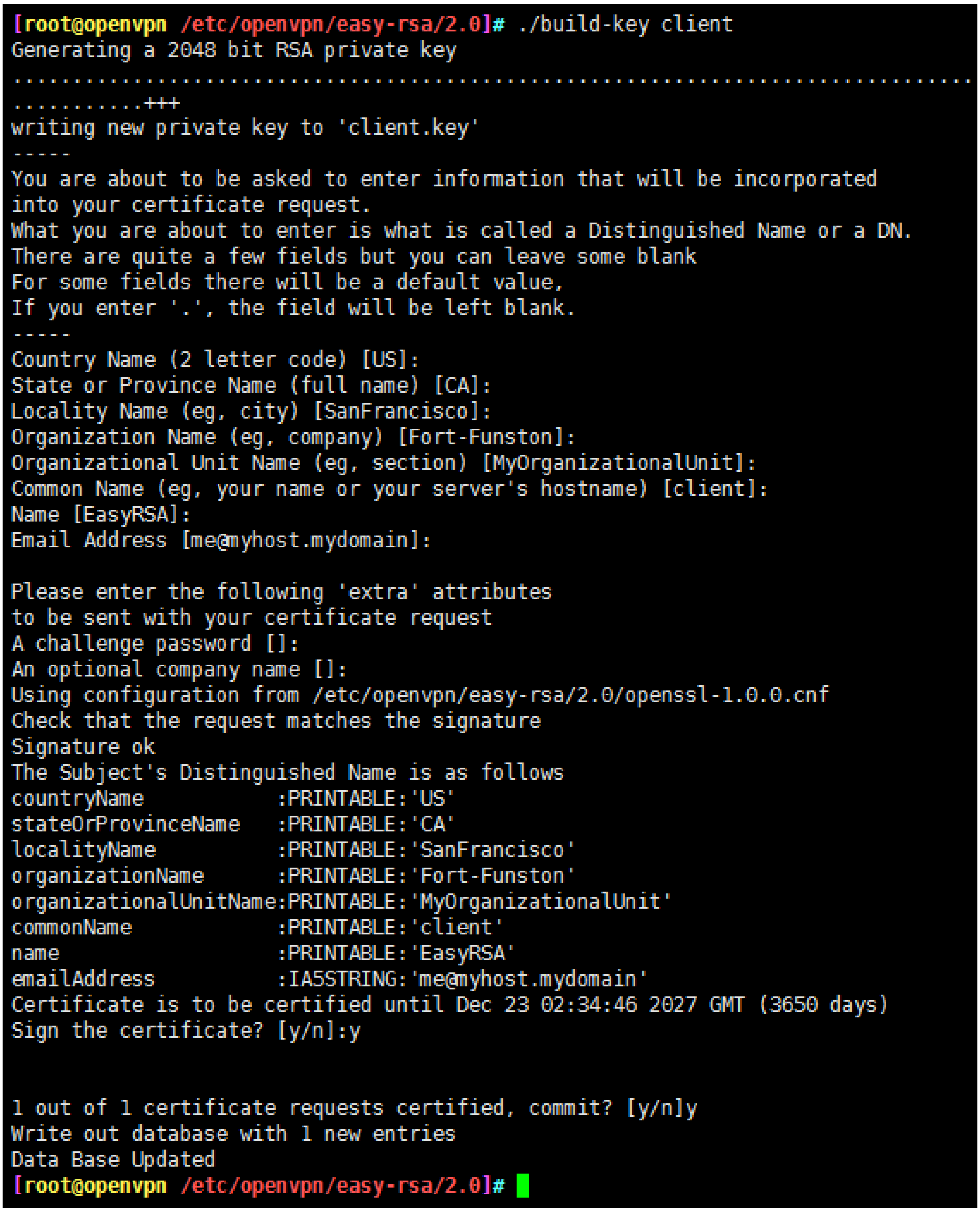


```
[root@openvpn /etc/openvpn/easy-rsa/2.0]# ./build-key-server server
Generating a 2048 bit RSA private key
......+++
.......+++
writing new private key to 'server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to 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]:
State or Province Name (full name) [CA]:
Locality Name (eg, city) [SanFrancisco]:
Organization Name (eg, company) [Fort-Funston]:
Organizational Unit Name (eg, section) [MyOrganizationalUnit]:
Common Name (eg, your name or your server's hostname) [server]:
Name [EasyRSA]:
Email Address [me@myhost.mydomain]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /etc/openvpn/easy-rsa/2.0/openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'US'
stateOrProvinceName   :PRINTABLE:'CA'
localityName          :PRINTABLE:'SanFrancisco'
organizationName      :PRINTABLE:'Fort-Funston'
organizationalUnitName:PRINTABLE:'MyOrganizationalUnit'
commonName            :PRINTABLE:'server'
name                  :PRINTABLE:'EasyRSA'
emailAddress          :IA5STRING:'me@myhost.mydomain'
Certificate is to be certified until Dec 23 02:32:59 2027 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
[root@openvpn /etc/openvpn/easy-rsa/2.0]#
```

3. 生成客户端证书和密钥

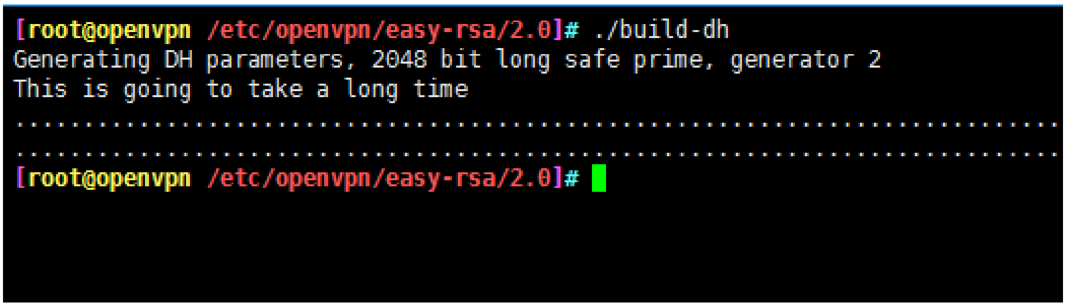
```
[root@openvpn /etc/openvpn/easy-rsa/2.0]# ./build-key client
```

一路回车 Y



```
[root@openvpn /etc/openvpn/easy-rsa/2.0]# ./build-key client
Generating a 2048 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]:
State or Province Name (full name) [CA]:
Locality Name (eg, city) [SanFrancisco]:
Organization Name (eg, company) [Fort-Funston]:
Organizational Unit Name (eg, section) [MyOrganizationalUnit]:
Common Name (eg, your name or your server's hostname) [client]:
Name [EasyRSA]:
Email Address [me@myhost.mydomain]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /etc/openvpn/easy-rsa/2.0/openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'US'
stateOrProvinceName   :PRINTABLE:'CA'
localityName          :PRINTABLE:'SanFrancisco'
organizationName      :PRINTABLE:'Fort-Funston'
organizationalUnitName:PRINTABLE:'MyOrganizationalUnit'
commonName            :PRINTABLE:'client'
name                  :PRINTABLE:'EasyRSA'
emailAddress          :IA5STRING:'me@myhost.mydomain'
Certificate is to be certified until Dec 23 02:34:46 2027 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
[root@openvpn /etc/openvpn/easy-rsa/2.0]#
```

4. 生成 Diffie Hellman 参数



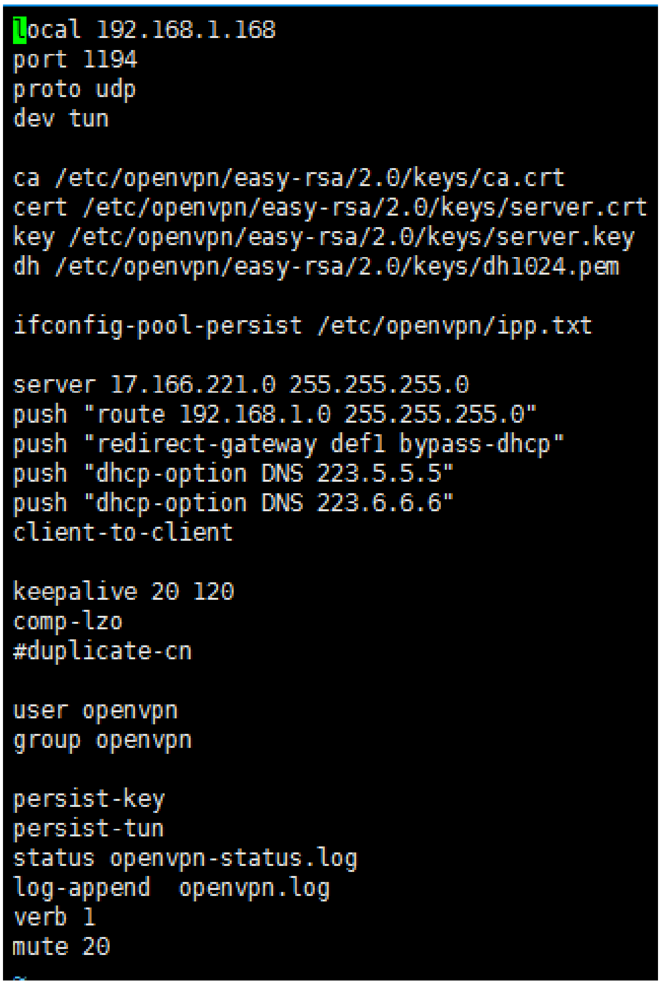
```
[root@openvpn /etc/openvpn/easy-rsa/2.0]# ./build-dh
Generating DH parameters, 2048 bit long safe prime, generator 2
This is going to take a long time
.............................................................................
.............................................................................
[root@openvpn /etc/openvpn/easy-rsa/2.0]#
```

该生成的都生成了，下面开始编写配置文件

配置 OpenVPN 服务器端文件

编辑 /etc/openvpn/server.conf 文件，没有就手动创建，我的配置文件如下。如果是云服务器，尽量不要使用 upd 协议和 1194 端口，因为在国内很多接入商都不允许，导致 1194 端被封不能用。当然你也可以试一下，如果被封了就换一下。

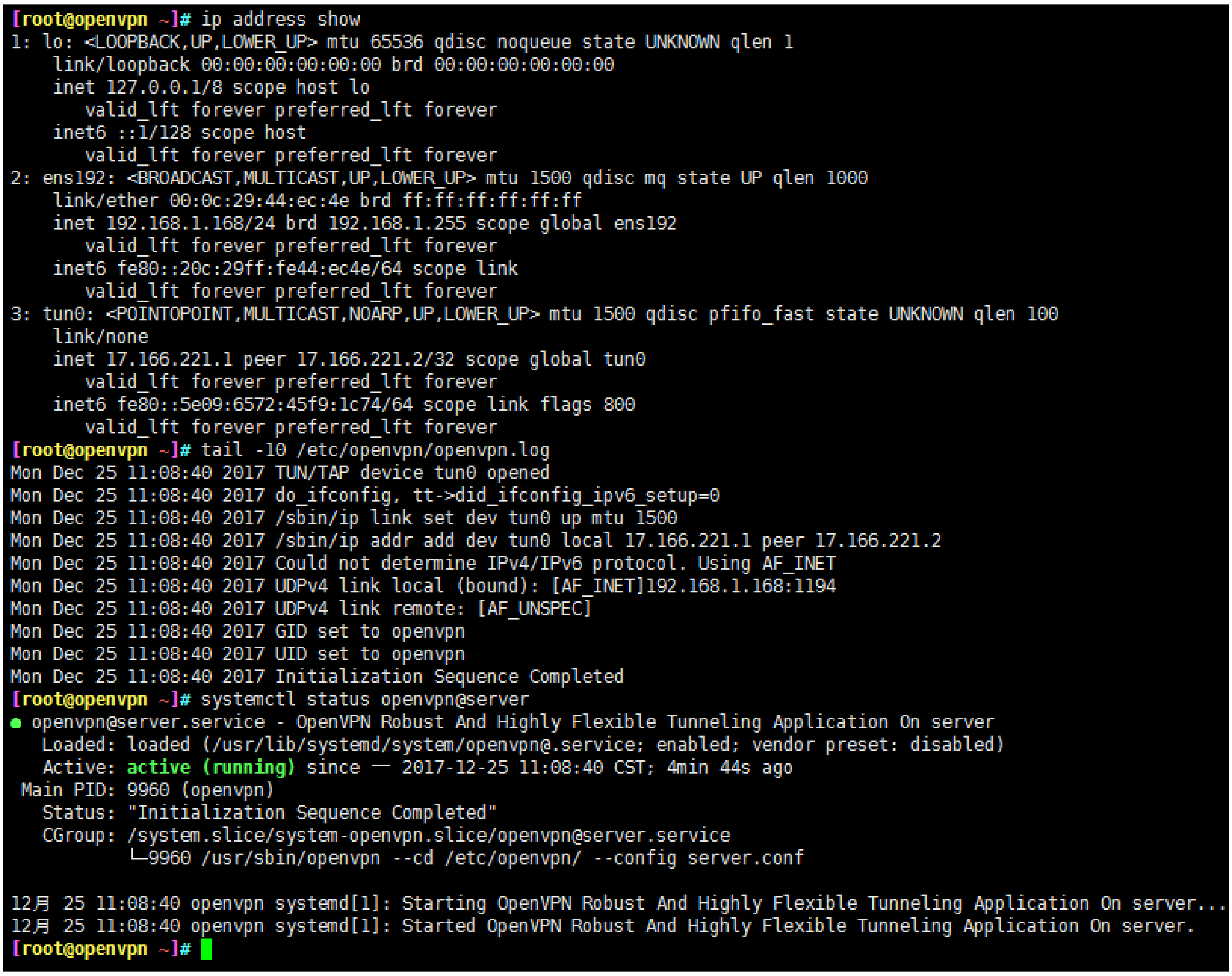
```
local 192.168.1.168   #服务器IP
port 1194             #占用端口
proto udp             #使用udp协议
dev tun               #使用tun模式，也可以使用tap

ca /etc/openvpn/easy-rsa/2.0/keys/ca.crt
cert /etc/openvpn/easy-rsa/2.0/keys/server.crt
key /etc/openvpn/easy-rsa/2.0/keys/server.key
dh /etc/openvpn/easy-rsa/2.0/keys/dh2048.pem        #指定证书位置

ifconfig-pool-persist /etc/openvpn/ipp.txt          #存放每个人使用的IP

server 17.166.221.0 255.255.255.0                   #客户端DHCP
push "route 192.168.1.0 255.255.255.0"               #VPN访问网段，我的内网是19
2.168.1.0网段
push "redirect-gateway def1 bypass-dhcp"             #所有流量都走VPN，如果不需
要将下三行去掉
push "dhcp-option DNS 223.5.5.5"                    #DNS1
push "dhcp-option DNS 223.6.6.6"                    #DNS2
client-to-client                                    #允许客户端之间互通

keepalive 20 120                                    #保持连接时间
comp-lzo                                            #开启vpn压缩
#duplicate-cn                                       #允许多人使用同一个证书连接V
PN，不建议使用，注释状态

user openvpn                                        #运行用户
group openvpn                                       #运行组

persist-key
persist-tun
status openvpn-status.log
log-append  openvpn.log
verb 1                                               #日志级别0-9，等级越高，记
录越多
mute 20
```



```
local 192.168.1.168
port 1194
proto udp
dev tun

ca /etc/openvpn/easy-rsa/2.0/keys/ca.crt
cert /etc/openvpn/easy-rsa/2.0/keys/server.crt
key /etc/openvpn/easy-rsa/2.0/keys/server.key
dh /etc/openvpn/easy-rsa/2.0/keys/dh1024.pem

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

server 17.166.221.0 255.255.255.0
push "route 192.168.1.0 255.255.255.0"
push "redirect-gateway def1 bypass-dhcp"
push "dhcp-option DNS 223.5.5.5"
push "dhcp-option DNS 223.6.6.6"
client-to-client

keepalive 20 120
comp-lzo
#duplicate-cn

user openvpn
group openvpn

persist-key
persist-tun
status openvpn-status.log
log-append  openvpn.log
verb 1
mute 20
```

启动 openvpn，看状态。

```
[root@openvpn ~]# systemctl start openvpn@server
[root@openvpn ~]# systemctl enable openvpn@server
Created symlink from /etc/systemd/system/multi-user.target.wants/openvpn@serv
er.service to /usr/lib/systemd/system/openvpn@.service.
```



```
[root@openvpn ~]# ip address show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
    link/ether 00:0c:29:44:ec:4e brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.168/24 brd 192.168.1.255 scope global ens192
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe44:ec4e/64 scope link
       valid_lft forever preferred_lft forever
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN qlen 100
    link/none
    inet 17.166.221.1 peer 17.166.221.2/32 scope global tun0
       valid_lft forever preferred_lft forever
    inet6 fe80::5e09:6572:45f9:1c74/64 scope link flags 800
       valid_lft forever preferred_lft forever
[root@openvpn ~]# tail -10 /etc/openvpn/openvpn.log
Mon Dec 25 11:08:40 2017 TUN/TAP device tun0 opened
Mon Dec 25 11:08:40 2017 do_ifconfig, tt->did_ifconfig_ipv6_setup=0
Mon Dec 25 11:08:40 2017 /sbin/ip link set dev tun0 up mtu 1500
Mon Dec 25 11:08:40 2017 /sbin/ip addr add dev tun0 local 17.166.221.1 peer 17.166.221.2
Mon Dec 25 11:08:40 2017 Could not determine IPv4/IPv6 protocol. Using AF_INET
Mon Dec 25 11:08:40 2017 UDPv4 link local (bound): [AF_INET]192.168.1.168:1194
Mon Dec 25 11:08:40 2017 UDPv4 link remote: [AF_UNSPEC]
Mon Dec 25 11:08:40 2017 GID set to openvpn
Mon Dec 25 11:08:40 2017 UID set to openvpn
Mon Dec 25 11:08:40 2017 Initialization Sequence Completed
[root@openvpn ~]# systemctl status openvpn@server
● openvpn@server.service - OpenVPN Robust And Highly Flexible Tunneling Application On server
   Loaded: loaded (/usr/lib/systemd/system/openvpn@.service; enabled; vendor preset: disabled)
   Active: active (running) since 一 2017-12-25 11:08:40 CST; 4min 44s ago
 Main PID: 9960 (openvpn)
   Status: "Initialization Sequence Completed"
   CGroup: /system.slice/system-openvpn.slice/openvpn@server.service
           └─9960 /usr/sbin/openvpn --cd /etc/openvpn/ --config server.conf

12月 25 11:08:40 openvpn systemd[1]: Starting OpenVPN Robust And Highly Flexible Tunneling Application On server...
12月 25 11:08:40 openvpn systemd[1]: Started OpenVPN Robust And Highly Flexible Tunneling Application On server.
[root@openvpn ~]# 
```

正常启动了，下面开始配置 iptables 及转发。

配置 iptables 及转发

关闭 firewall

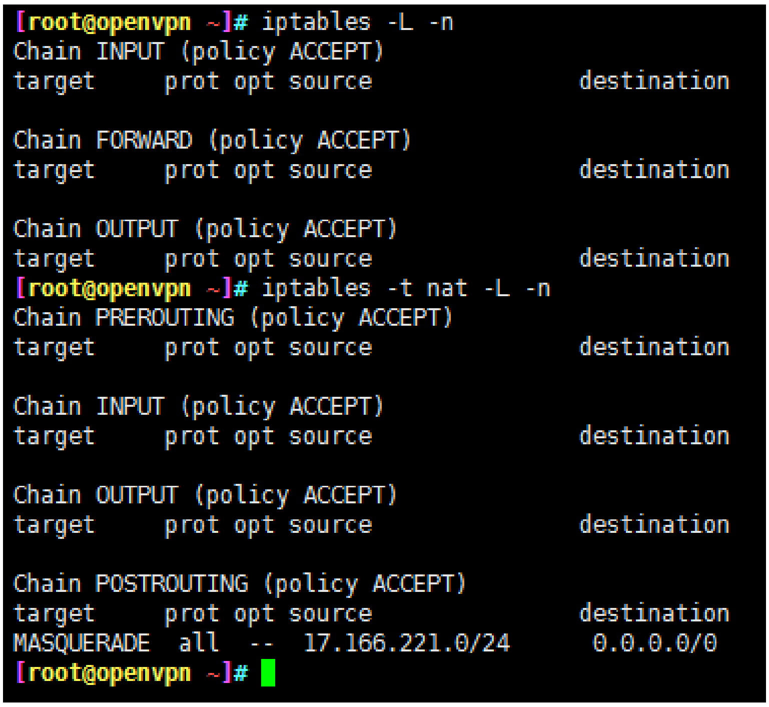
```
[root@openvpn ~]# systemctl stop firewalld.service    //停止服务
[root@openvpn ~]# systemctl disable firewalld.service //禁止开启动
[root@openvpn ~]# firewall-cmd --state                //查看状态
```

安装 iptables，写入策略

`iptables` 这里的话需要看自己的实际环境去操作，不要照搬，先说一下我这里的情况，我这个服务器是新装的，是放在公司内部的服务器，也不需要做什么端口限制和访问控制，所以我的操作如下。

```
[root@openvpn ~]# yum -y install iptables iptables-services
[root@openvpn ~]# iptables -t nat -A POSTROUTING -s 17.166.221.0/24 -o ens19
2 -j MASQUERADE   #NAT
[root@openvpn ~]# systemctl enable iptables.service
Created symlink from /etc/systemd/system/basic.target.wants/iptables.service
 to /usr/lib/systemd/system/iptables.service.
[root@openvpn ~]# systemctl start iptables.service
```

```
[root@openvpn ~]# iptables -L -n
[root@openvpn ~]# iptables -t nat -L -n
```

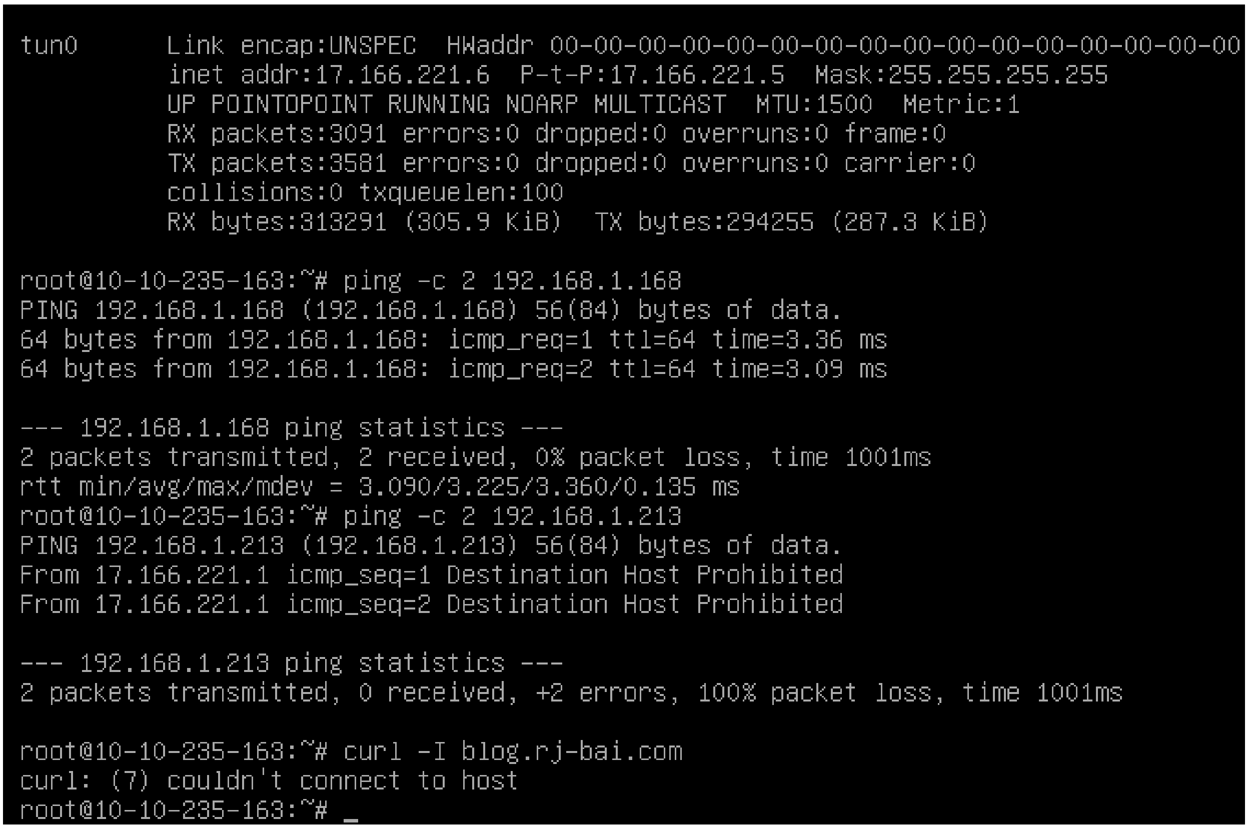


```
[root@openvpn ~]# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@openvpn ~]# iptables -t nat -L -n
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
MASQUERADE  all  --  17.166.221.0/24      0.0.0.0/0
[root@openvpn ~]#
```

我上面的操作只是单纯的添加了一个 nat，端口没做任何限制，全部开放，如果你的服务器 iptables 已经装好了，而且还有一系列的规则，你的操作就是放行 vpn 端口，添加 NAT，以上两项完成之后看一下现有的规则，看 FORWARD 链，如果发现这一个，就还需要添加 FORWARD 规则。

```
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
REJECT     all  --  0.0.0.0/0            0.0.0.0/0            reject-with icm
p-host-prohibited
```

现在是拒绝全部 FORWARD，如果不添加 FORWARD 规则，连接 vpn 之后，不会发现你的电脑断网了，只能访问到提供 vpn 服务的服务器，其他都访问不通，大概酱子。



```
tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:17.166.221.6  P-t-P:17.166.221.5  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:3091 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3581 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:313291 (305.9 KiB)  TX bytes:294255 (287.3 KiB)

root@10-10-235-163:~# ping -c 2 192.168.1.168
PING 192.168.1.168 (192.168.1.168) 56(84) bytes of data.
64 bytes from 192.168.1.168: icmp_req=1 ttl=64 time=3.36 ms
64 bytes from 192.168.1.168: icmp_req=2 ttl=64 time=3.09 ms

--- 192.168.1.168 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 3.090/3.225/3.360/0.135 ms
root@10-10-235-163:~# ping -c 2 192.168.1.213
PING 192.168.1.213 (192.168.1.213) 56(84) bytes of data.
From 17.166.221.1 icmp_seq=1 Destination Host Prohibited
From 17.166.221.1 icmp_seq=2 Destination Host Prohibited

--- 192.168.1.213 ping statistics ---
2 packets transmitted, 0 received, +2 errors, 100% packet loss, time 1001ms

root@10-10-235-163:~# curl -I blog.rj-bai.com
curl: (7) couldn't connect to host
root@10-10-235-163:~# _
```

现在这个测试服务器已经断网连不上了，我是在云后台以 `terminal` 模式连接的，这个问题的解决办法两种，第一种是编辑 `iptables` 配置文件，删除下面的规则重启 `iptables` 即可，这个比较简单。

```
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
```

第二种就是添加规则了，允许 `tun0` 网卡进行 `FORWARD`，两条规则。

```
[root@openvpn ~]# iptables -I FORWARD -i tun0 -j ACCEPT
[root@openvpn ~]# iptables -I FORWARD -m state --state ESTABLISHED,RELATED -j
ACCEPT
[root@openvpn ~]# iptables -L -n
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,E
STABLISHED
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with icm
p-host-prohibited
```

我添加的是规则，到这里 `iptables` 算是配置完成了。

开启转发

```
[root@openvpn ~]# vim /etc/sysctl.conf
net.ipv4.ip_forward = 1
[root@openvpn ~]# sysctl -p
```

服务端到此配置结束，生成证书开始连接。

客户端配置

1. 添加 openvpn 用户

使用 easy-rsa-3.0 的忽略这里撒，直接从编辑 `client.ovpn` 文件开始。

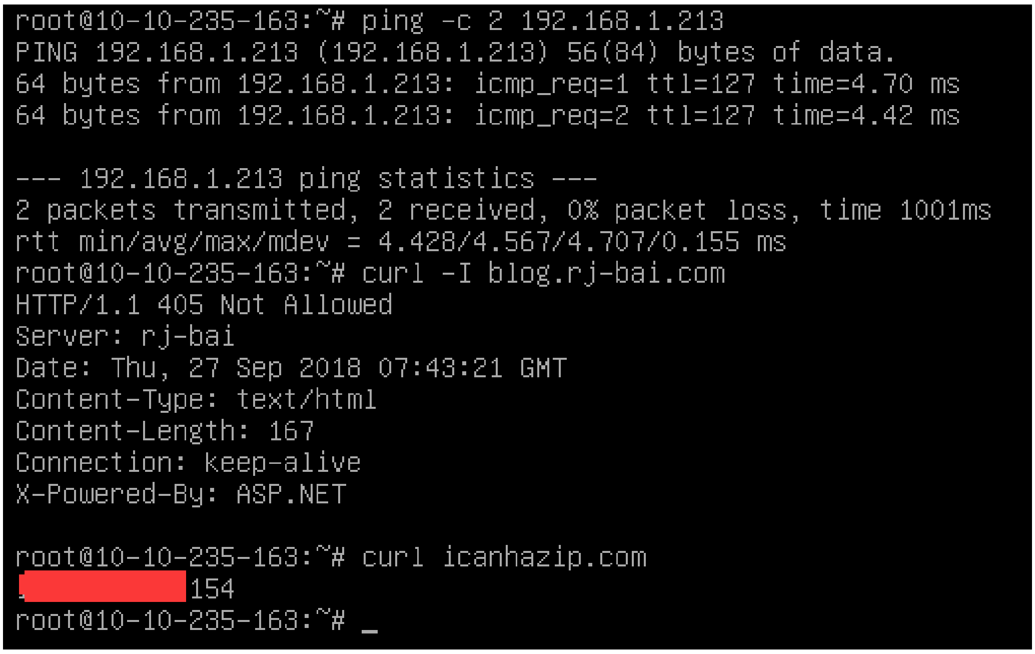
```
[root@openvpn ~]# cd /etc/openvpn/easy-rsa/2.0/
[root@openvpn /etc/openvpn/easy-rsa/2.0]# source vars
[root@openvpn /etc/openvpn/easy-rsa/2.0]# ./build-key dalin
[root@openvpn /etc/openvpn/easy-rsa/2.0]# sz keys/dalin.*   #下载用户证书文件
[root@openvpn /etc/openvpn/easy-rsa/2.0]# sz keys/ca.*      #下载CA
```

2. 编辑 client.ovpn 文件

至于客户端配置文件要怎么去写，之前写过，去这里看吧，从客户端配置第三步开始。

测试

最终效果，可以访问内部服务器，`IP` 地址变成公司的，结束。



```
root@10-10-235-163:~# ping -c 2 192.168.1.213
PING 192.168.1.213 (192.168.1.213) 56(84) bytes of data.
64 bytes from 192.168.1.213: icmp_req=1 ttl=127 time=4.70 ms
64 bytes from 192.168.1.213: icmp_req=2 ttl=127 time=4.42 ms

--- 192.168.1.213 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 4.428/4.567/4.707/0.155 ms
root@10-10-235-163:~# curl -I blog.rj-bai.com
HTTP/1.1 405 Not Allowed
Server: rj-bai
Date: Thu, 27 Sep 2018 07:43:21 GMT
Content-Type: text/html
Content-Length: 167
Connection: keep-alive
X-Powered-By: ASP.NET

root@10-10-235-163:~# curl icanhazip.com
[redacted]154
root@10-10-235-163:~# _
```

centos vpn

最后编辑于: 2019 年 01 月 02 日

返回文章列表 文章二维码 打赏