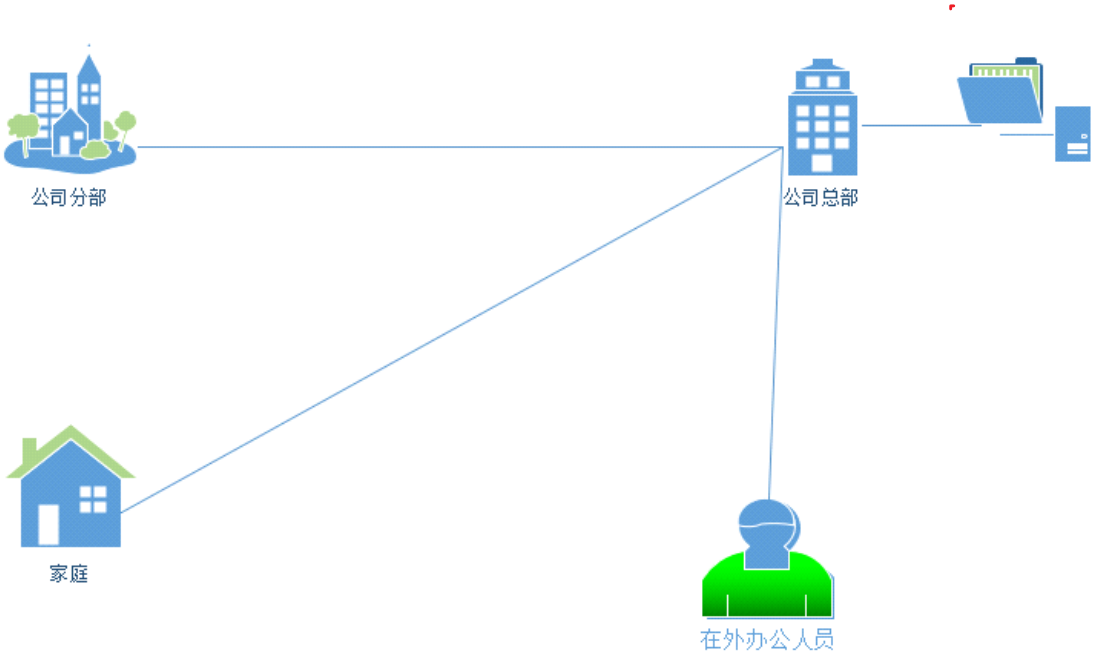
Wednesday, March 13, 2019 11:33 AM



1. 公司某重要服务器，比如ERP服务器存放在公司总部
2. 公司分部人员如何访问ERP服务器，进行办公。
3. 如果说下班时间或者国家法定假日，那些需要处理问题的人，如何连接到公司内部，进行处理问题。
4. 那些经常在外办公员，处理紧急事情，如何连到公司内部进行解决问题。

解决方案：

1. 把服务器进行网络映射到公网，这样就可以像我们访问其它网站一样进行访问。

带来问题：

1. 网络安全问题
2. 我们需要告诉他在公司内部如何连接，在公司外部如何连接。这也会增加运维员的负担。

VPN产品方案有两种：

1. 商业产品
   （1）硬件
   思科
   华为
   华三
   深信服
   （2）软件
   SoftEther VPN
   OpenVPN Acess Server :如果使用VPN人数不大于两人，是可以免费使用。大于2人，需

要购买授权。

2. 开源软件可以实现VPN

SoftEther VPN

OpenVPN 社区版，此版本是免费的。

VPN的介绍和对比

Wednesday, March 13, 2019 12:24 PM

VPN的种类：

1. PPTP

这是点到点的通信协议。

PPTP使用两个通道：

- 加密通道
- 数据连接通道

2. Ipsec

相对于PPTP安全一些。

ipsec使用两个通道：

- 加密通道
- 数据通道

3. SSL VPN:

主要用于远端访问，比如个人电脑或者出差人员。

4. OpenVPN社区版

   Openvpn使用基于虚拟网络适配器（tun或者tap设备）

   支持操作系统：

   linux各发行版：包括ubuntu,centos,redhat,debain....

   Unix：FreeBsd, Solaris, AIX

   Windows: xp, windows 7, windows 8 ,windows 10, windows server 2003....

   IOS设备： Mac

   Android: smart phone, 平板电脑

支持协议：

TCP

UDP

默认使用的是UDP协议，端口号为1194.

VPN的对比：

1. PPTP

优势：

大多数操作系统（linux,windows,安卓）几乎都 内置了这样的客户端，不需要额外 安装。

缺点： 主要是不安全。

2. Ipsec

优势：

几乎各大厂商都支持，并且很较强的扩展性。
GRE OVER IPSEC
PPTP OVER IPSEC

缺点：

难以配置和排错。
不同供应商设备如果按照默认配置，可能无法实现互通。不能够良好协同工作。

3. SSL VPN

优势： 号称无客户端的VPN，比如思科SSL VPN需要安装客户端。、Juniper VPN需要安装客户端。
一般几乎的的VPN在不安装客户端情况下，需要安装扩展包。

劣势： 几乎不支持站点到站点间的VPN。

4. OpenVPN （社区版）

优势： 简单部署，安全性相对较好（比如支持证书+用户名密码认证）

劣势： 缺乏可扩展性，并且需要客户端。几乎命令行操作，缺少良好的操作UI。

Key模式优缺点

Wednesday, March 13, 2019 1:11 PM

1. 系统环境

   服务器： centos 7.6(更新到最新版本)

   客户端：

   Linux : centos 7.6

   Windows : windows 10

2. 服务器的安装：

(1) 安装 EPEL源

[root@c720246 ~]# yum install epel*

（2）安装 openvpn

[root@c720246 ~]# yum install openvpn -y

key模式的优缺点：

优点：

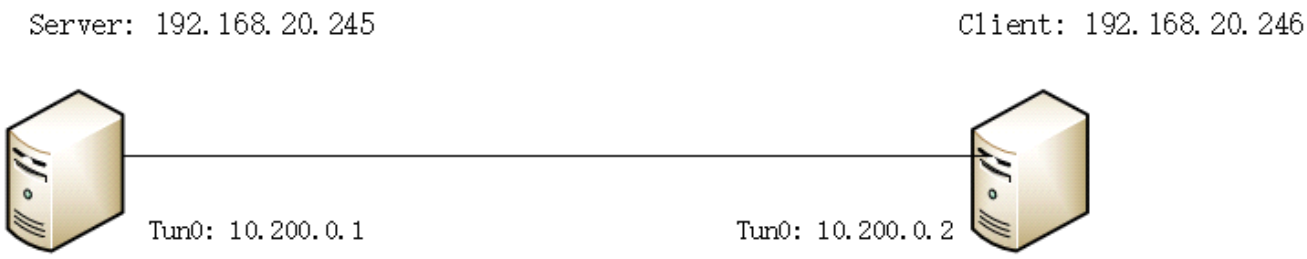
它很容易设置

不需要PKI（公共证书机构）或X509证书

缺点：

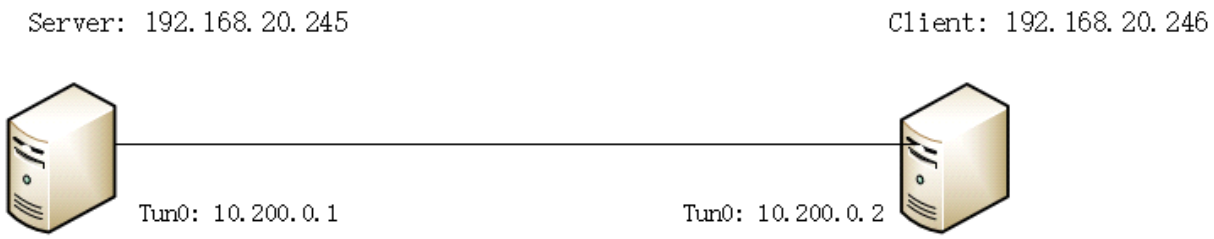
只能使用站点到站点之间，因为客户端往往不支持采用key模式，也不支持在安卓系统上。

容易带来安全性问题。



使用TCP协议和不同端口号通信

Wednesday, March 13, 2019 1:33 PM



1. 第一种方法： 使用TCP协议tun设备建立连接：

服务器端配置如下：

[root@c720245 ~]# openvpn --ifconfig 10.200.0.1 10.200.0.2 --dev tun --proto tcp-server

客户端配置如下：

[root@c720246 ~]# openvpn --ifconfig 10.200.0.2 10.200.0.1 --dev tun --proto tcp-client --remote 192.168.20.245

2. 第2种方法：使用TCP协议tap设备建立 连接：

服务器端配置如下：

[root@c720245 ~]# openvpn --ifconfig 10.200.0.1 255.255.255.0 --dev tap

客户端配置如下：

[root@c720246 ~]# openvpn --ifconfig 10.200.0.2 255.255.255.0 --dev tap --remote 192.168.20.245

总结： 使用第一种方法，服务器端会侦听1194端口，而客户端不会。

使用第二种方法：服务器端和客户端都会侦听1194端口。

使用第一种方法配置时需要指明对端的隧道地址和本端地址，而第二种方法只需要指明本端隧道地址即可，不需要指明对端。

openvpn的密钥

Wednesday, March 13, 2019 2:07 PM

使用一个密钥方式如下：

1. 产生一个密钥

[root@c720245 ~]# openvpn --genkey --secret secret.key

2. 把密钥想办法传给对端，方便使用相同密钥进行加密

[root@c720245 ~]# scp secret.key root@192.168.20.246:/root/

3. 服务器端配置

[root@c720245 ~]# openvpn --ifocnfig 10.200.0.1 10.200.0.2 --dev tun --secret secret.key --verb 7

配置为本端tun0 IP地址为10.200.0.1，对端为10.200.0.2 使用tun设备，显示日志等级为7级（为了更详细的说明问题）

4. 客户端配置

[root@c720246 ~]# openvpn --ifconfig 10.200.0.2 10.200.0.1 --dev tun --secret secret.key --remote 192.168.20.245

5. 如果配置都正确，日志中应该看到如下信息

   Wed Mar 13 14:19:48 2019 Initialization Sequence Completed

使用多个密钥方式如下：

6. 服务器端配置

[root@c720245 ~]# openvpn --ifconfig 10.200.0.2 10.200.0.1 --dev tun --secret secret.key 0 --verb 7

7. 客户端配置

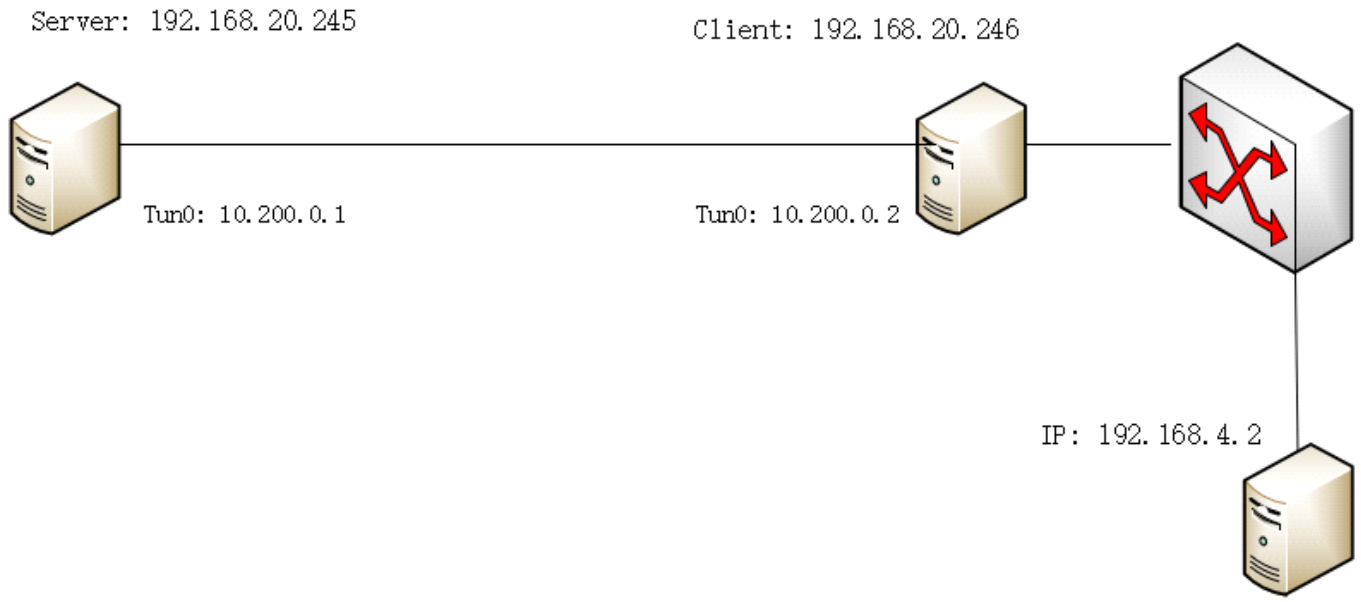
[root@c720246 ~]# openvpn --ifconfig 10.200.0.1 10.200.0.2 --dev tun --secret secret.key 1 --remote 192.168.20.245 --verb 7

备注：记住在密钥文件后面有两个数字0和1分别代表方向 感。

服务器和客户端的方向要正好相反，否则通信会失败。

openvpn的路由、命令行与配置文件区别

Wednesday, March 13, 2019 5:09 PM



服务器配置:

[root@c720245 ~]# openvpn --ifconfig 10.200.0.1 10.200.0.2 --dev tun --secret secret.key 0 --route 192.168.4.0 255.255.255.0 --daemon --log /var/log/openvpn-server.log

-- daemon:代表以守护进程方式进行启动

--log /var/log/openvpn-server.log:代表所有日志信息存储到/var/log/openvpn-server.log 文件中

--route 192.168.4.0 255.255.255.0 : 代表如果有流量 去往192.168.4.0网段的IP，转发至 10.200.0.2

客户端配置:

[root@c720246 ~]# openvpn --ifconfig 10.200.0.2 10.200.0.1 --dev tun --secret secret.key 1 --remote 192.168.20.245 --daemon --log /var/log/openvpn-client.log

开启路由转发功能：

如果192.168.4.2不是配置在本机的模拟环境，而是由另外一台主机。那么请开启转发功能

1. [root@c720246 ~]# vi /etc/sysctl.conf
   Net.ipv4.ip_forward = 1
2. 使用sysctl -p生效。

使用配置文件案例:

服务器端：openvpn-02-01-server.conf

ifconfig 10.200.0.1 10.200.0.2
dev tun

```
secret secret.key 0
route 192.168.4.0 255.255.255.0
daemon
log /var/log/openvpn-server.log
```

启动命令： openvpn --config openvpn-02-01-server.conf

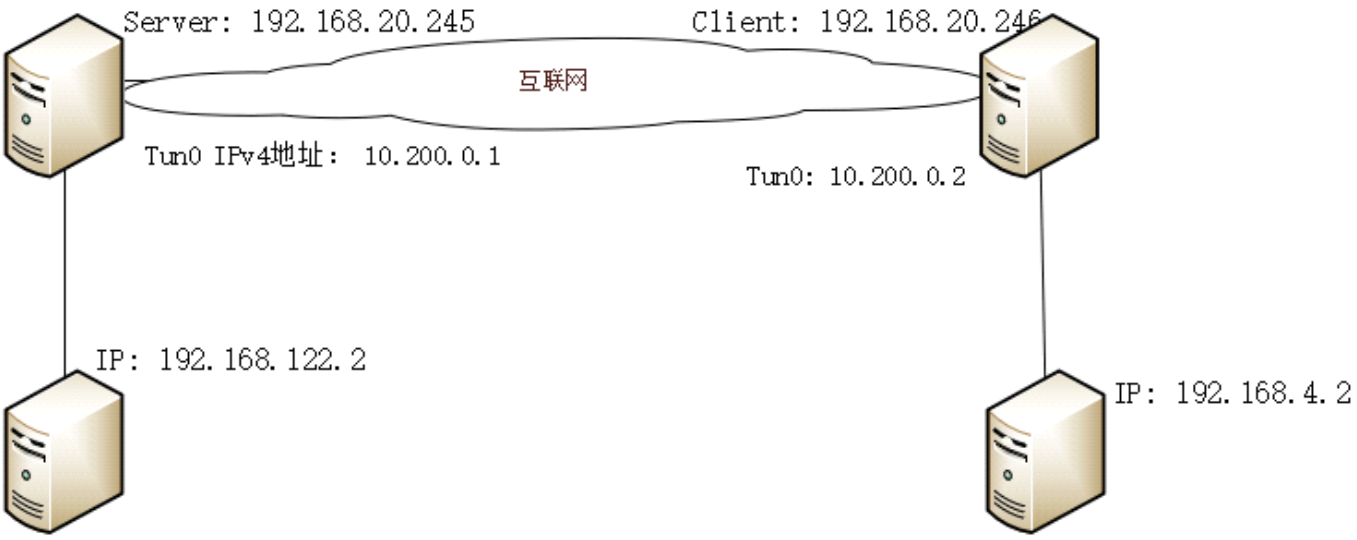
如果想停止服务器：

Ps -ef | grep openvpn # 查找到它运行的进程 ID

Kill -9 openvpn的进程 ID

完整的配置及无IP方式的实现

Wednesday, March 13, 2019 5:59 PM



1. 拓扑模拟

服务器端局域 网模拟：

[root@c720245 ~]# ifconfig eth0:0 192.168.122.2/24 up

客户端局域网模拟：

[root@c720246 ~]# ifconfig eth0:0 192.168.4.2/24 up

2. 配置文件

服务器端配置文件：

```
dev tun
local 192.168.20.245
lport 1234
remote 192.168.20.246
rport 4321

secret secret.key 0
ifconfig 10.200.0.1 10.200.0.2
route 192.168.4.0 255.255.255.0

user nobody
group nobody

persist-tun
persist-key
keepalive 10 60
ping-timer-rem

verb 3
daemon
log-append /var/log/openvpn-server.log
```

客户端配置文件：

```
dev tun
proto udp
local 192.168.20.246
lport 4321
remote 192.168.20.245
rport 1234

secret secret.key 1
ifconfig 10.200.0.2 10.200.0.1
route 192.168.122.0 255.255.255.0

user nobody
group nobody

persist-tun
persist-key
keepalive 10 60
ping-timer-rem

verb 3
daemon
log-append /var/log/openvpn-client.log
```

3. 服务器和客户端进行启动

   服务器端启动：

   ```
   [root@c720245 ~]# openvpn --config openvpn-02-02-server.conf
   ```

   客户端启动：

   ```
   [root@c720246 ~]# openvpn --config openvpn-02-02-client.conf
   ```

4. 校验结果

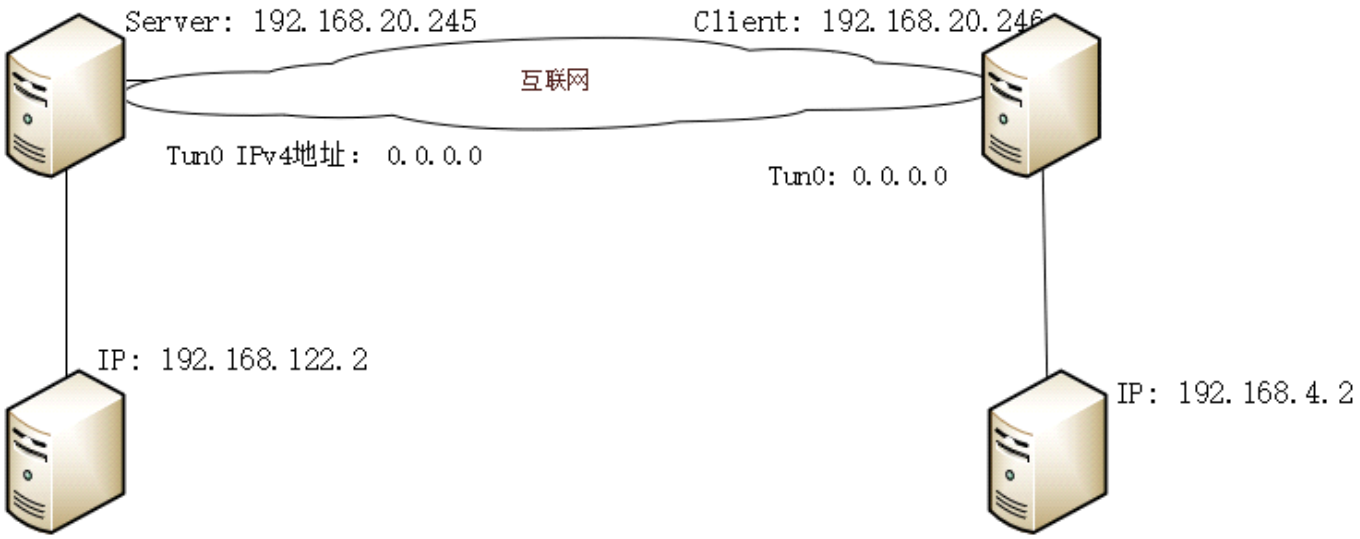
   服务器端进行校验：

   ```
   [root@c720245 ~]# ping 192.168.4.2 -I 192.168.122.2
   PING 192.168.4.2 (192.168.4.2) from 192.168.122.2 : 56(84) bytes of data.
   64 bytes from 192.168.4.2: icmp_seq=1 ttl=64 time=0.520 ms
   64 bytes from 192.168.4.2: icmp_seq=2 ttl=64 time=0.559 ms
   ```

   客户端进行校验：

   ```
   [root@c720246 ~]# ping 192.168.122.2 -I 192.168.4.2
   PING 192.168.122.2 (192.168.122.2) from 192.168.4.2 : 56(84) bytes of data.
   64 bytes from 192.168.122.2: icmp_seq=1 ttl=64 time=0.479 ms
   64 bytes from 192.168.122.2: icmp_seq=2 ttl=64 time=0.495 ms
   ```

高级的无IP设置：



配置文件：

服务器配置文件openvpn-02-03-server.conf

```
dev tun
secret secret.key
ifconfig-noexec

up /etc/openvpn/up.sh
script-security 2
verb 3

daemon
log-append /var/log/openvpn.log
```

脚本配置文件：

```
Vi /etc/openvpn/up.sh
#!/bin/bash
/usr/sbin/ifconfig $1 0.0.0.0 up
/usr /sbin/ip route 192.168.4.0/24 dev $1
```

客户端配置文件openvpn-02-03-client.conf

```
dev tun
secret secret.key
ifconfig-noexec
remote 192.168.20.245

up /etc/openvpn/up.sh
script-security 2
verb 3
daemon
log-append /var/log/openvpn-client.log
```

客户端脚本配置文件：/etc/openvpn/up.sh

```
#!/bin/bash
/usr/sbin/ifconfig $1 0.0.0.0 up
/usr/sbin/ip route add 192.168.122.0/24 dev $1
```

服务器和客户端启动：

Openvpn --config openvpn-02-03-server.conf

Openvpn --config oepnvpn-02-03-client.conf

测试结果：

注意：由于服务器端没有指定远端的IP，所以不能够首先发起连接。必须先由客户端发起连接。

客户端测试结果：

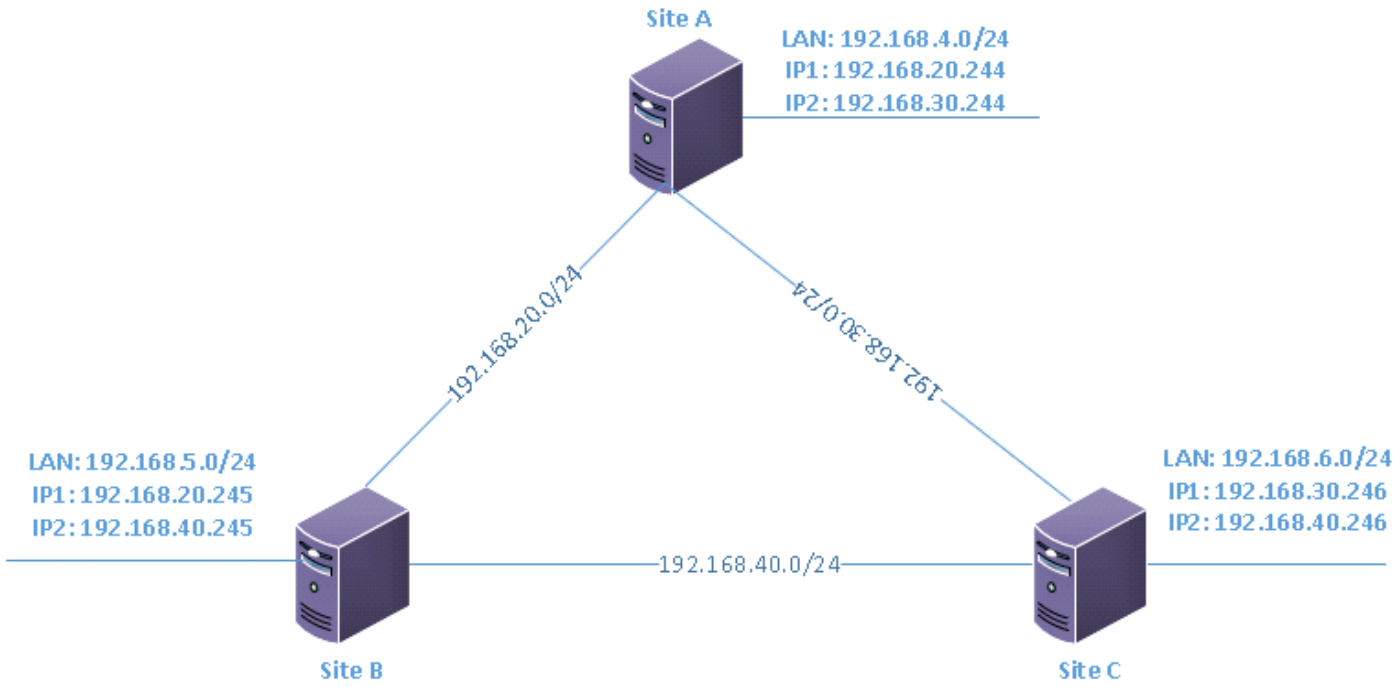
```
[root@c720246 ~]# ping 192.168.122.2 -I 192.168.4.2
PING 192.168.122.2 (192.168.122.2) from 192.168.4.2 : 56(84) bytes of data.
64 bytes from 192.168.122.2: icmp_seq=1 ttl=64 time=0.630 ms
64 bytes from 192.168.122.2: icmp_seq=2 ttl=64 time=0.432 ms
64 bytes from 192.168.122.2: icmp_seq=3 ttl=64 time=0.564 ms
64 bytes from 192.168.122.2: icmp_seq=4 ttl=64 time=0.455 ms
```

服务器端测试结果：

```
[root@c720245 ~]# ping 192.168.4.2 -I 192.168.122.2
PING 192.168.4.2 (192.168.4.2) from 192.168.122.2 : 56(84) bytes of data.
64 bytes from 192.168.4.2: icmp_seq=1 ttl=64 time=0.436 ms
64 bytes from 192.168.4.2: icmp_seq=2 ttl=64 time=0.465 ms
```

三方站点的路由

Wednesday, March 13, 2019 8:31 PM



1. 首先创建三方站点通信的密钥

   [root@c720244 ~]# openvpn --genkey --secret AtoB.key
   [root@c720244 ~]# openvpn --genkey --secret AtoC.key
   [root@c720244 ~]# openvpn --genkey --secret BtoC.key

2. 把三个秘钥文件分别复制到站点B， 站点C

   [root@c720244 ~]# scp AtoB.key AtoC.key BtoC.key root@192.168.20.245:/root/
   [root@c720244 ~]# scp AtoB.key AtoC.key BtoC.key root@192.168.20.246:/root/

3. 配置文件总共有个。

(1) AtoB.conf:

```
dev tun
proto udp
port 1194
remote 192.168.20.245
secret /root/AtoB.key 1
ifconfig 10.200.0.2 10.200.0.1
```

route 192.168.5.0 255.255.255.0 vpn_gateway 5
route 192.168.6.0 255.255.255.0 vpn_gateway 10
route-delay
keepalive 10 60
verb 3
daemon
log-append /var/log/openvpn-AtoB.log

(2) AtoC.conf

dev tun
proto udp
port 1195
remote 192.168.30.246
secret /root/AtoC.key 1
ifconfig 10.200.0.6 10.200.0.5
route 192.168.5.0 255.255.255.0 vpn_gateway 10
route 192.168.6.0 255.255.255.0 vpn_gateway 5
route-delay
keepalive 10 60
verb 3
daemon
log-append /var/log/openvpn-AtoC.log

(3) BtoA.conf
dev tun
proto udp
port 1194
remote 192.168.20.244
secret /root/AtoB.key 0
ifconfig 10.200.0.1 10.200.0.2
route 192.168.4.0 255.255.255.0 vpn_gateway 5
route 192.168.6.0 255.255.255.0 vpn_gateway 10
route-delay
keepalive 10 60
verb 3
daemon
log-append /var/log/openvpn-BtoA.log

(4) BtoC.conf
dev tun
proto udp
port 1196
remote 192.168.40.246
secret /root/BtoC.key 0
ifconfig 10.200.0.9 10.200.0.10
route 192.168.4.0 255.255.255.0 vpn_gateway 10
route 192.168.6.0 255.255.255.0 vpn_gateway 5
route-delay
keepalive 10 60
verb 3
daemon
log-append /var/log/openvpn-BtoC.log

(5) CtoA.conf

```
dev tun
proto udp
port 1195
remote 192.168.30.244
secret /root/AtoC.key 0
ifconfig 10.200.0.5 10.200.0.6
route 192.168.4.0 255.255.255.0 vpn_gateway 5
route 192.168.5.0 255.255.255.0 vpn_gateway 10
route-delay
keepalive 10 60
verb 3
daemon
log-append /var/log/openvpn-CtoA.log
```

(6) CtoB.conf

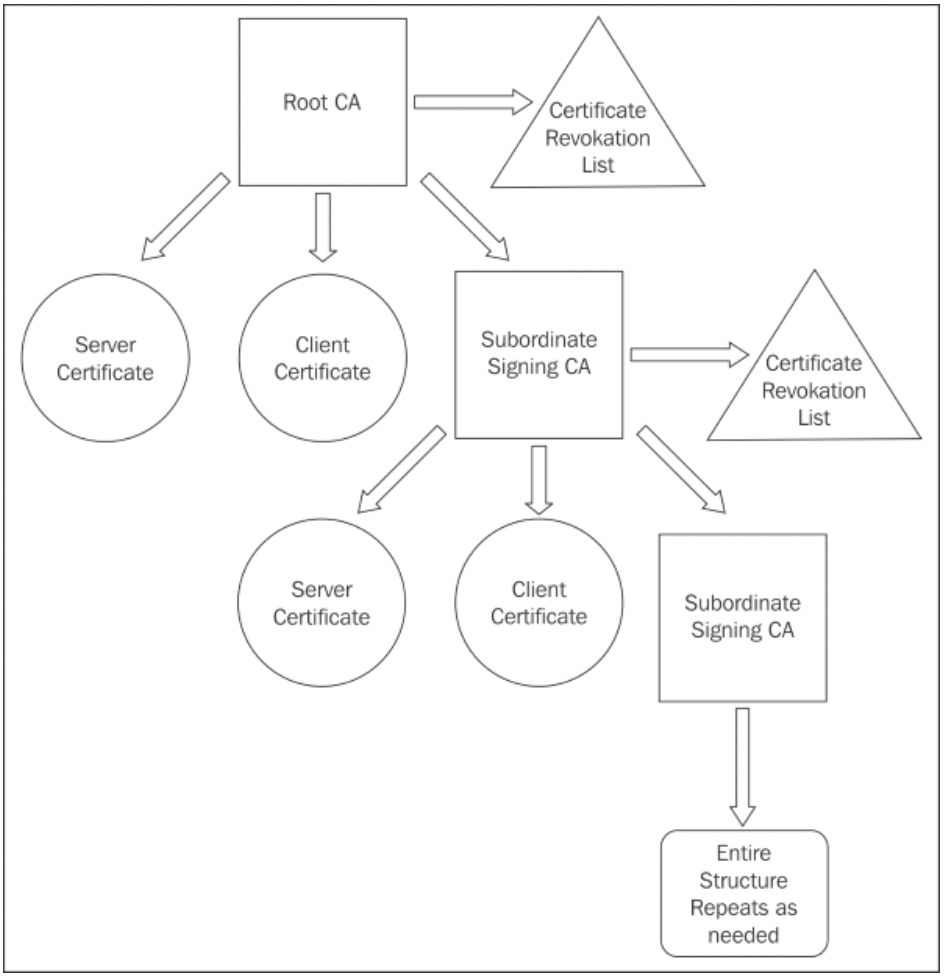
```
dev tun
proto udp
port 1196
remote 192.168.40.245
secret /root/BtoC.key 1
ifconfig 10.200.0.10 10.200.0.9
route 192.168.4.0 255.255.255.0 vpn_gateway 10
route 192.168.5.0 255.255.255.0 vpn_gateway 5
route-delay
keepalive 10 60
verb 3
daemon
log-append /var/log/openvpn-CtoB.log
```

4. 启动命令

   Openvpn --config 配置文件

PKI和证书

Thursday, March 14, 2019 12:40 PM



操作证书的三个工具:

1. Openssl
2. EasyRSA
3. SSL-admin

EasyRSA的使用:

1. 执行以下命令

   [root@c720245 ~]# tar -zxvf EasyRSA-unix-v3.0.6.tgz
   [root@c720245 ~]# cd /usr/local/
   [root@c720245 local]# ln -s /usr/local/EasyRSA-v3.0.6/ /usr/local/EasyRSA
   [root@c720245 local]# cd EasyRSA
   [root@c720245 EasyRSA]# cp vars.example vars

2. 修改默认值

   [root@c720245 EasyRSA]# vi vars

```
set_var EASYRSA_REQ_COUNTRY    "CN"
set_var EASYRSA_REQ_PROVINCE   "JiangSu"
set_var EASYRSA_REQ_CITY       "SuZhou"
set_var EASYRSA_REQ_ORG        "Xiodi"
set_var EASYRSA_REQ_EMAIL      "zangxueyuan@126.com"
set_var EASYRSA_REQ_OU         "IT"
```

3. 初始化
   [root@c720245 EasyRSA]# ./easyrsa init-pki

   Note: using Easy-RSA configuration from: ./vars

   init-pki complete; you may now create a CA or requests.
   Your newly created PKI dir is: /usr/local/EasyRSA/pki

4. 私有CA的创建
   [root@c720245 EasyRSA]# ./easyrsa build-ca

5. 查看CA的约束是否为TRUE.
   [root@c720245 EasyRSA]# openssl x509 -in ca.crt -text -noout

6. 创建一个吊销列表
   [root@c720245 EasyRSA]# ./easyrsa gen-crl

7. 查看吊销列表里面的吊销证书
   [root@c720245 EasyRSA]# openssl crl -noout -text -in /usr/local/EasyRSA/pki/crl.pem

8. 产生服务器证书
   [root@c720245 EasyRSA]# ./easyrsa build-server-full openvpnserver2.xiodi.cn

9. 校验产生的服务器证书信息
   [root@c720245 EasyRSA]# openssl x509 -noout -text -in /usr/local/EasyRSA/pki/issued/openvpnserver2.xiodi.cn.crt

10. 产生客户端证书
    [root@c720245 EasyRSA]# ./easyrsa build-client-full client1.xiodi.cn

11. 校验客户端证书
    [root@c720245 EasyRSA]# openssl x509 -noout -text -in /usr/local/EasyRSA/pki/issued/client1.xiodi.cn.crt

通过ssladmin管理证书

Thursday, March 14, 2019 3:13 PM

1. 解压缩ssl-admin
   [root@c720245 ~]# tar -zxvf ssa.tgz

2. 编译安装ssl-admin
   [root@c720245 ssl-admin-1.2.1]# ./configure

   [root@c720245 ssl-admin-1.2.1]# make install

3. 如果缺少perl，缺少失败，需要安装
   [root@c720245 ssl-admin-1.2.1]# yum install perl

4. 复制配置文件并授权更改权限
   [root@c720245 ssl-admin-1.2.1]# cp /etc/ssl-admin/ssl-admin.conf.sample /etc/ssl-admin/ssl-admin.conf
   [root@c720245 ssl-admin-1.2.1]# chmod ug+w /etc/ssl-admin/ssl-admin.conf

5. 使用vi修改/etc/ssl-admin/ssl-admin的环境变量文件，如下所示。具体根据您的场景更改。
   $ENV{'KEY_COUNTRY'} = "CN";
   $ENV{'KEY_PROVINCE'} = "JiangSu";
   $ENV{'KEY_CITY'} = "SuZhou";
   $ENV{'KEY_ORG'} = "IT";
   $ENV{'KEY_EMAIL'} = 'zangxueyuan@126.com';

6. 需要放置openssl.conf文件,并授权可写权限。
   [root@c720245 ssl-admin-1.2.1]# cp /etc/ssl-admin/openssl.conf.sample /etc/ssl-admin/openssl.conf

   [root@c720245 ssl-admin]# chmod ug+w openssl.conf

7. 修改签 名算法为sha256
   主要把sha1和md5更为sha256

8. 执行ssl-admin进行生成根证书。

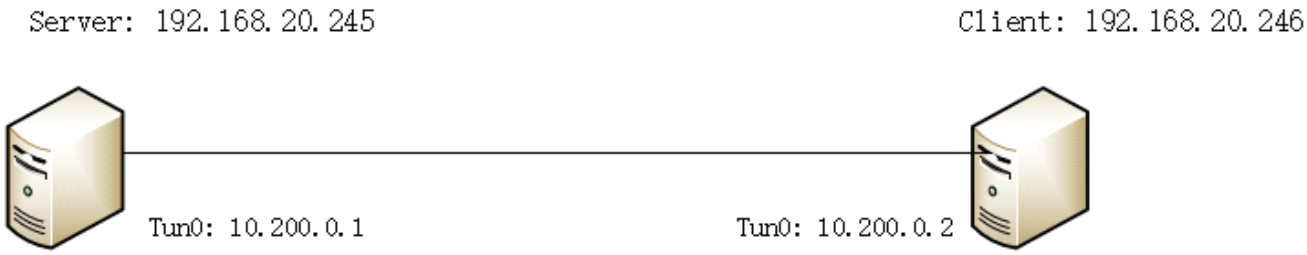
9. 选择S，按照步骤 一步步签发服务器证书即可。

10. 选择4，生成客户端证书。

提示：如果要校验证书，使用以下命令
Openssl x509 -noout -text -in 证书的路径

使用证书的点到点模式

Thursday, March 14, 2019 4:58 PM



1. 创建用于保存证书的文件夹，并授权（客户端和服务器均如此，方便我们记忆）
   [root@c720245 ~]# mkdir -p /etc/openvpn/movpn
   [root@c720245 ~]# chmod 700 /etc/openvpn/movpn

2. 复制证书到创建的文件夹下，例
   [root@c720245 movpn]# cp -a /etc/ssl-admin/active/ca.crt .
   [root@c720245 movpn]# cp -a /etc/ssl-admin/active/ca.key .
   [root@c720245 movpn]# cp /etc/ssl-admin/active/openvpn-server1.xiodi.cn.* .

3. 把客户端的证书复制到客户端的指定目录下
   [root@c720245 movpn]# scp ca.crt /etc/ssl-admin/active/openvpn-client1.xiodi.cn.* root@192.168.20.246:/etc/openvpn/movpn

4. 服务器端配置
   [root@c720245 ~]# cat openvpn-02-06-server.conf
   proto udp
   port 1194
   dev tun
   tls-server
   ifconfig 10.200.0.1 10.200.0.2
   dh /etc/openvpn/movpn/dh2048.pem
   ca /etc/openvpn/movpn/ca.crt
   cert /etc/openvpn/movpn/openvpn-server1.xiodi.cn.crt
   key /etc/openvpn/movpn/openvpn-server1.xiodi.cn.key
   persist-key
   persist-tun
   keepalive 10 60
   user nobody
   group nobody

   verb 3
   daemon
   log-append /var/log/openvpn.log

客户端配置文件：

```
[root@c720246 ~]# cat openvpn-02-06-client.conf
port 1194
dev tun
tls-client
ifconfig 10.200.0.2 10.200.0.1
remote 192.168.20.245
remote-cert-tls server
ca /etc/openvpn/movpn/ca.crt
cert /etc/openvpn/movpn/openvpn-client1.xiodi.cn.crt
key /etc/openvpn/movpn/openvpn-client1.xiodi.cn.key
persist-key
persist-tun
keepalive 10 60
user nobody
group nobody
verb 3
daemon
log-append /var/log/openvpn.log
```

5. 启动服务器和客户端的Openvpn

   Openvpn --config openvpn-02-06-server.conf

   Openvpn --config openvpn-02--06-client.conf

客户端服务器模式的初始配置

Thursday, March 14, 2019 5:28 PM

优点如下：

1. VPN服务器管理员可以控制哪些流量 在客户间流动。默认情况下，不允许客户机之间任何流量流动。可以通过特殊的设置允许客户机之间进行通信。
2. 易于部署： 相比于让每个客户机之间建立专门的连接，这种方式要简单的多。

缺点如下：

可伸缩性：如果设置客户机之间能够通信，有大量客户机的情况下，可能会对VPN服务器性能产生瓶颈。

转发：转发都是经过服务器的，可能会导致大的延迟。

客户端服务器模式最常见的情景：

1. 在外办公人员
2. 方便在那些在家办公人员

服务器端配置：

```
[root@c720245 ~]# cat openvpn-03-01-server.conf
proto udp
port 1194
dev tun
server 10.200.0.0 255.255.255.0
topology subnet
persist-key
persist-tun
keepalive 10 60
dh /etc/openvpn/movpn/dh2048.pem
ca /etc/openvpn/movpn/ca.crt
cert /etc/openvpn/movpn/openvpn-server1.xiodi.cn.crt
key /etc/openvpn/movpn/openvpn-server1.xiodi.cn.key

user nobody
group nobody

verb 3
daemon
log-append /var/log/openvpn.log
```

客户端配置：

```
[root@c720246 ~]# cat openvpn-03-01-client.conf

client
proto udp
remote 192.168.20.245
port 1194
dev tun
nobind
ca /etc/openvpn/movpn/ca.crt
cert /etc/openvpn/movpn/openvpn-client1.xiodi.cn.crt
key /etc/openvpn/movpn/openvpn-client1.xiodi.cn.key
```

启动服务器和客户端：

```
Openvpn --config openvpn-03-01-server.conf
Openvpn --config openvpn-03-01-client.conf
```

如何使用tls认证增强我们的远端VPN的安全

Thursday, March 14, 2019 5:53 PM

两种方式增加安全性

1. 通过添加tls-auth keys增加
2. 通过检查使用证书的扩展密钥使用属性

1. 产生tls认证密钥

   [root@c720245 ~]# openvpn --genkey --secret /etc/openvpn/movpn/ta.key

2. 把它复制到每个客户端
   [root@c720245 ~]# scp /etc/openvpn/movpn/ta.key root@192.168.20.246:/etc/openvpn/movpn

3. 可选项，检查服务器证书是否有可扩展属性，如果有的话，将会增加一定程度上的安全性。
   [root@c720245 ~]# openssl x509 -text -noout -in /etc/ssl-admin/active/openvpn-server1.xiodi.cn.crt | grep -C 1 "Key Usage"

```
X509v3 Extended Key Usage:
    TLS Web Server Authentication
X509v3 Key Usage:
    Digital Signature, Key Encipherment
```

UDP协议的配置：

服务器端：

```
[root@c720245 ~]# cat openvpn-03-05-server.conf
proto  udp
port 1194
dev tun
server 10.200.0.0 255.255.255.0
topology subnet
persist-key
persist-tun
keepalive 10 60

tls-auth /etc/openvpn/movpn/ta.key 0
dh /etc/openvpn/movpn/dh2048.pem
ca /etc/openvpn/movpn/ca.crt
cert /etc/openvpn/movpn/openvpn-server1.xiodi.cn.crt
key /etc/openvpn/movpn/openvpn-server1.xiodi.cn.key
```

```
user nobody
group nobody

verb 3
daemon
log-append /var/log/openvpn.log
```

客户端：

```
[root@c720246 ~]# cat openvpn-03-05-client.conf
client
proto udp
remote 192.168.20.245
port 1194
dev tun
nobind

remote-cert-tls server
tls-auth /etc/openvpn/movpn/ta.key 1
ca /etc/openvpn/movpn/ca.crt
cert /etc/openvpn/movpn/openvpn-client1.xiodi.cn.crt
key /etc/openvpn/movpn/openvpn-client1.xiodi.cn.key
```

TCP协议的配置：

服务器端配置：

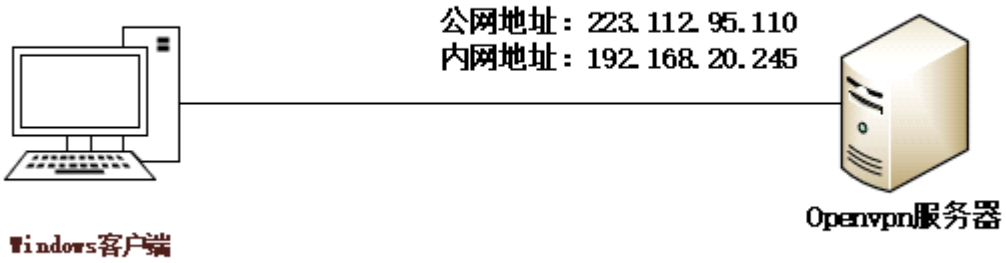
```
[root@c720245 ~]# cat openvpn-03-05-server.conf
proto tcp
port 1194
dev tun
server 10.200.0.0 255.255.255.0
topology subnet
persist-key
persist-tun
keepalive 10 60

tls-auth /etc/openvpn/movpn/ta.key 0
dh /etc/openvpn/movpn/dh2048.pem
ca /etc/openvpn/movpn/ca.crt
cert /etc/openvpn/movpn/openvpn-server1.xiodi.cn.crt
key /etc/openvpn/movpn/openvpn-server1.xiodi.cn.key

user nobody
group nobody

verb 3
daemon
log-append /var/log/openvpn.log
```

客户端配置：

```
[root@c720246 ~]# cat openvpn-03-05-client.conf
client
proto tcp
remote 192.168.20.245
port 1194
dev tun
nobind

remote-cert-tls server
tls-auth /etc/openvpn/movpn/ta.key 1
ca /etc/openvpn/movpn/ca.crt
cert /etc/openvpn/movpn/openvpn-client1.xiodi.cn.crt
key /etc/openvpn/movpn/openvpn-client1.xiodi.cn.key
```

使用windows客户端连接vpn服务器

Thursday, March 14, 2019 7:57 PM



服务器端配置：

Cat openvpn-03-6-server.conf

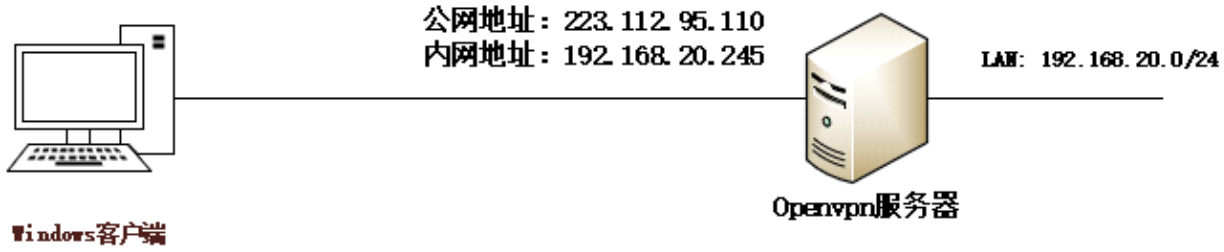
```
proto tcp
port 1198
dev tun
server 10.200.0.0 255.255.255.0
topology subnet
persist-key
persist-tun
keepalive 10 60

tls-auth /etc/openvpn/movpn/ta.key 0
dh /etc/openvpn/movpn/dh2048.pem
ca /etc/openvpn/movpn/ca.crt
cert /etc/openvpn/movpn/openvpn-server1.xiodi.cn.crt
key /etc/openvpn/movpn/openvpn-server1.xiodi.cn.key

user nobody
group nobody

verb 3
daemon
log-append /var/log/openvpn.log
```

客户端配置：

```
client
proto tcp
remote 223.112.95.110
port 1198
dev tun
nobind

remote-cert-tls server
tls-auth ta.key 1
ca ca.crt
cert oepnvpn-client2.xiodi.cn.crt
key oepnvpn-client2.xiodi.cn.key
```

客户端和服务器的路由

Thursday, March 14, 2019 8:27 PM



192.168.20.246

服务器端配置：

Cat openvpn-03-6-server.conf

```
proto tcp
port 1198
dev tun
server 10.200.0.0 255.255.255.0
topology subnet
persist-key
persist-tun
keepalive 10 60

tls-auth /etc/openvpn/movpn/ta.key 0
dh /etc/openvpn/movpn/dh2048.pem
ca /etc/openvpn/movpn/ca.crt
cert /etc/openvpn/movpn/openvpn-server1.xiodi.cn.crt
key /etc/openvpn/movpn/openvpn-server1.xiodi.cn.key

user nobody
group nobody

verb 3
daemon
log-append /var/log/openvpn.log

push "route 192.168.20.0 255.255.255.0"
```

客户端配置：

```
client
proto tcp
remote 223.112.95.110
port 1198
dev tun
nobind

remote-cert-tls server
tls-auth ta.key 1
ca ca.crt
cert oepnvpn-client2.xiodi.cn.crt
key oepnvpn-client2.xiodi.cn.key
```

重定向默认网关及客户端指定配置

Thursday, March 14, 2019 9:05 PM

1. 重定向默认网关

服务器配置：

```
proto tcp
port 1198
dev tun
server 10.200.0.0 255.255.255.0
topology subnet
persist-key
persist-tun
keepalive 10 60

tls-auth /etc/openvpn/movpn/ta.key 0
dh /etc/openvpn/movpn/dh2048.pem
ca /etc/openvpn/movpn/ca.crt
cert /etc/openvpn/movpn/openvpn-server1.xiodi.cn.crt
key /etc/openvpn/movpn/openvpn-server1.xiodi.cn.key

user nobody
group nobody

verb 3
daemon
log-append /var/log/openvpn.log

push "route 192.168.20.0 255.255.255.0"
push "redirect-gateway def1"
```

2. 客户端指定配置文件

服务器端配置文件：

```
proto tcp
port 1198
dev tun
server 10.200.0.0 255.255.255.0
topology subnet
persist-key
persist-tun
keepalive 10 60

tls-auth /etc/openvpn/movpn/ta.key 0
dh /etc/openvpn/movpn/dh2048.pem
ca /etc/openvpn/movpn/ca.crt
cert /etc/openvpn/movpn/openvpn-server1.xiodi.cn.crt
key /etc/openvpn/movpn/openvpn-server1.xiodi.cn.key
```

```
user nobody
group nobody

verb 3
daemon
log-append /var/log/openvpn.log

push "route 192.168.20.0 255.255.255.0"
push "redirect-gateway def1"
client-config-dir /etc/openvpn/movpn/clients
```

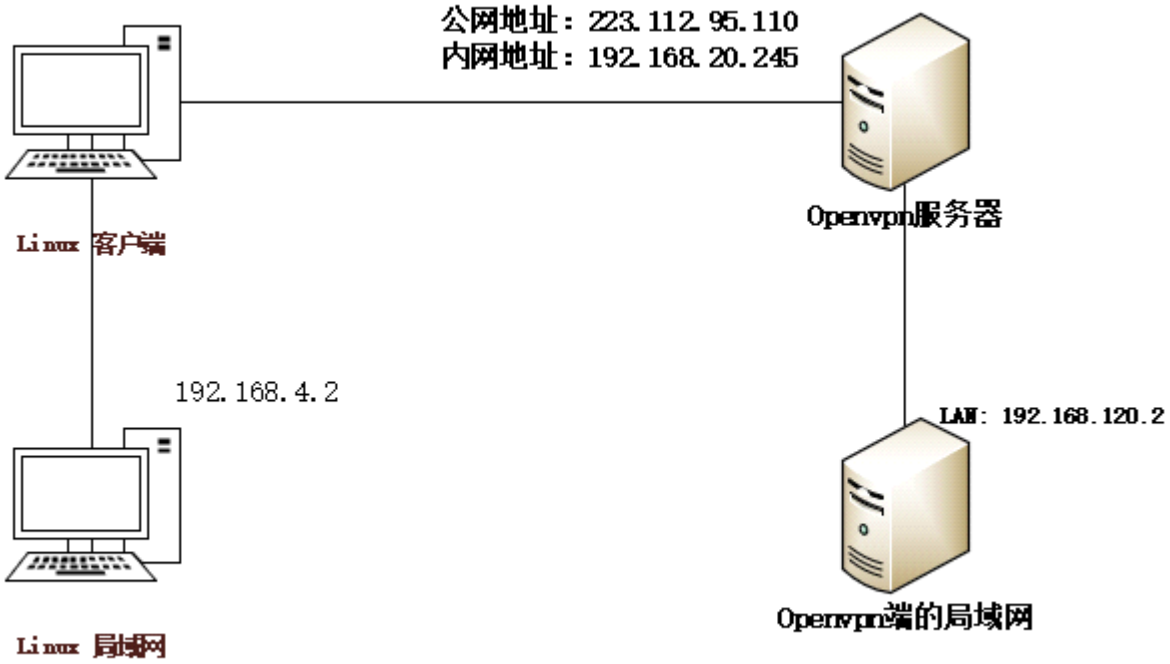
（2）opepnvpn-client2.xiodi.cn文件内容

```
[root@c720245 ~]# cat /etc/openvpn/movpn/clients/oepnvpn-client2.xiodi.cn
ifconfig-push 10.200.0.99 255.255.255.0
```

注意：一定要授权其它用户能够读取oepnvpn-client2.xiodi.cn文件的权限，否则启动将会失败。

服务器通向客户端的路由及Openvpn的状态文件

Thursday, March 14, 2019 9:28 PM



1. 环境模拟

   服务器端：

   [root@c720245 ~]# ifconfig eth0:0 192.168.120.2/24 up

客户端：

[root@c720246 ~]# ifconfig eth0:0 192.168.4.2/24 up

2. 配置文件

   服务器端配置：

   [root@c720245 ~]# cat openvpn-03-08-server.conf
   proto tcp
   port 1198
   dev tun
   server 10.200.0.0 255.255.255.0
   topology subnet
   persist-key
   persist-tun
   keepalive 10 60

   tls-auth /etc/openvpn/movpn/ta.key 0
   dh /etc/openvpn/movpn/dh2048.pem

```
ca /etc/openvpn/movpn/ca.crt
cert /etc/openvpn/movpn/openvpn-server1.xiodi.cn.crt
key /etc/openvpn/movpn/openvpn-server1.xiodi.cn.key

user nobody
group nobody

verb 3
daemon
log-append /var/log/openvpn.log

client-config-dir /etc/openvpn/movpn/clients
route 192.168.4.0 255.255.255.0 10.200.0.99


[root@c720245 ~]# cat /etc/openvpn/movpn/clients/openvpn-client1.xiodi.cn
ifconfig-push 10.200.0.99 255.255.255.0
iroute 192.168.4.0 255.255.255.0
push "route 192.168.120.0 255.255.255.0"
```

客户端配置：

```
client
proto tcp
remote 192.168.20.245
port 1198
dev tun
nobind

remote-cert-tls server
tls-auth /etc/openvpn/movpn/ta.key 1
ca /etc/openvpn/movpn/ca.crt
cert /etc/openvpn/movpn/openvpn-client1.xiodi.cn.crt
key /etc/openvpn/movpn/openvpn-client1.xiodi.cn.key
```

二. Openvpn状态文件

openvpn的状态文件包括如下信息：

连接哪些客户机

客户机的IP地址

每个客户端接收和传送的字节数

客户端连接的时间

此外，路由表还显示了哪些网络被路由到每个客户机

```
[root@c720245 ~]# cat openvpn-03-08-server.conf
proto tcp
port 1198
dev tun
```

```
server 10.200.0.0 255.255.255.0
topology subnet
persist-key
persist-tun
keepalive 10 60

tls-auth /etc/openvpn/movpn/ta.key 0
dh /etc/openvpn/movpn/dh2048.pem
ca /etc/openvpn/movpn/ca.crt
cert /etc/openvpn/movpn/openvpn-server1.xiodi.cn.crt
key /etc/openvpn/movpn/openvpn-server1.xiodi.cn.key

user nobody
group nobody

verb 3
daemon
log-append /var/log/openvpn.log

client-config-dir /etc/openvpn/movpn/clients
route 192.168.4.0 255.255.255.0 10.200.0.99
status /var/run/openvpn.status 3
```

openvpn管理接口和会话Key的重新协商

Friday, March 15, 2019 11:02 AM

服务器端配置文件：

```
[root@c720245 ~]# cat openvpn-03-08-server.conf
proto tcp
port 1198
dev tun
server 10.200.0.0 255.255.255.0
topology subnet
persist-key
persist-tun
keepalive 10 60

tls-auth /etc/openvpn/movpn/ta.key 0
dh /etc/openvpn/movpn/dh2048.pem
ca /etc/openvpn/movpn/ca.crt
cert /etc/openvpn/movpn/openvpn-server1.xiodi.cn.crt
key /etc/openvpn/movpn/openvpn-server1.xiodi.cn.key

user nobody
group nobody

verb 3
daemon
log-append /var/log/openvpn.log

client-config-dir /etc/openvpn/movpn/clients
route 192.168.4.0 255.255.255.0 10.200.0.99
status /var/run/openvpn.status 3
management 127.0.0.1 23000 stdin
```

服务器定期协商数据通道的密钥，主要是由三个选项来控制的。

Reneg-sec N： 在多少秒之后重新协商数据通道（默认是3600）

Reneg-bytes N: 在多少字节后重新协商数据通道。默认是关闭的

Regneg-pkts N: 在多少包之后重新协商数据通道。默认是关闭的。

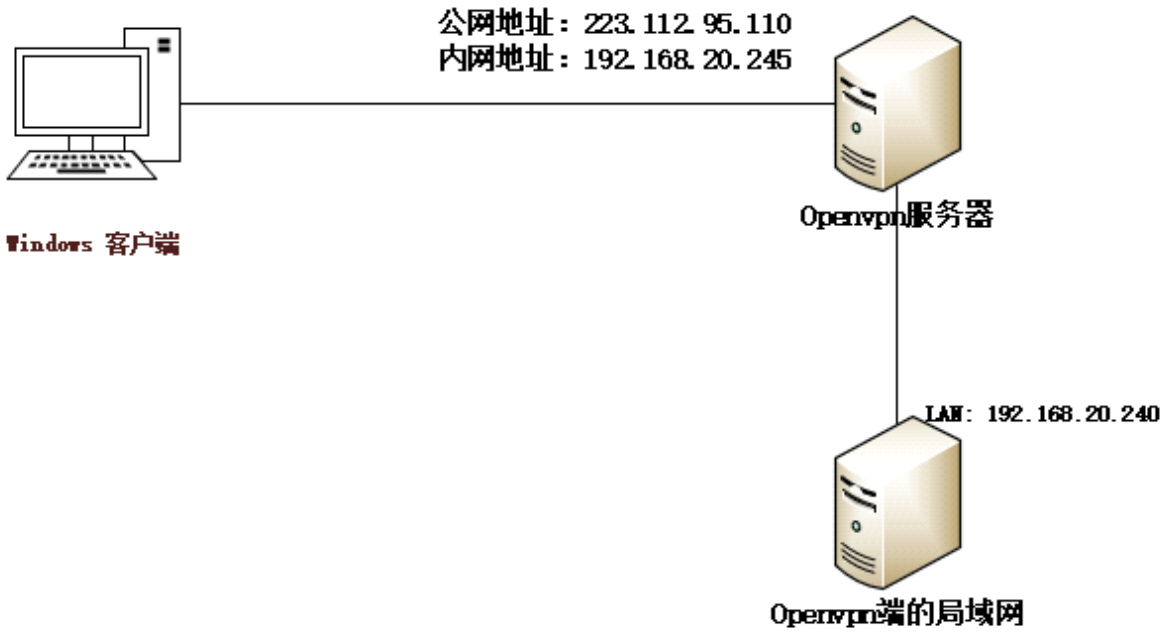
服务器端配置：

```
[root@c720245 ~]# cat openvpn-03-08-server.conf
proto tcp
port 1198
dev tun
server 10.200.0.0 255.255.255.0
topology subnet
persist-key
persist-tun
keepalive 10 60
```

```
tls-auth /etc/openvpn/movpn/ta.key 0
dh /etc/openvpn/movpn/dh2048.pem
ca /etc/openvpn/movpn/ca.crt
cert /etc/openvpn/movpn/openvpn-server1.xiodi.cn.crt
key /etc/openvpn/movpn/openvpn-server1.xiodi.cn.key

user nobody
group nobody

verb 5
daemon
log-append /var/log/openvpn.log

client-config-dir /etc/openvpn/movpn/clients
route 192.168.4.0 255.255.255.0 10.200.0.99
status /var/run/openvpn.status 3
management 127.0.0.1 23000 stdin
reneg-sec 10
reneg-pkts 1000
reneg-bytes 100000
```

通过VPN来实现文件的共享

Friday, March 15, 2019 11:30 AM



服务器端配置：

```
[root@c720245 ~]# cat openvpn-03-09-server.conf
proto tcp
port 1198
dev tun
server 10.200.0.0 255.255.255.0
topology subnet
persist-key
persist-tun
keepalive 10 60

tls-auth /etc/openvpn/movpn/ta.key 0
dh /etc/openvpn/movpn/dh2048.pem
ca /etc/openvpn/movpn/ca.crt
cert /etc/openvpn/movpn/openvpn-server1.xiodi.cn.crt
key /etc/openvpn/movpn/openvpn-server1.xiodi.cn.key

user nobody
group nobody

verb 3
daemon
log-append /var/log/openvpn.log
push "route 192.168.20.0 255.255.255.0"
```

注意一点：需要在openvpn端的局域 网电脑上指定路由或者在你IDC的路由器上指定路由。

使用证书+openldap的认证

Friday, March 15, 2019 12:44 PM

在服务器端：

第一步：安装Openldap的插件

[root@c720245 ~]# yum install openvpn-auth-ldap

第二步： 配置我们的服务器

[root@c720245 ~]# cat openvpn-03-09-server.conf
proto tcp
port 1198
dev tun
server 10.200.0.0 255.255.255.0
topology subnet
persist-key
persist-tun
keepalive 10 60

tls-auth /etc/openvpn/movpn/ta.key 0
dh /etc/openvpn/movpn/dh2048.pem
ca /etc/openvpn/movpn/ca.crt
cert /etc/openvpn/movpn/openvpn-server1.xiodi.cn.crt
key /etc/openvpn/movpn/openvpn-server1.xiodi.cn.key

user nobody
group nobody

verb 3
daemon
log-append /var/log/openvpn.log
push "route 192.168.20.0 255.255.255.0"

在客户端：

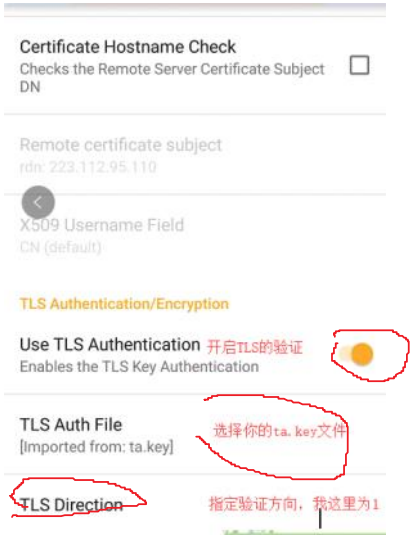
客户端配置：

```
client
proto tcp
remote 223.112.95.110
port 1198
dev tun
nobind

remote-cert-tls server
tls-auth ta.key 1
ca ca.crt
cert oepnvpn-client2.xiodi.cn.crt
key oepnvpn-client2.xiodi.cn.key
auth-user-pass
```

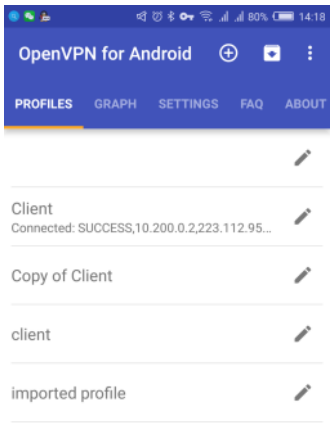
安卓手机客户端的连接

Friday, March 15, 2019 2:08 PM

客户端下载地址https://apkpure.com/openvpn-for-android/de.blinkt.openvpn/download?from=details或者使用google下载中心下载。




84% 14:47
OpenVPN Log
Connected: SUCCESS,10.222.0.6,223.112.95.110,1196,1..
14:47 SIGINT[hard,init_instance] received, process exiting
14:47 OpenVPN 2.5-icsopenvpn [git:icsopenvpn/v0.7.7-0-gbb481e41] arm64-v8a [SSL (OpenSSL)] [LZO] [LZ4] EPOLL] [MH/PKTINFO] [AEAD] built on Feb 25 2019
14:47 library versions: OpenSSL 1.1.1a 20 Nov 2018, LZO 2.10
14:47 TCP/UDP: Preserving recently used remote address: [AF_INET]223.112.95.110:1196
14:47 Attempting to establish TCP connection with AF_INET]223.112.95.110:1196 [nonblock]
14:47 TCP connection established with AF_INET]223.112.95.110:1196
14:47 TCP_CLIENT link local: (not bound)
14:47 TCP_CLIENT link remote: AF_INET]223.112.95.110:1196
14:47 [server2.xiodi.cn] Peer Connection Initiated with AF_INET]223.112.95.110:1196
14:47 OpenVPN ROUTE6: OpenVPN needs a gateway parameter for a --route-ipv6 option and no default was specified by either --route-ipv6-gateway or --ifconfig-ipv6 options
14:47 OpenVPN ROUTE: failed to parse/resolve route for host/network: ::/0
14:47 WARNING: OpenVPN was configured to add an IPv6 route over (null). However, no IPv6 has been configured for this interface, therefore the route installation may fail or may not work as expected.
14:47 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
14:47 Initialization Sequence Completed


80% 14:18
OpenVPN for Android
PROFILES
GRAPH
SETTINGS
FAQ
ABOUT
Client
Connected: SUCCESS,10.200.0.2,223.112.95...
Copy of Client
client
imported profile

22. tap模式的基本配置

Friday, March 15, 2019 2:37 PM

tap模式：往往使用二层的协议，不需要跨三层路由
tun模式：往往使用三层的协议，跑的就是ip.

tap模式的基本配置：

```
[root@c720245 ~]# cat openvpn-03-10-server.conf
proto tcp
port 1198
dev tap
server 10.200.0.0 255.255.255.0
topology subnet
persist-key
persist-tun
keepalive 10 60

tls-auth /etc/openvpn/movpn/ta.key 0
dh /etc/openvpn/movpn/dh2048.pem
ca /etc/openvpn/movpn/ca.crt
cert /etc/openvpn/movpn/openvpn-server1.xiodi.cn.crt
key /etc/openvpn/movpn/openvpn-server1.xiodi.cn.key

user nobody
group nobody

verb 5
daemon
log-append /var/log/openvpn.log
```

客户端配置：

```
proto tcp
remote 192.168.20.245
port 1198
dev tap
nobind

remote-cert-tls server
tls-auth /etc/openvpn/movpn/ta.key 1
ca /etc/openvpn/movpn/ca.crt
cert /etc/openvpn/movpn/openvpn-client1.xiodi.cn.crt
key /etc/openvpn/movpn/openvpn-client1.xiodi.cn.key
```

开启客户端到客户端的流量转发

Friday, March 15, 2019 4:02 PM

为了支持客户端到客户端的通信，主要有两个选项：

1. 使用client-to-client选项。这允许OPENVPN在内部处理客户机到客户机的通信。绕过系统路由表和系统防火墙iptables的规则。

2. 使用系统路由表和防火墙/iptables规则将流量 从一个客户机转发到另一个客户机并返回。

服务器端配置：

```
[root@c720245 ~]# cat openvpn-03-11-server.conf
proto tcp
port 1198
dev tap
server 10.200.0.0 255.255.255.0

persist-key
persist-tun
keepalive 10 60

tls-auth /etc/openvpn/movpn/ta.key 0
dh /etc/openvpn/movpn/dh2048.pem
ca /etc/openvpn/movpn/ca.crt
cert /etc/openvpn/movpn/openvpn-server1.xiodi.cn.crt
key /etc/openvpn/movpn/openvpn-server1.xiodi.cn.key

user nobody
group nobody

verb 3
daemon
log-append /var/log/openvpn.log
client-to-client
```

客户端配置：

```
[root@c720246 ~]# cat openvpn-03-09-client.conf
client
proto tcp
remote 192.168.20.245
port 1198
dev tap
nobind

remote-cert-tls server
tls-auth /etc/openvpn/movpn/ta.key 1
ca /etc/openvpn/movpn/ca.crt
```

```
cert /etc/openvpn/movpn/openvpn-client1.xiodi.cn.crt
key /etc/openvpn/movpn/openvpn-client1.xiodi.cn.key
```

客户端之间的流量过滤

Friday, March 15, 2019 4:46 PM

使用client-to-client选项开启客户机之间的流量 转发，缺点就是缺少过滤。

使用路由方式进行开启客户端到客户端的转发：

服务器配置：

```
proto tcp
port 1198
dev tap
server 10.200.0.0 255.255.255.0

persist-key
persist-tun
keepalive 10 60

tls-auth /etc/openvpn/movpn/ta.key 0
dh /etc/openvpn/movpn/dh2048.pem
ca /etc/openvpn/movpn/ca.crt
cert /etc/openvpn/movpn/openvpn-server1.xiodi.cn.crt
key /etc/openvpn/movpn/openvpn-server1.xiodi.cn.key

user nobody
group nobody

verb 3
daemon
log-append /var/log/openvpn.log
```

服务器配置第二个选项：开启转发

```
[root@c720245 ~]# echo 1 > /proc/sys/net/ipv4/conf/tap0/proxy_arp_pvlan
```

客户端配置：

```
client
proto tcp
remote 192.168.20.245
port 1198
dev tap
nobind

remote-cert-tls server
tls-auth /etc/openvpn/movpn/ta.key 1
```

ca /etc/openvpn/movpn/ca.crt
cert /etc/openvpn/movpn/openvpn-client1.xiodi.cn.crt
key /etc/openvpn/movpn/openvpn-client1.xiodi.cn.key

进行过滤流量 包:
[root@c720245 ~]# iptables -I FORWARD -i tap0 -0 tap0 -s 10.200.0.2 -d 10.200.0.3 -j DROP

如何使用openvpn的pf过滤器:

使用tap设备进行桥接

Friday, March 15, 2019 5:36 PM

服务器端配置:

```
[root@c720245 ~]# cat /etc/openvpn/movpn/movpn-bridge-start
#!/bin/bash

br="br0"
tap="tap0"
eth="ens19"
br_ip="192.168.30.245"
br_netmask="255.255.255.0"
br_broadcast="192.168.30.255"
openvpn --mktun --dev $tap
brctl addbr $br
brctl addif $br $eth
brctl addif $br $tap

ifconfig $tap 0.0.0.0 promisc up
ifconfig $eth 0.0.0.0 promisc up
ifconfig $br $br_ip netmask $br_netmask broadcast $br_broadcast

[root@c720245 ~]# chmod 755 /etc/openvpn/movpn/movpn-bridge-start

[root@c720245 ~]# sh /etc/openvpn/movpn/movpn-bridge-start

[root@c720245 ~]# cat openvpn-03-13-server.conf
proto tcp
port 1198

dev tap0

server-bridge 192.168.30.245 255.255.255.0 192.168.30.128 192.168.30.200

tls-auth /etc/openvpn/movpn/ta.key 0
dh /etc/openvpn/movpn/dh2048.pem
ca /etc/openvpn/movpn/ca.crt
cert /etc/openvpn/movpn/openvpn-server1.xiodi.cn.crt
key /etc/openvpn/movpn/openvpn-server1.xiodi.cn.key

persist-key
persist-tun
keepalive 10 60

user nobody
group nobody

verb 3
daemon
log-append /var/log/openvpn.log
```

客户端配置文件：

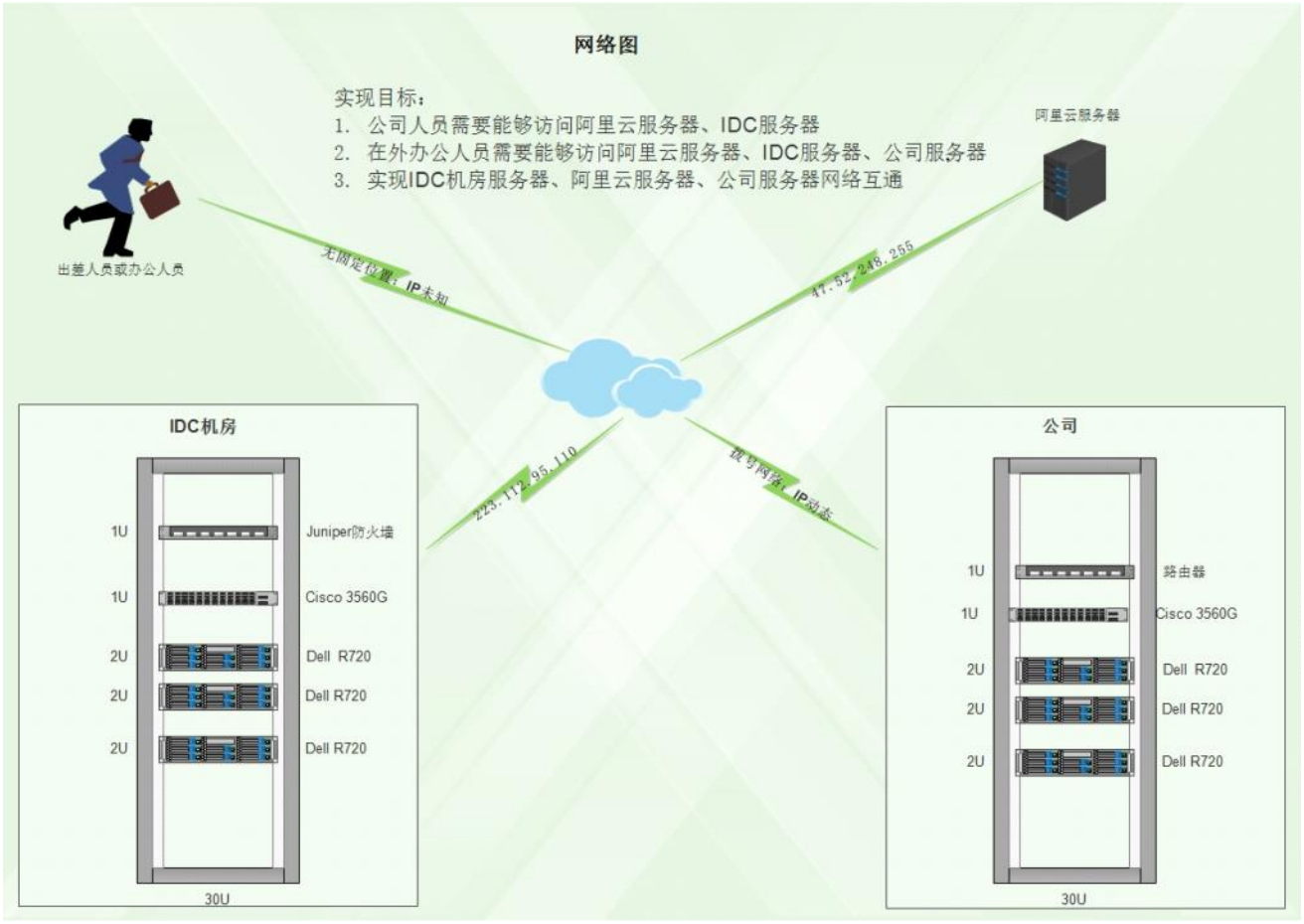
```
[root@c720246 ~]# cat openvpn-03-13-client.conf
proto tcp
port 1198
dev tap

client
remote 192.168.20.245
nobind

remote-cert-tls server
tls-auth /etc/openvpn/movpn/ta.key 1
ca /etc/openvpn/movpn/ca.crt
cert /etc/openvpn/movpn/openvpn-client1.xiodi.cn.crt
key /etc/openvpn/movpn/openvpn-client1.xiodi.cn.key
```

客户端进行校验分配 的IP地址是否和服务器相同的子网。

```
tap0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.30.128  netmask 255.255.255.0  broadcast 192.168.30.255
        inet6 fe80::d42e:2cff:fe4b:6d9  prefixlen 64  scopeid 0x20<link>
        ether d6:2e:2c:4b:06:d9  txqueuelen 100  (Ethernet)
```

OpenVPN在生产环境中的讲解

Friday, March 15, 2019 6:24 PM



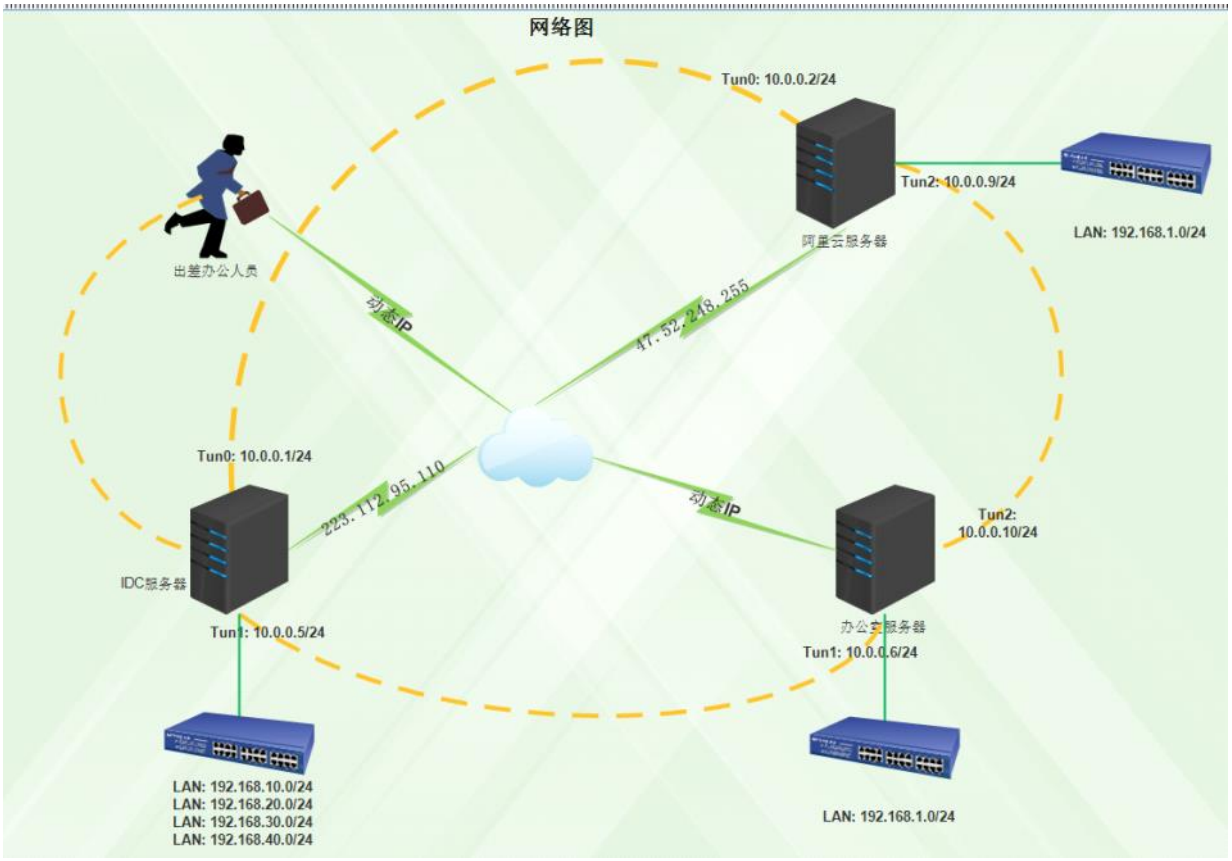
现存的问题：

IDC机房、公司服务器、阿里云服务器网络都相互独立。导致如下问题

1. 没有办法使用一套zabbix较好的监控完整的服务器和网络设备。
2. 无法使用一套ELK对所有服务器和设备进行日志收集、审计等。
3. 给企业实施DevOps方案带来困难。
4. 公司办公人员无法紧急处理公司服务器故障，或有一部分人在自己电脑上安装TeamView临时解决。
5. 由于连接阿里云服务器，IDC服务器（不管是mysql还是其它的服务）都是使用的外网直连。导致网络不安全。

实施步骤分析：

1. 阿里云服务器和IDC机房的服务器实现互通
2. 阿里云服务器和公司的实现互通
3. 公司服务器和阿里云的实现互通
4. 由于公司IP地址非固定 地址，所以移动办公人员连接VPN连入到IDC服务器



一. 环境准备

1. 系统版本

IDC、办公室、阿里云服务器系统版本均一样:

```
[root@c720101 ~]# cat /etc/redhat-release
CentOS Linux release 7.6.1810 (Core)
```

2. OpenVPN版本

```
[root@c720101 ~]# openvpn --version
OpenVPN 2.4.7 x86_64-redhat-linux-gnu [Fedora EPEL patched] [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Feb 20 2019
library versions: OpenSSL 1.0.2k-fips  26 Jan 2017, LZO 2.06
Originally developed by James Yonan
Copyright (C) 2002-2018 OpenVPN Inc <sales@openvpn.net>
Compile time defines: enable_async_push=no enable_comp_stub=no enable_crypto=yes enable_crypto_ofb_cfb=yes enable_debug=yes e nable_def_auth=yes enable_dependency_tracking=no
enable_dlopen=unknown enable_dlopen_self=unknown enable_dlopen_self_static=unknown enable_fast_install=yes enable_fragment=ye s enable_iproute2=yes enable_libtool_lock=yes enable_lz4
=yes enable_lzo=yes enable_management=yes enable_multihome=yes enable_pam_dlopen=no enable_pedantic=no enable_pf=yes enable_p kcs11=yes enable_plugin_auth_pam=yes
enable_plugin_down_root=yes enable_plugins=yes enable_port_share=yes enable_selinux=yes enable_server=yes enable_shared=yes e nable_shared_with_static_runtimes=no enable_small=no
enable_static=yes enable_strict=no enable_strict_options=no enable_systemd=yes enable_werror=no enable_win32_dll=yes enable_x 509_alt_username=yes with_aix_soname=aix
with_crypto_library=openssl with_gnu_ld=yes with_mem_check=no with_sysroot=no
```

3. CA服务器的搭建和签发证书（是放在IDC服务器上的）

3.1 解压缩ssl-admin

```
[root@c720101 ~]# tar -zxvf ssa.tgz
ssl-admin-1.2.1/
ssl-admin-1.2.1/man5/
ssl-admin-1.2.1/man1/
ssl-admin-1.2.1/ssl-admin
ssl-admin-1.2.1/ssl-admin.conf
ssl-admin-1.2.1/Makefile
ssl-admin-1.2.1/configure
ssl-admin-1.2.1/openssl.conf
ssl-admin-1.2.1/ssl-admin-e
ssl-admin-1.2.1/man1/ssl-admin.1
ssl-admin-1.2.1/man1/ssl-admin.1-e
ssl-admin-1.2.1/man5/ssl-admin.conf.5
ssl-admin-1.2.1/man5/ssl-admin.conf.5-e
```

3.2 ssl-admin的安装

```
[root@c720101 ~]# cd ssl-admin-1.2.1/
[root@c720101 ssl-admin-1.2.1]# ./configure
[root@c720101 ssl-admin-1.2.1]# make install
[ -e "//etc/ssl-admin" ] || mkdir -p //etc/ssl-admin
/usr/bin/sed s+~~~ETCDIR~~~+/etc+g man1/ssl-admin.1 > //usr/share/man/man1/ssl-admin.1
/usr/bin/sed s+~~~ETCDIR~~~+/etc+g man5/ssl-admin.conf.5 > //usr/share/man/man5/ssl-admin.conf.5
install -c -m 0660 -S -v ssl-admin.conf //etc/ssl-admin/ssl-admin.conf.sample
```

```
install -c -m 0660 -S -v openssl.conf //etc/ssl-admin/openssl.conf.sample
/usr/bin/sed -e "s+~~~ETCDIR~~~+/etc+g" -e "s+~~~BUILD~~~+prod+g" ssl-admin > ssl-admin.mod
install -c -m 0755 -S -v ssl-admin.mod //usr/bin/ssl-admin
chmod 0444 //etc/ssl-admin/*.conf.sample
```

3.3 ssl-admin的配置

3.3.1 ssl-admin.conf配置

```
[root@c720101 ssl-admin-1.2.1]# cp /etc/ssl-admin/ssl-admin.conf.sample /etc/ssl-admin/ssl-admin.conf
[root@c720101 ssl-admin-1.2.1]# chmod u+w /etc/ssl-admin/ssl-admin.conf
[root@c720101 ssl-admin-1.2.1]# cat /etc/ssl-admin/ssl-admin.conf
## Set default values here.
#
# The following values can be changed without affecting
# your CA key.

$ENV{'KEY_SIZE'} = "1024";
$ENV{'KEY_DAYS'} = "3650";
$ENV{'KEY_CN'} = "";
$ENV{'KEY_CRL_LOC'} = "URI:http://CRL_URI";


## WARNING!!! ##
#
# Changing the following values has vast consequences.
# These values must match what's in your root CA certificate.

$ENV{'KEY_COUNTRY'} = "CN";                    #修改此值，国家简写
$ENV{'KEY_PROVINCE'} = "JiangSu";              # 填写省份
$ENV{'KEY_CITY'} = "SuZhou";                   # 填写城市
$ENV{'KEY_ORG'} = "IT";                        # 填 写组织
$ENV{'KEY_EMAIL'} = 'zangxueyuan@126.com';     # 填写邮箱地址
```

3.3.2 openssl.conf配置

```
[root@c720101 ssl-admin-1.2.1]# cp /etc/ssl-admin/openssl.conf.sample /etc/ssl-admin/openssl.conf
[root@c720101 ssl-admin-1.2.1]# chmod u+w /etc/ssl-admin/openssl.conf
[root@c720101 ssl-admin-1.2.1]# cat /etc/ssl-admin/openssl.conf
# OpenSSL Configuration File for ssl-admin

dir                             = $ENV::KEY_DIR

[ca]
default_ca                      = CA_default

[CA_default]
serial                          = $dir/prog/serial
database                        = $dir/prog/index.txt
new_certs_dir                   = $dir/active
certificate                     = $dir/active/ca.crt
private_key                     = $dir/active/ca.key
default_days                    = $ENV::KEY_DAYS
default_crl_days                = 30
default_md                      = sha256                        # 更改为sha256
preserve                        = no
email_in_dn                     = yes
nameopt                                 = default_ca
certopt                         = default_ca
policy                          = policy_match

[ policy_match ]
countryName                     = match
stateOrProvinceName             = match
organizationName                = match
organizationalUnitName                  = optional
commonName                      = supplied
emailAddress                    = optional

[ policy_new_ca]
countryName                     = supplied
stateOrProvinceName             = supplied
organizationName                = supplied
organizationalUnitName                  = optional
commonName                      = supplied
emailAddress                    = optional


[ req ]
default_bits                    = $ENV::KEY_SIZE
default_keyfile         = privkey.pem
default_md                      = sha256                        #更改为sha256
string_mask                     = nombstr
distinguished_name              = req_distinguished_name
req_extensions                  = v3_req

[ req_distinguished_name ]
# Prompts
countryName                     = Country Name (2 letter code)
countryName_min                         = 2
countryName_max                         = 2
stateOrProvinceName             = State or Province Name (full name)
localityName                    = Locality Name (eg, city)
0.organizationName              = Organization Name (eg, company)
organizationalUnitName                  = Organizational Unit Name (eg, section)
```

```
commonName                      = Common Name (web address or username)
commonName_max                          = 64
emailAddress                    = Email Address
emailAddress_max                = 40

# Default Variables (environment variables set from ssl-admin.pl script.
countryName_default             = $ENV::KEY_COUNTRY
commonName_default              = $ENV::KEY_CN
emailAddress_default            = $ENV::KEY_EMAIL
0.organizationName_default      = $ENV::KEY_ORG
stateOrProvinceName_default     = $ENV::KEY_PROVINCE
localityName_default            = $ENV::KEY_CITY

[ server ]

# JY ADDED -- Make a cert with nsCertType set to "server"
basicConstraints=CA:FALSE
nsCertType                      = server
nsComment                       = "ssl-admin (OpenSSL) Generated Server Certificate"
subjectKeyIdentifier            = hash
authorityKeyIdentifier          = keyid,issuer:always
extendedKeyUsage                = serverAuth
keyUsage                        = digitalSignature, keyEncipherment

[ v3_req ]
basicConstraints                = CA:FALSE
keyUsage                        = keyAgreement, nonRepudiation, digitalSignature, keyEncipherment
extendedKeyUsage                = clientAuth
crlDistributionPoints           = $ENV::KEY_CRL_LOC

[ v3_ca ]
basicConstraints                = CA:TRUE
subjectKeyIdentifier            = hash
authorityKeyIdentifier          = keyid:always,issuer:always
crlDistributionPoints           = $ENV::KEY_CRL_LOC
```

3.3.3 安装 Perl

```
[root@c720101 ssl-admin-1.2.1]# yum install perl -y
```

3.4 产生CA证书、服务器证书、客户端证书

```
[root@c720101 active]# ls -al
total 60
drwxr-x--- 2 root root 4096 Mar 15 21:22 .
drwxr-xr-x 7 root root  172 Mar 15 21:22 ..
-rw-r--r-- 1 root root 1229 Mar 15 21:19 ca.crt
-rw-r--r-- 1 root root  887 Mar 15 21:19 ca.key
-rw-r--r-- 1 root root 3846 Mar 15 21:21 openvpn-ali.xiodi.cn.crt
-rw-r--r-- 1 root root  916 Mar 15 21:21 openvpn-ali.xiodi.cn.key
-rw-r--r-- 1 root root 3846 Mar 15 21:21 openvpn-ali.xiodi.cn.pem
-rw-r--r-- 1 root root 2579 Mar 15 21:22 openvpn-client.xiodi.cn.crt
-rw-r--r-- 1 root root  916 Mar 15 21:22 openvpn-client.xiodi.cn.key
-rw-r--r-- 1 root root 2579 Mar 15 21:22 openvpn-client.xiodi.cn.pem
-rw-r--r-- 1 root root 3846 Mar 15 21:21 openvpn-com.xiodi.cn.crt
-rw-r--r-- 1 root root  916 Mar 15 21:21 openvpn-com.xiodi.cn.key
-rw-r--r-- 1 root root 3846 Mar 15 21:21 openvpn-com.xiodi.cn.pem
-rw-r--r-- 1 root root 3846 Mar 15 21:20 openvpn-idc.xiodi.cn.crt
-rw-r--r-- 1 root root  912 Mar 15 21:20 openvpn-idc.xiodi.cn.key
-rw-r--r-- 1 root root 3846 Mar 15 21:20 openvpn-idc.xiodi.cn.pem
```

4. 产生tls-auth证书和dh证书

```
[root@c720101 active]# openvpn --genkey --secret ta.key --keysize 512
[root@c720101 active]# openssl dhparam -out dh2048.pem 2048
```

5. 在防火墙和阿里云上上放行到端口1200

6. 阿里云服务器和IDC服务器实现互通

6.1 IDC服务器配置

```
[root@c720101 active]# cat /etc/openvpn/server/idc-to-ali.conf
proto tcp-server
dev tun
local 192.168.20.101
lport 1200
remote 47.52.248.255
rport 1200
ifconfig 10.0.0.1 10.0.0.2
tls-server
tls-auth /etc/openvpn/cert/ta.key 0
dh /etc/openvpn/cert/dh2048.pem
ca /etc/openvpn/cert/ca.crt
cert /etc/openvpn/cert/openvpn-server1.xiodi.cn.crt
key /etc/openvpn/cert/openvpn-server1.xiodi.cn.key

persist-key
persist-tun

cipher AES256
auth SHA512

route 172.31.115.0 255.255.255.0
keepalive 10 60
ping-timer-rem

verb 3
```

daemon

log-append /var/log/openvpn-idc.log

6.2 阿里云服务器配置

```
[root@iZj6cd7yvpa3j0rjyou4l5Z ~]# cat /etc/openvpn/client/Ali-to-Idc.conf
proto tcp-client
local 172.31.115.185
lport 1200
remote 223.112.95.110
rport 1200
dev tun
ifconfig 10.0.0.2 10.0.0.1
remote-cert-tls server
tls-client
tls-auth /etc/openvpn/cert/ta.key 1
ca /etc/openvpn/cert/ca.crt
cert /etc/openvpn/cert/openvpn-client1.xiodi.cn.crt
key /etc/openvpn/cert/openvpn-client1.xiodi.cn.key
persist-key
persist-tun

cipher AES256
auth SHA512

route 192.168.10.0 255.255.255.0
route 192.168.20.0 255.255.255.0
route 192.168.30.0 255.255.255.0
route 192.168.40.0 255.255.255.0
keepalive 10 60
ping-timer-rem

verb 3
daemon

log-append /var/log/openvpn-idc.log
```

6.3 在IDC的openvpn服务器和阿里云的IDC 服务器均开启转发

6.3.1 编辑/etc/sysctl.conf文件，添加发下行：

```
net.ipv4.ip_forward = 1
```

6.3.2 加载文件

```
[root@c720101 active]# sysctl -p
net.ipv4.ip_forward = 1
```

6.4 在网关上配置路由（我这里网关是三层交换机）

```
switch3560-1(config)#ip route 172.31.115.0 255.255.255.0 192.168.20.101
switch3560-1(config)#ip route 10.0.0.0 255.255.255.0 192.168.20.101
```

7. 阿里云服务器和公司的实现互通

7.1 首先在阿里云服务器和办公室的路由器上，放行1201端口。

7.2 阿里云服务器配置：

```
proto tcp-server
port 1201
rport 1201
dev tun
ifconfig 10.0.0.9 10.0.0.10
tls-server
tls-auth /etc/openvpn/cert/ta.key 0
dh /etc/openvpn/cert/dh2048.pem
ca /etc/openvpn/cert/ca.crt
cert /etc/openvpn/cert/openvpn-server1.xiodi.cn.crt
key /etc/openvpn/cert/openvpn-server1.xiodi.cn.key

persist-key
persist-tun

cipher AES256
auth SHA512

route 192.168.1.0 255.255.255.0
keepalive 10 60
ping-timer-rem

verb 3
daemon

log-append /var/log/openvpn-office.log
```

7.3 公司服务器配置：（动态IP地址）

```
proto tcp-client
dev tun
remote 47.52.248.255
rport 1201
lport 1201
ifconfig 10.0.0.10 10.0.0.9
tls-client
```

```
tls-auth /etc/openvpn/cert/ta.key 1
dh /etc/openvpn/cert/dh2048.pem
ca /etc/openvpn/cert/ca.crt
cert /etc/openvpn/cert/openvpn-client1.xiodi.cn.crt
key /etc/openvpn/cert/openvpn-client1.xiodi.cn.key
tun-mtu 1600

persist-key
persist-tun

cipher AES256
auth SHA512

route 172.31.115.0 255.255.255.0
keepalive 10 60
ping-timer-rem

verb 3
daemon

log-append /var/log/openvpn-office.log
```

7.4 在公司服务器上开启转发：

```
[root@test1 cert]# cat /etc/sysctl.conf
net.ipv4.ip_forward = 1

[root@test1 cert]# sysctl -p
```

7.5 在公司的路由器上写路由

8. 公司服务器和阿里云服务器的互通

8.1 首先需要在IDC的防火墙上的公司的路由器上放行1202端口。

8.2 IDC服务器配置

```
proto tcp-server
port 1202
rport 1202
dev tun
ifconfig 10.0.0.5 10.0.0.6
tls-server
tls-auth /etc/openvpn/cert/ta.key 0
dh /etc/openvpn/cert/dh2048.pem
ca /etc/openvpn/cert/ca.crt
cert /etc/openvpn/cert/openvpn-server1.xiodi.cn.crt
key /etc/openvpn/cert/openvpn-server1.xiodi.cn.key

persist-key
persist-tun

cipher AES256
auth SHA512

route 192.168.1.0 255.255.255.0
keepalive 10 60
ping-timer-rem

verb 3
daemon

log-append /var/log/openvpn-idc-to-office.log
```

8.2 在公司服务器上的配置

```
[root@test1 cert]# cat /etc/openvpn/client/office-to-idc.conf
proto tcp-client
dev tun
remote 223.112.95.110
rport 1202
lport 1202
ifconfig 10.0.0.6 10.0.0.5
tls-client
tls-auth /etc/openvpn/cert/ta.key 1
dh /etc/openvpn/cert/dh2048.pem
ca /etc/openvpn/cert/ca.crt
cert /etc/openvpn/cert/openvpn-client1.xiodi.cn.crt
key /etc/openvpn/cert/openvpn-client1.xiodi.cn.key
tun-mtu 1600

persist-key
persist-tun

cipher AES256
auth SHA512

route 192.168.20.0 255.255.255.0
route 192.168.30.0 255.255.255.0
route 192.168.40.0 255.255.255.0
keepalive 10 60
ping-timer-rem

verb 3
```

```
daemon

log-append /var/log/openvpn-office.log
```

8.3 在公司路由器上和IDC的防火墙上写路由。

9. 办公人员连接IDC VPN服务器

9.1 首先IDC的防火墙上放行1203端口

9.2 服务器端配置如下：

```
[root@c720101 ~]# cat /etc/openvpn/server/access-server.conf
proto tcp
port 1203
dev tun
server 10.1.0.0 255.255.255.0
topology subnet
persist-key
persist-tun
keepalive 10 60

tls-auth /etc/openvpn/cert/ta.key 0
dh /etc/openvpn/cert/dh2048.pem
ca /etc/openvpn/cert/ca.crt
cert /etc/openvpn/cert/openvpn-server1.xiodi.cn.crt
key /etc/openvpn/cert/openvpn-server1.xiodi.cn.key

verb 3
daemon
log-append /var/log/openvpn-access-server.log

push "route 192.168.10.0 255.255.255.0"
push "route 192.168.20.0 255.255.255.0"
push "route 192.168.30.0 255.255.255.0"
push "route 192.168.40.0 255.255.255.0"
push "route 172.31.115.0 255.255.255.0"
push "route 192.168.1.0 255.255.255.0"
push "dhcp-option DNS 192.168.20.250"

plugin /usr/lib64/openvpn/plugin/lib/openvpn-auth-ldap.so "/etc/openvpn/server/openldap.conf cn=%u"


[root@c720101 ~]# cat /etc/openvpn/server/openldap.conf
<LDAP>
  URL             ldaps://openldap.xiodi.cn
  Timeout         15
  TLSEnable       no
  FollowReferrals  yes
  BindDN          "cn=client search,ou=admin,dc=xiodi,dc=cn"
  Password        xiodi.cn
</LDAP>

<Authorization>
  BaseDN        "ou=people,dc=xiodi,dc=cn"
  SearchFilter      "(uid=%u)"
  RequireGroup  false
</Authorization>
```

客户端配置如下：

```
client
proto tcp
remote 223.112.95.110
port 1203
dev tun
nobind

remote-cert-tls server
tls-auth ta.key 1
ca ca.crt
cert jack.xiodi.cn.crt
key jack.xiodi.cn.key
auth-user-pass
```