openvpn部署之部署基于AD域认证访问内网

# 安装环境

Centos6.

# 步骤

## 1.添加fedora的yum源

rpm -ivh http://mirrors.ustc.edu.cn/fedora/epel/6/x86\_64/epel-release-6-8.noarch.rpm

## 2.安装openvpn

yum install openvpn -y

yum -y install openssl openssl-devel -y

yum -y install lzo lzo-devel -y

yum install -y libgcrypt libgpg-error libgcrypt-devel

## 3.安装openvpn认证插件

yum install openvpn-auth-ldap -y

## 4.安装easy-rsa

由于openvpn2.3之后，在openvpn里面剔除了easy-rsa文件，所以需要单独安装

yum install easy-rsa

cp -rf /usr/share/easy-rsa/2.0 /etc/opevpn/easy-rsa

## 5.生成openvpn的key及证书

修改/opt/openvpn/etc/easy-rsa/2.0/vars参数

shell#vi vars

export KEY\_COUNTRY="CN" 国家

export KEY\_PROVINCE="ZJ" 省份

export KEY\_CITY="NingBo" 城市

export KEY\_ORG="TEST-VPN" 组织

exportKEY\_EMAIL="81367070@qq.com" 邮件

export KEY\_OU="baidu" 单位

保存退出

source vars 或者 . ./vars(两个点之间有空格) # 初始化命令

./clean-all #初始化，删除原证书文件

./build-ca #制作ca证书

./build-dh #

./build-key-server server #制作服务器证书

./build-key client #制作客户端证书

# 6.编辑openvpn服务端配置文件：

shell#cat /etc/openvpn/server.conf

port 1194

proto tcp

dev tun

ca keys/ca.crt

cert keys/server.crt

key keys/server.key # This file should be kept secret

dh keys/dh2048.pem

server 10.8.0.0 255.255.255.0 //客户端分配的ip地址

push "route 172.20.17.0 255.255.255.0" //推送客户端的路由

push "route 172.20.18.0 255.255.255.0"

push "route 172.20.19.0 255.255.255.0"

push "route 172.20.20.0 255.255.255.0"

push "route 172.20.22.0 255.255.255.0"

push "redirect-gateway" //修改客户端的网关，使其直接走vpn流量

ifconfig-pool-persist ipp.txt

keepalive 10 120

comp-lzo

persist-key

persist-tun

status openvpn-status.log

verb 3

plugin /usr/lib64/openvpn/plugin/lib/openvpn-auth-ldap.so "/etc/openvpn/auth/ldap.conf"

client-cert-not-required

username-as-common-name

log /var/log/openvpn.log

# 7.修改openvpn-ldap-auth的配置文件：

vi /etc/openvpn/auth/ldap.conf

<LDAP>

# LDAP server URL

#更改为AD服务器的ip

URL ldap://172.20.20.10:389

# Bind DN (If your LDAP server doesn't support anonymous binds)

# BindDN uid=Manager,ou=People,dc=example,dc=com

#更改为域管理的dn,可以通过ldapsearch进行查询,-h的ip替换为服务器ip，-d换为管理员的dn，-b为基础的查询dn，\*为所有

#ldapsearch -LLL -x -h 172.16.76.238 -D "administrator@xx.com" -W -b "dc=xx,dc=com" "\*"

BindDN " cn=administrator,cn=users,dc=dealeasy,dc=local"

# Bind Password

# Password SecretPassword

#域管理员的密码

Password passwd

# Network timeout (in seconds)

Timeout 15

# Enable Start TLS

TLSEnable no

# Follow LDAP Referrals (anonymously)

FollowReferrals no

# TLS CA Certificate File

#TLSCACertFile /usr/local/etc/ssl/ca.pem

# TLS CA Certificate Directory

#TLSCACertDir /etc/ssl/certs

# Client Certificate and key

# If TLS client authentication is required

#TLSCertFile /usr/local/etc/ssl/client-cert.pem

#TLSKeyFile /usr/local/etc/ssl/client-key.pem

# Cipher Suite

# The defaults are usually fine here

# TLSCipherSuite ALL:!ADH:@STRENGTH

</LDAP>

<Authorization>

# Base DN

#查询认证的基础dn

BaseDN " ou=de,dc=dealeasy,dc=local"

# User Search Filter

#SearchFilter "(&(uid=%u)(accountStatus=active))"

#其中sAMAccountName=%u的意思是把sAMAccountName的字段取值为用户名，后面“memberof=CN=myvpn,DC=xx,DC=com”指向要认证的vpn用户组，这样任何用户使用vpn，只要加入这个组就好了

SearchFilter "( (&(sAMAccountName=%u)(memberof=cn=myvpn,ou=vpn,ou=de,DC=dealeasy,DC=local"

# Require Group Membership

RequireGroup false

# Add non-group members to a PF table (disabled)

#PFTable ips\_vpn\_users

<Group>

#BaseDN "ou=Groups,dc=example,dc=com"

#SearchFilter "(|(cn=developers)(cn=artists))"

#MemberAttribute uniqueMember

# Add group members to a PF table (disabled)

#PFTable ips\_vpn\_eng

BaseDN " ou=vpn,ou=de,dc=dealeasy,dc=local"

SearchFilter " (cn=myvpn)"

MemberAttribute "member"

</Group>

</Authorization>

# 8.拷贝/etc/openvpn/key目录下的ca.crt证书，以备客户端使用。

**注：客户端使用ca.crt和客户端配置文件即可正常使用openvpn了**

## 配置客户端配置文件

#vi client.ovpn

client

dev tun

proto tcp //注意协议，跟服务器保持一致

remote 172.20.20.25 1194 //xx.xx.com替换为你的服务器ip

resolv-retry infinite

nobind

persist-key

persist-tun

ca ca.crt

auth-user-pass //客户端使用账户密码登陆的选项，用于客户端弹出认证用户的窗口

comp-lzo

verb 3

# 开启路由转发

vi /etc/sysctl.conf

1. 修改参数
2. net.ipv4.ip\_forward = 1 （默认为0，修改成1 表示开启路由转发，如果默认是空内容，请自行加上-腾讯云貌似就是空的）

重启sysctl生效路由转发：

sysctl -p

### 配置防火墙及路由转发策略：

iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o eth0 -j MASQUERADE

#做NAT转换

iptables -A INPUT -p TCP --dport 1194 -j ACCEPT #OpenVPN服务端口，可自定义，不可冲突

service iptables save

service iptables restart

#### 此处为策略转发示例2：

#### 配置内核路由转发和iptables转发：

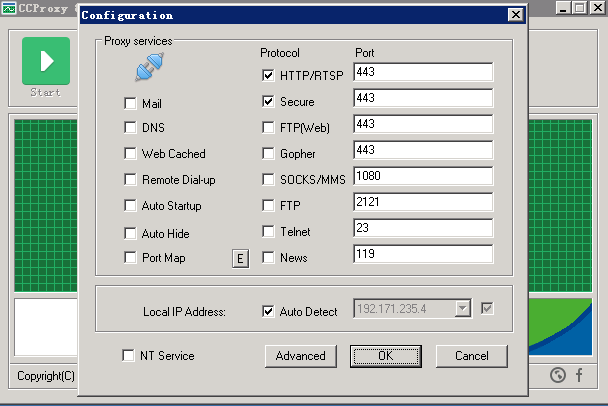
1. # sed -i '/net.ipv4.ip\_forward/s/0/1/' /etc/sysctl.conf
2. # sysctl -p
3. //可以先去熟悉如何定义iptables策略
4. # vi /etc/sysconfig/iptables（红色部分表示重要的策略）
5. # Generated by iptables-save v1.4.7 on Mon Nov  2 19:19:12 2015
6. \*nat
7. :PREROUTING ACCEPT [0:0]
8. :POSTROUTING ACCEPT [0:0]
9. :OUTPUT ACCEPT [0:0]
10. #不允许访问10.0.9/8/7/6.\*网段，这是因为内网网络是跟另外一个网络建立了vpn连接，所以不想用Openvpn直接访问另外一个网络
11. -A PREROUTING -d 10.0.9.0/24 -p tcp -m tcp --dport 22 -j DNAT --to-destination 127.0.0.1
12. -A PREROUTING -d 10.0.8.0/27 -p tcp -m tcp --dport 22 -j DNAT --to-destination 127.0.0.1
13. -A PREROUTING -d 10.0.8.128/25 -p tcp -m tcp --dport 22 -j DNAT --to-destination 127.0.0.1
14. -A PREROUTING -d 10.0.8.32/27 -p tcp -m tcp --dport 22 -j DNAT --to-destination 127.0.0.1
15. -A PREROUTING -d 10.0.8.64/27 -p tcp -m tcp --dport 22 -j DNAT --to-destination 127.0.0.1
16. -A PREROUTING -d 10.0.7.0/25 -p tcp -m tcp --dport 22 -j DNAT --to-destination 127.0.0.1
17. -A PREROUTING -d 10.0.7.128/26 -p tcp -m tcp --dport 22 -j DNAT --to-destination 127.0.0.1
18. -A PREROUTING -d 10.0.7.192/26 -p tcp -m tcp --dport 22 -j DNAT --to-destination 127.0.0.1
19. -A PREROUTING -d 10.0.6.0/26 -p tcp -m tcp --dport 22 -j DNAT --to-destination 127.0.0.1
20. -A PREROUTING -d 10.0.6.64/26 -p tcp -m tcp --dport 22 -j DNAT --to-destination 127.0.0.1
21. -A PREROUTING -d 10.0.6.128/26 -p tcp -m tcp --dport 22 -j DNAT --to-destination 127.0.0.1
22. -A PREROUTING -d 10.0.6.192/26 -p tcp -m tcp --dport 22 -j DNAT --to-destination 127.0.0.1
23. #伪装10.10.10.0/24的数据
24. -A POSTROUTING -s 10.10.10.0/24 -o eth0 -j MASQUERADE
25. #地址转换
26. -A POSTROUTING -s 10.10.10.0/24 -d 172.16.112.0/24 -j SNAT --to-source 172.16.112.171
27. COMMIT
28. # Completed on Mon Nov  2 19:19:12 2015
29. # Generated by iptables-save v1.4.7 on Mon Nov  2 19:19:12 2015
30. \*filter
31. :INPUT ACCEPT [603:48381]
32. :FORWARD ACCEPT [594:717393]
33. :OUTPUT ACCEPT [1777:901584]
34. -A INPUT -i lo -j ACCEPT
35. -A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
36. -A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
37. -A INPUT -p tcp -m tcp --dport 389 -j ACCEPT
38. -A INPUT -p tcp -m tcp --dport 943 -j ACCEPT
39. -A INPUT -p tcp -m tcp --dport 8080 -j ACCEPT
40. -A INPUT -p tcp -m tcp --dport 8088 -j ACCEPT
41. -A INPUT -p tcp -m tcp --dport 3306 -j ACCEPT
42. -A INPUT -p tcp -m tcp --dport 3389 -j ACCEPT
43. -A INPUT -p icmp -m icmp --icmp-type 8 -j ACCEPT
44. -A INPUT -m state --state ESTABLISHED -j ACCEPT
45. -A INPUT -s 172.16.112.0/24 -p tcp -j ACCEPT
46. -A INPUT -s 172.16.113.0/24 -p tcp -j ACCEPT
47. -A INPUT -s 172.16.114.0/24 -p tcp -j ACCEPT
48. -A INPUT -s 192.168.21.0/24 -p tcp -j ACCEPT
49. -A INPUT -s 10.10.10.0/24 -d 172.16.112.0/24 -i eth0 -p tcp -m tcp --dport 1194 -j ACCEPT
50. -A INPUT -i tun0 -j ACCEPT
51. -A FORWARD -i tun0 -j ACCEPT
52. COMMIT
53. # Completed on Mon Nov  2 19:19:12 2015
54. # service openvpn start
55. # chkconfig openvpn on
56. # chkconfig iptables on
57. # service iptables restart

# 开启 HTTP代理连接openvpn服务器

通过此方法可以解决跨运营商连接中断及缓慢的问题，首先需要有一台三网HTTP代理服务器。公司使用的是景安的云服务器做HTTP代理。

参考资料：<http://www.365mini.com/page/18.htm>

1. 在景安云服务器部署代理软件CCProxy,并开启HTTP代理，端口443（可自定义）。



1. 在客户端配置文件添加如下语句。

http-proxy 122.114.100.229 443

或者在客户端手动配置（如图）



配置完成。可以正常连接使用。