vpn ----- virtual Private network 虚拟专用网

实现：

隧道技术 tunnel

数据加密技术保证安全性

作用：跨互联网访问公司内网的资源

类型：

IPSEC VPN 配置网络设备(路由器、硬件防火墙)

总部、分部的通信

远程访问VPN remote access vpn

适用于在家办公人员、出差人员

ssl vpn

easy vpn

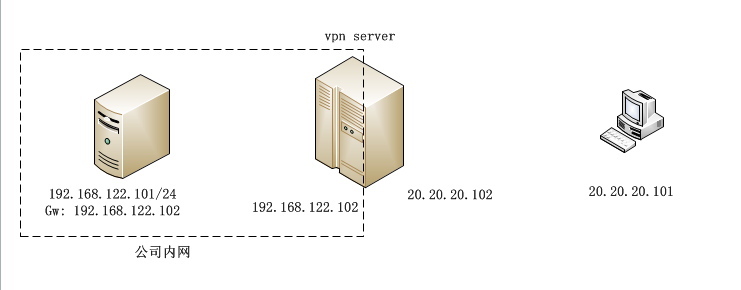
MPLS VPN

能源

Linux服务器

openvpn软件

数据安全性的保证：证书



配置vpn\_server

1、配置yum源，安装openvpn软件

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

2、生成CA的自签、vpn server的证书、客户端证书

[root@vpn\_server ~]# cp -r /usr/share/easy-rsa/ /etc/openvpn/

[root@vpn\_server ~]# ls /etc/openvpn/

client easy-rsa server

[root@vpn\_server ~]# vim /etc/openvpn/easy-rsa/2.0/vars

64 export KEY\_COUNTRY="cn"

65 export KEY\_PROVINCE="cn"

66 export KEY\_CITY="bj"

67 export KEY\_ORG="uplooking"

68 export KEY\_EMAIL="uplooking@qq.com"

69 export KEY\_OU="uplooking"

[root@vpn\_server ~]# cd /etc/openvpn/easy-rsa/2.0/

[root@vpn\_server 2.0]# source vars

NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/openvpn/easy-rsa/2.0/keys

生成keys目录，用于存放证书

[root@vpn\_server 2.0]# ./clean-all

注意：只有第一次部署openvpn服务器需要的执行，再次执行时， 它会删除keys

1) 生成CA的自签证书

[root@vpn\_server 2.0]# ./build-ca server

[root@vpn\_server 2.0]# ls keys/

ca.crt ca.key index.txt serial

2) 生成vpn服务器证书

[root@vpn\_server 2.0]# ./build-key-server server

[root@vpn\_server 2.0]# ls keys/

01.pem ca.crt ca.key index.txt index.txt.attr index.txt.old serial serial.old server.crt server.csr server.key

3) 生成客户端的证书

[root@vpn\_server 2.0]# ./build-key client

[root@vpn\_server 2.0]# ls keys/

01.pem ca.crt client.crt client.key index.txt.attr index.txt.old serial.old server.csr

02.pem ca.key client.csr index.txt index.txt.attr.old serial server.crt server.key

3、使用DH算法生成密钥

[root@vpn\_server 2.0]# ./build-dh

[root@vpn\_server 2.0]# ls keys/

01.pem ca.crt client.crt client.key index.txt index.txt.attr.old serial server.crt server.key

02.pem ca.key client.csr dh2048.pem index.txt.attr index.txt.old serial.old server.csr

4、复制openvpn配置文件

[root@vpn\_server ~]# cp /usr/share/doc/openvpn-2.4.3/sample/sample-config-files/server.conf /etc/openvpn/

5、编辑server.conf配置文件

[root@vpn\_server ~]# vim /etc/openvpn/server.conf

25 local 20.20.20.102

32 port 1194

36 proto udp

53 dev tun

78 ca /etc/openvpn/easy-rsa/2.0/keys/ca.crt

79 cert /etc/openvpn/easy-rsa/2.0/keys/server.crt

80 key /etc/openvpn/easy-rsa/2.0/keys/server.key

85 dh /etc/openvpn/easy-rsa/2.0/keys/dh2048.pem

101 server 10.8.0.0 255.255.255.0 ///不能与内网现有的任何网段冲突

142 push "route 192.168.122.0 255.255.255.0" //指定允许客户端访问内网的哪些网段的主机

267 max-clients 100 //并发连接数

296 log /var/log/openvpn.log

注释tls配置

# tls-auth ta.key 0 //取消使用tls加密机制

5、启动openvpn服务

[root@vpn\_server log]# /usr/sbin/openvpn --config /etc/openvpn/server.conf &

[root@vpn\_server log]# netstat -anup

Active Internet connections (servers and established)

Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name

udp 0 0 20.20.20.102:1194 0.0.0.0:\* 1881/openvpn

服务器端启动vpn服务器，会多一块tun0的虚拟网卡

6、通过iptables防火墙配置隧道分离

[root@vpn\_server ~]# echo 1 > /proc/sys/net/ipv4/ip\_forward

[root@vpn\_server ~]# echo 1 > /proc/sys/net/ipv4/ip\_forward

[root@vpn\_server ~]# iptables -t nat -A POSTROUTING -s 10.8.0.0 -j MASQUERADE

[root@vpn\_server ~]#

客户端连接vpn服务器：

确保时间一致

Linux客户端连接openvpn服务器

1、安装openvpn客户端软件

[root@client\_01 ~]# yum install -y openvpn

2、将服务器端生成的证书拷贝到客户端

[root@vpn\_server ~]# rsync -av /etc/openvpn/easy-rsa/2.0/keys/{ca.crt,client.crt,client.key} 20.20.20.101:/etc/openvpn/

3、复制客户端，修改配置文件连接vpn

[root@client\_01 ~]# cp /usr/share/doc/openvpn-2.4.3/sample/sample-config-files/client.conf /etc/openvpn/

[root@client\_01 ~]# vim /etc/openvpn/client.conf

remote 20.20.20.102 1194 //指定vpn服务器的连接地址及端口

ca /etc/openvpn/ca.crt

cert /etc/openvpn/client.crt

key /etc/openvpn/client.key

注释掉tls-auth

4、连接vpn服务器

[root@client\_01 ~]# /usr/sbin/openvpn --config /etc/openvpn/client.conf &

Fri Sep 14 16:14:56 2018 Initialization Sequence Completed

[root@client\_01 ~]# ping 192.168.122.101

PING 192.168.122.101 (192.168.122.101) 56(84) bytes of data.

64 bytes from 192.168.122.101: icmp\_seq=1 ttl=63 time=1.85 ms

64 bytes from 192.168.122.101: icmp\_seq=2 ttl=63 time=1.67 ms

[root@client\_01 ~]# ifconfig

tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500

inet 10.8.0.6 netmask 255.255.255.255 destination 10.8.0.5

unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 100 (UNSPEC)

RX packets 4 bytes 336 (336.0 B)

[root@client\_01 ~]# route -n

Kernel IP routing table

Destination Gateway Genmask Flags Metric Ref Use Iface

10.8.0.1 10.8.0.5 255.255.255.255 UGH 0 0 0 tun0

10.8.0.5 0.0.0.0 255.255.255.255 UH 0 0 0 tun0

20.20.20.0 0.0.0.0 255.255.255.0 U 100 0 0 eth0

192.168.122.0 10.8.0.5 255.255.255.0 UG 0 0 0 tun0

windows客户端连接openvpn：

1、windows安装openvpn客户端软件

2、将ca.cert, client.crt, client.key放到openvpn安装目录下的config目录