Vpn配置（支持l2tp协议）

参考文档：

http://blog.jobbole.com/24004/

**先安装Openswan**：

yum install -y ppp iptables make gcc gmp-devel xmlto bison flex xmlto libpcap-devel lsof

#安装依赖关系

获取安装资源：

wget <https://download.openswan.org/openswan/openswan-latest.tar.gz>

tar -zxf openswan-latest.tar.gz

cd openswan-2.6.49.1/

make programs install

安装时候自动创建的目录：



再安装xL2TPD

**默认的软件包在yum源中没有的需要安装epel扩展源**

rpm -Uvh <http://mirrors.kernel.org/fedora-epel/6/x86_64/epel-release-6-8.noarch.rpm>

yum install xl2tpd -y

**修改ipsec配置:**

vim /etc/ipsec.conf

内容后补

config setup

nat\_traversal=yes

virtual\_private=%v4:10.0.0.0/8,%v4:192.168.0.0/16,%v4:172.16.0.0/12

oe=off

protostack=netkey

conn L2TP-PSK-NAT

rightsubnet=vhost:%priv

also=L2TP-PSK-noNAT

conn L2TP-PSK-noNAT

authby=secret

pfs=no

auto=add

keyingtries=3

rekey=no

ikelifetime=8h

keylife=1h

type=transport

left=xxx.xxx.xxx.xxx

leftprotoport=17/1701

right=%any

注意缩进语法：

其中xxx.xxx.xxx.xxx为服务器的外网地址

设置key:（一种安装机制）

vim /etc/ipsec.secrets

112.126.72.190 %any: PSK "yunshididai666"

密码可以随机设置一个，这个密码是服务内部认证，外部是不需要使用的

**修改/etc/sysctl.conf，开启路由功能**

|  |  |
| --- | --- |
| 2 | net.ipv4.ip\_forward = 1    vm.swappiness = 0  net.ipv4.neigh.default.gc\_stale\_time=120  net.ipv4.conf.all.rp\_filter=0  net.ipv4.conf.default.rp\_filter=0  net.ipv4.conf.default.arp\_announce = 2  net.ipv4.conf.lo.arp\_announce=2  net.ipv4.conf.all.arp\_announce=2  net.ipv4.tcp\_max\_tw\_buckets = 5000  net.ipv4.tcp\_syncookies = 1  net.ipv4.tcp\_max\_syn\_backlog = 1024  net.ipv4.tcp\_synack\_retries = 2  net.ipv6.conf.all.disable\_ipv6 = 1  net.ipv6.conf.default.disable\_ipv6 = 1  net.ipv6.conf.lo.disable\_ipv6 = 1  net.ipv4.conf.default.accept\_source\_route = 0  net.ipv4.conf.all.send\_redirects = 0  net.ipv4.conf.default.send\_redirects = 0  net.ipv4.conf.all.log\_martians = 0  net.ipv4.conf.default.log\_martians = 0  net.ipv4.conf.all.accept\_redirects = 0  net.ipv4.conf.default.accept\_redirects = 0  net.ipv4.icmp\_ignore\_bogus\_error\_responses = 1 |

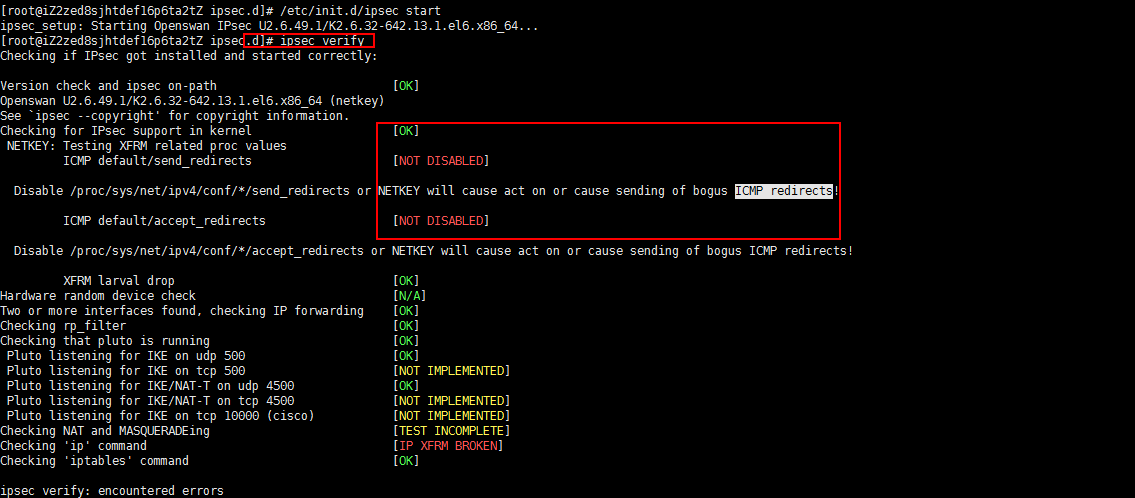
**刷新配置**

sysctl -p

service ipsec start

下面的操作是进行验证，建议在这里先不要验证因为我们还有很多配置没有配置完成

ipsec verify



for vpn in /proc/sys/net/ipv4/conf/\*;do echo 0 > $vpn/accept\_redirects;echo 0 > $vpn/send\_redirects;done

**修改xl2tpd配置：**

[root@iZ2558f2cl2Z ~]# cat /etc/xl2tpd/xl2tpd.conf | grep -v '^;'

[global]

ipsec saref = yes

listen-addr = 101.201.120.17 #修改为自己的外网地址

[lns default]

ip range = 192.168.1.128-192.168.1.254

local ip = 192.168.1.99

require chap = yes

refuse pap = yes

require authentication = yes

name = LinuxVPNserver

ppp debug = yes

pppoptfile = /etc/ppp/options.xl2tpd

length bit = yes

[root@iZ2558f2cl2Z ~]# cat /etc/ppp/options.xl2tpd | grep -v '^#'

require-mschap-v2

ms-dns 8.8.8.8

ms-dns 8.8.4.4

asyncmap 0

auth

crtscts

lock

hide-password

modem

debug

name l2tpd

proxyarp

lcp-echo-interval 30

lcp-echo-failure 4

**防火墙规则设定：**

iptables -A INPUT -m policy --dir in --pol ipsec -j ACCEPT

iptables -A FORWARD -m policy --dir in --pol ipsec -j ACCEPT

iptables -t nat -A POSTROUTING -m policy --dir out --pol none -j MASQUERADE

iptables -A FORWARD -i ppp+ -p all -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT

iptables -A INPUT -m policy --dir in --pol ipsec -p udp --dport 1701 -j ACCEPT

iptables -A INPUT -p udp --dport 500 -j ACCEPT

iptables -A INPUT -p udp --dport 4500 -j ACCEPT

iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -o eth0 -j MASQUERADE

**配置PPP密码认证**

vi /etc/ppp/chap-secrets

loginname \* loginpassword \*

zhangyage \* yunshididai666 \*

第一个\*号代表的是协议，（pptp和l2tp）第二个\*号代表的是授权地址就是那个地址可以链接我们vpn，\*代表所有地址

**配置我们的vpn支持pptp协议**

**安装软件pptp**

rpm -Uvh pptpd-1.3.4-2.el6.x86\_64.rpm

**配置文件修改：**

[root@iZ2zed8sjhtdef16p6ta2tZ /]# cat /etc/pptpd.conf | grep -v '^#'

option /etc/ppp/options.pptpd

logwtmp

localip 172.16.31.1

remoteip 172.16.31.10-50

解释下localip 是pptp的网关、remoteip 是vpn客户端的地址范围10-50能为40个客户端分配IP。

pptp配置：

[root@iZ2zed8sjhtdef16p6ta2tZ ppp]# cat options.pptpd | grep -v '^#'

name pptpd

refuse-pap

refuse-chap

refuse-mschap

require-mschap-v2

require-mppe-128

ms-dns 223.5.5.5

ms-dns 223.6.6.6

proxyarp

debug

dump

lock

nobsdcomp

novj

novjccomp

防火墙：

iptables -t nat -A POSTROUTING -s 172.16.31.0/24 -j SNAT --to-source 112.126.92.33

iptables -t nat -A POSTROUTING -o eth1 -s 172.16.31.0/24 -j MASQUERADE

iptables -A FORWARD -p tcp --syn -s 192.168.111.0/24 -j TCPMSS --set-mss 1436