搭建L2tp/ipsec

梅梅呐 关注
0.24 2019.08.08 09:58:04 字数 1,068 阅读 5,848

> 用到的软件
> openswan(ipsec)：提供一个密钥
> ppp：提供用户名和密码xl2tpd：提供L2TP服务
> sysctl：提供服务器内部转发
> iptables：提供请求从服务器内部转向外部，外部响应转向服务器内部

准备
搭建L2TP需要环境支持，所以需要提前查看是否支持，不支持的自行Google

```
# 查看主机是否支持pptp，返回结果为yes就表示通过
modprobe ppp-compress-18 && echo yes
# 查看是否开启了TUN# 有的虚拟机主机需要开启，返回结果为**cat: /dev/net/tun: File descriptor in bad state**。就表示通过。
cat /dev/net/tun
```

安装

```
yum install -y epel-release
yum install -y xl2tpd libreswan lsof
yum install iptables
```

配置xl2tp

```
[root@qianxi ~]# egrep -v "^#" /etc/xl2tpd/xl2tpd.conf
[global]
listen-addr  = 服务器内网ip地址
ipsec saref = yes
auth file = /etc/ppp/chap-secrets
port = 1701    //监听端口
[lns default]
ip range = 192.168.1.128-192.168.1.254    //设置IP池，是分配给用户的ip，有多少个用户就需要多少个ip,建议分配多一点。
local ip = 192.168.1.99    //分配给本机的ip地址
require chap = yes
refuse pap = yes
require authentication = yes
name = LinuxVPNserver
ppp debug = yes
pppoptfile = /etc/ppp/options.xl2tpd
length bit = yes
```

配置ppp

```
[root@qianxi ~]# cat /etc/ppp/options.xl2tpd
ipcp-accept-local
ipcp-accept-remote
ms-dns  8.8.8.8
ms-dns  8.8.4.4
#ms-wins 192.168.1.2
#ms-wins 192.168.1.4
name xl2tpd
noccp
auth
crtscts
idle 1800
mtu 1410
mru 1410
nodefaultroute
debug
lock
logfile /var/log/l2tpd.log
proxyarp
connect-delay 5000
refuse-pap
refuse-chap
refuse-mschap
require-mschap-v2     #Windows连接必须设置
persist
```

配置IPSec

```
cat /etc/ipsec.conf   \\有效行
config setup
        protostack=netkey
        dumpdir=/var/run/pluto/
        logfile=/var/log/pluto.log
        virtual_private=%v4:10.0.0.0/8,%v4:192.168.0.0/16,%v4:172.16.0.0/12,%v4:25.0.0.0/8,%v4:100.64.0.0/10,%v6:fd00::/8,%v6:fe80::/10
include /etc/ipsec.d/*.conf
第一行config setup必须左对齐，即前面不能有空格，否则会报错
其他每一行都必须以Tab开头，否则会报错
```

设置预共享密钥PSK

```
[root@qianxi ~]# cat /etc/ipsec.secrets
include /etc/ipsec.d/*.secrets
106.15.230.123 %any: PSK "xl2tpd"
格式为：公网IP  %any:  PSK "预共享密钥"
```

配置服务器

```
[root@qianxi ~]# cat /etc/ipsec.d/l2tp_psk.conf
conn L2TP-PSK-NAT
        rightsubnet=vhost:%priv
        also=L2TP-PSK-noNAT
conn L2TP-PSK-noNAT
        authby=secret
        pfs=no
        auto=add
        keyingtries=3
        dpddelay=30
        dpdtimeout=120
        dpdaction=clear
        rekey=no
        ikelifetime=8h
        keylife=1h
        type=transport
```

梅梅呐 关注
总资产0.271

nodev8.9.3安装
阅读 310
Mysql安装
阅读 86

热门故事
没有拆不散的婚姻，只有不努力的婆婆
和女上司单独被困电梯，出来后我升职了
结婚两年，风黑男吃了我全家
开始都说不会动心，最后哭得比谁都惨

推荐阅读
使用国内的镜像源搭建kubernetes(k8s)集群
阅读 374
Centos7 查看防火墙相关常用命令
阅读 378
本地启动 Hybris 服务器调试模式后，监听在 8000 端口
阅读 124
虚拟机linux搭建MySql集群（以及自己踩的坑）
阅读 77
Linux 部署 OpenVPN server
阅读 865

```
    left=2.2.2.2    //修改为服务器IP地址
    right=%any
    right=%any
    rightprotoport=17/%any
```

注意：conn开头的两行必须左对齐，开头不能有空格，其他每一行必须以Tab开头

添加账号密码

```
[root@qianxi ~]# cat /etc/ppp/chap-secrets
# Secrets for authentication using CHAP
# client server secret IP addresses
vpn * 123456 *
```

配置类型为：用户名　*　密码　*

第一个*代表的意思的服务类型，在这里是L2TP，因为PPTP的账号密码管理文件也是此文件，所以以通配符*代替更好。

第二个*代表的用户限制地址，如果填进去某个IP，则是限制只能此IP连接该VPN。

开启内核转发

```
cat /etc/sysctl.conf
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
net.ipv6.conf.lo.disable_ipv6 = 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
kernel.sysrq=1
net.ipv4.ip_forward = 1
net.ipv4.conf.default.rp_filter = 0
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
```

使用sysctl　-p 重新加载内核配置项，使之生效

启动服务

```
[root@qianxi ~]# systemctl start ipsec
[root@qianxi ~]# systemctl start xl2tpd
```

查看状态：

```
[root@qianxi ~]# ipsec verify
Verifying installed system and configuration files

Version check and ipsec on-path                         [OK]
Libreswan 3.25 (netkey) on 3.10.0-693.2.2.el7.x86_64
Checking for IPsec support in kernel                    [OK]
 NETKEY: Testing XFRM related proc values
         ICMP default/send_redirects                    [OK]
         ICMP default/accept_redirects                  [OK]
         XFRM larval drop                               [OK]
Pluto ipsec.conf syntax                                 [OK]
Two or more interfaces found, checking IP forwarding    [OK]
Checking rp_filter                                      [OK]
Checking that pluto is running                          [OK]
 Pluto listening for IKE on udp 500                     [OK]
 Pluto listening for IKE/NAT-T on udp 4500              [OK]
 Pluto ipsec.secret syntax                              [OBSOLETE]
  003 WARNING: using a weak secret (PSK)
Checking 'ip' command                                   [OK]
Checking 'iptables' command                             [OK]
Checking 'prelink' command does not interfere with FIPS [OK]
Checking for obsolete ipsec.conf options                [OK]
```

防火墙配置

```
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

service iptables save
service iptables restart
```


梅梅呐
总资产0.271　共写了4929字　获得5个赞　共5个粉丝

关注

写下你的评论...

评论1 赞2 ···