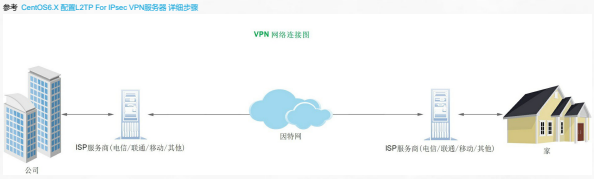
L2TP+IPsec vpn搭建

发表于: 2018-03-06 | 分类: 技术积累 | 标签: 软件工具 VPN L2TP

参考 CentOS6.X 配置L2TP For IPsec VPN服务器 详细步骤



声明：本文案例仅限用于企业远程办公或企业跨境电商用途参考，如果用于其他用途一概和本博文无关

**注意：使用windows系统自带的vpn连接，需要修改注册表后才可以连接的上！参考修改：
解决WIN10 vpn 连接错误 "无法建立计算机与VPN服务器之间的网络连接,因为远程服务器未响应"**

系统环境 Centos7.x

安装基础需要的软件包

```
yum install wget lsof net-tools vim nss nss-devel ppp ppp-devel iptables iptables-services -y
```

安装ipsec 和 xl2tpd

```
# openswan 包就是ipsec
yum install openswan -y

# 由于yum源中没有，我们手动下载xl2tpd rpm包
# centos8系统
wget http://ossjc-1252545319.cos.ap-shanghai.myqcloud.com/other/linux/xl2tpd/xl2tpd-1.3.15-1.el8.x86_64.rpm

# centos7系统
wget http://ossjc-1252545319.cos.ap-shanghai.myqcloud.com/other/linux/xl2tpd/xl2tpd-1.3.8-2.el7.x86_64.rpm
或者
wget http://ossjc-1252545319.cos.ap-shanghai.myqcloud.com/other/linux/xl2tpd/xl2tpd-1.3.15-1.el7.x86_64.rpm

# centos6系统
wget http://ossjc-1252545319.cos.ap-shanghai.myqcloud.com/other/linux/xl2tpd/xl2tpd-1.3.8-1.el6.x86_64.rpm

# 安装xl2tpd(注意文件名称)
yum localinstall xl2tpd-1.3.8-2.el7.x86_64.rpm -y
```

配置ipsec预共享密钥，和参数配置文件

(2020.10.10)注意:苹果手机升级ios14.0系统版本后，需要把ipsec.conf配置文件中sha2-truncbug=yes 注释掉才可以连接

```
# 添加预共享密钥，选择第一行，创建一行。ip可以为0.0.0.0也可以为你的内外网ip地址,"vpn"就是连接时候要用的ipsec密例，自己定义即可
vim /etc/ipsec.secrets
#include /etc/ipsec.d/*.secrets
0.0.0.0 %any: PSK "vpn"


# 修改ipsec.conf配置文件
vim /etc/ipsec.conf
.......
......
# 找到这个选项注释掉
#include /etc/ipsec.d/*.conf

#在下面新添加内容，注意:left这个IP地址，如果你是云服务器且还只能看到内网ip看不到外网ip的，这里x.x.x.x就填写内网ip地址。
conn l2tp-psk
    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=x.x.x.x
    leftprotoport=17/1701
    right=%any
    rightprotoport=17/%any
    dpddelay=40
    dpdtimeout=130
    dpdaction=clear
    sha2-truncbug=yes
```

修改xl2tpd 相关配置文件

```
# 修改vpn监听ip 和 分配客户端的地址池
vim /etc/xl2tpd/xl2tpd.conf
[global]
# 监听ip地址，填写内网ip地址或者0.0.0.0都可以用
listen-addr = x.x.x.x

# 分配的客户端地址段认同段，或者自定义网段也可以(默认的可以不用修改)
[lns default]
ip range = 192.168.1.128-192.168.1.254
local ip = 192.168.1.1
require chap = yes
refuse pap = yes
require authentication = yes
name = LinuxVPNserver
ppp debug = yes
pppoptfile = /etc/ppp/options.xl2tpd
length bit = yes


# 修改连接获取的参数
vim /etc/ppp/options.xl2tpd
ipcp-accept-local
ipcp-accept-remote
ms-dns  8.8.8.8
ms-dns 114.114.114.114
noccp
auth
# 注意:centos7下面要注释掉crtscts这个参数
crtscts
idle 1800
mtu 1410
mru 1410
nodefaultroute
debug
# 注意:centos7下面要注释掉lock这个参数
lock
proxyarp
connect-delay 5000
```

配置连接的用户账号和密码

```
# 添加用户格式(中间用空格或者tab隔开):用户名 pptpd 密码 *
# 密码有特殊字符最会的都要用""引起来

# Secrets for authentication using CHAP
# client    server    secret            IP addresses
test     * 123456 *

# 用户密码组合 复杂性例子
feifei     *     "!QAZxsw2#EDC"     *
Tx2022     *     "TX@xxxG6"     *
```

现在配置内核选项，linux的路由转发等(如果有的直接修改，没有的添加)

```
# 修改为: 表示打开路由转发功能
vim /etc/sysctl.conf
net.ipv4.ip_forward = 1

# 使修改的配置生效
sysctl -p
```

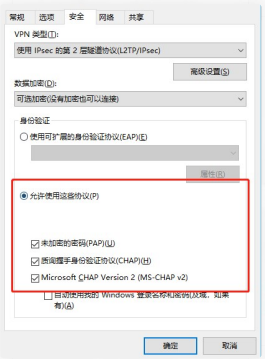
启动服务

```
# 启动服务   这里如果启动失败或者报错，请检查配置文件，或是否安装了需要的包
# centos6系统
service xl2tpd start
service ipsec start

# centos7系统
systemctl start xl2tpd
systemctl start ipsec

# 验证ipsec 是否完全正确
ipsec verify

# 只要没有error 和fail 就可以了
Version check and ipsec on-path                 [OK]
Libreswan 3.25 (netkey) on 3.10.0-514.26.2.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]


# 如果出现下面的几个红色提示
Checking rp_filter                              [ENABLED]
 /proc/sys/net/ipv4/conf/all/rp_filter          [ENABLED]
 /proc/sys/net/ipv4/conf/default/rp_filter      [ENABLED]
 /proc/sys/net/ipv4/conf/eth0/rp_filter         [ENABLED]
 /proc/sys/net/ipv4/conf/ip_vti0/rp_filter      [ENABLED]
  rp_filter is not fully aware of IPsec and should be disabled
# 解决：添加几个参数到/etc/sysctl.conf中
vim /etc/sysctl.conf
net.ipv4.conf.default.rp_filter = 0
net.ipv4.conf.all.rp_filter = 0
net.ipv4.conf.eth0.rp_filter = 0
net.ipv4.conf.lo.rp_filter = 0
net.ipv4.conf.ip_vti0.rp_filter = 0
# 使生效：
sysctl -p

#再重启下ipsec（重启完再次验证）
systemctl restart ipsec
```

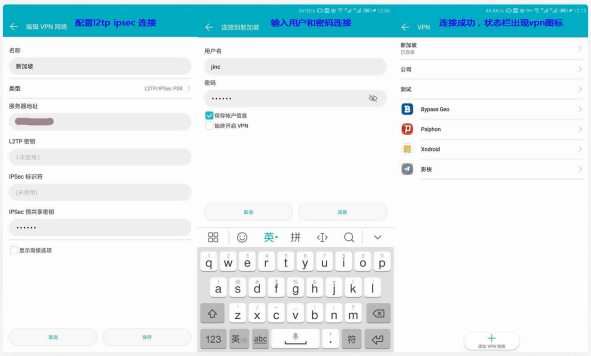
放行使用到的端口

```
防火墙|安全组需要开放UDP端口：1701、500、4500
```

windows10电脑里连接记得要在 vpn属性 - 安全 设置里面勾上 允许使用这些协议才行



手机端配置连接

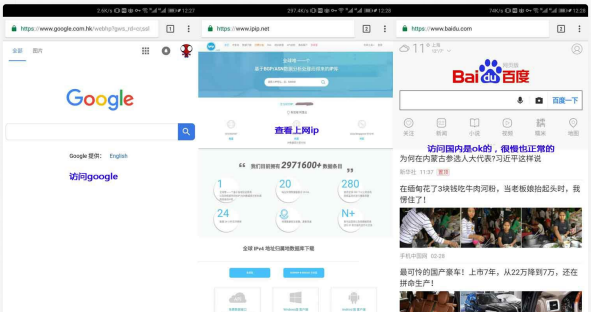



```
#观察日志
Mar  6 12:05:32 debug01000000015 xl2tpd[23389]: Connection established to 210.123.73.45, 58164.  Local: 65126, Remote: 50489 (ref=0/0
Mar  6 12:05:32 debug01000000015 xl2tpd[23389]: Call established with 210.123.73.45, Local: 8094, Remote: 17899, Serial: -1408866546
Mar  6 12:05:32 debug01000000015 pppd[24590]: pppd 2.4.5 started by root, uid 0
Mar  6 12:05:32 debug01000000015 pppd[24590]: Using interface ppp0
Mar  6 12:05:32 debug01000000015 pppd[24590]: Connect: ppp0 <--> /dev/pts/1
Mar  6 12:05:32 debug01000000015 pppd[24590]: Unsupported protocol 'Compression Control Protocol' (0x80fd) received
Mar  6 12:05:32 debug01000000015 pppd[24590]: Cannot determine ethernet address for proxy ARP
Mar  6 12:05:32 debug01000000015 pppd[24590]: local  IP address 192.168.1.1
Mar  6 12:05:32 debug01000000015 pppd[24590]: remote IP address 192.168.1.129
```

如果以上的配置你没有问题，连接也是没有问题的了，但是连接后不能上网的，接下来配置iptables转发

```
# 注意：请确认你的网卡名称是否eth0，如果不是请修改为你的网卡名称，这里同原对应上面/etc/xl2tpd/xl2tpd.conf配置文件中的同段
# iptables 默认是允许所有的，可以不用加这3条(如果是有额外的策略，需要加上允许这3条)
iptables -I INPUT -p udp --dport 4500 -j ACCEPT
iptables -I INPUT -p udp --dport 1701 -j ACCEPT
iptables -I INPUT -p udp --dport 500 -j ACCEPT

iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -o eth0 -j MASQUERADE
iptables -I FORWARD -s 192.168.1.0/24 -j ACCEPT
iptables -I FORWARD -d 192.168.1.0/24 -j ACCEPT
service iptables save

# centos6系统
service iptables restart

# centos7系统
systemctl restart iptables
```

手机访问测试没有翻试电脑连接】



快捷脚本:(也就是把上面步骤脚本化，只centos7上使用) l2tp-ipsec.sh 密码: l2tp

总结(有问题请先对照文章内容步骤和文章注释说明，然后再参考下面的问题说明)
此篇文章是以l2tp/Ipsec vpn都涉及到哪些文件和需要改动的配置进行搭建，需要有一定linux基础知识和理解
写此篇文章是为了记录下，方便以后用到好找，并不是教程文章，参考过程中有问题就请多 百度|谷歌|搜狗|360|bing ?
如果觉得麻烦或者完全不懂的建议去网上找别人弄好的一键脚本安装的

> 1：安装ppp包
> 2：安装ipsec和xl2tpd包
> 3：修改配置文件:
> /etc/ipsec.secrets
> /etc/ipsec.conf
> /etc/xl2tpd/xl2tpd.conf
> /etc/chap-secrets
> /etc/sysctl.conf
>
> 连接问题:
> 4：确认以上的配置文件无误
> 5：确认ipsec和xl2tpd服务启动正常
> 6：确认用户名密码和ipsec秘钥正确
> 7：确认服务端和客户端正确配置了连接参数
> 8：确认你服务端的L2tp vpn的协议和端口没有被运营商封掉
> 9：确认放行使用到的UDP端口（云安全组|外网防火墙等安全策略）
> !：特殊情况(你所用的网络运营商屏蔽了相关的协议和端口导致连接不上)
>
> 上网问题:
> 10：确认iptables转发规则无误和开放使用到的UDP端口（云安全组|外网防火墙等安全策略）
> 11：确认系统打开ipv4转发

相关博文:
Centos7搭建PPTP VPN服务
Centos7搭建Open VPN服务

如果这篇文章帮助到了你，我感到十分荣幸！
赞赏博主

◀好用的代理-Shadowsocks一键安装脚本

好工具-百度网盘下载器▶

留言内容 ↴

[11] 2021-04-16 14:27:43
配置好了，平板连不上

[J.C] 博主 2021-04-16 17:39:42
请参考文章底部问题说明，尝试解决问题

[littlemo] 2021-03-16 10:32:15
博主你好 warning: could not open include filename: '/etc/ipsec.d/*.conf'
要怎么修改

[J.C] 博主 2021-04-07 14:18:46
补充：注释掉/etc/ipsec.conf文件中的include /etc/ipsec.d/*.conf，因为配置直接写在ipsec.conf文件中了，这个选项就可以注释掉

[J.C] 博主 2021-03-16 11:57:35
这个错误没遇到过，你这个错误是启动服务时还是连接时的报错?

[littlemo] 2021-03-16 16:25:16
在验证ipsec 报错
然后我把他删除了就没有报错了，但是我不知道把它删除会不会影响
进入vim /etc/ipsec.conf //把/etc/ipsec.d/*.conf'他删了，就没有报错

[J.C] 博主 2021-03-16 19:00:31
你这个/etc/ipsec.d/目录下面是不是没有.conf结尾的文件啊，我当时配置时这个目录下面是有一个v6neighbor-hole.conf 文件的，这里面内容是ipv6相关的，你删除了应该没影响的。

[littlemo] 2021-03-16 20:30:40
/etc/ipsec.d/目录下面.conf 嗯我里面是的没有.conf文件

[littlemo] 2021-03-16 20:27:26
博主现在配置好了但是vp*en连不上

[littlemo] 2021-03-16 22:32:50
感谢博主，我现在可以用了

[littlemo] 2021-03-16 20:44:44
不知道问题出在哪

[liu] 2020-12-18 17:19:32
博主你好，按照你的教程搭建的 但是不能连接上。ipsec verify 验证没问题

[J.C] 博主 2020-12-18 17:50:12
连接提示的报错是什么?

[咸鱼王] 2020-10-22 15:11:49
博主你好，转发成功保存了，VPN也连接上 能正常上网 查询IP也是香港的IP，但为什么无法打开google和youtube之类的网站?

[J.C] 博主 2020-10-22 15:18:08
你香港服务器能访问google或者youtube吗?

[咸鱼王] 2020-10-22 15:22:06
可以访问的，我尝试过了

[J.C] 博主 2020-10-22 15:17:15
或许是DNS的问题，检查下配置文件里面的dns配置

[咸鱼王] 2020-10-22 15:22:29
DNS我配的8.8.8.8 8.8.4.4

[咸鱼王] 2020-10-22 15:03:55
博主你好，又是我....保存转发配置的时候出现“The service command supports only basic LSB actions (start, stop, restart, try-restart, reload, force-reload, status). For other actions, please try to use systemctl.”

[J.C] 博主 2020-10-22 15:06:49
iptables服务没装完整，yum install iptables-services -y

评论已关闭