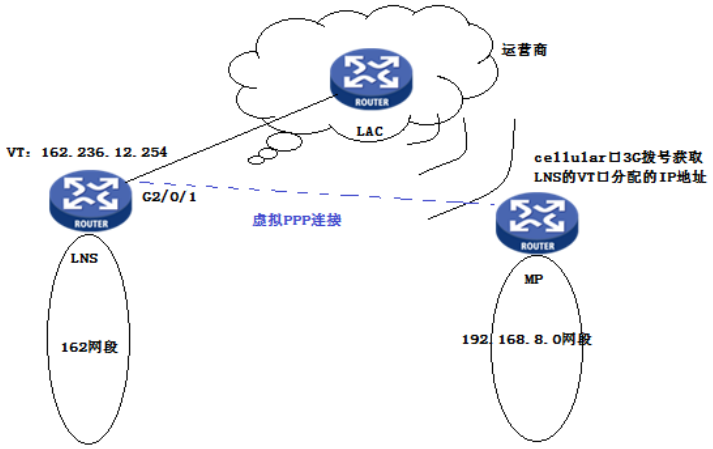
MSR5660对接迈普做IPSec over L2tp

杨超 2018-01-15 发表

客户的需求听起来很简单，原来客户一直用L2TP VPN，领导怕隐私被窃取，所以要求在原来L2TP上再加一个IPSec VPN进行加密。

LNS是MSR5660，LAC设备是运营商在维护，迈普的设备通过3G拨号连接到运营商的LAC再从LNS获取IP，实际的L2TP隧道是由LNS和迈普建立的。



现在已经搞清楚了L2TP是怎么做的，现在就是这个IPSec该怎么做的问题，是做L2TP over IPSec还是IPSec over L2TP，广泛采用的当然是L2TP over IPSec，所以建议客户用L2TP over IPSec，那么就得用LAC和LNS建立IPSec VPN，之前也提到过，LAC是运营商的设备，客户动不了手脚，方案泡汤。那么就只能用IPSec over L2TP，这样可以在LNS设备的VT口和迈普的cellular口上去应用IPSec。理论上说这样可行，但是实际做起来就是不通，也没有sa，最后也是多次尝试后才得出正确的配置：

LNS关键配置：

```
#
 ip pool 2 162.236.12.1 162.236.12.125 //该地址池供迈普设备3G拨号获取IP
#
interface Virtual-Template2
ppp authentication-mode chap domain tlxshczyh.vpdn.sx /指定ppp模式是chap并指定域
 remote address pool 2  //调用地址池pool2
 ip address 162.236.12.254 255.255.255.0
 ipsec apply policy l2tp //在VT口下应用IPSec策略
#
interface GigabitEthernet2/0/1（出接口）
 port link-mode route
 combo enable copper
 ip address 10.232.27.138 255.255.255.252
#
ip route-static 192.168.8.0 24 162.236.12.0//去往对端私网的明细路由
 ip route-static 220.192.176.0 24 10.232.27.137
#
domain system
 authorization-attribute user-profile network
 authentication ppp local
#
domain tlxshczyh.vpdn.sx
 authentication ppp local
 authorization ppp local
 accounting ppp local
#
domain default enable system
#
local-user vpdnuser class network //创建账号供L2TP拨号验证
 password cipher $c$3$DTPlys54nTTsLLf3k6+S6LZirVW8xoXw
 service-type ppp
 authorization-attribute user-role network-operator
```

```
#
ipsec transform-set l2tp
 esp encryption-algorithm des-cbc
 esp authentication-algorithm sha1
#
ipsec policy-template l2tp 10 //创建模板
 transform-set l2tp
 ike-profile l2tp
#
ipsec policy l2tp 10 isakmp template l2tp /策略关联模板
#
l2tp-group 1 mode lns /创建l2tp组1
 allow l2tp virtual-template 2
 tunnel name LNS
 tunnel password cipher $c$3$EaEsJ7TMOkclhpbr0Sid0MmFuHRDG5jIGw==
#
l2tp enable
#
 ike identity fqdn LNS
#
ike profile l2tp //创建profile
 keychain 123 //调用keychain
 exchange-mode aggressive //指定为野蛮模式
 local-identity fqdn LNS //本地fqdn为LNS
 match remote identity fqdn LAC //匹配对端的fqdn为LAC
 proposal 1 //调用proposal
#
ike keychain 123
 pre-shared-key hostname LAC key cipher $c$3$YVqv9301Ekdupc6KjLkXtFitBuUD4YTlyQ==
```

迈普设备所有配置:

```
router#show running-config
Building Configuration...done
! Current configuration : 2025 bytes
!
! Last configuration change at UTC THU JAN 01 00:01:12 1970 by admin
! Configuration version 0.39
!
!software version 6.3.17(integrity)
!software image file flash0: /flash/rp10-i-6.3.17.pck
!compiled on Apr  3 2014, 17:44:06
hostname router
service password-encrypt
no service md5-encrypt
no service new-encrypt
service login-secure
service shell-history
enable password OWRW[WWW\W encrypt
user admin privilege 15 password 7 OWRW[WWW\W
ip mef
ip load-sharing per-destination
aaa new-model
aaa authentication login default local
dialer-list 1 protocol ip permit
chat-script a ATDT
vlan 1
exit
!end
ip data-guard aware new-session
interface fastethernet0
exit
interface fastethernet1
exit
interface vlan1
```

```
ip address 192.168.8.1 255.255.255.0
exit
interface dot11radio0
 channel auto
 exit
!hsc_if_cellular3/0
interface cellular3/0
 encapsulation ppp
 ppp chap password 7 PUQURUSUTUUU
 ppp chap hostname tlznzd@tlxshczyh.vpdn.sx
 ip address negotiated
 bandwidth 384
 script dialer a
 dialer in-band
 dialer string #777
 dialer idle-timeout 0
 dialer-group 1
 dialer mode auto
 signal notify range 20
 exit
!end
interface null0
 no ip unreachables
 exit
crypto ike key e8dd73e24910cd4f€ address 162.236.12.254//指向LNS的VT口
crypto ike proposal 1
 exit
crypto ipsec proposal 2
 esp des sha1
 exit
crypto tunnel 3g
 local interface cellular3/0
 peer address 162.236.12.254//指向LNS的VT口
 set peer-id LNS
 set local-id LAC
 set authentication preshared
 set mode aggressive
 set ike proposal 1
 set ipsec proposal 2
 set auto-up
 exit
crypto policy 1
 flow 192.168.8.0 255.255.255.0 192.168.8.0 255.255.255.0 ip permit
 exit
crypto policy 2
 flow 192.168.8.0 255.255.255.0 162.0.0.0 255.0.0.0 ip tunnel 3g bypass//类似于ACL对感兴趣流进行
匹配
 exit
ip route 0.0.0.0 0.0.0.0 cellular3/0
ip http server web.rom
snmp-server contact Maipu Communication Technology Co.,Ltd.
snmp-server location No.16,Jiuxing Avenue,High-tech Park,Chengdu, P.R.China 610041
!end
```

刚配置完的时候是不通的，这和预想的一样。检查了迈普的配置，发现迈普上面填写隧道对端的地址填写错了：

crypto ike key e8dd73e24910cd4f€ address

这一条本来要求配置LNS的VT口地址，但客户配置成了LNS设备公网口的IP，让客户赶紧修改，还是不通，这也是我们预料到的。原因是LNS这端还没有配置去往迈普侧私网的路由，没配的原因是迈普设备获取的IP不固定，但又不能将pool改为只有一个IP，所以这条静态路由的下一跳就不确定，也不能只填写出接口，此时有一个想法，静态路由的下一跳可不可以配一个网段呢，马上搭建环境测试，发现是没问题的，于是赶紧让客户配置上去，问题解决。

对接的问题一般都比较难处理，一次配置完基本都不会通，需要做很多排查，就本案例来说，总结以下几点：

1. 了解清楚客户需求。//有时候客户可能自己也说不明白想做啥，需要攻城狮和客户多沟通。
2. 在和维护其他设备的攻城狮讨论时要明确思路，一定了解对方设备能配合我们做哪些配置，例如我们要做野蛮模式的IPSec，对方是否支持。
3. IPSec里面每个厂商默认的加密方式可能不一致，所以这一定要和对方设备调整一致，例如ike proposal下的加密算法是否一致。
4. Comvare V7的静态路由的下一跳可以配置成一个网段，不配置成具体的一个IP地址也行。
5. 在确认本端没有问题时，尝试去检查对端的配置，尤其检查对端填写的IP地址是否为正确的IP，本案例采用IPSec over L2TP，所以指对端IP一定是L2TP隧道口的IP，而不是公网接口的IP。