MSR5660 IPSEC OVER L2TP 不成功问题解决办法

IPSec VPN L2TP VPN 高子军 2019-03-28 发表

组网及说明

无

问题描述

某运营商客户要对网络设备进行升级改造，新购买了V7平台的MSR5660路由器来替换V5平台的MSR5060路由器。基于业务需求，需要创建IPSEC OVER L2TP VPN，现场将MSR5660替换MSR5060后，L2TP VPN能正常的拨入，但是IPSEC VPN无法建立成功。

过程分析

1．现场是使用V7平台MSR5660替换V5平台的MSR5060，MSR5060一直是在线运行的，并且业务正常，所以可以先对V5于V7设备的配置进行对比：

MSR5060路由器的配置：

```
#
acl number 3000
 rule 5 permit ip
#
l2tp enable
#
ike proposal 1
 encryption-algorithm 3des-cbc
 authentication-algorithm md5
#
ike dpd 1
 interval-time 3
 time-out 3
#
ike peer 3g
 proposal 1
 pre-shared-key simple XXXXXXX
 dpd 1
#
ipsec proposal 9
 esp encryption-algorithm 3des
#
ipsec policy ct3g 1 isakmp
 security acl 3000
 ike-peer 3g
 proposal 9
#
l2tp-group 1
 mandatory-lcp
 allow l2tp virtual-template 1
 tunnel password simple XXXXXX
#
interface Virtual-Template1
 ppp authentication-mode pap domain ******s.vpdn.qh
 l2tp-auto-client enable
 ip address 192.168.4.6 255.255.255.240
 ipsec policy ct3g
ip route-static 1*2.10.21.208 255.255.255.248 Virtual-Template1
ip route-static 1*2.10.21.216 255.255.255.248 Virtual-Template1
ip route-static 1*2.10.21.224 255.255.255.248 Virtual-Template1
```

MSR5660路由器的配置：

```
#
 ip pool 2 192.168.4.10 192.168.4.254
#
interface Virtual-Template1
 ppp authentication-mode pap domain ******s.vpdn.qh
 remote address pool 2
```

```
 ip address 192.168.4.1 255.255.255.0
 ipsec apply policy 3g
#
l2tp-group 1 mode lns
 allow l2tp virtual-template 1
 tunnel password cipher *******d3VBA=
#
 l2tp enable
#
ipsec transform-set anquantiyi
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm sha1
#
ipsec policy 3g 10 isakmp
 transform-set anquantiyi
 security acl 3100
 remote-address 192.168.4.10
 ike-profile ike1
#
ike profile ike1
 keychain keychain1
 exchange-mode aggressive
 local-identity fqdn test
 match remote identity address 192.168.4.10 255.255.255.255
 proposal 1
#
ike proposal 1
 encryption-algorithm 3des-cbc
 authentication-algorithm md5
#
ike keychain keychain1
pre-shared-key address 0.0.0.0 0.0.0.0 key cipher ********
#
domain jtyhpos.vpdn.qh
 authentication ppp local
 authorization ppp local
```

2.现场配置LAC-Auto-Initiated模式的L2TP VPN，当前L2TP VPN已经拨号成功了，并且获取到pool 2内的IP地址，但是IPSEC VPN无法建立成功。在V7设备上查看IPSEC VPN的配置没有问题，通过display ip routing-table 1*2.10.21.208发现走的是缺省路由。在V5设备上查看相同的路由，下一跳是VT接口。

3.在V7设备上增加相应的路由，但是在V7设备配置时，下一跳不能配置为VT接口：

```
[H3C]ip route-static 1*2.10.21.224 255.255.255.248 ?
  GigabitEthernet  GigabitEthernet interface
  NULL             NULL interface
  Serial           Serial interface
  X.X.X.X          Nexthop IP address
  vpn-instance     Destination VPN instance for gateway address
```

4. V5设备的实现方式是点到多点的发报文，LNS会给所有的VT口发报文，由于这样的实现方式有问题，所以在V7平台已经删除了。L2TP VPN使用LAC-Auto-Initiated模式大多数是点对点的应用场景，如果点对多点的应用场景，需要添加对应的路由来实现。

5. 由于LAC是从LNS侧的IP POOL内随机获取IP地址，所以在配置路由时需要配置多条路由；如果IP POOL内地址很多，需要添加对应条数的路由，增加路由配置难度。如果给LAC分配固定的IP地址后再添加静态路由就会避免配置多条路由的情况。

解决方法

现场配置的L2TP VPN认证方式为本地认证，在LNS配置用户时可以通过authorization-attribute ip来指定本地用户的静态IP地址，然后再添加静态路由后IPSEC VPN也正常建立。

增加如下配置：

```
local-user test class network
service-type ppp
authorization-attribute user-role network-operator
authorization-attribute ip 192.168.4.10
ip route-static 1*2.10.21.224 255.255.255.248 192.168.4.10
```