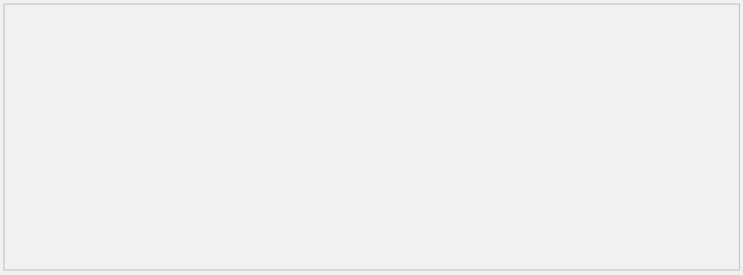
金融行业MSR3011+3G模块VPDN无线接入配置案例

朱福祥 2011-09-15 发表

MSR3011+3G模块VPDN无线接入配置案例

1、 需求描述

在某金融行业客户的网络中，客户网点使用我司MSR3011路由器，现打算把原有网点的两条有线线路改造为一条为有线线路另一条为3G无线线路，并在3G无线线路上对用户数据进行IPSEC加密，电信运营商侧设备作为L2TP隧道中的LAC，省行侧的MSR5040作为L2TP隧道中的LNS，并在网点的MSR3011上对业务数据进行IPSEC加密，整个隧道过程属于IPSEC over L2TP，电信运营商只提供L2TP的隧道密码。



2、 版本信息

H3C MSR3011版本Comware Software, version 5.20, Release 2105P12
H3C MSR5040版本Comware Software, version 5.20, Release 2105P12

3、 配置步骤

MSR3011路由器侧的配置
配置3G无线模块

```
user-interface tty 32
modem both
#
dialer-rule 1 ip permit
#
interface Cellular2/0
 async mode protocol
 link-protocol ppp
 ppp pap local-user boc@vpdn.ha password simple bocvpdn
 ip address 10.109.129.102 255.255.255.0
 dialer enable-circular
 dialer-group 1
 dialer timer idle 60
 dialer number #777
 ipsec policy xp                    ***对3G无线接口应用IPSEC策略 ***
```

创建IPSEC策略

```
interface Ethernet0/1
port link-mode route
ip address 10.56.53.17 255.255.255.240
#
acl number 3000
rule 0 permit ip source 10.56.53.16 0.0.0.15
rule 1 permit icmp source 10.56.53.16 0.0.0.15
#
ike peer xp
pre-shared-key cipher nw1kqzgZJnA=
remote-address 10.232.83.41
#
ipsec proposal 1
#
ipsec policy xp 1 isakmp
```

```
security acl 3000
ike-peer xp
proposal 1
#
将IPSEC策略应用到无线接口见①

配置路由
ip route-static 0.0.0.0 0.0.0.0 Cellular2/0                    ***配置缺省路由***


MSR5040路由器侧的配置
L2TP隧道配置
#
 l2tp enable
#
l2tp-group 1
 allow l2tp virtual-template 1
 tunnel password simple 111111
#
domain vpdn.ha
 authentication ppp radius-scheme msr                    ***采用Radius认证***
 authorization ppp radius-scheme msr
 accounting ppp radius-scheme msr
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
 accounting optional
#
domain default enable vpdn.ha
#
interface Ethernet8/0
 port link-mode route
 ip address 10.232.83.41 255.255.255.252
#
interface Virtual-Template1
 ppp authentication-mode pap domain
vpdn.ha
 ip address unnumbered interface Ethernet8/0
 ipsec policy xp                                    ***应用IPSEC策略 ***

创建IPSEC策略
acl number 3000
 rule 0 permit ip source 10.56.0.0 0.0.255.255 destination 10.56.53.16 0.0.0.15
 rule 1 permit ip source 10.56.10.162 0 destination 10.56.53.16 0.0.0.15
 rule 3 permit icmp source 10.56.0.0 0.0.255.255 destination 10.56.53.16
0.0.0.15
 rule 4 permit icmp source 10.56.10.162 0 destination 10.56.53.16 0.0.0.15
#
ike peer xp
 pre-shared-key cipher nw1kqzgZJnA=
 remote-address 24.109.129.102
#
ipsec proposal
1

#
ipsec policy xp 1 isakmp
 security acl 3000
 ike-peer xp
 proposal 1                              ***将 IPSEC策略应用到接口见 ①***

配置路由
ip route-static 0.0.0.0 0.0.0.0 10.232.83.42
```

ip route-static 10.56.53.16 255.255.255.240 24.109.129.102

4、 配置关键点

？ 由于该案例中采用的IPSEC over L2TP方式，所以在MSR5040侧要将IPSEC策略应用到interface Virtual-Template1接口下

？ 在MSR3011侧和MSR5040侧要配置安全ACL，只有命中安全ACL的数据报文才能进行IPSEC加密，如果在安全ACL中如果匹配的源地址为ANY，那么在MSR3011侧会对所有的报文进行IPSEC加密导致运营商侧的LAC设备无法识别报文。