联通CDMA无线上网方式实现与SecPath1000 VPN连接

王雪梅 2006-02-22 发表

联通CDMA无线上网方式实现与SecPath1000 VPN连接

【网络拓扑】
这种应用的网络拓扑都比较简单，网络出口放置一台路由器或者Secpath，用户通过联通CDMA无线上网卡连接Internet后对VPN的访问。
【网络概况】
某省电信局采用一台Secpath1000放置在网络出口，用户通过联通CDMA无线上网卡实现对VPN的访问；
该市采用联通公司提供的一台 R2610路由器，用户通过联通CDMA无线上网卡实现对VPN的访问。
【问题描述】
某省局用户采用网卡为神州数码 dcwl-390c，secpoint版本2.03，SecPath1000软件版本3.3-1000，Secpath放在用户局域网最外端，采用其他方式接入VPN都没有问题（电话线拨号 / ADSL拨号），现场拨号，笔记本可以上网，但是Ping Secpath外网地址不通，用Secpoint拨号提示找不到LNS。
该市用户采用上网卡拨号后上网正常，但是不能访问内网服务器。
【问题处理】
在该省电信局现场收集了Secpath信息，发现配置没有问题，只是采用联通CDMA无线上网卡不能访问。
在某政府网络是因为网络先期进行过改造，起初收集观察，由于切换后的防火墙缺少一条去往联通设备的路由，内网到联通提供的路由器无法Ping通，在防火墙上添加路由后，服务器可以Ping通联通路由器，但是广域网对端的地址无法Ping通，联通人员检查路由配置也没有问题。
【解决方案】
该电信用户问题，最终与联通人员协调，是因为在联通一端有一些访问限制，如果用户需要用CDMA上网卡访问一些地址，要在运营商一侧进行数据的修改，修改之后用户访问断断续续，原因是用户办公大楼内CDMA信号不好造成的。
该市用户问题比较复杂，到拨号端观察，发现用户拨号后可以访问到联通路由器的内网接口，但是不能Ping通内网的网关。查看发现用户获取地址为192.168.100.x网段，联通在中间做了NAT转换，从内网S8016上可以Ping通192.168.100.1，查看ARP表项，发现该地址在内网，进一步排查发现用户内网防火墙上的管理口配置了该段地址，虽然管理口上没有连网线，但是这台防火墙的管理地址还能起作用（安智防火墙）。最后确认问题应该在这里，修改该地址后，访问正常。
【总结】
此类问题比较简单，一般与设备配置 / 版本等没有关系，用户使用的CDMA上网卡与某些笔记本电脑存在兼容性问题，一般会认为Secpoint客户端软件会在使用CDMA上网卡时也会有问题，但实际上只要采用了2.03以上版本就没有问题；
联通人员对用户支持力度不够，用户一般也会认为是设备配置本身有问题；
无线上网卡信号在一些建筑物内信号较差，会对网络访问造成影响，这样的细节大家也应当注意；
如果是与联通技术人员配合，应当详细了解网络结构及运营商设备配置，否则就会出现与该市类似的问题，给定位带来很大的困难。
Secpath1000配置实例

```
<secpath1000>dis cur
#
 sysname secpath1000
#
 l2tp enable
#
 local-user test1 password simple test1
 local-user test2 password simple test2
 local-user test3 password simple test3
 local-user test4 password simple test4
#
 ip pool 1 10.1.1.2 10.1.1.150
#
 aaa enable
 aaa accounting-scheme optional
 radius server 219.144.196.196 authentication-port 1645 accounting-port 1646
 radius shared-key 12345
 radius timer response-timeout 120
 aaa accounting-scheme ppp default start-stop radius
 aaa authentication-scheme ppp default radius
#
```

```
 ike local-name zongbu-shanxi
#
ike peer huawei-3com
 exchange-mode aggressive
 pre-shared-key aaa
 id-type name
 remote-name secpoint
 nat traversal
 max-connections 100
#
ipsec proposal huawei-3com
#
ipsec policy-template secpoint 1
 ike-peer huawei-3com
 proposal huawei-3com
#
ipsec policy secpath 1 isakmp template secpoint
#
interface Virtual-Template1
 ppp authentication-mode pap
 ppp accounting scheme default
 ip address 10.1.1.1 255.255.255.0
 remote address pool 1
#
interface Aux0
 async mode flow
 link-protocol ppp
#
interface GigabitEthernet0/0
 description TO-Firewall
 ip address 公网地址
 undo ip fast-forwarding
#
interface GigabitEthernet0/1
 description TO-Internet
 ip address 公网地址
 undo ip fast-forwarding
 ipsec policy secpath
#
interface NULL0
#
l2tp-group 1
 undo tunnel authentication
 allow l2tp virtual-template 1
#
 ip route-static 0.0.0.0 0.0.0.0 XXX preference 60
 .....静态路由配置
#
user-interface con 0
user-interface aux 0
user-interface vty 0 4
 user privilege level 3
 set authentication password simple
#
return
<secpath1000>
```