野蛮模式下MSR与SecPathv100-s IPSec VPN无法建立问题

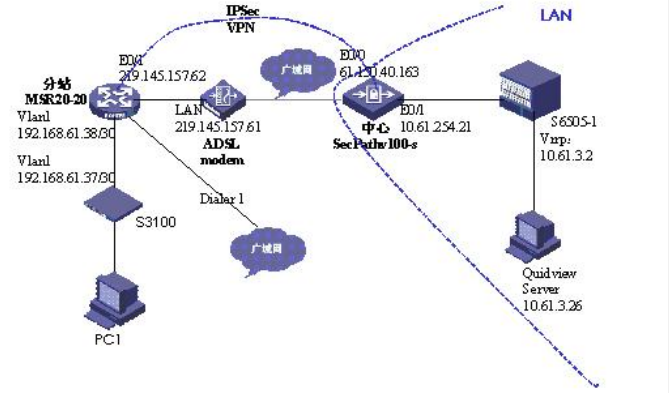
张瑞 2007-05-18 发表

野蛮模式下MSR与SecPathv100-s
IPSec VPN无法建立问题一例

一、 组网介绍：

中心SecPath v100-s与分站MSR20-20通过广域网互联，分站侧通过固定地址219.145.157.62与ADSL Modem互联，modem的互联地址为219.145.157.61，在分站MSR20-20与中心SecPath v100-s之间应用野蛮模式建立IPSec VPN隧道，允许私网10.61.0.0网段的数据进行互访；同时MSR20-20通过另外一条ADSL拨号线路（Dialer1）连接到公网，供内部用户访问Internet。其它设备与IP如图中所示。

本案例相关组网示意图



二、 问题描述：

在上图中，分站MSR20-20分别通过两条拨号链路连接到中心和Internet，在当前配置下分站用户可以通过Dialer1正常访问公网，但是IPSec VPN无法通过ADSLmodem正常
建立。

三、 过程分析：

step1：检查两端VPN的基本配置：

分站MSR20-20相关配置如下:

```
#
 ike local-name dishi-bj //指定ike协商时本端网关的名字为dishi-bj
#
ike peer dizhenju        //定义ike对等体名称为dizhenju
 exchange-mode aggressive  //采用野蛮模式
 pre-shared-key dizhen     //指定预共享密钥dizhen
 id-type name
 remote-name dizhenju      //指定IKE协商时对端的名字
 remote-address 61.150.40.163  //指定对端地址
 nat traversal                 //使能nat穿越
#
ipsec proposal default        //指定IPSec提议的名字为default
#
ipsec policy dizhenju 1 isakmp //指定安全策略的名字dizhenju，指定
    通过IKE协商建立安全联盟
 security acl 3000
 ike-peer dizhenju
 proposal default
#
acl number 3000     //定义需要保护的业务数据流
 rule 1 permit ip source 10.61.99.0 0.0.0.255 destination 10.61.0.0 0.0.255.255
 rule 10 permit ip source 10.61.253.41 0 destination 10.61.0.0 0.0.255.255
 rule 100 deny ip
acl number 3500     //其它数据流走公网
```

```
 rule 1 deny ip source 10.61.0.0 0.0.255.255 destination 10.61.0.0 0.0.255.255
 rule 2 deny ip source 192.168.61.0 0.0.0.25
 rule 100 permit ip
#
interface Dialer1
 nat outbound 3500
 link-protocol ppp
 ppp pap local-user ** password simple ***
 ip address ppp-negotiate
 dialer user baoji
 dialer-group 1
 dialer bundle 1
#
interface Ethernet0/0
 port link-mode route
 pppoe-client dial-bundle-number 1   //创建PPPOE会话
#
interface Ethernet0/1
 port link-mode route
 ip address 219.145.157.62 255.255.255.0
 ipsec policy dizhenju              //应用IPSec策略
#
 ip route-static 0.0.0.0 0.0.0.0 Dialer1  --- A
 ip route-static 10.61.0.0 255.255.0.0 219.145.157.61   --- B
```

中心侧SecPath安全策略采用模板方式，经对照确认双方IPSec的配置没有问题。

Step2：查看分站侧IKE SA显示如下：

```
total phase-1 SAs:  1
   connection-id  peer            flag        phase   doi
 -----------------------------------------------------------
       2          61.150.40.163   RD|ST         1     IPSEC
      24          <unnamed>       NONE          2     IPSEC
```

此处显示ike第一阶段协商成功而第二阶段协商失败。

经过分析当前配置与以下debug信息发现：

***Apr 24 09:20:21:135 2007 dishi-bj-h3c-r20 IPSEC/7/DBG:Set Local Address 219.145.157.62**

***Apr 24 09:20:21:235 2007 dishi-bj-h3c-r20 IPSEC/7/DBG:IPSec drop packet! Notify IKE to negotiate SA for IPsec policy: dizhenju-1**

//ike第一阶段协商成功后，进入第二阶段IPSec SA的协商，此时本地地址被设定为219.145.157.62，协商报文会从默认路由A发出，无匹配的IPSec策略，第二阶段协商失败

四、 解决方法：

通过在系统视图下添加静态路由：

```
ip route-static 61.150.40.163 255.255.255.255 219.145.157.61
```

问题解决。

五、 总结：

解决该问题的关键是要找出IKE协商第二阶段报文发向了公网接口Dialer1而并未走我们所期望的静态拨号接口219.145.157.62。