SR66与锐捷设备IPSEC over GRE互通IKE一阶段协商不成功经验案例

王继尧 2012-06-15 发表

SR66与锐捷设备IPSEC over GRE互通IKE一阶段协商不成功经验案例

一、 组网：

某局点锐捷3G路由器通过联通的设备（LAC）与SR6608（LNS）建立L2TP隧道，通过AAA服务器进行认证，认证通过后给3G路由器分配固定的IP地址。

为了加强数据的安全性，用户在锐捷3G路由器和SR6608之间部署了Ipsec_over_gre技术，保护关键的数据。

二、 问题描述：

配置完成后，3G拨号及GRE通道正常，两端Tunnel口地址可以正常ping通，路由学习也都正常。但是IPSEC建立不成功，通过命令行查看，IKE 第一阶段协商都不成功。

三、 过程分析：

1、IPSEC相关配置如下：

SR66侧配置：

```
acl number 3001
 rule 0 permit ip destination 10.39.134.0 0.0.0.255
 rule 5 permit ip destination 10.39.175.0 0.0.0.255
#
ike proposal 1
 encryption-algorithm 3des-cbc
 dh group2
 authentication-algorithm md5
 sa duration 6400
#
ike peer test-50
 pre-shared-key cipher 3AavyEcNMKo=
 remote-address 148.x.x.29
 local-address 148.x.x.30
#
ipsec proposal 1
 esp encryption-algorithm 3des
#
ipsec policy test 1 isakmp
 security acl 3001
 ike-peer test-50
 proposal 1
#
interface Tunnel50
 description to XXXX
 ip address 148.x.x.30 255.255.255.252
 source 10.74.42.218
 destination 148.y.y.8
 ipsec policy test
```

锐捷3G路由器配置：

```
    ip access-list extended 101
     10 permit ip 10.39.134.0 0.0.0.255 any
!
crypto isakmp policy 1
 encryption 3des
 authentication pre-share
 hash md5
 group 2
 lifetime 6400
!
crypto isakmp key 7 summer address 148.x.x.30
crypto ipsec transform-set myset  esp-3des esp-md5-hmac
crypto map mymap 1 ipsec-isakmp
 set peer 148.x.x.30
 set transform-set myset
 match address 101
!
interface Tunnel 1
 ip address 148.x.x.29 255.255.255.252
 crypto map mymap
 tunnel source Async 1
 tunnel destination 10.74.42.218
```

因为之前已经排查Tunnel接口UP，触发IPSEC保护的流的路由学习也是正常的，所以现在需比较IPSEC相关配置，查看IPSEC加密认证算法等相关配置是否对应，从配置上看两边配置都是主模式，而且加密及认证算法等都对应。

2、 在SR66侧打开debug ike sa，debug ipsec sa开关，在锐捷3G路由器上带保护流源地址ping 包，触发IPSEC建立，查看SR66打印出的debug信息如下：

//SR66收到的主模式的第一次交换消息1，用于IKE提议和转换方式的协商

```
*Jun 11 21:03:43:468 2012 liantong-VPDN IKE/7/DEBUG: received message:
*Jun 11 21:03:43:468 2012 liantong-VPDN IKE/7/DEBUG:  ICOOKIE: 0x1992b94d05fac7c4
*Jun 11 21:03:43:468 2012 liantong-VPDN IKE/7/DEBUG:  RCOOKIE: 0x0000000000000000
*Jun 11 21:03:43:468 2012 liantong-VPDN IKE/7/DEBUG:  NEXT_PAYLOAD: SA
*Jun 11 21:03:43:468 2012 liantong-VPDN IKE/7/DEBUG:  VERSION: 16
*Jun 11 21:03:43:468 2012 liantong-VPDN IKE/7/DEBUG:  EXCH_TYPE: ID_PROT
*Jun 11 21:03:43:469 2012 liantong-VPDN IKE/7/DEBUG:  FLAGS: [ ]
*Jun 11 21:03:43:469 2012 liantong-VPDN IKE/7/DEBUG:  MESSAGE_ID: 0x00000000
*Jun 11 21:03:43:469 2012 liantong-VPDN IKE/7/DEBUG:  LENGTH: 216
*Jun 11 21:03:43:469 2012 liantong-VPDN IKE/7/DEBUG: exchange lookup all list from COOKIE: iCOOKIE 1992b94d05fac7c4
*Jun 11 21:03:43:469 2012 liantong-VPDN IKE/7/DEBUG: parse payloads: payload SA
*Jun 11 21:03:43:469 2012 liantong-VPDN IKE/7/DEBUG: parse payloads: payload VENDOR
*Jun 11 21:03:43:470 2012 liantong-VPDN IKE/7/DEBUG: parse payloads: payload VENDOR
*Jun 11 21:03:43:470 2012 liantong-VPDN IKE/7/DEBUG: parse payloads: payload VENDOR
*Jun 11 21:03:43:470 2012 liantong-VPDN IKE/7/DEBUG: parse payloads: payload VENDOR
*Jun 11 21:03:44:270 2012 liantong-VPDN IKE/7/DEBUG: parse payloads: payload VENDOR
*Jun 11 21:03:44:270 2012 liantong-VPDN IKE/7/DEBUG: validate payload SA
*Jun 11 21:03:44:271 2012 liantong-VPDN IKE/7/DEBUG:  DOI: 1
*Jun 11 21:03:44:271 2012 liantong-VPDN IKE/7/DEBUG:
IKE_DPD: receive : afcad713 68a1f1c9 6b8696fc 77570100 (DPD)
*Jun 11 21:03:44:271 2012 liantong-VPDN IKE/7/DEBUG: exchange setup(R): 8fd4aa0
*Jun 11 21:03:44:271 2012 liantong-VPDN IKE/7/DEBUG: parse payloads: payload PROPOSAL
*Jun 11 21:03:44:271 2012 liantong-VPDN IKE/7/DEBUG: parse payloads: payload TRANSFORM
*Jun 11 21:03:44:271 2012 liantong-VPDN IKE/7/DEBUG: parse payloads: payload TRANSFORM
*Jun 11 21:03:44:272 2012 liantong-VPDN IKE/7/DEBUG: validate payload PROPOSAL
*Jun 11 21:03:44:272 2012 liantong-VPDN IKE/7/DEBUG:  NO: 1
*Jun 11 21:03:44:272 2012 liantong-VPDN IKE/7/DEBUG:  PROTO: ISAKMP
*Jun 11 21:03:44:272 2012 liantong-VPDN IKE/7/DEBUG:  SPI_SZ: 0
*Jun 11 21:03:44:272 2012 liantong-VPDN IKE/7/DEBUG:  NTRANSFORMS: 2
*Jun 11 21:03:44:272 2012 liantong-VPDN IKE/7/DEBUG: validate payload TRANSFORM
*Jun 11 21:03:44:273 2012 liantong-VPDN IKE/7/DEBUG:  NO: 1
*Jun 11 21:03:45:773 2012 liantong-VPDN IKE/7/DEBUG:  ID: 1
*Jun 11 21:03:45:773 2012 liantong-VPDN IKE/7/DEBUG:  Transform 1's attributes
*Jun 11 21:03:45:773 2012 liantong-VPDN IKE/7/DEBUG:  Attribute ENCRYPTION_ALGORITHM : 3DES_CBC
*Jun 11 21:03:45:774 2012 liantong-VPDN IKE/7/DEBUG:  Attribute HASH_ALGORITHM : MD5
*Jun 11 21:03:45:774 2012 liantong-VPDN IKE/7/DEBUG:  Attribute AUTHENTICATION_METHOD : PRE_SHARED
*Jun 11 21:03:45:774 2012 liantong-VPDN IKE/7/DEBUG:  Attribute GROUP_DESCRIPTION : MODP_1024
*Jun 11 21:03:45:774 2012 liantong-VPDN IKE/7/DEBUG:  Attribute LIFE_TYPE : SECONDS
*Jun 11 21:03:45:774 2012 liantong-VPDN IKE/7/DEBUG:  Attribute LIFE_DURATION : 6400
*Jun 11 21:03:45:774 2012 liantong-VPDN IKE/7/DEBUG: validate payload TRANSFORM
*Jun 11 21:03:45:775 2012 liantong-VPDN IKE/7/DEBUG:  NO: 2
*Jun 11 21:03:45:775 2012 liantong-VPDN IKE/7/DEBUG:  ID: 1
*Jun 11 21:03:45:775 2012 liantong-VPDN IKE/7/DEBUG:  Transform 2's attributes
```

```
*Jun 11 21:03:45:775 2012 liantong-VPDN IKE/7/DEBUG:   Attribute ENCRYPTION_ALGORITHM :
DES_CBC
*Jun 11 21:03:45:775 2012 liantong-VPDN IKE/7/DEBUG:   Attribute HASH_ALGORITHM : SHA
*Jun 11 21:03:47:276 2012 liantong-VPDN IKE/7/DEBUG:   Attribute AUTHENTICATION_METHOD :
RSA_SIG
*Jun 11 21:03:47:276 2012 liantong-VPDN IKE/7/DEBUG:   Attribute GROUP_DESCRIPTION : MOD
P_768
*Jun 11 21:03:47:276 2012 liantong-VPDN IKE/7/DEBUG:   Attribute LIFE_TYPE : SECONDS
*Jun 11 21:03:47:276 2012 liantong-VPDN IKE/7/DEBUG:   Attribute LIFE_DURATION : 86400
*Jun 11 21:03:47:276 2012 liantong-VPDN IKE/7/DEBUG: validate payload VENDOR
*Jun 11 21:03:47:277 2012 liantong-VPDN IKE/7/DEBUG:   vendor ID seen
*Jun 11 21:03:47:277 2012 liantong-VPDN IKE/7/DEBUG: validate payload VENDOR
*Jun 11 21:03:47:277 2012 liantong-VPDN IKE/7/DEBUG:   vendor ID seen
*Jun 11 21:03:47:277 2012 liantong-VPDN IKE/7/DEBUG: validate payload VENDOR
*Jun 11 21:03:47:277 2012 liantong-VPDN IKE/7/DEBUG:   vendor ID seen
*Jun 11 21:03:47:277 2012 liantong-VPDN IKE/7/DEBUG: validate payload VENDOR
*Jun 11 21:03:47:278 2012 liantong-VPDN IKE/7/DEBUG:   vendor ID seen
*Jun 11 21:03:47:278 2012 liantong-VPDN IKE/7/DEBUG: validate payload VENDOR
*Jun 11 21:03:47:278 2012 liantong-VPDN IKE/7/DEBUG:   vendor ID seen
*Jun 11 21:03:47:278 2012 liantong-VPDN IKE/7/DEBUG: exchange check: checking for required SA
*Jun 11 21:03:48:779 2012 liantong-VPDN IKE/7/DEBUG: negotiate sa: transform 1 proto 1 proposal
1 compatible
*Jun 11 21:03:50:280 2012 liantong-VPDN IKE/7/DEBUG: negotiate sa: proposal 1 succeeded
*Jun 11 21:03:50:281 2012 liantong-VPDN IKE/7/DEBUG: vendor[0] :
*Jun 11 21:03:50:281 2012 liantong-VPDN IKE/7/DEBUG: 4a131c81 07035845 5c5728f2 0e95452f
*Jun 11 21:03:50:281 2012 liantong-VPDN IKE/7/DEBUG: vendor[1] :
*Jun 11 21:03:50:281 2012 liantong-VPDN IKE/7/DEBUG: 439b59f8 ba676c4c 7737ae22 eab8f582
*Jun 11 21:03:50:281 2012 liantong-VPDN IKE/7/DEBUG: vendor[2] :
*Jun 11 21:03:50:281 2012 liantong-VPDN IKE/7/DEBUG: 7d9419a6 5310ca6f 2c179d92 15529d56
*Jun 11 21:03:50:282 2012 liantong-VPDN IKE/7/DEBUG: vendor[3] :
*Jun 11 21:03:50:282 2012 liantong-VPDN IKE/7/DEBUG: 90cb8091 3ebb696e 086381b5 ec427b1f
*Jun 11 21:03:50:282 2012 liantong-VPDN IKE/7/DEBUG: vendor[4] :
*Jun 11 21:03:50:282 2012 liantong-VPDN IKE/7/DEBUG: afcad713 68a1f1c9 6b8696fc 77570100
*Jun 11 21:03:50:282 2012 liantong-VPDN IKE/7/DEBUG:
IKE_DPD: receive : afcad713 68a1f1c9 6b8696fc 77570100 (DPD)
*Jun 11 21:03:50:282 2012 liantong-VPDN IKE/7/DEBUG: exchange state machine: unexpected payl
oad VENDOR
*Jun 11 21:03:51:783 2012 liantong-VPDN IKE/7/DEBUG: exchange state machine: unexpected payl
oad VENDOR
*Jun 11 21:03:51:783 2012 liantong-VPDN IKE/7/DEBUG: exchange state machine: unexpected payl
oad VENDOR
*Jun 11 21:03:51:783 2012 liantong-VPDN IKE/7/DEBUG: exchange state machine: unexpected payl
oad VENDOR
*Jun 11 21:03:51:783 2012 liantong-VPDN IKE/7/DEBUG: exchange state machine(R): finished step
0, advancing...
*Jun 11 21:03:51:784 2012 liantong-VPDN IKE/7/DEBUG: add payload to message: SA
*Jun 11 21:03:51:784 2012 liantong-VPDN IKE/7/DEBUG:   DOI: 1
*Jun 11 21:03:51:784 2012 liantong-VPDN IKE/7/DEBUG: add payload to message: PROPOSAL
*Jun 11 21:03:51:784 2012 liantong-VPDN IKE/7/DEBUG:   NO: 1
*Jun 11 21:03:51:785 2012 liantong-VPDN IKE/7/DEBUG:   PROTO: ISAKMP
*Jun 11 21:03:51:785 2012 liantong-VPDN IKE/7/DEBUG:   SPI_SZ: 0
*Jun 11 21:03:53:285 2012 liantong-VPDN IKE/7/DEBUG:   NTRANSFORMS: 1
*Jun 11 21:03:53:285 2012 liantong-VPDN IKE/7/DEBUG: add payload to message: TRANSFORM
*Jun 11 21:03:53:286 2012 liantong-VPDN IKE/7/DEBUG:   NO: 1
*Jun 11 21:03:53:286 2012 liantong-VPDN IKE/7/DEBUG:   ID: 1
*Jun 11 21:03:53:286 2012 liantong-VPDN IKE/7/DEBUG:   Transform 1's attributes
*Jun 11 21:03:53:286 2012 liantong-VPDN IKE/7/DEBUG:   Attribute ENCRYPTION_ALGORITHM :
3DES_CBC
*Jun 11 21:03:53:286 2012 liantong-VPDN IKE/7/DEBUG:   Attribute HASH_ALGORITHM : MD5
*Jun 11 21:03:53:286 2012 liantong-VPDN IKE/7/DEBUG:   Attribute AUTHENTICATION_METHOD :
PRE_SHARED
*Jun 11 21:03:53:287 2012 liantong-VPDN IKE/7/DEBUG:   Attribute GROUP_DESCRIPTION : MOD
P_1024
*Jun 11 21:03:53:287 2012 liantong-VPDN IKE/7/DEBUG:   Attribute LIFE_TYPE : SECONDS
```

```
*Jun 11 21:03:53:287 2012 liantong-VPDN IKE/7/DEBUG:  Attribute LIFE_DURATION : 6400
*Jun 11 21:03:53:287 2012 liantong-VPDN IKE/7/DEBUG: P1 construct VID: responder not support nat traversal.
*Jun 11 21:03:53:287 2012 liantong-VPDN IKE/7/DEBUG: exchange check: checking for required SA
//SR66发送主模式的第一次交换消息2，用于IKE提议和转换方式的协商
*Jun 11 21:03:53:287 2012 liantong-VPDN IKE/7/DEBUG: send message:
*Jun 11 21:03:54:794 2012 liantong-VPDN IKE/7/DEBUG:  ICOOKIE: 0x1992b94d05fac7c4
*Jun 11 21:03:54:795 2012 liantong-VPDN IKE/7/DEBUG:  RCOOKIE: 0xe0e726d3f22a58cd
*Jun 11 21:03:54:795 2012 liantong-VPDN IKE/7/DEBUG:  NEXT_PAYLOAD: SA
*Jun 11 21:03:54:795 2012 liantong-VPDN IKE/7/DEBUG:  VERSION: 16
*Jun 11 21:03:54:796 2012 liantong-VPDN IKE/7/DEBUG:  EXCH_TYPE: ID_PROT
*Jun 11 21:03:54:796 2012 liantong-VPDN IKE/7/DEBUG:  FLAGS: [ ]
*Jun 11 21:03:54:796 2012 liantong-VPDN IKE/7/DEBUG:  MESSAGE_ID: 0x00000000
*Jun 11 21:03:54:796 2012 liantong-VPDN IKE/7/DEBUG:  LENGTH: 80
*Jun 11 21:03:54:796 2012 liantong-VPDN IKE/7/DEBUG: exchange state machine(R): finished step 1, advancing...
//通过上面的2个消息完成主模式第一次交换，完成IKE提议和转换方式的协商
//SR66收到的主模式的第二次交换消息3，用于IKE DH和伪随机值nonce的交换
*Jun 11 21:03:54:796 2012 liantong-VPDN IKE/7/DEBUG: received message:
*Jun 11 21:03:54:797 2012 liantong-VPDN IKE/7/DEBUG:  ICOOKIE: 0x1992b94d05fac7c4
*Jun 11 21:03:56:297 2012 liantong-VPDN IKE/7/DEBUG:  RCOOKIE: 0xe0e726d3f22a58cd
*Jun 11 21:03:56:297 2012 liantong-VPDN IKE/7/DEBUG:  NEXT_PAYLOAD: KEY_EXCH
*Jun 11 21:03:56:297 2012 liantong-VPDN IKE/7/DEBUG:  VERSION: 16
*Jun 11 21:03:56:298 2012 liantong-VPDN IKE/7/DEBUG:  EXCH_TYPE: ID_PROT
*Jun 11 21:03:56:298 2012 liantong-VPDN IKE/7/DEBUG:  FLAGS: [ ]
*Jun 11 21:03:56:298 2012 liantong-VPDN IKE/7/DEBUG:  MESSAGE_ID: 0x00000000
*Jun 11 21:03:56:298 2012 liantong-VPDN IKE/7/DEBUG:  LENGTH: 184
*Jun 11 21:03:56:298 2012 liantong-VPDN IKE/7/DEBUG: check message duplicate
*Jun 11 21:03:56:298 2012 liantong-VPDN IKE/7/DEBUG: parse payloads: payload KEY_EXCH
*Jun 11 21:03:56:299 2012 liantong-VPDN IKE/7/DEBUG: parse payloads: payload NONCE
*Jun 11 21:03:56:299 2012 liantong-VPDN IKE/7/DEBUG: validate payload KEY_EXCH
*Jun 11 21:03:56:299 2012 liantong-VPDN IKE/7/DEBUG: validate payload NONCE
*Jun 11 21:03:57:700 2012 liantong-VPDN IKE/7/DEBUG: exchange check: checking for required KEY_EXCH
*Jun 11 21:03:57:700 2012 liantong-VPDN IKE/7/DEBUG: exchange check: checking for required NONCE
*Jun 11 21:03:57:700 2012 liantong-VPDN IKE/7/DEBUG: exchange state machine(R): finished step 2, advancing...
*Jun 11 21:03:57:700 2012 liantong-VPDN IKE/7/DEBUG: add payload to message: KEY_EXCH
*Jun 11 21:03:57:700 2012 liantong-VPDN IKE/7/DEBUG:  Group ID: 2
*Jun 11 21:03:57:701 2012 liantong-VPDN IKE/7/DEBUG: add payload to message: NONCE
*Jun 11 21:03:57:701 2012 liantong-VPDN IKE/7/DEBUG: add payload to message: VENDOR
*Jun 11 21:03:57:701 2012 liantong-VPDN IKE/7/DEBUG:
IKE_DPD:: send VID : afcad713 68a1f1c9 6b8696fc 77570100 (DPD)
*Jun 11 21:03:57:701 2012 liantong-VPDN IKE/7/DEBUG: exchange check: checking for required KEY_EXCH
*Jun 11 21:03:57:701 2012 liantong-VPDN IKE/7/DEBUG: exchange check: checking for required NONCE
//SR66发送的主模式的第二次交换消息4，用于IKE DH和伪随机值nonce的交换
*Jun 11 21:03:57:701 2012 liantong-VPDN IKE/7/DEBUG: send message:
*Jun 11 21:03:57:702 2012 liantong-VPDN IKE/7/DEBUG:  ICOOKIE: 0x1992b94d05fac7c4
*Jun 11 21:03:59:202 2012 liantong-VPDN IKE/7/DEBUG:  RCOOKIE: 0xe0e726d3f22a58cd
*Jun 11 21:03:59:202 2012 liantong-VPDN IKE/7/DEBUG:  NEXT_PAYLOAD: KEY_EXCH
*Jun 11 21:03:59:202 2012 liantong-VPDN IKE/7/DEBUG:  VERSION: 16
*Jun 11 21:03:59:203 2012 liantong-VPDN IKE/7/DEBUG:  EXCH_TYPE: ID_PROT
*Jun 11 21:03:59:203 2012 liantong-VPDN IKE/7/DEBUG:  FLAGS: [ ]
*Jun 11 21:03:59:203 2012 liantong-VPDN IKE/7/DEBUG:  MESSAGE_ID: 0x00000000
*Jun 11 21:03:59:203 2012 liantong-VPDN IKE/7/DEBUG:  LENGTH: 204
*Jun 11 21:03:59:203 2012 liantong-VPDN IKE/7/DEBUG: exchange state machine(R): finished step 3, advancing...
//通过上面的2个消息完成主模式第二次交换，完成IKE DH和伪随机值nonce的交换
//SR66收到的主模式的第三次交换消息5，用于通信双方的身份认证
*Jun 11 21:03:59:203 2012 liantong-VPDN IKE/7/DEBUG: received message:
*Jun 11 21:03:59:204 2012 liantong-VPDN IKE/7/DEBUG:  ICOOKIE: 0x1992b94d05fac7c4
```

```
*Jun 11 21:03:59:204 2012 liantong-VPDN IKE/7/DEBUG:   RCOOKIE: 0xe0e726d3f22a58cd
*Jun 11 21:03:59:204 2012 liantong-VPDN IKE/7/DEBUG:   NEXT_PAYLOAD: ID
*Jun 11 21:03:59:204 2012 liantong-VPDN IKE/7/DEBUG:   VERSION: 16
*Jun 11 21:03:59:204 2012 liantong-VPDN IKE/7/DEBUG:   EXCH_TYPE: ID_PROT
*Jun 11 21:03:59:204 2012 liantong-VPDN IKE/7/DEBUG:   FLAGS: [ ENC ]
*Jun 11 21:04:00:705 2012 liantong-VPDN IKE/7/DEBUG:   MESSAGE_ID: 0x00000000
*Jun 11 21:04:00:705 2012 liantong-VPDN IKE/7/DEBUG:   LENGTH: 68
*Jun 11 21:04:00:705 2012 liantong-VPDN IKE/7/DEBUG: check message duplicate
*Jun 11 21:04:00:705 2012 liantong-VPDN IKE/7/DEBUG: parse payloads: payload ID
*Jun 11 21:04:00:705 2012 liantong-VPDN IKE/7/DEBUG: parse payloads: invalid next payload type 223 in payload of type 5
```

通过debug信息可以分析出IKE主模式6个消息交互的第5个消息就进行不行去了，原因为parse payloads: invalid next payload type 223 in payload of type 5。

我们知道，消息5是用来进行双方身份认证的，对SR66来说，打印这个消息表示对端发过来的报文经解密之后认为是错的，一般情况下，两端密码配置不一致会导致这种情况。

四、　解决方法：

根据上面的debug信息，可以定位问题原因为两端设备pre-shared-key配置不一致。

通过办事处咨询友商，其反馈密码就是crypto isakmp key 7 summer address 148.10.2.30中配置的summer，因为SR66这边的配置为密文，不能判断是否密码配置正确，协调办事处修改为明文显示summer后，发现还是IKE第一阶段协商失败，debug信息与上面debug信息类似，消息5还是显示发过来的报文解密后是错的。这是为什么呢？

没有办法，我们这边密码修改后肯定是正确的，对端一定是像友商工程师说的吗？登录友商网站查询，发现其配置手册中有这样的命令说明：

crypto isakmp key 0|7 keystring { hostname peer-hostname | address peer-address }

指定与特定远程IKE 对等体一起使用的共享密钥。

数字0 为输入为明文

数字7 为输入为密文

友商原配置为crypto isakmp key 7 summer address 148.10.2.30，按照命令说明理解，这里输入的summer是密文，并不是真正的密码，而是密码在锐捷设备上加密后的显示。

协调将其配置修改为crypto isakmp key **0 summer** address 148.10.2.30，代表输入的summer是真正的密码，修改后SR66与其IPSEC协商成功，问题解决。