某局点分支V7 MSR对接总部V5 MSR建立IPSEC失败问题处理经验案例

IPSec VPN 孟普 2018-07-21 发表

组网及说明

某局点总部为V5 MSR设备，分支为很多个V7 MSR设备，分支出口是拨号上网，地址不固定，所以采用野蛮模式对接IPSEC。

问题描述

很多个分支都能正常对接，但是有一个分支却始终建立不起来。

过程分析

1.首先检查两边配置，对比两边没发现有什么异常

分支

```
  dis cu
#
 version 7.1.064, Release 0605P18
#
interface Eth-channel1/0:0
 dialer circular enable
 dialer-group 89
 dialer timer autodial 5
 dialer number #777 autodial
 ip address cellular-alloc
 nat outbound 3000
 apn-profile apply profile69
 ipsec apply policy zongbu
#
acl advanced 3000
 rule 2 deny ip source 10.10.200.0 0.0.0.255 destination 10.10.80.0 0.0.0.255
 rule 3 deny ip source 10.10.200.0 0.0.0.255 destination 10.10.82.0 0.0.0.255
 rule 5 deny ip source 10.10.200.0 0.0.0.255 destination 1.1.1.1 0
 rule 100 permit ip
#
acl advanced 3001
 rule 2 permit ip source 10.10.200.0 0.0.0.255 destination 10.10.80.0 0.0.0.255
 rule 3 permit ip source 10.10.200.0 0.0.0.255 destination 10.10.82.0 0.0.0.255
 rule 5 permit ip source 10.10.200.0 0.0.0.255 destination 1.1.1.1 0
#
ipsec transform-set skshu
#
ipsec transform-set zongbu
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
ipsec policy zongbu 65535 isakmp
 transform-set zongbu
 security acl 3001
 remote-address 59.X.X.66
 ike-profile zongbu
 sa duration time-based 3600
 sa duration traffic-based 1843200
#
 ike identity fqdn nanchang
#
ike profile zongbu
 keychain zongbu
 exchange-mode aggressive
 local-identity fqdn nanchang
 match remote identity address 59.X.X.66 255.255.255.255
```

```
 match remote identity fqdn zongbu
 proposal 65535
#
ike proposal 65535
 encryption-algorithm 3des-cbc
 dh group2
 authentication-algorithm md5
#
ike keychain zongbu
 pre-shared-key address 59.X.X.66 255.255.255.255 key cipher $c$3$djo7P0ag+OsDnerdgah
Z3Qnom6Nm+Jt1MvI=
#
```

总部

```
[SKS_BGB_2F_MSR5060_MASTER]dis cu
#
 version 5.20, Release 2511P02, Basic
#
 ike local-name zongbu
#
ike proposal 11
 encryption-algorithm 3des-cbc
 dh group2
 authentication-algorithm md5
#
ike peer nanchang
 exchange-mode aggressive
 proposal 11
 pre-shared-key cipher $c$3$9Iw1HrJDDiCer+J8rvgF8QGdJzI1RVXy
 id-type name
 remote-name nanchang
 local-address 59.X.X.66
 local-name zongbu
 nat traversal
#
ipsec transform-set zongbu
 encapsulation-mode tunnel
 transform esp
 esp authentication-algorithm md5
 esp encryption-algorithm 3des
#
ipsec policy skshu 34 isakmp
 security acl 3031
 ike-peer nanchang
 transform-set zongbu
#
interface GigabitEthernet0/2
 port link-mode route
 nat outbound 3000
 ip address 59.X.X.66 255.255.255.240
 tcp mss 1024
 ipsec policy skshu
#
acl number 3031
 rule 0 permit ip source 10.10.82.0 0.0.0.255 destination 10.10.200.0 0.0.0.255
 rule 1 permit ip source 10.10.80.0 0.0.0.255 destination 10.10.200.0 0.0.0.255
 rule 5 permit ip source 1.1.1.1 0 destination 10.10.200.0 0.0.0.255
```

2.查看分支debug信息如下：

```
Sending packet to 59.X.X.66 remote port 500, local port 500.
*Jan  1 19:11:17:899 2011 H3C IKE/7/PACKET: vrf = 0, local = 10.168.251.61, remote = 59.X.X.
66/500
```

I-COOKIE: 54e86bab2146b2b6
R-COOKIE: 0000000000000000
next payload: SA
version: ISAKMP Version 1.0
exchange mode: Aggressive
flags:
message ID: 0
length: 384
Request time out
*Jan 1 19:11:17:899 2011 H3C IKE/7/PACKET: vrf = 0, local = 10.168.251.61, remote = 59.X.X.66/500
Sending an IPv4 packet.
*Jan 1 19:11:17:900 2011 H3C IKE/7/EVENT: vrf = 0, local = 10.168.251.61, remote = 59.X.X.66/500
Sent data to socket successfully.//成功将协商报文发给对端总部
*Jan 1 19:11:18:011 2011 H3C IKE/7/EVENT: Received packet successfully.//收到对端的回应报文
*Jan 1 19:11:18:011 2011 H3C IKE/7/PACKET: vrf = 0, local = 10.168.251.61, remote = 59.X.X.66/500
Received packet from 59.X.X.66 source port 500 destination port 500.
*Jan 1 19:11:18:011 2011 H3C IKE/7/PACKET: vrf = 0, local = 10.168.251.61, remote = 59.X.X.66/500

1. COOKIE: 54e86bab2146b2b6
   R-COOKIE: 40faf251d656d518
   next payload: SA
   version: ISAKMP Version 1.0
   exchange mode: Aggressive
   flags:
   message ID: 0
   length: 350
   *Jan 1 19:11:18:012 2011 H3C IKE/7/EVENT: IKE thread 1097143584 processes a job.
   *Jan 1 19:11:18:012 2011 H3C IKE/7/EVENT: Phase1 process started.
   *Jan 1 19:11:18:012 2011 H3C IKE/7/PACKET: vrf = 0, local = 10.168.251.61, remote = 59.X.X.66/500
   Received ISAKMP Security Association Payload.
   Request time out
   *Jan 1 19:11:18:012 2011 H3C IKE/7/PACKET: vrf = 0, local = 10.168.251.61, remote = 59.X.X.66/500
   Received ISAKMP Key Exchange Payload.
   *Jan 1 19:11:18:012 2011 H3C IKE/7/PACKET: vrf = 0, local = 10.168.251.61, remote = 59.X.X.66/500
   Received ISAKMP Nonce Payload.
   *Jan 1 19:11:18:012 2011 H3C IKE/7/PACKET: vrf = 0, local = 10.168.251.61, remote = 59.X.X.66/500
   Received ISAKMP Vendor ID Payload.
   *Jan 1 19:11:18:012 2011 H3C IKE/7/PACKET: vrf = 0, local = 10.168.251.61, remote = 59.X.X.66/500
   Received ISAKMP Identification Payload.
   *Jan 1 19:11:18:012 2011 H3C IKE/7/PACKET: vrf = 0, local = 10.168.251.61, remote = 59.X.X.66/500
   Received ISAKMP Vendor ID Payload.
   *Jan 1 19:11:18:012 2011 H3C IKE/7/PACKET: vrf = 0, local = 10.168.251.61, remote = 59.X.X.66/500
   Received ISAKMP NAT-D Payload.
   *Jan 1 19:11:18:012 2011 H3C IKE/7/PACKET: vrf = 0, local = 10.168.251.61, remote = 59.X.X.66/500
   Received ISAKMP NAT-D Payload.
   *Jan 1 19:11:18:013 2011 H3C IKE/7/PACKET: vrf = 0, local = 10.168.251.61, remote = 59.X.X.66/500
   Received ISAKMP Hash Payload.
   *Jan 1 19:11:18:013 2011 H3C IKE/7/PACKET: vrf = 0, local = 10.168.251.61, remote = 59.X.X.66/500
   Process NONCE payload.

*Jan 1 19:11:18:013 2011 H3C IKE/7/PACKET: vrf = 0, local = 10.168.251.61, remote = 59.X.X.
66/500
Process KE payload.
*Jan 1 19:11:18:013 2011 H3C IKE/7/PACKET: vrf = 0, local = 10.168.251.61, remote = 59.X.X.
66/500
Process ID payload.
*Jan 1 19:11:18:013 2011 H3C IKE/7/PACKET: vrf = 0, local = 10.168.251.61, remote = 59.X.X.
66/500
Peer ID type: FQDN (2).
*Jan 1 19:11:18:013 2011 H3C IKE/7/PACKET: vrf = 0, local = 10.168.251.61, remote = 59.X.X.
66/500
Peer ID value: FQDN zongbu.
*Jan 1 19:11:18:013 2011 H3C IKE/7/PACKET: vrf = 0, local = 10.168.251.61, remote = 59.X.X.
66/500
Process SA payload.
*Jan 1 19:11:18:013 2011 H3C IKE/7/PACKET: vrf = 0, local = 10.168.251.61, remote = 59.X.X.
66/500
Check ISAKMP transform 1.
*Jan 1 19:11:18:014 2011 H3C IKE/7/PACKET: vrf = 0, local = 10.168.251.61, remote = 59.X.X.
66/500
Encryption algorithm is 3DES-CBC.
Request time out
*Jan 1 19:11:18:014 2011 H3C IKE/7/PACKET: vrf = 0, local = 10.168.251.61, remote = 59.X.X.
66/500
HASH algorithm is HMAC-MD5.
*Jan 1 19:11:18:014 2011 H3C IKE/7/PACKET: vrf = 0, local = 10.168.251.61, remote = 59.X.X.
66/500
DH group is 2.
*Jan 1 19:11:18:014 2011 H3C IKE/7/PACKET: vrf = 0, local = 10.168.251.61, remote = 59.X.X.
66/500
Authentication method is Pre-shared key.
*Jan 1 19:11:18:015 2011 H3C IKE/7/PACKET: vrf = 0, local = 10.168.251.61, remote = 59.X.X.
66/500
Lifetime type is 1.
*Jan 1 19:11:18:015 2011 H3C IKE/7/PACKET: vrf = 0, local = 10.168.251.61, remote = 59.X.X.
66/500
Life duration is 86400.
*Jan 1 19:11:18:015 2011 H3C IKE/7/EVENT: No pre-shared key found based on name zongb
u.
*Jan 1 19:11:18:015 2011 H3C IKE/7/EVENT: vrf = 0, local = 10.168.251.61, remote = 59.X.X.6
6/500
Found pre-shared key that matches address 59.X.X.66 in keychain zongbu.
*Jan 1 19:11:18:015 2011 H3C IKE/7/PACKET: vrf = 0, local = 10.168.251.61, remote = 59.X.X.
66/500
Attributes is acceptable.
*Jan 1 19:11:18:015 2011 H3C IKE/7/EVENT: Oakley transform 1 is acceptable.
*Jan 1 19:11:18:015 2011 H3C IKE/7/PACKET: vrf = 0, local = 10.168.251.61, remote = 59.X.X.
66/500
Process vendor ID payload.
*Jan 1 19:11:18:015 2011 H3C IKE/7/EVENT: Vendor ID DPD is matched.
*Jan 1 19:11:18:016 2011 H3C IKE/7/EVENT: Vendor ID NAT-T rfc3947 is matched.
*Jan 1 19:11:18:016 2011 H3C IKE/7/PACKET: vrf = 0, local = 10.168.251.61, remote = 59.X.X.
66/500
Received 2 NAT-D payload.
*Jan 1 19:11:18:016 2011 H3C IKE/7/EVENT: vrf = 0, local = 10.168.251.61, remote = 59.X.X.6
6/500
I am behind NAT.
*Jan 1 19:11:18:016 2011 H3C IKE/7/EVENT: vrf = 0, local = 10.168.251.61, remote = 59.X.X.6
6/4500
Float port to local port 4500 and remote port 4500
*Jan 1 19:11:18:080 2011 H3C IKE/7/PACKET: vrf = 0, local = 10.168.251.61, remote = 59.X.X.
66/4500
Verify HASH payload.
Request time out

*Jan 1 19:11:18:081 2011 H3C IKE/7/PACKET: vrf = 0, local = 10.168.251.61, remote = 59.X.X.66/4500
HASH:
756b0298 5f8d50fe 55e057b4 d711bf3a
*Jan 1 19:11:18:081 2011 H3C IKE/7/ERROR: vrf = 0, local = 10.168.251.61, remote = 59.X.X.66/4500
Failed to verify the peer HASH.//前面解开对端发来的协商报文后检查HASH信息报错
*Jan 1 19:11:18:081 2011 H3C IKE/7/PACKET: vrf = 0, local = 10.168.251.61, remote = 59.X.X.66/4500
Construct notification packet: AUTHENTICATION_FAILED.
*Jan 1 19:11:18:081 2011 H3C IKE/7/PACKET: vrf = 0, local = 10.168.251.61, remote = 59.X.X.66/4500
Sending packet to 59.X.X.66 remote port 4500, local port 4500.

3、从debug中可以很明显的看到Failed to verify the peer HASH，从对端发来的协商报文HASH报错，这种报错一般就是两边加密方式或者加密不一致，加密方式可以在配置中比对，前面已经检查两边是加密算法都是一致的了，那就有可能是两边的密钥不一致。

解决方法

在两边加密方式配置一致的情况下报错Failed to verify the peer HASH，很有可能就是密钥不一致，因为密钥在配置中是不可见的，那就只有将两边的密钥删除重新配置，然后重新协商，发现可以正常建立IPSEC隧道。