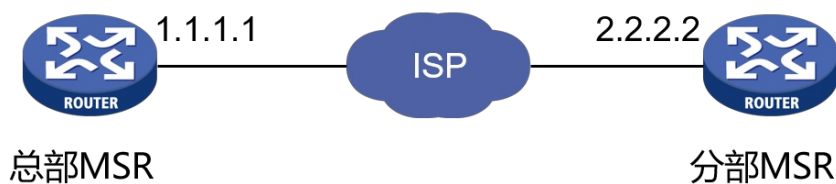


知 H3C MSR(V7) IPsec VPN野蛮模板方式IKE超时导致VPN建立失败问题

IPsec 丁犁 2018-03-23 发表

某局点总部与多个分支MSR之间部署IPsec VPN野蛮模板方式，其中发现一个分支节点MSR与总部设备IPsec VPN建立失败。



检查分支MSR设备IPsec VPN基本配置，未发现异常。其关键配置如下：

```
#
ipsec transform-set h3cnc
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
ipsec policy h3cnc 65534 isakmp
 transform-set h3cnc
 security acl 3000
 remote-address 1.1.1.1
 ike-profile h3cnc
 sa duration time-based 28800
 sa duration traffic-based 1843200
#
ike identity fqdn h3cnc
#
ike profile h3cnc
 keychain h3cnc
 exchange-mode aggressive
 local-identity fqdn h3cnc
 match remote identity fqdn sangfornc
 proposal 65534
#
ike proposal 65534
 encryption-algorithm 3des-cbc
 dh group2
 authentication-algorithm md5
 sa duration 3600
#
ike keychain h3cnc
 pre-shared-key address 1.1.1.1 255.255.255.255 key cipher $c$3$ESr300c6AM1cd8EoQgB0BHvbk
 SdNL3A5XA==
#
interface GigabitEthernet0/0
 port link-mode route
 ip address 2.2.2.2 255.255.255.252
 nat outbound 3001
 ipsec apply policy h3cnc
#
```

检查分支基本配置无异常，在分支MSR设备上开启debug ike all，使用感兴趣流触发IPsec VPN建立，观察报文交互情况，其中：

```
*Jan 3 00:56:54:205 2011 Nanchuan IKE/7/EVENT: vrf = 0, local = 2.2.2.2, remote = 1.1.1.1/500 IK
E SA state changed from IKE_P1_STATE_INIT to IKE_P1_STATE_SEND1. *Jan 3 00:56:54:205 20
11 Nanchuan IKE/7/PACKET: vrf = 0, local = 2.2.2.2, remote = 1.1.1.1/500 Sending packet to 1.1.1.1
remote port 500, local port 500. *Jan 3 00:56:54:205 2011 Nanchuan IKE/7/PACKET: vrf = 0, local =
2.2.2.2, remote = 1.1.1.1/500 I-COOKIE: bc1fffc0402cd7dd R-COOKIE: 0000000000000000 nex
t payload: SA version: ISAKMP Version 1.0 exchange mode: Aggressive flags: message ID: 0
```

length: 380 *Jan 3 00:56:54:205 2011 Nanchuan IKE/7/PACKET: vrf = 0, local = 2.2.2.2, remote = 1.1.1.1/500 Sending an IPv4 packet. *Jan 3 00:56:54:206 2011 Nanchuan IKE/7/EVENT: vrf = 0, local = 2.2.2.2, remote = 1.1.1.1/500 Sent data to socket successfully. //到这里ike协商报文已经成功发出去
Request time out *Jan 3 00:56:56:361 2011 Nanchuan IPSEC/7/EVENT: Found block-flow node. *Jan 3 00:56:56:361 2011 Nanchuan IPSEC/7/PACKET: Failed to find SA by SP, SP Index = 0, SP Convert-Seq = 4294836224. *Jan 3 00:56:56:361 2011 Nanchuan IPSEC/7/ERROR: The reason of dropping packet is no available IPsec tunnel. Request time out *Jan 3 00:56:58:564 2011 Nanchuan IPSEC/7/EVENT: Found block-flow node. *Jan 3 00:56:58:564 2011 Nanchuan IPSEC/7/PACKET: Failed to find SA by SP, SP Index = 0, SP Convert-Seq = 4294836224. *Jan 3 00:56:58:564 2011 Nanchuan IPSEC/7/ERROR: The reason of dropping packet is no available IPsec tunnel. *Jan 3 00:56:59:725 2011 Nanchuan IKE/7/PACKET: vrf = 0, local = 2.2.2.2, remote = 1.1.1.1/500 **Retransmit phase 1 packet. //但是分支MSR没有收到总部的IKE回应报文**

由于分支MSR设备无法收到总部发来的IKE协商报文，因此联系ISP调整线路后，IPSec VPN建立成功，问题解决。

对于IPSec VPN建立失败的问题，可通过debug ike all方式检查报文协商过程。