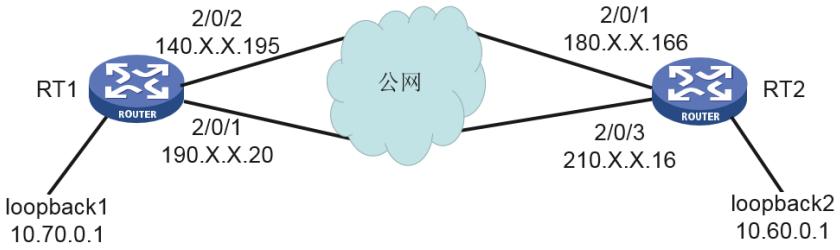
MSR5620 双出口配置IPSec vpn失败经验案例

IPSec VPN　苟新楼　2018-09-25 发表

组网及说明



问题描述

两台MSR5620作为出口设备，分别连接两根外网线，通过公网建立IPSec vpn。相关配置完成后，感兴趣流地址互ping不通。两台设备的display ike sa显示都为unknown，ike阶段都没有建立起来：

RT1：

```
< RT1>display ike sa
Connection-ID   Remote      Flag       DOI
-----------------------------------------------------------------
  117    180.X.X.166    Unknown     IPsec
```

RT2：

```
< RT2>display ike sa
Connection-ID   Remote      Flag       DOI
-----------------------------------------------------------------
  925    140.X.X.195    Unknown     IPsec
```

过程分析

1、两台设备公网地址互通的前提下，检查两端配置：

RT1：

```
#
interface LoopBack70
 ip address 10.70.0.1 255.255.255.0
#
interface GigabitEthernet2/0/2
 ip address 140.X.X.195 255.255.255.0
 nat outbound 3001
 ipsec apply policy sq
#
ip route-static 10.60.0.1 32 140.X.X.192
#
acl advanced 3001
 rule 12 deny ip source 10.70.0.1 0 destination 10.60.0.1 0
 rule 100 permit ip
#
acl advanced 3012
 rule 55 permit ip source 10.70.0.1 0 destination 10.60.0.1 0
#
ipsec transform-set 1
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
ipsec policy sq 1 isakmp
 transform-set 1
 security acl 3012
 local-address 140.X.X.195
 remote-address 180.X.X.166
 ike-profile sq
#
 ike identity fqdn dx
```

#
ike profile sq
 keychain sq
 local-identity address 140.X.X.195
 match remote identity address 180.X.X.166 255.255.255.255
 proposal 1
#
ike proposal 1
 encryption-algorithm 3des-cbc
 dh group2
 authentication-algorithm md5
#
ike keychain sq
 pre-shared-key address 180.X.X.166 255.255.255.255 key cipher c3$3M1ZR4VWG/7x81M
Qa+anzqKNObKUP1r8CVTx8=
#
RT2：
RT2配置除了相关地址与RT1不同，其他相关参数均一致。

2、核对两端IPSec vpn的配置无误，此时在RT2上开启debugging ike sa以及debugging ipsec sa，相关报错如下：
*Sep 10 16:47:09:053 2018 RT2 IKE/7/EVENT: **Phase1 process started**.
*Sep 10 16:47:09:054 2018 RT2 IKE/7/PACKET: vrf = 0, local = **180.X.X.166**, remote = **140.X.X.195/500**
Collision of phase 1 negotiation is found.
RT2收到了来自RT1的IKE报文，在IKE协商过程中提示了冲突。在设备上开启debugging ip packet查看数据包交互情况：
*Sep 10 16:47:22:721 2018 RT2 IPFW/7/IPFW_PACKET:
Receiving, interface = **GigabitEthernet2/0/1**, version = 4, headlen = 20, tos = 252,
pktlen = 204, pktid = 65, offset = 0, ttl = 254, protocol =17
checksum = 50690, s = 140.X.X.195, d = 180.X.X.166
prompt: Receiving IP packet.
* Sep 10 16:47:22:721 2018 RT2 IPFW/7/IPFW_PACKET:
Sending, interface = **GigabitEthernet2/0/3**, version = 4, headlen= 20, tos = 252,
pktlen = 144, pktid = 60, offset = 0, ttl = 255, protocol =17
checksum = 50499, s = 180.X.X.166, d = 140.X.X.195
prompt: Sending the packet from local at GigabitEthernet2/0/3
可以看出数据包从GigabitEthernet2/0/1接收，结果从GigabitEthernet2/0/3发出。在RT2上查看路由发现：
ip route-static 0.0.0.0 0 210.X.X.17
ip route-static 0.0.0.0 0 180.X.X.165 preference 70
从这里可以发现问题所在，当10.70.0.1去ping 10.60.0.1时，感兴趣流在RT1的GigabitEthernet2/0/2口进行IPSec封装后通过公网到达RT2的GigabitEthernet2/0/1。
RT2在回应报文的时候，由于RT2配置出接口为GigabitEthernet2/0/1的默认路由优先级比出接口为GigabitEthernet2/0/3的优先级低，数据包优先从GigabitEthernet2/0/3发出，路径不一致导致协商冲突。
在RT2上配置去往140.X.X.195的明细路由，下一跳指向180.X.X.165，此时ike sa和ipsec sa可以正常建立。
display ike sa
Connection-ID Remote   Flag   DOI
---
 116   180.X.X.166   RD   IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY
display ipsec sa

  IPsec policy: sq
  Sequence number: 1
  Mode: ISAKMP

    Tunnel id: 0
    Encapsulation mode: tunnel
    Perfect Forward Secrecy:
    Inside VPN:

Extended Sequence Numbers enable: N
Traffic Flow Confidentiality enable: N
Path MTU: 1444
Tunnel:
  local address: 140.X.X.195
  remote address: 180.X.X.166
Flow:
  sour addr: 10.70.0.1/255.255.255.255 port: 0 protocol: ip
  dest addr: 10.60.0.1/255.255.255.255 port: 0 protocol: ip
[Inbound ESP SAs]
 SPI: 1628414150 (0x610fa0c6)
 Connection ID: 545460846593
 Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
 SA duration (kilobytes/sec): 1843200/3600
 SA remaining duration (kilobytes/sec): 1843199/3299
 Max received sequence-number: 4
 Anti-replay check enable: Y
 Anti-replay window size: 64
 UDP encapsulation used for NAT traversal: N
 Status: Active
[Outbound ESP SAs]
 SPI: 2623005100 (0x9c57e1ac)
 Connection ID: 708669603842
 Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
 SA duration (kilobytes/sec): 1843200/3600
 SA remaining duration (kilobytes/sec): 1843199/3299
 Max sent sequence-number: 4
 UDP encapsulation used for NAT traversal: N
 Status: Active

解决方法

在两台路由器上配置去往对端公网地址的明细路由，保证感兴趣流到达对端设备后从一个端口接收，并且从该端口发出。

< RT1>ip route-static 180.X.X.166 24 140.X.X.192

< RT2>ip route-static 140.X.X.195 24 180.X.X.165

在双出口的组网下，不仅仅需要配置去往对端感兴趣流的明细路由，还需要注意公网之间互通的路由选择，确保感兴趣流到达对端设备后从一个接口接收，回应报文时也从该接口发出。