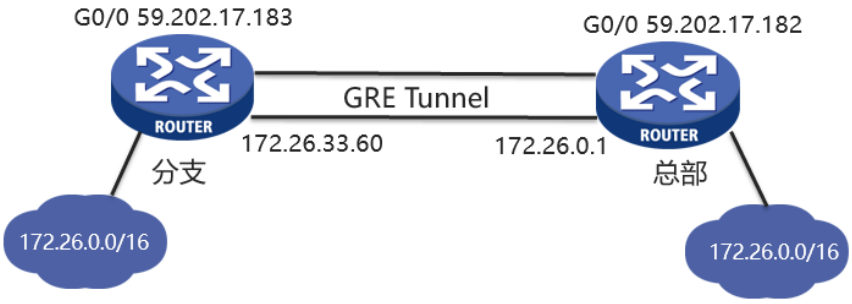
MSR810（国密）建立gre over ipsec隧道数据不通的经验排查案例

国密卡 IPSec VPN GRE VPN 李熙 2021-07-31 发表

组网及说明

MSR810作为分支采用国密方式同总部的MSR810建立gre over ispec，目前仅建立一条隧道。



问题描述

ike sa和ipsec sa都有，gre隧道口也是up的，但分布侧带tunnel源地址ping tunnel目的地址不通。

隧道口不通：

[测试]ping -a 172.26.33.60 172.26.0.1

Ping 172.26.0.1 (172.26.0.1) from 172.26.33.60: 56 data bytes, press CTRL+C to break

Request time out

Request time out

Request time out

Request time out

Request time out

--- Ping statistics for 172.26.0.1 --- 5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss

过程分析

1、查看ike sa和ipsec sa均建立

```
[测试]dis ike sa
    Connection-ID   Local              Remote             Flag      DOI
--------------------------------------------------------------------------------
    2               59.202.17.183      59.202.17.182      RD        IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY
```

```
[测试]dis ipsec sa
-------------------------------
Interface: GigabitEthernet0/0
-------------------------------

  ----------------------------
  IPsec policy: fenbu
  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: 1428
    Tunnel:
        local  address: 59.202.17.183
        remote address: 59.202.17.182
    Flow:
        sour addr: 172.26.33.60/255.255.255.255  port: 0  protocol: ip
        dest addr: 172.26.0.1/255.255.255.255  port: 0  protocol: ip
```

2、tunnel口是up的

```
Tun0                UP   UP       172.16.33.60
Vlan1               UP   UP       159.45.64.81    LAN-interface
```

3、分支侧display ipsec statistics计数无增长，但是debug ip paket有发出包
发出报文持续为0

```
[测试]dis ipsec statistics
  IPsec packet statistics:
    Received/sent packets: 0/0
    Received/sent bytes: 0/0
    Dropped packets (received/sent): 0/4

    Dropped packets statistics
      No available SA: 4
      Wrong SA: 0
      Invalid length: 0
      Authentication failure: 0
      Encapsulation failure: 0
      Decapsulation failure: 0
      Replayed packets: 0
      ACL check failure: 0
      MTU check failure: 0
      Loopback limit exceeded: 0
      Crypto speed limit exceeded: 0
```

分支debug看报文有发出

```
*Jan  1 01:29:09:242 2011 测试 IPFW/7/IPFW_PACKET:
Receiving, interface = GigabitEthernet0/0
version = 4, headlen = 20, tos = 252
pktlen = 112, pktid = 124, offset = 0, ttl = 255, protocol = 17
checksum = 7940, s = 59.202.17.182, d = 59.202.17.183
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Receiving IP packet from interface GigabitEthernet0/0.
Payload: UDP
  source port = 500, destination port = 500
  checksum = 0xffbb, length = 92.
```

4、总部ping分支时，计数正常增长，怀疑分支侧有问题

<zongbu>dis ipsec statistics

IPsec packet statistics:

Received/sent packets: 0/15

Received/sent bytes: 0/1440

Dropped packets (received/sent): 0/0

Dropped packets statistics
No available SA: 0
Wrong SA: 0
Invalid length: 0
Authentication failure: 0
Encapsulation failure: 0
Decapsulation failure: 0
Replayed packets: 0
ACL check failure: 0
MTU check failure: 0
Loopback limit exceeded: 0
Crypto speed limit exceeded: 0

5、当不用国密算法时，隧道能正常通信，怀疑是硬件加密模块故障。

解决方法

替换硬件加密模块。