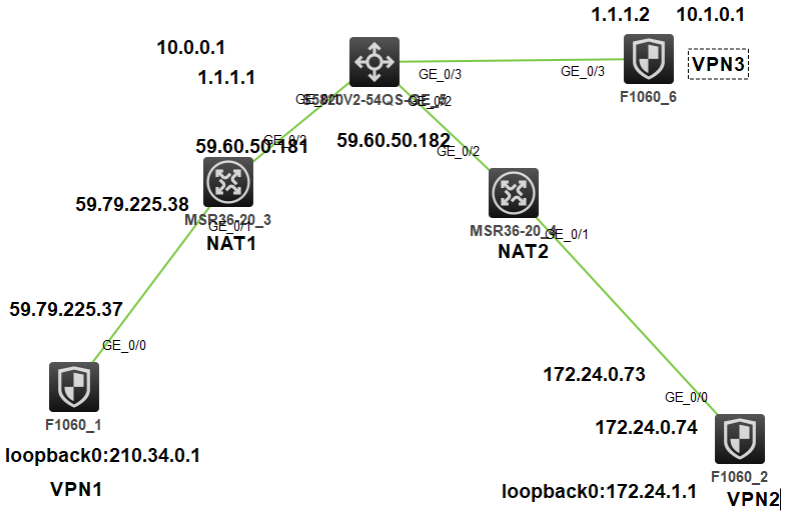
某局点F1000 IPSEC内网不通

IPSec VPN　孔德飞　2022-01-10 发表

组网及说明

现场VPN1与VPN2建立IPSEC，VPN1与VPN2分别做NAT穿越，对应的NAT设备为NAT1与NAT2,VPN1与VPN2以loopback地址作为感兴趣流

同时NAT1与VPN3也以NAT1接口的地址与VPN3建立IPSEC



问题描述

此时VPN1与VPN2的IPSEC已经建立，但是内网不通

```
<H3C>display ike sa
   Connection-ID   Remote              Flag        DOI
-------------------------------------------------------------------------
   2               59.60.50.182        RD          IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY
<H3C>dis
<H3C>display  ips
<H3C>display  ipsec sa
-------------------------------
Interface: GigabitEthernet1/0/0
-------------------------------

  ------------------------------
  IPsec policy: GE1/0/5
  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: 1420
    Tunnel:
        local  address: 59.79.225.37
        remote address: 59.60.50.182
    Flow:
        sour addr: 210.34.0.0/255.255.0.0  port: 0  protocol: ip
        dest addr: 172.24.1.0/255.255.255.0  port: 0  protocol: ip

    [Inbound ESP SAs]
      SPI: 1658787368 (0x62df1628)
      Connection ID: 12884901888
      Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843200/3582
      Max received sequence-number: 0
      Anti-replay check enable: Y
      Anti-replay window size: 64
      UDP encapsulation used for NAT traversal: Y
      Status: Active

    [Outbound ESP SAs]
      SPI: 1855698879 (0x6e9bb7bf)
      Connection ID: 4294967297
      Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843199/3582
      Max sent sequence-number: 4
      UDP encapsulation used for NAT traversal: Y
      Status: Active
<H3C>
```

过程分析

在NAT1设备上，Debug查看，有ISPEC丢包

*Jan 10 14:21:35:111 2022 H3C IPFW/7/IPFW_INFO:
MBUF was intercepted! Phase Num is 1(pre routing), Service ID is 7(ipsec), Bitmap is 1a00080, return 1(0:continue, 1:dropped, 2:consumed, 3:enqueued, 4:relay)! Interface is GigabitEthernet0/2,
s= 59.60.50.182, d= 59.60.50.181, protocol= 17, pktid = 46.

经分析，NAT1设备将VPN1设备建立IPSEC的地址做了NAT,但是使用的是接口地址，同时NAT1设备又以1.1.1.1的sub地址与VPN3的1.1.1.2地址建立IPSEC，当前设备处理的流程是，如果设备收到一个IPSEC报文的目的地址是本地接口地址，就会走本设备接口下的IPSEC解密流程，由于VPN1访问VPN2的时候，使用的是VPN1与VPN2的IPSEC隧道，这个回程报文走到NAT1设备上，当然走不了解密流程。

```
interface GigabitEthernet0/2
 port link-mode route
 combo enable copper
 ip address 59.60.50.181 255.255.255.0
 ip address 1.1.1.1 255.255.255.0 sub
 nat outbound 3001 port-preserved
 nat server global 59.60.50.181 inside 59.79.225.37 reversible
 ipsec apply policy test
```

解决方法

```
interface GigabitEthernet0/2
 port link-mode route
 combo enable copper
 ip address 59.60.50.183 255.255.255.0
 ip address 1.1.1.1 255.255.255.0 sub
 nat outbound 3001 port-preserved
 nat server global 59.60.50.181 inside 59.79.225.37 reversible
 ipsec apply policy test
```

在NAT1设备上配置NAT SERVER映射VPN1设备的地址的时候，使用的地址和接口同一个网段，但是改地址又不是设备地址

改过之后，VPN1设备可以以loopback地址访问VPN2设备的loopback地址

```
<H3C>
<H3C> ping -a 210.34.0.1  172.24.1.1
Ping 172.24.1.1 (172.24.1.1) from 210.34.0.1: 56 data bytes, press CTRL_C to break
Request time out
56 bytes from 172.24.1.1: icmp_seq=1 ttl=255 time=1.000 ms
56 bytes from 172.24.1.1: icmp_seq=2 ttl=255 time=2.000 ms
56 bytes from 172.24.1.1: icmp_seq=3 ttl=255 time=2.000 ms
56 bytes from 172.24.1.1: icmp_seq=4 ttl=255 time=2.000 ms
```