MSR5620 现场配置ADVPN无法建立成功

ADVPN 余发宇 2022-07-25 发表

组网及说明

spoke----hub-----spoke

问题描述

1.Spoke1的tunnel地址 ping HUB的tunnel地址不通

```
--- Ping statistics for 192.192.10.2 ---
5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss
[redacted]ping 192.192.10.2
Ping 192.192.10.2 (192.192.10.2): 56 data bytes, press CTRL+C to break
Request time out
Request time out
Request time out
Request time out
Request time out
```

2.HUB的tunnel地址ping Spoke1的tunnel地址正常通的

```
[redacted]ping 192.192.10.12
Ping 192.192.10.12 (192.192.10.12): 56 data bytes, press CTRL+C to break
56 bytes from 192.192.10.12: icmp_seq=0 ttl=255 time=3.571 ms
56 bytes from 192.192.10.12: icmp_seq=1 ttl=255 time=3.320 ms
56 bytes from 192.192.10.12: icmp_seq=2 ttl=255 time=3.274 ms
56 bytes from 192.192.10.12: icmp_seq=3 ttl=255 time=3.332 ms
56 bytes from 192.192.10.12: icmp_seq=4 ttl=255 time=3.317 ms
```

过程分析

1、 检查HUB和spoke1的配置如下

#HUB tunnel 100的配置

interface Tunnel100 mode advpn udp

ip address ri 255.255.255.0

ospf network-type broadcast

source GigabitEthernet2/0/0

tunnel protection ipsec profile hub

vam client hub2 compatible advpn0

#spoke tunnel 100的配置

interface Tunnel100 mode advpn udp

ip address 192.192.10.12 255.255.255.0

ospf network-type broadcast

ospf dr-priority 0

source GigabitEthernet2/0/1

tunnel protection ipsec profile spoke

vam client spoke12 compatible advpn0

2、 ospf邻居关系

采用的是ospf进行通信，并且ospf邻居关系已经起来了

==========display ospf peer==========

OSPF Process 10 with Router ID 192.192.10.2

Neighbor Brief Information

Area: 0.0.0.0

Router ID	Address	Pri	Dead-Time	State	Interface
192.192.10.12	192.192.10.12	0	37	Full/DROther	Tun100
192.192.10.23	192.192.10.23	0	39	Full/DROther	Tun100

3、查看现场的ike sa 和ipsec sa 都已经起来了

3.1 ike sa

==========display ike sa verbose==========

Connection ID: 26

Outside VPN:

Inside VPN:

Profile:

Transmitting entity: Responder

Initiator COOKIE: 8dce0c0c24af8e5d

Responder COOKIE: 16ef7e2740aae161

Local IP/port: 175.25.49.88/500

Local ID type: IPV4_ADDR

Local ID: 175.25.49.88

Remote IP/port: 120.133.226.87/500

Remote ID type: IPV4_ADDR

Remote ID: 120.133.226.87

Authentication-method: PRE-SHARED-KEY

Authentication-algorithm: SHA1

Encryption-algorithm: 3DES-CBC

Life duration(sec): 86400

Remaining key duration(sec): 82690

Exchange-mode: Main

Diffie-Hellman group: Group 2

NAT traversal: Not detected

Extend authentication: Disabled

Assigned IP address:

Vendor ID index:0xa59

Vendor ID sequence number:0x19

Connection ID: 27

Outside VPN:

Inside VPN:

Profile:

Local IP/port: 175.25.49.88/500

Authentication-algorithm: SHA1

Encryption-algorithm: 3DES-CBC

Life duration(sec): 86400

Remaining key duration(sec): 83803

Exchange-mode: Main

Diffie-Hellman group: Group 2

NAT traversal: Not detected

Extend authentication: Disabled

Assigned IP address:

Vendor ID index:0x793

Vendor ID sequence number:0x1a

Connection ID: 1

Outside VPN:

Inside VPN:

Profile: hub

Transmitting entity: Initiator

Initiator COOKIE: 2a7e7604289e3b74

Responder COOKIE: 37176d3ed068b5a7

Local IP/port: 175.25.49.88/500

Local ID type: IPV4_ADDR

Local ID: 175.25.49.88

Remote IP/port: 175.25.49.89/500

Remote ID type: IPV4_ADDR

Remote ID: 175.25.49.89

Authentication-method: PRE-SHARED-KEY

Authentication-algorithm: SHA1

Encryption-algorithm: 3DES-CBC

Life duration(sec): 86400

Remaining key duration(sec): 78266

Exchange-mode: Main

Diffie-Hellman group: Group 2

NAT traversal: Not detected

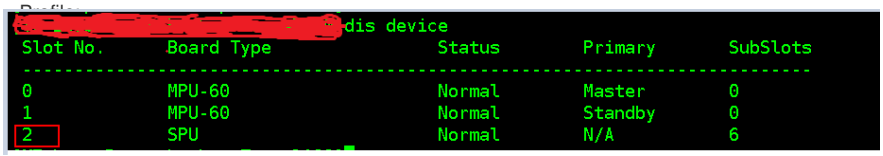
Extend authentication: Disabled

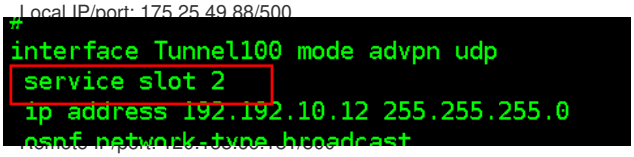
Assigned IP address:

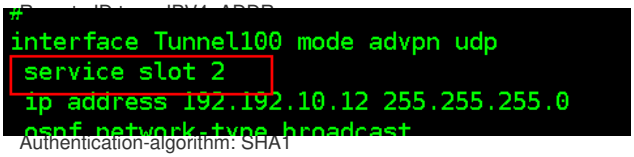
Vendor ID index:0x722

解决方法

在tunnel口下加了一个service slot 2







原因： msr多槽位的设备的逻辑接口处理会话报文时需要加上service slot命令指定一下接口， 不指定槽位的时候可能会有全局接口把会话报文被分开处理，然后时序问题或者报文匹配不上会话

注意事项： tunnel，route-aggregation 等全局性的接口如果涉及会话流量在非堆叠场景下都推荐配置service slot 命令

```
  Vendor ID sequence number:0x0
=============================================================
  ===============display ike proposal===============
 Priority Authentication Authentication Encryption  Diffie-Hellman Duration
             method       algorithm    algorithm       group      (seconds)
-------------------------------------------------------------------------------
```