



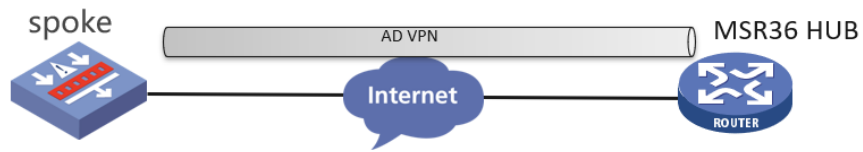
MSR ADVPN无法建立

ADVPN

郭尧

2023-10-31 发表

组网及说明



HUB和server是一台MSR36设备，spoke是一台设备（防火墙F1000-AK135）server连接运营商专线和HUB建立ADVPN。

问题描述

1. ADVPN隧道无法建立，HUB和spoke设备也没有注册上
2. 看不到VAM Client的IPv4私网地址映射信息

过程分析

1、首先检查两边设备配置，ADVPN实际上也是建立IPsec VPN隧道，检查发现配置中存在问题

(1) spoke中下面的地址

```
interface Tunnel1 mode advpn gre
```

```
ip address 172.32.254.9 255.255.255.0
```

检查发现这个地址不在server设备上Hub组内Spoke的IPv4私网地址范围，正常是要在这个范围内

server中的配置

```
vam server advpn-domain mem id 1
```

```
pre-shared-key cipher $c$3$qtHxMApstPa0BpKt51BUDS5B+tFoSg==
```

```
server enable hub-group 0
```

```
hub private-address 172.32.254.10
```

```
spoke private-address range 172.31.254.0 172.35.254.255
```

(2) HUB设备上IPv4 ADVPN隧道接口Tunnel1配置错误

```
interface Tunnel1 mode advpn gre
```

```
ip address 172.32.254.10 255.255.255.0
```

//要和server中Hub组内的Hub IPv4私网地址一致

```
ospf network-type broadcast
```

```
source GigabitEthernet1/4/3
```

```
tunnel protection ipsec profile dvpn
```

```
vam client mem
```

(3) 终端不结合服务器，在设备本地认证，这个需要HUB的用户名和SPOKE不能配置成一样的。do main域按照下面配置即可，如果是结合AAA服务器认证，就严格按照官网配置。

```
domain mem
```

```
authentication advpn local none
```

```
accounting advpn local none
```

(4) OSPF中发布的配置要包含私网地址信息

```
ospf 2
```

```
area 0.0.0.0
```

```
network 172.32.254.0 0.0.0.255
```

解决方法

1、按照如上检查修改配置后，HUB和SPOKE可以正常注册上线，也可以看到私网地址信息，隧道也可以正常建立。

```
[SERVER] display vam server address-map
ADVPN domain name: mem
Total private address mappings: 2
Group   Private address Public address      Type NAT Holding time
0       172.32.254.9    124.126.16.130    Spoke No  0H 14M 7S
0       172.32.254.10   124.65.137.178    Hub  No  0H 15M 22S

[SERVER]ping 172.32.254.9  （在server上ping spoke设备地址）
Ping 172.32.254.9 (172.32.254.9): 56 data bytes, press CTRL+C to break
56 bytes from 172.32.254.9: icmp_seq=0 ttl=255 time=4.575 ms
56 bytes from 172.32.254.9: icmp_seq=1 ttl=255 time=4.435 ms
56 bytes from 172.32.254.9: icmp_seq=2 ttl=255 time=4.343 ms
56 bytes from 172.32.254.9: icmp_seq=3 ttl=255 time=4.269 ms
56 bytes from 172.32.254.9: icmp_seq=4 ttl=255 time=4.288 ms
--- Ping statistics for 172.32.254.9 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 4.269/4.382/4.575/0.112 ms

[SERVER]dis ipsec sa
-----
Interface: Tunnel1
-----

IPsec profile: dvpn
Mode: ISAKMP
-----

Tunnel id: 0
Encapsulation mode: transport
Perfect forward secrecy:
Path MTU: 1404
Tunnel:
    local address: 124.65.137.178
    remote address: 124.126.16.130

Flow:
    sour addr: 124.65.137.178/255.255.255.255 port: 0 protocol: gre
    dest addr: 124.126.16.130/255.255.255.255 port: 0 protocol: gre

[Inbound ESP SAs]
SPI: 2965272858 (0xb0be791a)
Connection ID: 4294967296
Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-SHA1
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843187/2244
Max received sequence-number: 160
Anti-replay check enable: Y
Anti-replay window size: 64
UDP encapsulation used for NAT traversal: N
Status: Active

[Outbound ESP SAs]
SPI: 3922642703 (0xe9cec70f)
Connection ID: 4294967297
Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-SHA1
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843186/2244
Max sent sequence-number: 159
UDP encapsulation used for NAT traversal: N
Status: Active

[SERVER]dis ike sa
Connection-ID Local Remote Flag DOI
-----
9 124.65.137.178 124.126.16.130 RD IPsec
```

