v7对接v5设备 ipsec vpn建立不起来

IPSec VPN　陈泽勇　2022-11-30 发表

问题描述

渠道和对端v5路由器设备做ipsec vpn隧道建立，第一阶段都起来了 第二阶段起不来。本端msr3620 v7设备是固定端，对端是拨号端。使用野蛮模式与对端建立隧道但是建立不起来。

过程分析

1、查看debug信息debug ipsec sa all，可以看到如下的报错信息；即ipsec安全策略里面使用的ike profile与匹配上的不一样进一步查看报错信息

此时隧道建立失败提示的是匹配上了不正确的acl或者ike profile导致问题出现。于是进一步查看诊断信息里的配置。

2、查看配置信息可以看到：

v7端：

```
# ike keychain xa962
    pre-shared-key hostname xa962 key cipher
$c$3$rl4T4/dHFUnrfdPz0ZL6WUlDwEQFhaHnNDTJAxA7ug==
#
 ike identity fqdn yc467
#
 ipsec transform-set 1
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
 #
ike profile xa962
  keychain xa962
 dpd interval 10 periodic
 local-identity fqdn yc467
 match remote identity address 124.65.35.6 255.255.255.255
 proposal 1
#
ipsec policy bj961 3 isakmp
 transform-set bj961
 security acl 3100
 ike-profile xa962
 sa duration time-based 3600
#
```

V5端：

```
#
 ike local-name xa962
#
#
ipsec policy pol 3096 isakmp
 security acl 3096
 ike-peer yc467
 proposal pro
#
#
ike peer yc467
 exchange-mode aggressive
 pre-shared-key simple parksonblock
 id-type name
 remote-name yc467
 remote-address 223.84.
 dpd 1
```

2、感兴趣流都是互为镜像没有差别。

3、因为v7端为固定端，v5端为不固定地址端。所以渠道的v7端的配置，ipsec安全策略的认证方式不应该选择为isakmp直接方式，因为对端是不固定地址。v5端配置查看没有发现问题，现在就是怀疑是v7端的配置问题。尝试将isakmp直接方式改为template模板方式去认证之后问题解决。

解决方法

不固定端ipsec策略使用isakmp直接模式，固定地址端ipsec策略使用template模板模式进行认证。