MER8300 web界面配置多WAN口负载后IPsec不通

IPSec VPN　黄聪琴　2024-01-25 发表

组网及说明

问题描述

总部MER8300下接192.168.0.0网段，通过GE0/0经过公网对接IPsec对端MER5200下接10.2.0.0网段。

MER8300：183.6.3.62、MER5200：219.137.64.124，测试IP：192.168.0.223-10.2.7.1和192.168.0.223-10.2.7.2。

总部设备MER8300通过模板与分部MER5200建立IPsec：

```
#
ipsec policy-template WAN0(GE0) 900
 transform-set WAN0(GE0)@gz_branches_cd
 local-address 183.6.3.62
 remote-address 117.174.122.163
 description WAN0(GE0)@gz_branches_cd
 ike-profile WAN0(GE0)@gz_branches_cd
 sa duration time-based 3600
 sa duration traffic-based 1843200
 reverse-route dynamic
 reverse-route preference 50
#
```

现场在web界面上配置了多WAN出口负载，配置前可以正常建立IPsec且双方通信正常，配置后IPsec可以正常建立但本部侧ping分部侧不通，分部侧ping本部侧正常。

过程分析

本部侧ping分部目的IP为10.1.0.0/16网段，匹配到路由表中由反向路由注入生成的路由：

```
10.1.0.0/16       Static  50  0           117.174.122.163 Dia3
```

但IPsec对端地址219.137.64.124的路由没有明细出口路由可查，只能通过静态缺省路由进行迭代：

```
0.0.0.0/0     Static  60  0           0.0.0.0         Dia3
              Static  60  0           0.0.0.0         Dia1
              Static  60  0           183.6.3.61      GE0/0
              Static  60  0           183.6.184.161   GE0/4
```

迭代效果的结果就是下发到FIB表时，IPSEC私网的路由还是4个出口hash负载。

```
10.1.0.0/16       117.174.122.163 USR     Dia3                Null
10.1.0.0/16       117.174.122.163 USR     Dia1                Null
10.1.0.0/16       183.6.3.61      USGR    GE0/0               Null
10.1.0.0/16       183.6.184.161   USGR    GE0/4               Null
10.2.0.0/16       219.137.64.124  USR     Dia3                Null
10.2.0.0/16       219.137.64.124  USR     Dia1                Null
10.2.0.0/16       183.6.3.61      USGR    GE0/0               Null
10.2.0.0/16       183.6.184.161   USGR    GE0/4               Null
```

解决方法

要解决这个问题，需要明确指定IPSEC对端地址的路由出口。

增加两条单独的静态：

10.2.0.0/16 指向G0/0 接口，优先级50；

219.137.64.124/32 指向G0/0接口，优先级50；

如果MER5200的地址可能重播发生变化，那就需要将MER5200拨号可能获取的网段配置路由指向给0/0。