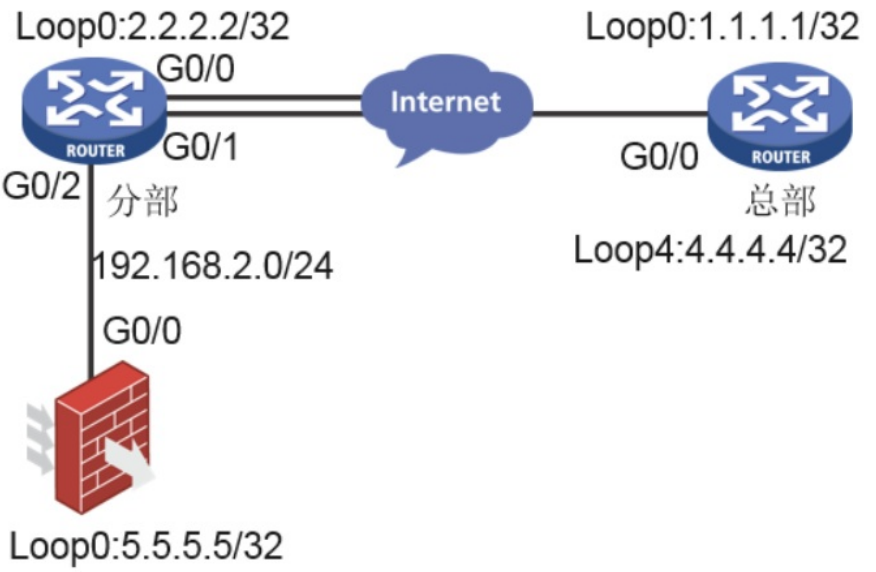
MSR双出口ipsec一个出口正常建立，另一个出口无法建立隧道

IPSec VPN　郭尧　2023-06-25 发表

组网及说明



分部MSR3620路由器的两个出口和总部路由器的一个出口建立两条隧道，让不同网段的流量走不同的出口到达总部路由器上。实现业务流量的保护以及负载分担。

问题描述

分部不同网段的流量通过策略路由的方式指向分部的不同出口，现场配置完后使用LOOPBACK口测试，2.2.2.2访问1.1.1.1走出口G0/0，5.5.5.5访问4.4.4.4走出口G0/1，发现G0/0口的隧道可以建立成功，但是G0/1口的隧道建立失败，看不到两边协商的第一阶段的SA。

过程分析

1、检查现场配置发现分部侧的IKE keychain配置存在交集，当系统配置了多个IKE keychain时，IKE keychain中pre-shared-key address配置地址范围不能有交集，不然会导致IKE keychain调用出现冲突，密码一样配置一条即可。另外现场总部侧采用了IPsec模板的方式，IPsec安全策略模板与直接配置的IKE协商方式的IPsec安全策略中可配置的参数类似，但是配置较为简单，除了IPsec安全提议和IKE profile之外的其它参数均为可选。应用了引用IPsec安全策略模板配置的IPsec安全策略的接口不能发起协商，仅可以响应远端设备的协商请求。而现场想两边都发起访问，那么需要通过直接配置多条序列号不同的IPsec策略的方式实现。

分部侧ike keychain配置

```
ike keychain 1
pre-shared-key address 117.131.119.27 255.255.255.255 key cipher
$c$3$+vPJnEQ1hfxTSC0iPNtEffSxpfIN/fO1mB/E2g==
#
ike keychain 2
pre-shared-key address 117.131.119.27 255.255.255.255 key cipher $c$3$eLziRcqbbX0TjpaQZBBe
VGTkrtQ+Z3wsmEDYug==
```

总部侧ipsec模板配置

```
ipsec policy aaa 1 isakmp template R1-ip-IP1
#
ipsec policy-template R1-ip-IP1 1          ##R1-IP1
 transform-set R1-IPA
 security acl 3200
 local-address 117.131.119.27
 remote-address 103.98.220.118
 ike-profile 1
#
ipsec policy-template R1-ip-IP1 3             ##R1-IP2
 transform-set R1-IPA
 security acl 3202
 local-address 117.131.119.27
 remote-address 140.207.81.252
 ike-profile 3
```

2、现场更改配置后发现G0/1口的隧道第一阶段的IKE SA可以正常建立，但是第二阶段的IPSEC SA建立失败。收集第二阶段的debug信息提示ACL或者IKE profile无法匹配上，该报错说明两边的ACL或者IKE profile调用有问题。检查两边配置发现两边的ACL配置是镜像的，但是IKE profile配置了两条，且指向了同一个remote identity address。IKE协商第一阶段中，IKE profile和IKE keychain均是在全局下匹配的，需要保证IKE协商第二阶段中找到的IPsec policy中引用的IKE profile和第一阶段匹配的IKE profile是一致的。ike profile中match remote identity address配置地址范围不能有交集，不然会导致第一阶段和第二阶段找到的IKE profile不一致。

Debug信息：

```
*Nov 25 15:48:10:861 2020 R1 IKE/7/EVENT: vrf = 0, local = 140.207.81.252, remote = 117.131.119.
27/500
IPsec SA state changed from IKE_P2_STATE_INIT to IKE_P2_STATE_GETSP.
*Nov 25 15:48:10:862 2020 R1 IPSEC/7/EVENT:
The policy's acl or ike profile does not match the flow, Name = R1-IP2, Seqnum = 1
```

IKE profile的配置：

```
ike profile 1
keychain 1
local-identity address 103.98.220.118
match remote identity address 117.131.119.27 255.255.255.255
proposal 1
#
ike profile 2
 keychain 1
local-identity address 140.207.81.252
match remote identity address 117.131.119.27 255.255.255.255
proposal 1
```

解决方法

由于总部侧只有一个IP地址，分部侧有两个出口，采用IP地址作为身份标识的方式就会造成远端地址相同，所以改为FQDN的形式，改成FQDN后由于RT3侧有两个身份标识都为FQDN的IKE profile，如果由RT1侧发起访问建立第二条隧道会匹配IKE profile1导致隧道建立失败，需要由RT3侧发起访问。

分部修改成如下:

```
ipsec policy aaa 1 isakmp
transform-set 1
security acl 3500
local-address 103.98.220.118
remote-address 117.131.119.27
ike-profile 1
#
ipsec policy R1-IP2 1 isakmp
transform-set 1
security acl 3501
local-address 140.207.81.252
remote-address 117.131.119.27
ike-profile 1
#
l2tp-group 1 mode lns
allow l2tp virtual-template 1
undo tunnel authentication
#
l2tp enable
#
ike profile 1
keychain 1
local-identity fqdn www
match remote identity address 117.131.119.27 255.255.255.255
proposal 1
```

总部侧修改如下：

```
ike profile 1
keychain 1
local-identity address 117.131.119.27
match remote identity address 103.98.220.118 255.255.255.255
match remote identity fqdn www
proposal 1

ike profile 3
keychain 3
local-identity address 117.131.119.27
match remote identity address 140.207.81.252 255.255.255.255
match remote identity fqdn www
proposal 1
```

注意事项：

1、当系统配置了多个ike keychain时，ike keychain中pre-shared-key address配置地址范围不能有交集。

2、当系统配置了多个ike profile时，ike profile中match remote identity address配置地址范围不能有交集。