防火墙GRE over ipsec不定时中断

IPSec VPN GRE VPN 吴昊A 2020-01-11 发表

组网及说明

不涉及

问题描述

隧道不定时中断，重新reset ike sa后恢复

分部配置:

```
 session statistics enable
#
 ipsec logging negotiation enable
#
ipsec transform-set to-hy
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
ipsec policy to-hy 10 isakmp
 transform-set to-hy
 security acl 3888
 local-address 218.76.174.50
 remote-address 59.51.68.68
 ike-profile to-hy
#
 ike identity fqdn zzzy
 ike logging negotiation enable
#
ike profile 1
#
ike profile to-hy
 keychain to-hy
 match remote identity address 59.51.68.68 255.255.255.255
 proposal 1
#
ike proposal 1
 encryption-algorithm 3des-cbc
 authentication-algorithm md5
#
ike keychain to-hy
 pre-shared-key address 59.51.68.68 255.255.255.255 key cipher $c$3$jnmibet3qrJ9dnNwV
RAwOwfBqxFqxwnP8UgU7uus
#
#
 ntp-service enable
 ntp-service unicast-server 10.33.28.11 source Tunnel1
#
```

总部配置:

```

 ipsec logging negotiation enable
#
ipsec transform-set to-zz
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
ipsec policy to-zz 10 isakmp
 transform-set to-zz
 security acl 3010
 remote-address 218.76.174.50
 ike-profile to-zz
#
 ike identity fqdn hyzy
 ike logging negotiation enable
```

```
#
ike profile to-zz
 keychain to-zz
 match remote identity address 218.76.174.50 255.255.255.255
 proposal 1
#
ike proposal 1
 encryption-algorithm 3des-cbc
 authentication-algorithm md5
#
ike keychain to-zz
 pre-shared-key address 218.76.174.50 255.255.255.255 key cipher $c$3$LZKIFmPlmQ3o17/TPIuvHNkZD/63+IfGRNyamnKY
#
```

过程分析

现场分部1030配置了ntp并且源接口为tunnel1口，这样的话就算没有流量触发，也会去发起协商，由于配置问题正常情况下会协商不起来，会报找不到ike profile，但是一阶段ike sa是d的状态，如果这时候总部1080发起流量，会直接引用一阶段的ike sa，直接进行二阶段协商，这时候就协商起来了。

解决方法

总部的ike profile to-zz下添加local-identity address 59.51.68.68

分部的ike profile to-hy下添加local-identity address 218.76.174.50

附件下载： diag_HYZY-F1030-01_20191223-095204.tar.gz
diag_ZZYS-HXJF-F1080-14_20191223-094835.tar.gz