某局点MSR5660 IPsec VPN无法建立处理经验案例

IPSec VPN 孙轶宁 2018-10-21 发表

组网及说明

总部为MSR5660，分部为F1030，采用主模式建立IPsec VPN。

问题描述

IKE SA无法正常建立

dis ike sa

```
  Connection-ID   Remote              Flag            DOI
-------------------------------------------------------------------------
  819             XXX.XXX.XXX.XXX   Unknown         IPsec
```

两边keychain、proposal和profile配置一致

分部配置

```
ike profile XX
 keychain XX
 local-identity address XXX.XXX.XXX.XXX
 match remote identity address XXX.XXX.XXX.XXX 255.255.255.255
 proposal 116
#
ike proposal 116
 encryption-algorithm 3des-cbc
#
ike keychain XX
 pre-shared-key address XXX.XXX.XXX.XXX 255.255.255.255 key cipher XXXXX
```

总部配置

```
ike profile XX
 keychain XX
 local-identity address XXX.XXX.XXX.XXX
 match remote identity address XXX.XXX.XXX.XXX 255.255.255.255
 proposal 116
#
ike proposal 116
 encryption-algorithm 3des-cbc
#
ike keychain XX
 pre-shared-key address XXX.XXX.XXX.XXX 255.255.255.255 key cipher XXXXX
```

过程分析

1、首先检查两边的配置，并没有发现问题。

2、收集debug信息，发现有如下报错

*Oct 12 09:26:41:494 2018 XX IKE/7/EVENT: -COntext=1; vrf = 0, local = XXX.XXX.XXX.XXX, remote = XXX.XXX.XXX.XXX/500

Notification PAYLOAD_MALFORMED is received.

3、仔细观察总部的所有配置，发现有两个加密算法一模一样的proposal

```
ike proposal 1
 encryption-algorithm 3des-cbc
#
ike proposal 116
 encryption-algorithm 3des-cbc
```

总部收到分部发起的协商报文时，查看协商报文的SA，会在本地全局配置中自上而下的寻找能够匹配到该SA的proposal（**并不一定是ike profile内调用的**），如果存在两个proposal内容一致，分别叫做1，116，但是ike profile内调用的116，实际在响应协商报文时设备会认为ike profile匹配的是proposal 1。在第5、6个报文时需要对报文进行解密，**此时会使用proposal 1进行解密，但是设备会发现ike profile内并没有配置proposal 1**，从而报错 。

4、去掉proposal 1之后，发现两边IKE SA协商成功，IPsec正常建立。

解决方法

去掉重复ike proposal的配置，确保每个ike proposal内容不一样。