l2tp over ipsec 拨号失败 显示用户名或密码不正确

L2TP VPN IPSec VPN 雨下整夜 2024-05-12 发表

组网及说明

F1020---ISP---家用路由器---pc

告警信息

关键配置

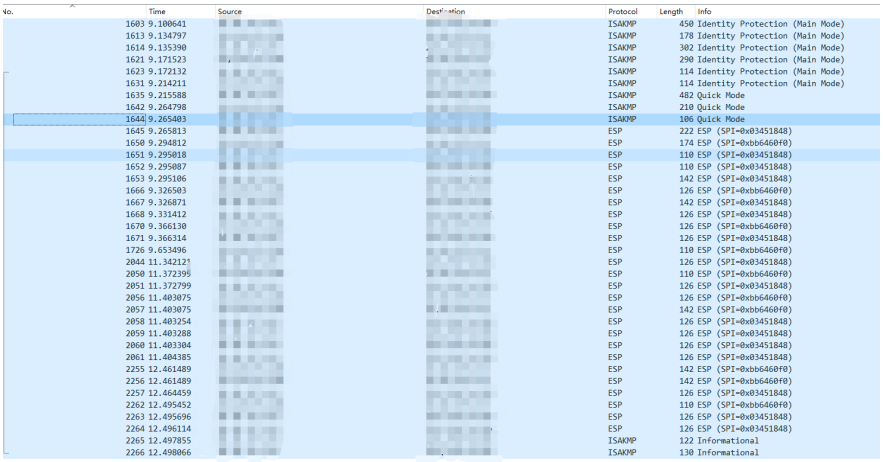
```
#
 ip pool aa 10.6.0.100 10.6.0.200
 ip pool aa gateway 10.6.0.1
#
interface Virtual-Template1
 ppp authentication-mode chap domain system
 ppp ipcp dns x.x.x.x
 remote address pool aa
 ip address 10.6.0.1  255.255.255.0
 dns server x.x.x.x
#
interface GigabitEthernet1/0/1
 port link-mode route
 description LINK-to-Internet
 ip address x.x.x.x 255.255.255.240
 ipsec apply policy GE1/0/1   // ipsec 为传输模式 不过多赘述配置
#
domain system
  authentication ppp radius-scheme aa
 authorization ppp radius-scheme aa
 accounting ppp radius-scheme aa
#
l2tp-group 1 mode lns
 allow l2tp virtual-template 1
 undo tunnel authentication
 tunnel name LNS
#
```

问题描述

用inode 和 pc自带的拨号软件拨号都失败了

过程分析

pc端拨号的同时抓网卡报文，发现ipsec正常建立了，但经过几个esp报文后，交互了informational信息，隧道中断。



No.	Time	Source	Destination	Protocol	Length	Info
1603	9.100641			ISAKMP	450	Identity Protection (Main Mode)
1613	9.134797			ISAKMP	178	Identity Protection (Main Mode)
1614	9.135390			ISAKMP	302	Identity Protection (Main Mode)
1621	9.171523			ISAKMP	290	Identity Protection (Main Mode)
1623	9.172132			ISAKMP	114	Identity Protection (Main Mode)
1631	9.214211			ISAKMP	114	Identity Protection (Main Mode)
1635	9.215588			ISAKMP	482	Quick Mode
1642	9.264798			ISAKMP	210	Quick Mode
1644	9.265403			ISAKMP	106	Quick Mode
1645	9.265813			ESP	222	ESP (SPI=0x03451848)
1650	9.294812			ESP	174	ESP (SPI=0xbb6460f0)
1651	9.295018			ESP	110	ESP (SPI=0x03451848)
1652	9.295087			ESP	110	ESP (SPI=0x03451848)
1653	9.295106			ESP	142	ESP (SPI=0x03451848)
1666	9.326503			ESP	126	ESP (SPI=0xbb6460f0)
1667	9.326871			ESP	142	ESP (SPI=0x03451848)
1668	9.331412			ESP	126	ESP (SPI=0x03451848)
1670	9.366130			ESP	126	ESP (SPI=0xbb6460f0)
1671	9.366314			ESP	126	ESP (SPI=0x03451848)
1726	9.653496			ESP	110	ESP (SPI=0xbb6460f0)
2044	11.342121			ESP	126	ESP (SPI=0x03451848)
2050	11.372395			ESP	110	ESP (SPI=0xbb6460f0)
2051	11.372799			ESP	126	ESP (SPI=0x03451848)
2056	11.403075			ESP	126	ESP (SPI=0xbb6460f0)
2057	11.403075			ESP	142	ESP (SPI=0xbb6460f0)
2058	11.403254			ESP	126	ESP (SPI=0x03451848)
2059	11.403288			ESP	126	ESP (SPI=0x03451848)
2060	11.403304			ESP	126	ESP (SPI=0x03451848)
2061	11.404385			ESP	126	ESP (SPI=0x03451848)
2255	12.461489			ESP	142	ESP (SPI=0xbb6460f0)
2256	12.461489			ESP	142	ESP (SPI=0xbb6460f0)
2257	12.464459			ESP	126	ESP (SPI=0x03451848)
2262	12.495452			ESP	110	ESP (SPI=0xbb6460f0)
2263	12.495696			ESP	126	ESP (SPI=0x03451848)
2264	12.496114			ESP	126	ESP (SPI=0x03451848)
2265	12.497855			ISAKMP	122	Informational
2266	12.498066			ISAKMP	130	Informational

这几个esp报文其实是被保护的l2tp协商报文，看抓包怀疑是终端l2tp拨号失败，主动把ipsec隧道删除，需要继续排查l2tp协商失败的原因。
报错显示用户名和密码失败，所以在设备上重新创建了一个ppp用户用于测试，还是拨号失败，报错依旧。
发现客户设备中有1个月前的诊断信息
对比配置后，发现客户的1个月前的配置中
ppp用户的认证方式为本地认证
而现在ppp用户的认证域的认证方式是结合了radius的

```
interface Virtual-Template1
 ppp authentication-mode chap domain system
#
domain system
 authentication ppp radius-scheme aa
 authorization ppp radius-scheme aa
 accounting ppp radius-scheme aa

#
```

随后将该domain中的认证方式改成local测试，拨号成功。

解决方法

配置ppp用户认证方式为local

```
interface Virtual-Template1
 ppp authentication-mode chap domain system
#
domain system
 authentication ppp local
 authorization ppp local
 accounting ppp local
```

处理故障问题的时候有条件可以先对配置。