某局点MSR 3610 无法建立IPSec

IPSec VPN　陈阳　2021-07-30 发表

组网及说明

两台MSR 3610跨公网以主模式建立IPSec

问题描述

隧道无法建立，查看ike sa是未知状态

<H3C>display ike sa

Connection-ID	Local	Remote	Flag	DOI
482	222.222.4.103	218.12.25.226	Unknow	IPSec

过程分析

IPSec无法建立，首先检查两端配置，确保加密和认证算法相同，本端和对端地址正确，感兴趣对称。检查配置后发现都正确，没有发现问题。
然后收集debug ike sa和debug ipsec sa进行分析。
本端：
*Jul 16 12:23:41:198 2021 H3C IKE/7/EVENT: vrf = 0, local = 222.222.4.103, remote = 218.12.25.226/500 Retransmission of phase 1 packet timed out.
*Jul 16 12:23:41:198 2021 H3C IKE/7/ERROR: vrf = 0, local = 222.222.4.103, remote = 218.12.25.226/500 Failed to negotiate IKE SA.

对端：
*Jul 16 12:24:38:954 2021 H3C IKE/7/EVENT: vrf = 0, local = 218.12.25.226, remote = 222.222.4.103/500 Retransmission of phase 1 packet timed out.
*Jul 16 12:24:38:954 2021 H3C IKE/7/ERROR: vrf = 0, local = 218.12.25.226, remote = 222.222.4.103/500 Failed to negotiate IKE SA.

从两边的debug可以看到都是相同的报错，重传超时，并没有提示参数上的问题，且500端口也是放通的。
为了进一步确认配置，在本地实测，两台路由器设备直连，将现场两端设备相关配置导入，发现能够正常建立隧道，说明配置正确，没有问题。

后续向现场了解到，一端的设备出口走的移动，另一端的设备出口走的联通。结合本地测试结果，怀疑是两端跨了运营商导致报文传输被丢弃。
于是建议现场修改一台设备的配置，走相同运营商接口，修改接口配置后，隧道能正常建立起来，证明确实是跨运营商导致报文被丢弃。

解决方法

修改两端走同一运营商链路。