MSR2600-6-X1分支对接总部SR66 ipsec建立不成功

IPSec VPN　zhiliao_vKoUlt　2023-01-18 发表

问题描述

5期Adwan分支方案，VXLAN over IPSEC，路由器的IPSEC配置由控制器下发。总部、分支对接的ipsec建立失败。

过程分析

配置看没什么问题。

看debug信息，已经在重传第2阶段，隧道建不起来的原因是sa冲突。

*Nov 22 15:14:23:974 2022 JJY-RT-0536-0318-01 IKE/7/EVENT: vrf = 0, local = 192.168.1.2, remote = 60.217.64.253/500
Collision of phase 2 negotiation is found when acquired sa.

查看设备IPSEC SA及IKE SA，发现SA数量异常。该组网环境IPSEC SA正常应为IKE SA的2至4倍，现网总部设备IPSEC SA的数量22944条，IKE SA数量1864条，IPSEC SA约为IKE SA的12倍。该现象与某已知软件问题相符。正常情况下，IPSEC SA因超期等原因需要重新协商时，会存在新旧两个SA，旧SA（RD|RL状态）删除后，新SA（RD状态）接替旧SA指导业务转发。在现网版本下，穿越NAT的IPSEC SA需要重新协商过程中软件处理异常，同一条IPSEC感兴趣流触发多条IPSEC SA协商，多条IPSEC SA之间判断存在冲突，导致协商失败。该问题非必现，多次IPSEC SA振荡过程中小概率触发，触发该问题后，IPSEC SA会持续累计，导致所有后续IPSEC SA协商失败。

解决方法

版本已知问题：

CMW710-R7821P14版本解决问题列表

202103301127 问题现象：ike进程反复异常退出，无法起来，并产生core 问题产生条件： ADWAN中心-分支组网，Internet穿NAT，建立IPsec隧道后，中心侧重启ike进程

建议升级总部SR6604设备版本至R8128P22解决该问题。