某局点 ADWAN组网下分支MSR tracert SR66不通但反向tracert测试正常

Tracert 林宇阳 2021-08-31 发表

组网及说明

分支设备：MSR3600-28-X1

总部设备：SR6608

组网：分支MSR36--公网--总部防火墙--SR66

组网说明：防火墙对SR66上的地址做了映射，ADWAN控制器给MSR和SR66下发ipsec、vxlan配置，ipsec打通设备loopback口，vxlan用loopback建立隧道 。

问题描述

故障现象：

客户计划部署链路探测功能时发现，从SR66 去 tracert MSR36正常，但是MSR36去tracert SR66 无回显，尝试过tracert SR66的loopback口地址和VSI接口地址都一样，且多个分支节点MSR测试存在相同情况。在tracert测试的同时，地址ping测试都能通且业务流量在vxlan隧道中运行无异常。

过程分析

实际业务流量正常说明SR66上流量转发没有问题，而tracert属于由报文TTL值控制的报文，当设备接收TTL=1时上送CPU处理，并回复ICMP不可达消息。

1、故障现象为MSR tracert SR66时不显示回包，为确认是否SR66侧没有给回应icmp差错报文，在SR66打开了debug ip packet acl xxx（ACL匹配loopback口地址），的确没有看到icmp差错报文的回包debug打印。说明tracert不回显的原因在于SR66确实没有发送ICMP差错报文。

2、在SR66打开debug ip icmp，发现设备有大量的icmp超限速报错，基本每0.001秒就弹一个：

*Jun 23 17:18:57:263 2021 XX SOCKET/7/ICMP: -MDC=1-Slot=3;

ICMP Discard:ICMP reached rate limit.

*Jun 23 17:18:57:264 2021 XX SOCKET/7/ICMP: -MDC=1-Slot=3;

ICMP Discard:ICMP reached rate limit.

3、ICMP超限速报错说明设备需要处理的ICMP差错报文已经超出当前处理能力，怀疑正是大量icmp差错报文造成超限速导致MSR tracert SR66无回显。尝试配置将差错令牌桶改成最大值ip icmp error-interval 10 200（缺省情况下为100 10）后，debug ip icmp还是以0.007s为间隔不断刷出超限速丢包。

4、与客户协商在非正式业务使用期间，关闭ICMP差错报文限速功能后debug ip icmp显示基本都是不可达类型的差错报文，且原因是acl过滤导致的。

type = 3, code = 13 (communication-filter-forbidden)

解决方法

确认原因：

检查配置，客户在SR66对接各分支MSR的VSI接口启用了packe-filter inbound过滤分支访问公网的报文，但在分支侧未做访问公网的出方向过滤，导致大量分支访问公网的报文在SR66被阻断，而SR66又开启了ip unreachables enable命令，此时会在SR66产生大量需要发送的icmp差错报文。

解决方案：

将ACL包过滤功能转移到分支MSR设备接口出方向进行，分担ICMP差错报文发送压力吗，修改配置后问题解决，双向tracert回显均正常。

总结：

filter-packet功能与ip unreachable enable同时配置，且有流量被包过滤命中时，设备会产生大量ICMP差错报文。这可能会影响其它需要ICMP差错报文处理功能的正常使用，现网部署时需要注意，请谨慎选择同时开启这两个功能。