某局点 S5560X-HI tracert跟踪路径异常

Tracert 许家豪 2022-03-09 发表

组网及说明

组网：不涉及

问题描述

问题描述:从本地测试终端10.242.17.41发起到远端服务器10.126.89.205的traceroute、ping和telnet。
设备接口配置包过滤后tracert跟踪不可达，ping和telnet正常，将包过滤取消后tracert跟踪正常

过程分析

接口配置

interface Ten-GigabitEthernet2/0/25.3000
description to-ZZmanCORE-BJDSoffice-1/0/25.3000
ip address 169.255.0.22 255.255.255.248
packet-filter 3888 inbound
 acl number 3888
description office-to-idc-security_filter_acl
rule 0 permit icmp //允许icmp报文通过
rule 10 permit ip destination 10.9.196.100 0.0.0.1
rule 10 comment zhuanzhuan_gitlab

配置包过滤前

```
不配置 packet-filter 3888 inbound
$ traceroute 10.126.89.205
traceroute to 10.126.89.205 (10.126.89.205), 64 hops max, 52 byte packets
1  10.242.16.1 (10.242.16.1)  4.500 ms  3.333 ms  3.163 ms                  //网关
2  169-255-0-22.pool.rocketnet.co.za (169.255.0.22)  4.522 ms  5.423 ms  3.808 ms          //5560X-HI 设备
3  10.10.11.194 (10.10.11.194)  3.954 ms  3.792 ms  3.730 ms
4  * * *
5  169.254.0.5 (169.254.0.5)  4.965 ms  4.419 ms  5.344 ms
6  10.200.44.17 (10.200.44.17)  7.869 ms
   10.200.28.45 (10.200.28.45)  8.200 ms
   10.200.44.17 (10.200.44.17)  7.137 ms
7  10.200.19.114 (10.200.19.114)  7.290 ms  8.086 ms
   10.200.43.165 (10.200.43.165)  7.716 ms
8  10.200.18.226 (10.200.18.226)  7.709 ms
   10.200.18.214 (10.200.18.214)  7.201 ms
   10.200.18.218 (10.200.18.218)  6.580 ms
9  10.200.30.169 (10.200.30.169)  5.980 ms
   10.200.30.177 (10.200.30.177)  8.029 ms  6.730 ms
10  169.254.78.182 (169.254.78.182)  7.710 ms  7.538 ms  7.105 ms
11  10.51.255.1 (10.51.255.1)  7.059 ms  7.403 ms  15.020 ms
12  100.126.225.178 (100.126.225.178)  8.920 ms
   100.126.225.170 (100.126.225.170)  9.035 ms
   100.126.225.182 (100.126.225.182)  7.302 ms
13  10.126.242.79 (10.126.242.79)  6.534 ms
   10.126.240.79 (10.126.240.79)  8.874 ms
   10.126.244.79 (10.126.244.79)  9.473 ms
14  tjtx-89-205.58os.org (10.126.89.205)  6.715 ms  6.613 ms  6.529 ms                  //服务器
```

配置包过滤后

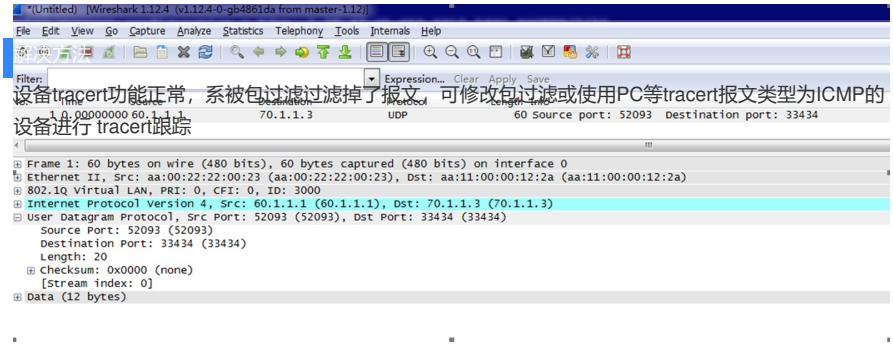
```
配置了 packet-filter 3888 inbound
traceroute to 10.126.89.205 (10.126.89.205), 64 hops max, 52 byte packets
1  10.242.16.1 (10.242.16.1)  24.716 ms  3.988 ms  3.784 ms
2  * * *                                                                  //5560X-HI 设备不显示了

...
```

这种情况只能抓包来看tracert的报文类型。

经抓包对比后得知，交换机tracert时，发出的报文类型是udp，并且udp的端口号是大于1024的，windows PC tracert 发出的报文类型是icmp，现场设备发出的报文类型是udp类型，被一条acl的rule 65050 deny udp destination-port gt 1024给deny掉了。

交换机发出的



设备tracert功能正常，系被包过滤过滤掉了报文，可修改包过滤或使用PC等tracert报文类型为ICMP的设备进行 tracert跟踪

PC发出的