网闸GAP-2000应用访问不通问题V1.0

网闸 孔凡安 2023-12-22 发表

组网及说明

网闸GAP-2000应用访问不通问题

组网简化为：

客户端---内端机（网闸）外端机---服务器

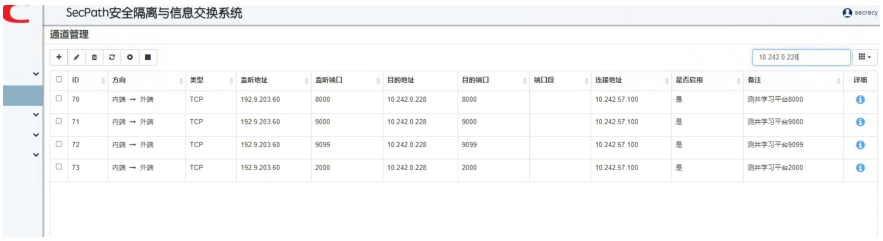
告警信息

不涉及

问题描述

现场配置了内端机到外端机的映射，类型为TCP通道，实际测试发现无法进行访问。

通道设置如下：



过程分析

针对ID 70的通道进行说明，排查手段如下：

对于正常的TCP业务，测试客户端到网闸内端机，以及网闸外端机到服务器的连通性即可。

(1) 客户端到网闸之间的网络连通性，可用从客户端telnet网闸通道端口来测试。如果telnet能通就没问题，如果telnet不到就说明网络有异常。需要找客户来进一步查明原因。检查链路上是否有其它安全产品拦截了，或者路由是否可达。

(2) 网闸到服务端之间的网络连通性，测试起来可能比较麻烦。由于网闸不带telnet客户端功能，所以只能让笔记本模拟成网闸IP，接到网络里telnet一下服务器。判断依据同上。

如果两边telnet都通的，那可能就是应用协议或配置上问题了。需要抓包具体分析了。

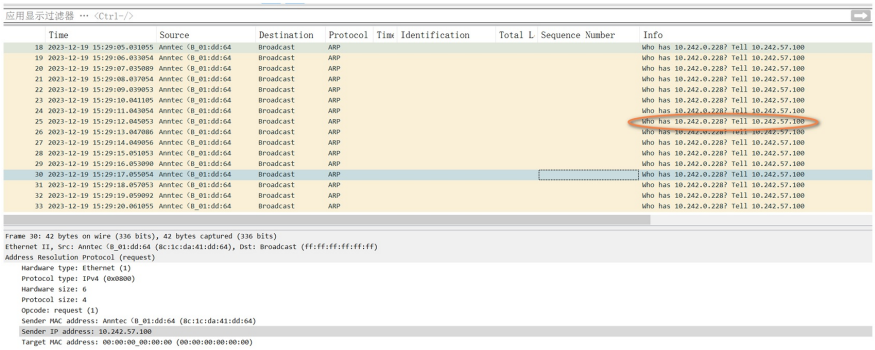
实际测试下来发现客户端到网闸内端机是通的，但是外端机ping服务器地址不通。

那么需要继续排查外端机侧网络不通问题，由于网闸不能在Web界面同时抓包和ping测试。因此可以登入网闸后台测试，Web界面抓包。

后台账户密码root/adminh3c，需要注意的是int标识为内端机，ext标识为外端机。在网闸内端机执行ssh 241.255.255.242/10.255.255.242(E6001P02及之前版本)即可进入外端机操作。需要注意网闸后台操作命令需要加ns，例如：

```
[root@ext ~]# ns ping 10.
ping: unknown host 10.
[root@ext ~]# ns ping 10.242.0.228
PING 10.242.0.228 (10.242.0.228) 56(84) bytes of data.
From 10.242.0.4 icmp_seq=1 Destination Host Unreachable
From 10.242.0.4 icmp_seq=2 Destination Host Unreachable
From 10.242.0.4 icmp_seq=3 Destination Host Unreachable
From 10.242.0.4 icmp_seq=4 Destination Host Unreachable
From 10.242.0.4 icmp_seq=5 Destination Host Unreachable
From 10.242.0.4 icmp_seq=6 Destination Host Unreachable
From 10.242.0.4 icmp_seq=7 Destination Host Unreachable
From 10.242.0.4 icmp_seq=8 Destination Host Unreachable
^C
```

抓包发现很奇怪的现象，网闸在请求目的地址10.242.0.228的arp信息。



这一点就很奇怪，连接地址为10.242.57.100/24，和目的地址（10.242.0.228）并非同一网段。在网闸后台查看路由，确实是直连路由。

```
242.155.0.0     0.0.0.0         255.255.0.0     U     0      0        0 br0
[root@ext ~]# ns route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         10.242.57.254   0.0.0.0         UG    0      0        0 slot0-4
10.33.96.0      0.0.0.0         255.255.255.0   U     0      0        0 slot0-4
10.242.0.0      0.0.0.0         255.255.255.0   U     0      0        0 slot0-4
10.242.57.0     0.0.0.0         255.255.255.0   U     0      0        0 slot0-4
192.9.203.0     0.0.0.0         255.255.255.0   U     0      0        0 slot0-4
241.255.255.208 241.255.255.225 255.255.255.240 UG    0      0        0 br0
241.255.255.224 0.0.0.0         255.255.255.240 U     0      0        0 br0
241.255.255.240 0.0.0.0         255.255.255.240 U     0      0        0 ctl
242.154.0.0     241.255.255.225 255.255.0.0     UG    0      0        0 br0
242.155.0.0     0.0.0.0         255.255.0.0     U     0      0        0 br0
[root@ext ~]# ns ping 10.242.57.254
PING 10.242.57.254 (10.242.57.254) 56(84) bytes of data.
64 bytes from 10.242.57.254: icmp_seq=1 ttl=254 time=0.826 ms
64 bytes from 10.242.57.254: icmp_seq=2 ttl=254 time=0.825 ms
64 bytes from 10.242.57.254: icmp_seq=3 ttl=254 time=0.858 ms
```

后续测试针对目的地址10.242.0.228添加主机路由到下一跳10.242.57.254之后业务正常。**此操作建议Web界面添加,不要后台操作。**

示例：

```
 6  10.242.0.228 (10.242.0.228)  32.659 ms !X  32.591 ms !X  32.528 ms !X
[root@ext ~]# ns route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         10.242.57.254   0.0.0.0         UG    0      0        0 slot0-4
10.33.96.0      0.0.0.0         255.255.255.0   U     0      0        0 slot0-4
10.242.0.0      0.0.0.0         255.255.255.0   U     0      0        0 slot0-4
10.242.0.228    10.242.57.254   255.255.255.255 UGH   0      0        0 slot0-4
10.242.57.0     0.0.0.0         255.255.255.0   U     0      0        0 slot0-4
192.9.203.0     0.0.0.0         255.255.255.0   U     0      0        0 slot0-4
241.255.255.208 241.255.255.225 255.255.255.240 UG    0      0        0 br0
241.255.255.224 0.0.0.0         255.255.255.240 U     0      0        0 br0
241.255.255.240 0.0.0.0         255.255.255.240 U     0      0        0 ctl
242.154.0.0     241.255.255.225 255.255.0.0     UG    0      0        0 br0
242.155.0.0     0.0.0.0         255.255.0.0     U     0      0        0 br0
[root@ext ~]#
```

解决方法

检查设备配置，slot4网卡配置了IP地址10.242.0.4。导致同一个网段内优先走二层转发。

因此针对网闸而言，网闸地址和目的地址存在多跳设备的场景下，不能配置同一网段。

☐	34	192.9.203.2	255.255.255.0
☐	35	192.9.203.41	255.255.255.0
☐	36	10.242.57.98	255.255.255.0
☐	38	192.9.203.43	255.255.255.0
☐	40	192.9.203.1	255.255.255.0
☐	41	10.242.57.97	255.255.255.0
☐	61	10.33.96.18	255.255.255.0
☐	67	10.242.0.4	255.255.255.0