SecPath ACG1000-PE acg突然业务不通

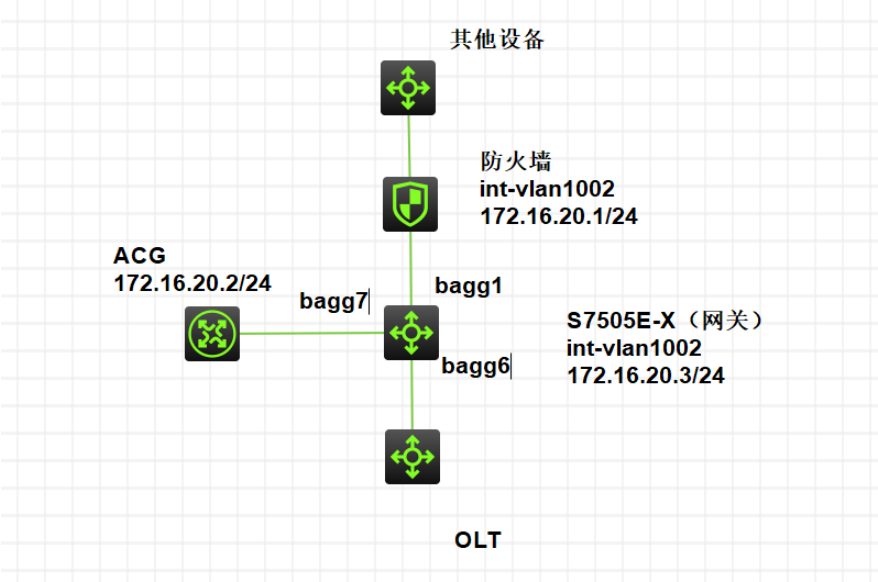
二层转发 转发不通 陈启敏 2021-05-30 发表

组网及说明

组网：如图，acg旁挂核心，从防火墙出去访问公网，olt下面为内网用户

户业务流向：用户（olt）--核心--ACG1000—核心----防火墙---公网 回来：公网-防火墙-核心-acg-核心-用户

：



问题描述

现场组网如上图所示。75E作为网关，旁挂ACG，上联FW。

业务流量走向为，终端访问外网时，报文从终端到了olt，然后到达网关75E设备，然后网关75E会通过缺省路由将报文通过bagg 7发给ACG设备，ACG设备上写了缺省路由，下一跳为FW上vlan 1002地址172.16.20.1，然后ACG将报文发给75E，由于目的mac是FW的地址，所以在75E上为二层转发，然后发给FW，FW再发给其他设备，出外网。

核心172.16.20.3 vlan1002 bag7（1/0/27,2/0/27）-------acg 172.16.20.2 agg0------核心 bag1（1/0/25,2/0/25）-----bag1(1/0/24,1/0/25) f1070 172.16.20.1---1/0/23 123.155.153.50出口

故障时：发现内网IP无法访问外网。

过程分析

1、通过核心S7506更改路由走向，跳过ACG，业务恢复正常

2、然后现场用OLT上同网段地址去ping 114.114.114.114发现，ping 5个包，在bagg 7上会有300多个包。

```
Interface: Ten-GigabitEthernet1/0/27
  Direction: Inbound
  Policy: ltj
   Classifier: ltj
     Operator: AND
     Rule(s) :
      If-match acl 3000
     Behavior: ltj
      Accounting enable:
        322 (Packets)
         0 (pps)

Interface: Ten-GigabitEthernet1/0/27
  Direction: Outbound
  Policy: ltj
   Classifier: ltj
     Operator: AND
     Rule(s) :
      If-match acl 3000
     Behavior: ltj
      Accounting enable:
        321 (Packets)
         0 (pps)
Interface: Ten-GigabitEthernet2/0/27
  Direction: Inbound
  Policy: ltj
   Classifier: ltj
     Operator: AND
     Rule(s) :
      If-match acl 3000
     Behavior: ltj
      Accounting enable:
        313 (Packets)
         0 (pps)

Interface: Ten-GigabitEthernet2/0/27
  Direction: Outbound
  Policy: ltj
   Classifier: ltj
     Operator: AND
     Rule(s) :
      If-match acl 3000
     Behavior: ltj
      Accounting enable:
        314 (Packets)
         0 (pps)
```

3、在acg上debug看有ttl=1丢弃的告警。

ACG 上的debug信息

<2021-05-17 00:34:30> Packet dropped 192.168.13.89:64630 -> 221.12.33.227:53 UDP len 64: ttl 1 is too small, send back icmp packet

<2021-05-17 00:34:30> Packet dropped 192.168.13.192:33469 -> 221.12.1.227:53 UDP len 64: ttl 1 is too small, send back icmp packet

<2021-05-17 00:34:30> Packet dropped 192.168.13.192:42695 -> 221.12.1.227:53 UDP len 64: ttl 1 is too small, send back icmp packet

<2021-05-17 00:34:30> Packet dropped 192.168.11.140:45177 -> 221.12.1.227:53 UDP len 68: ttl 1 is too small, send back icmp packet

<2021-05-17 00:34:30> Packet dropped 192.168.11.140:21384 -> 221.12.33.227:53 UDP len 68: ttl 1 is too small, send back icmp packet

<2021-05-17 00:34:30> Packet dropped 192.168.15.47:28565 -> 114.114.114.114:53 UDP len 60: ttl

1 is too small, send back icmp packet

<2021-05-17 00:34:30> Packet dropped 192.168.10.161:46070 -> 221.12.1.227:53 UDP len 61: ttl 1 i

s too small, send back icmp packet

<2021-05-17 00:34:30> Packet dropped 192.168.9.205:56466 -> 114.114.114.114:53 UDP len 62: tt

l 1 is too small, send back icmp packet

<2021-05-17 00:34:30> Packet dropped 192.168.14.8:52058 -> 180.76.76.76:53 UDP len 60: ttl 1 is t

oo small, send back icmp packet

<2021-05-17 00:34:30> Packet dropped 192.168.9.199:53436 -> 221.12.33.227:53 UDP len 62: ttl 1 is

too small, send back icmp packet

<2021-05-17 00:34:30> Packet dropped 192.168.9.199:53436 -> 221.12.33.227:53 UDP len 62: ttl 1 i

s too small, send back icmp packet

<2021-05-17 00:34:30> Packet dropped 192.168.14.8:37557 -> 221.12.33.227:53 UDP len 60: ttl 1 is

too small, send back icmp packet

定位报文在acg和核心之间来回互扔。

解决方法

通过查看交换机配置发现，现场int vlan1002下配置了本地arp代理，本地代理ARP的应用场景为：想要互通的主机连接到设备的同一个三层接口上，且这些主机不在同一个广播域中。

现场FW和ACG之间没有二层隔离，是在一个广播域下的，ACG请求FW上的下一跳地址的arp时，在可能会出现FW给ACG回复ARP response的情况，ACG收到后，应该会有一个学习的先后顺序，这时有可能会出现ACG学习的arp的目的mac为交换机的int vlan 1002的目的mac。这种情况下ACG发回给交换机的报文，目的mac则为交换机的目的mac，交换机此时会进行三层转发，而三层转发的路由表为默认路由，此时报文将从发回给ACG，而ACG又继续通过缺省路由把报文发回给交换机，从而出现路由环路，出现业务异常。

向现场确认，确实代理是最近才配置的。

现场删除int vlan 1002的arp代理，后故障未复现

建议现场修改不同网段互联acg、fw与交换机