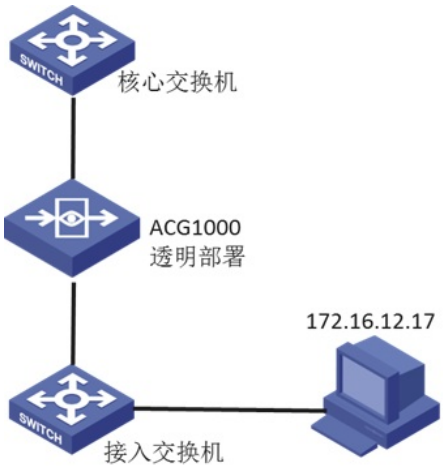
ACG1000透明部署打不开某一个网站

ACG1000 王奎银 2020-03-10 发表

组网及说明



ACG1000在网络中透明部署，版本6609P06。

问题描述

内网终端172.16.12.17访问某一个域名无法访问，其他都是正常，而且客户反馈之前是正常的，突然不行了，因为是透明部署，指导现场将ACG1000跳过就好，也尝试从公网侧去访问确实现场需要访问的域名是正常的。

过程分析

1.某个网页打不开，我们现场要确认该网站在公网环境中是否正常，排查这个网站本身故障的原因；
2.检查是否是域名解析失败；
3.如何有条件选择跳过设备进行测试，确实是否是设备影响的；
4.检查设备配置是否配置影响，是否有自定义URL阻断；
5.确定域名解析的地址，对终端访问域名进行抓包，有发出的报文没有回程报文，于是排查对端核心交换机是否正常收发该域名的ping报文；交换机流通显示收发正常，也就是说网站有回程报文从核心交换机发往ACG1000，但是ACG1000收不到回程报文；

No.	Time	Source	Destination	Protocol	Length	Info
101	1.172944	172.16.12.17	123.56.[redacted]	ICMP	78	Echo (ping) request
497	6.150745	172.16.12.17	123.56.[redacted]	ICMP	78	Echo (ping) request
894	11.151547	172.16.12.17	123.56.[redacted]	ICMP	78	Echo (ping) request
1333	16.150402	172.16.12.17	123.56.[redacted]	ICMP	78	Echo (ping) request

6.使用debug dp drop（这条命令非常常用）查看报文是否丢包在设备上；

```
H3C# display log debug 172.16.12.17
<2020-03-10 15:22:44> Packet dropped 172.16.12.17:57286 -> [redacted]49.11:443 TCP len 40: invalid flag  ACK  RST
<2020-03-10 15:22:44> Packet dropped 172.16.12.17:57286 -> [redacted]49.11:443 TCP len 40: new-check dropped
<2020-03-10 15:22:44> Packet dropped 172.16.12.17:57286 -> [redacted]49.11:443 TCP len 40: conntrack  init failed
<2020-03-10 15:22:53> Packet dropped 123.56.[redacted] -> 172.16.12.17 P 0 len 60: fw black list
<2020-03-10 15:22:54> Packet dropped 172.16.12.17:57287 -> [redacted]49.11:443 TCP len 40: invalid flag  ACK  RST
<2020-03-10 15:22:54> Packet dropped 172.16.12.17:57287 -> [redacted]49.11:443 TCP len 40: new-check dropped
<2020-03-10 15:22:54> Packet dropped 172.16.12.17:57287 -> [redacted]49.11:443 TCP len 40: conntrack  init failed
<2020-03-10 15:22:58> Packet dropped 123.56.[redacted] -> 172.16.12.17 P 0 len 60: fw black list
<2020-03-10 15:23:03> Packet dropped 123.56.[redacted] -> 172.16.12.17 P 0 len 60: fw black list
```

查看日志是黑名单丢弃报文。
再次检查设备配置：

现场确实将该地址加入黑名单

解决方法

将黑名单去掉后问题解决。
关于黑名单阻断业务报文的原理做一个说明：
现场抓包发现虽然配置了黑名单，但是还是有报文发送到网站的服务器，而且网站的服务器也给回包了。
经过确认黑名单的阻断原理是阻断IP地址的方式，所以是回程报文被黑名单丢弃。