某局点有线和无线不定时到外网不通经验案例

ACL 范书珩 2023-02-21 发表

组网及说明

组网情况：终端——AP——SW——AC——光猫——公网

告警信息

无

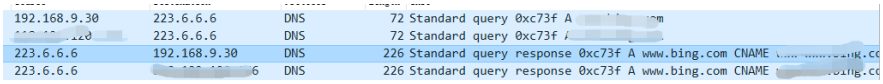
问题描述

无线终端和有线终端（直连AC）每天不定时出现能Ping通外网域名和dns但是打不开网页的情况，所有网页都出现过，故障一般持续一段时间后会自己恢复。故障复现时，电脑直连光猫打开网页正常，立刻接回AC就不正常。

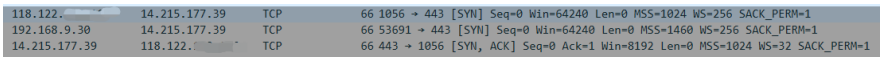
过程分析

终端偶发无法访问外网，且故障时间毫无规律性可言，初步检查AC的配置未发现异常，且故障出现的时候终端可以ping通外网域名，并且终端也能ping通dns，初步排除是链路不通的问题，怀疑是dns域名解析出现了问题，故在AC的出口和AC的下行口同时进行抓包分析。

如下为抓包的dns解析结果，192.168.9.30为故障终端的内网地址，223.6.6.6为dns地址，外网出口地址打码，从抓包中发现dns服务器是正常回复终端的域名解析请求，并且解析的ip地址没有任何问题。



排除了DNS域名解析的问题，那么继续查看抓包：



终端192.168.9.30向14.215.177.39公网ip发送了建立TCP链接握手报文，通过AC的公网ip的1056端口发送到 14.215.177.39的443端口，而14.215.177.39回复握手报文给AC的公网IP，目的端口为1056端口，但是没有后续第三次握手的交互，并且发现AC从公网口收到了TCP握手报文后没有将这个报文通过AC的下行口发送给192.168.9.30，因为抓包是没有抓到的，由此判断TCP三次握手的第二个报文被AC丢弃了导致后续交互出现问题。

找到了丢包位置，后续的工作就明确方向了，检查AC的配置发现AC的外网出口配置有包过滤策略：

interface GigabitEthernet1/0/7

packet-filter 3102 inbound

顺着包过滤策略应用的ACL继续排查，发现一条规则拒绝了目的ip是AC并且目的端口号低于5000的TCP报文：

acl advanced 3102

rule 103 deny tcp destination 118.122.xx.xx 0 destination-port lt 5000

再次查看抓包发现AC使用低于5000的端口号与外网ip建立TCP连接，外网ip回复的目的端口号也是低于5000的，因此TCP三次握手的第二个报文匹配到了上述acl规则，被AC丢弃。这也解释了为何会不定时的出现业务不通的情况，因为当AC使用大于5000的端口号向外网IP发送建立TCP链接的三次握手报文时是没有问题的。

解决方法

删除对应的ACL规则即可