ACG1000防共享误识别问题解决办法

ACG1000 胡伟 2020-02-20 发表

组网及说明

无

问题描述

ACG防共享功能存在误识别情况

过程分析

当前共享上网检测支持如下5种特征的识别：

1：基于时间戳识别技术

经统计移动终端安卓、IOS发出的报文的syn包均携带时间戳，pc端则不带时间戳，根据这个特性把所有不带时间戳的流量认为是一个PC端，带时间戳的通过统计时间戳的轨迹识别出移动终端个数。

2：基于webRTC+flash COOKIE识别技术

该方式通过劫持用户的get请求，推送脚本代码，在用户终端设备上获取唯一标识信息，并设置为COOKIE的形式发送给设备进行终端统计。

3：基于UA识别技术

User Agent中文名为用户代理，简称 UA，它是一个特殊字符串头，使得服务器能够识别客户使用的操作系统及版本、CPU 类型、浏览器及版本、浏览器渲染引 擎、浏览器语言、浏览器插件等。

4：基于应用特征识别技术

通过获取应用特征中的唯一性标识，来统计终端个数。微信特征识别出的特征个数为移动端终端数，搜狗特征识别出的特征个数为PC端终端数。

5：基于微信长连接识别技术

通过分析微信的特性发现微信会存在一条用于保活的长连接。通过提取特征识别出微信流量，创建节点保存当前流量的信息，并记录会话创建的时间，以及当前时间，统计正反向报文个数。后续命中节点更新当前时间。最终计算更新时间和创建时间的差值若超过5分钟并且正反向报文都超过2个则认为是微信长连接。

上述几种可能会存在误识别情况，以192.168.1.100为例，可以通过# display user-share check-info ip 192.168.1.100可以查看终端共享具体被什么机制识别为多终端

```
==========================================================================
TCP timestamp       count      ctime     uptime   duration
==========================================================================
         100       1640    1214654    1215999       1345
--------------------------------------------------------------------------


==========================================================================
wechat long connection                    sendpkts recvpkts    ctime   uptime duration      state     device
==========================================================================
192.168.1.100:63496 -> 101.226.211.46:8080          13       18  1214654  1215904     1250  confirmed
        pc
```

可以通过命令关闭对应的检测特征

```
H3C(config)# user-share wechat off
H3C(config)# user-share
  check        user-share check user
  deny         user-share check user
  except       user-share exception
  flashCOOKIE  Flash COOKIE（flash COOKIE识别机制）
  freeze       Freeze and block flow packets
  log          freezed syslog
  timestamp    Tcp timestamp（时间戳）
  useragent    Http useragent（UA字段）
  wechat       Wechat long connection（微信长连接）
  white        user-share whitelist（白名单）
```

解决方法

通过命令关闭对应的检测特征。