

知 ACG1000阻断p2p流量后web页面下载微信客户端失败问题

ACG1000 特征库 李超 2016-07-05 发表

客户配置了ipv4策略，对p2p软件进行阻断，测试时发现采用ie浏览器默认在下载工具下载微信客户端时失败。

测试，当把应用审计中针对p2p流量的动作设置为允许时，即可用ie浏览器自带的下载工具下载微信客户端，当设置为阻断时，则会下载失败，从现象上看确实被识别为p2p流量，接下来分析是被识别为p2p中哪种特征。

将策略调整为针对p2p流量的动作为阻断并记录日志，通过查看日志发现当采用ie浏览器自带的下载工具下载微信客户端时，日志显示的为腾讯资源，腾讯资源属于p2p流量，后来跟客户了解到，客户在微信的官网上面下载的微信客户端，该行为确实会被识别为腾讯资源。

The screenshot shows the H3C SecPath ACG1000 application audit logs. The search criteria are set to 2016-06-24, showing 112430 logs. The table below is a representation of the log entries shown in the image.

序号	用户	应用	行为	处理动作	系统	终端	级别	时间	操作
1	10.66.53.30	腾讯新闻(移动端)	网页浏览	放行	Android	Android Phone	信息	2016-06-24 16:12:19	连接
2	10.66.53.30	腾讯网	网页浏览	放行	Android	-	信息	2016-06-24 16:12:17	连接
3	10.66.53.30	支付宝	登录	放行	Android	-	信息	2016-06-24 16:12:17	连接
4	10.66.50.101	QQ音乐(VIEW版)	网页浏览	放行	Android	Android Phone	信息	2016-06-24 16:12:16	连接
5	10.66.40.110	TeamViewer	操作	放行	-	-	信息	2016-06-24 16:12:16	连接
6	10.66.53.166	腾讯网	网页浏览	放行	Android 4.4.2	zh-cn; PE-TL10 Build	信息	2016-06-24 16:12:14	连接
7	10.66.16.112	腾讯资源	下载	阻断	Windows	-	信息	2016-06-24 16:12:14	连接
8	10.66.18.91	搜狗云输入法	下载	放行	Windows	-	信息	2016-06-24 16:12:14	连接
9	10.66.53.166	腾讯(移动端)	网页浏览	放行	Android	Android Phone	信息	2016-06-24 16:12:14	连接
10	10.66.53.115	新浪微博	网页浏览	放行	Android	Android Phone	信息	2016-06-24 16:12:12	连接
11	10.66.19.114	优酷土豆(Android版)	网页浏览	放行	Android	-	信息	2016-06-24 16:12:12	连接
12	10.66.40.103	迅雷远程控制	操作	放行	Windows	-	信息	2016-06-24 16:12:09	连接
13	10.66.40.103	迅雷远程控制	操作	放行	Windows	-	信息	2016-06-24 16:12:09	连接
14	10.66.6.66	快车	下载	阻断	Windows	pc	信息	2016-06-24 16:12:08	连接
15	10.66.6.118	搜狗云输入法	下载	放行	Android 6.0	-cn; HUAWEI NXT-A	信息	2016-06-24 16:12:08	连接
16	10.66.13.101	快车	下载	阻断	Android	-	信息	2016-06-24 16:12:06	连接
17	10.66.16.112	腾讯网	网页浏览	放行	Windows	-	信息	2016-06-24 16:12:06	连接

自定义一个应用组，将除了腾讯资源之外的其他p2p软件加入到该应用组，然后在策略中引用即可解决该问题。

当发现误识别时，可以查看相关日志来确定具体被识别为哪种行为，然后调整策略即可。