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浏览器默认的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。

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。