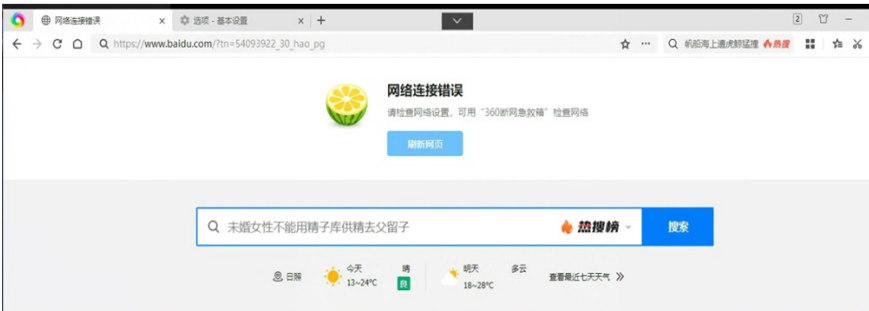


知 acg控制策略在微软浏览器上不生效

ACG1000 叶红兵 2024-05-28 发表

问题描述

控制的应用策略通过微软浏览器访问网站不生效，360浏览器可以



过程分析

查看审计策略，url过滤和应用过滤都开启



设备优先匹配url过滤，查看日志，使用360浏览器访问可以看到被阻断，使用微软浏览器没有控制日志

序号	时间	源IP	目标IP	应用分类	应用	策略类型	处理动作	策略类型	级别	时间	操作
1	172.16.2.3	6c82-d3-60-60-01	办公软件	WPS办公软件_网页浏览	应用控制	阻断	PC	信息	2024-05-15 15:51:28	详细	
2	172.16.2.3	6c82-d3-60-60-01	办公软件	WPS办公软件_网页浏览	应用控制	阻断	PC	信息	2024-05-15 15:51:26	详细	
3	172.16.2.3	6c82-d3-60-60-01	办公软件	WPS办公软件_网页浏览	应用控制	放行	PC	信息	2024-05-15 15:48:42	详细	
4	172.16.2.3	6c82-d3-60-60-01	搜索引擎	百度	应用控制	阻断	PC	信息	2024-05-15 15:44:29	详细	
5	172.16.2.3	6c82-d3-60-60-01	搜索引擎	百度	URL控制	阻断	PC	测试	2024-05-15 15:41:24	详细	
6	172.16.2.3	6c82-d3-60-60-01	搜索引擎	百度	URL控制	阻断	PC	测试	2024-05-15 15:41:24	详细	
7	172.16.2.3	6c82-d3-60-60-01	搜索引擎	百度	URL控制	阻断	PC	测试	2024-05-15 15:41:24	详细	
8	172.16.2.3	6c82-d3-60-60-01	搜索引擎	百度	URL控制	阻断	PC	测试	2024-05-15 15:41:24	详细	
9	172.16.2.3	6c82-d3-60-60-01	搜索引擎	百度	URL控制	阻断	PC	测试	2024-05-15 15:24:16	详细	
10	172.16.2.3	6c82-d3-60-60-01	搜索引擎	百度	URL控制	阻断	PC	测试	2024-05-15 15:24:16	详细	
11	172.16.2.3	6c82-d3-60-60-01	搜索引擎	百度	URL控制	阻断	PC	测试	2024-05-15 15:24:16	详细	
12	172.16.2.3	6c82-d3-60-60-01	搜索引擎	百度	URL控制	阻断	PC	测试	2024-05-15 15:24:16	详细	
13	172.16.2.3	6c82-d3-60-60-01	搜索引擎	百度	URL控制	阻断	PC	测试	2024-05-15 15:24:10	详细	
14	172.16.2.3	6c82-d3-60-60-01	搜索引擎	百度	URL控制	阻断	PC	测试	2024-05-15 15:24:10	详细	
15	172.16.2.3	6c82-d3-60-60-01	搜索引擎	百度	URL控制	阻断	PC	测试	2024-05-15 15:24:10	详细	
16	172.16.2.3	6c82-d3-60-60-01	搜索引擎	百度	URL控制	阻断	PC	测试	2024-05-15 15:24:10	详细	
17	172.16.2.3	6c82-d3-60-60-01	其他类	百度通行证	应用控制	阻断	PC	信息	2024-05-15 15:22:27	详细	
18	172.16.2.3	6c82-d3-60-60-01	其他类	百度通行证	应用控制	阻断	PC	信息	2024-05-15 15:19:19	详细	

查看acg设备适配的浏览器，版本高于推荐版本



31. 浏览器审计、控制支持哪些浏览器

浏览器审计、控制支持的浏览器及推荐版本如下表。

浏览器	推荐版本
谷歌 64 位	104.0.5112.81
火狐 64 位	106.0.2
Microsoft Edge 64 位	106.0.1370.52
IE11 64 位	9.11.19041.0
360安全 64 位	13.1.6230.0
360极速浏览器 32 位	13.5.2036.0
搜狗浏览器 64 位	11.0.1.34700

解决方法

通过抓包确认为谷歌、edge浏览器内核升级后ACG应用控制不生效问题。

因为edge和谷歌内核升级后，extension 扩展字段key_share（密钥交换参数） 字段长度扩大（仅该字段就扩大到1263字节），从而导致client hello 分片，设备目前不识别分片的servername请求，导致部分url无法识别进而被阻断。需要等待发布的6616P04版本解决。规避方法：使用其他浏览器

```

#shandaha.type == 1
No.    Time           Source           Destination      Protocol Length  Identification    Time to Live  Info
-----
205 16:03:47.489135  172.16.2.3      120.192.64.36   TLSv1.3         480  0x071c (28956)    127 Client Hello (SNI=www.baidustatic.com)
218 16:03:47.494231  172.16.2.3      39.156.66.14    TLSv1.2         389  0x2768 (38888)    127 Client Hello (SNI=www.baidu.com)
215 16:03:47.498643  172.16.2.3      39.156.66.14    TLSv1.2         389  0x78a3 (38883)    127 Client Hello (SNI=www.baidu.com)
586 16:03:47.712576  172.16.2.3      52.168.117.175  TLSv1.3         477  0x0265 (29565)    127 Client Hello (SNI=browser-events.data.msn.cn)
586 16:03:47.768619  172.16.2.3      120.220.67.38   TLSv1.3         486  0x71e8 (29160)    127 Client Hello (SNI=vectorstatic.baidu.com)
527 16:03:47.936296  172.16.2.3      52.168.117.175  TLSv1.3         703  0xa026 (42554)    127 Change Cipher Spec, Client Hello (SNI=browser-events.data.msn.cn)
536 16:03:48.074585  172.16.2.3      39.156.66.14    TLSv1.2         421  0x7915 (38997)    127 Client Hello (SNI=spl.baidu.com)
541 16:03:48.077992  172.16.2.3      39.156.66.14    TLSv1.2         389  0x7919 (31800)    127 Client Hello (SNI=spl.baidu.com)
558 16:03:48.101953  172.16.2.3      39.156.66.14    TLSv1.2         329  0x0c1c (1381)     127 Client Hello (SNI=spl.baidu.com)
634 16:03:48.415763  172.16.2.3      111.63.96.59    TLSv1.2         330  0x413f (14703)    127 Client Hello (SNI=passport.baidu.com)

-----
Extension: server_name (len=18) name=www.baidu.com
Type: server_name (0)
Length: 18
  Server Name Indication extension
Extension: extended_master_secret (len=0)
Type: extended_master_secret (22)
Length: 0
  Extension: key_share (len=1263) a25519k9ber7680raff80, a25519
Type: key_share (61)
Length: 1263
  Key Share extension
  Client Key Share Length: 1261
  Key Share Entry: Group: Reserved (GREASE), Key Exchange length: 1
  Key Share Entry: Group: a25519k9ber7680raff80, Key Exchange length: 1216
  Key Share Entry: Group: a25519, Key Exchange length: 32
Extension: Reserved (GREASE) (len=1)
Type: Reserved (GREASE) (43690)
  
```