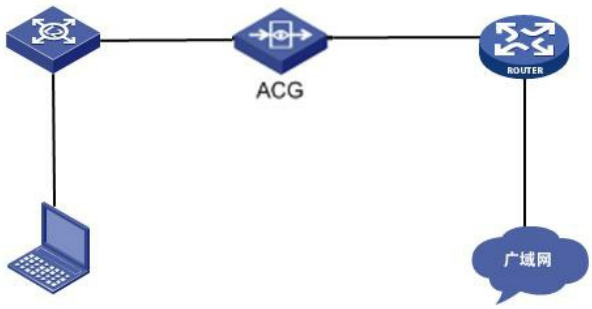
ACG1000 配置拒绝any应用后无法打开网页

ACG1000 应用审计 **周学丰** 2016-03-01 发表



用户需求是只允许QQ客户端和电子邮件（web和客户端）的应用程序，其它应用全部拒绝。当前设备软件版本和特征库版本都是最新的，在应用审计中分别配置允许QQ和电子邮件，最后配置拒绝所有应用，匹配方式为默认的全匹配。配置完成后无法打开各类网页，提示DNS无法解析。

1、当前版本针对应用审计的匹配规则包括全匹配和顺序匹配。默认为全匹配，即当报文可以匹配到该七元组策略的多条应用规则（同时包含拒绝、允许两种动作）时，执行拒绝动作。顺序匹配则按照匹配到的第一条应用规则执行。根据当前问题判断，应该选择顺序匹配。

2、打开浏览器，访问电子邮件的web界面，提示访问被禁止。查看应用日志信息，可以看到被网络协议中的域名解析协议（DNS）阻断了。

其它应用日志

查询 重置 **查询结果：** 在 2016-02-20 约 198 条日志记录中，从 1-198 搜索出相关结果 198 条，显示 1-20

	用户	应用	行为	处理动作	系统	终端	级别	时间	操作
1	192.168.9.76	域名解析协议(DNS)	网络协议	阻断	-	-	信息	2016-02-20 14:26:13	详细
2	192.168.9.76	域名解析协议(DNS)	网络协议	阻断	-	-	信息	2016-02-20 14:26:11	详细
3	192.168.9.76	域名解析协议(DNS)	网络协议	阻断	-	-	信息	2016-02-20 14:26:11	详细
4	192.168.9.76	域名解析协议(DNS)	网络协议	阻断	-	-	信息	2016-02-20 14:26:11	详细
5	192.168.9.76	域名解析协议(DNS)	网络协议	阻断	-	-	信息	2016-02-20 14:26:11	详细
6	192.168.9.76	域名解析协议(DNS)	网络协议	阻断	-	-	信息	2016-02-20 14:26:11	详细
7	192.168.9.76	域名解析协议(DNS)	网络协议	阻断	-	-	信息	2016-02-20 14:26:11	详细

3、在应用策略—应用审计中添加一条允许网络协议—域名解析协议（DNS）的策略，最后再配置拒绝any应用。此时访问邮件的web页面再查看应用日志信息，发现访问被网络协议中的NETBIOS名称服务阻断了。

4、根据前面的方法，再添加一条允许NETBIOS名称服务的策略，此时再查看应用日志信息，发现又被网络协议中的多播名称解析（MDNS）和网页浏览（HTTP）阻断。

其它应用日志

查询 重置 **查询结果：** 在 2016-02-20 约 2285 条日志记录中，从 1-2285 搜索出相关结果 2285 条，显示 1-20

	用户	应用	行为	处理动作	系统	终端	级别
1	192.168.9.5	多播名称解析(mDNS)	网络协议	阻断	-	-	信息
2	192.168.9.5	多播名称解析(mDNS)	网络协议	阻断	-	-	信息
3	192.168.9.76	网页浏览(HTTP)	Web浏览	阻断	Windows	-	信息
4	192.168.9.76	网页浏览(HTTP)	Web浏览	阻断	Windows	-	信息
5	192.168.9.76	网页浏览(HTTP)	Web浏览	阻断	Windows	-	信息

配置了拒绝any的应用审计策略后，ACG1000系列设备会根据应用的优先级逐条的进行匹配，根据前面处理过程可知这个工作量会非常大，且会存在其它的风险。

当遇到只允许访问部分应用且阻断其它所有应用的需求时，不建议配置拒绝any应用的方式，建议可以先配置允许any应用，然后观察应用日志信息，根据日志去确认需要阻断哪些应用，再逐条的配置这些策略。

后续遇到ACG1000配置拒绝any应用后无法打开网页问题时，可以这样做:

1. 先配置允许any应用，设备接入网络正常运行；
2. 观察应用日志，确认内网用户访问了哪些应用；
3. 根据用户实际需求，逐条将指定应用配置成拒绝，应用审计策略的配置是一个逐步完善的过程；

以上操作无法解决，及时收集信息反馈给我司工程师处理。