ACG1040无法使用指定URL打开应用缓存文件

ACG1000 曾泓杰 2016-04-28 发表

一、 问题现象：

客户在设备ACG1040的“网络优化 - 应用缓存”中配置了应用缓存文件，缓存文件能正常上传到设备本地。但是使用设定好的URL地址无法跳转到相应缓存文件的打开或下载页面，页面出现404的错误提示。客户已排查浏览器的兼容性问题和内外网之间的连通性问题。客户使用的URL为设备内网网关接口地址为——192.168.1.254/24，即指向设备本身的URL地址，具体配置如下图所示：

图1.1 设备应用缓存URL地址和应用缓存文件的配置

图1.2设备应用缓存URL地址和应用缓存文件的配置

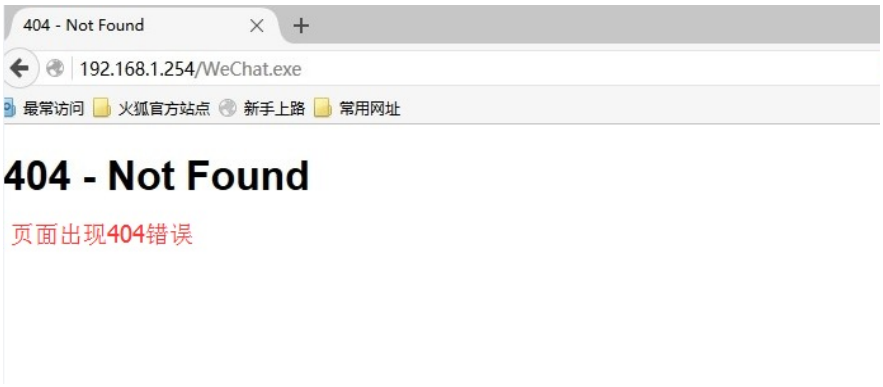


图1.3 打开设置的URL地址，页面提示404页面无法找到的错误提示

二、 组网

针对客户的情况，在实验室搭建了环境模拟客户现场环境进行测试验证。测试所使用的设备是ACG1040，下面单接一台PC客户端，PC的IP地址为172.168.1.2/24，设备内网口的地址为172.168.1.1/24。设备的外网口与因特网相连。

图2.1 模拟客户组网拓扑环境

步骤一：

进入设备web页面，点击“网络优化 - 应用缓存”，新建了以设备内网口地址为应用缓存请求发起的URL

进行测试，现象与用户的一致，抓包信息如下：

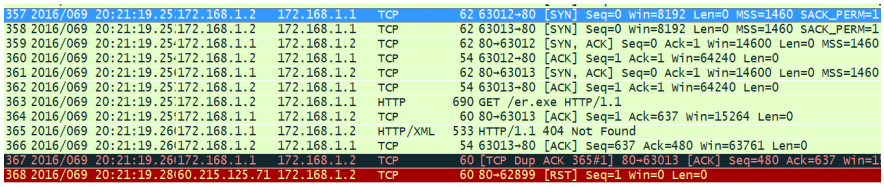


图3.1 URL填写为设备内网口地址

从抓包信息来看，客户端PC172.168.1.2/24与设备172.168.1.1/24建立了TCP三次握手连接以后，客户端向设备发送HTTP GET请求，请求应用缓存里配置的指定URL，接着设备向客户端回应了HTTP 404消息，表示没有找到所请求的文件。

根据这一现象，我猜想，有以下几种原因会导致这样的现象的出现：

1、设备可能配置不完整，导致不能正确识别出这是用于重定向应用缓存功能的HTTP GET报文。

2、URL规则填写不正确，设备不能正确进行重定向URL。

3、与组网测试的网络拓扑有关。

步骤二：

根据步骤一的猜想，我首先对照手册检查了设备相应的配置信息，发现没有其他相关的配置影响。接下来，针对第二点，我猜想URL是否应该改写成公网中能够正确DNS寻址的域名的形式去填写，就把应用缓存的URL改成广域网中真实存在的域名进行测试。

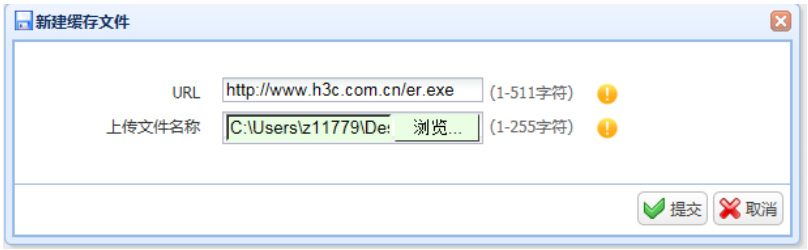


图3.2 URL填写为华三的官网去让设备寻址

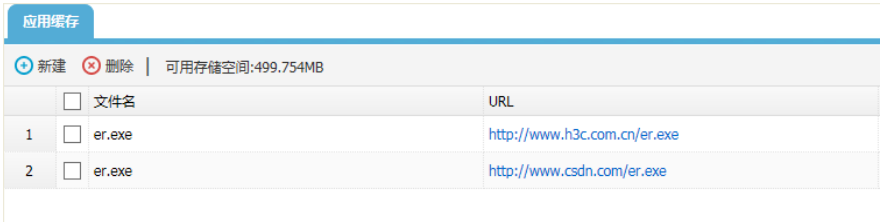


图3.3 新增了华三官网和CSDN官网两个URL进行测试

在浏览器输入这两个URL，都能成功重定向到设备本身172.168.1.1/24进行应用下载

图3.4 能正确重定向到ACG1040的应用缓存目录进行下载

同时，访问http://www.h3c.com.cn/er.exe这条URL的抓包信息如下：

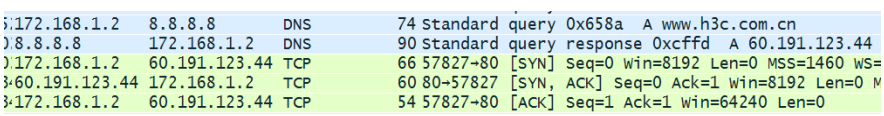


图3.5 客户端DNS寻址，与服务器60.191.123.44建立TCP三次握手连接

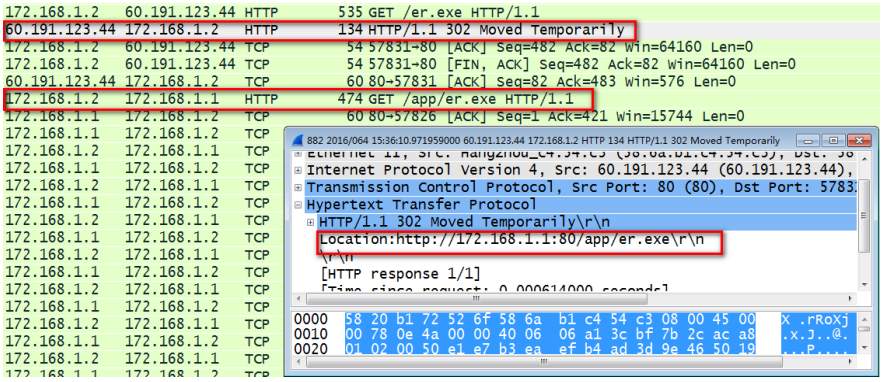


图3.6 HTTP GET请求被重定向到设备本身172.168.1.1/24，并能成功获取缓存文件

从图3.5的抓包信息来看，URL地址被正确DNS解析并寻址后，外网服务器60.191.123.44给客户端172.168.1.1发送了一条重定向信息，告诉客户端重定向到http://172.168.1.1/er/exe去请求相应页面。客户端重新向172.168.1.1发送了HTTP GET请求，并且能成功获得应用缓存文件。

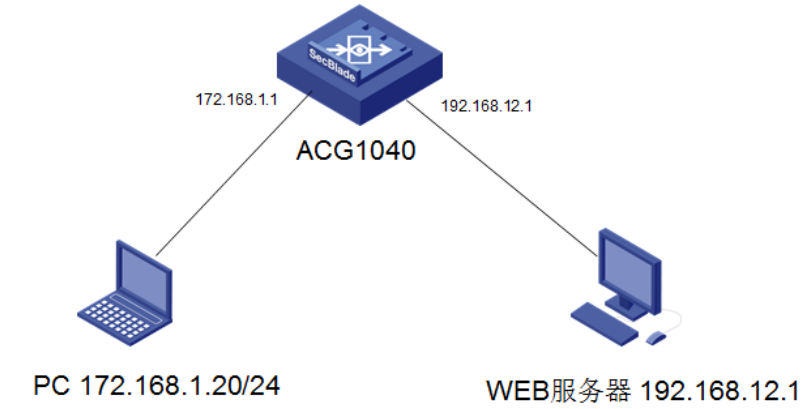
在这里，还存在以下两点疑问：

1、设备ACG1040审计到匹配了应用缓存的URL以后，应该是由设备本身172.168.1.1向客户端发送重定向消息，而抓包显示的是由外网服务器发送的重定向数据包，这个数据包是否是由设备伪造的呢？

2、这次测试使用的是域名的方式，使用固定IP的方式访问是否有问题呢？

步骤三：

根据上述的两个疑问，我们在内网搭建了一台WEB服务器，让客户端以请求内网WEB服务器地址的形式去发送HTTP GET请求报文。



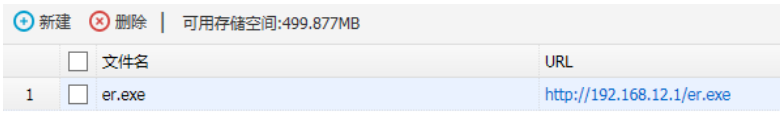


图3.8 应用缓存页面的设置

能正常打开应用缓存界面，抓包信息如下：

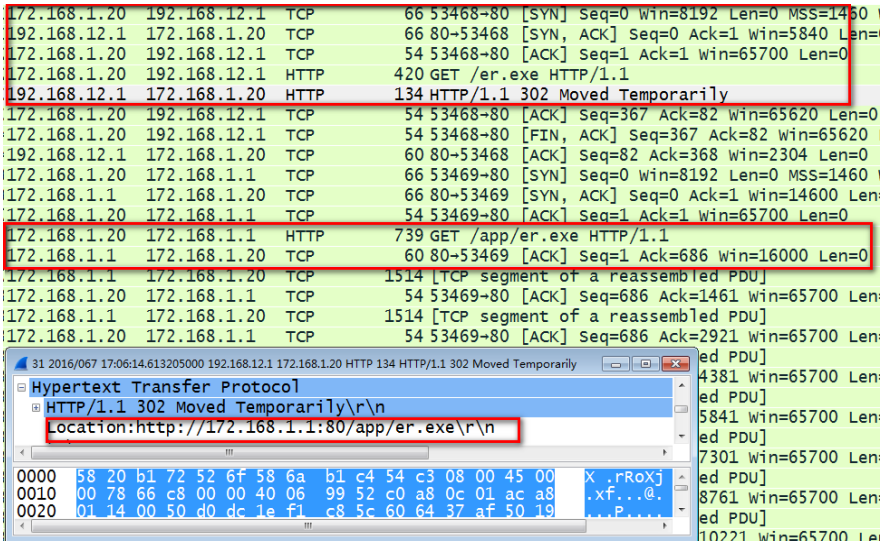


图3.9 以内网WEB服务器地址配置应用缓存URL，能成功访问的抓包信息

从抓包信息可看出，客户端直接向WEB服务器192.168.12.1发起HTTP GET请求，WEB服务器回复重定向信息，然后客户端再重新向设备发起请求并成功打开应用缓存页面。

步骤四：

通过以上实验的抓包分析，我们可以看出应用缓存的实际工作机制有以下几个关键的理解要点：

1、客户端发送的HTTP GET请求匹配到设备设置的应用缓存URL，设备会回复一条重定向的HTTP 302信息给客户端，告诉客户端应向设备本端重新发起HTTP GET请求。

2、抓包看到的HTTP重定向消息，实际上是设备伪造服务器的地址给客户端发送的，实际上重定向的消息是由设备自己发出。

3、应用缓存的URL地址无论是配置域名的形式还是IP地址的形式，只要设备能跟远端服务器建立起TCP三次握手连接，并且发送可匹配被重定向的HTTP GET请求消息即可。

4、应用缓存的URL地址设置成设备本身不合理，因为数据流不符合应用缓存的整个处理流程，设备不能进行伪造远端服务器回复HTTP重定向的信息这一步，所以请求失败，返回404错误提示。

5、必须是经过ACG设备的HTTP GET请求(不是请求设备本身)，才能触发设备进行HTTP GET重定向的处理。

配置数据流经过ACG设备审计的服务器URL即可，域名形式和IP地址的形式都可以触发重定向处理操作。