F1000-C-G带宽管理模块特征库误识别

特征库　曾泓杰　2016-04-28 发表

一、 问题现象：

客户的防火墙F1000-C-G在带宽管理策略的配置处,做了P2P模块相应的下载限制，配置之后发现在电脑上登录微信时，扫码界面的二维码加载不出来，将P2P下载限制取消之后就可以正常加载。客户猜想可能是P2P下载限制了二维码的加载，但是不确定具体是里面哪个模块与二维码加载产生了冲突。客户具体配置和现象反馈如图：

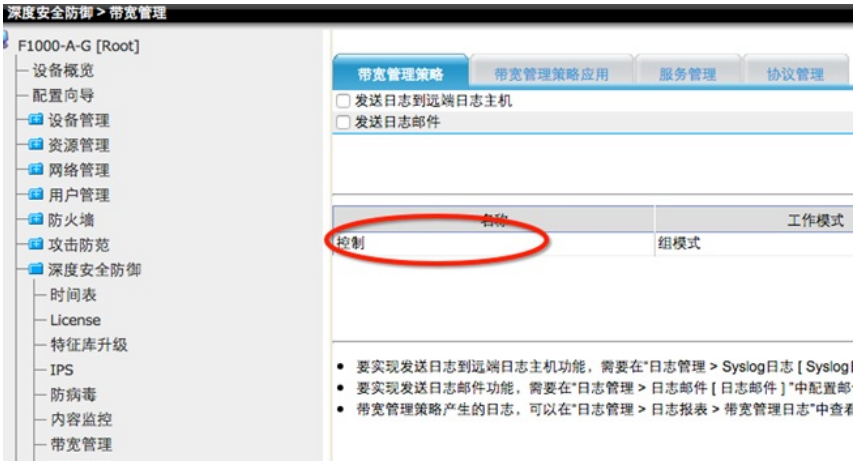

图1.1 设备新建了带宽管理策略

图1.2带宽管理策略的配置里面配置了P2P模块，动作设置为阻断

图1.3客户端无法获取二维码

图1.4 P2P动作改为允许后加载正常

一、 组网

根据客户反馈的实际情况，初步猜想，可能是由特征库误识别造成的。待客户反馈了设备软件版本、硬件信息和特征库版本信息后，根据客户实际组网的情况，在实验室搭建了相类似环境进行测试。

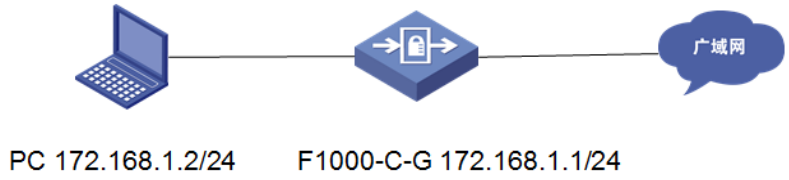

图2.1 模拟客户组网拓扑环境

步骤一：
首先，怀疑特征库的误识别问题，先将设备的特征库升级到最新，验证最新特征库对这方面应用的数据流是否有优化识别的措施。设备有两个特征库，一个是IPS特征库，里面包含了APP应用识别和IPS攻击防范的内容；一个为病毒库，里面包含AV特征库的内容。针对带宽管理的应用，我们升级IPS特征库。

图3.1 将设备的IPS特征库升级到官网最新2.1.323版本
接下来将带宽管理策略里的P2P模块配置为阻断，并且输出日志信息，同时在PC客户端上实时抓包。

图3.2 在带宽管理策略里面配置P2P模块的动作为阻断并输出日志
这时打开微信客户端验证，发现现象跟客户现场的一致，二维码无法成功加载，多次刷新后现象也一致。
步骤二：
根据步骤一的现象，我们的猜想得到了初步的验证。但还需检测出是P2P中哪个模块的影响。

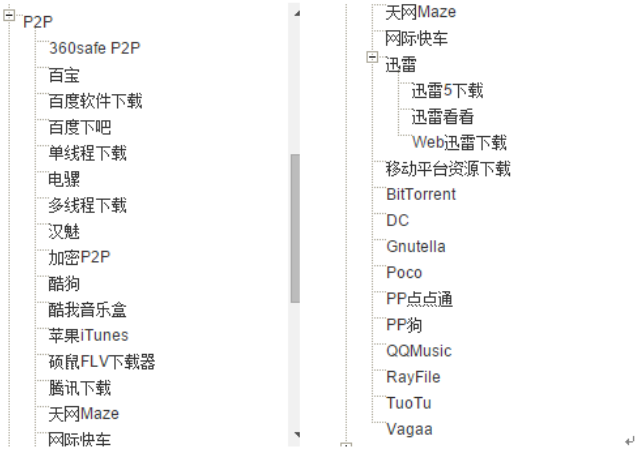

图3.3 设备服务管理里面P2P模块展开的信息

我们阻断的动作里面设置了日志输出，即结合抓包信息，只要找到相应的地址里面对应日志的阻断信息，就可以判断出P2P模块下哪个子项的协议起了作用。

时间	服务	动作	源域	目的域	源IP	目的IP	源端口	目的端口	应用协议
6:21:45	P2P	阻断	Trust	Untrust	172.168.1.2	140.207.54.116	60743	80	Download of MultiThread
6:21:40	P2P	阻断	Trust	Untrust	172.168.1.2	58.247.204.139	60738	80	Download of MultiThread
6:21:35	P2P	阻断	Trust	Untrust	172.168.1.2	223.167.105.115	60735	80	Download of MultiThread
6:21:34	P2P	阻断	Trust	Untrust	172.168.1.2	58.247.204.139	60734	80	Download of MultiThread
6:13:49	P2P	阻断	Trust	Untrust	172.168.1.2	140.206.160.213	60501	80	Download of MultiThread
6:13:44	P2P	阻断	Trust	Untrust	172.168.1.2	223.167.105.115	60497	80	Download of MultiThread
6:13:39	P2P	阻断	Trust	Untrust	172.168.1.2	58.247.204.139	60496	80	Download of MultiThread
6:13:38	P2P	阻断	Trust	Untrust	172.168.1.2	140.207.54.116	60495	80	Download of MultiThread
6:04:38	P2P	阻断	Trust	Untrust	172.168.1.2	140.206.160.213	60159	80	Download of MultiThread
6:04:33	P2P	阻断	Trust	Untrust	172.168.1.2	117.144.242.26	60156	80	Download of MultiThread
6:04:28	P2P	阻断	Trust	Untrust	172.168.1.2	117.144.242.26	60153	80	Download of MultiThread

图3.4 带宽管理日志的信息

在带宽管理日志里面看到，P2P模块的Download of MultiThread应用协议匹配到了阻断的动作。对照抓包信息，发现140.207.54.116等报文都出现了TCP交互失败的内容；查找P2P模块的内容，找到相应的模块。

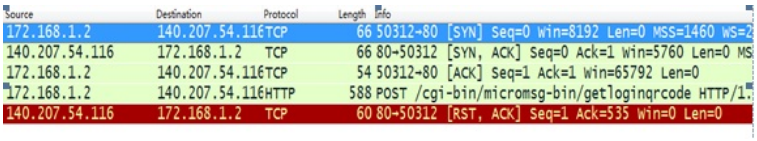

图3.5 日志里面的几个被阻断IP都出现TCP交互失败的报文

图3.6 Download of MultiThread应用协议相对应的服务模块

由上面的抓包信息和服务管理里面模块、应用协议的信息，可以发现是P2P服务里面的多线程下载这个子项对应了此协议。

步骤三：

接着，我们将P2P模块动作改为允许，微信客户端二维码就能正常加载了，更加确定了这一模块引起的误识别问题。

那么这样的问题是否有规避方法呢？

首先，我们考虑这个模块是否能取消勾选。在设备的WEB页面上操作发现，P2P模块只能进行整体的操作，不能对里面单独的子项进行增加、删减等操作。接着，我们发现带宽管理策略在被引用的时候，可以设置例外IP地址。通过设置例外IP地址的方法，可以让客户指定需要使用微信客户端的PC在设备上做IP与MAC地址绑定，然后设置为例外IP，P2P模块的阻断动作就不会对这些IP地址所绑定的终端生效了。

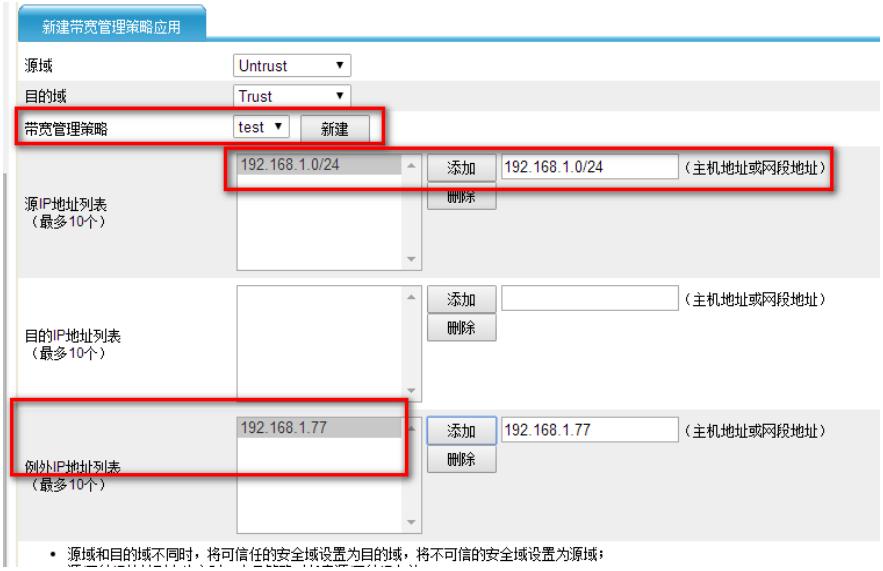

图3.7 带宽管理策略引用的时候设置例外IP

设置例外IP地址的方法可以对需要使用微信客户端操作的终端实现免P2P模块的阻断动作的效果，达到一时的规避效果，但一般客户都是要求所有用户都要实现这一操作，所以这种做法并不能完全解决客户问题。

最后，反馈特征库误识别问题给产品线研发，推动改进此特征库P2P服务模块对多线程下载这一应用数据流的识别方法。特征库进行改进更新以后，导入客户设备，问题解决。

遇上特征库误识别的问题，可以采取以下步骤验证

1、收集客户设备版本信息、特征库版本信息，搭建环境模拟客户实际组网进行测试。
2、查看日志内容，查看是哪个服务模块阻断了与有关IP地址的交互。
3、查看服务模块对应的应用协议，找出是哪个基本模块的问题。
4、可以采取例外IP的规避措施达到让一部分有这个需求的终端，跳过有问题的服务模块的阻断动作。
5、反馈产品线研发，更新特征库解决。