

通过WAF设备反向代理方式访问下载web服务器上应用时，流量显著变大情况问题分析

WAF 郑标 2020-04-26 发表

组网及说明

不涉及

问题描述

客户反馈在公司内网访问192.168.255.100:8520和外网同时访问srm.henglihydraulic.com:8520（流量过WAF设备，外网做了映射），每次都会下载请求400多M的文件，再次刷新还要重新下载400多M的文件，真实的SRM应用包只有90M左右；但如果不经WAF，直接在内网访问192.168.253.3：8520，每次下载只有90M左右，如果进行刷新测试将会下载更小的文件资源，客户疑问是为什么同一个应用，通过WAF来访问会增加这么多的流量。

过程分析

通过抓包对比分析，经过WAF的时候页面变大是由于现场开启了敏感信息监测规则，敏感信息的客服端的请求，WAF会去替换Accept-Encoding，要求服务器不要返回压缩后的数据，不然WAF没有办法解析响应包中的敏感信息数据，一般请求的acc编码格式是gzip默认的，但是如果启用了敏感词就会要求数据不压缩，server端的数据自身是有400m左右的，如果pc端访问请求后想展现所有的数据就要请求400m左右的全部数据，只是数据在传输过程中默认都是gzip等默认压缩传输，但是如果压缩之后WAF的敏感词规则就没办法去分析包中的敏感信息数据了。所以关闭了敏感信息检测规则的话就和不过WAF的大小一样了。



敏感信息检测：比如说网站有身份证信息需要展示给客户看，在WAF开启敏感信息监测，把身份证擦除。这个时候WAF和server交互的时候会处理server的响应中的身份证信息，把处理后的响应发给客户端，不仅仅服务器版本还有响应体重身份证、电话、银行卡邮箱等 还可以自定义，都同样包含敏感词信息。

解决方法

关闭敏感信息检测，流量大小恢复正常。