IIS和Apache服务器统计LB上X-Forward-For的方法

七层服务器负载均衡 朱尘炀 2015-11-20 发表

某些LB的七层服务器负载组网环境中，为了保证来回流量路径一致，针对LB调度后的HTTP流量做了SNAT，导致后端服务器上看到的访问请求的源IP都是LB的，此时服务器上就无法统计客户端的访问量，无法审计用户端的访问请求，无法针对客户端源IP执行相关策略.....

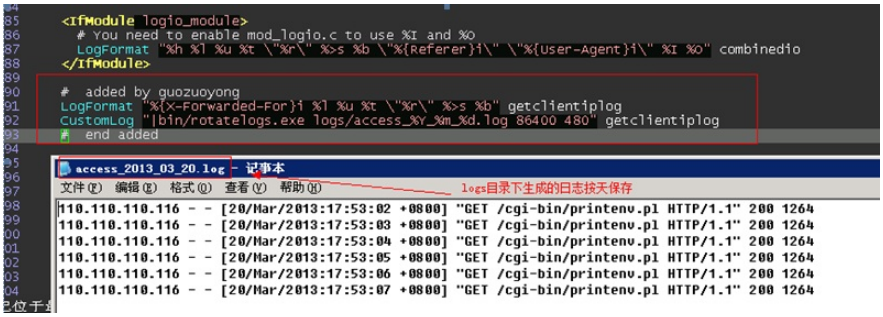
如果LB外网方向有针对某个虚服务的攻击，此时后端服务器上看到的攻击源IP都是LB的，可能导致误判LB“攻击”服务器，此时为了需要分析具体攻击行为，需要确切地知道客户端源IP！
无告警信息，服务器看到的所有的访问请求都是LB的地址

在该组网环境下，LB针对调度到实服务的流量，做了SNAT，所以服务器看到的IP地址都是LB的

1、LB上开启HTTP携带源地址，选择X-Forwarded-For

2、Linux-apache 版本server配置方法
测试拓扑： 单臂（旁路）部署

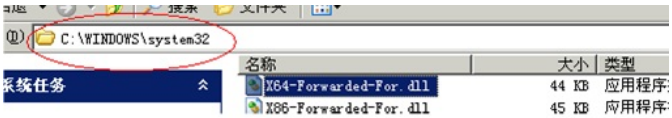
LB
| 110.110.110.154
|
客户端 110.110.110.116 ----------110.110.110.2 服务器
vi /etc/httpd/conf/httpd.conf （具体路径，以服务器实际路径为主）
自行手动按照如下格式配置，也可以直接复制粘贴过去：
插入头部： LogFormat "%{X-Forwarded-For}i %l %u %t \"%r\" %>s %b" getclientiplog
日志存放路径：CustomLog "|bin/rotatelogs.exe logs/access_%Y_%m_%d.log 86400 480" getclientiplog
如下图所示的配置和日志格式：



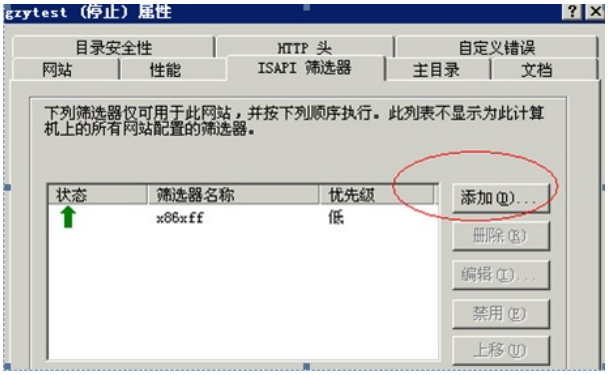
3、Windows Server-IIS版本server配置方法
测试站点名称：gzytest
验证拓扑 pc（10.10.10.116） ----SW---LB （10.10.10.3）

|
server （10.10.10.12）

（1）把插件放到下面这个目录，32位用x86的，64位用x64的

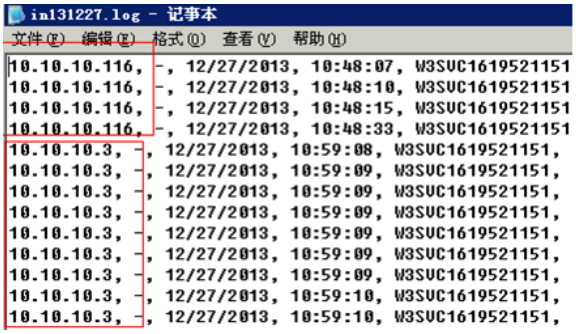


（2）停止站点运行，把对应插件加到isapi筛选器里，启动网站

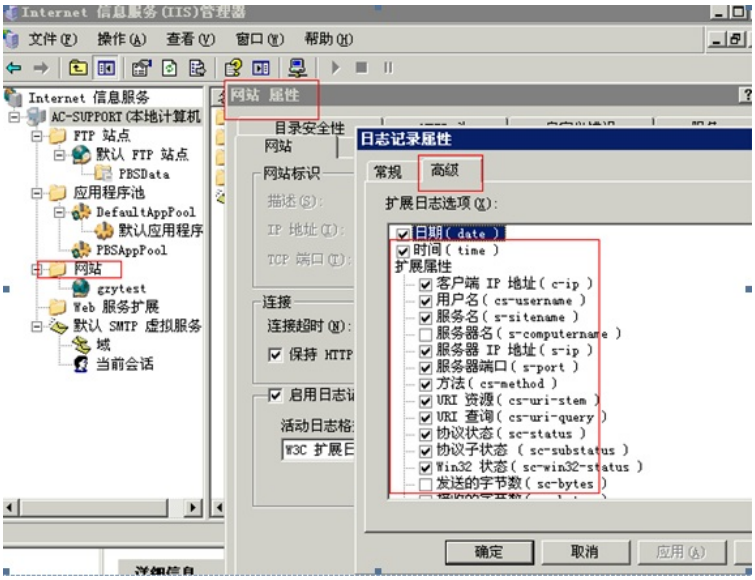


（3）日志目录看设置，默认日志是下面的目录

（4）图上面红框是用插件的，显示是客户端地址；下面是没用插件的，显示是LB snat的地址



注:日志字段是可选的



1、windows服务器上的X-Forward-For插件见附件文件，32位的用x86的插件，64位的用x64的插件

2、linux的服务器上X-Forward-For插件是手动配置的，详细可以参考给出的配置命令和截图中的配置命令

3、本文档给出的服务器上识别X-Forward-For插件的方法，适用于所有支持标准X-Forward-For方式的设备，同时必须是七层的HTTP流量