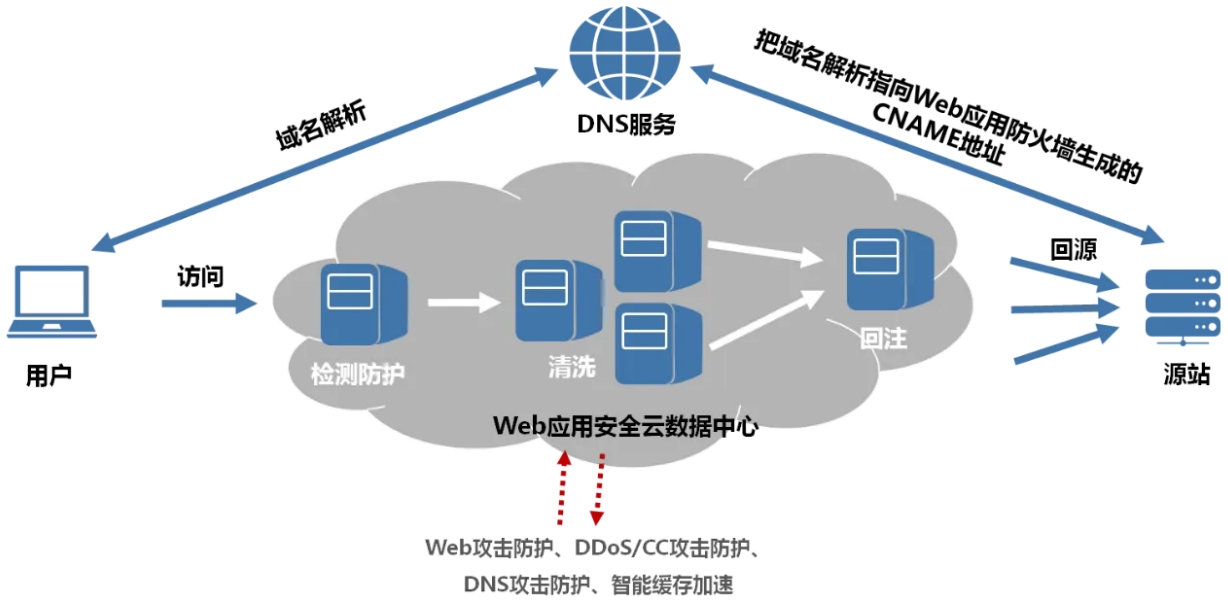
软防护dos攻击

笔记本: 应急
创建时间: 2022/4/14 8:57

一、概述

在如今互联网时代，小程序投票已经变得越来越普及，通过转发朋友圈，来让大家进行投票，原本这是一种相对公平的方法，让大家根据自己的喜好选出喜欢的作品。但是随着利益的驱使，网络上出现了很多“票贩子”，借助系统的漏洞，进行重复刷票，与用户签订协议刷到指定的名次就可以获取一定的收益。通过不停变化ip地址投票请求进行多次重放，由于所发的数据包为合法请求，多数安全设备可能不会给予拦截，但是却对服务器带来很大压力，造成服务器cpu、内存被一些非法连接占满，最终直接导致服务器卡死，系统无法正常给与响应，间接造成ddos攻击，解决这个问题最好的办法还是通过云waf、cdn等安全设备进行防护，通过前端的安全设备进行部分流量筛查之后在转发到服务器上进行流量转发，从而减轻应用服务器的自身压力，防护过程如下图（图片源于互联网），有硬件防护固然是好，那么在没有安全设备的防护情况下，我们如何利用现在的条件去做临时性防护呢，接下来讨论几个软防护方法。



二、常见防护方法

2.1 中间件屏蔽关键字

2.1.1 ngix中间件

如果应用程序采用了ngix的中间件，那可以通过修改ngix的配置文件去屏蔽到指定关键字，比如任意选取ngix日志中一条记录进行分析，红框标记的字段内容依次如下：

$remote_addr：与 $http_x_forwarded_for 用以记录客户端的ip地址；
$remote_user：用来记录客户端用户名称；
$time_local：用来记录访问时间与时区；
$request：用来记录请求的http的方式与url；
$request_time：用来记录请求时间；
$status：用来记录请求状态；成功是200，
$body_bytes_sent：记录发送给客户端文件主体内容大小；
$http_referer：用来记录从那个页面链接访问过来的；
$http_user_agent：记录客户端浏览器的相关信息。

可通过星图来查看日志分析情况，筛选出访问量比较大的ip

基于IP，分析IP对应地域、访问量、流量消耗

ID	访问次数	访问占比%	IP	国家/地区	流量	流量占比%
1	47,380	9.214%	125.123.120.132	中国-浙江嘉兴	7.98 M	9.038%
2	38,937	7.572%	123.157.144.99	中国-浙江绍兴	6.39 M	7.240%
3	30,115	5.857%	223.87.69.250	中国-四川攀枝花	4.98 M	5.638%
4	24,535	4.771%	139.206.155.244	中国-四川	4.09 M	4.631%
5	23,909	4.650%	223.87.69.4	中国-四川攀枝花	3.99 M	4.522%
6	21,909	4.261%	111.85.162.176	中国-贵州贵阳	3.58 M	4.052%
7	21,226	4.128%	112.192.106.153	中国-四川攀枝花	3.55 M	4.024%
8	21,183	4.120%	27.219.43.106	中国-山东青岛	3.99 M	4.517%
9	19,733	3.838%	60.12.177.120	中国-浙江绍兴	3.44 M	3.900%
10	17,229	3.351%	222.89.70.117	中国-河南新乡	2.87 M	3.251%

利用

```
cat  c740.log | awk -F\" '{A[$(NF-1)]++}END{for(k in A)print A[k],k}' | sort -n
```

查看useragent的访问情况，由于的日志数量较为庞大，可通过tail -n选取部分数据进行分析，在本次的日志分析中，可发现同一条agent出现511922次，肯定为非正常请求，可将其加入ngix的配置中

限制某useragent访问可利用如下脚本

```
if ($http_user_agent ~ 'Build/JZO54K')
    {
       return 403;
    }
```

禁止非GET|HEAD|POST方式的抓取

```
if ($request_method !~ ^(GET|HEAD|POST)$) {

return  403;

}
```

限制http_referer访问

```
if ($http_referer ~* "www.xxx.com") {
return 403;
```

防止特定IP的请求

```
  if ($remote_addr =  “IP地址“)  {
              return   500;
       }
```

也可以自己编写python脚本进行筛选，通过执行系统命令，筛选出连接请求大于80次的ip地址，并进行归属地判断，将结果保存在表格中，如下图

id	ip地址	ip_归属	count
3	139.206.155.244	中国_四川省_中坝	290
5	118.76.245.109	中国_山西_安阳	271
6	139.203.8.26	中国_四川省_中坝	264
2	139.203.8.236	中国_四川省_中坝	240
1	112.192.106.153	中国_四川省_成都	175

利用pyrhon脚本对日志进行处理，并统计访问ip地址、访问请求、useragent内容，存入表格中，统计结果依次如下

ip	ipcounts	ip_guishudi
125.123.120.132	47380	中国_浙江省_嘉兴
123.157.144.99	38937	中国_浙江省_杭州
223.87.69.250	30115	中国_广东_深圳
139.206.155.244	24535	中国_四川省_中坝
223.87.69.4	23909	中国_广东_深圳
111.85.162.176	21909	中国_贵州_贵阳市
112.192.106.153	21226	中国_四川省_成都
27.219.43.106	21183	中国_山东省_青岛市
60.12.177.120	19733	中国_浙江省_杭州
222.89.70.117	17229	中国_河南_颍川

	urlcounts
[redacted]te.html	103115
[redacted]x/openid	102890
/ad[redacted]tlocalopenid	102520
/ad[redacted]dex/start?r=	101930
[redacted]dex/vote	101660
[redacted]ico	398
/[redacted].html?page=13	63
/[redacted].html?page=15	63
/[redacted].html?page=11	62
/[redacted].html?page=14	62

useragent	useragentcounts
Mozilla/5.0 (Linux; U; Android 4.4.2; zh-cn; GT-I9300 Build/JZO54K) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 Mobile Safari/534.30 MicroMessenger/5.2.380	511922
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36 MicroMessenger/7.0.9.501 NetType/WIFI MiniProgramEnv/Windows WindowsWechat	1237
Mozilla/5.0 (Linux; Android 10; V1990A Build/QP1A.190711.020; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/86.0.4240.99 XWEB/3209 MMWEBSDK/20220204 Mobile Safari/537.36 MMWEBID/7359 MicroMessenger/8.0.20.2100(0x28001455) Process/appbrand1 WeChat/arm64 Weixin NetType/WIFI Language/zh_CN ABI/arm64 miniProgram/wx9debbbb0cbbe18e8	45
Mozilla/5.0 (Linux; Android 12; 2106118C Build/SKQ1.211006.001; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/86.0.4240.99 XWEB/3209 MMWEBSDK/20220303 Mobile Safari/537.36 MMWEBID/7539 MicroMessenger/8.0.21.2120(0x2800153B) Process/appbrand1 WeChat/arm64 Weixin NetType/WIFI Language/zh_CN ABI/arm64 miniProgram/wx9debbbb0cbbe18e8	42
Mozilla/5.0 (Linux; Android 10; YAL-AL00 Build/HUAWEIYAL-AL00; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/86.0.4240.99 XWEB/3209 MMWEBSDK/20220303 Mobile Safari/537.36 MMWEBID/2402 MicroMessenger/8.0.21.2120(0x2800153F) Process/appbrand2 WeChat/arm64 Weixin NetType/4G Language/zh_CN ABI/arm64 miniProgram/wx9debbbb0cbbe18e8	41
Mozilla/5.0 (Linux; Android 10; V1831A Build/QP1A.190711.020; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/86.0.4240.99 XWEB/3209 MMWEBSDK/20220204 Mobile Safari/537.36 MMWEBID/7683 MicroMessenger/8.0.20.2100(0x28001455) Process/appbrand1 WeChat/arm64 Weixin NetType/WIFI Language/zh_CN ABI/arm64 miniProgram/wx9debbbb0cbbe18e8	27
Mozilla/5.0 (Linux; Android 9; OPPO R11s Build/PKQ1.190414.001; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/86.0.4240.99 XWEB/3208 MMWEBSDK/20220303 Mobile Safari/537.36 MMWEBID/6851 MicroMessenger/8.0.21.2120(0x2800153E) Process/toolsmp WeChat/arm32 Weixin NetType/WIFI Language/zh_CN ABI/arm64	11
Mozilla/5.0 (iPhone; CPU iPhone OS 13_6 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148 MicroMessenger/8.0.18(0x1800123f) NetType/WIFI Language/zh_CN miniProgram/wx9debbbb0cbbe18e8	10
Mozilla/5.0 (Linux; Android 10; LIO-AN00P Build/HUAWEILIO-AN00P; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/86.0.4240.99 XWEB/3209 MMWEBSDK/20220303 Mobile Safari/537.36 MMWEBID/7570 MicroMessenger/8.0.21.2120(0x2800153F) Process/appbrand1 WeChat/arm64 Weixin NetType/WIFI Language/zh_CN ABI/arm64 miniProgram/wx9debbbb0cbbe18e8	8
Mozilla/5.0 (Linux; Android 10; PDVM00 Build/QKQ1.200614.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/86.0.4240.99 XWEB/3209 MMWEBSDK/20220303 Mobile Safari/537.36 MMWEBID/7330 MicroMessenger/8.0.21.2120(0x2800153F) Process/appbrand1 WeChat/arm64 Weixin NetType/WIFI Language/zh_CN ABI/arm64 miniProgram/wx9debbbb0cbbe18e8	8

可根据日志分析的情况将，相关字段加到ngix配置的黑名单中。

2.2bash脚本防护

查看连接数量，将连接数量大于15的地址，加入到ngix配置文档

```
#!/bin/bash
for i in `/usr/bin/netstat -anptu |  awk  '{print $5}' | awk -F':' '{print $1}' | sort |uniq -c | awk '{if($1>=15){print}}' | awk '{print $2}'`
do
    echo $i | perl -ne 'exit 1 unless /\b(?:(?:(?:[01]?\d{1,2}|2[0-4]\d|25[0-5])\.){3}(?:[01]?\d{1,2}|2[0-4]\d|25[0-5]))\b/'
    if [[ $? -eq 0 ]];then
        echo $i | grep -w 0.0.0.0 &> /dev/null
        if [[ $? -ne 0 ]];then
            sed -i "53a deny $i;" /etc/nginx/nginx.conf
            echo "ip $i 加入到黑名单" >> /tmp/nginx-list.log
        fi
    fi
done
systemctl reload nginx
```

将ip地址添加到防火墙策略

```
备份iptables规则：iptables-save > iptables.bak
 清除iptables规则：iptables -F
 iptables配置文件：/etc/sysconfig/iptables
拒绝95.26.0.0 B段连接：
iptables -I INPUT -s 95.0.0.0/8 -j DROP
查看iptables：
iptables -L INPUT --line-numbers
iptables -L -n
iptables 保存：
service iptables save
删除规则：
iptables -D INPUT 11
```

也可利用bash脚本对netstat连接进行筛选，将ip地址批量加入到防火墙策略中，也可直接将ip加入边界出口安全设备中。

三、小结

通过修改配置文件或防火墙策略的措施并不能从根本上解决ddos攻击的问题，只能是在一定程度上缓解，但当流量很大时服务器可能来不及反应而造成系统死机。日志统计脚本已经上传到github：
https://github.com/tide-emergency/yingji/blob/master/%E5%BA%94%E6%80%A5%E5%93%8D%E5%BA%94%E4%B9%8B%E5%B7%A5%E5%85%B7%E7%AF%87/%E6%97%A5%E
https://github.com/tide-emergency/yingji/blob/master/%E5%BA%94%E6%80%A5%E5%93%8D%E5%BA%94%E4%B9%8B%E5%B7%A5%E5%85%B7%E7%AF%87/%E6%97%A5%E