手记 /后端开发

记一次真实的网站被DDOS攻击经历

2018.06.27 16:32 37549浏览

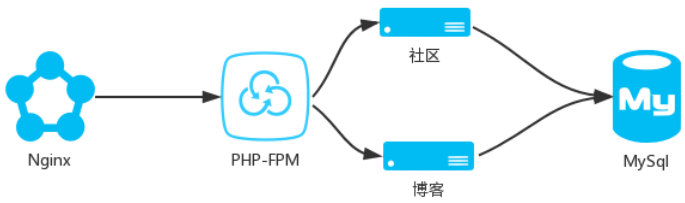
前言

距离上次被DDOS攻击已经有10天左右的时间，距离上上次已经记不起具体那一天了，每一次都这么不了了只。然而近期一次相对持久的攻击，我觉得有必要静下心来，分享一下被黑的那段经历。

在叙述经历之前，先简单的介绍一下服务器配置情况：

- ECS 1核2G内存1MB带宽，Linux系统
- RDS 2核240MB内存，最大连接数60
- Redis 256MB共享实例，搬家之后没用到
- CDN 按量付费，缓存小文件

以上配置，对于一个日访问量几千的网站来说应该绰绰有余了，并发撑死十几个左右，以下是简单的网站部署情况：



经历

前段时间听说过互联网大佬阮一峰博客被DDOS的经历，可谓是持久啊，最终被迫

难道我比阮大神长得帅？

好吧，故事开始，2018年6月14日，凌晨两点三十收到了阿里云系统告警通知，告知网站无法访问，然而那会我还在睡梦中。

跟往常一样，差不多六点左右醒来，习惯性的翻看手机，恰好此时又发来了短信告警。要在平时的话是可以再睡两个小时的，然而此时一个激灵，瞬间困意全无，怎么说我也是有几千访问量的博主了。

于是，赶紧爬起来打开电脑，尝试访问下博客和论坛，果不其然浏览器在一直打转转。

问题排查

尝试远程登录服务器：

- 查看Nginx 和 PHP-FPM，ps -ef|grep xxxx
- 查看系统剩余内存 free -m
- 查看CPU使用情况 top
- 查看Nginx错误日志 tail -f error.log
- 查看日志容量 ll -h
- 查看并发连接数 netstat -nat|grep ESTABLISHED|wc -l

一顿骚操作之后，并没有什么异常，内存和CPU平稳，Nginx和PHP 进程没问题。然后分别重启了一下 PHP 和 Nginx，开始网站还可以访问，进入社区首页就被卡死。

查看错误日志，后台使劲的刷日志，随便查看了几个IP，有印度的，美国的，菲律宾的等等，当然大多数还是国内的IP。一晚上的时间居然刷了上百兆日志(上次被D我清理过一次)，反正我觉得是不少了，对比网站平时的访问量来说。

之前有过几次攻击，但都是三三俩俩的过来，使用Nginx禁掉IP就是了。然而此次，显然不是禁掉IP可以解决问题的了，这么多IP收集是个问题(当然可以通过正则匹配获取)，还有可能造成误伤。

上班途中

然而上班才是正事，心思着一时半会解决不了问题，瞄了一眼错误日志，还在使劲

路上一路嘟念，心想是不是到了9点，他们准时下夜班然后就可以正常访问了，自我开解一下。

上班中

到了公司，第一件事当然是远程登录下服务器，看了一下，错误日志还在使劲刷。正常来说这个是时间点是不会有用户来访问的。

重启了服务多次，访问一下首页就被卡死，然后瞬间瘫痪，整个网站(社区+博客)都不能访问了。既然这样，还是老实上班，坐等攻击停止吧。

期间群里的小伙伴们问网站怎么了，打不开了椰？将近中午的时候，查看了一下错误日志，还有那么几个IP再尝试请求不同的地址，一瞅就不是什么好东西，果断deny了一下。话说，现在请求没那么多了，重启了一些Nginx 和 PHP 进程，访问首页还是卡死？真是怪了个蛋。

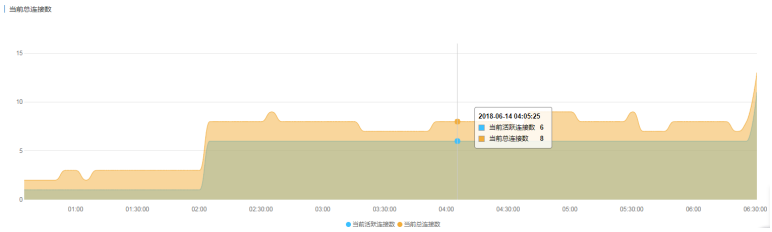
心想是不是RDS数据库的问题，查看了监控报警面板，CPU和内存利用率和当前总连接数都正常，没有什么异常，凌晨两点-六点左右的确有波动，但是不至于被D死。既然都登录了，要不顺便把 ECS 和 RDS 都重启了吧。

果然，重启一下居然神奇的好了，吃午饭的时候还用手机访问了一下，正常，可以安心吃饭了。

问题解决

其实，最终问题怎么解决的，我并不清楚，说几个比较疑惑的点：

- ECS 服务器 CPU 和内存也在正常阈值
- Nginx 和 PHP-FPM 进程都分别重启过
- RDS 数据库连接数尽管有所波动，但是并没有占满未释放
- 看错误日志请求都是来自上百个不同的IP，并且大多都是访问的社区URL
- 还有这些肉鸡为什么都是晚上？晚上便宜？还是说在西半球组织攻击
- 此次是有针对性的，还是随机的？但愿是随机的
- 中间停止过一次社区，博客是可以一直正常访问的，怀疑是首页数据库查询的问题，基于连接数应该不是这个问题，难道是Discuz的Bug？但是后来重启数据库后的确可以正常访问了。



其实阿里云有基础的DDOS防护，清洗触发值：

- 每秒请求流量：300M
- 每秒报文数量：70000

对于一般小站来说，是万万不可能达到300M的流量阈值的，博客的CDN峰值才3M而已。

所以说，这些小波流的攻击只能自身去默默承受，而机器配置不高，买不起带宽只能任攻击自由的撒欢，还不如直接关站，扔给他一个Nginx + 静态页面让它D去吧。

攻防策略

如果有人真D你的站点，你还真没有办法，当然我所说的群体是针对中小站长而言，你连DDOS基础防护的清洗阈值都达不到。

如果你只是一个默默无闻的小站，根本不需要想那么多。尽管现在DDOS成本很低，但谁不是无利不起早，除非你得罪了什么人。

当然对于一般的攻击我们也不能坐以待毙，这里总结了几个小技巧，分享给大家，反向代理使用的是openresty。

Nginx优化

Nginx号称最大并发5W，实际上对于中小站点来说几十或者上百个并发就不错了，最基本的参数就可以满足需求。但是为了安全期间，我们最好隐藏其版本号。

```
# 隐藏版本，防止已知漏洞被利用
server_tokens off; #在http 模块当中配置
```

PHP优化

在php渲染的网页header信息中，会包含php的版本号信息，比如: X-Powered-by: php/5.6.30，这有些不安全，有些黑客可能采用扫描的方式，批量寻找低版本的php服务器，利用php漏洞(比如hash冲突)来攻击服务器。

```
# 隐藏版本，防止已知漏洞被利用
php_admin_flag[expose_php] = off
```

IP黑名单

对付那种最low的攻击，加入黑名单的确是一个不错的选择，不然别人AB就能把你压死：

```
# 在Nginx的http模块添加以下配置即可
deny 61.136.197.xxx;
# 禁封IP段
deny 61.136.197.0/24;
```

IP日访问次数

限制单个IP的日访问次数，正常来说一个用户的访问深度很少超过10个，跳出率

内即可。

限制并发数

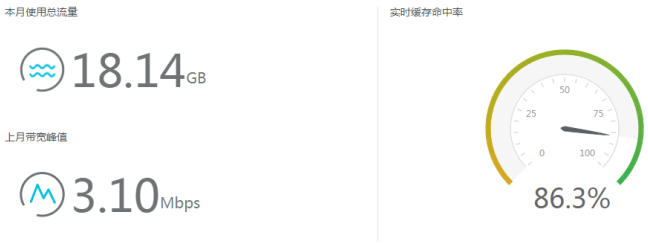
光限制访问次数还是不够的，攻击者可能瞬间涌入成百上千的请求，如果这些请求到后端服务，会打垮数据库服务的，所以我们还要基于我们自身网站访问情况设置并发数。

- 限制单个IP的并发数
- 限制总并发数

这里建议大家使用漏桶算法限流，来整形流量请求。

配置CDN

基于带宽以及正常用户访问速度的考量，建议配置CDN，以下是博客的流量使用情况，峰值3MB，对于我这1MB带宽的服务器肯定是抗不住啊，况且还有社区的访问。



配置缓存

数据库资源是宝贵的，所以尽量不要让请求直达后端。其实搬家之前，博客和社区都是配置过redis缓存的。由于之前购买的Redis服务是专有网络，新账号无法连接，然后就作罢了。

看来这次，需要在空闲服务器上配置一把了，反正闲着也是闲着，能起一丢丢作用也是好的。

- 阿里云Redis加速Discuz论坛访问
- 阿里云Redis加速Typecho博客访问

总结

前面也说了，对于攻击，小站真的无解，能做好基础的防护就可以了。但是对于那些肉鸡们或者即将成为肉鸡的人来说：

- 软件漏洞一定要及时打补丁，时刻关注互联网相关动态。
- 黑客利用被入侵的路由器获取网络流量，从而控制大连肉鸡。
- 大多数肉鸡是没有安全意识的，并且被长期利用，经发现，不少是云服务商主机、托管服务器主机，被黑客利用漏洞控制。

- DDoS黑客攻击正在向产业化、平台服务化转变，如果有人想害你，一个按钮、几百块钱，就可以实现一整月的攻击，然后一首《凉凉》送给自己。

参考

各种限流脚本：从构建分布式秒杀系统聊聊限流特技

JAVA SpringBoot

13人点赞

7 评论

评论 共同学习，写下你的评论

7楼 **4447477**

免费DDOS,可测压自有服务器，最高可达100G-UDP：www.xddos.me

1 回复 2019.04.25

6楼 **慕仔3249856**

网站 服务器 ddos 防御 攻击 + Q 120-5210-169

```
1 网站 服务器 ddos 防御 攻击 + Q 120-5210-169
```

0 回复 2018.12.21

5楼 **慕仔3249856**

网站 服务器 ddos 防御 攻击 + Q 120-5210-169

0 回复 2018.11.15

展开查看剩余评论

相关文章推荐

记一次真实的网站被黑经历

相关课程

玩转算法与数据结构

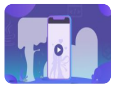
¥166 · 中级 · 8545

从0开始 独立完成企业级Ja...

¥348 · 中级 · 7696

2019版 微服务时代Spring ...

¥348 · 中级 · 4493



【告白神器】N种语言实现...

入门 · 3793

Java入门第一季

入门 · 999310

Java Web基础入门2018版

¥468 · 4步骤/21门课 · 716

记一次博客被群压的经历

1704 小柒2012 Nginx 02.15

怎样防御DDoS攻击

3 慕神8447489 Premiere 12.05

怎么检测网站是否有被人攻击的风险?

13 慕虎5022942 职场生活・深度学习・安全 06.24

记一次服务器被木马攻击以及排查，修复过程

3102 chokingwin PHP・云计算・测试 11.03

DDOS 攻击的防范教程 第1章

10 Mr杨001 JAVA 01.27

经历过DDOS的"洗礼"，你还好么

60 GavinHsueh Linux・架构・安全 05.24

一次Asp.NET小网站部署踩坑和解决经历

0 linux零基础学习视频 资讯 08.05

DDOS 攻击的防范教程 第2章

2 Mr杨001 JAVA 01.27

如果全球的沙子都对你发起DDoS攻击，如何破?

7 慕码人2005090 算法・安全 11.28

Swoole Go Django Python C++

C# ThinkPHP Spring MVVM PHP

零碎笔记：浏览器访问一个网站所经历的步骤

2631 Dunizb Node.js・JavaScript 10.08

谈谈我的第一次建站经历（阿里云）

4226 陈心似水 PHP・职场生活 05.18

用 JavaScript 对抗 DDOS 攻击

41 PIPIONE JavaScript・安全 04.17

浅谈 JavaScript DDoS 攻击原理与防御

5 一只斗牛犬 JavaScript 06.24

记一次面试腾讯的奇葩经历

10 黄小斜 职场生活 03.30

相关课程

玩转算法与数据结构

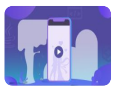
¥166・中级・8545

从0开始 独立完成企业级Ja...

¥348・中级・7696

2019版 微服务时代Spring ...

¥348・中级・4493



【告白神器】N种语言实现...

入门・3793

Java入门第一季

入门・999310

Java Web基础入门2018版

¥468・4步骤/21门课・716

13 12 收藏 共同学习，写下你的评论