链滴

使用 NGINX 流控和 fail2ban 防止 CC 攻击

作者：88250

原文链接：https://ld246.com/article/1486914848288

来源网站：链滴

背景知识

CC 攻击

攻击者通过创建大量请求导致服务器资源耗尽，主要针对特定服务接口，属于实现 DoS 攻击的一种式（DoS 攻击更多是针对网络端口，而不是具体服务接口）。

NGINX 流控

- limit_req_zone：通过“漏桶”算法限制每个 IP 发起的请求频率。
- limit_conn_zone：限制每个 IP 发起的连接数。

fail2ban

通过匹配服务器日志操作 iptables 来限制客户端网络连接。

实践配置

NGINX 部分

在 http 部分中配置：

```
limit_req_zone $binary_remote_addr zone=sym:10m rate=5r/s;
limit_conn_zone $binary_remote_addr zone=conn_sym:10m;
```

然后在需要流控的 location 部分配置：

```
limit_req zone=sym burst=5;
limit_conn conn_sym 10;
```

重启 NGINX 后当有超流客户端请求时将在 NGINX error.log（默认在 /var/log/nginx/error.log）看到类似记录：

```
2017/02/12 18:03:57 [error]15965#15965: *61240 limiting requests, excess: 6.000 by zone "sy
", client: 121.41.106.121, server: hacpai.com, request: "GET / HTTP/1.0", host: "hacpai.com"
```

此时请求已经被 NGINX 限流，但是客户端仍然能够继续发送请求，占用服务器资源。

fail2ban 部分

新建 /etc/fail2ban/jail.d/sym.conf 文件，加入如下内容：

```
[sym-cc]
enabled  = true
port     = https,http
filter   = sym
logpath  = /var/log/nginx/*error.log
maxretry = 120
findtime = 60
```

```
bantime  = 120
action   = iptables-multiport[name=Sym, port="https,http", protocol=tcp]
           sendmail-whois-lines[name=Sym, dest=youremail@gmail.com]
```

findtime 60 秒内如果有超过 maxretry 120 次匹配到则禁止连接 bantime 120 秒。禁止连接通过操 iptables 实现 。（要发送邮件，需要安装配置好 sendmail）

重启 fail2ban 后当发生超流时可以在 /var/log/fail2ban.log 中看到类似记录：

2017-02-12 18:01:26,968 fail2ban.actions: WARNING [sym-cc] Ban 121.41.106.121

另外：

- fail2ban-client status、fail2ban-client status sym-cc 可以查看当前禁止信息
- fail2ban-regex /var/log/nginx/error.log /etc/fail2ban/filter.d/sym.conf 可以查看配置匹配情

。

注意事项

fail2ban

- 服务重启可能较慢，耐心等待
- findtime 不要小于 60 秒
- action 用 iptables-multiport 同时设置 HTTPS 和 HTTP
- 可能需要自己手动加入操作系统启动项

如果 NGINX 开了 access_log，其实也可以简单粗暴一点直接将 fail2ban 配置到访问日志上，这样不用配置 NGINX 流控模块了，不过缺点是失去了“弹性”。

NGINX

上面提到的 NGINX 流控模块的“弹性”主要指的是 limit_req_zone 模块中 burst 和 nodelay 两个数的组合使用。

- rate：按照固定速率“漏请求”给后端服务器
- burst：可理解为桶大小，能装多少个请求
- nodelay：带了这个参数的话在桶装不下时将请求“全部倒给”后端服务器；如果不带的话请求还按照速率慢慢漏

日志清理

需要定时清理 NGINX、fail2ban 日志，防止磁盘空间占用过大。

参考

- CC 攻击
- DoS 攻击

- Module ngx_http_limit_req_module
- Module ngx_http_limit_conn_module
- fail2ban

原文链接：使用 NGINX 流控和 fail2ban 防止 CC 攻击