DDOS на WEB сервер

Утро началось не с кофе. Просматривая логи, обнаружил, что на web сервере аномальная нагрузка. Причем, ping еще шел, а по ssh я уже не мог достучаться. Соответственно все сайты лежали. Идем на шлюз и смотрим кто мешает.

GATE

```
# tcpdump -i bge0 host 19x.xxx.xxx.xx4


....
10:58:29.348293 IP site.com.ua.49864 > 130.0.237.242.https: Flags [S], seq 142297589, win 29200, options [mss 1460,sackOK,TS val 95348608 ecr 0,nop,wscale 7], length 0
10:58:29.348303 IP site.com.ua.49888 > 130.0.237.242.https: Flags [S], seq 3563334456, win 29200, options [mss 1460,sackOK,TS val 95348608 ecr 0,nop,wscale 7], length 0
10:58:29.348313 IP site.com.ua.49880 > 130.0.237.242.https: Flags [S], seq 1828917869, win 29200, options [mss 1460,sackOK,TS val 95348608 ecr 0,nop,wscale 7], length 0
10:58:29.348324 IP site.com.ua.49878 > 130.0.237.242.https: Flags [S], seq 1635255414, win 29200, options [mss 1460,sackOK,TS val 95348608 ecr 0,nop,wscale 7], length 0
10:58:29.348333 IP site.com.ua.49876 > 130.0.237.242.https: Flags [S], seq 3432924249, win 29200, options [mss 1460,sackOK,TS val 95348608 ecr 0,nop,wscale 7], length 0
....
```

Здесь все понятно. Блокируем IP, сразу падает нагрузка, и идем подкручивать WEB сервер.

WEB SERVER NGINX

Здесь стоит nginx. Редактируем конфиг. В секции http {…} вставляем строку:

```
limit_req_zone $binary_remote_addr zone=one:10m rate=1r/s;
```

10m is size of zone. 1MB can hold 16000 states. I *think* this means 16000 unique IP addresses. In case you have way too many

sites or very high traffic sites, you may want to increase it to 20MB or 100MB.

1r/s means 1 request per second is allowed. You cannot specify fractions. If you want to slowdown further, means less requests per second try 30r/m which means 30 requests per min, effectively 1 request per 2 second.

```
location ~ \.php$ {
            limit_req   zone=one  burst=1 nodelay;
}
```

Limiting number of connections

You can limit the number of connections that can be opened by a single client IP address,

Here we tweak the ***limit_conn_zone*** and ***limit_conn*** directives to limit the number of connections per IP address.

```
limit_conn_zone $binary_remote_addr zone=two:1m;

server {
    location / {
        limit_conn two 10;
    }
}
```

Timeout parameters

Slow connections can represent an attempt to keep connections open for a long time. As a result, the server can’t accept new connections.

```
server {
    client_body_timeout 5s;
    client_header_timeout 5s;
}
```

WEB SERVER IPTABLES

Теперь подправим iptables, добавив вверх правила:

```
### DDOS PROTECTION ###
### 1: Limit connections per source IP ###
/sbin/iptables -A INPUT -p tcp -m connlimit --connlimit-above
111 -j REJECT --reject-with tcp-reset

### 2: Limit RST packets ###
/sbin/iptables -A INPUT -p tcp --tcp-flags RST RST -m limit --
limit 2/s --limit-burst 2 -j ACCEPT
/sbin/iptables -A INPUT -p tcp --tcp-flags RST RST -j DROP

### 3: Limit new TCP connections per second per source IP ###
/sbin/iptables -A INPUT -p tcp -m conntrack --ctstate NEW -m
limit --limit 60/s --limit-burst 20 -j ACCEPT
/sbin/iptables -A INPUT -p tcp -m conntrack --ctstate NEW -j
DROP
```

Block wp-login.php bruteforce attack

https://gist.github.com/mattia-beta/bd5b1c68e3d51db933181d8a3dc0ba64
https://inmediatum.com/en/blog/engineering/ddos-attacks-prevention-nginx/
https://cryptoworld.su/ddos-ataka-kak-ee-ustroit-i-zashhita-ot-nee/
https://mozgovoy.in.ua/centos-7/103-nastrojka-yadra-linux-dlya-tyazhelykh-proektov-i-zashchity-ot-ddos