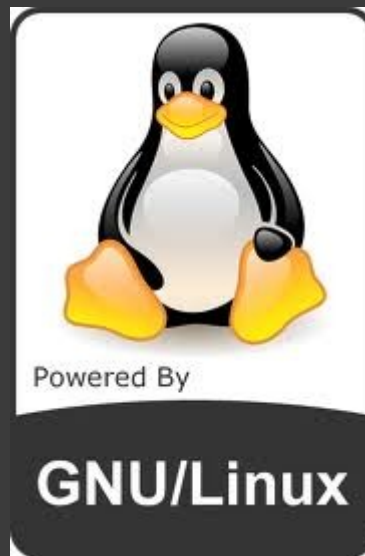


# DDOS MITIGATION SOFTWARE SOLUTIONS

## Организация программной защиты от DDoS-атак

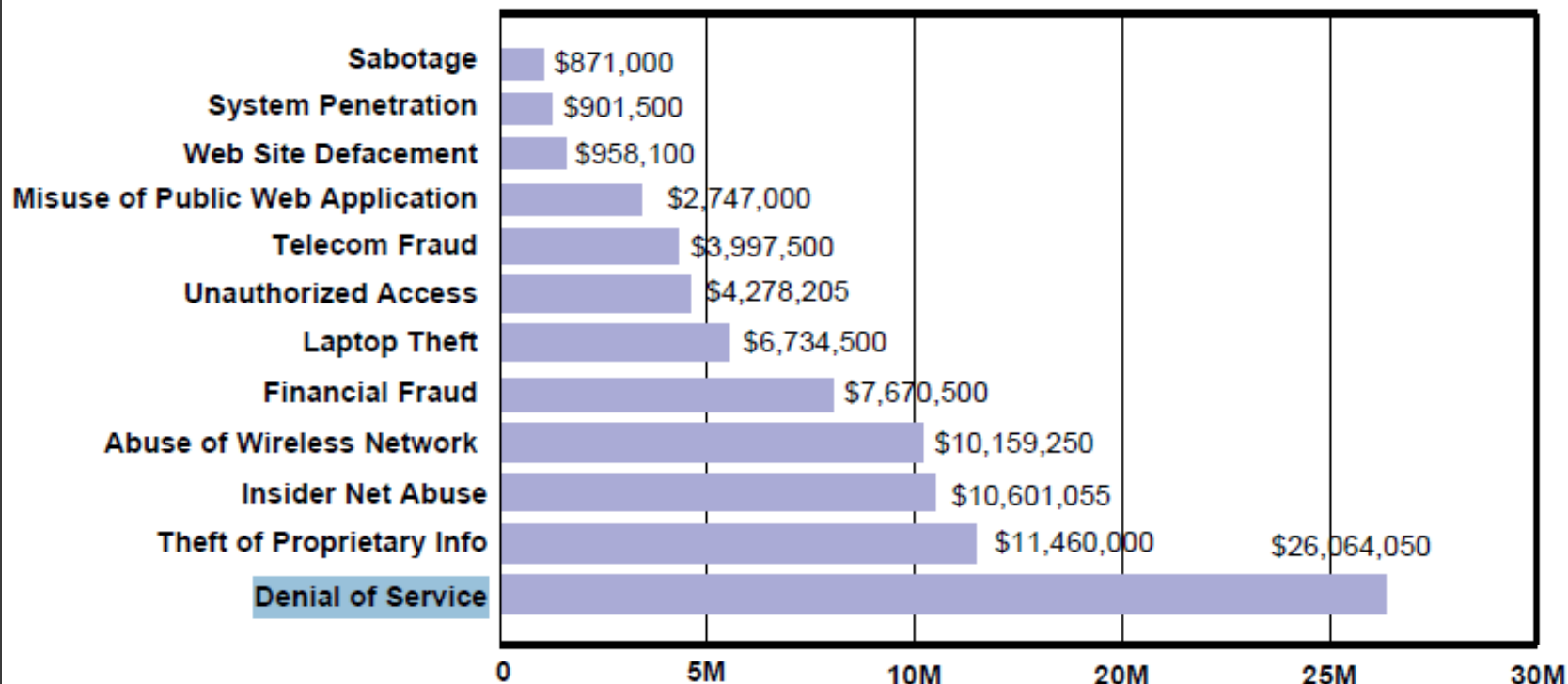


Олег Бойцев, [mega-admin.com](http://mega-admin.com)  
LVEE 2011

# Сравнительная оценка стоимости IT-угроз

## The Cost of Threats

### Dollar Amount of Loss by Type of Attack (CSI/FBI 2004 Survey)



2004 CSI/FBI Computer Crime and Security Survey  
Source: Computer Security Institute

**Total Losses for 2004—\$141,496,560**

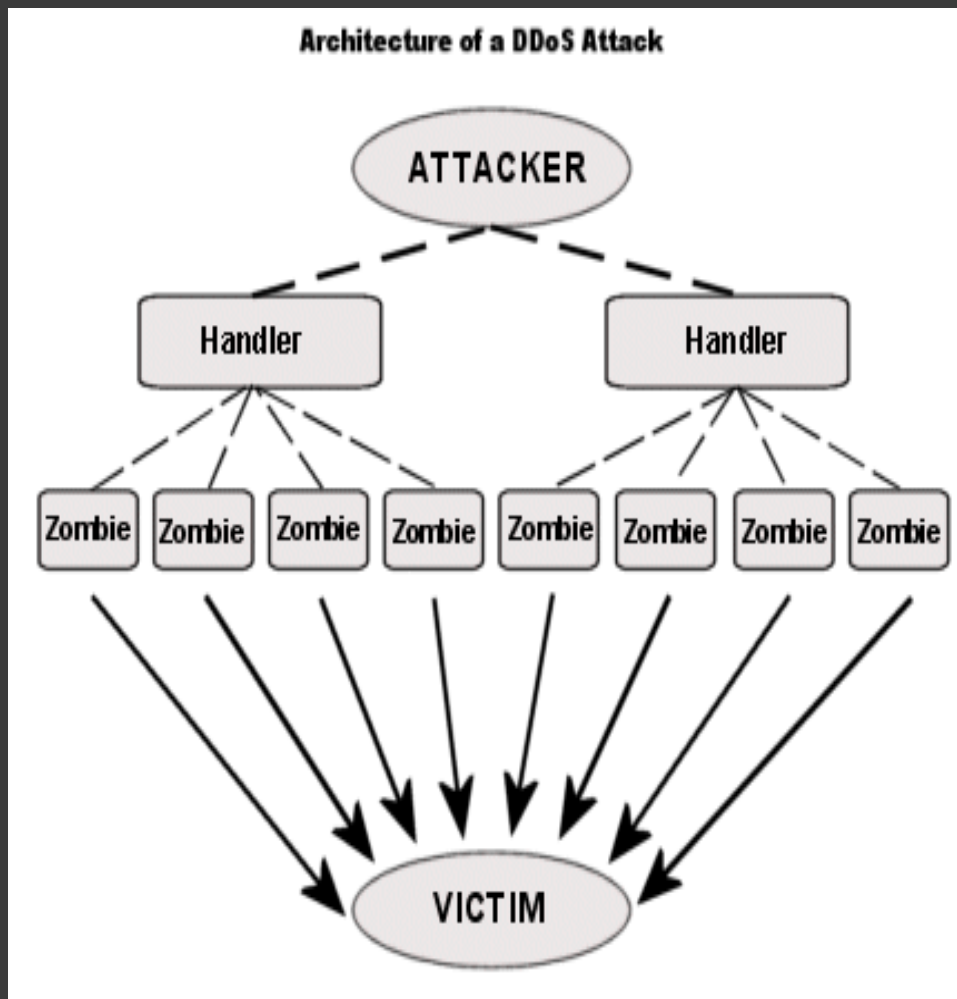
2004: 289 Respondents

Cisco DDoS Mitigation  
Enterprise Solutions

© 2005 Cisco Systems, Inc. All rights reserved.

MEGA-ADMIN.COM

## Что такое DDoS?



DDoS-атака (от англ. *Distributed Denial of Service*, *распределённая атака типа «отказ в обслуживании»*) — атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых легитимные (правомерные) пользователи системы не могут получить доступ к предоставляемым системой ресурсам, либо этот доступ затруднён.

## Виды DDoS-атак

**SYN-флуд** - при данном виде атаки на атакуемый узел направляется большое количество SYN-пакетов по протоколу TCP (запросов на открытие соединения). При этом на атакуемом сервере через некоторое время исчерпывается количество свободных сокетов и сервер перестаёт отвечать.

▪ **HTTP-флуд** - в случае HTTP-флуда в рамках уже установленного TCP-соединения к серверу происходят множественные обращения, как простейшее GET /, так и более сложные наподобие GET /index.php?search=<oooooooooooooogle>, приводящие, как правило, к исчерпанию системных ресурсов.

▪ **UDP-флуд** - этот тип флуда предназначен прежде всего для затопления канала связи.

▪ **ICMP-флуд** - то же, но с помощью ICMP-пакетов.

▪ Другие виды DDoS (Distributed Reflection Attack, DNS Amplification Attack, Smurf, Slowloris, JavaScript DDoS)

# SYN-флуд

```
root@u1 /home/exorcist - PuTTY
[root@u1 /home/exorcist]# netstat -an|awk '/tcp/ {print $6}'|sort|uniq -c
  4 CLOSED
  1 CLOSE_WAIT
 394 ESTABLISHED
2433 FIN_WAIT_1
 568 FIN_WAIT_2
 269 LAST_ACK
  26 LISTEN
1441 SYN_RCVD
 501 TIME_WAIT
[root@u1 /home/exorcist]#
```

MEGA-ADMIN.COM

# HTTP-флуд

```
85.107.214.237 - - [23/Dec/2010:15:28:11 +0300] "POST / HTTP/1.0" 200 6681 "http://fomenko.ru" "Mozilla/5.0 (Windows; U; Windows NT 5.1; ru; rv:1.9.0.2) Gecko/2008091620 Firefox/3.0.2"
41.232.78.226 - - [23/Dec/2010:15:28:11 +0300] "POST / HTTP/1.0" 200 6681 "http://gazeta.ru" "Mozilla/5.0 (Windows; U; Windows NT 5.1; ru; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0.3 (.NET CLR 3.5.30729)"
180.190.148.204 - - [23/Dec/2010:15:28:11 +0300] "POST / HTTP/1.0" 408 0 "http://gismeteo.ru" "Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US) AppleWebKit/532.5 (KHTML, like Gecko) Chrome/4.0.249.89 Safari/532.5"
109.251.97.229 - - [23/Dec/2010:15:28:11 +0300] "POST / HTTP/1.0" 200 6681 "http://yahoo.com" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1) Gecko/20090624 Firefox/3.5"
200.215.222.201 - - [23/Dec/2010:15:28:11 +0300] "POST / HTTP/1.1" 200 6681 "http://google.com" "Mozilla/5.0 (Windows; U; Windows NT 5.1; ru; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0.3"
178.93.67.247 - - [23/Dec/2010:15:28:11 +0300] "POST / HTTP/1.0" 200 6681 "http://yandex.ru" "Mozilla/4.0 (compatible; MSIE 6.0; Nitro) Opera 8.50 [it]"
93.74.58.138 - - [23/Dec/2010:15:28:11 +0300] "POST / HTTP/1.0" 200 6681 "http://fomenko.ru" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.7.9) Gecko/20050711 Firefox/1.0.5"
81.90.234.87 - - [23/Dec/2010:15:28:11 +0300] "POST / HTTP/1.0" 200 6681 "http://referat.ru" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US)"
123.49.61.120 - - [23/Dec/2010:15:28:11 +0300] "POST / HTTP/1.0" 200 6681 "http://lenta.ru" "Mozilla/5.0 (Windows; U; Windows NT 5.1; ru; rv:1.9.0.7) Gecko/2009021910 Firefox/3.0.7"
115.87.141.67 - - [23/Dec/2010:15:28:11 +0300] "POST / HTTP/1.0" 200 6681 "http://gismeteo.ru" "Mozilla/4.0 (compatible; MSIE 6.0; Nitro) Opera 8.50 [es-es]"
195.238.117.35 - - [23/Dec/2010:15:28:11 +0300] "POST / HTTP/1.0" 200 6681 "http://subscribe.ru" "Mozilla/2.0 (compatible; MSIE 3.01; Windows 98)"
^C
[root@u1 /home/exorcist/DDoS]#
```

# Прогрузка апачем процессора при сильном HTTP-флуде

```
exorcist@d23: ~ MEGA-ADMIN.COM
```

1 [||||||||||||||||||||||||||||||||| 100.0%]  
2 [||||||||||||||||||||||||||||||||| 100.0%]  
3 [||||||||||||||||||||||||||||||||| 100.0%]  
4 [||||||||||||||||||||||||||||||||| 100.0%]  
Mem [||||||||||||||||||||||||||||| 3467/12011MB]  
Swp [||||||||||||||||||||||||| 0/12013MB]

Tasks: 223 total, 151 running  
Load average: 150.18 131.34 73.90  
Uptime: 8 days, 04:34:54

PID	USER	PRI	NI	VIRT	RES	SHR	S	CPU%	MEM%	TIME+	Command
12569	www-data	20	0	248M	56580	3872	R	3.0	0.5	0:16.58	/usr/sbin/apache2
12559	www-data	20	0	244M	52912	3900	R	3.0	0.4	0:17.19	/usr/sbin/apache2
12489	www-data	20	0	245M	53536	3872	R	2.0	0.4	0:18.41	/usr/sbin/apache2
12574	www-data	20	0	245M	53860	3984	R	2.0	0.4	0:16.39	/usr/sbin/apache2
12469	www-data	20	0	246M	55148	4376	R	2.0	0.4	0:20.50	/usr/sbin/apache2
12558	www-data	20	0	244M	52468	3792	R	2.0	0.4	0:17.03	/usr/sbin/apache2
12502	www-data	20	0	246M	54360	3780	R	2.0	0.4	0:18.21	/usr/sbin/apache2
12540	www-data	20	0	244M	53248	3952	R	2.0	0.4	0:17.48	/usr/sbin/apache2
12423	www-data	20	0	250M	59024	4392	R	2.0	0.5	0:35.78	/usr/sbin/apache2
12438	www-data	20	0	245M	53708	4004	R	2.0	0.4	0:24.33	/usr/sbin/apache2
12565	www-data	20	0	246M	54680	4000	R	2.0	0.4	0:17.08	/usr/sbin/apache2
12647	www-data	20	0	245M	53604	3840	R	2.0	0.4	0:15.72	/usr/sbin/apache2
12487	www-data	20	0	245M	53804	3928	R	2.0	0.4	0:18.33	/usr/sbin/apache2
12534	www-data	20	0	242M	50168	3572	R	2.0	0.4	0:17.65	/usr/sbin/apache2
12639	www-data	20	0	245M	54060	3976	R	2.0	0.4	0:15.80	/usr/sbin/apache2
12552	www-data	20	0	244M	52800	3712	R	2.0	0.4	0:17.30	/usr/sbin/apache2
12511	www-data	20	0	241M	49284	3228	R	2.0	0.4	0:17.80	/usr/sbin/apache2
12467	www-data	20	0	244M	53048	3940	R	2.0	0.4	0:20.67	/usr/sbin/apache2
12566	www-data	20	0	245M	54204	3916	R	2.0	0.4	0:17.10	/usr/sbin/apache2
12447	www-data	20	0	246M	54984	3920	R	2.0	0.4	0:21.46	/usr/sbin/apache2
12477	www-data	20	0	245M	53400	4224	R	2.0	0.4	0:20.17	/usr/sbin/apache2
12507	www-data	20	0	246M	54676	3864	R	2.0	0.4	0:18.08	/usr/sbin/apache2
12527	www-data	20	0	242M	49420	3192	R	2.0	0.4	0:17.60	/usr/sbin/apache2
12533	www-data	20	0	244M	52448	3948	R	2.0	0.4	0:17.60	/usr/sbin/apache2
12536	www-data	20	0	245M	54020	4360	R	2.0	0.4	0:17.55	/usr/sbin/apache2

F1 Help F2 Setup F3 Search F4 Invert F5 Tree F6 SortBy F7 Nice -F8 Nice +F9 Kill F10 Quit





# UDP-флуд Counter-Strike сервера

```
21:57:03.185076 IP 134.159.131.65.27005 > 212.67.2.74.27016: UDP, length 1
21:57:03.185080 IP 78.151.151.63.27005 > 212.67.2.74.27016: UDP, length 1
21:57:03.185085 IP 184.36.201.120.27005 > 212.67.2.74.27016: UDP, length 1
21:57:03.185089 IP 31.175.236.134.27005 > 212.67.2.74.27016: UDP, length 1
21:57:03.185094 IP 16.101.63.130.27005 > 212.67.2.74.27016: UDP, length 1
21:57:03.185098 IP 120.131.52.85.27005 > 212.67.2.74.27016: UDP, length 1
21:57:03.185103 IP 78.32.120.249.27005 > 212.67.2.74.27016: UDP, length 1
21:57:03.185107 IP 206.137.242.16.27005 > 212.67.2.74.27016: UDP, length 1
21:57:03.185112 IP 78.32.251.75.27005 > 212.67.2.74.27016: UDP, length 1
21:57:03.185121 IP 219.63.200.27.27005 > 212.67.2.74.27016: UDP, length 1
21:57:03.185125 IP 145.130.51.134.27005 > 212.67.2.74.27016: UDP, length 1
21:57:03.185130 IP 212.3.85.36.27005 > 212.67.2.74.27016: UDP, length 1
21:57:03.185139 IP 31.174.164.168.27005 > 212.67.2.74.27016: UDP, length 1
21:57:03.185229 IP 178.35.73.139.27005 > 212.67.2.74.27016: UDP, length 1
21:57:03.185245 IP 33.194.145.131.27005 > 212.67.2.74.27016: UDP, length 1
21:57:03.185261 IP 35.122.21.16.27005 > 212.67.2.74.27016: UDP, length 1
21:57:03.185277 IP 201.61.212.20.27005 > 212.67.2.74.27016: UDP, length 1
```

# Инструменты для проведения DDoS-атак



Следующий материал приводится исключительно в образовательных целях

# Панель управления Black Energy Botnet

total bot's: 0  
bot's per hour: 0  
bot's per day: 0  
bot's for all time: 0

## Control bots

### Flooders options

ICMP flooder

freq:

packetsize:

SYN flooder

freq:

HTTP-GET flooder

freq:

threads:

UDP and TCP/UDP data flooders

UDP/TCP freq:

UDP size:

TCP size:

### Advanced SYN and ICMP options

spoof sender IP:

attack mode:  ▼

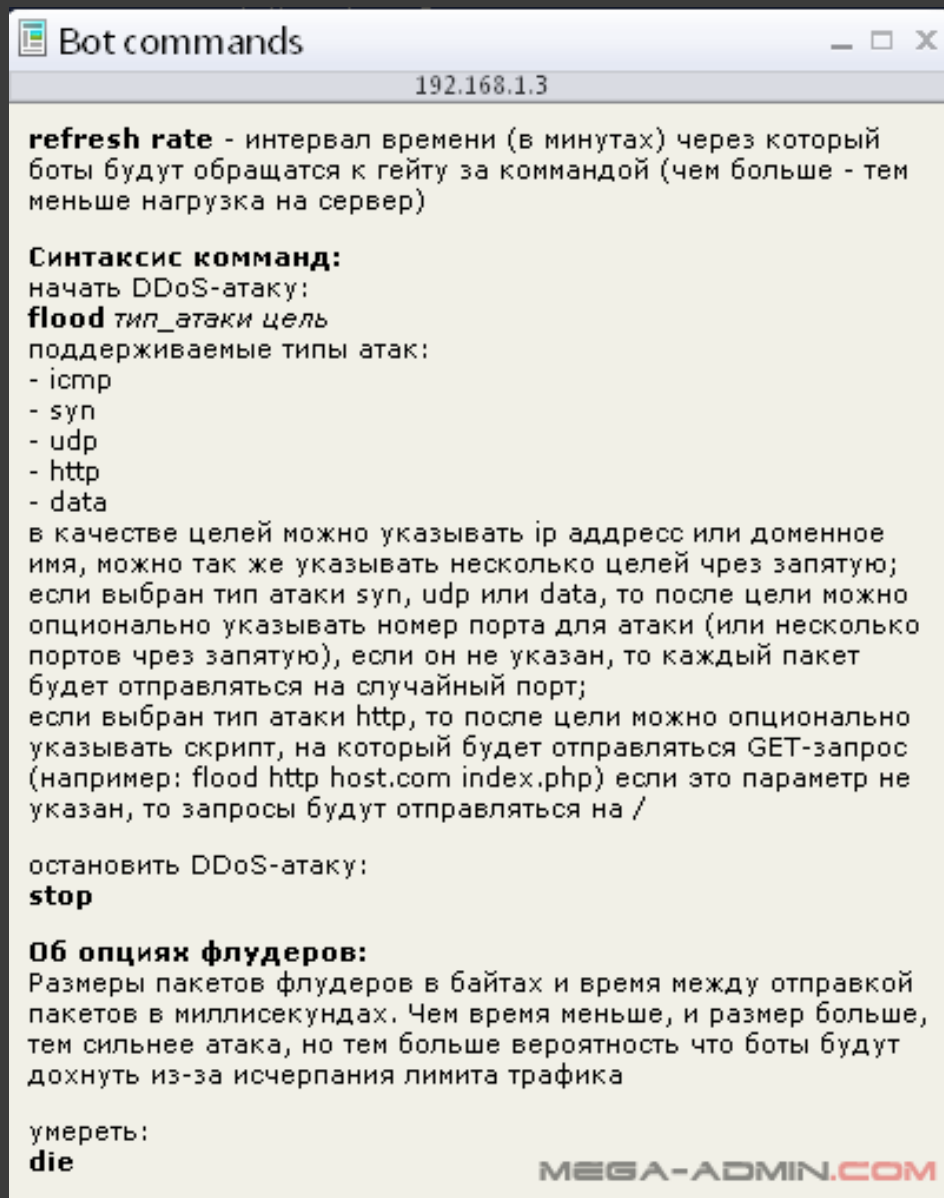
max sessions:  (for 'drop by timeout')

### Command

[ help ]

refresh rate:  (in minutes)

# Команды управления ботнетом



**refresh rate** - интервал времени (в минутах) через который боты будут обращаться к гейту за командой (чем больше - тем меньше нагрузка на сервер)

**Синтаксис команд:**  
начать DDoS-атаку:  
**flood** *тип\_атаки цель*  
поддерживаемые типы атак:  
- icmp  
- syn  
- udp  
- http  
- data

в качестве целей можно указывать ip адресс или доменное имя, можно так же указывать несколько целей чрез запятую; если выбран тип атаки syn, udp или data, то после цели можно опционально указывать номер порта для атаки (или несколько портов чрез запятую), если он не указан, то каждый пакет будет отправляться на случайный порт;  
если выбран тип атаки http, то после цели можно опционально указывать скрипт, на который будет отправляться GET-запрос (например: flood http host.com index.php) если это параметр не указан, то запросы будут отправляться на /

остановить DDoS-атаку:  
**stop**

**Об опциях флудеров:**  
Размеры пакетов флудеров в байтах и время между отправкой пакетов в миллисекундах. Чем время меньше, и размер больше, тем сильнее атака, но тем больше вероятность что боты будутдохнуть из-за исчерпания лимита трафика

умереть:  
**die**

MEGA-ADMIN.COM

# МОДЕЛЬ МНОГОУРОВНЕВОЙ ЗАЩИТЫ ОТ DDOS-АТАК

**Firewall**

**Linux  
kernel**

**Скрипты**

**NGINX**

**Apache**

Олег Бойцев, mega-admin.com  
LVEE 2011



# IPTABLES

Устанавливаем лимит на количество новых соединений с одного IP в единицу времени

```
iptables -A INPUT -p tcp -m hashlimit --hashlimit-upto 1/sec --  
hashlimit-burst 3 --hashlimit-mode srcip --hashlimit-name  
HTTPD_DOS -m tcp --dport 80 -m state --state NEW -j ACCEPT
```

Режем ботов с “неправильным” UserAgent

```
iptables -I INPUT 1 -p tcp --dport 80 -m string --string  
"America Online Browser" --algo kmp -j DROP
```

# IPTABLES

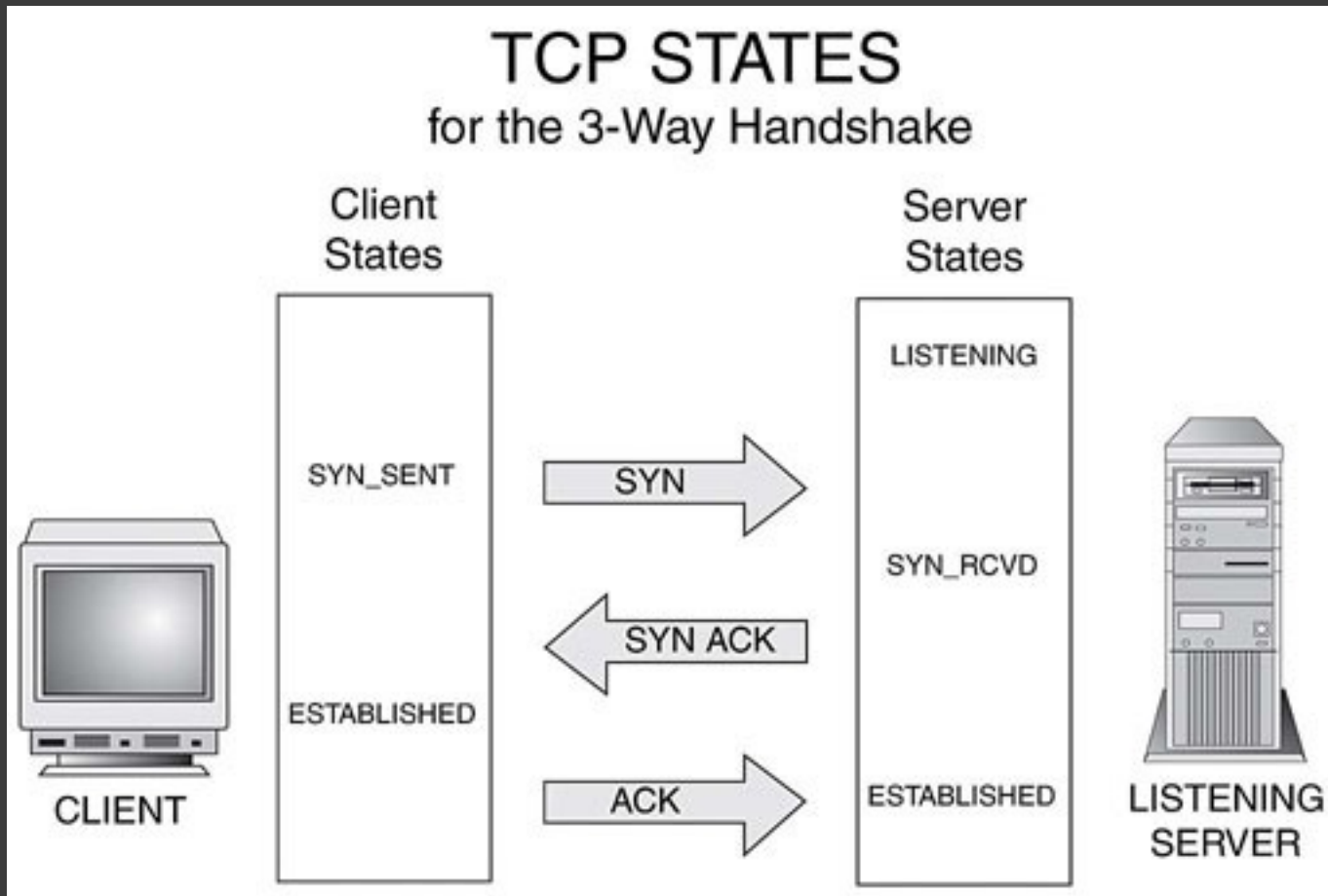
Режем входящий icmp

```
iptables -I INPUT -p icmp -j DROP --icmp-type 8
```

Ограничиваем udp-флуд

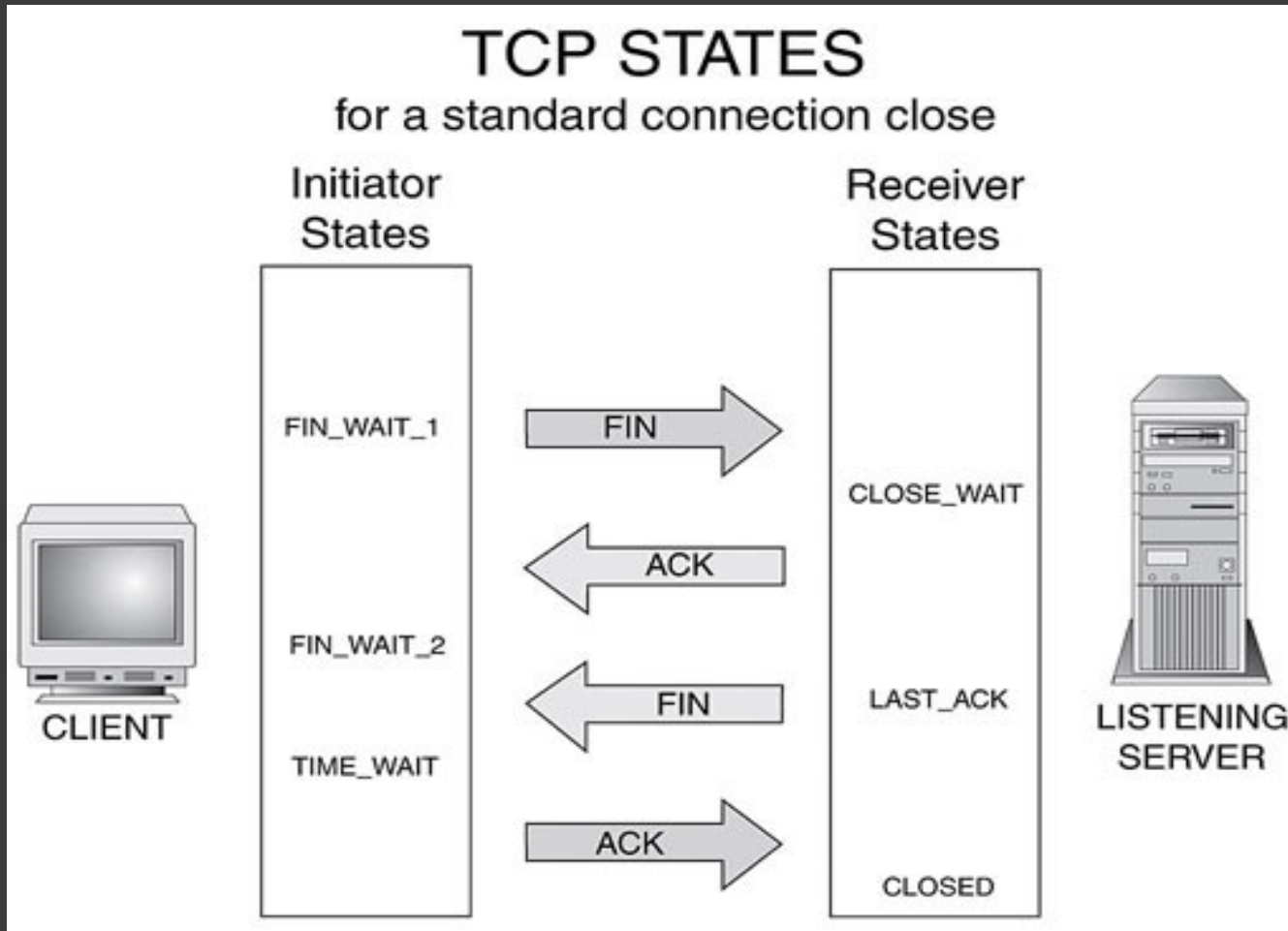
```
iptables -I INPUT -p udp --dport 53 -j DROP -m connlimit  
--connlimit-above 1
```

# TCP OPENING





# TCP CLOSING

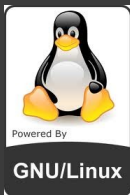


# LINUX KERNEL

```
net.ipv4.tcp_syncookies = 1
net.ipv4.tcp_max_syn_backlog = 4096
net.ipv4.tcp_synack_retries = 1
net.ipv4.tcp_keepalive_time = 60
net.ipv4.tcp_keepalive_intvl = 10
net.ipv4.tcp_keepalive_probes = 5
net.ipv4.tcp_fin_timeout = 7
net.ipv4.netfilter.ip_conntrack_max = 65536
net.ipv4.netfilter.ip_conntrack_tcp_timeout_close = 10
net.ipv4.netfilter.ip_conntrack_tcp_timeout_time_wait = 30
net.ipv4.netfilter.ip_conntrack_tcp_timeout_last_ack = 30
net.ipv4.netfilter.ip_conntrack_tcp_timeout_close_wait = 30
net.ipv4.netfilter.ip_conntrack_tcp_timeout_fin_wait = 60
net.ipv4.netfilter.ip_conntrack_tcp_timeout_established = 30
net.ipv4.netfilter.ip_conntrack_tcp_timeout_syn_recv = 30
net.ipv4.netfilter.ip_conntrack_tcp_timeout_syn_sent = 30
```

**\*Подробно см. приложение**

Олег Бойцев, mega-admin.com  
LVEE 2011



# БАН-СКРИПТ

```
#!/bin/sh
counter=1
reqno=0
for i in `netstat -nap|grep 'SYN_RECV'|awk '{print $5}'|cut -d ':' -f 1|
sort|uniq -c|sort -gr|head`
do
if [ `expr $counter % 2` -ne 0 ]
then
reqno=$i
else
if [ $reqno -gt 4 ]
then route add $i reject
fi
fi
counter=`expr $counter + 1`
done
```

# NGINX

## Общий тюнинг

```
# Увеличиваем максимальное количество используемых файлов
worker_rlimit_nofile 80000;
events {
# Увеличиваем максимальное количество возможных
соединений
    worker_connections 65536;
}
http {
# Отключаем таймаут на закрытие keep-alive соединений
keepalive_timeout 0;
# Не отдаем версию nginx в заголовке ответа
server_tokens off;
# Сбрасываем полужакрытое соединение
reset_timedout_connection on;
```

# NGINX

**Задаем лимит на количество одновременных соединений  
с одного IP-адреса:**

```
http {
    include      /usr/local/etc/nginx/mime.types;
    default_type application/octet-stream;
    access_log   /var/log/nginx/access.log;

    server_tokens off;
    log_format IP '$remote_addr';
    reset_timedout_connection on;

    limit_zone one $binary_remote_addr 10m;
    ...
    location / {
        limit_conn one 3;
    }
    ...
```

# АРАСНЕ

## Общий тюнинг

```
# Уменьшаем таймауты на обработку соединений  
Timeout 9 (default value is 300!)  
KeepAliveTimeout 9 (default value is 15)
```

# APACHE

Ставим **mod\_evasive** - Apache модуль для организации защиты от DDoS-атак:

```
cd /usr/local/src/  
wget http://www.zdziarski.com/blog/wp-  
content/uploads/2010/02/mod_evasive_1.10.1.tar.gz  
tar -xzvf mod_evasive_1.10.1.tar.gz  
cd mod_evasive/  
apxs2 -c -i -a mod_evasive20.c  
cd /etc/apache2/mods-available/  
nano evasive20.load  
LoadModule evasive20_module  
/usr/lib/apache2/modules/mod_evasive20.so  
nano evasive20.conf  
a2enmod  
apachectl configtest && /etc/init.d/apache2 restart
```

Олег Бойцев, mega-admin.com  
LVEE 2011



# APACHE

## Рабочий пример конфигурации mod-evasive:

```
<IfModule mod_evasive20.c>  
DOSHashTableSize 3097  
DOSPageCount 2  
DOSSiteCount 100  
DOSPageInterval 1  
DOSSiteInterval 1  
DOSBlockingPeriod 5  
DOSWhiteList 8.8.8.8  
</IfModule>
```



# APACHE

## Параметры mod\_evasive

**DOSHashTableSize** is the size of the hash table that is created for the IP addresses monitored.

**DOSPageCount** is the number of pages allowed to be loaded for the DOSPageInterval setting. In our case, 2 pages per 1 second before the IP gets flagged.

**DOSSiteCount** is the number of objects (ie: images, style sheets, javascripts, SSI, etc) allowed to be accessed in the DOSSiteInterval second. In our case, 50 objects per 1 second.

**DOSPageInterval** is the number of seconds the intervals are set for DOSPageCount

**DOSSiteInterval** is the number of seconds the intervals are set for DOSSiteCount

**DOSBlockingPeriod** is the number of seconds the IP address will receive the Error 403 (Forbidden) page when they have been flagged.

# Спасибо за внимание!

Олег Бойцев, mega-admin.com  
LVEE 2011



# ЛИТЕРАТУРА

<http://www.xakep.ru/post/16071/default.asp>

<http://forum.antichat.ru/showthread.php?t=10918>

<http://ha.ckers.org/blog/20090617/slowloris-http-dos/>

<http://www.xakep.ru/post/49752/default.asp?print=true>

[http://sysoev.ru/nginx/docs/http/nginx\\_http\\_limit\\_zone\\_module.html](http://sysoev.ru/nginx/docs/http/nginx_http_limit_zone_module.html)

[http://httpd.apache.org/docs/2.3/misc/security\\_tips.html](http://httpd.apache.org/docs/2.3/misc/security_tips.html)

<http://www.watchguard.com/infocenter/editorial/41649.asp>

# Приложение

## Список полезных команд

#Общее количество соединений  
`cat /proc/net/ip_contrack | wc -l`

#Количество SYN\_RECV сокетов  
`netstat -an | grep SYN_RECV | wc -l`

#С каких IP сколько запросов:  
`netstat -ntu | awk '{print $5}' | cut -d: -f1 | sort | uniq -c | sort -nr | more`

#Количество апаче-процессов в системе  
`ps waX | grep apache | wc -l`

# Приложение

## AntiDDoS kernel tuning with sysctl\*

```
net.ipv4.tcp_keepalive_time = 60
net.ipv4.tcp_keepalive_intvl = 10
net.ipv4.tcp_keepalive_probes = 5
net.ipv4.tcp_syncookies = 1
net.ipv4.tcp_max_syn_backlog = 4096
net.ipv4.tcp_synack_retries = 1
net.ipv4.tcp_fin_timeout = 7
net.ipv4.netfilter.ip_conntrack_max = 65536
net.ipv4.netfilter.ip_conntrack_tcp_timeout_close = 10
net.ipv4.netfilter.ip_conntrack_tcp_timeout_time_wait = 30
net.ipv4.netfilter.ip_conntrack_tcp_timeout_last_ack = 30
net.ipv4.netfilter.ip_conntrack_tcp_timeout_close_wait = 30
net.ipv4.netfilter.ip_conntrack_tcp_timeout_fin_wait = 60
net.ipv4.netfilter.ip_conntrack_tcp_timeout_established = 30
net.ipv4.netfilter.ip_conntrack_tcp_timeout_syn_rcv = 30
net.ipv4.netfilter.ip_conntrack_tcp_timeout_syn_sent = 30
net.core.rmem_max = 996777216
net.core.wmem_max = 996777216
net.ipv4.tcp_rmem = 4096 87380 4194304
net.ipv4.tcp_mem = 786432 1048576 996777216
net.ipv4.tcp_wmem = 4096 87380 4194304
net.ipv4.tcp_max_orphans = 2255360
net.core.netdev_max_backlog = 10000
kernel.msgmnb = 65536
kernel.msgmax = 65536
kernel.shmmax = 494967295
kernel.shmall = 268435456
net.core.somaxconn = 16096
net.ipv4.tcp_sack = 0
net.ipv4.tcp_timestamps = 0
net.ipv4.tcp_window_scaling = 0
```

\*Приведенные параметры могут быть изменены целесообразно в случае DDoS

# The Joy of Tech

by Nitrozac & Snaggy

