IPSet: простая блокировка DDOS по списку

Чтобы заблокировать небольшой DDOS - можно воспользоваться iptables. Добавлять много IP в iptables не вариант, т.к. чем больше правил в цепочках - тем больше нагрузка на CPU хоста. Лучше использовать довольно простой способ: берем список атакующих IP-адресов из файла, добавляем в список ipset и блокируем при помощи IPTables.

Если атака серьезная - данный способ не подойдет, нужно уходить под защиту компаний, специализирующихся на данной услуге. Просто по той причине что ваш хостер получит забитые входящие каналы и отключит ваши IP для уменьшения нагрузки на других клиентов.

```
ipset -N DDOS iphash
xargs < ddos-addresses.txt -n 1 ipset -A DDOS
iptables -A INPUT -m set --match-set DDOS dst -j DROP
```

Осталось периодически обновлять список (в зависимости от скорости атаки) и перечитывать адреса из файла.

Получить список адресов можно примерно так:

```
iftop -nNPt -L 5000 -s 1 1> iftop-log.txt 2>/dev/null
cat iftop-log.txt | grep ":22005" -A 1 | awk '{ print $1 }' | grep -x
'[0-9\.\:]\{9,25\}' | grep -Eo "[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+" > dump.txt
<code>

далее обрабатывал список  ip  адресов, убирая валидные адреса:

<code>
grep -Fvxf valid-addrs.txt dump.txt | uniq > ddos-addresses.txt
```

iptables, ipset, ddos, block ddos