

# Блокировка источников динамическим листом IP с UFW

Устанавливаем необходимые пакеты:

```
apt-get -y install ipset
```

Создаем блок лист:

```
ipset create "IP_ipsum4_block" hash:ip
```

Добавляем туда значения от общедоступных фидов IPsum (агрегационный фид level 4 - very low false positives) и сохраняем в файл `/etc/ipset.rules`:

```
ipset flush "IP_ipsum4_block"; for IP in $(wget -O -  
https://raw.githubusercontent.com/stamparm/ipsum/master/levels/4.txt); do ipset add "IP_ipsum4_block" $IP;  
done; ipset save > /etc/ipset.rules
```

Добавляем ежедневное обновление фидов с crontab (для редактирования планировщика:  
`crontab -e`):

```
0 0 * * * ipset flush "IP_ipsum4_block"; for IP in $(wget -O -  
https://raw.githubusercontent.com/stamparm/ipsum/master/levels/4.txt); do ipset add "IP_ipsum4_block" $IP;  
done; ipset save > /etc/ipset.rules
```

Для восстановления ipset при перезагрузке зайдите в CRON:

```
crontab -e
```

Добавьте запись и выйдите с сохранением:

```
@reboot ipset restore < /etc/ipset.rules; ufw reload
```

Далее добавим правило в UFW:

```
sudo nano /etc/ufw/before.rules
```

Добавьте следующее значение до COMMIT:

```
# block by ipsum4 src IPs  
-A ufw-before-input -m set --match-set IP_ipsum4_block src -j DROP
```

```
# allow MULTICAST UPnP for service discovery (be sure the MULTICAST line above  
# is uncommented)  
-A ufw-before-input -p udp -d 239.255.255.250 --dport 1900 -j ACCEPT  
# block by ipsum4 src IPs  
-A ufw-before-input -m set --match-set IP_ipsum4_block src -j DROP  
# don't delete the 'COMMIT' line or these rules won't be processed  
COMMIT
```

Перезапустите UFW:

```
sudo ufw reload
```

Убедитесь, что правило применяется (добавленная запись должна появиться в списке вывода):

```
sudo iptables -S ufw-before-input
```

---

Revision #3

Created 20 December 2024 10:57:54 by Boris RZR

Updated 19 March 2025 11:28:48 by Boris RZR