

Ограничение доступа/блокировка определенной страны

Две недели подряд брутили почтовый сервер на предмет подбора паролей от dovecot. Так как стоял fail2ban я не сильно заморачивался, но когда заблокированных IP перевалило за 50 тыс. я озаботился. Просмотрев внимательно логи я выяснил, что 99% IP принадлежат Малайзии. Погуглив я нашел [сервис](#) который предоставляет базы сетей по странам. Пишем скрипт для выборки малазийских сетей:

```
# cat grep_ip.sh
#!/bin/bash
# парсинг IP из скачанного файла для дальнейшего добавления в
iptables/ipfw
# дописать проверку скачанного файла
# если тот же - не работать с ним,
# если разные - старый удалить!
# дописать rm и не забыть очистку правил файервола перед
добавлением
user=$(who | awk '{print $1}' | uniq)
cd /home/$user/GE0IP/tmp
rm GeoLite2-Country-CSV.zip && sleep 2

wget
https://geolite.maxmind.com/download/geoip/database/GeoLite2-Country-CSV.zip
unzip GeoLite2-Country-CSV.zip -d .

ls -l | grep GeoLite2-Country-CSV_ | sed 's/_/ /g' | awk
'{print $10}' > tmp.txt
d=$(<tmp.txt)
cd GeoLite2-Country-CSV_$d

# 733045 - id Малайзии, его смотрим в файлах GeoLite2-Country-
Locations-*.csv
cat GeoLite2-Country-Blocks-IPv4.csv | grep "733045" >
```

```
GE0IP_MY.txt
```

```
# Копируем результат, на всякий случай, и работаем с копией  
cp GE0IP_MY.txt GE0IP_MY2.txt
```

```
cat GE0IP_MY2.txt | sed 's/,/ /g' > test  
cat test | awk '{print $1}' > GE0IP_MY_end.txt
```

```
# Эта строка просто посмотреть результат  
#cat GE0IP_MY_end.txt | wc -l
```

```
rm ../GeoLite2-Country-CSV.zip
```

Дописываем правило в firewall.script (там у меня FreeBSD):

```
${ipfw} add 1 deny log all from table\4\ to me
```

Можно было указать конкретный порт (143, 993), но мне трафик оттуда ненужен, поэтому блокирую все.

Добавляем в ipfw скриптом:

```
# cat add_ip_to_ipfw.sh
```

```
#!/bin/sh  
# IPFW table 4  
#user=$(who | awk '{print $1}' | uniq);  
user=`who | awk '{print $1}' | uniq`  
cat /home/$user/GE0IP_MY_end.txt | { while read ip;  
do  
/sbin/ipfw table 4 add $ip;  
done;  
}
```

Радуемся тишине в логах.

[Продолжение \)\)](#)

<https://dev.maxmind.com/geoip/geoip2/geolite2/>

<http://qaru.site/questions/570060/loading-variables-from-a-text-file-into-bash-script>