Fail2ban

приклад мого файрвола:

```
ee /etc/rc.firewall
```

```
#!/bin/sh -
f='/sbin/ipfw'

ifOut='vmx0'
ifCap='vmx1'

${f} -f flush

# TABLE 1 WHITE LIST
${f} table 1 add 1.1.1.1
${f} table 1 add 8.8.8.8

# TABLE 2 BLACKLIST

# RULE 10 FORWARDING TO CAP
${f} add 5 fwd 127.0.0.1,8080 tcp from any to not me 80 via $ifCap

#
${f} add 10 allow ip from "table(1)" to me
${f} add 20 allow ip from me to "table(1)"


${f} add 30 deny ip from "table(2)" to me
${f} add 40 deny ip from "table(2)"
```

```
${f} add 50 deny log all from "table(3)" to me
${f} add 60 deny log all from me to "table(3)"



${f} add 70 allow tcp from any to me 22,443,8000,8080
${f} add 80 allow tcp from me 22,443,8000,8080 to any

# OTHER SETTINGS
${f} add 110 allow ip from any to any via lo0
${f} add 130 deny icmp from 1 to 5,9,13,14,15,16,17
${f} add 1100 allow ip from any to any
```

Встановлення

```
pkg search fail2ban
```

```
py27-fail2ban-0.10.4 Scans log files and bans IP, що makes too many password failures
py37-fail2ban-0.10.4 Scans log files and bans IP, що makes too many password failures
py38-fail2ban-0.11.2 Scans log files and bans IP, що makes too many password failures
```

```
pkg install py38-fail2ban
```

Налаштування

```
cp -r /usr/local/etc/fail2ban /usr/local/etc/fail2ban.orig
cd /usr/local/etc/fail2ban
cp jail.conf jail.local
```

Правимо конфіг

```
ee /usr/local/etc/fail2ban/action.d/bsd-ipfw.conf
```

і наводимо параметри до вигляду:

```
actionban = /sbin/ipfw table <table> add <ip> <tablearg>
actionunban = /sbin/ipfw table <table> delete <ip>
```

Для функціонування fail2ban потрібно додати у файрвол правило:

```
ipfw add 50 deny log all from "table(3)" to me
ipfw add 60 deny log all from me to "table(3)"
```

Дивимось на мій приклад /etc/rc.firewall на початку статті.

```
# Пропишемо в автозавантаження
sysrc fail2ban_enable="YES"
За бажанням - ротація логів
echo '/var/log/fail2ban.log 600 7 200 * JC' >> /usr/local/etc/newsyslog.conf.d/fail2ban.conf
# Запустимо сервіс.
service fail2ban start
```

SSH

Створимо конфіг для ssh

```
ee /usr/local/etc/fail2ban/jail.d/ssh-ipfw.local
```

з таким вмістом

```
[ssh-ipfw]
# Включаємо фільтр.
```

```
enabled = true
# Порт
port = 22
# використовуємо фільтр та прикладів у  conf.d
filter = bsd-sshd
# Вказуємо профіль  bsd-ipfw.
action = bsd-ipfw[table=3, tablearg=22]
# Лог бана
logpath = /var/log/auth.log
# У який проміжок часу відловлюватиме брут
findtime = 600
кількість невдалих спроб
maxretry = 3
час бана в секундах або в хвилинах (60m)
bantime = 3600
# білий список  ip  для цього правила (через пробіл)! їх не буде банити.
ignoreip = 127.0.0.1/8
```

```
# Перезапустимо сервіс.
service fail2ban restart
```

phpmyadmin

Створимо конфіг для phpmyadmin

```
ee /usr/local/etc/fail2ban/jail.d/phpmyadmin.local
```

з таким вмістом

```
[phpmyadmin]
# Включаємо фільтр.
enabled = true
```

```
# Порт
port = http,https
# використовуємо фільтр та прикладів у conf.d
filter = phpmyadmin-syslog
# Вказуємо профіль bsd-ipfw.
action = bsd-ipfw[table=3, tablearg=80]
# Лог бана
logpath = /var/log/auth.log
# У який проміжок часу відловлюватиме брут
findtime = 600
кількість невдалих спроб
maxretry = 3
час бана в секундах або в хвилинах (60m)
bantime = 273600
# білий список ip для цього правила (через пробіл)! їх не буде банити.
ignoreip = 127.0.0.1/8
```

```
# Перезапустимо сервіс.
service fail2ban restart
```

Перевірка

```
fail2ban-client status
```

```
Status
- Number of jail: 1
- Jail list: ssh-ipfw
```

```
fail2ban-client status ssh-ipfw
```

```
Status for the jail: ssh-ipfw
|- Filter
| |- Currently failed: 0
| |- Total failed: 8
| `- File list: /var/log/auth.log
`- Actions
   |- Currently banned: 0
   |- Total banned: 1
   `- Banned IP list: 10.10.10.10
```

Ручний бан/розбан

```
fail2ban-client set <JAIL> banip <IP>
```

```
fail2ban-client set <JAIL> unbanip <IP>
```

new

nano /usr/local/etc/fail2ban/action.d/ipfw-table.local

```
# Fail2Ban configuration file
#
# Author: Method

[Definition]

actionstart = ipfw table all list | fgrep -c -m 1 -s 'table(f2b_<name>)' > /dev/null 2>&1 || ipfw -q table
```

```
f2b_<name> create
actionstop = ipfw table all list | fgrep -c -m 1 -s 'table(f2b_<name>)' > /dev/null 2>&1  ipfw -q table
f2b_<name> flush
actioncheck =
actionban = e=`ipfw table f2b_<name> add <ip> 2>&1`; x=$?; [ $x -eq 0 -o "$e" = 'ipfw:
setsockopt(IP_FW_TABLE_XADD): File exists' ] || echo "$e" | grep -q "record already exists" || { echo "$e" 1>&2;
exit $x; }
actionunban = e=`ipfw table f2b_<name> delete <ip> 2>&1`; x=$?; [ $x -eq 0 -o "$e" = 'ipfw:
setsockopt(IP_FW_TABLE_XDEL): No such process' ] || echo "$e" | grep -q "record not found" || { echo "$e" 1>&2;
exit $x; }
```

nano /usr/local/etc/fail2ban/jail.d/sshd.local

```
# Fail2Ban configuration file
#
# Author: Method

[DEFAULT]
ignoreip = 127.0.0.1/8

# JAILS
[sshd]
enabled = true
mode = aggressive
action = ipfw-table[name=SSH,port=ssh,protocol=tcp]
logpath = /var/log/auth.log
findtime = 600
maxretry = 3
bantime = 3600
```

From:
https://ndp.pp.ua/ - **my NoDeny Wiki**

Permanent link:
https://ndp.pp.ua/doku.php/freebsd/fail2ban?rev=1680278960

Last update: **31/03/2023 16:09**