Fail2ban

приклад мого файрвола:

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

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

ifOut='vmx0'
ifCap='vmx1'

${f} -f flush

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

${f} add 41 allow ip from "table(WHITE_LIST)" to me
${f} add 42 allow ip from me to "table(WHITE_LIST)"

# Fail2Ban reserved rules range 51 - 100
${f} add 51 deny ip from "table(f2b_SSH)" to me 22

# RULE 10 FORWARDING TO CAP
${f} add 105 fwd 127.0.0.1,8080 tcp from any to not me 80 via $ifCap

${f} add 170 allow tcp from any to me 80,443,8000,8080
${f} add 171 allow tcp from me 80,443,8000,8080 to any

# OTHER SETTINGS
```

```
${f} add 1110 allow ip from any to any via lo0
${f} add 1130 deny icmp from any to any in icmptype 5,9,13,14,15,16,17
${f} add 1190 allow ip from any to any
```

Встановлення

```
pkg search fail2ban
```

```
py27-fail2ban-0.10.4 Scans log files and bans IP that makes too many password failures
py37-fail2ban-0.10.4 Scans log files and bans IP that makes too many password failures
py38-fail2ban-0.11.2 Scans log files and bans IP that makes too many password failures
py39-fail2ban-1.0.2  Scans log files and bans IP that makes too many password failures
```

```
pkg install py39-fail2ban
```

Налаштування

```
cp -a /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/ipfw-tables.local
```

і наводимо параметри до вигляду:

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

```
# Automaticaly create tables for any jail with prefix "f2b_" by action argument <name> like "f2b_SSH"

[Definition]
actionstart = ipfw table all list | grep 'table(f2b_<name>)' || ipfw -q table f2b_<name> create
actionstop  = ipfw table all list | grep 'table(f2b_<name>)' && 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; }
```

SSH

Створимо конфіг для ssh

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

з таким вмістом

```
# Fail2Ban sshd jail configuration file
#
# Author: Method
# Atempt: Need manuali aad rule into firewall configuration file by template :
#         ipfw add <lowest_rule_number> (unreach port|deny) (ip|tcp|udp) from "table(f2b_<name>)" to me <ports
list>
# Example: ipfw add 51 unreach port ip from "table(f2b_SSH)" to me 22

[DEFAULT]
ignoreip = 127.0.0.1/8
```

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

Для функціонування fail2ban потрібно додати у файрвол правило:

```
${f} add 51 deny ip from "table(f2b_SSH)" to me 22
```

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
```

Перевірка

```
fail2ban-client status
```

```
Status
- Number of jail: 1
```

```
 - Jail list: sshd
```

```
fail2ban-client status sshd
```

```
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>
```

phpmyadmin

Створимо конфіг для phpmyadmin

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

з таким вмістом

```
# Fail2Ban phpmyadmin jail configuration file
#
# Author: Method
# Atempt: Need manuali aad rule into firewall configuration file by template :
#         ipfw add <lowest_rule_number> (unreach port|deny) (ip|tcp|udp) from "table(f2b_<name>)" to me <ports
list>
# Example: ipfw add 51 unreach port ip from "table(f2b_SSH)" to me 22

[DEFAULT]
ignoreip = 127.0.0.1/8

# JAILS
[phpmyadmin]
enabled  = true
port     = http,https
filter   = phpmyadmin-syslog
action   = ipfw-tables[name=phpmyadmin,port=80,443,protocol=tcp]
logpath  = /var/log/auth.log
findtime = 600
maxretry = 3
bantime  = 273600
```

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