Fail2Ban

Встановимо fail2ban

```
apt install fail2ban -y
```

Збережемо оригінальні налашування (на всякий випадок)

```
cp -a /etc/fail2ban/ /etc/fail2ban.orig/
```

Додамо виправлення до '/etc/fail2ban/jail.local' для роботи з nftables

```
cat <<EOF > /etc/fail2ban/jail.local
[DEFAULT]
# Destination email for action that send you an email
destemail = fail2ban@mydomain.example

# Sender email. Warning: not all actions take this into account. Make sure to test if you rely on this
sender    = fail2ban@mydomain.example

# Specify chain where jumps would need to be added in ban-actions expecting parameter chain
chain     = input

# configure nftables
banaction = nftables-multiport
banaction_allports = nftables-allports

# Default action. Will block user and send you an email with whois content and log lines.
## action    = %(action_mwl)s
action    = %(action_)s
EOF
```

Додамо виправлення до /etc/fail2ban/fail2ban.local

```
cat <<EOF > /etc/fail2ban/fail2ban.local
[Definition]
allowipv6 = auto
#allowipv6 = yes
EOF
```

```
systemctl enable fail2ban
fail2ban-client reload
fail2ban-client status
```

Створюємо каталог для конфігурації fail2ban для файрвола

```
mkdir -p /etc/nftables/
```

```
cat <<EOF > /etc/nftables/fail2ban.conf
#!/usr/sbin/nft -f

# Use ip as fail2ban doesn't support ipv6 yet
table inet fail2ban {
        chain input {
                # Assign a high priority to reject as fast as possible and avoid more complex rule evaluation
                type filter hook input priority 100;
        }
}
EOF
```

Додамо створений файл в оновну конфігурацію файрвола

```
echo "include \"/etc/nftables/fail2ban.conf\"" >> /etc/nftables.conf
```

Також підвантажимо його в роботу

```
nft -f /etc/nftables/fail2ban.conf
```

Налаштування Fail2Ban для запуску/зупинки за допомогою nftables

Ми намагаємося досягти наступного:

- під час завантаження сервер запускає спочатку nftables.service, а потім fail2ban.service;
- якщо ми запускаємо nftables.service, він також повинен запускати fail2ban.service;
- якщо ми зупинимо nftables.service, він також має зупинити fail2ban.service;
- якщо ми перезапустимо nftables.service, він також має перезапустити fail2ban.service;
- якщо ми запускаємо fail2ban.service, він також повинен запускати nftables.service;
- зупинка та перезапуск дій на fail2ban.service не повинні впливати на nftables.service.

Ми можемо зробити все це, створивши файл перевизначення для fail2ban, вказавши йому, що він залежить від nftables, а потім nftables хоче, щоб він запустився:

```
mkdir -p /etc/systemd/system/fail2ban.service.d/
```

```
cat <<EOF >  /etc/systemd/system/fail2ban.service.d/override.conf
[Unit]
Requires=nftables.service
PartOf=nftables.service

[Install]
WantedBy=multi-user.target nftables.service
EOF
```

Оскільки ми змінили розділ [Install], нам потрібно повторно ввімкнути відповідну службу, щоб створити відповідні символічні посилання. Ми також переконаємося, що nftables спочатку встановлено як сервісний блок:

```
# systemctl enable nftables.service
Created symlink /etc/systemd/system/sysinit.target.wants/nftables.service → /lib/systemd/system/nftables.service.
```

```
# systemctl enable fail2ban.service
Created symlink /etc/systemd/system/nftables.service.wants/fail2ban.service →
/lib/systemd/system/fail2ban.service.
# systemctl daemon-reload
```

Як саме це працює?

У нашому файлі заміни або повному файлі конфігурації (див. нижче) ми включаємо такі параметри:

```
[Unit]
Requires=nftables.service "запуск цієї служби спочатку запустить  nftables.service."
PartOf=nftables.service "змушує цю службу зупинятися або перезапускатися (але не запускатися) за допомогою
nftables.service."

[Install]
WantedBy=multi-user.target nftables.service "змушує цю службу запускатися, коли запускається будь-яка з перелічених служб."
```

Як бачите, нам потрібно встановити Requires, PartOf і WantedBy, щоб отримати бажану поведінку.

Блокувальники

Після додавання або видалення блокувальниуів необхідно перезавантажити fail2ban

```
fail2ban-client reload
```

Також можна переглянути статус fail2ban

```
fail2ban-client status
```

Рецедив

Повторно блокує по всіх портах іп адреси які раніше вже блокувались по іншим блокувальникам

```
cat <<EOF > /etc/fail2ban/jail.d/recidive.local
# Jail for more extended banning of persistent abusers
# !!! WARNINGS !!!
# 1. Make sure that your loglevel specified in fail2ban.conf/.local
#    is not at DEBUG level -- which might then cause fail2ban to fall into
#    an infinite loop constantly feeding itself with non-informative lines
# 2. If you increase bantime, you must increase value of dbpurgeage
#    to maintain entries for failed logins for sufficient amount of time.
#    The default is defined in fail2ban.conf and you can override it in fail2ban.local
#
# Manages the fail2ban history for hosts repeatedly banned by Fail2Ban and bans them
# according to the settings defined
#

[recidive]
enabled   = true
logpath   = /var/log/fail2ban.log
banaction = nftables-allports
backend   = systemd
bantime   = 9w
findtime  = 3d
maxretry  = 3
protocol  = 0-255
EOF
```

SSH

Вмикаємо блокувальник ssh. Оскільки всі значення стандартні то файл простий

```
cat <<EOF > /etc/fail2ban/jail.d/sshd.local
[sshd]
enabled   = true
backend   = systemd
EOF
```