Fail2Ban

```
apt install fail2ban -y
cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
nano /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

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

# configure nftables
banaction = nftables-multiport
banaction_allports = nftables-allports
chain     = input
```

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

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

```
nano /etc/nftables/fail2ban.conf
```

```
#!/usr/sbin/nft -f

# Use ip as fail2ban doesn't support ipv6 yet
table ip 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;
        }
}
```

Then add line include “/etc/nftables/fail2ban.conf” in /etc/nftables.conf.

Finally activate your rule in nftables

```
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/
nano /etc/systemd/system/fail2ban.service.d/override.conf
```

```
[Unit]
Requires=nftables.service
PartOf=nftables.service

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

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.