Linux ?? nftables ? Fail2ban ????

????

- **Debian 12**

`nftables` 是 **Linux** 取代舊版 `iptables` 的新一代封包過濾與 **NAT** 框架，由於 **Linux** 各發行版已開始使用 `nftables`，以下使用 `nftables` 和 `Fail2ban` 檢測登入失敗並封鎖

??Fail2ban

```
apt install fail2ban python3-systemd
```

??Fail2ban

建立 `/etc/fail2ban/fail2ban.local` 並配置啟用 **ipv6**

```
[DEFAULT]
allowipv6 = auto
```

建立 `/etc/fail2ban/jail.local`

```
[DEFAULT]
# Debian 12 has no log files, just journalctl
backend = systemd
# Destination email for action that sends you an email
#destemail = alerts@your-domain.com
# Sender email. Warning: not all actions take this into account. Make sure to test if you rely
on this
#sender    = fail2ban@your-domain.com
# Default action. Will block user and send you an email with whois content and log lines.
action    = %(action_mwl)s
# ignoreip can be a list of IP addresses, CIDR masks, or DNs hosts. Fail2ban
# # will not ban a host which matches an address in this list.
```

```
ignoreip = 127.0.0.1/8 ::1/128

# configure nftables
banaction = nftables-multiport
chain     = input

# regular banning
bantime = 7d
findtime = 1m
maxretry = 3

# "bantime.increment" allows to use database for searching of previously banned ip's to
increase a
# default ban time using special formula, default it is banTime * 1, 2, 4, 8, 16, 32...
bantime.increment = true
# "bantime.rndtime" is the max number of seconds using for mixing with random time
# to prevent "clever" botnets calculate exact time IP can be unbanned again:
bantime.rndtime = 30m
# "bantime.maxtime" is the max number of seconds using the ban time can reach (don't grows
further)
bantime.maxtime = 60d
# "bantime.factor" is a coefficient to calculate exponent growing of the formula or common
multiplier,
# default value of factor is 1 and with default value of formula, the ban time
# grows by 1, 2, 4, 8, 16 ...
bantime.factor = 2

# purge database entries after
dbpurgeage = 30d

[sshd]
mode      = aggressive
enabled   = true
backend   = systemd
port      = 2222
maxretry  = 3
```

- **backend = systemd**，**Debian12** 使用 **journalctl** 紀錄 **log**故使用 **systemd**
- 忽略來自本機主機和 **IPv6** 本機的連線
- 將 **nftables** 配置為防火牆後端
- 設定禁止相關設置和監聽 **port**

可設定 **Recidive**進行額外保護，重複觸發者將永久封鎖，該規則將監控 **fail2ban.log**，需啟用 **rsyslog**

```
[recidive]
backend = auto
logpath  = /var/log/fail2ban.log
enabled = true
maxretry = 2
banaction = nftables-allports
```

```
systemctl restart fail2ban
systemctl status fail2ban
```

??????

```
fail2ban-client status
fail2ban-client status sshd
fail2ban-client set sshd unbanip <ip>
```

```
root@remote:~# fail2ban-client status
Status
|- Number of jail:      2
`- Jail list:   recidive, sshd
root@remote:~# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
root@remote:~# fail2ban-client status recidive
Status for the jail: recidive
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- File list:        /var/log/fail2ban.log
`- Actions
```

```
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
root@remote:~#
```

Revision #2
Created 8 October 2025 05:02:45 by Jason
Updated 8 October 2025 06:39:50 by Jason