Introduction

The following example protect Exim4 from external attacks, for instance open relay.

The filter consist in parsing '/var/log/exim4/rejectlog' file with messages that contains 'relay not permitted' or 'check_mail_01'. The last message is a output of a custom ACL that protect Exim server from Phishing.

Procedure

- Edit */etc/fail2ban/jail.conf* and add the following section:

```
[exim]
enabled = true
filter  = exim
port    = smtp,ssmtp
action  = iptables-allports[name=exim, protocol=tcp]
#action   = iptables[name=exim, port="smtp", protocol=tcp]
logpath = /var/log/exim4/rejectlog
maxretry = 1
```

- Edit /etc/fail2ban/filter.d/exim.conf and ajust the line 'failregex' with:

```
failregex = .*\[<HOST>\].*(?:relay not permitted|check_mail_01).*
```

- Restart Fail2ban:

```
service restart fail2ban
```

Resources

- http://www.zaphinath.com/custom-filter-for-exim-through-fail2ban/