

## Linux Intrusion Prevention System

**Budi Santosa,ST**

**Kurusetra Computer**

Website: [www.kurusetra.web.id](http://www.kurusetra.web.id)

Email: [linux.multimedia@gmail.com](mailto:linux.multimedia@gmail.com)

Whatsapp: 085 736 167 850

### Pengenalan Intrusion Prevention System

Fail2Ban adalah aplikasi Linux Intrusion Prevention System (Linux IPS) opensource yang berjalan pada sistem operasi Linux (saya menggunakan Linux Ubuntu Server 12.04). Fail2Ban digunakan untuk mencegah Brute Force ke Server kita, maupun mencegah DDOS pada Web Server Apache. Prinsip kerja Fail2Ban adalah dengan memantau File Log, apabila sesuai dengan Regex misalkan failed auth, access denied, user not found, batas request yang di izinkan. Maka Fail2Ban akan memerintahkan firewall IPTables untuk melakukan blocking pada alamat IP pengakses. Kita bisa tentukan waktu BAN (cegah) misalkan hanya 1 jam, setelah itu di Unban (lepas).

Fail2Ban di pasang pada server yang ingin kita proteksi, Postfix SMTP, Asterisk, Wordpress, Roundcube, Apache2 Web Server, SSH, Server FTP dll.

Kelemahan Fail2Ban, kita tidak bisa melepas (UnBan) manual IP yang terblokir. Harus menunggu Bantime habis masa berlakunya.

#Buatapa #Beli #IPS #Hardware

#Pakai #Opensource #Murah #Meriah #Handal

# Fail2Ban

## LINUX INTRUSION PREVENTION SYSTEM

```
login as: root
root@192.168.56.95's password:
Access denied
root@192.168.56.95's password:
Access denied
root@192.168.56.95's password:
Access denied
root@192.168.56.95's password:
Access denied
root@192.168.56.95's password: 
```

```
Jul 11 17:48:33 mail postfix/smtpd[92608]: NOQUEUE: r
218.dynamic-ip.hinet.net[36.224.132.218]: 554 5.7.1
y access denied; from=<wopuugxmvin@yahoo.com.tw> to=
SMTP helo=<124.81.234.186>
Jul 11 17:48:33 mail postfix/smtpd[92608]: NOQUEUE: f
218.dynamic-ip.hinet.net[36.224.132.218]: <wopuugxm
ddress triggers FILTER smtp-amavis:[127.0.0.1]:10026
om.tw> to=<gonerilbaby@yahoo.com.tw> proto=SMTP helo
Jul 11 17:48:33 mail postfix/smtpd[92608]: NOQUEUE: f
218.dynamic-ip.hinet.net[36.224.132.218]: <wopuugxm
ddress triggers FILTER smtp-amavis:[127.0.0.1]:10026
om.tw> to=<gonerilbaby@yahoo.com.tw> proto=SMTP helo
Jul 11 17:48:33 mail postfix/smtpd[92608]: NOQUEUE: r
218.dynamic-ip.hinet.net[36.224.132.218]: 554 5.7.1
Relay access denied; from=<wopuugxmvin@yahoo.com.t
n.tw> proto=SMTP helo=<124.81.234.186>
```

### Instalasi Fail2Ban

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

### Konfigurasi Default Fail2Ban

```
vim /etc/fail2ban/jail.local  
[DEFAULT]
```

```
# "ignoreip" can be an IP address, a CIDR mask or a DNS host  
ignoreip = 127.0.0.1/8  
bantime = 600  
maxretry = 6  
destemail = linux.multimedia@gmail.com
```

### Fail2Ban SSH

```
[ssh]  
enabled = true  
port = ssh  
filter = sshd  
logpath = /var/log/auth.log  
bantime = 3600  
maxretry = 3
```

### Restart Fail2Ban

```
service fail2ban restart
```

### Status Fail2Ban

```
root@freepbx3:~# fail2ban-client status  
Status  
|- Number of jail:      1  
`- Jail list:           ssh
```

---

## Linux Intrusion Prevention System

---

```
root@freepbx3:~# fail2ban-client status ssh
```

```
Status for the jail: ssh
```

```
| - filter
|   | - File list: /var/log/auth.log
|   | - Currently failed: 0
|   ` - Total failed: 6
| - action
|   | - Currently banned: 1
|   ` - IP list: 192.168.56.37
| - Total banned: 1
```

```
root@freepbx3:~# iptables -L
```

```
Chain fail2ban-ssh (1 references)
```

target	prot	opt	source	destination
DROP	all	--	192.168.56.37	anywhere
RETURN	all	--	anywhere	anywhere

### Fail2Ban Apache2

Fail2Ban pada Apache2 Web Server digunakan untuk melindungi dari serangan DDOS. Apabila ada lebih dari 400 request dalam jangka waktu maksimal 120 detik dengan satu alamat IP. Maka IP tersebut di blok selama 600 detik (Ban Time Default).

```
root@freepbx3:~# vim /etc/fail2ban/jail.local
```

```
[apache-multiport]
enabled      = true
port         = http,https
filter       = http-get-dos
maxretry     = 400    # max amount of retries
findtime     = 120    # in max amount of seconds. 400 retries in 120 seconds from 1
unique IP    = ban hammer.
logpath      = /var/log/apache*/access.log
```

### Konfigurasi RegeX Apache2

```
vim /etc/fail2ban/filter.d/http-get-dos.conf
```

```
[Definition]
failregex = ^<HOST> -.*\\"(GET|POST).*
ignoreregex = ^<HOST> -.*\\"(GET|POST).*Googlebot
```

### Restart Fail2Ban

```
root@freepbx3:~# service fail2ban restart
```

### Test dari Komputer Lain

```
root@ubuntu:~# ab -n 1000 -c 50 -g dos.dat http://192.168.56.95/coba.php
This is ApacheBench, Version 2.3 <$Revision: 655654 $>
Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/
Licensed to The Apache Software Foundation, http://www.apache.org/

Benchmarking 192.168.56.95 (be patient)
Completed 100 requests
Completed 200 requests
Completed 300 requests
Completed 400 requests
Completed 500 requests
Completed 600 requests
apr_poll: The timeout specified has expired (70007)
Total of 676 requests completed
root@ubuntu:~#
```

### Log Fail2Ban

```
less /var/log/fail2ban.log
2014-07-11 16:19:57,277 fail2ban.actions: WARNING [apache-multiport] Ban
192.168.56.77
2014-07-11 16:19:58,299 fail2ban.actions: WARNING [apache-multiport]
192.168.56.77 already banned
2014-07-11 16:20:00,302 fail2ban.actions: WARNING [apache-multiport]
192.168.56.77 already banned
2014-07-11 16:20:01,303 fail2ban.actions: WARNING [apache-multiport]
192.168.56.77 already banned
```

### Lihat Status Banned Apache2

```
root@freepbx3:~# fail2ban-client status apache-multiport
Status for the jail: apache-multiport
|- filter
|  |- File list: /var/log/apache2/access.log
|  |- Currently failed: 0
|  `-- Total failed: 676
`- action
   |- Currently banned: 1
   |  `-- IP list: 192.168.56.77
   `-- Total banned: 1
```

### Status IPTables

```
root@freepbx3:~# iptables -L
Chain fail2ban-apache-multiport (1 references)
target      prot opt source                destination
DROP        all  --  192.168.56.77          anywhere
RETURN      all  --  anywhere              anywhere
```

### Fail2Ban Postfix

Fail2Ban Postfix kita gunakan untuk memblokir Klien email / Mesin Spammer yang berusaha menjadikan kita sebagai Open Relay. Walaupun sudah kita set bukan Open Relay Mesin Spam tetap berusaha mengirim email keluar melalui SMTP kita. Salah satu cara menangkal adalah dengan menggunakan Fail2Ban.


```
vim /etc/fail2ban/jail.local
[postfix]
enabled = true
port    = smtp,ssmtp
filter  = postfix
logpath = /var/log/mail.log
maxretry = 3
bantime = 3600
```

### Konfigurasi RegeX Postfix

```
vim /etc/fail2ban/filter.d/postfix.conf
[Definition]
#failregex = reject: RCPT from (.*)\[<HOST>\]: 554
failregex = reject: RCPT from (.*)\[<HOST>\]: * *
ignoreregex =
```

### Status Fail2Ban Postfix

```
root@mail:~# fail2ban-client status postfix
```



```
Status for the jail: postfix
|- filter
|   |- File list:      /var/log/mail.log
|   |- Currently failed: 10
|   `-- Total failed:  110537
`- action
    |- Currently banned: 65
    |   `-- IP list:    220.141.82.103 111.249.33.1
    |                  36.224.141.108 118.161.233.218 36.224.140.121 118.1
    |                  .20.135 36.224.132.193 36.224.135.4 118.166.238.45
    |                  36.224.136.210 220.141.80.240 220.141.83.228 114.43
    |                  .134.94 114.43.240.94 118.169.3.22 36.224.133.20 36
    |                  8.166.214.146 118.166.241.201 36.224.128.88 118.169
    |                  .13 36.224.141.145 1.160.123.45 36.224.130.231 118.
    |                  160.213.75 118.166.234.56 118.166.238.249 1.160.119
    |                  .181 118.169.2.218 36.225.31.37 114.37.186.115 118.
    |                  24.129.110 114.37.186.37 36.224.136.74 118.161.248.
    |                  67 36.224.138.84 118.161.246.56 118.169.1.139 118.1
    |                  161.248.186 1.160.116.239 36.224.139.206 118.161.25
    |                  38.91
    `-- Total banned:    11829
```

## Linux Intrusion Prevention System

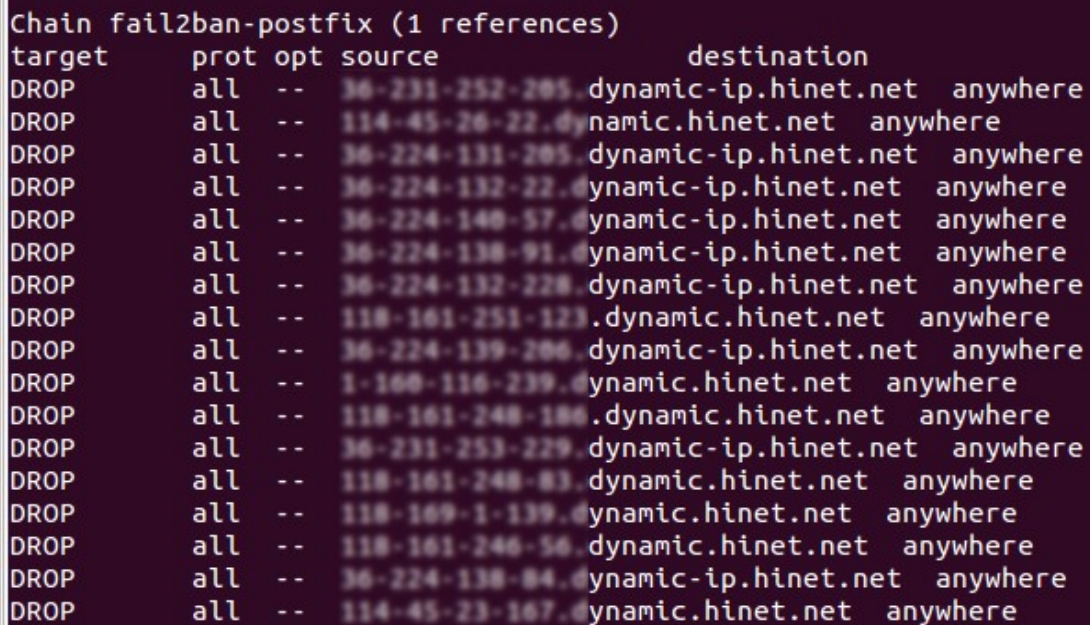
---

### Log Fail2Ban Postfix

```
less /var/log/fail2ban.log
2014-07-06 08:05:53,458 fail2ban.actions: WARNING [postfix] Unban 114.45xxx.xx
2014-07-06 08:06:08,481 fail2ban.actions: WARNING [postfix] Ban 114.45.24.243
2014-07-06 08:06:20,500 fail2ban.actions: WARNING [postfix] Unban 111.249.xxx
2014-07-06 08:06:35,525 fail2ban.actions: WARNING [postfix] Unban 111.249.xxx
2014-07-06 08:06:51,549 fail2ban.actions: WARNING [postfix] Unban 111.249.xxxx
2014-07-06 08:06:56,559 fail2ban.actions: WARNING [postfix] Ban 111.249.xxxx
2014-07-06 08:07:18,590 fail2ban.actions: WARNING [postfix] Unban 114.xxxx
2014-07-06 08:07:54,638 fail2ban.actions: WARNING [postfix] Ban 220.xxxx
2014-07-06 08:07:59,651 fail2ban.actions: WARNING [postfix] Ban 36.224.1xxx
2014-07-06 08:08:00,660 fail2ban.actions: WARNING [postfix] 36.2xx.1xx.9x
already banned
```

### Status IPTables

```
iptables -L
```



```
Chain fail2ban-postfix (1 references)
target      prot opt source                destination
DROP        all  -- 36-231-252-205.dynamic-ip.hinet.net anywhere
DROP        all  -- 114-45-26-22.dynamic.hinet.net anywhere
DROP        all  -- 36-224-131-205.dynamic-ip.hinet.net anywhere
DROP        all  -- 36-224-132-22.dynamic-ip.hinet.net anywhere
DROP        all  -- 36-224-140-57.dynamic-ip.hinet.net anywhere
DROP        all  -- 36-224-138-91.dynamic-ip.hinet.net anywhere
DROP        all  -- 36-224-132-228.dynamic-ip.hinet.net anywhere
DROP        all  -- 118-161-251-123.dynamic.hinet.net anywhere
DROP        all  -- 36-224-139-206.dynamic-ip.hinet.net anywhere
DROP        all  -- 1-160-116-239.dynamic.hinet.net anywhere
DROP        all  -- 118-161-248-186.dynamic.hinet.net anywhere
DROP        all  -- 36-231-253-229.dynamic-ip.hinet.net anywhere
DROP        all  -- 118-161-248-83.dynamic.hinet.net anywhere
DROP        all  -- 118-169-1-139.dynamic.hinet.net anywhere
DROP        all  -- 36-224-138-84.dynamic-ip.hinet.net anywhere
DROP        all  -- 114-45-23-167.dynamic.hinet.net anywhere
```

Sumber:

<https://help.ubuntu.com/community/Fail2ban>

<http://www.dedmeet.com/software-projects-mainmenu-12/fail2ban-to-limit-ddos-attacks-on-webserver.html>

<http://manpages.ubuntu.com/manpages/saucy/man5/jail.conf.5.html>

<https://community.rackspace.com/products/f/18/t/998>

[http://www.fail2ban.org/wiki/index.php/MANUAL\\_0\\_8](http://www.fail2ban.org/wiki/index.php/MANUAL_0_8)