# PF

*author: Budi Ang*

PF (Packet Filter) adalah firewall yang dikembangkan pertama kali oleh Daniel Hartmeier untuk OpenBSD dan menggantikan IPF yang berhubungan dengan masalah lisensi [1]. Mulai dari OpenBSD 3.0, PF sudah tersedia pada `base system`, sekarang, FreeBSD dan DragonFlyBSD telah mengimport PF dalam `base system`, untuk NetBSD bisa diinstalasi melalui pkgsrc, sedangkan untuk `Linux`, dapat diambil di http://abstractvoid.se/pf4lin.html (experimental)

## Aktivasi PF

```
$ sudo echo "pf=YES" > /etc/rc.conf.local
$ sudo reboot
```

atau

```
$ sudo pfctl -e
$ sudo ifconfig pflog0 up
```

untuk menonaktifkan pf di gunakan perintah berikut

```
pfctl -d
```

## Konsep Filtering di PF

```
dari PF host -> internet = out

dari internet -> PF host = in
```

Mohon maaf jika tidak ada fitur `forward`

### Macro

`Macro` di PF digunakan seperti variable program dalam mendefinisi interface, alamat IP, dan port, ataupun `reserved word` di PF.

Penggunaan `Macro` dapat mengurangi `complex`nya ruleset PF

```
server_if = "fxp0"
udp_port = "{ 53 123 }"
pass in on $server_if inet proto udp from any to any port $udp_port keep
state
```

Ruleset di atas diexpand menjadi:

```
pass in on fxp0 inet proto udp from any to any port 53 keep state
pass in on fxp0 inet proto udp from any to any port 123 keep state
```

## Tables

Tables dapat digunakan untuk menyimpan alamat IP dan network. Penggunaan yang lain seperti block network bogon atau IIX, seperti contoh di bawah ini

```
table <iix> { 114.120.0.0/13, 125.166.0.0/15, 125.162.0.0/16,
125.163.0.0/16, 125.160.0.0/16, 125.161.0.0/16, 125.164.0.0/16,
125.165.0.0/16, 222.124.0.0/16, 61.94.0.0/16, 167.205.0.0/16,
202.158.0.0/17, 61.5.0.0/17, 124.195.0.0/17, 121.52.0.0/17, 119.11.128.0/17,
114.57.0.0/18, 117.102.64.0/18, 210.210.128.0/18, 207.209.192.0/18,
61.14.0.0/18, 206.182.192.0/18, 125.208.128.0/18, 203.130.192.0/18,
124.153.0.0/18, 152.118.128.0/18, 221.132.192.0/18, 152.118.192.0/18,
152.118.0.0/18, 152.118.64.0/18, 222.165.192.0/18, 202.152.0.0/18,
209.93.224.0/19, 202.173.64.0/19, 114.199.96.0/19, 202.171.0.0/19,
202.47.192.0/19, 202.169.32.0/19, 202.182.160.0/19, 117.102.224.0/19,
202.51.192.0/19, 202.149.128.0/19, 202.147.224.0/19, 202.146.224.0/19,
114.58.32.0/19, 114.58.0.0/19, 202.159.64.0/19, 202.95.128.0/19,
202.152.224.0/19, 61.247.0.0/19, 61.247.32.0/19, 114.57.64.0/19,
117.104.192.0/19, 118.98.160.0/19, 118.98.192.0/19, 118.136.0.0/19,
118.136.32.0/19, 118.136.64.0/19, 118.136.96.0/19, 118.136.128.0/19,
118.136.160.0/19, 118.136.192.0/19, 118.136.224.0/19, 118.137.0.0/19,
118.137.32.0/19, 118.137.64.0/19, 118.137.96.0/19, 118.137.128.0/19,
118.137.160.0/19, 118.137.192.0/19, 118.137.224.0/19, 124.81.0.0/19,
124.81.32.0/19, 124.81.64.0/19, 124.81.96.0/19, 124.81.128.0/19,
124.81.192.0/19, 124.81.224.0/19, 202.10.32.0/19, 202.53.224.0/19,
202.57.0.0/19, 202.73.96.0/19, 202.77.96.0/19, 202.81.32.0/19,
202.137.0.0/19, 202.138.224.0/19, 202.148.0.0/19, 202.150.64.0/19,
202.153.128.0/19, 202.154.0.0/19, 202.154.32.0/19, 202.155.0.0/19,
202.155.32.0/19, 202.155.128.0/19, 202.159.0.0/19, 202.159.32.0/19,
202.162.192.0/19, 203.128.64.0/19, 219.83.0.0/19, 219.83.32.0/19,
219.83.64.0/19, 60.253.112.0/20, 61.8.64.0/20, 114.57.96.0/20,
114.57.160.0/20, 114.141.48.0/20, 114.199.80.0/20, 116.68.160.0/20,
117.20.48.0/20, 117.103.0.0/20, 118.98.240.0/20, 119.2.64.0/20,
119.110.64.0/20, 119.235.208.0/20, 119.252.160.0/20, 121.50.128.0/20,
122.129.96.0/20, 122.129.192.0/20, 122.200.0.0/20, 124.81.176.0/20,
202.3.208.0/20, 202.6.208.0/20, 202.6.224.0/20, 202.46.64.0/20,
202.46.144.0/20, 202.47.64.0/20, 202.51.224.0/20, 202.58.64.0/20,
202.58.160.0/20, 202.59.160.0/20, 202.59.192.0/20, 202.65.112.0/20,
202.67.32.0/20, 202.69.96.0/20, 202.70.48.0/20, 202.72.208.0/20,
202.73.224.0/20, 202.77.64.0/20, 202.80.112.0/20, 202.80.208.0/20,
202.87.176.0/20, 202.93.16.0/20, 202.93.32.0/20, 202.93.128.0/20,
202.93.224.0/20, 202.123.224.0/20, 202.127.96.0/20, 202.133.80.0/20,
202.143.32.0/20, 202.145.0.0/20, 202.146.48.0/20, 202.147.192.0/20,
202.152.160.0/20, 202.152.192.0/20, 202.153.16.0/20, 202.153.240.0/20,
```

202.155.64.0/20, 202.155.112.0/20, 202.159.112.0/20, 202.165.32.0/20,
202.182.48.0/20, 203.78.112.0/20, 203.83.32.0/20, 203.89.16.0/20,
203.123.224.0/20, 203.153.96.0/20, 203.161.16.0/20, 203.166.192.0/20,
203.201.160.0/20, 207.83.112.0/20, 210.57.208.0/20, 210.79.208.0/20,
219.83.96.0/20, 220.157.96.0/20, 60.253.96.0/21, 61.45.224.0/21,
114.57.232.0/21, 114.134.72.0/21, 114.141.88.0/21, 116.0.0.0/21,
116.12.40.0/21, 116.50.24.0/21, 116.68.224.0/21, 116.90.208.0/21,
116.197.128.0/21, 116.254.96.0/21, 117.18.16.0/21, 117.74.120.0/21,
117.103.32.0/21, 117.103.48.0/21, 117.103.168.0/21, 119.2.40.0/21,
119.10.176.0/21, 119.82.232.0/21, 119.82.240.0/21, 119.110.80.0/21,
119.160.200.0/21, 119.235.248.0/21, 120.29.152.0/21, 121.52.136.0/21,
121.58.184.0/21, 121.100.16.0/21, 121.101.128.0/21, 121.101.184.0/21,
122.49.224.0/21, 122.128.16.0/21, 122.129.112.0/21, 122.144.0.0/21,
122.200.48.0/21, 122.200.144.0/21, 123.108.8.0/21, 124.66.160.0/21,
124.81.168.0/21, 124.158.128.0/21, 202.43.160.0/21, 202.43.176.0/21,
202.43.248.0/21, 202.46.24.0/21, 202.46.80.0/21, 202.51.16.0/21,
202.58.176.0/21, 202.62.16.0/21, 202.67.8.0/21, 202.72.192.0/21,
202.74.72.0/21, 202.87.248.0/21, 202.89.208.0/21, 202.91.8.0/21,
202.91.24.0/21, 202.93.240.0/21, 202.122.8.0/21, 202.129.184.0/21,
202.133.0.0/21, 202.134.0.0/21, 202.149.64.0/21, 202.149.80.0/21,
202.150.128.0/21, 202.153.224.0/21, 202.155.80.0/21, 202.155.104.0/21,
202.158.136.0/21, 202.159.96.0/21, 202.162.32.0/21, 202.164.216.0/21,
202.169.224.0/21, 202.169.240.0/21, 202.179.184.0/21, 202.180.0.0/21,
202.180.48.0/21, 203.77.224.0/21, 203.80.8.0/21, 203.84.136.0/21,
203.84.152.0/21, 203.123.240.0/21, 203.134.232.0/21, 203.135.176.0/21,
203.142.80.0/21, 203.153.24.0/21, 203.153.112.0/21, 203.174.8.0/21,
203.176.176.0/21, 203.190.48.0/21, 203.190.112.0/21, 203.190.184.0/21,
203.190.240.0/21, 203.191.40.0/21, 219.83.112.0/21, 220.247.168.0/21,
222.229.80.0/21, 58.65.244.0/22, 58.145.168.0/22, 60.253.104.0/22,
61.45.232.0/22, 114.30.80.0/22, 114.31.240.0/22, 116.66.200.0/22,
116.68.248.0/22, 116.90.176.0/22, 116.199.204.0/22, 117.102.160.0/22,
117.103.56.0/22, 118.98.228.0/22, 118.98.236.0/22, 119.2.48.0/22,
119.18.156.0/22, 119.82.224.0/22, 119.235.16.0/22, 119.252.132.0/22,
120.136.16.0/22, 122.102.48.0/22, 124.6.32.0/22, 124.81.164.0/22,
146.23.252.0/22, 202.2.92.0/22, 202.43.184.0/22, 202.46.0.0/22,
202.46.88.0/22, 202.51.28.0/22, 202.51.252.0/22, 202.55.164.0/22,
202.55.168.0/22, 202.62.8.0/22, 202.62.24.0/22, 202.72.200.0/22,
202.75.16.0/22, 202.75.24.0/22, 202.78.196.0/22, 202.81.4.0/22,
202.87.240.0/22, 202.93.112.0/22, 202.146.0.0/22, 202.146.128.0/22,
202.146.176.0/22, 202.149.72.0/22, 202.149.88.0/22, 202.153.236.0/22,
202.155.92.0/22, 202.155.96.0/22, 202.158.132.0/22, 202.159.108.0/22,
202.162.40.0/22, 202.173.16.0/22, 202.180.16.0/22, 203.77.208.0/22,
203.77.236.0/22, 203.77.248.0/22, 203.81.184.0/22, 203.99.96.0/22,
203.123.60.0/22, 203.123.248.0/22, 203.128.248.0/22, 203.142.68.0/22,
203.142.76.0/22, 203.160.56.0/22, 203.190.40.0/22, 219.83.120.0/22,
32.234.170.0/23, 32.234.172.0/23, 58.65.240.0/23, 60.253.108.0/23,
61.45.236.0/23, 116.66.204.0/23, 116.90.166.0/23, 116.199.202.0/23,
116.212.100.0/23, 117.102.166.0/23, 117.103.60.0/23, 118.82.0.0/23,
118.82.12.0/23, 119.235.20.0/23, 119.252.128.0/23, 121.52.134.0/23,
123.176.120.0/23, 124.158.136.0/23, 194.146.106.0/23, 202.20.106.0/23,
202.43.168.0/23, 202.43.188.0/23, 202.46.4.0/23, 202.46.14.0/23,

202.46.92.0/23, 202.46.130.0/23, 202.46.240.0/23, 202.46.252.0/23,
202.51.56.0/23, 202.51.98.0/23, 202.51.106.0/23, 202.55.160.0/23,
202.55.172.0/23, 202.58.196.0/23, 202.62.28.0/23, 202.65.236.0/23,
202.75.20.0/23, 202.78.192.0/23, 202.78.200.0/23, 202.78.204.0/23,
202.89.216.0/23, 202.89.222.0/23, 202.90.194.0/23, 202.90.198.0/23,
202.93.116.0/23, 202.129.216.0/23, 202.135.6.0/23, 202.135.134.0/23,
202.146.4.0/23, 202.146.132.0/23, 202.149.78.0/23, 202.149.92.0/23,
202.150.136.0/23, 202.153.232.0/23, 202.154.176.0/23, 202.154.184.0/23,
202.155.100.0/23, 202.158.130.0/23, 202.159.106.0/23, 202.162.46.0/23,
202.169.232.0/23, 202.169.236.0/23, 202.173.20.0/23, 202.180.8.0/23,
202.191.2.0/23, 203.31.164.0/23, 203.34.118.0/23, 203.77.214.0/23,
203.77.220.0/23, 203.77.232.0/23, 203.77.246.0/23, 203.81.190.0/23,
203.99.102.0/23, 203.123.252.0/23, 203.142.64.0/23, 203.153.120.0/23,
203.160.60.0/23, 203.189.88.0/23, 203.190.36.0/23, 203.190.46.0/23,
203.194.70.0/23, 203.223.90.0/23, 204.61.216.0/23, 206.73.208.0/23,
206.73.234.0/23, 206.73.238.0/23, 219.83.124.0/23, 32.234.169.0/24,
32.234.175.0/24, 58.65.243.0/24, 58.145.173.0/24, 58.145.175.0/24,
58.147.189.0/24, 60.253.110.0/24, 61.45.238.0/24, 114.4.0.0/24,
114.4.5.0/24, 114.4.6.0/24, 114.30.84.0/24, 116.58.197.0/24,
116.66.207.0/24, 116.68.252.0/24, 116.68.255.0/24, 116.90.163.0/24,
116.90.164.0/24, 116.212.96.0/24, 117.102.164.0/24, 118.82.14.0/24,
118.82.18.0/24, 118.82.31.0/24, 119.2.55.0/24, 119.47.88.0/24,
119.82.231.0/24, 119.252.130.0/24, 120.136.23.0/24, 121.52.129.0/24,
121.52.130.0/24, 122.102.52.0/24, 122.201.39.0/24, 123.176.122.0/24,
123.176.127.0/24, 124.81.160.0/24, 124.81.162.0/24, 124.158.138.0/24,
144.5.46.0/24, 152.158.247.0/24, 192.5.5.0/24, 192.23.186.0/24,
192.36.148.0/24, 192.92.81.0/24, 194.0.1.0/24, 194.0.2.0/24,
194.146.108.0/24, 202.14.255.0/24, 202.20.109.0/24, 202.22.31.0/24,
202.43.170.0/24, 202.43.173.0/24, 202.43.175.0/24, 202.43.190.0/24,
202.46.9.0/24, 202.46.11.0/24, 202.46.94.0/24, 202.46.129.0/24,
202.51.96.0/24, 202.51.100.0/24, 202.51.104.0/24, 202.51.109.0/24,
202.51.110.0/24, 202.51.122.0/24, 202.58.203.0/24, 202.58.204.0/24,
202.62.31.0/24, 202.65.227.0/24, 202.65.228.0/24, 202.65.238.0/24,
202.75.22.0/24, 202.75.29.0/24, 202.75.30.0/24, 202.78.195.0/24,
202.78.203.0/24, 202.78.207.0/24, 202.87.245.0/24, 202.87.247.0/24,
202.92.192.0/24, 202.92.207.0/24, 202.122.162.0/24, 202.122.165.0/24,
202.122.166.0/24, 202.135.5.0/24, 202.135.16.0/24, 202.135.23.0/24,
202.135.28.0/24, 202.135.42.0/24, 202.135.54.0/24, 202.135.129.0/24,
202.135.133.0/24, 202.135.145.0/24, 202.135.155.0/24, 202.135.161.0/24,
202.135.248.0/24, 202.146.32.0/24, 202.146.34.0/24, 202.146.47.0/24,
202.146.135.0/24, 202.146.180.0/24, 202.149.77.0/24, 202.151.9.0/24,
202.154.183.0/24, 202.154.187.0/24, 202.154.190.0/24, 202.155.88.0/24,
202.155.91.0/24, 202.155.102.0/24, 202.158.129.0/24, 202.160.254.0/24,
202.162.44.0/24, 202.167.97.0/24, 202.169.234.0/24, 202.180.10.0/24,
202.180.20.0/24, 203.14.176.0/24, 203.77.212.0/24, 203.77.216.0/24,
203.77.223.0/24, 203.77.252.0/24, 203.77.255.0/24, 203.99.100.0/24,
203.99.119.0/24, 203.99.120.0/24, 203.99.127.0/24, 203.119.13.0/24,
203.119.17.0/24, 203.123.254.0/24, 203.142.66.0/24, 203.153.122.0/24,
203.160.62.0/24, 203.163.66.0/24, 203.163.76.0/24, 203.163.81.0/24,
203.163.88.0/24, 203.163.95.0/24, 203.163.113.0/24, 203.173.89.0/24,
203.173.90.0/24, 203.174.5.0/24, 203.194.90.0/24, 203.196.90.0/24,

```
205.248.57.0/24, 205.248.151.0/24, 205.248.158.0/24, 206.73.79.0/24,
206.73.80.0/24, 206.73.194.0/24, 206.73.203.0/24, 206.73.205.0/24,
206.73.222.0/24, 206.73.227.0/24, 206.73.228.0/24, 206.73.240.0/24,
206.73.244.0/24, 206.73.248.0/24, 206.182.36.0/24, 207.117.234.0/24,
218.100.32.0/24 }
```

**will be continued**

## Packet Filtering

Filtering untuk `block` atau `pass` packet sesuai yang didefinisikan. `Ruleset` di file /etc/pf.conf (default), dibaca dari atas ke bawah.

`block` PF host dari satu host

```
block in from ip.add.re.ss
```

`block` satu subnet atau lebih

```
block in from sub.net.ho.st/mask
```

`block` satu host, dan `pass` host yang lain

```
block in from bad.ip
pass in from good.ip
```

`Default` deny adalah kebijakan yang direkomendasi sewaktu menyiapkan firewall apapun, hal ini berlaku untuk PF juga.

```
block in all
block out all
```

Tambahkan keyword `log`, sehingga dapat melihat packet mana yang diblock oleh PF, dengan menggunakan `tcpdump(8)`

```
block in  log all
block out log all
```

Dapat disederhanakan menjadi

```
block log all
```

Catatan: jika host mempunyai >=4 NIC, semua traffic in/out di block by default.

## Contoh Kasus

<server> —– [switch] —– {router}

Server menyediakan service SMTP Relay dan POP3

Policy:

- default deny
- incoming ke port 25 dan 110
- outgoing bebas

```
# macro
server_if = "fxp0"
lo_if = "lo0"
tcp_port = "{ 25 110 }"
ks = "keep state"

# default deny
block log all

# untuk loopback
pass quick on $lo_if all

# incoming
pass in on $server_if inet proto tcp from any     to $server_if port
$tcp_port $ks
pass in on $server_if inet proto tcp from $admin to $server_if port
$adm_port $ks

# outgoing
pass out on $server_if all $ks
```

# Referensi

- http://openbsd.cbn.net.id/faq/
- http://www.benzedrine.cx/pf.html
- http://openbsd.cbn.net.id/faq/pf/
- http://www.openbsd.org/cgi-bin/man.cgi?query=pf.conf&sektion=5&manpath=OpenBSD+3.7
- http://www.openbsd.org/cgi-bin/man.cgi?query=pfctl&sektion=8&manpath=OpenBSD+3.7
- https://solarflux.org/pf/
- http://www.thedeepsky.com/howto/newbie_pf_guide.php

[1)]

http://slashdot.org/article.pl?sid=01/05/30/124255