

# 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 <sup>1)</sup>. 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
```

## 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 complexnya 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](#)

**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  $\geq 4$  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.benedrine.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](http://www.thedeepsky.com/howto/newbie_pf_guide.php)

1)

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

From:  
<http://wiki.corebsd.or.id/> - **CoreBSD Wiki**

Permanent link:  
<http://wiki.corebsd.or.id/doku.php/coreprojects:pf?rev=1218991173>

Last update: **2025/10/25 17:09**

