

Konfigurasi Rule Firewall IPFW pada FreeBSD 6.0

Ricki Zurwindar <rz.bangka@gmail.com>
Universitas YARSI
Copyright © 2007

Pada Sistem Operasi FreeBSD, ada beberapa aplikasi yang digunakan sebagai firewall, diantaranya adalah PF dan IPFW.

Agar sistem FreeBSD 6.0 bisa menjalankan IPFW, maka kernel yang berjalan harus mensupport IPFW (bisa lewat modul atau kompilasi ulang kernel).

Note: Sebelum mulai melakukan konfigurasi, pastikan dalam kernel telah terdapat listing seperti berikut:

```
options      IPFWALL
options      IPFWALL_VERBOSE
options      IPFWALL_VERBOSE_LIMIT=100
options      IPFWALL_DEFAULT_TO_ACCEPT
```

Untuk mengaktifkan logging dan mengatur logging verbose limit tambahkan listing sebagai berikut ke dalam file `/etc/sysctl.conf`.

```
net.inet.ip.fw.verbose=1
net.inet.ip.fw.verbose_limit=100
```

Sedangkan untuk mengaktifkan firewall tambahkan listing berikut ini ke dalam file `/etc/rc.conf`:

```
firewall_enable="YES"
```

Untuk memilih type default firewall yang disediakan FreeBSD, lihat file `/etc/rc.firewall` dan tambahkan listing berikut ke dalam file `/etc/rc.conf`:

```
firewall_type="OPEN"
```

Value yang disediakan adalah

- open -- mengizinkan semua traffic.
- client -- hanya akan melindungi mesin yang digunakan.
- simple -- melindungi seluruh jaringan.

- closed -- menonaktifkan semua IP traffic kecuali loopback interface.
- UNKNOWN -- menonaktifkan loading rule-rule firewall.
- filename -- path tertentu yang berisi rule-rule firewall.

Jika firewall_type diatur menjadi client or simple, default route dapat ditemukan di file /etc/rc.firewall. Dalam contoh ini akan digunakan firewall_script yang diatur di dalam file /etc/ipfw.rules.

Sedangkan untuk mengaktifkan logging tambahkan listing berikut ini ke dalam file /etc/rc.conf:

```
firewall_logging="YES"
```

Command IPFW

Beberapa command IPFW adalah sebagai berikut:

Untuk list semua rule secara berurutan:

- ipfw list

Untuk list semua rule dengan time stamp ketika terakhir kali rule match:

- ipfw -t list

Untuk list informasi accounting:

- ipfw -a list

Untuk list dynamic rule yang ditambahkan ke dalam static rule:

- ipfw -d list

Untuk menampilkan dynamic rule yang telah expired:

- ipfw -d -e list

Untuk mengosongkan counters:

- ipfw zero

Mengosongkan counters hanya untuk rule NUM:

- ipfw zero NUM

Syntax Rule IPFW

Syntax yang digunakan untuk mengatur rule firewall IPFW:

```
CMD  RULE_NUMBER  ACTION  LOGGING  SELECTION  STATEFULL
```

CMD

Setiap rule baru harus dimulai dengan **add** untuk menambahkan rule ke tabel internal.

RULE_NUMBER

Setiap rule harus mempunyai sebuah rule number.

ACTION

Setiap rule bisa berasosiasi dengan satu pilihan actions, yang mana akan dieksekusi ketika paket match dengan pemilihan kriteria rule.

allow | accept | pass | permit

Semuanya berarti sama yang digunakan untuk mengizinkan paket yang match dengan rule untuk keluar dari proses rule firewall.

check-state

Mengecek paket yang berlawanan dengan tabel dynamic rule.

deny | drop

Keduanya berarti sama yang mana digunakan untuk men-discard paket yang match dengan rule.

Logging

log atau logamount

Ketika suatu paket match dengan sebuah rule yang menggunakan kata log, sebuah pesan akan dimasukkan ke syslogd dengan fasilitas yang bernama SECURITY.

Selection

Digunakan untuk mendeskripsikan atribut dari paket yang akan diinterogasi ketika menentukan apakah rule match atau tidak dengan paket.

ucd | tcp | icmp

atau protocol lainnya yang dapat ditemukan di /etc/protocols bisa dikenal dan digunakan.

from src to dst

Kata **from** dan **to** digunakan untuk mencocokkan IP address yang berlawanan. Rule parameter source dan destination harus spesifik. **any** adalah kata khusus yang digunakan untuk mencocokkan IP address mana saja. **me** adalah kata khusus yang digunakan untuk mencocokkan IP address yang diatur di interface dalam sistem FreeBSD.

port number

Untuk protocols yang mendukung port number (seperti TCP dan UDP). Kode port number dari services yang akan digunakan dapat dilihat dalam file /etc/services.

in | out

Mencocokkan masuknya atau keluarnya paket, berturut-turut. Kata **in** dan **out** merupakan satu kode sebagai bagian untuk mencocokkan kriteria rule.

via IF

Mencocokkan paket yang melalui spesifik interface dengan nama exact. Kata **via** dikarenakan interface selalu di-cek sebagai bagian dari proses pencocokkan.

setup

Merupakan kata perintah untuk mengidentifikasi session start request untuk paket TCP.

keep-state

Merupakan kata perintah. Ketika cocok, firewall akan membuat dynamic rule. Kebiasaan default dalam pencocokkan traffic bidirectional antara source dan destination IP/port menggunakan protokol yang sama.

limit { src-addr | src-port | dst-addr | dst-port }

Firewall hanya akan mengizinkan koneksi *N* dengan mengatur parameter yang sama sebagai spesifikasi dalam rule. 'limit' dan 'keep-state' tidak bisa digunakan dalam rule yang sama.

Logging Firewall Messages

Semua pencatatan pesan dari paket secara default ditulis ke file /var/log/security, yang mana didefinisikan dalam file /etc/syslog.conf.

Membuat Script Rule

Seperti yang telah dikatakan sebelumnya, script firewall akan diatur dalam file baru yang bernama ipfw.rules yang berada di direktori /etc.

Langkah pertama buat file yang bernama ipfw.rules dan tempatkan di direktori /etc dengan perintah vi /etc/ipfw.rules, dan tambahkan listing berikut:

```
##### start ipfw rules script #####
ipfw -q -f flush
ipfw -q add divert natd all from any to any via vr0
ipfw -q add allow ip from any to any via lo0
ipfw -q add deny ip from any to 127.0.0.0/8
ipfw -q add deny ip from 127.0.0.0/8 to any
##### End ipfw rules script #####
```

Atau dengan Rule Stateful + NATD seperti berikut:

```

##### Start of IPFW rules file #####
# Flush out list sebelum dimulai.
ipfw -q -f flush

# Set rules command prefix
cmd="ipfw -q add"
skip="skipto 800"
pif="vr0" # public interface name of Nic card
            # facing the public internet

#####
# Tidak ada pembatasan interface LAN dalam untuk private network
# Ganti xl0 dengan nama interface LAN internal
#####
$cmd 005 allow all from any to any via xl0

#####
# Tidak ada pembatasan dalam Loopback Interface
#####
$cmd 010 allow all from any to any via lo0

#####
# Cek jika paket adalah inbound dan alamat NAT-nya
#####
$cmd 014 divert natd ip from any to any in via $pif

#####
# Izinkan paket melalui-nya jika sebelumnya telah ditambahkan ke
# tabel dynamic rule dengan mengizinkan statement keep-state.
#####
$cmd 015 check-state

#####
# Interface Public internet (bagian Outbound)
# Tanyakan session start requests dimulai dari belakang
# firewall dalam the private network atau server gateway ini
# dengan tujuan untuk public internet.
#####

# Izinkan akses keluar untuk ISP's Domain name server.
# x.x.x.x harus merupakan IP address dari ISP's DNS
# Tambahkan baris ini jika IP address dari ISP's lebih dari satu DNS server
# Dapatkan IP address dari file /etc/resolv.conf
# $cmd 020 $skip tcp from any to x.x.x.x 53 out via $pif setup keep-state
$cmd 020 $skip tcp from any to 172.16.1.12 53 out via $pif setup keep-state

```

```

# Izinkan akses keluar untuk ISP's DHCP server untuk konfigurasi kabel/DSL.
#$cmd 030 $skip udp from any to x.x.x.x 67 out via $pif keep-state
$cmd 030 $skip udp from any to 172.16.1.12 67 out via $pif keep-state

# Izinkan fungsi www standar non-secure keluar
$cmd 040 $skip tcp from any to any 80 out via $pif setup keep-state

# Izinkan fungsi www standar secure melalui TLS SSL keluar
$cmd 050 $skip tcp from any to any 443 out via $pif setup keep-state

# Izinkan fungsi untuk mengirim dan mendapatkan email keluar
$cmd 060 $skip tcp from any to any 25 out via $pif setup keep-state
$cmd 061 $skip tcp from any to any 110 out via $pif setup keep-state

# Izinkan fungsi-fungsi FBSD (make install & CVSUP) keluar
# Pada dasarnya diberikan kepada user root "GOD" privileges.
$cmd 070 $skip tcp from me to any out via $pif setup keep-state uid root

# Izinkan ping keluar
$cmd 080 $skip icmp from any to any out via $pif keep-state

# Izinkan time keluar
$cmd 090 $skip tcp from any to any 37 out via $pif setup keep-state

# Izinkan nntp news (IE: news groups) keluar
$cmd 100 $skip tcp from any to any 119 out via $pif setup keep-state

# Izinkan secure FTP, Telnet, and SCP keluar
# Fungsi pada rule ini menggunakan SSH (secure shell)
$cmd 110 $skip tcp from any to any 22 out via $pif setup keep-state
# Izinkan whois keluar
$cmd 120 $skip tcp from any to any 43 out via $pif setup keep-state

# Izinkan ntp time server
$cmd 130 $skip udp from any to any 123 out via $pif keep-state

#####
# Interface Public internet (bagian Inbound)
# Tanyakan paket dimulai dari public internet
# dengan tujuan untuk gateway server ini atau private network.
#####

# Tolak semua inbound traffic dari non-routable reserved address spaces
$cmd 300 deny all from 192.168.0.0/16 to any in via $pif #RFC 1918 private IP
$cmd 301 deny all from 172.16.0.0/12 to any in via $pif #RFC 1918 private IP
$cmd 302 deny all from 10.0.0.0/8 to any in via $pif #RFC 1918 private IP

```

```

$cmd 303 deny all from 127.0.0.0/8 to any in via $pif #loopback
$cmd 304 deny all from 0.0.0.0/8 to any in via $pif #loopback
$cmd 305 deny all from 169.254.0.0/16 to any in via $pif #DHCP auto-config
$cmd 306 deny all from 192.0.2.0/24 to any in via $pif #reserved for doc's
$cmd 307 deny all from 204.152.64.0/23 to any in via $pif #Sun cluster
$cmd 308 deny all from 224.0.0.0/3 to any in via $pif #Class D & E multicast

# Tolak ident
$cmd 315 deny tcp from any to any 113 in via $pif

# Tolak semua servis Netbios. 137=name, 138=datagram, 139=session
# Netbios adalah servis sharing MS/Windows
# Block MS/Windows hosts2 name server requests 81
$cmd 320 deny tcp from any to any 137 in via $pif
$cmd 321 deny tcp from any to any 138 in via $pif
$cmd 322 deny tcp from any to any 139 in via $pif
$cmd 323 deny tcp from any to any 81 in via $pif

# Tolak kedatangan paket apa saja yang terlambat
$cmd 330 deny all from any to any frag in via $pif

# Tolak paket ACK jika tidak cocok dengan tabel dynamic rule
$cmd 332 deny tcp from any to any established in via $pif

# Izinkan traffic dari ISP's DHCP server. Rule ini harus berisi
# IP address dari ISP's DHCP server hanya sebagai
# authorized source untuk mengirim tipe paket ini.
# Hanya dibutuhkan untuk konfigurasi kabel or DSL.
# Rule ini tidak dibutuhkan untuk tipe koneksi 'user ppp' ke
# public internet. Ini adalah ip address yang sama
# dan digunakan di bagian outbound
#$cmd 360 allow udp from x.x.x.x to any 68 in via $pif keep-state
$cmd 360 allow udp from 172.16.1.12 to any 68 in via $pif keep-state

# Izinkan fungsi standar www kedalam karena memiliki server apache
$cmd 370 allow tcp from any to me 80 in via $pif setup limit src-addr 2

# Izinkan secure FTP, Telnet, dan SCP kedalam dari public Internet
$cmd 380 allow tcp from any to me 22 in via $pif setup limit src-addr 2

# Izinkan non-secure Telnet session kedalam dari public Internet
# label non-secure digunakan karena harus mengizinkan ID & PW melalui public
# internet sebagai clear text.
# Hapus contoh ini jika tidak mengaktifkan server telnet.
#$cmd 390 allow tcp from any to me 23 in via $pif setup limit src-addr 2

```

```
# Reject & Log semua koneksi-koneksi unauthorized kedalam dari public internet
$cmd 400 deny log all from any to any in via $pif

# Reject & Log semua koneksi-koneksi unauthorized keluar ke public internet
$cmd 450 deny log all from any to any out via $pif

# Ini adalah lokasi skipto untuk stateful rules keluar
$cmd 800 divert natd ip from any to any out via $pif
$cmd 801 allow ip from any to any

# Apapun yang lainnya dengan default ditolak
# tolak dan log semua paket
$cmd 999 deny log all from any to any
##### End of IPFW rules file #####
```

Setelah membuat script, edit file /etc/rc.conf dengan perintah vi /etc/rc.conf dan tambahkan listing berikut untuk mengaktifkan rule firewall IPFW saat booting:

```
...
firewall_script="/etc/ipfw.rules"
...
```

Semoga artikel ini dapat membantu saat melakukan konfigurasi rule IPFW pada sistem operasi FreeBSD 6.0.

Pustaka: dari berbagai sumber

