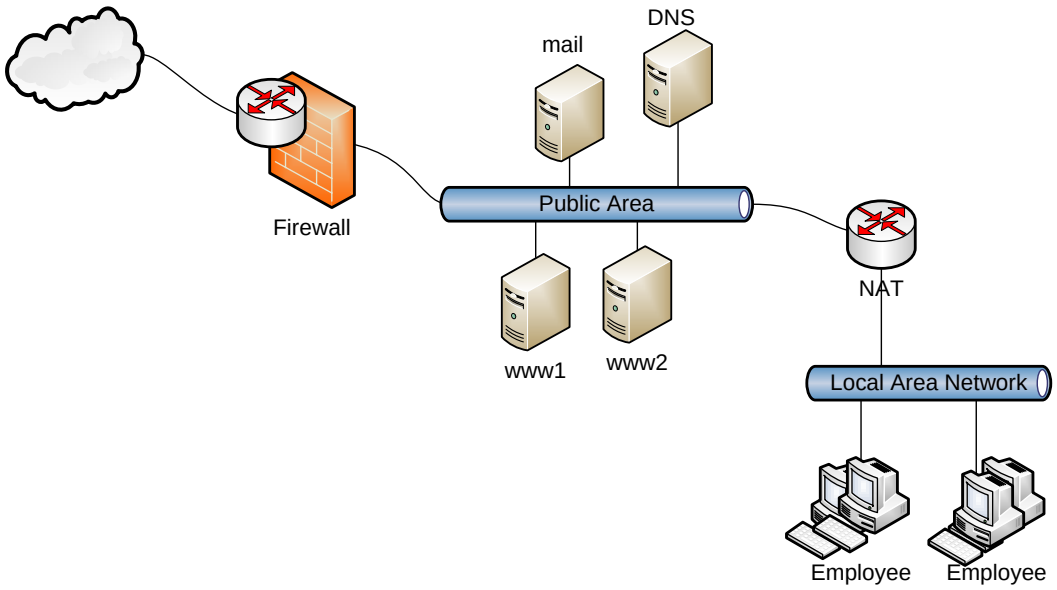
Membangun Firewall Dengan OpenBSD

Anjik Sukmaaji
Program Studi Sistem Informasi
STMIK (STIKOM) Surabaya, 60298
anjik@stikom.edu

Sebelum dijelaskan tentang tahapan dalam membangun firewall, terlebih dahulu harus difahami konsep firewall. Secara umum yang di sebut dengan firewall dijelaskan dalam penjelasan detailnya seperti pada kutipan ini. "*A firewall can either be software-based or hardware-based and is used to help keep a network secure. Its primary objective is to control the incoming and outgoing network traffic by analyzing the data packets and determining whether it should be allowed through or not, based on a predetermined rule set. A network's firewall builds a bridge between the internal network or computer it protects, upon securing that the other network is secure and trusted, usually an external (inter)network, such as the Internet, that is not assumed to be secure and trusted*."



Gambar 1. Topologi jaringan dengan Firewall

Dari kutipan tersebut bentuk firewall bisa berupa perangkat lunak *"A firewall can either be software-based"* atau dapat juga merupakan perangkat keras yang sudah didesain khusus "*A firewall can either be hardware-based".* Perangkat lunak yang dimaksudkan adalah serangkai sistem yang dapat bertugas sebagai fungsi kerja yang melakukan pekerjaan sesuai dengan tugas-

tugas firewall dan berjalan diatas sistem operasi yang umum misalnya Ms. Windows, Linux atau Unix. Perangkat lunak firewall ini di setiap sistem operasi umumnya sudah tersedia, sebagai contoh pada sistem operasi windows terdapat pada bagian control panel – firewall, pada sistem operasi Linux yaitu IPTABLES, pada OpenBSD yaitu *packet filter (PF)* dan pada Unix yang menggunakan *IPFilter*. Pada sistem operasi perangkat keras jaringan, misalnya router umumnya juga menyediakan fungsi firewall yang di kenal dengan sebutan *packet filter*. Sedangkan untuk perangkat keras firewall adalah sistem yang didesain khusus yang bekerja untuk melakukan tugas-tugas firewall saja tanpa ada tugas lain. Peralatan ini disebut dengan mesin firewall yang dikeluarkan oleh pabrik perangkat keras jaringan. Perangkat keras firewall ini bermacam-macam merk, tipe, fungsi dan kelebihan masing-masing.

Firewall jika di bedakan dari generasinya, terdapat tiga macam yaitu firewall generasi pertama (1988), firewall generasi kedua (1989-1990) dan firewall generasi ke-tiga (1994).

- Generasi pertama : *packet filter*
- Generasi kedua : *state full (Transport layer) filter*
- Generasi ketiga : *Application layer*

Tipe Firewall

Tipe firewall berdasarkan layer komunikasi, penyaringan dan keadaan data yang diprosesnya dapat dikategorikan menjadi :

1. Network layer
2. Application layer
3. Proxy
4. Network Address Translation

OpenBSD Firewall dikategorikan pada tipe network firewall karena pada aplikasi OpenBSD firewall ini melakukan proses filter terhadap paket yang masuk pada sistem ini. Disebut dengan network filter karena yang di filter adalah protocol data unit pada layer network yaitu packet (*Low level of the TCP/IP protocol stack*). Filter yang dimaksudkan adalah dengan tidak mengijinkan paket lewat selama kondisi packet yang melalui firewall sesuai dengan daftar *rule* yang sudah ditentukan.

Network layer firewall di kategorikan menjadi dua kategori utama yaitu statefull dan stateless. ***Stateful*** *firewalls can watch traffic streams from end to end. They are are aware of communication paths and can implement various IP Security (IPsec) functions such as tunnels and encryption. In technical terms, this means that stateful firewalls can tell what stage a TCP connection is in (open, open sent, synchronized, synchronization acknowledge or established), it can tell if the MTU has changed, whether packets have fragmented etc.* ***Stateless*** *firewalls watch*

network traffic, and restrict or block packets based on source and destination addresses or other static values. They are not 'aware' of traffic patterns or data flows. A stateless firewall uses simple rule-sets that do not account for the possibility that a packet might be received by the firewall 'pretending' to be something you asked for.

Network firewall dapat melakukan filter terhadap paket berdasarkan atribut-atributnya yang meliputi : alamat IP asal/tujuan, port asal/tujuan, serta tujuan dari layanan aplikasi misalnya www atau FTP.

OpenBSD adalah turunan dari sistem operasi UNIX dari *Berkeley Software Distribution (BSD)*, yang dikembangkan di Universitas California, Berkeley. Sistem operasi OpenBSD memiliki moto "FREE, FUNCTIONAL AND SECURE" sehingga pada websitenya (www.openbsd.org) dapat dijumpai tulisan "Only two remote holes in the default install, in a heck of a long time!".

OpenBSD secara default install sudah dijanjikan aman, atau istilahnya adalah "*secure by default"*. Dapat dikutip dari website OpenBSD tentang hal ini yaitu "*To ensure that novice users of OpenBSD do not need to become security experts overnight (a viewpoint which other vendors seem to have), we ship the operating system in a Secure by Default mode. All non-essential services are disabled. As the user/administrator becomes more familiar with the system, he will discover that he has to enable daemons and other parts of the system. During the process of learning how to enable a new service, the novice is more likely to learn of security considerations".*

Membuat Network Firewall dengan OpenBSD.

Untuk membuat Network firewall menggunakan sistem operasi OpenBSD terlebih dahulu mempersiapkan perangkat kerasnya yaitu PC dengan minimal 2 Network Interface Card (NIC). Diperlukan dua NIC karena digunakan untuk memfilter jaringan luar dan dalam. Selanjutnya PC diinstall OpenBSD dan memfungsikan PC ini menjadi penghubung dua jaringan dengan fungsi sebagai Network Bridge atau Network address Translation (NAT).

Jika sebagai Network Bridge, secara default akan seperti perangkat layer-2 (Datalink) yakni antar kedua sisi jaringan bisa saling berkomunikasi yang mirip jika menghubungkan kedua jaringan dengan switch atau bridge. Model ini lebih popular dikenal dengan istilah transparent firewall. Transparent firewall bekerja sebagai sebuah bridge yang bertugas untuk menyaring lalu lintas jaringan antara dua segmen jaringan. Transparent Firewall bekerja pada lapisan data-link, dan tidak membutuhkan alamat IP untuknya. Karena itulah, transparent firewall tidak dapat

terlihat oleh para penyerang. Karena tidak dapat diakses oleh penyerang (tidak memiliki alamat IP), penyerang pun tidak dapat menyerangnya.

Mengkonfigurasi OpenBSD sebagai Bridge (Transparent Firewall).

Untuk mengkonfigurasi OpenBSD menjadi bridge tentunya harus mengenal dua NIC yang digunakan. Misalnya kedua NIC tersebut adalah Intel EtherExpress/100 (fxp0) and a 3c590-Combo card (xl0), maka pada konfigurasi kedua NIC tersebut sbb :

Pada Intel EtherExpress/100 (fxp0) dikenal pada sistem BSD adalah /etc/hostname.fxp0, dan jika ditampilkan isinya sbb :

```
$cat /etc/ hostname.fxp0
  up
```

Pada 3c590-Combo card (ep0) dikenal pada sistem BSD adalah /etc/hostname.xl0, dan jika ditampilkan *isinya sbb :*

```
$cat /etc/hostname.xl0
   Up
```

Setelah itu mengkonfigurasi bridge dengan membuat file /etc/hostname.bridge0 dengan isinya sebagai berikut :

```
$ cat /etc/hostname.bridge0
add fxp0
add xl0
up
```

Setelah konfigurasi OpenBSD sebagai bridge, selanjutnya mengaktifkan fungsi packet filter pada OpenBSD yaitu :

```
$cat /etc/rc.conf.local
pf=YES
```

Konfigurasi PC firewall menggunakan OpenBSD sudah selesai, dan jika sistem di restart maka sudah dapat menjalankan fungsi-fungsi paket filter. Packet filter dapat dioperasi menggunakan command line interface dan tidak harus melakukan reboot komputer PC tersebut. Sedangkan jika saat komputer di reboot sudah menjalankan aturan-aturan firewall maka aturan firewall (*rules)* di tulis dalam file /etc/pf.conf

File /etc/pf.conf memiliki tujuh bagian penting yaitu :

- *Macros* : variable user-defined yang dapat menahan IP address, nama interfaces, dll.

- *Tables* : sebuah struktur digunakan untuk menyatakan sekumpulan dari IP address
- *Option* :variasi pilihan untuk mengontrol bagaimana pf bekerja
- *Scrub* : Re-processing paket untuk menjadi normal dan mendefrag mereka.
- *Queueing* : Memberikan kontrol bandwidth dan proritas paket.
- *Transalation* : Kontrol Network Address Translation (NAT) dan paket redirection.
- *Filter Rules* : Memperbolehkan selektif terhadap filtering atau blocking terhadap paket ketika mereka melalui interfaces.

Jika pada saat PC firewall dihidupkan dan dalam file /etc/pf.conf tidak ada difinisi rules firewall maka, rules firewall dapat dioperasikan dengan menggunakan perintah pfctl. Beberapa perintah pfctl yang digunakan untuk mengendalikan firewall terdapat beberapa contoh fungsi sebagai berikut :

pfctl -f /etc/pf.conf digunakan untuk me-Load file pf.conf

pfctl -nf /etc/pf.conf digunakan untuk me-Parse file, tapi tidak load

pfctl -Nf /etc/pf.conf digunakan untuk me-Load hanya rule NAT dari file

pfctl -Rf /etc/pf.conf digunakan untuk me-Load hanya rule filter dari file

pfctl -sn untuk menampilkan rule NAT yang sedang berjalan

pfctl -sr untuk menampilkan rule filter yang sedang berjalan

pfctl -ss untuk menampilkan bentuk table yang sedang berjalan

pfctl -si untuk menampilkan bentuk filter dan counters

pfctl -sa untuk menampilkan SEMUANYA

pfctl –Fa; pfctl –f /etc/pf.conf digunakan untuk menghapus semua rules yang sudah dijalanlan dan memanggil kembali rules baru.

OpenBSD yang digunakan disini adalah versi terbaru pada saat penulisan OpenBSD 5.0. Pada OpenBSD 4.6 keatas, pf sudah enable secara default, dengan konfigurasi minimal. Untuk OpenBSD 4.6 kebawah kita bisa aktifkan PF secara default dengan mengedit atau menambahkan baris "pf=YES" pada /etc/rc.conf.local file seperti pada penjelasan sebelumnya. Untuk mengaktifkan PF kita bisa gunakan perintah berikut:

```
# pfctl -e
pf enabled
```

Dasar Sintak untuk perintah PF adalah

action [direction] [quick] [on interface] [af] [proto protokol] [from alamat_sumber] [to detinasi_port]

action: melakukan pass atau block packet

direction: in atau out paket

quick: jika packet sesuai dengan spesifikasi quick, maka di tunjuk sebagai rule terakhir.

interface: alamat fisik interface network

af: inet untuk ipv4 atau inet6 untuk ipv6

proto: udp, tcp, icmp atau icmp6

Contoh-contoh sederhana PF.

pass in quick on xl0 proto tcp to port 80

artinya Rule di tersebut membolehkan semua trafik masuk yang datangnya dari interface network xl0 menuju port 80 (http).

pass in quick on xl1 proto tcp to port domain
pass in quick on xl1 proto udp to port domain

Artinya membolehkan semua trafik masuk yang datang dari interface network xl1 menuju port 53 (domain)

pass in quick inet proto icmp all icmp-type echoreq

Membolehkan trafik masuk dengan protokol icmp berstatus request

Pada saat semua rules sudah didefinisikan, jangan lupa pada bagian akhir dilengkapi dengan rules yang mengijinkan semua yang keluar dan memblokir sisanya selain yang sudah ditentukan dalam rules dengan rules sbb :

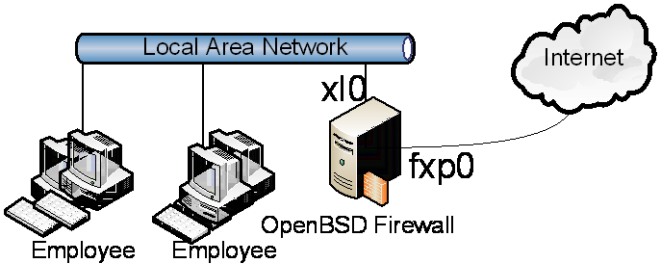
block in all
pass out all

Contoh script PF yang mengijinkan seluruh trafik keluar adalah sbb :

pass in quick on xl0 proto tcp to port 80
pass in quick on xl1 proto udp to port domain
block in all
pass out all

Contoh script packet filter firewall pada jaringan kecil yang terhubung ke Internet menggunakan OpenBSD sebagai firewall geteway dan NAT.

Pada contoh konfigurasi pada gambar-2 ini, sebuah network local dengan beberapa komputer yang ada dengan mengkonfigurasi OpenBSD sebagai Gateway jaringan sekaligus sebagai firewall. Firewall yang dibuat dengan ketentuan atau policy adalah :



1. Tidak mengijinkan Internet untuk mengakses langsung komputer-komputer yang ada di LAN.
2. Dibuat konfigurasi default deny
3. Hanya mengijinkan lalulintas data (traffic) dari internet berupa SSH(TCP port 22), ICMP Echo Request untuk mengijinakan akses menggunakan aplikasi ping, Auth/Ident (TCP port 113) yang umumnya digunakan untuk SMTP dan IRC, me-redirect port TCP 80 ke komputer3 (COMP3), mengijinkan lalulintas TCP port 80 untuk komputer3 melalui firewall, membuat log untuk filter pada external NIC.

Maka konfigurasi pada /etc/pf.conf adalah sebagai berikut :

```
# macros
int_if="xl0"
tcp_services="{ 22, 113 }"
icmp_types="echoreq"
comp3="192.168.0.3"
# options
set block-policy return
set loginterface egress
set skip on lo
# FTP Proxy rules
anchor "ftp-proxy/*"
pass in quick on $int_if inet proto tcp to any port ftp \
   divert-to 127.0.0.1 port 8021
# match rules
match out on egress inet from !(egress:network) to any nat-to (egress:0)
# filter rules
block in log
pass out quick
antispoof quick for { lo $int_if }
pass in on egress inet proto tcp from any to (egress) \
   port $tcp_services
pass in on egress inet proto tcp to (egress) port 80 rdr-to $comp3
pass in inet proto icmp all icmp-type $icmp_types
pass in on $int_if
```