VOL. I. NO. 3. Desember 2000 ISSN:1411-3201

JURNAL ILMIAH

DASI

DATA EKONOMI, BISNIS DAN TEKNOLOGI INFORMASI

AKADEMI MANAJEMEN INFORMATIKA DAN KOMPUTER
"AMIKOM" YOGYAKARTA

JURNAL ILMIAH

DASI

BUILT IN FIREWALL DALAM LINUX

Oleh : Ema Utami

Pendahuluan

Internet kini sudah menjadi suatu hal yang umum digunakan di berbagai macam bidang. Berbagai macam kegiatan diupayakan bisa dilakukan lewat internet, belanja lewat internet, telephon leat internet dan lain-lain .kita sudah mengenal e-comerce, e-bussines, e-tailing dan e-e yang lain.

Kini dengan mudah kita dapat membeli barang yang kita inginkan dengan cara browsing lewat internet dan pembayaran melalui kartu kredit, atau cek account kita di bank dengan internet atau kegiatan lain sudah banyak yang dapat dilakukan di internet. Sedemikian dimanja kita dengan teknologi yang dinamakan internet, Internet dapat dikatakan sebagai salah sutu keajaiban teknologi, banyak hal yang dapat dilakukan dengan internet yang tidak terbayangkan orang sebelumnya.

Namun apakah hanya "enak saja" yang kita dapat dari internet ?, tentu saja ada segi positif dari internet pasti ada segi negatifnya. Dengan adanya transaksi secara online, membeli lewat kartu kredit dan lainya, hal tersebut pasti meninggalkan data dari pemilik kartu kredit. Nah disini sering kita mendenggar atau pernah melihat penggunaan kartu kredit milik orang lain untuk belanja di internet. Atau suatu perusahaan yang telah online dan mempunyai dokumen rahasia perusahaan, msialnya rancangan pengembangan perusahaan, analisis keuangan ataupun hutang perusahaan tiba-tiba dokumenn tersebut telah tersebar luas tentu akan berakibat mengerikan bagiperusahaan.

Hal tersebut merupakan beberapa dari sekian banyak hal negatif dalam internet, untuk itu diperlukan semacam satpam untuk menjaga agar data atau dokumen tetap aman, *firewall* merupakan salah satu solusi yang bisa diguankan.

Apa yang dimaksud dengan *firewall* ?

Sebelum kita tinjau apa yang dimaksud dengan *firewall* kita perlu melihat bahwa perkembangang pesat dalam penggunaan teknologi internet pada umumnya dan teknologi TCP/IP pada khususnya menjadikan pengalamatan suatu host di internet sangat berkembang dengan cepat, hal tersebut dikarenakan karena pengalamatan di internet adalah bersifat unik sehingga antara host satu dengan yang lain harus berbeda alamat. Juga penggunaan teknologi TCP/IP yang diluar internet juga membutuhkan pengalamatan tersendiri sehingga secara garis besar dapat dikatakan bahwa pengalamatan suatu host dapat kita bagi menjadi 3 katagori :

1. Hosts yang tidak memerlukan akses ke internet
2. Hosts yang memerlukan akses terbatas ke internet
3. Hosts yang memerlukan akses internet secara langsung.

Pada katagori pertama dapat kita katakan adalah suatu LAN yang tidak terkoneksi ke internet sedang katagori ke dua adalah LAN yang dapat terkoneksi ke internet, sedang kategori ke tiga adalah host yang terhubung keinternet secara langsung pada kategori pertama dan kedua dinamakan *private address* dan ketiga dinamakan *public address.*

Pada kategori ke dua diamana suatu LAN yang terhubung ke internet dengan ada pembatasan akses maka dapat diguanakan *firewall* sebagai pembatas tersebut. Juga bagi host yang terhubung langsung dengan internet dapat menggunakan *firewall* sebagai pengaman host tersebut.

Secara harafiah atau secara sederhana sesuai dengan namanya *firewall* dapat dikatakan sebagai suatu struktur yang dimaksudkan agar agar api tidak menajalar kemana-mana. dalam bangunan *firewall* dapat dikatakan sebuah dinding pemisah antara satu dengan yang lain. atau juga dapat diakatakan sebagai sebuah pos satpam pada suatu rumah yang bertugas menjaga rumah tersebut. Dalam internet *firewall* juga berfungsi seperti hal diatas yaitu menjaga agar suatu kawasan tertentu (*private* LAN) tidak terkotaminasi atau terjaga dari pengaruh buruk internet. Internet seperti kita ketahui mempunyai banyak manfaat akan tetapi tentu saja juga banyak menyimpan hal-hal buruk, seperti kegiatan cracker, virus dan lain-lainnya.

Untuk itu maka diperlukan suatu "dinding pembatas" yang akan menjaga dari pengaruh buruk tersebut. *firewall* dengan menggunakan komputer pertama kali adalan sebuah mesin Unix yang terkoneksi 2 jaringan

Pada saat itu jika komputer pada workstation akan mengakses internet maka merekan harus log in dulu dalam mesin Unix kemudian baru menggunakannya untuk akses ke internet. Kini dalam perkembangannya tabnpa harus login ke server kita dapat keluar mengakses internet dengan aman.

Tujuan *Firewall*

Seperti yang telah kita bahas di atas maka tujuan dari penggunaan *firewall* secara sederhana dapat dikatakan adalah untuk :

1. Menjaga dari luar

   menjaga dari pengaruh buruk internet yang datang dari luar (internet)

2. Menjaga dari dalam

   Menjaga agar ada pembatasan jika akan ke luar (internet)

Misal dalam kasus nyata sebuah perusahaan yang kantornya terhubung ke internet selamajam kantor bagaimana cara perusahaan tersebut menjaga agar semua karyawan tetap bekerja dengan baik, tanpa takut bahwa pekerjanya mencuri-curi untuk melihat situs-situs porno ?. dengan tujuan ke 2 maka fiewall

dapat berfungsi untuk hal ini. *firewall* dapat memberikan akses terbatsa misalnya hanya mail saja yang dapat keluar.

Tipe *Firewall*

Secara umum dapat dikatakan ada dua macam tipe firewall yaitu *packet filter firewall* dan *proxy server firewall*. *Packet filter firewall* bekerja pada lapisan network (*network layer*). Dalam sistem ini data harus mengikuti aturan yang ditetapkan oleh firewall. Disini kita akan membahas sedikit tentang *packet filter firewall* ini dimana linux memiliki ini secara *built in.*

Letak Firewall

Firewall dapat dipasang dalam berbagai asritektur tergantung dari kebutuhan dan tujuan yang akan didapat. sistem firewall dapat diletakan di belakang router atau dijadikan satu dengan proxy server

Bagaimana Firewall Bekerja

Untuk memahami bagaimana firewall bekerja kita harus terlebih dahulu mengerti bagaimana suatu data dikirimkan atau diterima. Sekarang kita mengasumsikan kita mengirim sebuah file dengan ukuran 1 MB dari yogya ke server di Amerika. apakah file yang kita kirimkan akan "bejalan" sebesar 1 MB ? apakah data kita akan melewati jakarta, singapura dan seterusnya ?
Kita tentu jarang membayangkan atau tidak pernah membayakan hal tersebut.

Seperti kasus diatas bagaimana dua komputer dapat berhubungan ? untuk dapat melakukan hubungan maka dua komputer atau lebih harus mentaati sekumpulan aturan,secara sederhana protokol dapat diartikan sebagai bahasa, jadi dua komputer dapat berhubungan jika bahasanya sama. Fungsi dari protokol adalah :

1. membuat hubungan antara pengirim dan penerima
2. menyalurkan informasi / data.

TCP/IP, protokol yang digunakan dalam internet. TCP (*Trasmission Control Protocol*) berfungsi untuk memecah pesan dalam datagram-datagram dan mengumpulkannya kembali bila telah sampai tujuan,mengirim kembali bila ada datagramyang hilang dan menyusun dalam urutan yang benar. IP (*Interner Protocol*) mempunyai tanggung jawab pada perjalanan datagram. Jadi dapat diilustrasikan bila terdapat data yang besar akan dikirimkan ke komputer lain :

.....

maka TCP akan memecah datgram tersebut yang besarnya sesuai dengan kemampuan dari jaringan yang ada ke dalam beberapa datagram.

....

Pada tiap datagram TCP akan meletakan header yang berisi antara lain : *port* sumber dan tujuan , *squence number*, *Acknowledment number*, *data offset*, *Control Bits*, *Windows*, *cheksum* yang berisi alamat sumber dan tujuan, dan lain-lain.

Dengan adanya *port*, *address* dari sumber dan tujuan serta jenis informasi yang terkadung dalam paket datagram yang dikirim atau diterima maka paket tersebut dapat disaring dengan firewall. *Packet filtering firewall* akan memeriksa header tersebut ketika paket akan dilewatkan dan akan menentukan nasib dari paket tersebut sesuai dengan aturan yang ditetapkan.

Linux Firewall

Linux telah memiliki firewall dengan tipe *packet filtering* yang telah tertanam dalam kernel (*built ini*), selain yang telah tertanam dalam kernel Linux juga dapat dipasang *proxy server* seperti *squid proxy server* juga dapat dipasng dua-duanya.

Dengan *packet filtering* yang telah tertanam di kernel dalam linux mempunyai 3 rantai (*chain*) yaitu :

1. input
2. output
3. forward

yang masing-masing rantai tersebut dapat berisi berbagai macam aturan (*rule*). Jika ada paket yang datang akan ditest dengan mengunakan aturan yang ada dalam *chain input* sebelum paket diterima dengan keputusan accept, deny atau reject. Juga paket yang akan keluar akan ditest dengan menggunakan aturan *chain output* dan paket yang akan di *forward* akan ditest dengan *chain forward*. Sedang keputusan yang akan diterima oleh suatu paket dalam Linux firewall adalah :

1. accept
2. deny
3. reject
4. masq
5. redirect
6. return

IPCHAINS

Linux dengan kernel 2.2.0 ke atas pemeliharaan dan setup atas *packet filtering* dialjukan dengan perintah ipchains yang menggatikan perintah ipfadm untuk kernel 2.0.x kebawah. Jadi bagaimana firewall yang akan diperoleh tergantung dari setup administratornya. Contoh penggunaan ipchains adalah sebagai berikut:

```
ipchains –A output –d www.rasendriya.net –j REJECT
ipchains –A input –i eth1 –p tcp-d 0/0 23 –j DENY
```


pada contoh pertama maka bila akan ada paket yang keluar menuju ke www.rasendriya.net maka akan di tolak dan yang kedua bila ada paket yang masuk dari interface ethernet pada protokoltcp port telnet makajuga akan ditolak.
Contoh diatas masih cukup sederhana selain option A(append) dan parameter d, i, p masih cukup banyak parameter dan option-option yang harus diperhatikan.

Pentup

Perkembangan sistem keamanan komputer telah sangat pesat dan tentu saja dibarengi dengan perkembangan kejahatan terhadap sistem keamanan yang juga pesat. Hal ini tentu saja menjadikan sistem keamanan menajadi suatu hal yang mempunyai nilai ekonomis yang tinggi.

Oleh karena itu dengan sedikit tulisan ini penulis berharap dapat memberikan sedikit informasi mengenai firewall umumnya dan packet filtering firewall dalam linux khususnya sehingga apabila kita ingin bergabung dengan dunia internet kita telah memiliki bekal sistem keamanan yang baik

Referensi

Firewall-HOWTO
Rfc1918
Linux Network Servers 24 seven . Craig Hunt, Sybex Network Press
Ipchains manual