10.37817/ikraith-informatika.v9i2
P-ISSN :2580-4316
E-ISSN :2654-8054

Penerapan Firewall Dan Iptables Untuk Kemanana Data Pada Jaringan Publik Berbasis Linux Server

Iwan Setiawan
Email : iwan.setiawan@nusaputra.ac.id

ABSTRAK

Penelitian ini bertujuan untuk mengetahui penerapan firewall dan IPTables pada jaringan publik dan untuk keamanan data. Dalam pengelolaan jarinngan publik sangatlah penting untuk selalu rajin mengpatch dan update terhadap software-software bug yang ada di komputer. Karena hal ini cukup menolong untuk sedikit menyulitkan para hacker dan pengganggu lain untuk bisa bersenang-senang dengan komputer akan. Namun rasanya, patch yang up-to-date saja belum cukup untuk melindungi resource akan yang berharga di dalam jarinngan publik. Maka dari itu, rasanya cukup penting untuk akan bisa membatasi apa dan siapa saja yang boleh masuk dan keluar dari dan ke perangkat komputer Akan. Semua proses ini bisa Akan lakukan dengan mengakanlkan sebuah sistem pengaman khusus yang biasanya disebut dengan istilah firewall atau IP filter. Hasil dari pembuatan jurnal menunjukkan bahwa IPTables memilki banyak sekali keunggulan dalam implementasinya diantaranya: IPTables memiliki kemampuan untuk melakukan Connection Tracking Capability yaitu kemampuan untuk inspeksi paket serta bekerja sama dengan ICMP dan UDP sebagaimana koneksi TCP, Menyederhanakan perilaku paket-paket dalam negosiasi built in chain, dan lain-lainnya. Tapi Yang terpenting adalah Implementasi Firewall dan IPTables pada jarinngan publik sangat murah dan memiliki tingkat kemanan yang baik.

Keyword: jaringan publik, Firewall, IPTables,

ABSTRACT

In writing this paper is to determine the definition, characteristics and implementation of the iptables firewall and the computers on the network. In the management of computer networks is important to always be diligent mengpatch and update the software bugs that use on your computer. Because it is quite helpful for a little difficult for hackers and other intruders in order to have fun with your computer. But it seems, patches are up-to-date is not enough to protect your valuable resource in the computer. Therefore, it is important to limit what you can and anyone who may come in and out of your computer and to your device. All of these processes can do by relying on a special safety system which is usually referred to as a firewall or IP filter. The results from the manufacture of the journal suggests that once iptables has many advantages in its implementation are: IPTables has the ability to perform the Connection Tracking Capability packet inspection as well as the ability to work with ICMP and UDP as well as TCP connections, Simplify behavior in negotiation packages built-in chain, and others. But most important is the implementation of Firewalls and IPTables on a computer network is very cheap and has a good level of security.

Keyword: Computer Networking, Firewall, IPTables

I. PENDAHULUAN

Seiring dengan pesatnya perkembangan teknologi informasi dan komputerisasi, jarinngan publik tentu sangat bermanfaat, antara lain membuat seseorang dapat berkomunikasi dan berhubungan dengan orang lain tanpa mengenal lagi yang namanya jarak. Seseorang *telekomputer* dapat memiliki lebih dari satu perkerjaaan yang berbeda letak geografisnya dan dapat dilakukannya dengan baik. Keamanan jaringan, PC, server-server, dan perangkat komputer Akan yang lainnya memang merupakan faktor yang cukup penting untuk diperhatikan saat ini. Jika

P-ISSN :2580-4316
E-ISSN :2654-8054 10.37817/ikraith-informatika.v9i2

beberapa dekade yang lalu keamanan jaringan masih ditempatkan pada urutan prioritas yang rendah, namun akhir-akhir ini perilaku tersebut harus segera diubah. Pasalnya, kejahatan dengan menggunakan bantuan komputer, media komunikasi, dan perangkat elektronik lainnya meningkat sangat tajam belakangan. Hal ini sangat kontras dengan perkembangan kebutuhan perangkat komputer untuk kehidupan sehari-hari yang juga semakin meninggi. Tidak hanya di dalam kegiatan bisnis saja, kehidupan rumah tangga pun sudah sangat relevan jika dilengkapi dengan sebuah komputer. Maka dari itulah, mengapa keamanan jarinngan publik dan PC menjadi begitu penting untuk diperhatikan saat ini.

Apalagi jika kebutuhannya sudah berhubungan dengan kegiatan bisnis, dan kegiatan bisnis tersebut banyak berhubungan dengan server yang dapat diakses dari mana saja atau dengan koneksi Internet yang aktif 24x7. Tentu keamanan komunikasi data harus menjadi prioritas nomor satu. Mengapa demikian, karena semua fasilitas tersebut bisa juga diartikan sebagai titik celah baru menuju ke jaringan pribadi akan. Akan tidak bisa membiarkan begitu saja perangkat komputer akan tanpa perlindungan dalam dunia Internet yang sebenarnya. Jika akan biarkan, tentu segala macam jenis pengganggu akan bercokol di komputer Akan. Mulai dari virus sampai hacker yang menanam backdoor akan menggunakan komputer Akan sebagai alat bersenang-senang.

Begitu juga dengan kebutuhan perusahaan. Perusahaan yang besar dan memiliki banyak cabang di lokasi yang berbeda tentu harus dapat memonitor cabang perusahaanya. Dengan perkembangan teknologi dan jarinngan publik sekarang, perusahaan induk tersebut tidak harus langsung datang ke lokasi perusahaan cabang untuk mengecek keadaan perusahaan cabangnya, namun dengan manfaat jaringan computer perusahaan induk dapat langsung memeriksa keadaan perusahaan cabangnya tanpa datang langsung ke lokasinya. Perusahaan cabang dapat melakukan *sharing* datang ke perusahaan induk. Begitu juga dengan perusahaan induk.

Namun, dampak dari perkembangan itu adalah semakin banyaknya permasalahan yang muncul dalam melindungi jarinngan publik dari gangguan luar seperti virus, spam, DOS, dll.

Oleh karena itu, sebuah jarinngan publik pun perlu memiliki ’pagar’ layaknya sebuah rumah. ’Pagar’ yang dapat melindungi tempat vital dalam komunikasi data dan menyimpan komponen penting dalam jarinngan publik.

Dalam istilah komputer, ’pagar’ tersebut sering disebut dengan istilah firewall.

Sebuah sistem yang mengizinkan paket data lewat untuk paket yang dianggapnya aman dan menolaknya jika paket data tersebut dianggap tidak aman.

II **LAKANSAN TEORI**

II. 1 Pengertian Firewall

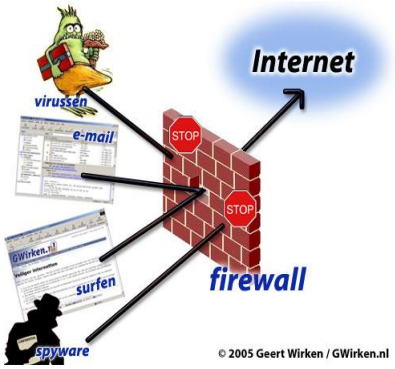
"Firewall adalah sebuah sistem atau perangkat yang mengizinkan lalu lintas jaringan yang dianggap aman untuk melaluinya dan mencegah lalu lintas jaringan yang tidak aman. Umumnya, sebuah firewall diimplementasikan dalam sebuah mesin terdedikasi, yang berjalan pada pintu gerbang (gateway) antara jaringan lokal dan jaringan lainnya. Firewall umumnya juga digunakan untuk mengontrol akses terhadap siapa saja yang memiliki akses terhadap jaringan pribadi dari pihak luar. Saat ini, istilah firewall menjadi istilah generik yang merujuk pada sistem

P-ISSN :2580-4316
E-ISSN :2654-8054

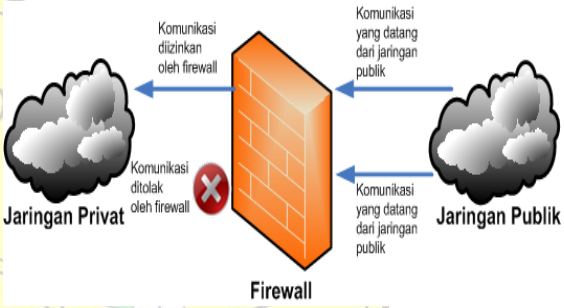
yang mengatur komunikasi antar dua jaringan yang berbeda. Mengingat saat ini banyak perusahaan yang memiliki akses ke Internet dan juga tentu saja jaringan korporat di dalamnya, maka perlindungan terhadap aset digital perusahaan tersebut dari serangan para hacker, pelaku spionase, ataupun pencuri data lainnya, menjadi esensial."

Sumber :
http://id.wikipedia.org/wiki/Firewall

Jadi firewall adalah suatu mekanisme untuk melindungi keamanan jarinngan publik dengan menyaring paket data yang keluar dan masuk di jaringan. Paket data yang '*baik'* diperbolehkan untuk melewati jaringan dan paket dapa yang dianggap *'jahat'* tidak diperbolehkan melewati jaringan. Firewall dapat berupa perangkat lunak atau perangkat keras yang ditanam perangkat lunak yang dapat menfilter paket data. Firewall dapat juga berupa suatu sikap yang ditanam dan diajarkan kepada staf IT suatu perusahaan untuk tidak membocorkan data perusahaan kepada perusahaan. Ini untuk mencegah salah satu jenis hacking yaitu *social enggeneering*. Ataupun memberi kunci pengaman pada alat-alat komputer dan jaringan, contohnya memasukan server ke dalam ruangan khusus dan dikunci. Kunci ruangan tersebut hanya dipegang oleh staf IT dan diperbolehkan menggunakan ruang tersebut atas seizin staf IT. Ini berfungsi selain menjaga kehilangan alat komputer dan jaringan secara fisik oleh pencuri atau perampokan, namun juga berfungsi menjaga kehilangan data yang tersimpan pada alat komputer tersebut. Bisa saja seseorang mencuri dan menghapus data penting perusahaan. Tentunya ini sangat merugikan perusahaan tersebut.



Gambar ilustrasi firewall 1



Gambar ilustrasi firewall 2

How to make Firewall ?

Firewall bisa didapatkan dengan berbagai cara. Jika tidak ingin repot-repot membuat dari nol, maka harus mengeluarkan uang yang cukup banyak untuk membeli perangkat keras firewall yang sudah jadi dan tinggal pasang saja di jaringan. Tetapi perlu diingat, tidak semua perangkat keras firewall dapat bekerja hebat dalam melakukan IP filtering. Jadi akan percuma saja uang yang akan dikeluarkan jika akan membeli firewall.

Jika mau sedikit repot, namun hasilnya mungkin akan memuaskan, buat saja sendiri perangkat firewall. Yang diperlukan hanyalah sebuah PC dengan processor dan memory yang lumayan besar dan sebuah aplikasi firewall yang canggih dan lengkap yang dapat memenuhi semua kebutuhan yang diperlukan. Aplikasi

P-ISSN :2580-4316
E-ISSN :2654-8054 10.37817/ikraith-informatika.v9i2

firewall yang lengkap dan canggih pada umumnya juga mengharuskan untuk mengeluarkan kocek yang tidak sedikit. Seperti misalnya Checkpoint yang sudah sangat terkenal dalam aplikasi firewall, untuk memilikinya akan harus merogoh kocek yang lumayan banyak pula.

Namun jika pecinta produk-produk open source dan sudah sangat familiar dengan lingkungan open source seperti misalnya operating system Linux, ada satu aplikasi firewall yang sangat hebat. Aplikasi ini tidak hanya canggih dan banyak fasilitasnya, namun aplikasi ini juga tidak akan membuat kantong Akan dirogoh dalam-dalam. Bahkan Akan bisa mendapatkannya gratis karena aplikasi ini pada umumnya merupakan bawaan default setiap distro Linux. Aplikasi dan system firewall di sistem open source tersebut dikenal dengan nama IPTables.

Dengan menggunakan IPTables, Akan dapat membuat firewall yang cukup canggih dengan program open source yang bisa dengan mudah didapatkan di Internet. Memang perlu diakui, firewall dengan menggunakan IPTables cukup sulit bagi pemula baik di bidang networking maupun pemula di bidang operating system Linux. Namun jika akan mempelajari lebih lanjut, sebenarnya firewall ini memiliki banyak sekali fitur dan kelebihan yang luar biasa.

II. 2 Fungsi Firewall

Fungsi firewall, antara lain :

1. Mengontrol dan mengawasi paket data yang mengalir di jaringan

   Firewall harus dapat mengatur, memfilter dan mengontrol lalu lintas data yang diizin untuk mengakses jaringan privat yang dilindungi firewall. Firewall harus dapat melakukan pemeriksaan terhadap paket data yang akan melawati jaringan privat.

   Beberapa kriteria yang dilakukan firewall apakah memperbolehkan paket data lewati atau tidak, antara lain :

   a. Alamat IP dari komputer sumber
   b. Port TCP/UDP sumber dari sumber
   c. Alamat IP dari komputer tujuan
   d. Port TCP/UDP tujuan data pada komputer tujuan
   e. Informasi dari header yang disimpan dalam paket data
2. Melakukan autentifikasi terhadap akses.
3. Applikasi proxy

   Firewall mampu memeriksa lebih dari sekedar header dari paket data, kemampuan ini menuntut firewall untuk mampu mendeteksi protokol aplikasi tertentu yang spesifikasi
4. Mencatat semua kejadian di jaringan

   Mencatat setiap transaksi kejadian yang terjadi di firewall. Ini memungkinkan membantu sebagai pendeteksian dini akan kemungkinan penjebolan jaringan.

II. 3 Cara Kerja Firewall

Cara kerja firewall pada umumnya :

Cara-cara firewall dalam melindungi jarinngan publik internal, antara lain :

1. Menolak dan memblokir paket data yang datang berdasarkan sumber dan tujaun yang tidak diinginkan.
2. Menolak dan menyaring paket data yang berasal dari jaringan intenal ke internet. Contoh nya

10.37817/ikraith-informatika.v9i2
P-ISSN :2580-4316
E-ISSN :2654-8054

ketika ada pengguna jaringan internel akan mengakses situs-situs porno.

3. Menolak dan menyaring paket data berdasakan konten yang tidak diinginkan. Misalnya firewall yang terintegrasi pada suatu antivirus akan menyaring dan mencegah file yang sudah terjangkit virus yang mencoba memasuki jaringan internal.
4. Melaporkan semua aktivitas jaringan dan kegiatan firewall.

II. 4 Tipe-tipe Firewall

Tipe-tipe Firewall, antara lain

1. Packet-Filtering Firewall

   Packet-Filtering Firewall adalah tipe firewall yang memeriksa dan membandingkan alamat sumber dari paket lewat dengan aturan atau kebijakan yang telah terdaftar pada filtering firewall. Pada firewall tipe ini akan diatur apakah paket data tersebut akan diperbolehkan lewat atau menolaknya.

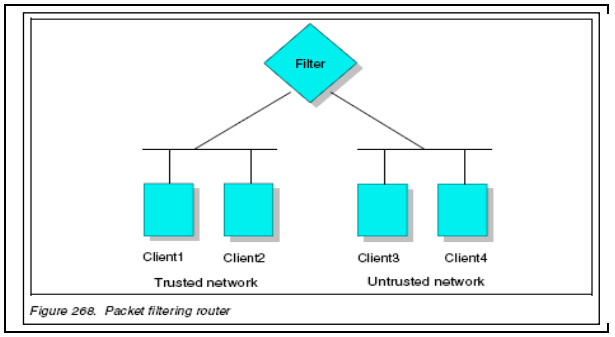
   Aturan atau kebijakan pemeriksaan didasarkan informasi yang dapat ditangkap dari packet header, yaitu antara lain :

   a. IP address sumber dan tujuan
   b. Nomor port TCP/UDP sumber dan tujuan
   c. Tipe ICMP message

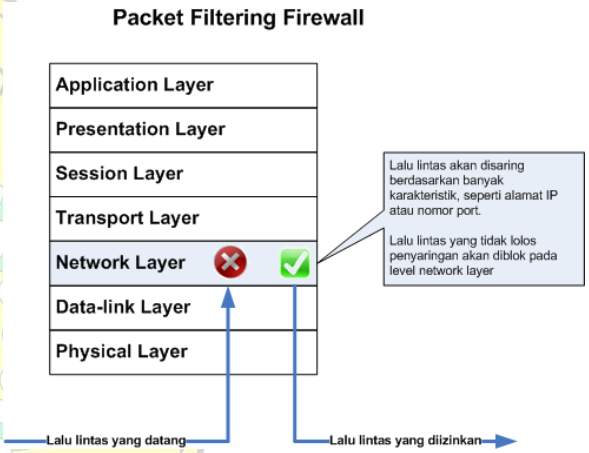
   Contoh aturan atau kebijakan packet filtering firewall :

from	to	src port	dst port	proto	rule
*	www	*	80	tcp	allow
*	mail-gw	*	25	tcp	allow
squids	proxy	*	8080, 3128	*	allow
mynet	*	*	*	*	allow
*	*	*	*	*	deny

Gambar contoh rule packet filtering firewall



Gambar Ilustrasi cara kerja packet filtering firewall



Gambar ilustrasi packet filtering firewall

Contoh satu aturan pada firewall jenis adalah melakukan penonaktifan port 23 yaitu protokol yang digunakan untuk telnet. Ini bertujuan untuk mencegah pengguna internet untuk mengakses layanan yang terdapat pada jaringan yang di firewallkan. Firewall ini juga dapat melakukan pengecualian terhadap aplikasi-aplikasi yang dapat berdapat berjalan di jaringan. Inilah salah satu kerumitan pada packet filtering tipe firewall, dikarena sulitnya menbuat aturan atau kebijakan yang akan diberlakuan untuk firewall.

P-ISSN :2580-4316
E-ISSN :2654-8054
10.37817/ikraith-informatika.v9i2

Kelebihan packet filtering firewall antara lain relatif mudah dalam pengimplementasikannya, tranparan untuk pengguna, dan relatif lebih cepat.

Adapun kekurangan tipe firewall ini antara lain sulit dalam membuat aturan dan kebijakan pada packet filtering firewall ini secara tepat guna dan aturan tersebut akan semakin banyak seiiring dengan banyak alamat IP sumber dan tujuan, port sumber dan tujuan yang dimasukan dalam kebijakan packet filtering firewall ini.

2. Application-Level Gateway (Proxy)

Application-levet gateway sering juga disebut application level firewall atau proxy firewall. Firewall ini tidak memperbolehkan paket data yang datang untuk melewati firewall sacara langsung. Applicatin level gateway menyediakan kontrol tingkat tinggi pada traffic antara dua jaringan yang isi layanan tertentu didalamnya dapat dimonitor dan difilter sesuai dengan kebijakan keamanan jaringan. Firewall tipe ini akan mengatur semua yang berkaitan dengan layer aplikasi, seperti ftp, telner, dll.

Kebanyakan, proxy firewall ini akan melakukan autentifikasi terhadap pengguna sebelum pengguna dapat melewati jaringan. firewall ini juga melakukan mekanisme pencatatan (logging) sebagai bagian dari aturan dan kebijakan keamanan yang diterapkannya. Contohnya apabila ada pengguna salah satu aplikasi seperti telnet untuk mengakses secara remote, maka gateway akan meminta pengguna untuk memasukan alamat remote host. Ketika pengguna mengirimkan username dan password serta informasi lain maka gateway akan melakukan pemeriksaan dan melakukan hubungan terhadap aplikasi tersebut yang sesuai dengan remote host. Apabila tidak sesuai, firewall tidak akan meneruskan dan menolak data tersebut.

Ilustrasi cara kerja application layer firewall

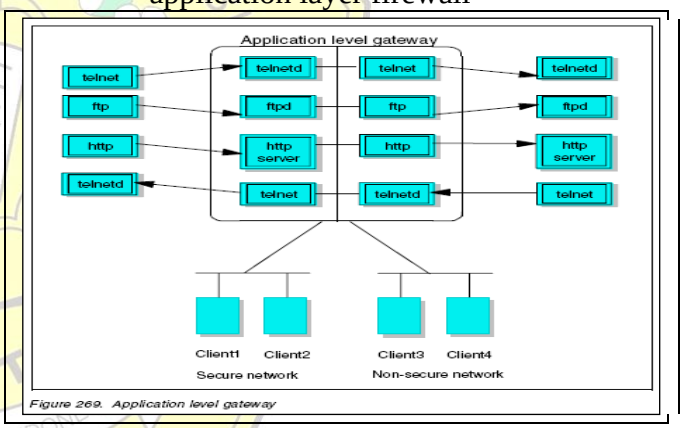
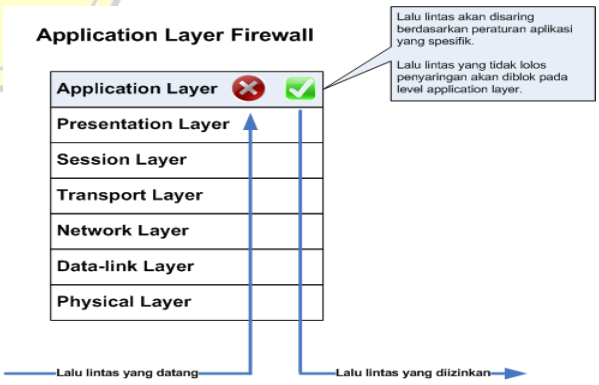


Figure 269. Application level gateway



Gambar ilustrasi application layer firewall

Kelebihan application layer firewall antara lain : relatif lebih aman dibandingkan

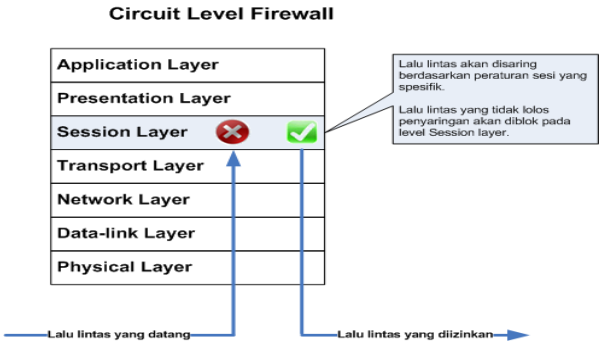
dengan packet filtering firewall, adanya pencatatan log setiap transaksi yang terjadi pada level aplikasi.

Kekurangan application layer firewall antara lain : pemrosesan tambahan yang berlebih pada setiap hubungan yang akan mengakibatkan terdapat dua buah sambungan koneksi antara pengguna dan gateway, dimana gateway akan memeriksa dan meneruskan semua arus dari dua arah.

3. Circuit Level Gateway

Circuit lavel gateway dapat dikatakan sebagai tipe khusus dari proxy karena proxy dapat dikonfigurasi untuk melewatkan semua informasi pengguna yang sudah di authentifikasi sebagai circuit level gatewai. Circuit level gateway meng*handle* koneksi TCP dan tidak menyediakan paket tambahan seperti prosessing atau filtering. Firewall jenis akan menyembunyikan jaringan dari pengguna ketika koneksi akan terjadi dari pengguna. Pengguna akan berhadapan langsung dengan firewall pada saat proses pembuatan koneksi dan firewall akan membentuk koneksi dengan sumber daya di jaringan yang hendak di akses oleh pengguna setelah mengubah alamat IP dari paket yang ditransmisikan oleh dua belah pihak

Firewall jenis ini bekerja pada lapisan session layer.



Kelebihan firewall jenis ini antara lain lebih aman dibandingkan dengan jenis packet filtering firewall karena pengguna luar tidak dapat melihat alamat IP jaringan internal dalam paket-paket yang ia terima, melainkan alamat IP dari firewall. Protokol yang populer digunakan sebagai Circuit-Level Gateway adalah SOCKS v5.

Ilustrasi Circuit Level Gateway

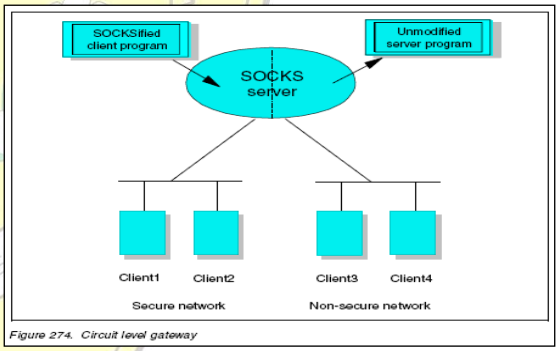


Figure 274. Circuit level gateway

Why IPTABLES ?

IPTables merupakan sebuah fasilitas tambahan yang tersedia pada setiap perangkat komputer yang diinstali dengan sistem operasi Linux dan resmi diluncurkan untuk massal pada LINUX 2.4 kernel pada January 2001 (www.netfilter.org). Akan harus mengaktifkannya terlebih dahulu fitur ini pada saat melakukan kompilasi

P-ISSN :2580-4316
E-ISSN :2654-8054 10.37817/ikraith-informatika.v9i2

kernel untuk dapat menggunakannya. IPTables merupakan fasilitas tambahan yang memiliki tugas untuk menjaga keamanan perangkat komputer akan dalam jaringan. Atau dengan kata lain, IPTables merupakan sebuah firewall atau program IP filter build-in yang disediakan oleh kernel Linux untuk tetap menjaga agar perangkat akan aman dalam berkomunikasi.

Mengapa Linux bersusah payah menyediakan fasilitas ini untuk Akan? Karena dari dulu Linux memang terkenal sebagai operating system yang unggul dalam segi keamanannya. Mulai dari kernel Linux versi 2.0, Linux sudah memberikan fasilitas penjaga keamanan berupa fasilitas bernama ipfwdm. Kemudian pada kernal 2.2, fasilitas bernama ipchain diimplementasikan di dalamnya dan menawarkan perkembangan yang sangat signifikan dalam menjaga keamanan.

Sejak kernel Linux memasuki versi 2.4, sistem firewall yang baru diterapkan di dalamnya. Semua jenis firewall open source yang ada seperti ipfwadm dan ipchains dapat berjalan di atasnya. Tidak ketinggalan juga, IPTables yang jauh lebih baru dan canggih dibandingkan keduanya juga bisa berjalan di atasnya. Maka itu, IPTables sangatlah perlu untuk dipelajari untuk Akan yang sedang mempelajari operating system Linux atau bahkan yang sudah menggunakannya. Karena jika menguasai IPTables, mengamankan jaringan Akan atau jaringan pribadi orang lain menjadi lebih hebat.

Fitur yang dimiliki IPTables:

1. Connection Tracking Capability yaitu kemampuan unutk inspeksi paket serta bekerja dengan icmp dan udp sebagaimana koneksi TCP.
2. Menyederhanakan perilaku paket-paket dalam melakukan negosiasi built in chain (input,output, dan forward).
3. Rate-Limited connection dan logging capability. Kita dapat membatasi usaha-usaha koneksi sebagai tindakan preventif serangan Syn flooding denial of services(DOS).
4. Kemampuan untuk memfilter flag-flag dan opsi tcp dan address-address MAC.

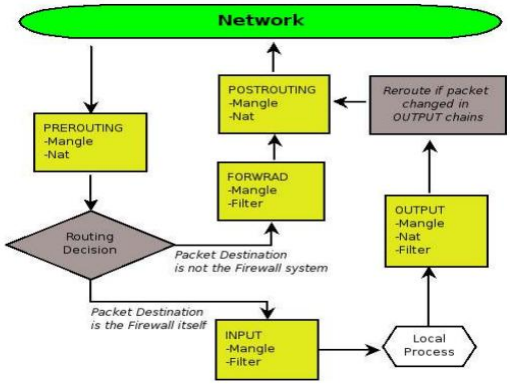
III. Pembahasan

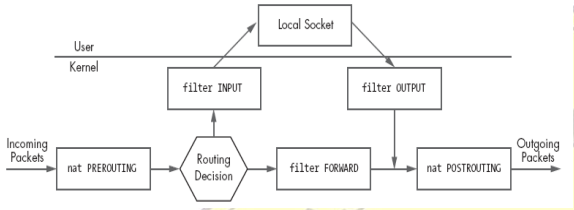
III. 1 Pengenalan Iptables

Iptables adalah salah satu tools firewall default pada system operasi linux. Iptables ini bekerja baik di kernel 2.4.x-2.6.x sedangkan untuk kernel 2.2.x masih menggunakan ipchains. Perintah 'iptables' digunakan untuk mengelola, memaintain, menginspeksi rule-rule IP packet filter dalam kernel linux.

Diagram Iptables

P-ISSN :2580-4316
E-ISSN :2654-8054





Gambar Diagram Perjalanan Paket data pada IPTables

Konsep chain :

1. INPUT
   => semua paket yang masuk ke komputer melalui chain/rantai ini.
2. OUTPUT
   => semua paket yang kelua ke komputer melalui chain/rantai ini.
3. FORWARD
   =>paket data yang diterima dari satu jaringan dan diteruskan ke jaringan lainya.

Perintah umum iptables :

$iptables [-t table] command [match] [target/jump]

Berikut beberapa option dasar yang cukup sering dalam mengkonfigurasi iptables :

- -A
  Tambahan aturan ini ke rantai aturan yang ada. Rantai atau chain yang valid adalah INPUT, FORWARD, dan OUTPUT. Biasanya lebih banyak menggunakan rantai INPUT yang berdampak pada paket data yang masuk
- -L
  Memperlihatkan daftar aturan yang telah dipasang di iptables.
- -m state
  Menjelaskan daftar dari kondisi / state bagi aturan untuk di bandingkan. Beberapa state yang valid, adalah :
  NEW => sambungan baru dan belum pernah terlihat sebelumnya
  RELATED => sambungan baru, tapi berhubungan dengan sambungan lain telah diizinkan.
  ESTABLISHED => sambungan yang telah terjadi.
  INVALID => lalu lintas paket data yang karena berbagai alasan tidak bisa di identifikasi
- -m limit
  Dibutuhkan oleh aturan jika ingin melakukan pembandingan dan pencocokan dalam waktu / jumlah tertentu. Mengizinkan penggunaan option –limit. Berguna untuk membatasi aturan logging.
- --limit
  Kecepatan maksimum pencocokan, diberikan dalam bentuk angka yang diikuti oelh ”/seconf”,”/minute”,”/hour”, atau ”/day” tergantung seberapa

Pada jurnal ini , penulis mencoba berbagi sedikit cara mengkonfigurasi firewall pada iptables di sistem operasi linux, khususnya distribusi ubuntu. Penulis menggunakan Ubuntu 8.04 kernel 2.6.24-16-generic dalam mencoba iptables.

Pada ubuntu, biasa telah terinstall iptables secara default.

P-ISSN :2580-4316
E-ISSN :2654-8054 10.37817/ikraith-informatika.v9i2

sering kita ingin melakukan pencocokan aturan. Jika option ini tidak digunakan maka secara defaultnya adalah ”3/hour”

- -p
  Protokol yang digunakan untuk sambungan.
- --dport
  Port tujuan yang digunakan oleh aturan iptables. Bisa berupa satu port, bisa juga satu batasan jangkauan ditulis sebagai start:end, yang akan mencocokan semua port start sampai end
- -j
  Jump ke target yang spesifik. Iptables mempunyai empat target default, yaitu :

  ACCEPT
  ⇨ Accept / menerima paket dan berhenti memproses aturan dalam rantai aturan ini.

  REJECT
  ⇨ Reject /tolak paket data dan beritahu ke pengirim bahwa aturan firewall menolak paket data tersebut, stop pemrosesan aturan dalam rantai aturan ini

  DROP
  ⇨ Diam-diam mengacuhkan paket ini, dan stop pemrosesan aturan di rantai aturan ini.

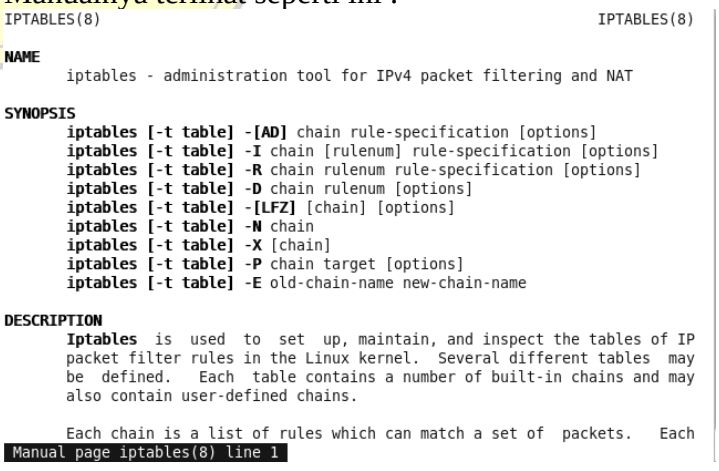
  LOG
  ⇨ Log/catat paket, dan teruskan pemrosesan aturan di rantai aturan ini.
  ⇨ Mengijinkan penggunaan option --log –prefix dan --log -level
- --log –prefix
  Jika pencatatan dilakukan, letakan text atau tulisan sebelum catatan.
- --log –level
  Pencatatan menggunakan syslog level.
- -i
  Melakukan pencocokan jika paket yang masuk dari interface tertentu.
- -I
  Memasukan aturan ke iptables.
- -v
  Menampilkan lebih banyak informasi di layar

Option diatas adalah hanya sedikit dari option yang terdapat pada iptables. Silakan pembaca kembangan sendiri.

Untuk dapat melihat *manual* iptables, silakan ketik perintah ini pada terminal :

$man iptables

Manualnya terlihat seperti ini :



Perintah dasar Iptables :

10.37817/ikraith-informatika.v9i2
P-ISSN :2580-4316
E-ISSN :2654-8054

1. Untuk melihat aturan yang sudah ada di iptables :

   $iptables -L

   Jika komputer baru diinstall, aturan yang terpasang akan terlihat seperti ini :

```
root@ladast-laptop:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

2. mengijinkan sesi sambungan yang terbentuk untuk menerima lalu lintas paket data

   $iptables -A INPUT -m state –state ESTABLISHED, RELATED -j accept

   Contohnya akan mengijinkan semua lalu lintas paket data di jaringan untuk masuk adalah sebagai berikut :

   $iptables -A INPUT -p tcp –dport 80 -j ACCEPT

```
root@ladast-laptop:~# iptables -A INPUT -p tcp --dport 80 -j ACCEPT
root@ladast-laptop:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:www

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

   Contohnya lain akan mengijinkan lalu lintas paket data masuk ke defaut port SSH nomor 22, maka harus mengizinkan semua TCP paket data masuk ke port 22, perintahnya :

   $iptables -A INPUT -p tcp --dport ssh -j ACCEPT

```
root@ladast-laptop:~# iptables -A INPUT -p tcp --dport ssh -j ACCEPT
root@ladast-laptop:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:www

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

   Dari perintah diatas, kita dapat mengetahui bahwa aturan iptables tersebut mangatur agar masukan aturan ini ke rantai input (-A INPUT) artinya kita melihat lalu lintas paket data yang masuk cek protokol yang digunakan adalah TCP (-p tcp). Jika TCP, apakah paket data menuju port SSH (--dport ssh). Jika ya, maka paket diterima,

3. Untuk melakukan pemblokiran paket data.

   Apabila aturan telah memutuskan untuk menerima paket data (ACCEPT), maka aturan selanjutnya tidak akan berefek pada paket data tersebut. Karena aturan yang kita buat mengijinkan SSH dan Web traffic, selama aturan untuk memblok semua traffic kita letakan terakhir sesudah aturan mengijinkan SSH dan Web, maka kita akan tetap dapat menerima traffic SSH dan Web yang kita inginkan. Jadi kita harus menambahkan (-A) aturan untuk mem-block traffic di akhir.

   Perintahnya :

   $iptables -A INPUT -j DROP

```
root@ladast-laptop:~# iptables -A INPUT -j DROP
root@ladast-laptop:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:www
DROP       all  --  anywhere             anywhere
DROP       all  --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

P-ISSN :2580-4316
E-ISSN :2654-8054 10.37817/ikraith-informatika.v9i2

4. Untuk melakukan pencatatan paket yang di log , perintah yang paling cepat adalah :

   $iptables -I INPUT 5 -m limit --limit 5/min -j LOG --log-prefix "iptables denied: " --log-level 7

5. Untuk menyimpan konfigurasi iptables

   Jika akan *booting* komputer yang digunakan, maka apa yang dilakukan ini akan hilang. itupun harus mengetikkan ulang semua perintah yang dimasukan satu per satu ketika komputer hidup. Agar lebih effesien, mK dapat menggunakan iptables-save dan iptables-restore untuk menyimpan dan me*restore* iptables

   Selanjutnya dapat menyimpan konfigurasi iptables agar di start setiap kali booting menggunakan perintah : $sh -c "iptables-save > /etc/iptables.rules"

   Setelah itu memodifikasi /etc/network/interfaces agar aturan iptables yang digunakan dapat berjalan secara automatis. Maka perlu mengetahui ke interface mana aturan yang akan digunakan. Biasanya menggunakan eth0. Untuk interface wireless, kita dapat mencek penggunaaannya mengunakan perintah,

   $ iwconfig

   Kemudian perlu mengedit file /etc/network/interfaces misalnya menggunakan perintah

   $ sudo nano /etc/network/interfaces

   Apabila telah menemukan nama interface yang digunakan, maka di akhir interface kita dapat menambahkan perintah,
   pre-up iptables-restore < /etc/iptables.rules
   Selanjutnya di bawahnya kita tambahkan perintah sesudah interface down, menggunakan perintah,
   post-down iptables-restore < /etc/iptables.rules

   Hasil gambarnya :

6. Untuk menonaktifkan atau mematikan fiewall, maka perintahnya :

   $iptables –F

   Perintahnya akan seperti dibawah ini :

Adapun jika kesulitan dalam menkonfigurasi iptables secara *command line*, pada ubuntu telah tersedia perangkat lunak yang dapat mengkonfigurasi firewall secara menggunakan GUI yaitu firestater.

IV. KESIMPULAN

Tidak ada satupun sistem buatan manusia yang dikatakan aman. Namun firewall adalah salah satu cara untuk melindungi jaringan dari pihak

luar yang akan berbuat jahat ataupun iseng. Dengan membuat aturan dan kebijakan pada firewall secara tepat setidaknya dapat melindungi jaringan dari ganggaun pihak luar. Firewall juga mencatat semua kejadian di jaringan sehingga dapat melakukan pendeteksian dini terhadap segala serangan yang mengancam di jaringan.

Iptables merupakan salah satu perangkat lunak firewall yang bekerja pada sistem operasi linux. Walaupan bersifat *free*,namun iptables cukup *powerfull* asalkan aturan dan kebijakan yang diterapkan di firewall tersebut sangat tepat dalam melindungi jaringan.

Di dalam penulisan jurnal ini, penulis hanya sedikit memberikan penjelasan mengenai iptables. Penulis menyerahkan kepada pembaca untuk dapat berkreasi dan mengembangkan lagi mengenai firewall dan pada iptables ini. Penulis memberikan solusi IPTables sebagai Firewall karena memiliki beberapa keunggulan:

1. Implementasinya yang murah karena telah terdapat pada Linux System Version 2.4 dan gratis.
2. Connection Tracking Capability yaitu kemampuan unutk inspeksi paket serta bekerja dengan icmp dan udp sebagaimana koneksi TCP.
3. Menyederhanakan perilaku paket-paket dalam melakukan negosiasi built in chain (input,output, dan forward).
4. Rate-Limited connection dan logging capability. Kita dapat membatasi usaha-usaha koneksi sebagai tindakan preventif serangan Syn flooding denial of services(DOS).
5. Kemampuan untuk memfilter flag-flag dan opsi tcp dan address-address MAC.

Daftar Pustaka

Pribadi, Harijanto.2008.*Firewall melindungi jaringan dari DdoS menggunakan LINUX+MIKROTIK*. Penerbit Andi : Yogyakarta.

Michael Rash, *Linux Firewalls.* William Pollock Publishing, 2007

Deris Stiawan, *Sistem Keamanan Komputer*. Elex media Komputindo, 2005

Janner Simarmata, *Pengamanan istem Keamanan Komputer*. Penerbit ANDI , 2006

Rakhmat Farunuddin, *Membangun Firewall dengan IPTables di Linux.* Elex Media Komputindo,

Aswin Dwiyono, Pengenalan Firewall dab IPTables pada jarinngan publik, universitas sriwijaya, 2008

Ahmad Muammar. W. K.2004. *FireWall*. Ilmukomputer.com

JiroKul. Bermain dengan Firewall Default.Terbitan Online Kecoak Elektronik

http://k-elektronik.org

http://ezine.echo.or.id

Sriwijaya, Riki.2003.Firewall. ilmukomputer.com

FIREWALL.IDS.INDOCISC/BIN

http://id.wikipedia.org/wiki/Firewall

http://linux.or.id/node/2929

http://students.ukdw.ac.id/%7E22022807/kommasd.html

http://dwiyatmoko.multiply.com/journal

http://sdn.vlsm.org/share/ServerLinux/node161.html