SISTEM KEAMANAN INTERNET DENGAN MENGGUNAKAN IPTABLES SEBAGAI FIREWALL

Sujito[1], Mukhamad Fatkhur Roji[2]

[1]Dosen Program Studi Sistem Informasi STMIK Pradnya Paramita
[2] Mahasiswa Program Studi Teknik Informatika STMIK Pradnya Paramita

ABSTRAK

Perkembangan teknologi jaringan terutama teknologi internet, menuntut setiap institusi pendidkan untuk menyediakan fasilitas internet yang memadai. SMK Negeri 8 Malang, sebagai institusi pendidikan, memahami bahwa kebutuhan teknologi internet mutlak dibutuhkan, di lingkungan pendidikan dengan segala keterbatasan yang ada.

Oleh karena itu, penelitian ini bertujuan untuk membatu lingkungan pendidikan, terutama SMK Negeri 8 malang, dalam mengatasi beberapa kendala pada sistem kemanan jaringan. Pemakaian firewall adalah salah satu cara dalam mengatasi lemahnya sistem keamanan jaringan, terutama pada institusi pendidikan.

***Kata kunci** : Iptables, Firewall, Chain*

ABSTRACT

Growth networking technology especially internet technology, demand for every institution of education to prepare requirements of internet facility. Public Vocational High School 8 Malang, like institution of education, understanding if requirements of internet technology is absolutly needed, in education environment wich all limitation.

By because that, this research have to support education environment, especially Public Vocational High School 8 Malang, for solving several constraint at internet security sistem. Usage of firewall be one of method for solving of low networking security sistem, especially in institution of education.

***Keyword** : Iptables, Firewall, Chain*

PENDAHULUAN

Sejak memasyarakatnya internet dan dipasarkannya beberapa sistem operasi baik yang *close source* maupun *open source,* membangun sebuah jaringan komputer merupakan suatu yang biasa. Demikian pula penerapan konsep *downsizing* maupun *lightsizing*, yang bertujuan menekan anggaran belanja (efisiensi anggaran), khususnya dalam peralatan komputer.

Internet merupakan sebuah jaringan komputer yang sangat terbuka di dunia, konsekuensi yang harus ditanggung adalah tidak ada jaminan keamanan bagi jaringan yang terhubung ke internet. Artinya jika operator jaringan tidak hati-hati dalam menset-up sistemnya, maka kemungkinan besar jaringan yang terhubung ke internet, akan dengan mudah dimasuki orang yang tidak berhak dari luar. Adalah tugas dari operator jaringan yang bersangkutan, untuk menekan resiko seminimal mungkin. Pemilihan strategi dan kecakapan administrator jaringan berpengaruh besar terhadap keamanan jaringan.

Hal yang juga perlu dipertimbangkan, adalah kemampuan dari administrator, dalam memaksimalkan jaringan internet yang ada. Sebesar apapun *bandwidth* yang disediakan, tidak akan terlalu berarti, apabila tidak ada pengaturan pemakaian atau hak akses bagi pengguna atau *user*. Disamping itu, dengan banyaknya fasilitas yang disediakan oleh internet (*browsing, chatting, download, facebook, game online, bloging*, dan lain-lain), memerlukan pengaturan yang tepat, agar jaringan yang dikelola berjalan dengan baik.

Jaringan internet yang sudah ada di Sekolah Menengah Kejuruan Negeri 8 Malang (SMKN 8 Malang), masih memiliki beberapa kendala, diantaranya; desain sistem jaringan yang kurang memadai, penggunaan hardware yang tidak sebanding dengan padatnya arus komunikasi data, *bandwidth* yang tersedia kurang memadai dibanding dengan jumlah pengguna, perilaku pengguna (sebagian besar siswa) yang menggunakan fasilitas internet diluar bidang pendidikan dan ilmu pengetahuan (*download music/ film, games online,* situs porno, dan lain-lain), serta keamanan jaringan internet yang kurang memadai. Dengan adanya kendala tersebut, mengharuskan administrator melakukan pembatasan-pembatasan akses, agar fasilitas yang sudah ada dapat dipergunakan sesuai dengan koridor yang sudah ada. Hal ini bisa diatasi dengan menambah perangkat *PC Firewall* pada jaringan internet yang sudah ada.

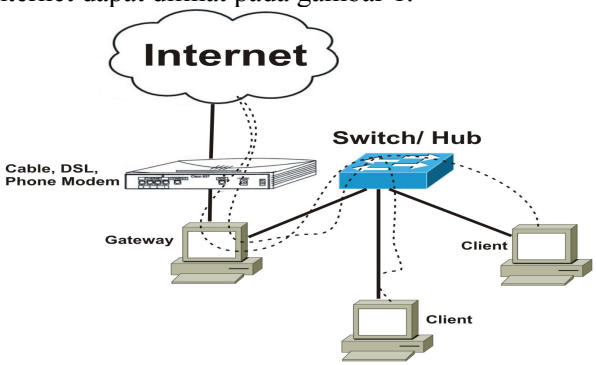
Berdasarkan kondisi tersebut, penelitian ini dilaksanakan untuk menjawab pertanyaan bagaimana merancang dan mengimplementasikan sistem firewall yang sesuai dengan kebutuhan di SMK Negeri 8 Malang?. Sehingga tujuan dari penelitian ini adalah, terwujudnya rancangan sistem firewall yang berfungsi untuk memaksimalkan sistem keamanan jaringan pada lembaga pendidikan, khususnya di SMKN 8 Malang. Dengan memberikan regulasi-regulasi yang sesuai dengan kapasitasnya sebagai lembaga pendidikan, sehingga tujuan penggunaan media internet sesuai dengan tujuan dunia pendidikan.

KAJIAN TEORI

Jaringan komputer merupakan suatu koleksi komputer-komputer terpisah yang berkomunikasi satu dengan lainnya memanfaatkan media komunikasi yang dipakai bersama-sama.

LAN (*Local Area Network*) merupakan komunikasi sejumlah komputer di dalam suatu area terbatas, di mana satu komputer dengan komputer lain umumnya terkoneksi melalui media kabel maupun *wireless*/gelombang radio. Sedangkan WAN (*Wide Area Network*) adalah komunikasi antar LAN, antara satu LAN dengan LAN lain dipisahkan oleh jarak yang cukup jauh, misalnya antar gedung, antar sekolah yang terhubung melalui media telepon, kabel, satelit, gelombang radio atau media lainnya.

LAN juga dapat dikatakan sebagai jaringan yang dikhususkan untuk suatu area geografis, misalnya di sebuah gedung atau kampus. LAN dapat berbentuk jaringan kecil yang hanya menghubungkan 2 atau 3 komputer, tetapi sering juga digunakan untuk menghubungkan ratusan komputer yang digunakan oleh banyak orang sebagaimana dapat dijumpai di beberapa *internet center* di Indonesia dan luar negeri. Secara garis besar komponen-komponen LAN yang terkoneksi ke internet dapat dilihat pada gambar 1.



Gambar 1: LAN yang terkoneksi ke internet

Terdapat tiga peran yang dapat dijalankan oleh komputer-komputer di dalam *Local Area Network* (LAN). Peran pertama adalah menjadi *client*, hanya sebagai pengguna tetapi tidak menyediakan sumber daya jaringan untuk dipakai oleh anggota jaringan lain. Peran kedua adalah menjadi peer, menjadi client yang menggunakan sekaligus menyediakan sumber daya jaringan, disebut juga peer-to-peer. Peran terakhir adalah menjadi server yang menyediakan sumber daya jaringan.

Jaringan Berbasis Server

Jaringan berbasis server atau *client-server* didefinisikan dengan kehadiran server di dalam suatu jaringan yang menyediakan mekanisme pengamanan dan pengelolaan jaringan tersebut. Jaringan ini terdiri dari banyak *client* dan satu atau lebih server. *Client* yang juga biasa disebut *front-end*

meminta layanan seperti penyimpanan dan pencetakan data ke printer jaringan, sedangkan server yang sering disebut *back-end* menyampaikan permintaan tersebut ke tujuan yang tepat.

Jaringan Peer-to-Peer

Setiap komputer di dalam jaringan peer mempunyai fungsi yang sama dan dapat berkomunikasi dengan komputer lain yang telah memberikan izin. Jadi, secara sederhana, setiap komputer pada jaringan peer berfungsi sebagai client dan server sekaligus. Jaringan peer biasanya digunakan di sebuah kantor kecil dengan jumlah komputer sedikit, dibawah 10 workstation.

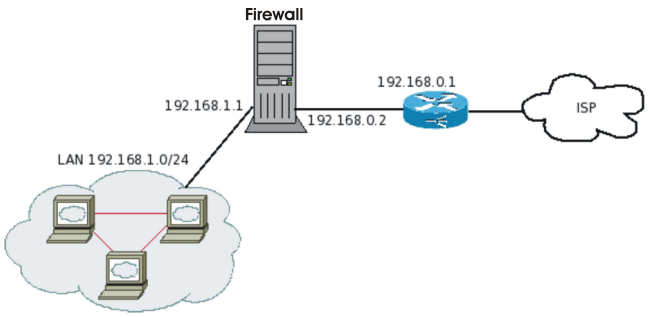
Jaringan Hybrid

Jaringan hybrid memiliki semua yang terdapat pada tiga tipe jaringan diatas. Ini berarti pengguna dalam jaringan dapat mengakses sumber daya yang di-*share* oleh jaringan peer, sedangkan di waktu yang bersamaan juga dapat memanfaatkan sumber daya yang disediakan oleh server.

Keuntungan jaringan hybrid adalah sama dengan keuntungan menggunakan jaringan berbasis server dan berbasis peer. Jaringan hybrid memiliki kekurangan seperti pada jaringan berbasis server.

Pengertian Firewall

Firewall merupakan suatu cara atau mekanisme yang diterapkan baik terhadap hardware, software ataupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan/kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkupnya. Segmen tersebut dapat merupakan sebuah *workstation, server, router*, atau *local area network* (LAN) anda. konfigurasi sederhana dari *firewall,* dapat dilihat pada gambar 2.



Gambar 2: Desain sederhana sebuah firewall

Firewall untuk komputer, pertama kali dilakukan dengan menggunakan prinsip "*non-routing*" pada sebuah Unix host yang menggunakan 2 buah *network interface card, network interface card* yang pertama di hubungkan ke internet (jaringan lain) sedangkan yang lainnya dihubungkan ke personal computer

(jaringan lokal) (dengan catatan tidak terjadi "route" antara kedua network interface card di PC ini). Untuk dapat terkoneksi dengan Internet (jaringan lain) maka harus memasuki *server firewall* (bisa secara remote, atau langsung), kemudian menggunakan resource yang ada pada komputer ini untuk berhubungan dengan Internet (jaringan lain), apabila perlu untuk menyimpan file/data maka dapat menaruhnya sementara di PC firewall anda, kemudian mengkopikannya ke PC (jaringan lokal). Sehingga internet(jaringan luar) tidak dapat berhubungan langsung dengan PC(jaringan lokal) .

Dikarenakan masih terlalu banyak kekurangan dari metoda ini, sehingga dikembangkan berbagai bentuk, konfigurasi dan jenis firewall dengan berbagai policy (aturan) didalamnya. Firewall secara umum di peruntukkan untuk melayani: (1) Mesin/Komputer, Setiap mesin/komputer yang terhubung langsung ke jaringan luar atau internet dan menginginkan semua yang terdapat pada komputernya terlindungi. (2) Jaringan, Jaringan komputer yang terdiri lebih dari satu buah komputer dan berbagai jenis topologi jaringan yang digunakan, baik yang di miliki oleh perusahaan, organisasi dsb.

Karakteristik Sebuah Firewall

a. Seluruh hubungan/kegiatan dari dalam ke luar, harus melewati firewall. Hal ini dapat dilakukan dengan cara memblok/membatasi baik secara fisik semua akses terhadap jaringan Lokal, kecuali melewati firewall. Banyak sekali bentuk jaringan yang memungkinkan agar konfigurasi ini terwujud.
b. Hanya Kegiatan yang terdaftar/dikenal yang dapat melewati/melakukan hubungan, hal ini dapat dilakukan dengan mengatur *policy* pada konfigurasi keamanan lokal. Banyak sekali jenis firewall yang dapat dipilih sekaligus berbagai jenis policy yang ditawarkan.
c. Firewall itu sendiri haruslah kebal atau relatif kuat terhadap serangan/ kelemahan. Hal ini berarti penggunaan sistem yang dapat dipercaya dan dengan sistem yang relatif aman.

Teknik Yang digunakan Oleh Sebuah Firewall

Ada empat teknik yang dapat digunakan oleh sebuah firewall, yaitu: *service control, direction control, user control* dan *behavior control.*

Service Kontrol (Kendali Terhadap Layanan), berdasarkan tipe-tipe layanan yang digunakan di Internet dan boleh diakses baik untuk kedalam ataupun keluar firewall. Biasanya firewall akan mencek no IP Address dan juga nomor port yang di gunakan baik pada protokol TCP dan UDP, bahkan bisa dilengkapi software untuk *proxy* yang akan menerima dan menterjemahkan setiap permintaan akan suatu layanan sebelum mengijinkannya. Bahkan bisa jadi software pada server itu sendiri, seperti layanan untuk web ataupun untuk mail.

Direction Control (kendali terhadap arah), berdasarkan arah dari berbagai permintaan (request) terhadap layanan yang akan dikenali dan diijinkan melewati firewall.

User control (kendali terhadap pengguna), Berdasarkan pengguna/user untuk dapat menjalankan suatu layanan, artinya ada user yang dapat dan ada yang tidak dapat menjalankan suatu servis,hal ini di karenakan user tersebut tidak di ijinkan untuk melewati firewall. Biasanya digunakan untuk membatasi user dari jaringan lokal untuk mengakses keluar, tetapi bisa juga diterapkan untuk membatasi terhadap pengguna dari luar.

Behavior Control (kendali terhadap perlakuan), Berdasarkan seberapa banyak layanan itu telah digunakan. Misalnya, firewall dapat memfilter email untuk menanggulangi/mencegah spam.

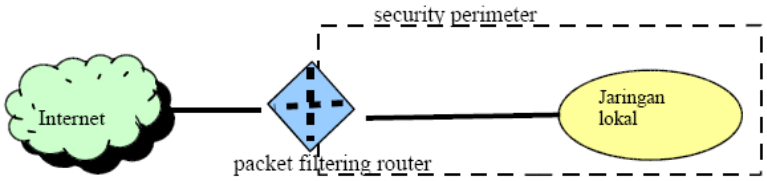
Tipe-Tipe Firewall

Berdasarkan tipenya firewall dapat diklasifikasikan menjadi 3 kelompok yaitu: *Packet Filtering Router, Application-Level Gateway*, dan *Circuit-level Gateway*.

Packet Filtering Router, Packet Filtering diaplikasikan dengan cara mengatur semua packet IP baik yang menuju, melewati atau akan dituju oleh packet tersebut. Pada tipe ini packet tersebut akan diatur apakah akan di terima dan diteruskan atau di tolak. Penyaringan packet ini di konfigurasikan untuk menyaring packet yang akan di transfer secara dua arah (baik dari dan ke jaringan lokal). Aturan penyaringan didasarkan pada header IP dan transport header, termasuk juga alamat awal (IP) dan alamat tujuan (IP), protokol transport yang di gunakan (UDP,TCP), serta nomor port yang digunakan. Kelebihan dari tipe ini adalah mudah untuk di implementasikan, transparan untuk pemakai, relatif lebih cepat. Adapun kelemahannya adalah cukup rumitnya untuk menyetting paket yang akan difilter secara tepat, serta lemah dalam hal authentikasi. Adapun serangan yang dapat terjadi pada firewall dengan tipe ini adalah:

- IP address spoofing : Intruder (penyusup) dari luar dapat melakukan ini dengan cara menyertakan/menggunakan ip address jaringan lokal yang telah diijinkan untuk melalui firewall.
- Source routing attacks : Tipe ini tidak menganalisa informasi routing sumber IP, sehingga memungkinkan untuk membypass firewall.
- Tiny Fragment attacks : Intruder membagi IP kedalam bagian-bagian (fragment) yang lebih kecil dan memaksa terbaginya informasi mengenai TCP header. Serangan jenis ini di design untuk menipu aturan penyaringan yang bergantung kepada informasi dari TCP header.

Penyerang berharap hanya bagian (fragment) pertama saja yang akan di periksa dan sisanya akan bisa lewat dengan bebas. Hal ini dapat ditanggulangi dengan cara menolak semua packet dengan protokol TCP dan memiliki Offset = 1 pada IP fragment. Ilustrasi packet filtering router disajikan pada gambar 3.

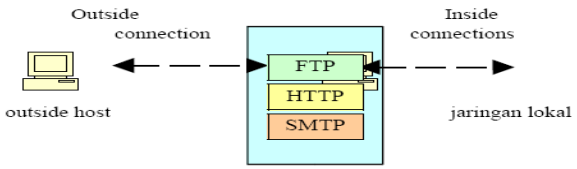


Gambar 3: Packet Filtering Router

Application-Level Gateway, Application-level Gateway yang biasa juga di kenal sebagai proxy server yang berfungsi untuk memperkuat/menyalurkan arus aplikasi. Tipe ini akan mengatur semua hubungan yang menggunakan layer aplikasi ,baik itu FTP, HTTP, GOPHER dll.

Cara kerjanya adalah apabila ada pengguna yang menggunakan salah satu aplikasi semisal FTP untuk mengakses secara remote, maka gateway akan meminta user memasukkan alamat remote host yang akan di akses.Saat pengguna mengirimkan useer ID serta informasi lainnya yang sesuai maka gateway akan melakukan hubungan terhadap aplikasi tersebut yang terdapat pada remote host, dan menyalurkan data diantara kedua titik. apabila data tersebut tidak sesuai maka firewall tidak akan meneruskan data tersebut atau menolaknya. Lebih jauh lagi, pada tipe ini Firewall dapat di konfigurasikan untuk hanya mendukung beberapa aplikasi saja dan menolak aplikasi lainnya untuk melewati firewall.

Kelebihannya adalah relatif lebih aman daripada tipe packet filtering router lebih mudah untuk memeriksa (audit) dan mendata (log) semua aliran data yang masuk pada level aplikasi. Kekurangannya adalah pemrosesan tambahan yang berlebih pada setiap hubungan. yang akan mengakibatkan terdapat dua buah sambungan koneksi antara pemakai dan gateway, dimana gateway akan memeriksa dan meneruskan semua arus dari dua arah, seperti disajikan pada gambar 4.

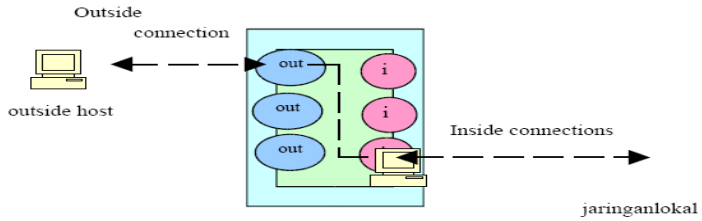


Gambar 4: Application-Level Gateway

Circuit-level Gateway, Tipe ketiga ini dapat merupakan sistem yang berdiri sendiri , atau juga dapat merupakan fungsi khusus yang terbentuk dari tipe application-level gateway.tipe ini tidak mengijinkan koneksi TCP end to end (langsung)

Cara kerjanya : Gateway akan mengatur kedua hubungan TCP tersebut, 1 antara dirinya (gw) dengan TCP pada pengguna lokal (inner host) serta 1 lagi antara dirinya (gw) dengan TCP pengguna luar (outside host). Saat dua buah hubungan terlaksana, gateway akan menyalurkan TCP segment dari satu hubungan ke lainnya tanpa memeriksa isinya. Fungsi pengamanannya terletak pada penentuan hubungan mana yang diijinkan.

Penggunaan tipe ini biasanya dikarenakan administrator percaya dengan pengguna internal (*internal users*). Seperti diilustrasikan pada gambar 5.



Gambar 5: Circuit-level Gateway

Langkah-Langkah Membangun Firewall

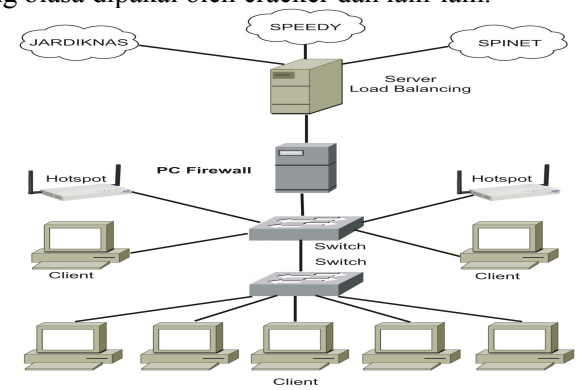
Untuk membangun firewall dapat dilakukan dengan langkah-langkah sebagai berikut:

a. Mengidenftifikasi bentuk jaringan yang dimiliki, khususnya topologi yang digunakan serta protocol jaringan
b. Menentukan Policy atau kebijakan. Penentuan kebijakan atau policy merupakan hal yang harus dilakukan karena baik atau buruknya sebuah firewall yang dibangun sangat ditentukan oleh policy/kebijakan yang di terapkan. Kebijakan yang dimaksud, diantaranya:
   - Menentukan apa saja yang perlu di layani. Artinya, apa saja yang akan dikenai policy atau kebijakan yang akan kita buat.
   - Menentukan individu atau kelompok-kelompok yang akan dikenakan policy atau kebijakan tersebut.
   - Menentukan layanan-layanan yang di butuhkan oleh tiap tiap individu atau kelompok yang menggunakan jaringan.
   - Berdasarkan setiap layanan yang di gunakan oleh individu atau kelompok tersebut akan ditentukan bagaimana konfigurasi terbaik yang akan membuatnya semakin aman
   - Menerapkankan semua policy atau kebijakan tersebut.
c. Menyiapkan Software atau Hardware yang akan digunakan
   Baik itu operating sistem yang mendukung atau software-software khusus pendukung firewall seperti iPChains, atau iptables pada linux, dsb. Serta konfigurasi hardware yang akan mendukung firewall tersebut.
d. Melakukan test konfigurasi
   Pengujian terhadap firewall yang telah selesai di bangun haruslah dilakukan, terutama untuk mengetahui hasil yang akan kita dapatkan, caranya dapat menggunakan tool tool yang biasa dilakukan untuk mengaudit seperti nmap.

RANCANGAN SISTEM

Melihat permasalahan yang sudah dipaparkan diatas, maka dianggap perlu untuk mengusulkan desain dan pembangunan jaringan yang lebih baik, sehingga permasalahan yang terjadi dapat diatasi. Mengingat kemampuan finansial sekolah juga terbatas, maka yang perlu didahulukan adalah

memaksimalkan jaringan yang ada. Beda antara jaringan yang lama dengan jaringan yang diusulkan adalah, adanya penambahan proxy server yang digunakan sebagai internet cache, yitu jika halaman web pernah diakses, maka halaman tersebut disimpan pada cache internet proxy server. Proxy server juga bisa digunakan untuk memfilter situs-situs yang tidak dikehendaki, misalya situs porno, situs yang biasa dipakai oleh cracker dan lain-lain.



Gambar 6: Jaringan komputer yang diusulkan

Spesifikasi Perangkat Keras

Perangkat keras yang dibutuhan untuk membangun firewall yang dibahas dalam tulisan ini adalah seperangkat PC dengan spesifikasi seperti disajikan pada tabel 1 berikut ini.

Tabel 1: Spesifikasi Perangkat Keras

Nama Perangkat Keras	Spesifikasi
Processor	Pentium IV 2.66. GHz
Mainboard	Intel D865
Memory	512 MB
Hardisk	40 GB
Lancard	10/100 Mbps
Kabel	Peer-to-Peer UTP

Spesifikasi Perangkat Lunak

Spesifikasi perangkat lunak yang dibutuhkan seperti tabel 2 berikut ini.

Tabel 2: Spesifikasi Perangkat Lunak

Nama Perangkat Lunak	Spesifikasi
Sistem Operasi	Linux Debian ETCH Ver. 4.2
Software Iptables	

Instalasi Sistem

Instalasi Iptables, Iptables adalah modul di linux, yang memberikan dukungan langsung terhadap kernel linux mulai versi 2.4, Untuk keamanan sistem serta beberapa keperluan jaringan lainnya. Iptables dapat digunakan untuk melakukan seleksi terhadap paket-paket yang datang baik *input*, *output* maupun *forward* berdasarkan Ip address, identitas jaringan, nomor *port*, *source* (asal), *destination* (tujuan), protokol yang digunakan bahkan berdasarkan tipe koneksi terhadap setiap paket (data) yang dinginkan.

Iptables dapat melakukan perhitungan terhadap paket dan menerapkan prioritas trafik berdasar jenis layanan (*service*). Iptables dapat digunakan untuk mendefinisikan sekumpulan aturan keamanan berbasis *port* untuk mengamankan *host-host* tertentu. Iptables juga dapat dimanfaatkan untuk membangun sebuah *router* atau *gateway*, tentunya hanya untuk sistem operasi linux.

Konfigurasi Iptables paling sederhana setidaknya menangani 3 kumpulan aturan yang disebut *chain*. Paket-paket yang diarahkan ke mesin firewall dinamakan *chain* INPUT, paket-paket yang diteruskan melewati firewall dinamakan FORWARD dan paket-paket yang menuju jaringan eksternal meniggalkan mesin firewall disebut OUTPUT.

Paket-paket yang masuk diperiksa, apakah rusak, salah information atau tidak, kemudian diberikan ke *chain* INPUT. Tergantung pada informasi yang terdapat di dalam *header* paket dan kebijakan dalam ruleset, keputusan yang diambil untuk suatu paket dapat berupa:

a. ACCEPT, Menerima paket dan diproses lebih lanjut oleh kernel.
b. DROP, Menolak paket tanpa pemberitahuan sama sekali.
c. REJECT, Mengembalikan paket ke asalnya dengan pesan kesalahan ICMP.
d. LOG, Melakukan *log* (pencatatan)terhadap paket yang bersesuaian.
e. RETURN, Untuk chain *user-defined* akan dikembalikan ke *chain* yang memanggil, sedangkan untuk *chain* INPUT, OUTPUT dan FORWARD akan dijalankan kebijakan default.
f. Mengirim ke chain *user-defined*.

Keputusan kebijakan di atas dibuat oleh pernyataan *jump* yang terdapat di dalam *ruleset*. Keputusan-keputusan yang serupa dibuat dalam *chain* FORWARD dan OUTPUT. Iptables juga memberikan fasilitas pembuatan proxy transparan dan IP *masquerade* dengan skema NAT (*Network Address Translation*).

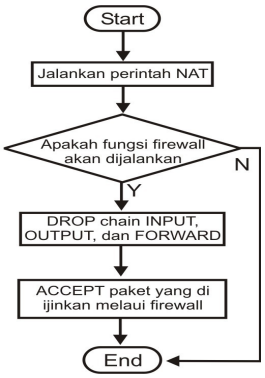
Algoritma Iptables Yang Digunakan

Proses yang terjadi pada sisi firewall, ketika firewall mulai dihidupkan, adalah sebagai berikut:

a. Proses booting, sistem operasi memeriksa konfigurasi hardware pada PC firewall tersebut.
b. Sistem menjalankan *script ip forwarding* yang ditulis pada file rc.local.

c. Perintah NAT (*Network Address Translation*) dijalankan.
d. Untuk menjalankan fungsi firewall, terlebih dahulu blok/ drop seluruh paket, dengan mematikan *chain* INPUT, OUTPUT, dan FORWARD.
e. Aktifkan paket-paket yang diijinkan melalui firewall, dengan membuka chain INPUT, OUTPUT, dan FORWARD, dengan fungsi ACCEPT.

Proses-proses tersebut jika disajikan dalam bentuk flowchart adalah seperti gambar 7



Gambar 7: Proses bekerjanya firewall, dilihat dari sisi firewall itu sendiri.

Algoritma Untuk Mem-blokir IP Address.

Pada saat pemblokiran IP address, proses-proses yang terjadi adalah:

a. Paket data masuk melalui jaringan lokal/ eth1.
b. Seluruh chain diblokir/ DROP (INPUT, OUTPUT, dan FORWARD).
c. Selain IP address 192.168.215.10 di ijinkan melalui chain INPUT.
d. Selain IP address 192.168.215.10 di ijinkan melalui chain FORWARD.

Algoritma Untuk Mem-blokir Situ Web.

Untuk mem-blokir situs-situs web yang tidak diijinkan masuk dan diakses jaringan lokal, adalah sebagai berikut :

a. Paket data masuk dari jaringan publik/ eth0.
b. Seluruh chain diblokir/ DROP (INPUT, OUTPUT, dan FORWARD).
c. Selain www.hackers.net di ijinkan melalui chain INPUT.
d. Selain www.hackers.net di ijinkan melalui chain FORWARD

Algoritma Mem-blokir FTP (File Transfer Protocol)

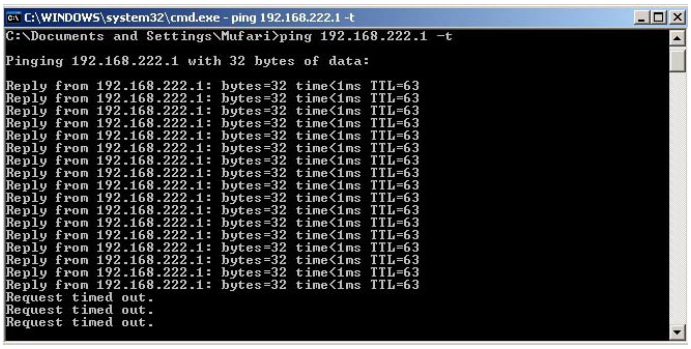
Untuk mem-blokir user lokal yang tidak diijinkan mengakses *ftp server*, adalah sebagai berikut :

a. Paket data masuk dari jaringan publik/ eth0.
b. Seluruh chain diblokir/ DROP (INPUT, OUTPUT, dan FORWARD).
c. Selain ftp.microsoft.com di ijinkan melalui chain INPUT.
d. Selain ftp.microsoft.com di ijinkan melalui chain FORWARD

HASIL PENELITIAN

Setelah dilakukan seting seperti di atas, PC firewall siap digunakan, untuk menguji kemampuan firewall, maka lakukan hal-hal seperti berikut:

Ping ke IP Address Tertentu.

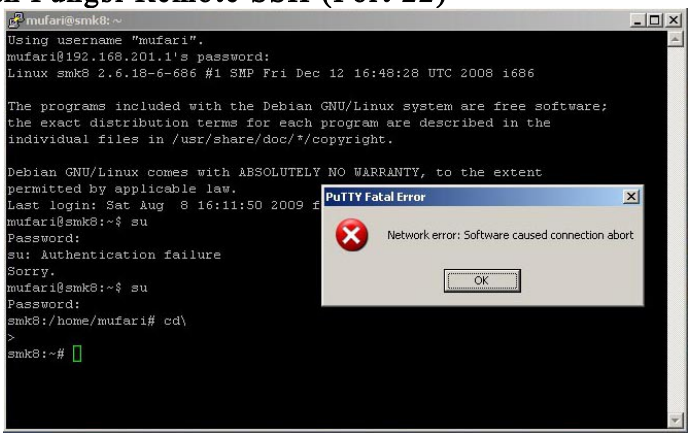


Gambar 8: Ping ke DNS server

Pada gambar 8, ping ke arah IP Address (DNS) 192.168.222.1 di blok, dengan memberikan perintah sebagai berikut :

```
# iptables -A INPUT -d 192.168.222.1 -p icmp -j DROP
```

Mematikan Fungsi Remote SSH (Port 22)



Gambar 9: Fungsi remote SSH dari putty dimatikan

Pada gambar 9, merupakan efek dari penggunaan script :

```
# iptables -A INPUT -s tcp –dpor 22 -j DROP
```

PENUTUP

Kesimpulan

Setelah melakukan penelitian dan percobaan, kesimpulan yang dapat diambil adalah, penggunaan iptables sebagai aplikasi dari firewall, dapat membantu

administrator untuk memfilter jaringan dari pemakai yang tidak mempunyai hak akses, agar tidak bebas keluar masuk jaringan internet/ WAN.

Saran

Dengan mengamati dan mengevaluasi dari hasil kerja firewall tersebut, maka kami memberikan saran bahwa: (1) Dimungkinkan bagi administrator untuk selalu memeriksa kondisi firewall apakah masih berfungsi dengan baik, dan memeriksa log-log, apakah ada pihak yang tidak mempunyai hak akses, mencoba mengakses jaringan dengan cara illegal. (2) Dimungkinkan dalam pengoperasiannya untuk selalu melakukan *trial* and *error*, agar jika terjadi kerusakan dapat diketahui lebih dini.

DAFTAR PUSTAKA

Geier, Jim .2005. *Wireless Networks First-Step*. Yogyakarta: Andi Offset

Husni.2003. *Implementasi Jaringan Komputer dengan Linux Redhat 9*. Yogyakarta: Andi Offset.

Http://iptables-tutorial.frozentux.net/iptables-tutorial.html Minggu, 02 Agustus 2009. 11.45.20 WIB.

Http://onno.vlsm.org/v09/onno-ind-1/network/network-security/firewall-sekuriti-internet-11-1997.zip. Minggu, 02 Agustus 2009. 09.25.34 WIB.

Kadir, Abdul.2002. *Pengenalan Unix dan Linux*. Yogyakarta: Andi Offset

Syahrizal, Melwin .2005.*Pengantar Jaringan komputer*. Yogyakarta: Andi Offset