Jurnal Armada Informatika

p-ISSN: 2598-0416 http://jurnal.stmikmethodistbinjai.ac.id e- ISSN: 2615-6891

Membangun PCrouter Dengan UbuntuServer dan Keamanan Jaringan Dengan Shorewall

Mhd. Dicky Syahputra Lubis[1], Allwine[2]
STMIK Methodist Binjai Jl. Jend. Sudirman No. 136 Binjai 061-88742021
Teknik Informatika

e-mail: mhddicky@stmikmethodistbinjai.ac.id[1] ,allwin@stmikmethodistbinjai.ac.id[2]

Abstrak

Router adalah salah satu komponen pada jaringan komputer yang mampu melewatkan data melalui sebuah jaringan atau internet menuju sasarannya, melalui sebuah proses yang dikenal sebagai routing. Router berfungsi sebagai penghubung antar 2 (dua) atau lebih jaringan untuk meneruskan data dari jaringan ke jaringan lainnya. Router sendiri berharga tinggi dan masih sulit dijangkau oleh kalangan masyarakat. Router Ubuntu adalah solusi murah bagi mereka yang membutuhkan sebuah router handal dengan hanya bermodalkan standalone komputer dengan sistem operasi Ubuntu. Dewasa ini router yang menggunakan sistem operasi Linux semakin meningkat, selain biayanya murah, pengguna Linux juga dapat memanfaatkan aplikasi-aplikasi tambahan yang memudahkan dalam pengoperasian Linux. Salah satu aplikasi yang digunakan untuk sistem keamanan pada jaringan komputer adalah firewall. Firewall adalah salah satu aplikasi Linux yang dibutuhkan sebuah router Linux untuk menjaga integritas data yang ada dari serangan-serangan hacker yang tidak bertanggung jawab dengan melakukan filterisasi terhadap paket-paket yang datang kepadanya. Linux telah menyiapkan aplikasi untuk dijadikan sebuah firewall diantaranya ipchains, iptables dan Shorewall. Pada sistem operasi Linux kemampuan filter paket data sudah dimasukkan dalam kernel, kernel Linux sudah punya kemampuan filter paket data. Pada saat ini, digunakan program Shorewall dari Linux Ubuntu Desktop. Ipchains, iptables, dan shorewall ini dapat digunakan sebagai firewall yang handal dan murah. Berbeda dengan ipchains dan iptables, selain murah dan handal, shorewall juga mudah dikonfigurasi. Shorewall yang merupakan kependekan dari Shoreline Firewal, merupakan firewall yang berbasiskan kepada iptables yang dipermudah dalam penggunaanya, Shorewall dapat di installasi pada kebanyakan sistem pada Linux, akan tetapi shorewall paling banyak diaplikasikan untuk pembuatan gateway atau firewall atau router PC berbasiskan UNIX. Shorewall juga banyak diujicobakan pada 2 distro yaitu Mandrake dan Ubuntu. Shorewall (Shoreline Firewall) merupakan firewall yang berbasis iptable yang dapat digunakan pada suatu sistem deticated, gateway/router/server multifungsi atau pada standalone linux. shorewall merupakan software yang dipakai untuk setting aturan masuk dan keluar serta kebijakan-kebijakan yang perlu dilakukan dalam pengamanan komputer yang terhubung ke jaringan.

Kata Kunci: Jaringan Komputer, Linux, Shorewall, Firewall, PCRouter

Abstract

Router is a component of a computer network that is capable of passing data over a network or the internet to a target, which is called routing. The router works as a liaison between 2 (two) or more networks to complete data from other networks. The router itself is high and still difficult to implement by the public. Ubuntu routers are a very useful solution for routers

that only have standalone computers with the Ubuntu operating system. Nowadays routers that use the Linux operating system are increasing, in addition to the costs, Linux users canalso access it. One application that is used for firewalls on network computers is a firewall. A firewall is one of the Linux applications that a Linux router needs to keep existing data from hacking attacks that are not responsible by filtering the packets that come logical. Linux has created an application to activate the firewall, iptables and Shorewall. In the Linux operating system the ability of a data packet filter has been entered into the kernel, the Linux kernel already has the ability to filter data packets. At this time, the Shorewall program is from Linux Ubuntu Desktop. Ipchains, iptables, and shorewall can be used as reliable and inexpensive firewalls. Unlike ipchains and iptables, besides being cheap and reliable, shorewall is also easy to configure. Shorewall, which is short for Shoreline Firewal, is a firewall based on iptables that is facilitated in its use, Shorewall can be installed on most systems on Linux, but Shorewall is the most widely used for creating UNIX-based PC gateways or firewalls. Shorewall has also been tested on 2 distributions, Mandrake and Ubuntu. Shorewall (Shoreline Firewall) is an iptable-based firewall that can be used on detective systems, multifunction gateways / routers / servers or on standalone Linux. shorewall is software that is used to regulate entry and exit rules and policies that need to be done in securing a computer connected to the network.

Keywords: Computer Network, Linux, Shorewall, Firewall, PCRouter

1. PENDAHULUAN

Kemajuan teknologi khususnya jaringan komputer sangat membantu dibidang informasi dan pengolahan data informasi. Komputer memegang peranan penting dalam teknologi informasi, melalui komputer akan didapatkan informasi yang diinginkan tanpa keterbatasan ruang dan waktu dengan mendaya gunakan secara maksimal sistem komputer dalam jaringan komputer yang terintegrasi akan didapatkan informasi data dengan cepat dan tepat. Salah satu jenis alat Bantu berteknologi tinggi yaitu Komputer. Pada era *high-tech* ini tidak dapat di pungkiri lagi apabila komputer adalah salah satu alat bantu elektronik yang menempati posisi teratas. Manfaat komputer itu sendiri dapat kita rasakan didalam kehidupan kita sehari-hari yang tentu sangat menunjang baik dalam ilmu pengetahuan, pendidikan, bisnis, administrasi perkantoran, komunikasi dan lain-lain. Sejalan dengan itu pengguna komputer harus diimbangi dengan kemampuan dari si pemakai untuk dapat memanfaatkannya dengan sebaik mungkin. Sejalan dengan perkembangan teknologi informasi, peralatan-peralatan pendukung jaringan komputer masih sangat diperlukan. Peralatan tersebut pun kini menjadi komponen penting dalam pembangunan jaringan komputer.

Jaringan komputer dengan menggunakan *server linux* mampu mengelola semua servis internet, antara lain : *router, database server, proxy server dan FTP server,* dan sebagainya.

Jenis jaringan yang banyak digunakan dalam suatu perusahaan adalah jenis jaringan *client server* dimana *servernya* kebanyakan menggunakan sistem operasi *linux* yang berfungsi sebagai *database server* sekaligus juga sebagai *router*. Sehingga *server linux* ini harus memiliki 2 *ethernet card*, *ethernet card* 1 menggunakan nomor *IP publik* (internet) sedangkan *ethernet card 2* menggunakan *IP lokal (LAN).* Komputer *client* juga menggunakan *IP lokal* dan menjadi satu jaringan dengan *server*. Agar *client* dapat mengakses *internet* maka *server* menggunakan perannya sebagai *router* untuk mem-*forward IP* masing-masing *client*.

Adapun manfaat jaringan komputer adalah sebagai berikut :

1. *Sharing resources*
2. Media komunikasi
3. Integrasi data
4. Sumber daya lebih efisien dan informasi terkini

1.1 Keamanan Jaringan Komputer

Sistem keamanan jaringan komputer yang terhubung ke Internet harus direnacanakan dan dipahami dengan baik agar dapat melindungi investasi dan sumber daya di dalam jaringan komputer tersebut secara efektif. Sebelum mulai mengamankan suatu jaringan, harus ditentukan terlebih dahulu tingkat ancaman/serangan yang harus diatasi, dan resiko yang harus diambil maupun yang harus dihindari. Untuk itu jaringan komputer harus dianalisa untuk mengetahui apa yang harus diamankan, untuk apa diamankan, dan jenis-jenis keamanannya. Pada dasarnya ada tiga hal yang perlu dilindungi diantaranya :

a. Data

Data merupakan informasi yang ada di dalam komputer. Data merupakan hal yang sangat berharga yang perlu untuk dilindungi, pertukaran data di dunia maya *(internet)* merupakan hal yang sering dimanfaatkan oleh orang-orang yang tidak bertanggung jawab.

Ada tiga kategori data yang perlu dilindungi :

1. Rahasia : Data yang tidak ingin orang lain mengetahuinya.
2. *Integritas* : Data yang tidak boleh ditukar atau dirubah oleh orang lain.
3. Ketersediaan : Hanya digunakan oleh orang-orang tertentu.

Keamanan data dapat dibedakan menjadi dua, yaitu keamanan fisik dan keamanan sistem. Keamanan fisik merupakan bentuk keamanan yang berupa fisik dari *server*, terminal atau klient *router* sampai dengan *cabling* sedangkan keamanan sistem adalah keamanan pada sistem pengoperasiannya atau lebih khususnya pada *softwarenya*.

Keamanan merupakan isu utama dalam jaringan. Apalagi jika seluruh *host* tersambung ke Internet. Melindungi jaringan, berarti melindungi setiap *hos*t yang ada dalam jaringan, baik *workstation* maupun *server.* Fokus bahasan laporan ini adalah melindungi linux server baik ancaman dari luar jaringan (misalnya dari *Internet*), maupun *internal* jaringan (ancaman dari salah satu *user*). Jika komputer terhubung ke *Internet, Linux* menjanjikan keamanan yang cukup memadai. Selain tangguh sebagai komputer pribadi, *Linux* menawarkan kinerja optimal untuk dijadikan sebagai server. Di dunia *Linux* dikenal istilah *distribution* atau di Indonesia disebut distribusi, atau oleh pecinta *Linux* indonesia disebut Distro.

Distro adalah *Kernel Linux* ditambah dengan kumpulan paket-paket *softwere* dari *GNU* dan yang lain, yang digabung menjadi satu, dengan tujuan untuk mempermudah proses distribusi *software* tersebut. Berbagai macam *distro linux yaitu Redhat, Slackware, SUSE, FedoraCore, Mandrake*. Pada perancangan *firewall* ini menggunakan *distro Mandarake* yang merupakan turunan dari *RedHat, Mandrake* selalu menggunakan kernel terbaru dalam rilis versi terbaru mereka dan salah satu keunggulannya dalah adanya *x windows* yang sangat *userfriendly* sehingga lebih mudah untuk digunakan.

2. METODE PENELITIAN

Sebelum menginstal *shorewall* diperlukan 2 *ethernet card, ethernet card* pertama di pakai untuk menuju ke internet dan *ethernet card* ke dua di pakai menuju jaringan lokal. *Shorewall* dibangun diatas fasilitas kernel *Netfilter*. Sebelum mengkonfigurasi *shorewall*, kita harus :

1. Menentukan zona sumber.
2. Menetukani zona tujuan.
3. Menentukan apa saja yang perlu dilayani dengan memberikan kebijakan kepadanya.
4. Dapat menentukan suatu aturan dari kebijakan yang kita berikan untuk klien.

p-ISSN: 2598-0416 http://jurnal.stmikmethodistbinjai.ac.id e- ISSN: 2615-6891

2.1 File-file *shorewall*

Berikut adalah file-file penting yang harus disetting dalam mengkonfigurasi *Shorewall*, yaitu :

A. */etc/shorewall/zone*

File ini untuk mendefinisikan zona asal trafik pada jaringan. *Server* tempat shorewall diinstal dikenal sebagai zona yang disebut *fw*.Pada file ini, *local* yang merupakan *interface* yang terhubung dengan jaringan *local* dan *net* merupakan *interface* yang terhubung dengan jaringan *network*.

```
# ZONE DISPLAY COMMENTS
net net Internet
loc local local networks
```

B. /etc/shorewall/policy

File ini berisi aturan untuk semua trafik yang lewat pada *firewall* diatur pada */etc/shorewall/rules*, jika tidak terdefinisikan pada file tersebut maka akan dicek pada */etc/shorewall/policy*.

```
#SOURCE ZONE DESTINATION POLICY LOG
loc net ACCEPT
```

C. /etc/shorewall/interface

File ini untuk menentukan *interface* yang akan terhubung dengan suatu zona, pada file ini, *eth0* terhubung dengan jaringan internet dan *eth1* terhubung dengan jaringan lokal.

```
#ZONE INTERFACE BROADCAST OPTIONS
net eth0
loc eth1
```

D. /etc/shorewall/masq

File ini untuk mendefinikan *masquerade* jaringan lokal dengan jaringan internet. Untuk mensetting apakah trafik yang melalui *eth1* akan dibungkus *(dimasquerade)* dengan dengan *IP* pada *eth0*.

```
#INTERFACE SUBNET ADDRESS
eth0 eth1
```

E. /etc/shorewall/rules

File ini berisi aturan-aturan dari semua trafik yang melewati *firewall*. Berikut contok konfigurasinya :

```
#Rule dari local ke mesin firewall
ACCEPT loc fw tcp 23
ACCEPT loc fw tcp 80
```

F. /etc/shorewall/shorewall.conf

Digunakan untuk mengaktifkan shorewall agar dapat di *load* pada saat *startup.*

```
Startup_ENABLE = Yes
```

3.7.2 Kebijakan-Kebijakan *Shorewall*

1. *Accept*

Dengan opsi ini setiap paket akan langsung diterima oleh firewall dan diteruskan kepada tujuan dari paket tersebut. Misalnya paket tersebut menuju server kita dengan tujuan *port 80* maka paket tersebut akan langsung diteruskan untuk diproses oleh *server*.

```
ACCEPT loc fw tcp 80
```

2. *Drop*

Berbeda dengan *REJECT*, bila firewall menemukan paket yang di-*DROP*, *firewall* akan langsung ”membuang” setiap paket yang memiliki target ini tanpa mengirim pesan error kepada pengirim paket tersebut.

DROP loc fw tcp 23

3. *Reject*
   Berbeda dengan *ACCEPT*, setiap paket yang memiliki embel-embel *reject* ini akan ditolak, tapi firewall akan mengirimkan pesan *ICMP error* kepada sipengirim paket. Secara default, *firewall* akan mengirimkan pesan *ICMP* berupa *port-unreachable*.
   all all REJECT

3.7.3 Perintah-Perintah *Shorewall*

Tabel 3.5 Perintah-perintah *Shorewall*

Perintah Shorewall	Keterangan
Shorewall start	Perintah untuk memulai firewall dengan shorewall
Shorewall stop	Perintah untuk menghentikan firewall dengan shorewall
Shorewall restart	Perintah untuk Kembali ke konfigurasi awal
Shorewall clear	Perintah untuk menghapus semua aturan aturan shorewal

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

4.1 Tujuan Pembuatan *Firewall* dengan *Shorewall*

Adapun tujuan pembuatan *firewall* dengan *shorewall* adalah untuk melindungi jaringan lokal dari jaringan internet dengan cara mengendalikan aliran paket yang melewatinya, berdasarkan asal paket data, tujuan paket data, dan *port* data.

4.2 Perencanaan *Firewall* dengan *Shorewall*

Perencanaan merupakan suatu tahapan yang sangat penting dalam pembuatan sistem karena dengan perencanaan tersebut diharapkan nantinya akan mendapatkan suatu sistem yang baik seperti yang diharapkan. Perencanaan perancangan *firewall* dengan *shorewall* mengenai bagaimana cara mengkonfigurasi *shorewall* untuk mengatur keluar dan masuknya paket data serta kebijakan-kebijakan yang perlu dilakukan dalam pengamanan komputer yang terhubung ke jaringan.

4.3 Langkah-langkah Membangun Firewall

4.3.1 Mengidentifikasi Bentuk Jaringan

Sebelum membangun sebuah *firewall* pertama kali kita harus mengetahui terlebih dahulu bentuk jaringan yang dimiliki, khususnya topologi yang digunakan, yang mana ini akan memudahkan kita dalam mendesain sebuah *firewall*. Pada perancangan *firewall* kali ini akan dibangun sebuah *firewall* dengan dua *interface*, dimana *firewall* terletak diantara jaringan lokal dan jaringan *global (internet)*. Sebelum membangun *firewall* kita harus membuat sebuah *pc* yang akan dijadikan *router*, dimana IP:192.168.0.8 pada eth0 untuk jaringan lokal dan IP:192.168.1.8 pada *eth1* untuk jaringan internet.

1. Instalasi *Shorewall*

Pada perancangan firewall ini *Operating System* (OS) yang digunakan adalah *Linux Ubuntu Server 10, Shorewall di Ubuntu Server 10* belum terinstall saat kita melakukan instalasi di komputer kita, jadi kita perlu melakukan *installasi Shorewall* secara tersendiri. Di sini penulis melakukan installasi Shorewall langsung menggunakan internet dengan perintah sebagai berikut :

apt-get install shorewall

p-ISSN: 2598-0416 http://jurnal.stmikmethodistbinjai.ac.id e- ISSN: 2615-6891

3. HASIL DAN PEMBAHASAN

3.1 Konfigurasi *Firewall* Menggunakan *Shorewall*

Firewall adalah sebuah system atau perangkat yang terdapat dalam berbagai system operasi misalkan *windows* dan *linux* yang berfungsi sebagai filter untuk mengizinkan lalu lintas jaringan yang dianggap aman untuk melaluinya dan mencegah lalu lintas jaringan yang tidak aman.Sedangkan *shorewall* adalah salah satu tools *firewall* pada *linux* yang berbasiskan *iptables*. Dalam *shorewall* terdapat konsep *"zone"* yang memudahkan kita untuk menentukan *policy firewall*, dari pada kita melakukan konfigurasi secara manual dengan *iptables.*
Untuk memudahkan kita, asumsikan saja ada 3 zona yang dapat di definisikan, yaitu :

1. LAN, yaitu jaringan lokal, kita definisikan sebagai *zona lok*
2. Internet, yaitu koneksi kita ke internet, kita definisikan sebagai zona *net*
3. Komputer Firewall kita secara otomatis bernama zona *$FW*

Berikut ini adalah step-by-step konfigurasi yang diterapkan.

1. Copy konfigurasi dari template yg ada
   cd /usr/share/doc/shorewall-common/default-config
   cp zones /etc/shorewall/
   cp interfaces /etc/shorewall/
   cp policy /etc/shorewall/
   cp rules /etc/shorewall/
2. Setting Shorewall sebagai berikut :

a. Konfigurasi zona

nano /etc/shorewall/zones

Kemudian isikan berikut ini :

fw firewall
lok ipv4
net ipv4

b. Konfigurasi interface

nano /etc/shorewall/interfaces

Kemudian isi konfigurasi berikut ini :

lok eth0 detect tcpflags,logmartians,nosmurfs
net eth1 detect tcpflags,logmartians,nosmurfs

c. Konfigurasi policy

nano /etc/shorewall/policy

$FW all ACCEPT
lok $FW DROP info
lok net DROP info
net $FW DROP info
netlok DROP info

d. Konfigurasi rules

nano /etc/shorewall/rules

Kemudian isi konfigurasi berikut ini :

SECTION NEW
ACCEPT lok $FW tcp 80
ACCEPT net $FW tcp 80
Ping/ACCEPT lok $FW
SSH/ACCEPT lok:192.168.0.1 $FW

p-ISSN: 2598-0416 http://jurnal.stmikmethodistbinjai.ac.id e- ISSN: 2615-6891

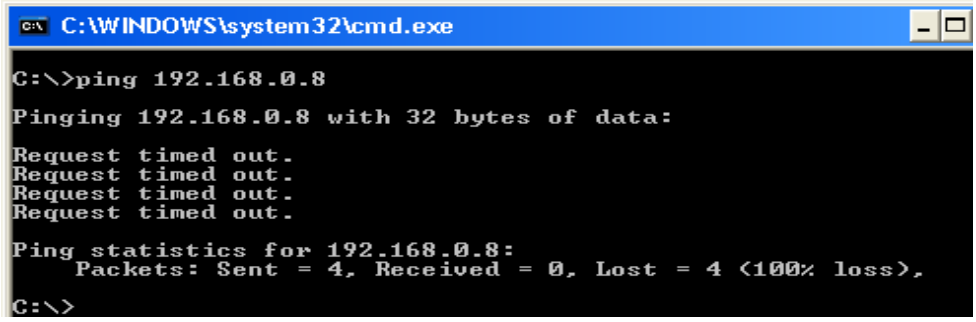
Ping/ACCEPT lok $FW adalah membolehkan akses *ping* dari jaringan, *SSH/ACCEPT lok*:*192.168.0.1 $FW* adalah yang boleh mengakses *router* yaitu *client* pada jaringan yang bernomor *IP:192.168.0.1*.

3.2 Hasil Pengujian

Dalam pengujian *firewall* dengan *shorewall* ini penulis menggunakan 2 (dua) macam pengujian yaitu dengan pengiriman *paket ping* dan dengan program *telnet yaitu putty*.

3.2.1 Pengiriman Paket Ping

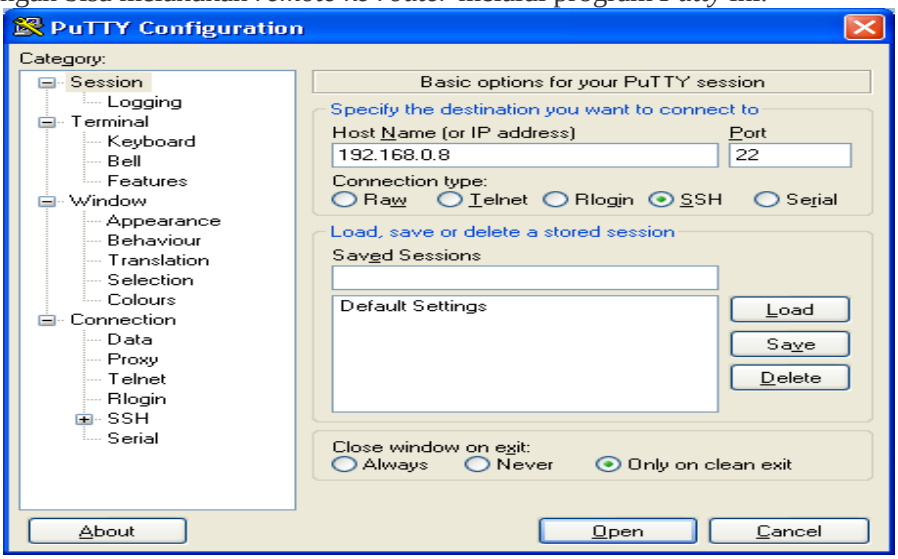
Pada saat sebelum shorewall dikonfigurasi pengiriman paket ping dalam keadaan lancar-lancar saja. Namun setelah dilakukan konfigurasi pada *rules shorewall* yaitu pada bagian *Ping/ACCEPT lok $FW* maka yang boleh melakukan pengiriman paket *ping* ke *router* hanya dalam jaringan *local* saja, sedangkan pada jaringan internet tidak biasa dilakukan.



Gambar 5.6 : Hasil Pengiriman Paket Ping yang Di lok

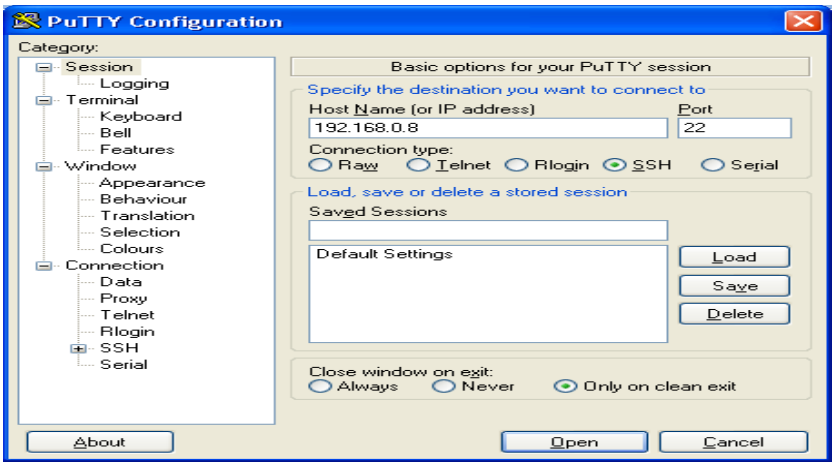
3.2.2 Remote Router Dengan Telnet Putty

Telnet Putty biasa digunakan untuk *meremote* atau masuk ke dalam *resource operating* sistem yang berbasis *unix*. Dalam keadaan normal atau sebelum *rules shorewall* dikonfigurasi semua jenis jaringan bisa melakukan *remote ke router* melalui program *Putty* ini.

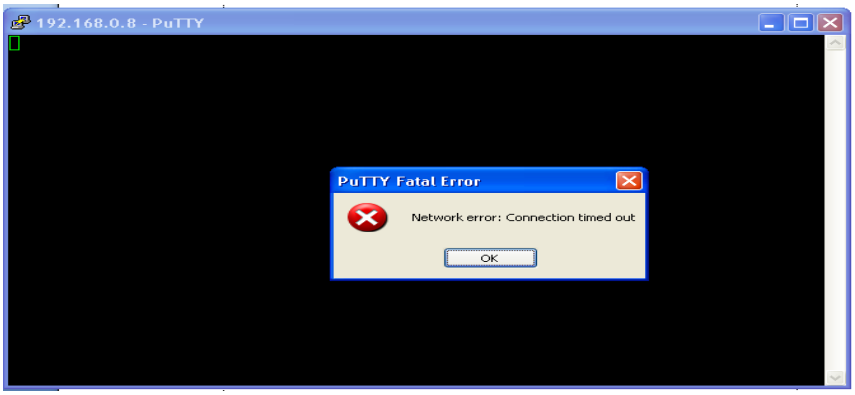


Gambar 5.7 : Remote router Dengan Telnet Putty

Kemudian setelah dilakukan konfigurasi pada *rules shorewall* yaitu pada bagian *SSH/ACCEPT lok:192.168.0.1 $FW* maka tidak semua jenis jaringan atau nomor IP yang bias meremotnya, hanya nomor IP 192.168.0.1 saja yang biasa melakukannya.



Gambar 5.9 : Configuration Telnet Putty



Gambar 5.10 : Hasil Configuration Telnet Putty

4. Kesimpulan

Dari hasil dan pembahasan serta perancangan yang telah dibuat maka dapat di tarik kesimpulan sebagai berikut :

1. *Firewall* menggunakan *Shorewall* dapat menjaga keamanan data di *Server* , *clien* yang terhubung pada jaringan komputer.
2. Keluarnya paket data pada *server* melalui *pc router* dan masuk ke *klien* yang terhubung pada jaringan komputer yang tergantung dari kebijakan yang di berikan *shorewall.*
3. *Shorewall* lebih mudah di konfigurasi dari pada *software Firewall* yang

5. Saran

Berikut saran saran yang akan penulis berikan untuk pengembangan lebih lanjut:

1. Sebaiknya *shorewall* di konfigurasi di *Linux Ubuntu* karena file-file yang di butuhkan untuk mengkonfigurasinya sudah di sediakan di *Ubuntu* jadi kita tidak perlu lagi mencari *kode binernya*.
2. Gunakan *topologi DMZ (De-Milatarized Zone)* untuk mempermudah kita membangun *firewall* dengan jumlah server yang banyak.

Daftar pustaka

Aceng, Sobana. *Jaringan Komputer dan Internet (Sebuah Pengantar)*. 2006

Budiyono, Avon & Hendra Adi H. *Instalasi & Konfigurasi Jaringan Intranet – Internet*. Laboratorium Computer & Communication Sekolah Tinggi Teknologi Telkom Bandung: 2005

Irawan. *Jaringan Komputer untuk Orang Awam* Edisi 2. Palembang. Maxicom: 2013

Purbo, Onno W. *Jaringan Wireless di Dunia Berkembang Edisi Kedua (Terjemahan)*. One Destination Center: 2007

Suarna ST, Nana. *Pengantar Jaringan (Pedoman Panduan Praktikum)*. Bandung. Yrama Widya: 2009

Sukaridhoto, Sritrusta. *Buku Wireless*. Surabaya. PENS-ITS: 2008

Sumarwanto, Dwi. *Pengenalan Jaringan Komputer Serta Pemanfaatannya*. Pusat Teknologi Informasi Dan Komunikasi Departemen Pendidikan Nasional: 2008

http://www.amazinglight.info/tipe-jaringan-komputer.html

http://dc336.4shared.com/doc/dTyOFKMc/preview.html

http://risnotes.com/2012/01/pengertian-antena-dan-directive-gain

http://commons.wikimedia.org/wiki/File:Spillover.png

http://opensource.telkomspeedy.com/wiki/index.php/Kabel_coax