Makalah Seminar Tugas Akhir

Desain dan Implementasi Firewall dengan Layer 7 Filter Pada Jaringan Teknik Elektro

Adhi Laksono[1], Agung B.P.[2], Adian Facturrochim[2]

[1]Mahasiswa dan [2]Dosen Jurusan Teknik Elektro, Fakultas Teknik, Universitas Diponegoro,
Jl. Prof. Sudharto, Tembalang, Semarang, Indonesia

Abstrak

Keamanan pada suatu jaringan sangat mutlak dibutuhkan karena rawannya jaringan apabila terhubung dengan jaringan luar (WAN). Salah satu solusinya adalah dengan membangun firewall sebagai pertahanan pertama pada jaringan yang dimiliki. Firewall itu sendiri berfungsi sebagai filtrasi semua paket yang masuk pada jaringan lokal. Firewall memiliki patch layer 7 filter yang dapat digunakan untuk mem-filter paket berdasakan aplikasinya. Pada tugas akhir ini mencoba mengimplementasikan firewall layer 7 filter pada jaringan Teknik Elektro. Dalam pengaruhnya dengan koneksi pada internet dari jurusan-jurusan lain, ternyata sangat signifikan perbedaannya.

Kata kunci : firewall, layer 7 filter

1. Pendahuluan

1.1 Latar Belakang Masalah

Beberapa tahun terakhir ini perkembangan di bidang informatika dan teknologi bergerak begitu pesat. Komputer dan kemampuannya dalam berkomunikasi dengan komputer lain dalam suatu jaringan adalah contoh keberhasilan dari perkembangan di bidang ini.

Kebutuhan suatu perusahaan atau instansi dengan ruang lingkup yang luas dan tersebar di suatu wilayah memerlukan suatu koneksi antar gedung. Disinilah pentingnya peran komputer dalam membuat jaringan antar cabang. Dengan penerapan teknologi ini, sangatlah mudah untuk mengirim file dan dokumen-dokumen penting dari tempat satu ke tempat yang lain. Namun teknologi inipun memiliki kelemahan, yaitu sangat rentan terhadap pencurian, perusakan, dan kerahasiaan dokumen. Hal ini terjadi karena komputer berada dalam suatu jaringan umum, sehingga file dan dokumen pada suatu perusahaan atau instansi dapat dilihat oleh banyak orang dalam jaringan. Oleh sebab itu, mutlak bagi suatu perusahaan atau untuk memiliki sistem pengamanan (*Computer Security*) dalam jaringannya.

Firewall merupakan salah satu solusi dalam mencegah serangan penyusup tersebut. Dengan mempelajari dengan seksama dan mengaturan hak akses yang dibutuhkan dalam suatu jaringan dan menggunakan software yang sesuai, maka kita dapat merancang firewall yang cocok untuk diterapkan. Firewall sendiri diterapkan untuk dapat melindungi dengan melakukan filtrasi, membatasi ataupun menolak suatu koneksi pada jaringan.

Tugas akhir ini akan membahas mengenai bagaimana merancang suatu keamanan jaringan berbentuk *firewall* dengan mengatur *policy-policy* pada *firewall* tersebut agar didapatkan suatu jaringan yang aman dan analisis *firewall* serta penerapan *layer* 7 *filter* pada jaringan Teknik Elektro serta dampak yang ditimbulkan.

1.2 Identifikasi Masalah

Dalam mengimplementasikan *firewall layer* 7 *filter*, dapat diidentifikasi dua masalah utama, yaitu :

1. Pengamanan berdasarkan *port* untuk melakukan filtrasi hak akses yang bertentangan dan berbahaya bagi jaringan lokal.
2. Pengamanan berdasarkan aplikasi seperti bittorrent yang merupakan masalah utama dari jaringan Fakultas Teknik dan Teknik Elektro pada khususnya.

1.3 Batasan Masalah

1. Tugas akhir ini membahas mengenai Perancangan Keamanan Jaringan berupa *Firewall*.
2. Aplikasi utama yang digunakan adalah IPTABLES.
3. Tugas akhir ini akan merancang *Firewall* dengan mengatur *policy-policy* yang diperlukan dalam suatu jaringan komputer serta konsep-konsep yang dapat diterapkan dalam menyusun *firewall* tersebut.
4. *Layer* 7 *Filter* yang digunakan didapat dari l7filter-filter.sourceforge.net.
5. Tugas Akhir ini dirancang untuk berjalan di atas Sistem Operasi Linux.
6. Tidak membahas mengenai *source code* yang menghasilkan fitur yang digunakan oleh iptables.
7. Tidak membahas secara detail program penampil aliran data iptraf dan MRTG.

1.4 Tujuan Penelitian

Tujuan penelitian adalah menghasilkan suatu jaringan komputer yang aman dengan menerapkan *firewall* dengan *layer* 7 *filter* sebagai filtrasi, pembatas dan sebagai gateway pada jaringan Teknik Elektro dengan cara menentukan *policy-policy* yang diperlukan dalam jaringan tersebut serta memahami konsep-konsep yang diterapkan dalam menyusun *firewall* tersebut.

1.5 Kegunaan Hasil Penelitian

1. Menghasilkan keamanan pada jaringan Teknik Elektro dari serangan penyusup atau penyalahgunaan hak akses ke jaringan lokal Teknik Elektro.
2. Menghasilkan keamanan pada jaringan Teknik Elektro dari penyalahgunaan *bandwidth* yang merupakan masalah utama dari jaringan Fakultas Teknik khususnya Teknik Elektro.

2. IP Routing dan Firewall

Dalam keamanan jaringan, tidak akan lepas dengan istilah routing, manajemen alamat IP, manajemen routing IP dan Firewall. Dimana suatu komputer harus dapat berinteraksi dengan komputer yang lain baik ia berada dalam satu jaringan ataupun pada jaringan yang berbeda. Dan apabila telah terkoneksi semua, dibutuhkan suatu aturan hak akses antar tiap komputer dan antar tiap jaringan. Disinilah peran suatu Firewall.

2.1 Pengertian Routing

Dalam suatu perusahaan pasti memiliki banyak komputer yang harus terkoneksi satu sama lain. Dalam satu perusahaanpun memiliki jaringan komputer yang banyak yang harus bisa terkoneksi dengan jaringan lain dalam perusahaan tersebut. Dalam linux, routing dapat dilakukan untuk menyelesaikan masalah diatas.

Perancangan IP routing dalam jaringan sederhana tidak serumit perancangan dalam jaringan kompleks. Namun konsep dasar IP routing tidak berbeda, yaitu bagaimana memilih dan menetapkan address agar bisa mencapai tujuan dengan tepat dan efisien.

Tabel Routing

Pengaturan routing tidak akan lepas dari tabel routing (*routing table*). Tabel routing yang bisa digunakan ada tiga jenis, yaitu tabel local, tabel main dan tabel default.

Karena tabel main yang merupakan tabel yang akan digunakan dalam pernyusunan Tugas Akhir ini, maka akan dikaji lebih dalam mengenai tabel ini.

Tabel routing main merupakan tabel routing yang sering dipanggil secara umum. Tabel ini dapat dipanggil dan dimanipulasi dengan perintah `route`. Contoh penerapannya adalah seperti berikut :

```
# route add –net 10.1.0.0 netmask 255.255.0.0 gw
20.1.0.254
```

Arti dari perintah diatas adalah, tambahkan pertintah pada tabel routing sebanyak satu baris dengan maksud melakukan koneksi ke jaringan 10.1.0.0 dengan netmask 255.255.0.0 melalui gateway 20.1.0.254.

Tampilan tabel routing itu sendiri adalah sebagai berikut :

```
root@ryota:/home/adhi# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.1.0.0        20.1.0.254      255.255.0.0     UG    0      0        0 eth0
localnet        *               255.255.0.0     U     0      0        0 eth0
root@ryota:/home/adhi#
```

2.2 Manajemen IP Address

Dalam linux, manajemen IP address dilakukan dengan menggunakan perintah `ifconfig`. Program ini sudah default dalam instalasi sistem operasi linux sehingga dapat dipanggil langsung. Berikut penjelasan lebih lanjut mengenai perintah `ifconfig`.

2.2.1 ifconfig

ifconfig berguna untuk beragam keperluan, diantaranya me-review IP address dan penggunaan opsi interface, menghidupkan dan mematikan sebuah interface.

Kegunaan paling dasar perintah ifconfig adalah melaporkan IP address sebuah interface dan statistik yang berkaitan lainnya seperti device Ethernet yang dimiliki, address hardware, IP address, broadcast, netmask, dan state IP interface.

2.3 Manajemen IP routing

Routing IP merupakan bagian mendasar dalam suatu jaringan. Penentuan route IP dilakukan untuk mengetahui bahwa mesin memiliki rute tepat ke setiap jaringan yang perlu melakukan pertukaran paket IP.

Dalam merancang suatu jaringan, satu elemen kunci yang penting diperhatikan adalah tabel routing yang telah dijelaskan diatas. Berikut akan dijelaskan lebih lanjut mengenai manipulasi tabel routing dengan menggunakan perintah `route`.

2.3.1 route

Perintah `route` datang dalam sistem Unix untuk melakukan tugas menampilkan rute, menambahkan rute (terutama rute default), menghapus rute dan memeriksa routing cache. Tampilan tabel routing adalah seperti pada penjelasan sebelumnya.

Tabel routing ini yang nantinya akan mengatur gateway antar jaringan untuk dapat terkoneksi satu sama lainnya.

2.4 Pengertian Firewall

Firewall adalah suatu aturan yang diterapkan baik terhadap *hardware*, *software* ataupun jaringan dengan maksud untuk melindungi, baik dengan melakukan filterisasi, membatasi ataupun menolak suatu koneksi pada jaringan yang dilindunginya. Firewall itu sendiri memiliki tiga peran, yaitu mengendalikan, mengamankan dan mencegah serangan pada jaringan.

Firewall terbagi menjadi empat jenis menurut fungsinya, yaitu Packet Filtering Gateway, Application Level Gateway, Circuit Level Gateway dan Stateful Multilayer Inspection Firewall. Pada tugas akhir ini, firewall yang disusun adalah jenis *staeful multilayer inspection firewall*yang bekerja pada tiga lapisan OSI.

2.5 IPTABLES

IPTABLES adalah suatu aplikasi yang membantu user dalam mengatur *policy-policy* untuk menciptakan suatu pengamanan dalam jaringan. IPTABLES itu sendiri terdiri dari table table yaitu table INPUT, OUTPUT, FORWARD, NAT (*Network Address Traslation*) dan *Mangle* (*Mark*). Dimana aturan-aturan yang diberlakukan dan dibuat oleh user pada table ini yang menentukan tingkat keamanan pada jaringan.

Tabel 2.1 Tabel filter pada IPTABLES

No.	Input	Output	Forward
1	Aturan no. 1	Aturan no. 1	Aturan no. 1
2	Aturan no. 2	Aturan no. 2	Aturan no. 2
POLICY	**ACCEPT/DROP**	**ACCEPT/DROP**	**ACCEPT/DROP**

Tabel 2.2 Tabel NAT pada IPTABLES

No.	Postrouting (SNAT)	Prerouting (DNAT)	Output
1	Aturan no. 1	Aturan no. 1	Aturan no. 1
2	Aturan no. 2	Aturan no. 2	Aturan no. 2
POLICY	**ACCEPT/DROP**	**ACCEPT/DROP**	**ACCEPT/DROP**

Tabel 2.3 Tabel Mangle

No.	Prerouting	Input	Forward	Output	Postrouting
1.	Aturan no.1	Aturan no.1	Aturan no.1	Aturan no.1	Aturan no.1
2.	Aturan no.2	Aturan no.2	Aturan no.2	Aturan no.2	Aturan no.2
POLICY	**ACCEPT/ DROP**	**ACCEPT/ DROP**	**ACCEPT/ DROP**	**ACCEPT/ DROP**	**ACCEPT/ DROP**

2.6 Layer 7 Filter

Firewall yang dahulu terbatas dengan melakukan filtrasi berdasarkan port yang dilaluinya, sekarang tidak lagi. Dengan menggunakan patch yang disediakan oleh netfilter, firewall sekarang ini memungkinkan untuk melakukan filter berdasarkan aplikasi yang dibawa oleh paket yang melewati firewall tersebut. Hal ini sangat berguna dalam melakukan filtrasi aplikasi seperti bittorrent yang senantiasa mencari dan memanfaatkan port yang terbuka dalam suatu jaringan tanpad tergantung pada satu port pun.

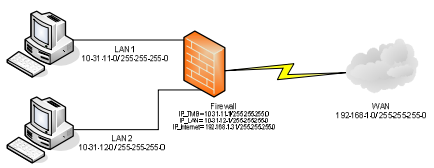
Patch ini juga membutuhkan suatu patch *protocol definition* untuk dapat menterjemahkan aplikasi yang dibawa oleh paket yang melewati firewall tersebut. Setelah layer 7 filter ini aktif, maka struktur perintahnya dapat dituliskan sebagai berikut :

iptables […] –m layer7 --l7proto […] –j […]

3 Desain dan Implementasi Perancangan dan Analisis Firewall Layer 7 Filter

Tugas akhir ini akan merancang *firewall* dengan konsep ACCEPT yang nantinya akan diterapkan pada jaringan Teknik Elektro. Seperti yang telah dijelaskan, bahwa dengan konsep ACCEPT *firewall* membuka semua port yang ada dan menyeleksi satu per satu port yang ingin diblok. Untuk membantu meningkatkan keamanan pada *firewall* yang diterapkan, menggunakan *layer* 7 *filter* yang dapat melakukan filtrasi berdasarkan aplikasi.

3.1 Topologi Jaringan



Gambar 3.1 Topologi jaringan Teknik Elektro

Terdapat dua zona yang ada pada topologi di atas, yaitu Intranet (LAN) dan Internet. Sebagai penghubung antara kedua zona tersebut adalah sebuah *firewall*. Di komputer *firewall* inilah aturan-aturan dan *policy-policy* diterapkan untuk membatasi hak akses untuk tiap zona yang yang ada.

Pada Jaringan Teknik Elektro, zona LAN tersegmentasi menjadi dua, yaitu jaringan dengan alamat 10.31.11.0/ 255.255.255.0 dan alamat jaringan 10.31.12.0/ 255.255.255.0. Jaringan WAN terkoneksi dengan LAN *Backbone* Fakultas Teknik dan secara tidak langsung terhubung dengan jaringan internet.

3.3 Hak Akses Jaringan

Setelah menentukan topologi jaringan yang akan digunakan dan servis-servis yang telah diterangkan di atas, hak akses antar zona harus ditentukan. Secara garis besar dapat dijelaskan bahwa topologi jaringan yang digunakan adalah *Bastion Host* dimana menghubungkan dua zona yaitu intranet dan internet yang diantaranya terhubung suatu firewall. Firewall inilah yang bertugas sebagai pengatur hak akses dari intranet dan internet.

Tabel 3.1 Daftar koneksi-koneksi yang tidak diperbolehkan pada konsep *default policy* ACCEPT

No.	Zona	Servis	Koneksi		Port
			Dari	Ke	
1	Firewall	Ping	Firewall	LAN 1	ICMP
2	Firewall	FTP	Firewall	LAN 1	21/ tcp
3	Firewall	SSH	Firewall	LAN 1	22/ tcp
4	Internet	All	Internet	Firewall	0-65535
5	Internet	All	Internet	Firewall	0-65535
6	LAN 1	Bittorrent, Gnutella, eDonkey	LAN 1	Internet	Layer 7 Filter
7	Firewall	Ping	Firewall	LAN 2	ICMP
8	Firewall	FTP	Firewall	LAN 2	21/ tcp
9	Firewall	SSH	Firewall	LAN 2	22/ tcp
10	LAN 2	Bittorrent, Gnutella, eDonkey	LAN 2	Internet	Layer 7 Filter
11	Internet	Bittorrent	Internet	LAN 1 dan LAN 2	Layer 7 Filter
12	LAN 2	Ping	LAN 2	LAN 1	ICMP
13	LAN 2	FTP	LAN 2	LAN 1	21/ tcp
14	LAN 2	SSH	LAN 2	LAN 1	22/ tcp

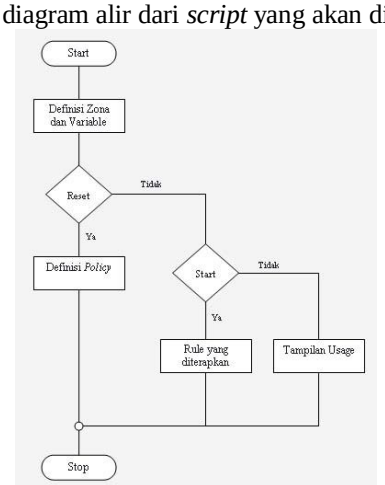
Script yang akan disusun dalam konsep ini menggunakan dua pencatatan (*log*), yaitu DROPLOG dan L7DROPLOG yang digunakan untuk mencatat paket-paket yang melanggar aturan yang telah ditentukan oleh firewall. Berikut tugas setiap *log* yang digunakan :

1 DROPLOG : Log ini mencatat semua paket yang diblok berdasarkan port yang dilaluinya
2 L7DROPLOG : Log ini mencatat semua paket yang diblok berdasarkan aplikasi

4. Implementasi dan Pengujian

Script ini akan dibagi menjadi dua bagian, yaitu bagian “reset” dan “start”. Reset berisikan perintah-perintah pembersihan pada tabel iptables. Pembersihan ini meliputi pembersihan perintah yang ada pada iptables dan menghapus tabel-tabel yang ditambahkan secara manual ke tabel iptables. Sedangkan bagian start berisikan aturan-aturan yang akan diterapkan pada *firewall*. Konsep dasar dari *firewall* ini adalah membuka semua port yang ada (0-65535) dan mem-*filter* serta menolak paket-paket yang dianggap tidak perlu atau membahayakan. Untuk proses filtrasi sendiri, juga dibantu dengan *layer* 7 *filter* untuk

melakukan filtrasi berdasarkan aplikasi. Berikut pada gambar 4.1 diagram alir dari *script* yang akan dibuat :



Gambar 4.1 Diagram alir *script* firewall dengan *default policy* ACCEPT

4.1 Implementasi

Script dengan konsep *default policy* ini diberi nama iptables.coba dan untuk mengaktifkannya adalah dengan memanggil alamat letak *script* tersebut dengan dua tahapan, yaitu perintah reset dan start. Perintahnya adalah sebagai berikut :

```
debian:~# /usr/local/src/iptables-1.3.5/iptables.coba reset
```

Maka akan tampil pesan yang menerangkan bahwa *firewall* sedang dalam proses pembersihan, lalu apabila telah selesai akan menampilkan pesan bahwa *firewall* telah dibersihkan. Pesannya dapat terlihat sebagai berikut :

```
resetting firewall...
firewall has been reset!
```

Langkah berikutnya adalah memasukkan *policy* dan *rule* yang telah diatur dan ditetapkan dengan menggunakan perintah sebagai berikut :

```
debian:~# /usr/local/src/iptables-1.3.5/iptables.coba start
```

Maka akan tampil pesan bahwa *policy* sedang dimasukkan pada tabel-tabel iptables. Dan apabila telah selesai mengatur *policy* pada iptables, akan tampil pesan bahwa *firewall* telah siap digunakan.

```
applying firewall…
setting POLICY..... done!
APPLIYING RULES..... done!
#### FIREWALL IS READY ####
```

Dan apabila tidak mencantumkan reset atau start pada perintah, maka akan tampil pesan penggunaan sebagai berikut :

```
debian:~# /usr/local/src/iptables-1.3.5/iptables.coba
Cara penggunaan rule : iptables.adhi [reset|start]
debian:~#
```

4.2 Pengujian

Pengujian meliputi pengujian koneksi dan pengujian firewall. Berikut pengujian untuk tiap-tiap koneksi.

4.2.1 Koneksi Router

Prinsip dari suatu router yang telah dijelaskan sebelumnya adalah untuk dapat menghubungkan suatu jaringan dengan alamat network yang berbeda. Pada tugas akhir ini akan menghubungkan dua zona dan tiga jaringan yang memiliki alamat *network* yang berbeda. Sehingga untuk menguji router adalah dengan melakukan ping antar jaringan. Berikut perintah ping dari LAN ke jaringan luar :

1. Zona LAN (10.31.12.0/ 255.255.255.0)
   - Ping DNS Kampus
     ```
     adhi@LAN:~$ ping 192.168.1.47
     PING 192.168.1.47 (192.168.1.47) 56(84) bytes of data
     64 bytes from 192.168.1.47: icmp_seq=1 ttl=63 time=0.355
     ms
     64 bytes from 192.168.1.47: icmp_seq=2 ttl=63 time=0.320
     ms
     ```
   - Ping Gateway Kampus
     ```
     adhi@LAN:~$ ping 10.31.12.1
     PING 10.31.12.1 (10.31.12.1) 56(84) bytes of data
     64 bytes from 10.31.12.1: icmp_seq=1 ttl=63 time=0.355 ms
     64 bytes from 10.31.12.1: icmp_seq=2 ttl=63 time=0.320 ms
     ```
   - Ping Internet
     ```
     adhi@LAN:~$ ping www.google.com
     PING www.google.com (64.233.189.104) 56(84) bytes of data
     64 bytes from 64.233.189.104: icmp_seq=1 ttl=63
     time=0.855 ms
     64 bytes from 64.233.189.104: icmp_seq=2 ttl=63
     time=0.930 ms
     ```

4.2.2 Firewall

Pengujian *firewall* yang diterapkan dalam jaringan Teknik Elektro dengan *default policy* ACCEPT meliputi pengujian Ping, SSH, FTP, HTTP, Traceroute, pencatatan dan blok paket. Berikut penjelasan lebih terperinci :

4.2.2.1 Ping

Pengujian ping dilakukan pada zona LAN (10.31.12.0/ 255.255.255.0) dan *firewall*. Hak akses ping disini memperbolehkan kedua zona LAN untuk melakukan ping pada jaringan manapun, namun tidak dapat antar zona melakukan ping. Tidak diperbolehkan pula *firewall* dan jaringan luar untuk melakukan ping pada jaringan LAN. Akan diujikan hak akses ping sebagai berikut :

- Ping dari zona LAN 2 (10.31.12.0/ 255.255.255.0) ke firewall
  ```
  adhi@LAN:~$ ping 10.31.12.1
  PING 10.31.12.1 (10.31.12.1) 56(84) bytes of data
  64 bytes from 10.31.12.1: icmp_seq=1 ttl=63 time=0.386 ms
  64 bytes from 10.31.12.1: icmp_seq=2 ttl=63 time=0.340 ms
  ```
- Ping dari zona LAN 2 (10.31.12.0/ 255.255.255.0) ke 0/0
  ```
  adhi@LAN:~$ ping www.google.com
  PING www.google.com (64.233.189.104) 56(84) bytes of data
  64 bytes from 64.233.189.104: icmp_seq=1 ttl=63 time=1111
  ms
  64 bytes from 64.233.189.104: icmp_seq=2 ttl=63
  time=2453 ms
  ```
- Ping dari Firewall ke LAN 2(10.31.12.0/ 255.255.255.0)
  ```
  debian:~# ping 10.31.12.169
  PING 10.31.12.169 (10.31.12.169) 56(84) bytes of data
  ping: sendmsg: Operation not permitted
  ping: sendmsg: Operation not permitted
  ```
- Ping dari Firewall ke 0/0
  ```
  debian:~# ping www.google.com
  PING www.google.com (64.233.189.104) 56(84) bytes of data
  64 bytes from 64.233.189.104: icmp_seq=1 ttl=63 time=442
  ms
  64 bytes from 64.233.189.104: icmp_seq=2 ttl=63 time=442
  ms
  ```

4.2.2.2 FTP (*File Transfer Protocol*)

FTP adalah servis yang digunakan untuk melakukan pemindahan data antar jaringan. Untuk semua zona dapat menggunakan hak akses ini, namun untuk zona internet tidak dapat melakukan FTP pada zona manapun. Berikut pengujian FTP tiap zona :

- FTP dari zona LAN ke firewall

```
adhi@LAN:~$ ftp 10.1.0.254
Connected to 20.1.0.254.
Name (20.1.0.2:root):adhi
Password :
ftp>
```

4.2.2.3 SSH (*Secure Shell*)

Pengujian SSH juga dilakukan antara tiap zona, akan disimulasikan akses SSH dari LAN 2 (10.31.12.0/ 255.255.255.0) ke *firewall* pada jaringan yang telah dibuat.

```
adhi@LAN:~$ ssh root@10.31.12.1
Are you sure you want to continue connecting (yes/no)? yes
root@10.31.12.1's password:
debian:~#
```

4.2.2.4 HTTP

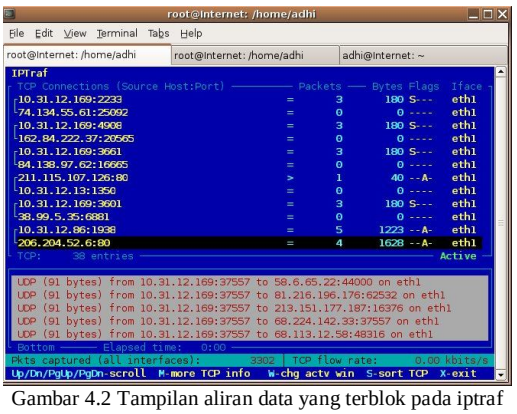
Pengujian servis HTTP tidak lepas dengan pengujian DNS dan SSL. Pengujian HTTP ini adalah dengan membuka web yang diperoleh dari internet dari zona LAN ataupun *firewall*. Dengan menggunakan salah satu program yang telah disediakan oleh sistem operasi Linux Ubuntu, yaitu Opera, *browse* ke salah satu web yang menggunakan servis SSL seperti contoh yaitu situs yahoo dan google. Apabila telah berhasil membuka halaman situs tersebut, maka hak akses HTTP, SSL dan DNS telah terbukti aktif dan diperbolehkan oleh *firewall*.

4.2.2.5 Traceroute

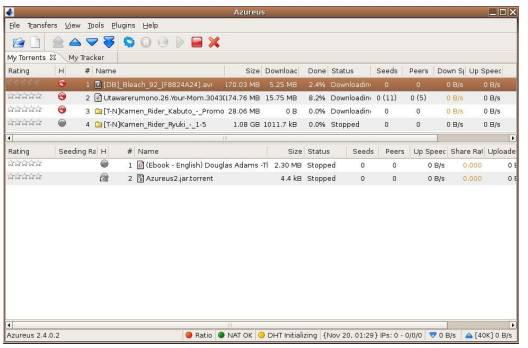
Traceroute disini dapat diujikan pada koneksi antara *Firewall* dan Internet, atau LAN ke Internet. Satu contoh kinerja traceroute dari LAN ke Internet adalah sebagai berikut :

```
adhi@LAN:~$ traceroute www.google.com
traceroute to www.l.google.com (64.233.189.104), 30 hops
max, 38 byte packets
  1 10.31.12.1 (10.31.12.1) 0.332 ms 0.290 ms 0.272 ms
  2 192.168.1.95 (192.168.1.95) 1351.494 ms 2715.396 ms
  3 49.subnet222-124-22.astinet.telkom.net.id
  (222.124.22.49) 2190.976 ms
  4 * *
```

Dalam pengujian *filter* pada *layer* 7 dicontohkan pada program bittorrent. Pada zona LAN 2 (10.31.12.0/ 255.255.255.0) menjalankan program bittorrent. Pengujian yang benar adalah apabila tidak ada file sedikitpun yang masuk ke LAN 2 dari port-port yang digunakan oleh bittorrent. Berikut pada gambar memperlihatkan aliran paket dengan menggunakan program iptraf, serta program torrent Azureus yang tidak dapat melakukan download.



Gambar 4.2 Tampilan aliran data yang terblok pada iptraf

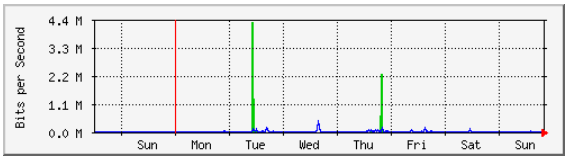


Gambar 4.3 Tampilan program Azureus yang terblok oleh layer 7 filter

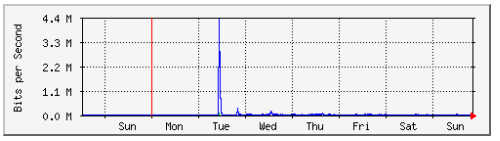
Disinilah kelebihan utama dari *firewall* yang disusun. Kemampuannya dalam melakukan filtrasi pada *layer* 7 dan tidak hanya berdasarkan port. Konsep ini sangat cocok dengan jaringan Teknik Elektro yang selama ini masih sulit untuk melakukan filtrasi pada bittorrent.

4.3 Perbandingan Traffic pada Penerapan Firewall

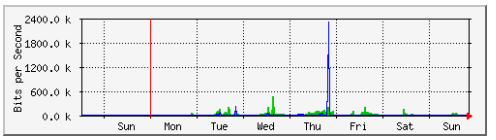
Dengan menerapkan *firewall layer* 7 *filter* ini pada jaringan Teknik Elektro, terbukti menstabilkan *traffic* dan tidak ada lagi pembanjiran data pada *traffic*. Pada penelitian yang dilakukan, *traffic* jaringan Teknik Elektro sangat berpengaruh pada jaringan Fakultas Teknik. Hal ini dikarenakan banyaknya komputer pada Teknik Elektro yang menggunakan program-program bittorrent. Berikut pada gambar 4.4, 4.5 dan 4.6 akan ditampilkan grafik *traffic* pada jaringan Teknik Elektro setelah satu minggu pemasangan dengan menggunakan program MRTG.



Gambar 4.4 Tampilan *traffic* tiap hari pada interface eth0 jaringan Teknik Elektro



Gambar 4.5 Tampilan *traffic* tiap hari pada interface eth1 jaringan Teknik Elektro

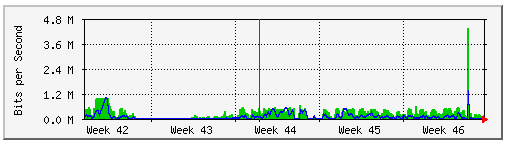


Gambar 4.6 Tampilan *traffic* tiap hari pada interface eth2 jaringan Teknik Elektro

Pada grafik, warna biru mewakili data yang keluar dari *interface* (*Outgoing*) dan warna hijau mewakili data yang masuk ke *interface* (*Incoming*). Dengan hak akses yang dibatasi pada jaringan Teknik Elektro, tidak ada lagi pembanjiran data baik pada *traffic* jaringan Teknik Elektro maupun pada *traffic* jaringan Fakultas Teknik.

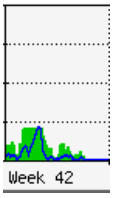
Jaringan Fakultas Teknik memiliki dua interface yang terhubung keluar jaringan, dan satu interface yang

menghubungkan semua jurusan Teknik di Universitas Diponegoro, yaitu jurusan Teknik Elektro, Teknik Mesin, Teknik Planologi dan Teknik Sipil. *Interface* eth0 dan eth1 pada *gateway* Fakultas Teknik terhubung dengan jaringan luar (WAN) dan *interface* eth3 terhubung dengan jaringan lokal. Pada gambar 4.7 akan menampilkan grafik Fakultas Teknik setelah penerapan *firewall layer* 7 *filter* ini pada minggu ke-46.



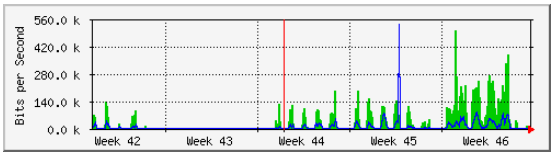
Gambar 4.7 Tampilan *traffic* tiap minggu pada interface eth0 jaringan Fakultas Teknik

Firewall layer 7 *filter* ini diterapkan pada minggu ke 46, hari Senin tanggal 13 November 2006. Terlihat bahwa data yang masuk pada interface eth0 terlihat normal pada masa pemasangan *firewall* "week 46". Salah satu contoh banjir data yang terjadi sebelum pemasangan *firewall* adalah pada minggu ke-42 dimana data yang masuk sama besar dengan data yang keluar, yaitu berkisar antara 800 sampai 900 kbit per second. Pada gambar 4.8 menampilkan salah satu banjir data yang terjadi pada jaringan Fakultas Teknik.



Gambar 4.8 Tampilan banjir data yang terjadi pada jaringan Fakultas Teknik

Dengan menerapkan firewall pada jurusan Teknik Elektro, ternyata juga berpengaruh pada koneksi internet pada jurusan yang lain. Contohnya adalah pada grafik berikut :



Gambar 4.9 Tampilan grafik *traffic* tiap minggu pada *interface* eth0 jaringan Teknik Mesin

Pada minggu ke-46 terlihat bahwa bandwidth yang dapat dipergunakan oleh jaringan Teknik Mesin meningkat dua kali lipat. Karena bandwidth tidak lagi dipenuhi oleh paket-paket download, maka dapat dipergunakan secara merata oleh jurusan-jurusan yang terkoneksi pada Fakultas Teknik.

5.Kesimpulan dan Saran

5.1 Kesimpulan

1. Ada dua konsep yang dapat digunakan dalam merancang suatu firewall, yaitu konsep *default policy* DROP dan *default policy* ACCEPT. *Policy* DROP bekerja dengan menutup semua port yang ada dan menyeleksi satu per satu servis dan port yang dibuka. Sebaliknya, pada *policy* ACCEPT, semua port dibuka lalu menyeleksi satu per satu servis dan port yang akan ditutup. Pada penerapan firewall pada jaringan Teknik Elektro menggunakan konsep ACCEPT.
2. Penulisan *rule* pada script memiliki aturan yang harus dipenuhi, yaitu menulis aturan yang bersifat khusus dahulu pada script, lalu semakin ke bawah semakin umum. Menghindari pula ketidakkonsistenan pada aturan *script*, menuliskan semua port dan servis yang di ACCEPT dahulu lalu menuliskan port yang ditutup pada akhir script.
3. Filtrasi yang digunakan pada *firewall* menggunakan filtrasi berdasarkan port dan aplikasi.
4. Dengan menggunakan *patch layer* 7 *filter*, dapat menambah tingkat keamanan *firewall* karena kemampuannya yang tidak hanya dapat mem-*filter* paket berdasarkan port tetapi juga berdasarkan aplikasi yang dibawa oleh paket tersebut.
5. Dengan menggunakan *firewall layer* 7 *filter*, terbukti dapat memberikan pengaruh yang signifikan pada jaringan Fakultas Teknik baik dari segi *bandwidth* maupun keamanan jaringan pada Teknik Elektro pada khususnya. Pembagian *bandwidth* untuk tiap jurusan semakin stabil dan koneksi semakin cepat.

5.2 Saran

1. Keamanan jaringan pada Fakultas Teknik dapat ditingkatkan dengan menerapkan *firewall layer* 7 *filter* pada tiap gateway jurusan, serta untuk gateway utama Fakultas Teknik dapat menggunakan firewall dengan *filter* biasa.
2. Meningkatkan keamanan jaringan tidak hanya menggunakan *firewall layer* 7 *filter*, namun lebih baik juga dengan menggunakan manajemen *bandwidth* untuk mengatur *bandwidth* antar jurusan.

6. Referensi

[1] Farunuddin, R., *Membangun Firewall dengan IPTables di Linux*, Penerbit PT. Elex Media Komputindo Kelompok Gramedia, Jakarta, 2005.

[2] Rafiudin, R., *IP Routing dan Firewall Dalam Linux*, Penerbit ANDI, Yogyakarta, 2006.

[3] Linux Learning Center, *Modul Pelatihan Linux System Administrator*, 2004.

[4] Linux Learning Center, *Linux Security*, 2004.

[5] Mike Chappel, *Choosing The Right Firewall Topology*, 2006

[6] ---, en.wikipedia.org

[7] ---, http://searchsecurity.techtarget.com/

[8] ---, http://www.howtoforge.com/forum

[9] ---, http://l7-filter.sourceforge.net

BIOGRAFI PENULIS

Adhi Laksono, lahir di Semarang, Jawa Tengah 3 Juni 1984. Menempuh pendidikan di SD Don Bosko Semarang, SD Ysgol Y Borth Wales, SD Boyolali 9, SD Sompok Semarang, SLTP Negeri 5 Semarang dan SMU Negeri 1 Semarang. Saat ini sedang menyelesaikan pendidikan program Strata 1 Jurusan Teknik Elektro Universitas Diponegoro dengan mengambil konsentrasi Teknik Informatika dan Komputer. Topik tugas akhir yang diambil tentang desain dan implementasi firewall dengan layer 7 filter pada jaringan Teknik Elektro.

Menyetujui dan mengesahkan,

Dosen Pembimbing I

Agung B. P., S.T., M.I.T.
NIP. 132 137 932
Tanggal……...

Dosen Pembimbing II

Adian Facturrochim, S.T., M.T.
NIP. 132 205 680
Tanggal……...