BAB IV
METODE PENELITIAN

Metode penelitian yang digunakan pada pembuatan perangkat lunak (*software*) yaitu berasal dari studi kepustakaan. Dengan cara ini penulis berusaha untuk mendapatkan dan mengumpulkan data-data, informasi, konsep-konsep yang bersifat teoritis dari buku, bahan-bahan kuliah dan internet yang berkaitan dengan permasalahan yang akan diselesaikan.

4.1. Pemahaman Literatur

Dalam kerja praktek yang yang kami kerjakan di CV. Dika Tekindo Jaya terdapat permasalahan dalam hal keamanan jaringan komputer yang salah satunya adalah pengendalian akses baik di jaringan internal maupun eksternal. Untuk membantu menyelesaikan permasalahan yang disebutkan diatas kami mencoba memberikan solusi dengan menerapkan suatu aplikasi yang berbasis open source. Aplikasi berbasis Linux disini kami pilih karena selain bersifat open source sehingga bebas dipergunakan dan dikembangkan sesuai keinginan juga sudah terbukti handal digunakan sebagai sistem operasi pada server.

Untuk menyelesaikan permasalahan kendali akses seperti diatas kami menggunakan metode firewall untuk mengatur hak akses dalam jaringan internal, sedangkan pada jaringan eksternal digunakan metode proxy server. Aplikasi firewall di jaringan internal menggunakan iptables sedangkan untuk aplikasi proxy server menggunakan squid. Penggunaan Iptables dan Squid pada kerja praktek ini dikarenakan kedua aplikasi tersebut memiliki performa dan fitur yang baik untuk pengaturan konfigurasinya.

Penyelesaian yang kami utarakan diatas dibagi menjadi beberapa tahap. Pada tahapan pertama kami melakukan konfigurasi firewall dengan menggunakan iptables untuk mengatur hak akses di jaringan intenal. Hak akses yang dimaksudkan disini adalah untuk memberikan aturan terminal mana saja yang diperbolehkan untuk mengakses server yang tersedia. Tahapan kedua kami gunakan untuk melakukan konfigurasi Squid yang berfungsi sebagai proxy server.

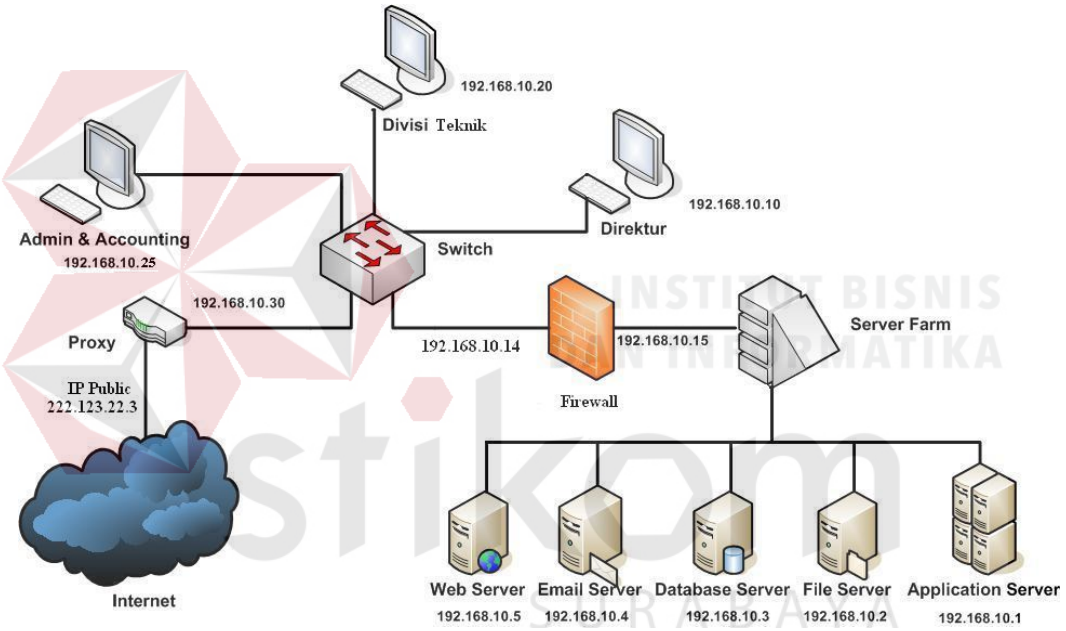
Perancangan firewall kami terapkan pada jaringan internal dimana dalam jaringan internal ini terdapat beberapa divisi yaitu divisi administrasi, divisi teknik dan direktur dengan hak akses yang berbeda pada masing-masing divisi. Untuk lebih jelasnya, pada perancangan firewall terdapat aturan hak akses terhadap server sebagai berikut:

1. Direktur memiliki hak akses terhadap *server farm* sehingga dapat mengakses ke semua bagian pada server kecuali pada Database server.
2. Divisi administrasi *dan accounting* memiliki hak akses terhadap Web server, Email server, dan Database server.
3. Sedangkan divisi teknik perusahaan dapat memiliki hak akses terhadap web server, email server dan aplikasi server.
4. Semua terminal komputer yang berada pada jaringan internal dapat terhubung ke internet.

Sedangkan untuk mengatur koneksi internet serta hak akses dari beberapa divisi, kami gunakan aplikasi Squid proxy server. Perancangan Squid proxy server disini terutama untuk membatasi akses ke situs-situs yang dilarang serta akses ke internet harus melalui proxy server.

4.2 Pemodelan Sistem

Sebelum melangkah ketahap berikutnya, diperlukan sebuah *planning* / perencanaan yang detail terhadap sistem keamanan yang akan diaplikasikan di perusahaan. Perencanaan tersebut meliputi pola desain sistem, pengendalian akses dari setiap terminal divisi maupun koneksi terhadap server perusahaan serta terhadap jaringan internet. Secara garis besar desain perencanaan sistem yang akan dipergunakan terdapat pada gambar 4.1:



Gambar 4.1. Perencanaan Desain Jaringan CV. Dika Tekindo Jaya

Berdasarkan gambar perencanaan diatas peletakan firewall berada diantara switch dan server farm sehingga masing-masing divisi perusahaan yang terhubung dengan switch harus melalui firewall ini untuk dapat mengakses server. Sedangkan sebagai jembatan penghubung antara terminal komputer di setiap divisi atau jaringan internal dengan jaringan eksternal (internet) kami mengaplikasikan proxy server Squid, sehingga setiap komputer di jaringan internal yang hendak mengakses internet harus melalui proxy maupun sebaliknya.

Dalam desain perencanaan disini, kami hanya membatasi user / terminal komputer yang terhubung dalam jaringan yakni : divisi *accounting* / *admin*, divisi teknik, dan direktur. Sebenarnya banyak bagian-bagian lainnya yang terhubung dalam jaringan di CV. Dika Tekindo Jaya, hanya saja karena keterbatasan sarana dan sistem tersebut hanya dipakai untuk sarana pembelajaran jaringan komputer maka kami membatasi jumlah user yang terhubung dalam jaringan.

4.3 Peralatan Penelitian

Peralatan yang digunakan dalam riset ini antara lain komputer AMD Duron 850 MHz dengan *memory* sebesar 256 Mb Hardisk 40 Gb untuk system operasinya menggunakan linux red hat 9.

4.4 Perancangan Perangkat Lunak

A. Konfigurasi Firewall:

Firewall disini digunakan untuk mengendalikan akses terhadap server atau dengan kata lain melakukan seleksi komputer mana saja, protokol maupun port yang diperbolehkan untuk mengakses server. Dalam perancangan jaringan di CV. Dika Tekindo Jaya kami mencoba menerapkan aplikasi firewall menggunakan iptables dengan file konfigurasi yang disimpan pada /etc/rc.local seperti berikut:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

 # Menghapus semua aturan , tabel nat,chain dan menghapus chain yang berada di dalam tabel nat.

```
iptables –flush
```

iptables –table nat –flush

iptables –delete-chain

iptables –table nat –delete-chain

 # Mengaktifkan masquerade untuk membolehkan LAN mengakses internet

Iptables –table nat – append POSTROUTING –out-interface eth0 –j MASQUERADE

 # Meneruskan trafik LAN dari eth1 menuju internet (eth0)

Iptables – A forward –I eth1 –O eth0 –m state - -state NEW,ESTABLISHED –j ACCEPT

Iptables –table nat – append POSTROUTING –out-interface eth0 –j SNAT - - to –source eth1

 # Mengalihkan semua akses yang ke port 80(http) agar melalui proxy server

Iptables –table nat – append PREROUTING –in-interface eth0 –p TCP - - DPORT 80 – j REDIRECT - - to – PORT 3128

 # Hak akses komputer Direktur

Iptables –A INPUT –p tcp–s 192.168.10.10 –d 192.168.10.3 –j DROP

 # Hak akses komputer divisi *account*

Iptables –A INPUT –p tcp –s 192.168.10.25 –d 192.168.10.1 –j DROP

Iptables –A INPUT –p tcp –s 192.168.10.25 –d 192.168.10.2 –j DROP

 # Hak akses komputer divisi teknik

Iptables –A INPUT –p tcp –s 192.168.10.20 –d 192.168.10.2 -j DROP

Iptables –A INPUT –p tcp –s 192.168.10.20 –d 192.168.10.3 –j DROP

 # untuk mengijinkan agar komputer di jaringan eksternal (internet) bisa mengakses port FTP, HTTP

Iptables –A INPUT –p tcp –i eth0 –dport 8080 –j ACCEPT

Iptables –A INPUT –p udp –i eth0 –dport 8080 –j ACCEPT

Iptables –A INPUT –p tcp –i eth0 –dport 21 –j ACCEPT

Iptables –A INPUT –p tcp –i eth0 –dport 21 –j ACCEPT

 # menolak semua akses selain yang tersebut diatas

Iptables –P INPUT DROP

B. Konfigurasi Squid Server Proxy

Berikut konfigurasi SQUID berdasarkan aturan yang diinginkan dalam perusahaan yang terdapat pada file **/etc/squid/squid.conf** :

 # Parameter port

http_port 8080

icp_port 0

 # Parameter option ukuran cache

cache_mem 256 MB

cache_swap_low 94

cache_swap_high 96

maximum_object_size 16384 KB

minimum_object_size 4 KB

maximum_object_size_in_memory 2048 KB

fqdncache_size 1024

 # Parameter direktori log dan cache

cache_dir aufs /var/spool/squid 9000 16 256

access_log /var/log/squid/access.log squid

cache_log /var/log/squid/cache.log

cache_store_log none

 # Parameter *blacklist*

acl noblacklist dstdomain "/etc/squid/blacklist/no-blacklist.txt"

acl domainblacklist dstdomain "/etc/squid/blacklist/domain-blacklist.txt"

acl katablacklist url_regex -i "/etc/squid/blacklist/kata-blacklist.txt"

acl ipblacklist dst "/etc/squid/blacklist/ip-blacklist.txt"

acl tdkfreedownload time 08:00-13:00

 # Parameter Kendali akses

acl all src 0.0.0.0/0.0.0.0

acl manager proto cache_object

acl localhost src 127.0.0.1/255.255.255.255

acl to_localhost dst 127.0.0.0/8

acl SSL_ports port 443

acl Safe_ports port 80 # http

acl Safe_ports port 21 # ftp

acl Safe_ports port 443 # https

acl Safe_ports port 70 # gopher

acl Safe_ports port 210 # wais

acl Safe_ports port 1025-65535 # unregistered ports

```
acl Safe_ports port 280 # http-mgmt
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
acl CONNECT method CONNECT

# Parameter daftar IP address
acl divaccadmin src 192.168.10.25/255.255.255.0
acl divteknik src 192.168.10.20/255.255.255.0
acl direktur src 192.168.10.10/255.255.255.0

acl lan src 192.168.100.0/255.255.255.0

# Parameter status blacklist
http_access allow noblacklist
http_access deny katablacklist
http_access deny domainblacklist
http access deny ipblacklist
http_access allow manager localhost
http_access deny manager

# Parameter status akses
http_access allow divaccadmin
http_access allow divteknik
http_access allow direktur
http_access allow lan
```

```
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost
http_access deny all
http_reply_access allow all
icp_access allow all

# Parameter administrator
cache_mgr kp@yahoo.com
cache_effective_user squid
cache_effective_group squid
visible_hostname proxy.kp.lokal
```

Pada parameter *blacklist* yang terdapat pada file konfigurasi diatas agar dapat digunakan, sebelumnya kita harus membuat direktori yang berisi file-file yang telah disebutkan dengan *command line*:

```
#  mkdir /etc/squid/blacklist
#  cd /etc/squid/blacklist/
```

Setelah direktori *blacklist* berhasil dibuat , masuk ke direktori yang telah dibuat dan selanjutnya *create* file *.txt dengan menggunakan editor vi seperti berikut :

```
#  vi no-blacklist.txt
# vi kata-blacklist.txt
```

```
# vi ip-blacklist.txt

# vi domainblacklist.txt
```

Pada setiap file *blacklist* diatas minimal dimasukkan satu item yang diinginkan, karena jika tidak, maka saat kita melihat *error log squid* sesaat setelah *service* dijalankan, akan ada pesan error tidak menemukan item pada file tersebut.

Setelah semua konfigurasi diatas dilakukan, kita aktifkan service Squid dengan menggunakan *command line*:

```
#  squid –z

# service squid start
```