

BAB IV

IMPLEMENTASI

Langkah yang dilakukan pada bab implementasi mengacu pada perancangan sistem server proxy yang sudah dibuat sebelumnya. Dimana raspberry pi (*embedded system*) sebagai server proxy juga dimanfaatkan sebagai *access point* yang nantinya diakses oleh client. Implementasi meliputi lingkungan perangkat keras dan perangkat lunak.

4.1 Implementasi Perangkat Keras dan Perangkat Lunak

Untuk membangun sistem server proxy dibutuhkan perangkat keras dan perangkat lunak sebagai berikut (Tabel 4.1).

Tabel 4.1 Daftar Perangkat Keras dan Perangkat Lunak

<i>Embedded System</i>	Raspberry Pi Model B
Storage	SDHC Card 8 GB
Network Interface	Ethernet LAN, Nano Wireless Adapter
Sistem Operasi	Linux Raspbian Wheezy
Perangkat Lunak	Squid3, Calamaris, Hostapd, Udhcpd

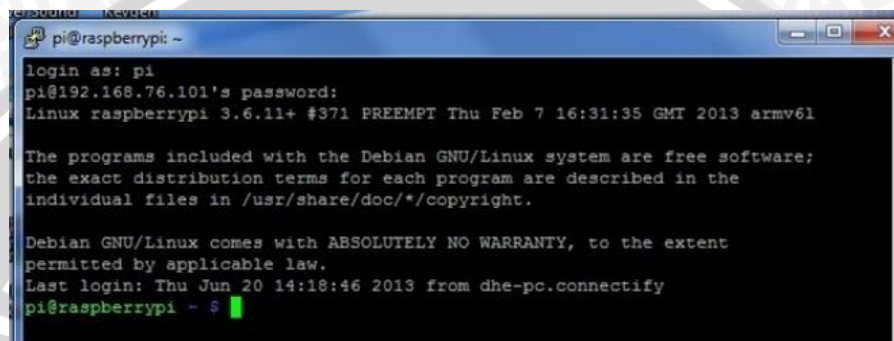
4.2 Instalasi dan Konfigurasi Sistem Operasi Embedded System

Embedded system yang digunakan untuk membangun sistem server proxy adalah Raspberry Pi (Gambar 4.1).



Gambar 4.1 Raspberry Pi Model B

Sistem operasi yang digunakan adalah Raspbian Wheezy (Debian Base) karena merupakan standart *operating system* dari Raspberry Pi. Untuk mengakses Raspberry dipergunakan aplikasi Putty (Gambar 4.2) sebagai remote Raspberry melalui eth0 (IP DHCP) atau wlan0 (IP Static : 10.0.0.1).



```
pi@raspberrypi: ~
login as: pi
pi@192.168.76.101's password:
Linux raspberrypi 3.6.11+ #371 PREEMPT Thu Feb 7 16:31:35 GMT 2013 armv6l

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Jun 20 14:18:46 2013 from dhe-pc.connectify
pi@raspberrypi ~ $
```

Gambar 4.2 Putty

4.3 Implementasi Raspberry Pi sebagai Server Proxy

Implementasi server proxy dalam *embedded system* Raspberry Pi menggunakan aplikasi proxy dasar yaitu squid3.

Konfigurasi Squid3

File konfigurasi squid3 adalah squid.conf.

Aturan yang diterapkan dalam konfigurasi untuk mengatur squid server proxy, sebagai berikut:

1. Pada saat jam kerja, social network, streaming dan portal download tidak dapat diakses. Daftar web yang tidak dapat diakses pada saat jam kerja berada dalam file kenablok.txt.
2. *Content* kata domain yang berbau pornografi dan judi tidak dapat diakses. Daftar *content* kata domain tersebut berada dalam file fullblok.txt.
3. IP server proxy 10.0.0.1 dengan port 3128.
4. Metode proxy yang digunakan adalah *transparent/intercept proxy*.

5. Cache memory yang digunakan 128 MB.
6. Besar maksimum objek yang disimpan di memory 128 KB
7. Directif yang digunakan untuk mengatur kapasitas memory dan kapasitas cache adalah heap GDSF (Greedy-Dual Size Frequency).
8. Minimum objek yang disimpan sebesar 8 KB sedangkan maximum objek yang disimpan sebesar 4 MB.
9. Mengijinkan jaringan WLAN (*access point*) 10.0.0.0/24 menggunakan cache.

Konfigurasi pada squid.conf sebagai berikut (Gambar 4.3).

```

http_port 10.0.0.1:3128 intercept
cache_mem 128 MB
maximum_object_size 4 MB
minimum_object_size 8 KB
cache_swap_low 90
cache_swap_high 95
maximum_object_size_in_memory 128 KB
cache_replacement_policy heap GDSF
memory_replacement_policy heap GDSF
cache_dir aufs /var/spool/squid3 4096 32 128
cache_access_log /var/log/squid3/access.log
cache_log /var/log/squid3/cache.log
cache_store_log /var/log/squid3/store.log
coredump_dir /var/spool/squid3
tcp_outgoing_address 10.0.0.1

#ADMINISTRATIF#
cache_mgr delisukma@gmail.com
visible_hostname ptiik.ub.ac.id/labsiskombot

#KENDALI AKSES#
#blok situs
acl kenablok url_regex -i "/etc/squid3/kenablok.txt"
acl fullblok url_regex -i "/etc/squid3/fullblok.txt"

#time setting
acl morning time MTWHF 08:00-11:59
acl afternoon time MTWHF 13:00-15:59
acl forbidden time SMTWHFA 00:00-24:00

http_access deny kenablok morning
http_access deny kenablok afternoon
http_access deny fullblok forbidden
http_access allow localnet
http_access allow localhost

```

```

http_access deny all

acl localnet src 10.0.0.0/24

#TUNING
refresh_pattern -i (.html|htm|css|js) 1440 75% 40320
refresh_pattern -i (.gif|png|jpg|jpeg|ico|bmp|tiff?) 10080
95% 43200 override-expire override-lastmod reload-into-ims
ignore-reload ignore-no-cache ignore-private
refresh_pattern -i \.gif$ 10080 90% 43200 override-expire
override-lastmod reload-into-ims ignore-reload ignore-no-
cache ignore-private
refresh_pattern -i \.jpg$ 10080 95% 1440 override-expire
override-lastmod reload-into-ims ignore-reload ignore-no-
cache ignore-private
refresh_pattern -i \.png$ 10080 95% 1440 override-expire
override-lastmod reload-into-ims ignore-reload ignore-no-
cache ignore-private
refresh_pattern -i \.jpeg$ 10080 90% 43200 override-expire
override-lastmod reload-into-ims ignore-reload ignore-no-
cache ignore-private
refresh_pattern -i \.bmp$ 10080 90% 43200 override-expire
override-lastmod reload-into-ims ignore-reload ignore-no-
cache ignore-private
refresh_pattern -i \.psd$ 10080 90% 43200 override-expire
override-lastmod reload-into-ims ignore-reload ignore-no-
cache ignore-private
refresh_pattern -i \.ad$ 10080 90% 43200 override-expire
override-lastmod reload-into-ims ignore-reload ignore-no-
cache ignore-private
refresh_pattern -i \.gif\?$ 10080 90% 43200 override-expire
override-lastmod reload-into-ims ignore-reload ignore-no-
cache ignore-private
refresh_pattern -i \.jpg\?$ 10080 90% 43200 override-expire
override-lastmod reload-into-ims ignore-reload ignore-no-
cache ignore-private
refresh_pattern -i \.png\?$ 10080 90% 43200 override-expire
override-lastmod reload-into-ims ignore-reload ignore-no-
cache ignore-private
refresh_pattern -i \.jpeg\?$ 10080 90% 43200 override-expire
override-lastmod reload-into-ims ignore-reload ignore-no-
cache ignore-private
refresh_pattern -i \.psd\?$ 10080 90% 43200 override-expire
override-lastmod reload-into-ims ignore-reload ignore-no-
cache ignore-private

refresh_pattern -i \.psf$ 1440 90% 43200
refresh_pattern -i \.html$ 1440 90% 43200
refresh_pattern -i \.htm$ 1440 90% 43200
refresh_pattern -i \.swf$ 1440 90% 43200
refresh_pattern .*\. (css)$ 1440 90% 1440 ignore-
no-cache override-expire override-lastmod ignore-private
refresh_pattern .*\. (js)$ 1440 90% 1440 ignore-
private
refresh_pattern -i \.xml$ 1440 90% 43200

refresh pattern ^ftp: 1440 20% 10080

```



```
refresh_pattern ^gopher:      1440    0%    1440
refresh_pattern -i (/cgi-bin/|\?) 0      0%    0
refresh_pattern .              0      20%   4320
```

Gambar 4.3 Konfigurasi squid

Daftar website yang termasuk dalam *blacklist* yang tidak dapat diakses pada jam-jam tertentu terdapat dalam file *kenablok.txt*. Berikut isi data dari file *kenablok.txt* (Gambar 4.4).

```
facebook.com
friendster.com
instagram.com
tumblr.com
twitter.com

youtube.com
mivo.com

4shared.com
fileshare.com
indowebster.com
mediafire.com
```

Gambar 4.4 Data *kenablok.txt*

Daftar *content* kata domain yang termasuk dalam *blacklist* yang tidak boleh diakses terdapat dalam file *fullblok.txt*. Berikut isi data dari file *fullblok.txt* (Gambar 4.5).

```
Gambling
judi
kotor
porno
porn
seks
sex
```

Gambar 4.5 Data *fullblok.txt*

Konfigurasi routing untuk mengarahkan *client* ke IP server proxy pada *embedded system*, sebagai berikut (Gambar 4.6).

```
/sbin/iptables -t nat -A PREROUTING -s 10.0.0.0/24 -d 0/0 -p
tcp -dport 80 -j DNAT -to-destination 10.0.0.1:3128
```

Gambar 4.6 Konfigurasi Routing

Konfigurasi network yang digunakan adalah sebagai berikut (Gambar 4.7).

```
auto lo
iface lo inet loopback
iface eth0 inet dhcp
```

```
#allow-hotplug wlan0
iface wlan0 inet static
address 10.0.0.1
network 10.0.0.0
netmask 255.255.255.0

up iptables-restore < /etc/iptables.ipv4.nat
```

Gambar 4.7 Konfigurasi network

4.4 Implementasi Raspberry Pi sebagai Access Point

Embedded system Raspberry Pi dimanfaatkan juga sebagai *access point* yang berfungsi untuk membuat jaringan WLAN terhadap *client*. File yang dibutuhkan untuk konfigurasi pembuatan *access point* adalah *hostapd* dan *udhcpd*.

4.4.1 Konfigurasi hostapd

Konfigurasi *hostapd* digunakan untuk membuat *access point* pada Raspberry pi. Konfigurasi *hostapd* ada pada Gambar 4.8.

```
#Basic configuration
interface=wlan0
ssid=wifi raspberry pi
channel=1

#WPA and WPA2 configuration
macaddr_acl=0
auth_algs=1
ignore_broadcast_ssid=0
wpa=2
wpa_passphrase=raspi123
wpa_key_mgmt=WPA-PSK
wpa_pairwise=TKIP
rsn_pairwise=CCMP

#Hardware configuration
driver=rtl871xdrv
ieee80211n=1
hw_mode=g
device_name=RTL8188CUS
manufacturer=Realtek

beacon_int=100
auth_algs=3
wmm_enabled=1
```

Gambar 4.8 Konfigurasi hostapd

4.4.2 Konfigurasi udhcpd

Konfigurasi udhcpd dipergunakan untuk menentukan IP Pool untuk *client* yang terhubung dengan WLAN Raspberry Pi. Konfigurasi udhcpd ada pada Gambar 4.9.

Start	10.0.0.2
end	10.0.0.11
interface	wlan0
remaining	yes

Gambar 4.9 Konfigurasi udhcpd

