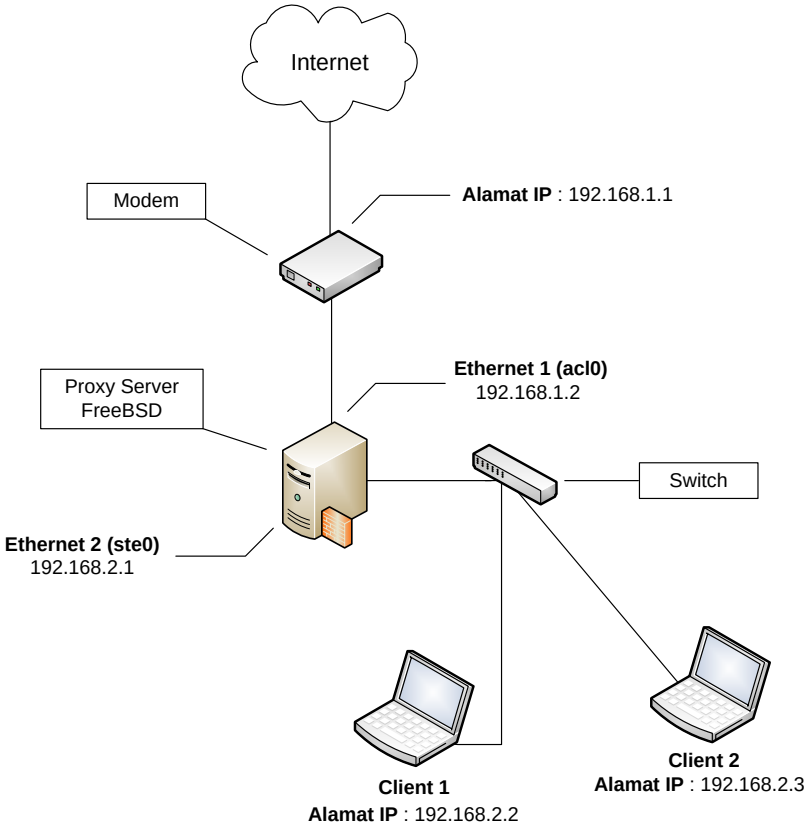
BAB 3
PERANCANGAN SISTEM

Bab ini menjelaskan tentang perancangan sistem pada *proxy server*, perancangan dikerjakan dari topologi jaringan yang digunakan, kebutuhan perangkat yang digunakan, instalasi sistem, serta konfigurasi *proxy server*. Untuk topologi jaringan yang digunakan bisa dilihat pada gambar 3.1 berikut :



Gambar **Error! No text of specified style in document.**.1 Topologi Perancangan Sistem

Penjelasan topologi perancangan sistem *proxy server* sebagai berikut:

a. Topologi jaringan yang digunakan adalah topologi *star*, dimana terdapat 1 buah *switch* sebagai konsentator bagi perangkat-perangkat yang terhubung dengan *switch*.

b. Modem sebagai *gateway* dengan alamat IP kelas C 192.168.1.1 yang berfungsi untuk menghubungkan jaringan lokal dengan jaringan *Internet*.
c. *Proxy server* berfungsi untuk melakukan *filtering* pada alamat DNS dan alamat IP, serta menampilkan hasil *filtering* dalam bentuk *report* untuk administrator dalam memberikan informasi seperti, alamat IP klien, alamat situs dan waktu akses. *Proxy server* memiliki 2 buah *ethernet card*, dimana *ethernet card* 1 (acl0) dengan alamat IP 192.168.1.2 digunakan untuk menghubungkan *proxy server* dengan modem, dan *ethernet card* 2 (ste0) dengan alamat IP 192.168.2.1 digunakan untuk menghubungkan *proxy server* dengan *switch*.
d. *Switch* berfungsi menghubungkan klien 1 dengan alamat IP kelas C 192.168.2.2, dan klien 2 dengan alamat IP kelas C 192.168.2.3 supaya terhubung dengan *proxy server*.
e. *Klien* berupa *notebook*/PC *desktop* yang berjumlah 2 unit.
f. Semua perangkat yang terhubung pada *switch* menggunakan media kabel UTP (*unshielded twisted pair*).

1.2 Kebutuhan Perangkat

Untuk perancangan *proxy server* membutuhkan perangkat keras maupun perangkat lunak, berikut perangkat keras dan perangkat lunak yang digunakan:

1.2.1 Perangkat Keras

Perangkat keras yang dibutuhkan untuk perancangan *proxy server*, dijelaskan pada tabel 3.1.

Tabel **Error! No text of specified style in document.**.1 Perangkat Keras Yang Dibutukan Proxy Server

Perangkat Keras	Jumlah	Spesifikasi
Proxy Server	1 unit	a) Prosesor i386 438 b) Memory 64MB c) Harddisk 20 GB d) 2 buah Ethernet Card 10/100 Fast Ethernet PCI

Pada tabel 3.1 dijelaskan perangkat keras yang dibutuhakan *proxy server* seperti: prosesor menggunakan minimal i386 438 merupakan prosesor yang termasuk keluarga x86 Intel. Untuk kapasitas *memory* sebesar 64MB, dengan media penyimpan sebuah *harddisk* sebesar 20GB. Perangkat keras yang dibutuhkan untuk menghubungkan *proxy server* dengan perangkat pendukung adalah 2 buah ethernet card PCI.

Tabel **Error! No text of specified style in document.**.2 Perangkat Pendukung Yang Dibutuhkan

Perangkat Pendukung	Jumlah
Modem	1 Unit
Switch	1 Unit
Kabel UTP	5 Meter
Klien	2 Unit

Pada tabel 3.2 dijelaskan untuk perangkat pendukung pada *proxy server* seperti: satu unit modem yang memberikan layanan *Internet*. Satu unit *switch* digunakan sebagai penghubung antara *proxy server* dengan klien. Untuk media transmisi menggunakan kabel UTP (*Unshield Twisted Pair*) sepanjang 5 meter serta dua unit klien yang digunakan untuk pengujian.

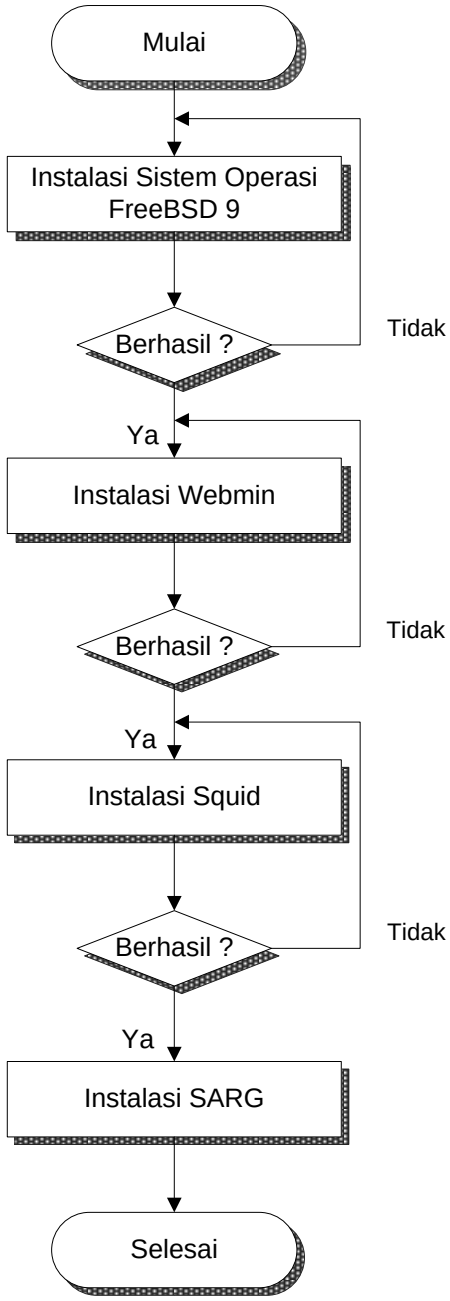
1.2.2 Perangkat Lunak

Perangkat lunak yang dibutuhkan untuk perancangan *proxy server* sebagai berikut:

a. FreeBSD 9 sebagai sistem operasi *proxy server*.
b. Squid sebagai program *proxy server* yang berfungsi melakukan proses *filtering*.
c. SARG (*Squid Analysis Report Generator*) berfungsi menampilkan *report* yang berisi alamat IP *klien*, alamat situs dan waktu.
d. Webmin digunakan untuk melakukan konfigurasi pada *proxy server*.

1.3 Instalasi Sistem

Setelah perangkat keras dan perangkat lunak dibutuhkan dalam perancangan *proxy server* telah siap, selanjutnya instalasi sistem operasi dan aplikasi yang digunakan. Sistem operasi yang digunakan adalah FreeBSD, aplikasi pendukung berupa *Webmin* berfungsi untuk melakukan konfigurasi pada *proxy server*, *squid* bertugas sebagai program *proxy server* untuk melakukan *filtering* dan SARG (*Squid Analys Report Generator*) bertugas menampilkan penggunaan *Internet*, Berikut gambar 3.2 tentang diagram alir instalasi sistem secara keseluruhan pada *proxy server*.



Gambar **Error! No text of specified style in document.**.2 Diagram Alir Proses Instalasi Sistem Secara Keseluruhan

Berdasarkan pada gambar 3.2 dijelaskan sebagai berikut:

a. Pada proses pertama yaitu diawali dengan instalasi sistem operasi pada *proxy server*. Sistem operasi yang digunakan pada *proxy server* adalah FreeBSD.

Setelah selesai instalasi dan berhasil selanjutnya instalasi Webmin, bila tidak berhasil kembali pada proses instalasi sistem operasi.

b. Selanjutnya instalasi *Webmin* yang berfungsi untuk melakukan konfigurasi pada *proxy server*. Setelah proses instalasi Webmin berhasil, selanjutnya instalasi *squid*, bila tidak berhasil kembali pada proses instalasi Webmin.
c. Berikutnya adalah instalasi Squid berfungsi sebagai program *proxy server* untuk melakukan proses *filtering.* Bila proses instalasi Squid selasai, selanjut ke tahap instalasi SARG (*Squid Analys Report Generator*) dan jika gagal kembali ke tahap sebelumnya.
d. Melakukan instalasi SARG (*Squid Analys Report Generator*) yang berfungsi untuk menampilkan hasil filtering, seperti: Alamat IP klien, alamat situs, dan waktu akses. Setelah semua proses instalasi sistem selesai tahap berikut melakukan konfigurasi *proxy server*.

1.4 Konfigurasi Proxy Server

Selanjutnya melakukan konfigurasi sistem operasi FreeBSD dan Squid sebagai program *filtering* serta SARG (*Squid Analys Report Generator*) yang digunakan untuk mencatat *report* dari hasil *filtering*. Konfigurasi pada *proxy server* sebagai berikut:

1.4.1 Konfigurasi Sistem Operasi FreeBSD

Konfigurasi sistem operasi FreeBSD bertujuan untuk menambah modul-modul tambahan yang digunakan untuk proses *filtering*. Modul yang ditambahkan adalah NAT (*Network Address Translation*) yang berfungsi memberikan layanan agar *klien* dapat mengakses *Internet*, dan mengaktifkan fitur salah satu *firewall* di FreeBSD yaitu PF (*Packet Filter*) yang berfungsi mengalihkan paket-paket dari klien agar melewati *proxy server* sebelum menuju *server* yang ada di *Internet*. Konfigurasi sistem operasi FreeBSD sebagai berikut:

1. Kompilasi Kernel FreeBSD

   Kompilasi *kernel* pada FreeBSD untuk menambahkan modul dari NAT dan PF. Kernel FreeBSD terletak pada direktori /usr/src/sys/i386/conf, dan nama kernel FreeBSD adalah GENERIC. Sebelum melalukan konfigurasi kernel,

terlebih dahulu menyalin kernel GENERIC menjadi nama lain misalnya PROXY. Untuk menyalin kernel GENERIC menjadi PROXY dengan perintah berikut:

```
cd /usr/src/sys/i386/conf
cp GENERIC PROXY
ee PROXY
```

Setelah melakukan penyalinan *kernel*, selanjutnya menambahkan modul NAT pada *kernel* PROXY dengan menambahkan perintah seperti dibawah ini.

```
ident PROXY
options     IPFIREWALL
options     IPDIVERT
options     IPFIREWALL_DEFAULT_TO_ACCEPT
options     IPFIREWALL_VERBOSE
device      pf
device      pflog
device      pfsync
```

Keterangan perintah diatas sebagai berikut:

- ident: Nama *kernel* yang sudah diubah menjadi PROXY.
- options IPFIREWALL: opsi untuk mengaktifkan *firewall*.
- options IPDIVERT: opsi untuk mengaktifkan fungsi dari NAT.
- options IPFIREWALL_DEFAULT_TO_ACCEPT: opsi untuk memperbolehkan segala sesuatu melewati *firewall* secara *default*.
- options IPFIREWALL_VERBOSE: opsi untuk mengaktifkan sistem *logging* dari sebuah paket.
- device pf : digunakan untuk mengaktifkan fitur PF.
- device pflog : digunakan untuk mencatat trafik pada perangkat jaringan.
- device pfsync : digunakan untuk memantau *state* pada perangkat jaringan.

Selanjutnya melakukan kompilasi dan instalasi *kernel* PROXY dengan perintah berikut.

#config PROXY

#cd ../compile/PROXY

#make cleandepend && make && make install && reboot

2. Membuat peraturan pada pf.conf

   Peraturan pada pf.conf bertujuan untuk membuat peraturan dalam mengalihkan paket-paket dari klien supaya melewati *proxy server*. Untuk membuat peraturan pada pf.conf sebagai berikut:

   #cp /usr/share/examples/pf.log /etc/pf.log

   #ee /etc/pf.log tambahkan baris berikut

   int_if="alc0" #(a)

   ext_if="ste0" #(b)

   rdr on $int_if inet proto tcp from any to any port www -> 192.168.1.2 port 3128 #(c)

   pass in on $int_if inet proto tcp from any to 192.168.1.2 port 3128 keep state #(d)

   pass out on $ext_if inet proto tcp from any to any port www keep state #(e)

   Keterangan baris diatas sebagai berikut:

   a. Kartu jaringan yang terhubung ke jaringan Internet.
   b. Kartu jaringan yang terhubung ke jaringan lokal.
   c. Mengalihkan paket yang terhubung pada antarmuka internal yang menggunakan protokol TCP melalui *port* www menuju alamat IP 192.168.1.2 dengan port 3128.
   d. Memperbolehkan paket dari alamat IP 192.168.1.2 menggunakan protokol TCP pada 3128 yang masuk dari antarmuka internal.
   e. Memperbolehkan paket keluar dari antarmuka eksternal menuju *port* www.

#ESC dan Save Change

#pfctl -f /etc/pf.log #untuk mengecek *error* pada pf.log

#pf -e #mengaktifkan PF secara manual

3. Menjalankan fitur NAT dan PF pada saat proses *booting* awal

   Untuk menjalankan fitur NAT dan PF pada saat proses booting awal dengan menambahkan perintah pada rc.conf. Untuk menambahkan perintah pada rc.conf sebagai berikut:

   #ee /etc/rc.conf, tambahkan perintah berikut:

   gateway_enable=”YES” #mengaktifkan fitur *gateway* pada *server*

   firewall_enable=”YES” #mengaktifkan *firewall*

   firewall_enable=”OPEN” #*firewall* memperbolehkan semua trafik

   natd_enable=”YES” #mengaktifkan fitur NAT

   natd_interface=”alc0” #perangkat yang terhubung dengan *Internet*

   pf_enable=”YES” #mengaktifkan fitur PF

   pf_rules=”/etc/pf.log” #letak set peraturan PF

   #ESC dan Save Change

4. Konfigurasi DHCP (*Dynamic Host Configuration Protocol*)

   Instalasi DHCP bertujuan untuk memberikan layanan pengalamatan otomatis bagi klien, sehingga klien tidak perlu melakukan pengaturan alamat IP. Untuk instalasi DHCP seperti berikut:

   Install DCHP melalui *ports*

   #cd /usr/ports/net/isac-dhcp42-server

   #make install clean

   Masuk ke file dhcpd.conf

   Konfigurasi dhcpd.conf bertujuan untuk mengatur opsi-opsi yang digunakan agar DHCP *server* dapat memberikan pengalamatan IP secara otomatis bagi klien.

   #ee /usr/local/etc/dhcpd.conf, ubah seperti baris berikut.

   option domain-name "freebsd.proxyserver.local" #(a)

   option domain-name-servers 8.8.8.8 #(b)

option subnet-mask 255.255.255.0 #(c)

subnet 192.168.2.0 netmask 255.255.255.0 { #(d)

range 192.168.2.2 192.168.2.1 #(e)

option routers 192.168.1.1} #(f)

Keterangan baris diatas sebagai berikut:

a. opsi yang berisi *hostname* dari *proxy server* untuk pencarian domain yang diberikan kepada klien.
b. opsi yang berisi DNS *server* yang akan digunakan oleh klien.
c. opsi yang berisi subnet-mask yang akan digunakan oleh klien.
d. Berisi alamat *subnet* dan *netmask* untuk jaringan lokal.
e. Jarak alamat IP yang disediakan oleh DHCP *server* untuk jaringan lokal.
f. opsi berisi default router yang digunakan DHCP *server*.

#ESC dan Save Change

1.4.2 Konfigurasi Squid

Selanjutnya melakukan instalasi dan konfigurasi Squid. Berikut instalasi dan konfigurasi Squid:

a. Instalasi Squid dengan perintah berikut:

   # su

   # pkg_add -r squid

b. Mengaktifkan Squid sebagai *startup*

   # ee /etc/rc.conf, tambahkan baris berikut:

   squid_enable=”YES”

c. Membuat direktori untuk file cache.log dan access.log

   File cache.log digunakan untuk menyimpan riwayat alamat situs yang telah dikunjungi, sedangan access.log digunakan untuk menyimpan alamat IP klien, alamat situs yang di akses dan waktu. Membuat direktori file cache.log dan access.log dengan perintah berikut:

   # mkdir /var/logs/squid

touch -f cache.log

touch -f access.log

d. Merubah kepemilikkan direktori agar dapat ditulis oleh Squid dengan perintah berikut:

chown -R squid:squid /var/logs/squid/cache.log

chown -R squid:squid /var/logs/squid/access.log

e. Konfigurasi squid.conf

Squid.conf berisi *file* yang berisi aturan-aturan yang terdapat pada Squid seperti; ACL (*access control list*) yang bertugas dalam pemberian hak akses terhadap *proxy server* dalam melakukan *filtering* alamat situs, alamat IP dan *port* mana saja yang di perbolehkan. Konfigurasi squid.conf dengan perintah berikut:

su

ee /usr/local/etc/squid/squid.conf, tambahkan baris berikut:

visible_hostname (misalnya freebsd.proxyserver.local)

Simpan dan tutup dengan tekan ESC kemudian pilih *save change*.

f. Konfigurasi *squid module config*

Squid module config berisi kumpulan *option* untuk mengatur *Squid*, seperti lokasi squid.conf, perintah untuk mengaktifkan Squid, lokasi tempat penyimpanan access.log dan opsi pendukung lainnya dalam melakukan konfigurasi Squid. Langkah-langkah konfigurasi *squid module config* sebagai berikut:

1. Pilih *module config* yang berada di pojok kiri atas.
2. Pada *Full path to squid config file*, kemudian isikan /usr/local/etc/squid/squid.conf.
3. Pada *Full path to squid log directory*, isikan /var/log/squid/access.log. Untuk *option* pendukung lainnya dalam kondisi *default* (awal).
4. Pilih *Save*.

g. Konfigurasi *Port*

Konfigurasi *port* bertujuan untuk menentukan *port* yang digunakan *proxy server* dalam melakukan proses *filtering*. *Port* yang digunakan adalah *port* 3128. Langkah-langkat konfigurasi *port* sebagai berikut:

1. Masuk *Webmin*.
2. Klik modul *Squid Proxy server*.
3. Pada tabel *Proxy Address and Ports*, pilih opsi *Listed Below.*
4. Pada kolom *port* tambahkan nomor 3128. Pada kolom *Hostname/IP Address* pilih *All*, untuk memperbolehkan semua alamat IP mengakses *port* tersebut.
5. Klik tombol *Save*.

h. Konfigurasi ACL untuk alamat IP jaringan lokal

Konfigurasi ACL untuk alamat IP jaringan lokal bertujuan untuk mendaftarkan alamat IP jaringan lokal yang terhubung pada *proxy server*. Langkah-langkah konfigurasi ACL untuk alamat IP jaringan lokal sebagai berikut:

1. Klik modul *Access Control*.
2. Pilih *Klien Address* pada tabel ACLs. Kemudian klik tombol *Create New ACL*. Masukkan nama ACLs contoh: *ournetwork*.
3. Masukkan alamat IP *Network* pada kolom *From* IP isikan 192.168.2.0 Untuk kolom *Netmask* isikan 24 (alamat IP kelas C).
4. Klik *Add Proxy Restriction* pada tabel *Proxy Restriction*.
5. ACL dengan internal akan muncul pada *form Proxy Restriction*, pilih *Allow* pada *form Action* supaya alamat IP di *network* 192.168.2.0 dapat mengakses *proxy server*.
6. Klik tombol *Save* dan *Apply Change*.

i. Membuat ACL untuk alamat situs dan alamat IP yang akan difilter.

Membuat ACL untuk alamat situs dan alamat IP bertujuan membuat daftar ACL dari kumpulan alamat situs dan alamat IP yang akan difilter, supaya alamat situs dan alamat IP tidak dapat diakses oleh klien. Membuat ACL untuk alamat situs sebagai berikut:

1. Klik modul *Access Control*.
2. Pilih *web server hostname*. Kemudian klik tombol *Create New ACL*. Masukkan nama ACLs contoh: *bad_dns_and_ip*.
3. Masukkan alamat situs dan alamat IP yang akan di *filter* pada *form URL_Regexp ACL* seperti: .redtube.com, .situsjudi.com, 202.93.17.135, 62.236.2.223 dan sebagainya.
4. Klik *Add Proxy Restriction* pada tabel *Proxy Restriction*.
5. ACL dengan nama *bad_dns_and_ip* akan muncul pada *form Proxy Restriction*, pilih *Deny* pada form *Action*, supaya alamat situs dan alamat IP yang sudah didaftarkan pada ACL tidak dapat diakses.
6. Klik tombol *Save* dan *Apply Change*.

1.4.3 Konfigurasi SARG

Konfigurasi SARG (*Squid Analys Report Generator*) berfungsi untuk menampilkan hasil *filtering*, berupa alamat IP, alamat situs, dan waktu. Instalasi dan konfigurasi SARG sebagai berikut:

a. Instalasi SARG ketikkan perintah berikut:

   # su

   # pkg_add -r sarg

b. Konfigurasi SARG sebagai berikut:
   1. Klik modul *Squid Report Generator*.
   2. Pilih *Module config*. Pada *Full Path To Sarg Executable* isikan /usr/local/bin/sarg.
   3. Pilih *Full Path to SARG Configuration file,* kemudian isikan /usr/local/etc/sarg/sarg.conf.
   4. Pada *add header webmin sarg report* pilih *Yes*.
   5. Pilih *Save*.
   6. Pilih *Menu Log Source and Report Destination*.
   7. Pada *Source Squid log file* pilih other file, kemudian isikan /var/log/squid/access.log

8. Pada *Destinition report directory*, kemudian isikan /var/www/html/squid-reports.
9. Pilih *Save*.