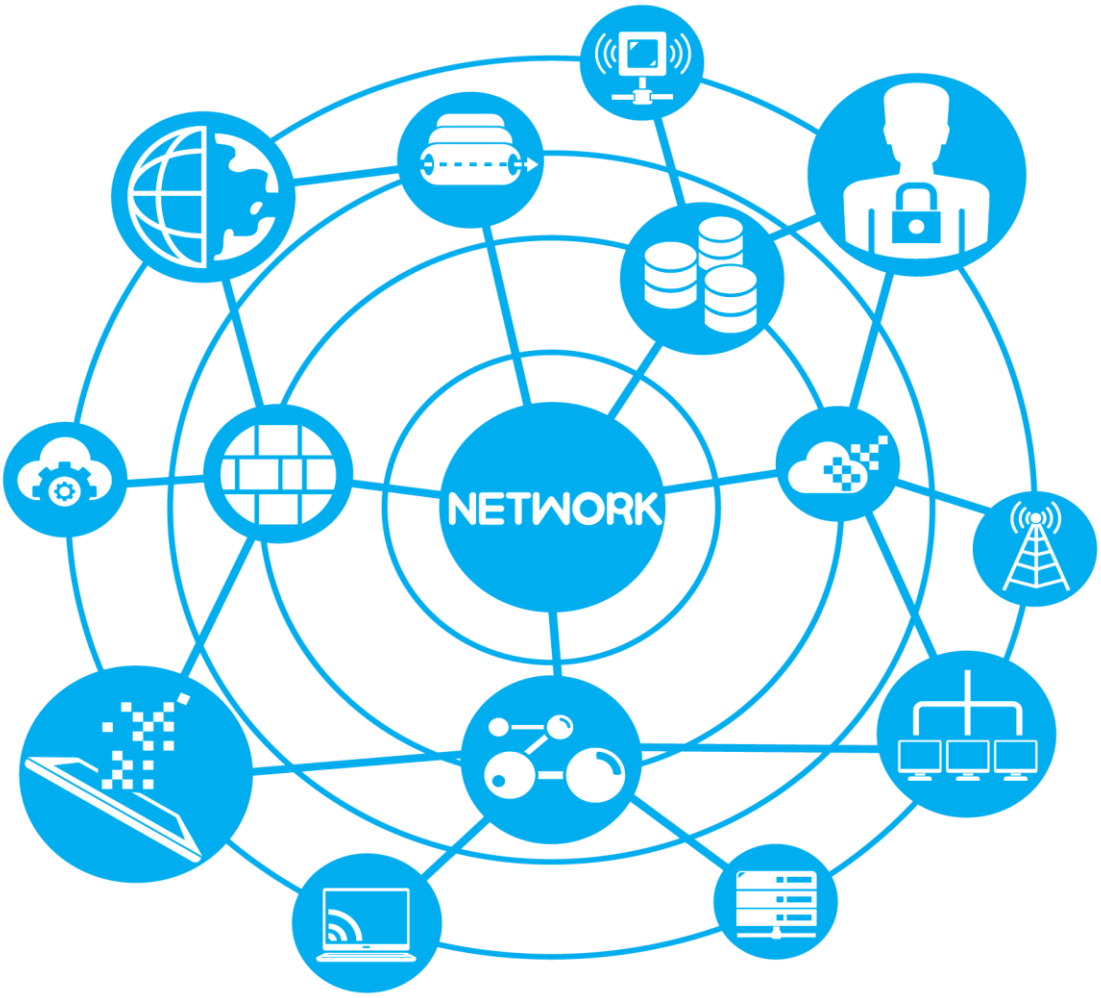
MODUL PANDUAN

JARINGAN KOMPUTER LANJUT

UNIVERSITAS GUNADARMA



Laboratorium Sistem Komputer Lanjut
Universitas Gunadarma

DAFTAR ISI

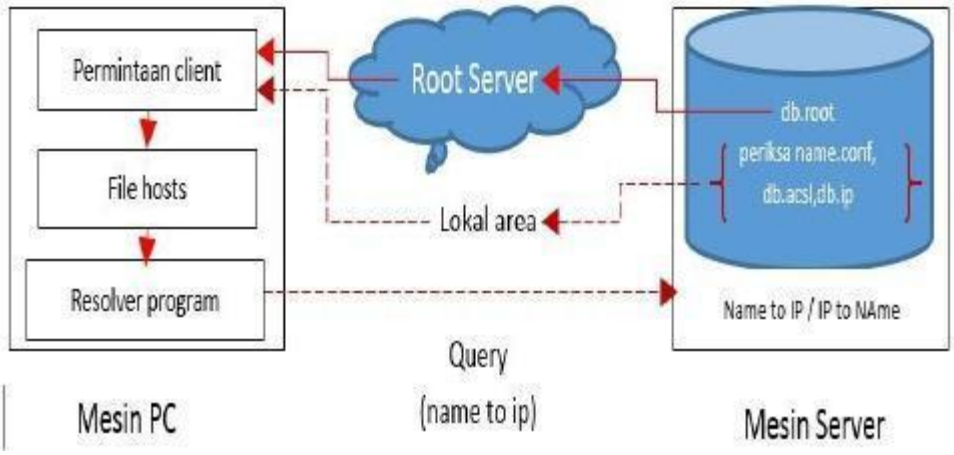
BAB 1 DNS (Domain Name System) dan Web Server

1.1 Pengenalan DNS (Domain Name System)

Domain Name System adalah sistem distribusi database yang mengelola seluruh segment database, tentunya data dalam setiap jaringan dengan model client – server. Awal dari suatu sistem DNS berawal mula dari jaringan kecil ARPANET, dengan menggunakan mekanisme single file hosts.txt (/etc/hosts pada sistem Unix) pada setiap client yang terhubung ke jaringan, sehingga mampu untuk mengenali satu sam lainnya. File tersebut digunakan untuk proses resolusi. File Hosts berisi nama – nama domain yang pointing ke informasi tentang individual hostname – hostname dan ip dan sebuah domain berisi semua host – host yang terdapat nama – nama didalamnya.

DNS Name Server berisi informasi tentang beberapa segment database dan menyediakan informasi yang diperlukan oleh client untuk proses resolusi. Programnya dinamakan resolver. Resolver itu sendiri merupakan library routine yang membuat query dan mengirim permintaan tersebut melalui jaringan ke name server yang telah didefinisikan di resolver (/etc/resolve.conf).

1.2 Cara Kerja DNS Name Server



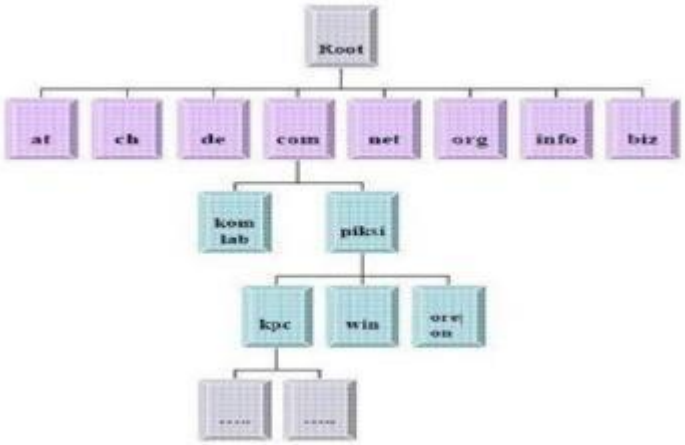
Gambar 1. 1 Cara Kerja DNS Server Resolver

Setiap permintaan client akan diarahkan ke file hosts untuk mengetahui letak hostname server-nya. Apakah hostname atau mesin server yang dituju milik dia atau bukan? Jika bukan untuk dirinya, maka permintaan akan di teruskan ke resolver untuk mencari tahu letak nameserver, sehingga resolver akan memberikan route permintaan

query ke nameserver yang ditunjuk oleh resolver.

Name server yang berisi informasi database semua host server, kemudian akan melakukan proses penerjemahan baik dari nama domain ke ip address atau sebaliknya, berdasarkan file database yagn ada pada mesin itu sendiri. Yang perlu diperhatikan adalah jika ternyata permintaan masih dalam area lokal jaringan maka permintaan akan langsung diteruskan ke server tujuan. Namun bila bukan maka file db.root dan direktif forward dns publik akan digunakan untuk menghubungkan ke root DNS public internet, sehingga permintaan diproses oleh dns publik. Server dns publik tersebutlah yang menjawab permintan client.

1.3 Struktur Database DNS



Gambar 1. 2 Struktur Database DNS

Sturktur Database DNS sama seperti file system pada system Unix. Tingkatan palingatas disebut sebagai root atau node root. Root node ditulis sebagai single dot "." (titik).

Setiap root terbagi ke dalam beberapa Domain. Pada level ini disebut sebagai Top Lvel domain yang memiliki tugas dan tanggung jawab masing – masing. Pembagian tugas tersebut dijelaskan beirkut ini :

a) edu merupakan institusi pendidikan atau universitas.
b) org merupakan organisasi non profit
c) net merupakan backbone internet
d) gov merupakan organisasi pemerintah non militer
e) mil merupakan organisasi pemerintah militer, dll.

Pada DNS. Setiap domain mampu terbagi lagi ke dalam subdomain dan membedakan pertanggung jawabannya untuk berbeda organisasi. Proses penurunan domain ke dalam subdomain disebut dengan delegasi. Contoh sebuah organisasi yang dinamakan ACSL mengatur domain ac.id, tetapi mendelegasikan pertanggung jawabannya kepada subdomain acsl.ac.id (ac.id adalah untuk domain pendidikan di indonesia) ke LAB Lanjut (nama permisalan saja). Otoritas pendelegasian untuk acsl.ac.id ke LAB Lanjut mebuat zone baru. Zone acsl.ac.id sekarang independen dari ac.id dan berisi semua nama - nama domain yang berakhiran acsl.ac.id. Zone ac.id tersebut, dalam kata lain, hanya berisi nama – nama yang diakhiri ac.id tetapi tidak pada pendelegasian zone, seperti acsl.ac.id. Jadi untuk memisahkan tanggung jawab lagi maka harus membagi ke dalam sub – sub domain, seperti jkl.acsl.ac.id, bukan pada acsl.ac.id. Jika suatu nama domain tampak langsung di belakang root top level domain (www.google.com). Software intepreter menganggap nama tersebut nama domain absolute. Sebuah nama domain yang relative ke root domain juga dikenal dengan istilah Full Qualified Domain Name (FQDN).

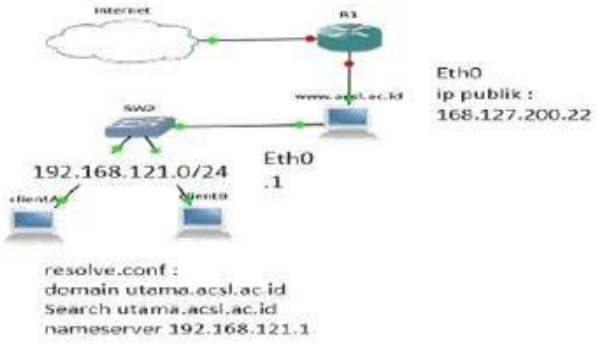
1.4 Peran DNS Server

A. DNS Server Name Otoritatif

DNS Server Name Otoritatif adalah suatu server DNS yang hanya bertanggung jawab terhadap suatu nama domain untuk pelayanan web server. DNS ini tidak akan melayani proses query dan resolusi dari client. Cara yang digunakan untukvmembatasinya adalah dengan melakukan pendefinisian directiv acl di dalamvkonfigurasi dns named.

B. DNS Server Cache/Resolver

DNS Server Cache merupakan DNS Server yang ditujukan hanya untuk melayani proses query dan resolusi dari client. Dimana setiap permintaan alamat atau ip address server tujuan yang diminta oleh client kemudian akan disimpan. Jadi apabila terdapat suatu client yang mengakses tujuan yang sama maka server ini hanya akan mengambil data dari local mesin saja.



Gambar 1. 3 Model Topologi Split DNS Server

C. DNS Server Multihomed

DNS Server Multihomed adalah DNS Server yang akan melayani dua proses sekaligus yaitu untuk domain dan query dalam satu mesin. Pelyanan akan tergantung kepada dari ip address client yang meminta. Apabila permintaan datangnya dari publik maka permintaan akan diarahkan ke server name dan tidak akan dilayani proses query, sebaliknya jika permintaan datangnya dari lokal maka permintaan dapat mengkases name server ataupun query. Pelayanan tersebut dapat dilakukan dengan mendefinisikan direktif view dan acl di dalam konfigurasi dns server.

1.5 Tipe DNS Server Name

DNS Server name terbagi menjadi dua buah yaitu :

A. Primary/Master DNS Server Name

Yaitu server yang hanya akan membaca file data zone dari lokal mesin itu sendiri

B. Secondary/slave DNS Server Name

Yaitu server yang akan memperoleh file data zone dari nameserver lain yang otoritatif untuk zone-nya. Secondary nameserver hanya akan menunggu pengiriman data zone selama waktu yang telah didefinisikan di master server. Secondary master dapat meload file data zone dari secondary lainnya. Ketika secondary telah start up, kemudian menghubungi master nameserver-nya dan mengambil data darinya. Proses tersebut dikenal dengan istiah zone transfer.

1.6 Pembagian DNS Menurut Model Pelayanannya

A. DNS Server Publik

yaitu merupakan dns server yang digunakan untuk proses resolusi dimana setiap permintaan akan dilayani. Baik akses dari jaringan localnya ataupun internet. DNS server ini akan menggunakan ip publik yang akan tidak dibatasi oleh penggunaan acl. Contohnya seperti :

∗8.8.8.8, 8.8.4.4 (google)

∗208.67.222.222, 208.67.220.220 (OpenDNS),

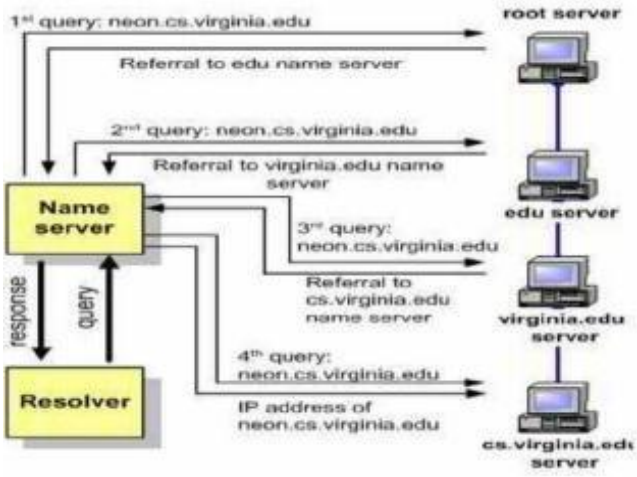
∗202.134.2.5, 203.130.196.5 (Telkom Speedy), dsb.

B. DNS Server Lokal

DNS server yang hanya akan melayani proses resolusi permintaan dari jaringan lokal yang telah didefinisikan pada acl.

1.7 Proses Resolusi Resolver

Awalnya name server akan menghubungi server root. Server root tidak mengetahui IP Address domain tersebut, ia hanya akan memberikan IP Address server edu.



Gambar 1. 4 Proses Resolusi Resolver Dari ROOT Server

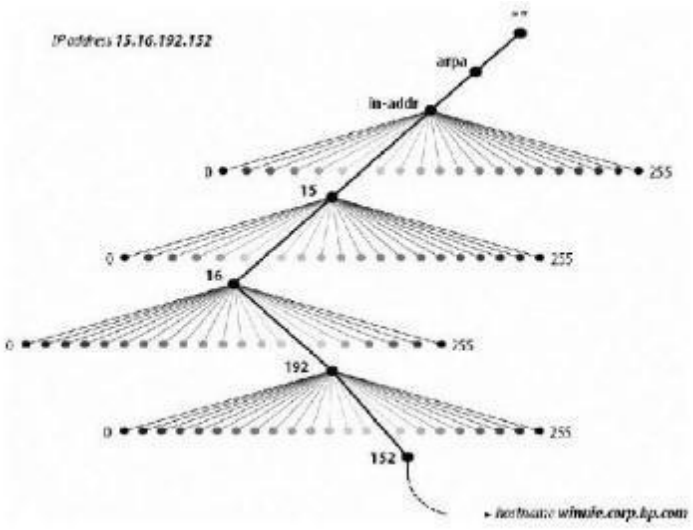
Awalnya name server akan menghubungi server root. Server root tidak mengetahui IP Address domain tersebut, ia hanya akan memberikan IP Address server edu. Selanjutnya name server akan bertanya lagi pada server edu berpa IP Address domain neon.cs.virginia.edu. Server edu tidak mengetahui IP Address domain tersebut,

ia hanya akan memberikan IP Address server virginia.edu. Selanjutnya name server akan bertanya ke server virginia.edu tentang IP Address neon.cs.virginia.edu. Dan server virginia.edu hanya mengetahui dan memberikan jawaban berupa IP Address server cs.virginia.edu

Selanjutnya name server akan bertanya ke server cs.virginia.edu tentang IP Address neon.cs.virginia.edu. Dan barulah cs.virginia.edu mengetahui dan menjawab berapa IP Address domain neon.cs.virginia.edu.

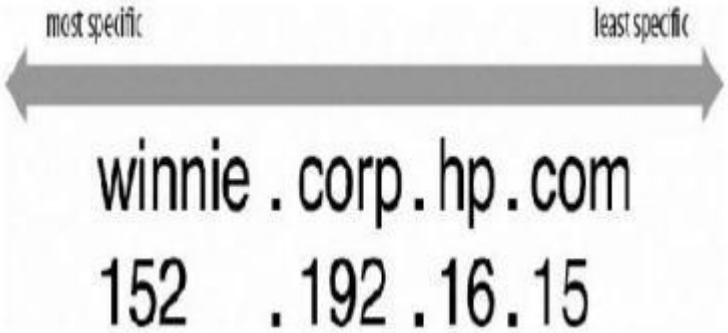
Terakhir barulah computer client bisa secara langsung menghubungi domain neon.cs.virginia.edu dengan menggunakan IP Address yang diberikan oleh server cs.virginia.edu. IP Address milik neon.cs.virginia.edu kemudian akan disimpan sementara oleh DNS server Anda untuk keperluan nanti. Proses ini disebut caching, yang berguna untuk mempercepat pencarian nama domain yang telah dikenalnya.

1.8 Analogi Mapping IP Address ke Nama Domain



Gambar 1. 5 Proses Mapping ke Domain

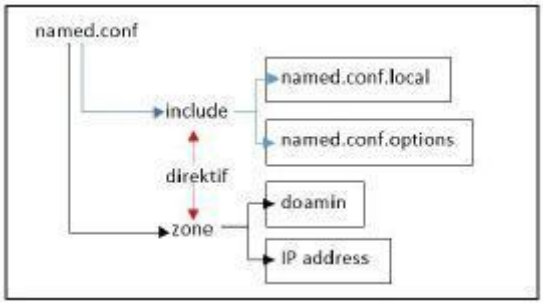
Ketika membaca nama domain dalam file konfigurasi seringkali ditemukan ip address yang dimulai dari belakang, karena memang pembacaan nama dimulai dari urutan belakang nama domain (seperti pada proses resolusi) sampai ke root, contoh winnie.corp.hp.com. IP address-nya adalah 15.16.192.152, maka bila dikaitkan dengan in-addr.arpa domain adalah 152.192.16.15.in-addr.arpa, dimana struktur tersebut akan map kembali ke nama domain winnie.corp.hp.com.



Gambar 1. 6 Alamat Hostname Winnie Pada Zona Data

152 merupakan alamat untuk hostname server dengan nama winnie. Host tersebut merupakan hasil proses delegasi dari domain corp.hp.com.

1.9 Berkas File-file Konfigurasi BIND



Gambar 1. 7 Berkas File Zone DNS

Terdapat 3 file konfigurasi utama yaitu named.conf, named.conf.local dan named.conf.options. Apabila 3 file tersebut digunakan, maka pada konfigurasi named.conf 2 file konfigurasi harus didefinisikan menggunakan direktif include didalamnya.

Fungsi :

a. Named.conf digunakan untuk mendefinisikan nama domain, lokasi file zone transfer dan master /slave dns server, acl, direktif bersifat options dan lain – lain.
b. Named.conf.local biasanya digunakan untuk keperluan pemisahan antara akses local dengan akses publik dengan mendeskripsikan direktif acl di dalamnya.
c. Named.conf.options yaitu digunakan untuk mendefinisikan direktif – direktif yang bersifat optionaldan harus di definisikan di antara options { ….. } (isi di titik – titik nya).

Macam – macam direktif tersebut adalah :

1. listen-on [port integer] { address_match_element; ... };
2. dump-file queted_string;
3. cache-file queted_string;
4. querylog boolean;
5. allow-recursion { address_match_element; ... };
6. sortlist { address_match_element; ... };
7. recursion boolean;
8. allow-query { address_match_element; ... };
9. allow-transfer { address_match_element; ... };
10. allow-notify { address_match_element; ... };
11. forward (first | only);
12. forwarders [port integer] {
13. (ipv4_address | ipv6_address) [port integer]; ...};

Namun 3 konfigurasi tersebut dapat diringkas menjadi 1 konfigurasi utama yaitu file named.conf. Untuk melakukan hal tersebut cukup dengan tidak mendefinisikan 2 file konfigurasi named.conf.local dan named,conf.options yang menggunakan direktif include. tetapi isi konfigrasi (named.conf.local dan named,conf.options) langsung didefinisikan pada file named.conf.

Direktif zone digunakan untuk mendefinisikan nama zone domain beserta dengan file kofigurasi zona yang di tunjuk oleh direktif file. File yang ditunjuk merupakan file zona data Resource Record.

Contoh isi file named.conf :

```
acl lokal {127.0.0.0/8; 192.168.121.0/24;}; zone
"."
{
type hint;
file "/etc/bind/db.cache"; };
zone "0.0.127.in-addr.arpa" { type
master;
file "/etc/bind/db.127.0.0"; };
zone "acsl.ac.id"
{
type master;
file "/etc/bind/db.acsl"; //file zona data RR untuk mapping domain ke ip };
```

```
zone "121.168.192.in-addr.arpa"
{
type master;
file "/etc/bind/db.192.168.121"; //file zona data RR untuk mapping ip domain };
include "/etc/bind/named.conf.options";//penggunaan direktif include
```

Contoh isi file konfigurasi named.conf.options :

```
options {
directory "/var/cache/bind";
forwarders { 8.8.8.8; };
forward only ;
// Baca hanya di lokal interface
listen-on-v6 {none ;};
listen-on {127.0.0.1; 192.168.121.234;};
};
```

1.10 File Zona Data

Zona data merupakan file konfigurasi yang dipanggil oleh file utama dns server bind named.conf dan DNS Resouce Record. File ini berisi pendefinisian SOA Record, A (Alias), NS, CNMAE, PTR dan lain – lain. File zona data terbagi ke 2 file utama saat kita membuat DNS Server Otoritatif yaitu db.domain dan db.ip_address.

Berikut ini merupakan contoh konfigurasi dari file Zona data :

a.File db.acsl

```
$TTL 1D
@ SOA origincontact (
                                        1 ; Serial
                                        3h ; Refresh after 3 hours
                                        1h ; Retry after 1 hour
                                        1w ; Expire after 1 week
                                        1h ) ; Negative caching TTL of 1 hour

                                        NSutama
Localhost               A               127.0.0.1

www                     A               192.168.121.3

                        MX              10 www

acsl05                  CNAME           www
```

b.File db.192.168.121

```
$TTL 1D
@ SOA utama.acsl.ac.id. smtp.acsl.ac.id. (
                                        1 ; Serial
                                        3h ; Refresh after 3 hours
                                        1h ; Retry after 1 hour
                                        1w ; Expire after 1 week
                                        1h ) ; Negative caching TTL of 1 hour

                    NS          utama.acsl.ac.id.
      234           PTR         utama.acsl.ac.id.
      5             PTR         proxy.acsl.ac.id.
```

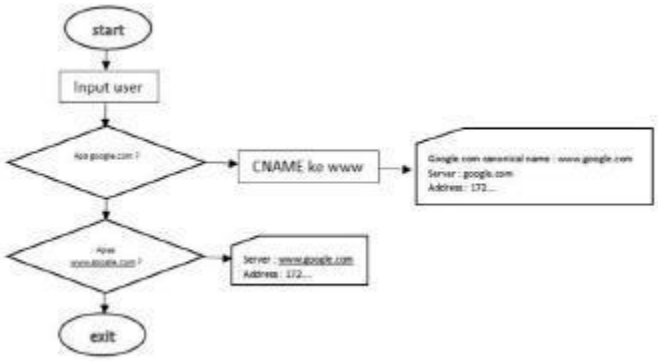
Keterangan :

Keterangan	Arti Argumen
@	Bagian ini identik dengan zona yang telah didefinsikan di file named.conf, yaitu dalam contoh ini acsl.ac.id atau huruf @ dapat diganti pula dengan acsl.ac.id
IN	Singkatan dari Internet Name, digunakan jika kita menggunakan protokol TCP/IP.
SOA	Singkatan dari Start of Authority, menyatakan bahwa NS ini authoritive unutk zona yang sebelumnya didefinisikan
origin	Mendeklarasikan hostname yang menjadi master server, hostname biasanya ditulis secara FQDN (dalam contoh adalah utama.acsl.ac.id.)
	jangan lupa diakhir nama harus diberi tanda . untuk pemisah dengan nama emal.
contact	Mendeklarasikan email admin Name Server yang melayani penerima email dan mengirim email. Disini perannya sebagai forwarders.
Serial	Nomor seri dari zona, dimana penomoran dalam serial harus berubah apabila kita meng-update atau merubah zona kita. Format dapat berdasarkan angka atau YYYYMMDD (20130115).

refresh	Mendeklarasikan selang waktu (dalam detik) yang diperlukan oleh secondary server untuk melakukan pengecekan terhadap primary server untuk melakukan pengecekan terhadap perubahan file zona
Retry	Menentukan lamanya waktu (dalam detik) secondary server menunggu mengulangi pengecekan terhadap primary server apabila primary server tidak memberikan respon.
expire	Menentukan lamanya waktu (dalam detik) file zona dipertahankan pada secondary server apabila secondary server tidak dapat melakukan refresh.
Minimum ttl	Menentukan nilai default time to live (ttl) untuk semua resource record pada file zona
(…..)	Nilai refresh, serial, expire, minimum ttl ditulis antara tanda kurung
A Record	Memetakan sebuah nama host ke alamat IP 32-bit (IPv4)
AAAA record	Memetakan sebuah nama host ke alamat IP 128-bit (IPv6)
CNAME record	Membuat alias untuk nama domain
MX record	Memetakan sebuah nama domain ke dalam daftar mail exchange server untuk domain tersebut
PTR record	Memetakan sebuah nama host ke nama kanonik untuk host tersebut. Pembuatan record PTR untuk sebuah nama host di dalam domain in-

Tabel 1. 1 Penjelasan Konfigurasi File Zona

1.11 Analogikal Canonical NAME



Gambar 1. 8 Proses Analogikal CNAME

Saat seorang melakukan permintaan terhadap suatu domain maka server resolver.

Maka server apak menanyakan. Domain mana yang menjadi tujuan anda ?. Bila permintaan anda untuk google.com (dalam contoh ini) maka server resolver telah mengetahui (file db.domain) bahwa nama tersebut memiliki CNAME ke domain www.google.com, dimana artinya setiap permintaan tersebut akan dilemparkan ke mesin yang sama seperti www.google.com. Namun yang berbeda adalah saat masuk ke google.com server resolver tidak menyertakan nama CNAME-nya dalam menjawab. Untuk lebih jelasnya lihat hasil percobaan praktik pada poin testing ke domain gunadarma.ac.id menggunakan nslookup. CNAME digunakan untuk mengatasi masalah permintaan yang tidak tepat dari user yang hendak ke webserver.

Contoh penggunaan CNAME :

Nama_host	CNAME name_server_aliases
acsl05	CNAME www

Artinya adalah acsl05 merupakan nama pengganti untuk www apabila tidak dapat dihubungi ke nama delegasi tersebut. Sedangkan www merupakan nama host untuk serveryang telah di pointing ke (A = alias) ip_address yang ditunjuk sebelumnya.

1.12 Direktif ACL (Access Control List)

Direktif ini merupakan direktif yang dapat digunakan untuk membatasi akses user terhadap DNS Server. Direktif ini dapat dideklarasikan pada file konfigurasi named.conf atau named.conf.local. Jika direktif ini dideklarasikan pada named.conf.local maka terlebih dahulu kita harus menyertakan direktif include pada file named.conf untuk mendefinisikan letak konfigurasinya (named.conf.local). Format : acl name { ip_address/ip_address_network; }; Contoh : acl lokal {127.0.0.0/8;192.168.121.0/24;}; Direktif tersebut akan terikat dengan direktif lainnya yaitu : allow-query dan allow-recursion. 2 direktif tersebutlah yang memberikan ijin kepada client yang telah didefinisikan. Apa saja yang boleh mereka lakukan. allow-query adalah direktif yang digunakan untuk memperbolehkan suatu client melakukan proses resolusi nama domain ke ip atau sebaliknya. Format : allow-query { nama_acl ; }; Allow-recursion adalah direktif yang digunakan untuk memperbolehkan suatu client meminta pengulangan proses resolusi. Implementasi lain dari direktif acl adalah untuk

pembuatan DNS server multihomed untuk membedakan akse publik dan akses lokal. Acl tersebut digunakan secara bersamaan dengan direktif view yang akan dijelaskan selanjutnya.

1.13 Direktif View

Direktif view akan digunakan saat kita akan memisahkan akses layanan publik dan lokal tetapi yang melayani adalah satu mesin dns server. Cara kerja tersebut diterapkan bersama dengan direrktif acl. Format : view nama { pernyataan_konfigurasi || pernyataan_options };

Contoh :

```
options {

directory "/etc/bind";

};

////////////////////////////////////////////////////////////////////////////

acl "lokal" { 192.168.121/24; };

view "internal" { // internal view zone lokal kita

match-clients { "lokal"; }; // hanya memperbolehkan client tersebut yang mengakses
zone zone "acsl.ac.id" {

type master;

file
"db.acsl.lokal"
; };

zone "121.168.192.in-
addr.arpa" { type master;

file
"db.192.168.121.lokal"
; }; };

////////////////////////////////////////////////////////////////////////////

view "publik" { // view zone untuk akse publik
match-clients { any; }; // perbolehkan dari ip
berapapun
```

```
recursion no; // akses publik tidak diperbolehkan melakukan
recursive zone "acsl.ac.id" {

type master;

file "db.acsl.publik"; // file zona data akses
publik };

zone "121.168.192.in-
addr.arpa" { type master;

file "db.192.168.121.publik"; // file zona data akses
publik }; };
```

1.14 Wordpress

Gambar 1. 9 Logo Wordpress

Hadir di tahun 2003, Wordpress kini telah menjadi amat populer. Berawal popular digunakan sebagai mesin blog, kini wordpress juga dikembangkan menjadi CMS. Wordpress merupakan CMS opensource, yang artinya bisa dilihat source codenya oleh siapapun, dari kelebihan tersebut kini wordpress semakin lengkap fiturnya dan populer. Inti dari CMS worpress yaitu bahasa pemrogaman PHP dan basis data MySQL.

Keunggulan :

- Gratis. Tidak perlu mengeluarkan biaya untuk mengguakan CMS ini
- OpenSource. Pengguna bisa melihat sourcecodenya dan jika merasa kurang pas dengan keinginan bisa dikembangkan lebih lanjut
- User Frienly. Selain pengoperasiannya yang mudah, template dan tampilannya juga mudah untuk dimodifikasi sesuai keinginan

- 1 Blog = Banyak Pengguna. Biasanya dengan adanya kelebihan ini, wordpress sering digunakan untuk blog komunitas
- Banyak Plugin. Selain banyak pilihan plugin di dalam wordpress, plugin yang ada juga selal dikembangkan, sehingga pengguna lebih nyaman kedepannya
- Kemampuan SEO. Dengan adanya kelebihan ini, tidak menuntut kemungkinan jika blog/website lebih mudah terindeks oleh mesin pencari

1.15 Cara Install CMS Wordpress

CMS atau singaktan dari Content Management System merupakan suatu system yang digunakan untuk menambah atau mengedit sebuah artikel yang ada. Dapat dimisalkan disebuah tempat produksi buku, ditempat tersebut ada satu komputer yang digunakan untuk membuat buku, di komputer tersebut juga ada daftar berbagai macam buku yang telah dicetak. Sehingga admin lebih mudah dalam membuat buku ataupun merevisi dari buku sebelumnya yang telah dicetak. Nah CMS bisa diibaratkan sebagai komputer tersebut.

CMS Wordpress bisa dipasang di server secara cuma - cuma tanpa mengeluarkan biaya sedikitpun. Selain gratis CMS Wordpress juga bersifat open source, sehingga bisa dikembangkan lagi bagi penggunanya.

BAB 2 MAIL SERVER

2.1 Pengertian Mail Server

Gambar 2. 1 Mail Server

Email merupakan sebuah layanan pengiriman surat elektronik yang dikirim melalui internet. Email dikirim dari suatu alamat email yang terdapat pada sebuah mail server kepada alamat email yang lainnya yang terdapat pada mail server yang sama maupun pada mail server yang berbeda. Email dapat dianalogikan dengan kotak surat yang ada di kantor POS sedangkan server email dapat diibaratkan sebagai kantor POS. Dengan analogi ini sebuah mail server dapat memiliki banyak account email yang ada didalamnya. Untuk mengirim sebuah email dari alamat email yang satu ke alamat email yang lain digunakan sebauh protocol (aturan) yaitu Simple Mail Transfer Protocol SMTP. Protocol SMTP telah menjadi aturan dasar yang disepakati untuk pengiriman email. Dengan demikian semua software email server pasti mendukung protokol ini. SMTP merupakan protokol yang digunakan untuk megirim email (komunikasi antar mail server), dan tidak digunakan untuk berkomunikasi dengan client. Sedangkan untuk client, digunakan protokol imap imaps pop3 pop3s Supaya sebuah mail server dapat di akses oleh cliet, dikembangkan sebuah aplikasi dimana client dapat mengakses email dari sebuah email server. IMAP adalah sebuah aplikasi pada layer Internet protokol yang memungkinkan client untuk mengakses email yang ada di server. Selain IMAP ada juga POP3 yang fungsinya sama dengan imap, akan tetapi memiliki karakteristik yang berbeda dalam cara pengaksesan pada server.

2.2 Sejarah mail server

Sejarah mail server yaitu sebelumnya dikenal sebagai VMailer dan IBM Secure Mailer, itu pada awalnya ditulis oleh Wietse Venema selama tinggal di IBM Thomas J. Watson Research Center, dan terus dikembangkan secara aktif hari ini. Postfix pertama

kali dirilis pada pertengahan tahun 1999. Surat elektronik sudah mulai dipakai di tahun 1960-an. Pada saat itu Internet belum terbentuk, yang ada hanyalah kumpulan 'mainframe' yang terbentuk sebagai jaringan. Mulai tahun 1980-an, surat elektronik sudah bisa dinikmati oleh khalayak umum. Sekarang ini banyak perusahaan pos di berbagai Negara menurun penghasilannya disebabkan masyarakat sudah tidak memakai jasa pos lagi.

2.3 Program-program Email

Secara umum program atau aplikasi email diklasifikasikan menjadi tiga klasifikasi yaitu:

a. Mail Transfer Agent (MTA), Mail Delivery Agent (MDA), dan Mail User Agent (MUA) . Ketiga klasifikasi program email ini masing-masing memiliki tugas dan peran peting dalam proses pergerakan dan manajemen pesan pesan email.

b. Mail User Agent (MUA), mengirimkan /mentransfer email antar komputer dengan menggunakan SMTP. Sebuah pesan email mungkin saja sebelum sampai ketujuan melewati beberapa SMTP server lain. Contoh aplikasi MTA yaitu :Sendmail, Postfix, qmail, exim dll.

c. Mail Delivery Agent(MDA), bekerjasama dengan MTA untuk menagani pesan-pesan email yang datang untuk di letakkan /di distribusikan sesuai pada mailbox user masing-masing.

Di beberapa sistem , program MTA biasanya adalah program MDA juga. Di dalam beberapa kasus , MDA sebenarnya adalah sebuah Local Delivery Agent (LDA) seperti mail atau procmail. Mail User Agent(MUA), merupakan sinonim dari aplikasi email client. Sebuah MUA adalah sebuah program yang memungkinkan user membaca dan membuat pesan-pesan email. Selain itu banyak juga beberapa MUA yang memungkinkan mendownload email melalui protokol POP atau IMAP. Beberapa contoh MUA yaitu Mozilla mail, mutt, pine, Kmail, Netscape Mail, Eudora Microsoft Outlook dll.

2.4 Protokol layanan E-Mail

Terdapat tiga protokol utama yang sering digunakan dalam layanan E-Mail :

A.Simple Mail Transfer Protokol (SMTP)

Fungsi utama SMTP adalah menyampaikan E-Mail dari suatu host ke host lainnya dalam jaringan. Protokol ini tidak memiliki kemampuan untuk melakukan penyimpanan dan pengambilan E-Mail dari suatu mailbox. Service SMTP berjalan pada protokol TCP port 25, yang merupakan port standar service SMTP. Karena SMTP tidak memiliki kemampuan penyimpanan E-Mail dalam mailbox, maka diperlukan protokol lain untuk menjalankan fungsi tersebut yaitu POP3 dan IMAP. Dari sisi klien E-Mail, server SMTP merupakan sarana untuk melakukan outgoing connection atau mengirimkan pesan. Sedangkan untuk incoming connection digunakan protokol POP3.

B.Post Office Protocol Version 3 (POP3)

Protokol POP yang banyak digunakan saat ini adalah versi 3 atau lebih dikenal sebagai POP3. Peran potokol ini adalah untuk mengambil E-Mail yang tersimpan dalam mailbox tiap user di mail server, yang biasanya juga berfungsi sekaligus sebagai SMTP server. Sebagaimana telah dijelaskan sebelumnya bahwa SMTP tidak memiliki mekanisme penyimpanan E-Mail ke mailbox dan mendistribusikannya tiap user, sehingga protokol POP3 mengambil peran tersebut. Server POP3 menyimpan sementara E-Mail tiap user di dalam mail boxnya masing-masing sebelum akhirnya didownload oleh user bersangkutan menggunakan klien E-Mail seperti Outlook maupun Eudora. Dalam proses pengambilan tersebut klien E-Mail terhubung ke mail server menggunakan protokol POP3 yang berjalan pada TCP port 110.

C.IMAP (Internet massage access protocol)

IMAP merupakan protocol standar untuk mengakses atau mengambil e-mail dari server dengan kelebihan sebagai berikut :

-Dapat memilih email yang akan diambil

-Membuat folder di server

-Mencari pesan e-mail di server

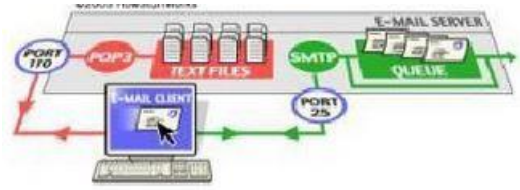
-Menghapus pesan e-mail yang ada

-Mempertahankan e-mail pada server sehingga e-mail dapat dibuka kembali melalui device yang berbeda

Mail server menggunakan protocol IMAP yang berjalan pada TCP port 143.

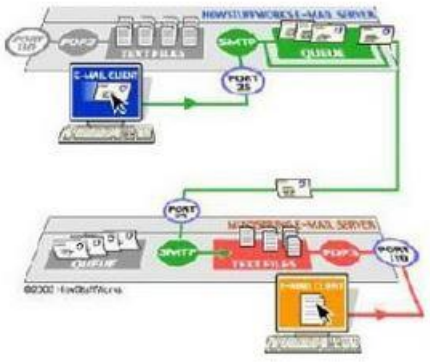
2.5 Cara kerja mail server

Pada email server terdapat dua server yang berbeda yaitu incoming dan outgoing server. server yang biasa menangani outgoing email adalah server SMTP(Simple Mail Transfer Protocol) pada port 25 sedangkan untuk menangani incoming email adalah POP3(Post Office Protcol) padaport 110 atau IMAP(Internet Mail Access Protocol) pada port 143.



Gambar 2. 2 Cara Kerja Mail Server

Saat mengirim email maka email akan ditangani oleh SMTP server dan akan dikirim ke SMTP server tujuan, baik secara langsung maupun melalui melalui beberapa SMTP server dijalurnya. apabila server tujuan terkoneksi maka email akan dikirim, namun apabila tidak terjadi koneksi maka akan dimasukkan ke dalam queue dan di ‘resend setiap 15menit’. Apabila dalam 5 hari tidak ada perubahan maka akan diberikan undeliver notice ke inbox pengirim.



Gambar 2. 3 Cara Kerja Server & client

Apabila email terkirim email akan masuk pada POP3 server atau IMAP server. jika menggunakan POP3 server maka apabila kita hendak membaca email maka

email pada server di download sehingga email hanya akan ada pada mesin yang mendownload email tersebut, dengan kata lain kita hanya bisa membaca email tersebut pada device yang mendownload email tersebut.berbeda dengan POP3 IMAP server mempertahankan email pada server sehingga email dapat dibuka kembali lewat device yang berbeda.

2.6 Kelebihan dan Kekurangan Mail Server

a.Kelebihan

- Lebih menghemat bandwith
- Lebih cepat & efisien
- Mudah mengatur account
- Jika ada masalah dapat ditangani sendiri

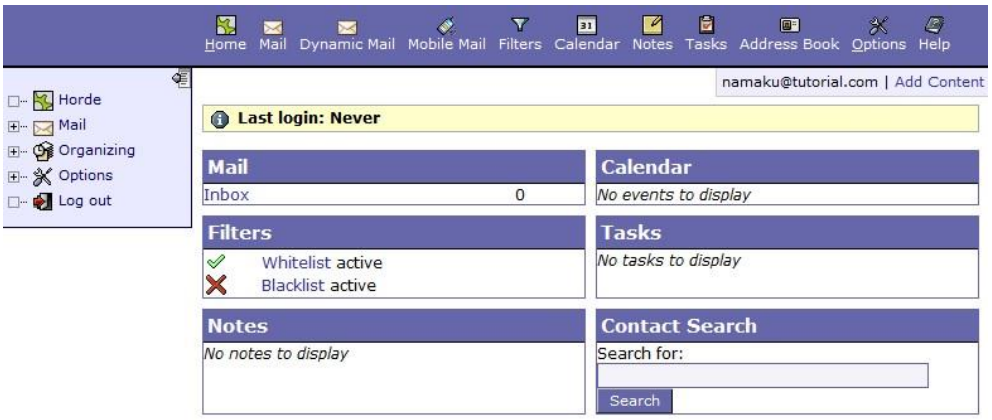
b.Kekurangan

- Tidak praktis (infrastruktur, administrasi, dll)
- Keamanan email dari hacker
- Jika email keluar terkadang membutuhkan proses waktu yang lama
- Jika server down dan tidak ada backup maka dapat terjadi kehilangan email.

2.7 Aplikasi web pengakses e-mail

Aplikasi e-mail yang menggunakan halaman web sebagai media untuk mengelola e-mail, berikut ini merupakan macam-macam aplikasi web pengakses e-mail :

A.Horde



Gambar 2. 4 Tampilan Horde

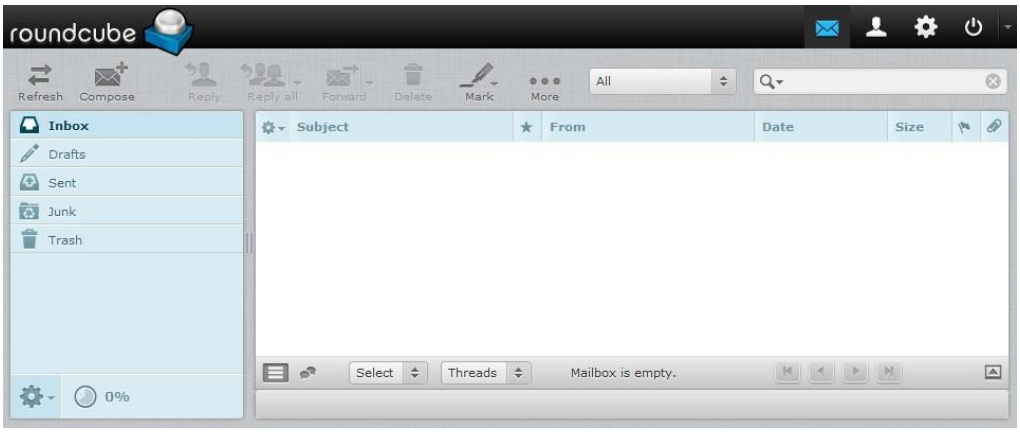
Memiliki fitur yang lengkap. Tetapi jika diakses agak sedikit lambat. Jadi ini tergantung dari akses internet yang anda miliki, dan memiliki tampilan yang sangat kuno.

B.SquirrelMail

Gambar 2. 5 Tampilan Squirrelmail

Dari segi interface cukup sederhana, sehingga jelas fiturnya tidak selengkap Horde. Dan tentu saja aksesnya pun menjadi lebih cepat, lebih mudah di organisir email yang dimiliki dengan leluasa, tanpa harus mensetting ulang layanan (tidak memerlukan mail client), tetapi jika server mengalami masalah, ada kemungkinan email dan akunnya akan hilang, dan tidak prakris.

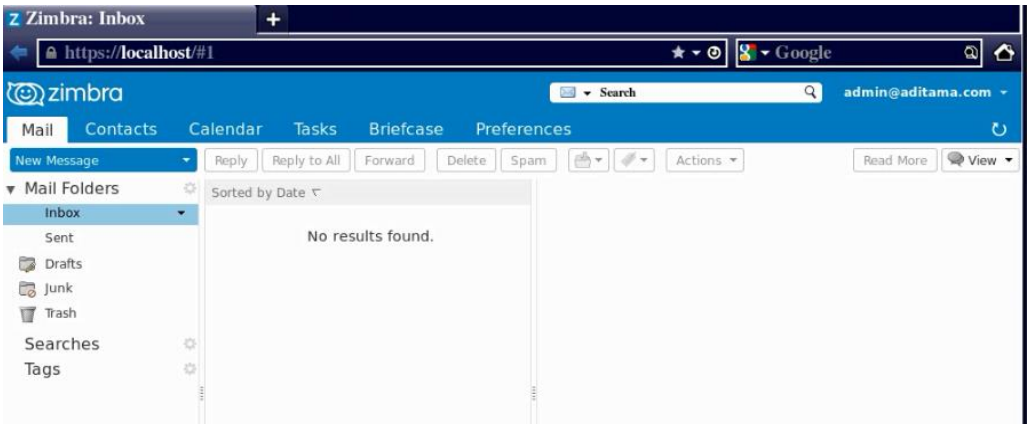
C.Rouncube



Gambar 2. 6 Tampilan Roundcube

Dari fitur tentu saja tidak selengkap Horde tapi lebih baik dari SquirrelMail. Tampilannya lebih menarik dibandingkan SquirrelMail. Akses untuk membukanya tidak selambat anda membuka Horde, tetapi sayanganya roundcube tidak terdapat pada distro debian jadi harus mendownload file mentahannya terlebih dahulu .

D.Zimbra



Gambar 2. 7 Tampilan Zimbra

Kelebihan :

-ClamAV adanya antivirus yang dapat melindungi email dari searanga virus yang dapat menghilangkan data.

-Dapat mengakses email walaupun account dalam keadaan offline.

-Spam Asasin mail filter yang mengidentifikasi adanya spam pada account.

-Zimbra menggunakan aplikasi open source openLDAP sebagai active directory server, menyediakan autentikasi user, masing-masing account yang terdapat pada zimbra mempunyai mailbox yang berbeda dengan program email yang lain dan ID untuk mengidentifikasi account.

-Terdapat alat untuk syslog penggabungan,pelaporan,pelacak pesan.

-Dapat berjalan pada service port RQM 22, postfix 25, HTTP 80, POP3 110, IMAP 143, LDAP 389, HTTPS 443 dll.

-Zimbra ini dapat di install pada semua system operasi yang ada pada pc sekarang ini tapi yang umumnya lebih banyak digunakan pada SO linux.

-Zimbra ini sangat unggul dari beberapa program lainnya yang ada pada saat ini.

-Kita dapat menambahkan beberapa fitur lainnya yang dapat mengoptimalkan akses email kita.

Kekurangan :

-Aplikasi ini agak berat pada penggunaan AJAXnya.

-Biasa terjadi error pada javascriptx kalau bandwitch yang digunakan agak sedikt.

-Adanya kesulitan pada saat penginstalan pertama pada SO linux.

-Yahoo zimbra ini agak susah untuk di pahami dalam apalagi yang menggunakan IE 6, IE 7.

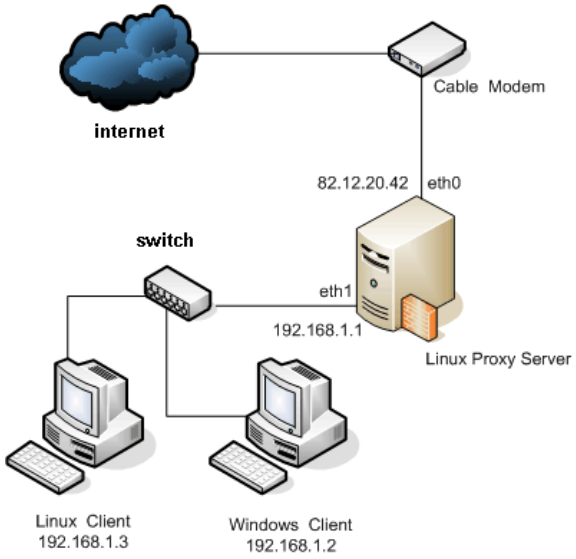
BAB 3 PROXY

3.1Pengertian Proxy Server

A.Penjelasan Proxy

Pengertian proxy adalah server yang menyediakan suatu layanan untuk meneruskan setiap permintaan user kepada server lain yang terdapat di Internet. Atau definisi proxy server yang lainnya yaitu suatu server atau program komputer yang mempunyai peran sebagai penghubung antara suatu komputer dengan internet.

B.Cara Kerja Proxy Server



Gambar 3. 1 Cara Kerja Proxy

Bagaimanakah proxy bekerja? Proxy merupakan pihak ketiga yang berdiri ditengah-tengah antara kedua pihak yang saling berhubungan dan berfungsi sebagai perantara secara prinsip pihak pertama dan pihak kedua tidak secara langsung berhubangan, akan tetapi masing-masing berhubungan dengan perantara yaitu proxy.

Proxy server memotong hubungan langsung antara pengguna dan layanan yang diakases dilakakukan pertama-tama dengan mengubah lamat IP,membuat pemetaan dari alamat Ipjaringan lokal ke suatu alamat IP proxy,yang digunakan untuk jaringan luar atau internet.pada prinsipnya hanya alamat IP proxy tersebut

yang akan diketahui secara umum di internet,Berfungsi sebagai network address translator.

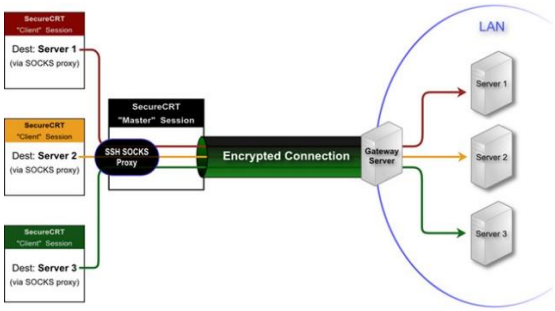
Proxy server juga dapat dipasangkan Firewall sebagai cara untuk membatasi komputer anda menemukan tempat-tempat tertentu di internet (situs web tertentu).

C.Fungsi Proxy

Berikut di bawah ini adalah beberapa fungsi proxy:

1. Fungsi conecting sharing

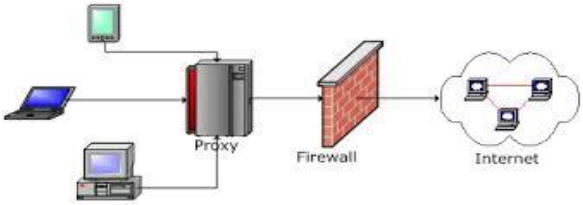
Connection sharing merupakan konsep dasar, user tidak langsung berhubungan dengan jaringan luar atau internet, tetapi harus melewati suatu gateway, gateway bertindak sebagai batas antara jaringan lokal dan jaringan luar. Gateway ini sangat penting, karena jaringan harus dilindungi dari bahaya yang mungkin berasal dari internet, dan hal tersebut akan sulit dilakukan bila tidak ada garis batas yang jelas pada jaringan lokal dan internet. Gateway bertindak sebagai titik dimana sejumlah koneksi dari pengguna lokal akan terhubung, dan jaringan luar juga akan terhubung. Dalam hal ini, gateway bisa sebagai proxy server, karena menyediakan layanan sebagai perantara antara jaringan lokal dan jaringan luar atau internet



Gambar 3. 2 Fungsi Sharing

2. Fungsi filtering

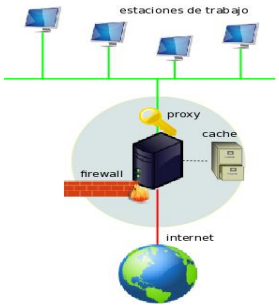
Terdapat beberapa proxy yang dilengkapi dengan firewall yang dapat memblokir beberapa atau sebuah alamat IP yang tidak diinginkan, sehingga beberapa website tidak dapat diakses dengan memakai proxy tersebut. Itulah salah satu fungsi dari proxy sebagai filtering.



Gambar 3. 3 Fungsi Filtering

3. Fungsi caching

fungsi proxy yang lainnya yaitu sebagai fungsi caching, disini maksudnya proxy juga dilengkapi dengan media penyimpanan data dari suatu web, dari query ataupun permintaan akses user. Misalnya permintaan untuk mengakses suatu web dapat lebih cepat jika telah ada permintaan akses ke suatu web pada pemakai proxy sebelumnya. Itulah fungsi proxy sebagai chacing.



Gambar 3. 4 Caching

D.Hal-hal Yang Dapat Dilakukan Oleh Web Proxy

Web proxy adalah komputer server yang bertindak sebagai komputer lainnya berfungsi untuk melakukan request terhadap konten dari suatu jaringan internet ataupun jaringan intranet. Adapun hal-hal yang dapat dilakukan oleh web proxy diantaranya sebagai berikut ini:

- Dapat menyembunyikan alamat IP address.
- Dapat dipakai untuk mengakses suatu website yang telah di blok oleh ISP (Internet service provider) atau oleh suatu organisasi. .
- Dapat di gunakan untuk men-blok beberapa atau sebuah website yang nantinya didak dapat diakses.
- Dapat men-filter cookies yang tidak di inginkan dan seluruh cookies yang tersimpan di encrypt.

- Dan dapat meningkatkan keamanan privacy pengguna.

3.2Kelebihan dan Kekurangan Proxy Server

A.Kelebihan

1. Proxy bisa menyembunyikan identitas IP anda.
2. Mempercepat akses ke suatu website.
3. Dapat digunakan untuk mengakses suatu website atau IP yang diblokir oleh Penyedia ISP atau Penyedia jaringan Internet tertentu (Dengan Proxy Tertentu).
4. Proxy dapat digunakan untuk memblokir akses ke suatu IP atau website (Dengan Proxy tertentu).
5. Meningkatkan Privacy atau keamanan karena proxy ini akan menfilter cookies yang tidak diinginkan dan tersimpan dalam keadaan ter- encrypsi (Proxy Tertentu).

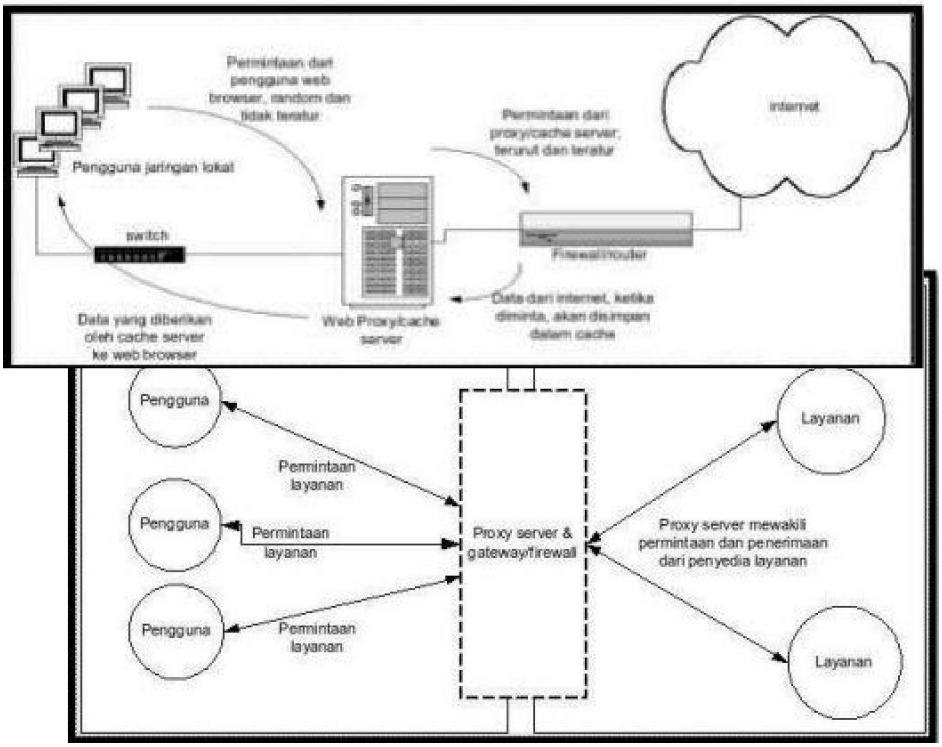
B.Kekurangan

1. Pengaksesan terhadap situs yang belum pernah dibuka sebelumnya akan menjadi lebih lambat, karena client harus meminta terlebih dahulu ke pada proxy, setelah itu baru proxy yang akan meminta request dari client tersebut ke pada penyedia layanan internet.
2. Bila proxy server terlambat melakukan update cache, maka client akan mendapatkan content yang belum update ketika melakukan request content tersebut.

3.3 Proxy Sebagai Gateway

Dalam suatu jaringan lokal yang terhubung ke jaringan lain atau internet, pengguna tidak langsung berhubungan dengan jaringan luar atau internet, tetapi harus melewati suatu gateway, yang bertindak sebagai batas antara jaringan lokal dan jaringan luar. Gateway ini sangat penting, karena jaringan lokal harus dapat dilindungi dengan baik dari bahaya yang mungkin berasal dari internet, dan hal tersebut akan sulit dilakukan bila tidak ada garis batas yang jelas jaringan lokal dan internet.

Gateway juga bertindak sebagai titik dimana sejumlah koneksi dari pengguna lokal akan terhubung kepadanya, dan suatu koneksi ke jaringan luar juga terhubung kepadanya. Dengan demikian, koneksi dari jaringan lokal ke internet akan menggunakan sambungan yang dimiliki oleh gateway secara bersama-sama (connection sharing). Dalam hal ini, gateway adalah juga sebagai proxy server, karena menyediakan layanan sebagai perantara antara jaringan lokal dan jaringan luar atau internet. Diagram berikut menggambarkan posisi dan fungsi dari proxy server, diantara pengguna dan penyedia layanan:



Gambar 3. 5 Gateway Pada Proxy

3.4 Jenis-Jenis Proxy Server

Seperti yang telah disebutkan di atas bahwa sebuah proxy server memiliki berbagai macam fungsi atau tujuan potensial. Berikut ini akan dijelaskan proxy server yang berfungsi sebagai cache proxy (mempercepat akses ke sumber daya), filter proxy (memfilter akses ke situs-situs tertentu), dan juga jenis proxy yang lain.

A.Cache Proxy

Seperti yang telah disebutkan di atas bahwa sebuah proxy server memiliki berbagai macam fungsi atau tujuan potensial. Berikut ini akan dijelaskan proxy server yang berfungsi sebagai cache proxy (mempercepat akses ke sumber daya),

filter proxy (memfilter akses ke situs-situs tertentu), dan juga jenis proxy yang lain.

B. Filter Proxy

Sebuah content-filtering web proxy memberikan kontrol administratif terhadap konten yang mungkin disampaikan melalui proxy. Dengan ini kita bisa membatasi akses komputer klien ke situs-situs atau konten tertentu. Hal ini umumnya digunakan baik di organisasi non-komersial maupun di organisasi komersial (terutama sekolah-sekolah) untuk memastikan bahwa penggunaan internet sesuai dengan kebijakan penggunaan yang diterima.Beberapa metode yang umum digunakan untuk konten penyaringan meliputi: URL atau blacklist DNS, URL regex penyaringan, MIME penyaringan, atau kata kunci penyaringan konten.

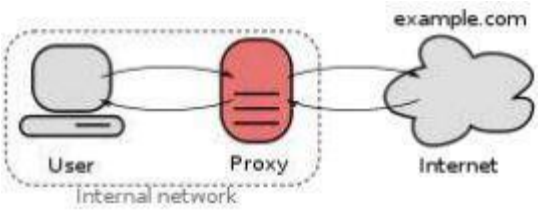
C. Transparent Proxy

Dengan menggunakan transparent proxy maka kita tidak perlu menyetting proxy pada web browser klien, sehingga browser akan otomatis melewati proxy pada saat mengakses web.Jadi transparent proxy ini sangat bermanfaat untuk memastikan bahwa semua klien pastimelewati proxy.

D. SOCKS Proxy

SecureSocket (SOCKS) adalah internet protokol yang rute paket jaringan antara klien dan server nya melalui proxy server. Socks5 menyediakan layanan tambahan yakni otentikasi sehingga hanya pengguna yang sah dapat mengakses server. Praktis, server SOCKS akan memperantarai koneksi TCP ke alamat IP yang berubah- ubah serta menyediakan sarana untuk paket UDP agar dapat diteruskan. SOCKS terdapat pada Layer 5 dari model OSI (lapisan perantara antara lapisan presentasi dan lapisan transport).

SOCKS adalah standar de-facto untuk circuit-level gateway. Penggunaan lain dari SOCKS adalah sebagai alat pengelakan, yang memungkinkan untuk melewati penyaringan Internet untuk mengakses konten jika diblokir oleh pemerintah, tempat kerja, sekolah dan layanan web negara tertentu.



Gambar 3. 6 SOCKS Proxy

Beberapa klien SSH mendukung port forwarding dinamis yang memungkinkan pengguna untuk membuat SOCKS proxy lokal. Hal ini dapat membebaskan pengguna dari keterbatasan menghubungkan hanya ke remote port yang telah ditetapkan oleh server.

E. Froward Proxy

Forward proxy merupakan proxy yang paling umum, dan ditemukan online sebagai open proxy. Forward proxy meneruskan (forward) sebuah request dari komputer pada sebuah website, dan kemudian mengakses server untuk mengambil informasi. Forward proxy memiliki kemampuan untuk mengakses lebih banyak website dibandingkan reverse proxy.

Pada konfigurasi forward proxy, request berasal dari sebuah komputer dalam bentuk percobaan pengguna mengakses website. Request disaring melalui forward proxy dan kemudian melalui sebuah firewall. Firewall memastikan request bersifat legal atau sah, atau dari pengguna sebenarnya dan bukan dari program jahat (malicious program). Jika request-nya merupakan request yang benar, maka proxy akan meneruskannya (forward). Namun jika tidak, maka request ditolak (request denied).

Setelah mendapatkan informasi dari server website, maka proses akan membalik sehingga informasi akan tertuju pada komputer yang membuat request. Forward proxy dibuat untuk meneruskan traffic dari server ke tahapan berikutnya.

F. Reverse Proxy

Pada Reverse Proxy ini, Proxy berada di garda depan menerima permintaan HTTP Request (umumnya diport 80). Seperti Forward Proxy, salah satu tugas dari Reverse Proxy ini yaitu untuk melakukan caching halaman-halaman web yang pernah di-request sebelumnya.

Reverse proxy berjalan di port 80 untuk melayani request Http. Di port 80 Reverse Proxy tidak menggantikan fungsi Web Server, melainkan dia akan

melanjutkan request Http tersebut ke Web Server untuk diolah. Dan apabila Web Server telah selesai mengolah permintaanya tersebut, Web Server akan mengembalikan kembali ke Reverse Proxy. Sebelum Reverse Proxy mengirim kembali request Http tersebut ke client sebagai respons (HTTP Response), Reverse Proxy akan menyimpan respon Http tersebut kedalam media penyimpanan sekunder. Sehingga, apabila ada request Http yang sama kembali, Reverse Proxy akan mengambil langsung response Http tersebut tanpa meneruskan request Http tersebut ke Web Server.

Keuntungan penerapan Reverse Proxy ini, apalagi di Web Server dengan traffic yang tinggi yakni memberikan nilai plus di sisi user-experience. Client akan mendapatkan response dari halaman yang direquest lebih cepat ketimbang merequest ke Web Server yang tidak menggunakannya. Dan keuntungan dari sisi server yaitu load server akan turun karena tugas dari Web Server akan lebih ringan dengan sedikitnya request yang diterimanya.

Sebagai catatan, Request Header yang diterima oleh Web Server adalah Request Header dari Proxy, bukan dari client. Buat yang melakukan analisa statistik web (Urchin, AwStat) maupun trace/debug log Web Server, perlu dilakukan setting tambahan di sisi Proxy dan Web Server.

3.5 Proxy Squid

Gambar 3. 7 Proxy Squid

Squid adalah sebuah daemon yang digunakan sebagai proxy server dan web cache. Squid memiliki banyak jenis penggunaan, mulai dari mempercepat server web dengan melakukan caching permintaan yang berulang-ulang, caching DNS, caching situs web, dan caching pencarian komputer di dalam jaringan untuk sekelompok

komputer yang menggunakan sumber daya jaringan yang sama, hingga pada membantu keamanan dengan cara melakukan penyaringan (filter) lalu lintas. Meskipun seringnya digunakan untuk protokol HTTP dan FTP, Squid juga menawarkan dukungan terbatas untuk beberapa protokol lainnya termasuk Transport Layer Security (TLS), Secure Socket Layer (SSL), Internet Gopher, dan HTTPS. Versi Squid 3.1 mencakup dukungan protokol IPv6 dan Internet Content Adaptation Protocol (ICAP).

Squid pada awalnya dikembangkan oleh Duane Wessels sebagai "Harvest object cache", yang merupakan bagian dari proyek Harvest yang dikembangkan di University of Colorado at Boulder. Pekerjaan selanjutnya dilakukan hingga selesai di University of California, San Diego dan didanai melalui National Science Foundation. Squid kini hampir secara eksklusif dikembangkan dengan cara usaha sukarela.

Squid umumnya didesain untuk berjalan di atas sistem operasi mirip UNIX, meski Squid juga bisa berjalan di atas sistem operasi Windows. Karena dirilis di bawah lisensi GNU General Public License, maka Squid merupakan perangkat lunak bebas.

A.ACL (Access Control List) Pada Squid

Selanjutnya konfigurasi-konfigurasi lanjutan squid, selain sebagai cache server, squid yang memang bertindak sebagai “parent” untuk meminta object dari kliennya dapat juga dikonfigurasikan untuk pengaturan hak akses lebih lanjut, untuk pertama kali yang dibicarakan adalah ACL (Access Control List), ACL sendiri terdiri dari beberapa tipe antara lain :

1.src= IP Address asal yang digunakan klien
2.dst= IP Address tujuan yang diminta klien
3.myip= IP Address lokal dimana klien terhubung
4.srcdomain= Nama domain asal klien
5.dstdomain= Nama domain tujuan klien
6.srcdom_regex= Pencarian pola secara string dari nama domain asal klien
7.dstdom_regex= Pencarian pola secara string dari nama domain tujuan klien
8.time = Waktu dinyatakan dalam hari dan jam
9.proto= Protokol transfer (http, ftp, gopher)
10.method= Metode permintaan http (get, post, connect)
11.url_regex= Regex yang cocok di URL secara keseluruhan

12.cache_dir= Mendefinisikan suatu direktori cache

13.delay_pools= Menspesifikasikan jumlah pool yang digunakan untuk membatasi jumlah bandwith dari ACL.

14.delay_class= Menspesifikasikan kelompok dari masing-masing pool yang telah didefinisikan pada objek delay_pools

15.delay_parameters= Menspesifikasikan rumus bandwidth yang akandi dapatkan oleh ACL yang akan memasuki delay_pools

16.delay_access= Mendefinisikan ACL yang akan dimasukkan ke pool tertentu untuk mendapatkan "perlambatan" bandwidth

17.deny_info= Mendefinisikan output halaman HTML pada Squid untuk ACL tertentu

Selanjutnya adalah control list yang akan digunakan untuk mengatur kontrol dari ACL, control list tersebut antara lain :

1.http_access= Memperbolehkan access http

2.icp_access= Memperbolehkan peer untuk mengirimkan icp untuk men-query objek

3.miss_access= Memperbolehkan klien meminta objek yang belum ada (miss) di dalam cache

4.no_cache= Objek yang diminta klien tidak perlu disimpan ke harddisk

5.always_direct = Permintaan yang ditangani secara langsung ke server origin

6.never_direct= Permintaan yang ditangani secara tidak langsung ke server origin

3.6 Sistem Autentikasi Pada Squid

Squid dapat memproteksi suatu jaringan dengan sistem autentikasi. Contohnya di kampus Gunadarma, setelah laptop kita terkoneksi dalam jaringan hotspot maka kita haru login terlebih dahulu menggunakan email dan password studentsite agar kita bisa mengakses situs yang lain. Hal yang seperti ini bisa ditangani dengan menggunakan Squid.

Squid mengenal beberapa macam skema autentikasi seperti berikut :

1.Basic Authentication

Ini adalah skema autentikasi yang didukung oleh semua peramban (browser) utama dan berfungsi dengan baik di semua OS. Sayangnya skema *Basic Authentication* ini memiliki satu kelemahan utama, yaitu proses pengriman data user dan password dikirim dalam format *plain text*. Jadi sangat rentan terhadap proses sniff atau penyadapan saat proses autentikasi berlangsung. Contoh program pembantu untuk skema *Basic Authentication* ini adalah LDAP.

2.Digest Authentication

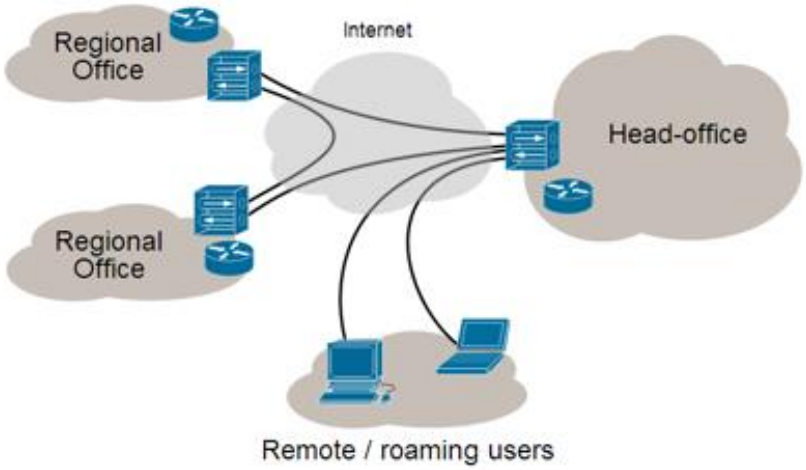
Skema ini lebih aman, karena pada saat autentikasi, data username dan password tidak dikirm dalam format *plain text*. Secara umum, kelebihan skema *Digest Authentication* dibandingkan *Basic Authenctication*, yaitu lebih aman. Tapi sayangnya tidak didukung oleh beberapa browser, yakni Internet Explorer 5 & 6.

3.NTLM Authentication

Dengan Menggunakan skema *NTLM Authentication*, semua user yang sudah login ke domain, ketika mengakses squid tidak akan diminta untuk memasukkan username dan password lagi. Ini yang kita kenal sebagai proses *Single Sign On.* Jika sudah sukses autentikasi di satu layanan, ketika ingin menggunakan layanan lain tidak perlu memasukkan login dan password lagi, proses autentikasi berlangsung secara transparan. Sayangnya skema ini hanya berfungsi dengan baik di sistem operasi Windows dan hanya mendukung browser Internet Explorer dan FireFox.

BAB 4 VPN (Virtual Private Network)

6.1 Pengertian VPN



Gambar 4. 1 VPN

VPN atau Virtual Private Network adalah suatu koneksi antara satu jaringan dengan jaringan lainnya secara privat melalui jaringan publik (Internet). VPN disebut Virtual network karena menggunakan jaringan publik (Internet) sebagai media perantaranya alias bukan koneksi langsung. Dan disebut Private network karena jaringannya bersifat privat, dimana hanya orang tertentu saja yang bisa mengaksesnya. Data yang dikirimkan pun terenkripsi sehingga aman dan tetap rahasia meskipun dikirim melalui jaringan publik.

6.2 Cara Kerja VPN

Cara kerja VPN ibarat seperti membuat jaringan di dalam jaringan atau biasa disebut tunneling (membuat terowongan). Tunneling adalah suatu cara untuk membuat jalur koneksi secara privat dengan menggunakan infrastruktur jaringan lain. Pada dasarnya VPN juga membutuhkan sebuah server sebagai penghubung dan pengatur antar client.

Gambar 4. 2 Cara Kerja VPN

Penjelasan :

internet <—> VPN Server <—-> VPN Client <—-> Client

bila digunakan untuk menghubungkan 2 komputer secara private dengan jaringan internet maka seperti ini:

Komputer A <—> VPN Clinet <—> Internet <—> VPN Server <—> VPN Client <—> Komputer B

Jadi semua koneksi diatur oleh VPN Server sehingga dibutuhkan kemampuan VPN Server yang memadai agar koneksinya bisa lancar.

6.3 Fungsi VPN

Teknologi VPN atau Private Network mempunyai tiga fungsi utama yaitu :

A.Confidentially (Kerahasiaan)

Teknologi VPN merupakan teknologi yang memanfaatkan jaringan publik yang tentunya sangat rawan terhadap pencurian data. Untuk itu, VPN menggunakan metode enkripsi untuk mengacak data yang lewat. Dengan adanya teknologi enkripsi itu, keamanan data menjadi lebih terjamin. Walaupun ada pihak yang dapat menyadap data yang melewati internet bahkan jalur VPN itu sendiri, namun belum tentu dapat membaca data tersebut, karena data tersebut telah teracak. Jadi, confidentially ini dimaksudkan agar informasi yang ditransmisikan hanya boleh diakses oleh sekelompok pengguna yang berhak.

B.Data Integrity (Keutuhan Data)

Ketika melewati jaringan internet, sebenarnya data telah berjalan sangat jauh melintasi berbagai negara. Pada saat perjalanan tersebut, berbagai gangguan dapat terjadi terhadap isinya, baik hilang, rusak, ataupun dimanipulasi oleh orang yang tidak seharusnya. Pada VPN terdapat teknologi yang dapat menjaga keutuhan data mulai dari data dikirim hingga data sampai di tempat tujuan.

C.Origin Authentication (Autentikasi Sumber)

Teknologi VPN memiliki kemampuan untuk melakukan autentikasi terhadap sumber-sumber pengirim data yang akan diterimanya. VPN akan melakukan pemeriksaan terhadap semua data yang masuk dan mengambil informasi dari sumber datanya. Kemudian, alamat sumber data tersebut akan disetujui apabila proses autentikasinya berhasil. Dengan demikian, VPN menjamin semua data yang dikirim dan diterima berasal dari sumber yang seharusnya. Tidak ada data yang dipalsukan atau dikirim oleh pihak-pihak lain.

6.4 Kelebihan VPN

VPN memungkinkan karyawan/pengguna untuk terkoneksi dengan jaringan internal kantornya dari manapun diseluruh dunia, yang penting terhubung dengan internet.

A.Efektif dan Efesien

Waktu yang dibutuhkan untuk menghubungkan jaringan kantor-kantor cabang ke jaringan kantor pusat lebih cepat, karena hanya dengan menyediakan akses internet di kantor-kantor cabang otomatis kantor cabang tersebut bisa langsung dikoneksikan ke jaringan di kantor pusat. Sedangkan penggunaan leased line sebagai WAN akan membutuhkan waktu yang lama untuk membangun jalur koneksi khusus dari kantor cabang yang baru dengan perusahaan induknya. Dengan demikian penggunaan VPN secara tidak langsung akan meningkatkan efektivitas dan efisiensi kerja.

B.Hemat Biaya

Penggunaan VPN dapat mengurangi biaya operasional, karena VPN menggunakan infrastruktur jaringan publik yang sudah ada, sehingga tidak perlu membangun infrastruktur jaringan yang baru.

C.Meningkatkan Skalabilitas

Penggunaan VPN akan meningkatkan skalabilitas. Ketika Perusahaan berkembang dan membuat kantor cabang baru dibeberapa tempat akan lebih terhubung dengan jaringan lokal kantor pusat.

6.5 Kekurangan VPN

Karena penyediaan akses ke pegawai secara global, faktor keamanan menjadi suatu resiko, hal tersebut dapat menempatkan informasi yang sensitif dari organisasi ataupun perusahaan dapat diakses secara global, karena dengan menggunakan VPN memerlukan perhatian yang lebih untuk penetapan sistem keamanan yang cukup baik dan jelas.

6.6 Manfaat Dari VPN

Beberapa manfaat VPN, diantaranya seperti di bawah ini:

1. Remote Access – Maksudnya dengan menggunakan VPN kita bisa mengakses komputer ataupun jaringan kantor, dari mana saja selama terhubung ke jaringan internet atau publik.
2. Keamanan – dengan menggunakan koneksi VPN kita bisa browsing, searching dengan aman saat mengakses dunia maya atau jaringan internet publik misalnya seperti hotspot atau internet yang ada di cafe-cafe.
3. Dapat menghemat biaya setup jaringan – VPN juga dapat dipakai sebagai cara alternatif untuk menghubungkan jaringan lokal yang cukup luas dengan biaya yang lebih rendah. Karena transmisi data yang digunakan pada VPN memakai media jaringan internet atau jaringan publik yang sebelumnya telah ada tanpa perlu membangun jaringan sendiri.

6.7 Perbedaan TCP dengan UDP

TCP (Transmission Control Protocol) adalah salah satu jenis protokol yang memungkinkan sekumpulan komputer untuk berkomunikasi dan bertukar data didalam suatu jaringan. Sedangkan UDP (User Datagram Protocol) adalah salah satu protokol lapisan transport TCP/IP yang mendukung komunikasi yang tidak handal (unreliable), tanpa koneksi antara host-host dalam jaringan yang menggunakan TCP/IP.

UDP (User Datagram Protocol) adalah transport layer yang tidak handal (unreliable), connectionless dan merupakan kebalikan dari transport layer TCP. Dengan menggunakan UDP, setiap aplikasi socket dapat mengirimkan paket – paket yang berupa datagram. Istilah datagram diperuntukkan terhadap paket dengan koneksi yang tidak handal (unreliable service). Koneksi yang handal selalu memberikan keterangan apabila pengiriman data gagal, sedangkan koneksi yang tidak handal tidak akan mengirimkan keterangan meski pengiriman data gagal.

Contoh aplikasi yang menggunakan protocol TCP :

– TELNET

– FTP (File Transfer Protocol)

– SMTP (Simple Mail Transfer Protocol)

Contoh aplikasi yang menggunakan protocol UDP

– DNS (Domain Name System)

– SNMP (Simple Network Management Protocol)

– TFTP (Trivial File Transfer Protocol)

– SunRPC

	TCP	UDP
PROTOCOL	TCP mempunyai karakteristik sebagai protokol yang	UDP mempunyai karateristik connectionless (tidak berbasis koneksi). Data yang dikirimkan dalam

	berorientasi koneksi (Connection oriented). Protokol TCP menggunakan jalur data full duplex yang berarti antara kedua host terdapat dua buah jalur, jalur masuk dan jalur keluar sehingga data dapat dikirimkan secara simultan.	bentuk packet tidak harus melakukan call setup seperti pada TCP. Data dalam protokol UDP akan dikirimkan sebagai datagram tanpa adanya nomor identifier. Sehingga sangat besar sekali kemungkinan data sampai tidak berurutan dan sangat mungkin hilang/rusak dalam perjalananan dari host asal ke host tujuan.
	TCP	UDP
PORT	Port – port yang digunakan dalam transport layer menggunakan 16-bit integer (0 – 65535), dengan satu sama lain harus berbeda (unique).	Port dalam UDP menggunakan 16-bit integer, port – port yang bisa digunakan adalah antara 1 sampai 65535. Port – port yang digunakan dibagi menjadi 3 bagian yaitu well-known port (antara 1 – 1023), registered port (1024 – 49151) dan ephemeral port (49152 – 65535).
KOMUNIKASI	Memungkinkan sekumpulan komputer untuk berkomunikasi dan bertukar data didalam suatu jaringan.	Kurang handal dalam komunikasi tanpa koneksi antara host-host dalam jaringan yang menggunakan TCP/IP.

Tabel 4. 1 Perbedaan TCP dan UDP

BAB 5 FIREWALL

5.1 Pengertian Dan Cara Kerja Firewall

Jika Anda telah menggunakan Internet secara teratur atau bekerja di sebuah perusahaan besar dan surfing internet saat Anda berada di tempat kerja, Anda harus memiliki pasti datang di firewall panjang. Anda mungkin juga telah mendengar orang mengatakan "firewall melindungi firewall di tempat kerja mereka**".**Jika Anda pernah bertanya-tanya untuk mengetahui apa sebenarnya firewall ini dan bagaimana cara kerjanya, di sini kita pergi. Dalam posting ini saya akan mencoba menjelaskan "Bagaimana firewall bekerja" dalam istilah awam.

Firewall merupakan suatu cara/sistem/mekanisme yang diterapkan baik terhadap hardware , software ataupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan/kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkupnya. Segmen tersebut dapat merupakan sebuah workstation, server, router, atau local area network (LAN) anda.

Firewall secara umum di peruntukkan untuk melayani **:**

1.Mesin/Komputer

Setiap individu yang terhubung langsung ke jaringan luar atau internet dan menginginkan semua yang terdapat pada komputernya terlindungi.

2.Jaringan

Jaringan komputer yang terdiri lebih dari satu buah komputer dan berbagai jenis topologi jaringan yang digunakan, baik yang di miliki oleh perusahaan, organisasi dsb.

5.2 Karakteristik Firewall

1.Seluruh hubungan/kegiatan dari dalam ke luar , harus melewati firewall. Hal ini dapat dilakukan dengan cara memblok/membatasi baik secara fisik semua akses terhadap jaringan Lokal, kecuali melewati firewall. Banyak sekali bentuk jaringan yang memungkinkan.

2.Hanya Kegiatan yang terdaftar/dikenal yang dapat melewati/melakukan hubungan, hal ini dapat dilakukan dengan mengatur policy pada konfigurasi

keamanan lokal. Banyak sekali jenis firewall yang dapat dipilih sekaligus berbagai jenis policy yang ditawarkan.

3.Firewall itu sendiri haruslah kebal atau relatif kuat terhadap serangan/kelemahan. hal ini berarti penggunaan sistem yang dapat dipercaya dan dengan Operating system yang relatif aman.

5.3 Teknik Yang Digunakan Oleh Firewall

A.Sevice Control (kendali terhadap layanan)

Berdasarkan tipe-tipe layanan yang digunakan di Internet dan boleh diakses baik untuk kedalam ataupun keluar firewall. Biasanya firewall akan mencek no IP Address dan juga nomor port yang di gunakan baik pada protokol TCP dan UDP, bahkan bisa dilengkapi software untuk proxy yang akan menerima dan menterjemahkan setiap permintaan akan suatu layanan sebelum mengijinkannya.Bahkan bisa jadi software pada server itu sendiri , seperti layanan untuk web ataupun untuk mail.

B.Direction Control (kendali terhadap arah)

Berdasarkan arah dari berbagai permintaan (request) terhadap layanan yang akan dikenali dan diijinkan melewati firewall.

C. User control (kendali terhadap pengguna)

Berdasarkan pengguna/user untuk dapat menjalankan suatu layanan, artinya ada user yang dapat dan ada yang tidak dapat menjalankan suatu servis,hal ini di karenakan user tersebut tidak di ijinkan untuk melewati firewall. Biasanya digunakan untuk membatasi user dari jaringan lokal untuk mengakses keluar, tetapi bisa juga diterapkan untuk membatasi terhadap pengguna dari luar.

D.Behavior Control (kendali terhadap perlakuan)

Berdasarkan seberapa banyak layanan itu telah digunakan. Misal, firewall dapat memfilter email untuk menanggulangi/mencegah spam.

5.4 Tipe – Tipe Firewall

A. Pake Fitering Routing

Packet Filtering diaplikasikan dengan cara mengatur semua packet IP baik yang menuju, melewati atau akan dituju oleh packet tersebut.pada tipe ini packet tersebut akan diatur apakah akan di terima dan diteruskan , atau di tolak.penyaringan packet ini di konfigurasikan untuk menyaring packet yang akan di transfer secara dua arah (baik dari atau ke jaringan lokal). Aturan penyaringan didasarkan pada header IP dan transport header,termasuk juga alamat awal(IP) dan alamat tujuan (IP),protokol transport yang di gunakan(UDP,TCP), serta nomor port yang digunakan. Kelebihan dari tipe ini adalah mudah untuk di implementasikan, transparan untuk pemakai, lebih cepat Adapun kelemahannya adalah cukup rumitnya untuk menyetting paket yang akan difilter secara tepat, serta lemah dalam hal authentikasi.

Adapun serangan yang dapat terjadi pada firewall dengan tipe ini adalah:

- IP address spoofing : intruder (penyusup) dari luar dapat melakukan ini dengan cara menyertakan/menggunakan ip address jaringan lokal yanbg telah
  diijinkan untuk melalui firewall.
- Source routing attacks : tipe ini tidak menganalisa informasi routing sumber IP, sehingga memungkinkan untuk membypass firewall.
- Tiny Fragment attacks : intruder (penyusup) membagi IP kedalam bagian-bagian (fragment) yang lebih kecil dan memaksa terbaginya informasi mengenai TCP header. Serangan jenis ini di design untuk menipu aturan penyaringan yang bergantung kepada informasi dari TCP header. Penyerang berharap hanya bagian (fragment) pertama saja yang akan di periksa dan sisanya akan bisa lewat dengan bebas. Hal ini dapat di tanggulangi dengan cara menolak semua packet dengan protokol TCP dan memiliki Offset = 1 pada IP fragment (bagian IP)

B. Application-Level Gateway

Application-level Gateway yang biasa juga di kenal sebagai proxy server yang berfungsi untuk memperkuat/menyalurkan arus aplikasi. Tipe ini akan mengatur semua hubungan yang menggunakan layer aplikasi ,baik itu FTP, HTTP, GOPHER dll.

Cara kerjanya adalah apabila ada pengguna yang menggunakan salah satu aplikasi semisal FTP untuk mengakses secara remote, maka gateway akan meminta user memasukkan alamat remote host yang akan di akses.Saat pengguna mengirimkan USer ID serta informasi lainnya yang sesuai maka gateway akan melakukan hubungan terhadap aplikasi tersebut yang terdapat pada remote host, dan menyalurkan data diantara kedua titik. apabila data tersebut tidak sesuai maka firewall tidak akan meneruskan data tersebut atau menolaknya. Lebih jauh lagi, pada tipe ini Firewall dapat di konfigurasikan untuk hanya mendukung beberapa aplikasi saja dan menolak aplikasi lainnya untuk melewati firewall.

Kelebihannya adalah relatif lebih aman daripada tipe packet filtering router lebih mudah untuk memeriksa (audit) dan mendata (log) semua aliran data yang masuk pada level aplikasi.

Kekurangannya adalah pemrosesan tambahan yang berlebih pada setiap hubungan. yang akan mengakibatkan terdapat dua buah sambungan koneksi antara pemakai dan gateway, dimana gateway akan memeriksa dan meneruskan semua arus dari dua arah.

C. Circuit-level Gateway

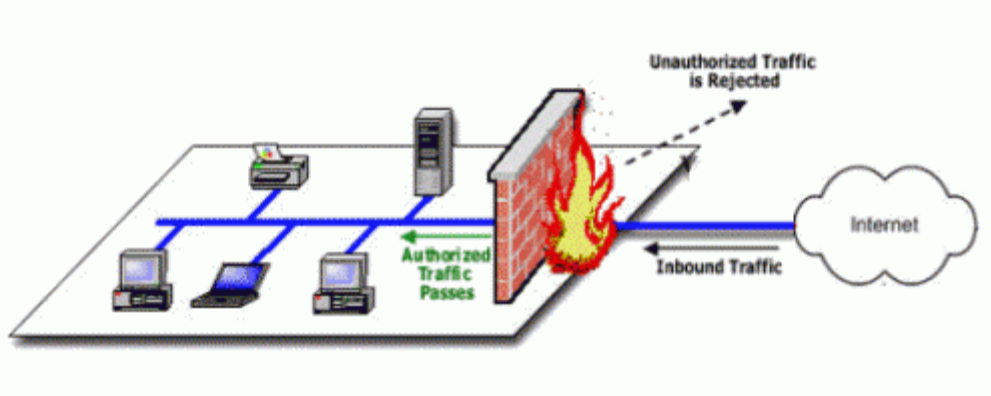
Tipe ketiga ini dapat merupakan sistem yang berdiri sendiri , atau juga dapat merupakan fungsi khusus yang terbentuk dari tipe application-level gateway.tipe ini tidak mengijinkan koneksi TCP end to end (langsung)

cara kerjanya : Gateway akan mengatur kedua hubungan tcp tersebut, 1 antara dirinya (gw) dengan TCP pada pengguna lokal (inner host) serta 1 lagi antara dirinya (gw) dengan TCP pengguna luar (outside host). Saat dua buah hubungan terlaksana, gateway akan menyalurkan TCP segment dari satu hubungan ke lainnya tanpa memeriksa isinya. Fungsi pengamanannya terletak

pada penentuan hubungan mana yang di ijinkan. Penggunaan tipe ini biasanya dikarenakan administrator percaya dengan pengguna internal (internal users).

5.5 Cara Kerja Firewall

Firewall pada dasarnya merupakan penghalang antara komputer Anda (atau jaringan) dan Internet (luar dunia). Firewall bisa hanya dibandingkan dengan seorang penjaga keamanan yang berdiri di pintu masuk rumah Anda dan menyaring pengunjung yang datang ke tempat AndaDia mungkin mengizinkan beberapa pengunjung untuk masuk sementara menyangkal orang lain yang ia tersangka penyusup yang. Demikian pula firewall adalah sebuah program perangkat lunak atau perangkat keras yang menyaring informasi (paket) yang datang melalui internet ke komputer pribadi Anda atau jaringan komputer.



Gambar 5. 1 Cara Kerja Firewall

Firewall dapat memutuskan untuk mengizinkan atau memblokir lalu lintas jaringan antara perangkat berdasarkan aturan yang pra-dikonfigurasi atau ditentukan oleh administrator firewall. Kebanyakan personal firewall seperti firewall Windows beroperasi pada seperangkat aturan pra-konfigurasi yang paling cocok dalam keadaan normal sehingga pengguna tidak perlu khawatir banyak tentang konfigurasi firewall.
firewall pribadi adalah mudah untuk menginstal dan menggunakan dan karenanya disukai oleh pengguna-akhir untuk digunakan pada komputer pribadi mereka. Namun jaringan besar dan perusahaan-perusahaan lebih memilih orang-orang firewall yang memiliki banyak pilihan untuk mengkonfigurasi sehingga untuk memenuhi kebutuhan khusus mereka. Sebagai contoh, perusahaan mungkin membuat aturan firewall yang berbeda untuk server FTP, Telnet server dan server Web. Selain itu perusahaan bahkan

dapat mengontrol bagaimana karyawan dapat terhubung ke Internet dengan memblokir akses ke situs web tertentu atau membatasi transfer file ke jaringan lain. Jadi selain keamanan, firewall dapat memberikan perusahaan kontrol luar biasa atas bagaimana orang menggunakan jaringan.

Firewall menggunakan satu atau lebih metode berikut untuk mengatur lalu lintas masuk dan keluar dalam sebuah jaringan:

1.Packet Filtering

Pada metode ini paket (potongan kecil data) dianalisa dan dibandingkan dengan**filter.** filter paket memiliki seperangkat aturan yang datang dengan tindakan menerima dan menolak yang pra-dikonfigurasi atau dapat dikonfigurasi secara manual oleh administrator firewall.. Jika paket berhasil membuatnya melalui filter ini maka itu diperbolehkan untuk mencapai tujuan, kalau tidak akan dibuang.

2.**Stateful Inspeksi**

Metode baru yang tidak menganalisa isi dari paket. Sebaliknya ia membandingkan aspek kunci tertentu setiap paket database sumber terpercaya.. Kedua paket yang masuk dan keluar dibandingkan terhadap database ini dan jika perbandingan menghasilkan pertandingan yang wajar, maka paket yang diizinkan untuk melakukan perjalanan lebih lanjut. Jika tidak, mereka akan dibuang.

5.6 Konfigurasi Firewall

Firewall dapat dikonfigurasi dengan menambahkan satu atau lebih filter berdasarkan beberapa kondisi seperti tersebut di bawah ini:

1.Alamat IP

Dalam kasus apapun jika sebuah alamat IP di luar jaringan dikatakan kurang baik, maka dimungkinkan untuk mengatur filter untuk memblokir semua lalu lintas ke dan dari alamat IP. Misalnya, jika alamat IP cetain ditemukan akan membuat terlalu banyak koneksi ke server, administrator dapat memutuskan untuk memblokir lalu lintas dari IP ini menggunakan firewall.

2.Nama Domain

Karena sulit untuk mengingat alamat IP, itu adalah cara yang lebih mudah dan lebih cerdas untuk mengkonfigurasi firewall dengan menambahkan filter berdasarkan nama domain. Dengan mendirikan domain filter, perusahaan dapat memutuskan untuk memblokir semua akses ke nama domain tertentu, atau mungkin menyediakan akses hanya untuk daftar nama domain yang dipilih.

3.Port / Protokol

Setiap layanan yang berjalan pada server dibuat tersedia ke Internet menggunakan nomor port, satu untuk setiap layananDengan kata sederhana, port bisa dibandingkan dengan pintu virtual dari server melalui layanan yang tersedia. Sebagai contoh, jika server adalah menjalankan Web (HTTP) layanan maka akan biasanya tersedia pada port 80. Untuk memanfaatkan layanan ini, klien ingin terhubung ke server melalui port 80. Demikian pula berbagai layanan seperti Telnet (Port 23), FTP (port 21) dan SMTP (port 25) Layanan dapat berjalan pada server. Jika layanan ini ditujukan untuk publik, mereka biasanya tetap terbuka. Jika tidak, mereka yang diblok menggunakan firewall sehingga mencegah penyusup menggunakan port terbuka untuk membuat sambungan tidak sah. Firewall dapat dikonfigurasi untuk menyaring satu atau lebih kata atau frase spesifik sehingga, baik dan keluar paket yang datang dipindai untuk kata-kata dalam saringan. Misalnya, Anda mungkin mengatur aturan firewall untuk menyaring setiap paket yang berisi istilah ofensif atau frase yang mungkin Anda memutuskan untuk memblokir dari memasuki atau meninggalkan jaringan Anda.

Firewall dapat dibedakan menjadi :

1.Dedicated firewall

Firewall yang berupa perangkat keras khusus yang dirancang untuk kepentingan keamanan jaringan, misalnya Cisco PIX Firewall

2. Server Based-Firewall

Berupa Network Operating System (misalnya Linux, UNIX) yang menjalankan fungsi-fungsi firewall.

3. **Integrated Firewall**

   Fungsi firewall yang ditambahkan pada suatu perangkat jaringan, misalnya router yang menjalan fungsi firewall.

4. **Personal Firewall**

   Berupa firewall yang dipasang pada personal computer (host dalam jaringan), biasanya merupakan bawaan OS, Anti Virus maupun software dari vendor tertentu.

5.7 Kelebihan Firewall

1. Mendeteksi adanya malware atau ancaman dari sebuah situs
2. Menjaga agar user tidak diarahkan ke dalam situs yang berbahaya
3. Memblokir situs – situs tertentu
4. Memperingatkan user ketika akan mendownload apapun yang berasal dari situs yang tidak aman
5. Mencegah pembajakan terhadap komputer user melalui jaringan computer
6. Sangat berguna ketika user melakukan koneksi jaringan pada tempat umum

5.8 Kekurangan Firewall

1. Bukan merupakan antivirus, sehingga tidak pas untuk mencegah masuknya virus
2. Firewall tidak dapat membantu mencegah pencurian data ataupun peretasan yang dilakukan dari dalam
3. Tidak semua malware bisa terdeteksi dengan baik

5.9 IPTABLES

Linux merupakan Network Operating System yang sudah dilengkapi dengan aplikasi firewall. Fungsi-fungsi firewall pada suatu sistem Linux dijalankan oleh Iptables. Pada sistem Linux terdahulu, fungsi firewall dijalankan oleh Ipchains. Selain menjalankan fungsi firewall, Iptables juga dapat menjalankan fungsi NAT. NAT merupakan fungsi yang dijalankan oleh sebuah Internet Gateway untuk menghubungkan jaringan lokal (Private IP Address) dengan jaringan Internet (Public IP Address). Secara default Iptables telah terinstall pada sistem Linux Fedora Core maupun RedHat. Untuk memeriksa apakah Iptables telah terinstall dapat digunakan perintah :

[root@gateway]# rpm –q iptables

iptables-1.3.5-1.2.1

Setiap paket data yang diterima oleh Sistem Linux yang menjalankan fungsi firewall akan diperiksa oleh Iptables. Iptables akan melakukan pemeriksaan dengan memasukkan setiap paket data ke dalam tabel-tabel

Iptables memiliki 3 buah tabel built-in, yaitu :

1. **Mangle**, digunakan untuk manipulasi paket data, misalnya melakukan perubahan TCP Header
2. **Filter**, digunakan untuk melakukan filter paket data yang diterima firewall
3. **Nat**, digunakan untuk melakukan network address translation.

5.10 Chain

Setiap tabel memiliki rule-rule atau aturan-aturan yang disebut chain.

A.Mangle

Mangle pada mikrotik merupakan suatu cara untuk menandai paket data dan koneksi tertentu yang dapat diterapkan pada fitur mikrotik lainnya, sepeti pada routes, pemisahan bandwidth pada queues, NAT dan filter rules. Tanda mangle yang ada pada router mikrotik hanya bisa digunakan pada router itu sendiri. Dan yang perlu diingat bahwa proses pembacaan rule mangle ini dilakukan dari urutan pertama ke bawah.

Ada beberapa jenis penandaan (Mark) yang ada pada Mangle yaitu Packet Mark (Penandaan Paket), Connection Mark (Penandaan Koneksi), dan Routing Mark (Penandaan Routing). Secara default parameter mangle terbagi menjadi beberapa chain, yaitu :

1. Chain Input digunakan untuk menandai trafik yang masuk menuju ke router mikrotik dan hanya bisa memilih In. Interface saja.

2. Chain Output digunakan untuk menandai trafik yang keluar melalui router mikrotik dan hanya bisa memilih Out. Interface saja.

3. Chain Forward digunakan untuk menandai trafik yang keluar masuk melalui router dan dapat memilih In dan Out Interface.

4. Chain Prerouting digunakan untuk menandai trafik yang masuk menuju dan melalui router (trafik download). Chain ini hanya bisa memilih Out. Interface saja.
5. Chain Postrouting digunakan untuk menandai trafik yang keluar dan melalui router (trafik upload) dan hanya bisa memilih In. Interface saja.

Semua chains diperuntukkan untuk TCP Packet Quality of Service sebelum proses routing dijalankan.

B.FILTER RULES

Filter rule biasanya digunakan untuk melakukan kebijakan boleh atau tidaknya sebuah trafik ada dalam jaringan, identik dengan accept atau drop. Pada menu **Firewall → Filter Rules** terdapat 3 macam chain yang tersedia. Chain tersebut antara lain adalah ***Forward***, ***Input***, ***Output***. Adapun fungsi dari masing-masing chain tersebut adalah sebagai berikut:

1.Forward :

Digunakan untuk memproses trafik paket data yang hanya melewati router. Misalnya trafik dari jaringan public ke local atau sebaliknya dari jaringan local ke public, contoh kasus seperti pada saat kita melakukan browsing. Trafik laptop browsing ke internet dapat dimanage oleh firewall dengan menggunakan chain forward.

2.Input

Digunakan untuk memproses trafik paket data yang masuk ke dalam router melalui interface yang ada di router dan memiliki tujuan IP Address berupa ip yang terdapat pada router. Jenis trafik ini bisa berasal dari jaringan public maupun dari jaringan lokal dengan tujuan router itu sendiri. Contoh: Mengakses router menggunakan winbox, webfig, telnet baik dari Public maupun Local.

3.Output

Digunakan untuk memproses trafik paket data yang keluar dari router. Dengan kata lain merupakan kebalikan dari 'Input'. Jadi trafik yang berasal dari dalam router itu sendiri dengan tujuan jaringan Public maupun jaringan Local.Misal dari new terminal winbox, kita ping ke ip google. Maka trafik ini bisa ditangkap dichain output.

C.NAT (Network Address Translation)

Pada menu **Firewall → NAT** terdapat 2 macam opsi chain yang tersedia, yaitu ***dst-nat*** dan ***src-nat***. Dan fungsi dari NAT sendiri adalah untuk melakukan pengubahan *Source Address* maupun *Destination Address*. Kemudian fungsi dari masing-masing chain tersebut adalah sebagai berikut:

1.dstnat

Memiliki fungsi untuk mengubah destination address pada sebuah paket data. Biasa digunakan untuk membuat host dalam jaringan lokal dapat diakses dari luar jaringan (internet) dengan cara NAT akan mengganti alamat IP tujuan paket dengan alamat IP lokal. Jadi kesimpulan fungsi dari chain ini adalah untuk mengubah/mengganti IP Address tujuan pada sebuah paket data.

2.srcnat

Memiliki fungsi untuk mengubah source address dari sebuah paket data. Sebagai contoh kasus fungsi dari chain ini banyak digunakan ketika kita melakukan akses website dari jaringan LAN. Secara aturan untuk IP Address local tidak diperbolehkan untuk masuk ke jaringan WAN, maka diperlukan konfigurasi 'srcnat' ini. Sehingga IP Address lokal akan disembunyikan dan diganti dengan IP Address public yang terpasang pada router.

5.11 Pengertian UFW (UNCOMPLICATED FIREWALL)

UFW adalah kependekan dari *Uncomplicated Firewall* sebuah aplikasi *front-end* dari iptables yang ringan, powerful dan sangat mudah digunakan untuk mengatur *firewall*. UFW ini saya sangat merekomendasikan bagi Anda yang pemula dalam mengatur iptables. Biar bagaimana pun *front-end*dari iptables jadi dengan kata lain ketika Anda mengatur *firewall* dengan UFW sama saja mengatur firewall di iptables.

Kelebihan :

1. Kita dapat mengatur hak ip mana saja yang dapat mengakses layanan pada server yang kita bangun,

2. Dalam konfigurasinya cukup mudah karena hanya menggunakan perintah allow dan denny serta terdapat versi gui-nya mungkin belum ane post untuk versi gui-nya,
3. Untuk pengaturan ulang atau bisa dibilang dalam meresetnya sangat mudah karena tinggal menggunakan perintah "sudo ufw reset",
4. Untuk pengaturan kita bisa melakukan sesuai yang kita inginkan,

Kekurangan :

1. Kita tidak dapat menentukan range ip yang dapat mengakses protokol yang aktif,
2. Sedangkan untuk keamanan sendiri, pastilah ada celah karena menurut saya setiap *firewall* terdapat celah keamanan yang perlu pembenahan,
3. Ketika ini digunakan untuk remote server dari jarak jauh sedangkan kita tidak dapat menentukan range ip untuk konfigurasinya ditambah kita menggunakan akses internet yang ip-nya statik maka kita akan mengalami kesulitan dalam melakukan remote server terutama jika server yang kita remote berada dicukup jauh dari lokasi kita.

5.12 PSAD (Port Scanner Attack Detector)

Psad merupakan suatu software yang pada dasarnya merupaka suatu tools untuk melakukan log analysis dengan menggunakan pesan-pesan log iptables untuk mendeteksi, memberikan alert kepada admin dan (secara opsional) dapat mem-blok suatu port scans dan traffic mencurigakan lainnya (IDS/Intrusion Detection System) . Untuk TCP Scans, psad menganalisis TCP Flags untuk menentukan tipe scan (syn, fin, xmas, dan lain-lain) dan opsi command line yang bersangkutan agar nmap melakukan scan tersebut. Psad memasukkan banyak signature dari Snort IDS untuk mendeteksi probes dari berbagai macam backdoor programs (contoh EvilFTP, SubSeven), DDoS tools (mstream, shaft) dan advanced port scans (FIN, NULL, XMAS) yang dimana mudah dilakukan terhadap sistem dengan menggunakan nmap. Cara kerja psad secara umum adalah psad membaca semua iptables log data secara default yang disimpan pada file /var/log/messages.

Dengan men-parsing (menerjemahkan) firewall log messages, psad menyediakan dengan data yang merepresentasikan paket-paket yang telah di-log (dan mungkin di drop) oleh policy dan rules iptables yang berjalan. Dengan kata lain, psad diberi masukan dengan sebuah data stream murni yang secara eksklusif mengandung paket-paket yang oleh firewall ditentukan tidak cocok untuk masuk ke dalam jaringan. Psad terdiri dari tiga daemons (modul/program yang berjalan di system), yaitu psad,kmsgsd, dan psadwatchd. Berikut merupakan penjelasan lebih detilnya:

1.Psad

Psad bertanggung jawab untuk memproses semua paket yang telah di-log oleh firewall dan mengaplikasikan signature logic dengan tujuan agar dapat menentukan tipe scan/serangan apa yang digunakan kepada sistem atau jaringan.

2.Kmsgsd

Kmsgsd bertanggung jawab untuk membaca semua pesan yang telah ditulis pada /var/lib/psad/psadfifo yang bernama pipe dan menulis pesan apapun yang cocok terhadap suatu regular expression (atau string) ke /var/log/psad/fwdata. Kmsgsd hanya digunakan jika variabel ENABLE_SYSLOG_FILE disabled pada psad.conf .

3.Psadwatchd

Psadwatchd merupakan sebuah software watchdog (pengawas) yang akan menrestart kedua daemon yang lain ketika daemon tersebut mengalami kegagalan/mati karena suatu alasan. Psad pertama kali dikembangkan pada akhir tahun 1999 yang dimana pada saat itu masih bagian dari software project Bastille Linux, yang dimana dimulai ketika tim pengembangan memutuskan bahwa Bastille seharusnya menawarkan sebuah komponen NIDS yang ringan. Pada waktu yang sama, Peter Watkins juga sedangkan mengembangkan script firewall yang bagus yang masih dibundel dengan Bastille sampai sekarang, sehingga merupakan hal yang alami untuk melakukan langkah selanjutnya untuk mngembangkan sebuah tools IDS berdasarkan informasi yang disediakan dalam log iptables. Pada tahun 2001, Michael Rash memisahkan proyek Bastille-NIDS menjadi proyeknya sendiri yang dimana dapat berjalan dengan

sendirinya tanpa dibutuhkan Bastille harus diinstal pada sistem, dan proyek tersebut bernama Port Attack Scanner Detector (Psad)

5.13 Intrusion Detection System (IDS)

Intrusion Detection System (IDS) merupakan suatu sistem keamanan yang bekerja dengan cara melakukan pengawasan terhadap paket yang ada pada jaringan serta pengawasan kegiatan-kegiatan paket yang mencurigakan dalam jaringan. Jika ditemukan paket atau kegiatan yang mencurigakan dalam jaringan, IDS secara umum akan memberikan peringatan kepada sistem atau administrator jaringan. Tetapi secara khusus selain memberi peringatan kepada sistem atau admin jaringan, secara native IDS dapat juga reaktif terhadap paket atau kegiatan mencurigakan tersebut. Salah satu caranya dengan melakukan pemblokiran user atau alamat IP sumber dari paket mencurigakan tersebut. IDS sendiri terbagi menjadi beberapa macam, yaitu:

1.Active and Passive IDS

Active IDS (atau lebih dikenal dengan Intrusion Prevention System/IPS), merupakan sebuah sistem yang dikonfigurasi/diatur untuk memblok suatu serangan yang sedang berlangsung tanpa "ikut campur" pengguna/user. Dengan kata lain, IPS secara otomatis memblok serangan tersebut tanpa perlu admin turun tangan. Sedangkan, Passive IDS merupakan sebuah sistem yang dikonfigurasi hanya untuk memonitor/memantau dan menganalisa aktivitas trafik jaringan dan meng-alert operator ketika ada celah potensial dan serangan. Passive IDS tidak dapat secara otomatis melindungi jaringan dengan sendirinya.

2.Network-based and Host-based IDS

Network-based IDS terdiri dari sebuah peralatan jaringan (atau sensor) dengan NIC-nya yang beroperasi dalam mode promiscuous (mode mendengar) dan sebuah management interface yang terpisah. Host-based IDS membutuhkan program-program kecil (atau biasa disebut agents) untuk diinstal pada sistem individu untuk dimonitor. Agents tersebut memonitor sistem operasi dan menulis data untuk mencatat (log) file dan/atau men-trigger alarms.

3.Knowledged-based and Behavior-based

Knowledge-based (atau sering disebut Signature-based) merupakan sebuah IDS yang memiliki basis data yang berisi profil-profil serangan sebelmnya dan celah sistem yang diketahui untuk mengidentifikasi usaha penyusupan. Knowledge-based merupakan IDS yang lebih umum digunakan dibandingkan Behavior-based. Behavior-based (atau sering disebut Anomaly-based) merupakan IDS yang dimana mendeteksi suatu penyusupan/serangan dengan cara membandingkan trafik yang sedang discan dengan trafik dalam keadaan normal. Penyimpangan dari keadaan trafik normal ini yang dianggap sebagai sebuah serangan.

BAB 6 BANDWIDTH MANAGEMENT

6.1 Pengenalan MikroTik

MikroTik RouterOS™ merupakan sistem operasi yang diperuntukkan sebagai network router.Disesain untuk memberikan kemudahan bagi penggunannya. Administrasinya bias dilakukan melalui Windows application (WinBox), webbrowser serta via remote Shell (telnet dan SSH). Selain itu instalasi dapat dilakukan pada standard computer PC. PC yang akan dijadikan router mikrotikpun tidak memerlukan resource yang cukup besar untuk penggunaan standard, misalnya hanya sebagai gateway. Untuk keperluan beban yang besar (network yang kompleks, routing yang rumit dll) disarankan untuk mempertimbangkan pemilihan resource PC yang memadai. Fasilitas pada mikrotik antara lain sebagai berikut:

1.Protokoll routing RIP, OSPF, BGP.

2.Statefull firewall

3.HotSpot for Plug-and-Play access

4.Remote Winbox GUI admin

6.2 Sejarah MikroTik

Mikrotik adalah perusahaan kecil berkantor pusat di Latvia, bersebelahan dengan Rusia, pembentukannya diprakarsai oleh John Trully dan Arnis Riekstins. John Trully yang berkebangsaan Amerika Serikat berimigrasi ke Latvia dan berjumpa Arnis yang sarjana Fisika dan Mekanika di sekitar tahun 1995. Tahun 1996 John dan Arnis mulai me-routing dunia (visi Mikrotik adalah me-routing seluruh dunia). Mulai dengan sistem Linux dan MS DOS yang dikombinasikan dengan teknologi Wireless LAN (WLAN) Aeronet berkecepatan 2Mbps di Moldova, tetangga Latvia, baru kemudian melayani lima pelanggannya di Latvia, karena ambisi mereka adalah membuat satu peranti lunak router yang handal dan disebarkan ke seluruh dunia.Ini agak kontradiksi dengan informasi yang ada di web Mikrotik, bahwa mereka mempunyai 600 titik (pelanggan) wireless dan terbesar di dunia. Prinsip dasar mereka bukan membuat Wireless ISP (WISP), tapi membuat program router yang handal dan dapat dijalankan di seluruh dunia. Latvia hanya merupakan “tempat eksperimen” John dan Arnis, karena saat ini mereka sudah membantu negara-negara lain termasuk Srilanka yang melayani sekitar

empat ratusan pelanggannya. Linux yang mereka gunakan pertama kali adalah Kernel 2.2 yang dikembangkan secara bersama-sama dengan bantuan 5 - 15 orang staf R&D Mikrotik yang sekarang menguasai dunia routing di negara-negara berkembang. Selain staf di lingkungan Mikrotik, menurut Arnis, mereka merekrut juga tenaga-tenaga lepas dan pihak ketiga yang dengan intensif mengembangkan Mikrotik secara maraton.

6.3 Jenis – Jenis MikroTik

Berdasarkan bentuk hardware yang di gunakan, mikrotik dapat digolongkan dalam dua jenis. Dua jenis tersebut adalah :

1.Mikrotik RouterOS™

Adalah versi MikroTik dalam bentuk perangkat lunak yang dapat diinstal pada Personal Computer (PC) melalui CD. File yang dibutuhkan dapat diunduh dalam bentuk file image MikroTik RouterOS dari website resmi MikroTik, www.mikrotik.com. Namun, file image ini merupakan versi trial MikroTik yang hanya dapat dalam waktu 24 jam saja. Untuk dapat menggunakannya secara full time, harus membeli lisensi key dengan catatan satu lisensi hanya untuk satu harddisk.

2.Build in Hardware Mikrotik

Merupakan MikroTik dalam bentuk perangkat keras yang khusus dikemas dalam board router, atau sering disebut routerBoard, yang di dalamnya sudah terinstal sistem operasi MikroTik RouterOS. Untuk versi ini, lisensi sudah termasuk dalam board MkroTik. Pada Router board ini penguna langsung dapat memakainya, tanpa harus melakukan insatalasi sistem operasi. Router Board ini dikemas dalam beberapa bentuk dan kelengkapannya sendiri sendiri. Ada yang difungsikan sebagai Indoor Router, Outdoor Router maupun ada yang dilengkapi dengan wireless router.

6.4 Level RouterOS dan Kemampuannya

Mikrotik RouterOS hadir dalam berbagai level. Tiap level memiliki kemampuannya masing-masing, mulai dari level 3, hingga level 6. Secara singkat, level 3 digunakan untuk router berinterface ethernet, level 4 untuk wireless client atau serial interface, level 5 untuk wireless AP, dan level 6 tidak mempunyai limitasi apapun.

Untuk aplikasi hotspot, bisa digunakan level 4 (200 user), level 5 (500 user) dan level 6 (unlimited user).

Detail perbedaan masing-masing level dapat dilihat pada tabel di bawah ini:

Level number	1 (DEMO)	3 (ISP)	4 (WISP)	5 (WISPAP)	6 (Controller)
Wireless Client and Bridge	-	-	yes	yes	yes
Wireless AP	-	-	-	yes	yes
Synchronous interfaces	-	-	yes	yes	yes
EoIP tunnels	1	unlimited	unlimited	unlimited	Unlimited
PPPoE tunnels	1	200	200	500	Unlimited
PPTP tunnels	1	200	200	unlimited	Unlimited
L2TP tunnels	1	200	200	unlimited	Unlimited
VLAN interfaces	1	unlimited	unlimited	unlimited	Unlimited
P2P firewall rules	1	unlimited	unlimited	unlimited	Unlimited
NAT rules	1	unlimited	unlimited	unlimited	Unlimited
HotSpot active users	1	1	200	500	unlimited
RADIUS client	-	yes	yes	yes	Yes
Queues	1	unlimited	unlimited	unlimited	Unlimited
Web proxy	-	yes	yes	yes	Yes
RIP, OSPF, BGP protocols	-	yes	yes	yes	Yes
Upgrade	configuration erased on upgrade	yes	yes	yes	Yes

Tabel 6. 1 PerbedaanLevel RouterOS

6.5 Sistem Level Lisensi Mikrotik

Mikrotik bukanlah perangkat lunak yang gratis jika anda ingin memanfaatkannya secara penuh, dibutuhkan lisensi dari MikroTikls untuk dapat menggunakanya alias berbayar. Mikrotik dikenal dengan istilah Level pada lisensinya. Tersedia mulai dari Level 0 kemudian 1, 3 hingga 6, untuk Level 1 adalah versi Demo Mikrotik dapat digunakan secara gratis dengan fungsi-fungsi yang sangat terbatas. Tentunya setiap level memilki kemampuan yang berbeda-beda sesuai dengan harganya, Level 6 adalah level tertinggi dengan fungsi yang paling lengkap. Secara singkat dapat digambarkan jelaskan sebagai berikut:

- Level 0 (gratis): tidak membutuhkan lisensi untuk menggunakannya dan penggunaan fitur hanya dibatasi selama 24 jam setelah instalasi dilakukan.
- Level 1 (demo): pada level ini kamu dapat menggunakannya sbg fungsi routing standar saja dengan 1 pengaturan serta tidak memiliki limitasi waktu untuk menggunakannya.

- Level 3: sudah mencakup level 1 ditambah dengan kemampuan untuk menajemen segala perangkat keras yang berbasiskan Kartu Jaringan atau Ethernet dan pengelolan perangkat wireless tipe klien.
- Level 4: sudah mencakup level 1 dan 3 ditambah dengan kemampuan untuk mengelola perangkat wireless tipe akses poin.
- Level 5: mencakup level 1, 3 dan 4 ditambah dengan kemampuan mengelola jumlah pengguna hotspot yang lebih banyak.
- Level 6: mencakup semua level dan tidak memiliki limitasi apapun.

6.6 Istilah – istilah dalam MikroTik RouterOS

Berikut beberapa istilah-istilah yang berhubungan dengan mikrotik :

1.System : Packet yang wajib diinstall karena merupakan inti dari system mikrotik

2.PPP : Untuk membuat Point to Point Protocol Server

3.dhcp : Packet yang dibutuhkan apabila ingin membuat dhcp-server atau untuk mendapatkan dynamic ip address

4.Advanced tool : Tools tambahan seperti ip-scan, bandwidth test dan lainnya.

5.arlan : Packet untuk konfigurasi chipset wireless aironet arlan

6.gps : Packet untuk support GPS Device

7.hotspot : Packet untuk membuat hotspot gateway, seperti authentication , traffic quota dan SSL

8.hotspot –fix : Tambahan packet hotspot

9.isdn : Packet untuk isdn server dan isdn client membutuhkan packet PPP

10.lcd : Packet untuk customize port lcd

11. ntp : Packet untuk ntp server dan ntp client

12.radiolan : Driver for legacy RadioLAN cards

13.Routerboard : Routerboard spesifikasi BIOS

14.Routing : Packet untuk routing OSPF, BGP dan static

15.Routing-test : Packet tambahan (optional)

16.security : Packet untuk mendukung ssh dan ip sec

17.synchronous : Untuk synchronous dengan device lain

18.telephony : Packet for VOIP (H.323)

19.ups : packet for ups monitor seperti alarm

20.user-manager : Packet tool user manager untuk radius server

21.web-proxy : packet untuk setting proxy server

22.web-proxy test : optional

23.wireless : Packet untuk dukung cisco aironet cards

6.7 Fungsi Menu Pada Winbox Mikrotik

Memahami Menu-Menu yang ada di Winbox (Mikrotik), Dimana menu-menu itu terdiri dari :

1.Interfaces

Menu interface merupakan gerbang trafik keluar atau masuk ke mikrotik. Secara default mikrotik hanya mengenali interface yang secar fisik memang ada. Kita dapat merubah nama interface tersebut dengan tujuan untuk memudahkan dalam mengindetifikasi fungsi.

a.Bridge

Dapat memisahkan suatu paket data yang harus dikirimkan pada jaringannya sendiri atau pada jaringan yang lain, apabila kedua jaringan terhubung. Bridge dapat berfungsi sebagai router pada jaringan lebih luas. Hal tersebut dinamakan dengan istilah brouter (bridge-router). Bridge juga dapat meng-copy frame data dari suatu jaringan yang lain. asalkan jaringan teresbut masih terhubung.

b.PPP

Memeriksa apakah kondisi line atau saluran telepon yang sedang beroperasi bekerja dengan baik. Point to Point Protocol juga memeriksa password dan setelah melalui semua pemeriksaan awal kemudian menetapkan koneksi dengan ISP dan melakukan permintaan alamat IP.

c.Switch

Membuat mikrotik menjadi switch

d.Mesh

Digunakan untuk routing dalam jaringan wireless mesh. Penambahan protokol MME pada Mikrotik didasarkan pada metode B.A.T.M.A.N (Better Approach To Mobile Ad-hoc Networking).

e.IP

Pada Menu IP ada sub menu lagi, yaitu :

1)ARP

Untuk memonitor list IP yang sedang berjalan

2)Accounting

Sama seperti ARP

3)Addresses

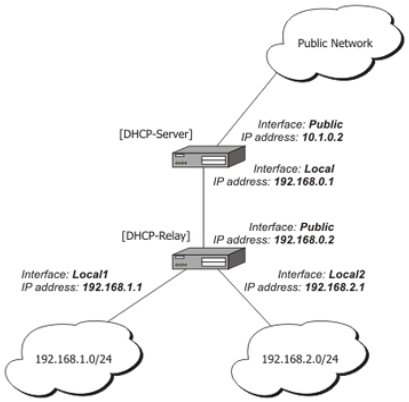
- Menunjukkan IP Addres Ethernet.
- Membuat /Menyeting IP Ethernet sesuai kebutuhan. Dimana Ethernet pada mikrotik ada beberapa port.
- Biasanya Ethernet 1 Untuk IP Publik dari ISP(Penyedia Internet), Port 2-5 bisa untuk LAN atau yang lainnya, menyesuaikan kebutuhan.

4)DHCP Client

Menjadikan Router (Mikrotik) DHCP Client, yaitu apabila kita berlangganan internet yang memberikan IP Public DHCP. Dengan DHCP Client, kita akan otomatis mendapatkan IP Publik, DNS dan Gateway.

5)DHCP Relay

Berfungsi untuk menyebarkan jaringan dengan jaringan baru, sebagai pemahaman bisa kita lihat gambar dibawah ini :



Tabel 6. 2 DHCP Relay

6)DHCP Server

Tempat menyeting DHCP Server. Jika kita minginginkan tiap computer dalam jaringan mendapatkan IP, DNS dan Gateway secara otomatis.

7)DNS

Tempat memasukkan DNS yang diperoleh dari ISP(Penyedia Internet).

2.Firewall

Kata firewall mengandung kata kunci wall yang berarti dinding. Fungsi dinding adalah melindungi segala sesuatu di dalam dinding tersebut. Nah firewall pun berfungsi sama, yaitu melindungi komputer atau jaringan dari akses komputer lain yang tidak memiliki hak untuk mengakses komputer atau jaringan Anda.

Adapun fungsi Firewall di dalam jaringan adalah sebagai berikut :

a.Packet Filtering : memeriksa header dari paket TCP/IP (tergantung arsitektur jaringannya, dalam contoh ini adalah TCP IP) dan memutuskan apakah data ini memiliki akses ke jaringan.

b.Network Address Translation (NAT) : biasanya sebuah jaringan memiliki sebuah IP public dan di dalam jaringan sendiri memiliki IP tersendiri. Firewall berfungsi untuk meneruskan paket data dari luar jaringan ke dalam jaringan dengan benar sesuai IP komputer lokal.

c.Application Proxy : firewall bisa mendeteksi protocol aplikasi tertentu yang lebih spesifik.

d.Traffic management : mencatat dan memantau trafik jaringan

e.Pada menu firewal ini kita bisa menutup akses dari web-web tertentu yang tidak diperbolehkan diakses

f.Pada menu ini juga bisa mengatur waktu akses user, pembatasan waktu user berinternet.

3.Hotspot

a.Menu untuk Pembangunan hotspot

b.Pengaturan user login hotspot

c.Pengaturan waktu akses user

d.Pengaturan pembuatan paket internet untuk voucer internet

e.Digunakan untuk melakukan *authentication*, *authorization* dan *accounting* pengguna yang melakukan *access* jaringan melalui gerbang *hotspot*. Pengguna *hotspot* sebelum melakukan *access* jaringan perlu melakukan *authentication* melalui *web browser* baik dengan protokol http maupun https(*secure http*).

f.Menu hotspot digunakan untuk membuat hotspot Wizard, dimana kita bisa menentukan port dari mikrotik untuk output HOTSPOT. Kita tinggal colokin Acces Point/Werreles maka kita sudah bisa membangun hotspot dengan mikrotik.

g.Untuk seting IP di tentukan dari Interface dan IP, kemudian untuk filter akses hotspotnya, kita bisa menggunakan Firewal->>Filter

4.IPsec

Tempat mensecan IP Address yang ada dijaringan, menghindari dari pemakaian IP oleh Orang yang tak bertanggung jawab.

5.Neighbors

Untuk mendeteksi jumlah perangkat yang menggunakan router os. Bukan hanya mikrotik, produk UBNT & Cisco pun terdeteksi di tools neighbors.

6.Packing

Digunakan untuk menandai setiap paket yang melewati router

7.Pool

Untuk membatasi range / deretan IP yang akan didistribusikan secara otomatis oleh sistem DHCP yang kita aktifkan

8.Reutes

Untuk setting sumber internet dan lan

9.SNMP

Untuk monitoring device jaringan, bandwith dan troughput pun bisa di lihat dengan grafik (snmp client tertentu). Ya minimalnya hal standar yang dilakukan untuk monitoring perangkat jaringan kita

10.Services

Untuk memudahkan user dalam mengakses dan memanage router dan menjalankan semua fitur yang terdapat di dalamnya.

11.Socks

Untuk sebuah aplikasi client server dan biasanya sering disebut sebut didalam proxy server karena socks itu adalah sebuah protokoler internet yang memfasilitasi sebuah routing network antara client dengan server via proxy server.

12.TFTP

Untuk transfer file antar komputer yang sama maupun berbeda jaringan

13.Traffic Flow

Merupakan sebuah sistem yang menampilkan informasi statistik akan besar atau banyaknya paket-paket yang melewati sebuah router

14.UPnP

Untuk mengaktifkan port forwarding konfigurasi dinamis di mana layanan Anda menjalankan dapat meminta router menggunakan UPnP untuk maju beberapa port untuk itu.

15.Web Proxy

Mikrotik web proxy dalam saat yang bersamaan dapat difungsikan sebagai *proxy* HTTP normal maupun transparant.

6.8 Instalasi MikroTik RouterOS pada PC

Instalasi Mikrotik ada beberapa cara :

1.Instalasi melalui NetInstall via jaringan

2.Instalasi melalui Floppy disk

3.Instalasi melalui CD-ROM.

Kali ini akan membahas instalasi melalui CD-ROM. Untuk mendapatkan ISOnya dapat didownload di http://www.mikrotik.co.id/download.php.

A.Persiapan Instalasi MikroTik RouterOS

Tahapan instalasi ini dilakukan hanya pada PC yang dijadikan Mikrotik RouterOS.

1.Persiapan yang diperlukan sebelum tahapan instalasi yaitu:

2.Untuk PC Router Siapkan PC, minimal Pentium I, RAM 64, HD 500M atau pake flash memory 64 - Sebagai Web proxy, Siapkan PC, minimal Pentium III 450Mhz, RAM 256 Mb, HD 20 Gb.

3.Siapkan minimal 2 ethernet card, 1 ke arah luar/Internet dan 1 lagi ke Network local.

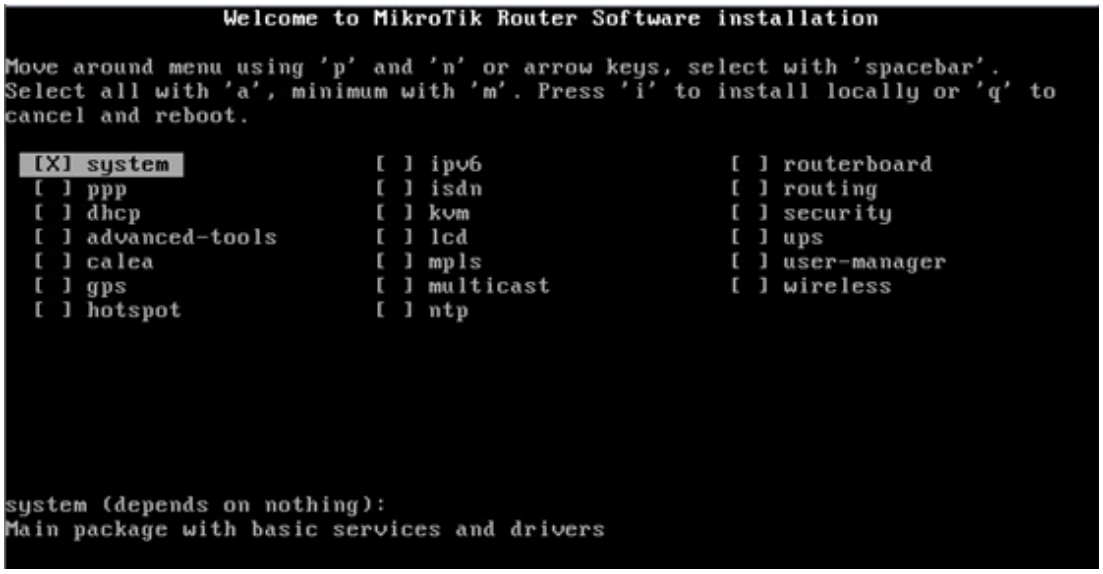
4.Burn Source CD Mikrotik OS masukan ke CDROM.

5.Versi mikrotik yang digunakan adalah Mikrotik RouterOS versi 5.18 atau lebih.

B.Tahap – Tahap Instalasi MikroTik RouterOS

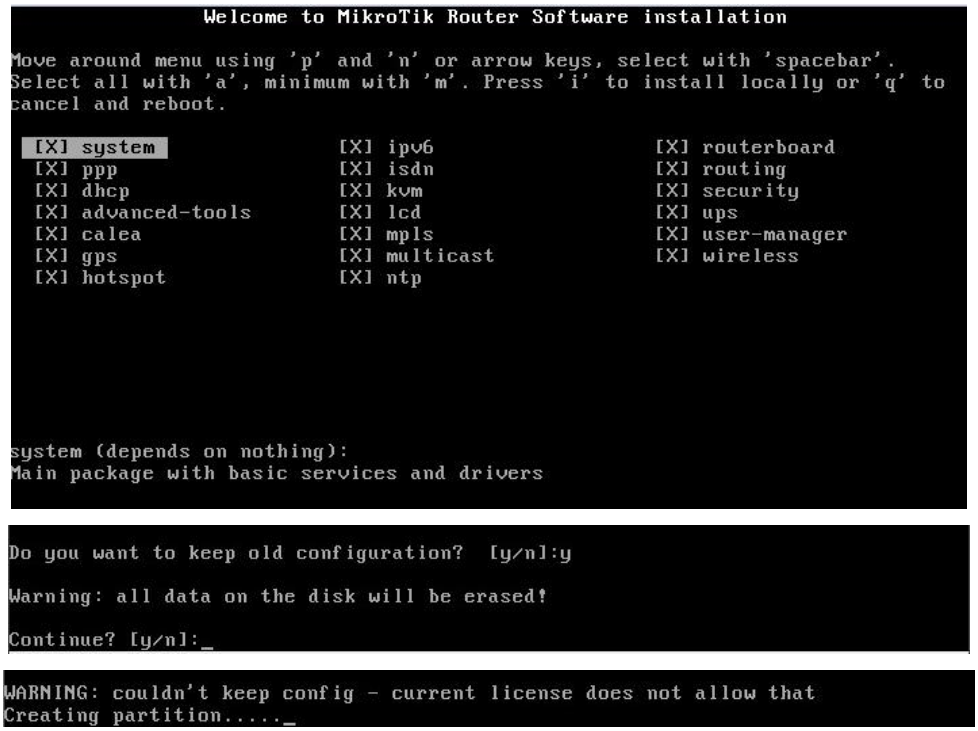
Setelah semua persiapan yang diperlukan sudah disediakan, sekarang saatnya dimulai tahapan instalasi, yaitu:

1.Setting bios agar boot pertama kali dijalankan dari CD-Rom. Kemudian akan muncul tampilan awal pada saat proses instalasi.



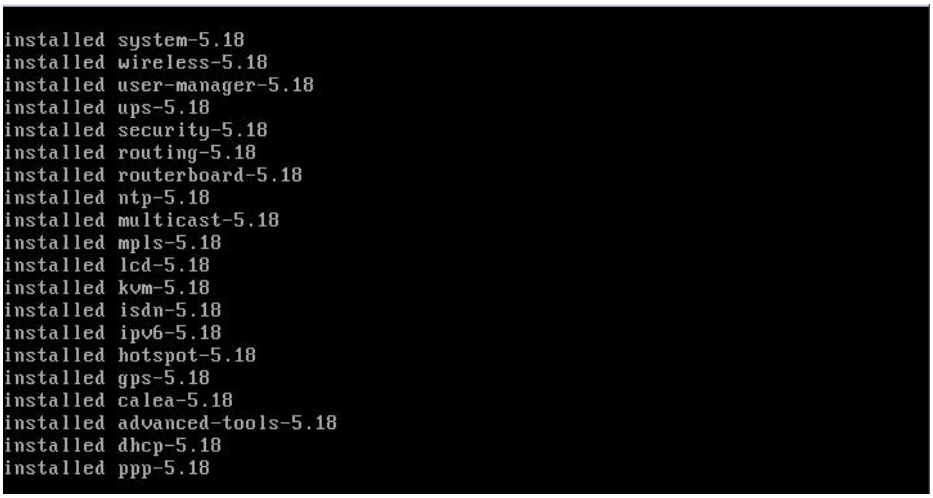
Gambar 6. 1 Setting BIOS

2.Install semua package dengan menekan tombol a kemudian tekan i untuk memulai proses instalasi. Kemudian akan muncul peringatan bahwa data dalam harddisk atau konfigurasi lama akan terhapus bila melakukan proses instalasi. Tekan tombol n, karena dalam hal ini kita akan membuat konfigurasi baru router.



Gambar 6. 2 Menginstall Semua Package

3.Proses instalasi berlangsung, dan user tidak perlu membuat partisi harddisk karena secara otomatis akan membuat partisi sendiri.



Gambar 6. 3 Proses Instalasi

4.Setelah proses installasi selesai restart system, tekan enter

Gambar 6. 4 Menekan Tombol ENTER

5.Jika sudah selesai, akan diminta untuk login kedalam Mikrotiknya. Sebelum itu muncul perintah /system check-disk, lalu tekan tombol y.

Gambar 6. 5 /System check-disk

6.Masuk ke halaman login mikrotik ketikkan username : admin, dan password : (kosongkan) lalu tekan enter.

Gambar 6. 6 Tampilan Mikrotik

6.9 Penggunaan MikroTik RouterOS pada PC atau Routerboard

Perintah mikrotik sebenarnya hampir sama dengan perintah yang ada dilinux, sebab pada dasarnya mikrotik ini merupakan kernel Linux, hasil pengolahan kembali Linux dari Distribusi Debian. Pemakaian perintah shellnya sama, seperti penghematan perintah, cukup menggunakan tombol TAB di keyboard maka perintah yang panjang, tidak perlu lagi diketikkan, hanya ketikkan awal nama perintahnya, nanti secara otomatis Shell akan menampilkan sendiri perintah yang berkenaan. Misalnya perintah IP ADDRESS di mikrotik. Cukup hanya mengetikkan IP ADD spasi tekan tombol

TAB, maka otomatis shell akan mengenali dan menterjemahkan sebagai perintah IP ADDRESS.

6.10 Akses MikroTik

Ada 4 cara pengaksesan Mikrotik Router, antara lain :

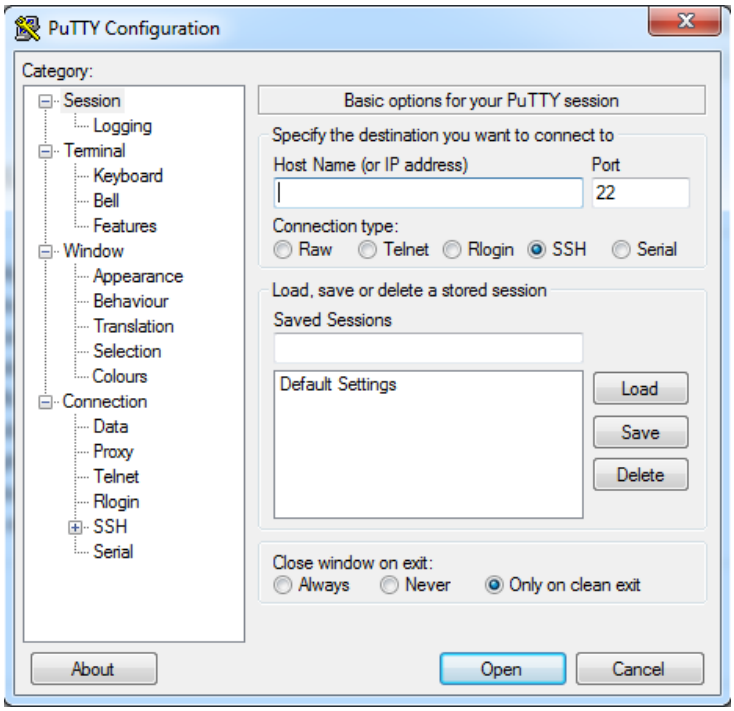
1.Via Console/Command Mikrotik

Jenis router board maupun PC bisa kita akses langsung via console/shell maupun remote akses menggunakan PUTTY (www.putty.nl).

Tips Command:

a.Manfaatkan auto compile (mirip bash auto complete di linux), yaitu dengan menekan tombol TAB dikeyboard untuk mengetahui/melengkapi daftar perintah selanjutnya. Contoh:

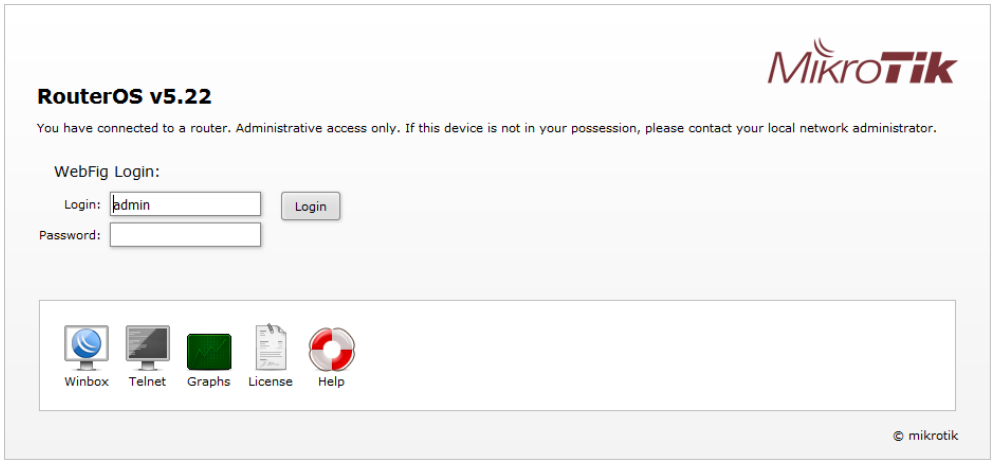
Cukup ketikkan Ip Fir >>> lalu tekan TAB >>> maka otomatis shell akan melengkapi menjadi Ip Firewall. Lalu ketik ".." (titik dua) untuk kembali ke sub menu diatasnya, dan ketik "/" untuk kembali ke root menu.



Gambar 6. 7 Putty

2.Via Web Browser

Mikrotik bisa juga diakses via web/port 80 pada browser. Contoh: ketik di browser IP mikrotik kita: 192.168.1.1.

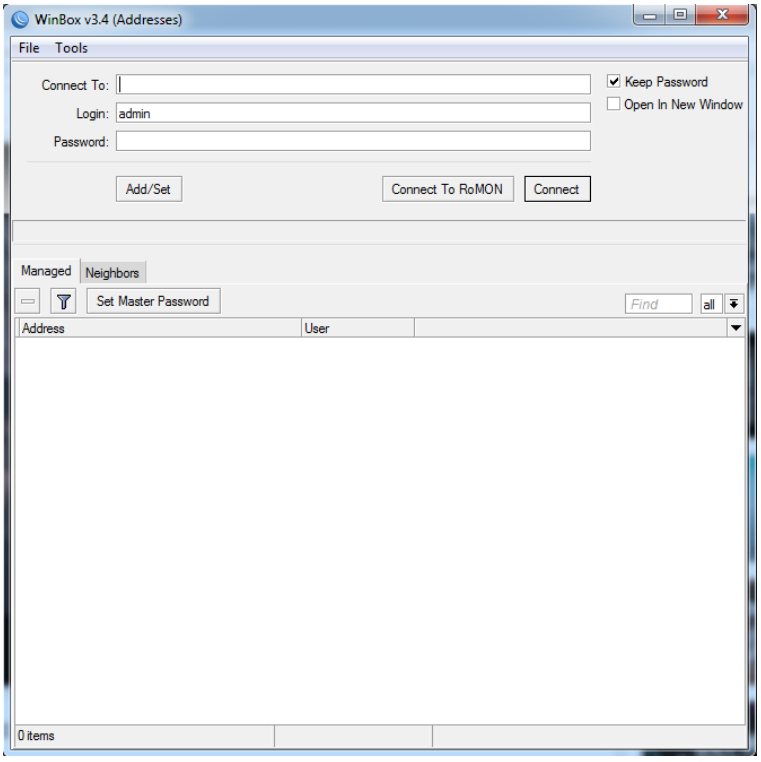


Gambar 6. 8 Mikrotik Via Web

3.Via Winbox

Mikrotik bisa juga diakses/remote menggunakan tool winbox (utility sederhana di windows yang sangat praktis dan cukup mudah digunakan).

Tampilan awal menampilkan winbox seperti dibawah ini:



Gambar 6. 9 Via WinBox

4.Via Telnet

Kita dapat me-remote Mikrotik menggunakan telnet melalui program aplikasi command prompt (cmd) yang ada pada windows. Namun, pengunaan telnet tidak dianjurkan dalam jaringan karena masalah keamanannya.

Contoh: c:\>telnet 192.168.2.1

6.11 Pengertian Bandwidth

Bandwidth adalah luas atau lebar cakupan frekuensi yang digunakan oleh sinyal dalam medium transmisi. Dalam kerangka ini, Bandwidth dapat diartikan sebagai perbedaan antara komponen sinyal frekuensi tinggi dan sinyal frekuensi rendah. frekuensi sinyal diukur dalam satuan Hertz. sinyal suara tipikal mempunyai Bandwidth sekitar 3 kHz, analog TV broadcast (TV) mempunyai Bandwidth sekitar 6 MHz.

Bandwidth (lebarpita) dalam ilmu komputer adalah suatu penghitungan konsumsi data yang tersedia pada suatu telekomunikasi. Dihitung dalam satuan bits per seconds (bit per detik). Perhatikan bahwa bandwidth yang tertera komunikasi nirkabel, modem transmisi data, komunikasi digital, elektronik, dll, adalah bandwidth yang mengacu pada sinyal analog yang diukur dalam satuan hertz (makna asli dari istilah tersebut) yang lebih tepat ditulis bitrate daripada bits per second.

Dalam dunia web hosting, bandwidth capacity (kapasitas lebarpita) diartikan sebagai nilai maksimum besaran transfer data (tulisan, gambar, video, suara, dan lainnya) yang terjadi antara server hosting dengan komputer klien dalam suatu periode tertentu. Contohnya 5 GB per bulan, yang artinya besaran maksimal transfer data yang bisa dilakukan oleh seluruh klien adalah 5 GB, jika bandwidth habis maka website tidak dapat dibuka sampai dengan bulan baru. Semakin banyak fitur di dalam website seperti gambar, video, suara, dan lainnya, maka semakin banyak bandwidth yang akan terpakai.

6.12 Manfaat dan Tujuan Manajemen Bandwidth

Manajemen bandwidth adalah proses memberikan alokasi saluran yang digunakan untuk proses upload maupun download agar qualitas layanan yang dijalankan berjalan dengan baik Ada beberapa metode yang digunakan untuk mengatur trafik, diantaranya adalah:

1.Discard Packet, yaitu membuang trafik yang telah melewati batas parameter tertentu yang telah ditetapkan.

2.TCP rate control, yaitu mengatur transmisi data berdasarkan pengaturan besarnya ukuran window TCP. Sesuai dengan namanya maka metode ini hanya berjalan untuk aplikasi berbasiskan protokol TCP.

3.Queueing, mengklasifikasikan paket, selanjutnya menempatkan paket pada antriannya dan kemudian dilakukan penjadwalan pengiriman. Pada metode ini terdapat banyak algoritma yang dapat digunakan untuk mengatur trafik misalnya RED, CBQ, HTB,PCQ dll.

Manfaat yang dari manajemen bandwidth adalah :

1.Semua komputer dapat menggunakan internet dengan lancar dan stabilwalaupun semua unit komputer menggunakan internet dalam waktu yangbersamaan.

2.Semua bagian unit komputer mendapatkan bandwidth sesuai dengan kebutuhan koneksi internet.

3.Memaksimalkan Bandwidth di semua unit komputer.

4.Membantu admin dalam mengontrol bandwidth.

6.13 Manajemen Bandwidth pada MikroTik

Dengan MikroTik ini kita bisa mengatur manajemen bandwidth di jaringan local kita. Dengan kata lain digunakan untuk bandwidth limiter (queue), yaitu untuk mengontrol mekanisme alokasi data rate. Secara umum terdapat 2 jenis manajemen bandwidth pada MikroTik, yaitu queue tree dan queue simple.

6.14 Manajemen Bandwidth Menggunakan Simple Queue

Manajemen bandwidth dengan metode Queue Simple umumnya ditujukan untuk melimit bandwidth per IP Address. Contohnya anda langganan internet Speedy 1Mbps, anda mempunyai 10 PC, maka kecepatan 1Mbps itu akan anda bagi dengan 10 PC

1 Mbps = 1024 Kbps

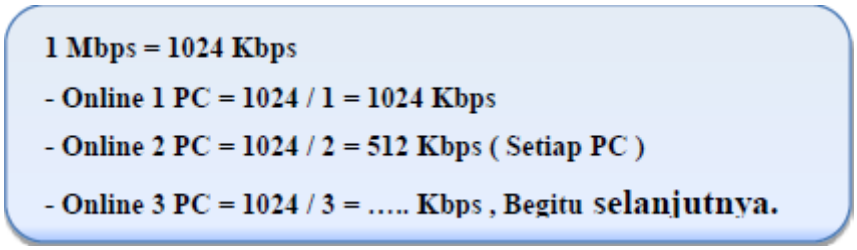
1024 Kbps : 10 PC = 102,4 Kbps, Dirata -ratakan menjadi 102 Kbps

Gambar 6. 10 Manajemen Bandwidth

Dari perhitungan diatas menunjuwkan bahwa kecepatan maksimal untuk setiap PC adalah 102 Kbits/second. Jika dari ke 10 PC tersebut, yang online hanya 1 PC saja, maka bandwidth yang didapat adalah tetap 102 Kbps. Dalam arti sisa bandwidth yang tidak digunakan tidak terpakai.

6.15 Manajemen Bandwidth Menggunakan Queue Tree

Manajemen bandwidth dengan metode Queue Tree umumnya ditujukan untuk melimit bandwidth secara keseluruhan (bukan per IP Address tetapi keseluruhan IP Address). Contohnya anda langganan internet Speedy 1Mbps, anda mempunyai 10 PC. Maka kecepatan 1Mbps itu akan anda bagi rata ke setiap PC, dengan catatan jika dari 10 PC tersebut yang online hanya 1 PC saja, maka bandwidth yang didapat adalah 1Mbps. Dalam arti bandwidth yang tidak terpakai dapat digunakan.



Gambar 6. 11 Manajemen Bandwidth Dengan Queue Tree

6.16 Manajemen Bandwidth Berdasarkan Jenis File dan Waktu Akses

Selain kedua konfigurasi diatas, MikroTik juga dapat melakukan pembatasan bandwith berdasarkan jenis file maupun waktu akses. Disini akan dibahas manajemen berdasarkan jenis file secara sederhana. Dimana setiap file untuk ekstensi tertemtu akan dibatasi kecepatan aksesnya.

A.Cara kerja Layer 7 Protocol

Cara kerja L7 adalah mencocokkan (*mathcer*) 10 paket koneksi pertama atau 2KB koneksi pertama dan mencari pola/pattern data yang sesuai dengan yang tersedia. Jika pola ini tidak ditemukan dalam data yang tersedia, matcher tidak memeriksa lebih lanjut. Dan akan dianggap *unknown connections*. Anda harus mempertimbangkan bahwa banyak koneksi secara signifikan akan meningkatkan penggunaan memori pada RB maupun PC Router anda. Untuk menghindari hal tersebut, maka tambahkan *regular firewall matchers* (*pattern*) untuk mengurangi jumlah data yang dikirimkan ke layer-7 filter.

Layer 7 matcher harus melihat kedua arah lalu lintas (masuk dan keluar). Untuk memenuhi persyaratan ini rule L7 harus diatur dalam *chain Forward*. Jika rule pada *chain input/prerouting*, maka aturan yang sama juga harus diatur dalam *chain output/postrouting*, jika tidak, maka data mungkin dianggap tidak lengkap sehingga pola/pattern dianggap tidak benar/cocok.

B.Arti Perintah Regexp

1. Karakter meta | (Garis Vertikal) Karakter | : menjadikan karakter meta text sebagai pilihan pada pola untuk di cocokan dengan sumber.
2. Karakter [dan] kurung siku buka dan tutup : pada prinsipnya tanda kurung siku buka dan tutup sama dengan karakter | yaitu memberikan pilihan.
3. Karakter titik (.) : untuk mewakili sebuah karakter tunggal apapun
4. Karakter + (tambah)meta + : untuk mewakili setidaknya satu dari sekelompok karakter dari kiri tanda + tersebut
5. Karakter * (bintang) : Fungsinya sama dengan tanda +, bedanya pada tanda asterik ini karakter di sebelah kiri boleh ada atau tidak
6. Karakter ^ : hanya berarti narasi jika di gunakan di awal karakter yang ada dalam kurung siku, sedangkan jika ada di luar kurung siku akan berarti “di awal”
7. Karakter { dan } (tutup dan buka kurawal) : untuk menangani pengulangan karakter di sebelah kiri tanda,

6.17 Web Filtering

Situs *web* (*web*site) atau sering disingkat dengan istilah situs adalah sejumlah halaman *web* yang memiliki topik saling terkait, terkadang disertai dengan berkas-berkas gambar, video, atau jenis-jenis berkas lainnya. Sebuah situs *web* biasanya ditempatkan setidaknya pada sebuah *server web* yang dapat diakses melalui jaringan seperti *internet*, ataupun jaringan wilayah local (LAN) melalui alamat *internet* yang dikenali sebagai URL. Gabungan atas semua situs yang dapat diakses publik di *internet* disebut pula sebagai World Wide *Web* atau lebih dikenal dengan singkatan WWW. Meskipun setidaknya halaman beranda situs *internet* umumnya dapat diakses publik secara bebas, pada prakteknya tidak semua situs memberikan kebebasan bagi publik untuk mengaksesnya, beberapa situs *web* mewajibkan pengunjung untuk melakukan

pendaftaran sebagai anggota, atau bahkan meminta pembayaran untuk dapat menjadi anggota untuk dapat mengakses isi yang terdapat dalam situs *web* tersebut, misalnya situs-situs yang menampilkan pornografi, situs-situs berita, layanan surel (*e-mail*), dan lain-lain. Pembatasan-pembatasan ini umumnya dilakukan karena alasan keamanan, menghormati privasi, atau karena tujuan komersil tertentu.

Gambar 6. 12 WEB Filtering

Sebuah halaman *web* merupakan berkas yang ditulis sebagai berkas teks biasa (plain text) yang diatur dan dikombinasikan sedemikian rupa dengan instruksi-instruksi berbasis HTML, atau XHTML, kadang-kadang pula disisipi dengan sekelumit bahasa skrip. Berkas tersebut kemudian diterjemahkan oleh peramban *web* dan ditampilkan seperti layaknya sebuah halaman pada monitor komputer.

Halaman-halaman *web* tersebut diakses oleh pengguna melalui protokol komunikasi jaringan yang disebut sebagai HTTP, sebagai tambahan untuk meningkatkan aspek keamanan dan aspek privasi yang lebih baik, situs *web* dapat pula mengimplementasikan mekanisme pengaksesan melalui protokol HTTPS.

Mencegah terjadinya akses *web* ke situs-situs yang tidak diinginkan (seperti situs porno) bukan hal yang sulit jika melengkapi jaringan komputer dengan HTTP *proxy server*. Umumnya HTTP *proxy server* digunakan untuk memfilter koneksi HTTP (*web*) dari LAN ke *internet*.

Kebijakan *web filtering* perlu dilakukan secara fleksibel. Artinya tidak disama ratakan. Untuk organisasi kecil seperti di perusahaan dan skala nasional. Tapi pada prinsipnya *policy* dapat diterapkan selama pemerintah/ISP memiliki profil pengguna *internet* yang lengkap.

BAB 7 HOTSPOT & RADIUS

7.1 Hotspot System

Gambar 7. 1 Topologi Hotspot System

Hotspot digunakan untuk melakukan autentikasi pada jaringan local. Autentikasi yang digunakan berdasarkan pada HTTP atau HTTPS protocol dan dapat diakses dengan menggunakan Web Browser. Hotspot sendiri adalah sebuah system yang mengkombinasikan beberapa macam features dari MikroTik RouterOS yang sangat mudah dikonfigurasi. Hotspot System adalah sebuah teknologi autentikasi yang biasa digunakan ketika kita akan menyediakan akses internet pada areal publik, seperti : Hotel, café, airport, taman, mall dll. Teknologi akses internet ini biasanya menggunakan jaringan wireless atau wired. Kita bisa menyediakan akses internet gratis dengan menggunakan hotspot atau bisa juga menggunakan Voucer untuk autentikasinya.

7.2 Cara Kerja Hotspot System

Ketika kita memcoba membuka sebuah web page maka router yang sudah memiliki hotspot system, akan men cek apakah user sudah di autentikasi pada system hotspot tersebut. Jika belum melakukan autentikasi, maka user akan di arahkan pada hotspot login page yang harus di isikan berupa usernama dan password. Jika informasi login yang dimasukkan sudah benar, maka router akan memasukkan user tersebut kedalam hotspot sytem dan client sudah bisa mengakses halaman web. Selain itu akan muncul popup windows berisi status ip address, byte rate dan time live. Dari urutan proses diatas, maka user sudah bisa mengakses halaman internet melalui hotspot gateway.

7.3 Keunggulan Hotspot System

Hotpost system digunakan untuk autentikasi user, penggunaan akses internet dapat dihitung berdasarkan waktu dan data yang di download / upload. Selain itu dapat juga dilakukan limitasi bandwidth berdasarkan data rate, total data upload/download atau bisa juga di limit berdasarkan lama pemakaian. Hotspot system juga mendukung system Radius.

Terdapat beberapa metode autentikasi yang berbeda dalam profile setting, jenis autentikasi tersebut adalah:

1. HTTP PAP - Metode yang paling sederhana, yang menunjukkan halaman login HotSpot dan mengharapkan untuk mendapatkan info otentikasi (username dan password yaitu) dalam teks biasa. Perhatikan bahwa password yang tidak dienkripsi saat ditransfer melalui jaringan. Penggunaan lain dari metode ini adalah kemungkinan informasi otentikasi keras-kode di halaman login servlet hanya menciptakan link yang sesuai.

2. HTTP CHAP - metode standar, yang meliputi tantangan CHAP di halaman login. Tantangan CHAP MD5 hash akan digunakan bersama-sama dengan password user untuk menghitung string yang akan dikirim ke gateway HotSpot. Hasil hash (sebagai password) bersama dengan username yang dikirim melalui jaringan ke layanan Hotspot (sehingga, sandi tidak pernah dikirim dalam teks biasa melalui IP jaringan). Pada sisi klien, MD5 algoritma diimplementasikan dalam applet JavaScript, jadi jika browser tidak mendukung JavaScript (seperti, misalnya, Internet Explorer 2.0 atau beberapa browser PDA), tidak akan dapat mengotentikasi pengguna. Hal ini dimungkinkan untuk memungkinkan password yang tidak terenkripsi dapat diterima dengan menghidupkan metode otentikasi HTTP PAP, tetapi tidak direkomendasikan (karena pertimbangan keamanan) untuk menggunakan fitur itu.

3. HTTPS - protokol SSL ini hampir sama seperti HTTP PAP, tetapi menggunakan untuk mengenkripsi transmisi. HotSpot pengguna hanya mengirim passwordnya tanpa tambahan hashing (catatan bahwa tidak ada perlu khawatir tentang paparan plain-text password melalui jaringan, sebagai transmisi itu sendiri dienkripsi). Dalam kedua kasus, metode HTTP POST (jika tidak

memungkinkan, maka - HTTP GET method) digunakan untuk mengirim data ke gateway HotSpot.

4. HTTP cookie - setelah setiap login berhasil, ada cookie yang dikirim ke browser web dan sama cookie akan ditambahkan ke daftar cookie HTTP aktif. Lain kali pengguna yang sama akan mencoba untuk log in, web browser akan mengirimkan cookie http. Cookie ini akan dibandingkan dengan yang disimpan pada gateway HotSpot dan hanya jika sumber alamat MAC dan ID secara acak yang dihasilkan sesuai dengan yang tersimpan pada gateway, pengguna akan secara otomatis login menggunakan informasi login (Username dan pasangan password) digunakan bila ada cookie yang pertama kali dihasilkan. Jika tidak, user akan diminta untuk login, dan di otentikasi kasus berhasil, cookie lama akan dihapus dari lokal HotSpot daftar cookie aktif dan yang baru dengan ID acak yang berbeda dan waktu kedaluwarsa akan ditambahkan ke daftar dan dikirim ke web browser. Hal ini juga memungkinkan untuk menghapus cookie di logoff user manual (tidak di halaman server default). Metode ini hanya dapat digunakan bersama dengan HTTP PAP, HTTP CHAP atau metode HTTPS karena akan ada apa-apa untuk menghasilkan cookie di tempat pertama sebaliknya. MAC address - mencoba untuk mengotentikasi klien segera setelah mereka muncul di daftar host (yaitu, segera setelah mereka telah mengirim paket apapun ke server HotSpot), klien menggunakan alamat MAC sebagai username.

7.4 Radius Server

Adalah server Remote Authentikasi Dial-in Service (RADIUS), sebuah protocol keamanan jaringan komputer berbasis server yang sering digunakan untuk melakukan authentikasi dan otorisasi serta pendaftaran akun (account) pengguna secara terpusat untuk mengakses jaringan yang aman. Server Radius menyediakan mekanisme keamanan dengan menangani otentikasi dan otorisasi koneksi yang dilakukan user. Pada saat komputer client akan menghubungkan diri dengan jaringan maka server Radius akan meminta identitas user (username dan password) untuk kemudian dicocokkan dengan data yang ada dalam database server Radius untuk kemudian ditentukan apakah user diijinkan untuk menggunakan layanan dalam jaringan komputer. Jika proses otentikasi dan otorisasi berhasil maka proses pelaporan dilakukan, yakni dengan mencatat semua aktifitas koneksi user, menghitung durasi waktu dan jumlah transfer

data dilakukan oleh user. Proses pelaporan yang dilakukan server Radius bisa dalam bentuk waktu (detik, menit, jam, dll) maupun dalam bentuk besar transfer data (Byte, KByte, Mbyte) (Anonim-B, 2006). Software server Radius yang digunakan dalam penelitian ini adalah Freeradius yang bersifat modular dan memiliki banyak fitur. Freeradius merupakan software server yang berbasis pada open source dan berlisensi GPL.

7.5 Konsep cara kerja secara singkatnya adalah sebagai berikut :

Gateway router akan mengarahkan user pada halaman login dan memaksa untuk melakukan otentifikasi atau payment terlebih dahulu (jika diimplementasikan system akunting) sebelum user mengakses external network, otentifikasi yang dilakukan user pada form login yg disebut captive portal, lalu user dan password yang diisikan kedalam form tersebut akan disingkronkan dengan user yang ada pada server radius.

Kelebihan dan Kelemahan RADIUS

Beberapa kelebihan yang diberikan oleh protokol RADIUS yaitu :

1) Menjalankan sistem administrasi terpusat,
2) Protokol connectionless berbasis UDP yang tidak menggunakan koneksi langsung,
3) Mendukung autentikasi Password Authentication Protocol (PAP) dan Challenge
4) Handshake Authentication Protocol (CHAP) Password melalui PPP.

Pada protokol RADIUS juga masih ditemukan beberapa kelemahan seperti :

1) Tidak adanya autentikasi dan verifikasi terhadap access request,
2) Tidak sesuai digunakan pada jaringan dengan skala yang besar,
3) MD5 dan shared secret; metode shared secret sudah berisiko untuk diterapkan, hal ini dikarenakan lemahnya MD5 hash yang menyimpan tanggapan autentikator sehingga Hacker / penyusup dapat dengan mudah mengetahui paket access-request beserta tanggapannya dengan cara melakukan penghitungan awal terhadap perhitungan MD5,
4) Pemecahan password ; skema proteksi password yang dipakai adalah stream-chiper, dimana MD5 digunakan sebagai sebuah ad hoc pseudorandom number generator (PRNG). 16 oktet pertama bertindak sebagai sebuah synchronous

stream chiper dan yang menjadi masalah adalah keamanan dari cipher ini

7.6 User Manager

UserManager merupakan fitur AAA server yang dimiliki oleh Mikrotik. Sesuai kepanjangan AAA (Authentication, Authorization dan Accounting), UserManager memiliki DataBase yang bisa digunakan untuk melakukan autentikasi user yang login kedalam network kita, memberikan kebijakan terhadap user tersebut misalnya limitasi transfer rate, dan juga perhitungan serta pembatasan quota yang dilakukan user kita nantinya.

UserManager ini akan memudahkan kita yang ingin membuat layanan internet publik secara luas, misalnya hotspot-hotspot di cafe, mall, hotel dan sebagainya, karena dengan menggunakan UserManager ini kita cukup membuat 1 account user, dan account user tersebut bisa digunakan atau diakses dari router-router Hotspot yang sudah kita pasang.

Informasi service yang bisa kita simpan dalam database UserManager meliputi:

HotSpot users.

PPP (PPtP/PPPoE) users.

DHCP Lease.

Wireless AccessList.

RouterOS users.

7.7 Tipe autentikasi pada security profile

A. WEP

WEP adalah security untuk wireless yang agak lama. Tipe security ini mudah untuk dicrack atau di sadap orang luar. WEP menggunakan 64bit dan 128bit. Ada dua cara untuk memasukkan WEP key, apakah Anda setkan sendiri atau generate menggunakan passphrase.Passphrase akan generate otomatis WEP key untuk Anda bila Anda masukkan abjad dan tekan generate. Untuk pengatahuan Anda, ia hanya bisa memasukkan 0-9 dan AF (hexadecimal).Panjang key tergantung jenis securiy Anda, jika 64bit, Anda masukkan 10key, dan untuk 128key Anda kena masukkan 26key. Tak bisa kurang dan lebih.

B.WPA-PSK

WPA-PSK adalah security yang lebih update dari WEP. WPA-PSK memiliki decryption yang ada pada WEP. Bahkan ia menambahkan security yang lebih pada wireless Anda. WPA-PSK masih bisa dicrack atau disadap, tetapi memakan waktu lebih lama dari WEP. Panjang key adalah 8-63, Anda bisa memasukkan apakah 64 hexadecimal atau ASCII (seperti biasa).

C.WPA2-PSK

WPA2-PSK adalah security terbaru untuk wireless, dan lebih bagus dari WEP dan WPA-PSK, tetapi masih bisa untuk dicrack atau disadap tetapi sangat memakan banyak waktu. Dalam WPA2-PSK ada dua jenis decryption, Advanced Encryption Standard (AES) dan Temporal Key Integrity Protocol (TKIP). TKIP banyak kelemahan sehingga lebih baik Anda menggunakan AES. Panjang key adalah 8-63, Anda bisa memasukkan apakah 64 hexadecimal atau ASCII (seperti biasa)

BAB 8 FAILOVER & LOAD BALANCING

8.1 Fail Over

Fail over pada Mikrotik adalah suatu teknik jaringan dengan memberikan dua jalur koneksi atau lebih dimana ketika salah satu jalur mati, maka koneksi masih tetap berjalan dengan disokong oleh jalur lainnya. Teknik failover ini cukup penting ketika kita menginginkan adanya koneksi jaringan internet yang handal.

Gambar 8. 1 Fail Over

Perhatikan gambar 8.1, dalam keadaan normal (tidak ada kendala dalam jaringan) LINK UTAMA akan digunakan untuk berkomunikasi antar PC (ACSL1 dan 2), jika LINK UTAMA

mengalami gangguan maka LINK CADANGAN akan digunakan.

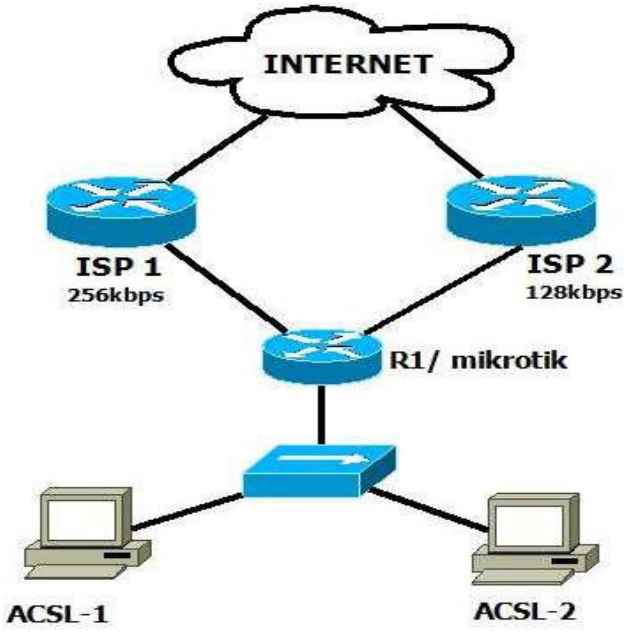
Gambar 8. 2 Topologi Jaringan

Perhatikan gambar 8.2 , topologi diatas adalah topologi yang sering digunakan warnet atau kantor untuk menghubunkan jaringannya ke internet, dalam kasus di gambar 7.3 ada dua buah ISP yang digunakan , ISP 1 adalah ISP UTAMA yang akan digunakan jaringan (PC ACSL) untuk terhubung kejaringan, dalam kondisi normal (ISP1 tidak mengalami masalah) R1/mikrotik akan menggunakan ISP1 untuk terkoneksi ke internet, sedangkan bila terjadi masalah di ISP1 maka R1/Mikrotik bertugas untuk mengalihkan koneksi ke ISP2.

Teknik failover yang sering digunakan adalah dengan membuat koneksi dari Fiber Optic sebagai Jalur utama dan ketika jalur utama mati (down) maka koneksi akan langsung pindah ke jalur cadangan. Dan jika koneksi utama kembali normal (up) maka koneksi akan kembali pindah ke jalur utama. Hal ini tidak dapat dilakukan dengan menggunakan teknik Failover biasa yang hanya menggunakan ping check gateway pada Route.

8.2 Load Balancing

Load balance pada mikrotik adalah teknik untuk mendistribusikan beban trafik pada dua atau lebih jalur koneksi secara seimbang, agar trafik dapat berjalan optimal, memaksimalkan throughput, memperkecil waktu tanggap dan menghindari overload pada salah satu jalur koneksi.



Gambar 8. 3 Kecepatan ISP

Perhatikan gambar 8.3 , ISP 1 memiliki kecepatan 256kbps dan ISP 2 memiliki kecepatan 128kbps, dengan menggunakan load balancing kedua ISP tersebut akan digunakan, total kecepatan yang didapat adalah 256kbps+128kbps (bukan 384kbps).

Untuk mencoba Load balancing minimal koneksi internet yang digunakan adalah dua

koneksi. Istilah load balancing mungkin akan mengacu pada jumlah bandwidth yang didapat dari beberapa koneksi internet sehingga mendapatkan besar bandwidth akumulasi dari ISP tersebut. Load balance tidak menambah besar bandwidth yang didapatkan, namun fungsi tersebut digunakan untuk membagi trafik dari beberapa bandwidth tersebut sehingga dapat digunakan secara seimbang atau saling mengisi kekurangan dan kelebihan bandwidth pada jalur koneksi.

8.3 Load Balancing NTH Pada Mikrotik

Metode NTH dengan koneksi yang masuk ke proses pada router akan menjadi satu arus yang sama, walaupun koneksi tersebut datang dari interface yang berbeda. Penerapan metode NTH, tentunya memberikan batasan ke router untuk hanya memproses koneksi dari sumber tertentu saja. Setelah router membentuk suatu antrian (Round-Robin)untuk pembatasan koneksi yang diberikan maka proses NTH akan dilakukan. Misalkan jika terdapat dua koneksi internet di satu router dengan dua NAT yang berbeda, koneksi pertama didapat dari ISP1dan koneksi kedua didapat dari ISP2. Maka konsep metode NTH menggunakan teknik round-robin, dimana client yang terkoneksi ke jaringan akan selalu berpindah-pindah secara berurutan pada kedua ISP tersebut.

Dengan metode ini, setiap client yang terkoneksi tidak harus secara antrian mengisi salah satu ISP hingga batas trafik bandwidth penuh, tetapi client akan secara round-robin sesuai dengan counter jumlah NTH yang dibuat menggunakan trafik bandwidth dari kedua ISP. Misalnya tersedia 2 ISP, maka antrian packet akan di koneksikan secara bergantian pada setiap client dengan format round-robin 1 2 1 2 1 2 dan seterusnya. Salah satu kelebihan dari NTH yaitu pembebanan packet yang merata sesuai dengan konsep round-robin. Sedangkan kekurangan NTH yaitu kadang mengalami kendala karena beberapa requestnya dari ip yang berganti-ganti.

8.4 Load Balancing PCC Pada Mikrotik

Metode PCC dapat mengelompokan trafik koneksi yang melalui atau keluar masuk router menjadi beberapa kelompok. Router akan mengingat-ingat jalur gateway yang dilewati diawal trafik koneksi, sehingga pada paket-paket selanjutnya yang masih berkaitan dengan koneksi awalnya akan dilewatkan pada jalur gateway yang sama juga. Kelebihan dari PCC dapat mengarahkan pengguna saat terputus koneksi dari gateway ISP 1 ke ISP lain yang digunakan. Sebelum membuat mangle load balance, untuk mencegah terjadinya loop routing pada trafik, maka semua trafik client yang menuju network yang terhubung langsung dengan router, harus kita bypass dari load balancing.

Selama ini banyak dari kita yang beranggapan salah, bahwa dengan menggunakan load balancing dua jalur koneksi , maka besar bandwidth yang akan kita dapatkan menjadi dua kali lipat dari bandwidth sebelum menggunakan load balancing (akumulasi dari kedua bandwidth tersebut). Hal ini perlu kita perjelas dahulu, bahwa loadbalance tidak akan menambah besar bandwidth yang kita peroleh, tetapi hanya bertugas untuk membagi trafik dari kedua bandwidth tersebut agar dapat terpakai secara seimbang.

Penggunaan PCC matcher memungkinkan untuk membagi lalu lintas ke dalam aliran yang sama dengan kemampuan untuk menjaga paket dengan serangkaian tertentu pada pilihan dalam satu aliran tertentu. Saat menggunakan type both address and port pada metode PCC, berarti ketika salah satu packet melakukan koneksi akan dicatat alamat sumber, alamat tujuan dan portnya. Ketika packet pada sumber yang sama melakukan koneksi kembali ke alamat tujuan yang sama dan port yang sama tentunya akan melalui jalur PCC yang sama dengan sebelumnya. Penggunaan metode PCC akan berjalan cukup efektif dan mendekati kondisi seimbang jika semakin banyak client yang terkoneksi. Salah satu kelebihan dari PCC yaitu hubungan client server terjalin utuh (terjamin) karena selalu pada ip sumber dan route yang sama. Sedangkan kekurangan dari metode PCC akan memungkinkan terjadinya over load pada salah satu jalur,sehingga ketika banyak akses yang kebetulan jalurnya sama dan beban nya bersama-sama.