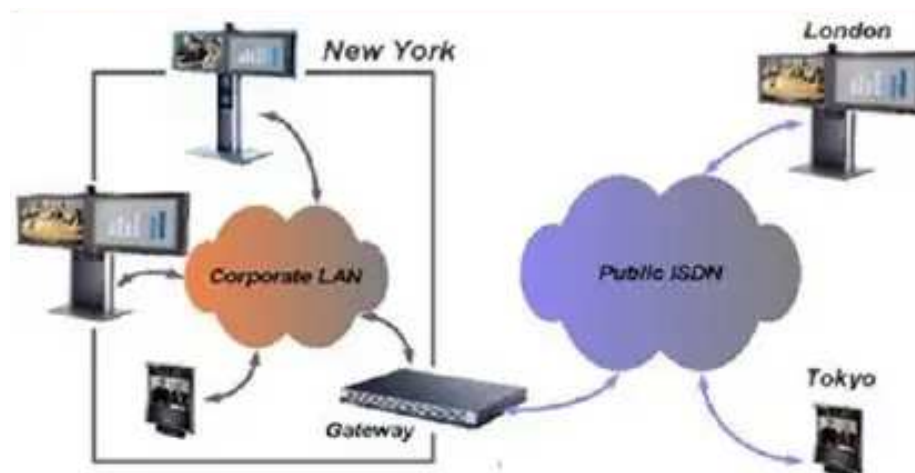


A. Internet Gateway

Gateway atau yang sering disebut juga dengan “Gerbang Jaringan” merupakan sebuah perangkat yang dapat memudahkan pengguna komputer dan internet. Salah satu aplikasi atau contoh dari penggunaan Gateway yang dapat kita lihat adalah pada Email. Seperti yang kita tahu bahwa pertukaran email dapat dilakukan meskipun dalam sistem yang tidak sama. Kini, seiring dengan semakin merebaknya penggunaan internet, pengertian Gateway pun sering melakukan pergeseran atau mengalami salah arti. Banyak orang yang menyamakan Gateway dengan Router, tapi sebenarnya Gateway dan Router adalah dua perangkat yang berbeda.



Gambar 2.15 Contoh Infrastruktur Gateway

1. Fungsi Gateway

Setelah kita membahas mengenai Pengertian Gateway pada jaringan komputer, maka kini membahas mengenai fungsi Gateway untuk sebuah jaringan internet komputer. Dilihat dari pengertiannya, secara umum Gateway berfungsi untuk menghubungkan sebuah jaringan komputer dengan jaringan komputer yang lain dengan protocol yang berbeda. Gateway dapat digunakan dalam menghubungkan IBM SNA dengan digital SNA, Local Area Network atau LAN dengan Wide Area Network atau WAN. Namun, terdapat pula beberapa fungsi dari Gateway yang lain yaitu:

- a. Sebagai Protocol Converting. Seperti yang telah dijelaskan di atas bahwa gateway dapat menghubungkan sebuah jaringan komputer dengan jaringan komputer lain dengan protocol yang berbeda. Untuk dapat menghubungkan dua jaringan dengan protocol yang berbeda inilah gateway harus memiliki kemampuan untuk melakukan konversi protocol sehingga dua protocol yang berbeda ini dapat saling dikaitkan atau dihubungkan. Sebuah Gateway jaringan merupakan sebuah sistem internet working yang mengkoneksikan dua jaringan dalam waktu yang sama dan dapat dikonfigurasi dalam

sebuah perangkat lunak atau software. Nah, jaringan gateway ini dapat beroperasi dalam setiap tingkat yang ada pada model lapisan dari OSI atau yang disebut juga dengan Open System Interconnection.

- b. Memudahkan akses Informasi. Tanpa gateway, jaringan komputer dengan protocol yang berbeda tidak akan pernah dapat dihubungkan satu sama lain. Ketika ini terjadi, maka sudah pasti bahwa sebuah jaringan komputer tidak akan mampu untuk melakukan akses informasi dari komputer yang lainnya. Ketika gateway sudah digunakan dan jaringan komputer tersebut tersambung, maka tentu saja akses informasi pun dapat berjalan dengan jauh lebih mudah. Maka Gateway pun sangat berguna untuk digunakan dalam memudahkan melakukan akses informasi.
- c. Hardware Sharing, Bagi pakai hardware secara bersama-sama. Contoh dari Penerapannya adalah penggunaan Printer Server, dimana 1buah Printer dapat digunakan secara bersama oleh Client dalam Jaringan.
- d. Keamanan dan pengaturan data, komputer dalam sebuah lingkungan bisnis, dengan adanya jaringan tersebut memungkinkan seorang administrator untuk mengorganisasi data-data kantor yang paling penting. Dari pada setiap departemen menjadi terpisah-pisah dan data-datanya tercecer dimana-mana. Data penting tersebut dapat di manage dalam sebuah server back end untuk kemudian di replikasi atau dibackup sesuai kebijakan perusahaan. Begitu pula seorang admin akan dapat mengontrol data-data penting tersebut agar dapat diakses atau di edit oleh orang-orang yang berhak saja.
- e. Kestabilan dan Peningkatan Performa Komputasi, Dalam kondisi tertentu sebuah jaringan dapat digunakan untuk meningkatkan performa keseluruhan dari aplikasi bisnis, Dengan cara memberikan tugas komputasi “lebih” kepada suatu Perangkat yg di distribusikan ke Komputer yang lain.

2. Konfigurasi Sederhana Gateway Internet Dengan Router Cisco

Perlu diingat bahwa untuk membangun Gateway Internet sebetulnya hanya butuh 2 (dua) tahap umum saja, yaitu : Setting koneksi Router ke Internet, dan Setting NAT pada Router.

Untuk memudahkan dalam mempraktikkan Gateway Internet, kita mencoba mengimplementasikan pada Cisco Packet Tracer dengan ketentuan: PC Admin, berfungsi melakukan setting Router Cisco melalui port Console menggunakan Hyper Terminal. PC Client, berfungsi menguji akses Internet saat Router Cisco telah selesai disetting sebagai Gateway Internet.

fa0/0, IP Publik, contoh: 110.76.148.78/30

fa0/1, IP Private, contoh: 192.168.88.1/24

IP Address ISP, 110.76.148.77

Di bawah ini diuraikan Cara setting Router Cisco sebagai Gateway Internet Berdasarkan 2 (dua) tahap tersebut.

3. Setting/Konfigurasi Koneksi Router ke Internet

Sebelumnya pastikan masuk ke Privileged Exec Mode (Administrator / root), dengan cara:

```
Router>enable
```

Setting/konfigurasi IP Address

Setting IP Address fa0/0

```
Router#configure terminal
```

```
Router(config)#interface fa0/0
```

```
Router(config-if)#ip address 110.76.148.78 255.255.255.252
```

```
Router(config-if)#no shutdown
```

Setting IP Address fa0/1

```
Router(config)#interface fa0/1
```

```
Router(config-if)#ip address 192.168.88.1 255.255.255.0
```

```
Router(config-if)#no shutdown
```

Cek apakah Interface telah memiliki IP Address dan dalam keadaan aktif, dengan perintah:

```
Router#show ip interface brief
```

```
Interface IP-Address OK? Method Status Protocol
```

```
FastEthernet0/0 110.76.148.78 YES manual up up
```

```
FastEthernet0/1 192.168.88.1 YES manual up up
```

Setting Default Gateway ke ISP

Melakukan setting Default Gateway berfungsi agar Router Cisco dapat melakukan terhubung (ping) ke IP Publik yang lain yang ada di Internet.

```
Router(config)#ip route 0.0.0.0 0.0.0.0 110.76.148.77
```

Untuk memeriksa apakah Default Gateway telah tersetting dengan benar, gunakan perintah:

```
Router#show ip route
```

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 110.76.148.77 to network 0.0.0.0

110.0.0.0/30 is subnetted, 1 subnets

C 110.76.148.76 is directly connected, FastEthernet0/0

C 192.168.88.0/24 is directly connected, FastEthernet0/1

S* 0.0.0.0/0 [1/0] via 110.76.148.77

Setting DNS Resolver

Agar Router Cisco dapat melakukan koneksi (ping) ke Hostname atau nama domain yang ada di Internet, maka perlu disetting DNS Resolver dengan cara (kita gunakan dns google):

```
Router(config)#ip name-server 8.8.8.8
```

4. Setting/Konfigurasi NAT (Network Address Translation)

Konfigurasi NAT (Masquerade) berfungsi agar jaringan LAN dapat terhubung ke Internet melalui Router Cisco. Maka dari itu, Router Cisco harus disetting untuk melakukan NAT (Masquerade) untuk network 192.168.88.0/24. Caranya adalah sebagai berikut.

```
Router(config)#access-list 1 permit 192.168.88.0 0.0.0.255
```

```
Router(config)#ip nat inside source list 1 interface f0/0 overload
```

```
Router(config)#interface f0/0
```

```
Router(config-if)#ip nat outside
```

```
Router(config-if)#interface f0/1
```

```
Router(config-if)#ip nat inside
```

Sampai disini, beberapa PC Client yang ada pada Jaringan LAN akan dapat mengakses Internet melalui Router Cisco yang telah dikonfigurasi sebagai Gateway Internet.

Konfigurasi DHCP (Opsional)

Langkah ini opsional yang berfungsi memberikan IP Address otomatis kepada PC Client. Perintah yang digunakan adalah sebagai berikut.

```
Router(config)#ip dhcp excluded-address 192.168.88.2 192.168.88.10
```

```
Router(config)#ip dhcp pool NAMA-pool-BEBAS
```

```
Router(dhcp-config)#network 192.168.88.0 255.255.255.0
```

```
Router(dhcp-config)#default-router 192.168.88.1
```

```
Router(dhcp-config)#dns-server 8.8.8.8
```

```
Router(dhcp-config)#exit
```

IP Address 192.168.88.2 sampai dengan 192.168.88.10 adalah IP Address yang tidak akan diberikan kepada PC Client pada LAN.

Dengan konfigurasi di atas, client sudah mendapatkan koneksi internet via router cisco.

Dalam sistem cisco, jika kita tidak menyimpan konfigurasi maka akan hilang ketika shutdown maupun reboot. Karena itu, setiap saat usahakan menyimpan konfigurasi yang ada. Untuk menyimpan bisa menggunakan perintah:

```
Router#copy running-config startup-config
```

Atau

```
Router#write
```

Hal ini harus dilakukan karena setiap sintaks yang di konfigurasikan akan masuk kedalam RAM (running config). Namun konfigurasi tersebut tidak akan masuk kedalam NVRAM (start-up config).

Untuk melihat konfigurasi yang berjalan dapat dilihat dengan syntax :

```
Router#show running-config
```

B. Firewall Jaringan

1. Pengenalan Firewall

Firewall adalah perangkat yang digunakan untuk mengontrol akses terhadap siapapun yang memiliki akses terhadap jaringan privat dari pihak luar. Saat ini, pengertian firewall difahami sebagai sebuah istilah generik yang merujuk pada fungsi firewall sebagai sistem pengatur komunikasi antar dua jaringan yang berlainan.

Mengingat sekarang ini banyak perusahaan yang memiliki akses ke Internet maka perlindungan terhadap aset digital perusahaan tersebut dari serangan para hacker, pelaku spionase, ataupun pencuri data lainnya, sehingga fungsi firewall menjadi hal yang sangat esensial.”

Firewall adalah *sistem keamanan jaringan komputer* yang digunakan untuk melindungi komputer dari beberapa jenis serangan dari komputer luar.

Menurut Wabopedia.com Definisi Firewall adalah sebuah sistem yang didesain untuk mencegah akses yang tidak sah ke atau dari jaringan pribadi (Privat Network). Firewall dapat diimplementasikan dalam perangkat keras dan perangkat lunak, atau kombinasi keduanya. Firewall sering digunakan untuk mencegah pengguna Internet yang tidak sah mengakses jaringan pribadi yang terhubung ke Internet, terutama intranet. Semua pesan masuk atau keluar dari intranet melewati firewall, firewall bertindak sebagai pengawas (controller) setiap pesan dan memblokir jika tidak memenuhi kriteria keamanan tertentu.

Menurut Pengertian Firewall yang dimaksudkan diatas, firewall adalah sebuah sistem atau perangkat yang memberi otorisasi pada lalu lintas jaringan komputer yang dianggapnya aman untuk melaluinya dan melakukan pencegahan terhadap jaringan yang dianggap tidak aman. Firewall dapat berupa perangkat lunak (program komputer atau aplikasi) atau perangkat keras (peralatan khusus untuk menjalankan program fire-wall) perangkat yang menyaring lalu lintas jaringan antara jaringan. Perlindungan dengan Firewall adalah mutlak diperlukan untuk komputasi perangkat seperti komputer yang diaktifkan dengan koneksi Internet. Meningkatkan tingkat keamanan jaringan komputer dengan memberikan informasi rinci tentang pola-pola lalu lintas jaringan. Perangkat ini penting dan sangat diperlukan karena bertindak sebagai gerbang keamanan antara jaringan komputer internal dan jaringan komputer eksternal.

2. Fungsi Firewall

Sebelum memahami fungsi firewall mari kita fahami atribut pentingnya sbb:

- a. Semua jaringan komunikasi melewati fire wall
- b. Hanya lalu lintas resmi diperbolehkan oleh fire wall
- c. Memiliki kemampuan untuk menahan serangan Internet

Fungsi firewall sebagai pengontrol, mengawasi arus paket data yang mengalir di jaringan. Fungsi Firewall mengatur, memfilter dan mengontrol lalu lintas data yang diizinkan untuk mengakses jaringan privat yang dilindungi, beberapa kriteria yang dilakukan fire-wall apakah memperbolehkan paket data lewati atau tidak, antara lain :

- a. Alamat IP dari komputer sumber
- b. Port TCP/UDP sumber dari sumber.
- c. Alamat IP dari komputer tujuan.
- d. Port TCP/UDP tujuan data pada komputer tujuan
- e. Informasi dari header yang disimpan dalam paket data.

Secara sfesifik Fungsi Firewall adalah melakukan autentifikasi terhadap akses ke jaringan. Aplikasi proxy Fire-wall mampu memeriksa lebih dari sekedar header dari paket data, kemampuan ini menuntutnya untuk mampu mendeteksi protokol aplikasi tertentu yang spesifikasi.

3. Manfaat Firewall

- a. Manfaat firewall adalah untuk menjaga informasi rahasia dan berharga yang menyelip keluar tanpa sepengetahuan. Sebagai contoh, FTP (File Transfer Protocol) lalu lintas dari jaringan komputer organisasi dikendalikan oleh fire-wall. Hal ini dilakukan untuk mencegah pengguna di jaringan mengirim file rahasia yang disengaja atau tidak sengaja kepada pihak lain.
- b. *Manfaat Firewall* sebagai filter juga digunakan untuk mencegah lalu lintas tertentu mengalir ke subnet jaringan. Hal ini mencegah pengguna berbagi file, dan bermain-main di jaringan. Aplikasi jenis ini berguna terutama dalam sektor korporasi.
- c. Manfaat firewall lainnya adalah untuk memodifikasi paket data yang datang di fire-wall. Proses ini disebut Network Address Translation (NAT). Ada jenis NAT disebut NAT dasar, di mana alamat IP (Internet Protocol) pribadi dari jaringan komputer yang tersembunyi di balik satu alamat IP tertentu. Proses ini disebut sebagai IP samaran. Hal ini membantu pengguna dalam sebuah jaringan yang meliputi sistem tanpa nomor IP publik yang beralamat, untuk mengakses Internet.
- d. Akurasi data seperti informasi keuangan, spesifikasi produk, harga produk dll, sangat penting bagi setiap perkembangan bisnis. Jika informasi tersebut

diubah oleh sumber eksternal, maka akan memberikan dampak merugikan. *Manfaat Firewall* disini adalah mencegah modifikasi data yang tidak sah di website.

4. Cara Kerja Firewall

Bagaimana cara kerja firewall? Komputer memiliki ribuan port yang dapat diakses untuk berbagai keperluan. *Cara Kerja Firewall* dari komputer adalah menutup port kecuali untuk beberapa port tertentu yang perlu tetap terbuka. Firewall di komputer bertindak sebagai garis pertahanan terdepan dalam mencegah semua jenis hacking ke dalam jaringan, karena, setiap hacker yang mencoba untuk menembus ke dalam jaringan komputer akan mencari port yang terbuka yang dapat diaksesnya.

Firewall dapat berupa perangkat keras atau perangkat lunak namun cara kerja firewall optimal bila kedua jenis perangkat digabungkan. Selain membatasi akses ke jaringan komputer, firewall juga memungkinkan akses remote ke jaringan privat melalui secure authentication certificates and logins (sertifikat keamanan otentikasi dan login).

Hardware firewall dapat dibeli sebagai produk yang berdiri sendiri, tetapi biasanya pada router broadband ditemukan , dan seharusnya dilakukan setting pada perangkat ini untuk akses ke jaringan komputer. Kebanyakan hardware firewall adalah memiliki minimal empat port jaringan untuk menghubungkan komputer lain,

Teknologi firewall saat ini sudah sangat canggih. Sebelumnya, cara kerja firewall adalah dengan menyaring lalu lintas jaringan yang menggunakan alamat IP, nomor port, dan protokol, tapi saat ini fire-wall dapat menyaring data dengan mengidentifikasi pesan konten itu sendiri. Dengan bantuan fire-wall, informasi sensitif atau tidak layak dapat dicegah melalui interface. Pastikan sistem keamanan jaringan di lapiasi firewall.

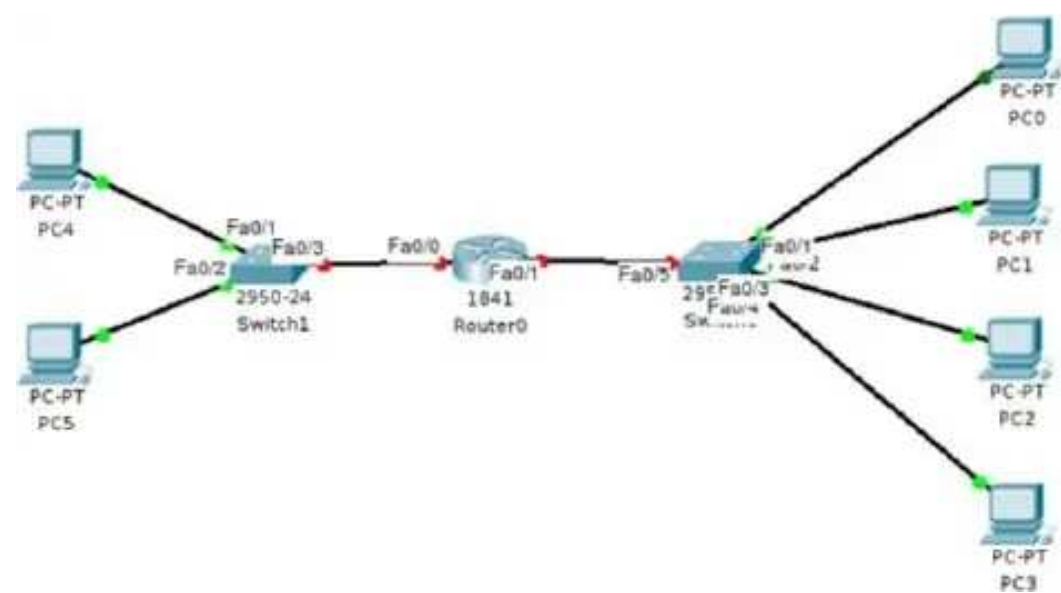
Network security merupakan suatu metode untuk mengamankan suatu jaringan komputer dari ancaman pengguna yang ingin merusak atau masuk ke dalam jaringan tersebut secara ilegal. Metode yang dapat dilakukan untuk mengamankan jaringan komputer tersebut bervariasi, mulai dari mengatur hak akses, membangun firewall maupun menerapkan algoritma kriptografi pada setiap koneksi yang sedang berlangsung pada jaringan komputer. Salah satu

yang akan dibahas pada kesempatan kali ini adalah mengamankan suatu jaringan komputer dengan mengatur hak akses setiap user pada satu atau lebih jaringan komputer yang tersedia. Pada device cisco sendiri memiliki command khusus untuk megatur hak akses user tersebut yaitu “*access-list*”.

Peralatan yang digunakan:

- a. 6 PC
- b. 2 Switch 2950-24
- c. 1 Router 1814

Topologi



Gambar 2.16 Contoh Topologi Jaringan

Tabel Pembagian IP Address

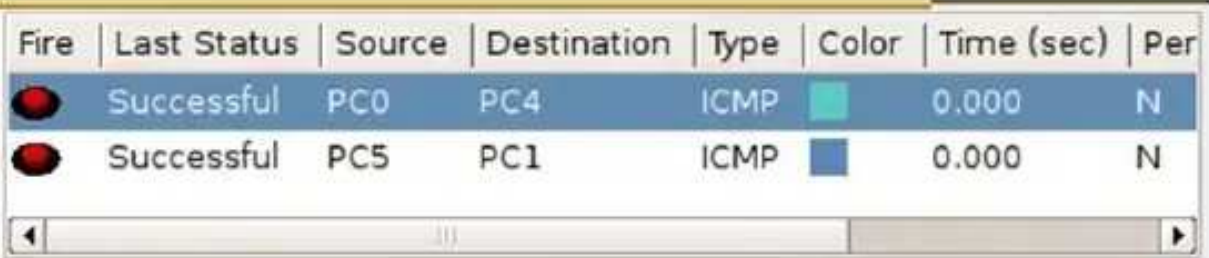
No. PC	Network	IP Address	Gateway
0	1	192.168.1.2	192.168.1.1
1	1	192.168.1.3	192.168.1.1
2	1	192.168.1.4	192.168.1.1
3	1	192.168.1.5	192.168.1.1
4	2	192.168.2.2	192.168.2.1
5	2	192.168.2.3	192.168.2.1





Pada Gambar 2.16 terdapat tanda titik merah yang memberitahukan bahwa koneksi antar *network* belum diproses oleh *user*, agar setiap *user* yang berbeda *network* dapat terkoneksi dengan baik lakukan konfigurasi berikut :

```
Interface 0/1 (Network 1)

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa 0/1
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no sh
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
Interface 0/1 (Network 2)
Router(config-if)#exit
Router(config)#int fa 0/0
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no sh
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up
Router(config-if)#
```

Kemudian uji koneksi antar network tersebut dengan mengirimkan PDU pada 2 PC yang berbeda *network*. Jika berhasil maka akan muncul pesan yang akan ditunjukkan pada Gambar 2.17.







Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Per
	Successful	PC0	PC4	ICMP		0.000	N
	Successful	PC5	PC1	ICMP		0.000	N



Gambar 2.17 Uji Koneksi PC0 – PC4 & PC5 – PC1

PC0 dan PC4 merupakan PC yang berbeda network. Pada Gambar 2.17, memberitahukan bahwa koneksi antara kedua PC tersebut berhasil dengan baik. Setelah beberapa PC yang berbeda network berhasil terkoneksi dengan baik maka langkah selanjutnya adalah membatasi akses pada PC yang terdapat pada kedua network. Untuk network 1 yang akan dibatasi adalah PC0 dengan IP Address 192.168.1.2. Sedangkan pada network 2 adalah PC4 dengan IP Address 192.168.2.2. Ikuti konfigurasi berikut :

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa 0/1
Router(config-if)#ip access-group 1 in
Router(config-if)#access-list 1 deny 192.168.1.2 255.255.255.0
Router(config)#access-list 1 permit any
Router(config)#int fa 0/0
Router(config-if)#ip access-group 1 in
Router(config-if)#access-list 1 deny 192.168.2.2 255.255.255.0
Router(config)#access-list 1 permit any
Router(config)#
```

Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Per
	Failed	PC0	PC5	ICMP		0.000	N
	Successful	PC1	PC5	ICMP		0.000	N

Gambar 2.18 Uji Koneksi PC0 –PC5

Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Per
	Failed	PC4	PC3	ICMP		0.000	N
	Successful	PC5	PC3	ICMP		0.000	N

Gambar 2.19 Uji Koneksi PC4– PC3

Dari Gambar 2.18 dan 2.19 dijelaskan bahwa PC0 tidak bisa mengakses PC yang berbeda *network* karena pembatasan hak akses yang dilakukan. PC0 hanya dapat melakukan koneksi dengan PC yang satu *network*. Hal ini sama halnya dengan PC4 yang tidak bisa mengakses PC yang berbeda *network*.

Untuk menghapus Access List tersebut, cukup jalankan perintah “*no access-list 1*” pada *console router*.

C. Manajemen Bandwidth

Ada sebuah jaringan yang mempunyai banyak client, diperlukan sebuah mekanisme pengaturan bandwidth dengan tujuan mencegah terjadinya monopoli penggunaan bandwidth sehingga semua client bisa mendapatkan jatah bandwidth masing-masing. QOS(Quality of services) atau lebih dikenal dengan Bandwidth Manajemen, merupakan metode yang digunakan untuk memenuhi kebutuhan tersebut. Pada RouterOS Mikrotik penerapan QoS bisa dilakukan dengan fungsi Queue.

1. Limitasi Bandwidth Sederhana

Cara paling mudah untuk melakukan queue pada RouterOS adalah dengan menggunakan Simple Queue. Kita bisa melakukan pengaturan bandwidth secara sederhana berdasarkan IP Address client dengan menentukan kecepatan upload dan download maksimum yang bisa dicapai oleh client.

Contoh

Kita akan melakukan limitasi maksimal upload: 128kbps dan maksimal download: 512kbps terhadap client dengan IP 192.168.10.2 yang terhubung ke Router. Parameter **Target Address** adalah IP Address dari client yang akan dilimit. Bisa berupa :

- a) Single IP (192.168.10.2)
- b) Network IP (192.168.10.0/24)
- c) Beberapa IP (192.168.10.2,192.168.10.13) dengan menekan tombol panah bawah kecil di sebelah kanan kotak isian.

Penentuan kecepatan maksimum client dilakukan pada parameter target upload dan target download max-limit. Bisa dipilih dengan drop down menu atau ditulis manual. Satuan bps (bit per second).

Gambar 2.20 Konfigurasi *limit bandwidth*

Dengan pengaturan tersebut maka Client dengan IP 192.168.10.2 akan mendapatkan kecepatan maksimum Upload 128kbps dan Download 256kbps dalam keadaan apapun selama bandwidth memang tersedia.

2. Metode Pembagian Bandwidth Share

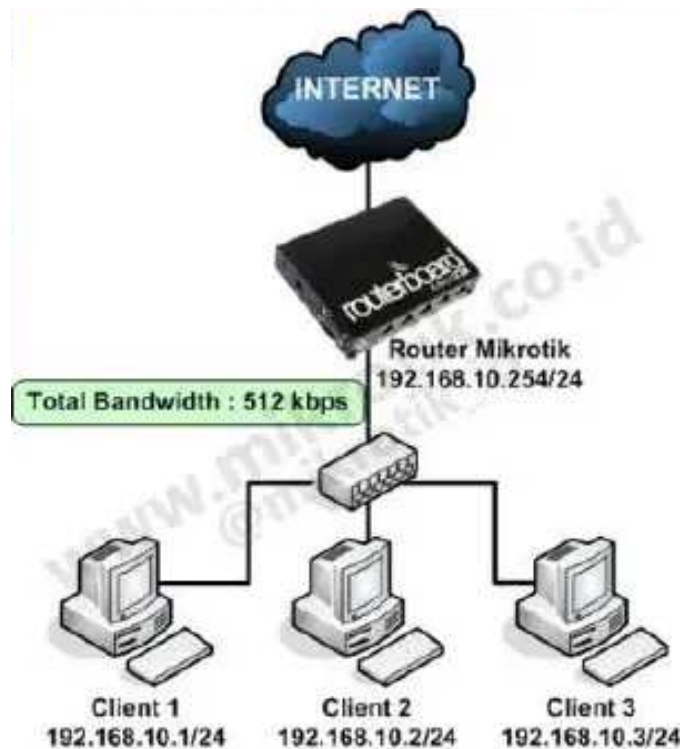
Selain digunakan untuk melakukan manajemen bandwidth fix seperti pada contoh sebelumnya, kita juga bisa memanfaatkan Simple Queue untuk melakukan pengaturan bandwidth share dengan menerapkan Limitasi Bertingkat. Konsep Limitasi Bertingkat bisa anda baca pada artikel Mendalami HTB pada QOS RouterOS Mikrotik.

Contoh :

Kita akan melakukan pengaturan bandwidth sebesar 512kbps untuk digunakan 3 client.

Konsep:

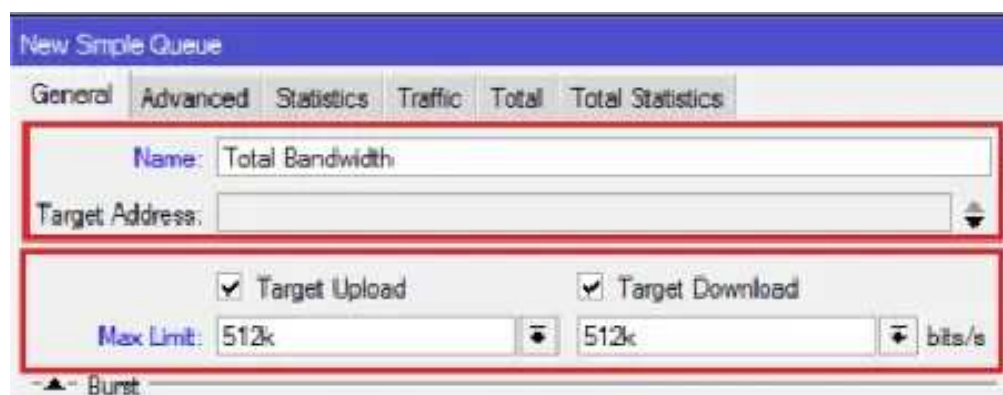
- Dalam keadaan semua client melakukan akses, maka masing-masing client akan mendapat bandwidth minimal 128kbps.
- Jika hanya ada 1 Client yang melakukan akses, maka client tersebut bisa mendapatkan bandwidth hingga 512kbps.
- Jika terdapat beberapa Client (tidak semua client) melakukan akses, maka bandwidth yang tersedia akan dibagi rata ke sejumlah client yg aktif.



Gambar 2.21 Pembagian bandwidth

3. Topologi Jaringan

Router kita tidak tahu berapa total bandwidth real yang kita miliki, maka kita harus definisikan pada langkah pertama. Pendefinisian ini bisa dilakukan dengan melakukan setting Queue Parent. Besar bandwidth yang kita miliki bisa diisikan pada parameter **Target Upload Max-Limit** dan **Target Download Max-Limit**.

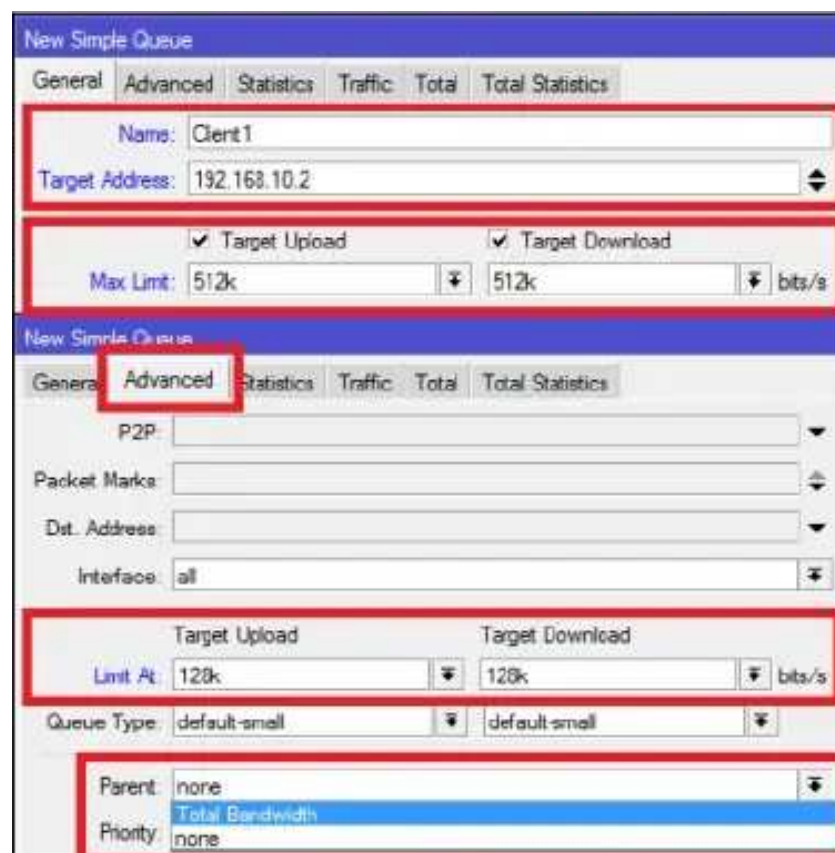


Gambar 2.22 Konfigurasi target *upload* dan *download*

Langkah selanjutnya kita akan menentukan limitasi per client dengan melakukan setting child-queue.

Pada child-queue kita tentukan target-address dengan mengisi IP address masing-masing client. Terapkan **Limit-at (CIR)** : 128kbps dan **Max-Limit (MIR)** : 512kbps. Arahkan ke Parent Total Bandwidth yang kita buat sebelumnya.

Ulangi untuk memberikan limitasi pada client yang lain, sesuaikan Target-Address.



Gambar 2.23 Konfigurasi limit setiap klien

Selanjutnya lakukan pengetesan dengan melakukan download di sisi client. Pada gambar berikut menunjukkan perbedaan kondisi penggunaan bandwidth client setelah dilakukan limitasi bertingkat.

Queue List						
Simple Queues						
#	Name	Target Address	Tx Max Limit	Tx Limit At	Parent	Tx
0	Total Bandwidth		512k	unlimited	none	513.8 kbps
1	Client1	192.168.10.1	512k	128k	Total Bandwidth	513.5 kbps
2	Client2	192.168.10.2	512k	128k	Total Bandwidth	0 bps
3	Client3	192.168.10.3	512k	128k	Total Bandwidth	0 bps

Gambar 2.24 Penggunaan bandwidth

Kondisi 1

Kondisi 1 menunjukkan ketika hanya 1 client saja yg menggunakan bandwidth, maka Client tersebut bisa mendapat hingga Max-Limit.

Perhitungan : Pertama Router akan memenuhi Limit-at Client yaitu 128kbps. Bandwidth yang tersedia masih sisa $512\text{kbps} - 128\text{kbps} = 384\text{kbps}$. Karena client yang lain tidak aktif maka 384kbps yang tersisa akan diberikan lagi ke Client1 sehingga mendapat $128\text{kbps} + 384\text{kbps} = 512\text{kbps}$ atau sama dengan max-limit.

#	Name	Target Address	Tx Max Limit	Tx Limit At	Parent	Tx
0	Total Bandwidth		512k	unlimited	none	515.5 kbps
1	Client1	192.168.10.1	512k	128k	Total Bandwidth	256.4 kbps
2	Client2	192.168.10.2	512k	128k	Total Bandwidth	259.0 kbps
3	Client3	192.168.10.3	512k	128k	Total Bandwidth	0 bps

Gambar 2.25 Penggunaan Bandwidth hanya digunakan pada 1 client

Kondisi 2

Kondisi 2 menggambarkan ketika hanya 2 client yang menggunakan bandwidth.

Perhitungan : Pertama router akan memberikan limit-at semua client terlebih dahulu. Akumulasi Limit-at untuk 2 client = $128\text{kbps} \times 2 = 256\text{kbps}$. Bandwidth total masih tersisa 256kbps . Sisa diberikan kemana.? Akan dibagi rata ke kedua Client.

Sehingga tiap client mendapat $\text{Limit-at} + (\text{sisa bandwidth} / 2) = 128\text{kbps} + 128\text{kbps} = 256\text{kbps}$

#	Name	Target Address	Tx Max Limit	Tx Limit At	Parent	Tx
0	Total Bandwidth		512k	unlimited	none	505.6 kbps
1	Client1	192.168.10.1	512k	128k	Total Bandwidth	179.2 kbps
2	Client2	192.168.10.2	512k	128k	Total Bandwidth	173.1 kbps
3	Client3	192.168.10.3	512k	128k	Total Bandwidth	170.8 kbps

Gambar 2.26 Penggunaan Bandwidth hanya digunakan pada 2 client

Kondisi 3

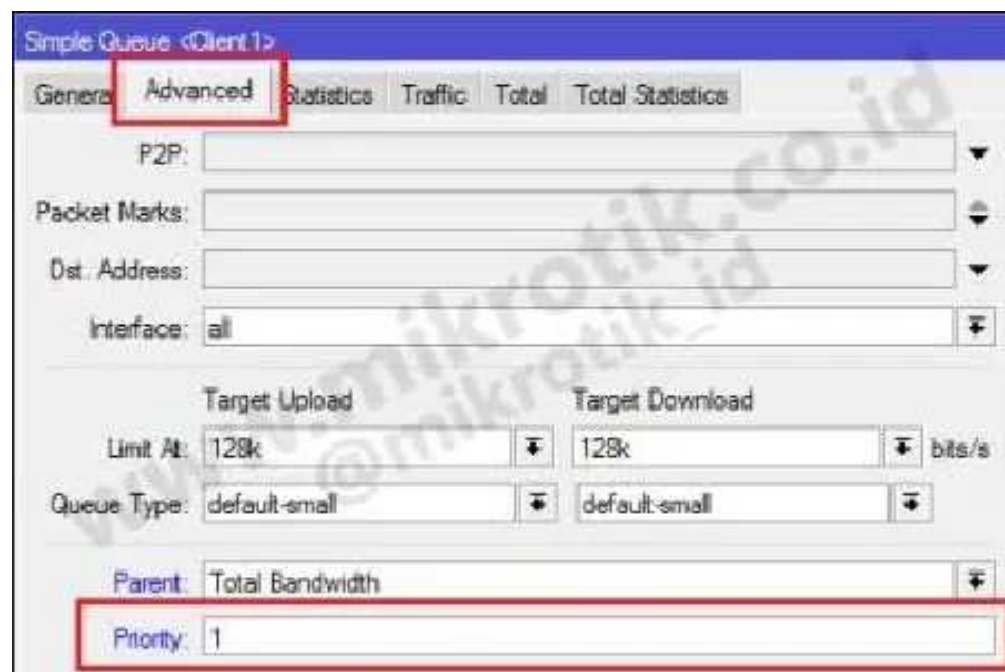
Kondisi 3 menunjukkan apabila semua client menggunakan bandwidth.

Perhitungan: Pertama Router akan memenuhi Limit-at tiap client lebih dulu, sehingga bandwidth yang digunakan $128\text{kbps} \times 3 = 384\text{kbps}$. Bandwidth total masih tersisa 128kbps . Sisa bandwidth akan dibagikan ke ketiga client secara merata sehingga tiap client mendapat $128\text{kbps} + (128\text{kbps}/3) = 170\text{kbps}$.

Pada Limitasi bertingkat ini juga bisa diterapkan **Priority** untuk client. Nilai priority queue adalah 1-8 dimana terendah 8 dan tertinggi 1.

Contoh

Client 1 adalah VVIP user, maka bisa diberikan Priority 1 (tertinggi).



Gambar 2.27 Konfigurasi Bandwidth untuk klien prioritas

Jika kita menerapkan priority perhitungan pembagian bandwidth hampir sama dengan sebelumnya. Hanya saja setelah limit-at semua client terpenuhi, Router akan melihat priority client. Router akan mencoba memenuhi Max-Limit client priority tertinggi dengan bandwidth yang masih tersedia.

#	Name	Target Address	Tx Max Limit	Tx Limit At	Parent	Priority	Tx
0	Total Bandwidth		512k	unlimited	none	1	8 518.9 kbps
1	Client1	192.168.10.1	512k	128k	Total Bandwidth	1	1.0 kbps
2	Client2	192.168.10.2	512k	128k	Total Bandwidth	1	8 239.5 kbps
3	Client3	192.168.10.3	512k	128k	Total Bandwidth	1	8 268.4 kbps

#	Name	Target Address	Tx Max Limit	Tx Limit At	Parent	Priority	Tx
0	Total Bandwidth		512k	unlimited	none	1	8 514.0 kbps
1	Client1	192.168.10.1	512k	128k	Total Bandwidth	1	1.249.2 kbps
2	Client2	192.168.10.2	512k	128k	Total Bandwidth	1	8 124.6 kbps
3	Client3	192.168.10.3	512k	128k	Total Bandwidth	1	8 125.8 kbps

Gambar 2.28 Penggunaan Bandwidth menggunakan klien prioritas

Perhitungan: Client 1 mempunyai priority tertinggi maka router akan mencoba memberikan bandwidth sampai batas Max-Limit yaitu 512kbps. Sedangkan bandwidth yang tersisa hanya 128kbps, maka Client1 mendapat bandwidth sebesar Limit-at + Sisa Bandwidth = 128kbps+128kbps = 256kbps.

Konsep pembagian bandwidth ini mirip ketika anda berlangganan internet dengan sistem Bandwidth share. Limitasi bertingkat juga bisa diterapkan ketika dibutuhkan sebuah pengelompokan pembagian bandwidth.

#	Name	Target Address	Tx Max Limit	Tx Limit At	Parent	Priority	Tx
0	Total Bandwidth	192.168.10.0/24	512k	unlimited	none	8	514.0 kbps
1	Limitasi Manager	192.168.10.2	256k	unlimited	Total Bandwidth	8	257.1 kbps
3	Client 2	192.168.10.2	256k	256k	Limitasi Manager	8	254.9 kbps
2	Limitasi Staff	192.168.10.1...	256k	unlimited	Total Bandwidth	8	256.8 kbps
5	Client 1	192.168.10.1	256k	128k	Limitasi Staff	8	131.5 kbps
4	Client 3	192.168.10.3	256k	128k	Limitasi Staff	8	132.1 kbps

Gambar 2.29 Penggunaan Bandwidth pada limitasi klien 1 dan 3

Tampak pada gambar, limitasi Client1 dan Client3 tidak mengganggu limitasi Client2 karena sudah berbeda parent. Perhatikan max-limit pada **Limitasi Manager** dan **Limitasi Staff**.

4. Bypass Traffic Lokal

Ketika kita melakukan implementasi Simple Queue, dengan hanya berdasarkan target-address, maka Router hanya akan melihat dari mana traffic itu berasal. Sehingga kemanapun tujuan traffic nya (dst-address) tetap akan terkena limitasi. Tidak hanya ke arah internet, akan tetapi ke arah jaringan Lokal lain yang berbeda segment juga akan terkena limitasi.

Contoh :

- IP LAN 1 : 192.168.10.0/24
- IP LAN 2 : 192.168.11.0/24

Jika hanya dibuat Simple Queue dengan target-address : 192.168.10.0/24, traffic ke arah 192.168.11.0/24 juga akan terlimit. Agar traffic ke arah jaringan lokal lain tidak terlimit, kita bisa membuat Simple Queue baru dengan mengisi dst-address serta tentukan Max-Limit sebesar maksimal jalur koneksi, misalnya 100Mbps. Kemudian letakkan rule tersebut pada urutan teratas (no. 0).

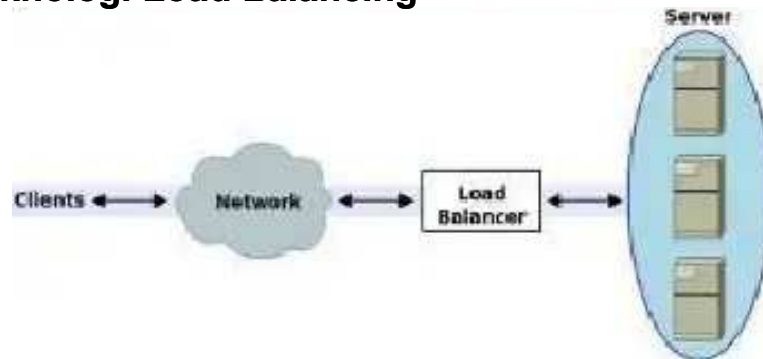
#	Name	Target Address	Rx Max Limit	Tx Max Limit	Dst. Address	Rx Limit At	Tx Limit At
0	ByPassLokal	192.168.10.0/24	100M	100M	192.168.11.0/24	unlimited	unlimited
3	Total Bandwidth		512k	512k		unlimited	unlimited
1	LimitLAN1	192.168.10.0/24	512k	512k		256k	256k
2	LimitLAN2	192.168.11.0/24	512k	512k		256k	256k

Gambar 2.30 konfigurasi simple queue

Rule Simple Queue dibaca dari urutan teratas (no. 0) sehingga dengan pengaturan tersebut traffic dari LAN1 ke LAN2 dan sebaliknya maksimum transfer rate sebesar 100Mbps atau setara dengan kecepatan kabel ethernet.

D. Load Balancing

1. Mengenal Teknologi Load Balancing



Gambar 2.31 Load Balancing

Load balancing 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. Load balancing digunakan pada saat sebuah server telah memiliki jumlah user yang telah melebihi maksimal kapasitasnya. Load balancing juga mendistribusikan beban kerja secara merata di dua atau lebih komputer, link jaringan, CPU, hard drive, atau sumber daya lainnya, untuk mendapatkan pemanfaatan sumber daya yang optimal.

2. Mengapa Menggunakan *Load balancer*

Ada banyak alasan mengapa menggunakan load balancing untuk website atau aplikasi berbasis web lainnya. Dua alasan yang utama adalah:

- Waktu Respon.** Salah satu manfaat terbesar adalah untuk meningkatkan kecepatan akses website saat dibuka. Dengan dua atau lebih server yang saling berbagi beban lalu lintas web, masing-masing akan berjalan lebih cepat karena beban tidak berada pada 1 server saja. Ini berarti ada lebih banyak sumber daya untuk memenuhi permintaan halaman website.
- Redundansi.** Dengan load balancing, akan mewarisi sedikit redundansi. Sebagai contoh, jika website kita berjalan seimbang di 3 server dan salah satu server bermasalah, maka dua server lainnya dapat terus berjalan dan pengunjung website kita tidak akan menyadarinya downtime apapun.

3. Cara Kerja Load Balancing

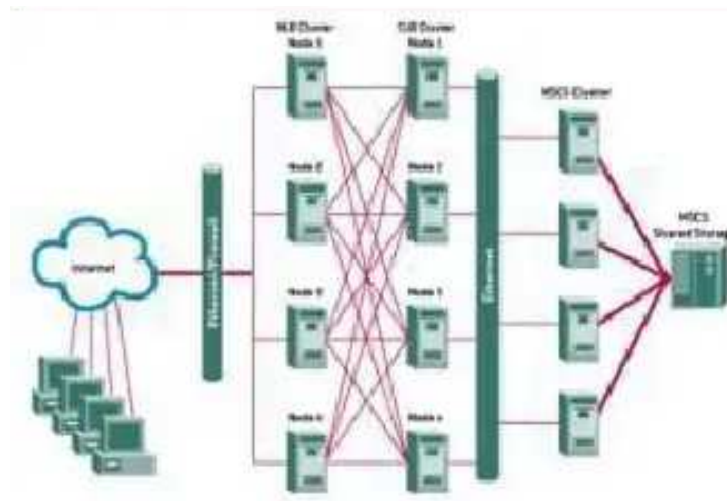
Load balancer (perangkat *load balancing*) menggunakan beberapa peralatan yang sama untuk menjalankan tugas yang sama. Hal ini memungkinkan pekerjaan dilakukan dengan lebih cepat dibandingkan apabila dikerjakan oleh hanya 1 peralatan saja dan dapat meringankan beban kerja

peralatan, serta mempercepat waktu respons. *Load balancer* bertindak sebagai penengah di antara layanan utama dan pengguna, dimana layanan utama merupakan sekumpulan server/mesin yang siap melayani banyak pengguna.

Disaat *Load balancer* menerima permintaan layanan dari *user*, maka permintaan tersebut akan diteruskan ke server utama. Biasanya *Load balancer* dengan pintar dapat menentukan server mana yang memiliki load yang lebih rendah dan respons yang lebih cepat. Bahkan bisa menghentikan akses ke server yang sedang mengalami masalah dan hanya meneruskannya ke server yang dapat memberikan layanan. Hal ini salah satu kelebihan yang umumnya dimiliki *load balancer*, sehingga layanan seolah olah tidak ada gangguan di mata pengguna.

4. Algoritma Load Balancing

- a. *Round Robin*. Algoritma Round Robin merupakan algoritma yang paling sederhana dan banyak digunakan oleh perangkat load balancing. Algoritma ini membagi beban secara bergiliran dan berurutan dari satu server ke server lain sehingga membentuk putaran.



Gambar 2.32 Infrastruktur Roun Robin

- b. *Ratio*. Ratio (rasio) sebenarnya merupakan sebuah parameter yang diberikan untuk masing-masing server yang akan dimasukkan kedalam sistem load balancing. Dari parameter Ratio ini, akan dilakukan pembagian beban terhadap server-server yang diberi rasio. Server dengan rasio terbesar diberi beban besar, begitu juga dengan server dengan rasio kecil akan lebih sedikit diberi beban.
- c. *Fastest*. Algoritma yang satu ini melakukan pembagian beban dengan mengutamakan server-server yang memiliki respon yang paling cepat. Server

di dalam jaringan yang memiliki respon paling cepat merupakan server yang akan mengambil beban pada saat permintaan masuk.

- d. *Least Connection*. Algoritma Least connection akan melakukan pembagian beban berdasarkan banyaknya koneksi yang sedang dilayani oleh sebuah server. Server dengan pelayanan koneksi yang paling sedikit akan diberikan beban yang berikutnya akan masuk.

5. Fitur Load Balancing

Beberapa fitur yang ada pada baik *load balancer* hardware maupun *load balancer* software, yaitu:

- a. *Asymmetric load*. rasio dapat dibuat dengan menentukan koneksi yang menjadi primary yang dianggap paling baik backbonenya dan terbaik dalam path routingnya, jadi kita dapat membuat mesin untuk mencari best path determination dan routing yang terpendek dan terbaik untuk sampai ketujuan.
- b. Aktivitas berdasarkan prioritas. Disaat load jaringan lagi peek, server akan dapat membagi aktivitas berdasarkan prioritas dan ke link cadangan.
- c. Proteksi dari serangan DDoS. karena kita dapat membuat fitur seperti SYN Cookies dan delayed-binding (suatu metode di back-end server pada saat terjadi proses TCP handshake) pada saat terjadi serangan SYN Flood.
- d. Kompresi HTTP. Memungkinkan data untuk bisa mentransfer objek HTTP dengan dimungkinkannya penggunaan utilisasi kompresi gzip yang berada di semua web browser yang modern.
- e. *TCP Buffering*. dapat membuat respon buffer dari server dan berakibat dapat memungkinkan task akses lebih cepat.
- f. *HTTP Caching*. dapat menyimpan content yang static, dengan demikian request dapat di handel tanpa harus melakukan kontak ke web server diluar jaringan yang berakibat akses terasa semakin cepat.
- g. *Content Filtering*. Beberapa load balancing dapat melakukan perubahan trafik pada saat dijalankan.
- h. *HTTP Security*. beberapa system load balancing dapat menyembunyikan HTTP error pages, menghapus identifikasi header server dari respon HTTP, dan melakukan enkripsi cookies agar user tidak dapat memanipulasinya.
- i. *Priority Queuing*. berguna untuk memberikan perbedaan prioritas traffic paket.

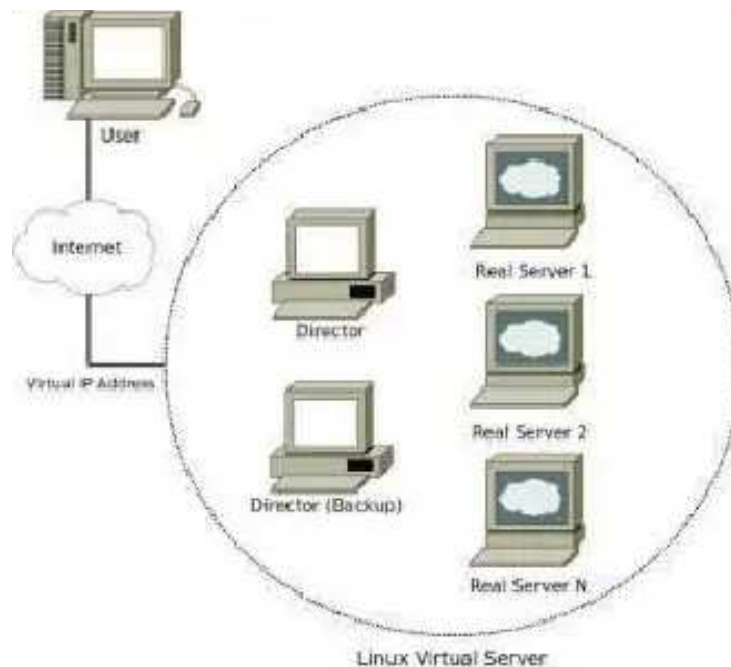
- j. *Spam Filtering*. Spam istilah lainnya *junk mail* merupakan penyalahgunaan dalam pengiriman berita elektronik untuk menampilkan berita iklan dan keperluan lainnya yang mengakibatkan ketidaknyamanan bagi para pengguna web. Bentuk berita spam yang umum dikenal meliputi: spam surat elektronik, spam instant messaging, spam Usenet newsgroup, spam mesin pencari informasi web (web search engine spam), spam blog, spam berita pada telepon genggam, spam forum Internet, dan lain lain. Spam ini biasanya datang bertubi-tubi tanpa diminta dan sering kali tidak dikehendaki oleh penerimanya. Beberapa contoh lain dari spam ini bisa berupa surat elektronik berisi iklan, sms pada telepon genggam, berita yang masuk dalam suatu forum newsgroup berisi promosi barang yang tidak terkait dengan aktifitas newsgroup tersebut, spamdexing yang mendominir suatu mesin pencari (search engine) untuk mencari popularitas bagi suatu URL tertentu, ataupun bisa berupa berita yang tak berguna dan masuk dalam suatu blog, buku tamu situs web, dan lain-lain.

6. Tipe Load balancer

Dalam dunia load-balancing, ada dua pilihan untuk dipertimbangkan ketika merancang solusi load-balancing. Pilihan solusinya adalah menggunakan software load balancing atau hardware load balancing. Setiap pilihan memiliki persyaratan, kelebihan, dan kelemahan tersendiri. Terserah kepada kita untuk mengevaluasi kebutuhan bisnis kita, konfigurasi, dan jalur pertumbuhan sehingga kita dapat mengidentifikasi solusi optimal untuk memenuhi kebutuhan. Dan dari tipenya Load Balancing dapat dibedakan menjadi 2 tipe, yaitu:

- a. *Software Load Balancing*. Dimana Load Balancing berjalan disebuah PC/Server, dan aplikasi Load Balancing di install dan perlu dikonfigurasi sebelum dapat berfungsi. Keuntungannya adalah jika ada penambahan fitur atau fasilitas tambahan tidak perlu mengganti keseluruhan perangkat load balancing. Performa proses load balancing dipengaruhi oleh perangkat komputer yang digunakan, tidak bisa hanya mengandalkan kemampuan software yang canggih saja. Perangkat keras yang dapat mempengaruhi performa metode ini adalah kartu jaringan (*Network Interface Card*) yang digunakan, besarnya RAM pada perangkat, media penyimpanan yang besar dan cepat, dsb. Sehingga performa metode ini sulit untuk bisa diperkirakan.

Ada banyak sekali *Load balancer* Software, beberapa diantaranya yang paling banyak digunakan adalah: Linux Virtual Server, Ultra Monkey, dan Network Load Balancing.



Gambar 2.33 Linux Virtual Server

- b. *Hardware Load Balancing*. Dimana Load Balancing berjalan disebuah device/alat yang sudah disiapkan dari pabrik dan siap digunakan. Tipe Hardware Load Balancing banyak digunakan karena kemudahannya. Beberapa *Load balancer* Hardware diantaranya adalah: Cisco System Catalyst, Coyote Point, F5 Network BIG-IP, Baraccuda *Load balancer*.

7. Penggunaan Load balancer

Pada umumnya *Load balancer* digunakan oleh perusahaan/pemilik layanan yang menginginkan layanannya selalu tersedia setiap saat (*high availability*)

walaupun secara kenyataan terdapat kendala yang membuat layanan tidak dapat diakses. Misalnya untuk layanan web server/email server. Dengan *load balancer*, apabila ada 2 mail server dengan konfigurasi dan tugas yang sama, maka *load balancer* akan membagi beban ke 2 mail server tersebut. Dan apabila salah satu Mail server tersebut down/tidak dapat diakses/mengalami gangguan, maka Mail server yang lain dapat terus melayani layanan yang diakses oleh user.

Untuk jaringan komputer, *Load balancer* digunakan di ISP/Internet provider dimana memungkinkan tersedianya akses internet selama 24x7x365 tanpa ada down time. Tentu hal ini yang diinginkan oleh pelanggan yang menggunakan layanan akses internet ISP tersebut. ISP/Provider hanya perlu memiliki 2 Link internet yang memiliki jalur berbeda, agar disaat salah satu link down, masih ada

1 link yang dapat melayani akses internet ke pelanggannya. Dan ISP menggunakan *Load balancer* untuk membagi beban akses internet tersebut sehingga kedua Link Internet tersebut maksimal penggunaannya dan beban terbagi dengan baik.

8. Perbandingan Software vs Hardware Load balancer

Kelebihan *Load balancer* Software:

- 1) Lebih murah.
- 2) Beberapa software aplikasi memiliki banyak pilihan konfigurasi yang dapat disesuaikan dengan kebutuhan kita.

Kekurangan *Load balancer* Software:

- 1) Sebagian besar aplikasi tidak dapat menangani situs besar atau jaringan kompleks.
- 2) Paket aplikasi yang akan mendukung sistem yang lebih besar memerlukan jumlah hardware lebih banyak.

Kelebihan *Load balancer* Hardware:

- 1) Pendekatan biasanya lebih kuat dari pilihan perangkat lunak.
- 2) Proses lalu lintas pada tingkat jaringan, yang secara nominal lebih efisien daripada dekripsi perangkat lunak.
- 3) Bekerja dengan banyak OS atau platform.

Kekurangan *Load balancer* Hardware:

Biaya lebih tinggi dibandingkan menggunakan software *load balancer*.

Teknologi load balancing dapat menjadi salah satu solusi yang efektif dan efisien untuk menciptakan sistem yang handal dengan tingkat ketersediaan tinggi (*high availability*), khususnya sebagai web server. Untuk pemanfaatan teknologi load balancing menggunakan software load balancing saat ini memang lebih banyak digunakan pada sistem operasi open source seperti linux

I. Proxy Server

Server adalah sebuah sistem komputer yang menyediakan jenis layanan tertentu dalam sebuah jaringan komputer. Server didukung dengan prosesor yang bersifat *scalable* dan RAM yang besar, juga dilengkapi dengan sistem operasi khusus, yang disebut sebagai sistem operasi jaringan. Server juga menjalankan perangkat lunak administratif yang mengontrol akses terhadap

jaringan dan sumber daya yang terdapat di dalamnya, seperti halnya berkas atau pencetak, dan memberikan akses kepada stasiun kerja anggota jaringan.

Umumnya, di dalam sistem operasi server terdapat berbagai macam layanan yang menggunakan arsitektur klient/server. Contoh dari layanan ini adalah Protokol Konfigurasi Hos Dinamik, server surat, server PTH, server PTB, DNS server, dan lain sebagainya. Setiap sistem operasi server umumnya membundel layanan-layanan tersebut, meskipun pihak ketiga dapat pula membuat layanan tersendiri. Setiap layanan tersebut akan merespon *request* dari klien. Sebagai contoh, klien PKHD akan memberikan *request* kepada server yang menjalankan layanan server PKHD; ketika sebuah klien membutuhkan alamat IP, klien akan memberikan *request* kepada server, dengan bahasa yang dipahami oleh server PKHD, yaitu protokol PKHD itu sendiri.

Server biasanya terhubung dengan klien dengan kabel UTP dan sebuah kartu jaringan. Kartu jaringan ini biasanya berupa kartu PCI atau ISA. Dilihat dari fungsinya, server bisa di kategorikan dalam beberapa jenis, seperti: server aplikasi, server data maupun server proksi. Server aplikasi adalah server yang digunakan untuk menyimpan berbagai macam aplikasi yang dapat diakses oleh klien, server data sendiri digunakan untuk menyimpan data baik yang digunakan klien secara langsung maupun data yang diproses oleh server aplikasi. Server proksi berfungsi untuk mengatur lalu lintas di jaringan melalui pengaturan proxy. Orang awam lebih mengenal proxy server untuk mengkoneksikan komputer klien ke Internet.

Proxy server (peladen proxy) adalah sebuah komputer server atau program komputer yang dapat bertindak sebagai komputer lainnya untuk melakukan request terhadap content dari Internet atau intranet.

Proxy Server bertindak sebagai gateway terhadap dunia Internet untuk setiap komputer klien. Proxy server tidak terlihat oleh komputer klien: seorang pengguna yang berinteraksi dengan Internet melalui sebuah proxy server tidak akan mengetahui bahwa sebuah proxy server sedang menangani request yang dilakukannya. Web server yang menerima request dari proxy server akan menginterpretasikan request-request tersebut seolah-olah request itu datang secara langsung dari komputer klien, bukan dari proxy server.

Proxy server juga dapat digunakan untuk mengamankan jaringan pribadi yang dihubungkan ke sebuah jaringan publik (seperti halnya Internet). Proxy

server memiliki lebih banyak fungsi daripada router yang memiliki fitur packet filtering karena memang proxy server beroperasi pada level yang lebih tinggi dan memiliki kontrol yang lebih menyeluruh terhadap akses jaringan. Proxy server yang berfungsi sebagai sebuah "agen keamanan" untuk sebuah jaringan pribadi, umumnya dikenal sebagai firewall.

Langkah-langkah Konfigurasi Proxy Server

Sebelum melakukan konfigurasi proxy server, terlebih dahulu perhatikan hal-hal berikut ini :

- a. IP Address proxy server untuk adalah 192.168.100.1/24, untuk klien menyesuaikan
- b. Jenis Proxy server yang akan dibangun adalah forward http proxies untuk proxy untuk menangani aplikasi http / web.
- c. Menggunakan aplikasi squid pada linux debian dan port 3128

d. Siapkan DVD Master instalasi

Kemudian ikuti langkah-langkah berikut :

- a. Lakukan instalasi paket squid dengan perintah **#apt-get install squid** dan pastikan tidak menemukan error.

```
debian:~# apt-get install squid
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  squid-common
Suggested packages:
  squidclient squid-cgi logcheck-database resolvconf smbclient winbind
The following NEW packages will be installed:
  squid squid-common
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 0B/1188kB of archives.
After this operation, 6791kB of additional disk space will be used.
Do you want to continue [Y/n]? y_
```

- b. Buka file konfigurasi squid.conf dengan perintah **#pico /etc/squid/squid.conf** kemudian lakukan konfigurasi sebagai berikut, konfigurasi ini adalah konfigurasi minimal agar proxy dapat berjalan.

```

GNU nano 2.8.7      File: /etc/squid/squid.conf      Modified
#
#       the port specification (port or addr:port)
#
#       keepalive[=idle,interval,timeout]
#       Enable TCP keepalive probes of idle connections
#       idle is the initial time before TCP starts probing
#       the connection, interval how often to probe, and
#       timeout the time before giving up.
#
#       If you run Squid on a dual-homed machine with an internal
#       and an external interface we recommend you to specify the
#       internal address:port in http_port. This way Squid will only be
#       visible on the internal address.
#
# Squid normally listens to port 3128
http_port 3128 transparent_
#
# ToG: https_port
# Note: This option is only available if Squid is rebuilt with the
#       --enable-ssl option
#
#G Get Help  #O WriteOut  #B Read File  #Y Prev Page  #X Cut Text  #C Cur Pos
#X Exit      #J Justify   #U Where Is  #U Next Page  #U UnCut Text #T To Spell

```

Gambar 2.34 Konfigurasi port proxy

Keterangan script: **http_port 3128 transparent** = Menentukan proxy bekerja pada port 3128 secara transparant.

- c. Kemudian tutup / non aktifkan baris script `acl localnet` dengan memberi tanda pagar (#), untuk `acl` nantinya akan kita definisikan sendiri sesuai dengan network yang kita bangun.

```

GNU nano 2.8.7      File: /etc/squid/squid.conf      Modified
#
#Recommended minimum configuration:
acl all src all
acl manager proto cache_object
acl localhost src 127.0.0.1/32
acl to_localhost dst 127.0.0.0/8
#
# Example rule allowing access from your local networks.
# Adapt to list your (internal) IP networks from where browsing
# should be allowed
#acl localnet src 10.0.0.0/8      # RFC1918 possible internal network
#acl localnet src 172.16.0.0/12 # RFC1918 possible internal network
#acl localnet src 192.168.0.0/16 # RFC1918 possible internal network
#
acl SSL_ports port 443          # https
acl SSL_ports port 563          # snews
acl SSL_ports port 873          # rsync
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443          # https
[ Search Wrapped ]
#G Get Help  #O WriteOut  #B Read File  #Y Prev Page  #X Cut Text  #C Cur Pos
#X Exit      #J Justify   #U Where Is  #U Next Page  #U UnCut Text #T To Spell

```

Gambar 2.35 Menutup `acl localnet`

- d. Kemudian kita definisikan network yang kita bangun, perhatikan penempatannya karena script akan dibaca urut dari atas ke bawah.

```
GNU nano 2.8.7 File: /etc/squid/squid.conf Modified

#http_access deny to_localhost
#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
#http_access allow localnet
http_access allow localhost

acl jaringanku src 192.168.100.0/24
http_access allow jaringanku

# And finally deny all other access to this proxy
http_access deny all

# TAG: http_access2
#   Allowing or Denying access based on defined access lists
#
#   Identical to http_access, but runs after redirectors. If not set

G Get Help  O WriteOut  R Read File  Y Prev Page  K Cut Text  C Cur Pos
X Exit      J Justify    W Where Is  U Next Page  U UnCut Text  T To Spell
```

Gambar 2.36 Membuat acl jaringan sendiri

Keterangan script

- 1) `acl jaringanku src 192.168.100.0/24`

mendefinisikan acl (Access Control List) untuk jaringan yang akan kita kontrol hak aksesnya yaitu jaringan dengan alamat network 192.168.100.0/24. Ini berarti seluruh Alamat IP yang valid dari alamat network 192.168.100.0/24 termasuk dalam acl ini.

- 2) `http_access allow jaringanku`

memberikan akses http (browsing) untuk acl jaringanku, jika ingin menutup akses http (browsing) maka kata allow cukup diganti deny

- 3) Kemudian setting visible hostname, yaitu mendefinisikan nama komputer untuk server proxy sesuai DNS yang kita bangun (FQDN).


```
GNU nano 2.8.7      File: /etc/squid/squid.conf      Modified
#
#Default:
# none

# TAG: httpd_suppress_version_string on/off
#       Suppress Squid version string info in HTTP headers and HTML error pages.
#
#Default:
# httpd_suppress_version_string off

# TAG: visible_hostname
#       If you want to present a special hostname in error messages, etc.,
#       define this. Otherwise, the return value of gethostname()
#       will be used. If you have multiple caches in a cluster and
#       get errors about IP-forwarding you must set them to have individual
#       names with this setting.
#
#Default:
visible_hostname proxy.sekolah.sch.id

#
# Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^X Cut Text  ^C Cur Pos
# Exit      ^J Justify   ^W Where Is  ^U Next Page  ^U UnCut Text ^T To Spell
```

Gambar 2.37 Konfigurasi visible_hostname

Keterangan

visible_hostname proxy.sekolah.sch.id
menentukan hostname (nama komputer) untuk server proxy yaitu proxy.sekolah.sch.id

e. Menentukan cache manager (email administrator dari proxy server

```
GNU nano 2.8.7      File: /etc/squid/squid.conf      Modified
#
#       during shutdown mode. Any active clients after this many
#       seconds will receive a 'timeout' message.
#
#Default:
# shutdown_lifetime 30 seconds

# ADMINISTRATIVE PARAMETERS
# -----
#
# TAG: cache_mgr
#       Email-address of local cache manager who will receive
#       mail if the cache dies. The default is "webmaster".
#
#Default:
cache_mgr jadmiko@ymail.com

# TAG: mail_from_
#       From: email-address for mail sent when the cache dies.
#       The default is to use 'appname@unique_hostname'.

#
# Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^X Cut Text  ^C Cur Pos
# Exit      ^J Justify   ^W Where Is  ^U Next Page  ^U UnCut Text ^T To Spell
```

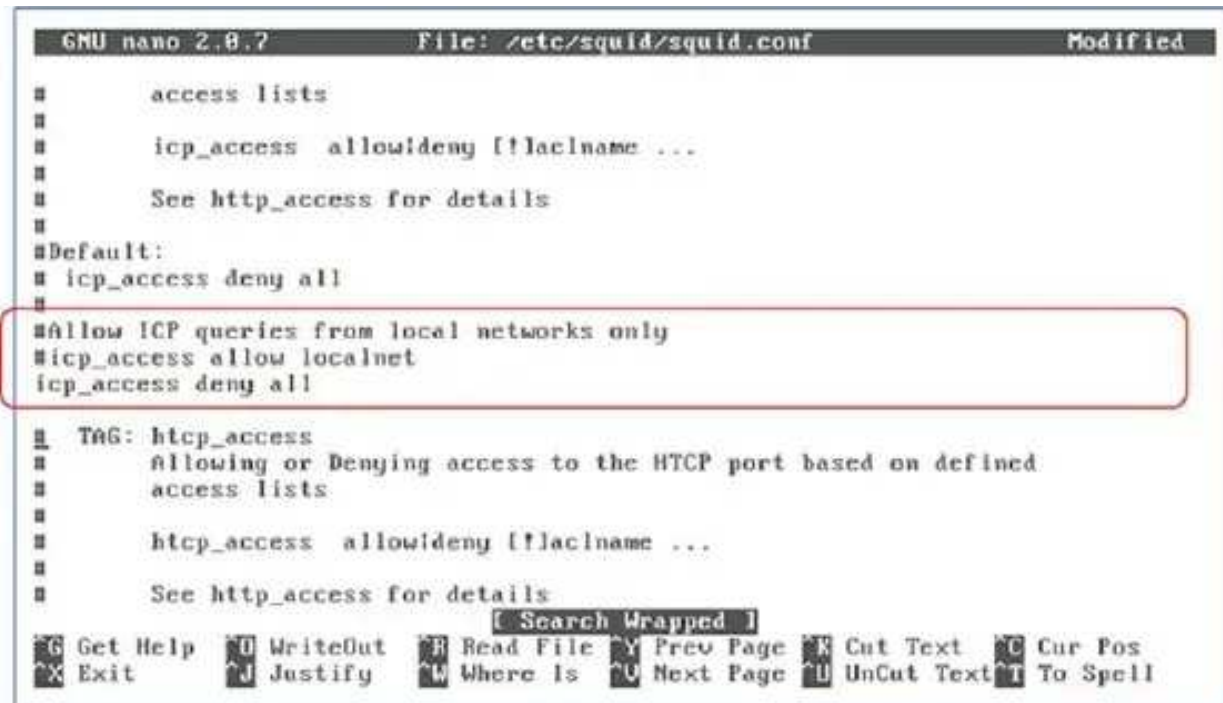
Gambar 2.38 Konfigurasi cache manager

Keterangan

cache_mgr jadmiko@ymail.com

Menentukan email administrator dari proxy server yaitu jadmiko@ymail.com

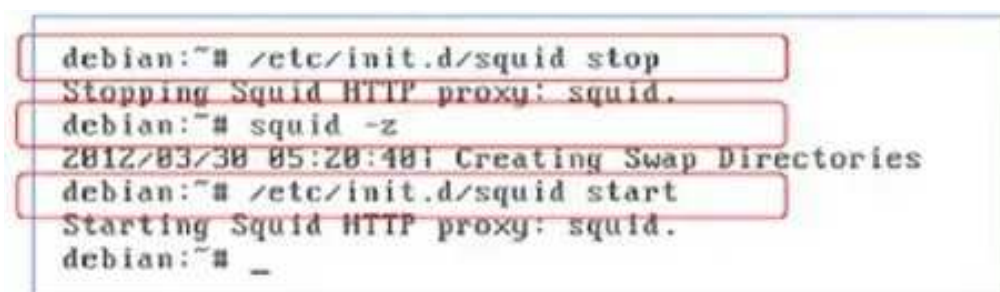
- f. Kemudian tutup / non aktifkan icp access untuk acl localnet, hal ini karena proxy server yang kita bangun tidak mempunyai hirarki (tingkatan).



```
GNU nano 2.8.7 File: /etc/squid/squid.conf Modified
#
# access lists
#
# icp_access allowdeny [!aclname ...
#
# See http_access for details
#
#Default:
# icp_access deny all
#
#Allow ICP queries from local networks only
#icp_access allow localnet
icp_access deny all
#
# TAG: http_access
#
# allowing or Denying access to the HTTP port based on defined
# access lists
#
# http_access allowdeny [!aclname ...
#
# See http_access for details
[ Search Wrapped ]
G Get Help  O WriteOut  R Read File  Y Prev Page  X Cut Text  C Cur Pos
X Exit      J Justify    W Where Is  U Next Page  U UnCut Text  T To Spell
```

Gambar 2.39 Menutup icp access

- g. Kemudian keluar dan simpan file tersebut. Selanjutnya buat direktori cache squid dengan perintah **#squid -z**, terlebih dahulu stop service squid dengan perintah **#/etc/init.d/squid stop**
- h. Kemudian jalankan kembali service squid dengan perintah **#/etc/init.d/squid start**



```
debian:~# /etc/init.d/squid stop
Stopping Squid HTTP proxy: squid.
debian:~# squid -z
2812/03/30 05:20:40: Creating Swap Directories
debian:~# /etc/init.d/squid start
Starting Squid HTTP proxy: squid.
debian:~# _
```

Gambar 2.40 Langkah menjalankan squid pertama kali

- i. Untuk memastikan tidak terdapat error, cek melalui file system log dengan perintah **#tail -f /var/log/syslog**

```

debian:~# /etc/init.d/squid restart
Restarting Squid HTTP proxy: squid.
debian:~# tail -f /var/log/syslog
Mar 30 05:17:23 debian dhcpd: DHCPACK on 192.168.100.10 to 08:50:56:c8:00:01 (jadmiko) via eth0
Mar 30 05:20:33 debian squid[2252]: Squid Parent: child process 2254 exited with status 0
Mar 30 05:21:03 debian squid[2339]: Squid Parent: child process 2341 started
Mar 30 05:22:24 debian dhcpd: DHCPREQUEST for 192.168.100.10 from 08:50:56:c8:00:01 (jadmiko) via eth0
Mar 30 05:22:24 debian dhcpd: DHCPACK on 192.168.100.10 to 08:50:56:c8:00:01 (jadmiko) via eth0
Mar 30 05:27:25 debian dhcpd: DHCPREQUEST for 192.168.100.10 from 08:50:56:c8:00:01 (jadmiko) via eth0
Mar 30 05:27:25 debian dhcpd: DHCPACK on 192.168.100.10 to 08:50:56:c8:00:01 (jadmiko) via eth0
Mar 30 05:31:40 debian dhcpd: DHCPRELEASE of 192.168.100.10 from 08:50:56:c8:00:01 (jadmiko) via eth0 (found)
Mar 30 05:31:59 debian squid[2339]: Squid Parent: child process 2341 exited with status 0
Mar 30 05:32:01 debian squid[2390]: Squid Parent: child process 2401 started

```

Gambar 2.41 Log system squid

- j. Kemudian kita lakukan pengalihan paket browsing agar masuk pada aplikasi proxy dengan menggunakan iptables, buka file rc.local dengan perintah **#pico /etc/rc.local** kemudian tambahkan script seperti berikut

```

GNU nano 2.0.7      File: /etc/rc.local      Modified
#!/bin/sh -e
#
# rc.local
#
# This script is executed at the end of each multiuser runlevel.
# Make sure that the script will "exit 0" on success or any other
# value on error.
#
# In order to enable or disable this script just change the execution
# bits.
#
# By default this script does nothing.

iptables -t nat -F
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
iptables -t nat -A PREROUTING -i eth1 -s 192.168.100.0/24 -p tcp --dport 80 -j S
exit 0

^G Get Help  ^O WriteOut  ^B Read File ^V Prev Page ^X Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^U Where Is  ^N Next Page ^_ UnCut Text ^T To Spell

```

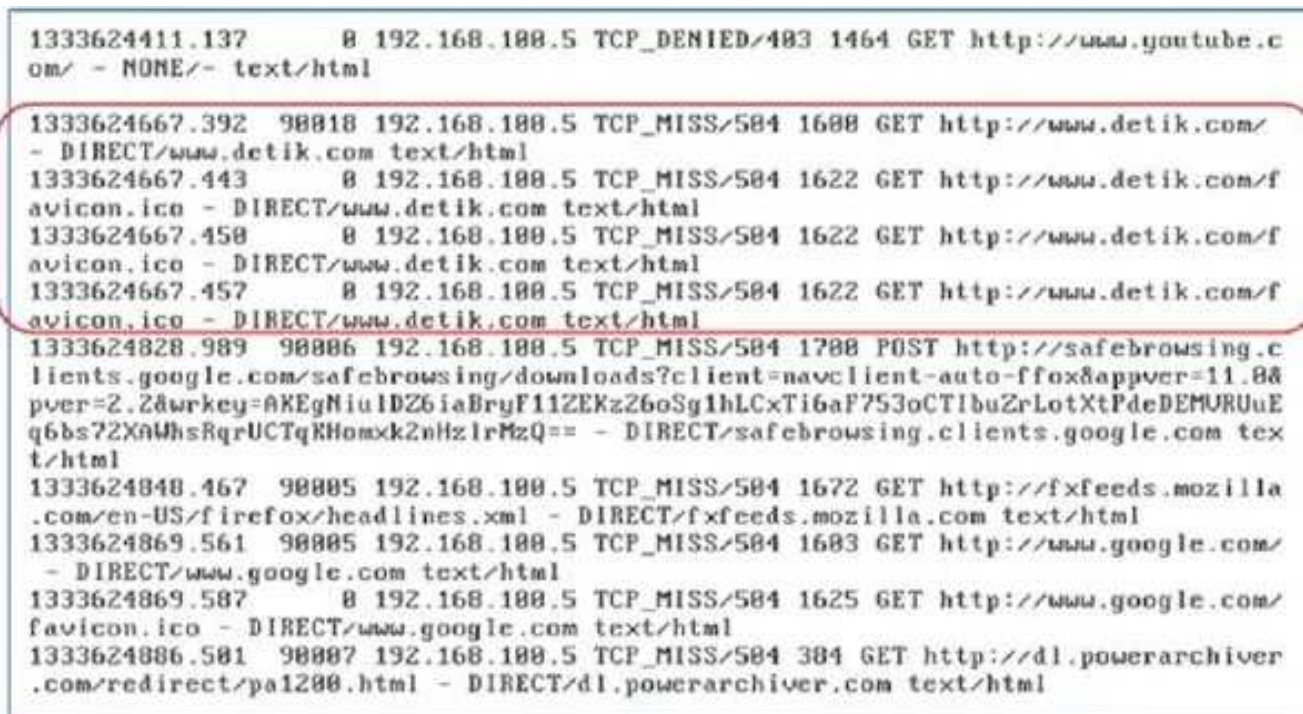
Gambar 2.42 Konfigurasi NAT untuk proxy

Keterangan

iptables -t nat -A PREROUTING -i eth1 -s 192.168.100.0/24 -p tcp --dport 80 -j REDIRECT -to-port 3128

Mengalihkan paket yang menuju port 80 (browsing) yang masuk ke eth1 yang berasal dari network 192.168.100.0/24 menuju port proxy server yaitu 3128

- k. Kemudian jalankan file **rc.local** dengan perintah **#/etc/rc.local** atau restart PC Server.
- l. Kemudian uji dengan browsing dari klien dan pada saat bersamaan buka file **access.log** untuk melihat aktifitas browsing klien dengan perintah **#tail -f /var/log/squid/access.log**



```

1333624411.137      0 192.168.100.5 TCP_DENIED/403 1464 GET http://www.youtube.c
om/ - NONE/- text/html
1333624667.392    90018 192.168.100.5 TCP_MISS/504 1600 GET http://www.detik.com/
- DIRECT/www.detik.com text/html
1333624667.443      0 192.168.100.5 TCP_MISS/504 1622 GET http://www.detik.com/f
avicon.ico - DIRECT/www.detik.com text/html
1333624667.450      0 192.168.100.5 TCP_MISS/504 1622 GET http://www.detik.com/f
avicon.ico - DIRECT/www.detik.com text/html
1333624667.457      0 192.168.100.5 TCP_MISS/504 1622 GET http://www.detik.com/f
avicon.ico - DIRECT/www.detik.com text/html
1333624828.989    90006 192.168.100.5 TCP_MISS/504 1700 POST http://safebrowsing.c
lients.google.com/safebrowsing/downloads?client=navclient-auto-ffox8appver=11.0&
pver=2.2&wrkey=AKEgNiuIDZ6iaBryF11ZEKz26oSg1hLCxTi6aF753oCTIbuZrLotXtPdeDEMURUuE
q6bs72XaWhsRqrUCTqKH0mxk2nHzlrMzQ== - DIRECT/safebrowsing.clients.google.com tex
t/html
1333624848.467    90005 192.168.100.5 TCP_MISS/504 1672 GET http://fxfeeds.mozilla
.com/en-US/firefox/headlines.xml - DIRECT/fxfeeds.mozilla.com text/html
1333624869.561    90005 192.168.100.5 TCP_MISS/504 1603 GET http://www.google.com/
- DIRECT/www.google.com text/html
1333624869.587      0 192.168.100.5 TCP_MISS/504 1625 GET http://www.google.com/
favicon.ico - DIRECT/www.google.com text/html
1333624886.501    90007 192.168.100.5 TCP_MISS/504 304 GET http://dl.powerarchiver
.com/redirect/pa1200.html - DIRECT/dl.powerarchiver.com text/html

```

Gambar 2.43 Log access squid

Keterangan

Dapat dilihat klien dengan IP Address sedang mengakses (browsing) situs **www.detik.com**

- m. Kemudian untuk melakukan pemblokiran terhadap situs-situs tertentu, maka kita tambahkan **acl** untuk memblokir situs-situs tersebut, misalkan kita akan memblokir situs **facebook.com** dan **youtube.com**. Perhatikan letak **acl** nya, tidak boleh salah karena script akan dibaca secara berurutan dari atas ke bawah. Pemblokiran ini dapat berdasarkan alamat tujuan (domain) seperti **www.facebook.com**, artinya klien tidak diizinkan mengakses situs dengan alamat **www.facebook.com**.
Pada pengembangan lebih lanjut pemblokiran tidak hanya berdasarkan alamat situs, tetapi juga dapat berdasarkan kata, misalkan kata porno, jadi setiap alamat situs yang terdapat kata porno akan diblokir. Lebih lanjut jika

jumlah situs yang akan diblokir banyak maka kita dapat buat file terpisah untuk menuliskan daftar situs-situs yang diblokir tersebut sehingga lebih mudah dalam pengelolaannya.



```
GNU nano 2.8.7 File: /etc/squid/squid.conf Modified
# from where browsing should be allowed
#http_access allow localnet
http_access allow localhost

acl situsdilarang dstdomain -i www.facebook.com www.youtube.com

http_access deny situsdilarang

acl jaringanku src 192.168.100.0/24
http_access allow jaringanku

# And finally deny all other access to this proxy
http_access deny all

# TAG: http_access2
#   Allowing or Denying access based on defined access lists
#
#   Identical to http_access, but runs after redirectors. If not set
#   then only http_access is used.
#

G Get Help  O WriteOut  R Read File  Y Prev Page  E Cut Text  C Cur Pos
X Exit      J Justify    W Where Is  U Next Page  U UnCut Text  T To Spell
```

Gambar 2.44 Konfigurasi blokir situs

Keterangan

1. **acl situsdilarang dstdomain -i www.facebook.com www.youtube.com**
membuat acl dengan nama situsdilarang yang isinya alamat situs yang tidak boleh diakses www.facebook.com dan www.youtube.com. Option -i berarti incase sensitive, yang akan menganggap sama antara huruf besar dan huruf kecil.
 2. **http_access deny situsdilarang**
menutup akses http klien untuk acl situsdilarang
- n. Reconfigure squid dengan perintah **#squid -k reconfigure**, perintah ini harus dijalankan setiap ada perubahan konfigurasi squid. Tujuannya untuk membaca ulang konfigurasi squid tanpa melakukan restart terhadap service squid.

```
debian:~# squid -k reconfigure
debian:~# _
```

- o. Kemudian uji pada klien dengan browsing kepada alamat yang kita blokir tadi



Gambar 2.45 Tampilan situs yang diblokir

- p. Maka akan tampil halaman yang menunjukkan akses terhadap situs youtube.com diblokir oleh proxy. Perhatikan juga email administrator dan hostname dari server proxy sesuai dengan yang dikonfigurasi pada file squid.conf
- q. Untuk konfigurasi lainnya dapat dikembangkan lebih lanjut agar proxy server dapat bekerja lebih maksimal terutama untuk menjalankan fungsi caching untuk meningkatkan kecepatan akses internet klien dan menghemat bandwidth yang kita miliki.

Rangkuman

VLAN (Virtual Local Area Network) merupakan sekelompok perangkat pada satu LAN atau lebih yang dikonfigurasi (menggunakan perangkat lunak pengelolaan) sehingga dapat berkomunikasi seperti halnya bila perangkat tersebut terhubung ke jalur yang sama, padahal sebenarnya perangkat tersebut berada pada sejumlah segmen LAN yang berbeda.

Berikut ini beberapa keuntungan menggunakan VLAN:

- Security** : keamanan data dari setiap divisi dapat dibuat tersendiri, karena segmennya bisa dipisah secara logika. Lalu lintas data dibatasi segmennya.
- Cost reduction** : penghematan biaya dihasilkan dari tidak diperlukannya biaya yang mahal untuk upgrades jaringan dan efisiensi penggunaan bandwidth dan uplink yang tersedia.

- c. *Higher performance* : pembagian jaringan layer 2 ke dalam beberapa kelompok broadcast domain yang lebih kecil, yang tentunya akan mengurangi lalu lintas packet yang tidak dibutuhkan dalam jaringan.
- d. *Broadcast storm mitigation* : pembagian jaringan ke dalam VLAN-VLAN akan mengurangi banyaknya device yang berpartisipasi dalam pembuatan broadcast storm. Hal ini terjadinya karena adanya pembatasan broadcast domain.
- e. *Improved IT staff efficiency* : VLAN memudahkan manajemen jaringan karena pengguna yang membutuhkan sumber daya yang dibutuhkan berbagi dalam segmen yang sama.
- f. *Simpler project or application management* : VLAN menggabungkan para pengguna jaringan dan peralatan jaringan untuk mendukung perusahaan dan menangani permasalahan kondisi geografis.

Secara prinsip proses routing itu tidaklah sulit, mudah untuk dipelajari dan prinsip routing sifatnya universal, berlaku sama pada semua kondisi network. Sulit atau gampangya melakukan routing tergantung pada kondisi tingkat kompleksitas sebuah network.

Routing Statik yaitu routing yang konfigurasinya harus dilakukan secara manual, administrator jaringan harus memasukkan atau menghapus rute statis jika terjadi perubahan topologi.

Dynamic router (*router* dinamis): adalah sebuah *router* yang memiliki dab membuat tabel *routing* dinamis, dengan mendengarkan lalu lintas jaringan dan juga dengan saling berhubungan dengan *router* lainnya.

Gateway atau yang sering disebut juga dengan “Gerbang Jaringan” merupakan sebuah perangkat yang dapat memudahkan pengguna komputer dan internet. Salah satu aplikasi atau contoh dari penggunaan Gateway yang dapat kita lihat adalah pada Email.

Secara umum Gateway berfungsi untuk menghubungkan sebuah jaringan komputer dengan jaringan komputer yang lain dengan protocol yang berbeda. Gateway dapat digunakan dalam menghubungkan IBM SNA dengan digital SNA, Local Area Network atau LAN dengan Wide Area Network atau WAN. Namun, terdapat pula beberapa fungsi dari

Firewall adalah perangkat yang digunakan untuk mengontrol akses terhadap siapapun yang memiliki akses terhadap jaringan privat dari pihak luar. Saat ini, pengertian firewall difahami sebagai sebuah istilah generik yang merujuk pada fungsi firewall sebagai sistem pengatur komunikasi antar dua jaringan yang berlainan.

Firewall adalah *sistem keamanan jaringan komputer* yang digunakan untuk melindungi komputer dari beberapa jenis serangan dari komputer luar.

Sebelum memahami fungsi firewall mari kita fahami atribut pentingnya sbb:

- a. Semua jaringan komunikasi melewati fire wall
- b. Hanya lalu lintas resmi diperbolehkan oleh fire wall
- c. Memiliki kemampuan untuk menahan serangan Internet

Fungsi firewall sebagai pengontrol, mengawasi arus paket data yang mengalir di jaringan. Fungsi Firewall mengatur, memfilter dan mengontrol lalu lintas data yang diizinkan untuk mengakses jaringan privat yang dilindungi, beberapa kriteria yang dilakukan fire-wall apakah memperbolehkan paket data lewat atau tidak, antara lain :

- a. Alamat IP dari komputer sumber
- b. Port TCP/UDP sumber dari sumber.
- c. Alamat IP dari komputer tujuan.
- d. Port TCP/UDP tujuan data pada komputer tujuan
- e. Informasi dari header yang disimpan dalam paket data.

Secara sfesifik Fungsi Firewall adalah melakukan autentifikasi terhadap akses ke jaringan. Aplikasi proxy Fire-wall mampu memeriksa lebih dari sekedar header dari paket data, kemampuan ini menuntutnya untuk mampu mendeteksi protokol aplikasi tertentu yang spesifikasi.

Ada sebuah jaringan yang mempunyai banyak client, diperlukan sebuah mekanisme pengaturan bandwidth dengan tujuan mencegah terjadinya monopoli penggunaan bandwidth sehingga semua client bisa mendapatkan jatah bandwidth masing-masing. QOS(Quality of services) atau lebih dikenal dengan Bandwidth Manajemen, merupakan metode yang digunakan untuk memenuhi kebutuhan tersebut.

Load balancing 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.

Load balancer (perangkat load balancing) menggunakan beberapa peralatan yang sama untuk menjalankan tugas yang sama. Hal ini memungkinkan pekerjaan dilakukan dengan lebih cepat dibandingkan apabila dikerjakan oleh hanya 1 peralatan saja dan dapat meringankan beban kerja peralatan, serta mempercepat waktu respons.

Server adalah sebuah sistem komputer yang menyediakan jenis layanan tertentu dalam sebuah jaringan komputer. Server didukung dengan prosesor yang bersifat *scalable* dan RAM yang besar, juga dilengkapi dengan sistem operasi khusus, yang disebut sebagai sistem operasi jaringan.

Umumnya, di dalam sistem operasi server terdapat berbagai macam layanan yang menggunakan arsitektur klient/server. Contoh dari layanan ini adalah Protokol Konfigurasi Hos Dinamik, server surat, server PTH, server PTB, DNS server, dan lain sebagainya. Setiap sistem operasi *server* umumnya membundel layanan-layanan tersebut, meskipun pihak ketiga dapat pula membuat layanan tersendiri. Setiap layanan tersebut akan merespon *request* dari klien. Sebagai contoh, klien PKHD akan memberikan *request* kepada server yang menjalankan layanan server PKHD; ketika sebuah klien membutuhkan alamat IP, klien akan memberikan *request* kepada server, dengan bahasa yang dipahami oleh server PKHD, yaitu protokol PKHD itu sendiri.

Server biasanya terhubung dengan klien dengan kabel UTP dan sebuah kartu jaringan. Kartu jaringan ini biasanya berupa kartu PCI atau ISA. Dilihat dari fungsinya, server bisa di kategorikan dalam beberapa jenis, seperti: server aplikasi, server data maupun server proksi. Server aplikasi adalah server yang digunakan untuk menyimpan berbagai macam aplikasi yang dapat diakses oleh klien, server data sendiri digunakan untuk menyimpan data baik yang digunakan klien secara langsung maupun data yang diproses oleh server aplikasi. Server proksi berfungsi untuk mengatur lalu lintas di jaringan melalui pengaturan proksi. Orang awam lebih mengenal proxy server untuk mengkoneksikan komputer klien ke Internet.