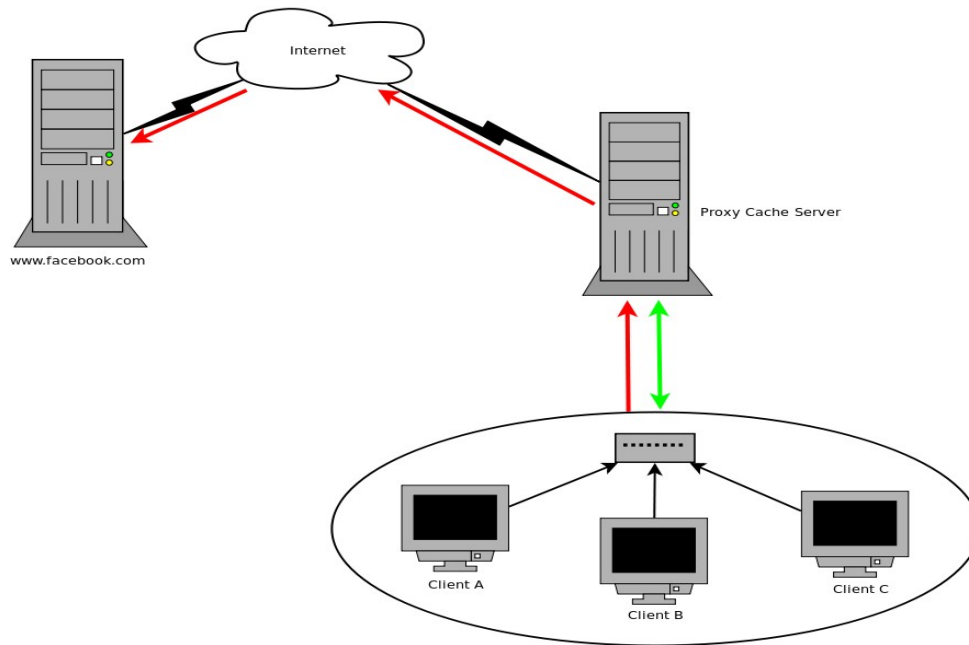


Mengenal Proxy Server

Proxy umumnya digunakan untuk memberikan layanan caching ke jaringan lokal, dengan menggunakan squid cache client-client proxy tidak perlu mengakses langsung halaman web yang ditujunya, melainkan cukup dengan mengambilnya di cache server (proxy), cara kerjanya adalah ketika ada client yang mengakses suatu alamat web, misalkan client A mengakses ke alamat www.facebook.com, maka squid akan menyimpan file-file halaman web tersebut ke dalam cache lokal proxy tersebut, ketika ada client lain, misalkan Client B mengakses halaman web yang sama dari www.facebook.com maka proxy server hanya melakukan pengecekan ke server yang dituju (www.facebook.com), apakah obyek yang disimpan di cache local proxy masih sama dengan yang ada di server web tujuan, apabila tidak ada perubahan obyek pada server maka proxy akan memberikan obyek yang diminta ke client B tersebut, dan apabila ternyata telah ada perubahan barulah proxy server memintakanya ke server (www.facebook.com) untuk Client B yang mengakses server web tersebut, sementara itu file yang diberikan kepada client tersebut juga akan disimpan di direktori cache pada proxy sever, dan begitu seterusnya sehingga secara tidak langsung metode ini akan menghemat bandwidth dan secara tidak langsung akan mempercepat koneksi internet.

Selain fungsi caching, proxy server juga dapat digunakan untuk membuat kebijakan keamanan untuk jaringan lokal, misalkan dengan membatasi content yang di akses oleh client. Aplikasi proxy server yang paling populer digunakan adalah squid, dikarenakan squid memiliki tingkat performa yang baik dan keamanan yang relatif lebih baik daripada aplikasi-aplikasi proxy server lainnya. Skema cara kerja proxy secara sederhana dapat digambarkan seperti berikut



Instalasi Paket Squid dari Repository

Untuk memudahkan kita dalam menginstall squid proxy server maka kita akan menggunakan instalasi squid dari repository dengan menggunakan yum, adapun cara instalasi squid melalui yum adalah sebagai berikut

```
yum install squid
```

jika tidak terjadi kesalahan dalam proses instalasi maka seharusnya squid telah terinstal dengan baik di sistem, untuk melakukan pengecekan file-file hasil instalasi squid kita dapat menggunakan perintah rpm berikut

```
rpm -ql squid
```

dengan perintah diatas maka akan terlihat dimana saja file-file instalasi squid yang baru saja kita install diletakan di sistem kita.

Instalasi Squid dari Source

Alasan yang sering digunakan oleh para administrator untuk lebih memilih melakukan instalasi squid dari source adalah untuk lebih menyesuaikan opsi-opsi instalasi yang bertujuan adalah meningkatkan performa squid itu sendiri, sebelum kita menginstall squid dari source tentunya kita membutuhkan source squid yang nantinya akan kita compile, source squid dapat kita unduh dari

<http://squid-cache.org>, setelah source squid kita dapatkan maka selanjutnya dalam mengekstraknya dengan perintah berikut

```
tar -xvzf squid-2.7.STABLE7.tar.gz
```

Setelah proses ekstrak selesai maka selanjutnya kita masuk ke direktori hasil ekstrak dan jalankan perintah configure untuk mensetup squid sebelum kita install

```
cd squid-2.7.STABLE7  
./configure
```

Untuk melihat opsi-opsi apa saja yang bisa kita tambahkan ketika kita menjalankan perintah configure, kita bisa menggunakan perintah berikut

```
./configure -help
```

Setelah itu jika tidak terjadi error lanjutkan dengan menjalankan perintah make untuk mengkompilasi squid

```
make
```

Kemudian install dengan perintah make install

```
make install
```

Konfigurasi Squid

Setelah proses instalasi squid proxy server selesai maka yang harus kita lakukan selanjutnya adalah menyesuaikan konfigurasi default squid agar sesuai dengan kebutuhan kita, adapun file konfigurasi squid pada distribusi CentOS Linux terdapat di `/etc/squid/squid.conf`.

Berikut adalah beberapa opsi-opsi konfigurasi dasar yang harus kita sesuaikan

Access Control list (ACL)

```
acl local_net src 192.168.1.0/24  
http_access allow local_net
```

Opsi diatas dapat dijelaskan sebagai berikut :

Pernyataan `acl *local_net src*` menunjukan jaringan local kita yang akan kita perbolehkan untuk mengakses mesin proxy server, sebagai contoh disini kita hanya akan mengizinkan jaringan

192.168.1.0/24 yang diperbolehkan mengakses proxy server

Pernyataan **http_access allow local_net** harus diletakan sebelum baris **http_access deny all**. berikut contoh penggunaan acl dalam squid

```
acl local_net src 192.168.1.0/24

http_access allow localhost
http_access allow local_net
http_access deny all
```

Logging

Secara default squid akan membuat beberapa file log yang berhubungan dengan aktifitas squid itu sendiri, dan berikut adalah konfigurasi default squid yang digunakan

```
access_log /var/log/squid/access.log squid
cache_log /var/log/squid/cache.log
cache_store_log none
```

Dengan opsi diatas squid akan menyimpan pesan-pesan error dalam file /var/log/squid/cache.log, kemudian informasi akses dari client akan disimpan dalam file access_log /var/log/squid/access.log dan pada bagian opsi cache store log karena tidak terlalu penting maka kita dapat menonaktifkannya dengan mengisikan opsi none sehingga menjadi cache_store_log none

Cache Managemen

Pada bagian ini merupakan opsi konfigurasi yang digunakan untuk melakukan manajemen cache, adapun opsi penting yang harus kita perhatikan adalah sebagai berikut

```
cache_dir ufs /var/spool/squid 100 16 256
```

Keterangan opsi diatas adalah menentukan letak (path) dari direktori cache yang akan kita gunakan, sedangkan ufs merupakan metode cache storing yang nantinya akan digunakan, ada beberapa metode yang dapat digunakan dalam opsi ini, yaitu ufs,aufs dan diskd, opsi selanjutnya menentukan besaran ukuran direktori yang nantinya akan dialokasikan untuk menaruh cache squid, ukuran yang digunakan disini adalah MegaByte(MB), sehingga apabila kita mengisinya dengan 100, maka berarti kita akan mengalokasikan direktori untuk meletakkan cache squid sebesar 100MB, opsi selanjutnya adalah jumlah direktori tree yang akan kita buat dalam directory cache, pada contoh diatas kita

mengisinya dengan 16 dan 254, maka artinya di dalam direktori cache nantinya akan memiliki jumlah direktori sebanyak 16 dan masing-masing direktori akan memiliki sub direktori sebanyak 254.

Berkomunikasi Dengan Proxy Server Eksternal

Squid mempunyai fasilitas yang memungkinkan kita untuk menghubungkan proxy server kita dengan proxy server lain (eksternal) tentunya dengan tujuan untuk meningkatkan performa caching agar lebih baik. Metode komunikasi antar proxy server yaitu dengan menggunakan port ICP yang menggunakan protokol UDP, sehingga antara beberapa proxy server yang saling terhubung bisa saling bertukar cache file, adapun model yang dapat digunakan ada dua macam, yaitu parent dan sibling.

Parent

Pada model ini berarti proxy kita hanya akan meminta ke proxy yang berfungsi sebagai parent, apabila obyek yang dicari ditemukan maka obyek itu akan kita mintakan dari cache parent proxy kita, namun tidak sebaliknya, opsinya adalah sebagai berikut

```
cache_peer ip_parent_proxy type (parent|sibling) proxy_port icp_port  
opsi
```

Contoh penggunaan dari parent proxy adalah sebagai berikut

```
cache_peer 10.55.1.50 parent 3128 7 no-query
```

keterangan dari opsi diatas adalah sebagai berikut, cache_peer merupakan opsi yang digunakan agar proxy server kita bisa berkomunikasi dengan proxy eksternal, ip 10.55.1.50 disini merupakan parent proxy yang akan kita mintai cache file-nya, parent merupakan type dari proxy peer (parent| sibling), 3128 merupakan proxy port, 7 merupakan ICP port dan no-query merupakan contoh opsi yang dapat kita gunakan, yang berarti kita tidak akan meminta icp (icp query)

Sibling

Berbeda dengan type parent, pada tipe ini berarti kita akan saling bertukar cache file antara proxy server kita dan proxy server eksternal yang akan kita ajak bekerja sama, penggunaan opsi pada type ini hampir sama, hanya saja pada bagian parent kita ganti dengan sibling agar proxy kita dan proxy eksternal bisa saling bertukar cache, contoh penggunaan opsi sibling

```
cache_peer 10.55.1.50 sibling 3128 7 no-query
```

Content Filtering Menggunakan Squid

Seperti yang telah disinggung sebelumnya, selain difungsikan sebagai cache server, squid juga dapat sekaligus berfungsi sebagai content filtering untuk mengeblok alamat-alamat situs yang tidak boleh di akses oleh client. Opsi yang digunakan pada dasarnya adalah hanya dengan memanfaatkan fitur ACL pada squid, contoh penggunaannya adalah sebagai berikut

```
acl block dstdomain "/etc/squid/block"  
  
http_access deny block
```

Sedangkan isi dari file /etc/squid/block adalah alamat-alamat situs yang akan kita larang untuk di akses oleh clien proxy, contoh isi file block adalah sebagai berikut

```
rapidshare.com  
facebook.com  
friendster.com  
indowebster.com
```

Setelah ini maka alamat-alamat yang terdapat di dalam file /etc/squid/block tidak akan dapat diakses lagi oleh client dengan pesan error access denied, selain alamat-alamat yang dapat kita block sebenarnya kita juga dapat memblok ekstensi-ekstensi file yang akan kita larang untuk di akses oleh client dengan jam dan pada hari-hari tertentu, berikut adalah contoh untuk memblock beberapa ekstensi file yang akan kita larang untuk di akses oleh client pada jam dan hari tertentu

```
acl blok url_regex -i \.mpeg$ \.avi$ \.mpg$  
acl jam_kerja time MTWHF 08:00-16:00  
  
http_access deny blok jam_kerja
```

Keterangan opsi diatas adalah sebagai berikut :

kita akan menolak client mengakses file-file dengan ekstensi mpeg, avi dan mpg pada hari senin sampai jumat (MTWHF) mulai jam 08-14.

Autentikasi

Otentikasi pada squid dapat digunakan untuk memberi batasan user-user mana saja yang boleh mengakses proxy server dan user mana yang diperbolehkan, untuk mengaktifkan autentikasi kita memerlukan otentikator yang akan menangani urusan autentikasi, berikut adalah contoh konfigurasi squid untuk menangani autentikasi menggunakan metode autentikasi NCSA

```
auth_param basic program /usr/local/libexec/ncsa_auth
/etc/squid/auth_squid
acl ugos proxy_auth REQUIRED

http_access allow ugos
```

Dari opsi konfigurasi diatas dapat dijelaskan sebagai berikut :

Opsi `auth_param basic program` merupakan parameter autentikasi, `/etc/squid/auth_squid` merupakan file dimana kita akan meletakkan daftar user yang akan kita perbolehkan untuk menggunakan squid, pada bagian `acl ugos proxy_auth REQUIRED` dan `http_access allow ugos` merupakan format acl squid untuk penanganan autentikasi yang berarti selain user yang terautentikasi maka tidak akan di izinkan untuk menggunakan proxy squid, dan berikut adalah konfigurasi autentikasi dengan menggunakan ldap

```
/usr/lib/squid/squid_ldap_auth -b "dc=domain,dc=com" -f "uid=%s"
ldap.server.com
```

dimana ***ldap.server.com*** merupakan ldap server yang memberikan layanan autentikasi, pada opsi ini kita bisa menggunakan ip server ldap atau domainnya.

Konfigurasi Transparent Proxy

Transparent proxy merupakan metode dimana kita menempatkan proxy server diantara jaringan LAN dan jaringan internet kemudian semua koneksi web dari jaringan LAN yang menuju internet akan secara otomatis di belokan untuk dipaksa melalui proxy server kita, metode ini akan mempermudah kita dalam melakukan pengaturannya, karena dengan menggunakan metode ini kita tidak harus menseting client satu-persatu untuk menggunakan proxy server, dan metode ini sangat cocok untuk penerapan kebijakan keamanan krena client mau atau tidak mau harus melewati proxy untuk mengakses internet, dan berikut adalah seting squid dan juga iptables untuk konfigurasi transparent proxy.

Agar squid bisa menjalankan fungsi transparent proxy maka kita perlu menambahkan baris berikut ke file konfigurasi squid

```
http_port 3128 transparent
```

kemudian kita harus menambahkan rules iptables berikut :

```
/sbin/iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j  
REDIRECT --to-port 3128  
/sbin/iptables -t nat -A PREROUTING -i eth0 -p udp --dport 80 -j  
REDIRECT --to-port 3128
```

dengan menggunakan rules diatas maka semua koneksi (tcp/udp) yang menuju port 80 akan secara otomatis di belokan ke port proxy server (3128).

Menjalankan Squid

Ketika kita pertama kali akan menjalankan squid maka kita harus menjalankan perintah berikut agar squid membuat file cache terlebih dahulu.

```
squid -z
```

Kemudian untuk menjalankan squid kita dapat menggunakan perintah berikut

```
/etc/inint.d/squid start
```

atau menggunakan perintah service

```
/sbin/service squid start
```

atau apabila kita menginstall squid dari source maka kita menjalankan squid dengan perintah berikut

```
/usr/local/sbin/squid
```

Kemudian untuk mematikan service squid jalankan perintah berikut

```
/etc/inint.d/squid stop
```


atau dengan menggunakan perintah service

```
/sbin/service squid stop
```

atau apabila kita menginstall squid dari source maka jalankan perintah berikut

```
/usr/local/sbin/squid -k shutdown
```

Apabila tidak terdapat error dalam file konfigurasi seharusnya squid telah berjaan dengan baik.